

## **AWS exam:**

### **Section 1: Multiple Choice Questions (MCQs):**

1. C
2. A
3. C
4. A
5. B
6. B
7. A
8. B
9. C
10. C
11. A

### **Research-based AWS Questions - using google only:**

**12. What are AWS Landing Zones, and how do they help with multi-account governance?**

AWS Landing Zones:

a well-architected, multi account AWS environment that is a starting point from which you can deploy workloads and applications. It's a good baseline for multi-account architecture, identity and access management, governance, data security, network design and logging.

how they help with multi account governance:

enables enforcement of controls to ensure compliance with corporate guidelines, across multiple accounts in your environment. LZ is a recommended cloud environment that includes default accounts, account structure, network deployment and security.

**13. Explain how AWS WAF protects web applications from common attacks.**

WAF - web application firewall- a security tool, protect our web app by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, prevents any unauthorized data from leaving the app.

how:

-WAF creates rules to filter web requests based on conditions like IP addresses, http structure, or custom URIs.

-monitor the application's login page for unauthorized access to user accounts using compromised credentials.

-create and maintain rules automatically and incorporate them into the development and design process.

#### **14. What is AWS Snowball, and when should it be used?**

AWS Snowball is a service that provides secure devices capable of storing large amounts of data (like 100 TB) with strong end-to-end encryption. It allows clients to bring AWS computing and storage capabilities to edge locations and transfer data securely into and out of AWS. The service accelerates the transfer of large amounts of data to and from the AWS cloud using physical storage devices for transport.

You should use AWS Snowball when you need to Run computing in rugged, austere, mobile, or disconnected environments, or when you transfer large-scale data when bandwidth is insufficient for high-speed online transfer.

#### **What are the key differences between AWS Backup and manual snapshot backups?**

AWS snapshot is a point of time copy of an Amazon EBS volume for an EC2 instance with limited storage and recovery options.

AWS ec2 backup is more comprehensive and flexible copy of your cloud workloads, offering reliable protection and ensuring fast and consistent recovery.

##### **key differences:**

##### **purpose:**

snapshot: quick recovery, testing, virtual environments

backup: focus on data protection and disaster recovery

##### **recovery speed:**

snapshot: faster restoration

backup: slower restoration due to larger data volume

##### **storage efficiency:**

snapshot: stores changes since last snapshot

backup: Stores complete data regardless of changes

##### **Risk of Data Loss:**

snapshot: potential loss of interim data

backup: minimal risk if backups are properly managed

#### **15. How does AWS Shield help mitigate DDoS attacks?**

AWS shield managed DDoS protection service by providing dynamic detection and automatic inline mitigation that minimize application downtime and latency.

all AWS customers get am automatic protection with no additional cost.

its always on monitoring, means the AWS shield continuously monitors AWS global network traffic, searching for possible signs of DDoS malicious activity or targeting customer resources DDoS attacks.

when AWS shield detect DDoS attack, it automatically deploy inline mitigations to remove malicious traffic and helps regular traffic to reach intended customer systems.

#### **16. Explain the differences between AWS Transit Gateway and VPC Peering.**

VPC peering is network connection between two VPC, enables to route traffic between them privately.

AWS Transit Gateway is service that connects VPCs and on premises networks through a broker- central hub without relying on few point to point connections or transit VPC.

**differences:**

**connection type:**

AWS Transit Gateway: central hub connection

VPC peering: direct connection between VPCs

**Scalability:**

AWS Transit Gateway: highly scalable, easily connects multiple of VPCs - good at connection many VPCs

VPC peering: complex as more VPCs added - best for connecting small numbers of VPCs

**complexity:**

AWS Transit Gateway: simpler-one connection to the transit gateway connects to all

VPC peering: more VPCs = more complex

**cost:**

AWS Transit Gateway: additional cost

VPC peering: no additional charge (beyond data transfer)

**17. What is AWS Step Functions, and how does it help with workflow automation?**

AWS step function is visual workflow, fully managed service that enable the orchestration of microservices and serverless applications.

the service enable developers to create and managed multi step application workflow in the cloud. It help you to coordinate individual tasks into visual workflow, makes you build and update applications quickly by coordinate multiple services automatically, handling transitions between tasks, without manual intervention.

The workflow defines each step as an AWS lambda function task.

It helps with workflow automation by coordinate multiple services automatically, handling transitions between tasks, without manual intervention. automate IT security and processes, running tasks in parallel, visual and easy to use, .

**18. How does AWS Control Tower assist organizations in managing multiple AWS accounts?**

AWS control tower used to be cloud administrator and design to set up and govern a secure, multi account AWS environment. It automate the creation of AWS account.

The automatically implements allows. It assist organization in managing multiple AWS accounts by keep your organization and accounts from drift, it applies controls and guardrails. Give the ability to use controls to help ensure that security logs and necessary cross-account access permissions are created, and not altered.

Enable end users in the distributed teams to provide new AWS account quickly by Configurable account templates in Account Factory.

**19. What is the significance of AWS Outposts in hybrid cloud solutions?**

AWS Outposts is offer the same virtual infrastructure, services, APIs and tools of AWS in on-premises data centers or colocation space for hybrid experience. Enable customers to build and run applications on premises using the same programming interfaces in AWS regions. AWS Outposts helps brings the gap between the on premises infrastructure and the public cloud.

**20. Explain the key use cases for AWS Elastic File System (EFS) compared to S3 and EBS.**

Amazon EFS is a file system, provides simple. Scalable, elastic file storage.

S3 is a static storage service, secure and highly scalable object storage, objects are stored in Buckets.

EBS is Amazon's block-level storage solution used with ec2 cloud service to store persistent data.

