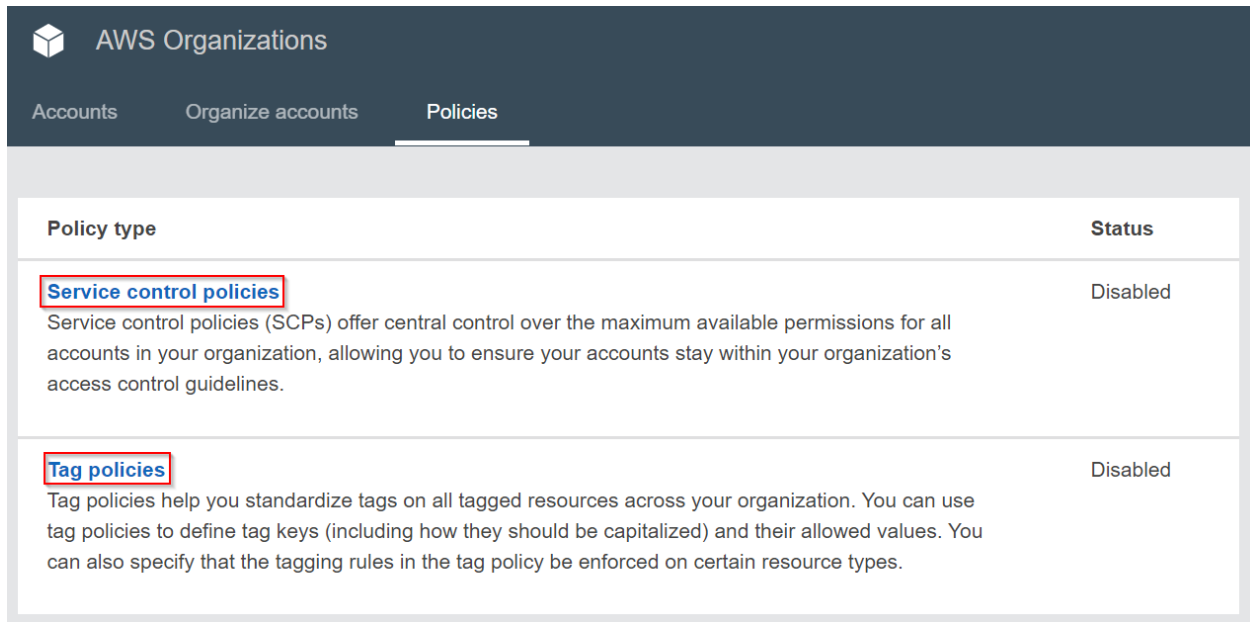


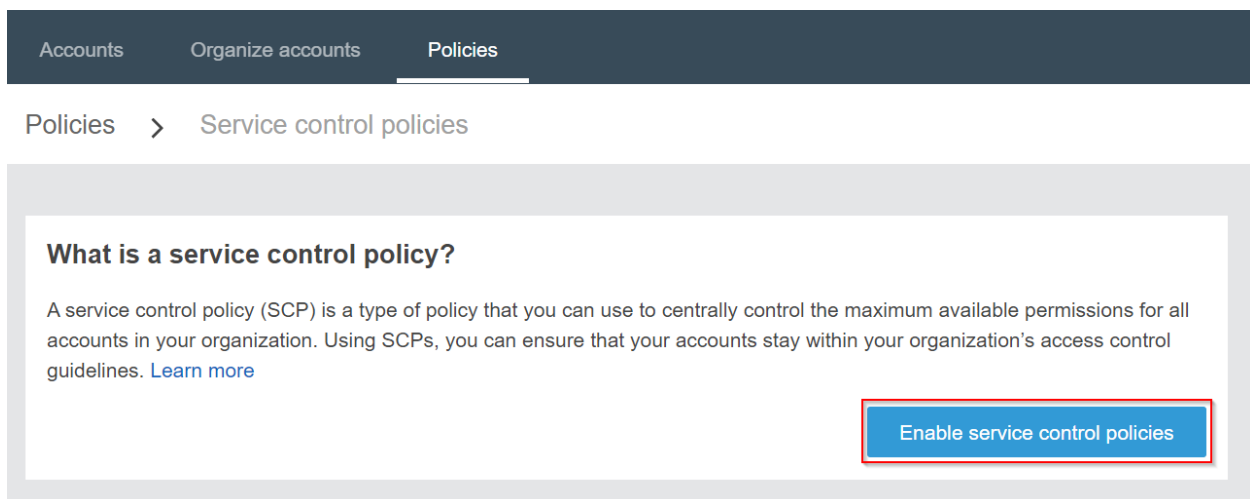
## Module 10: Hands-On- AWS Organizations Policies

**Step 1:** Launch an Amazon Linux 2 instance with a custom TCP rule of port 988 open



Policy type	Status
<b>Service control policies</b> Service control policies (SCPs) offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines.	Disabled
<b>Tag policies</b> Tag policies help you standardize tags on all tagged resources across your organization. You can use tag policies to define tag keys (including how they should be capitalized) and their allowed values. You can also specify that the tagging rules in the tag policy be enforced on certain resource types.	Disabled

**Step 2:** To enable either one of the policies, click on Service control policies or Tag policies and enable it



Policies > Service control policies

### What is a service control policy?

A service control policy (SCP) is a type of policy that you can use to centrally control the maximum available permissions for all accounts in your organization. Using SCPs, you can ensure that your accounts stay within your organization's access control guidelines. [Learn more](#)

**Enable service control policies**

[Accounts](#) [Organize accounts](#) [Policies](#)

Policies > Tag policies

### What is a tag policy?

Tag policies help you standardize tags on all tagged resources across your organization.

Enabling the use of tag policies is a one-time task that you perform for your organization and its accounts. After you enable tag policies, you can create the tag policies that you want. To specify which parts of your organization the policies apply to, you attach them to the organization root, organizational units (OUs), or individual accounts within your organization. [Learn more](#)

Enable tag policies

**Step 3:** After clicking the Enable button, you will get the options to create a policy

[Accounts](#) [Organize accounts](#) [Policies](#)

Policies > Service control policies

Service control policies (SCPs) offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines. [Learn more](#)

Service control policies are enabled

Create policy

Delete policy

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	FullAWSAccess	Service cont...	Allows access to every operation

**Step 4:** Now enter a policy name. Then give a description, it is optional.

Policy name \*

OneEC2Type

The policy name can have up to 128 characters.

Description

This policy is to restrict all but one EC2 type

The description can have up to 512 characters.

**Step 5:** Search for RDS and then choose All actions under it. After selecting it, click on Create policy.

#### Policy \*

To allow actions, include statements with the format "Effect": "Allow". All other actions are implicitly denied.

To explicitly deny actions, include statements with the format "Effect": "Deny". Only Deny statements can include resources and conditions. [Learn more](#)

#### 'RequireMicroInstanceType' statement

1. Choose service to add actions for.

Filter services

- API Gateway
- Access Analyzer
- Account
- Alexa for Business
- Amplify
- App Mesh


```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "RequireMicroInstanceType",
6       "Effect": "Deny",
7       "Action": "ec2:RunInstances",
8       "Resource": [
9         "arn:aws:ec2:*:*:instance/*",
10        ""
11      ],
12      "Condition": {
13        "StringNotEquals": {
14          "ec2:InstanceType": "t2.micro"
15        }
16      }
17    }
18  ]
19 }
```

[Add statement](#)
[Remove statement](#)

[Cancel](#)
[Create policy](#)

**Step 5:** We have successfully created a policy successfully


**AWS Organizations**

[Accounts](#)
[Organize accounts](#)
[Policies](#)

Policies > Service control policies

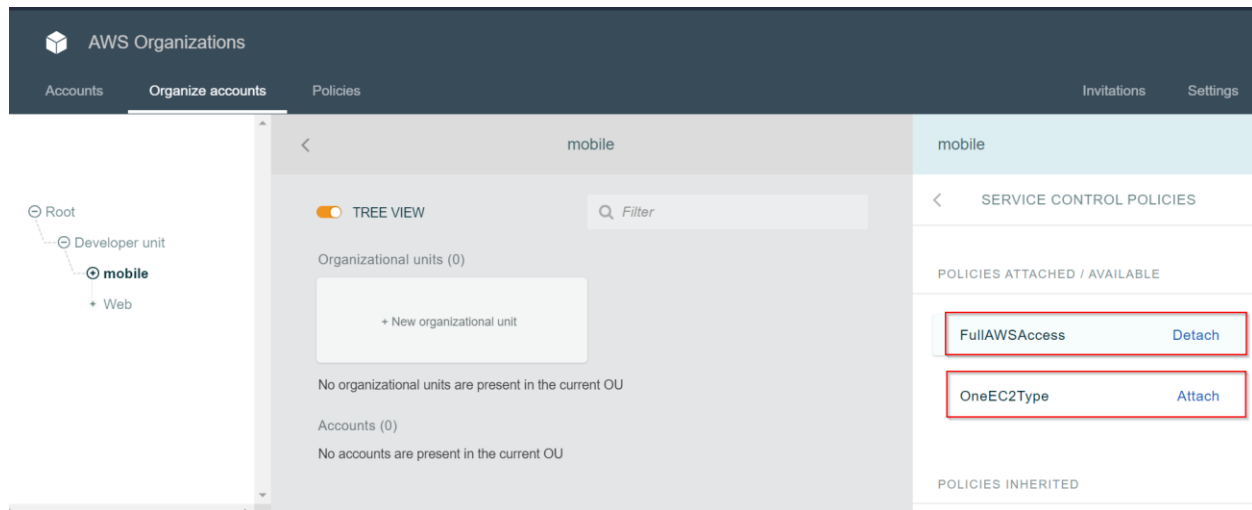
Service control policies (SCPs) offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines. [Learn more](#)

OneEC2Type has been created. ✕

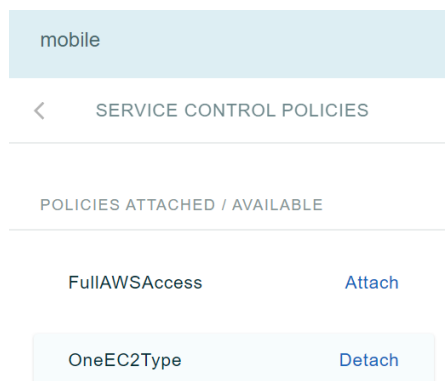
[Create policy](#)
[Delete policy](#)

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	FullAWSAccess	Service cont...	Allows access to every operation
<input type="checkbox"/>	OneEC2Type	Service cont...	This policy is to restrict all but one EC2 type

**Step 6:** Now, let's attach this policy to the **mobile** Organizational unit and detach the Full AWS Access policy



The screenshot shows the AWS Organizations console. On the left, a tree view shows the hierarchy: Root > Developer unit > mobile > Web. The main panel shows the 'mobile' organizational unit. It displays 'Organizational units (0)' and 'Accounts (0)'. On the right, under 'SERVICE CONTROL POLICIES', there are two policies listed: 'FullAWSAccess' with a 'Detach' button, and 'OneEC2Type' with an 'Attach' button. Both policy rows are highlighted with red boxes.



This is a zoomed-in view of the 'mobile' organizational unit page. It shows the 'SERVICE CONTROL POLICIES' section. Under 'POLICIES ATTACHED / AVAILABLE', there are two policies: 'FullAWSAccess' with an 'Attach' button, and 'OneEC2Type' with a 'Detach' button. Both policy rows are highlighted with red boxes.