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 throw 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

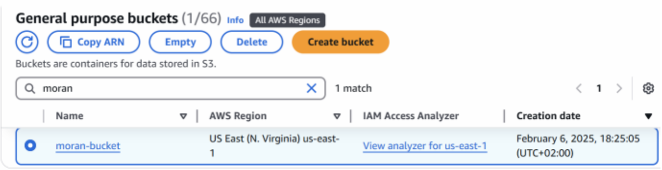
service endpoint:
EFS: within VPC
S3: within or without VPC
EBS: within VPC

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 backet versioning

   after creating bucket:



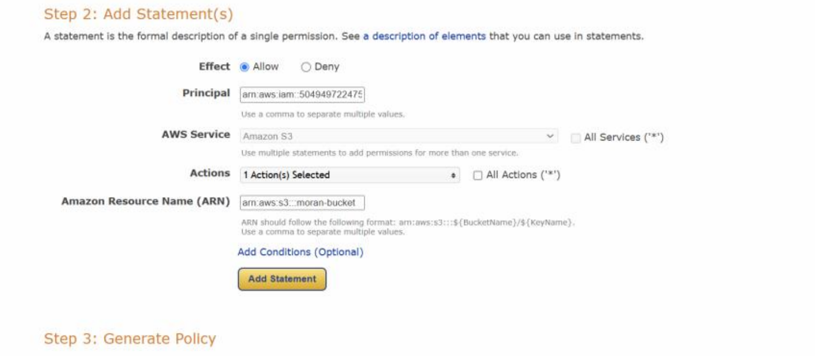
General purpose buckets (1/66)

Buckets are containers for data stored in S3.

moran

	Name	AWS Region	IAM Access Analyzer	Creation date
●	moran-bucket	US East (N. Virginia) us-east-1	View analyzer for us-east-1	February 6, 2025, 18:25:05 (UTC+02:00)

   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: arn:aws:iam::50494972247

Use a comma to separate multiple values.

AWS Service: Amazon S3 □ All Services ('*')

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

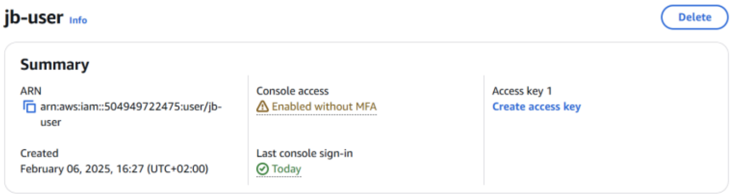
Actions: 1 Action(s) Selected □ All Actions ('*')

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

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

Step 3: Generate Policy

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



jb-user

Summary

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

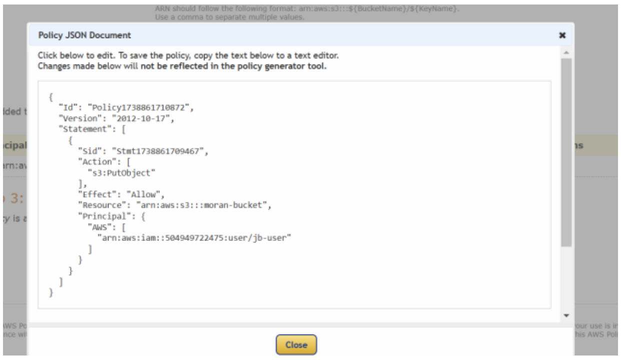
Console access: Enabled without MFA

Access key 1: Create access key

Created: February 06, 2025, 16:27 (UTC+02:00)

Last console sign-in: Today

   And create Jason file with the generastor:



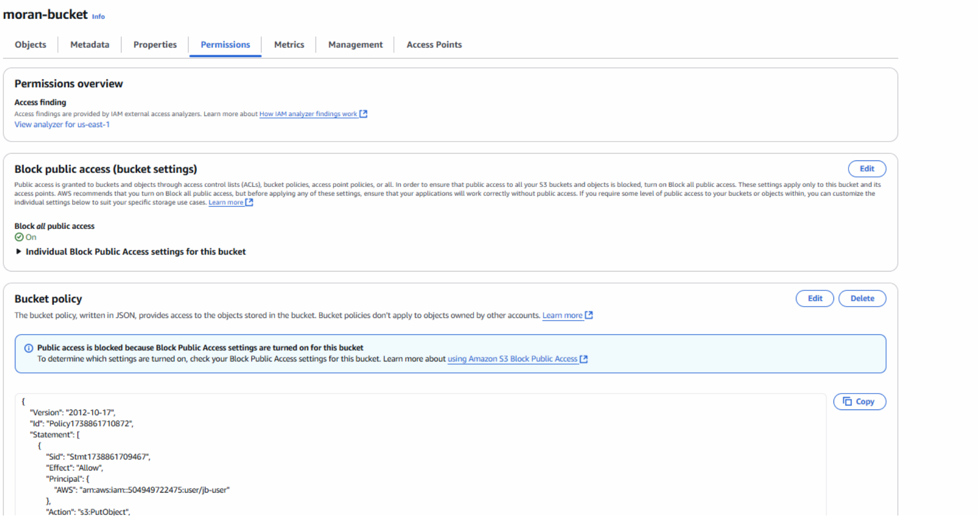
Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will not be reflected in the policy generator tool.

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

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

final:



moran-bucket

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

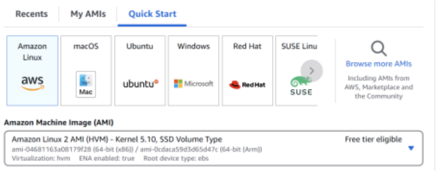
ⓘ **Public access is blocked because Block Public Access settings are turned on for this bucket**
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access

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

2. Launch ec2 instance:

ec2 name: moran-instance

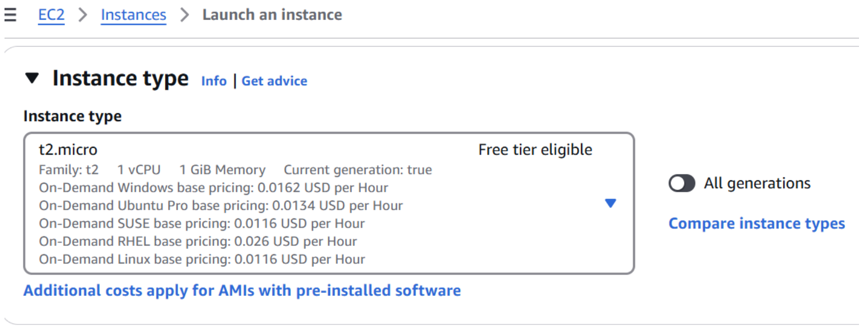
amazon machine image in my decision



Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type   Free tier eligible
ami-04681163a08179f28 (64-bit (x86)) / ami-0cdaca59d3d65d47c (64-bit (Arm))
Virtualization: hvm   ENA enabled: true   Root device type: ebs

Instance type as we asked for:



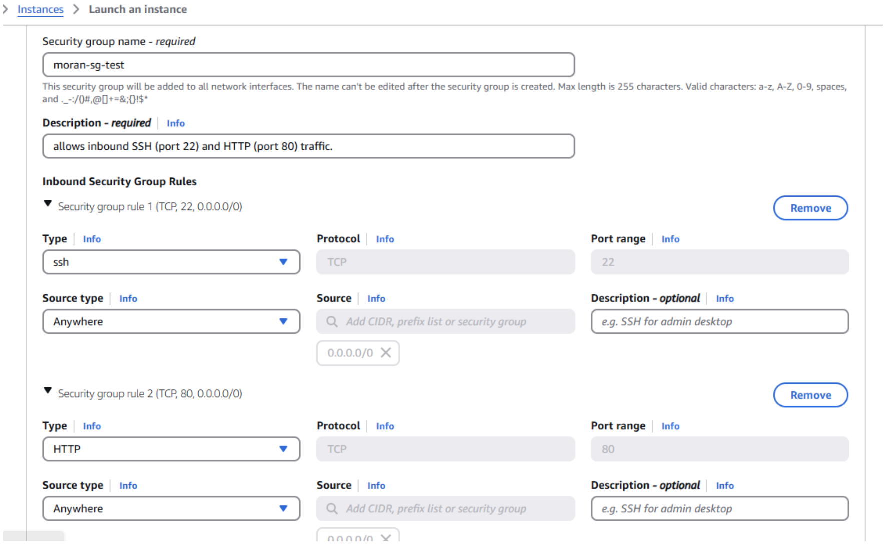
▼ Instance type

Instance type

t2.micro   Free tier eligible
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

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

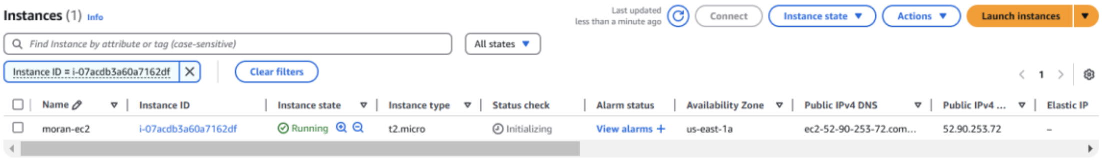
▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) — Remove

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 0.0.0.0/0 ✕	e.g. SSH for admin desktop

