Security Management using Amazon Web Services (AWS) – Lab Manual

How to Create an AWS Account?

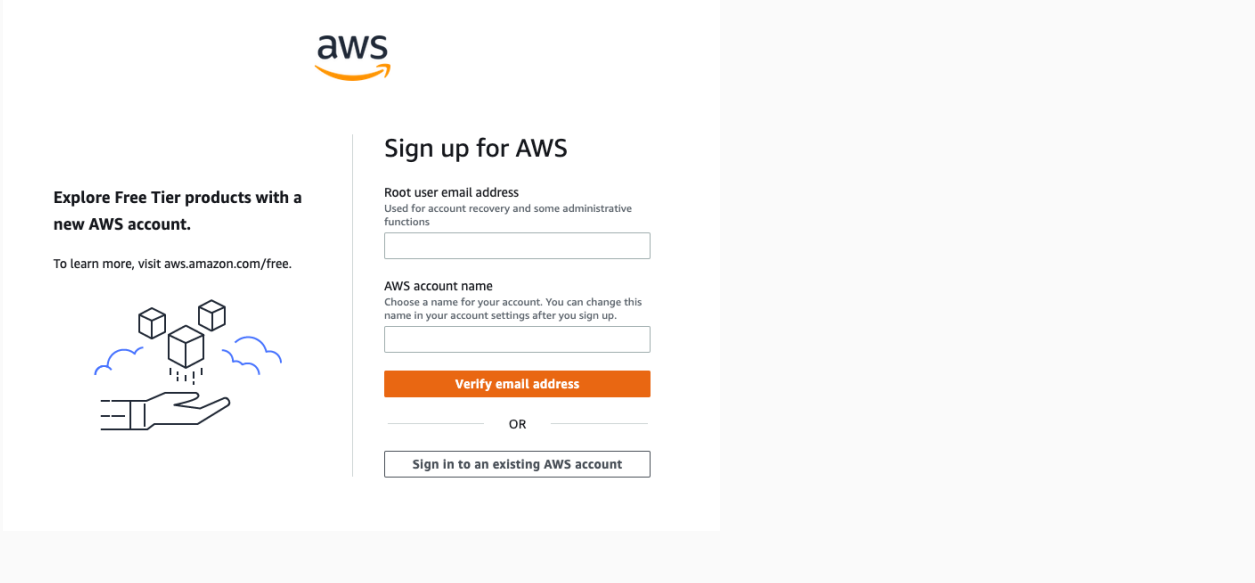
To create a new AWS account, go to aws.amazon.com and choose Create an AWS Account.

1 - Enter an email address and an account name.

> Carefully consider which email address you want to use. If you are setting up a personal account, AWS don't recommend using a work email address because you may change jobs at some point. Conversely, for business accounts, AWS recommend using an email alias that can be managed because the person setting up the account may, at some point, change roles or companies.

2 - Select Verify email address.

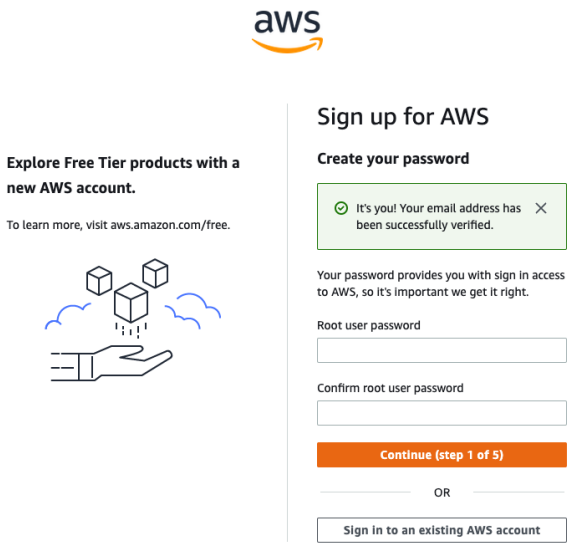
> You will get a verification code in your email. Enter the verification code and choose Verify.
>
> You will be redirected to a new screen where you will create your root user password.



3 - Create your root user password.

> The password you choose is extremely sensitive and should be shared only with people who have access to the credit card that will be used on this account.
>
> Your password must include uppercase letters, lowercase letters, numbers, and non-alphabetic characters.

4 - Once you have entered and confirmed your password, choose Continue (step 1 of 5).



5 - Now you need to add your contact information and select how you plan to use AWS.

a) - Choose between a business or personal account.

There is no difference in account type or functionality, but there is a difference in the type of information required to open the account for billing purposes.

For a business account, choose a phone number that is tied to the business and can be reached if the person setting up the account is not available.

b) - Once you have selected the account type, fill out the contact information about the account.

Save these details in a safe place. If you ever lose access to the email or your two-factor authentication device, AWS Support can use these details to confirm your identity.

c) - At the end of this form, please read through the terms of the AWS Customer Agreement and select the checkbox to accept them.

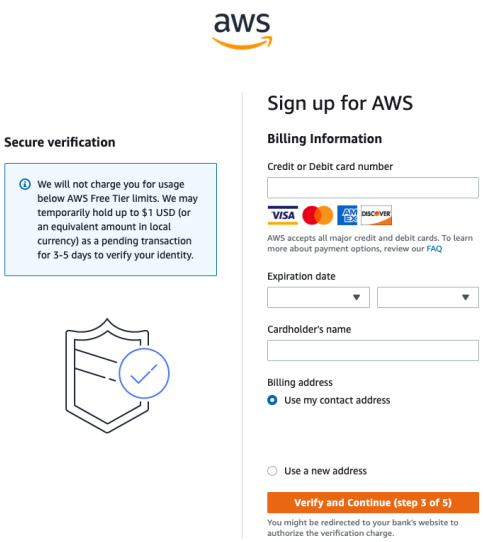
d) - Choose Continue (step 2 of 5) to proceed to the next screen.

6 - In the following screen, add your preferred credit or debit card to use for payment.

a) - Enter your Billing Information details.

A small hold will be placed on the card, so the address must match what your financial institution has on file for you or your business.

b) - Select Verify and Continue (step 3 of 5) to proceed.



7 - Now you need to verify your account.

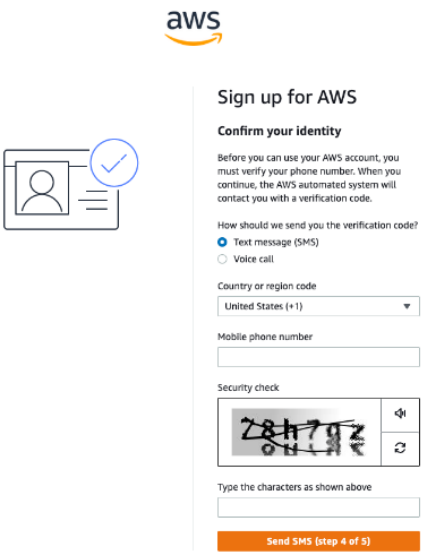
a) - Choose how you want to confirm your identity.

You can verify your account either through a text message (SMS) or a voice call on the number you are associated with this account.

For the text message (SMS) option, you will be sent a numeric code to enter on the next screen after you choose Send SMS.

For the Voice call option, you will be shown a code on the screen to enter after being prompted by the automated voice verification system.

b) - Enter the code as appropriate for your verification choice, then choose Continue to proceed to the final step.



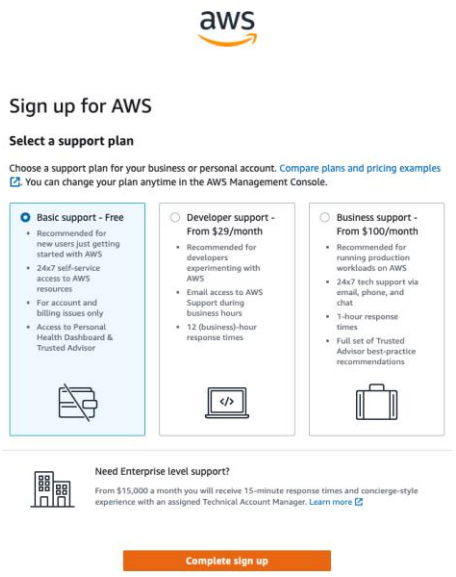
8 - Choose a support plan for your AWS account.

a) - Choose a support plan. For this tutorial, we recommend the default selection.

You have three options for support plans. The default option is called Basic Support and is free of charge. If you are not sure, select Basic Support. You can always change support tiers at a later date.

To see the full list of differences between the tiers, see Compare AWS Support Plans.

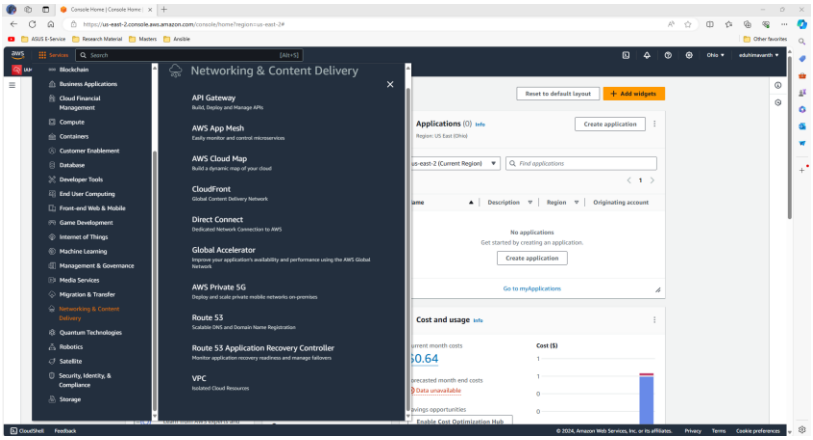
b) - To finish creating your account, choose Complete sign up.



Creating a Virtual Private Cloud (VPC):

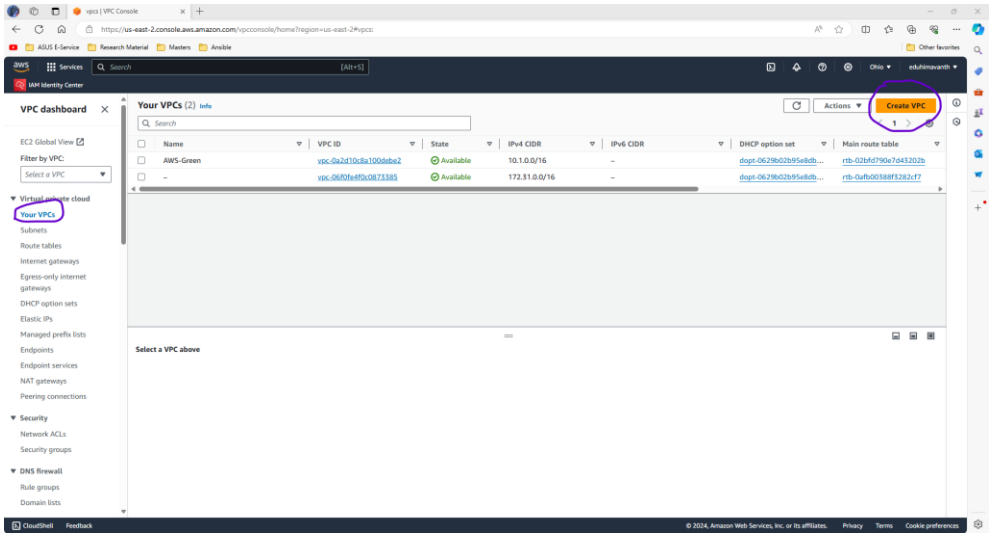
1 - Navigate to the VPC Dashboard

- In the top navigation bar, click on "Services."
- Under "Networking & Content Delivery," select "VPC."



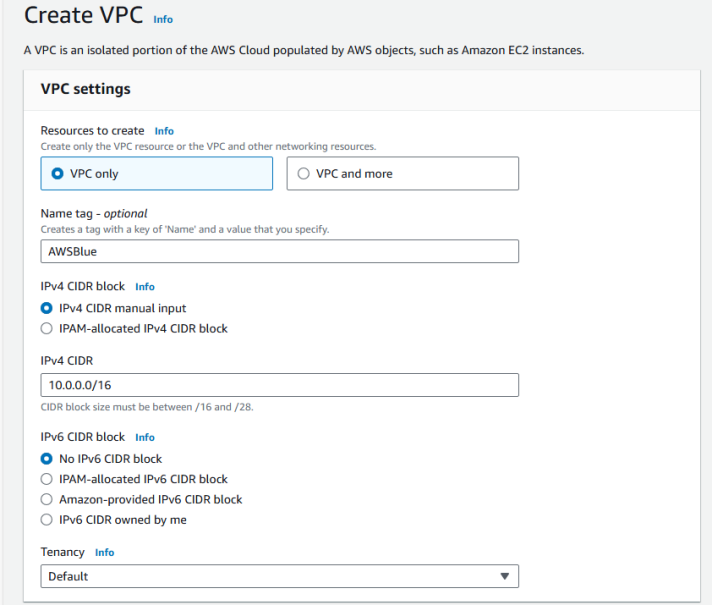
2 - Create a VPC

- In the VPC Dashboard, click on "Your VPCs" in the left-hand navigation pane.
- Click on the "Create VPC" button.



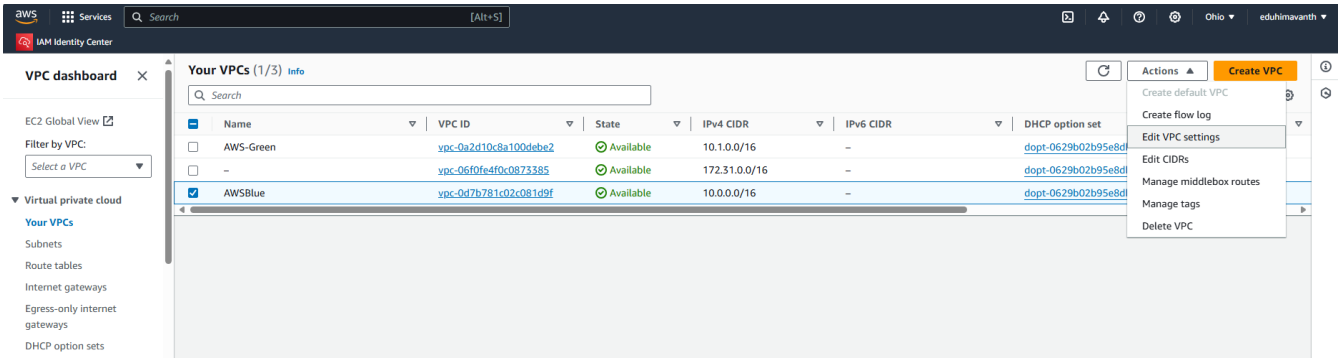
3 - Configure the VPC

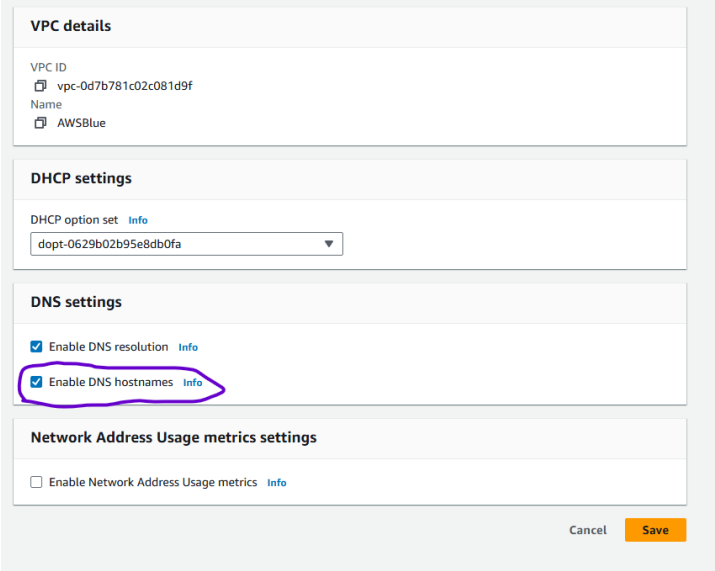
- **Name Tag:** Provide a name for your VPC.
- **IPv4 CIDR block:** Enter the IPv4 CIDR block (e.g., 10.0.0.0/16).
- **IPv6 CIDR block:** Leave it as "No IPv6 CIDR Block" for now (optional).
- **Tenancy:** Choose "Default" unless you have specific requirements for dedicated instances.
- Click "Create VPC.



4 - Enable DNS Hostnames

- Select your newly created VPC from the list.
- Click on "Actions," then select "Edit DNS Resolution."
- Ensure "Enable DNS resolution" is checked.
- Click "Save."
- Next, click on "Actions" again and select "Edit DNS Hostnames."
- Ensure "Enable DNS hostnames" is checked.
- Click "Save."





This allows instances launched into the VPC to receive DNS hostnames, which is useful for DNS resolution.

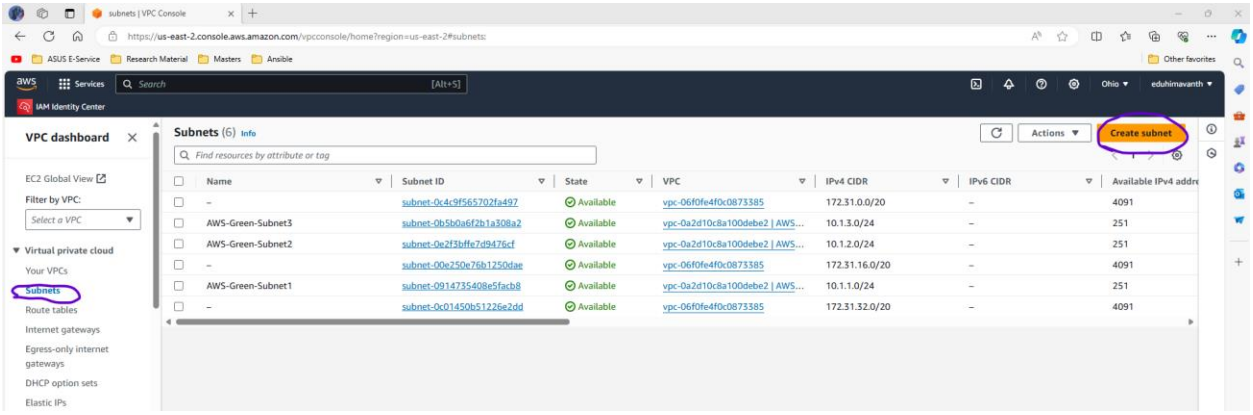
Creating Subnets:

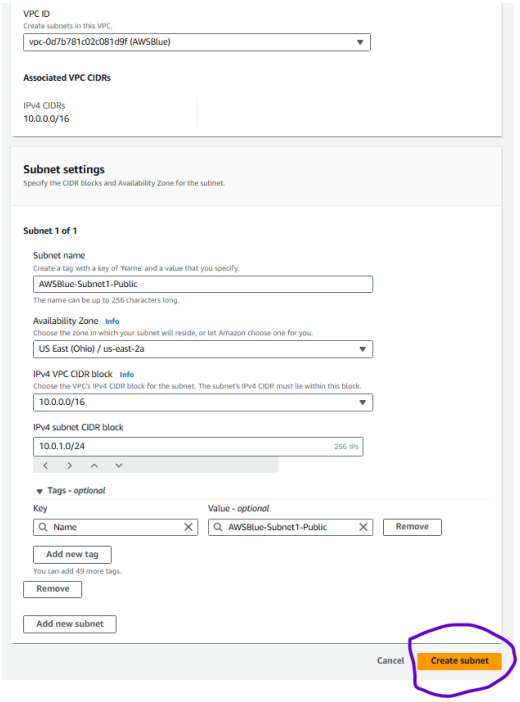
As we have created a VPC, we will now create Subnets. We will create 3 subnets (1-Private; 2-Public).

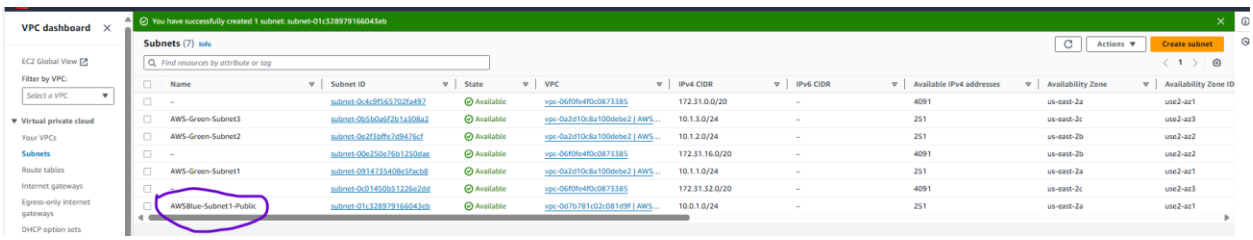
1 - Creating Public Subnet 1

- In the VPC Dashboard, click on "Subnets" in the left-hand navigation pane.
- Click on the "Create subnet" button.

- **Name Tag:** Enter a name for the first public subnet (e.g., Public-Subnet-1).
- **VPC:** Select your VPC from the dropdown list.
- **Availability Zone:** Choose an availability zone (e.g., us-east-1a).
- **IPv4 CIDR block:** Enter a subnet CIDR block for the first public subnet (e.g., 10.0.1.0/24).
- Click "Create subnet."

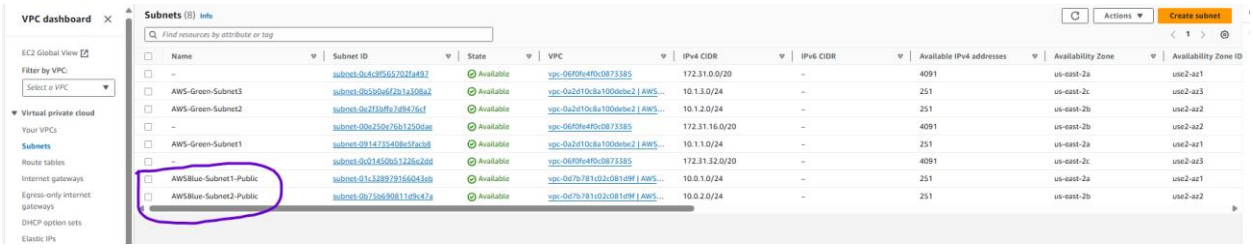






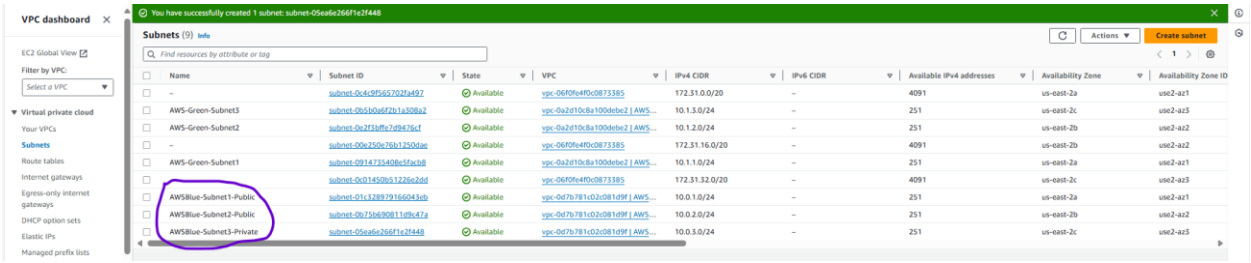
2 - Creating Public Subnet 2

- Click on the "Create subnet" button again.
- **Name Tag:** Enter a name for the second public subnet (e.g., Public-Subnet-2).
- **VPC:** Select your VPC from the dropdown list.
- **Availability Zone:** Choose a different availability zone for high availability (e.g., us-east-1b).
- **IPv4 CIDR block:** Enter a subnet CIDR block for the second public subnet (e.g., 10.0.2.0/24).
- Click "Create subnet."



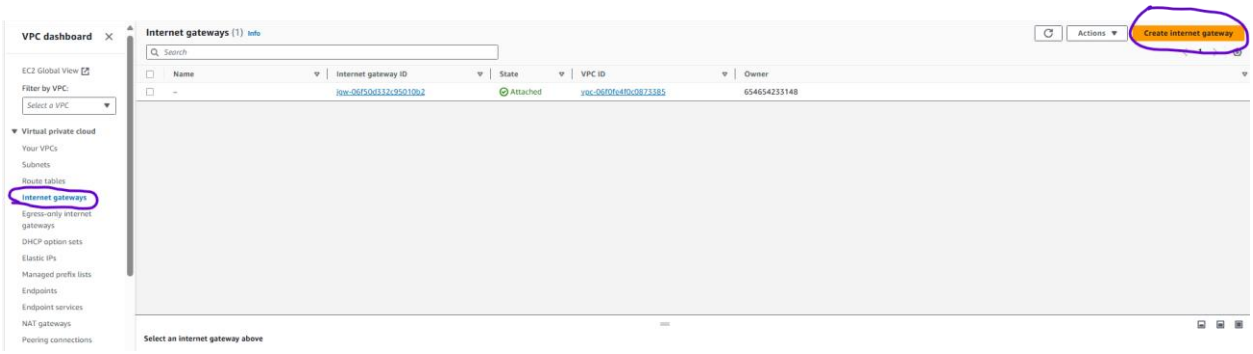
3 - Creating Private Subnet

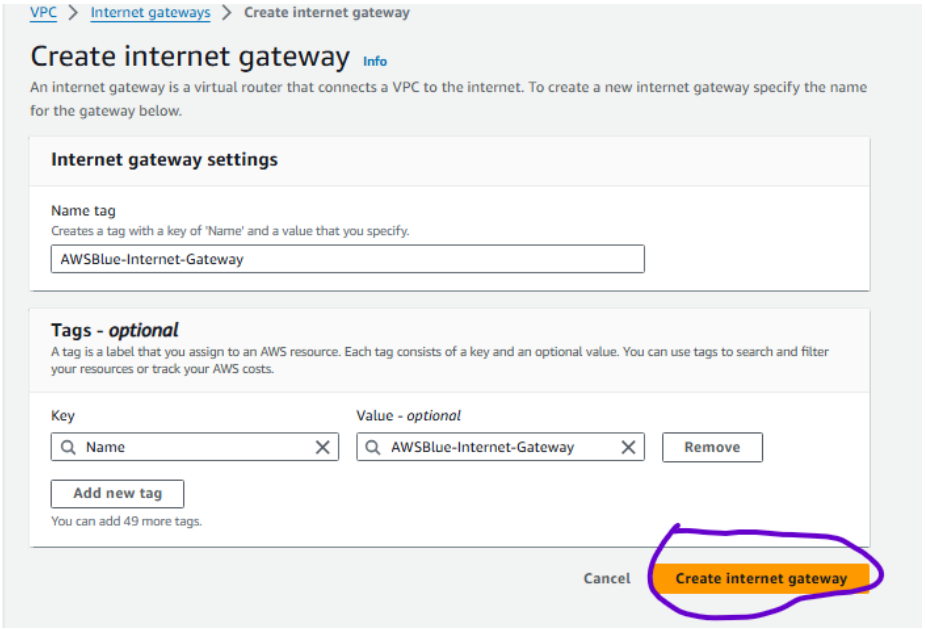
- Click on the "Create subnet" button again.
- **Name Tag:** Enter a name for the private subnet (e.g., Private-Subnet).
- **VPC:** Select your VPC from the dropdown list.
- **Availability Zone:** Choose an availability zone (you can use the same as one of the public subnets or a different one, e.g., us-east-1a).
- **IPv4 CIDR block:** Enter a subnet CIDR block for the private subnet (e.g., 10.0.3.0/24).
- Click "Create subnet."

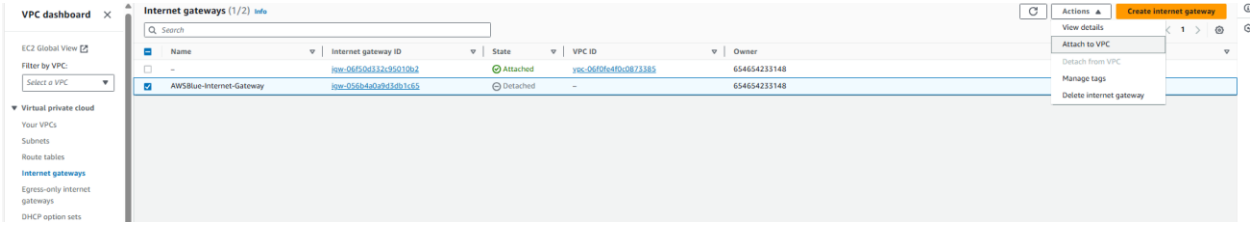


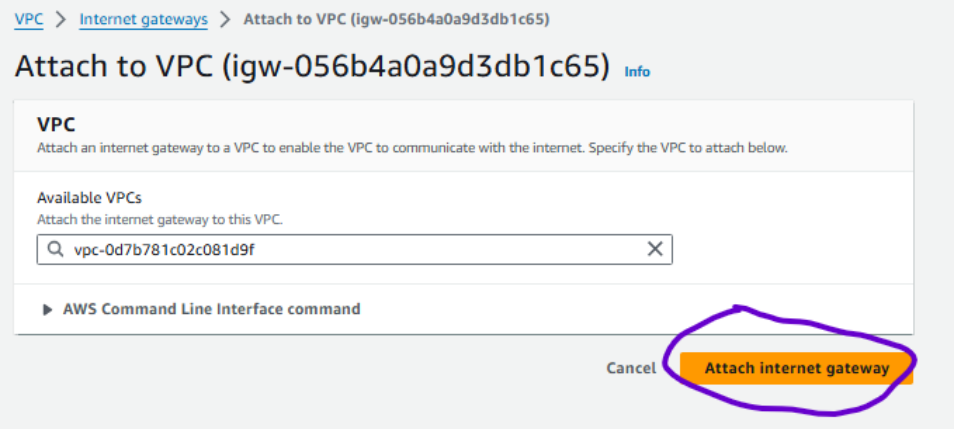
Attaching an Internet Gateway to the VPC:

- In the VPC Dashboard, click on "Internet Gateways."
- Click "Create internet gateway."
- **Name Tag:** Provide a name for the internet gateway (e.g., My-Internet-Gateway).
- Click "Create internet gateway."
- Once created, select the internet gateway, click on "Actions," and choose "Attach to VPC."
- Select your VPC and click "Attach internet gateway."


VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Internet gateways (1) Info
Search
Actions
Create internet gateway
Name
Internet gateway ID
State
VPC ID
Owner
igw-06f50d332c95010b2
Attached
vpc-06f0fe4f0c0873385
654654233148
Select an internet gateway above

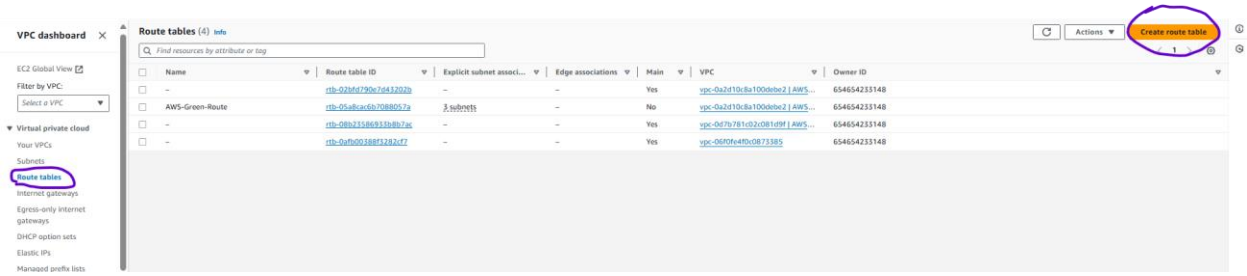

VPC > Internet gateways > Create internet gateway
Create internet gateway Info
An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.
Internet gateway settings
Name tag
Creates a tag with a key of 'Name' and a value that you specify.
AWSBlue-Internet-Gateway
Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Value - optional
Name
AWSBlue-Internet-Gateway
Remove
Add new tag
You can add 49 more tags.
Cancel
Create internet gateway

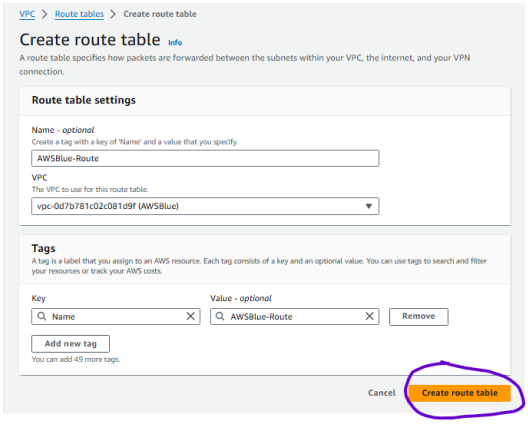

VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Internet gateways (1/2) Info
Search
Actions
Create internet gateway
View details
Attach to VPC
Detach from VPC
Manage tags
Delete internet gateway
Name
Internet gateway ID
State
VPC ID
Owner
igw-06f50d332c95010b2
Attached
vpc-06f0fe4f0c0873385
654654233148
AWSBlue-Internet-Gateway
igw-056b4a0a9d5db1c65
Detached
654654233148

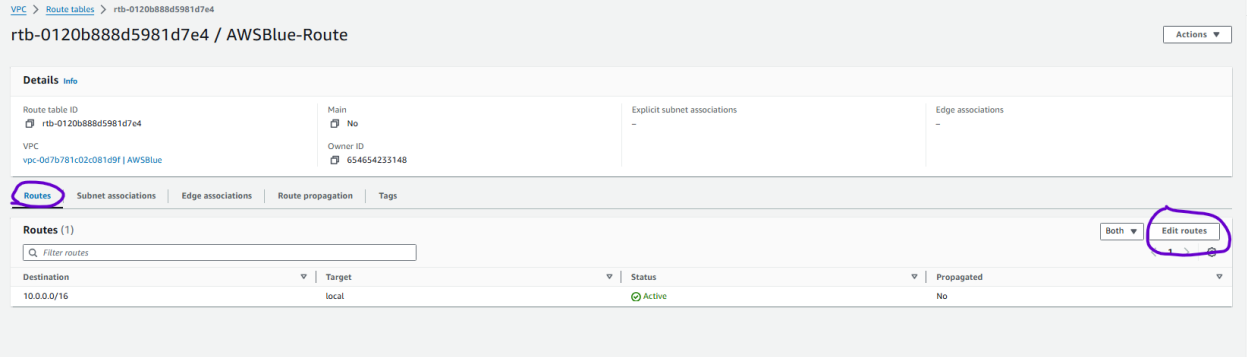


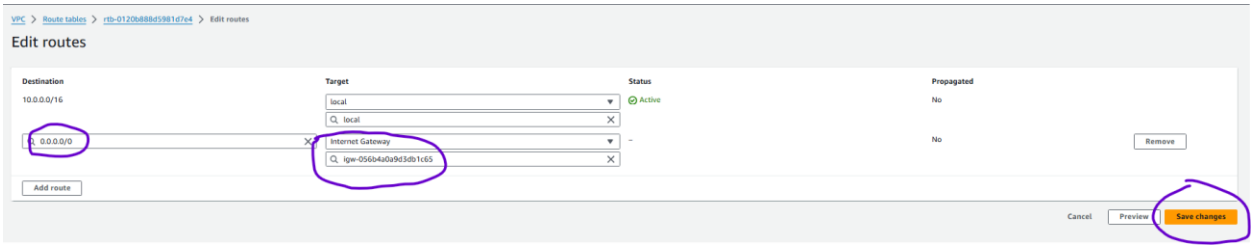
Creating a Route Table for the Public Subnets:

- In the VPC Dashboard, click on "Route Tables."
- Click "Create route table."
- **Name Tag:** Provide a name for the route table (e.g., Public-Route-Table).
- **VPC:** Select your VPC.
- Click "Create route table."
- Select the newly created route table, go to the "Routes" tab, and click "Edit routes."
- Click "Add route" and enter 0.0.0.0/0 for the Destination and select your Internet Gateway as the Target.
- Click "Save routes."



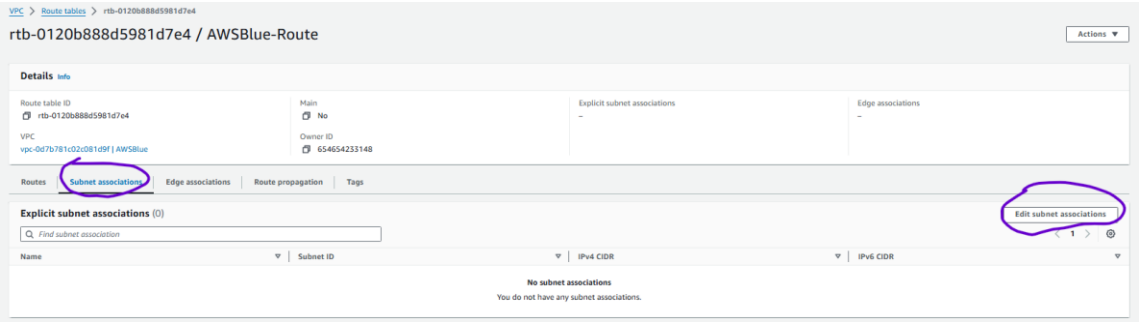


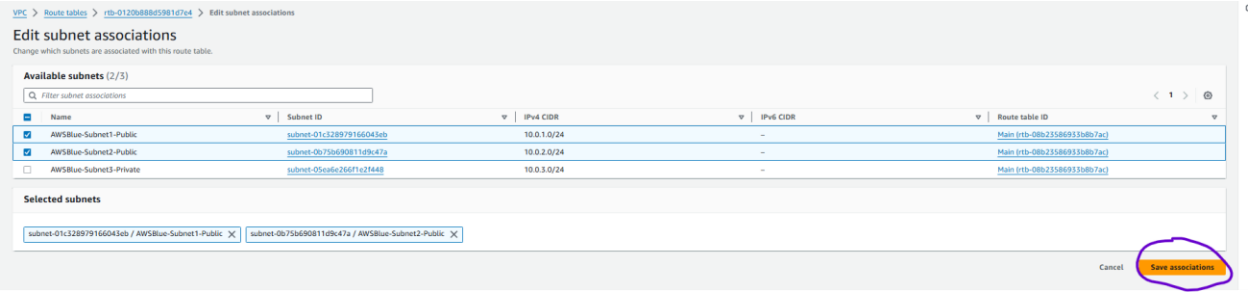




Associating the Route Table with Public Subnets:

- Select the route table you created for the public subnets.
- Go to the "Subnet associations" tab and click "Edit subnet associations."
- Select your public subnets (Public-Subnet-1 and Public-Subnet-2) and click "Save."



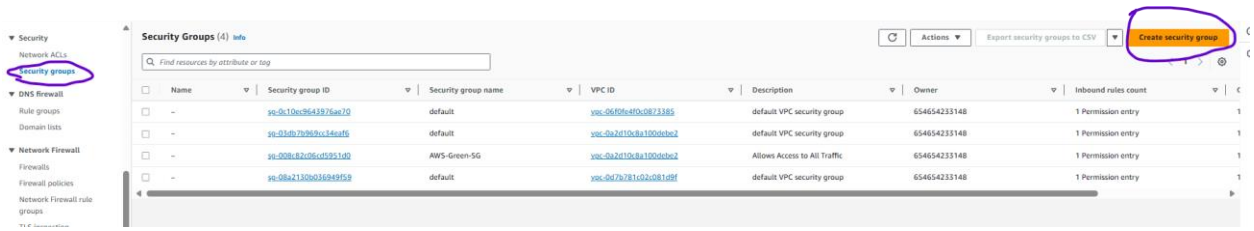


Note: The private subnet does not need direct access to an Internet Gateway, so it will use the default route table that doesn't route traffic to the Internet.

Creating a Security Group to All Traffic:

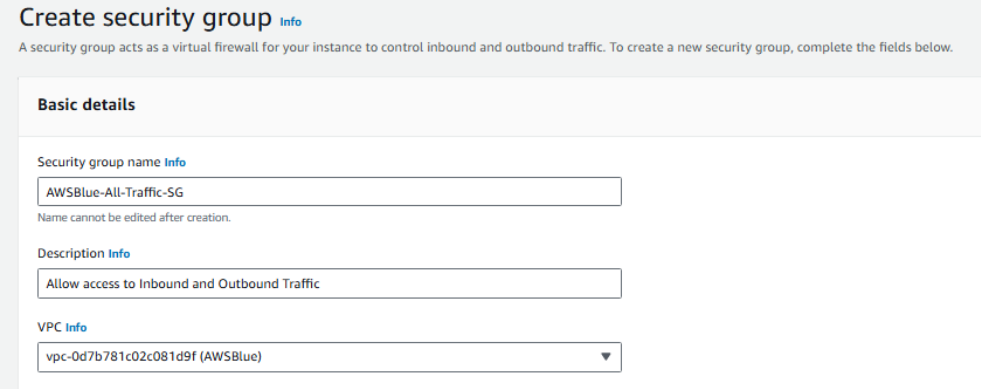
1 - Create a Security Group

- In the VPC Dashboard, click on "Security Groups" in the left-hand navigation pane.
- Click on the "Create security group" button.



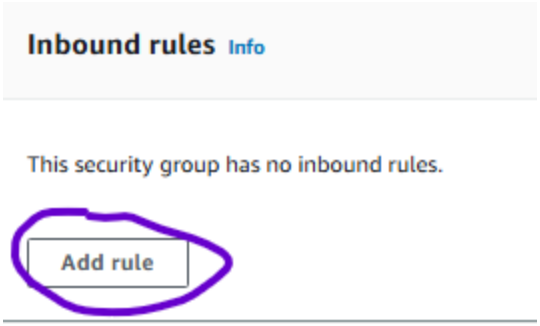
2 - Configure Security Group Details

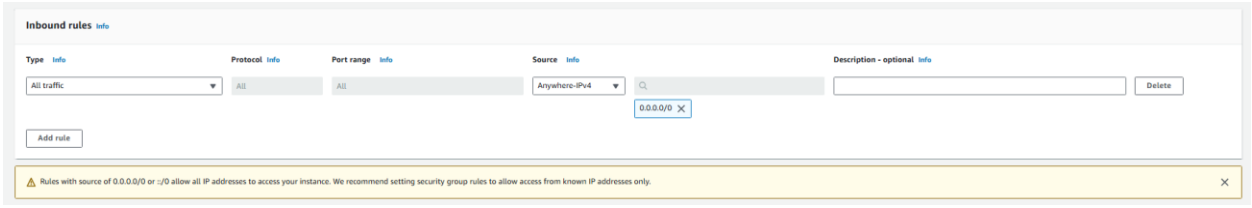
- **Name:** Enter a name for the security group (e.g., All-Traffic-SG).
- **Description:** Enter a description for the security group (e.g., Security group allowing all inbound and outbound traffic for testing purposes).
- **VPC:** Select the VPC where you want to create the security group.



3 - Configure Inbound Rules

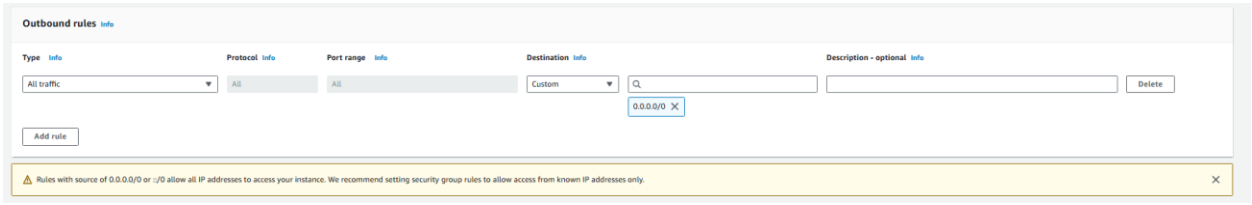
- Click on the "Inbound rules" tab.
- Click on "Add Rule."
- **Type:** Select "All Traffic."
- **Protocol:** Select "All."
- **Port Range:** Leave it as default (all ports).
- **Source:** Select "Anywhere-IPv4" (0.0.0.0/0) and "Anywhere-IPv6" (::/0) to allow traffic from any IP address.
- Click "Add Rule" to save the inbound rule.





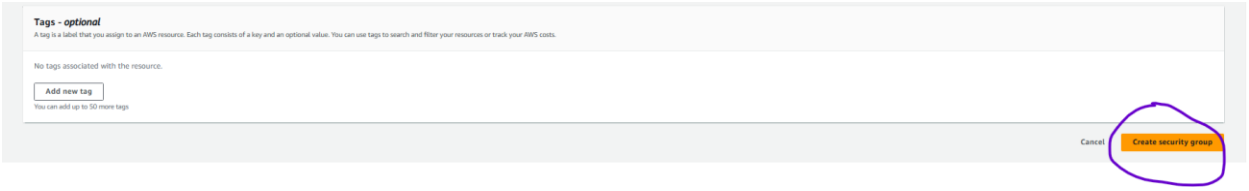
4 - Configure Outbound Rules

- Click on the "Outbound rules" tab.
- Click on "Add Rule."
- **Type:** Select "All Traffic."
- **Protocol:** Select "All."
- **Port Range:** Leave it as default (all ports).
- **Destination:** Select "Anywhere-IPv4" (0.0.0.0/0) and "Anywhere-IPv6" (::/0) to allow traffic to any IP address.
- Click "Add Rule" to save the outbound rule.



5 - Review and Create Security Group

- Review the security group settings.
- Click on the "Create security group" button to create the security group.



Note: This security group configuration allows all inbound and outbound traffic and should be used only for testing purposes. In real-time production environments, such a configuration poses significant security risks. Instead, restrict inbound and outbound traffic to only approved IP addresses and specific ports necessary for your application.

Example of a More Secure Configuration for Production

1 - Inbound Rules:

- Allow traffic from specific IP addresses or ranges.
- Limit access to necessary ports (e.g., 22 for SSH, 443 for HTTPS).

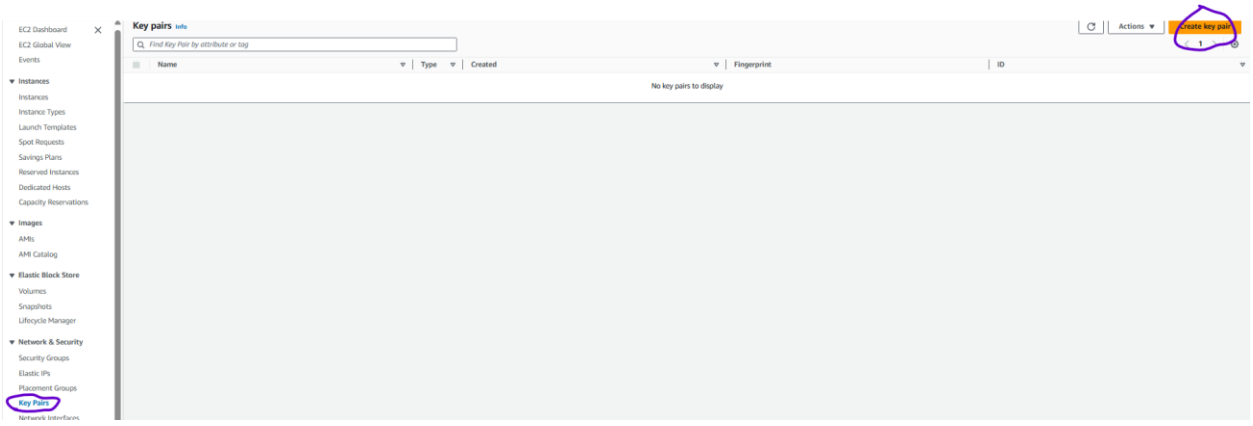
2 - Outbound Rules:

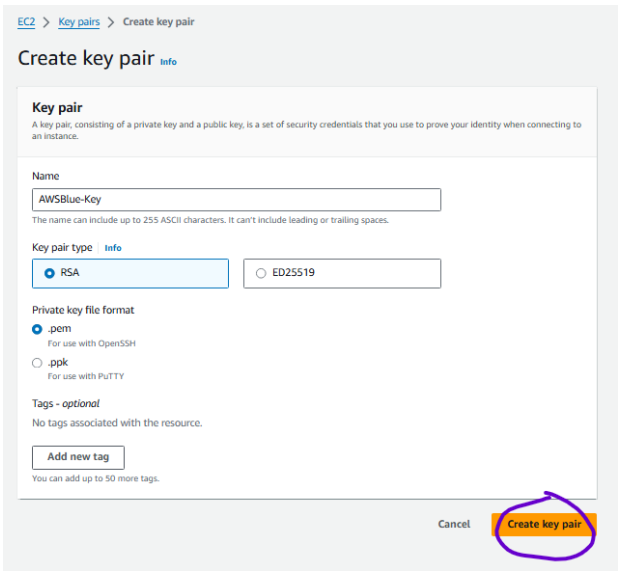
- Allow traffic only to specific IP addresses or ranges.
- Limit traffic to necessary ports and protocols.
- Example Inbound Rule for Production
- **Type:** SSH
- **Protocol:** TCP
- **Port Range:** 22
- **Source:** Specify a particular IP address or range (e.g., 203.0.113.0/24).

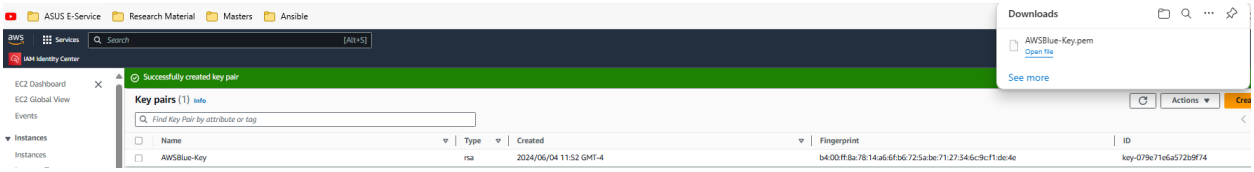
By carefully configuring security group rules, you can ensure that your AWS resources are protected against unauthorized access while maintaining necessary functionality.

Creating a Key Pair:

- In the EC2 navigation pane, under Network & Security, choose Key Pairs.
- Click on Create Key Pair.
- For Key pair name, enter a descriptive name that you can easily remember. This name will be associated with the public key.
- Choose the type of key pair you want to create: RSA or ED25519.
- Select the format for your private key file: PEM (for OpenSSH) or PPK (for PuTTY).
- Click Create.





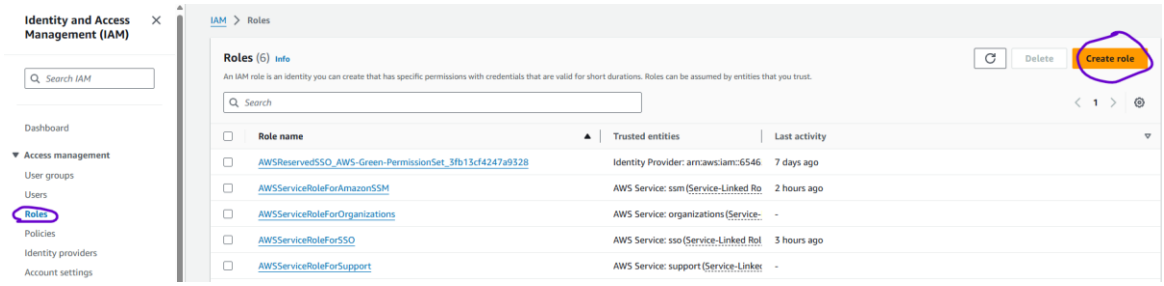


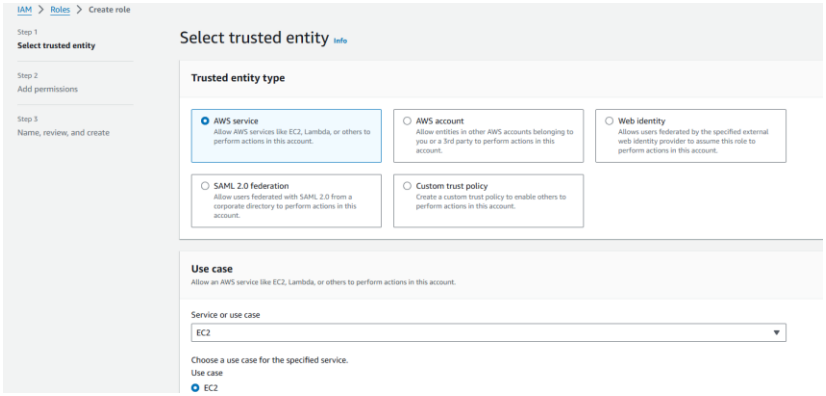
Note: When you click Create, a dialog box appears with the downloaded private key content. It is crucial to save this key pair in a secure location. You will need this private key to connect to your EC2 instance later.

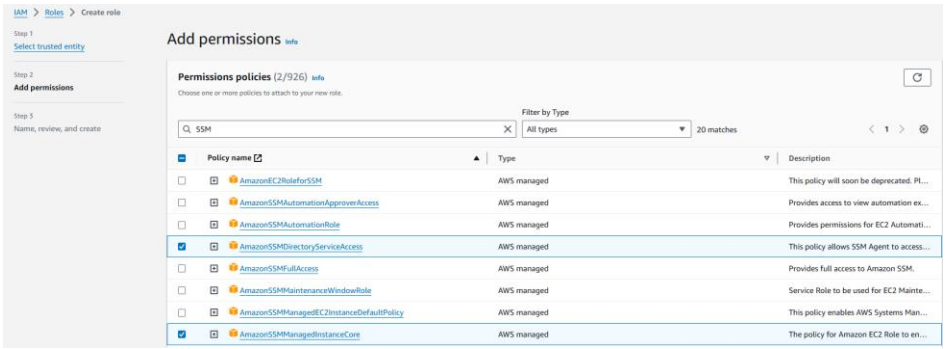
Creating an IAM Role:

- In the IAM navigation pane, under Security, choose Roles.
- Click Create role.
- Under Trusted entity type, choose AWS service.
- Under Use case, choose EC2.
- Click Next: Permissions.
- Under Add policy, search for the policy name AmazonSSMManagedInstanceCore, AmazonSSMDirectoryServiceAccess and select the checkbox next to it.
- Click Next: Review.
- Enter a descriptive name for your role (e.g., SSMInstanceRole) and an optional role description.
- Click Create role.

