Project in AWS
Practice Lab

Create and Assume Roles in AWS

Andra-Diana Popescu

2023

ABOUT THIS LAB

AWS Identity and Access Management (IAM) is a service that allows AWS customers to manage user access and permissions for the accounts and available APIs/services within AWS. IAM can manage users, security credentials (such as API access keys), and allow users to access AWS resources.

In this lab, we discover how security policies affect IAM users and groups, and we go further by implementing our own policies while also learning what a role is, how to create a role, and how to assume a role as a different user. An IAM role is similar to an IAM user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have standard long-term credentials such as a password or access keys associated with it. Instead, when you assume a role, it provides you with temporary security credentials for your role session.

By the end of this lab, you will understand IAM policies and roles, and how assuming roles can assist in restricting users to specific AWS resources.

LEARNING OBJECTIVES

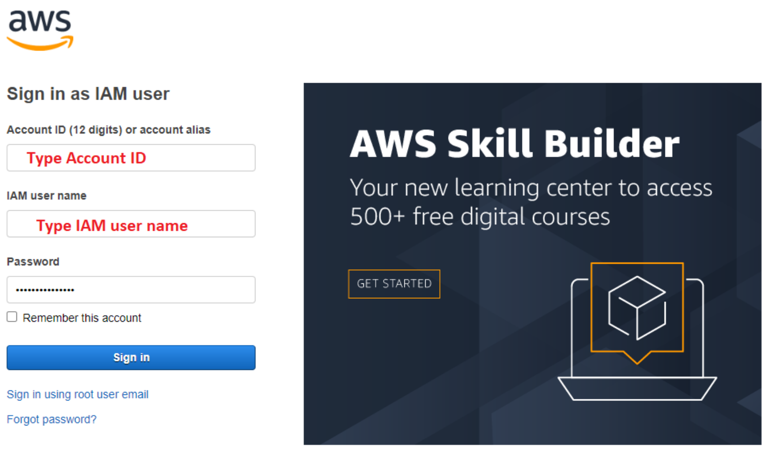
- Create the Correct S3 Restricted Policies and Roles
- Configure IAM So the dev3 User Can Assume the Role

AWS Documentation about IAM roles:
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html

Source: https://learn.acloud.guru/course/certified-solutions-architect-associate/

Table of Contents

Log in to your AWS account



Sign in as IAM user

Account ID (12 digits) or account alias

Type Account ID

IAM user name

Type IAM user name

Password

················

□ Remember this account

Sign in

Sign in using root user email

Forgot password?

AWS Skill Builder

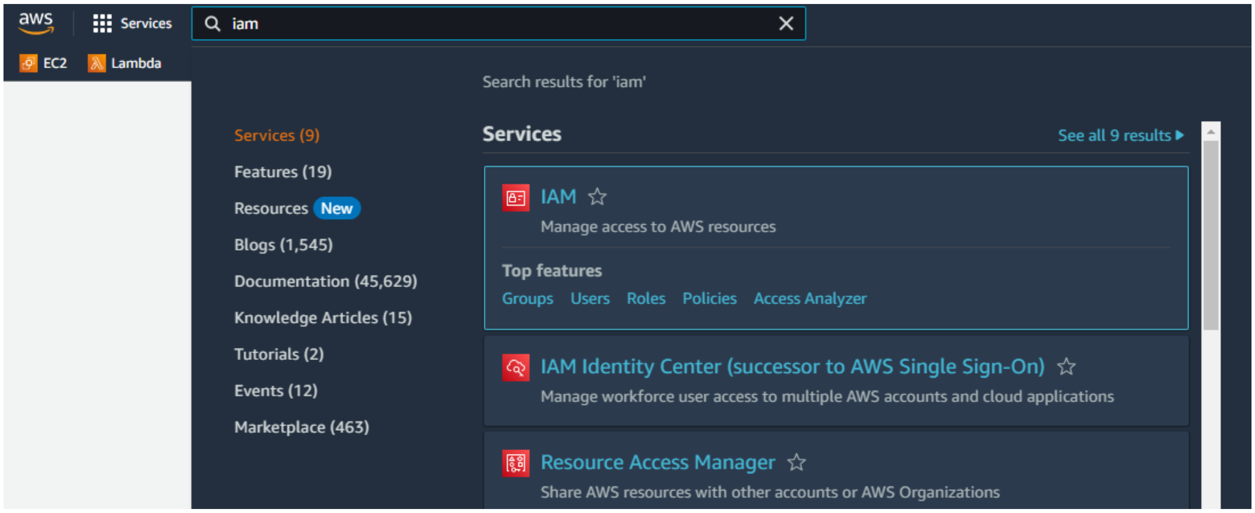
Your new learning center to access 500+ free digital courses

GET STARTED

1. Create the Correct S3 Restricted Policies and Roles

1.1. Create the S3RestrictedPolicy

1. Once you are logged in to the AWS Management Console, navigate to IAM.



iam

Search results for 'iam'

Services

See all 9 results

IAM

Manage access to AWS resources

Top features

Groups Users Roles Policies Access Analyzer

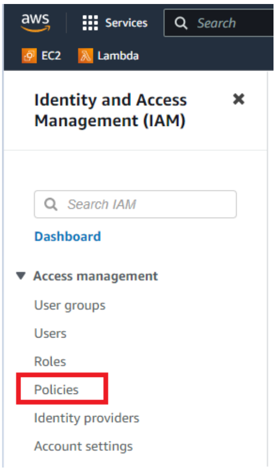
IAM Identity Center (successor to AWS Single Sign-On)

Manage workforce user access to multiple AWS accounts and cloud applications

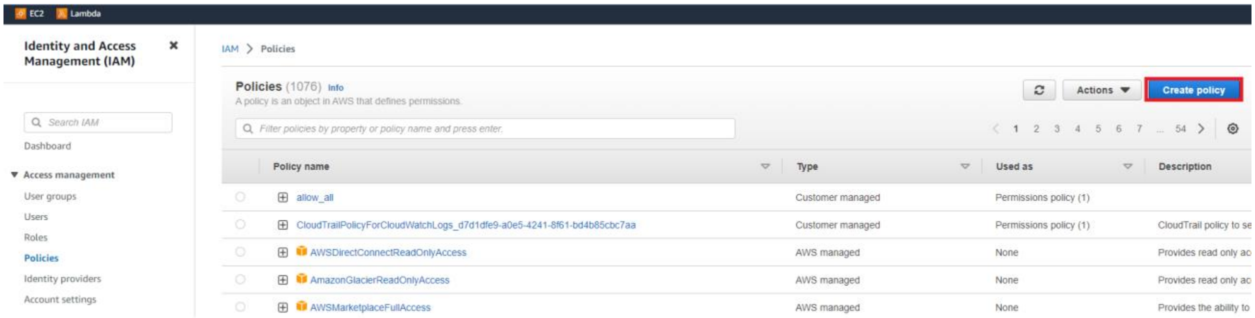
Resource Access Manager

Share AWS resources with other accounts or AWS Organizations

2. From the left-side menu, click **Policies**.



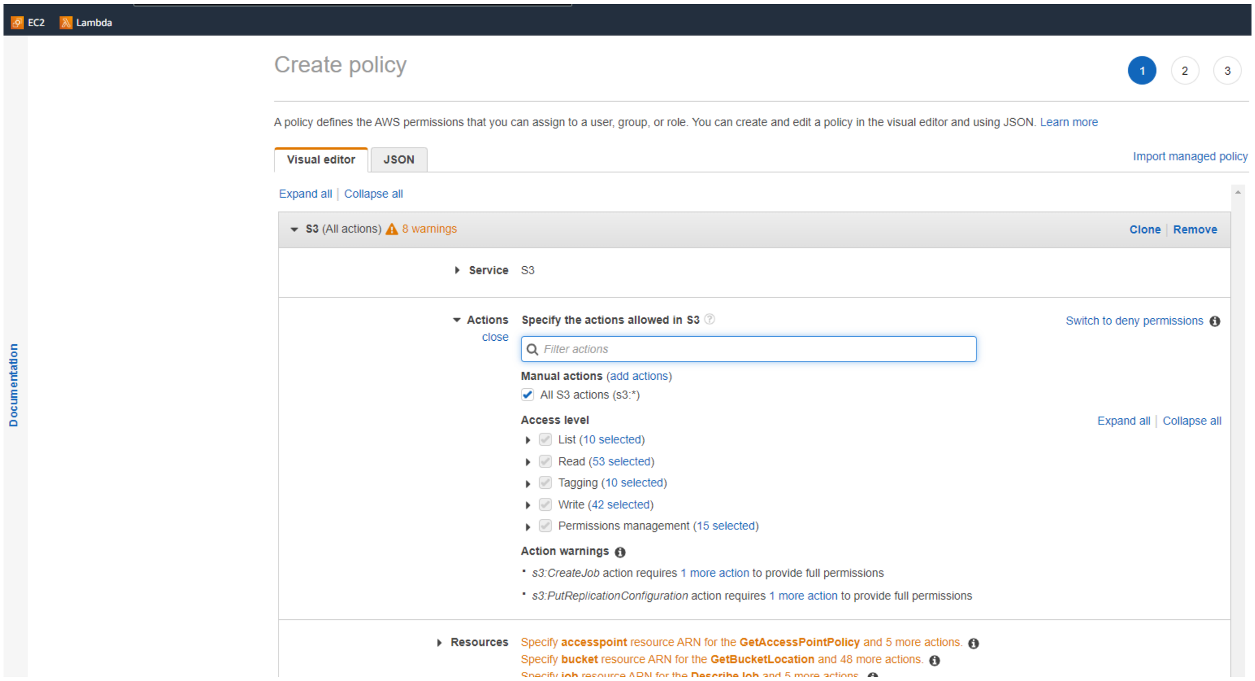
3. Click **Create Policy**.



Policies (1076)
A policy is an object in AWS that defines permissions.

Policy name	Type	Used as	Description
allow_all	Customer managed	Permissions policy (1)	
CloudTrailPolicyForCloudWatchLogs_d7d1dfe9-a0e5-4241-8f61-bd4b85cbc7aa	Customer managed	Permissions policy (1)	CloudTrail policy to se
AWSDirectConnectReadOnlyAccess	AWS managed	None	Provides read only ac
AmazonGlacierReadOnlyAccess	AWS managed	None	Provides read only ac
AWSMarketplaceFullAccess	AWS managed	None	Provides the ability to

4. In Service, click **Choose a service**.
5. Type and select **S3**.
6. In Actions, select **All S3 actions**.



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 (All actions) ⚠ 8 warnings

Service S3

Actions Specify the actions allowed in S3

Manual actions (add actions)

☑ All S3 actions (s3:*)

Access level

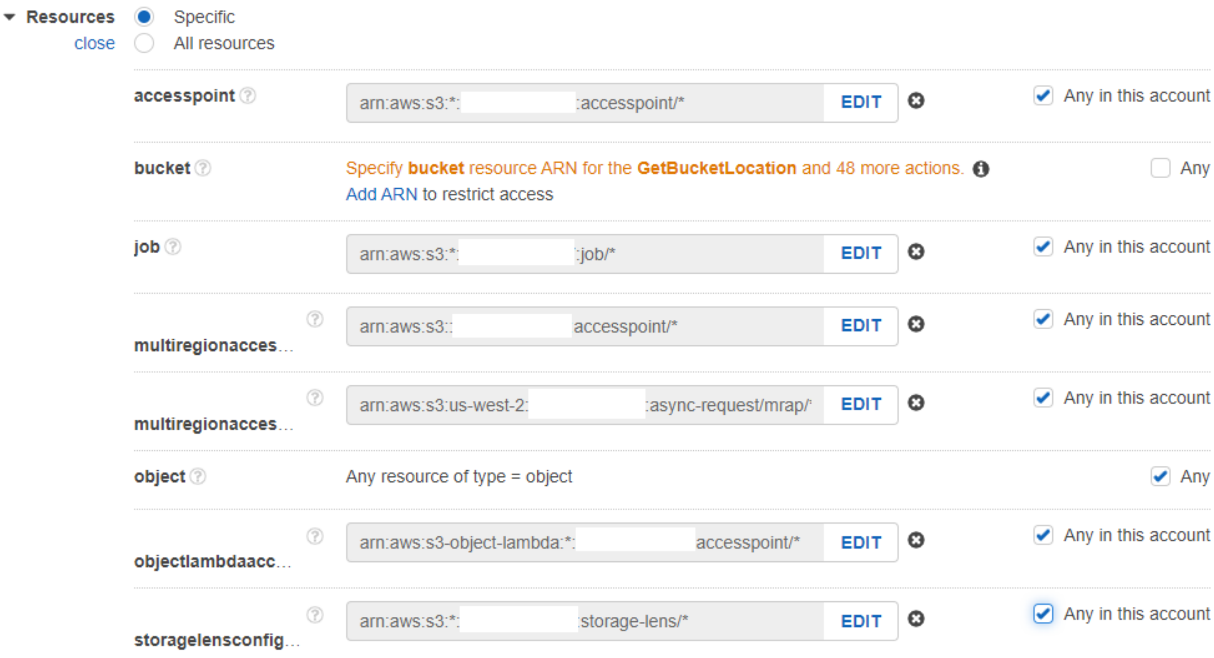
- ☑ List (10 selected)
- ☑ Read (53 selected)
- ☑ Tagging (10 selected)
- ☑ Write (42 selected)
- ☑ Permissions management (15 selected)

Action warnings

- *s3:CreateJob* action requires 1 more action to provide full permissions
- *s3:PutReplicationConfiguration* action requires 1 more action to provide full permissions

Resources Specify **accesspoint** resource ARN for the **GetAccessPointPolicy** and 5 more actions.
Specify **bucket** resource ARN for the **GetBucketLocation** and 48 more actions.
Specify **job** resource ARN for the **DescribeJob** and 5 more actions.

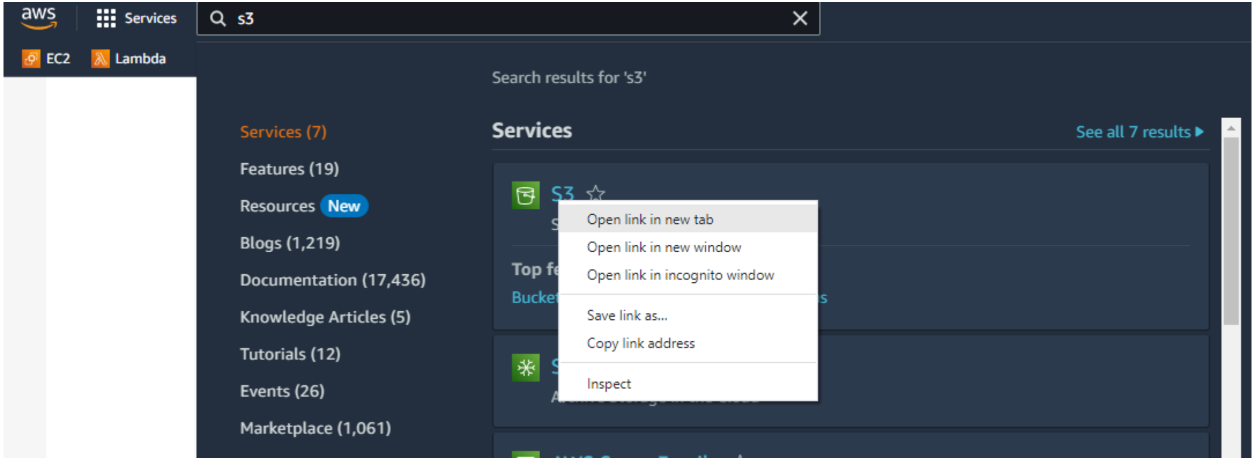
7. Click the arrow next to *Resources*, and select **Any** or **Any in this account** for all resources other than bucket.



