

Module 3: IAM Users Assignment

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 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, Test1 and Test2 to the Ops Team.

Created 4 IAM User Dev1,Dev2,Test1 & Test2

Inbox (738) - ratre.raj@gmail.co

Start Course | Intellipaat

Users | IAM | Global

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

aws

Services

Search

[Alt+S]

Global

prakash24

EC2

EC2 Image Builder

S3

IAM

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

IAM > Users

Users (7) Info

Delete

Create user

Search e

5 matches

< 1 >

	User name	Path	Group:	Last activity	MFA	Pass
<input type="checkbox"/>	Dev1	/	0	-	-	-
<input type="checkbox"/>	Dev2	/	0	-	-	-
<input type="checkbox"/>	ec2-user	/	0	-	-	-
<input type="checkbox"/>	Test1	/	0	-	-	-
<input type="checkbox"/>	Test2	/	0	-	-	-

CloudShell

Feedback

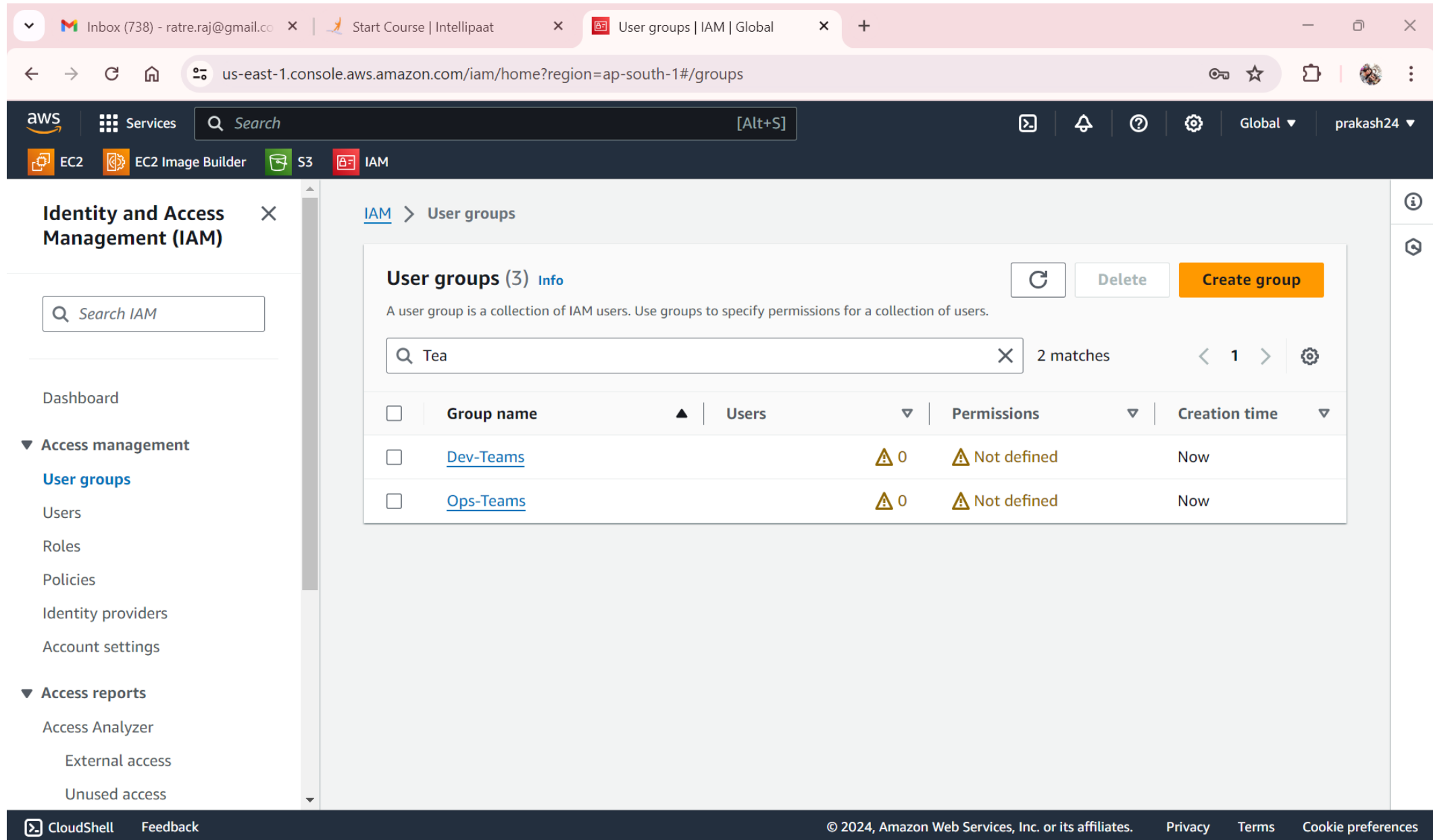
© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

