

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](#).

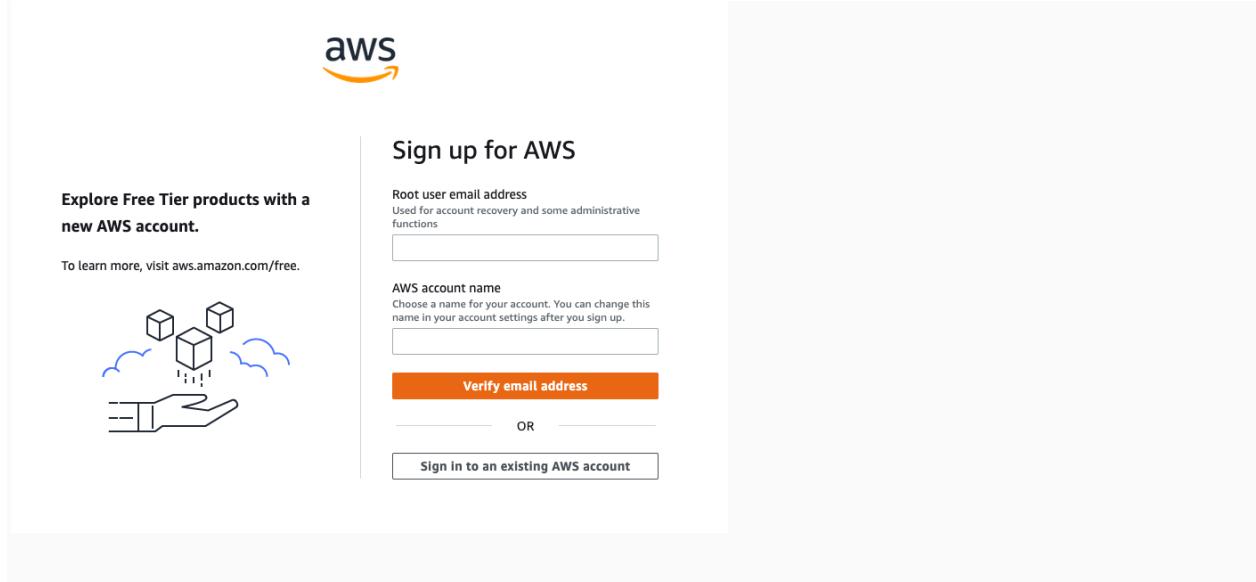
1 - Enter an email address and an account name.

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.



aws

Sign up for AWS

Explore Free Tier products with a new AWS account.
To learn more, visit [aws.amazon.com/free.](https://aws.amazon.com/free/)



Root user email address
Used for account recovery and some administrative functions

AWS account name
Choose a name for your account. You can change this name in your account settings after you sign up.

Verify email address

OR

Sign in to an existing AWS account

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).

The screenshot shows the AWS sign-up process. At the top, there's a banner with the text "Explore Free Tier products with a new AWS account." Below it, a message says "To learn more, visit aws.amazon.com/free". To the left, there's a small icon of a hand holding three cubes. The main form area has a title "Sign up for AWS" and a section "Create your password". A green box at the top right of the password field contains the message "It's you! Your email address has been successfully verified." Below this, instructions say "Your password provides you with sign in access to AWS, so it's important we get it right." There are two input fields for "Root user password" and "Confirm root user password". A large orange button labeled "Continue (step 1 of 5)" is centered below the password fields. Below the button, a horizontal line with the word "OR" and a link "Sign in to an existing AWS account" are shown.

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.

aws

Sign up for AWS

Secure verification

We will not charge you for usage below AWS Free Tier limits. We may temporarily hold up to \$1 USD (or an equivalent amount in local currency) as a pending transaction for 3-5 days to verify your identity.



Billing Information

Credit or Debit card number

VISA MASTERCARD AMEX DISCOVER

AWS accepts all major credit and debit cards. To learn more about payment options, review our [FAQ](#).

Expiration date

Cardholder's name

Billing address

Use my contact address

Use a new address

Verify and Continue (step 3 of 5)

You might be redirected to your bank's website to authorize the verification charge.

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.

aws

Sign up for AWS

Confirm your identity



Before you can use your AWS account, you must verify your phone number. When you continue, the AWS automated system will contact you with a verification code.

How should we send you the verification code?

Text message (SMS)

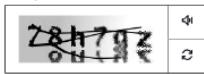
Voice call

Country or region code

 United States (+1)

Mobile phone number

Security check



Type the characters as shown above

Send SMS (step 4 of 5)

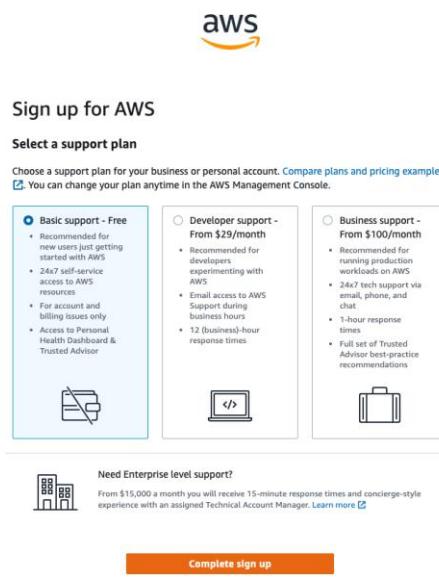
8 - Choose a support plan for your AWS account.

- 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](#).

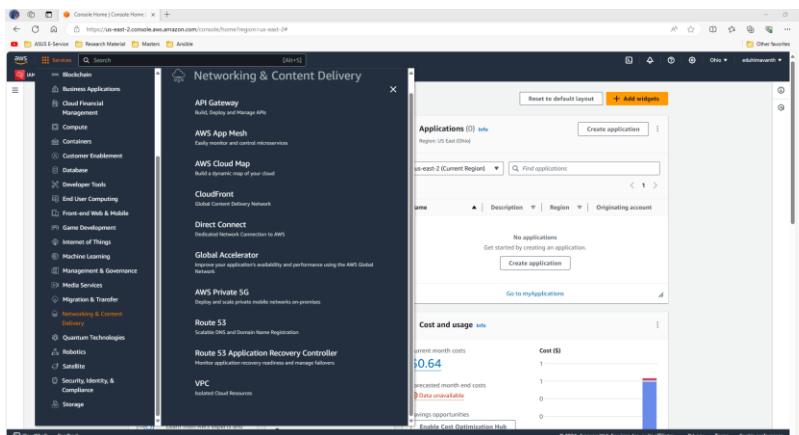
- To finish creating your account, choose Complete sign up.



Creating a Virtual Private Cloud (VPC):

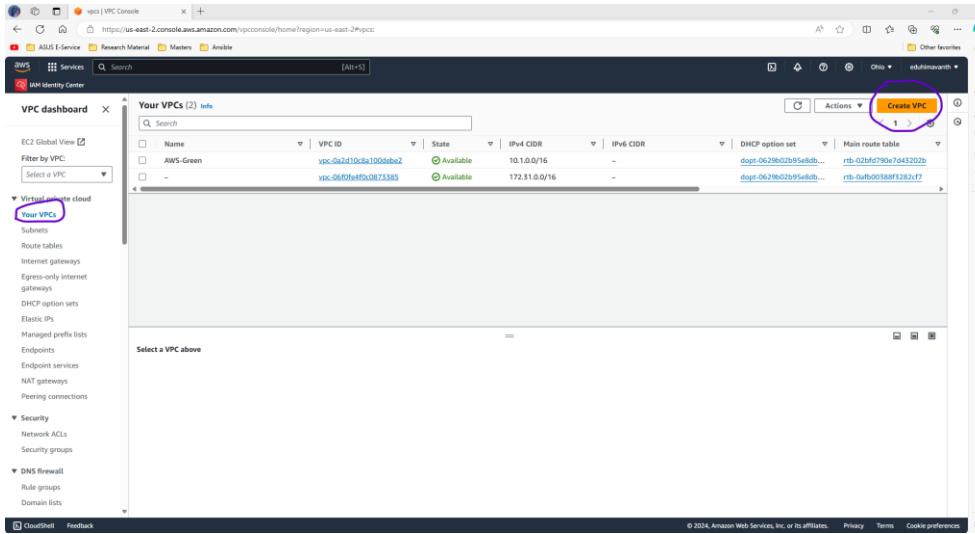
1 - Navigate to the VPC Dashboard

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



2 - Create a VPC

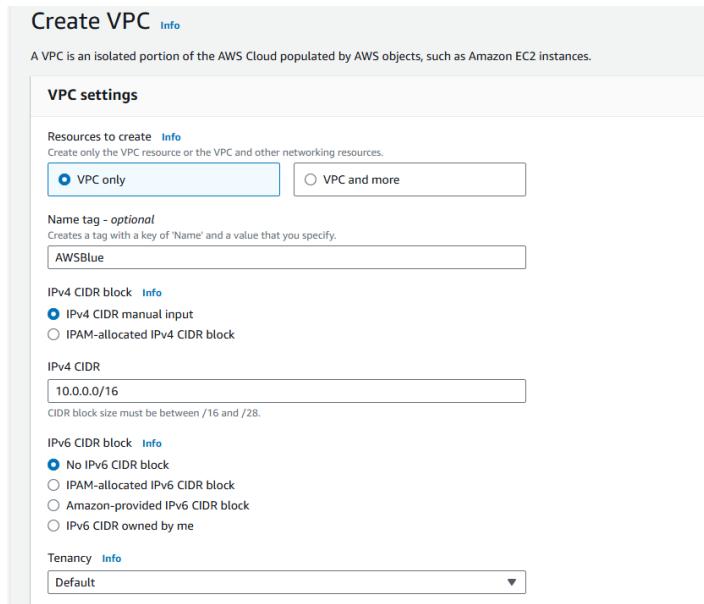
- In the VPC Dashboard, click on "Your VPCs" in the left-hand navigation pane.
- Click on the "Create VPC" button.



The screenshot shows the AWS VPC Dashboard. On the left, there's a navigation sidebar with various options like EC2 Global View, Filter by VPC, Subnets, Route tables, Internet gateways, Egress-only internet gateways, DHCP option sets, Elastic IPs, Managed profile lists, Endpoints, Endpoint services, NAT gateways, Peering connections, Security (Network ACLs, Security groups), DNS firewall, Rule groups, and Domain lists. The main area is titled 'Your VPCs (2) Info' and lists two existing VPCs: 'AWS-Green' and another unnamed one. At the top right of this list, there's a blue 'Create VPC' button with a red circle around it. Below the list, there's a message 'Select a VPC above'.

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".



The screenshot shows the 'Create VPC' configuration page. The 'VPC settings' section is expanded. Under 'Resources to create', the 'VPC only' radio button is selected. Under 'Name tag - optional', the value 'AWSBlue' is entered. Under 'IPv4 CIDR block', the value '10.0.0.0/16' is entered. Under 'IPv6 CIDR block', the 'No IPv6 CIDR block' radio button is selected. Under 'Tenancy', the 'Default' dropdown is set to 'Default'.

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."

The screenshot shows the AWS VPC dashboard. On the left, there's a navigation pane with 'Your VPCs (1/3)'. It lists three VPCs: 'AWS-Green' (vpc-0a2d10c8a100debe2), an unnamed VPC (vpc-06f0fe4ff0c0873385), and 'AWSBlue' (vpc-0d7b781c02c081d9f). The 'AWSBlue' VPC is selected. On the right, the 'Actions' menu is open, displaying various options such as 'Create default VPC', 'Create flow log', 'Edit VPC settings', 'Edit CIDRs', 'Manage middlebox routes', 'Manage tags', and 'Delete VPC'.

The screenshot shows the 'Edit VPC' dialog box. It has four main sections: 'VPC details' (VPC ID: vpc-0d7b781c02c081d9f, Name: AWSBlue), 'DHCP settings' (DHCP option set: dopt-0629b02b95e8db0fa), 'DNS settings' (checkboxes: 'Enable DNS resolution' and 'Enable DNS hostnames' are both checked and highlighted with a purple oval), and 'Network Address Usage metrics settings' (checkbox: 'Enable Network Address Usage metrics' is unchecked). At the bottom are 'Cancel' and 'Save' buttons.

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."

Screenshots illustrating the creation of a new subnet in the AWS VPC console:

Step 1: Subnets List

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone	Availability Zone ID
subnet-0c4cf9565702fa497	Available	vpc-06f0fe4f0c0873385	172.31.0.0/20	-	-	4091	us-east-2a	use2-a2t
subnet-0b5b0a6f2b1a308a2	Available	vpc-0a2d10c8a100debe2 AWS...	10.1.3.0/24	-	-	251	us-east-2c	use2-a2z
subnet-0e2f3bfe7d9476cf	Available	vpc-0a2d10c8a100debe2 AWS...	10.1.2.0/24	-	-	251	us-east-2b	use2-a2z
subnet-00e250e76b1250da	Available	vpc-06f0fe4f0c0873385	172.31.16.0/20	-	-	4091	us-east-2a	use2-a2t
subnet-0914735408e5facb8	Available	vpc-0a2d10c8a100debe2 AWS...	10.1.1.0/24	-	-	251	us-east-2a	use2-a2t
subnet-00145051226e2dd	Available	vpc-06f0fe4f0c0873385	172.31.32.0/20	-	-	4091	us-east-2c	use2-a2z

Step 2: Create Subnet Form

Step 3: Success Message

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone	Availability Zone ID
subnet-01328979166043eb	Available	vpc-06f0fe4f0c0873385	172.31.0.0/20	-	-	4091	us-east-2a	use2-a2t
subnet-0b5b0a6f2b1a308a2	Available	vpc-0a2d10c8a100debe2 AWS...	10.1.3.0/24	-	-	251	us-east-2c	use2-a2z
subnet-0e2f3bfe7d9476cf	Available	vpc-0a2d10c8a100debe2 AWS...	10.1.2.0/24	-	-	251	us-east-2b	use2-a2z
subnet-00e250e76b1250da	Available	vpc-06f0fe4f0c0873385	172.31.16.0/20	-	-	4091	us-east-2a	use2-a2t
subnet-0914735408e5facb8	Available	vpc-0a2d10c8a100debe2 AWS...	10.1.1.0/24	-	-	251	us-east-2a	use2-a2t
subnet-00145051226e2dd	Available	vpc-06f0fe4f0c0873385	172.31.32.0/20	-	-	4091	us-east-2c	use2-a2z
AWSBlue-Subnet1-Public	Available	vpc-007b781c02c081d9f AWS...	10.0.1.0/24	-	-	251	us-east-2a	use2-a2t

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."

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone	Availability Zone ID
subnet-0c40f565702fa497	subnet-0b00aef2b1a308a2	Available	vpc-06f0fe4fc0873385	172.31.0.0/20	-	4091	us-east-2a	use2-az1
AWS-Green-Subnet3	subnet-0b00aef2b1a308a2	Available	vpc-0a2ef0ba100debc2 AWS...	10.1.3.0/24	-	251	us-east-2c	use2-az3
AWS-Green-Subnet2	subnet-0e2f0bf7d98476f	Available	vpc-0a2ef0ba100debc2 AWS...	10.1.2.0/24	-	251	us-east-2b	use2-az2
-	subnet-00a250b761250de	Available	vpc-06f0fe4fc0873385	172.31.16.0/20	-	4091	us-east-2a	use2-az2
AWS-Green-Subnet1	subnet-09147140beefac88	Available	vpc-0a2ef0ba100debc2 AWS...	10.1.1.0/24	-	251	us-east-2a	use2-az1
-	subnet-01a4506512262d0	Available	vpc-06f0fe4fc0873385	172.31.32.0/20	-	4091	us-east-2c	use2-az3
AWSBlue-Subnet1-Public	subnet-01328979166043cb	Available	vpc-0d7b781c02081ef1 AWS...	10.0.1.0/24	-	251	us-east-2a	use2-az1
AWSBlue-Subnet2-Public	subnet-0b7bd90811dfc47a	Available	vpc-0d7b781c02081ef1 AWS...	10.0.2.0/24	-	251	us-east-2b	use2-az2

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."

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone	Availability Zone ID
subnet-0c40f565702fa497	subnet-0b00aef2b1a308a2	Available	vpc-06f0fe4fc0873385	172.31.0.0/20	-	4091	us-east-2a	use2-az1
AWS-Green-Subnet3	subnet-0b00aef2b1a308a2	Available	vpc-0a2ef0ba100debc2 AWS...	10.1.3.0/24	-	251	us-east-2c	use2-az3
AWS-Green-Subnet2	subnet-0e2f0bf7d98476f	Available	vpc-0a2ef0ba100debc2 AWS...	10.1.2.0/24	-	251	us-east-2b	use2-az2
-	subnet-00a250b761250de	Available	vpc-06f0fe4fc0873385	172.31.16.0/20	-	4091	us-east-2a	use2-az2
AWS-Green-Subnet1	subnet-09147140beefac88	Available	vpc-0a2ef0ba100debc2 AWS...	10.1.1.0/24	-	251	us-east-2a	use2-az1
-	subnet-01a4506512262d0	Available	vpc-06f0fe4fc0873385	172.31.32.0/20	-	4091	us-east-2c	use2-az3
AWSBlue-Subnet1-Public	subnet-01328979166043cb	Available	vpc-0d7b781c02081ef1 AWS...	10.0.1.0/24	-	251	us-east-2a	use2-az1
AWSBlue-Subnet2-Public	subnet-0b7bd90811dfc47a	Available	vpc-0d7b781c02081ef1 AWS...	10.0.2.0/24	-	251	us-east-2b	use2-az2
AWSBlue-Subnet3-Private	subnet-05e61c26d1c7f448	Available	vpc-0d7b781c02081ef1 AWS...	10.0.3.0/24	-	251	us-east-2c	use2-az3

You have successfully created 1 subnet: subnet-05e61c26d1c7f448

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

Internet gateways [1] Info

Name	Internet gateway ID	State	VPC ID	Owner
How-06f50d332c95010b2	Attached	vpc-060feef0c0873385	654654233148	

Actions ▾ Create internet gateway

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

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
Q Name X	Q AWSBlue-Internet-Gateway X

Add new tag

You can add 49 more tags.

Cancel **Create internet gateway**

VPC dashboard

Internet gateways [1/2] Info

Name	Internet gateway ID	State	VPC ID	Owner
How-06f50d332c95010b2	Attached	vpc-060feef0c0873385	654654233148	
AWSBlue-Internet-Gateway	How-06f50d332c95010b2	Detached	-	654654233148

Actions ▾ Attach to VPC

View details
Detach from VPC
Manage tags
Delete internet gateway

Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets

VPC > Internet gateways > Attach to VPC (igw-056b4a0a9d3db1c65)

Attach to VPC (igw-056b4a0a9d3db1c65) Info

VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs
Attach the internet gateway to this VPC.

X

▶ AWS Command Line Interface command

Cancel Attach internet gateway

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."

VPC dashboard ×

Route tables (4) Info

Find resources by attribute or tag

Name	Route table ID	Explicit subnet associ...	Main	VPC	Owner ID
-	rtb-02fbff96e7643207b	-	Yes	vpc-0x2fbff96e7643207b AWS...	654654233148
AWS-Green-Route	rtb-05a58ac6b7088057a	3 subnets	No	vpc-0x2fbff96e7643207b AWS...	654654233148
-	rtb-08b215b6931bb077a	-	Yes	vpc-0d7b781c02c081d9f AWS...	654654233148
-	rtb-0afbf0931881282cf7	-	Yes	vpc-0600fe40b0873385	654654233148

Actions Create route table

VPC > Route tables > Create route table

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

VPC
The VPC to use for this route table.

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
<input type="text" value="Name"/>	<input type="text" value="AWSBlue-Route"/> X Remove

Add new tag Cancel Create route table

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.

The screenshot shows the AWS VPC Security Groups page. On the left, there's a navigation sidebar with sections like Security, Network ACLs, Security groups (which is selected and highlighted), and DNS Firewall. The main area displays a table titled 'Security Groups (4) Info' with columns for Name, Security group ID, Security group name, VPC ID, Description, Owner, and Inbound rules count. Four security groups are listed: 'default' (sg-0c10e364597aae70), 'default' (sg-01db796d9cc14eaf0), 'AWS-Green-SG' (sg-00068205cd195100), and 'default' (sg-08a2130636949f58). At the top right of the table, there's a blue 'Create security group' button, which is circled in orange in the screenshot.

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.

The screenshot shows the 'Create security group' wizard. The first step, 'Basic details', is shown. It has three fields: 'Security group name' (set to 'AWSBlue-All-Traffic-SG'), 'Description' (set to 'Allow access to Inbound and Outbound Traffic'), and 'VPC' (set to 'vpc-0d7b781c02c081d9f (AWSBlue)'). Below these fields, there's a note: 'A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.'

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).

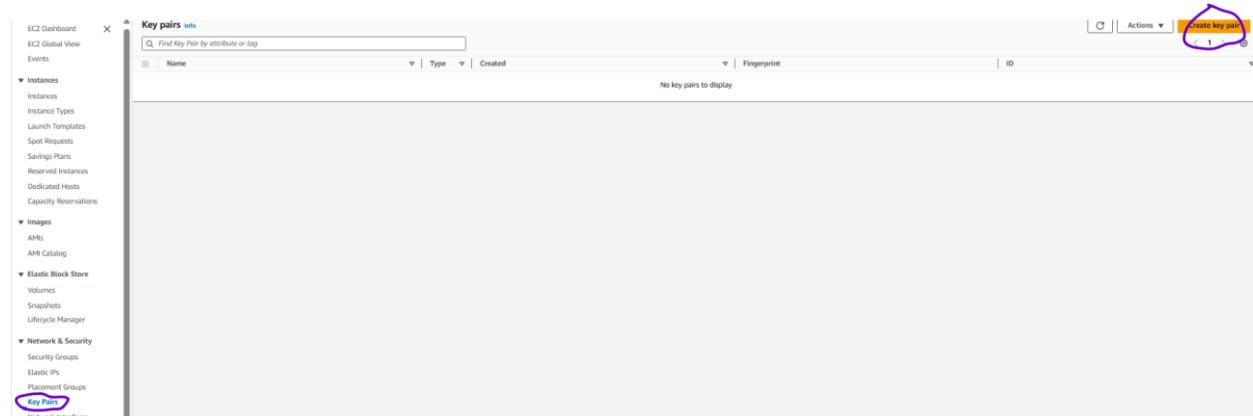
2 - Outbound Rules:

- 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.



Create key pair Info

Key pair
A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type Info RSA ED25519

Private key file format
 .pem For use with OpenSSH
 .ppk For use with PuTTY

Tags - optional
No tags associated with the resource.
[Add new tag](#)
You can add up to 50 more tags.

[Cancel](#) **Create key pair**

Successfully created key pair

Key pairs (1) <small>Info</small>					
<input type="text"/> Find Key Pair by attribute or tag					
Name	Type	Created	Fingerprint	ID	Actions
AWSBlue-Key	rsa	2024/06/04 11:52 GMT-4	b4:00:ff:8a:78:14:a6:6f:b6:72:5a:be:71:27:34:6c:9cf1:dc:4e	key-079e71e6a572b9f74	Actions Create

See more

Downloads [AWSBlue-Key.pem](#) [Open file](#)

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.

Identity and Access Management (IAM)			
IAM > Roles			
Roles (6) Info			
			Create role
<input type="checkbox"/> Role name	▲ Trusted entities	Last activity	
<input type="checkbox"/> AWSReservedSSO_AWS-Green-PermissionSet_3fb13cf4247a9328	Identity Provider: armawsiam:6546	7 days ago	
<input type="checkbox"/> AWSServiceRoleForAmazonSSM	AWS Service: ssm (Service-Linked Ro	2 hours ago	
<input type="checkbox"/> AWSServiceRoleForOrganizations	AWS Service: organizations (Service-	-	
<input type="checkbox"/> AWSServiceRoleForSSO	AWS Service: sso (Service-Linked Ro	3 hours ago	
<input type="checkbox"/> AWSServiceRoleForSupport	AWS Service: support (Service-Linker	-	

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.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2

Choose a use case for the specified service.

