



Changing policy from Deny to Allow

In this lab, you're exploring how to switch from a deny list policy to an allow list policy using AWS Organizations and Service Control Policies (SCPs). You start by creating an allow policy that grants full access to specific AWS services (EC2 and CloudWatch). Then, you attach this allow policy to a member account, ensuring that only the specified services are accessible. Finally, you remove the member account from the deny list policy to complete the transition. Through this process, you observe the effects of the new allow list policy on the member account's access permissions.

1. Now, in the earlier lab, we were discussing about the basics of SCP (Service Control Policies) and how by default, using the full Access SCP, the denialist strategy is taken into effect.
2. So, in this lab you are going to see how you can switch to allow list policy from deny list policy.
3. First, go to organizations and then move to policies. Here you can see by default we get Full AWS access policy.

The screenshot shows the AWS Organizations Service Control Policies page. At the top, there is a breadcrumb navigation: AWS Organizations > Policies > Service control policies. On the right side, there is a "Disable service control policies" button. Below the breadcrumb, the title "Service control policies" is displayed. A descriptive text states: "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." There is a "Learn more" link with a blue question mark icon. Below this, there is a table titled "Available policies". The table has columns: "Name", "Kind", and "Description". It contains one row for the "FullAWSAccess" policy, which is described as an "AWS managed policy" that "Allows access to every operation". There are "Actions" and "Create policy" buttons at the top of the table.

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

4. Now you are going to click on create policy and paste the policy below. In this policy the actions are to give EC2 full access and cloud watch full access.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "ec2:*",  
        "cloudwatch:*"  
      ],  
      "Resource": "*"  
    }  
  ]}
```