▾ **Resources** ● Specific
close ○ All resources

accesspoint	arn:aws:s3:*:[redacted]:accesspoint/* EDIT	⊗	☑ Any in this account
bucket	Specify **bucket** resource ARN for the **GetBucketLocation** and 48 more actions. Add ARN to restrict access		☐ Any
job	arn:aws:s3:*:[redacted]:job/* EDIT	⊗	☑ Any in this account
multiregionacces…	arn:aws:s3::[redacted]accesspoint/* EDIT	⊗	☑ Any in this account
multiregionacces…	arn:aws:s3:us-west-2:[redacted]:async-request/mrap/* EDIT	⊗	☑ Any in this account
object	Any resource of type = object		☑ Any
objectlambdaacc…	arn:aws:s3-object-lambda:*:[redacted]accesspoint/* EDIT	⊗	☑ Any in this account
storagelensconfig…	arn:aws:s3:*:[redacted]:storage-lens/* EDIT	⊗	☑ Any in this account

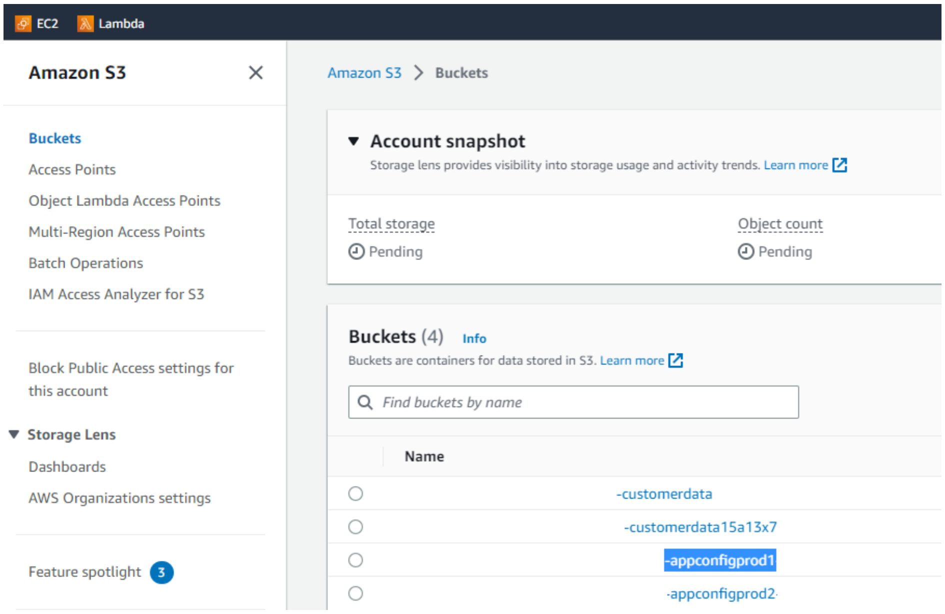
8. Open a new browser tab, and navigate to S3.



s3

Search results for 's3'

9. Under *Buckets*, copy the bucket name containing **appconfigprod1.**


EC2
Lambda
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
Amazon S3 > Buckets

Account snapshot

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

Total storage: Pending

Object count: Pending

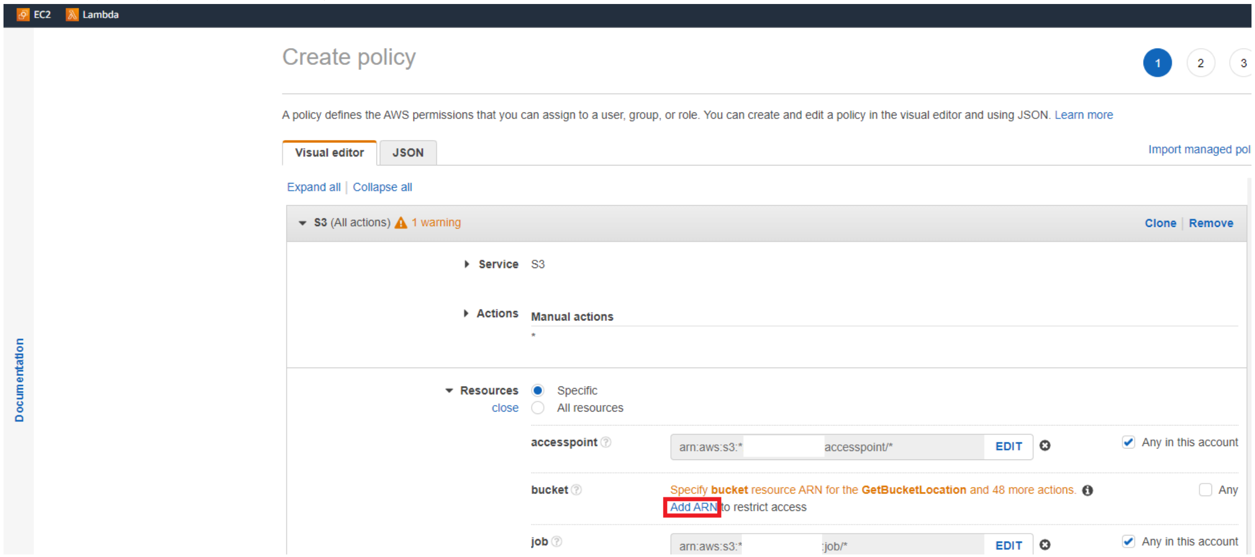
Buckets (4) Info

Buckets are containers for data stored in S3. Learn more

Find buckets by name

	Name
○	-customerdata
○	-customerdata15a13x7
○	-appconfigprod1
○	-appconfigprod2-

10. Return to IAM.
11. In *Resources*, under bucket, click **Add ARN**.



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 (All actions) ⚠ 1 warning

Service: S3

Actions: Manual actions *

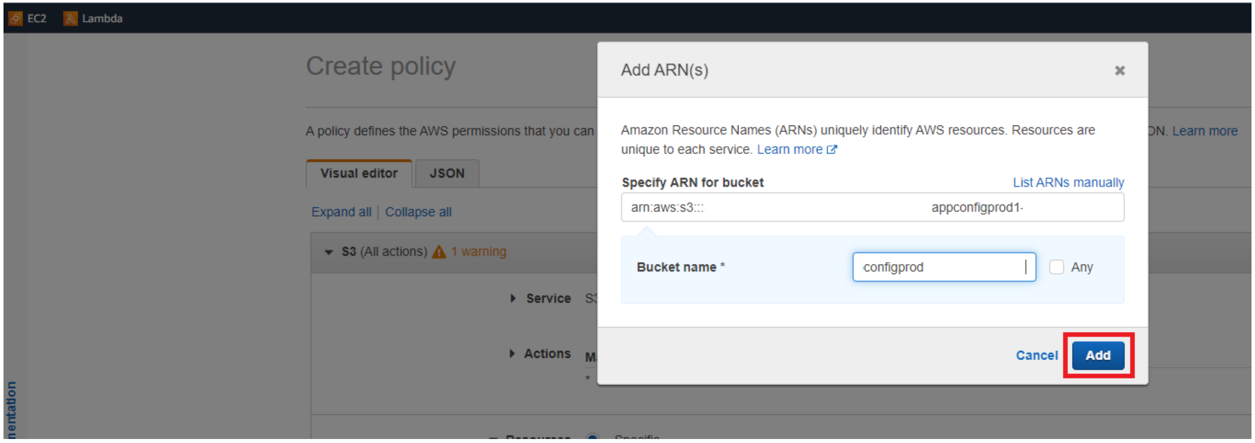
Resources (close): ● Specific ○ All resources

accesspoint: arn:aws:s3:* accesspoint/* EDIT ☑ Any in this account

bucket: Specify **bucket** resource ARN for the **GetBucketLocation** and 48 more actions. Add ARN to restrict access □ Any

job: arn:aws:s3:* job/* EDIT ☑ Any in this account

12. Paste in the *Bucket name* you just copied and click **Add**.



Add ARN(s)

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more

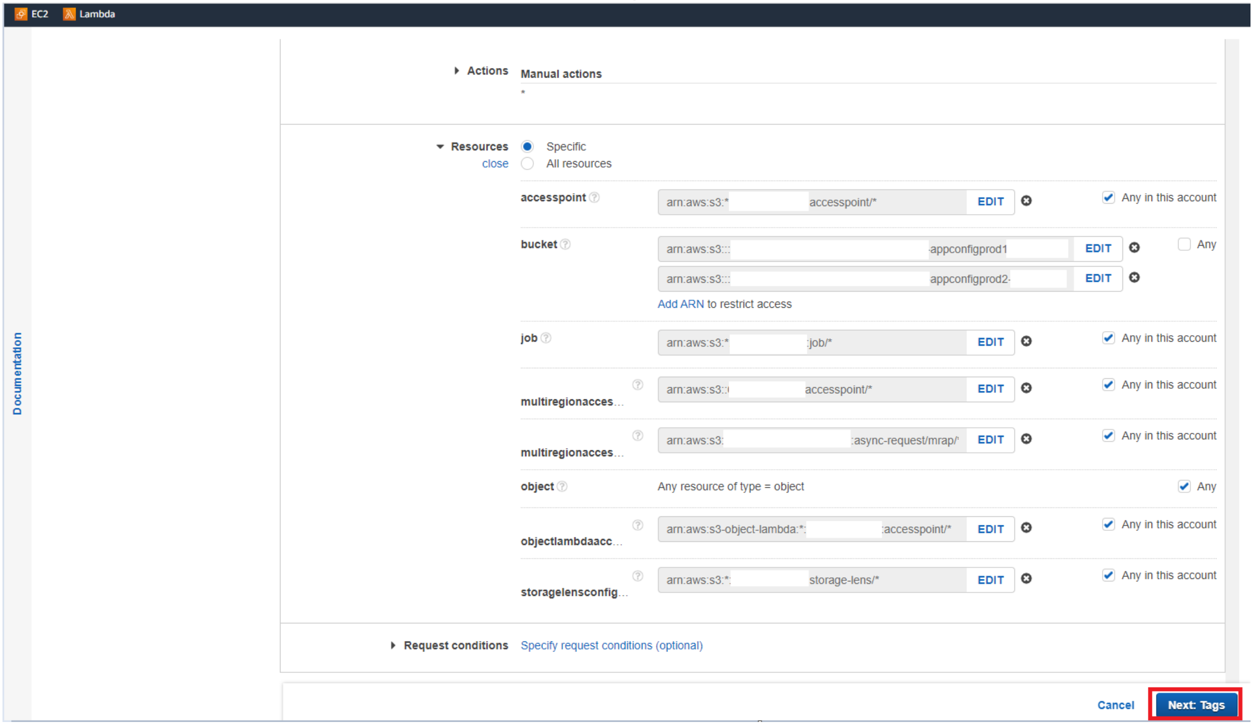
Specify ARN for bucket — List ARNs manually

arn:aws:s3::: appconfigprod1-

Bucket name *: configprod □ Any

Cancel **Add**

13. Return to S3 and repeat the process with the bucket name containing **appconfigprod2**.
14. In IAM, once both buckets are added, click **Next: Tags**.



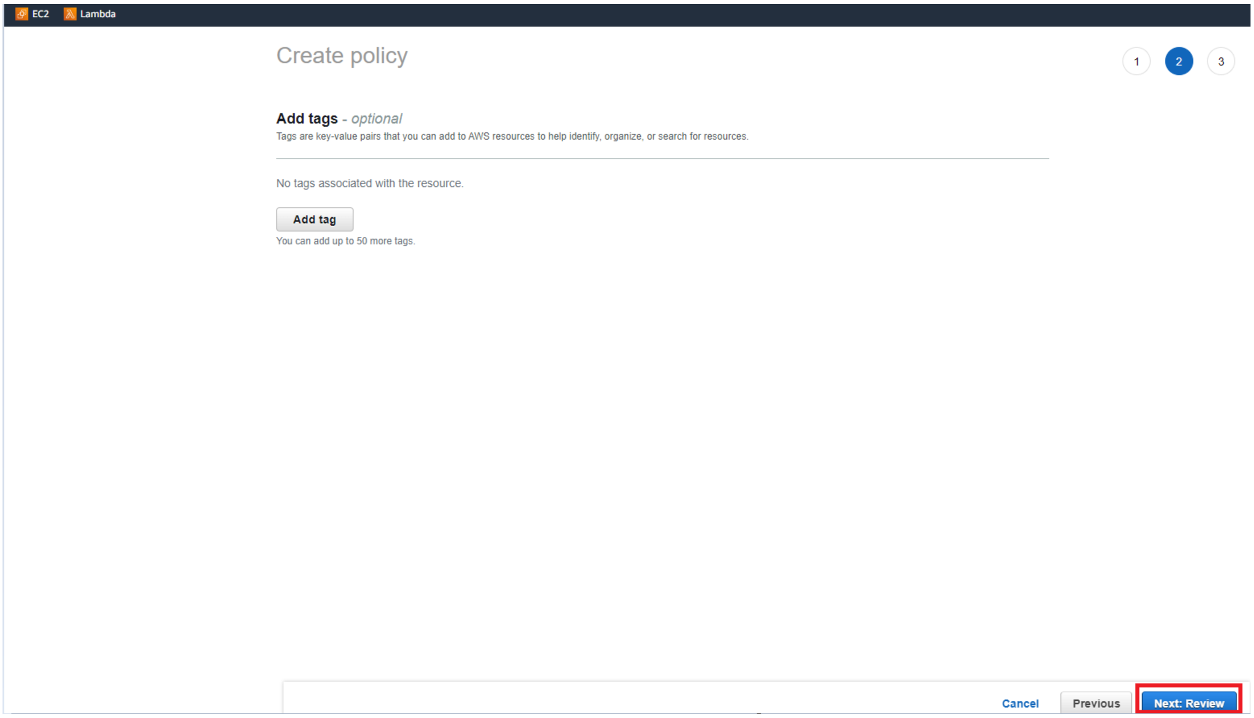
Actions — Manual actions
*

Resources ● Specific ○ All resources
close

accesspoint	arn:aws:s3:* accesspoint/*	EDIT	☑ Any in this account
bucket	arn:aws:s3::: appconfigprod1	EDIT	□ Any
	arn:aws:s3::: appconfigprod2-	EDIT	
	Add ARN to restrict access		
job	arn:aws:s3:* job/*	EDIT	☑ Any in this account
multiregionacces...	arn:aws:s3:: accesspoint/*	EDIT	☑ Any in this account
multiregionacces...	arn:aws:s3: :async-request/mrap/	EDIT	☑ Any in this account
object	Any resource of type = object		☑ Any
objectlambdaacc...	arn:aws:s3-object-lambda:*: :accesspoint/*	EDIT	☑ Any in this account
storagelensconfig...	arn:aws:s3:*: storage-lens/*	EDIT	☑ Any in this account

Request conditions — Specify request conditions (optional)

15. Click **Next: Review**.



Create policy

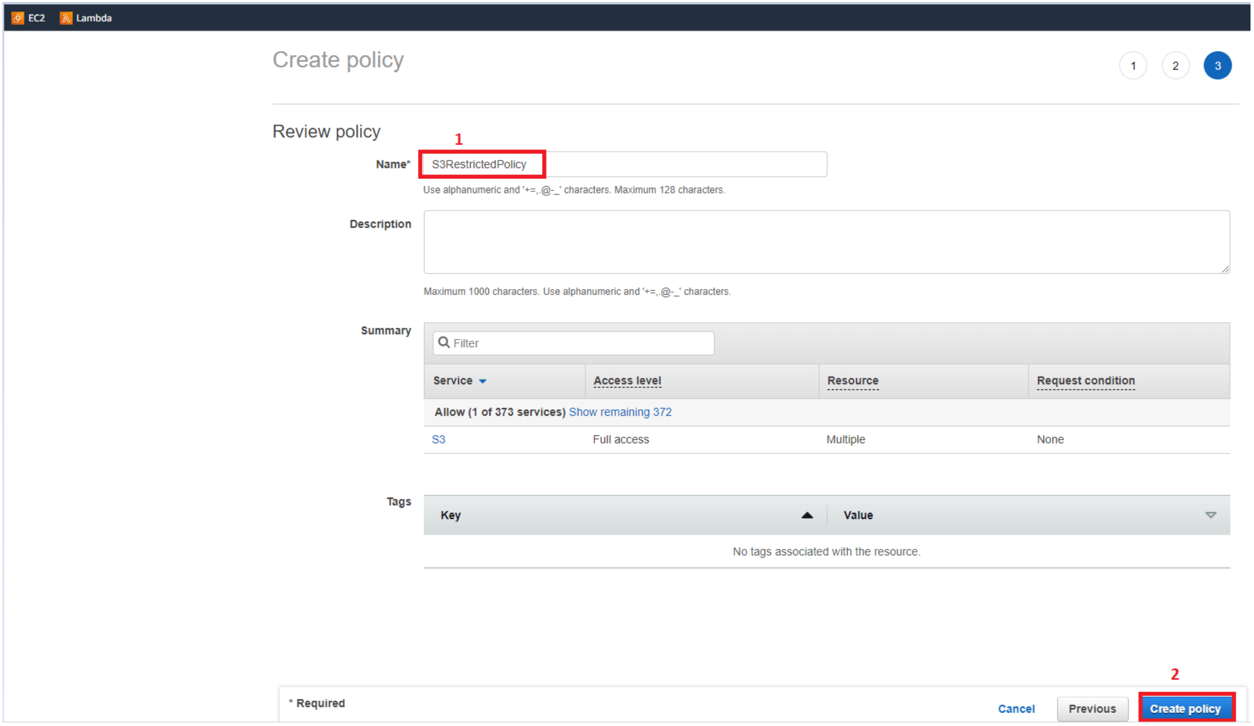
Add tags - *optional*

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.

