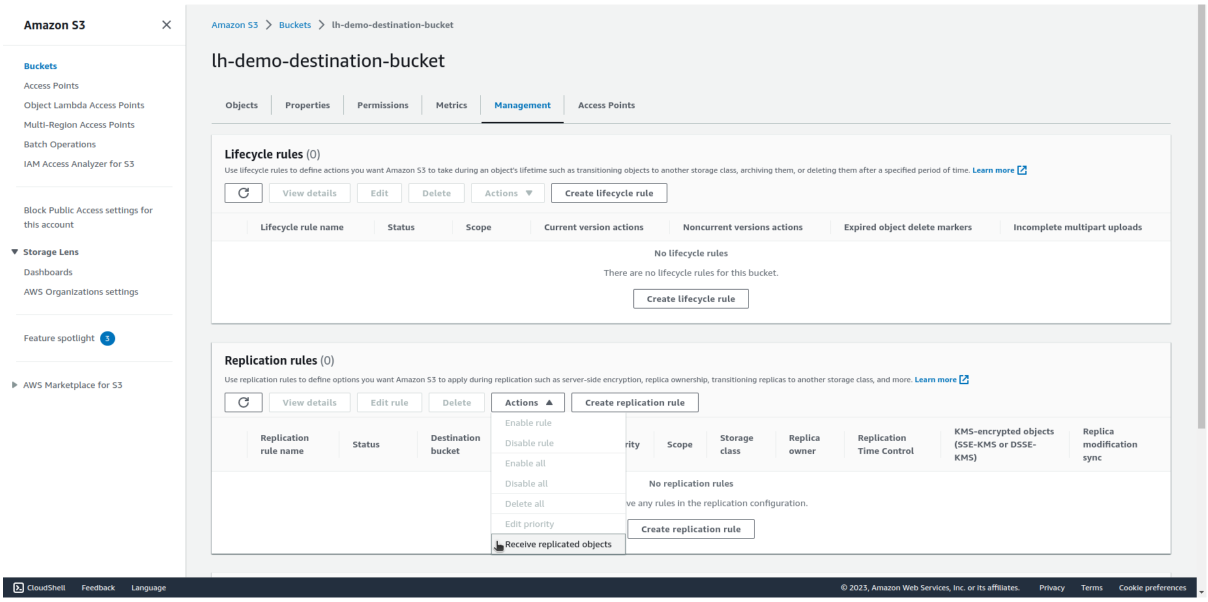
AWS S3 bucket replication

1. Open the AWS Management Console and navigate to the S3 service.

2. Create a destination S3 bucket to replicate Your source bucket to. Enable bucket versioning and leave the rest of the settings default.

3. Click on the newly created destination bucket, go to the "Management" tab, click on "Actions," and select "Receive replicated objects".



lh-demo-destination-bucket

Lifecycle rules (0)

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 markers	Incomplete multipart uploads

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	rity	Scope	Storage class	Replica owner	Replication Time Control	KMS-encrypted objects (SSE-KMS or DSSE-KMS)	Replica modification sync

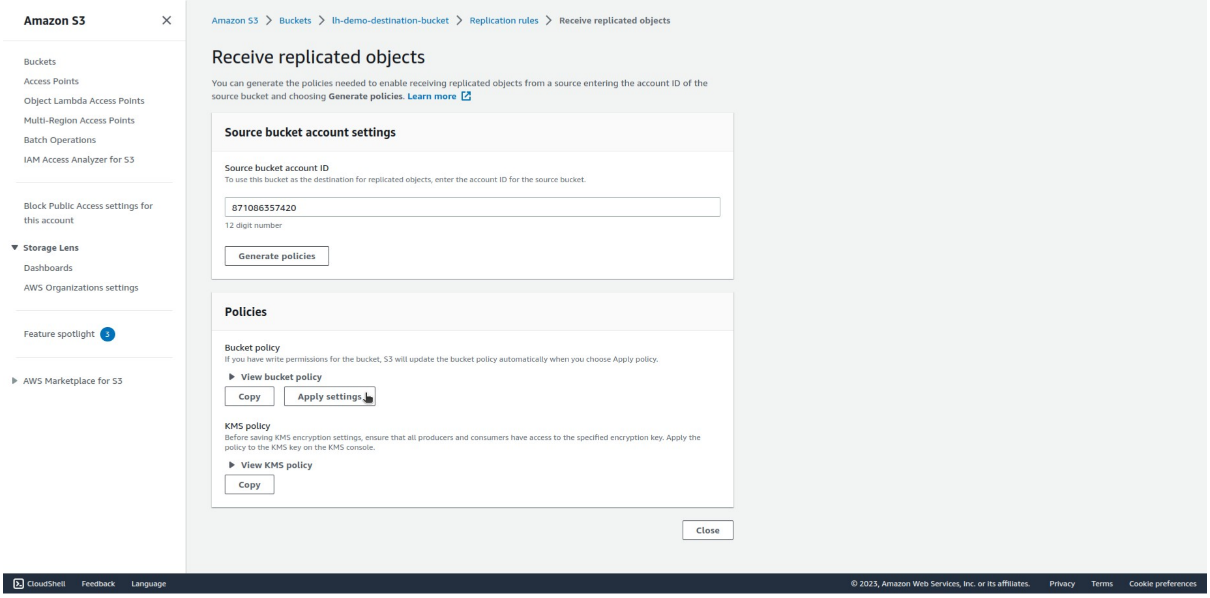
No replication rules

ve any rules in the replication configuration.