**Type of storage:**

EFS: file systems storage for multiple ec2-instance

S3: object storage (like photos, videos, documents...)

EBS: block storage for an EC2 instance

**durability:**

EFS: stored redundantly across multiple az

S3: stored redundantly across multiple az, high durability

EBS: Stored redundantly in a single az

**performance:**

EFS: moderate- depends on network conditions

S3: lower- object based access

EBS: high- predictable i/o throughout

**typical use cases:**

EFS: application data, shared files, content management systems

S3: backups, archives, static website content, big data analytics

EBS: databases, operating systems, mission critical applications

**max storage:**

EFS: unlimited

S3: unlimited

EBS: has limitations (16 TB for one volume)

**scalability:**

EFS: automatically grow and shrink as adding and remove files

S3: highly scalable

EBS: limited, manually increase or decrease the memory size, add and remove additional volumes to and from your EC2 instance when you need more space

**service endpoint:**

EFS: within VPC

S3: within or without VPC

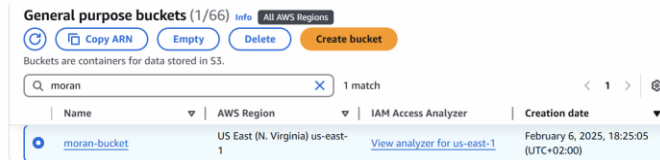
EBS: within VPC

## Section 2: Hands-on UI-Based Questions

### 1. S3 bucket:

finding s3 create bucket → gives the bucket name: "moran-bucket" → kept the default settings (bucket type, object ownership, Block Public Access settings for this bucket) → chose enable in bucket versioning

**after creating bucket:**



**edit permission section and generate policy according to the mission:**

#### Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a [description of elements](#) that you can use in statements.

Effect ☒ Allow ☐ Deny

Principal

Use a comma to separate multiple values.

AWS Service  ☐ All Services (\*)

Use multiple statements to add permissions for more than one service.

Actions  ☐ All Actions (\*)

Amazon Resource Name (ARN)

ARN should follow the following format: arn:aws:s3:::(BucketName)/\${KeyName}.  
Use a comma to separate multiple values.

Add Conditions (Optional)

#### Step 3: Generate Policy

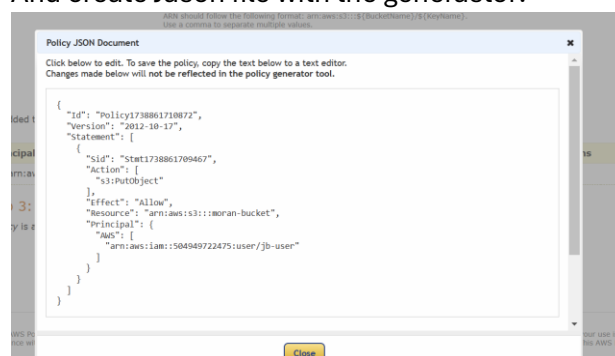
Copy our arn user:

arn:aws:iam::504949722475:user/jb-user

jb-user [Info](#)

<b>Summary</b>		
ARN <a href="#">arn:aws:iam::504949722475:user/jb-user</a>	Console access <a href="#">Enabled without MFA</a>	Access key 1 <a href="#">Create access key</a>
Created February 06, 2025, 16:27 (UTC+02:00)	Last console sign-in <a href="#">Today</a>	

And create Jason file with the generator:



with action "put object" only for upload objects (only upload objects).

final:

moran-bucket info

<a href="#">Objects</a>	<a href="#">Metadata</a>	<a href="#">Properties</a>	<a href="#">Permissions</a>	<a href="#">Metrics</a>	<a href="#">Management</a>	<a href="#">Access Points</a>
-------------------------	--------------------------	----------------------------	-----------------------------	-------------------------	----------------------------	-------------------------------

### Permissions overview

**Access finding**

Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#).

[View analyzer for us-east-1](#)

