Introduction to IAM and CloudWatch

Agenda

1. Why Access Management ?
2. IAM Features and MFA
3. IAM Policies
4. IAM Permissions and Roles
5. Introduction to CloudWatch
6. AWS STS
7. Metrics and Namespaces
8. Dashboard and CloudWatch Alarms
9. CloudWatch Logs
10. IAM Policy Simulator
11. AWS Access Analyzer
12. CloudTrail and Config

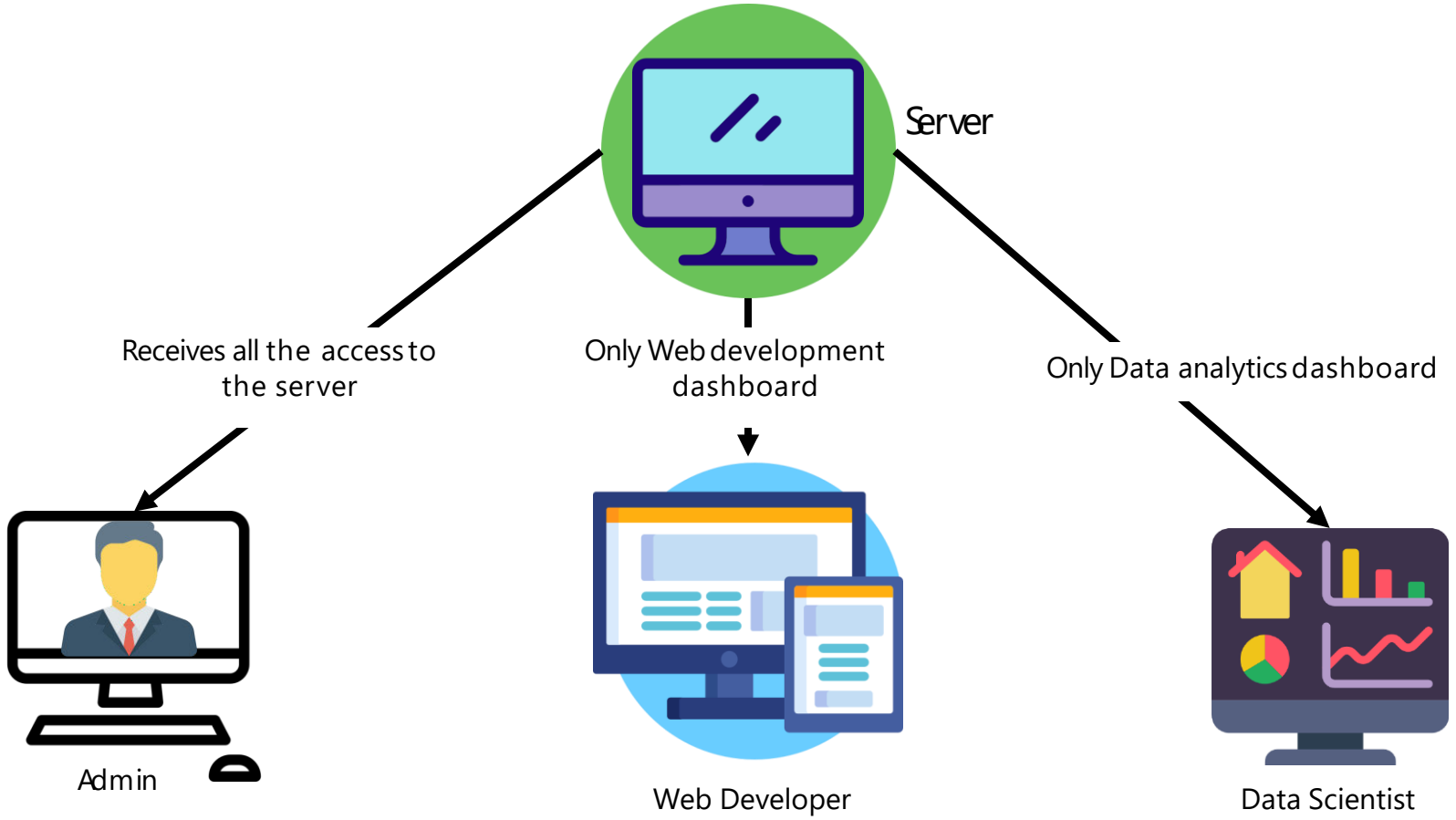
Introduction to IAM

Introduction to IAM

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources.

You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

Introduction to IAM



Amazon Resource Name

Amazon Resource Name

Amazon Resource Names uniquely identify AWS resources. Every resource in AWS is provided with an ARN.

ARN Format:

arn:partition:service:region:account-id:resource

arn:partition:service:region:account-id:resourcetype/resource

arn:partition:service:region:account-id:resourcetype:resource

Amazon Resource Name

- EC2
  - ***Instance*** > arn:aws:ec2:region:account-id:instance/instance-id
  - ***AMI*** > arn:aws:ec2:region::image/image-id
  - ***Key-pair*** > arn:aws:ec2:region:account-id:key-pair/key-pair-name
  - ***N/W Interface*** > arn:aws:ec2:region:account-id:network-interface/eni-id
- EBS
  - ***Volume*** > arn:aws:ec2:region:account-id:volume/volume-id
  - ***Snapshot*** > arn:aws:ec2:region:account-id:snapshot/snapshot-id

Amazon Resource Name

VPC > arn:aws:ec2:region:account-id:vpc/vpc-id

Route Table > arn:aws:ec2:region:account-id:route-table/route-table-id

SG > arn:aws:ec2:region:account-id:security-group/security-group-id

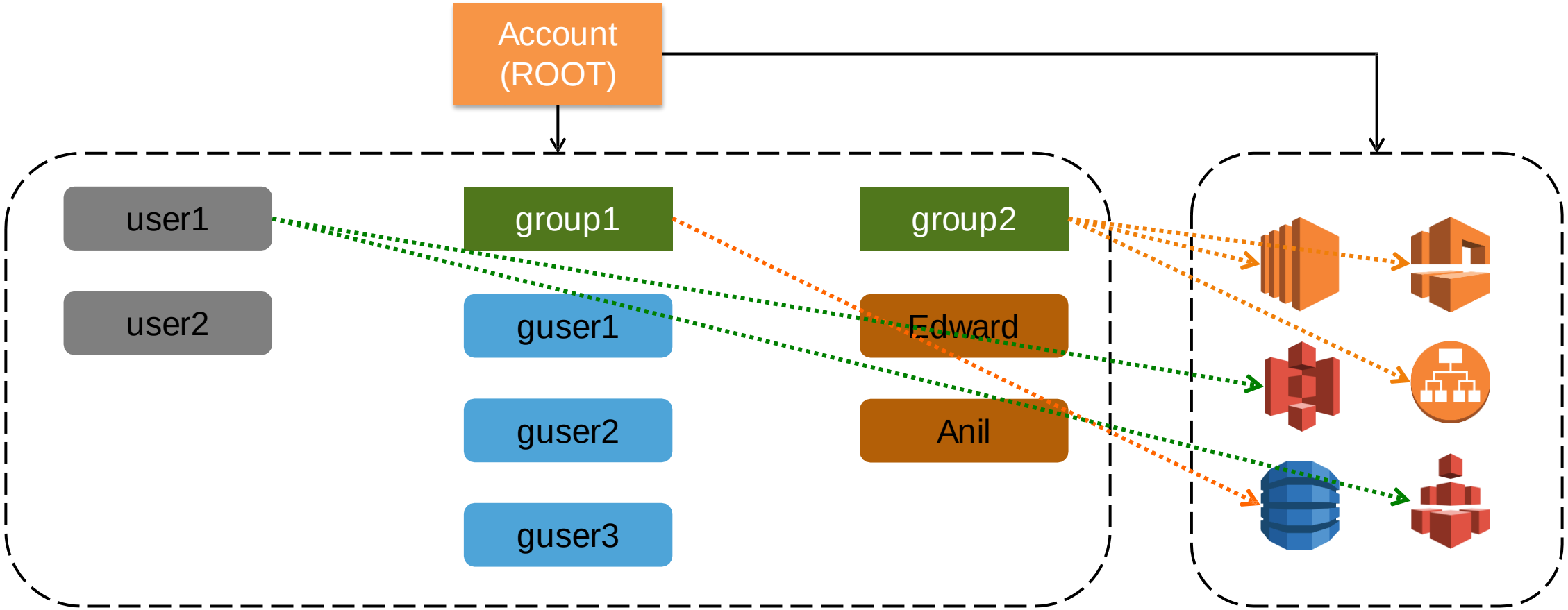
NACL > arn:aws:ec2:region:account-id:network-acl/nacl-id

IGW > arn:aws:ec2:region:account-id:internet-gateway/igw-id

Subnet > arn:aws:ec2:region:account-id:subnet/subnet-id

Peering > arn:aws:ec2:region:account-id:vpc-peering-connection/peering-id

IAM Hierarchy

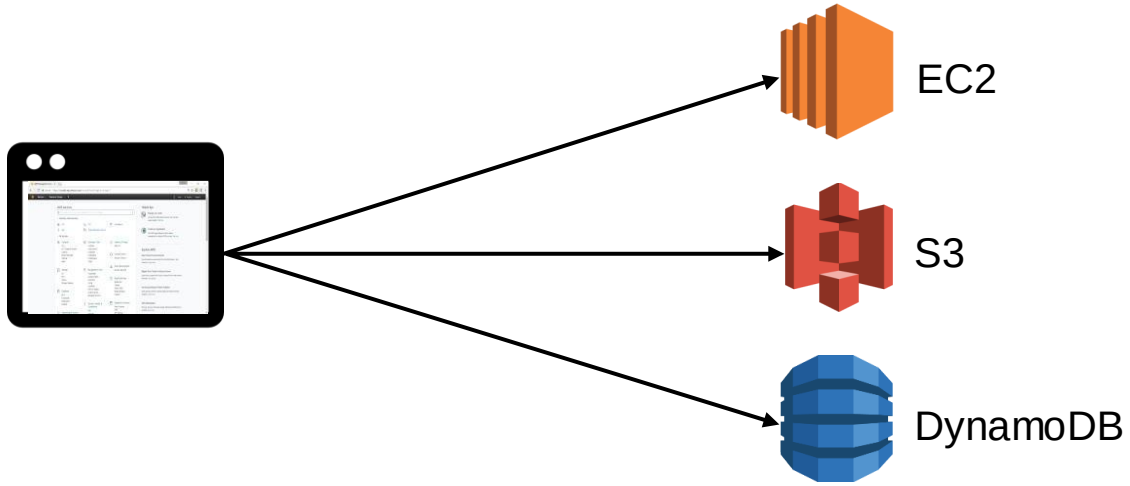


IAM Features

IAM Features

IAM Users

- Represents an entity that is created in AWS, can be a person or service.
- No permissions by default. Nothing is allowed.
- Access requirement
  - Programmatic Access: User needs to make API calls from programs or uses CLI to access AWS resources.
  - Management Console Access: User needs to access AWS resources from management console.

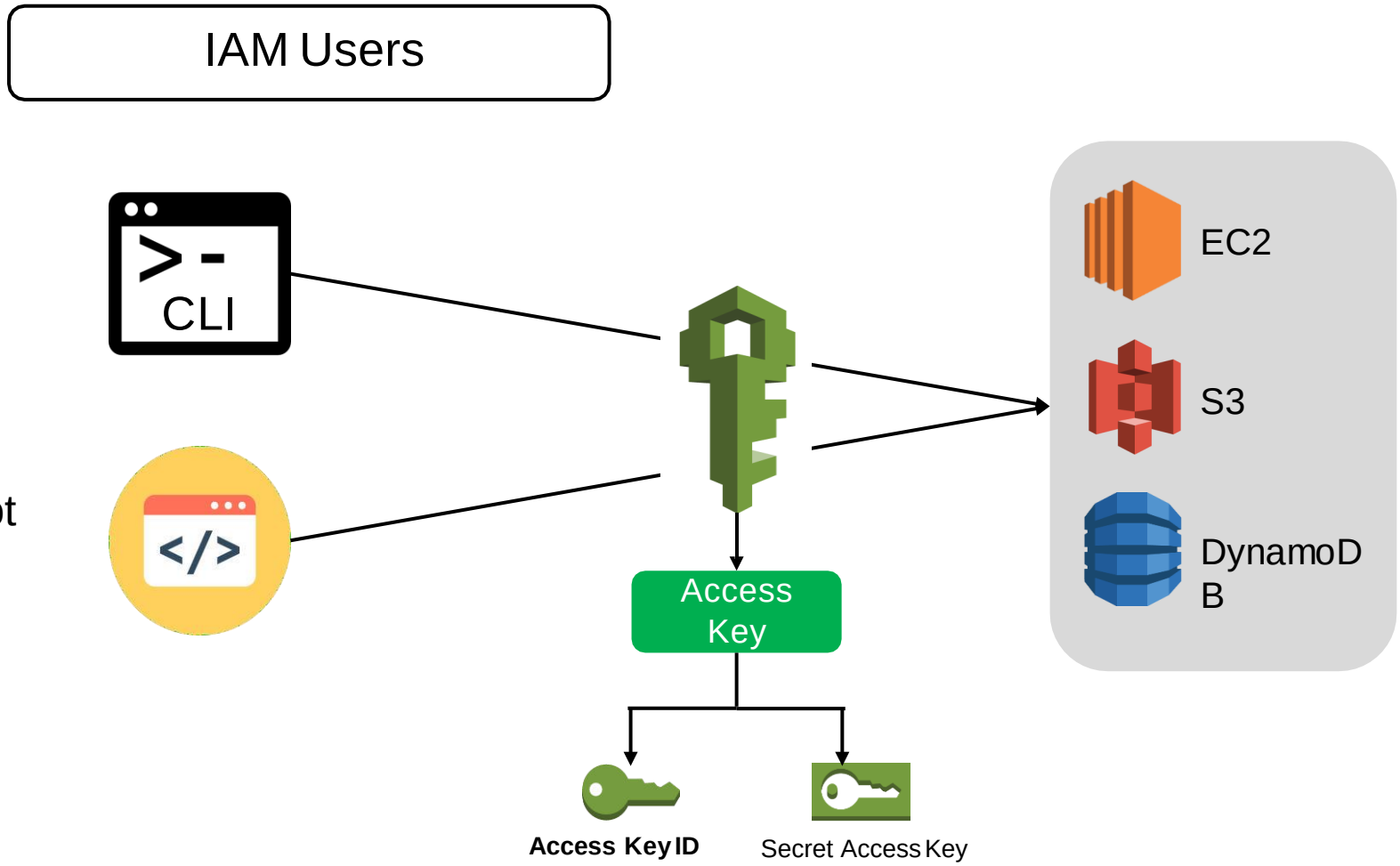


IAM Features

Access Keys

Max 2 ACTIVE access keys at a time.