© 2023, Amazon Web Services, Inc. or its affiliates.

4. Enter your account ID and click on "Generate policies".

5. Next, click on "Apply settings".


Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Amazon S3 > Buckets > lh-demo-destination-bucket > Replication rules > Receive replicated objects

Receive replicated objects

You can generate the policies needed to enable receiving replicated objects from a source entering the account ID of the source bucket and choosing **Generate policies**. Learn more

Source bucket account settings

Source bucket account ID
To use this bucket as the destination for replicated objects, enter the account ID for the source bucket.

871086357420
12 digit number

Generate policies

Policies

Bucket policy
If you have write permissions for the bucket, S3 will update the bucket policy automatically when you choose Apply policy.

▶ View bucket policy

Copy Apply settings

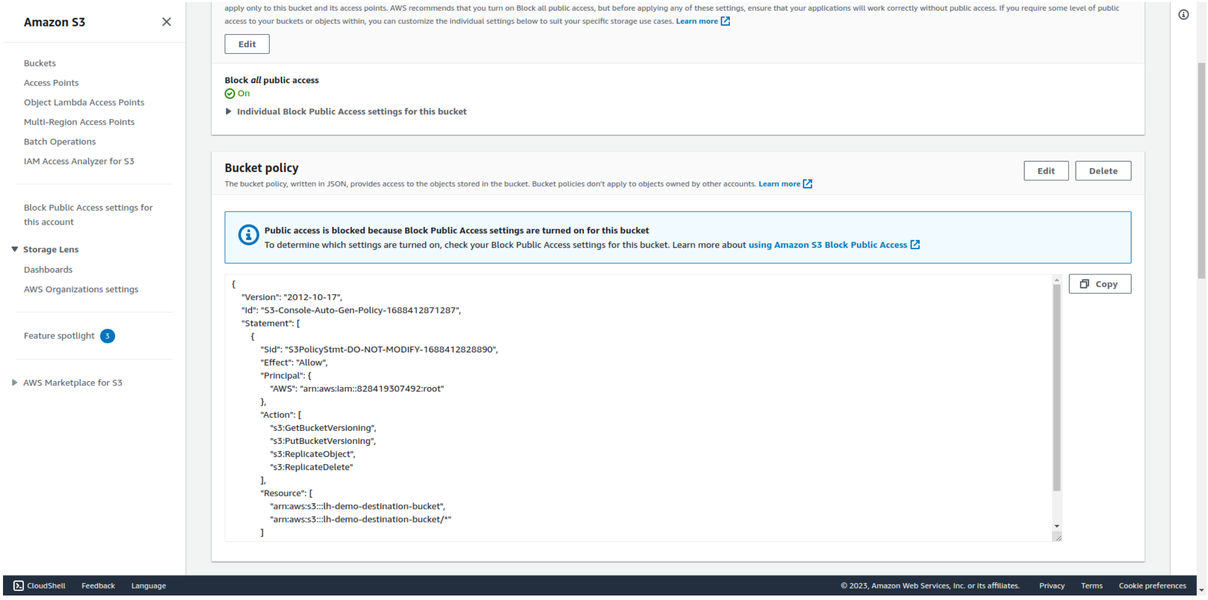
KMS policy
Before saving KMS encryption settings, ensure that all producers and consumers have access to the specified encryption key. Apply the policy to the KMS key on the KMS console.

▶ View KMS policy

Copy

Close

6. Go back to the destination bucket and check if the policy has been applied in the "Permissions" tab.


Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

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

Edit

Block *all* public access
✓ On

▶ Individual Block Public Access settings for this bucket

Bucket policy

Edit Delete

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

Copy

```
{
   "Version": "2012-10-17",
   "Id": "S3-Console-Auto-Gen-Policy-1688412871287",
   "Statement": [
      {
         "Sid": "S3PolicyStmt-DO-NOT-MODIFY-1688412828890",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::828419307492:root"
         },
         "Action": [
            "s3:GetBucketVersioning",
            "s3:PutBucketVersioning",
            "s3:ReplicateObject",
            "s3:ReplicateDelete"
         ],
         "Resource": [
            "arn:aws:s3:::lh-demo-destination-bucket",
            "arn:aws:s3:::lh-demo-destination-bucket/*"
         ]
```