16. For Name, enter "S3RestrictedPolicy", and click **Create policy**.



Create policy

Review policy

Name* S3RestrictedPolicy

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

Description

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

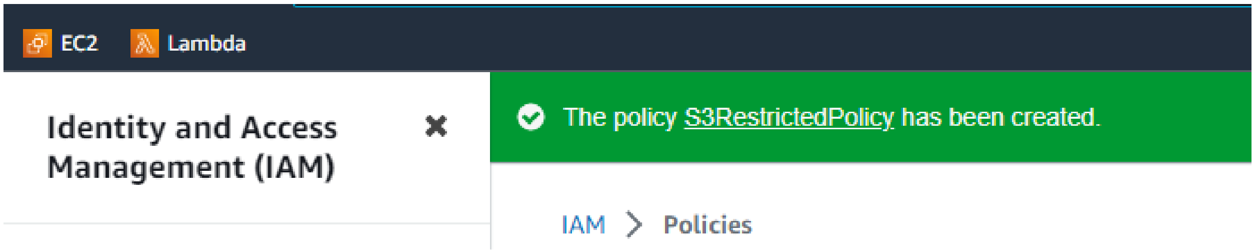
Summary

Service	Access level	Resource	Request condition
Allow (1 of 373 services) Show remaining 372			
S3	Full access	Multiple	None

Tags

Key	Value
No tags associated with the resource.	

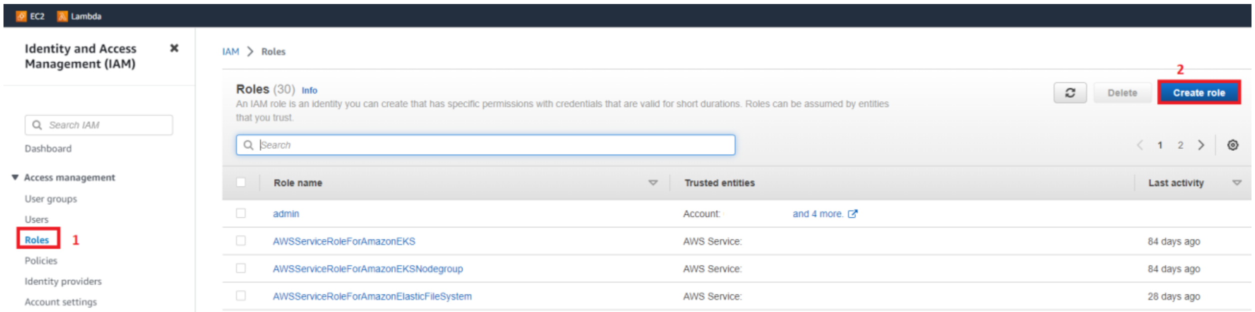
* Required



The policy S3RestrictedPolicy has been created.

1.2. Create the S3RestrictedRole

1. From the IAM dashboard menu, select **Roles**.
2. Click **Create role**.

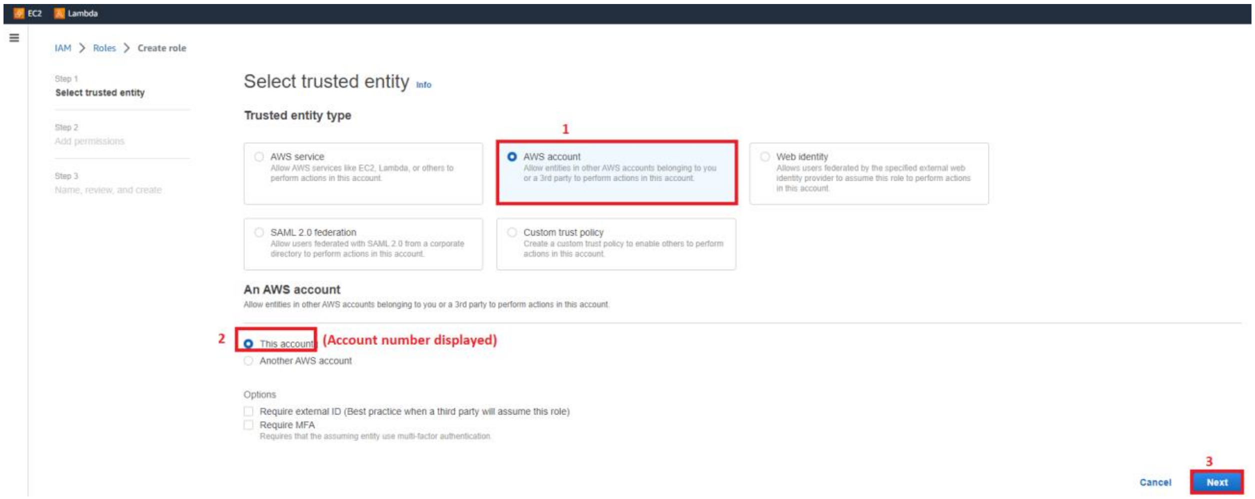


Roles (30) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities	Last activity
admin	Account: and 4 more.	
AWSServiceRoleForAmazonEKS	AWS Service:	84 days ago
AWSServiceRoleForAmazonEKSNodegroup	AWS Service:	84 days ago
AWSServiceRoleForAmazonElasticFileSystem	AWS Service:	28 days ago

3. Under *Trusted entity type*, select **AWS account**.
4. Under the *AWS account* section that pops up, make sure **This account** is selected.
5. Copy the account number next to *This account*. You will need this later in the lab.
6. Click **Next**.



Select trusted entity

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.

An AWS account

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

● This account (Account number displayed)

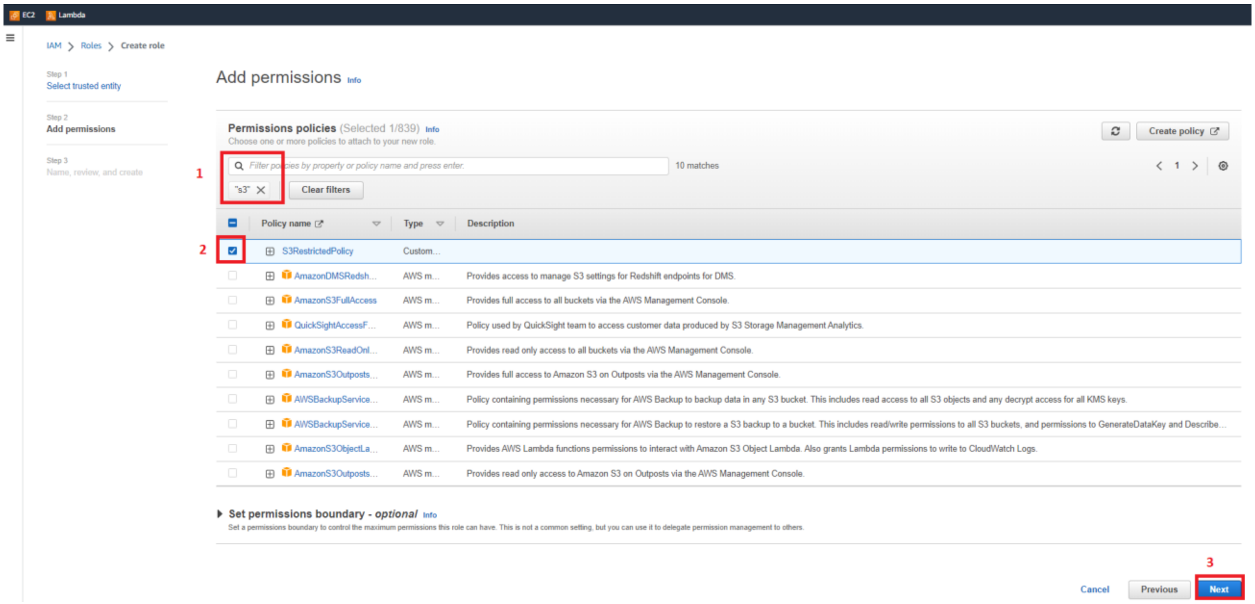
○ Another AWS account

Options

□ Require external ID (Best practice when a third party will assume this role)

□ Require MFA
Requires that the assuming entity use multi-factor authentication.

7. In the search field, enter "S3" and select **S3RestrictedPolicy**.
8. Click **Next**.



Add permissions

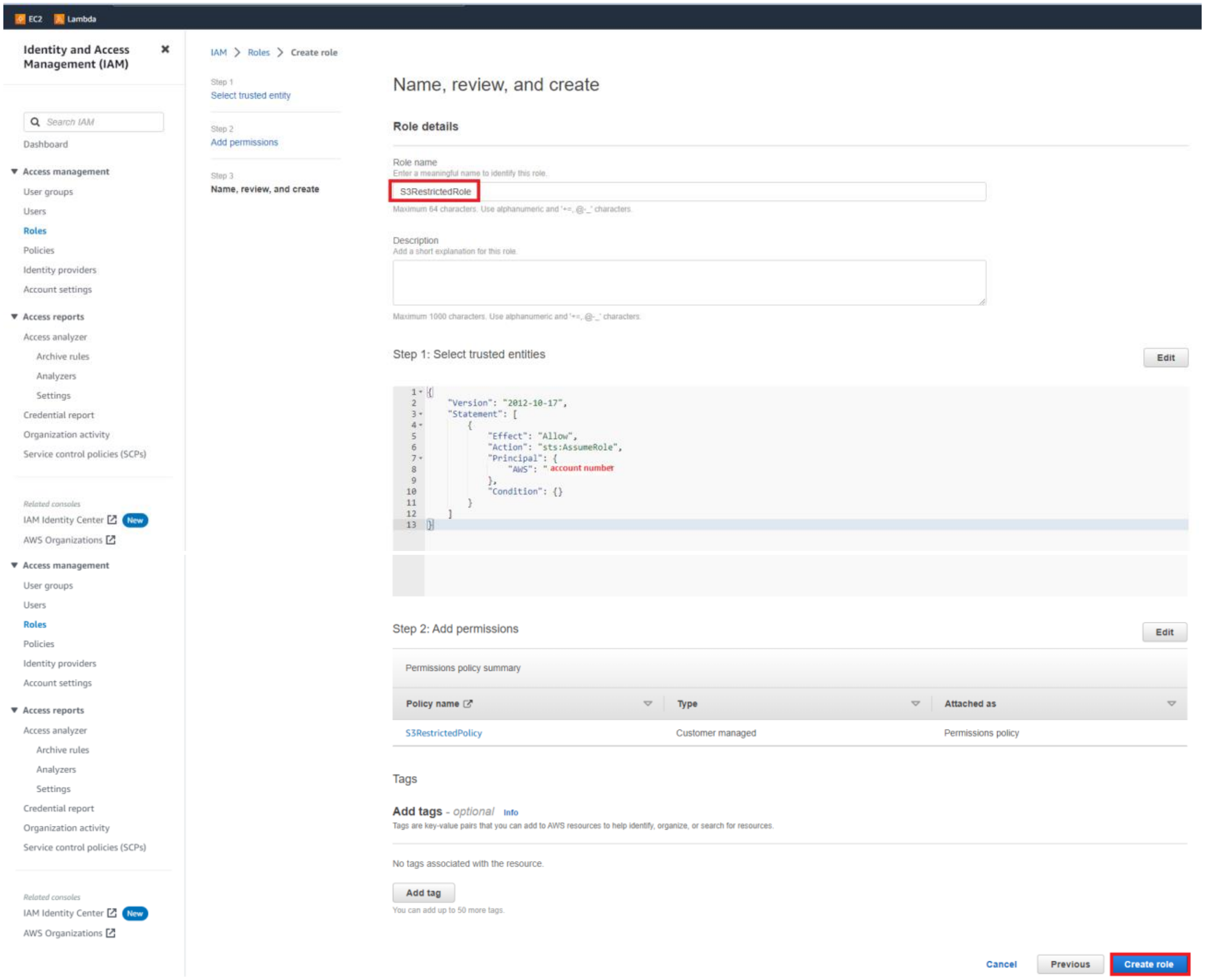
Permissions policies (Selected 1/839)
Choose one or more policies to attach to your new role.

Filter policies by property or policy name and press enter. "s3" ✕ 10 matches

	Policy name	Type	Description
☑	S3RestrictedPolicy	Custom...	
□	AmazonDMSRedsh...	AWS m...	Provides access to manage S3 settings for Redshift endpoints for DMS.
□	AmazonS3FullAccess	AWS m...	Provides full access to all buckets via the AWS Management Console.
□	QuickSightAccessF...	AWS m...	Policy used by QuickSight team to access customer data produced by S3 Storage Management Analytics.
□	AmazonS3ReadOnl...	AWS m...	Provides read only access to all buckets via the AWS Management Console.
□	AmazonS3Outposts...	AWS m...	Provides full access to Amazon S3 on Outposts via the AWS Management Console.
□	AWSBackupService...	AWS m...	Policy containing permissions necessary for AWS Backup to backup data in any S3 bucket. This includes read access to all S3 objects and any decrypt access for all KMS keys.
□	AWSBackupService...	AWS m...	Policy containing permissions necessary for AWS Backup to restore a S3 backup to a bucket. This includes read/write permissions to all S3 buckets, and permissions to GenerateDataKey and Describe...
□	AmazonS3ObjectLa...	AWS m...	Provides AWS Lambda functions permissions to interact with Amazon S3 Object Lambda. Also grants Lambda permissions to write to CloudWatch Logs.
□	AmazonS3Outposts...	AWS m...	Provides read only access to Amazon S3 on Outposts via the AWS Management Console.

▸ Set permissions boundary - *optional*
Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

9. In Role name, enter "S3RestrictedRole". You should see in the JSON block that the trusted entity is your account number. This means that anything that is in this account can assume this role.
10. Click Create role.



Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
S3RestrictedRole
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",
            "Action": "sts:AssumeRole",
            "Principal": {
                "AWS": " account number
            },
            "Condition": {}
        }
    ]
}
```

Step 2: Add permissions

Permissions policy summary

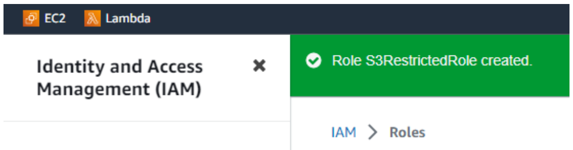
Policy name	Type	Attached as
S3RestrictedPolicy	Customer managed	Permissions policy

Tags

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.

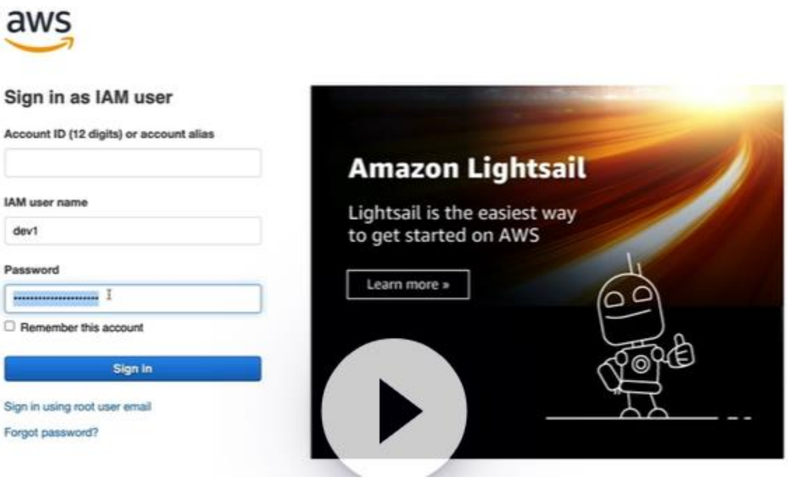
Add tag
You can add up to 50 more tags.



Role S3RestrictedRole created.

1.3. Revoke the S3 Administrator Access Policy to the dev1 User

1. AWS now auto logs out when logging in as another user (even if in a new Incognito/Private Window). As a work around, you can right-click the lab's blue “Open Link in Incognito/Private Window” button and copy the link into a different browser. You'll then be able to be logged into the other account using the lab provided credentials.
2. Use the following credentials to log in:
   Account ID: The same account ID
   User: dev1
   Password:



Sign in as IAM user

Account ID (12 digits) or account alias

IAM user name

dev1

Password

••••••••••••••••••••••

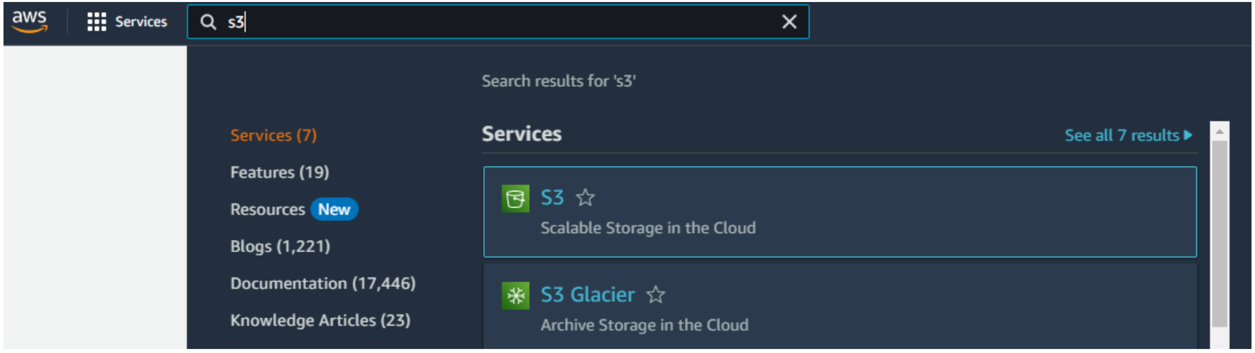
□ Remember this account

Sign in

Sign in using root user email

Forgot password?

3. Navigate to S3 to see what this user has access to.



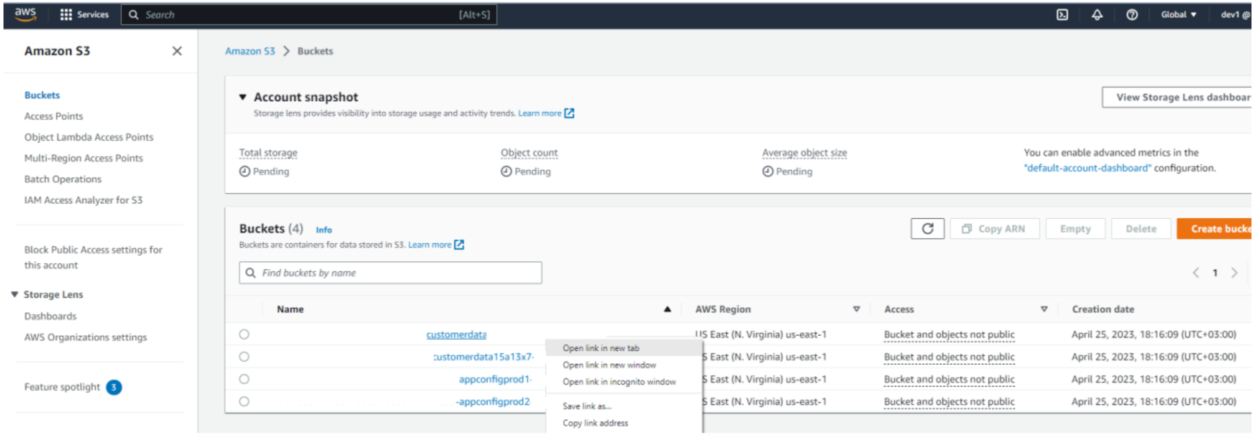
s3

Search results for 's3'

S3 ☆ Scalable Storage in the Cloud

S3 Glacier ☆ Archive Storage in the Cloud

4. Select one of the **customerdata** buckets and open it in a new tab. You should see that there are no objects, but you do have access to it.



▼ Account snapshot

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

Total storage: Pending

Object count: Pending

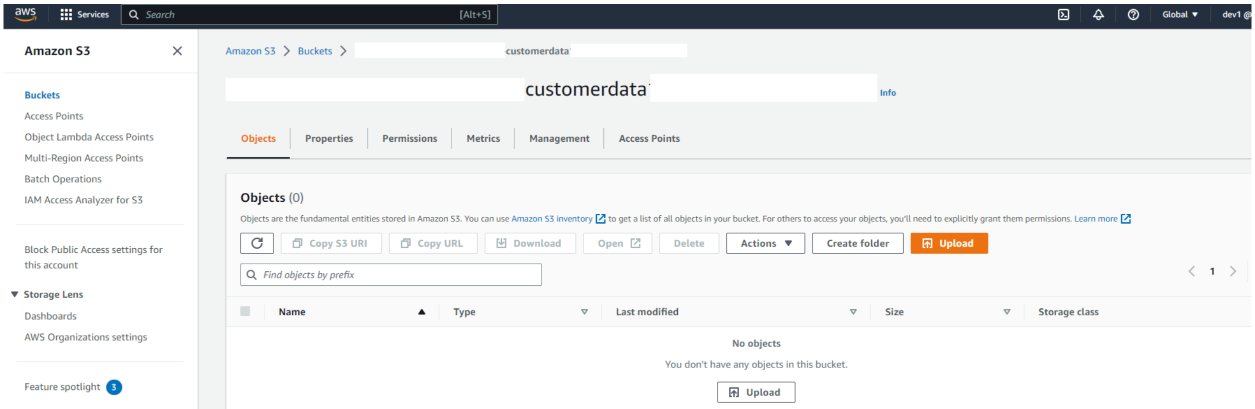
Average object size: Pending

You can enable advanced metrics in the "default-account-dashboard" configuration.

Buckets (4)

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	customerdata	US East (N. Virginia) us-east-1	Bucket and objects not public	April 25, 2023, 18:16:09 (UTC+03:00)
○	customerdata15a13x7-	S East (N. Virginia) us-east-1	Bucket and objects not public	April 25, 2023, 18:16:09 (UTC+03:00)
○	appconfigprod1-	S East (N. Virginia) us-east-1	Bucket and objects not public	April 25, 2023, 18:16:09 (UTC+03:00)
○	-appconfigprod2-	S East (N. Virginia) us-east-1	Bucket and objects not public	April 25, 2023, 18:16:09 (UTC+03:00)



[redacted]customerdata[redacted]

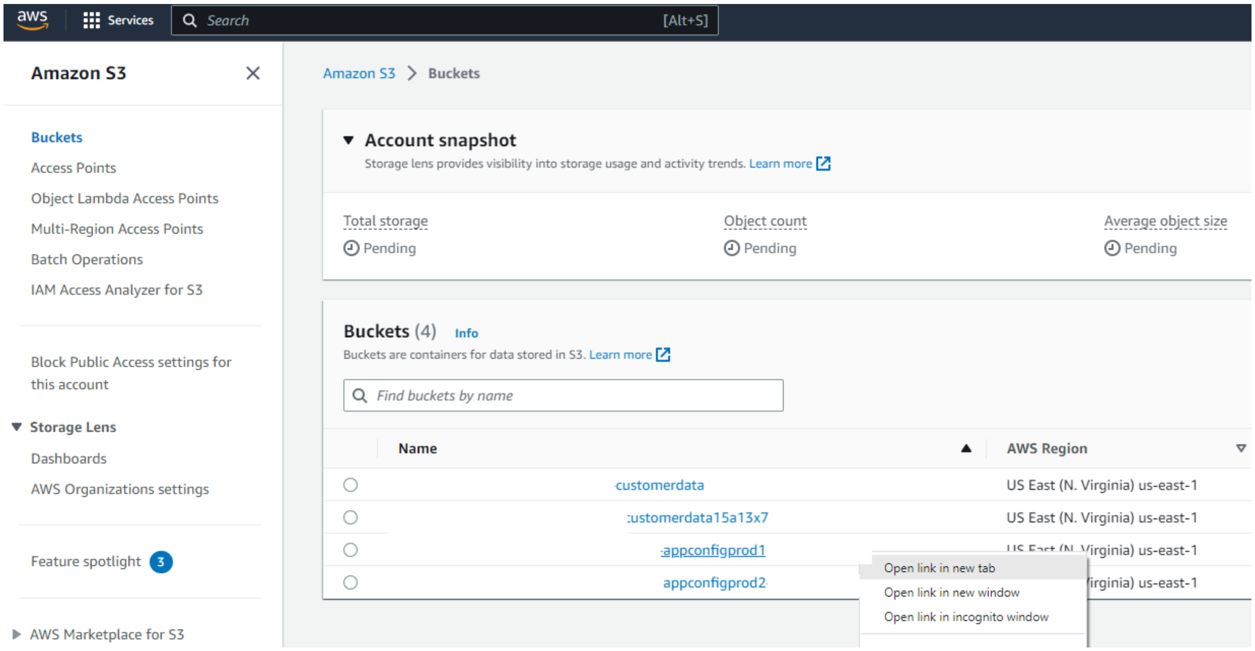
Objects (0)

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

No objects

You don't have any objects in this bucket.

5. Back in S3, select one of the **appconfig** buckets, and open it in a new tab. You should see the same access as the **customerdata** bucket.



▼ Account snapshot

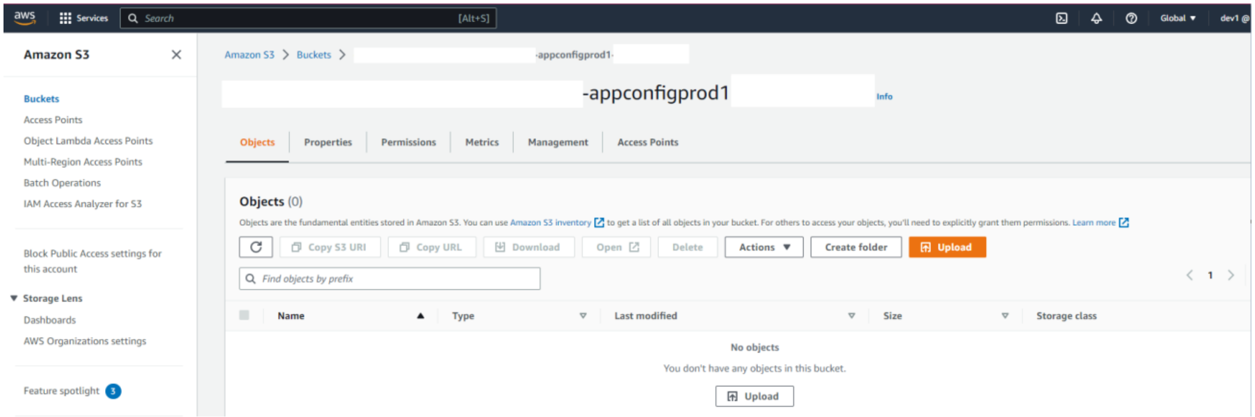
Storage lens provides visibility into storage usage and activity trends. Learn more

Total storage	Object count	Average object size
Pending	Pending	Pending

Buckets (4) Info

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region
○	[redacted]customerdata	US East (N. Virginia) us-east-1
○	[redacted]customerdata15a13x7	US East (N. Virginia) us-east-1
○	[redacted]appconfigprod1	US East (N. Virginia) us-east-1
○	[redacted]appconfigprod2	US East (N. Virginia) us-east-1



[redacted]-appconfigprod1[redacted]

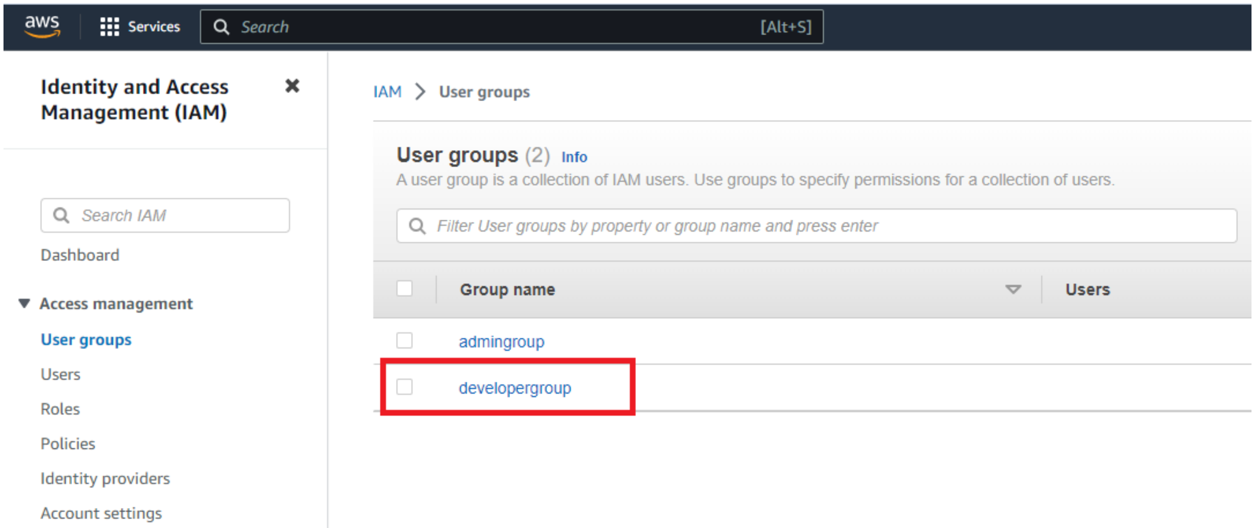
Objects (0)

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

No objects

You don't have any objects in this bucket.

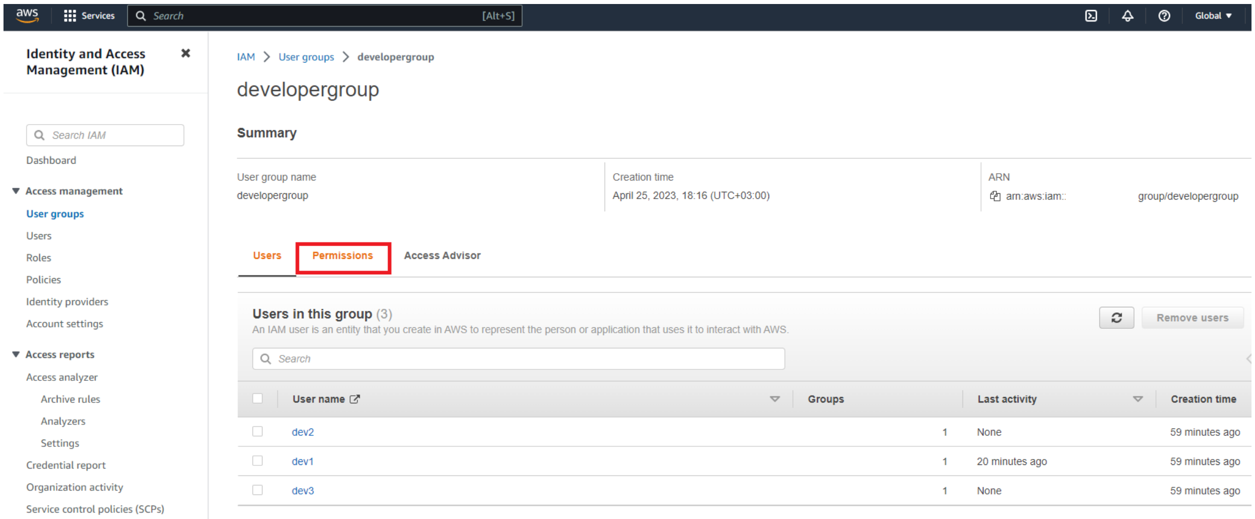
6. Go back to the **original IAM browser** window that you had open.
7. From the left-side menu, select **User groups**.
8. Select the **developergroup**.



A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

□	Group name	Users
□	admingroup	
□	developergroup	

9. Select Permissions.



User group name: developergroup

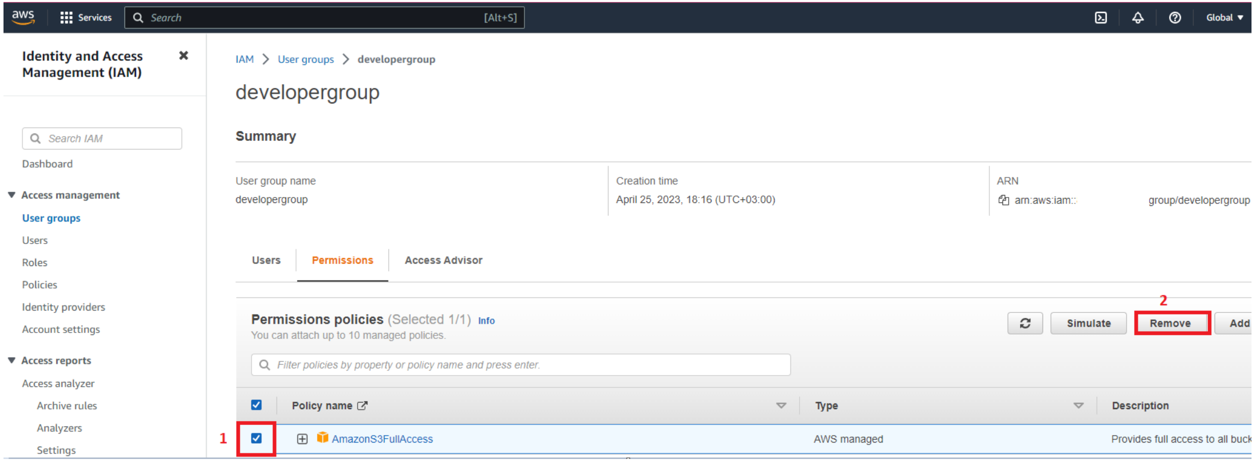
Creation time: April 25, 2023, 18:16 (UTC+03:00)

ARN: arn:aws:iam:: group/developergroup

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

□	User name	Groups	Last activity	Creation time
□	dev2	1	None	59 minutes ago
□	dev1	1	20 minutes ago	59 minutes ago
□	dev3	1	None	59 minutes ago

10. Select the **AmazonS3FullAccess** policy and click **Remove**.



User group name: developergroup

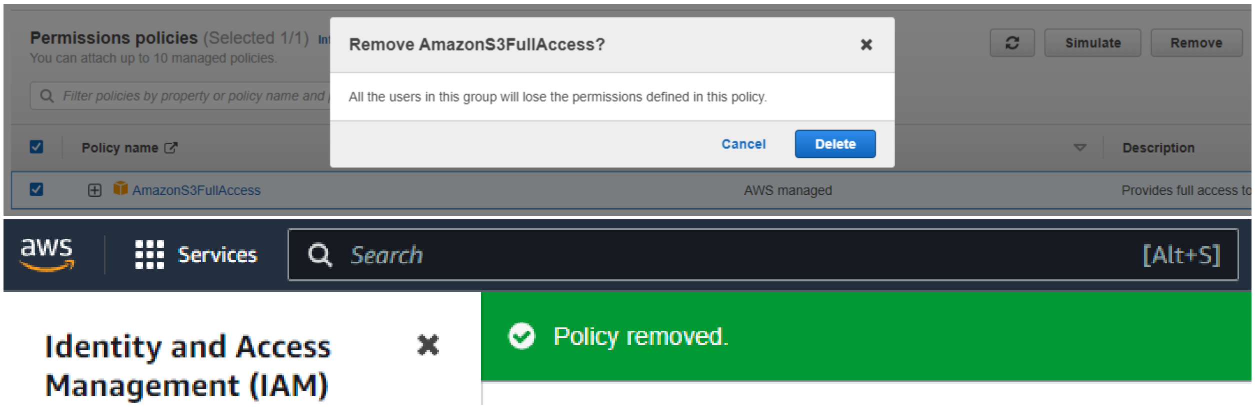
Creation time: April 25, 2023, 18:16 (UTC+03:00)

ARN: arn:aws:iam:: group/developergroup

You can attach up to 10 managed policies.

☑	Policy name	Type	Description
