AWS Solutions architect

2017, December, 15

8:47 AM

10k overview part 1

10k overview part 2

Management tools

* Cloud Watch - Very important for sysops
  + Monitoring service
* Cloud Formation - Very important for Solutions architect associate and pro
  + Configurations for deploying sites (wordpress, sharepoint) and servers
  + Turning infrastructure to code
* Cloud trail - Important for security specialty and solutions/sysops assoc solutions and pro
  + Logs changes to AWS environment
  + Cant be used if your hacked and someone is mining bitcoins on your service
* AWS Config - Important for security specialty and solutions/sysops assoc solutions and pro
  + Monitors configs
  + Can show configs backwards in times (hours, days, weeks, months)
* Opsworks - Important for sysops
  + Automating environments (chef and puppet)
* Service catalog - not in any exams
  + Catalog of IT services approved for AWS
  + Important for big companies
* Systems Managers - not in any exams
  + Can be used for patch maintenance across a bunch of ec2 instances
  + Can group resources
  + Doesn’t feature in any exams but needed for sysops role
* Trusted advisor
  + Advice across different disciplines
  + Will tell you if you left your ports open
  + Not using your resources as much as you can
  + Will tell you if you can save money
* Managed services
  + Manages autoscaling and other things

Media services - Not in any exams

* Elastic Transcoder
  + Takes videos that are recording and resizes it so it works on any type of device
* Media convert
  + Video transcoding service
* Media Live
  + Broadcast grade live video processing service
* Media Package
  + Prepares and protects video for delivery over internet
* Media Store
  + Storage service optimized for media
* Media Tailor
  + Targeted advertising on videos without sacrificing quality

Machine Learning - Not in any exams

* Sagemaker
  + Makes it easy for developers to use deep learning
* Comprehend
  + Sentiment analysis
    - People are saying good things or bad things
* Deep lens
  + Artificially aware camera
* Lex
  + Powers amazon Alexa service
* Machine Learning
  + Different from deep learning
    - Deep learning around neural networks
  + Throw a dataset into AWS and analyze dataset and give results
  + Powers amazon recommended items
* Polly
  + Takes text and turns it into speech
* Recognition
  + Video and images
    - Will tell you whats in the image or video
    - Gives you a % of whats in the video
* Amazon translate
  + Just like google translate
* Transcribe
  + Automatic speech recognition of video and mp3
    - Converts it to text

Analytics

* Athena - Not in any exams
  + Run SQL queries against S3 buckets
  + Will go through everything in S3 buckets
* Elastic Map reduce (EMR) - Solutions architect associate and big data specialty
  + Processing large amount of data
  + Chops data up for analysis
* Cloud Search
  + Data search
* Elastic Search
  + Data search
* Kinesis - Solutions architect associate and pro
  + Amazons version of kafka
  + Ingesting large amounts of data into AWS
  + Run processing while loading data
  + Check Owen code from DIG lab
* Kinesis video streams
* QuickSight - Not in any exams
  + Business Intelligence tools
* Data pipeline - Solutions architect profession and dev assoc
  + Moving data between aws service
* Amazon Glue - Not in any exams
  + Amazons ETL (extract transform and load) service

