

# 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

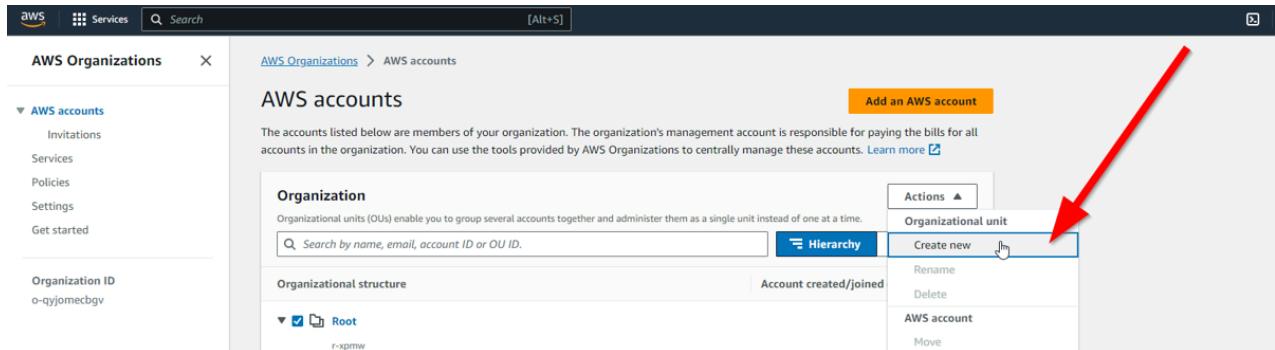
The following walkthrough will go through how to apply an AWS Service Control Policy on an AWS Organization Account in this case, the AWS "PROD" account, and to test the capability of the policy.

- 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": "*"
        }
    ]
}
```

```

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



AWS Organizations > AWS accounts > Root > Create organizational unit

### Create organizational unit in Root

An organizational unit (OU) can contain both accounts and other OUs. This enables you to create an inverted tree hierarchy. The structure has a root at the top and branches of OUs that reach down. The branches end in accounts that act as the leaves of the tree. [Learn more](#)

**Details**

Organizational unit name  
DEV

An OU name can be up to 128 characters.

**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.

Cancel Create organizational unit

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

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**

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Actions ▾

Search by name, email, account ID or OU ID.

Hierarchy List

Organizational structure Account created/joined date

- Root
  - DEV
    - ou-xpmw-o63n9k5w
  - PROD
    - ou-xpmw-j21d7ylu
  - Development
    - 284073959379 | gregoryfuentes80+development@gmail.com Created 2023/10/16
  - General management account
    - 612068038704 | gregoryfuentes80@gmail.com Joined 2023/10/16
  - Production
    - 899643271908 | gregoryfuentes80+awstest1@gmail.com Joined 2023/10/16

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

**AWS Organizations**

**AWS accounts**

- Invitations
- Services
- Policies
- Settings
- Get started

Organization ID  
o-qjomecbgv

**AWS accounts**

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**

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

**Actions**

**Organizational unit**

- Create new
- Rename
- Delete

**AWS account**

- Move** 
- Remove from organization
- Export account list

**Hierarchy**

**Organizational structure**

**Account created/joined**

**Root**

- DEV**
- PROD**
- Development**  284073959379 | gregoryfuentes80+development@gmail.com Created 2023/10/16
- General management account**  612068038704 | gregoryfuentes80@gmail.com Joined 2023/10/16
- Production**  899643271908 | gregoryfuentes80+awstest1@gmail.com Joined 2023/10/16

**AWS Organizations**

**AWS accounts**

- Invitations
- Services
- Policies
- Settings
- Get started

Organization ID  
o-qjomecbgv

**AWS accounts > AWS accounts > Root > Development > Move AWS account**

### Move AWS account 'Development'

When you move an AWS account from one organization unit (OU) to another, it changes the policies that apply to the account. This can change the permissions for the account and how supported AWS services can interact with the account. [Learn more](#)

**AWS account to be moved**

| Account name       | Account ID   | Email                                  |
|--------------------|--------------|--|
| <b>Development</b> | 284073959379 | gregoryfuentes80+development@gmail.com |

**Destination**

Select root or organizational unit that account should be moved to.

