Introduction to IAM and Cloudwatch

Assignment -1 IAM User

Problem Statement

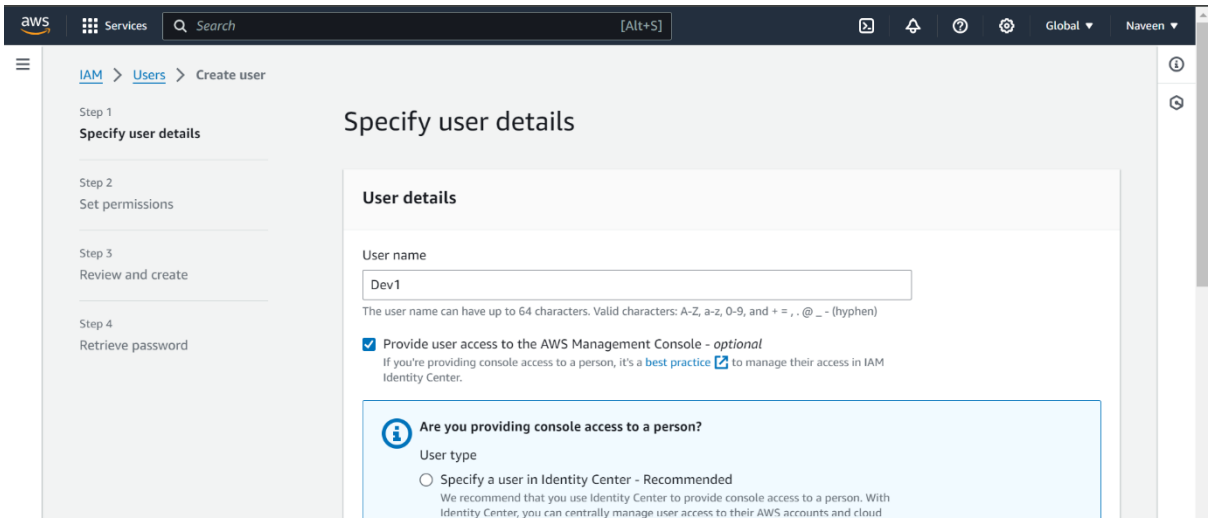
You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

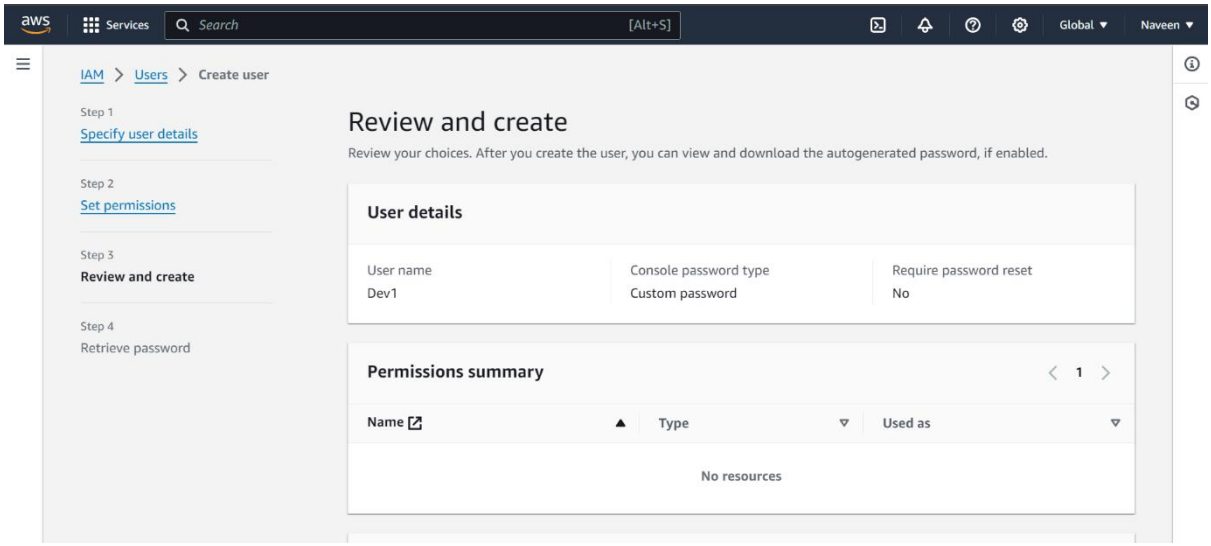
Task to be performed:

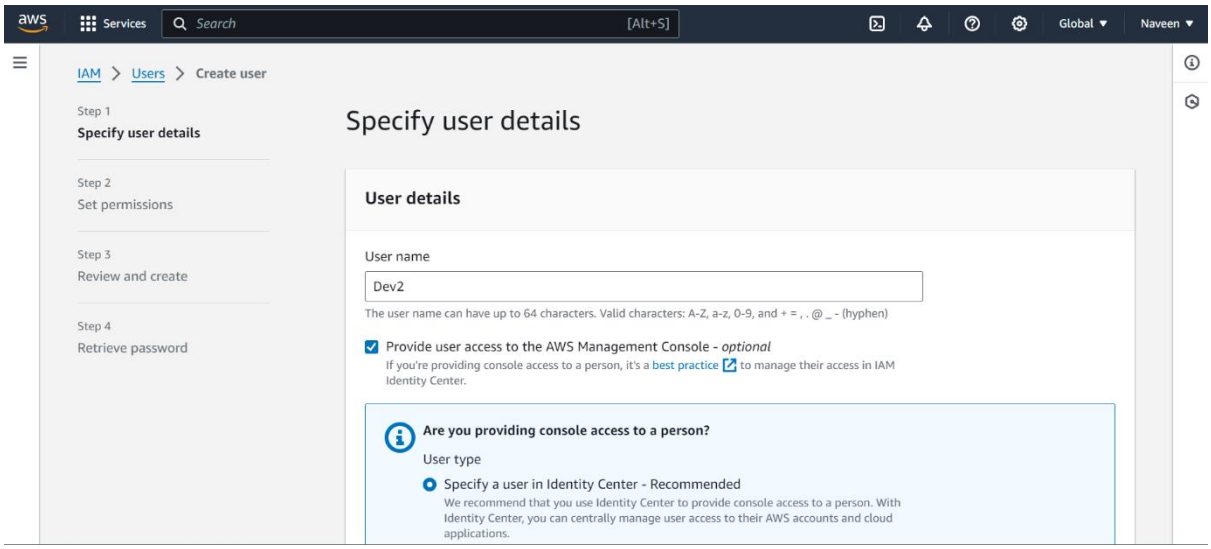
1. Create 4 IAM users named “Dev1”, “Dev2”, “Test1” and “Test2”
2. Create 2 groups named “Dev Team” and “Ops Team”
3. Add Dev1 and Dev2 to the dev Team.
4. Add Dev1, Test and Test2 to the Ops team.

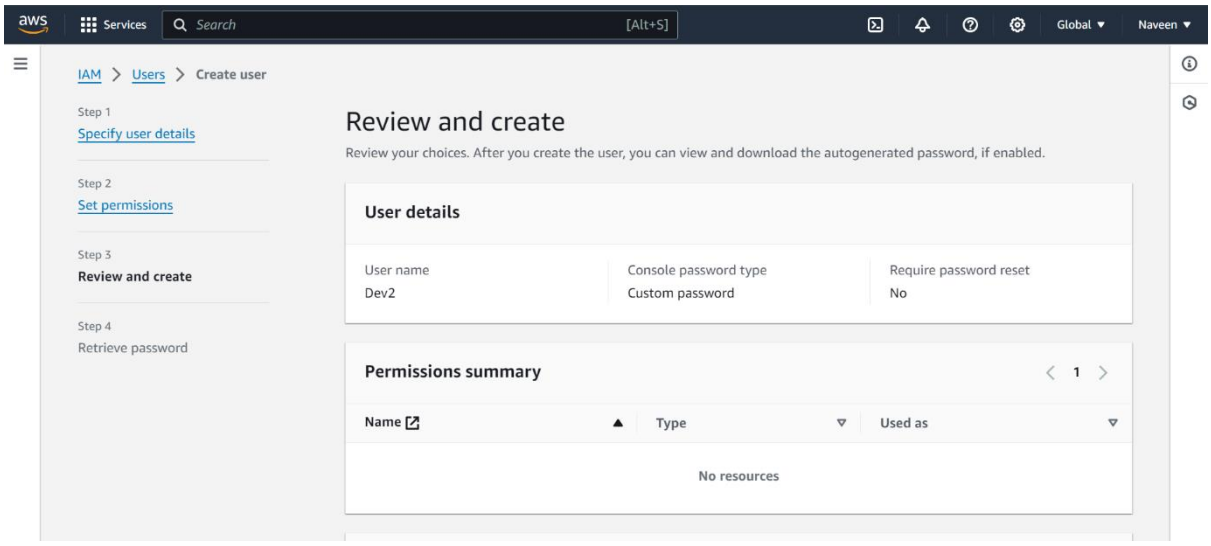
Septs

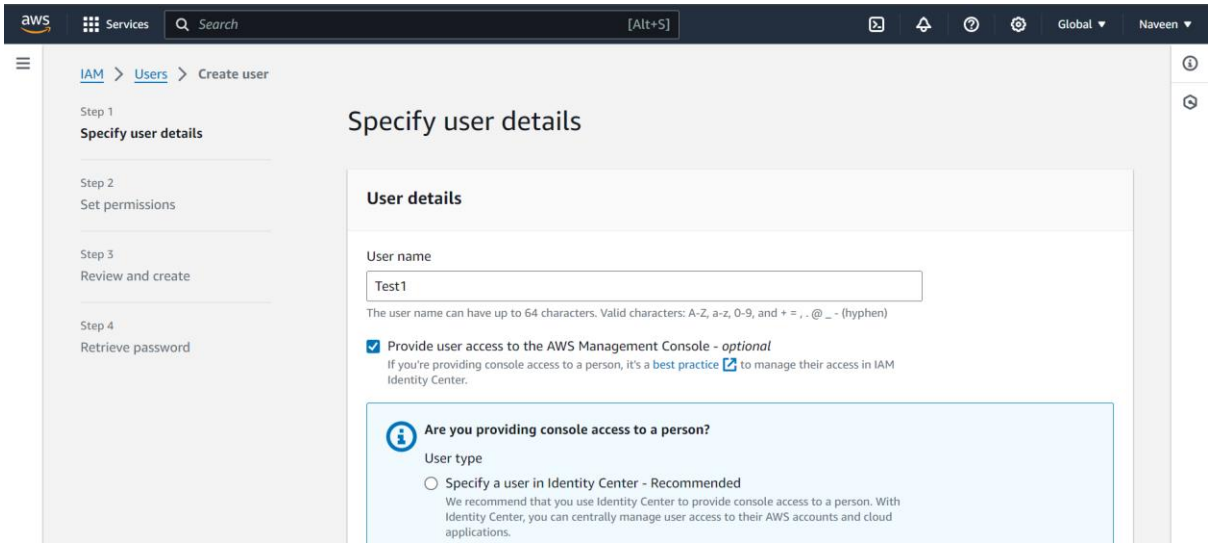
- Click the create user
- Provide the user name and password
- Create 4 IAM users

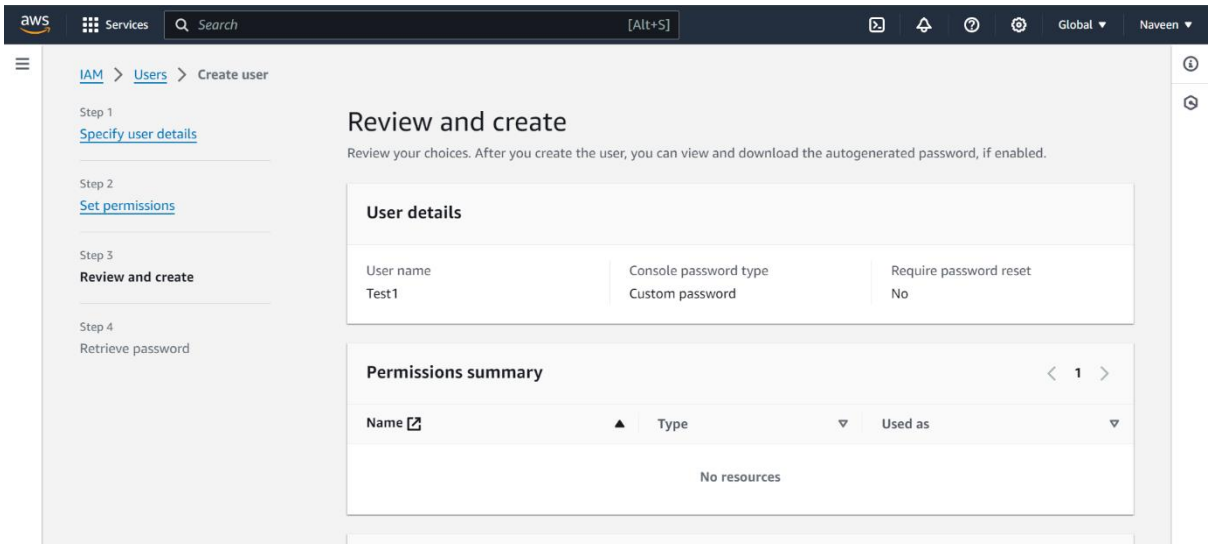


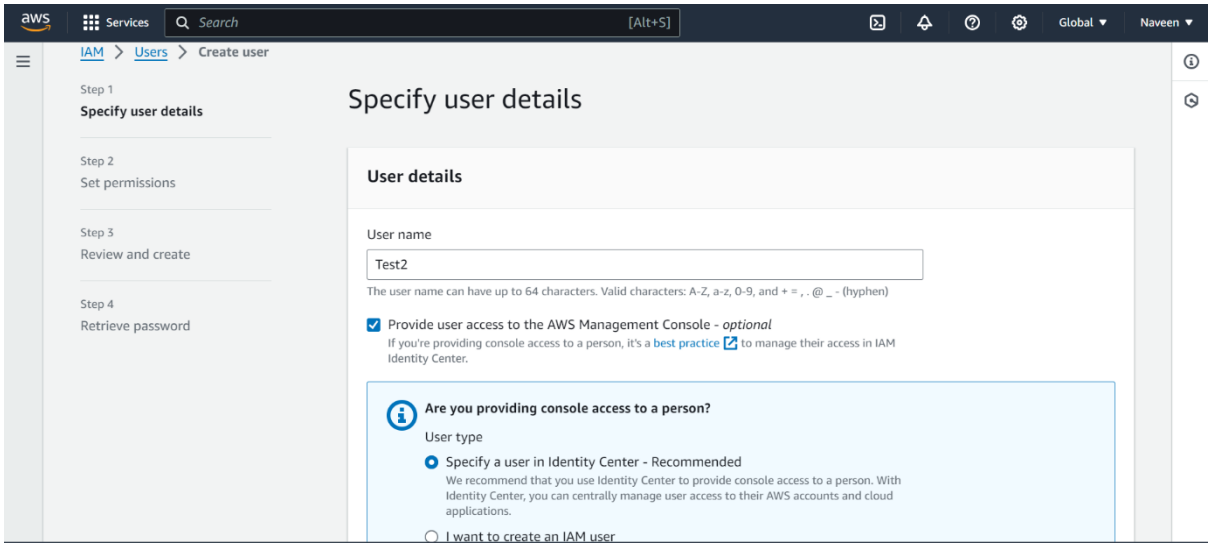

aws
Services
Search
[Alt+S]
Global
Naveen
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
Dev1
Console password type
Custom password
Require password reset
No
Permissions summary
1
Name
Type
Used as
No resources

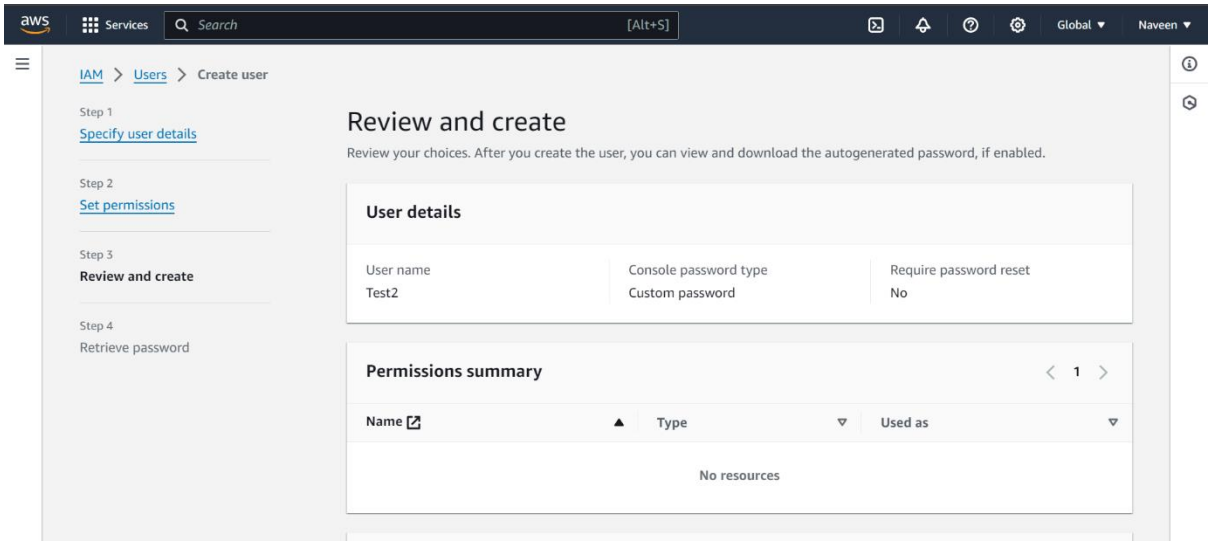

aws
Services
Search
[Alt+S]
Global
Naveen
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
Dev2
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.
Are you providing console access to a person?
User type
Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

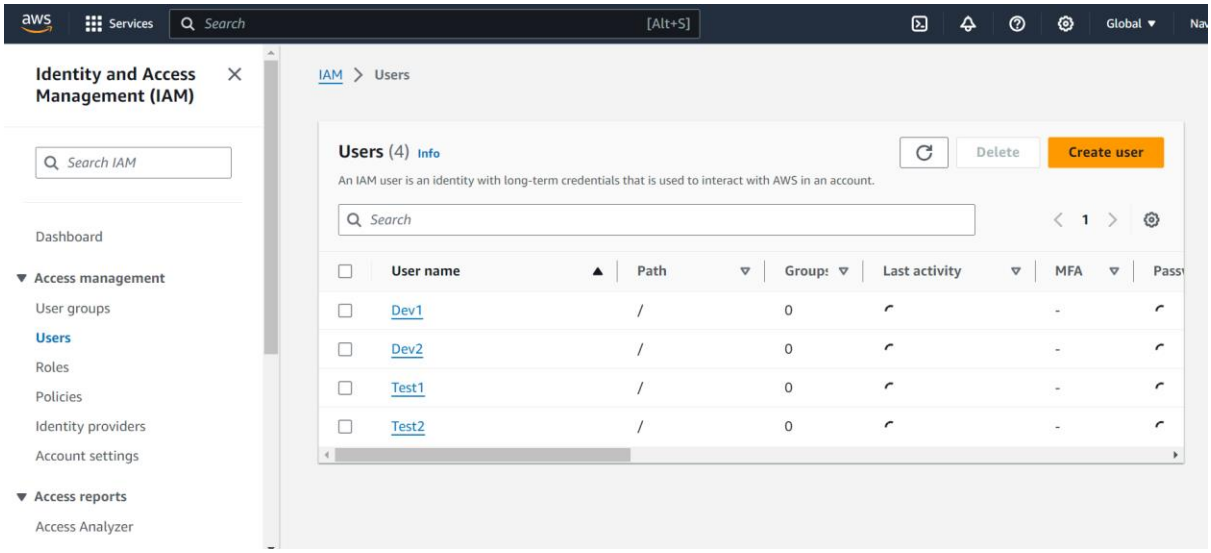

aws
Services
Search
[Alt+S]
Global
Naveen
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
Dev2
Console password type
Custom password
Require password reset
No
Permissions summary
1
Name
Type
Used as
No resources


aws
Services
Search
[Alt+S]
Global
Naveen
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
Test1
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.
Are you providing console access to a person?
User type
Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

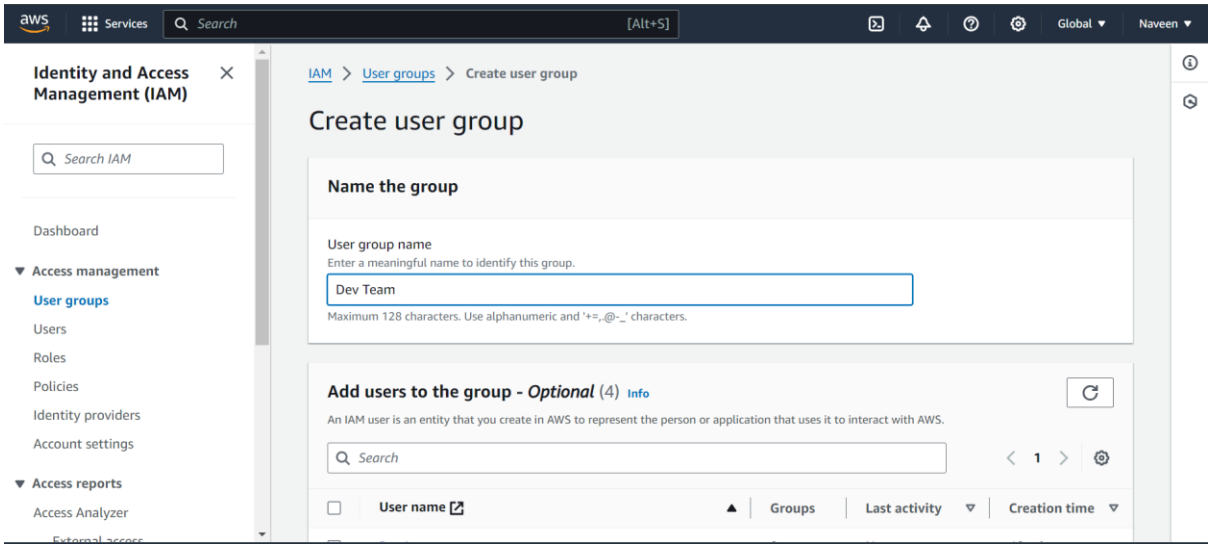

aws
Services
Search
[Alt+S]
Global
Naveen
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
Test1
Console password type
Custom password
Require password reset
No
Permissions summary
1
Name
Type
Used as
No resources

