aws

IAM

What is IAM?

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. With IAM, you can centrally manage permissions that control which AWS resources users can access. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

AUTHENITICATION

Some common synonyms of authenticate are confirm, corroborate, substantiate, validate, and verify to user.

AUTHORIZATION

Determines what an identity can access within a system once it's been authenticated to it.

WHAT IS USER?

An AWS Identity and Access Management (IAM) user is an entity that you create in AWS. The IAM user represents the human user or workload who uses the IAM user to interact with AWS. A user in AWS consists of a name and credentials.

WHO TO CREATE USER IAM

Steps1: Users, and then select Add user.

Steps2: In the User name field, enter the name of the new user

Steps3: In the Access type field, and selection AWS Management Console access.

Steps4: Select Attach existing policies directly, and then select Create policy.

Steps5: and click the “Attach existing policies directly” to add the policy .

Steps6: Filter the policies for the name of the policy that you created and select the policy. Select Next: Tags and optionally assign user tags . When you're ready, select Create user.

Steps 7: Download and save the credentials of the new user (Access key iD and Secret access key).

WHAT IS GROUP?

- An IAM group is an identity that specifies a collection of IAM users. You can't use
- a group to sign-in. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users.

Who can create the group?

Steps1: Sign in to the AWS Management Console and open the IAM console .

Steps2: In the navigation pane, choose **User groups** and then choose **Create group**.

Steps3: For **User group name**, type the name of the group.

Steps4: In the list of users, select the check box for each user that you want to add to the group.

Steps5: In the list of policies, select the check box for each policy that you want to apply to all members of the group.

Steps6: Choose **Create group**.

HOW DOES IAM WORKS :

IAM workflow includes the following

1- Principal - (IAM users)

2. Authentication- (valid user)

3. Request - (Sending to AWS)

4. Authorization (Accessing Aws Resources)

5. Actions - (Some Tasks performed) eg:(edit, delete, etc)

6. Resources-(some resource)

WHAT IS POLICY

- A policy is an object in AWS that, when associated with an identity or resource, defines their permissions.
- When you create a permissions policy to restrict access to a resource, you can choose an identity-based policy or a resource-based policy.

TYPES OF POLICY

There TWO Types

1 Identity-based policies

2 Resource-based policies .

Identity-based policies

identity-based policies are JSON permissions policy documents that control what actions an identity (users, groups of users, and roles) can perform, on which resources, and under what conditions.

Identity-based policies can be further categorized.

1.AWS Managed policy.

2. Custom Managed policy.

3. Inline Policy.

1Aws Managed policy:

Policy can created a aws,and managed by aws and we can use that policy.

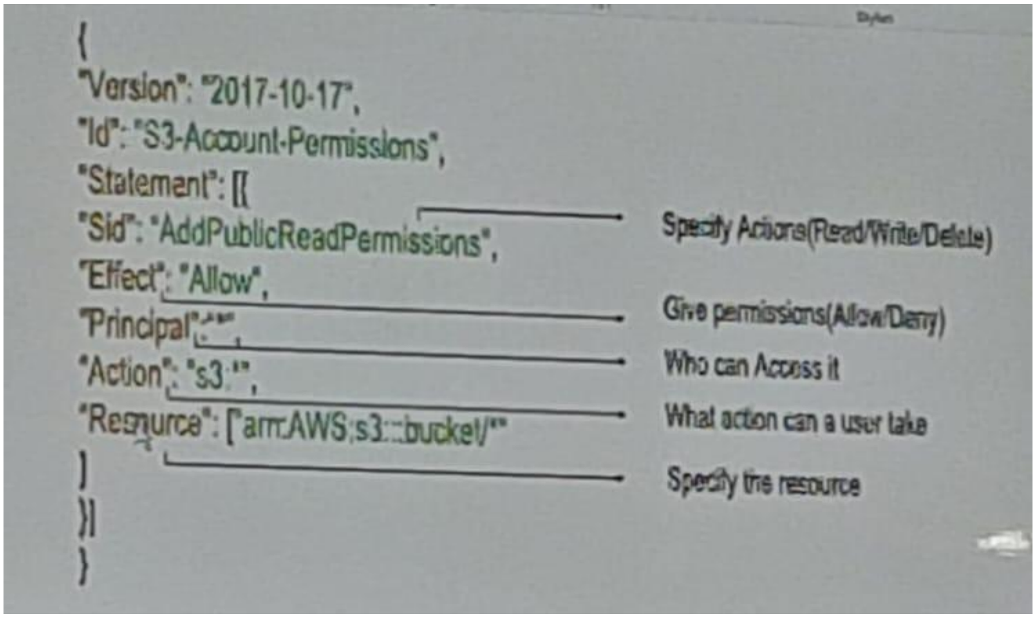
2. custom Managed policy:

(It can be modified) Some Managed policies that you create and Managed in your Aws account.

3- Inline policy :

(policy used one person uses) one policies that you add directly to a single user, group, or sale .It is Principle a one-to-one relationship with

JSON FOR MEET OF CUSTOM MANGED POLICY



```
{
"Version": "2017-10-17",
"Id": "S3-Account-Permissions",
"Statement": [{
"Sid": "AddPublicReadPermissions",
"Effect": "Allow",
"Principal":"*",
"Action": "s3:*",
"Resource": ["arn:AWS:s3:::bucket/*"
]
}]
}
```

Specify Actions(Read/Write/Delete)

Give permissions(Allow/Deny)

Who can Access it

What action can a user take

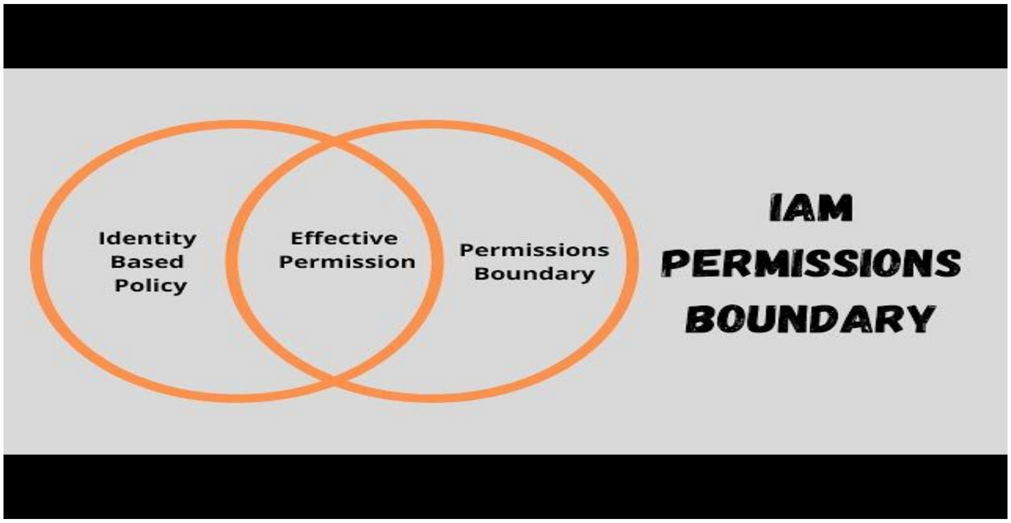
Specify the resource

Resource-based policies

Resource-based policies are attached to a resource.

PERMISSION BOUNDARY

A permissions boundary is an advanced feature for using a managed policy to set the maximum permissions that an identity-based policy can grant to an IAM entity.



What is password policy

Minimum password length of 8 characters and a maximum length of 128 characters. Minimum of three of the following mix of character types: uppercase, lowercase, numbers, and non-alphanumeric character (! @ # $ % ^ & * ( ) _ + - = [ ] { } | ') Not be identical to your AWS account name or email address.

What is MFA

AWS multi-factor authentication (MFA) is an AWS Identity and Access Management (IAM) best practice that requires a second authentication factor in addition to user name and password sign-in credentials. You can enable MFA at the AWS account level for root and IAM users you have created in your account.

WHAT IS ROLES

You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources
And user should know the roles address and roles should know the user address.

How to create roles

Step1:create role and click 'aws account'.

Step2: next , add policy.

Step3: roles name.

Step4: create role.

What is trusted account?

The Trusted accounts page allows you to automatically create IAM roles that are required in order to utilize specific features and capabilities.

(user account)

What is trusting account?

The trusting account owns the resource to be accessed and the trusted account contains the users who need access to the resource.

(roles account)

What is CLI

Command line interface

Step for CLI

Install the CLI verison2.0

And go command prompt

Aws configure

Access key:

Secret Access Key:

Default region name [None]:

Default output format [None]:

What is region

Each AWS Region is a separate geographic area. Each AWS Region has multiple, isolated locations known as Availability Zones.

There is 32 region .

What is data center

A data center is a physical location that stores computing machines and their related hardware equipment.

What is availability zone

Distinct locations within an AWS Region that are engineered to be isolated from failures in other Availability Zones.

There is 102 Availability Zones.

Different iam roles and resource base policy

Unlike an identity-based policy for a role, a resource-based policy specifies who (which principal) can access that resource. Use a role as a proxy when you want to access resources in another account that do not support resource-based policies.

Role trust relationships

1 Create the role

2 and that id click the ‘trust relationships select edit

And give the ARN number and update the trust relationship.

Switch ROLE

Click the account and switch role

Account:

Role:

Display name :

And switch role
Anthor user accessing roles ,User should have the ARN number

IAM= Identity and Access Management
ARN= amazon resource number.
MFA= multi-factor authentication
CIF= Command line interface

S3

What is s3

Amazon Simple Storage Service (Amazon S3) is an object storage service offering industry-leading scalability, data availability, security, and performance.

Why s3 is global

his is because every object in a bucket can be directly accessed using an end endpoint which contains the S3 bucket name.

bucket naming convention

unique and descripitive , lowcase letters, Hyphens or Underscores, Length Limits, No IP Addresses, DNS Compliant, Avoid PII, Avoid Reserved Words, Consider Future Scalability.

What is buckets

A bucket is a container for objects

What is object

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.

What is URL

Uniform Resource Locator: a protocol for specifying addresses on the internet.

HOW TO CREATE BUCKETS

1. Choose Create bucket.

2.For Bucket name,

3.enter a name for your bucket. ...

4.For Region,

5.choose the AWS Region where you want the bucket to reside.

Uploading object

1. In the Buckets list, choose the name of the bucket that you want to upload your object to.
2. On the Objects tab for your bucket, choose Upload.
3. Under Files and folders, choose Add files.
4. Choose a file to upload, and then choose Open.
5. Choose Upload.

ACL

Amazon S3 access control lists (ACLs) enable you to manage access to buckets and objects.

OBJECT OWNERSHIP

S3 Object Ownership is an Amazon S3 bucket-level setting that you can use to control ownership of objects uploaded to your bucket and to disable or enable access control lists (ACLs).

MAKE BUCKET & OBJECT PUBLIC USING BUCKET POLICY

1. Under Buckets, choose the name of your bucket.
2. Choose Permissions.
3. Under Bucket Policy, choose Edit.
4. To grant public read access for your website, copy the following bucket policy, and paste it in the Bucket policy editor. ...
5. Update the Resource to your bucket name. ...
6. Choose Save changes.

S3 DATA ENCRYTION

Amazon S3 encrypts your data at the object level as it writes it to disks in AWS data centers and decrypts it for you when you access it.

There are two types:

1.Sse-s3

SSE-S3 is AES256 ALGORITHEM.

2.SSE-KMS – KEY MANGEMENT SERICE.

2.1.ASYMMETRIC.(PUBLIC KEY FOR ENCRYTION,PRIVATE KEY FOR DECRYTION).

2.2.SYMMETRIC.(it s single key for both).

3.SSE-C- CILENT.

HOW TO CREATE ENCRYTION S3 OBJECT USING “KMS”SERVICE.

1. Open the Amazon S3 console.
2. Choose the bucket that you want to use for objects encrypted by AWS KMS.
3. Choose the Properties view.
4. Choose Default encryption, then select AWS-KMS.
5. Under AWS KMS key, choose your AWS KMS Key.

6. Under Bucket Key, choose Enable. ...
7. Choose Save.

IAM user:

1.And user can permission s3 read only.

2.user can not access data file and it can be encryption and root user can add IAM user to KMS.

3.the IAM user can access the file and open it.

KMS- KEY MANGEMENT SERICE

AWS KMS generates, encrypts, and decrypts data keys.

S3 DATA CONSISTENCY MODEL

1.read-after-write consistency for PUTS of new object.

2.euentual consistency over write PUTS and DELETS

PUTS

The PUT request operation is used to add an object to a bucket.

GET

The GET request operation is used to rewrite and delete object to a bucket

STATIC WEBSITE HOSTING

Static websites deliver HTML, JavaScript, images, video and other files to your website visitors. Static websites are very low cost, provide high-levels of reliability, require almost no IT administration, and scale to handle enterprise-level traffic with no additional work.

CREATE OF STATIC WEBSITE HOSTING

Download The CCS free temples in google

And extract files and folder.