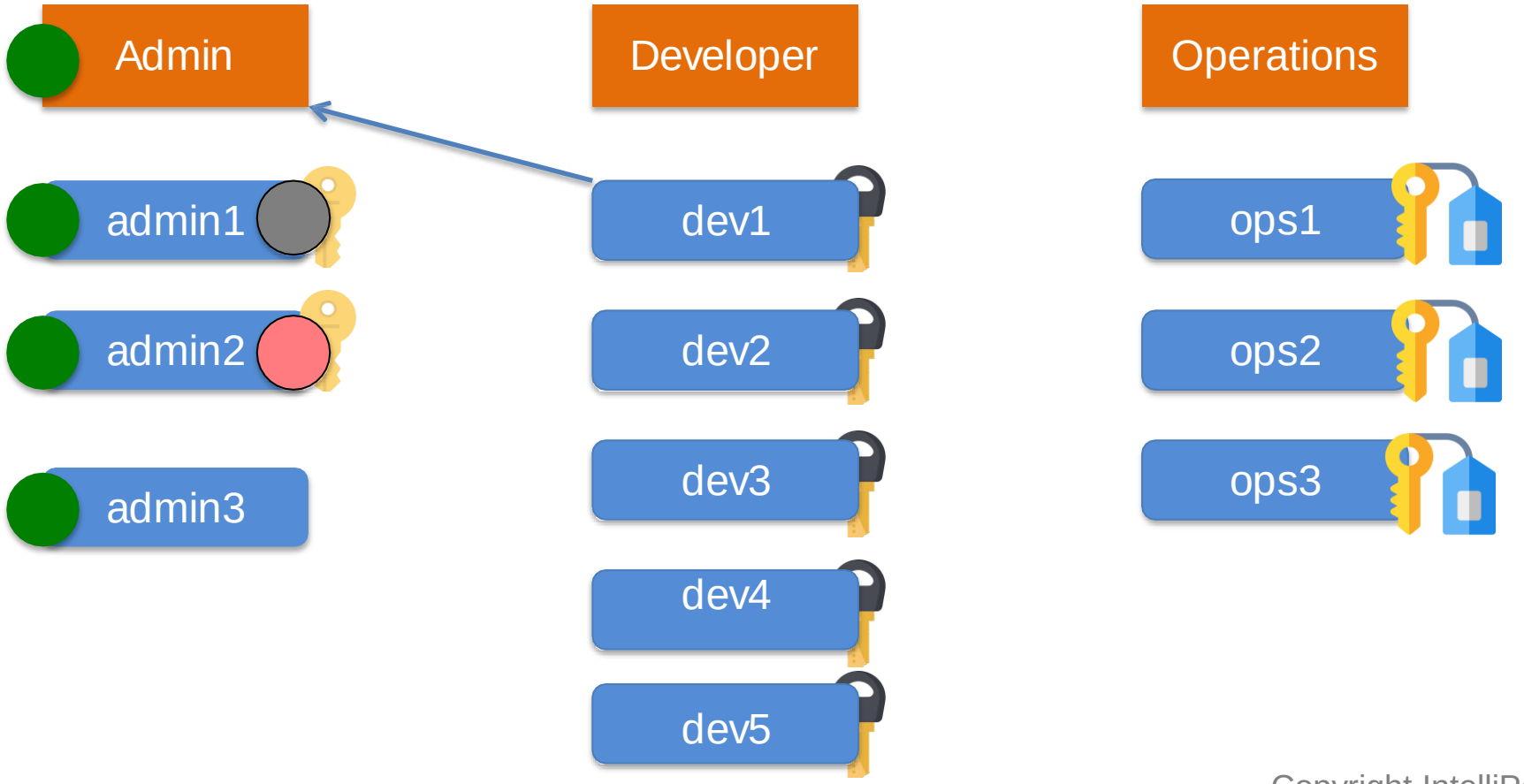
When disabled access keys cannot be used to make CLI or API calls.



IAM Features

IAM Groups

- Groups are collection of IAM users.



IAM Features

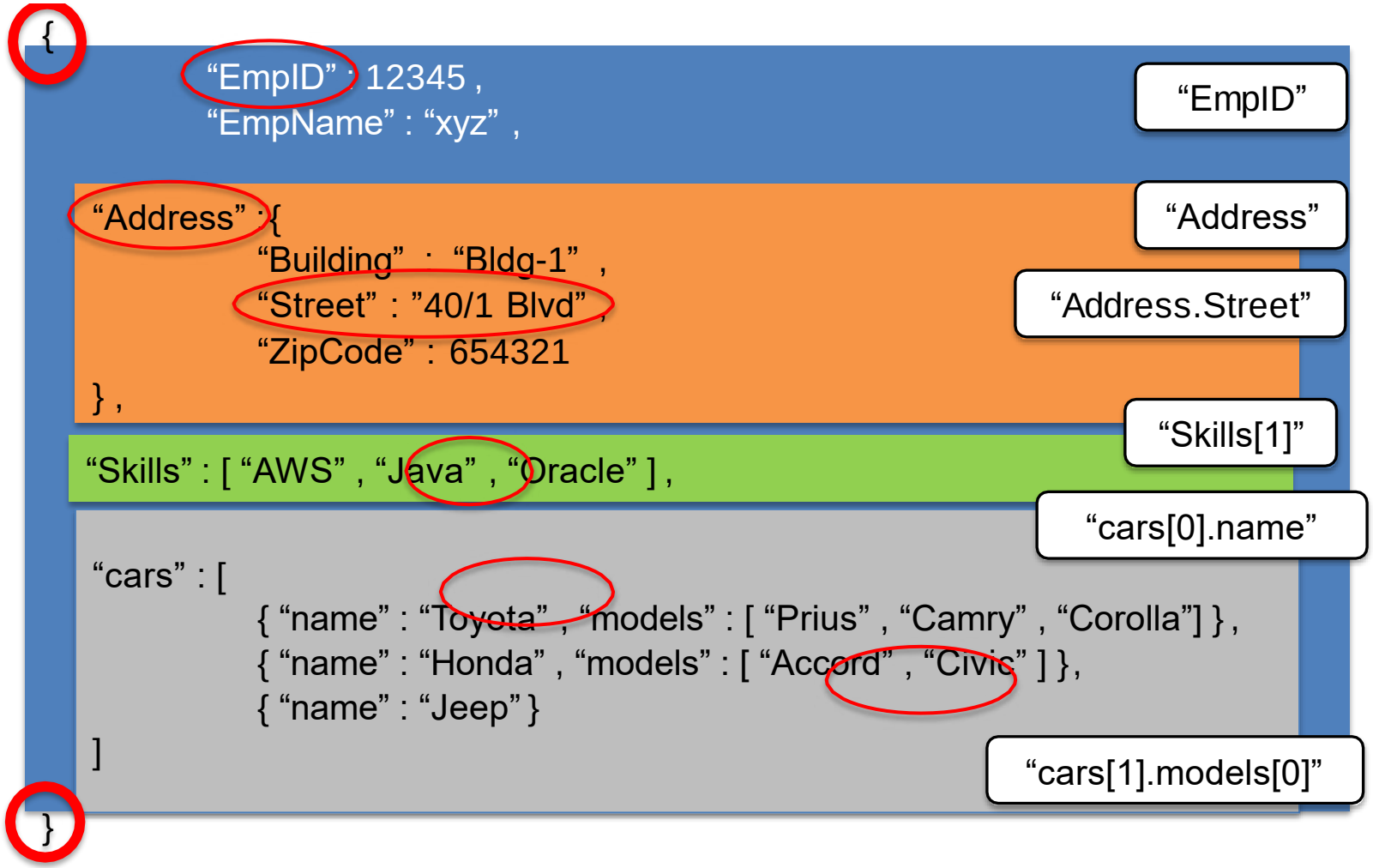
Multi-Factor Authentication

Security Token Based

SMS Based

JSON

Introduction to JSON – Java Script Object Notation



JSON

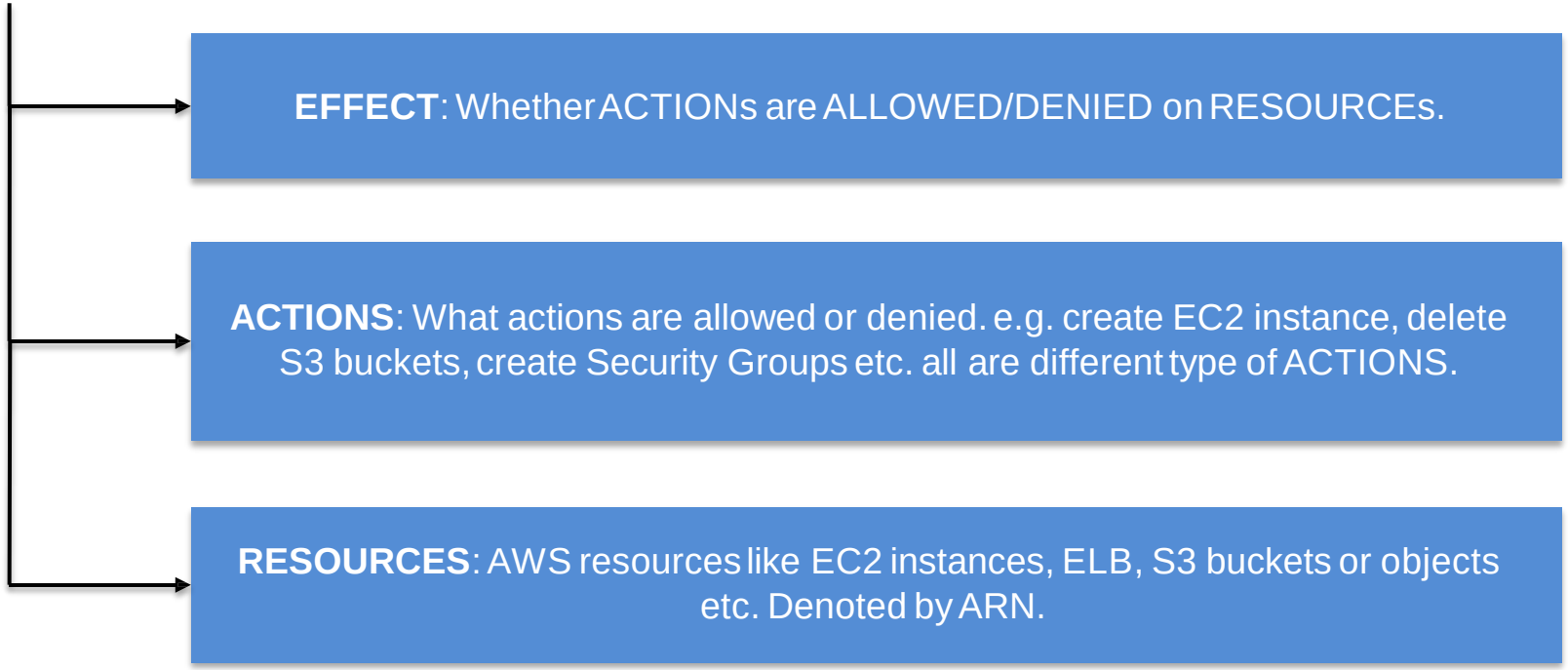
Previous Record

```
{
        "EmpID" : 12345 ,
        "EmpName" : "xyz" ,
        "Address" : {
                "Building" : "Bldg-1" ,
                "Street" : "40/1 Blvd" ,
                "ZipCode" : 654321 ,
        } ,
        "Skills" : [ "AWS" , "Java" , "Oracle" ] ,
        "cars" : [
                { "name" : "Toyota" , "models" : [ "Prius" , "Camry" , "Corolla"] } ,
                { "name" : "Honda" , "models" : [ "Accord" , "Civic" ] } ,
                { "name" : "Jeep" }
        ]
}
```

IAM Policies

IAM Policies

- Policies are JSON documents which mention what an user or group can do on AWS resources. It defines the Authorization paradigm for AWS resources.
- Contains 3 components at the least (EAR):



- Policies can be attached to Users or Groups.

IAM Policies

- Resource based policies: when policies are attached to resources.

PRINCIPAL: An entity that can take action on an AWS Resource.

Group

Effect, Action,
Resource : “S3”

S
3

Effect, Action,
Resource : “S3”
Principal : “user-1”

IAM Policies

Policy with a single statement

```
{
 "Version" : "2012-10-17" ,

"Statement " : [
 {   "Effect" : "Allow" ,
     "Action " : "s3:ListBucket" ,
     "Resource" : "arn:aws:s3:::aws-foundation-bucket"
 }
 ]
}
```

Version →
2012-10-17, current version.
2008-10-17, previous version.

IAM Policies

IAM Policies

"Statement" : [{ } , { } , { }]

- Sid : Statement ID.
- Effect : Allow/Deny.
- Principal : ARN of AWS user, account or service which is allowed or denied access to a AWS resource.
- Action : Specific action that is allowed or denied on an AWS resource.
- Resource : ARN of the AWS resource.
- Condition : Condition when a policy is in effect.

- AWS Managed Policies.
- Customer Managed Policies.
- Inline Policies

IAM Policies

Examples

Allow users to access a specific S3 bucket (aws-foundation)

```
{
  "Version": "2012-10-17",
  "Statement": [ // Statement STARTs here
                {
                                "Effect": "Allow",
                                "Action": "s3:ListAllMyBuckets",
                                "Resource": "arn:aws:s3:::*"
                } ,
                {
                                "Effect": "Allow",
                                "Action": [
                                                "s3:ListBucket",
                                                "s3:GetBucketLocation"
                                ],
                                "Resource": "arn:aws:s3:::aws-foundation"
                },
                {
                                "Effect": "Allow",
                                "Action": [
                                                "s3:PutObject",
                                "s3:GetObject",
                                "s3:DeleteObject"
                                ] ,
                                "Resource": "arn:aws:s3:::aws-
                                foundation/*"
                }
  ] // Statement ENDs here
}
```

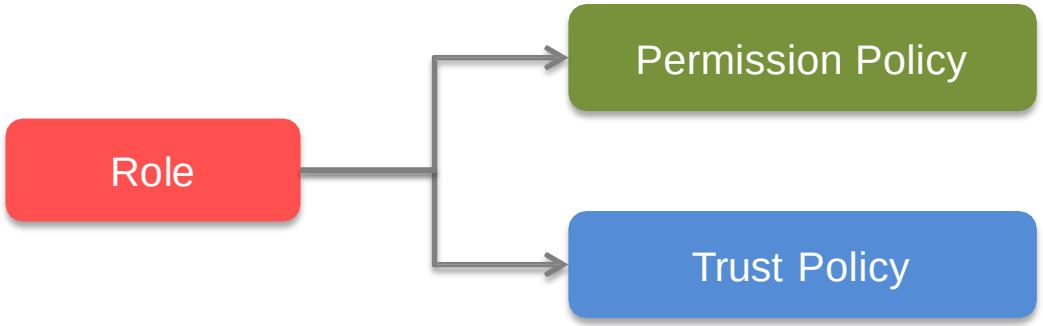
IAM Permission

IAM Permissions

- Permissions are given by attaching policies to users or groups.
- No permission by default for all IAM users.
- AWS account “root” credential.
- Use the policies defined earlier to provide access to users and groups.

