Cloud Walkthrough: How to apply Service Control Policies in AWS Organizations

General Information about Service Control Policies

- JSON Policy document that can be attached to AWS Organization / AWS Organization Units / AWS Organization Member accounts
- Service Control Policies are inherited down the Organizational tree
- AWS Management account cant be restricted with Service Control Policies in AWS Organization
- SCPs are account permission boundaries. They limit what the account including the root user can do
- SCPs dont grant any permissions just define a limit

Walkthrough Background Info

- 1 AWS Organization
- 3 AWS Organization Member Accounts
  - General Account (Management Account)
  - DEV Account
  - PROD Account

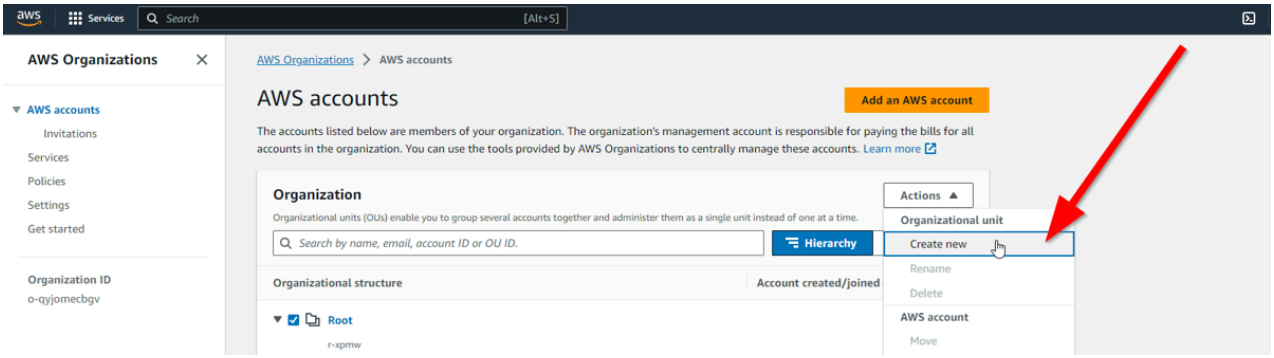
Walkthrough on How to Apply an AWS Service Control Policy

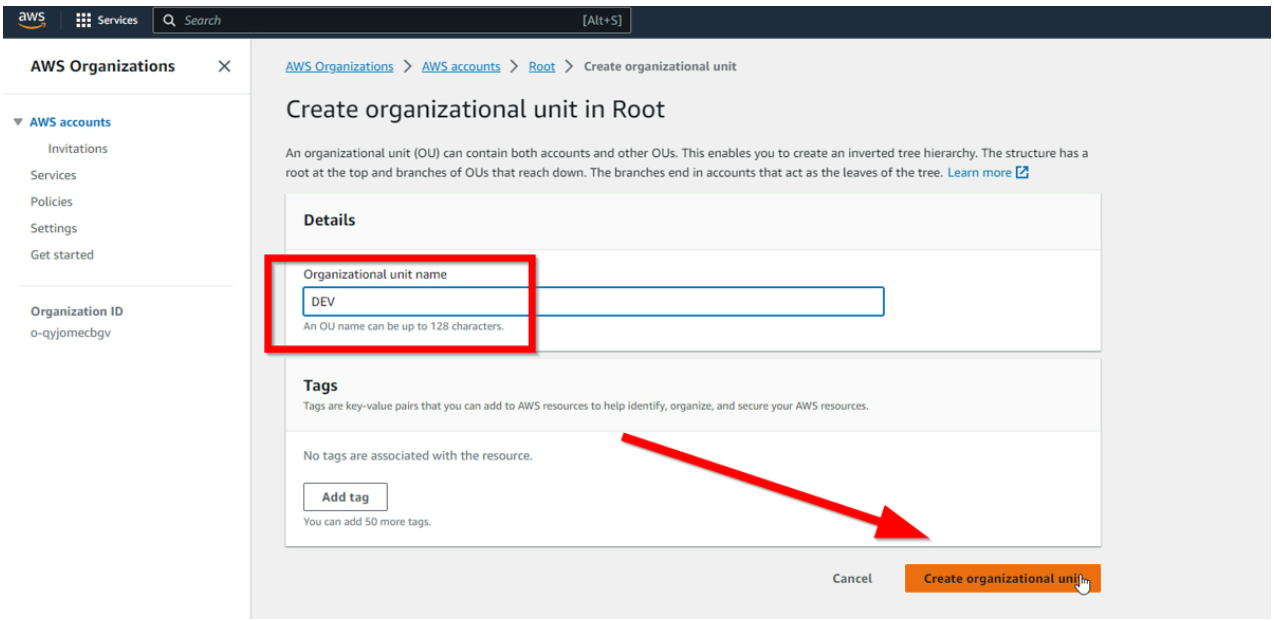
The following walkthrough will go through how to apply an AWS Service Control Policy on an AWS Organization Account in this case, the AWS "PROD" account, and to test the capability of the policy.

1. First, create an AWS Policy that contains a statement ALLOWS all actions on all resources and another statement detailing a DENY on all s3 actions. The following policy will be named denys3.json.

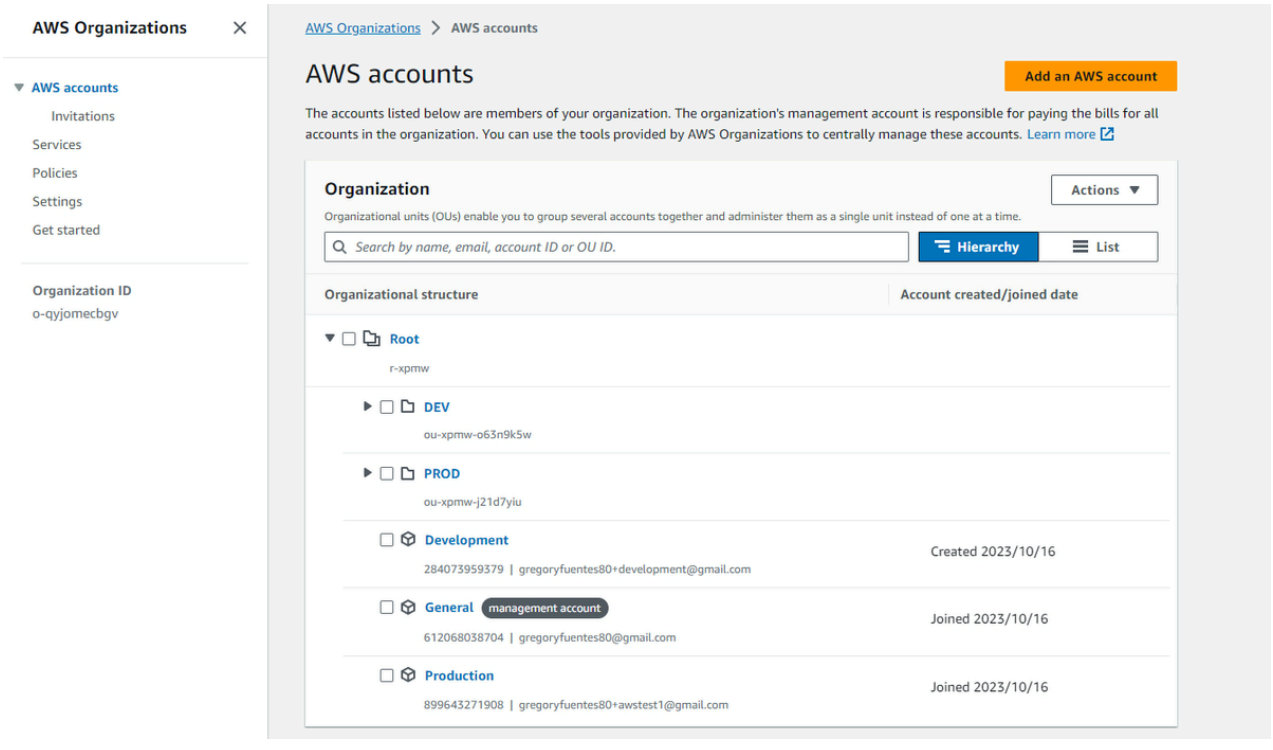
```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": "*"
        }
    ]
}
```

2. Next, create 2 AWS Organization Units named "DEV" and "PROD" within the AWS Organization Root structure.

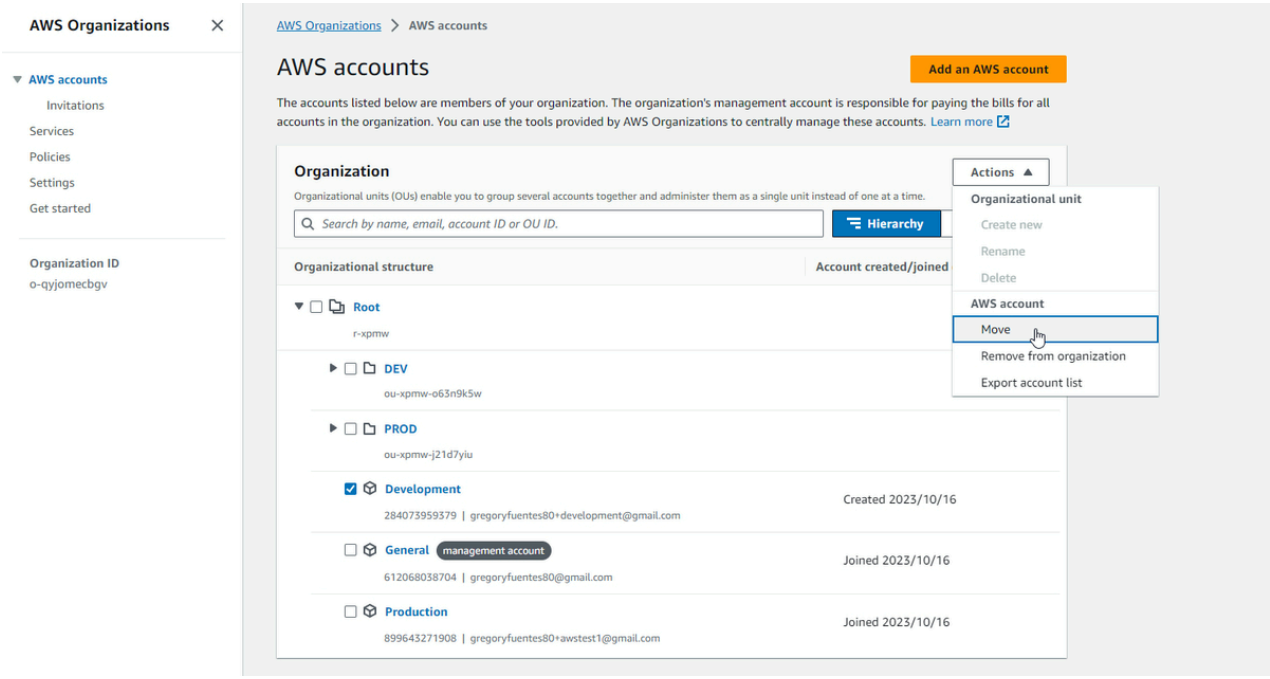


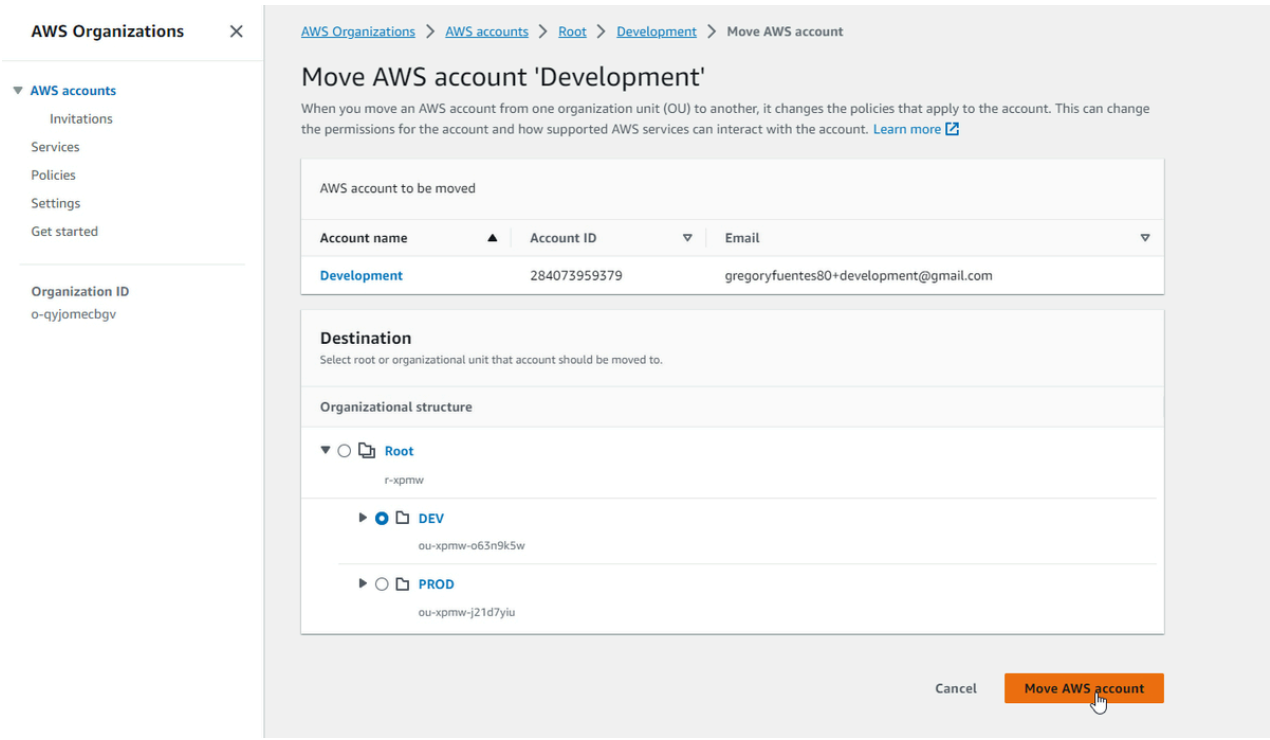


Finally, this is what the AWS Organization should look like after having created 2 AWS Organization Units named "DEV" and "PROD".

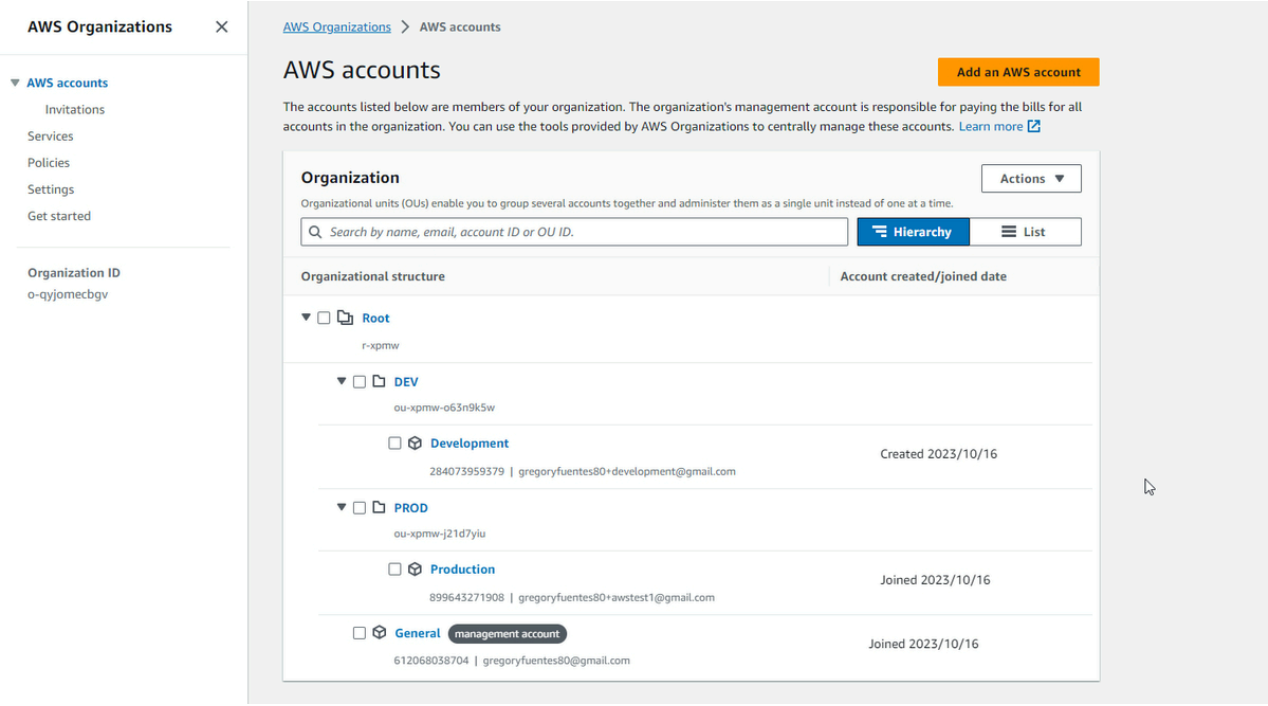


3. Additionally, move the AWS member accounts "Production" and "Development" within the AWS Organization into their respective AWS Organization Units.

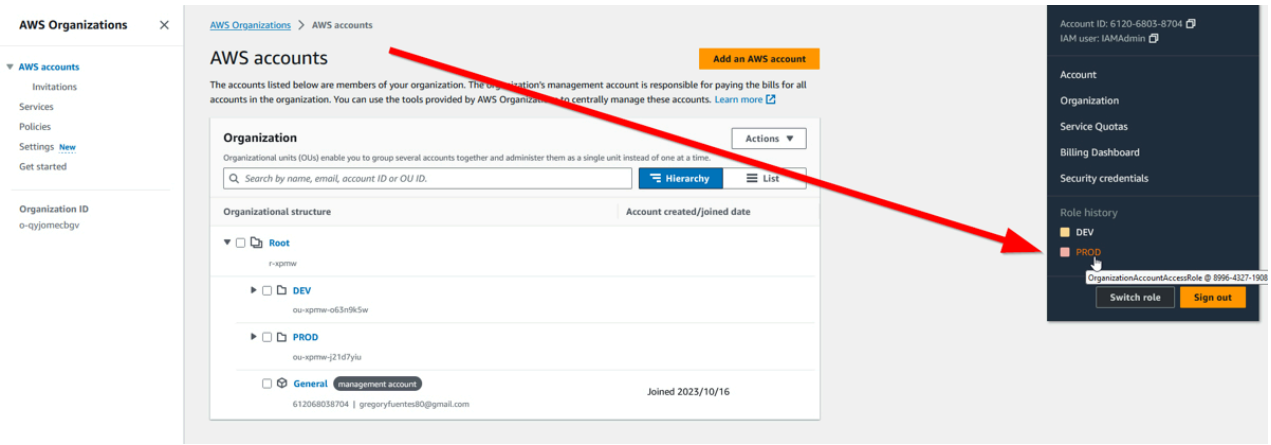


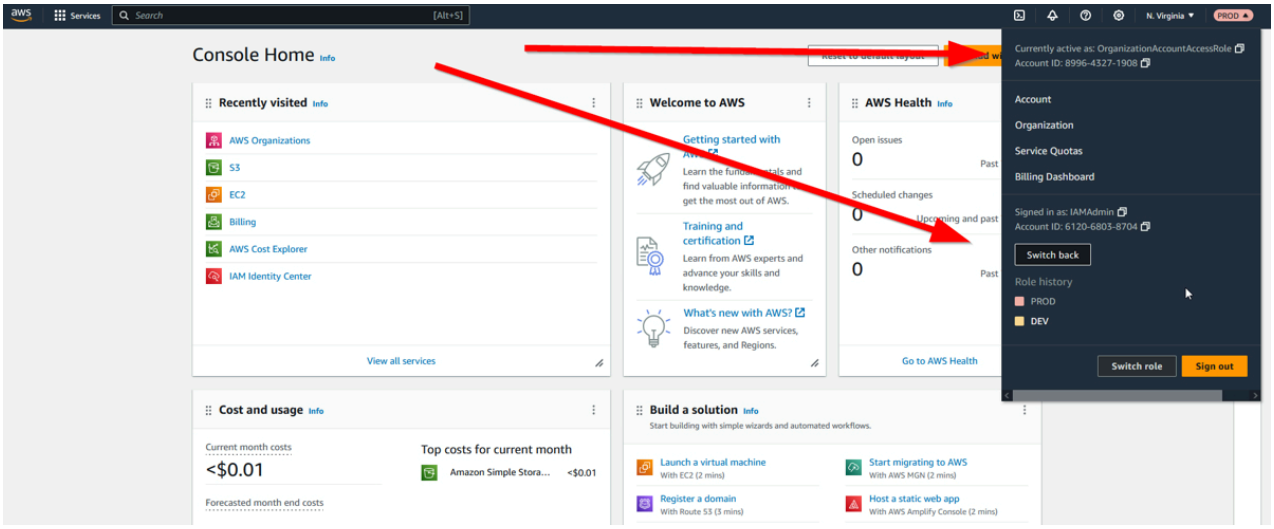


Finally, this is what the AWS Organization should look like after moved the respective AWS Organization member accounts into the AWS Organization Units.

