



# AWS Organizations

AWS Organizations is a service provided by Amazon Web Services (AWS) that allows you to centrally manage and govern multiple AWS accounts. It helps you organize your accounts into a hierarchical structure called an organization and offers tools for managing policies, permissions, and billing.

## Key Features of AWS Organizations:

1. **Centralized Management:** It lets you manage multiple AWS accounts from a single location, making it easier to set up and govern your AWS environment.
2. **Consolidated Billing:** You can consolidate billing for multiple AWS accounts into a single payment, which can help simplify tracking costs and optimize spending.
3. **Policy Management:** AWS Organizations allows you to apply policies across accounts, such as security and compliance requirements. These policies can control what actions can be performed within each account.
4. **Account Grouping:** You can group accounts into organizational units (OUs) and apply policies to these units, simplifying management.
5. **Resource Sharing:** The service enables sharing resources across accounts, such as AWS License Manager licenses or AWS Transit Gateway, without needing to create duplicate resources in each account.

## Why Use AWS Organizations?

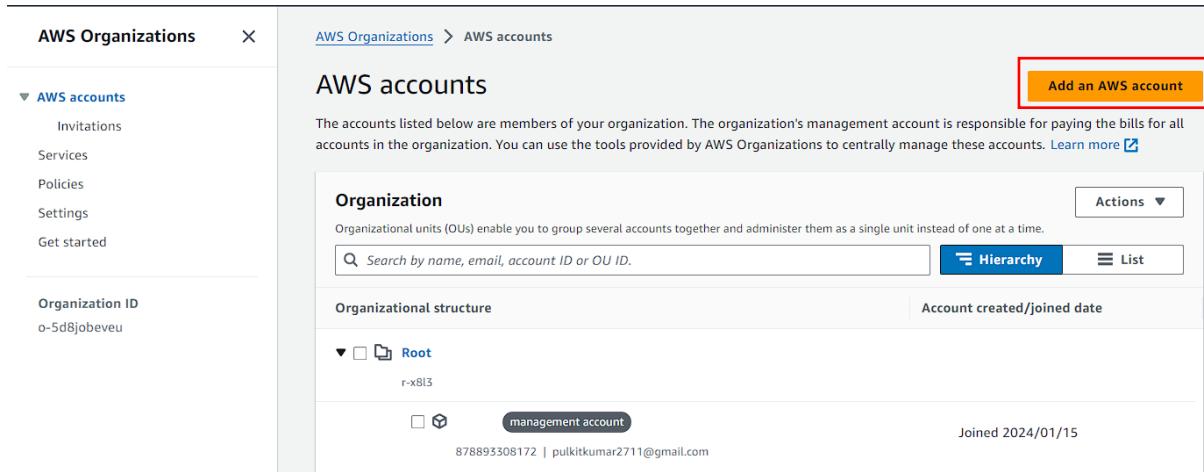
- **Simplified Management:** It simplifies the management of multiple accounts, especially for large enterprises or organizations with different departments, projects, or environments (e.g., development, testing, production).
- **Cost Efficiency:** With consolidated billing, you can benefit from volume discounts and simplified cost tracking.
- **Enhanced Security and Compliance:** By enforcing policies at the organization level, you can ensure consistent security and compliance across all accounts.
- **Scalability:** It makes it easier to scale your infrastructure by adding new accounts and resources as needed.

In simple terms, AWS Organizations helps you keep all your AWS accounts under control, ensuring they are organized, secure, and efficiently managed.

**End Goal:** In this lab, you're working with AWS Organizations to manage multiple AWS accounts within an organization. The goal is to invite another AWS account to join the organization, apply a service control policy (SCP) from the management account to restrict access to a specific AWS service (S3 in this case) for the member account, and then observe the effects of the policy on the member account's access permissions. Finally, you'll detach the policy to restore access to the restricted service for the member account.