**Organizational structure**

**Root**

- DEV**
- PROD**

**Move AWS account** 

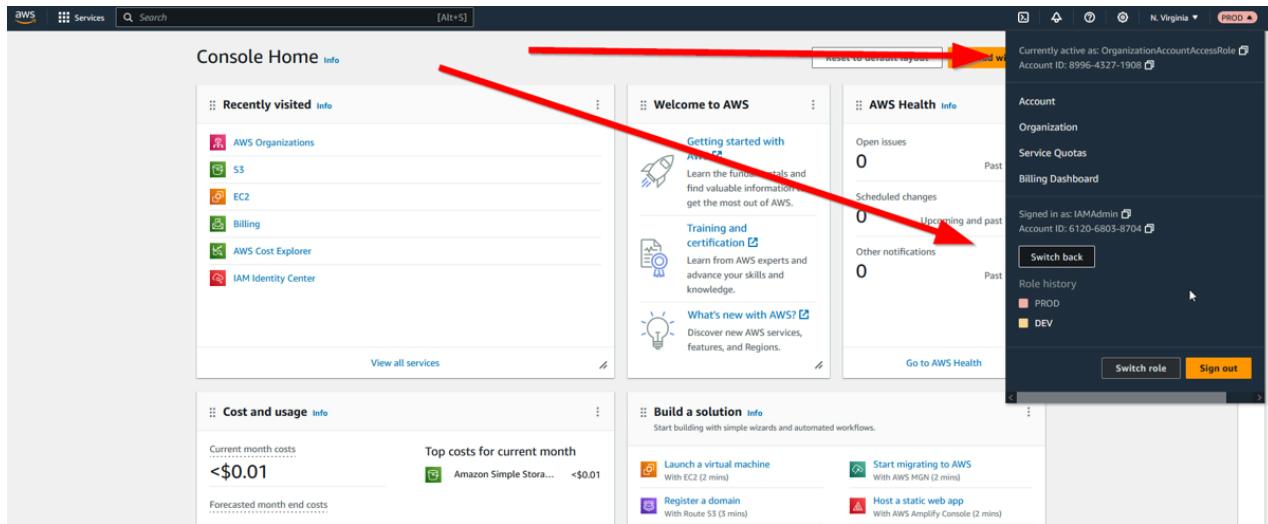
Finally, this is what the AWS Organization should look like after moved the respective AWS Organization member accounts into the AWS Organization Units.

The screenshot shows the AWS Organizations AWS accounts page. On the left, there's a sidebar with 'AWS Organizations' and 'AWS accounts' sections. The main area displays the 'AWS accounts' section with the title 'AWS accounts'. It says, '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.' There's a search bar, a 'Hierarchy' button, and a 'List' button. The account structure is as follows:

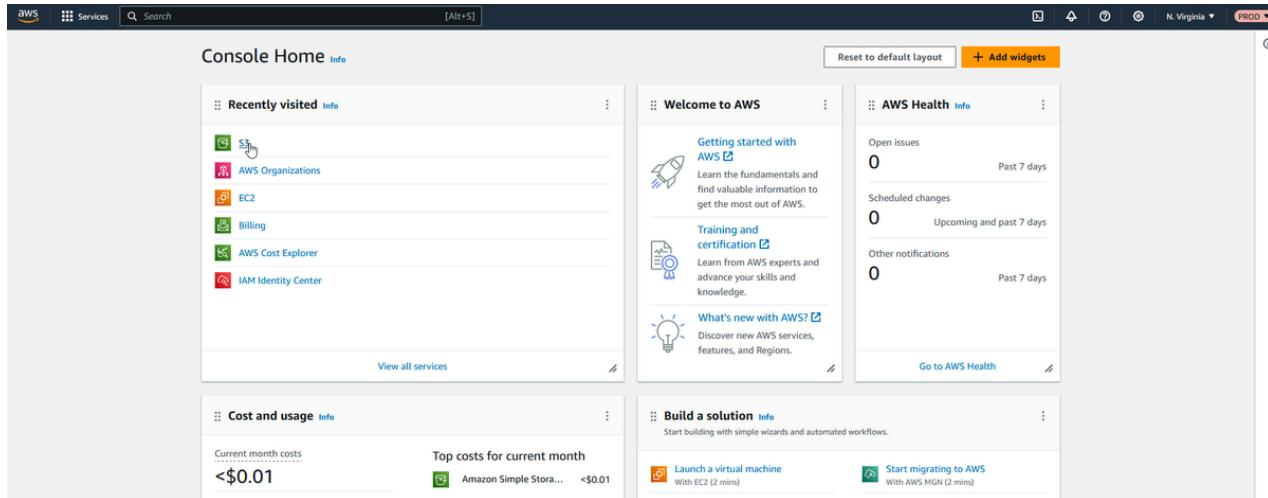
- Root** (r-xpmw)
  - DEV** (ou-xpmw-o63n9k5w)
    - Development** (Created 2023/10/16) - Account ID: 284073959379 | gregoryfuentes80+development@gmail.com
  - PROD** (ou-xpmw-j21d7yiu)
    - Production** (Joined 2023/10/16) - Account ID: 899643271908 | gregoryfuentes80+awstest1@gmail.com
  - General** (management account) (Joined 2023/10/16) - Account ID: 612068038704 | gregoryfuentes80@gmail.com

