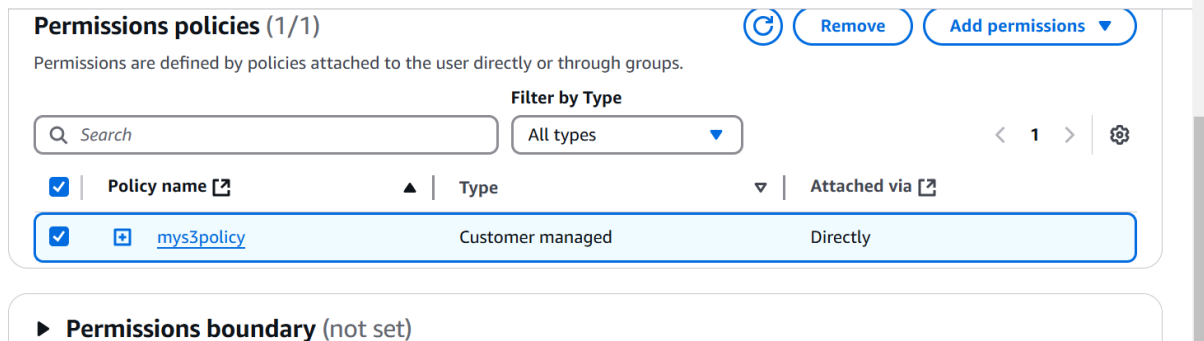


Lab4 -> Assume Role

- Remove policy from the user



Permissions policies (1/1) Remove Add permissions

Permissions are defined by policies attached to the user directly or through groups.

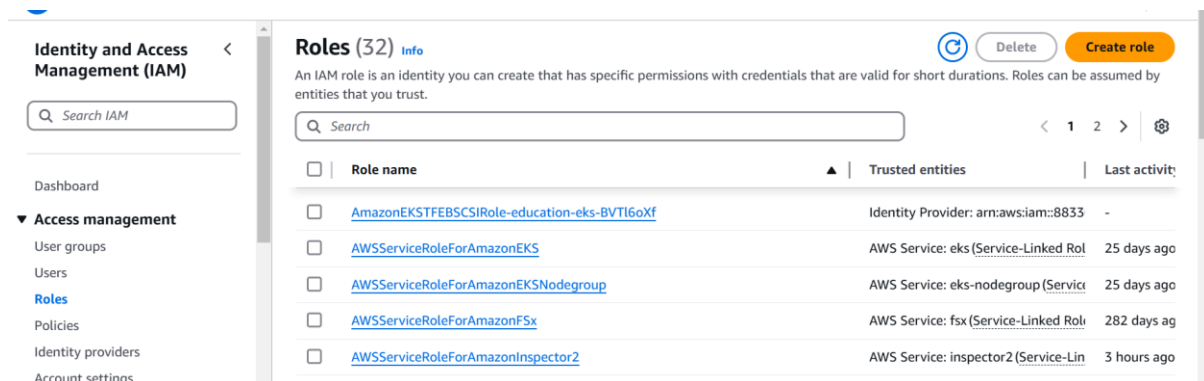
Filter by Type

Search All types

<input checked="" type="checkbox"/>	Policy name	Type	Attached via
<input checked="" type="checkbox"/>	mys3policy	Customer managed	Directly

► **Permissions boundary** (not set)

Create Role



Identity and Access Management (IAM)