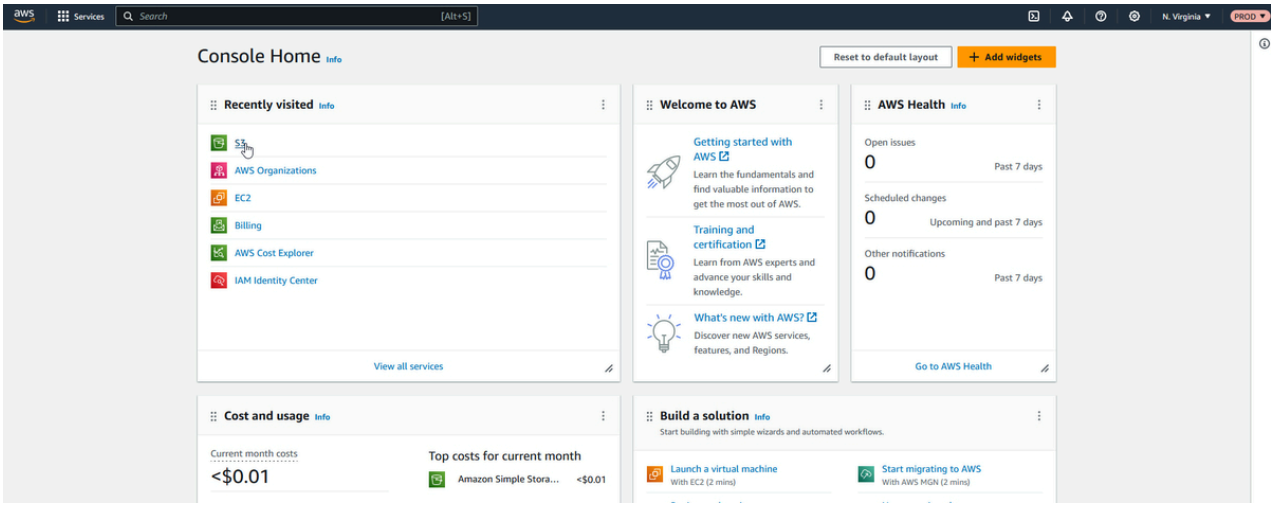


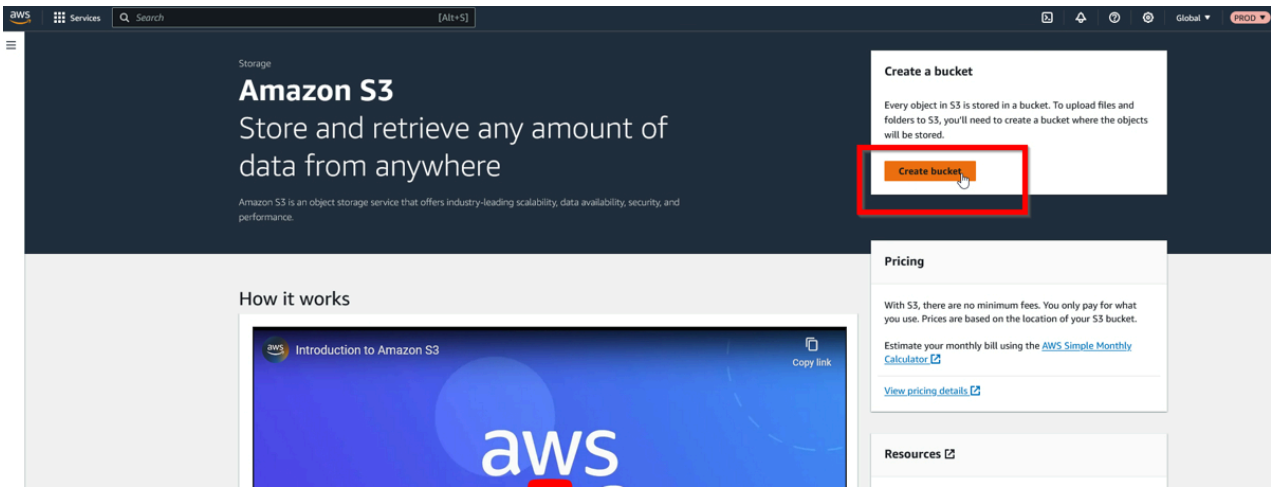
4. Next, switch to the AWS member account "Production" using the OrganizationAccountAccessRole that was created when the account was created in the AWS Organization using SwitchRole history. If there is not a saved AWS Organization Member Account name to use then click SwitchRole and input the required information to access the AWS Organization Member account which includes account id, role name, and saved account alias for the dashboard. This walkthrough will assume you have a saved account alias for the AWS Organization member account you want to switch into using the AWS console dashboard.

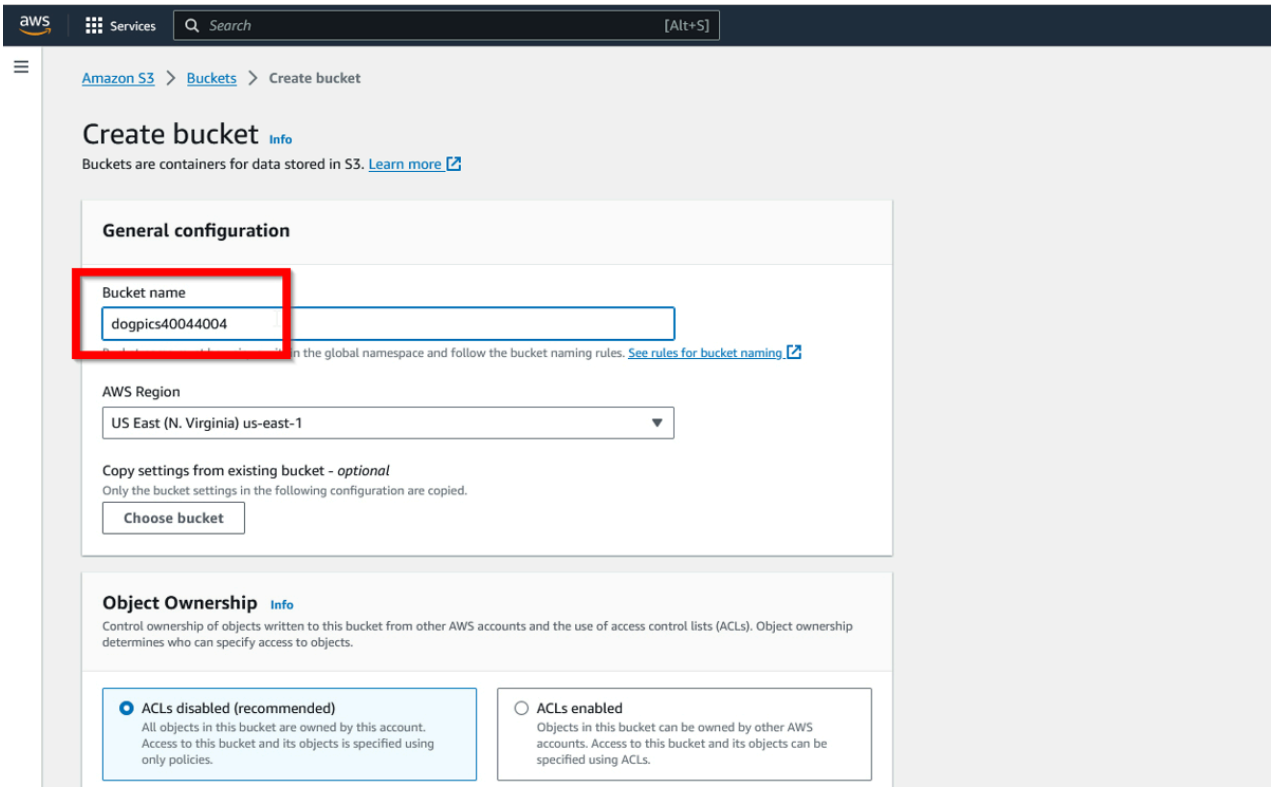


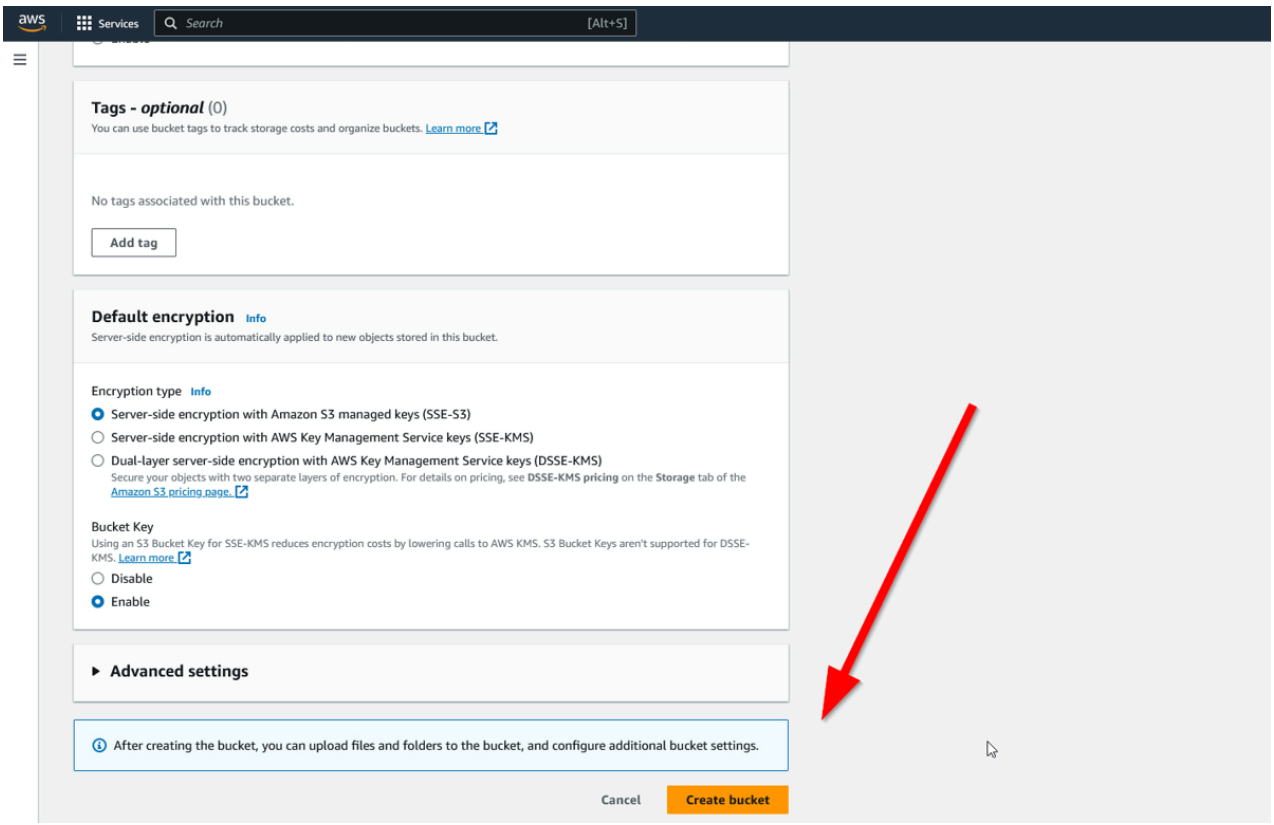


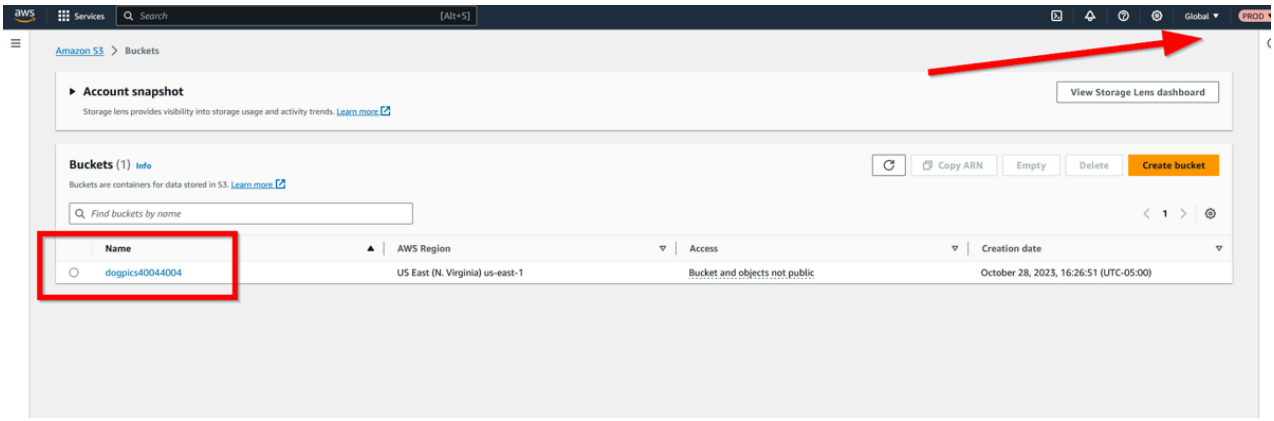
5. Furthermore, create an S3 bucket in the AWS Member account "Production" named "dogpics" with a random number at the end to make it globally unique in the "us-east-1" region. Once created, upload a picture into the AWS S3 "dogpics" bucket in this instance I will be uploading a picture of my dog "Winston" as "dog1.jpg". Open the picture in the AWS S3 "dogpics" bucket to confirm access to the uploaded picture object.

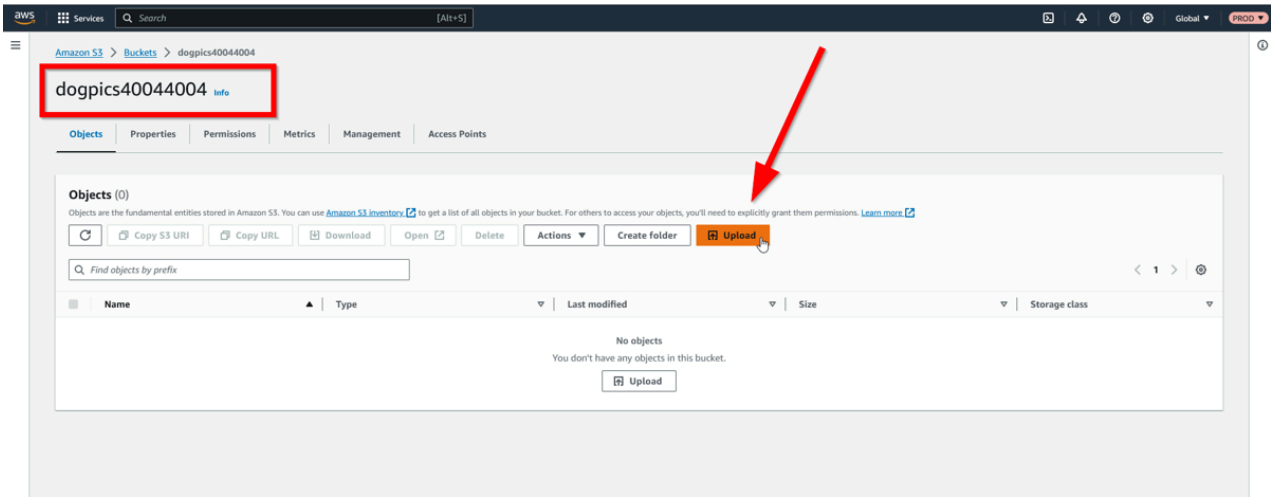


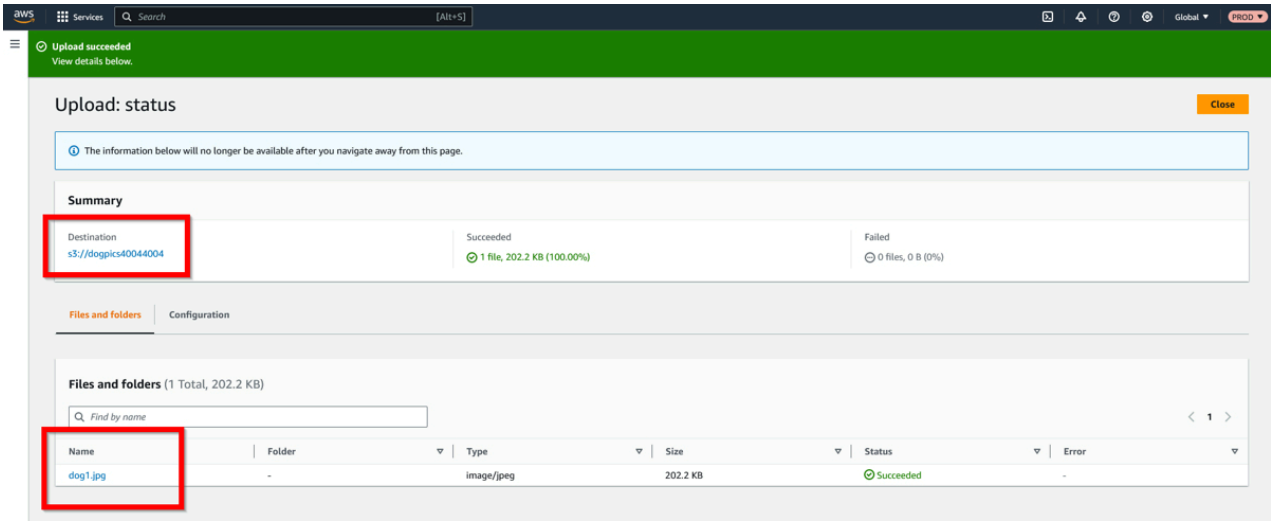

Services
Search
[Alt+S]
Global
PROD
Storage
Amazon S3
Store and retrieve any amount of data from anywhere
Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.
Create a bucket
Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.
Create bucket
Pricing
With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.
Estimate your monthly bill using the AWS Simple Monthly Calculator
View pricing details
Resources
How it works
Introduction to Amazon S3
Copy link
aws

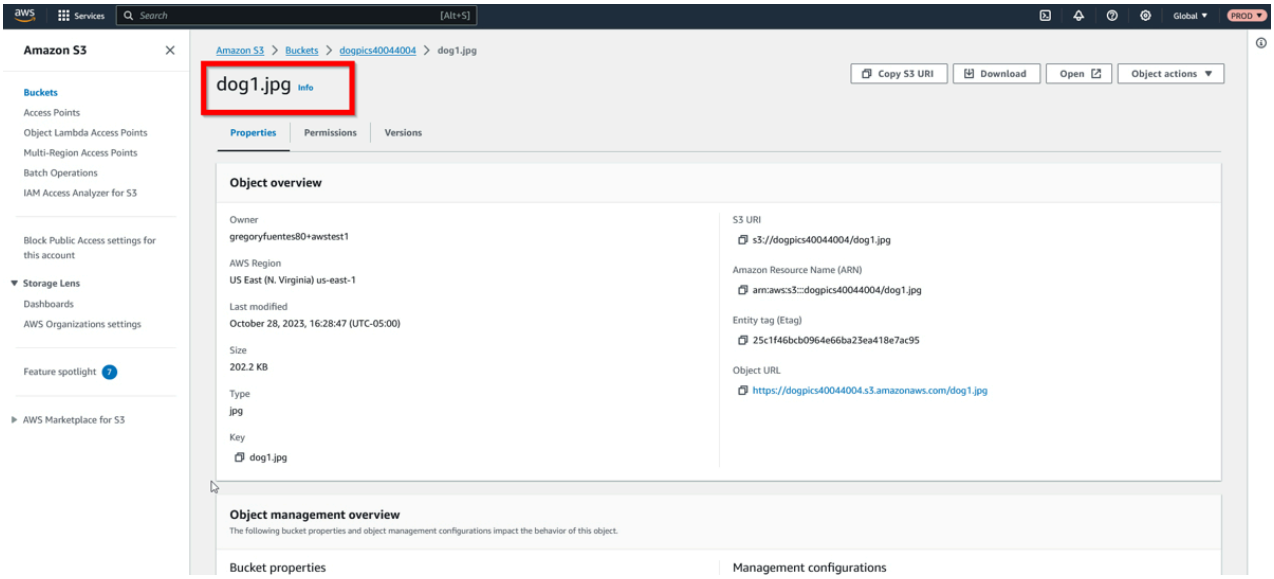

Services
Search
[Alt+S]
Amazon S3 > Buckets > Create bucket
Create bucket Info
Buckets are containers for data stored in S3. Learn more
General configuration
Bucket name
dogpics40044004
n the global namespace and follow the bucket naming rules. See rules for bucket naming
AWS Region
US East (N. Virginia) us-east-1
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

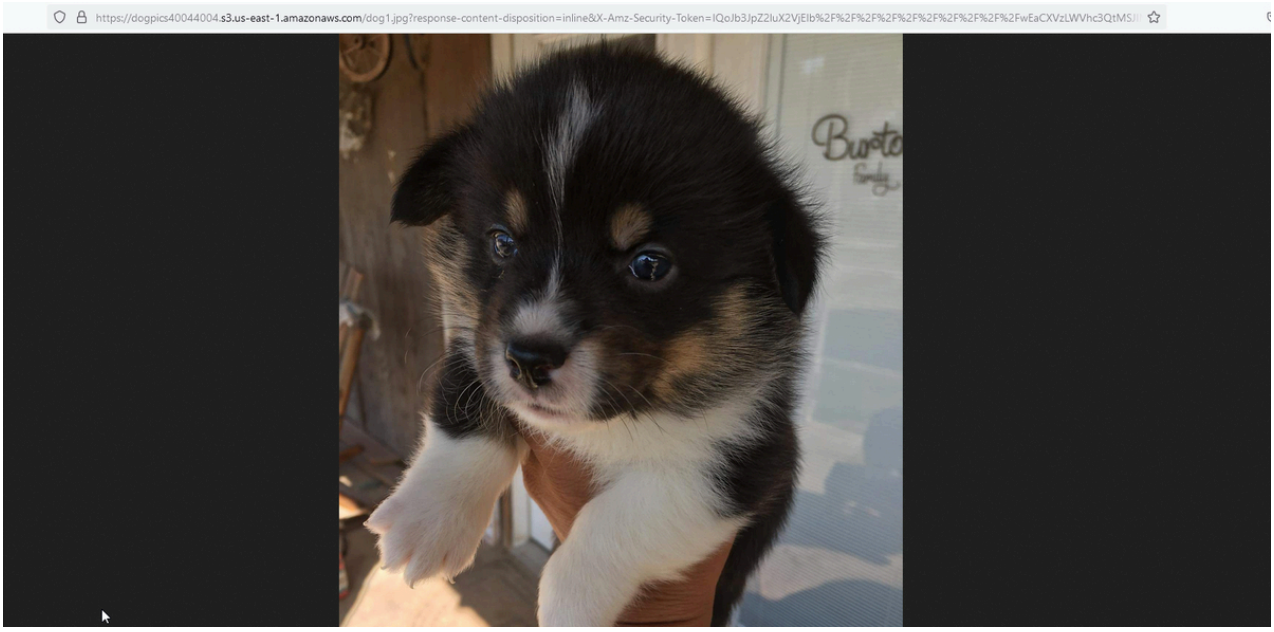

Tags - optional (0)
You can use bucket tags to track storage costs and organize buckets. Learn more
No tags associated with this bucket.
Add tag
Default encryption Info
Server-side encryption is automatically applied to new objects stored in this bucket.
Encryption type Info
Server-side encryption with Amazon S3 managed keys (SSE-S3)
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the Amazon S3 pricing page.
Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more
Disable
Enable
Advanced settings
After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.
Cancel
Create bucket


