

# Cloud Security

# Why Cloud Security?

Let's talk about some security breaches in the past:



LinkedIn

SONY

Sony



iCloud

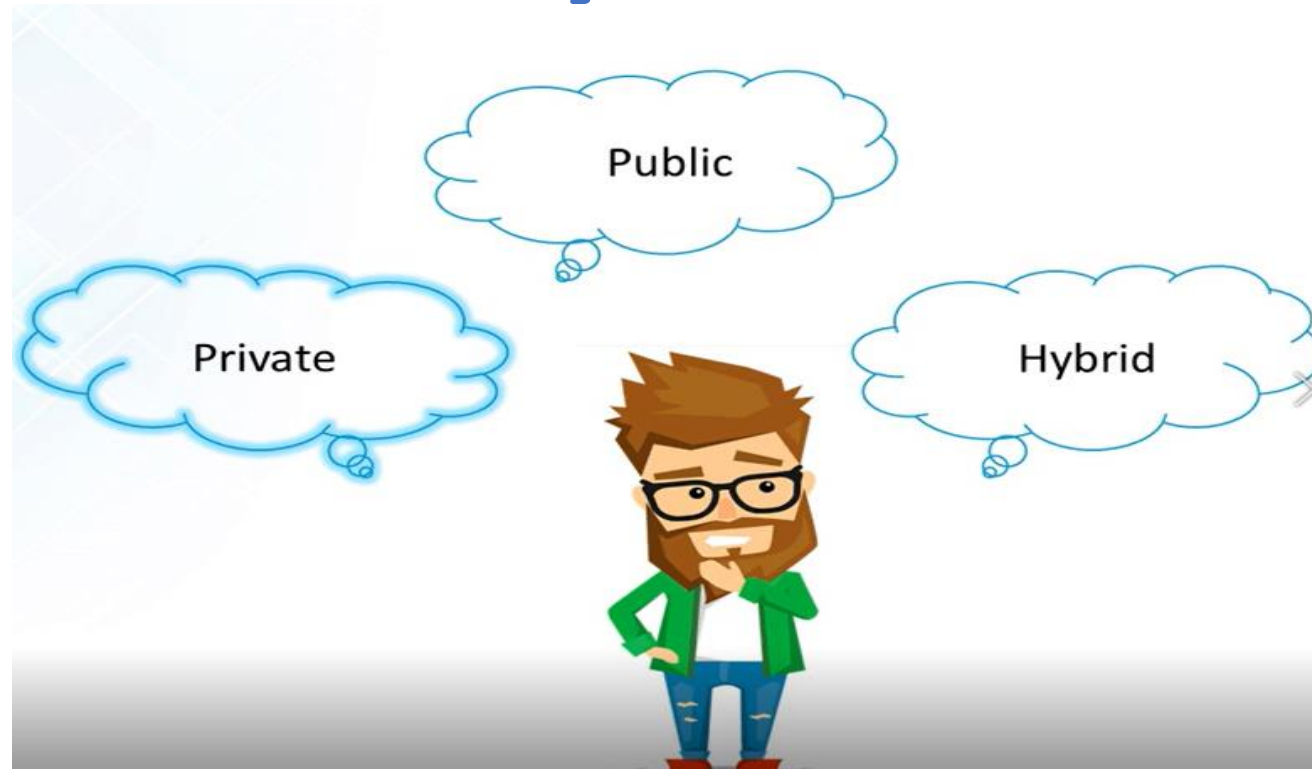
- **LinkedIn 6.5M Username-Passwords were hacked from LinkedIn site & published to public sites**
- **Sony experienced the most aggressive cyber attack in history where in their financials, Movie projects and much more was published publicly by hackers.**
- **iCloud faced a similar hack wherein private images of users from their database were made public.**

# What is Cloud Security?



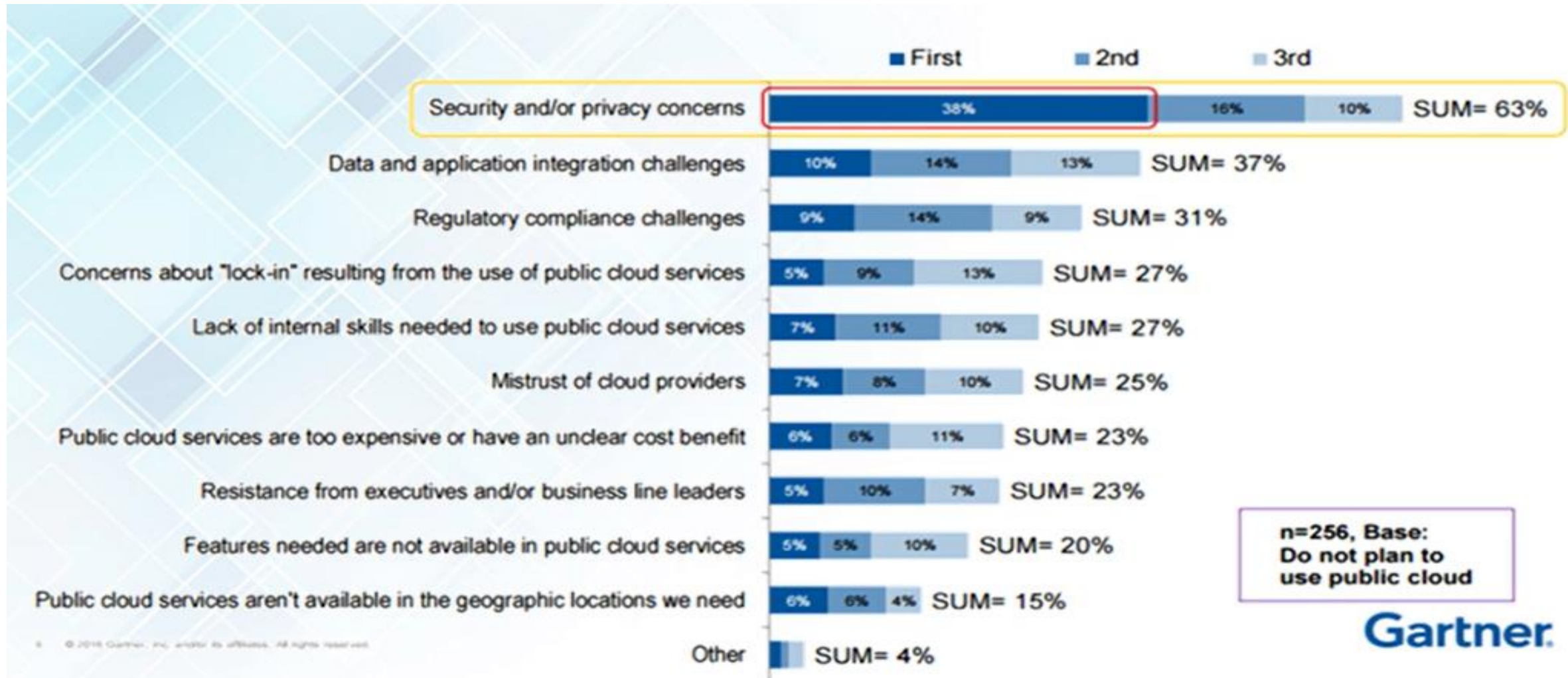
- **Cloud Security is the use of latest technologies & security techniques to protect your data, application & infrastructure associated with cloud computing.**
- **Cloud Security is defending the confidentiality(C), integrity(I) and availability(A) of enterprise assets (data, application, infrastructure), using cloud services, from an outside or inside threat**

# Public, Private or Hybrid?



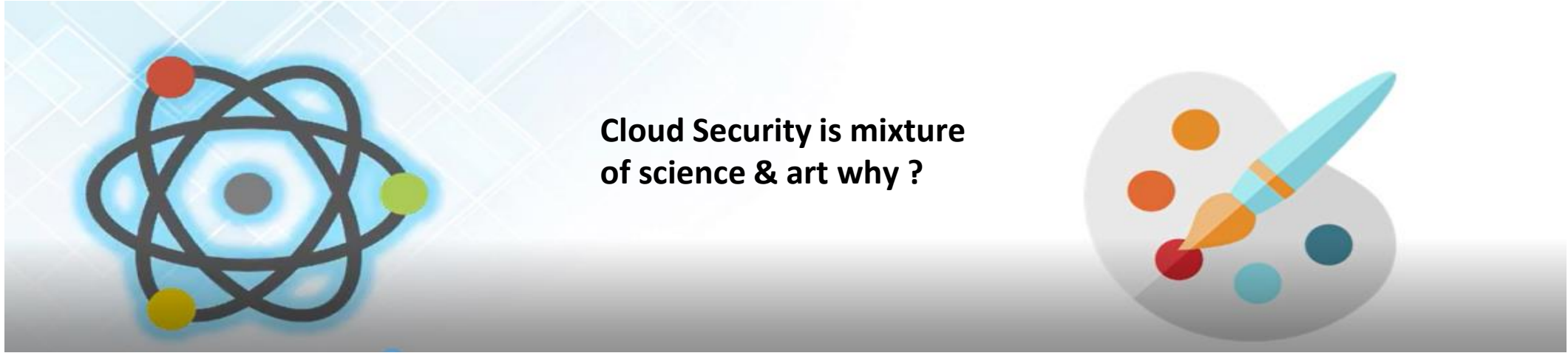
- **Data Security critical.**
- **No issue with data security.**
- **Some Part secure some not.**

# Is Cloud Security really a concern?



- According Gartner Survey report regarding concern for switching to cloud

# How secure should you make your application?



- In general term cloud security is combination of art and science (like technique and technology)for example we have resources but no idea to manage it or having techniques but no resource
- Science will give us new way of securing your application.
- Art because authentication should be defined with user experience in mind ( or user mindset) –How many issue can be generate?, How many type of security expect ?

# How to troubleshoot a thread in the cloud?

- Use Case: “While login in Facebook or google on your phone, you get a random message”
  - Two facta authentication process
  - Enter Password then Enter OTP send on registered mobile
  - Not easy for user but it made more security for environment
- Use Case “ While accessing a message on Facebook it become spam & all your contact on Facebook get the same message from u r account”
  - This thing happened because it is hacked by someone

# Understanding Data Security

Since all the data is transferred using Internet, data security is of major concern in the cloud. Here are key mechanisms for protecting data.

- Access Control
- Auditing
- Authentication
- Authorization

All of the service models should incorporate security mechanism operating in all above-mentioned areas



# Isolated Access to Data

Since data stored in cloud can be accessed from anywhere, we must have a mechanism to isolate data and protect it from client's direct access.

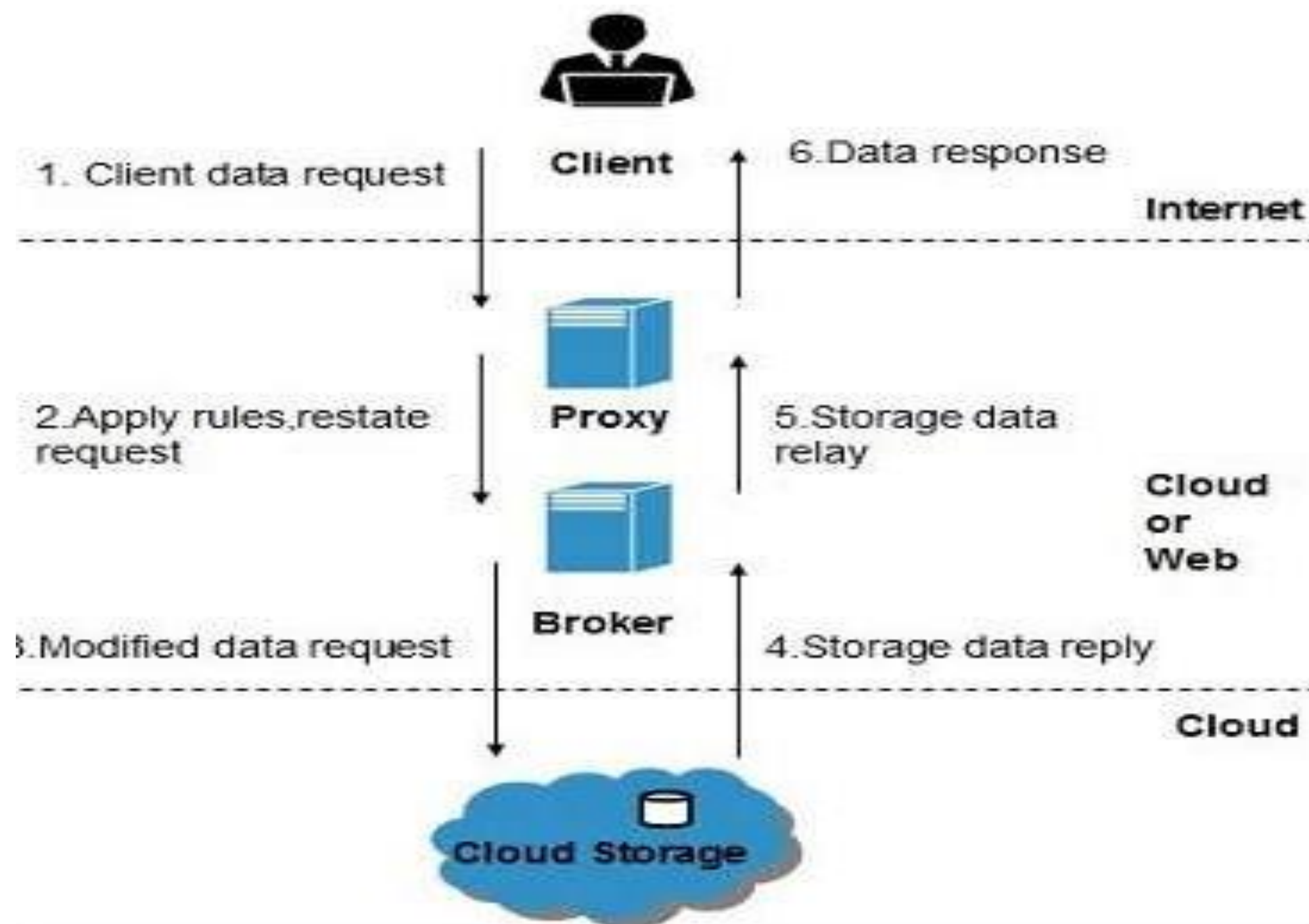
**Brokered Cloud Storage Access** is an approach for isolating storage in the cloud. In this approach, two services are created:

- A broker with full access to storage but no access to client.
- A proxy with no access to storage but access to both client and broker.

# Brokered Cloud Storage Access System

When the client issues request to access data:

- The client data request goes to the external service interface of proxy.
- The proxy forwards the request to the broker.
- The broker requests the data from cloud storage system.
- The cloud storage system returns the data to the broker.
- The broker returns the data to proxy.
- Finally the proxy sends the data to the client.



# Encryption

Encryption helps to protect data from being compromised. It protects data that is being transferred as well as data stored in the cloud. Although encryption helps to protect data from any unauthorized access, it does not prevent data loss.

# Thread Identification in Cloud Computing

Threat identification is done in 3 stages in the Cloud :



- **Monitoring Data:** Using Machine learning algorithms you can set your monitoring application to flag an event


# AWS Cloud Watch





AWS Cloudwatch

- Monitor EC2 and other AWS resources
- The ability to monitor custom metrics
- Monitor and store logs
- Set Alarms
- View Graphs and Statistics
- Monitor and React to Resource Changes


# How AWS manage three identification stage




Services ▾ Resource Groups ▾ 


 Edureka ▾ Oregon ▾ Support ▾


## AWS services


Find a service by name (for example, EC2, S3, Elastic Beanstalk) 


▾ Recently visited services

 CloudTrail


 CloudFormation


 CloudWatch


 S3


 EC2


▾ All services


 **Compute**  
EC2  
EC2 Container Service  
Lightsail  
Elastic Beanstalk  
Lambda  
Batch


 **Developer Tools**  
CodeCommit  
CodeBuild  
CodeDeploy  
CodePipeline  
X-Ray


 **Internet of Things**  
AWS IoT

 **Contact Center**  
Amazon Connect


 **Game Development**  
Amazon GameLift

 **Mobile Services**  
Mobile Hub


 **Management Tools**  
CloudWatch  
CloudFormation  
CloudTrail  
Config

 **Storage**  
S3  
EFS  
Glacier

## Featured next steps



**Manage your costs**  
Get real-time billing alerts based on your cost and usage budgets. [Start now](#)



**Get best practices**  
Use AWS Trusted Advisor for security, performance, cost and availability best practices. [Start now](#)

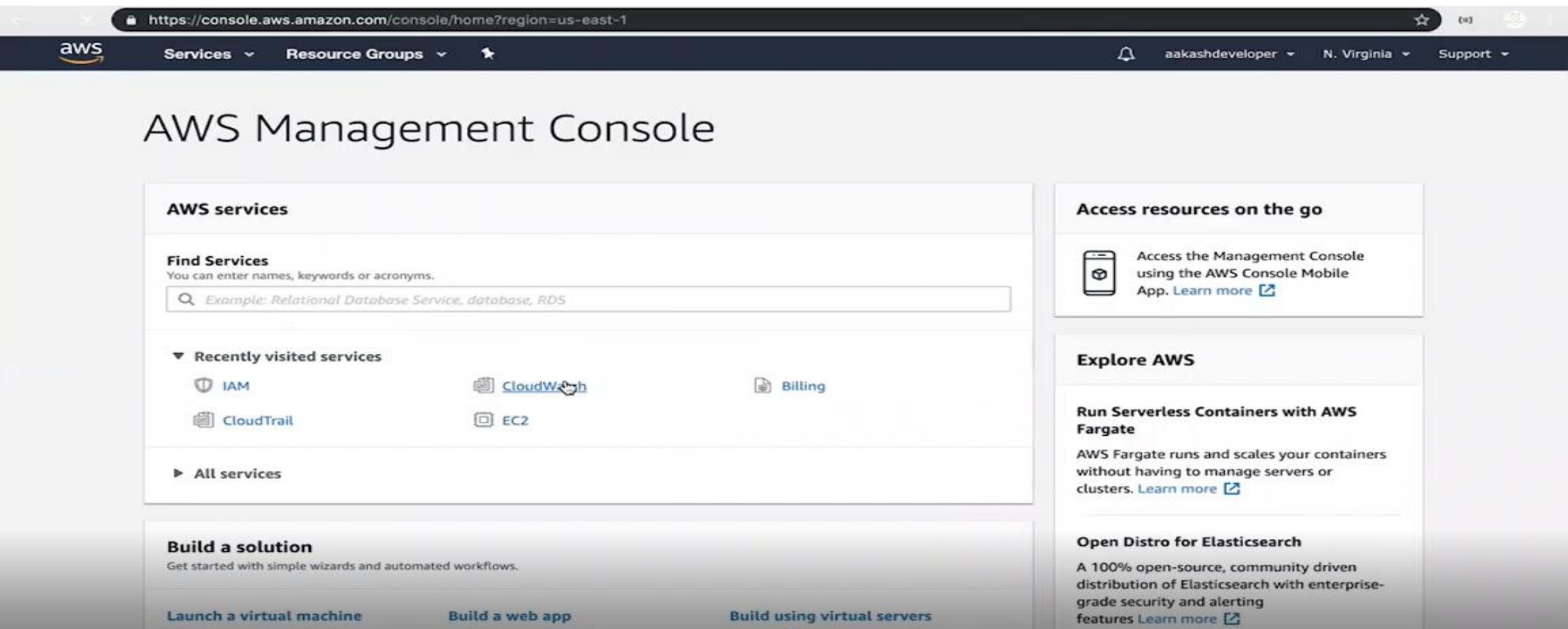
## What's new?

**Announcing AWS Batch**  
Now generally available, AWS Batch enables developers, scientists, and engineers to process large-scale batch jobs with ease. [Learn more](#)

**Announcing Amazon Lightsail**  
See how this new service allows you to launch and manage your



# How AWS manage three identification stage



- Monitoring Data: AWS console having a service name Cloud watch
- Cloud watch : It keep tracking every instance of an assigned task.



# AWS: Cloud Watch

https://console.aws.amazon.com/cloudwatch/home?region=us-east-1

aws Services Resource Groups

CloudWatch: Overview

Time range 1h 3h 12h 1d 3d 1w custom Actions

All resources

### Alarms by AWS service

Services	Status	Alarm	Insufficient	OK
Classic ELB	-	-	-	
EC2	-	-	-	
Elastic Beanstalk	-	-	-	
Elastic Block Store	-	-	-	
RDS	-	-	-	
Route 53	-	-	-	
S3	-	-	-	

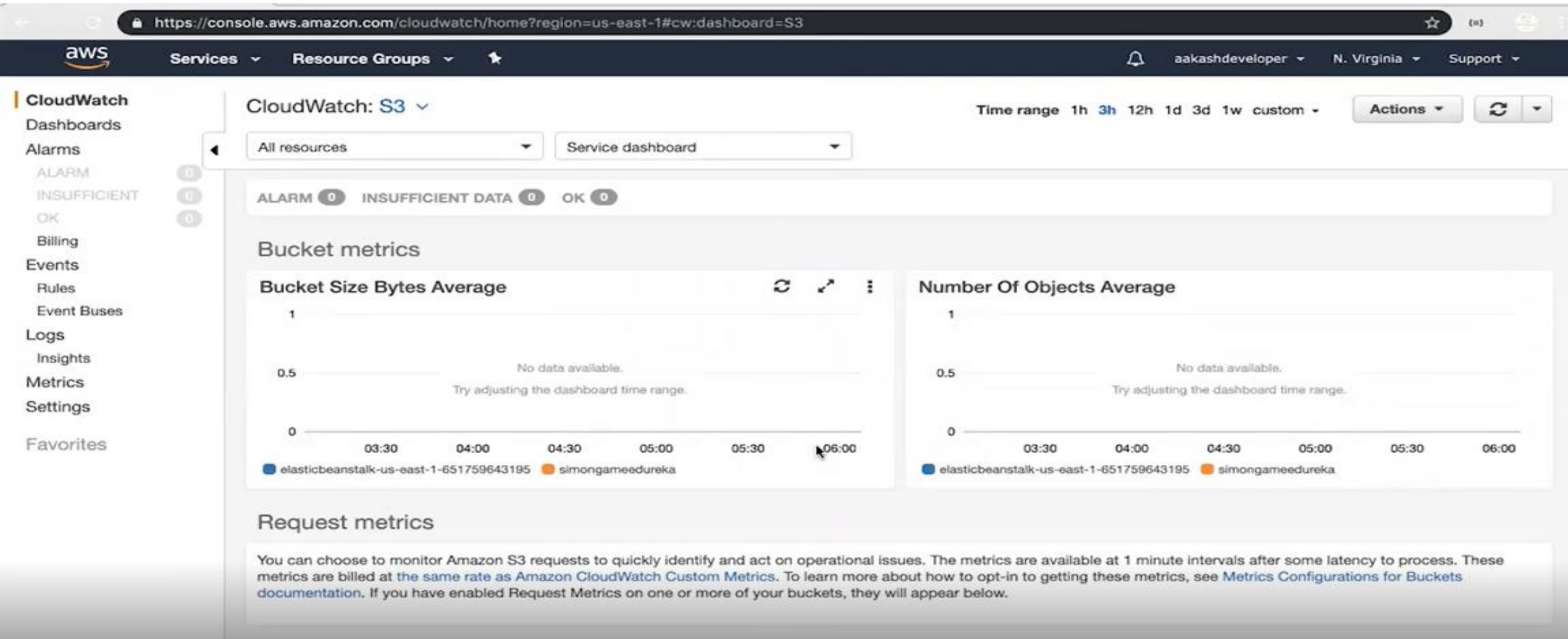
### Recent alarms

Recent alarms will appear here.  
[Learn more about CloudWatch Alarms.](#)

### Cross service dashboard

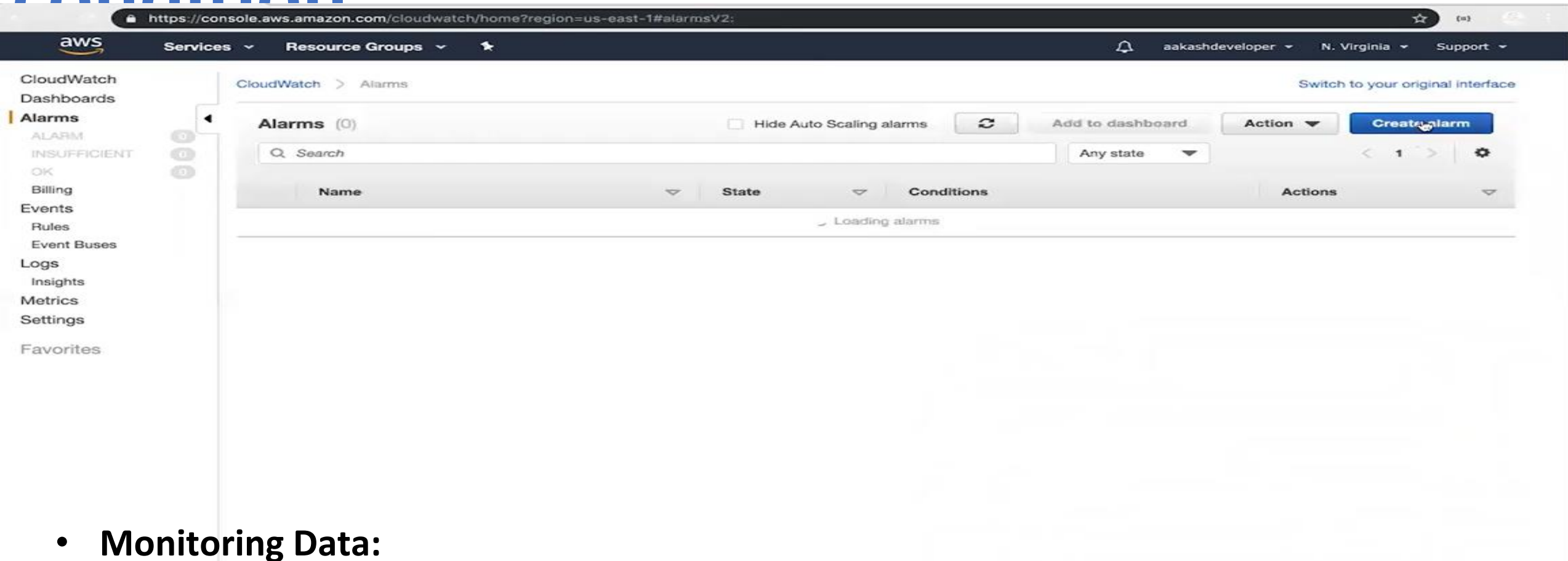
The cross service dashboard aggregates key metrics from each of the services in your account. [View cross service dashboard](#)

# AWS: Cloud Watch for bucket



- **Monitoring Data:**  
Shows how many user using that and what is size of memory used. by graphical manner or logs

# AWS: Cloud Watch for setting alarm condition







- **Monitoring Data:**  
Here there is option for setting alarm when define situation occur.

# AWS: Cloud Watch for setting alarm condition metric

https://console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create

Select metric

Untitled graph 



1h 3h 12h 1d 3d 1w custom  Line  

Your CloudWatch graph is empty.  
Select some metrics to appear here.

03:15 03:30 03:45 04:00 04:15 04:30 04:45 05:00 05:15 05:30 05:45 06:00

\*\*\*

All metrics Graphed metrics Graph options Source

All > S3 > Storage Metrics  Search for any metric, dimension or resource id 

<input type="checkbox"/>	BucketName (6)	StorageType	Metric Name
<input type="checkbox"/>	elasticbeanstalk-us-east-1-651759643195	AllStorageTypes	NumberOfObjects
<input type="checkbox"/>	elasticbeanstalk-us-east-1-651759643195 ▾	StandardStorage ▾	BucketSizeBytes ▾
<input type="checkbox"/>	simongameedureka	AllStorageTypes	NumberOfObjects
<input type="checkbox"/>	simongameedureka	StandardStorage	BucketSizeBytes
<input type="checkbox"/>	testwebsites312	AllStorageTypes	NumberOfObjects
<input type="checkbox"/>	testwebsites312	StandardStorage	BucketSizeBytes

Cancel Select metric

# Thread Identification in Cloud Computing

Once you get to know something wrong is going on , you would want to know when and where.



- **Gaining Visibility:**  
Here there is option for get detail of service which perform wrong option .

# AWS Cloud Trail

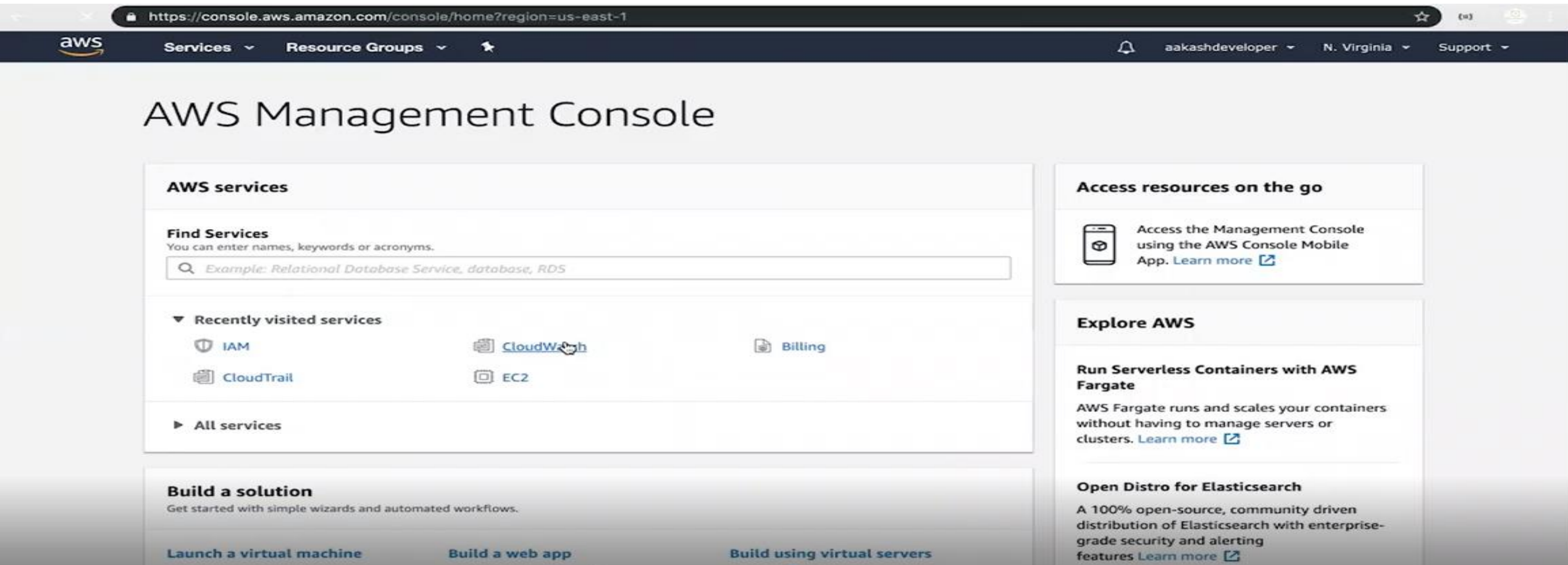


AWS CloudTrail

- CloudTrail is a logging service which can be used to log the history of API calls.
- It can also be used to identify which user from AWS Management Console requested the particular service.
- Taking reference from our example, this is the tool from where you will identify the notorious “hacker”.

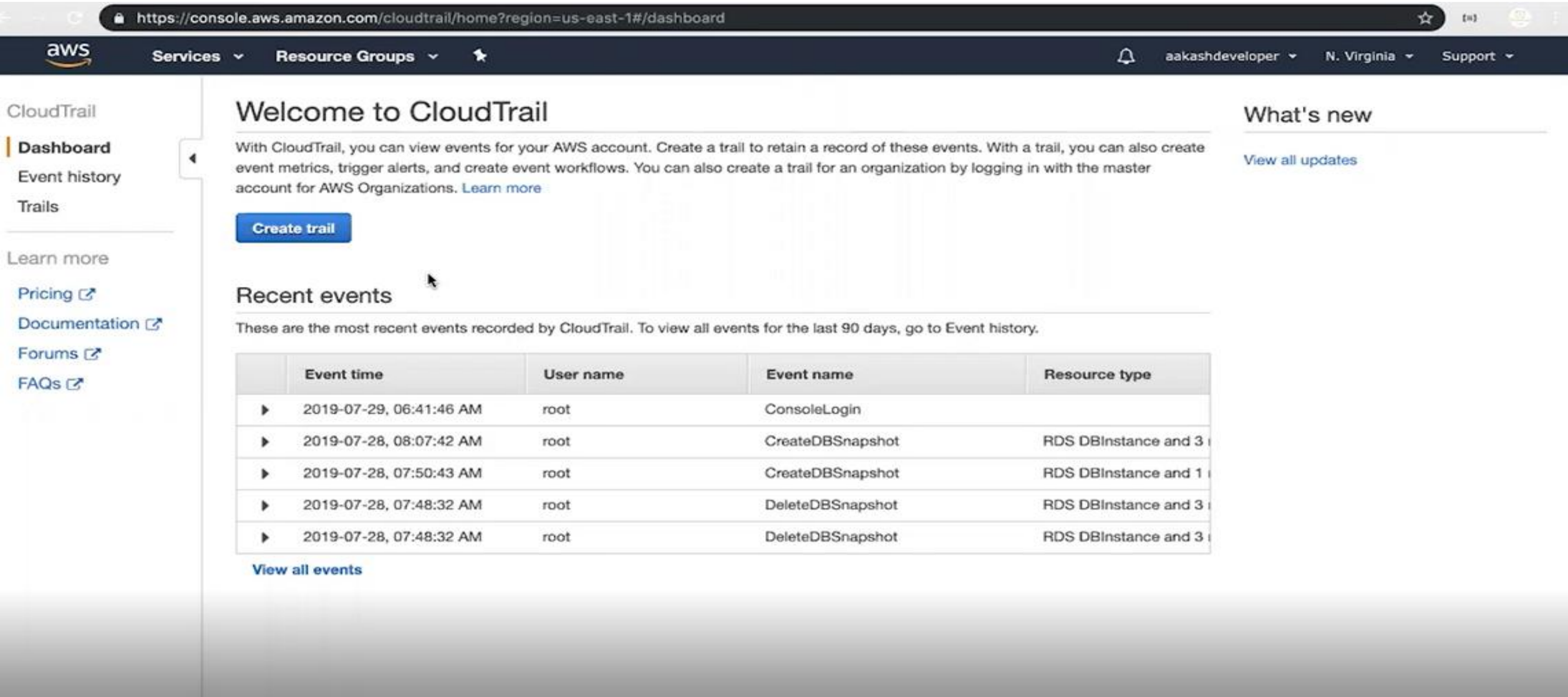


# AWS: Gaining Visibility



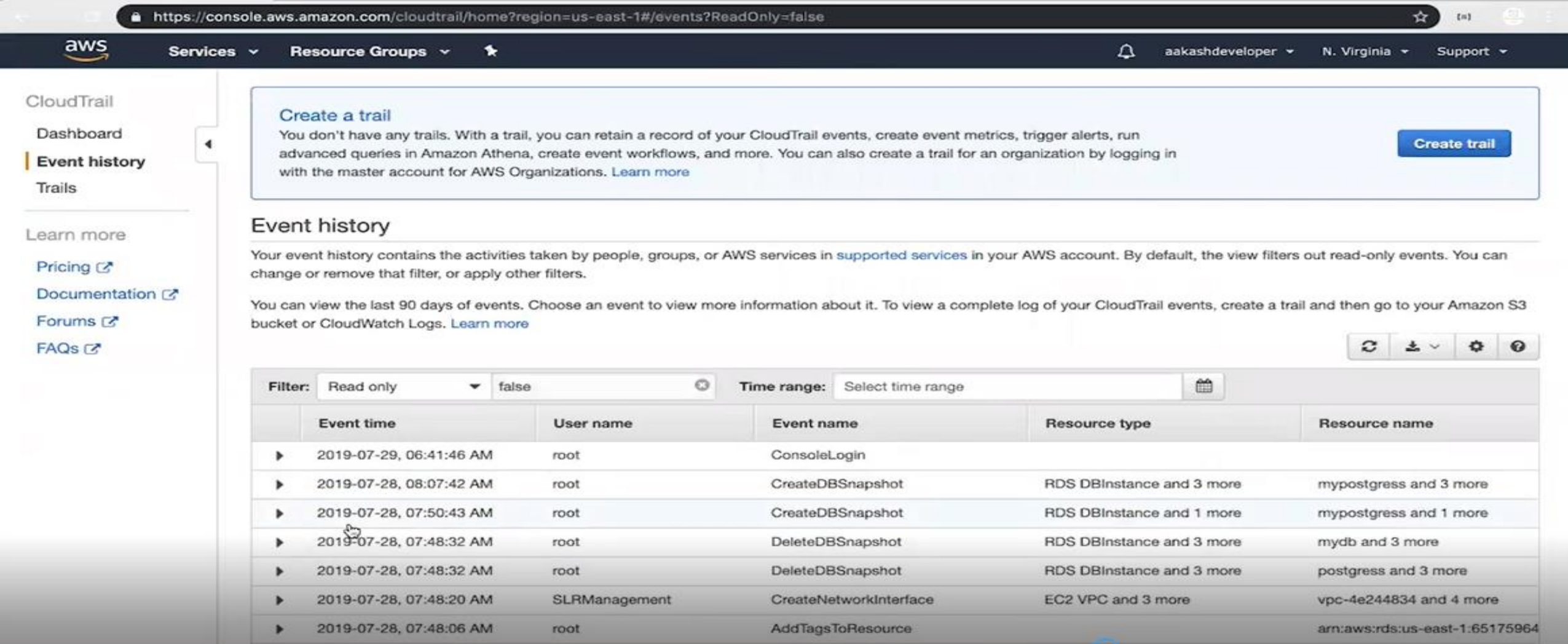
- Gaining Visibility: AWS provide Cloud Trail service to get detail

# AWS: Cloud Trail for Gaining Visibility





# AWS: Cloud Trail for Gaining Visibility



The screenshot displays the AWS CloudTrail console interface. At the top, the navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information for 'aakashdeveloper' in 'N. Virginia'. The left sidebar shows 'CloudTrail' with options for 'Dashboard', 'Event history' (selected), and 'Trails'. The main content area features a 'Create a trail' section with a 'Create trail' button. Below this is the 'Event history' section, which includes a descriptive paragraph and a table of events. The table has columns for 'Event time', 'User name', 'Event name', 'Resource type', and 'Resource name'. The events listed are from July 28 and 29, 2019, showing actions like 'ConsoleLogin', 'CreateDBSnapshot', 'DeleteDBSnapshot', 'CreateNetworkInterface', and 'AddTagsToResource'.

**Create a trail**  
You don't have any trails. With a trail, you can retain a record of your CloudTrail events, create event metrics, trigger alerts, run advanced queries in Amazon Athena, create event workflows, and more. You can also create a trail for an organization by logging in with the master account for AWS Organizations. [Learn more](#) [Create trail](#)

### Event history

Your event history contains the activities taken by people, groups, or AWS services in [supported services](#) in your AWS account. By default, the view filters out read-only events. You can change or remove that filter, or apply other filters.

You can view the last 90 days of events. Choose an event to view more information about it. To view a complete log of your CloudTrail events, create a trail and then go to your Amazon S3 bucket or CloudWatch Logs. [Learn more](#)

Filter: Read only false Time range: Select time range

	Event time	User name	Event name	Resource type	Resource name
▶	2019-07-29, 06:41:46 AM	root	ConsoleLogin		
▶	2019-07-28, 08:07:42 AM	root	CreateDBSnapshot	RDS DBInstance and 3 more	mypostgress and 3 more
▶	2019-07-28, 07:50:43 AM	root	CreateDBSnapshot	RDS DBInstance and 1 more	mypostgress and 1 more
▶	2019-07-28, 07:48:32 AM	root	DeleteDBSnapshot	RDS DBInstance and 3 more	myddb and 3 more
▶	2019-07-28, 07:48:32 AM	root	DeleteDBSnapshot	RDS DBInstance and 3 more	postgres and 3 more
▶	2019-07-28, 07:48:20 AM	SLRManagement	CreateNetworkInterface	EC2 VPC and 3 more	vpc-4e244834 and 4 more
▶	2019-07-28, 07:48:06 AM	root	AddTagsToResource		arn:aws:rds:us-east-1:65175964

- It keep record of all service for last 90 days even those service which is deleted in system.

# AWS: Cloud Trail for Gaining Visibility

https://console.aws.amazon.com/cloudtrail/home?region=us-east-1#/configuration/new?ReadOnly=false

aws Services Resource Groups

CloudTrail

- Dashboard
- Event history
- Trails

Learn more

- Pricing
- Documentation
- Forums
- FAQs

**Creating a trail might incur charges. For more information, see [AWS CloudTrail Pricing](#).**

## Create Trail

Trail name\*

Apply trail to all regions ☒ Yes ☐ No  
Creates the same trail in all regions and delivers log files for all regions.

### Management events

Management events provide insights into the management operations that are performed on resources in your AWS account. [Learn more](#)

Read/Write events ☒ All ☐ Read-only ☐ Write-only ☐ None ⓘ

### Data events

Data events provide insights into the resource operations performed on or within a resource. Additional [charges](#) apply. [Learn more](#)

**S3** **Lambda**

You can record S3 object-level API activity (for example, GetObject and PutObject) for individual buckets, or for all current and future buckets in your AWS account. Additional [charges](#) apply. [Learn more](#)

Showing 0 of 0 resources			
Bucket name	Prefix	Read	Write
<input type="checkbox"/> Select all S3 buckets in your account ⓘ			
		<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Write

No resources found

# AWS: Cloud Trail for Gaining Visibility

aws

Services ▾ Resource Groups ▾

🔔

aakashdeveloper ▾

N. Virginia ▾

Support ▾

CloudTrail

Dashboard

Event history

Trails

Learn more

Pricing ↗

Documentation ↗

Forums ↗

FAQs ↗

https://console.aws.amazon.com/cloudtrail/home?region=us-east-1#/configuration/new?ReadOnly=false

☆ [n]

Data events provide insights into the resource operations performed on or within a resource. Additional [charges](#) apply. [Learn more](#)

S3

Lambda

You can record S3 object-level API activity (for example, GetObject and PutObject) for individual buckets, or for all current and future buckets in your AWS account. Additional [charges](#) apply. [Learn more](#)

Showing 1 of 1 resources

Bucket name ▾	Prefix ▾	Read ▾	Write ▾	
<input type="checkbox"/> Select all S3 buckets in your account ⓘ		<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Write	
<input type="text" value="simongameedureka"/>	<input type="text" value="/ /.mp3"/>	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Write	ⓘ

+

 Add S3 bucket

Storage location

Create a new S3 bucket ☒ Yes ☐ No

S3 bucket\*

ⓘ

▶ Advanced

\* Required field

Additional charges may apply. [Learn more](#)

Create

# Thread Identification in Cloud Computing

With managing access you will have a list of users who have access, and hence wipe the culprit out of the system.



**Managing Access :**

**Here there is option for get detail of service which used by users**

# AWS Cloud IAM

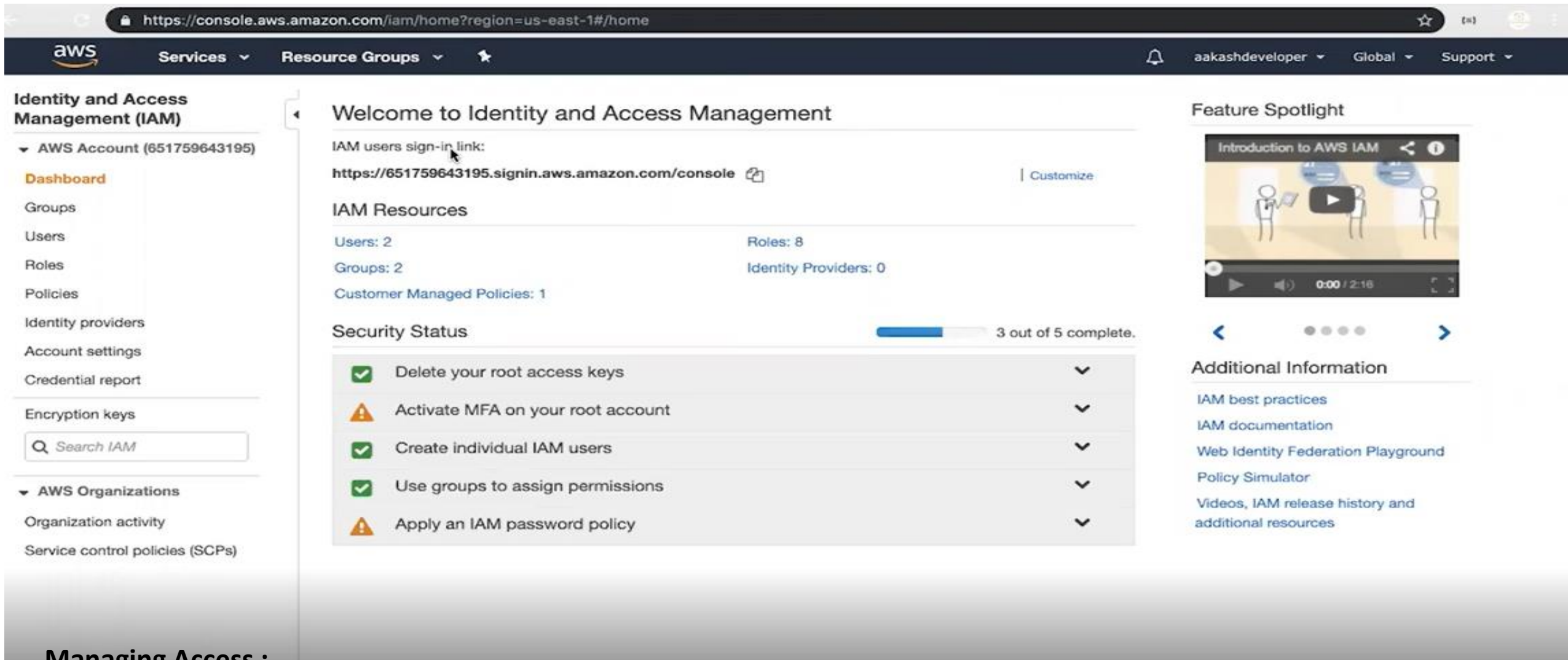


AWS IAM

- Granular permissions
- Secure access to applications running on EC2 environment
- Free to use



# AWS: Managing Access

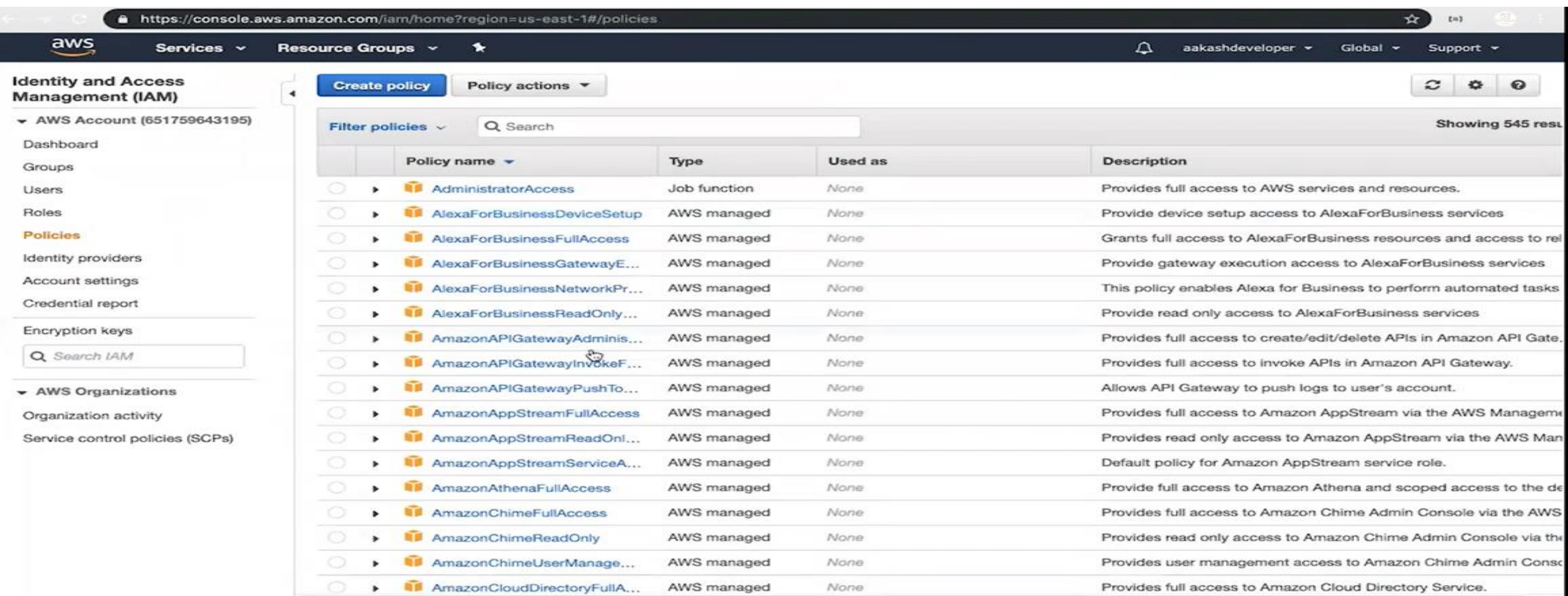


The screenshot displays the AWS IAM console interface. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information for 'aakashdeveloper'. The left sidebar lists navigation options: 'Identity and Access Management (IAM)', 'AWS Account (651759643195)', 'Dashboard', 'Groups', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Credential report', 'Encryption keys', 'AWS Organizations', 'Organization activity', and 'Service control policies (SCPs)'. The main content area is titled 'Welcome to Identity and Access Management' and provides the IAM sign-in link: <https://651759643195.signin.aws.amazon.com/console>. It also shows IAM resource counts: Users: 2, Roles: 8, Groups: 2, Identity Providers: 0, and Customer Managed Policies: 1. A 'Security Status' section indicates '3 out of 5 complete' with a progress bar and a list of tasks: 'Delete your root access keys' (checked), 'Activate MFA on your root account' (warning), 'Create individual IAM users' (checked), 'Use groups to assign permissions' (checked), and 'Apply an IAM password policy' (warning). The right sidebar features a 'Feature Spotlight' video titled 'Introduction to AWS IAM' and a section for 'Additional Information' with links to IAM best practices, documentation, the Web Identity Federation Playground, the Policy Simulator, and videos/release history.

## Managing Access :

In IAM service of AWS we can create permission level for a service and this permission can be from any level from higher to lower.

# AWS: Managing Access



The screenshot displays the AWS IAM console interface. The left sidebar shows the navigation menu with 'Policies' highlighted. The main content area shows a table of policies. The table has columns for 'Policy name', 'Type', 'Used as', and 'Description'. The policies listed include 'AdministratorAccess', 'AlexaForBusinessDeviceSetup', 'AlexaForBusinessFullAccess', 'AlexaForBusinessGatewayE...', 'AlexaForBusinessNetworkPr...', 'AlexaForBusinessReadOnly...', 'AmazonAPIGatewayAdminis...', 'AmazonAPIGatewayInvokeF...', 'AmazonAPIGatewayPushTo...', 'AmazonAppStreamFullAccess', 'AmazonAppStreamReadOnl...', 'AmazonAppStreamServiceA...', 'AmazonAthenaFullAccess', 'AmazonChimeFullAccess', 'AmazonChimeReadOnly', 'AmazonChimeUserManage...', and 'AmazonCloudDirectoryFullA...'. Each policy has a radio button in the first column and a right-pointing arrow in the second column.

		Policy name	Type	Used as	Description
<input type="radio"/>	▶	AdministratorAccess	Job function	None	Provides full access to AWS services and resources.
<input type="radio"/>	▶	AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaForBusiness services
<input type="radio"/>	▶	AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resources and access to rel
<input type="radio"/>	▶	AlexaForBusinessGatewayE...	AWS managed	None	Provide gateway execution access to AlexaForBusiness services
<input type="radio"/>	▶	AlexaForBusinessNetworkPr...	AWS managed	None	This policy enables Alexa for Business to perform automated tasks
<input type="radio"/>	▶	AlexaForBusinessReadOnly...	AWS managed	None	Provide read only access to AlexaForBusiness services
<input type="radio"/>	▶	AmazonAPIGatewayAdminis...	AWS managed	None	Provides full access to create/edit/delete APIs in Amazon API Gate.
<input type="radio"/>	▶	AmazonAPIGatewayInvokeF...	AWS managed	None	Provides full access to invoke APIs in Amazon API Gateway.
<input type="radio"/>	▶	AmazonAPIGatewayPushTo...	AWS managed	None	Allows API Gateway to push logs to user's account.
<input type="radio"/>	▶	AmazonAppStreamFullAccess	AWS managed	None	Provides full access to Amazon AppStream via the AWS Managemen
<input type="radio"/>	▶	AmazonAppStreamReadOnl...	AWS managed	None	Provides read only access to Amazon AppStream via the AWS Man
<input type="radio"/>	▶	AmazonAppStreamServiceA...	AWS managed	None	Default policy for Amazon AppStream service role.
<input type="radio"/>	▶	AmazonAthenaFullAccess	AWS managed	None	Provide full access to Amazon Athena and scoped access to the de
<input type="radio"/>	▶	AmazonChimeFullAccess	AWS managed	None	Provides full access to Amazon Chime Admin Console via the AWS
<input type="radio"/>	▶	AmazonChimeReadOnly	AWS managed	None	Provides read only access to Amazon Chime Admin Console via the
<input type="radio"/>	▶	AmazonChimeUserManage...	AWS managed	None	Provides user management access to Amazon Chime Admin Consc
<input type="radio"/>	▶	AmazonCloudDirectoryFullA...	AWS managed	None	Provides full access to Amazon Cloud Directory Service.

Managing Access :

In IAM service of AWS provide some predefined policy for creating permission level for a service

# AWS: Managing Access

The screenshot shows the AWS IAM console interface for creating a new policy. The browser address bar displays the URL: `https://console.aws.amazon.com/iam/home?region=us-east-1#/policies$new?step=edit`. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information for 'aakashdeveloper'. The main heading is 'Create policy', with step indicators '1' and '2'. A descriptive text states: 'A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)'. Below this, there are two tabs: 'Visual editor' (selected) and 'JSON'. A link 'Import managed policy' is on the right. Under the 'Visual editor' tab, there are links for 'Expand all' and 'Collapse all'. A dropdown menu 'Select a service' is visible, with 'Clone' and 'Remove' links. The main content area contains four sections: 'Service' with a 'Choose a service' link, 'Actions' with the instruction 'Choose a service before defining actions', 'Resources' with 'Choose actions before applying resources', and 'Request conditions' with 'Choose actions before specifying conditions'. At the bottom right, there is a link '+ Add additional permissions' and two buttons: 'Cancel' and 'Review policy'.

**Managing Access :**

**In IAM service of AWS we can create policy according to our concern or choice using visual editor or by writing JSON script**



# AWS: Managing Access

The screenshot shows the AWS IAM console interface. The left sidebar contains navigation links for Identity and Access Management (IAM), including AWS Account, Dashboard, Groups, Users, Roles (highlighted), Policies, Identity providers, Account settings, Credential report, Encryption keys, AWS Organizations, Organization activity, and Service control policies (SCPs). The main content area displays a help page titled 'What are IAM roles?'. It explains that IAM roles are a secure way to grant permissions to entities that you trust, with examples including IAM users in other accounts, application code on EC2 instances, AWS services, and users from corporate directories. It also mentions that IAM roles issue keys with short durations for enhanced security. Below the text are links for 'Additional resources' such as IAM Roles FAQ, IAM Roles Documentation, a tutorial on cross-account access, and common scenarios for roles. At the bottom of the main area are 'Create role' and 'Delete role' buttons. Below these is a table showing existing roles, with a search bar and 'Showing 8 results' indicator. The table has columns for Role name, Description, and Trusted entities.

**What are IAM roles?**

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

**Additional resources:**

- [IAM Roles FAQ](#)
- [IAM Roles Documentation](#)
- [Tutorial: Setting Up Cross Account Access](#)
- [Common Scenarios for Roles](#)

[Create role](#) [Delete role](#)

Search Showing 8 results

Role name	Description	Trusted entities
<input type="checkbox"/> <a href="#">aws-elasticbeanstalk-ec2-role</a>		AWS service: ec2
<input type="checkbox"/> <a href="#">aws-elasticbeanstalk-service-role</a>		AWS service: elasticbeanstalk

## Managing Access :

In IAM service of AWS you want that your application should be accessible by Facebook or by Google, then for that we can create a role for application.

# AWS: Managing Access

The screenshot shows the AWS IAM console interface for creating a new role. The browser address bar displays the URL: `https://console.aws.amazon.com/iam/home?region=us-east-1#/roles$new?step=type&roleType=wip`. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information 'aakashdeveloper'. The main heading is 'Create role', with a progress indicator showing four steps, where the first step is active. Below the heading, the section 'Select type of trusted entity' presents four options: 'AWS service' (EC2, Lambda and others), 'Another AWS account' (Belonging to you or 3rd party), 'Web identity' (Cognito or any OpenID provider), and 'SAML 2.0 federation' (Your corporate directory). The 'Web identity' option is highlighted with a blue border. A descriptive text below states: 'Allows users federated by the specified external web identity or OpenID Connect (OIDC) provider to assume this role to perform actions in your account. [Learn more](#)'. The next section, 'Choose a web identity provider', contains a form with 'Identity provider' set to 'Facebook', a 'Create new provider' link, a 'Refresh' button, 'Application ID\*' set to 'uhuugu', and a 'Condition' section with an 'Add condition (optional)' link.

## Managing Access :

In IAM service of AWS you want that your application should accesable by Facebook or by google then for that we can create a role for application.