10k overview part 3

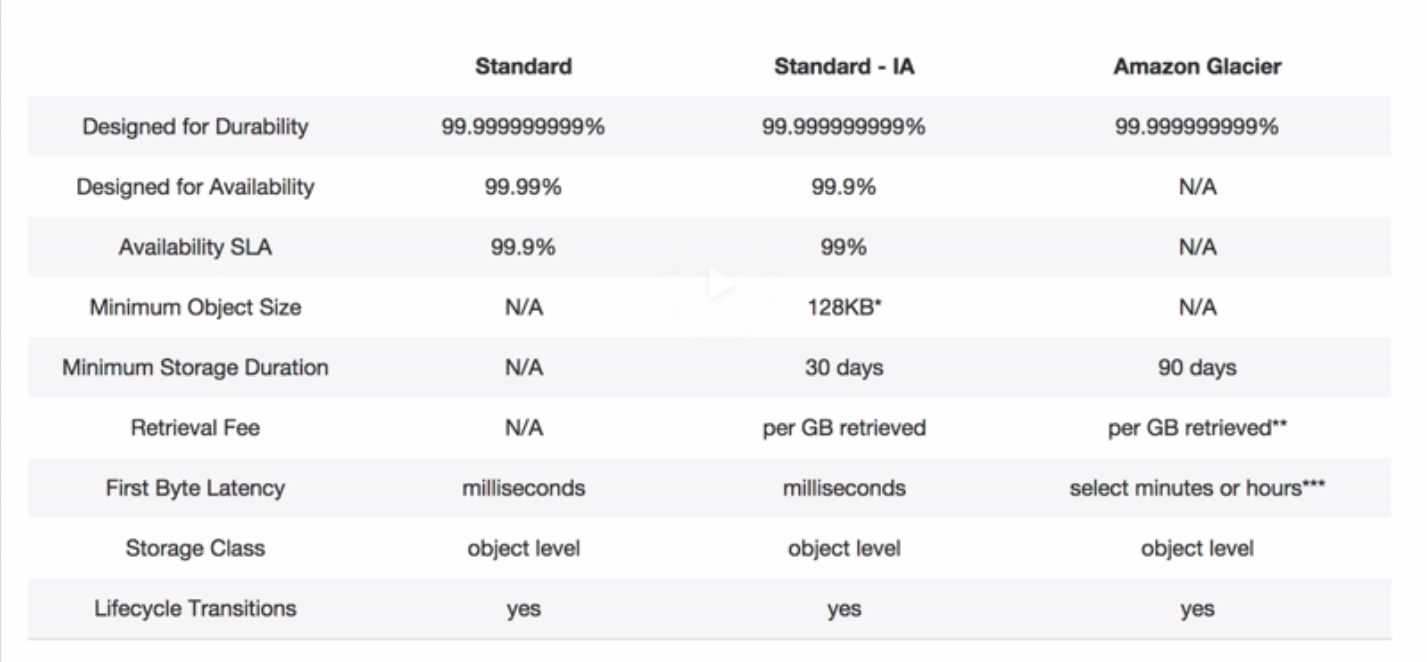
IAM

* Root account is the account when you first setup AWS, it has complete admin access

S3

* Simple Storage Service
* Place to store files on the cloud
* **Object based storage**
  + **There is object and block based storage**
  + **Objects are videos, pdfs, excel sheets (also called flat files)**
  + **Block based storage is somewhere where you would need an OS and you would install a database (EC2)**
* Data is spread over multiple devices and facilities
* **Files can be anywhere from 0 Bytes to 5 TB**
  + **Unlimited Storage**
* Files are stored in buckets (folders)
* **S3 is a universal service so bucket names must be unique globally**
* *Bucket url would be -* [*https://s3-region.amazonaws.com/bucketname*](https://s3-region.amazonaws.com/bucketname)
* If you upload a file you will receive http responses (200 if success)
* **Read after write consistency of PUTS of new Objects**
  + **You will be able to read the file immediately after writing**
* **Eventual consistence for overwrite PUTS and DELETES (can take some time to propogate)**
  + **Don’t get the immediate consistency on changes and deletes due to S3 files being synced across multiple devices and facilities**
    - **If you make a change to a word file and try to read it (quickly withing a few milliseconds) you may get the new data or the old data**
  + **Updates are atomic (one operation at a time) meaning you will always get the new data or the old data, you will not get partially written or corrupted data as the files will be locked for writing**
* **S3 uses a key value store**
  + **Object based and the object consists of**
    - **a key (the name of the object, S3 sorts objects in alphabetical order (lexagraphical))**
      * *If files names are very similar they will be stored in the same location in S3 potentially causing performance hit, to combat this you can add some randomness to the beginning of the name (important note for possible exam question)*
    - **a value (the data, simply a sequence of bytes)**
    - **Version ID**
    - **Metadata (info about data you are storing)**
    - Subresources
      * Access Control Lists (ACLs)
      * Torrent (bit torrent protocol)
* Built for 99.99% availability
* Amazon guarantee 99.9% availability
* Amazon Guarentees 99.999999999% (11 9's) durability of S3 information
* **S3 Tiers**
  + **Standard** 
    - **99.99% availability and 99.999999999% durability**
    - **Can sustain the loss of 2 facilities concurrently**
  + **S3 - IA (infrequently access)**
    - **Data that is needed less frequently but still needs to be accessed rapidly when needed**
    - **Lower fees then S3 (charged a retrieval Fee)**
    - **Example: Data you will only access once a year (payroll info)**
    - **99.9% available**
  + **Reduced redundancy storage**
    - **Designed to provided 99.99% durability (less then 11 9's)**
    - **And 99.99% availability (same as regular S3 service)**
    - **Cheaper then S3**
    - **Example: Data you can regenerate (pictures)**
  + **Glacier**
    - **Very cheap**
      * **As low as 1 penny per GB per month**
      * **Fee for retrieval**
    - **Archival only**
    - **Takes from 3-5 hours to restore (retrieve) from Glacier**

Machine generated alternative text:
Durability 
Availability 
Concurrent facility fault tolerance 
SSL support 
First byte latency 
Lifecycle Management Policies 
Standard 
99.999999999% 
99.99% 
Yes 
Milliseconds 
Yes 
Standard - Infrequent 
99.999999999% 
99.9% 
Yes 
Milliseconds 
Yes 
Reduced Redundancy 
Storage 
99.99% 
99.99% 
Yes 
Milliseconds 
Yes 



* S3 Charges
  + Charged for Storage
  + # of requests being made to objects in buckets
  + Storage Management Pricing on a per tag basis
    - Add tags to data (this data is for HR etc)
  + Data transfer pricing
    - Data coming into S3 is free
    - Data transfer or replication across regions has a cost
  + Transfer Acceleration (this is a service)
    - Fast and secure way of transferring files over long distances between you end users and an S3 bucket
    - Takes advantage of CloundFronts globally distributed edge locations
      * As data arrives at an edge location it is route to S3 over an optimized network path
* \*\*\*\* Before Exam Read through the S3 FAQ \*\*\*\*\*

**Versioning Lab**

* Once versioning is turned on you cannot disable it only suspend
* Once enabled multiple copies of each file will be kept in S3
  + Versioning not a good idea for large files that can change often
* To restore from previous version
  + Download old version and reupload to S3
  + Hit delete button on the drop down menu to delete the latest version
* When you delete an item with version control on it places a delete marker when you select show versions
  + This delete market can be "deleted" which will restore the object
* <https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html>
* MFA Delete is an option that can be added to add an extra layer to versioning by utilizing their security credentials + a valid serial#, space, and a 6 digit code displayed on a authentication device
  + Users cannot change the versioning state
  + Or Delete an object
* Initial objects have a versioning state of NULL

**Cross Region Replication (Rewatch and do lab - Need CLI)**

* <https://docs.aws.amazon.com/AmazonS3/latest/dev/crr-what-is-isnot-replicated.html>
* <https://aws.amazon.com/answers/infrastructure-management/crr-monitor/>
* <https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region\>
* Cross region replication requires versioning to be enabled
* **Only new/changed objects will be replicated, existing files in source bucket will not be replicated**
* Cross region replication does not copy the permissions
  + Even if permissions are then updated on original bucket
  + **Permissions of newly created objects are replicated**
* Deleted files (markers in versioned files) from the source bucket it is replicated to the destination bucket
  + Deleting individual delete markers does not replicate
    - When you delete the delete market the destination bucket does not delete the delete marker
* Deleting a specific version of a file in the source bucket will not delete the version on the replicated bucket
  + *Therefore if you revert to a version in your main bucket you must also perform this change on your replicated buckets*
* *Regions must be unique if using CRR but if you use the copy command they can be in same region*
* *You cannot replicate to multiple to multiple buckets (or use daisy chaining) at this time*

**IA and Glacier (Rewatch and do lab)**

* Lifecycle management
  + When data is only really used for a certain time period may be a good idea to transition it to IA (after 30 days) then to glacier (after 60 days)
  + Can set different lifecyles for different versions compared to the current version
  + Can set a lifecycle for objects to be expire (cleaned up)
  + Used in conjunction with versioning
  + **Following actions can be done**
    - **Transition to Standard Infrequently access storage**
      * **128KB and 30 days minimum**
    - **Archive to glacier**
      * **By default 30 days after migrate to IA**
    - **Permanently Delete objects**