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.

The screenshot shows the same AWS Organizations AWS accounts page as before, but with a red arrow pointing from the 'Switch role' button in the sidebar to the 'PROD' account entry in the hierarchy. The sidebar also shows the account ID (612068038704) and IAM user (IAMAdmin). The 'Role history' section shows entries for 'DEV' and 'PROD', with 'PROD' being the current selection. The 'Switch role' button is highlighted with a red arrow.



- 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.



The screenshot shows the Amazon S3 landing page. At the top right, there is a call-to-action box titled "Create a bucket" with a large orange "Create bucket" button. This button is highlighted with a red rectangular box. Below the main heading "Amazon S3" and sub-heading "Store and retrieve any amount of data from anywhere", there is a section titled "How it works" featuring a video thumbnail. To the right of the main content area, there are sections for "Pricing" and "Resources".

The screenshot shows the "Create bucket" configuration page. The "General configuration" section is visible, containing fields for "Bucket name" (set to "dogpics40044004") and "AWS Region" (set to "US East (N. Virginia) us-east-1"). A red box highlights the "Bucket name" input field. Below these, there is a section for "Copy settings from existing bucket - optional" with a "Choose bucket" button. The "Object Ownership" section follows, with two options: "ACLs disabled (recommended)" (selected) and "ACLs enabled".

The screenshot shows the 'Advanced settings' section of the AWS S3 Bucket creation wizard. It includes fields for 'Encryption type' (set to 'Server-side encryption with Amazon S3 managed keys (SSE-S3)'), 'Bucket Key' (set to 'Enable'), and a note about uploading files and configuring additional settings. A red arrow points from the top right towards the 'Create bucket' button.

**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](#)

The screenshot shows the 'Buckets (1) info' section of the AWS S3 Buckets list. A red box highlights the first row, which contains the bucket name 'dogpics40044004'. A red arrow points from the top right towards the 'Create bucket' button in the header.

**Account snapshot**  
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

**Buckets (1) info**  
Buckets are containers for data stored in S3. [Learn more](#)

| 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) |

[View Storage Lens dashboard](#)

[Create bucket](#)

The screenshot shows the 'Objects (0)' section of the AWS S3 Bucket properties page for 'dogpics40044004'. A red box highlights the 'Upload' button. A red arrow points from the bottom right towards the 'Upload' button.

**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](#)

[Actions](#) [Create folder](#) [Upload](#)

| Name   | Type | Last modified | Size | Storage class |
|--|------|---------------|------|---------------|
| No objects<br>You don't have any objects in this bucket. |      |               |      |               |

**Upload succeeded**  
View details below.

### Upload: status

The information below will no longer be available after you navigate away from this page.

| Summary  | Succeeded                         | Failed            |
|--|-----------------------------------|-------------------|
| Destination<br><code>s3://dogpics40044004</code> | <b>1 file, 202.2 KB (100.00%)</b> | 0 files, 0 B (0%) |

**Files and folders** Configuration

**Files and folders (1 Total, 202.2 KB)**

| Name     | Folder | Type       | Size     | Status           | Error |
|----------|--------|------------|----------|------------------|-------|
| dog1.jpg | -      | image/jpeg | 202.2 KB | <b>Succeeded</b> | -     |

