# AWS

## No of AWS Regions, AZ, Edge locations ?

Regions = 25

AZ = 81

Edge Locations = 121

## Alternative ways for connecting your console ?

* AWS CLI
* Session Manager

## Some AWS CLI commands

* aws ec2 describe-instances
* aws ec2 start/stop/terminate instance id
* aws s3 ls
* aws s3 cp
* aws ec2 import

## How to backup a running instance ?

* Snapshot
* AMI
* Aws Backup

## What is AWS Outpost ?

AWS Data Center on-premise.

## Issues during login to & PC If your Linux-build server getting slow down, what will you do to check ?

* MAX CPU
* MAX FILE Usage
* PEM FILE issues
* Port no not open in NACL or Security Group

## While connecting to your EC2 instances, what are the possible connection issues one might face ?

* Connection time out: Connection may time out due to long running processes or low network speed.
* Permission denied: You may be denied permission to connect to EC2 instance if the host key is not found.
* Security Group is not check the port no.

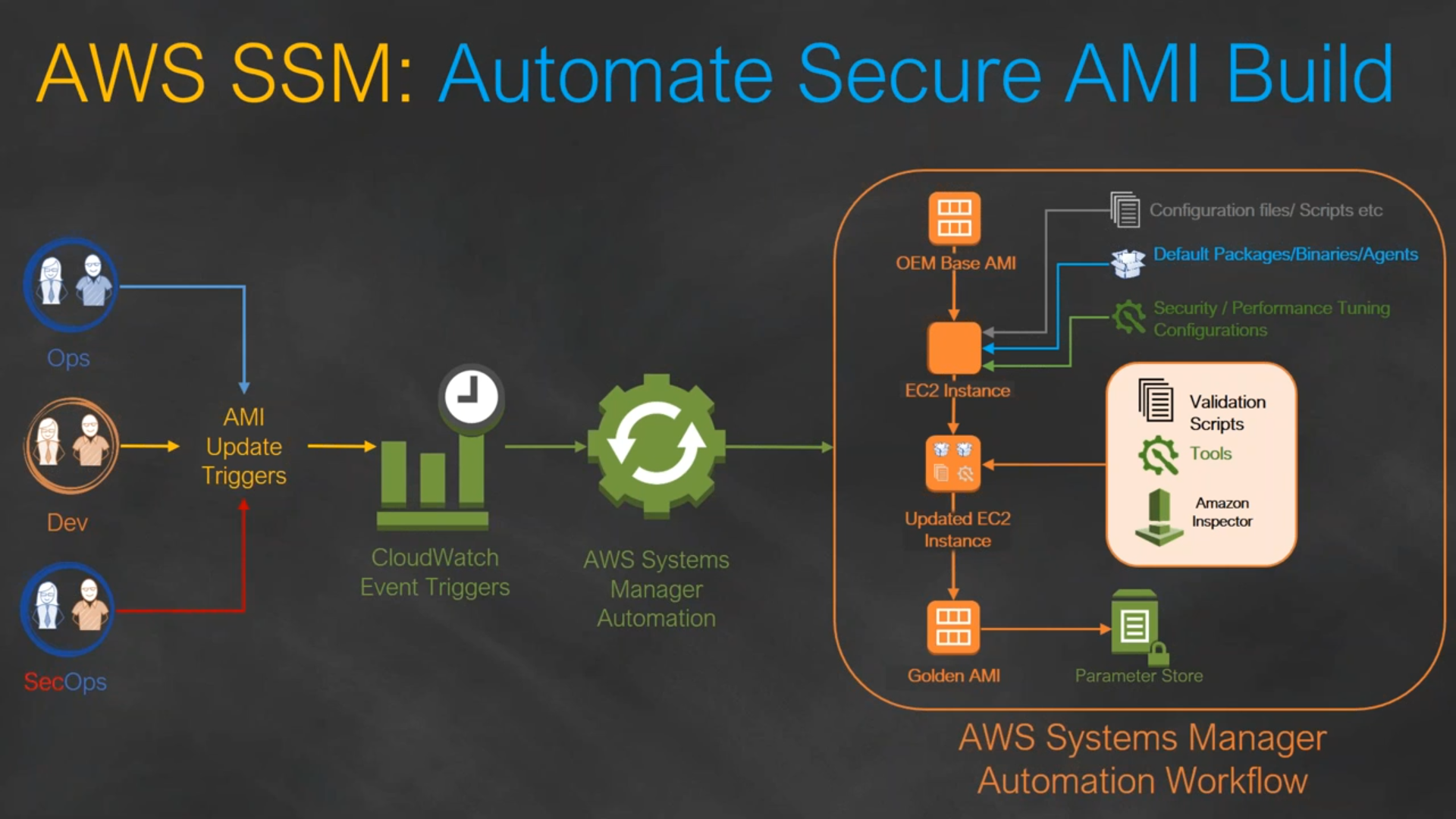
## What are the Global Services in AWS ?

* IAM
* Route53
* S3
* CloudFront

## How to automate ami update in autoscaling ?

CloudFormation or Elastic Beanstalk or CodeDeploy

## What is Systems Manager (SSM) & Golden AMI ?



Link: <https://github.com/miztiik/AWS-Demos/tree/master/How-To/setup-ami-lifecycle-management-using-ssm>

## Synchronous vs Asynchronous application ?

* A synchronous request blocks the client until operation completes
* Examples of synchronous communication are phone calls or video meetings.
* An asynchronous request doesn’t block the client i.e. browser is responsive.At that time, user can perform another operations also.
* Examples of Asynchronous communication happens when information can be exchanged independent of time. Examples of asynchronous communication are emails, online forums, and collaborative documents.

## Statefull vs Stateless Application ?

A Stateless app is an application program that does not save client data generated in one session for use in the next session with that client.

In a stateless application, different servers can be used to process different information

while in a stateful application, only one server is used to process all requests that are linked to the same state information.

A Stateful application saves data about each client session and uses that data the next time the client makes a request.

## What to do when PEM is Lost ?

We can take AMI of the instance and create a new Instance or If we need access to the particular instance withour creating a new one we should unmount the drive attach it to a different instance change the public keys in authorised keys file under .shh folder. and re mount it to the existing instance.