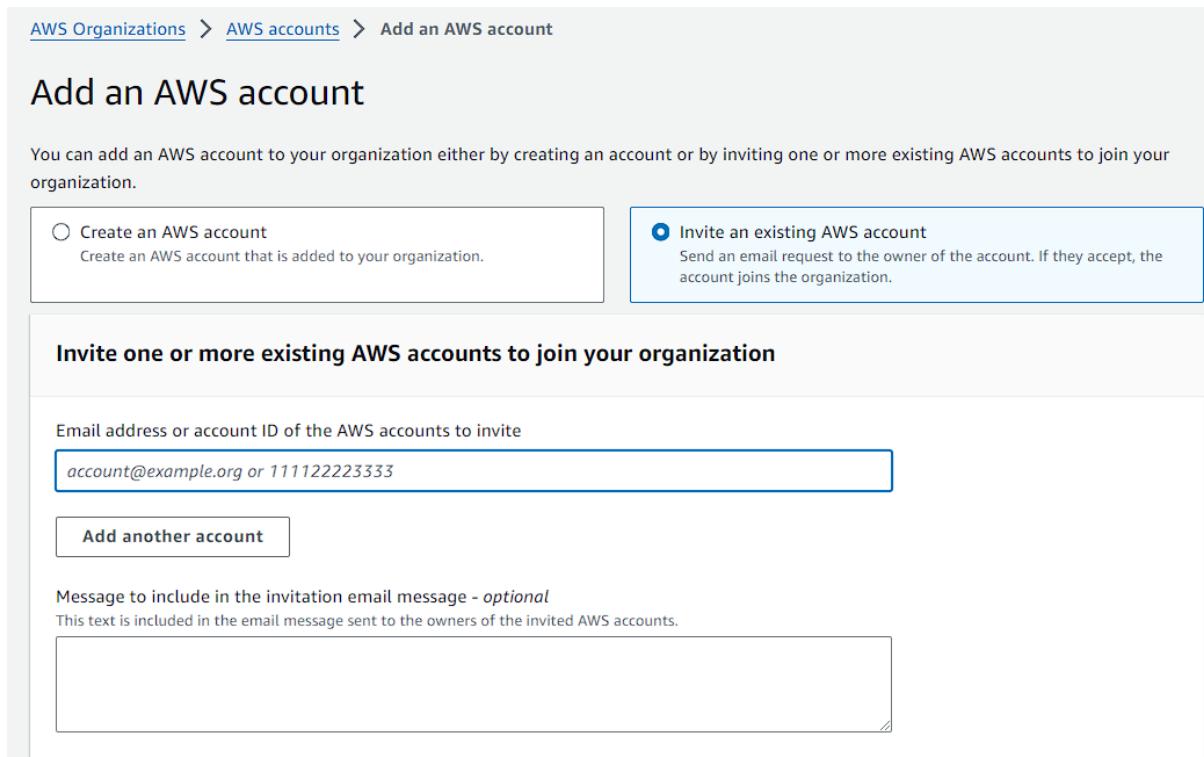
## To begin with this Lab:

1. Now for this lab you should have AWS Organizations setup in your AWS Account.
2. Once you have setup the organizations you will see this type of dashboard for it.
3. Now at this stage you will see that you have one account and it is also showing you that this is a management account. So, from this account you can go ahead and do various things like apply policies to member account and various others.



