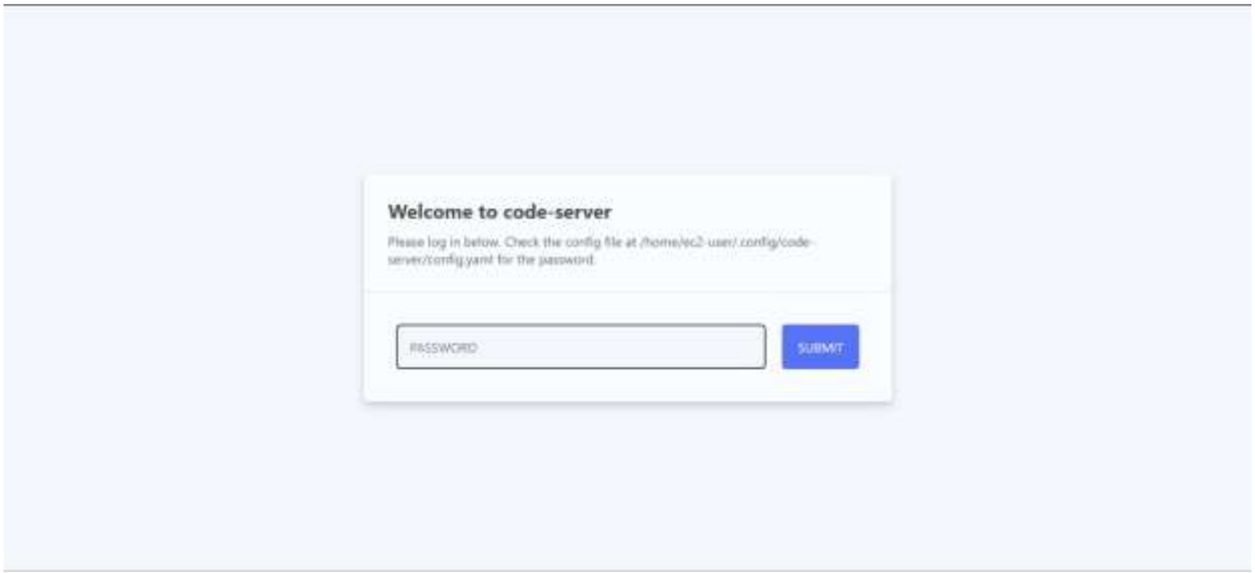
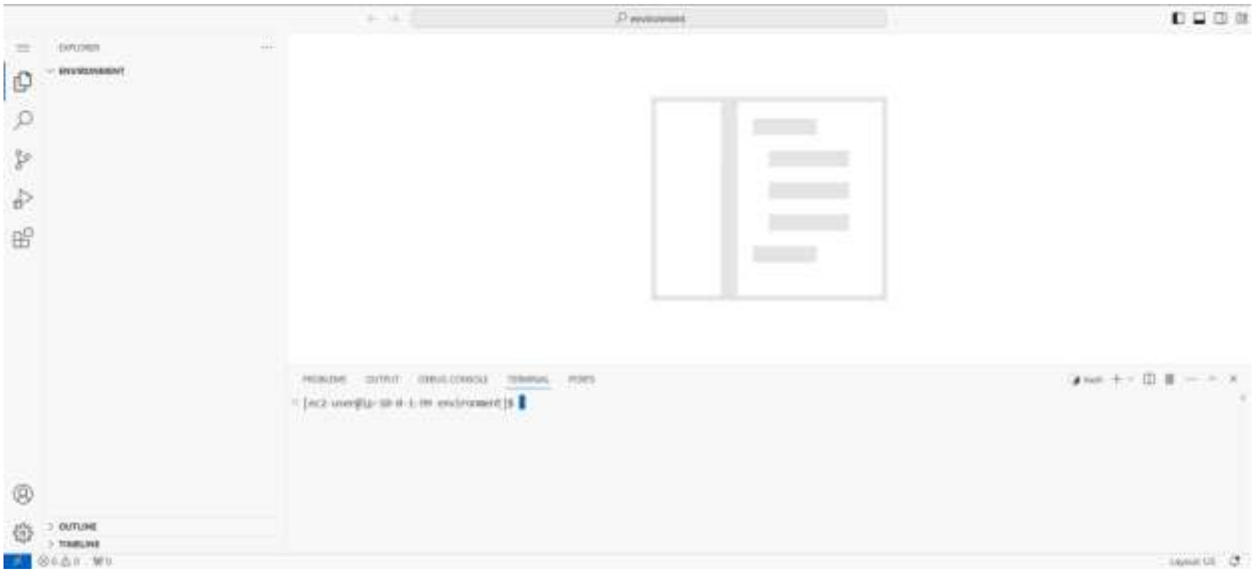
Michael M. Orenze
CLDSRV 3

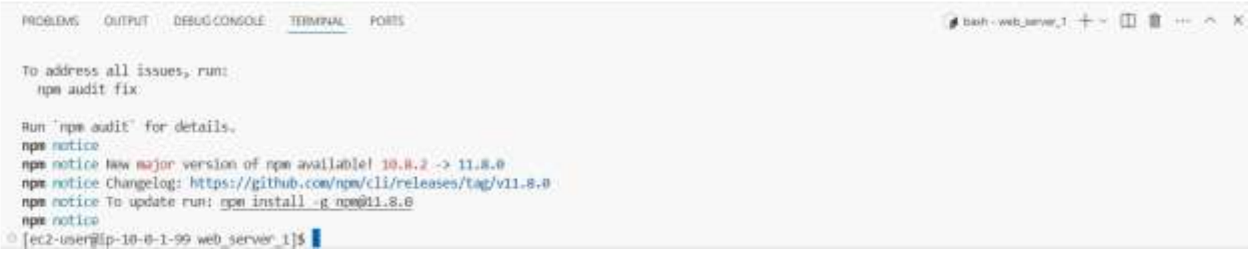


Welcome to code-server

Please log in below. Check the config file at /home/ec2-user/.config/code-server/config.yaml for the password.

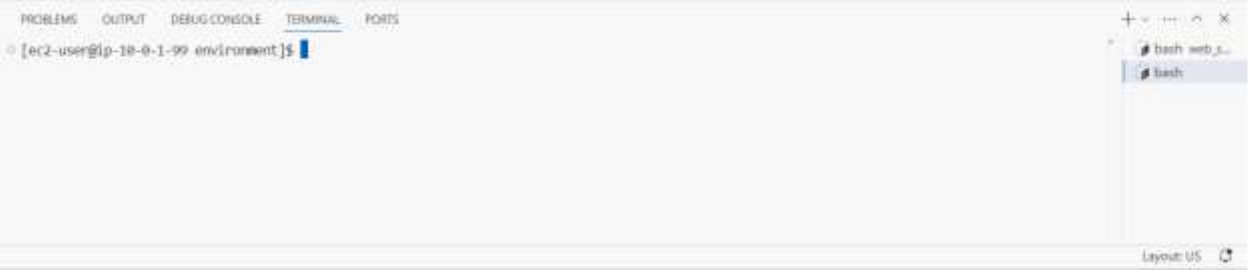


```
[ec2-user@ip-10-0-1-99 environment]$
```

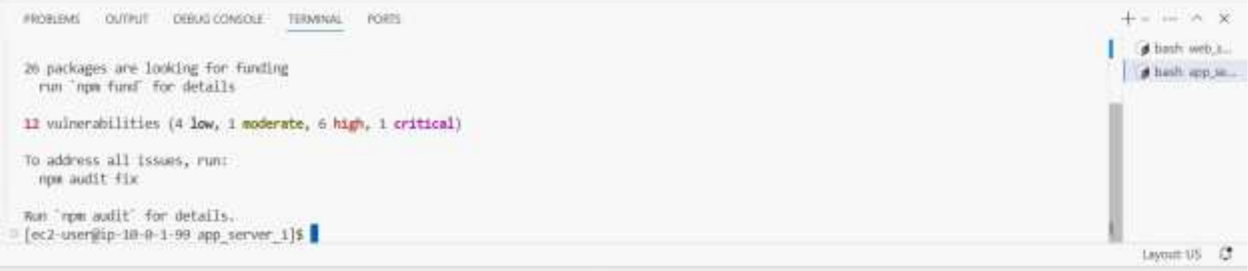


```
To address all issues, run:
  npm audit fix

Run `npm audit` for details.
npm notice
npm notice New major version of npm available! 10.8.2 -> 11.8.0
npm notice Changelog: https://github.com/npm/cli/releases/tag/v11.8.0
npm notice To update run: npm install -g npm@11.8.0
npm notice
[ec2-user@ip-10-0-1-99 web_server_1]$
```

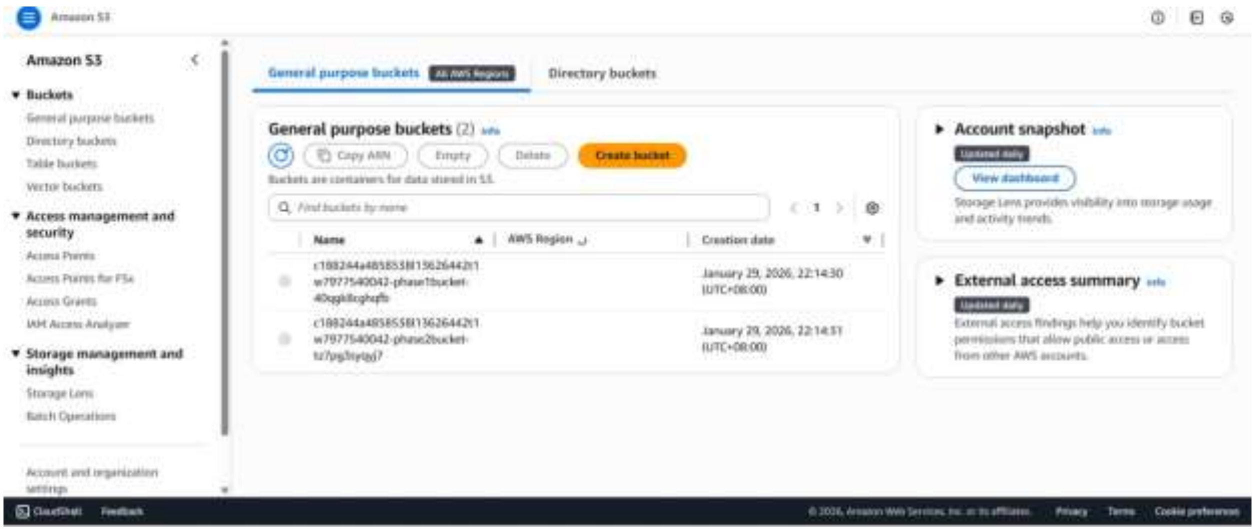
Michael M. Orenze
CLDSRV 3



```
[ec2-user@ip-10-0-1-99 environment]$ 
```



```
26 packages are looking for funding
  run `npm fund` for details

12 vulnerabilities (4 low, 1 moderate, 6 high, 1 critical)

To address all issues, run:
  npm audit fix

Run `npm audit` for details.
[ec2-user@ip-10-0-1-99 app_server_1]$ 
```



General purpose buckets (2)

Buckets are containers for data stored in S3.

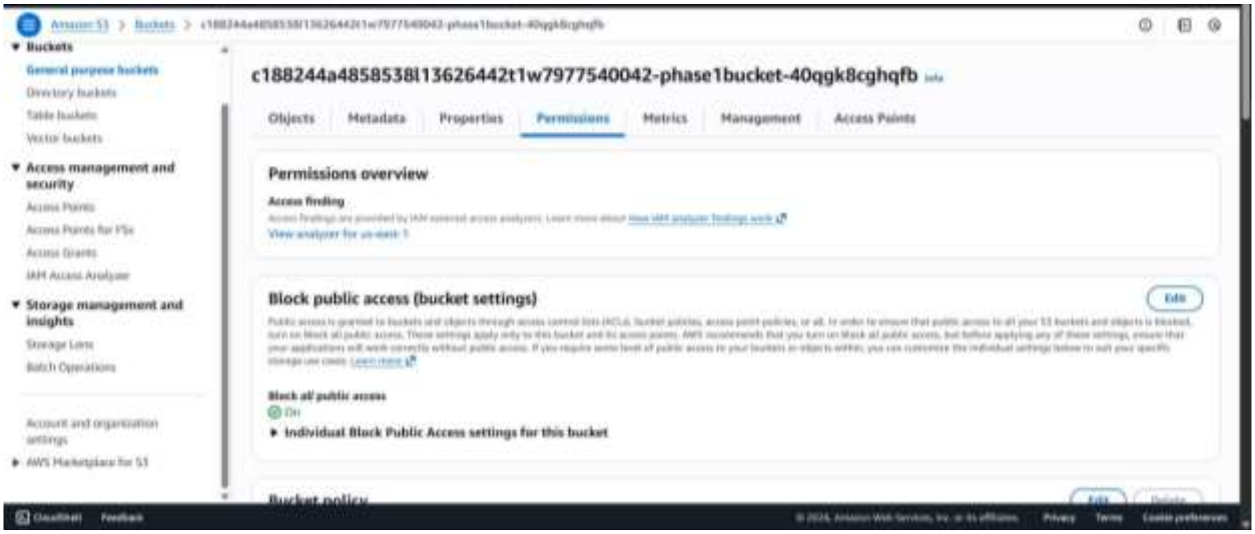
Name	AWS Region	Creation date
c188244a4858538113626442t1w7977540042-phase1bucket-40qgk8cghqfb		January 29, 2026, 22:14:30 (UTC+08:00)
c188244a4858558113626442t1w7977540042-phase2bucket-tz7pg3nytqd7		January 29, 2026, 22:14:31 (UTC+08:00)

Account snapshot

Storage Lens provides visibility into storage usage and activity trends.

External access summary

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.