Note: This IAM role helps you securely manage your EC2 instances using AWS Systems Manager. It ensures your instances have the least privilege access required for core SSM functionalities and allows for optional directory service access if needed.







Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

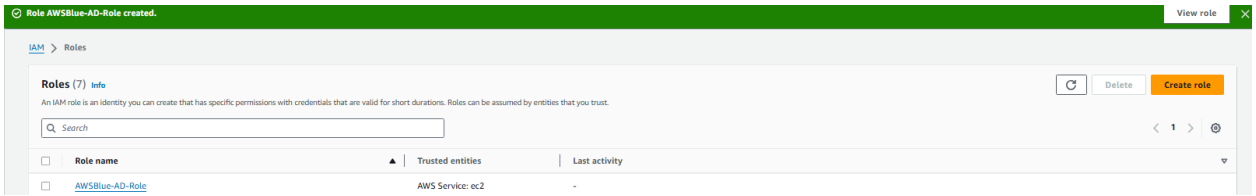
AWSBlue-AD-Role

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this role.

Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=, .@-/\[{}]!#$%^&*();:"'<>`



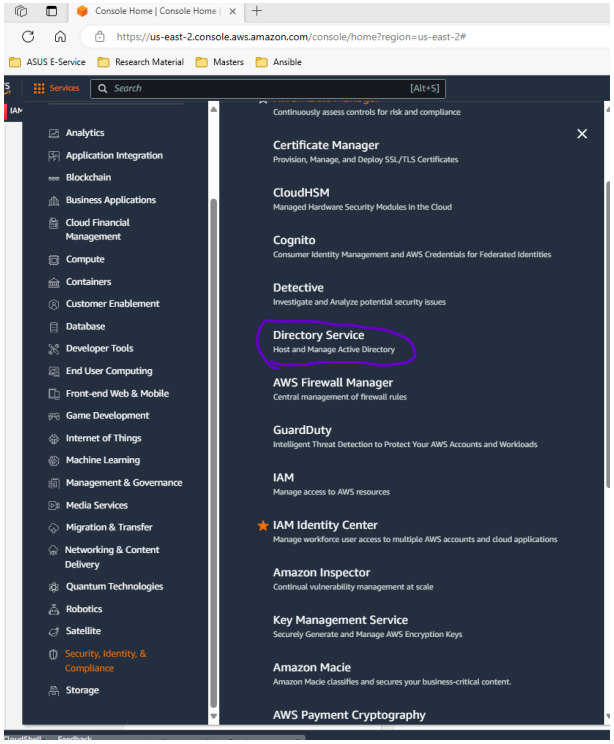
Creating Active Directory:

In AWS, there are two types of Active Directory (AD) services available: AWS Managed Microsoft AD and AD Connector. AWS Managed Microsoft AD is a fully managed service that runs Microsoft Active Directory in the AWS Cloud, providing high availability and seamless integration with your on-premises AD environment. It offers advanced features such as trust relationships and support for AWS applications that require AD integration. AD Connector, on the other hand, is a directory gateway that allows you to redirect directory requests to your on-premises Microsoft Active Directory without caching any information in the cloud. This enables you to extend your existing AD to AWS without complex configurations. In our implementation, we will start with AWS Managed Microsoft AD to leverage its comprehensive feature set and ease of integration. After successfully setting up and exploring AWS Managed Microsoft AD, we will proceed to implement AD Connector to understand its capabilities and how it can extend on-premises AD functionality to AWS.

Creating Active Directory (AWS Managed Microsoft AD):

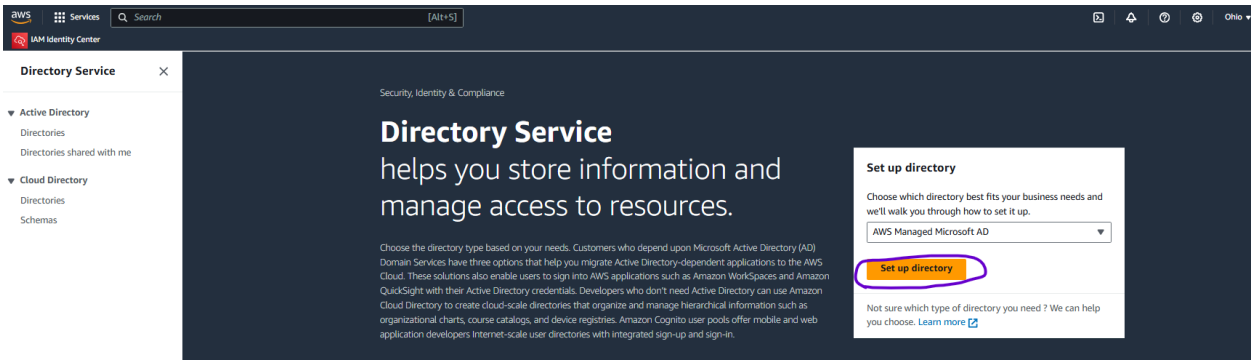
1 - Navigate to the Directory Service

- In the top navigation bar, click on "Services."
- Under "Security, Identity, & Compliance," select "Directory Service."



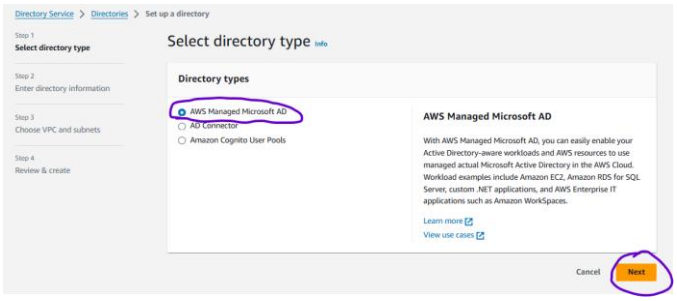
2 - Choose to Create a Directory

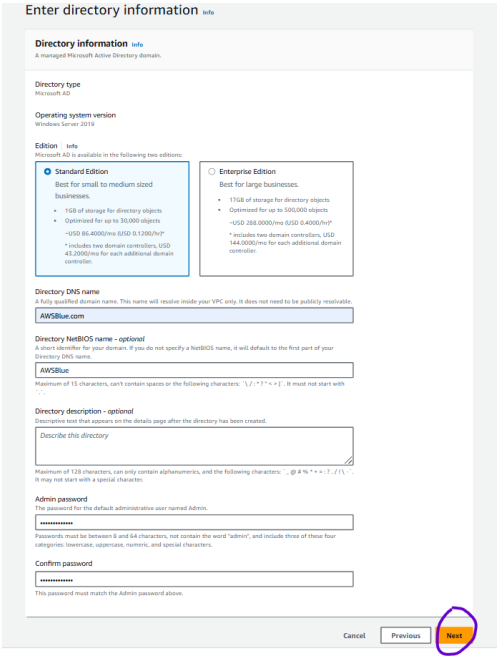
- On the AWS Directory Service dashboard, click on "Set up directory."
- Select "AWS Managed Microsoft AD."



3 - Configure Directory Details

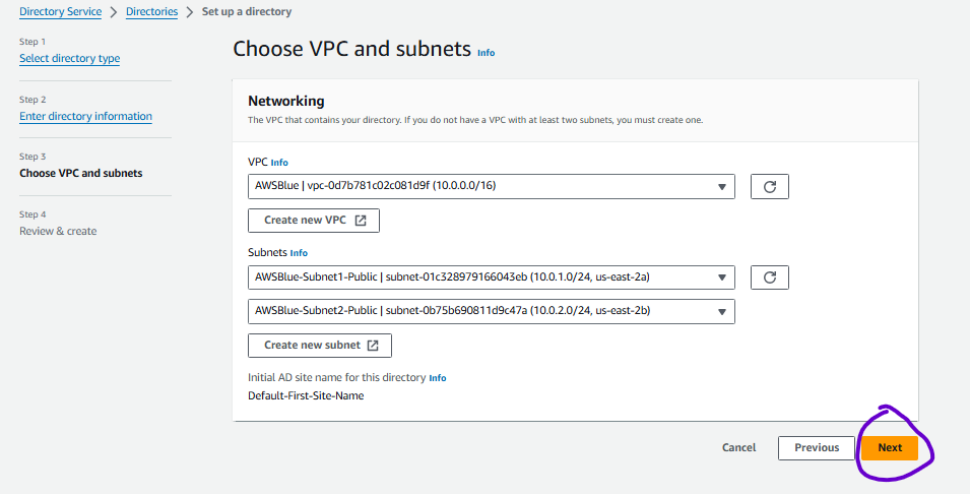
- **Edition:** Choose between "Standard Edition" (up to 30,000 users) and "Enterprise Edition" (up to 500,000 users) based on your needs.
- **Directory DNS Name:** Enter the fully qualified domain name (FQDN) for your directory (e.g., corp.example.com).
- **NetBIOS Name:** Enter the NetBIOS name for your directory (e.g., CORP).
- **Description:** (Optional) Enter a description for the directory.
- **Admin Password:** Enter a strong password for the default administrator account.
- Confirm the password.





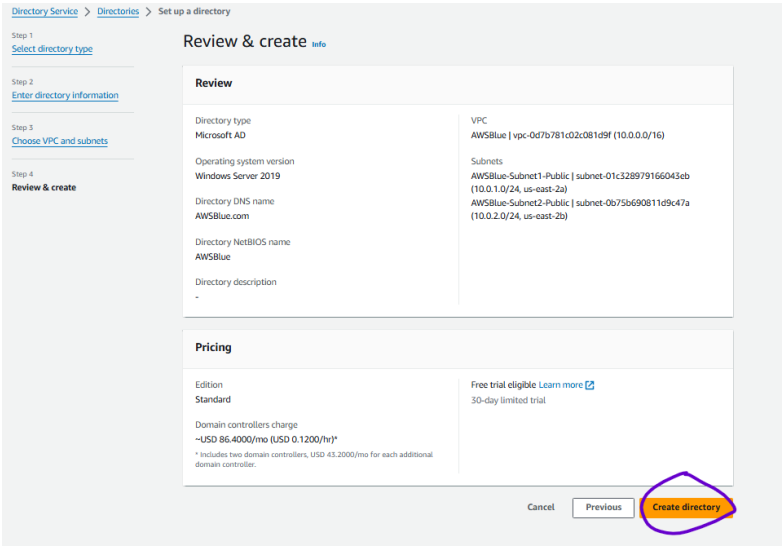
4 - Specify VPC and Subnets

- **VPC:** Select the VPC where you want to deploy the directory.
- **Subnets:** Choose two subnets in different Availability Zones for high availability. Ensure these subnets have sufficient IP addresses available.



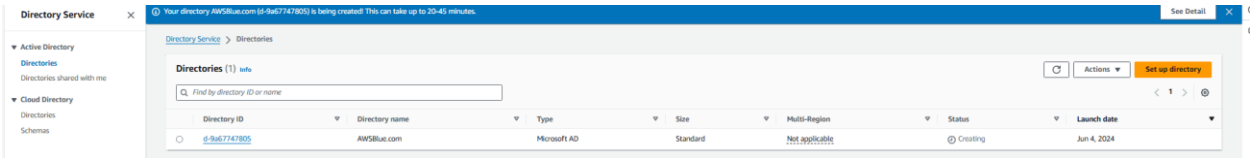
5 - Review and Create

- Review the configuration details to ensure everything is correct.
- Click "Create directory."



6 - Directory Creation Process

- The directory status will initially be "Creating." It can take 20-45 minutes for the directory to be fully created.
- Once the directory is created, its status will change to "Active."



7 - Configure Security Group Rules

- In the VPC Dashboard, click on "Security Groups."
- Find the security group associated with your directory.
- Edit the inbound and outbound rules to ensure that the necessary traffic is allowed. Common ports to consider:
  TCP/UDP 53 (DNS)
  TCP 88 (Kerberos)
  TCP/UDP 389 (LDAP)
  TCP 445 (SMB)
  TCP/UDP 464 (Kerberos password change)
  TCP/UDP 636 (LDAPS)
  TCP 3268-3269 (Global Catalog)

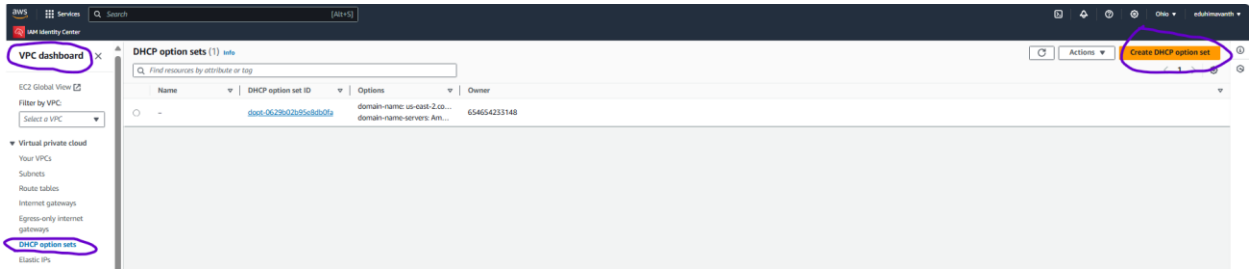
Note: Since we have allowed all traffic for both inbound and outbound connections, security group rules are no longer a concern.

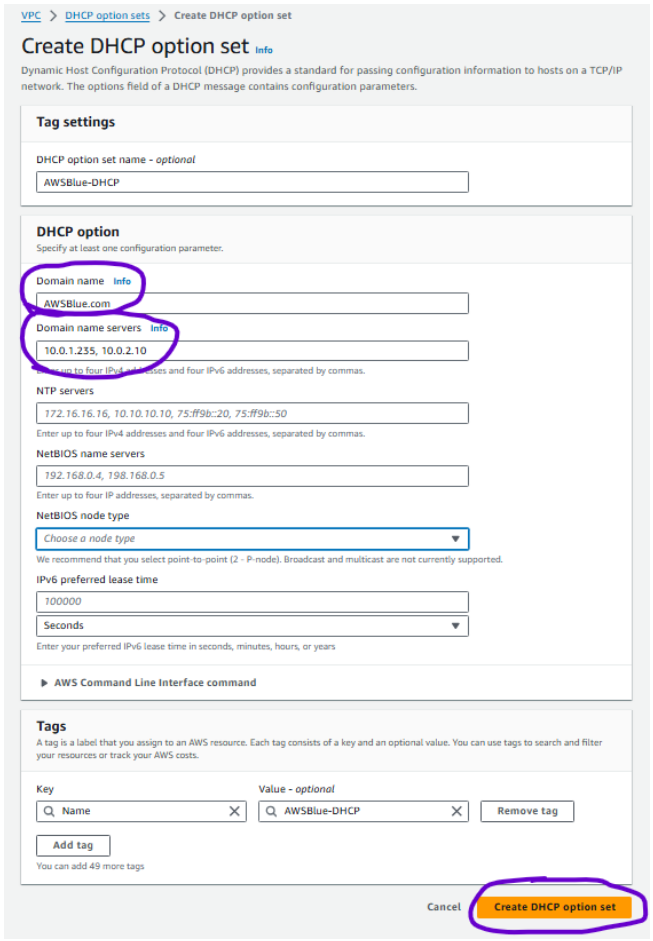
Case 1 - If the EC2 instance is not yet launched and we need to attach the created Active Directory to the EC2 instance, follow these steps to configure the AD and then launch the EC2 Windows instance for easy connectivity.

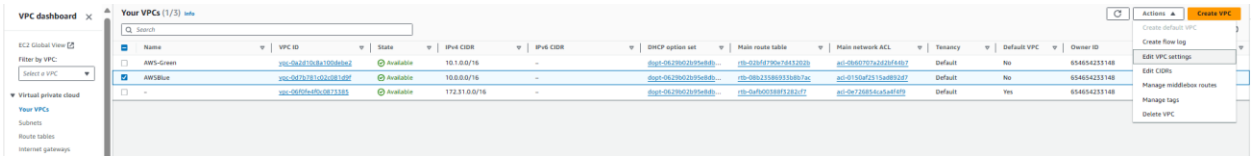
1 - Configure DHCP Options Set

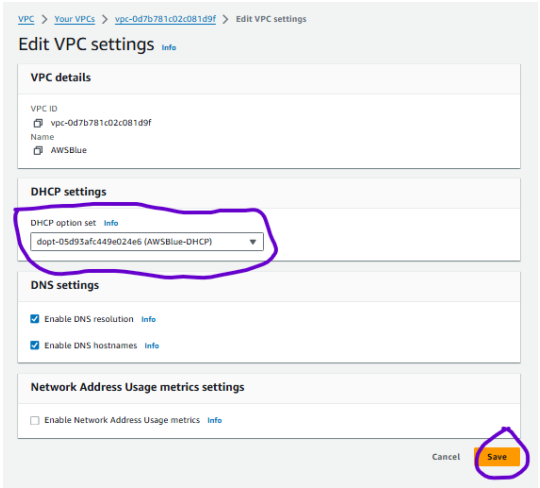
- In the VPC Dashboard, click on "DHCP Options Sets."
- Create a new DHCP options set with the domain name and domain name servers (DNS servers) pointing to the directory.
- Associate this DHCP options set with your VPC.

Note: This is an optional step required only if you are configuring the Active Directory for an instance that has not yet been deployed.

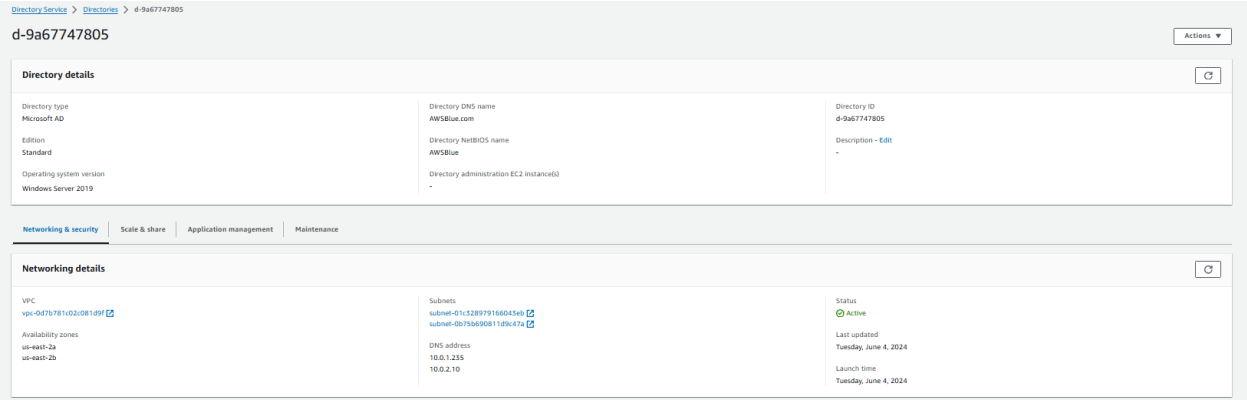



VPC > DHCP option sets > Create DHCP option set
Create DHCP option set Info
Dynamic Host Configuration Protocol (DHCP) provides a standard for passing configuration information to hosts on a TCP/IP network. The options field of a DHCP message contains configuration parameters.
Tag settings
DHCP option set name - optional
AWSBlue-DHCP
DHCP option
Specify at least one configuration parameter.
Domain name Info
AWSBlue.com
Domain name servers Info
10.0.1.235, 10.0.2.10
Enter up to four IPv4 addresses and four IPv6 addresses, separated by commas.
NTP servers
172.16.16.16, 10.10.10.10, 75:ff9b::20, 75:ff9b::50
Enter up to four IPv4 addresses and four IPv6 addresses, separated by commas.
NetBIOS name servers
192.168.0.4, 198.168.0.5
Enter up to four IP addresses, separated by commas.
NetBIOS node type
Choose a node type
We recommend that you select point-to-point (2 - P-node). Broadcast and multicast are not currently supported.
IPv6 preferred lease time
100000
Seconds
Enter your preferred IPv6 lease time in seconds, minutes, hours, or years
AWS Command Line Interface command
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Value - optional
Name
AWSBlue-DHCP
Remove tag
Add tag
You can add 49 more tags
Cancel
Create DHCP option set


VPC dashboard
Your VPCs (1/3) Info
Actions
Create VPC
Edit VPC settings
AWS-Green
AWSBlue
Available


VPC > Your VPCs > vpc-0d7b781c02c081d9f > Edit VPC settings
Edit VPC settings Info
VPC details
VPC ID
vpc-0d7b781c02c081d9f
Name
AWSBlue
DHCP settings
DHCP option set Info
dopt-05d93afc449e024e6 (AWSBlue-DHCP)
DNS settings
Enable DNS resolution Info
Enable DNS hostnames Info
Network Address Usage metrics settings
Enable Network Address Usage metrics Info
Cancel
Save

Note: The IP Addresses provided in the Domain Name Servers are the DNS Addresses of the Active Directory Created.



2 - Launch a Windows Instance in the VPC

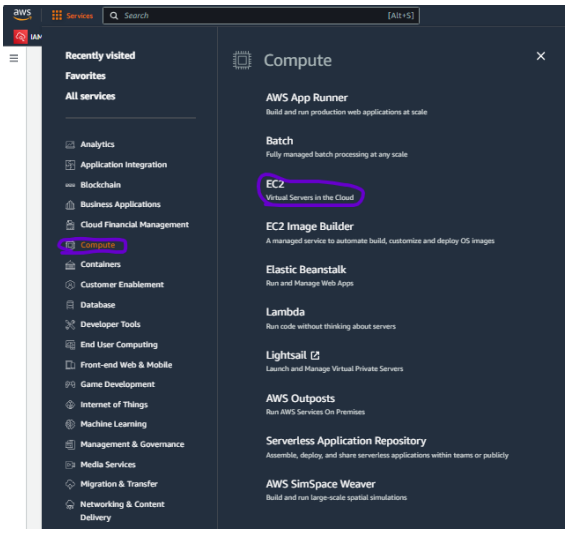
- In the AWS Management Console, go to the EC2 Dashboard.
- Click on "Launch Instance."
- Choose an Amazon Machine Image (AMI) that is a Windows Server version (e.g., Windows Server 2019 Base).
- Select the instance type based on your requirements (e.g., `t2.medium`).
- Configure the instance details

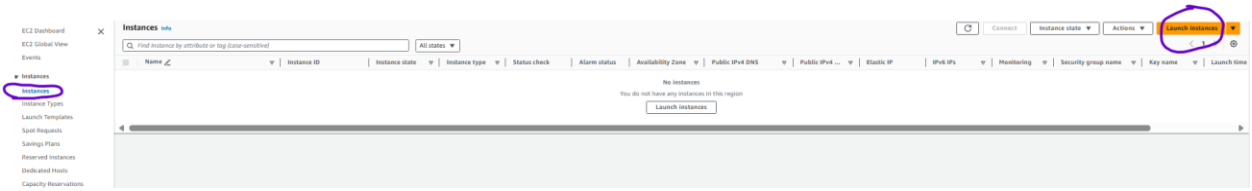
  Ensure the instance is launched within the VPC where your AWS Managed Microsoft AD is set up.

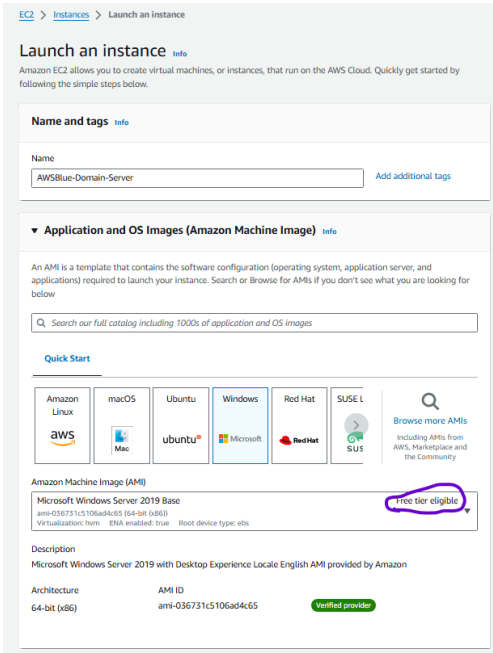
  Assign a public IP if you need to access the instance remotely via the internet.
- Add storage if needed and configure tags.
- Configure the security group

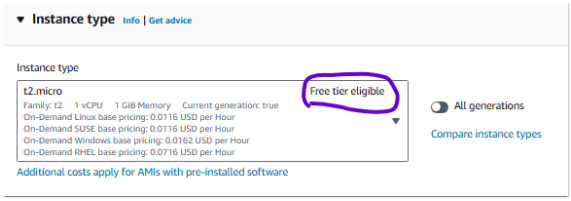
  Ensure that the security group allows inbound RDP traffic (TCP port 3389).

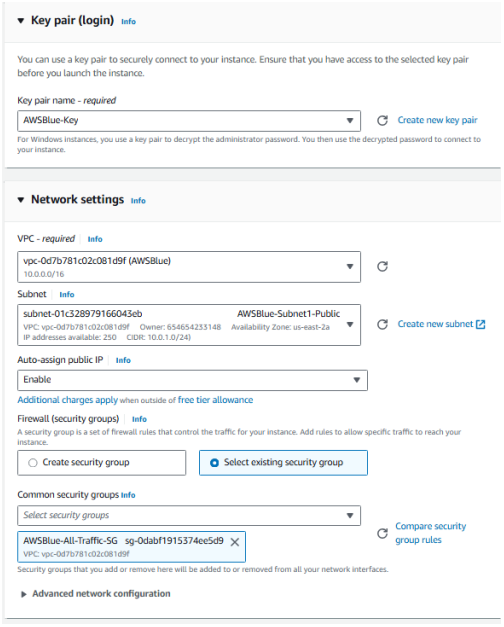
  Note: Since we have allowed all traffic for both inbound and outbound connections, security group rules are no longer a concern.
- Review and launch the instance.

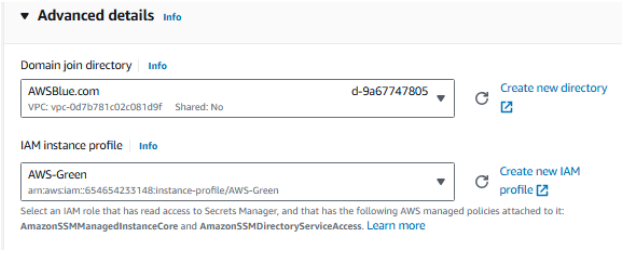


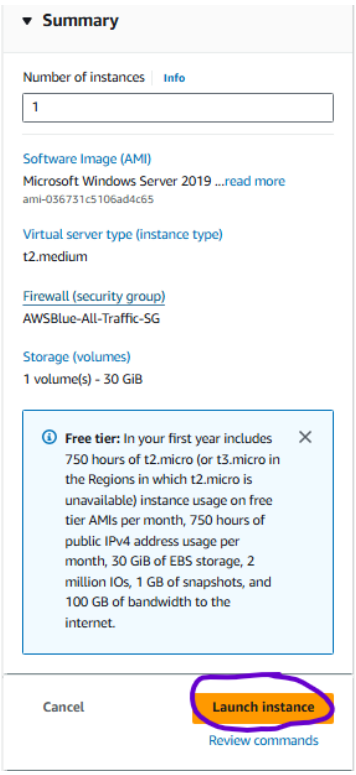

Instances
Launch instances
No instances
You do not have any instances in this region
Launch instances

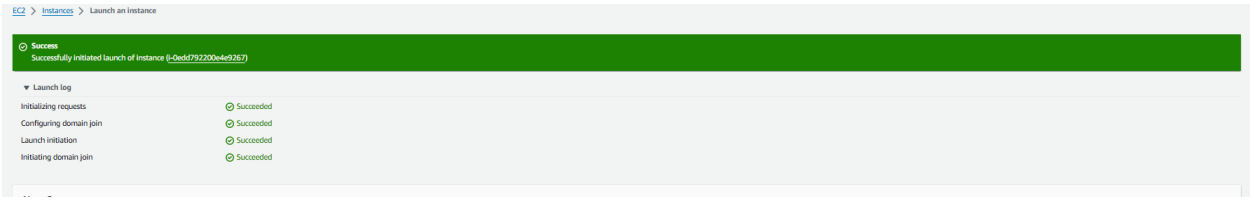

EC2 > Instances > Launch an instance
Launch an instance
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags
Name
AWSBlue-Domain-Server
Add additional tags
Application and OS Images (Amazon Machine Image)
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
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)
Microsoft Windows Server 2019 Base
Free tier eligible
Description
Microsoft Windows Server 2019 with Desktop Experience Locale English AMI provided by Amazon
Architecture
64-bit (x86)
AMI ID
ami-036731c5106ad4c65
Verified provider


Instance type
Info | Get advice
Instance type
t2.micro
Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0116 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand RHEL base pricing: 0.0716 USD per Hour
All generations
Compare instance types
Additional costs apply for AMIs with pre-installed software


Key pair (login)
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
AWSBlue-Key
Create new key pair
For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.
Network settings
VPC - required
vpc-0d7b781c02c081d9f (AWSBlue)
10.0.0.0/16
Subnet
subnet-01c328979166043eb
AWSBlue-Subnet1-Public
Create new subnet
Auto-assign public IP
Enable
Additional charges apply when outside of free tier allowance
Firewall (security groups)
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Common security groups
Select security groups
AWSBlue-All-Traffic-SG sg-0dabf1915374ee5d9
VPC: vpc-0d7b781c02c081d9f
Compare security group rules
Security groups that you add or remove here will be added to or removed from all your network interfaces.
Advanced network configuration

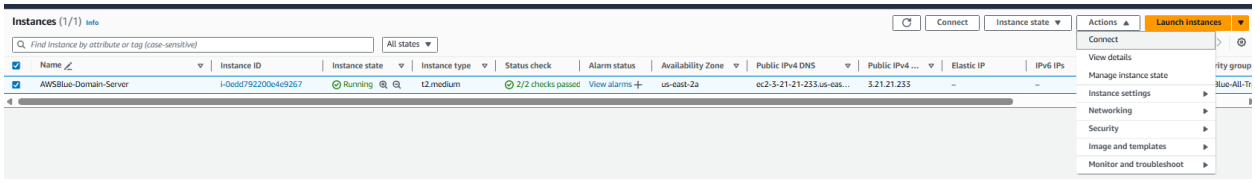

Advanced details
Info
Domain join directory
Info
AWSBlue.com
d-9a67747805
VPC: vpc-0d7b781c02c081d9f Shared: No
Create new directory
IAM instance profile
Info
AWS-Green
arn:aws:iam::654654233148:instance-profile/AWS-Green
Create new IAM profile
Select an IAM role that has read access to Secrets Manager, and that has the following AWS managed policies attached to it:
AmazonSSMManagedInstanceCore and AmazonSSMDirectoryServiceAccess. Learn more

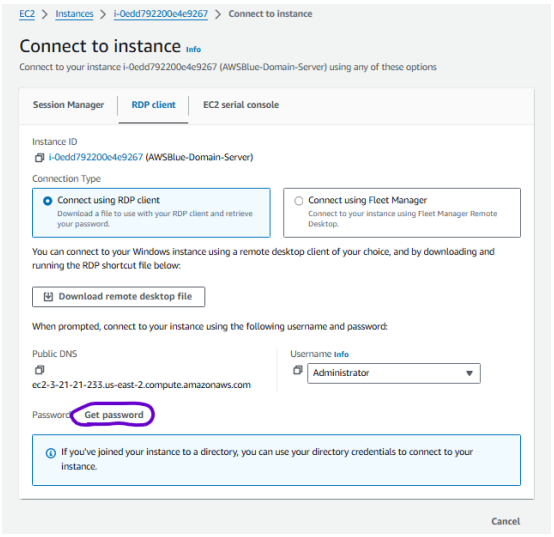


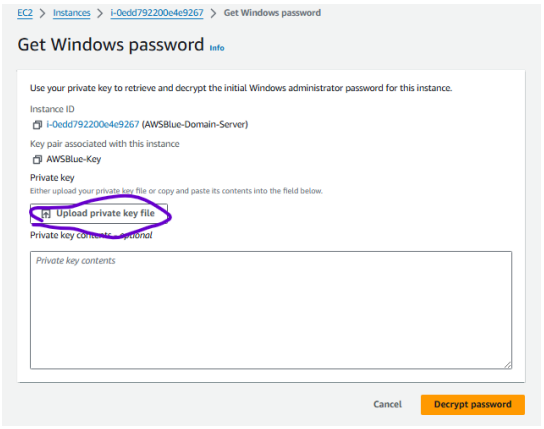


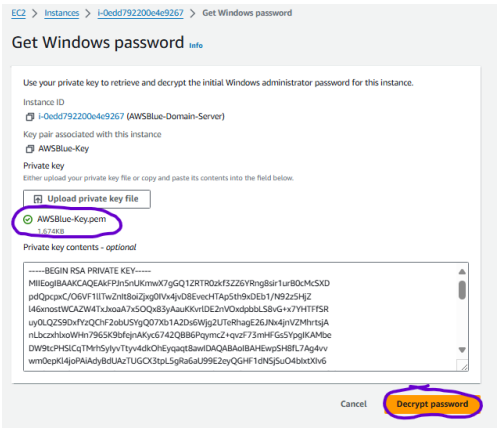
3 - Connect to the Windows Instance

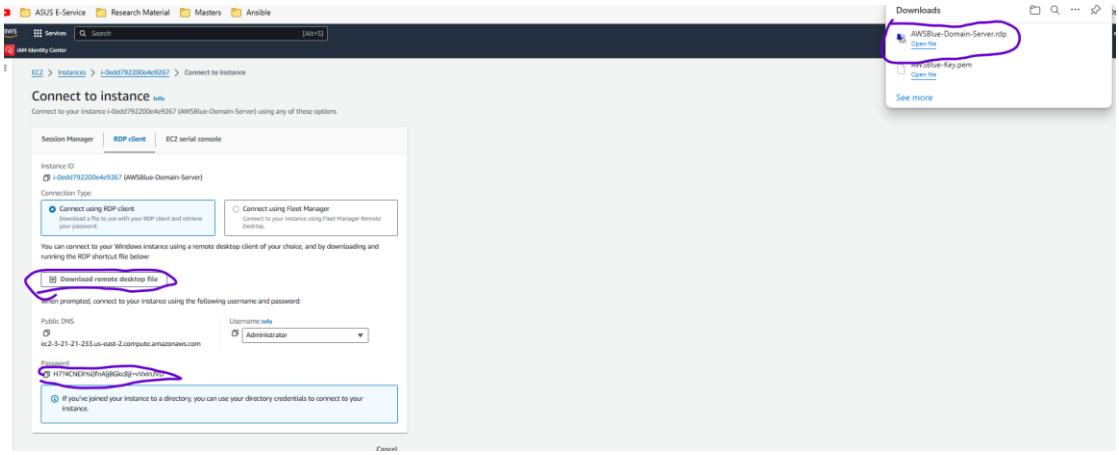
- Once the instance is running, select the instance in the EC2 Dashboard.
- Click "Connect" and choose the "RDP Client" tab.
- Download the Remote Desktop Protocol (RDP) file and use it to connect to the instance.
- Log in using the default administrator credentials for the instance.

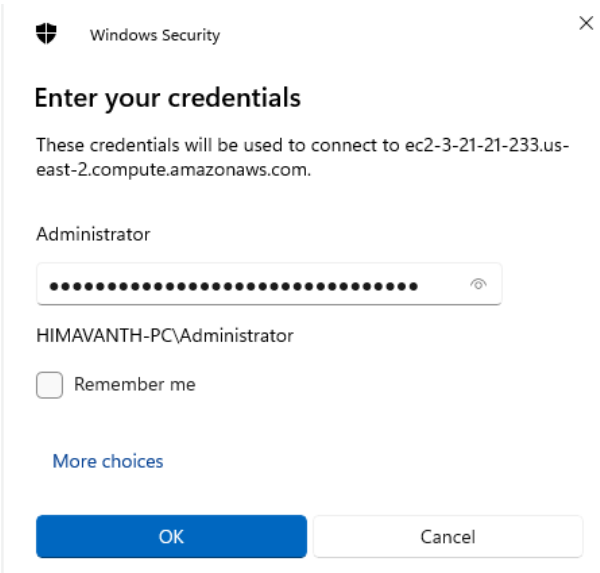


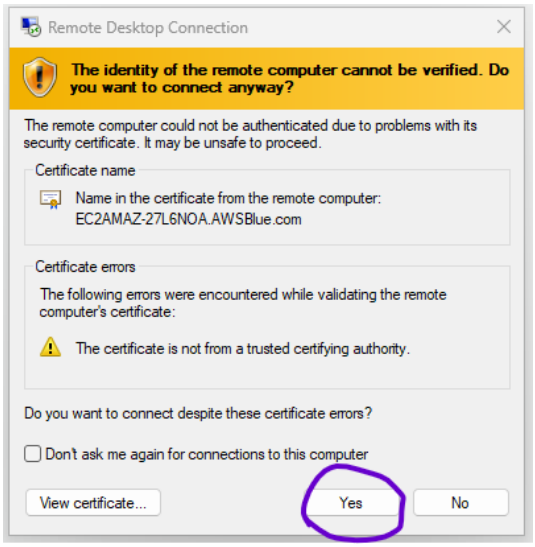

EC2 > Instances > i-0edd792200e4e9267 > Connect to instance
Connect to instance Info
Connect to your instance i-0edd792200e4e9267 (AWSBlue-Domain-Server) using any of these options
Session Manager
RDP client
EC2 serial console
Instance ID
i-0edd792200e4e9267 (AWSBlue-Domain-Server)
Connection Type
Connect using RDP client
Download a file to use with your RDP client and retrieve your password.
Connect using Fleet Manager
Connect to your instance using Fleet Manager Remote Desktop.
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 username and password:
Public DNS
ec2-3-21-21-233.us-east-2.compute.amazonaws.com
Username Info
Administrator
Password
Get password
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.
Cancel

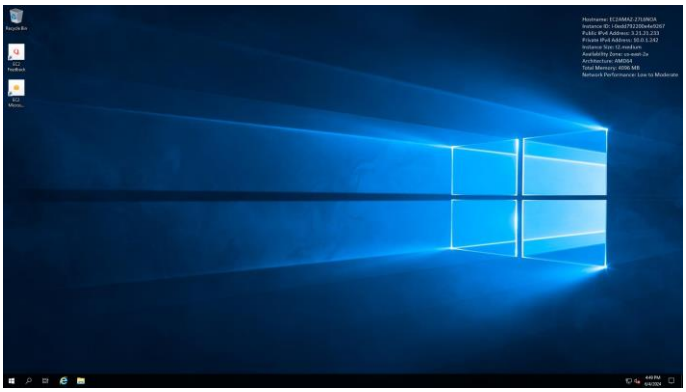

EC2 > Instances > i-0edd792200e4e9267 > Get Windows password
Get Windows password Info
Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.
Instance ID
i-0edd792200e4e9267 (AWSBlue-Domain-Server)
Key pair associated with this instance
AWSBlue-Key
Private key
Either upload your private key file or copy and paste its contents into the field below.
Upload private key file
Private key contents - optional
Private key contents
Cancel
Decrypt password


EC2 > Instances > i-0edd792200e4e9267 > Get Windows password
Get Windows password Info
Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.
Instance ID
i-0edd792200e4e9267 (AWSBlue-Domain-Server)
Key pair associated with this instance
AWSBlue-Key
Private key
Either upload your private key file or copy and paste its contents into the field below.
Upload private key file
AWSBlue-Key.pem
1.674KB
Private key contents - optional
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAkFPJn5nUKmwX7gGQ1ZRTR0zkf3ZZ6YRng8sir1urB0cMcSXD
pdQpcpxC/O6VF1lITwZnIt8oiZjxg0IVx4jvD8EvecHTAp5th9xDEb1/N92z5HjZ
l46xnostWCAZW4TxJxoaA7xSOQx83yAauKKvrIDE2nVOxdpbbLS8vG+x7YHTfSR
uy0LQZS9DxfY2QChF2obUSYgQ07Xb1A2Ds6Wjg2UTeRhagE26JNx4jnVZMhrtsjA
nLbczxhIxoWHn7965K9bfejnAKyc6742QB86PqymcZ+qvzF73mHFGsSYpgIKAMbc
DW9tcPHSICqTMrhSyIyvTtyv4dkOhEyqaqt8awIDAQABAoIBAHEwpSH8fL7Ag4vv
wm0epKl4joPAlAdyBdUAz1UGCX3tpLSgRa6aU99E2eyQGHF1dNSjSuO4bktXlv6
Cancel
Decrypt password


ASUS E-Service
Research Material
Masters
Ansible
Downloads
AWSBlue-Domain-Server.rdp
Open file
AWSBlue-Key.pem
Open file
See more
EC2 > Instances > i-0edd792200e4e9267 > Connect to instance
Connect to instance Info
Session Manager
RDP client
EC2 serial console
Instance ID
i-0edd792200e4e9267 (AWSBlue-Domain-Server)
Connection Type
Connect using RDP client
Connect using Fleet Manager
Download remote desktop file
Public DNS
ec2-3-21-21-233.us-east-2.compute.amazonaws.com
Username Info
Administrator
Password
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.







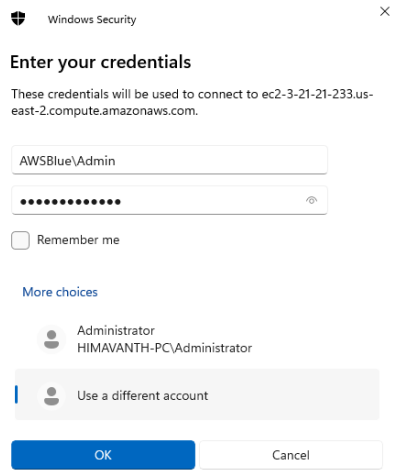
4 - Join the Windows Instance to the Domain

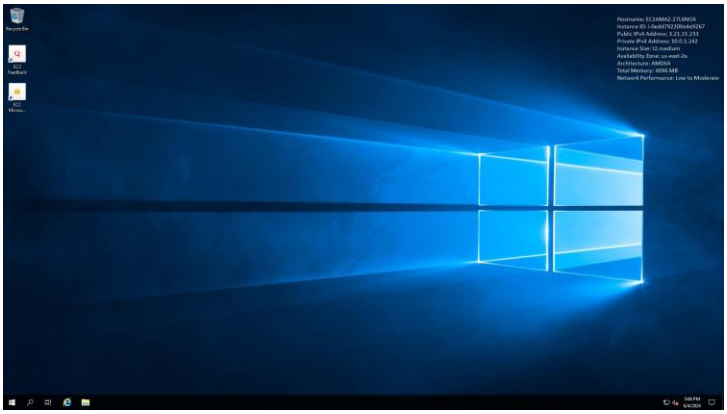
- In the Windows instance, open the "Server Manager."
- Click on "Local Server" in the left pane.

Note: As the Instance is already registered with the Domain “AWSBlue.com”, We can proceed to restart the system and log back in with the AD Admin credentials.

5 - Log in with AD Admin Credentials

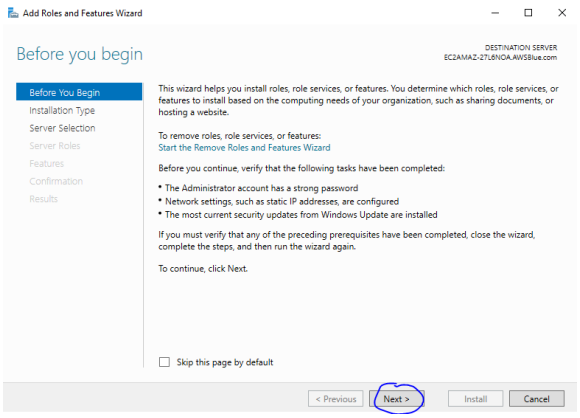
- After the instance restarts, connect to it again using RDP.
- This time, log in with the AD admin credentials (e.g., `AWSBlue\Admin`).

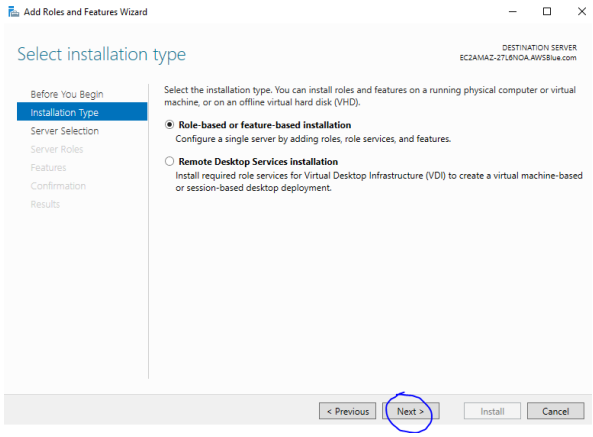


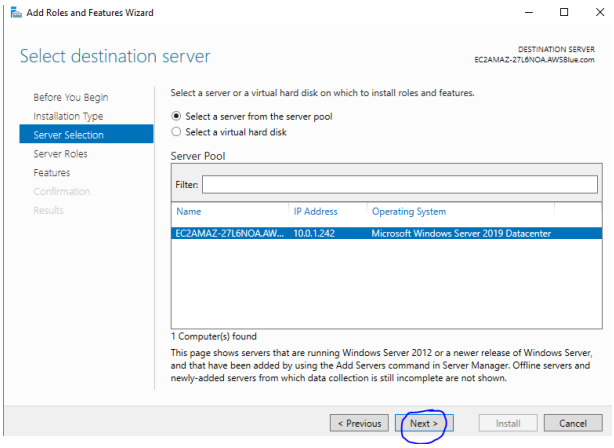


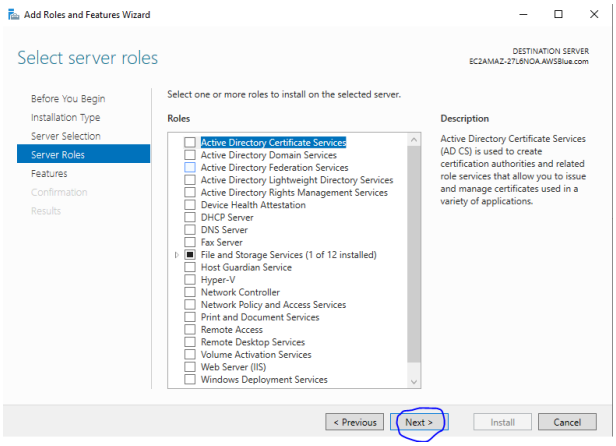
6 - Install Active Directory Administrative Tools (RSAT)

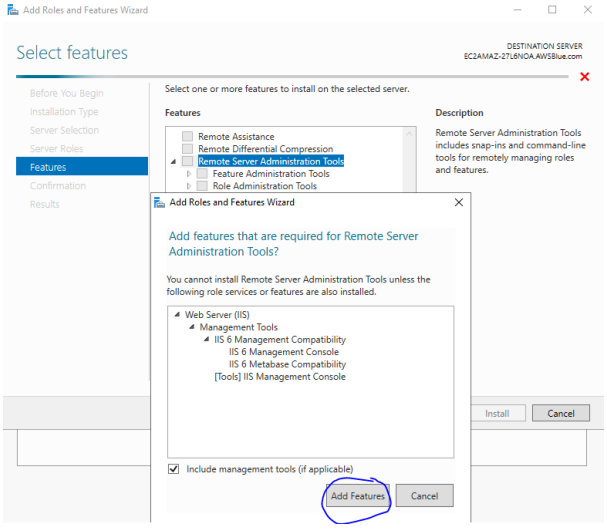
- In the Windows instance, open the "Server Manager."
- Click on "Manage" and select "Add Roles and Features."
- In the "Add Roles and Features Wizard," click "Next" until you reach the "Features" page.
- In the "Features" page, scroll down and expand "Remote Server Administration Tools."
- Expand "Role Administration Tools."
- Select "AD DS and AD LDS Tools" and ensure all sub-options are checked.
- Click "Next" and then "Install."

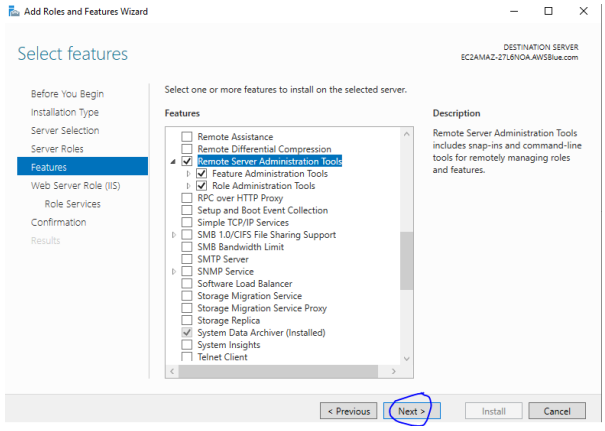

Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
EC2AMAZ-27L6NOA.AWSBlue.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel

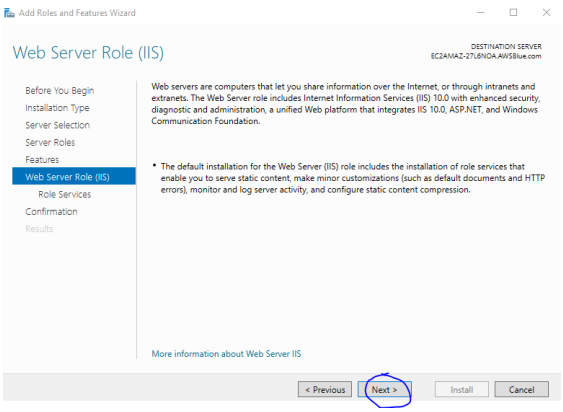

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
EC2AMAZ-27L6NOA.AWSBlue.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel

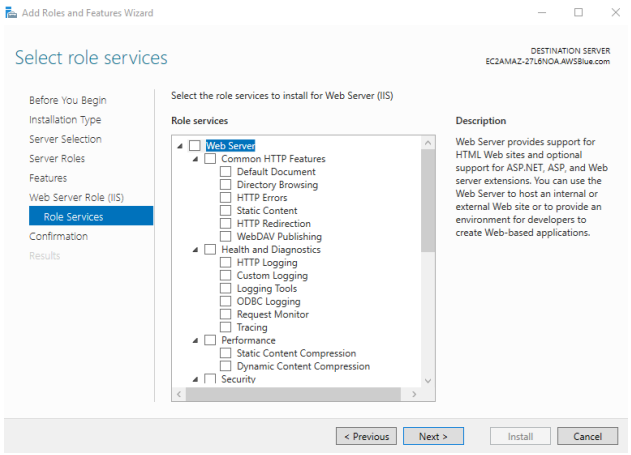

Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
EC2AMAZ-27L6NOA.AWSBlue.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
EC2AMAZ-27L6NOA.AW...
10.0.1.242
Microsoft Windows Server 2019 Datacenter
1 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel

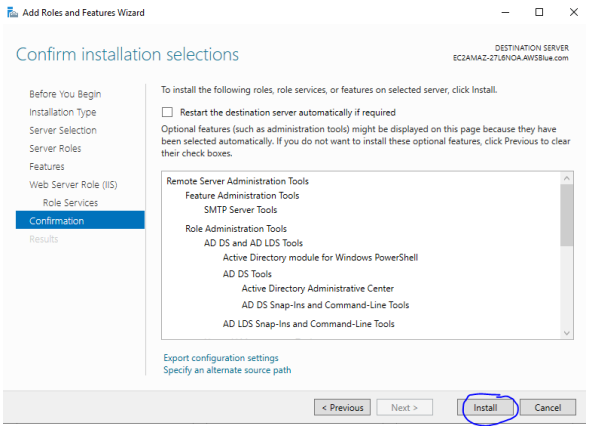

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
EC2AMAZ-27L6NOA.AWSBlue.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Description
Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
< Previous
Next >
Install
Cancel

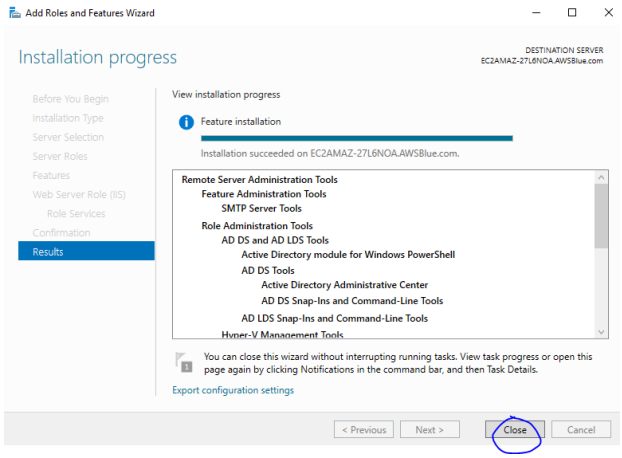

Add Roles and Features Wizard
Select features
DESTINATION SERVER
EC2AMAZ-27L6NOA.AWSBlue.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more features to install on the selected server.
Features
Remote Assistance
Remote Differential Compression
Remote Server Administration Tools
Feature Administration Tools
Role Administration Tools
Description
Remote Server Administration Tools includes snap-ins and command-line tools for remotely managing roles and features.
Add Roles and Features Wizard
Add features that are required for Remote Server Administration Tools?
You cannot install Remote Server Administration Tools unless the following role services or features are also installed.
Web Server (IIS)
Management Tools
IIS 6 Management Compatibility
IIS 6 Management Console
IIS 6 Metabase Compatibility
[Tools] IIS Management Console
Include management tools (if applicable)
Add Features
Cancel
Install
Cancel


Add Roles and Features Wizard
Select features
DESTINATION SERVER
EC2AMAZ-27L6NOA.AWSBlue.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select one or more features to install on the selected server.
Features
Remote Assistance
Remote Differential Compression
Remote Server Administration Tools
Feature Administration Tools
Role Administration Tools
RPC over HTTP Proxy
Setup and Boot Event Collection
Simple TCP/IP Services
SMB 1.0/CIFS File Sharing Support
SMB Bandwidth Limit
SMTP Server
SNMP Service
Software Load Balancer
Storage Migration Service
Storage Migration Service Proxy
Storage Replica
System Data Archiver (Installed)
System Insights
Telnet Client
Description
Remote Server Administration Tools includes snap-ins and command-line tools for remotely managing roles and features.
< Previous
Next >
Install
Cancel



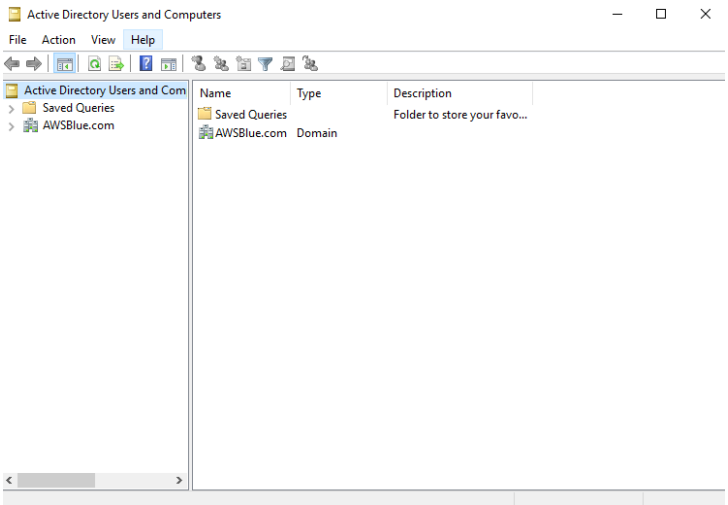






7 - Open Active Directory Users and Computers

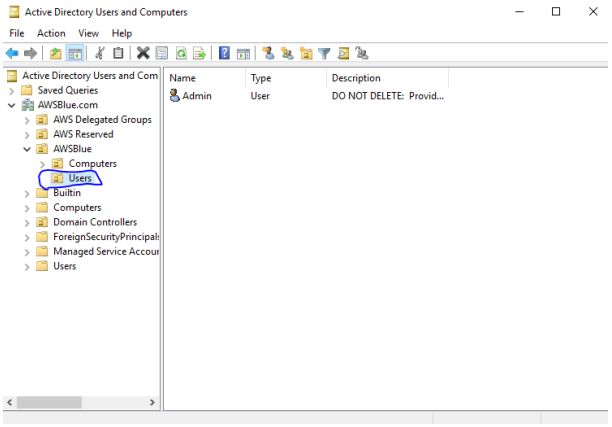
- After the installation is complete, go to the "Tools" in the Server Manger.
- Select "Active Directory Users and Computers" and open it.