Created Two Groups Dev-Teams & Ops-Teams



Added User Dev1 & Dev2 in Dev-Teams Group

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/details/Dev-Teams?section=users

aws

Services

Search

[Alt+S]

EC2

EC2 Image Builder

S3

IAM

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

IAM > User groups > Dev-Teams

Dev-Teams

Info

Delete

Summary

Edit

User group name

Dev-Teams

Creation time

July 06, 2024, 16:19 (UTC+05:30)

ARN

arn:aws:iam::654654393526:group/Dev-Teams

Users (2)

Permissions

Access Advisor

Users in this group (2)

Refresh

Remove

Add users

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 >

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	Dev1	1	None	8 minutes ago
<input type="checkbox"/>	Dev2	1	None	7 minutes ago

Added Test1 & Test2 user to Group Ops-Teams

Start Course | Intellipaat

Ops-Teams | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/details/Ops-Teams?section=users

aws

Services

Search

[Alt+S]

EC2

EC2 Image Builder

S3

IAM

Global

prakash24

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Ops-Teams

Info

Delete

Summary

Edit

User group name

Ops-Teams

Creation time

July 06, 2024, 16:19 (UTC+05:30)

ARN

arn:aws:iam::654654393526:group/Ops-Teams

Users (2)

Permissions

Access Advisor

Users in this group (2)

Remove

Add users

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 >

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	Test1	1	None	8 minutes ago
<input type="checkbox"/>	Test2	1	None	7 minutes ago

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

Module 3: IAM Policies Assignment

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

Policy Number 1

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

aws

Services

Search

[Alt+S]

EC2

EC2 Image Builder

S3

IAM

VPC

Global

prakash24

Step 2

Review and create

Policy details

Policy name

Enter a meaningful name to identify this policy.

number1

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 420 services)

Show remaining 417 services

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

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

Policy Number 2

number2 | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A654654393526%3Apolicy%3Anumber2

Services

EC2EC2 Image BuilderS3IAMVPC

Search [Alt+S]

Globalprakash24

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

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

Access reports

- Access Analyzer
 - External access
 - Unused access
 - Analyzer settings
- Credential report
- Organization activity
- Service control policies

number2

EditDelete

Policy details

Type	Creation time	Edited time	ARN
Customer managed	July 23, 2024, 08:42 (UTC+05:30)	July 23, 2024, 08:42 (UTC+05:30)	arn:aws:iam::654654393526:policy/number2

Permissions

Entities attached

Tags

Policy versions (1)

Access Advisor

Permissions defined in this policy

EditSummaryJSON

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 420 services) Show remaining 416 services

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

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

Attaching Policy Number 1 to Dev-Teams

Dev-Teams | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/details/Dev-Teams?section=permissions

Incognito

Services

Search

[Alt+S]

Global

prakash24

EC2

EC2 Image Builder

S3

IAM

VPC

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Policies attached to this user group.

IAM > User groups > Dev-Teams

Dev-Teams

Delete

Summary

Edit

User group name

Dev-Teams

Creation time

July 06, 2024, 16:19 (UTC+05:30)

ARN

arn:aws:iam::654654393526:group/Dev-Teams

Users (2)

Permissions

Access Advisor

Permissions policies (1)

Info

You can attach up to 10 managed policies.