**Cloud Front (Imporant - Review)**

* Content delivery Network is a system of distributed servers (network) that deliver webpages and other web content to a user based on the geographic location of the user, the origin of the web page and a content delivery server
* **Edge location**
  + **A location where content will be cached (separate from AWS region / AZ)**
  + **Not read only, can be written to as well**
    - **This file will be replicated back to origin server**
  + **You can clear cached objects but you will be charged**
* Origin
  + The is the origin of all the files that the CDN will distribute
    - This can be
      * S3 bucket
      * EC2 Instance
      * Elastic Load Balancer
      * Route 53
* Distribution
  + This is the name given to the CDN which consists of a collection of edge locations
    - Consists of
      * Web distribution (Used for websites)
      * RTMP (Used for Media Streaming)
* Users will make a request to an edge location using a distribution URL
  + **The edge location will first check if the content is cached at this edge location**
    - **If it is not cached then the Edge location makes a request back to the source (S3 bucket etc) and caches it for the *term to live (TTL)***
  + **Not necessarily faster then traditional method of user pulling file from Original source but only for the first user, once file is cached in CDN it is dramaticall faster**

Machine generated alternative text:


* **Origin server can be a non - AWS server that stores the original version of your files**

**Cloud front lab - Creating a CDN (rewatch this and do lab)**

**S3 Security and Encryption**

* By default buckets are set to PRIVATE
* You can setup access to buckets using
  + Bucket polocies are bucket wide
  + Access Control Lists
    - These can drill down and apply permissions to specific objects
* Buckets can be configured to create access logs
  + This will log all requests to S3
    - Can be logged to another bucket
* **Encryption**
  + **In Transit**
    - **When you are transferring data from your PC to AWS**
    - **SSL/TLS**
      * **HTTPS**
  + **Data At rest**
    - **Server Side**
      * **S4 Managed Keys - SSE-S3 (AES-256)**
        + **AWS manages keys and the keys are encrypted by a master key which is regularly rotated**
      * **AWS key management service SSE-KMS**
        + **Uses an envelope key which encrypts your data keys**
        + **Provides an audit trail (when and who keys were used by)**
        + **Can manage encryption keys yourself**
      * **Server Side encryption with customer provided keys SSE-C**
        + **You manage keys but AWS manages the encryption as its written to disk and when it is decrypted**
    - **Client Side encryption**
      * **Data is encrypted before being uploaded to S3**

**Storage Gateway - popular exam topic**

* **Service that connects an on-premises software appliance with cloud storage**
* Will replicate data from a dataware house to S3 Via a hypervisor virtual machine
* Is a virtual appliance
* 4 Different types
  + File Gateway (NFS)
    - **For flat files only**
      * **For the storage of Word files, pdfs, pictures / videos**
      * **Not storing any files locally they are sent directly to S3**
    - Files are stored in S3
      * Once files are stored in S3 they can be managed as native S3 objects
        + Lifecycle management
        + Bucket policies
        + Versioning
        + Cross region replication
    - Access through a Network File System (NFS) mount point

Machine generated alternative text:
mrect Cuæct 
NFS 
Storage Gateway 
Amana VE 
Arnazon 
Glacier 
Application 

* Volumes Gateway (iSCSI)
  + Block storage
    - Storage you would install an OS on
    - Examples
      * Virtual hardisk
      * Server that you would install SQL Server on
  + Not date you will store on S3
  + **Take virtual on premises hard disks and back them up into AWS**
  + Snapshots are incremental backups so only changes are captured
  + Data is compressed to lower costs
  + 2 types
    - Stored Volumes
      * When you store an entire copy of you dataset on-site (on-premises)
      * Entire dataset store on premises and backed up to S3
    - Cached Volumes
      * When you are storing the most recent copy of the dataset on-site and the rest of the data is stored in AWS
      * Only the newest copy is retained on prem and everything goes to AWS
      * 1GB - 32TB sizes

* Tape Gateway (Virtual Tape Library)
  + Lets you leverage your existing tape based backup application
  + Allows you to create virtual tapes and send them to S3
    - Can use lifecycle tools to send to glacier etc..
  + Data written to these virtual hard disks can be asynchronously backed up as point in time snapshots and stored as Amazon EBS snapshots

Machine generated alternative text:
Volume Gateway 
Your Data Center 
Application 
Server 
- Stored Volumes 
Gateway VM 
A CLOUD GURU 
Amazon S3 
Snapshots 
Volume 
Stor. 
Buffer 
Storage Area Network. Network 
Attached Direct Attached Stora 

Machine generated alternative text:
Volume Gateway - Cached Volumes 
A CLOUD GURU 
Amazon S3 
Snapshots 
Volume Storage 
Your Data Center 
Cliert 
Application 
Server 
Gateway VM 
Cache 
Stor. 
Upload 
Buffer 
Hypervisor 
Storage Area Network, Network 
Attached, or Direct Attached Storage 

Machine generated alternative text:
Volume Gateway 
- Tape Gateway 
Gateway VM 
A CLOUD GURU 
Tap. 
Tap. 
by 
T. by 
Sty. NetMA. 
Attxt.d 
Gateway V" 
C' Attxr.a 

**Snowball**

* Import/Export
  + Old system before snowball
  + Sent in own discs to Amazon
    - This became unsustainable
* Petabyte scale data transport solution
* Stream data to AWS without using internet
* Load data into appliance and send it to amazon
  + They load this data into S3
* Cheaper then streaming over internet
* Multiple layer of security
  + Tamper proof enclosure
  + 256 bit encryption
  + Trusted platform module (TPM)
    - Ensures security and chain of custody
    - Can track where snowball is at anytime
* Amazon wipes all snowball appliances after use
* **3 types**
  + **Snowball**
    - **80TB in size**
    - **Import to S3**
    - **Export from S3**
  + **Snowball Edge**
    - **Looks similar to snowball**
    - **100TB of storage**
    - **Contains compute capabilities**
      * **To run lambda functions**
      * **Allows you to bring compute to external facilities not connected via internet**
        + **EG: Deployed on airplanes**
  + **Snowmobile**
    - **Petabyte or Exabyte levels of data**
    - **100PB per snowmobile**

**S3 Transfer Acceleration**

* **Utilises cloudFront edge networks to accelerate your uploads to S3**
  + **Instead of uploading directly to your S3 bucket you can use a distinct URL to upload directly to an edge location which will then transfer that file to S3**
  + Utilise backbone AWS network instead of internet
    - This network is more optimised to make it faster
  + *EG: <bucketname>.s3-accelerate.amazonaws.com*
  + Setting to enable is in bucket settings

**Making an S3 Site**

* Website URL and bucket name need to be the same
  + URL: hotmail.com
  + Bucket: hotmail
* Static website hosting URL
  + **<bucketname>.s3-website-<region>.amazonaws.com**

**S3 Summary - (Finish summary ~7:30)**

* S3 is Object storage
  + Not suitable for installign an OS
  + Not suitable for installing a database on
* Files can be 0 to 5TB
  + Virtual unlimited storage
* Files stored in buckets
  + Universal namespace
  + Names must be unique globally
  + S3-<region>.amazonaws.com/<bucket name>
* Read after write consistency for puts of new objects
* Eventual consistency for puts and deletes
* S3 Storage Tiers
  + S3 (Durable, Immediately available, frequently accessed)
    - 11 9s durability
  + S3 - IA (durable, immediately available, infrequently accessed)
  + S3 - Reduced redundancy Storage (Data that is easily reproducable)
    - 99.99% durability
  + Glacier
    - Archived Data
    - Wait 3-5 hour wait
    - Cheapest
* Core fundamentals
  + Key value store
    - Key (name)
    - Value (data)
    - Version ID
      * Stores all versions
      * Pay for all versions
    - Metadata
    - Access control Lists

**EC2 101 - Part 1**

* EC2 Is a server that provides resizable compute capacity in the cloud
  + Reduces time required to obtain and boot new server instances to minutes
  + Paying only for the capacity you use
* EC2 Options
  + On Demand
    - Allows you to pay a fixed rate by the hour (or by the second) with no commitment
    - Useage
      * No up front or long term commitment
      * Applications with short term spiky unpredictable workloads
      * Applications being developed or tested on EC2 for the first time

* Reserved
  + Capacity reservation
  + 1 or 3 year terms
  + Offer a significant discount over hourly
  + Usage
    - Applications with steady state or predictable usage
    - Applications that require reserved capacity
    - Standard Ris
      * Can save up to 75% off on demand
    - Convertible Ris
      * Can be converted to an instance type of equal or greater value
    - Scheduled Ris
      * Available to launch within reserved time window
* Spot
  + Enable you to bid whatever price you want for instance capacity
  + Providing greater savings if you have flexible start and end times
  + With spot instances if you terminate after 30 mins you still pay for the whole hour
    - If AWS terminates the spot instance because the price went up you get that hour for free
  + Usage
    - Applications that have flexible start and end time
    - Applications that are only feasible at very low compute prices
    - Users with urgent need for extra compute capacity
* Dedicated hosts
  + Physical EC2 servers dedicated for your use
  + Help reduce costs by allowing you to use your existing server-bound software licenses
  + Usage
    - Useful for regulatory requirements that may not support multi-tenant virtualization
    - Great for licensing which does not support multi-tenancy or cloud deployments
    - Can be purchases on demand or reserved

Pneumonic: DR Mc GIFT PX

* Machine generated alternative text:
  Family 
  G2 
  Speciality 
  Dense Storage 
  Memory Optimized 
  General Purpose 
  Compute Optimized 
  Graphics Intensive 
  High Speed Storage 
  Field Programmable Gate Array 
  Lowest Cost, General Purpose 
  Graphics/General Purpose GPI-J 
  Memory Optimized 
  Use case 
  Fileservers/Data Warehousing/Hadoop 
  Memory Intensive Apps,'DBs 
  Application Servers 
  CPU Intensive Apps/DBs 
  Video Encoding/ 3D Application Streaming 
  NoSOL DBS, Data Warehousing etc 
  Hardware acceleration for your code. 
  Web Servers,'Small DBS 
  Machine Learning. Bit Coin Mining etc 
  SAP HANA/Apache Spark etc 

Machine generated alternative text:
How I remember them now; 
D for Density 
R for RAM 
M - main choice for general purpose a 
C for Compute 
G - Graphics 
I for IOPS 
F for FPGA 
ps 
T cheap general purpose (think T 2 Micro) 
P - Graphics (think Pics) 
X - Extreme Memory 
ScoTCANts 

**EC2 101 - Part 2**

* What is EBC
  + Allows you to create block storage volumes and attach them to EC2 instances
    - Block storage so unlike S3 you can install databases, OS's and applications on them
  + Placed in a specific Availability Zone where they are automatically replicated against the failure of a storage array (not to different AZs)
* General Purpose SSD (GP2)
  + General performance SSDs
  + 3 IOPS per GB with up to 10,000 IOPS
    - Ability to burst up to 3000 IOPS at 3334GiB and above
* Provsioned IOPS SSD (IO1)
  + Designed for I/O intensive applications such as large relational or NoSQL Databases
  + Use if you need more then 10,000 IOPS
  + Can go up to 20,000 IOPS per volume
* Throughput Optimised HDD (ST1)
  + Magnetic disk
  + Big Data
  + Data warehouse
  + Log processing
  + Sequential data
    - Data that is written in sequence
  + Cannot be a boot volume
* Cold HDD (SC1)
  + Lowest cost storage for infrequently access workloads
  + File server
  + Cannot be a boot volume
* Magnetic (Standard)
  + Lowest cost per GB of all EBS volume types that is bootable
  + Ideal for workloads where data is accessed infrequently and low cost is important

**Well architected framework - Intro**

* <https://d0.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf>
* Written by solutions architects world wide based on their experiences
* 5 pillars
  + Security
  + Reliability
  + Performance Efficiency
  + Cost Optimization
  + Operational Excellence
* General Design Principles
  + Stop guessing capacity needs
    - Use auto scaling
  + Test systems at production scale
  + Automate to make architectural experimentation easier
  + Allow for evolutionary architectures
  + Data Driven Architectures
  + Improve through game days
    - Simulate major events in production

**Well Architected Framework - Pillar One Security**

* Design principles
  + Apply security to all layers
  + Enable Tracability

Appendix - Well architected framework: Security