▼ 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 0.0.0.0/0 ✕	e.g. SSH for admin desktop

Final:



Instances (1) Info

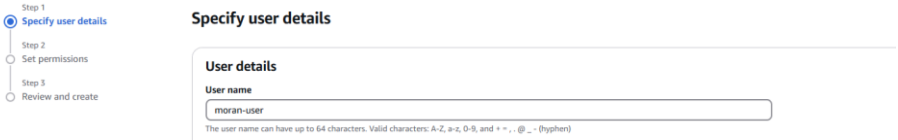
Find Instance by attribute or tag (case-sensitive)

Instance ID = i-07acdb3a60a7162df ✕

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
☐	moran-ec2	i-07acdb3a60a7162df	✓ Running	t2.micro	Initializing	View alarms +	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:



Specify user details

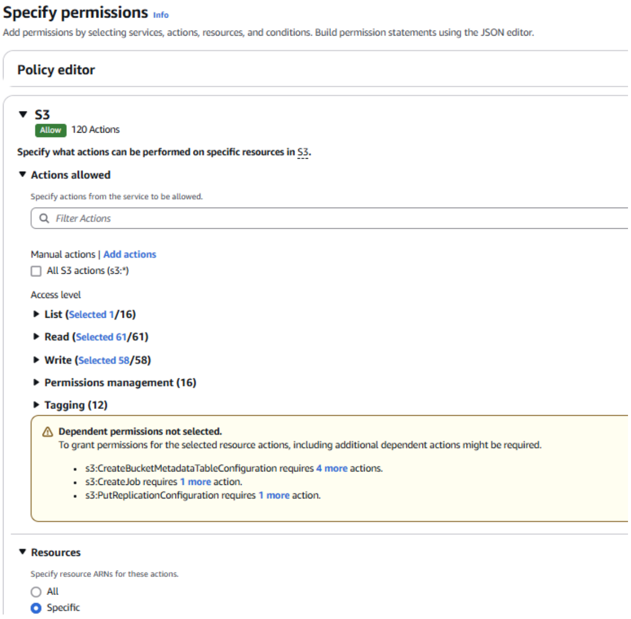
User details

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 perrmisions:



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.

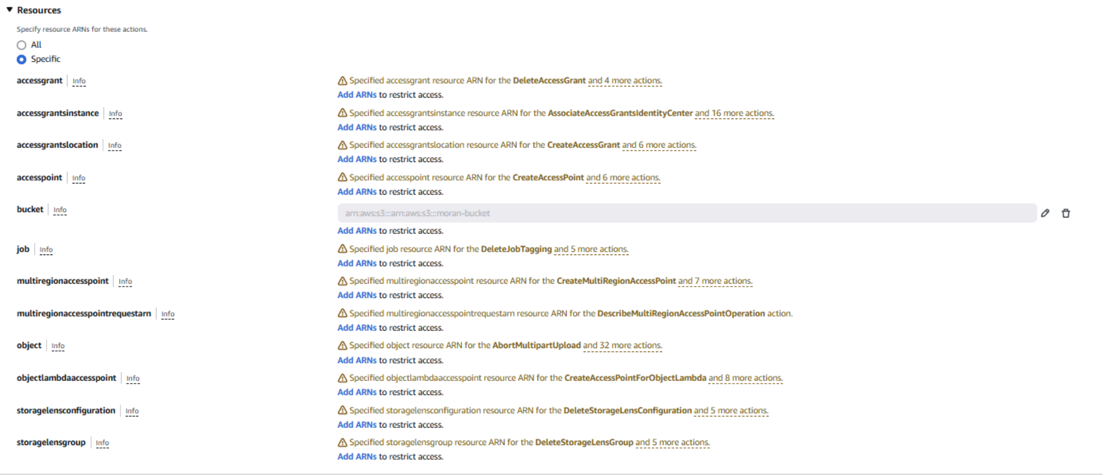
▼ **Resources**

Specify resource ARNs for these actions.

○ All
● Specific

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

only one specific bucket:

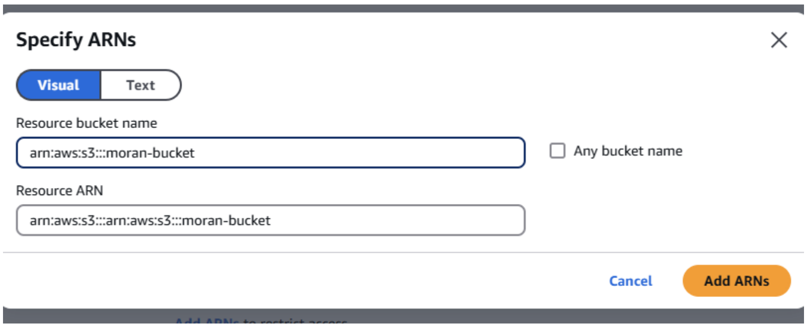


▼ Resources

Specify resource ARNs for these actions.

○ All
● Specific

accessgrant | Info	⚠ Specified accessgrant resource ARN for the **DeleteAccessGrant** and 4 more actions. Add ARNs to restrict access.
accessgrantsinstance | Info	⚠ Specified accessgrantsinstance resource ARN for the **AssociateAccessGrantsIdentityCenter** and 16 more actions. Add ARNs to restrict access.
accessgrantslocation | Info	⚠ Specified accessgrantslocation resource ARN for the **CreateAccessGrant** and 6 more actions. Add ARNs to restrict access.
accesspoint | Info	⚠ Specified accesspoint resource ARN for the **CreateAccessPoint** and 6 more actions. Add ARNs to restrict access.
bucket | Info	arn:aws:s3:::arn:aws:s3:::moran-bucket Add ARNs to restrict access.
job | Info	⚠ Specified job resource ARN for the **DeleteJobTagging** and 5 more actions. Add ARNs to restrict access.
multiregionaccesspoint | Info	⚠ Specified multiregionaccesspoint resource ARN for the **CreateMultiRegionAccessPoint** and 7 more actions. Add ARNs to restrict access.
multiregionaccesspointrequestarn | Info	⚠ Specified multiregionaccesspointrequestarn resource ARN for the **DescribeMultiRegionAccessPointOperation** action. Add ARNs to restrict access.
object | Info	⚠ Specified object resource ARN for the **AbortMultipartUpload** and 32 more actions. Add ARNs to restrict access.
objectlambdaaccesspoint | Info	⚠ Specified objectlambdaaccesspoint resource ARN for the **CreateAccessPointForObjectLambda** and 8 more actions. Add ARNs to restrict access.
storagelensconfiguration | Info	⚠ Specified storagelensconfiguration resource ARN for the **DeleteStorageLensConfiguration** and 5 more actions. Add ARNs to restrict access.
storagelensgroup | Info	⚠ Specified storagelensgroup resource ARN for the **DeleteStorageLensGroup** and 5 more actions. Add ARNs to restrict access.



Specify ARNs

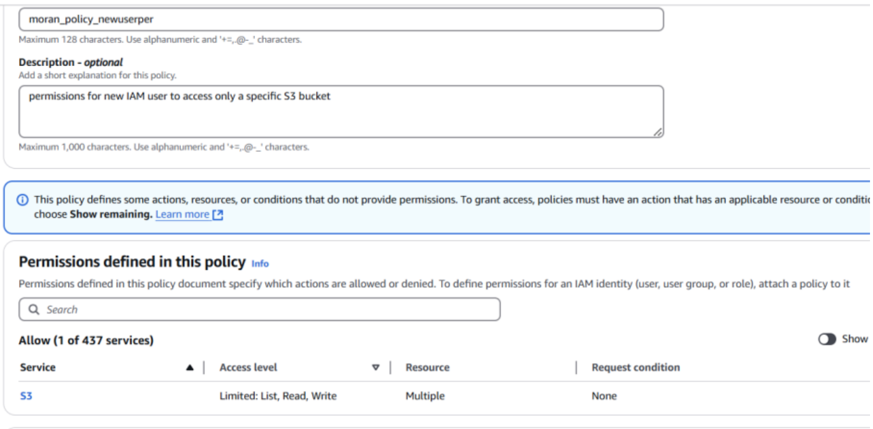
Resource bucket name

arn:aws:s3:::moran-bucket

□ Any bucket name

Resource ARN

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 conditi
choose **Show remaining.** Learn more

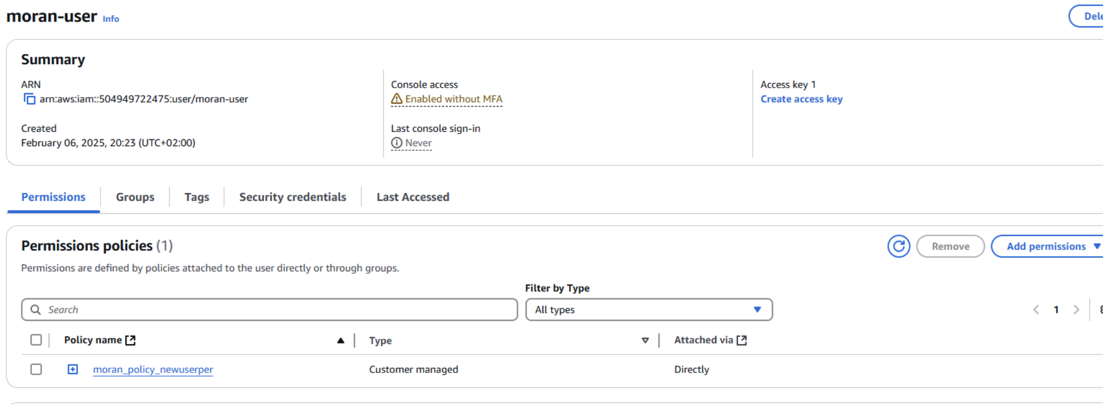
Permissions defined in this policy Info

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

Allow (1 of 437 services)