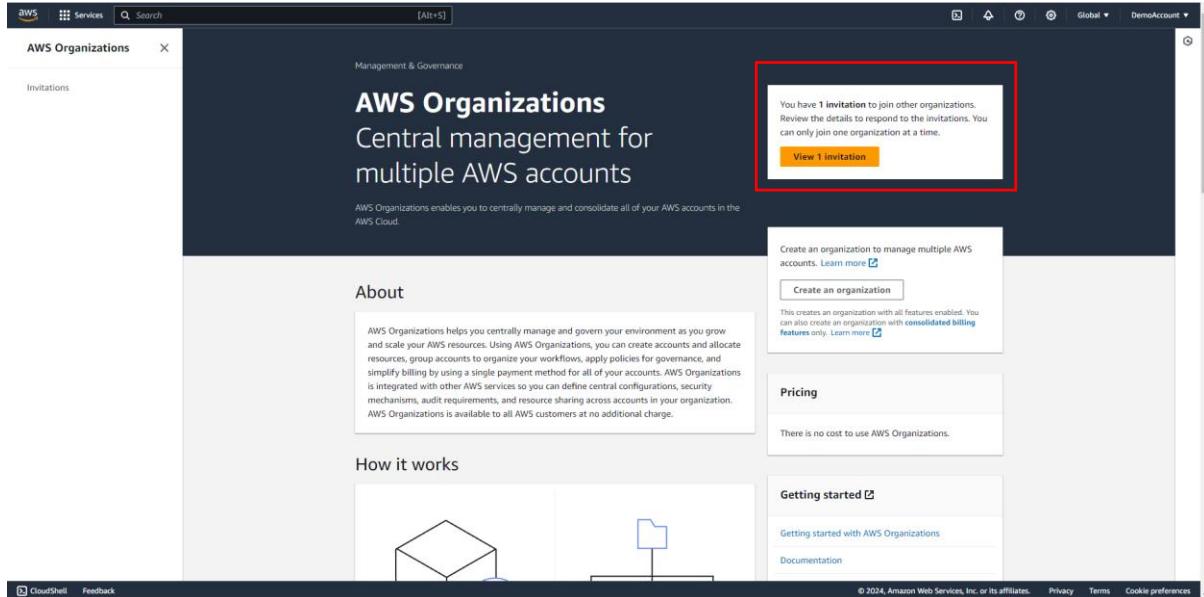
The screenshot shows the AWS Organizations AWS accounts dashboard. On the left, there's a sidebar with 'AWS accounts' expanded, showing options like Invitations, Services, Policies, Settings, and Get started. Below that is an 'Organization ID' section with 'o-5d8jobeveu'. The main area is titled 'AWS accounts' and contains a heading 'Organization'. It says 'Organizational units (OUS) enable you to group several accounts together and administer them as a single unit instead of one at a time.' There's a search bar, a 'Hierarchy' button, and a 'List' button. A table lists accounts under the 'Root' OU. One account is shown: 'management account' (878893308172 | pulkitkumar2711@gmail.com), joined on 2024/01/15. An 'Actions' dropdown menu is visible next to the account row.

4. Now you can go ahead and invite other AWS account. For that click on Add an AWS Account.
5. You can either create an AWS account or you can add an existing account in it.
6. Now click on invite an existing AWS Account. Then paste the account ID of the other account. After that just click on send invitation.

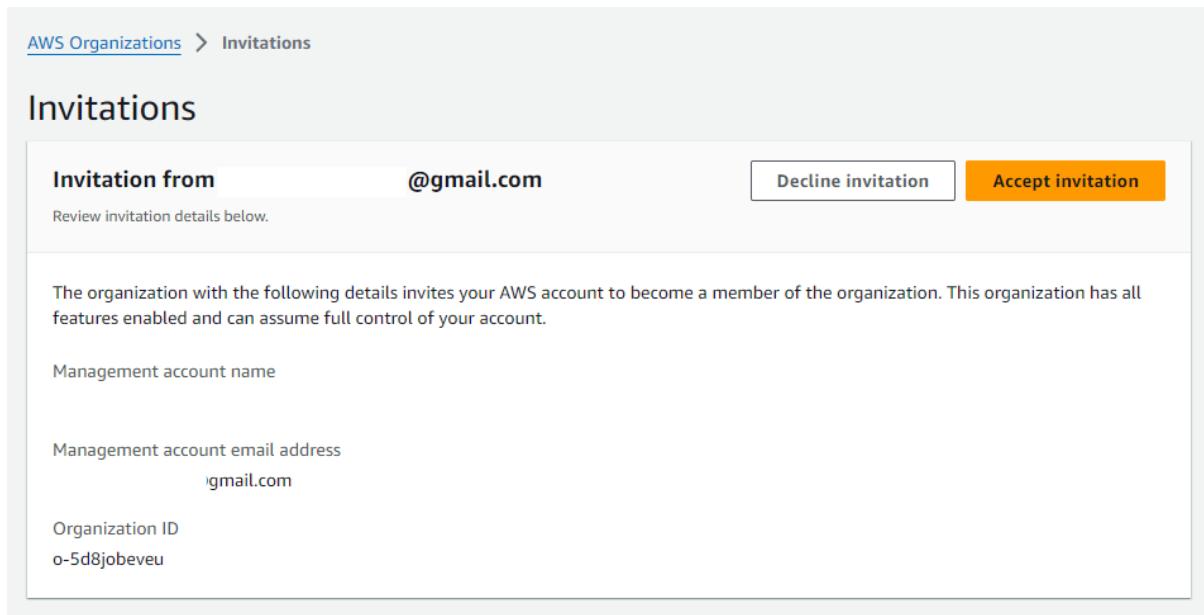


The screenshot shows the 'Add an AWS account' invitation page. At the top, the URL is 'AWS Organizations > AWS accounts > Add an AWS account'. The title is 'Add an AWS account'. A sub-instruction says 'You can add an AWS account to your organization either by creating an account or by inviting one or more existing AWS accounts to join your organization.' Two options are presented: 'Create an AWS account' (radio button not selected) and 'Invite an existing AWS account' (radio button selected). The selected option has a description: 'Send an email request to the owner of the account. If they accept, the account joins the organization.' Below this, a section titled 'Invite one or more existing AWS accounts to join your organization' contains a text input field for 'Email address or account ID of the AWS accounts to invite' with the placeholder 'account@example.org or 111122223333'. There's a button 'Add another account'. At the bottom, there's a note about an optional message: 'Message to include in the invitation email message - optional' followed by a text input field.

- Now from the other account in the AWS Console navigate to Organizations. There you will see an invitation.
- Now click on View invitation and accept the invitation.



- Here you will see the details where the invitation came from. What is the management account name and the email address.
- Now click on accept invite.



- After that you will see this kind of dashboard.

⌚ You accepted an invitation to join an organization.

AWS Organizations > Dashboard

## Dashboard

### Organization details

Organization ID  
o-5d8jobeveu

Management account email address  
@gmail.com

Management account ID  
878893308172

#### Feature set

Your organization has all features enabled. You can apply policies that can configure and limit what the accounts in the organization can do. Trusted AWS services can access your organization and accounts. The management account can create, manage and pay for the organization's accounts through consolidated billing.

12. Now come back to your main account and refresh the organization page you will be able to see the account that you had just invited.

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-x8l3

 DemoAccount

Joined 2024/02/26

533267094905 | @gmail.com

 management account

Joined 2024/01/15

878893308172 | @gmail.com

13. So, now let's do one thing similar to the policy demo that we had seen, where we go ahead and apply a specific policy to an account. And once the policy is applied, not even a root user of that account can access that service.
14. Now in your management account go to policies, from there click on service control policies.

AWS Organizations Policies

Policies

Policies in AWS Organizations enable you to manage different features of the AWS accounts in your organization. [Learn more](#)

Policy type	Status
AI services opt-out policies	Disabled
Backup policies	Disabled
<b>Service control policies</b>	Disabled
Tag policies	Disabled

15. First you are going to enable your service control policies.

AWS Organizations > Policies > Service control policies

## Service control policies

Service control policies (SCPs) enable central administration over the permissions that determine which services and actions that all identities (users and roles) can use across the accounts in your organization. [Learn more](#)

**Enable service control policies**

16. Then you will see that at this time you have full AWS Access.

AWS Organizations > Policies > Service control policies

## Service control policies

Service control policies (SCPs) enable central administration over the permissions that determine which services and actions that all identities (users and roles) can use across the accounts in your organization. [Learn more](#)

Available policies		Actions ▾	Create policy
	Name	Kind	Description
<input type="checkbox"/>	FullAWSAccess	AWS managed policy	Allows access to every operation

17. Now let's go ahead and create a new policy. Click on create policy.

18. Now here first you are going to specify a name for it. Then if you'll scroll down to edit statement. Here you going to choose a S3 as a service.

