AWS S3 – Buckets & Alerts

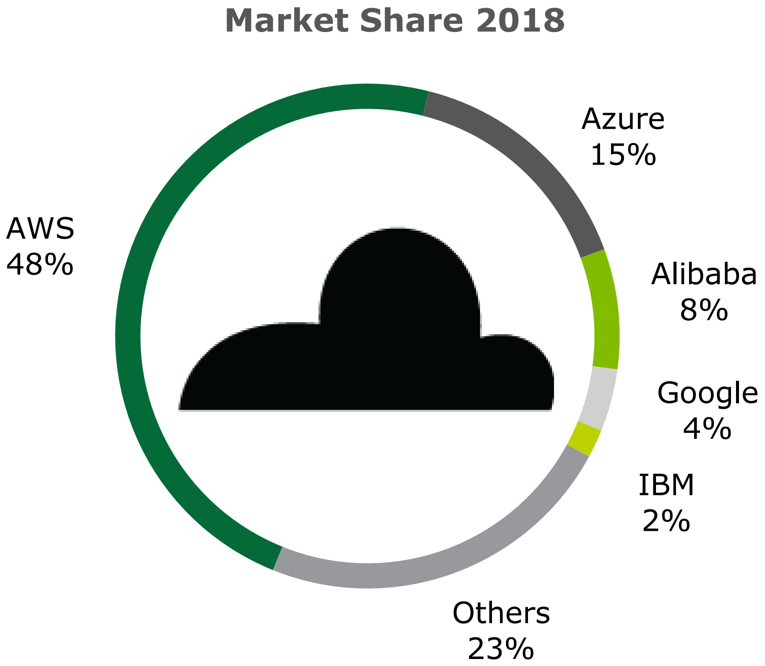
By: Eido Epstein

November 2019

www.linkedin.com
/in/
eido-epstein

The Big Players

Market share & an introduction of the top two



Microsoft Azure

- Estimated annual revenue run rate: 11B
- Growth rate Q3‘19: 59%
- Top services: AppS, VMs, DevOps

- Windows & Linux compatible
- 12 months free

amazon web services

- Annual revenue ‘18: 25.65B
- Growth rate Q3‘19: 35%
- Top services: EC2, RDS, S3

- Highly customizable
- Free Trial option

Amazon S3

Introduction

"Provides developers and IT teams with safe secure object Storage". - AWS

👍

- Durability
- Low cost
- Scalability
- Secured
- Availability
- Flexible

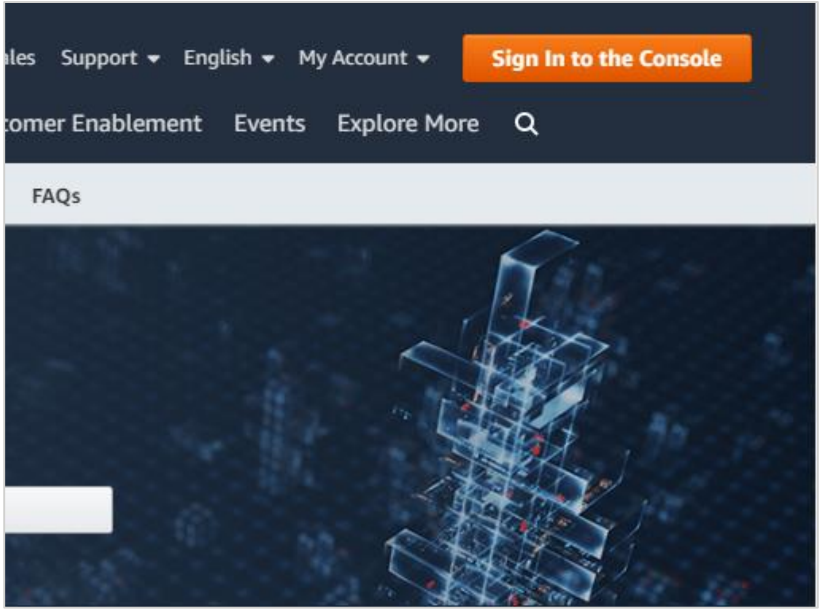
👎

- UI
- Documentation
- Only static websites

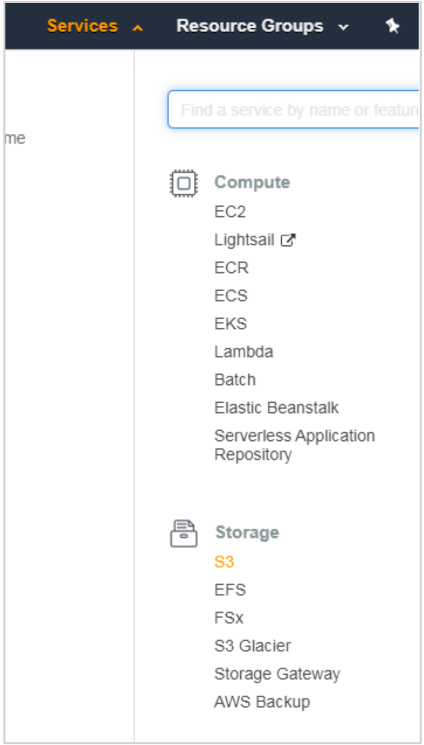
S3 Bucket

Step by step process- creating a bucket

01 Go to AWS S3 and press- “Sign in to the console”.
Following, input your credentials.



02 In your ACP, under the “Services” tab,
go to “Storage”, “S3”.



Definition:
An object consists of data, key (assigned name) and metadata.
A bucket stores objects.

S3 Bucket

Step by step process- creating a bucket

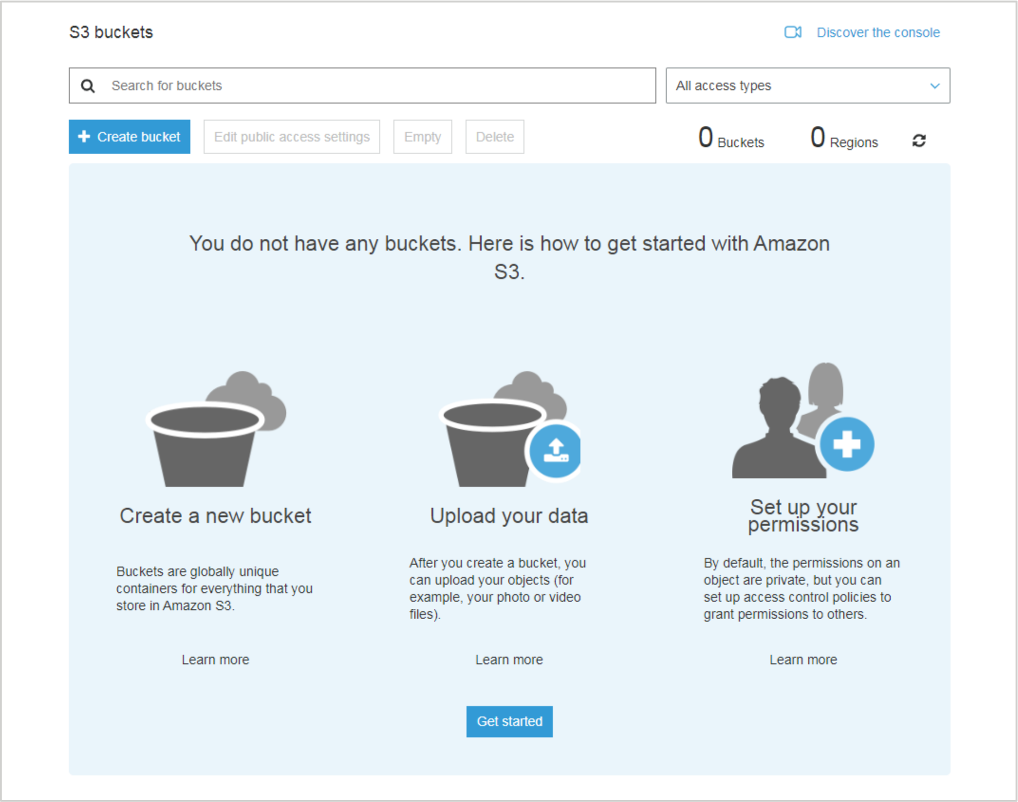
03

In the S3 Console, press on "Create Bucket".

04

"Create Bucket – Name and region"

- **Bucket name**
- **Region**



S3 buckets

Discover the console

Search for buckets

All access types

+ Create bucket | Edit public access settings | Empty | Delete

0 Buckets 0 Regions

You do not have any buckets. Here is how to get started with Amazon S3.

Create a new bucket

Buckets are globally unique containers for everything that you store in Amazon S3.

Learn more

Upload your data

After you create a bucket, you can upload your objects (for example, your photo or video files).

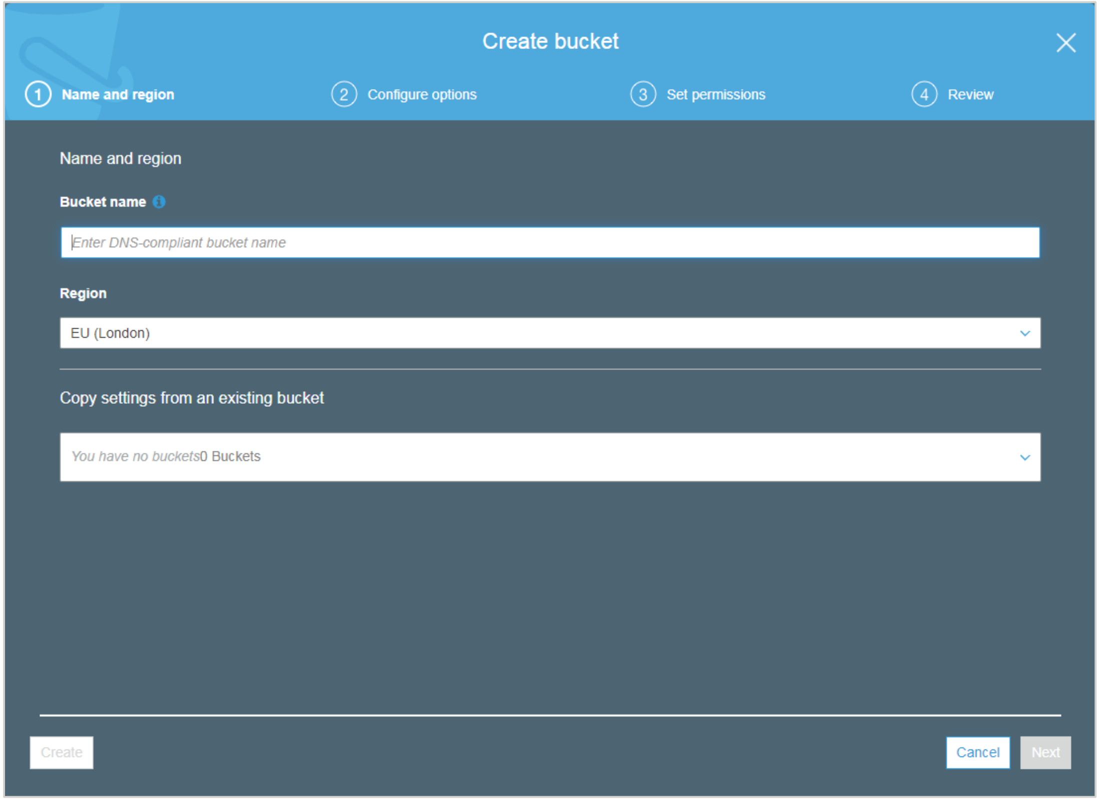
Learn more

Set up your permissions

By default, the permissions on an object are private, but you can set up access control policies to grant permissions to others.

Learn more

Get started



Create bucket

1 Name and region | 2 Configure options | 3 Set permissions | 4 Review

Name and region

Bucket name

Enter DNS-compliant bucket name

Region

EU (London)

Copy settings from an existing bucket

You have no buckets0 Buckets

Create | Cancel | Next

S3 Bucket

Step by step process- creating a bucket

05

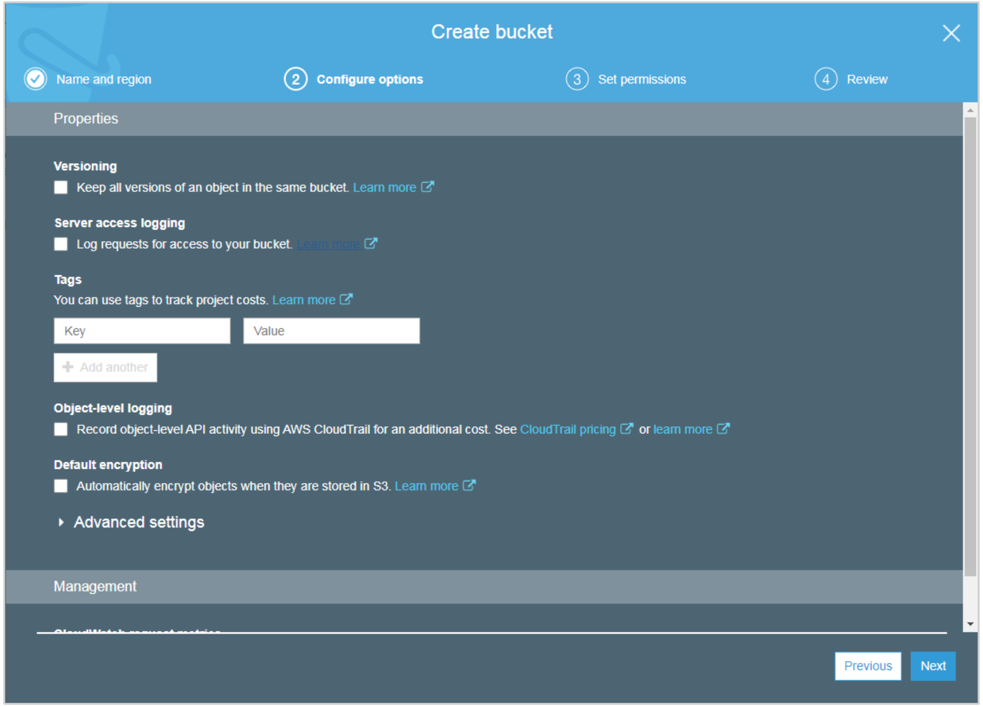
"Create Bucket – Configure options"

- **Versioning**
- **Server access logging**

06

"Create Bucket – Set permissions"

- **Block *all* public access**



Create bucket

✓ Name and region
② **Configure options**
③ Set permissions
④ Review

Properties

Versioning

□ Keep all versions of an object in the same bucket. Learn more

Server access logging

□ Log requests for access to your bucket. Learn more

Tags

You can use tags to track project costs. Learn more

Key | Value

+ Add another

Object-level logging

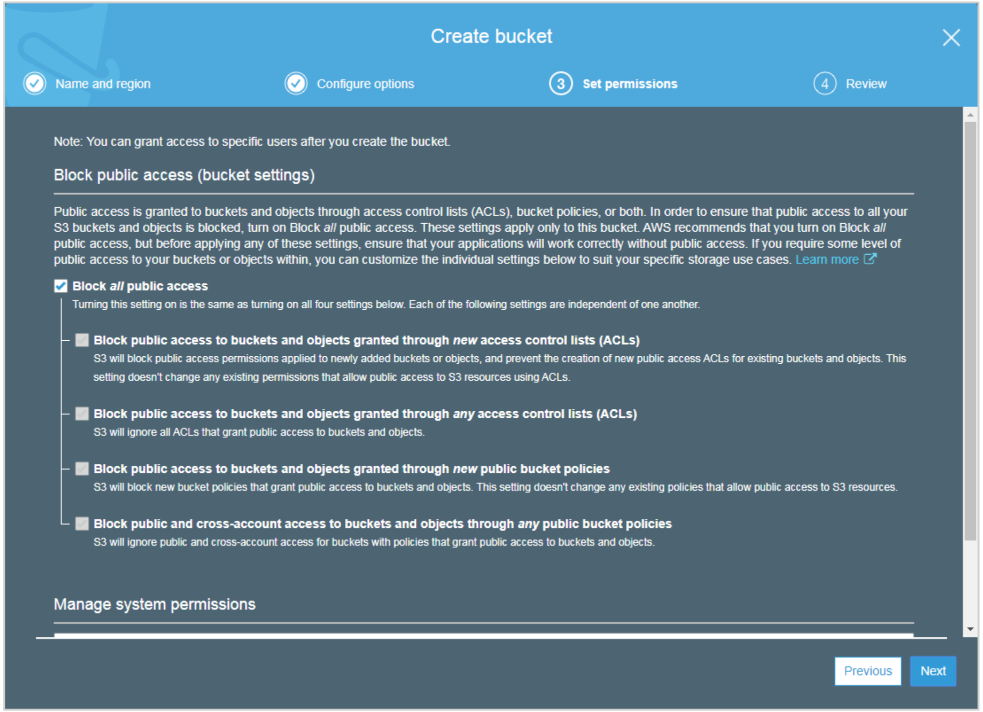
□ Record object-level API activity using AWS CloudTrail for an additional cost. See CloudTrail pricing or learn more

Default encryption

□ Automatically encrypt objects when they are stored in S3. Learn more

▸ Advanced settings

Management



Create bucket

✓ Name and region
✓ Configure options
③ **Set permissions**
④ Review

Note: You can grant access to specific users after you create the bucket.

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. 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. 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**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- □ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- □ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  S3 will ignore all ACLs that grant public access to buckets and objects.
- □ **Block public access to buckets and objects granted through *new* public bucket policies**
  S3 will block new bucket policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- □ **Block public and cross-account access to buckets and objects through *any* public bucket policies**
  S3 will ignore public and cross-account access for buckets with policies that grant public access to buckets and objects.

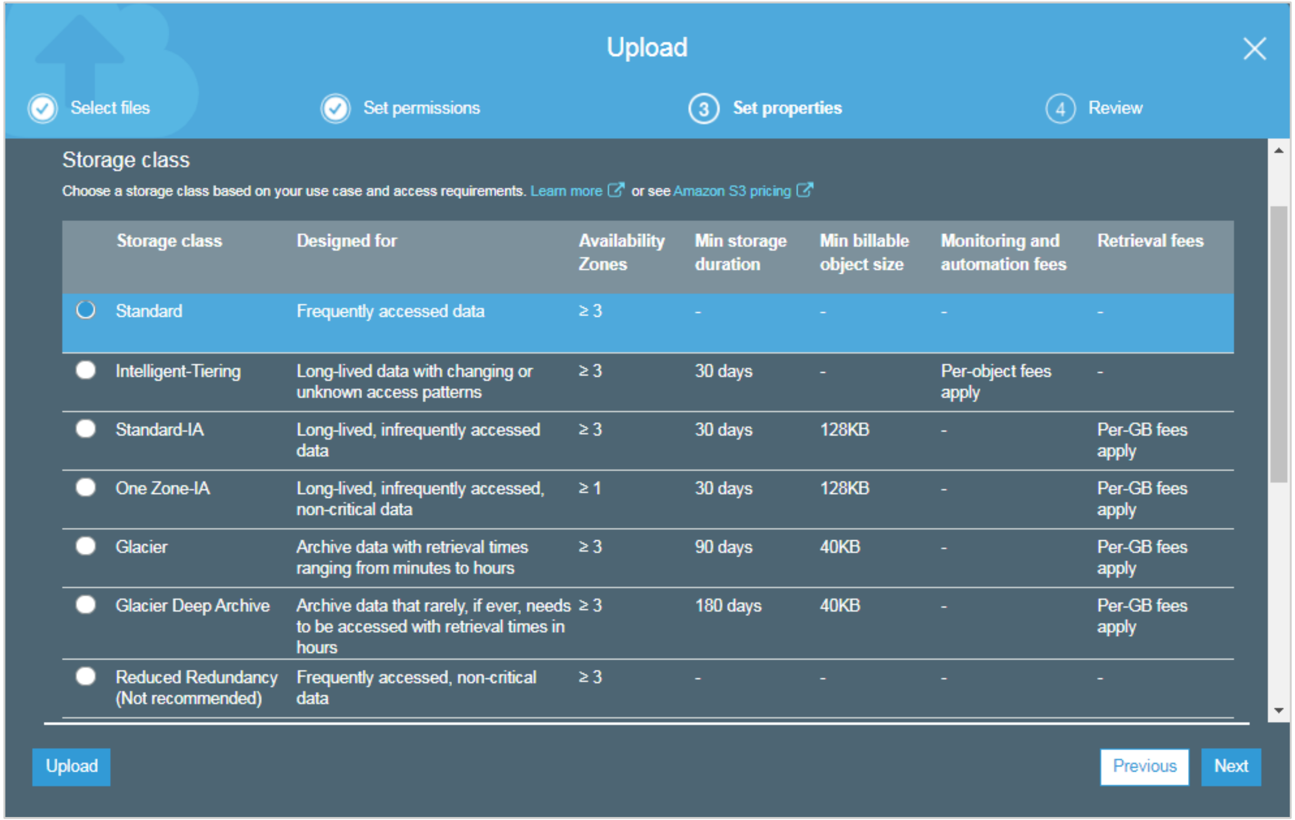
Manage system permissions

S3 Bucket

Step by step process- adding data

“Bucket Name” → “Upload” → “Set properties”