7. Next, navigate to the IAM service, and choose "Policies".

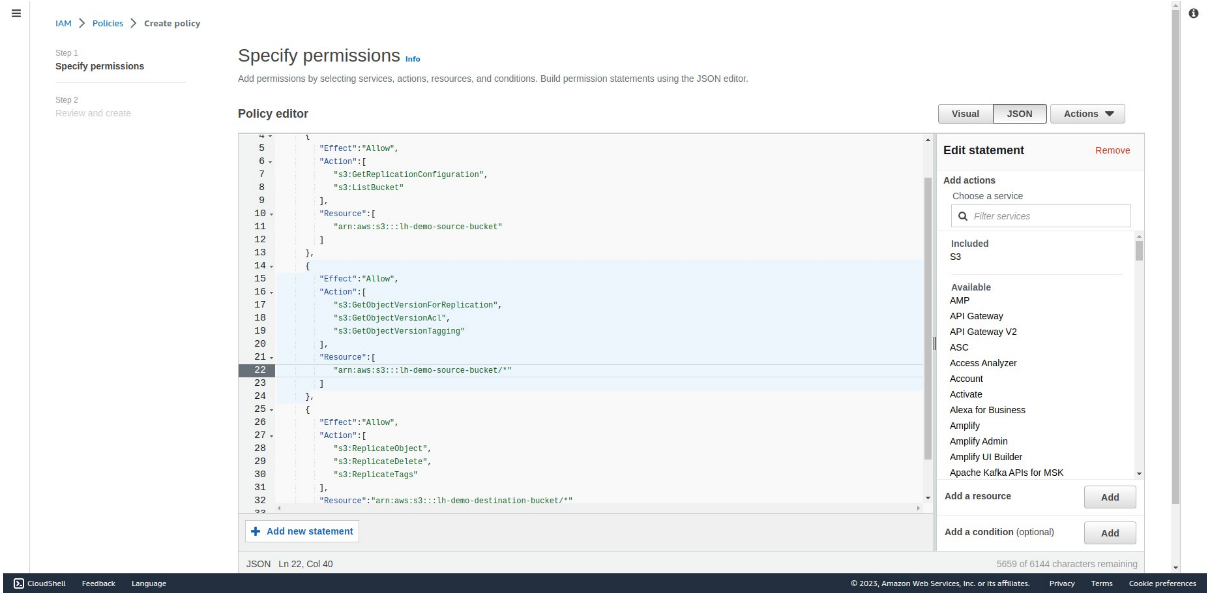
8. Click on "Create policy".

9. Choose JSON editor and copy the following policy:

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetReplicationConfiguration",
        "s3:ListBucket"
      ],
      "Resource":[
        "arn:aws:s3:::SOURCE-BUCKET"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource":[
        "arn:aws:s3:::SOURCE-BUCKET/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:ReplicateObject",
        "s3:ReplicateDelete",
        "s3:ReplicateTags"
```

```
         ],
         "Resource":"arn:aws:s3:::DESTINATION-BUCKET/*"
      }
   ]
}
```

Replace "SOURCE-BUCKET" with your source bucket name and "DESTINATION-BUCKET" with your destination bucket name, and then click on "Next" in the bottom right corner.



Specify permissions Info

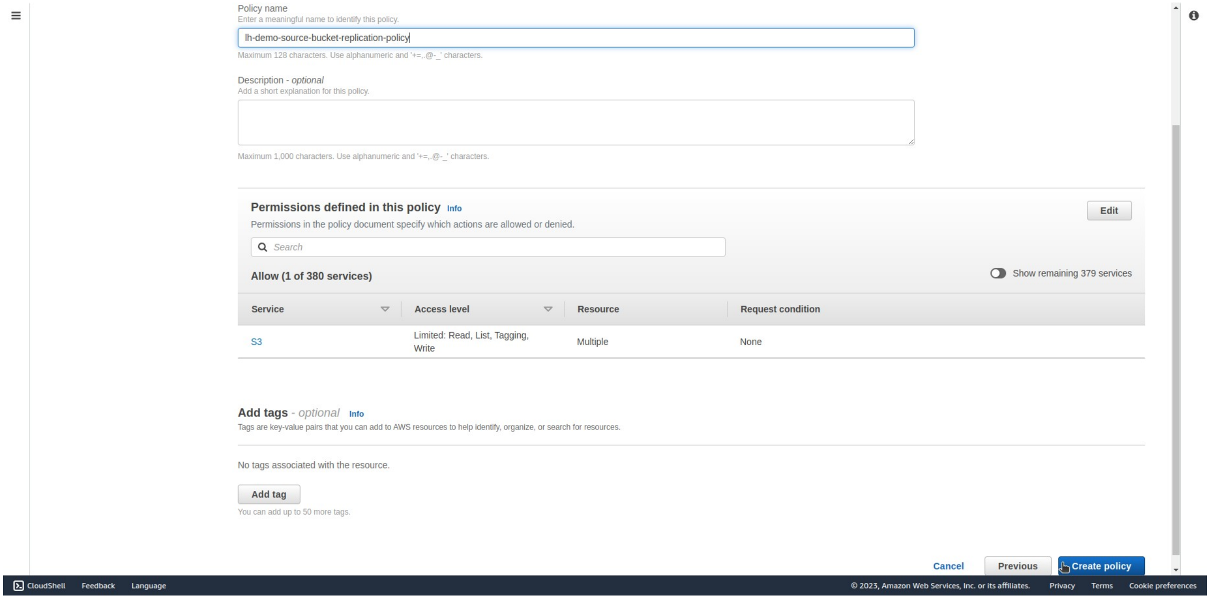
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