Service	Access level	Resource	Request condition
S3	Limited: List, Read, Write	Multiple	None

user details:



moran-user Info

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 policies (1)

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

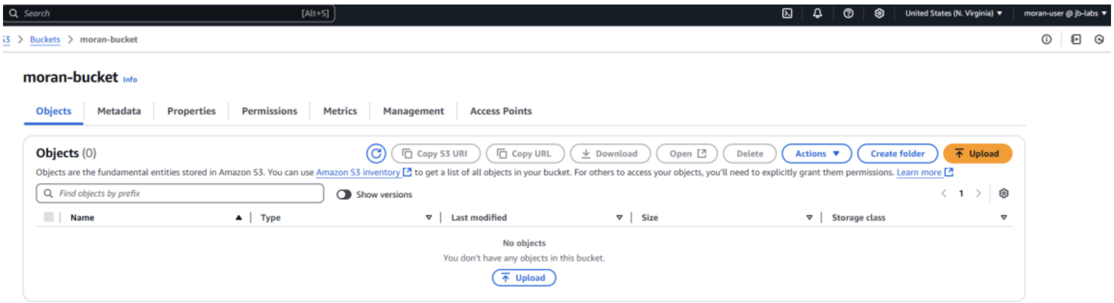
Filter by Type: All types

□	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:



moran-bucket

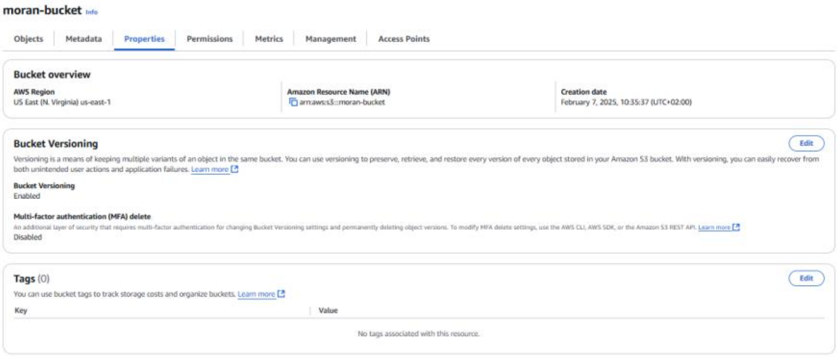
Objects (0)

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

Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.



moran-bucket

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, 10:35:37 (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

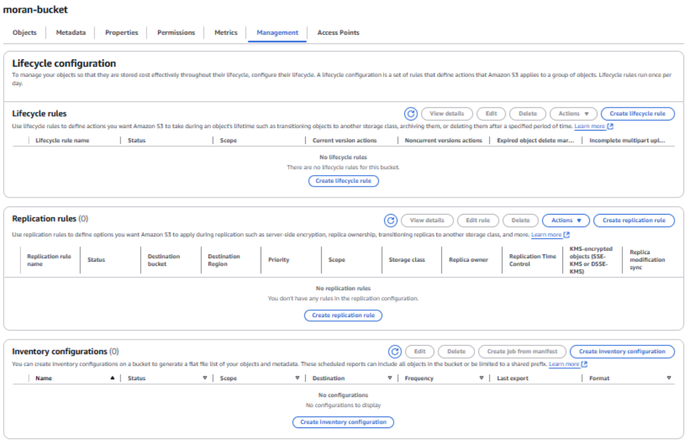
Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled

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

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.

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 DSSE-KMS)	Replica modification sync

No replication rules

You don't have any rules in the replication configuration.

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

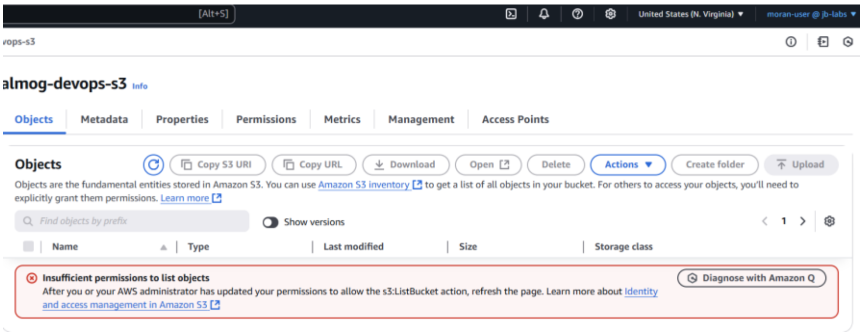
Name	Status	Scope	Destination	Frequency	Last export	Format

No configurations

No configurations to display

has permission!

Other buckets:



almog-devops-s3

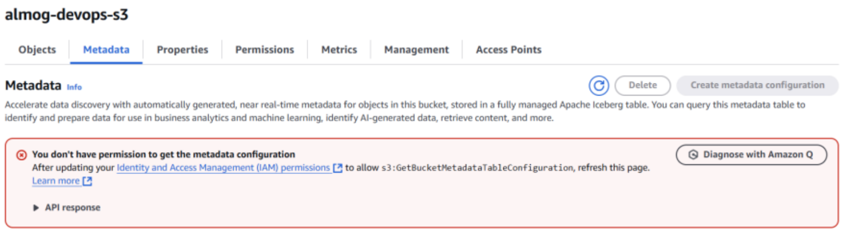
Objects

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

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

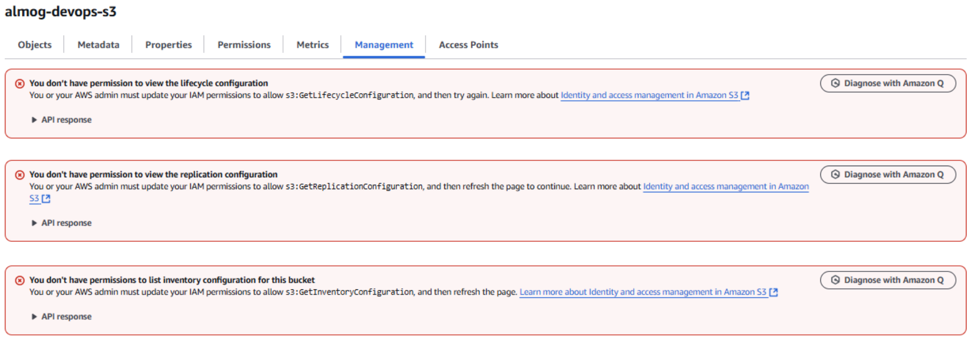


Accelerate data discovery with automatically generated, near real-time metadata for objects in this bucket, stored in a fully managed Apache Iceberg table. You can query this metadata table to identify and prepare data for use in business analytics and machine learning, identify AI-generated data, retrieve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

▶ API response



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

▶ API response

You don't have permission to view the replication configuration

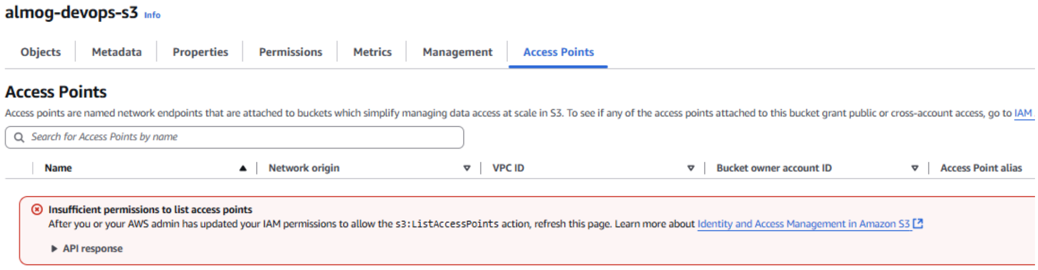
You or your AWS admin must update your IAM permissions to allow `s3:GetReplicationConfiguration`, and then refresh the page to continue. Learn more about Identity and access management in Amazon S3

▶ 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

▶ API response



Access Points

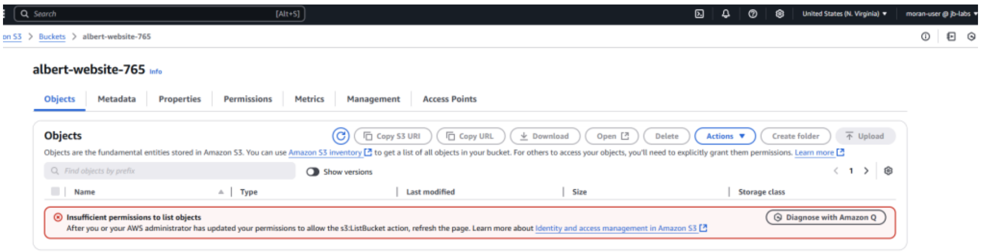
Access points are named network endpoints that are attached to buckets which simplify managing data access at scale in S3. To see if any of the access points attached to this bucket grant public or cross-account access, go to IAM