- **Standard**
- **Intelligent-Tiering**
- **Standard-IA**
- **One Zone-IA**
- **Glacier**
- **Glacier Deep Archive**
- **Reduced Redundancy**



Storage class

Choose a storage class based on your use case and access requirements. Learn more or see Amazon S3 pricing

	Storage class	Designed for	Availability Zones	Min storage duration	Min billable object size	Monitoring and automation fees	Retrieval fees
●	Standard	Frequently accessed data	≥ 3	-	-	-	-
○	Intelligent-Tiering	Long-lived data with changing or unknown access patterns	≥ 3	30 days	-	Per-object fees apply	-
○	Standard-IA	Long-lived, infrequently accessed data	≥ 3	30 days	128KB	-	Per-GB fees apply
○	One Zone-IA	Long-lived, infrequently accessed, non-critical data	≥ 1	30 days	128KB	-	Per-GB fees apply
○	Glacier	Archive data with retrieval times ranging from minutes to hours	≥ 3	90 days	40KB	-	Per-GB fees apply
○	Glacier Deep Archive	Archive data that rarely, if ever, needs to be accessed with retrieval times in hours	≥ 3	180 days	40KB	-	Per-GB fees apply
○	Reduced Redundancy (Not recommended)	Frequently accessed, non-critical data	≥ 3	-	-	-	-

S3 Bucket

Step by step process- permissions

01

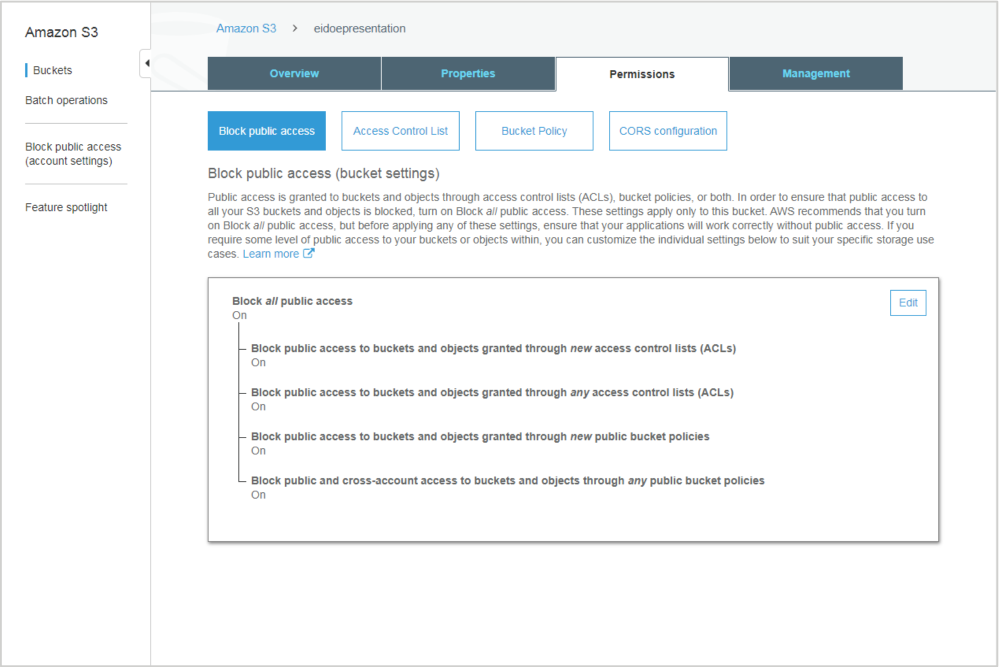
"Permissions" tab ➡ "Block public access"

- ***New ACLs***
- ***Any ACLs***
- ***New public bucket policies***
- ***Any public bucket policies (+CAA)***

02

"Permissions" tab ➡ "Access Control List"

- **Bucket owner**
- **AWS accounts**
- **Public access**
- **S3 log delivery group**

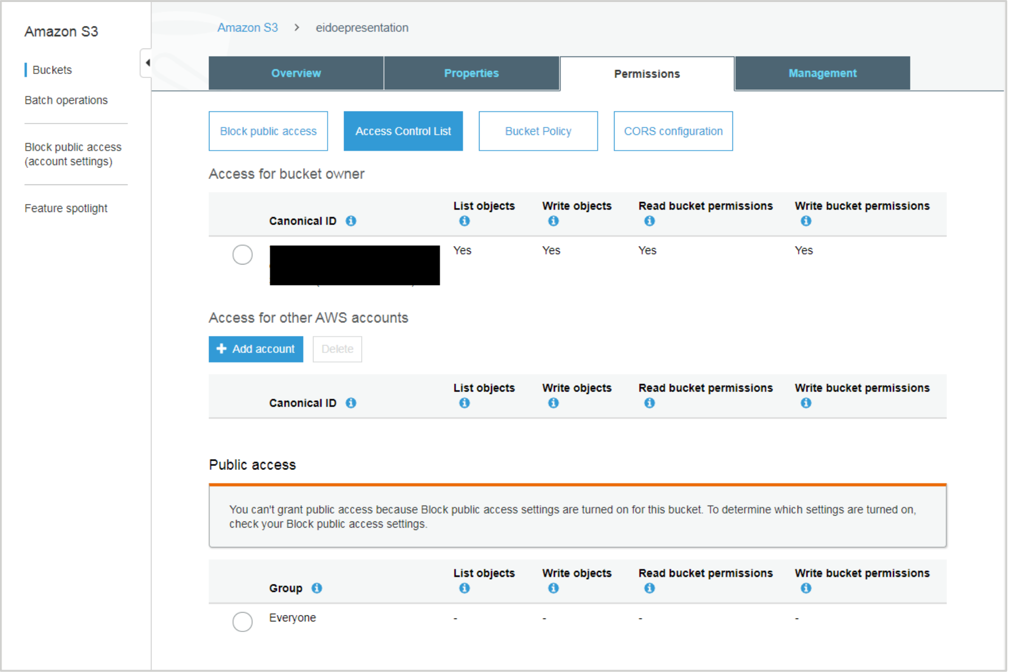


Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. 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. 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

- **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  On
- **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  On
- **Block public access to buckets and objects granted through *new* public bucket policies**
  On
- **Block public and cross-account access to buckets and objects through *any* public bucket policies**
  On



Access for bucket owner

	Canonical ID	List objects	Write objects	Read bucket permissions	Write bucket permissions
○	[redacted]	Yes	Yes	Yes	Yes

Access for other AWS accounts

	Canonical ID	List objects	Write objects	Read bucket permissions	Write bucket permissions

Public access

You can't grant public access because Block public access settings are turned on for this bucket. To determine which settings are turned on, check your Block public access settings.