Amazon S3 > Buckets > c188244a4858538l13626442t1w7977540042-phase1bucket-40qgk8cghqfb

c188244a4858538l13626442t1w7977540042-phase1bucket-40qgk8cghqfb

Permissions overview

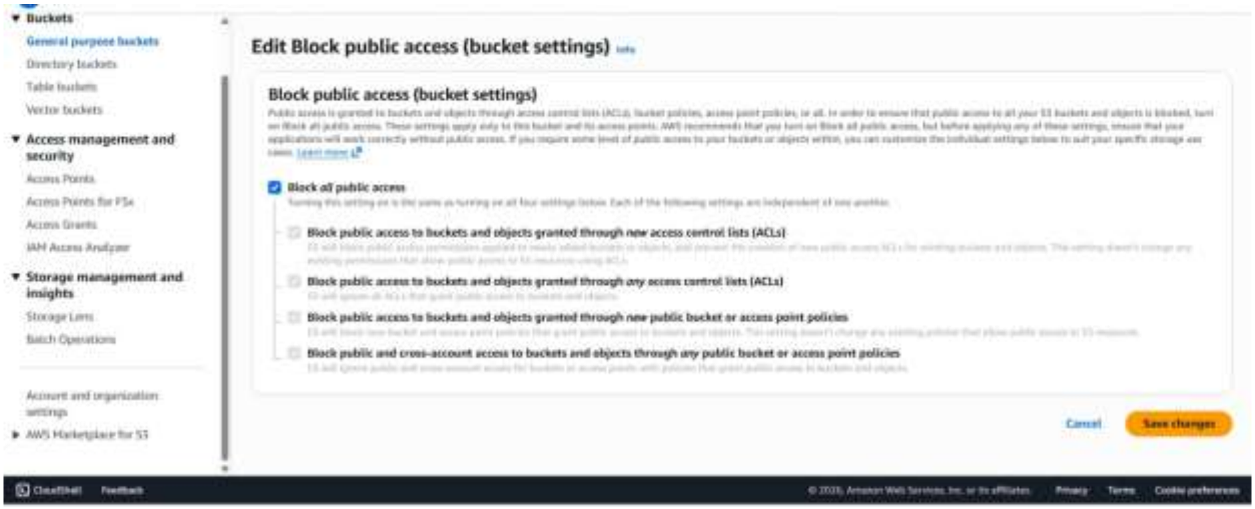
Access finding

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



Edit Block public access (bucket settings)

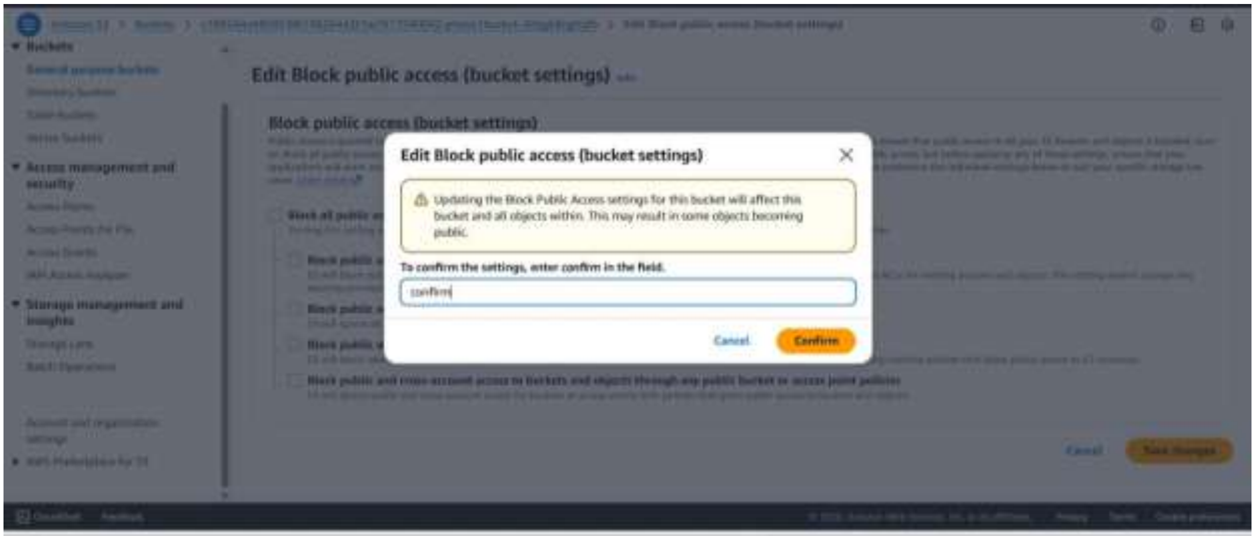
Block public access (bucket settings)

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**
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 or access point policies**
  S3 will block new bucket and access point 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 or access point policies**
  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Michael M. Orenze
CLDSRV 3



Edit Block public access (bucket settings)

Block public access (bucket settings)

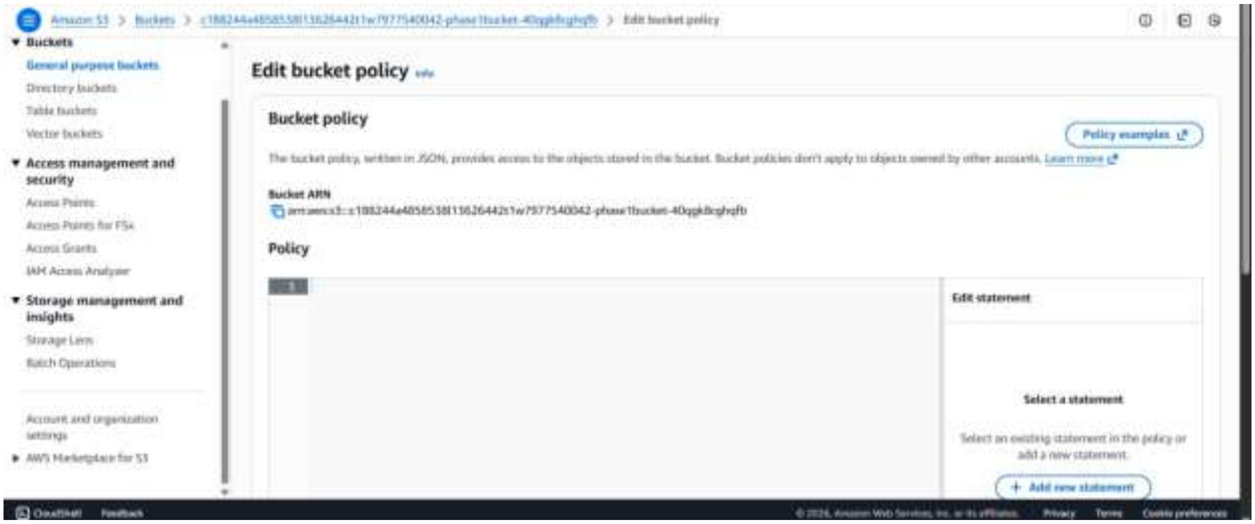
Edit Block public access (bucket settings)

Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, enter confirm in the field.

confirm

Cancel
Confirm
Block public and cross-account access to buckets and objects through any public bucket or access point policies
Cancel
Save changes



Amazon S3 > Buckets > c188244a48585381136264421w7977540042-phase1bucket-40qgk8cghqfb > Edit bucket policy

Edit bucket policy

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

Bucket ARN

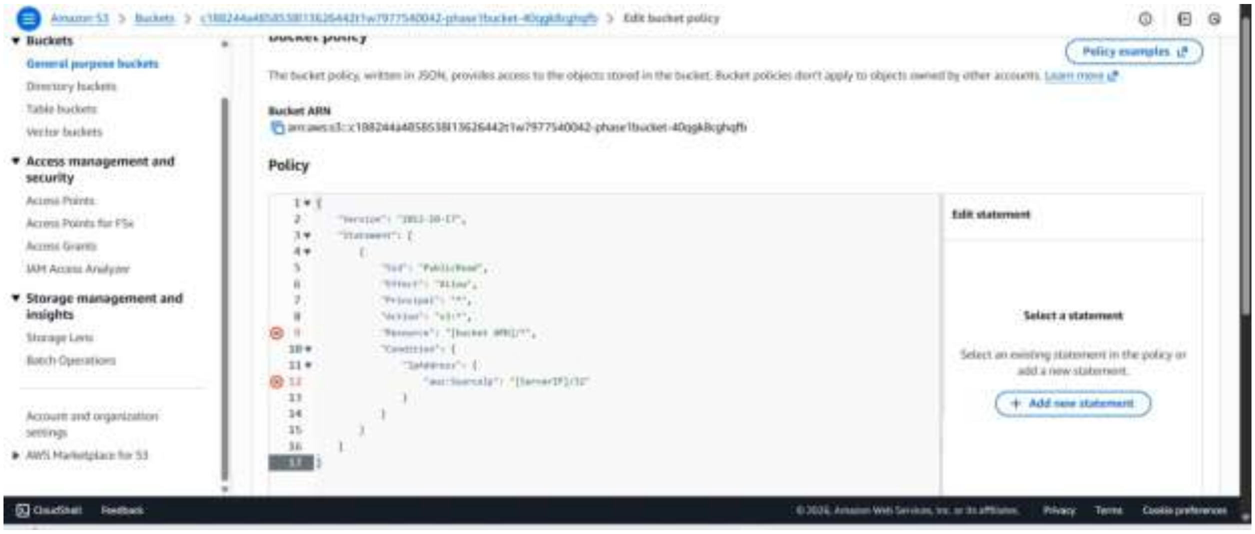
arn:aws:s3:::c188244a48585381136264421w7977540042-phase1bucket-40qgk8cghqfb

Policy

Select a statement

Select an existing statement in the policy or add a new statement.

Michael M. Orenze
CLDSRV 3


Amazon S3 > Buckets > c188244a4858538113626442t1w7977540042-phase1bucket-40qgk8cghqfb > Edit bucket policy
Buckets
General purpose buckets
Directory buckets
Table buckets
Vector buckets
Access management and security
Access Points
Access Points for FSx
Access Grants
IAM Access Analyzer
Storage management and insights
Storage Lens
Batch Operations
Account and organization settings
AWS Marketplace for S3
Policy examples
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement
CloudShell
Feedback
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

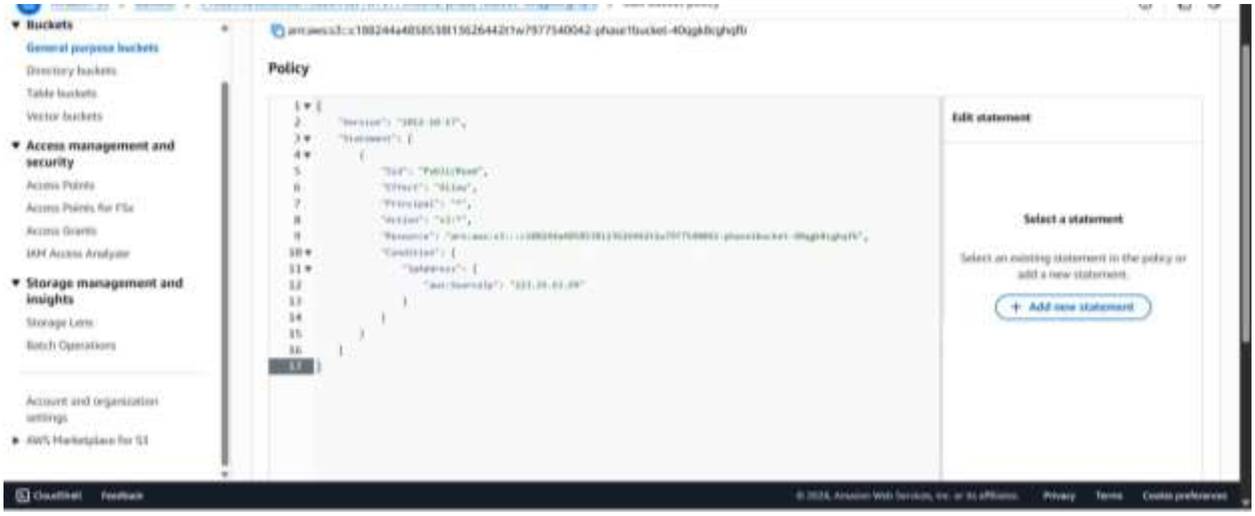
Bucket policy

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

Bucket ARN
arn:aws:s3:::c188244a4858538113626442t1w7977540042-phase1bucket-40qgk8cghqfb

Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicRead",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "[bucket ARN]/*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "[ServerIP]/32"
                }
            }
        }
    ]
}
```

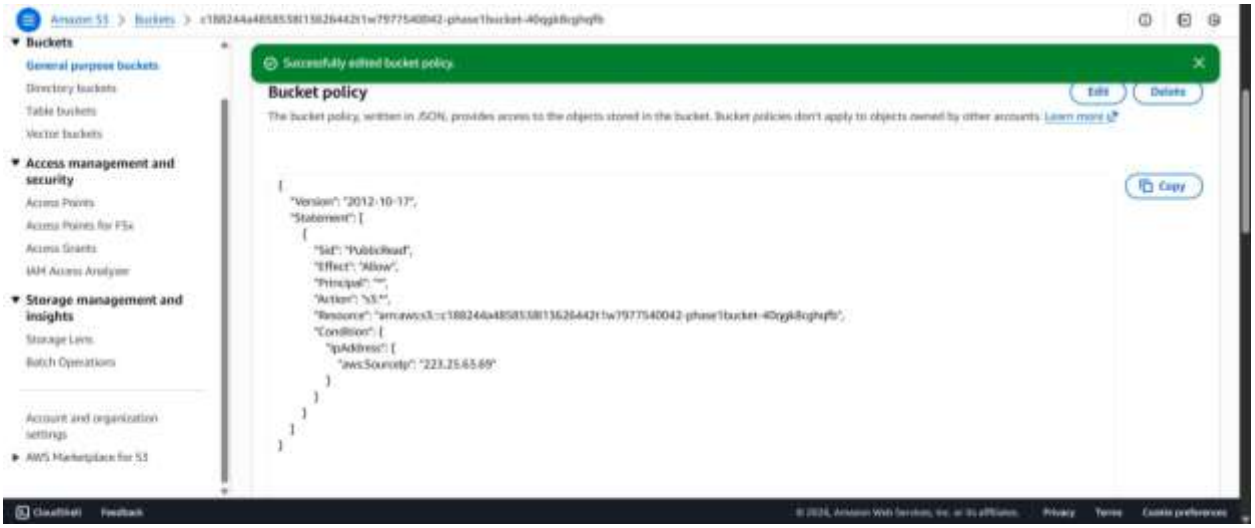


arn:aws:s3:::c188244a4858538113626442t1w7977540042-phase1bucket-40qgk8cghqfb

Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicRead",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::c188244a4858538113626442t1w7977540042-phase1bucket-40qgk8cghqfb",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "221.39.63.09"
                }
            }
        }
    ]
}
```

Michael M. Orenze
CLDSRV 3

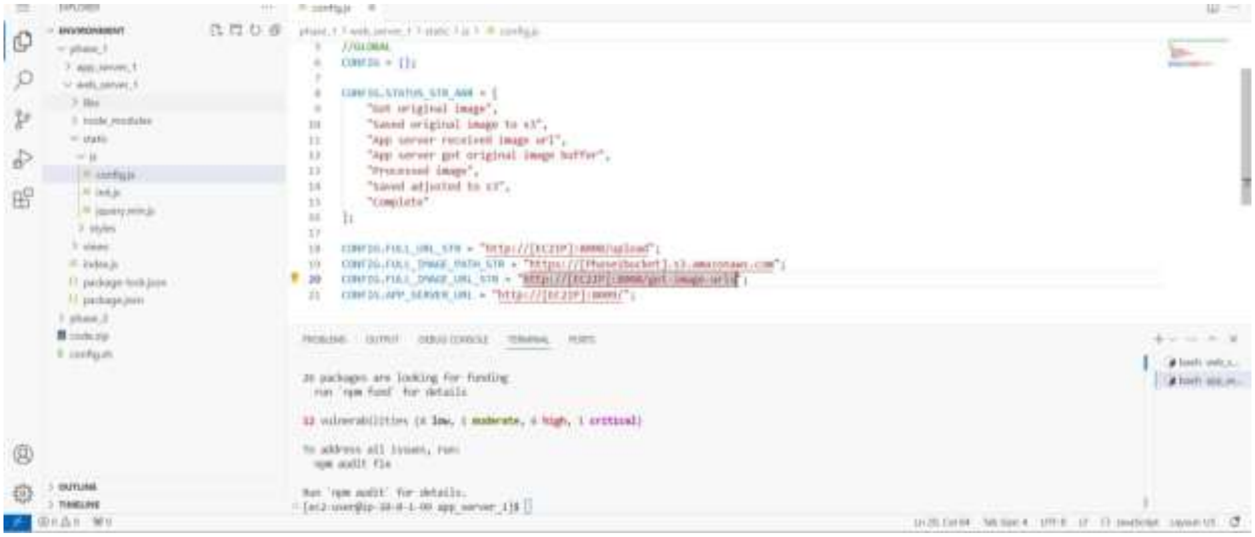


Successfully edited bucket policy.

Bucket policy

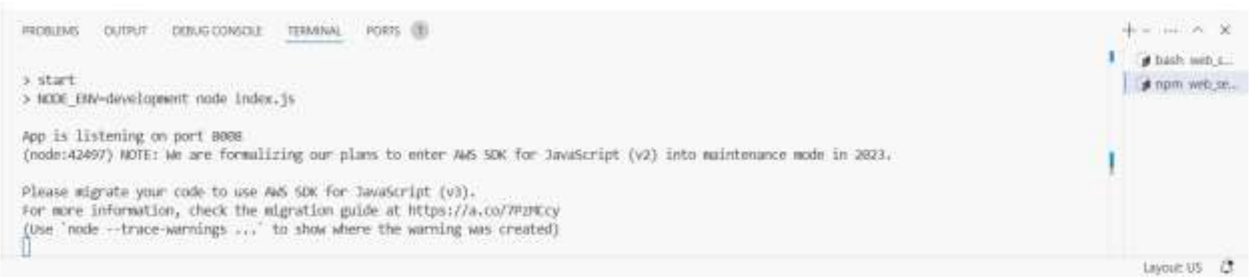
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicRead",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::c188244a4858538136264421w7977540042-phase1bucket-40qgk8cghqfb",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "223.25.63.69"
        }
      }
    }
  ]
}
```



```
//GLOBAL
CONFIG = [];

CONFIG.STATUS_STR_ARR = [
    "Got original image",
    "Saved original image to s3",
    "App server received image url",
    "App server got original image buffer",
    "Processed image",
    "Saved adjusted to s3",
    "Complete"
];

CONFIG.FULL_URL_STR = "http://[EC2IP]:8000/upload";
CONFIG.FULL_IMAGE_PATH_STR = "https://[Phase1bucket].s3.amazonaws.com";
CONFIG.FULL_IMAGE_URL_STR = "http://[EC2IP]:8000/get-image-url";
CONFIG.APP_SERVER_URL = "http://[EC2IP]:8001/";
```

```
20 packages are looking for funding
  run `npm fund` for details

12 vulnerabilities (6 low, 1 moderate, 4 high, 1 critical)

To address all issues, run:
  npm audit fix

Run `npm audit` for details.
[ec2-user@ip-10-0-1-99 app_server_1]$ 
```



```
> start
> NODE_ENV=development node index.js

App is listening on port 8000
(node:42497) NOTE: We are formalizing our plans to enter AWS SDK for JavaScript (v2) into maintenance mode in 2023.

Please migrate your code to use AWS SDK for JavaScript (v3).
For more information, check the migration guide at https://a.co/7PzMCcy
(Use `node --trace-warnings ...` to show where the warning was created)
```

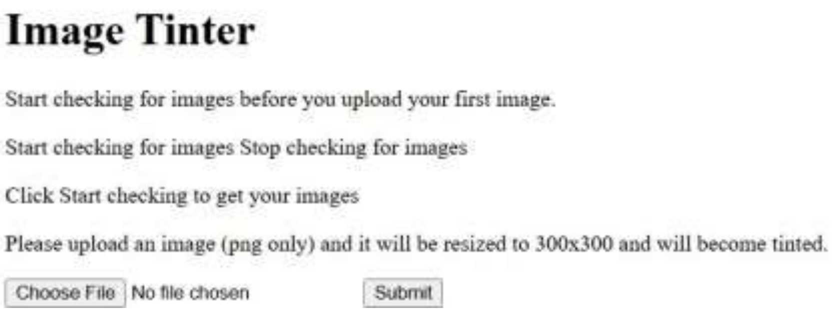


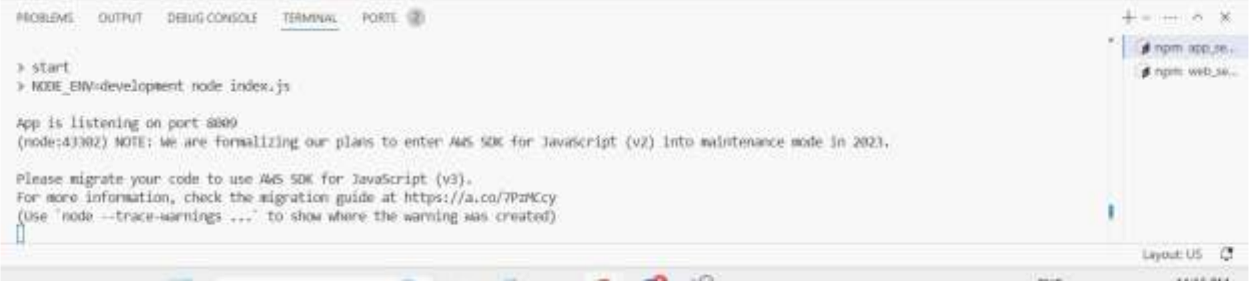
Image Tinter

Start checking for images before you upload your first image.

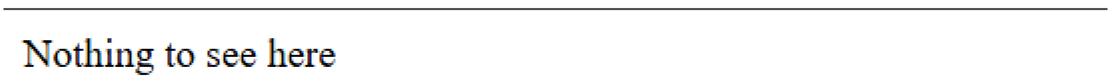
Start checking for images Stop checking for images

Click Start checking to get your images

Please upload an image (png only) and it will be resized to 300x300 and will become tinted.

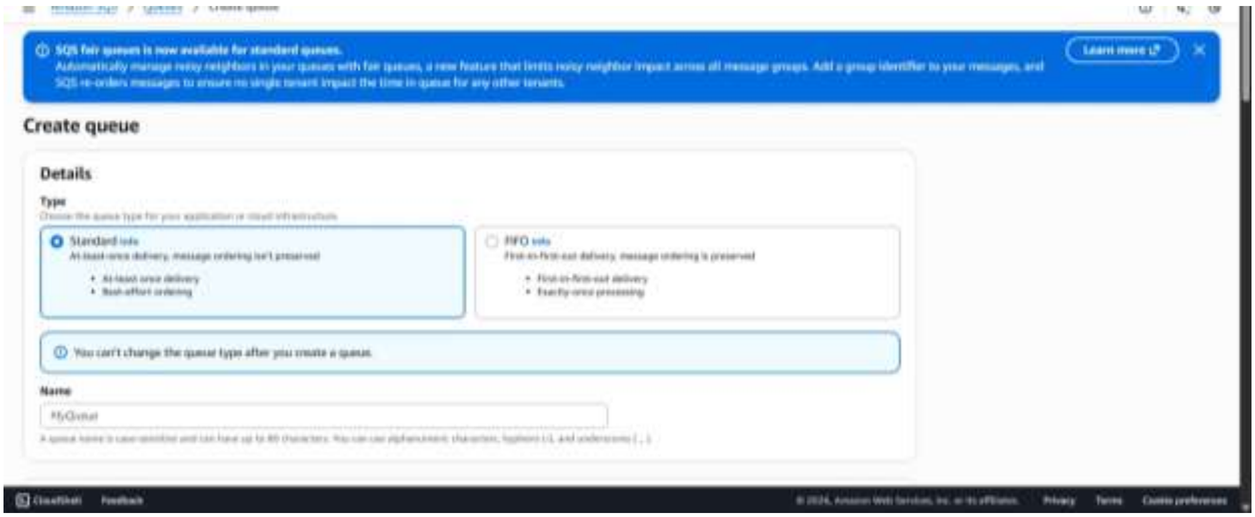


```
> start
> NODE_ENV=development node index.js

App is listening on port 8009
(node:43302) NOTE: We are formalizing our plans to enter AWS SDK for JavaScript (v2) into maintenance mode in 2023.

Please migrate your code to use AWS SDK for JavaScript (v3).
For more information, check the migration guide at https://a.co/7PzMCcy
(Use `node --trace-warnings ...` to show where the warning was created)
```



Nothing to see here

Michael M. Orenze
CLDSRV 3



Amazon SQS > Queues > Create queue

SQS fair queues is now available for standard queues.
Automatically manage noisy neighbors in your queues with fair queues, a new feature that limits noisy neighbor impact across all message groups. Add a group identifier to your messages, and SQS re-orders messages to ensure no single tenant impact the time in queue for any other tenants.

Learn more

Create queue

Details

Type
Choose the queue type for your application or cloud infrastructure.

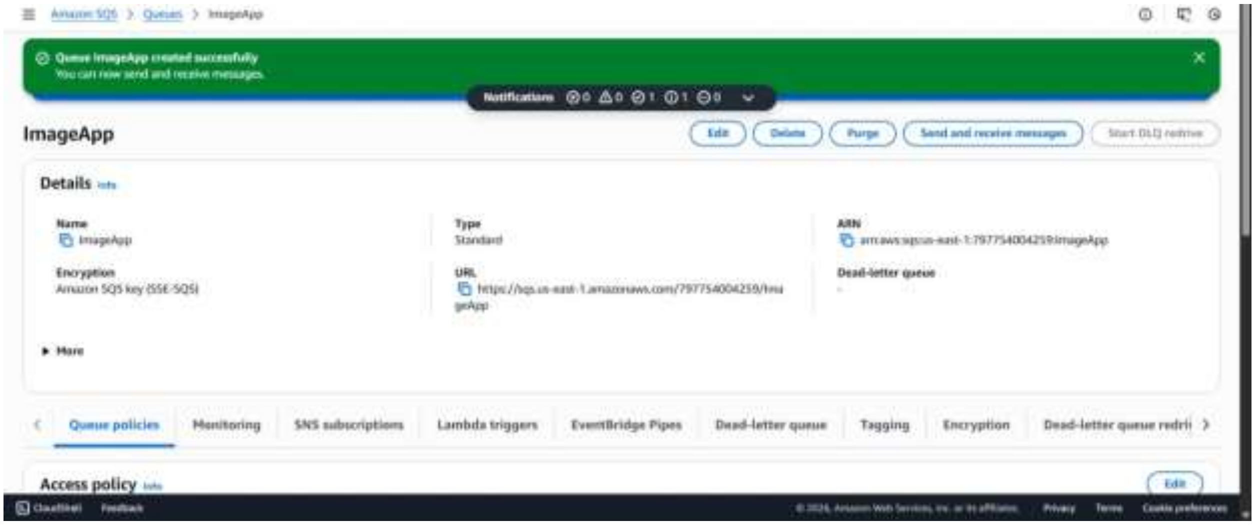
● Standard Info
At-least-once delivery, message ordering isn't preserved
- At-least once delivery
- Best-effort ordering

○ FIFO Info
First-in-first-out delivery, message ordering is preserved
- First-in-first-out delivery
- Exactly-once processing

You can't change the queue type after you create a queue.

Name
MyQueue
A queue name is case-sensitive and can have up to 80 characters. You can use alphanumeric characters, hyphens (-), and underscores (_).

CloudShell Feedback © 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



Amazon SQS > Queues > ImageApp

Queue ImageApp created successfully
You can now send and receive messages.

ImageApp

Details Info

Name
ImageApp

Type
Standard

ARN
arn:aws:sqs:us-east-1:797754004259:ImageApp

Encryption
Amazon SQS key (SSE-SQS)

URL
https://sqs.us-east-1.amazonaws.com/797754004259/ImageApp

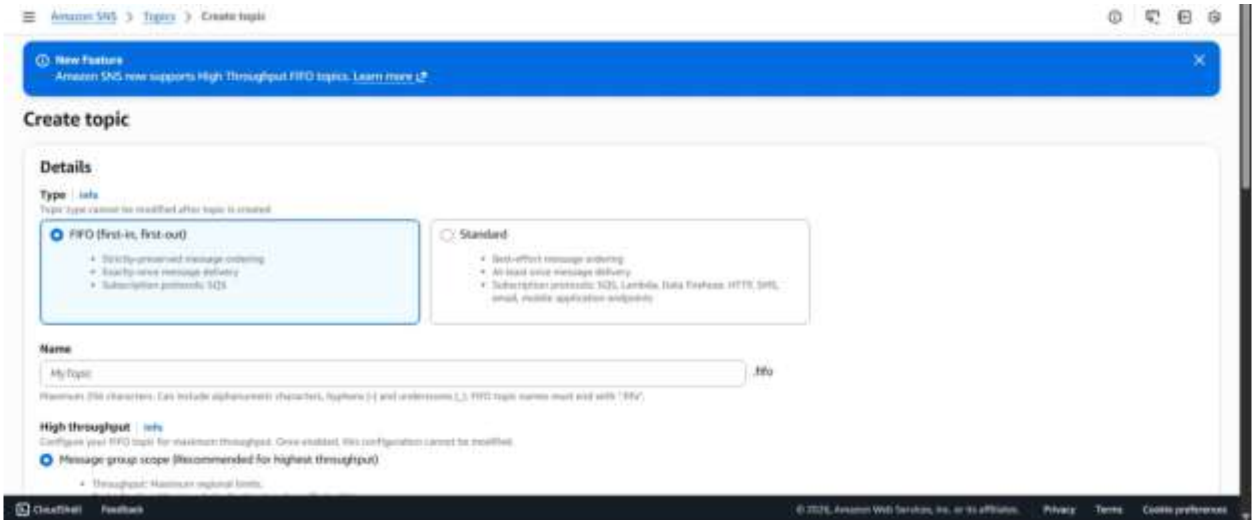
Dead-letter queue
-

▶ More

Access policy Info

CloudShell Feedback © 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Michael M. Orenze
CLDSRV 3



New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more

Create topic

Details

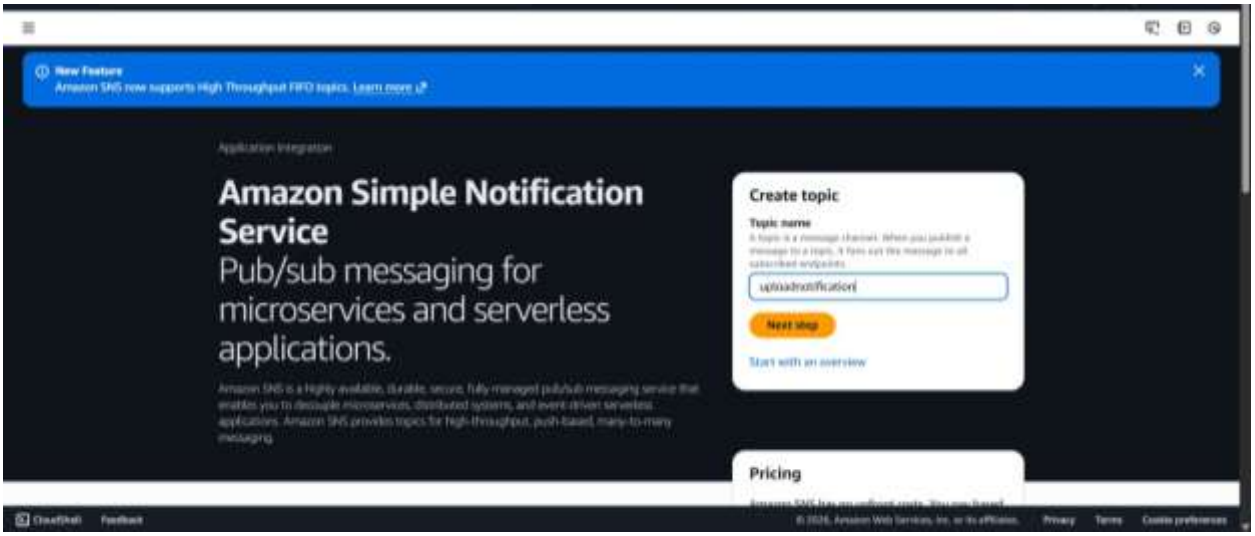
Type | Info
Topic type cannot be modified after topic is created

● FIFO (first-in, first-out)
- Strictly-preserved message ordering
- Exactly-once message delivery
- Subscription protocols: SQS

○ Standard
- Best-effort message ordering
- At-least once message delivery
- Subscription protocols: SQS, Lambda, Data Firehose, HTTP, SMS, email, mobile application endpoints

Name
My Topic .fifo
Maximum 256 characters. Can include alphanumeric characters, hyphens (-) and underscores (_). FIFO topic names must end with ".fifo".

High throughput | Info
Configure your FIFO topic for maximum throughput. Once enabled, this configuration cannot be modified.
● Message group scope (Recommended for highest throughput)
- Throughput: Maximum regional limits.

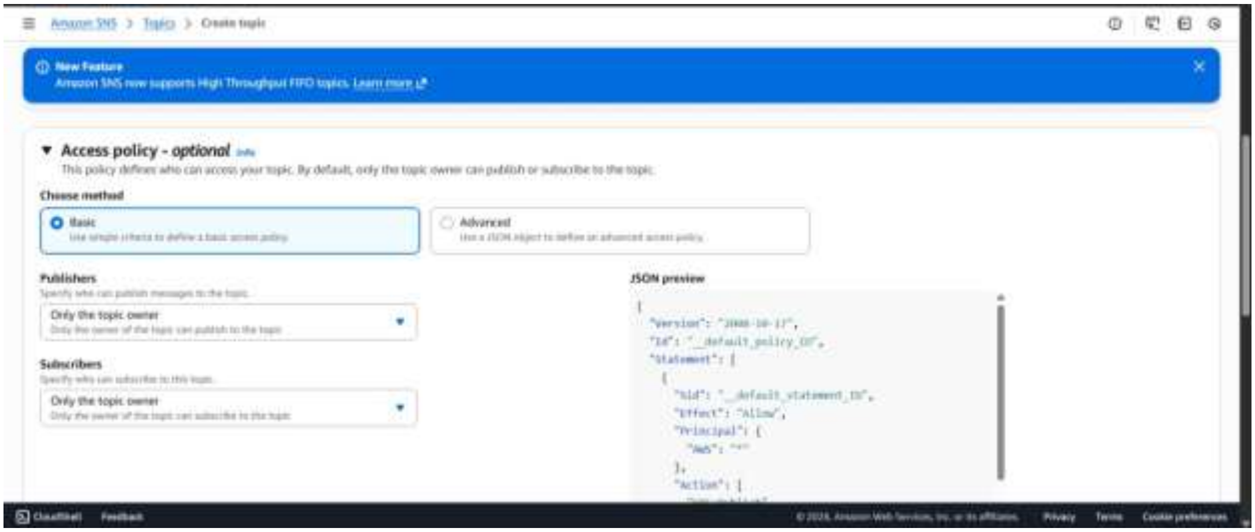

New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more

Application Integration

Amazon Simple Notification Service
Pub/sub messaging for microservices and serverless applications.

Amazon SNS is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and event-driven serverless applications. Amazon SNS provides topics for high-throughput, push-based, many-to-many messaging.

Create topic
Topic name
A topic is a message channel. When you publish a message to a topic, it fans out the message to all subscribed endpoints.
uploadnotification



ⓘ New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more

▼ Access policy - *optional* Info

This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic.

Choose method

● Basic
Use simple criteria to define a basic access policy.

○ Advanced
Use a JSON object to define an advanced access policy.

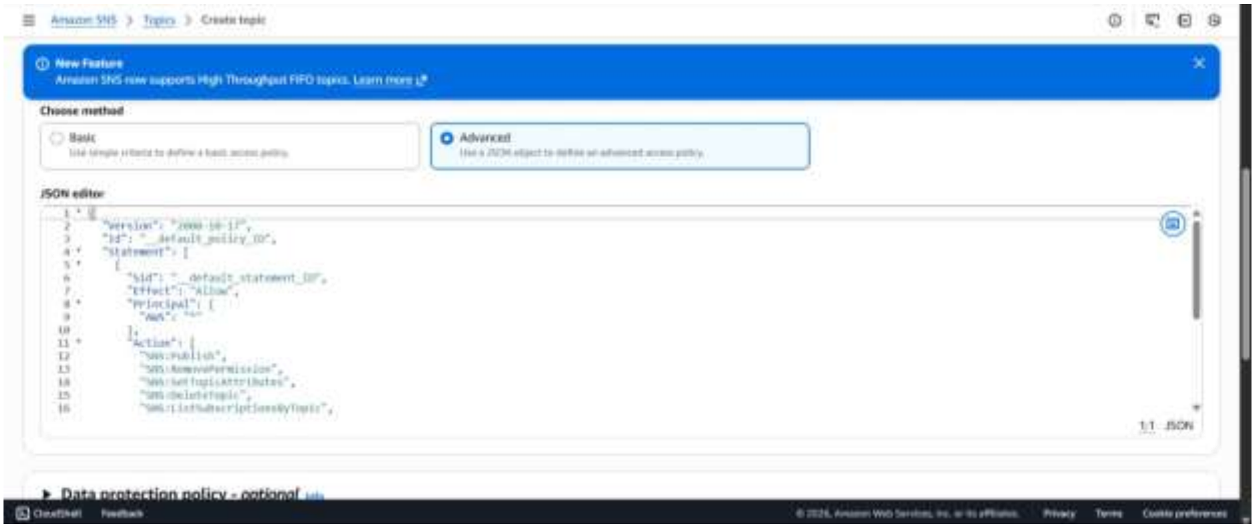
Publishers
Specify who can publish messages to the topic.
Only the topic owner
Only the owner of the topic can publish to the topic

Subscribers
Specify who can subscribe to this topic.
Only the topic owner
Only the owner of the topic can subscribe to the topic

JSON preview

```
{
  "Version": "2008-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "__default_statement_ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
```

CloudShell
Feedback
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Amazon SNS > Topics > Create topic

ⓘ New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more

Choose method

○ Basic
Use simple criteria to define a basic access policy.

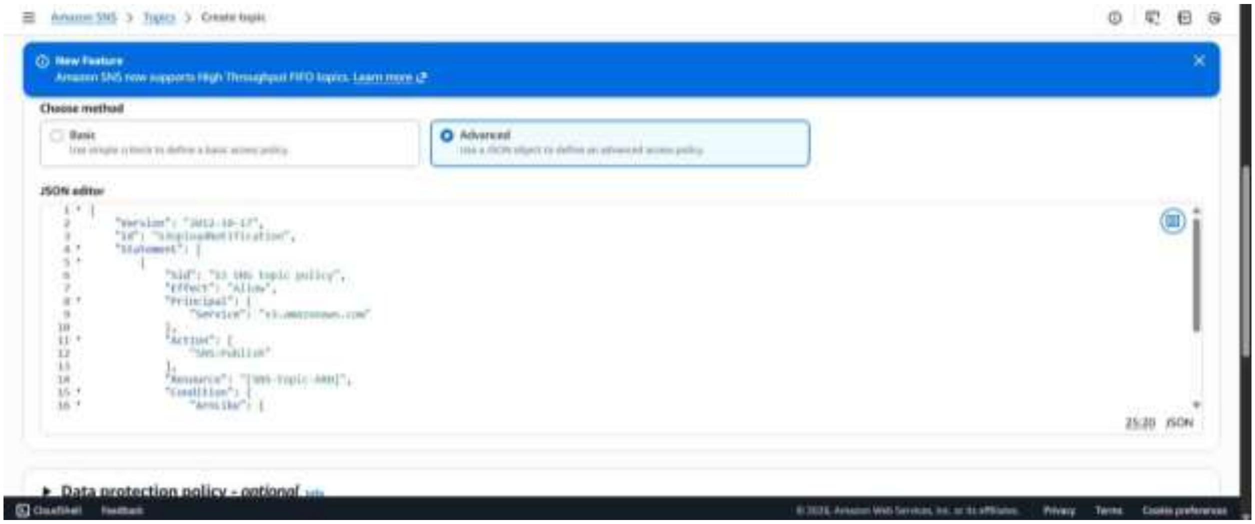
● Advanced
Use a JSON object to define an advanced access policy.

JSON editor

```
{
  "Version": "2008-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "__default_statement_ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "SNS:Publish",
        "SNS:RemovePermission",
        "SNS:SetTopicAttributes",
        "SNS:DeleteTopic",
        "SNS:ListSubscriptionsByTopic",
```

▶ Data protection policy - *optional* Info

Michael M. Orenze
CLDSRV 3



New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more

Choose method

○ Basic
Use simple criteria to define a basic access policy.

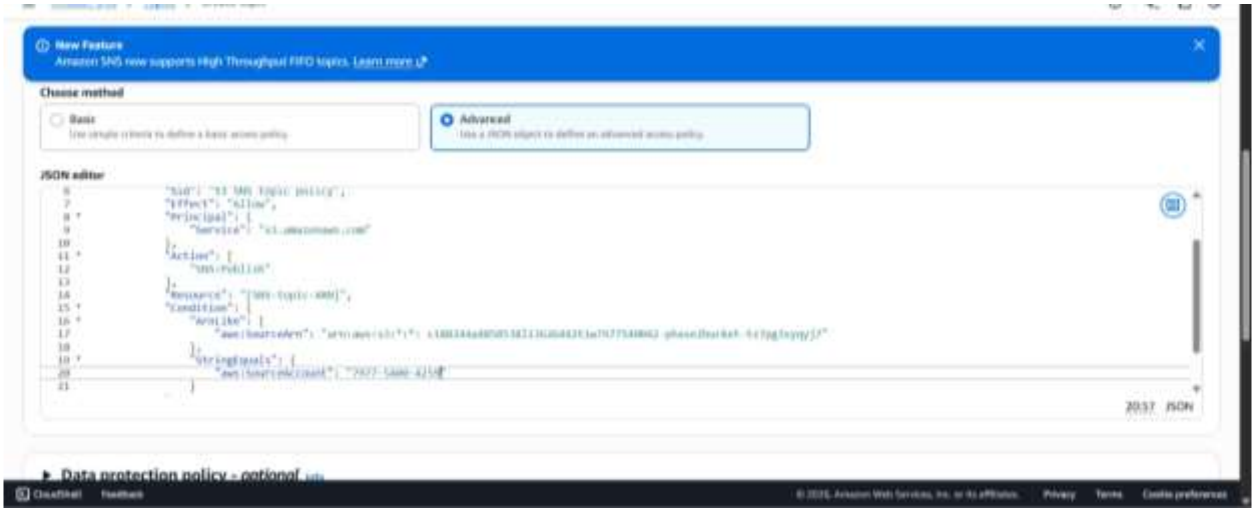
● Advanced
Use a JSON object to define an advanced access policy.

JSON editor

```
{
    "Version": "2012-10-17",
    "Id": "[illegible]",
    "Statement": [
        {
            "Sid": "S3 SNS topic policy",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "SNS:Publish"
            ],
            "Resource": "[SNS-topic-ARN]",
            "Condition": {
                "ArnLike": {
```

25:20 JSON

▶ Data protection policy - optional Info


New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more

Choose method

○ Basic
Use simple criteria to define a basic access policy.

● Advanced
Use a JSON object to define an advanced access policy.

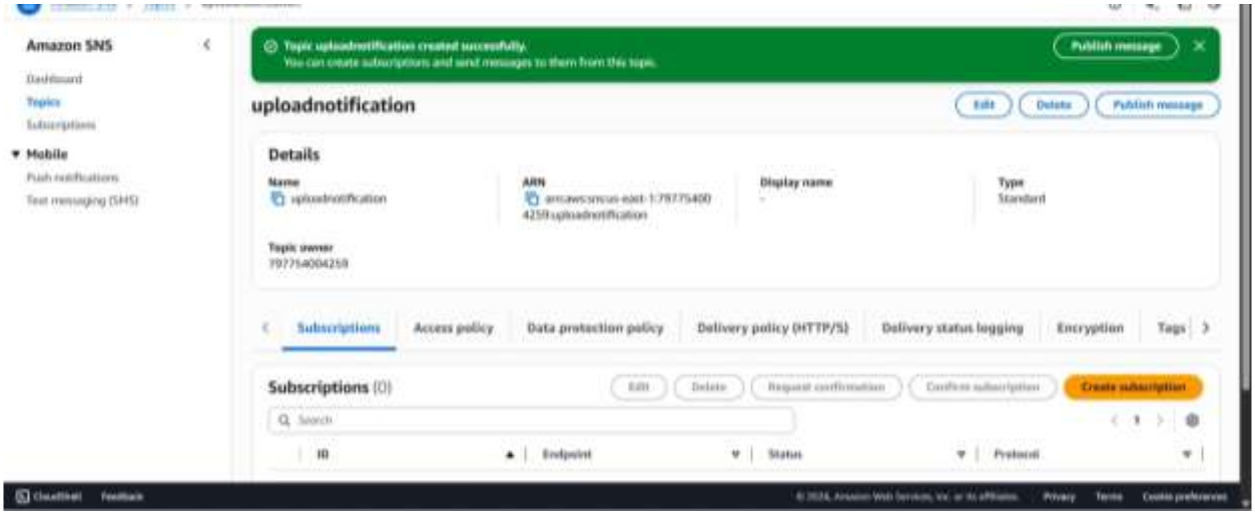
JSON editor

```
            "Sid": "S3 SNS topic policy",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "SNS:Publish"
            ],
            "Resource": "[SNS-topic-ARN]",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:*:*: [illegible]"
                },
                "StringEquals": {
                    "aws:SourceAccount": "[illegible]"
                }
```

20:57 JSON

▶ Data protection policy - optional Info

Michael M. Orenze
CLDSRV 3



Topic uploadnotification created successfully.
You can create subscriptions and send messages to them from this topic.

uploadnotification

Details

Name: uploadnotification

ARN: arn:aws:sns:us-east-1:79775400 4259:uploadnotification

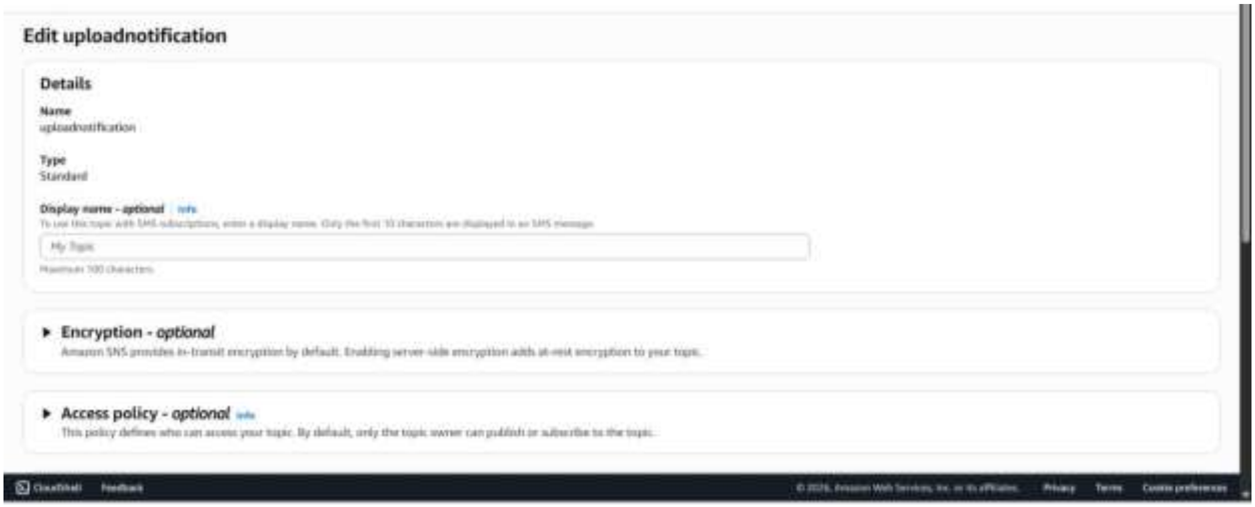
Display name: -

Type: Standard

Topic owner: 797754004259

Subscriptions (0)

ID	Endpoint	Status	Protocol



Edit uploadnotification

Details

Name
uploadnotification

Type
Standard

Display name - *optional* Info
To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message.

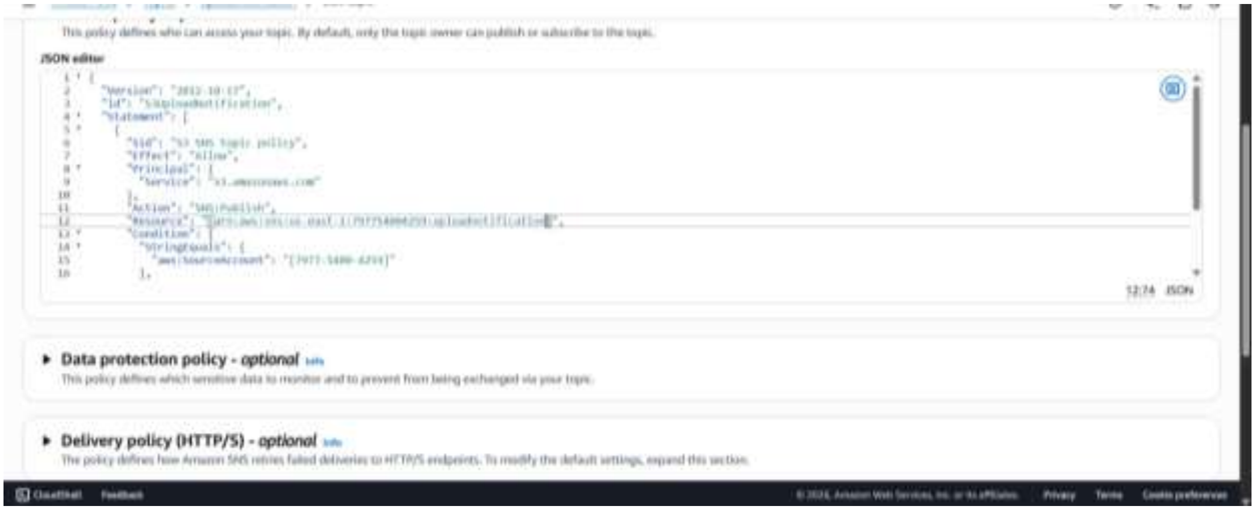
My Topic

Maximum 100 characters.

Encryption - *optional*
Amazon SNS provides in-transit encryption by default. Enabling server-side encryption adds at-rest encryption to your topic.

Access policy - *optional* Info
This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic.

Michael M. Orenze
CLDSRV 3



This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic.

JSON editor

```
{
  "Version": "2012-10-17",
  "Id": "S3uploadNotification",
  "Statement": [
    {
      "Sid": "S3 SNS topic policy",
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-east-1:797754004259:uploadnotification",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "[7977-5400-4259]"
        },
```

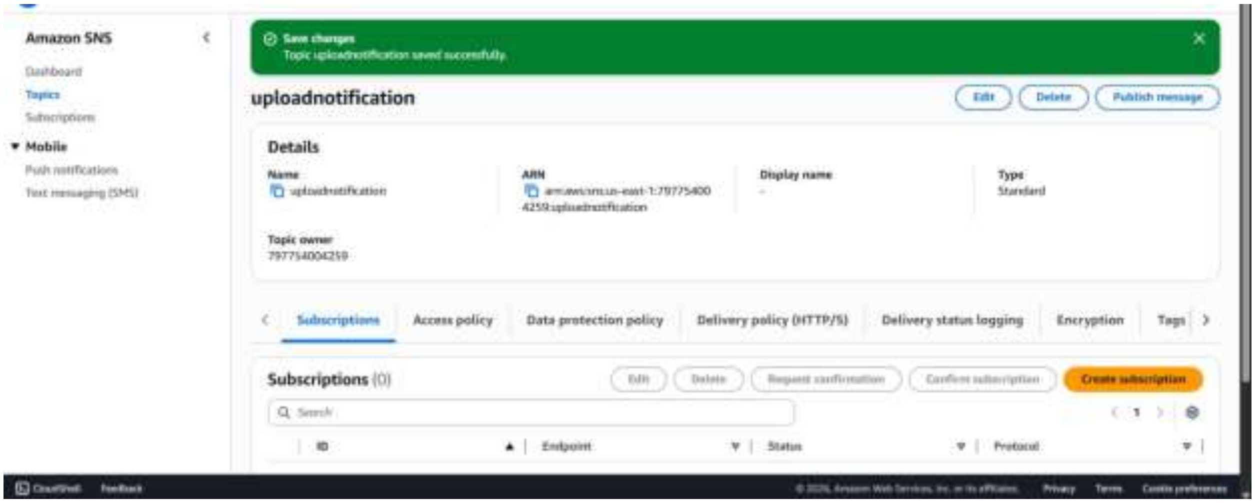
12:74 JSON

▸ **Data protection policy - *optional*** Info

This policy defines which sensitive data to monitor and to prevent from being exchanged via your topic.

▸ **Delivery policy (HTTP/S) - *optional*** Info

The policy defines how Amazon SNS retries failed deliveries to HTTP/S endpoints. To modify the default settings, expand this section.



Save changes
Topic uploadnotification saved successfully.

uploadnotification

Details

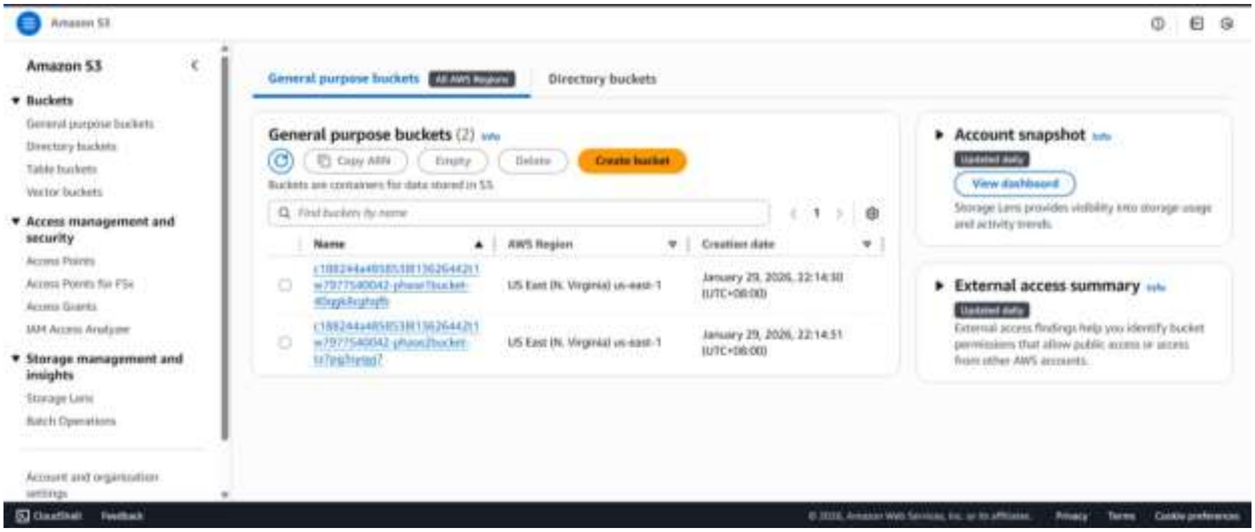
Name	ARN	Display name	Type
uploadnotification	arn:aws:sns:us-east-1:797754004259:uploadnotification	-	Standard

Topic owner
797754004259

Subscriptions (0)

ID	Endpoint	Status	Protocol

Michael M. Orenze
CLDSRV 3



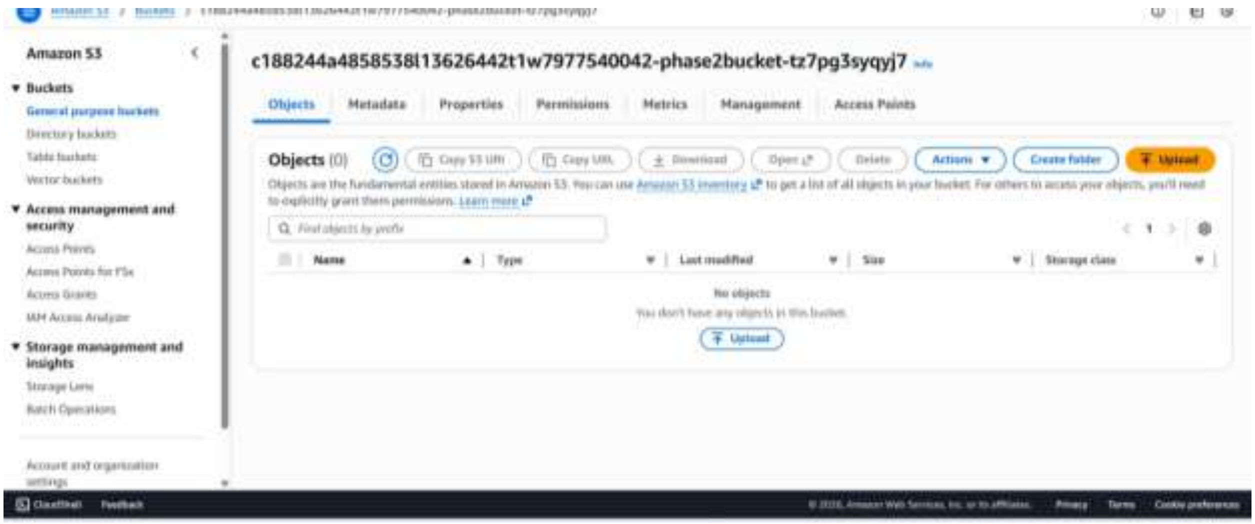
General purpose buckets (2) Info

Buckets are containers for data stored in S3.

Name	AWS Region	Creation date
c188244a4858538l13626442t1w7977540042-phase1bucket-40qgk8cghqfb	US East (N. Virginia) us-east-1	January 29, 2026, 22:14:30 (UTC+08:00)
c188244a4858538l13626442t1w7977540042-phase2bucket-tz7pg3syqyj7	US East (N. Virginia) us-east-1	January 29, 2026, 22:14:51 (UTC+08:00)

Storage Lens provides visibility into storage usage and activity trends.

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.



c188244a4858538l13626442t1w7977540042-phase2bucket-tz7pg3syqyj7 Info

Objects (0)

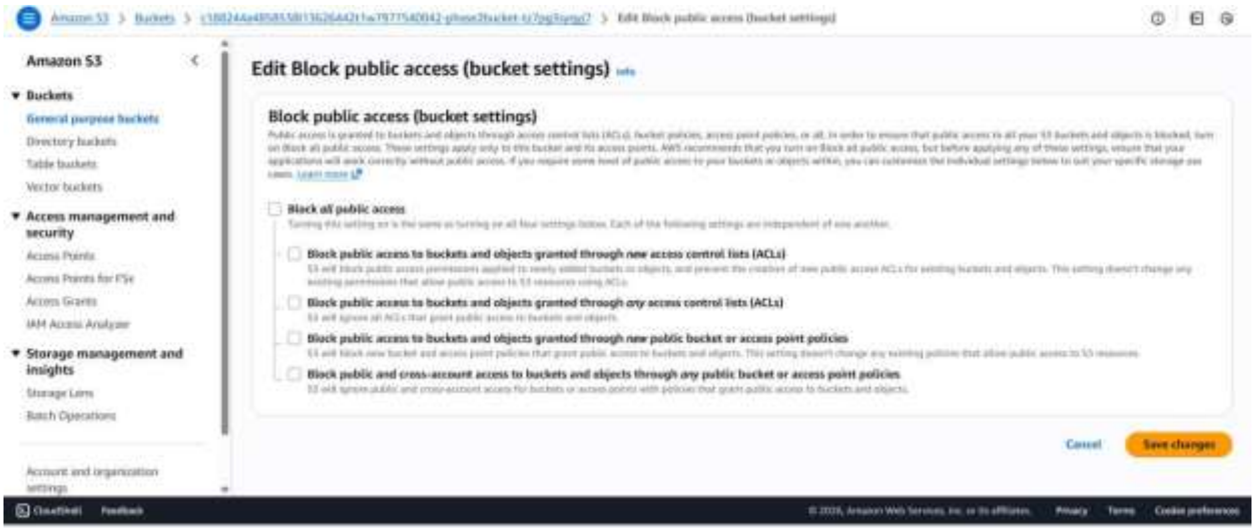
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.

Michael M. Orenze
CLDSRV 3


Amazon S3 > Buckets > c188244a4858538l13626442t1w7977540042-phase2bucket-tz7pg3syqyj7 > Edit Block public access (bucket settings)
Amazon S3
▼ Buckets
General purpose buckets
Directory buckets
Table buckets
Vector buckets
▼ Access management and security
Access Points
Access Points for FSx
Access Grants
IAM Access Analyzer
▼ Storage management and insights
Storage Lens
Batch Operations
Account and organization settings
CloudShell
Feedback
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Edit Block public access (bucket settings) Info

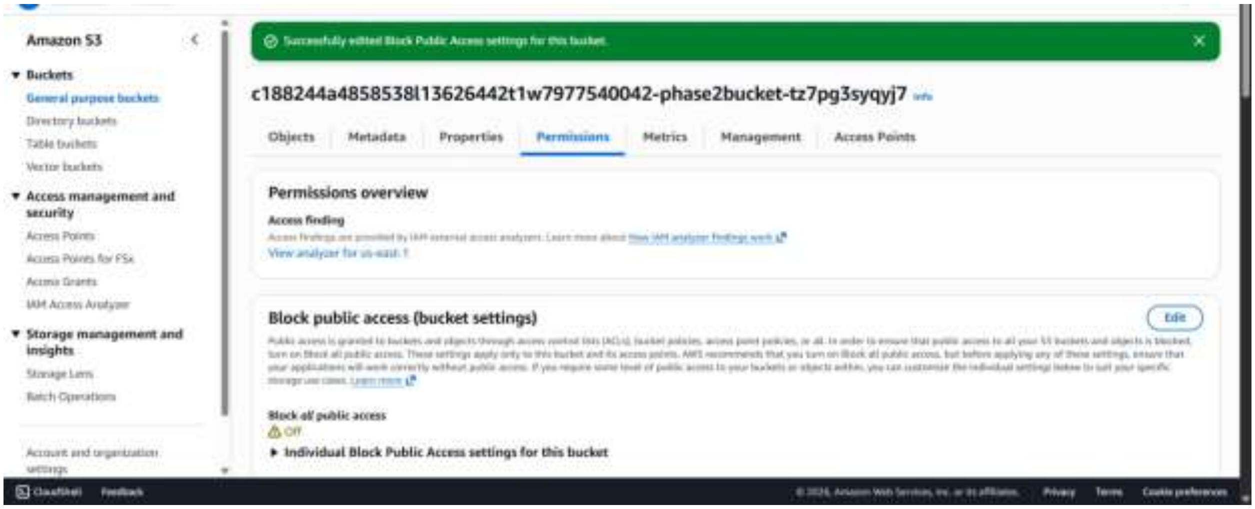
Block public access (bucket settings)

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**
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 or access point policies**
  S3 will block new bucket and access point 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 or access point policies**
  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Cancel | Save changes



Successfully edited Block Public Access settings for this bucket.

c188244a4858538l13626442t1w7977540042-phase2bucket-tz7pg3syqyj7 Info

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

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)

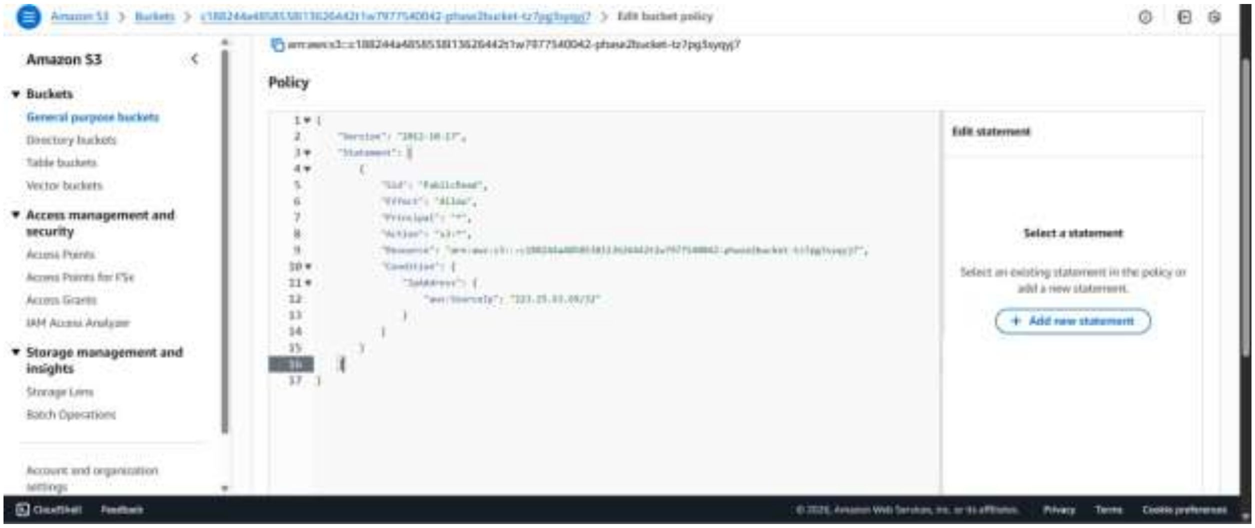
Edit

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
⚠ Off

▶ **Individual Block Public Access settings for this bucket**

Michael M. Orenze
CLDSRV 3



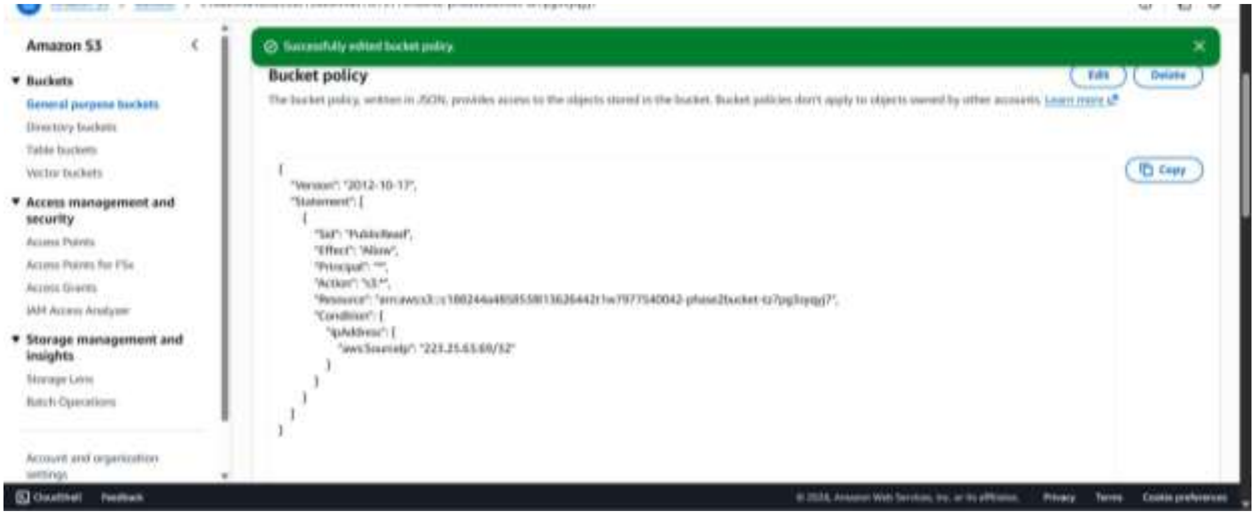
Amazon S3 > Buckets > c188244a48585581136264421w7977540042-phase2bucket-tz7pg3syqyj7 > Edit bucket policy

arn:aws:s3:::c188244a48585581136264421w7977540042-phase2bucket-tz7pg3syqyj7

Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicRead",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::c188244a48585581136264421w7977540042-phase2bucket-tz7pg3syqyj7",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "223.25.63.69/32"
                }
            }
        }
    ]
}
```

Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



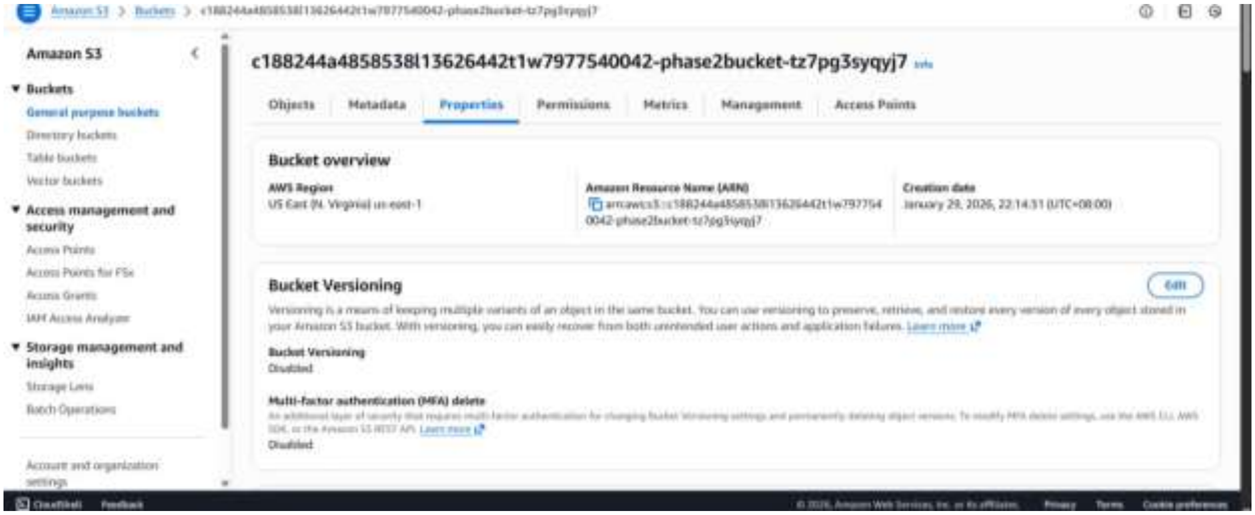
Successfully edited bucket policy.

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicRead",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::c188244a48585581136264421w7977540042-phase2bucket-tz7pg3syqyj7",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "223.25.63.69/32"
        }
      }
    }
  ]
}
```

Michael M. Orenze
CLDSRV 3



c188244a4858538l13626442t1w7977540042-phase2bucket-tz7pg3syqyj7

Bucket overview

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

Amazon Resource Name (ARN)
arn:aws:s3:::c188244a4858538l13626442t1w7977540042-phase2bucket-tz7pg3syqyj7

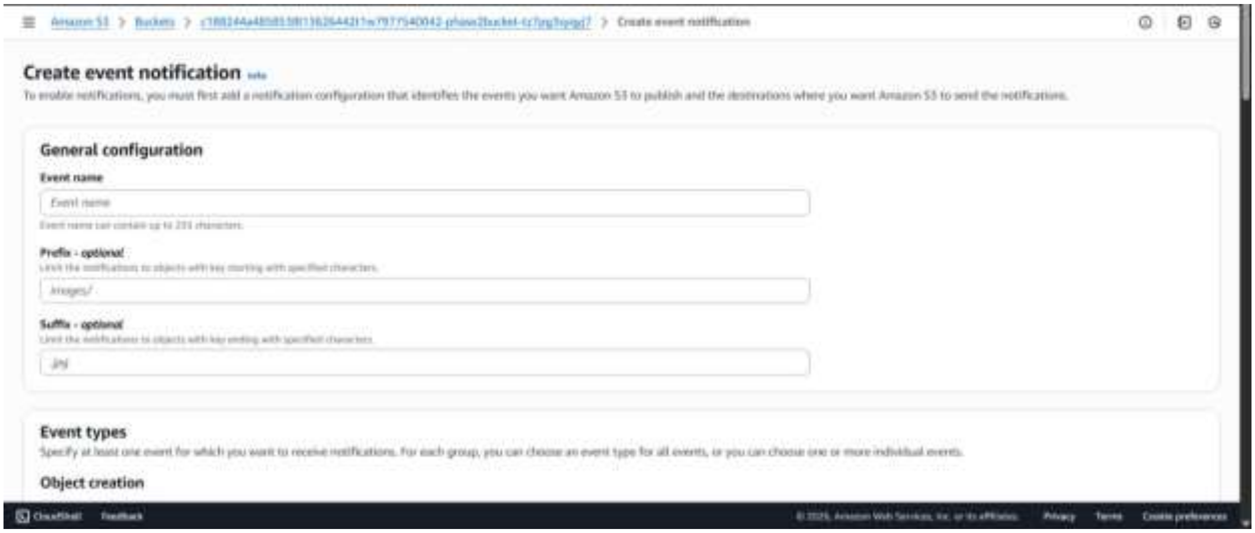
Creation date
January 29, 2026, 22:14:31 (UTC+08:00)

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
Disabled

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


Amazon S3 > Buckets > c188244a4858538l13626442t1w7977540042-phase2bucket-tz7pg3syqyj7 > Create event notification
Info
CloudShell
Feedback
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Create event notification

To enable notifications, you must first add a notification configuration that identifies the events you want Amazon S3 to publish and the destinations where you want Amazon S3 to send the notifications.

General configuration

Event name
Event name
Event name can contain up to 255 characters.

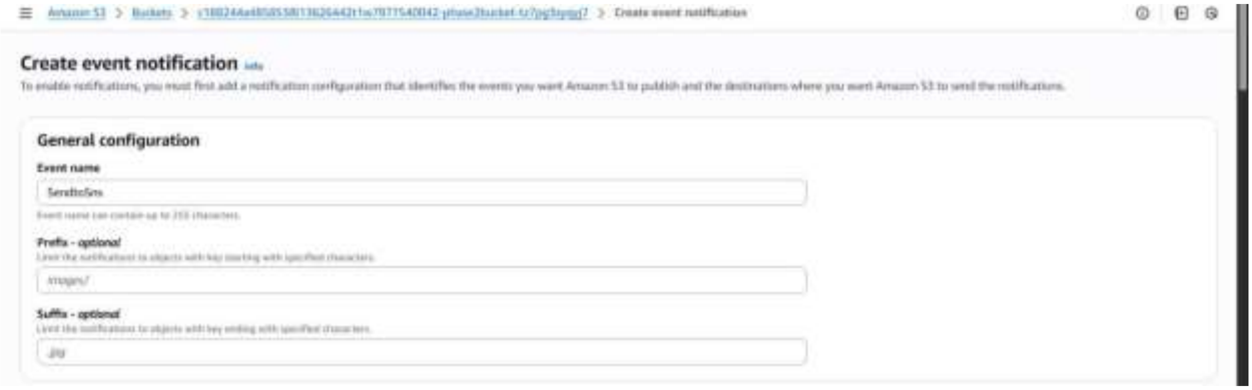
Prefix - optional
Limit the notifications to objects with key starting with specified characters.
images/

Suffix - optional
Limit the notifications to objects with key ending with specified characters.
.jpg

Event types

Specify at least one event for which you want to receive notifications. For each group, you can choose an event type for all events, or you can choose one or more individual events.

Object creation


Amazon S3 > Buckets > c188244a4858538l13626442t1w7977540042-phase2bucket-tz7pg3syqyj7 > Create event notification
Info

Create event notification

To enable notifications, you must first add a notification configuration that identifies the events you want Amazon S3 to publish and the destinations where you want Amazon S3 to send the notifications.

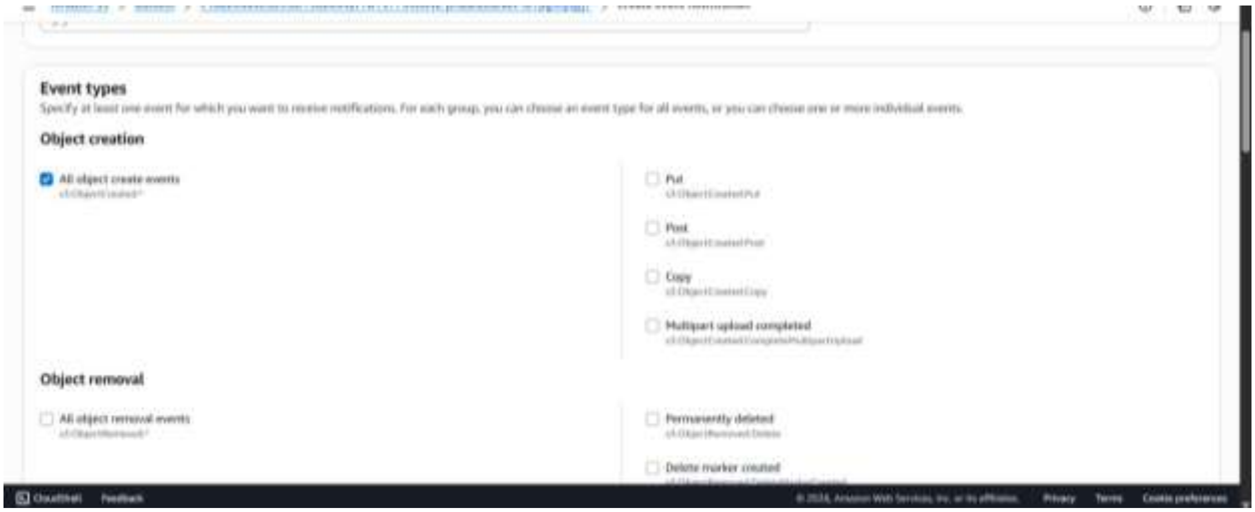
General configuration

Event name
SendtoSns
Event name can contain up to 255 characters.

Prefix - optional
Limit the notifications to objects with key starting with specified characters.
images/

Suffix - optional
Limit the notifications to objects with key ending with specified characters.
.jpg

Michael M. Orenze
CLDSRV 3



Event types

Specify at least one event for which you want to receive notifications. For each group, you can choose an event type for all events, or you can choose one or more individual events.

Object creation

☑ All object create events
s3:ObjectCreated:*

□ Put
s3:ObjectCreated:Put

□ Post
s3:ObjectCreated:Post

□ Copy
s3:ObjectCreated:Copy

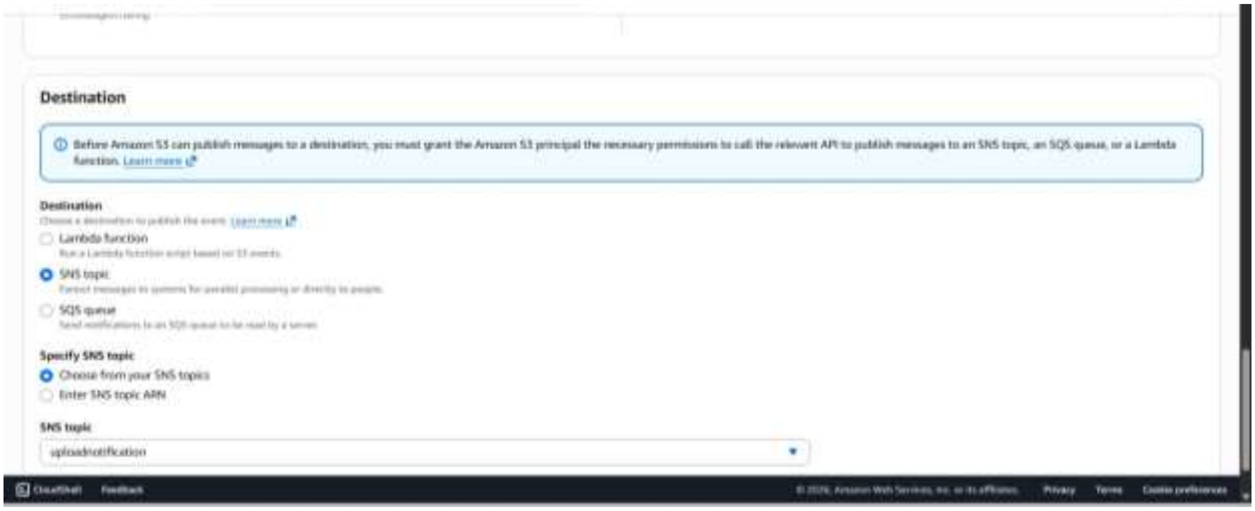
□ Multipart upload completed
s3:ObjectCreated:CompleteMultipartUpload

Object removal

□ All object removal events
s3:ObjectRemoved:*

□ Permanently deleted
s3:ObjectRemoved:Delete

□ Delete marker created



Destination

ⓘ Before Amazon S3 can publish messages to a destination, you must grant the Amazon S3 principal the necessary permissions to call the relevant API to publish messages to an SNS topic, an SQS queue, or a Lambda function. Learn more

Destination
Choose a destination to publish the event. Learn more

○ Lambda function
Run a Lambda function script based on S3 events.

● SNS topic
Fanout messages to systems for parallel processing or directly to people.

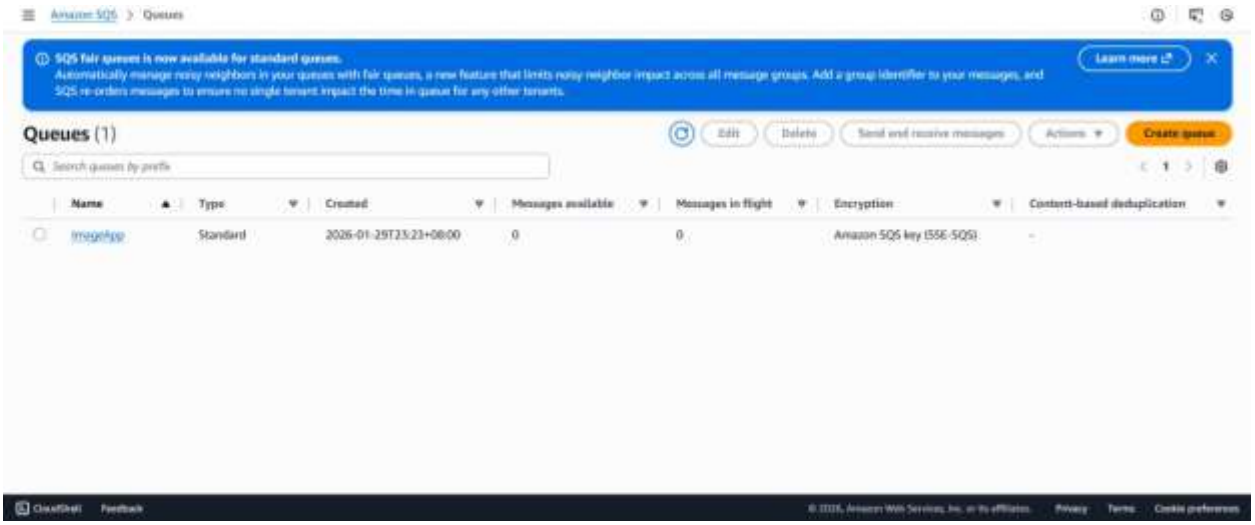
○ SQS queue
Send notifications to an SQS queue to be read by a server.

Specify SNS topic

● Choose from your SNS topics
○ Enter SNS topic ARN

SNS topic
uploadnotification ▾

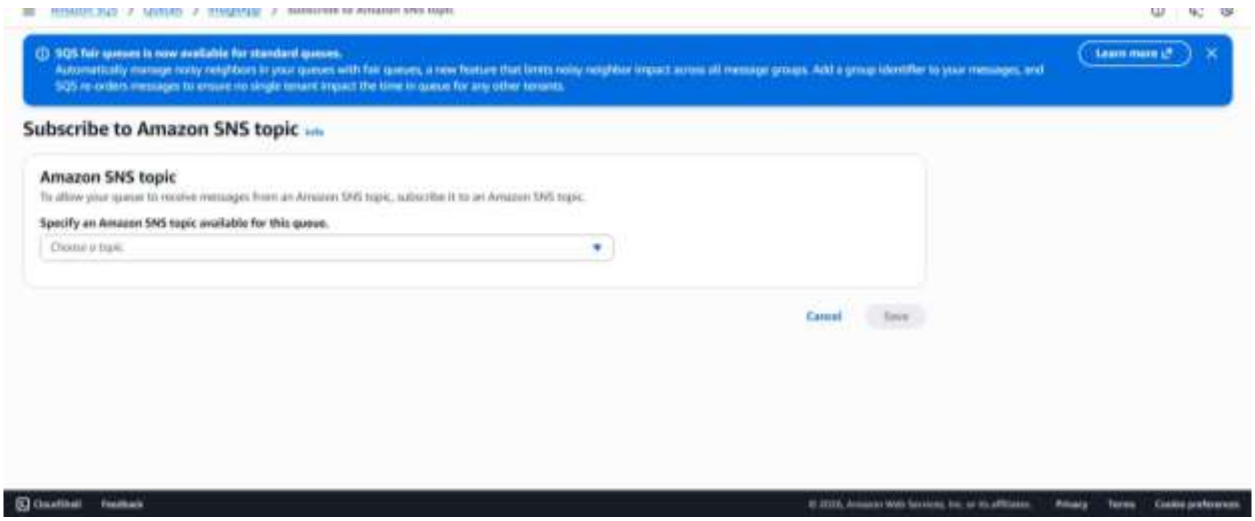
Michael M. Orenze
CLDSRV 3



SQS fair queues is now available for standard queues.
Automatically manage noisy neighbors in your queues with fair queues, a new feature that limits noisy neighbor impact across all message groups. Add a group identifier to your messages, and SQS re-orders messages to ensure no single tenant impact the time in queue for any other tenants.

Queues (1)

	Name	Type	Created	Messages available	Messages in flight	Encryption	Content-based deduplication
○	imageApp	Standard	2026-01-29T23:23+08:00	0	0	Amazon SQS key (SSE-SQS)	-


Amazon SQS > Queues > imageApp > Subscribe to Amazon SNS topic
Learn more
Info
Cancel
Save
CloudShell
Feedback
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

SQS fair queues is now available for standard queues.
Automatically manage noisy neighbors in your queues with fair queues, a new feature that limits noisy neighbor impact across all message groups. Add a group identifier to your messages, and SQS re-orders messages to ensure no single tenant impact the time in queue for any other tenants.

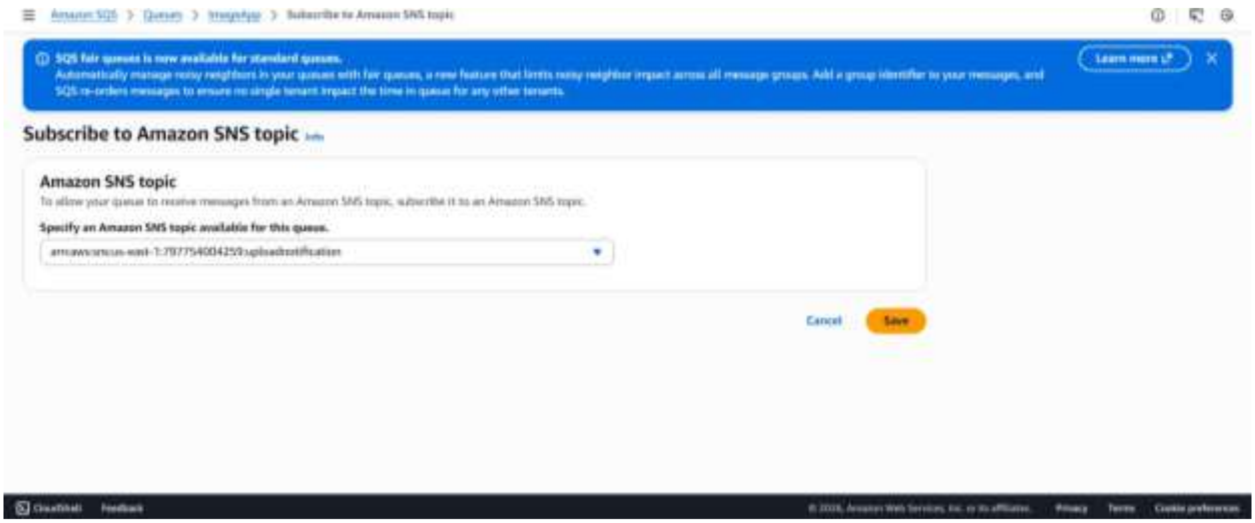
Subscribe to Amazon SNS topic

Amazon SNS topic

To allow your queue to receive messages from an Amazon SNS topic, subscribe it to an Amazon SNS topic.

Specify an Amazon SNS topic available for this queue.

Choose a topic


Amazon SQS > Queues > imageApp > Subscribe to Amazon SNS topic
Learn more
Info
Cancel
Save
CloudShell
Feedback
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

SQS fair queues is now available for standard queues.
Automatically manage noisy neighbors in your queues with fair queues, a new feature that limits noisy neighbor impact across all message groups. Add a group identifier to your messages, and SQS re-orders messages to ensure no single tenant impact the time in queue for any other tenants.

Subscribe to Amazon SNS topic

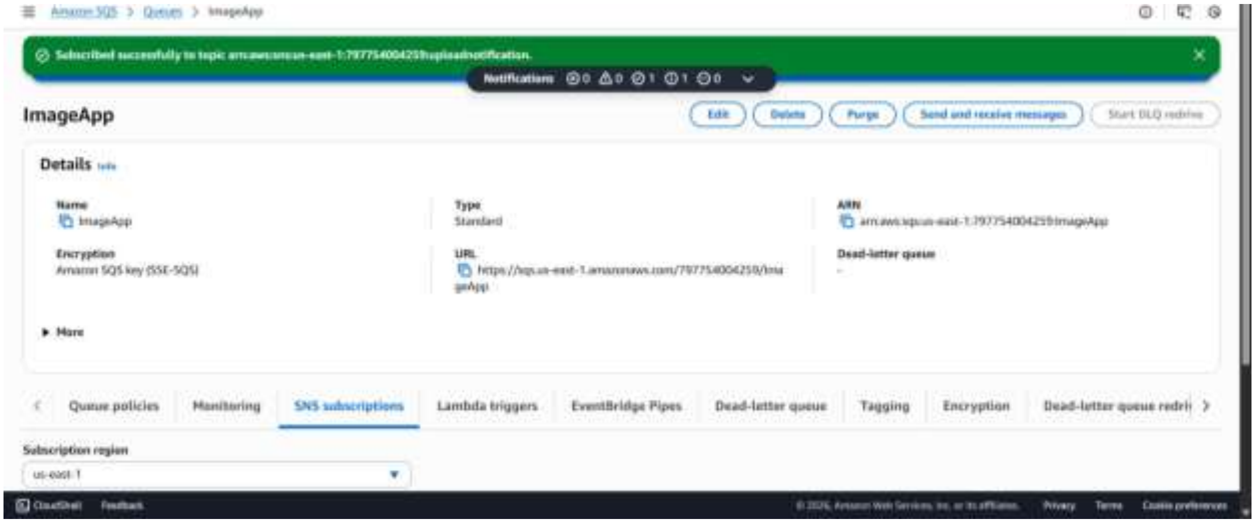
Amazon SNS topic

To allow your queue to receive messages from an Amazon SNS topic, subscribe it to an Amazon SNS topic.

Specify an Amazon SNS topic available for this queue.

arn:aws:sns:us-east-1:787754004259:uploadnotification

Michael M. Orenze
CLDSRV 3



Subscribed successfully to topic arn:aws:sns:us-east-1:797754004259:uploadnotification.

ImageApp

Details

Name
ImageApp

Type
Standard

ARN
arn:aws:sqs:us-east-1:797754004259:ImageApp

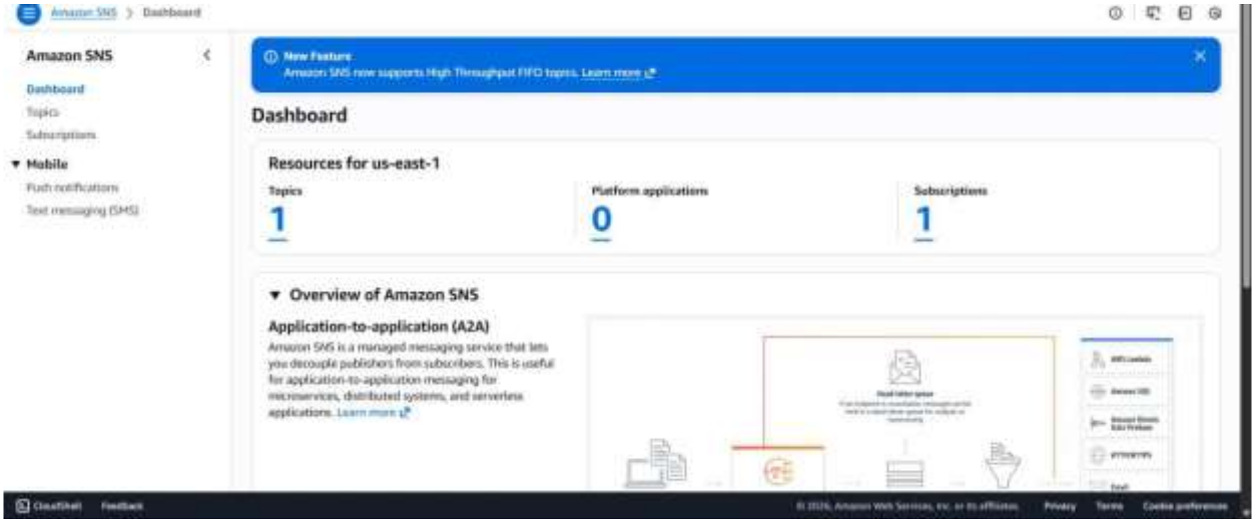
Encryption
Amazon SQS key (SSE-SQS)

URL
https://sqs.us-east-1.amazonaws.com/797754004259/ImageApp

Dead-letter queue
-

Subscription region
us-east-1

© 2026, Amazon Web Services, Inc. or its affiliates.



New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more

Dashboard

Resources for us-east-1

Topics
1

Platform applications
0

Subscriptions
1

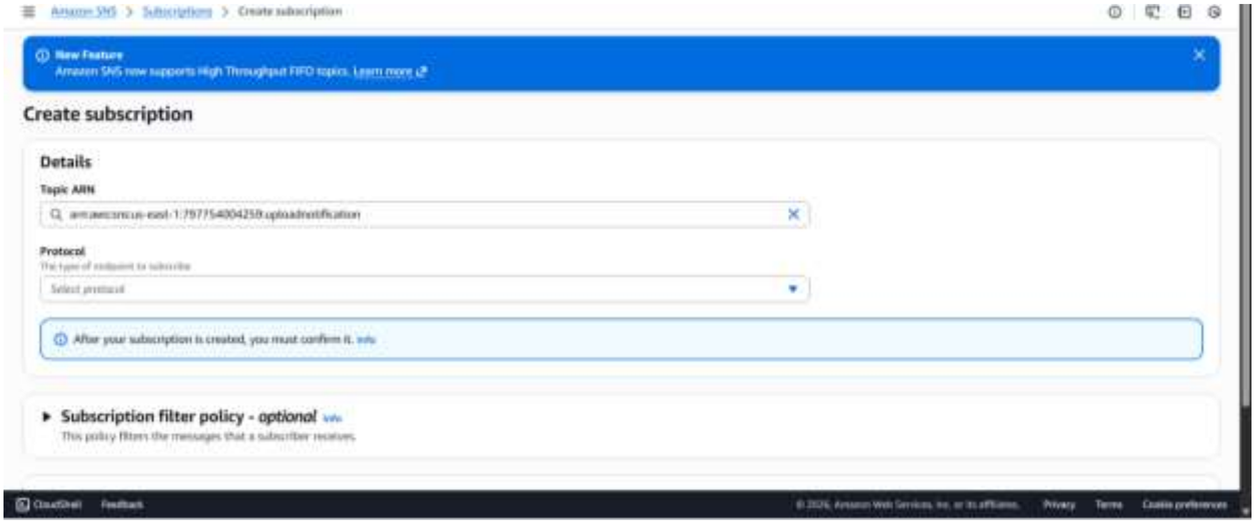
Overview of Amazon SNS

Application-to-application (A2A)

Amazon SNS is a managed messaging service that lets you decouple publishers from subscribers. This is useful for application-to-application messaging for microservices, distributed systems, and serverless applications. Learn more

© 2026, Amazon Web Services, Inc. or its affiliates.

Michael M. Orenze
CLDSRV 3


Amazon SNS > Subscriptions > Create subscription
CloudShell
Feedback
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more

Create subscription

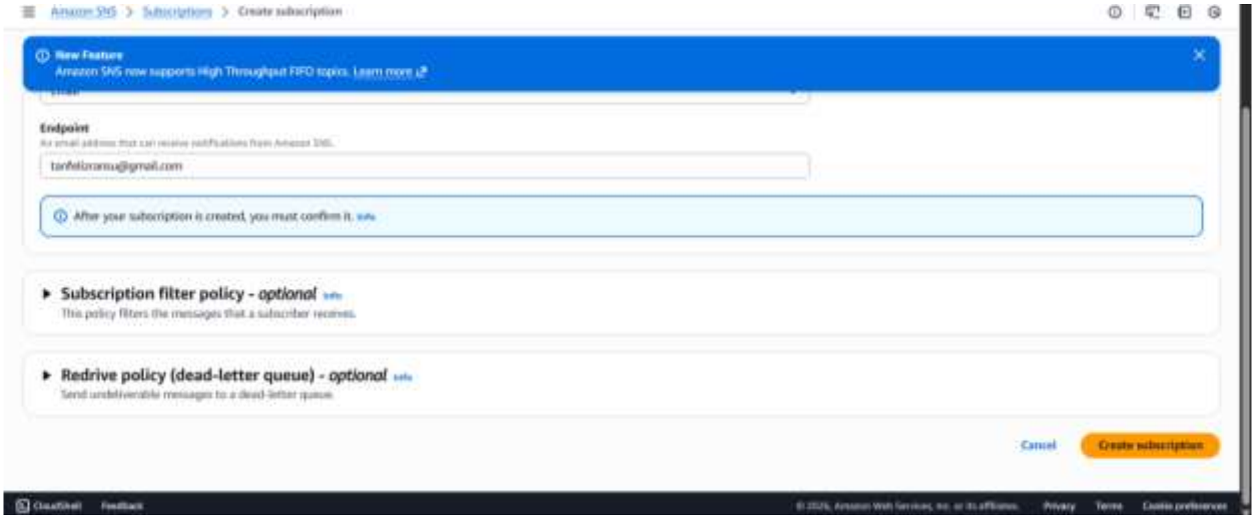
Details

Topic ARN
arn:aws:sns:us-east-1:797754004259:uploadnotification

Protocol
The type of endpoint to subscribe
Select protocol

After your subscription is created, you must confirm it. Info

▶ Subscription filter policy - *optional* Info
This policy filters the messages that a subscriber receives.


Amazon SNS > Subscriptions > Create subscription
Cancel
Create subscription
CloudShell
Feedback
© 2026, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more

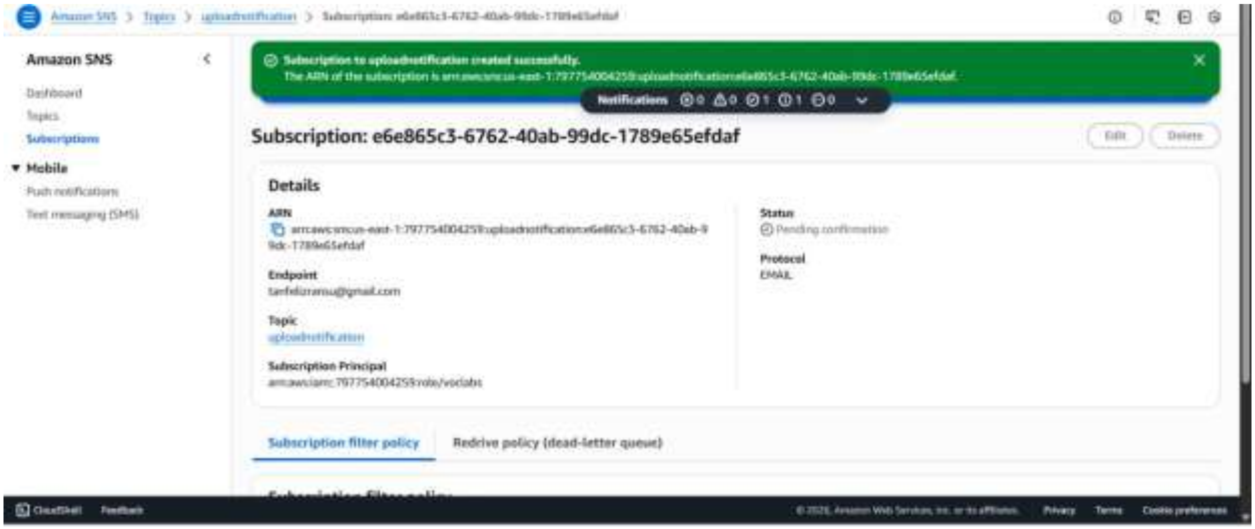
Endpoint
An email address that can receive notifications from Amazon SNS.
tanfelizransu@gmail.com

After your subscription is created, you must confirm it. Info

▶ Subscription filter policy - *optional* Info
This policy filters the messages that a subscriber receives.

▶ Redrive policy (dead-letter queue) - *optional* Info
Send undeliverable messages to a dead-letter queue.

Michael M. Orenze
CLDSRV 3


Amazon SNS > Topics > uploadnotification > Subscription: e6e865c3-6762-40ab-99dc-1789e65efdaf
Amazon SNS
Dashboard
Topics
Subscriptions
▼ Mobile
Push notifications
Text messaging (SMS)
Notifications ⊗0 △0 ⊘1 ⓘ1 ⊖0
Edit
Delete
Subscription filter policy
Redrive policy (dead-letter queue)
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Subscription to uploadnotification created successfully.
The ARN of the subscription is arn:aws:sns:us-east-1:797754004259:uploadnotification:e6e865c3-6762-40ab-99dc-1789e65efdaf.

Subscription: e6e865c3-6762-40ab-99dc-1789e65efdaf

Details

ARN
arn:aws:sns:us-east-1:797754004259:uploadnotification:e6e865c3-6762-40ab-99dc-1789e65efdaf

Endpoint
tanfelizransu@gmail.com

Topic
uploadnotification

Subscription Principal
arn:aws:iam::797754004259:role/voclabs

Status
Pending confirmation

Protocol
EMAIL

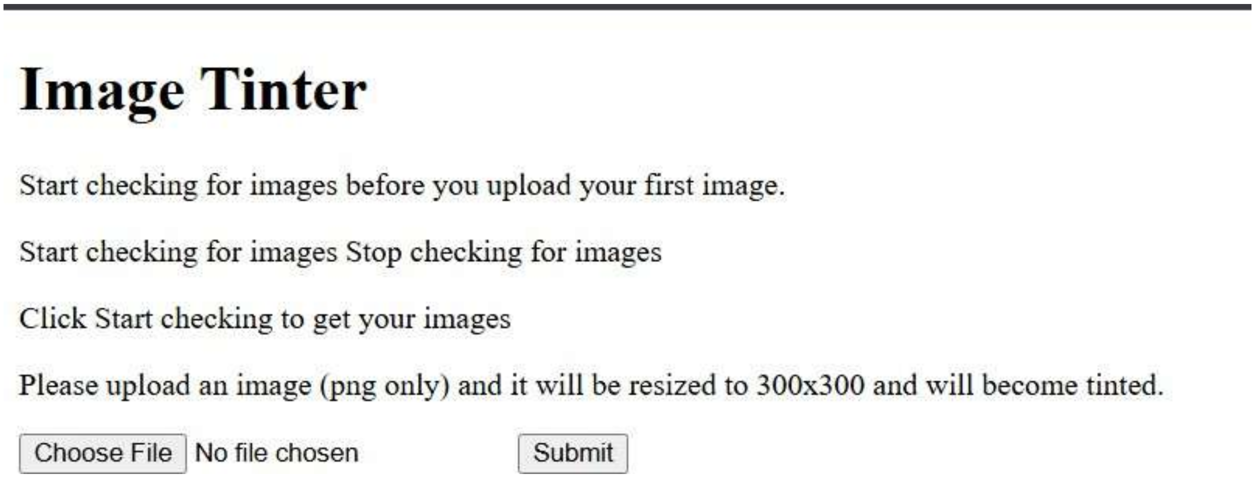


Image Tinter

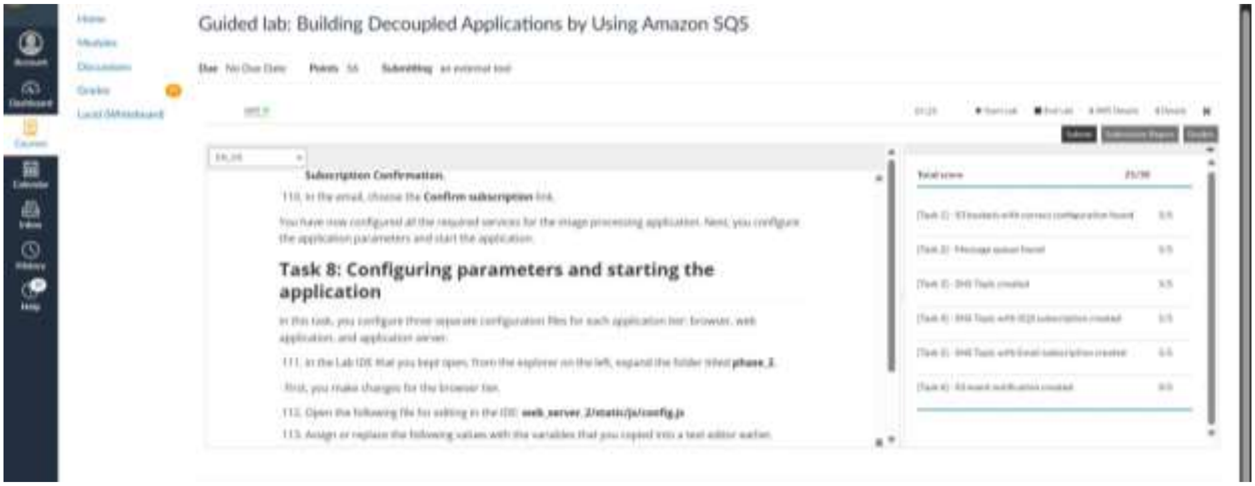
Start checking for images before you upload your first image.

Start checking for images Stop checking for images

Click Start checking to get your images

Please upload an image (png only) and it will be resized to 300x300 and will become tinted.

Michael M. Orenze
CLDSRV 3



Guided lab: Building Decoupled Applications by Using Amazon SQS

Due No Due Date **Points** 56 **Submitting** an external tool

Subscription Confirmation

110. In the email, choose the **Confirm subscription** link.

You have now configured all the required services for the image processing application. Next, you configure the application parameters and start the application.

Task 8: Configuring parameters and starting the application

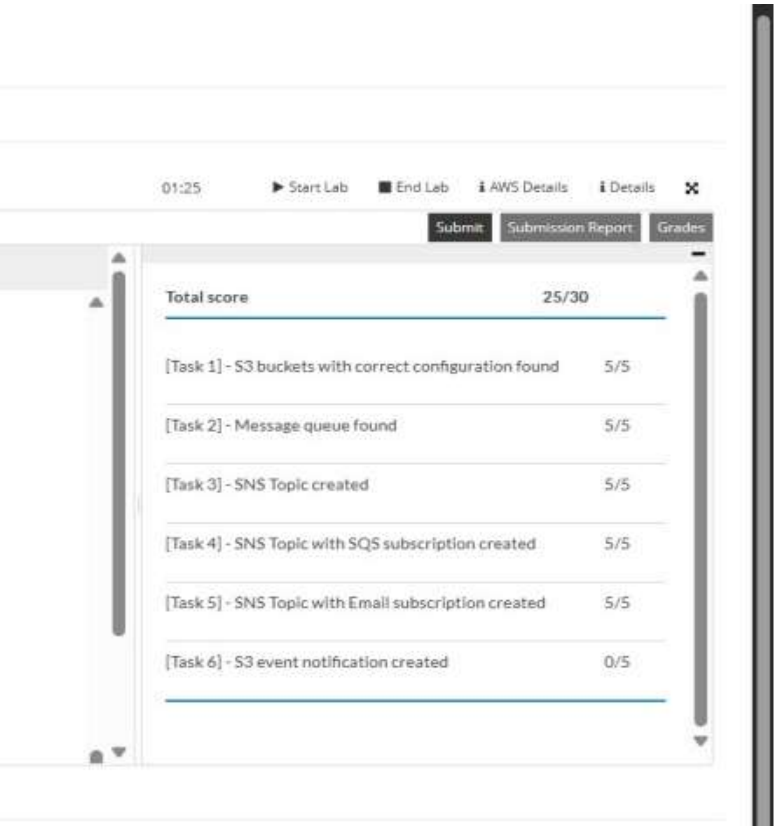
In this task, you configure three separate configuration files for each application tier: browser, web application, and application server.

111. In the Lab IDE that you kept open, from the explorer on the left, expand the folder titled **phase_2**.

First, you make changes for the browser tier.

112. Open the following file for editing in the IDE: **web_server_2/static/js/config.js**

113. Assign or replace the following values with the variables that you copied into a text editor earlier.



Total score	25/30
[Task 1] - S3 buckets with correct configuration found	5/5
[Task 2] - Message queue found	5/5
[Task 3] - SNS Topic created	5/5
[Task 4] - SNS Topic with SQS subscription created	5/5
[Task 5] - SNS Topic with Email subscription created	5/5
[Task 6] - S3 event notification created	0/5