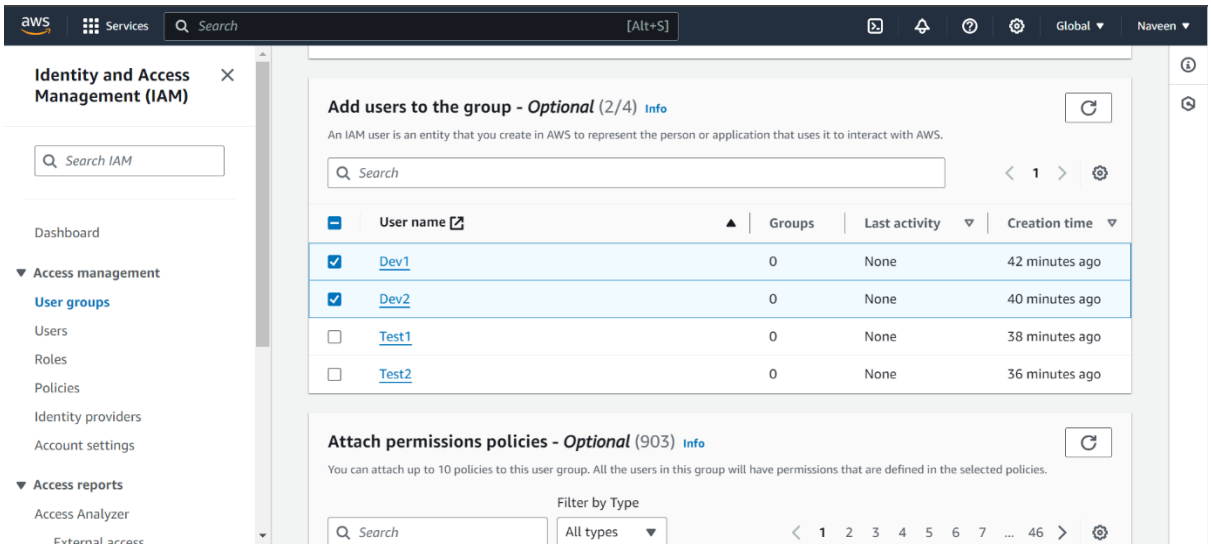

aws
Services
Search
[Alt+S]
Global
Naveen
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
Test2
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.
Are you providing console access to a person?
User type
Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
I want to create an IAM user

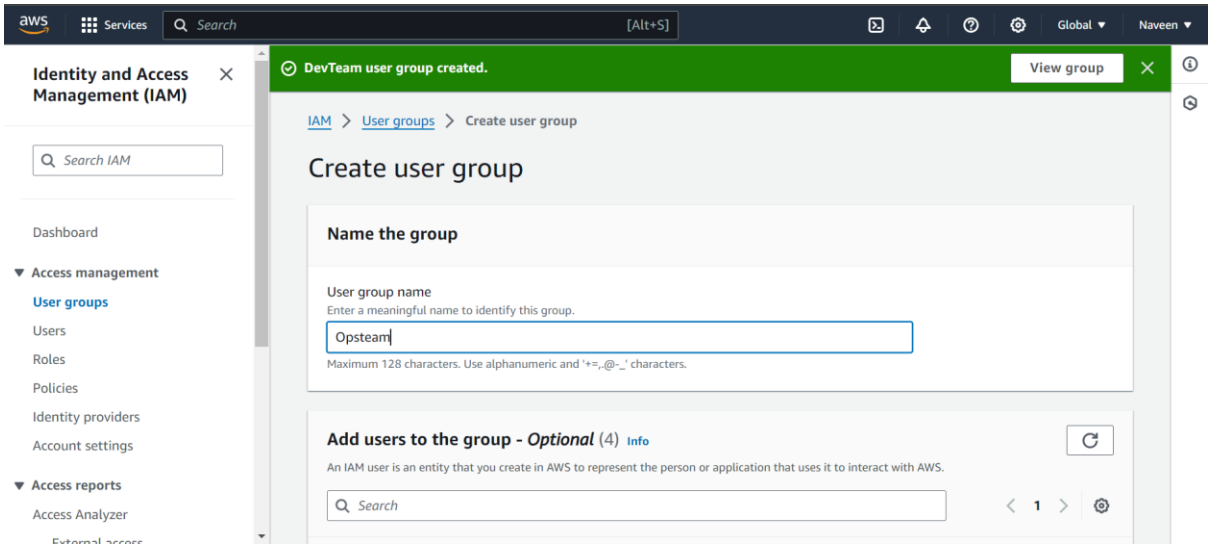


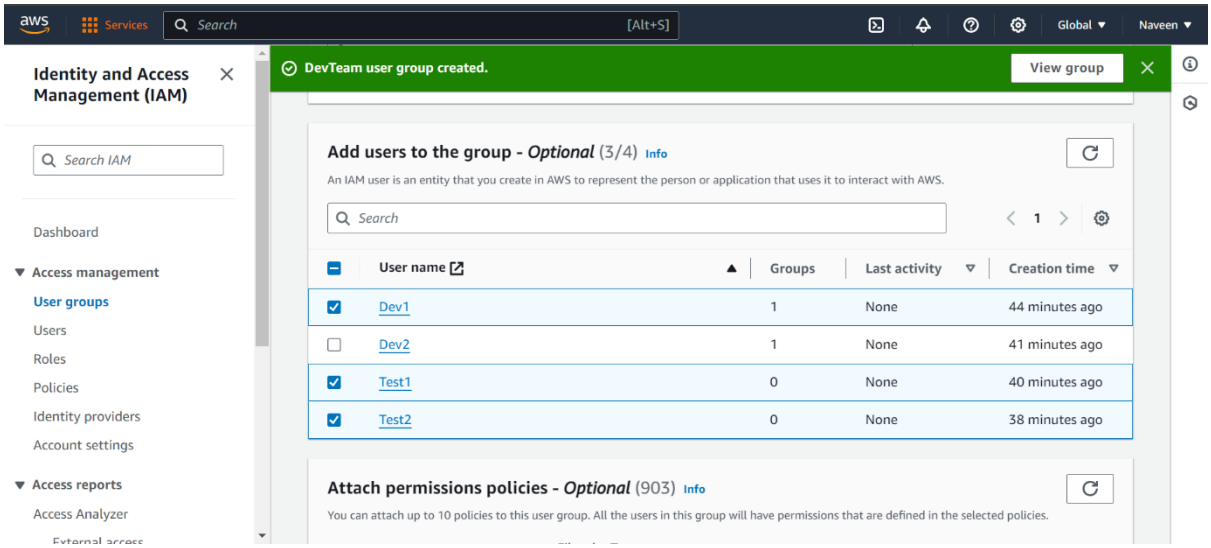


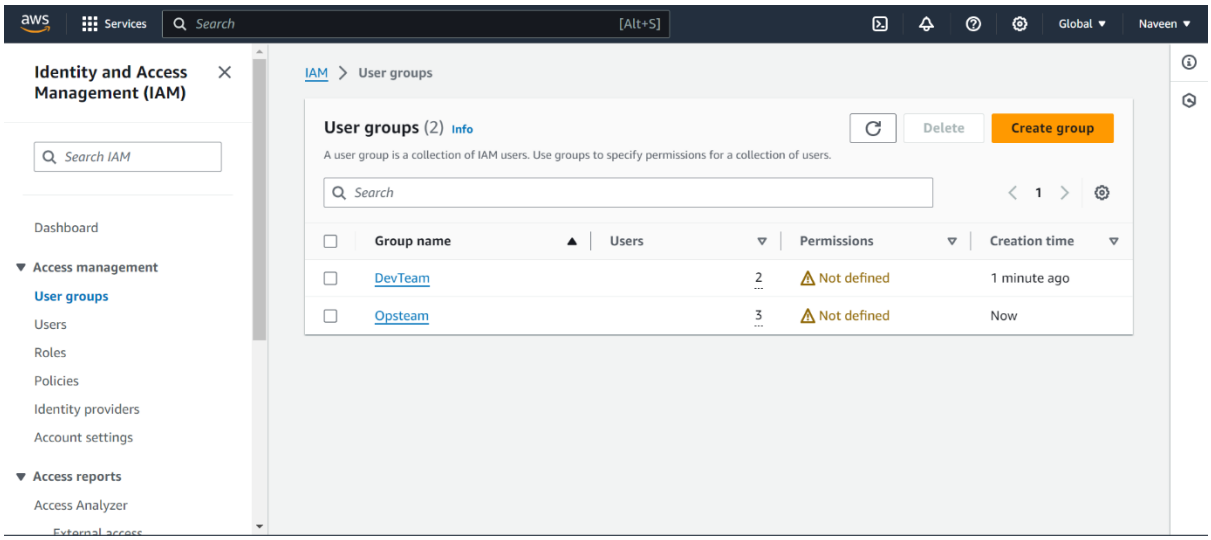
- Click the create group
- Provide the user group name
- Add user to the group (Add Dev1 and Dev2 to the dev Team; Add Dev1, Test and Test2 to the Ops team)
- Create 2 groups


aws
Services
Search
[Alt+S]
Global
Naveen
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
IAM > User groups > Create user group
Create user group
Name the group
User group name
Enter a meaningful name to identify this group.
Dev Team
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Add users to the group - Optional (4) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Search
1
User name
Groups
Last activity
Creation time


aws
Services
Search
[Alt+S]
Global
Naveen
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
Add users to the group - Optional (2/4) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Search
1
User name
Groups
Last activity
Creation time
Dev1 0 None 42 minutes ago
Dev2 0 None 40 minutes ago
Test1 0 None 38 minutes ago
Test2 0 None 36 minutes ago
Attach permissions policies - Optional (903) Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.
Filter by Type
Search
All types
1 2 3 4 5 6 7 ... 46


aws
Services
Search
[Alt+S]
Global
Naveen
Identity and Access Management (IAM)
DevTeam user group created.
View group
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
IAM > User groups > Create user group
Create user group
Name the group
User group name
Enter a meaningful name to identify this group.
Opsteam
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Add users to the group - Optional (4) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Search
1


aws
Services
Search
[Alt+S]
Global
Naveen
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
DevTeam user group created.
View group
Add users to the group - Optional (3/4) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Search
1
User name
Groups
Last activity
Creation time
Dev1 1 None 44 minutes ago
Dev2 1 None 41 minutes ago
Test1 0 None 40 minutes ago
Test2 0 None 38 minutes ago
Attach permissions policies - Optional (903) Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.


aws
Services
Search
[Alt+S]
Global
Naveen
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
IAM > User groups
User groups (2) Info
Delete
Create group
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Search
1
Group name
Users
Permissions
Creation time
DevTeam 2 Not defined 1 minute ago
Opsteam 3 Not defined Now

Assignment – 2 IAM Policies

Problem Statement

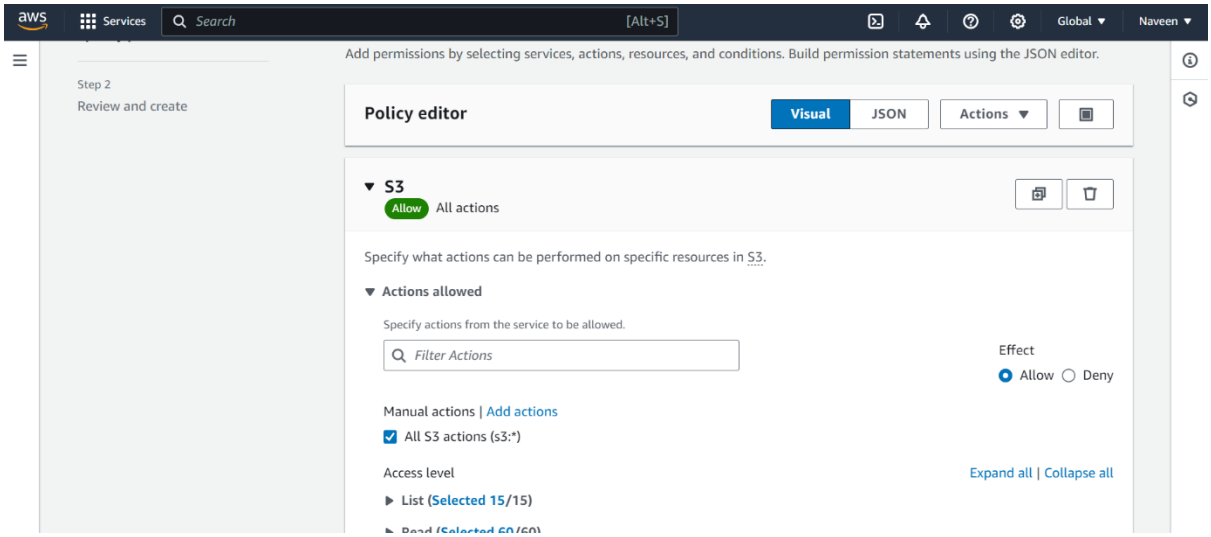
You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

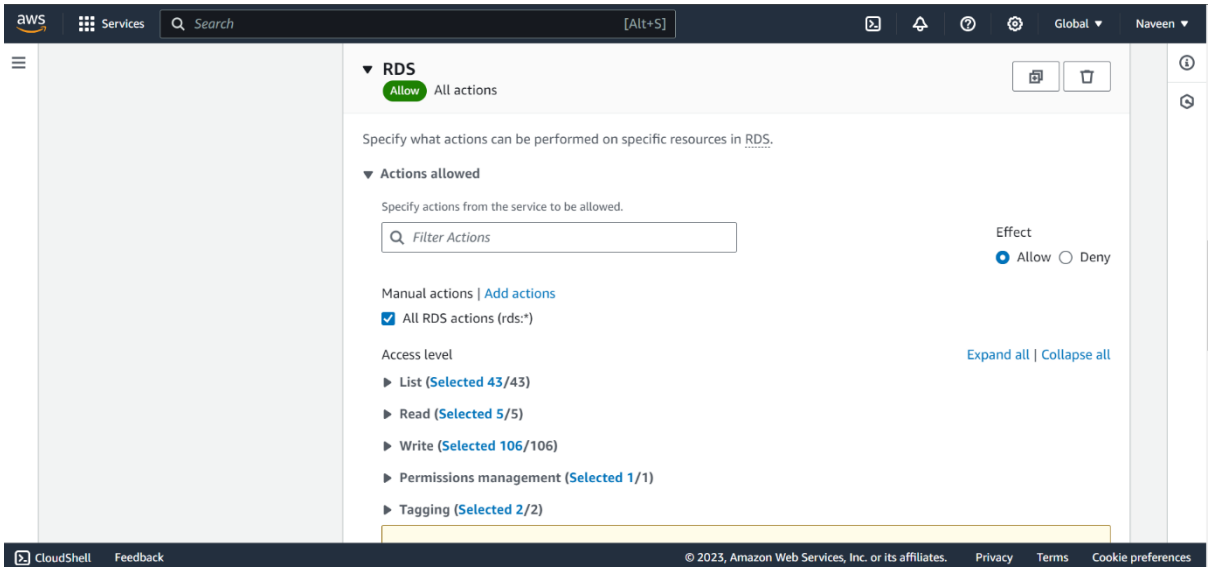
Task to be performed:

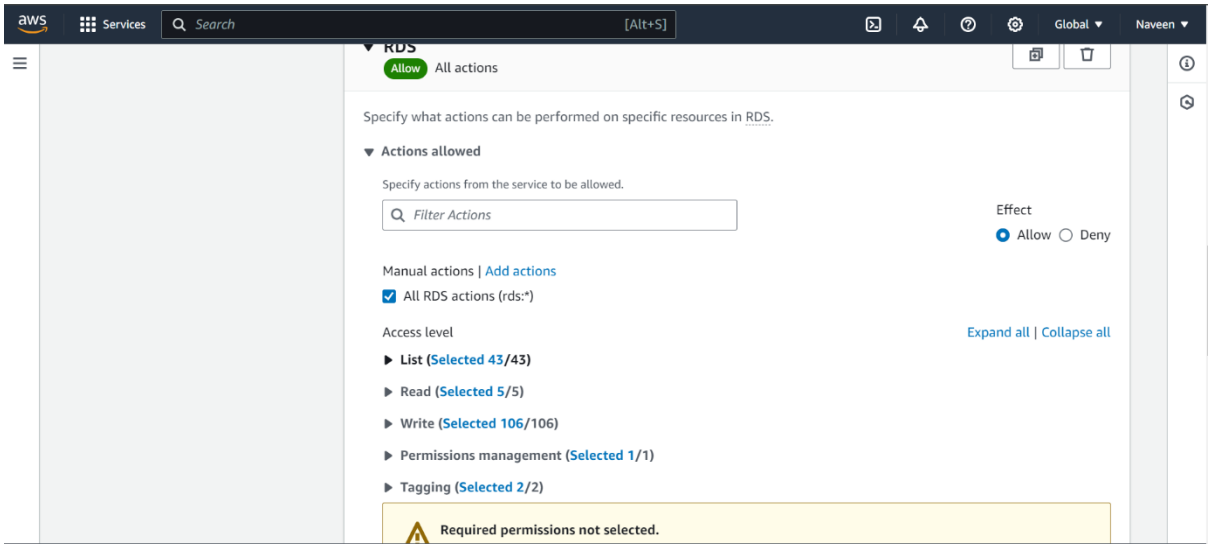
1. Create policy number 1 which lets the users to:
    a) Access S3 completely
    b) Only create EC2 instances
    c) Full access to RDS
2. Create a policy number 2 which allows the users to:
    a) Access cloudwatch and billing completely
    b) Can only list EC2 and S3 resources
3. Attach policy number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

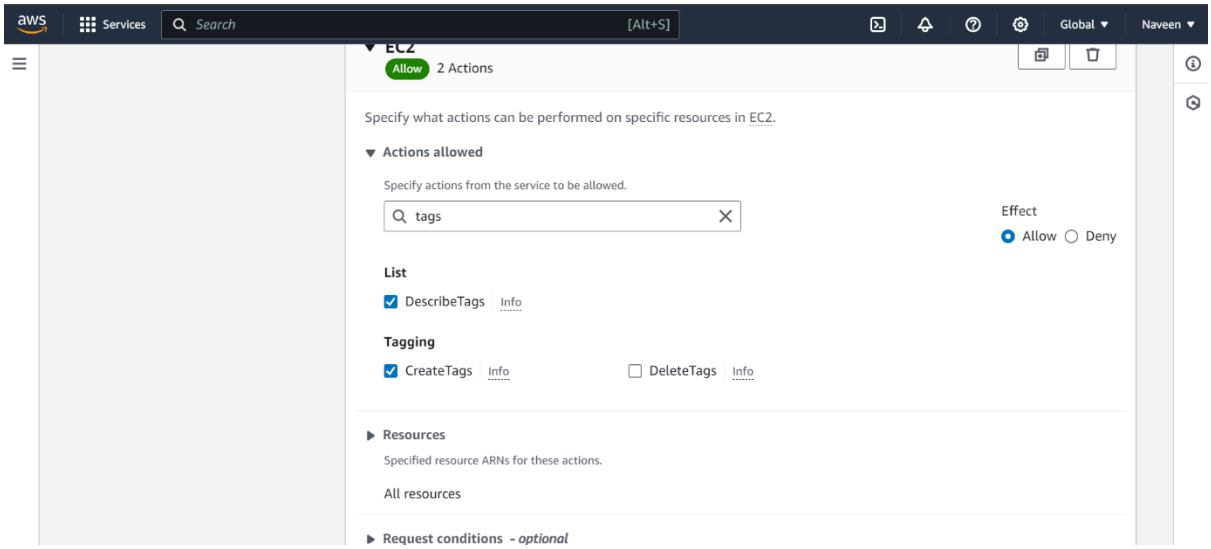
Steps:

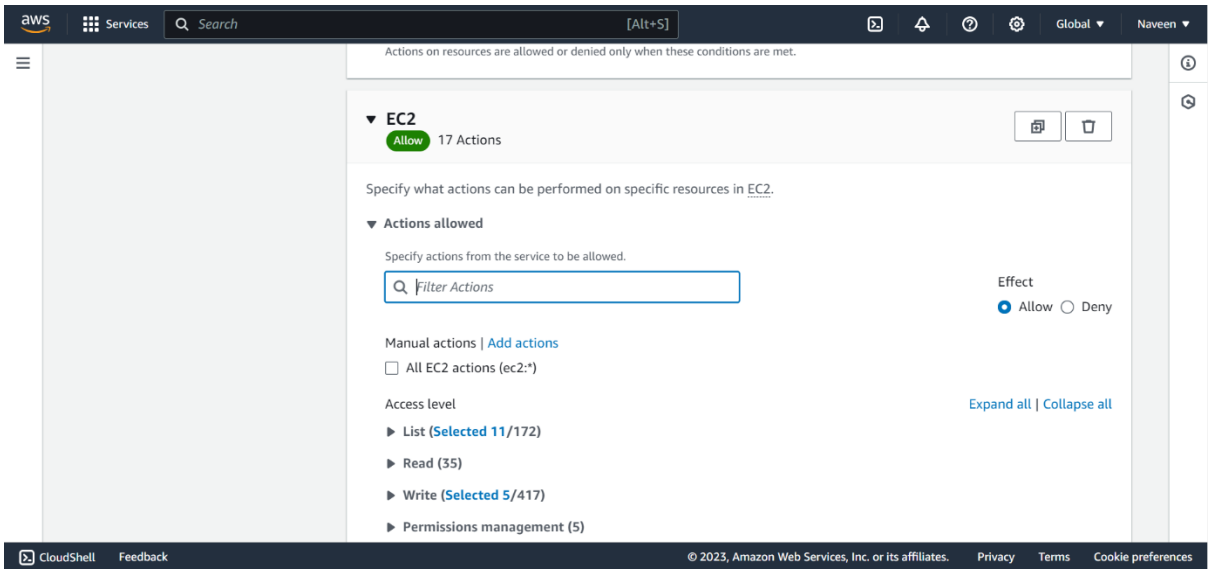
- Click the create policy (policy – 1)
    a) Provide S3 full access, RDS full access and EC2 create only instance
    b) Provide a policy name
    c) Finally policy 1 is created
- Click the create policy (policy – 2)
    a) Provide cloudwatch full access and billing full access
    b) And provide list access for EC2 and S3
    c) Provide a policy name
    d) Finally policy 2 is created
- Go inside the user group which was created in task-1
- Go permission and click add permission
- And attach the policy which was created (Attach policy number 1 to the Dev team and Attach policy number 2 to Ops team)
- Finally policy have been attached