```
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetReplicationConfiguration",
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::lh-demo-source-bucket"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectVersionTagging"
         ],
         "Resource":[
            "arn:aws:s3:::lh-demo-source-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ReplicateTags"
         ],
         "Resource":"arn:aws:s3:::lh-demo-destination-bucket/*"
```

JSON Ln 22, Col 40

10. Give the IAM policy name and click on "Create policy" in the bottom right corner.



Policy name
Enter a meaningful name to identify this policy.
lh-demo-source-bucket-replication-policy
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

Permissions defined in this policy Info

Permissions in the policy document specify which actions are allowed or denied.

Allow (1 of 380 services)

Show remaining 379 services

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

Add tags - *optional* Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

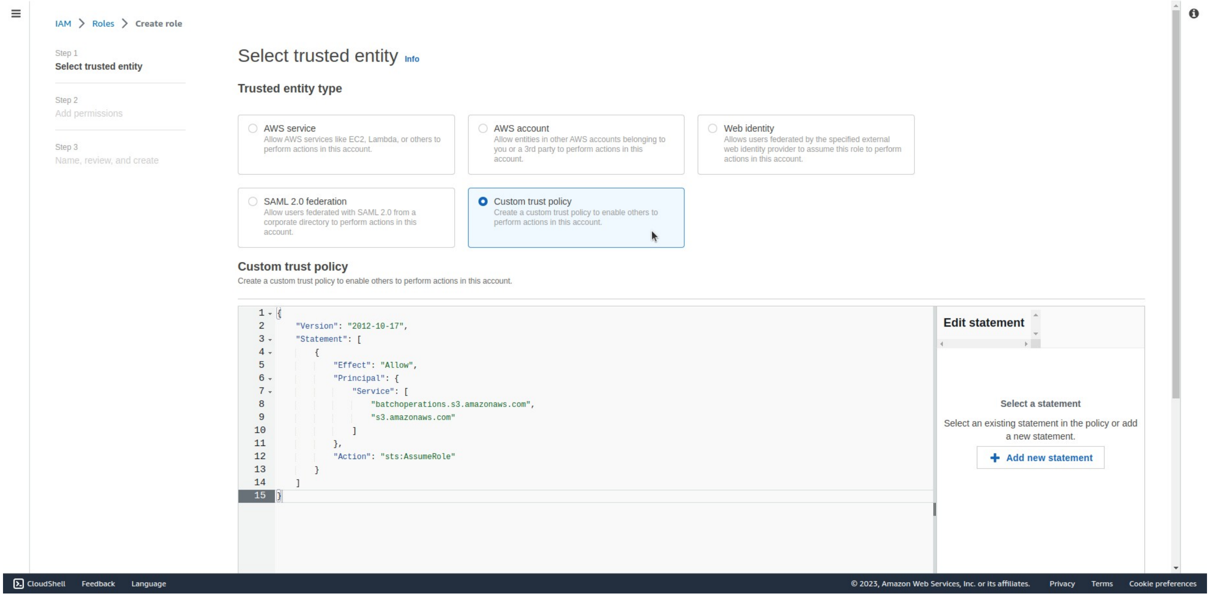
You can add up to 50 more tags.

11. Next, go to IAM Roles and click on "Create role".

12. In the "Select trusted entity" section, choose "Custom trust policy" and copy the following policy:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "Service": [
               "batchoperations.s3.amazonaws.com",
               "s3.amazonaws.com"
            ]
         },
         "Action": "sts:AssumeRole"
      }
   ]
}
```

Then click on "Next" in the bottom right corner.



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

○ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

● Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Custom trust policy

Create a custom trust policy to enable others to perform actions in this account.

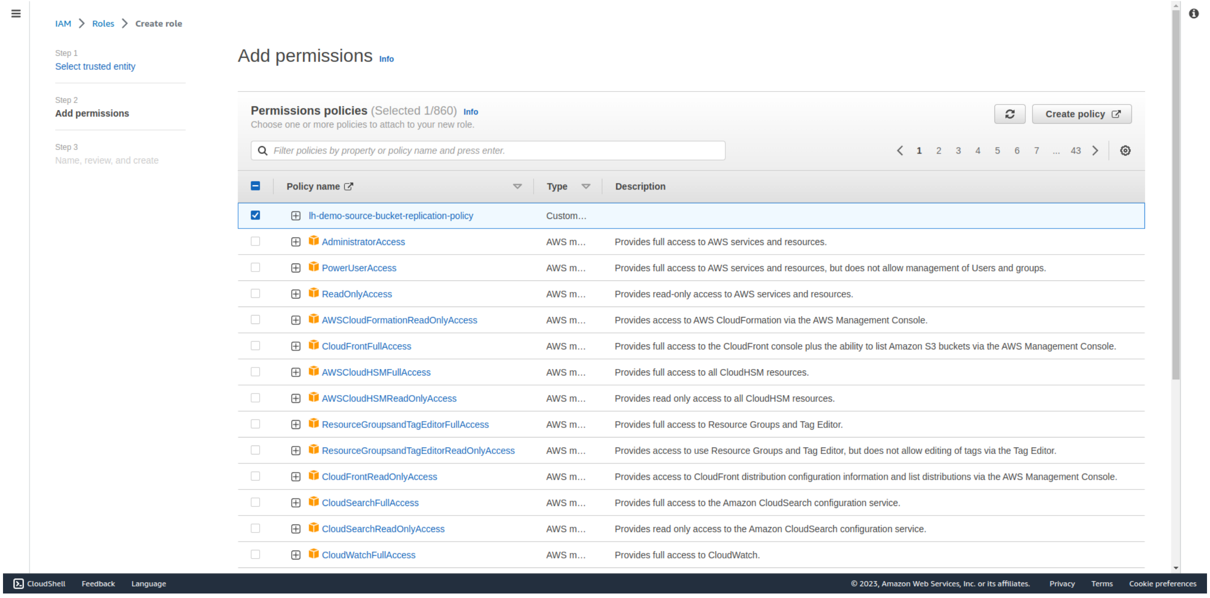
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "batchoperations.s3.amazonaws.com",
                    "s3.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Edit statement

Select a statement

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

13. Select the newly created policy and click on "Next" in the bottom right corner.



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

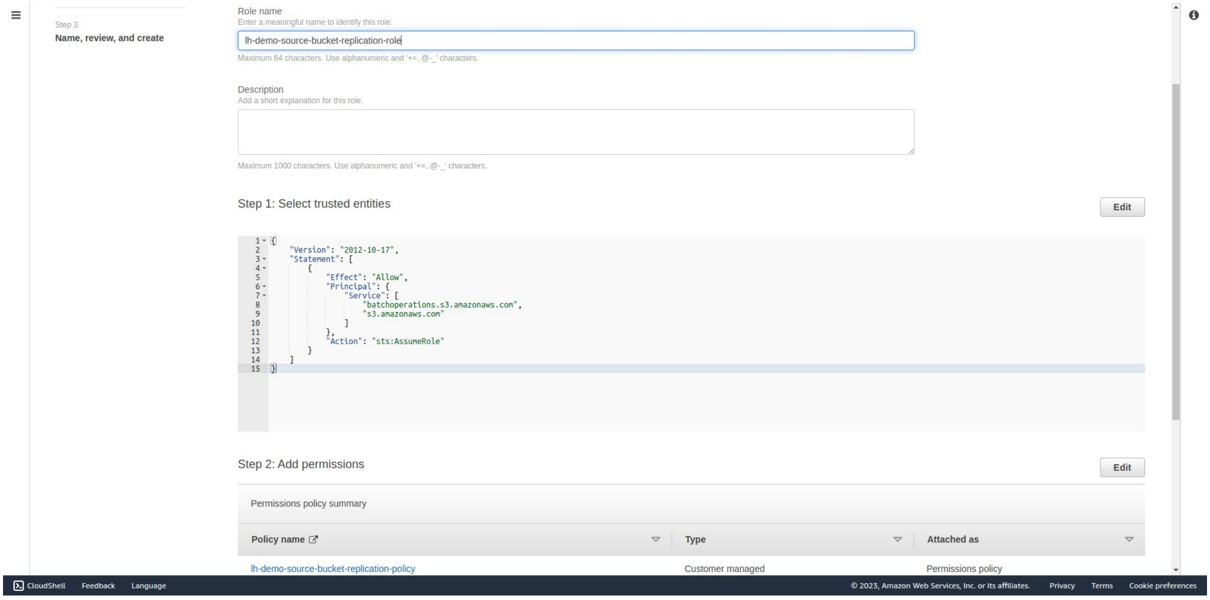
Add permissions Info

Permissions policies (Selected 1/860) Info

Choose one or more policies to attach to your new role.

	Policy name	Type	Description
☑	lh-demo-source-bucket-replication-policy	Custom...	
□	AdministratorAccess	AWS m...	Provides full access to AWS services and resources.
□	PowerUserAccess	AWS m...	Provides full access to AWS services and resources, but does not allow management of Users and groups.
□	ReadOnlyAccess	AWS m...	Provides read-only access to AWS services and resources.
□	AWSCloudFormationReadOnlyAccess	AWS m...	Provides access to AWS CloudFormation via the AWS Management Console.
□	CloudFrontFullAccess	AWS m...	Provides full access to the CloudFront console plus the ability to list Amazon S3 buckets via the AWS Management Console.
□	AWSCloudHSMFullAccess	AWS m...	Provides full access to all CloudHSM resources.
□	AWSCloudHSMReadOnlyAccess	AWS m...	Provides read only access to all CloudHSM resources.
□	ResourceGroupsandTagEditorFullAccess	AWS m...	Provides full access to Resource Groups and Tag Editor.
□	ResourceGroupsandTagEditorReadOnlyAccess	AWS m...	Provides access to use Resource Groups and Tag Editor, but does not allow editing of tags via the Tag Editor.
□	CloudFrontReadOnlyAccess	AWS m...	Provides access to CloudFront distribution configuration information and list distributions via the AWS Management Console.
□	CloudSearchFullAccess	AWS m...	Provides full access to the Amazon CloudSearch configuration service.
□	CloudSearchReadOnlyAccess	AWS m...	Provides read only access to the Amazon CloudSearch configuration service.
□	CloudWatchFullAccess	AWS m...	Provides full access to CloudWatch.

14. Give the IAM role name and click on "Create role" in the bottom right corner.



Step 3

Name, review, and create

Role name

Enter a meaningful name to identify this role.

lh-demo-source-bucket-replication-role

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description

Add a short explanation for this role.

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Step 1: Select trusted entities

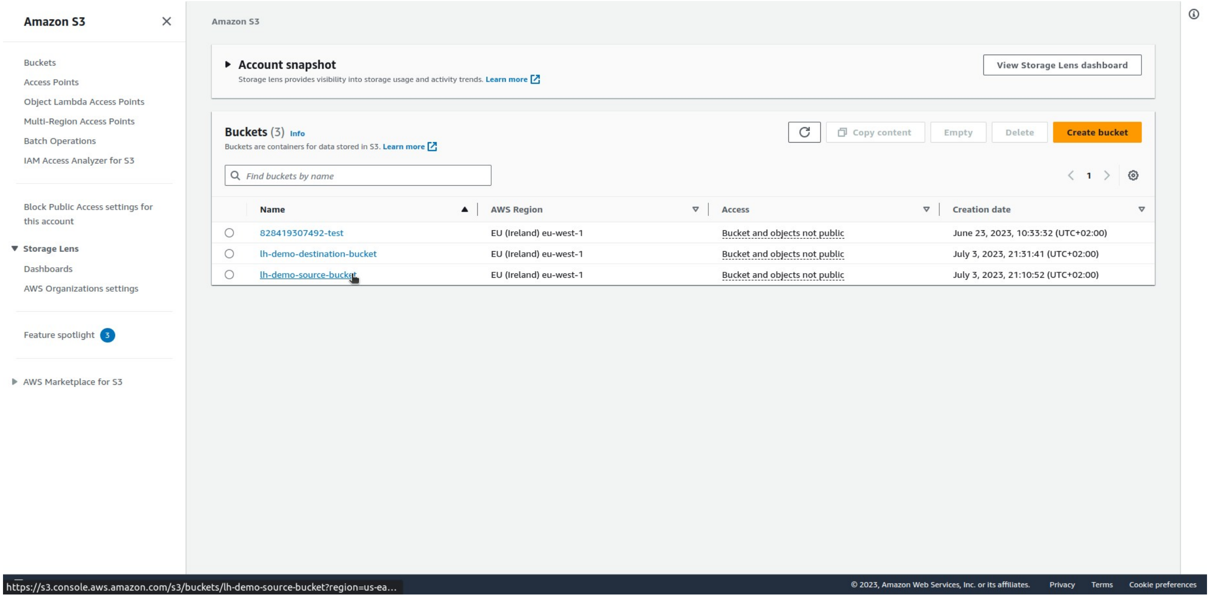
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "batchoperations.s3.amazonaws.com",
                    "s3.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
lh-demo-source-bucket-replication-policy	Customer managed	Permissions policy

15. Next, go back to the S3 buckets list and click on your source bucket name.



Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3

Account snapshot

Storage lens provides visibility into storage usage and activity trends. Learn more

View Storage Lens dashboard

Buckets (3) Info

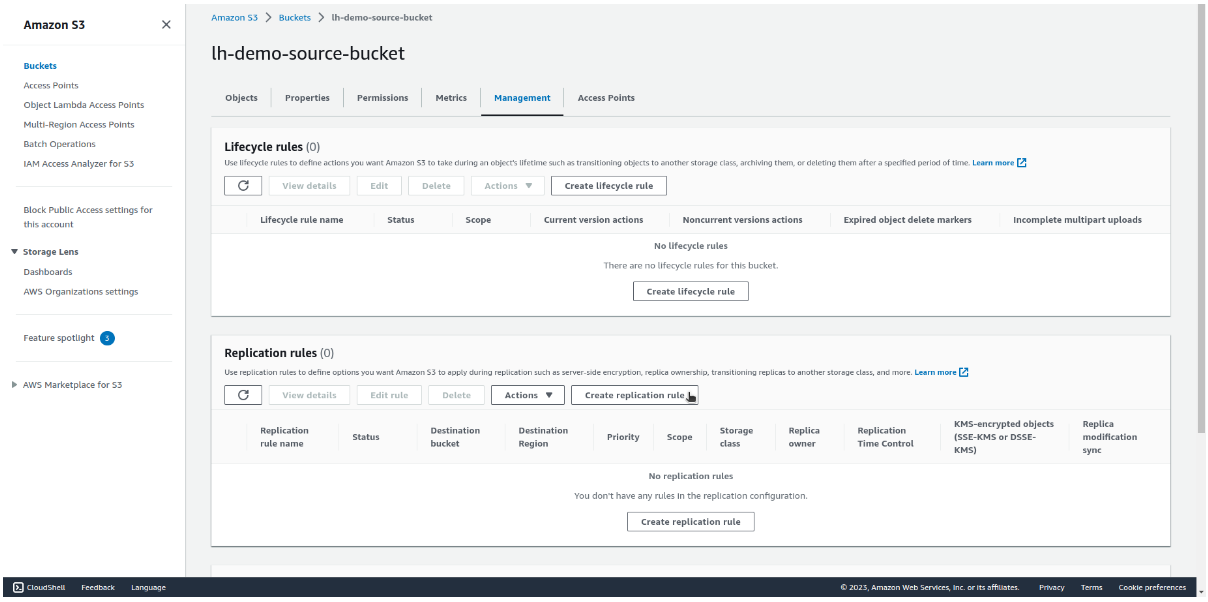
Buckets are containers for data stored in S3. Learn more

Copy content
Empty
Delete
Create bucket
Find buckets by name
1

Name	AWS Region	Access	Creation date
828419307492-test	EU (Ireland) eu-west-1	Bucket and objects not public	June 23, 2023, 10:33:32 (UTC+02:00)
lh-demo-destination-bucket	EU (Ireland) eu-west-1	Bucket and objects not public	July 3, 2023, 21:31:41 (UTC+02:00)
lh-demo-source-bucket	EU (Ireland) eu-west-1	Bucket and objects not public	July 3, 2023, 21:10:52 (UTC+02:00)

https://s3.console.aws.amazon.com/s3/buckets/lh-demo-source-bucket?region=us-ea...

16. In the "Management" tab, in the "Replication rules" section, click on "Create replication rule".



lh-demo-source-bucket

Lifecycle rules (0)

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 markers	Incomplete multipart uploads

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

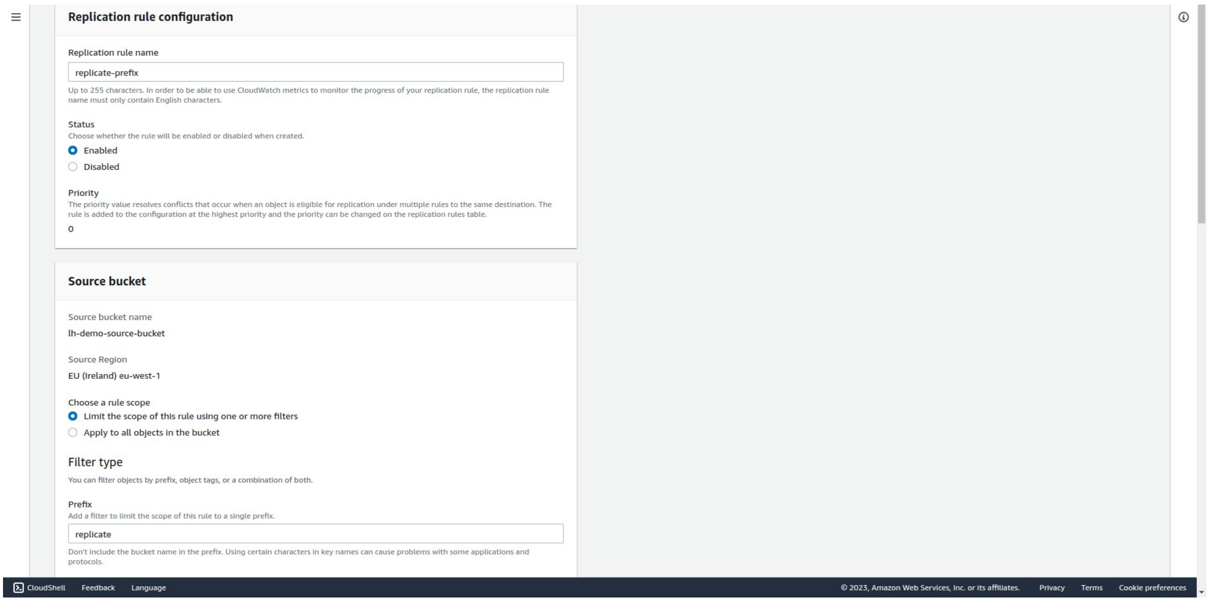
Replication rule name	Status	Destination bucket	Destination Region	Priority	Scope	Storage class	Replica owner	Replication Time Control	KMS-encrypted objects (SSE-KMS or DSSE-KMS)	Replica modification sync

No replication rules

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

© 2023, Amazon Web Services, Inc. or its affiliates.

17. Enter the rule ID, enter the specific prefix that you want to replicate in the "Source bucket" section, then choose the destination bucket in the "Destination" section.



Replication rule configuration

Replication rule name

replicate-prefix

Up to 255 characters. In order to be able to use CloudWatch metrics to monitor the progress of your replication rule, the replication rule name must only contain English characters.

Status

Choose whether the rule will be enabled or disabled when created.

● Enabled

○ Disabled

Priority

The priority value resolves conflicts that occur when an object is eligible for replication under multiple rules to the same destination. The rule is added to the configuration at the highest priority and the priority can be changed on the replication rules table.

0

Source bucket

Source bucket name

lh-demo-source-bucket

Source Region

EU (Ireland) eu-west-1

Choose a rule scope

● Limit the scope of this rule using one or more filters

○ Apply to all objects in the bucket

Filter type

You can filter objects by prefix, object tags, or a combination of both.

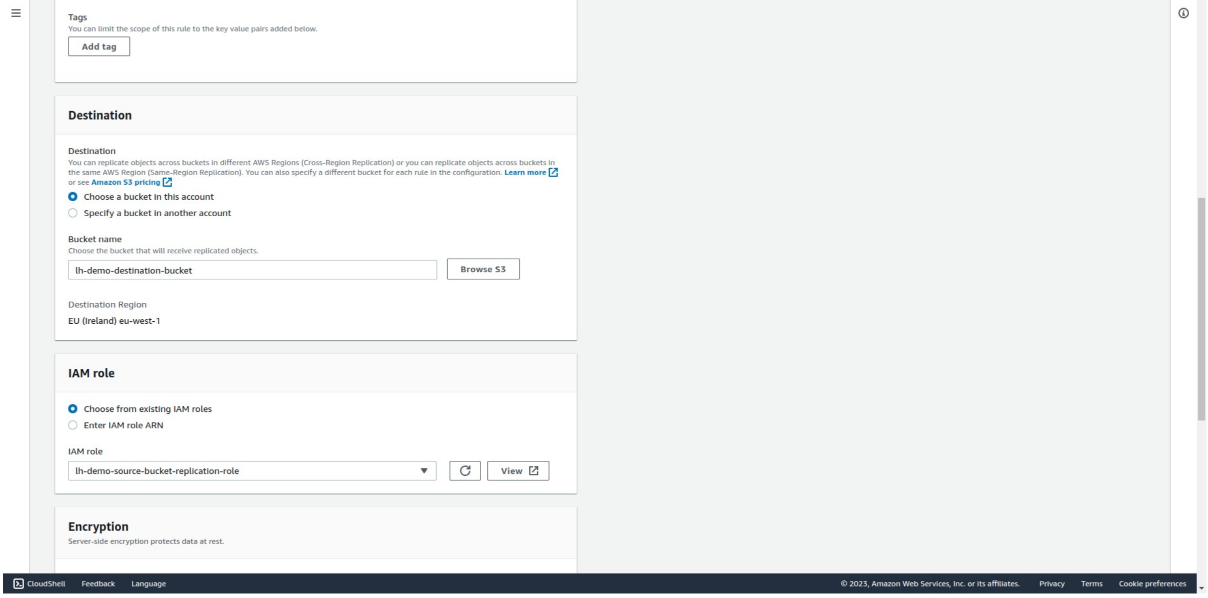
Prefix

Add a filter to limit the scope of this rule to a single prefix.

replicate

Don't include the bucket name in the prefix. Using certain characters in key names can cause problems with some applications and protocols.

© 2023, Amazon Web Services, Inc. or its affiliates.



Tags
You can limit the scope of this rule to the key value pairs added below.

Destination

Destination
You can replicate objects across buckets in different AWS Regions (Cross-Region Replication) or you can replicate objects across buckets in the same AWS Region (Same-Region Replication). You can also specify a different bucket for each rule in the configuration. Learn more or see Amazon S3 pricing

● Choose a bucket in this account
○ Specify a bucket in another account

Bucket name
Choose the bucket that will receive replicated objects.
lh-demo-destination-bucket

Destination Region
EU (Ireland) eu-west-1

IAM role

● Choose from existing IAM roles
○ Enter IAM role ARN

IAM role
lh-demo-source-bucket-replication-role

Encryption
Server-side encryption protects data at rest.

© 2023, Amazon Web Services, Inc. or its affiliates.

18. In the "IAM role" section, choose the previously created IAM role.

19. Choose additional replication options as per your needs and click on "Save".

20. If You want to replicate existing files select “Yes, replicate existing objects.” in the pop-up window and click on “Submit”.

21. Choose the path in S3 bucket for completion report or disable this option. Leave the rest of the settings default and click on “Save”.

22. Repeat steps 16-21 for every prefix that You want to replicate.