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

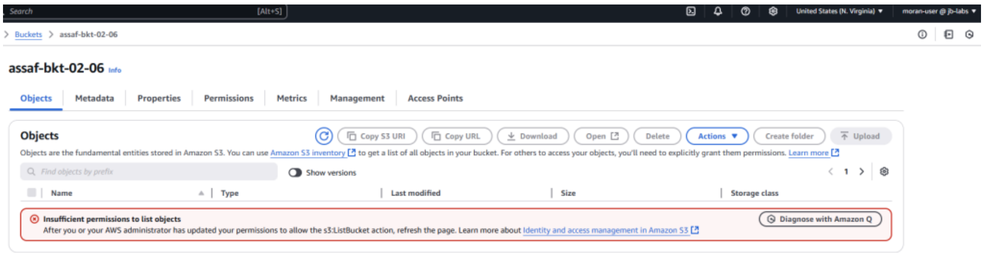


Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□ 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



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

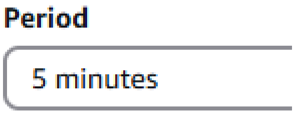
□ Name	Type	Last modified	Size	Storage class

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

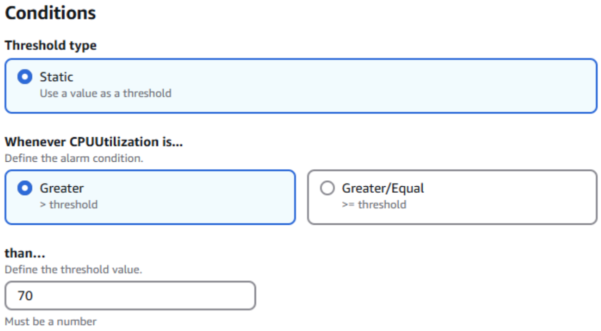
no permission! All the options are block.

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

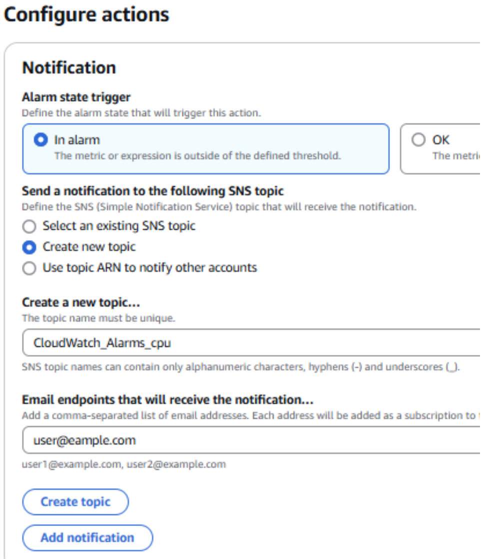
○ Greater/Equal
>= threshold

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 metri

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

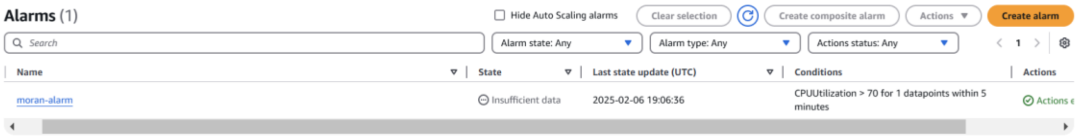
SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

Email endpoints that will receive the notification...
Add a comma-separated list of email addresses. Each address will be added as a subscription to t

user@eample.com

user1@example.com, user2@example.com

final:

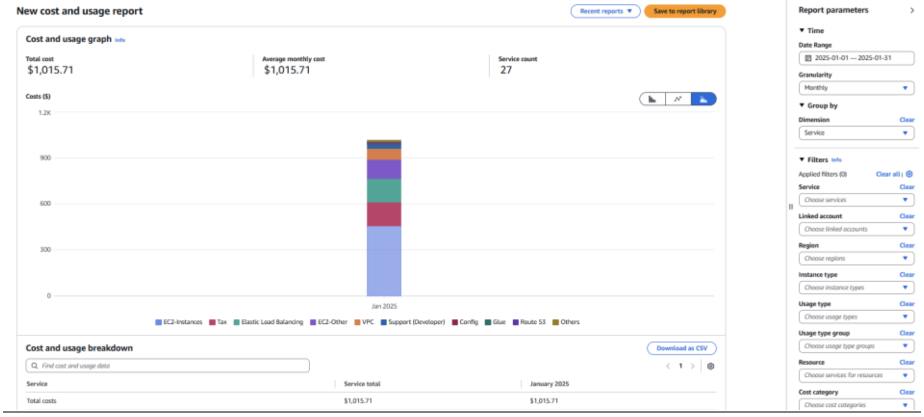


Alarms (1)

Name	State	Last state update (UTC)	Conditions	Actions
moran-alarm	Insufficient data	2025-02-06 19:06:36	CPUUtilization > 70 for 1 datapoints within 5 minutes	✓ Actions e

5. **Identify AWS Billing Costs:**

billing details from the last month:



New cost and usage report

Cost and usage graph

Total cost $1,015.71

Average monthly cost $1,015.71

Service count 27

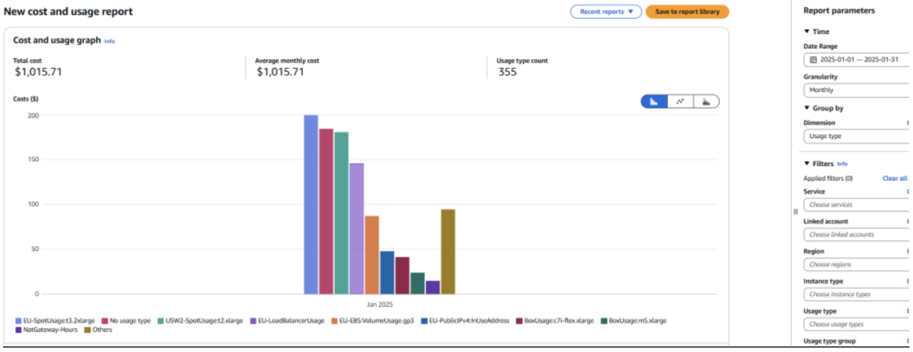
Cost and usage breakdown

Service	Service total	January 2025
Total costs	$1,015.71	$1,015.71

Report parameters

- Time
  - Date Range: 2025-01-01 — 2025-01-31
  - Granularity: Monthly
- Group by
  - Dimension: Service
- Filters
  - Applied filters (0)
  - Service
  - Linked account
  - Region
  - Instance type
  - Usage type
  - Usage type group
  - Resource
  - Cost category

analyze usage:



New cost and usage report

Cost and usage graph

Total cost $1,015.71

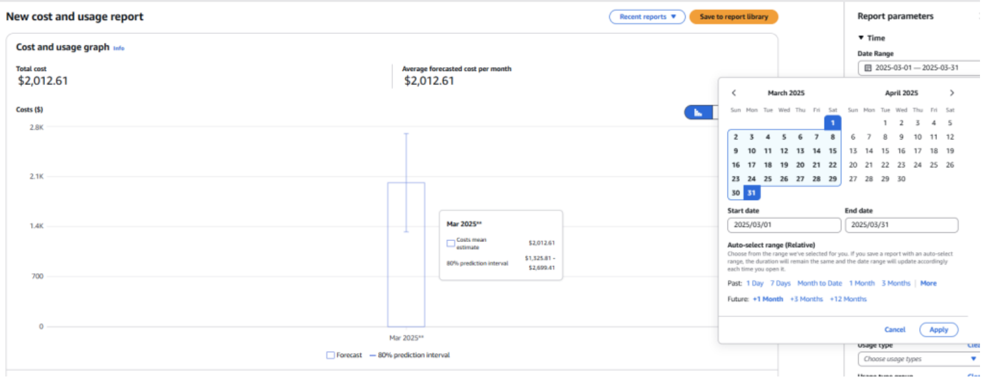
Average monthly cost $1,015.71

Usage type count 355

Report parameters

- Time
  - Date Range: 2025-01-01 — 2025-01-31
  - Granularity: Monthly
- Group by
  - Dimension: Usage type
- Filters
  - Applied filters (0)
  - Service
  - Linked account
  - Region
  - Instance type
  - Usage type
  - Usage type group

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.



New cost and usage report

Cost and usage graph

Total cost $2,012.61

Average forecasted cost per month $2,012.61

Mar 2025**
Costs mean estimate $2,012.61
80% prediction interval $1,325.81 - $2,699.41

Report parameters

- Time
  - Date Range: 2025-03-01 — 2025-03-31

Start date 2025/03/01

End date 2025/03/31

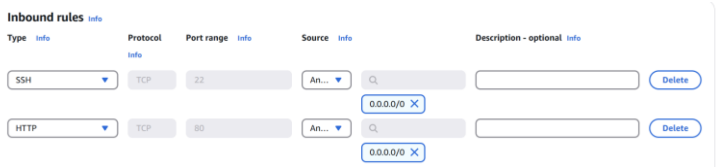
Auto-select range (Relative)

Choose from the range we've selected for you. If you save a report with an auto-select range, the duration will remain the same and the date range will update accordingly each time you open it.

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

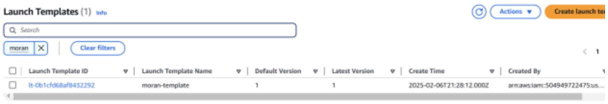
Type	Protocol	Port range	Source		Description - optional
SSH	TCP	22	An...	0.0.0.0/0	
HTTP	TCP	80	An...	0.0.0.0/0	

Creating auto scaling:

launch template: moran-template

AMI: Amazon Linux 2 AMI

instance type: t2.micro

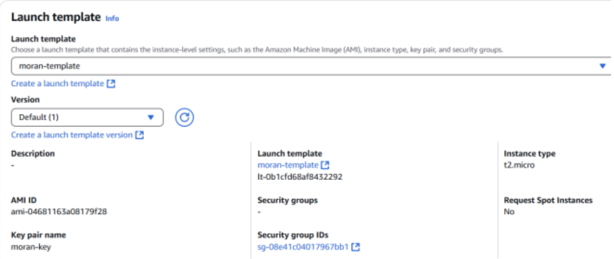


Launch Templates (1)

moran

Launch Template ID	Launch Template Name	Default Version	Latest Version	Create Time	Created By
lt-0b1cfd68af8432292	moran-template	1	1	2025-02-06T21:28:12.000Z	arn:aws:iam::504949722475:us...

using launch template in the auto scaling



Launch template

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.

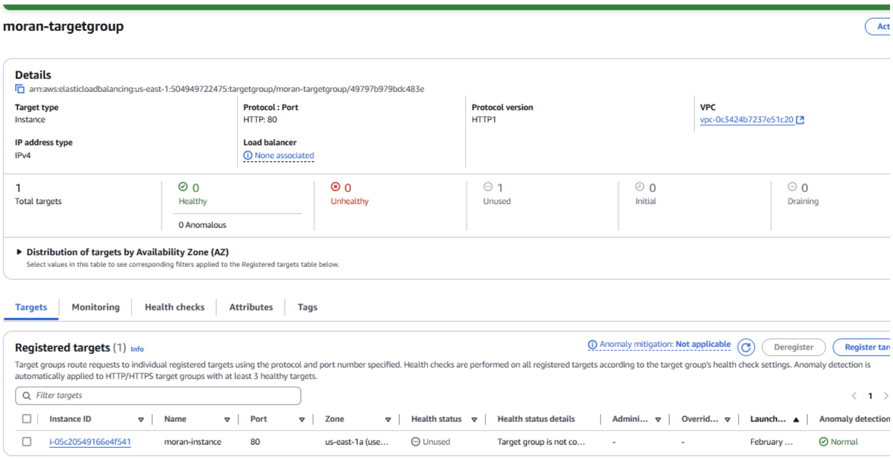
moran-template

Version

Default (1)

Description -	Launch template moran-template lt-0b1cfd68af8432292	Instance type t2.micro
AMI ID ami-04681163a08179f28	Security groups -	Request Spot Instances No
Key pair name moran-key	Security group IDs sg-08e41c04017967bb1	

Create target group:



moran-targetgroup

Details

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

Target type Instance	Protocol : Port HTTP: 80	Protocol version HTTP1	VPC vpc-0c3424b7237e51c20
IP address type IPv4	Load balancer None associated		

1 Total targets	0 Healthy 0 Anomalous	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.

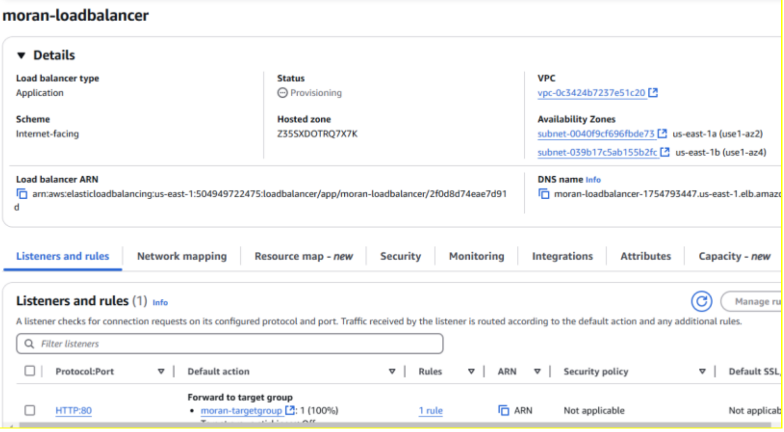
Registered targets (1)

Anomaly mitigation: Not applicable

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	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
Z35SXDOTRQ7X7K

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/2f0d8d74eae7d91
d

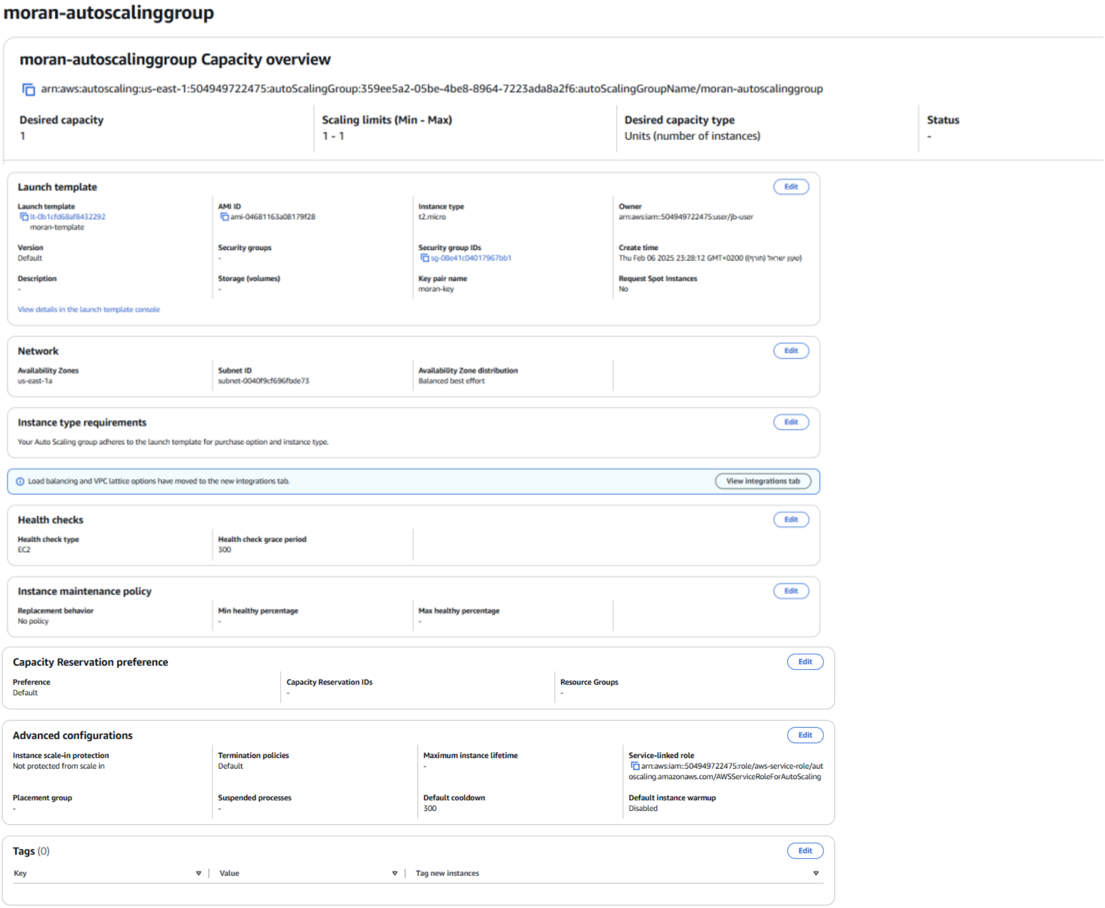
DNS name Info
moran-loadbalancer-1754793447.us-east-1.elb.amaz

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
□	HTTP:80	Forward to target group • moran-targetgroup: 1 (100%)	1 rule	ARN	Not applicable	Not applicab

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	Scaling limits (Min - Max)	Desired capacity type	Status
1	1 - 1	Units (number of instances)	-

Launch template

Launch template	AMI ID	Instance type	Owner
lt-0b1cfd68af8432292 moran-template	ami-04681163a08179f28	t2.micro	arn:aws:iam::504949722475:user/jb-user
Version Default	**Security groups** -	**Security group IDs** sg-08e41c04017967bb1	**Create time** Thu Feb 06 2025 23:28:12 GMT+0200 (שעון ישראל (חורף))
Description -	**Storage (volumes)** -	**Key pair name** moran-key	**Request Spot Instances** No

View details in the launch template console

Network

Availability Zones	Subnet ID	Availability Zone distribution
us-east-1a	subnet-0040f9cf696fbde73	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.