Use case

EC2

IAM > Roles > Create role

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

Add permissions [Info](#)

Permissions policies (2/926) [Info](#)

Choose one or more policies to attach to your new role.

Filter by Type: All types | 20 matches

Policy name	Type	Description
AmazonEC2RoleforSSM	AWS managed	This policy will soon be deprecated. Pl...
AmazonSSMAutomationApproveAccess	AWS managed	Provides access to view automation ex...
AmazonSSMAutomationRule	AWS managed	Provides permissions for EC2 Automati...
AmazonSSMDirectoryServiceAccess	AWS managed	This policy allows SSM Agent to access...
AmazonSSMFullAccess	AWS managed	Provides full access to Amazon SSM.
AmazonSSMMaintenanceWindowRole	AWS managed	Service Role to be used for EC2 Mainte...
AmazonSSMManagedEC2InstanceDefaultPolicy	AWS managed	This policy enables AWS Systems Man...
AmazonSSMManagedInstanceCore	AWS managed	The policy for Amazon EC2 Role to en...

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

AWSBlue-AD-Role

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: +-=_,@-,_.

Role AWSBlue-AD-Role created.			
View role X			
IAM > Roles			
Roles (7) 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.			
<input type="checkbox"/> Search			
<input type="checkbox"/> Role name ▲ Trusted entities Last activity			
<input type="checkbox"/> AWSBlue-AD-Role AWS Service: ec2 -			

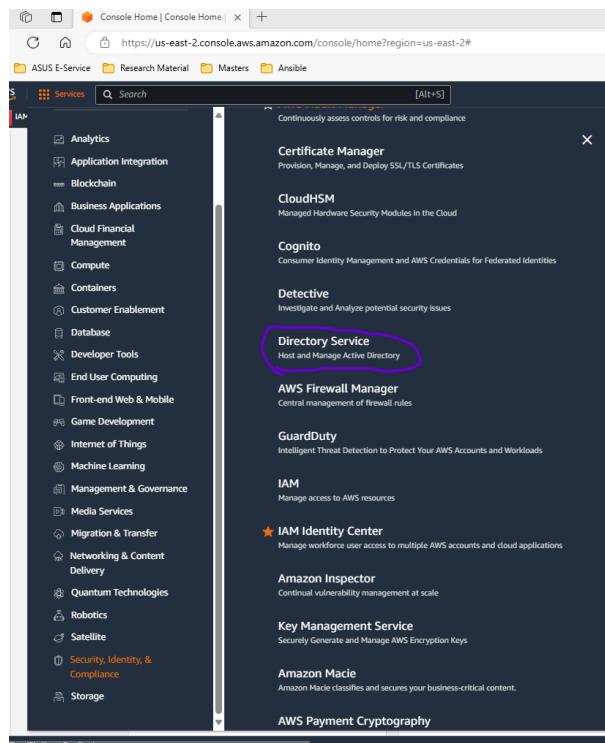
Creating Active Directory:

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):

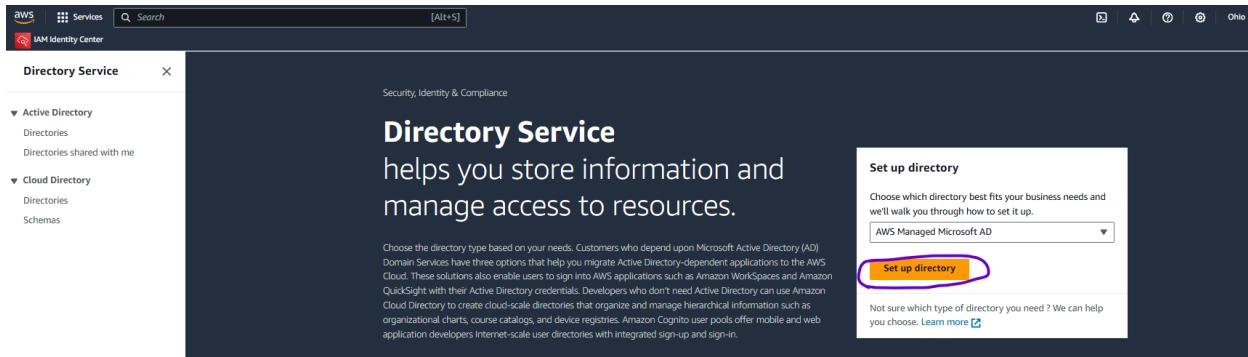
1 - Navigate to the Directory Service

- 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.

Directory Service > Directories > Set up a directory

Step 1 Select directory type

Step 2 Enter directory information

Step 3 Choose VPC and subnets

Step 4 Review & create

Choose VPC and subnets Info

Networking
The VPC that contains your directory. If you do not have a VPC with at least two subnets, you must create one.

VPC Info
AWSBlue | vpc-0d7b781c02c081d9f (10.0.0.0/16)

Subnets Info
AWSBlue-Subnet1-Public | subnet-01c328979166043eb (10.0.1.0/24, us-east-2a)
AWSBlue-Subnet2-Public | subnet-0b75b690811d9c47a (10.0.2.0/24, us-east-2b)

Initial AD site name for this directory Info
Default-First-Site-Name

5 - Review and Create

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

Directory Service > Directories > Set up a directory

Step 1 Select directory type

Step 2 Enter directory information

Step 3 Choose VPC and subnets

Step 4 Review & create

Review & create Info

Review

Directory type	Microsoft AD	VPC
Operating system version	Windows Server 2019	AWSBlue vpc-0d7b781c02c081d9f (10.0.0.0/16)
Directory DNS name	AWSBlue.com	Subnets
Directory NetBIOS name	AWSBlue	AWSBlue-Subnet1-Public subnet-01c328979166043eb (10.0.1.0/24, us-east-2a) AWSBlue-Subnet2-Public subnet-0b75b690811d9c47a (10.0.2.0/24, us-east-2b)
Directory description	-	

Pricing

Edition	Standard	Free trial eligible <small>Learn more</small>
Domain controllers charge		30-day limited trial
~USD 86.4000/mo (USD 0.1200/hr)*		
* Includes two domain controllers, USD 43.2000/mo for each additional domain controller.		

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."

Directory Service

Your directory AWSBlue.com (d-9a67747805) is being created! This can take up to 20-45 minutes.

Directories (1) Info

Directory ID	Directory name	Type	Size	Multi-Region	Status	Launch date
d-9a67747805	AWSBlue.com	Microsoft AD	Standard	Not applicable	<small>Creating</small>	Jun 4, 2024

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)

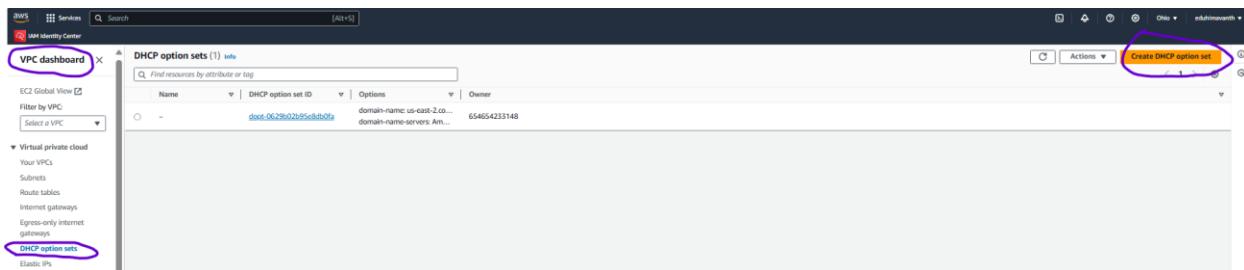
Note: Since we have allowed all traffic for both inbound and outbound connections, security group rules are no longer a concern.

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

NTP servers
172.16.16.16, 10.10.10.10, 75::ff9b::20, 75::ff9b::50

NetBIOS name servers
192.168.0.4, 198.168.0.5

NetBIOS node type
Choose a node type

IPv6 preferred lease time
100000
Seconds

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
<input type="text" value="Name"/> Name	<input type="text" value="AWSBlue-DHCP"/> AWSBlue-DHCP

Add tag
You can add 49 more tags

Cancel **Create DHCP option set**

VPC dashboard

Your VPCs (1/3) Info

EC2 Global View Actions Create VPC

Filter by VPC Select a VPC

Virtual private cloud

Virtual private cloud

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table	Main network ACL	Tenancy	Default VPC	Owner ID
AWS-Green	vpc-0x2f108a100bba2	Available	10.1.0.0/16	-	dopt-0229020105ebfb...	rb-03f4790c74d12022	pol-000707a242fb4f07	Default	No	654654233148
AWSBlue	vpc-0d7b781c02c081d9f	Available	10.0.0.0/16	-	dopt-0229020105ebfb...	rb-0023580315bd72w	pol-0150701515bd932d7	Default	No	654654233148
-	vpc-0604e080873385	Available	172.31.0.0/16	-	dopt-0229020105ebfb...	rb-0f0503880f1183cf7	pol-02084dca5a8f848	Default	Yes	654654233148

Actions Create default VPC
Create flow log
Edit VPC settings
Edit CIDs
Manage middlebox routes
Manage tags
Delete VPC

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

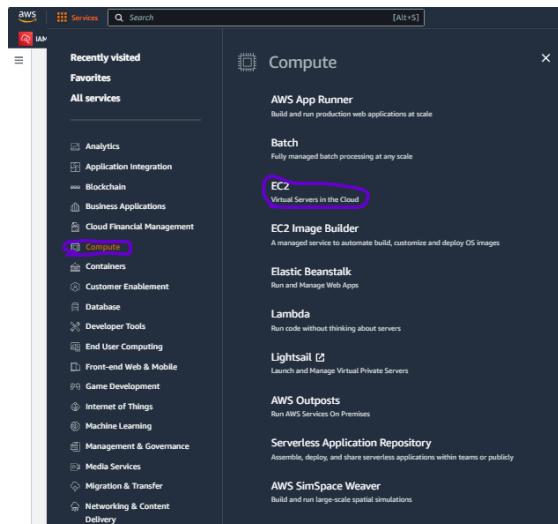
Cancel **Save**

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

The screenshot shows the AWS Directory Service console. At the top, it displays the path: Directory Service > Directories > d-9a67747805. Below this, the directory details are shown, including the directory type (Microsoft AD), edition (Standard), and operating system version (Windows Server 2019). The networking details section shows a VPC (vpc-0f7b78102c081d9f) with two subnets: subnet-01c328979166045eb and subnet-0b75b690811d9c47a. Availability zones listed are us-east-1a and us-east-1b. The DNS address is 10.0.1.255 and 10.0.2.10. The status is Active, last updated on Tuesday, June 4, 2024, and the launch time is also Tuesday, June 4, 2024.

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.



EC2 Dashboard

- EC2 Global View
- Events
- Instances
 - Instances
 - Instance Types
 - Launch Templates
 - Spot Requests
 - Savings Plans
 - Reserved Instances
 - Dedicated Hosts
 - Capacity Reservations

Instances Info

Find instance by attribute or tag (case-sensitive)

All states

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4	Elastic IP	IPv6 IPs	Monitoring	Security group name	Key name	Launch time
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 full catalog including 1000s of application and OS images

Quick Start

Amazon Linux, macOS, Ubuntu, Windows, Red Hat, SUSE, Browse more AMIs

Amazon Machine Image (AMI)

Microsoft Windows Server 2019 Base
ami-036731c5106ad4c65 (64-bit (x86))
Virtualization: hvm ENA enabled: true Root device type: ebs

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

t2.micro

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

Free tier eligible

All generations

Compare instance types

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, 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
VPC: vpc-0d7b781c02c081d9f Owner: 654654233148 Availability Zone: us-east-2a
IP addresses available: 250 CIDR: 10.0.1.0/24

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

AWSBlue-All-Traffic-5G sg-0dabf1915374ee5d9 X
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

Domain join directory

AWSBlue.com d-9a67747805

Create new directory

IAM instance profile

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

Summary

Number of instances | [Info](#)

1

Software Image (AMI)
Microsoft Windows Server 2019 ...[read more](#)
ami-036731c5106ad4c65

Virtual server type (instance type)
t2.medium

Firewall (security group)
[AWSBlue-All-Traffic-SG](#)

Storage (volumes)
1 volume(s) - 30 GiB

Free tier: In your first year includes
750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel **Launch instance** Review commands

Success
Successfully initiated launch of instance i-0edd792200e4e9267

Launch log
Initializing requests: Succeeded
Configuring domain join: Succeeded
Launch initiation: Succeeded
Initiating domain join: Succeeded

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.

Instances (1/1) Info											
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/> All states											
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4	Elastic IP	IPv6 IPs	Actions
<input checked="" type="checkbox"/> AWSBlue-Domain-Server	i-0edd792200e4e9267	Running	t2.medium	2/2 checks passed	View alarms	us-east-2a	ec2-3-21-21-233.us-eas...	3.21.21.233	-	-	Actions Launch Instances

Actions ▾ **Launch Instances** ▾

- Connect
- View details
- Manage instance state
- Instance settings
- Networking
- Security
- Image and templates
- Monitor and troubleshoot

[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

[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

Private key contents - optional

```
--BEGIN RSA PRIVATE KEY--
MIIEogIBAAKCAQEAkfPjnLnLkmwX7gQ1ZTRQzsf5Z26YRngBslrUr80dMcSXD
pdJpcwC/OFvH1TwzntBzq2zqf0W4y098EcIATq5h9xOElN/9B2z5H4Z
146nosnTWCAZ4W1Txb0aa/h5QOq83yAqkKvrlDE2nV0xdppbLS1q+xtYHTfSR
uyQ.LQ2S90ryVnQChf2obLjSyq07xhA2D6Wjg2LTrRagE26JNw4rnV2MhrtjsA
nLbczhlxWhn7965k9bfqjAkyc6742QB86Pgymc2+qvzf73m#GgSYpglKAm5e
DW9tcPHSlCqJMrhSlyfTty4dkOHeypaqqt8anDQAABa0IBAHewp5fHfl7Ag4vv
wm0epk4j4pAIAdy8dJAzTUGCX3tpL5grRa6uJ99E2eyQGHF1dnSJ5uO4bxtxl6
```

[Cancel](#) [Decrypt password](#)

[ASUS E-Service](#) [Research Material](#) [Masters](#) [Ansible](#)

[AWS Identity Center](#)

[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

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

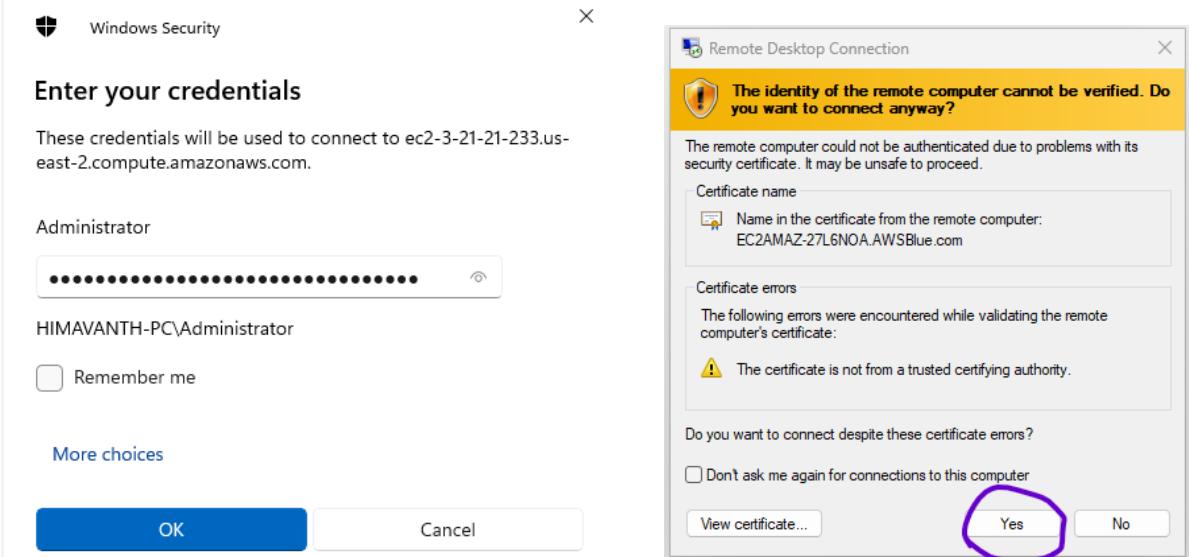
[Cancel](#)

[Downloads](#)

AWSBlue-Domain-Server.rdp

AWSBlue-Key.pem

[See more](#)



4 - Join the Windows Instance to the Domain

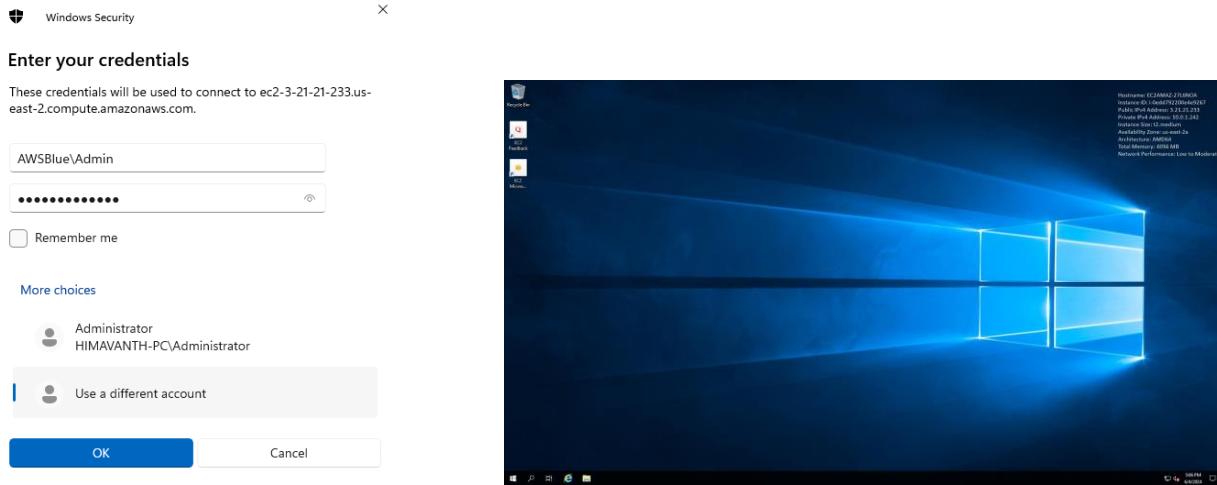
- In the Windows instance, open the "Server Manager."
- Click on "Local Server" in the left pane.

PROPERTIES	
For EC2AMAZ-27L6NOA	
Computer name	EC2AMAZ-27L6NOA AWSBlue.com
Windows Defender Firewall	Domain: On
Remote management	Enabled
Remote Desktop	Enabled
NIC Teaming	Disabled
Ethernet	IPv4 address assigned by DHCP; IPv6-enabled
Operating system version	Microsoft Windows Server 2019 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

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."



Before you begin

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

Select destination server

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

Name	IP Address	Operating System
EC2AMAZ-2T6NOA.AWSSblue.com	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

Select server roles

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
- Active Directory Schema 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
- Performance Management 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 certificates, certificate templates, and related role services that allow you to issue and manage certificates used in a variety of applications.

< Previous | **Next >** | Install | Cancel

Select features

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 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

Select features

Select one or more features to install on the selected server.

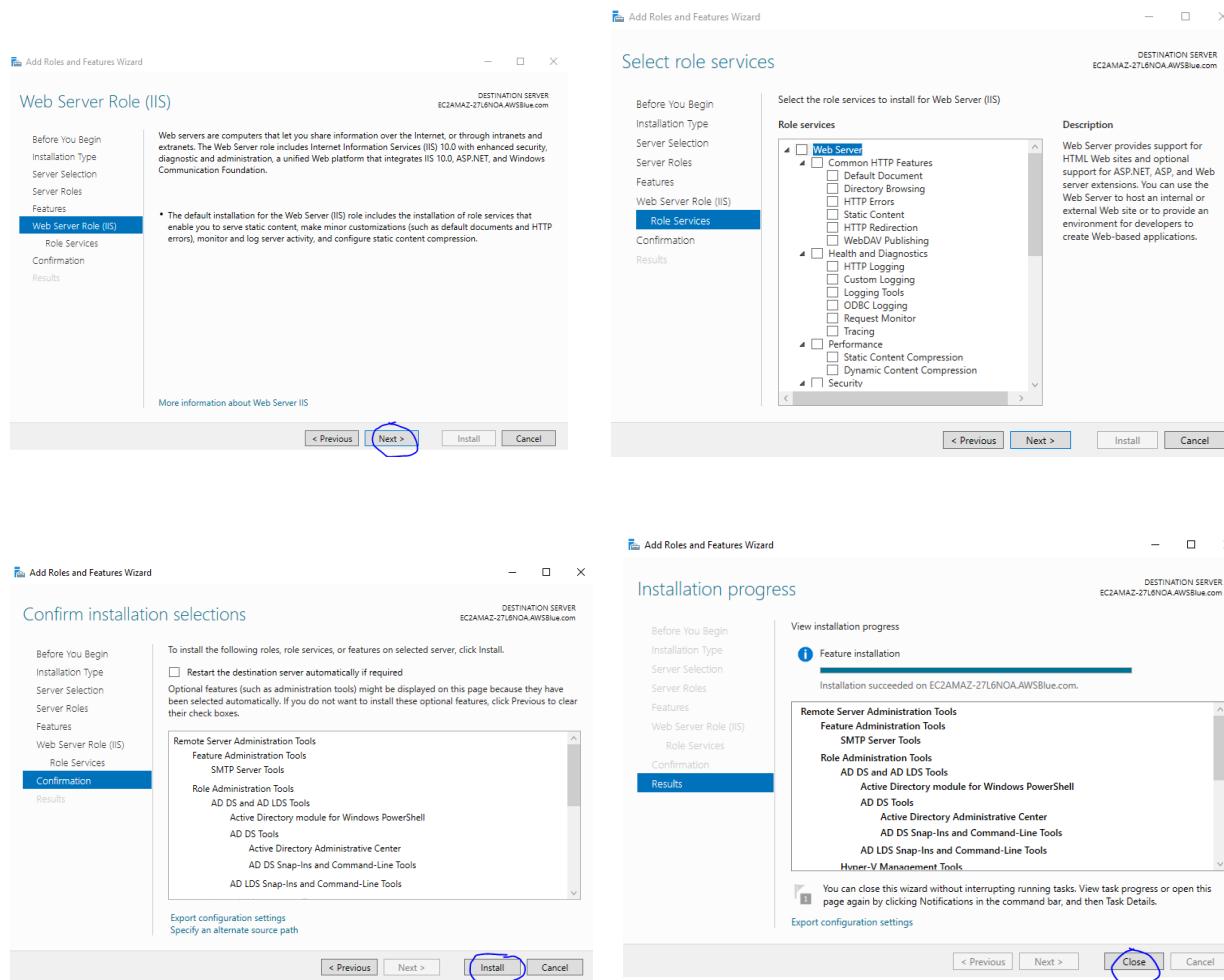
Features

- 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 Limiting
- SNMP Service
- Software Load Balancer
- Storage Migration Service
- Storage Migration Service Proxy
- Storage Replica
- System Data Archiver (Installed)
- System Insights
- Telnet Client

Description

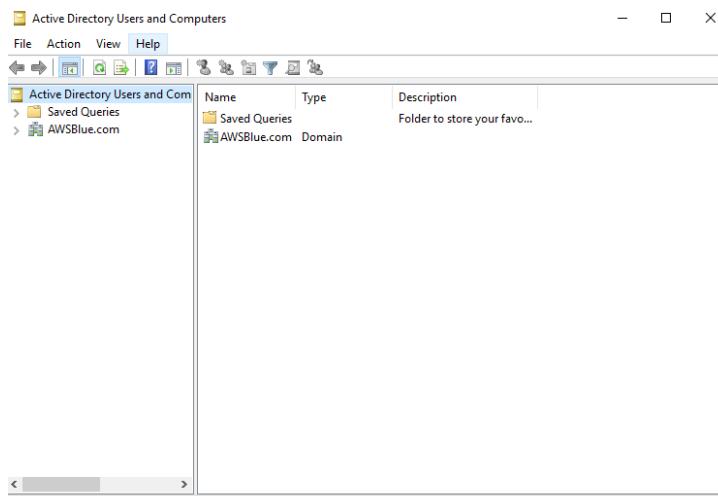
Remote Server Administration Tools includes snap-ins and command-line tools for remotely managing roles and features.

< Previous | **Next >** | Install | Cancel



7 - Open Active Directory Users and Computers

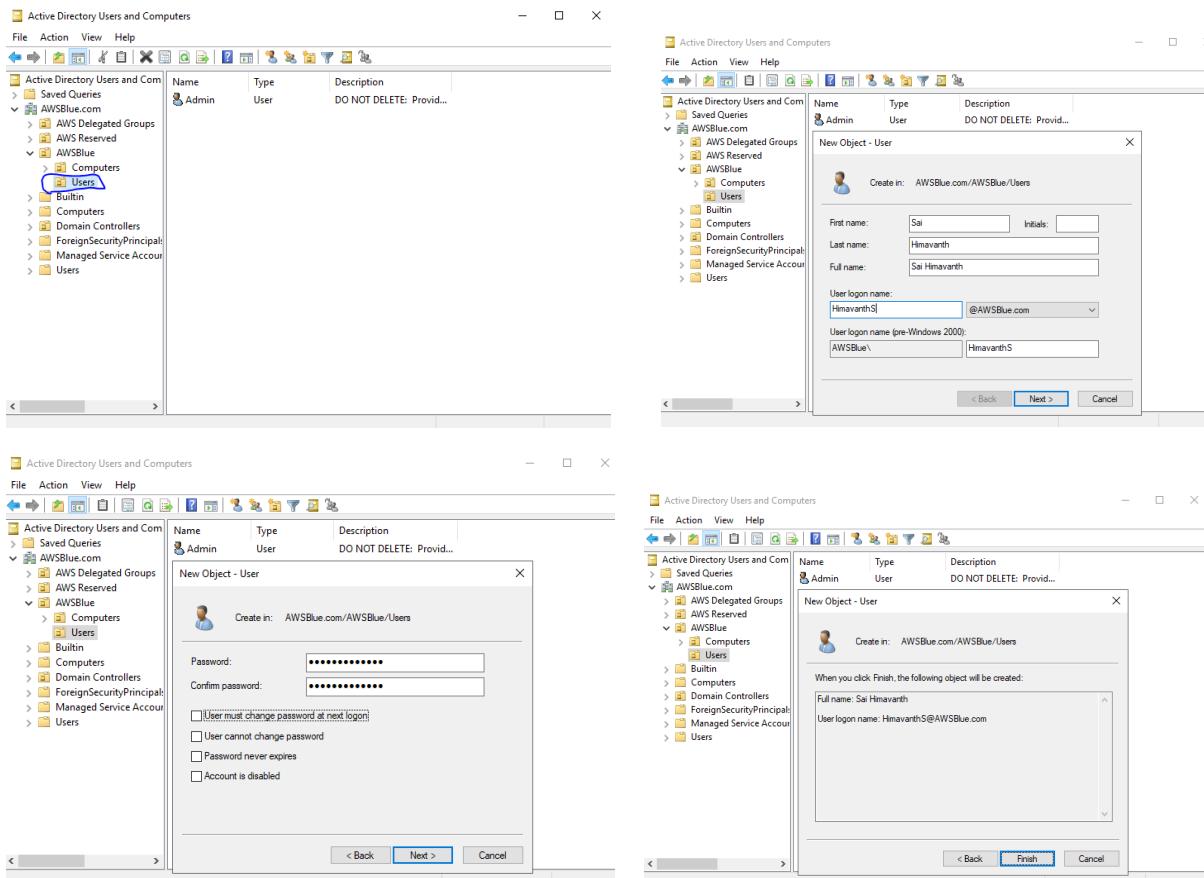
- After the installation is complete, go to the "Tools" in the Server Manager.
- Select "Active Directory Users and Computers" and open it.

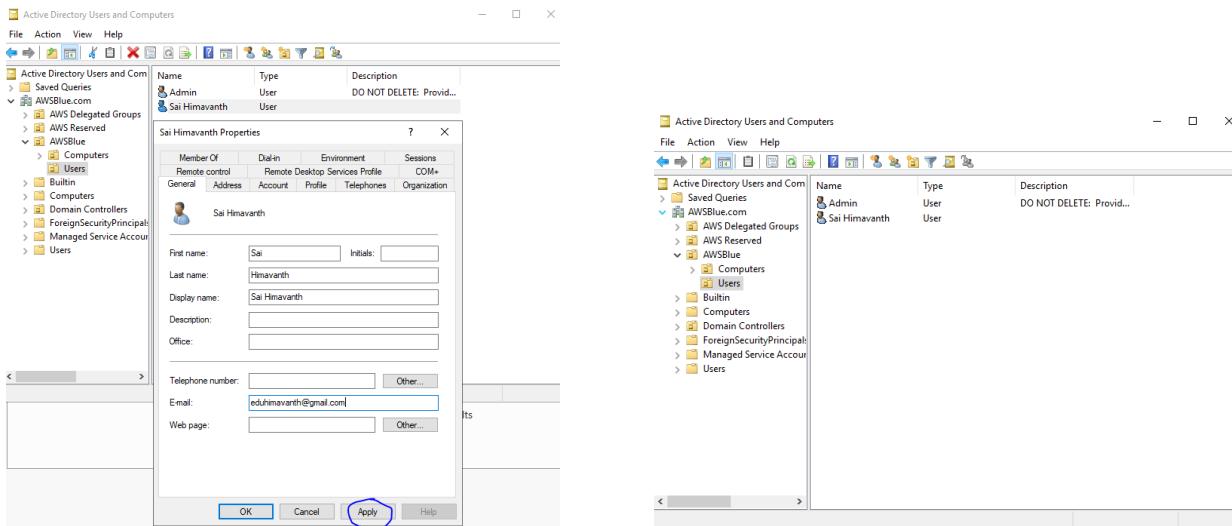


8 - Manage Users and Create New Users

- 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.

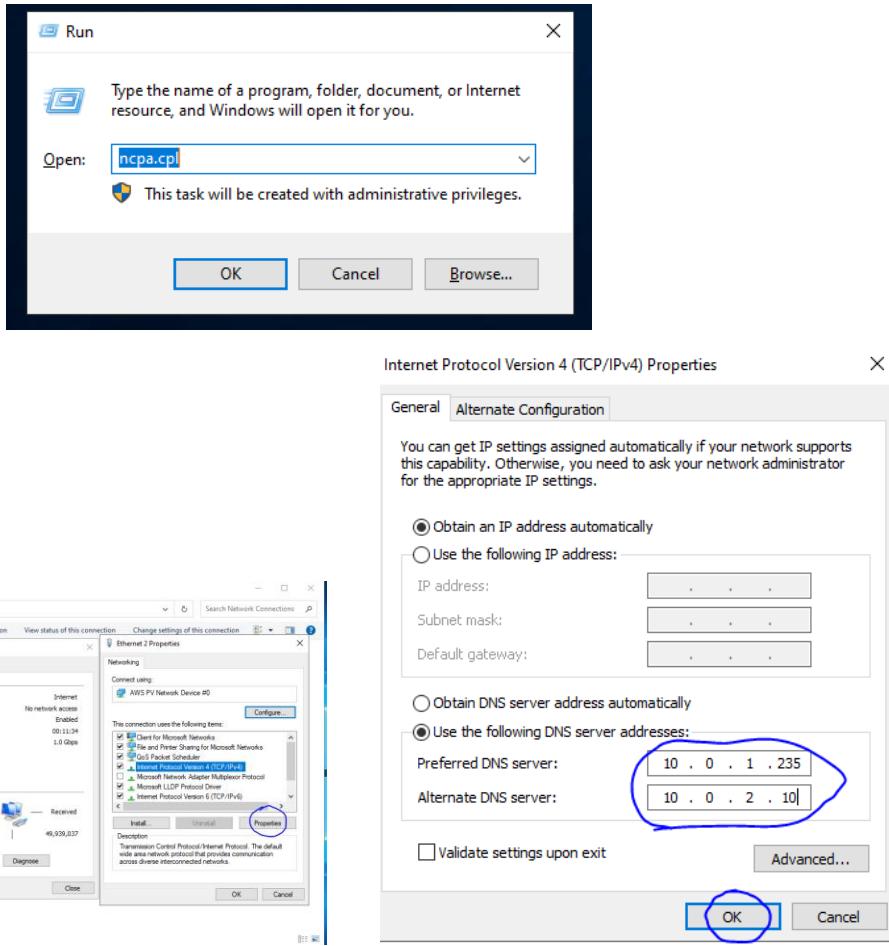
The screenshot shows the AWS Management Console interface for the EC2 service. The top navigation bar includes 'Instances (1/1) Info', a search bar, and buttons for 'Connect', 'Actions', and 'Launch instances'. Below the header is a table with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, Public IPv4 IP, Elastic IP, IPv6 IPs, Monitoring, and Security group. One row is selected, showing 'AWSBlue-PreLaunched-Instance' with details like 'Running', 't2.medium', and 'us-east-2a'. The bottom of the page has navigation arrows and a 'Next' button.

The screenshot shows a 'Windows Security' dialog box. It displays the message: 'Enter your credentials' and 'These credentials will be used to connect to ec2-3-141-0-163.us-east-2.compute.amazonaws.com.'. Below this, it shows the 'Administrator' account and the full path 'HIMAVANTH-PC\Administrator'. There is a password field with masked text, a 'Remember me' checkbox, and a 'More choices' link. At the bottom are 'OK' and 'Cancel' buttons. To the right of the dialog, a portion of the Windows desktop is visible, showing the Start menu and taskbar.

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

PROPERTIES
For EC2AMAZ-P0849QQ

Computer name	EC2AMAZ-P0849QQ
Workgroup	WORKGROUP
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
Operating system version	Microsoft Windows Server 2022 Datacenter
Hardware information	Xen HVM domU
Last installed updates	Windows Update
	Never check for updates
	Never
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
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...

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:

Full computer name:

Member of:

Domain:

Workgroup:

Windows Security

Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

Computer Name/Domain Changes

 Welcome to the AWSBlue.com domain.

Computer Name/Domain Changes

i You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

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.

Windows Security

Enter your credentials

These credentials will be used to connect to ec2-18-117-133-120.us-east-2.compute.amazonaws.com.

AWSBlue\Admin
•••••••••••••
 Remember me

More choices

Administrator
HIMAVANTH-PC\Administrator
 Use a different account

OK Cancel



Server Manager

Server Manager • Local Server

Dashboard Local Server All Servers

PROPERTIES For EC2AMAZ-P0849QQ

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

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

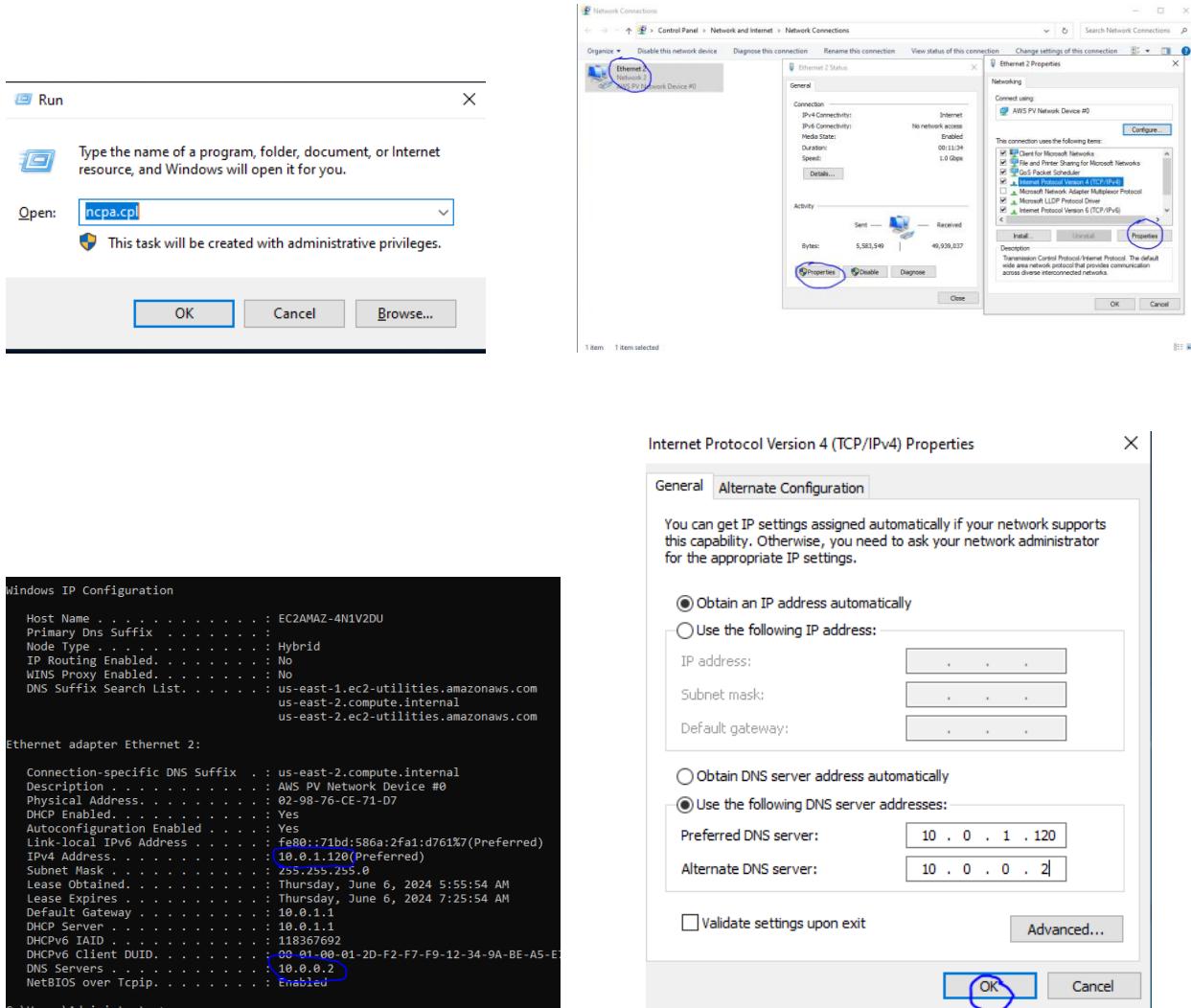
- Open the EC2 Dashboard in the AWS Management Console.
- Select the existing Windows EC2 instance.
- Click "Connect" and choose the "RDP Client" tab.
- Download the RDP file and use it to connect to the instance with the default administrator credentials.

The screenshot shows the AWS Management Console interface for the EC2 service. It displays a table of instances with one entry: 'AD-Windows-Machine'. The instance is listed with the following details: Instance ID (i-0745f508432262e83), Instance State (Running), Instance type (t2.medium), Status check (2/2 checks passed), Availability Zone (us-east-2a), Public IPv4 DNS (ec2-3-147-73-224.us-east-2.compute.amazonaws.com), and Elastic IP (3.147.73.224). The 'Launch Instances' button is visible at the top right of the table.

The screenshot shows a Windows Security dialog box titled 'Windows Security'. It prompts the user to 'Enter your credentials' to connect to the instance. The text in the dialog states: 'These credentials will be used to connect to ec2-3-147-73-224.us-east-2.compute.amazonaws.com.' Below this, there is a text input field for the 'Administrator' password, which contains several dots. To the right of the password field is a 'Remember me' checkbox and a 'More choices' link. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'. To the right of the dialog, a portion of the Windows desktop is visible, showing the Start menu and system status.

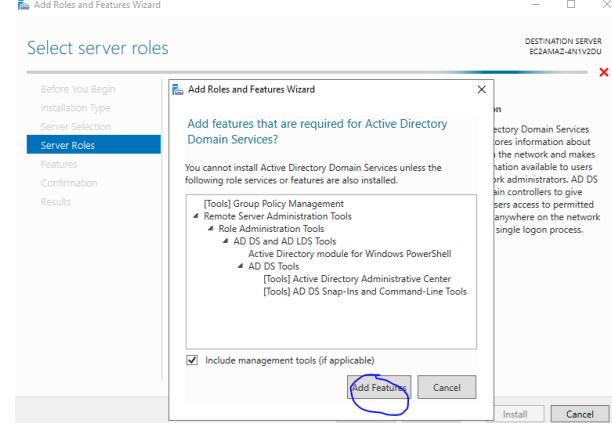
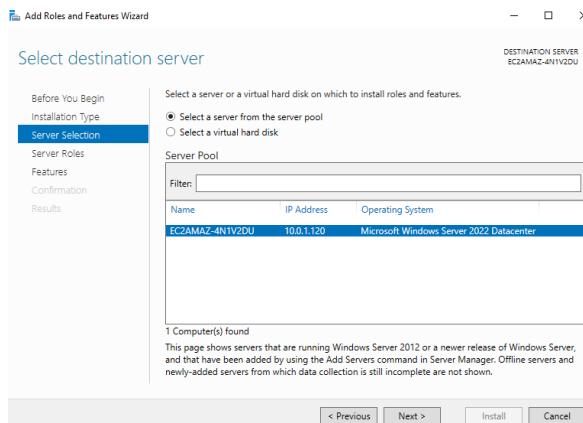
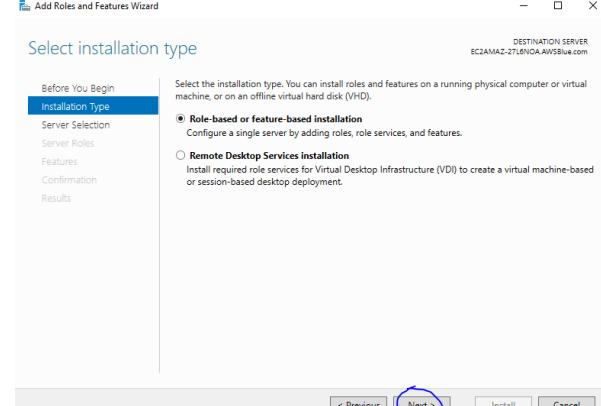
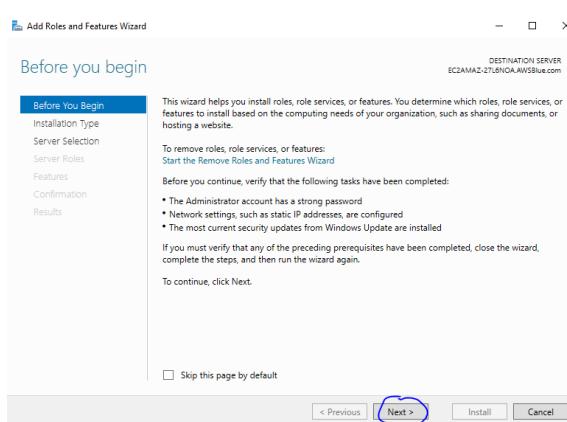
2 - Update DNS IP Addresses

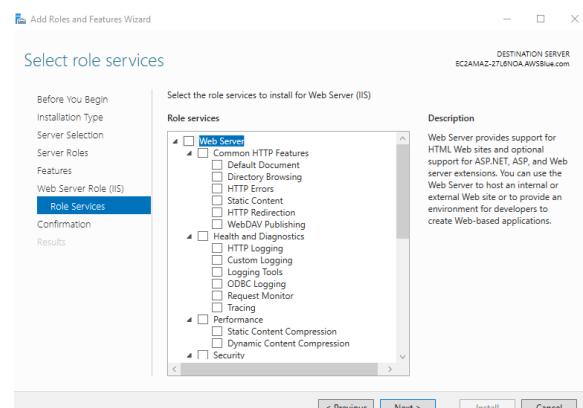
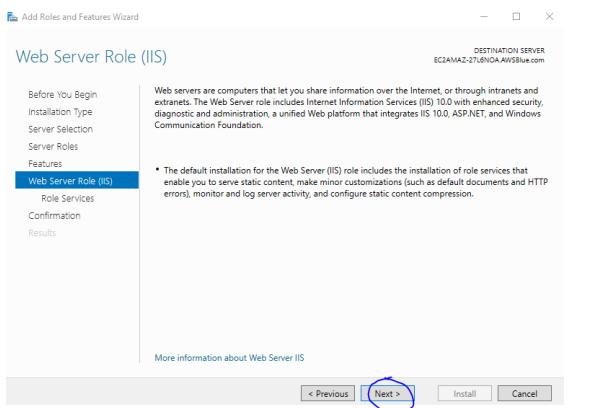
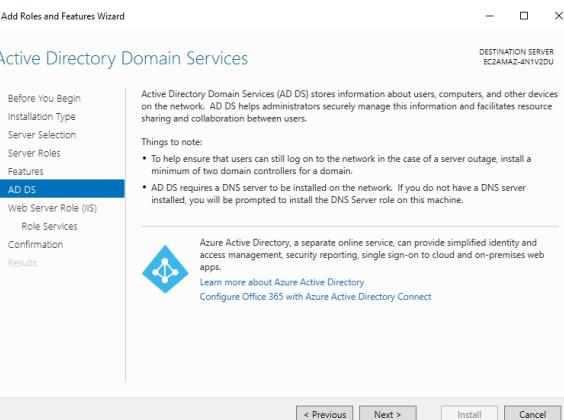
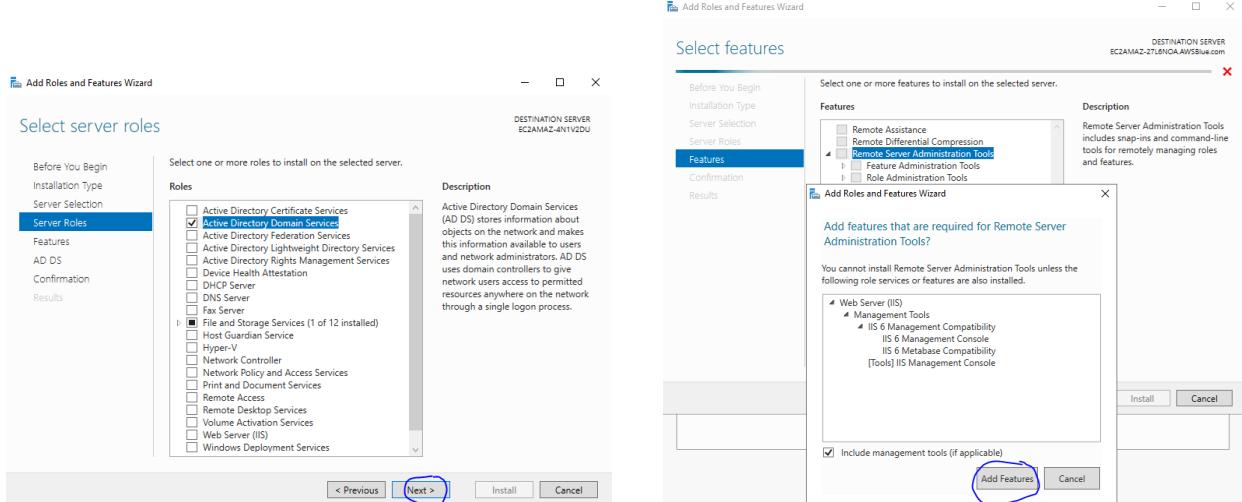
- Open "Network Connections" by typing `ncpa.cpl` in the Run dialog (press 'Win + R').
- Right-click on the active network connection and select "Properties."
- Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties."
- Choose "Use the following DNS server addresses" and enter the IP address 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.

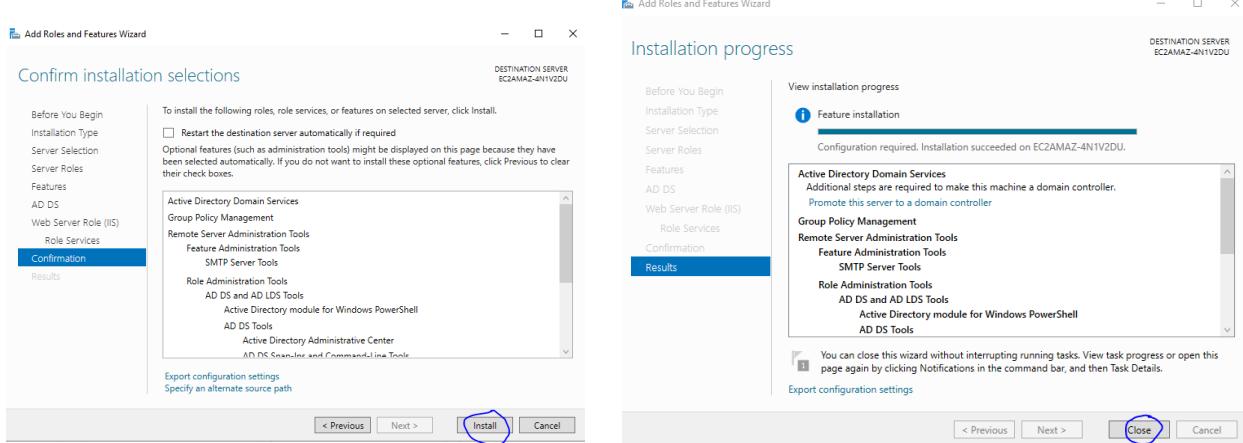


2 - Install Active Directory Domain Services (AD DS)

- 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."

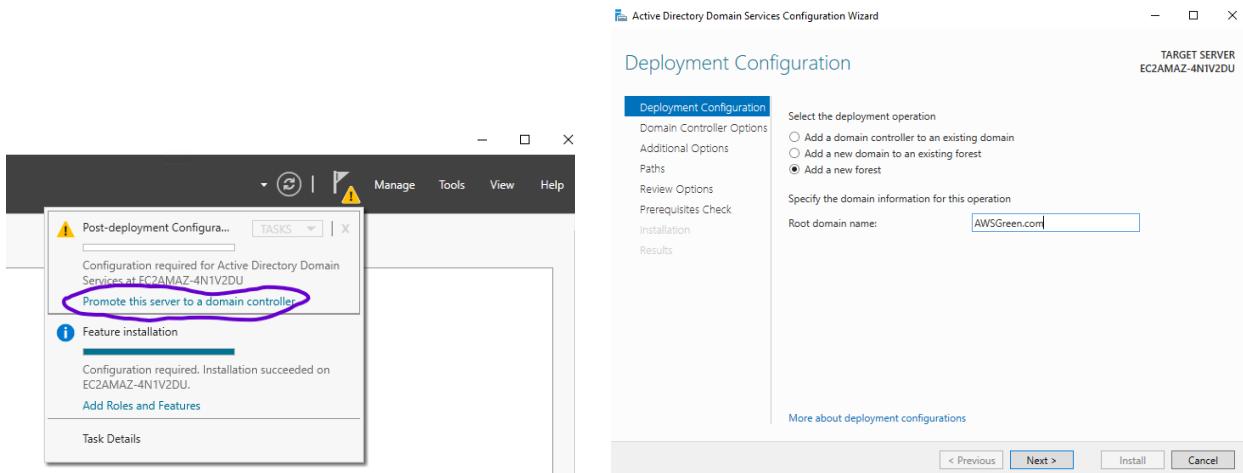


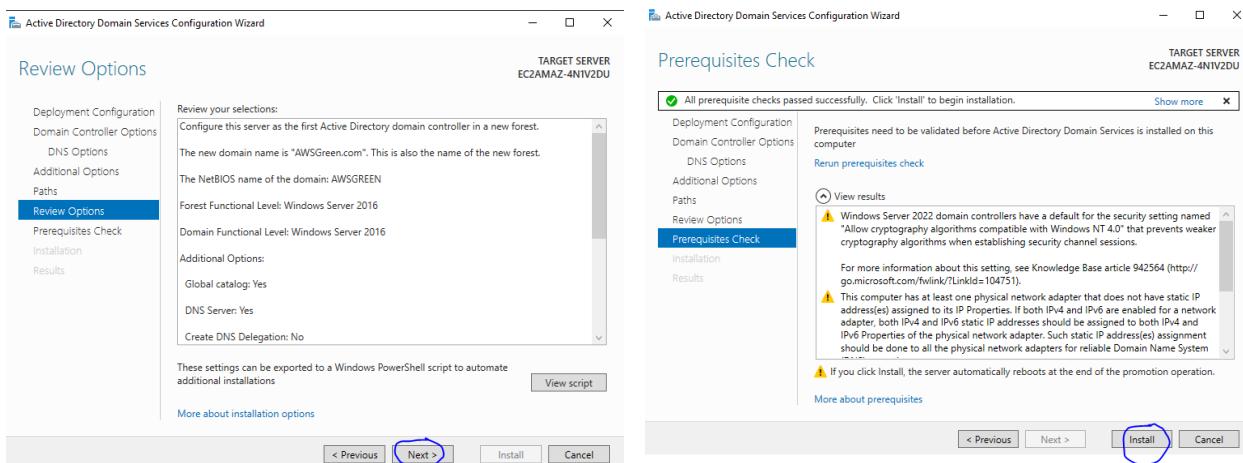
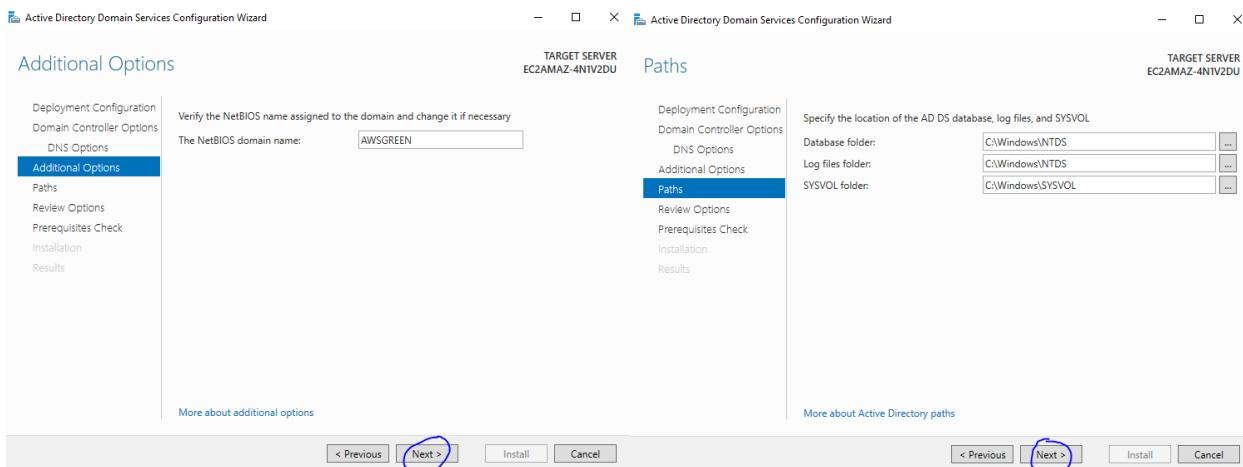
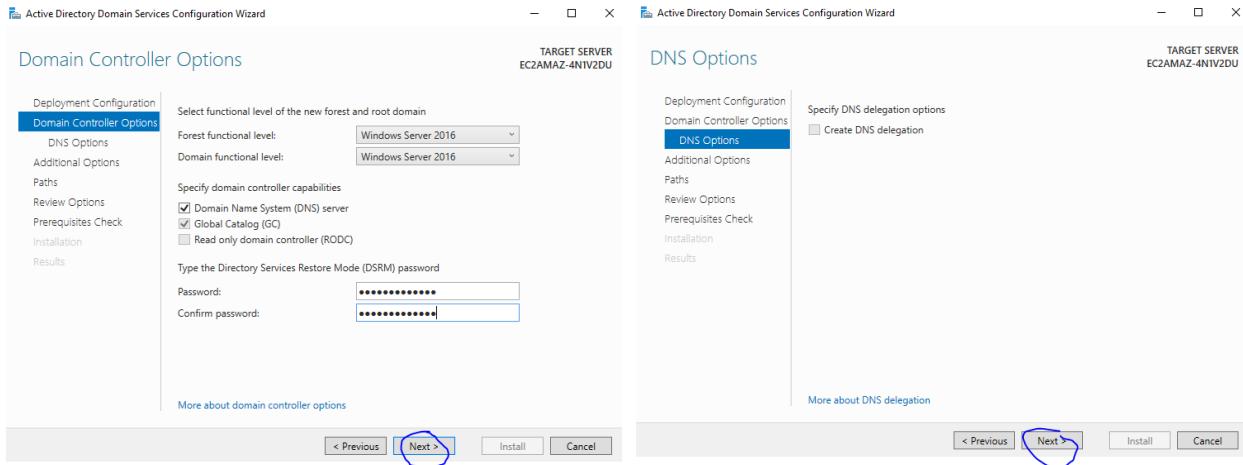




3 - Promote the Server to a Domain Controller

- 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.

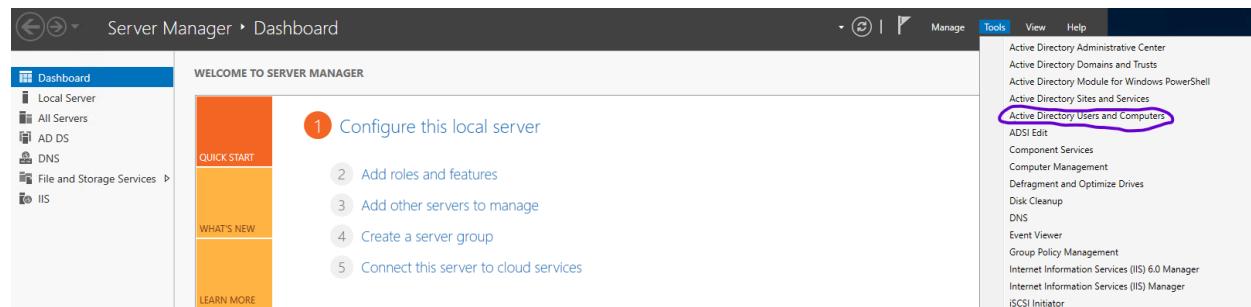
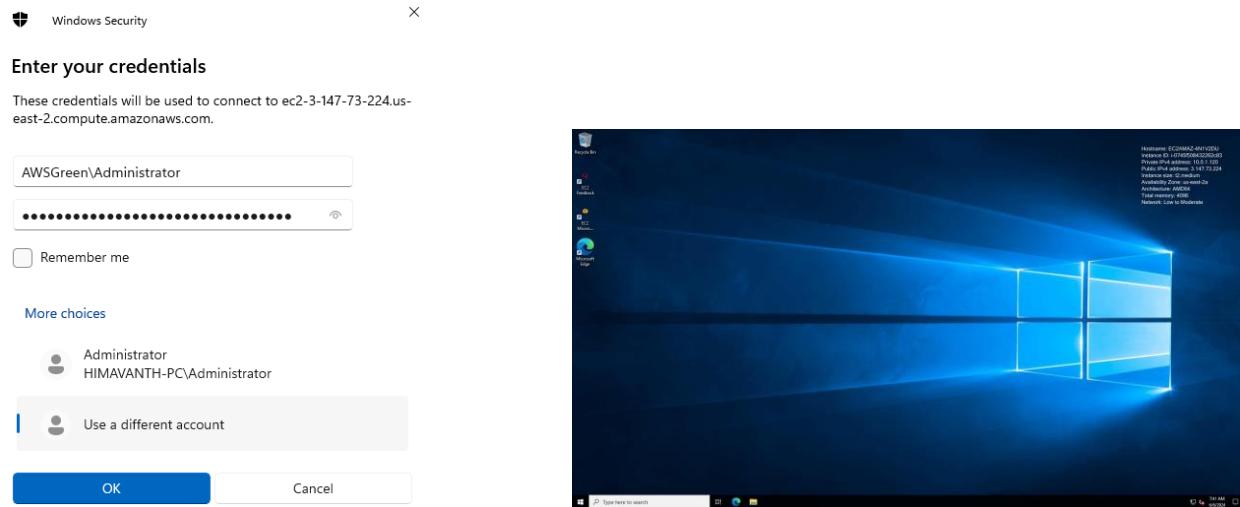




Note: After Installation the system automatically reboots. Relogin into the system with the Active Directory Administrator Credentials.

5 - Verify Active Directory Installation

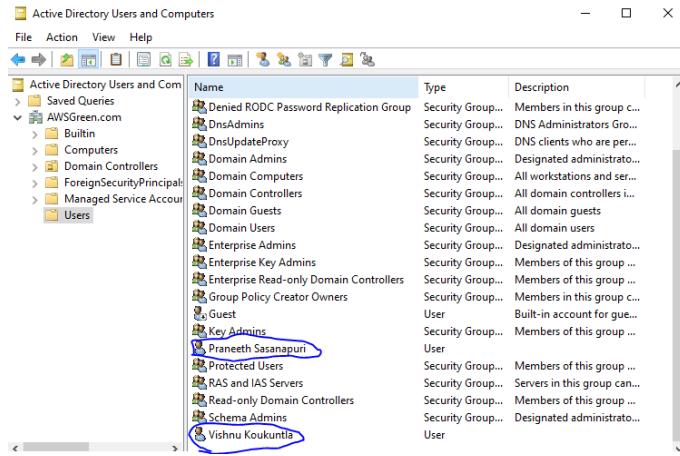
- After the server restarts, reconnect using RDP.
- Log in with the domain credentials (e.g., 'CORP\Administrator').
- Open "Active Directory Users and Computers" to verify the AD installation.
- Ensure you can manage the domain, users, and computers.



The image shows the 'Active Directory Users and Computers' console window. The left pane shows a tree view of the directory structure under 'AWSGreen.com', including 'Saved Queries', 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'Managed Service Accounts', and 'Users'. The right pane displays a table of security groups with columns for 'Name', 'Type', and 'Description'. Some entries are truncated. The table includes:

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...

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



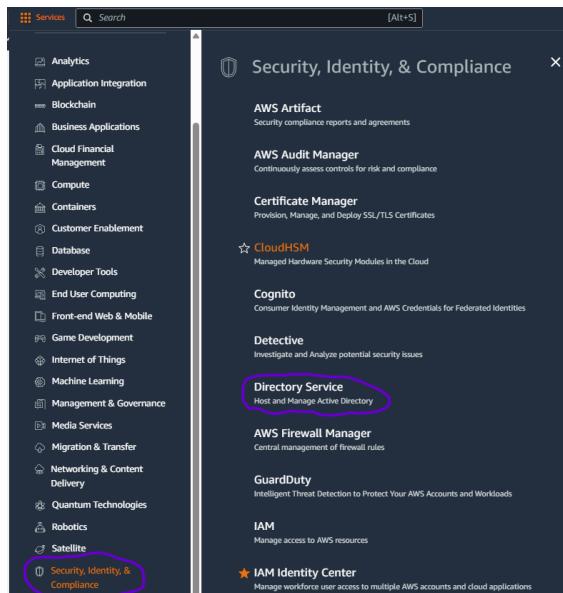
I have added two users to the Active Directory. We will use these users for our next task, which is synchronizing the Active Directory with AWS SSO using AD Connector.

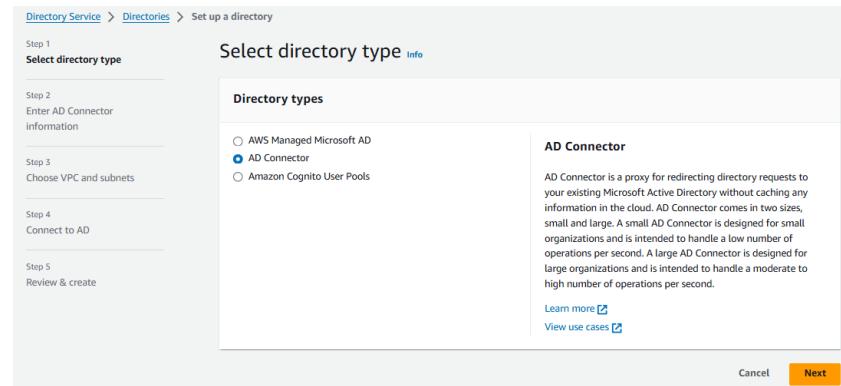
Note: Ensure that the email addresses for the created users are provided, as this is mandatory for AWS SSO to sync with the AD.

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

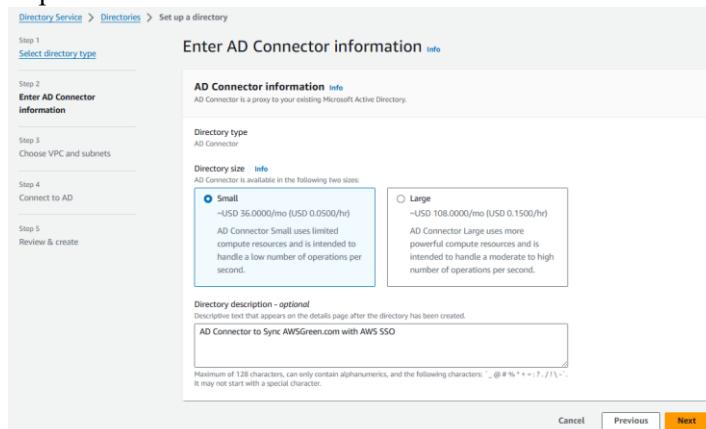
- In the top navigation bar, click on "Services."
- Under "Security, Identity, & Compliance," select "Directory Service."
- On the AWS Directory Service dashboard, click on "Set up directory."
- Select "AD Connector."
- Click "Next."





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.



Directory Service > Directories > Set up a directory

Step 1
[Select directory type](#)

Step 2
[Enter AD Connector information](#)

Step 3
Choose VPC and subnets

Step 4
Connect to AD

Step 5
Review & create

Choose VPC and subnets Info

Networking
The VPC that contains your directory. If you do not have a VPC with at least two subnets, you must create one.

VPC Info
AWSBlue | vpc-0d7b781c02c081d9f (10.0.0.0/16) C

[Create new VPC](#) X

Subnets Info
AWSBlue-Subnet1-Public | subnet-01c328979166043eb (10.0.1.0/24, us-east-2a) C

AWSBlue-Subnet2-Public | subnet-0b75b690811d9c47a (10.0.2.0/24, us-east-2b) C

[Create new subnet](#) X

Initial AD site name for this directory Info
Default-First-Site-Name

[Cancel](#) [Previous](#) Next

Connect to AD Info

Active Directory information
Enter the networking and service account details necessary to connect to your existing Active Directory.

Directory DNS name
The fully qualified domain name of the directory you are connecting to.

Directory NetBIOS name - *optional*
The NetBIOS name of the directory you are connecting to.

DNS IP addresses
The IP addresses of DNS servers you are connecting to. These must be reachable inside the VPC you chose on the previous page.

Service account username Info
Provide the username of the service account you created in your existing Active Directory.

Service account password
The password for the service account provided above.

Maximum of 128 characters.

Confirm password

This password must match the service account password above.

[Cancel](#) [Previous](#) Next

3 - Review and Create:

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

Directory ID	Directory name	Type	Size	Multi-Region	Status	Launch date
d-9a6777e035	AWSGreen.com	AD Connector	Small	Not applicable	Creating	Jun 15, 2024

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 Directory”
- In the "Active Directory" settings, choose the AD Connector you created.
- Review the details, ACCEPT the change and Click “Change Idendity Source”

Identity source

Choose the directory where you want to manage your users and groups. [Learn More](#)

Identity source
Identity Center directory

Authentication method
Password

AWS access portal URL
<https://d-9a6774e035.awsapps.com/start>

Issuer URL
<https://identitycenter.amazonaws.com/ssoins-6684a3aff53e929e>

Provisioning method
Direct

Identity store ID
d-9a6774e035

Actions ▾
Customize AWS access portal URL
Change identity source

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 an AWS Managed Microsoft AD directory. 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

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-9a6774e035)

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-9a6774e035 (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. X

✓ 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 X

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"

IAM Identity Center > Permission sets

Managing instance: iami-6684a3af53c929e

Dashboard | Users | Groups | Settings | Multi-account permissions | AWS accounts | **Permission sets** (highlighted) | Application assignments | Applications | Related consoles: CloudTrail | Recommended | AWS Organizations | IAM

Create permission set

Permission set type

Types

- Predefined permission set** Create a predefined permission set by choosing an AWS-defined template. This template enables you to select a single AWS managed policy. For example, you can select a policy that grants permissions for a common job function, such as Billing, or a specific level of access to AWS services and resources, such as ViewOnlyAccess. You can update the permission set as your needs evolve.
- Custom permission set** Create a custom permission set by selecting AWS managed policies and creating an inline policy (recommended). You can also attach customer managed policies and set a permissions boundary (advanced).

Policy for predefined permission set

Select an AWS managed policy

- AdministratorAccess** Provides full access to AWS services and resources.
- Billing** Grants permissions for billing and cost management. This includes viewing account usage and viewing and modifying budgets and payment methods.
- DatabaseAdministrator** Grants full access permissions to AWS services and actions required to set up and configure AWS database services.
- DataScientist** Grants permissions to AWS data analytics services.
- NetworkAdministrator** Grants full access permissions to AWS services and actions required to set up and configure AWS network resources.
- PowerUserAccess** Provides full access to AWS services and resources, but does not allow management of users and groups.
- ReadOnlyAccess** Provides read-only access to AWS services and resources.
- SecurityAudit** The security audit template grants access to read security configuration metadata. It is useful for software that audits the configuration of an AWS account.
- SupportUser** This policy grants permissions to troubleshoot and resolve issues in an AWS account. This policy also enables the user to contact AWS Support to create and manage cases.
- SystemAdministrator** Grants full access permissions necessary for resources required for application and development operations.
- ViewOnlyAccess** This policy grants permissions to view resources and basic metadata across all AWS services.

Specify permission set details

Permission set name: **ReadOnlyAccess**

Description: Provides ReadOnlyAccess to all the AWS Resources and Services

Session duration: 12 hours

Relay state - optional: Enter relay state

Tags - optional (not set)

Cancel | **Next**

Cancel | Previous | **Next**

Review and create

Step 1: Select permission set type

Permission set type	
Type	AWS managed policy ReadOnlyAccess
Predefined permission set	

Step 2: Define permission set details

Permission set details	
Permission set name	Session duration
ReadOnlyAccess	12 hours
Description	Relay state
Provides ReadOnlyAccess to all the AWS Resources and Services	-

Tags (not set)

Key	Value
No resources You have not added any tags	

Cancel Previous Create

IAM Identity Center > Permission sets

IAM Identity Center now supports customer managed policies and permissions boundaries in your permission sets
This feature enables you to create customer managed policies in IAM and attach them to this permission set when you need to define custom permissions. You can also set a permissions boundary to control the maximum permissions for the permission set. [Learn more](#)

Permission sets (1)

Permission sets define the level of access that users in IAM Identity Center have to their assigned AWS accounts. The names of permission sets appear as available roles in the AWS access portal. Users who are assigned to multiple AWS permission sets can sign in to the AWS access portal, choose an account, and then choose a role that AWS created from an assigned permission set. [Learn more](#)

Find permission sets by full ARN or permission set ID (i.e., ps-abcdefg123456789).	<	1	>	@
Permission set Description ARN Provisioned status Creation time				
<input checked="" type="radio"/> ReadOnlyAccess	Provides ReadOnlyAccess to all the AWS Resources and Se...	arn:aws:ssc:permissionSet:ssoinst-6684a3aff53e929e/ps-590b/c4d7b9...	<input checked="" type="radio"/> Not provisioned	Now

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

IAM Identity Center > Users

Users (0)

Users listed here can sign in to the AWS access portal to access AWS accounts and assigned cloud applications. [Learn more](#)

Username	Display name	Status	Created by
No users found			

C Delete users Manage sync < 1 > @

IAM Identity Center > Settings > Manage sync

Manage sync

Specify the users and groups to sync from Active Directory to IAM Identity Center. After your users and groups are fully synced, you can go to the AWS accounts or Applications page to manage which resources they can access. You can add or remove users and groups to change the sync scope at any time. Changes to the sync scope are implemented in IAM Identity Center the next time that users and groups are synced from Active Directory. [Learn more](#)

Users **Groups**

Users in sync scope

Username	Date added
No item	

Add users and groups

Specify the users and groups to sync from Active Directory to IAM Identity Center. After your users and groups are synced to IAM Identity Center, you can assign them access to AWS accounts and cloud applications. [Learn more](#)

User

AWSGreen.com

Add users or groups

Specify the users and groups to sync from Active Directory to IAM Identity Center. After your users and groups are synced to IAM Identity Center, you can assign them access to AWS accounts and cloud applications. [Learn more](#)

Users **Groups**

User

AWSGreen.com

Added users and groups (2)

Username / Group name	Type	Domain
VishnuK	User	AWSGreen.com
PraneethS	User	AWSGreen.com

Success Message: 2 users and 0 groups added to the sync scope successfully.

IAM Identity Center > Settings > Manage sync

Manage sync

Specify the users and groups to sync from Active Directory to IAM Identity Center. After your users and groups are fully synced, you can go to the AWS accounts or Applications page to manage which resources they can access. You can add or remove users and groups to change the sync scope at any time. Changes to the sync scope are implemented in IAM Identity Center the next time that users and groups are synced from Active Directory. [Learn more](#)

Users **Groups**

Users in sync scope

Username	Date added
PraneethS@AWSGreen.com	2024-06-15T18:42:29.341Z
VishnuK@AWSGreen.com	2024-06-15T18:42:28.820Z

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

IAM Identity Center > Users

Managing instance ssoinst-66843aff53e929e

Users **Groups** **Setting** **Mult-account permissions** **Application assignments**

Users (2)

Users listed here can sign in to the AWS access portal to access AWS accounts and assigned cloud applications. [Learn more](#)

Username	Display name	Status	Created by
VishnuK@AWSGreen.com	Vishnu Koukuntla	Enabled	Manual
PraneethS@AWSGreen.com	Praneeth Sasanapuri	Enabled	Manual

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.

The screenshot shows the IAM Identity Center interface. On the left, there's a sidebar with options like Dashboard, Users, Groups, Settings, Multi-account permissions (with AWS accounts selected), Application assignments, and Applications. The main area is titled 'AWS accounts' and shows a tree structure under 'Organizational structure'. At the top right, there are buttons for 'Assign users or groups', 'Hierarchy', and 'List'. A user named 'eduhimavanth' is selected, highlighted with a red circle.

This screenshot shows the 'eduhimavanth' user profile page. It includes an 'Overview' section with account details (Account name: eduhimavanth, Account ID: 054654231148, Email: eduhimavanth@gmail.com). Below it is a 'Users and groups' tab, which is active. Under 'Assigned users and groups (0)', there's a note that no users or groups have been assigned. A button labeled 'Assign users or groups' is circled in red. The 'Permission sets' tab is also visible.

This screenshot shows the 'Assign users and groups to "eduhimavanth"' step of the wizard. It has three steps: Step 1 (Select users and groups), Step 2 (Select permission sets), and Step 3 (Review and submit). Step 1 is active, showing the 'Users' tab selected. Under 'Users (2/2)', two users are listed: 'VishnuK@AWSGreen.com' and 'PraneethS@AWSGreen.com', both with the status 'Enabled'. A 'Selected users and groups (2)' summary is at the bottom. Buttons for 'Cancel' and 'Next' are at the bottom right, with 'Next' circled in red.

IAM Identity Center > AWS Organizations: AWS accounts > eduhimavanth > Assign users and groups

Step 1
Select users and groups

Step 2
Select permission sets

Step 3
Review and submit

Assign permission sets to "eduhimavanth"

Permission sets define the level of access that users and groups in IAM Identity Center have to an AWS account. You can assign more than one permission set to a user. To ensure least privilege access to AWS accounts, users in IAM Identity Center with multiple permission sets on an AWS account must pick a specific permission set when selecting the account and then return to the AWS access portal to pick a different set when necessary. [Learn more](#)

Permission set	Description	ARN
<input checked="" type="checkbox"/> ReadOnlyAccess	Provides ReadOnlyAccess to all the AWS Resources and Services	arn:aws:ss:::permission Set:ssoin-6684a3aff53e929e/ps-590b7ce4d7b9ff08

Cancel Previous **Next**

IAM Identity Center > AWS Organizations: AWS accounts > eduhimavanth > Assign users and groups

Step 1
Select users and groups

Step 2
Select permission sets

Step 3
Review and submit

Review and submit assignments to "eduhimavanth"

Step 1: Select users and groups

Username / group name	Type
Praneeth@AWSGreen.com	User
VishnuK@AWSGreen.com	User

Step 2: Select permission sets

Permission set	Description	ARN	Creation time
ReadOnlyAccess	Provides ReadOnlyAccess to all the AWS Resources and Services	arn:aws:ss:::permission Set:ssoin-6684a3aff53e929e/ps-590b7ce4d7b9ff08	25 minutes ago

Cancel Previous **Submit**

We reprovisioned your AWS account successfully and applied the updated permission set to the account.

IAM Identity Center > AWS Organizations: AWS accounts > eduhimavanth

eduhimavanth

Overview

Account name eduhimavanth	Account ID 654654233148	Email eduhimavanth@gmail.com
------------------------------	----------------------------	---------------------------------

Users and groups (2) **Permission sets (1)**

Assigned users and groups (2)

The following users and groups in IAM Identity Center can select this AWS account from within their AWS access portal. [Learn more](#)

Username / group name	Permission sets	Type
awsgreen.com/praneeth5@AWSGreen.com	ReadOnlyAccess	User
awsgreen.com/vishnuK@AWSGreen.com	ReadOnlyAccess	User

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>



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.



Sign in

Username:

PraneethS ([not you?](#))

Password

Show password

[Forgot password](#)

[Sign in](#)

[Cancel](#)

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](#)

[Praneeth](#) [MFA devices](#) [Sign out](#)

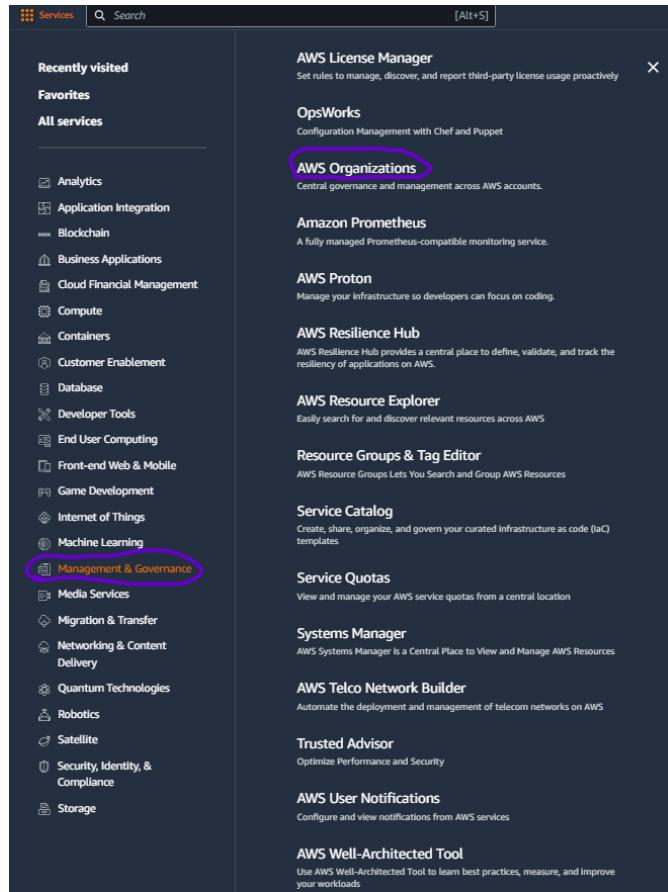
Note: The above snippet confirms that ReadOnlyAccess has been successfully implemented for the AD users to access the AWS account.

- 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 and 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.



The screenshot shows the AWS Organizations console. On the left, there's a sidebar with 'AWS accounts' (which is expanded), 'Invitations', 'Services', 'Policies', 'Settings' (with a 'New' button), and 'Get started'. Below that is an 'Organization ID' section with 'o-1u9ns73r1t'. The main area is titled 'AWS accounts' and shows a list of accounts. At the top right, there's a blue button labeled 'Add an AWS account'. The list includes one account: 'eduhimavanth management account' (ID: r-kqj0), which joined on '2024/05/26'. There are 'Actions' and 'Hierarchy' buttons at the top of the list table.

Add an AWS account

You can add an AWS account to your organization either by creating an account or by inviting one or more existing AWS accounts to join your organization.

Create an AWS account
Create an AWS account that is added to your organization.

Invite an existing AWS account
Send an email request to the owner of the account. If they accept, the account joins the organization.

Invite one or more existing AWS accounts to join your organization

Email address or account ID of the AWS accounts to invite

Add another account

Message to include in the invitation email message - optional
This text is included in the email message sent to the owners of the invited AWS accounts.

Tags
Tags are key-value pairs that you can add to AWS resources to help identify, organize, and secure your AWS resources.

No tags are associated with the resource.

Add tag
You can add up to 50 more tags.

Cancel **Send invitation**

An invitation to join your AWS organization has been sent.

AWS accounts

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

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	
<input type="checkbox"/> Root r-kqg9	Joined 2024/05/26	
<input type="checkbox"/> eduhimavanth [management account] 654654233148 eduhimavanth@gmail.com		

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.

Your AWS account has been
invited to join an AWS
organization [Inbox](#)

no-reply-aws 3:34 PM
to me ▾

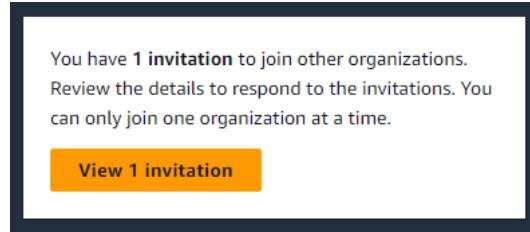


Invitation to join an organization

[eduhimavanth](#) (owned by [redacted@gmail.com](#)) would like to add your AWS account [redacted@gmail.com](#) to their organization as a member account, using AWS Organizations.

To view the invitation, including which features are enabled, click the following link:

[Accept invitation](#)



AWS Organizations > Invitations

Invitations

Invitation from [REDACTED]@gmail.com

Review invitation details below.

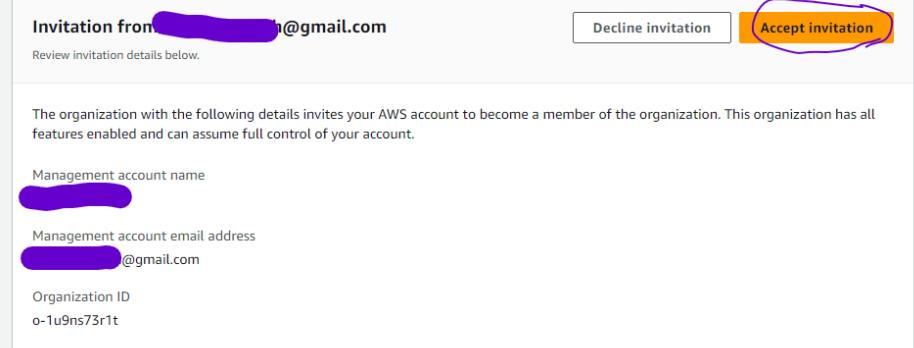
The organization with the following details invites your AWS account to become a member of the organization. This organization has all features enabled and can assume full control of your account.

Management account name
[REDACTED]

Management account email address
[REDACTED]@gmail.com

Organization ID
o-1u9ns73r1t

[Decline invitation](#) [Accept invitation](#)



You accepted an invitation to join an organization.

AWS Organizations > Dashboard

Dashboard

Organization details

Organization ID
o-1u9ns73r1t

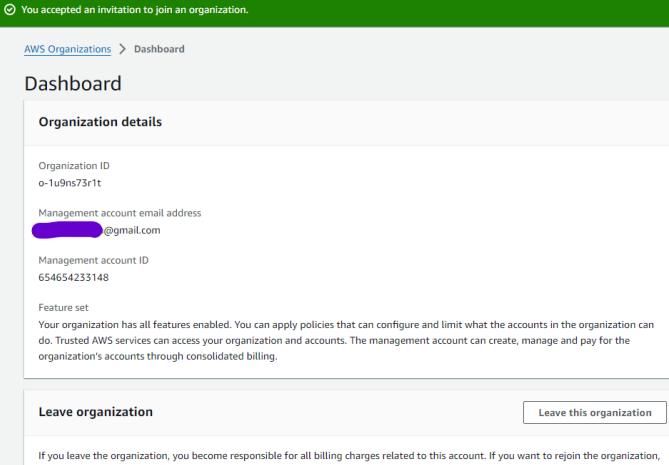
Management account email address
[REDACTED]@gmail.com

Management account ID
654654233148

Feature set
Your organization has all features enabled. You can apply policies that can configure and limit what the accounts in the organization can do. Trusted AWS services can access your organization and accounts. The management account can create, manage and pay for the organization's accounts through consolidated billing.

Leave organization [Leave this organization](#)

If you leave the organization, you become responsible for all billing charges related to this account. If you want to rejoin the organization, you must receive and approve a new invitation. [Learn more](#)



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.

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

Organizational units (OUS) enable you to group several accounts together and administer them as a single unit instead of one at a time.

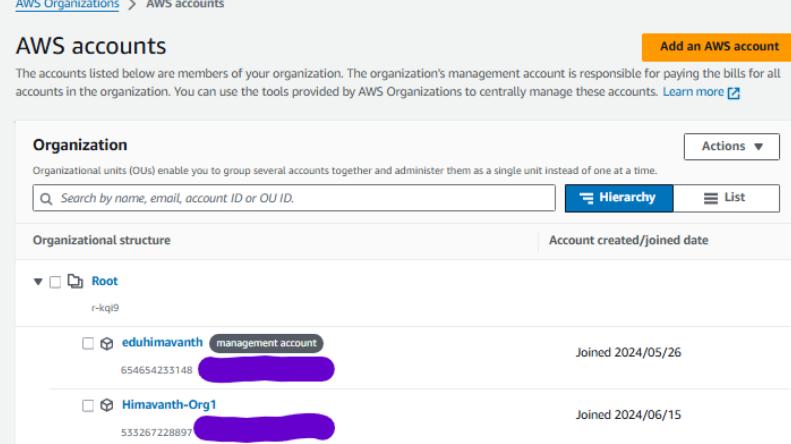
Actions ▾

Search by name, email, account ID or OU ID. [Hierarchy](#) [List](#)

Organizational structure [Account created/joined date](#)

Root
eduhimavanth management account
654654233148 [REDACTED] Joined 2024/05/26

Himavanth-Org1
533267228897 [REDACTED] Joined 2024/06/15



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.

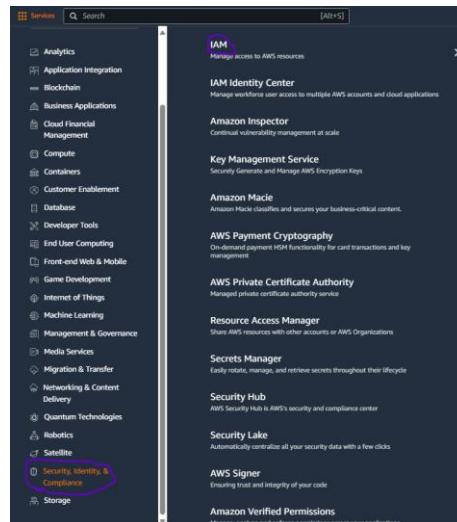
The screenshot shows the AWS Access Portal interface. At the top, there's a banner with the text "Introducing the Create shortcut button" and a link to learn more. Below the banner, the title "AWS access portal" is displayed. There are two tabs: "Accounts" (which is selected) and "Applications". Under the "Accounts" tab, the heading "AWS accounts (2)" is shown. A search bar with the placeholder "Filter accounts by name, ID, or email address" is present. Two accounts are listed: "eduhimavanth" (with ID 654654233148) and "Himavanth-Org1" (with ID 533267228897). Each account entry includes a "Create shortcut" button and links for "ReadOnlyAccess" and "Access keys". The user "Praneeth" is logged in at the top right, along with "MFA devices" and "Sign out".

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."

The screenshot shows the IAM User Groups page. On the left, there's a navigation sidebar with 'User groups' highlighted. The main area shows a table with one row for 'Infra'. At the top right of the table is a yellow 'Create group' button, which is circled in red. The URL in the browser bar is 'IAM > User groups'.

This is the first step of the 'Create user group' wizard. It asks for a group name ('Infra') and lists users to add to the group. Below it, the 'Attach permissions policies' section is shown, listing the 'AdministratorAccess' policy.

This is the second step of the wizard, showing the selected 'AdministratorAccess' policy attached to the group.

Create Dev Group:

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

IAM > User groups > Create user group

Create user group

Name the group

User group name
Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and "+,-,_," characters.

Add users to the group - **Optional (0)** Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

User name
No resources to display

Attach permissions policies - **Optional (928)** Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Policy name	Type	Used as	Description
<input checked="" type="checkbox"/> AdministratorAccess	AWS managed - job function	Permissions policy (1)	Provides full access to AWS services a...
<input checked="" type="checkbox"/> AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permis...
<input checked="" type="checkbox"/> AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permis...
<input checked="" type="checkbox"/> AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaFo...
<input checked="" type="checkbox"/> AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness ...
<input checked="" type="checkbox"/> AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to A...
<input checked="" type="checkbox"/> AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS managed	None	Provide access to Lifesize AVS devices
<input checked="" type="checkbox"/> AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None	Provide access to Poly AVS devices
<input checked="" type="checkbox"/> AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForB...

Dev user group created. View group

IAM > User groups

User groups (2) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Group name	Users	Permissions	Creation time
<input checked="" type="checkbox"/> Dev	0	Not defined	Now
<input checked="" type="checkbox"/> Infra	0	Defined	24 minutes ago

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.

The screenshot shows the AWS IAM Policies list page. At the top right, there is a prominent orange "Create policy" button. The main table lists three policies: "AccessAnalyzerServiceRolePolicy", "AdministratorAccess", and "AdministratorAccess-Amplify". Each row includes columns for Policy name, Type, Used as, and Description. The "AdministratorAccess" row is expanded to show its detailed permissions.

This screenshot shows the "Specify permissions" step of the IAM policy creation wizard. It displays a JSON editor with a large block of JSON code representing the policy's permissions. On the right, there is a sidebar titled "Edit statement" with a "Select a statement" dropdown and a "Add new statement" button. At the bottom right of the editor, the "Next" button is highlighted with a purple circle.

This screenshot shows the "Review and create" step of the IAM policy creation wizard. It displays the "Policy details" section where the policy name "S3FullAccessWithoutDelete" and description "Policy granting full access to S3 except for delete operations" are reviewed. At the bottom right, the "Create policy" button is highlighted with a purple circle.

This screenshot shows the IAM Policies list page again, but now it includes the newly created policy "S3FullAccessWithoutDelete" at the bottom of the list. The "View policy" button for this new policy is highlighted with a purple circle.

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”

The screenshot shows the IAM User groups page. A user group named "Dev" is selected, indicated by a red circle around its name in the "Group name" column. The "Permissions" column for the Dev group shows "Not defined". The "Creation time" column shows "31 minutes ago". The "ARN" column shows "arn:aws:iam:654654233148:group/Dev".

The screenshot shows the Dev group's Permissions tab. The "Permissions policies (0)" section has a "Add permissions" button highlighted with a red circle. Other buttons visible include "Simulate", "Remove", and "Attach policies".

The screenshot shows the "Add permission policies" dialog. The "S3FullAccessWithoutDelete" policy is selected and highlighted with a red circle. The "Attach policies" button at the bottom right of the dialog is also highlighted with a red circle.

The screenshot shows the Dev group's Permissions tab again. The "Permissions policies (1)" section now lists the "S3FullAccessWithoutDelete" policy, which is highlighted with a red circle. The "Attached entities" column shows "1".

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."

The screenshot shows the AWS IAM 'Users' page. On the left sidebar, 'User groups' is selected. The main area displays a table with columns: User name, Path, Group, Last activity, MFA, Password age, Console last sign-in, Access key ID, Active key age, Access key last use, ARN, and Creation date. A single row is present with the status 'No resources to display'. At the top right of the table, there is a 'Create user' button, which is circled in red in the screenshot.

The screenshot shows the 'Specify user details' step of the IAM User creation wizard. The left sidebar lists steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). The main form has a title 'Specify user details' and a section 'User details' with a 'User name' field containing 'Paneth-Infra'. Below it is a note: 'The user name can have up to 16 characters. Valid characters: A-Z, a-z, 0-9, and + - _ (hyphen).'. There is also a checkbox 'Provide user access to the AWS Management Console - optional' with a note: 'If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.' A large callout box highlights the 'Are you providing console access to a person?' section, which contains two radio button options: 'Specify a user in Identity Center - Recommended' (selected) and 'I want to create an IAM user'. Both options have associated notes. The next section is 'Console password' with three options: 'Autogenerated password' (selected), 'Custom password', and 'Show password'. A note states: 'Users must create a new password at next sign-in - Recommended'. The final note at the bottom is: 'If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Kinesis, you can generate them after you create this IAM user. Learn more'.

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more 

Permissions options

- Add user to group Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/2)

Group name	Users	Attached policies	Created
Dev	0	-	2024-06-18 (28 minutes ago)
Infra	0	AdministratorAccess	2024-06-18 (52 minutes ago)

Set permissions boundary - optional

Cancel Previous **Next** 

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Praneeth-Infra	Console password type	Autogenerated	Require password reset	Yes
-----------	----------------	-----------------------	---------------	------------------------	-----

Permissions summary

Name	Type	Used as
iAMUserChangePassword	AWS managed	Permissions policy
Infra	Group	Permissions group

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag 

You can add up to 30 more tags.

Cancel Previous **Create user** 

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL	https://654654233148.signin.aws.amazon.com/console	Email sign-in instructions 
User name	Praneeth-Infra	
Console password	Show	

Cancel Download .CSV file Return to users list 

Note down the user credentials securely.

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Ready to streamline human access to AWS and cloud apps?

Identity Center is enabled. We recommend managing workforce users' access to AWS accounts and cloud applications in Identity Center.

Learn more  Watch how it works 

Users (1) 

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age	Access key last use	ARN	Creation date
Praneeth-Infra	/	1	-	-	-	-	-	-	-	arn:aws:iam::654654233148:user/Praneeth-Infra	1 minute ago

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:

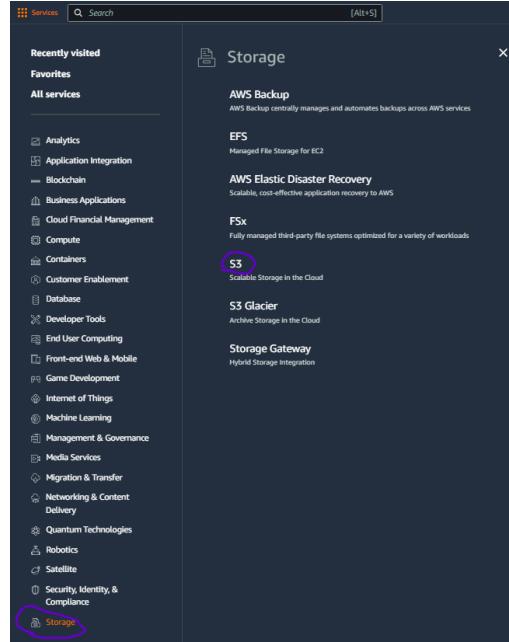
- User1 (Infra) has full access to AWS services through membership in the "Infra" group.
- User2 (Dev) has create/list access to Amazon S3, excluding delete access to S3 objects.
- Ensure to manage user credentials securely and follow the principle of least privilege when assigning permissions in IAM.

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.



The screenshot shows the Amazon S3 landing page. It features a sidebar with links for Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and IAM Access Analyzer for S3. The main content area displays the heading 'Amazon S3' and the sub-headline 'Store and retrieve any amount of data from anywhere'. Below this, it states 'Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.' On the right, there is a 'Create a bucket' section with a 'Create bucket' button, which is circled in blue.

The screenshot shows the 'Create bucket' configuration page for Amazon S3. The top navigation bar includes 'Amazon S3 > Buckets > Create bucket'. The main form is divided into several sections:

- General configuration** (selected tab):
 - AWS Region:** US East (N. Virginia) us-east-1
 - Bucket type:** 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.)
 - Bucket name:** awstestbucket-ws (Info)
 - Copy settings from existing bucket - optional:** Only the bucket settings in the following configuration are copied. A 'Choose bucket' dropdown is shown, with 'Format: /\$2/bucket/prefix'.
- Object Ownership** (Info):
 - 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.)
- Block Public Access settings for this bucket** (Info):
 - 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.)

Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning
 Disable
 Enable

Tags - optional (0)
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.
[Add tag](#)

Default encryption [Info](#)
Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)
 Server-side encryption with Amazon S3 managed keys (SSE-S3)
 Server-side encryption with AWS Key Management Service keys (SSE-KMS)
 Dual-layer server-side encryption with AWS Key Management Service keys (DSS-E-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see [DSS-E-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSS-E-KMS. [Learn more](#)
 Disable
 Enable

Advanced settings

① After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#) [Create bucket](#) (circled)

Successfully created bucket "awstestbucket-ws"
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Amazon S3 > Buckets

► Account snapshot - updated every 24 hours [All AWS Regions](#)
Storage lens provides visibility into storage usage and activity trends. [Learn more](#) [View Storage Lens dashboard](#)

General purpose buckets | Directory buckets

General purpose buckets (1) [Info](#) [All AWS Regions](#)
Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
awstestbucket-ws	US East (N. Virginia) us-east-1	View analyzer for us-east-1	June 20, 2024, 04:07:55 (UTC-04:00)

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.

Amazon S3 > Buckets

► Account snapshot - updated every 24 hours [All AWS Regions](#)
Storage lens provides visibility into storage usage and activity trends. [Learn more](#) [View Storage Lens dashboard](#)

General purpose buckets | Directory buckets

General purpose buckets (1) [Info](#) [All AWS Regions](#)
Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
awstestbucket-ws	US East (N. Virginia) us-east-1	View analyzer for us-east-1	June 20, 2024, 04:07:55 (UTC-04:00)

Amazon S3 > Buckets > awstestbucket-wsu

awstestbucket-wsu [Info](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

Objects (0) [Info](#)
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

[Actions](#) [Create folder](#) [Upload](#)

Name	Type	Last modified	Size	Storage class
No objects You don't have any objects in this bucket.				
Upload				

Amazon S3 > Buckets > awstestbucket-wsu > Upload

Upload [Info](#)

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

All files and folders in this table will be uploaded.

[Remove](#) [Add files](#) [Add folder](#)

Files and folders (0)
All files and folders in this table will be uploaded.

Name	Folder
No files or folders You have not chosen any files or folders to upload.	

Destination [Info](#)

Destination
<s3://awstestbucket-wsu>

▶ **Destination details**
Bucket settings that impact new objects stored in the specified destination.

▶ **Permissions**
Grant public access and access to other AWS accounts.

▶ **Properties**
Specify storage class, encryption settings, tags, and more.

[Cancel](#) [Upload](#)

Amazon S3 > Buckets > awstestbucket-wsu > Upload

Upload [Info](#)

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

All files and folders in this table will be uploaded.

[Remove](#) [Add files](#) [Add folder](#)

Files and folders (1 Total, 4.0 KB)
All files and folders in this table will be uploaded.

Name	Folder
AWSS3-GUIDE.txt	-

Destination [Info](#)

Destination
<s3://awstestbucket-wsu>

▶ **Destination details**
Bucket settings that impact new objects stored in the specified destination.

▶ **Permissions**
Grant public access and access to other AWS accounts.

▶ **Properties**
Specify storage class, encryption settings, tags, and more.

[Cancel](#) [Upload](#)

Upload: status

[Upload succeeded](#)
View details below.

The information below will no longer be available after you navigate away from this page.

Summary

Destination	Succeeded	Failed
s3://awstestbucket-wsu	1 file, 4.0 KB (100.00%)	0 files, 0 B (0%)

[Files and folders](#) [Configuration](#)

Files and folders (1 Total, 4.0 KB)

Name	Folder	Type	Size	Status
AWSS3-GUIDE.txt	-	text/plain	4.0 KB	Succeeded

Amazon S3 > Buckets > awstestbucket-wsu

awstestbucket-wsu [Info](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

Objects (1) [Info](#)
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

[Actions](#) [Create folder](#) [Upload](#)

Name	Type	Last modified	Size	Storage class
AWSS3-GUIDE.txt	txt	June 20, 2024, 04:18:37 (UTC-04:00)	4.0 KB	Standard

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".

The figure consists of three vertically stacked screenshots of the AWS S3 console interface, illustrating the process of enabling Bucket Versioning for the 'awstestbucket-wsu' bucket.

Screenshot 1: Bucket Properties
Shows the 'Properties' tab selected in the navigation bar. The 'Objects' section displays one object named 'AWS3-GUIDE.txt' with details like Name, Type (txt), Last modified (June 20, 2024, 04:18:37 (UTC-04:00)), Size (4.0 KB), and Storage class (Standard). A purple circle highlights the 'Properties' tab.

Screenshot 2: Bucket Overview
Shows the 'Bucket overview' section. It includes details such as AWS Region (US East (N. Virginia) us-east-1), ARN (arn:aws:s3:::awstestbucket-wsu), and Creation date (June 20, 2024, 04:07:55 (UTC-04:00)). The 'Bucket Versioning' section is visible, showing that Versioning is currently Disabled. A purple circle highlights the 'Edit' link next to the Versioning status.

Screenshot 3: Edit Bucket Versioning
Shows the 'Edit Bucket Versioning' dialog. The 'Bucket Versioning' section contains two options: 'Suspend' (which suspends creation of object versions) and 'Enable' (which is selected). A purple circle highlights the 'Enable' button. Below it, a callout box provides a note: 'After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.' The 'Multi-factor authentication (MFA) delete' section is also visible, showing that MFA delete is Disabled. At the bottom right, there are 'Cancel' and 'Save changes' buttons, with 'Save changes' being highlighted by a purple circle.

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".

The screenshot shows the AWS S3 console after a successful upload. At the top, a green bar indicates "Upload succeeded" with a link to "View details below". Below this, a summary table shows the destination as "s3://awstestbucket-wsu" and the status as "Succeeded" with "1 File, 4.0 KB (100.00%)". There is also a "Failed" section showing "0 files, 0 B (0%)". The "Files and folders" tab is selected, displaying a table with one item: "AWS3-GUIDE.txt" (Type: text/plain, Size: 4.0 KB, Status: Succeeded). A "Find by name" search bar is at the top of the table.

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.

The three screenshots illustrate the viewing of object versions for "AWS3-GUIDE.txt".
1. The first screenshot shows the "Objects" tab for the bucket "awstestbucket-wsu". It lists one object, "AWS3-GUIDE.txt", with its properties: Type: txt, Last modified: June 20, 2024, 04:19:17 (UTC-04:00), and Storage class: Standard. A purple circle highlights the "Show versions" checkbox in the top right of the table header.
2. The second screenshot shows the "Properties" tab for the object "AWS3-GUIDE.txt". It has tabs for "Properties", "Permissions", and "Versions". A purple circle highlights the "Versions" tab.
3. The third screenshot shows the "Versions" tab for the object "AWS3-GUIDE.txt". It lists two versions:

- Version ID: #f505e028-140mWqJnGf9je3kJHNfc0 (Current version)
- Version ID: 4d (null)

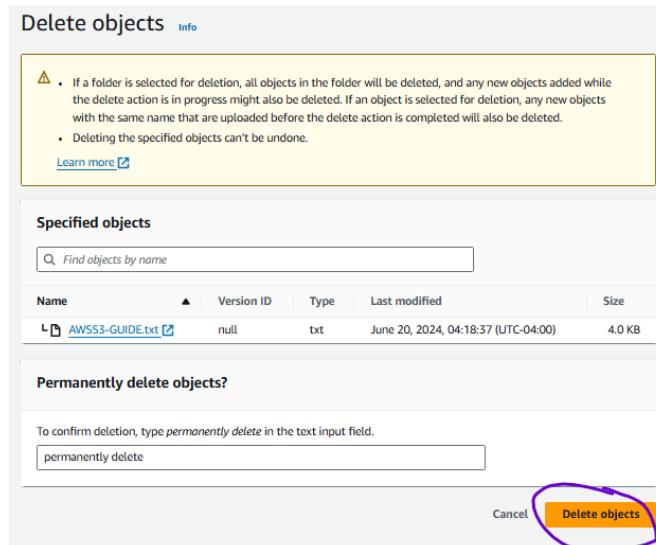
Both entries show the same last modified date and time: June 20, 2024, 04:19:17 (UTC-04:00). A purple circle highlights the "null" entry in the "Type" column.

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.



The screenshot shows the AWS S3 object details page for 'AWSS3-GUIDE.txt'. It displays two versions: the current version (Version ID: Dh5D...09) and a previous version (Version ID: D...). The 'Actions' dropdown menu is open, showing options like 'Download', 'Open', 'Delete', and 'Actions'.

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".

The screenshot shows the AWS S3 console interface for a bucket named 'awstestbucket-ws'. The 'Properties' tab is selected. In the 'Objects' section, there is one object named 'AWSS3-GUIDE.txt'. Below this, the 'Static website hosting' section is visible, with the 'Edit' button highlighted.

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

Disable

Enable

Hosting type

Host a static website

Use the bucket endpoint as the web address. [Learn more](#)

Redirect requests for an object

Redirect requests to another bucket or domain. [Learn more](#)

Index document

Specify the home or default page of the website.

index.html

Error document - optional

This is returned when an error occurs.

error.html

Redirection rules - optional

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

1

JSON Ln 1, Col 1 Errors: 0 Warnings: 0

Cancel 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".

Edit bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

```

1 * {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": "*",
7       "Action": "s3:GetObject",
8       "Resource": "arn:aws:s3:::awstestbucket-ws1/*"
9     }
10    {
11      "Effect": "Allow",
12      "Principal": "arn:aws:iam::123456789012:root",
13      "Action": "s3:ListBucket"
14    }
15  ]
16 }

```

+ Add new statement

Preview external access

Cancel **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.

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Enabled

Hosting type
Bucket hosting

Bucket website endpoint

When you enable static website hosting, AWS creates a new endpoint for the bucket's specific website endpoint of the bucket. [Learn more](#)

<http://awstestbucket-ws1.s3-website-us-east-1.amazonaws.com>

My Beautiful Static Website

Welcome to My Static Website

About This Site

This is a simple static website hosted on Amazon S3. It demonstrates how you can use HTML, CSS, and some simple styling to create a visually appealing webpage. Hosting static websites on S3 is cost-effective and scalable.

Features

Here are some features of this static website:

- Responsive Design
- Beautiful Styling
- Hosted on AWS S3
- Cool E-Recipes

Contact

Feel free to reach out for more information or collaboration opportunities:

- Email: george@georgebright.ted
- Phone: +1-234-567-690

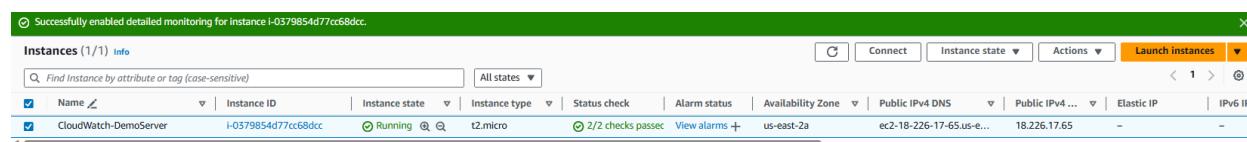
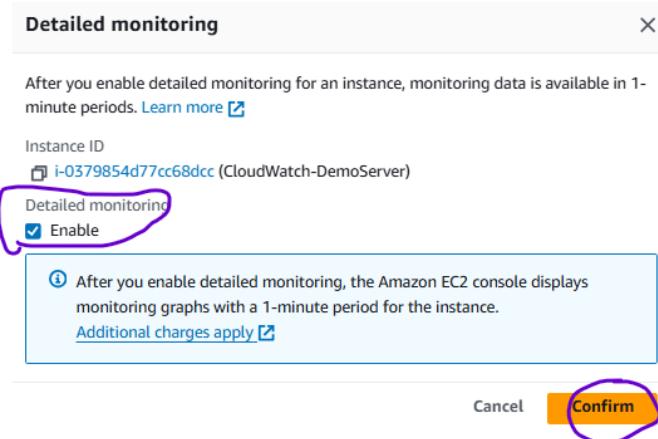
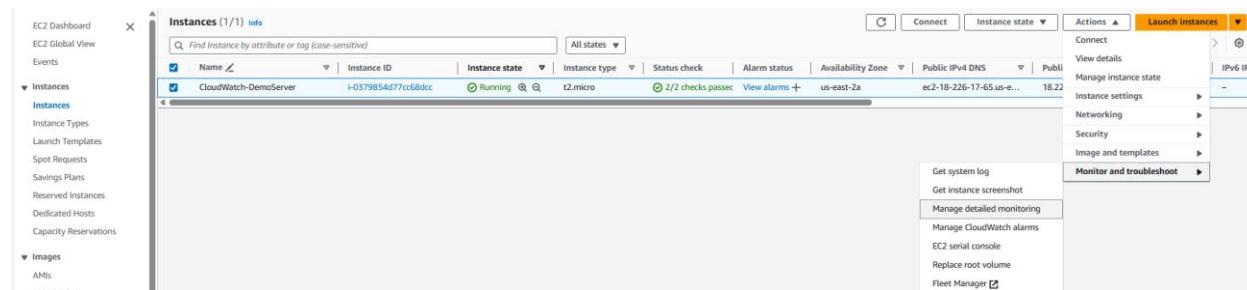
Implementing Cloud Watch Alarms

TASK – Deploy an EC2 Instance with Ubuntu AMI

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

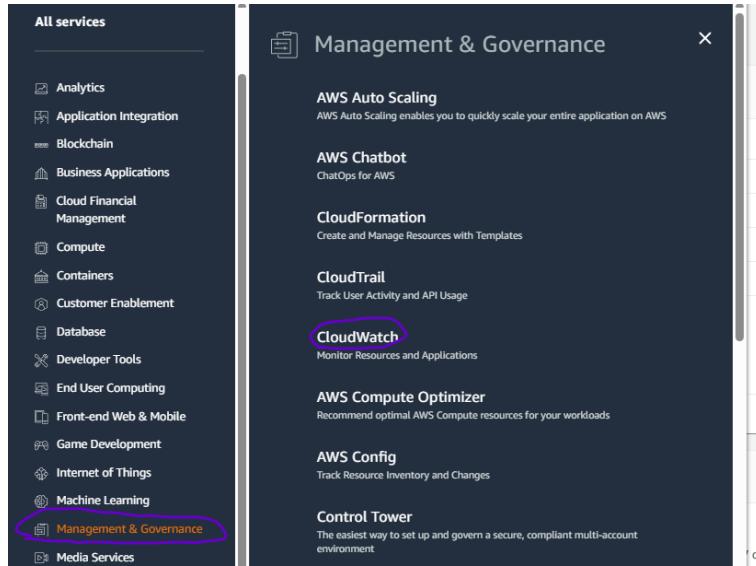
Detailed Monitoring provides more frequent monitoring of your EC2 instance's performance data. Follow these steps to enable it

- 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".

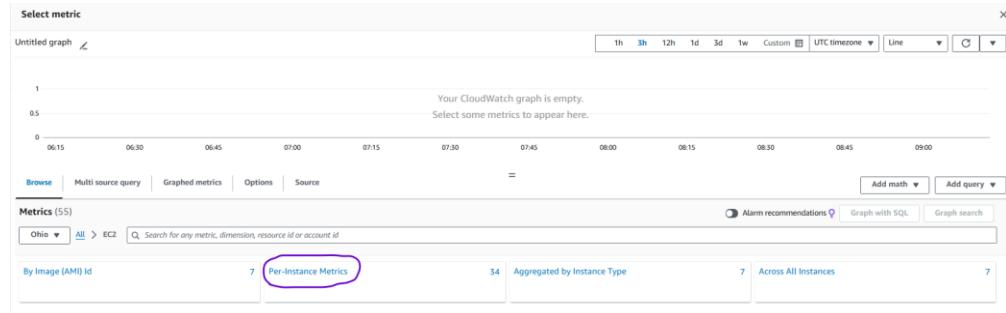
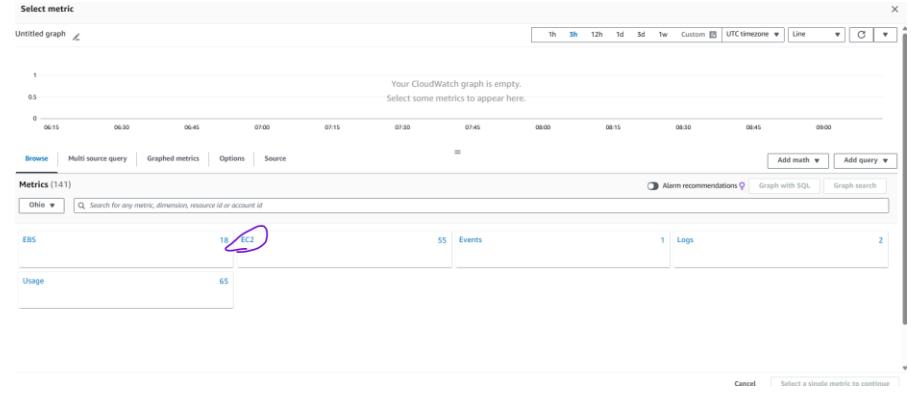
This screenshot shows the 'CloudWatch' service in the AWS Management Console. The left sidebar has 'Alarms' selected, indicated by a blue oval. The main area is titled 'CloudWatch Overview' and contains sections for getting started with CloudWatch alarms, metrics, and events. It also includes a 'Get started with Application Insights' section. At the top right, there are time range and filter options, and at the bottom right, a 'Create alarm' button.

This screenshot shows the 'Create alarm' step in the CloudWatch Alarms wizard. The left sidebar shows 'Alarms' selected. The main page title is 'CloudWatch > Alarms'. It features a search bar and filters for 'Alarm state', 'Alarm type', and 'Actions status'. A large 'Create alarm' button is prominently displayed at the top right. The main content area shows a message 'No alarms. No alarms to display.' and a 'Create alarm' button.

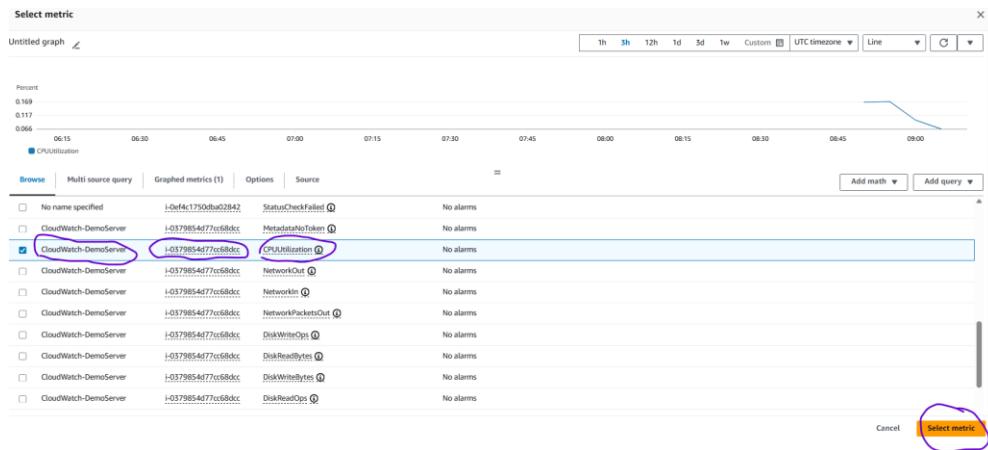
- Click on "Select metric".

This screenshot shows the 'Specify metric and conditions' step of the CloudWatch Alarms wizard. The left sidebar shows the steps: Step 1 (Specify metric and conditions), Step 2 (Configure actions), Step 3 (Add name and description), and Step 4 (Preview and create). The main area is titled 'Specify metric and conditions' and contains a 'Metric' section with a 'Graph' preview and a 'Select metric' button, which is circled in purple. At the bottom right are 'Cancel' and 'Next' buttons.

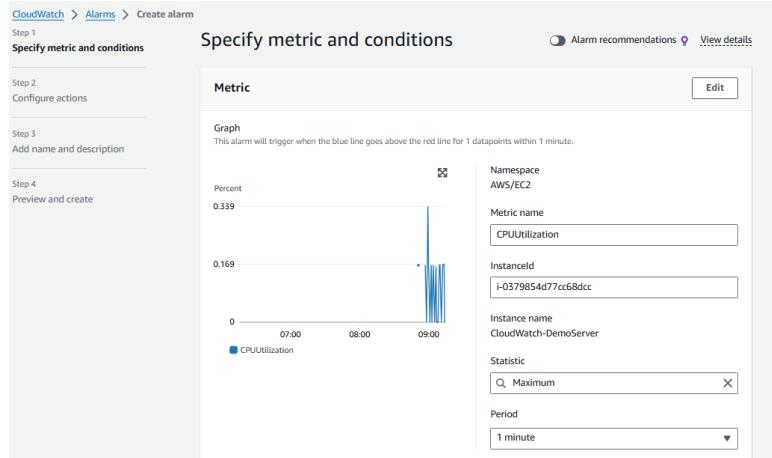
- In the "Browse" tab, choose "EC2" and then "Per-Instance Metrics".



- 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.

Conditions

Threshold type

Static
Use a value as a threshold

Anomaly detection
Use a band as a threshold

Whenever CPUUtilization is...

Define the alarm condition.

Greater
> threshold

Greater/Equal
>= threshold

Lower/Equal
<= threshold

Lower
< threshold

than...

Define the threshold value.

60

Must be a number

▶ Additional configuration

Cancel **Next**

- 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".

Configure actions

Notification

Alarm state trigger

Define the alarm state that will trigger this action.

In alarm
The metric or expression is outside of the defined threshold.

OK
The metric or expression is within the defined threshold.

Insufficient data
The alarm has just started or not enough data is available.

Remove

Create a new topic...

The topic name must be unique.

Default_CloudWatch_Alarms_Topic

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

Email endpoints that will receive the notification...

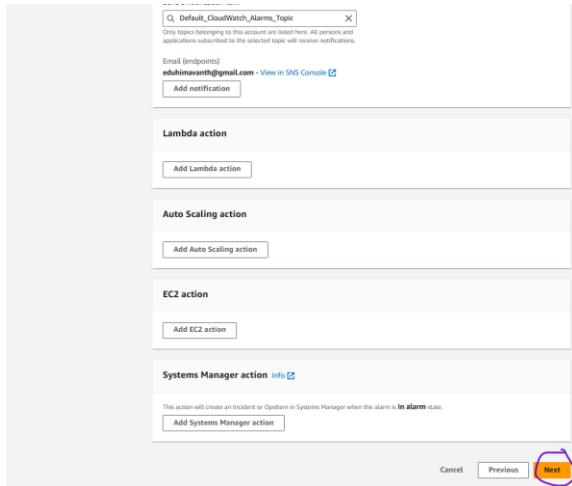
Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

eduhimavarth@gmail.com

user1@example.com, user2@example.com

Create topic

Add notification



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

CloudWatch > Alarms > Create alarm

Step 1
[Specify metric and conditions](#)

Step 2
[Configure actions](#)

Step 3
Add name and description

Step 4
Preview and create

Add name and description

Name and description

Alarm name

Alarm description - optional [View formatting guidelines](#)

Edit	Preview
Hello Team, This is an Automated Email from CloudWatch generated in the process of testing the CloudWatch Alarm Functionality.	
Up to 1024 characters (126/1024)	

ⓘ Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.

Cancel [Previous](#) **Next**

Step 3: Add name and description

[Edit](#)

Name and description

Name
CloudWatch-CPU-Monitoring-DemoServer

Description
Hello Team,
This is an Automated Email from CloudWatch generated in the process of testing the CloudWatch Alarm Functionality.

ⓘ Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.

Cancel [Previous](#) **Create alarm**

Successfully created alarm CloudWatch-CPU-Monitoring-DemoServer.

Some subscriptions are pending confirmation
Amazon SNS doesn't send messages to an endpoint until the subscription is confirmed

CloudWatch > Alarms

Alarms (1)

Search

Hide Auto Scaling alarms Clear selection Create composite alarm Actions

Name State Last state update (UTC) Conditions Actions

CloudWatch-CPU-Monitoring-DemoServer Insufficient data 2024-06-26 09:24:27 CPUUtilization >= 60 for 1 datapoints within 1 minute Actions enabled Warning

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.

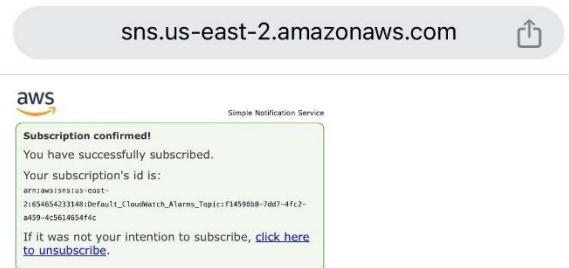
AWS Notification - Subscription Confirmation



You have chosen to subscribe to the topic:
arn:aws:sns:us-east-2:654654233148:Default_CloudWatch_Alarms_Topic

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
[Confirm subscription](#)

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to [sns-opt-out](#)



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)

```

ubuntu@ip-10-0-1-237:~$ 
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:~$ 

```

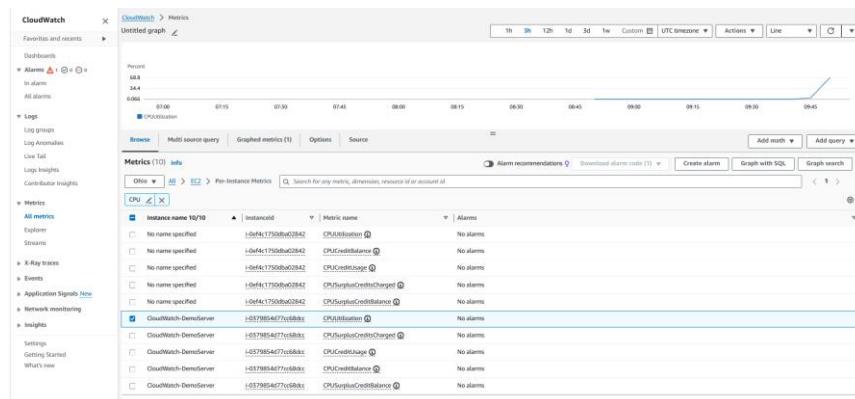
```

ubuntu@ip-10-0-1-237:~$ stress --cpu 8 --timeout 600
stress: info: [1743] dispatching hogs: 8 cpu, 0 io, 0 vm, 0 hdd

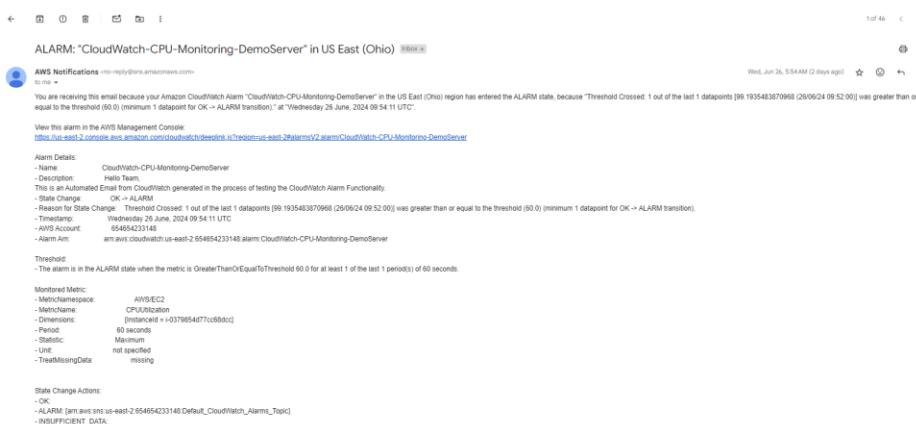
```

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.

The screenshot shows the AWS IAM Policies page. On the left, there's a navigation sidebar with 'Identity and Access Management (IAM)' selected. Under 'Access management', 'Policies' is highlighted and circled in red. At the top right, there's a 'Create policy' button, which is also circled in red.

The screenshot shows the 'Specify permissions' step of the IAM policy creation wizard. It displays a JSON editor containing the custom policy code shown above. A large curly brace is drawn over the JSON code to highlight it. On the right side of the screen, there's a 'Select a statement' panel with a 'Next' button at the bottom, which is circled in red.

IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Policy details

Policy name
Enter a meaningful name to identify this policy.
VPCFlowLogPolicy
Maximum 128 characters. Use alphanumeric and '+-,.,@-' characters.

Description - optional
Add a short explanation for this policy.
Maximum 1,000 characters. Use alphanumeric and '+-,.,@-' characters.

Permissions defined in this policy Info
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Service Access level Resource Request condition

CloudWatch Logs Limited: List, Write All resources None

Add tags - optional Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag You can add up to 50 more tags.

Cancel Previous **Create policy**

Identity and Access Management (IAM)

Policies (1219) Info

A policy is an object in AWS that defines permissions.

Policy name	Type	Used as	Description
VPCFlowLogPolicy	Customer managed	None	-

View 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)

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.

Role name	Trusted entities	Last activity
AWSBlue-AD-Role	AWS Service: ec2	24 days ago
AWSServiceRoleForAmazonSSM	AWS Service: ssm [Service-Linked Role]	1 hour ago
AWSServiceRoleForOrganizations	AWS Service: organizations [Service-Linked Role]	-
AWSServiceRoleForSSO	AWS Service: sso [Service-Linked Role]	4 hours ago
AWSServiceRoleForSupport	AWS Service: support [Service-Linked Role]	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor [Service-Linked Role]	-

Create role

IAM > Roles > Create role

Select trusted entity

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

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.

```
1 | {
2 |   "Version": "2012-10-17",
3 |   "Statement": [
4 |     {
5 |       "Sid": "Statement1",
6 |       "Effect": "Allow",
7 |       "Principal": "*",
8 |       "Service": "vpc-flow-logs.amazonaws.com",
9 |       "Action": "sts:AssumeRole"
10 |     }
11 |   ]
12 |
13 | }
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

Add new statement

IAM > Roles > Create role

Add permissions

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

Permissions policies (1/944) Info

Choose one or more policies to attach to your new role.

Policy name	Type	Description
VPCFlowLogPolicy	Customer managed	

Set permissions boundary - optional

Next

IAM > Roles > Create role

Name, review, and create

Step 1 Select trusted entities

Step 2 Add permissions

Step 3 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

The screenshot shows the AWS IAM Roles page. At the top, a green banner indicates 'Role VPCFlowLogCloudwatch created.' Below this, the 'Roles (7) Info' section displays a table of roles. One row, 'VPCFlowLogCloudwatch', is highlighted with a purple oval. The table columns include 'Role name', 'Trusted entities', and 'Last activity'. The 'Create role' button is located at the top right of the table.

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'.

The screenshot shows the CloudWatch Log groups page. The left navigation pane includes 'Log groups' under 'Logs'. The main area shows a table with one entry: 'No log groups'. A message says 'You have not created any log groups.' Below the table is a 'Create log group' button, which is circled in purple.

The screenshot shows the 'Create log group' wizard. The first step, 'Log group details', has a sub-section titled 'Log group name' with the value 'AWSBlue-FlowLog'. It also includes 'Retention setting' (set to 'Never expire'), 'Log class' (set to 'Standard'), and a 'KMS key ARN - optional' field. Below this is a 'Tags' section with a note about tags and an 'Add new tag' button. The 'Create' button at the bottom is circled in purple.

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.

Your VPCs (1/3) Info

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table
AWS-Green	vpc-02d10c8a100debe2	Available	10.1.0.0/16	-	dopt-062902195e8db...	rtb-02ff4f790e7d43302
AWSBlue	vpc-0d7b781c02c081d9f	Available	10.0.0.0/16	-	dopt-062902195e8db...	rtb-09823586931b8b7
	vpc-06f0f4fc0c0873395	Available	172.31.0.0/16	-	dopt-062902195e8db...	rtb-0af0b00388f5282cf7

Create flow log Info

Flow logs can capture IP traffic flow information for the network interfaces associated with your resources. You can create multiple flow logs to send traffic to different destinations.

Selected resources Info

Name	Resource ID	State
AWSBlue	vpc-0d7b781c02c081d9f	Available

Flow log settings

Name - optional: AWSBlue-FlowLog

Filter: All

Maximum aggregation interval: 1 minute

Destination: Send to CloudWatch Logs

Destination log group: AWSBlue-FlowLog

IAM role: VPCFlowLogCloudwatch

Log record format: AWS default format

Additional metadata: \${version} \${account-id} \${interface-id} \${srcaddr} \${dstaddr} \${srcport} \${dstport} \${protocol} \${packets} \${bytes} \${start} \${end} \${action} \${log-status}

Format preview: \${version} \${account-id} \${interface-id} \${srcaddr} \${dstaddr} \${srcport} \${dstport} \${protocol} \${packets} \${bytes} \${start} \${end} \${action} \${log-status}

Tags: Name: AWSBlue-FlowLog

Create flow log

The screenshot shows the AWS VPC dashboard. In the top navigation bar, there is a success message: "Successfully created flow log for vpc-0d7b781c02c081d9f". Below this, the "Your VPCs (1/3) Info" table lists one VPC: AWSBlue (vpc-0d7b781c02c081d9f). The "Flow logs" tab is selected, showing a single entry for "awsblue-flowlog" with the status circled in green as "Active".

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.

The screenshot shows the AWS CloudWatch Log Groups page. The left sidebar has a "Logs" section with a "Log groups" button highlighted with a red circle. The main area shows a table of log groups, with "AWSBlue-FlowLog" highlighted with a red circle. The table includes columns for Log group, Log class, Anomaly detection, Data protection, Sensitive data count, Retention, Metric filters, and Contributor insights. A "Configure" button is also visible for the selected log group.

The screenshot shows the AWS CloudWatch Log Groups interface. On the left, a sidebar navigation includes: CloudWatch, Favorites and recent, Dashboards, Alarms, Logs (Log groups, Log Anomalies, Live Tail, Logs Insights, Contributor Insights), Metrics (All metrics, Explorer, Streams), X-Ray traces, Events (Rules, Event Buses), Application Signals (New), Network monitoring, and Insights.

The main pane displays the AWSBlue-FlowLog log group details. It shows the Log class (Info, Standard), ARN (arn:aws:logs:us-east-2:654654233148:log-group:AWSBlue-FlowLog:*), Creation time (20 minutes ago), Retention (Never expire), and Stored bytes (~). Metric filters, Subscription filters, Contributor Insights rules, and KMS key ID are listed under Log group details. Anomaly detection, Data protection, and Sensitive data count are also shown.

The Log streams tab is selected, displaying a list of log streams. One entry, "eni-0e3b338d5fd383512-all", is highlighted with a purple oval. The list includes columns for Log stream, Last event time (2024-06-29 18:38:53 (UTC)), and Actions.

The second screenshot shows the AWS CloudWatch Log Events interface for the eni-0e3b338d5fd383512-all log stream. It lists several log events with timestamp, message, and source information. The interface includes a search bar, filter patterns, and a timeline for event times.

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."

The screenshot shows the CloudWatch Log Groups page. On the left, the navigation pane has 'Logs' expanded, with 'Log groups' selected. A purple circle highlights the 'Log groups' link. In the main content area, there is a table titled 'Log groups (1/1)'. A single row is shown for 'AWSBlue-FlowLog', which is also highlighted with a purple circle. The 'Actions' dropdown menu on the right is open, and the 'Export data to Amazon S3' option is circled in purple.

The screenshot shows the 'Create export task' dialog. It has two main sections: 'Define data export' and 'Choose S3 bucket'. In the 'Define data export' section, the 'Time range' is set from '2024-06-28T19:12:08' to '2024-06-29T19:12:08' in 'UTC timezone'. The 'Stream prefix - optional' field is empty. In the 'Choose S3 bucket' section, 'This account' is selected, and the 'S3 bucket name' field contains 'awsblue-vpcflowlogs'. The 'S3 bucket prefix - optional' field is empty. At the bottom, the 'Export' button is highlighted with a purple circle. A green success message box on the right states 'Successfully created export task. Task Id: 19067169-ff55-49be-a0cb-b7e36aca0b0e'.

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

Amazon S3

Amazon S3

General purpose buckets (1) info All AWS Regions

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
awsblue-vpcflowlogs	US East (Ohio) us-east-2	View analyzer for us-east-2	June 29, 2024, 14:50:51 (UTC-04:00)

[Create bucket](#)

Amazon S3

Amazon S3 > Buckets > awsblue-vpcflowlogs

awsblue-vpcflowlogs info

Objects (2) info

Name	Type	Last modified	Size	Storage class
aws-logs-write-test	Folder	June 29, 2024, 15:13:54 (UTC-04:00)	-	-
exportedlogs/	Folder	-	-	-

Amazon S3

Amazon S3 > Buckets > awsblue-vpcflowlogs > exportedlogs/

exportedlogs/

Objects (2) info

Name	Type	Last modified	Size	Storage class
19067169-ff55-49be-a0cb-b7e56aca0b0e/	Folder	-	-	-
b84b6024b-d4cf-4c16-a844-53236a9f675/	Folder	-	-	-

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)

Instances (2) Info										
Find Instance by attribute or tag (case-sensitive) All states										
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
□	Web-Server-2	i-0fc4cfcd34508ea7	Running Q Q	t2.micro	2/2 checks passed	View alarms +	us-east-2b	ec2-3-19-123-217.us-e...	3.19.123.217	-
□	Web-Server-1	i-06939bb11870d25f6	Running Q Q	t2.micro	2/2 checks passed	View alarms +	us-east-2a	ec2-18-221-13-146.us-...	18.221.13.146	-

TASK – Install Apache2 Webserver in both the Instances

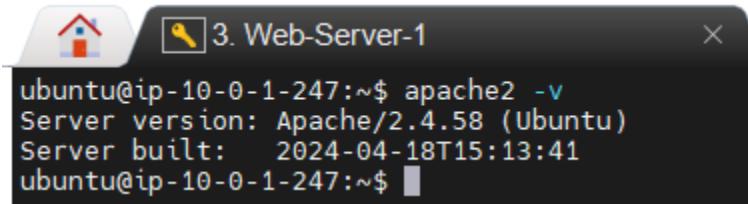
Note: Visit my GIT repo to get the commands used for installing the Apache webserver in ubuntu.

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.

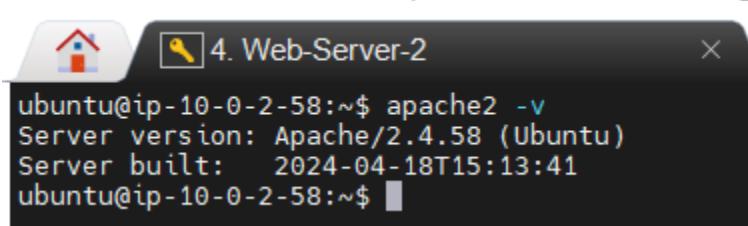
```
apache2 -v
```

Web-Server-1:



```
ubuntu@ip-10-0-1-247:~$ apache2 -v
Server version: Apache/2.4.58 (Ubuntu)
Server built:   2024-04-18T15:13:41
ubuntu@ip-10-0-1-247:~$
```

Web-Server-2:



```
ubuntu@ip-10-0-2-58:~$ apache2 -v
Server version: Apache/2.4.58 (Ubuntu)
Server built:   2024-04-18T15:13:41
ubuntu@ip-10-0-2-58:~$
```

- 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 –

```
ubuntu@ip-10-0-1-247:~$ apache2 -v
Server version: Apache/2.4.58 (Ubuntu)
Server built:   2024-04-18T15:13:41
ubuntu@ip-10-0-1-247:~$ sudo su -
root@ip-10-0-1-247:~#
```

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

```
ubuntu@ip-10-0-1-247:~$ apache2 -v
Server version: Apache/2.4.58 (Ubuntu)
Server built:   2024-04-18T15:13:41
ubuntu@ip-10-0-1-247:~$ sudo su -
root@ip-10-0-1-247:~# cd /var/www/html
root@ip-10-0-1-247:/var/www/html#
```

- Edit the default HTML file.
vi index.html

```
ubuntu@ip-10-0-1-247:~$ apache2 -v
Server version: Apache/2.4.58 (Ubuntu)
Server built:   2024-04-18T15:13:41
ubuntu@ip-10-0-1-247:~$ sudo su -
root@ip-10-0-1-247:~# cd /var/www/html
root@ip-10-0-1-247:/var/www/html# vi index.html
```

- Replace "Apache2 Default Page" with "Web-Server-1".

Note: Press "i" to add or remove data into the HTML file

```
</head>
<body>
  <div class="main_page">
    <div class="page_header floating_element">
      
    <div>
      <span style="margin-top: 1.5em;" class="floating_element">
        Apache2 Default Page
      </span>
    </div>
    <div class="banner">
      <div id="about"></div>
      It works!
    </div>
  </div>
```

```
</head>
<body>
  <div class="main_page">
    <div class="page_header floating_element">
      
    <div>
      <span style="margin-top: 1.5em;" class="floating_element">
        Web-Server-1
      </span>
    </div>
    <div class="banner">
      <div id="about"></div>
      It works!
    </div>
  </div>
```

- Save and exit the editor.

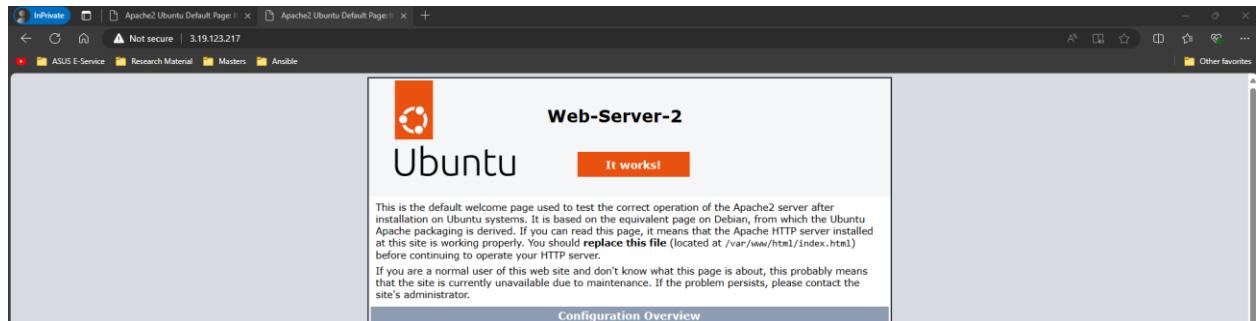
Note: Press esc button followed by :wq! And hit enter to save and exit the editor

```
ubuntu@ip-10-0-1-247:~$ apache2 -v
Server version: Apache/2.4.58 (Ubuntu)
Server built:   2024-04-18T15:13:41
ubuntu@ip-10-0-1-247:~$ sudo su -
root@ip-10-0-1-247:~# cd /var/www/html
root@ip-10-0-1-247:/var/www/html# vi index.html
root@ip-10-0-1-247:/var/www/html#
```

- 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:

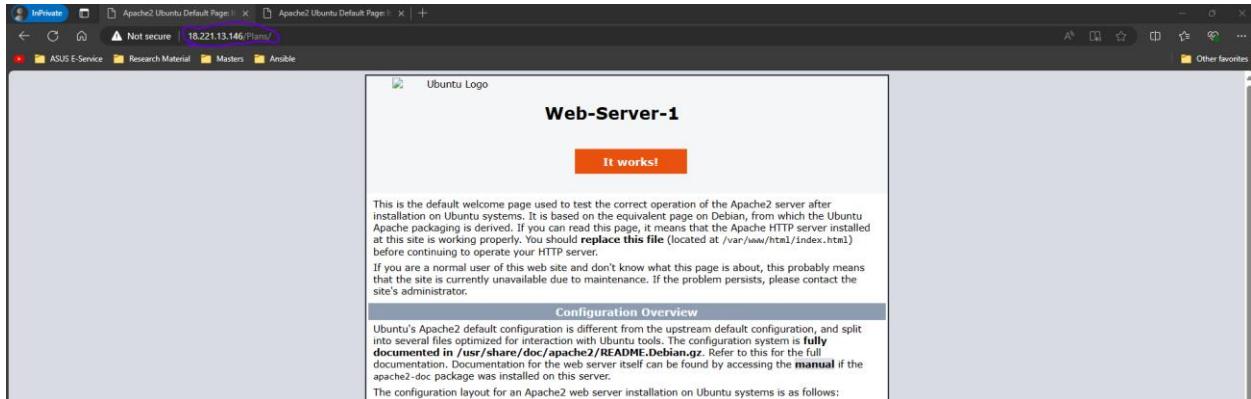
- Under /var/www/html, Create a folder “Plans”
- Move all the file present under /var/www/html into /var/www/html/Plans

```

root@ip-10-0-1-247:/var/www/html# mkdir Plans
root@ip-10-0-1-247:/var/www/html# mv index.html Plans/
root@ip-10-0-1-247:/var/www/html#

```

- 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

```

root@ip-10-0-2-58:/var/www/html# mkdir Payments
root@ip-10-0-2-58:/var/www/html# mv index.html Payments/
root@ip-10-0-2-58:/var/www/html#

```

- 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.

The screenshot shows the AWS EC2 Target Groups page. On the left, there's a sidebar with various AWS services like S3, Lambda, and CloudWatch. The 'Target Groups' section is highlighted with a purple oval. In the main content area, there's a table header for 'Target groups' with columns for Name, ARN, Port, Protocol, Target type, Load balancer, and VPC ID. Below the table, it says 'No target groups' and has a 'Create target group' button. A small modal window titled '0 target groups selected' is open at the bottom, with the instruction 'Select a target group above.'

This is a step-by-step configuration wizard. The first step, 'Choose a target type', has four options: 'Instances' (selected), 'IP addresses', 'Lambda function', and 'Application Load Balancer'. Each option has a list of benefits. The 'Instances' section includes a note about managing EC2 capacity via Auto Scaling. The 'Protocol' dropdown is set to 'HTTP' and the 'Port' is '80'. The 'Target group name' is 'ALB-TG'. The 'Attributes' section notes that certain defaults apply. The 'Tags - optional' section is shown at the bottom right. The 'Next Step' button is highlighted with a purple oval.

Step 1
Specify group details

Step 2
Register targets

Available instances (2/2)

Instance ID	Name	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
i-0fc4cfcb3450bea7	Web-Server-2	Running	AWSBlue-All-Traffic-SG	us-east-2b	10.0.2.58	subnet-0b75b690811d9c47a	July 1, 2024, 16:06
i-06939bb11870d25f6	Web-Server-1	Running	AWSBlue-All-Traffic-SG	us-east-2a	10.0.1.247	subnet-01c328979166043eb	July 1, 2024, 16:05

2 selected

Ports for the selected instances:
80 - 40335 (selected) 80-40335 (not selected)

Include as pending below

Review targets

Targets (0)

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
-------------	------	------	-------	-----------------	------	----------------------	-----------	-------------

No instances added yet
Specify instances above, or delete the group empty if you prefer to add targets later.

0 pending

Cancel Previous **Create target group**

Review targets

Targets (2)

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
i-0fc4cfcb3450bea7	Web-Server-2	80	Running	AWSBlue-All-Traffic-SG	us-east-2b	10.0.2.58	subnet-0b75b690811d9c47a	July 1, 2024, 16:06 (UTC-04:00)
i-06939bb11870d25f6	Web-Server-1	80	Running	AWSBlue-All-Traffic-SG	us-east-2a	10.0.1.247	subnet-01c328979166043eb	July 1, 2024, 16:05 (UTC-04:00)

2 pending

Cancel Previous **Create target group**

Successfully created the target group ALB-TG. Anomaly detection is automatically applied to all registered targets. Results can be viewed in the Targets tab.

ALB-TG

Details

Target type: Instance Protocol: Port: HTTP: 80 Protocol version: HTTP/1 VPC: [vpcl-027b791c02010ff2](#)

Total targets	Healthy	Unhealthy	Unused	Initial	DRAINING
2	2	0	0	0	0

Distribution of targets by Availability Zone (AZ)

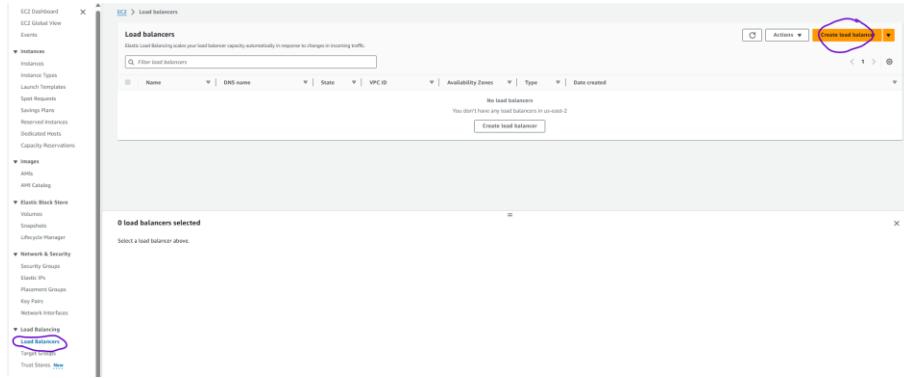
Registered targets (2) info

Instance ID	Name	Port	Zone	Health status	Health status details	Launch time	Anomaly detection result
i-0fc4cfcb3450bea7	Web-Server-2	80	us-east-2b	Unhealthy	Target group is not co... July 1, 20...	July 1, 20...	Normal
i-06939bb11870d25f6	Web-Server-1	80	us-east-2a	Unhealthy	Target group is not co... July 1, 20...	July 1, 20...	Normal

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".



Compare and select load balancer type

A complete feature-by-feature comparison along with detailed highlights is also available. [Learn more](#)

Load balancer types

Application Load Balancer	Network Load Balancer	Gateway Load Balancer
Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.	Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.	Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.
Create	Create	Create

Classic Load Balancer - previous generation

[Close](#)

[EC2 > Load balancers > Create Application Load Balancer](#)

Create Application Load Balancer

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

How Application Load Balancers work

Basic configuration

Load balancer name
Name must be unique within your AWS account and can't be changed after the load balancer is created.
 ALB-WebServers

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme
Scheme can't be changed after the load balancer is created.

Internet-facing
An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#)

Internal
An internal load balancer routes requests from clients to targets using private IP addresses. Compatible with the IPv4 and Dualstack IP address types.

Load balancer IP address type
Select the type of IP addresses that your subnets use: Public IPv4 addresses have an additional cost.

IPv4
Includes only IPv4 addresses.

Dualstack
Includes IPv4 and IPv6 addresses.

Dualstack without public IPv4
Includes a public IPv4 address, and private IPv4 and IPv6 addresses. Compatible with [internet-facing](#) load balancers only.

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-0b5b690811d9c47a 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

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

Protocol	Port	Default action
HTTP	: 80	Forward to ALB-TG Create target group
1-65535		

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	Security groups	Network mapping	Listeners and routing
ALB-WebServers • Internet-facing • IPv4	AWSBlue-All-Traffic-SG sg-0dabf1915374ee5d9	VPC vpc-0d7b781c02c081d9f AWSBlue us-east-2a subnet-01c328979166043eb AWSBlue-Subnet1-Public us-east-2b subnet-0b5b690811d9c47a AWSBlue-Subnet2-Public	HTTP:80 defaults to ALB-TG

Service integrations

AWS WAF: None
AWS Global Accelerator: None

Tags

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**

Successfully created load balancer: ALB-WebServers

It might take a few minutes for your load balancer to fully set up and route traffic. Targets will also take a few minutes to complete the registration process and pass initial health checks.

[EC2](#) > [Load balancers](#) > ALB-WebServers

ALB-WebServers

[Actions](#)

Details

Load balancer type Application	Status Provisioning	VPC vpc-0d7b781c02:081d9f1	Load balancer IP address type IPv4
Scheme Internet-facing	Hosted zone Z3AADJGX6KTTL2	Availability Zones subnet-01c328979166043eb us-east-2a (use2-az1) subnet-0b75b690811d9c47a us-east-2b (use2-az2)	Date created July 1, 2024, 21:26 (UTC-04:00)
Load balancer ARN arn:aws:elasticloadbalancing:us-east-2:654654233148:loadbalancer/app/ALB-WebServers/3fe6ff7991b46376	DNS name Info ALB-WebServers-1902282845.us-east-2.elb.amazonaws.com (A Record)		

[Listeners and rules](#) | [Network mapping](#) | [Resource map - new](#) | [Security](#) | [Monitoring](#) | [Integrations](#) | [Attributes](#) | [Tags](#)

Listeners and rules (1) Info

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

Protocol/Port	Default action	Rules	ARN	Security policy	Default SSL/TLS certificate	mTLS	Trust store	Tags
HTTP-80	Forward to target group • ALB-TG (100%) • Target group stickiness: Off	1 rule	ARN	Not applicable	Not applicable	Not applicable	Not applicable	0 tags

[EC2](#) > [Load balancers](#)

Load balancers (1)

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

[Actions](#) | [Create load balancer](#)

Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
ALB-WebServers	ALB-WebServers-1902282...	Active	vpc-0d7b781c02:081...	2 Availability Zones	application	July 1, 2024, 21:26 (UTC-04:00)

[Targets](#) | [Monitoring](#) | [Health checks](#) | [Attributes](#) | [Tags](#)

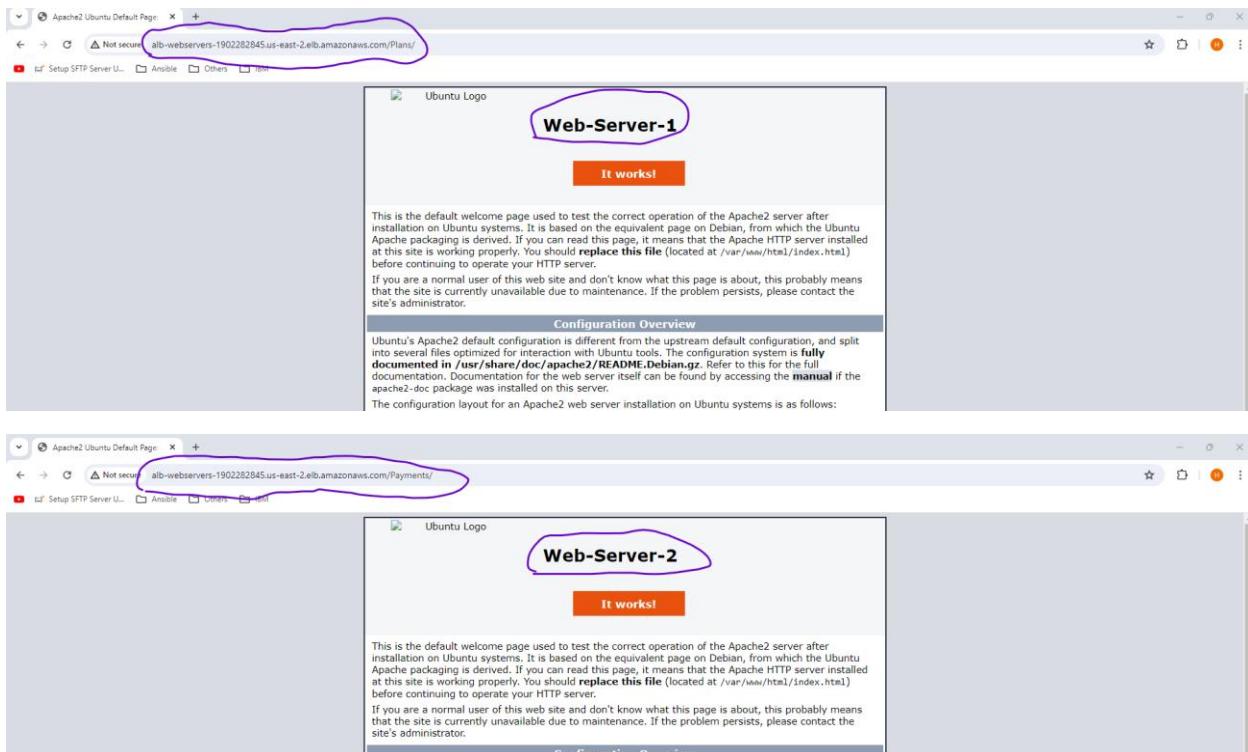
Registered targets (2) Info

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

Instance ID	Name	Port	Zone	Health status	Health status details	Launch...	Anomaly detection result
i-0fc4cfdb34508ea7	Web-Server-2	80	us-east-2b	Healthy	-	July 1, 20...	Normal
i-06939b0a11870d25f	Web-Server-1	80	us-east-2a	Healthy	-	July 1, 20...	Normal

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:
- ' [will route traffic to 'Web-Server-2'.](http://<ALB_DNS_Name>/plans' will route traffic to 'Web-Server-1'.</p>
<p>'<a href=)



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.

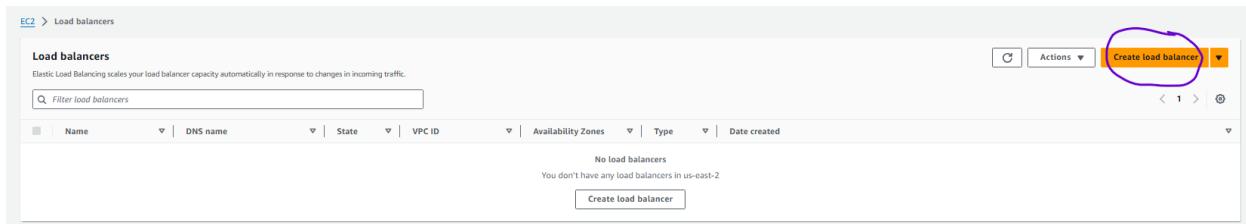
Demonstrating the functionality of AWS Network Load Balancer (NLB)

TASKS

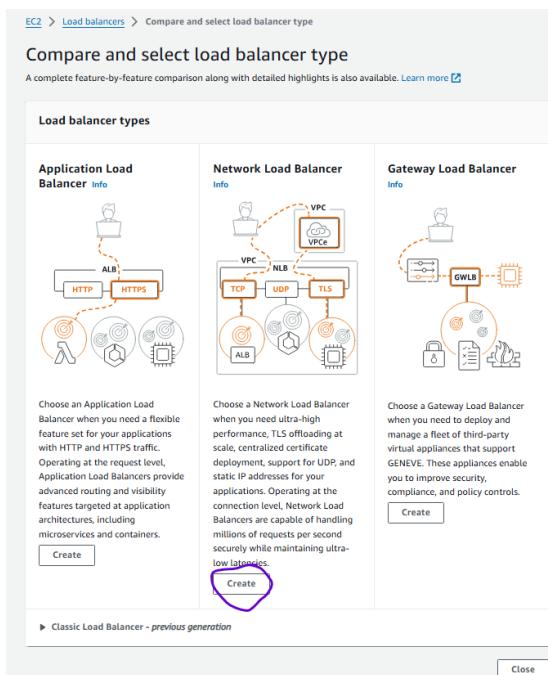
- Deploy 2 EC2 Instances (Ubuntu) i.e., Web-Server-1 & Web-Server-2
 - Install Apache2 in both the system and start Apache2
 - Access the Webservers using its respective URL's i.e., (<http://publicipoftheinstance>) to confirm the Apache2 installation and working.
 - Create a Target Group and register 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):

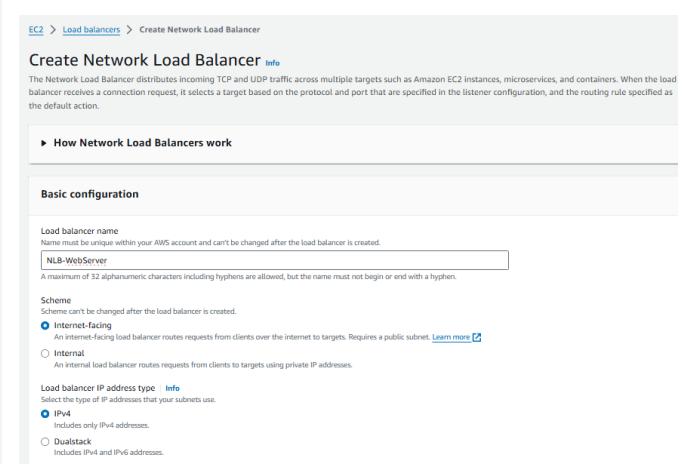
- In the AWS Management Console, go to the EC2 Dashboard.
- Select "Load Balancers" from the sidebar and click on "Create Load Balancer".
- Choose "Network Load Balancer".
- Set the "Name" for your NLB.
- For "Scheme", select "Internet-facing" if you want the NLB to be accessible from the internet.
- 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".



The screenshot shows the AWS EC2 Load Balancers page. At the top right, there is a yellow button labeled "Create load balancer" with a circled arrow around it. Below the button, there is a message: "No load balancers" and "You don't have any load balancers in us-east-1". At the bottom of the page, there is a "Create load balancer" button.



The screenshot shows the "Compare and select load balancer type" page. It compares three types: Application Load Balancer, Network Load Balancer, and Gateway Load Balancer. The "Network Load Balancer" section is highlighted with a circled arrow around its "Create" button. Below the comparison table, there is a note about the "Classic Load Balancer - previous generation" and a "Close" button.



The screenshot shows the "Create Network Load Balancer" configuration page. Under the "Basic configuration" section, the "Scheme" dropdown is set to "Internet-facing" (radio button selected). Other options include "Internal" and "Dualstack". Below the scheme, there is a "Load balancer IP address type" section with "IPv4" selected. A note says "Includes only IPv4 addresses." and "Dualstack" is also listed. At the bottom, there are "Next Step" and "Close" buttons.

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	<input type="button" value="Edit"/>
--	-------------------------------------

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-a21)
Subnet
 AWSBlue-Subnet1-Public

IPv4 address
 Assigned by AWS Use an Elastic IP address

us-east-2b (use2-a22)
Subnet
 AWSBlue-Subnet2-Public

IPv4 address
 Assigned by AWS Use an Elastic IP address

us-east-2c (use2-a23)

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	<input type="button" value="Edit"/>
--------------------------------	-------------------------------------

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	<input type="button" value="Remove"/>
Protocol: TCP Port: 80 1-65535	Default action: Info Forward to: NLB-TG Target type: Instance, IPv4 TCP <input type="button" value="Edit"/>

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.

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.

Load balancers (1/1)						
Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.						
<input type="checkbox"/> <input type="text"/> Filter load balancers						
Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
NLB-WebServer	NLB-WebServer-4a65983359de9ca5.elb.us-east-2.amazonaws.com	Active	vpc-0d7b781c02c081...	2 Availability Zones	network	July 1, 2024, 21:55 (UTC-04:00)

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.

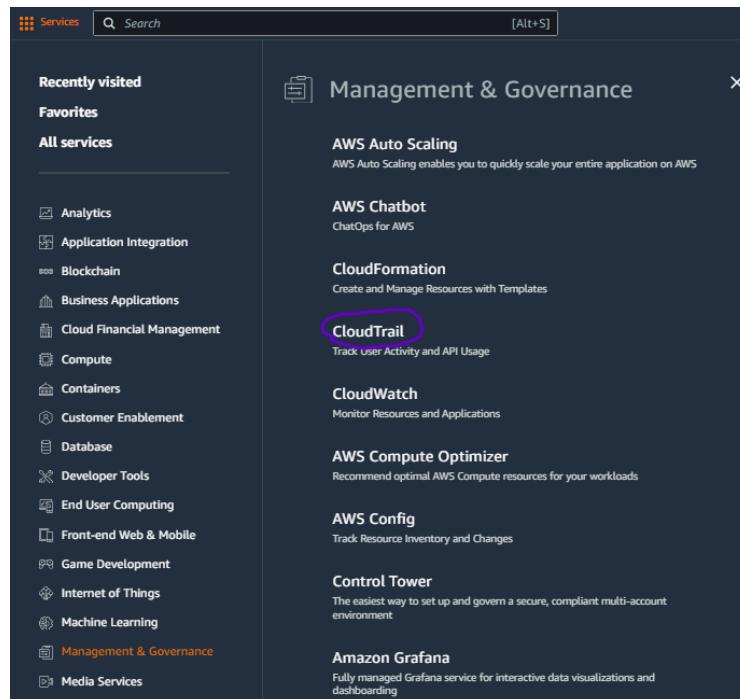


Note: An AWS Network Load Balancer (NLB) distributes incoming network traffic across multiple EC2 instances, ensuring high performance and low latency. It operates at Layer 4 (transport layer) of the OSI model, handling millions of requests per second. NLB supports static IP addresses and performs health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

- 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.



Management & Governance

AWS CloudTrail

Continuously log your AWS account activity

Use CloudTrail to meet your governance, compliance, and auditing needs for your AWS accounts.

[Create a trail with AWS CloudTrail](#)

Pricing

[CloudTrail](#) > Quick trail create

Quick trail create

Trail details

Start logging management events by creating a trail with simplified settings. Logs are sent to an S3 bucket we create on your behalf. To choose a different bucket or additional events, go to the full [Create trail](#) workflow.

A trail created in the console is a multi-region trail. [Learn more](#)

Trail name
Enter a display name for your trail.

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

Trail log bucket and folder

Logs will be stored in `aws-cloudtrail-logs-654654233148-b90edfa4/AWSLogs/654654233148`

ⓘ Though there is no cost to log these events, you incur charges for the S3 bucket that we create to store your logs.

[Cancel](#) [Create trail](#)

[CloudTrail](#) > Trails

Name	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
<input checked="" type="radio"/> management-events	US East (Ohio)	Yes	Disabled	No	aws-cloudtrail-logs-654654233148-b90edfa4			

[Copy events to Lake](#) [Edit](#) [Delete](#) [Create trail](#)

[CloudTrail](#) > [Trails](#) > [arn:aws:cloudtrail:us-east-2:654654233148:trail/management-events](#)

management-events

[Delete](#) [Stop logging](#)

[Edit](#)

General details

Trail logging 	Trail log location <code>aws-cloudtrail-logs-654654233148-b90edfa4/AWSLogs/654654233148</code>	Last log file delivered 8	SNS notification delivery Disabled
Trail name management-events	Log file validation Disabled	Last file validation delivered -	Last SNS notification -
Multi-region trail Yes	Log file SSE-KMS encryption Not enabled		
Apply trail to my organization Not enabled			

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.

The screenshot shows the 'General details' section of a CloudTrail configuration. The 'Trail log location' field is highlighted with a purple oval, showing the path: 'aws-cloudtrail-logs-654654233148-b90edfa4/AWSLogs/654654233148/'. Other fields include 'Trail name: management-events', 'Multi-region trail: Yes', 'Apply trail to my organization: Not enabled', 'Log file validation: Disabled', 'Last file validation delivered: -', 'SNS notification delivery: Disabled', and 'Last SNS notification: -'.

The screenshot shows the 'Objects' tab of an S3 bucket listing. A folder named 'CloudTrail/' is highlighted with a purple oval. The object list table has columns for Name, Type, Last modified, Size, and Storage class. One object is listed: '654654233148_CloudTrail_us-east-2_20240710T0750Z_x5mzxByA89bTSV7L.json.gz'.

The screenshot shows the 'Objects' tab of an S3 bucket listing, focusing on the log file '654654233148_CloudTrail_us-east-2_20240710T0750Z_x5mzxByA89bTSV7L.json.gz'. The file is a gzip archive (gz) from July 10, 2024, at 03:51:02 UTC, with a size of 2.0 KB and Standard storage class. The file is selected, indicated by a checked checkbox.

```
C:\Users\pegal\Downloads> 0 654654233148.CloudTrail_us-east-2.20240710107502.x5mDyAB95fV7U.json ...  
1  {"Records": [{"eventVersion": "1.10", "userIdentity": {"type": "Root", "principalId": "654654233148"}, "accountId": "654654233148", "accessKeyId": "ASIAZQ3D0316KGLSO1CQ", "sessionContext": {"attributes": {"creationDate": "2024-07-10T03:26:40Z", "mAFAuthenticated": "true"}}, "eventTime": "2024-07-10T07:46:02Z", "eventSource": "cloudtrail.amazonaws.com", "eventName": "CreateTrail", "awsRegion": "us-east-2", "sourceIPAddress": "70.60.60.197", "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0", "requestParameters": {"name": "management-events", "s3BucketName": "aws-cloudtrail-logs-654654233148-b9edfed4", "includeGlobalServiceEvents": "true", "includeMultiRegionTrail": "true", "requestParameters": {"name": "management-events", "s3BucketName": "aws-cloudtrail-logs-654654233148-b9edfed4", "includeGlobalServiceEvents": "true", "isOrganizationTrail": "false", "isMultiRegionTrail": "true", "trailARN": "arn:aws:cloudtrail:us-east-2:654654233148:trail/management-events", "logFileValidationEnabled": "false", "isOrganizationTrail": "false"}, "requestID": "a8493b61_3983_4b20_a72f-b0e0c0ebfb06", "eventID": "bc52a5b-5991-4509-a5f6-03bf43bdeed", "readOnly": "false", "eventType": "AwsApiCall", "managementEvent": "true", "recipientAccountId": "654654233148", "eventCategory": "Management", "tlsDetails": {"tlsVersion": "TLSv1.3", "cipherSuite": "TLS_AES_128_GCM_SHA256", "clientProvidedHostHeader": "cloudtrail.us-east-2.amazonaws.com", "sessionCredentialFromConsole": "true"}, "principalId": "654654233148", "arn": "arn:aws:iam:654654233148:root", "accountId": "654654233148", "accessKeyId": "ASIAZQ3D0316KGLSO1CQ", "sessionContext": {"attributes": {"creationDate": "2024-07-10T03:26:40Z", "mAFAuthenticated": "true"}}, "eventTime": "2024-07-10T07:46:03Z", "eventSource": "cloudtrail.amazonaws.com", "eventName": "PutEventSelectors", "awsRegion": "us-east-2", "sourceIPAddress": "70.60.60.197", "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0", "requestParameters": {"trailName": "management-events", "advancedEventSelectors": [{"name": "Management events selector", "fieldSelectors": [{"field": "eventCategory", "equals": ["Management"]}], "responseElements": {"trailARN": "arn:aws:cloudtrail:us-east-2:654654233148:trail/management-events", "advancedEventSelectors": [{"name": "Management events selector", "fieldSelectors": [{"field": "eventCategory", "equals": ["Management"]}]}, {"requestID": "b8bae86-8ad2-47bc-9146-09127850d57", "eventID": "e0e12880-add4-459a-8f6a-f1a64c56f6f", "readOnly": "false", "eventType": "AwsApiCall", "managementEvent": "true", "recipientAccountId": "654654233148", "eventCategory": "Management", "tlsDetails": {"tlsVersion": "TLSv1.3", "cipherSuite": "TLS_AES_128_GCM_SHA256", "clientProvidedHostHeader": "cloudtrail.us-east-2.amazonaws.com", "sessionCredentialFromConsole": "true"}, "principalId": "654654233148", "arn": "arn:aws:iam:654654233148:root", "accountId": "654654233148", "accessKeyId": "ASIAZQ3D0316KGLSO1CQ", "sessionContext": {"attributes": {"creationDate": "2024-07-10T03:26:40Z", "mAFAuthenticated": "true"}}, "eventTime": "2024-07-10T07:46:03Z", "eventSource": "cloudtrail.amazonaws.com", "eventName": "StartLogging", "awsRegion": "us-east-2", "sourceIPAddress": "70.60.60.197", "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0", "requestParameters": {"name": "arn:aws:cloudtrail:us-east-2:654654233148:trail/management-events", "responseElements": null}, "responseID": "55d1a098-4b98-45a5-9e5a-49593133757", "eventID": "a3379209-4e87-4616-8f48-000000000000", "readOnly": "true", "eventType": "AwsApiCall", "managementEvent": "true"}]
```

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.