---

**Block public access (bucket settings)**

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

**Block all public access**

☒ On

► Individual Block Public Access settings for this bucket

---

**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](#)

**Public access is blocked because Block Public Access settings are turned on for this bucket**

To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about [using Amazon S3 Block Public Access](#)

```
{
  "Version": "2012-10-17",
  "Id": "Policy1738861710872",
  "Statement": [
    {
      "Sid": "Stmt1738861709467",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::504949722475:user/jb-user"
      },
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

## 2. Launch ec2 instance:

ec2 name: moran-instance

amazon machine image in my decision

The screenshot shows the AWS Marketplace console interface. At the top, there are navigation tabs: 'Recents', 'My AMIs', and 'Quick Start'. The 'Quick Start' tab is selected and highlighted with a blue underline. Below the tabs is a grid of operating system logos and names: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, and SUSE Linux. To the right of this grid is a search icon and a link that says 'Browse more AMIs'. Below the grid, the details for the 'Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type' are displayed. This section includes the AMI ID 'ami-048175b2d81779218', the architecture 'x86\_64', and a 'Free tier eligible' badge. The interface is clean and modern, with a white background and blue accents.

Instance type as we asked for:

☰ EC2 > Instances > Launch an instance

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro

Family: t2   1 vCPU   1 GiB Memory   Current generation: true

On-Demand Windows base pricing: 0.0162 USD per Hour

On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour

On-Demand SUSE base pricing: 0.0116 USD per Hour

On-Demand RHEL base pricing: 0.026 USD per Hour

On-Demand Linux base pricing: 0.0116 USD per Hour

Free tier eligible

☒ All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

## Create Security Group that allows inbound SSH (port 22) and HTTP (port 80) traffic:

> [Instances](#) > Launch an instance

Security group name - *required*  
moran-sg-test

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_-./()#,@!+=&:~\*`

Description - *required* | [Info](#)  
allows inbound SSH (port 22) and HTTP (port 80) traffic.

**Inbound Security Group Rules**

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) [Remove](#)

Type | [Info](#) | Protocol | [Info](#) | Port range | [Info](#)  
ssh | TCP | 22

Source type | [Info](#) | Source | [Info](#) | Description - *optional* | [Info](#)  
Anywhere | [Add CIDR, prefix list or security group](#) | e.g. SSH for admin desktop  
0.0.0.0/0 ✕

▼ Security group rule 2 (TCP, 80, 0.0.0.0/0) [Remove](#)

Type | [Info](#) | Protocol | [Info](#) | Port range | [Info](#)  
HTTP | TCP | 80

Source type | [Info](#) | Source | [Info](#) | Description - *optional* | [Info](#)  
Anywhere | [Add CIDR, prefix list or security group](#) | e.g. SSH for admin desktop  
0.0.0.0/0 ✕

## Final:

Instances (1) [Info](#)

Find instance by attribute or tag (case-sensitive) [All states](#) [Clear filters](#)

Instance ID `i-07acdb3a60a7162df` ✕

Last updated less than a minute ago [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input type="checkbox"/>	moran-ec2	i-07acdb3a60a7162df	Running	t2.micro	Initializing	<a href="#">View alarms</a>	us-east-1a	ec2-52-90-253-72.com...	52.90.253.72	-

## 3. Configure an IAM User with S3 Access:

go to IAM and create new user named moran-user:

Step 1 [Specify user details](#)  
Step 2 [Set permissions](#)  
Step 3 [Review and create](#)

**Specify user details**

User details

User name  
moran-user

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , @ \_ - (hyphen)

## And create password, then create policy with specific permissions:

**Specify permissions** [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

**Policy editor**

▼ **S3** [Allow](#) 120 Actions

Specify what actions can be performed on specific resources in S3.

▼ **Actions allowed**

Specify actions from the service to be allowed.

[Filter Actions](#)

Manual actions | [Add actions](#)

☐ All S3 actions (s3:\*)

Access level

► **List** (Selected 1/16)

► **Read** (Selected 61/61)

► **Write** (Selected 58/58)

► **Permissions management** (16)

► **Tagging** (12)

⚠ **Dependent permissions not selected.**  
To grant permissions for the selected resource actions, including additional dependent actions might be required.

- s3:CreateBucketMetadataTableConfiguration requires [4 more](#) actions.
- s3:CreateJob requires [1 more](#) action.
- s3:PutReplicationConfiguration requires [1 more](#) action.

▼ **Resources**

Specify resource ARNs for these actions.

☐ All

☒ Specific

**\*list- only access to ListBucket, all the options for read and write.**

only one specific bucket:

▼ Resources

Specify resource ARNs for these actions.

All

Specific

accessgrant

info

accessgrantsinstance

info

accessgrantslocation

info

accesspoint

info

bucket

info

job

info

multiregionaccesspoint

info

multiregionaccesspointrequestarn

info

object

info

objectlambdaccesspoint

info

storageensconfiguration

info

storageensgroup

info

△ Specified accessgrant resource ARN for the DeleteAccessGrant and 4 more actions. Add ARNs to restrict access.

△ Specified accessgrantsinstance resource ARN for the AssociateAccessGrantsIdentityCenter and 16 more actions. Add ARNs to restrict access.

△ Specified accessgrantslocation resource ARN for the CreateAccessGrant and 6 more actions. Add ARNs to restrict access.

△ Specified accesspoint resource ARN for the CreateAccessPoint and 6 more actions. Add ARNs to restrict access.

arn:aws:s3::arn:aws:s3::moran-bucket

△ Specified job resource ARN for the DeleteJobTagging and 5 more actions. Add ARNs to restrict access.

△ Specified multiregionaccesspoint resource ARN for the CreateMultiRegionAccessPoint and 7 more actions. Add ARNs to restrict access.

△ Specified multiregionaccesspointrequestarn resource ARN for the DescribeMultiRegionAccessPointOperation action. Add ARNs to restrict access.

△ Specified object resource ARN for the AbortMultipartUpload and 32 more actions. Add ARNs to restrict access.

△ Specified objectlambdaccesspoint resource ARN for the CreateAccessPointForObjectLambda and 8 more actions. Add ARNs to restrict access.

△ Specified storageensconfiguration resource ARN for the DeleteStorageLensConfiguration and 5 more actions. Add ARNs to restrict access.

△ Specified storageensgroup resource ARN for the DeleteStorageLensGroup and 5 more actions. Add ARNs to restrict access.

Specify ARNs

×

Visual

Text

Resource bucket name

arn:aws:s3::moran-bucket

☐ Any bucket name

Resource ARN

arn:aws:s3::arn:aws:s3::moran-bucket

Cancel

Add ARNs

arn:aws:s3::arn:aws:s3::moran-bucket

moran\_policy\_newuserper

Maximum 128 characters. Use alphanumeric and "+=, @, \_" characters.

Description - optional

Add a short explanation for this policy.

permissions for new IAM user to access only a specific S3 bucket

Maximum 1,000 characters. Use alphanumeric and "+=, @, \_" characters.

ⓘ This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition. Choose **Show remaining**. [Learn more](#)

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

Q Search

Allow (1 of 437 services)

Service

Access level

Resource

Request condition

S3

Limited: List, Read, Write

Multiple

None

user details:

moran-user

info

Del

Summary

ARN

arn:aws:iam::504949722475:user/moran-user

Created

February 06, 2025, 20:23 (UTC+02:00)

Console access

△ Enabled without MFA

Last console sign-in

Never

Access key 1

Create access key

Permissions

Groups

Tags

Security credentials

Last Accessed

Permissions policies (1)

Remove

Add permissions

Permissions are defined by policies attached to the user directly or through groups.

Q Search

Filter by Type

All types

☐ Policy name

Type

Attached via

☐ moran\_policy\_newuserper

Customer managed

Directly

How to verify the user has the correct permissions:

a possible solution can be to login to moran-user and check if the user have access



to moran-bucket and do not have permissions to the other buckets.

I login and see this happening:

Search [Alt+S] United States (N. Virginia) moran-user @ jh-labs

Buckets moran-bucket

**moran-bucket** info

Objects Metadata Properties Permissions Metrics Management Access Points

**Objects (0)**

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](#)

Find objects by prefix Show versions

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

Upload

**moran-bucket** info

Objects Metadata Properties Permissions Metrics Management Access Points

**Bucket overview**

AWS Region: US East (N. Virginia) us-east-1 Amazon Resource Name (ARN): arn:aws:s3::moran-bucket Creation date: February 7, 2025, 10:55:37 (UTC-02:00)

**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: Enabled

**Multi-factor authentication (MFA) delete**

An additional layer of security that requires multi-factor authentication for changing bucket versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

MFA delete: Disabled

**Tags (0)**

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

Key	Value
No tags associated with this resource.	

**moran-bucket**

Objects Metadata Properties Permissions Metrics Management Access Points

**Lifecycle configuration**

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Lifecycle rules run once per day.

**Lifecycle rules**

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. [Learn more](#)

Lifecycle rule name	Status	Scope	Current version actions	Noncurrent version actions	Expired object delete mar...	Incomplete multipart upl...
No lifecycle rules						
There are no lifecycle rules for this bucket.						

Create lifecycle rule

**Replication rules (0)**

Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more. [Learn more](#)

Replication rule name	Status	Destination bucket	Destination Region	Priority	Scope	Storage class	Replica owner	Replication Time Control	KMS-encrypted objects (SSE-KMS or SSE-KMS)	Replica modification sync
No replication rules										
You don't have any rules in the replication configuration.										

Create replication rule

**Inventory configurations (0)**

You can create inventory configurations on a bucket to generate a flat file list of your objects and metadata. These scheduled reports can include all objects in the bucket or be limited to a shared prefix. [Learn more](#)

Name	Status	Scope	Destination	Frequency	Last export	Format
No configurations						
No configurations to display						

Create inventory configuration

has permission!

Other buckets:

Search [Alt+S] United States (N. Virginia) moran-user @ jh-labs

ropps-s3

**almog-devops-s3** info

Objects Metadata Properties Permissions Metrics Management Access Points

**Objects**

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](#)

Find objects by prefix Show versions

Name	Type	Last modified	Size	Storage class
<b>Insufficient permissions to list objects</b>				
After you or your AWS administrator has updated your permissions to allow the s3:ListBucket action, refresh the page. Learn more about <a href="#">identity and access management in Amazon S3</a>				