## Application FLow ?



Reference architecture for hosting WordPress on AWS



# EC2

## How to create AMI ?

Choose a running Instance and actions create Image. It will create a new AMI. We can also use vmie to export our onpremise VM as a AMI to the cloud.

## Types of ec2 Models ?

Cost Based : ON demand, Reserved Ec2, Spot, Dedicated

Memory Based : CPU optimised, Memory Optimised, GPU OPtimised

## t2 vs t4 ?

<https://aws.amazon.com/ec2/instance-types/>

## What is CPU credits ?

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-credits-baseline-concepts.html>

1 CPU credit = 1 vCPU \* 100% utilization \* 1 minute.

1 CPU credit = 1 vCPU \* 50% utilization \* 2 minutes

1 CPU credit = 2 vCPU \* 25% utilization \* 2 minutes

## What is EC2, S3, EBS ?

EC2 is used to Provision VM instances

S3 is a Simple Storage Service where we can store documant data upto 5TB per file size and virtually unlimited.

EBS is a volume which we attach to our EC2 instance. EBS volumes include SSD HDD Magnetic.

## EC2 vs ami ?

EC2 is a running server/instance provided by AWS. EC2 is created with the help of AMI

AMI image is a backup of an entire EC2 instance. Associated with an AMI image are EBS snapshots. AMI + Snapshot creates a EC2 Instance. we can create multiple EC2 instances with Single AMI.

AMI works in a single region only

## AMI vs Snapshot ?

Snapshot is a point in time backup of specific volume while AMI is is backup of the entire EC2 instance that might have multiple attached volumes

An EBS snapshot is a backup of a single EBS volume. ... An AMI image is a backup of an entire EC2 instance. Associated with an AMI image are EBS snapshots. Those EBS snapshots are the backups of the individual EBS volumes attached to the EC2 instance at the time the AMI image was created.

## EBS Volume Types ?

[Amazon EBS volume types - Amazon Elastic Compute Cloud](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html)

**General Purpose SSD** – Standard - gp2, gp3 - 1 GiB - 16 TiB

**Provisioned IOPS SSD** - High Input/Output - io1, io2, io2 Block Express - 4 GiB - 16 TiB

**Throughput Optimized HDD** - Big Data, Data Warehouses, log processing - st1 - 125 GiB - 16 TiB

**Cold HDD** - Scenarios where the lowest storage cost is important - sc1 - 125 GiB - 16 TiB

**Magnetic** - Workloads where data is infrequently accessed - standard - 1 GiB-1 TiB

## Volume Add & Volume Create in EC2 ?

df -h -> File system

lsblk -> Shows attached Volumes

sudo mkfs -t xfs /dev/nvme1n1 -> Formatting

sudo mkdir /data -> Create a Folder

sudo mount /dev/nvme1n1 /data -> Mount folder with Disk

## How to move EBS volume from one AZ to Another ?

We can use Snapshot to take a backup copy & Launch it as new Instance.

## Can we share AMI across Region ?

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/CopyingAMIs.html#ami-copy-steps>

AMI -> Copy AMI

## Block Instance Store ?

A block device is a storage device that moves data in sequences of bytes or bits. a temporary storage type located on disks that are physically attached to a host machine.

Instance store volumes (virtual devices whose underlying hardware is physically attached to the host computer for the instance) EBS volumes (remote storage devices)

Some Amazon Elastic Compute Cloud (Amazon EC2) instance types come with a form of directly attached, block-device storage known as the instance store. The instance store is ideal for temporary storage, because the data stored in instance store volumes is not persistent through instance stops, terminations, or hardware failures.

For data you want to retain longer, or if you want to encrypt the data, use Amazon Elastic Block Store (Amazon EBS) volumes instead. EBS volumes preserve their data through instance stops and terminations, can be easily backed up with EBS snapshots, can be removed from one instance and reattached to another, and support full-volume encryption.

## Launch Template vs Launch Configuration ?

We cant edit both the LC and LT after it has been created.

Launch Configuration are used with ASG.

Launch Template are used with creating a new EC2 instance as well as ASG. LT allows you to have multiple versions of a template.

## In-Place Deployment ?

During In-place Deployment the there will be a down time the system will be offline during the deployment. Load balancer so that each instance is deregistered during its deployment and then restored to service after the deployment is complete.

## Blue Green Deployment or Update EC2 without Downtime?

Set of Server in under Blue and Green. While updating ill change the lb to point Blue while I update the Green with Code with Latest code. After Updation change the LB to point green again.

## How is a spot Instance different from an On-demand Instance ?

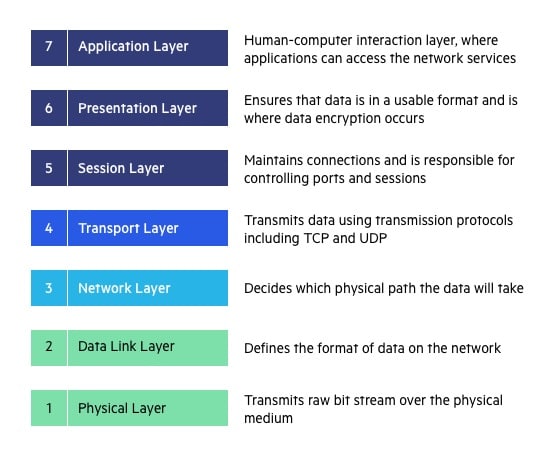
A Spot Instance is an instance that uses spare EC2 capacity that is available for less than the On-Demand price.

The instances are acquired through a bidding process in which the customer specifies a price per hour he is willing to pay.

Because Spot Instances enable you to request unused EC2 instances at steep discounts, you can lower your Amazon EC2 costs significantly. We should not use Spot instances for hosting our servers. Spot Requests is used to check on the orders

## Types of Load Balancer ?

1. Classic Load Balancer (4th 7th Layer of OSI)
2. Application Load Balancer (7th Layer of OSI)
3. Network Load Balancer -> (4th Layer of OSI) Used for Micro services / container based application
4. Gateway Load Balancer-> (3rd Layer of OSI)



## What is difference between application load balancer & classic load balancer & Network Load Balancer?

[Load balancer types - Amazon Elastic Container Service](https://docs.aws.amazon.com/AmazonECS/latest/developerguide/load-balancer-types.html)

**ELB** - ELB works at both layer 4 (TCP) and 7 (HTTP) and is the only load balancer that works in EC2-Classic. ELB only allows routing based on port number.

**ALB** - An Application Load Balancer (ALB) only works at layer 7 (HTTP). ALB can route requests to many ports on a single target. Plus, ALB can route requests to Lambda functions.

**NLB** - A Network Load Balancer (NLB) works at layer 4 (network layer)only and can handle both TCP and UDP, it uses static IP addresses and can be assigned Elastic IPs—not possible with ALB and ELB.

## What is gateway Loadbalancer (Newly Launched)

A Gateway Load Balancer operates at the third layer (network layer) of the Open Systems Interconnection (OSI) model, the network layer. It listens for all IP packets across all ports and forwards traffic to the target group.

## Is is possible to scale an Ec2 Instance vertically ?

To vertically scale an individual AWS EC2 instance up or down the instance has to be stopped, then the instance size changed, then restarted.

## Horizontal Scaling vs Vertical Scaling ?

Horizontal Scaling - Increasing the no of Instances using Auto Scaling Group

Vertical Scaling - Increasing the Power of Instance (Not available in Cloud)

## How session is maintained in LB ?

With sticky sessions, a load balancer assigns an identifying attribute to a user, typically by issuing a cookie or by tracking their IP details.

Then, according to the tracking ID, a load balancer can start routing all of the requests of this user to a specific server for the duration of the session.

## How to add Load Balancer to existing Instance ?

Open load balancer and edit targets and add your instances.

## Traffic manager vs Load balancer ?

Traffic manager is used to route traffic between regions. It works on a Global level

Load Balancer is used to route traffic inside region. Routes between instances Inside AZs

## What is Auto Scaling Group ?

ASG works based on Launch Template or Launch Configuration

Desired Value, Minimum Value, Maximum Value

AWS Auto Scaling is a service that automatically monitors and adjusts compute resources to maintain performance

As demand spikes, the AWS Auto Scaling service can automatically scale those resources, and, as demand drops, scale them back down.

## Which type of ELB is good for application load ?

Classic Load Balancer is likely to be the best choice if your routing and load-balancing needs can all be handled based on IP addresses and TCP ports. In contrast, the Application Load Balancer can address more complex load-balancing needs by managing traffic at the application level.

## Template Deployment ?

Deployment using AMI templates

# IAM

## Security in AWS ?

Assign policy to Users using IAM.

We can connect via CLI using SSH.

## What is inline policy/ managed policy/ customer managed policy ?

use managed policies instead of inline policies.

**inline policy** -> directly attached to the users/group/roles, Non-resuable

**customer managed policy** -> creates reusable object which we can apply to multiple users/groups

**aws managed policy** -> they are policies managed by aws so they will update it and manage it overtime

## Permission Boundary

<https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html>

AWS supports permissions boundaries for IAM entities (users or roles). 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. An entity's permissions boundary allows it to perform only the actions that are allowed by both its identity-based policies and its permissions boundaries.

{

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

"Statement": [

{

"Effect": "Allow",

"Action": [

"s3:\*",

"cloudwatch:\*",

"ec2:\*"

],

"Resource": "\*"

}

]

}

## Time based IAM access ?

{

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

"Statement": [

{

"Effect": "Allow",

"Action": "*service-prefix*:*action-name*",

"Resource": "\*",

"Condition": {

"DateGreaterThan": {"aws:CurrentTime": "2020-04-01T00:00:00Z"},

"DateLessThan": {"aws:CurrentTime": "2020-06-30T23:59:59Z"}

}

}

]

}

# S3

## What is S3 ?

Amazon S3 or Amazon Simple Storage Service is a service offered by Amazon Web Services that provides object storage through a web service interface.

Offering **99.999999999% (11 9’s)** of Durability

Max file size **5TB**

Max no of buckets **100** but can be increased.

## S3 Storage Classes

1. Standard
2. Intelligent Tiering
3. Standard-IA
4. One zone-IA
5. S3 Glacier
6. S3 Glacier Deep Archive
7. S3 Outpost.

## What is Glacier vs Glacier Deep Archive ?

S3 Glacier extremely low-cost cloud storage service for long-term backup.

Customers can reliably store large or small amounts of data for as little as $0.004 per gigabyte per month.

**Amazon S3 Glacier**: Expedited – 1-5 minutes, Standard – 3-5 hours, Bulk – 5-12 hours.

**Amazon S3 Glacier Deep Archive**: Expedited – Not available, Standard – within 12 hours, Bulk – within 48 hours

## How to secure s3 bucket/ What are the security available for users to access S3 ?

While creating bucket give Block Public Access to restrict Bucket access.

Using IAM, ACL, Bucket Policy

We can encrypt our data

Create CloudTrial Logs to check object level access and track

## S3 Encryption ?

objects are encrypted using server-side encryption with either **Amazon S3-managed keys (SSE-S3)** or AWS **KMS keys** stored in **AWS Key Management Service** (AWS KMS) (SSE-KMS).

## S3 Buck policy vs ACL ?

An S3 ACL is a sub-resource that's attached to every S3 bucket and object. It defines which AWS accounts or groups are granted access and the type of access.

S3 bucket policies and IAM policies define object-level permissions by providing those objects in the Resource element in your policy statements.

## S3 Bucket share region to region or. Account to Account ?

By enabling **Cross-origin resource sharing** (CORS) . CORS defines a way for client web applications that are loaded in one domain to interact with resources in a different domain.

We can also use Acess Control List ACL to share data between accounts.

Cross Region Replication is another way of sharing information

## Life Cycle Policy ?

Lifecycle policies allow you to automatically review objects within your S3 Buckets and have them moved to Glacier or have the objects deleted from S3. We can set life cycle rule suggesting that after 30 days move to Standard IA and after 60 days move to Glacier.

# Route 53

## What is Hosted Zone ?

Hosted zone is analogous to a traditional DNS zone file

It represents a collection of records that can be managed together, belonging to a single parent domain name

All resource record sets within a hosted zone must have the hosted zone's domain name as a suffix

Public hosted zones contain records that specify how you want to route traffic on the internet.