Search

Filter by Type

All types

< 1 >

Policy name

Type

Attached entities

number1

Customer managed

1

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

Attaching Policy Number 2 to Ops-Teams

Ops-Teams | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/groups/details/Ops-Teams?section=permissions

Services

Search

[Alt+S]

EC2

EC2 Image Builder

S3

IAM

VPC

Globalprakash24

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Policies attached to this user group.

IAM > User groups > Ops-Teams

Ops-Teams

Delete

Summary

Edit

User group name

Ops-Teams

Creation time

July 06, 2024, 16:19 (UTC+05:30)

ARN

arn:aws:iam::654654393526:group/Ops-Teams

Users (2)

Permissions

Access Advisor

Permissions policies (1)

Info

Refresh

Simulate

Remove

Add permissions

You can attach up to 10 managed policies.

Search

Filter by Type

All types

< 1 >

Settings

☐

Policy name

▲

☐

+

number2

▲

Type

▼

Customer managed

Attached entities

▼

1

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

Module 3: IAM Roles Assignment

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 a role which only lets user1 and user2 from task 1 to have complete access to VPCs and DynamoDB.
2. Login into user1 and shift to the role to test out the feature.

Created a IAM Role having VPC Full access & DynamoDB Full Access

Role-user-vpcfull-dynamodbfull

Test2 | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/Role-user-vpcfull-dynamodbfull?section=permissions

Incognito

aws

Services

Search

[Alt+S]

EC2

EC2 Image Builder

S3

IAM

VPC

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Role-user-vpcfull-dynamodbfull

VCP Full Access and DynamoDB full access

Summary

Creation date

July 23, 2024, 09:05 (UTC+05:30)

ARN

arn:aws:iam::654654393526:role/Role-user-vpcfull-dynamodbfull

Link to switch roles in console

https://signin.aws.amazon.com/switchrole?roleName=Role-user-vpcfull-dynamodbfull&account=654654393526

Last activity

-

Maximum session duration

1 hour

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

Permissions policies (2)

You can attach up to 10 managed policies.

Search

Filter by Type

All types

Policy name

Type

Attached entities

AmazonDynamoDBFullAccess

AWS managed

2

AmazonVPCFullAccess

AWS managed

1

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

Adding Test1 & Test2 User to trust policy so use can access as role

The screenshot shows the AWS IAM console interface. The browser address bar indicates the URL: `us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/Role-user-vpcfull-dynamodbfull/edit-trust-policy`. The page title is "Edit trust policy".

The main content area displays a JSON policy statement with the following structure:

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": [
8           "arn:aws:iam::654654393526:user/Test1",
9           "arn:aws:iam::654654393526:user/Test2"
10        ]
11      },
12      "Action": "sts:AssumeRole",
13      "Condition": {}
14    }
15  ]
16 }
```

The right-hand sidebar contains the following sections:

- Edit statement** (with a "Remove" link)
- Add actions for STS** (with a "Filter actions" search bar)
- Access level - read** (with checkboxes for `GetAccessKeyInfo`, `GetCallerIdentity`, `GetFederationToken`, `GetServiceBearerToken`, and `GetSessionToken`)
- Access level - read or write** (with a dropdown arrow)
- Add a principal** (with an "Add" button)
- Add a condition (optional)** (with an "Add" button)

At the bottom left, there is a button labeled "+ Add new statement".

Login as Test1 user

Console Home | Console Home

ap-south-1.console.aws.amazon.com/console/home?region=ap-south-1#

Incognito

aws

Services

Search

[Alt+S]

EC2

EC2 Image Builder

S3

IAM

VPC

Mumbai

Test1 @ 6546-5439-3526

Console Home

Reset to default layout

Add widgets

Recently visited

CloudWatch

Application Composer

CloudFormation

Lambda

S3

Billing and Cost Management

RDS

EC2

DynamoDB

IAM

View all services

Applications (0)

Create application

Region: Asia Pacific (Mumbai)

ap-south-1 (Current Region)

Find applications

1

Name	Description	Region	Originating account
Access denied			

Go to myApplications

Welcome to AWS

Getting started with

AWS Health

Cost and usage

Current month costs

Cost breakdown

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

Switched as Assigned Role

Console Home | Console Home

ap-south-1.console.aws.amazon.com/console/home?region=ap-south-1#

Incognito

Services

Search

[Alt+S]

EC2

EC2 Image Builder

S3

IAM

VPC

Mumbai

Test User

Console Home

Info

Recently visited

Info

IAM

DynamoDB

EC2

RDS

Billing and Cost Management

S3

Lambda

CloudFormation

Application Composer

CloudWatch

View all services

Applications (0)

Info

Region: Asia Pacific (Mumbai)

ap-south-1 (Current Region)

Name

Description

Access denied

Go to my

Account

Organization

Service Quotas

Billing and Cost Management

Signed in as: Test1

Account ID: 6546-5439-3526

Switch back

Role history

Test User

Switch role

Sign out

Welcome to AWS

Info

Getting started with

AWS Health

Info

Cost and usage

Info

Current month costs

Cost breakdown

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

User Can access the VPC Dashboard

Home | VPC Console

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#Home:

Search [Alt+S]

EC2 EC2 Image Builder S3 IAM VPC

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only Internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

Introducing the new VPC console experience

We've made updates to the VPC console. This new experience won't change how you work in the console. If you experience a problem with your access, see the [troubleshooting documentation](#) to get information about how to resolve it. You can [opt out of the new experience](#) until 31 July 2024. Before that date, you must resolve the access issues to continue using the console. You can also [report issue details](#).

Create VPC

Launch EC2 Instances

Note: Your Instances will launch in the Asia Pacific region.

Resources by Region

You are using the following Amazon VPC resources

VPCs

Asia Pacific 1

See all regions

NAT Gateways

Asia Pacific 0

See all regions

Subnets

Asia Pacific 3

See all regions

VPC Peering Connections

Asia Pacific 0

See all regions

Route Tables

Asia Pacific 1

See all regions

Network ACLs

Asia Pacific 1

See all regions

Internet Gateways

Asia Pacific 1

See all regions

Security Groups

Asia Pacific 3

See all regions

Service Health

[View complete service health details](#)

Settings

[Zones](#)

[Console Experiments](#)

Additional Information

[VPC Documentation](#)

[All VPC Resources](#)

[Forums](#)

[Report an Issue](#)

AWS Network Manager

AWS Network Manager provides

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

User Can access the DynamoDB

Dashboard | Amazon DynamoDB

ap-south-1.console.aws.amazon.com/dynamodbv2/home?region=ap-south-1#dashboard

aws

Services

Search

[Alt+S]

EC2

EC2 Image Builder

S3

IAM

VPC

Share your feedback on Amazon DynamoDB

Your feedback is an important part of helping us provide a better customer experience. Take this short survey to let us know how we're doing.

Share feedback

DynamoDB

Dashboard

Tables

Explore items

PartiQL editor

Backups

Exports to S3

Imports from S3

Integrations New

Reserved capacity

Settings

DAX

Clusters

Subnet groups

Parameter groups

Events

DynamoDB > Dashboard

Dashboard

Alarms (0) Info

Manage in CloudWatch

Find alarms

< 1 >

Alarm name Status

No custom alarms

DAX clusters (0) Info

View details

Find clusters

< 1 >

Create resources

Create an Amazon DynamoDB table for fast and predictable database performance at any scale. [Learn more](#)

Create table

Amazon DynamoDB Accelerator (DAX) is a fully-managed, highly-available, in-memory caching service for DynamoDB. [Learn more](#)

Create DAX cluster

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

Module 3: CloudWatch Dashboard Assignment

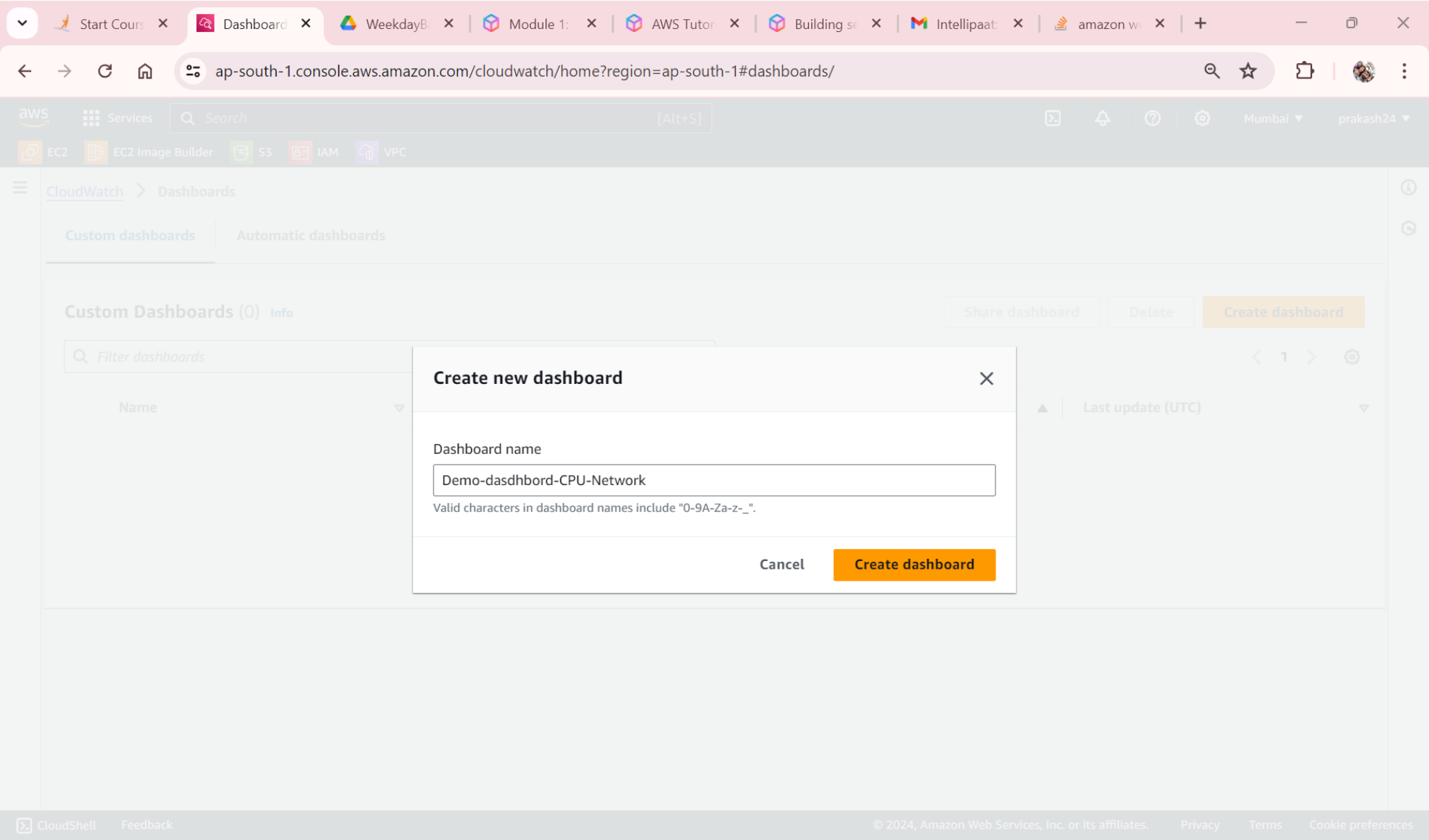
Problem Statement:

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. Also, you will be monitoring the machines created by these users for any errors or misconfigurations.

Tasks To Be Performed:

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

Cloudwatch dashboard creation Step 1



Adding metric to dashboard

Start Co x Instance x Dashbo x Weekda x Module x AWS Tu x Building x Intellipa x amazon x +

← → ↻ 🏠 🔍 ☆ 📌 🎵 👤 ⋮

ap-south-1.console.aws.amazon.com/cloudwatch/home?region=ap-south-1#dashboards

aws Services 🔍 Search [Alt+S]

📦 EC2 📦 EC2 Image Builder 📦 S3 📦 IAM 📦 VPC

☰ CloudWatch > Dashboards

Custom dashboards Automatic dashboards

Custom Dashboards (1) Info

🔍 Filter dashboards

Name

Demo-dasdhbord-CPU-Network

Share dashboard Delete Create dashboard

< 1 > ⚙️

▲ Last update (UTC) ▼

2024-07-23 05:00

Add to dashboard

Select a dashboard

Select an existing dashboard or create a new one.

🔍 Demo-dasdhbord-CPU-Network

Create new

Cancel Add to dashboard

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Demo Instance for cloudwatch dashboard

Start

Insta

EC2

Clou

Wee

Moc

AW

Build

Inte

ama

Test

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

aws Services Search [Alt+S]

EC2 EC2 Image Builder S3 IAM VPC

EC2 Dashboard

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive)

All states

Instance state = running

Clear filters

1

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input checked="" type="checkbox"/>	demo-ec2	i-0a12f880380783fd0	Running	t2.micro	2/2 checks passed	View alarms	ap-south-1b

i-0a12f880380783fd0 (demo-ec2)

Details Status and alarms Monitoring Security Networking Storage Tags

Instance summary Info

Instance ID

i-0a12f880380783fd0 (demo-ec2)

IPv6 address

—

Public IPv4 address

3.109.1.0 | open address

Instance state

Running

Private IPv4 addresses

172.31.6.162

Public IPv4 DNS

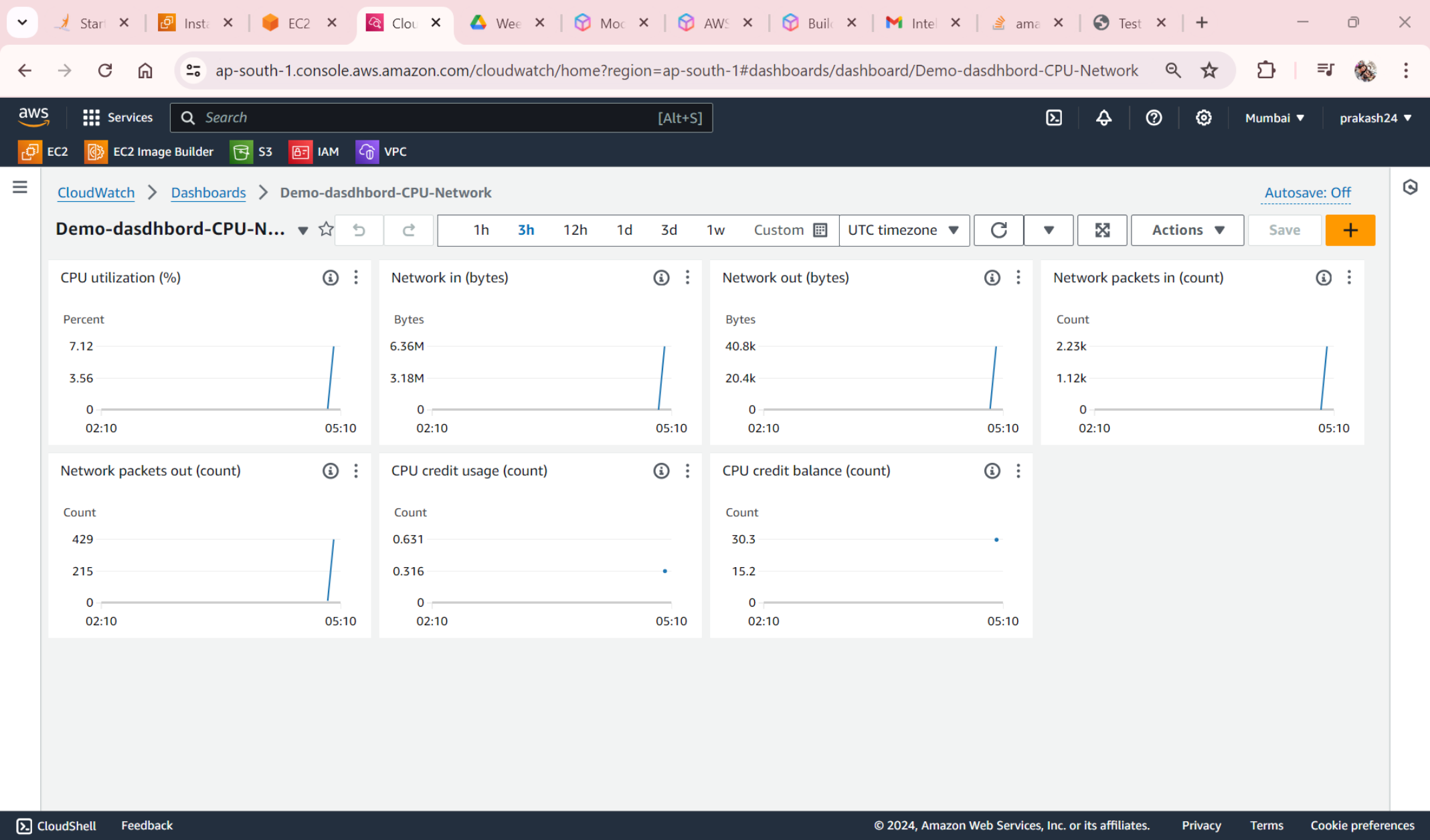
ec2-3-109-1-0.ap-south-1.compute.amazonaws.com | open address

Private IP DNS name (IPv4 only)

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

CPU & Network utilization of demo-ec2



Module 3: CloudWatch Alarms Assignment

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. 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.

Alarm Creation Step 1

The screenshot shows the AWS CloudWatch console in the 'Create alarm' wizard, specifically Step 1: 'Specify metric and conditions'. The browser address bar shows the URL: `ap-south-1.console.aws.amazon.com/cloudwatch/home?region=ap-south-1#alarmsV2:create?~(Page~'MetricSelection~AlarmType~'Metric...`. The AWS navigation bar at the top includes the 'Services' search bar and various service icons like EC2, S3, IAM, and VPC. The left sidebar shows the breadcrumb 'CloudWatch > Alarms > Create alarm' and a list of steps: Step 1 (Specify metric and conditions), Step 2 (Configure actions), Step 3 (Add name and description), and Step 4 (Preview and create). The main content area is titled 'Specify metric and conditions' and contains a 'Metric' section with a 'Graph' preview area. The 'Graph' section includes the text 'Preview of the metric or metric expression and the alarm threshold.' and a 'Select metric' button. At the bottom right of the main content area are 'Cancel' and 'Next' buttons. The footer of the page includes 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc. or its affiliates, along with links for 'Privacy', 'Terms', and 'Cookie preferences'.