Health checks

Health check type	Health check grace period
EC2	300

Instance maintenance policy

Replacement behavior	Min healthy percentage	Max healthy percentage
No policy	-	-

Capacity Reservation preference

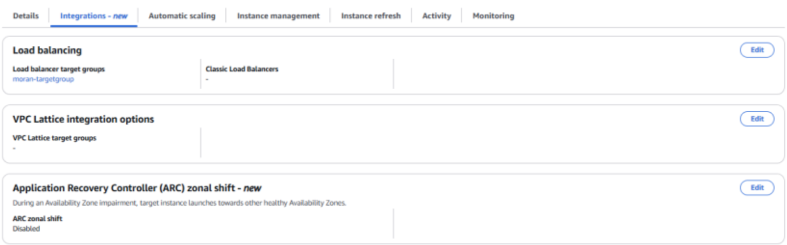
Preference	Capacity Reservation IDs	Resource Groups
Default	-	-

Advanced configurations

Instance scale-in protection	Termination policies	Maximum instance lifetime	Service-linked role
Not protected from scale in	Default	-	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



Load balancing

Load balancer target groups	Classic Load Balancers
moran-targetgroup	-

VPC Lattice integration options

VPC Lattice target groups
-

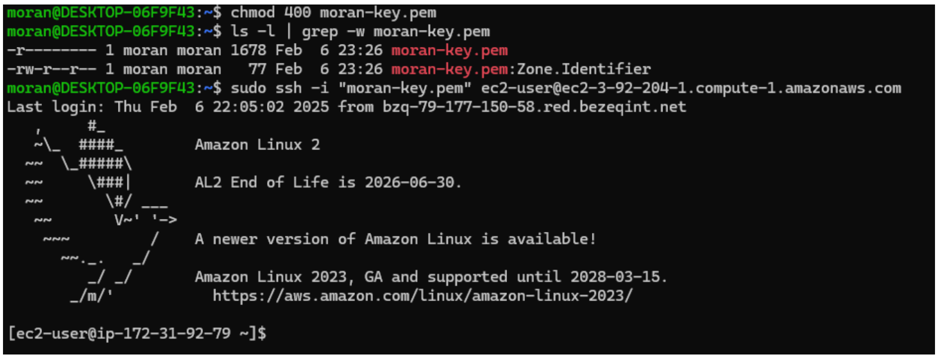
Application Recovery Controller (ARC) zonal shift - *new*

During an Availability Zone impairment, target instance launches towards other healthy Availability Zones.

ARC zonal shift
Disabled

2. Connect to the EC2 Instance and Install Nginx

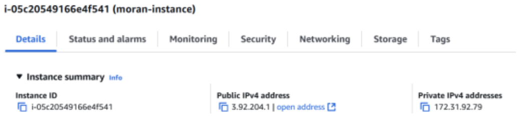
connecting to the machine with ssh:



```
moran@DESKTOP-06F9F43:~$ chmod 400 moran-key.pem
moran@DESKTOP-06F9F43:~$ ls -l | grep -w moran-key.pem
-r-------- 1 moran moran 1678 Feb  6 23:26 moran-key.pem
-rw-r--r-- 1 moran moran   77 Feb  6 23:26 moran-key.pem:Zone.Identifier
moran@DESKTOP-06F9F43:~$ sudo ssh -i "moran-key.pem" ec2-user@ec2-3-92-204-1.compute-1.amazonaws.com
Last login: Thu Feb  6 22:05:02 2025 from bzq-79-177-150-58.red.bezeqint.net
   ,     #_
   ~\_  ####_        Amazon Linux 2
  ~~  \_#####\
  ~~     \###|       AL2 End of Life is 2026-06-30.
  ~~       \#/ ___
   ~~       V~' '->
    ~~~         /    A newer version of Amazon Linux is available!
      ~~._.   _/
         _/ _/       Amazon Linux 2023, GA and supported until 2028-03-15.
       _/m/'           https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-172-31-92-79 ~]$
```

checking same privet ip:

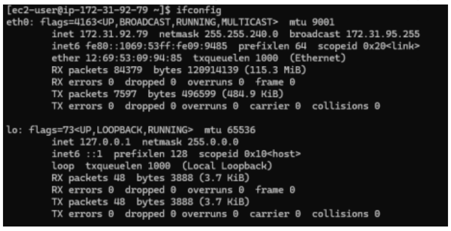


i-05c20549166e4f541 (moran-instance)

Instance ID: i-05c20549166e4f541

Public IPv4 address: 3.92.204.1

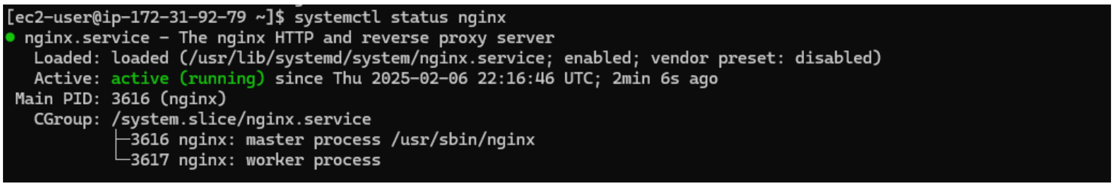
Private IPv4 addresses: 172.31.92.79



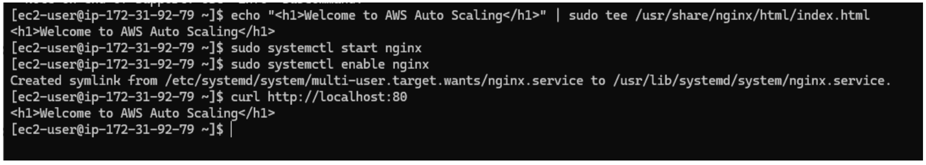
```
[ec2-user@ip-172-31-92-79 ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 172.31.92.79  netmask 255.255.240.0  broadcast 172.31.95.255
        inet6 fe80::1069:53ff:fe09:9485  prefixlen 64  scopeid 0x20<link>
        ether 12:69:53:09:94:85  txqueuelen 1000  (Ethernet)
        RX packets 84379  bytes 120914139 (115.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7597  bytes 496599 (484.9 KiB)
        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
```

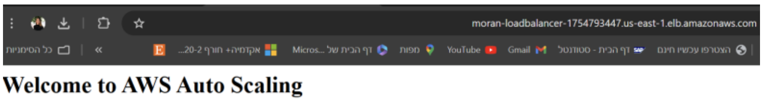


```
[ec2-user@ip-172-31-92-79 ~]$ echo "<h1>Welcome to AWS Auto Scaling</h1>" | sudo tee /usr/share/nginx/html/index.html
<h1>Welcome to AWS Auto Scaling</h1>
[ec2-user@ip-172-31-92-79 ~]$ sudo systemctl start nginx
[ec2-user@ip-172-31-92-79 ~]$ sudo systemctl enable nginx
Created symlink from /etc/systemd/system/multi-user.target.wants/nginx.service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

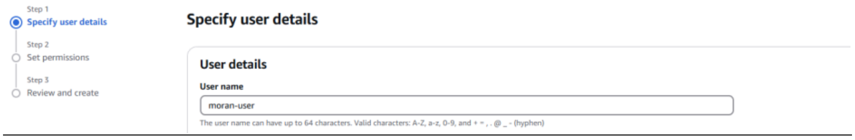


moran-loadbalancer-1754793447.us-east-1.elb.amazonaws.com

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:



Specify user details

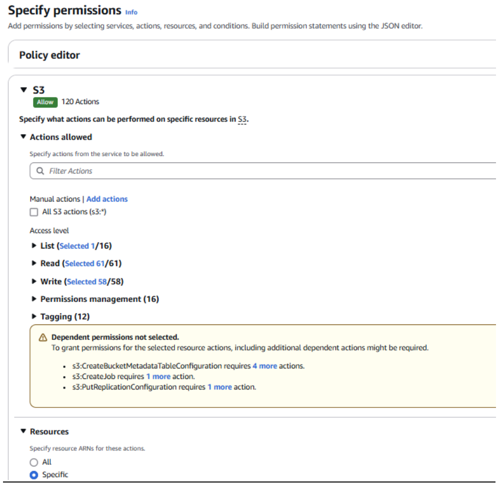
User details

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 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.

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.

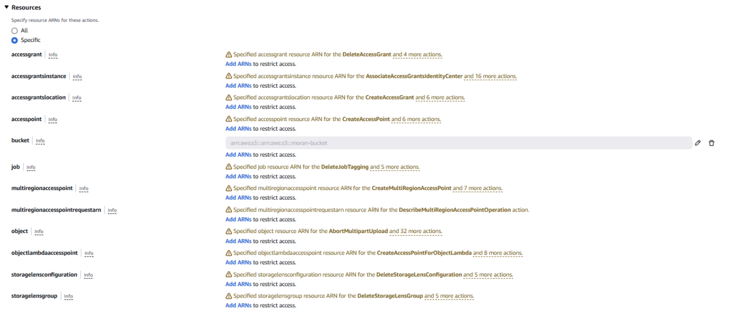
▼ Resources

Specify resource ARNs for these actions.

○ All

● Specific

only one specific bucket- moran-bucket:

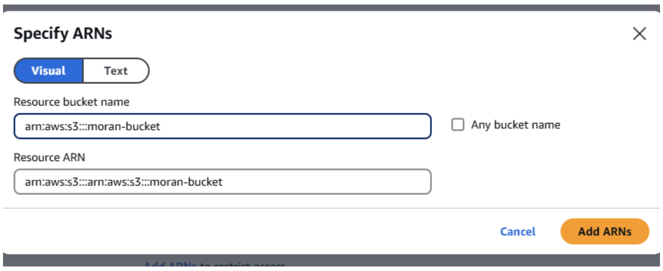

▼ Resources

Specify resource ARNs for these actions.

○ All

● Specific

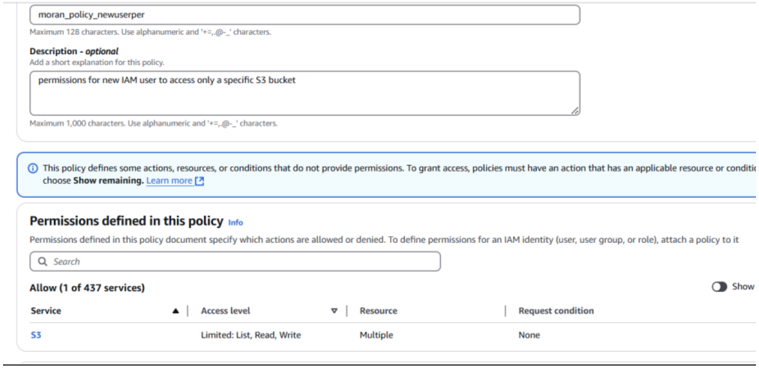
accessgrant | Info	⚠ Specified accessgrant resource ARN for the DeleteAccessGrant and 4 more actions. Add ARNs to restrict access.
accessgrantsinstance | Info	⚠ Specified accessgrantsinstance resource ARN for the AssociateAccessGrantsIdentityCenter and 16 more actions. Add ARNs to restrict access.
accessgrantslocation | Info	⚠ Specified accessgrantslocation resource ARN for the CreateAccessGrant and 6 more actions. Add ARNs to restrict access.
accesspoint | Info	⚠ Specified accesspoint resource ARN for the CreateAccessPoint and 6 more actions. Add ARNs to restrict access.
bucket | Info	arn:aws:s3:::arn:aws:s3:::moran-bucket Add ARNs to restrict access.
job | Info	⚠ Specified job resource ARN for the DeleteJobTagging and 5 more actions. Add ARNs to restrict access.
multiregionaccesspoint | Info	⚠ Specified multiregionaccesspoint resource ARN for the CreateMultiRegionAccessPoint and 7 more actions. Add ARNs to restrict access.
multiregionaccesspointrequestarn | Info	⚠ Specified multiregionaccesspointrequestarn resource ARN for the DescribeMultiRegionAccessPointOperation action. Add ARNs to restrict access.
object | Info	⚠ Specified object resource ARN for the AbortMultipartUpload and 32 more actions. Add ARNs to restrict access.
objectlambdaaccesspoint | Info	⚠ Specified objectlambdaaccesspoint resource ARN for the CreateAccessPointForObjectLambda and 8 more actions. Add ARNs to restrict access.
storagelensconfiguration | Info	⚠ Specified storagelensconfiguration resource ARN for the DeleteStorageLensConfiguration and 5 more actions. Add ARNs to restrict access.
storagelensgroup | Info	⚠ Specified storagelensgroup resource ARN for the DeleteStorageLensGroup and 5 more actions. Add ARNs to restrict access.


Specify ARNs

Resource bucket name: arn:aws:s3:::moran-bucket

□ Any bucket name

Resource ARN: 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 conditi choose **Show remaining.** Learn more

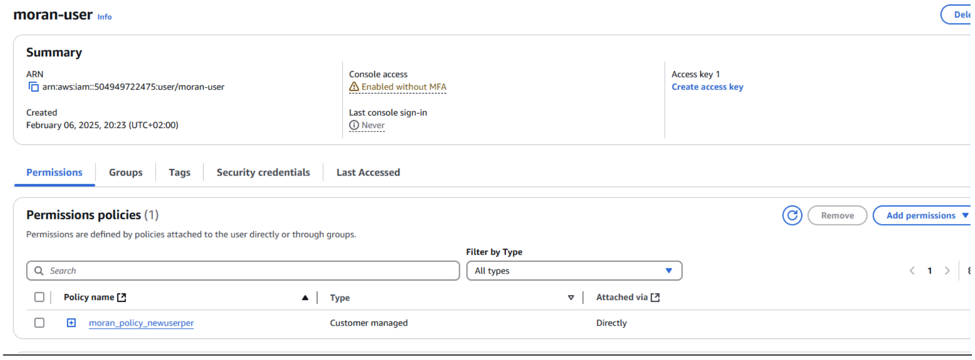
Permissions defined in this policy Info

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

Allow (1 of 437 services)

Service	Access level	Resource	Request condition
S3	Limited: List, Read, Write	Multiple	None

user details + we can see the attached policy:



moran-user Info

