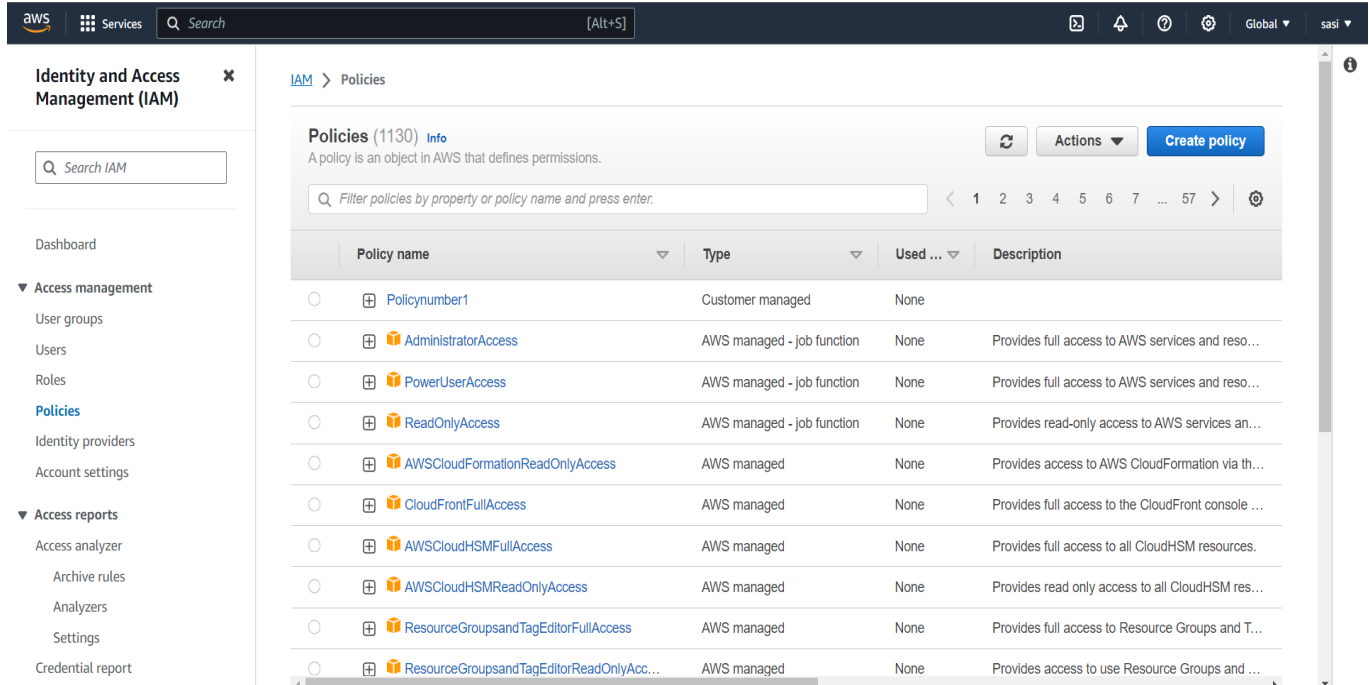


Tasks To Be Performed:

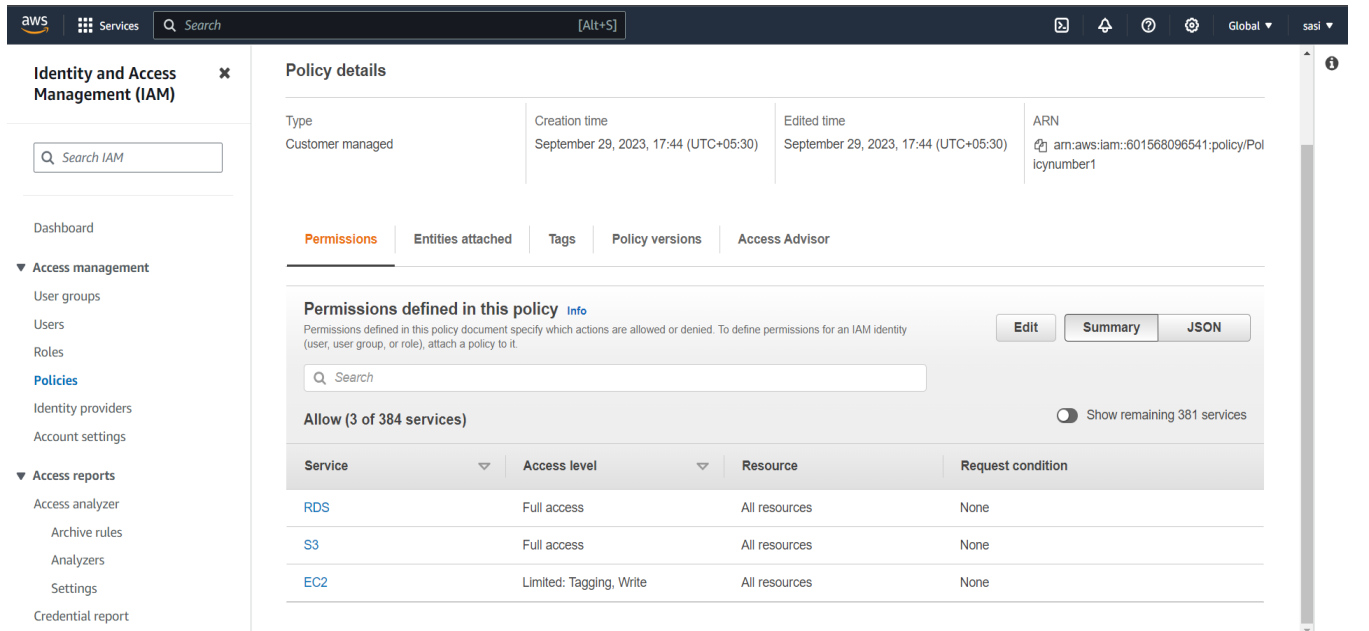
1. Create policy number 1 which lets the users to:
 - a. Access S3 completely
 - b. Only create EC2 instances
 - c. Full access to RDS resources

Answer :



The screenshot shows the AWS IAM console's 'Policies' page. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, User groups, Users, Roles, Policies (selected), Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, and Credential report. The main content area shows a list of 11 policies. The first policy, 'Policynumber1', is highlighted. The table below lists the policies:

Policy name	Type	Used ...	Description
Policynumber1	Customer managed	None	
AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services and reso...
PowerUserAccess	AWS managed - job function	None	Provides full access to AWS services and reso...
ReadOnlyAccess	AWS managed - job function	None	Provides read-only access to AWS services an...
AWSCloudFormationReadOnlyAccess	AWS managed	None	Provides access to AWS CloudFormation via th...
CloudFrontFullAccess	AWS managed	None	Provides full access to the CloudFront console ...
AWSCloudHSMFullAccess	AWS managed	None	Provides full access to all CloudHSM resources.
AWSCloudHSMReadOnlyAccess	AWS managed	None	Provides read only access to all CloudHSM res...
ResourceGroupsandTagEditorFullAccess	AWS managed	None	Provides full access to Resource Groups and T...
ResourceGroupsandTagEditorReadOnlyAcc...	AWS managed	None	Provides access to use Resource Groups and ...



The screenshot shows the 'Policy details' page for 'Policynumber1'. The left sidebar is the same as the previous screenshot. The main content area shows the policy details, including its type (Customer managed), creation time (September 29, 2023, 17:44 (UTC+05:30)), edited time (September 29, 2023, 17:44 (UTC+05:30)), and ARN (arn:aws:iam::601568096541:policy/Policynumber1). The 'Permissions' tab is selected, showing a table of permissions defined in the policy:

Service	Access level	Resource	Request condition
RDS	Full access	All resources	None
S3	Full access	All resources	None
EC2	Limited: Tagging, Write	All resources	None

- 2) Create a policy number 2 which allows the users to:
- Access CloudWatch and billing completely
 - Can only list EC2 and S3

Answer :

The screenshot shows the AWS IAM console 'Specify permissions' page for the 'CloudWatch' service. The page is titled 'Specify permissions' with a sub-header 'Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.' The 'Policy editor' section has tabs for 'Visual', 'JSON', and 'Actions'. Under 'CloudWatch', there is a green 'Allow' button and '1 Actions'. The 'Actions allowed' section has a search bar and a 'Switch to deny permissions' link. The 'Manual actions' section shows 'All CloudWatch actions (cloudwatch:*)' selected. The 'Access level' section shows 'List (Selected 4/4)', 'Read (Selected 12/12)', and 'Write (Selected 21/21)' selected. There are also links for 'Expand all' and 'Collapse all'.

The screenshot shows the AWS IAM console 'Specify permissions' page for the 'EC2' service. The page is titled 'Specify permissions' with a sub-header 'Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.' The 'Policy editor' section has tabs for 'Visual', 'JSON', and 'Actions'. Under 'EC2', there is a green 'Allow' button and '168 Actions'. The 'Actions allowed' section has a search bar and a 'Switch to deny permissions' link. The 'Manual actions' section shows 'All EC2 actions (ec2:*)' selected. The 'Access level' section shows 'List (Selected 168/168)' selected. The 'All list actions' section shows a grid of 24 actions, all of which are selected with checkboxes. The actions are: DescribeAccountAttributes, DescribeAddresses, DescribeAddressesAttribute, DescribeAddressTransfers, DescribeAggregateIdFormat, DescribeAvailabilityZones, DescribeAwsNetworkPerformanceMetricSubscriptions, DescribeBundleTasks, DescribeByoipCidrs, DescribeCapacityReservations, DescribeCarrierGateways, DescribeClientVpnConnections, DescribeClassicLinkInstances, DescribeClientVpnAuthorizationRules, DescribeClientVpnEndpoints, DescribeClientVpnRoutes, DescribeClientVpnTargetNetworks, DescribeCoipPools, DescribeConversionTasks, and DescribeCustomerGateways.

aws

Services

Search

[Alt+S]

Global

sasi

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

▼ Billing

Allow 1 Actions

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

▼ Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Switch to deny permissions

Manual actions | Add actions

☒ All Billing actions (billing:*)

Access level

▶ Read (Selected 9/9)

▶ Write (Selected 4/4)

▶ Resources

Specified resource ARNs for these actions.

*

▶ Request conditions - optional

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

aws

Services

Search

[Alt+S]

Global

sasi

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

VisualJSONActions

▶ CloudWatch

Allow 1 Actions

▶ Billing

Allow 1 Actions

▶ EC2

Allow 168 Actions

▶ S3

Allow 10 Actions

+ Add more permissions

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

aws

Services

Search

[Alt+S]

Global

sasi

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

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

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report

TypeCustomer managed

Creation timeOctober 01, 2023, 21:57 (UTC+05:30)

Edited timeOctober 01, 2023, 21:57 (UTC+05:30)

ARNarn:aws:iam::601568096541:policy/policynumber2

PermissionsEntities attachedTagsPolicy versionsAccess Advisor

Permissions defined in this policy

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 (4 of 384 services)

Show remaining 380 services

Service	Access level	Resource	Request condition
S3	Full: List	All resources	None
CloudWatch	Full access	All resources	None
EC2	Limited: List	All resources	None
Billing	Full access	All resources	None

3) Attach policy number 1 to the Dev Team from task 1

Answer :

aws

Services

Search

[Alt+S]

Global

sasi

Attach policy number 1 as a permissions policy

To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

IAM Entities (10)

Entities are IAM users, user groups and roles.

Search

Any entity types

< 1 >

Entity name

Entity type

<input type="checkbox"/>	Dev1	IAM Users
<input type="checkbox"/>	Dev2	IAM Users
<input type="checkbox"/>	Test1	IAM Users
<input type="checkbox"/>	Test2	IAM Users
<input checked="" type="checkbox"/>	DevTeam	User groups
<input type="checkbox"/>	OpsTeam	User groups
<input type="checkbox"/>	AWSServiceRoleForAmazonElasticFileSystem	Roles
<input type="checkbox"/>	AWSServiceRoleForBackup	Roles
<input type="checkbox"/>	AWSServiceRoleForSupport	Roles
<input type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	Roles

Services
 [Alt+S]

Identity and Access Management (IAM)

- Dashboard
- Access management
 - User groups
 - Users
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analyzers
 - Settings
 - Credential report

Policy details

Type Customer managed	Creation time September 29, 2023, 17:44 (UTC+05:30)	Edited time September 29, 2023, 17:44 (UTC+05:30)	ARN arn:aws:iam::601568096541:policy/PolicyNumber1
--------------------------	--	--	---

Permissions |
 Entities attached |
 Tags |
 Policy versions |
 Access Advisor

▼ Attached as a permissions policy (1)

To grant permissions to an entity, attach a permissions policy to it.

Any entity types ▼

Attach
Detach

<input type="checkbox"/>	Entity name	Entity type
<input type="checkbox"/>	DevTeam	User groups

▼ Attached as a permissions boundary (0)

Use this policy as a permissions boundary to control the maximum permissions that an entity can have. This is an

aws

Services

Search

[Alt+S]

Global

sasi

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

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

Access reports

- Access analyzer
 - Archive rules
 - Analyzers
 - Settings
- Credential report

IAM > Policies > policynumber2

policynumber2

Delete

Policy details

Type	Creation time	Edited time	ARN
Customer managed	October 01, 2023, 21:57 (UTC+05:30)	October 01, 2023, 21:57 (UTC+05:30)	arn:aws:iam::601568096541:policy/policynumber2

Permissions

Entities attached

Tags

Policy versions

Access Advisor

Attached as a permissions policy (1)

To grant permissions to an entity, attach a permissions policy to it.

AttachDetach

Search

Any entity types

< 1 >

Entity name	Entity type
OpsTeam	User groups