Search IAM

Dashboard

▼ **Access management**

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

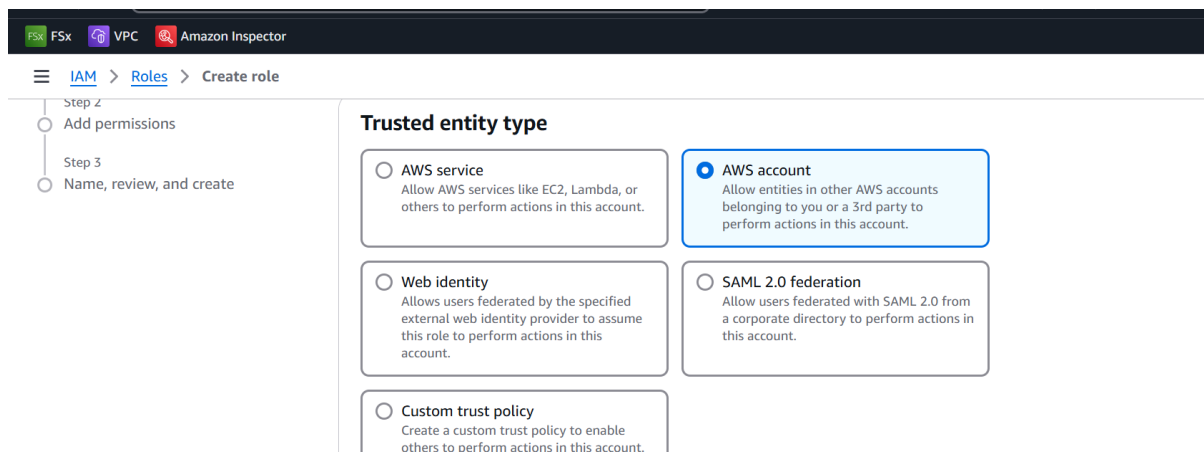
Roles (32) info Delete Create role

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

<input type="checkbox"/>	Role name	Trusted entities	Last activity
<input type="checkbox"/>	AmazonEKSTFEBSCSIRole-education-eks-BVTI6oXf	Identity Provider: arn:aws:iam::8833	-
<input type="checkbox"/>	AWSServiceRoleForAmazonEKS	AWS Service: eks (Service-Linked Rol	25 days ago
<input type="checkbox"/>	AWSServiceRoleForAmazonEKSNodegroup	AWS Service: eks-nodegroup (Service	25 days ago
<input type="checkbox"/>	AWSServiceRoleForAmazonFSx	AWS Service: fsx (Service-Linked Rol	282 days ag
<input type="checkbox"/>	AWSServiceRoleForAmazonInspector2	AWS Service: inspector2 (Service-Lin	3 hours ago

Select option -> AWS account



FSx VPC Amazon Inspector

IAM > Roles > Create role

Step 2: Add permissions

Step 3: Name, review, and create

Trusted entity type

- ☐ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☒ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ **Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Press next

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

- ### Options

- Cancel

Next

Add permissions [Info](#)

Choose one or more policies to attach to your new role.

Filter by Type

Q mys

All types

1 match

< 1 >

Policy name [↗](#)

Type

▲

Description

☒

 [mys3policy](#)

Customer managed

—

- Set permissions boundary - *optional*

Cancel

[Previous](#)

Next

FSxVPCAmazon Inspector

IAM > Roles > Create role

Step 2

Add permissions

Step 3

Create role

Role details

Role name

Enter a meaningful name to identify this role.

mys3role

Maximum 64 characters. Use alphanumeric and '+=, @-.' characters.

Description

Add a short explanation for this role.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=, @-./[]!#\$%^&*~`

Step 1: Select trusted entities

Trust policy

Step 1: Select trusted entities

Edit

Trust policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "sts:AssumeRole",
7       "Principal": {
8         "AWS": "883308508227"
9       },
10      "Condition": {}
11    }
12  ]
13 }
```

Step 2: Add permissions

Edit

Create role

Note down the arn of IAM role

mys3role Info

Delete

Summary

Creation date

January 11, 2025, 22:26 (UTC+05:30)

ARN copied

arn:aws:iam::883308508227:role/mys3role

Link to switch roles in console

https://signin.aws.amazon.com/switchrole?roleName=mys3role&account=883308508227

Last activity

-

Maximum session duration

1 hour

Edit

Go to your user → testuser

Create inline policy

Users and Access Management (IAM)

arn:aws:iam::883308508227:user/testuser

Enabled without MFA

Created

January 11, 2025, 22:29 (UTC+05:30)

Last console sign-in

Today

Create access key

Permissions

Groups

Tags

Security credentials

Last Accessed

Permissions policies (0)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type

Search

All types

Policy name

Type

Attached via

No resources to display

Add permissions

Create inline policy

In policy check for STS and action search for assume role

Policy editor

VisualJSONActions

▼ STS

Allow1 Action

Specify what actions can be performed on specific resources in STS.

▼ Actions allowed

Specify actions from the service to be allowed.

Q assuX

Effect

AllowDeny

Write

☒ AssumeRoleInfo

☐ AssumeRoleWithSAMLInfo

☐ AssumeRoleWithWebIdentityInfo

☐ AssumeRootInfo

Provide role ARN

▼ Resources

Specify resource ARNs for these actions.

☐ All

☒ Specific

roleInfo

⚠ Specified role resource ARN for the AssumeRole and 5 more actions. Add ARNs to restrict access.

☐ Any in this account

► Request conditions - optional

Specify ARNs

X

VisualText

Resource in

☒ This account

☐ Any account

☐ Other account

Resource role name with path

mys3role

☐ Any role name with path

Resource ARN

arn:aws:iam::883308508227:role/mys3role

CancelAdd ARNs

JSON

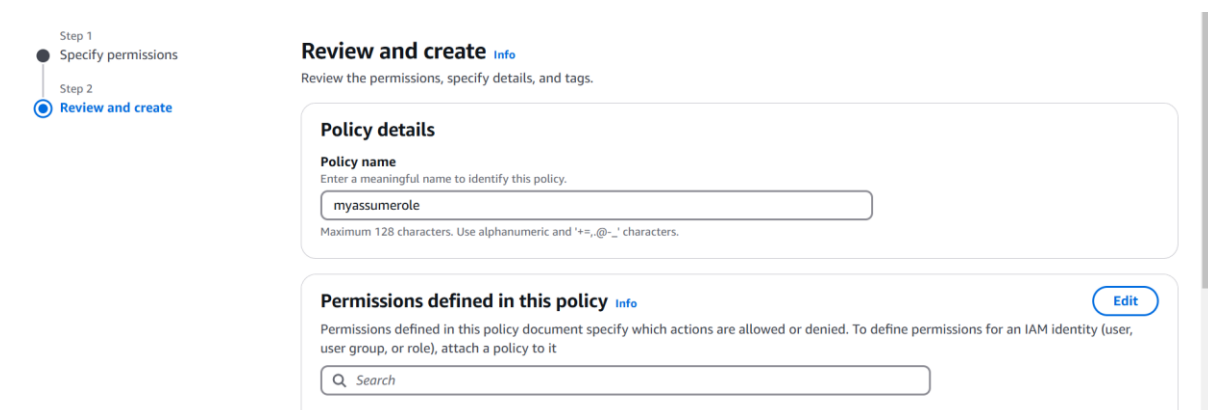
{

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "VisualEditor0",
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::883308508227:role/mys3role"
  }
]
}

