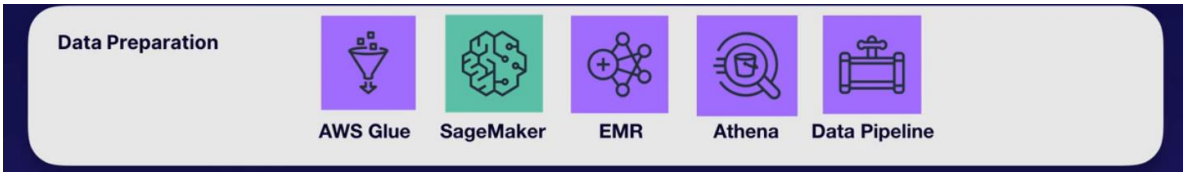
Table of content

Data preparation



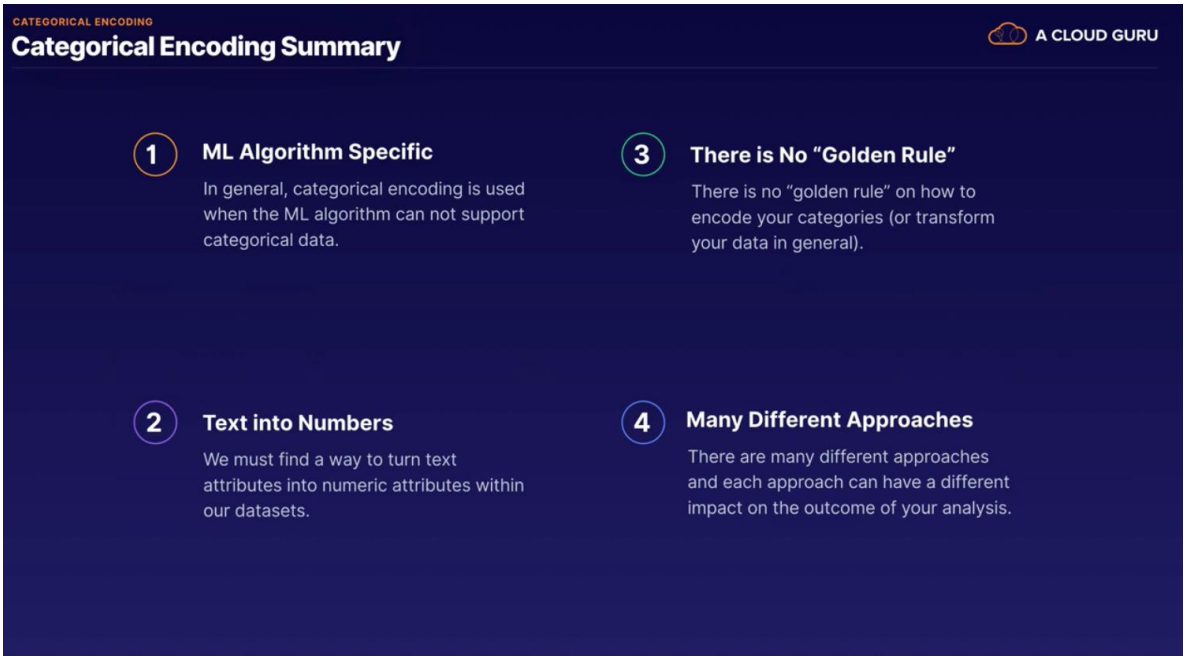
Categorical encoding

Changing category into a number

Categorical value = Categorical Feature = Discrete feature

Ordinal is when the order matters (ex. Bronze, silver and gold)

Nominal is when it doesn't matter



One hot encoding

Transforms nominal categorical features and creates new binary columns for each observation

Text feature engineering

Splitting text into byte size pieces

Bag of words

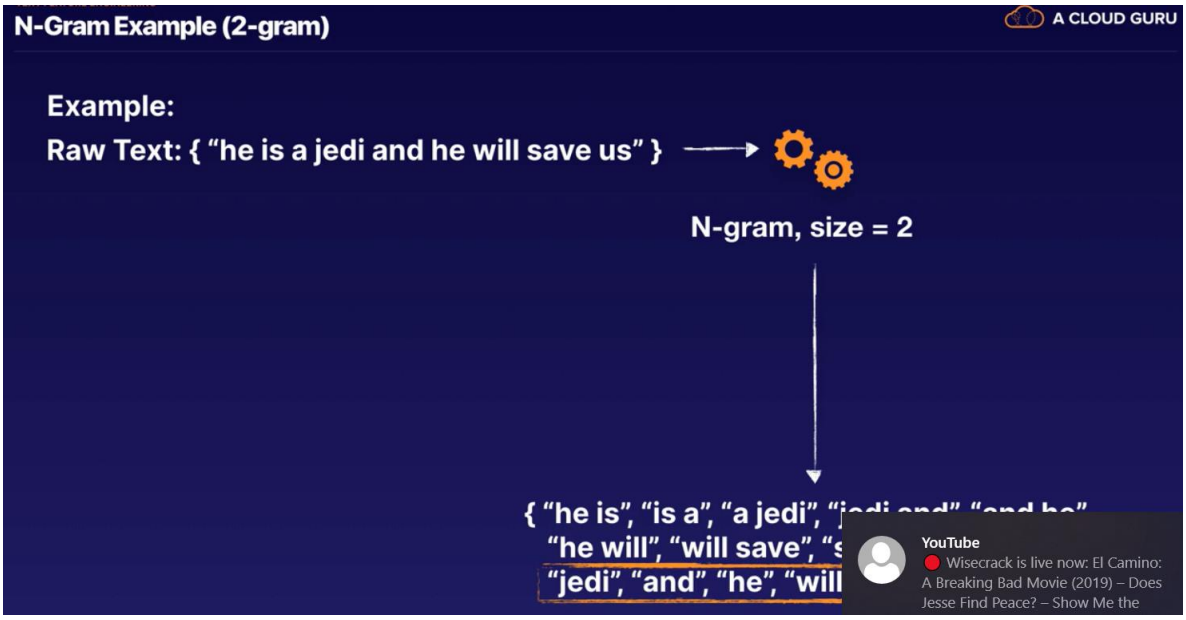
Breaks up text by white space into single words

N-grams

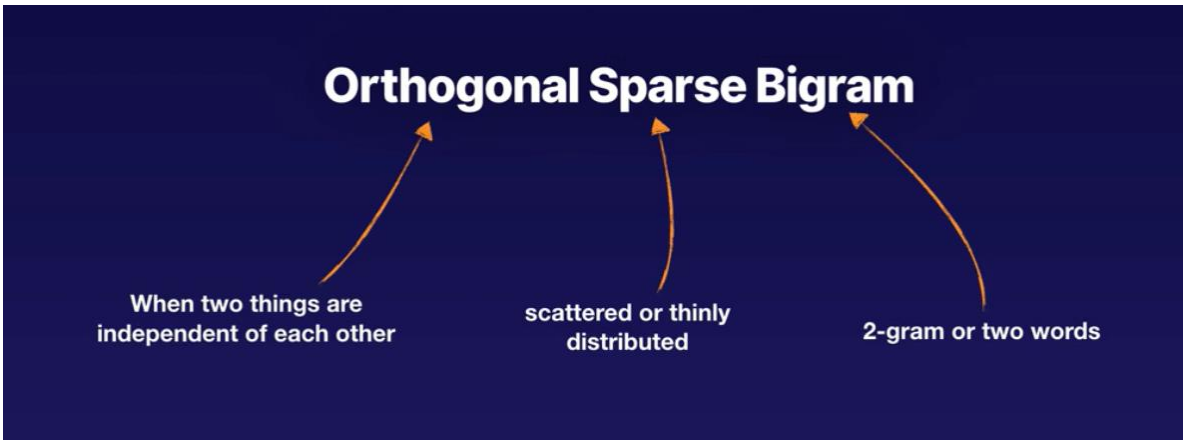
Produces groups of words of n-sizes

It produces also n-grams of all sizes

Unigram, bigram, trigram, etc..



Orthogonal Sparse Bigram

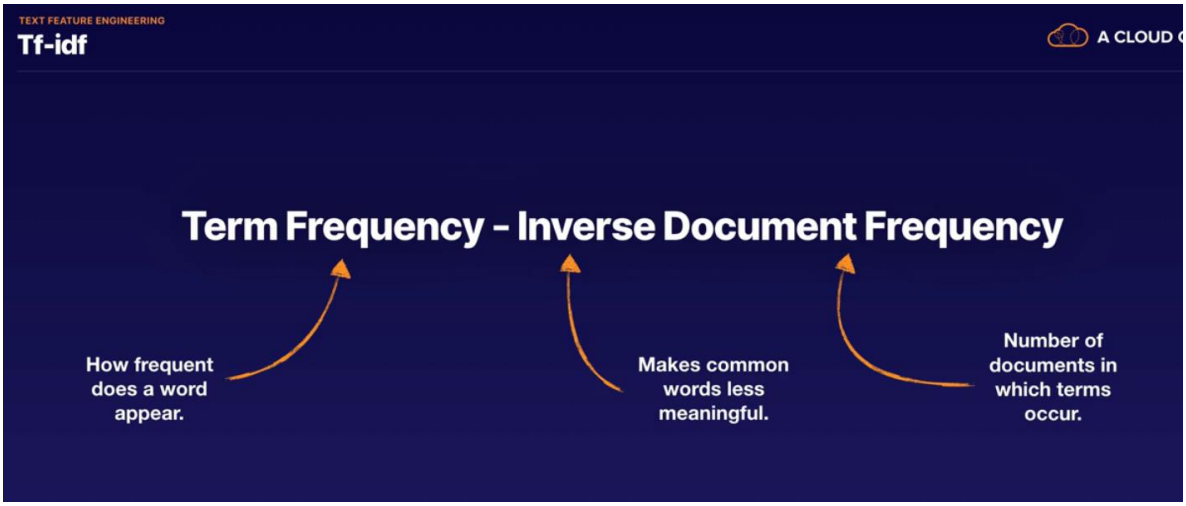


Example:

OSB, size =4

He is a Jedi = he_is, he__a, he___Jedi, is_a, is__Jedi

TF-IDF



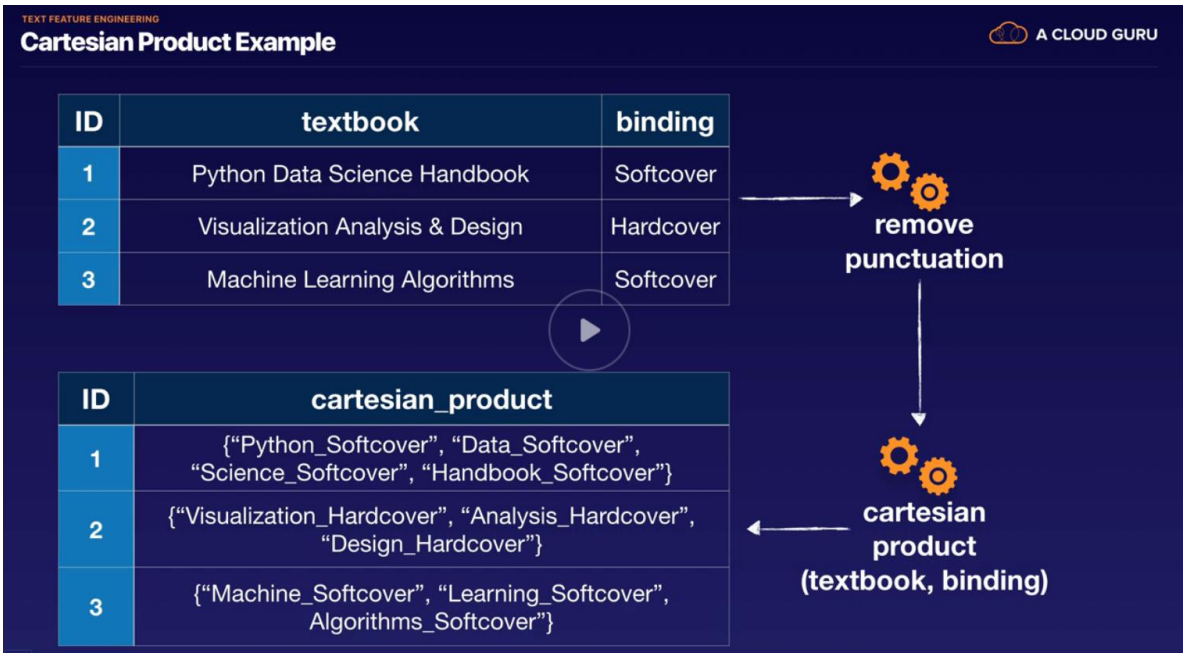
Remove punctuation

Cleaning and standardization

Lowercase transformation

Cleaning and standardization

Cartesian Product Transformation



Numeric feature engineering

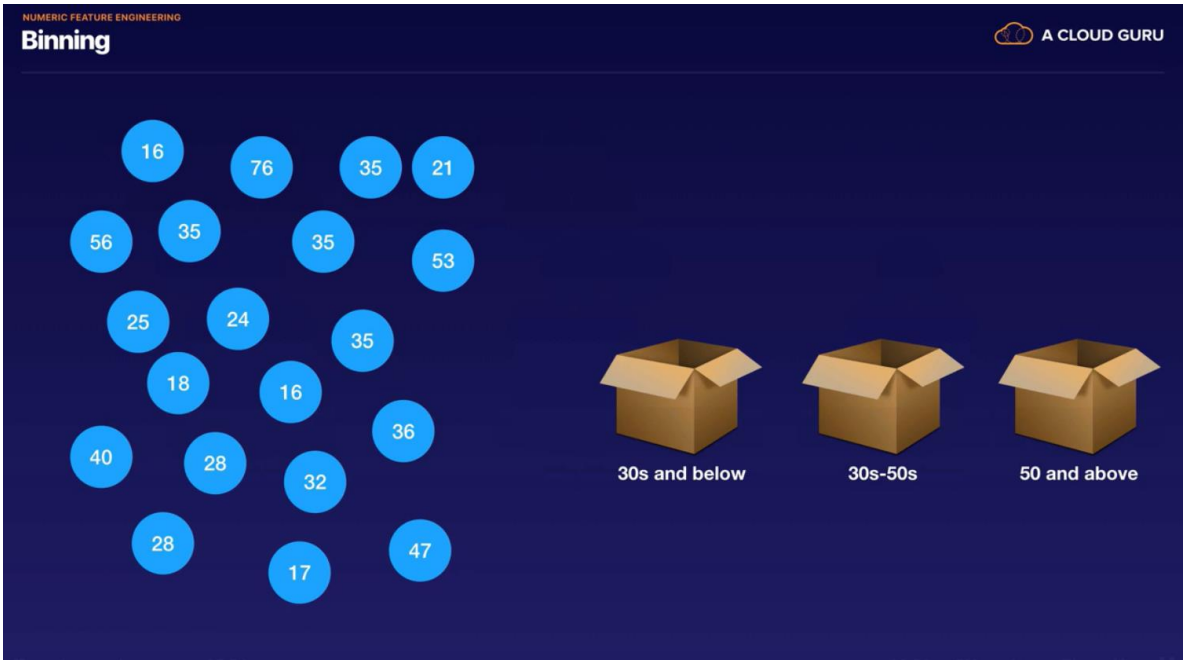
Normalization

The max number becomes 1, the lowest becomes 0

Standardization

Average price is 0, and z-score to smooth out numbers

Binning

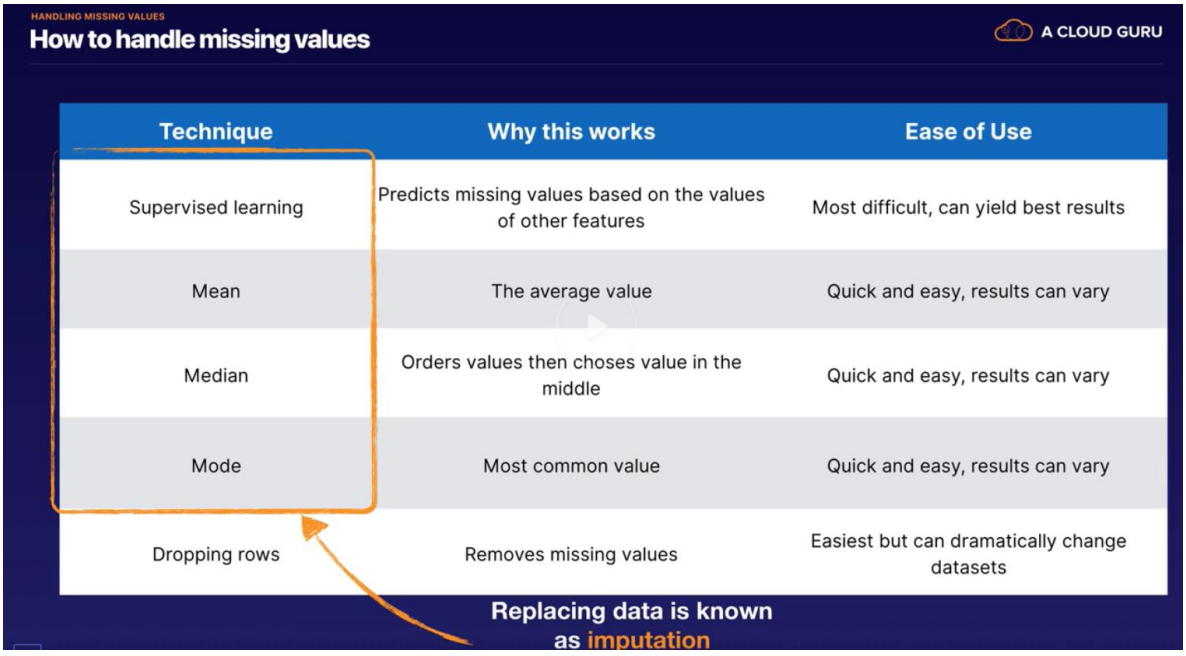


Quantile binning

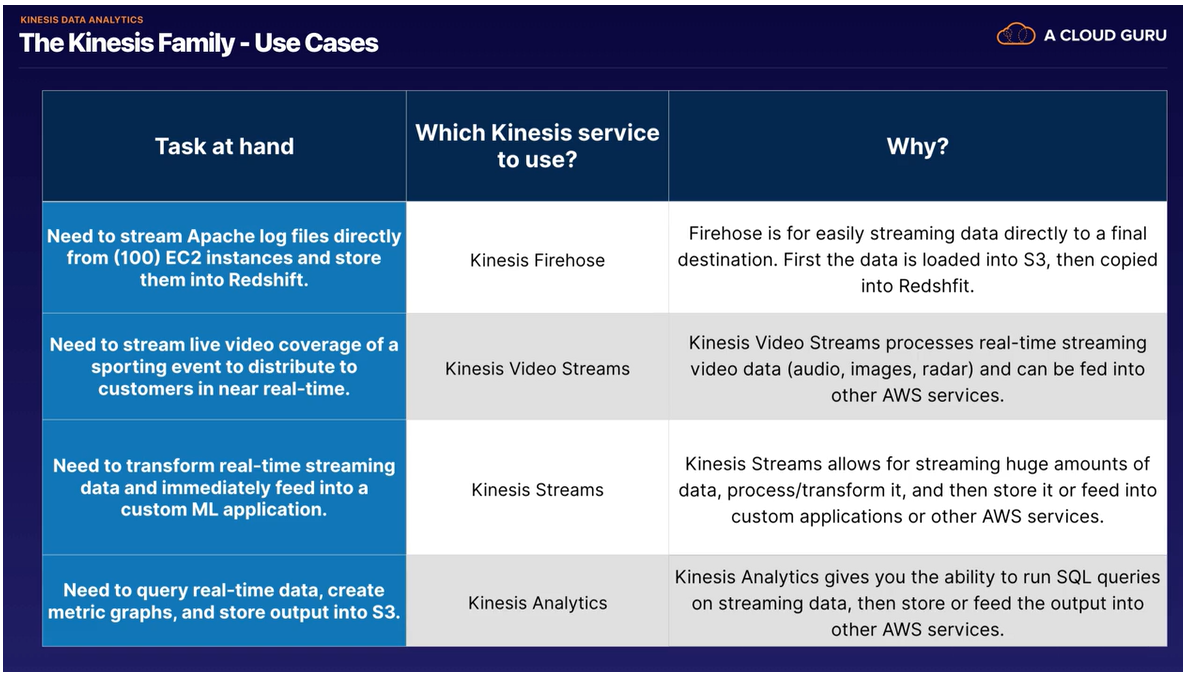
Grouping things together in bins with same number of data

Other types of feature engineering

Handling missing values



The Kinesis Family – Use Cases



Task at hand	Which Kinesis service to use?	Why?
Need to stream Apache log files directly from (100) EC2 instances and store them into Redshift.	Kinesis Firehose	Firehose is for easily streaming data directly to a final destination. First the data is loaded into S3, then copied into Redshfit.
Need to stream live video coverage of a sporting event to distribute to customers in near real-time.	Kinesis Video Streams	Kinesis Video Streams processes real-time streaming video data (audio, images, radar) and can be fed into other AWS services.
Need to transform real-time streaming data and immediately feed into a custom ML application.	Kinesis Streams	Kinesis Streams allows for streaming huge amounts of data, process/transform it, and then store it or feed into custom applications or other AWS services.
Need to query real-time data, create metric graphs, and store output into S3.	Kinesis Analytics	Kinesis Analytics gives you the ability to run SQL queries on streaming data, then store or feed the output into other AWS services.

AWS Migration Tools

- Data Pipeline
    - Migrate data between different data sources to S3
- DMS
    - Migrate data between different databases platforms
        - Homogenous: MySQL to MySQL
        - Heterogeneous: SQL server to MySQL
- AWS Glue
    - Fully managed ETL service (extract, transform and load)

Data repositories

Databases

- Strict defined schema

Data Warehouse

- Processing done on import (schema-on-write)

Data Lakes

- Processing done on export (schema-on-read)

Machine learning data terminology

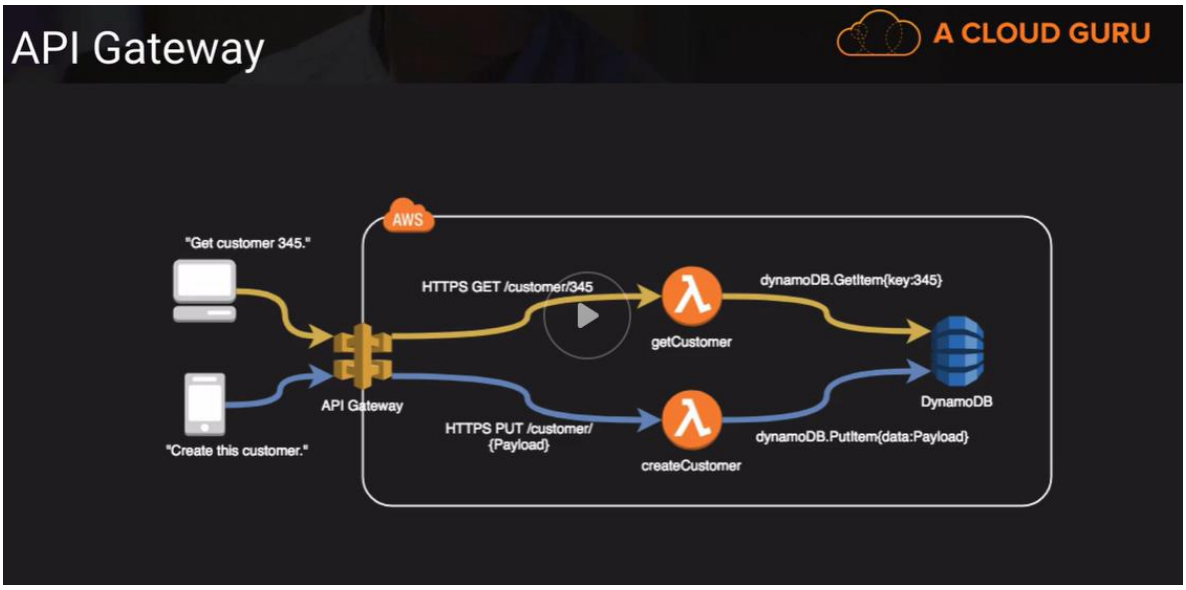
- Labeled data
    - Supervised learning
    - Target attribute (labels)
- Unlabeled data
    - Unsupervised learning
    - No target attributes
- Features of the data
    - Categorical
        - Values that are associated with a group
        - Qualitative
            - Example: breed of a dog (fox terriers, Doberman, etc.)
            - If it's SPAM or not spam
        - Discrete
    - Continuous
        - Quantitative
            - 1, 2, 3, 4, etc.
            - 125,000 USD, 165,000 USD, etc.
        - Infinite
- Text data (Corpus data)
- Ground truth data
    - Ground truth datasets refers to factual data that has been observed or measured. This can be trusted as "truth" data.
    - Amazon SageMaker Ground Truth
- Image data
    - Image data refers to datasets with tagged images
    - Example: MNIST data, ImageNet, etc.
- Time series data
    - Data that changes over time
    - Example: Stock market data, sensors on IOT devices, etc.

AWS Data Stores

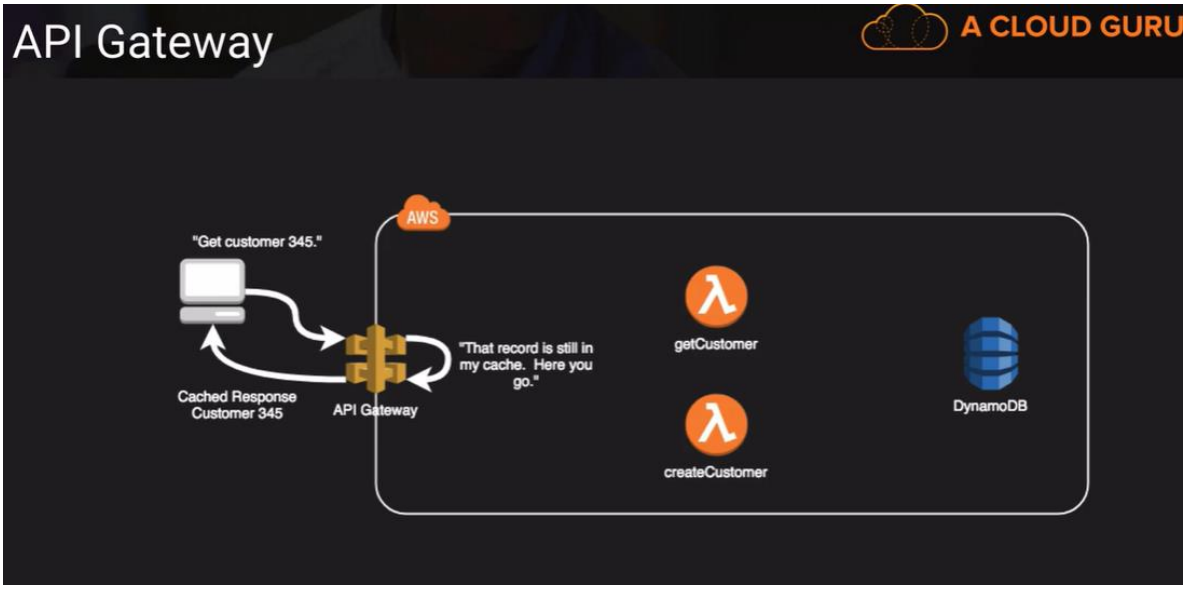
- S3
- RDS
- DynamoDB
- Redshift
    - Redshift Spectrum allows you to use a data store from S3
    - The difference of Redshit Spectrum and Athena is that you need a Redshift Clusters and it's made for existing Redshift customers.
- Timestream
- DocumentDB

Amazon API Gateway

- Example architecture:



- How cache works:



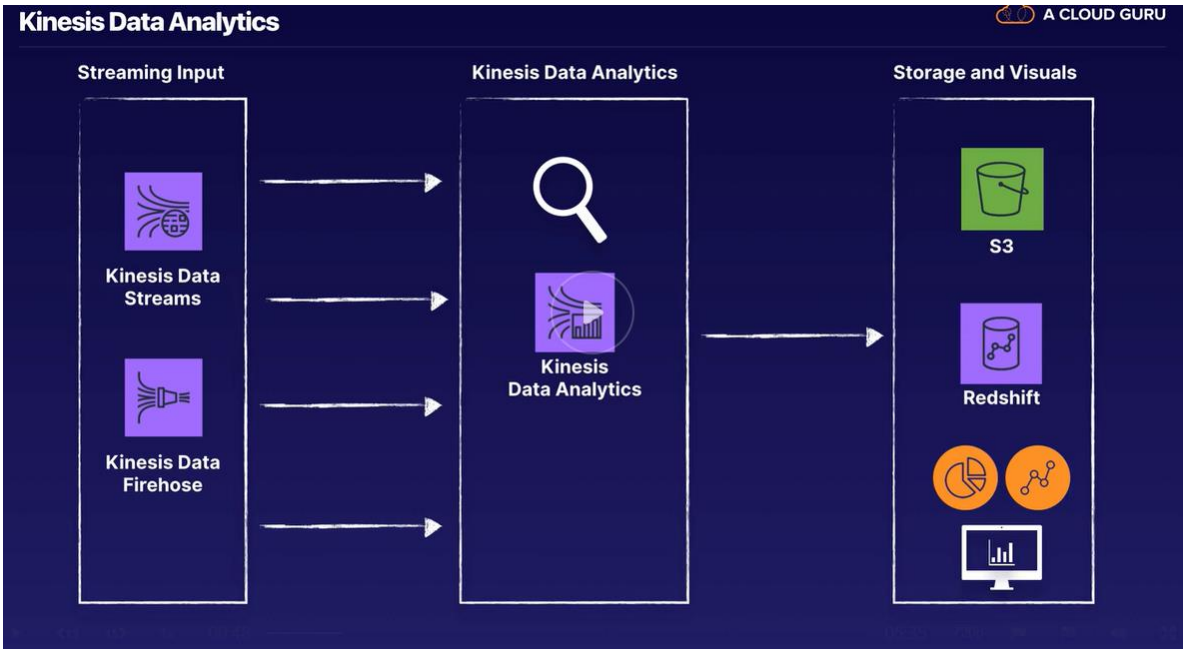
Amazon Kinesis Data Firehose

- You do not need to worry about shards.
- There is no data retention (since there is no shards).
- You can stream the data to a processing tool like Lambda, or stream directly to storage
- You can use S3 events to stream data from a producer to S3 and invoking Lambda to insert data to DynamoDB.
- Streaming data directly to storage.

AWS Kinesis Video Stream

- For video.
- Data producer to data consumers (EC2 continuous consumer or EC2 batch consumer)
- Data retention

AWS Kinesis Data Analytics



Use cases

- Send real-time alarms or notifications when certain metrics reach predefined threshold.
- Stream raw sensor data then, clean, enrich, organize, and transform it before it lands into a data warehouse or data lake.

Amazon Aurora

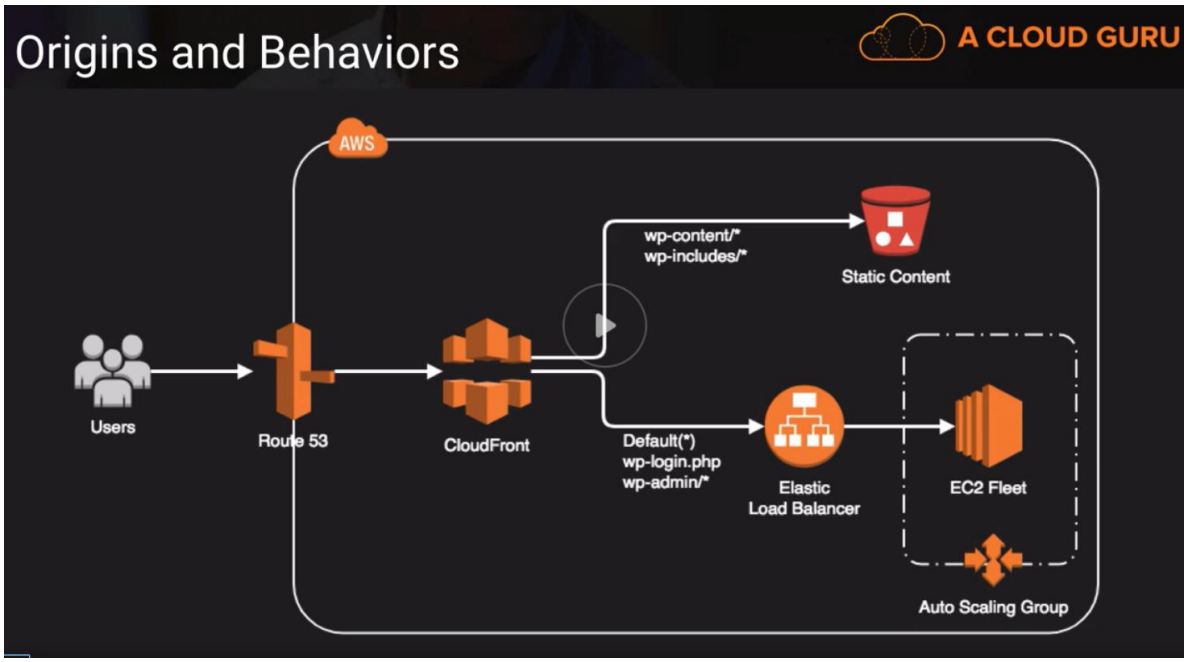
- Amazon Aurora has in some cases, 5x the performance of MySQL.
- Amazon Aurora scales from 10GB to 64TB.
- Scales from 64 vCPU to 488 vCPU.
- It stores a minimum of 2 copies of your data in 3 AZ.
- The limit of read replicas is 15, and replication is async.
- If you have 100% CPU utilization, you need to scale up (Scaling up means increasing the instance size).
- If you have a bottleneck in reads, you need to scale out (Scaling out means adding read replicas).
- Aurora serverless, is an on demand, auto scaling configuration for Aurora where the database will automatically start stop shutdown and scale up our out based on the application needs.
- Aurora is MultiAZ by default.

Tips

- If you encrypt at rest, all your read nodes are going to be encrypted.
- If you set up a cross region read replica, make it AZ since if it disrupted you have to set it up again.
- To delete the cluster, you need to delete nodes.
- Encryption at rest is turned on by default.
- The lower the tier, the higher the priority.
- Tier 0 is the highest priority.

Amazon CloudFront

- How does origins and behaviors work?



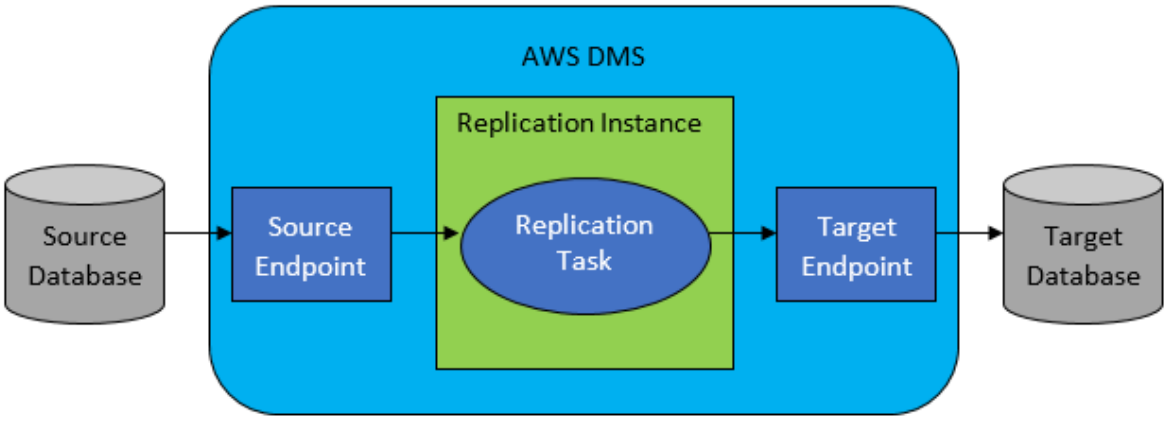
Amazon CloudWatch

- AWS Config is for resource configuration, AWS CloudTrail is to log API calls and AWS CloudWatch is to measure performance.
- RAM is a custom metric. You need AWS SDK or CLI to send the metric using.
- Disk usage is another custom metric.
    - https://docs.aws.amazon.com/cli/latest/reference/cloudwatch/put-metric-data.html

Amazon Cognito

- The AWS preferred sign-up, sign-in and ACL for web and mobile apps.
- An identity pool can also handle anonymous users.

Amazon Database Migration Service (DMS)



On-premises and EC2 instance databases

- Oracle versions 10.2 and later (for versions 10.x), 11g and up to 12.2, and 18c for the Enterprise, Standard, Standard One, and Standard Two editions

  Note

  Support for Oracle version 8c as a source is available in AWS DMS versions 3.3.0 and later.
- Microsoft SQL Server versions 2005, 2008, 2008R2, 2012, 2014, and 2016, for the Enterprise, Standard, Workgroup, and Developer editions. The Web and Express editions are not supported.
- MySQL versions 5.5, 5.6, and 5.7.
- MariaDB (supported as a MySQL-compatible data source).
- PostgreSQL version 9.4 and later (for versions 9.x), 10.x, and 11.x.

  Note

  PostgreSQL versions 11.x are supported as a source only in AWS DMS versions 3.3.0 and later. You can use PostgreSQL version 9.4 and later (for versions 9.x) and 10.x as a source in any DMS version.
- MongoDB versions 2.6.x and 3.x and later.
- SAP Adaptive Server Enterprise (ASE) versions 12.5, 15, 15.5, 15.7, 16 and later.
- IBM Db2 for Linux, UNIX, and Windows (Db2 LUW) versions:
  - Version 9.7, all fix packs are supported.
  - Version 10.1, all fix packs are supported.
  - Version 10.5, all fix packs except for Fix Pack 5 are supported.

Microsoft Azure

- Azure SQL Database.

Amazon RDS instance databases, and Amazon Simple Storage Service (Amazon S3)

- Oracle versions 10.2 and later (for versions 10.x), 11g and up to 12.2, and 18c for the Enterprise, Standard, Standard One, and Standard Two editions.

  Note

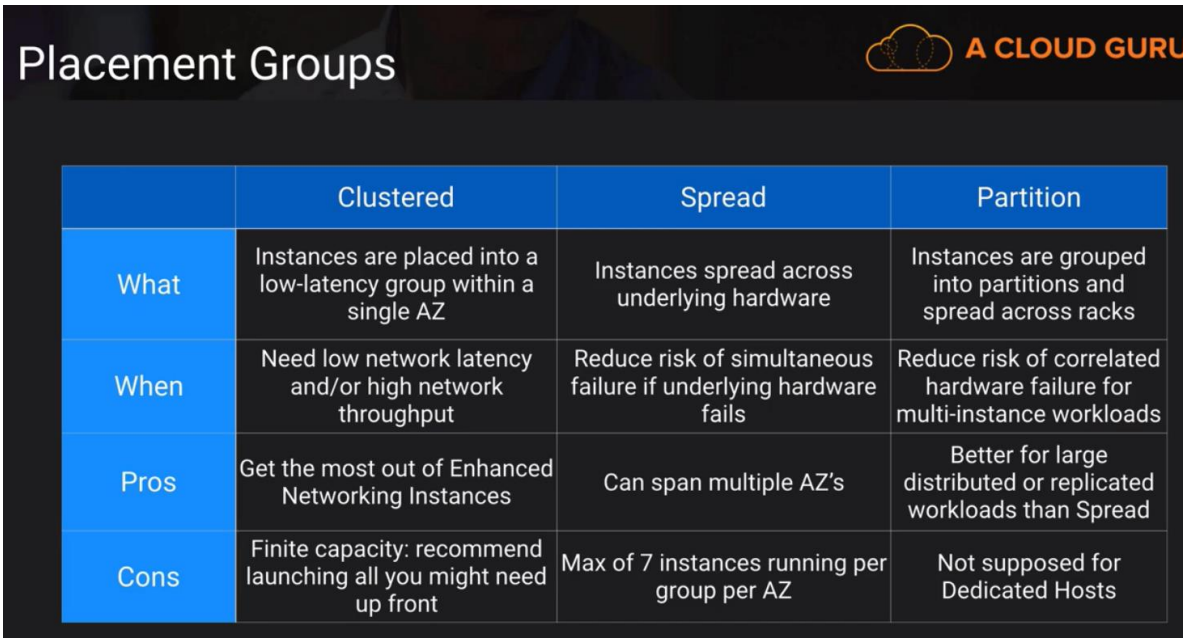
  Support for Oracle version 8c as a source is available in AWS DMS versions 3.3.0 and later.
- Microsoft SQL Server versions 2008R2, 2012, 2014, and 2016 for the Enterprise, Standard, Workgroup, and Developer editions. The Web and Express editions are not supported.
- MySQL versions 5.5, 5.6, and 5.7.
- MariaDB (supported as a MySQL-compatible data source).
- PostgreSQL version 9.4 and later (for versions 9.x), 10.x, and 11.x. Change data capture (CDC) is only supported for versions 9.4.9 and later, 9.5.4 and later, 10.x, and 11.x. The rds.logical_replication parameter, which is required for CDC, is supported only in these versions and later.

  Note

  PostreSQL versions 11.x are supported as a source only in AWS DMS versions 3.3.0 and later. You can use PostgreSQL version 9.4 and later (for versions 9.x) and 10.x as a source in any DMS version.
- Amazon Aurora (supported as a MySQL-compatible data source).
- Amazon S3.

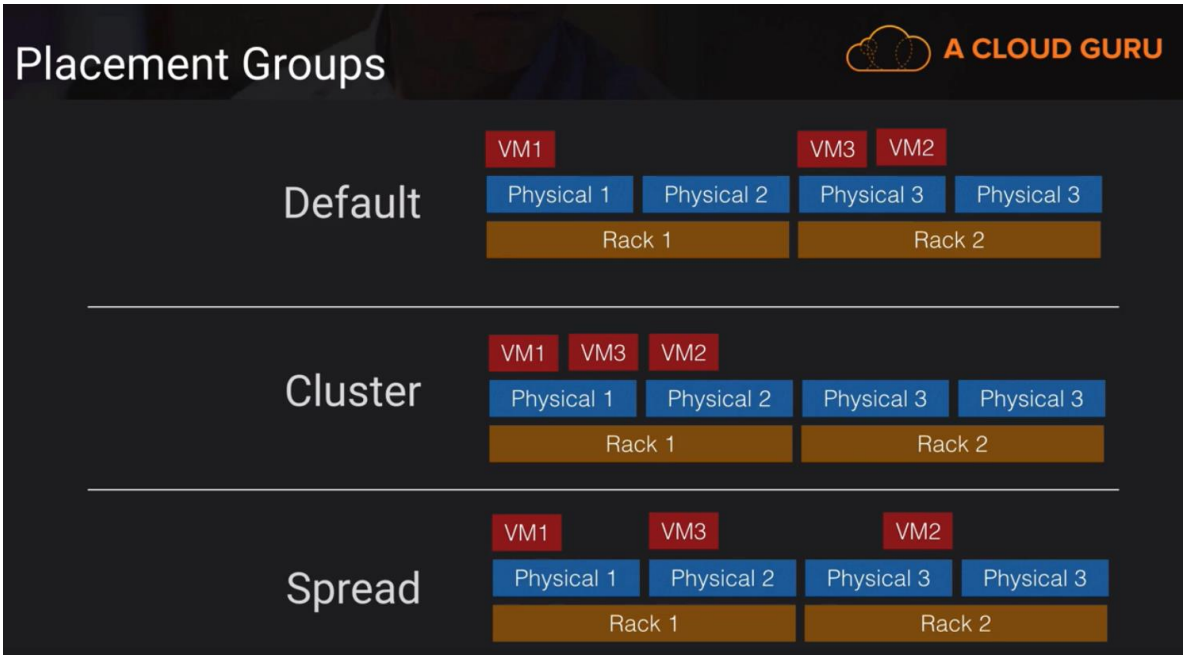
Amazon EC2

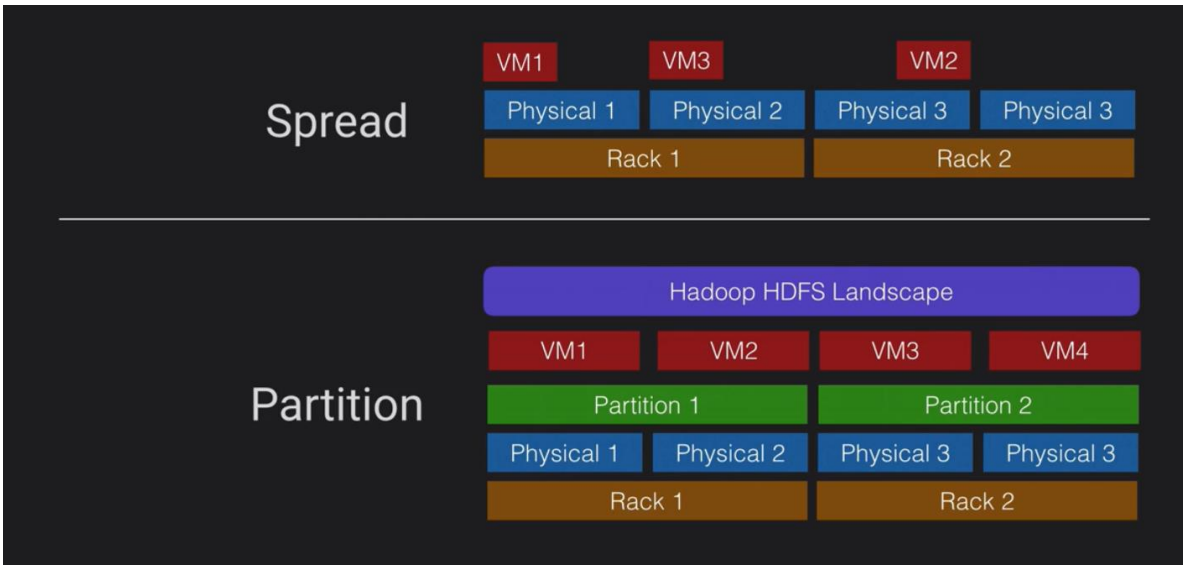
Placement group



	Clustered	Spread	Partition
What	Instances are placed into a low-latency group within a single AZ	Instances spread across underlying hardware	Instances are grouped into partitions and spread across racks
When	Need low network latency and/or high network throughput	Reduce risk of simultaneous failure if underlying hardware fails	Reduce risk of correlated hardware failure for multi-instance workloads
Pros	Get the most out of Enhanced Networking Instances	Can span multiple AZ's	Better for large distributed or replicated workloads than Spread
Cons	Finite capacity: recommend launching all you might need up front	Max of 7 instances running per group per AZ	Not supposed for Dedicated Hosts

- Clustered is for low-latency.
- Spread is for HA.
- Partition reduces the risk of hardware failure for multi-instance workloads.1



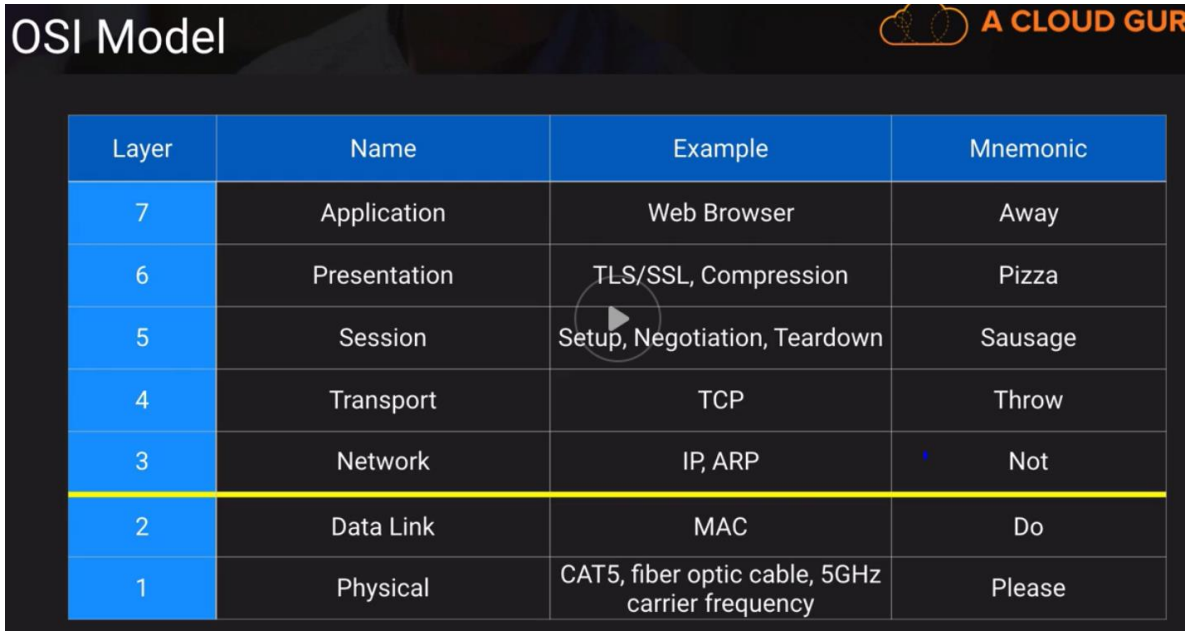


Enhanced networking

- Enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types.
- Supported instances types:
    - Elastic Network Adapter (ENA)
        - The Elastic Network Adapter (ENA) supports network speeds of up to 100 Gbps for supported instance types.
        - A1, C5, C5d, C5n, F1, G3, H1, I3, I3en, m4.16xlarge, M5, M5a, M5ad, M5d, P2, P3, R4, R5, R5a, R5ad, R5d, T3, T3a, u-6tb1.metal, u-9tb1.metal, u-12tb1.metal, X1, X1e, and z1d instances use the Elastic Network Adapter for enhanced networking.
    - Intel 82599 Virtual Function (VF) interface
        - The Intel 82599 Virtual Function interface supports network speeds of up to 10 Gbps for supported instance types.
        - C3, C4, D2, I2, M4 (excluding m4.16xlarge), and R3 instances use the Intel 82599 VF interface for enhanced networking.

Elastic Load Balancers

- Distribute inbound connections to one or many backed endpoints (EC2 for example).



Layer	Name	Example	Mnemonic
7	Application	Web Browser	Away
6	Presentation	TLS/SSL, Compression	Pizza
5	Session	Setup, Negotiation, Teardown	Sausage
4	Transport	TCP	Throw
3	Network	IP, ARP	Not
2	Data Link	MAC	Do
1	Physical	CAT5, fiber optic cable, 5GHz carrier frequency	Please

- Type of load balancers:
  - Application is layer 7.
  - Network is layer 4.
  - Classic Load Balancer (legacy).
- Remember, 4XX errors are client side, 5XX are server side.
- You can prewarm your ALB / ELB.
- You can put an ALB behind and ELB to get static IP (one per subnet).

SpilloverCount	The total number of requests that were rejected because the surge queue is full. [HTTP listener] The load balancer returns an HTTP 503 error code. [TCP listener] The load balancer closes the connection. **Reporting criteria**: There is a nonzero value **Statistics**: The most useful statistic is Sum. Note that Average, Minimum, and Maximum are reported per load balancer node and are not typically useful. **Example**: Suppose that your load balancer has us-west-2a and us-west-2b enabled, and that instances in us-west-2a are experiencing high latency and are slow to respond to requests. As a result, the surge queue for the load balancer node in us-west-2a fills, resulting in spillover. If us-west-2b continues to respond normally, the sum for the load balancer will be the same as the sum for us-west-2a.
SurgeQueueLength	The total number of requests (HTTP listener) or connections (TCP listener) that are pending routing to a healthy instance. The maximum size of the queue is 1,024. Additional requests or connections are rejected when the queue is full. For more information, see SpilloverCount. **Reporting criteria**: There is a nonzero value. **Statistics**: The most useful statistic is Maximum, because it represents the peak of queued requests. The Average statistic can be useful in combination with Minimum and Maximum to

- Functionalities:

	Application LB	Network LB	Classic LB
Protocols	HTTPS, HTTP	TCP, UDP, TLS	TCP, SSL,HTTP, HTTPS
Path or Host-based Routing	Yes	No	No
WebSockets	Yes	Yes	No
Server Name Indication (SNI)	Yes	No	No
Sticky Sessions	Yes	No	Yes
Static IP, Elastic IP	No	Yes	No
User Authentication	Yes	No	No

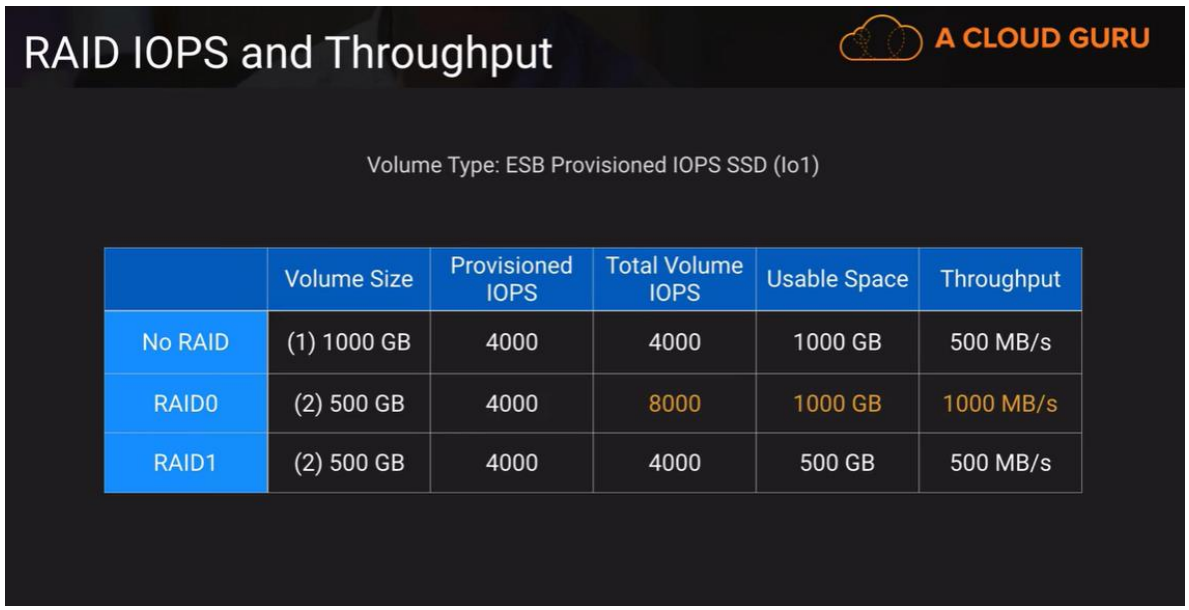
Example of an ALB with routing with paths:

EBS

- EBS is 10x more expensive than S3.

- RAID0 offers no redundancy.
- RAID1 is often called mirroring, because that is exactly what we are doing.
- RAID5, 1 drive can fail
- RAID6, 2 drives can fail

Regarding throughput:



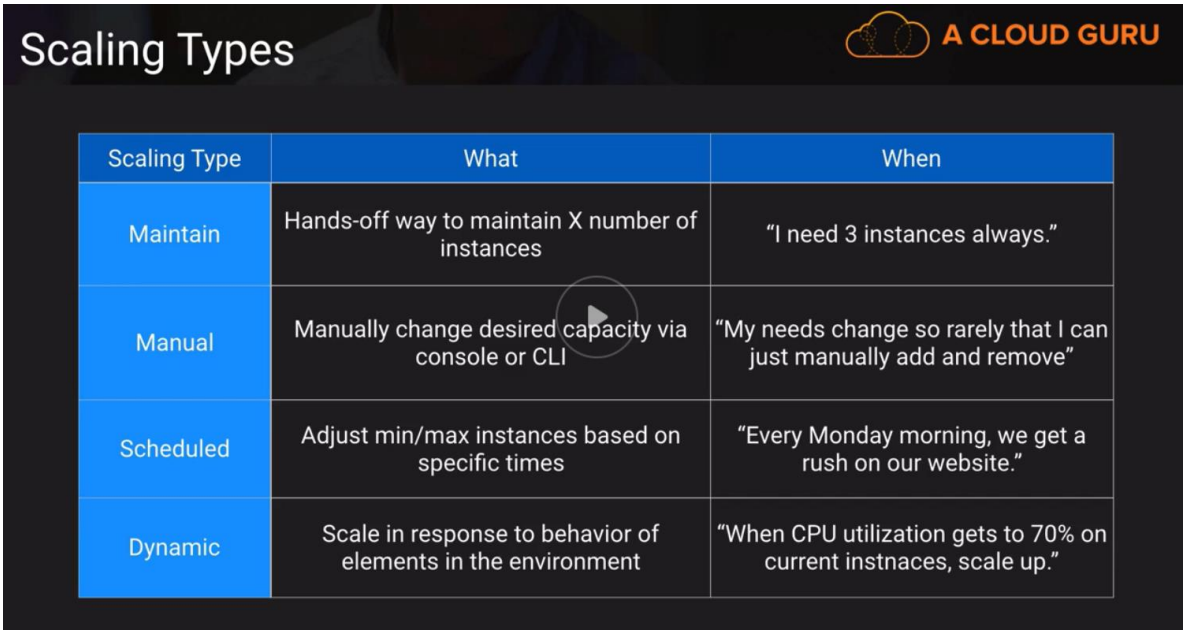
- IOPS is dependent on the size of the volume in GP2.
- Maximum IOPS per disk type:
    - Gp2 16,000.
    - Io1 64,000.

    - St1 500.
    - Sc1 250.
- Amazon EBS-Backed:
    - Persistence: Not deleted on termination.
    - Maximum Storage: 16TB.
- Amazon Instance Store-Backed:
    - Persistence: Deleted on termination.
    - Maximum Storage: 10 GB.
- Snapshots exist on s3.
- Snapshots are point in time copies of volumes.
- Snapshots are incremental, that means that only blocks that have changed since your last snapshot are moved to S3.
- AMIs are region bound.
- You can't copy AMIs with a "billingProducts" code.
- IO is how fast the car is going (fast car).
- Throughput how much the car can carry (big truck).

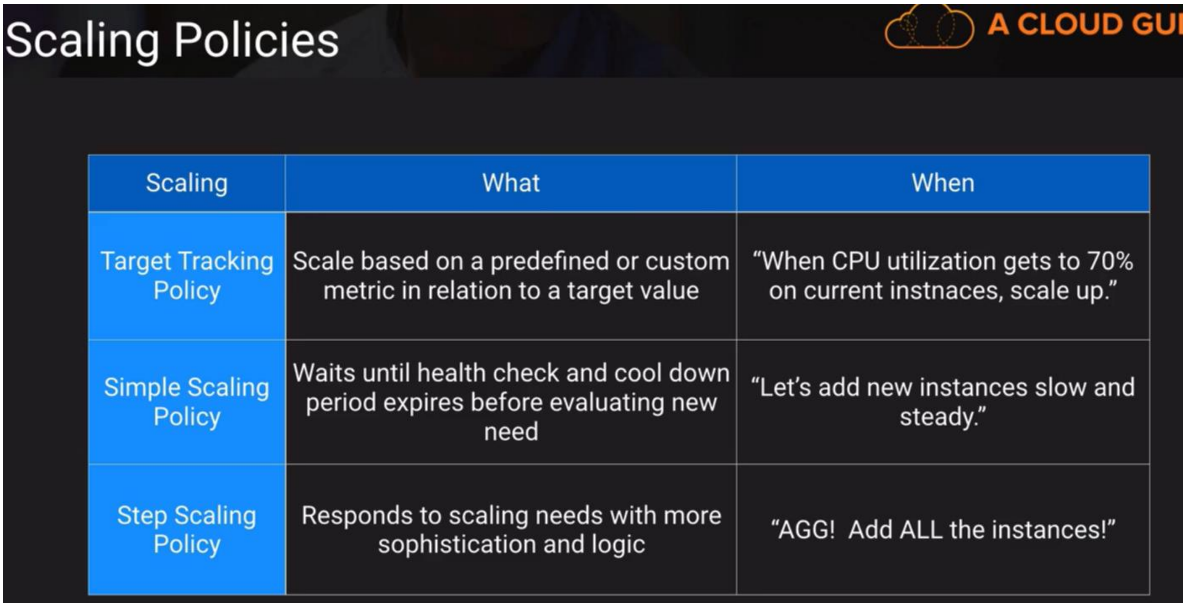
Dedicated hosts and dedicated instances

- Dedicated Hosts reserve capacity because you are paying for the whole physical server that cannot be allocated to anyone else. Dedicated Instances are available as on-demand, reserved and spot instances. Further information: https://aws.amazon.com/ec2/dedicated-hosts/

Autoscaling



Scaling Type	What	When
Maintain	Hands-off way to maintain X number of instances	"I need 3 instances always."
Manual	Manually change desired capacity via console or CLI	"My needs change so rarely that I can just manually add and remove"
Scheduled	Adjust min/max instances based on specific times	"Every Monday morning, we get a rush on our website."
Dynamic	Scale in response to behavior of elements in the environment	"When CPU utilization gets to 70% on current instnaces, scale up."

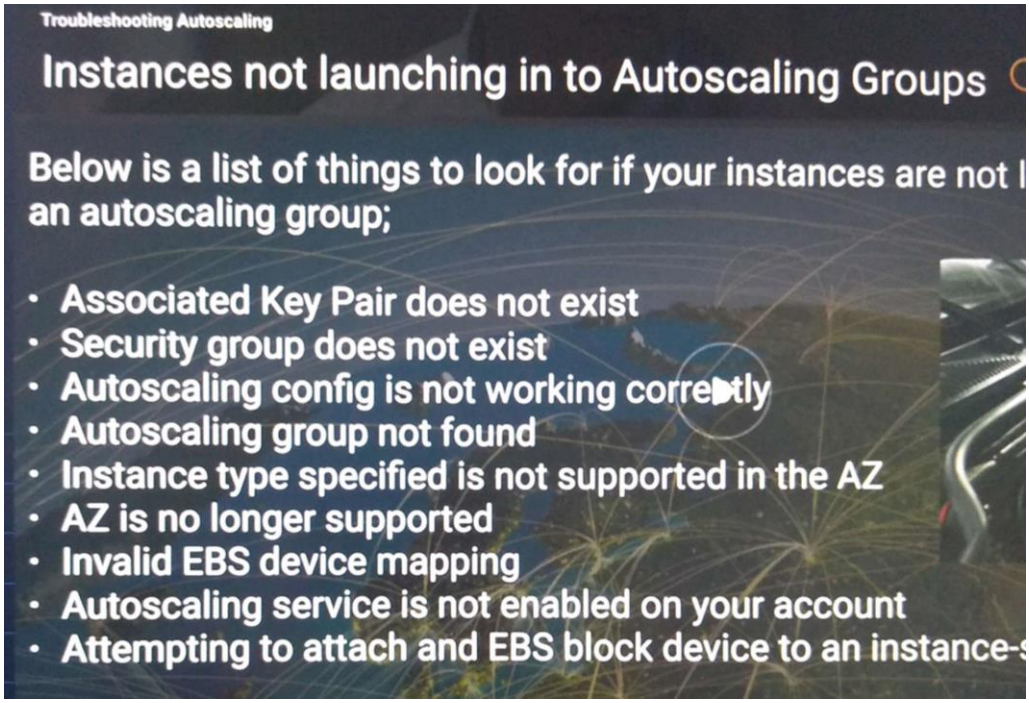


Scaling	What	When
Target Tracking Policy	Scale based on a predefined or custom metric in relation to a target value	"When CPU utilization gets to 70% on current instnaces, scale up."
Simple Scaling Policy	Waits until health check and cool down period expires before evaluating new need	"Let's add new instances slow and steady."
Step Scaling Policy	Responds to scaling needs with more sophistication and logic	"AGG! Add ALL the instances!"

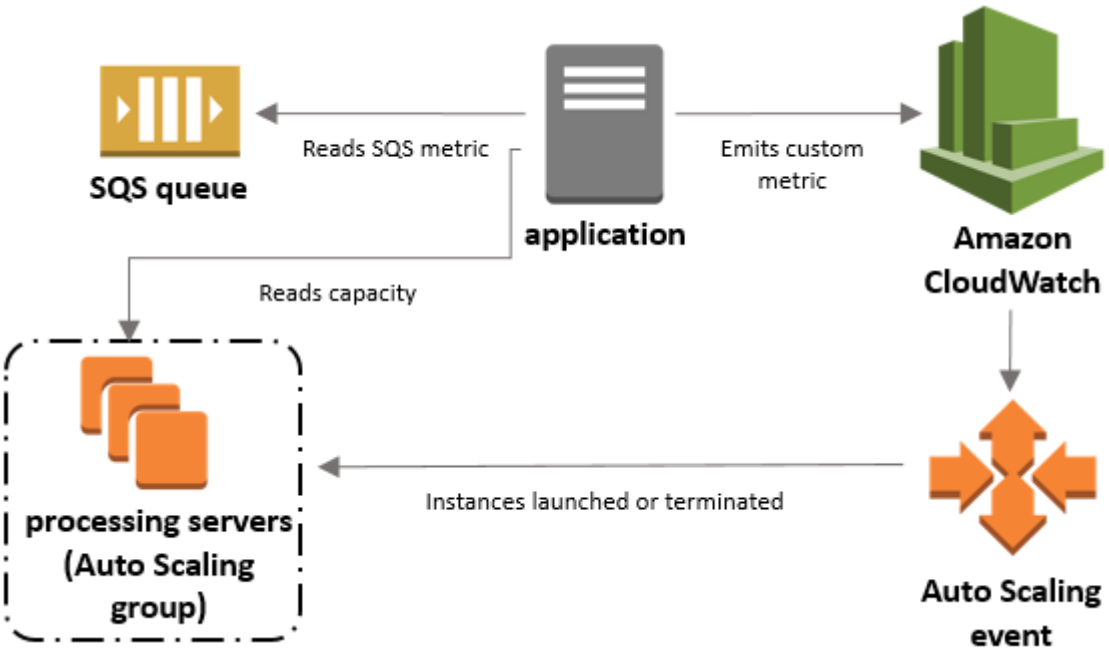
- Types of deployment:
  - Rolling deployment: Create a new launch configuration with an updated version and start terminating instances to bring them up with version 2.
  - A/B testing: Very popular in websites, you can send 90% to Version 1, and send 10% to Version 2.

- Blue-green deployment: Create another ELB and a fleet of EC2 instances with version 2, change Route 53 DNS record to point to "green" deployment".
  - Really easy rollback.
- Canary deployment: Canary release, you deploy in just one EC2 instance, and sit back and measure if everything is working correctly.

Tips



- Types of errors:
  - InstanceLimitExceeded: means you have exceeded the number of EC2 instances you can have of that type, you need to raise the limit with AWS Support.
  - InsuficientInstanceCapacity: Try later, change number or type, buy RI.
- Once you created a launch configuration, you can't modify it.
- Scaling based on Amazon SQS:

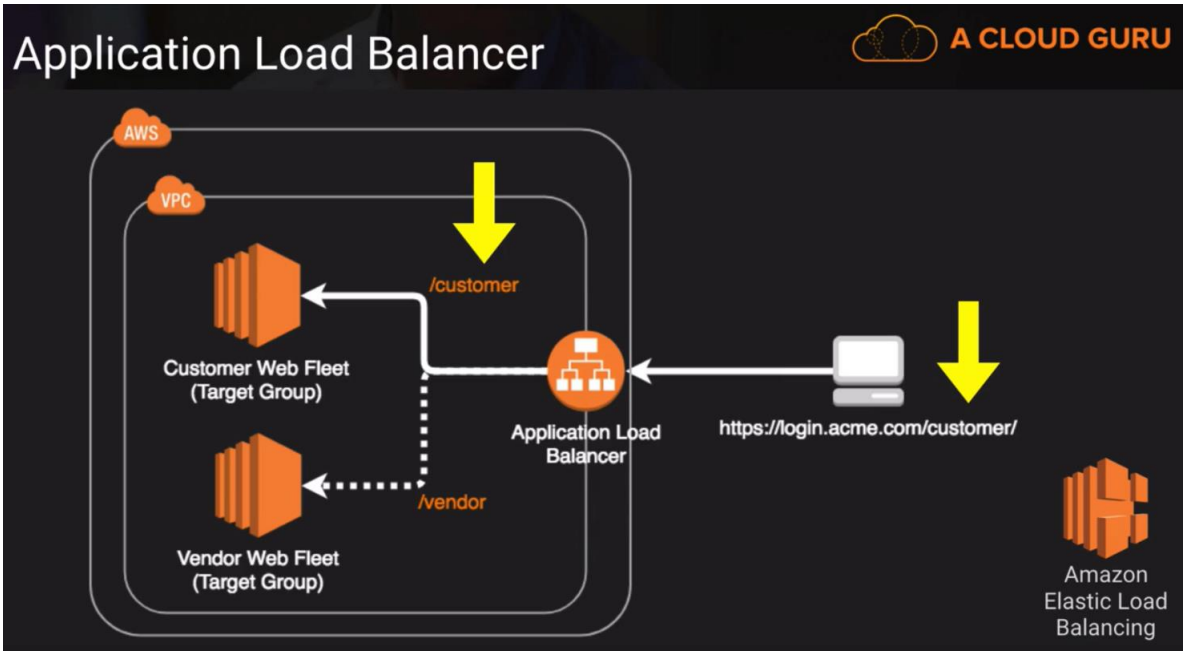

SQS queue
Reads SQS metric
application
Emits custom metric
Amazon CloudWatch
Reads capacity
processing servers (Auto Scaling group)
Instances launched or terminated
Auto Scaling event

Amazon EFS

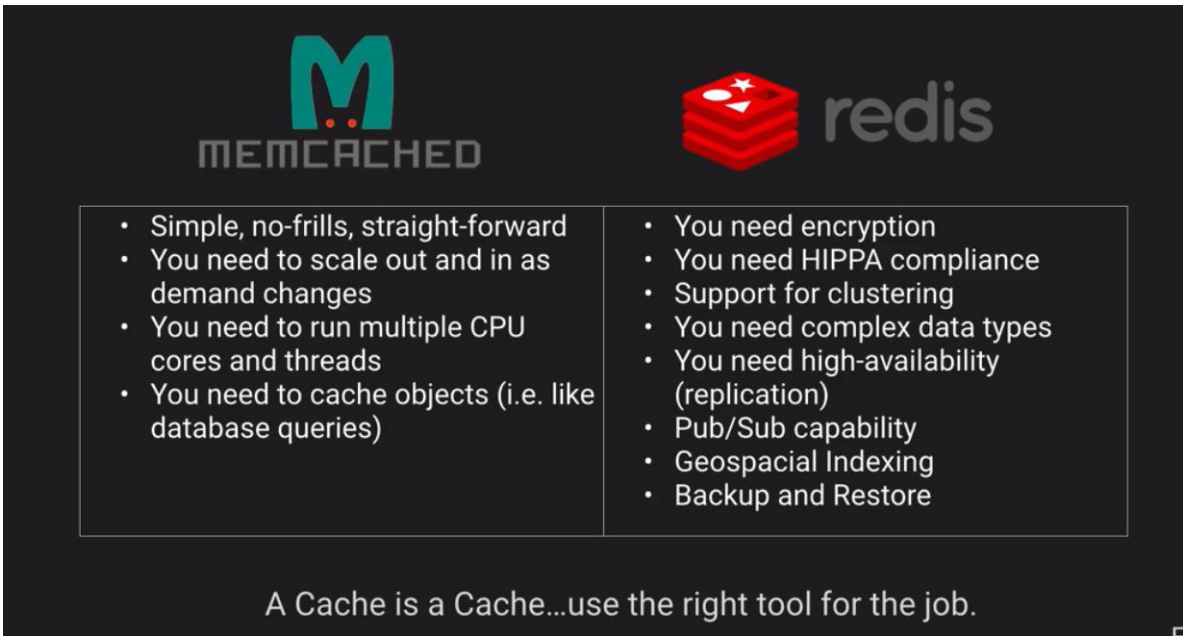
- EFS is 2x cost as EBS, 15x as S3.
- EFS File Sync Agent.

Amazon Elastic Container Services

- Managed, highly scalable container platforms.
- Types of container services at AWS:
    - Amazon ECS
        - Leverages AWS services like Route53, ALB and CloudWatch.
        - “Tasks” are instances of containers.
        - You can use EC2 as provisioned instances
        - Fargate is a “serverless” solution, it provisions compute as needed.
    - Amazon EKS
        - Handles many things with the K8 platform.
        - “Pods” are collection of containers.



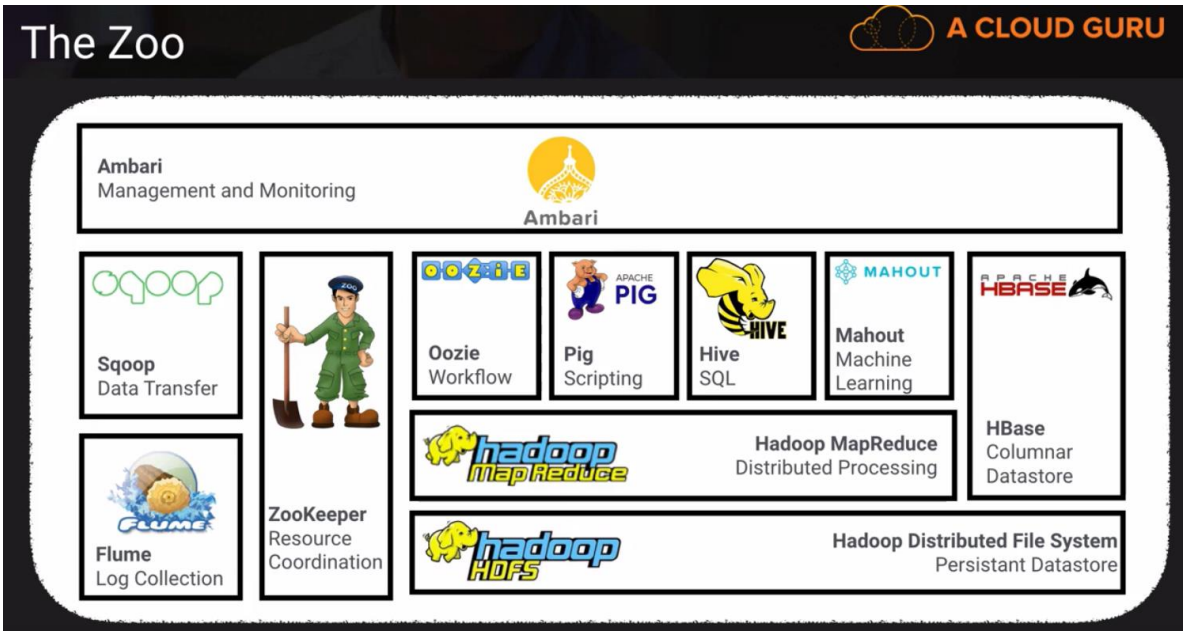
Amazon ElastiCache

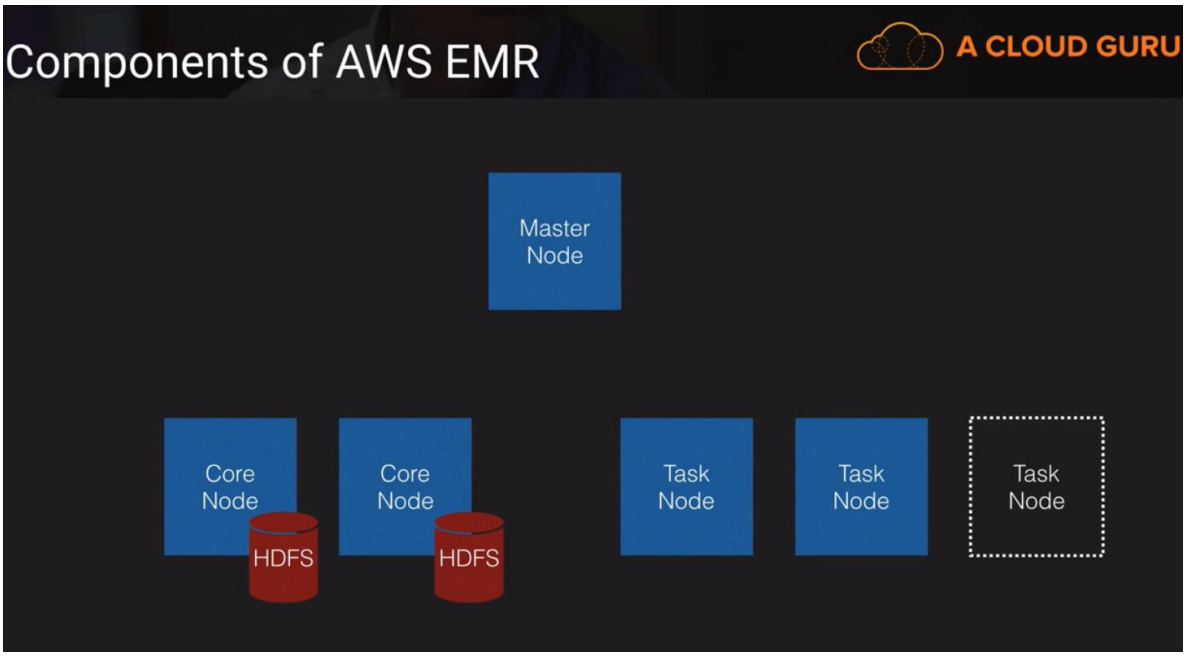


- ElastiCache is an excellent choice if your database is particularly read-heady.
- Memcached does NOT support MultiAZ.
- Redis support MultiAZ.
- Analogy for evictions: if you have tenants in your building, and you need to evict old tenants to put new ones.

Amazon EMR

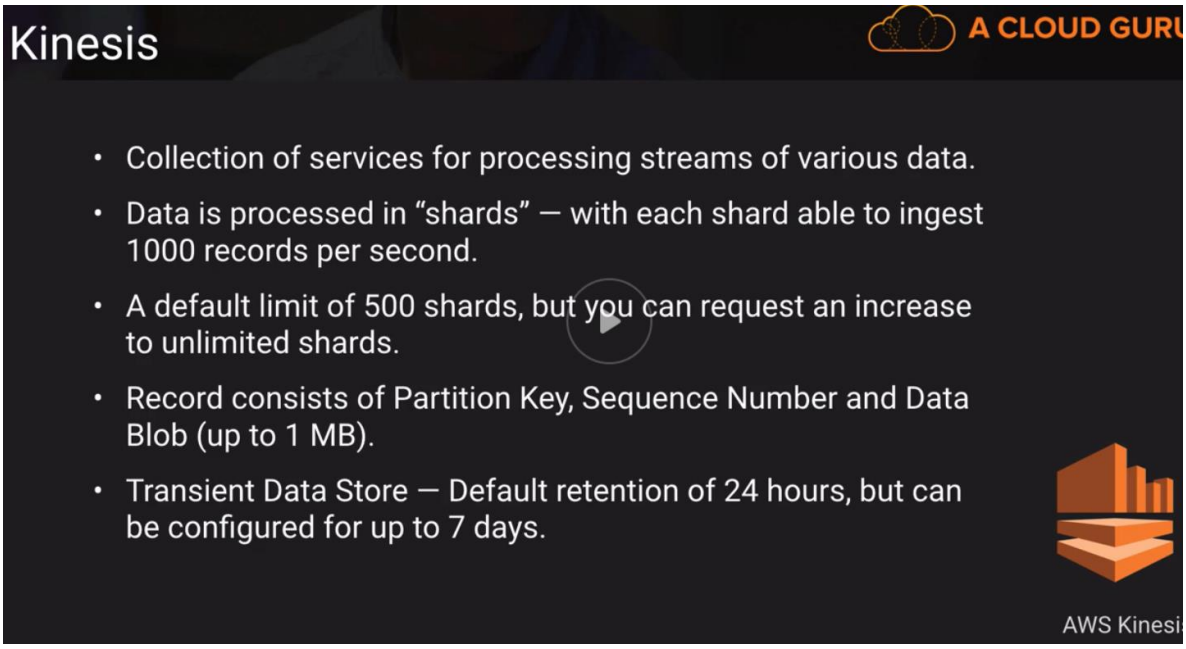
- Leveraged technologies by Amazon Elastic MapReduce:

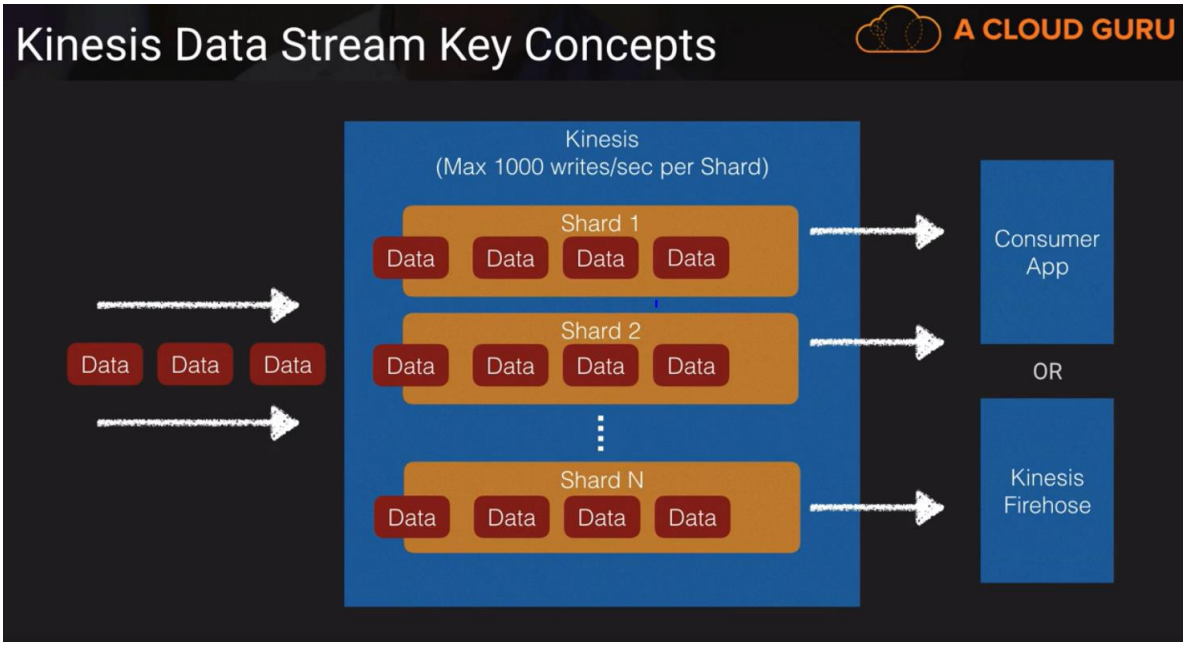




- You have master nodes, core nodes and task nodes.
- Data stored on HDFS in an EMR cluster is ephemeral so it will be deleted when a cluster is terminated. If persistence is required, S3 might be an option using the EMRFS file system. Further information: https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-file-systems.html

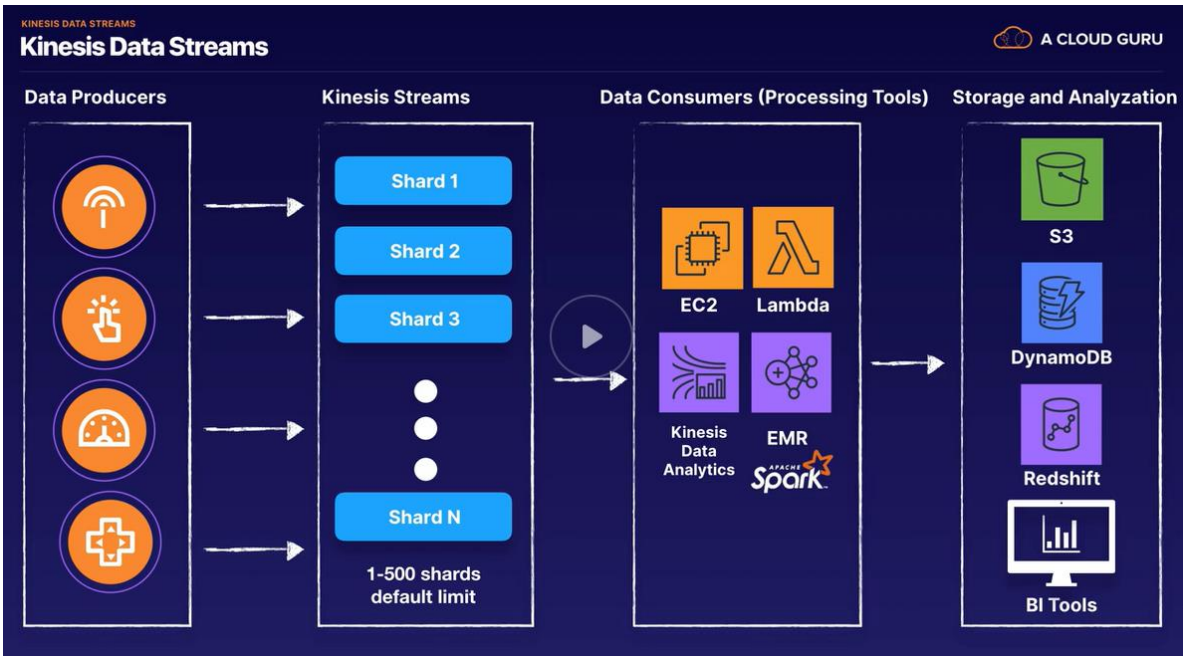
Amazon Kinesis





- Q: When developing an Amazon Kinesis Data Stream application, what is the recommended method to read data from a shard?
- A: Although data can be read (or consumed) from shards within Kinesis Streams using either the Kinesis Data Streams API or the Kinesis Consumer Library (KCL), AWS always recommend using the KCL. The KPL (Kinesis Producer Library) will only allow writing to Kinesis Streams and not reading from them. You cannot interact with Kinesis Data Streams via SSH. Further

information: https://docs.aws.amazon.com/streams/latest/dev/developing-consumers-with-kcl.html



Shards

- 1,000 records per second
- Default limit of 500 shards, buy you can request increase to unlimited shards.
- A dara recod is the unit of data captures:
    - Sequence number
    - Partition key
    - Data blog (your payload, up to 1 MB)
- Transient Data Store – The retention period for data records are 24 hours to 7 days

How you can interact with Kinesis Data Streams?

1. Kinesis Producer Library (KPL)
2. Kinesis Client Library (KCL)
3. Kinesis API (AWS SDK)

When to use Kinesis Data Streams?

- Process and evaluate logs immediately
- Real-time data analytics

Amazon KSM/HSM

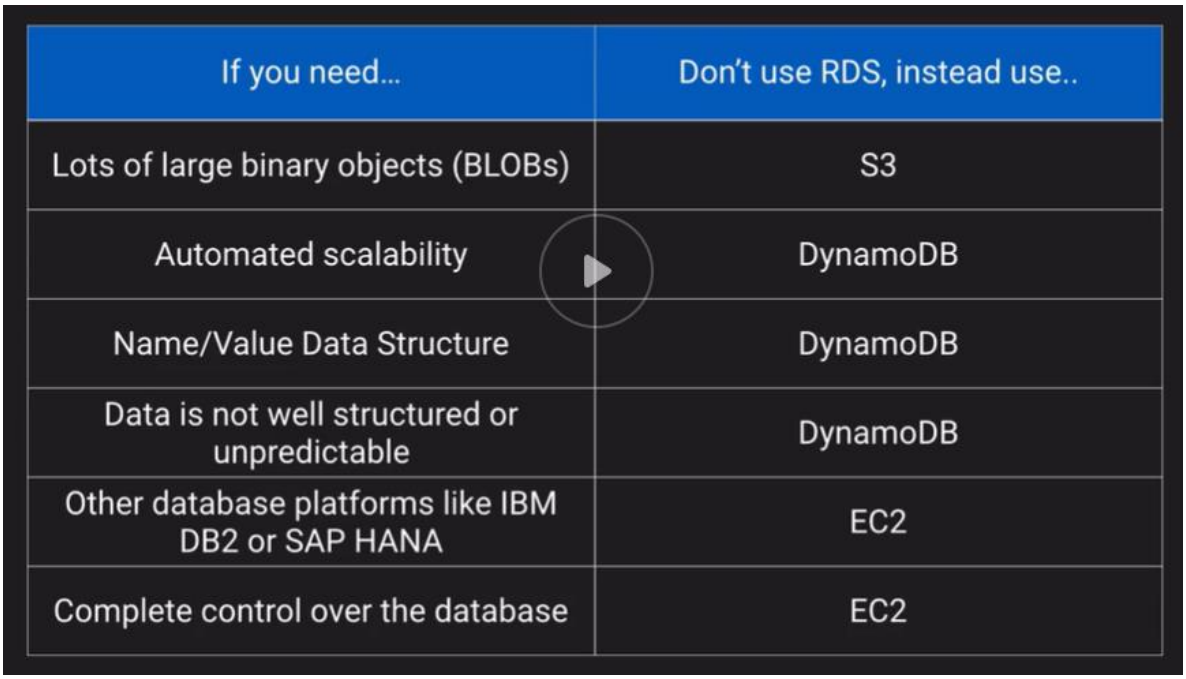
- Allow you to generate, store and manage cryptographic keys to protect your data in AWS.
- KMS uses shared hardware multitenant managed service.
- Is suitable where multi-tenancy is not an issue.
- If there is regulatory (like banking), you need HSM.
- Symmetric keys, same key to encrypt and decrypt.
- HSM.
- Dedicated HSM instance, hardware is not shared with other tenants, it lives in your VPC.
- Is compliant with FIPS 140-2 Level 3 Compliance, includes tamper-evident physical security mechanisms.
- It's suitable for applications which have a contractual or regulatory requirement (banking, financial, PCI, etc.).

Amazon Neptune

- Fully managed graph database.

Amazon RDS

- RDS Anti-Patterns



If you need...	Don't use RDS, instead use..
Lots of large binary objects (BLOBs)	S3
Automated scalability	DynamoDB
Name/Value Data Structure	DynamoDB
Data is not well structured or unpredictable	DynamoDB
Other database platforms like IBM DB2 or SAP HANA	EC2
Complete control over the database	EC2

- If you want to build a data warehouse, you should use read replicas to query the read replica, not the master.
- MultiAZ helps with snapshots, since it uses the read replica to create snapshots and it doesn't affect your master.
- You need to connect to different endpoints to the read replicas.
- Read replicas can be MultiAZ.
- Read replicas can exist in different regions.
- Read replicas is async replication.
- In order to have read replicas, you need to have enabled automated snapshots.
- The limit of read replicas is 5, and replication is async.
- RDS can't use System Manager (SSM) Parameter Store.

Tips

- MySQL: Non-transactional storage engines like MYISAM don't support replication; you must use InnoDB or XtraDB in MariaDB.
- Promoting a read replica is a big deal, so maybe you want to do it manually.
- Aurora PostgreSQL do not support cross-region replicas at present.

Amazon Redshift

- Petabyte and cost-effective data warehouse.
- Redshift is for on-line analytical processing (OLAP).
- Redshift Spectrum adds the ability to query S3 data directly.

Amazon Route53

- Simple routing:
  - At random IP.
- Weighted:
  - Example, 20% for one region, 80% to another region.

$$\frac{\text{Weight for a specified record}}{\text{Sum of the weights for all records}}$$

    - For example, if you want to send a tiny portion of your traffic to one resource and the rest to another resource, you might specify weights of 1 and 255. The resource with a weight of 1 gets $1/256^{th}$ of the traffic (1/1+255), and the other resource gets 255/256ths (255/1+255). You can gradually change the balance by changing the weights. If you want to stop sending traffic to a resource, you can change the weight for that record to 0.
- Latency
  - Lowest latency for the region that gives the user the least latency.
- Failover:
  - Active/passive setup.
- Geolocation:
  - Decide based on where the DNS queries are done.
- And APEX domain is your principal domain, for example “inbest.cloud”.
-

Amazon S3

- Requester pays bucket:
    - Typically, you configure buckets to be Requester Pays when you want to share data but not incur charges associated with others accessing the data. You might, for example, use Requester Pays buckets when making available large datasets, such as zip code directories, reference data, geospatial information, or web crawling data.
    - https://docs.aws.amazon.com/AmazonS3/latest/dev/RequesterPaysBuckets.html
- 99.99999999999& durability for all storage classes, but different availability (From 99.99% to 99.5%).
- Types of policies you can apply to S3 bucket:
    - Bucket Policy.
    - Access Control list objects and bucket, not for folders.
    - IAM.
- For standard storage:
    - 99.99% availability.
- Some functionalities:
    - Tiered Storage Available.
    - Lifecycle Management.
    - Versioning.
    - Encryption.
    - MFA Delete.
- You need an MFA code to delete a file or to enable/disable versioning on a bucket
    - How to enable it?

```
Aws s3api list-buckets -query ‘acloudgurusysops’

aws s3api get-bucket-versioning –bucket ‘acloudgurusysops’

aws s3api put-bucket-versioning –bucket ‘acloudgurusysops’ –versioning-
configuration ‘MFADelete=Enabled,Status=Enabled’ –mfa
‘arn:aws:iam::882692629600:mfa/root-account-mfa-device 799460’
```

- Different storage tiers:
    - S3 (Standard).
    - Infrequently Accessed (IA).

    - One Zone Infrequently Accessed (One-zone IA) (20% cheaper than IA).
    - Reduced Redundancy Storage (RSS) (Deprecated).
    - Glacier (More than 3 hours to restore information).
    - Intelligent tiering:
        - 2 tiers – frequent and infrequent access.
    - Automatically moves your data.
- Think about S3 more than a database than object store:
    - Key (name).
    - Value (data).
    - Version ID.
    - Metadata.
- You can secure your data in transit with:
    - SSL/TLS.
- You can secure your data at rest with:
    - AES-256 Use Server-side Encryption with Amazon S3-Managed keys (SSE-S3).
    - AWS-KMS User Server-side Encryption with AWS KMS managed keys (SSE-KSM).
    - SSE-C: Server-side encryption with customer provided keys (SSE-C).
- S3, consistency for PUT.
- Eventual consistency for overwrite for PUTs and DELETs.
- If you want to send encrypted objects to S3, you need to send them using the header:

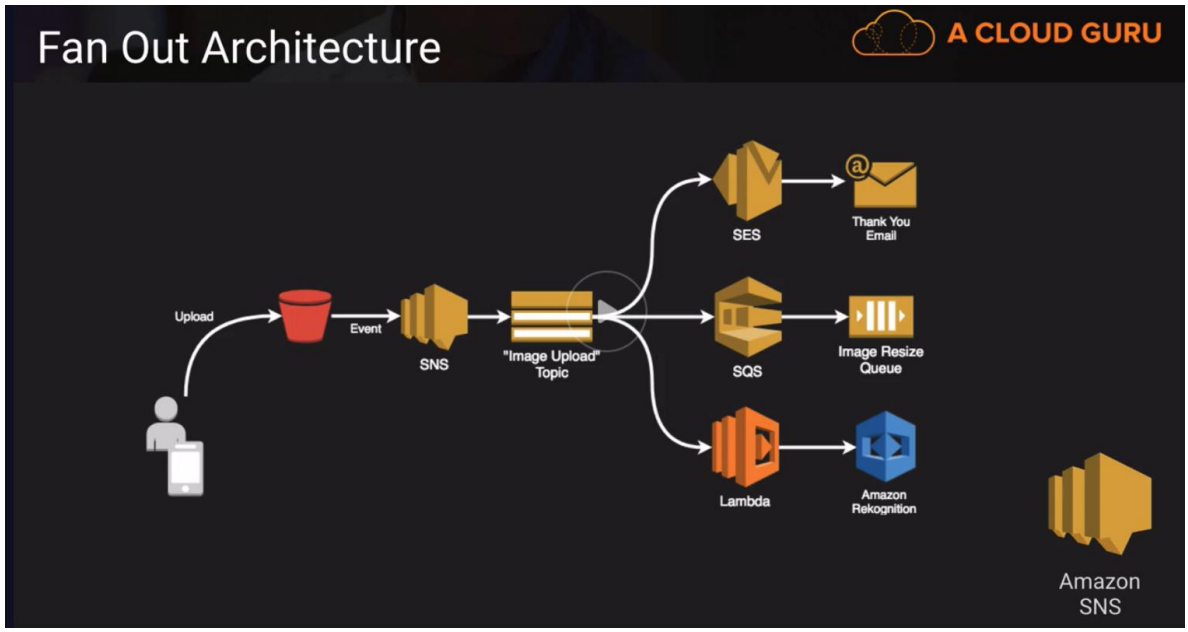
```
x-amz-server-side-encryption-aws-kms-key-id
```

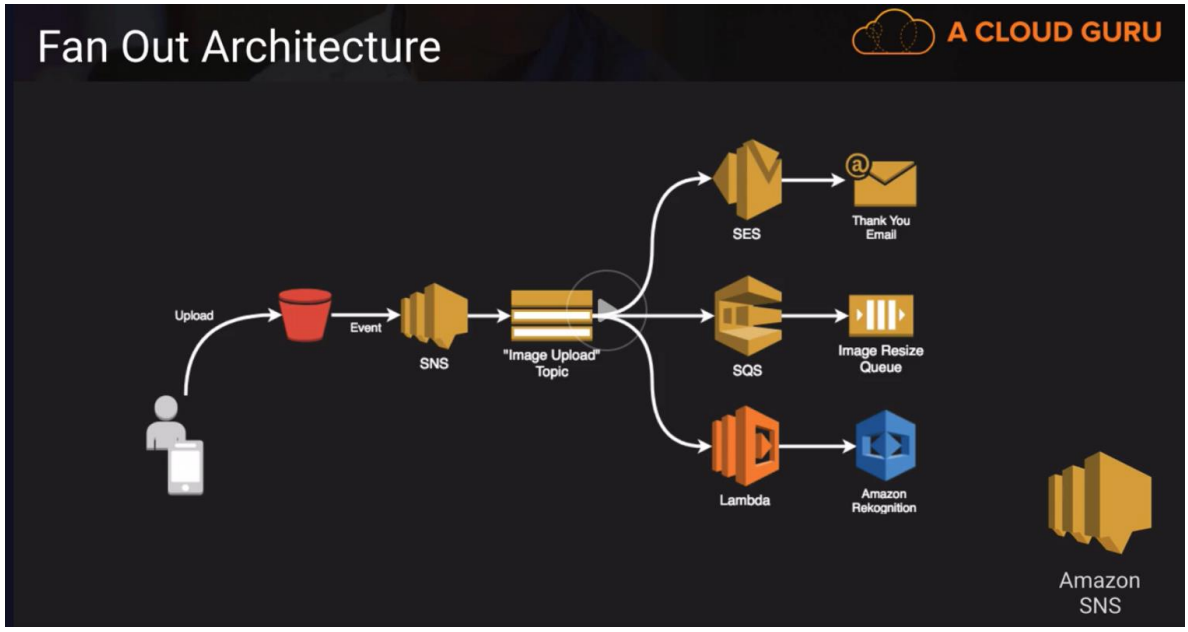
- Preassigned URLs can be created from the CLI or SKD, default is one hour, you can select the expires on the command line

Tips

- If you want to encrypt an existing RFS/RDS, you need to create a new EBS/DB/EFS and migrate your data.
- You can't change the encrypted status, but you can migrate your data.
- S3 is much more flexible, you can on/off encryption at bucket/object level

Amazon SNS

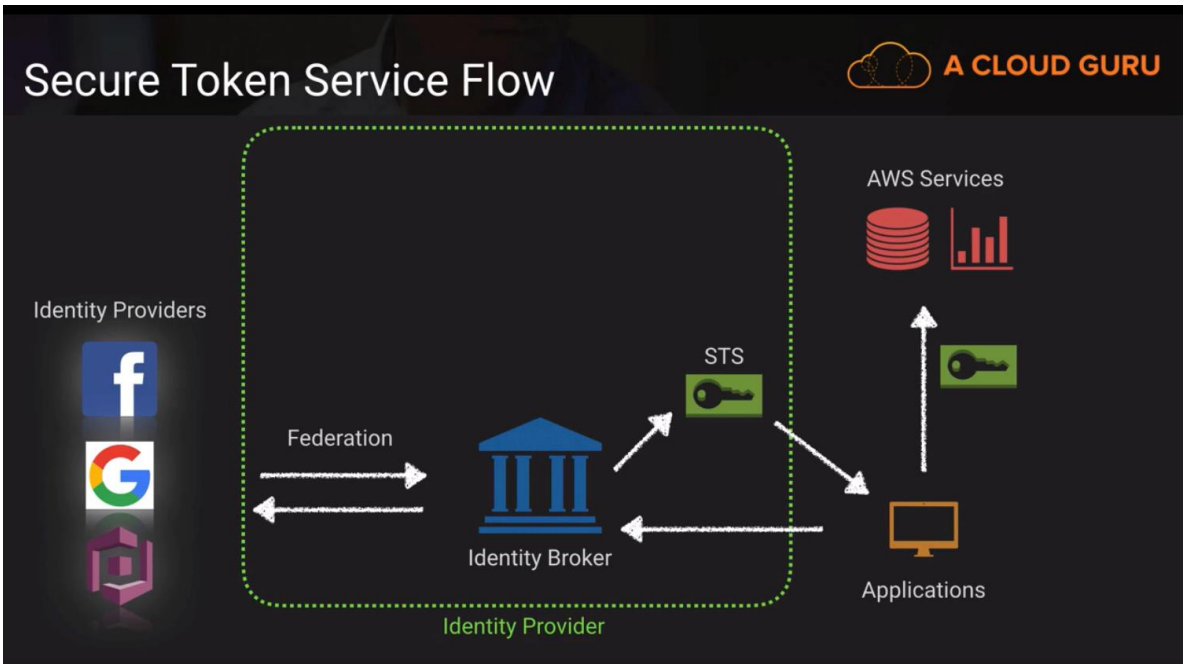

Fan Out Architecture
A CLOUD GURU
Upload
Event
SNS
"Image Upload" Topic
SES
Thank You Email
SQS
Image Resize Queue
Lambda
Amazon Rekognition
Amazon SNS


Fan Out Architecture
A CLOUD GURU
Upload
Event
SNS
"Image Upload" Topic
SES
Thank You Email
SQS
Image Resize Queue
Lambda
Amazon Rekognition
Amazon SNS

Amazon SQS

- Standard queues do not follow the order of the message stream, if you need to follow the order, you need FIFO queues.
- It's different to Amazon MQ. Amazon MQ it's an implementation of Apache ActiveMQ.

Amazon STS (Security Token Service)

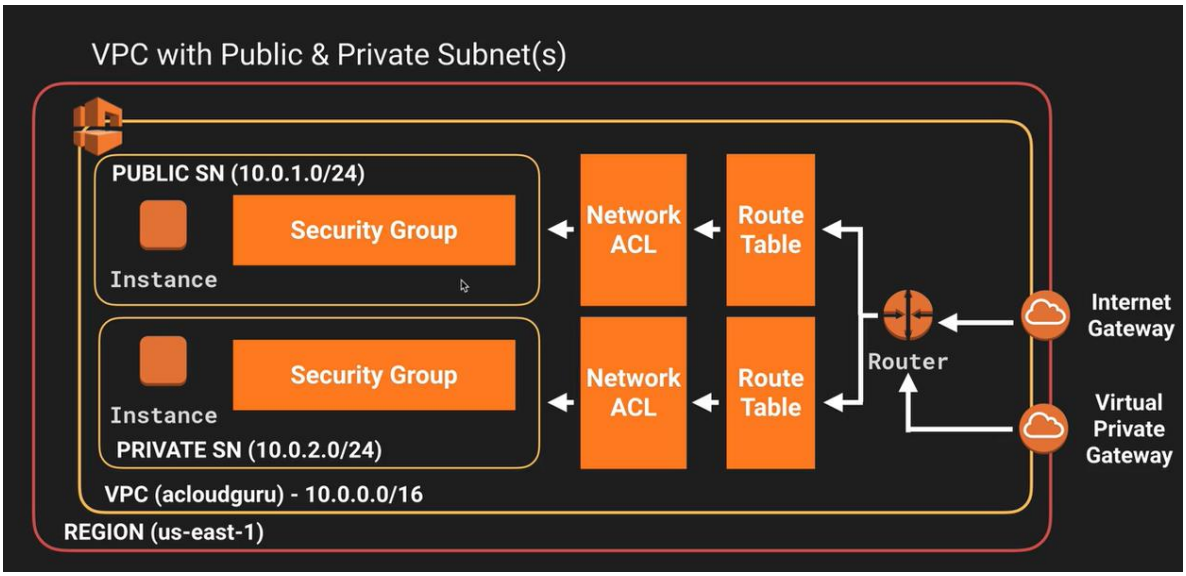


- Grants users limited and temporary access to AWS resources. From three sources:
  - Federation (Like AD).
  - Federation with mobile apps.
  - Cross Account Access.
- Federation: combining or joining a list of users in one domain (like IAM) with a list of users in another domain (like AD).
- Identity Broker: a service that allows you to take an identity from point A and join it with B.
- Identity Store: Facebook, AD.
- Identity.

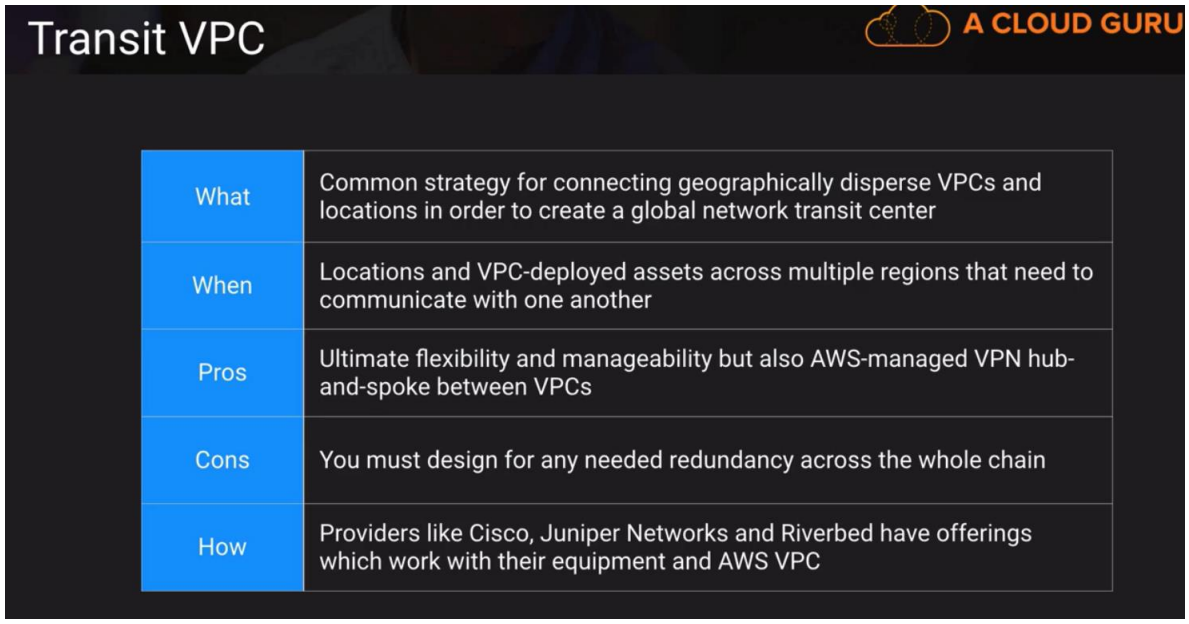
Tips:

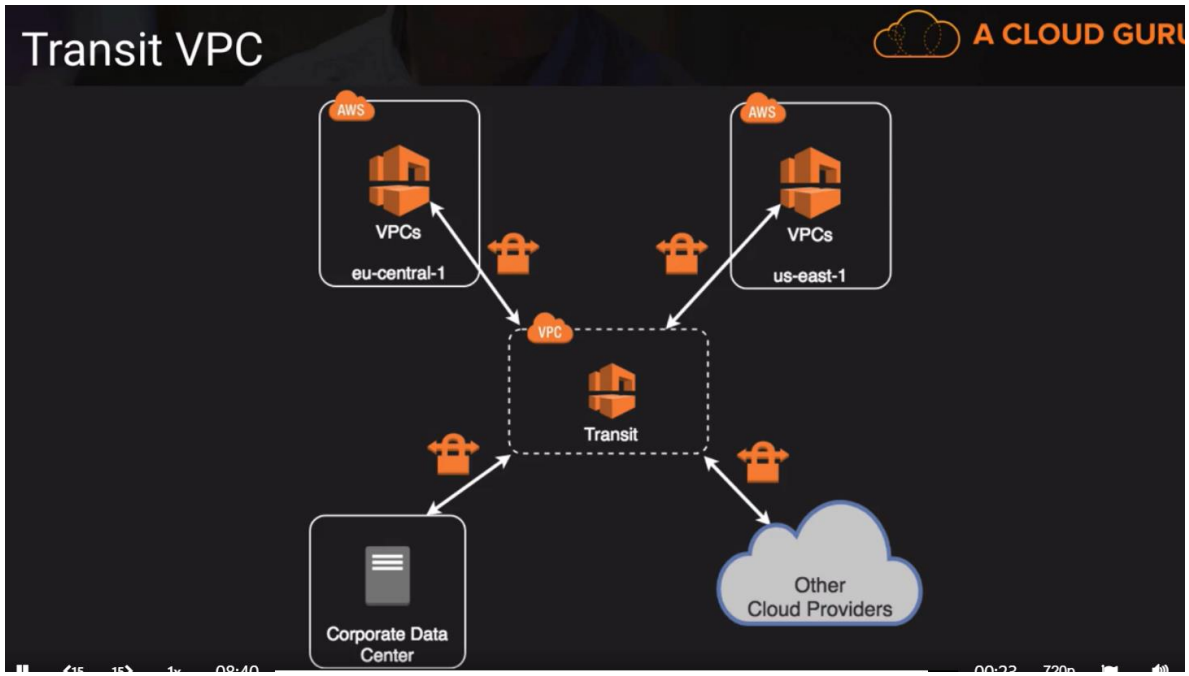
- Q: Which feature can be used to configure console access for users authenticated by Active Directory?
- A: Federated authentication with STS
- Do tests using the "Web Identity Federation Playground" at https://web-identity-federation-playground.s3.amazonaws.com/index.html

Amazon VPC

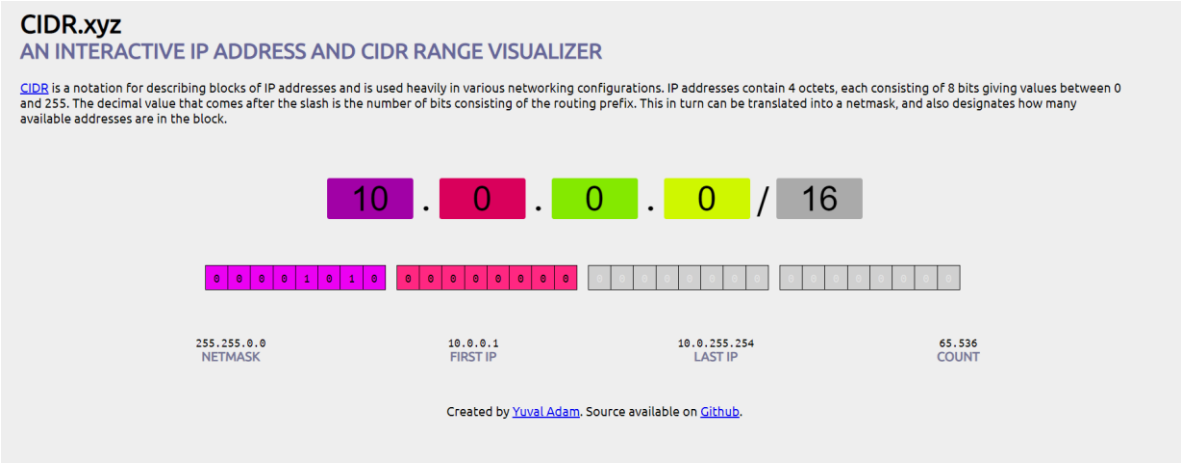


- One subnet = One availability zone.
- 10/8 (10.0.0.0) Highest IP range.
- 172.16/12 (172.162) Medium IP range.
- 192.168.0.0 (192.168/16) Low IP range.
- NAT Instances must be in a public subnet.
- NAT instance vs NAT gateway use NAT gateway.
- You need to add to your route tables your NAT gateway.
- Default VPC vs Custom VPC.
- Default is user friendly, all subnets have a route out to the internet.
- Each EC2 has both a public and a private IP address.
- VPC Peering – Allows you to connect one VPC with another via direct network route using private IP address.
- You can do VPC peering between different accounts.
- VPC peers can peer with 4 VPCS, no transitive peering.
- You can create transitive VPCs to do peering.





- Security groups are stateful (if open 80, I can send and receive traffic), with NACL, are stateless, need to open ingress and outbound-
- After creating a VPC, it creates security group, network ACL and route table.



- There are 5 reserved Ips in each subnet:
    - 10.0.0.0 Network address.
    - 10.0.0.1 Reserved by AWS for the VPC router.
    - 10.0.0.2 For the DNS.
    - 10.0.0.3 Reserved by AWS for future use.
- You can only have an IGW for one VPC:
- CIDR ranges:
    - /24 es 256
    - /25 es 128
    - /26 es 64
    - /27 es 32
    - /28 es 16
    - (Minus 5 reserved Ips in each range to get available IP)
- Security groups do not expand VPCs, they are just for one VPC.
- NACL by default, they are prohibited ingress.
- Ephemeral ports are a short-lived transport protocol port, depends on the client.
- Rules are evaluated in numerical order.
- The default ACL allows all inbound and outbound traffic.
- You can create and ACL, the default behavior is denying everything.
- ACL to many subnets.
- Direct Connect from ON PREMISE.
- Direct Connect Gateway can connect to different regions.

Unicast vs. Multicast

A CLOUD GURU

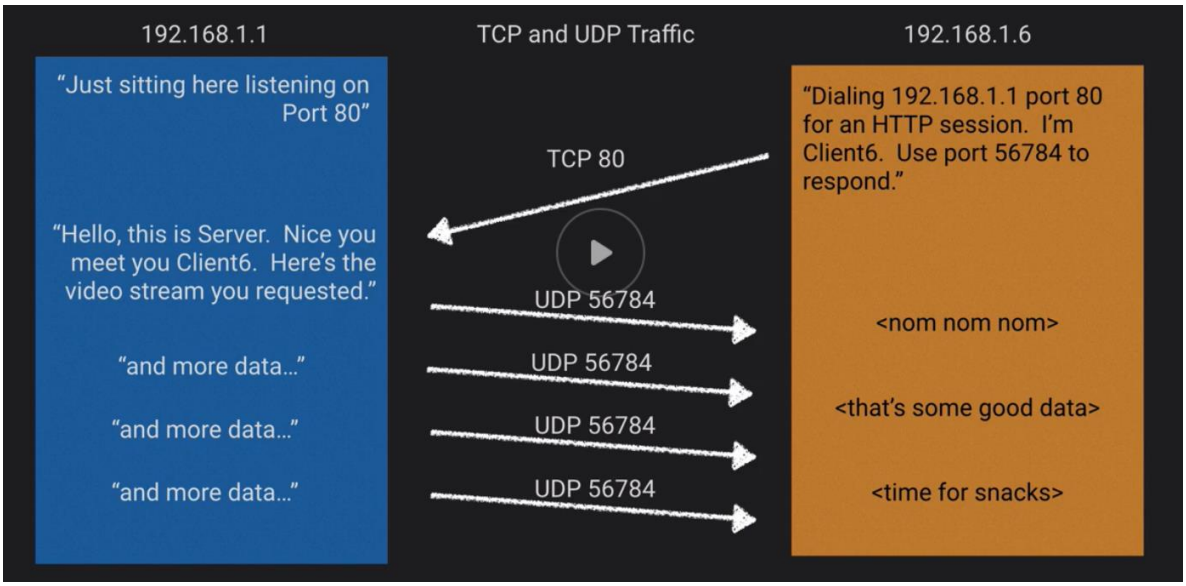
Unicast

Multicast

TCP vs UDP vs ICMP

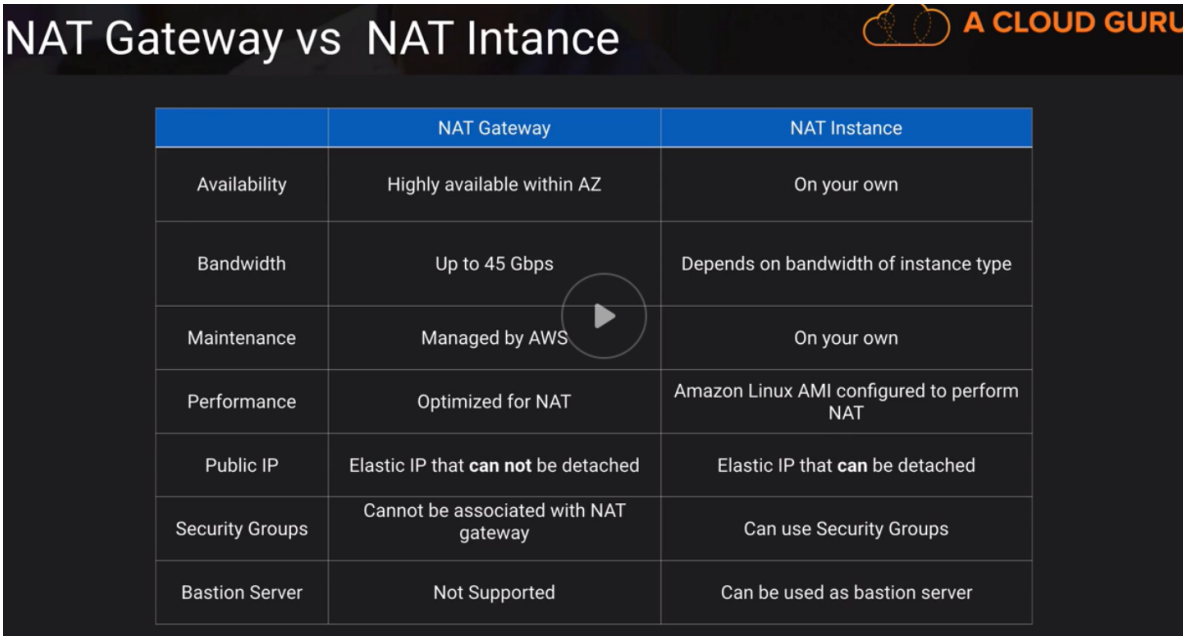
A CLOUD GURU

Layer 4 Protocol	Characteristics	Plain Speak	Uses
TCP	Connection-based, stateful, acknowledges receipt	After everything I say, I want you to confirm that you received it.	Web, Email, File Transfer
UDP	Connectionless, stateless, simple, no retransmission delays	I'm going to start talking and its ok if you miss some words	Streaming media, DNS
ICMP	Used by network devices to exchange info	We routers can keep in touch about the health of the network using our own language	traceroute, ping



- VPC Endpoints:
- A VPC endpoint enables you to connect to certain AWS services without the data travelling over the Internet. This is done by routing the traffic within the Amazon VPC network. "API Gateway", "Kinesis Data Streams" and "DynamoDB" are all services that can be connected to via VPC endpoints, however the "Amazon MQ" service is currently only available by using an Internet Gateway. Further information: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html
- Interface endpoint
    - Amazon API Gateway
    - Amazon AppStream 2.0
    - AWS App Mesh
    - AWS CloudFormation
    - AWS CloudTrail
    - Amazon CloudWatch
    - Amazon CloudWatch Events
    - Amazon CloudWatch Logs
    - AWS CodeBuild
    - AWS CodeCommit
    - AWS CodePipeline
    - AWS Config
    - Amazon EC2 API
    - Elastic Load Balancing
    - Amazon Elastic Container Registry

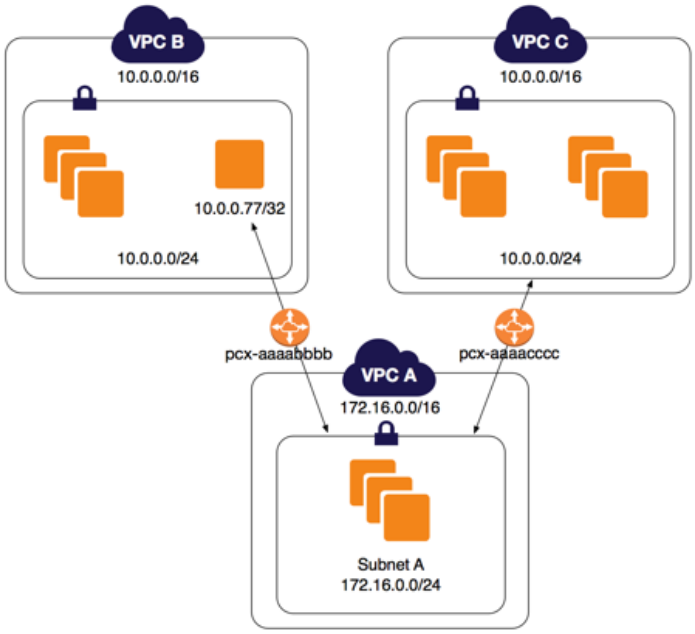
    - Amazon Elastic Container Service
    - AWS Glue
    - AWS Key Management Service
    - Amazon Kinesis Data Firehose
    - Amazon Kinesis Data Streams
    - Amazon SageMaker and Amazon SageMaker Runtime
    - Amazon SageMaker Notebook Instance
    - AWS Secrets Manager
    - AWS Security Token Service
    - AWS Service Catalog
    - Amazon SNS
    - Amazon SQS
    - AWS Systems Manager
    - AWS Storage Gateway
    - AWS Transfer for SFTP
    - Endpoint services hosted by other AWS accounts
    - Supported AWS Marketplace partner services
- Gateway endpoints
    - Supported services:
        - Amazon
        - DynamoDB



	NAT Gateway	NAT Instance
Availability	Highly available within AZ	On your own
Bandwidth	Up to 45 Gbps	Depends on bandwidth of instance type
Maintenance	Managed by AWS	On your own
Performance	Optimized for NAT	Amazon Linux AMI configured to perform NAT
Public IP	Elastic IP that **can not** be detached	Elastic IP that **can** be detached
Security Groups	Cannot be associated with NAT gateway	Can use Security Groups
Bastion Server	Not Supported	Can be used as bastion server

Tips

- Internet Gateways do not have any type of bandwidth issues.
- Customers can now use Jumbo Frames for traffic between their Virtual Private Cloud (VPC) and on-premises networks over AWS Direct Connect.
- The maximum transmission unit (MTU) of a network connection is the size, in bytes, of the largest permissible packet that can be passed over the connection. The larger the MTU of a connection, the more data can be passed in a single packet. Until now, traffic over AWS Direct Connect was limited to 1,500 MTU.
- With this release, customers can use Jumbo Frames for their AWS Direct Connect traffic. Jumbo Frames allow more than 1,500 bytes (up to 9,001 bytes) of data by increasing the payload size per packet, and thus lowering the packet overhead. As a result, you need fewer packets to send the same amount of data, which improves the end-to-end network performance. In addition, this release enables new use cases, such as supporting network overlay protocols, for on-premises connectivity over AWS Direct Connect.
- https://docs.aws.amazon.com/vpc/latest/peering/peering-configurations-partial-access.html



Architecture - One VPC Peered with Two VPCs Using Longest Prefix Match

Additional reading

- "AWS re:Invent 2018: AWS Direct Connect: Deep Dive (NET403)", https://www.youtube.com/watch?v=DXFooR95BYc.

AWS Cloud Adoption Framework

- The AWS Cloud Adoption Framework (AWS CAF) helps organizations understand how cloud adoption transforms the way they work, and it provides structure to identify and address gaps in skills and processes. Applying the AWS CAF in your organization results in an actionable plan with defined work streams that can guide your organization's path to cloud adoption. This framework leverages our experiences and best practices in assisting organizations around the world with their cloud adoption journey.

Figure 1: The AWS Cloud Adoption Framework (CAF)

- Business Perspective – Common roles: Business Managers, Finance Managers, Budget Owners, and Strategy Stakeholders.
    - Helps stakeholders understand how to update the staff skills and organizational processes they will need to optimize business value as they move their operations to the cloud.
- People Perspective – Common roles: Human Resources, Staffing, and People Managers.
    - Provides guidance for stakeholders responsible for people development, training, and communications. Helps stakeholders understand how to Amazon Web Services – An Overview of the AWS Cloud Adoption Framework Page 3 update the staff skills and organizational processes they will use to optimize and maintain their workforce, and ensure competencies are in place at the appropriate time.

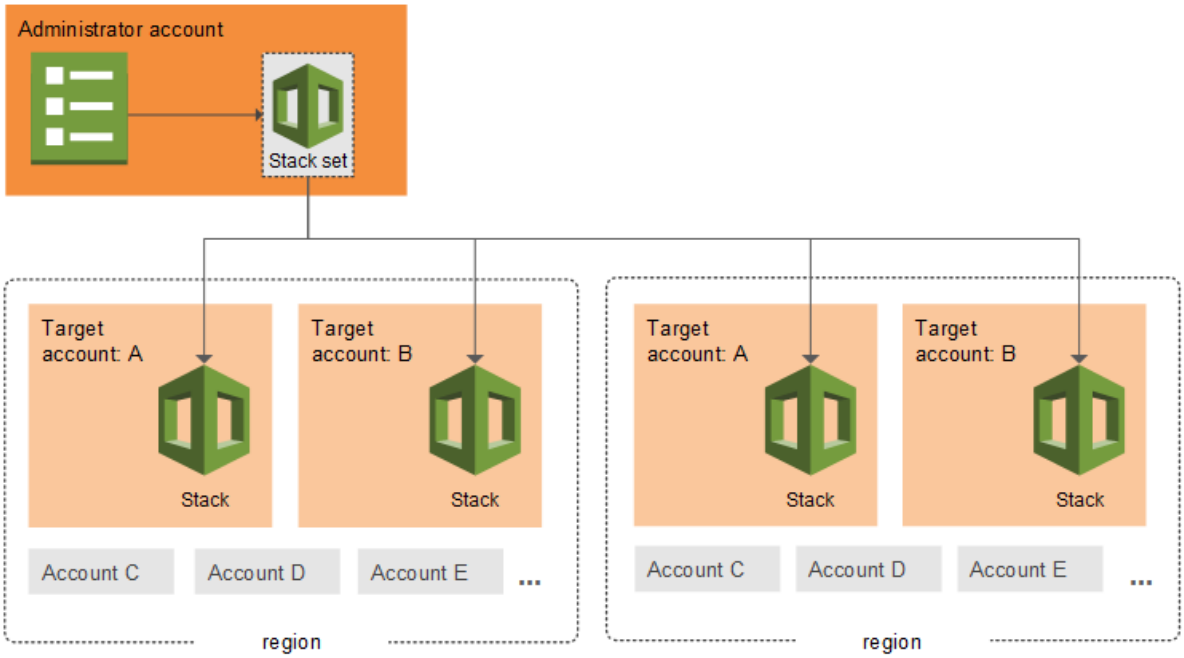
- Governance Perspective – Common roles: CIO, Program Managers, Project Managers, Enterprise Architects, Business Analysts, and Portfolio Managers.
    - Provides guidance for stakeholders responsible for supporting business processes with technology. Helps stakeholders understand how to update the staff skills and organizational processes that are necessary to ensure business governance in the cloud and manage and measure cloud investments to evaluate their business outcomes.
- Platform Perspective – Common roles: CTO, IT Managers, and Solution Architects.
    - Helps stakeholders understand how to update the staff skills and organizational processes that are necessary to deliver and optimize cloud solutions and services.
- Security Perspective – Common roles: CISO, IT Security Managers, and IT Security Analysts.
    - Helps stakeholders understand how to update the staff skills and organizational processes that are necessary to ensure that the architecture deployed in the cloud aligns to the organization's security control requirements, resiliency, and compliance requirements.
- Operations Perspective – Common roles: IT Operations Managers and IT Support Managers.
    - Helps stakeholders understand how to update the staff skills and organizational processes that are necessary to ensure system health and reliability during the move of operations to the cloud and then to operate using agile, ongoing, cloud computing best practices.

AWS CloudFormation

- Stack template version is always 2010 09 09
- Parameters: its input values user defined
- Conditions: For example, if a parameter is "prod", do a validation
- Mappings: is for mappings, for example AMI ID for each region
- Transform: You can use it to include code outside the template
- Resources: what is going to be deployed
- Outputs, what is going to be outputs to the Console
- Stack policies: Protect specific resources within your stack from being unintentionally deleted or updated.
    - It can't be deleted once launched, but it can be modified using the CLI.
    - Example:

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "Update:*",
      "Principal": "*",
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : "Update:*",
      "Principal": "*",
      "Resource" : "LogicalResourceId/ProductionDatabase"
    }
  ]
}
```

- This policy by defaults deny changes on your stack. You need to explicitly allow changes to the stack, and deny (in this case, deny changes to "LogicalResourceId/ProductionDatabase").
    - https://d0.awsstatic.com/whitepapers/aws-amazon-vpc-connectivity-options.pdf
- Changesets:
    - When you need to update a stack, understanding how your changes will affect running resources before you implement them can help you update stacks with confidence. Change sets allow you to preview how proposed changes to a stack might impact your running resources, for example, whether your changes will delete or replace any critical resources, AWS CloudFormation makes the changes to your stack only when you decide to execute the change set, allowing you to decide whether to proceed with your proposed changes or explore other changes by creating another change set. You can create and manage change sets using the AWS CloudFormation console, AWS CLI, or AWS CloudFormation API.
- Stacksets:
    - AWS CloudFormation StackSets extends the functionality of stacks by enabling you to create, update, or delete stacks across multiple accounts and regions with a single operation. Using an administrator account, you define and manage an AWS CloudFormation template, and use the template as the basis for provisioning stacks into selected target accounts across specified regions.



Additional reading

- "AWS re:Invent 2017: Deep Dive on AWS CloudFormation", https://www.youtube.com/watch?v=01hy48R9Kr8.

AWS CloudTrail

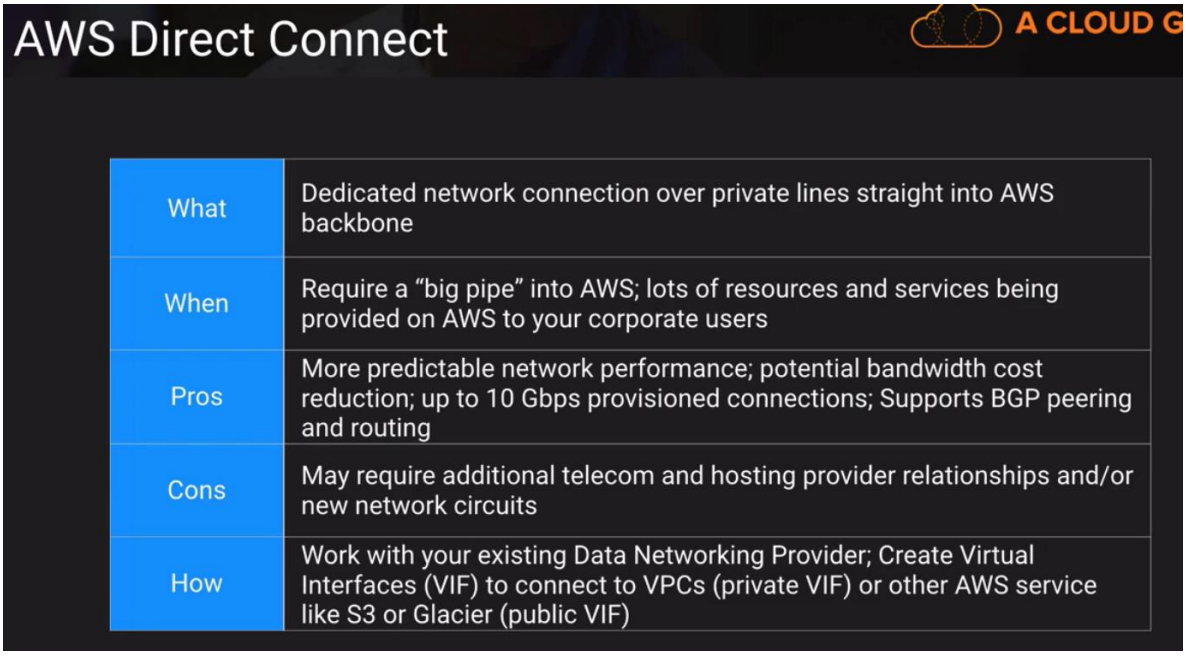
- AWS Config is for resource configuration, AWS CloudTrail is to log API calls and AWS CloudWatch is to measure performance.

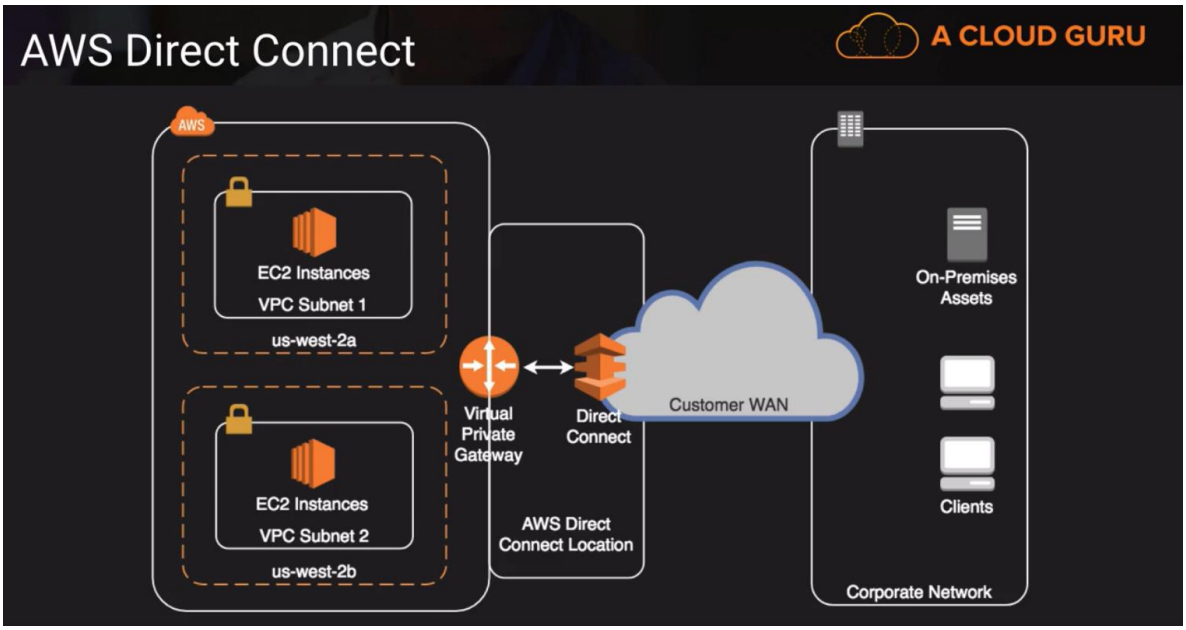
AWS Config

- AWS Config is for resource configuration, AWS CloudTrail is to log API calls and AWS CloudWatch is to measure performance.
- Compliance checks are triggered periodically or by configuration changes.
- Managed or custom rules.

AWS Direct Connect

- Whenever we enable Direct Connect, it is recommended to use Direct Connect Gateway to connect multiple regions.





- What is a VIF?
- Types of VIF
    - Private virtual interface: A private virtual interface should be used to access an Amazon VPC using private IP addresses.

    - **Public virtual interface:** A public virtual interface can access all AWS public services using public IP addresses.
    - **Transit virtual interface:** A transit virtual interface should be used to access one or more Amazon VPC Transit Gateways associated with Direct Connect gateways.
- What is a LAG?

Additional reading

- "AWS re:Invent 2018: AWS Direct Connect: Deep Dive (NET403)", https://www.youtube.com/watch?v=DXFooR95BYc

AWS Directory Services

Types of Directory Services Offered

A CLOUD GURU

Directory Service Option	Description	Best for...
AWS Cloud Directory	Cloud-native directory to share and control access to hierarchical data between applications	Cloud applications that need hierarchical data with complex relationships
Amazon Cognito	Sign-up and sign-in functionality that scales to millions of users and federated to public social media services	Develop consumer apps or SaaS
AWS Directory Service for Microsoft Active Directory	AWS-managed full Microsoft AD (standard or enterprise) running on Windows Server 2012 R2	Enterprises that want hosted Microsoft AD or you need LDAP for Linux apps
AD Connector	Allows on-premises users to log into AWS services with their existing AD credentials. Also allows EC2 instances to join AD domain.	Single sign-on for on-prem employees and for adding EC2 instances to the domain
Simple AD	Low scale, low cost AD implementation based on Samba	Simple user directory, or you need LDAP compatibility

AD Connector vs. Simple AD

A CLOUD GURU

AD Connector

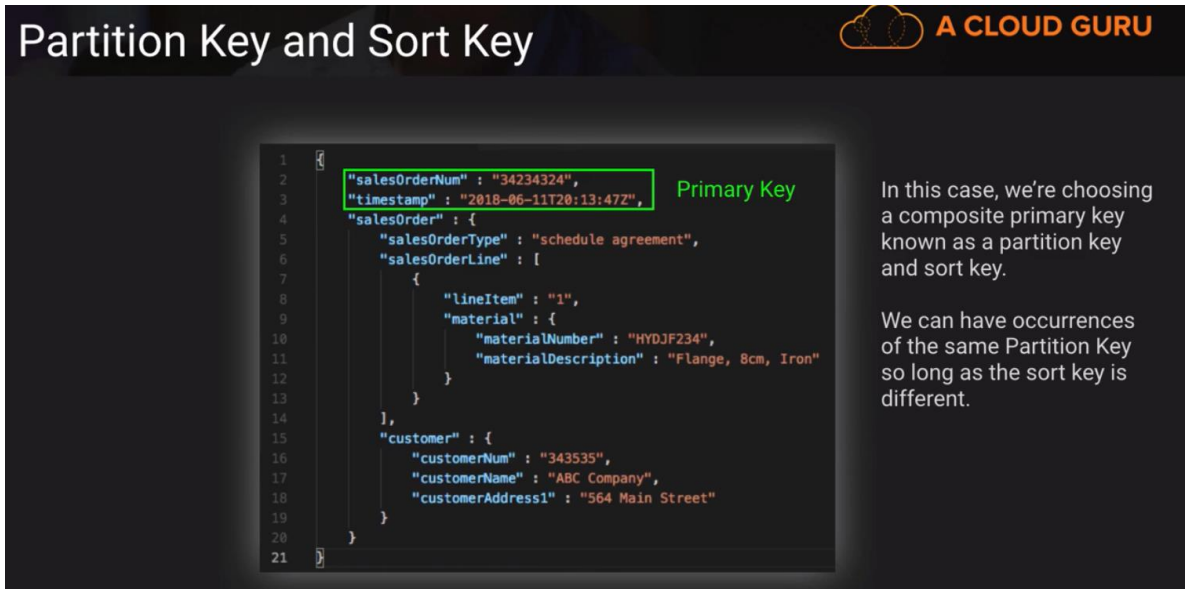
- Must have existing AD
- Existing AD users can access AWS assets via IAM roles.
- Supports MFA via existing RADIUS-based MFA infrastructure

Simple AD

- Stand-alone AD based on Samba
- Supports user accounts, groups, group policies, and domains
- Kerberos-based SSO
- MFA not supported
- No Trust Relationships

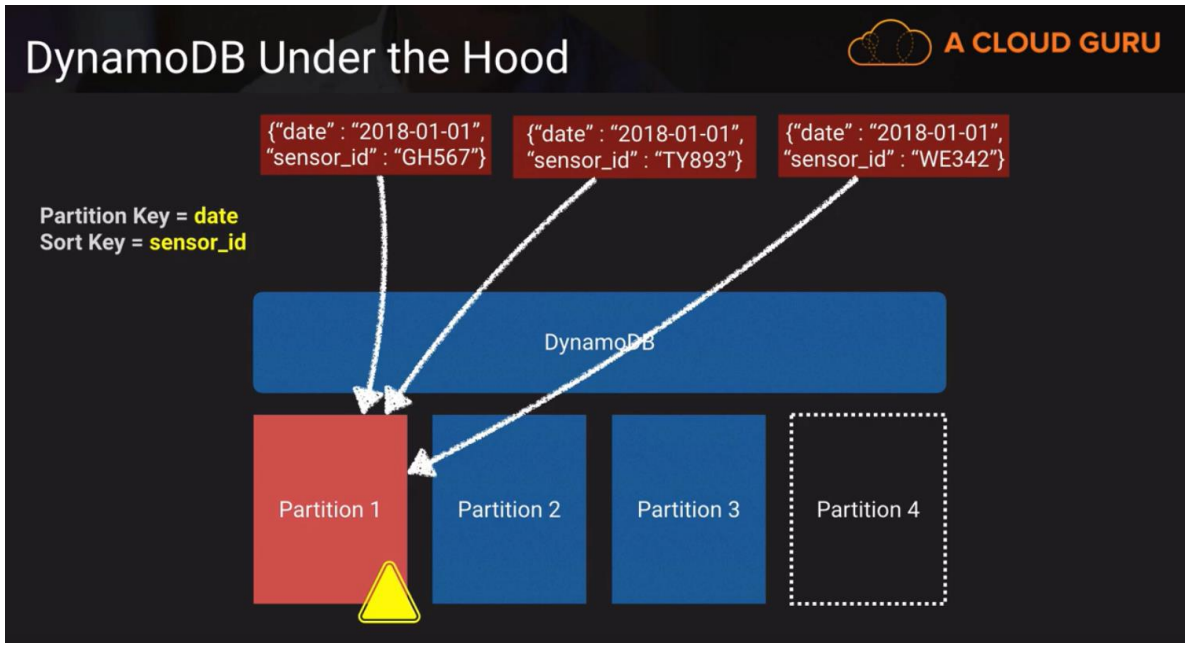
AWS DynamoDB

- Managed MultiAZ cross region replicated document database.
- All reads all eventually consisted, but you can specify strong consistency in the query.
- Priced on throughput rather than compute.
- You can provision read/write capacity in anticipation of need.
- You can select auto scale capacity based on maximum and minimum.

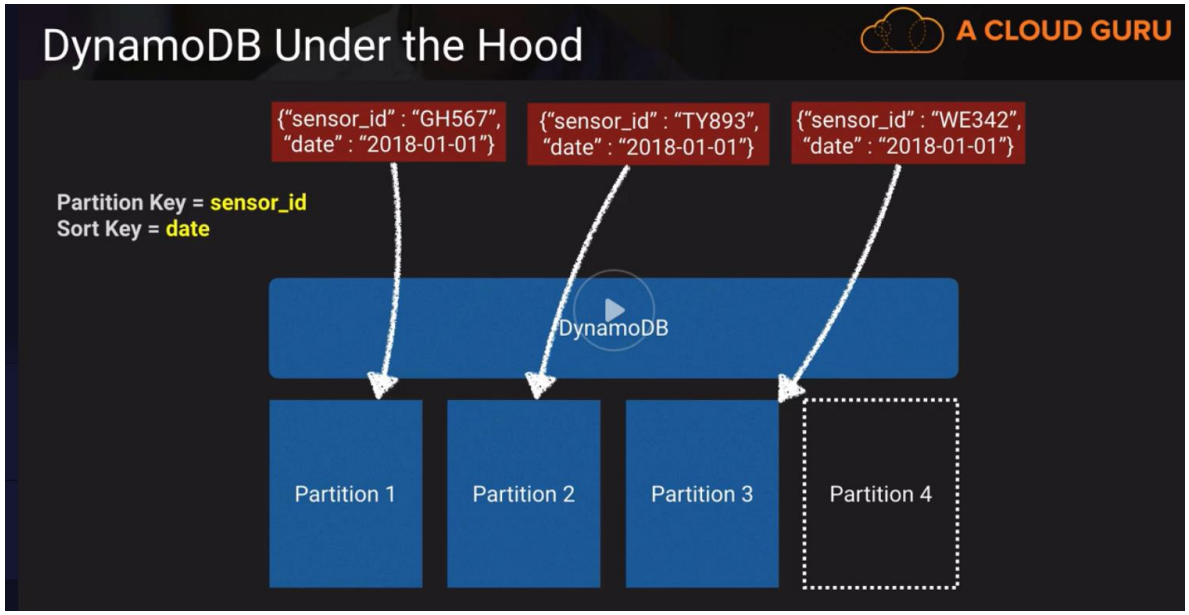


How partition key and sort key work out on the background?

Antipattern:



Correct usage:



Secondary Indexes

A CLOUD GURU

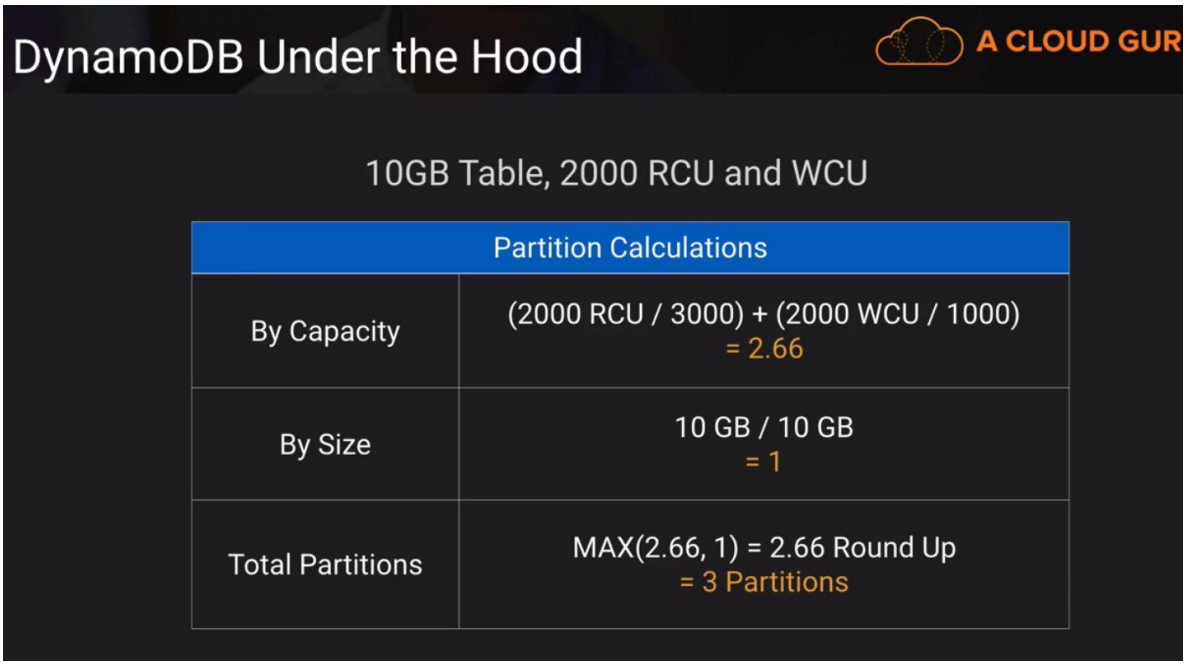
Index Type	Description	How to Remember
Global Secondary Index	Partition key and sort key can be different from those on the table.	I'm not restricted to just the partitioning set forth by the partition key. I'm GLOBAL BABY!
Local Secondary Index	Same partition key as the table but different sort key	I have to stay local and respect the table's partition key, but I can choose whatever sort key I want.

- Max 5 local and 5 global secondary indexes
- Max 20 attributes across all indexes
- Indexes take up storage space

Secondary Indexes

A CLOUD GU

If you need to...	Consider...	Cost	Benefit
...access just a few attributes the fastest way possible	Projecting just those few attributes in a global secondary index	Minimal	Lowest possible latency access for non-key items
...frequently access some non-key attributes	Projecting those attributes in a global secondary index	Moderate; aim to offset cost of table scans	Lowest possible latency access for non-key items
...frequently access most non-key attributes	Projecting those attributes or even the entire table in a global secondary index	Up to Double	Maximum flexibility
...rarely query but write or update frequently	Projecting keys only for the global secondary index	Minimal	Very fast write or updates for non-partition-key items



Uses cases for DynamoDB streams:

- Many applications can benefit from the ability to capture changes to items stored in a DynamoDB table, at the point in time when such changes occur. The following are some example use cases:
    - An application in one AWS Region modifies the data in a DynamoDB table. A second application in another Region reads these data modifications and writes the data to another table, creating a replica that stays in sync with the original table.
    - A popular mobile app modifies data in a DynamoDB table, at the rate of thousands of updates per second. Another application captures and stores data about these updates, providing near-real-time usage metrics for the mobile app.
    - A global multi-player game has a multi-master topology, storing data in multiple AWS Regions. Each master stays in sync by consuming and replaying the changes that occur in the remote Regions.
    - An application automatically sends notifications to the mobile devices of all friends in a group as soon as one friend uploads a new picture.
    - A new customer adds data to a DynamoDB table. This event invokes another application that sends a welcome email to the new customer.

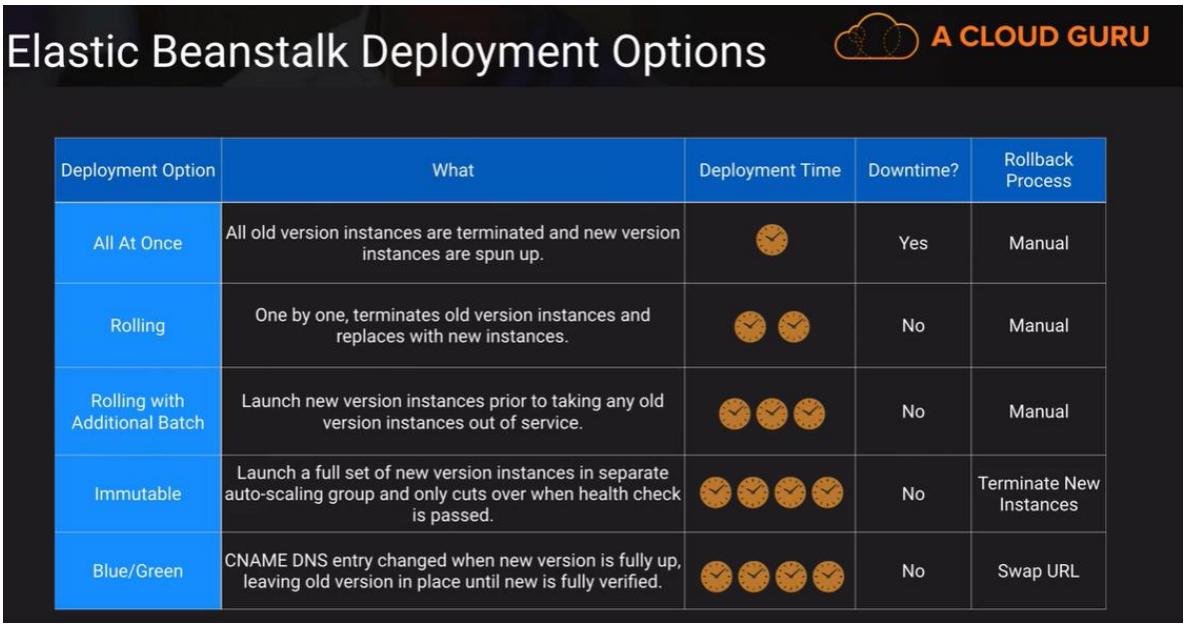
- DynamoDB Streams enables solutions such as these, and many others. DynamoDB Streams captures a time-ordered sequence of item-level modifications in any DynamoDB table and stores this information in a log for up to 24 hours. Applications can access this log and view the data items as they appeared before and after they were modified, in near-real time.

Additional reading

- "AWS re:Invent 2018: Amazon DynamoDB Deep Dive: Advanced Design Patterns for DynamoDB (DAT401)", https://www.youtube.com/watch?v=HaEPXoXVf2k.

AWS Elastic Beanstalk

- Types of deployments:



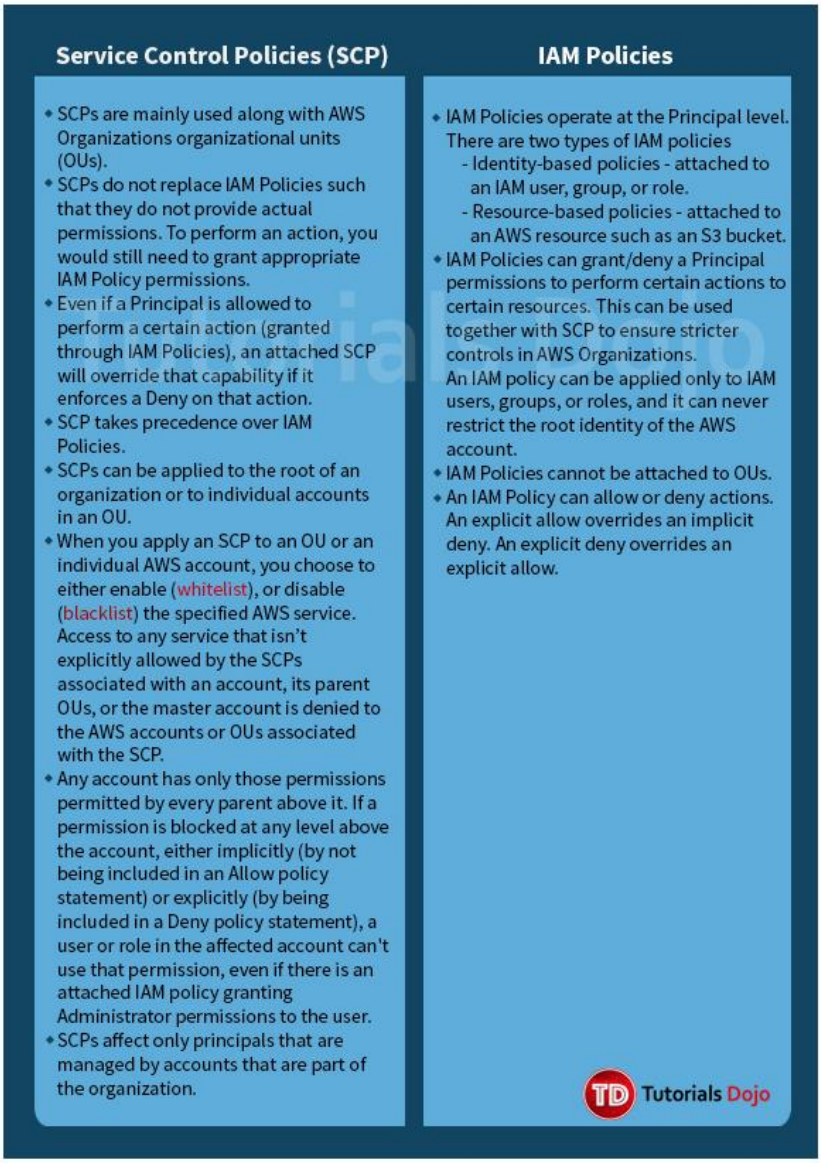
Deployment Option	What	Deployment Time	Downtime?	Rollback Process
All At Once	All old version instances are terminated and new version instances are spun up.		Yes	Manual
Rolling	One by one, terminates old version instances and replaces with new instances.		No	Manual
Rolling with Additional Batch	Launch new version instances prior to taking any old version instances out of service.		No	Manual
Immutable	Launch a full set of new version instances in separate auto-scaling group and only cuts over when health check is passed.		No	Terminate New Instances
Blue/Green	CNAME DNS entry changed when new version is fully up, leaving old version in place until new is fully verified.		No	Swap URL

AWS Elastic Search

- Kibana accesses Elastic Search using Cognito.

AWS Identity and Access Management (IAM)

- The maximum number of users is 5,000.
- Difference between SCP and IAM Policies:
    - SCPs operate on Organizations organizational units (OUs)
    - IAM Policies operate at the principal level.
    - Even if a principal is allowed to perform a certain action, an attached SCP policy will override that capability if it's enforcing a Deny.



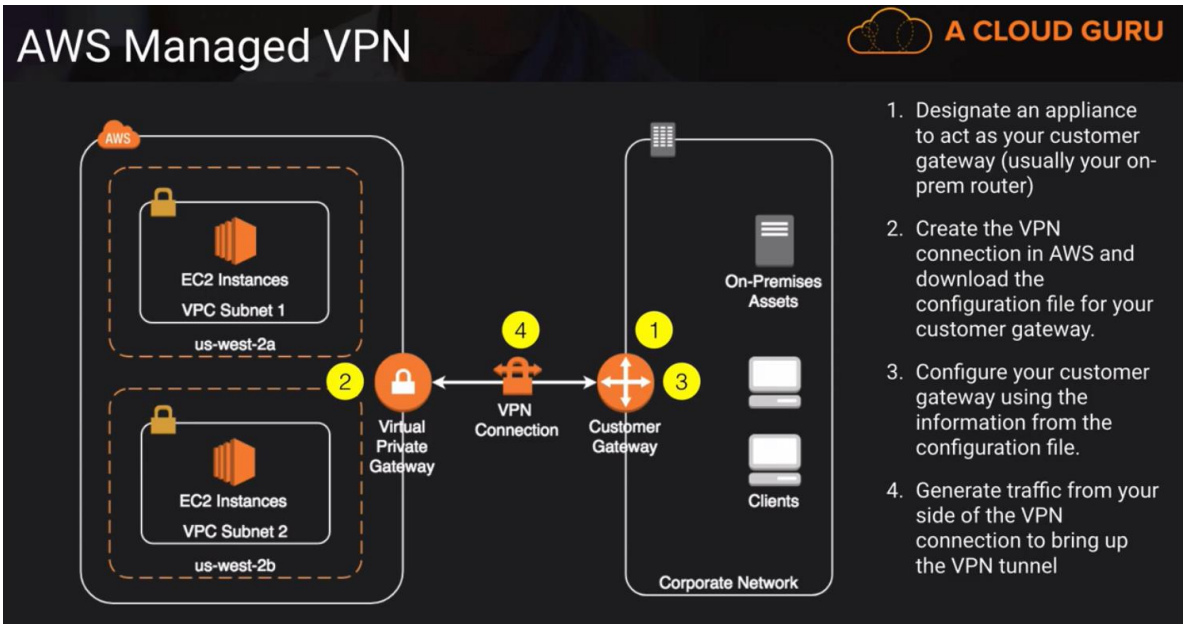
Additional reading

- "AWS re:Invent 2017: IAM Policy Ninja" https://www.youtube.com/watch?v=aISWoPf_XNE.

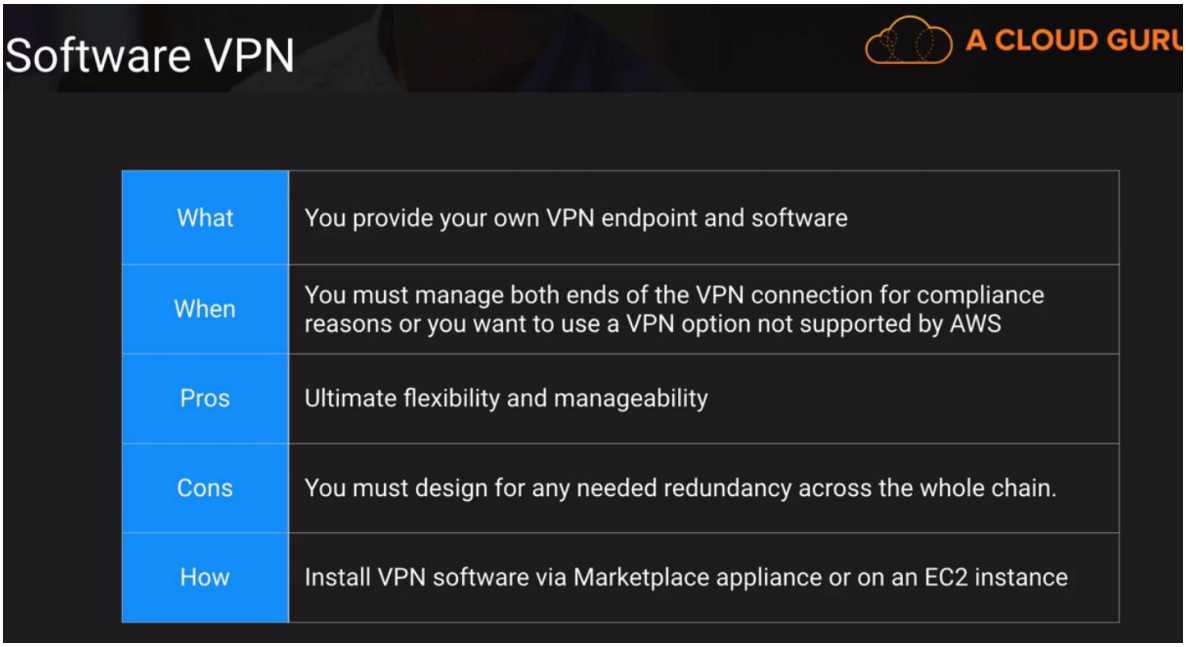
AWS Lambda

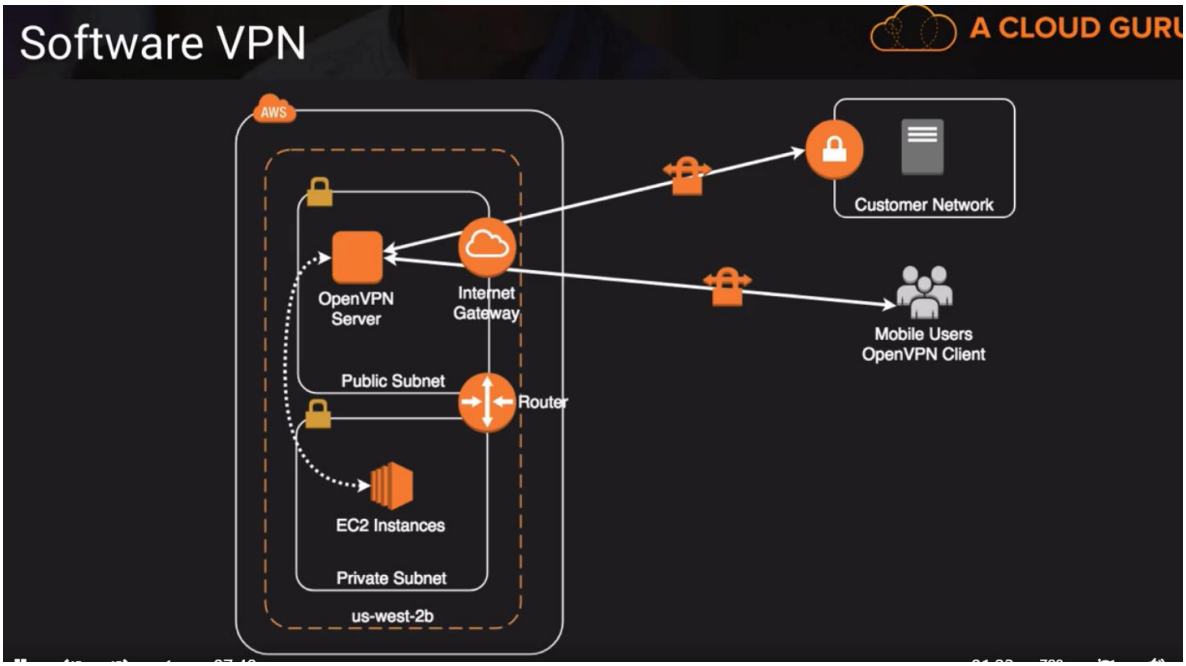
- If the Lambda is inside a VPC, you can use a NAT Gateway to connect to an RDS with the appropriate security group.
- You can break the process into two, one Lambda to query the RDS inside the VPC and then invokes the second Lambda outside the VPC.

AWS Managed VPN



VS Software VPN




Software VPN
A CLOUD GURU
AWS
Customer Network
OpenVPN Server
Internet Gateway
Mobile Users OpenVPN Client
Public Subnet
Router
EC2 Instances
Private Subnet
us-west-2b

AWS OpsWorks

- Difference between CloudFormation:
  - CloudFormation is JUST for infrastructure.
  - OpsWorks is for infrastructure AND application level.
- Check example recipes at https://github.com/aws/opsworks-cookbooks.
- Example of OpsWorks Chef recipe to configure an Apache stack:
  - https://github.com/aws/opsworks-cookbooks/blob/release-chef-11.10/apache2/definitions/apache_site.rb
- OpsWorks is a global service but when creating a stack you must specify a region and it will not allow you to clone to another region. Further information: https://docs.aws.amazon.com/opsworks/latest/userguide/workingstacks-cloning.html

AWS Rekognition

- Amazon Rekognition makes it easy to add image and video analysis to your applications.
    - Object, scene and activity detection
    - Facial recognition
    - Facial analysis
    - Pathing
    - Unsafe content detection
    - Celebrity recognition
    - Text in images

AWS Serverless Application Model (AWS SAM)?

The AWS Serverless Application Model (AWS SAM) is an open-source framework that you can use to build serverless applications on AWS.

A serverless application is a combination of Lambda functions, event sources, and other resources that work together to perform tasks. Note that a serverless application is more than just a Lambda function—it can include additional resources such as APIs, databases, and event source mappings.

You can use AWS SAM to define your serverless applications. AWS SAM consists of the following components:

AWS SAM template specification. You use this specification to define your serverless application. It provides you with a simple and clean syntax to describe the functions, APIs, permissions, configurations, and events that make up a serverless application. You use an AWS SAM template file to operate on a single, deployable, versioned entity that's your serverless application. For the full AWS SAM template specification, see AWS Serverless Application Model Specification.

AWS SAM command line interface (AWS SAM CLI). You use this tool to build serverless applications that are defined by AWS SAM templates. The CLI provides commands that enable you to verify that AWS SAM template files are written according to the specification, invoke Lambda functions locally, step-through debug Lambda functions, package and deploy serverless applications to the AWS Cloud, and so on. For details about how to use the AWS SAM CLI, including the full AWS SAM CLI Command Reference, see AWS SAM CLI.

- It is an AWS CloudFormation extension optimized for serverless.
- New serverless resource types: functions, APIs and tables.
- Open specification.

Additional reading

- "Authoring and Deploying Serverless Applications with AWS SAM", https://www.youtube.com/watch?v=MSsMOtLZXKc.

AWS Snowball

- **Snowball Edge:** Is used when you need transformation (since it has Lambda@Edge).
- **Snowball:** Is used when you need just data transfer to AWS.

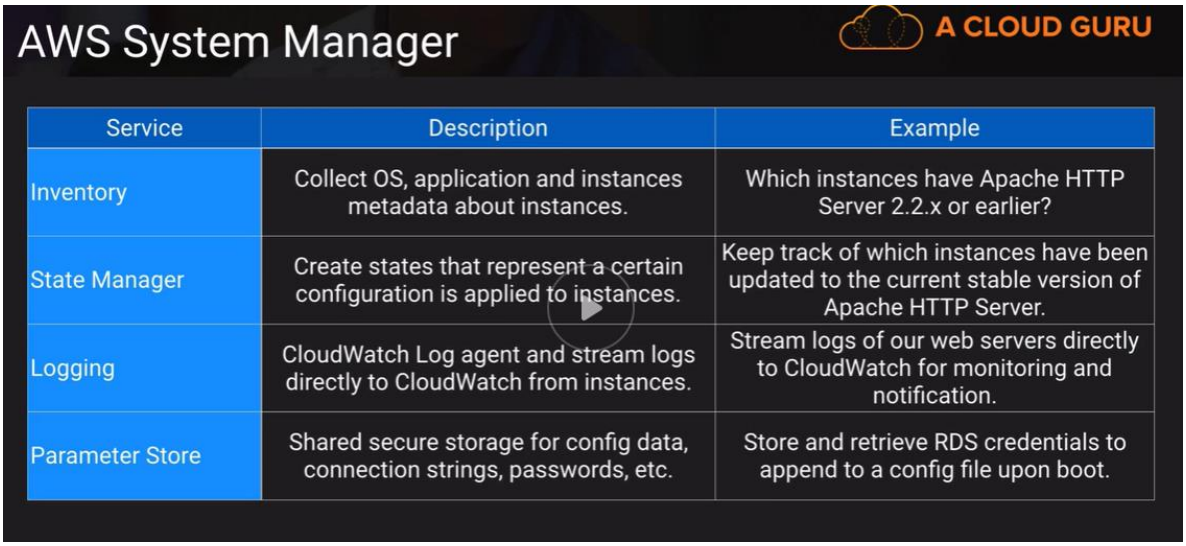
AWS Storage Gateway

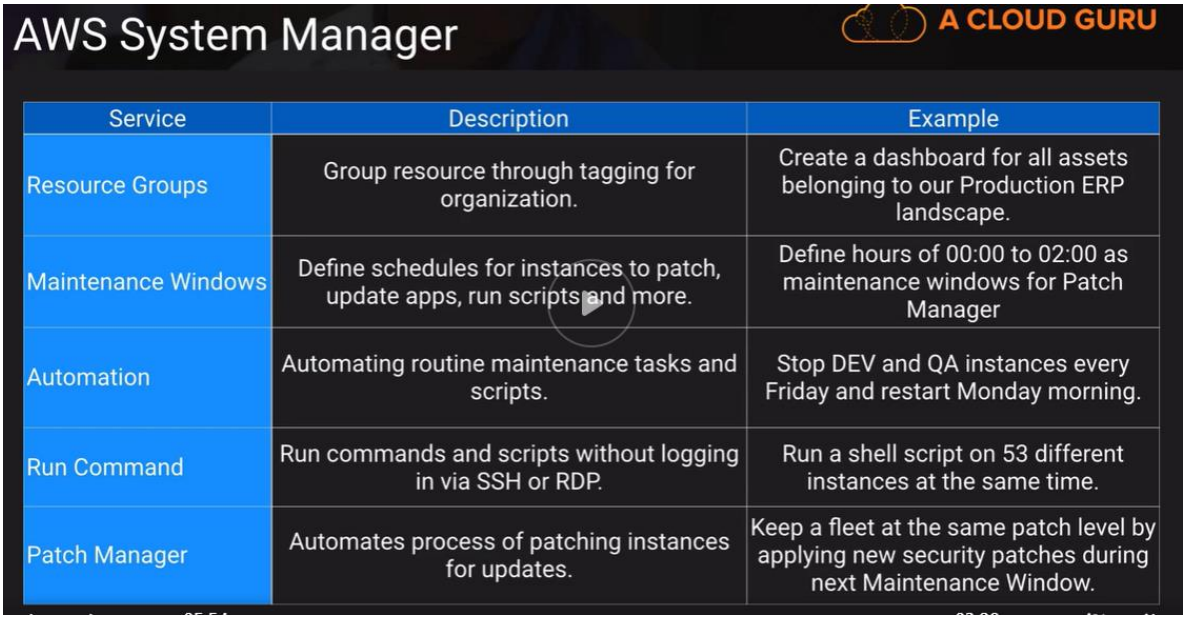
- Provides local storage solutions backed with S3 and Glacier.

New Name	Old Name	Interface	Function
File Gateway	None	NFS, SMB	Allow on-prem or EC2 instances to store objects in S3 via NFS or SMB mount point
Volume Gateway Stored Mode	Gateway-stored Volumes	iSCSI	Async replication of on-prem data to S3
Volume Gateway Cached Mode	Gateway-cached Volumes	iSCSI	Primary data stored in S3 with frequently access data cached locally on-prem
Tape Gateway	Gateway-Virtual Tape Library	iSCSI	Virtual media changer and tape library for use with existing backup software

AWS System Manager (SSM)

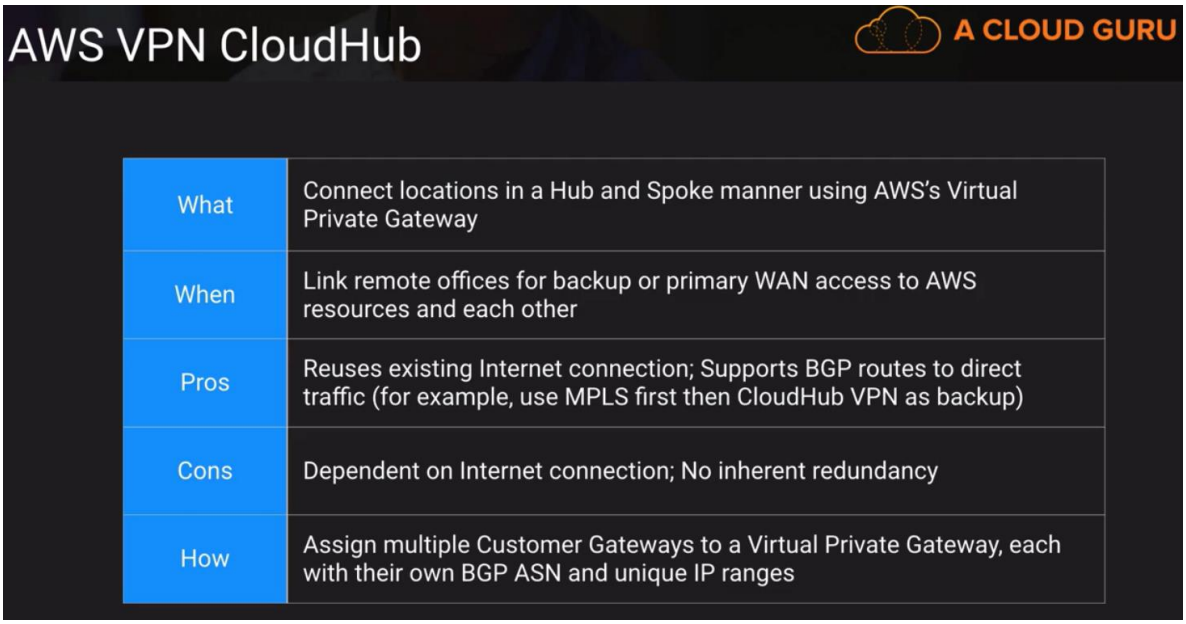
- System Manager (SSM), is a management tool which gives you visibility and control over your AWS Infrastructure.
- Integrates with CloudWatch.
- You can do resource groups within SSM.
- Run command helps you automated tasks, such as apply patched, start up, etc. Or run your base scripts.
- You can control AWS and on-premise resources.
- Example uses cases:

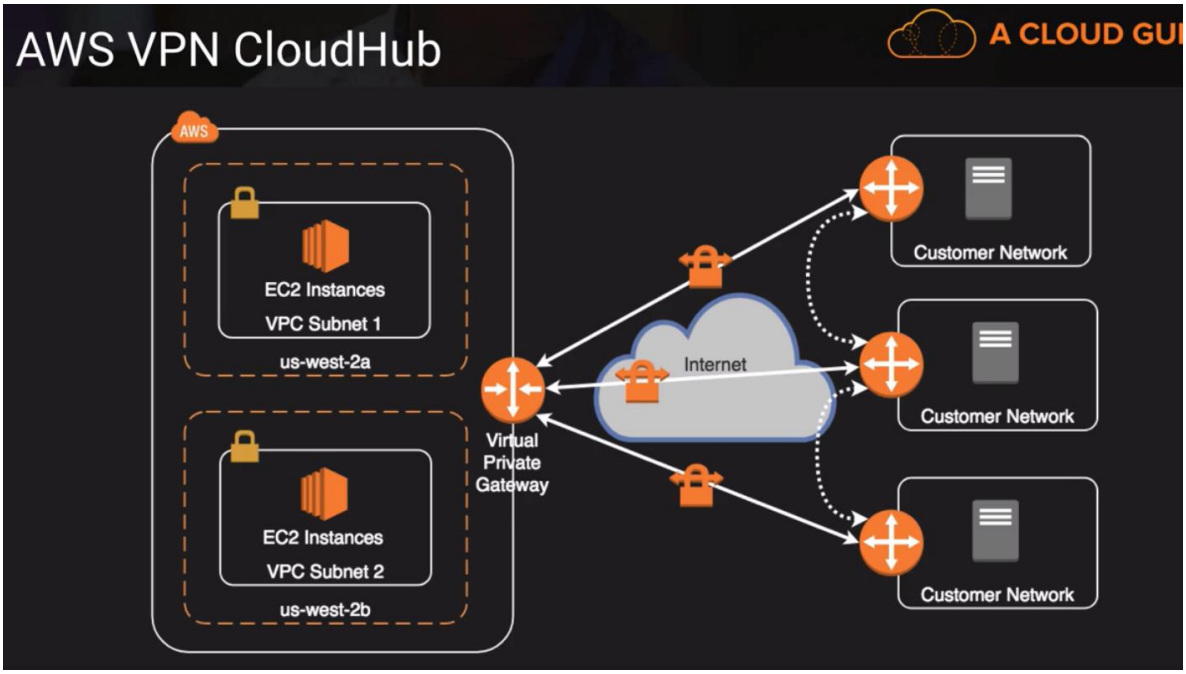




AWS VPN CloudHub

- It's like a software MLPS.





Certification

What I need to study? (TODO: Migrate this to the appropriate section)

- Curso de Linux Academy
- Learn CloudFormation filter
- See video of SQS
- See video of EMR
- See video of DynamoDB
- See video of MobileHub
- Hacer un ejercicio de EMR
- Hacer un ejercicio con Redshift
- See video of CloudFront, understand permissions, signed URLs and origins (s3, restrict access and so on)
- Code Deploy
- Code Pipeline
- CloudFormation
- Direct Connect
- BGP
- Additional Reading:
    - Architecting for the Cloud AWS Best Practices whitepaper, October 2018
    - Microservices on AWS whitepaper, September 2017
    - Amazon Web Services: Overview of Security Processes whitepaper, May 2017
    - https://d0.awsstatic.com/whitepapers/aws-amazon-vpc-connectivity-options.pdf
    - https://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf
    - https://aws.amazon.com/es/premiumsupport/knowledge-center/cloudfront-access-to-amazon-s3/
    - https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html
    - https://docs.aws.amazon.com/es_es/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html
    - https://aws.amazon.com/es/blogs/aws/amazon-dynamodb-accelerator-dax-in-memory-caching-for-read-intensive-workloads/
    - https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.rollingupdates.html?icmpid=docs_elasticbeanstalk_console

- Videos:
  - https://www.aws.training/learningobject/wbc?id=16362
  - https://www.aws.training/Details/Curriculum?id=25384
  - https://www.aws.training/Details/eLearning?id=16368
  - https://www.aws.training/Details/Curriculum?id=13830
  - https://www.aws.training/Details/Curriculum?id=12049
- Labs:
  - EMR
  - Redshift
  - https://acloud.guru/series/acg-projects/view/107
  - https://github.com/ACloudGuru-Resources/Course_Certified_Solutions_Architect_Professional/tree/master/lab-scaling
  - https://github.com/ACloudGuru-Resources/Course_Certified_Solutions_Architect_Professional/tree/master/lab-deployments
- Machine learning speciality
  - https://d1.awsstatic.com/whitepapers/Size-Cloud-Data-Warehouse-on-AWS.pdf
  - https://d1.awsstatic.com/whitepapers/Big_Data_Analytics_Options_on_AWS.pdf
  - https://d1.awsstatic.com/whitepapers/enterprise-data-warehousing-on-aws.pdf
  - https://d1.awsstatic.com/whitepapers/Migrating_to_Apache_Hbase_on_Amazon_S3_on_Amazon_EMR.pdf
  - https://d1.awsstatic.com/whitepapers/RDS/AWS_Database_Migration_Service_Best_Practices.pdf
  - https://www.youtube.com/watch?v=QZ4LAZCbsrQ
  - https://www.youtube.com/watch?v=v5lkNHib7bw
  - https://aws.amazon.com/blogs/big-data/build-a-data-lake-foundation-with-aws-glue-and-amazon-s3/
  - https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html
  - https://www.youtube.com/watch?v=jKPlGznbfZ0
  - https://www.youtube.com/watch?v=0AGNcZfYkzw
  - https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html

- https://www.youtube.com/watch?v=EzxRtfSKlUA
- https://aws.amazon.com/es/blogs/machine-learning/analyze-live-video-at-scale-in-real-time-using-amazon-kinesis-video-streams-and-amazon-sagemaker/
- https://www.youtube.com/watch?v=dNp1emFFGbU
- https://aws.amazon.com/blogs/big-data/create-real-time-clickstream-sessions-and-run-analytics-with-amazon-kinesis-data-analytics-aws-glue-and-amazon-athena/
- https://aws.amazon.com/blogs/big-data/joining-and-enriching-streaming-data-on-amazon-kinesis/
- https://d0.awsstatic.com/whitepapers/whitepaper-streaming-data-solutions-on-aws-with-amazon-kinesis.pdf
- https://www.youtube.com/watch?v=M8jVTI0wHFM
- https://d1.awsstatic.com/whitepapers/aws-power-ml-at-scale.pdf
- https://www.youtube.com/watch?v=S_xeHvP7uMo
- https://www.youtube.com/watch?v=3tHUGmlclI4
- https://www.youtube.com/watch?v=PHYWI4Y9mzs
- https://aws.amazon.com/blogs/big-data/build-a-data-lake-foundation-with-aws-glue-and-amazon-s3/
- https://www.youtube.com/watch?v=3tHUGmlclI4

QA: AWS Certified Solutions Architect – Professional

- Q: Can you migrate non-VM servers using SMS?
- A: No, you can only migrate Virtual Machines: https://docs.aws.amazon.com/server-migration-service/latest/userguide/prereqs.html
- Q: When to use AWS Serverless Application Model (SAM) vs CloudFormation in deploying Lambda with DynamoDB?
- A: N/A
- Q:What is the default baseline in SSM to patch Windows Servers?
- A: AWS-WindowsPredefinedPatchBaseline-OS (https://console.aws.amazon.com/systems-manager/patch-manager/baselines/arn%253Aaws%253Assm%253Aus-east-1%253A075727635805%253Apatchbaseline%252Fpb-09ca3fb51f0412ec3?region=us-east-1)

QA: AWS Certified Sysops Administrator - Associate

- https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html
- If its customer imported, you need to manually rotate keys
    - https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html#rotate-keys-manually
- To do string match, it has to be in the first 5,120 bytes of the response body.
    - https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/health-checks-creating-values.html#health-checks-creating-values-string-matching.
- The flow log is still in the process of being created. In some cases, it can take ten minutes or more after you've created the flow log for the log group to be created, and for data to be displayed.
- There has been no traffic recorded for your network interfaces yet. The log group in CloudWatch Logs is only created when traffic is recorded.
    - https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-troubleshooting.html
- https://aws.amazon.com/es/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/

QA: AWS Certified Machine Learning Specialist

- In general within your dataset, what is the minimum number of observations you should have compared to the number of features?
    - 10 times as many observations as features: https://en.wikipedia.org/wiki/Sample_size_determination

General concepts

Network Maximum Transmission Unit (MTU) for Your EC2 Instance

The maximum transmission unit (MTU) of a network connection is the size, in bytes, of the largest permissible packet that can be passed over the connection. The larger the MTU of a connection, the more data that can be passed in a single packet. Ethernet packets consist of the frame, or the actual data you are sending, and the network overhead information that surrounds it.

Ethernet frames can come in different formats, and the most common format is the standard Ethernet v2 frame format. It supports 1500 MTU, which is the largest Ethernet packet size supported over most of the Internet. The maximum supported MTU for an instance depends on its instance type. All Amazon EC2 instance types support 1500 MTU, and many current instance sizes support 9001 MTU, or jumbo frames.

Serverless

- No servers to provision or manage.
- Scales with usage.
- Never pay for idle.
- Availability and fault tolerance built in.

Continuous integration, continuous delivery and continuous deployment

- The main difference between continuous delivery and continuous deployment is that continuous delivery still includes manual processes to release to production.

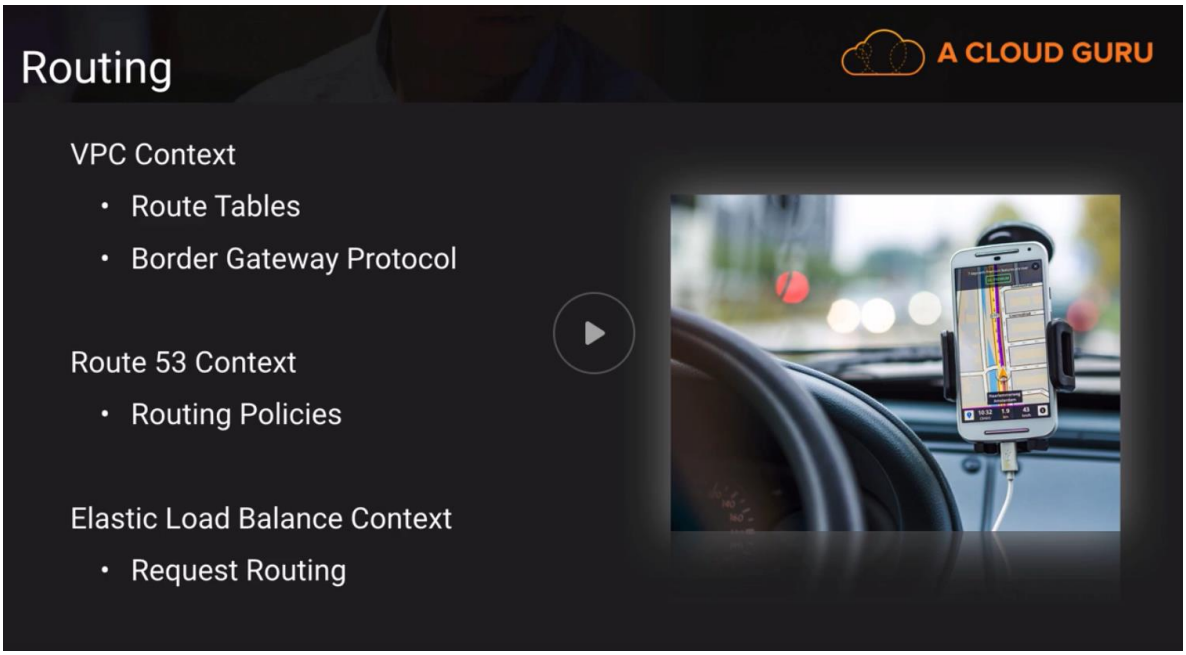
Additional reading

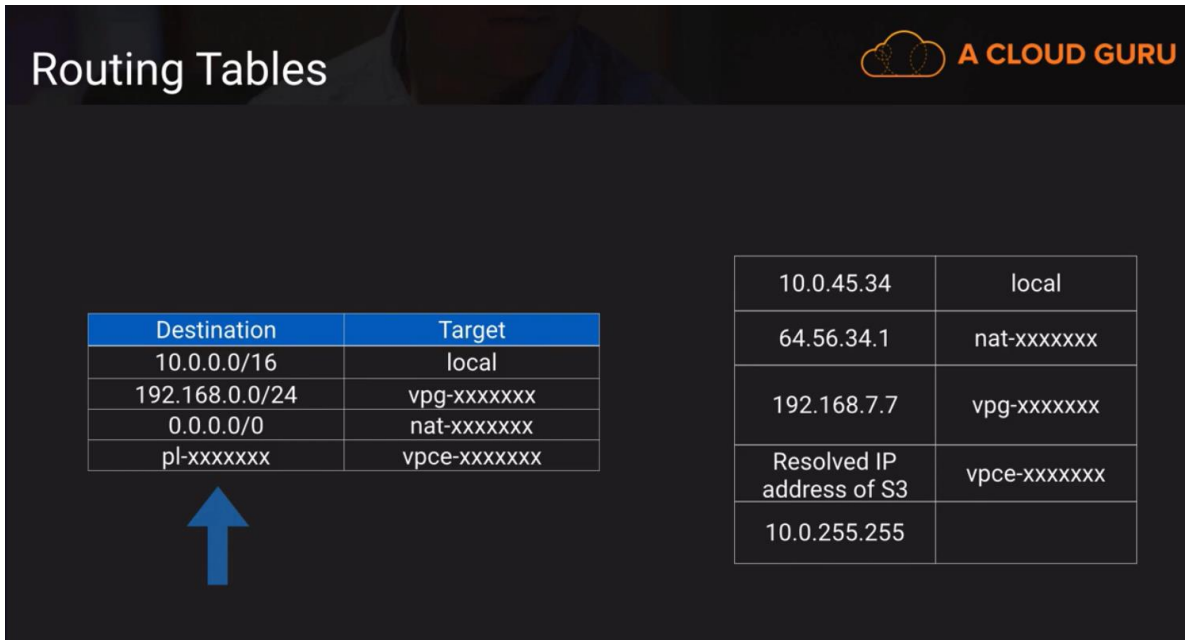
- "Practicing Continuous Integration and Continuous Delivery on AWS", https://d1.awsstatic.com/whitepapers/DevOps/practicing-continuous-integration-continuous-delivery-on-AWS.pdf

iSCSI

In computing, iSCSI is an acronym for Internet Small Computer Systems Interface, an Internet Protocol (IP)-based storage networking standard for linking data storage facilities.

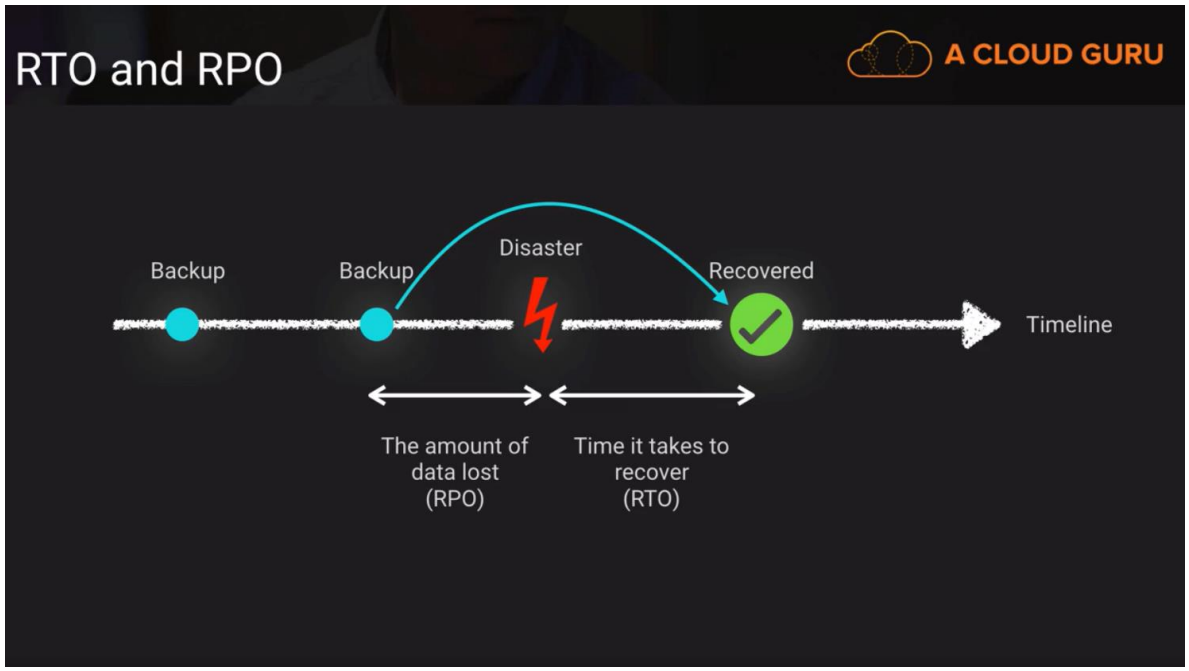
Routing





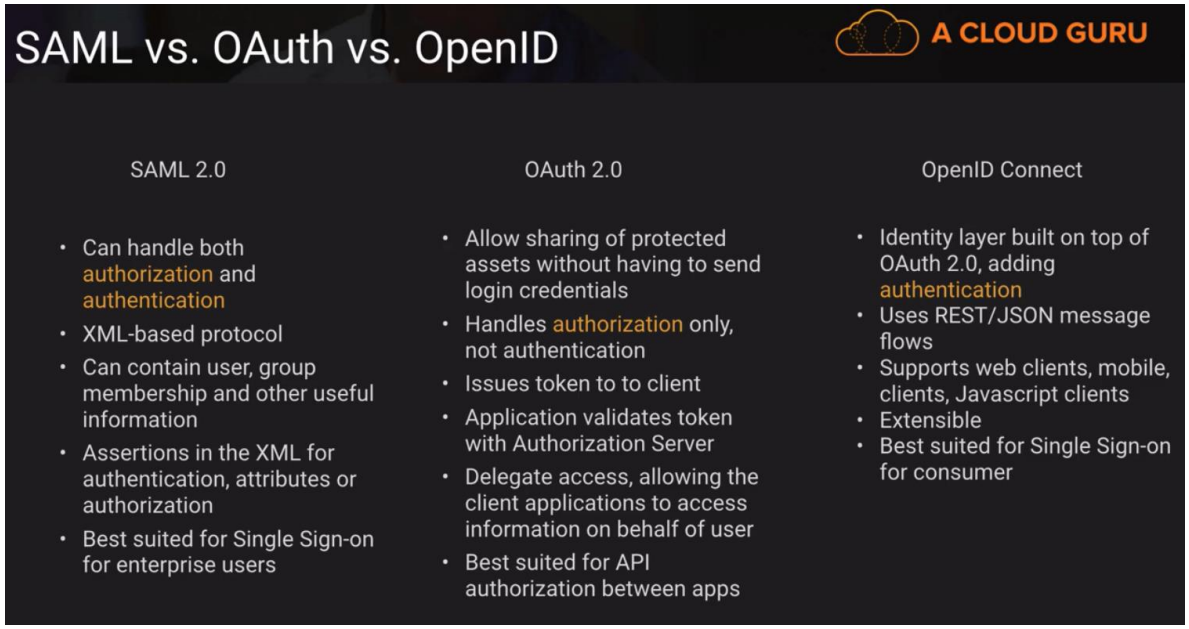
Fault tolerance

- Fault-tolerance defines the ability for a system to remain in operation even if some of the components used to build the system fail.
- In RDS, MultiAZ is for DRP (disaster recovery planning).
- In a MultiAZ RDS database, the DNS pointing to the endpoint is updated automatically.



Federated authentication

- Difference between methods:

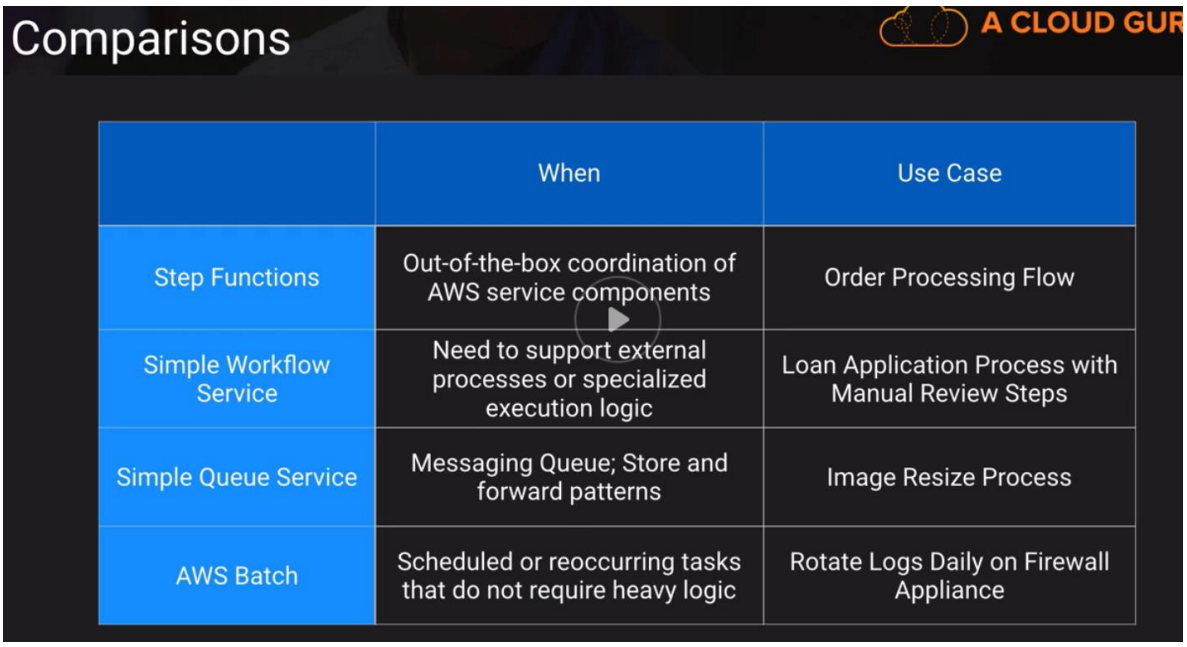


High availability

- Elasticity is the ability to increase or decrease really fast your infrastructure.
- Read replicas are an excellent mechanism for elasticity.
- Scalability - Longer periods (Ability to grow your infrastructure without any limits).
- Elasticity - Smaller periods (Ex. autoscaling).

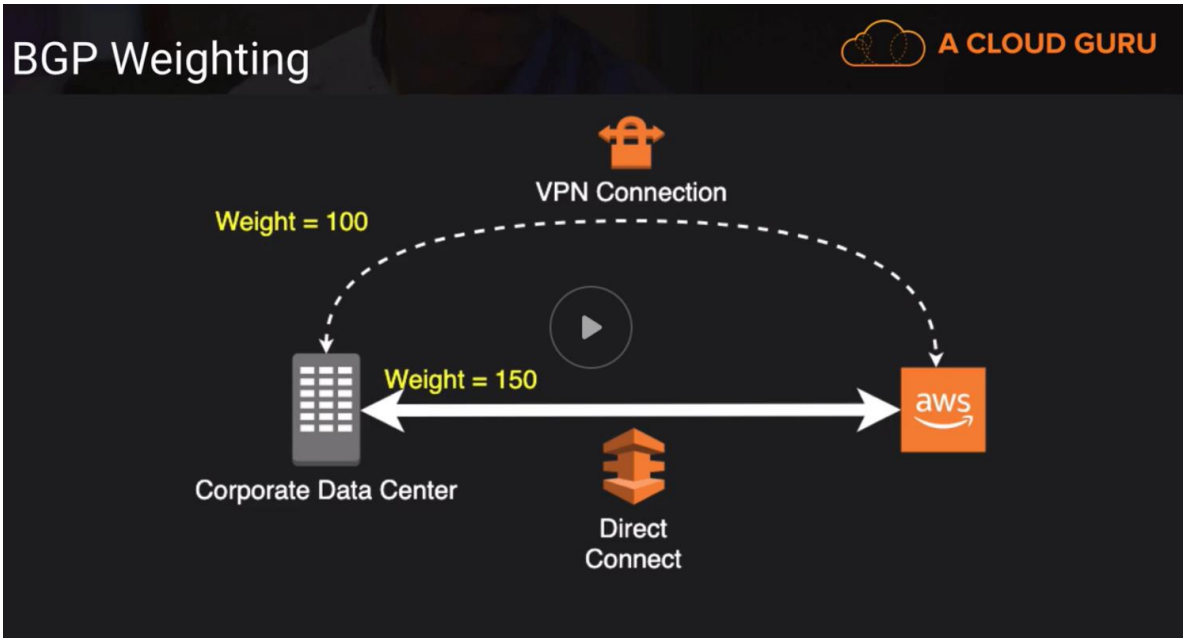
- 99.99% is = 52.6 minutes / year.
- 99.9% is = 8.76 hours / year.
- 99.5% is = 1.83 days / year.
- Load testing is pretty self-explanatory.
- Smoke testing is functional testing.

Difference between step functions, Simple Workflow Service, SQS and AWS Batch



	When	Use Case
Step Functions	Out-of-the-box coordination of AWS service components	Order Processing Flow
Simple Workflow Service	Need to support external processes or specialized execution logic	Loan Application Process with Manual Review Steps
Simple Queue Service	Messaging Queue; Store and forward patterns	Image Resize Process
AWS Batch	Scheduled or reoccurring tasks that do not require heavy logic	Rotate Logs Daily on Firewall Appliance

BGP

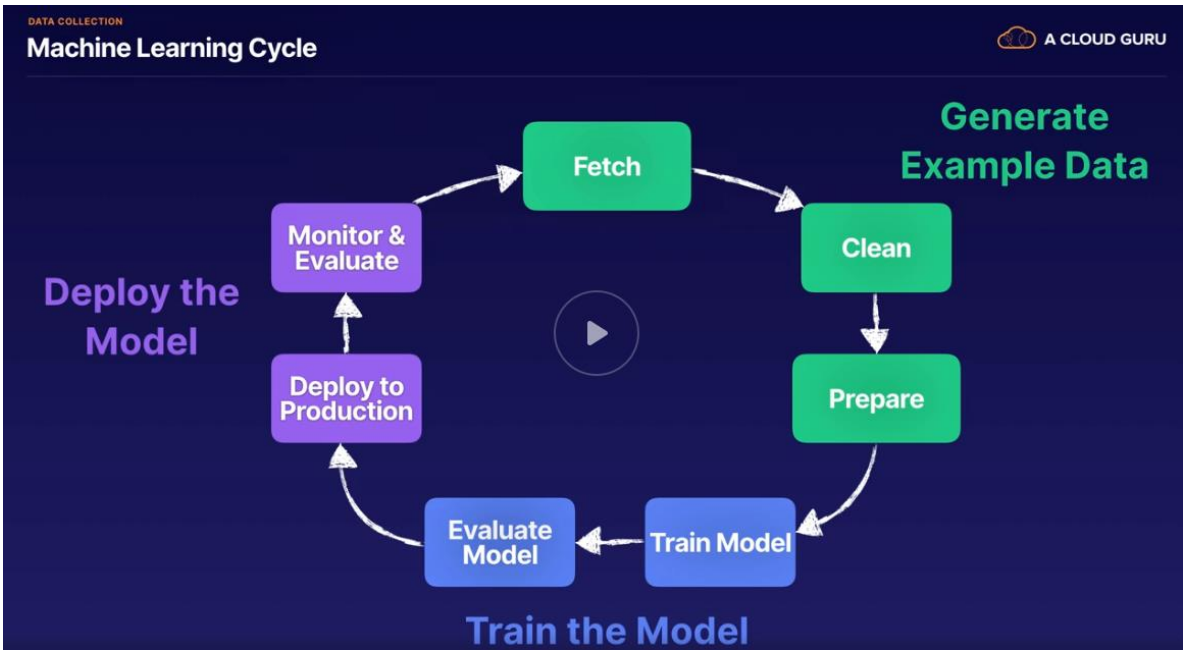


Consistency models (ACID & BASE)

- ACID
  - **Atomic transactions:** are all or nothing.
  - **Consistent:** Transactions must be valid.
  - **Isolated:** Transactions can't mess with one or another.
  - **Durable**: Completed transactions must stick around.
- BASE
  - **Basic availability:** Values availability even if stale.
  - **Soft-state:** Might not be instantly consisted across stores.
  - **Eventual consistency:** Will achieve consistency at some point.

Machine Learning

Machine learning cycle

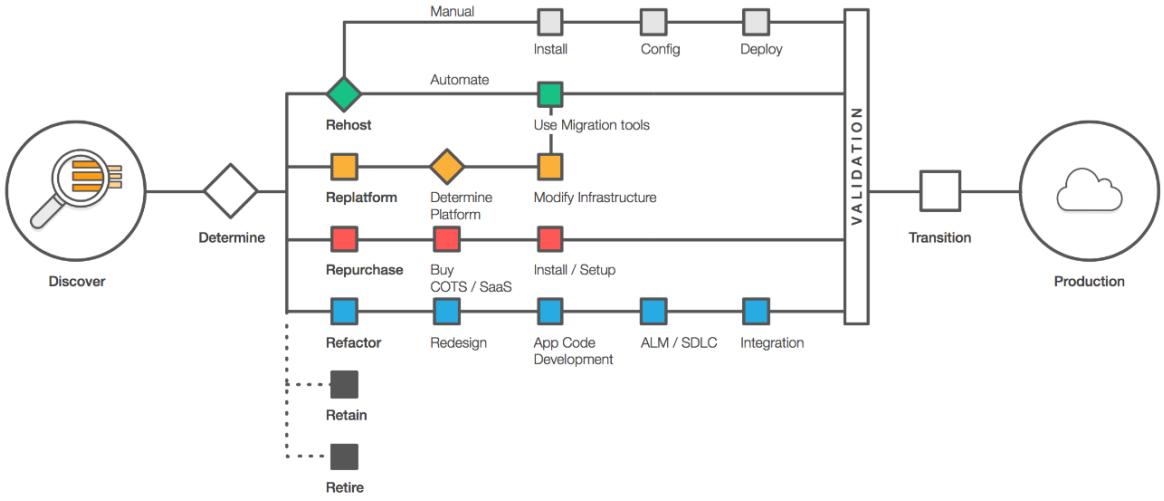


Migrations

Six Common Application Migration Strategies

Organizations usually begin to think about how they will migrate an application during Phase 2 of the migration process. This is when you determine what is in your environment and the migration strategy for each application. The six approaches detailed below are common migration strategies employed and build upon "The 5 R's" that Gartner outlined in 2011.

You should gain a thorough understanding of which migration strategy will be best suited for certain portions of your portfolio. It is also important to consider that while one of the six strategies may be best for migrating certain applications in a given portfolio, another strategy might work better for moving different applications in the same portfolio.



1. Rehost ("lift and shift")

In a large legacy migration scenario where the organization is looking to quickly implement its migration and scale to meet a business case, we find that the majority of applications are rehosted. Most rehosting can be automated with tools such as AWS SMS although you may prefer to do this manually as you learn how to apply your legacy systems to the cloud.

You may also find that applications are easier to re-architect once they are already running in the cloud. This happens partly because your organization will have developed better skills to do so and partly because the hard part - migrating the application, data, and traffic - has already been accomplished.

2. Replatform ("lift, tinker and shift")

This entails making a few cloud optimizations in order to achieve some tangible benefit without changing the core architecture of the application. For example, you may be looking to reduce the amount of time you spend managing database instances by migrating to a managed relational database service such as Amazon Relational Database Service (RDS), or migrating your application to a fully managed platform like AWS Elastic Beanstalk.

3. Repurchase ("drop and shop")

This is a decision to move to a different product and likely means your organization is willing to change the existing licensing model you have been using. For workloads that can easily be upgraded to newer versions, this strategy might allow a feature set upgrade and smoother implementation.

4. Refactor / Re-architect

Typically, this is driven by a strong business need to add features, scale, or performance that would otherwise be difficult to achieve in the application's existing environment. If your organization is looking to boost agility or improve business continuity by moving to a service-oriented architecture (SOA) this strategy may be worth pursuing - even though it is often the most expensive solution.

5. Retire

Identifying IT assets that are no longer useful and can be turned off will help boost your business case and direct your attention towards maintaining the resources that are widely used.

6. Retain

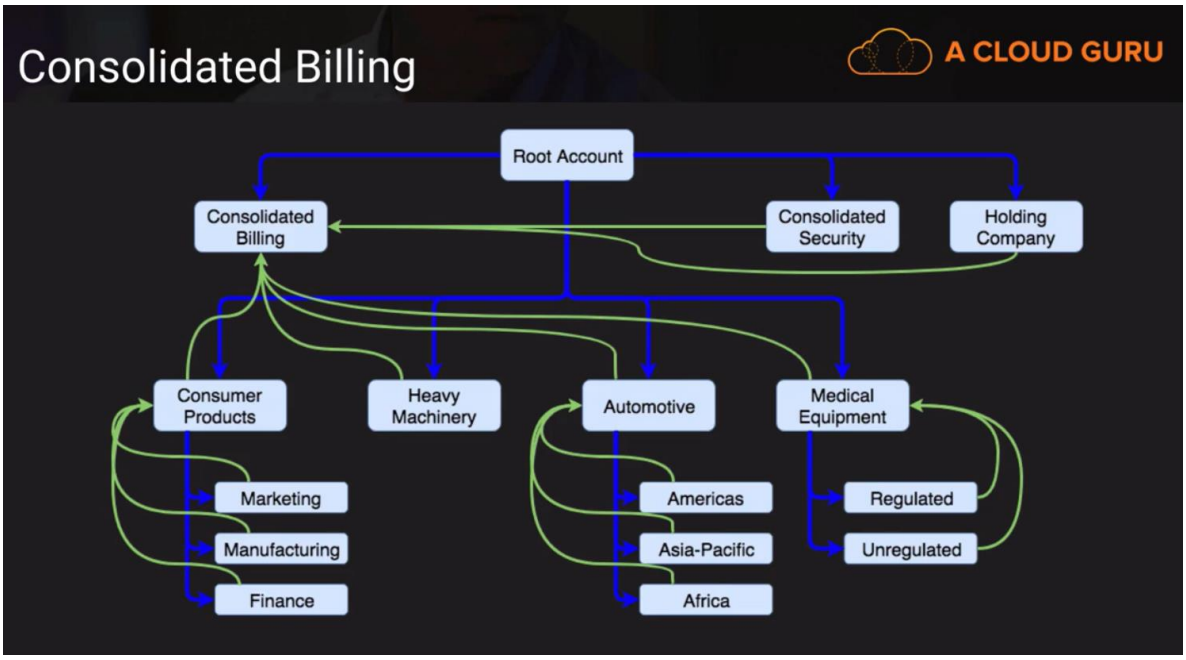
You may want to retain portions of your IT portfolio because there are some applications that you are not ready to migrate and feel more comfortable keeping them on-premises, or you are not ready to prioritize an application that was recently upgraded and then make changes to it again.

Additional reading

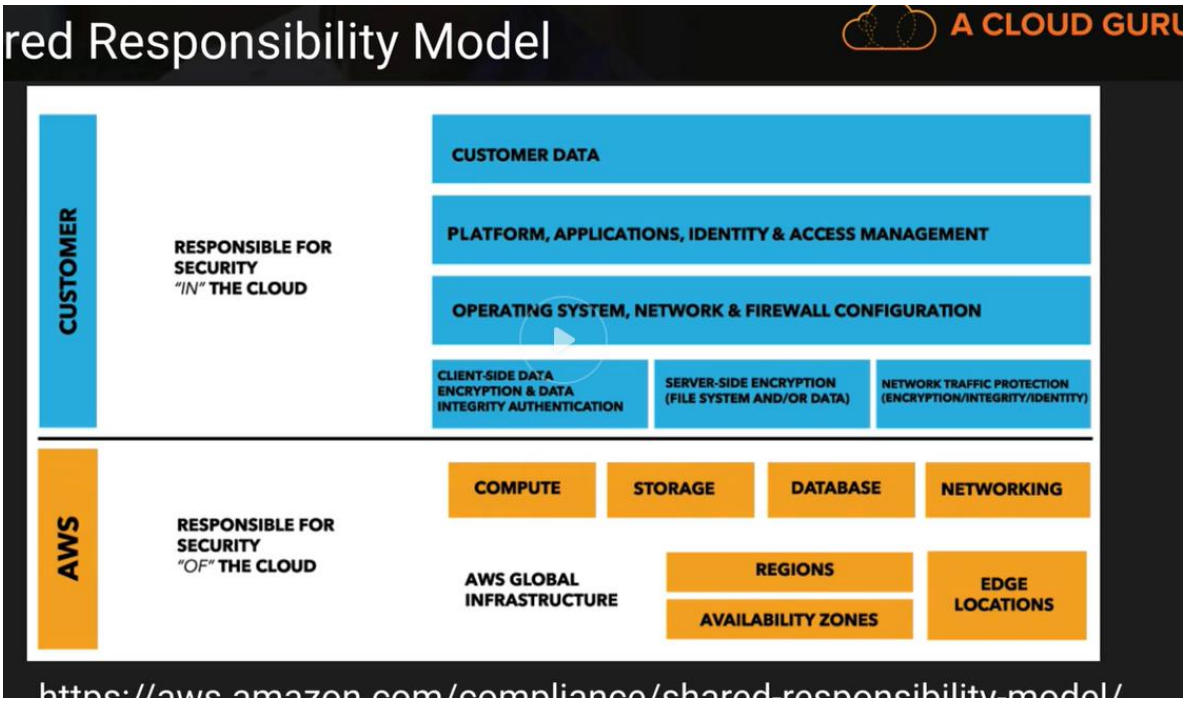
- "An Overview of the AWS Cloud Adoption Framework", https://d1.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf.

Security

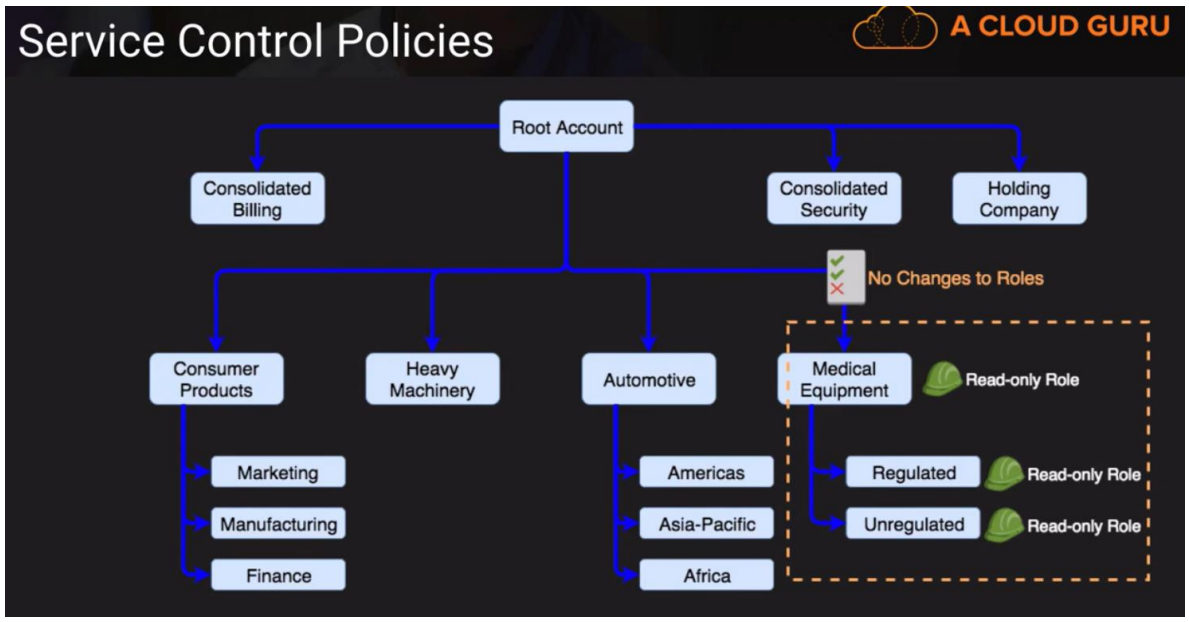
- NACLs are stateless and support DENY rules while SGs are stateful and have no DENY rules: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html

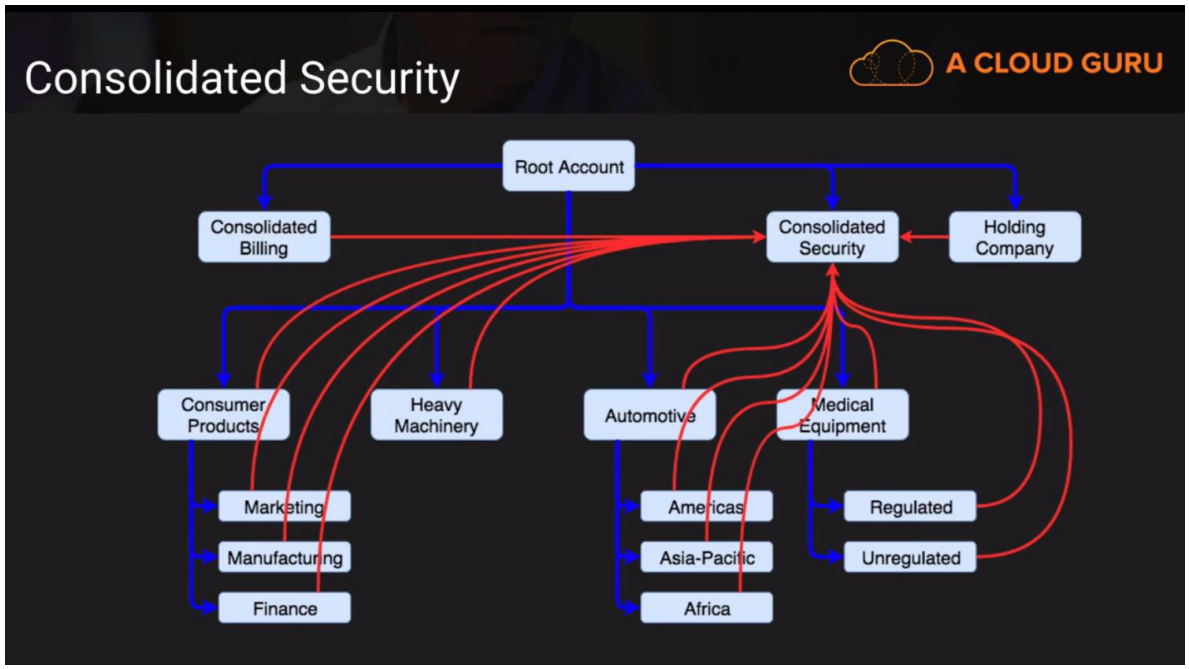


Shared responsibility model



- Security IN the cloud is the responsibility of the customer
- Security of THE cloud is the responsibility of AWS (Compute, storage, database, networking, etc.)





Additional reading

- "AWS Security Best Practices", https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

Well-Architected Framework

Additional reading

- "AWS Well-Architected Framework", https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf