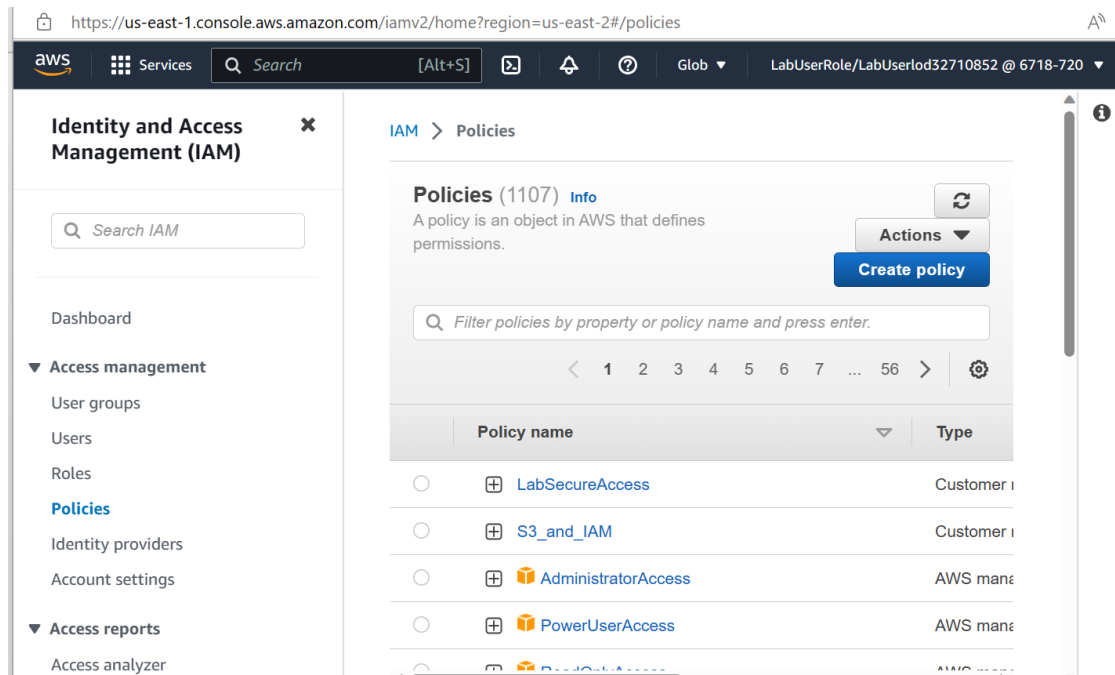
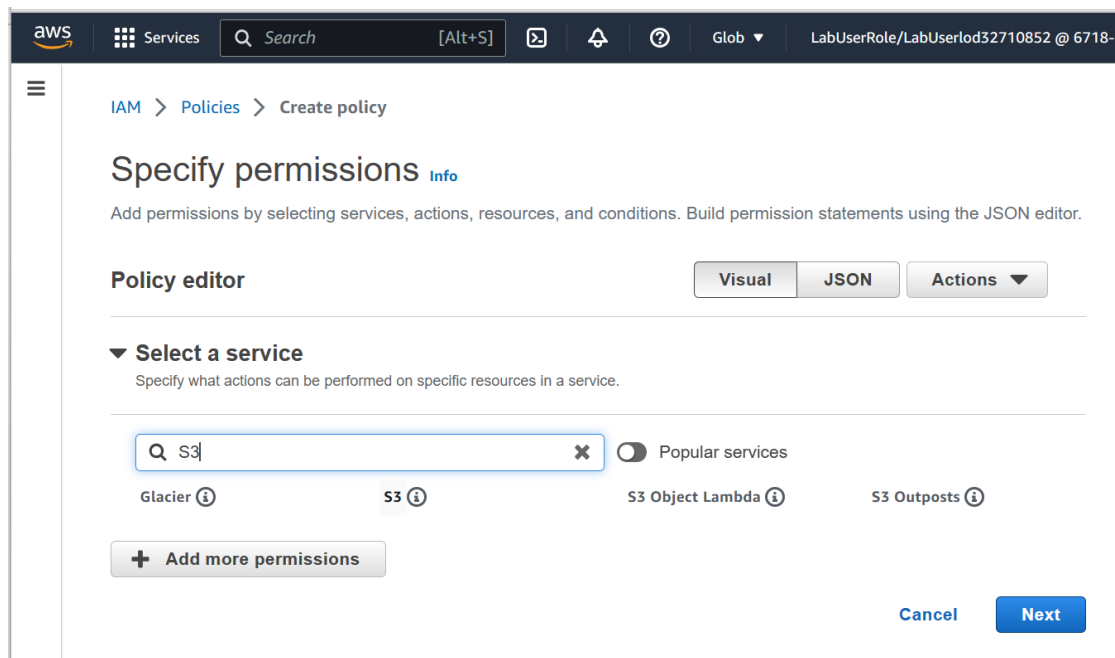


Policies and Permissions:



This screenshot shows the AWS IAM console's 'Policies' page. The left-hand navigation pane is open, displaying the 'Identity and Access Management (IAM)' section with a search bar and a list of links: Dashboard, Access management (expanded), User groups, Users, Roles, Policies (highlighted), Identity providers, Account settings, Access reports, and Access analyzer. The main content area is titled 'Policies (1107)' and includes an 'Info' link, a description of policies, a 'Create policy' button, and a search filter. Below this is a table listing several policies:

	Policy name	Type
<input type="radio"/>	LabSecureAccess	Customer managed
<input type="radio"/>	S3_and_IAM	Customer managed
<input type="radio"/>	AdministratorAccess	AWS managed
<input type="radio"/>	PowerUserAccess	AWS managed
<input type="radio"/>	ReadOnlyAccess	AWS managed



This screenshot shows the 'Specify permissions' page in the AWS IAM console. The breadcrumb trail indicates the path: IAM > Policies > Create policy. The page title is 'Specify permissions' with an 'Info' link. Below the title is a brief instruction: 'Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.' The 'Policy editor' section has tabs for 'Visual' (selected), 'JSON', and 'Actions'. Under the 'Visual' tab, the 'Select a service' section is active, with the instruction 'Specify what actions can be performed on specific resources in a service.' A search bar contains 'S3', and a list of services is displayed: Glacier, S3, S3 Object Lambda, and S3 Outposts. At the bottom, there is an 'Add more permissions' button and 'Cancel' and 'Next' buttons.

▼ Resources

Specify resource ARNs for these actions.

☒ Specific ☐ All

bucket ⓘ

⚠ Specified bucket resource ARN for the **GetBucketLocation** and **48 more** actions.

[Add Arn](#) to restrict access.

multiregionacce... ⓘ

⚠ Specified multiregionaccesspointrequestarn resource ARN for the **DescribeMultiRegionAccessPointOperation** action.

[Add Arn](#) to restrict access.

objectlambdaac... ⓘ

⚠ Specified objectlambdaaccesspoint resource ARN for the **PutAccessPointConfigurationForObjectLambda** and **8 more** actions.

[Add Arn](#) to restrict access.

aws Services Search [Alt+S] [?] Glob LabUserRole/LabUserIod32710852 @ 6718-720

• s3:PutReplicationConfiguration requires **1 more** actions.

Specify ARNs

☒ Visual ☐ Text

Resource bucket name

☐ Any bucket name

bucket-32710852

ARN

☐ Any resource

bucket-32710852

arn:aws:s3:::bucket-32710852

Cancel Add ARNs

aws

Services

Search

[Alt+S]

Glob

LabUserRole/LabUserlod32710852 @ 6718-720

IAM > Policies > Create policy

Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

s3webadminpolicy-32710852

Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.

Description - optional

Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+=, @-_' characters.

CloudShell

Feedback

Language

Privacy

Terms

Cookie preferences

© 2023, Amazon Web Services, Inc. or its affiliates.

https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-2#/policies

aws

Services

Search

[Alt+S]

Glob

LabUserRole/LabUserlod32710852 @ 6718-

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Policy s3webadminpolicy-32710852 created.

View policy

IAM > Policies

Policies (1108)

Info

A policy is an object in AWS that defines permissions.

Actions

Create policy

Filter policies by property or policy name and press enter.

< 1 2 3 4 5 6 7 ... 56 >