

Problem Statement:

You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

Tasks To Be Performed:

1. Create policy number 1 which lets the users to:
 - a. Access S3 completely
 - b. Only create EC2 instances
 - c. Full access to RDS
2. Create a policy number 2 which allows the users to:
 - a. Access CloudWatch and billing completely
 - b. Can only list EC2 and S3 resources
3. Attach policy number 1 to the Dev Team from task 1
4. Attach policy number 2 to Ops Team from task 1

←

→

↺

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies

☆

☰

📱

Finish update ⋮

aws

Services

Q Search

[Option+S]

🖨

🔔

?

⚙

Global ▾

rsujithsri16@gmail.com ▾

EC2

Identity and Access Management (IAM) X

Q Search IAM

Dashboard

▼ Access management

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

▼ Access reports

- Access Analyzer
 - External access
 - Unused access
 - Analyzer settings

IAM > Policies

Policies (1190) Info

A policy is an object in AWS that defines permissions.

Filter by Type

Q Search

All types ▾

< 1 2 3 4 5 6 7 ... 60 >

⚙

🔄

Actions ▾

Delete

Create policy

	Policy name ▲	Type ▾	Used as ▾	Description
<input type="radio"/>	AccessAnalyzerSer...	AWS managed	None	Allow Access Analyzer to analyze resou...
<input type="radio"/>	AdministratorAccess	AWS managed - job function	Permissions policy (1)	Provides full access to AWS services an...
<input type="radio"/>	AdministratorAcce...	AWS managed	None	Grants account administrative permiss...
<input type="radio"/>	AdministratorAcce...	AWS managed	None	Grants account administrative permiss...
<input type="radio"/>	AlexaForBusinessD...	AWS managed	None	Provide device setup access to AlexaFo...
<input type="radio"/>	AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusiness ...
<input type="radio"/>	AlexaForBusinessG...	AWS managed	None	Provide gateway execution access to A...
<input type="radio"/>	AlexaForBusinessLi...	AWS managed	None	Provide access to Lifesize AVS devices
<input type="radio"/>	AlexaForBusinessN...	AWS managed	None	This policy enables Alexa for Business ...



Services

Search

[Option+S]



Global

rsujithsri16@gmail.com



IAM > Policies > Create policy

Step 1

Specify permissions

Step 2

Review and create

Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

Visual

JSON

Actions



▼ EC2

Allow All actions



Specify what actions can be performed on specific resources in [EC2](#).

▼ Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Manual actions | [Add actions](#)

☒ All EC2 actions (ec2:*)

Access level

► List (Selected 174/174)

► Read (Selected 35/35)

Effect

☒ Allow ☐ Deny

[Expand all](#) | [Collapse all](#)



- ec2:AssociateIamInstanceProfile requires [1 more](#) action.
- ec2:CreateFlowLogs requires [1 more](#) action.
- ec2:CreateIam requires [1 more](#) action.
- ec2:CreateIamResourceDiscovery requires [1 more](#) action.
- ec2:CreateLaunchTemplate requires [1 more](#) action.
- ec2:CreateLaunchTemplateVersion requires [1 more](#) action.
- ec2:CreateVpcEndpoint requires [1 more](#) action.
- ec2:DisableIamOrganizationAdminAccount requires [1 more](#) action.
- ec2:EnableIamOrganizationAdminAccount requires [3 more](#) actions.
- ec2:EnableReachabilityAnalyzerOrganizationSharing requires [2 more](#) actions.
- ec2:ReplacesIamInstanceProfileAssociation requires [1 more](#) action.
- ec2:RequestSpotInstances requires [1 more](#) action.
- ec2:RunInstances requires [2 more](#) actions.
- ec2:DescribeLaunchTemplateVersions requires [1 more](#) action.

▼ Resources

Specify resource ARNs for these actions.

- ☒ All
- ☐ Specific

⚠ The all wildcard "*" may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

S3

Allow All actions

Specify what actions can be performed on specific resources in S3.

Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect

☒ Allow ☐ Deny

Manual actions | [Add actions](#)

☒ All S3 actions (s3:*)

Access level

[Expand all](#) | [Collapse all](#)

► List (Selected 15/15)

► Read (Selected 60/60)

► Write (Selected 56/56)

► Permissions management (Selected 15/15)

► Tagging (Selected 12/12)



Dependent permissions not selected.

To grant permissions for the selected resource actions, including additional dependent actions might be required.

- s3:CreateJob requires [1 more](#) action.
- s3:PutReplicationConfiguration requires [1 more](#) action.

Access level

Expand all | Collapse all

- ▶ List (Selected 15/15)
- ▶ Read (Selected 60/60)
- ▶ Write (Selected 56/56)
- ▶ Permissions management (Selected 15/15)
- ▶ Tagging (Selected 12/12)



Dependent permissions not selected.

To grant permissions for the selected resource actions, including additional dependent actions might be required.

- s3:CreateJob requires [1 more](#) action.
- s3:PutReplicationConfiguration requires [1 more](#) action.

▼ Resources

Specify resource ARNs for these actions.

- ☒ All
- ☐ Specific

⚠ The all wildcard "*" may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

▶ Request conditions - optional

Actions on resources are allowed or denied only when these conditions are met.

←

→

↺

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create

☆

☰

🖨

Finish update ⋮

aws

Services

Q Search

[Option+S]

Global ▾

rsujithsri16@gmail.com ▾

EC2

☰

▼ RDS

Allow All actions

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

▼ Actions allowed

Specify actions from the service to be allowed.

Q Filter Actions

Manual actions | [Add actions](#)

☒ All RDS actions (rds:*)

Access level

► List (Selected 45/45)

► Read (Selected 5/5)

► Write (Selected 114/114)

► Permissions management (Selected 1/1)

► Tagging (Selected 2/2)

Dependent permissions not selected.

To grant permissions for the selected resource actions, including additional dependent actions might be required.

- rds:AddRoleToDBCluster requires [1 more](#) action.

Effect

☒ Allow ☐ Deny

[Expand all](#) | [Collapse all](#)

rd:RestoreDBClusterFromSnapshot requires [1 more](#) action.

- rds:RestoreDBClusterToPointInTime requires [1 more](#) action.
- rds:RestoreDBInstanceFromDBSnapshot requires [1 more](#) action.
- rds:RestoreDBInstanceFromS3 requires [7 more](#) actions.
- rds:RestoreDBInstanceToPointInTime requires [1 more](#) action.
- rds:StartExportTask requires [1 more](#) action.

▼ Resources

Specify resource ARNs for these actions.

- ☒ All
- ☐ Specific

⚠ The all wildcard "*" may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

► Request conditions - optional

Actions on resources are allowed or denied only when these conditions are met.

+ Add more permissions

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Cancel

Next



[IAM](#) > [Policies](#) > Create policy

Step 1

[Specify permissions](#)

Step 2

Review and create

Review and create [Info](#)

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

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

Description - *optional*

Add a short explanation for this policy.

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

Permissions defined in this policy [Info](#)

Edit

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

←

→

↺

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create

☆

☰

📱

Finish update ⋮

aws

Services

Q

Search

[Option+S]

Global ▾

rsujithsri16@gmail.com ▾

EC2

☰

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Q

Search

Allow (3 of 409 services)

☐ Show remaining 406 services

Service ▲	Access level ▼	Resource	Request condition
EC2	Full access	All resources	None
RDS	Full access	All resources	None
S3	Full access	All resources	None

Add tags - optional [Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create policy

←

→

↺

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create

☆

☰

🖨

Finish update ⋮

aws

Services

Q

Search

[Option+S]

Global ▾

rsujithsri16@gmail.com ▾

EC2

☰

Set permissions

Step 3

Review and create

Permissions options

☐ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

☒ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1193)

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

dev-t

×

Filter by Type

All types

▼

1 match

<

1

>

<input checked="" type="checkbox"/>	Policy name	Type	Attached entities
<input checked="" type="checkbox"/>	Dev-Team1	Customer managed	0

► Set permissions boundary - optional

Cancel

Previous

Next



Step 2
[Set permissions](#)

Step 3
Review and create

User details

User name
Dev-Team1

Console password type
None

Require password reset
No

Permissions summary

< 1 >

Name



Type



Used as



[Dev-Team1](#)

Customer managed

Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel


Previous

Create user

Console Home

Reset to default layout Add widgets

Recently visited



No recently visited services

Explore one of these commonly visited AWS services.

[EC2](#) [S3](#) [RDS](#) [Lambda](#)


[View all services](#)

Applications (0)

Region: US East (N. Virginia)

us-east-1 (Current Region)

< 1 >

Name	Description	Region	Originating account
<div> Access denied</div>			

[Go to myApplications](#)

Welcome to AWS

AWS Health

Cost and usage

←→↻us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create

☆📄👤Finish update

awsServicesSearch[Option+S]

🖨🔔🔍⚙Global▼rsujithsri16@gmail.com▼

EC2

☰

Access level

Expand all | Collapse all

▶ List (Selected 6/6)

▶ Read (Selected 20/20)

▶ Write (Selected 25/25)

▶ Tagging (Selected 2/2)

▼ Resources

Specify resource ARNs for these actions.

☒ All

☐ Specific

⚠

The all wildcard "*" may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

▶ Request conditions - optional

Actions on resources are allowed or denied only when these conditions are met.

+ Add more permissions

🛡 Security: 0

⊗ Errors: 0

⚠ Warnings: 0

💡 Suggestions: 0

Cancel

Next



[IAM](#) > [Policies](#) > Create policy

Step 1

[Specify permissions](#)

Step 2

Review and create

Review and create [Info](#)

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

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

Description - *optional*

Add a short explanation for this policy.

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

Permissions defined in this policy [Info](#)

Edit

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it



Permissions defined in this policy [Info](#)

Edit

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

Allow (1 of 409 services)

☐ Show remaining 408 services

Service ▲	Access level ▼	Resource	Request condition
CloudWatch	Full access	All resources	None

Add tags - optional [Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create policy

←

→

↺

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:instanceState=running

☆

☰

📱

Finish update ⋮

aws

Services

Search

[Option+S]

N. Virginia ▾

ops-team1 @ 6020-9316-2468 ▾

EC2

EC2 Dashboard

EC2 Global View

Events

Console-to-Code [Preview](#)

► Instances

▼ Images

AMIs

AMI Catalog

▼ Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

▼ Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Instances (1) [Info](#)

Connect

Instance state ▾

Actions ▾

Launch instances ▾

All states ▾

Instance state = running ✕

Clear filters

< 1 > ⚙

<input type="checkbox"/>	Name	Instance ID	Instance state ▾	Instance type ▾	Status check	Alarm status	Availability Zone ▾	PU
<input type="checkbox"/>	instance-mrg	i-04d858dd64f8c9f13	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec

Select an instance

=

✕

←→↺

us-east-1.console.aws.amazon.com/s3/home?region=us-east-1#

☆🔊📱👤

Finish update ⋮

aws

Services

Q Search

[Option+S]

🖨🔔🔗⚙

N. Virginia ▾

ops-team1 @ 6020-9316-2468 ▾

EC2

Amazon S3

×

Buckets

Access Grants

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

▼ Storage Lens

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight 7

▼ Account snapshot All AWS Regions

View Storage Lens dashboard

Last updated: Apr 22, 2024 by Storage Lens. Metrics are generated every 24 hours. Metrics don't include directory buckets. [Learn more](#)

Total storage

Object count

Average object size

3.0 MB

30

103.4 KB

You can enable advanced metrics in the "default-account-dashboard" configuration.

General purpose buckets

Directory buckets

General purpose buckets (6) Info All AWS Regions

🔄

📄 Copy ARN

Empty

Delete

Create bucket

Find buckets by name

< 1 > ⚙

	Name ▲	AWS Region ▾	IAM Access Analyzer	Creation date ▾
<input type="radio"/>	aws-morning-lambda	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 16, 2024, 14:22:09 (UTC+05:30)
<input type="radio"/>	cf-templates-15tthmkg161g-us-east-1	US East (N. Virginia) us-east-1	View analyzer for us-east-1	April 11, 2024, 08:53:16 (UTC+05:30)
<input type="radio"/>	elasticbeanstalk-us-east-1-			December 16, 2023, 09:19:43