☑	AmazonS3FullAccess	AWS managed	Provides full access to all buck

11. Click **Delete**.


Permissions policies (Selected 1/1)

You can attach up to 10 managed policies.

Remove AmazonS3FullAccess?

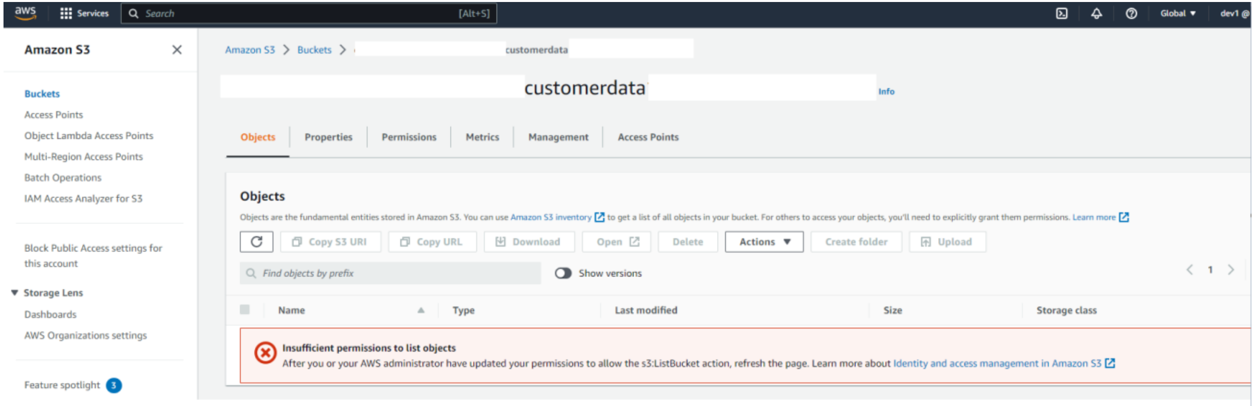
All the users in this group will lose the permissions defined in this policy.

Policy name		Description
AmazonS3FullAccess	AWS managed	Provides full access to

Policy removed.

Filter policies by property or policy name and
Cancel
Delete
Simulate
Remove
aws
Services
Search
[Alt+S]
Identity and Access Management (IAM)

12. Go back to the other incognito windows for the **dev1** user.
13. Refresh both windows for the **customerdata** and **appconfig** buckets. Note that you will now see an error indicating the user has insufficient permissions to list objects.


customerdata

Objects

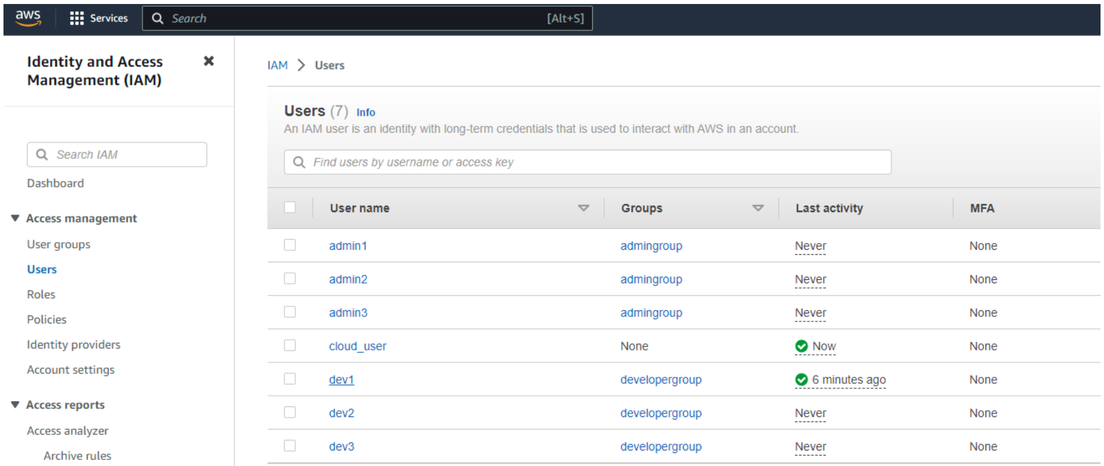
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Insufficient permissions to list objects

After you or your AWS administrator have updated your permissions to allow the s3:ListBucket action, refresh the page. Learn more about Identity and access management in Amazon S3

1.4. Attach the S3RestrictedPolicy to the dev1 User

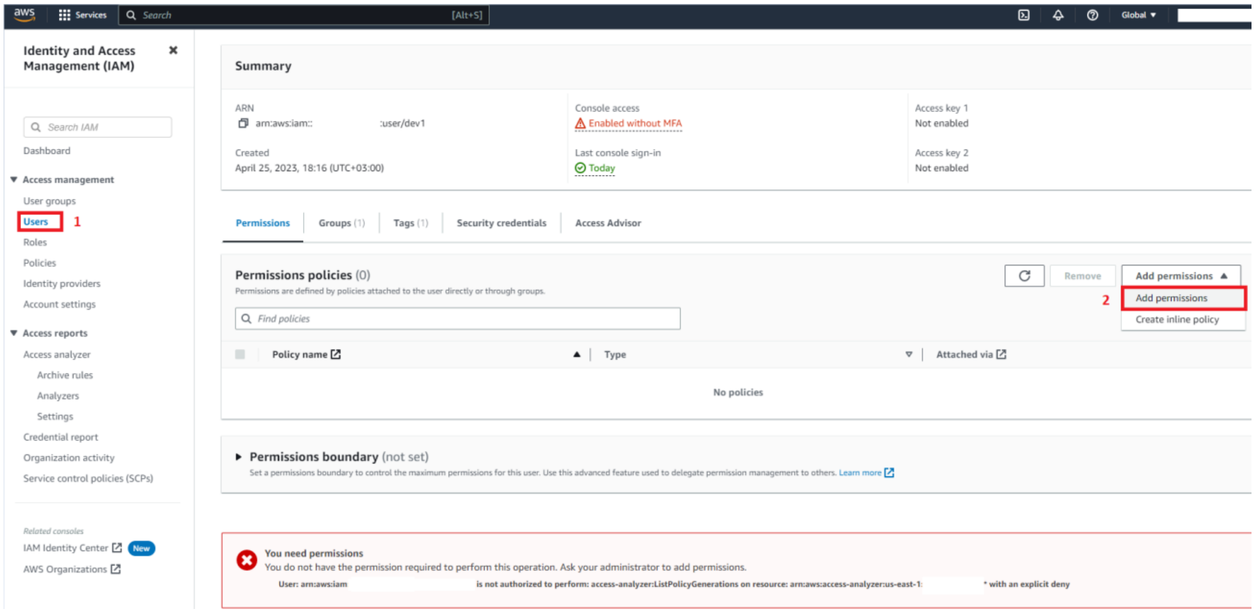
1. Go back to the original IAM browser window.
2. On the left-side menu, select **Users**.
3. Select the **dev1** user.


Users (7) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Groups	Last activity	MFA
admin1	admingroup	Never	None
admin2	admingroup	Never	None
admin3	admingroup	Never	None
cloud_user	None	Now	None
dev1	developergroup	6 minutes ago	None
dev2	developergroup	Never	None
dev3	developergroup	Never	None

4. Under Permissions, click **Add permissions**.



Summary

ARN: arn:aws:iam:: :user/dev1

Console access: Enabled without MFA

Access key 1: Not enabled

Created: April 25, 2023, 18:16 (UTC+03:00)

Last console sign-in: Today

Access key 2: Not enabled

Permissions policies (0)

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

Policy name	Type	Attached via
No policies		

Permissions boundary (not set)

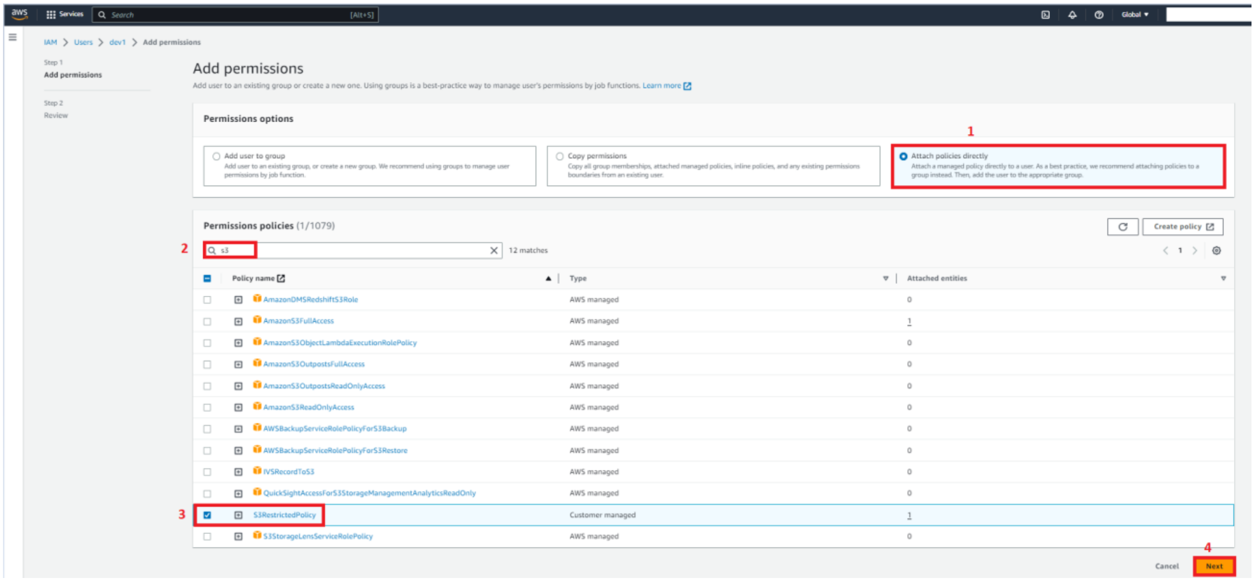
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more

You need permissions

You do not have the permission required to perform this operation. Ask your administrator to add permissions.

User: arn:aws:iam is not authorized to perform: access-analyzer:ListPolicyGenerations on resource: arn:aws:access-analyzer:us-east-1: * with an explicit deny

5. Select **Attach existing policies directly**.
6. In the search bar, type "S3" and select **S3RestrictedPolicy**.
7. Click Next.



Add permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Permissions options

○ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ Copy permissions
Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.

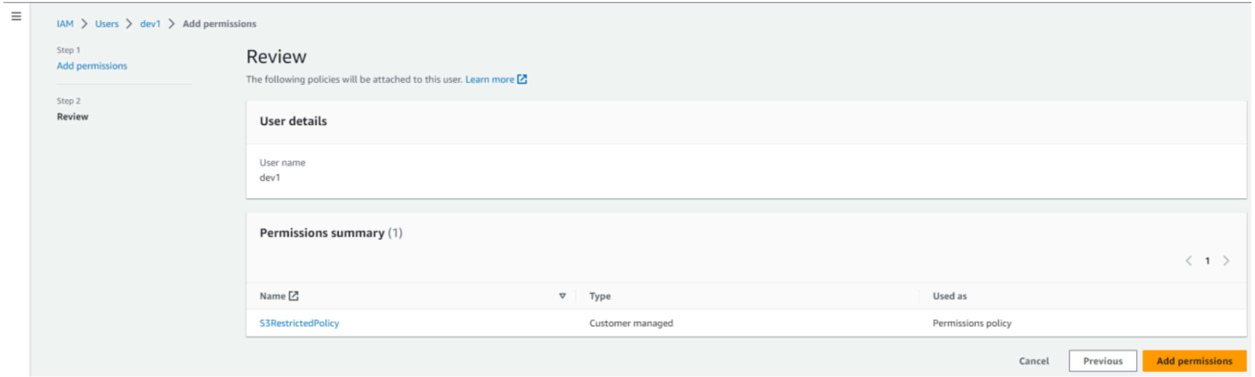
● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1079)

s3 — 12 matches

	Policy name	Type	Attached entities
□	AmazonDMSRedshiftS3Role	AWS managed	0
□	AmazonS3FullAccess	AWS managed	1
□	AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	0
□	AmazonS3OutpostsFullAccess	AWS managed	0
□	AmazonS3OutpostsReadOnlyAccess	AWS managed	0
□	AmazonS3ReadOnlyAccess	AWS managed	0
□	AWSBackupServiceRolePolicyForS3Backup	AWS managed	0
□	AWSBackupServiceRolePolicyForS3Restore	AWS managed	0
□	IVSRecordToS3	AWS managed	0
□	QuickSightAccessForS3StorageManagementAnalyticsReadOnly	AWS managed	0
☑	S3RestrictedPolicy	Customer managed	1
□	S3StorageLensServiceRolePolicy	AWS managed	0

8. Click Add permissions.



Review

The following policies will be attached to this user. Learn more

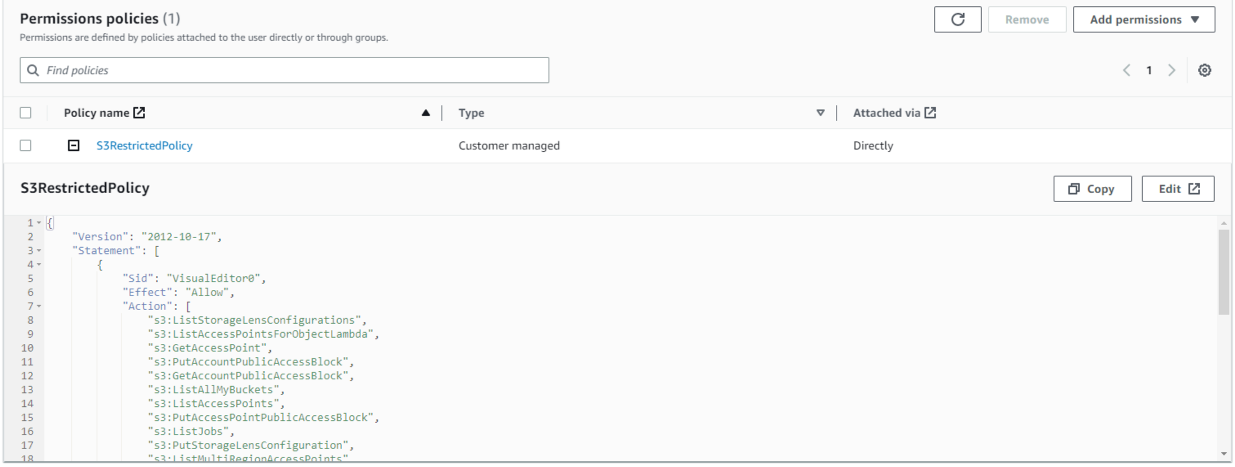
User details

User name: dev1

Permissions summary (1)

Name	Type	Used as
S3RestrictedPolicy	Customer managed	Permissions policy

9. Click the arrow next to the policy and select {} JSON to display and review the policy's contents.



Permissions policies (1)

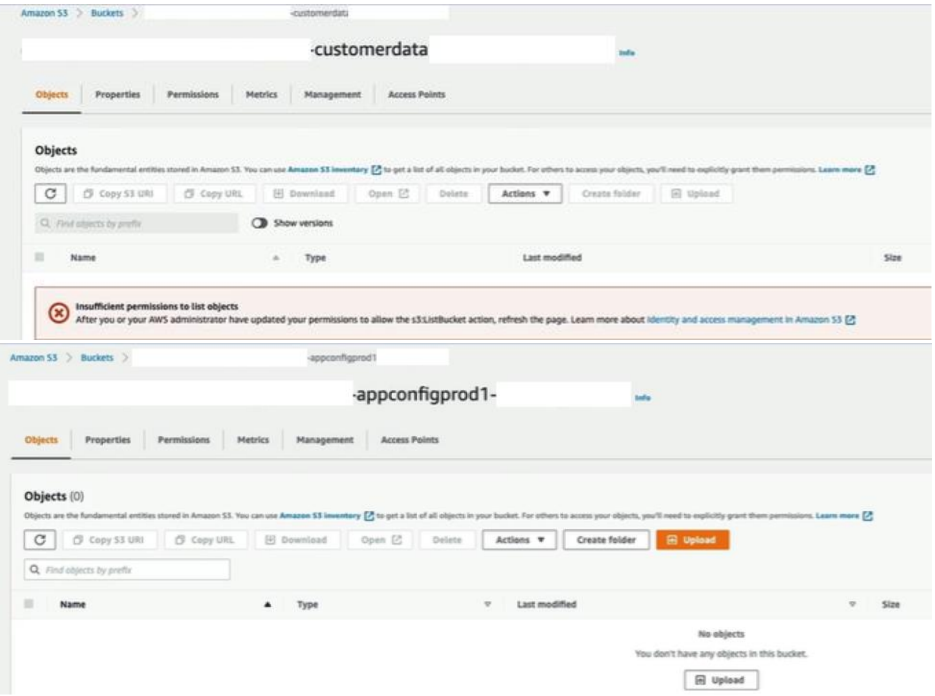
Permissions are defined by policies attached to the user directly or through groups.

□	Policy name	Type	Attached via
□	S3RestrictedPolicy	Customer managed	Directly

S3RestrictedPolicy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:ListStorageLensConfigurations",
                "s3:ListAccessPointsForObjectLambda",
                "s3:GetAccessPoint",
                "s3:PutAccountPublicAccessBlock",
                "s3:GetAccountPublicAccessBlock",
                "s3:ListAllMyBuckets",
                "s3:ListAccessPoints",
                "s3:PutAccessPointPublicAccessBlock",
                "s3:ListJobs",
                "s3:PutStorageLensConfiguration",
                "s3:ListMultiRegionAccessPoints",
```

10. To verify the configuration, return to the **dev1** browser and attempt to access the appconfig and customerdata buckets. You should now have access to appconfig buckets, while customerdata buckets are still denied.



Amazon S3 > Buckets > [redacted]-customerdat

[redacted]-customerdata [redacted] Info

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

Objects

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

Insufficient permissions to list objects
After you or your AWS administrator have updated your permissions to allow the s3:ListBucket action, refresh the page. Learn more about Identity and access management in Amazon S3

Amazon S3 > Buckets > [redacted]-appconfigprod1

[redacted]-appconfigprod1-[redacted] Info

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

Objects (0)

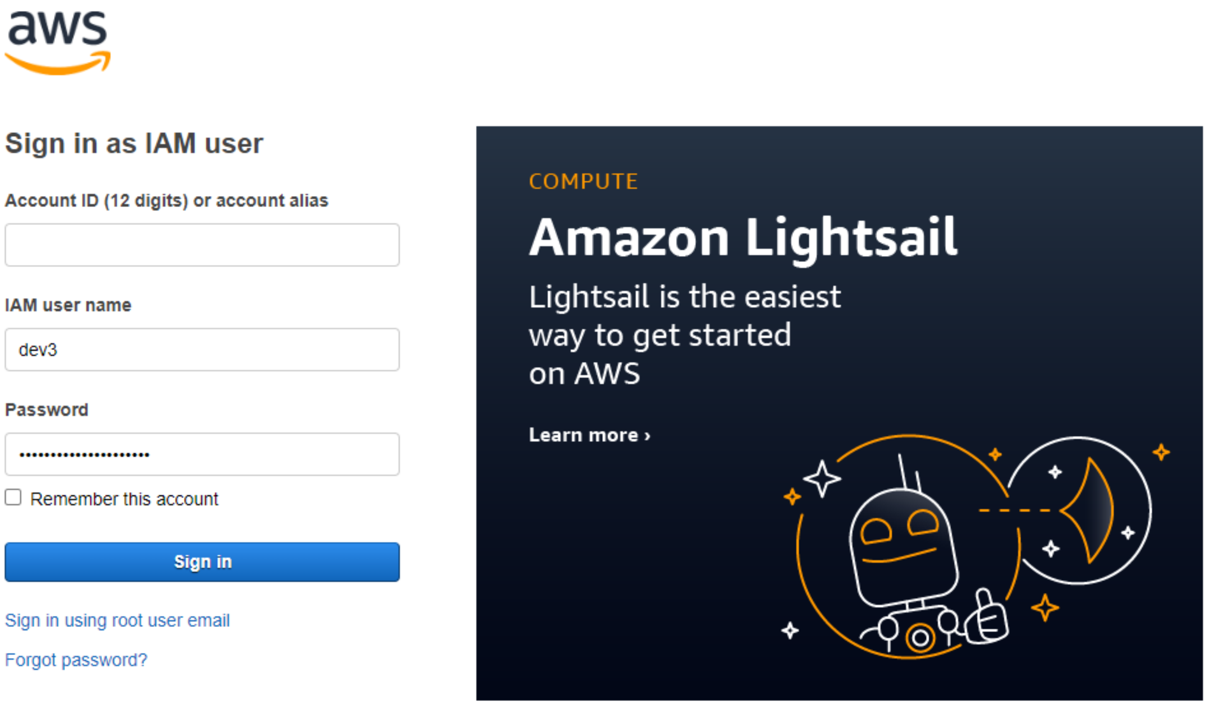
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

No objects
You don't have any objects in this bucket.

2. Configure IAM So the dev3 User Can Assume the Role

2.1. Create the AssumeS3Policy IAM Policy

1. Open a new incognito browser window using the same account ID as before. Log in as the **dev3** user using the following credentials:
User: dev3
Password:



Sign in as IAM user

Account ID (12 digits) or account alias

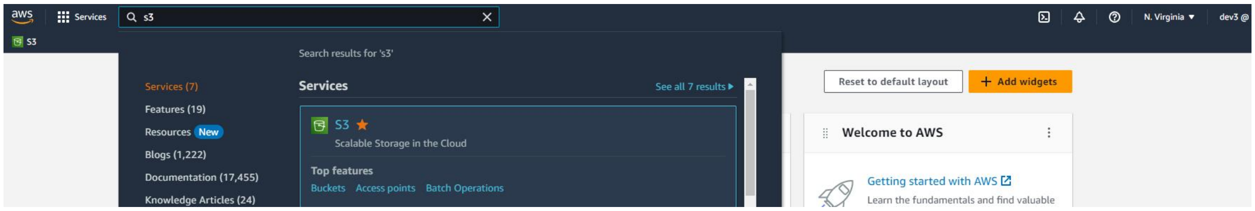
IAM user name: dev3

Password: ••••••••••••••••••••

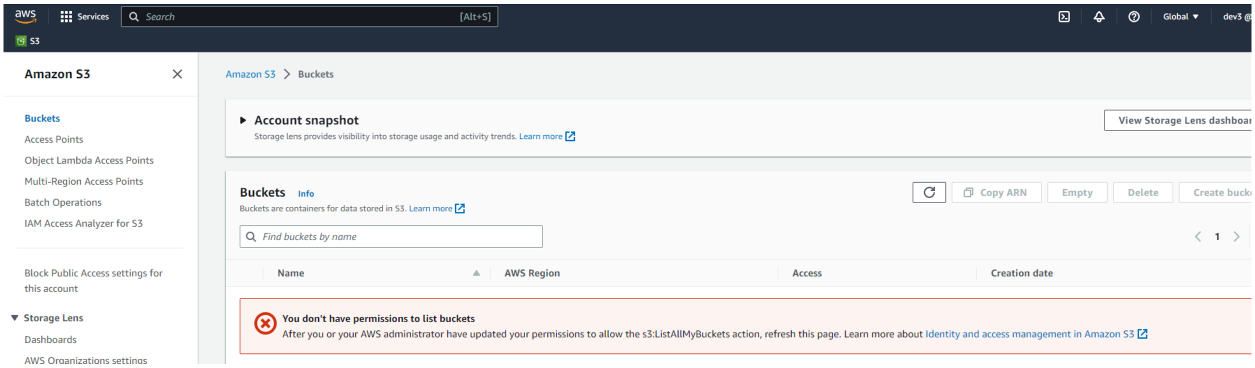
□ Remember this account

Sign in
Sign in using root user email
Forgot password?
COMPUTE
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more ›

2. Navigate to S3. Note that **dev3** and verify the user's current access.



You can see the buckets.

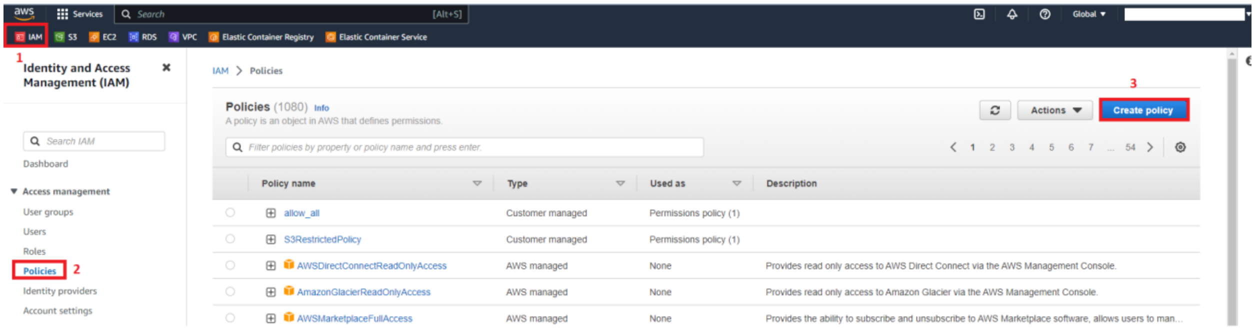


aws
Services
Search
[Alt+S]
Global ▼
dev3 @
S3
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
▼ Storage Lens
Dashboards
AWS Organizations settings
Amazon S3 > Buckets
▸ Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboar
Buckets Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create buck
Find buckets by name
1
Name
AWS Region
Access
Creation date

You don't have permissions to list buckets

After you or your AWS administrator have updated your permissions to allow the s3:ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3

3. Go back to the original IAM browser window.
4. From the left-side menu, select **Policies**.
5. Click **Create policy**.

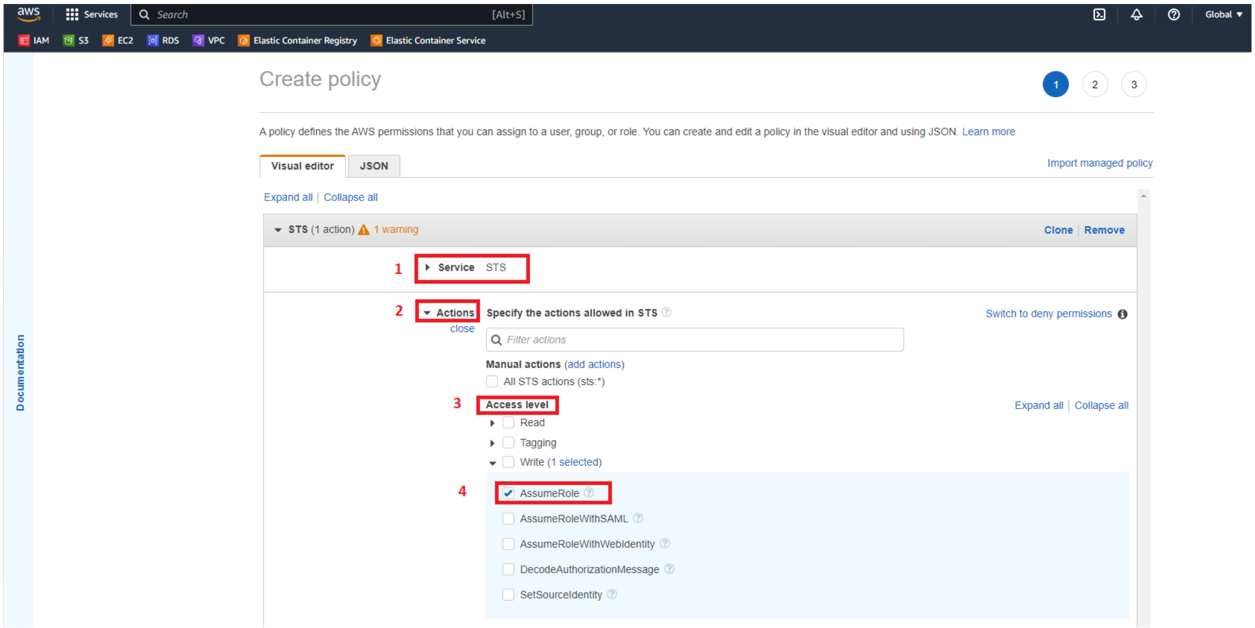


Policies (1080) Info

A policy is an object in AWS that defines permissions.

	Policy name	Type	Used as	Description
○	⊞ allow_all	Customer managed	Permissions policy (1)	
○	⊞ S3RestrictedPolicy	Customer managed	Permissions policy (1)	
○	⊞ AWSDirectConnectReadOnlyAccess	AWS managed	None	Provides read only access to AWS Direct Connect via the AWS Management Console.
○	⊞ AmazonGlacierReadOnlyAccess	AWS managed	None	Provides read only access to Amazon Glacier via the AWS Management Console.
○	⊞ AWSMarketplaceFullAccess	AWS managed	None	Provides the ability to subscribe and unsubscribe to AWS Marketplace software, allows users to man...

6. In *Service*, click **Choose a service**.
7. Type and select **STS** (Security Token Service that allows you to assume roles in AWS).
8. In *Actions* under *Access level*, click the arrow next to *Write* to expand its options, and select **AssumeRole**.



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

▼ STS (1 action) ⚠ 1 warning

▸ Service STS

▼ Actions Specify the actions allowed in STS

Manual actions (add actions)

□ All STS actions (sts:*)

Access level

▸ □ Read

▸ □ Tagging

▾ □ Write (1 selected)

☑ AssumeRole

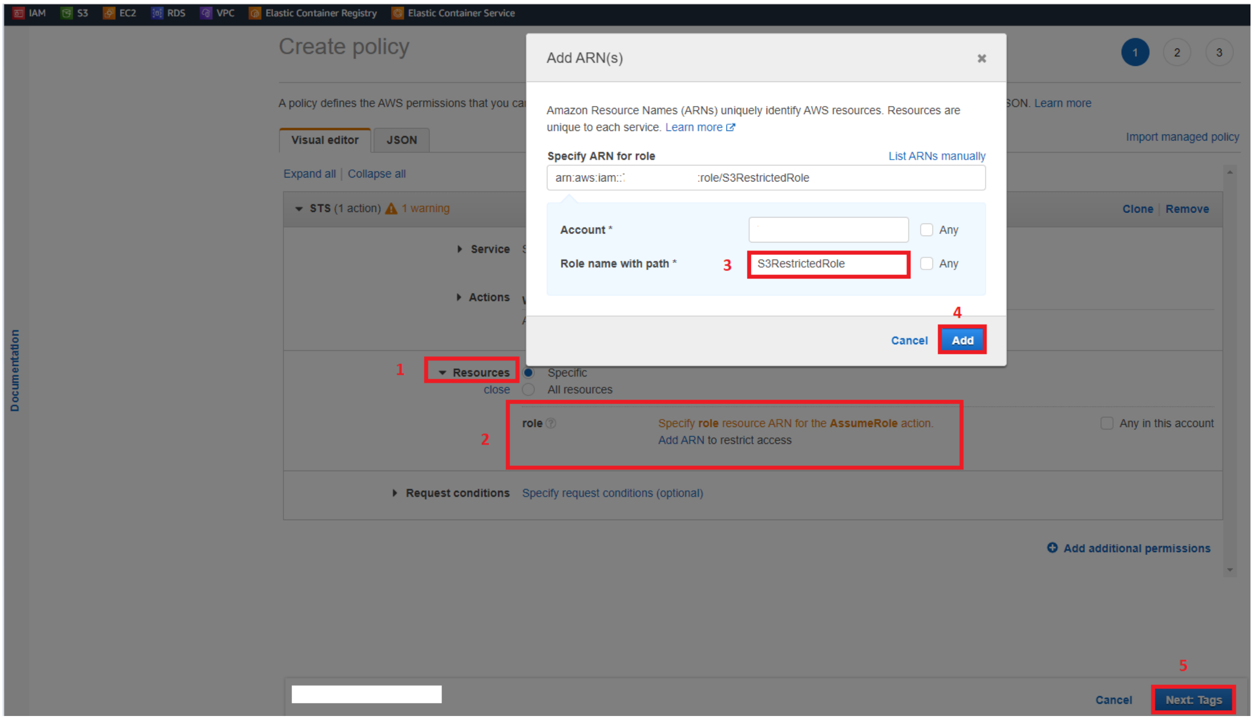
□ AssumeRoleWithSAML

□ AssumeRoleWithWebIdentity

□ DecodeAuthorizationMessage

□ SetSourceIdentity

9. In *Resources* under *role*, click **Add ARN**.
10. In the *Add ARN(s)* pop-up window, set *Role name* with path to "S3RestrictedRole" and click Add.
11. Click Next: Tags.



Create policy

A policy defines the AWS permissions that you ca ... SON. Learn more

STS (1 action) ⚠ 1 warning

▾ Resources ● Specific
close ○ All resources

role Specify role resource ARN for the AssumeRole action.
Add ARN to restrict access

□ Any in this account

Specify request conditions (optional)

Add ARN(s)

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more

Specify ARN for role List ARNs manually

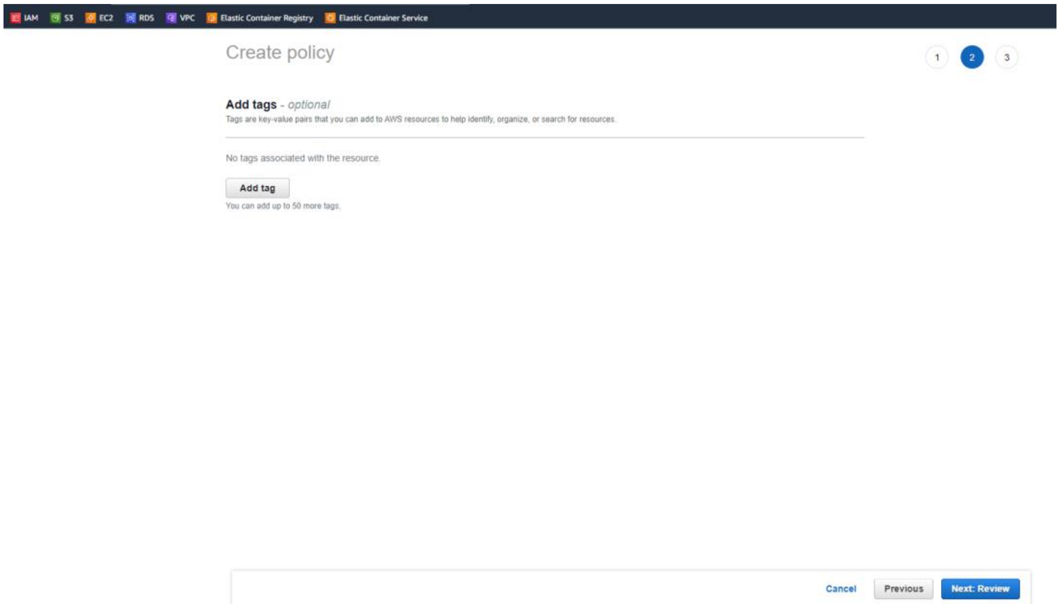
arn:aws:iam:: :role/S3RestrictedRole

Account * □ Any

Role name with path * S3RestrictedRole □ Any

Cancel Add

12. Click **Next: Review**.



Create policy

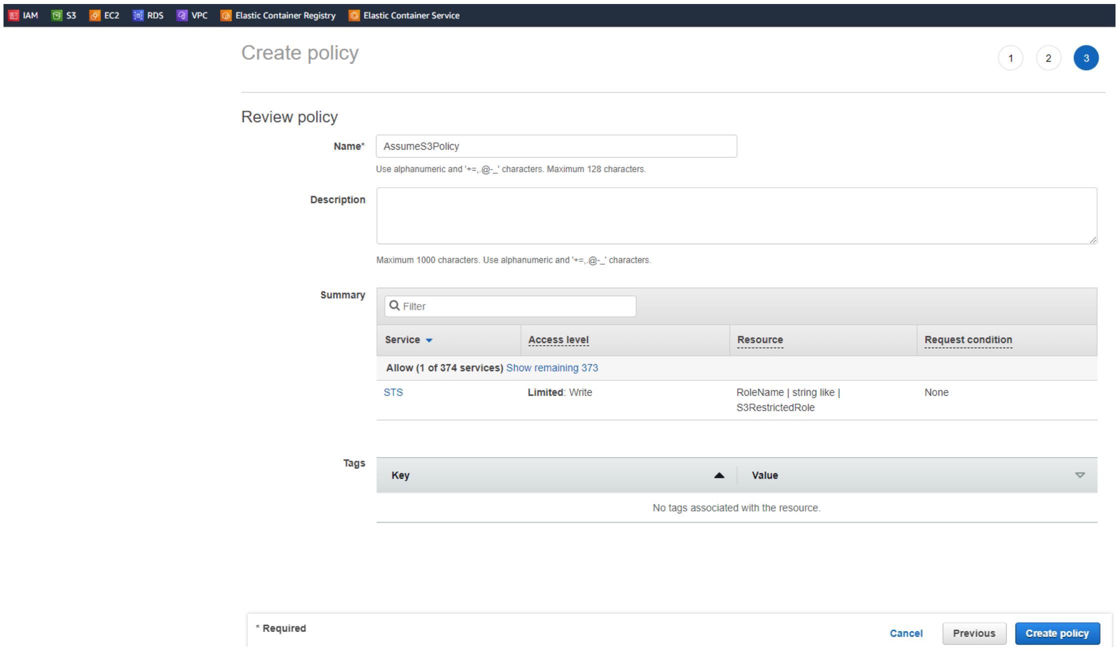
Add tags - *optional*

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.

13. For *Name*, enter "AssumeS3Policy", and click **Create policy**.



Create policy

Review policy

Name* AssumeS3Policy

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

Description

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

Summary

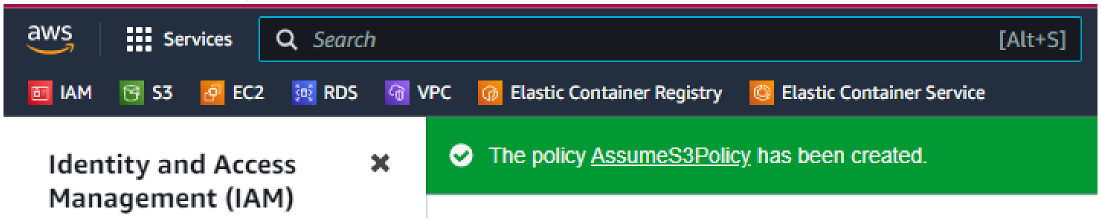
Service	Access level	Resource	Request condition
Allow (1 of 374 services) Show remaining 373			
STS	**Limited**: Write	RoleName | string like | S3RestrictedRole	None

Tags

Key	Value
No tags associated with the resource.	

* Required

Cancel
Previous
Create policy

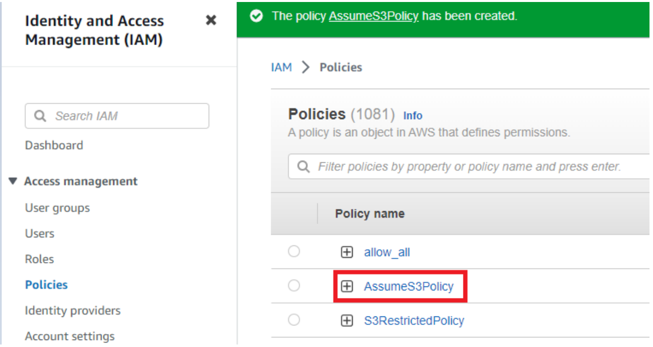


aws
Services
Search
[Alt+S]
IAM
S3
EC2
RDS
VPC
Elastic Container Registry
Elastic Container Service
Identity and Access Management (IAM)

The policy AssumeS3Policy has been created.

2.2. Attach the AssumeS3Policy to the dev3 User

1. Select the new policy.



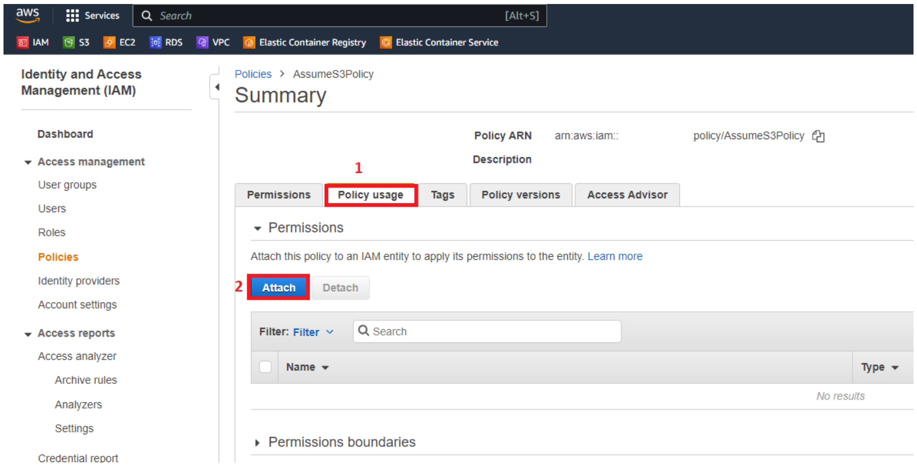
The policy AssumeS3Policy has been created.

Policies (1081) Info

A policy is an object in AWS that defines permissions.

	Policy name
○	⊞ allow_all
○	⊞ AssumeS3Policy
○	⊞ S3RestrictedPolicy

2. Select the *Policy usage* tab, and click **Attach**.

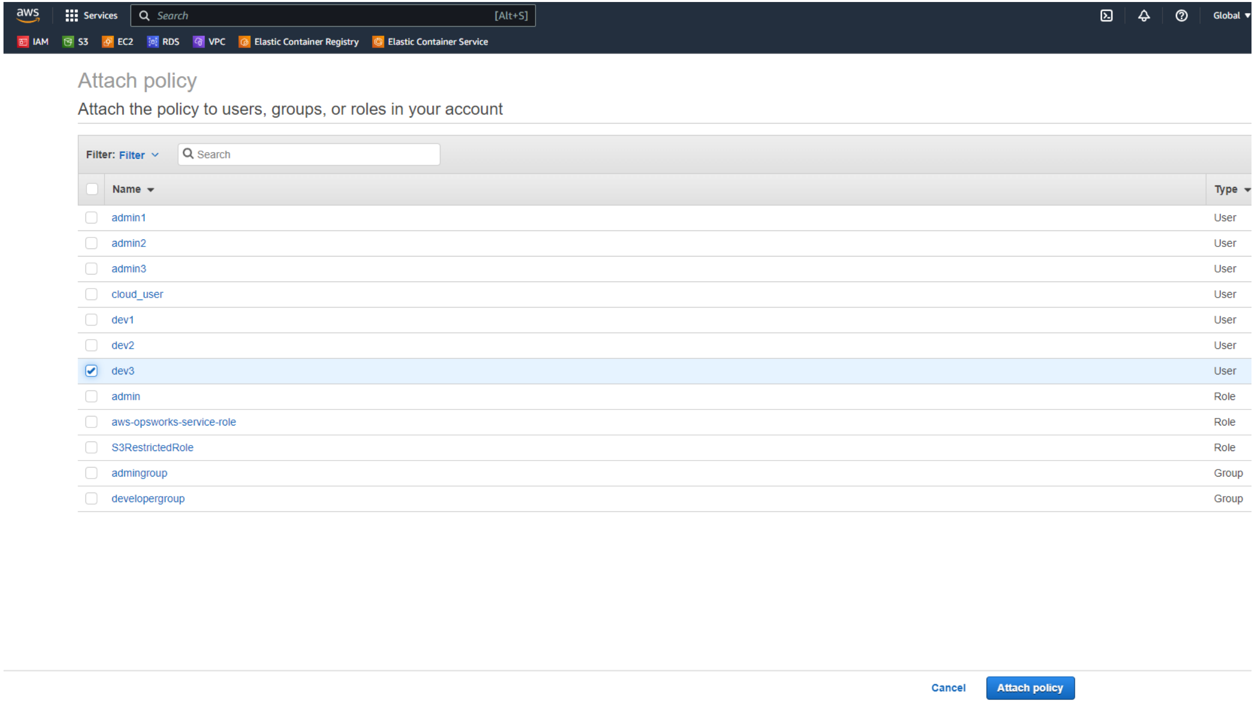


Policy ARN arn:aws:iam:: policy/AssumeS3Policy

Description

Attach this policy to an IAM entity to apply its permissions to the entity. Learn more

3. Select **dev3**, and click **Attach policy**.



Attach policy

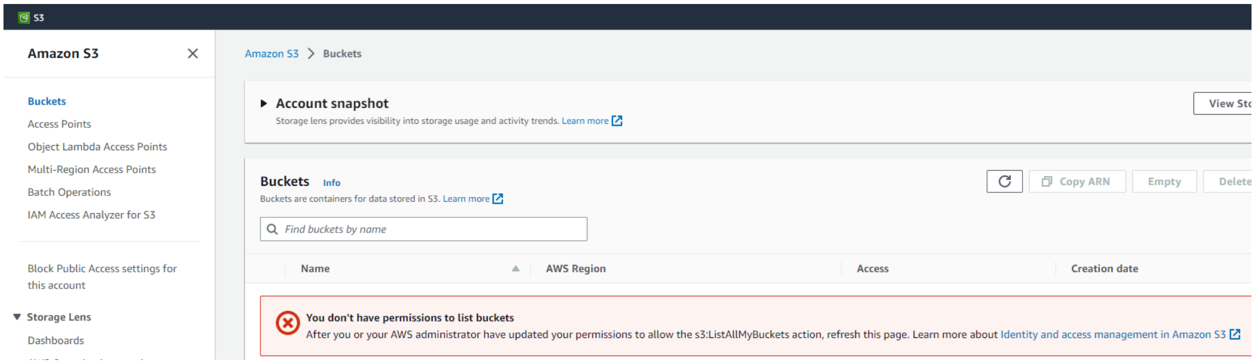
Attach the policy to users, groups, or roles in your account

	Name	Type
□	admin1	User
□	admin2	User
□	admin3	User
□	cloud_user	User
□	dev1	User
□	dev2	User
☑	dev3	User
□	admin	Role
□	aws-opsworks-service-role	Role
□	S3RestrictedRole	Role
□	admingroup	Group
□	developergroup	Group

Now, our dev3 user should be able to assume the appropriate permissions.

2.3. Assume the S3RestrictedRole as the dev3 User

1. Go back to the other browser window where you are logged in as **dev3** in S3.
2. Notice that the **dev3** user still doesn't have bucket access because the role has not yet been assumed (our restricted S3 role).

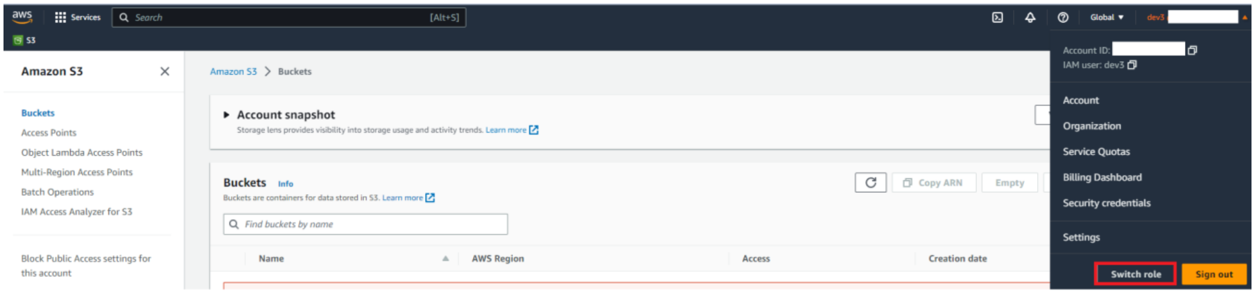


Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets are containers for data stored in S3. Learn more

You don't have permissions to list buckets
After you or your AWS administrator have updated your permissions to allow the s3:ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3

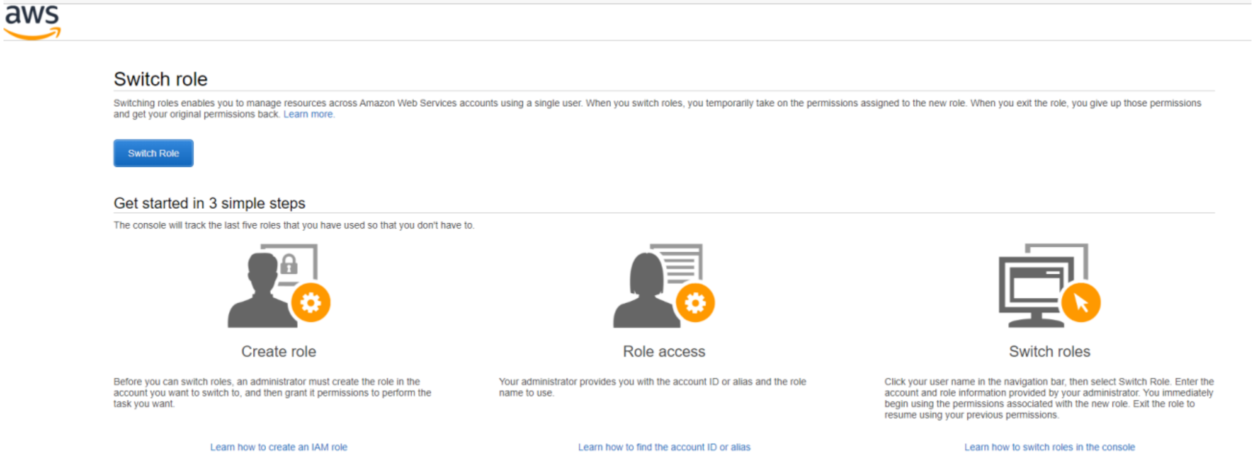
3. To assume the role, click the user dropdown on the top menu, and copy your account ID in your clipboard.
4. Click **Switch Roles**.



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

Buckets are containers for data stored in S3. Learn more

5. In the new window, click Switch Role.


aws
Switch Role
Create role
Role access
Switch roles
Learn how to create an IAM role
Learn how to find the account ID or alias
Learn how to switch roles in the console

Switch role

Switching roles enables you to manage resources across Amazon Web Services accounts using a single user. When you switch roles, you temporarily take on the permissions assigned to the new role. When you exit the role, you give up those permissions and get your original permissions back. Learn more.

Get started in 3 simple steps

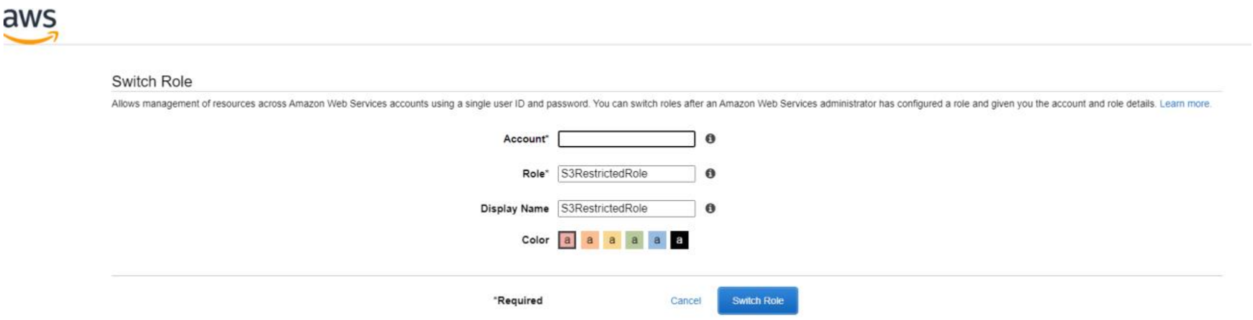
The console will track the last five roles that you have used so that you don't have to.

Before you can switch roles, an administrator must create the role in the account you want to switch to, and then grant it permissions to perform the task you want.

Your administrator provides you with the account ID or alias and the role name to use.

Click your user name in the navigation bar, then select Switch Role. Enter the account and role information provided by your administrator. You immediately begin using the permissions associated with the new role. Exit the role to resume using your previous permissions.

6. Set the following values:
   Account: The account ID you just copied
   Role: S3RestrictedRole
   Display Name: S3RestrictedRole
7. Click **Switch Role**.



Switch Role

Allows management of resources across Amazon Web Services accounts using a single user ID and password. You can switch roles after an Amazon Web Services administrator has configured a role and given you the account and role details. Learn more.

Account*

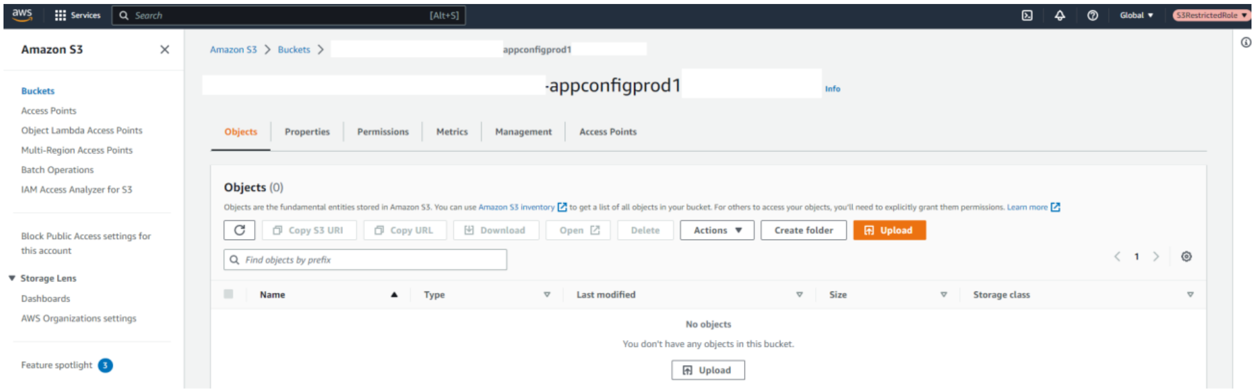
Role* S3RestrictedRole

Display Name S3RestrictedRole

Color a a a a a a

*Required

8. To verify the role has been assumed, attempt to access the **appconfig** and **customer data** buckets. You should now have access to **appconfig** buckets, while **customer data** buckets are still denied.



Amazon S3 > Buckets > [redacted] appconfigprod1

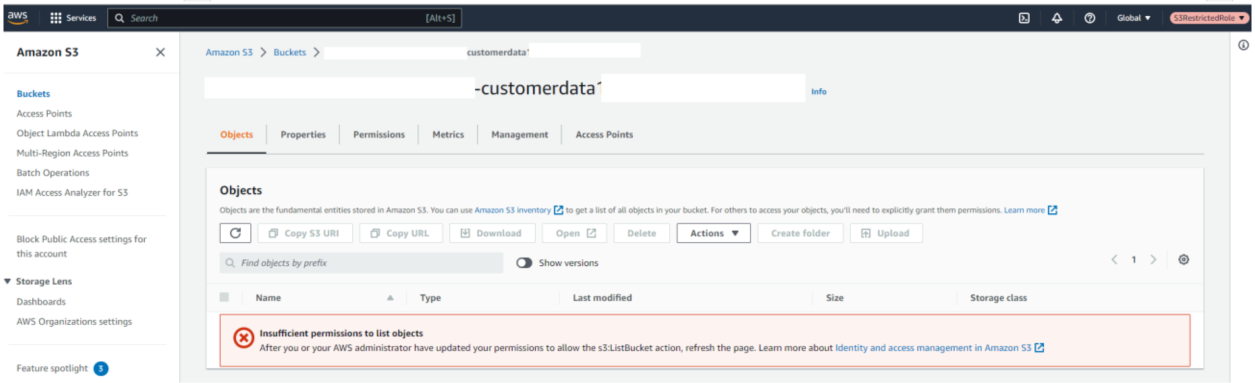
[redacted]-appconfigprod1 Info

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

No objects

You don't have any objects in this bucket.



Amazon S3 > Buckets > [redacted] customerdata[redacted]

[redacted]-customerdata[redacted] 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

Insufficient permissions to list objects

After you or your AWS administrator have updated your permissions to allow the s3:ListBucket action, refresh the page. Learn more about Identity and access management in Amazon S3