Amazon S3 > Buckets
Account snapshot
View Storage Lens dashboard
Buckets (1) Info
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
dogpics40044004
US East (N. Virginia) us-east-1
Bucket and objects not public
October 28, 2023, 16:26:51 (UTC-05:00)

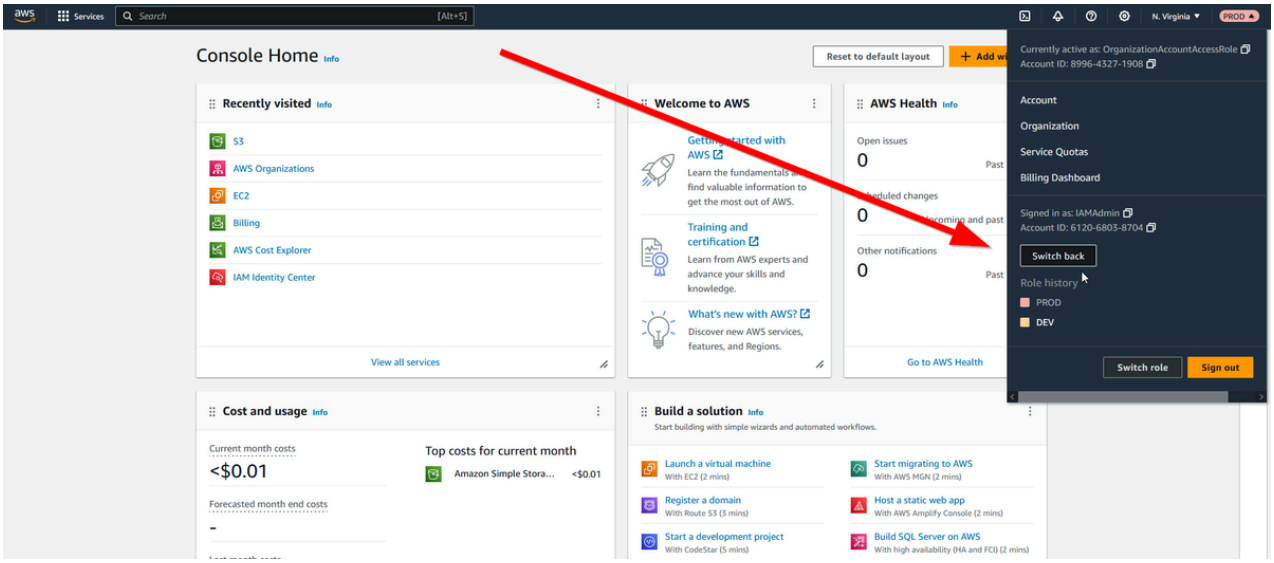

Amazon S3 > Buckets > dogpics40044004
dogpics40044004 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (0)
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
Name
Type
Last modified
Size
Storage class
No objects
You don't have any objects in this bucket.
Upload

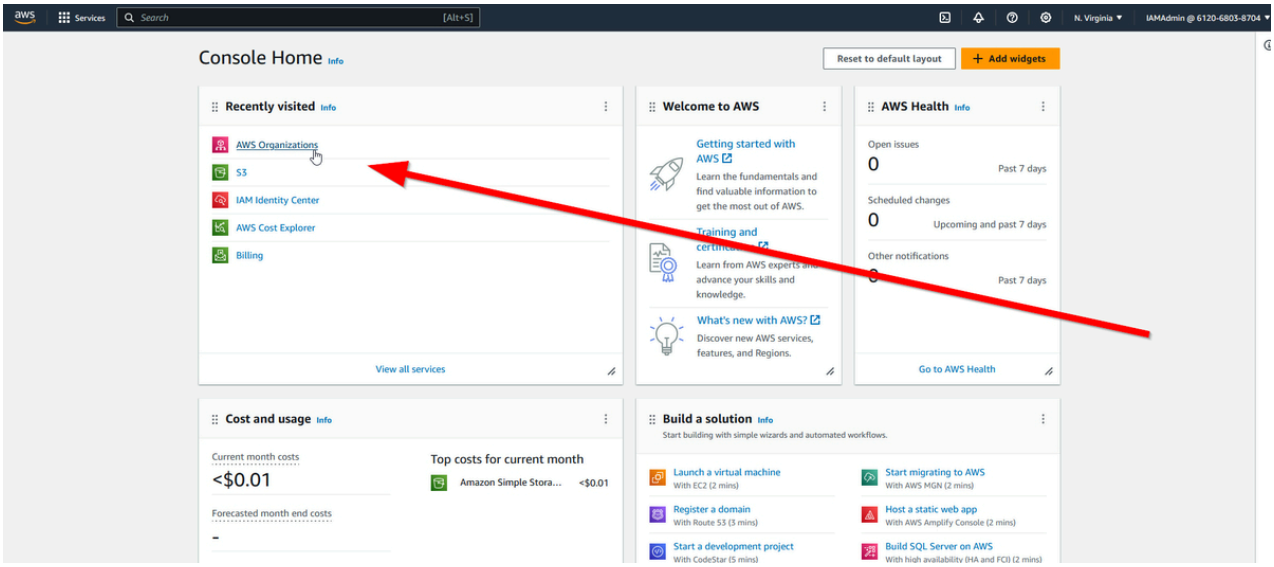

Upload succeeded
View details below.
Upload: status
Close
The information below will no longer be available after you navigate away from this page.
Summary
Destination
s3://dogpics40044004
Succeeded
1 file, 202.2 KB (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 Total, 202.2 KB)
Find by name
Name
Folder
Type
Size
Status
Error
dog1.jpg
image/jpeg
202.2 KB
Succeeded

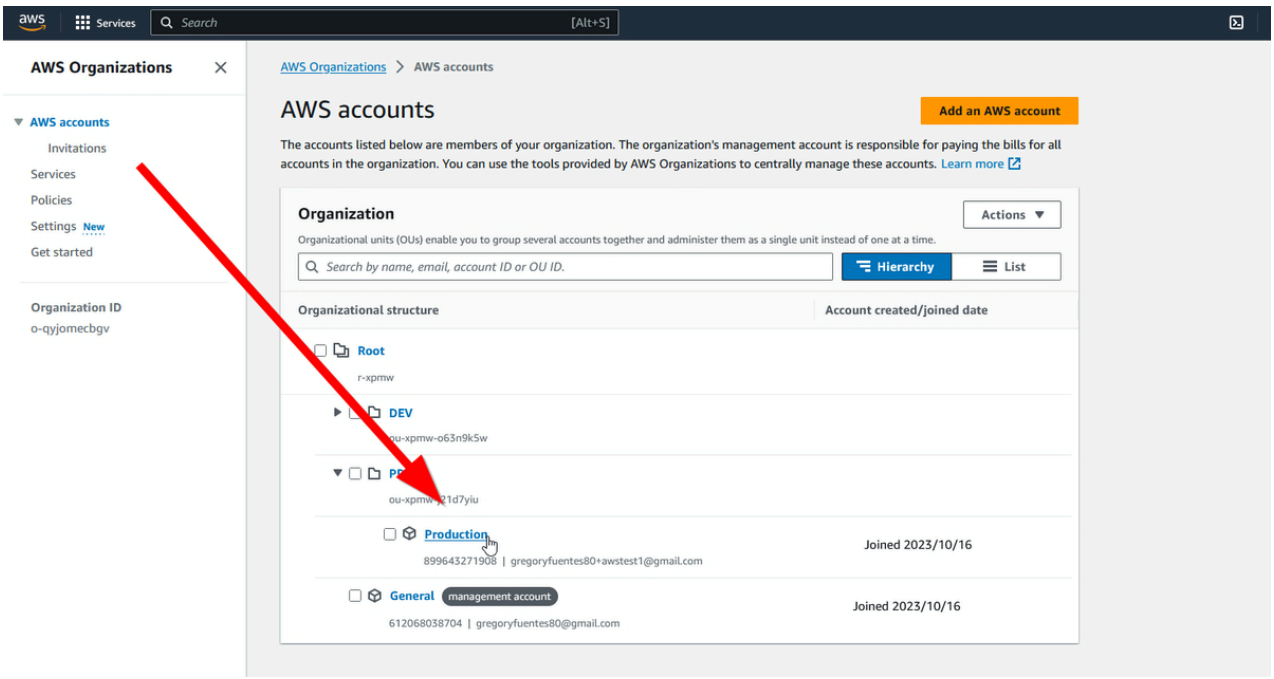

Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > dogpics40044004 > dog1.jpg
dog1.jpg Info
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Object overview
Owner
gregoryfuentes80+awstest1
AWS Region
US East (N. Virginia) us-east-1
Last modified
October 28, 2023, 16:28:47 (UTC-05:00)
Size
202.2 KB
Type
jpg
Key
dog1.jpg
S3 URI
s3://dogpics40044004/dog1.jpg
Amazon Resource Name (ARN)
arn:aws:s3:::dogpics40044004/dog1.jpg
Entity tag (Etag)
25c1f46bcb0964e66ba23ea418e7ac95
Object URL
https://dogpics40044004.s3.amazonaws.com/dog1.jpg
Object management overview
The following bucket properties and object management configurations impact the behavior of this object.
Bucket properties
Management configurations