The screenshot shows the AWS IAM Policy Editor interface. On the left, a JSON policy document is displayed:

```
1▼ {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "Statement1",  
6       "Effect": "Deny",  
7       "Action": [],  
8       "Resource": []  
9     }  
10    ]  
11  }
```

On the right, the 'Edit statement' panel is open for 'Statement1'. It includes a 'Remove' button, a 'Choose a service' dropdown set to 's3', and a list of available services: S3, S3 Express, S3 Object Lambda, and S3 Outposts.

19. Then click on All actions. After that click on add resource.

The screenshot shows the AWS IAM Policy Editor interface. The JSON policy remains the same as in the previous step:

```
1▼ {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "Statement1",  
6       "Effect": "Deny",  
7       "Action": [  
8         "s3:*"  
9       ],  
10      "Resource": []  
11    }  
12  ]  
13 }
```

The 'Edit statement' panel now shows 'All services > s3' in the 'Add actions' section. A checkbox for 'All actions (s3:\*)' is checked and highlighted with a red box. Below it, the 'Access level - list' section contains several checked items. At the bottom, there are 'Add a resource' and 'Add' buttons, both highlighted with a red box.

20. Select service as S3 and in the resource type choose all resources. Then click on add resource.

**Add resource**

Specify the resource type and ARN to add for the selected service.

Service

S3

Resource type

All Resources

Resource ARN

\*

**Cancel** **Add resource**

21. After that just create your policy.
22. Then you will see your policy here.

AWS Organizations > Policies > Service control policies

**Service control policies**

Service control policies (SCPs) enable central administration over the permissions that determine which services and actions that all identities (users and roles) can use across the accounts in your organization. [Learn more](#)

**Available policies**

	Name	Kind	Description
<input type="checkbox"/>	deny-S3	Customer managed policy	-
<input type="checkbox"/>	FullAWSAccess	AWS managed policy	Allows access to every operation

**Actions** **Create policy**

23. Now you are going to associate this policy with your member account.
24. For that select your policy and click on attach policy.

Available policies			
	Name	Kind	Description
<input checked="" type="checkbox"/>	deny-S3	Customer managed policy	-
<input type="checkbox"/>	FullAWSAccess	AWS managed policy	Allows access to every operation

**Actions** **Create policy**

**Attach policy** **Delete policy**

25. Once you have clicked on attach policy you will see it is asking you to select your member account. Select it and click on attach policy.

AWS Organizations > Policies > Service control policies > deny-S3 > Attach a policy

Attach deny-S3 to one or more targets

**AWS Organization**

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-x8l3

DemoAccount Joined 2024/02/26  
533267094905 | @gmail.com

management account Joined 2024/01/15  
878893308172 | @gmail.com

Cancel Attach policy

26. Now if you will go to your member account and navigate to S3 then you will see access denied.

Amazon S3 Services Search [Alt+S]

Amazon S3 > Buckets

Account snapshot

General purpose buckets Info View Storage Lens dashboard

Buckets are containers for data stored in S3.

General purpose buckets Info

Name ▲ AWS Region ▼ Access ▼ Creation date ▼

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.

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

27. Now you can also detach your policy go to your policy in your management account and open it. Then if you will targets in it and select the account then click on detach.

AWS Organizations > Policies > Service control policies > deny-S3

## deny-S3

Delete
Edit policy

### Policy details

Name	deny-S3
ARN	arn:aws:organizations::878893308172:policy/o-5d8jobjeveu/service_control_policy/p-t3p8owth
Policy type	Service control policy (customer managed)
Description	-

**Content** | **Targets** | Tags

### Targets

Detach
Attach

Name	ID	Type
DemoAccount	533267094905	ACCOUNT

28. Then if you will again navigate to your member account and refresh the page you can see that you have the permission now to view S3.

The screenshot shows the AWS S3 console interface. The left sidebar has a navigation tree with 'Amazon S3' selected under 'Buckets'. The main content area displays an 'Account snapshot' with a link to 'View Storage Lens dashboard'. Below this is a section for 'General purpose buckets' with a table header including columns for Name, AWS Region, Access, and Creation date. A search bar at the top of the table allows finding buckets by name. At the bottom of the table, there is a message stating 'No buckets' and 'You don't have any buckets.', followed by a prominent orange 'Create bucket' button.