**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](#)

[Properties](#) [Permissions](#) [Versions](#)

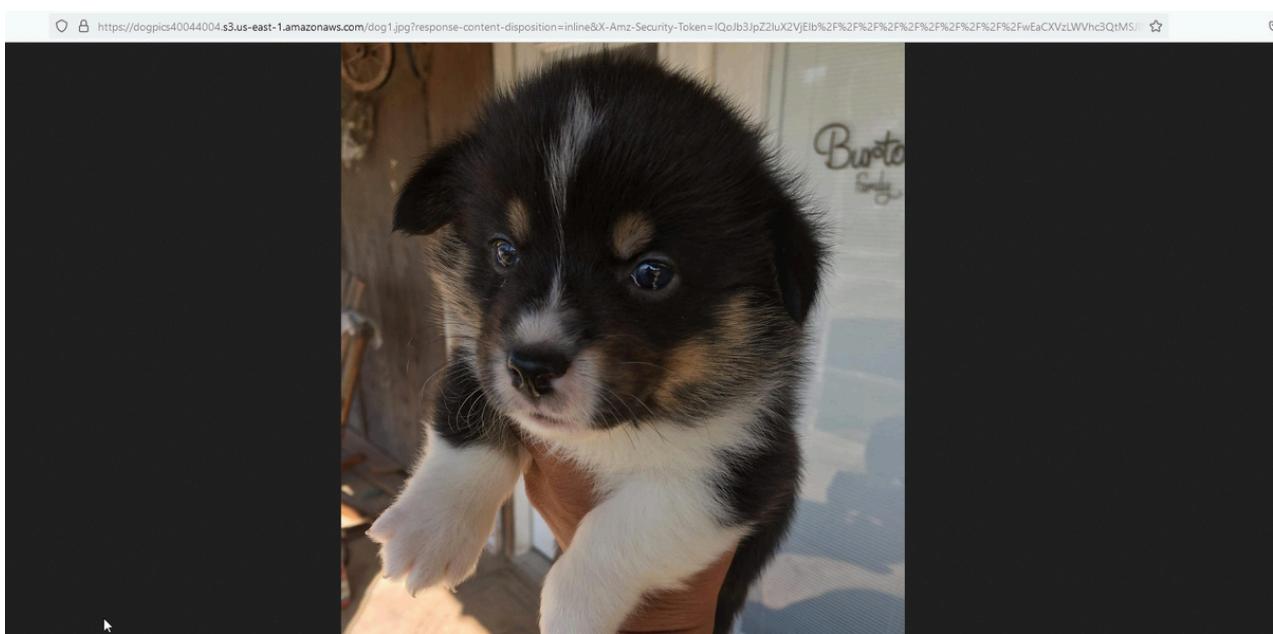
**Object overview**

|               |  |                            |   |
|---------------|--|----------------------------|---|
| Owner         | gregoryfuentes80+awstest1              | S3 URI                     | <a href="https://s3://dogpics40044004/dog1.jpg">s3://dogpics40044004/dog1.jpg</a>                                 |
| AWS Region    | US East (N. Virginia) us-east-1        | Amazon Resource Name (ARN) | <a href="#">arn:aws:s3:::dogpics40044004/dog1.jpg</a>   |
| Last modified | October 28, 2023, 16:28:47 (UTC-05:00) | Entity tag (Etag)          | <a href="#">25c1f46bcb0964e66ba23ea418e7ac95</a>  |
| Size          | 202.2 KB                               | Object URL                 | <a href="https://dogpics40044004.s3.amazonaws.com/dog1.jpg">https://dogpics40044004.s3.amazonaws.com/dog1.jpg</a> |
| Type          | jpg                                    |                            |   |
| Key           | <a href="#">dog1.jpg</a>               |                            |   |