Diagnose with Amazon Q

## almog-devops-s3

Objects **Metadata** Properties Permissions Metrics Management Access Points

### Metadata Info



Delete

Create metadata configuration

Accelerate data discovery with automatically generated, near real-time metadata for objects in this bucket, stored in a fully managed Apache Iceberg table. You can query this metadata table to identify and prepare data for use in business analytics and machine learning. Identify AI-generated data, retrieve content, and more.

#### You don't have permission to get the metadata configuration

After updating your [Identity and Access Management \(IAM\) permissions](#) to allow s3:GetBucketMetadataTableConfiguration, refresh this page. [Learn more](#)

Diagnose with Amazon Q

► API response

## almog-devops-s3

Objects Metadata Properties Permissions Metrics **Management** Access Points

#### You don't have permission to view the lifecycle configuration

You or your AWS admin must update your IAM permissions to allow s3:GetLifecycleConfiguration, and then try again. Learn more about [Identity and access management in Amazon S3](#)

Diagnose with Amazon Q

► API response

#### You don't have permission to view the replication configuration

You or your AWS admin must update your IAM permissions to allow s3:GetReplicationConfiguration, and then refresh the page to continue. Learn more about [Identity and access management in Amazon S3](#)

Diagnose with Amazon Q

► API response

#### You don't have permissions to list inventory configuration for this bucket

You or your AWS admin must update your IAM permissions to allow s3:GetInventoryConfiguration, and then refresh the page. [Learn more about Identity and access management in Amazon S3](#)

Diagnose with Amazon Q

► API response

## almog-devops-s3 Info

Objects Metadata Properties Permissions Metrics Management **Access Points**

### Access Points

Access points are named network endpoints that are attached to buckets which simplify managing data access at scale in S3. To see if any of the access points attached to this bucket grant public or cross-account access, go to [IAM](#)

**Name** ▲ **Network origin** ▼ **VPC ID** ▼ **Bucket owner account ID** ▼ **Access Point alias**

#### Insufficient permissions to list access points

After you or your AWS admin has updated your IAM permissions to allow the s3:ListAccessPoints action, refresh this page. Learn more about [Identity and Access Management in Amazon S3](#)

► API response

[Alt+S]

on S3 > Buckets > albert-website-765

**albert-website-765** Info

Objects Metadata Properties Permissions Metrics Management Access Points

**Objects** Copy S3 URI Copy URL Download Open Delete **Actions** ▼ Create folder Upload

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](#)

Show versions < 1 >

	Name	Type	Last modified	Size	Storage class
<b>Insufficient permissions to list objects</b> After you or your AWS administrator has updated your permissions to allow the s3:ListBucket action, refresh the page. Learn more about <a href="#">Identity and access management in Amazon S3</a> Diagnose with Amazon Q					

[Alt+S]

> Buckets > assaf-bkt-02-06

**assaf-bkt-02-06** Info

Objects Metadata Properties Permissions Metrics Management Access Points

**Objects** Copy S3 URI Copy URL Download Open Delete **Actions** ▼ Create folder Upload

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](#)

Show versions < 1 >

	Name	Type	Last modified	Size	Storage class
<b>Insufficient permissions to list objects</b> After you or your AWS administrator has updated your permissions to allow the s3:ListBucket action, refresh the page. Learn more about <a href="#">Identity and access management in Amazon S3</a> Diagnose with Amazon Q					

no permission! All the options are block.

#### 4. Set Up a CloudWatch Alarm:

**create -> select metric ec2 -> per instance metric -> CPUUtilization**

**Period**

5 minutes

**Conditions**

**Threshold type**

☒ Static  
Use a value as a threshold

**Whenever CPUUtilization is...**  
Define the alarm condition.

☒ Greater  
> threshold

☐ Greater/Equal  
>= threshold

**than...**  
Define the threshold value.

70

Must be a number

#### Configuration of notification:

**alarm state trigger- in alarm (when it does outside of the threshold)**

##### 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 is within the defined threshold.

**Send a notification to the following SNS topic**  
Define the SNS (Simple Notification Service) topic that will receive the notification.

☐ Select an existing SNS topic

☒ Create new topic

☐ Use topic ARN to notify other accounts

**Create a new topic...**  
The topic name must be unique.

CloudWatch\_Alarms\_cpu

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.

user@example.com

user1@example.com, user2@example.com

Create topic

Add notification

final:

**Alarms (1)**

☐ Hide Auto Scaling alarms

Clear selection

Create composite alarm

Actions

Create alarm

Alarm state: Any

Alarm type: Any

Actions status: Any

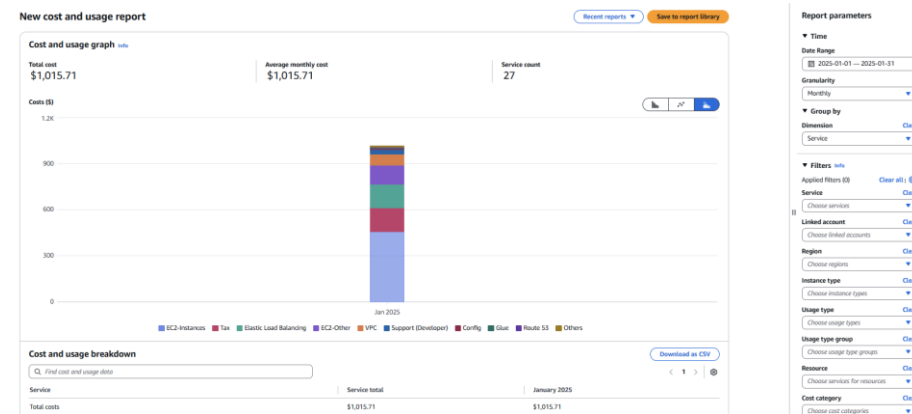
< 1 >

⚙

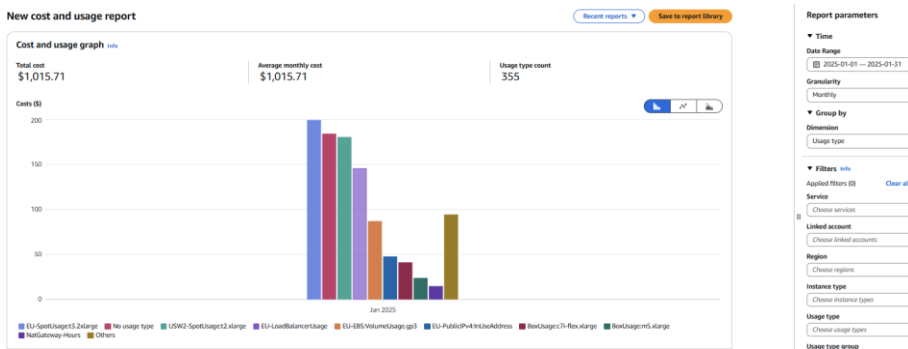
Name	State	Last state update (UTC)	Conditions	Actions
<a href="#">moran-alarm</a>	⚠ Insufficient data	2025-02-06 19:06:36	CPUUtilization > 70 for 1 datapoints within 5 minutes	<a href="#">Actions</a>

## 5. Identify AWS Billing Costs:

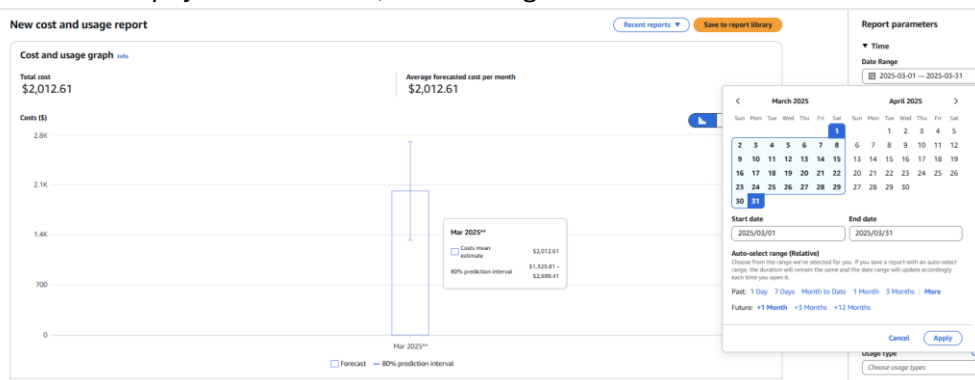
billing details from the last month:



## analyze usage:



for example, if I filtered with S3 service, they spend 2.98\$ on January.  
For forecast costs, I chose in data range 1 month in the future – march,  
the forecast payment will be 2,012.61\$ avg.