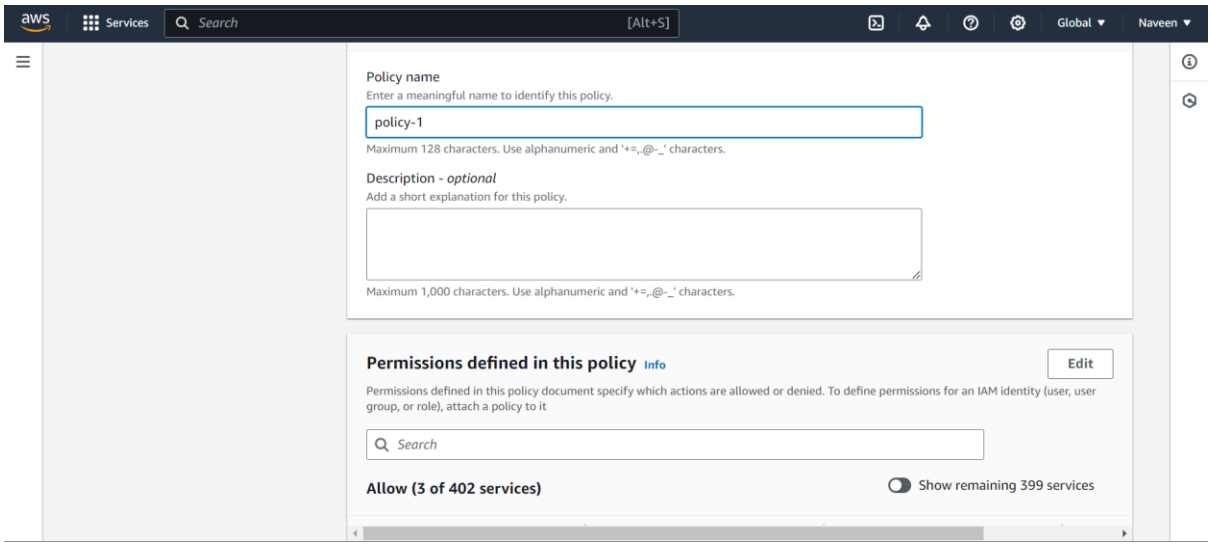

aws
Services
Search
[Alt+S]
Global
Naveen
Step 2
Review and create
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
S3
Allow
All actions
Specify what actions can be performed on specific resources 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)

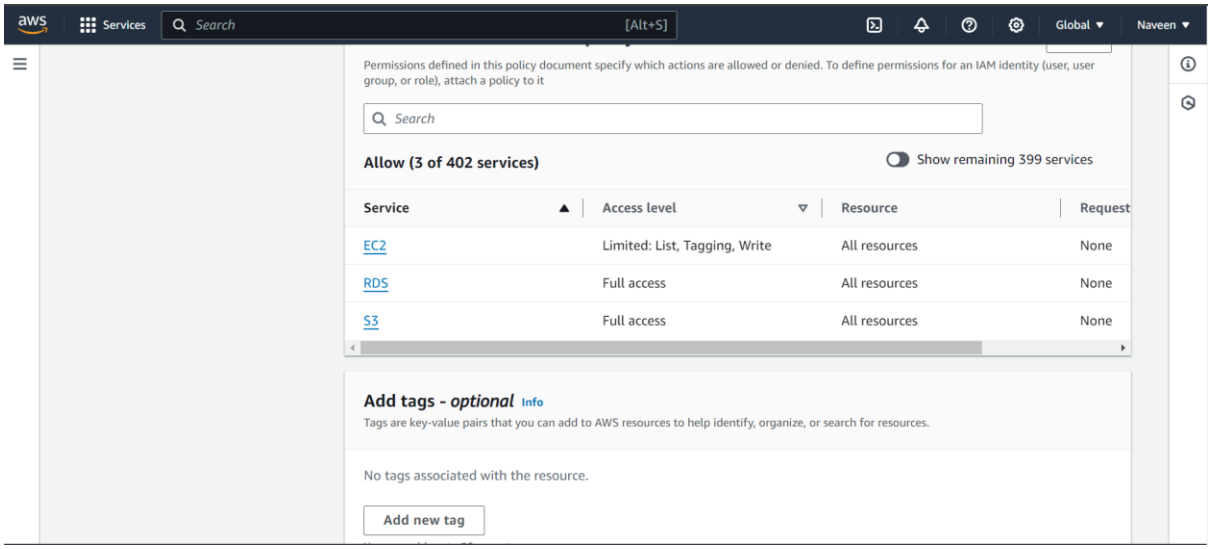

aws
Services
Search
[Alt+S]
Global
Naveen
RDS
Allow
All actions
Specify what actions can be performed on specific resources in RDS.
Actions allowed
Specify actions from the service to be allowed.
Filter Actions
Effect
Allow
Deny
Manual actions | Add actions
All RDS actions (rds:*)
Access level
Expand all | Collapse all
List (Selected 43/43)
Read (Selected 5/5)
Write (Selected 106/106)
Permissions management (Selected 1/1)
Tagging (Selected 2/2)
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

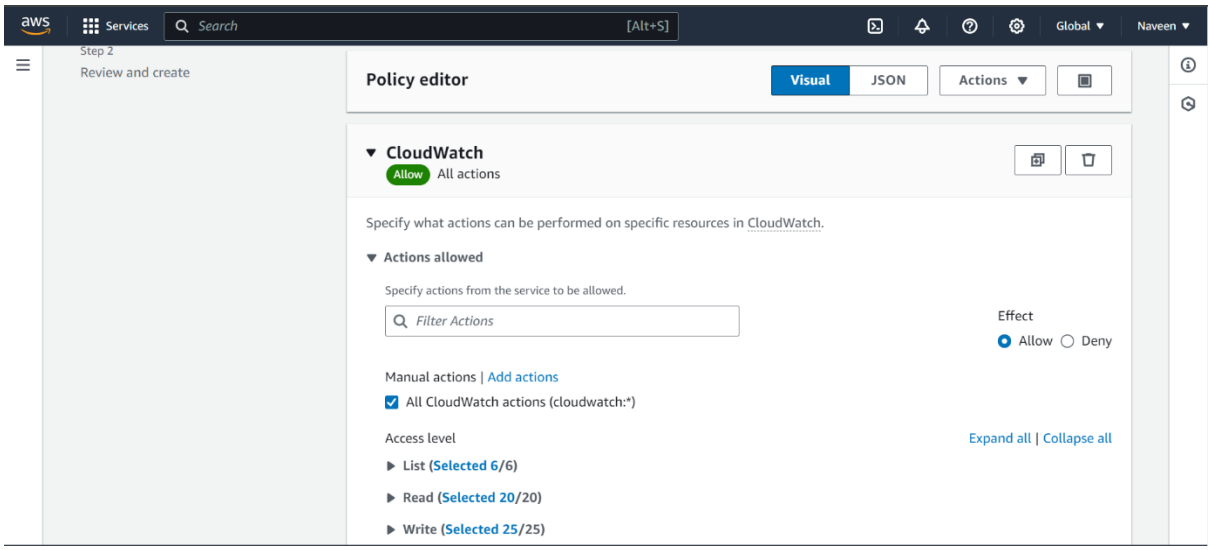

aws
Services
Search
[Alt+S]
Global
Naveen
RDS
Allow
All actions
Specify what actions can be performed on specific resources in RDS.
Actions allowed
Specify actions from the service to be allowed.
Filter Actions
Effect
Allow
Deny
Manual actions | Add actions
All RDS actions (rds:*)
Access level
Expand all | Collapse all
List (Selected 43/43)
Read (Selected 5/5)
Write (Selected 106/106)
Permissions management (Selected 1/1)
Tagging (Selected 2/2)
Required permissions not selected.

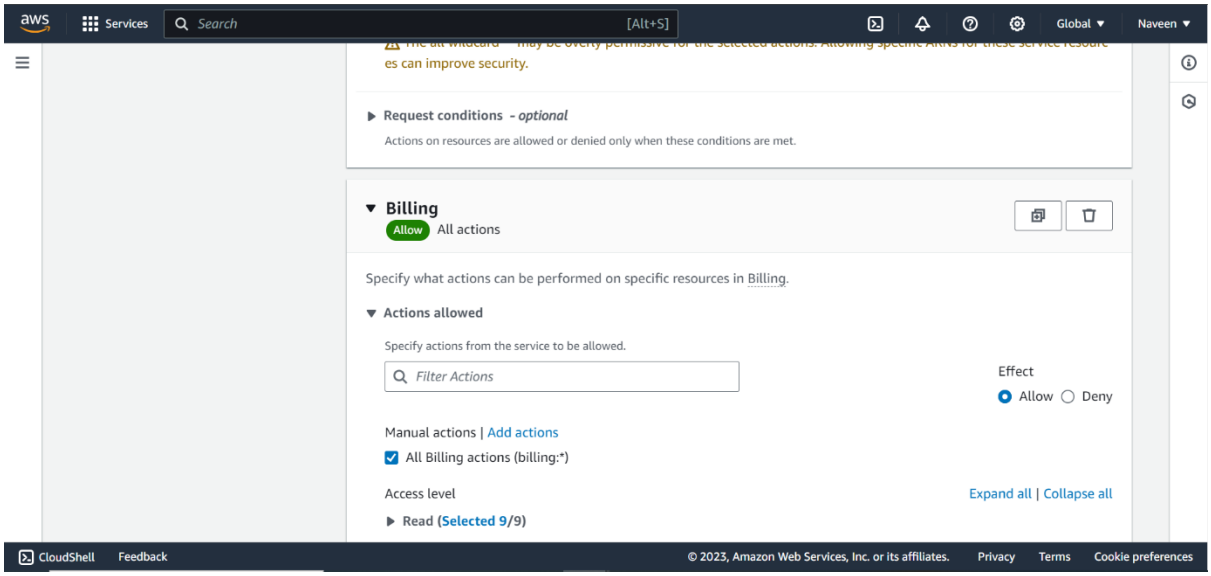

aws
Services
Search
[Alt+S]
Global
Naveen
EC2
Allow
2 Actions
Specify what actions can be performed on specific resources in EC2.
Actions allowed
Specify actions from the service to be allowed.
tags
Effect
Allow
Deny
List
DescribeTags
Info
Tagging
CreateTags
Info
DeleteTags
Info
Resources
Specified resource ARNs for these actions.
All resources
Request conditions - optional

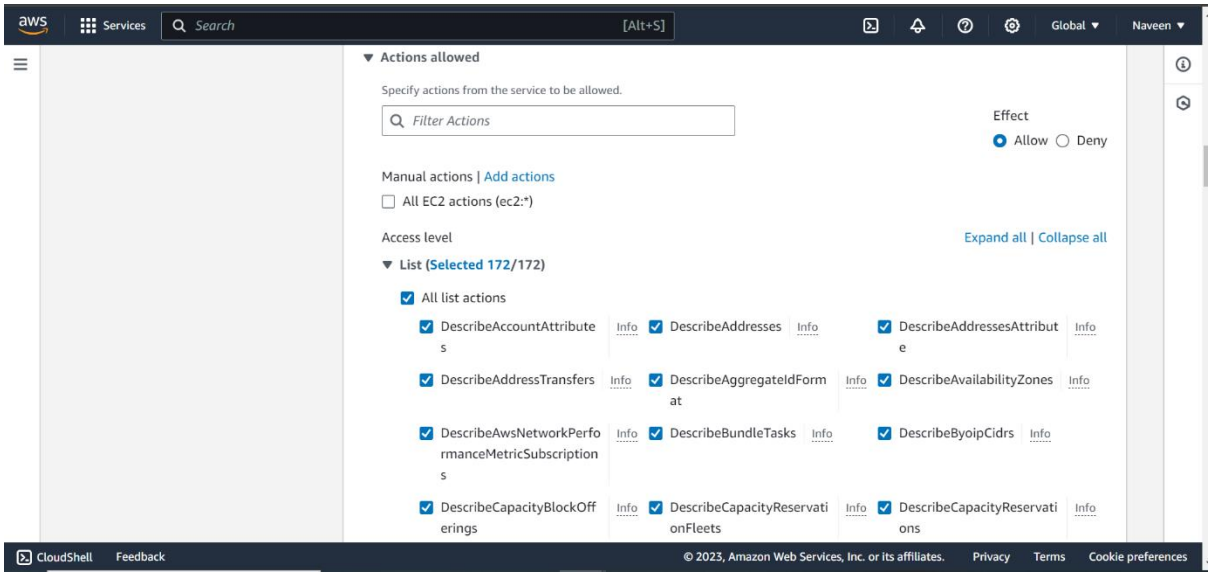

aws
Services
Search
[Alt+S]
Global
Naveen
Actions on resources are allowed or denied only when these conditions are met.
EC2
Allow
17 Actions
Specify what actions can be performed on specific resources in EC2.
Actions allowed
Specify actions from the service to be allowed.
Filter Actions
Effect
Allow
Deny
Manual actions | Add actions
All EC2 actions (ec2:*)
Access level
Expand all | Collapse all
List (Selected 11/172)
Read (35)
Write (Selected 5/417)
Permissions management (5)
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

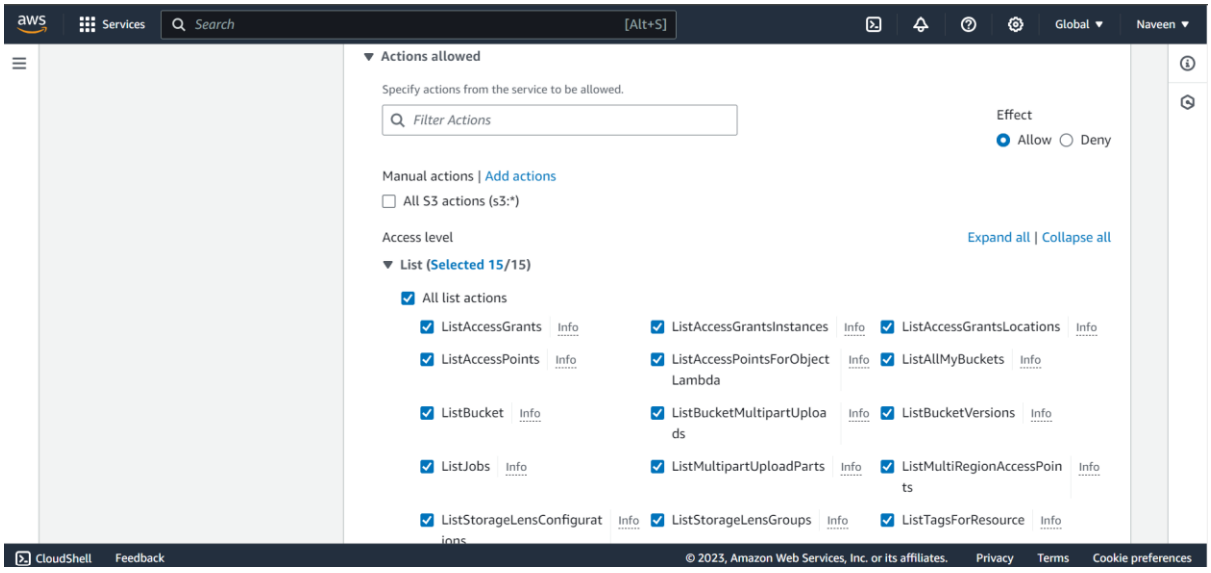

aws
Services
Search
[Alt+S]
Global
Naveen
Policy name
Enter a meaningful name to identify this policy.
policy-1
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.
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
Search
Allow (3 of 402 services)
Show remaining 399 services

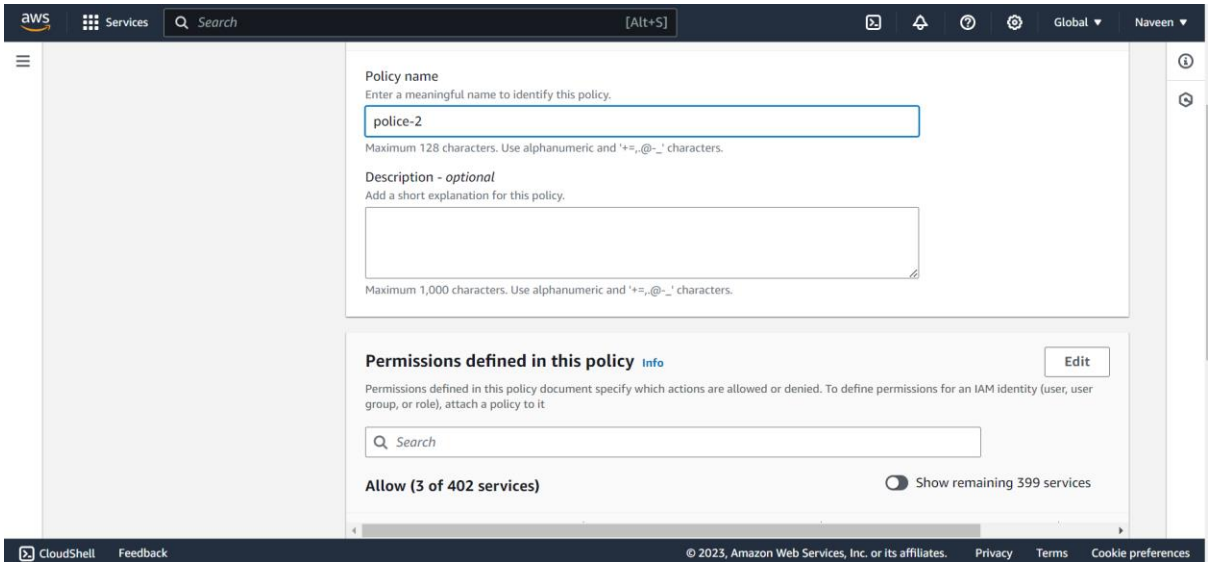

aws
Services
Search
[Alt+S]
Global
Naveen
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
Search
Allow (3 of 402 services)
Show remaining 399 services
Service
Access level
Resource
Request
EC2
Limited: List, Tagging, Write
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

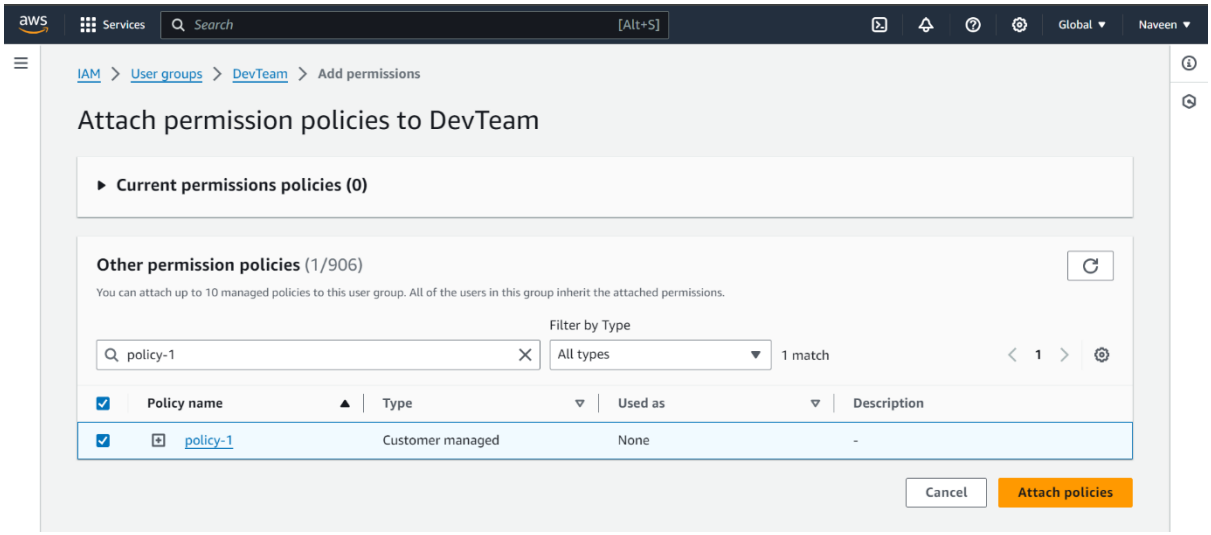

aws
Services
Search
[Alt+S]
Global
Naveen
Step 2
Review and create
Policy editor
Visual
JSON
Actions
CloudWatch
Allow
All actions
Specify what actions can be performed on specific resources in CloudWatch.
Actions allowed
Specify actions from the service to be allowed.
Filter Actions
Effect
Allow
Deny
Manual actions | Add actions
All CloudWatch actions (cloudwatch:*)
Access level
Expand all | Collapse all
List (Selected 6/6)
Read (Selected 20/20)
Write (Selected 25/25)

