AWS Cloud Solutions Architect Associate Course:

**AWS – History So Far:**

“Invention requires two things: ability to try a lot of experiments, and 2. Not having to live with the collateral damage of failed experiments.”

2003 – paper on what Amazon’s own internal infrastructure should look like

selling it as a service and prepared a business case.

SQS launched 2004

AWS launched 2006

2007 had over 180,000 developered

2010 all of amazon.com moved over

2012 Re-Invent conference

2013 Certifications Launched

2014 Committed to achieved 100% renewable energy

2015 AWS breaks out its revenue. $6 billion per year

2016 Run rate of 13 billion USD

2016 Cisco, Dell, IBM had a 15 billion reduction

New service announcements grow substantially every year.

Subscribe to YouTube on Cloudguru, Jeff Bar’s Blog and twitter of ACloudGuru.

May 2015 AWS was named as a leader in the IaaS for the 5th consecutive year in the leader category. Same for 2016.

CenturyLink VmWare and Softlayer are now niche players.

**10,000 ft overview:**

Messaging, Desktop& App Streaming, Security & Identity, Management Tools, Storage, Databases, Networking & Content Delivery, Compute, and AWS Global Infrastructure will need to be known for **the exam.**

Global Infrastructure

* **Regions** – where availability zones reside. Geographical area. Consists of 2 or more availability zones
  + some regions don’t have all the services in them.
* **Availability Zones** – simply a data center. Isolated from other availability zones.
* **Edge Location** – CDN end point for CloudFront. A way to cache media objects in the cloud. More edge locations than regions. POP for CloudFront

Networking & Content Delivery

* **VPC (Virtual Private Cloud)** – virtual datacenter. Multiple VPC’s to a region and connect other VPC’s to another. **Important on exam.** How to build a VPC from memory?
* **Route53 –** DNS service. Can register domain names through this. 53 is the DNS port.
* **CloudFront** – Part of CDN. Edge locations that cache assets.
* **Direct Connect** – a way to connect an office or physical datacenter to AWS directly with a dedicated telephone line. **Can come up in the exam.**

Compute

* **EC2 (Elastic Compute Cloud)** – virtual machines in the cloud.
  + SSH/RDP
* **EC2 Container Service** – container management service geared towards Docker containers. Don’t have to install cluster management system. Doesn’t come up in the system.
* **Elastic Beanstalk** – comes up in developer exam. Upload code and then this service will deploy the needed infrastructure for the application.
* **Lambda** – Serverless, upload code and code will respond to events. Not in exams yet.
* **Lightsail** – out of the box cloud. Wordpress/etc.

Storage

* **S3 (Simple Storage Service)** – virtual disk in the cloud which can store object. Files, pictures, movies, etc. Does come up in the developer and CSAA exam. Object based storage.
* **Glacier** – place to archive your files off of S3.
* **EFS** (Elastic File Service) – Block based storage which can be shared. Could install databases/applications and share it with multiple VM’s.
* **Storage Gateway –** a way to connect S3 to your physical datacenter. VM on premise but pulls the data from S3.

Databases

* **RDS (Relational Database Service)** – MariaDB, SQL, MySQL, Oracle, Comes up in the CSAA
* **Aurora** – MySQL, PostGres
* **DynamoDB** – non-relational database. NoSQL. Developer exam
* **Redshift** – datawarehousing solution. Big Data.
* **Elasticcache** – a way to cache your data in the cloud.

Migration

* **Snowball** – initially import/export. Briefcase size appliance for loading the data on it. S3/EBS transfer. Traditionally consisted of just storage. Added compute capacity to it which can be taken on premise. SysOps/Associate exam.
* **DMS (Database Migration Services)** – migrate databases on premise or databases in the cloud for shifting them over. Migrate databases inside AWS to other regions or into Redshift. Don’t have to stay with the database you’re migrating from. Handles the entire conversion process. Zero downtime. Oracle, Aurora, SAP ESE, MySQL, SQL. Not in exam yet.
* **SMS (Server Migration Services)** – migrate VM (vmWare) on premise to replicate them to the cloud and can do 50 concurrent at the same time. Not on exam yet.