# Section 3: Hands-on advanced:

## 1. Deploy an Auto Scaling Group with a Single EC2 Instance

Creating security group called moran-sg with the inbound rules

Inbound rules

Type

Info

Protocol

Port range

Info

Source

Info

Description - optional

Info

SSH

TCP

22

Any...

0.0.0.0/0

Delete

HTTP

TCP

80

Any...

0.0.0.0/0

Delete

Creating auto scaling:  
launch template: moran-template  
AMI: Amazon Linux 2 AMI  
instance type: t2.micro

Launch Templates (1)

Search

Clear filters

1

Launch Template ID	Launch Template Name	Default Version	Latest Version	Create Time	Created By
lt-0b1c68d8f8432292	moran-template	1	1	2025-02-08T21:28:12.000Z	arn:aws:iam::504949722475:u...

using launch template in the auto scaling

Launch template

Info

Launch template

Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

moran-template

Create a launch template

Version

Default (1)

Create a launch template version

Description

AMI ID

ami-04681163a08179f28

Key pair name

moran-key

Launch template

moran-template

lt-0b1c68d8f8432292

Security groups

Security group IDs

sg-08e41cd4017967bb1

Instance type

t2.micro

Request Spot Instances

No

Create target group:

moran-targetgroup

Act

Details

arn:aws:elasticloadbalancing:us-east-1:504949722475:targetgroup/moran-targetgroup/49797b979bdc483e

Target type

Instance

IP address type

IPv4

Protocol : Port

HTTP: 80

Protocol version

HTTP1

VPC

vc-0c342467237e51c30

1

Total targets

0

Healthy

0

Unhealthy

1

Unused

0

Initial

0

Draining

Distribution of targets by Availability Zone (AZ)

Select values in this table to see corresponding filters applied to the Registered targets table below.

Targets

Monitoring

Health checks

Attributes

Tags

Registered targets (1)

Info

Anomaly mitigation: Not applicable

De-register

Register tan

Filter targets

1

Instance ID	Name	Port	Zone	Health status	Health status details	Admini...	Overrid...	Launch...	Anomaly detection
i-05c20549166e4f541	moran-Instance	80	us-east-1a (use...	Unused	Target group is not co...	-	-	February ...	Normal

create load balancer with the target group:

moran-loadbalancer

▼ Details

Load balancer type

Application

Scheme

Internet-facing

Status

Provisioning

Hosted zone

Z355XDTRQ7X7K

VPC

vpc-0c3424b7237e51c20

Availability Zones

subnet-0040f9cf696fbde73 us-east-1a (use1-az2)  
subnet-039b17c5ab155b2fc us-east-1b (use1-az4)

Load balancer ARN

arn:aws:elasticloadbalancing:us-east-1:504949722475:loadbalancer/app/moran-loadbalancer/2f0d8d74ee7d91d

DNS name

Info

moran-loadbalancer-1754793447.us-east-1.elb.amazonaws.com

Listeners and rules

Network mapping

Resource map - new

Security

Monitoring

Integrations

Attributes

Capacity - new

Listeners and rules (1) Info

Manage rules

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.

Filter listeners

Protocol:Port

Default action

Rules

ARN

Security policy

Default SSL

Forward to target group

moran-targetgroup 1 (100%)

1 rule

ARN

Not applicable

Not applicable

auto scaling group information:

moran-autoscalinggroup

moran-autoscalinggroup Capacity overview

arn:aws:autoscaling:us-east-1:504949722475:autoScalingGroup:359ee5a2-05be-4be8-8964-7223ada8a2f6:autoScalingGroupName/moran-autoscalinggroup

Desired capacity

1

Scaling limits (Min - Max)

1 - 1

Desired capacity type

Units (number of instances)

Status

-

Launch template

Launch template

is-do-1c65d8f8432292

moran-launch-template

Version

Default

Description

-

View details in the launch template console

AMI ID

ami-04681163a08179f28

Security groups

-

Storage (volumes)

-

Instance type

t2.micro

Security group IDs

sg-08e41c04217967db1

Key pair name

moran-key

Owner

arn:aws:iam::504949722475:user/jp-user

Create time

Thu Feb 06 2025 23:28:12 GMT+0200 (EYET) %w %p

Request Spot Instances

No

Network

Availability Zones

us-east-1a

Subnet ID

subnet-0040f9cf696fbde73

Availability Zone distribution

Balanced best effort

Instance type requirements

Your Auto Scaling group adheres to the launch template for purchase option and instance type.

Load balancing and VPC lattice options have moved to the new integrations tab.

View integrations tab

Health checks

Health check type

EC2

Health check grace period

300

Instance maintenance policy

Replacement behavior

No policy

Min healthy percentage

-

Max healthy percentage

-

Capacity Reservation preference

Preference

Default

Capacity Reservation IDs

-

Resource Groups

-

Advanced configurations

Instance scale-in protection

Not protected from scale in

Termination policies

Default

Maximum instance lifetime

-

Service-linked role

arn:aws:iam::504949722475:role/aws-service-role/autoscaling.amazonaws.com/AWSServiceRoleForAutoScaling

Placement group

-

Suspended processes

-

Default cooldown

300

Default instance warmup

Disabled

Tags (0)

Key

Value

Tag new instances

Details

Integrations - new

Automatic scaling

Instance management

Instance refresh

Activity

Monitoring

Load balancing

Load balancer target groups

moran-targetgroup

Classic Load Balancers

-

VPC Lattice integration options

VPC Lattice target groups

-

Application Recovery Controller (ARC) zonal shift - new

ARC zonal shift

Disabled

## 2. Connect to the EC2 Instance and Install Nginx

## connecting to the machine with ssh:

[illegible]

checking same privet ip:

i-05c20549166e4f541 (moran-instance)

[Details](#)
[Status and alarms](#)
[Monitoring](#)
[Security](#)
[Networking](#)
[Storage](#)
[Tags](#)

▼ Instance summary info

Instance ID  
i-05c20549166e4f541

Public IPv4 address  
3.192.204.1 | [open address](#)

Private IPv4 addresses  
172.31.92.79