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 policies (1)

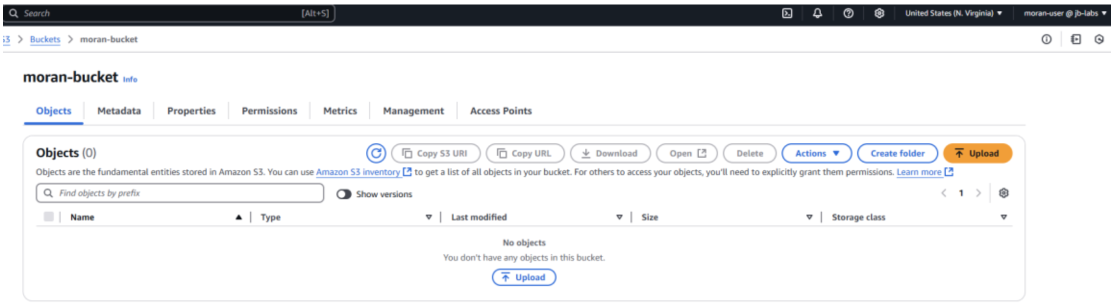
Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

□	Policy name	Type	Attached via
□	moran_policy_newuserper	Customer managed	Directly

Verify:

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



moran-bucket Info

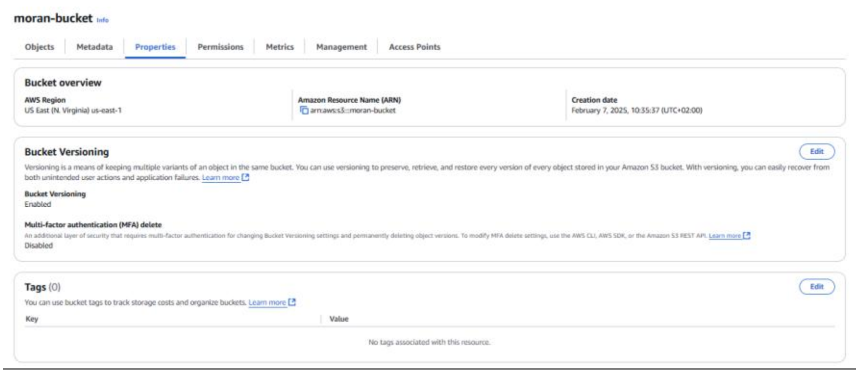
Objects (0)

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

□	Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.



moran-bucket Info

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, 10:35:37 (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

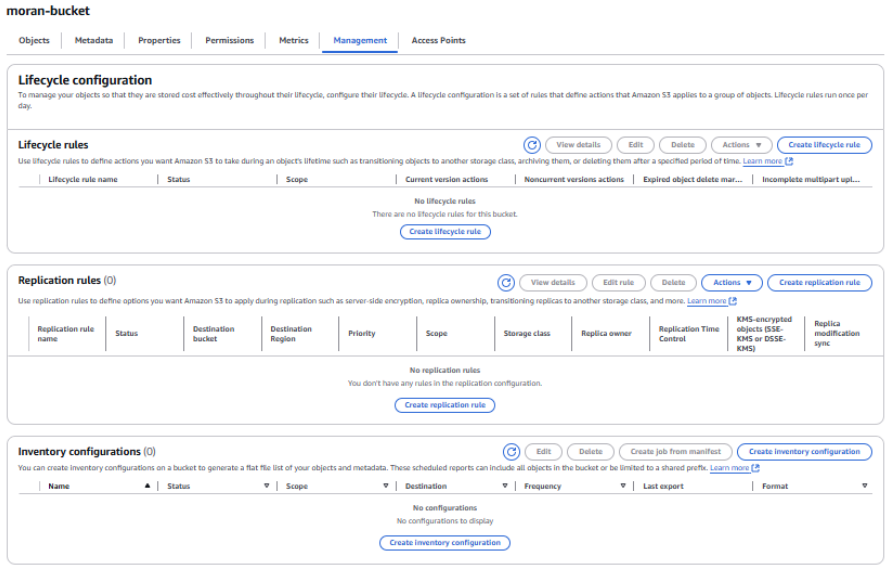
Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled

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

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.

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 DSSE-KMS)	Replica modification sync

No replication rules

You don't have any rules in the replication configuration.

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

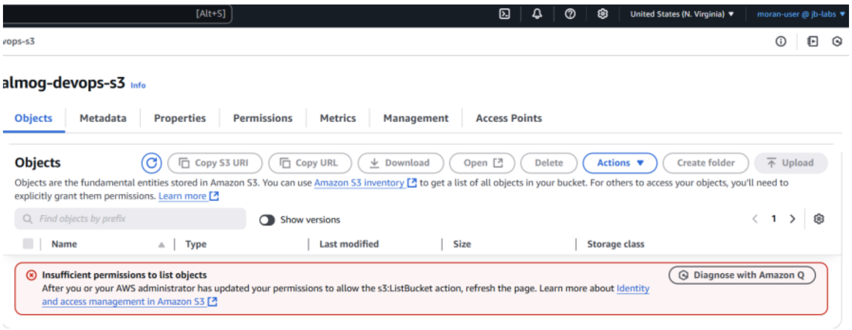
Name ▲	Status ▽	Scope ▽	Destination ▽	Frequency ▽	Last export	Format ▽

No configurations

No configurations to display

<u>has permission!</u>

Other buckets:



almog-devops-s3

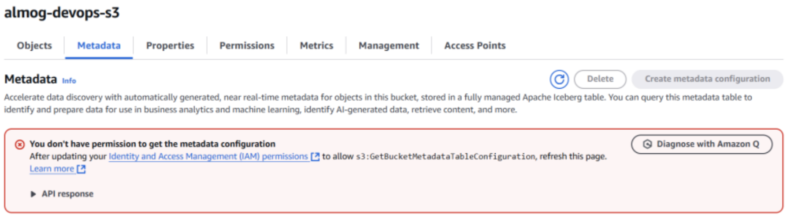
Objects

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

□	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



almog-devops-s3

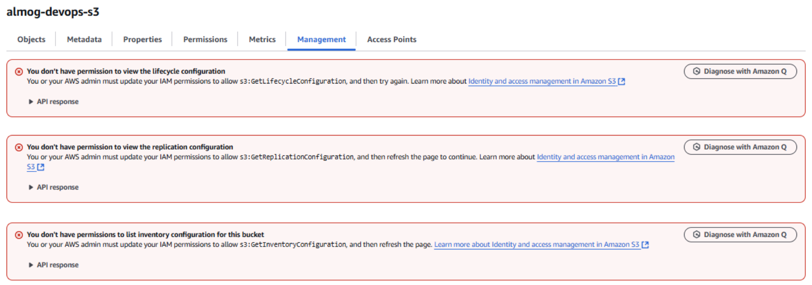
Metadata

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

▶ API response



almog-devops-s3

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

▶ API response

You don't have permission to view the replication configuration

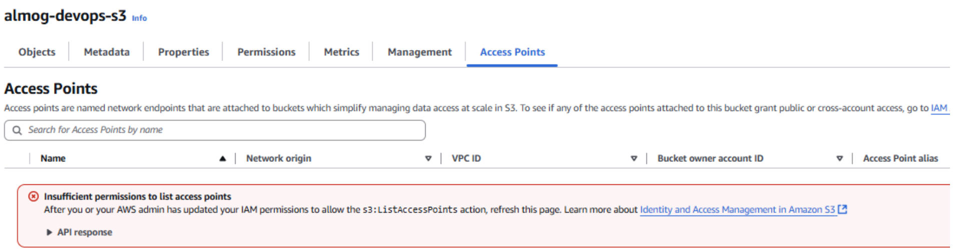
You or your AWS admin must update your IAM permissions to allow `s3:GetReplicationConfiguration`, and then refresh the page to continue. Learn more about Identity and access management in Amazon S3

▶ 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

▶ API response



almog-devops-s3 Info

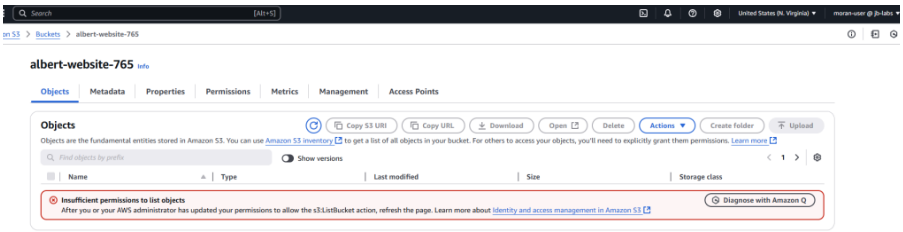
Access Points

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



Search [Alt+S]
United States (N. Virginia) ▾
moran-user @ jb-labs ▾
on S3 > Buckets > albert-website-765

albert-website-765 Info

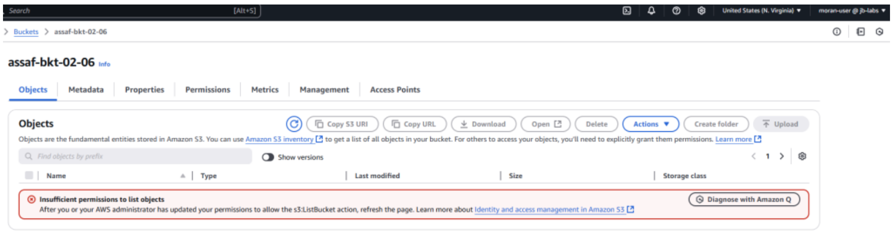
Objects

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

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



assaf-bkt-02-06 Info

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

Name	Type	Last modified	Size	Storage class

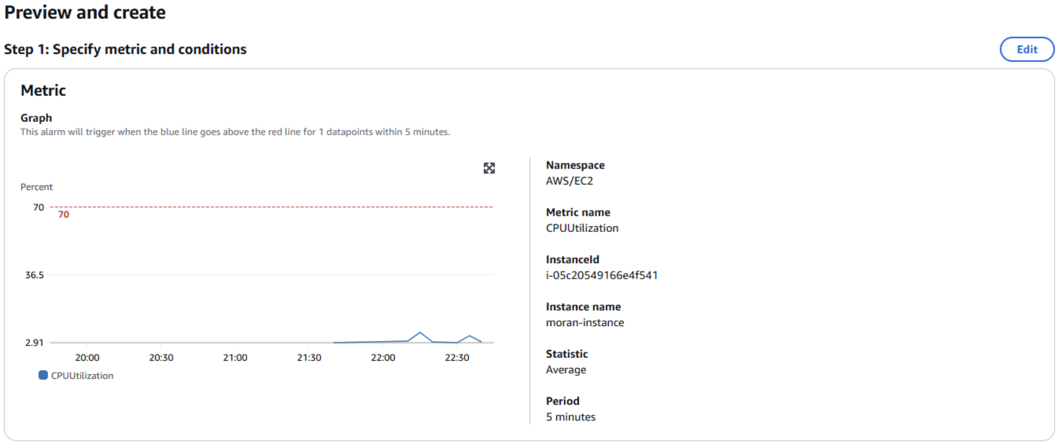
Insufficient permissions to list objects

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

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

Metric

Graph

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

Namespace
AWS/EC2

Metric name
CPUUtilization

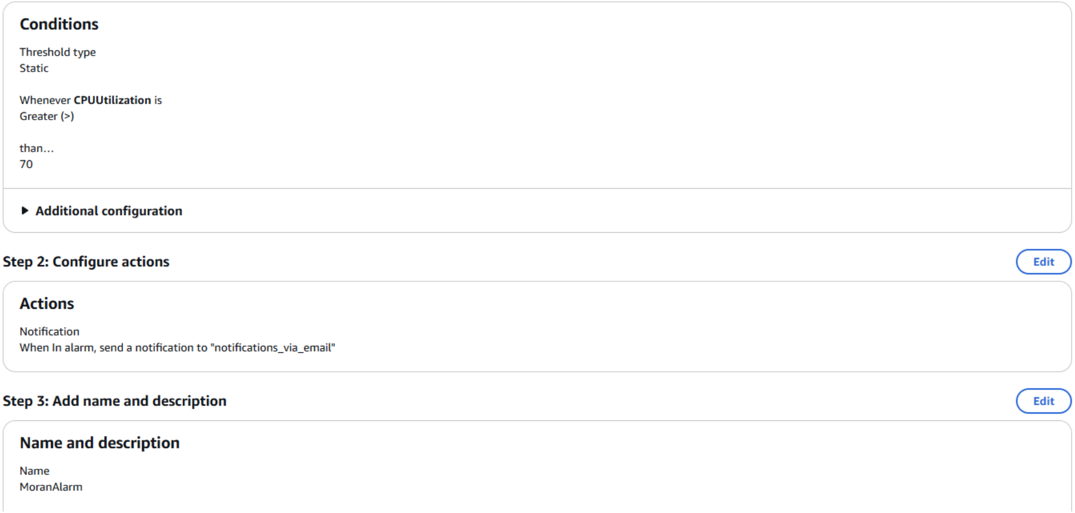
InstanceId
i-05c20549166e4f541

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

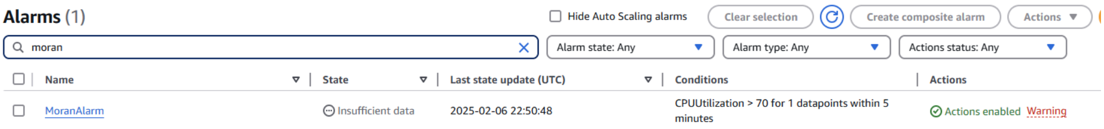
Actions

Notification
When In alarm, send a notification to "notifications_via_email"

Step 3: Add name and description

Name and description

Name
MoranAlarm



Alarms (1)

□	Name	State	Last state update (UTC)	Conditions	Actions
□	MoranAlarm	Insufficient data	2025-02-06 22:50:48	CPUUtilization > 70 for 1 datapoints within 5 minutes	✓ Actions enabled Warning