IAM Permission

IAM Permissions



JSON Permission

```
{
    "Effect" : "Allow",
    "Action" : "sts:AssumeRole",
    "Principal" : "ec2.amazonaws.com"
}
```

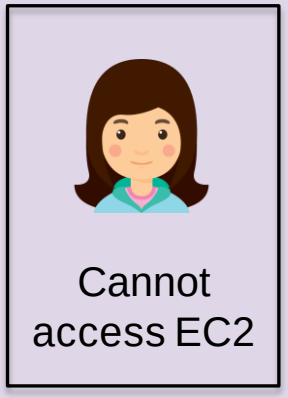
- IAM user in the same account
- IAM user in different account
- Another AWS service
- An external user

IAM Roles

IAM Roles

IAM Roles

- Role is similar to an user/group which has permissions/policies attached to it.
- Roles are temporary access given to anyone who needs to perform the specific task mentioned in the Role.



- Permissions attached to the users are taken away till the time role is getting used.

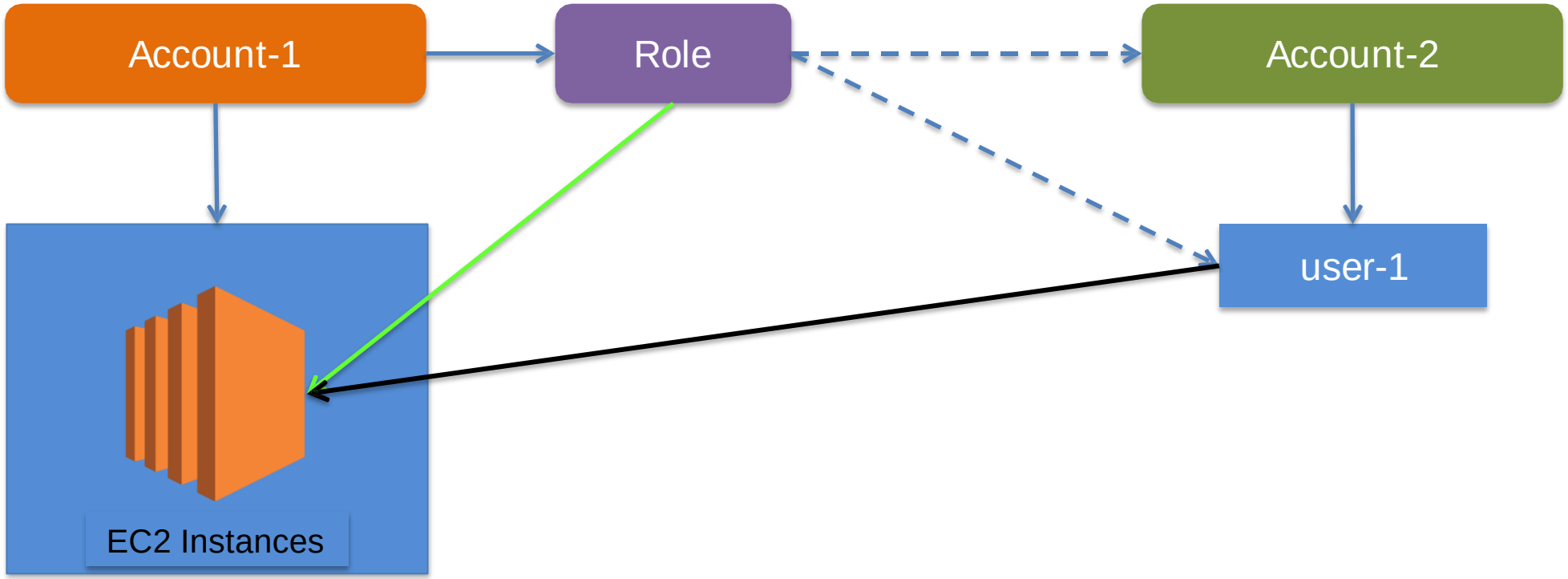
Role: Can access EC2

Role: Can access RDS

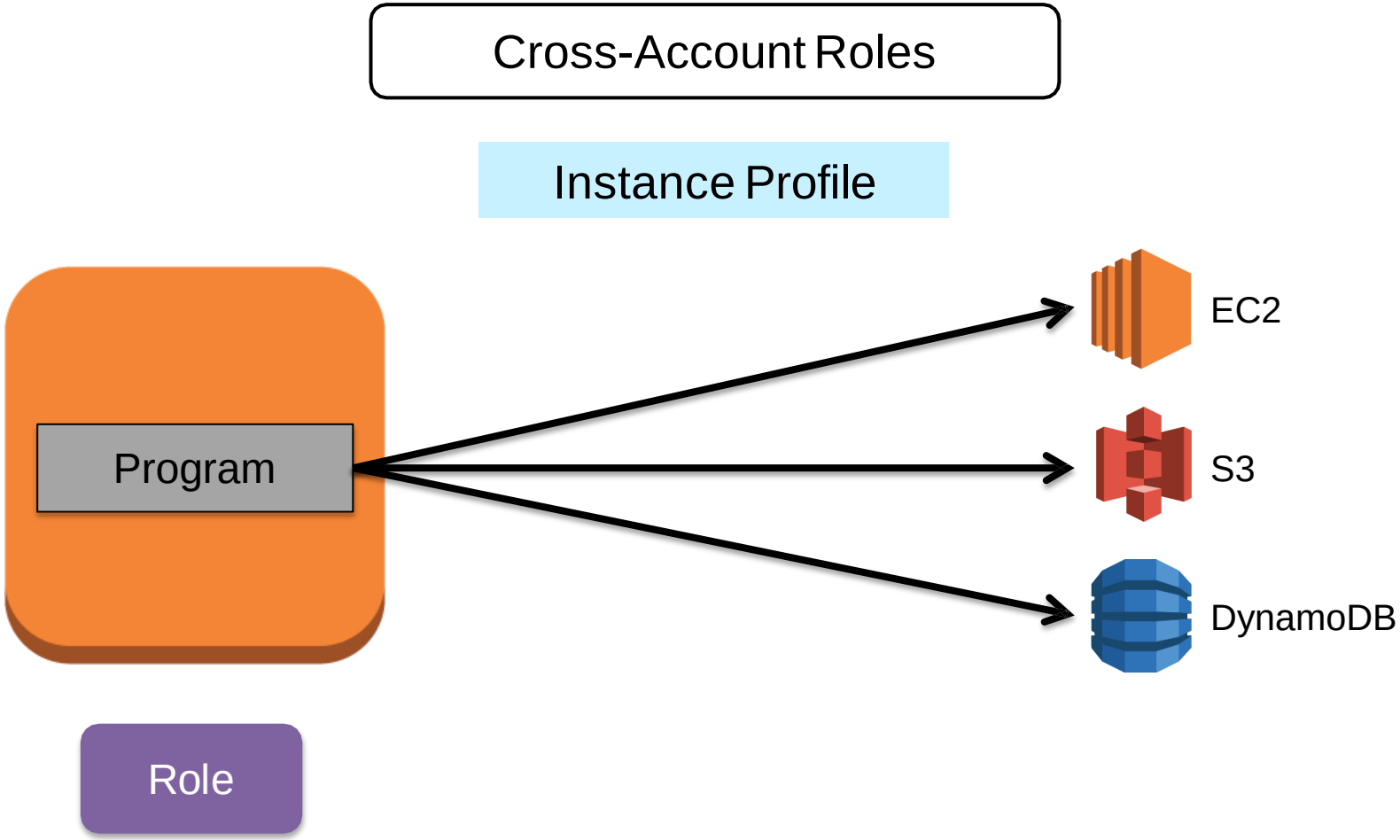
IAM Roles

Cross-Account Roles

- Roles and Permissions between Different Accounts and Users.



IAM Roles



IAM Roles

Cross-Account Roles

- Identity Federation: AWS resources can be accessed by third party Identity Providers (IdP)
  - *Web*: Facebook, Google, Amazon or any OIDC
  - *SAML2.0*: LDAP or Microsoft AD

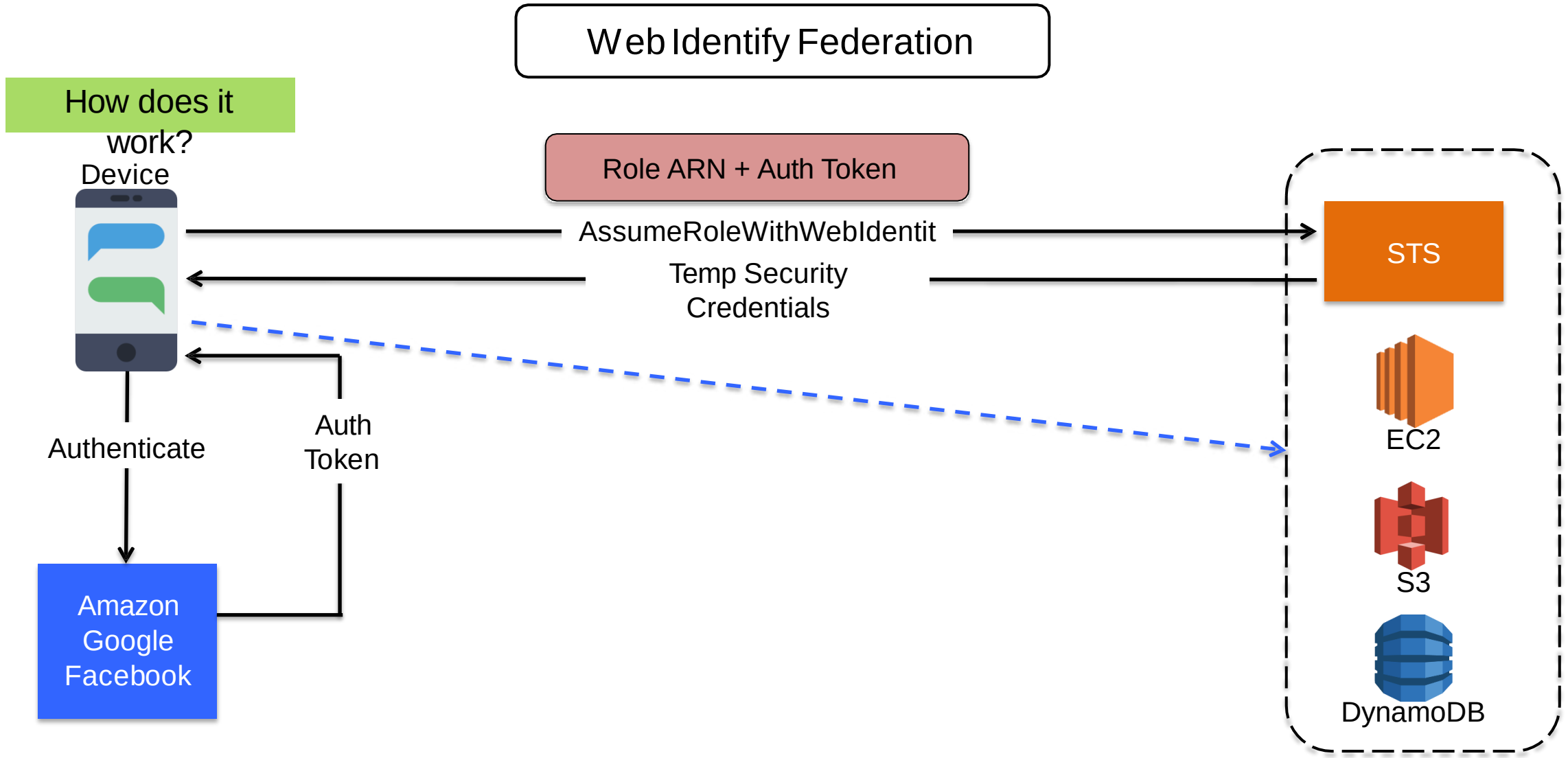
- Steps (Web Identity Federation)
  - Sign up as developer in Facebook or Google or Amazon account.
  - Create an Identity Provider in IAM.
  - Create Role with Trust and Permission Policy
  - In Trust Policy Principal should be the Web IdP
  - Cognito can be used as Identity Broker.

"Principal" : { "Federated" : "www.amazon.com" }
"Principal" : { "Federated" : "graph.facebook.com" }
"Principal" : { "Federated" : "accounts.google.com"}

"Action" : "sts:AssumeRoleWithWebIdentity"

Identity Federations

IAM Federation



IAM Federation

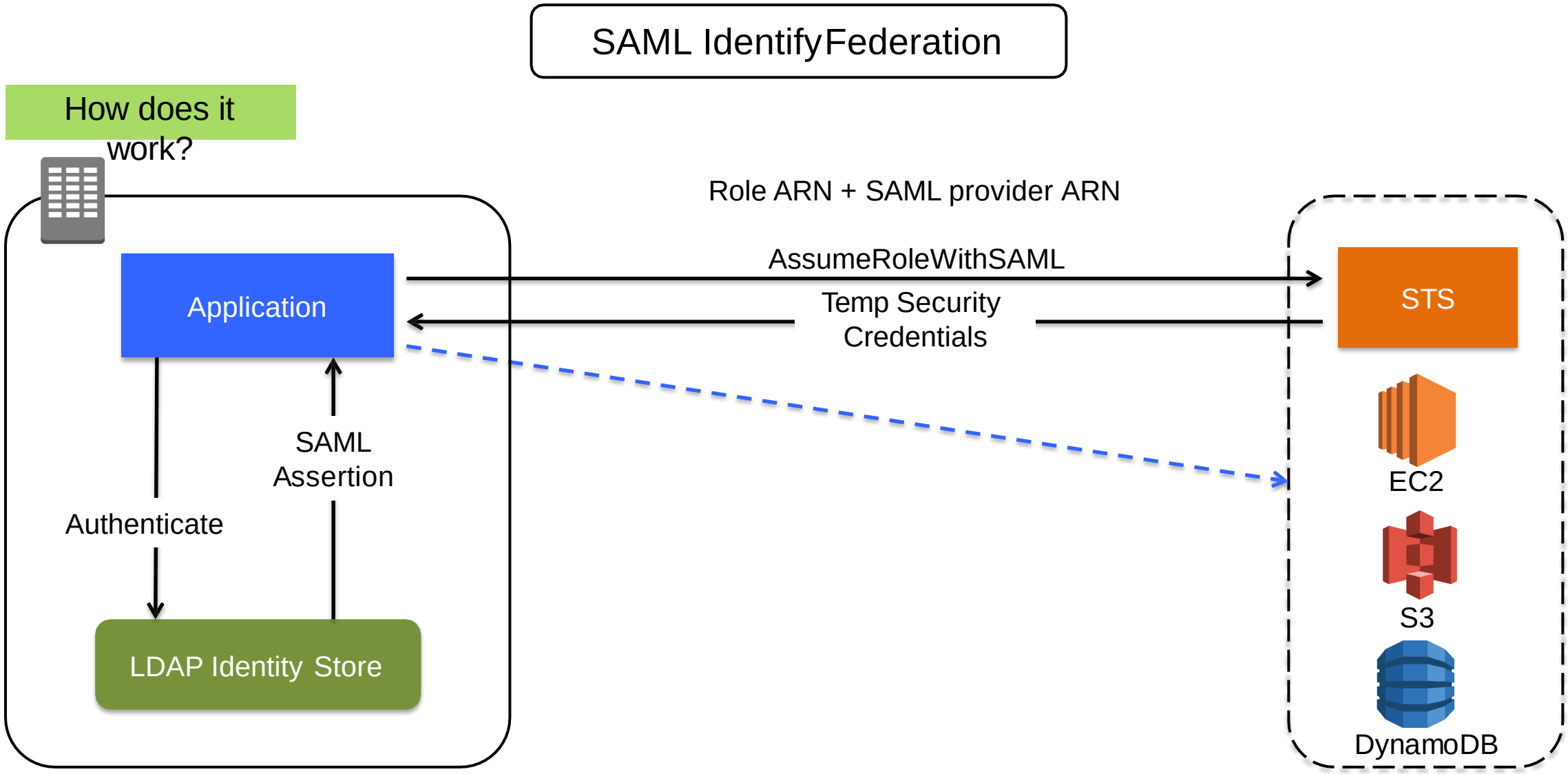
SAML IdentifyFederation

- Steps (SAML Federation)
  - Register AWS with Corporate IdP (LDAP).
  - That will generate a Metadata XML.
  - Create a SAML identity provider with the SAML metadata.
  - Create Roles.
  - These roles should be mapped with Organization's assertions.