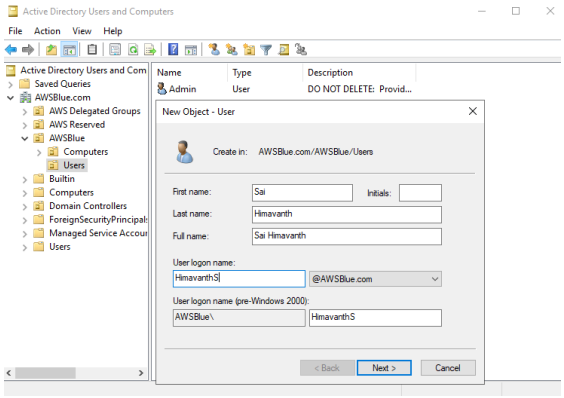


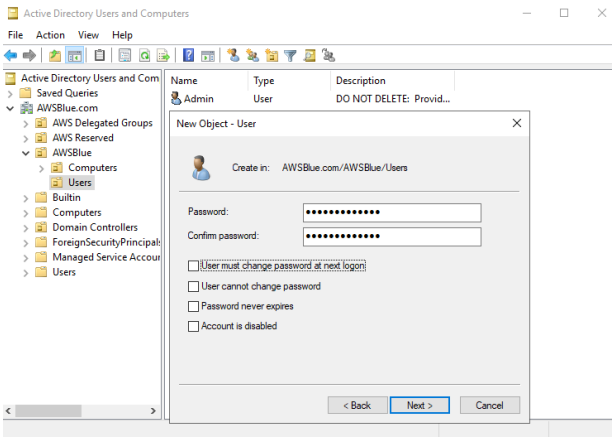
8 - Manage Users and Create New Users

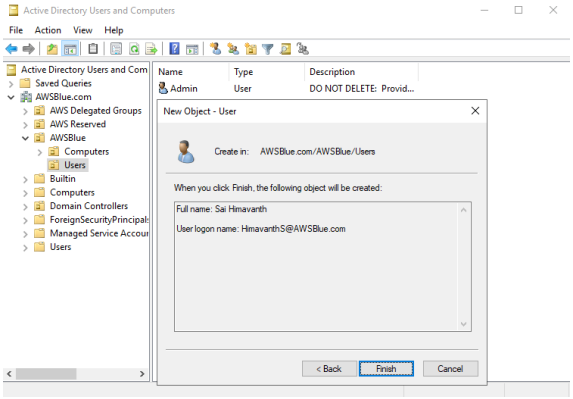
- In the "Active Directory Users and Computers" window, expand your domain (e.g., `AWSBlue.com`).
- Right-click on the "Users" container or any OU (Organizational Unit) where you want to create new users.
- Select "New" and then "User."
- Fill in the required details for the new user (e.g., First name, Last name, User logon name).
- Click "Next" and set the password for the new user.
- Configure the user account options as needed (e.g., Password never expires).
- Click "Next" and then "Finish" to create the user.
- After creating the user, right-click on the user account and select "Properties."
- Go to the "General" tab and enter the user's email address.
- Click "OK" to save the changes.

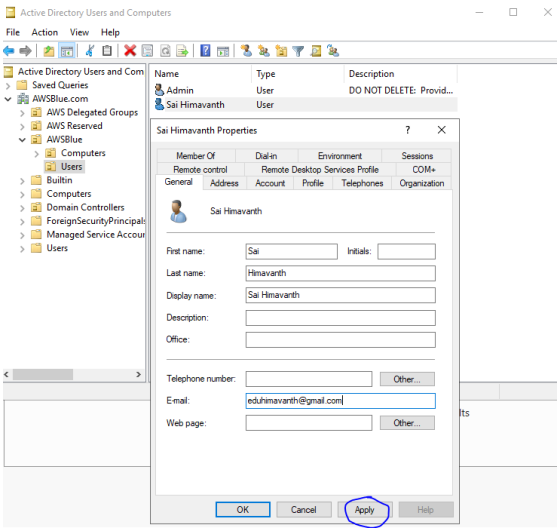
Note: Providing the user's email address is mandatory for AWS SSO to sync with the AD in future use cases.

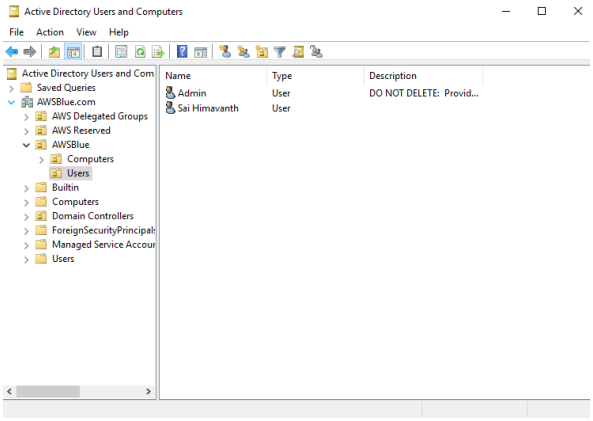












TASK: Verifying the Access of a Created User in AWS Managed Microsoft AD:

1 - Launch and join a Windows Instance to the Domain

- Launch a Windows instance in the same VPC as your AD.
- Join the instance to the domain using AD admin credentials.

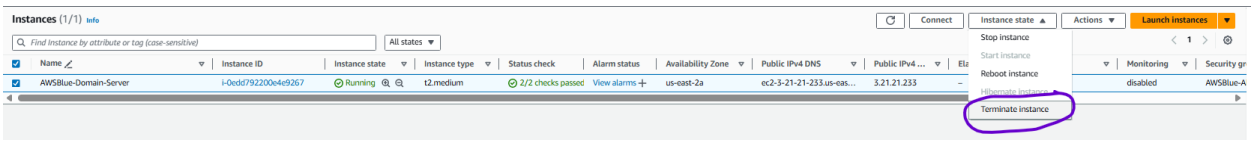
2 - Connect to the Windows Instance

- Use the RDP client to connect to the instance.
- Log in with the newly created user's credentials (e.g., `DOMAIN\NewUser`).

3 - Verify User Access

- Confirm the user can log in and access the desktop.
- Check network shares and file access permissions.
- Verify internet access if applicable.

Note: Make sure to terminate every instance deployed and every resource created to avoid heavy charges.



Case 2: Attaching the AWS Managed Microsoft AD to an Existing EC2 Instance

If there is already an EC2 instance launched and you need to attach the created Active Directory to the existing EC2 Windows machine, follow the steps below.

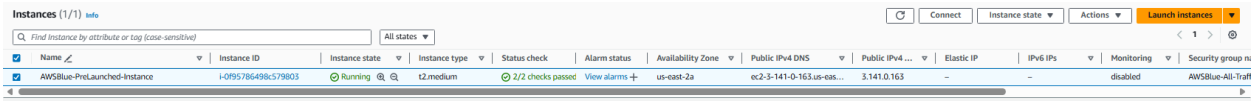
Note: DHCP Options set is not required for this process.

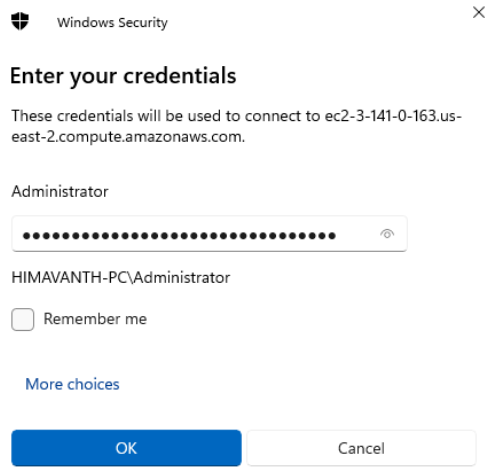
1 - Ensure Active Directory is Configured:

- Confirm that your AWS Managed Microsoft AD is set up and configured correctly.

2 - Connect to the Existing EC2 Instance:

- Open the EC2 Dashboard in the AWS Management Console.
- Select the existing Windows EC2 instance.
- Click "Connect" and choose the "RDP Client" tab.
- Download the RDP file and use it to connect to the instance with the default administrator credentials.

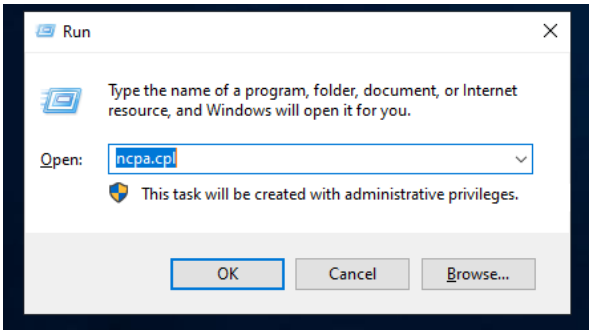


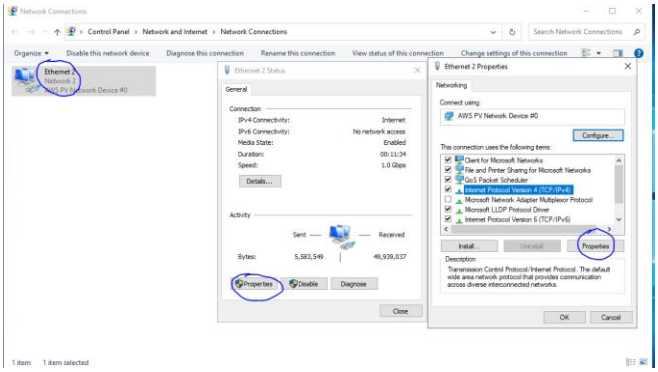


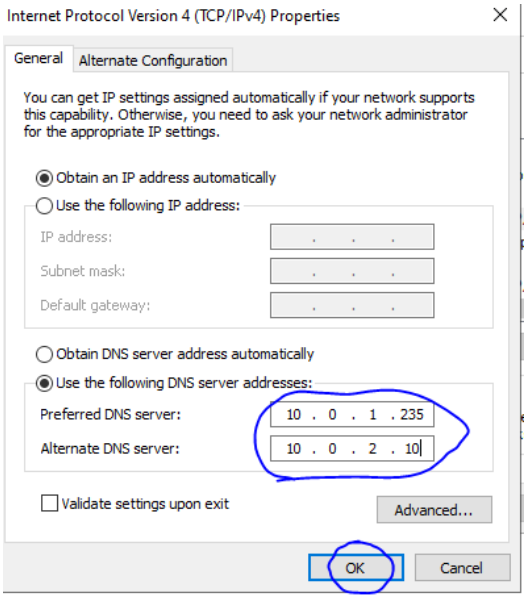
Note: Before launching the above instance, I detached the DHCP Option Sets from AWSBlue-VPC and deleted the AWSBlue-DHCP-Optionsets.

3 - Update DNS IP Addresses:

- Open the "Network Connections" by typing `ncpa.cpl` in the Run dialog (press `Win + R`).
- Right-click on the active network connection and select "Properties."
- Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties."
- Choose "Use the following DNS server addresses" and enter the IP addresses of your AWS Managed Microsoft AD DNS servers.
- Click "OK" to apply the changes.

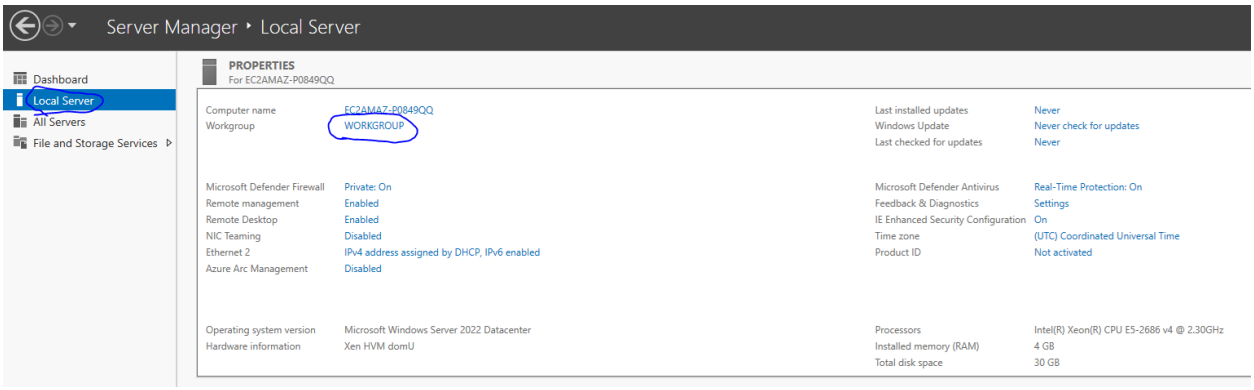


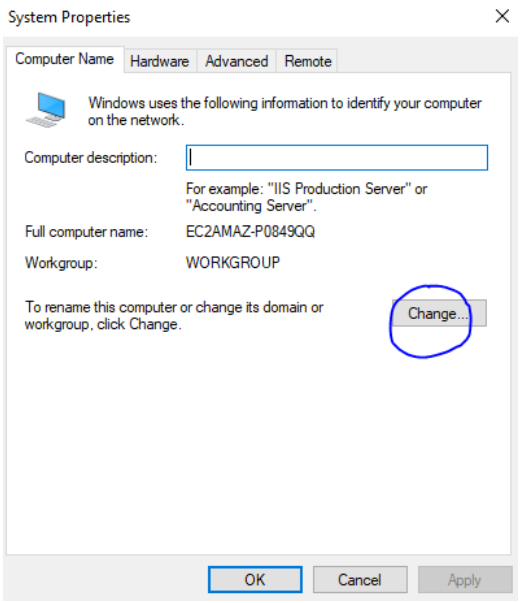


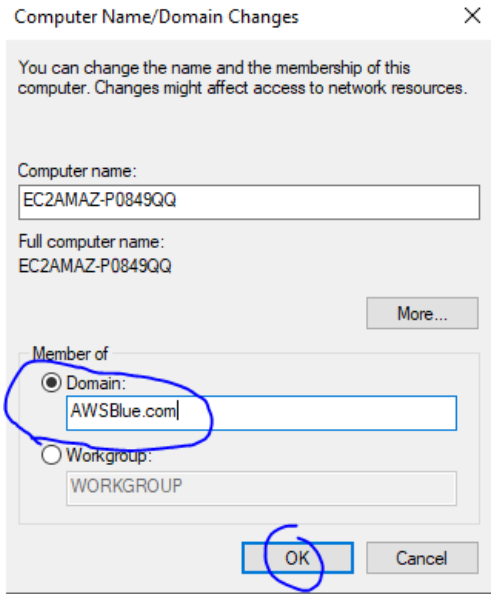


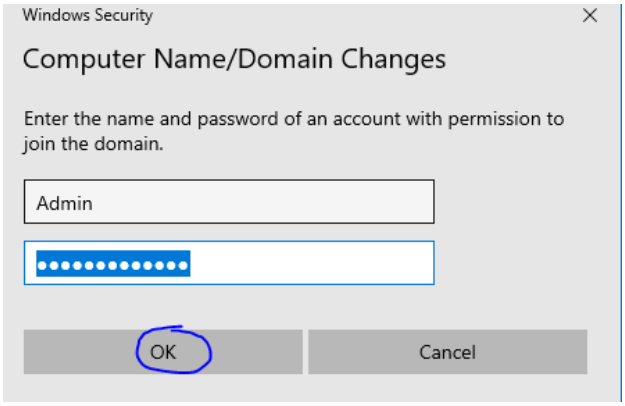
4 - Join the Instance to the Domain:

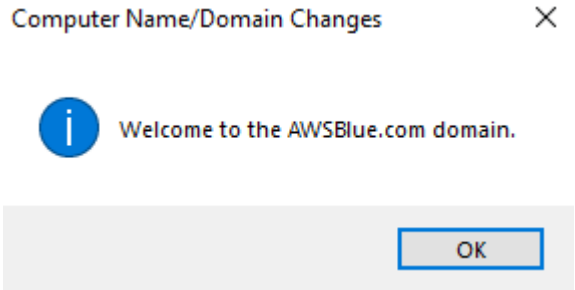
- Open "Server Manager" in the Windows instance.
- Click "Local Server" in the left pane.
- Next to "Computer name," click on "Workgroup" and then "Change."
- Select "Domain" and enter the domain name of your AWS Managed Microsoft AD (e.g., `corp.example.com`).
- Click "OK" and enter the AD admin credentials when prompted.
- Restart the instance to complete the domain join process.

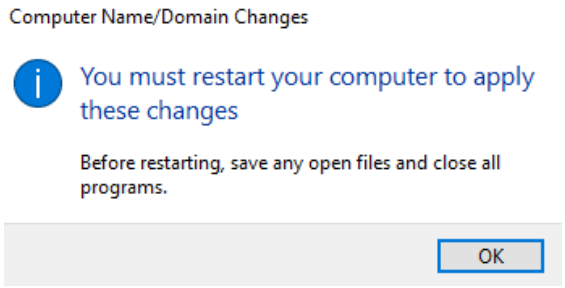

Server Manager • Local Server
Dashboard
Local Server
All Servers
File and Storage Services
PROPERTIES
For EC2AMAZ-P0849QQ
Computer name
EC2AMAZ-P0849QQ
Workgroup
WORKGROUP
Last installed updates
Never
Windows Update
Never check for updates
Last checked for updates
Never
Microsoft Defender Firewall
Private: On
Remote management
Enabled
Remote Desktop
Enabled
NIC Teaming
Disabled
Ethernet 2
IPv4 address assigned by DHCP, IPv6 enabled
Azure Arc Management
Disabled
Microsoft Defender Antivirus
Real-Time Protection: On
Feedback & Diagnostics
Settings
IE Enhanced Security Configuration
On
Time zone
(UTC) Coordinated Universal Time
Product ID
Not activated
Operating system version
Microsoft Windows Server 2022 Datacenter
Hardware information
Xen HVM domU
Processors
Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz
Installed memory (RAM)
4 GB
Total disk space
30 GB


System Properties
Computer Name
Hardware
Advanced
Remote
Windows uses the following information to identify your computer on the network.
Computer description:
For example: "IIS Production Server" or "Accounting Server".
Full computer name:
EC2AMAZ-P0849QQ
Workgroup:
WORKGROUP
To rename this computer or change its domain or workgroup, click Change.
Change...
OK
Cancel
Apply


Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer name:
EC2AMAZ-P0849QQ
Full computer name:
EC2AMAZ-P0849QQ
More...
Member of
Domain:
AWSBlue.com
Workgroup:
WORKGROUP
OK
Cancel

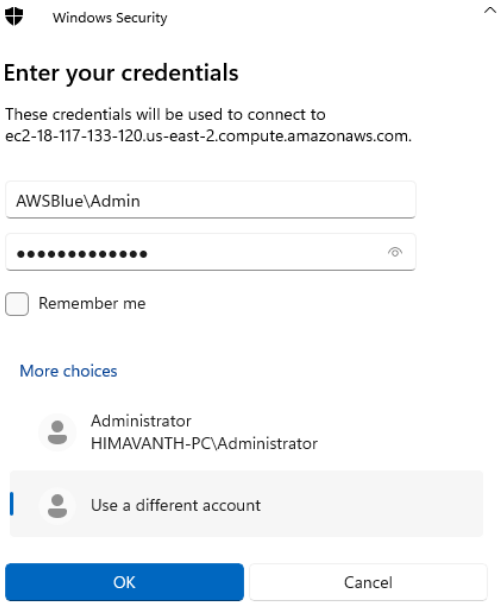

Windows Security
Computer Name/Domain Changes
Enter the name and password of an account with permission to join the domain.
Admin
OK
Cancel

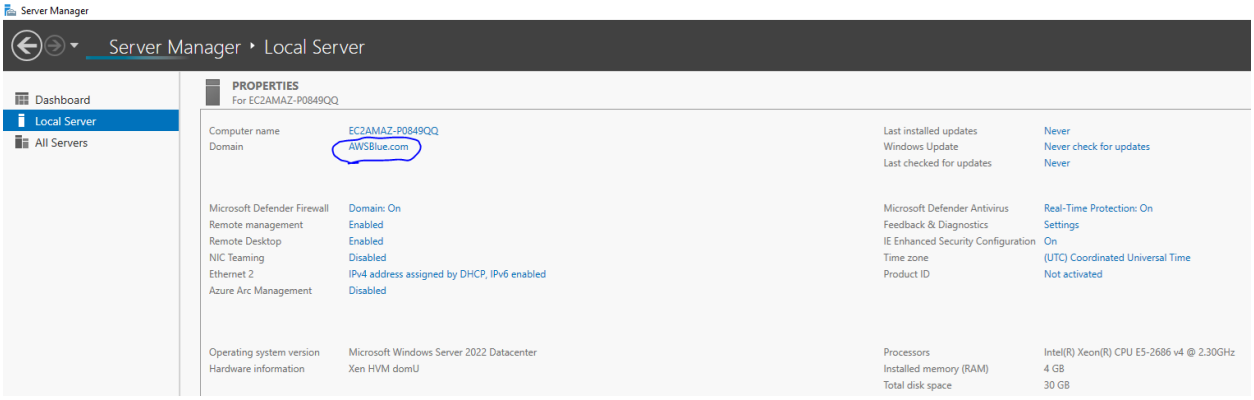

Computer Name/Domain Changes
Welcome to the AWSBlue.com domain.
OK



5 - Verify Domain Join and Re-login with AD Admin Credentials:

- After the instance restarts, reconnect using RDP.
- At the login screen, select "Other user."
- Enter the AD admin credentials (e.g., CORP\Administrator).
- Verify that you can log in and access domain resources, confirming the instance is successfully joined to the AD.





Note: Installing the AD roles allows you to manage the AD, its users, and computers.

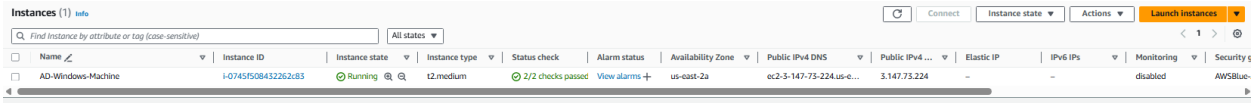
Case 3 - Installing an Active Directory on a Windows EC2 Instance

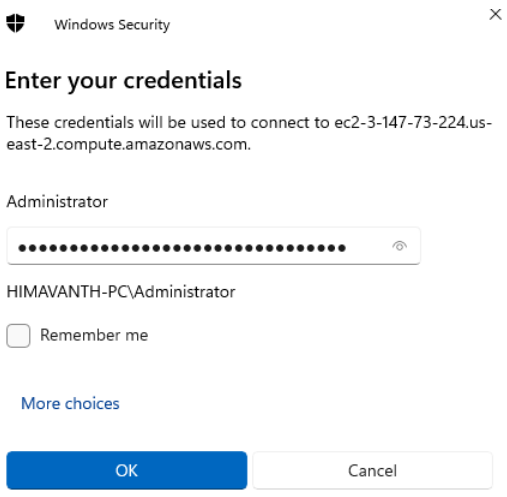
In this scenario, we have an EC2 Windows machine in AWS and are not using AWS Managed Microsoft AD. Instead, we are installing AD directly on the Windows machine.

Note: I have deleted the previously created AWS Managed Microsoft AD and its respective DHCP Option sets. You need to launch a new Windows EC2 instance and follow the steps below to install Active Directory on the Windows machine.

1 - Connect to the EC2 Instance

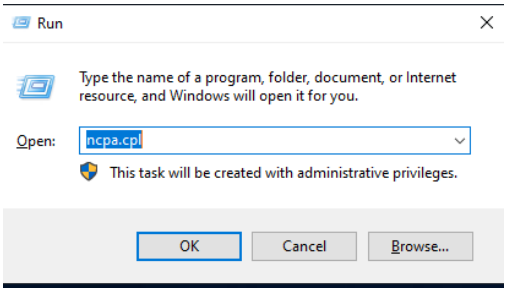
- Open the EC2 Dashboard in the AWS Management Console.
- Select the existing Windows EC2 instance.
- Click "Connect" and choose the "RDP Client" tab.
- Download the RDP file and use it to connect to the instance with the default administrator credentials.

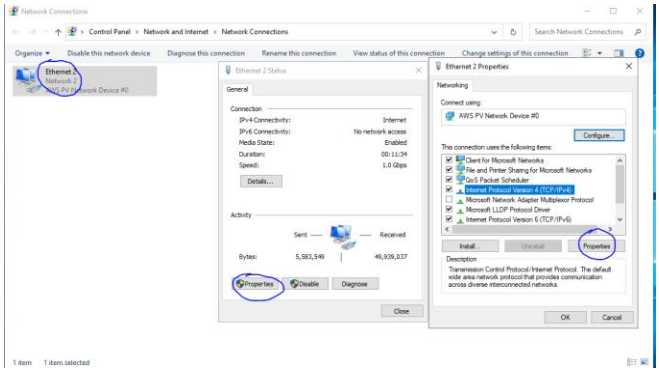


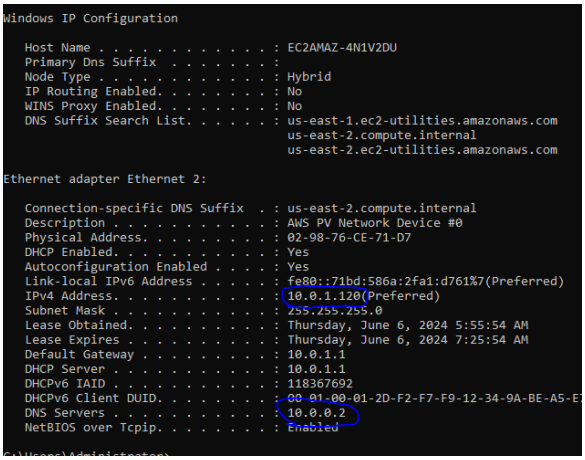


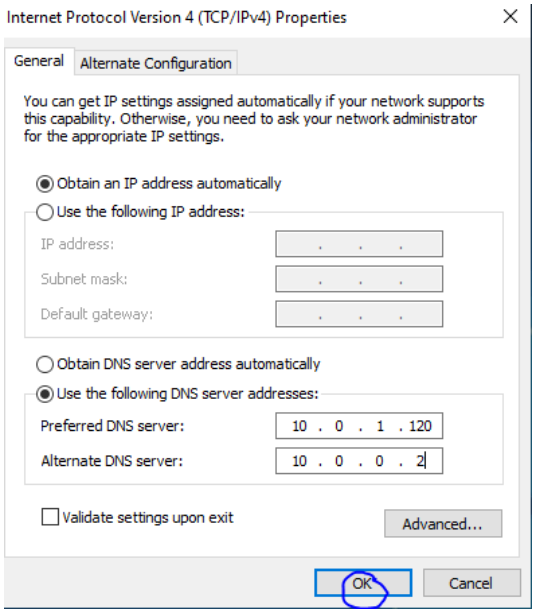
2 - Update DNS IP Addresses

- Open "Network Connections" by typing `ncpa.cpl` in the Run dialog (press `Win + R`).
- Right-click on the active network connection and select "Properties."
- Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties."
- Choose "Use the following DNS server addresses" and enter the IP address of the new domain controller (usually the same as the instance's private IP).
- To find the instance's private IP:
- Open Command Prompt and type `ipconfig`.
- Look for the "IPv4 Address" under the active network connection.
- Click "OK" to apply the changes.





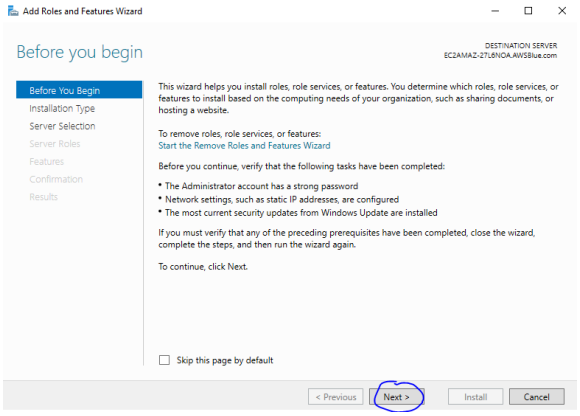


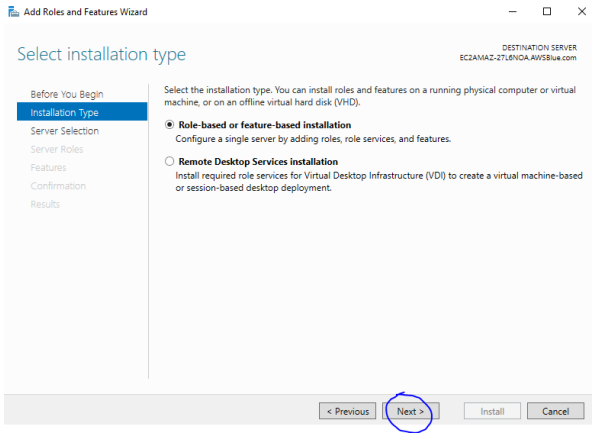


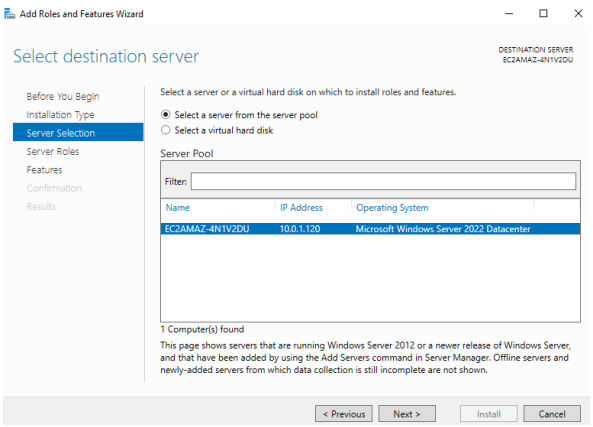
2 - Install Active Directory Domain Services (AD DS)

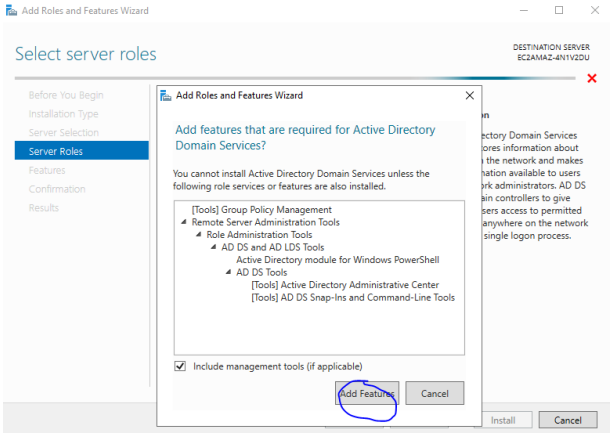
- Open "Server Manager" on the Windows instance.
- Click "Add roles and features" to open the wizard.
- Click "Next" through the wizard until you reach the "Server Roles" page.
- Select "Active Directory Domain Services" and click "Next."
- In the "Features" page, scroll down and expand "Remote Server Administration Tools."
- Expand "Role Administration Tools."
- Select "AD DS and AD LDS Tools" and ensure all sub-options are checked.
- Proceed through the wizard, accepting the default selections, and click "Install" on the confirmation page.
- Wait for the installation to complete and then click "Close."

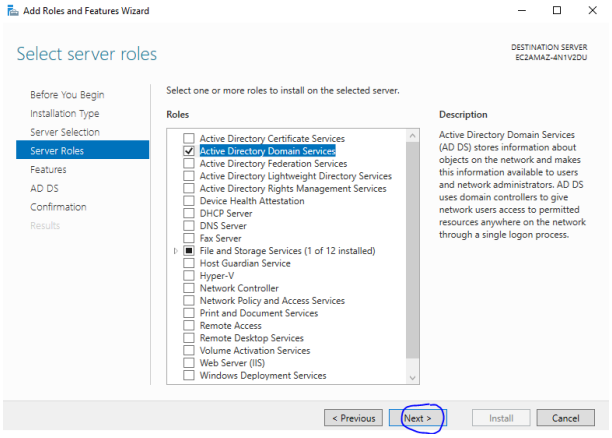

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide

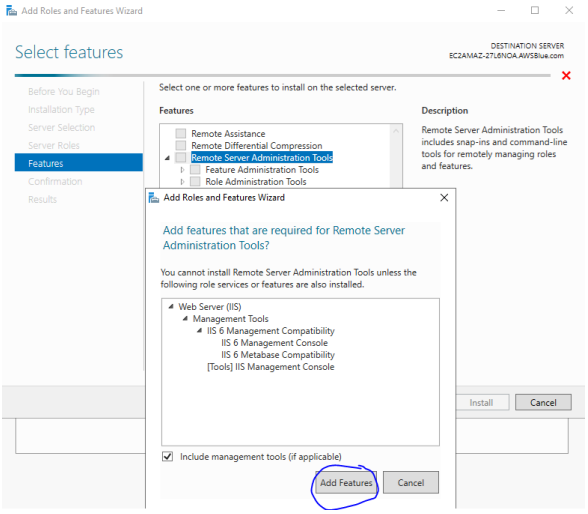

Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
EC2AMAZ-27L6NOA.AWSBlue.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel

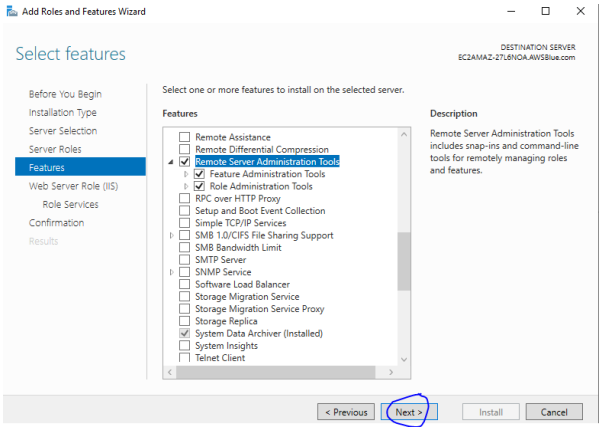

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
EC2AMAZ-27L6NOA.AWSBlue.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel

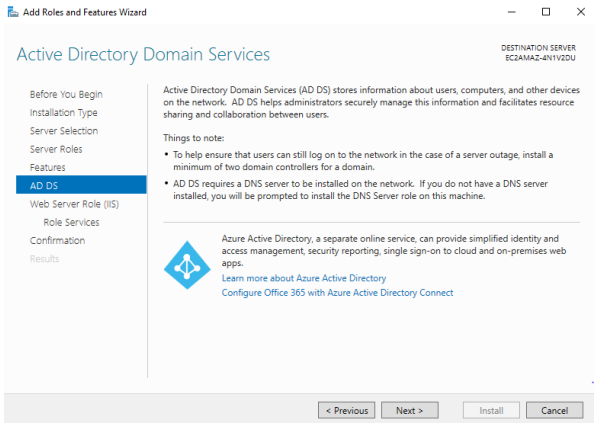

Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
EC2AMAZ-4N1V2DU
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
EC2AMAZ-4N1V2DU
10.0.1.120
Microsoft Windows Server 2022 Datacenter
1 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel

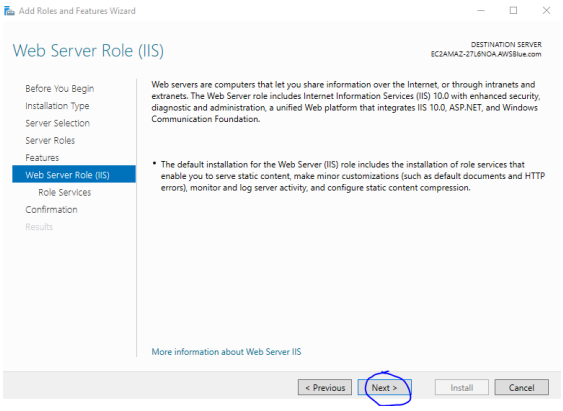

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
EC2AMAZ-4N1V2DU
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for Active Directory Domain Services?
You cannot install Active Directory Domain Services unless the following role services or features are also installed.
[Tools] Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
[Tools] Active Directory Administrative Center
[Tools] AD DS Snap-Ins and Command-Line Tools
Include management tools (if applicable)
Add Features
Cancel
Install
Cancel

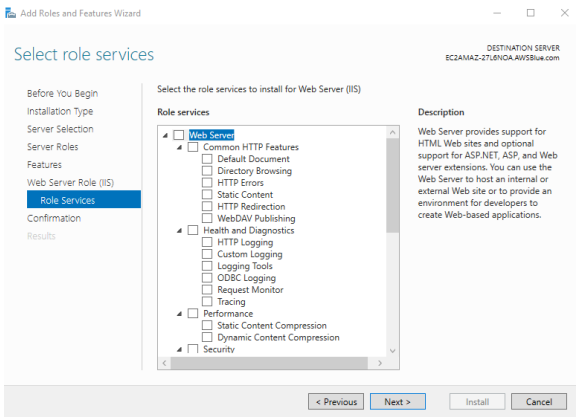

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
EC2AMAZ-4N1V2DU
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Description
Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
< Previous
Next >
Install
Cancel

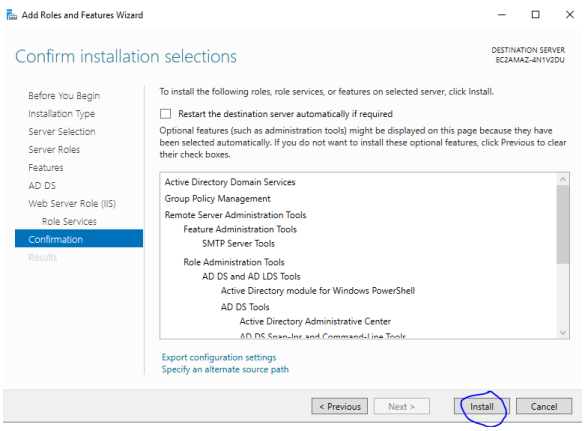

Add Roles and Features Wizard
Select features
DESTINATION SERVER
EC2AMAZ-27L6NOA.AWSBlue.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more features to install on the selected server.
Features
Remote Assistance
Remote Differential Compression
Remote Server Administration Tools
Feature Administration Tools
Role Administration Tools
Description
Remote Server Administration Tools includes snap-ins and command-line tools for remotely managing roles and features.
Add Roles and Features Wizard
Add features that are required for Remote Server Administration Tools?
You cannot install Remote Server Administration Tools unless the following role services or features are also installed.
Web Server (IIS)
Management Tools
IIS 6 Management Compatibility
IIS 6 Management Console
IIS 6 Metabase Compatibility
[Tools] IIS Management Console
Include management tools (if applicable)
Add Features
Cancel
Install
Cancel

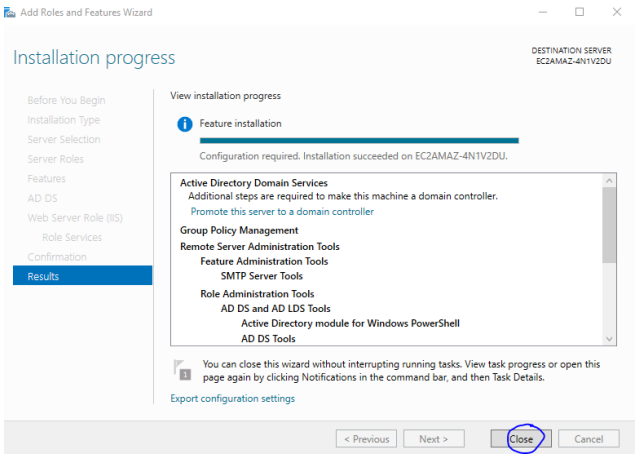

Add Roles and Features Wizard
Select features
DESTINATION SERVER
EC2AMAZ-27L6NOA.AWSBlue.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select one or more features to install on the selected server.
Features
Remote Assistance
Remote Differential Compression
Remote Server Administration Tools
Feature Administration Tools
Role Administration Tools
RPC over HTTP Proxy
Setup and Boot Event Collection
Simple TCP/IP Services
SMB 1.0/CIFS File Sharing Support
SMB Bandwidth Limit
SMTP Server
SNMP Service
Software Load Balancer
Storage Migration Service
Storage Migration Service Proxy
Storage Replica
System Data Archiver (Installed)
System Insights
Telnet Client
Description
Remote Server Administration Tools includes snap-ins and command-line tools for remotely managing roles and features.
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Active Directory Domain Services
DESTINATION SERVER
EC2AMAZ-4N1V2DU
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Web Server Role (IIS)
Role Services
Confirmation
Results
Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.
Things to note:
To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.
Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.
Learn more about Azure Active Directory
Configure Office 365 with Azure Active Directory Connect
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Web Server Role (IIS)
DESTINATION SERVER
EC2AMAZ-27L6NOA.AWSBlue.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 10.0 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 10.0, ASP.NET, and Windows Communication Foundation.
The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.
More information about Web Server IIS
< Previous
Next >
Install
Cancel

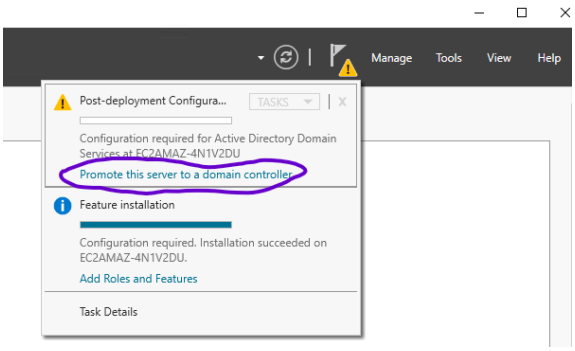

Add Roles and Features Wizard
Select role services
DESTINATION SERVER
EC2AMAZ-27L6NOA.AWSBlue.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Web Server (IIS)
Role services
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
HTTP Redirection
WebDAV Publishing
Health and Diagnostics
HTTP Logging
Custom Logging
Logging Tools
ODBC Logging
Request Monitor
Tracing
Performance
Static Content Compression
Dynamic Content Compression
Security
Description
Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
< Previous
Next >
Install
Cancel

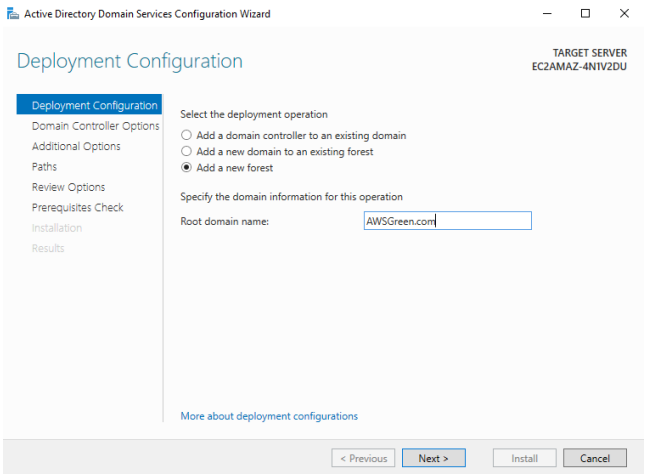


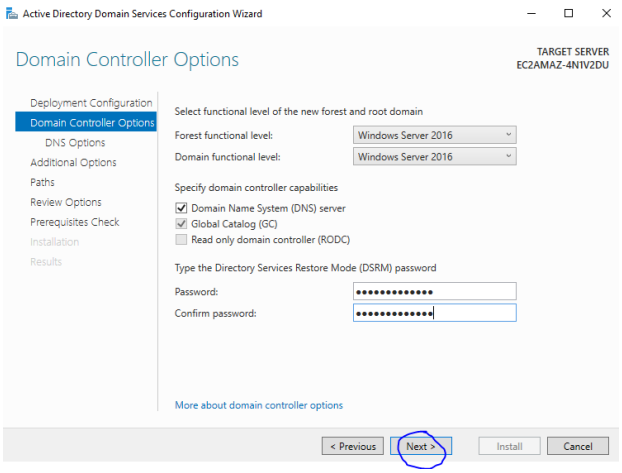


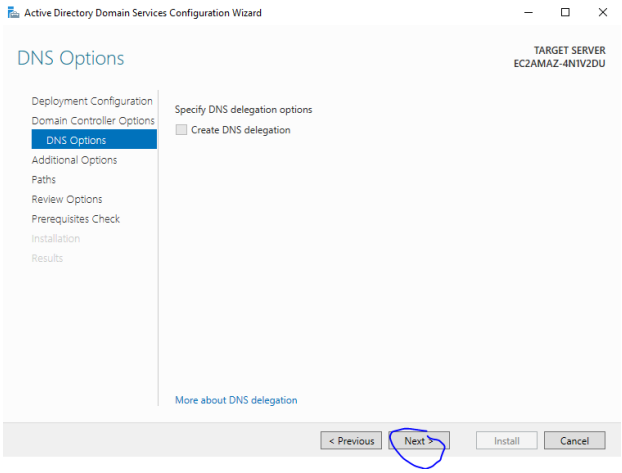
3 - Promote the Server to a Domain Controller

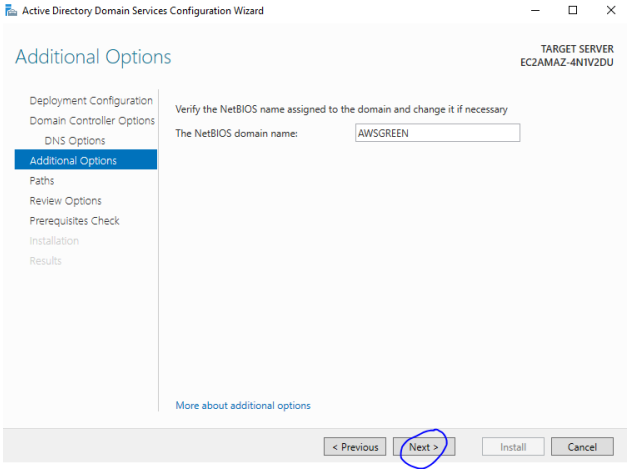
- After the AD DS role is installed, a notification will appear in the "Server Manager" indicating additional steps are required.
- Click the notification flag and select "Promote this server to a domain controller."
- In the "Deployment Configuration" tab, select "Add a new forest" and enter a root domain name (e.g., `corp.example.com`).
- Click "Next" and follow the prompts to configure the domain controller options, DNS options, and additional settings.
- Set a Directory Services Restore Mode (DSRM) password when prompted.
- Continue through the wizard, review the selections, and click "Install" on the final page.

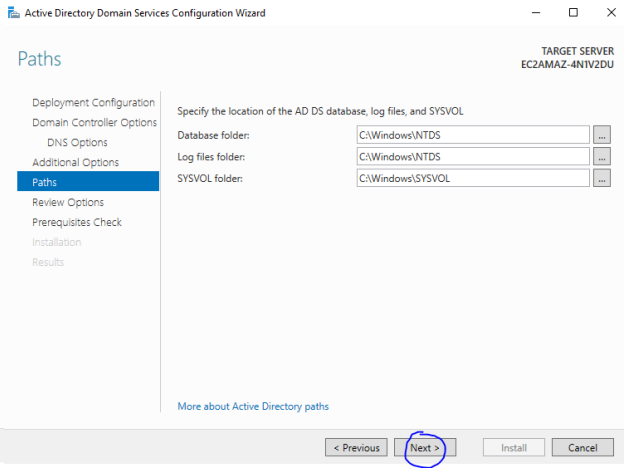


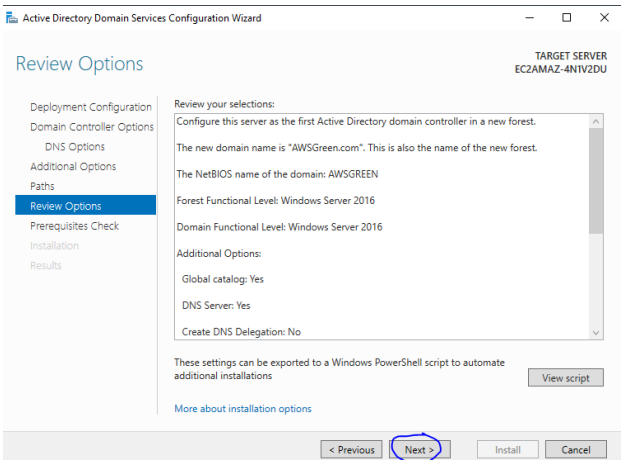


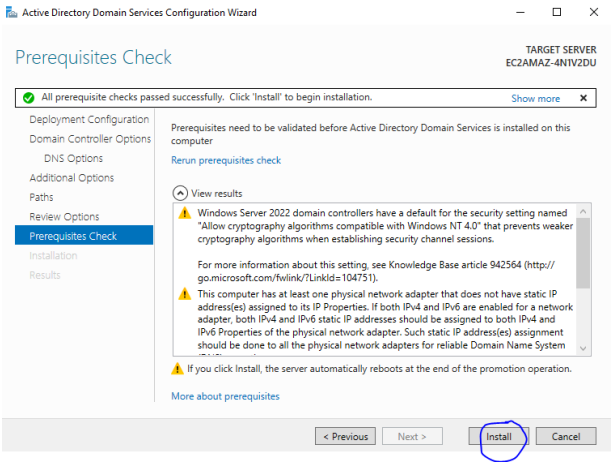








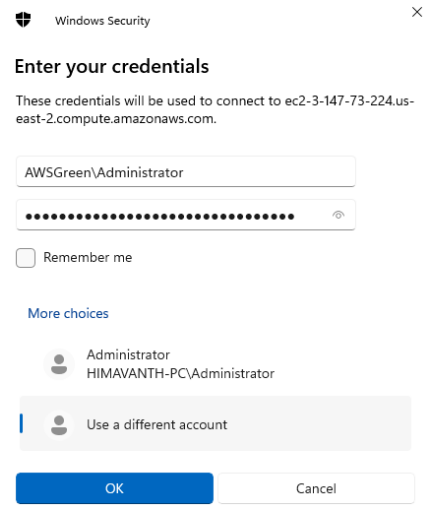


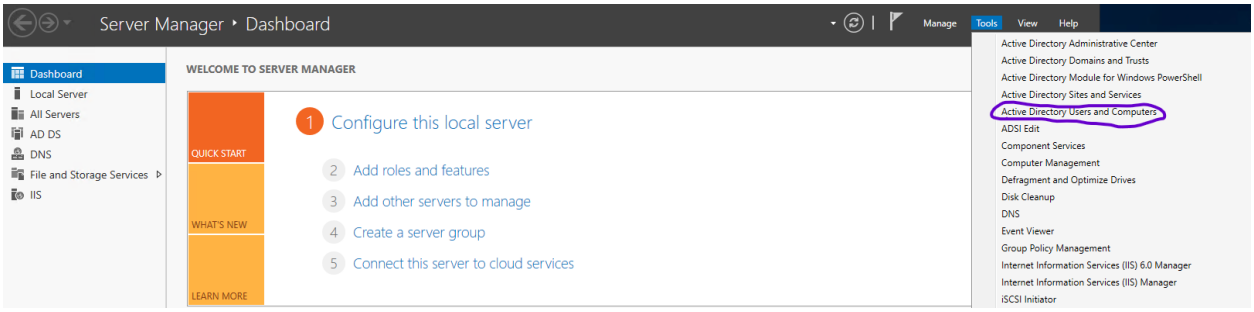


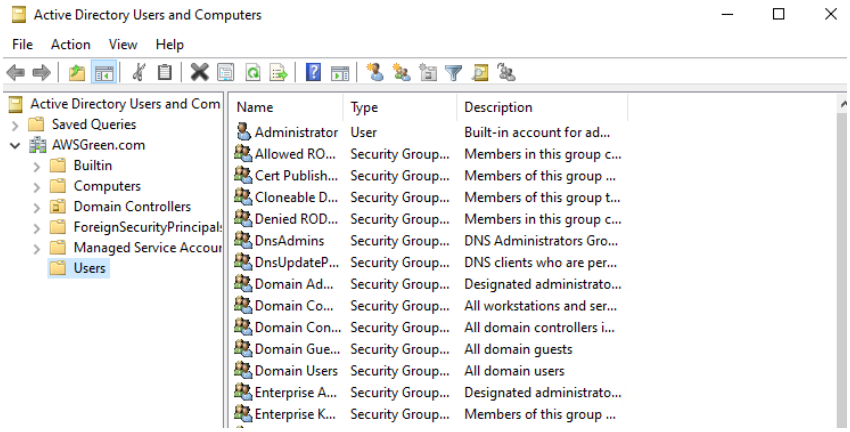
Note: After Installation the system automatically reboots. Relogin into the system with the Active Directory Administrator Credentials.

5 - Verify Active Directory Installation

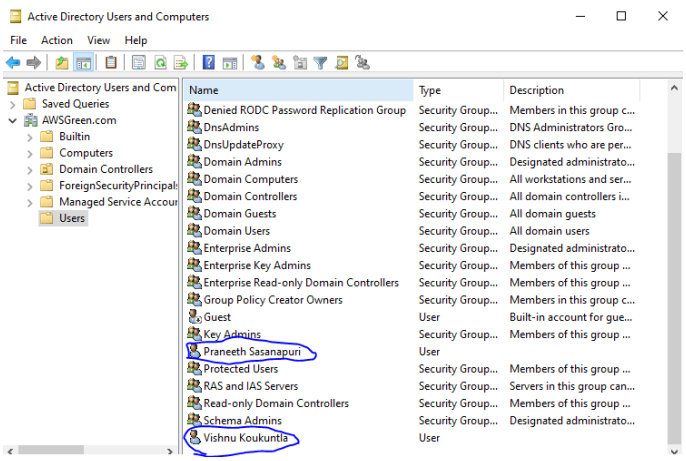
- After the server restarts, reconnect using RDP.
- Log in with the domain credentials (e.g., `CORP\Administrator`).
- Open "Active Directory Users and Computers" to verify the AD installation.
- Ensure you can manage the domain, users, and computers.







Note: Create users in the Active Directory to confirm its functionality.



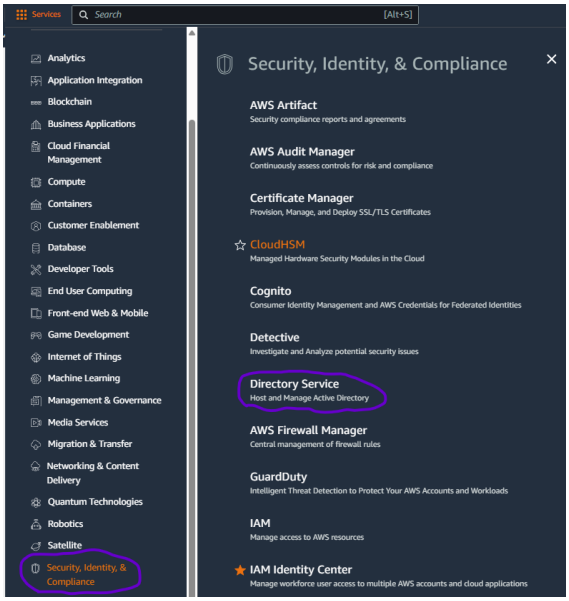
I have added two users to the Active Directory. We will use these users for our next task, which is synchronizing the Active Directory with AWS SSO using AD Connector.

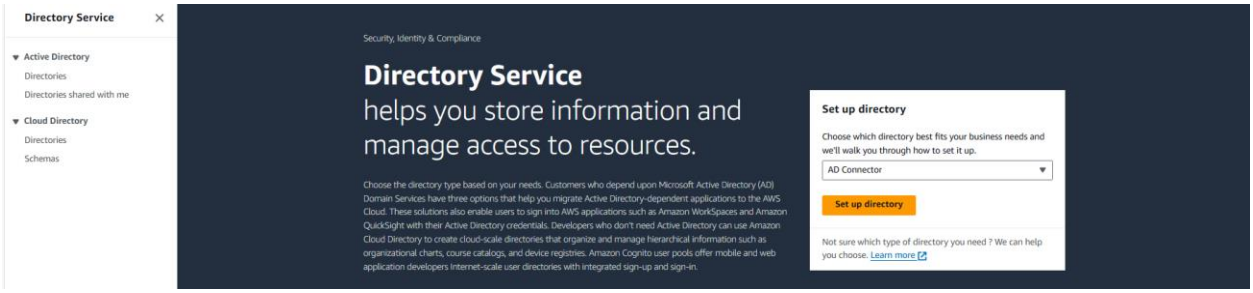
Note: Ensure that the email addresses for the created users are provided, as this is mandatory for AWS SSO to sync with the AD.

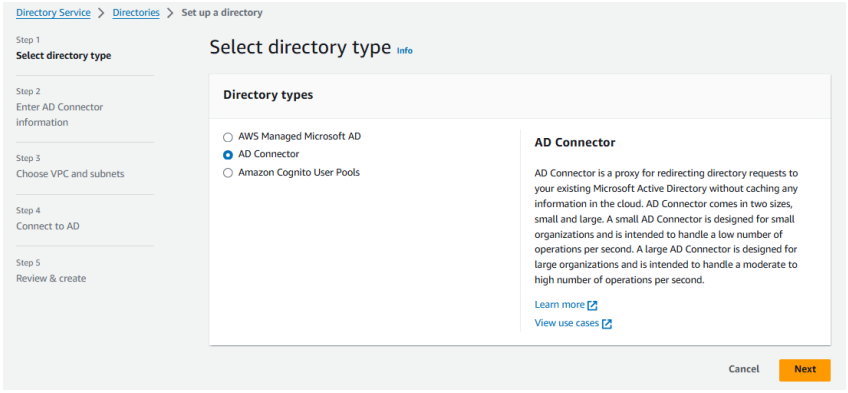
Case 4: Setting Up AWS AD Connector and Synchronizing the AD from Case 3 with AWS SSO to Grant AWS Access to AD Users

1 - Navigate to Directory Service

- In the top navigation bar, click on "Services."
- Under "Security, Identity, & Compliance," select "Directory Service."
- On the AWS Directory Service dashboard, click on "Set up directory."
- Select "AD Connector."
- Click "Next."

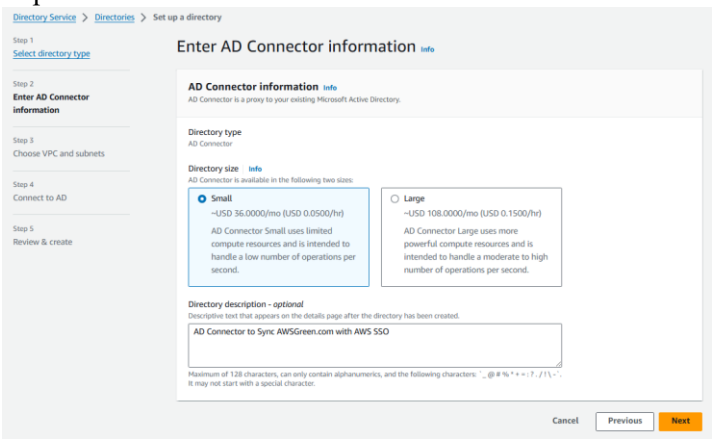


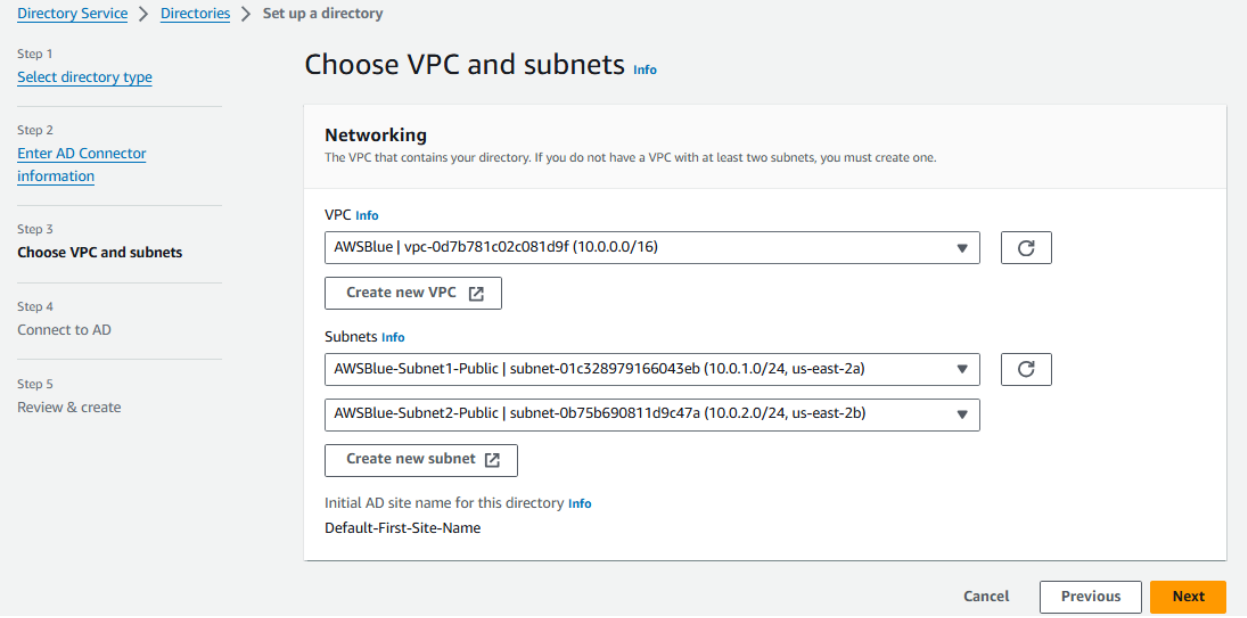


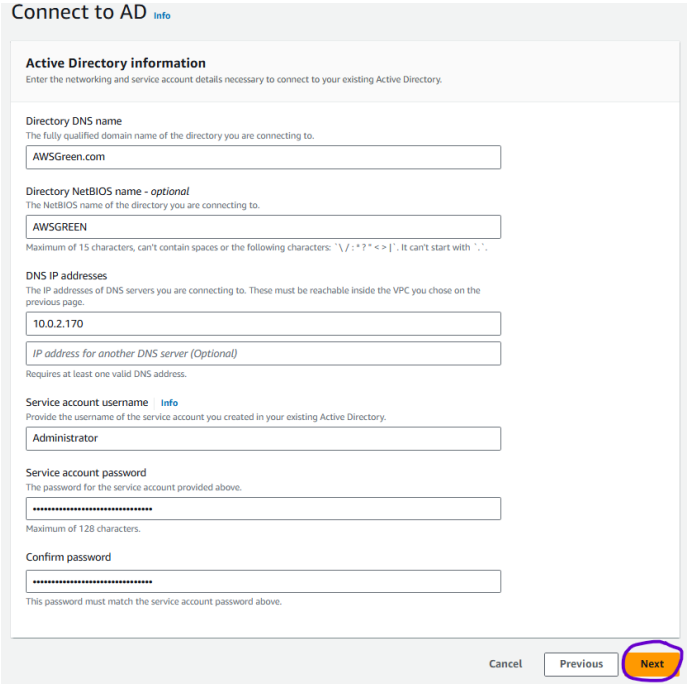


2 - Configure Directory Details

- **Connector Type:** Choose the appropriate type (Small or Large) based on your requirements.
- **Description:** (Optional) Enter a description for the AD Connector.
- **VPC:** Select the VPC where the AD Connector will be deployed.
- **Subnets:** Choose two subnets in different Availability Zones for high availability.
- **Directory DNS Name:** Enter the fully qualified domain name (FQDN) of your on-premises AD (e.g., corp.example.com).
- **NetBIOS Name:** Enter the NetBIOS name of your on-premises AD (e.g., AWSGREEN).
- **DNS IP Addresses:** Enter the IP addresses of your on-premises DNS servers.
- **Username:** Enter the username of an account with sufficient permission to connect to the on-premises AD
- **Password:** Enter the password for the above account.

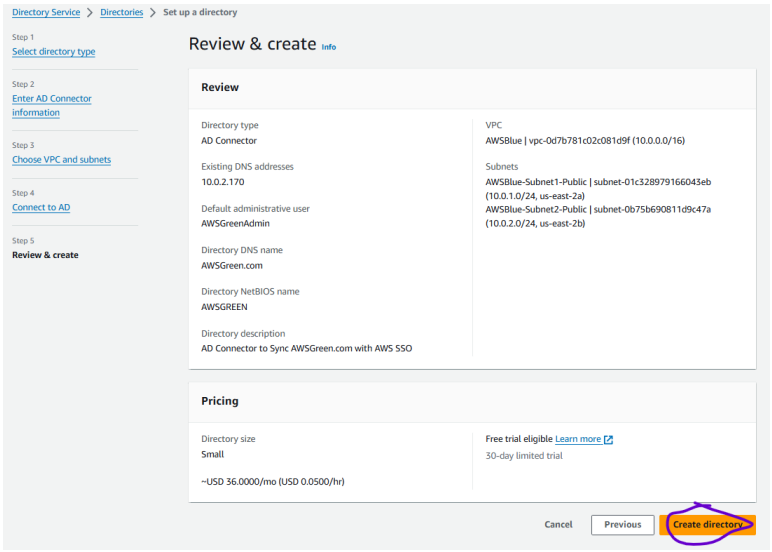


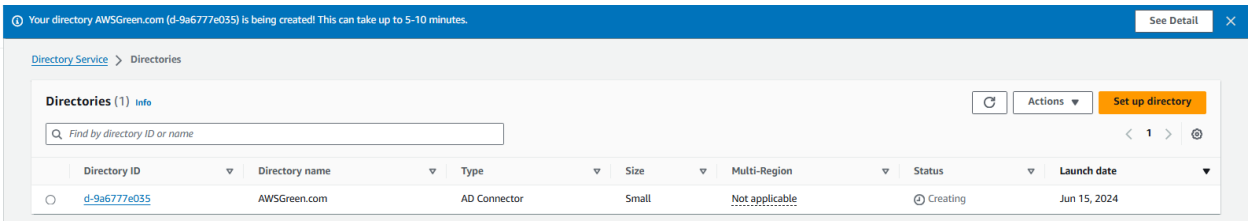




3 - Review and Create:

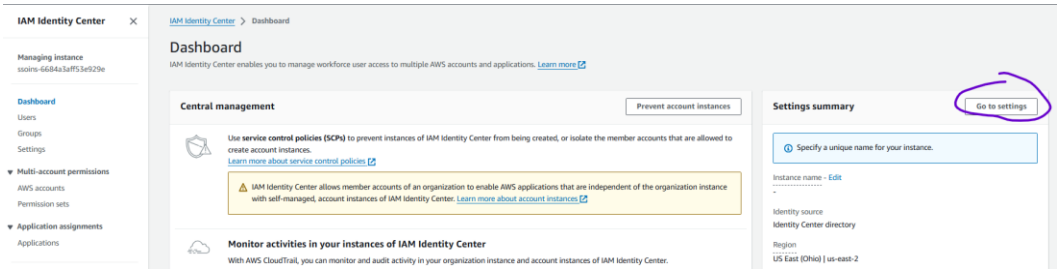
- Review the configuration details.
- Click "Create AD Connector."

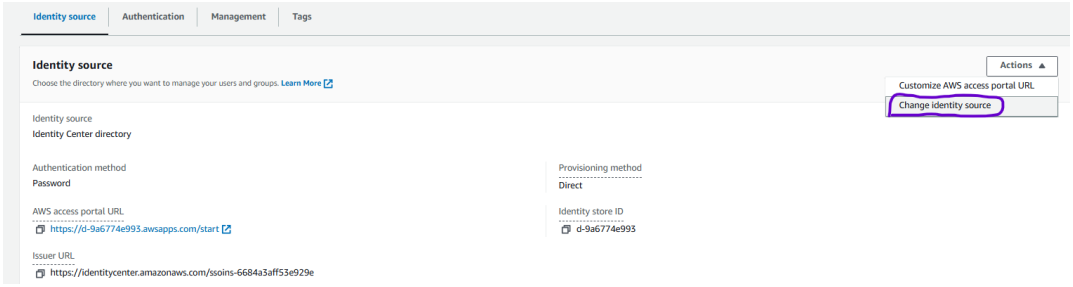


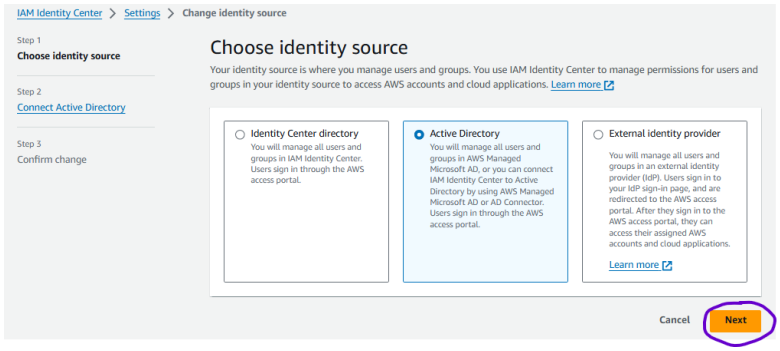


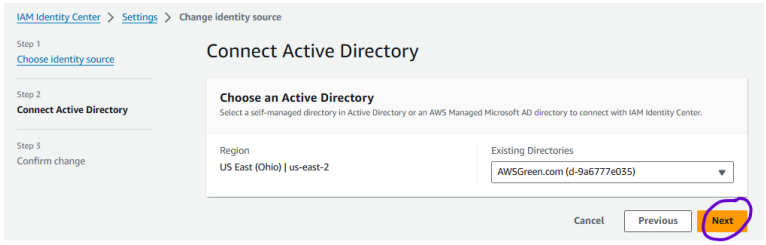
4 - Configure AWS Identity Center

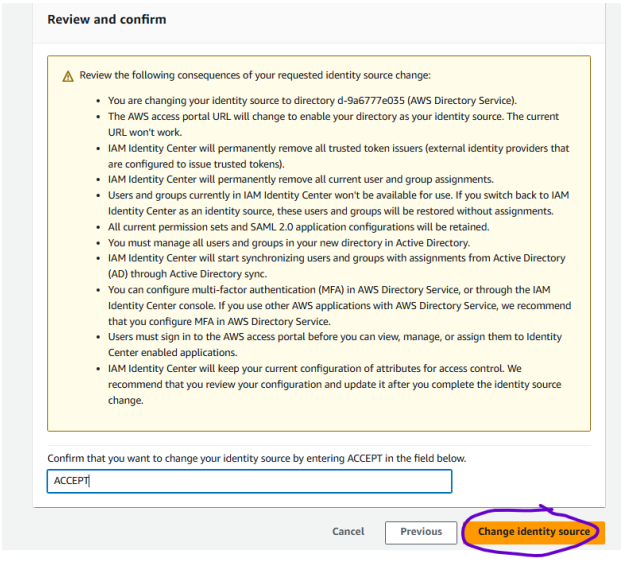
- Navigate to the AWS Identity Center service in the AWS Management Console.
- Click on "Settings" in the AWS Identity Center dashboard.
- Under "Actions," select "Change Identity Source" and select “Active Diretcory”
- In the "Active Directory" settings, choose the AD Connector you created.
- Review the details, ACCEPT the change and Click “Change Idendity Source”

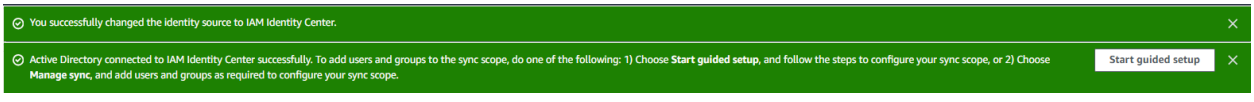



Identity source
Authentication
Management
Tags
Identity source
Choose the directory where you want to manage your users and groups. Learn More
Actions
Customize AWS access portal URL
Change identity source
Identity source
Identity Center directory
Authentication method
Password
Provisioning method
Direct
AWS access portal URL
https://d-9a6774e993.awsapps.com/start
Identity store ID
d-9a6774e993
Issuer URL
https://identitycenter.amazonaws.com/ssoins-6684a3aff53e929e


IAM Identity Center > Settings > Change identity source
Step 1
Choose identity source
Step 2
Connect Active Directory
Step 3
Confirm change
Choose identity source
Your identity source is where you manage users and groups. You use IAM Identity Center to manage permissions for users and groups in your identity source to access AWS accounts and cloud applications. Learn more
Identity Center directory
You will manage all users and groups in IAM Identity Center. Users sign in through the AWS access portal.
Active Directory
You will manage all users and groups in AWS Managed Microsoft AD, or you can connect IAM Identity Center to Active Directory by using AWS Managed Microsoft AD or AD Connector. Users sign in through the AWS access portal.
External identity provider
You will manage all users and groups in an external identity provider (IdP). Users sign in to your IdP sign-in page, and are redirected to the AWS access portal. After they sign in to the AWS access portal, they can access their assigned AWS accounts and cloud applications.
Learn more
Cancel
Next

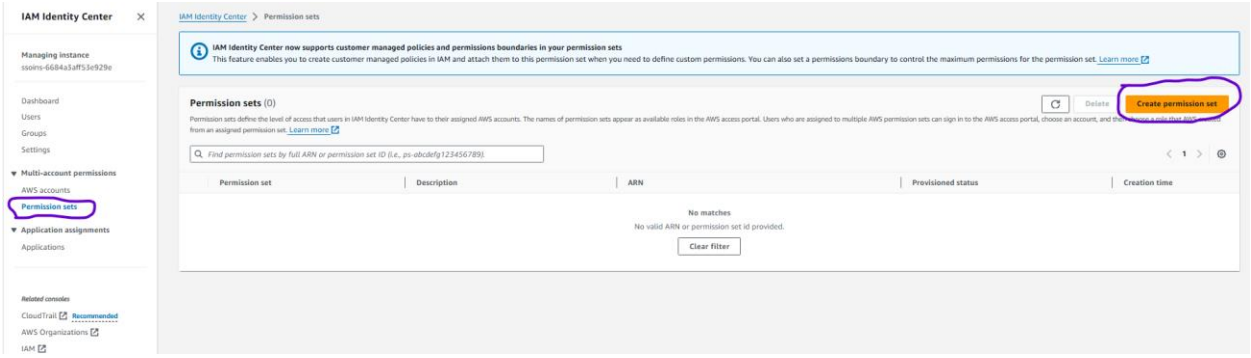

IAM Identity Center > Settings > Change identity source
Step 1
Choose identity source
Step 2
Connect Active Directory
Step 3
Confirm change
Connect Active Directory
Choose an Active Directory
Select a self-managed directory in Active Directory or an AWS Managed Microsoft AD directory to connect with IAM Identity Center.
Region
US East (Ohio) | us-east-2
Existing Directories
AWSGreen.com (d-9a6777e035)
Cancel
Previous
Next

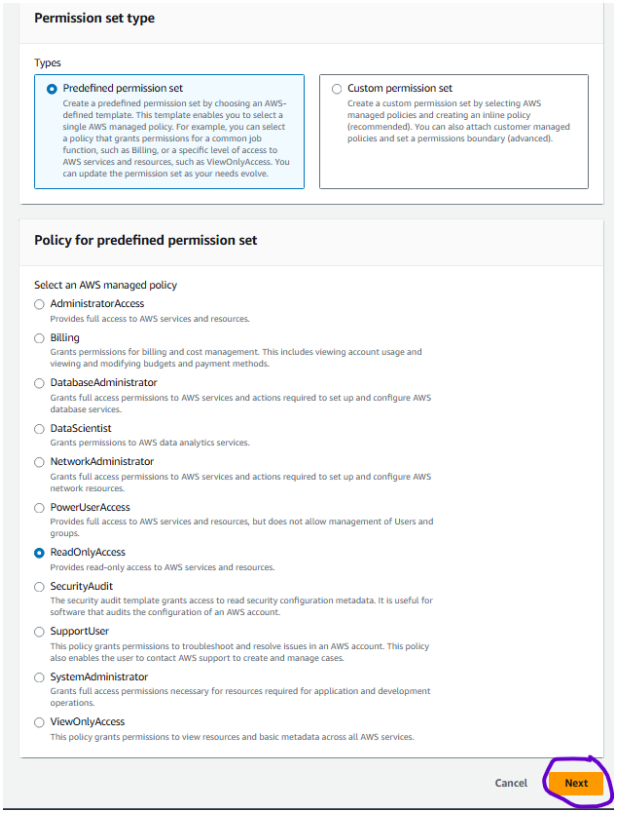

Review and confirm
Review the following consequences of your requested identity source change:
You are changing your identity source to directory d-9a6777e035 (AWS Directory Service).
The AWS access portal URL will change to enable your directory as your identity source. The current URL won't work.
IAM Identity Center will permanently remove all trusted token issuers (external identity providers that are configured to issue trusted tokens).
IAM Identity Center will permanently remove all current user and group assignments.
Users and groups currently in IAM Identity Center won't be available for use. If you switch back to IAM Identity Center as an identity source, these users and groups will be restored without assignments.
All current permission sets and SAML 2.0 application configurations will be retained.
You must manage all users and groups in your new directory in Active Directory.
IAM Identity Center will start synchronizing users and groups with assignments from Active Directory (AD) through Active Directory sync.
You can configure multi-factor authentication (MFA) in AWS Directory Service, or through the IAM Identity Center console. If you use other AWS applications with AWS Directory Service, we recommend that you configure MFA in AWS Directory Service.
Users must sign in to the AWS access portal before you can view, manage, or assign them to Identity Center enabled applications.
IAM Identity Center will keep your current configuration of attributes for access control. We recommend that you review your configuration and update it after you complete the identity source change.
Confirm that you want to change your identity source by entering ACCEPT in the field below.
ACCEPT
Cancel
Previous
Change identity source

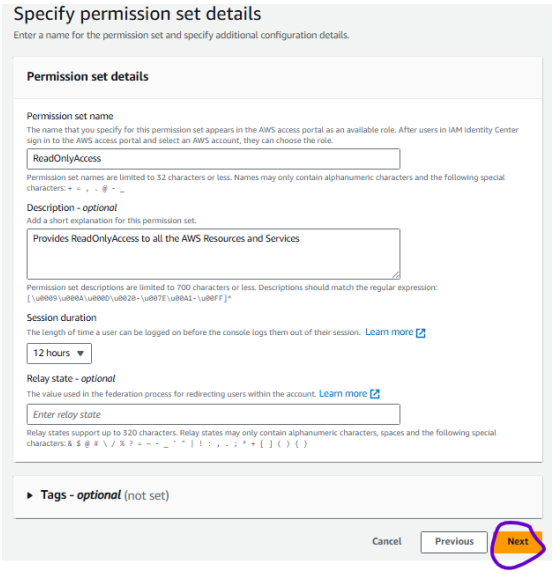

You successfully changed the identity source to IAM Identity Center.
Active Directory connected to IAM Identity Center successfully. To add users and groups to the sync scope, do one of the following: 1) Choose Start guided setup, and follow the steps to configure your sync scope, or 2) Choose Manage sync, and add users and groups as required to configure your sync scope.
Start guided setup

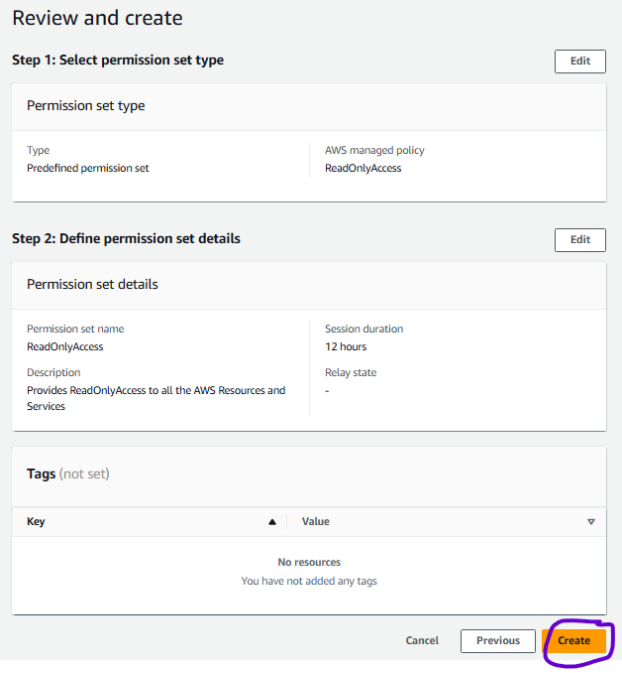
5 - Create a Permission Set

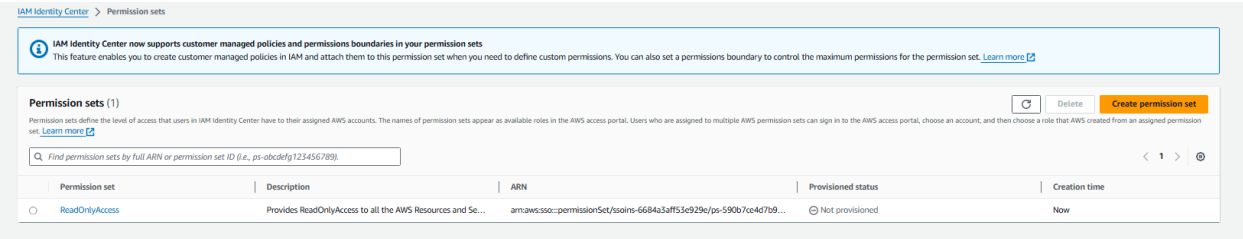
- In the AWS Identity Center dashboard, click on "Permission sets."
- Click "Create permission set."
- Select a Template: Choose "Predefined permission Set" to select the policies provided by AWS.
- **Name and Description:** Provide a name for the permission set (e.g., "ReadOnlyAccess-EC2-VPC-IAM") and an optional description.
- **Policies:** Click "Next" to move to the policy configuration.
- Review the Details and Click on “Create”









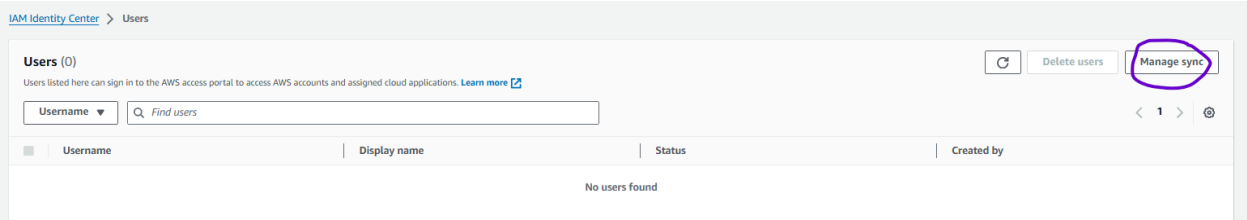


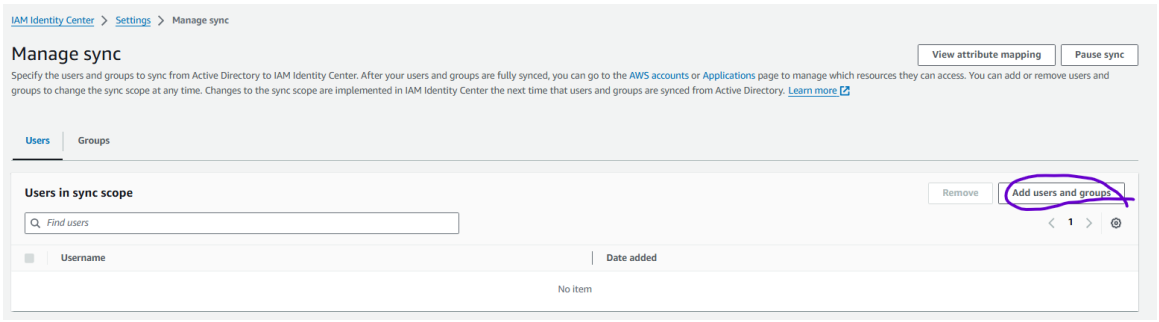
Note: We have chosen predefined permission sets as we haven't gone through the IAM in detail. Once we get more familiar with IAM, we can create custom policies and permission sets based on our specific requirements.

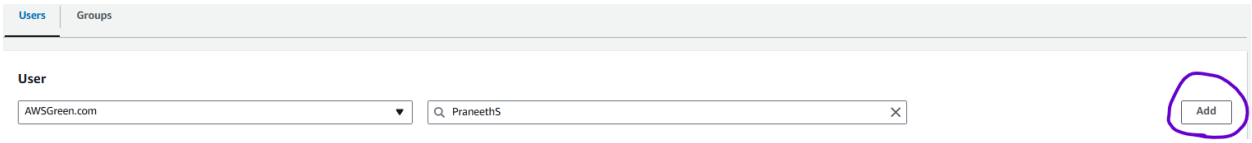
6 - Adding AD Users to AWS Identity Center

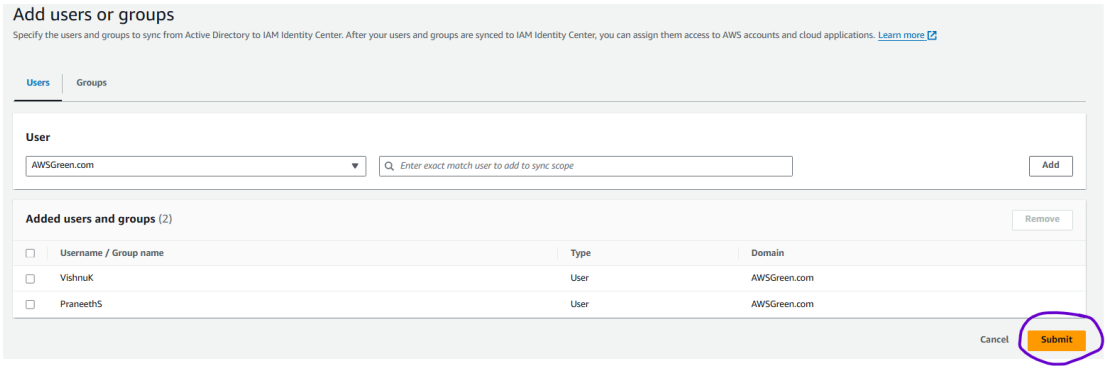
- In the AWS Identity Center dashboard, click on "Users."
- Click "Manage Sync" and Click "Add user."
- Select Domain as “AWSGreen.com”
- In the "Add user" dialog, you can search for and select the AD user(s) you want to add.
- Click "Add user" to complete the process and “Submit”

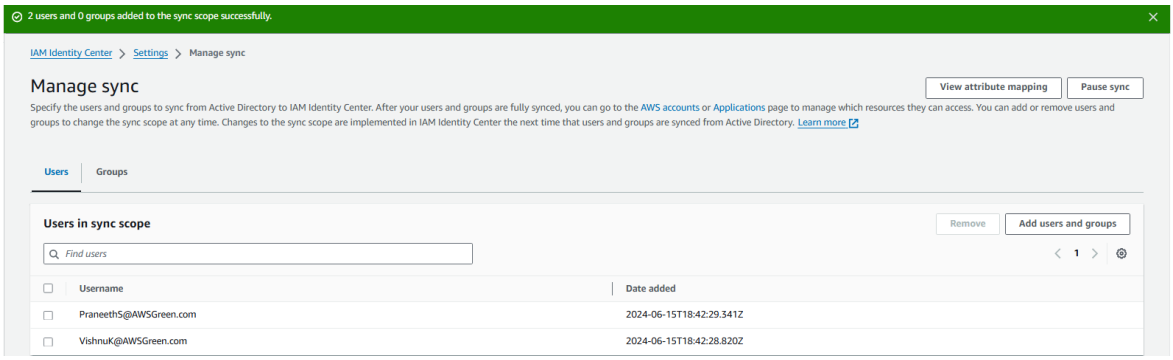
Note: The process might take 5-10 minutes to add the users from AD to AWS Identity Center



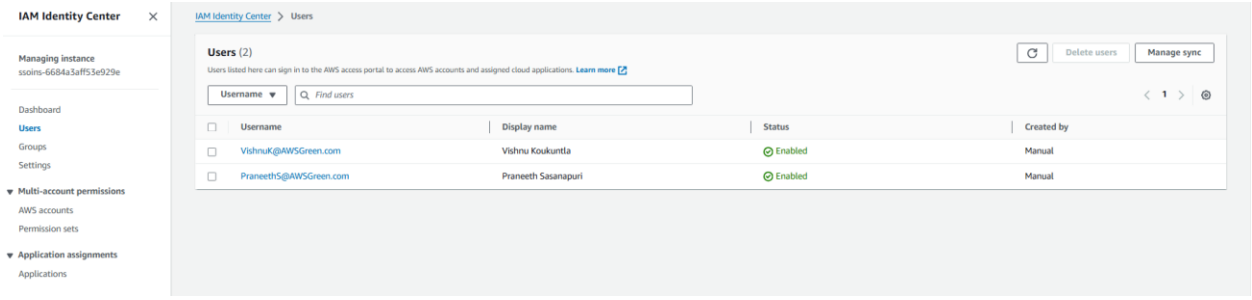








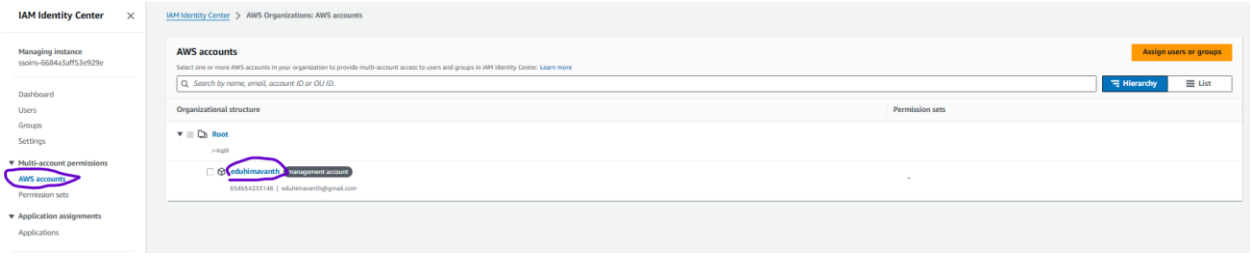
Note: After 5 Minutes you will be able to see the AD users in the AWS Identity Center Users Tab.

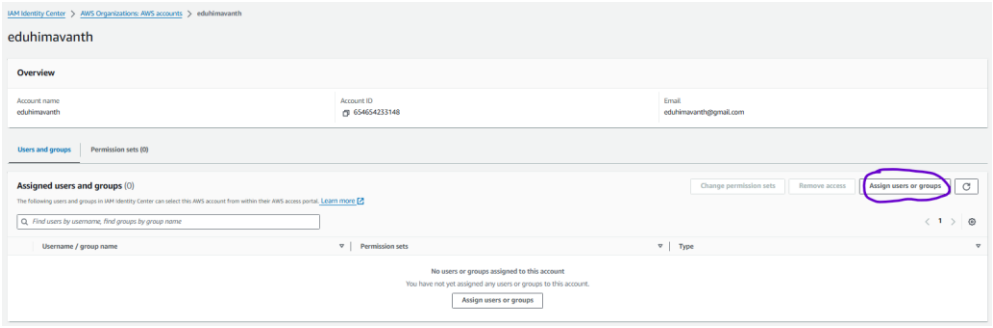


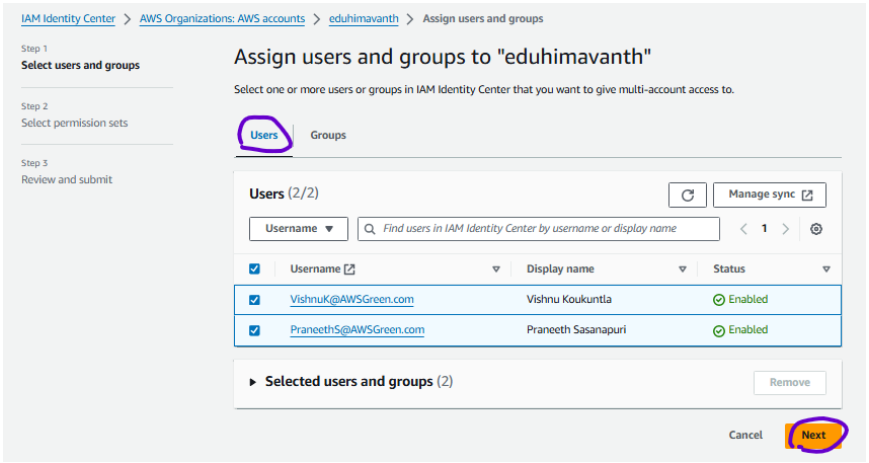
7 - Assign Permission Sets to Users

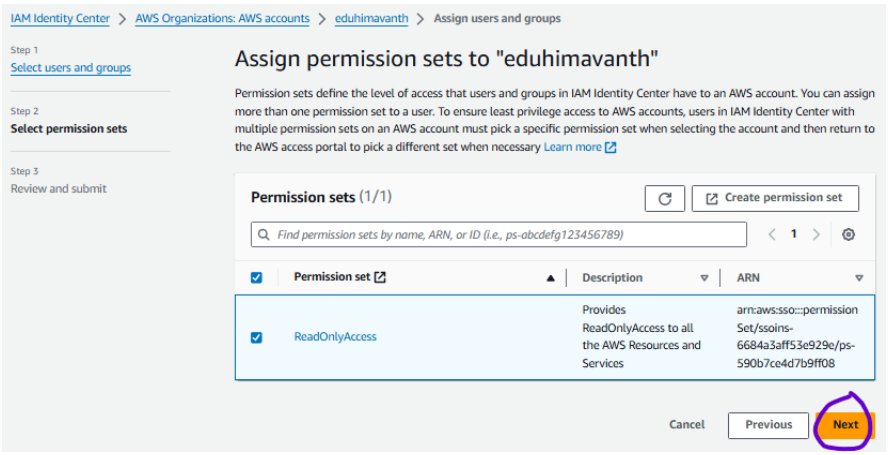
- In the AWS Identity Center dashboard, click on "AWS accounts."
- Select the AWS account where you want to grant access.
- Click "Assign users."
- Search for and select the AD users you added earlier.
- Click "Next."
- Select the permission set you want to assign to the users (e.g., "ReadOnlyAccess").
- Click "Next."
- Review the assignments and click "Submit."

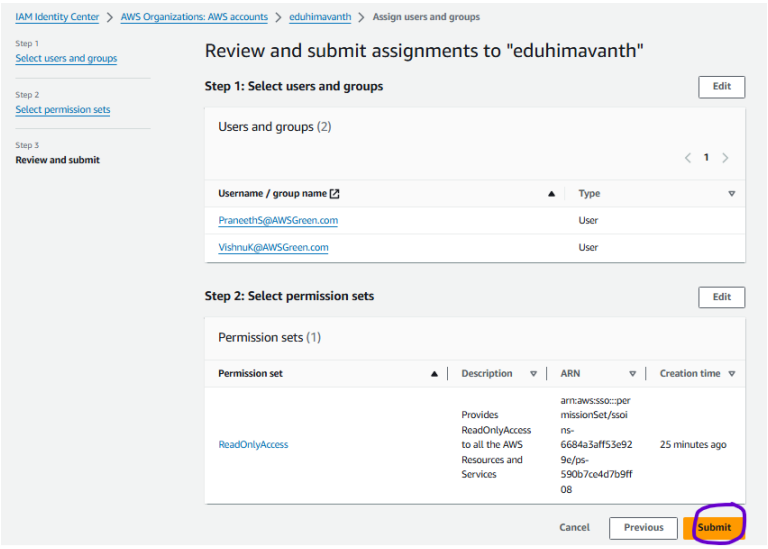
Note: We are choosing the AWS account we are using currently. We haven't gone through the AWS Organizations concept yet. Once we are familiar with AWS Organizations, we can provide access to the AD users for multiple AWS accounts registered in AWS Organizations.

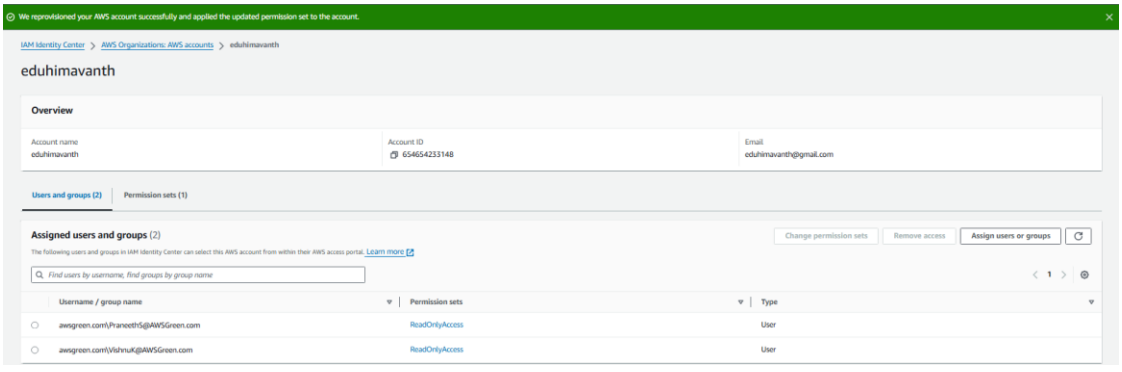






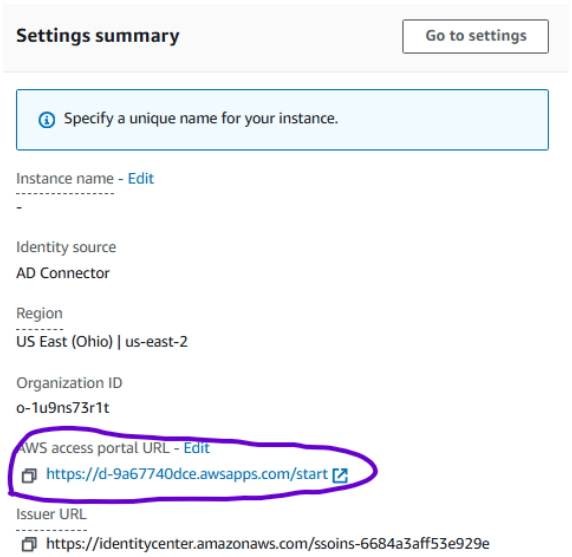


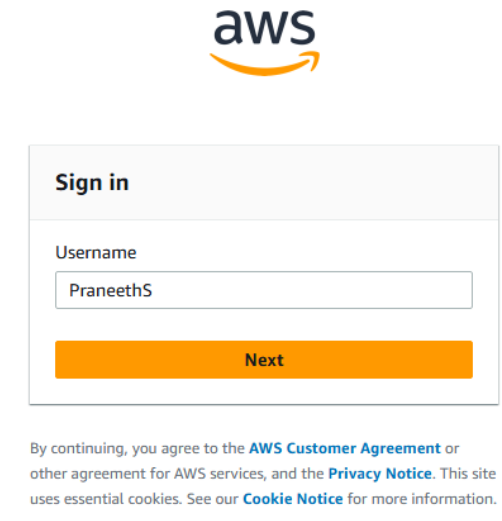


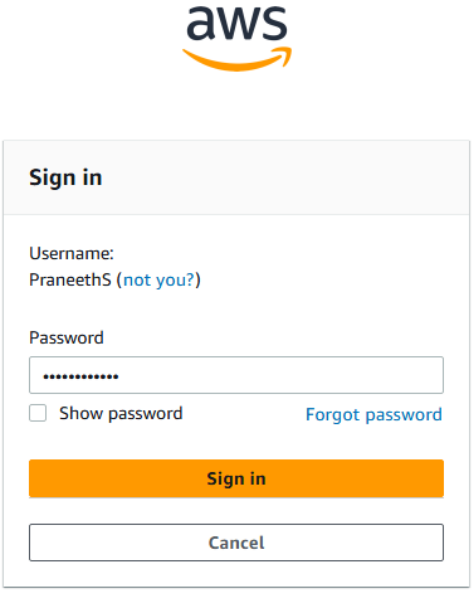


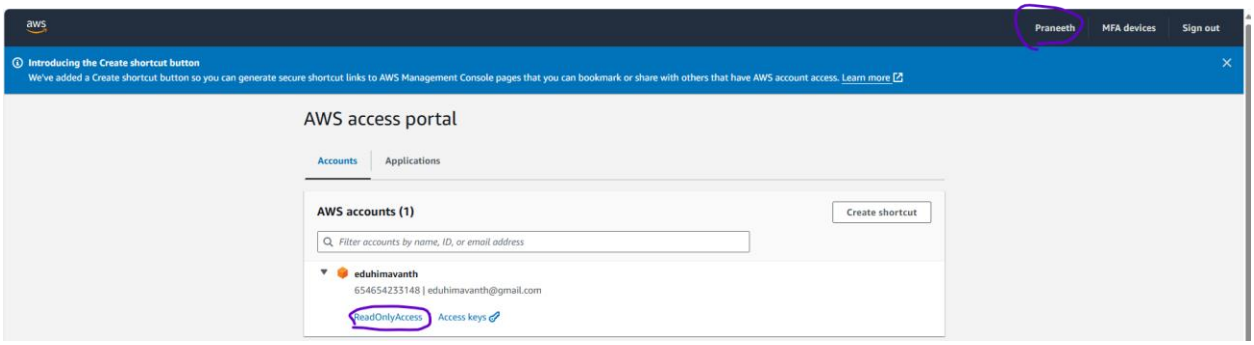
8 - Verification:

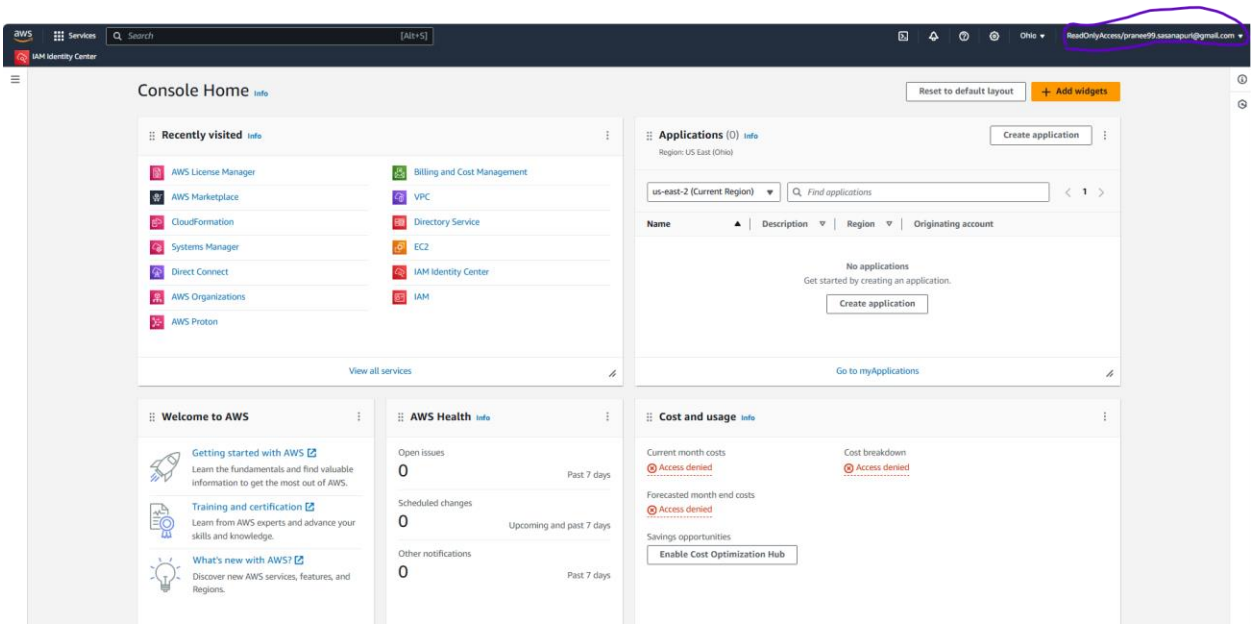
- Open the AWS access portal using the URL
- Log in using the AD credentials of a user assigned the permission set.
- Ensure the user can see and access the assigned AWS accounts and permissions.