Private hosted zones contain records that specify how you want to route traffic in an Amazon VPC.

## Types of routing policy and scenario ?

* **Simple routing policy** – Use for a single resource that performs a given function for your domain, for example, a web server that serves content for the example.com website.
* **Failover routing policy** – Use when you want to configure active-passive failover.
* **Geolocation routing policy** – Use when you want to route traffic based on the location of your users.
* **Geoproximity routing policy** – Use when you want to route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another.
* **Latency routing policy** – Use when you have resources in multiple AWS Regions and you want to route traffic to the Region that provides the best latency with less round-trip time.
* **Multivalue answer routing policy** – Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random.
* **Weighted routing policy** – Use to route traffic to multiple resources in proportions that you specify.

## Types of record set in Route 53 ?

Like a phone book, Route 53 lets you manage the IP addresses listed for your domain names in the Internet's DNS phone book. Route 53 also answers requests to translate specific domain names like into their corresponding IP addresses

A record type – Ipv4 routing to a resource

AAAA record type – Ipv6 Routing to resource

CNAME record type - A CNAME record maps DNS queries for the name of the current record, such as acme.example.com, to another domain (example.com or example.net) or subdomain (acme.example.com or zenith.example.org).

MX record type - An MX record specifies the names of your mail servers and, if you have two or more mail servers, the priority order. Each value for an MX record contains two values, priority and domain name.

NS record type - An NS record identifies the name servers for the hosted zone.

PTR record type - A PTR record maps an IP address to the corresponding domain name.

SOA record type - A start of authority (SOA) record provides information about a domain and the corresponding Amazon Route 53 hosted zone. For information about the fields in an SOA record

# SQS & SNS

## Max size of message in SQS

Amazon Simple Queue Service (SQS) now has an **Extended Client Library** by JAVA that enables you to send and receive messages with payloads up to 2GB. Previously, message payloads were limited to 256KB. Using the Extended Client Library, message payloads larger than 256KB are stored in an Amazon Simple Storage Service (S3) bucket, using SQS to send and receive a reference to the payload location.

## What to connect queue from one account to another account ?

Create multiple Queue and make sure one is subscribed to another queue

# VPC

## VPC types ?

Custom

Default

## What is VPC ?

Virtual Private cloud is a isolated Network like we use in our onpremise Network.VPC lets us add subnets, associate security groups, and configure route tables and NACL. A subnet is a range of IP addresses in your VPC. We create our Instances in the Subnets

## why we require to create VPC ?

Amazon VPC enables you to build a virtual network in the AWS cloud - no VPNs, hardware, or physical datacenters required. You can define your own network space, and control how your network and the Amazon EC2 resources inside your network are exposed to the Internet.

## What is Subnet ? max no of subnets per VPC ?

A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting. Computers that belong to the same subnet are addressed with an identical most-significant bit-group in their IP addresses.

MAX 200 subnets per VPC

## What are the 5 Ip’s Reserved by the Subnet ?

**10.0.0.0:** Network address.

**10.0.0.1:** Reserved by AWS for the VPC router.

**10.0.0.2:** Reserved by AWS. The IP address of the DNS server is the base of the VPC network range plus two. For VPCs with multiple CIDR blocks, the IP address of the DNS server is located in the primary CIDR. We also reserve the base of each subnet range plus two for all CIDR blocks in the VPC. For more information, see Amazon DNS server.

**10.0.0.3:** Reserved by AWS for future use.

**10.0.0.255:** Network broadcast address. We do not support broadcast in a VPC, therefore we reserve this address.

## Minimum Subenet Range ?

The minimum size of a subnet is a **/28** (or 14 IP addresses.) for IPv4. Subnets cannot be larger than the VPC in which they are created.

## Public vs Private Instance ?

Public Instance, Can be accessed from anywhere from the Globe. They have a Public IP address.

Private Instance Can be accessed from the resources within the VPC. They dont have a Public IP address. They will also have restriction ins the CIDR range in Security Group limiting access to certain resources.

## How to Troubleshoot VPC ?

Check CIDR range

Public and Elastic IP addresses

System and instance status checks

Security groups

VPC route table

Network ACLs

## Why do we make subnets ?

After creating a VPC with a CIDR we can create Subnet using by selecting the VPC which we want to create our VPC and giving CIDR range within the VPC range

## NACL (Network Access Control List) VS Security Group ?

Nacl are stateless i.e setting applied to Inbound rule is not applied to output rule , It is associated with Subnets. NACL has applied automatically to all the instances which are associated with an subnet.

Security Group are Stateful i.e settings applied to Inbound rule is also applied to outbound rule, It is associated with EC2 instance. Security Group is applied to an instance only when you specify a security group while launching an instance.

## What is routing table ?

A route table contains a set of rules, called routes, that are used to determine where network traffic from your subnet or gateway is directed. To put it simply, a route table tells network packets which way they need to go to get to their destination.

## What is Route Propogation in VPC ?

Route propagation allows a virtual private gateway to automatically propagate routes to the route tables. This means that you don't need to manually enter VPN routes to your route tables.

| Destination | Target |
| --- | --- |
| 10.0.0.0/16 | Local |
| 172.31.0.0/24 | vgw-11223344556677889 (propagated) |
| 172.31.0.0/24 | igw-12345678901234567 (static) |

## How you can connect a private subnet with a public subnet ?

Using Nat gateway.

## What is VPC peering ?

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.

## Can VPC peering possible in two different region ?

Inter-Region VPC Peering allows VPC resources like EC2 instances, RDS databases and Lambda functions running in different AWS regions to communicate with each other using private IP addresses, without requiring gateways, VPN connections or separate network appliances.

## VPC peering steps ?

<https://docs.aws.amazon.com/vpc/latest/peering/create-vpc-peering-connection.html>

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the navigation pane, choose **Peering Connections**, **Create Peering Connection**.
3. Configure the following information, and choose **Create Peering Connection** when you are done:
   * **Peering connection name tag**: You can optionally name your VPC peering connection.
   * **VPC (Requester)**: Select the VPC in your account with which you want to create the VPC peering connection.
   * Under **Select another VPC to peer with**: Ensure **My account** is selected, and select another of your VPCs.
   * (Optionally add or remove a tag.