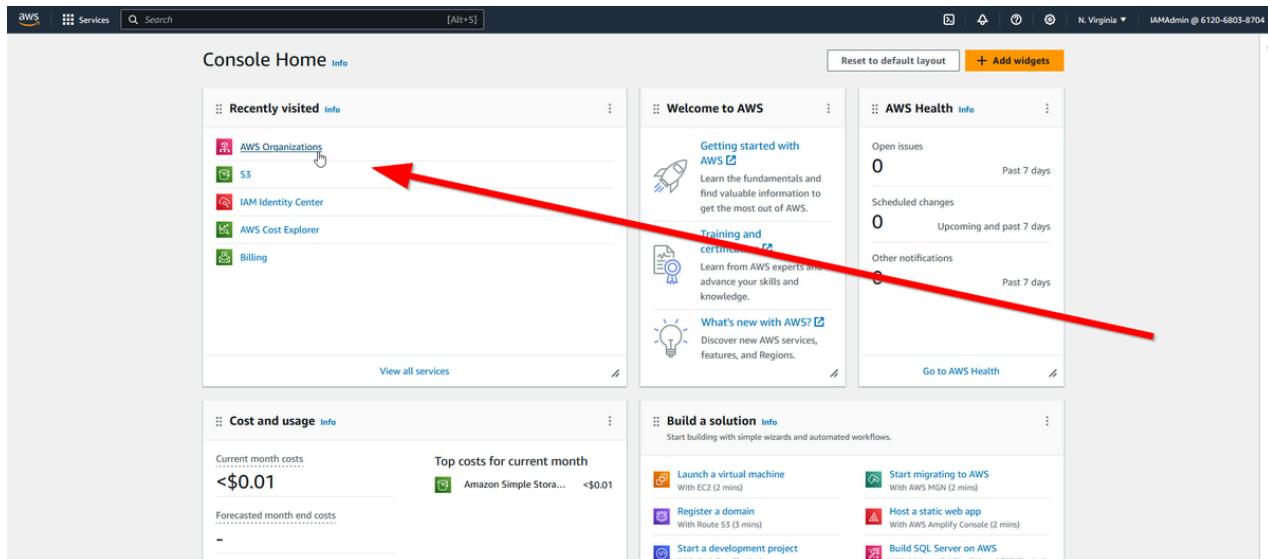
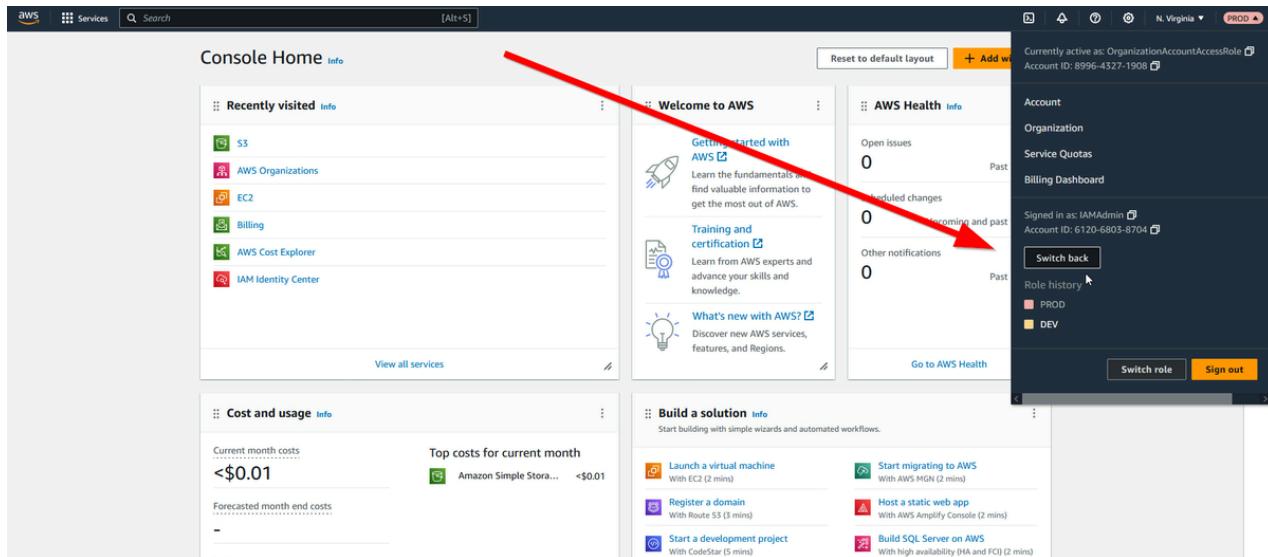
**Object management overview**

The following bucket properties and object management configurations impact the behavior of this object.

**Bucket properties** **Management configurations**



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 Organizations**

**AWS accounts**

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**

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

**Actions**

**Hierarchy** **List**

**Organizational structure**

**Account created/joined date**

- Root** r-xpmw
- DEV** ou-xpmw-o63n9k5w
- PROD** ou-xpmw-z1d7yiu
  - Production** #899643271908 | gregoryfuentes80+awstest1@gmail.com  
Joined 2023/10/16
  - General** management account 612068038704 | gregoryfuentes80@gmail.com  
Joined 2023/10/16

**AWS Organizations**

**AWS accounts**

**Production (#899643271908)**

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: am:aws:organizations::612068038704:account/o-qjomecbgv/899643271908  
Email: gregoryfuentes80+awstest1@gmail.com  
Status: Joined on 2023/10/16

**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**

AWS Organizations

**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)**

| Name                               | Source              | Description                      |
|------------------------------------|---------------------|----------------------------------|
| FullAWSAccess (AWS managed policy) | Attached directly   | Allows access to every operation |
| FullAWSAccess (AWS managed policy) | Inherited from PROD | Allows access to every operation |
| FullAWSAccess (AWS managed policy) | Inherited from Root | Allows access to every operation |

Detach Attach Attach Service control policy

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 > 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

| Name                | Kind                    | Description                      |
|---------------------|-------------------------|----------------------------------|
| Allow All Except S3 | Customer managed policy | -                                |
| FullAWSAccess       | AWS managed policy      | Allows access to every operation |

Create policy Cancel Attach policy

```

1 /**
2  * Version: "2012-10-17",
3  * Statement: [
4  *   {
5  *     "Effect": "Allow",
6  *     "Action": "*",
7  *     "Resource": "*"
8  *   },
9  *   {
10 *     "Effect": "Deny",
11 *     "Action": "s3:*",
12 *     "Resource": "*"
13 *   }
14 ]
15 */

```

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

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

| 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**

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

| Name                                       | Kind                    | Description                      |
|--|-------------------------|----------------------------------|
| Allow All Except S3                        | Customer managed policy | -                                |
| <input checked="" type="checkbox"/> denyS3 | Customer managed policy | -                                |
| FullAWSAccess                              | AWS managed policy      | Allows access to every operation |

Cancel **Attach policy**

Successfully created the policy named 'denyS3'.

**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**

| Name                | Kind                    | Description                      |
|---------------------|-------------------------|----------------------------------|
| Allow All Except S3 | Customer managed policy |                                  |
| denyS3              | Customer managed policy |                                  |
| FullAWSAccess       | AWS managed policy      | Allows access to every operation |

**Create policy**

**Cancel** **Attach policy**

Account ID: 6120-6803-8704  
IAM user: IAMAdmin

Global Account Organization Service Quotas Billing Dashboard Security credentials Role history PROD DEV Switch role Sign out

Console Home

Recently visited

- AWS Organizations
- S3
- EC2
- Billing
- AWS Cost Explorer
- IAM Identity Center

Cost and usage

Current month costs: <\$0.01

Top costs for current month: Amazon Simple Storage Service <\$0.01

Forecasted month end costs: -

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

Build a solution

Launch a virtual machine With EC2 (2 mins)

Start migrating to AWS With AWS MGN (2 mins)

Register a domain With Route 53 (3 mins)

Host a static web app With AWS Amplify Console (2 mins)

Start a development instance With Lambda (1 min)

Amazon 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.

How it works

Watch on YouTube

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

User guide

API reference

Faqs

Discussion forums

[\\$3 on the AWS news blog](#)

https://s3.console.aws.amazon.com/s3/buckets/?region=us-east-1

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

5:43 PM 10/29/2023

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 "doggpics" 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.

The screenshot shows the AWS S3 Buckets page. The left sidebar includes links for 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, and AWS Marketplace for S3. The main content area has a header for 'Account snapshot' and a 'Buckets' section. The 'Buckets' section includes a search bar, buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket', and a table with columns for Name, AWS Region, Access, and Creation date. A red-bordered error message box at the bottom states: 'You don't have permissions to list buckets. After you or your AWS administrator has updated your permissions to allow the s3>ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3.'