Step 1: Create a bucket

Step 2: Enable static website hosting

Step 3: Edit Block Public Access settings

Step 4: Add a bucket policy that makes your bucket content publicly available

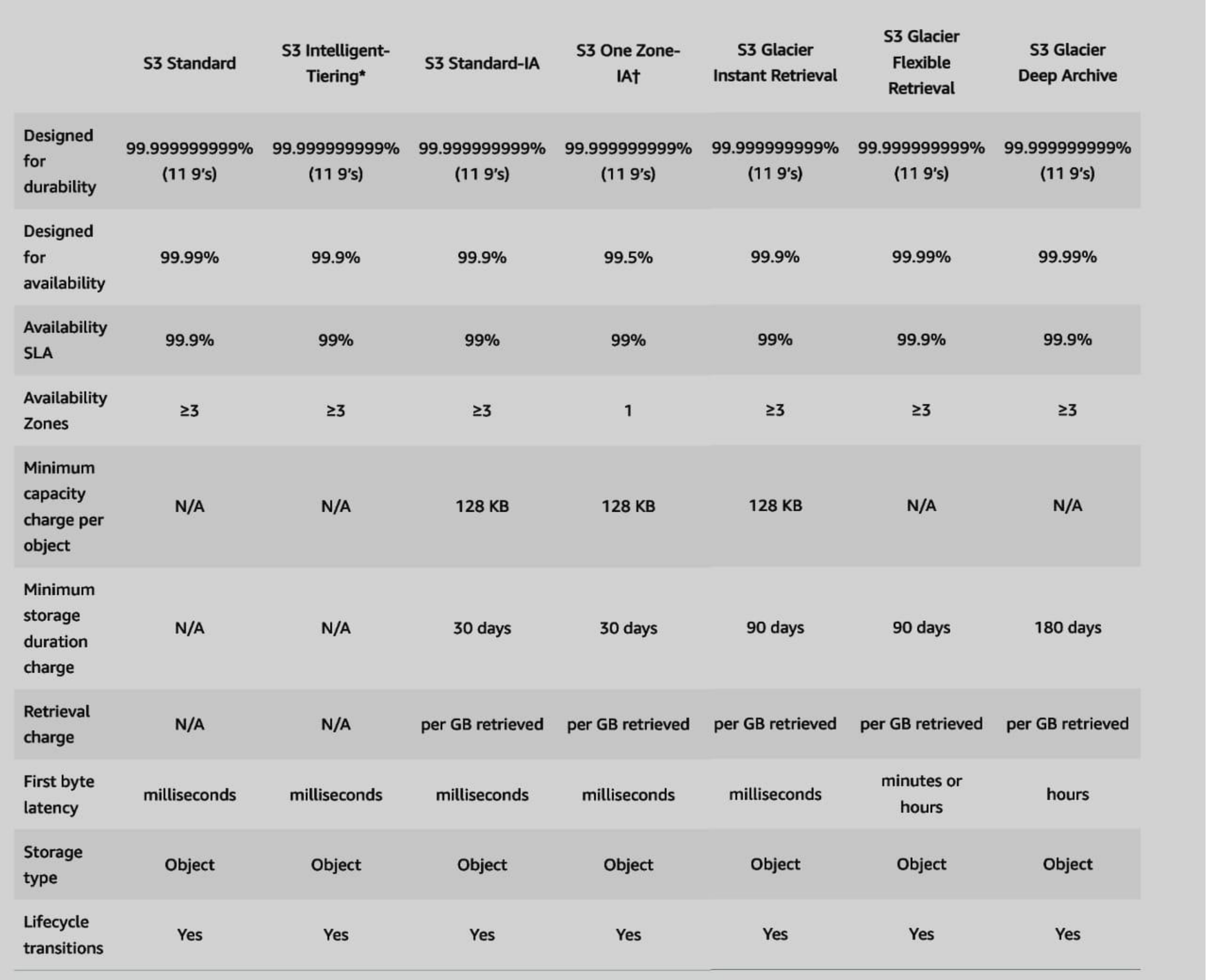
Step 5: Configure an index document

Step 6: Configure an error document

Step 7: Test your website endpoint

Step 8: Clean up

S3 STORAGE CLASS



	S3 Standard	S3 Intelligent-Tiering*	S3 Standard-IA	S3 One Zone-IA†	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval	S3 Glacier Deep Archive
Designed for durability	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)
Designed for availability	99.99%	99.9%	99.9%	99.5%	99.9%	99.99%	99.99%
Availability SLA	99.9%	99%	99%	99%	99%	99.9%	99.9%
Availability Zones	≥3	≥3	≥3	1	≥3	≥3	≥3
Minimum capacity charge per object	N/A	N/A	128 KB	128 KB	128 KB	N/A	N/A
Minimum storage duration charge	N/A	N/A	30 days	30 days	90 days	90 days	180 days
Retrieval charge	N/A	N/A	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved
First byte latency	milliseconds	milliseconds	milliseconds	milliseconds	milliseconds	minutes or hours	hours
Storage type	Object	Object	Object	Object	Object	Object	Object
Lifecycle transitions	Yes	Yes	Yes	Yes	Yes	Yes	Yes

S3 Standard (S3 Standard)

s3 Standard offers high durability, availability, and performance object storage for frequently accessed data.

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering)

Is the first cloud storage that automatically reduces your storage costs on a granular object level by automatically moving data to the most cost-effective access tier based on access frequency, without performance impact, retrieval fees, or operational overhead.

Amazon S3 Standard-Infrequent Access (S3 Standard-IA)

S3 Standard-IA is for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval charge.

Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA)

S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed.

Amazon S3 Glacier Instant Retrieval

Amazon S3 Glacier Instant Retrieval is an archive storage class that delivers the lowest-cost storage for long-lived data that is rarely accessed and requires retrieval in milliseconds

Amazon S3 Glacier Flexible Retrieval (Formerly S3 Glacier)

S3 Glacier Flexible Retrieval delivers low-cost storage, up to 10% lower cost (than S3 Glacier Instant Retrieval), for archive data that is accessed 1—2 times per year and is retrieved asynchronously.

Amazon S3 Glacier Deep Archive

S3 Glacier Deep Archive is Amazon S3's lowest-cost storage class and supports long-term retention and digital preservation for data that may be accessed once or twice in a year.

LIFE CYCLE RULE(storage class rules)

An S3 Lifecycle configuration is an XML file that consists of a set of rules with predefined actions that you want Amazon S3 to perform on objects during their lifetime.

Steps for life cycle rule

1.create a bucket .

2.upload object –management create a life cycle rule.

3.save a life cycle can enable the process.

OBJECT LOCK

S3 Object Lock blocks permanent object deletion during a customer-defined retention period

governance mode:

Object Lock can help prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely.

compliance mode:

In compliance mode, a protected object version can't be overwritten or deleted by any user, including the root user in your AWS account

Create for object lock:

1. Create a new bucket with Object Lock enabled.
2. And upload the object properties object lock enable and default retention mode choose the mode governance, compliance and set default retention period and save change.
3. And show vision we cannot delete object there the retention periods end
4. .**governance mode** :Root user or any user that has higher privileges can delete the file during its retention period
5. **Compliance:** None of the users including the root user can delete the file during its retention period.

OBJECT LEGAL HOLD

a legal hold prevents an object version from being overwritten or deleted.

SERVER ACCESS LOGGING

Server access logging provides detailed records for the requests that are made to an Amazon S3 bucket. Server access logs are useful for many applications.

STEPS OF SERVER ACCESS LOGGING

1.create a two buckets files1,files2.

2.files1 properties ,server access logging edit and enable ,target bucket select files2 and save change .

3.upload a files in files1,and and files2 can show the file1 action of files and date and time.

REPLICATION

Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets.

1.SSR-same region replication.

2.CRR-cross region replication.

SSR

SRR helps you address data sovereignty and compliance requirements by keeping a copy of your data in a separate AWS account in the same region as the original.

CRR

S3 Cross-Region Replication (CRR) is used to copy objects across Amazon S3 buckets in different AWS Regions.

Steps for SSR replication:

1.create a two bucket object1,object2.

2.object1 ,management, replication rules and create replication rules.

3.enter rules name ,choose a rules scope –apple to all object in the bucket, destination- choose a bucket in this account , and choose the object2, IAM role-create new role, save .

4.upload a files in object1,and the object2 can replication object1 files.

CRR

All the steps are same SRR and region only can be change.

TRANFER ACCERIERATION

Amazon S3 Transfer Acceleration is a bucket-level feature that enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration is designed to optimize transfer speeds from across the world into S3 buckets.

URL- Uniform Resource Locator

ACL- access control lists

CRR-Cross region replication

SRR-same region replication

Sse-s3-simple storage serivce

SSE-KMS – KEY MANGEMENT SERICE.

SSE-C-client

AES256-Advanced Encryption Standard.

EC2-Elastic Compute Cloud

WHAT IS EC2

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud.

It create a instances and it resource.

WHAT IS AMI

An Amazon Machine Image (AMI) is a supported and maintained image provided by AWS that provides the information required to launch an instance. You must specify an AMI when you launch an instance. You can launch multiple instances from a single AMI when you require multiple instances with the same configuration. You can use different AMIs to launch instances when you require instances with different configurations.

WHAT IS INSTANCES

An Amazon EC2 instance is a virtual server in Amazon's Elastic Compute Cloud (EC2) for running applications on the Amazon Web Services (AWS) infrastructure.

Who to launch instances with these AMI

A.LINUX

1: choose launch instance.

2: choose an Amazon Machine image (AMI), find an Amazon Linux 2 AMI at the top of the list and choose select

3: the list and choose Select

4. In Step 2: Choose an Instance Type, choose Next: Configure Instance Details

5. In Step 3: Configure Instance Details, provide the following information: Leave Number of instances at one

6.And choose the network and For Subnet, choose a default subnet in any Availability Zone.

7. Choose Next: Add Storage

8. Name your instance and choose Next: Configure Security Group

9. Select the check box for the key pair that you created, and then choose Launch Instances.

CMD COMMENT:

1.And go to the document and go to CMD.

2. In cmd type " ssh –i key-pair file name.pem ec2-user@public ip."

B.UBUNTU

1. All step are create instances and select ubuntu AMI .and step are same

CMD COMMENT:

1.And go to the document and go to CMD.

2. In cmd type " ssh –i key-pair file name.pem ubuntu user@public ip.

C. window :

1. All step are create instances and select window(AMI) and step are same .

FOR WINDOW WE WANT TO BY REMOTE DESKTOP CONNECTION.

1.go to rdc(REMOTE DESKTOP CONNECTION) and give the instances public ip address .

2.username as a administrator and connect .

3.next go to instance – select the instance and connect – RDP client – and get password .

4. select the key-pair file and decrypted the password and password will show .

5. and give the password to RDC and connect.

EBS(Amazon Elastic Block Store)

Amazon EBS allows you to create storage volumes and attach them to Amazon EC2 instances. Once attached, you can create a file system on top of these volumes, run a database, or use them in any other way you would use block storage.

What is volume

The user volume is meant for your users to store their data in. In the case of a rebuild of the WorkSpace the root volume gets reverted back to default whereas the users data is persistent.

All instance have the volume part and we went to increase the store part of the instance like a pen drive or it part

How to create volume

1.create instances and click volume and create volume

2. volume type we be general purpose SSD(gp3)-size(of the volume it min 1 and max 16384)-availability zone (set the zone of instance which have).

3.and click create volume .

Volume will create successfully ,we went attach the volume to instance

1.Click action and select attach volume .

2.Select instance and attach volume .

Connect CMD
Lsblk - for list the volume of instance
Sudo su - change the root user
File –s /dev /xvdf - this can see the data of files and data mean it empty.
Mkfs.ext4 /dev/xvdf - it format the volume.
Mkdir /text - it will create a direct of folder.
Cd text/ - it will go inside of the folder.
Cat >text - write same data in the file.
Ctrl c – it will out the file.
Mount /dev/xvdf/text - to conneting volume to the instances
Lsblk - to view the volume.

And volume can attach any instance and zone can be same.

Snapshots

A snapshot is a base feature for creating backups of your EBS volumes. A snapshot takes a copy of the EBS volume and places it in Amazon S3, where it is stored redundantly in multiple Availability Zones. The initial snapshot is a full copy of the volume; ongoing snapshots store incremental block-level changes only.

In volume we can create a snapshots and attach it and it is AZ specific(Availability Zones)

How to create snapshots

1.volume – action-create snapshots – description give name – and size(GIB)we cannot min of previous volume set that can give more that-snapshot can be create .

2.same step for attach the volume and CMD command .

And snapshots have recycle bin

Recycle bin

If you have access to the account that owns the snapshot, then you can delete it and store the snapshoot for retention period end it.

create recycle bin

1.snapshot –recycle bin-EBS snapshoot-create retention rule-name of rule –period of rules-create retention rule.

2.and set the rule 30days we can use the snapshot till the period end.

Securely copying any file - from your local machine to remote machine.

1.we went create instance of Linux AMI .

2.go to CMD and type "cp -i Downloads\key-pair name.pen downloads\file name.txt ec2-user@public ip:/home/ec2-user.

3.and go to CMD and check it

Sudo su

Cd/

Ls

Cd home/

Ls

Cd ec2-user

Ls

4.And the file view there .

EFS(Amazon Elastic File System)

Amazon Elastic File System (EFS) is designed to provide server less, fully elastic file storage that lets you share file data without provisioning or managing storage capacity and performance.

security group

A security group controls the traffic that is allowed to reach and leave the resources that it is associated with. For example, after you associate a security group with an EC2 instance, it controls the inbound and outbound traffic for the instance.

How create EFS:

1.first we create security group :

1.1 security group – name of SG - description type "allow ssh access to developers" – inbound rule – type ssh source type anywhere – add roules – type http source types anywhere.

1.2 and click create sg

2.create instances :

2.1 create the instance – name-AMI-keypair - and select the subnet zone a – firewall security – select the sg we create – create instances.

We wait create 2 instances like 2.1

3.create EFS:

3.1 Select EFS- click create EFS – name of efs –click customize-next-network access select the zone create in instances and give the SG we create –next-create EFS.

4.connet the instances :

CMD COMMENTS OF LUNIX

```
Ssh –i keypair.pem ec2-user@public ipv4

Yes

Sudo su

Mkdir efs

Yum install –y amazon –efs-utils
```

Go to EFS and attach the efs copy the comments and pate it

```
Ls
Cd efs
Touch 1 2 a b
Ls
Cat >data.txt
Ctrl c
Ls
```

The 1 instances can connect EFS and 2 instances also connect like this and we wait remove the data.txt in 2 instances and see the 1 instances can show the same output.

EFS IN UBUTU :

Same in instances can create like LINUX and security group also same and we wants to change the AMI , key pair .

CMD COMMENTS FOR UBUNTU

```
 Ssh –i keypair.pem UBUNTU user@public ipv4
Mkdir efs
sudo apt-get update
sudo apt-get -y install git binutils
git clone https://github.com/aws/efs-utils
cd /path/efs-utils
./build-deb.sh
```

sudo apt-get -y install ./build/amazon-efs-utils*deb

Go to EFS and attach the efs copy the comments and pate it

Ls

Cd efs

Touch 1 2 a b

Ls

Cat >data.txt

Ctrl c

Ls

The 1 instances can connect EFS and 2 instances also connect like this and we wait remove the data.txt in 2 instances and see the 1 instances can show the same output.

WEBHOSTING APACHO AND NGINX

APACHO:FOR LINUX

As a Web server, Apache is responsible for accepting directory (HTTP) requests from Internet users and sending them their desired information in the form of files and Web pages. Much of the Web's software and code is designed to work along with Apache's features.

UBUNTU NGINX:FOR

NGINX Ingress Controller is flexible, powerful, easy-to-use, and can be quickly deployed for advanced security, resilience, and scalability in your container environment. Ideal for all environments – from dev testing to production – it turns your AWS clusters into production-grade application delivery powerhouses.

CREATE OF APACHO:

1.create a instances – ec2-instance name of instances - AMI linux- key pair – and select allow ssh traffic from the internet , allow https traffic from the internet , allow http traffic from the internet – create instances.

2.Connect the instances cmd:

```
Ssh –I keypair.pem ec2-user@public ip

Sudo su

Cd  /var

Ls

Yum install httpd –y

Ls

Cd www

Ls

Cd html

Systemctl start httpd

Systemctl status httpd

Go to google and css templates free copy the link address

Wget past the link address

Ls

Unzip name of template
```

```
Rm –I palani.html

Mv –f /*/var/www/html/

Ls

C ..
```

And copy the public ip in google run it.

NGINX:FOR UBUNTU

1.create a instances – ec2-instance name of instances - AMI ubuntu- key pair – and select allow ssh traffic from the internet , allow https traffic from the internet , allow http traffic from the internet – create instances.

2.Connect the instances CMD:

```
Ssh –I keypair.pem ubuntu user@public ip

Sudo su

Cd  /usr

Yum install nginx –y

Systemctl start nginx

Systemctl status nginx

Cd  share/

Ls

Cd nginx

Cd html
```

Go to google and css templates free copy the link address

```
Wget past the link address

Ls

Unzip name of template

Rm –I palani.html

Mv –f /*/var/www/html/

Ls

C ..
```

And copy the public ip in google run it.

IAM ROLE FOR 2 SERVICES COMMUNICATING WITH EACH OTHER ACCESSING S3 FROM EC2

1.create EC2 instances and s3 bucket.

2.create IAM ROLE - aws service-use case “EC2”- policy “s3full access – my role name of IAM role-create role.

3.EC2 select the instances and click action- security-modification IAM role select my role .

4.next click instances and connect it

CMD commands:

```
Sudo su

Aws s3 ls
```

USERDATA SHELL SCRIPT

Ubuntu-nginx

```
 #!bin/bash

apt-get update

apt-get install nginx -y

service nginx start

echo "this is $(hostname) address" > /var/www/html/index.html
```

(b careful abt spaces).

Linux-Apache

```
 #!bin/bash

yum update -y

yum install httpd -y

systemctl start httpd

echo "this is $(hostname) address" > /var/www/html/index.html
```

AUTOSCALING :

AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to setup application scaling for multiple resources across multiple services in minutes.

CREATE AUTOSCALING:

1. security group – name of sg- description type “allow ssh access to developers” – inbound rule – type ssh source type anywhere – add roules – type http source types anywhere.

2.lanch templates-name of templates-description “a prod webserver for myapp” – AMI select linux-instance type – keypair-security group select existing security group - advanced details-user data

```
#!bin/bash

yum update -y

yum install httpd -y

systemctl start httpd

echo "this is $(hostname) address" > /var/www/html/index.html
```

create launch template.

3.autoscaliing – name of auto template – launch template select we create – next- network give two AZ- a,b-next-change only seconds 60 give-desicped capacity 1 ,min 1,mix 6-next-next-review page-create auto scaling- do dynamic scaling police – target tracking –CPU-30-80seconds.

4. next go instances and copy the public ip and past google the webpage can run.

5. connect the instances CMD COMMANDS

```
Sudo su

Yum update –y

Yum install stress

Stress –c 5

Top
```

6.stress command for increase the use of the website it can 40 percentage we get new instances run it mix is 6 instances we create .

UNBUTU IN AUTO SCALING :

1.security group and lanch instances are same change the AMI and user data

UBUNTU CMD COMMANDS

```
#!bin/bash

apt-get update
```

```
apt-get install nginx -y

service nginx start

echo "this is $(hostname) address" > /var/www/html/index.html
```

AUTO SCALING is all so same .

2.connets is instances – cmd

```
Sudo su

Apt-get update

Apt-get install stress
```

WINDOWS: AUTO SCALING

1.security group and lanch instances are same change the AMI

2. FOR WINDOW WE WANT TO BY REMOTE DESKTOP CONNECTION.

2.1.go to rdc(REMOTE DESKTOP CONNECTION) and give the instances public ip address .

2.2.username as a administrator and connect .

2.3.next go to instance – select the instance and connect – RDP client – and get password .

2.4. select the key-pair file and decrypted the password and password will show .

2.5. and give the password to RDC and connect.

3. the windows can open and go to notepad and type same data and save it and go file and click double time the will running and cpu utilis come 40 percentages .

4.the new instances can be run.

ALB(AMAZON LOAD BALANCER)

Elastic Load Balancing (ELB) is a load-balancing service for Amazon Web Services (AWS) deployments. ELB automatically distributes incoming application traffic and scales resources to meet traffic demands.

TYPES OF ALB

1.Classic Load Balancers .

2.Application Load Balancer.

3.Network Load Balancer.

Classic Load Balancers:

Classic Load Balancer provides basic load balancing across multiple Amazon EC2 instances and operates at both the request level and connection level. Classic Load Balancer is intended for applications that are built within the EC2-Classic network.

Application Load Balancer:

An Application Load Balancer makes routing decisions at the application layer (HTTP/HTTPS), supports path-based routing, and can route requests to one or more ports on each container instance in your cluster. Application Load Balancers support dynamic host port mapping.

Network Load Balancer

Network Load Balancer is optimized to handle sudden and volatile traffic patterns while using a single static IP address per Availability Zone. It is integrated with other popular AWS services such as Auto Scaling, Amazon EC2 Container Service (ECS), Amazon Cloud Formation, and AWS Certificate Manager (ACM).

CREATE Classic Load Balancers:

1. security group – name of sg- description type “allow ssh access to developers” –inbound rule –type ssh source type anywhere –add roules –type http source types anywhere.

2.Instances:

2.1 ec2-1- AMI select linux-instance type –keypair-security group create sg –ssh,http,anywhere - advanced details-user data

```
#!bin/bash

yum update -y

yum install httpd -y

systemctl start httpd

echo "this is $(hostname) address" > /var/www/html/index.html
```

2.2 ec2-2 - AMI select linux-instance type –keypair-security group select exiting group - advanced details-user data

```
#!bin/bash

yum update -y

yum install httpd -y

systemctl start httpd

echo "this is $(hostname) address"  > /var/www/html/index.html
```

3 . load balancer:

3.1 – name of lb-network mapping select the az –security group, select the security group –add instances select the instances- create load balancer .

Load balancer: state-active.

Lb: copy the dns name past in google web and it can run .

Create Application load balancer

1. security group – name of sg- description type “allow ssh access to developers” –inbound rule –type ssh source type anywhere –add roules –type http source types anywhere.

2.Instances:

2.1 ec2-1- AMI select linux-instance type –keypair-security group create sg – ssh ,http,anywhere - advanced details-user data

```
#!bin/bash

yum update -y

yum install httpd -y

systemctl start httpd

echo "this is $(hostname) address" > /var/www/html/index.html
```

2.2 ec2-2 - AMI select linux-instance type –keypair-security group select exiting group - advanced details-user data

```
#!bin/bash

yum update -y

yum install httpd -y

systemctl start httpd

echo "this is $(hostname) address"  > /var/www/html/index.html
```

3.target group:

3.1 choose a target type.instances – target group name – available instances .select the all instances and click include as pending below - create target group . (check the heath status)

4. **LOAD BALANCER**:

4.1 create load balancer and select application load balancer create.

4.2 name of lb-network mapping select the (az) –security group, select the security group –listeners and rooting.select a target group - create load balancer .

Load balancer: status-active.

Target group : target – health status –healthy.

Load balancer: copy the DNS name past in google web and it can run .

We can SSH (CONNECT) the Instances 3 types

1 CDM

2 AWS source

3 putty and putty gen

What is putty

PUTTY is most commonly used: as a File Transfer Protocol PUTTY can connect to a remote machine through SSH. SSH (Secure shell) is a protocol that allows a secure connection. In this way, a PC can securely send and receive data from a remote server.

WHAT IS PUTTY GEN

PuTTYgen is an key generator tool for creating SSH keys for PuTTY. It is analogous to the ssh-keygen tool used in some other SSH implementations. The basic function is to create public and private key pairs. PuTTY stores keys in its own format in .

Vpc- Virtual private clouds

What is Virtual private clouds (VPC)

A VPC is a virtual network that closely resembles a traditional network that you'd operate in your own data center. After you create a VPC, you can add subnets.

what is Subnets

A subnet is a range of IP addresses in your VPC. A subnet must reside in a single Availability Zone. After you add subnets, you can deploy AWS resources in your VPC.

What are public and private subnets in AWS?

Public subnet

The subnet has a direct route to an internet gateway. Resources in a public subnet can access the public internet.

Private subnet

The subnet does not have a direct route to an internet gateway. Resources in a private subnet require a NAT device to access the public internet.

What is IP addressing

You can assign IP addresses, both IPv4 and IPv6, to your VPCs and subnets. You can also bring your public IPv4 and IPv6 GUA addresses to AWS and allocate them to resources in your VPC, such as EC2 instances, NAT gateways, and Network Load Balancers.

What is IPV4

IPv4 stands for Internet Protocol version 4. It is the underlying technology that makes it possible for us to connect our devices to the web. Whenever a device accesses the Internet, it is assigned a unique, numerical IP address such as 99.48. 227.227.

WHAT IS IPV6

IPv6 is the newest version of internet protocol formulated by the IETF, which helps identify and local endpoint systems on a computer network and route online traffic while addressing the problem of IPv4 address depletion due to prolonged internet use worldwide.

What is Routing

Use route tables to determine where network traffic from your subnet or gateway is directed.

what is internet gate ways

An Internet Gateway is a network connecting device/appliance that can be used to connect two devices in two different networks implementing different networking protocols and overall network architecture. In other words, a gateway is a node on a network that serves as an entrance to another network.

Classes of IPV4

- Class A (0.0.0.0 - 127)
- Class B (128.0.0.0.0-191)
- Class C (192.0.0.0.0 - 223)
- Class D (224.0.0.0.0 - 239)
- Class E (240.0.0.0.0 -255)

Private & public range

	Public IP Range	Private IP Range
Class A	1.0.0.0 to 127.0.0.0	10.0.0.0 to 10.255.255.255
Class B	128.0.0.0 to 191.255.0.0	172.16.0.0 to 172.31.255.255
Class C	192.0.0.0 to 223.255.255.0	192.168.0.0 to 192.168.255.255

How to create VPC to instances

VPC:

Create vpc – resource to create (VPC) - name of the VPC(myvpc) – IPV4 CIDR (10.0.0.0/16) – create VPC.

SUBNET:

Create subnet – VPC ID select the vpc we created(myvpc) – subnet setting – name of the subnet (my subnet) – select availability zone we wait (a) – IPV4 subnet CIDR block (10.0.1.0/24) – if we wait more subnets in this vpc click add new subnet .

INSTANCES:

Create instances – name of the instances (myec2)- AMI(AMAZON LINUX) – keypairs(mykey) – network settings EDIT (select the VPC(myvpc) and subnets AZ(a) and auto sign public ip(ENABLE) - security groups (create SG (SSH , anywhere) and (ALL ICMP-IPV4 , anywhere) – create instances .

INTERNET GATEWAYS:

Create internet gateways – name IGW (my gateway) – Create internet gateways and attach to VPC .

Go and select internet gateways and action select attach toVPC .

ROUTE TABLES:

In route table the we not create it is as default we create subnets and we name your route (my route) and edit route and add route – destination (0.0.0.0/0) target (internet gateway and select the IGW "we create") and edit subnet associations – available subnets (select the subnets we create (my subnet)).

NAT GATEWAY:

A NAT gateway is a Network Address Translation (NAT) service. You can use a NAT gateway so that instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances.

BASTION HOST OR JUMP SERVER

A Bastion Host (or a jump server) is a dedicated computer used to access infrastructure resources and helps compartmentalize them. From a security perspective, a Bastion host is the only node in the network exposed for external

IN NAT GATEWAY

We create public and private subnets for single VPC and we create 2 instance public and private and we connect the public instances and with key pair we SSH to private instance.

HOW TO CREATE NAT GATEWAY FOR VPC

VPC:

Create vpc – resource to create (VPC) - name of the VPC(myvpc) – IPV4 CIDR (10.0.0.0/16) – create VPC.

SUBNET:

Create subnet – VPC ID select the vpc we created(myvpc) – subnet setting – name of the subnet (PUBLIC SN) – select availability zone we wait (a) – IPV4 subnet CIDR block (10.0.1.0/24) – if we wait more subnets in this vpc click add new subnet – name of the subnet (PRIVATE SN) – select availability zone we wait (b) – IPV4 subnet CIDR block (10.0.2.0/24)

INSTANCES:

Create instances

PUBLIC:

name of the instances (PUBLIC EC2) -AMI(AMAZON LINUX) – keypairs (mykey) – network settings EDIT (select the VPC(myvpc) and select the public subnets AZ(a) and auto sign public ip(ENABLE) - security groups (create SG (SSH , anywhere) and (ALL ICMP-IPV4 , anywhere) – create instances .

PRIVATE:

name of the instances (PRIVATE EC2) -AMI(AMAZON LINUX) – keypairs (mykey) – network settings EDIT (select the VPC(myvpc) and select the private subnets AZ(b) and auto sign public ip(DISENABLE) - security groups (create SG (SSH , anywhere) and (ALL ICMP-IPV4 , anywhere) – create instances .

INTERNET GATEWAYS:

Create internet gateways – name IGW (my gateway) – Create internet gateways and attach to VPC .

Go and select internet gateways and action select attach toVPC and attach it.

ROUTE TABLES:

In route table the we not create it is as default we create subnets and we name your route (PUBLIC) and edit route and add route – destination (0.0.0.0/0) target (internet gateway and select the IGW “we create”) and edit subnet associations – available subnets (select the subnets we create (PUBLIC SN)) .

CREATE ROUTE FOR PRIVATE SN

Name of routes as (PRIVATE) – select the VPC (MY VPC) – create route table - and edit route and add route – destination (0.0.0.0/0) target (NAT gateway and select the NAT “we create”) and edit subnet associations – available subnets (select the subnets we create (PRIVATE SN)).

NAT GATEWAY

Name of nat gateway (my ngw) – subnet (select the public subnet (psn) – connectivity type(public) – click elastic ip allocation id – create nat gateway.

AND CONNECT THE PUBLIC INSTANCES :

CDM COMMENTS :

Ssh –i mykey.pem ec2-user@public ip

Yes

Ping 8.8.8.8

Vi private.pem – (is the comments for notepad)

And copy the keypairs and past it

Ec2 –shift- : -wq – (to exit the notepad)

Ls

Chmod 400 private.pem

```
Ls –l
Ssh  –i private.pem ec2-user@private ip
```

NAT INSTANCES

A NAT instance provides network address translation (NAT). You can use a NAT instance to allow resources in a private subnet to communicate with destinations outside the virtual private cloud (VPC), such as the internet or an on-premises network.

VPC peering connection

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network.

VPC:

Vpc1

Create vpc – resource to create (VPC) - name of the VPC(vpc1) – IPV4 CIDR (192.168.0.0/16) – create VPC.

Vpc2

Create vpc – resource to create (VPC) - name of the VPC(vpc2) – IPV4 CIDR (10.0.0.0/16) – create VPC.

SUBNET:

Subnet 1

Create subnet – VPC ID select the vpc we created(vpc1) – subnet setting – name of the subnet (PUBLIC SN) – select availability zone we wait (a) – IPV4 subnet CIDR block (192.168.1.0/24) – create subnets

Subnet 2

Create subnet – VPC ID select the vpc we created(vpc2) – subnet setting – name of the subnet (PUBLIC SN) – select availability zone we wait (b) – IPV4 subnet CIDR block (10.0.1.0/24) – create subnets

INSTANCES:

Create instances

1ec2

name of the instances (VPC 1EC2) -AMI(AMAZON LINUX) – keypairs (mykey) – network settings EDIT (select the VPC(vpc1) and select the public subnets AZ(a) and auto sign public ip(ENABLE) -security groups (create SG (SSH , anywhere) and (ALL TRAFFIC , anywhere) – create instances .

2ec2

name of the instances (VPC 2 EC2) -AMI(AMAZON LINUX) – keypairs (mykey) – network settings EDIT (select the VPC(vpc2) and select the private subnets AZ(b) and auto sign public ip(ENABLE) -security groups (create SG (SSH , anywhere) and (ALL TRAFFIC , anywhere) – create instances .

INTERNET GATEWAYS:

Vpc1 igw

Create internet gateways – name IGW (vpc1 igw) – Create internet gateways and attach to VPC .

Go and select internet gateways and action select attach toVPC1 and attach it.

Vpc 2 igw

Create internet gateways – name IGW (vpc2 igw) – Create internet gateways and attach to VPC .

Go and select internet gateways and action select attach toVPC2 and attach it.

ROUTE TABLES:

VPC1 RT

In route table the we not create it is as default we create subnets and we name your route (VPC1 rt) and edit route and add route – destination (0.0.0.0/0) target (internet gateway and select the IGW "we create") and edit subnet associations – available subnets (select the subnets we create (VPC1 SN)) .

VPC 2RT

In route table the we not create it is as default we create subnets and we name your route (VPC2 rt) and edit route and add route – destination (0.0.0.0/0) target (peering connection we created ") and edit subnet associations – available subnets (select the subnets we create (VPC2 SN)) .

PEERING CONNECTION

Create peering connection – name of the pc (my pc) – select a local vpc to peer with vpc id requester (vpc1) – select another vpc to peer with account (my account) – region (this region(us-east-1)) – vpc id accepter(vpc2) – create peering connection.

AND CONNECT THE VPC1 INSTANCES :

Ssh –i mykey.pem ec2-user@ VPC1 EC2 public ip

Ping vpc2 ec2 public ip

AND CONNECT THE VPC2 INSTANCES :

```
Ssh  –i mykey.pem ec2-user@ VPC2 EC2 public ip
```

```
Ping vpc1 ec2 public ip
```

What is transit gateway

AWS Transit Gateway connects your Amazon Virtual Private Clouds (VPCs) and on-premises networks through a central hub. This connection simplifies your network and puts an end to complex peering relationships. Transit Gateway acts as a highly scalable cloud router—each new connection is made only once.

VPC:

myVpc

Create vpc – resource to create (VPC) - name of the VPC(myvpc) – IPV4 CIDR (192.168.0.0/16) – create VPC.

Vpc1

Create vpc – resource to create (VPC) - name of the VPC(vpc1) – IPV4 CIDR (10.1.0.0/16) – create VPC.

Vpc2

Create vpc – resource to create (VPC) - name of the VPC(vpc2) – IPV4 CIDR (10.2.0.0/16) – create VPC.

Vpc3

Create vpc – resource to create (VPC) - name of the VPC(vpc3) – IPV4 CIDR (10.3.0.0/16) – create VPC.

SUBNET:

My Subnet

Create subnet – VPC ID select the vpc we created(my vpc) – subnet setting – name of the subnet (MY PUBLIC SN) – select availability zone we wait (a) – IPV4 subnet CIDR block (192.168.1.0/24) – create subnets

Subnet vpc1

Create subnet – VPC ID select the vpc we created(vpc1) – subnet setting – name of the subnet (VPC1 SN) – select availability zone we wait (b) – IPV4 subnet CIDR block (10.1.1.0/24) – create subnets

Subnet vpc2

Create subnet – VPC ID select the vpc we created(vpc2) – subnet setting – name of the subnet (VPC2 SN) – select availability zone we wait (C) – IPV4 subnet CIDR block (10.2.1.0/24) – create subnets

Subnet vpc3

Create subnet – VPC ID select the vpc we created(vpc3) – subnet setting – name of the subnet (VPC3 SN) – select availability zone we wait (D) – IPV4 subnet CIDR block (10.3.1.0/24) – create subnets.

INTERNET GATEWAY

My Vpc igw

Create internet gateways – name IGW (my vpc igw) – Create internet gateways and attach to VPC .

Go and select internet gateways and action select attach to (MYVPC) and attach it.

ROUTE TABLE :

My vpc rt

In route table the we not create it is as default we create subnets and we name your route (MY VPC rt) and edit route and add route – destination (0.0.0.0/0) target (internet gateway and select the IGW “we create”) and add route - destination (10.0.0.0/8) target(transit gateway)-we create.

And edit subnet associations – available subnets (select the subnets we create (MY VPC SN))

Vpc1 rt

In route table the we not create it is as default we create subnets and we name your route (VPC1 rt) and edit route and add route – destination (192.168.0.0/16) target (transit gateway and select the TGW “we create”) and add route - destination (10.2.0.0/16) target(transit gateway) - and add route - destination (10.3.0.0/16) target(transit gateway)-we create.

And edit subnet associations – available subnets (select the subnets we create (VPC1 SN)) .

Vpc2 rt

In route table the we not create it is as default we create subnets and we name your route (VPC2 rt) and edit route and add route – destination (192.168.0.0/16) target (transit gateway and select the TGW “we create”) and add route - destination (10.1.0.0/16) target(transit gateway) - and add route - destination (10.3.0.0/16) target(transit gateway)-we create.

And edit subnet associations – available subnets (select the subnets we create (VPC2 SN)).

Vpc3 rt

In route table the we not create it is as default we create subnets and we name your route (VPC3 rt) and edit route and add route – destination (192.168.0.0/16) target (transit gateway and select the TGW "we create") and add route - destination (10.2.0.0/16) target(transit gateway) - and add route - destination (10.1.0.0/16) target(transit gateway)-we create.

And edit subnet associations – available subnets (select the subnets we create (VPC3 SN)) .

TRANSIT GATE WAY

Create transit gateway – name of the transit gateway (my tgw) – click description info (and copy the ARN and past it) – create transit gateway .

TRANSIT GATEWAY ATTACHMENT`

Attach the all myvpc ,vpc1,vpc2,vpc3

CDM COMMENTS:

Connect the myvpc

```
Ssh  -i keys.pem ec2-user@public ip

Vi luffy.pem
```

Copy the keypair file notepad and past it

```
:wq

Ls

Ls –l

Chmod 400 luffy.pem

Ls –l
```

```
Ssh  -I luffy.pem ec2-user@vpc2 private ip
Ping vpc3 private ip
```

ENDPOINTS:

A VPC endpoint enables customers to privately connect to supported AWS services and VPC endpoint services powered by AWS Private Link. Amazon VPC instances do not require public IP addresses to communicate with resources of the service. Traffic between an Amazon VPC and a service does not leave the Amazon network.

- interface endpoints
- gateway endpoints

gateway endpoints

Instances in an Amazon VPC do not require public IP addresses to communicate with VPC endpoints, as interface endpoints use local IP addresses within the consumer Amazon VPC. Gateway endpoints are destinations that are reachable from within an Amazon VPC through prefix-lists within the Amazon VPC's route table. Refer to the following figure, which shows connectivity to AWS services using VPC endpoints.

Interface endpoints

interface endpoints enable connectivity to services over AWS Private Link. These services include some AWS managed services, services hosted by other AWS customers and partners in their own Amazon VPCs (referred to as endpoint services), and supported AWS Marketplace partner services. The owner of a service is a service provider. The principal creating the interface endpoint and using that service is a service consumer.

Create gateway endpoints

VPC:

Create vpc – resource to create (VPC) - name of the VPC(myvpc) – IPV4 CIDR (10.0.0.0/16) – create VPC.

SUBNET:

Create subnet – VPC ID select the vpc we created(myvpc) – subnet setting – name of the subnet (PUBLIC SN) – select availability zone we wait (a) – IPV4 subnet CIDR block (10.0.1.0/24) – if we wait more subnets in this vpc click add new subnet – name of the subnet (PRIVATE SN) – select availability zone we wait (b) – IPV4 subnet CIDR block (10.0.2.0/24)

INSTANCES:

Create instances

PUBLIC:

name of the instances (PUBLIC EC2) -AMI(AMAZON LINUX) – keypairs (mykey) – network settings EDIT (select the VPC(myvpc) and select the public subnets AZ(a) and auto sign public ip(ENABLE) - security groups (create SG (SSH , anywhere) and (ALL ICMP-IPV4 , anywhere) – create instances .

PRIVATE:

name of the instances (PRIVATE EC2) -AMI(AMAZON LINUX) – keypairs (mykey) – network settings EDIT (select the VPC(myvpc) and select the private subnets AZ(b) and auto sign public ip(DISENABLE) - security groups (create SG (SSH , anywhere) and (ALL ICMP-IPV4 , anywhere) – create instances .

INTERNET GATEWAYS:

Create internet gateways – name IGW (my gateway) – Create internet gateways and attach to VPC .

Go and select internet gateways and action select attach toVPC and attach it.

ROUTE TABLES:

In route table the we not create it is as default we create subnets and we name your route (PUBLIC RT) and edit route and add route – destination (0.0.0.0/0) target (internet gateway and select the IGW “we create”) and edit subnet associations – available subnets (select the subnets we create (PUBLIC SN)) .

CREATE ROUTE FOR PRIVATE RT

Name of routes as (PRIVATE RT) – select the VPC (MY VPC) – create route table - and edit route and add route – destination (0.0.0.0/0) target (NAT gateway and select the NAT “we create”) and edit subnet associations – available subnets (select the subnets we create (PRIVATE SN)).

ENDPOINTS:

Create endpoints –name of the endpoints – types(gateways) – click(com.amazonaws.us-east.s3) – vpc(myvpc) – routes table(PRIVATE RT) – create endpoints.

WE WAIT ACCESS KEYS FOR AWS CONFIGURE SO

CLICK(Security credentials – access key (create access key) and download csv file.

CMD COMMENTS:

```
Sudo su

Aws configure

	Access keys:

	Secret access keys:
```

```
Aws s3 ls

Aws s3 mb s3://bucket name

Aws s3 ls

Aws s3  rb s3://bucket name

Aws s3 ls
```

Create interface endpoints

VPC:

Create vpc – resource to create (VPC) - name of the VPC(myvpc) – IPV4 CIDR (10.0.0.0/16) – create VPC.

SUBNET:

Create subnet – VPC ID select the vpc we created(myvpc) – subnet setting – name of the subnet (PUBLIC SN) – select availability zone we wait (a) – IPV4 subnet CIDR block (10.0.1.0/24) – if we wait more subnets in this vpc click add new subnet – name of the subnet (PRIVATE SN) – select availability zone we wait (b) – IPV4 subnet CIDR block (10.0.2.0/24)

INSTANCES:

Create instances

PUBLIC:

name of the instances (PUBLIC EC2) -AMI(AMAZON LINUX) – keypairs (mykey) – network settings EDIT (select the VPC(myvpc) and select the public subnets AZ(a) and auto sign public ip(ENABLE) - security groups (create SG (SSH , anywhere) and (ALL ICMP-IPV4 , anywhere) – create instances .

PRIVATE:

name of the instances (PRIVATE EC2) -AMI(AMAZON LINUX) – keypairs (mykey) – network settings EDIT (select the VPC(myvpc) and select the private subnets AZ(b) and auto sign public ip(DISENABLE) - security groups (create SG (SSH , anywhere) and (ALL ICMP-IPV4 , anywhere) – create instances .

INTERNET GATEWAYS:

Create internet gateways – name IGW (my gateway) – Create internet gateways and attach to VPC .

Go and select internet gateways and action select attach toVPC and attach it.

ROUTE TABLES:

In route table the we not create it is as default we create subnets and we name your route (PUBLIC RT) and edit route and add route – destination (0.0.0.0/0) target (internet gateway and select the IGW “we create”) and edit subnet associations – available subnets (select the subnets we create (PUBLIC SN)) .

CREATE ROUTE FOR PRIVATE RT

Name of routes as (PRIVATE RT) – select the VPC (MY VPC) – create route table - and edit route and add route – destination (0.0.0.0/0) target (NAT gateway and select the NAT “we create”) and edit subnet associations – available subnets (select the subnets we create (PRIVATE SN)).

ENDPOINTS:

Create endpoints –name of the endpoints – types(interfaces) – click(com.amazonaws.us-east.s3) –vpc(myvpc) – subnets (choose the subnets we create) - security groups (choose the sg we create) – create endpoints.

WE WAIT ACCESS KEYS FOR AWS CONFIGURE SO

CLICK(Security credentials – access key (create access key) and download csv file.

CMD COMMENTS:

```
Sudo su

Aws configure

        Access keys:

        Secret access keys:

Aws s3 ls

Aws s3 mb s3://bucket name

Aws s3 ls

Aws s3  rb s3://bucket name

Aws s3 ls
```

NACL

One of the tools in the AWS security toolkit for enabling defense-in-depth, is the Network Access Control List (NACL). A NACL is a security layer for your VPC,that acts as a firewall for controlling traffic in and out of one or more subnets.

What is inbound security rules?

Inbound firewall rules protect your network by blocking the traffic from known malicious sources and thereby prevent malware attacks, DDoS attacks, and more. Malicious traffic can be blocked based on ports, type of traffic, or IP addresses.

What are outbound rules in AWS?

Outbound means outgoing traffic from your EC2 instances. To connect internet or any browser you have to add outbound rule. For a detailed, You can even check out the details of Inbound and Outbound with the help of AWS Cloud Migration

CREATE NACL

VPC:

Create vpc – resource to create (VPC) - name of the VPC(myvpc) – IPV4 CIDR (10.0.0.0/16) – create VPC.

SUBNET:

Create subnet – VPC ID select the vpc we created(myvpc) – subnet setting – name of the subnet (PUBLIC1 SN) – select availability zone we wait (a) – IPV4 subnet CIDR block (10.0.1.0/24) – if we wait more subnets in this vpc click add new subnet – name of the subnet (PUBLIC2 SN) – select availability zone we wait (b) – IPV4 subnet CIDR block (10.0.2.0/24) click add new subnet - name of the subnet (PRIVATE SN) – select availability zone we wait (c) – IPV4 subnet CIDR block (10.0.2.0/24).

INSTANCES

PUBLIC1 EC2:

name of the instances (PUBLIC1 EC2) -AMI(AMAZON LINUX) – keypairs (mykey) – network settings EDIT (select the VPC(myvpc) and select the public subnets AZ(a) and auto sign public ip(ENABLE) - security groups (create SG (ALL TRAFFIC - anywhere) – create instances .

PUBLIC2 EC2:

name of the instances (PUBLIC1 EC2) -AMI(AMAZON LINUX) – keypairs (mykey) – network settings EDIT (select the VPC(myvpc) and select the public subnets AZ(b) and auto sign public ip(ENABLE) - security groups (create SG (ALL TRAFFIC - anywhere) – create instances .

PRIVATE:

name of the instances (PRIVATE EC2) -AMI(AMAZON LINUX) – keypairs (mykey) – network settings EDIT (select the VPC(myvpc) and select the private subnets AZ(b) and auto sign public ip(DISENABLE) - security groups (create SG (ALL TRAFFIC - anywhere) – create instances .

INTERNET GATEWAY:

Create internet gateways – name IGW (my gateway) – Create internet gateways and attach to VPC .

Go and select internet gateways and action select attach toVPC and attach it.

ROUTE TABLE:

In route table the we not create it is as default we create subnets and we name your route (MYROTE) and edit route and add route – destination (0.0.0.0/0) target (internet gateway and select the IGW "we create") and edit subnet associations – available subnets (select the subnets we create (PUBLIC1,PUBLIC2,PRIVATE SN)) .

NACL:

Create a nacl – name as (my nacl) – select the VPC (my vpc) – create nacl.

We wait to do subnet associations for all subnets public1, public2 ,private1.

And we chances also inbound and outbound rules in NACL for communication public to private.

Edit - INBOUND RULES – add new rules – rules number(1) – type (all traffic) – source (public1 sn 10.0.1.0/24) – save

Edit – OUT BOUND RULES – add new rules – rules number(2) – type (all traffic) – source (public1 sn 10.0.1.0/24) – save

CONNECT THE PUBLIC1 EC2 AND PING TO PRIVATE EC2

CMD COMMENTS:

```
Sudo su
```

```
Ping ( private ip)
```

WHAT IS DNS

The Domain Name System (DNS) turns domain names into IP addresses, which browsers use to load internet pages. Every device connected to the internet has its own IP address, which is used by other devices to locate the device.

Rule groups

A rule group is a group of transformation rules. It contains one transformation rule for each key field of the target. A transformation can contain multiple rule groups. Rule groups allow you to combine various rules.

VPC:

Create vpc – resource to create (VPC) - name of the VPC(myvpc) – IPV4 CIDR (10.0.0.0/16) – create VPC.

SUBNET:

Create subnet – VPC ID select the vpc we created(myvpc) – subnet setting – name of the subnet (PUBLIC SN) – select availability zone we wait (a) – IPV4 subnet CIDR block (10.0.1.0/24) – create subnets.

INSTANCES

PUBLIC EC2:

name of the instances (PUBLIC EC2) -AMI(AMAZON LINUX) – keypairs (mykey) – network settings EDIT (select the VPC(myvpc) and select the public subnets AZ(a) and auto sign public ip(ENABLE) - security groups (create SG (ALL TRAFFIC - anywhere) – create instances .

INTERNET GATEWAY:

Create internet gateways – name IGW (mygateway) – Create internet gateways and attach to VPC .

Go and select internet gateways and action select attach to VPC and attach it.

ROUTE TABLE

In route table the we not create it is as default we create subnets and we name your route (MYROTE) and edit route and add route – destination (0.0.0.0/0) target (internet gateway and select the IGW “we create”) and edit subnet associations – available subnets (select the subnets we create (PUBLIC).

DOMAIN LIST:

Create domain list – name as (mydomain) – descriptions(google.com) , (facebook.com) – create domain list.

RULEGROUPS :

Create the rule group – name as (my rule groups) – next – next – create rule groups .

We create rules - add rules – my roles – domain (.add my own domain list) – choose a domain list (my domain) – action (block)

Associated VPC we wait select our vpc – select (my vpc) – associate .

CONNECT THE EC2

Sudo su

Ping googel.com

It will block the google.com

Amazon RDS-Amazon Relational Database Service

WHAT IS RDS

Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the AWS Cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks.

DB instances

A DB instance is an isolated database environment in the AWS Cloud. The basic building block of Amazon RDS is the DB instance.

DB engines

A DB engine is the specific relational database software that runs on your DB instance. Amazon RDS currently supports the following engines:

- Db2
- MariaDB
- Microsoft SQL Server
- MySQL
- Oracle
- PostgreSQL

DB instance classes

A DB instance class determines the computation and memory capacity of a DB instance. A DB instance class consists of both the DB instance type and the size. Each instance type offers different compute, memory, and storage capabilities.

DB instance storage

Amazon EBS provides durable, block-level storage volumes that you can attach to a running instance. DB instance storage comes in the following types:

- General Purpose (SSD)
- Provisioned IOPS (PIOPS)
- Magnetic

AWS Regions and Availability Zones

- Amazon cloud computing resources are housed in highly available data center facilities in different areas of the world (for example, North America, Europe, or Asia). Each data center location is called an AWS Region.
- Each AWS Region contains multiple distinct locations called Availability Zones, or AZs. Each Availability Zone is engineered to be isolated from failures in other Availability Zones. Each is engineered to provide inexpensive, low-latency network connectivity to other Availability Zones in the same AWS Region.

Security

A security group controls the access to a DB instance. It does so by allowing access to IP address ranges or Amazon EC2 instances that you specify.

For more information about security groups, see Security in Amazon RDS.

Amazon RDS monitoring

There are several ways that you can track the performance and health of a DB instance. You can use the Amazon Cloud Watch service to monitor the performance and health of a DB instance. Cloud Watch performance charts are shown in the Amazon RDS console. You can also subscribe to Amazon RDS events to be notified about changes to a DB instance, DB snapshot, or DB parameter group. For more information, see Monitoring metrics in an Amazon RDS instance.

CREATE RDS(MARIADB IN LINUX)

Create database - choose a database creation method (standard create) – engine options (mariaDB) – templates (free tier) – db instances identifier (database1) – credentials settings user name (admin) –master password (palani005) , confirm password (palani005) – connectivity(dont connect to an ec2 compute resource) – network type (ipv4) – public access(yes) – vpc security group (create new) – new vpc sg name(my sg) – additional configurations database port(3306) – database authentication (password authentication) – additional configuration , initial database(mydata) – create database .

INSTANCES

name of the instances (mariaDB) -AMI(old vision of AMAZON LINUX) – keypairs (mykey) - security groups (select SG (my sg) – create instances .

SELECT THE INCSTANCES AND GO TO SECURITY AND SG WE CREATE EDIT

Add role – ssh - anywhere – and change the ip mysql/ anywhere .

CONNECT THE INSTANCES

CMD COMMENTS

```
Sudo su

Yum update –y

Yum install meriaDB-server –y

Systemctl start meriaDB

Systemctl status mariaDB

Mysql –h (entpoint) –P 3306 –u admin –p
```

Hit enter the password will be enter : palani005

mariaDB will came

\q (for quit mariadb)

UBUNTU FOR RDS(POST GRESSAL)

Create database - choose a database creation method (standard create) – engine options (post gressal) – templates (free tier) – db instances identifier (database1) – credentials settings user name (admin) –master password (palani005) , confirm password (palani005) – connectivity(don t connect to an ec2 compute resource) – network type (ipv4) – public access(yes) – vpc security group (create new) – new vpc sg name(my sg) – additional configurations database port(5432) – database authentication (password authentication) – additional configuration , initial database(mydata) – create database .

INSTANCES

name of the instances (postgressal) -AMI(AMAZON UBUNTU) – keypairs (mykey) - security groups (select SG (my sg) – create instances .

SELECT THE INCSTANCES AND GO TO SECURITY AND SG WE CREATE EDIT

Add role – ssh - anywhere – and change the ip mysql/ anywhere .

CONNECT THE INSTANCES

CMD COMMENTS

Sudo su

Sudo apt update

Sudo apt install postgressal –y

Systemctl start postgeressal

Systemctl status postgerssal

Psql - -host=(endpoint) - -port=5432 - - username=postgressal - - password - - dbname =db1

Hit enter the password will be enter : palani005

psql will came

\q (for quit psql)

AWS DYNAMO DATABASE

What is Amazon DynamoDB?

Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. DynamoDB lets you offload the administrative burdens of operating and scaling a distributed database so that you don't have to worry about hardware provisioning, setup and configuration, replication, software patching, or cluster scaling. DynamoDB also offers encryption at rest, which eliminates the operational burden and complexity involved in protecting sensitive data. For more information, see DynamoDB encryption at rest.

High availability and durability

DynamoDB automatically spreads the data and traffic for your tables over a sufficient number of servers to handle your throughput and storage requirements, while maintaining consistent and fast performance. All of your data is stored on solid-state disks (SSDs) and is automatically replicated across multiple Availability Zones in an AWS Region, providing built-in high availability and data durability.

What is the use of DynamoDB over RDS?

DynamoDB has advantages over Aurora and RDS in terms of seamless scalability, high performance, schema flexibility, automatic replication ,durability, pay-as-you-go pricing, and integrated caching (DAX). The choice depends on specific needs and workload characteristics.

CREATE DYNAMODB
1.click create table – name –parition key(mydomain) – table settings(default settings)choose it – create table.
2. select the table and go to explore item – click create item – click add new attribute.

AWS-BACKUP

What is AWS backup for?

AWS Backup is a fully-managed service that makes it easy to centralize and automate data protection across AWS services, in the cloud, and on premises. Using this service, you can configure backup policies and monitor activity for your AWS resources in one place.

Backup window

Backup windows consist of the time that the backup window begins and the duration of the window in hours. Backup jobs are started within this window. The default settings in the console are:

- **1:00 AM** local to your system's time zone (1:00 in 24-hour systems)
- **Start within** 8 hours
- **Complete within** 7 days

You can customize the backup frequency and backup window start time using a cron expression. To see the six fields of AWS cron expressions, see Cron Expressions in the Amazon Cloud Watch Events User Guide.

Template for aws backups

You can create a backup plan using the AWS Backup console, API, CLI, SDK, or an AWS Cloud Formation template.

Topics

- Creating backup plans using the AWS Backup console
- Creating backup plans using a JSON document and the AWS Backup CLI
- Backup plan options and configuration
- AWS Cloud Formation templates for backup plans

Backup vault

In AWS Backup, a backup vault is a container that stores and organizes your backups.

When creating a backup vault, you must specify the AWS Key Management Service (AWS KMS) encryption key that encrypts some of the backups placed in this vault. Encryption for other backups is managed by their source AWS services. For more information about encryption, see the chart in Encryption for backups in AWS.

On-demand backup

An on-demand backup begins to back up your resource immediately. You can choose an on-demand backup if you wish to create a backup at a time other than the scheduled time defined in a backup plan.

An on-demand backup can be used, for example, to test backup and functionality at any time.

On-demand backups cannot be used with point-in-time restore (PITR) since an on-demand backup preserves resources in the state they are in when the backup is taken, whereas PITR uses continuous backups which record changes over a period of time.

AWS ELASTIC BEAN STALK

Is Amazon Elastic Beanstalk a PAAS?

AWS Elastic Beanstalk is a fully managed service that makes it easy for developers to deploy, run, and scale web applications and services. It is a Platform as a Service (PAAS) offered by Amazon Web Services (AWS).

What is AWS Elastic Beanstalk used for?

Why AWS Elastic Beanstalk? Elastic Beanstalk is a service for deploying and scaling web applications and services. Upload your code and Elastic Beanstalk automatically handles the deployment—from capacity provisioning, load balancing, and auto scaling to application health monitoring.

Application

An Elastic Beanstalk application is a logical collection of Elastic Beanstalk components, including environments, versions, and environment configurations. In Elastic Beanstalk an application is conceptually similar to a folder.

Application version

In Elastic Beanstalk, an application version refers to a specific, labeled iteration of deployable code for a web application,

An application version points to an Amazon Simple Storage Service (Amazon S3) object that contains the deployable code, such as a Java WAR file. An application version is part of an application.

Environment

An environment is a collection of AWS resources running an application version. Each environment runs only one application version at a time, however, you can run the same application version or different application versions in many environments simultaneously. When you create an environment, Elastic Beanstalk provisions the resources needed to run the application version you specified.

PAAS

AWS Elastic Beanstalk, Google App Engine, and Adobe Commerce.

CREATE ELASTIC BEAN STALH

1. create IAM role for the policies (AWS elastic bean stack full access)name as (my –ebs).

2.CONFIGURE ENVIRONMENT – (web server environment)

Application information – (my app) name of the application-environment name (myapp.env) – plat from type(managed platform) – plat from(tomcat) – application code(sample application) – next.

3.service access – service role(use an existing service role)existing service roles (select my-ebs) – ec2 instances profile (my-ebs)-next.

4.vpc(default) - instances settings – public ip address (activation) – instances subnets (select the subnets) – ec2 security group (select default) – instances types (t3.micro) – heath reporting (enhanced) – next .

5.create the elastic bean stack .

AND THE INSTANCES WILL LANCH AND COPY THE PUBLIC IP THE APPLICATION WEB SERVED WILL RUN SUCCESS FULL.

AWS SSM- Simple Systems Manager

SSM

AWS Systems Manager (Systems Manager) was formerly known as "Amazon Simple Systems Manager (SSM)" and "Amazon EC2 Systems Manager (SSM)". The original abbreviated name of the service, "SSM", is still reflected in various AWS resources, including a few other service consoles.

How Systems Manager works

The following diagram describes how some Systems Manager capabilities perform actions on your resources. The diagram doesn't cover all capabilities. Each enumerated interaction is described before the diagram.

1. Access Systems Manager
2. Choose a Systems Manager capability
3. Verification and processing
4. Reporting
5. Systems Manager operations management capabilities

What is session-Manager

Session Manager is a fully managed AWS Systems Manager capability that lets you manage your Amazon EC2 instances through an interactive one-click browser-based shell or through the AWS CLI. You can use Session Manager to start a session with an instance in your account.

The function of the session Manager

Helps you improve your security posture by letting you close these inbound ports, freeing you from managing SSH keys and certificates, bastion hosts, and jump boxes.

What is SSM patch Manager AWS?

Patch Manager, a capability of AWS Systems Manager, automates the process of patching managed nodes with both security-related updates and other types of updates.

CREATE THE SYSTEM -MANAGER

In system-manager we use run a command

1.create IAM roles for system manger polities (AWS SSM full access)

2.**instances**:

Create instances – name of the (no-1) – AMI(LINUX) – key pairs(luffy) – security group (all traffic).

Like this we create no-2,no-3,no-4 instances .

And attaché the instances to role (action – security modify IAM role – choose the role we created –update)

3.**go to SSM and click(run command)**

Command document – select the (shell and (aws-run shell script) – command parameters(type the commands would to use)

```
Sudo su

Yum update –y

Yum install httpd –y

Systemctl start httpd
```

-target selection (choose instances manually) and select the instances we created.
Run .

CREATE SESSION MANAGER

1.create IAM role for session manager policies (amzoan SSM manged instances core)

2.**instances**:

Create instances – name of the (session ec2) – AMI(LINUX) – key pairs(luffy) – security group (all traffic).

And attaché to role (action – security modify IAM role – choose the role we created –update)

3.**go SSM and session manager**

Start session – reason for session (my-instances) – target instances (select the instances we created) wait for some time it will come .

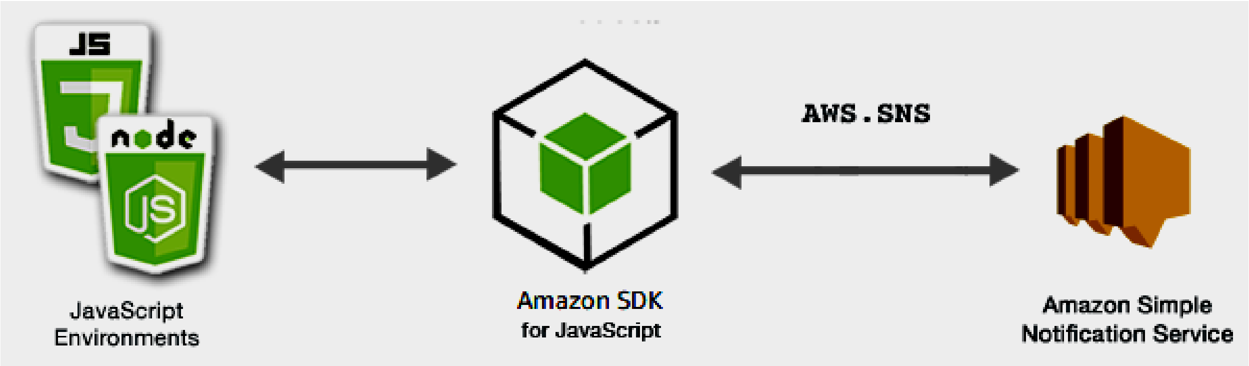
And start session.

AWS SNS – SIMPLE NOTIFICATION SERVECE

WHAT IS SNS

Amazon Simple Notification Service (Amazon SNS) is a web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients.

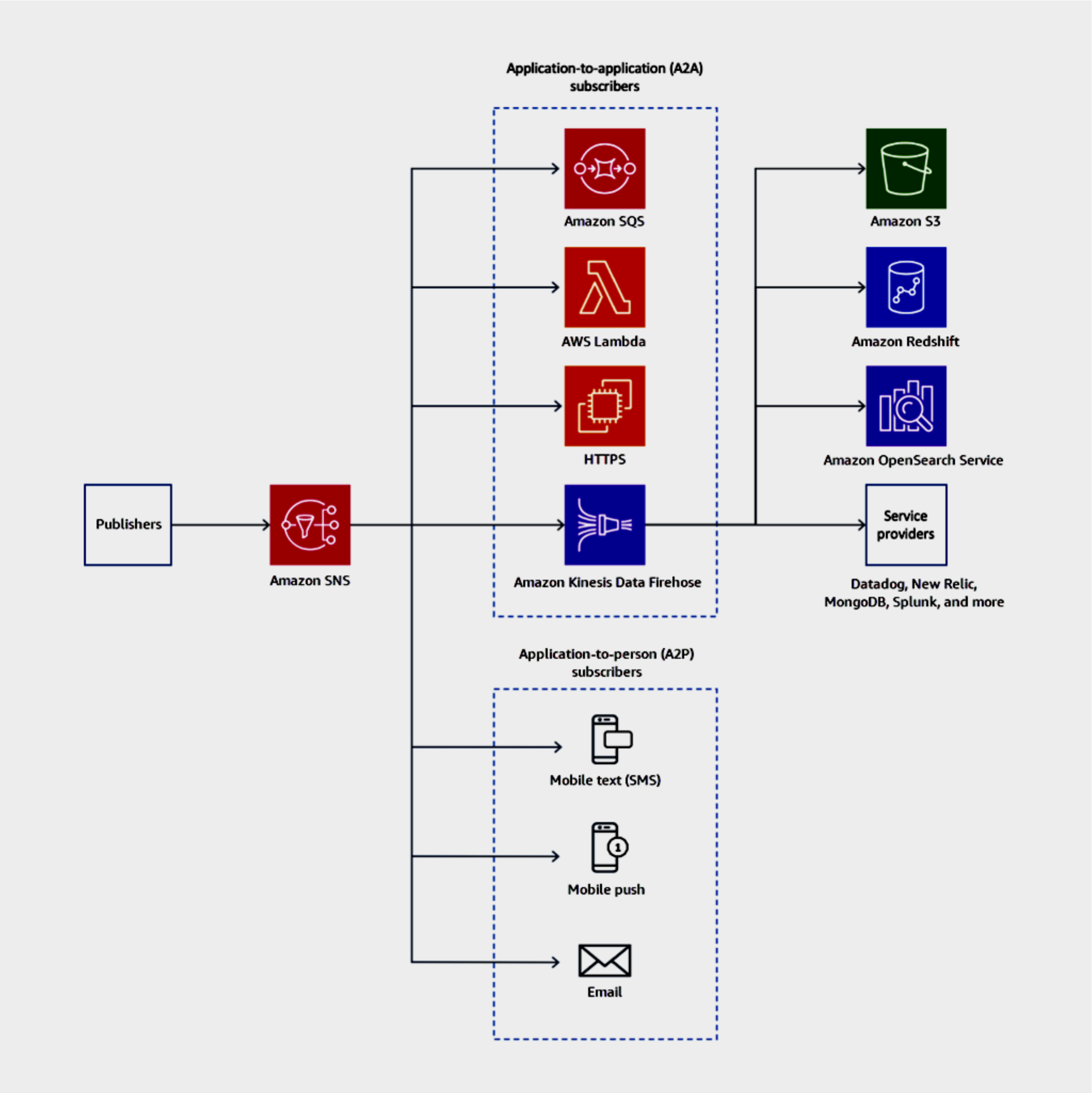
In Amazon SNS, there are two types of clients—publishers and subscribers—also referred to as producers and consumers.



What is AWS SNS push notification?

Amazon Simple Notification Service (Amazon SNS) is a managed service that provides message delivery from publishers to subscribers (also known as producers and consumers). Publishers communicate asynchronously with subscribers by sending messages to a topic, which is a logical access point and communication channel.

This is push based servies


Application-to-application (A2A) subscribers
Amazon SQS
AWS Lambda
HTTPS
Amazon Kinesis Data Firehose
Amazon S3
Amazon Redshift
Amazon OpenSearch Service
Service providers
Datadog, New Relic, MongoDB, Splunk, and more
Publishers
Amazon SNS
Application-to-person (A2P) subscribers
Mobile text (SMS)
Mobile push
Email

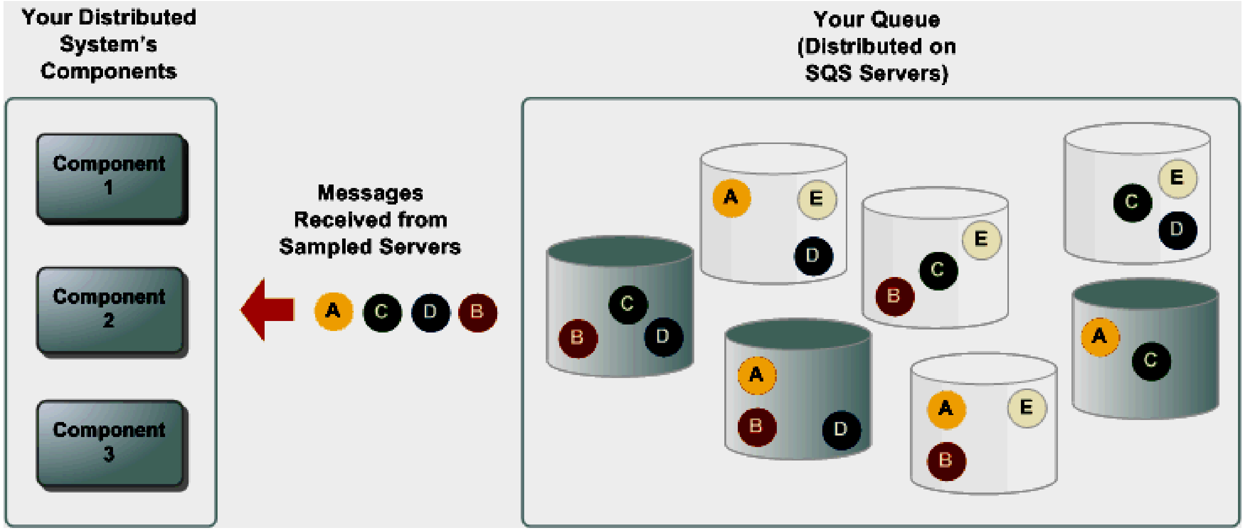
AWS SQS- Simple Queue Service

What is Amazon Simple Queue Service?

Amazon Simple Queue Service (Amazon SQS) offers a secure, durable, and available hosted queue that lets you integrate and decouple distributed software systems and components. Amazon SQS offers common constructs such as dead-letter queues and cost allocation tags. It provides a generic web services API that you can access using any programming language that the AWS SDK supports.

What is SQS polling?

Amazon SQS provides short polling and long polling to receive messages from a queue.


Your Distributed System's Components
Component 1
Component 2
Component 3
Messages Received from Sampled Servers
A
C
D
B
Your Queue (Distributed on SQS Servers)
A
E
D
C
E
B
C
E
D
C
B
D
A
B
D
A
E
B
A
C

Differences between long and short polling

Short polling occurs when the Wait Time Seconds parameter of a Receive Message request is set to 0 in one of two ways:

- The Receive Message call sets Wait Time Seconds to 0.

- The Receive Message call doesn’t set Wait Time Seconds, but the queue attribute Receive Message Wait Time Seconds is set to 0.

What are the benefits of SQS?

Reliability – Amazon SQS locks your messages during processing, so that multiple producers can send and multiple consumers can receive messages at the same time. Customization – Your queues don't have to be exactly alike.

When would you use SQS?

Developers can use Amazon SQS to safely exchange messages between different software components.

AWS CLOUD TRAIL

What Is AWS Cloud Trail?

AWS Cloud Trail is an AWS service that helps you enable operational and risk auditing, governance, and compliance of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in Cloud Trail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

What AWS service logs all API requests?

IAM and AWS STS are integrated with AWS Cloud Trail, a service that provides a record of actions taken by an IAM user or role. Cloud Trail captures all API calls for IAM and AWS STS as events, including calls from the console and from API calls.

How Cloud Trail works

Cloud Trail is active in your AWS account when you create it. When activity occurs in your AWS account, that activity is recorded in a Cloud Trail event. You can view the past 90 days of recorded API activity (management events) in an AWS Region in the Cloud Trail console by going to **Event history**.

Cloud Trail trails

You can also create a Cloud Trail trail to archive, analyze, and respond to changes in your AWS resources. Trails can log Cloud Trail management events, data events, and Insights events.

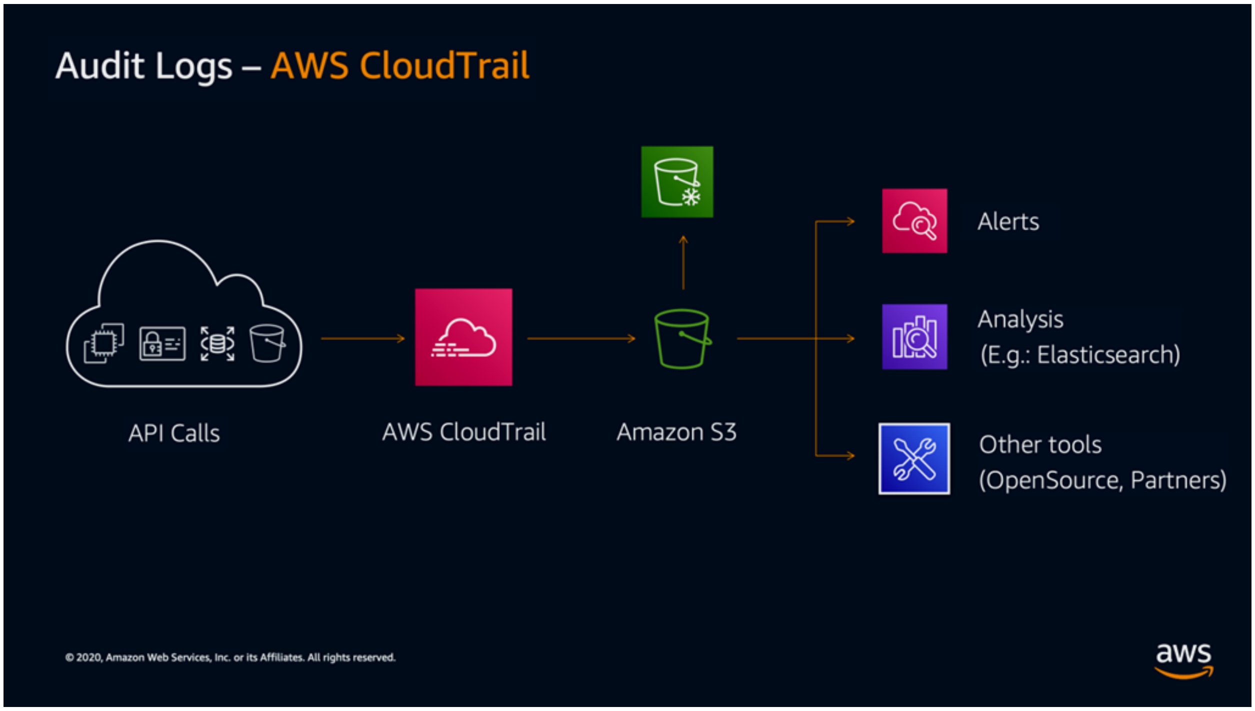
A trail is a configuration that enables delivery of events to an Amazon S3 bucket that you specify. You can also deliver and analyze events in a trail with Amazon Cloud Watch Logs and Amazon Event Bridge. You can create trails with the Cloud Trail console, the AWS CLI, or the Cloud Trail API.

Security in AWS Cloud Trail

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security of the cloud

Security in the cloud



AWS GUARD DUTY

What is AWS guard duty used for?

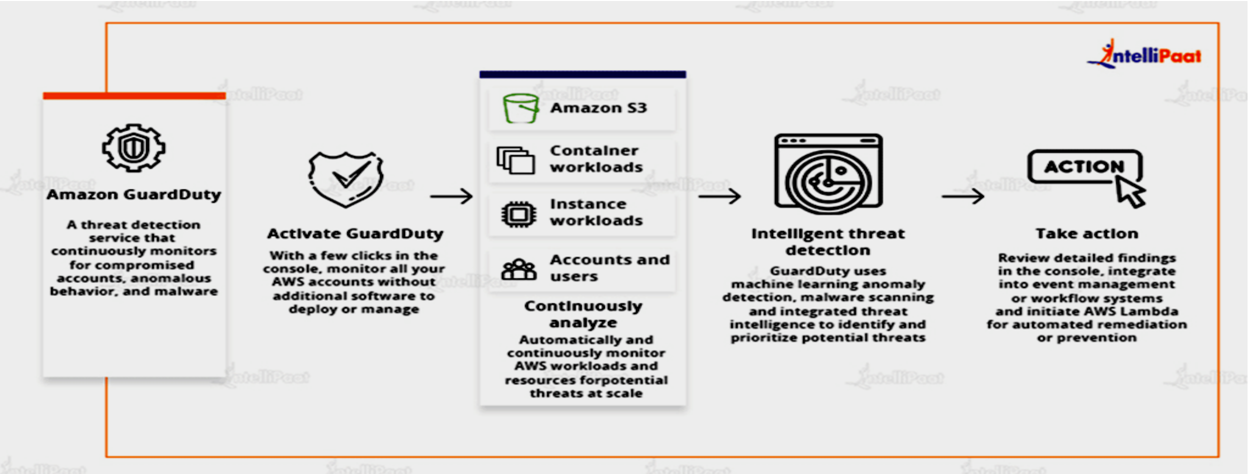
Amazon Guard Duty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.

Does Guard Duty use machine learning?

The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats.

Guard Duty RDS Protection

RDS Protection in Amazon Guard Duty analyzes and profiles RDS login activity for potential access threats to your Amazon Aurora databases (Amazon Aurora MySQL-Compatible Edition and Aurora Postgre SQL-Compatible Edition)



Amazon GuardDuty

A threat detection service that continuously monitors for compromised accounts, anomalous behavior, and malware

Activate GuardDuty

With a few clicks in the console, monitor all your AWS accounts without additional software to deploy or manage

Continuously analyze

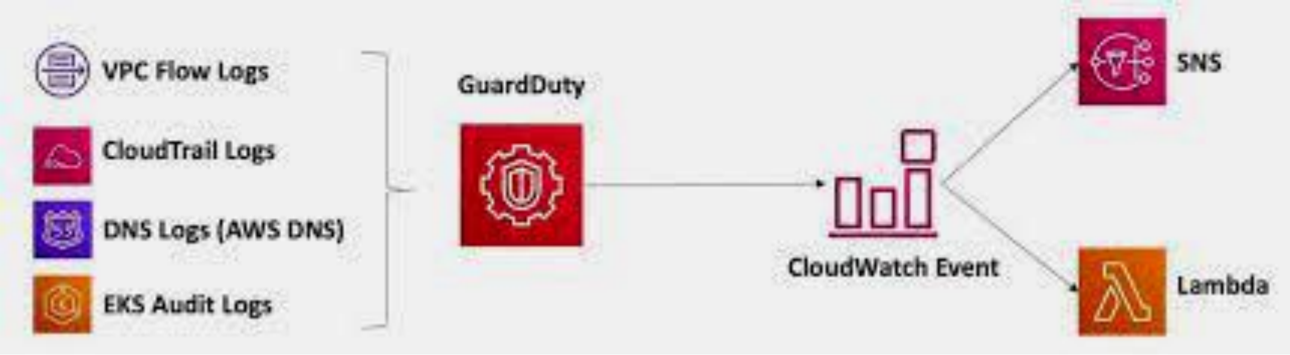
Automatically and continuously monitor AWS workloads and resources forpotential threats at scale

Intelligent threat detection

GuardDuty uses machine learning anomaly detection, malware scanning and integrated threat intelligence to identify and prioritize potential threats

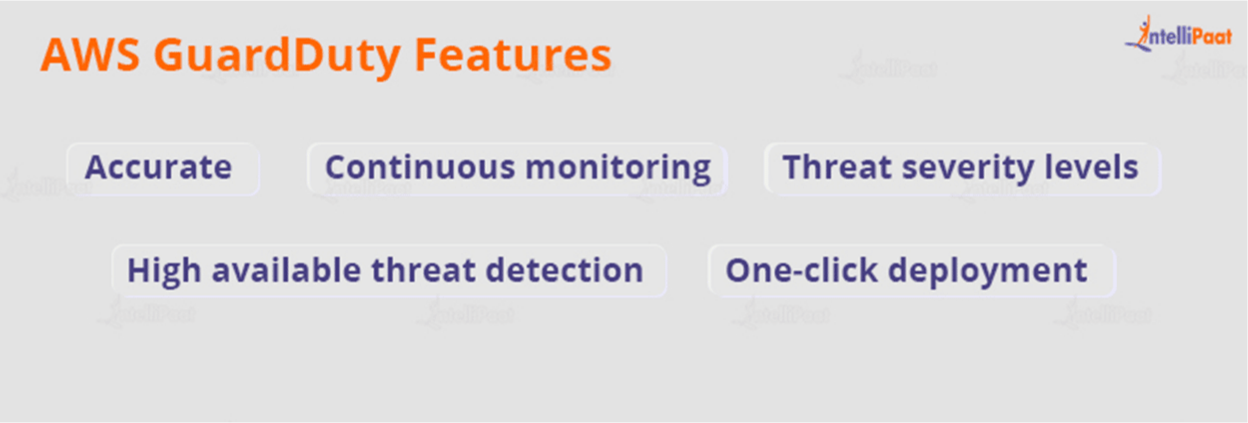
Take action

Review detailed findings in the console, integrate into event management or workflow systems and initiate AWS Lambda for automated remediation or prevention



Continuous monitoring

Amazon GuardDuty monitors and evaluates AWS account & workload data from AWS CloudTrail, VPC Flow Logs, and DNS Logs on a continuous basis.



AWS GuardDuty Features

Accurate

Continuous monitoring

Threat severity levels

High available threat detection

One-click deployment

IntelliPaat

AWS GuardDuty Use cases

- **Protect your compute workloads:** detect whether your EC2 instance is mining cryptocurrency or communicating with IP addresses and domains connected with known dangerous actors.
- **Protect your AWS credentials:** detect whether your AWS credentials are used in an unusual or suspicious manner, such as from IP addresses connected with known malicious actors, or in a manner that differs from their expected behavior.
- **Protect your data stored in Amazon S3 buckets:** identify when data stored in your Amazon S3 buckets are accessed in an unusually suspicious manner, such as when an unusual volume of items is obtained from an odd location, or when the S3 bucket is visited from IP addresses connected with known malicious actors.

AWS ROUTE 53

What is Amazon Route 53?

Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service. You can use Route 53 to perform three main functions in any combination: domain registration, DNS routing, and health checking.

What is a DNS server for the Route 53?

A DNS service such as Amazon Route 53 is a globally distributed service that translates human-readable names like www.example.com into the numeric IP addresses like 192.0. 2.1. Computers use these numbers to connect with each other.

www aws.com

www –sub level domain .
com – top level domain
aws- root

What is a sub level domain?

A sub domain name is a piece of additional information added to the beginning of a website's domain name. It allows websites to separate and organize content for a specific function — such as a blog or an online store — from the rest of your website.

Top level domain
In simpler terms, a TLD is everything that follows the final dot of a domain name. For example, in the domain name 'google.com', '.com' is the TLD. Some other popular TLDs include '.

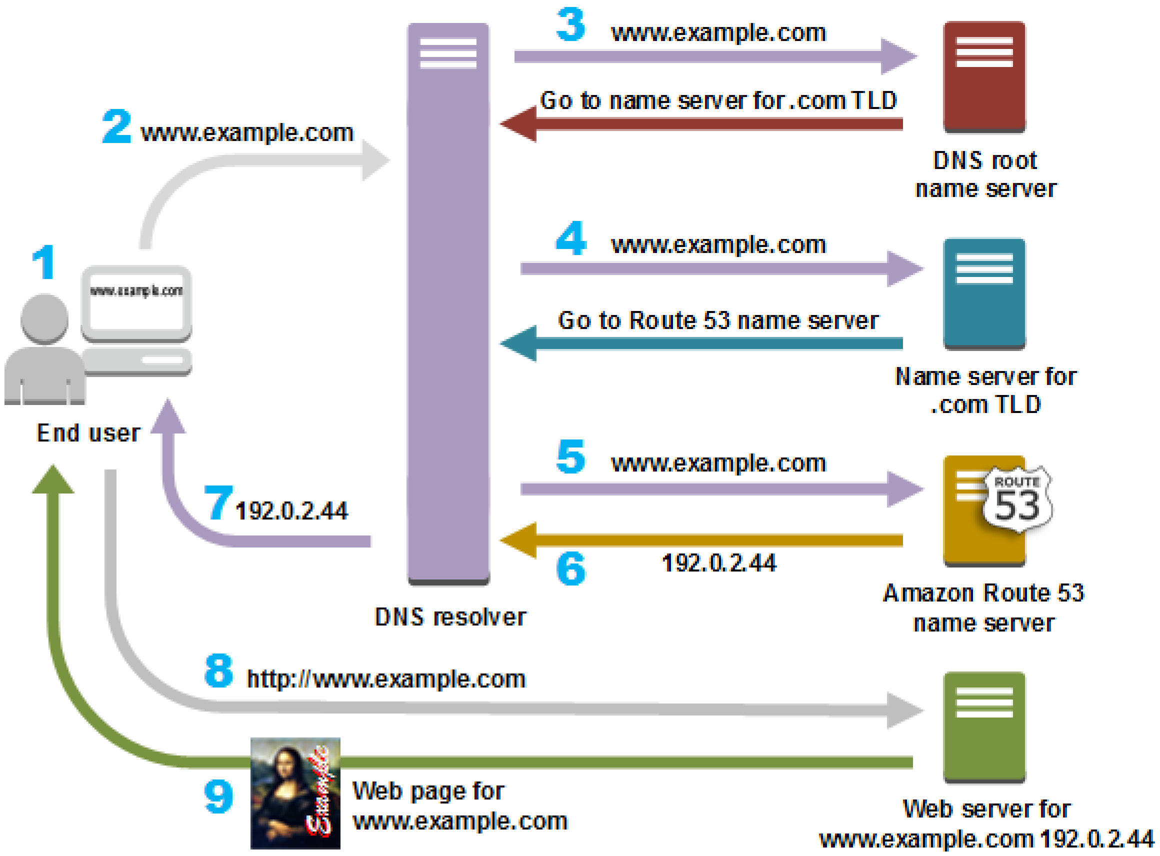
Domain Name System (DNS)

A worldwide network of servers that help computers, smart phones, tablets, and other IP-enabled devices to communicate with one another. The Domain Name System translates easily understood names such as example.com into the numbers, known as *IP addresses*, that allow computers to find each other on the internet.

See also IP address.

name servers

Servers in the Domain Name System (DNS) that help to translate domain names into the IP addresses that computers use to communicate with one another. Name servers are either recursive name servers (also known as DNS resolver) or authoritative name server.



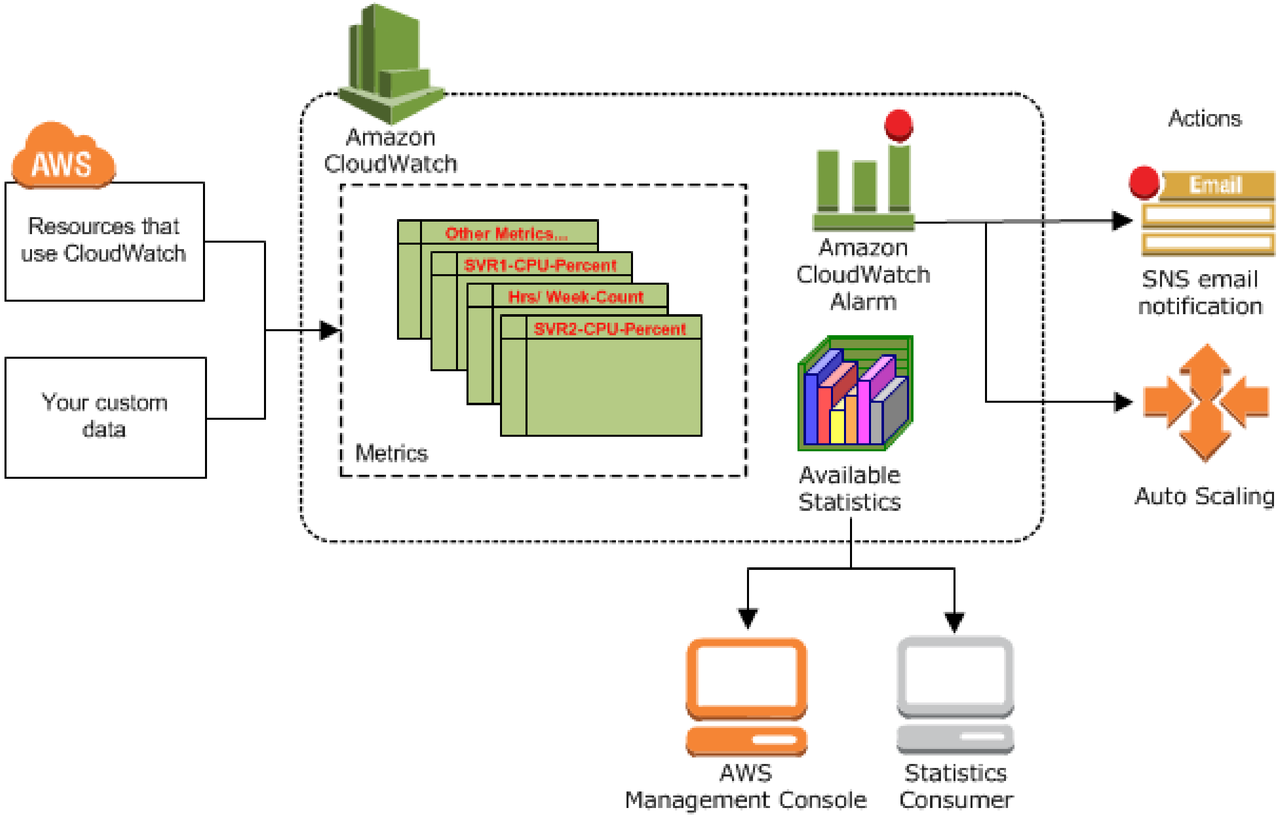
AWS -CLOUD WATCH

WHAT IS CLOUD WATCH

Cloud Watch enables you to monitor your complete stack (applications, infrastructure, network, and services) and use alarms, logs, and events data to take automated actions and reduce mean time to resolution (MTTR). This frees up important resources and allows you to focus on building applications and business value.

What is Cloud Watch vs Cloud Trail?

Cloud Watch is a monitoring service for AWS resources and applications.
Cloud Trail is a web service that records API activity in your AWS account.



Amazon Cloud Watch Logs

Amazon Cloud Watch Logs is a log aggregation and monitoring service. AWS Code Build, Code Commit, Code Deploy and Code Pipeline provide integrations with Cloud Watch logs so that all of the logs can be centrally monitored. In addition, the previously mentioned services various other AWS services provide direct integration with Cloud Watch.

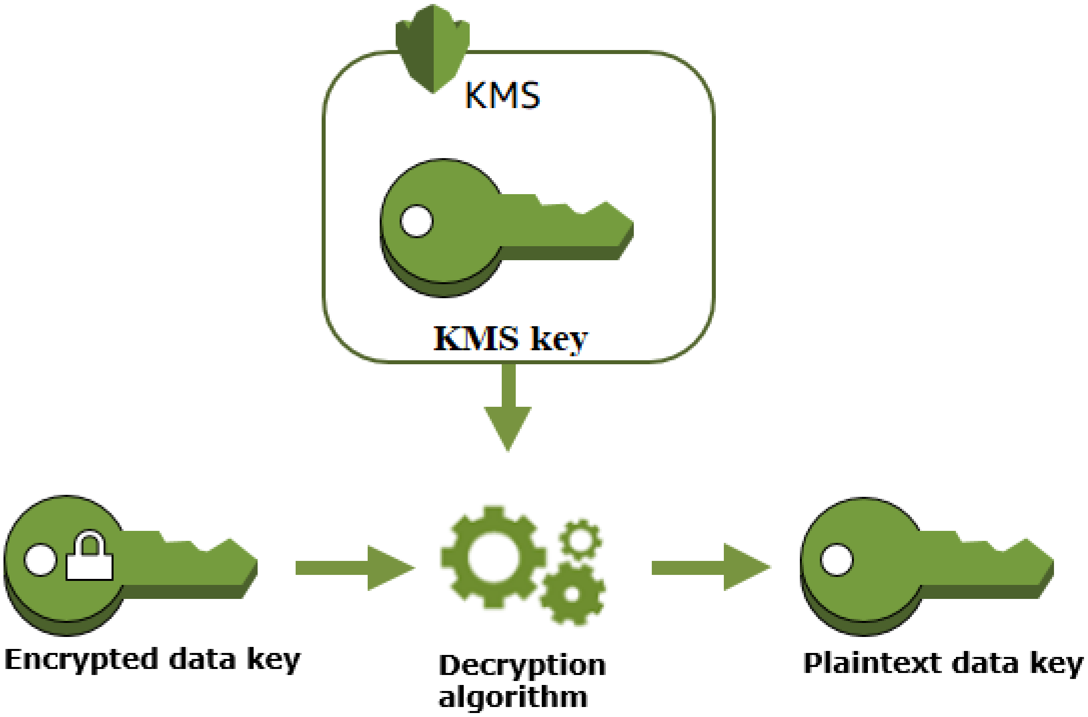
With Cloud Watch Logs you can:

- Query your log data
- Monitor logs from Amazon EC2 instances
- Monitor AWS Cloud Trail logged events
- Define log retention policy

KMS- Key Management Service

WHAT IS KMS

AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the cryptographic keys that are used to protect your data. AWS KMS uses hardware security modules (HSM) to protect and validate your AWS KMS keys under the FIPS 140-2 Cryptographic Module Validation Program.



What is data key in encryption?

In cybersecurity, a data key is a string of data representing a variable value that is used for encryption and decryption.

DECRYPTION ALGORITHEM

Decryption is a process that transforms encrypted information into its original format. The process of encryption transforms information from its original format — called plaintext — into an unreadable format — called cipher text — while it is being shared or transmitted.

What is data key used for?

In cyber security, a data key is a string of data representing a variable value that is used for encryption and decryption.

CLOUD FRONT

WHAT IS CLOUD FRONT

Amazon Cloud Front is a content delivery network operated by Amazon Web Services. The content delivery network was created to provide a globally-distributed network of proxy servers to cache content, such as web videos or other bulky media, more locally to consumers, to improve access speed for downloading the content.

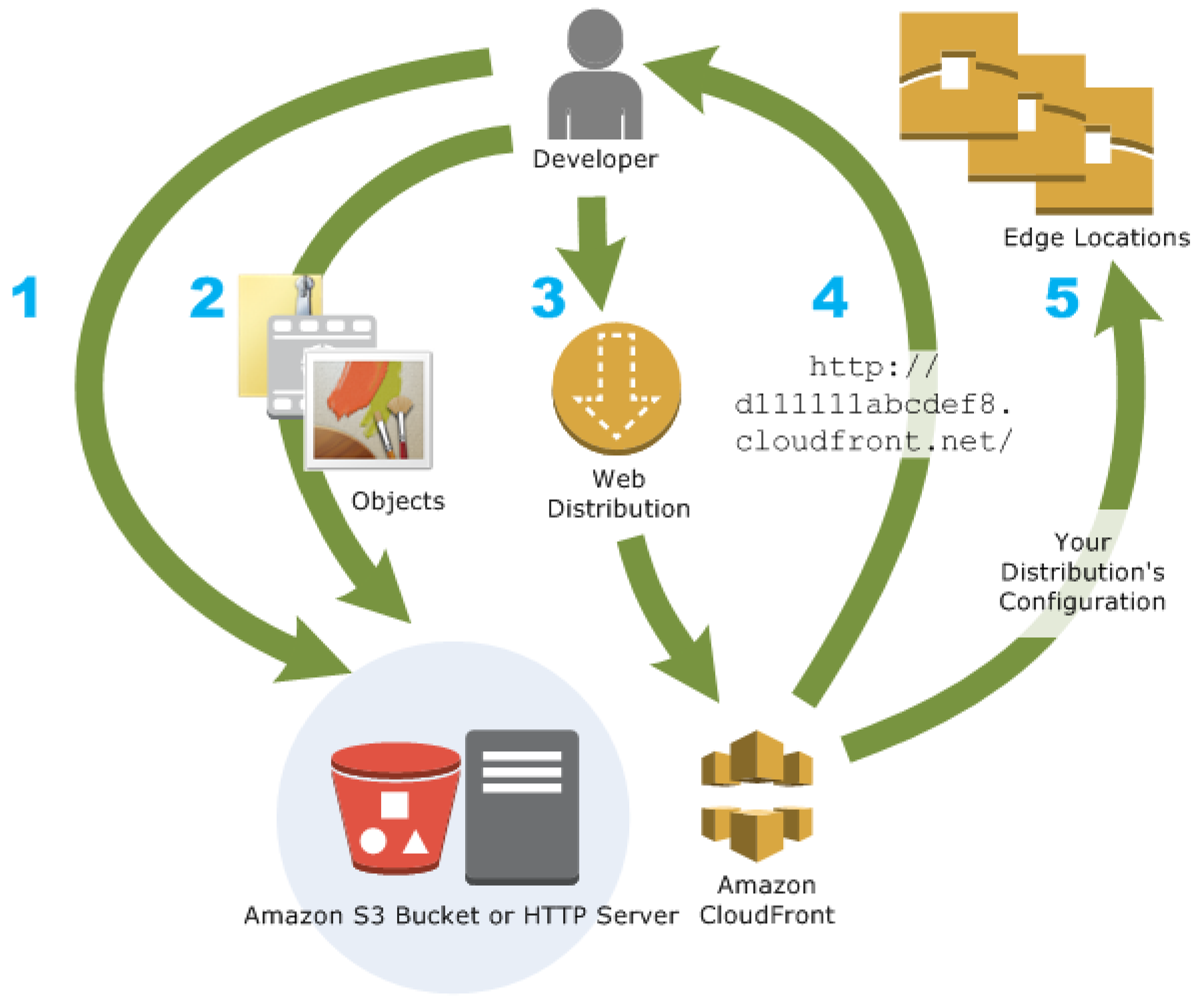
How you set up Cloud Front to deliver content

You create a Cloud Front distribution to tell Cloud Front where you want content to be delivered from, and the details about how to track and manage content delivery. Then Cloud Front uses computers—edge servers—that are close to your viewers to deliver that content quickly when someone wants to see it or use it.

Cloud Front use cases

Using Cloud Front can help you accomplish a variety of goals. This section lists just a few, together with links to more information, to give you an idea of the possibilities.

- Accelerate static website content delivery.
- Serve video on demand or live streaming video.
- Encrypt specific fields throughout system processing.
- Customize at the edge.
- Serve private content by using Lambda @ Edge customizations.



- **AWS Management Console** – The procedures throughout this guide explain how to use the AWS Management Console to perform tasks.

- **AWS SDKs** – If you're using a programming language that AWS provides an SDK for, you can use an SDK to access Cloud Front. SDKs simplify authentication, integrate easily with your development environment, and provide access to Cloud Front commands. For more information, see Tools for Amazon Web Services.

- **Cloud Front API** – If you're using a programming language that an SDK isn't available for, see the Amazon Cloud Front API Reference for information about API actions and about how to make API requests.

- **AWS Command Line Interface** – For more information, see Getting Set Up with the AWS Command Line Interface in the AWS Command Line Interface User Guide

- **AWS Tools for Windows Power Shell** – For more information, see Setting up the AWS Tools for Windows Power Shell in the AWS Tools for Windows Power Shell User Guide.

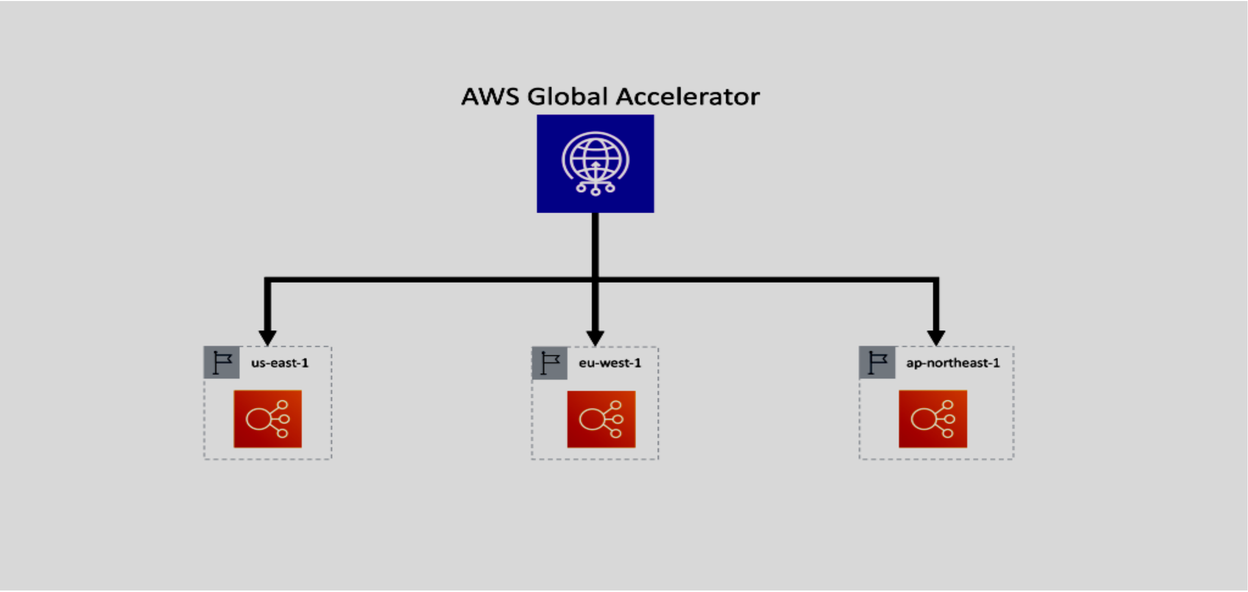
AWS - GOBAL ACCLERATION

AWS Global Accelerator (AMS SSPS)

Global Accelerator is a network layer service in which you create accelerators to improve availability and performance for internet applications used by a global audience. To learn more, see Global Accelerator.

What is the difference between Cloud Front and Global Accelerator?

Cloud Front uses multiple sets of dynamically changing IP addresses while Global Accelerator will provide you a set of static IP addresses as a fixed entry point to your applications.



What is Global Accelerator endpoint?

Global Accelerator continually monitors the health of all endpoints that are included in a standard endpoint group. It routes traffic only to the active endpoints that are healthy. If Global Accelerator doesn't have any healthy endpoints to route traffic to, it routes traffic to all endpoints in the Region.

Why does Global Accelerator have two IP addresses?

Global Accelerator for Multi Region Applications
GA simplifies this by providing just two static IP addresses that are anycast from the AWS edge locations giving a single entry point to your application regardless of how many regions it is deployed in.

AWS Cloud Shell

What is AWS Cloud Shell?

AWS Cloud Shell is a browser-based, pre-authenticated shell that you can launch directly from the AWS Management Console. You can navigate to Cloud Shell from the AWS Management Console a few different ways.

AWS - pricing calculator

What does the AWS pricing calculator do?

AWS Pricing Calculator is a free tool to use. It provides an estimate of your AWS fees and charges, but the estimate doesn't include any taxes that might apply. AWS Pricing Calculator provides pricing details for only the information you enter.

Features of AWS Pricing Calculator

- **View transparent prices** – View the calculations behind the estimated prices for your service configurations. You can view price estimates by service or by groups of services to analyze your architecture costs.
- **Use groups for hierarchical estimates** – Sort your estimates into groups to align with your architecture for clear service cost analysis.
- **Save your estimates** – Save the link to each estimate to share or revisit at a later time. Estimates are saved to the AWS public servers.
- **Export your estimates** – Export your estimates in CSV or PDF format to share locally with your stakeholders.