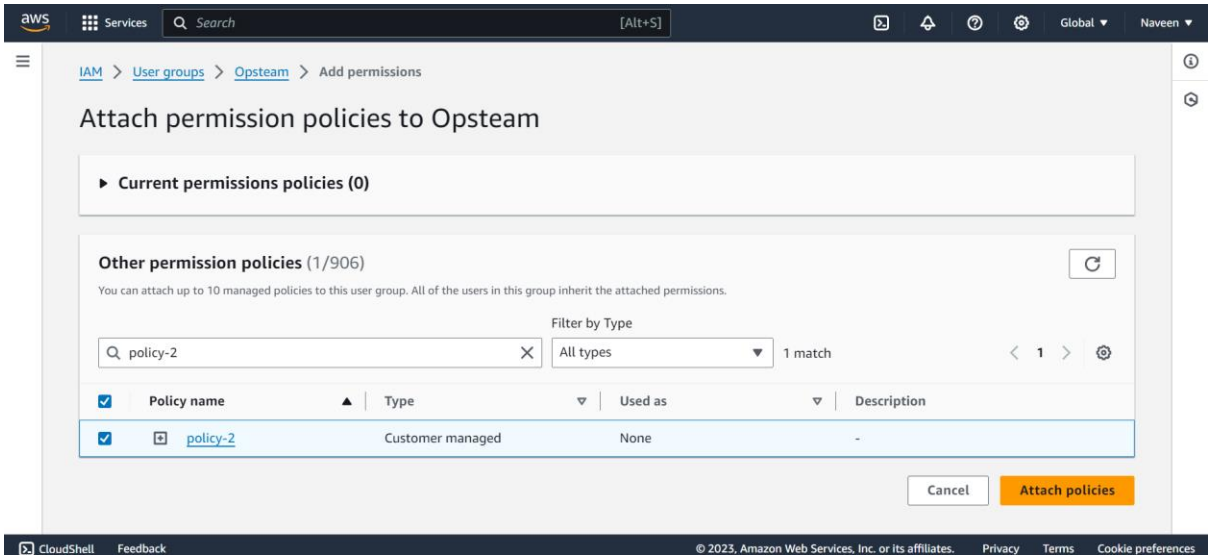

aws
Services
Search
[Alt+S]
Global
Naveen
es can improve security.
Request conditions - optional
Actions on resources are allowed or denied only when these conditions are met.
Billing
Allow
All actions
Specify what actions can be performed on specific resources in Billing.
Actions allowed
Specify actions from the service to be allowed.
Filter Actions
Effect
Allow
Deny
Manual actions | Add actions
All Billing actions (billing:*)
Access level
Expand all | Collapse all
Read (Selected 9/9)
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

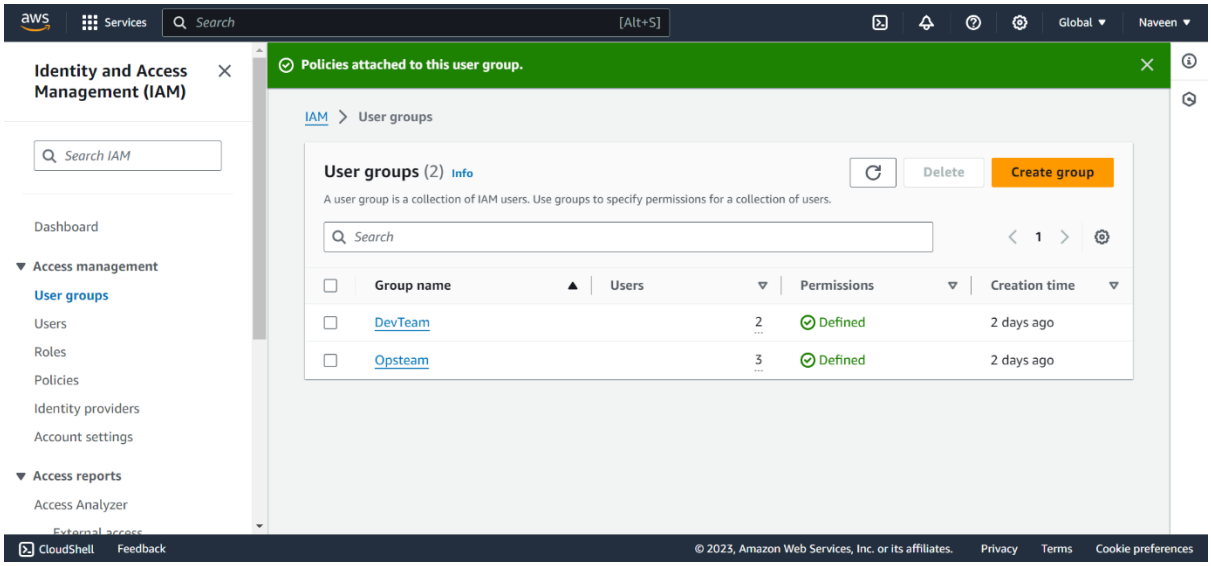

aws
Services
Search
[Alt+S]
Global
Naveen
Actions allowed
Specify actions from the service to be allowed.
Filter Actions
Effect
Allow
Deny
Manual actions | Add actions
All EC2 actions (ec2:*)
Access level
Expand all | Collapse all
List (Selected 172/172)
All list actions
DescribeAccountAttributes
DescribeAddresses
DescribeAddressesAttribute
DescribeAddressTransfers
DescribeAggregateIdFormat
DescribeAvailabilityZones
DescribeAwsNetworkPerformanceMetricSubscriptions
DescribeBundleTasks
DescribeByoipCidrs
DescribeCapacityBlockOfferings
DescribeCapacityReservationFleets
DescribeCapacityReservations
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Global
Naveen
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)
All list actions
ListAccessGrants
ListAccessGrantsInstances
ListAccessGrantsLocations
ListAccessPoints
ListAccessPointsForObjectLambda
ListAllMyBuckets
ListBucket
ListBucketMultipartUploads
ListBucketVersions
ListJobs
ListMultipartUploadParts
ListMultiRegionAccessPoints
ListStorageLensConfigurations
ListStorageLensGroups
ListTagsForResource
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Global
Naveen
Policy name
Enter a meaningful name to identify this policy.
police-2
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
Search
Allow (3 of 402 services)
Show remaining 399 services
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Global
Naveen
IAM > User groups > DevTeam > Add permissions
Attach permission policies to DevTeam
Current permissions policies (0)
Other permission policies (1/906)
You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.
Filter by Type
policy-1
All types
1 match
1
Policy name
Type
Used as
Description
policy-1
Customer managed
None
-
Cancel
Attach policies


aws
Services
Search
[Alt+S]
Global
Naveen
IAM > User groups > Opsteam > Add permissions
Attach permission policies to Opsteam
Current permissions policies (0)
Other permission policies (1/906)
You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.
Filter by Type
policy-2
All types
1 match
1
Policy name
Type
Used as
Description
policy-2
Customer managed
None
-
Cancel
Attach policies
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Global
Naveen
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
Policies attached to this user group.
IAM > User groups
User groups (2) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Search
1
Group name
Users
Permissions
Creation time
DevTeam
2
Defined
2 days ago
Opsteam
3
Defined
2 days ago
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Assignment – 3 IAM Roles

Problem Statement

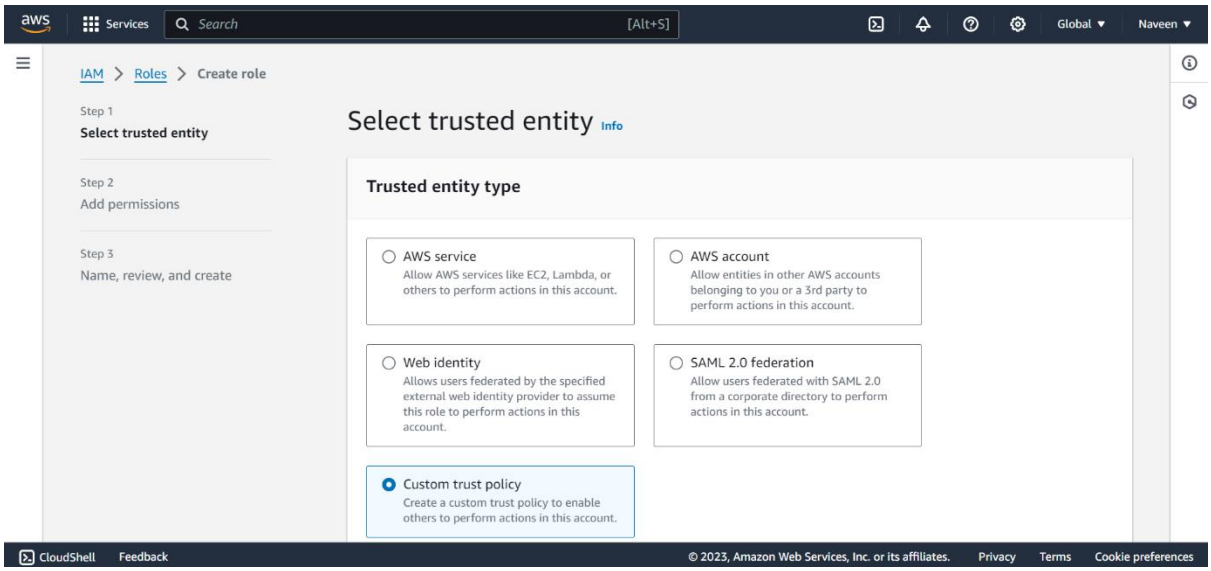
You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users.

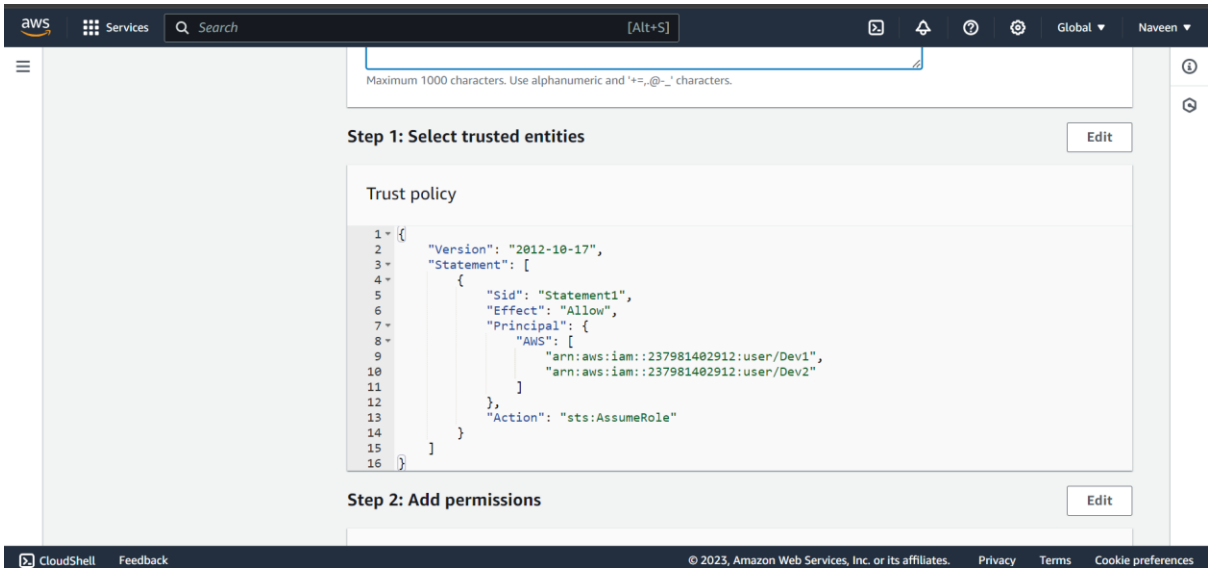
Task to be performed:

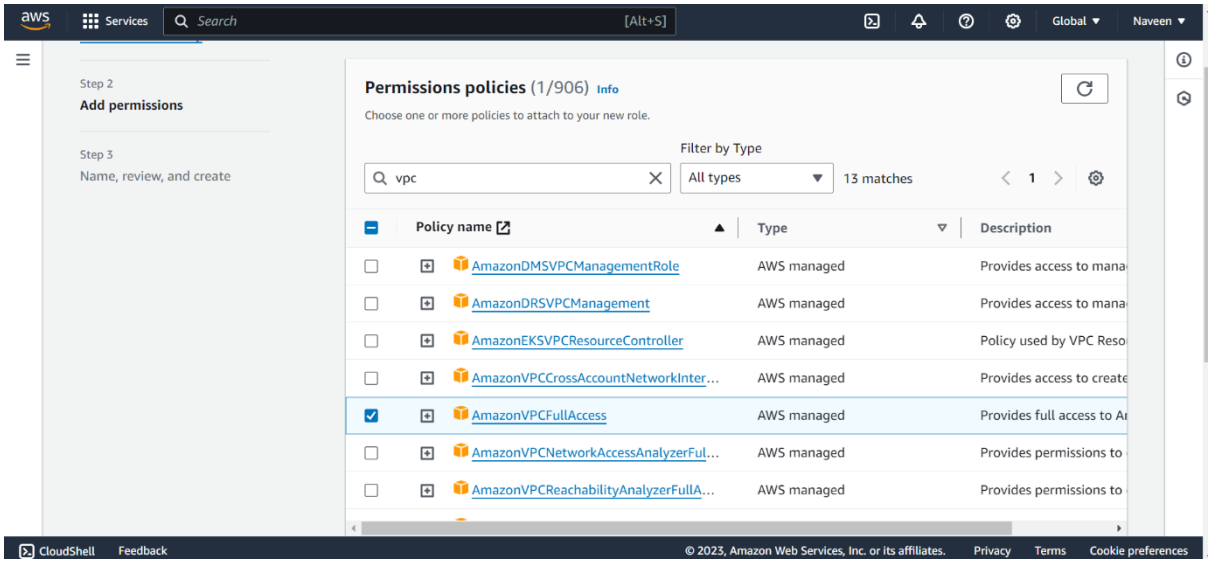
1. Create a role which only lets user 1 and user 2 from task 1 to have complete access to VPCs and DynamoDB.
2. Login into user 1 and shift to the role to test out the feature.

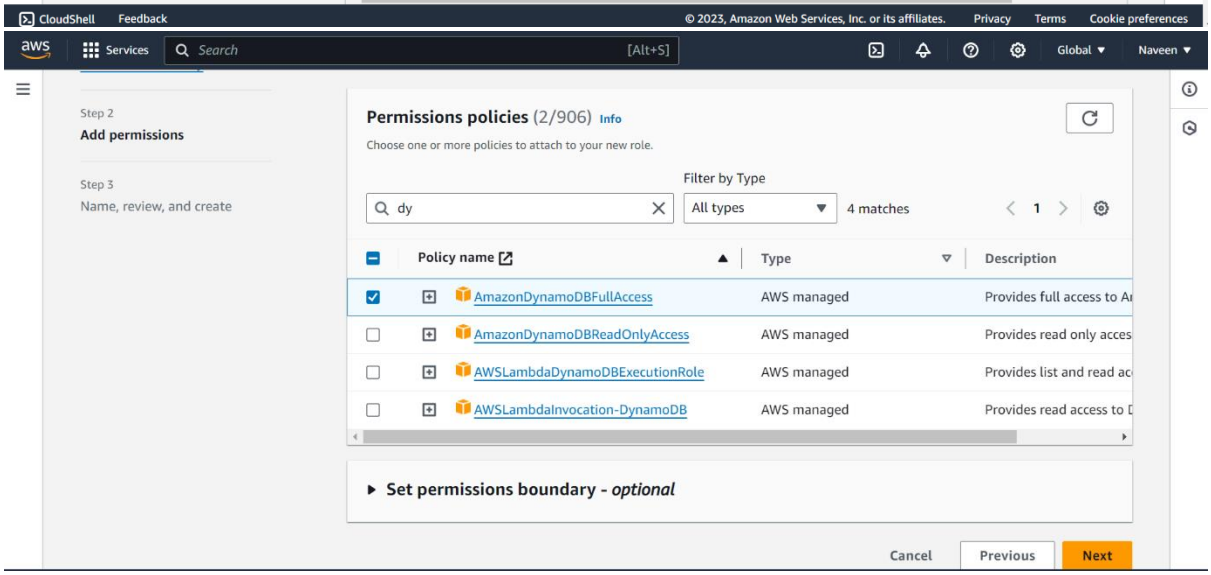
Steps

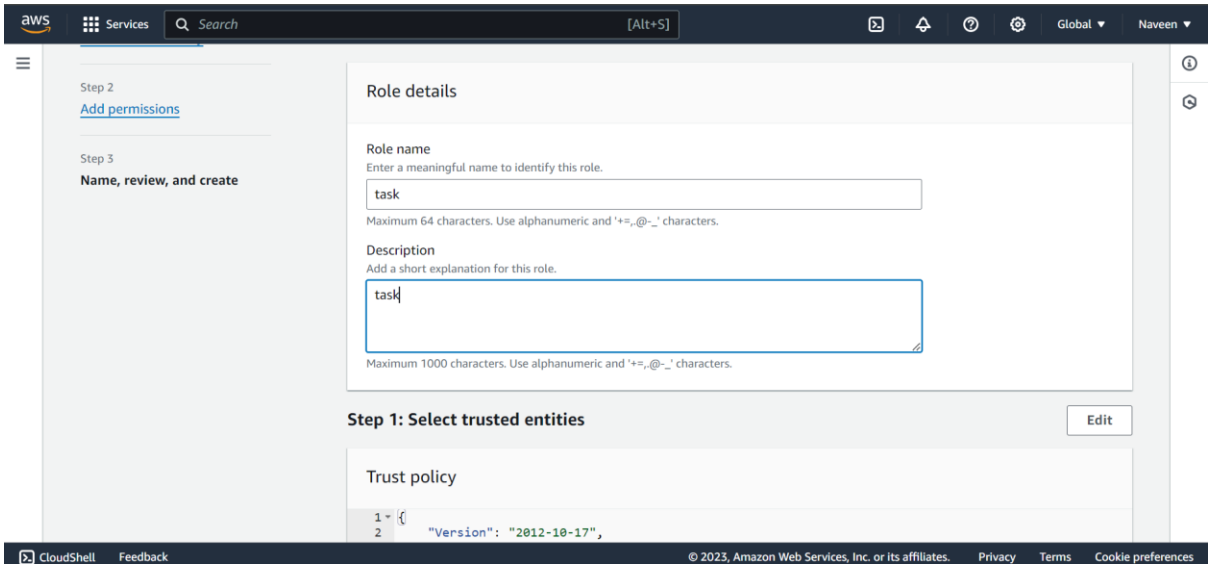
- Click the create role
- Select the custom trust policy in trusted entity type
- Provide ARN of the 2 users in custom trust policy
- Provide VPCs full access and DynamoDB full access
- Provide the role name
- Finally the role is created
- Sign is as IAM user 1 and click the switch role
- Finally the role page is reflected

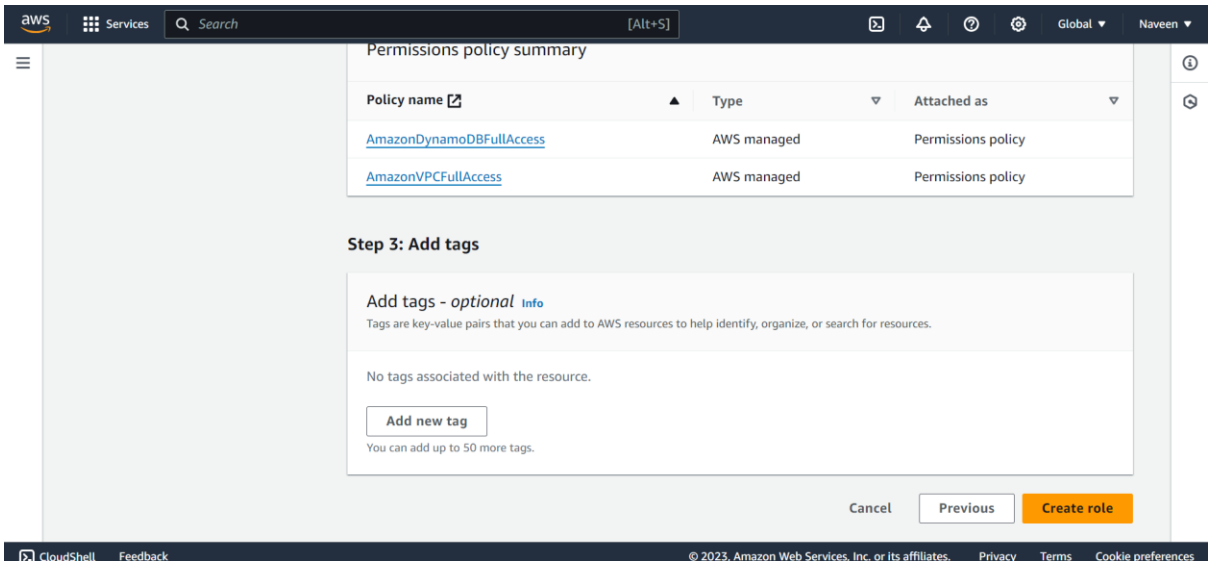


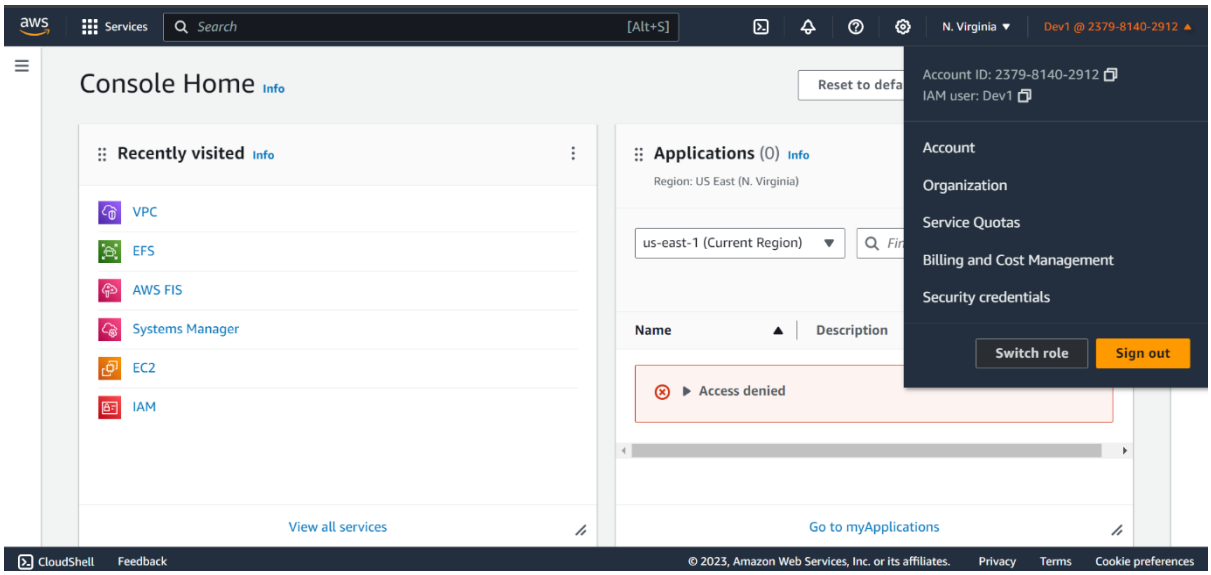

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Step 1: Select trusted entities
Edit
Trust policy
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Statement1",
"Effect": "Allow",
"Principal": {
"AWS": [
"arn:aws:iam::237981402912:user/Dev1",
"arn:aws:iam::237981402912:user/Dev2"
]
},
"Action": "sts:AssumeRole"
}
]
}
Step 2: Add permissions
Edit