Analytics

* **Athena** – run SQL queries on S3. JSON files. Flat files turning them into searchable details.
* **EMR (Elastic Map Reduce)** – Produce large amount of data. Web indexing. Using Hadoop and other frameworks. Big Data.
* **Cloud Search –** Managed service. Create search capabilities with your website.
* **Elastic Search** – open source framework. Create search capabilities with your website.
  + Angola
* **Kinesis** – A way of analysis streaming data and storing data like financial transactions. Social media streams.
* **Data Pipeline** – Data that allows to be transferred from one location to another.
* **Quick Sight** – Business analytics tool, create visualizations and can use data from S3. Dashboards.

Security & Identity

* **IAM (Identity Access Management)** – comes up in every exam. Basic way to sign in/authenticate. Group users
* **Inspector** – agent installed on VM. Inspects them. Does reporting
* **Certificate Manager** – free SSL certs for your domains
* **Directory Service** – way to connect AD to AWS.
* **WAF (Web Application Firewall)** – application level protection to your website. SQL injection, cross-site scripting.
* **Artifacts** – where to get your documentation in the console.

Management Tools

* **Cloud Watch** – monitor performance on AWS environment. Monitor disk utilization, filters.
* **Cloud Formation** – a way to turn your infrastructure into code. Document that describes your environment. Templates. Know inside and out. Doesn’t come up in exam.
* **Cloud Trail** – a way to audit changes to your AWS environment.
* **Opsworks** – automating deployments via chef.
* **Config** – a way to monitor and automate your environment. You can set alerts.
* **Service Catalog** – allows enterprises to build out what can be authorized and not authorized.
* **Trusted Advisor** – a way to recommend tips like cost optimization, etc.

Application Services

* **Step Functions** – a way to visualize what is happening inside your application or microservices.
* **SWF (Simple Workflow Service)** – a way to coordinate human ordinated tasks and non-human tasks.
* **API Gateway** – a door to create publish, secure API’s at scale. A way for apps to access backend data.
* **AppStream** – streaming desktop applications to your users
* **Elastic Transcoder** – changes video format to suite multiple devices.

Developer Tools

* **CodeCommit** – Github. A place to store your code like Github
* **CodeBuild** – a way to compile your code
* **CodeDeploy** – a way to deploy your code to EC2 instances
* **CodePipeline** – a way to keep track of all versions of your codes.

Mobile Services

* **Mobile Hub** – let’s you add/configure features for your apps. Backend logic, notfications. Own console for the apps.
* **Cognito** – easy for users to sign in and sign up for your apps. Gmail credentials for example.
* **Device Farm** – provides a way to enhance usable android/ios apps. Can test on hundreds of real smart phones.
* **Mobile Analytics** – Cost effective collect mobile app usage data
* **Pinpoint** – enables you to understand and engage with your users. Gather data on what users are doing what with your apps. Can look at human behavior. Can market to your users.

Business Productivity

* **WorkDocs** – store your important work documents in the cloud.
* **WorkMail** – exchange for AWS. A way to send/receive email

Internet of Things

* **iOT** – millions of devices out there and a way to keep track of them.

Desktop & App Streaming

* **WorkSpaces** – VDI, a way of having your desktop in the cloud.
* **AppStream 2**.**0** – a way to stream desktop applications to your users.

Artificial Intelligence

* Superintelligence book by Nick Bostrom
* **Lex** – don’t need an echo to communicate with alexa
* **Polly** – text to speech in 47 different languages. Mp3 file. Synthesis Speech language.
* **Machine Learning** – Give AWS a data set and what the outcomes are. Uses machine learning to predict outcomes based on the data center. Predict data based on previous data.
* **Rekognition** – Upload a picture. Provides tags, facial recognition.

Messaging

* **SNS (Simple Notification Service)** – email, text message, HTTP endpoints
* **SQS (Simple Queue Service)** - a way of decoupling your applications. Post jobs to a queue. If message dies, it stays in the SQS queue. No tightly coupled dependencies.
* **SES (Simple Email Service)** – a way of sending/receiving email in this service.

**IAM (Identity Access Management) 101**

* Allows you to manage users and their level of access to the AWS Console.
* Gives you centralized control of your AWS account
* Shared access to your AWS account
* You can peer AWS accounts to other accounts
* Granular Permissions
* Identity Federation (AD, FB, LinkedIn). SSO
  + Create apps that authenticate against FB, etc.
* Multifactor authentication
* Provide temporary access for users/services when necessary.
* Allows you to setup your own rotation policy.
* Integrate with other AWS services.
* Supports PCI DSS compliance – taking online payments and storing credit card details yourself.
* **Users** – End Users (think people)
* **Groups** – collection of users under one set of permissions
* **Roles** – create roles and can then assign them to AWS resources.
* **Policies** – a document that defines one or more permissions (JSON) – Attribute/Value

Lab:

**Global regions can come up on the exam for IAM. It can be accessed in any region.**

Root account is your email address you used to create your account.

**Access key id and secret access key id can only be used for programmatic access on IAM.**

You can attach more than one policy to a user and group.

New users have no permissions when created.

Can only view access key and secret access key once.

Always setup MFA on your root account.

Read AWS Security Best Practices - AWS Security Best Practice

**S3 Storage 101**

Simple Storage Service provides developers and IT teams with secure, durable, highly-scalable object storage. S3 is easy to use, with a simple web services interface to store and retrieve any amount of data from anywhere on the web.

Place to store files in the cloud. Object based (Video’s, word docs, flat files). Data is spread across multiple devices and facilities. Designed to sustain the loss of 2 facilitiesBlock storage (OS, database).

Allows you to upload files. 0 to 5 TB per files. Unlimited storage. Files stored in buckets

Name must be unique globally as it’s a universal namespace.

**Always receive an HTTP 200 status code**

**Read S3 FAQ before taking the exam.**

* **Key** – name of object (Can put data in alphabetical order. Can add dates to make sure their unique. )
* **Value** – simply the data and is made up of a sequence of bytes
* **Version ID** – Version
* **Metadata** – data about the data you are storing
* **Subresources** – exist underneath an object
  + **ACL’s**
  + **Torrent**

Built for 99.99% availability

Guarantee 99.9% availability

Amazon Guarantee’s 99.9^11 durability

Tiered storage options

Lifecycle Management

Versioning

Encryption

Secure your data using Access Control Lists and Bucket Policies

**S3** – 99.99% availability, 99.99^11% durability, stored redundantly across multiple devices in multiple facilities and is designed to sustain the loss of 2 facilities concurrently.

**S3 – IA(infrequently accessed)** –for data that is accessed less frequently, but requires rapid access when needed. Lower fee than S3, but you are charged a retrieval fee.

**Reduced Redundancy Storage** – Designed to provide 99.99% durability and 99.99% availability of objects over a given year. (reproducible data like thumb nails.)

**Glacier** – very cheap, but used for archival only. It takes 3-5 hours to restore from Glacier.

Data Consistency:

* **Read after Write consistency for PUTS of new Objects**
* **Eventual Consistency for overwrite PUTS and DELETES (can take some time to propagate) Atomic – get new or old data. Won’t get partial data.**

<https://s3-eu-west-1.amazonaws.com/acloudguru>

* **region – bucket name at end.**

**Glacier** – extremely low-cost storage service for data archival. Stores data as little as $0.01 per gigabyte per month and is optimized for data that is infrequently accessed and for which retrieval times of 3 to 5 hours are suitable.

Charges:

* Storage
* Requests
* Storage Management Pricing
* Data Transfer Pricing. Data in S3 is free. Data around in S3 is charged
* **Transfer Acceleration** – enables fast, easy and secure transfers of file over long distances between you end users and an S3 bucket. Transfer Acceleration takes advantage of Amazon CloudFront’s globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path. Users upload to edge location

Lab:

Bucket names can only be created with lowercase characters.

Can run a static website hosting. Tags, cross-region replication, logging.

Lifecycle allows objects to be moved over to different S3 Tiers.

Can allow permissions on specific buckets, etc.

**Have to make an object public before being able to view it**.

Use permissions at the object or bucket level.

Lab:

**Cant delete versioning once it is enabled.**

Versions will be the sum of all the different documents in one in the bucket.

**If you delete a version, it can’t be restored. If you delete and object, it can be restored.**

**If an object is deleted, it shows as a delete Marker.**

Versioning MFA Delete capability – uses multi-factor authentication can be used to provide an additional layer of security.

Lab:

Prefix means sub folders in bucket.

Doesn’t support multiple replication region buckets

Delete markers/other versions don’t replicate to other regions. Unless you delete the object will it come up in the replicated region.

Versioning must be turned on for cross replication on target and source endpoints.

Files in an existing bucket are not replicated automatically. All subsequent updated files will be replicated automatically.

<http://docs.aws.amazon.com/AmazonS3/latest/dev/crr-what-is-isnot-replicated.html>

All previous versions are replicated.

Lab:

Versioning can be on with lifecycle management or not. Lifecycle rules – help manage your storage costs by controlling the lifecycle of your objects.

Can’t recover permanently deleted items.

Glacier has a 90-day minimum of storage duration.

Can be used in conjunction with versioning. Can be applied to current version or previous versions.

**CloudFront CDN Overview**

A system of distributed servers that deliver webpages and other web content to a user based on the geographic location of the user, The origin of the webpage and a content delivery server.

**Edge Location** – location where content will be cached. This is separate to an AWS Region/AZ. **Cache is TTL. Not just for read only. Clearing cache objects means you’ll be charged.**

**Origin** – origin of all the files that the CDN will distribute. This can be an S3 Bucket, EC2 Instance, Elastic Load Balancer or Route 53.

**Distribution** – this is the name given the CDN which consists of a collection of edge locations.

Cloud Front - can be used to deliver your entire website, including dynamic, static, streaming, and interactive content using a global network of edge locations. Requests for your content are automatically routed to the nearest edge location, so content is delivered with the best possible performance. Optmiized to work with other AWS services. Works seamlessly with any non-AWS origin server which stores the original, definitive versions of your files.

**Web Distribution** – Typically used for websites.

**RTMP** – Used for Media Streaming.

<https://aws.amazon.com/cloudfront/details/>

**Lab:**

Can restrict users to use cloudfront only versus the s3 url. If objects consistenly change, it would be good to change the TTL if it happens often. Acloud guru uses signed urls that are geared towards users and can’t be shared with users based on who or who didn’t pay.

Supports HTTP/2 and IPv6.

**You can enable Geo-restriction with either whitelist/blacklist. You can only have one or the other.**

**Invalidating objects can remove them from CloudFront edge locations. Costs money by removing it Stops content from being cached before the TTL if it is in process. Used not only for downloading but uploading.**

Hi Team,

The have been a number of Forum posts and Support contacts about problems with this Lab. I have been able to recreate the problem and find a resolution.

In a word, Patience.

The Lab does work, however there appears to be a problem that the delay caused by the distribution's settings and DNS values replication causes the initial accesses to fail and cache the 'failure'.

While the Distribution is being created and activated, CloudFront will simply redirect back to S3. However if the objects in S3 are not available an 'AccessDenied' is cached. This behaviour also appears to be inconsistent which doesn't help.

I have confirmed that by waiting (I have been testing for at least an hour) or Disabling and then Enabling will also allow the system to stabilize.

Here are my recommendation as a work around until we get to the bottom of this.

A/ Do not attempt to access the objects in the S3 bucked until after the CloudFront distribution is fully "Deployed". And even then I suggest waiting another 15 - 20 minutes.

B/ Delay the UpLoading of your test images until after the Cloud Distribution is Deployed.

C/ If you are stuck now. UpLoad a different image and use the new Image for testing

Here is some additional info.

https://forums.aws.amazon.com/thread.jspa?threadID=216814

Rusty

**S3 – Security & Encryption**

All buckets are private. Access controls can be setup by bucket policies or ACL’s.

S3 buckets can be configured to create access logs which log all requests made to the S3 bucket. Can be done to another bucket.

**In Transit** – when sending information to and from buckets

* **SSL/TLS**

**At Rest** –

* **Server Side Encryption**
  + **S3 Managed Keys** **– SSE-S3** (encrypt it with a master key. AWS handles keys) AES-256
  + **AWS Key Management Service, SSE-KMS** ( Envelope key protects the encryption key from unwanted access, audit trail when keys are used, or you can use own key)
  + **Service Side Encryption with Customer Provided Keys – SSE-C –** Management of key is done by the key.
* **Client Side Encryption** – encrypt on the client side then upload to S3.

**Storage Gateway**

**Storage Gateway** is a service that connects an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organization’s on-premises IT environment and AWS’s storage infrastructure. The service enables you to securely store data to the AWS cloud for scalable and cost-effective storage.

* Available for download as a VM image that you install on a host in your datacenter
* Supports VMware ESXi or Hyper-V
* Could be on a VM on EC2 instance in AWS

Types:

* **File Gateway (NFS)** – store flat files in S3.
  + Files are stored in S3. Accessed through NFS (Network File System) mount point. Once objects are transferred to S3, they can be managed natively in S3
* **Volume Gateway (iSCSI)** – block based storage.
  + - Presents applications with disk volumes by iSCSI. Data can be asynchronously backed up as PIT snapshots and stored in EBS snapshots.
    - EBS virtual block disk.
    - **Snapshots** – **incremental backups** that capture only changed blocks. Compressed to minimize your storage charges.
  + **(Gateway) Stored Volumes** – store entire copy of data set on premise.
    - * Store data locally and asynchronously backing up data to AWS. Provide durable off-site backup. Backed to S3 in the form of EBS snapshots. 1GB to 16TB in size. 100% copy on site and incremental to S3.
  + **(Gateway) Cached Volumes** – store most recently accessed data.
    - * Frequently accessed data (Cached volumes) is kept locally with S3 being your primary data storage. Can create up to 32 TB size and attach the volumes as iSCSI devices to on-premise application servers. 1 GB – 32 TB in cached volumes. Volumes are written to S3. Most likely EBS volumes in S3.
* **Tape Gateway (VTL (Virtual Tape Library))** – backup and archive solution that creates virtual tapes to send them to S3
  + Use existing tape-based backup application to store data on virtual tape cartridges that you create on your tape gateway. Preconfigured with media changer and tape drives which are available as iSCSI devices. Supported by Veam, NetBackup, etc. Sent to S3 and then shelfed to Glacier

**Snowball**

**Import/Export Disk service** – accelerate moving large amount of data in and out of AWS cloud with portable storage devices for transport. Transfers data directly onto and off of storage devices using AWS internal network and bypass internet. Still available.

**Snowball** – PB data transport solution that uses secure appliance to transfer large amount of data into and out of AWS. Cost is 1/5 that of High-speed internet. 80 TB in all regions. Supports TPM and 256-bit encryption with tamper-resistant enclosures. AWS performs software erasure after all the data is transferred. Import to S3 or export from S3.

**Snowball Edge** – contains 100 TB with onboard storage and compute capabilities. Little datacenter to bring on premise. You can run lambda functions locally as well. Supports local workloads in remote locations or transfer storage. Can cluster together and form a local storage tier, etc.

**Snowmobile** – PB or EB of data. Transfer 100PB per snowmobile. 45-foot long shipping container pulled by a semi-trailer truck. Easy to move massive amounts of volumes. Could take up to 6 months.

Lab: