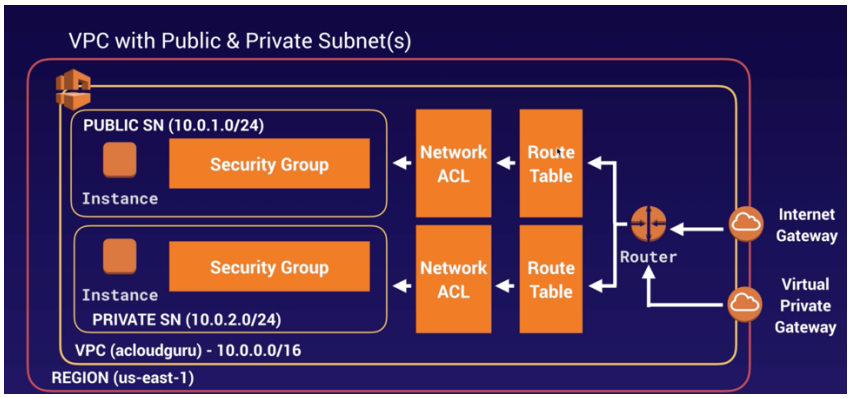
What is a VPC??

Think of a VPC as a virtual data centre in the cloud.

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

You can easily customize the network configuration for your Amazon Virtual Private Cloud. For example, you can create a public-facing subnet for your webservers that has access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

What are we Building today??

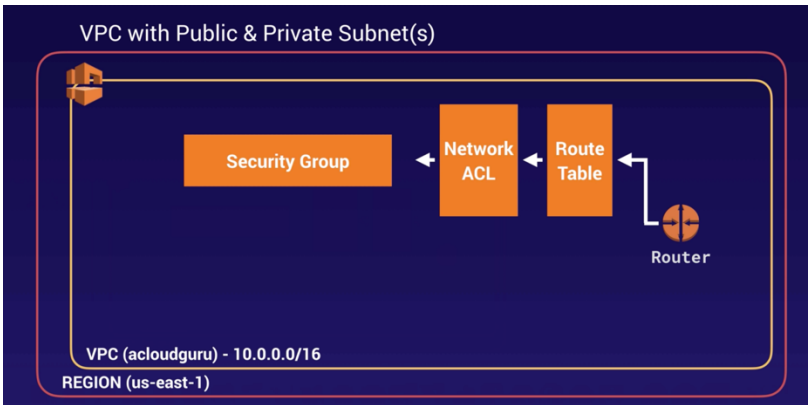


Important Things to remember:

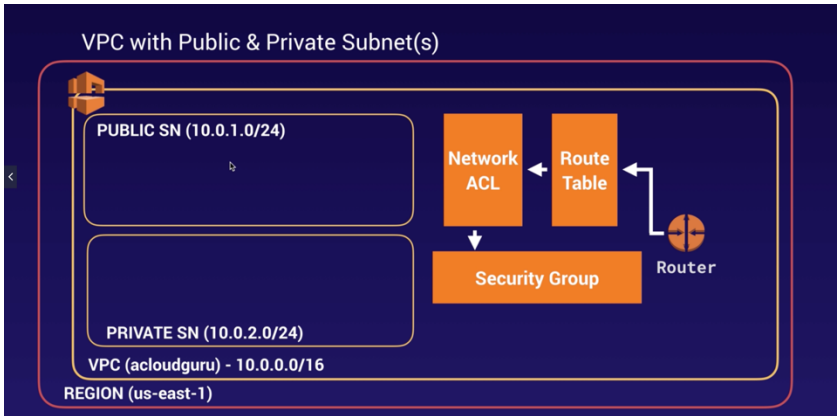
- Largest CIDR block for creating a VPC is /16 (2^16 = 65536 IP addresses)
- Smallest CIDR block for creating a VPC is /28 (2^4 = 16 IP addresses)
- Private IP address ranges: (Link to play with CIDRs: https://cidr.xyz/)
    1. 10.0.0.0 - 10.255.255.255 (10.0.0.0 / 8 prefix).
    2. 172.16.0.0 – 172.31.255.255 (172.16.0.0 / 12 prefix)
    3. 192.168.0.0 – 192.168.255.255 (192.168.0.0 /16 prefix)
- 1 subnet is 1 Availability zone.

Practical Demo:

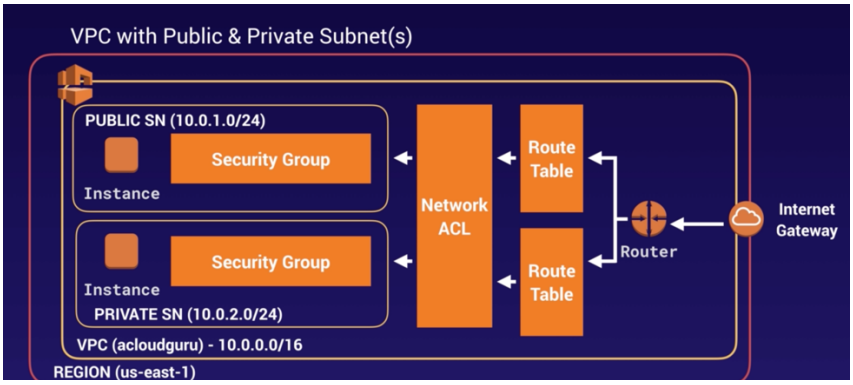
1) Create a VPC in the console by specifying the CIDR range mentioned above.



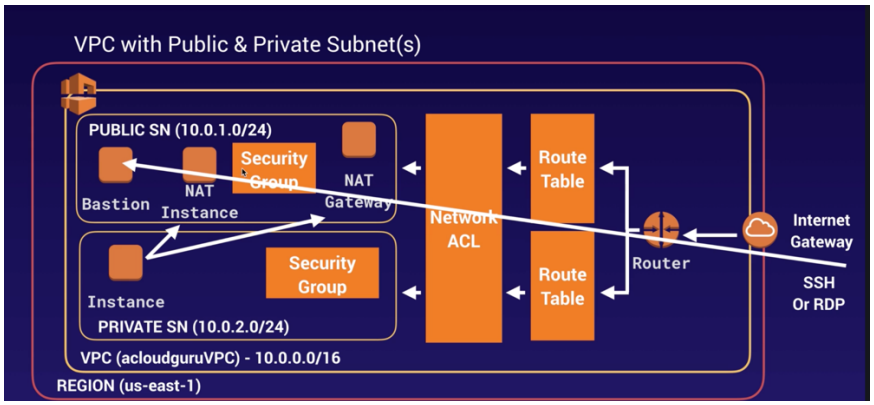
2) Create two subnets ---> Public and private subnets (10.0.1.0/24 and 10.0.2.0/24)
3) Enable auto assign public ip's for the public subnet.



4) Add an internet gateway and attach it to the VPC. NOTE: Only 1 internet gateway per VPC.
5) Since all the subnets are associated with the main route table adding IG will make subnets public so we can create another route table for public subnet.
6) Configure the public route table to add the internet gateway.
7) Create corresponding EC2 instances/Security groups in the public and private subnet.



8) Test the connections. How to SSH securely into private subnet from outside world and install software updates.

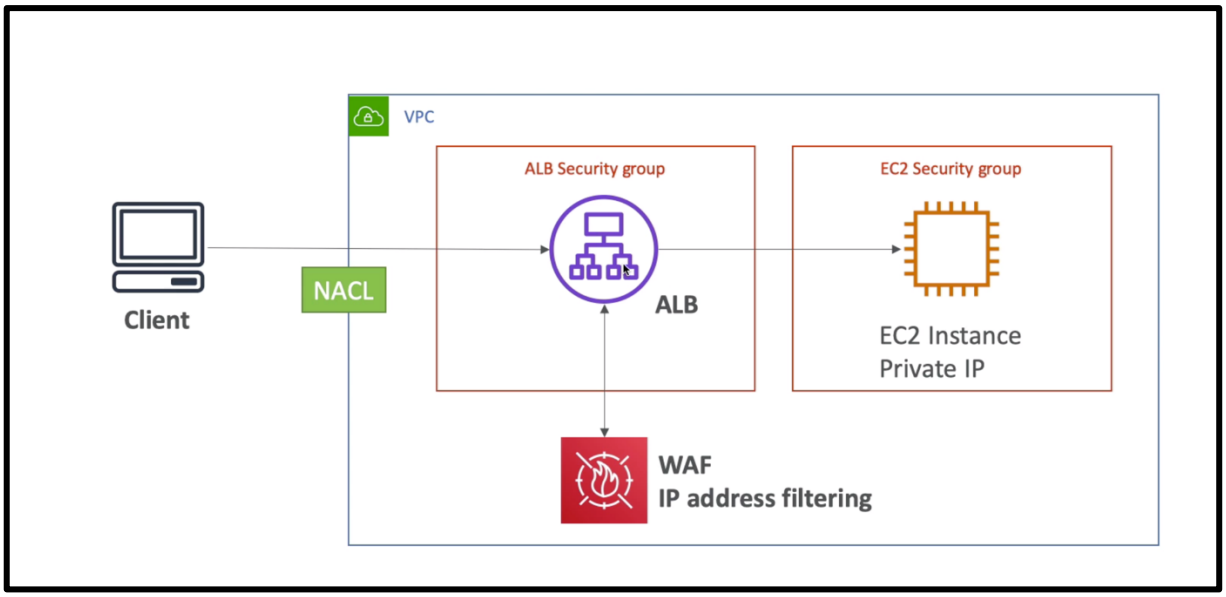


How to install the updates for the Private subnet instances / DB server??

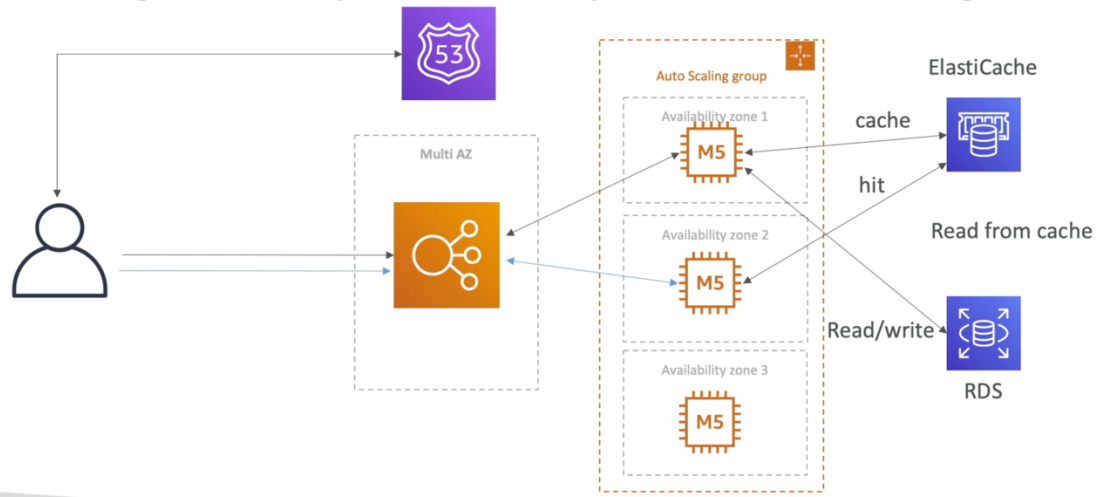
- Option1: Nat Instances ---> Not recommended. Not a managed service we need to setup high availability, monitor, configuration changes, etc.…
- Option2: Nat Gateway ----> Recommended, Managed service, highly available.

9) Add the corresponding routes in the private Route table. Ensure to disable source and destination checks for the Nat instance.
10) Overview on NACL.

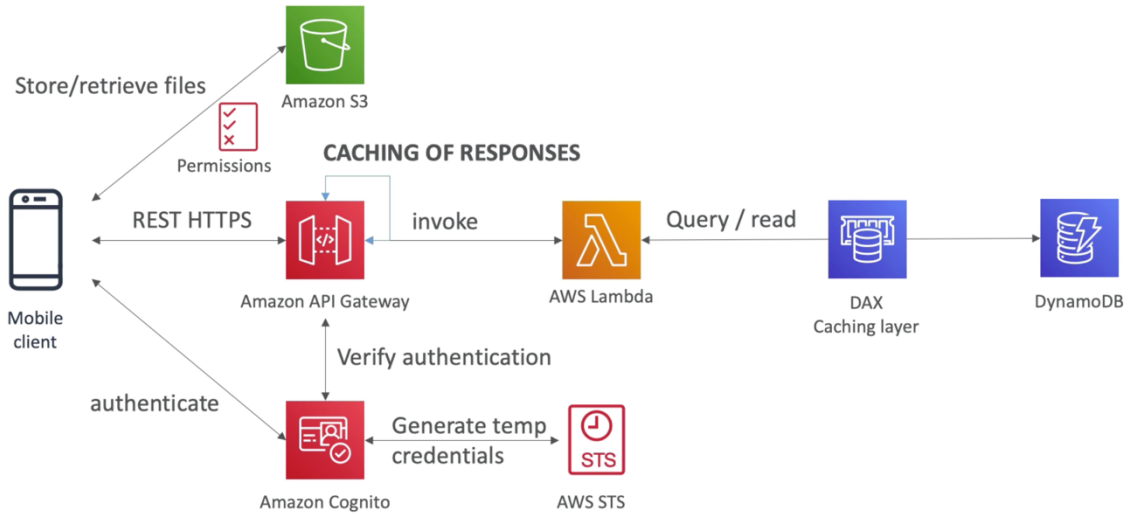
COMMON Architectures:



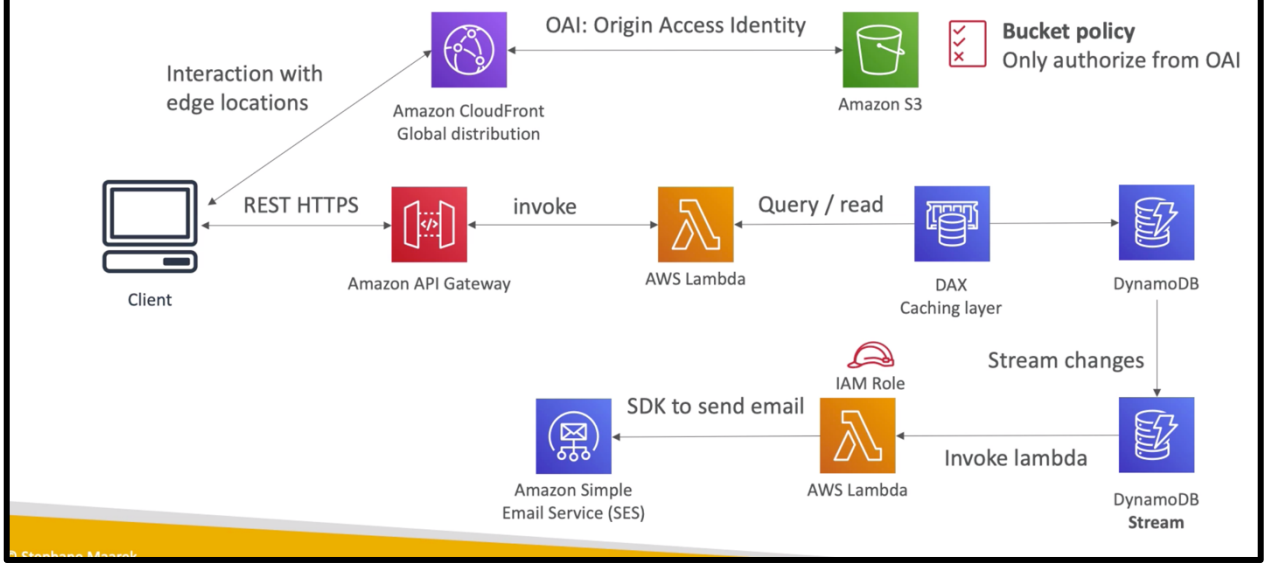
Stateful Web App: MyClothes.com
Scaling Reads (Alternative) – Write Through



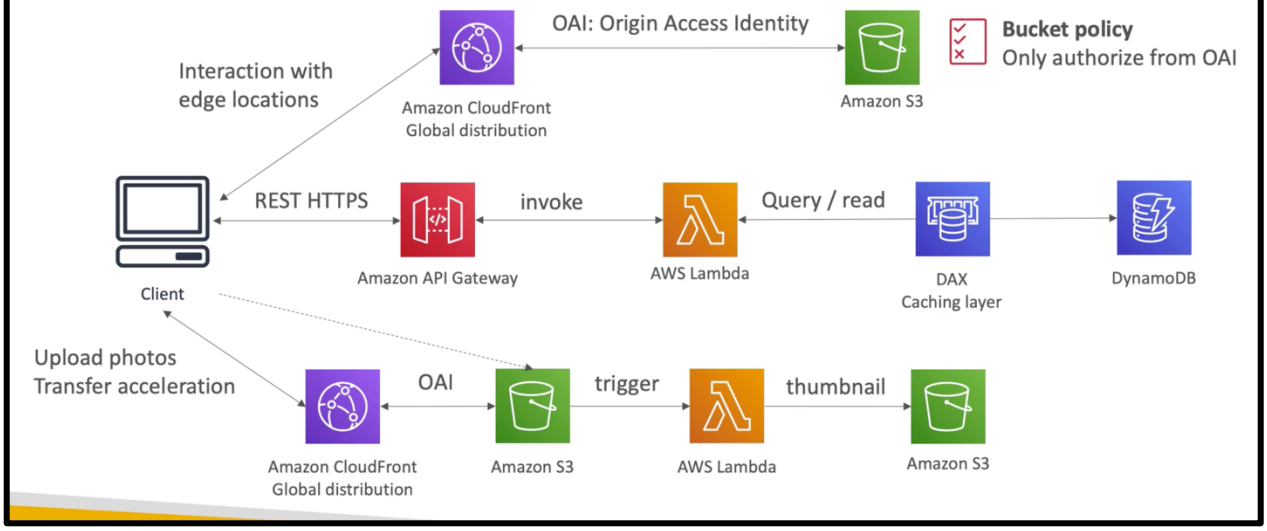
Mobile app: caching at the API Gateway



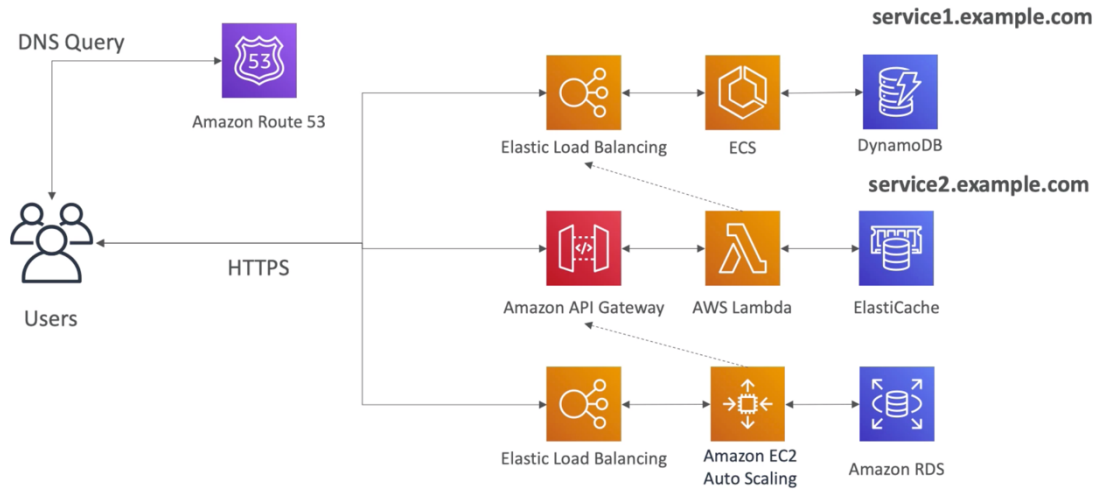
User Welcome email flow



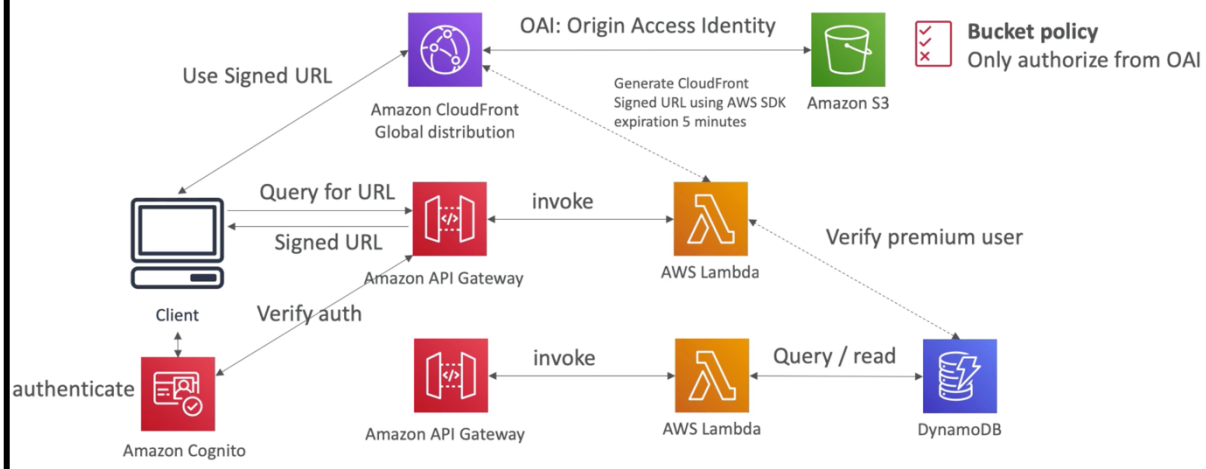
Thumbnail Generation flow

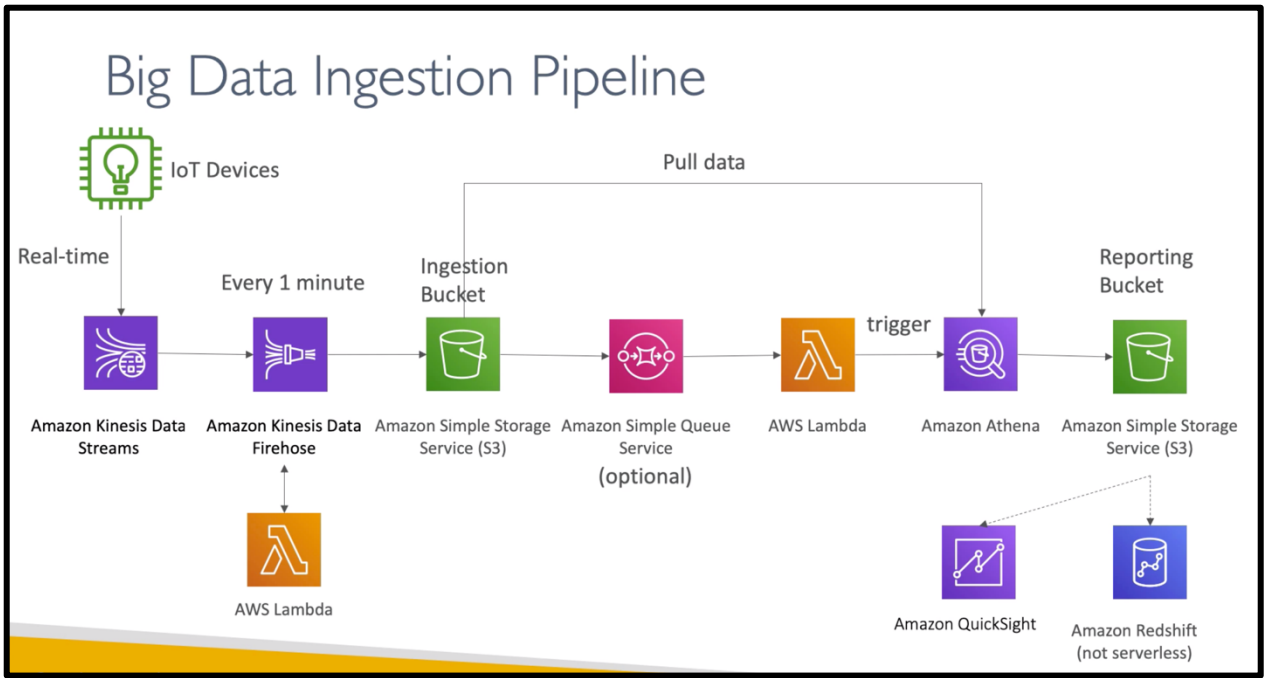


Micro Services Environment



Distribute Content only to premium users




Big Data Ingestion Pipeline
IoT Devices
Pull data
Real-time
Every 1 minute
Ingestion Bucket
Reporting Bucket
trigger
Amazon Kinesis Data Streams
Amazon Kinesis Data Firehose
Amazon Simple Storage Service (S3)
Amazon Simple Queue Service
(optional)
AWS Lambda
Amazon Athena
Amazon Simple Storage Service (S3)
AWS Lambda
Amazon QuickSight
Amazon Redshift
(not serverless)