```

eth2-userip-172-31-92-79 - $ ifconfig
eth2: flags=163<UP, BROADCAST, RUNNING, MULTICAST>    mtu 9001
    inet 172.31.92.79 netmask 255.255.240.0    broadcast 172.31.95.255
    inet6 fe80::1069:53ff:fe09:9405 prefixlen 64 scopeid 0x20<link>ether
    ether 12:69:53:09:94:05    txqueuelen 1000    (Ethernet)
    RX packets 80379    bytes 120914139    (115.3 MiB)
    RX errors 0    dropped 0    overruns 0    TX
    TX packets 7597    bytes 496599    (0.48 MiB)
    TX errors 0    dropped 0    overruns 0    carrier 0    collisions 0

lo: flags=73<UP, LOOPBACK, RUNNING>    mtu 65536
    inet 127.0.0.1    netmask 255.0.0.0
    inet6 ::1    prefixlen 128    scopeid 0x10<host>
    loop txqueuelen 1000    (Local Loopback)
    RX packets 48    bytes 3888    (3.7 KiB)
    RX errors 0    dropped 0    overruns 0    frame 0
    TX packets 48    bytes 3888    (3.7 KiB)
    TX errors 0    dropped 0    overruns 0    carrier 0    collisions 0

```

installing and running nginx and check that the curl works:

```
[ec2-user@ip-172-31-92-79 ~]$ systemctl status nginx
● nginx.service - The nginx HTTP and reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2025-02-06 22:16:46 UTC; 2min 6s ago
     Main PID: 3616 (nginx)
       CGroup: /system.slice/nginx.service
               └─3616 nginx: master process /usr/sbin/nginx
                 └─3617 nginx: worker process

[ec2-user@ip-172-31-92-79 ~]$ echo "<h1>Welcome to AWS Auto Scaling</h1>" | sudo tee /usr/share/nginx/html/index.html
<h1>Welcome to AWS Auto Scaling</h1>
[ec2-user@ip-172-31-92-79 ~]$ sudo systemctl start nginx
[ec2-user@ip-172-31-92-79 ~]$ sudo systemctl enable nginx
Created symlink from /etc/systemd/system/multi-user.target.wants/nginx.service to /usr/lib/systemd/system/nginx.service.
[ec2-user@ip-172-31-92-79 ~]$ curl http://localhost:80
<h1>Welcome to AWS Auto Scaling</h1>
[ec2-user@ip-172-31-92-79 ~]$
```

### **3. Access the Web Page via the Load Balancer**

### Putting DNS name in the browser:

dns name: moran-loadbalancer-1754793447.us-east-1.elb.amazonaws.com

moran-loadbalancer-1754793447-us-east-1.elb.amazonaws.com

## Welcome to AWS Auto Scaling

## 4. IAM User Setup for S3 Access: - same as section2-(3)

go to IAM and create new user named moran-user:

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

### Specify user details

User details

User name

moran-user

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, -, ., @, \_ (hyphen)

create password, then create policy with specific permissions:

I decided to give read, write and list(only access to ListBucket to see the list buckets) permissions.

### Specify permissions

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

▼ S3  
120 Actions

Specify what actions can be performed on specific resources in S3.

▼ Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Manual actions | Add actions

☐ All S3 actions (s3:\*)

Access level

► List (Selected 1/16)

► Read (Selected 61/61)

► Write (Selected 58/58)

► Permissions management (16)

► Tagging (12)

⚠ Dependent permissions not selected.  
To grant permissions for the selected resource actions, including additional dependent actions might be required.

- s3:CreateBucketMetadataTableConfiguration requires 4 more actions.
- s3:CreateJob requires 1 more action.
- s3:PutReplicationConfiguration requires 1 more action.

▼ Resources

Specify resource ARNs for these actions.

☐ All

☒ Specific

only one specific bucket- moran-bucket:

Specify ARNs

Visual Text

Resource bucket name

arn:aws:s3::moran-bucket

☐ Any bucket name

Resource ARN

arn:aws:s3::arn:aws:s3::moran-bucket

Cancel Add ARNs



user details + we can see the attached policy:

Verify:

login to moran-user and check if I have access only to moran-bucket and not others:

moran-bucket

info

Objects

Metadata

Properties

Permissions

Metrics

Management

Access Points

Bucket overview

AWS Region  
US East (N. Virginia) us-east-1

Amazon Resource Name (ARN)  
 arn:aws:s3::moran-bucket

Create date  
February 7, 2025, 10:35:37 UTC+02:00

Bucket Versioning

Edit

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

Enabled

Multi-factor authentication (MFA) delete  
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more >](#)  
Disabled

Tags (0)

Edit

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

Key	Value
No tags associated with this resource.	

moran-bucket

ObjectsMetadataPropertiesPermissionsMetricsManagementAccess Points

Lifecycle configuration

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Lifecycle rules run once per day.

Lifecycle rules

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. [Learn more](#)

Lifecycle rule name	Status	Scope	Current version actions	Noncurrent versions actions	Expired object delete mar...	Incomplete multipart upl...
No lifecycle rules There are no lifecycle rules for this bucket.						

Create lifecycle rule

Replication rules (0)

Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more. [Learn more](#)

Replication rule name	Status	Destination bucket	Destination Region	Priority	Scope	Storage class	Replica owner	Replication Time Control	KMS encrypted objects (SSE-KMS or SSE-KMS)	Replica modification sync
No replication rules You don't have any rules in the replication configuration.										

Create replication rule

Inventory configurations (0)

You can create inventory configurations on a bucket to generate a flat file list of your objects and metadata. These scheduled reports can include all objects in the bucket or be limited to a shared prefix. [Learn more](#)

Name	Status	Scope	Destination	Frequency	Last export	Format
No configurations No configurations to display						

Create inventory configuration

has permission!

Other buckets:

rops-s3

almog-devops-s3

almog-devops-s3

almog-devops-s3

almog-devops-s3

ObjectsMetadataPropertiesPermissionsMetricsManagementAccess Points

Objects

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](#)

Find objects by prefix

Show versions

Name	Type	Last modified	Size	Storage class
<div><div>Insufficient permissions to list objects</div><div>After you or your AWS administrator has updated your permissions to allow the s3:ListBucket action, refresh the page. <a href="#">Learn more about identity and access management in Amazon S3</a></div><div>Diagnose with Amazon Q</div></div>				

almog-devops-s3

ObjectsMetadataPropertiesPermissionsMetricsManagementAccess Points

Metadata

Accelerate data discovery with automatically generated, near real-time metadata for objects in this bucket, stored in a fully managed Apache Iceberg table. You can query this metadata table to identify and prepare data for use in business analytics and machine learning. Identify AI-generated data, retrieve content, and more.

You don't have permission to get the metadata configuration

After updating your [Identity and Access Management \(IAM\) permissions](#) to allow s3:GetBucketMetadataTableConfiguration, refresh this page. [Learn more](#)

Diagnose with Amazon Q

API response

almog-devops-s3

ObjectsMetadataPropertiesPermissionsMetricsManagementAccess Points

You don't have permission to view the lifecycle configuration

You or your AWS admin must update your IAM permissions to allow s3:GetLifecycleConfiguration, and then try again. [Learn more about identity and access management in Amazon S3](#)

Diagnose with Amazon Q

API response

You don't have permission to view the replication configuration

You or your AWS admin must update your IAM permissions to allow s3:GetReplicationConfiguration, and then refresh the page to continue. [Learn more about identity and access management in Amazon S3](#)

Diagnose with Amazon Q

API response

You don't have permissions to list inventory configuration for this bucket

You or your AWS admin must update your IAM permissions to allow s3:InventoryConfiguration, and then refresh the page. [Learn more about identity and access management in Amazon S3](#)

Diagnose with Amazon Q

API response

almog-devops-s3

Info

Objects

Metadata

Properties

Permissions

Metrics

Management

Access Points

Access Points

Access points are named network endpoints that are attached to buckets which simplify managing data access at scale in S3. To see if any of the access points attached to this bucket grant public or cross-account access, go to [IAM](#).

Q Search for Access Points by name

Name

Network origin

VPC ID

Bucket owner account ID

Access Point alias

Insufficient permissions to list access points

After you or your AWS admin has updated your IAM permissions to allow the s3:ListAccessPoints action, refresh this page. Learn more about [Identity and Access Management in Amazon S3](#).

API response

Search

Albert-website-765

United States (N. Virginia)

moran-user @ j-164

almog-devops-s3

Info

Objects

Metadata

Properties

Permissions

Metrics

Management

Access Points

Objects

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](#).

Find objects by prefix

Show versions

Name

Type

Last modified

Size

Storage class

Insufficient permissions to list objects

After you or your AWS administrator has updated your permissions to allow the s3:ListBucket action, refresh the page. Learn more about [identity and access management in Amazon S3](#).

Diagnose with Amazon Q

Search

assaf-bkt-02-06

United States (N. Virginia)

moran-user @ j-164

assaf-bkt-02-06

Info

Objects

Metadata

Properties

Permissions

Metrics

Management

Access Points

Objects

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](#).

Find objects by prefix

Show versions

Name

Type

Last modified

Size

Storage class

Insufficient permissions to list objects

After you or your AWS administrator has updated your permissions to allow the s3:ListBucket action, refresh the page. Learn more about [identity and access management in Amazon S3](#).

Diagnose with Amazon Q

no permission! All the options are block.

## 5. Create a CloudWatch Alarm for CPU Usage:

CPU utilization exceeds 70% for 5 minutes.

Preview and create

Step 1: Specify metric and conditions

Edit

Metric

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.

Percent

70

36.5

2.91

20:00

20:30

21:00

21:30

22:00

22:30

CPUUtilization

Namespace

AWS/EC2

Metric name

CPUUtilization

Instanceid

i-05c20549166e4f541

Instance name

moran-instance

Statistic

Average

Period

5 minutes

Configure notifications via email (SNS).

Conditions

Threshold type

Static

Whenever CPUUtilization is Greater (->)

than...

70

► Additional configuration

Step 2: Configure actions

Edit

Actions

Notification

When in alarm, send a notification to "notifications\_via\_email"

Step 3: Add name and description

Edit

Name and description

Name

MoranAlarm

Alarms (1)

☐ Hide Auto Scaling alarms

Clear selection

Create composite alarm

Actions

Q moran

X

Alarm state: Any

Alarm type: Any

Actions status: Any

<input type="checkbox"/>	Name	State	Last state update (UTC)	Conditions	Actions
<input type="checkbox"/>	<a href="#">MoranAlarm</a>	Insufficient data	2025-02-06 22:50:48	CPUUtilization > 70 for 1 datapoints within 5 minutes	Actions enabled <b>Warning</b>