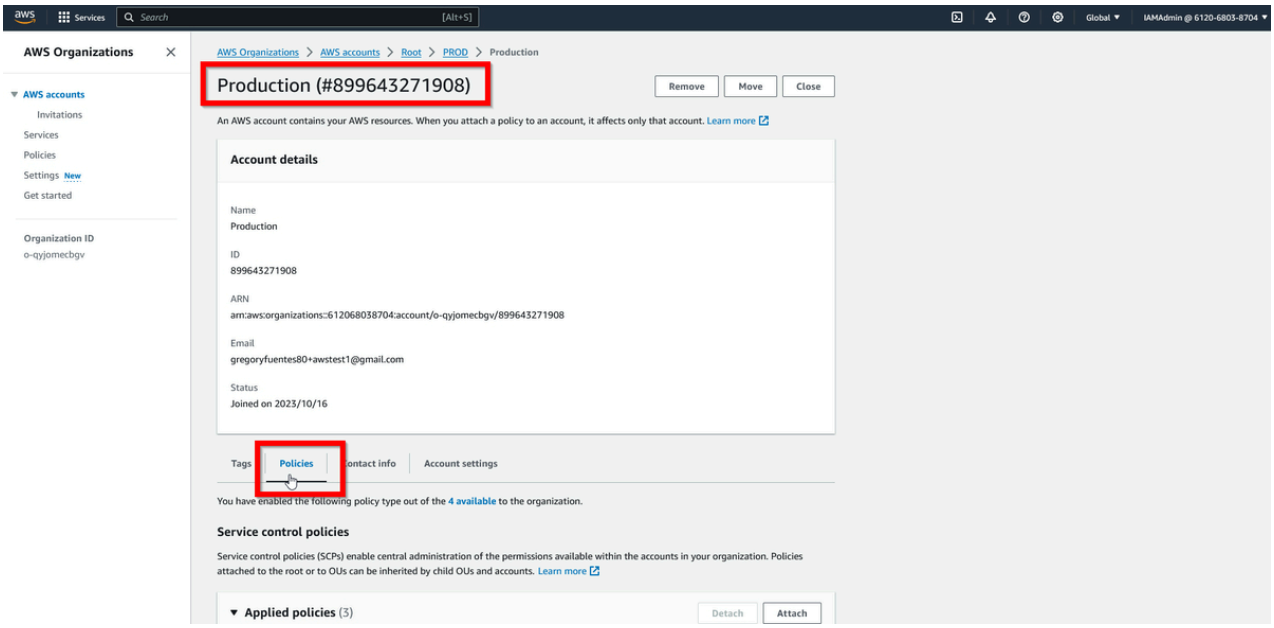

https://dogpics40044004.s3.us-east-1.amazonaws.com/dog1.jpg?response-content-disposition=inline&X-Amz-Security-Token=IQoJb3JpZ2luX2VjEIb%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCXVzLWVhc3QtMS

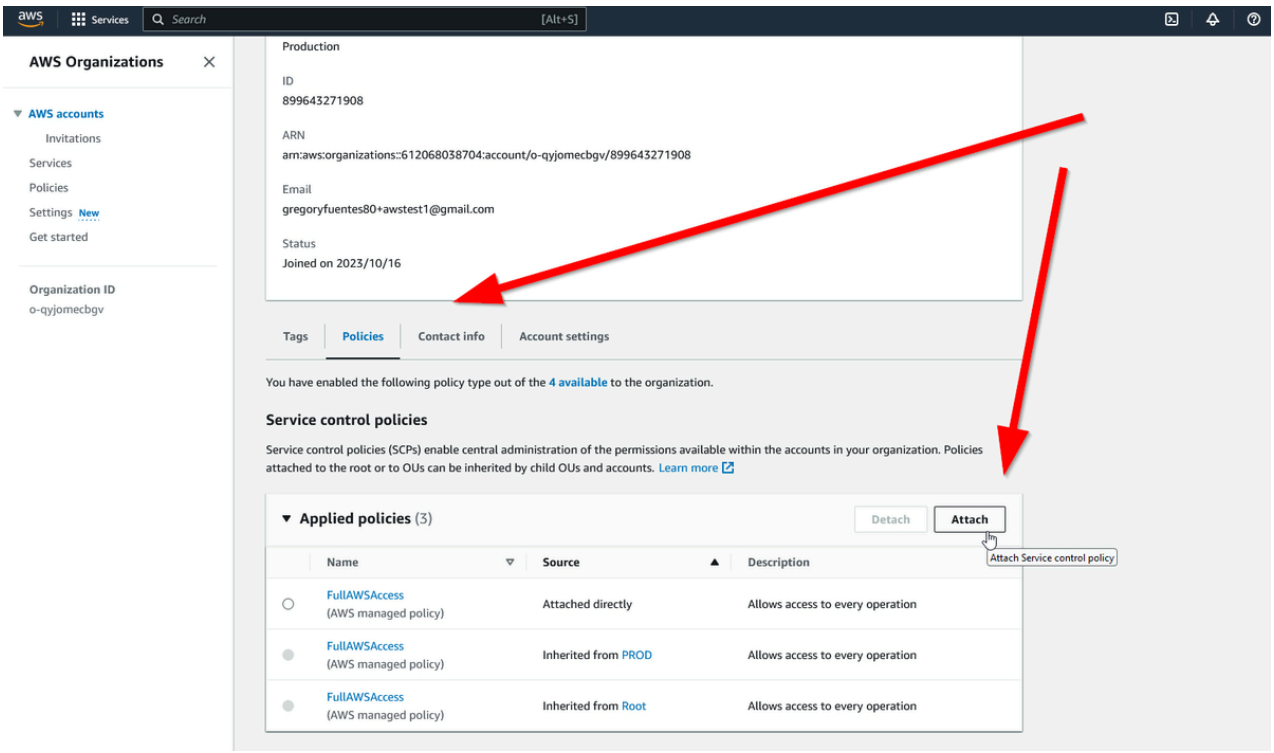
6. Finally, switch back to the AWS Organization management account and attach the denyS3.json policy to the AWS Member account "Production" as a Service Control Policy within the AWS Organization. Once attached, switch back to the AWS Member account "Production" and attempt to access the S3 bucket "dogpics" again but this with the denyS3 Service Control Policy attached.



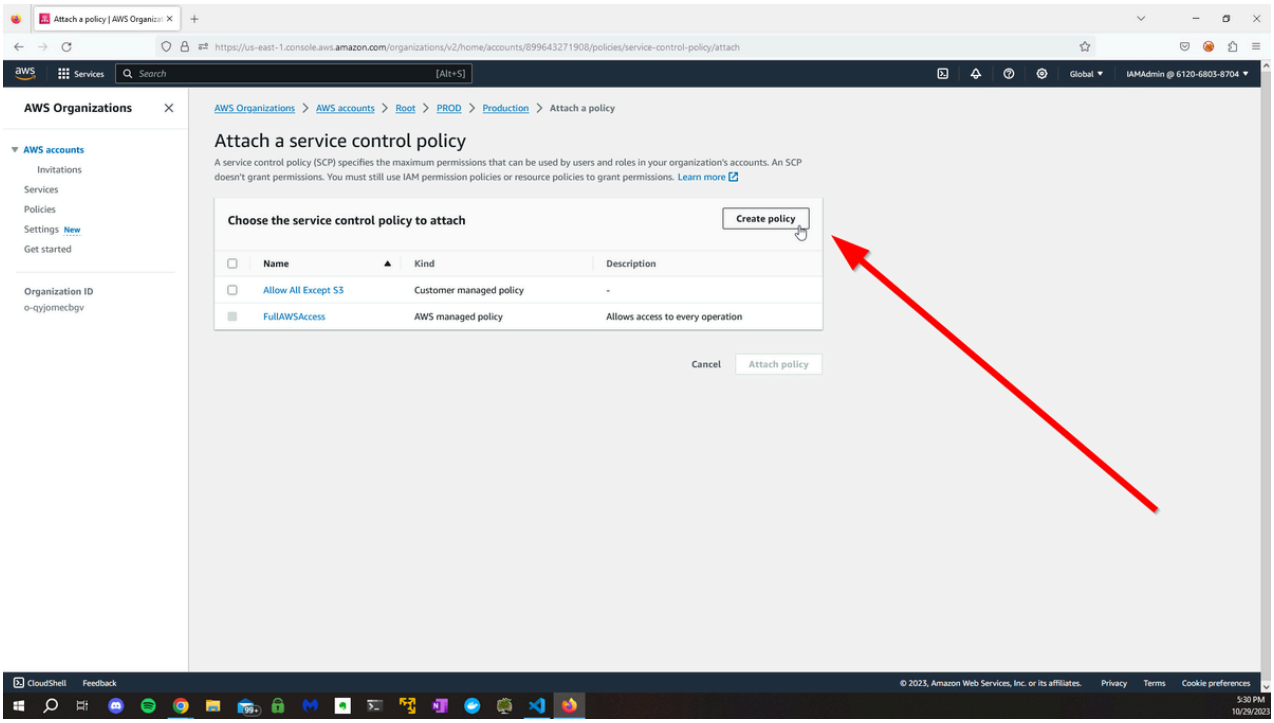


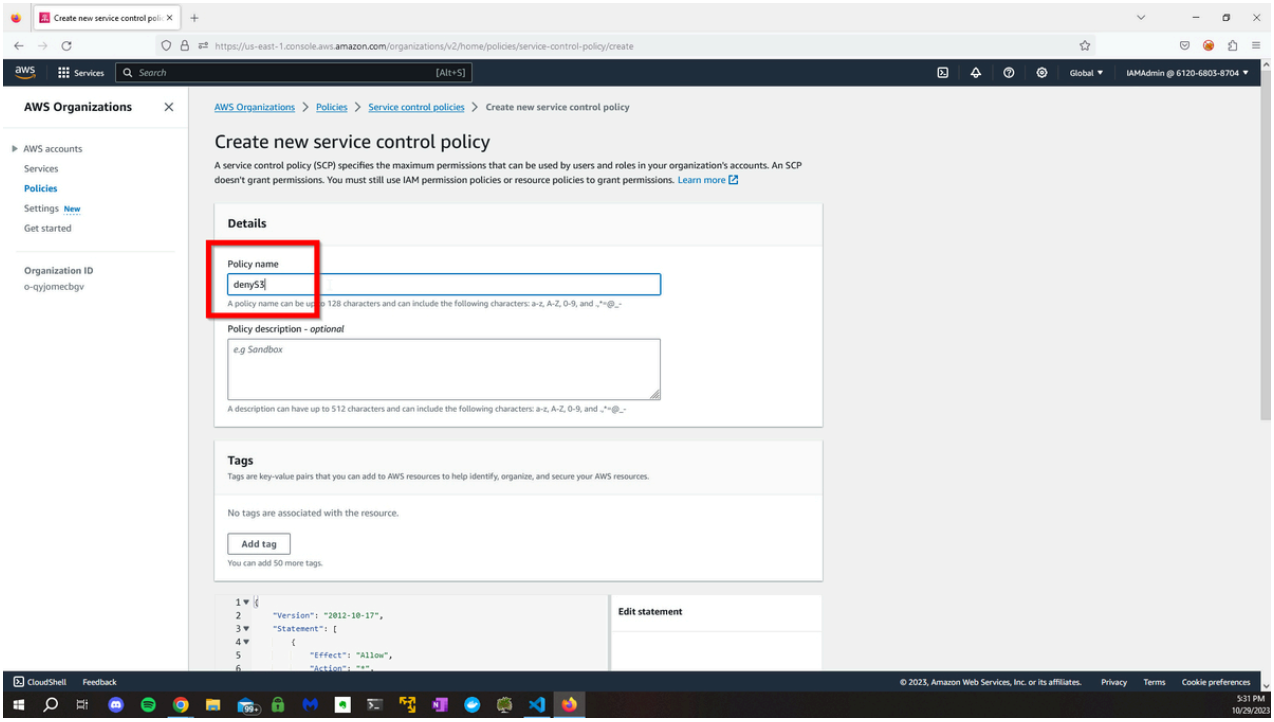

aws
Services
Search
[Alt+S]
AWS Organizations
AWS accounts
Invitations
Services
Policies
Settings New
Get started
Organization ID
o-qyjomecbgv
AWS Organizations > AWS accounts
AWS accounts
Add an AWS account
The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. Learn more
Organization
Actions
Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.
Search by name, email, account ID or OU ID.
Hierarchy
List
Organizational structure
Account created/joined date
Root
r-xpmw
DEV
ou-xpmw-o63n9k5w
ou-xpmw-q21d7yiu
Production
899643271908 | gregoryfuentes80+awstest1@gmail.com
Joined 2023/10/16
General
management account
612068038704 | gregoryfuentes80@gmail.com
Joined 2023/10/16