```

1 Version: "2012-10-17",
2 Statement: [
3   {
4     Effect: "Allow",
5     Action: [
6       "ec2:*",
7       "cloudwatch:)"
8     ],
9     Resource: "*"
10   }
11 ]
12
13 }

```

Edit statement

Select a statement

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

+ Add new statement

- Once you are done just create your policy. Below you can see that you have a allow policy.

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

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

Actions ▾ Create policy

- Now if you will open your member account.
- And if you look there in the policies it is attached to 2 policies. One is attached directly and the other is inherited.

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 (2)

<input type="checkbox"/>	Name	Source	Description
<input type="radio"/>	FullAWSAccess (AWS managed policy)	Attached directly	Allows access to every operation
<input checked="" type="radio"/>	FullAWSAccess (AWS managed policy)	Inherited from Root	Allows access to every operation

Detach Attach

- Now go back to your policy and attach your allow policy to member account. So, to attach your policy select your policy then click on actions and then click on attach policy.

The screenshot shows the AWS Organizations Service control policies page. At the top, there's a breadcrumb navigation: AWS Organizations > Policies > Service control policies. On the right, there's a "Disable service control policies" button. Below the navigation, the title "Service control policies" is displayed. A callout box labeled "Actions" points to the "Attach policy" and "Delete policy" buttons in the table header. The table has columns for Name, Kind, and Description. There are two rows: one for "AllowPolicy" (Customer managed policy) which is checked, and another for "FullAWSAccess" (AWS managed policy) which is not checked. The "Description" column for "AllowPolicy" is empty, while for "FullAWSAccess" it says "Allows access to every operation".

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

- Now you will see that is asking you to select the account on which you want to attach this policy.
- So, select your member account and root then click on attach policy.

The screenshot shows the AWS Organization page. At the top, there's a search bar, a "Hierarchy" button, and a "List" button. Below the search bar, the title "Organizational structure" is displayed. The main area shows a tree view of accounts under "Root". One account, "DemoAccount", is selected and highlighted with a blue checkmark. Its details are shown: ID 533267094905, Email @gmail.com, and Joined date 2024/02/26. Another account, "management account", is also listed with ID 878893308172, Email l@gmail.com, and Joined date 2024/01/15. At the bottom right, there are "Cancel" and "Attach policy" buttons.

- Now if you will open the targets of your allow policy you can see the member's account and root user.

AllowPolicy

Policy details

Name
AllowPolicy

ARN
arn:aws:organizations::878893308172:policy/o-5d8jobeveu/service_control_policy/p-04c6fsne

Policy type
Service control policy (customer managed)

Description
-

Content | **Targets** | Tags

Targets

Detach | Attach

	Name	ID	Type
<input type="radio"/>	DemoAccount	533267094905	ACCOUNT
<input type="radio"/>	Root	r-x8l3	ROOT

12. Plus, if you go back to member's account and open its policies you will see your allow policy which is now attach to it directly.

Policies

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 (4)

Detach | Attach

	Name	Source	Description
<input type="radio"/>	FullAWSAccess (AWS managed policy)	Attached directly	Allows access to every operation
<input type="radio"/>	AllowPolicy	Attached directly	-
<input checked="" type="radio"/>	FullAWSAccess (AWS managed policy)	Inherited from Root	Allows access to every operation
<input checked="" type="radio"/>	AllowPolicy	Inherited from Root	-

13. Now go back to policies and open your AWS full access policy and from the targets remove the member account and root from there.
14. Once this is done just reverify to check only allow policy should be attached to member account.

Policy details

Name
FullAWSAccess

ARN
arn:aws:organizations::aws:policy/service_control_policy/p-FullAWSAccess

Policy type
Service control policy (AWS managed)

Description
Allows access to every operation

Content | **Targets**

Targets			
	Name	ID	
	Type		
<input checked="" type="radio"/>	DemoAccount	533267094905	ACCOUNT
<input type="radio"/>		878893308172	ACCOUNT
<input type="radio"/>	Root	r-x8l3	ROOT

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 (2)			
	Name	Source	
		Description	
<input type="radio"/>	AllowPolicy	Attached directly	-
<input checked="" type="radio"/>	AllowPolicy	Inherited from Root	-

15. Now you have to login to your member account and try to visit any service other than cloud watch and EC2. You will see that you are getting permission denied.

The screenshot shows the AWS S3 console with the 'Buckets' tab selected. On the left, there's a sidebar with various options like 'Access Grants', 'Access Points', and 'Storage Lens'. The main area is titled 'Account snapshot' and contains a message: 'You don't have permissions to list buckets'. Below this message, it says: '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.'

16. But you will see that you have access to EC2 and cloud watch.

The screenshot shows the AWS EC2 Dashboard. The left sidebar includes sections for 'Instances', 'Images', and 'Elastic Block Store'. The main area is titled 'Resources' and shows a table of EC2 resources. The table includes:

Category	Count	Details
Instances (running)	0	
Auto Scaling Groups	0	API Error
Dedicated Hosts	0	
Elastic IPs	0	
Instances	0	
Key pairs	0	
Load balancers	0	API Error
Placement groups	0	
Security groups	1	
Snapshots	0	
Volumes	0	

On the right, there's a section for 'EC2 Free Tier' which shows 0 offers in use and a warning about IAM permissions. It also includes a 'Service health' section with a link to the 'AWS Health Dashboard'.

The screenshot shows the AWS CloudWatch Dashboards interface. The left sidebar contains navigation links for CloudWatch services like Alarms, Logs, Metrics, X-Ray traces, Events, Application Signals, Network monitoring, Insights, and Settings. The main content area is titled "Custom dashboards" and shows a table with one row: "No dashboards". It includes a "Create dashboard" button. The top right corner shows the location as "Stockholm" and the account as "DemoAccount".

CloudWatch > Dashboards

Custom dashboards Automatic dashboards

Custom Dashboards (0) [Info](#)

Share dashboard Delete Create dashboard

No dashboards

You have not created any dashboards.

Read more about Dashboards

Create dashboard

Name Sharing Favorite Last update (UTC)

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)