```

Provide name and create



The screenshot shows the 'Review and create' step in the AWS IAM console. On the left, a progress bar indicates 'Step 1: Specify permissions' and 'Step 2: Review and create' (the current step). The main content area is titled 'Review and create' with an 'Info' link. Below the title, it says 'Review the permissions, specify details, and tags.' There are two main sections: 'Policy details' and 'Permissions defined in this policy'. The 'Policy details' section has a 'Policy name' field with the value 'myassumerole' and a note: 'Enter a meaningful name to identify this policy. Maximum 128 characters. Use alphanumeric and '+=, @-.' characters.' The 'Permissions defined in this policy' section has a search bar with the placeholder 'Search' and an 'Edit' button. At the bottom, there is a horizontal bar with icons for navigation.

Check the option to switch the role: Link to switch the role

mys3role

Info

Delete

Summary

Creation date

January 11, 2025, 22:26 (UTC+05:30)

Last activity

-

Maximum session duration

1 hour

Link to switch roles in console

<https://signin.aws.amazon.com/switchrole?roleName=mys3role&account=883308508227>

ARN copied

arn:aws:iam::883308508227:role/mys3role

Edit

Permissions

Trust relationships

Tags

Last Accessed

Revoke sessions

Switch Role

permissions back. [Learn more](#)

Account ID

The 12-digit account number or the alias of the account in which the role exists.

883308508227

IAM role name

The name of the role that you want to assume which can be found at the end of the role's ARN. For example, provide the `TestRole` role name from the following role ARN: `arn:aws:iam::123456789012:role/TestRole`.

mys3role

Display name - optional

This name will appear in the console navigation bar when active. Choose a name to help identify the permission set assigned to the role.

mys3role @ 883308508227

Display color - optional

The selected color displays in the console navigation when this role is active

None

Cancel

Switch Role

© 2025 Amazon Web Services, Inc. or its affiliates. Privacy

eu-north-1.console.aws.amazon.com/s3/home?region=eu-north-1#

Search [Alt+S] Europe (Stockholm) mys3role @ 883308508227

Amazon S3

Account snapshot - updated every 24 hours All AWS Regions View Storage Lens dashboard

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

General purpose buckets Directory buckets

General purpose buckets (1) Info All AWS Regions

Copy ARN Empty Delete Create bucket

Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	IAM Access Analyzer	Creation date
myamit23bucket	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	January 11, 2025, 18:15:26 (UTC+05:30)

Click on the role and switch back

eu-north-1.console.aws.amazon.com/s3/buckets?region=eu-north-1

Search [Alt+S] Europe (Stockholm) testuser @ 8833-0850-8227

S3 > Buckets

Account snapshot - updated every 24 hours All AWS Regions View Storage Lens dashboard

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

General purpose buckets Directory buckets