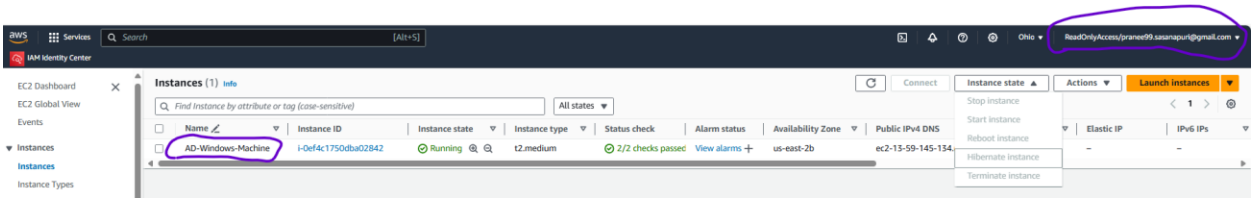

Settings summary
Go to settings
Specify a unique name for your instance.
Instance name - Edit
-
Identity source
AD Connector
Region
US East (Ohio) | us-east-2
Organization ID
o-1u9ns73r1t
AWS access portal URL - Edit
https://d-9a67740dce.awsapps.com/start
Issuer URL
https://identitycenter.amazonaws.com/ssoins-6684a3aff53e929e


aws
Sign in
Username
PraneethS
Next
By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.


aws
Sign in
Username:
PraneethS (not you?)
Password
Show password
Forgot password
Sign in
Cancel


aws
Praneeth
MFA devices
Sign out
Introducing the Create shortcut button
We've added a Create shortcut button so you can generate secure shortcut links to AWS Management Console pages that you can bookmark or share with others that have AWS account access. Learn more
AWS access portal
Accounts
Applications
AWS accounts (1)
Create shortcut
Filter accounts by name, ID, or email address
eduhimavanth
654654233148 | eduhimavanth@gmail.com
ReadOnlyAccess
Access keys





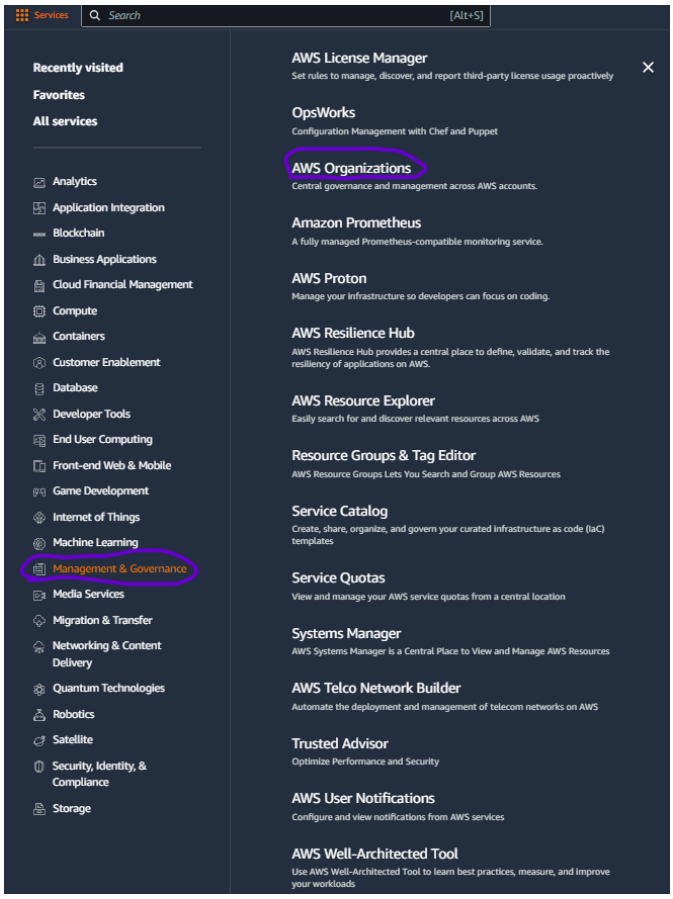
Note: The above snippet confirms that ReadOnlyAccess has been successfully implemented for the AD users to access the AWS account.

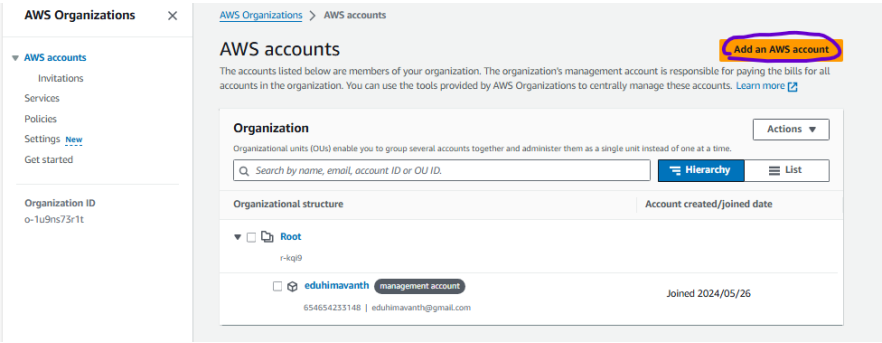
- Additionally, we can add custom or AWS predefined applications to the AD user access.
- We can also enable Multi-Factor Authentication (MFA) for the AD users when logging into the AWS access portal. In this case, the MFA was removed for a quicker approach.

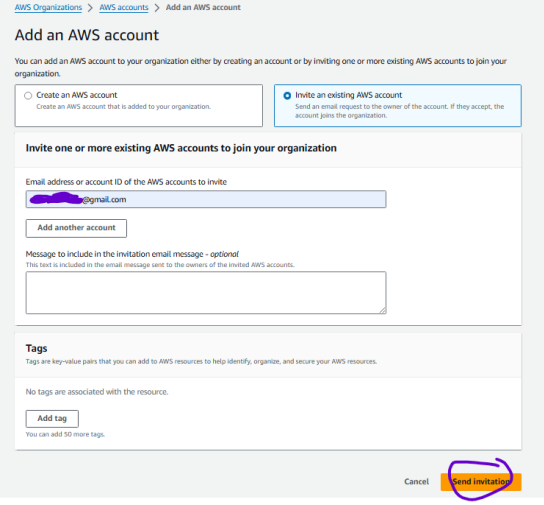
Adding an AWS Account to the Master AWS Account using AWS Organizations:

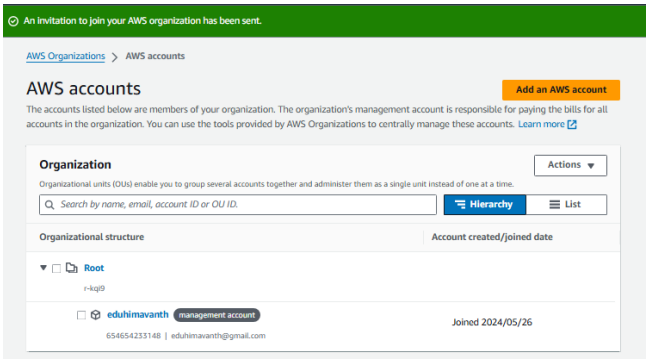
1- Creating an organization

- Under "Management & Governance," select "AWS Organizations."
- Click the "Add account" button adnd Choose How to Add an Account
- You have two options to add an account:
  Create an AWS Account: Create a new AWS account within the organization.
  Invite an AWS Account: Invite an existing AWS account to join the organization.
- Select "Invite an AWS Account" and Click "Invite account."
- Enter the email address or the AWS account ID of the existing account you want to invite.
- Optionally, add tags for better management and tracking.
- Click "Send Invitation" to send an invitation to the account.


Services
Search
[Alt+S]
Recently visited
Favorites
All services
Analytics
Application Integration
Blockchain
Business Applications
Cloud Financial Management
Compute
Containers
Customer Enablement
Database
Developer Tools
End User Computing
Front-end Web & Mobile
Game Development
Internet of Things
Machine Learning
Management & Governance
Media Services
Migration & Transfer
Networking & Content Delivery
Quantum Technologies
Robotics
Satellite
Security, Identity, & Compliance
Storage
AWS License Manager
Set rules to manage, discover, and report third-party license usage proactively
OpsWorks
Configuration Management with Chef and Puppet
AWS Organizations
Central governance and management across AWS accounts.
Amazon Prometheus
A fully managed Prometheus-compatible monitoring service.
AWS Proton
Manage your infrastructure so developers can focus on coding.
AWS Resilience Hub
AWS Resilience Hub provides a central place to define, validate, and track the resiliency of applications on AWS.
AWS Resource Explorer
Easily search for and discover relevant resources across AWS
Resource Groups & Tag Editor
AWS Resource Groups Lets You Search and Group AWS Resources
Service Catalog
Create, share, organize, and govern your curated infrastructure as code (IaC) templates
Service Quotas
View and manage your AWS service quotas from a central location
Systems Manager
AWS Systems Manager is a Central Place to View and Manage AWS Resources
AWS Telco Network Builder
Automate the deployment and management of telecom networks on AWS
Trusted Advisor
Optimize Performance and Security
AWS User Notifications
Configure and view notifications from AWS services
AWS Well-Architected Tool
Use AWS Well-Architected Tool to learn best practices, measure, and improve your workloads


AWS Organizations
AWS accounts
Invitations
Services
Policies
Settings New
Get started
Organization ID
o-1u9ns73r1t
AWS Organizations > AWS accounts
AWS accounts
Add an AWS account
The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. Learn more
Organization
Actions
Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.
Search by name, email, account ID or OU ID.
Hierarchy
List
Organizational structure
Account created/joined date
Root
r-kqi9
eduhimavanth
management account
654654233148 | eduhimavanth@gmail.com
Joined 2024/05/26

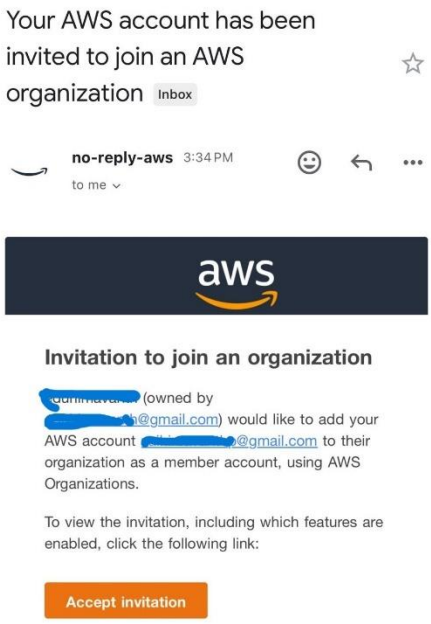


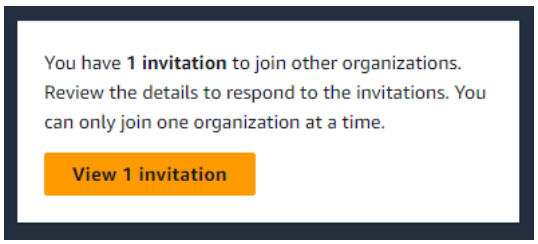


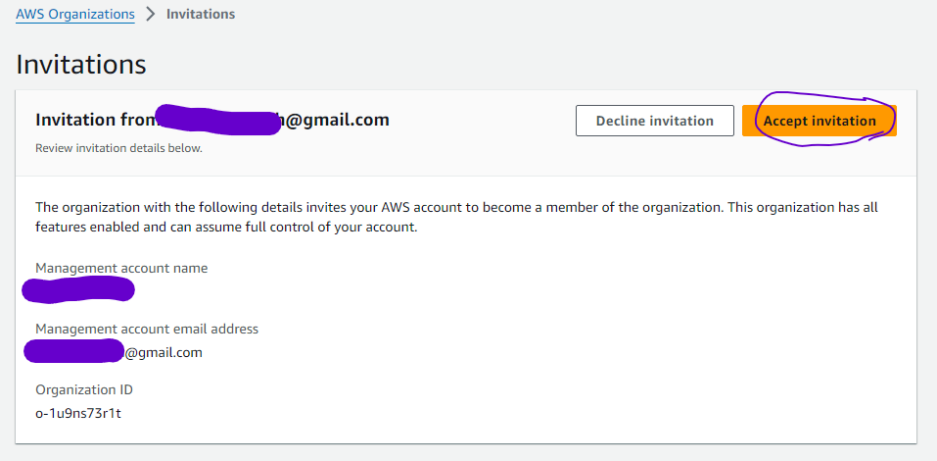
Note: I have chosen the "Invite an AWS Account" option as I have another AWS account created and ready to integrate.

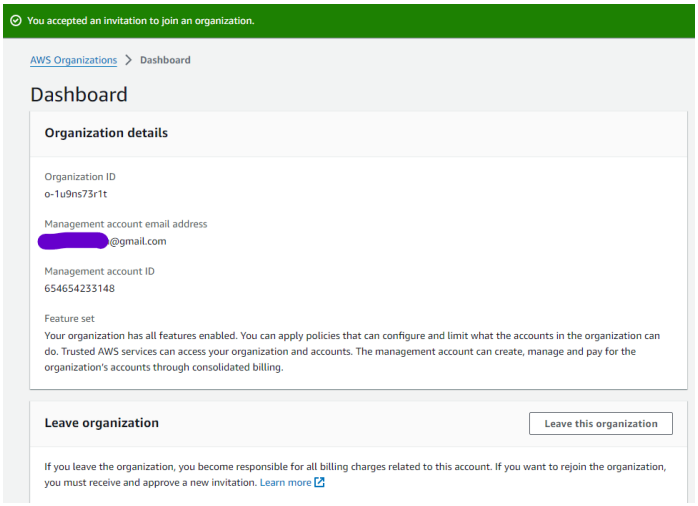
2 - Accept the Invitation (For Existing Accounts)

- The owner of the existing AWS account will receive an email invitation to join the organization.
- The account owner must log in to the AWS Management Console with the existing AWS account credentials.
- In the AWS Organizations dashboard, click on "Invitations" and accept the invitation to join the organization.



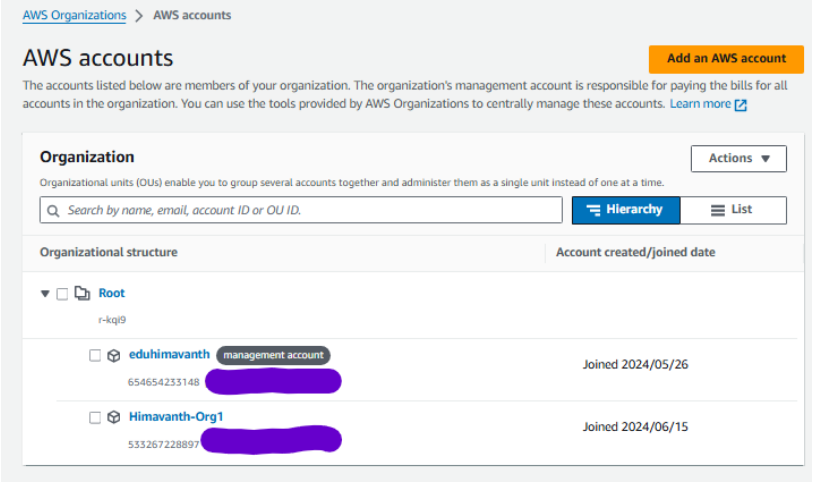






3 - Verify the Account Addition

- In the Master AWS account, go to the AWS Organizations dashboard.
- Click on "Accounts" in the left-hand menu
- Verify that the newly created or invited account appears in the list of accounts in the organization.

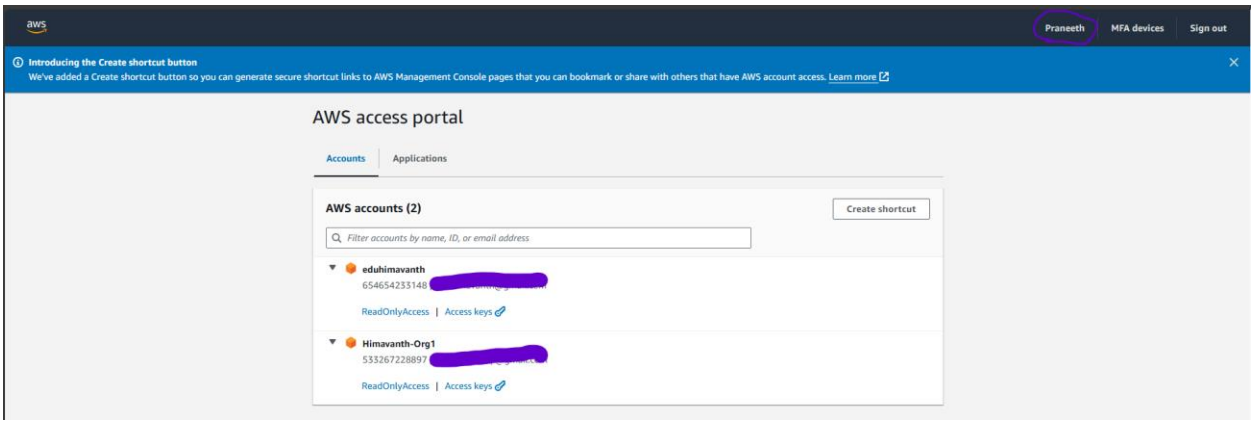


Billing: By default, all accounts in an AWS Organization share consolidated billing. This means the Master account receives a single bill for all member accounts.

Permissions: Ensure proper management of Service Control Policies (SCPs) to enforce access restrictions across accounts.

Account Structure: Organize accounts into Organizational Units (OUs) for better management and policy application.

Now, we can provide access to the newly added AWS account for the AD users added to the AWS Identity Center.

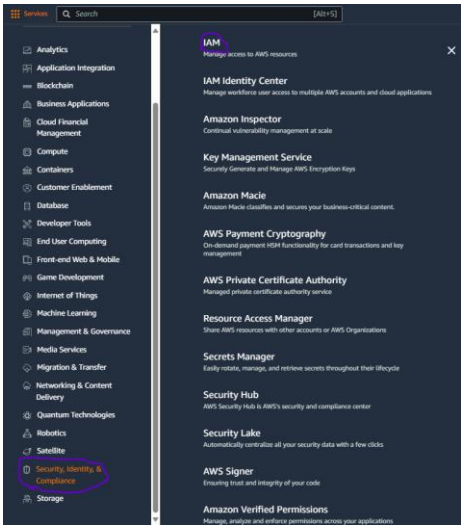


This is how it will appear after providing access to the AD users for the newly added AWS Account.

Creating Users and Groups in AWS IAM

1 - Navigating to IAM

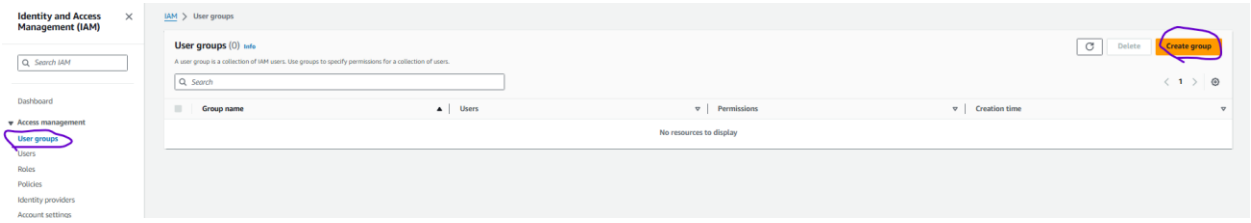
- In the top navigation bar, click on "Services."
- Under "Security, Identity, & Compliance," select "IAM."

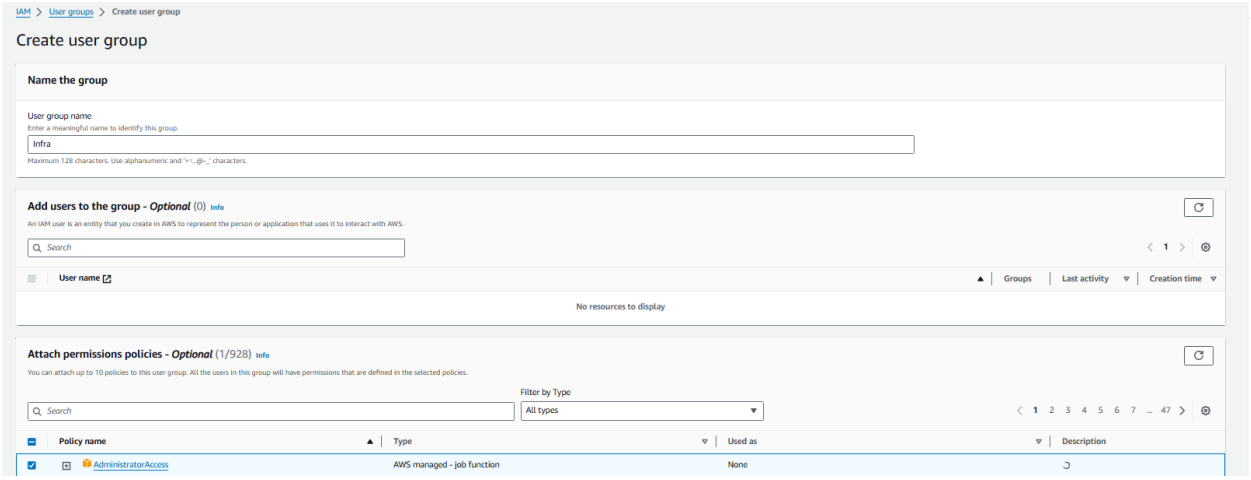


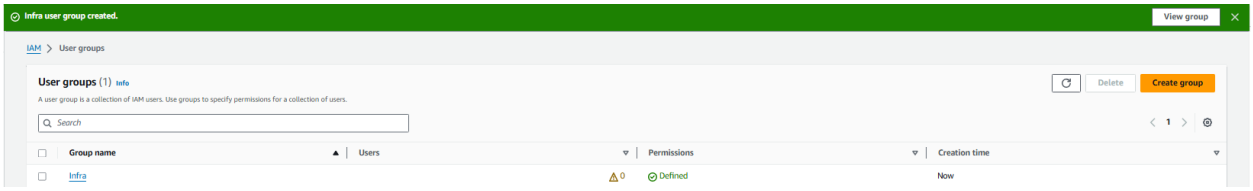
2 - Create Groups

Create Infra Group:

- Click on "User Groups" in the left-hand menu.
- Click on "Create group."
- Enter "Infra" as the group name and click "Next Step."
- Attach policies: Select policies that provide full access to AWS services (e.g., "AdministratorAccess").
- Click "Create group."

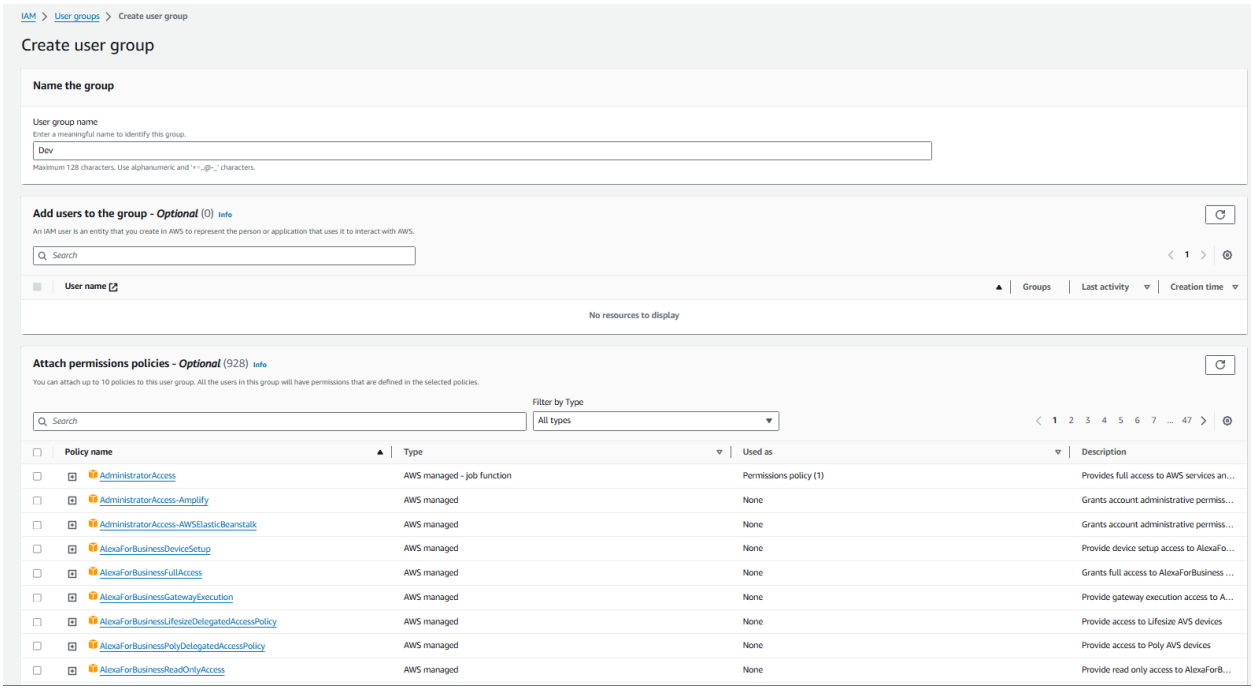


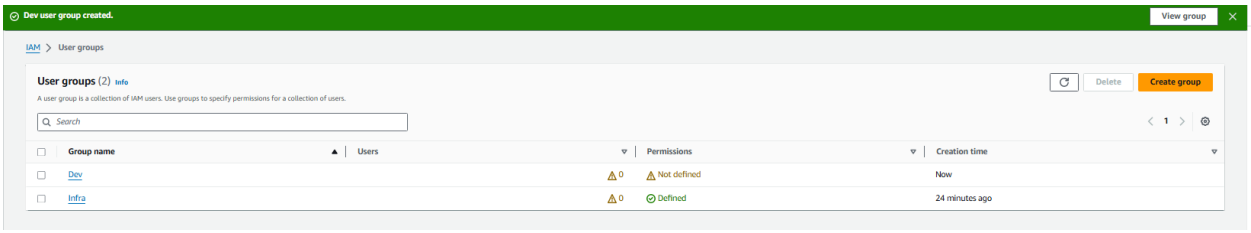




Create Dev Group:

- Click on "Create group."
- Enter "Dev" as the group name and click "Next Step."
- Click "Create group."





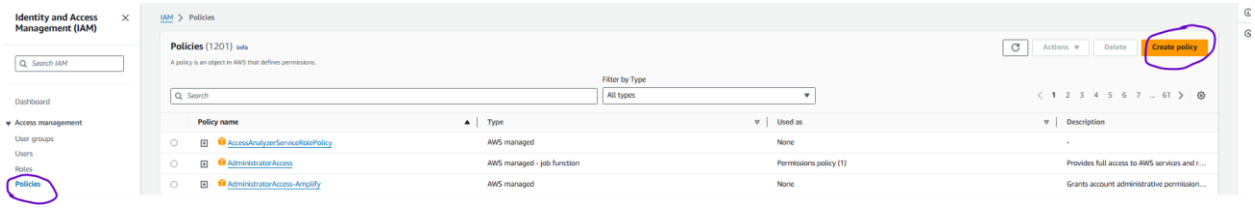
Note: No policies are attached to the "Dev" group as our requirement is to provide full access to S3 with restricted delete access.

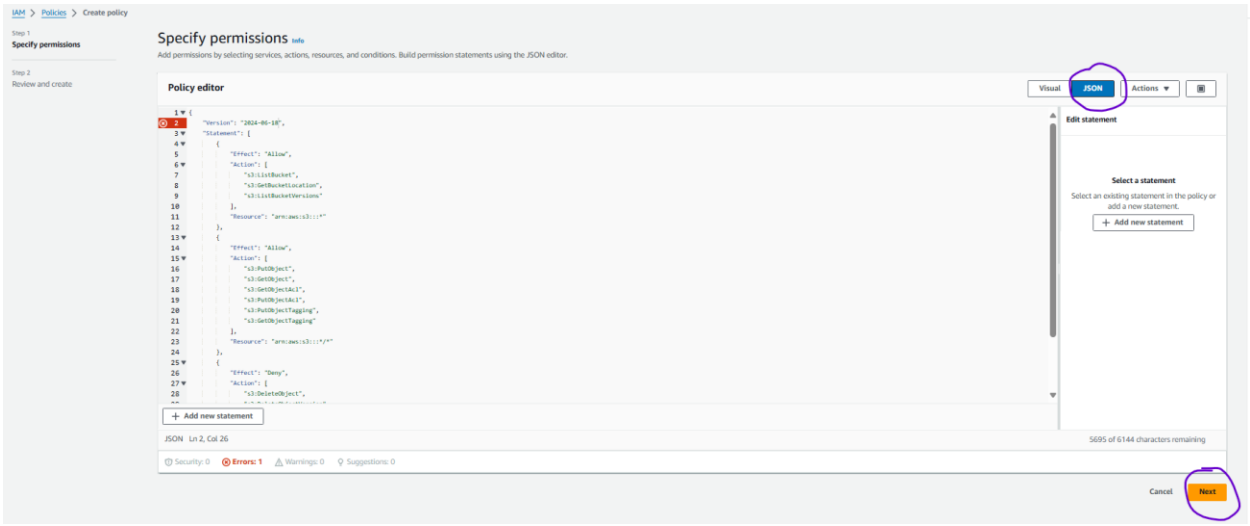
3 - Create a New Policy

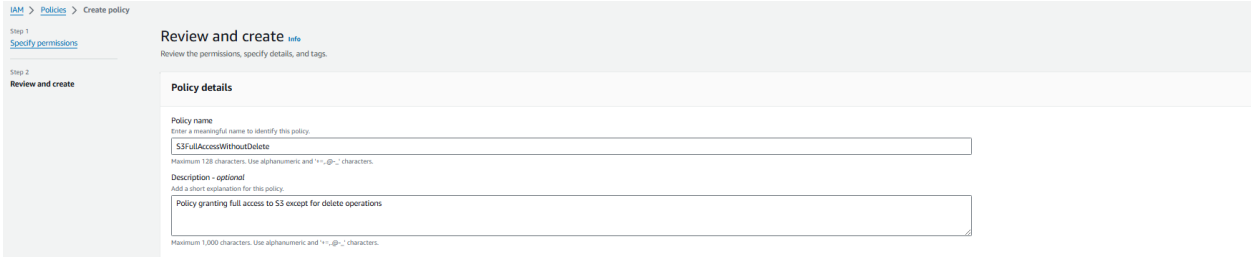
- In the IAM dashboard, click on "Policies" in the left-hand menu.
- Click on the "Create policy" button.
- Click on the "JSON" tab to enter the policy JSON directly.
- Enter the following JSON policy document:

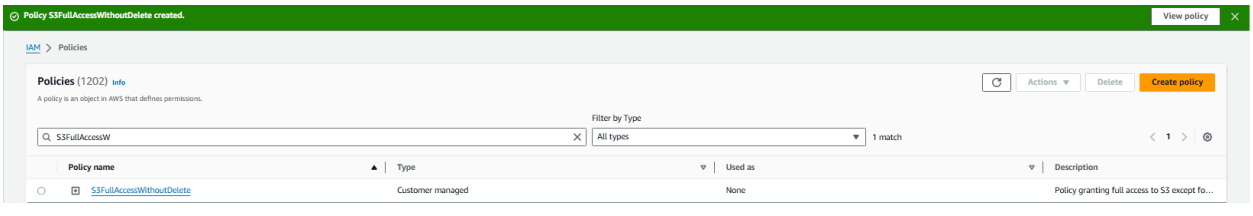
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:ListBucketVersions"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:PutObjectAcl",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging"
            ],
            "Resource": "arn:aws:s3:::*/*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:DeleteBucket"
            ],
            "Resource": "arn:aws:s3:::*/*"
        }
    ]
}
```

- Enter a name for the policy, e.g., S3FullAccessWithoutDelete.
- Enter an optional description, e.g., "Policy granting full access to S3 except for delete operations."
- Click on the "Create policy" button.





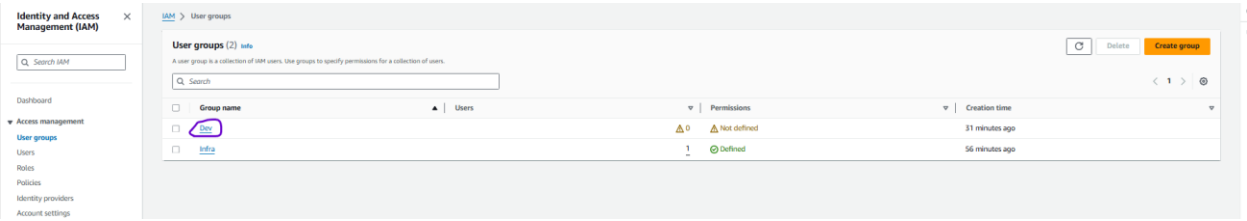


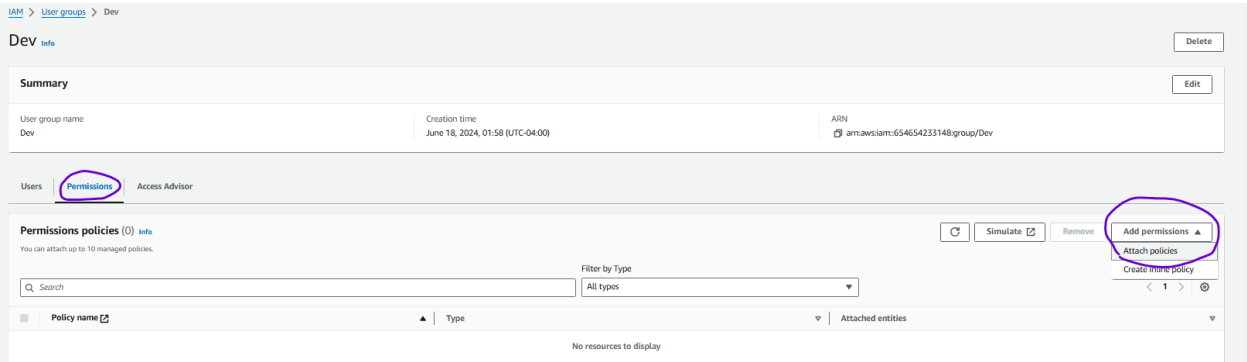


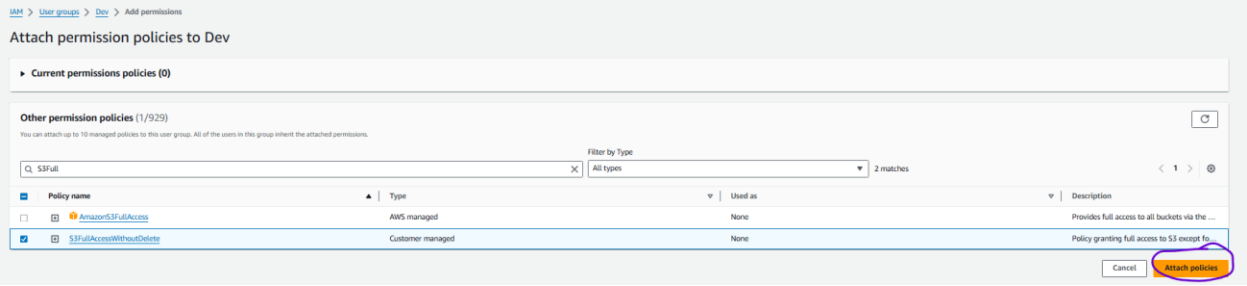
Note: The above IAM policy is created using JSON language. JSON is a lightweight data-interchange format that is easy for humans to read and write and easy for machines to parse and generate.

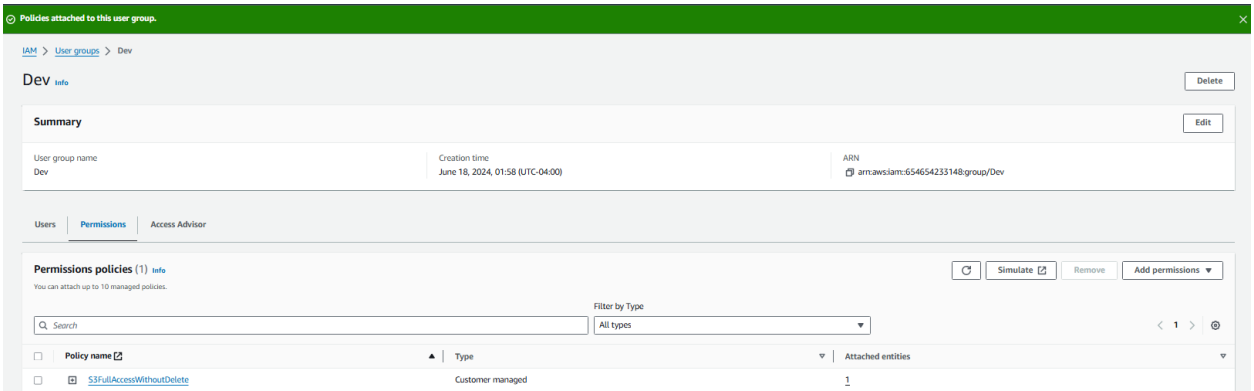
4 – Attaching the “S3FullAccessWithoutDelete” policy to “Dev” group

- Navigate to “User Groups” in the IAM Console
- Click on “Dev” Group
- Click on “Permissions”, “Add Permissions”, “Attach Policies”
- Select “S3FullAccessWithoutDelete” Policy and click “Attach Policies”





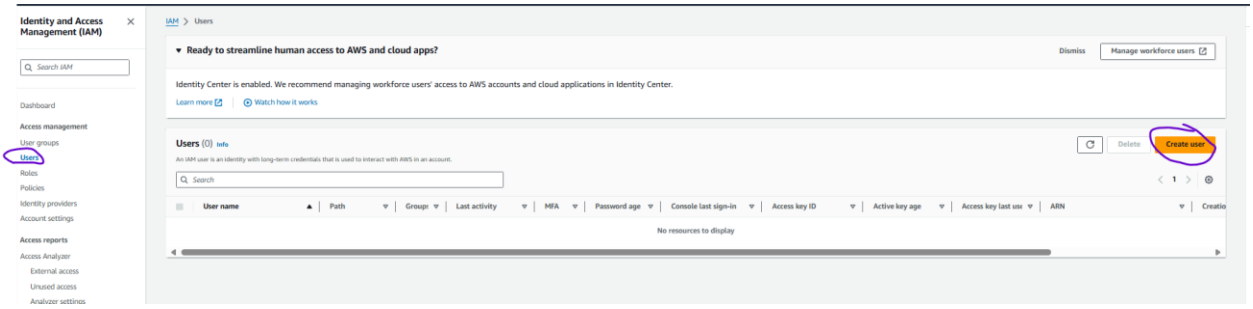


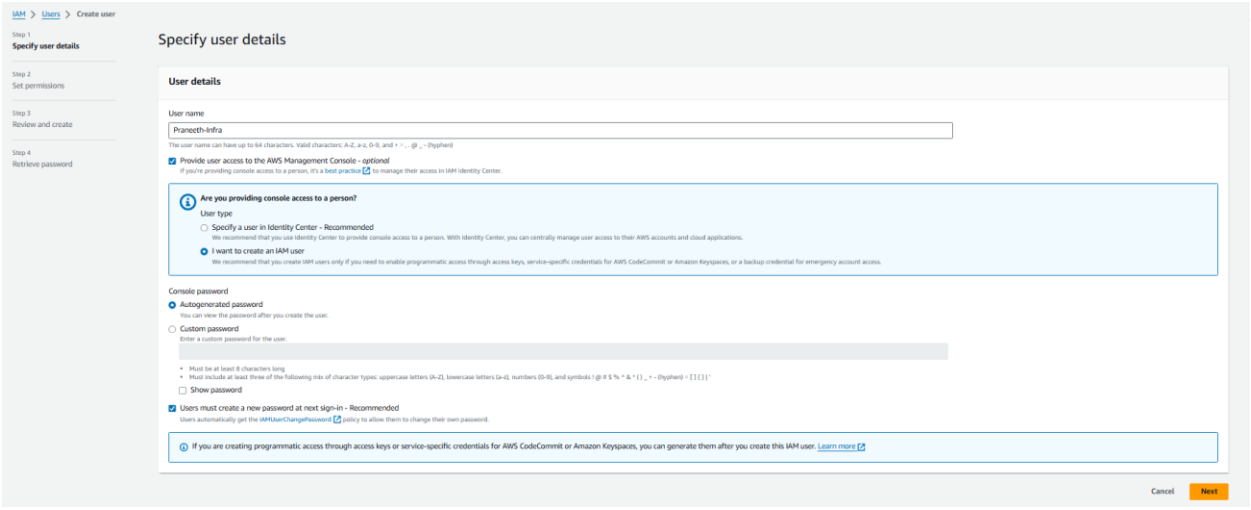


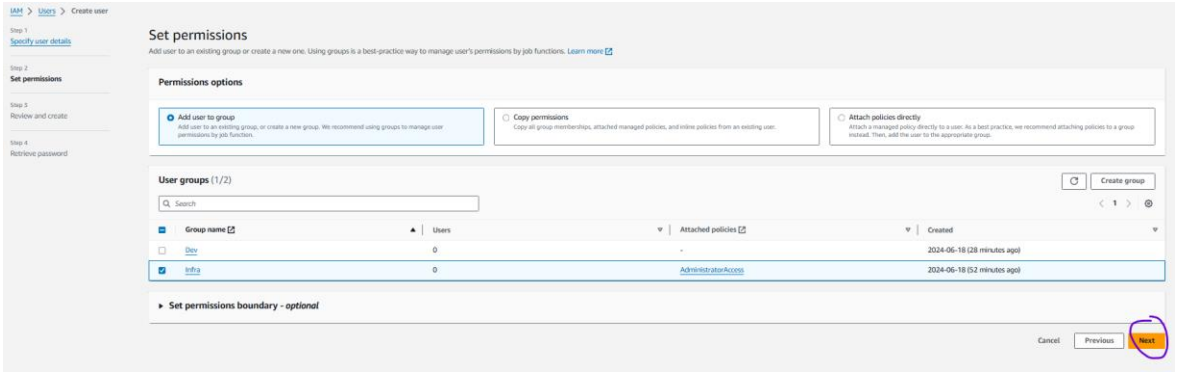
5 - Create Users

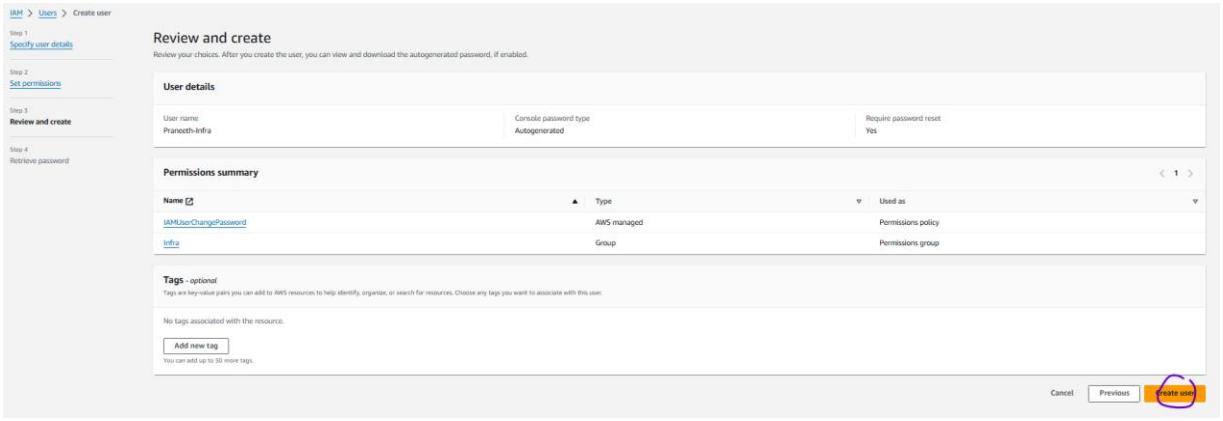
Create User1:

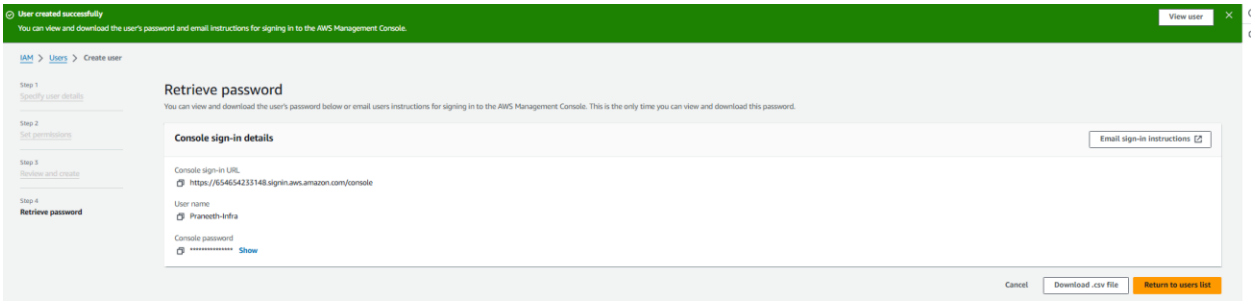
- Click on "Users" in the left-hand menu.
- Click on "Add user."
- Enter the username.
- Select "Programmatic access" and "AWS Management Console access" for access types.
- Set a custom password or let IAM generate one for you.
- Click "Next: Permissions."
- Add User to Groups: Select "Infra" group.
- Click "Next: Tags" (optional) and "Next: Review."
- Review and click "Create user."



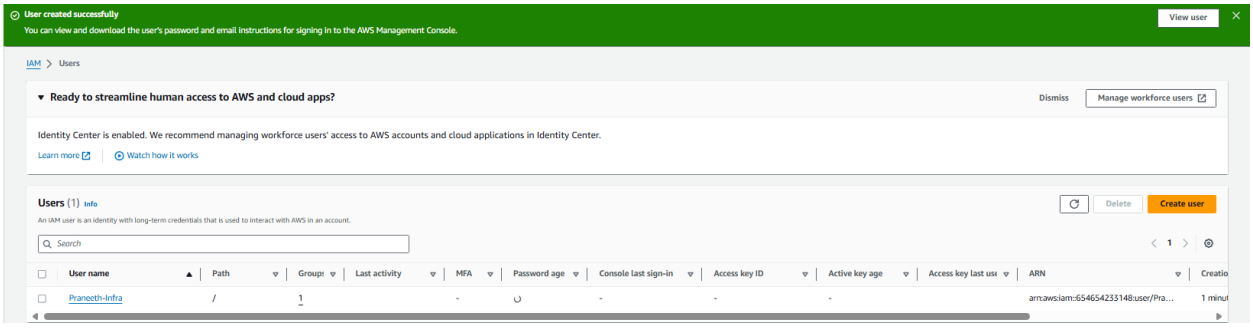








Note down the user credentials securely.



TASK: User Creation &Access Verification

Create User2:

- Click on "Users" in the left-hand menu.
- Click on "Add user."
- Enter username.
- Select "Programmatic access" and "AWS Management Console access" for access types.
- Set a custom password or let IAM generate one for you.
- Click "Next: Permissions."
- Attach policies directly: Attach the policy created for the "Dev" group above.
- Click "Next: Tags" (optional) and "Next: Review."
- Review and click "Create user."
- Note down the user credentials securely.

Access Verification:

- Using the Credential stored, Login into the AWS Console and verify the access.

Note:

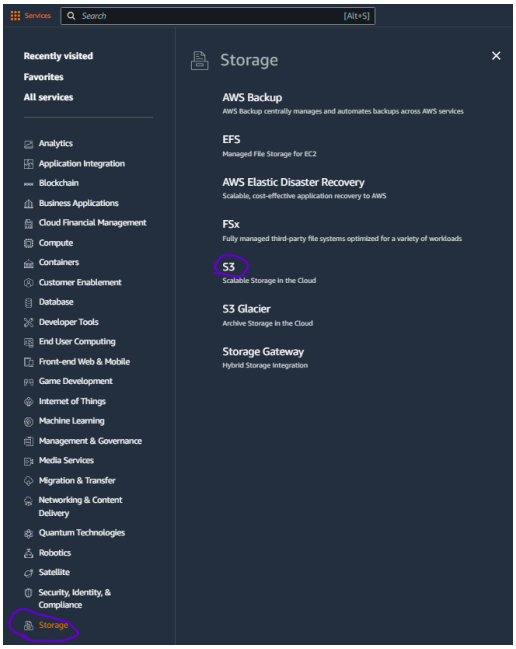
- User1 (Infra) has full access to AWS services through membership in the "Infra" group.
- User2 (Dev) has create/list access to Amazon S3, excluding delete access to S3 objects.
- Ensure to manage user credentials securely and follow the principle of least privilege when assigning permissions in IAM.

Creating AWS S3 Bucket

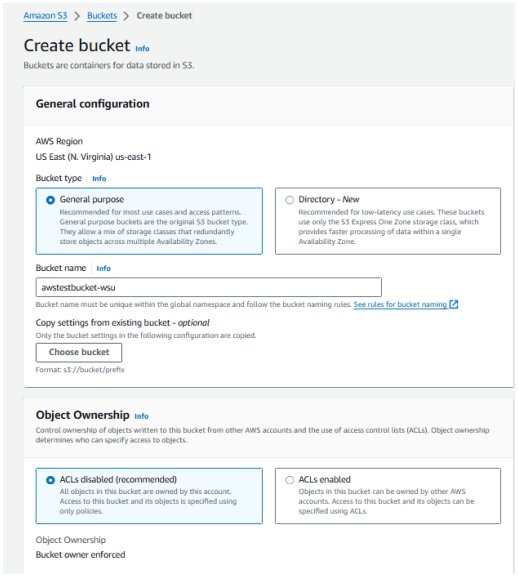
Case 1: Creating an S3 Bucket and Uploading a File

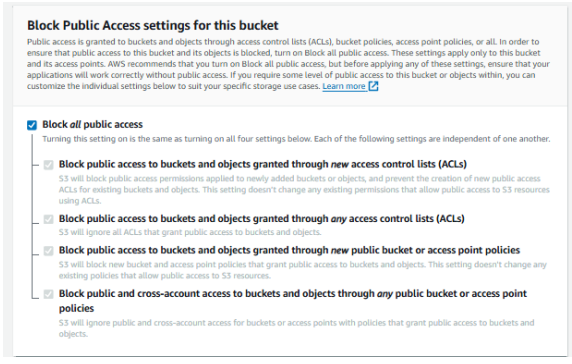
1 - Navigate to S3 and Create a Bucket

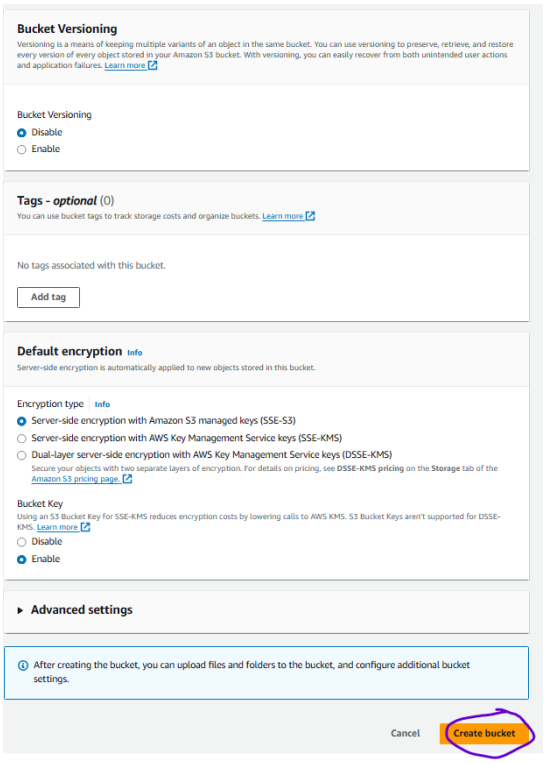
- In the AWS Management Console, Navigate to “Storage” and Click “S3”
- Click on the "Create bucket" button.
- Provide a unique bucket name (the name must be globally unique and follow certain naming rules).
- Select the AWS Region where you want to create the bucket.
- Configure any additional settings as needed, but for simplicity, leave most of them at their default values.
- Click "Create bucket" to finalize the creation.

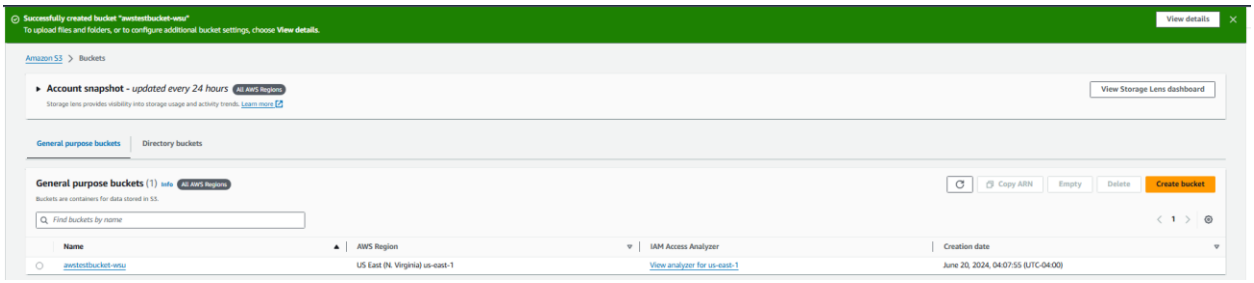

Services
Search
[Alt+S]
Recently visited
Favorites
All services
Analytics
Application Integration
Blockchain
Business Applications
Cloud Financial Management
Compute
Containers
Customer Enablement
Database
Developer Tools
End User Computing
Front-end Web & Mobile
Game Development
Internet of Things
Machine Learning
Management & Governance
Media Services
Migration & Transfer
Networking & Content Delivery
Quantum Technologies
Robotics
Satellite
Security, Identity, & Compliance
Storage
Storage
AWS Backup
AWS Backup centrally manages and automates backups across AWS services
EFS
Managed File Storage for EC2
AWS Elastic Disaster Recovery
Scalable, cost-effective application recovery to AWS
FSx
Fully managed third-party file systems optimized for a variety of workloads
S3
Scalable Storage in the Cloud
S3 Glacier
Archive Storage in the Cloud
Storage Gateway
Hybrid Storage Integration


Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Storage
Amazon S3
Store and retrieve any amount of data from anywhere
Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.
Create a bucket
Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.
Create bucket


Amazon S3 > Buckets > Create bucket
Create bucket Info
Buckets are containers for data stored in S3.
General configuration
AWS Region
US East (N. Virginia) us-east-1
Bucket type Info
General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
Directory - New
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.
Bucket name Info
awstestbucket-wsu
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Format: s3://bucket/prefix
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
Object Ownership
Bucket owner enforced

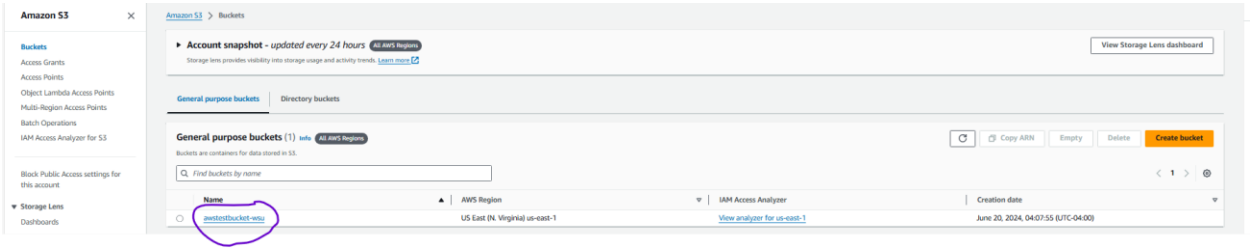

Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

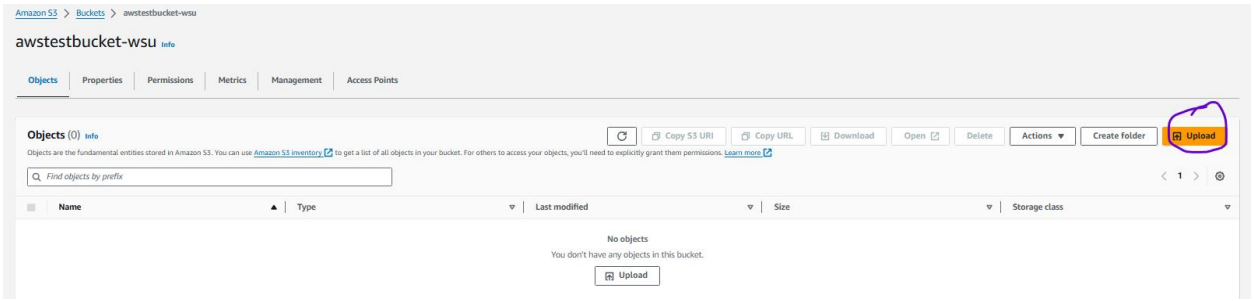


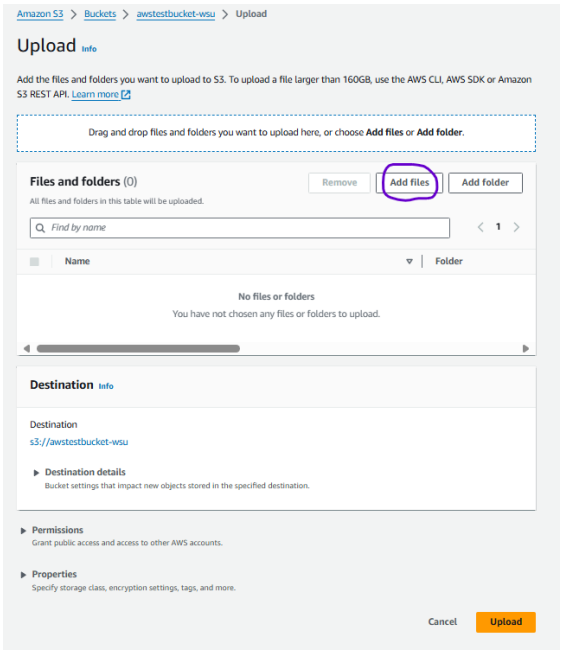


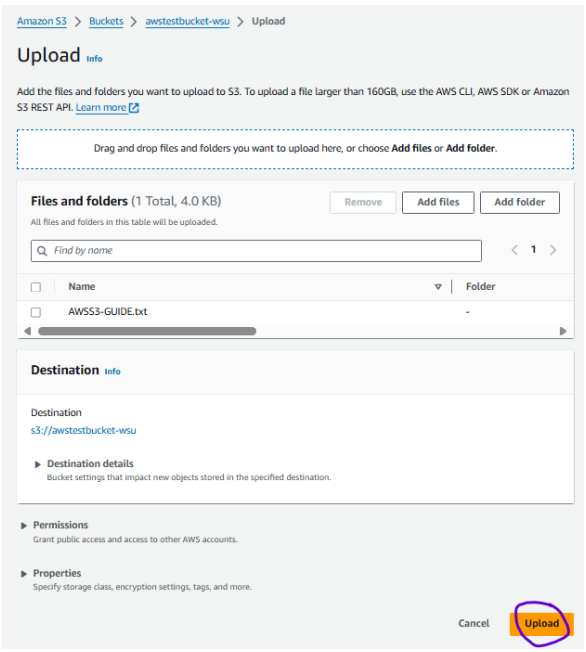
3 - Upload a File

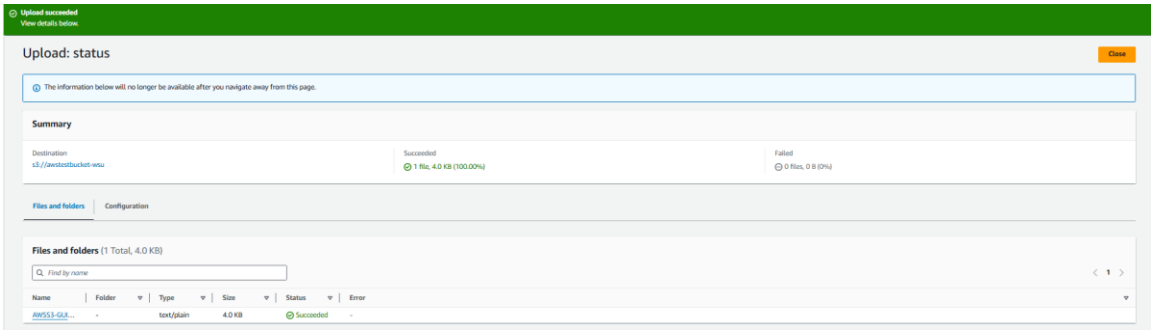
- Click on the name of the bucket you just created to open it.
- Click the "Upload" button.
- Click "Add files" and select the file you want to upload from your local machine.
- Click "Upload" to upload the file to your S3 bucket.

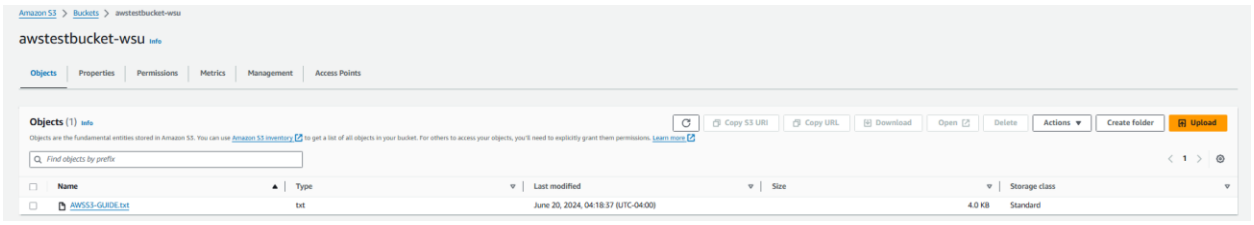












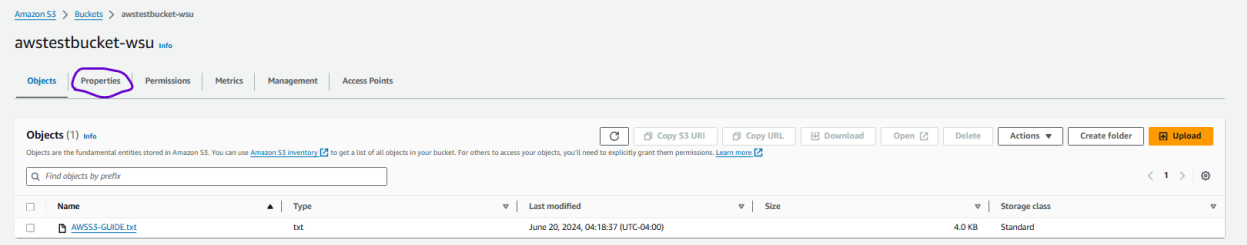
Note: You can also upload a folder to S3 by selecting the “Add Folder” option. This will upload the entire folder and all the files within it to the S3 bucket.

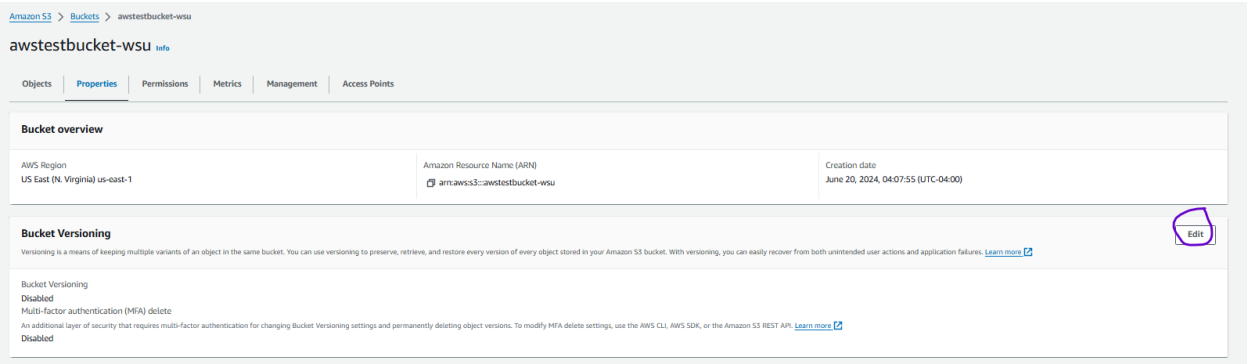
Case 2: Explaining How Versioning Works with Example

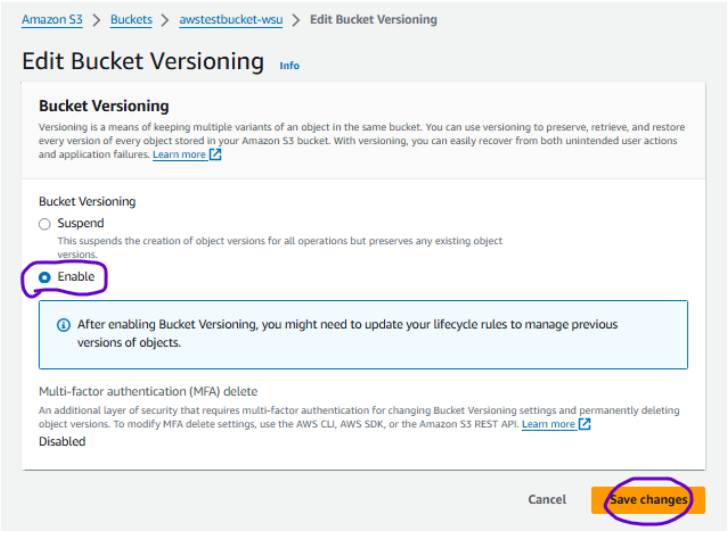
Versioning in S3 allows you to keep multiple versions of an object in a bucket, making it possible to recover from unintended user actions and application failures.

1 - Enabling Versioning

- Go to your S3 bucket in the AWS Management Console.
- Select the bucket where you want to enable versioning.
- Click on the "Properties" tab.
- Scroll down to the "Bucket Versioning" section and click "Edit".
- Select "Enable" and then click "Save changes".







2 - Uploading Multiple Versions of an Object

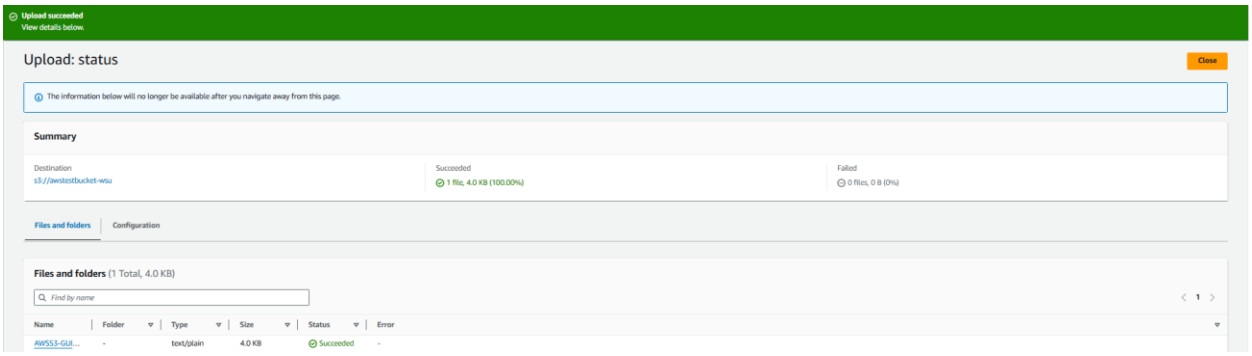
First Upload:

- Click on the name of the bucket you just created to open it.
- Click the "Upload" button.
- Click "Add files" and select a file, say example.txt, from your local machine.
- Click "Upload" to upload the file to your S3 bucket.

Note: I am skipping this step since we have already uploaded a file to the S3 bucket.

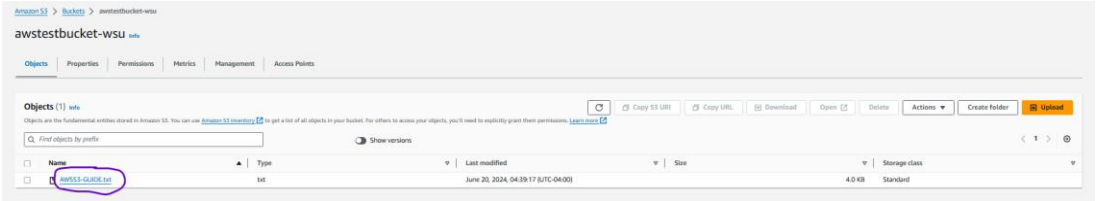
Second Upload (New Version)

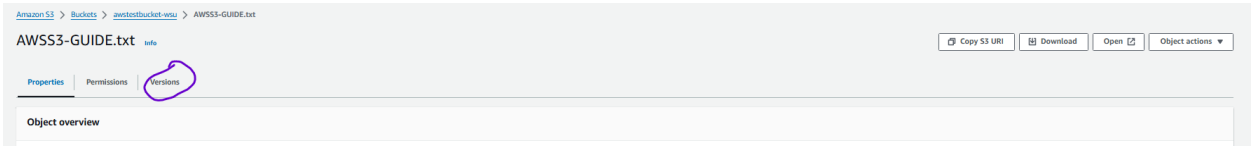
- Make some changes to example.txt on your local machine.
- Repeat the upload process: click "Upload", "Add files", select the modified example.txt, and click"Upload".

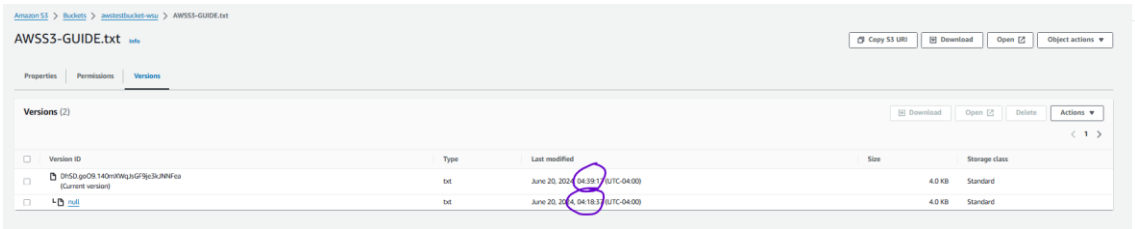


3 - Viewing Object Versions:

- Go to the "Objects" tab of your bucket.
- Click on the "Show versions" button (a checkbox) near the top-right corner.
- You will see multiple versions of example.txt listed with different version IDs.





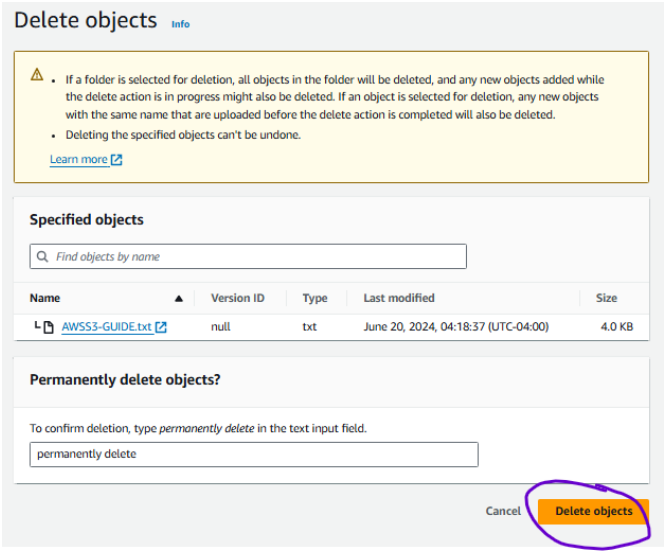


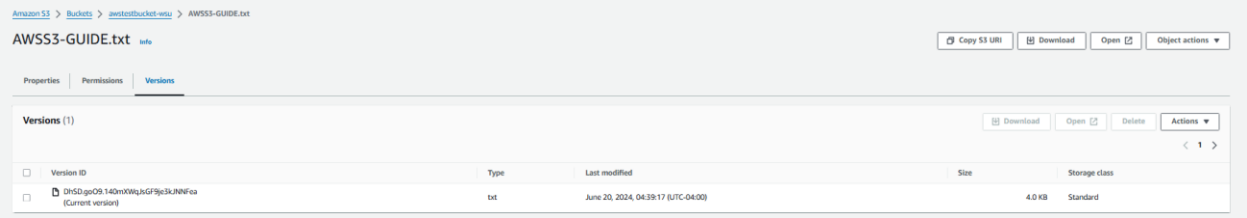
TASK - Restoring a Previous Version

- Suppose you want to restore the first version of example.txt. You can download that specific version and re-upload it if needed.
- Select the version you want to restore by clicking on the version ID.
- Click the "Download" button to download the specific version.

5 - Deleting an Object with Versioning:

- When you delete an object, a delete marker is added, but previous versions are not removed.
- To permanently delete an object, you must delete all versions individually.

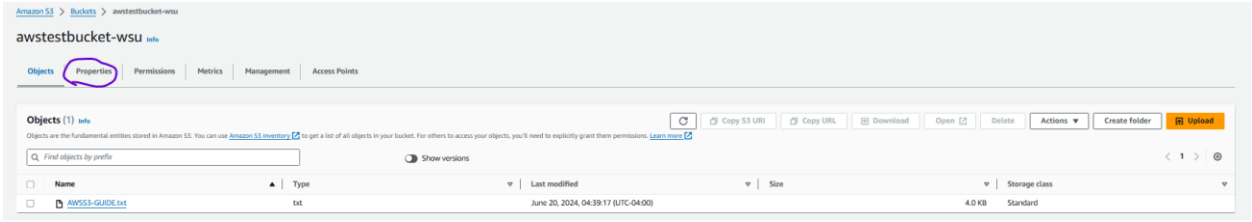


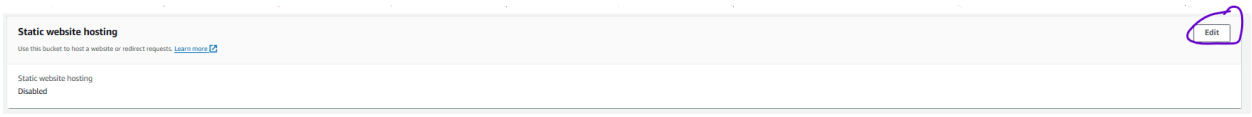


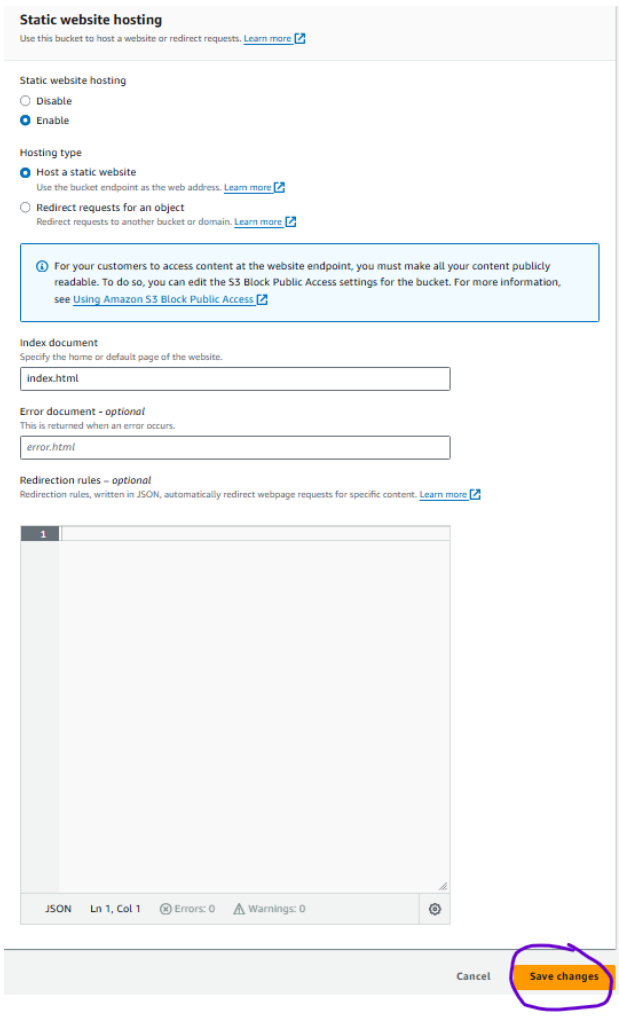
Case - 3: Hosting a Static Website Using S3

1 - Enable Static Website Hosting

- Open the Bucket Properties
- Select your bucket and click on the "Properties" tab.
- Scroll down to the "Static website hosting" section and click "Edit".
- Select "Enable".
- Specify an index document (e.g., index.html). You can also specify an error document if needed.
- Click "Save changes".

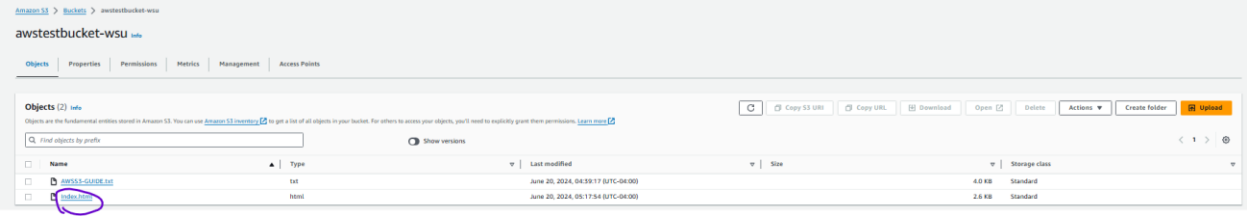






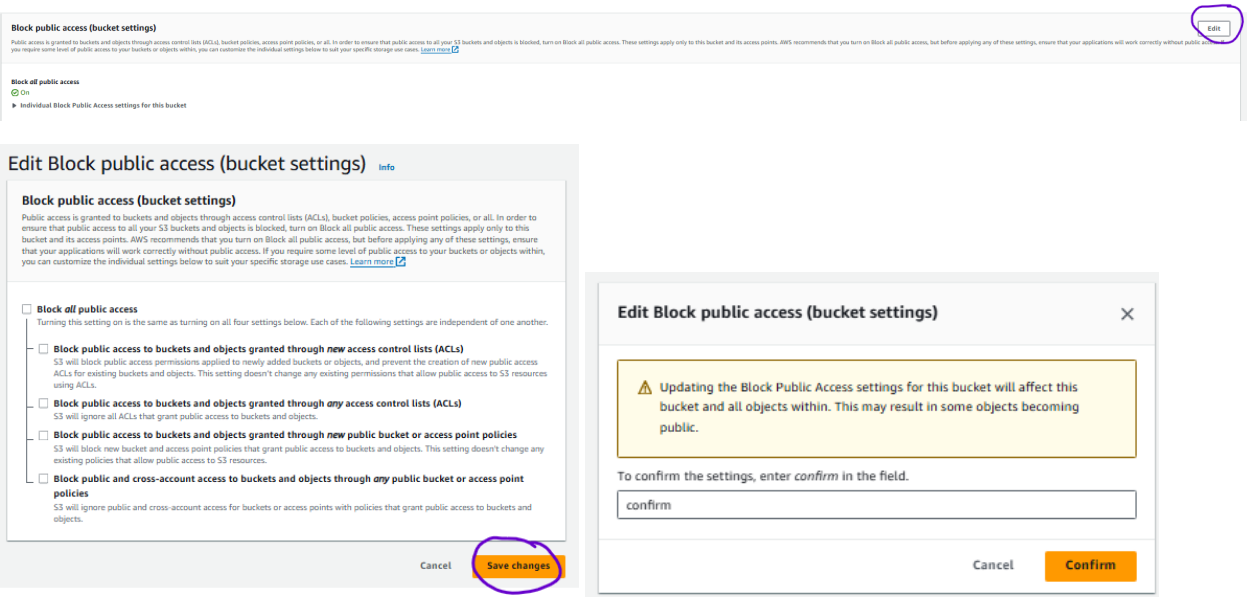
2 - Upload the HTML File

- Go back to the "Objects" tab of your bucket.
- Click "Upload".
- Click "Add files" and select your index.html file.
- Click "Upload" to upload the file to your S3 bucket.



3 - Configure Block Public Access Settings:

Ensure that the "Block all public access" settings do not block the public access settings for your bucket. Adjust them if necessary by clicking "Edit" under "Block public access (bucket settings)" and unchecking the necessary options.

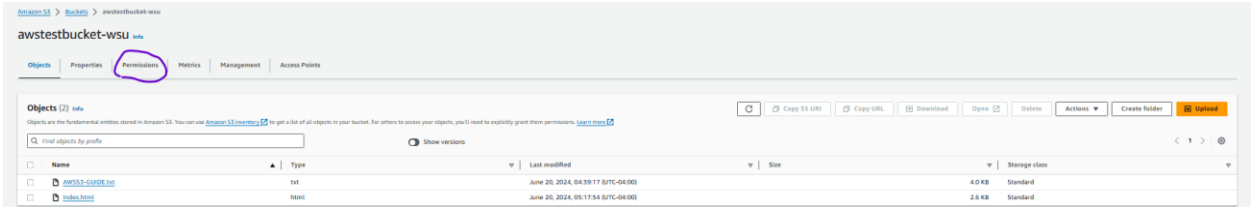


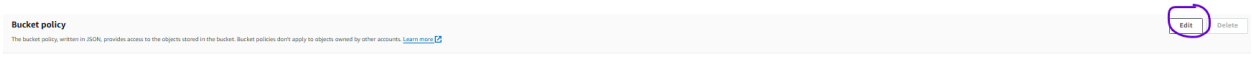
4 - Set Bucket Policy for Public Access

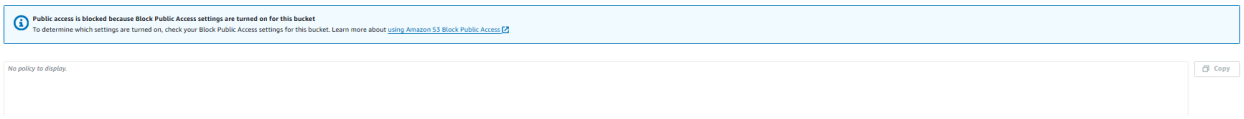
- Go to the "Permissions" tab of your bucket.
- Click on "Bucket policy".
- Enter the below policy to allow public read access to your bucket

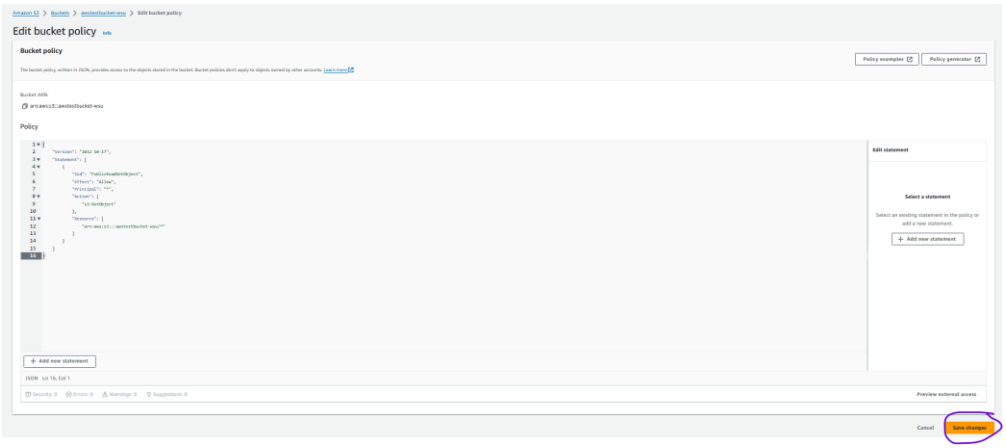
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::awstestbucket-wsu/*"
            ]
        }
    ]
}
```

- Click "Save changes".



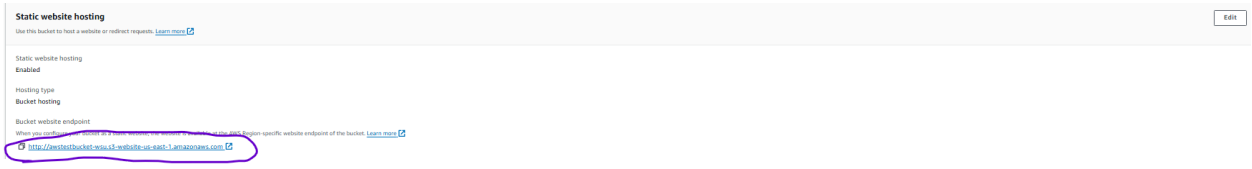


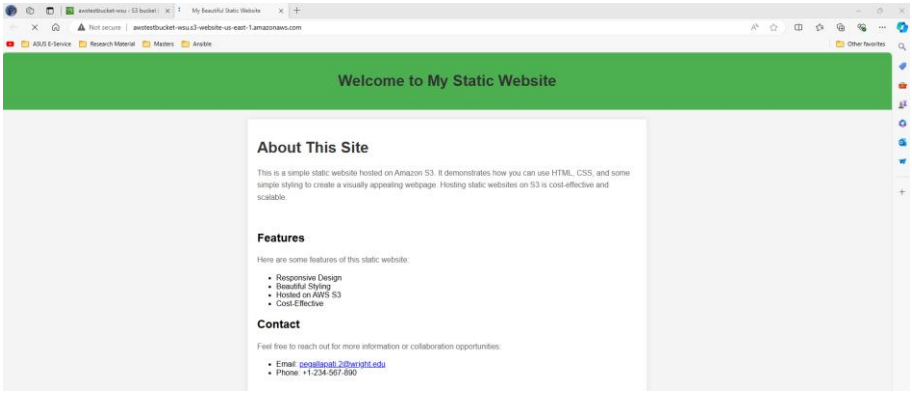




5 - Access the Website

- After enabling static website hosting, you will see a "Bucket website endpoint" URL in the "Static website hosting" section of the bucket properties.
- Open this URL in a web browser to access your static website.





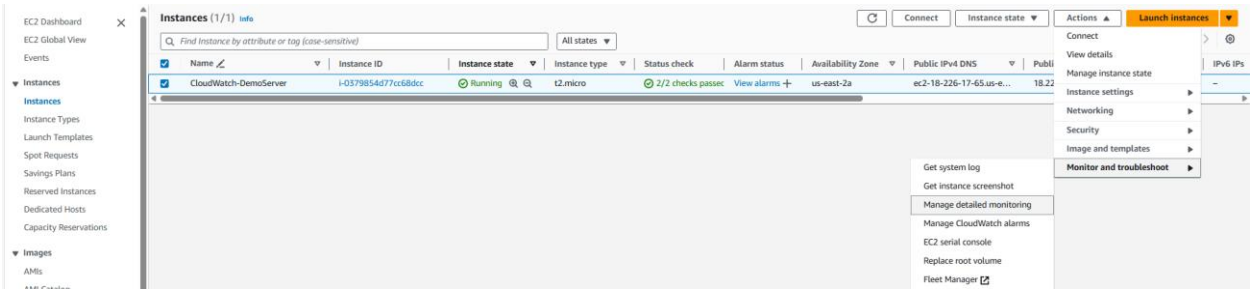
Implemening Cloud Watch Alarms

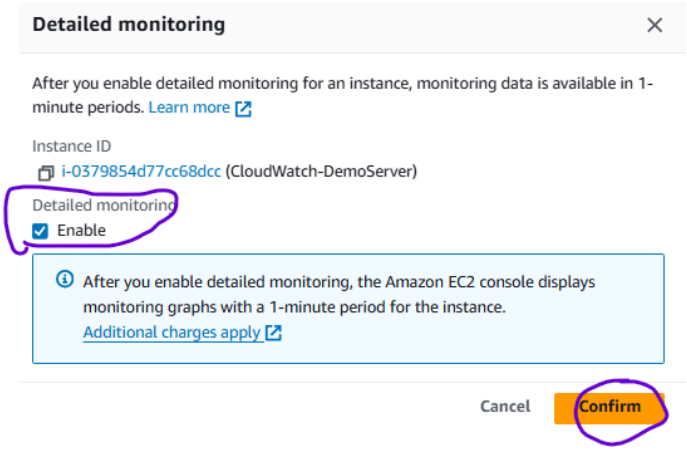
TASK – Deploy an EC2 Instance with Ubuntu AMI

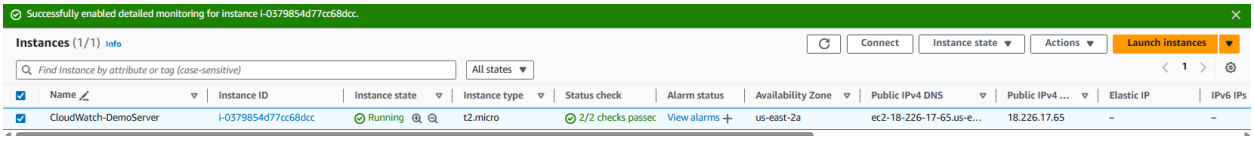
1 - Enabling Detailed Monitoring for an EC2 instance (Ubuntu)

Detailed Monitoring provides more frequent monitoring of your EC2 instance's performance data. Follow these steps to enable it

- In EC2, Select Your Instance
- With your instance selected, click on the "Actions" dropdown menu.
- Select "Monitor and troubleshoot" and then "Manage detailed monitoring".
- In the dialog box that appears, select "Enable".
- Click on the "Update" button.

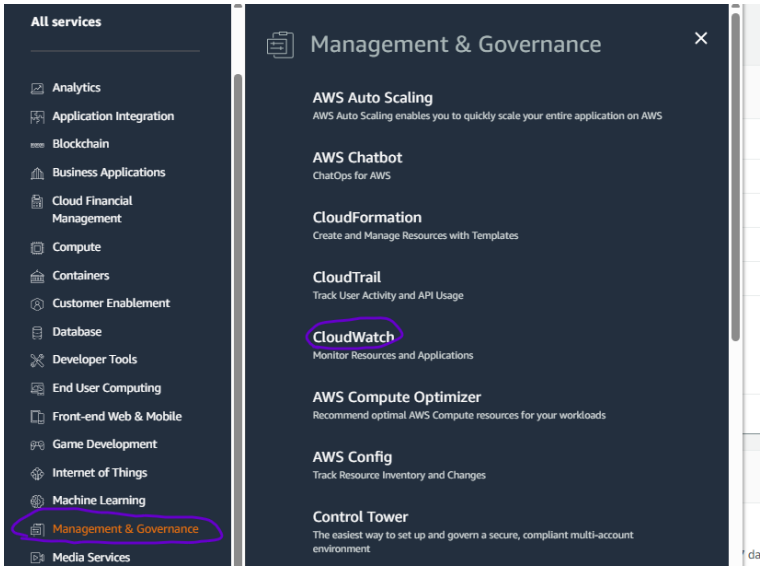




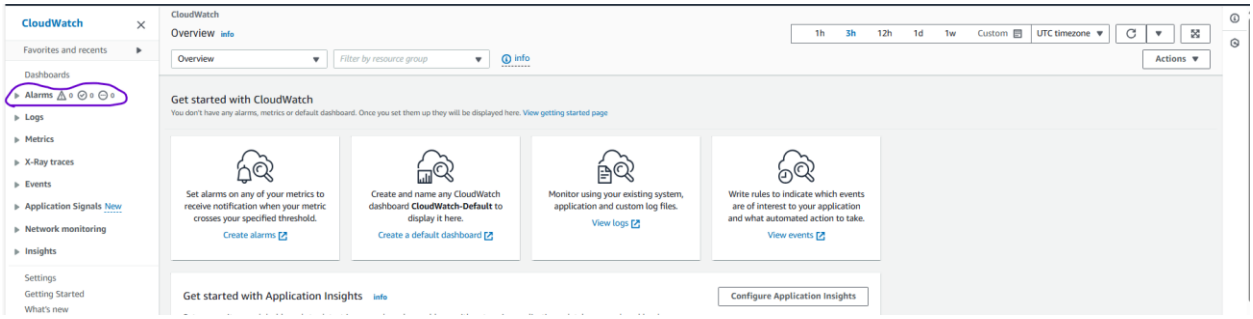


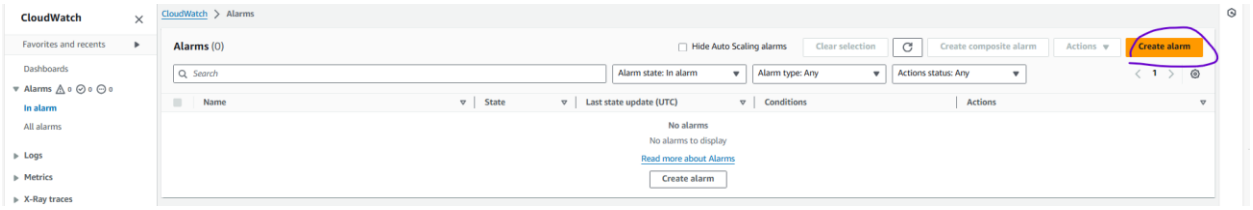
2 - Creating an Alarm in AWS CloudWatch to send an email if the CPU-Utilization of the instance exceeds 60%

- In the AWS Management Console, Navigate to “Management and Governance” and Click “CloudWatch”

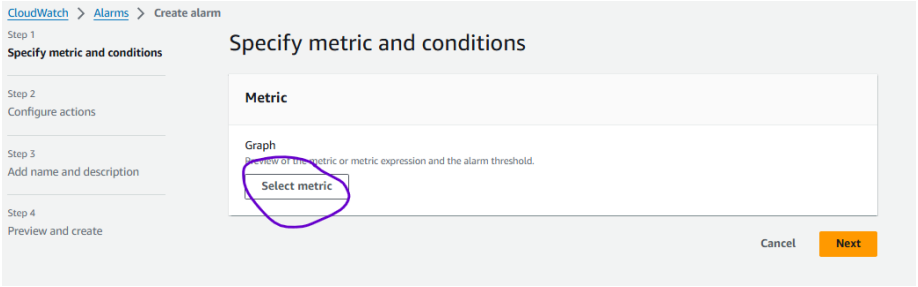


- In the left-hand menu, click on "Alarms" and then "Create Alarm".

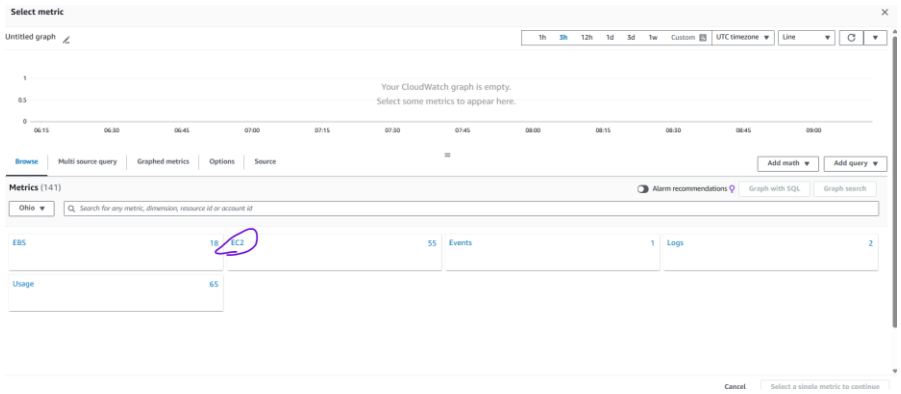


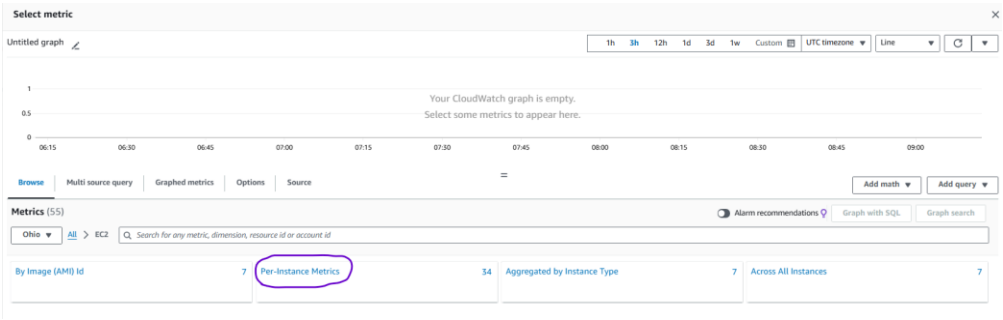


- Click on "Select metric".

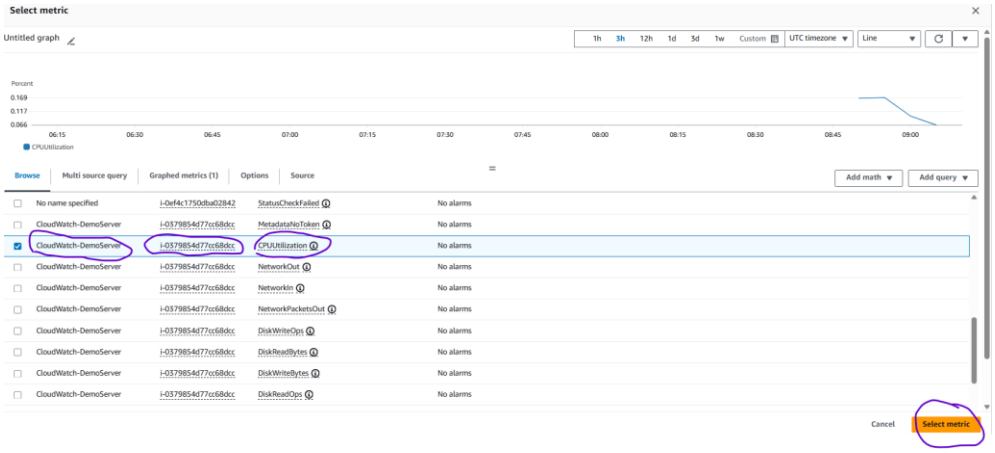


- In the "Browse" tab, choose "EC2" and then "Per-Instance Metrics".

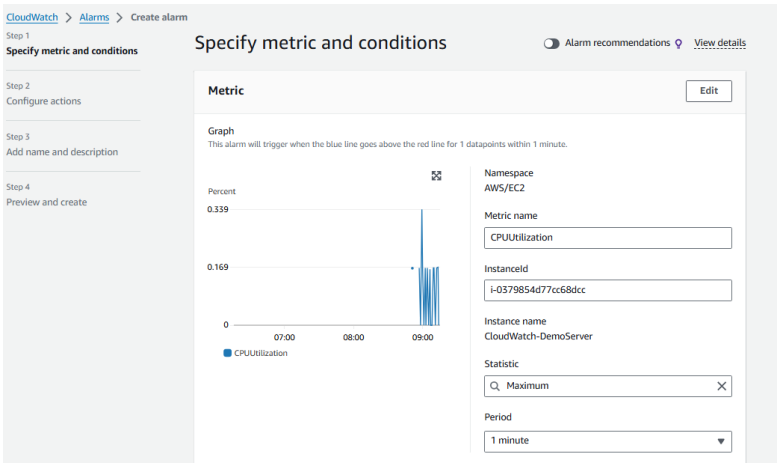




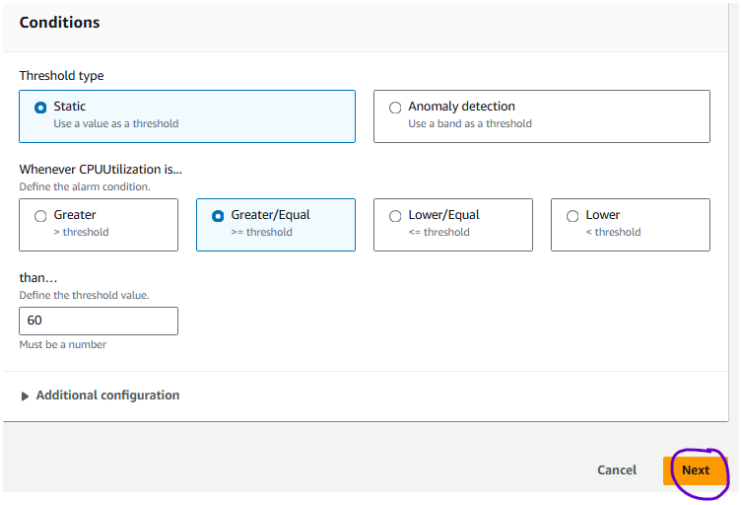
- Select your instance and then choose "CPUUtilization".
- Click "Select metric" after choosing the metric.



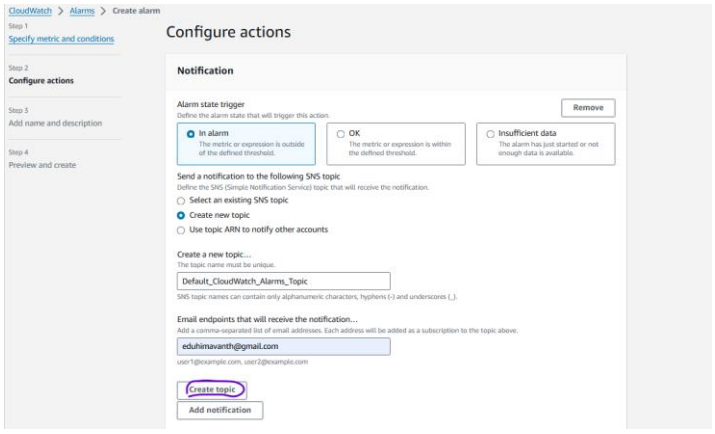
- In the "Specify metric and conditions" section, select the statistic as “Maximum” and period as ”1 minute”

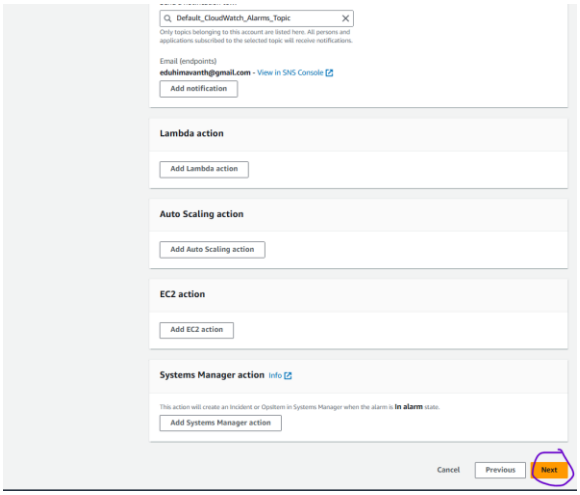


- Set the "Threshold type" to "Static".
- Set the "Whenever CPUUtilization is..." field to "Greater/Equal".
- Enter "60" in the "than..." field.

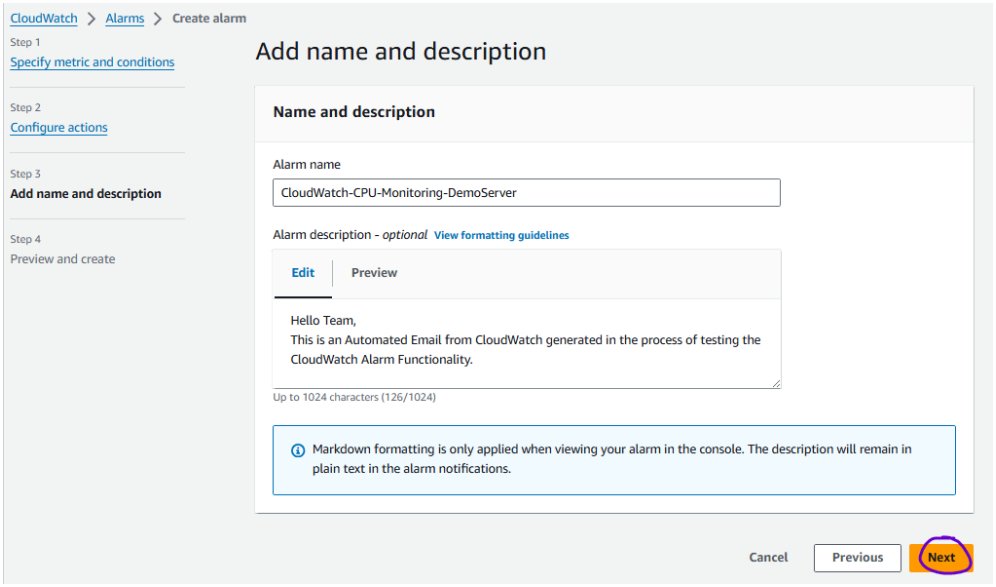


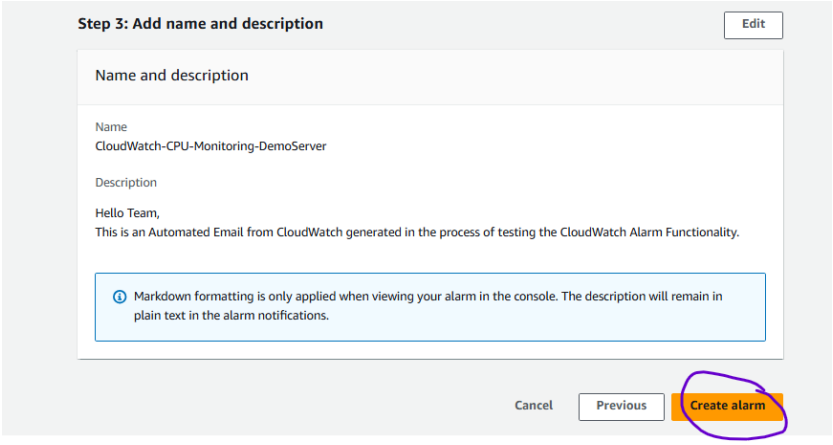
- In the "Notification" section, click on "Add notification".
- Choose "In alarm" in the "Whenever this alarm state is" field.
- In the "Send a notification to..." dropdown, Click on "Create new topic".
- Enter a name for the topic and the email addresses to notify. Click "Create topic".

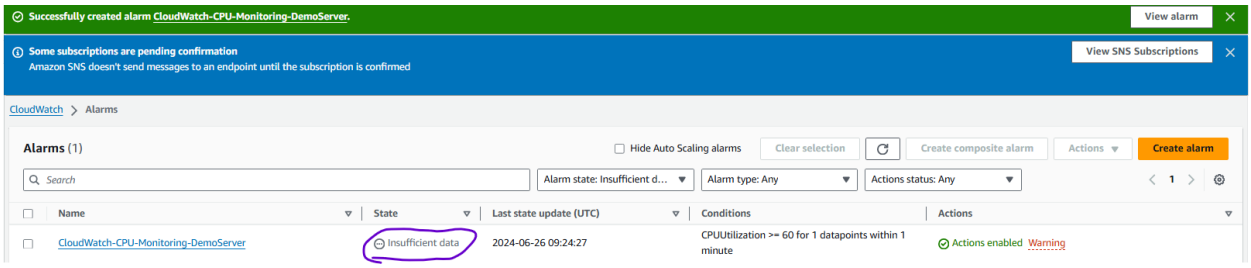




- Enter a name and description for your alarm.
- Click "Create alarm".



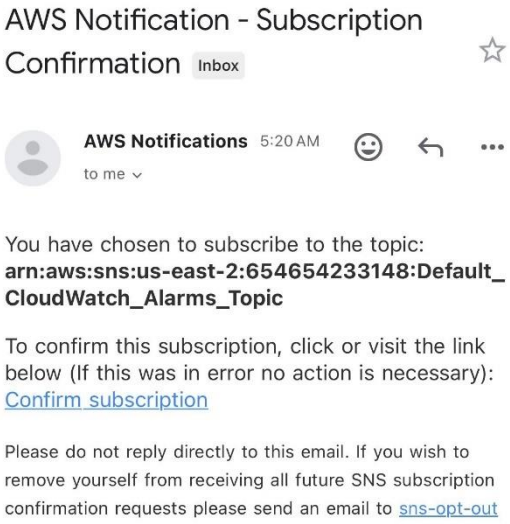


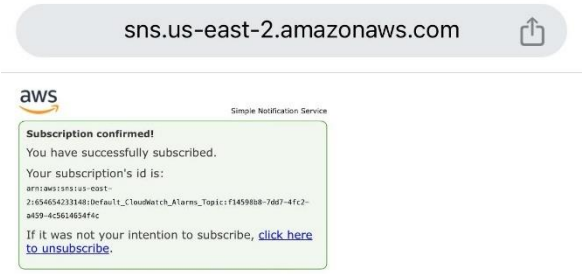


Note: For this test, the statistic is set to “Maximum” and the period to “1 minute.” Generally, organizations choose “Average” with a period of 5 minutes. Additionally, after creating an alarm, it will not be directly activated; you need to accept the subscription to activate the alarm.

3 - Accepting the AWS Cloud Watch Subscription in the Email

- Open your email client and look for an email from AWS Notifications.
- Open the email and click on the "Confirm subscription" link.

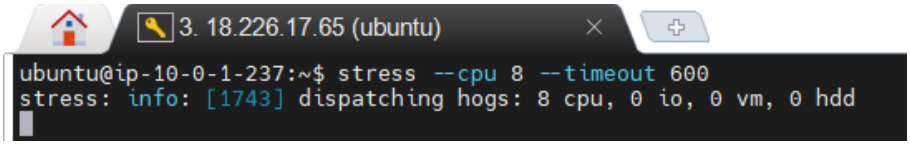




4 - Logging into the Ubuntu Instance and Entering a Command to Spike up the CPU Utilization

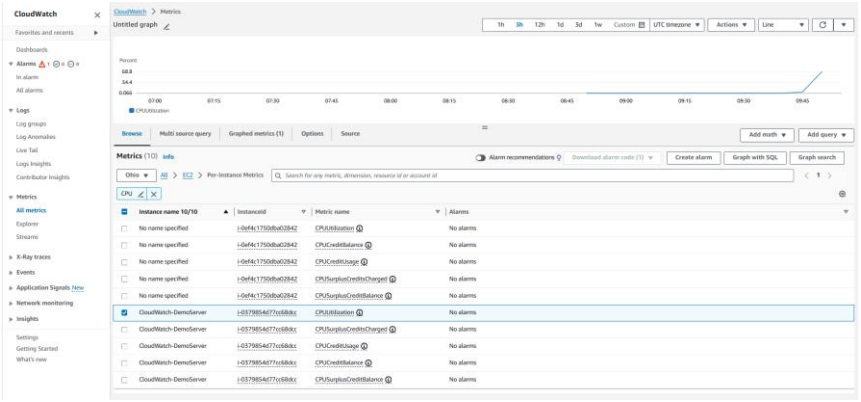
- Login into your EC2 Instance.
- Once logged in, install a stress tool to simulate high CPU usage.
  sudo apt update
  sudo apt install stress
- Run the following command to spike the CPU utilization.
  stress --cpu 8 --timeout 600
- This command will create CPU stress on 8 cores for 600 seconds (10 minutes)


```
Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-10-0-1-237:~$
```

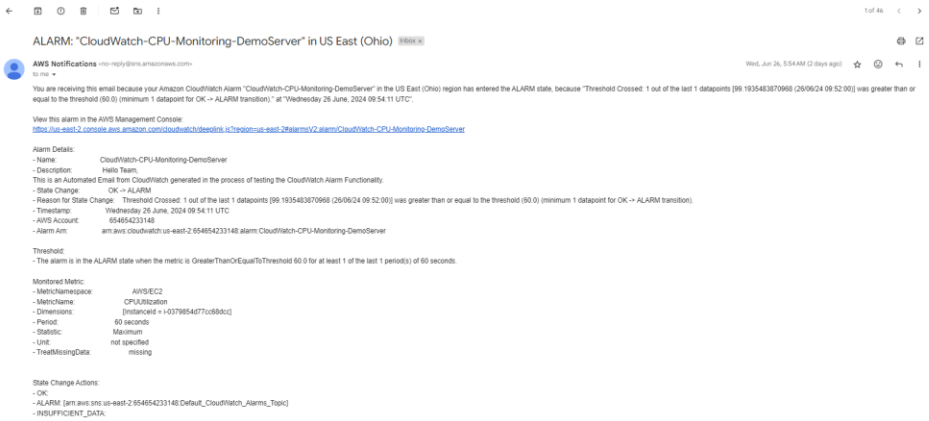


5 – Monitor the Graph and Check for the Alert

- Go to “CloudWatch” and Watch your Metric i.e. “CPUUtilization”



- Now, check your Inbox too see if you have received the Alert from AWS CloudWatch



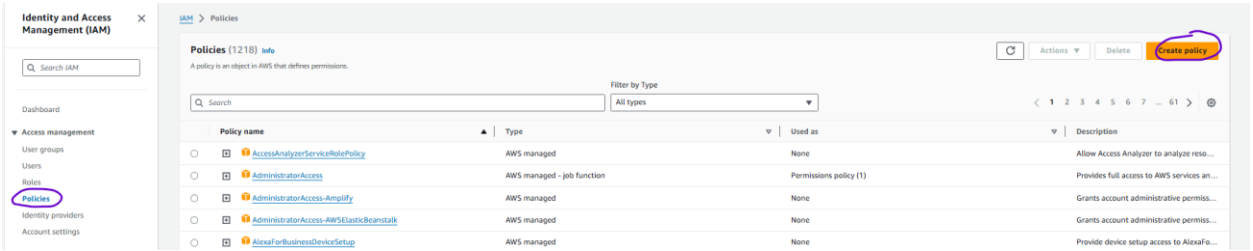
Case 1 - Creating a CloudWatch log for monitoring inbound and outbound traffic involves setting up AWS CloudWatch to collect and store network traffic data

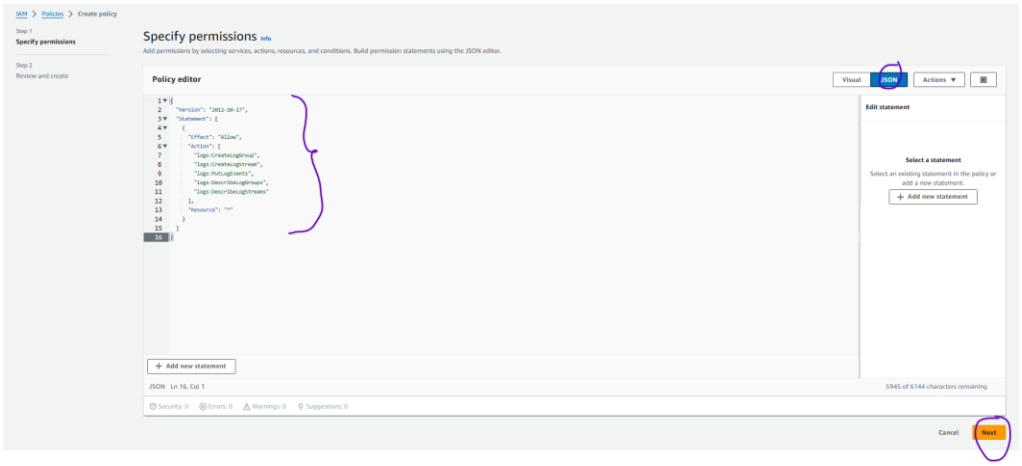
1 - Create the IAM Policy

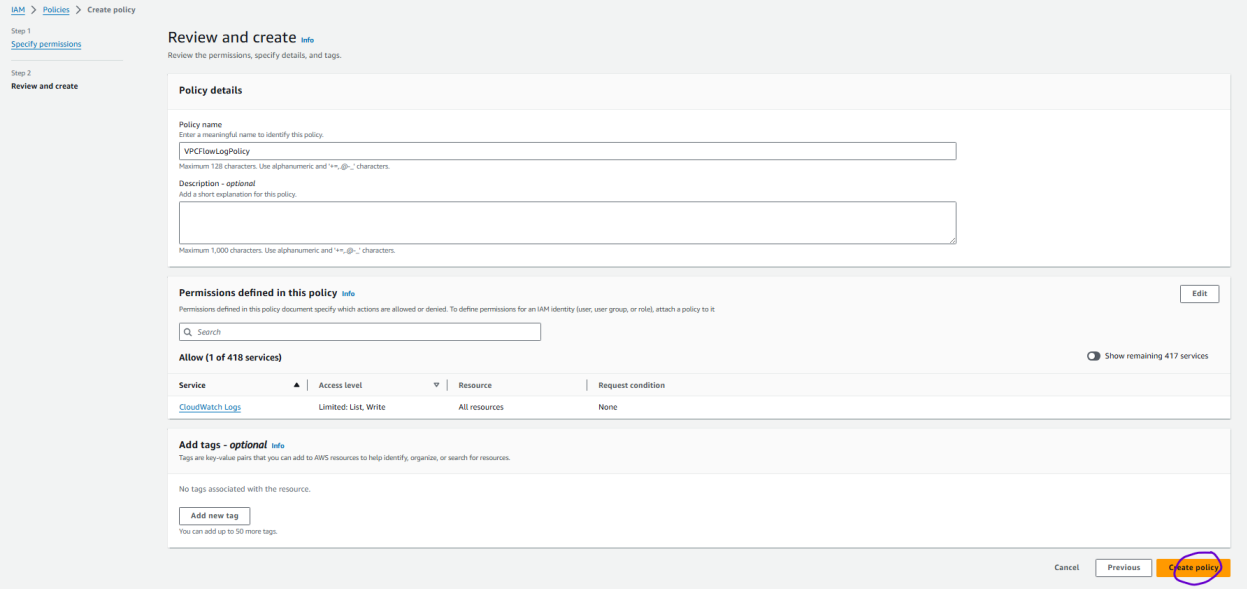
- Navigate to the IAM Console
- In the left-hand navigation pane, click Policies.
- Click Create policy.
- Copy and paste the below custom JSON policy into the editor.

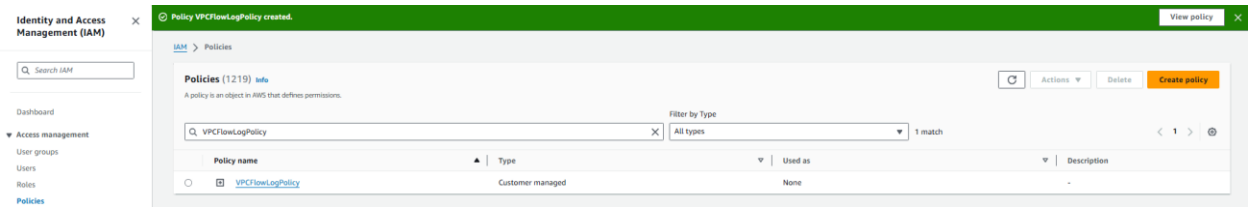
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

- Click Next: Tags (optional) and then Next: Review.
- Enter a name and description for your policy (e.g., VPCFlowLogPolicy).
- Click Create policy.







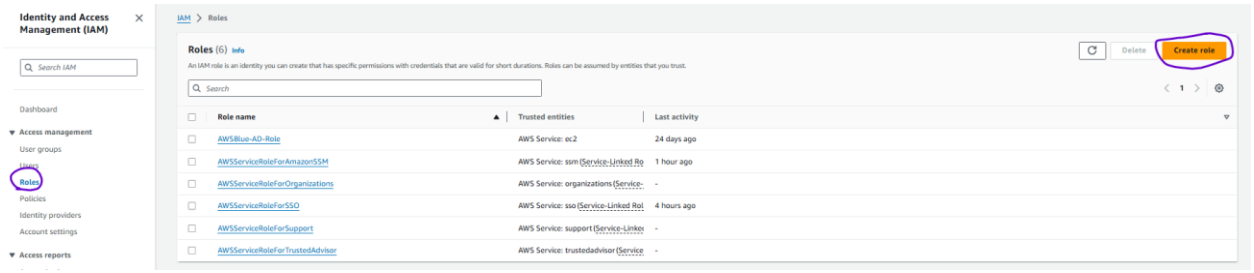


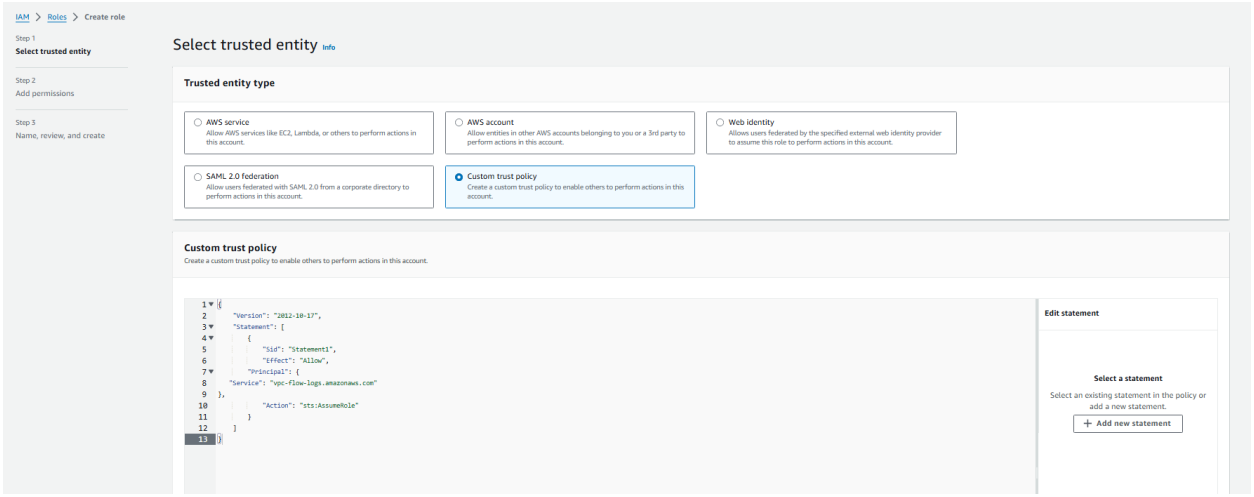
2 - Create the IAM Role

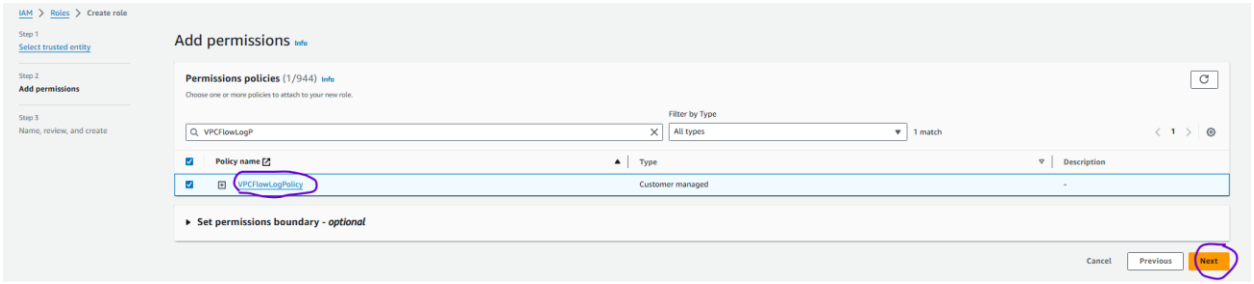
- In the left-hand navigation pane, click Roles.
- Click Create role.
- Choose the Custom trust policy.
- Paste your custom trust policy into the policy editor.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Principal": {
                            "Service": "vpc-flow-logs.amazonaws.com"
                        },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

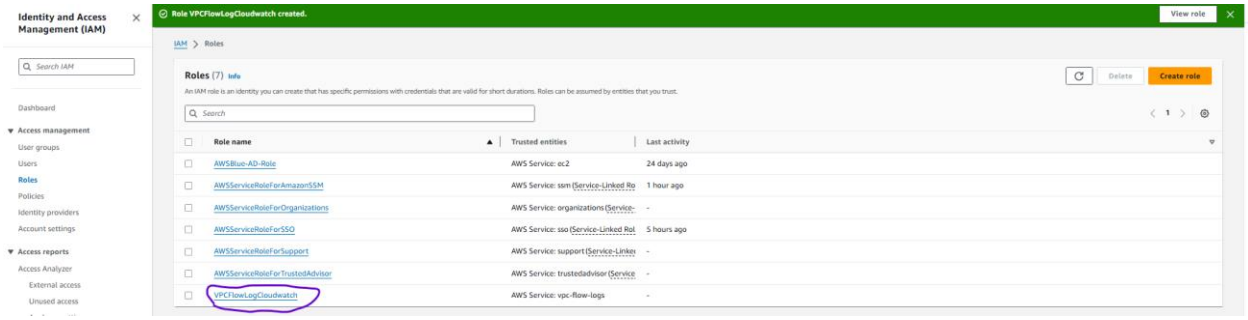
- Click Next: Permissions.
- Attach the necessary policies that define what actions the role can perform. (e.g,.VPCFlowLogPolicy)
- Click Next: Tags (optional) and then Next: Review.
- Enter a role name (e.g., VPCFlowLogCloudwatch) and an optional description.
- Review your settings and click Create role.


Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
IAM > Roles
Roles (6) Info
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.
Search
Delete
Create role
Role name
Trusted entities
Last activity
AWSBlue-AD-Role
AWS Service: ec2
24 days ago
AWSServiceRoleForAmazonSSM
AWS Service: ssm (Service-Linked Ro
1 hour ago
AWSServiceRoleForOrganizations
AWS Service: organizations (Service-
-
AWSServiceRoleForSSO
AWS Service: sso (Service-Linked Rol
4 hours ago
AWSServiceRoleForSupport
AWS Service: support (Service-Linke
-
AWSServiceRoleForTrustedAdvisor
AWS Service: trustedadvisor (Service
-


IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Select trusted entity Info
Trusted entity type
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Statement1",
"Effect": "Allow",
"Principal": {
"Service": "vpc-flow-logs.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
]
}
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
Add new statement

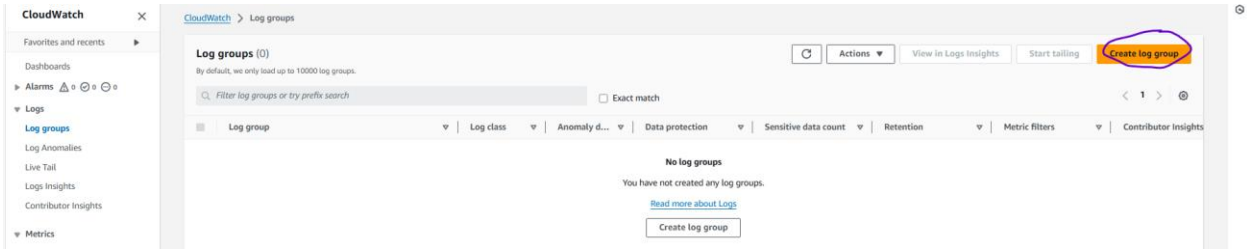

IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Add permissions Info
Permissions policies (1/944) Info
Choose one or more policies to attach to your new role.
VPCFlowLogP
Filter by Type
All types
1 match
Policy name
Type
Description
VPCFlowLogPolicy
Customer managed
-
Set permissions boundary - optional
Cancel
Previous
Next

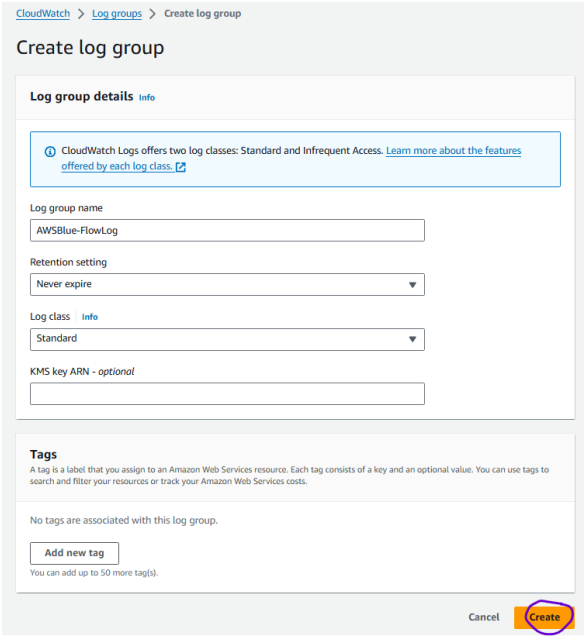

IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
VPCFlowLogCloudwatch
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=, .@-/\[{}]!#$%^&*();:?<>`
Step 1: Select trusted entities
Edit



3 - Create Log Group

- Navigate to the CloudWatch dashboard.
- In the left navigation pane, choose `Log groups`.
- Click `Create log group`.
- Enter a name for the log group and click `Create`.



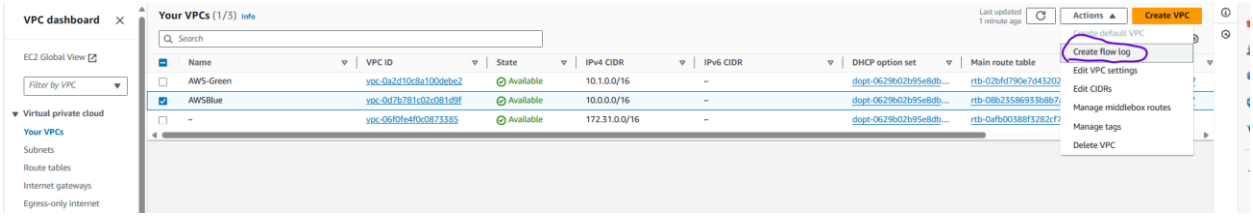


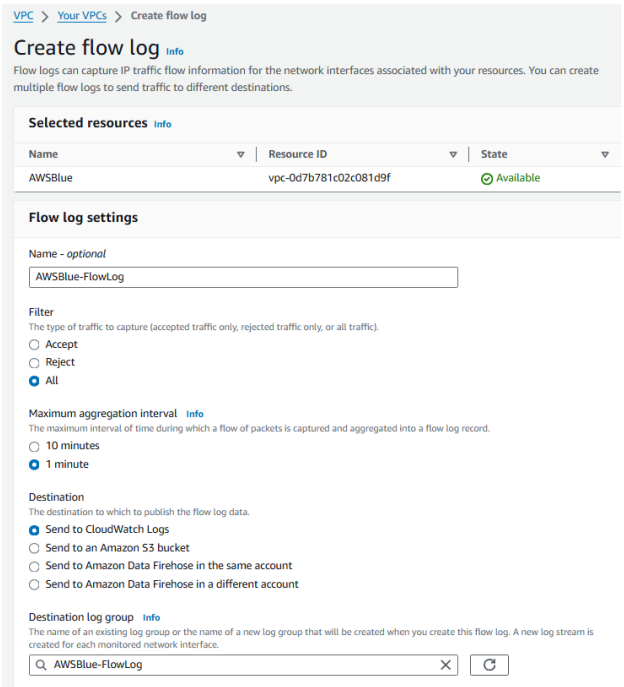
3 - Navigate to VPC Console

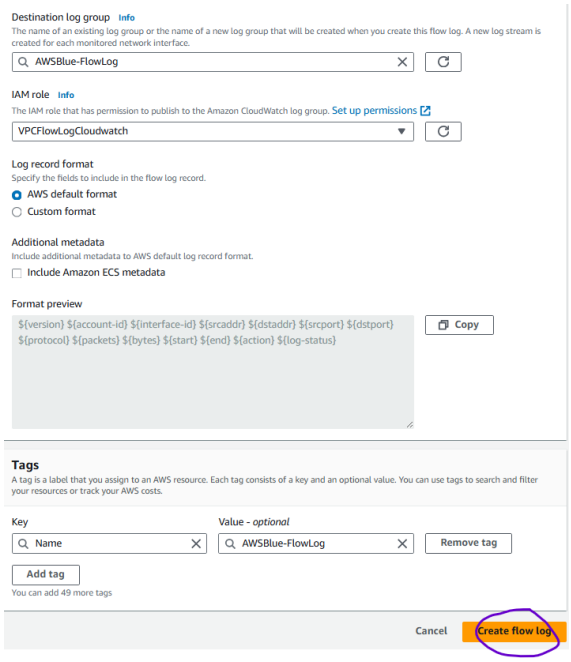
- Open the AWS Management Console.
- Navigate to the VPC dashboard.

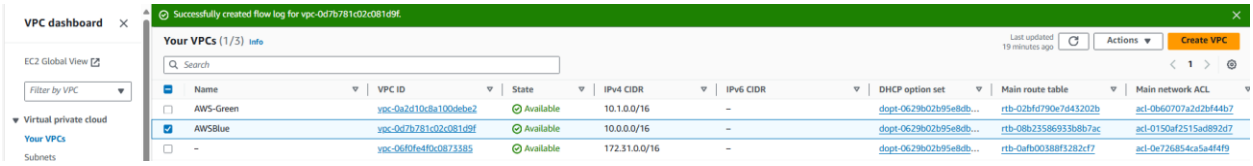
4 - Create a Flow Log

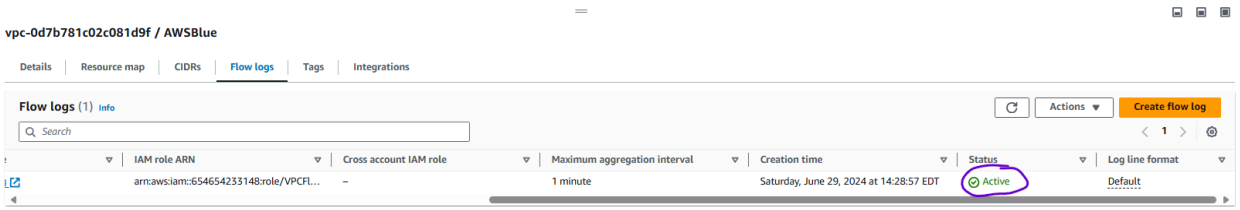
- Select the VPC where the server is deployed. Click “Actions” and Click `Create Flow Log
- Select the `Filter` (e.g., `All`, `Reject`, or `Accept` traffic) and `Maximum Aggregation Interval` (e.g., 10 minutes or 1 minute).
- Choose `Send to CloudWatch Logs`.
- Select or create a new IAM role that has the necessary permissions to publish flow logs to CloudWatch Logs.
- Choose the CloudWatch log group where the logs will be sent- You can create a new log group if needed.
- Select the VPC, subnet, or network interface for which you want to monitor traffic.
- Click `Create Flow Log` to start collecting traffic data.











Note: Make sure that the status of the created FlowLog is Active.

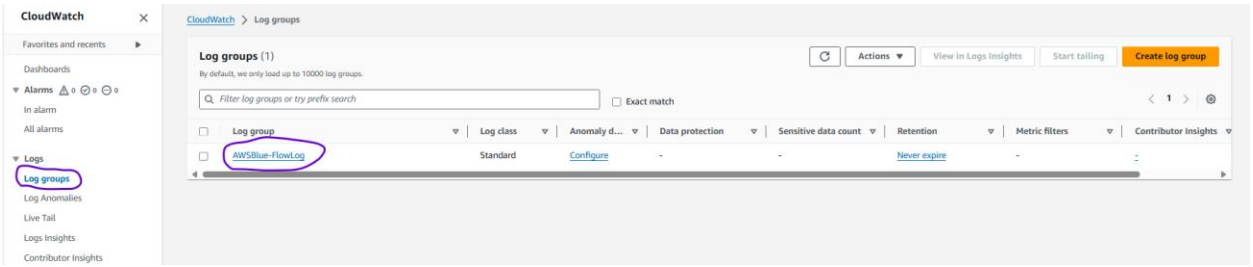
TASK:

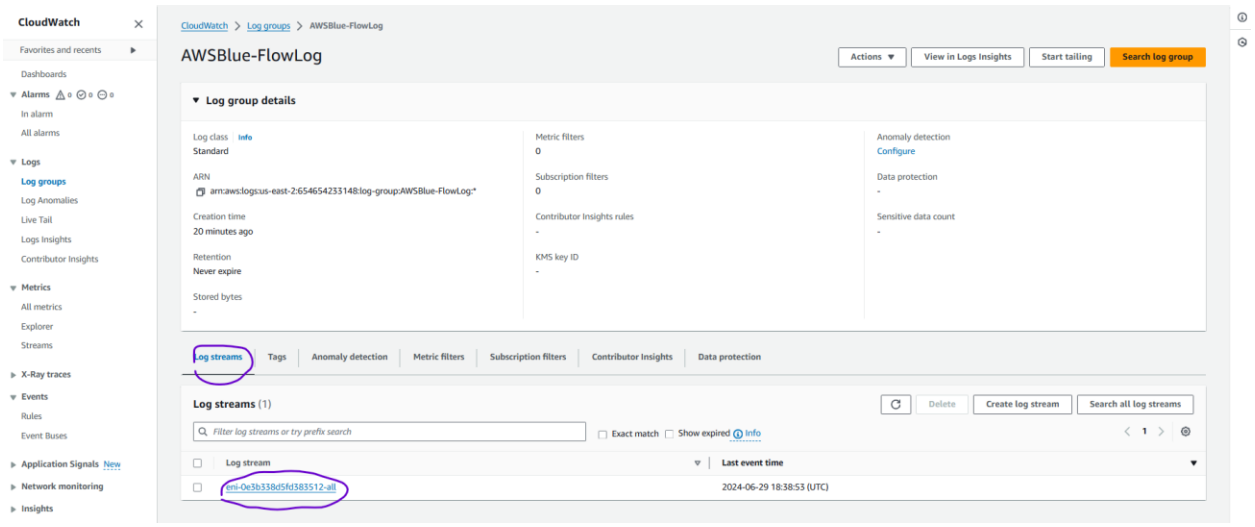
- **Launch an ubuntu Instance using the VPC which we have created FlowLog.**
- **Log into the ubuntu Instance.**
- **Install a webserver, Start the webserver and open the url of the webserver to generate some log events in the CloudWatch**
  Or
- **Try pinging the ubuntu instance from other servers or CMD**
- **After performing the above steps follow the below steps to check if the events are logged in the CloudWatch.**

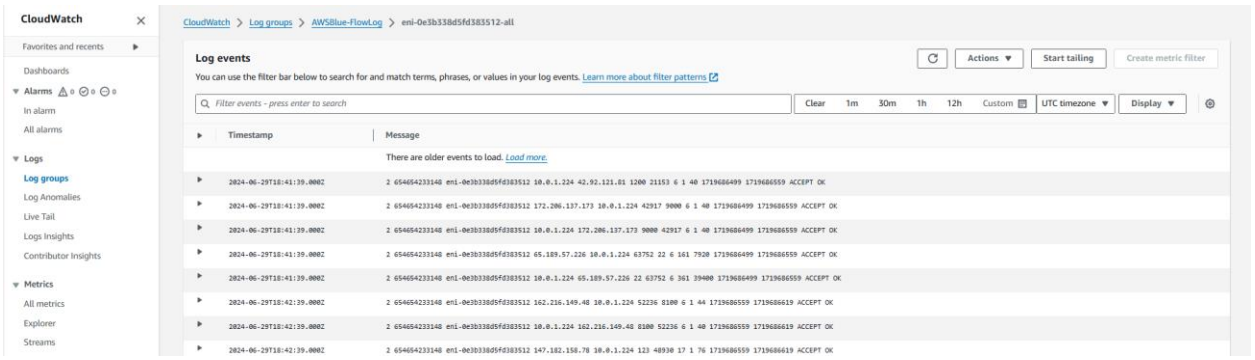
Note: In our case I have taken both above steps into consideration. Visit my GIT repo to get the commands used for installing the Apache webserver in ubuntu.

5 – Verification of the CloudWatch Logs

- Navigate to the CloudWatch Dashboard
- In the left-hand navigation pane, click on “Log groups” under the “Logs” section.
- Click on the Log group which we have created "AWSBlue-FlowLog"
- Under the “LogStreams” you will find a new logstream. Click on the logstream
- Now you will be able to see the Logs generated.







6 – Exporting the generated logs to S3 bucket

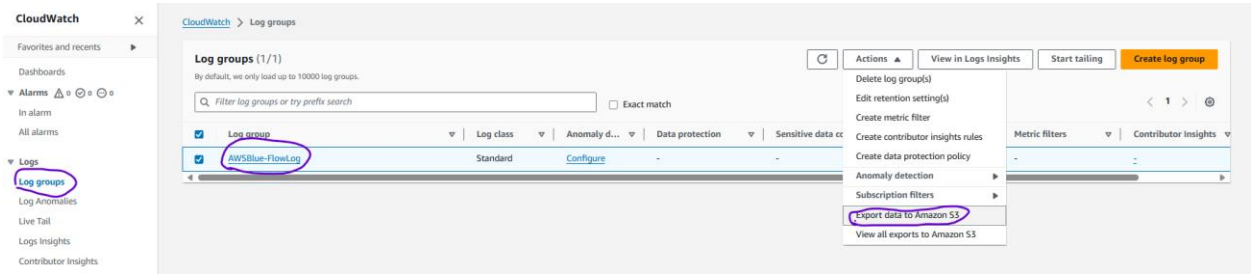
TASK – Create an S3 bucket and attach the below Bucket Policy to the bucket.

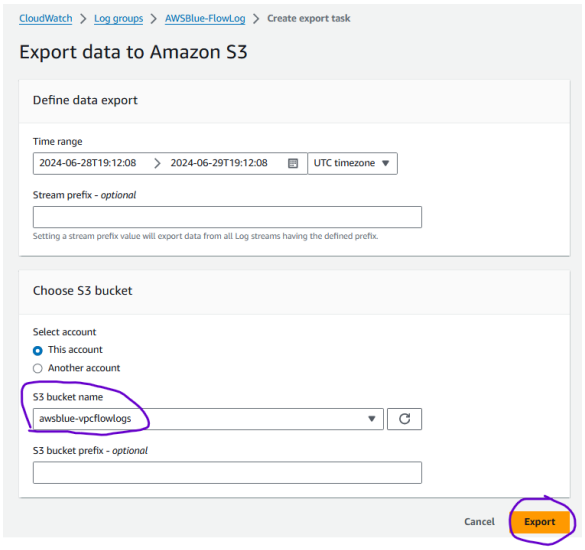
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "logs.amazonaws.com"
            },
            "Action": [
                "s3:GetBucketAcl",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::your-bucket-name",
                "arn:aws:s3:::your-bucket-name/*"
            ]
        }
    ]
}
```

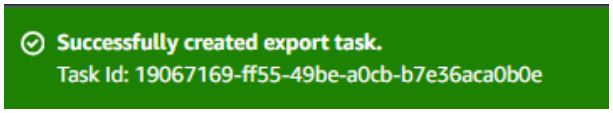
Note: This bucket policy allows complete access of the S3 bucket to CloudWatch

1 - Exporting the logs to S3

- Go to the CloudWatch Console.
- In the navigation pane, choose "Log groups."
- Select the log group you want to export.
- Click on the "Actions" dropdown menu.
- Select "Export data to Amazon S3."
- Bucket: Choose the S3 bucket where you want to store the logs.
- Prefix: Specify a prefix for the logs (optional).
- From and To: Specify the time range for the logs you want to export.
- Start Export: Click "Start Export."

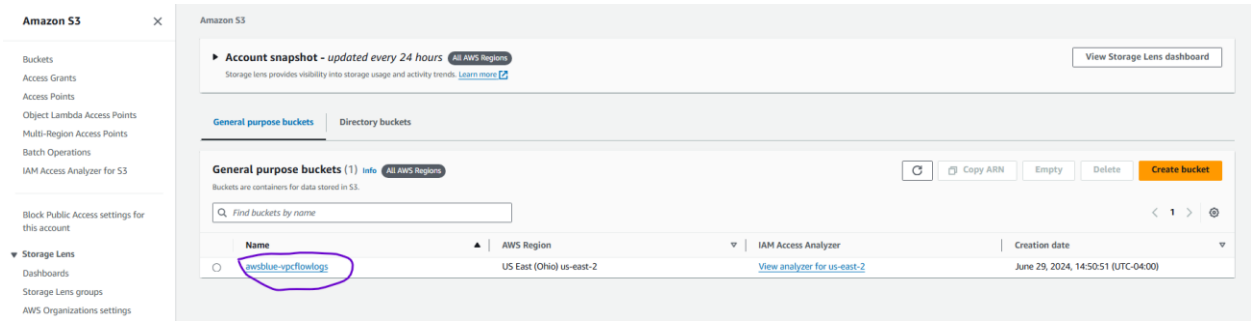


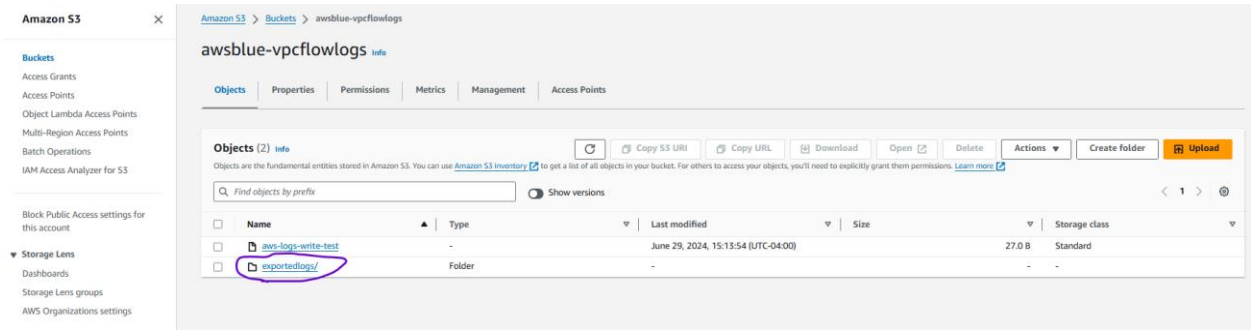


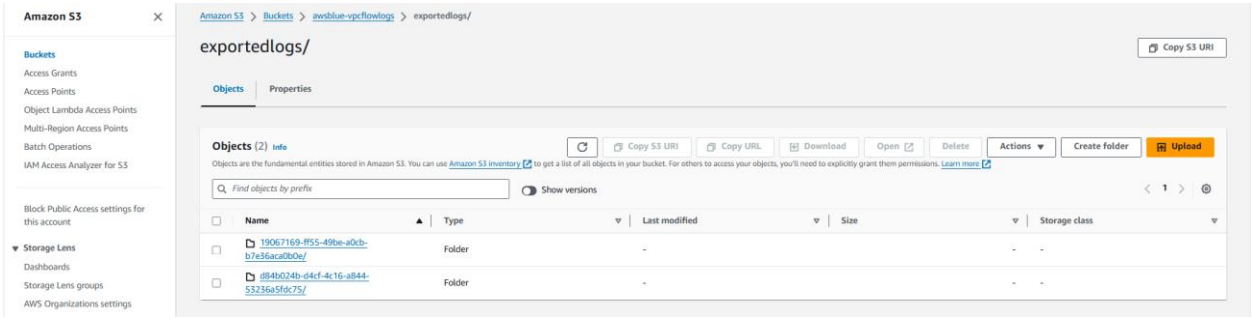


2 – Verification of the Exported Logs

- Go to the S3 Console
- Click on the Bucket to which the Logs are exported.
- Check if the logs are exported







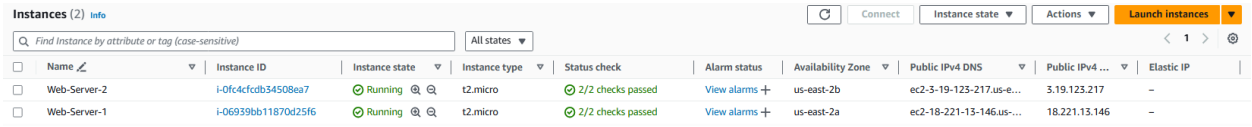
Note: We can automate exporting CloudWatch Logs to S3 by scheduling export tasks, setting filters for specific logs, defining destinations in S3, and ensuring proper permissions. This streamlines data backups and integration with analytics.

Demonstrating the functionality of AWS Application Load Balancer (ALB)

TASK – Deploy 2 EC2 Instances (Ubuntu) in same VPC but in 2 different subnets.

Note: UbuntuInstance-1 = Web-Server-1 (Subnet-1)

UbuntuInstance-2 = Web-Server-2 (Subnet-2)



TASK – Install Apache2 Webserver in both the Instances

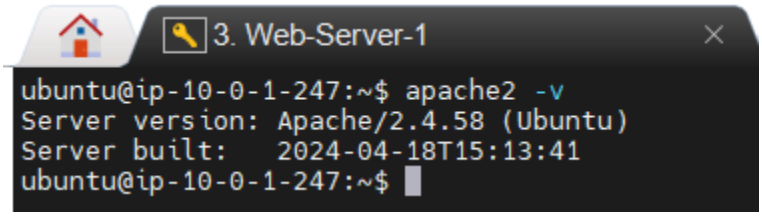
Note: Visit my GIT repo to get the commands used for installing the Apache webserver in ubuntu.

1 – Verifying the Installation of Apache2 in both the machines and accessing them using respective URL's

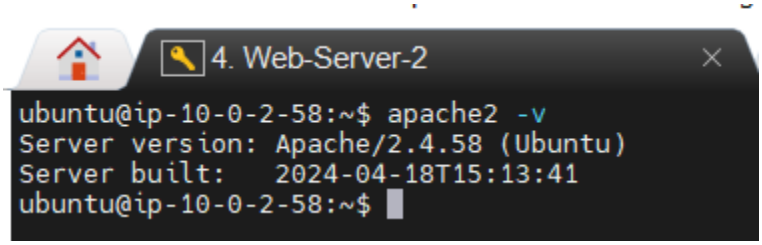
- Use the below command to confirm the installation of Apache2.

  apache2 -v

Web-Server-1:



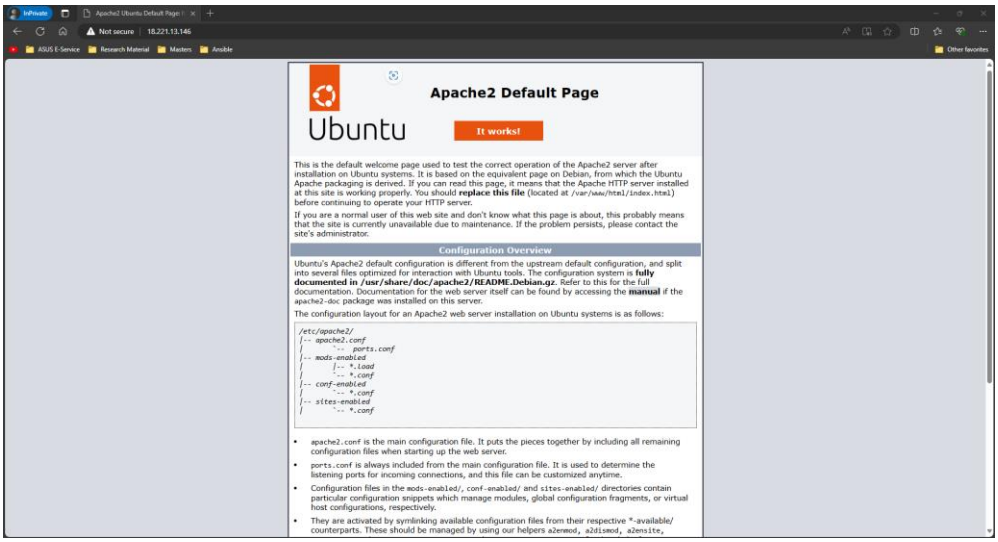
Web-Server-2:



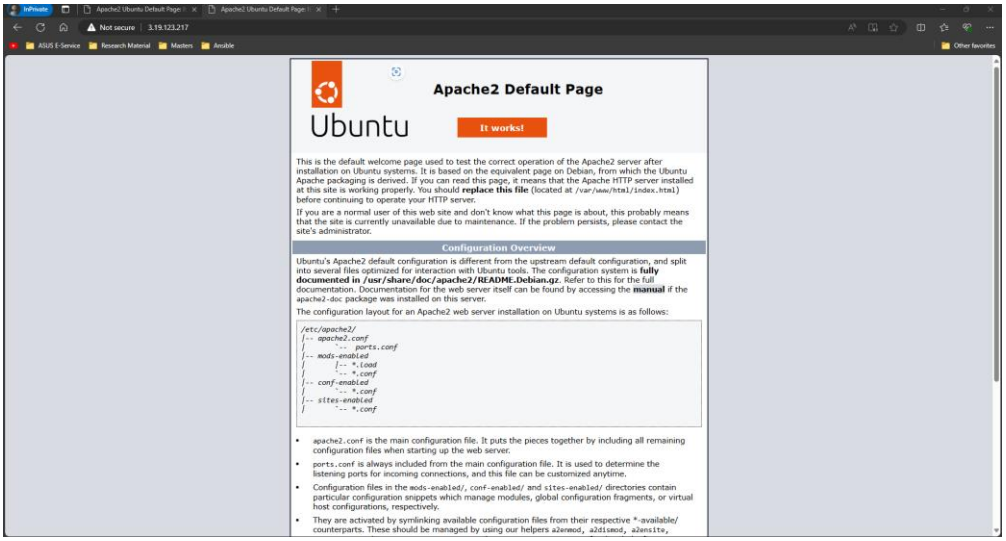
- Access the respective URL's and confirm the accessibility of the Webserver.

  Use http://Public-IP-of-Webserver

Web-Server-1:



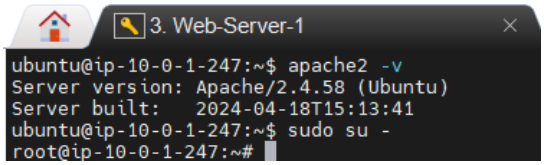
Web-Server-2:



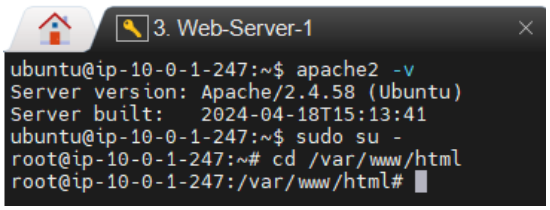
Note: As both webpages look similar, it will be difficult to identify which is Web-Server-1 and which is Web-Server-2. To make identification easier, let's modify the HTML files of the Apache2 servers and replace "Apache2 Default Page" with "Web-Server-1" and "Web-Server-2" respectively.

2 – Implementing changes to the HTML files of the Apache2 Servers.

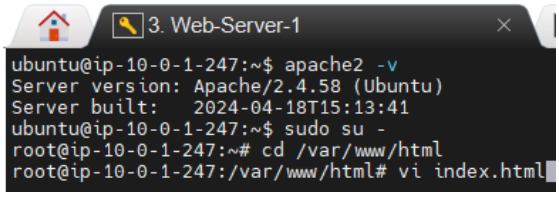
- Access Web-Server-1.
- Change the user from “ubuntu” to “root”.
  Sudo su –



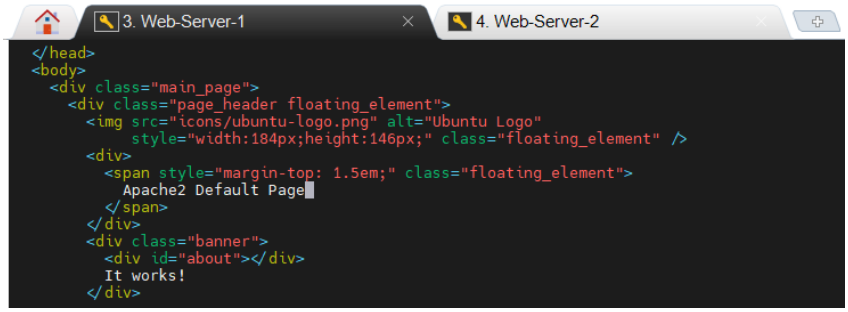
- Navigate to the directory where the HTML file of the Apache2 is location
  cd /var/www/html

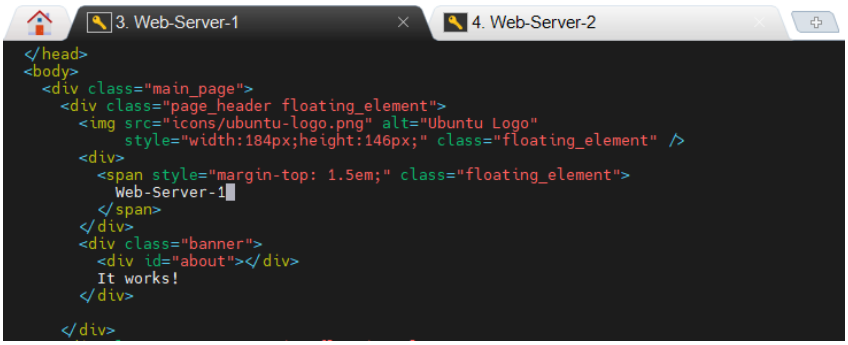


- Edit the default HTML file.
  vi index.html

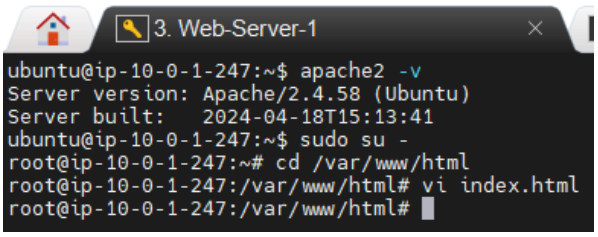


- Replace "Apache2 Default Page" with "Web-Server-1.
  Note: Press "i" to add or remove data into the HTML file

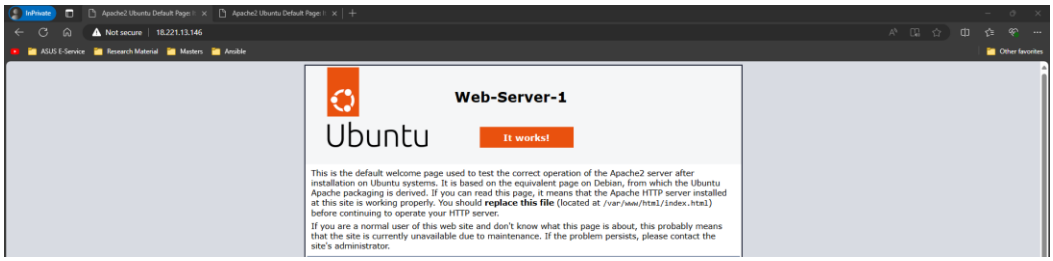




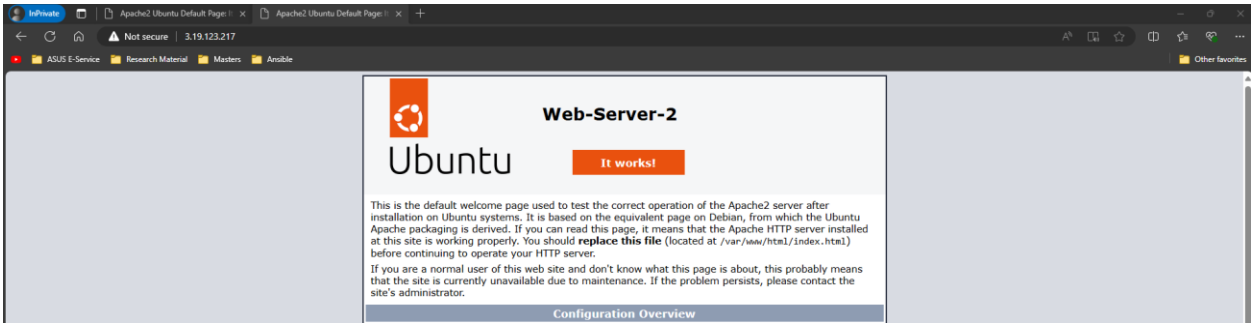
- Save and exit the editor.
  Note: Press esc button followed by :wq! And hit enter to save and exit the editor



- Refresh the Web-Server-1 URL to confirm if the changes have been applied.



TASK – Following the above steps implement the changes for Web-Server-2

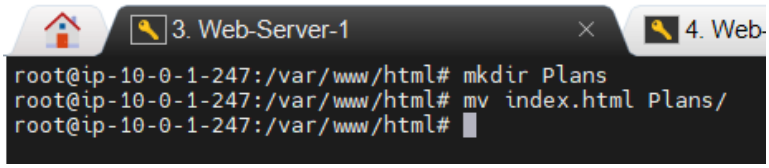


3 – Creating custom pages on both the servers.

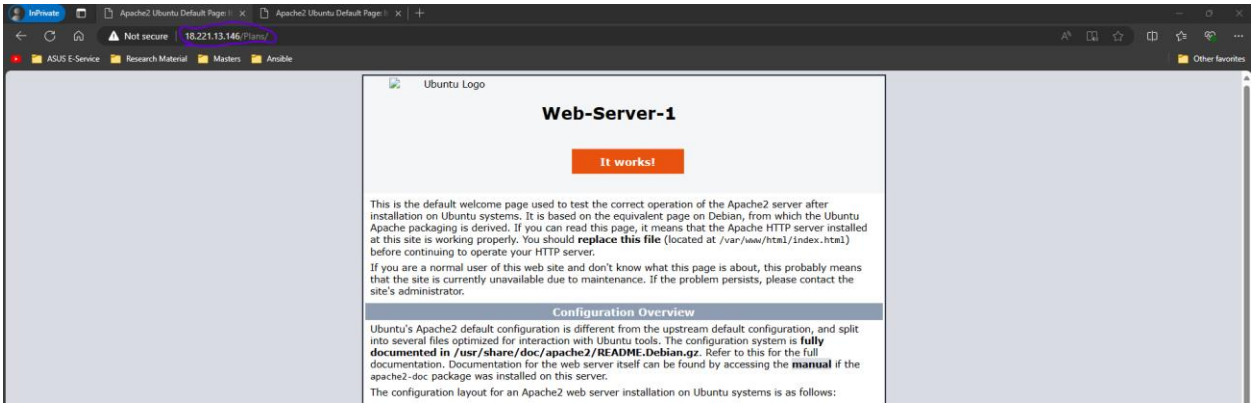
Note: Creating custom pages on each server allows you to demonstrate how an Application Load Balancer (ALB) can route traffic based on specific URL paths to different backend servers.

For Web-Server-1, Create a page for /Plans:

- Under /var/www/html, Create a folder “Plans”
- Move all the file present under /var/www/html into /var/www/html/Plans

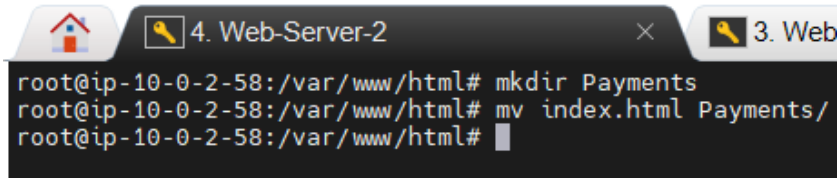


- Now, Verify the implementation of the custom page by accessing the Web-Server-1 using http://PublicIp-of-Webserver1/Plans



For Web-Server-2, Create a page for /Payments:

- Under /var/www/html, Create a folder “Payments”
- Move all the file present under /var/www/html into /var/www/html/Payments

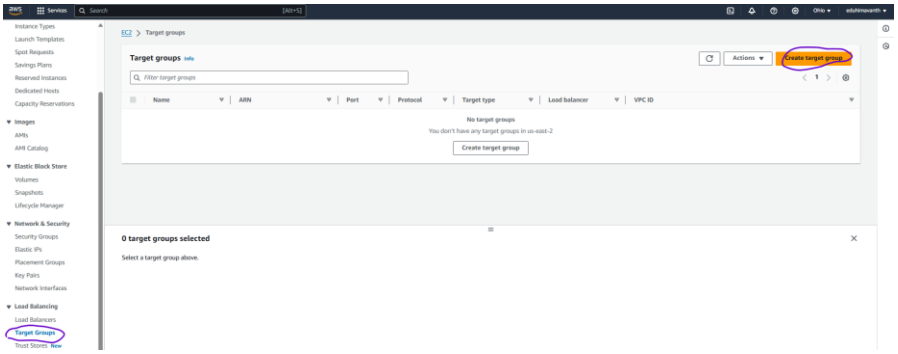


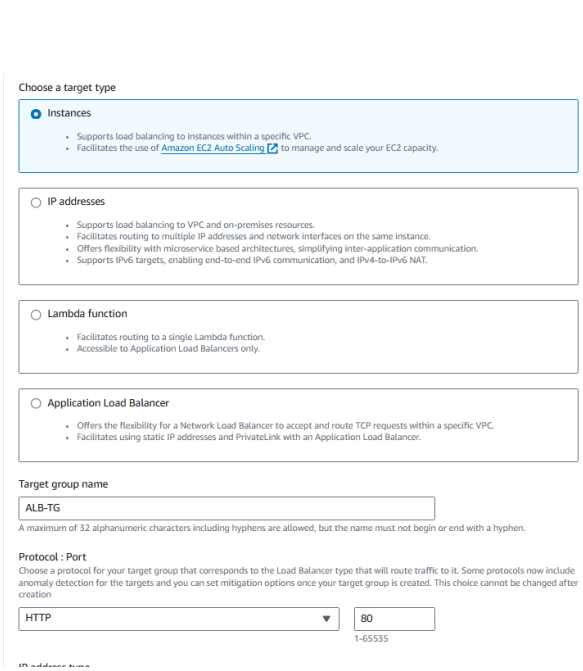
- Now, Verify the implementation of the custom page by accessing the Web-Server-1 using http://PublicIp-of-Webserver1/Payments

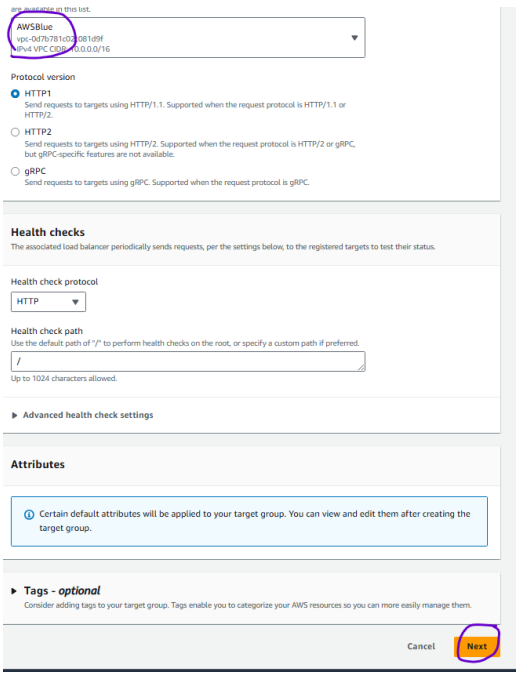
3 – Creating Target Group

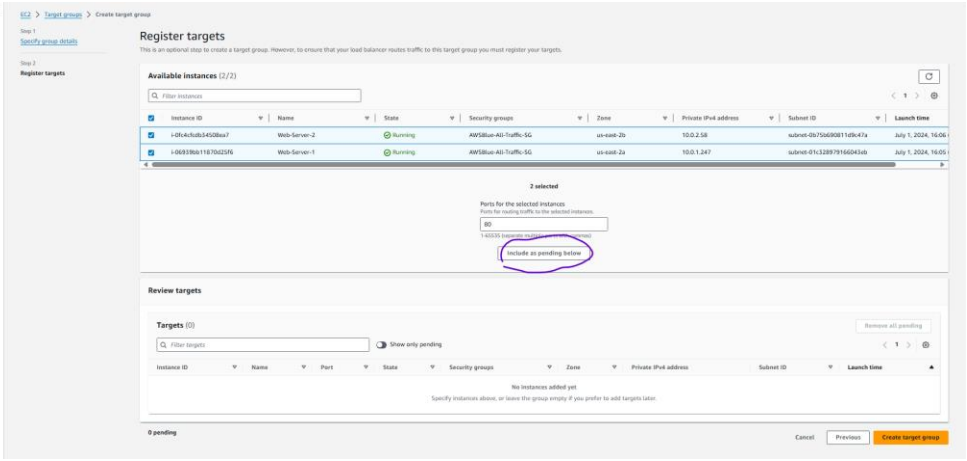
- Navigate to the EC2 Dashboard.
- Under "Load Balancing", click on "Target Groups".
- Click on "Create target group".
- Choose `Instances` as the target type.
- Provide a name for the target group, e.g., `web-servers-target-group`.
- Set the protocol to `HTTP` and the port to `80`.
- Choose the VPC where your instances are running.
- Click "Next" to register targets.
- Select `Web-Server-1` and `Web-Server-2` instances.
- Click "Include as pending below".
- Click "Create target group".

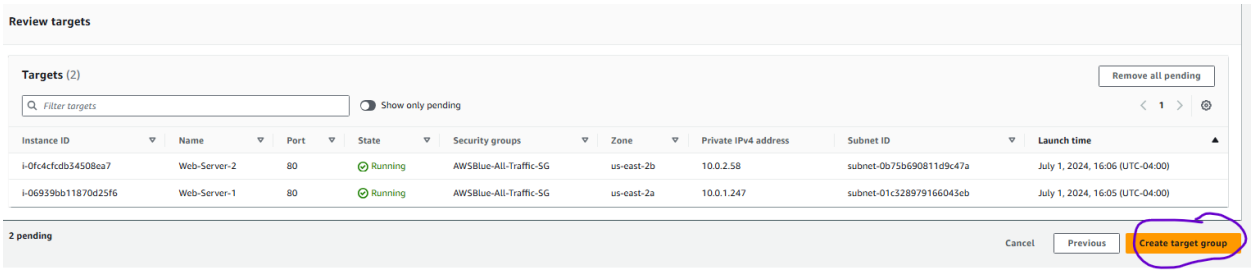
Note: Initially the health of the registered targets will be" unused" as we didn't configure and deployed the ALB.

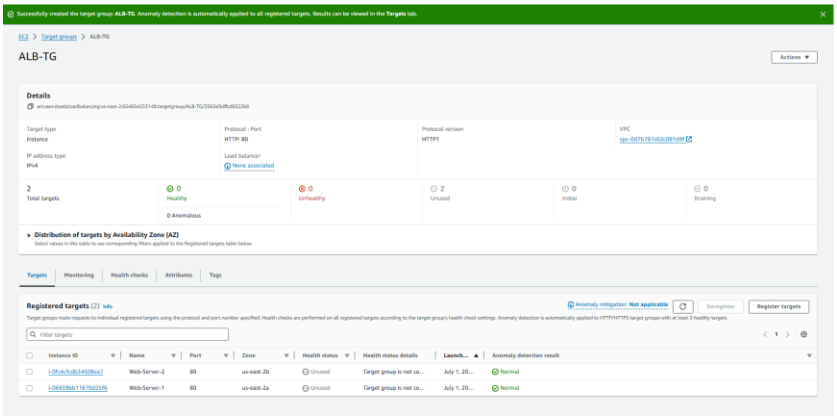








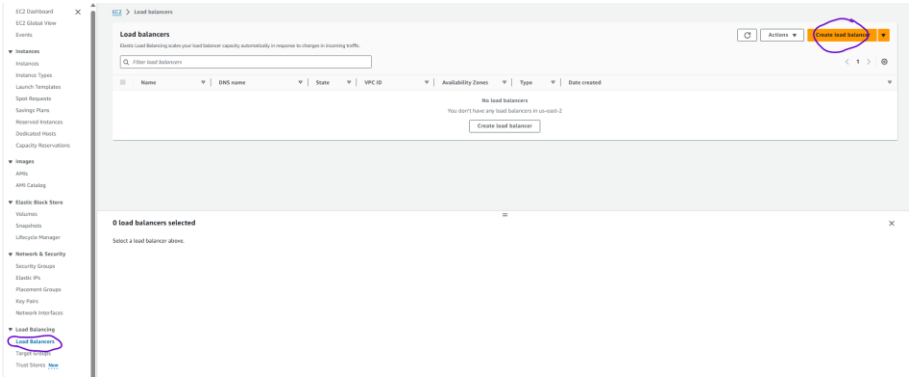


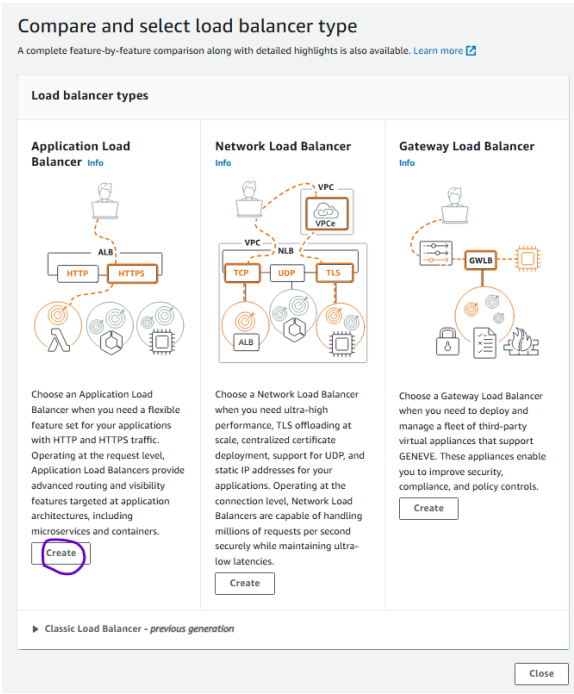


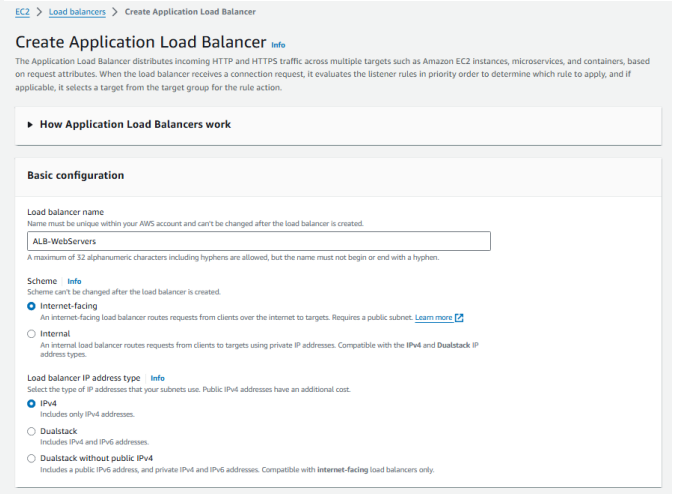
4 - Deploy Application Load Balancer (ALB):

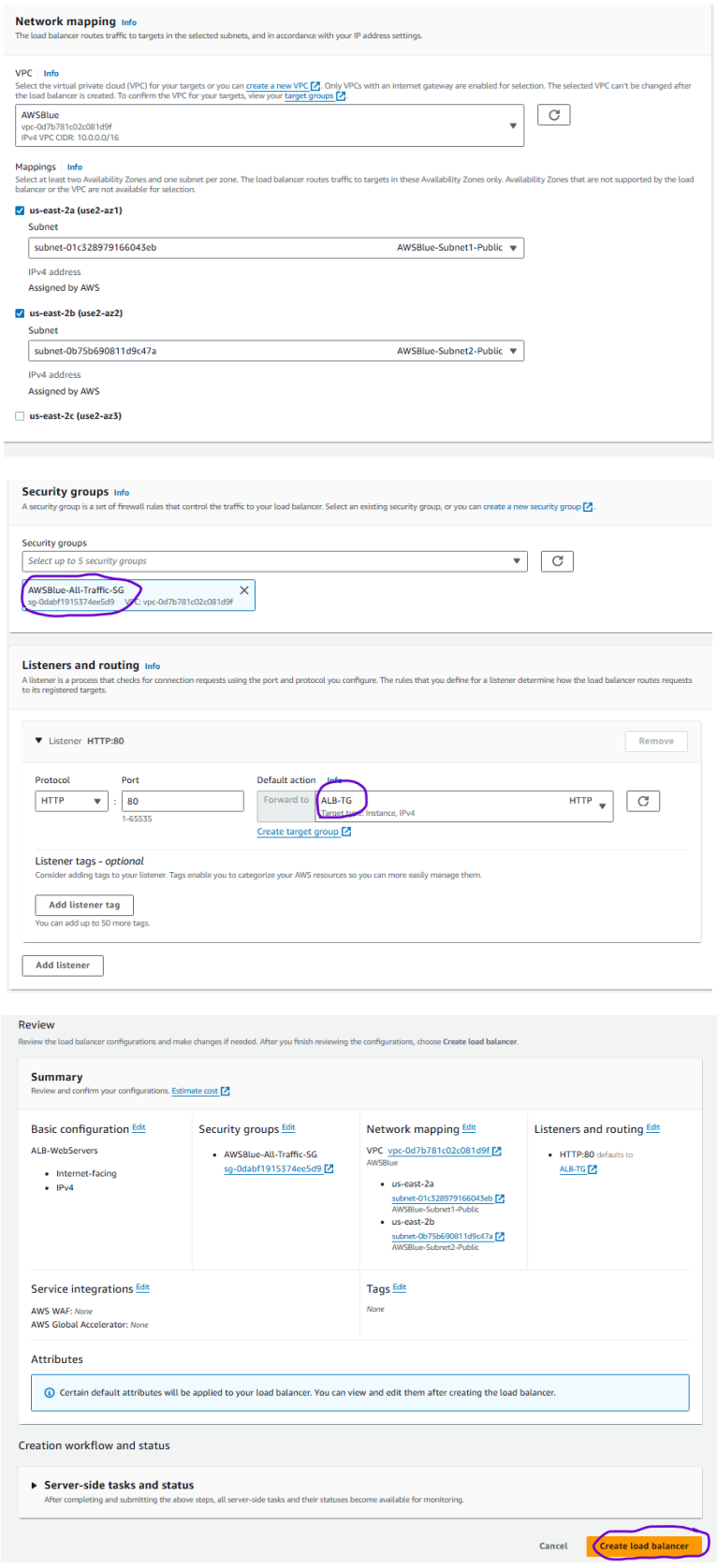
- In the EC2 Dashboard, click on "Load Balancers" under "Load Balancing".
- Click on "Create Load Balancer".
- Choose "Application Load Balancer".
- Click on "Create".
- Provide a name for the load balancer, e.g., `web-servers-alb`.
- Select "internet-facing".
- Configure listeners to use HTTP and port 80.
- Select the VPC and subnets (ensure at least two subnets in different availability zones are selected).

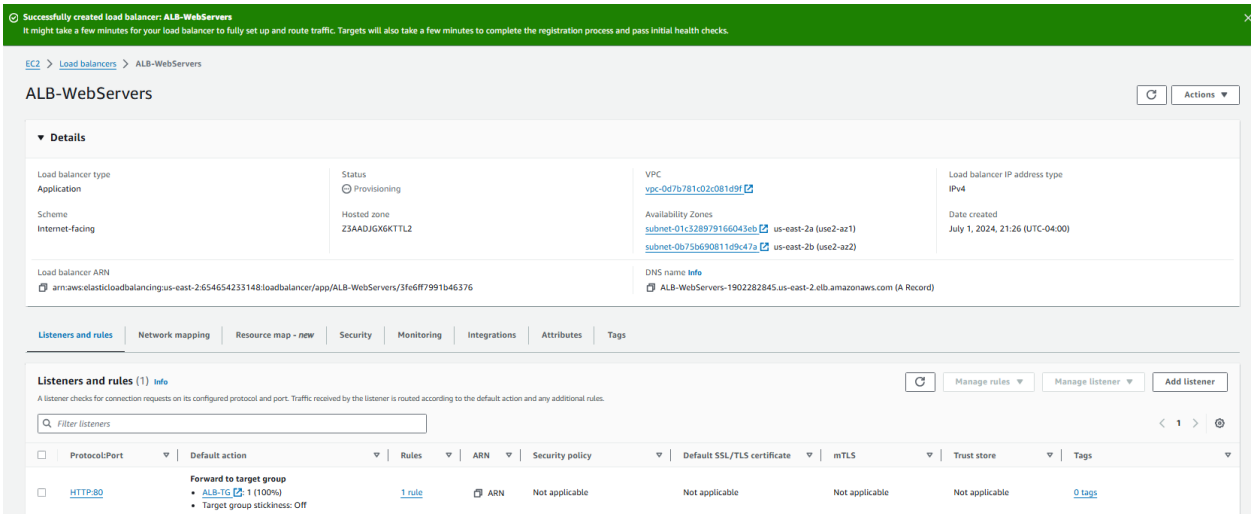
- Choose the security group created earlier that allows HTTP (port 80) and SSH (port 22) access.
- Under "Default action", choose "Forward to" and select the target group created earlier (`web-servers-target-group`).
- Ensure the correct targets (`Web-Server-1` and `Web-Server-2`) are registered.
- Click "Create load balancer".

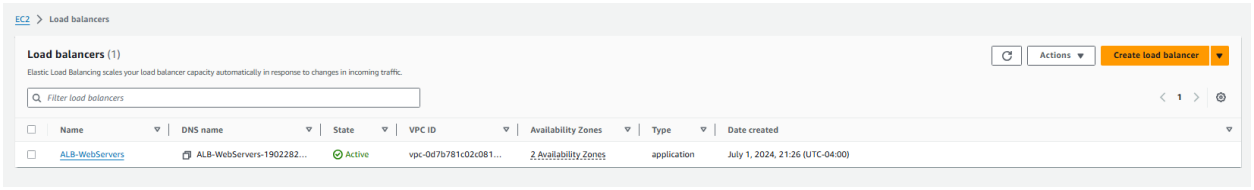


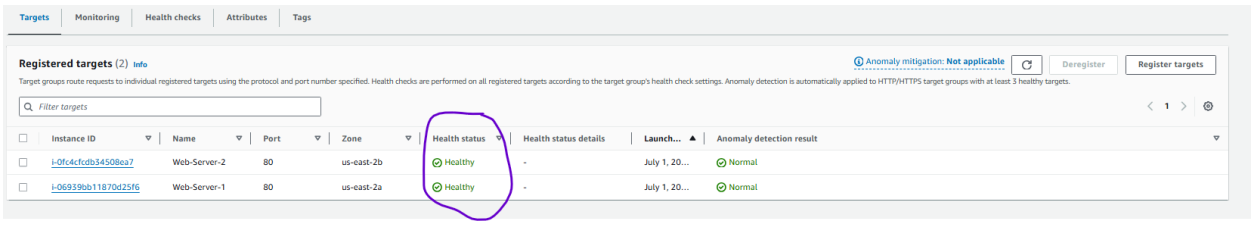





Network mapping Info
The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.
VPC Info
Select the virtual private cloud (VPC) for your targets or you can create a new VPC. Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your target groups.
AWSBlue
vpc-0d7b781c02c081d9f
IPv4 VPC CIDR: 10.0.0.0/16
Mappings Info
Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.
us-east-2a (use2-az1)
Subnet
subnet-01c328979166043eb
AWSBlue-Subnet1-Public
IPv4 address
Assigned by AWS
us-east-2b (use2-az2)
Subnet
subnet-0b75b690811d9c47a
AWSBlue-Subnet2-Public
IPv4 address
Assigned by AWS
us-east-2c (use2-az3)
Security groups Info
A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group.
Security groups
Select up to 5 security groups
AWSBlue-All-Traffic-SG
sg-0dabf1915374ee5d9
VPC vpc-0d7b781c02c081d9f
Listeners and routing Info
A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.
Listener HTTP:80
Remove
Protocol
HTTP
Port
80
1-65535
Default action Info
Forward to
ALB-TG
Target type: Instance, IPv4
HTTP
Create target group
Listener tags - optional
Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.
Add listener tag
You can add up to 50 more tags.
Add listener
Review
Review the load balancer configurations and make changes if needed. After you finish reviewing the configurations, choose Create load balancer.
Summary
Review and confirm your configurations. Estimate cost
Basic configuration Edit
ALB-WebServers
Internet-facing
IPv4
Security groups Edit
AWSBlue-All-Traffic-SG
sg-0dabf1915374ee5d9
Network mapping Edit
VPC vpc-0d7b781c02c081d9f
AWSBlue
us-east-2a
subnet-01c328979166043eb
AWSBlue-Subnet1-Public
us-east-2b
subnet-0b75b690811d9c47a
AWSBlue-Subnet2-Public
Listeners and routing Edit
HTTP:80 defaults to
ALB-TG
Service integrations Edit
AWS WAF: None
AWS Global Accelerator: None
Tags Edit
None
Attributes
Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.
Creation workflow and status
Server-side tasks and status
After completing and submitting the above steps, all server-side tasks and their statuses become available for monitoring.
Cancel
Create load balancer

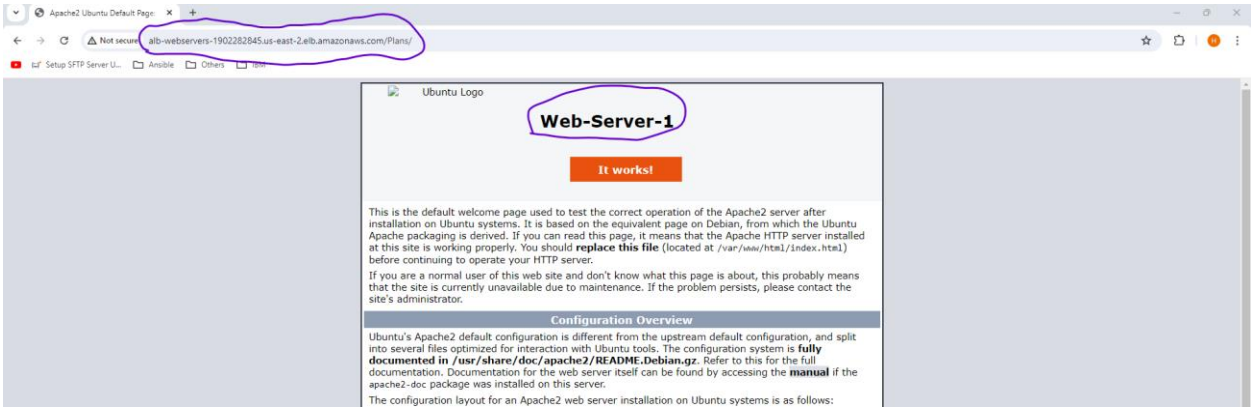






5 - Access Verification Through ALB:

- Once the ALB is created, it will provide a DNS name.
- Use this DNS name to access your web servers.
  For example:
  `http://<ALB_DNS_Name>/plans` will route traffic to `Web-Server-1`.
  `http://<ALB_DNS_Name>/payments` will route traffic to `Web-Server-2`.



Note:

- This completes the demonstration of how an Application Load Balancer (ALB) in AWS works, distributing traffic based on specific URL paths to different backend servers.
- Ensure to delete the Load Balancer and target group created, and terminate the two EC2 instances to avoid charges, as the Load Balancer can incur significant costs.

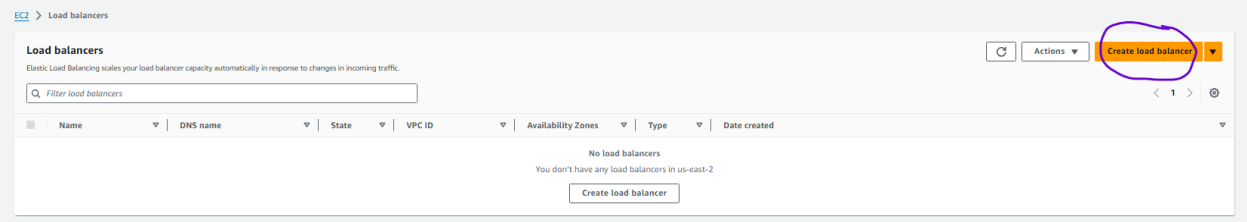
Demonstrating the functionality of AWS Network Load Balancer (NLB)

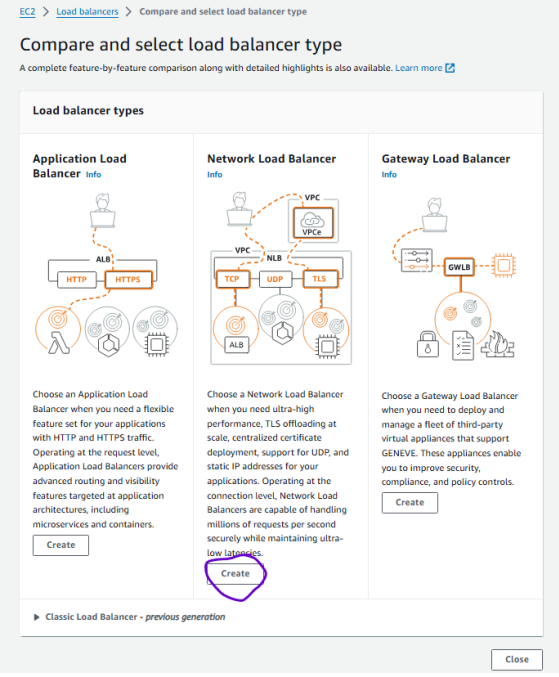
TASKS

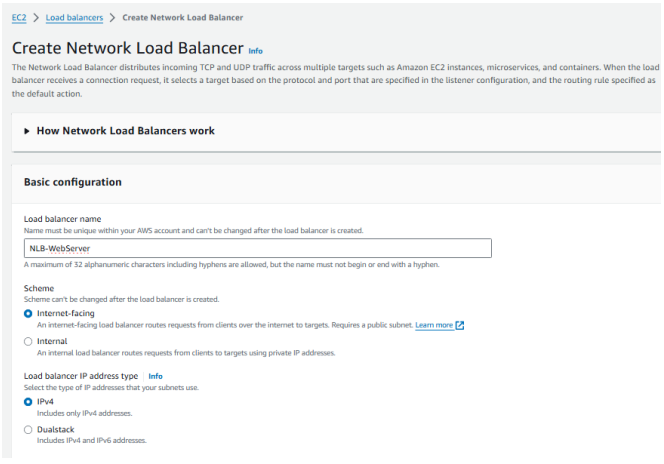
- **Deploy 2 EC2 Instances (Ubuntu) i.e., Web-Server-1 & Web-Server-2**
- **Install Apache2 in both the system and start Apache2**
- **Access the Webservers using its respective URL's i.e., (http://publicipoftheinstance) to confirm the Apache2 installation and working.**
- **Create a Target Group and register the above 2 Machines**
  Note: Make sure to select the TCP protocol and 80 as port during the configuration of the Target Group

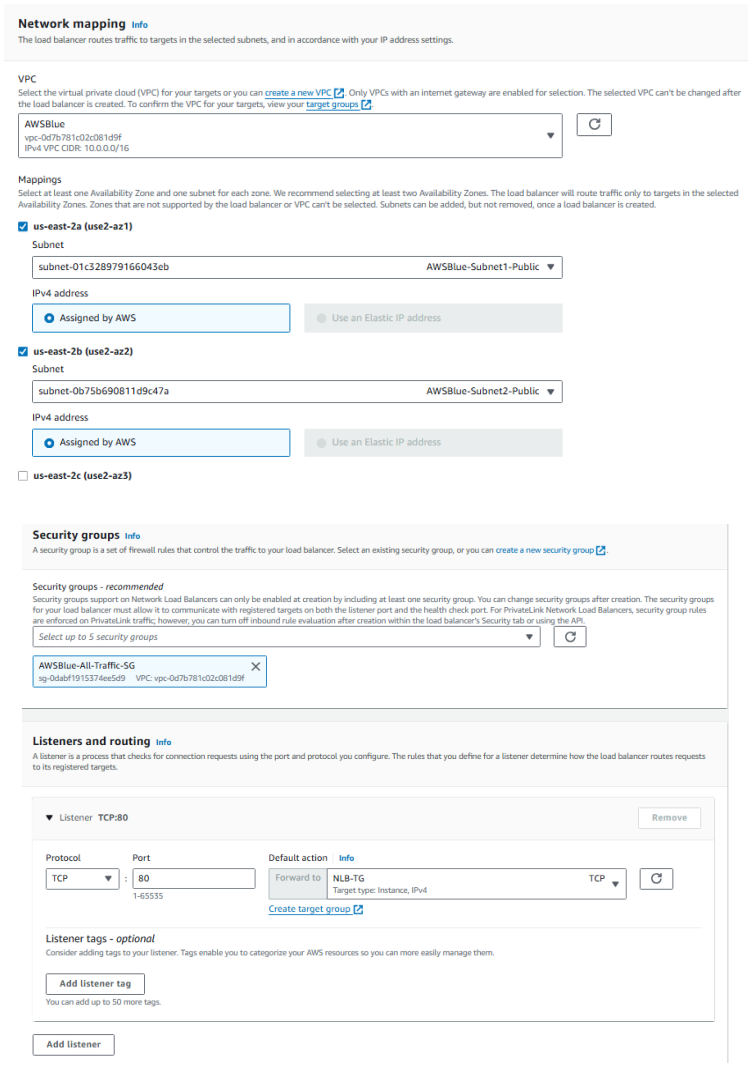
1 - Deploy Network Load Balancer (NLB):

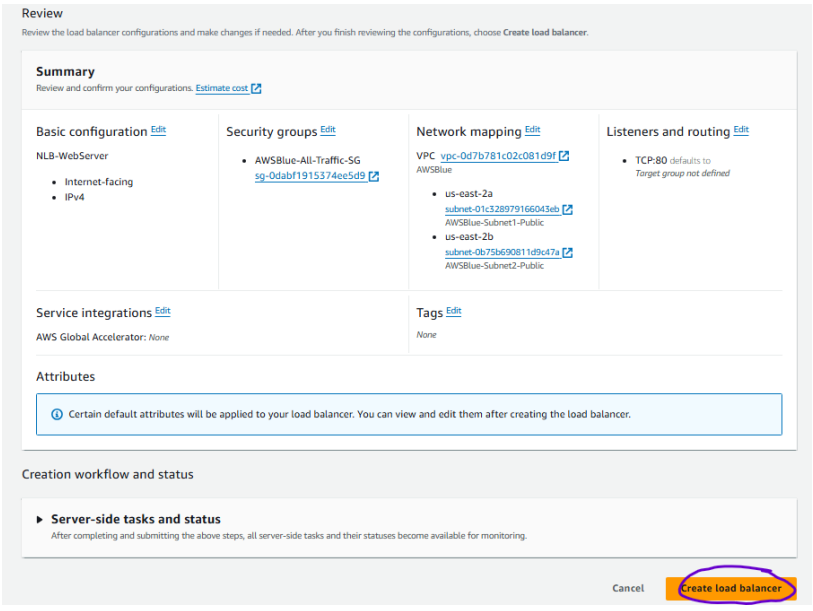
- In the AWS Management Console, go to the EC2 Dashboard.
- Select "Load Balancers" from the sidebar and click on "Create Load Balancer".
- Choose "Network Load Balancer".
- Set the "Name" for your NLB.
- For "Scheme", select "Internet-facing" if you want the NLB to be accessible from the internet.
- Choose the appropriate "IP address type" (IPv4 or Dualstack).
- By default, a TCP listener on port 80 is created. You can add other listeners if needed.
- Select the VPC and subnets (ensure at least two subnets in different availability zones are selected).
- Choose the security group created earlier that allows HTTP (port 80) and SSH (port 22) access.
- Under "Default action", choose "Forward to" and select the target group created earlier (`web-servers-target-group`).
- Ensure the correct targets (`Web-Server-1` and `Web-Server-2`) are registered.
- Click "Create load balancer".

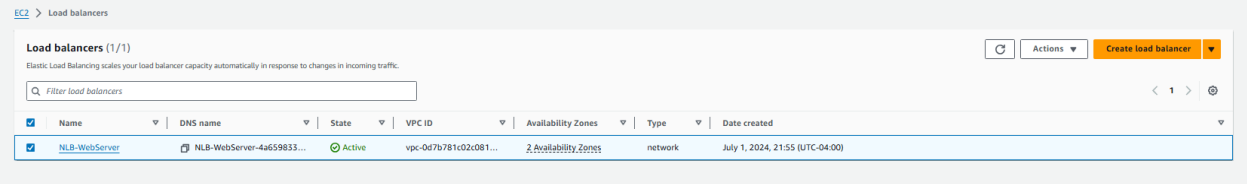






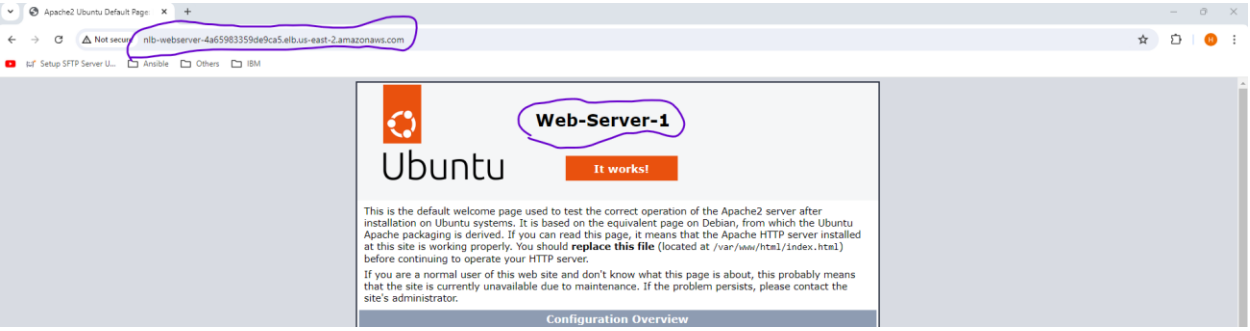

Network mapping Info
The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.
VPC
Select the virtual private cloud (VPC) for your targets or you can create a new VPC. Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your target groups.
AWSBlue
vpc-0d7b781c02c081d9f
IPv4 VPC CIDR: 10.0.0.0/16
Mappings
Select at least one Availability Zone and one subnet for each zone. We recommend selecting at least two Availability Zones. The load balancer will route traffic only to targets in the selected Availability Zones. Zones that are not supported by the load balancer or VPC can't be selected. Subnets can be added, but not removed, once a load balancer is created.
us-east-2a (use2-az1)
Subnet
subnet-01c328979166043eb
AWSBlue-Subnet1-Public
IPv4 address
Assigned by AWS
Use an Elastic IP address
us-east-2b (use2-az2)
Subnet
subnet-0b75b690811d9c47a
AWSBlue-Subnet2-Public
IPv4 address
Assigned by AWS
Use an Elastic IP address
us-east-2c (use2-az3)
Security groups Info
A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group.
Security groups - recommended
Security groups support on Network Load Balancers can only be enabled at creation by including at least one security group. You can change security groups after creation. The security groups for your load balancer must allow it to communicate with registered targets on both the listener port and the health check port. For PrivateLink Network Load Balancers, security group rules are enforced on PrivateLink traffic; however, you can turn off inbound rule evaluation after creation within the load balancer's Security tab or using the API.
Select up to 5 security groups
AWSBlue-All-Traffic-SG
sg-0dabf1915374ee5d9 VPC: vpc-0d7b781c02c081d9f
Listeners and routing Info
A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.
Listener TCP:80
Remove
Protocol
TCP
Port
80
1-65535
Default action Info
Forward to
NLB-TG
TCP
Target type: Instance, IPv4
Create target group
Listener tags - optional
Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.
Add listener tag
You can add up to 50 more tags.
Add listener


Review
Review the load balancer configurations and make changes if needed. After you finish reviewing the configurations, choose Create load balancer.
Summary
Review and confirm your configurations. Estimate cost
Basic configuration Edit
NLB-WebServer
Internet-facing
IPv4
Security groups Edit
AWSBlue-All-Traffic-SG
sg-0dabf1915374ee5d9
Network mapping Edit
VPC vpc-0d7b781c02c081d9f
AWSBlue
us-east-2a
subnet-01c328979166043eb
AWSBlue-Subnet1-Public
us-east-2b
subnet-0b75b690811d9c47a
AWSBlue-Subnet2-Public
Listeners and routing Edit
TCP:80 defaults to
Target group not defined
Service integrations Edit
AWS Global Accelerator: None
Tags Edit
None
Attributes
Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.
Creation workflow and status
Server-side tasks and status
After completing and submitting the above steps, all server-side tasks and their statuses become available for monitoring.
Cancel
Create load balancer



2 - Access Verification Through NLB:

- Once the NLB is created, find the DNS name of the NLB in the Load Balancers section.
- Open a web browser and enter the NLB DNS name.
- Refresh the page multiple times to see if the content switches between Web-Server-1 and Web-Server-2.

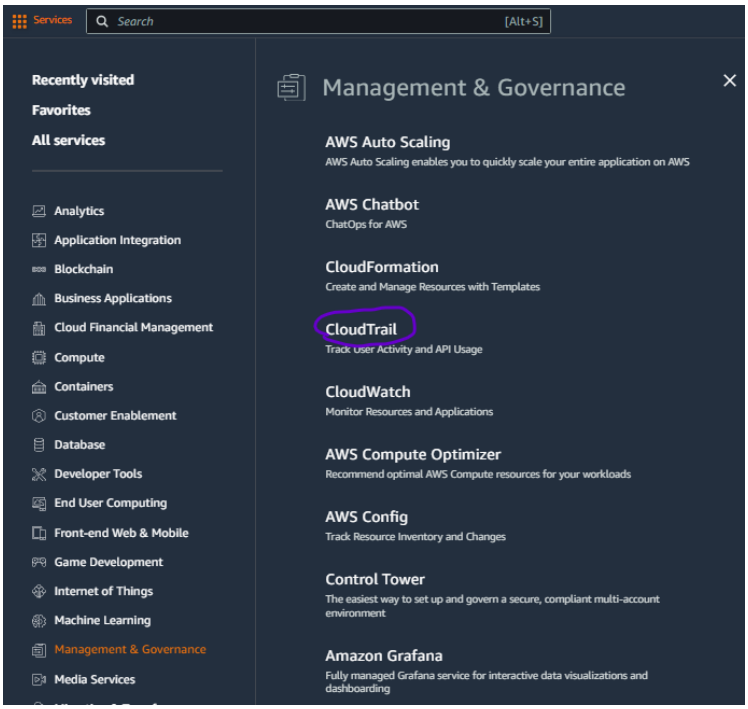


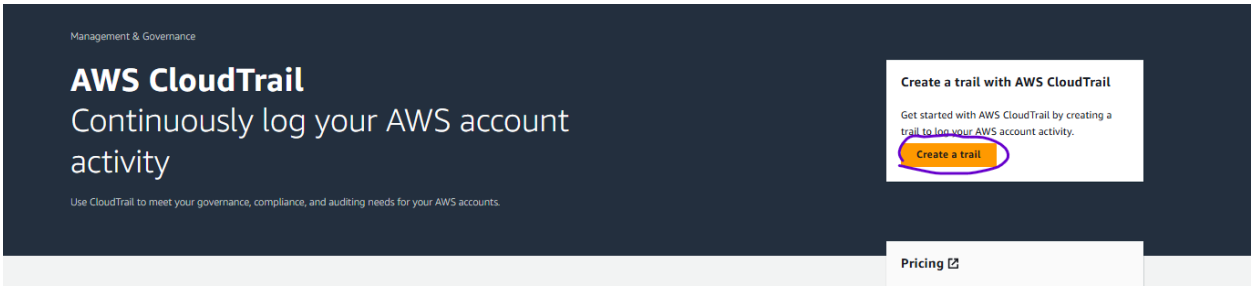
Note: An AWS Network Load Balancer (NLB) distributes incoming network traffic across multiple EC2 instances, ensuring high performance and low latency. It operates at Layer 4 (transport layer) of the OSI model, handling millions of requests per second. NLB supports static IP addresses and performs health checks to route traffic only to healthy instances.

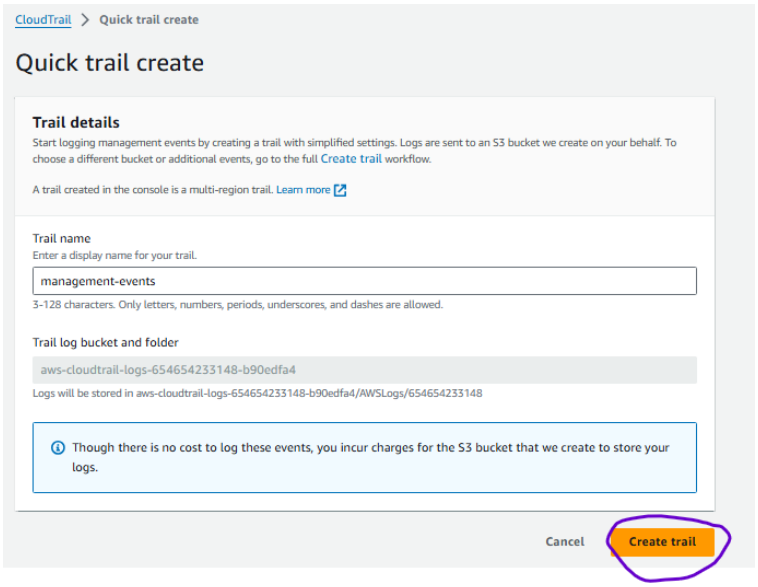
Note: The demonstration for ALB and NLB involved HTTP only, but in real-world scenarios, it is essential to purchase an SSL certificate and configure HTTPS for secure communication. For accessing the web servers, we used public IP addresses or the default AWS-provided domain/URL. In a real-world setup, a custom domain purchased from services like GoDaddy would be added in Route 53 and configured to point to the load balancer.

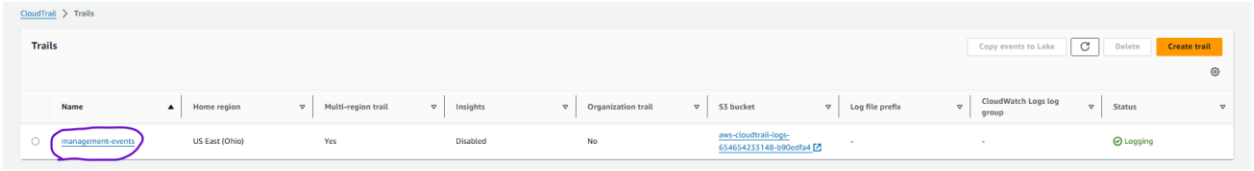
1 - Creating a CloudTrai

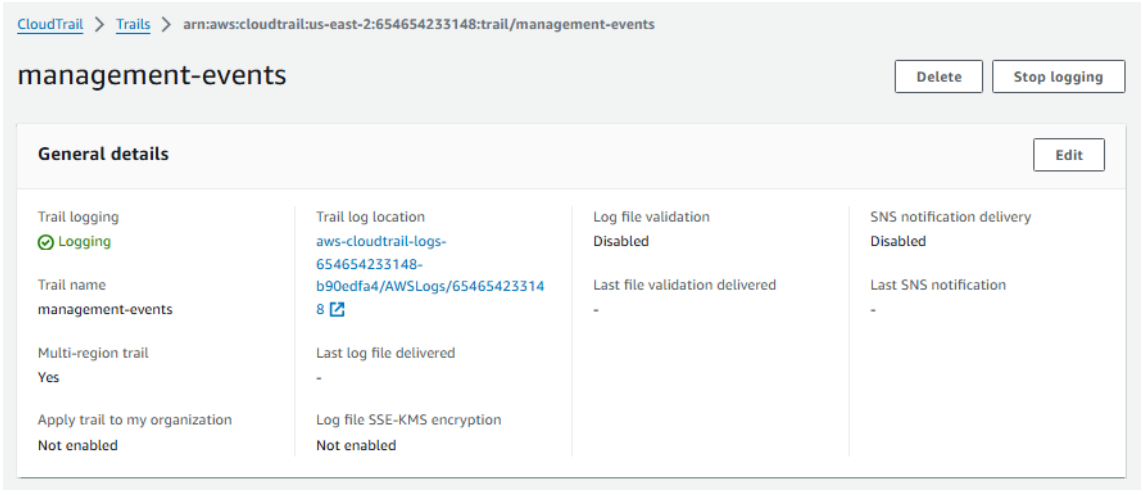
- In the console, navigate to the CloudTrail service.
- Click on Trails in the left navigation pane.
- **Trail name:** Enter a name for your trail (e.g., management-api-trails).
- Click on the Create trail button.
- Review your settings and click on Create trail.
- After the Creation, click on the Created trail and verify the below settings.
- **Apply trail to all regions:** Check this box to enable logging for all regions.
- **Management events:** Enable to read and write management events. These include API calls made by AWS services.
- **Data events:** Choose whether to log S3 and Lambda data events. These are high-volume events and may incur additional costs.
- **Specify an S3 Bucket:**
  Create a new S3 bucket: If you want CloudTrail to create a new bucket, enter a unique bucket name.
  Specify an existing bucket: If you have an existing bucket, provide its name.
- **Log file SSE-KMS encryption**: Enable this if you want to encrypt your log files using AWS KMS.
- **Log file prefix:** Specify an optional prefix for your log files.
- **SNS notification:** If you want to receive notifications, create or specify an SNS topic.
- **CloudWatch Logs:** Configure CloudTrail to send logs to CloudWatch Logs for real-time monitoring.









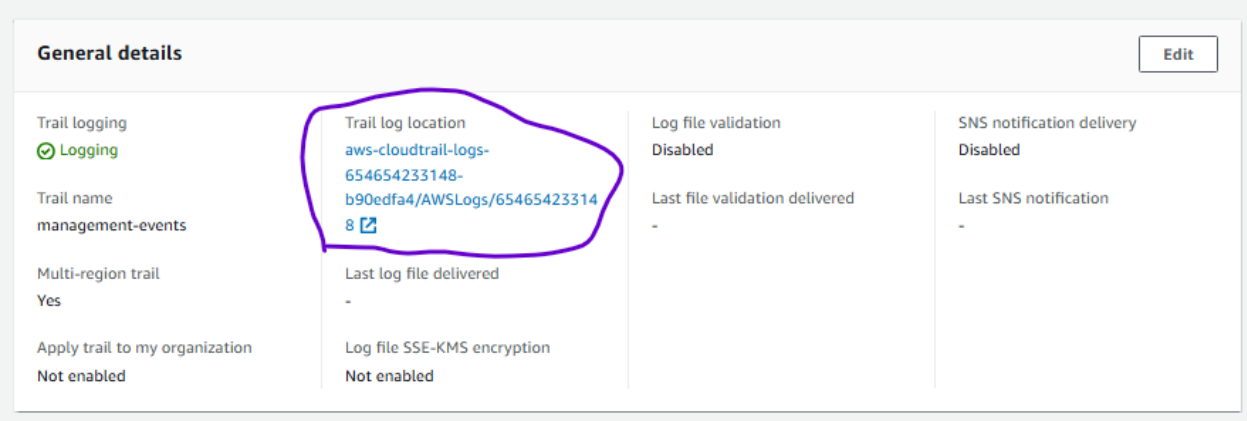


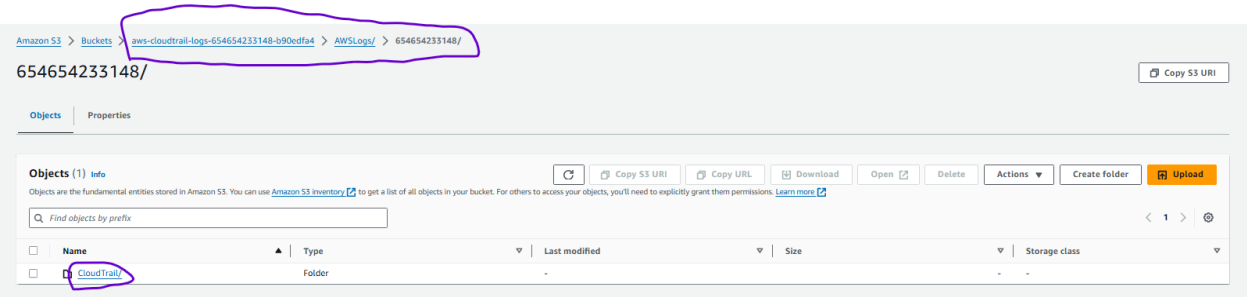
Note: We are not updating any settings in this guide as the goal is to verify the functionality of the CloudTrail logs. If needed, you can customize the settings based on the information provided above.

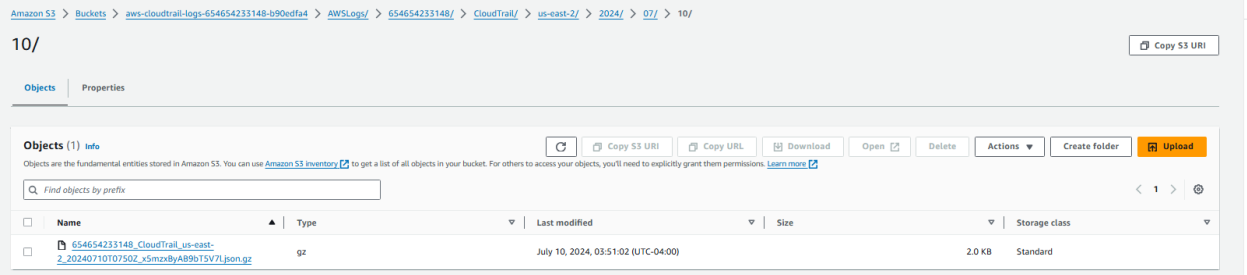
2 - Verify the Logs

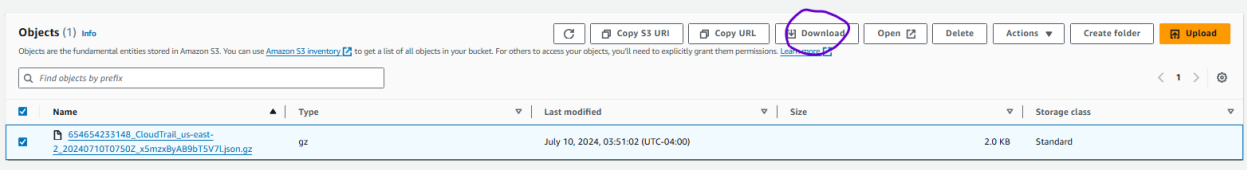
Note: It may take a few minutes for CloudTrail to start logging events and delivering log files to your S3 bucket.

- Navigate to the S3 console and open the bucket specified during trail creation.
- Browse the folder structure to find the log files (the structure typically includes AWS account ID, trail name, region, date, etc.).
- Download one of the log files (JSON format) to your local machine.
- Open the file using a text editor or JSON viewer to inspect the logged events.
- Ensure the log file contains recent events. Look for specific actions performed in your AWS account, such as API calls, changes to resources, etc.









Note:

When you add CloudWatch to CloudTrail, you will have the feasibility to create CloudWatch metrics and alarms based on specific log events to get notifications or automate responses.

Event History: In the CloudTrail console, you can also use the Event history feature to search and view a history of events without accessing the S3 logs directly.

Filter and Search Logs: Use the filtering options in CloudTrail Event history or CloudWatch Logs to search for specific events based on time range, event name, AWS service, etc.

AWS Athena: For advanced querying, you can use AWS Athena to run SQL queries on your CloudTrail logs stored in S3. This requires setting up a table schema for the CloudTrail logs.