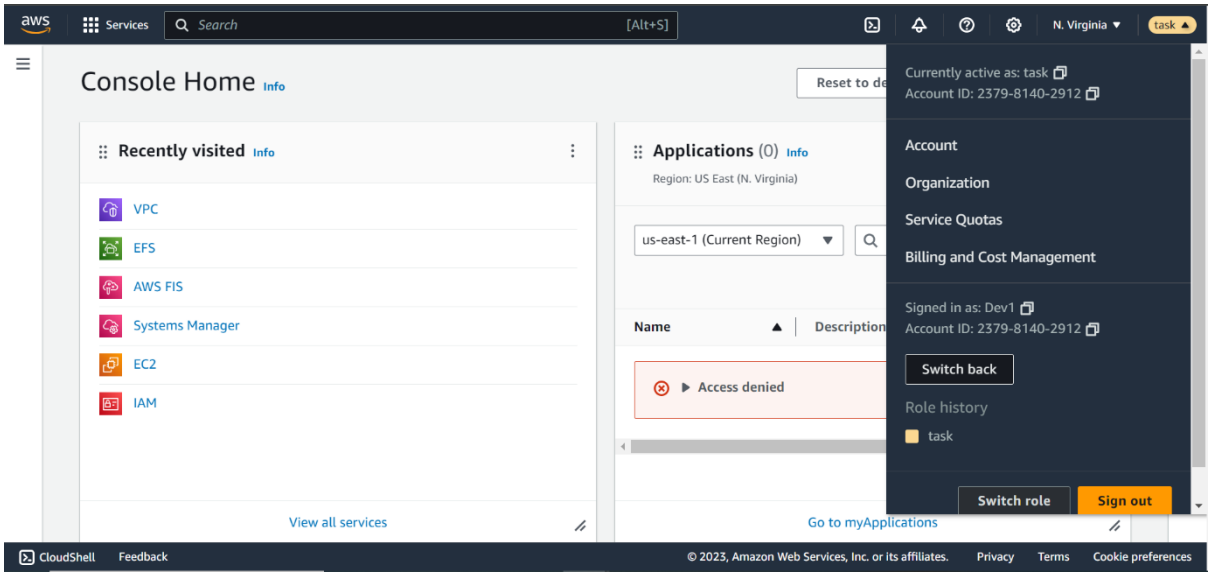

Step 2
Add permissions
Step 3
Name, review, and create
Permissions policies (1/906) Info
Choose one or more policies to attach to your new role.
Filter by Type
vpc
All types
13 matches
Policy name
Type
Description
AmazonDMSVPCManagementRole
AWS managed
Provides access to mana
AmazonDRSVPCManagement
AWS managed
Provides access to mana
AmazonEKSVPCResourceController
AWS managed
Policy used by VPC Reso
AmazonVPCCrossAccountNetworkInter...
AWS managed
Provides access to create
AmazonVPCFullAccess
AWS managed
Provides full access to A
AmazonVPCNetworkAccessAnalyzerFul...
AWS managed
Provides permissions to
AmazonVPCReachabilityAnalyzerFullA...
AWS managed
Provides permissions to

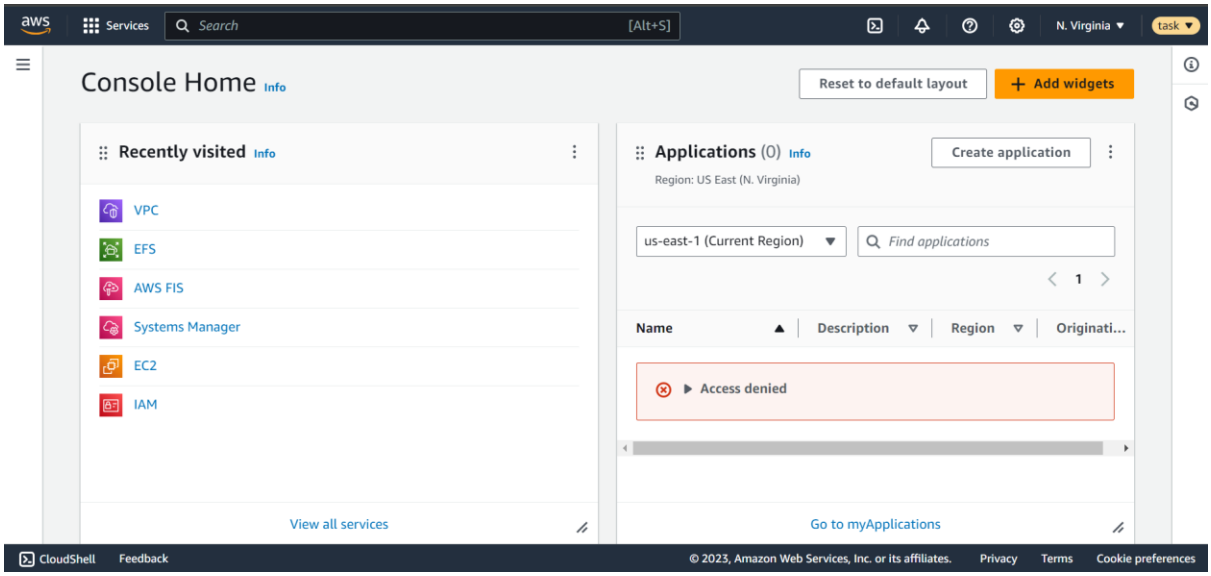

Step 2
Add permissions
Step 3
Name, review, and create
Permissions policies (2/906) Info
Choose one or more policies to attach to your new role.
Filter by Type
dy
All types
4 matches
Policy name
Type
Description
AmazonDynamoDBFullAccess
AWS managed
Provides full access to A
AmazonDynamoDBReadOnlyAccess
AWS managed
Provides read only acces
AWSLambdaDynamoDBExecutionRole
AWS managed
Provides list and read ac
AWSLambdaInvocation-DynamoDB
AWS managed
Provides read access to D
Set permissions boundary - optional
Cancel
Previous
Next


Services
Search
[Alt+S]
Global
Naveen
Step 2
Add permissions
Step 3
Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
task
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
task
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Step 1: Select trusted entities
Edit
Trust policy
{
"Version": "2012-10-17",
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
Global
Naveen
Permissions policy summary
Policy name
Type
Attached as
AmazonDynamoDBFullAccess
AWS managed
Permissions policy
AmazonVPCFullAccess
AWS managed
Permissions policy
Step 3: Add tags
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 role
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
N. Virginia
Dev1 @ 2379-8140-2912
Console Home Info
Reset to defa
Account ID: 2379-8140-2912
IAM user: Dev1
Account
Organization
Service Quotas
Billing and Cost Management
Security credentials
Switch role
Sign out
Recently visited Info
VPC
EFS
AWS FIS
Systems Manager
EC2
IAM
View all services
Applications (0) Info
Region: US East (N. Virginia)
us-east-1 (Current Region)
Name
Description
Access denied
Go to myApplications
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
task
Console Home Info
Reset to de
Recently visited Info
VPC
EFS
AWS FIS
Systems Manager
EC2
IAM
View all services
Applications (0) Info
Region: US East (N. Virginia)
us-east-1 (Current Region)
Name
Description
Access denied
Go to myApplications
Currently active as: task
Account ID: 2379-8140-2912
Account
Organization
Service Quotas
Billing and Cost Management
Signed in as: Dev1
Account ID: 2379-8140-2912
Switch back
Role history
task
Switch role
Sign out
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
task
Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
VPC
EFS
AWS FIS
Systems Manager
EC2
IAM
View all services
Applications (0) Info
Region: US East (N. Virginia)
Create application
us-east-1 (Current Region)
Find applications
1
Name
Description
Region
Originati...
Access denied
Go to myApplications
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Assignment – 4 CloudWatch

Problem Statement

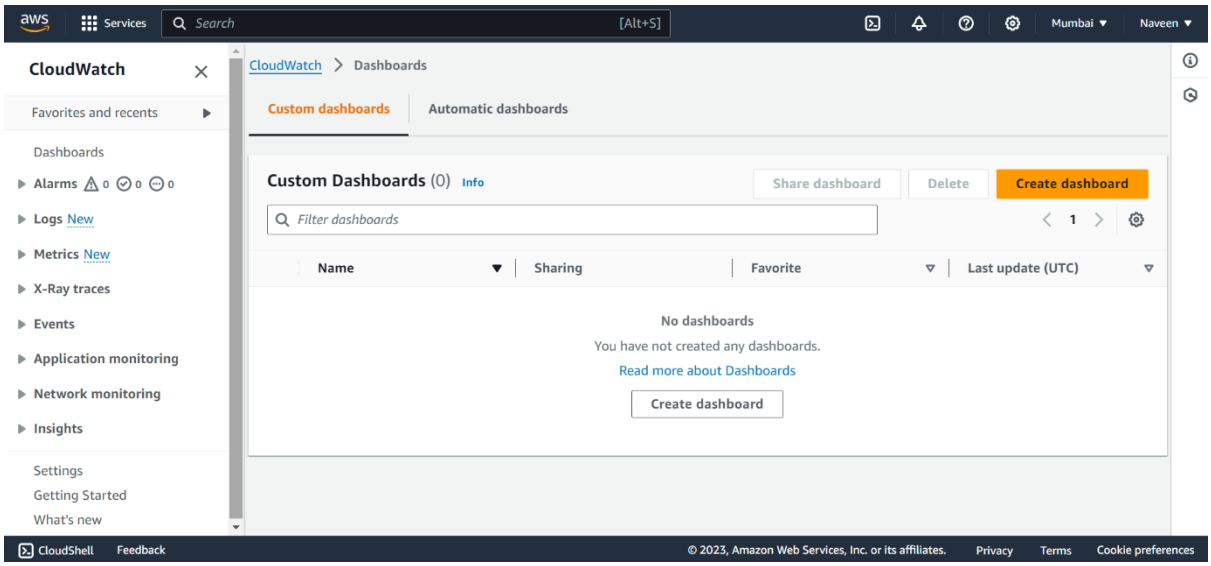
You work for XYZ Corporation. To maintain the security of the AWS account and the resources you been asked to implement a solution that can help easily recognize and monitor the different users. Also, you will be monitoring the machines created by these users for any errors or misconfigurations.

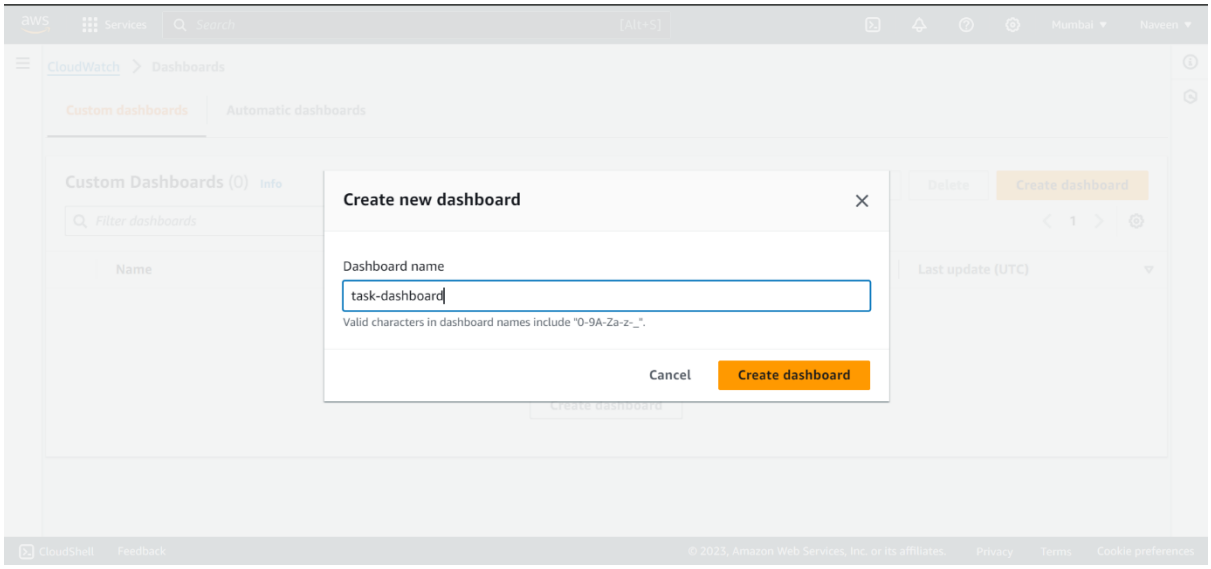
Tasks to be performed

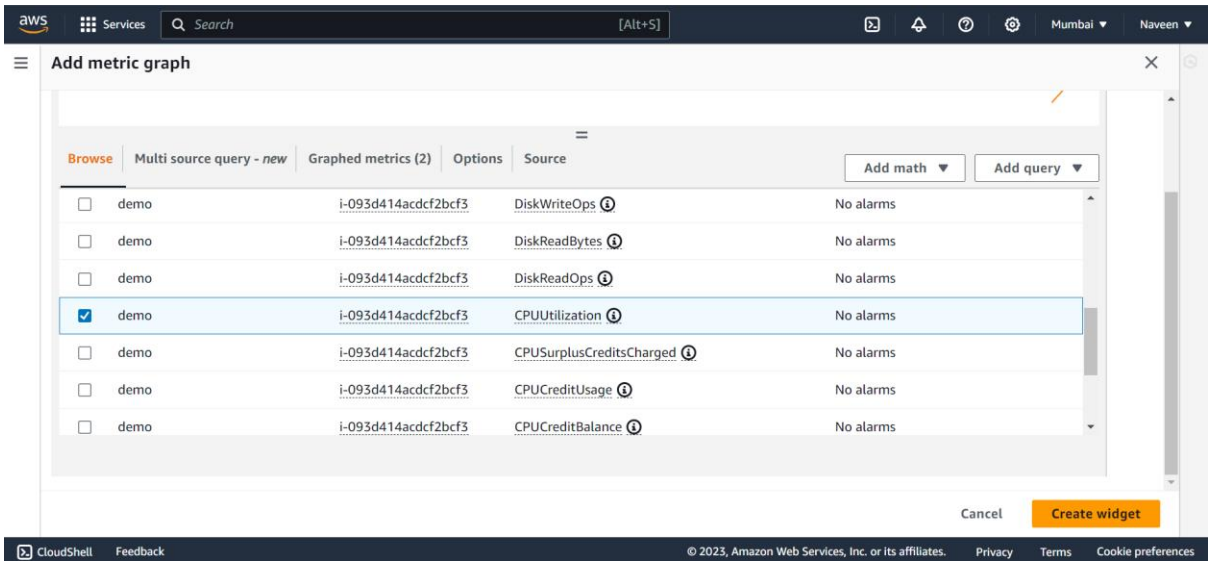
1. Created a dashboard which lets you check the CPU utilization and networking for a particular EC2 instance.

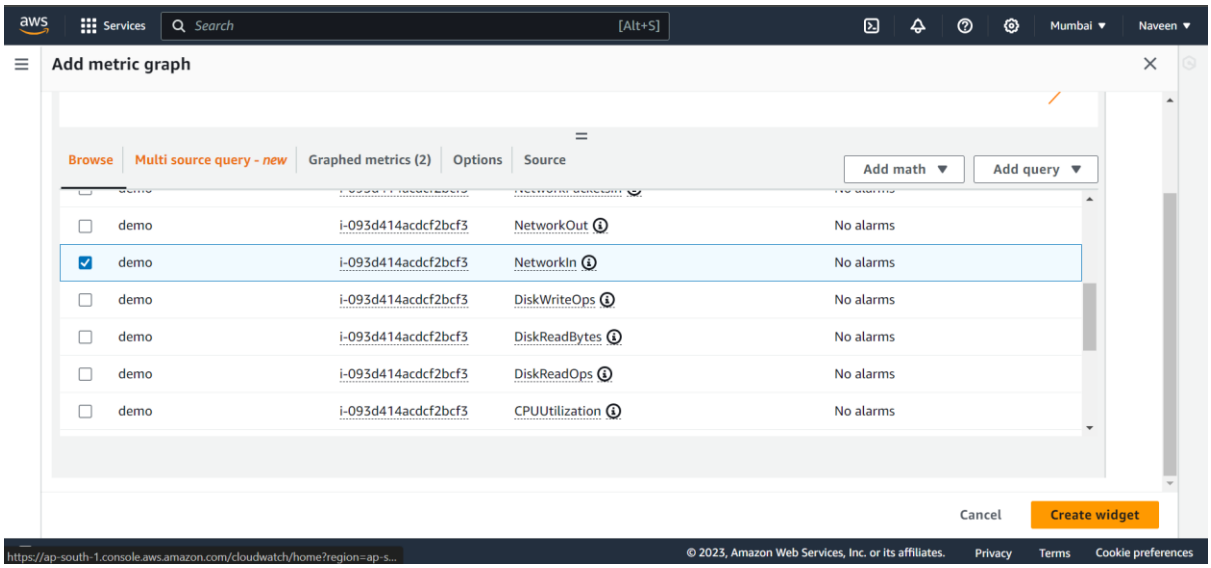
Steps

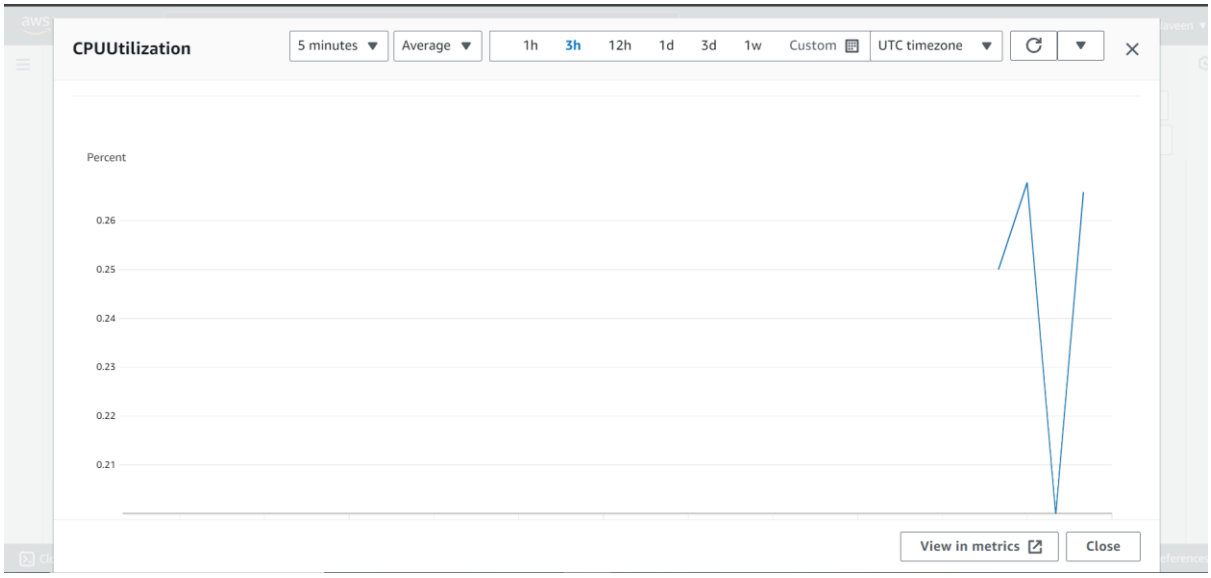
- Click the create dashboard
- Provide a dashboard name
- click the add widget and select a widget type
- select the CPU utilization for a particular EC2 instance
- select the Networking for a particular EC2 instance
- finally the dashboard is created

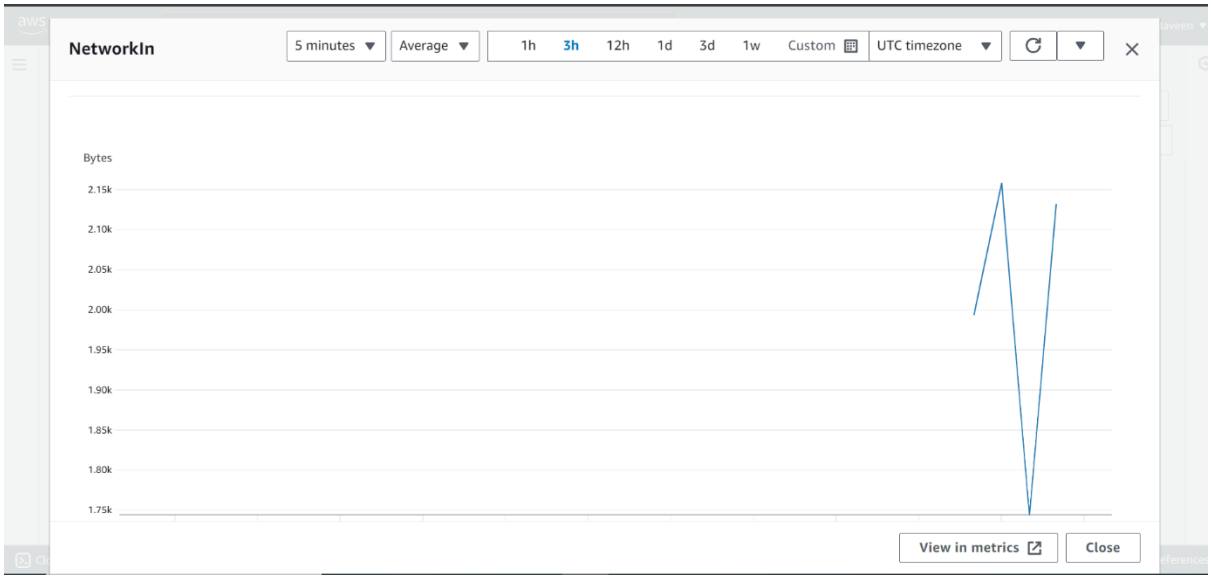


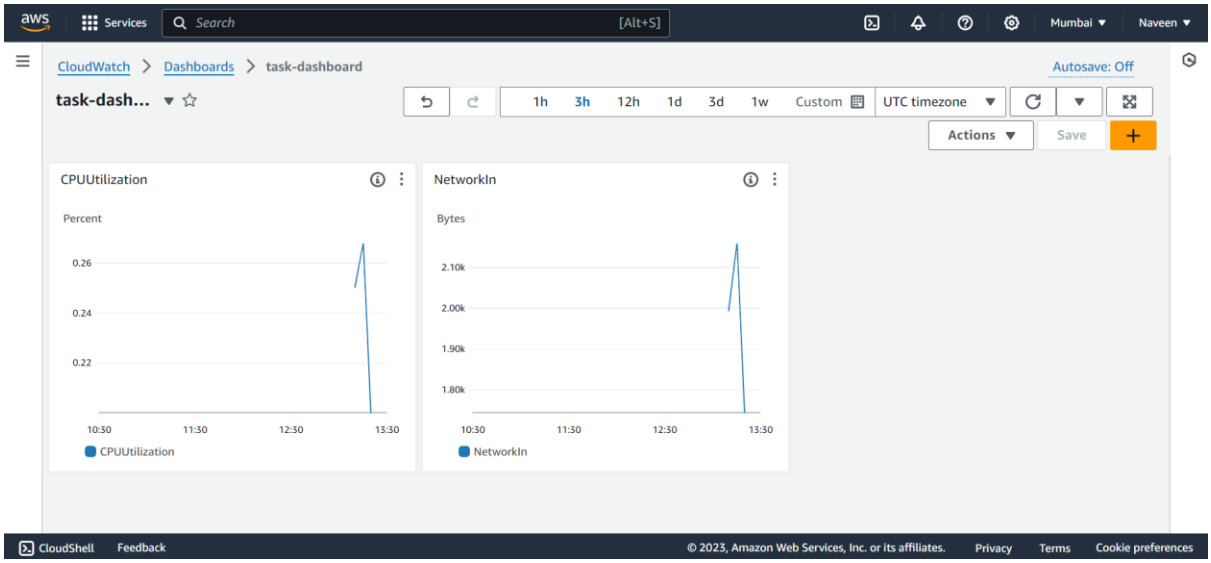

Create new dashboard
Dashboard name
task-dashboard
Valid characters in dashboard names include "0-9A-Za-z-_".
Cancel
Create dashboard

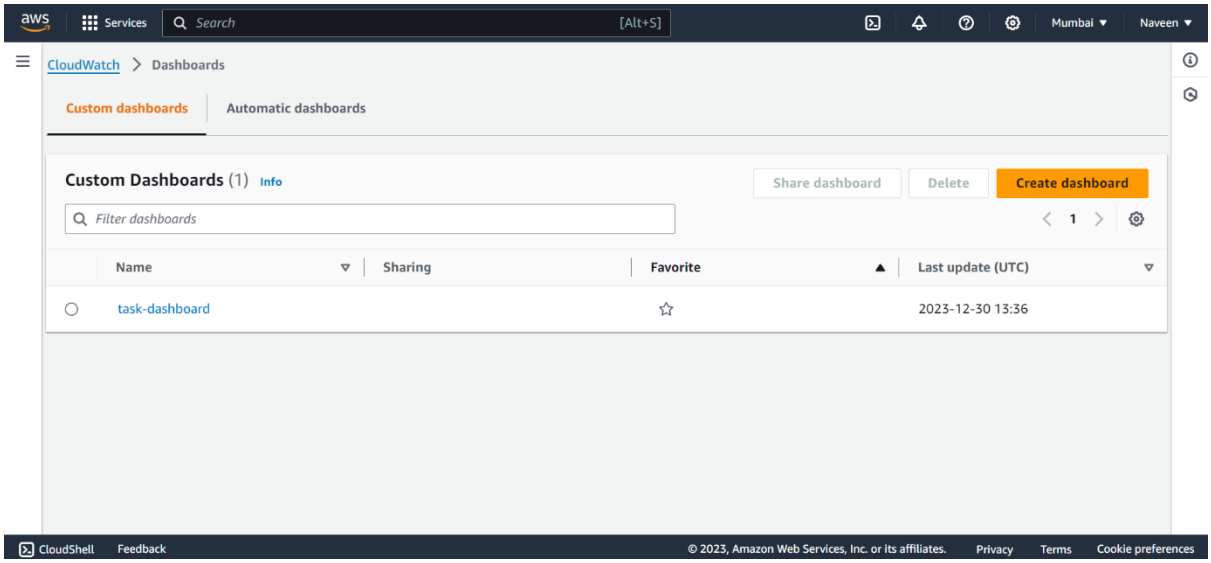

Add metric graph
Browse
Multi source query - new
Graphed metrics (2)
Options
Source
Add math
Add query
demo i-093d414acdcf2bcf3 DiskWriteOps No alarms
demo i-093d414acdcf2bcf3 DiskReadBytes No alarms
demo i-093d414acdcf2bcf3 DiskReadOps No alarms
demo i-093d414acdcf2bcf3 CPUUtilization No alarms
demo i-093d414acdcf2bcf3 CPUSurplusCreditsCharged No alarms
demo i-093d414acdcf2bcf3 CPUCreditUsage No alarms
demo i-093d414acdcf2bcf3 CPUCreditBalance No alarms
Cancel
Create widget


Add metric graph
Browse
Multi source query - new
Graphed metrics (2)
Options
Source
Add math
Add query
demo i-093d414acdcf2bcf3 NetworkOut No alarms
demo i-093d414acdcf2bcf3 NetworkIn No alarms
demo i-093d414acdcf2bcf3 DiskWriteOps No alarms
demo i-093d414acdcf2bcf3 DiskReadBytes No alarms
demo i-093d414acdcf2bcf3 DiskReadOps No alarms
demo i-093d414acdcf2bcf3 CPUUtilization No alarms
Cancel
Create widget


CPUUtilization
5 minutes
Average
1h
3h
12h
1d
3d
1w
Custom
UTC timezone
Percent
0.26
0.25
0.24
0.23
0.22
0.21
View in metrics
Close


NetworkIn
5 minutes
Average
1h
3h
12h
1d
3d
1w
Custom
UTC timezone
Bytes
2.15k
2.10k
2.05k
2.00k
1.95k
1.90k
1.85k
1.80k
1.75k
View in metrics
Close


Services
Search
[Alt+S]
Mumbai
Naveen
CloudWatch
Dashboards
task-dashboard
Autosave: Off
task-dash...
1h
3h
12h
1d
3d
1w
Custom
UTC timezone
Actions
Save
CPUUtilization
Percent
0.26
0.24
0.22
10:30
11:30
12:30
13:30
CPUUtilization
NetworkIn
Bytes
2.10k
2.00k
1.90k
1.80k
10:30
11:30
12:30
13:30
NetworkIn
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Mumbai
Naveen
CloudWatch
Dashboards
Custom dashboards
Automatic dashboards
Custom Dashboards (1) Info
Share dashboard
Delete
Create dashboard
Filter dashboards
1
Name
Sharing
Favorite
Last update (UTC)
task-dashboard
2023-12-30 13:36
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Assignment – 5 CloudWatch Alarms

Problem Statement

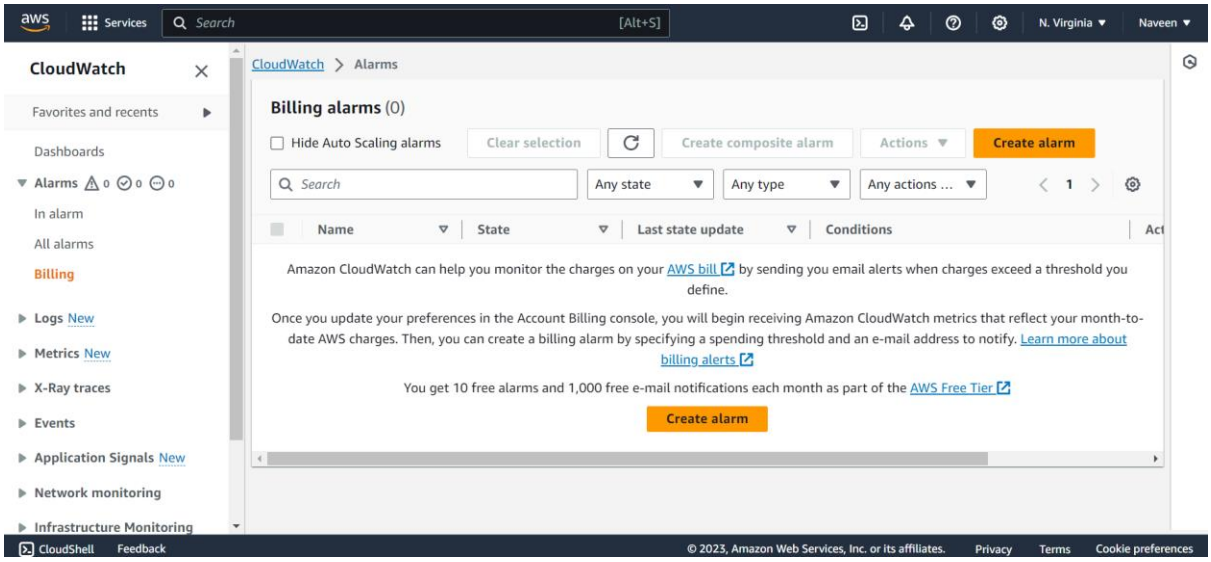
You work for XYZ Corporation. To maintain the security of the AWS account and the resources you been asked to implement a solution that can help easily recognize and monitor the different users. Also, you will be monitoring the machines created by these users for any errors or misconfigurations.

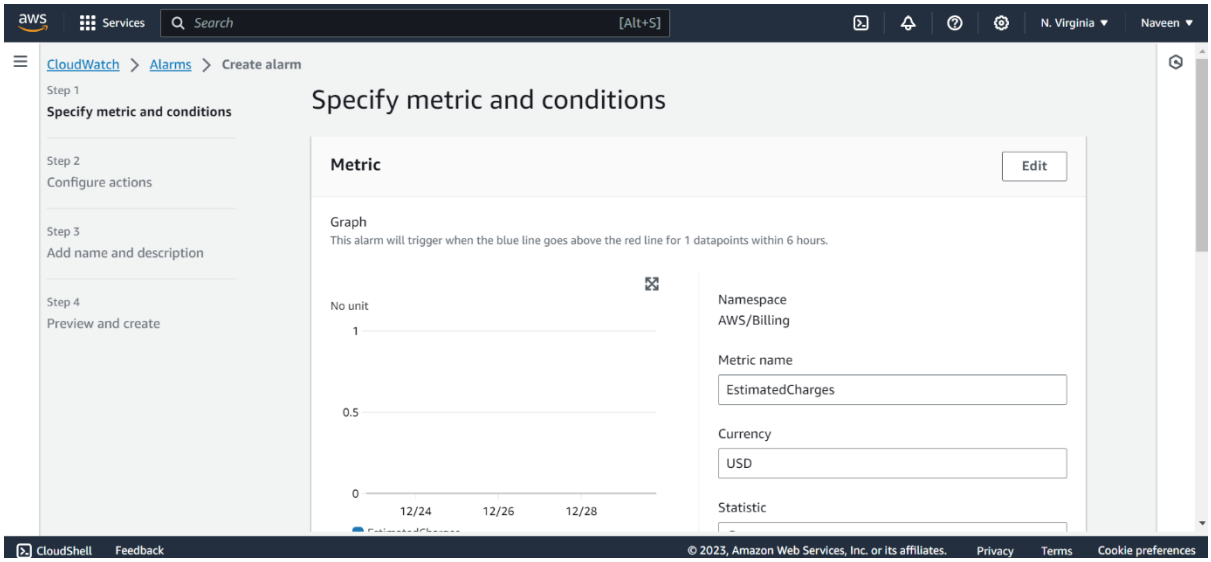
Tasks to be performed

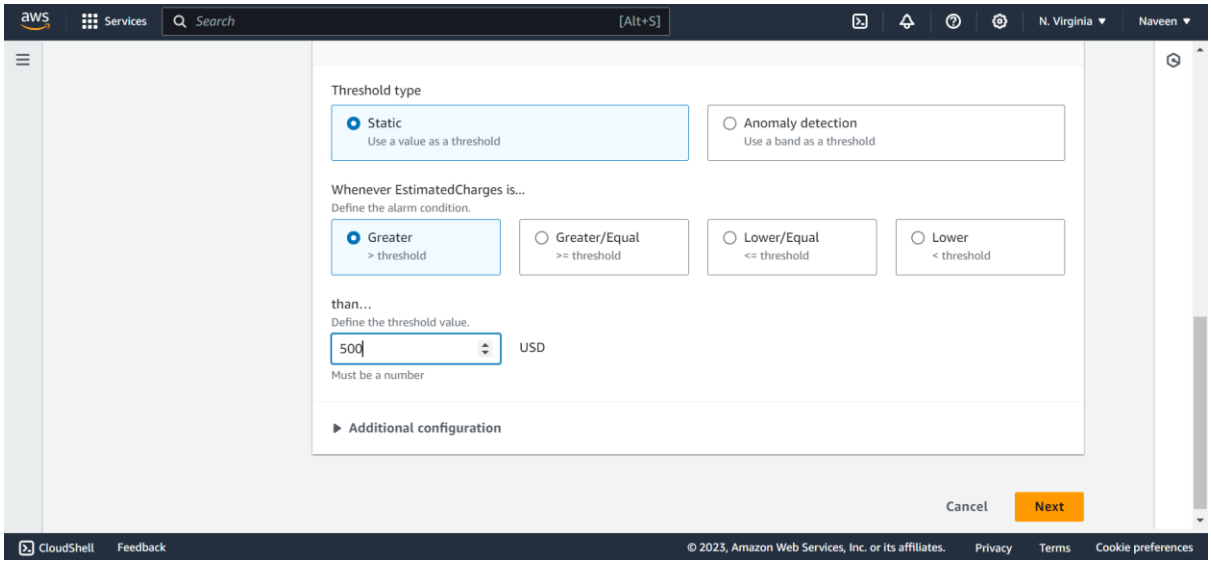
1. Create a cloudwatch billing alarm which goes off when the estimated charges go above $500.
2. Create a cloudwatch alarm which goes off to an alarm state when the CPU utilization of an EC2 instance goes above 65%. Also add an SNS topic so that it notifies the person when the threshold is crossed.

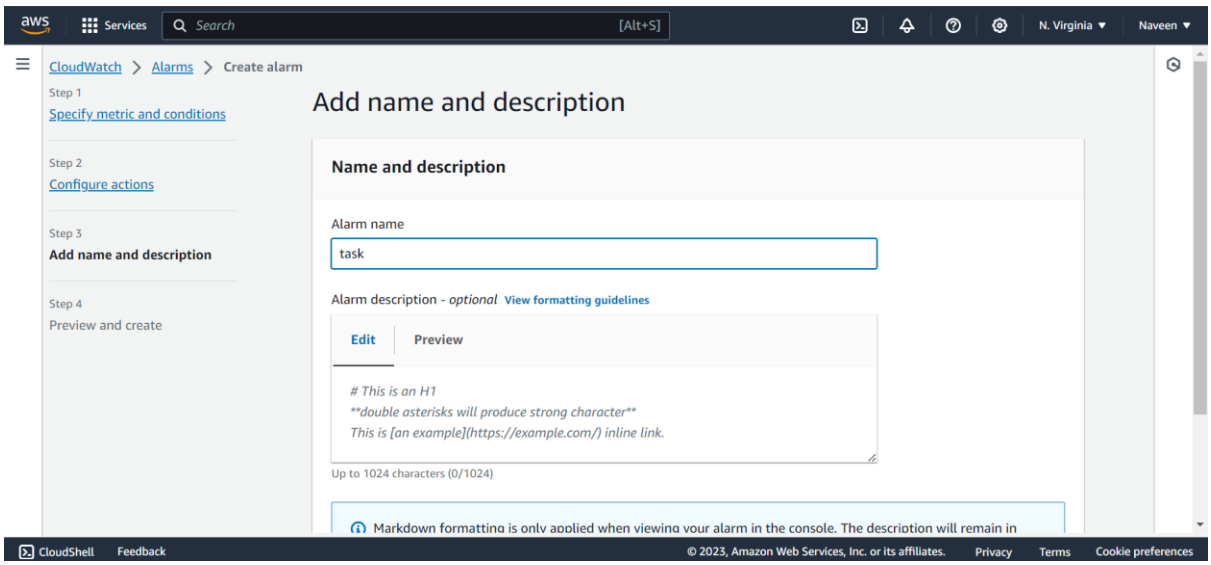
Steps

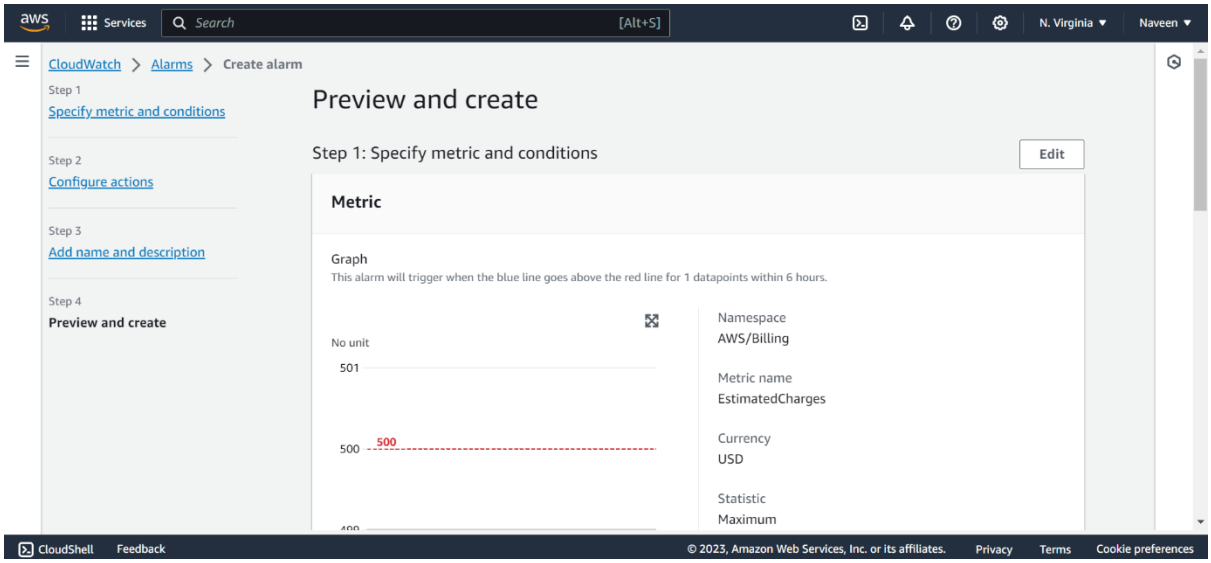
- Click the billing
- Click the create alarm
- Select as Greater and provide the threshold value as 500 USD
- Provide an alarm name
- Finally the alarm is created

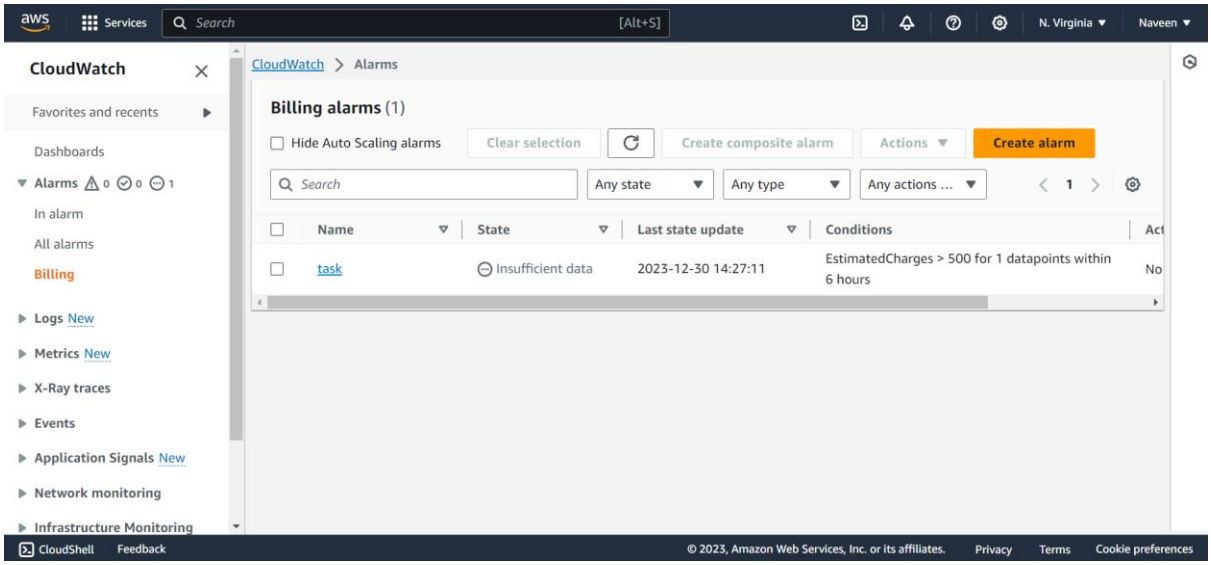


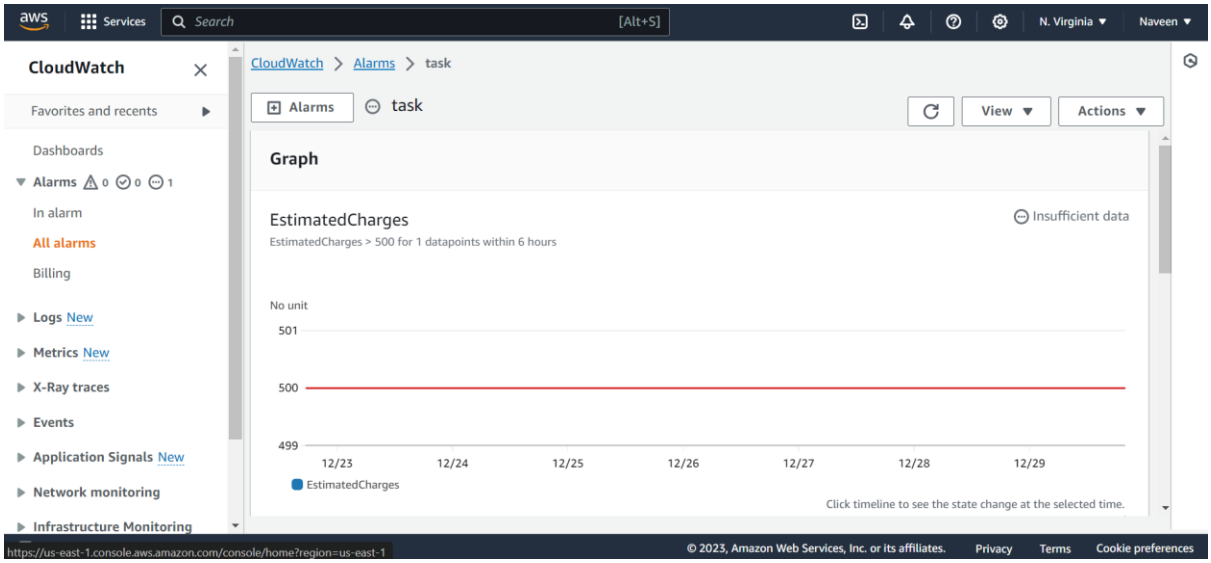

aws
Services
Search
[Alt+S]
N. Virginia
Naveen
CloudWatch > Alarms > Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add name and description
Step 4
Preview and create
Specify metric and conditions
Metric
Edit
Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 6 hours.
No unit
1
0.5
0
12/24
12/26
12/28
Namespace
AWS/Billing
Metric name
EstimatedCharges
Currency
USD
Statistic
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

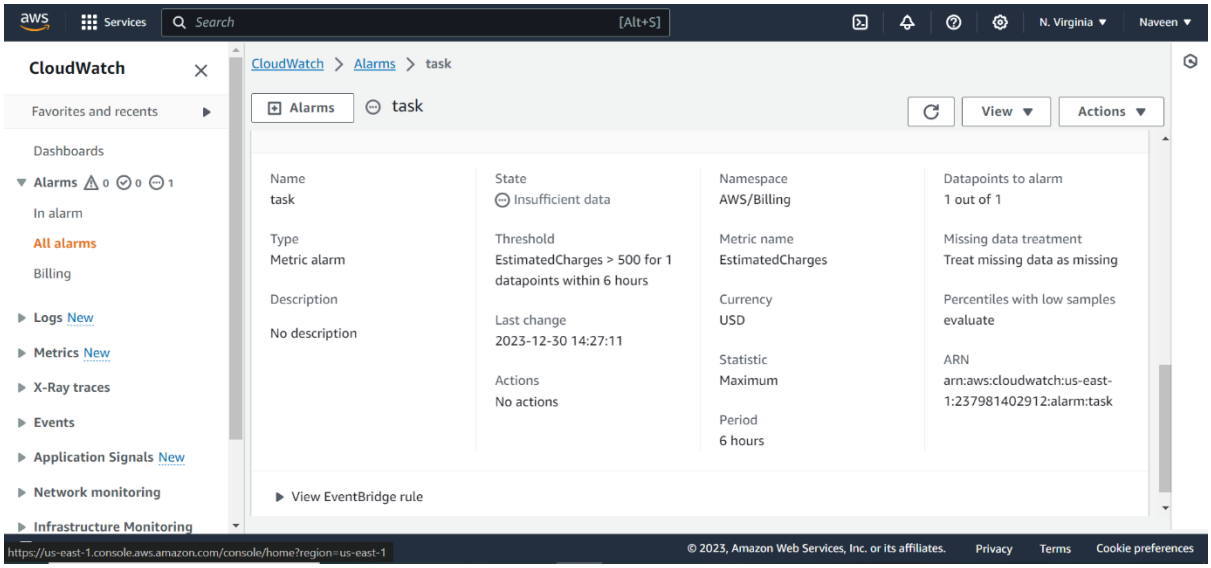

aws
Services
Search
[Alt+S]
N. Virginia
Naveen
Threshold type
Static
Use a value as a threshold
Anomaly detection
Use a band as a threshold
Whenever EstimatedCharges is...
Define the alarm condition.
Greater
> threshold
Greater/Equal
>= threshold
Lower/Equal
<= threshold
Lower
< threshold
than...
Define the threshold value.
500
USD
Must be a number
Additional configuration
Cancel
Next
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
Naveen
CloudWatch > Alarms > Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add name and description
Step 4
Preview and create
Add name and description
Name and description
Alarm name
task
Alarm description - optional
View formatting guidelines
Edit
Preview
This is an H1
double asterisks will produce strong character
This is [an example](https://example.com/) inline link.
Up to 1024 characters (0/1024)
Markdown formatting is only applied when viewing your alarm in the console. The description will remain in
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
Naveen
CloudWatch > Alarms > Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add name and description
Step 4
Preview and create
Preview and create
Step 1: Specify metric and conditions
Edit
Metric
Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 6 hours.
No unit
501
500
500
Namespace
AWS/Billing
Metric name
EstimatedCharges
Currency
USD
Statistic
Maximum
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
Naveen
CloudWatch
Favorites and recents
Dashboards
Alarms 0 0 1
In alarm
All alarms
Billing
Logs New
Metrics New
X-Ray traces
Events
Application Signals New
Network monitoring
Infrastructure Monitoring
CloudWatch > Alarms
Billing alarms (1)
Hide Auto Scaling alarms
Clear selection
Create composite alarm
Actions
Create alarm
Search
Any state
Any type
Any actions ...
1
Name
State
Last state update
Conditions
task
Insufficient data
2023-12-30 14:27:11
EstimatedCharges > 500 for 1 datapoints within 6 hours
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

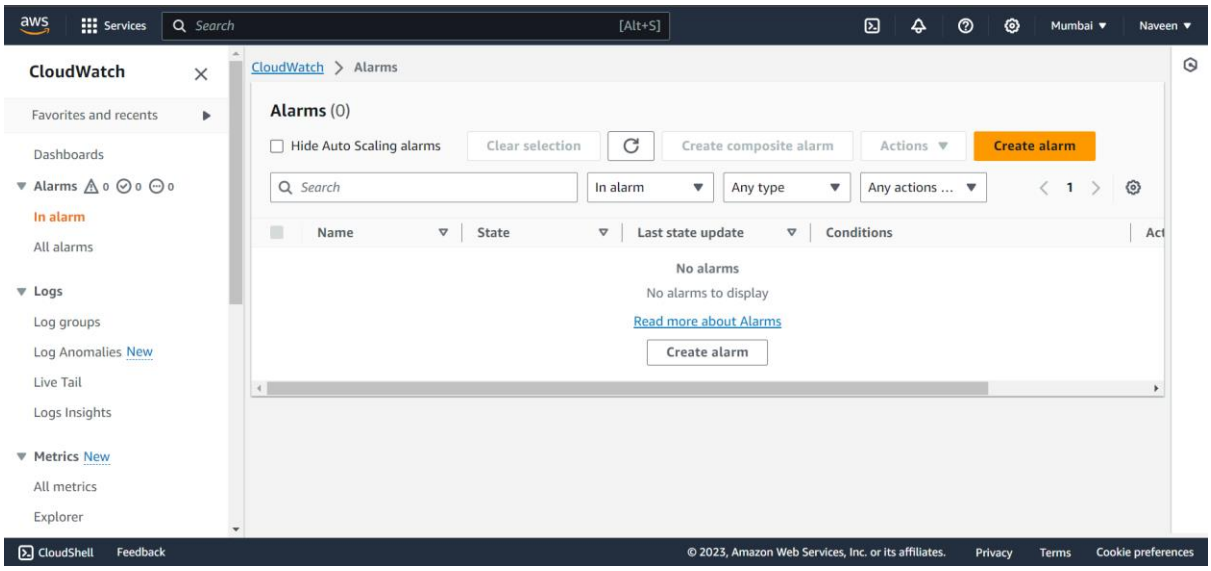

aws
Services
Search
[Alt+S]
N. Virginia
Naveen
CloudWatch
Favorites and recents
Dashboards
Alarms 0 0 1
In alarm
All alarms
Billing
Logs New
Metrics New
X-Ray traces
Events
Application Signals New
Network monitoring
Infrastructure Monitoring
CloudWatch > Alarms > task
Alarms
task
View
Actions
Graph
EstimatedCharges
EstimatedCharges > 500 for 1 datapoints within 6 hours
Insufficient data
No unit
501
500
499
12/23
12/24
12/25
12/26
12/27
12/28
12/29
EstimatedCharges
Click timeline to see the state change at the selected time.
https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

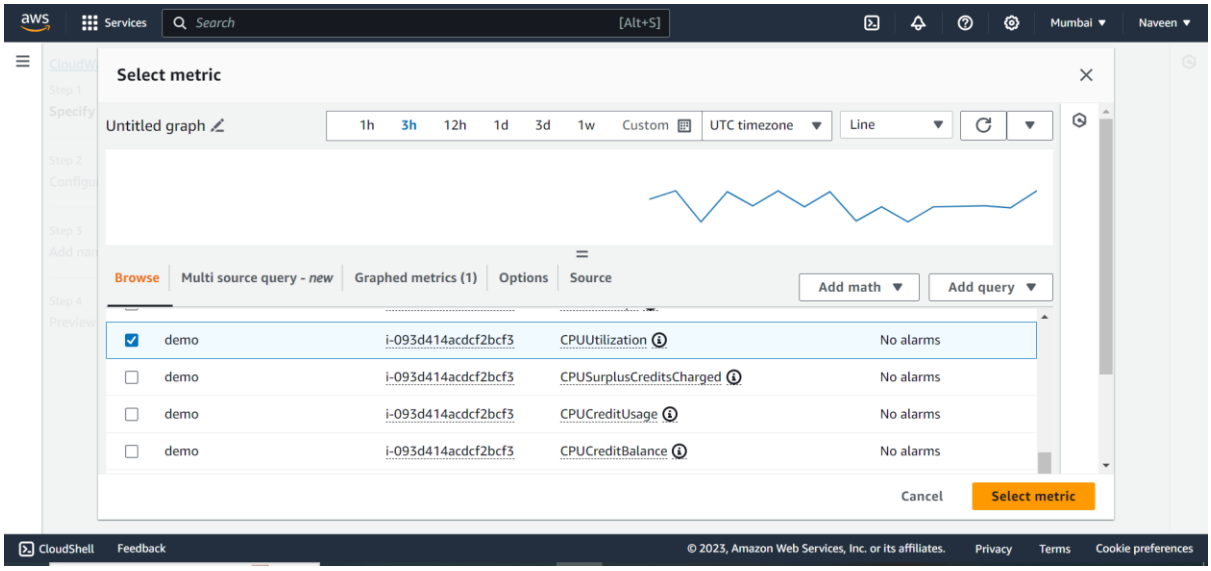

aws
Services
Search
[Alt+S]
N. Virginia
Naveen
CloudWatch
Favorites and recents
Dashboards
Alarms 0 0 1
In alarm
All alarms
Billing
Logs New
Metrics New
X-Ray traces
Events
Application Signals New
Network monitoring
Infrastructure Monitoring
CloudWatch > Alarms > task
Alarms
task
View
Actions
Name
task
State
Insufficient data
Namespace
AWS/Billing
Datapoints to alarm
1 out of 1
Type
Metric alarm
Threshold
EstimatedCharges > 500 for 1 datapoints within 6 hours
Metric name
EstimatedCharges
Missing data treatment
Treat missing data as missing
Description
No description
Last change
2023-12-30 14:27:11
Currency
USD
Percentiles with low samples
evaluate
Actions
No actions
Statistic
Maximum
ARN
arn:aws:cloudwatch:us-east-1:237981402912:alarm:task
Period
6 hours
View EventBridge rule
https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

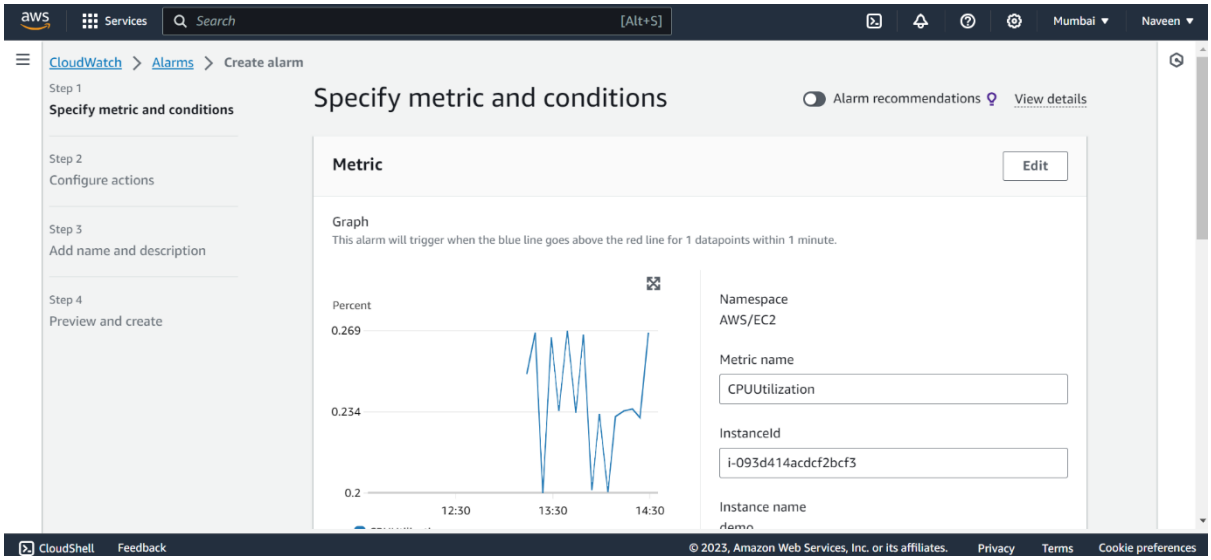
Create a cloudwatch alarm which goes off to an alarm state when the CPU utilization of an EC2 instance goes above 65%. Also add an SNS topic so that it notifies the person when the threshold is crossed.

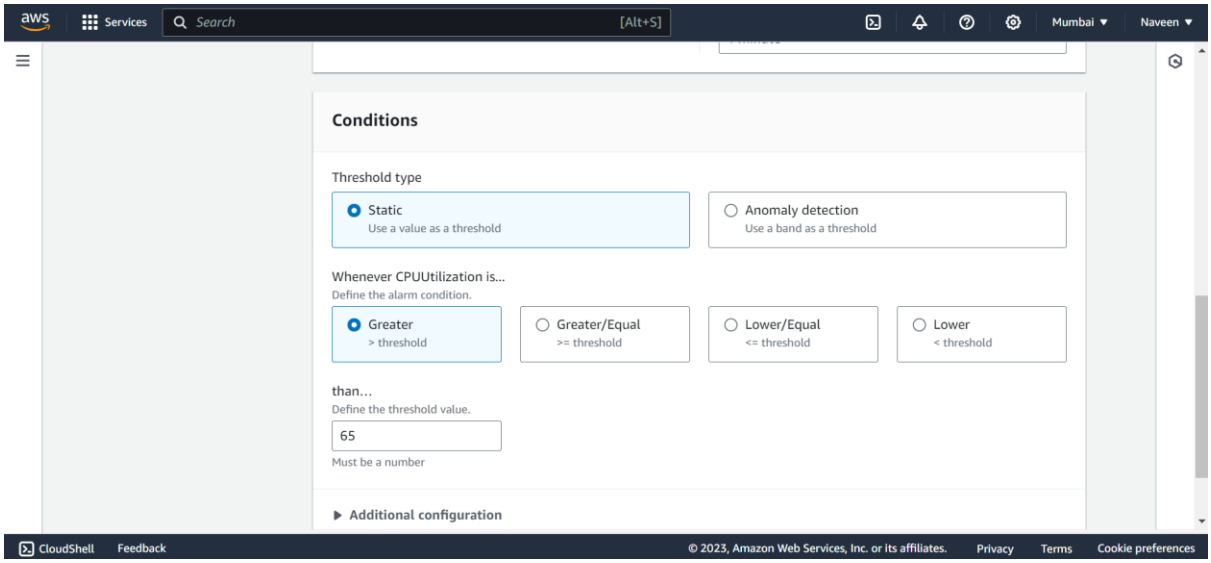
Steps

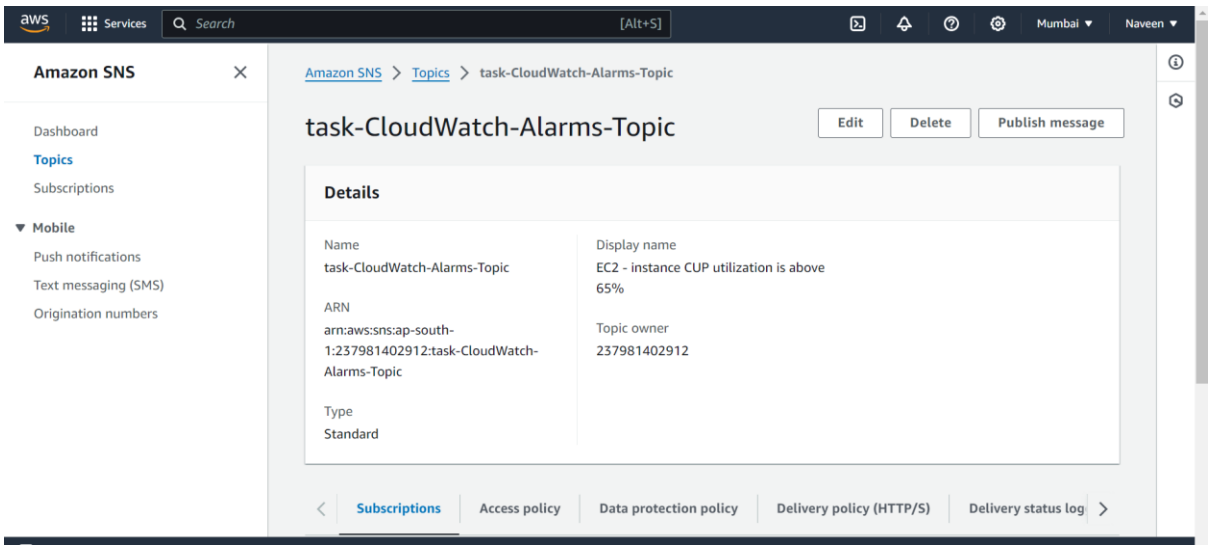
- Click the create alarm
- Select the metric as CPU utilization
- Select as Greater and provide the threshold value as 65%
- Create a new topic in SNS
- Select the topic which was created in send a notification
- Provide an alarm name
- Finally alarm is created

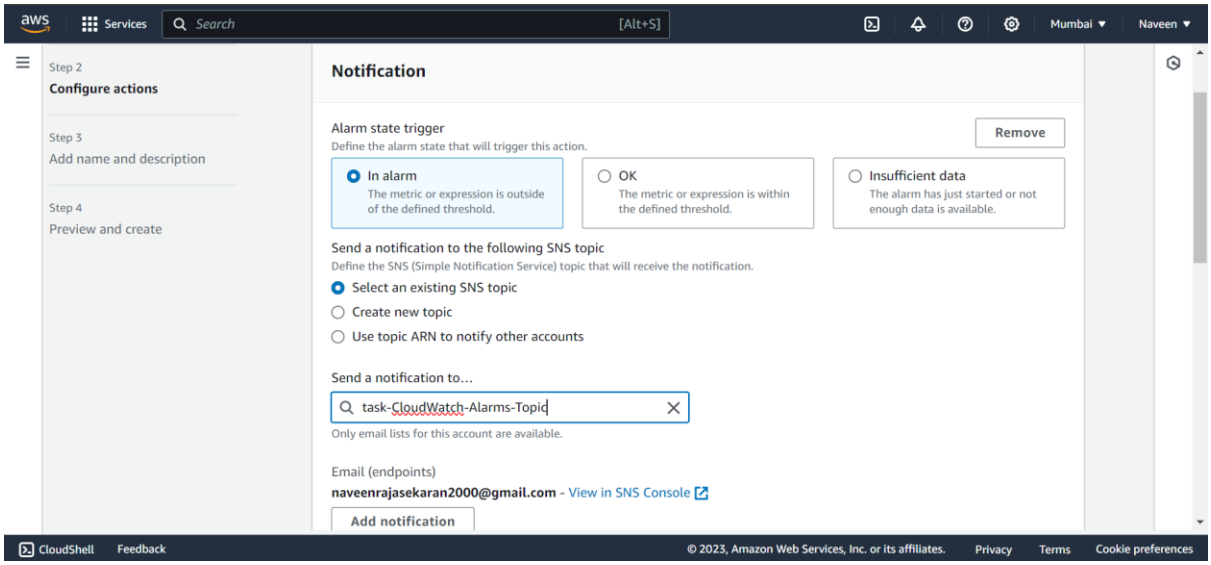


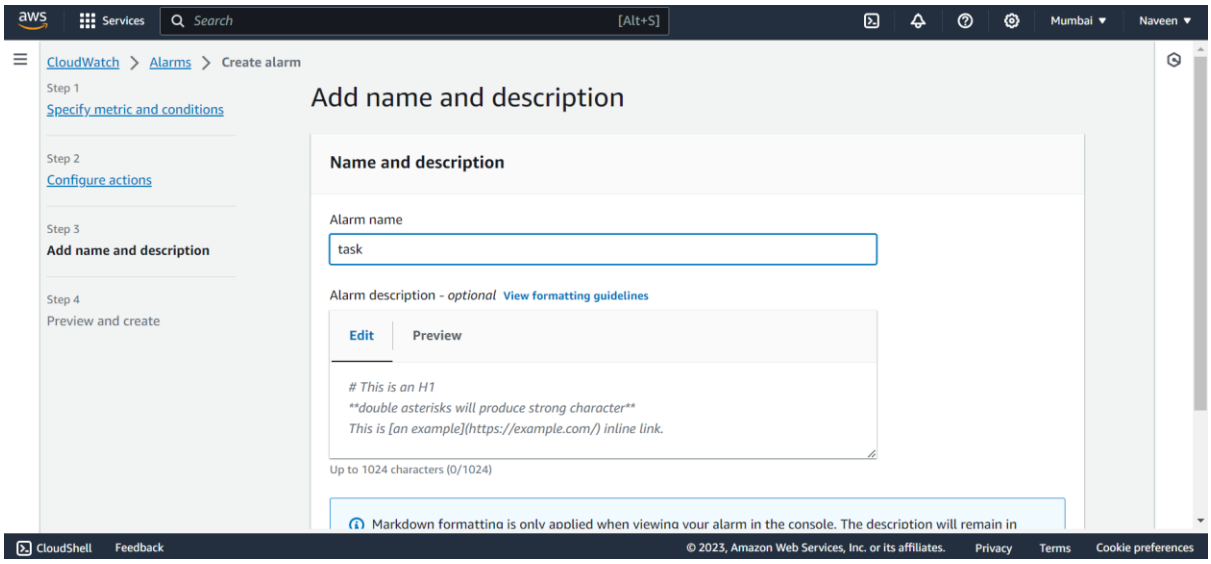


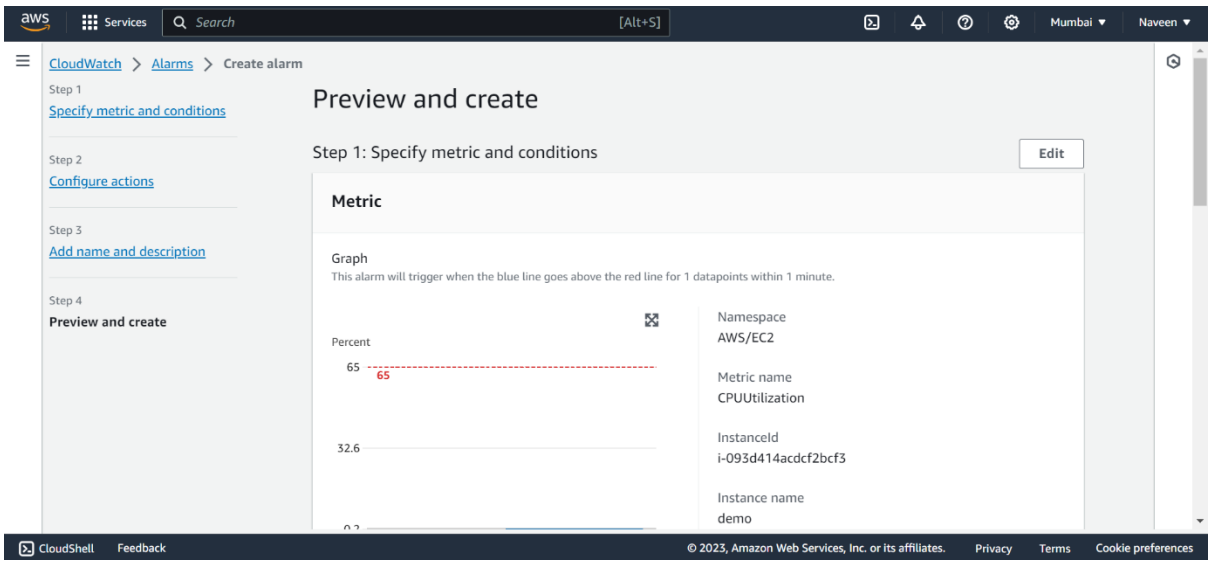

aws
Services
Search
[Alt+S]
Mumbai
Naveen
CloudWatch > Alarms > Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add name and description
Step 4
Preview and create
Specify metric and conditions
Alarm recommendations
View details
Metric
Edit
Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 minute.
Percent
0.269
0.234
0.2
12:30
13:30
14:30
Namespace
AWS/EC2
Metric name
CPUUtilization
InstanceId
i-093d414acdcf2bcf3
Instance name
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

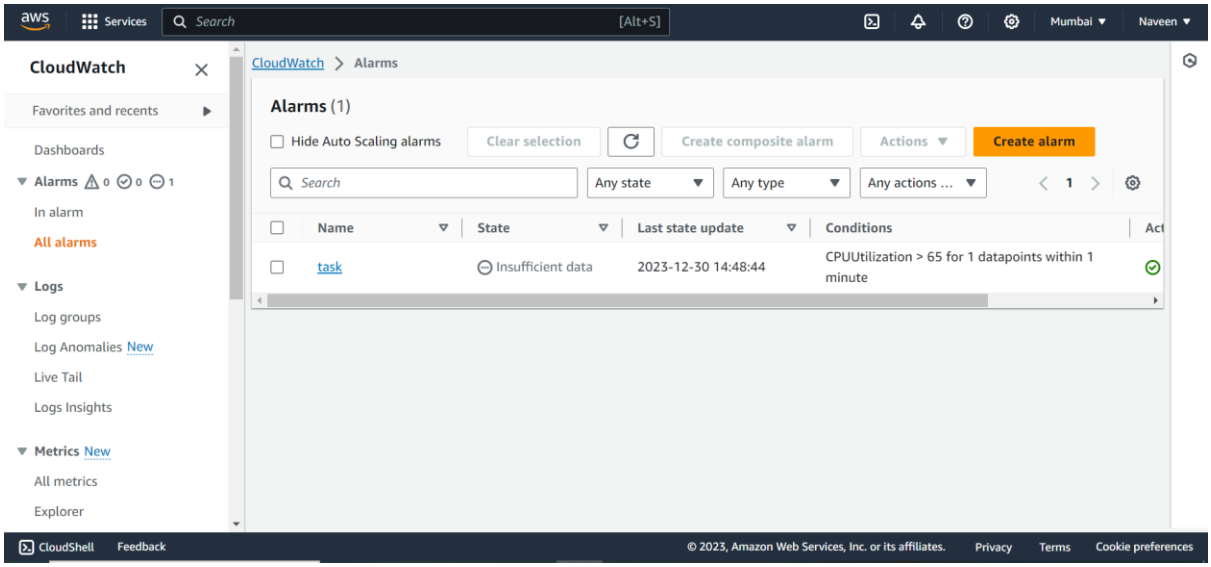

aws
Services
Search
[Alt+S]
Mumbai
Naveen
Conditions
Threshold type
Static
Use a value as a threshold
Anomaly detection
Use a band as a threshold
Whenever CPUUtilization is...
Define the alarm condition.
Greater
> threshold
Greater/Equal
>= threshold
Lower/Equal
<= threshold
Lower
< threshold
than...
Define the threshold value.
65
Must be a number
Additional configuration
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

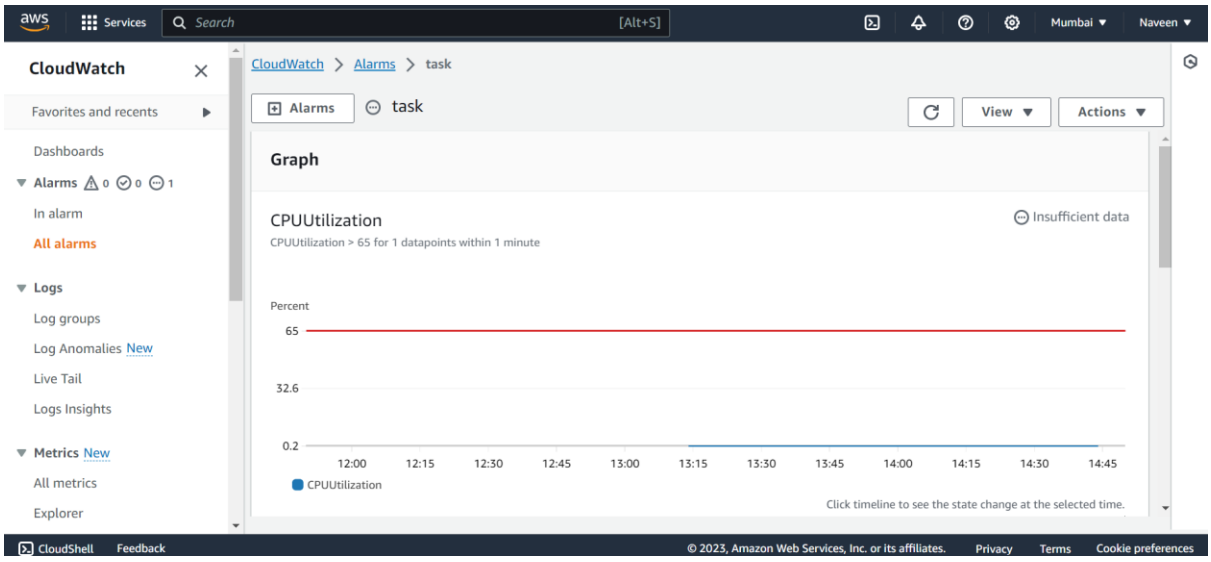

aws
Services
Search
[Alt+S]
Mumbai
Naveen
Amazon SNS
Dashboard
Topics
Subscriptions
Mobile
Push notifications
Text messaging (SMS)
Origination numbers
Amazon SNS > Topics > task-CloudWatch-Alarms-Topic
task-CloudWatch-Alarms-Topic
Edit
Delete
Publish message
Details
Name
task-CloudWatch-Alarms-Topic
ARN
arn:aws:sns:ap-south-1:237981402912:task-CloudWatch-Alarms-Topic
Type
Standard
Display name
EC2 - instance CUP utilization is above 65%
Topic owner
237981402912
Subscriptions
Access policy
Data protection policy
Delivery policy (HTTP/S)
Delivery status log

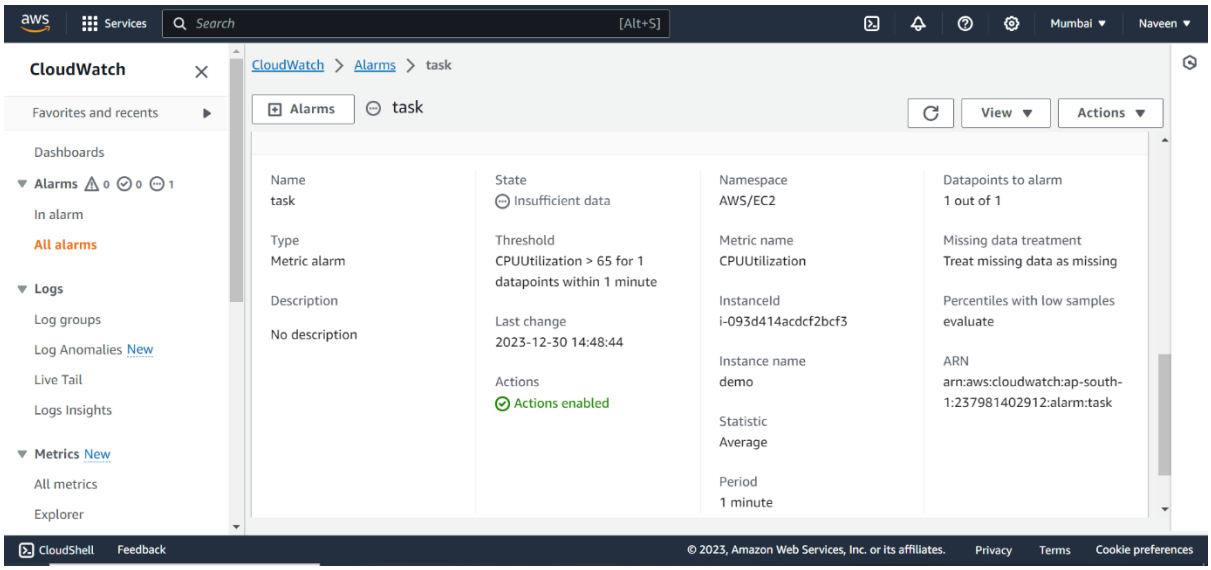

Services
Search
[Alt+S]
Mumbai
Naveen
Step 2
Configure actions
Step 3
Add name and description
Step 4
Preview and create
Notification
Alarm state trigger
Define the alarm state that will trigger this action.
Remove
In alarm
The metric or expression is outside of the defined threshold.
OK
The metric or expression is within the defined threshold.
Insufficient data
The alarm has just started or not enough data is available.
Send a notification to the following SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.
Select an existing SNS topic
Create new topic
Use topic ARN to notify other accounts
Send a notification to...
task-CloudWatch-Alarms-Topic
Only email lists for this account are available.
Email (endpoints)
naveenrajasekaran2000@gmail.com - View in SNS Console
Add notification
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

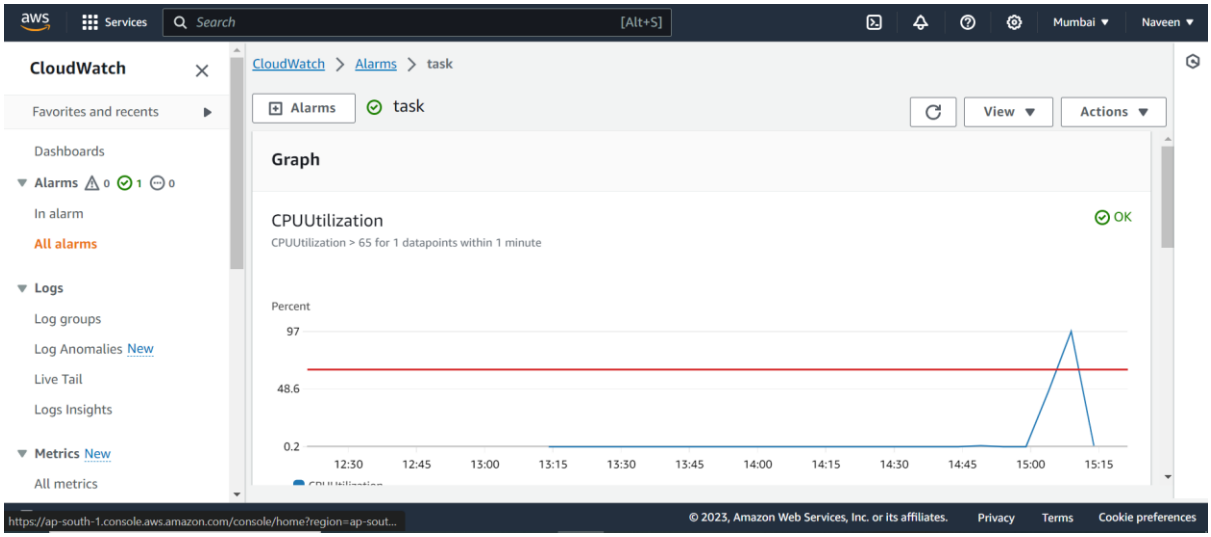

Services
Search
[Alt+S]
Mumbai
Naveen
CloudWatch
Alarms
Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add name and description
Step 4
Preview and create
Add name and description
Name and description
Alarm name
task
Alarm description - optional
View formatting guidelines
Edit
Preview
This is an H1
double asterisks will produce strong character
This is [an example](https://example.com/) inline link.
Up to 1024 characters (0/1024)
Markdown formatting is only applied when viewing your alarm in the console. The description will remain in
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

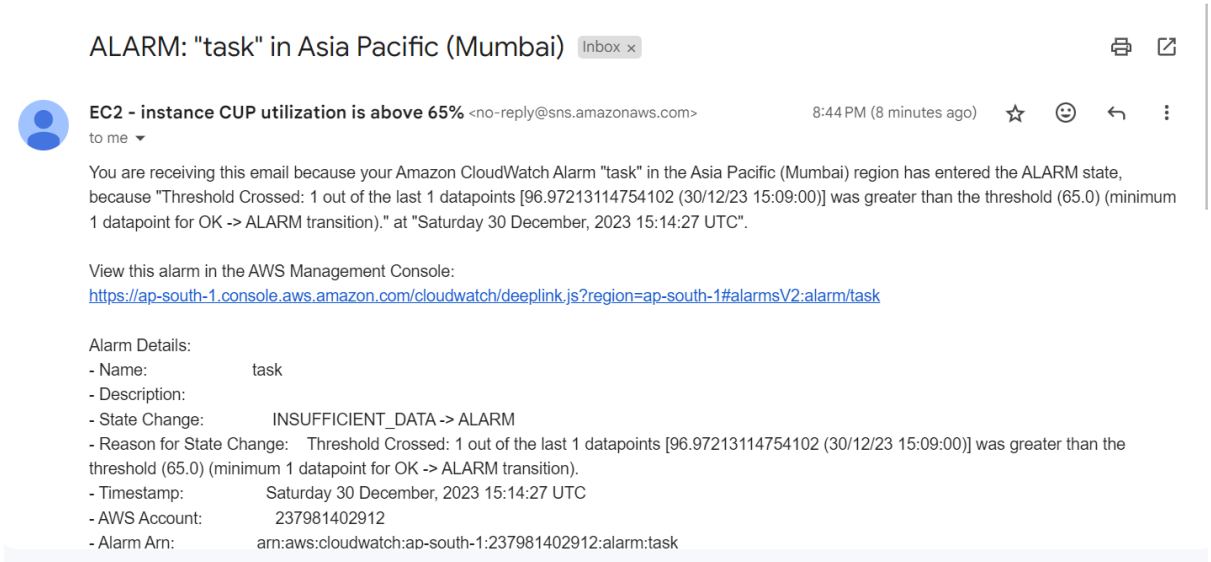

Services
Search
[Alt+S]
Mumbai
Naveen
CloudWatch
Alarms
Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add name and description
Step 4
Preview and create
Preview and create
Step 1: Specify metric and conditions
Edit
Metric
Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 minute.
Percent
65
65
32.6
Namespace
AWS/EC2
Metric name
CPUUtilization
InstanceId
i-093d414acdcf2bcf3
Instance name
demo
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Mumbai
Naveen
CloudWatch
Favorites and recents
Dashboards
Alarms 0 0 1
In alarm
All alarms
Logs
Log groups
Log Anomalies New
Live Tail
Logs Insights
Metrics New
All metrics
Explorer
CloudWatch > Alarms
Alarms (1)
Hide Auto Scaling alarms
Clear selection
Create composite alarm
Actions
Create alarm
Search
Any state
Any type
Any actions ...
1
Name
State
Last state update
Conditions
task
Insufficient data
2023-12-30 14:48:44
CPUUtilization > 65 for 1 datapoints within 1 minute
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Mumbai
Naveen
CloudWatch
Favorites and recents
Dashboards
Alarms 0 0 1
In alarm
All alarms
Logs
Log groups
Log Anomalies New
Live Tail
Logs Insights
Metrics New
All metrics
Explorer
CloudWatch > Alarms > task
Alarms
task
View
Actions
Graph
CPUUtilization
CPUUtilization > 65 for 1 datapoints within 1 minute
Insufficient data
Percent
65
32.6
0.2
12:00
12:15
12:30
12:45
13:00
13:15
13:30
13:45
14:00
14:15
14:30
14:45
CPUUtilization
Click timeline to see the state change at the selected time.
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Mumbai
Naveen
CloudWatch
Favorites and recents
Dashboards
Alarms 0 0 1
In alarm
All alarms
Logs
Log groups
Log Anomalies New
Live Tail
Logs Insights
Metrics New
All metrics
Explorer
CloudWatch > Alarms > task
Alarms
task
View
Actions
Name
task
State
Insufficient data
Namespace
AWS/EC2
Datapoints to alarm
1 out of 1
Type
Metric alarm
Threshold
CPUUtilization > 65 for 1 datapoints within 1 minute
Metric name
CPUUtilization
Missing data treatment
Treat missing data as missing
Description
No description
Last change
2023-12-30 14:48:44
InstanceId
i-093d414acdcf2bcf3
Percentiles with low samples
evaluate
Actions
Actions enabled
Instance name
demo
ARN
arn:aws:cloudwatch:ap-south-1:237981402912:alarm:task
Statistic
Average
Period
1 minute
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences





ALARM: "task" in Asia Pacific (Mumbai) Inbox ×

EC2 - instance CUP utilization is above 65% <no-reply@sns.amazonaws.com> 8:44 PM (8 minutes ago)

to me

You are receiving this email because your Amazon CloudWatch Alarm "task" in the Asia Pacific (Mumbai) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [96.97213114754102 (30/12/23 15:09:00)] was greater than the threshold (65.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Saturday 30 December, 2023 15:14:27 UTC".

View this alarm in the AWS Management Console:
https://ap-south-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=ap-south-1#alarmsV2:alarm/task

Alarm Details:
- Name: task
- Description:
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [96.97213114754102 (30/12/23 15:09:00)] was greater than the threshold (65.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Saturday 30 December, 2023 15:14:27 UTC
- AWS Account: 237981402912
- Alarm Arn: arn:aws:cloudwatch:ap-south-1:237981402912:alarm:task