[Add a tag] Choose **Add tag** and do the following:

* + - For **Key**, enter the key name.
    - For **Value**, enter the key value.

[Remove a tag] Choose the Delete button ("X") to the right of the tag’s Key and Value.

1. In the confirmation dialog box, choose **OK**.
2. Select the VPC peering connection that you've created, and choose **Actions**, **Accept Request**.
3. In the confirmation dialog, choose **Yes, Accept**. A second confirmation dialog displays; choose **Modify my route tables now** to go directly to the route tables page, or choose **Close** to do this later.

## What is transit gateway?

A transit gateway is a network transit hub that you can use to interconnect your virtual private clouds (VPCs) and on-premises networks.

## VPC peering vs VPC transit gateway

Transit Gateway solves the complexity involved with creating and managing multiple VPC peering connections at scale. While this makes TGW a good default for most network architectures, VPC peering is still a valid choice due to the following advantages it has over TGW:

1. **Lower cost** — With VPC peering you only pay for data transfer charges. Transit Gateway has an hourly charge per attachment in addition to the data transfer fees.
2. **No bandwidth limits** — With Transit Gateway, Maximum bandwidth (burst) per VPC connection is 50 Gbps. VPC peering has no aggregate bandwidth. Individual instance network performance limits and flow limits (10 Gbps within a placement group and 5 Gbps otherwise) apply to both options. Only VPC peering supports placement groups.
3. **Latency**— Unlike VPC peering, Transit Gateway is an additional hop between VPCs.
4. **Security Groups** compatibility — Security groups referencing works with intra-Region VPC peering. It does not currently work with Transit Gateway.

Within your Landing Zone setup, VPC Peering can be used in combination with the hub and spoke model enabled by Transit Gateway.

## What is NAT gateway ?

Network Address Translator Gateway is a highly available AWS managed service that makes it easy to connect to the Internet from instances within a private subnet in an Amazon Virtual Private Cloud (Amazon VPC). Public IP address is needed for connectivity to Internet, Since Private Instances does not have Public IP address we cannot connect to internet. NAT gateway solves that problem.

## How many IP’s does Nat gateway has ?

2

## NAT Gateway vs NAT Instance ?

|  |  |  |
| --- | --- | --- |
| Attribute | NAT gateway | NAT instance |
| Availability | Highly available. NAT gateways in each Availability Zone are implemented with redundancy. Create a NAT gateway in each Availability Zone to ensure zone-independent architecture. | Use a script to manage failover between instances. |
| Maintenance | Managed by AWS. You do not need to perform any maintenance. | Managed by you, for example, by installing software updates or operating system patches on the instance. |
| Bandwidth | Scale up to 45 Gbps. | Depends on the bandwidth of the instance type. |

## IGW vs Nat ?

An Internet Gateway is a logical connection between an Amazon VPC and the Internet. If a VPC does not have an Internet Gateway, then the resources in the VPC cannot be accessed from the Internet. We need a Route Table to Route Internet to our Subnets

NAT Gateway is a highly available AWS managed service that makes it easy to connect to the Internet from instances within a private subnet in an Amazon Virtual Private Cloud. You need one in each AZ since they can operate in a single AZ.

## VPC from A to B, B to C will it work for A to C ?

No

## What is VPC Endpoint ?

A VPC endpoint allows you to privately connect your VPC to supported AWS services without requiring an Internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Endpoints are virtual devices that are horizontally scaled, redundant, and highly available VPC components.

## Can we access a Endpoint without using Internet ?

VPC Endpoint which is free and lets you communicate to S3 and DynamoDB from private subnets without natting. For some AWS services, you can create an Interface VPC Endpoint which is cheaper than a NAT gateway.

## S3 to Vpc Connection ?

You can now access Amazon Simple Storage Service (Amazon S3) from your Amazon Virtual Private Cloud (Amazon VPC) using VPC endpoints. ... Additionally, you can control what buckets, requests, users, or groups are allowed through a specific VPC endpoint.

## Flow log in VPC ?

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs or Amazon S3. After you've created a flow log, you can retrieve and view its data in the chosen destination.

## How you monitor VPC ?

VPC flow logs

Cloud watch

# Cloud Watch & Cloud Trial

## Cloud Trial vs Cloud Watch ?

Cloud Trial is a logging tool. We can create a new Customized trial It logs the access in AWS and stores it in a S3

Cloud Watch is a monitoring tool. It has Metrics to Monitor the resources on AWS. We can create Alarm in CW when a metric crosses the certain threshold.

## What is Cloud Watch agent ?

Collect more system-level metrics from Amazon EC2 instances across operating systems. Collect logs from Amazon EC2 instances and on-premises servers, running either Linux or Windows Server.

## What is metrics in cloudwatch ?

Metric resources are the fundamental monitoring unit in CloudWatch. A metric represents a time-ordered set of data points that are published to CloudWatch. Think of a metric as a variable to monitor, and the data points as representing the values of that variable over time.

1. *disk\_total*
2. *disk\_used\_percent*
3. *swap\_free*
4. *netstat\_total*
5. *cpu\_time\_active*

## CloudWatch EC2 Metrices

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-monitoring.html>

1. CPUUtilization
2. DiskReadOps
3. DiskWriteOps
4. DiskReadBytes
5. DiskWriteBytes
6. MetadataNoToken
7. NetworkIn
8. NetworkOut
9. NetworkPacketsIn
10. NetworkPacketsOut

**CPU credit metrics**

1. CPUCreditUsage
2. CPUCreditBalance
3. CPUSurplusCreditBalance
4. CPUSurplusCreditsCharged

**Dedicated Host metrics**

1. DedicatedHostCPUUtilization

**Amazon EBS metrics for Nitro-based instances**

1. EBSReadOps
2. EBSWriteOps
3. EBSReadBytes
4. EBSWriteBytes
5. EBSIOBalance%
6. EBSByteBalance%

**Status check metrics**

1. StatusCheckFailed
2. StatusCheckFailed\_Instance
3. StatusCheckFailed\_System
4. AutoScalingGroupName

**Amazon EC2 metric dimensions**

1. ImageId
2. InstanceId
3. InstanceType

## How to conifgure Cloud Trial for Multi Account Buckets

Add Bucket Permission so files can be received from multiple accounts

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-set-bucket-policy-for-multiple-accounts.html>

# Cloud Front

## What is Cloud Front ?

Amazon CloudFront is a content delivery network operated by Amazon Web Services. Content delivery networks provide a globally-distributed network of proxy servers that cache content, such as web videos or other bulky media, more locally to consumers, thus improving access speed for downloading the content.

## Edge Location vs Server ?

### Edge location is a physical location where a w s has its servers that are used to stores cdn caching. Edge locations are used to provide low latency access to the data.Thus it will provide low latency access to your data and end users will have better experience.

## Cloud Front default ttl, Can we incerase the ttl ?

default ttl is 1 day 86400 seconds, minimum is 0 seconds and maximum is 1 year

## How to refresh CloudFront Cache ?

CloudFront instance and go to the `Invalidations` tab where you can 'Create Invalidation'. Then click on 'Invalidate' and the invalidation will run: All Done! Your cache should be cleared and you are good to go once the run completed.

# Lambda

## AWS Lambda ?

AWS Lambda is an event-driven, serverless computing platform provided by Amazon as a part of Amazon Web Services. It is a computing service that runs code in response to events and automatically manages the computing resources required by that code.

## What is purpose of using Lambda ?

AWS Lambda is a serverless compute service that runs your code in response to events and automatically manages the underlying compute resources for you. You can use AWS Lambda to extend other AWS services with custom logic, or create your own back-end services that operate at AWS scale, performance, and security.

## WHat is the difference between Lambda vs EC2

Lambda is just a serverless tool to run our code. Lambda will be executed based on the trigger. Lambda will be charged based on the Code execution.

Where as EC2 is a VM instance which will be always running and we can install applications on top it

## How to assign Public IP to Lambda ?

<https://digitalvarys.com/how-to-assign-a-static-ip-to-the-aws-lambda-function/>

STEP 1: Create a new VPC or use your existing VPC

STEP 2: Create Two Subnets: Public and Private

STEP 3: Create an Internet Gateway

STEP 4: Create a NAT Gateway

STEP 5: Create Two set for Route Table: Public and Private

STEP 6: Create Security Group

STEP 7: Assign the Configured settings to AWS Lambda Function

# RDS

## What is Database ?

A Database contains multi tables. Each table has entries in the form of Rows and Columns. Multiple data bases are handled by RDBMS.

In AWS we have RDS to create hassle free database in cloud. which provides max size of 64 TiB

## Data base Architecture ?

Master in one AZ and Standy in another AZ. Creating Read Replica to create a read only copy of a Database to decrease the server load

## What is Amazon RDS ?

Amazon Relational Database Service is a distributed relational database service by Amazon Web Services. It is a web service running "in the cloud" designed to simplify the setup, operation, and scaling of a relational database for use in applications.

## Aurora Advantage ?

Aurora works in the form of Cluster.

Up to 5 times the throughput of MySQL and 3 times the throughput of PostgreSQL

Up to 64TB of auto-scaling SSD storage

6-way replication across three Availability Zones

Up to 15 Read Replicas with sub-10ms replica lag

Automatic monitoring and failover in less than 30 seconds

## read replica vs write replica?

Read Replica -> Creates a Read only copy of a running Database they are in Synchronous Replication.

Write Replica -> Creates a Write only copy of a running Database they are in Synchronous Replication

## Multi AZ Deployment vs Multi Region Deployment vs Read Replicas ?

|  |  |  |
| --- | --- | --- |
| Multi-AZ deployments | Multi-Region deployments | Read replicas |
| Main purpose is high availability | Main purpose is disaster recovery and local performance | Main purpose is scalability |
| Non-Aurora: synchronous replication; Aurora: asynchronous replication | Asynchronous replication | Asynchronous replication |
| Non-Aurora: only the primary instance is active; Aurora: all instances are active | All regions are accessible and can be used for reads | All read replicas are accessible and can be used for readscaling |
| Non-Aurora: automated backups are taken from standby; Aurora: automated backups are taken from shared storage layer | Automated backups can be taken in each region | No backups configured by default |
| Always span at least two Availability Zones within a single region | Each region can have a Multi-AZ deployment | Can be within an Availability Zone, Cross-AZ, or Cross-Region |

## Security in RDS to DB

\s  
SSL Cipher

## RDS vs DynamoDB ?

### Rds

* Managed relational (SQL) database
* Has several database instance types for different kinds of workloads and supports six database engines – Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server.
* -128 TB for Aurora engine – 64 TB for MySQL, MariaDB, Oracle and PostgreSQL engines -16 TB for SQL Server engine.
* Can use VPC to give maximum security

### DynamoDB

* Fully managed key-value and document (NoSQL) database
* Delivers single-digit millisecond performance at any scale.
* Supports tables of virtually any size.
* Integrates with IAM

## How is Amazon RDS, Redshift & DynamoDB different ?

RDS is used to create RDBMS like MYSQL, Postgres, Aurora  
Dynamo DB is a No sql Database

Amazon Redshift is a fully-managed petabyte-scale cloud based data warehouse product designed for large scale data set storage and analysis. It is also used to perform large scale database migrations. Redshift is also used to analyze data.

## RDS vs EC2 in Mysql ?

Installing MYSQL in EC2 means we have to fully manage & maintain the Database. Where as if we choose MYSQL in RDS aws will take care of the configuration and maintanence of Database. We lose features like AutoScaling, Read Replica, Multi AZ deployment if we choose EC2 over RDS.

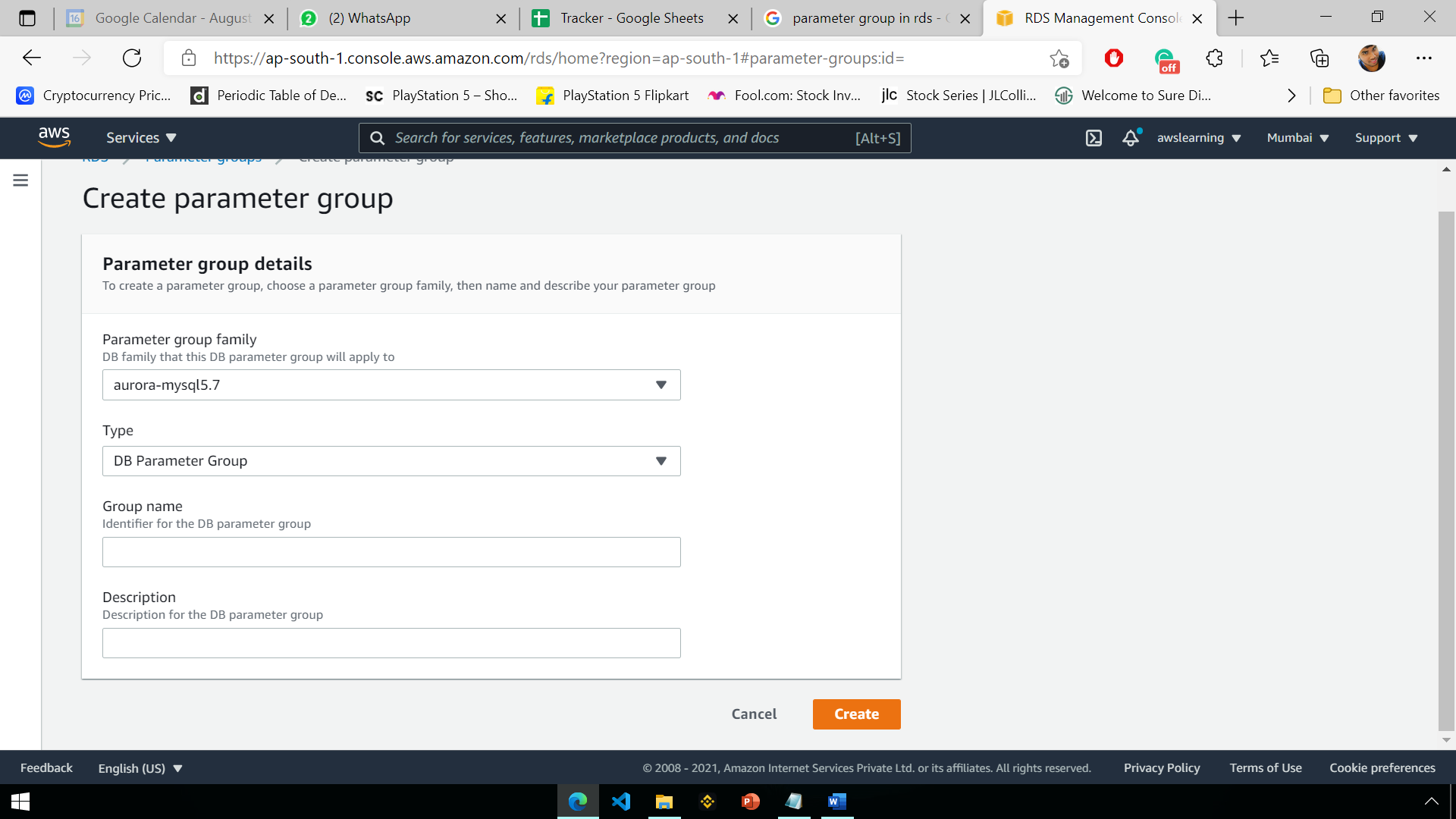
## Autoscaling in RDS ?

20gb – 16TB Storage. Only Storage Autoscaling is available and it increases the storage automatically as the storage gets full.

## Subnet Group in RDS ?

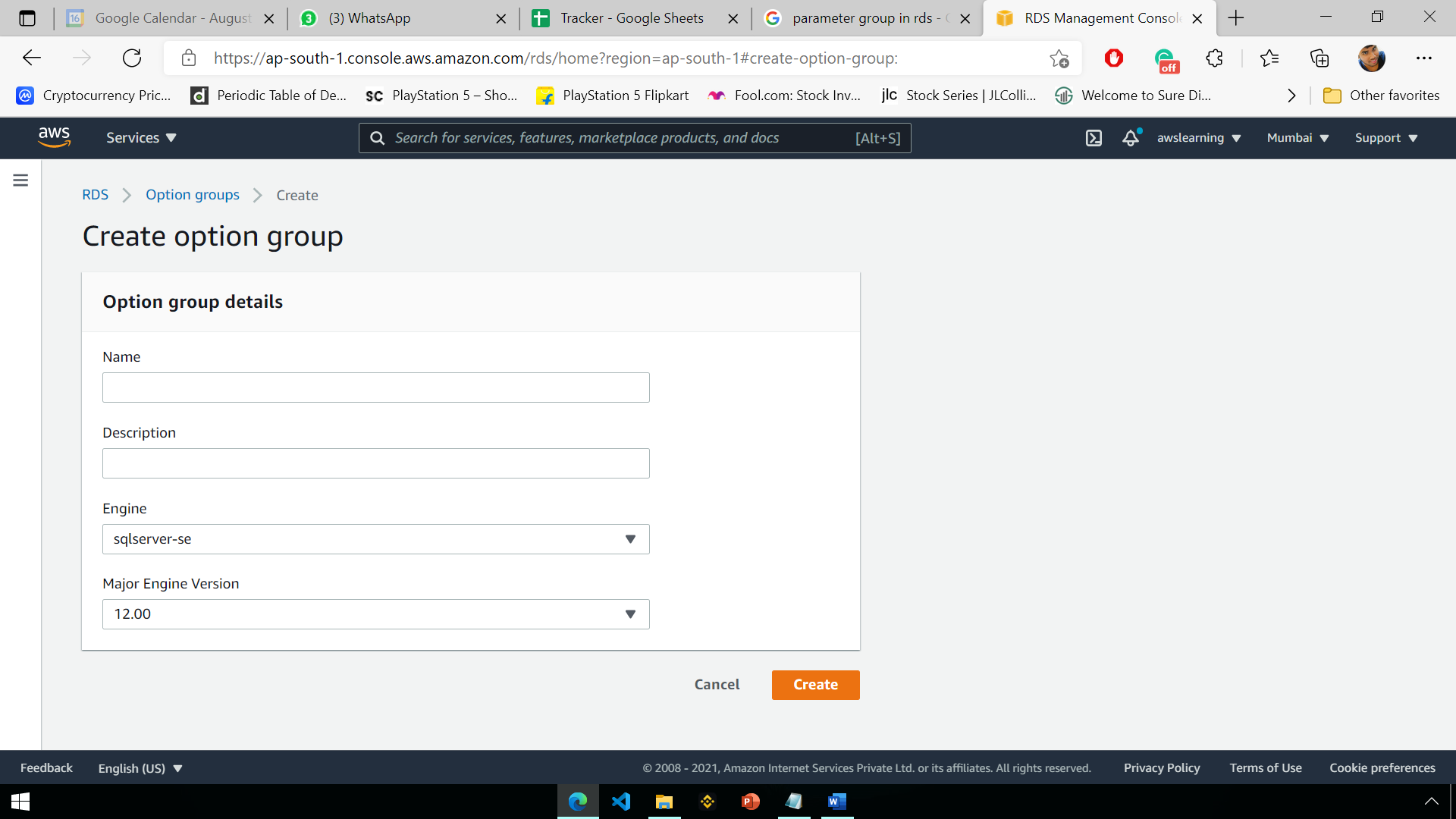
## Parameter Group in RDS ?

A DB parameter group acts as a container for engine configuration values that are applied to one or more DB instances. ... Each default DB parameter group contains database engine defaults and Amazon RDS system defaults based on the engine, compute class, and allocated storage of the instance.



## Options Group in RDS ?

Apart from parameter groups to define RDS instance type specific parameters, AWS RDS also support option groups. Options groups consist of optional features that can be added to your AWS RDS instance that are not already covered in parameter groups.



# Cloud Formation

## What is CF stack ?

A stack is a collection of AWS resources that you can manage as a single unit.

All the resources in a stack are defined by the stack's AWS CloudFormation template. A stack, for instance, can include all the resources required to run a web application, such as a web server, a database, and networking rules.

## What is mapping in cloudformation template ?

* Mappings is a section of CloudFormation to help organizing parameters by named keys and corresponding values for each group
* if you want to set values based on a region, you can create a mapping that uses the region name as a key and contains the values you want to specify for each specific region.

## What are the main components of CloudFormation ?

We can use either JSON or YAML to write CloudFormation Template,

A CloudFormation template consists of 6 sections – **Description, Parameters, Mappings, Conditions, Resources and Outputs.**

## How is YAML different from JSON ?

YAML uses Double spaces as its hierarchy

JSON uses braces and brackets.

## How Infrastructure As Code processed & executes in AWS ?

CloudFormation reads a template and generates a stack, a set of resources ready to use on AWS. By using CloudFormation, you can define complex multi-resource applications and automatically deploy the resources on AWS. You can test your Infrastructure as Code by fine-tuning your configuration and repeating the process.

## CloudFormation Drift\_status ?

Manual Changes made in the Stack will be shown in Drift Status

Stack -> Update Stack to New changes made

## Stack instances vs Stack Sets

A stack set lets **you create stacks in AWS** accounts across AWS Regions by using a single AWS CloudFormation template. A stack instance refers to a stack in a target account within an AWS Region and is associated with only one stack set. For more information, see StackSets Concepts.

You can use AWS CloudFormation StackSets to launch AWS Service Catalog products across multiple AWS Regions and accounts. You can specify the order in which products deploy sequentially within AWS Regions. Across accounts, products are deployed in parallel. When launching, users can specify failure tolerance and the maximum number of accounts in which to deploy in parallel.


            A stack set is a collection of resources, defined in a template and deployed
                into one or more accounts across one or more regions.
        

*A stack instance is a reference to a stack in a target account within a Region. A stack instance can exist without a stack*. For example, if the stack couldn't be created for some reason, the stack instance shows the reason for stack creation failure. A stack instance is associated with only one stack set.

# SSM

## Patch Manager and Amazon EC2 Systems Manager

<https://aws.amazon.com/blogs/mt/getting-started-with-patch-manager-and-amazon-ec2-systems-manager/>

1. Launch new Windows instances.
2. Create a custom patch baseline.
3. Set the patch group for the custom patch baseline.
4. Create a maintenance window.
5. Register targets for the maintenance window.
6. Register a task for the maintenance window.
7. Verify the patch compliance report.

# Extras

## Elastic cache ?

Amazon ElastiCache is a fully managed in-memory data store and cache service by Amazon Web Services. The service improves the performance of web applications by retrieving information from managed in-memory caches, instead of relying entirely on slower disk-based databases.

## ECS & ECR ?

Amazon ECS is a regional service that simplifies running containers in a highly available manner across multiple Availability Zones within a Region

ECR - EC2 Container Registry , To store the Docker Images, ECS Agent

Create ECS Cluster using ECS Task and write code to add meta data for individual Instance

## ELK & Kibana ?

ELK stack gives you the ability to aggregate logs from all your systems and applications, analyze these logs, and create visualizations for application and infrastructure monitoring, faster troubleshooting, security analytics

Log stash gives the file to Kibana

Kibana is an open-source data visualization and exploration tool used for log and time-series analytics, application monitoring, and operational intelligence use cases. It offers powerful and easy-to-use features such as histograms, line graphs, pie charts, heat maps, and built-in geospatial support

## EMR

Amazon EMR is the industry-leading cloud big data platform for processing vast amounts of data using open source tools such as Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi, and Presto. Amazon EMR makes it easy to set up, operate, and scale your big data environments by automating time-consuming tasks like provisioning capacity and tuning clusters. With EMR you can run petabyte-scale analysis at less than half of the cost of traditional on-premises solutions and over 3x faster than standard Apache Spark. You can run workloads on Amazon EC2 instances, on Amazon Elastic Kubernetes Service (EKS) clusters, or on-premises using EMR on AWS Outposts.

## Inspector

It is used to run secuiryt checks on the AMI

an automated security assessment service that helps improve the security and compliance of applications deployed

Penetration Testing

## File beat

Filebeat is a lightweight shipper for forwarding and centralizing log data. Installed as an agent on your servers, Filebeat monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.

## What is AWS Security Manager ?

AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.

## What is WAF ?

AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources. **cross-site request forgery (CSRF), cross-site-scripting (XSS), file inclusion, and SQL injection.**

## What is Parameter Store in System Manager ?

String, String List, SecureString -> KMS

aws ssm-get prameters by path --path /url/myapp/dev