"Principal" : { "AWS" : "ARN of the SAML provider" }

"Action" : "sts:AssumeRoleWithSAML"

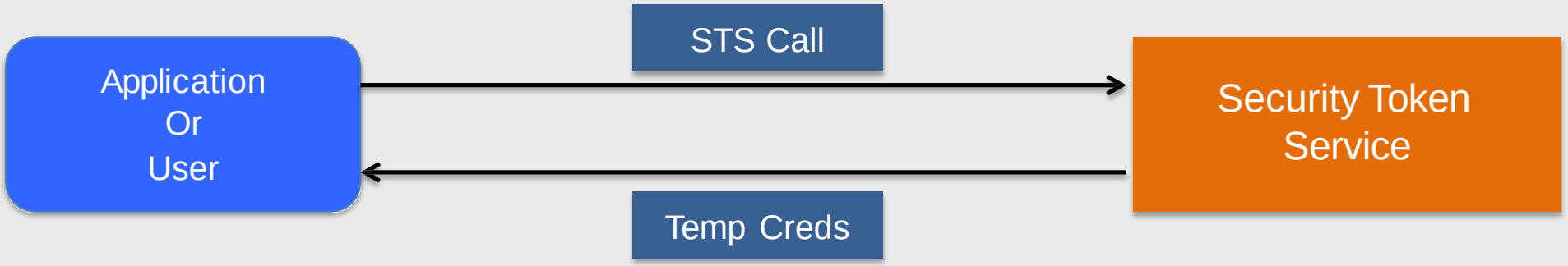
IAM Federation



Security Token Service

Temporary Security Credentials & STS

- STS (Security Token Service) can be used to get temporary security credentials.
  - Temporary Access Key ID, Secret Access Key and Security Token

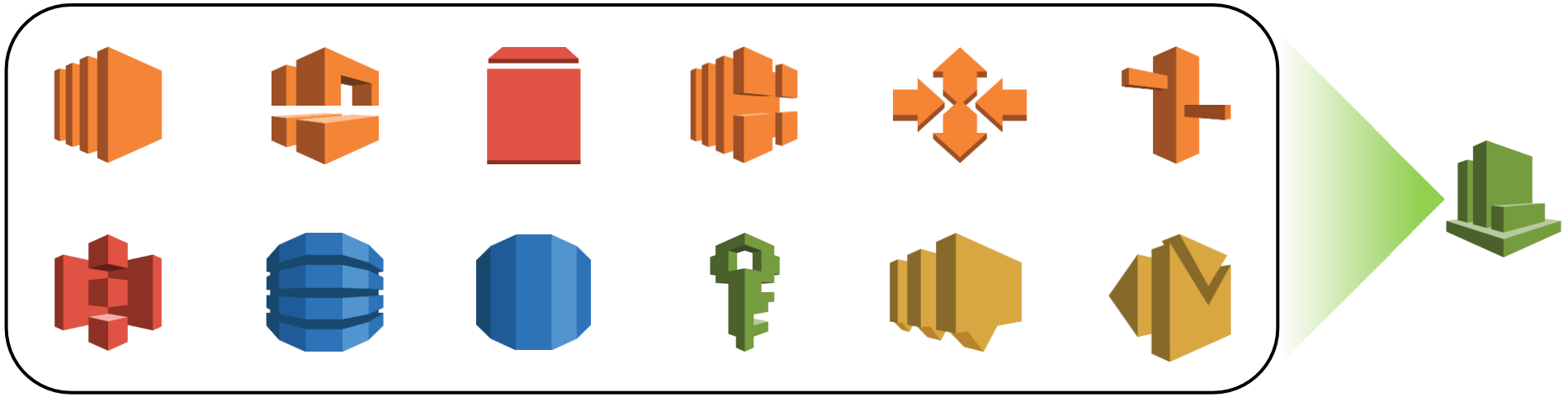


- STS Calls.
  - "AssumeRole": ARN of the Role, Duration (15 mins to 1 hour (Default))
  - "AssumeRoleWithWebIdentity": ARN of the Role, Auth Token, Duration (15 mins to 1 hour (Default))
  - "AssumeRoleWithSAML" : ARN of the Role, ARN of the SAML provider created in IAM, SAML assertion, Duration (15 min to 1 hour (Default)
  - "GetFederationToken"
  - "GetSessionToken"

Introduction to CloudWatch

CloudWatch Monitoring

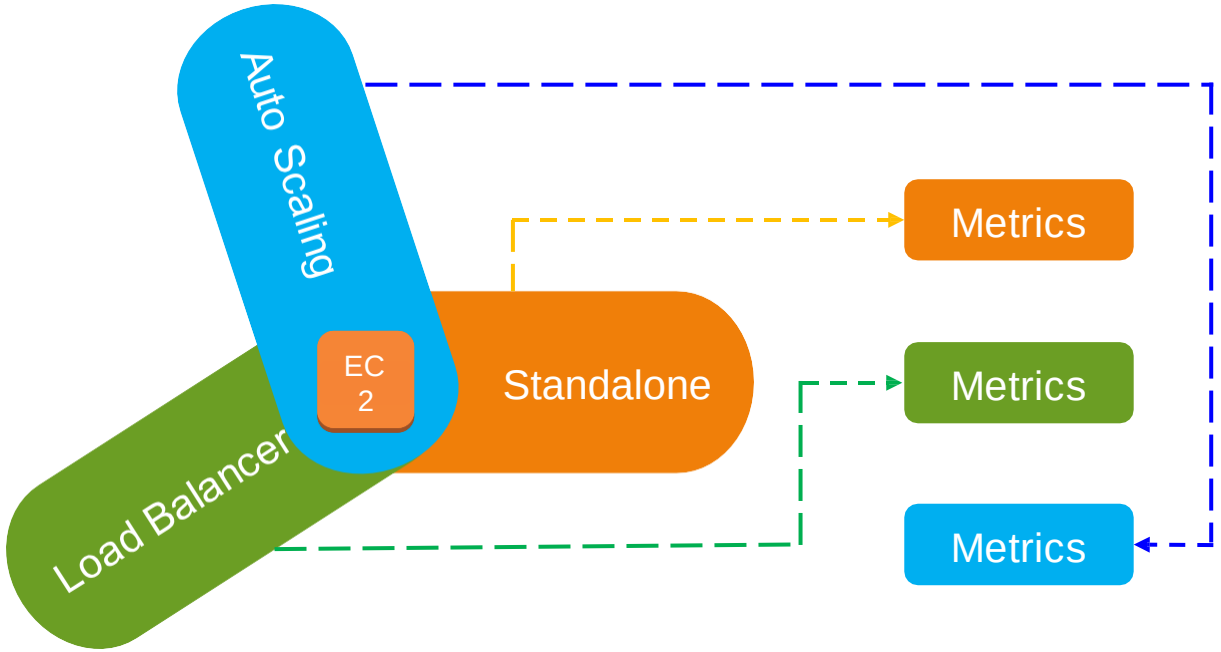
- Monitors all AWS resources provisioned and deployed.
- Sends notifications if anything goes wrong.
- **Following services are used in conjunction with CloudWatch:**



Dimensions and Statistics

Dimensions and Statistics

- Dimensions
- Statistics: Data aggregations over a period oftime.

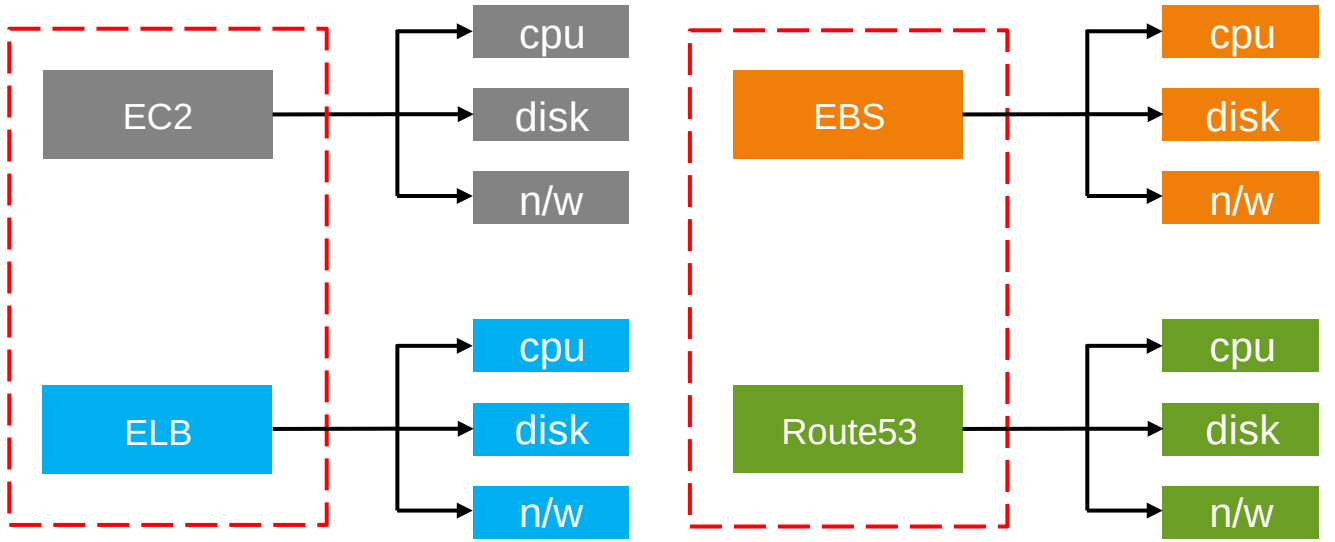


CloudWatch Metrics and Namespaces

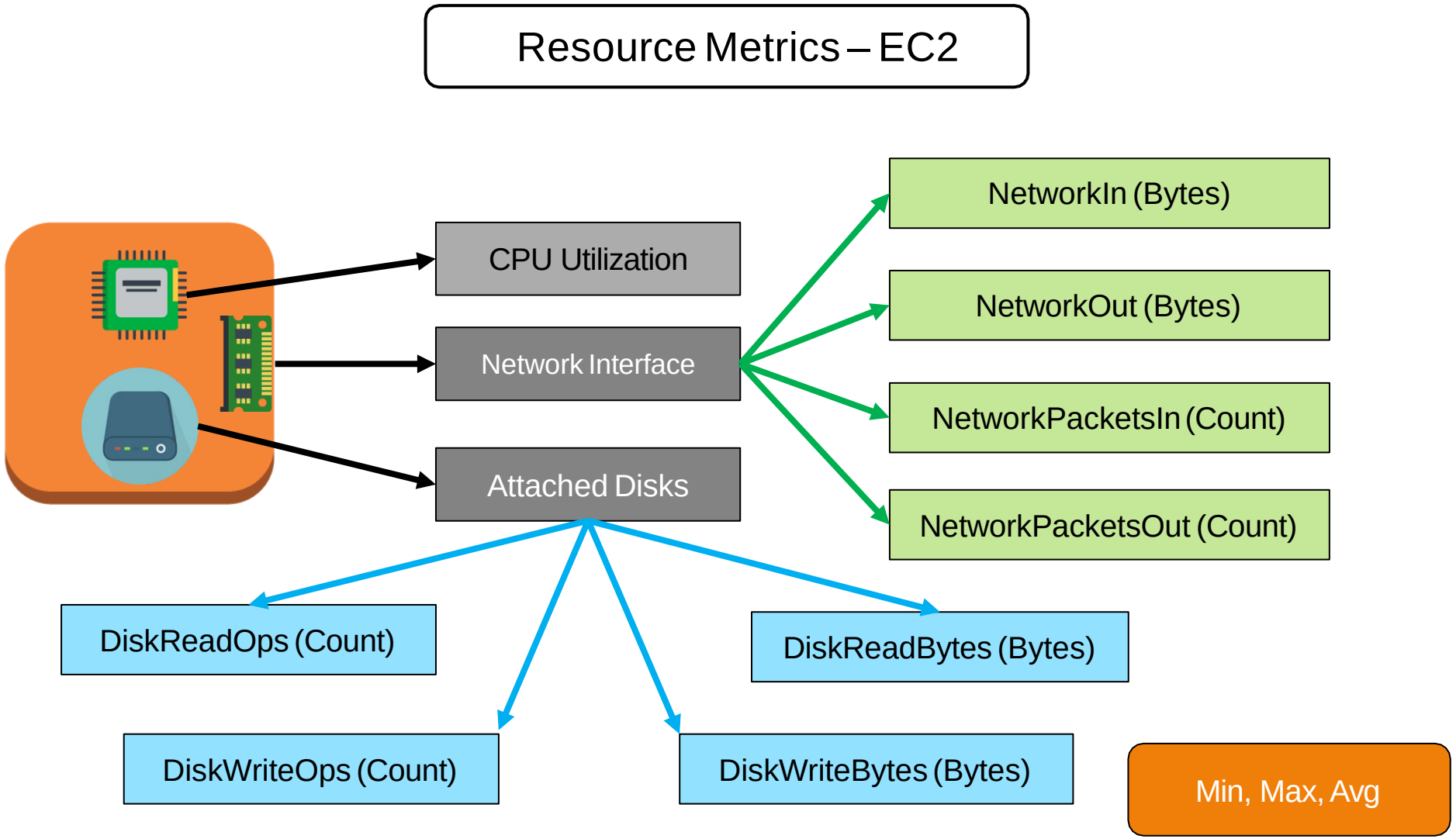
Metrics and Namespaces

Metric and Namespaces

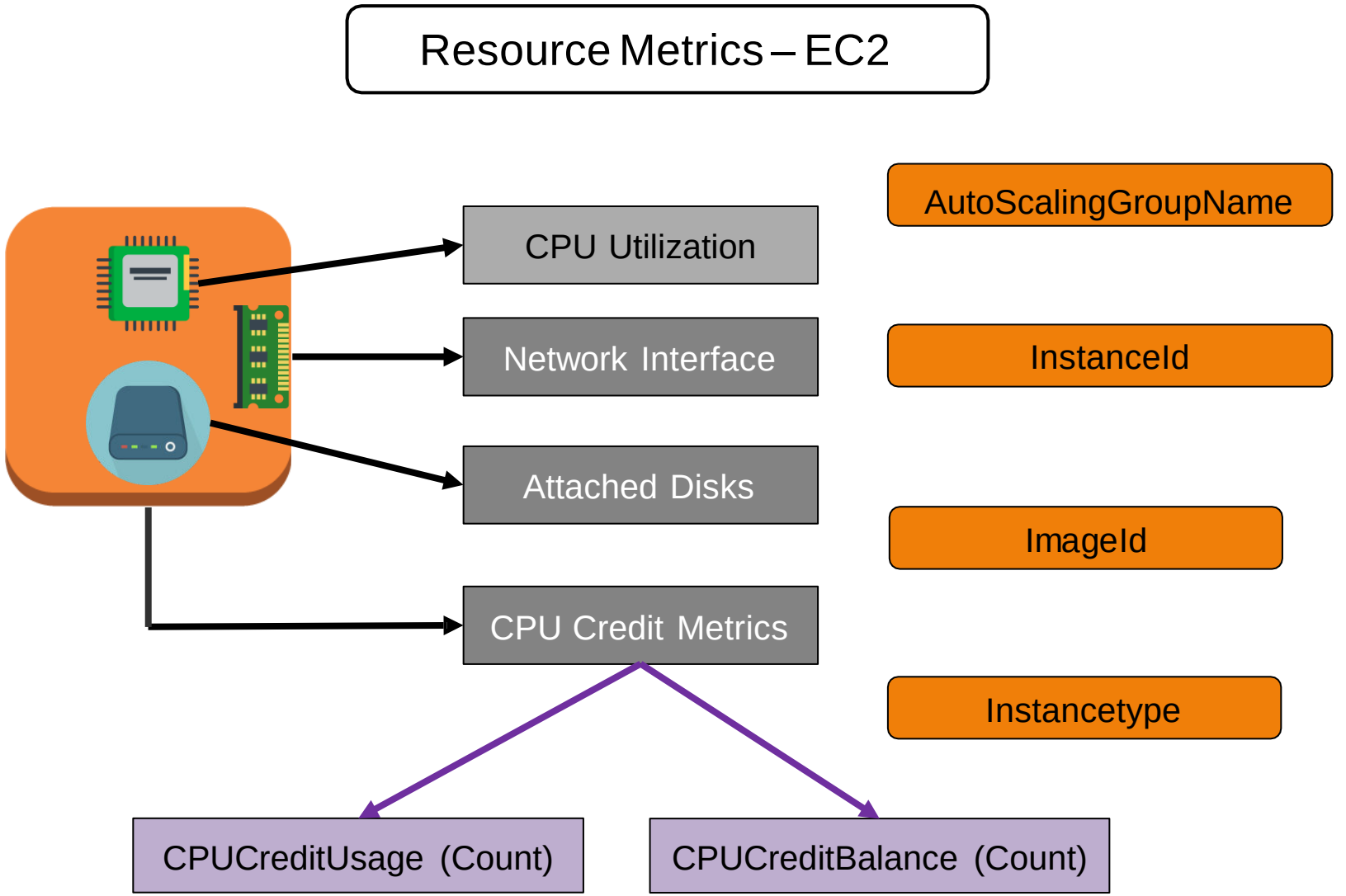
- Metrics are fundamental to CloudWatch monitoring.
- Individual data points which are monitored, all actions are based on metrics. e.g. CPU Utilization percentage.
- All AWS services send metrics to CloudWatch by default.



Metrics and Namespaces

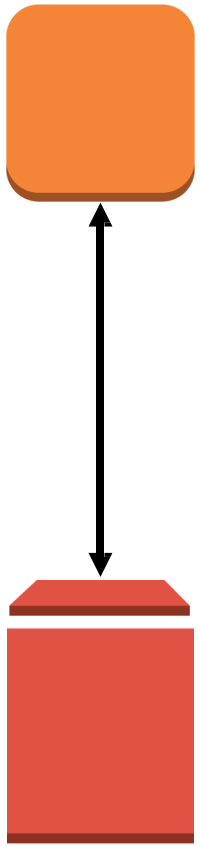


Metrics and Namespaces



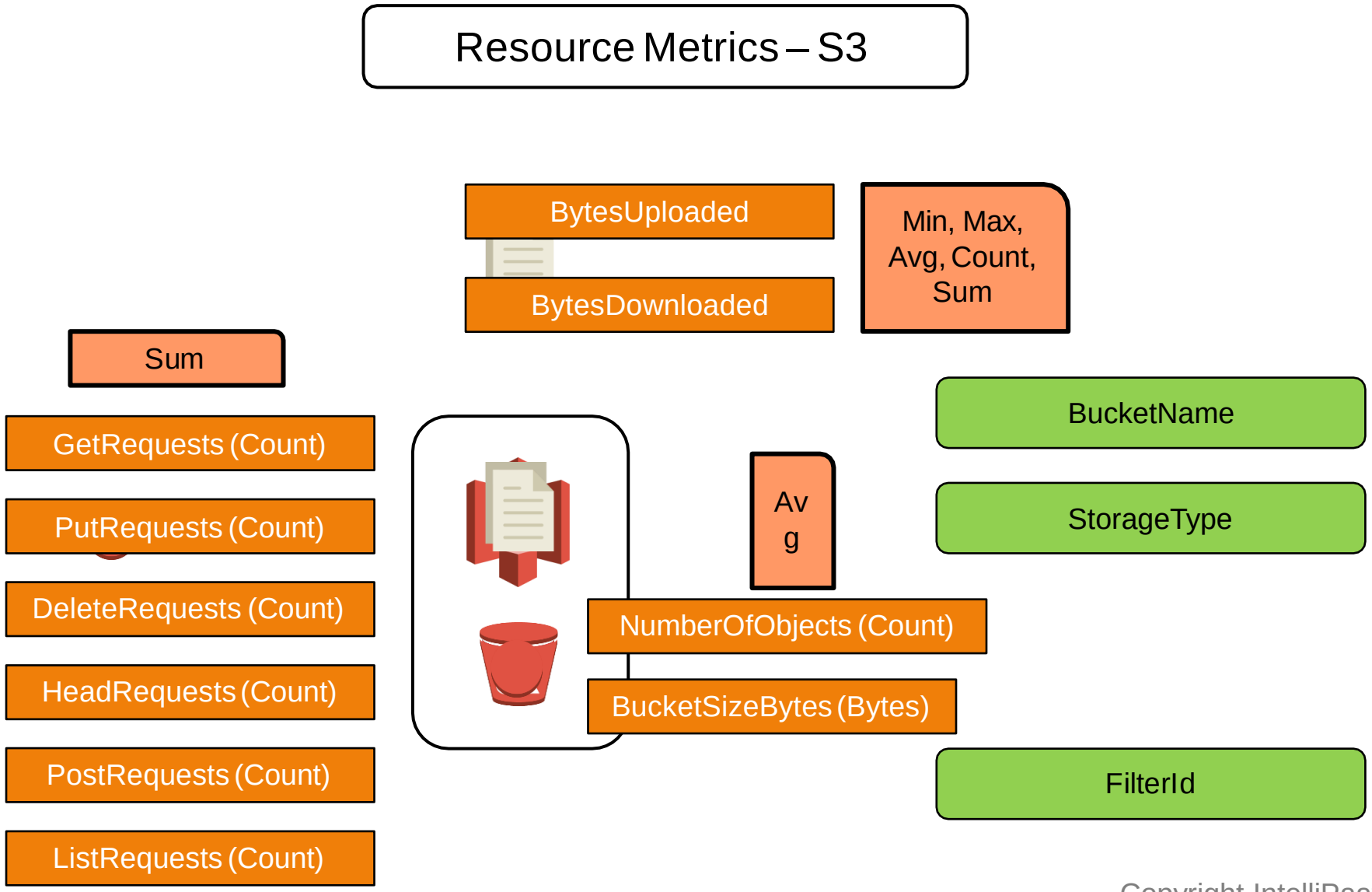
Metrics and Namespaces

Resource Metrics – EBS

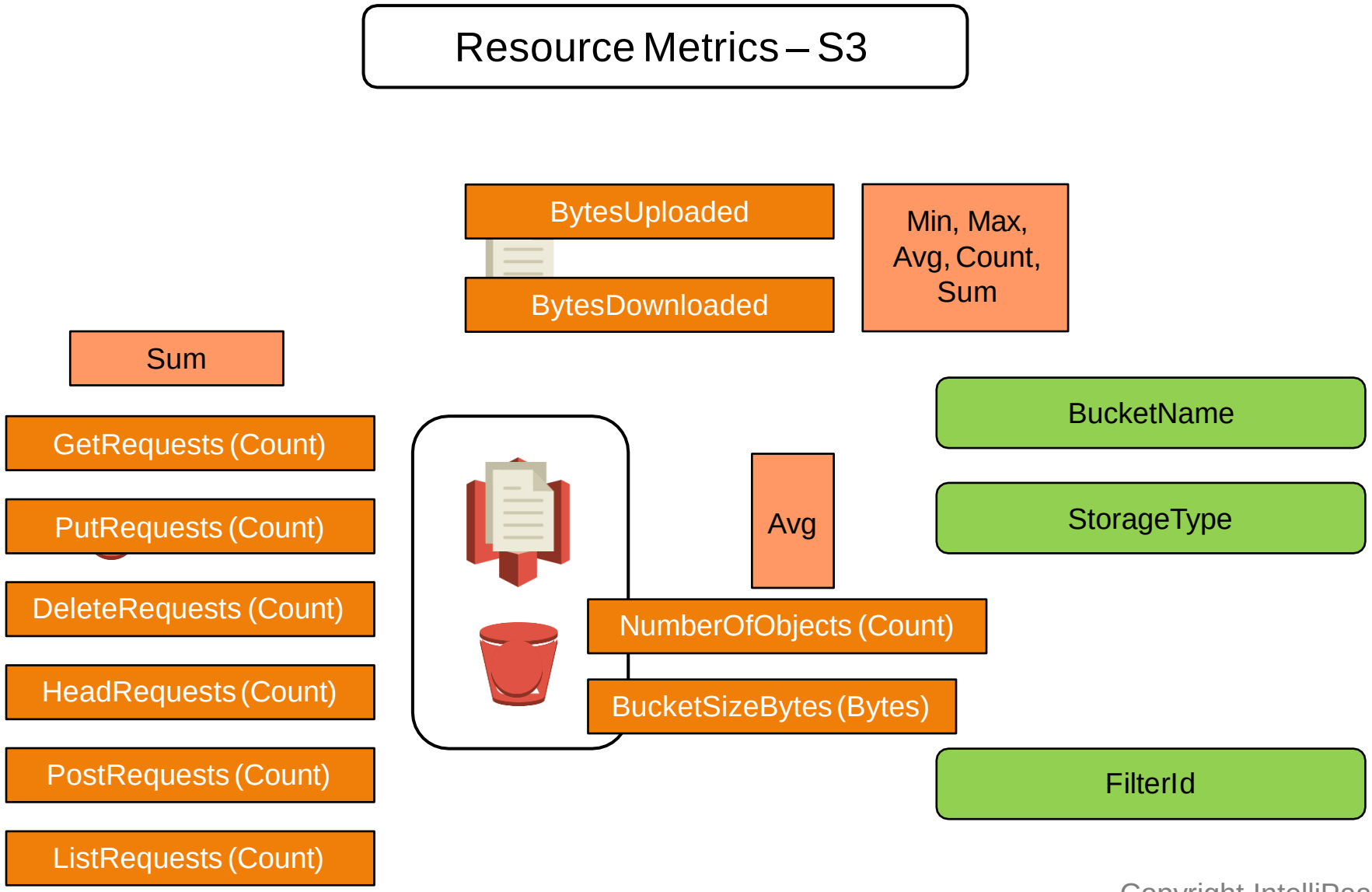


Metrics	Unit	Statistics
VolumeReadBytes	Bytes	Sum, Avg, Count
VolumeWriteBytes	Bytes	Sum, Avg, Count
VolumeReadOps	Count	
VolumeWriteOps	Count	
VolumeTotalReadTime	Seconds	
VolumeTotalWriteTime	Seconds	
VolumeIdleTime	Seconds	
VolumeQueueLength	Count	
VolumeThroughputPercentage	Percent	
VolumeConsumedReadWriteOps	Count	
BurstBalance	Percent	

Metrics and Namespaces



Metrics and Namespaces



Metrics and Namespaces

Resource Metrics–DynamoDB

GlobalSecondaryIndexName

StreamLabel

TableName

PutItem
DeleteItem
UpdateItem
GetItem
BatchGetItem
Scan
Query
BatchWriteItem

Table

Item

Attributes

Min, Max, Avg, Count, Sum

GSI/LSI

ConsumedReadCapacityUnits

ProvisionedReadCapacityUnits

ConsumedWriteCapacityUnits

ProvisionedWriteCapacityUnits

OnlineIndexConsumedWriteCapacity

ReadThrottleEvents

OnlineIndexPercentageProgress

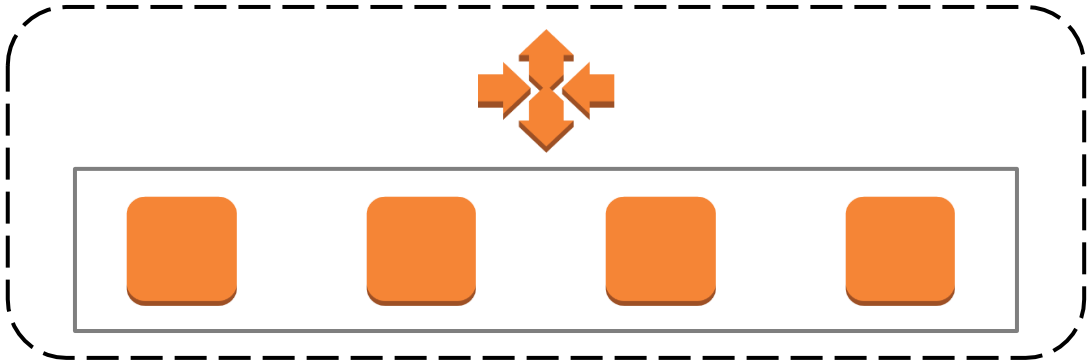
WriteThrottleEvents

OnlineIndexThrottleEvents

ThrottledRequests

Metrics and Namespaces

Resource Metrics – AS



GroupMinSize

GroupMaxSize

GroupDesiredCapacity

GroupInServiceInstances

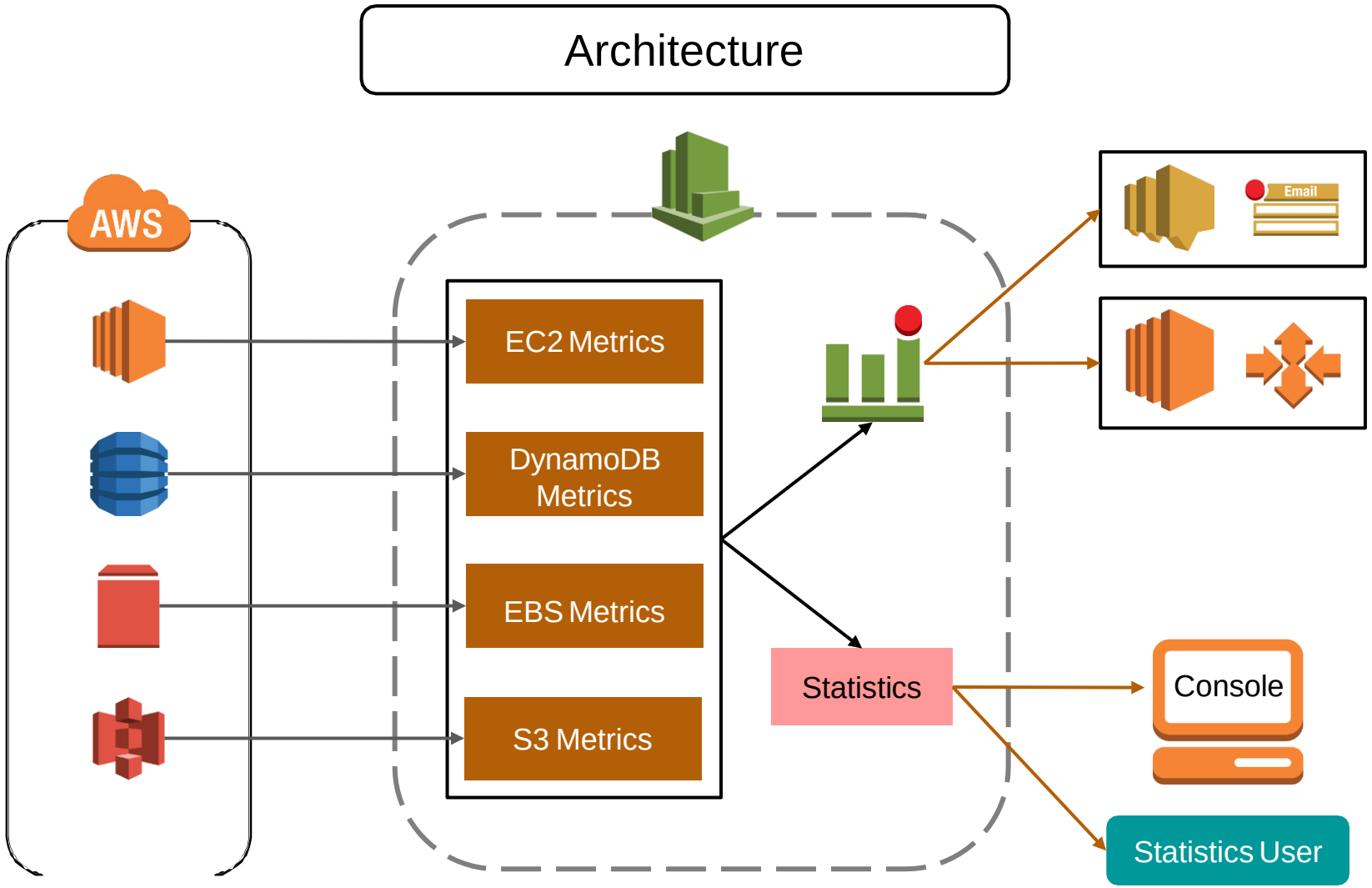
GroupPendingInstances

GroupStandbyInstances

GroupTerminatingInstances

GroupTotalInstances

Architecture



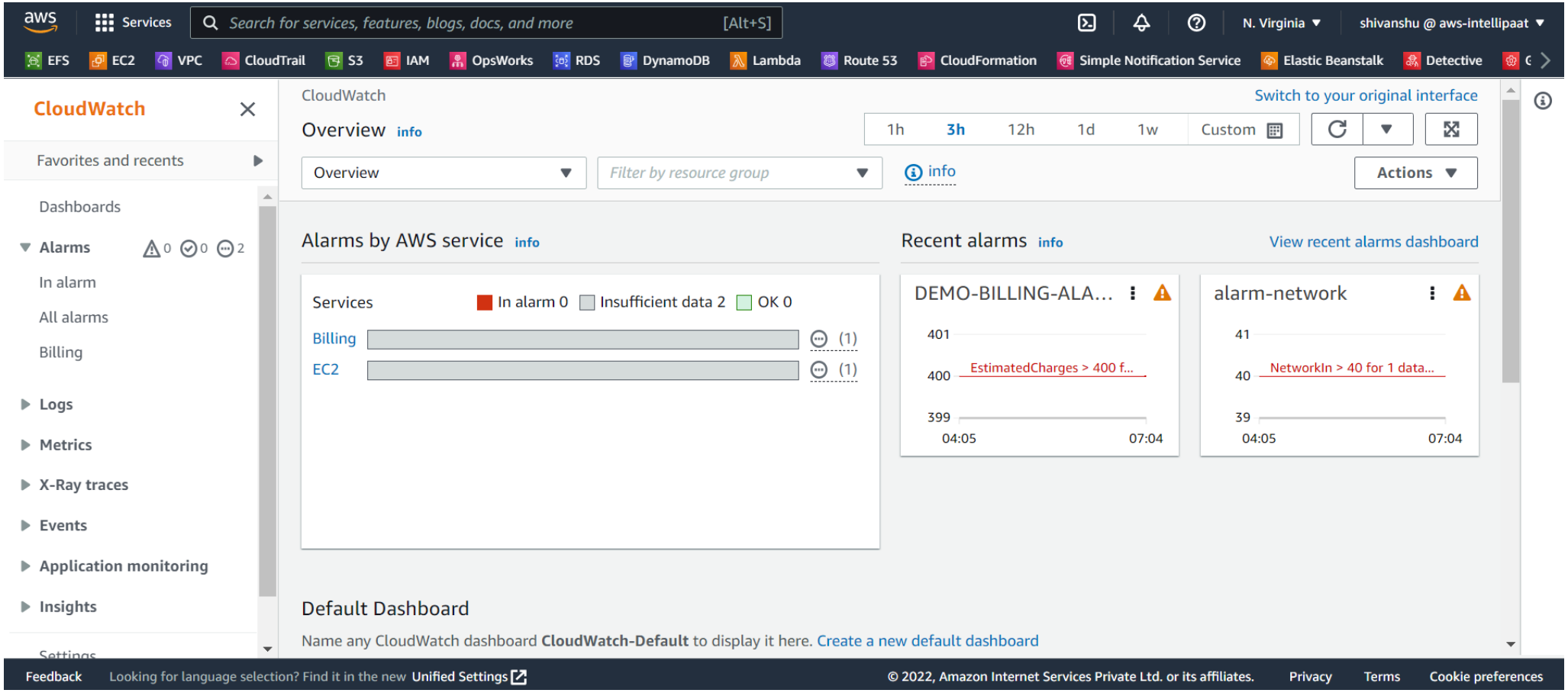
CloudWatch Dashboard

CloudWatch Dashboard

Dashboards

Dashboards are pages in the console which can be used to put all the important statistics deemed important at one place.

CloudWatch Dashboard

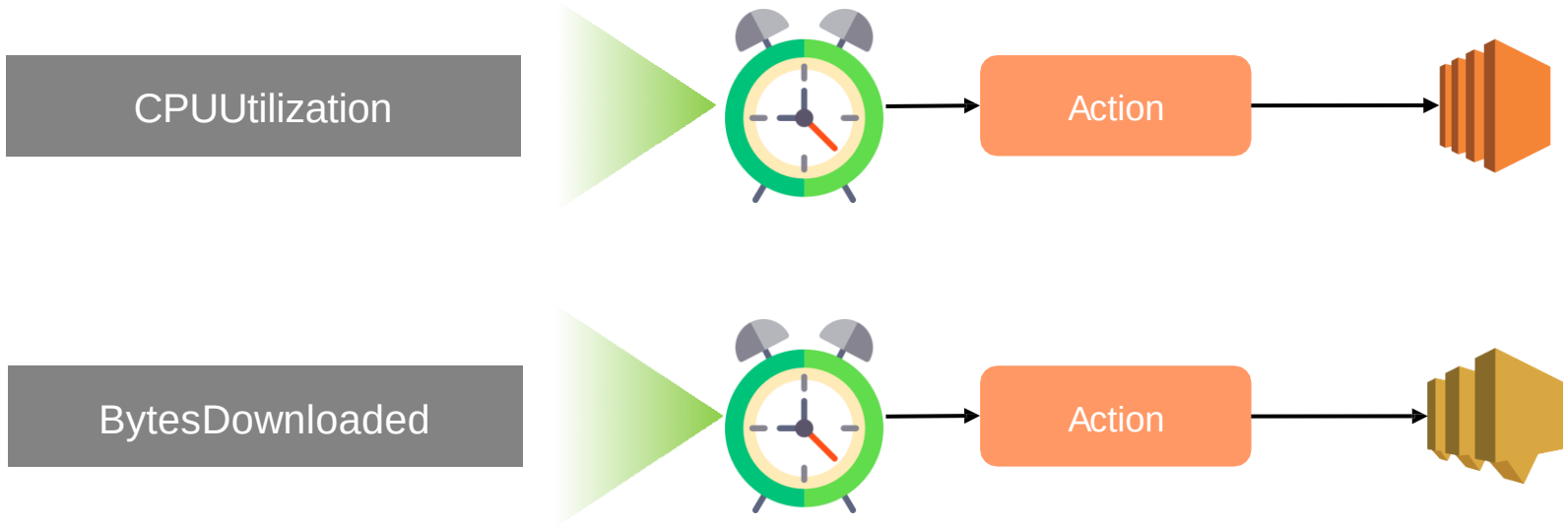


CloudWatch Alarm

CloudWatch Alarm

Alarm

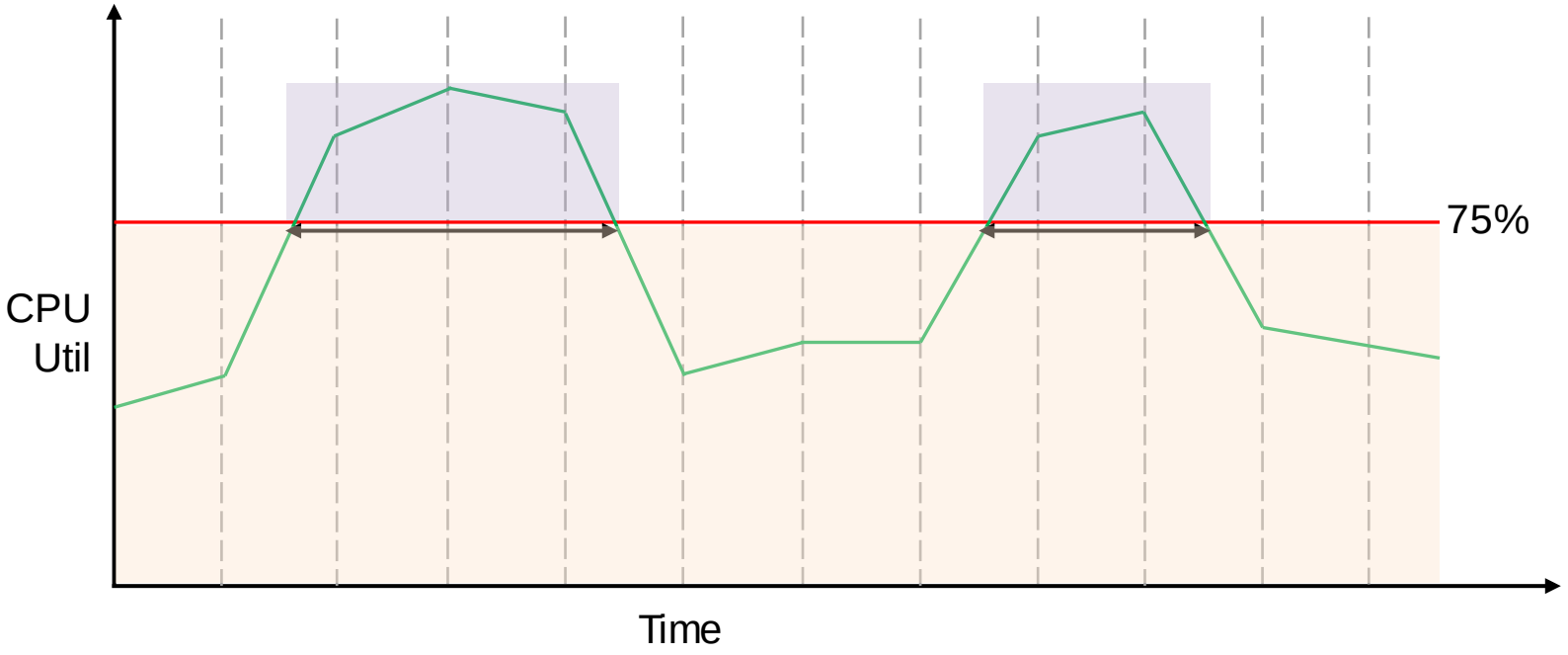
- Alarms watch over metrics and metrics only.
- Alarms can be set to take action based on metrics data.



CloudWatch Alarm

Alarm

Alarm Threshold and Period. (Threshold of 75% for 3 consecutive times)



Alarm States

- OK – Within Threshold.
- ALARM – Crossed Threshold.
- INSUFFICIENT_DATA – Metric not available/ Missing data (Good, Bad, Ignore, Missing).

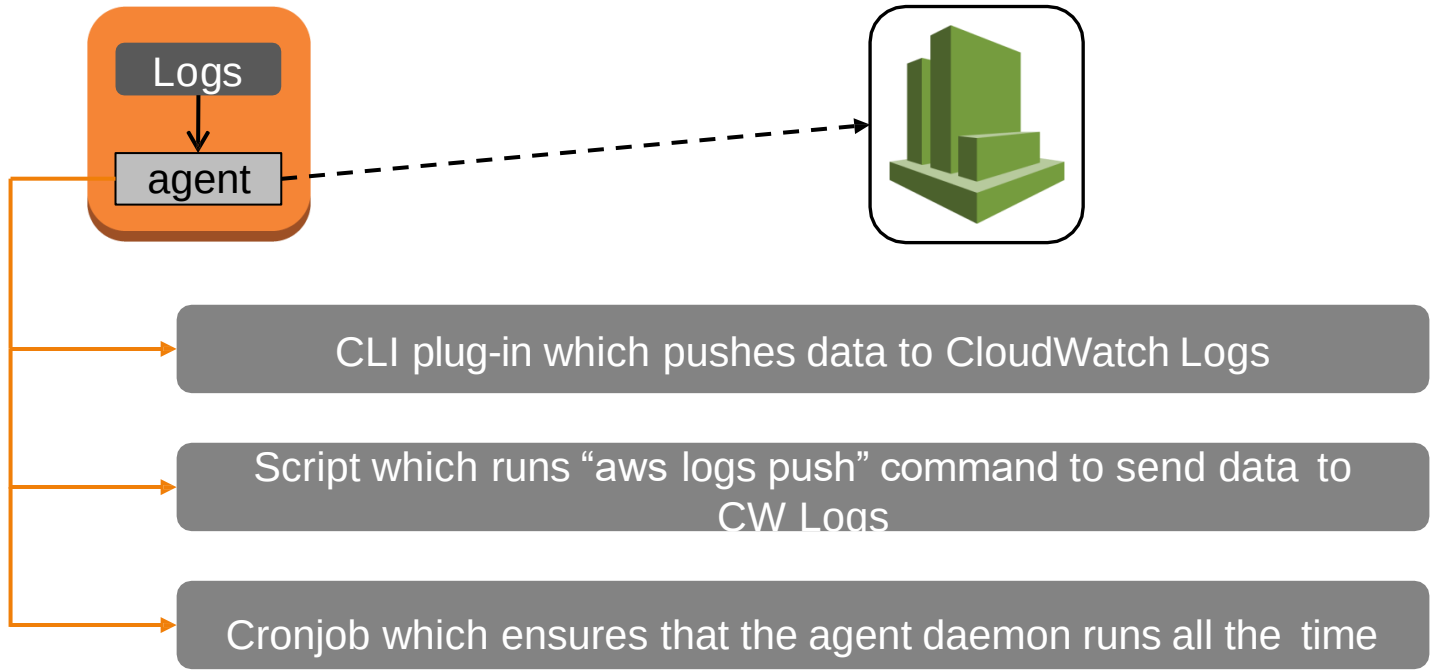
CloudWatch Logs

CloudWatch Logs

Logs

CloudWatch logs are used to monitor, store and access log files from various AWS resources including EC2 etc.

How does itwork:



CloudWatch Logs

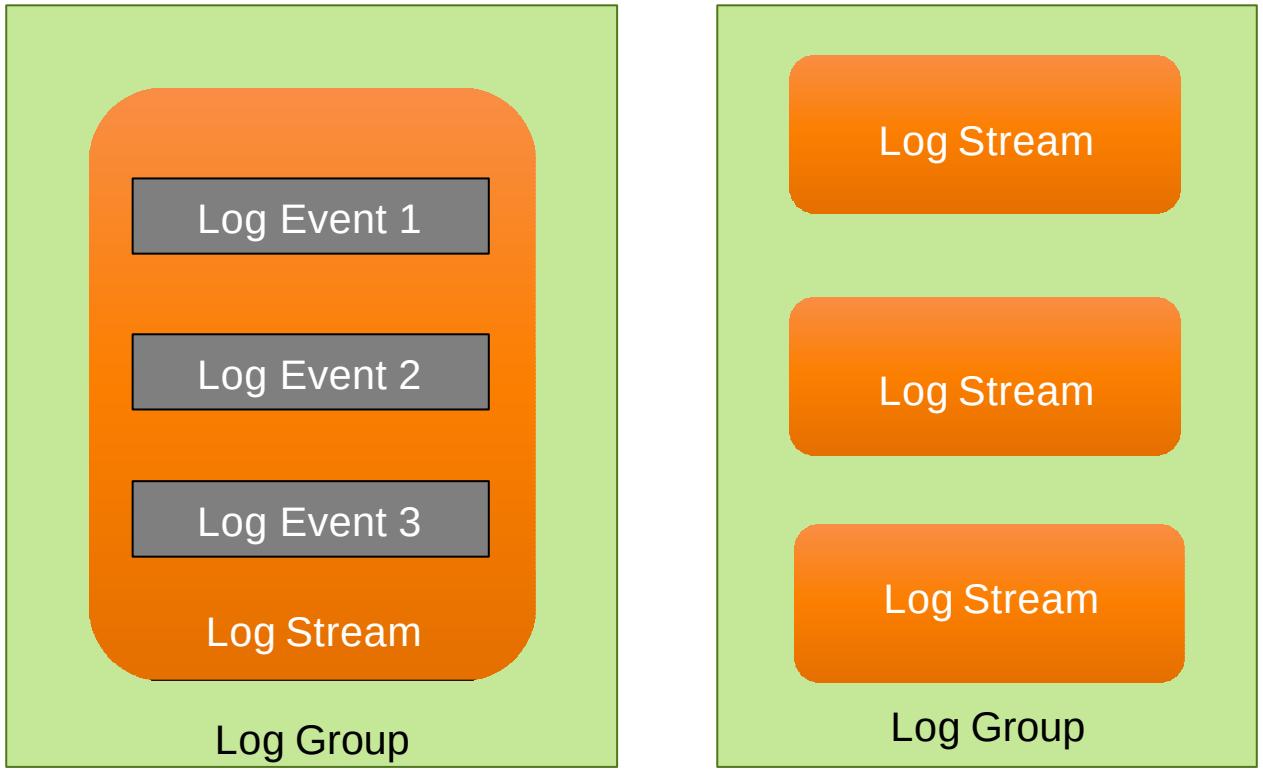
CloudWatch Log Components

Log Events: Record of some activity recorded by the application being monitored.

Log Streams: Sequence of log events from the same source

Log Groups: Group of Log Streams.

Metric Filters: Customized metrics created from received log data.



CloudWatch Logs

Installing Logs Agent

- Install and configure the agent

```
sudo yum install -y  awslogs
```

```
/etc/awslogs/awscli.conf
```

```
/etc/awslogs/awslogs.conf
```

```
sudo service  start awslogs
```

```
/var/log/awslogs.log
```

```
sudo chkconfig awslogs  on
```

CloudWatch Logs

Log Config File

Config File: Contains information needed by “aws logs push” command.

General Section:
- state_file
- logging_config_file

Logstream Section:
- log_group_name = value
- log_stream_name = value
- file = value
- batch_count = integer
- batch_size = integer

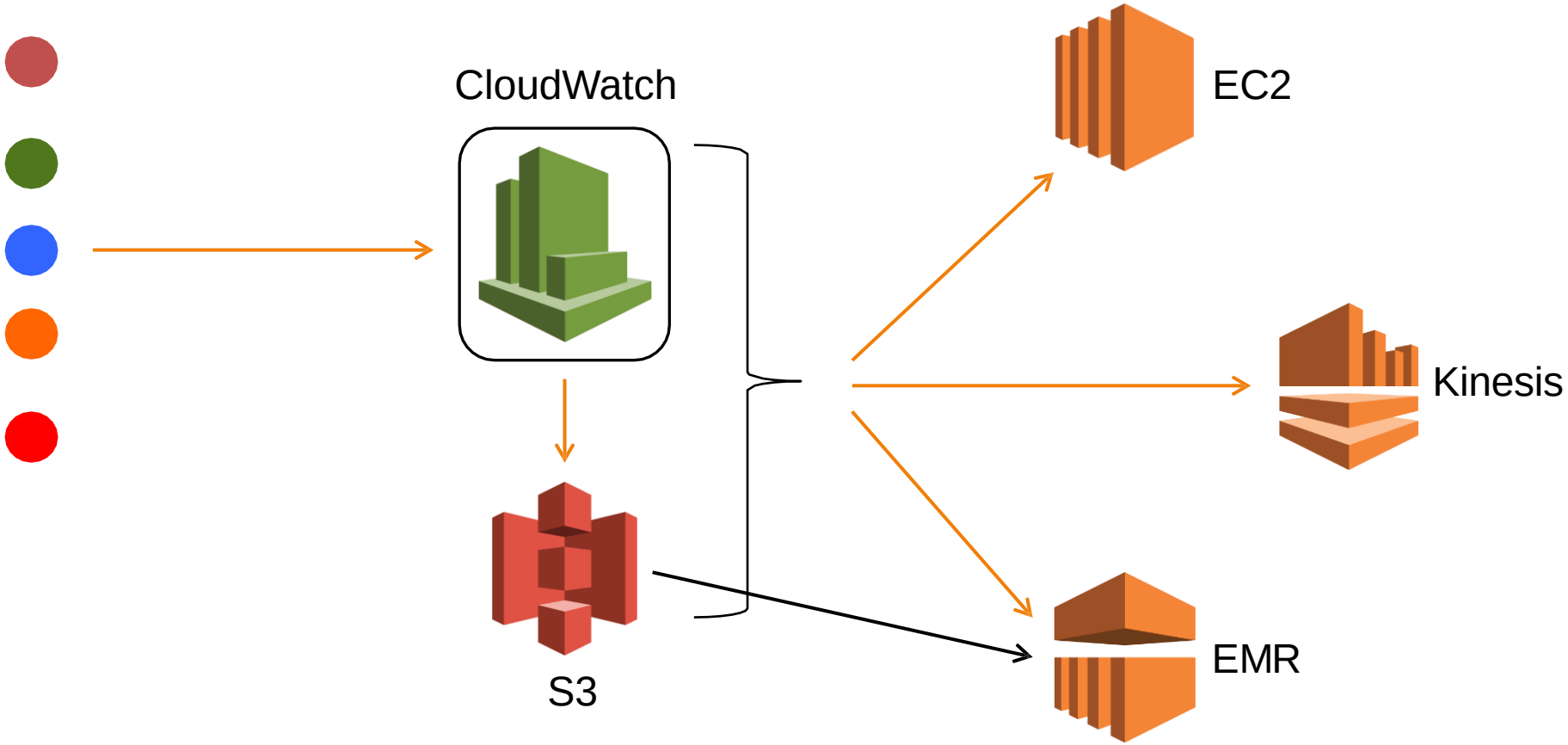
Pricing

CloudWatch Pricing: us-east1

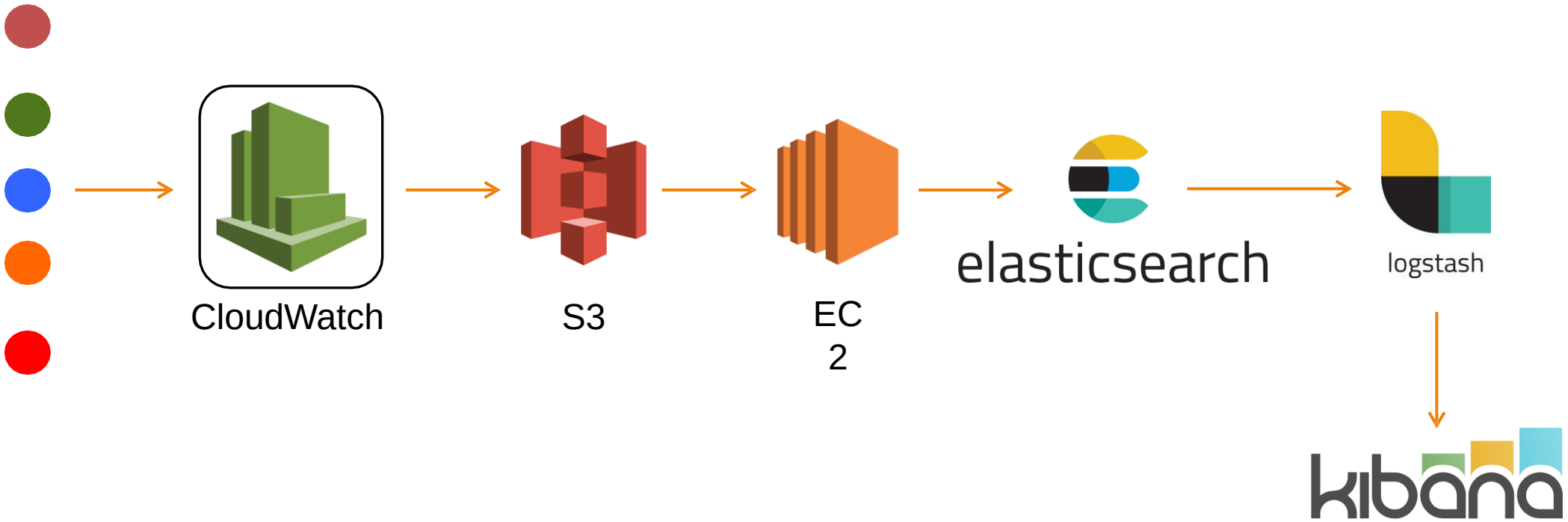
- Free Tier
  - 3 dashboards up to 50 metrics per month
  - Basic monitoring at 5 mins interval of EC2, EBS, ELB, RDS are free.
- https://aws.amazon.com/cloudwatch/pricing/
- Pricing
  - Dashboards: $3.00 per dashboard per month
  - Detailed monitoring for EC2 instances
  - Custom Metrics
  - Alarms: $0.10 per alarm/month
  - CloudWatch Logs
  - CloudWatch Events

Design Patterns

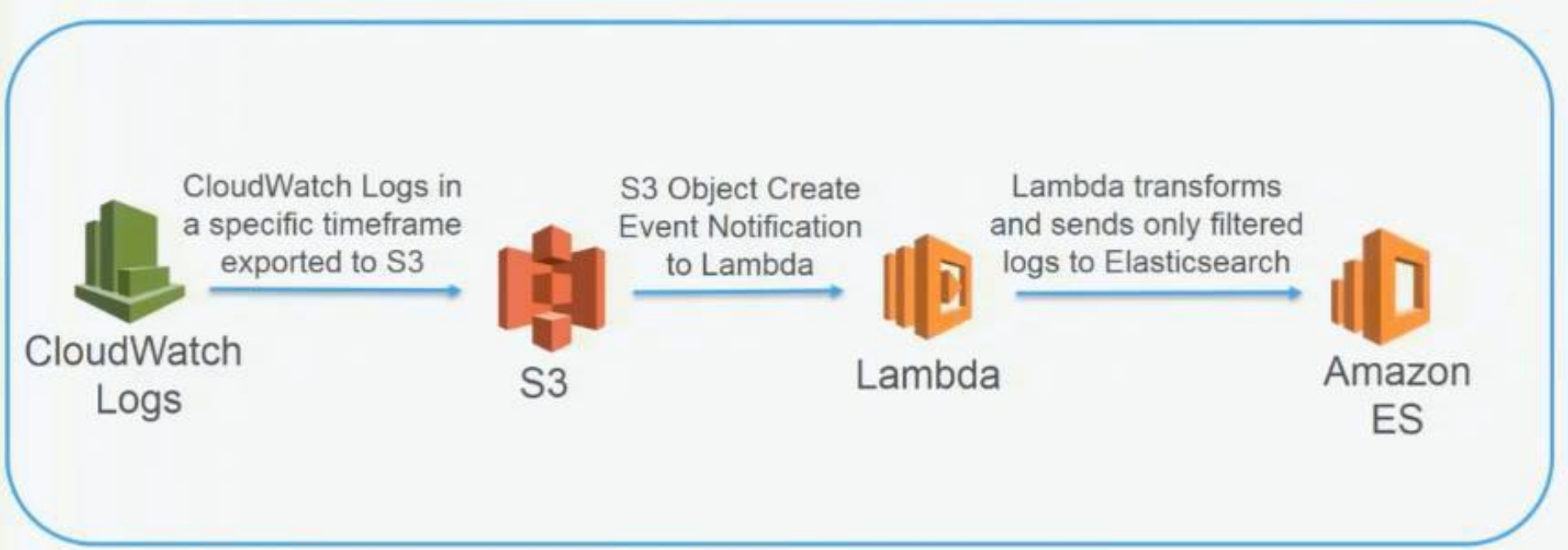
Design Pattern



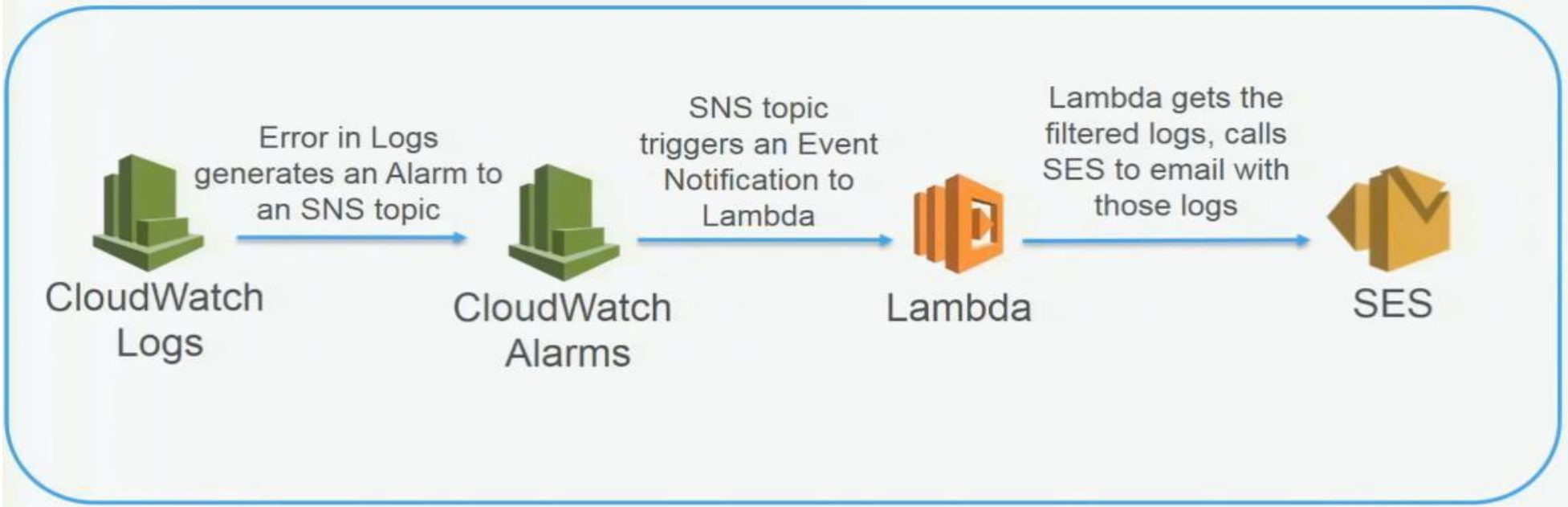
Design Pattern



Design Pattern



Design Pattern



Design Pattern

AWS STS

Security Token Service

AWS Security Token Service (AWS STS) is a web service provided by AWS that allows you to request temporary, limited-access credentials for AWS Identity and Access Management (IAM) users or users you authenticate (federated users).

Security Token Service

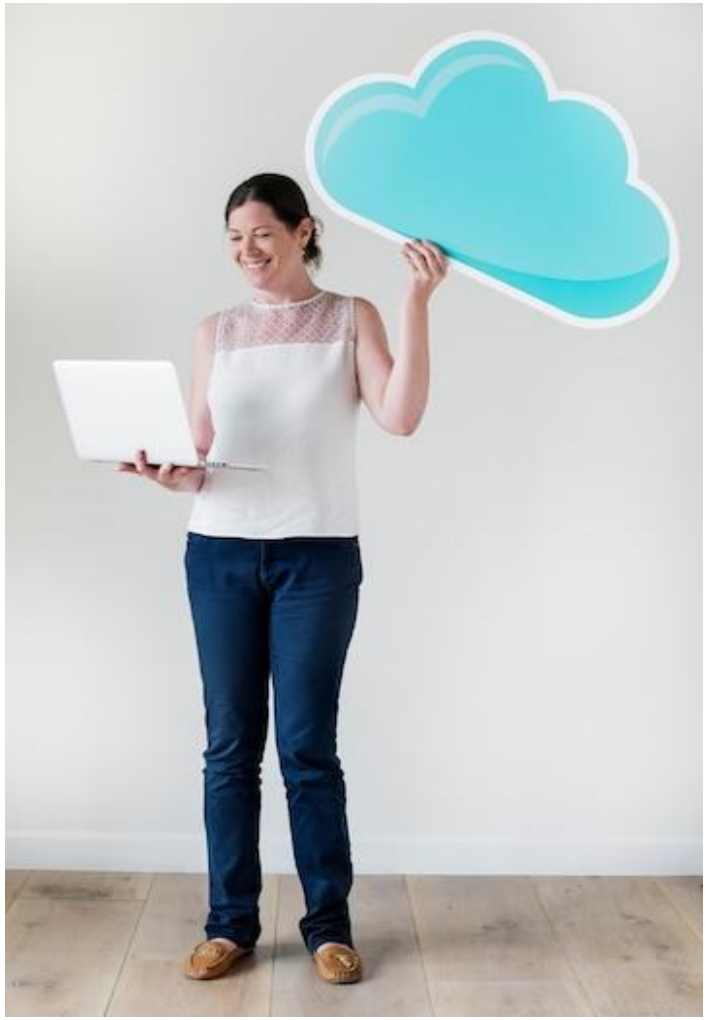
Use Case

- **Privilege elevation** - this is already mentioned, AssumeRole allows to become another role within the same or different aws account.
- **Authorization** to aws resources for identities authenticated a other way (AD, SAML, OIDC,..), see services AssumeRoleWithSAML or AssumeRoleWithWebIdentity.
- **Authorization** to aws resources with custom authorization, see GetFederationToken.

IAM
Access Analyzer

Access Analyzer

Identity and Access Management on AWS Access Analyzer assists in identifying potential resource-access risks by identifying any policies that grant access to an external principal. It accomplishes this by analysing resource-based policies in your AWS environment using logic-based reasoning. Another AWS account, a root user, an IAM user or role, a federated user, an AWS service, or an anonymous user can all be external principals.



Access Analyzer

Use Case

AWS IAM Access Analyzer provides the following capabilities:

- IAM Access Analyzer helps identify resources in your organization and accounts that are shared with an external entity.
- IAM Access Analyzer validates IAM policies against policy grammar and best practices.
- IAM Access Analyzer generates IAM policies based on access activity in your AWS CloudTrail logs.

IAM
Access Advisor

Access Advisor

The AWS Identity and Access Management (IAM) access advisor uses data analysis to help you confidently set permission guardrails by providing service last accessed information for your accounts, organizational units (OUs), and your AWS Organizations-managed organization.

IntelliPaat

Access Advisor

Use Case

Assume Arnav Desai is a security administrator for Example Corp. He works with several development teams and monitors their access across multiple accounts. To get his development teams up and running quickly, he initially created multiple roles with broad permissions that are based on job function in the development accounts. Now, his developers are ready to deploy workloads to production accounts. The developers need access to configure AWS, however, Arnav only wants to grant them access to what they need. To determine these permissions, he uses access advisor APIs to automate a process that helps him understand the services developers accessed in the last six months. Using this information, he authors policies to grant access to specific services in production. I'll now show you an example to achieve this in one account using AWS CLI commands.

IAM
Policy Simulator

IAM Policy Simulator

Identity-based policies, IAM permissions boundaries, Organizations service control policies (SCPs), and resource-based policies can all be tested and troubleshooted using the IAM policy simulator.

IAM Policy Simulator

The simulator assesses the policies you select and determines the effective permissions for each of the actions you specify. The simulator employs the same policy evaluation engine as real-world requests to AWS services.

IAM Policy Simulator

Benefits

- Improve developer agility.
- Application monitoring and auditing
- SaaS integrations expand functionality.
- AI/ML to personalize SaaS

.

CloudWatch EventBridge

CloudWatch EventBridge

Amazon EventBridge is a serverless event bus that makes it simple to connect applications using data from your own applications, SaaS applications, and AWS services.

CloudWatch EventBridge

Benefits

- Improve developer agility.
- Application monitoring and auditing
- SaaS integrations expand functionality.
- AI/ML to personalize SaaS

.

AWS CloudTrail

CloudTrail

AWS CloudTrail is a service provided by Amazon Web Services that enables operational and risk auditing, governance, and compliance for your AWS account. Events in CloudTrail are actions taken by a user, role, or AWS service. Events include AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs actions.

CloudTrail

Benefits

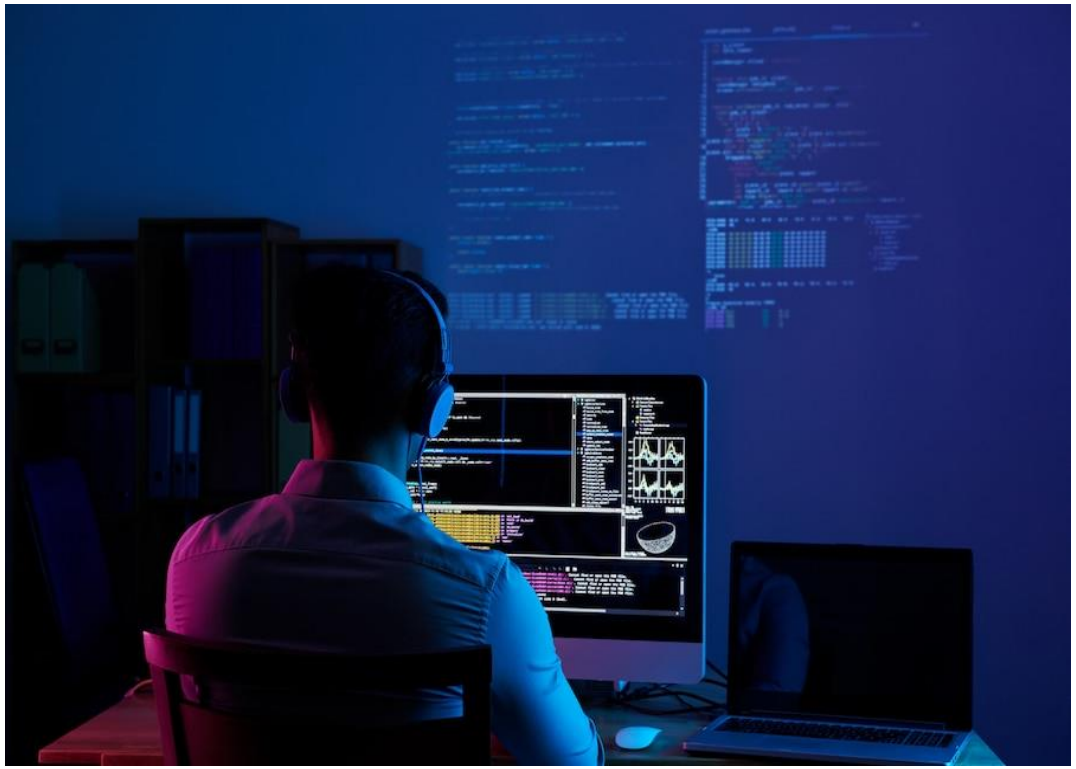
- Improves your security posture by recording user activity and events, and set up automated workflow rules with Amazon EventBridge.
- Protects your organization from penalties using CloudTrail logs to prove compliance with regulations such as SOC, PCI, and HIPAA.
- Captures and consolidate user activity and API usage across AWS Regions and accounts on a single, centrally controlled platform.

.

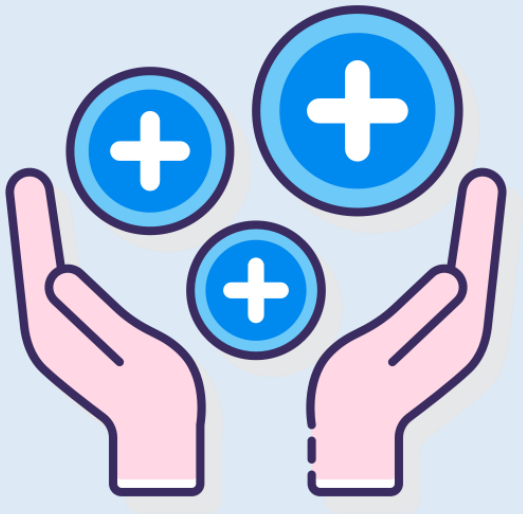
AWS Config

AWS Config

AWS Config displays a detailed view of the AWS resource configuration in your AWS account. This includes how the resources are related to one another as well as how they were previously configured, allowing you to see how the configurations and relationships change over time.



AWS Config



Benefits

- Security Analysis and Resource Administration
- Continuous monitoring
- Continuous assessment
- Monitoring compliance across the enterprise

.

India : +91-7847955955

US : 1-800-216-8930 (TOLLFREE)

sales@intellipaat.com

24X7 Chat with our Course Advisor