**AWS Solution Architect Certification**

Tuesday, February 19, 2019

3:02 PM

**S3 Summary -**

Object based storage for Flat files.

File size be from 0 byte to 5 TB.

Files are stored in buckets.

Universal Namespace.

Bucket Name - [https://s3-eu-west-1.amazonaws.com/<bucketname>](https://s3-eu-west-1.amazonaws.com/%3cbucketname%3e)

Read after write consistency for PUTS of new objects.

Eventual Consistency for overwrite PUTS and DELETES.

S3 Standards

99.9% Availability

00.99999999 % Durability

S3 IA - (Infrequently Accessed)

S3 One Zone IA - Lower cost for IA but don’t require multi AZ

Glacier - Very cheap. Standard Retrieval time 3 -5 hrs.

Key(NAME) Value (Data) Store

Supports Versioning of an object (include all writes and even if you delete it)

Versioning integrates with Life cycle rules

Versioning MFA delete capability

Transition to Standard IF access after 30 days of creation then to Glacier after 30 days in IFA.

Cloudfront -

Edge Location- content will be cached here

Can be used for both read/write.

Objects are cachedfor the life of TTL (Time to Live) Default - 24 hrs.

Can clear cahced objects but will be charged.

Security -

By default all created buckets are Private

Bucket Policy or Access Control List

Access log can be created for a bucket

Encryption -

In Transit

SSL/TLS

Rest

Server Side

S3 Managed Keys SSE-S3

AWS Key Management Service - SSE-KMS (envelope key that protects encryption key). Also provide audit trail

Server side encryption with Customer provided Key - SSE-C

Client side

File Gateway - For Flat files stored on S3

Volume Gateway -

Stored Volumes - Entire dataset is stored on site and its async backed on S3

Cached Volumes - Entire Dataset is stored on S3 and most frequentl access data is cached on site

Gateway Virtual Tape Library (VTL) - Used for backups like NetBackup, Backup Exec etc

Snowball - import to S3 and exprt from S3

Snowball edge - Storage + Compute capability

Snowmobile - 100 PB of storage

S3 Transfer Acceleration -

Speed up transfer to S3

Uploading files to Edge location.

Write To S3 - HTTP 2-- for successful write

Multipart upload - for Faster upload to S3

**EC2 Summary -**

EBS -

SSD - General Purpose upto 10000 IOPS

SSD - Provisioned more than 10000 IOPS

HDD - Throughput optimized - ST1 - Frequently accessed Data

HDD - COLD - SC1 - Less frequently accessed

HDD - Magnetic - Standard Cheap- Infrequently accessed Data

EFS for sharing Boot Volume (not EBS)

Termination protection is turned off by default. Root EBS Volume will be deleted.

EBS backed root volume can be encrypted.

Volume exist on EBS and Snapshot (incremental) exist on S3.

Snapshot can be shared other AWS account. (Only unencrypted).

Instance store Volumes are called Ephermal Storage. Can't be stopped as lose the data.

Instance Metadata - get information about an instance like public IP address.

Curl <http://169.254.169.254/latest/meta-data/>

Curl <http://169.254.169.254/latest/user-data/>

EFS - Network file system version 4 (NFSv4)..can scale upto peta bytes. Rad after write consistency.

Lambda- event driven compute service

Placement Group -

Clustered PG (default) - 1 AZ zone - Big data Low Latency high network throughput

Spread PG - critical EC2 instances spread across different hardware

**DNS/Route 53 -**

Simple Routing - 1 record with multiple ip address

Weighted - 50%- 50% traffic or based on %

Latency - send the traffic to nearest region

Failover - Active/Passive (IF region goes down then failover to passive form active site - uses health check)

Geolocation - directs the traffic to appropriate location

Multivalue Answer

**Database Summary -**

RDS (OLTP)

SQL, MYSQL, AURORA , POSTgreSQL

Multi AZ and read replicas of prod db (upto 5)

Aurora Scaling- 2 copies of data in each AZ with minimum 3 AZ

DynamoDB - NoSQL

Push button scaling (scaling with no downtime)

Stored on SSD. Eventual Consistency.

Redshift - OLAP

Single Node (for small business - 160 GB)

Multi Node

Elasticache - web service - In memory Caching

Memchahce

Redis

**VPC Summary -**

Machine generated alternative text:
VPC with Public & Private Subnet(s) 
PUBLIC SN (10.0.1.0/24) 
Security 
Grou 
Instance 
NAT Gateway 
Route 
Table 
Router 
Route 
Table 
Internet 
Gateway 
Udcmy 
Network 
ACL 
4 
Security Group 
Instance 
PRIVATE SN (10.0.2.0/24) 
VPC (acioudguruVPC) - 10.0.0.0/16 
REGION (us-east-I) 

NAT Instance -

While creating NAT instance, disable source/destination check on the instance.

Must be in public subnet.

Route of the private subnet to the NAT instance.

Behind a security group

NAT Gateways -

Scale automatically

Not associated with security group

Automatically assigned a public ip adrress

More secure

NACL -

VPC always comes with default Network ACL and by default it allows all incoming and outbound traffic.

Each custom NACL denies all inbound and outbound traffic until you add rules.

Separate inbound and outbound rules and stateless.

Block ip address using NCAL

Application Load balancer -

At least 2 public subnet

VPC Endpoints - instances in private subnet can communicate with S3. gateway inside private subnet.

Machine generated alternative text:
WebServerSG: Recommended Rules 
Inbound 
Source 
0.0.0.0/0 
0.0.0.0/0 
DBServerSG. 
Inbound 
Source 
Protocol Port Comments 
TCP 
TCP 
Range 
Allow inbound HTTP access to the web servers from any IPv4 address. 
80 
443 Allow inbound HTTPS access to the web servers from any IPv4 address. 
Comments 
Allow inbound Microsoft SQL Server access from the web servers associated with 
the WebServerSG security group. 
Allow inbound MySQL Server access from the web servers associated with the 
WebServerSG security group. 
• Recommended Rules 
Protocol Port 
TCP 
TCP 
Range 
1433 
3306 
The ID of your WebServerSG 
security group 
The ID of your WebServerSG 
security group 

**Application Services Summary -**

SQS -

Webservice that gives access to Message Queue.

Pull based

Messages are 256 KB in size

Messages can be kept in queue from 1 min to 14 days. Default - 4 days

Visibility time out - maximum is 12 hrs.

Guarantees message is processed at least once.

Long polling / short polling

Standard or FIFO queue.

Retention period = 14 days

SWF

1 year retention period

Task oriented API

Task is assigned only once. Never duplicated.

Keeps track of all task

Actos - Workflow Starters

Deciders

Activity workers - carry out the activity task

SNS

Subscribers - HTTP, HTTPS, Email , Email-JSON, SQL, Application, Lambda

Mobile service Push based

Elastic Transcoder -

Media Transcoder in the cloud

Converts media files

**Kinesis Streams -** Producer sends the data in the form of streams then converted to shard and consumed by consumers.

**Kinesis Firehose -** Query the data using Lamda function, sends directly to S3. **Firehose** is a fully managed service for delivering real-time streaming data to destinations such as S3, Redshift, Elastic Search service and Splunk

**Kinesis Analytics -** SQL queries and store data in S3 or Redshift.

**Important Points to remember -**

Public subnet for Elastic Load Balancer to ensure traffic flow via Internet.

The Web server can be in private subnet since the communication between the instances and ELB happens via Private IP.

The Database server should be in the private subnet since it does not need to communicate with the internet.

If you have resources in multi AZ, create a NAT gateway in each Availability Zone.

Application Load Balancers allows Container to use dynamic host port mapping (So the multiple task from the same service is allowed per container instance).

Application LB support **path based routing and priority rules**.

**AWS WAF** to control how Amazon Cloudfront or an ALB responds to web request. Web application firewall service.

**Cross Account IAM roles** allow customers to securely grant access to AWS resources in their account to third party, like PAN partner, while retaining the ability to control and audit who is accessing their AWS account.

**AWS Elastic Beanstalk** is used to quickly provision development environments.

Machine generated alternative text:
Volume Type 
Description 
Solid-State Drives (SSD) 
Hard disk Drives (HDD) 
General Purpose SSD 
(gp2)* 
General purpose SSD 
volume that balances 
price and performance 
for a wide variety of 
workloads 
Provisioned IOPS SSD (iol) 
Highest-performance SSD volume 
for mission-critical low-latency or 
high-throughput workloads 
Throughput Optimized 
HDD (sti) 
Low cost HDD volume 
designed for 
frequently accessed, 
throughput-intensive 
workloads 
Cold HDD (SCI) 
Lowest cost HDD 
volume designed for 
less frequently 
accessed workloads 

**VPC endpoint Interfaces** - They have to be in same Region.

**VPC Peering** - Different Region, VPC in another AWS account.

**AWS Direct Connect -** Service solution that make it easy to establish a dedicated network connections from your premises to AWS. (Private Network)

**Amazon Redshift -** You can configure Amazon Redshift to automatically copy snapshots (automated or manual) for a cluster to another region.

**Amazon Cloudfront** is a web service that speeds up distribution of static and dynamic content such as .html, .css. Jss and image files to the users.

Cloudfront delivers your content through a worldwide network of datacenters called edge location.

**Amazon Cognito** provides authentication, authorization and user management for your web and mobile apps. Users can directly sign in with a user name and password or through a third party such as Facebook, Amazon, Google.

Tuesday, February 19, 2019

6:10 PM