	Group	List objects	Write objects	Read bucket permissions	Write bucket permissions
○	Everyone	-	-	-	-

S3 Bucket

Step by step process- permissions

03

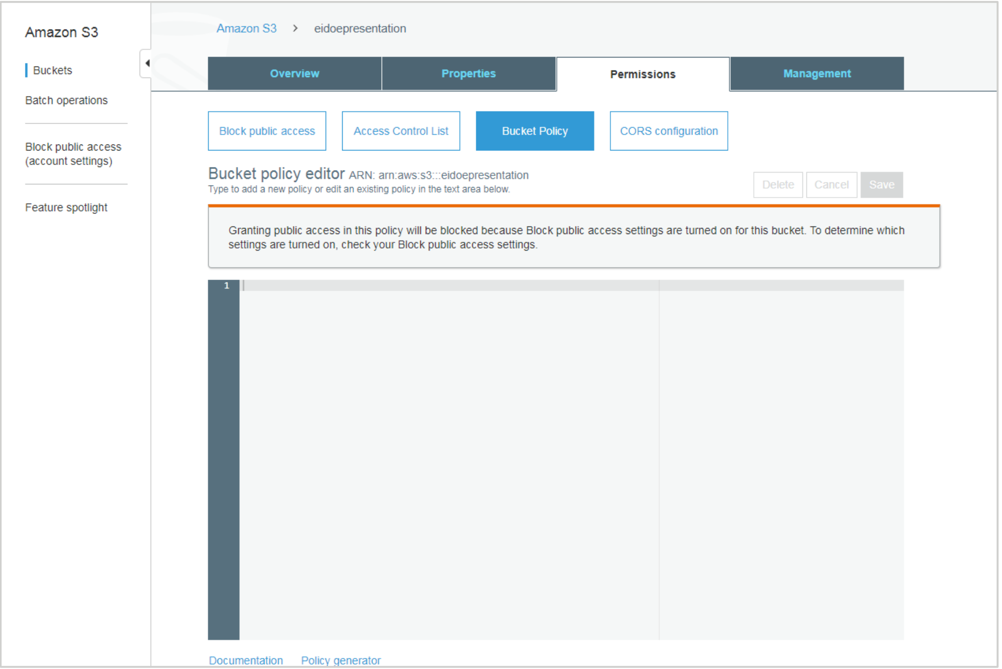
"Permissions" tab ➡ "Bucket Policy"

- **Policy generator (link)**

04

"Permissions" tab ➡ "CORS configuration"

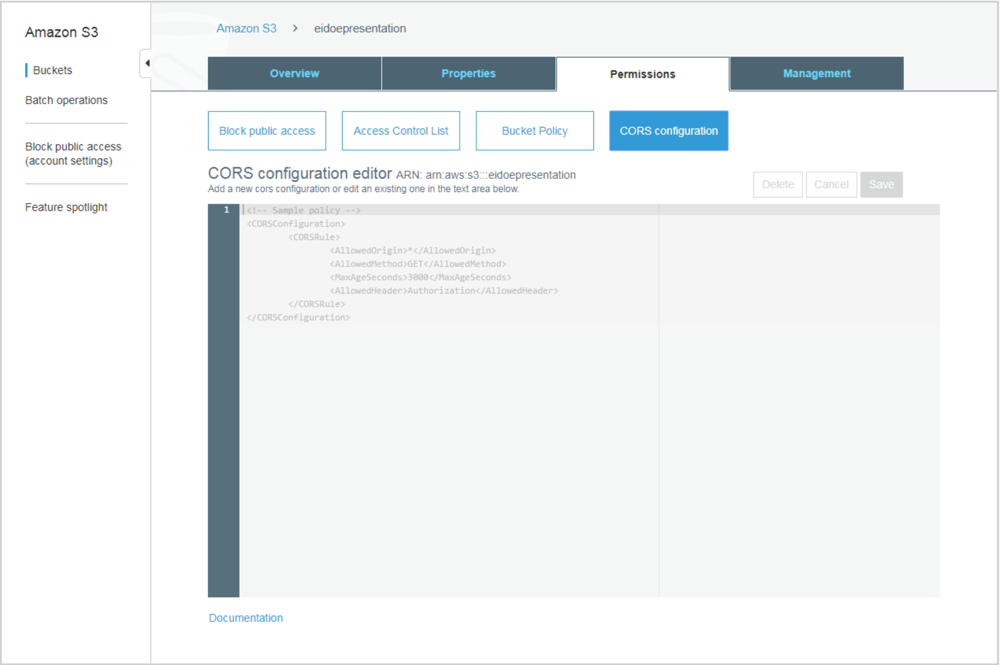
- **CORS configuration editor**



Bucket policy editor ARN: arn:aws:s3:::eidoepresentation

Type to add a new policy or edit an existing policy in the text area below.

Granting public access in this policy will be 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.



CORS configuration editor ARN: arn:aws:s3:::eidoepresentation

Add a new cors configuration or edit an existing one in the text area below.

```
<!-- Sample policy -->
<CORSConfiguration>
        <CORSRule>
                <AllowedOrigin>*</AllowedOrigin>
                <AllowedMethod>GET</AllowedMethod>
                <MaxAgeSeconds>3000</MaxAgeSeconds>
                <AllowedHeader>Authorization</AllowedHeader>
        </CORSRule>
</CORSConfiguration>
```

Amazon GuardDuty

Introduction

"An intelligent cloud scale manage threat detection service". - AWS

Benefits

- Simplicity
- Continuous Monitoring
- Global Coverage
- Threat intelligence
- Threat Behavior
- Management Tools

Threat Classes

- Backdoor
- Behavior
- Crypto Currency
- Pen-test
- Recon
- Stealth
- Trojan
- Unauthorized Access

Tools & Methods

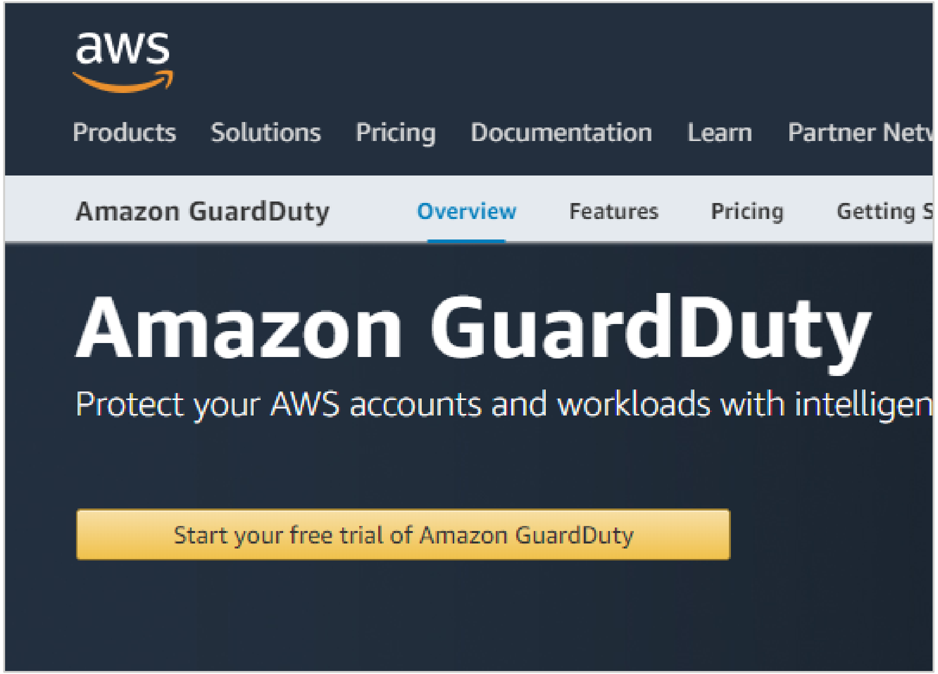
- Partners
- User Tools (API)
- Machine Learning
- Reconnaissance
- Instance Compromise
- Account Compromise

Amazon GuardDuty

Alert notification- creating detection

01

Go to AWS GuardDuty and press- “Start your free trial of Amazon GuardDuty”.
Following, input your credentials if needed.

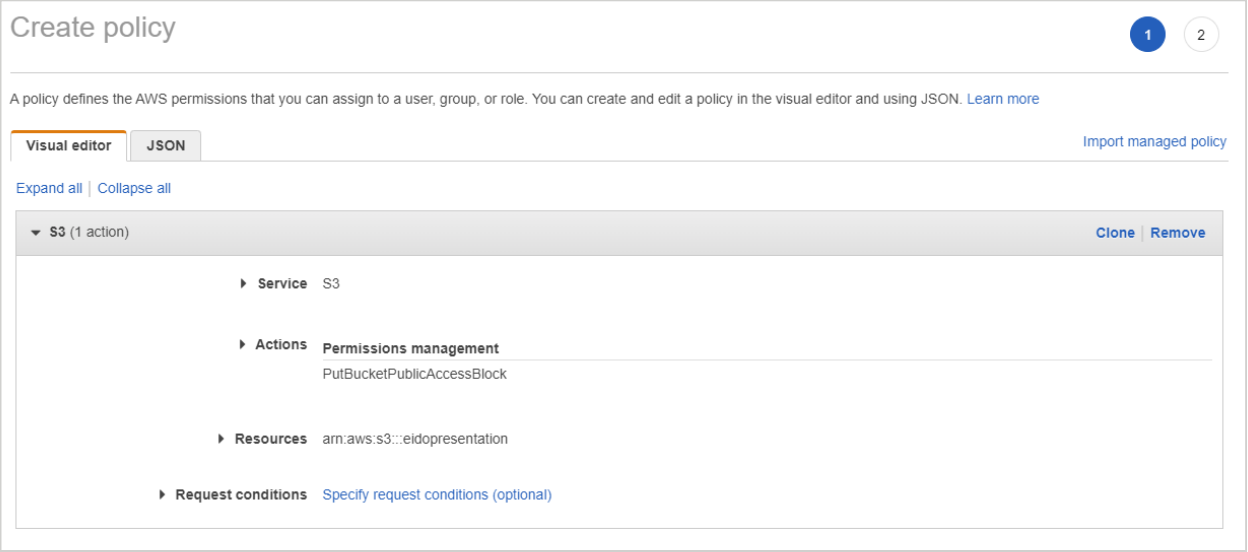


Amazon GuardDuty

Protect your AWS accounts and workloads with intelligen

02

AWS IAM ➡ “Policies” ➡ “Create policy”



A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

S3 (1 action)

Service S3

Actions Permissions management
PutBucketPublicAccessBlock

Resources arn:aws:s3:::eidopresentation

Request conditions Specify request conditions (optional)

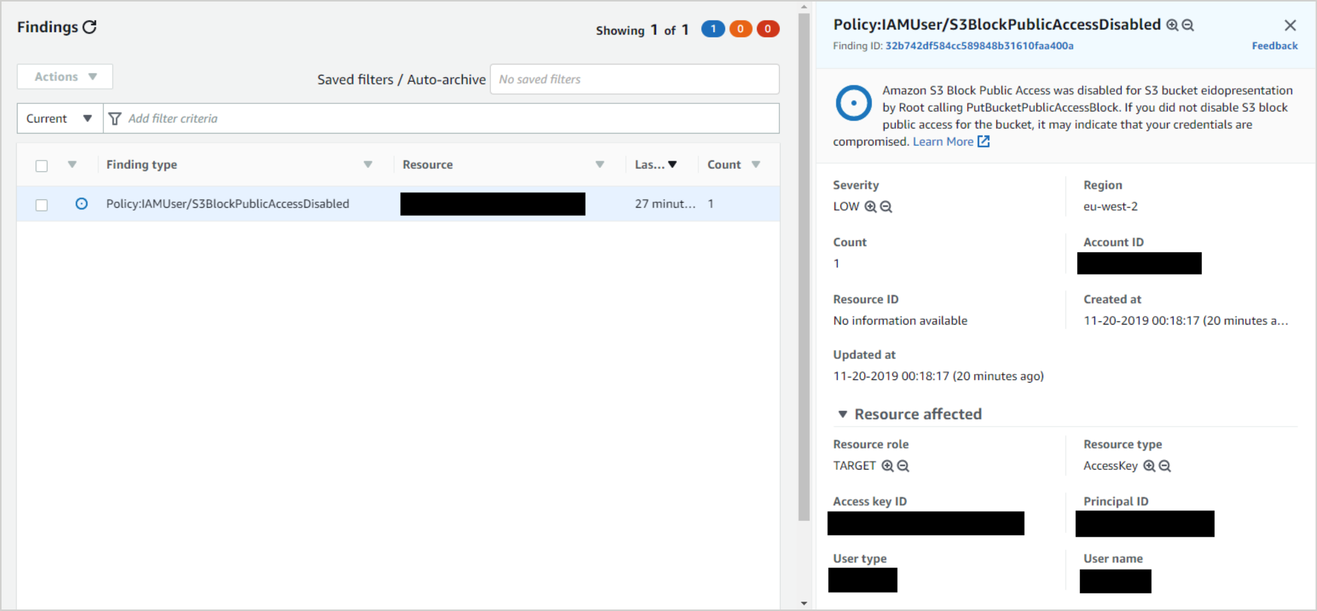
Amazon GuardDuty

Alert notification- creating a notification

03 AWS GuardDuty ➜ "Findings"

04 AWS SNS ➜ "Topics" ➜ "Create topic"

- **Subscription**
- **S3 bucket event**



Findings ↻ Showing 1 of 1 1 0 0

Actions ▼ Saved filters / Auto-archive No saved filters

Current ▼ Add filter criteria

□	▼	Finding type	Resource	Las...	Count
□	⊙	Policy:IAMUser/S3BlockPublicAccessDisabled	[redacted]	27 minut...	1