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

Graph
Preview of the metric or metric expression and the alarm threshold.

Select metric

Cancel Next

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Metric Selection for alarm creation

Start

Week

Modu

AWS

Buildi

Intelli

amaz

Settin

Creat

Select

us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~'MetricSelection~AlarmType~'MetricAlar...

aws Services Search [Alt+S]

EC2 EC2 Image Builder S3 IAM VPC

CloudWatch > Alarms > Create alarm

Step 1 Specify

Step 2 Configure

Step 3 Add name

Step 4 Preview

Select metric

×

Untitled graph

1h 3h 12h 1d 3d 1w Custom UTC timezone Line

No unit

1

0.5

0

00:00 00:30 01:00 01:30 02:00 02:30 03:00 03:30 04:00 04:30 05:00 05:30 06:00

EstimatedCharges

Browse

Multi source query

Graphed metrics (1)

Options

Source

Add math

Add query

Metrics (1)

Alarm recommendations

Graph with SQL

Graph search

N. Virginia

All > Billing > Total Estimated Charge

Search for any metric, dimension, resource id or account id

< 1 >

☒

Currency 1/1

▲

☒

USD

EstimatedCharges

No alarms

Cancel

Select metric

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 1 of alarm creation

Start

Week

Modu

AWS

Buildi

Intelli

amaz

Settin

Create

Create

us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~'MetricSelection~AlarmType~'MetricAlar...

ServicesSearch[Alt+S]

EC2EC2 Image BuilderS3IAMVPC

N. Virginiaprakash24

07/1607/1807/2007/22

EstimatedCharges

Maximum

Period6 hours

Conditions

Threshold type

StaticUse a value as a threshold

Anomaly detectionUse 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

CloudShellFeedback

© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

Step 2 of alarm creation

us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create?~(Page~'Actions~AlarmType~'MetricAlarm~Alar...

aws

Services

Search

[Alt+S]

EC2

EC2 Image Builder

S3

IAM

VPC

N. Virginia

prakash24

Step 1

[Specify metric and conditions](#)

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.

☒ 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.

Remove

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...

Default_CloudWatch_Alarms_Topic

X

Only topics belonging to this account are listed here. All persons and applications subscribed to the selected topic will receive notifications.

Email (endpoints)

ratre.raj@gmail.com - [View in SNS Console](#)

Add notification

Lambda action

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

A CloudWatch billing alarm which goes off when the estimated charges go above \$500

The screenshot displays the AWS CloudWatch console interface. The browser address bar shows the URL: `us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:alarm/billing-500usd`. The console header includes the AWS logo, a search bar, and navigation links for various services like EC2, IAM, and VPC. The left sidebar shows the 'CloudWatch' navigation menu with options like Alarms, Logs, Metrics, and Events. The main content area is titled 'billing-500usd' and shows a graph for 'EstimatedCharges'. The graph displays a red line at the 500 mark, indicating the alarm is in the 'In alarm' state. The legend at the bottom of the graph shows the following states: In alarm (red), OK (green), Insufficient data (grey), and Disabled actions (blue). The graph also includes a timeline view and a legend for the alarm states.

CloudWatch

Alarms (1)

Search

Alarm state: Any

Alarm type: Any

Actions status: Any

☐ Hide Auto Scaling alarms

< 1 >

billing-500usd

Metric alarm

Insufficient data

Graph

1h 3h 12h 1d 3d 1w Custom UTC timezone

EstimatedCharges

EstimatedCharges > 500 for 1 datapoints within 6 hours

Insufficient data

No unit

500

250

0

07/17 07/18 07/19 07/20 07/21 07/22 07/23

EstimatedCharges

Click timeline to see the state change at the selected time.

7/17 7/18 7/19 7/20 7/21 7/22 7/23

In alarm OK Insufficient data Disabled actions

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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

The screenshot displays the AWS CloudWatch console interface. The top navigation bar includes the AWS logo, a search bar, and various service icons. The main content area is titled "CloudWatch" and shows a list of alarms on the left sidebar. The "Alarms (2)" section is active, displaying two alarms: "ec2-cpu" and "billing-500usd". The "ec2-cpu" alarm is highlighted, showing its details in the main panel. The alarm is a "Metric alarm" for "CPUUtilization" on the "ec2-cpu" metric, with a threshold of 60. The alarm is currently in the "OK" state. The main panel also features a "Graph" section showing the "CPUUtilization" metric over time, with a red line indicating the alarm threshold at 60%. The graph shows the alarm is currently in the "OK" state.

CloudWatch

Alarms (2)

Search

Alarm state: Any

Alarm type: Any

Actions status: Any

☐ Hide Auto Scaling alarms

< 1 >

ec2-cpu

Metric alarm

OK

billing-500usd

Metric alarm

OK

Graph

1h 3h 12h 1d 3d 1w Custom Local timezone

CPUUtilization

CPUUtilization > 60 for 1 datapoints within 5 minutes

OK

Percent

60

31.7

3.49

09:00 09:15 09:30 09:45 10:00 10:15 10:30 10:45 11:00 11:15 11:30 11:45

CPUUtilization

Click timeline to see the state change at the selected time.

In alarm OK Insufficient data Disabled actions

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences