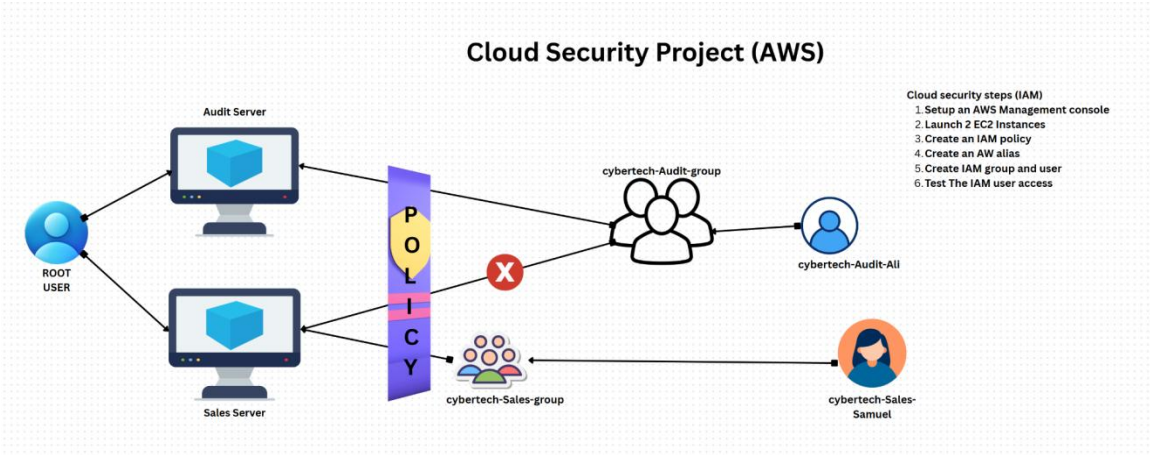
AWS IAM Cloud Security Project

1. Project Overview

I completed this project on cloud security controls in Amazon Web Services (AWS), focusing on Identity and Access Management (IAM). The goal was to create a least- privilege policy, attach it to a user group, and verify that the policy correctly restricts actions on two Amazon EC2 instances (audit and sales).

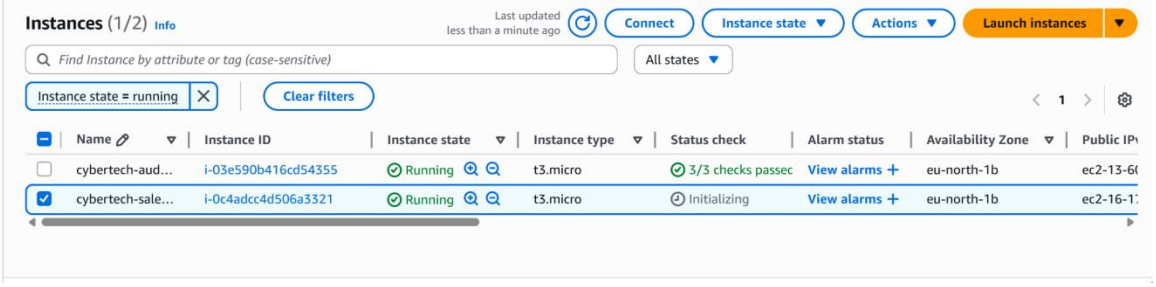


2. Tools & Concepts

- AWS IAM – users, groups, policies, account alias
- Amazon EC2 – instance tagging and lifecycle actions
- JSON policy syntax – Effect, Action, Resource
- Principle of least privilege and policy testing

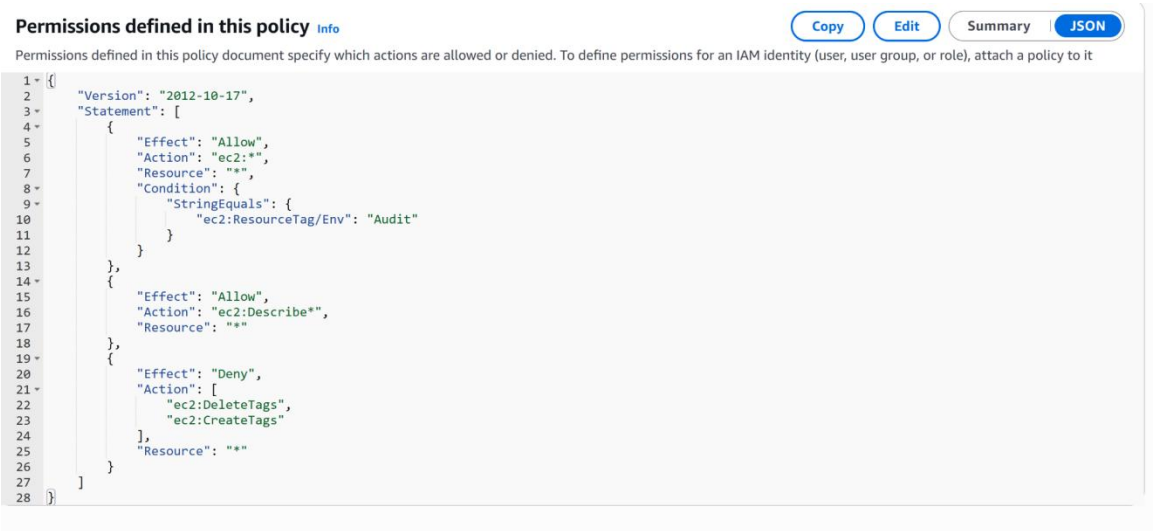
3. Tagging Strategy

I applied a descriptive tag to each EC2 instance:
Instance | Tag Key | Tag Value
audit | Environment | Audit
sales | Environment | Sales



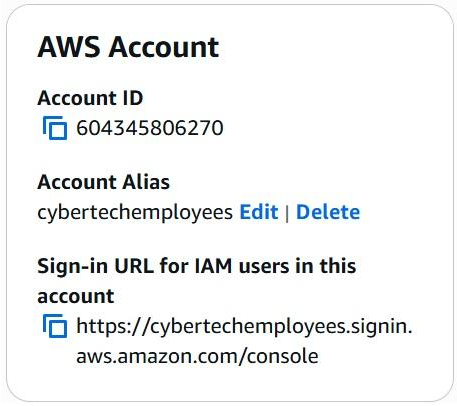
4. Creating the IAM Policy

I authored the following JSON policy to block instance stop/start actions on the audit server but allow those actions on the sales server:



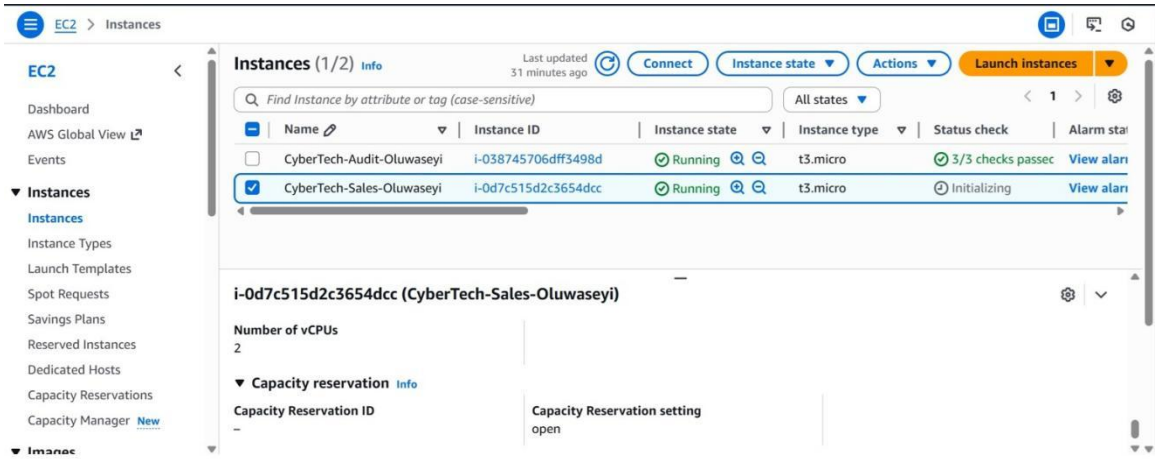
5. Account Alias

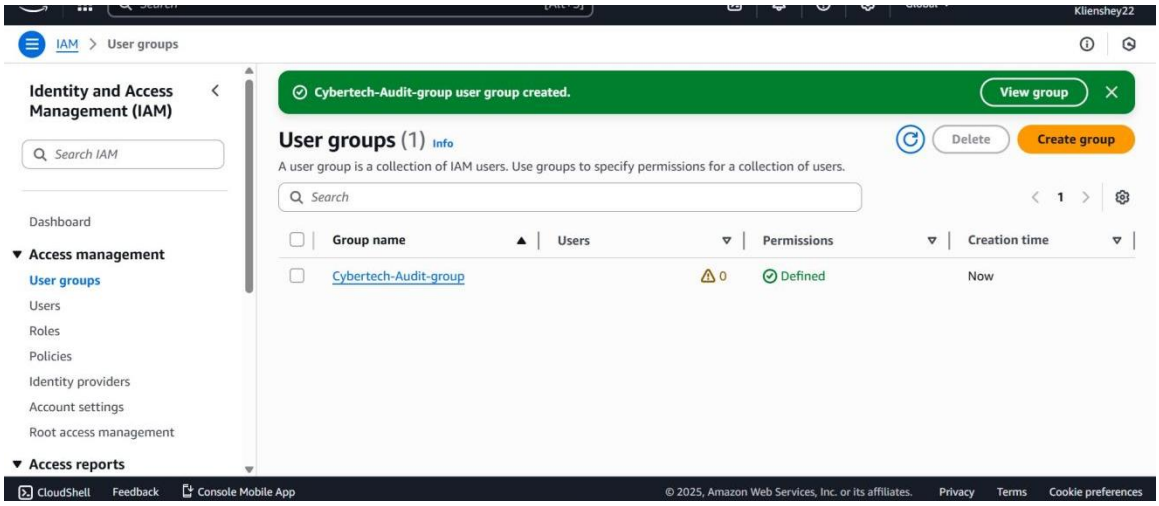
I set a memorable account alias to replace the default numeric URL, making sign- in easier for team members.

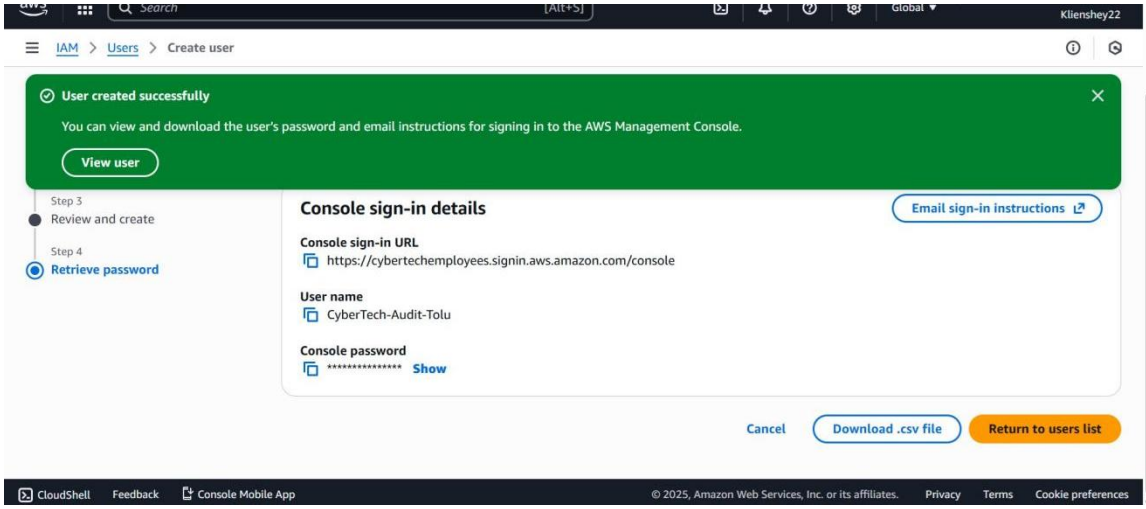


6. IAM Users & Groups

1. Created an IAM user group called Cybertech-Audit-group.
2. Attached the **CybertechAuditEnvPolicy** policy to the group.
3. Added individual IAM users who require controlled EC2 access.





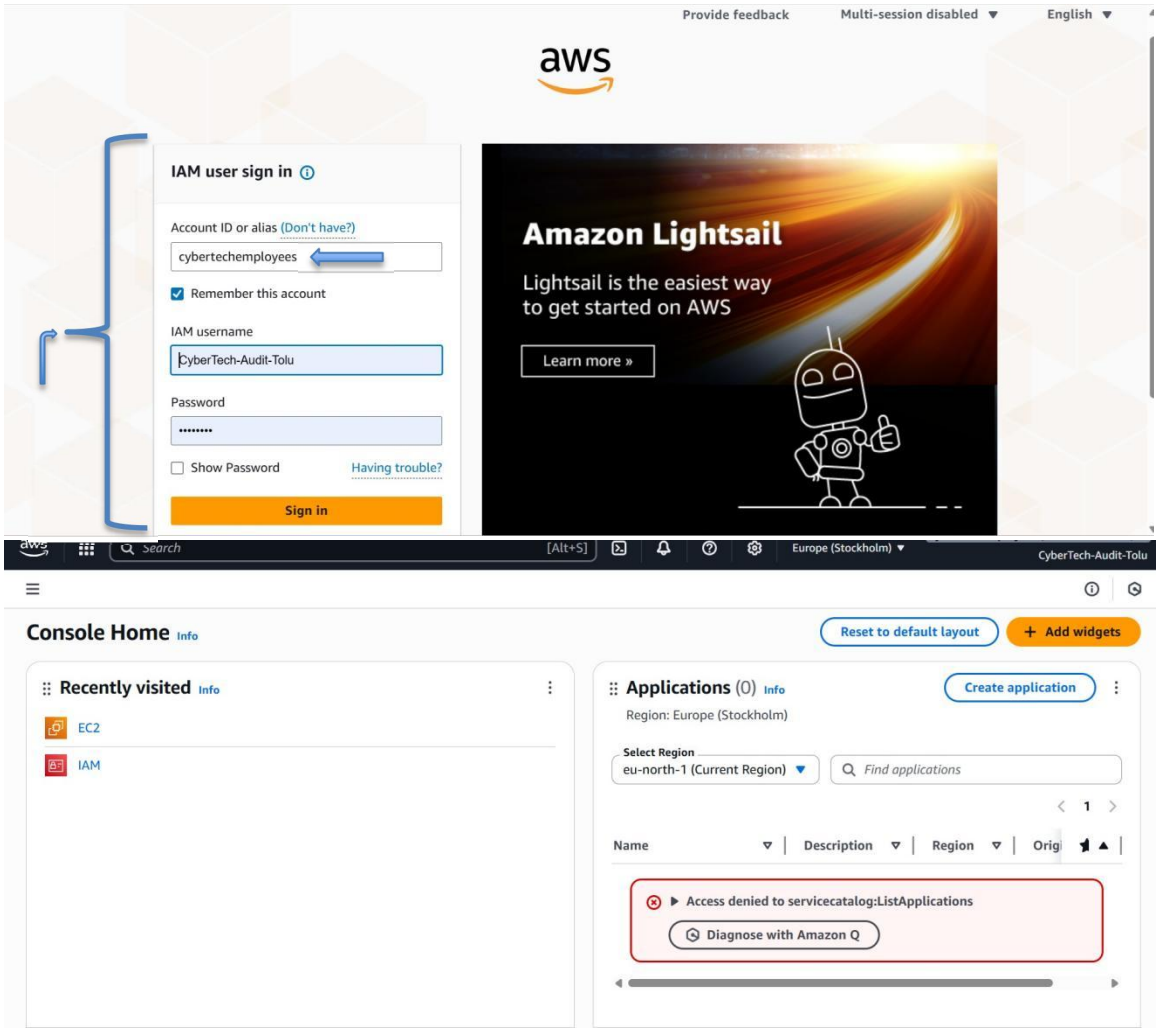


7. Logging in as an IAM User

IAM users can sign in through:

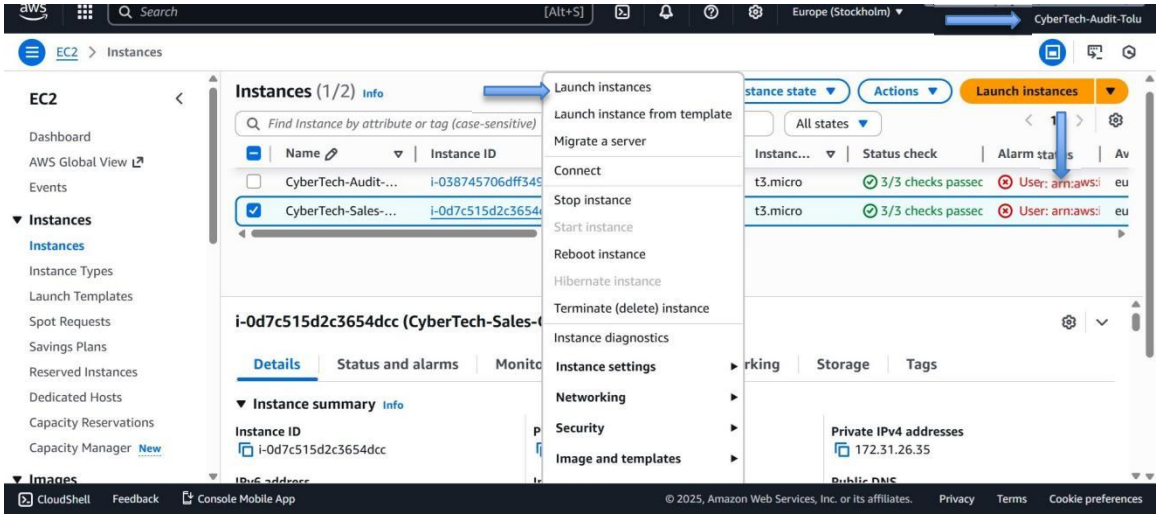
- AWS Management Console (using the new alias URL)

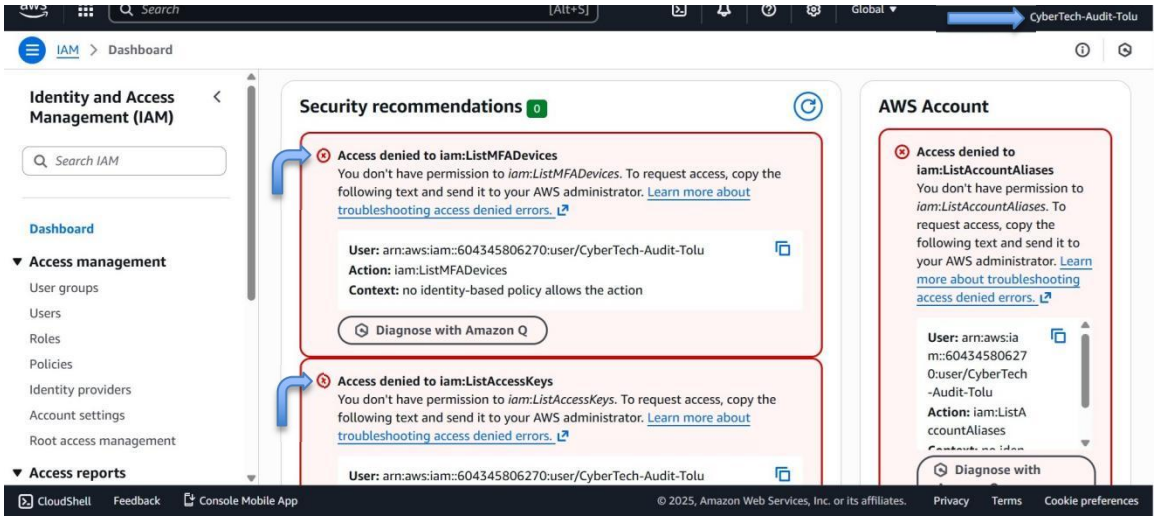
- AWS CLI via programmatic keys

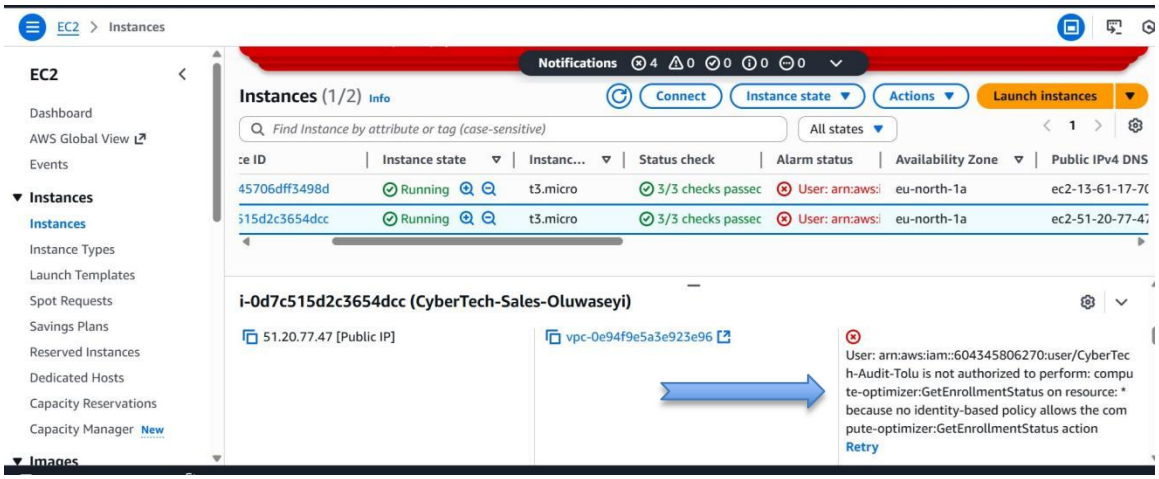


8. Testing the Policy

Test Action | Expected Result | Actual Result
Stop audit instance | Denied | Access denied error displayed
Stop sales instance | Allowed | Instance stopped successfully
Start audit instance | Denied | Access denied error displayed
Start sales instance | Allowed | Instance started successfully


Search
[Alt+S]
Europe (Stockholm)
CyberTech-Audit-Tolu
EC2 > Instances
EC2
Dashboard
AWS Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Capacity Manager New
Images
Instances (1/2) Info
Find Instance by attribute or tag (case-sensitive)
Name
Instance ID
CyberTech-Audit-...
i-038745706dff349
CyberTech-Sales-...
i-0d7c515d2c3654
Launch instances
Launch instance from template
Migrate a server
Connect
Stop instance
Start instance
Reboot instance
Hibernate instance
Terminate (delete) instance
Instance diagnostics
Instance settings
Networking
Security
Image and templates
Actions
Launch instances
All states
Instanc...
Status check
Alarm status
t3.micro
3/3 checks passec
User: arn:aws:i
i-0d7c515d2c3654dcc (CyberTech-Sales-
Details
Status and alarms
Storage
Tags
Instance summary Info
Instance ID
i-0d7c515d2c3654dcc
Private IPv4 addresses
172.31.26.35
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Alt+S]
Global
CyberTech-Audit-Tolu
IAM > Dashboard
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Access reports
Security recommendations 0
Access denied to iam:ListMFADevices
You don't have permission to iam:ListMFADevices. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.
User: arn:aws:iam::604345806270:user/CyberTech-Audit-Tolu
Action: iam:ListMFADevices
Context: no identity-based policy allows the action
Diagnose with Amazon Q
Access denied to iam:ListAccessKeys
You don't have permission to iam:ListAccessKeys. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.
User: arn:aws:iam::604345806270:user/CyberTech-Audit-Tolu
AWS Account
Access denied to iam:ListAccountAliases
You don't have permission to iam:ListAccountAliases. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.
User: arn:aws:iam::604345806270:user/CyberTech-Audit-Tolu
Action: iam:ListAccountAliases
Diagnose with
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


EC2 > Instances
EC2
Dashboard
AWS Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Capacity Manager New
Images
Notifications 4 0 0 0 0
Instances (1/2) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
ce ID
Instance state
Instanc...
Status check
Alarm status
Availability Zone
Public IPv4 DNS
45706dff3498d
Running
t3.micro
3/3 checks passec
User: arn:aws:i
eu-north-1a
ec2-13-61-17-7(
515d2c3654dcc
Running
t3.micro
3/3 checks passec
User: arn:aws:i
eu-north-1a
ec2-51-20-77-47
i-0d7c515d2c3654dcc (CyberTech-Sales-Oluwaseyi)
51.20.77.47 [Public IP]
vpc-0e94f9e5a3e923e96
User: arn:aws:iam::604345806270:user/CyberTech-Audit-Tolu is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: * because no identity-based policy allows the compute-optimizer:GetEnrollmentStatus action
Retry