Policy:IAMUser/S3BlockPublicAccessDisabled

Finding ID: 32b742df584cc589848b31610faa400a

Feedback

Amazon S3 Block Public Access was disabled for S3 bucket eidopresentation by Root calling PutBucketPublicAccessBlock. If you did not disable S3 block public access for the bucket, it may indicate that your credentials are compromised. Learn More

Severity: LOW

Region: eu-west-2

Count: 1

Account ID: [redacted]

Resource ID: No information available

Created at: 11-20-2019 00:18:17 (20 minutes a...

Updated at: 11-20-2019 00:18:17 (20 minutes ago)

▼ Resource affected

Resource role: TARGET

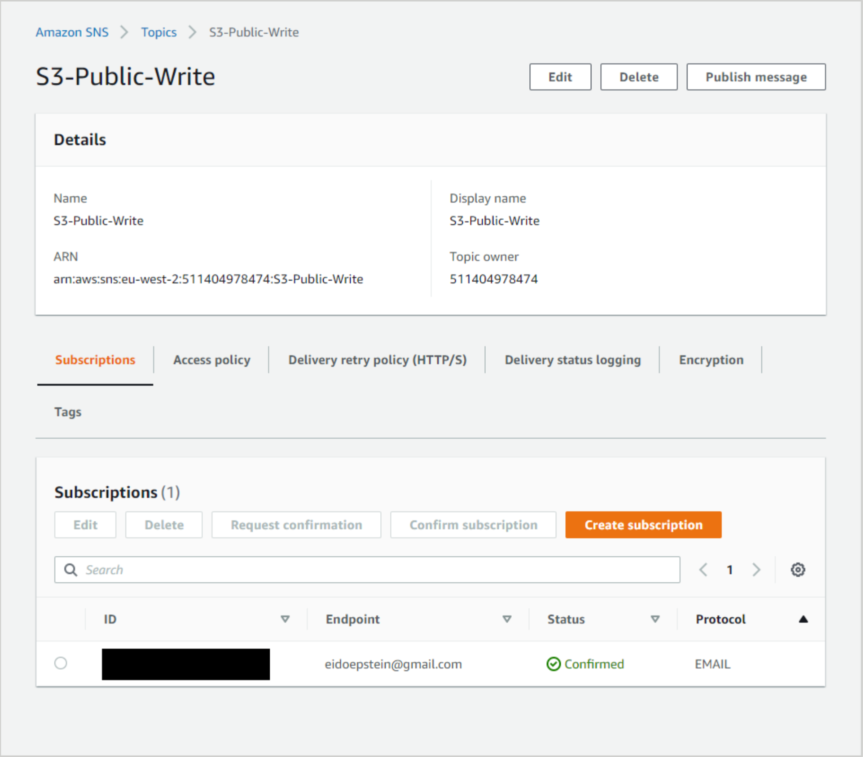
Resource type: AccessKey

Access key ID: [redacted]

Principal ID: [redacted]

User type: [redacted]

User name: [redacted]



Amazon SNS > Topics > S3-Public-Write

S3-Public-Write

Edit Delete Publish message

Details

Name: S3-Public-Write

Display name: S3-Public-Write

ARN: arn:aws:sns:eu-west-2:511404978474:S3-Public-Write

Topic owner: 511404978474

Subscriptions | Access policy | Delivery retry policy (HTTP/S) | Delivery status logging | Encryption | Tags

Subscriptions (1)

Edit Delete Request confirmation Confirm subscription Create subscription

Search

	ID	Endpoint	Status	Protocol
○	[redacted]	eidoepstein@gmail.com	✓ Confirmed	EMAIL

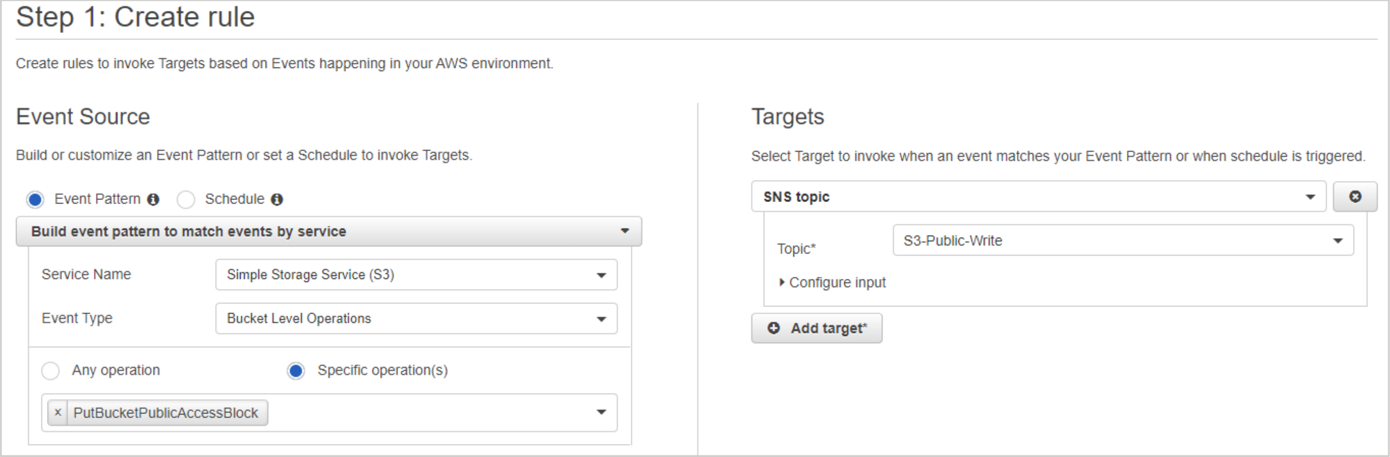
Amazon GuardDuty

Alert notification- creating mitigation

05

AWS CloudWatch ➡ "Rules" ➡ "Create rule"

- **AWS CloudTrail**



Step 1: Create rule

Create rules to invoke Targets based on Events happening in your AWS environment.

Event Source

Build or customize an Event Pattern or set a Schedule to invoke Targets.

● Event Pattern ○ Schedule

Build event pattern to match events by service

Service Name: Simple Storage Service (S3)

Event Type: Bucket Level Operations

○ Any operation ● Specific operation(s)

× PutBucketPublicAccessBlock

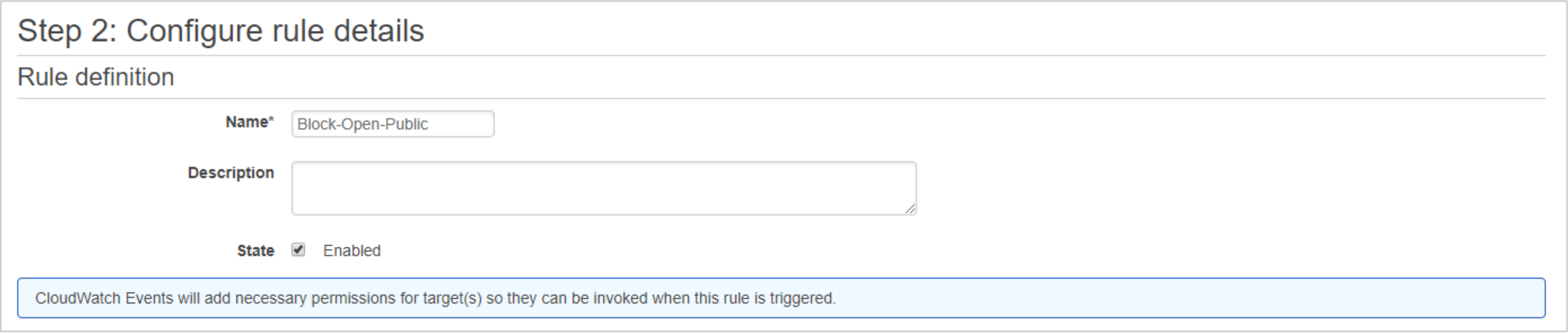
Targets

Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.

SNS topic

Topic*: S3-Public-Write

Configure input



Step 2: Configure rule details

Rule definition

Name* Block-Open-Public

Description

State ☑ Enabled

CloudWatch Events will add necessary permissions for target(s) so they can be invoked when this rule is triggered.

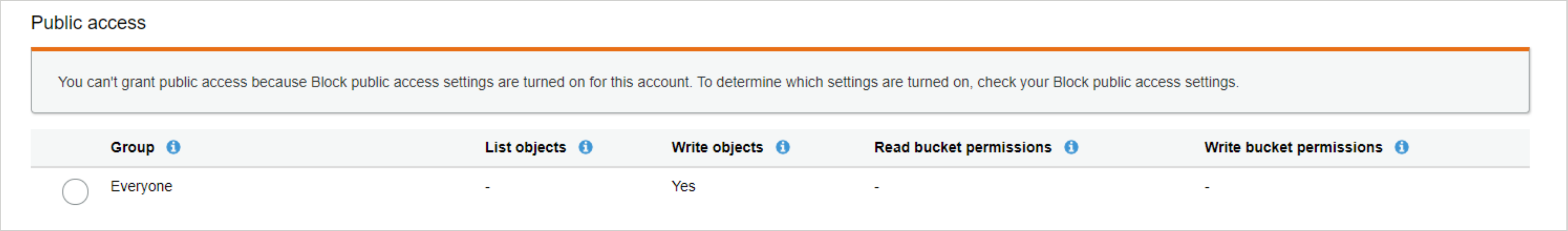
Amazon GuardDuty

Alert notification- the result

06

AWS S3 ➡ “bucket name” ➡ “Permissions”

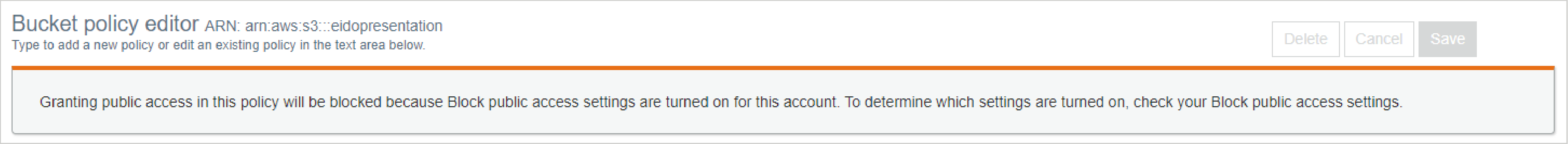
- **Block *all* public access - Off**



Public access

You can't grant public access because Block public access settings are turned on for this account. To determine which settings are turned on, check your Block public access settings.

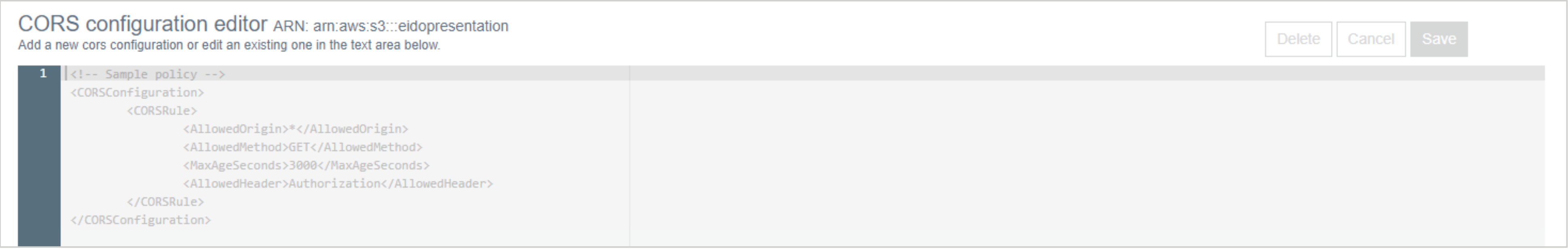
	Group	List objects	Write objects	Read bucket permissions	Write bucket permissions
○	Everyone	-	Yes	-	-



Bucket policy editor ARN: arn:aws:s3:::eidopresentation

Type to add a new policy or edit an existing policy in the text area below.

Granting public access in this policy will be blocked because Block public access settings are turned on for this account. To determine which settings are turned on, check your Block public access settings.



CORS configuration editor ARN: arn:aws:s3:::eidopresentation

Add a new cors configuration or edit an existing one in the text area below.

```
<!-- Sample policy -->
<CORSConfiguration>
        <CORSRule>
                <AllowedOrigin>*</AllowedOrigin>
                <AllowedMethod>GET</AllowedMethod>
                <MaxAgeSeconds>3000</MaxAgeSeconds>
                <AllowedHeader>Authorization</AllowedHeader>
        </CORSRule>
</CORSConfiguration>
```

AWS S3 – Buckets & Alerts

By: Eido Epstein

November 2019

Mail: eidoepstein@gmail.com
Phone: (+972) 507-513-270
LinkedIn: www.linkedin.com/in/eido-epstein