Cloud Security with AWS IAM - Step-by-Step Documentation

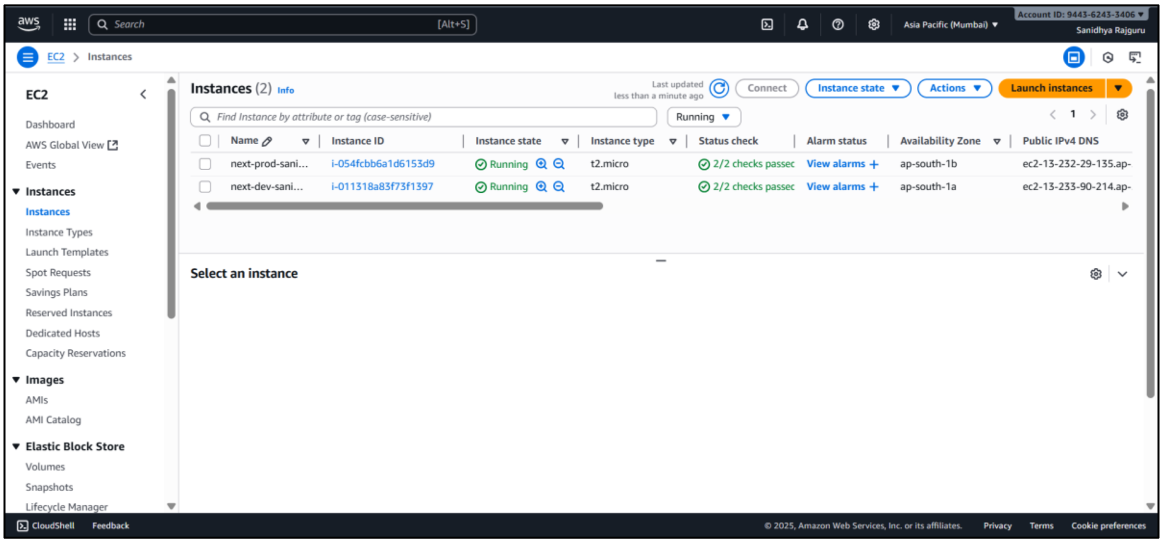
This documentation provides a detailed, step-by-step process for setting up IAM-based cloud security in AWS. You will launch EC2 instances, create IAM policies, configure an account alias, set up users and groups, and finally test access to ensure proper security controls.

Step 1: Launch EC2 Instances

Deploy EC2 instances for production and development environments.

Actions:

- - Log in to AWS Management Console.
- - Navigate to EC2 service.
- - Click 'Launch instance'.
- - Provide a Name and add tags (Env = production / development).
- - Select a Free tier eligible AMI and instance type.
- - Proceed without a key pair (for this project only).
- - Click 'Launch instance' to create the EC2 instance.
- - Repeat for another instance with Env = development tag.



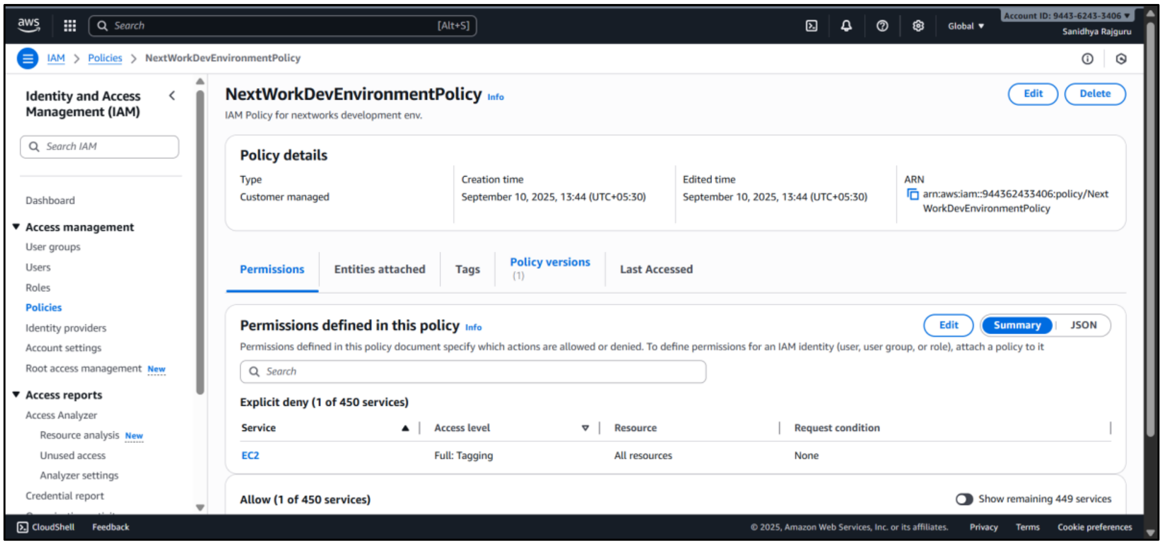
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
next-prod-sani...	i-054fcbb6a1d6153d9	Running	t2.micro	2/2 checks passec	View alarms +	ap-south-1b	ec2-13-232-29-135.ap-
next-dev-sani...	i-011318a83f73f1397	Running	t2.micro	2/2 checks passec	View alarms +	ap-south-1a	ec2-13-233-90-214.ap-

Step 2: Create an IAM Policy

Define an IAM policy to allow access to development instances but restrict production access.

Actions:

- - Navigate to IAM service from AWS Management Console.
- - Go to 'Policies' and click 'Create policy'.
- - Switch to the JSON editor and paste the policy code provided in the project.
- - Review the policy structure (Version, Statement, Effect, Action, Resource, Condition).
- - Name the policy 'NextWorkDevEnvironmentPolicy' and provide a description.
- - Click 'Create policy' to save it.



NextWorkDevEnvironmentPolicy Info

IAM Policy for nextworks development env.

Policy details

Type	Creation time	Edited time	ARN
Customer managed	September 10, 2025, 13:44 (UTC+05:30)	September 10, 2025, 13:44 (UTC+05:30)	arn:aws:iam::944362433406:policy/NextWorkDevEnvironmentPolicy

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

Explicit deny (1 of 450 services)

Service	Access level	Resource	Request condition
EC2	Full: Tagging	All resources	None

Allow (1 of 450 services)

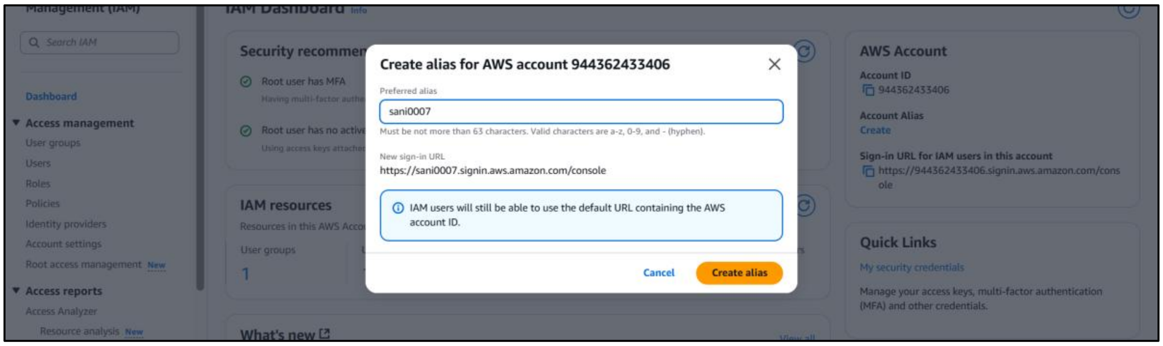
Show remaining 449 services

Step 3: Create an AWS Account Alias

Create an account alias for easier login access.

Actions:

- - In IAM console, navigate to 'Dashboard'.
- - On the right-hand side, choose 'Create' under Account Alias.
- - Enter a preferred alias (e.g., nextwork-alias-yourname).
- - Click 'Create alias' to apply.



Create alias for AWS account 944362433406

Preferred alias: sani0007

Must be not more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).

New sign-in URL: https://sani0007.signin.aws.amazon.com/console

IAM users will still be able to use the default URL containing the AWS account ID.

AWS Account

Account ID: 944362433406

Account Alias: Create

Sign-in URL for IAM users in this account: https://944362433406.signin.aws.amazon.com/console

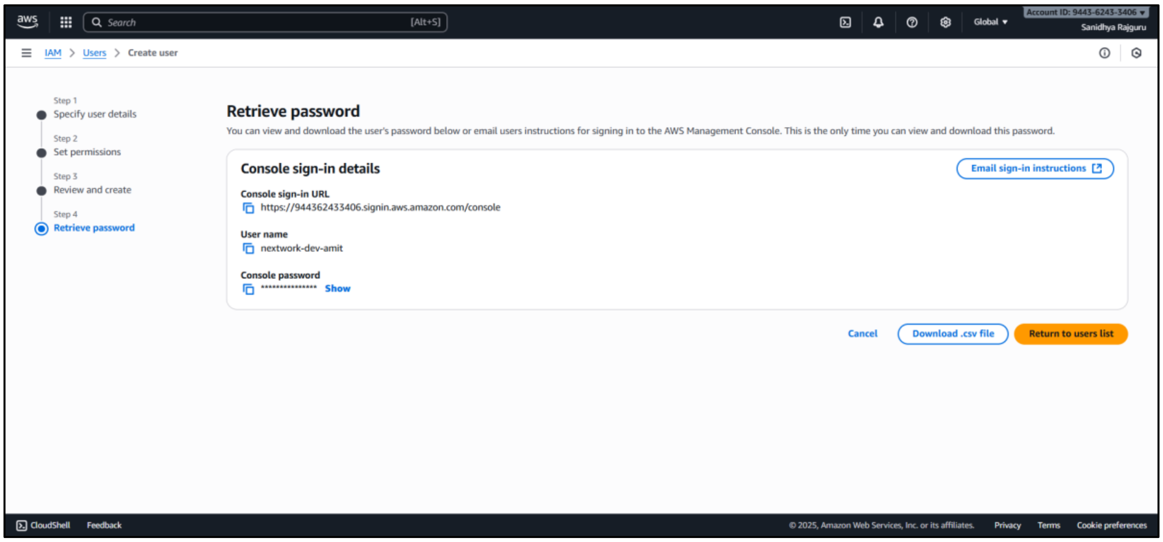
Step 4: Create IAM Users and User Groups

Set up IAM groups and users for structured permission management.

Actions:

- - In IAM console, go to 'User groups'.
- - Click 'Create group' and name it 'nextwork-dev-group'.
- - Attach the 'NextWorkDevEnvironmentPolicy' to the group.
- - Go to 'Users' and click 'Create user'.
- - Enter a username (e.g., nextwork-dev-yourname).
- - Provide AWS Management Console access and password settings.
- - Add the user to 'nextwork-dev-group'.

- - Click 'Create user' to finalize.



Account ID: 9443-6243-3406
Sanidhya Rajguru

IAM > Users > Create user

Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password

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://944362433406.signin.aws.amazon.com/console

User name
nextwork-dev-amit

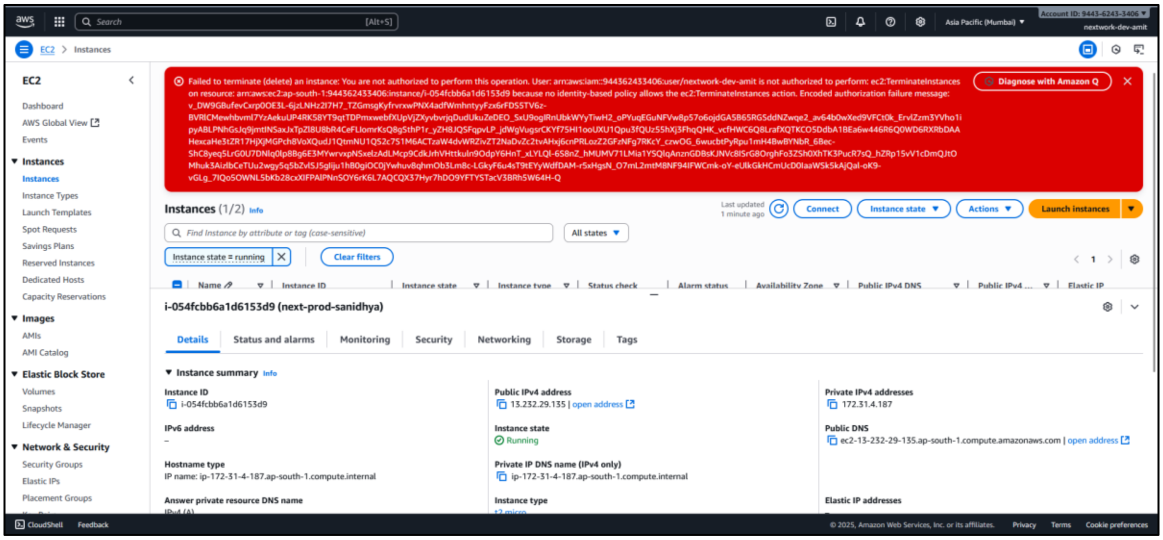
Console password
*************** Show

Step 5: Test Intern's Access

Log in as the new IAM user and verify restricted/allowed access.

Actions:

- - Copy the console sign-in URL with your account alias.
- - Open the URL in an incognito browser window.
- - Log in with the IAM user's username and password.
- - Navigate to EC2 and attempt to stop the production instance (should fail).
- - Attempt to stop the development instance (should succeed).
- - Confirm that access controls are working as expected.



Account ID: 9443-6243-3406
nextwork-dev-amit

EC2 > Instances

Failed to terminate (delete) an instance: You are not authorized to perform this operation. User: arn:aws:iam::944362433406:user/nextwork-dev-amit is not authorized to perform: ec2:TerminateInstances on resource: arn:aws:ec2:ap-south-1:944362433406:instance/i-054fcbb6a1d6153d9 because no identity-based policy allows the ec2:TerminateInstances action. Encoded authorization failure message: v_DW9GBufevCxrp0OE3L-6jzLNHz2I7H7_TZGmsgKyfrvrxwPNX4adfWmhntyyFzx6rFDS5TV6z-BVRlCMewhbvml7YzAekuUP4RK58YT9qtTDPmxwebfXUpVjZXyvbvrjqDudUkuZeDEO_SxU9oglRnUbkWYyTiwH2_oPYuqEGuNFVw8p57o6ojdGA5B65RGSddNZwqe2_av64b0wXed9VFCt0k_ErvlZzm3YVho1i pyABLPNhGsJq9jmtINSaxJxTpZl8U8bR4CeFLlomrKsQ8gSthP1r_yZH8JQSFqpvLP_jdWgVugsrCKYf75HI1ooUXU1Qpu3fQUz55hXj3FhqQHK_vcfHWC6Q8LrafXQTKCO5DdbA1BEa6w446R6Q0WD6RXRbDAA HexcaHe3tZR17HjXjMGPch8VoXQudJ1QtmNU1QS2c7S1M6ACTzaW4dvWRZivZT2NaDvZc2tvAHxj6cnPRLozZ2GFzNFg7RKcY_czwOG_6wucbtPyRpu1mH4BwBYNbR_6Bec-ShC8yeq5LrG0U7DNlq0lp8Bg6E3MYwrvxpNSxelzAdLMcp9CdkJrhVHttkuln9OdpY6HnT_xLYLQl-6S8nZ_hMUMV71LMia1YSQlqAnznGDBsKJNVc8ISrG8OrghFo3ZSh0XhTK3PucR7sQ_hZRp15vV1cDmQJtO Mhuk3AizlbCeTUu2wgy5q5bZvlSJ5glIju1hB0giOC0jYwhuv8qhmOb3Lm8c-LGkyF6u4sT9tEYyWdfDAM-r5xHgsN_O7mL2mtM8NF94IFWCmk-oY-eUlkGkHCmUcD0laaWSk5kAjQal-oK9-vGLg_7IQo5OWNL5bKb28cxXIFPAlPNnSOY6rK6L7AQCQX37Hyr7hDO9YFTYSTacV3BRh5W64H-Q

Instances (1/2)

Instance state = running

i-054fcbb6a1d6153d9 (next-prod-sanidhya)

Instance summary

Instance ID
i-054fcbb6a1d6153d9

IPv6 address
–

Hostname type
IP name: ip-172-31-4-187.ap-south-1.compute.internal

Answer private resource DNS name

Public IPv4 address
13.232.29.135 | open address

Instance state
Running

Private IP DNS name (IPv4 only)
ip-172-31-4-187.ap-south-1.compute.internal

Instance type

Private IPv4 addresses
172.31.4.187

Public DNS
ec2-13-232-29-135.ap-south-1.compute.amazonaws.com | open address

Elastic IP addresses