**Cloud Notes**

**AWS Global Infrastructure**

**Region** = physical location in the world which consists of two or more availably zones geographical area.

**Availability Zones (AZ)** = One or more data centres – housed in separate facilities still within the same region. Always put stuff across multiple AZ as if one fails you have stuff in another. Geographically isolated.

**AWS Edge location =** endpoints in AWS which are used for caching content. If someone in Sydny pulls down stuff from London this will be stored in a AWS edge location after the first person has pulled it down. 96 edge locations. Caching services.

**Cloud Front:** CDN network

**COMPUTE**

**EC2 –** Elastic compute cloud. VM’s within the AWS platform, can have dedicated machines as well.

**EC2 Container –** Run and Manage Docker Containers at scale.

**Elastic Beanstalk –** For devs who just want to upload code. This service provisions EC2 instances and Load Balancers.

**Lambda –** code upload to cloud and control when executes, not got to worry about VM’s/ operating systems. Severless.

**Lightsail -**  Virtual Private Server service: people who don’t want to understand AWS. Gives you a server, gives you an IP and gives you SSH. Watered down EC2, all you worry about is the OS

**Batch –** Batch computing in the cloud

**STORAGE**

**S3 –** Simple Storage Service, object based stored, upload into buckets

**EFT –** elastic filesystem – network attached storage and mount to multiple machines

**Glacier –** Data Archive. If you check something every year, it would be good putting it in here.

**Snowball –** bring in large amounts of data into AWS, instead of transmitting over broadband, bringing in terabytes of data straight into a data centre

**Storage Gateway –** VM’s you install in your data centre/ head office replicate information back to S3.

**DATABASES**

**RDS –** Relational Database Service – mySQL/ SQL Server/ Postgress. Any relational database

**DynamoDB –** For non relational DB – DB Service.

**Elastic cache –** Caching commonly queried things from your DB server. Freeing up DB servers to carry on querying.

**RedShift –** Used forData warehousing/ Business Intelligence queries

**MIGRATION –** Visualising the migrations to AWS

**AWS Migration Hub -**  Tracking service, tracking applications as they move to AWS

**Application Discovery Service –** Automated set of tools detects applications and dependencies if you have a sharepoint server this might have an SQL DB as a dependency.

**Database Migration Service –** Migrating on prem databases to AWS

**Server Migration Service –** Helps you migrate virtual and physical servers into AWS Cloud.

**Snowball –** Migrating large amounts of data into the cloud.

**NETWORKING/CDN**

**VPC – Virtual Private Cloud-**  Virtual Datacentre, configure firewalls/ Networking ect.

**Cloudfront –** Content Delivery network, caching service which allows storage nearer the users who are requesting the data from an edge location.

**Route 53 –** Amazon DNS – lookup service of URL to IPv4 and IPv6

**API Gateway –** Creating own API’s for other services to talk to.

**Direct Connect –** Running a dedicated line from corp head office/ data centre to VPC

**DEVELOPER TOOLS**

**CodeStar -**  Group of devs working together, set up code and release in mins.

**Code Commit –** Place to store code. Source Control Service, store own private GIT repos within codecommit.

**Code build –** When the code is ready, Code Build builds the code, runs tests against it and produces software packages which are ready to deploy.

**Code Deploy -** Automates deployments to EC2 instances/ on prem instance or lamda function.

**Code Pipeline –** Continuous Delivery Service model and visualise steps to release software.

**Xray-** Debug and analyse serverless applications**,** request tracing to see logs

**Cloud9 –** Develop code within AWS console don’t need. Integrated Development Environment.

**MANAGEMENT TOOLS**

**Cloud Watch –** Monitoring service can set billing alerts and billing alarm.

**Cloud Formation -**  way to script infrastructure, take a cloud formation template and deploy a word press site ect, reuse to deploy inside Sydney/London, people open source templates for cloud formation.

**Cloud Trail –** Logging changes to AWS environment, stores records for 1 week, ever get hacked figure out how and where using service.

**AWS config –**monitors entire config of AWS environment, point in time snapshots, move

**Ops works -**  Chef and Puppet way to automate environments so all environment config

**Service Catalog -**  Manage catolog of IT services which are approved for use on AWS from VM images/ databases/. Catalog service – used by goverments and regulatory envirionemtns

**Systems Manager –** Interface for managing AWS istancnes. Patch mantience, across thousands of EC2. Group all resources by deprtment finance/HR/ Sharepoint ect.