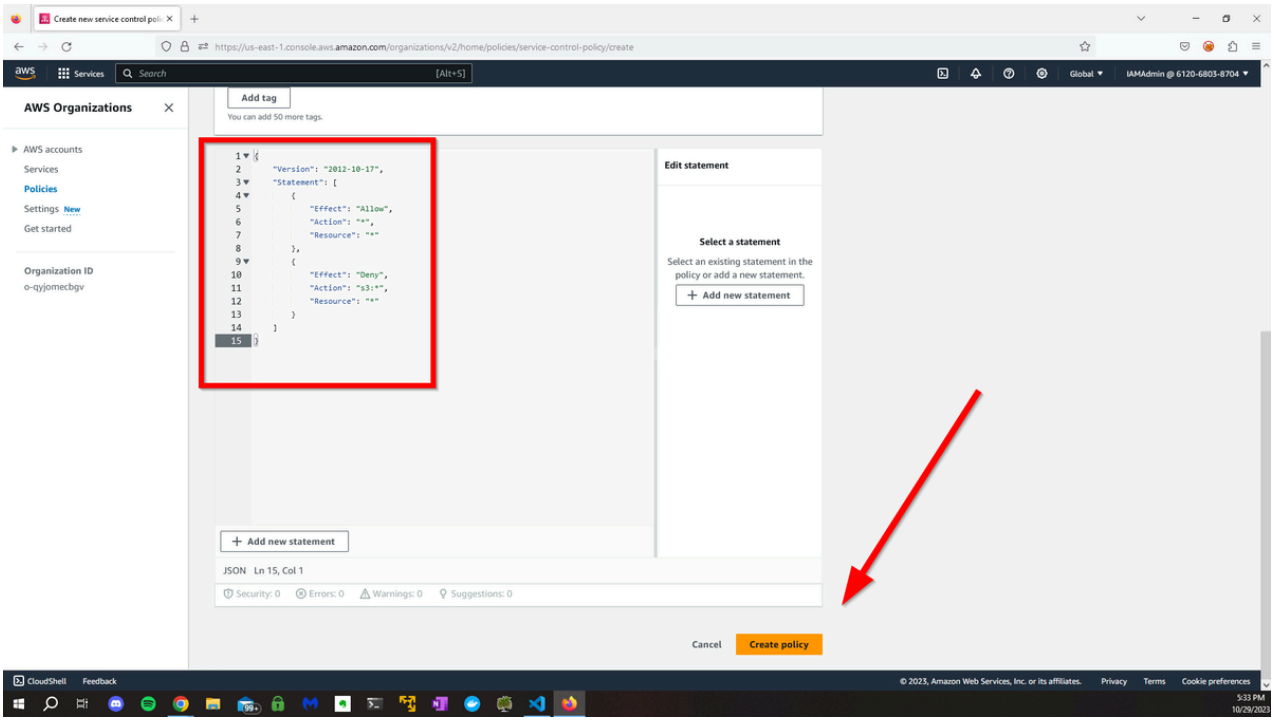

aws
Services
Search
[Alt+S]
Global
IAMAdmin @ 6120-6803-8704
AWS Organizations
AWS accounts
Invitations
Services
Policies
Settings New
Get started
Organization ID
o-qyjomecbgv
AWS Organizations > AWS accounts > Root > PROD > Production
Production (#899643271908)
Remove
Move
Close
An AWS account contains your AWS resources. When you attach a policy to an account, it affects only that account. Learn more
Account details
Name
Production
ID
899643271908
ARN
arn:aws:organizations::612068038704:account/o-qyjomecbgv/899643271908
Email
gregoryfuentes80+awstest1@gmail.com
Status
Joined on 2023/10/16
Tags
Policies
Contact info
Account settings
You have enabled the following policy type out of the 4 available to the organization.
Service control policies
Service control policies (SCPs) enable central administration of the permissions available within the accounts in your organization. Policies attached to the root or to OUs can be inherited by child OUs and accounts. Learn more
Applied policies (3)
Detach
Attach

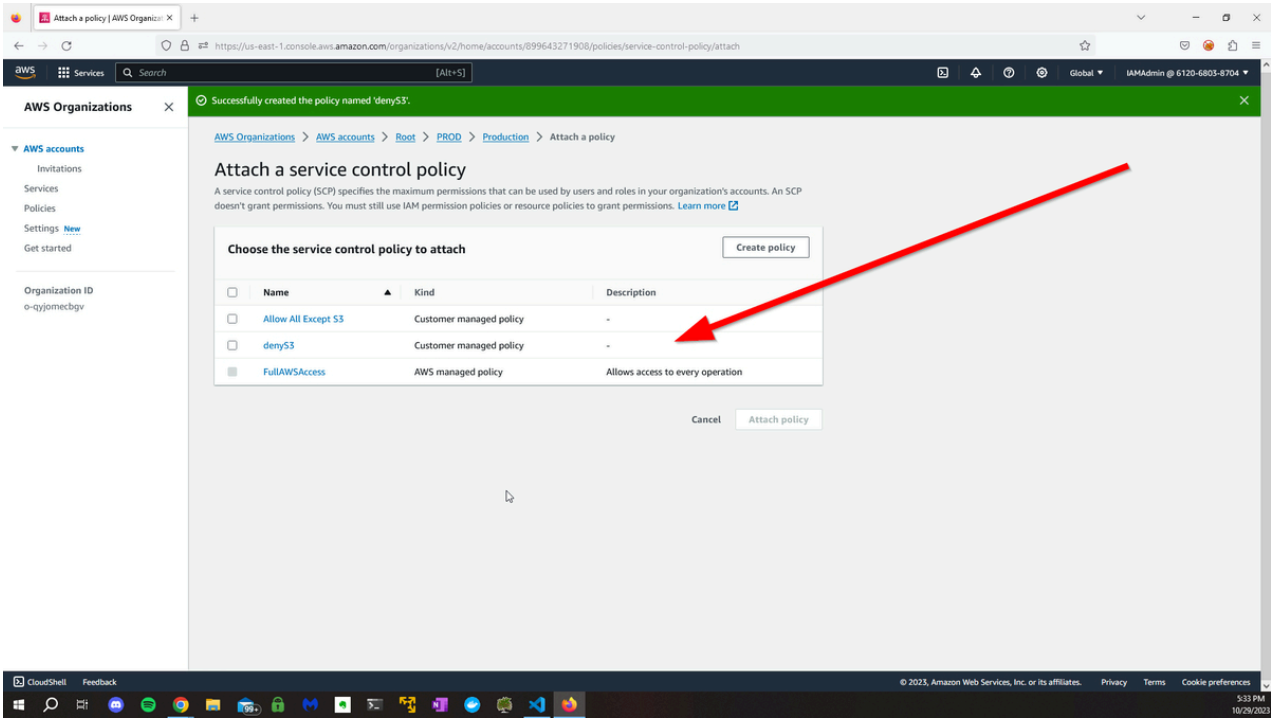


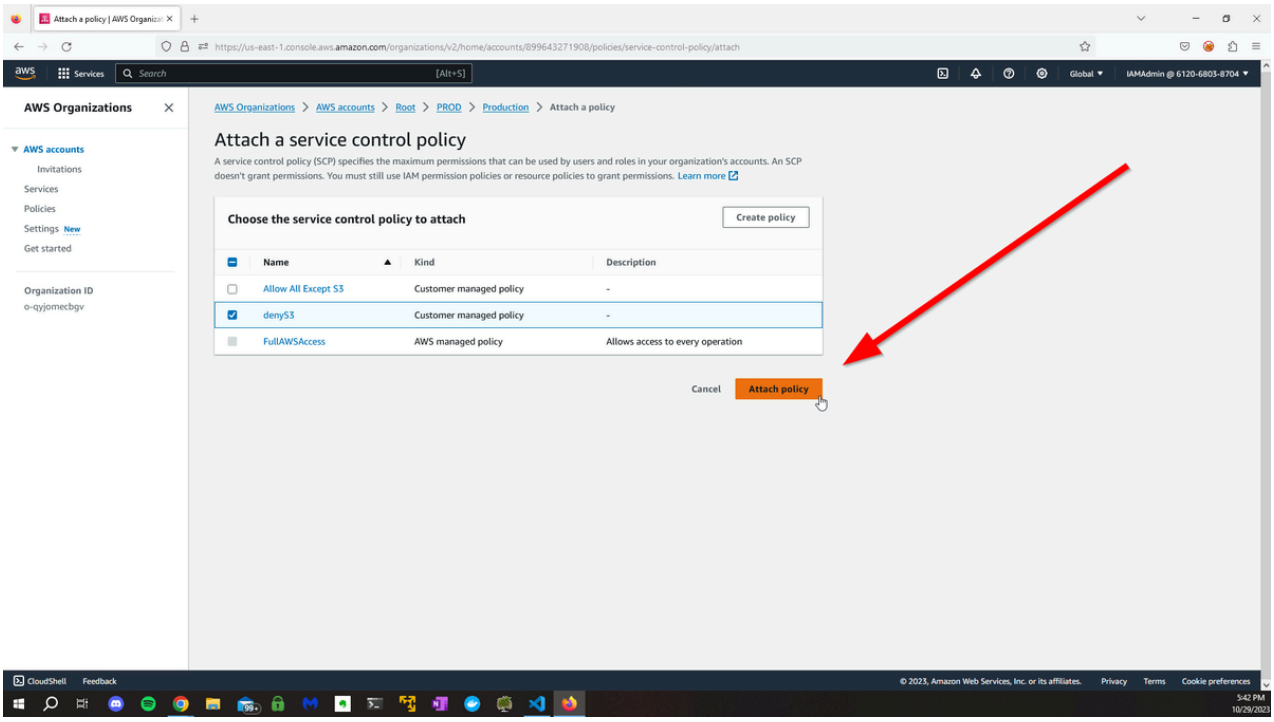
Notice that you will most likely need to create the policy if not already created to deny S3 events within the AWS Organization "Production" account with the denyS3.json SCP.

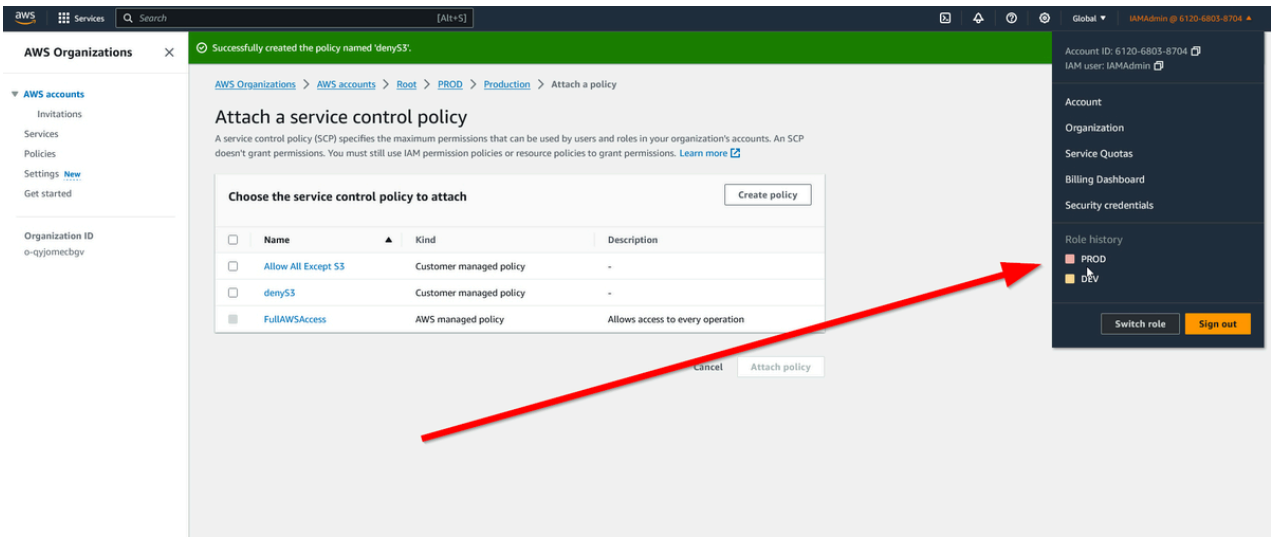


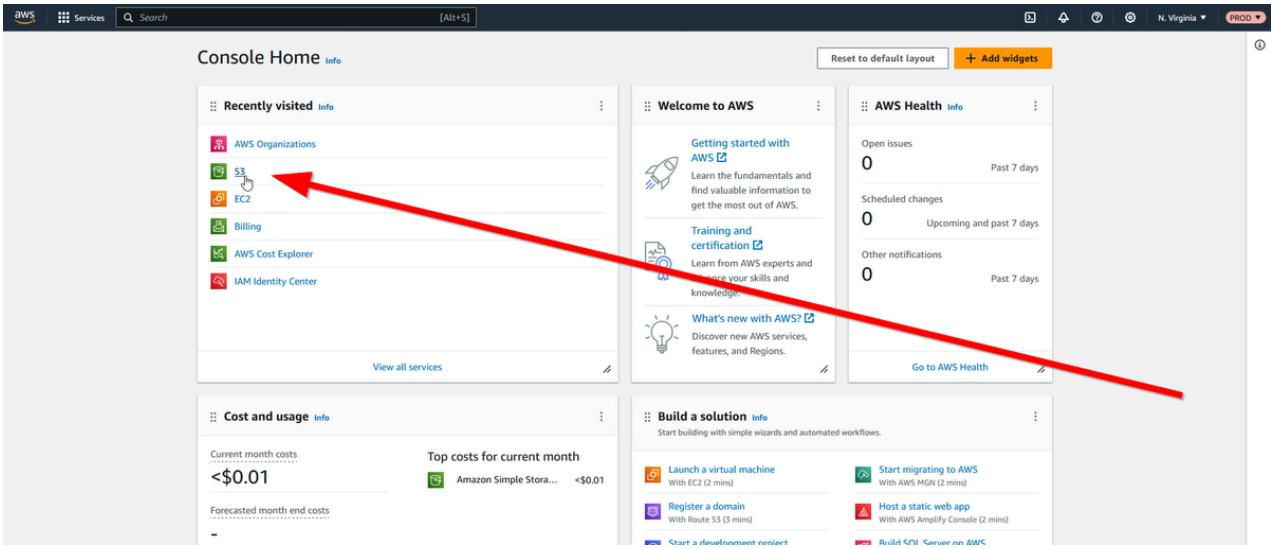

AWS Organizations
AWS accounts
Services
Policies
Settings New
Get started
Organization ID
o-qyjomecbgv
AWS Organizations > Policies > Service control policies > Create new service control policy
Create new service control policy
A service control policy (SCP) specifies the maximum permissions that can be used by users and roles in your organization's accounts. An SCP doesn't grant permissions. You must still use IAM permission policies or resource policies to grant permissions. Learn more
Details
Policy name
denyS3
Policy description - optional
e.g Sandbox
Tags
Tags are key-value pairs that you can add to AWS resources to help identify, organize, and secure your AWS resources.
No tags are associated with the resource.
Add tag
You can add 50 more tags.
Edit statement
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

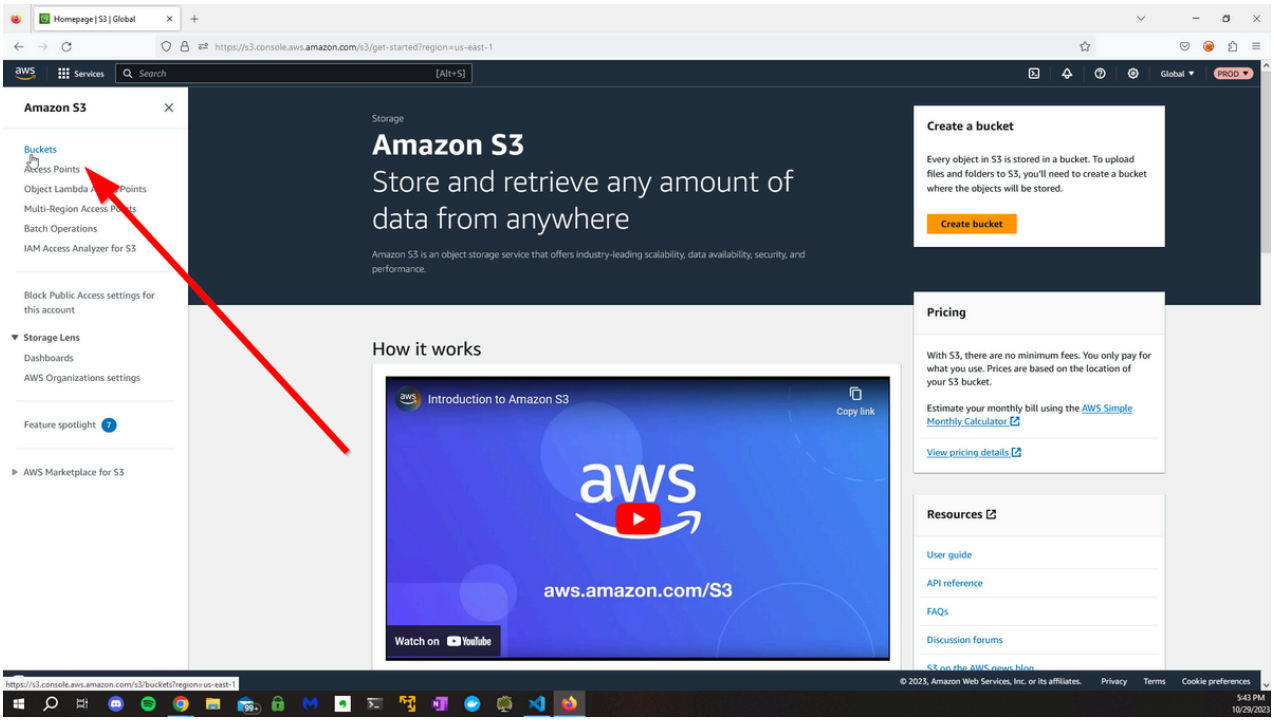

AWS Organizations
Add tag
You can add 50 more tags.
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
Add new statement
Add new statement
JSON Ln 15, Col 1
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
Cancel
Create policy
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


AWS Organizations
Successfully created the policy named 'denyS3'.
AWS Organizations > AWS accounts > Root > PROD > Production > Attach a policy
Attach a service control policy
A service control policy (SCP) specifies the maximum permissions that can be used by users and roles in your organization's accounts. An SCP doesn't grant permissions. You must still use IAM permission policies or resource policies to grant permissions. Learn more
Choose the service control policy to attach
Create policy
Name
Kind
Description
Allow All Except S3
Customer managed policy
denyS3
Customer managed policy
FullAWSAccess
AWS managed policy
Allows access to every operation
Cancel
Attach policy


AWS Organizations
AWS Organizations > AWS accounts > Root > PROD > Production > Attach a policy
Attach a service control policy
A service control policy (SCP) specifies the maximum permissions that can be used by users and roles in your organization's accounts. An SCP doesn't grant permissions. You must still use IAM permission policies or resource policies to grant permissions. Learn more
Choose the service control policy to attach
Create policy
Name
Kind
Description
Allow All Except S3
Customer managed policy
denyS3
Customer managed policy
FullAWSAccess
AWS managed policy
Allows access to every operation
Cancel
Attach policy


Successfully created the policy named 'denyS3'.
AWS Organizations > AWS accounts > Root > PROD > Production > Attach a policy
Attach a service control policy
Choose the service control policy to attach
Create policy
Name
Kind
Description
Allow All Except S3
Customer managed policy
denyS3
Customer managed policy
FullAWSAccess
AWS managed policy
Allows access to every operation
Cancel
Attach policy
Account
Organization
Service Quotas
Billing Dashboard
Security credentials
Role history
PROD
DEV
Switch role
Sign out


Console Home
Reset to default layout
+ Add widgets
Recently visited
AWS Organizations
S3
EC2
Billing
AWS Cost Explorer
IAM Identity Center
View all services
Welcome to AWS
Getting started with AWS
Training and certification
What's new with AWS?
AWS Health
Open issues
0
Past 7 days
Scheduled changes
0
Upcoming and past 7 days
Other notifications
0
Past 7 days
Go to AWS Health
Cost and usage
Current month costs
<$0.01
Top costs for current month
Forecasted month end costs
Build a solution
Launch a virtual machine
Start migrating to AWS
Register a domain
Host a static web app


Amazon S3
Buckets
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
AWS Marketplace for S3
Storage
Amazon S3
Store and retrieve any amount of data from anywhere
Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.
Create a bucket
Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.
Create bucket
Pricing
With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.
Estimate your monthly bill using the AWS Simple Monthly Calculator
View pricing details
How it works
Introduction to Amazon S3
Copy link
aws.amazon.com/S3
Watch on YouTube
Resources
User guide
API reference
FAQs
Discussion forums

Finally, the following error message in the AWS Organization "Production" account proves that the attached SCP denyS3 is denying any S3 events including accessing or even listing the S3 "dogpics" bucket. As a result, this shows the efficiency of limiting what accounts or OUs can do in AWS Organization using Service Control Policies by extending the Principle of Least Privilege within AWS.