**Trusted Advisor -**  give you advice around a lot of disciples, accountant/ advisor advice on AWS environment.

**Managed Services –** managed services.

**MEDIA SERVICES**

**Elastic Transcoder –** Takes the video and resizes it so it looks good on different devices.

**MACHINE LEARNING**

**Sage Maker –** makes it easy for develpers to use deep learning when coding for their environemnts

**Comprehend -**  Sentiment analysis on data (good/bad things about product).

**Deep lens -**  AI aware camera which

**Lex -**  What powers alexea service, AI way of chatting to customers.

**Machine Learning -**  thow a data set into AWS cloud analyse dataset and predict an outcome, every time you go to amazon.com the recommended products are from machine learning.

**Polly –** Takes text and turns into speech,

**Rekognition –** Tells you what is in pictures/ videos.

**Amazon Translate –** Translates languses.

**Amazon Transcribe –** Auto speech regognition, upload video files/mp3’s and takes what it regognises and turns into text.

**ANALYTICS**

**Athena –** run SQL queries agasint S3 buckets, servless.

**EMR –** Elastic Map Reduce, used for processing large amounts of data big data solutions, chops data up for analysis.

**Cloud Search + Elastic Search Service –** Searching service.

**Kinesis –** way of injesting large amounts of data into AWS, social media feeds ect.

**Kinesis Video Streams –** Injest video sterams and injest data.

**Quick Site –** BI tool for AWS

**Data Pipeline -**  way of moving your data between different AWS services.

**Glue -**  Extract Transform Load service which does this.

**SECURITY IDENTIY AND COMPLIANCE**

**IAM –** Identity Access Management,

**Cognitio -**  Device authentication, using facebook/ linkedin, once authenticated use cognito to request access to AWS resources. Authentication service which gives temporay access to AWS for mobile devices.

**Guard Duty -**  Monitors for malicious activity on AWS

**Inspector –** install on VM’s/ EC2’s run a lot of tests any security vulnerabilities and gives a repot. Severtity report.

**Macie -**  Scan S3 bucket and look for PII data.

**Cert Manager -**  SSL Managing certifcates.

**Cloud HSM –** Hardware Secuirty Module. Dedicated hardware to store keys which you use to access EC2 instance. Store other encypotion keys in there. Dedicated

**Directory Service -**  Integrating MS Active Directory services with AWS services.

**WAF-**  Webapplication firewall stops things like SQL injections/ Cross Site Scripting. Works at the application layer and looks at the users behaviour to prevent this.

**Shield -**  Default with Cloud Front + Load Balancers. DDOS mitigation. Advancwed Shield, dedicated team of people to prevent DDOS attacks

**Arifact –** Portal to download on demand AWS compliance reports + manage select agreements. PCI reports ect ect.

**MOBILE SERVCIES**

**Mobile Hub -**  Management console for mobile apps

**Pinpoint -**  targeted push notifications push out notifications to users

**AWS App Sync –** Updates data in web and mobile apps in real time updates data for offline data when they come back online.

**Device Farm -**  testing apps on real live devices.

**Mobile Analysitics -**  Analytics for mobile.

**AR/VR –** Augmented Reality and Virtual Reality

**Sumerian –** First language which was written down. Used for AR/VR and 3D application design allows.

**APPLICATION INTEGRATION**

**Step functions –** managing lambda functions and steps to go though them.

**Amazon MQ-**  Message queues

**SNS/ SQS/ SWF –** SQS is the oldest service.

SNS – Notification Service

SQS – Decoupling infrastructure sending requests to EC2 instance go though the SQS service

SWF – simple workflow service – can have human beings as a part in the process.

**CUSTOMER ENGAGEMENT**

**Connect –** Contact Center as a service.

**Simple Email Service –** Easy way of sending large amounts of emails and cost effective, pay as a you go.

**BUSINESS PRODUCTTIVITY**

**Alexa for business –** use it 4to dial into a meeting room/ order ink ect.

**Chime -**  Video conferencing works very accuracrtly.

**Work Docs –**Drop box for AWS storing work related docs

**Work Mail –** Email though amazon also like google mail.

**DESKTOP AND APP STREAMING**

**Workspaces –** VDI running operating system in amazon cloud and streaming down to device

**App Stream -**  Stream application to the device very similar to Citrix.

**IOT**

**IOT Device Management –**Managing IOT devces at scale.

**Free IOTS -**  Operations system for micro controllers.

**Greegrass –**Software which lets you run local

**GAME DEVELOPMENT**

**Gamelift –** Help you dvelp games in AWS cloud

**IDENTITY ACCESS MANAGEMENT**

Allows you to manage users access to console,

Gives you:

* Centralised Control to AWS account
* Shared Access to AWS account#
* Granular Permissions – user permissions
* Identity Federation – Connect IAM to Active Directory/ Facebook – means you can federate with different identity providers
* Multi factor Authentication – Two factor Auth
* Temporary Access for Devices/Services where necessary.
* Set up and manage password protection policy
* Supports PCI/DSS compliance

**Critical Terms**

**Users** = End users

**Groups** = collection of people under one set of permissions, grouping users together and setting one policy per group. Developers/ Sysops

**Roles** = Create roles and assign them to resources. Might have a virtual machine (EC2 instance) give it the role to access S3 and then that EC2 instance can write into S3, no need to set up username/password for that EC2 instance.

**Policies** – Document defines one or more permissions. Applied to users, groups and roles. Connect to each other. Policy sits on top of IAM. JSON format.

**IAM doesn’t have a region, it is global create users, groups and roles available all over the world.**

**Root Account =** Email add used to sign up with AWS, root account gives you unlimited access to do things in the cloud. Don’t want whole organisation to have all that power. Complete admin access by default.

**Power User -**  access to all AWS services except management of groups and users within IAM.

New users have no permissions when first created.

Always need MFA on root account to stop people from using the AWS without correct permission level.

Programmatic Access = command line / Application access.

Access Key ID + Secret Access Key – what you would use to programmatically access AWS instance can’t use it to log into console. Only get access to see once.

Can set password rotation policies.

Attach permissions (policies) directly to users as well as groups.

**Roles = grant permissions for entities which you trust like an EC2 instance.**

Allow EC2 instances to call AWS services on my behalf.

Have EC2 instance able to store files on S3.

Creating a role for EC2 instance to write to S3.

**S3**

Simple Storage Service.

Secure/ Durable/ Highly Scalable Object Storage

Place to store files

Object Based – Video/PDF/ Image = flat file

Block Based – Databases/ places where you would need operating systems.

Data spread across multiple devices and multiple locations

S3 is not where you would install a database/ operating system as performance would be awful.

0 bytes 🡪 5TB in file size.

Unlimited Storage

Files are stored in buckets (folder)

Buckets = folders

S3 universal namespace bucket name can only be used once using a DNS namespace.

**S3 – region amazon.aws.com/bucketname**

Upload a file, get a HTTP 200 code if successful

Data Consistency Model

New object in S3 – read straight away, when updating/deleting can take some time to propagate – few milliseconds.

Updates = Atomic, either new or old data.

S3 Objects consist of the following

**Key** – File name of object. S3 sorts things in alphabetical order (lexogrpahical)

**Value** – Data – sequence of bytes.

**Version ID** – important for versioning.

**Meta-data** – data about data, date uploaded ect.

**Sub resources –** Access control lists – who can access this object. Do this for an object or do it from bucket level.

**Torrent –**S3 supports Bit Torrent Protocol.

99.99% availability

99.99999999999% durability – (11 nines durability guarantee) – not going to loose file.

Lifecycle Management – If data is > 30 days old, move to another storage tier then >90 days archive it off.

**Tired Storage Options** –

S3: 11 nines durability model, designed for the loss of two facilities concurrently good for frequently accessed storage.

S3 Infrequent Access – For data that needs to be access less frequently Lower fee than S3 but are changed a retrieval fee.

Reduced Redundancy Storage – 99.99% durability opposed to the 11 nines of durability but a lot cheaper. Data you can generate again, such as thumbnails of images stored in S3.

First Byte Latency = Milliseconds

Glacier – 3/5 hours restore from Glacier, 11 nines durability, no SLA for glacier first byte latency = hours. Infrequently access data.

**Charging**

Storage – how much data storing

Requests – Number of requests that are being made for S3 buckets

Storage Management Pricing – Add tags to data to charge per tag basis so all HR can get charged for their data.

Data Transfer Pricing - data coming in is free, moving data around is charged.

**Transfer Acceleration** – Enables fast/easy/ secure transfers of files over a long distance. This uses Amazon Cloudfront globally distributed edge locations and data is then routed to S3 over optimised network path. Option to turn on/off.

Versioning -

Encryption:

Encryption – Sever Side encryption, means if looking at physical disk then look to encrypt the data on the disk.

* Client Side encryption – done locally
* Server Side encryption with Aamzon S3 managed Keys (SSE-S3)
* Sever Side encryption with KMS
* Server Side encryption with own keys

Secure data with access control lists/bucket policies

Manage S3 at a global level

By default all buckets are private

Objects within buckets don’t inherit the buckets tags automatically.

Minimum size is 0 bytes