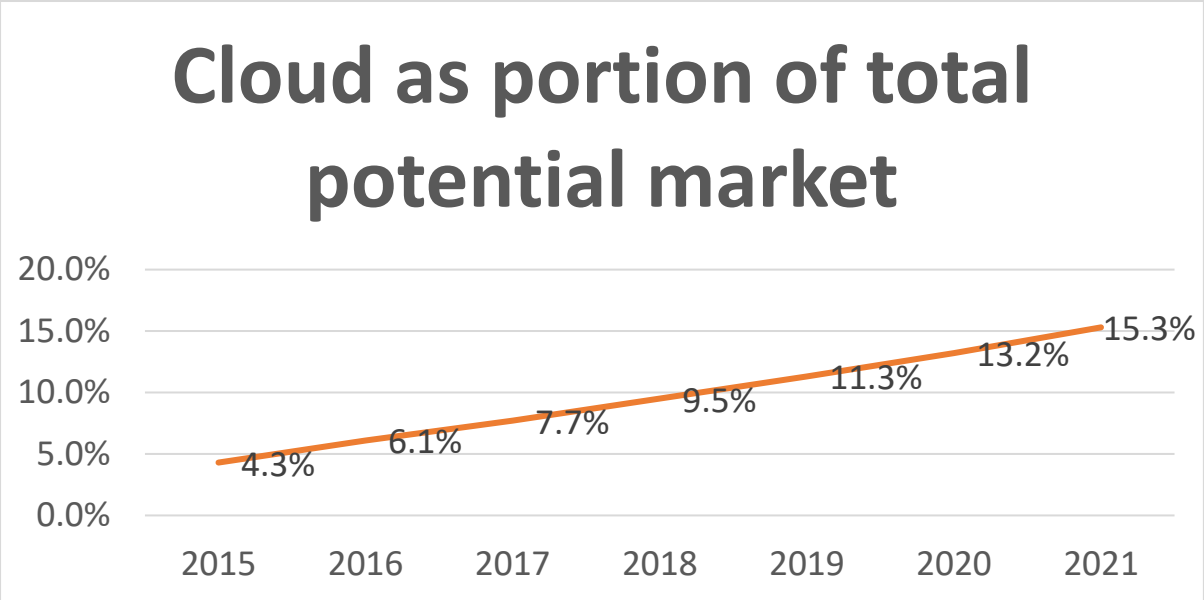
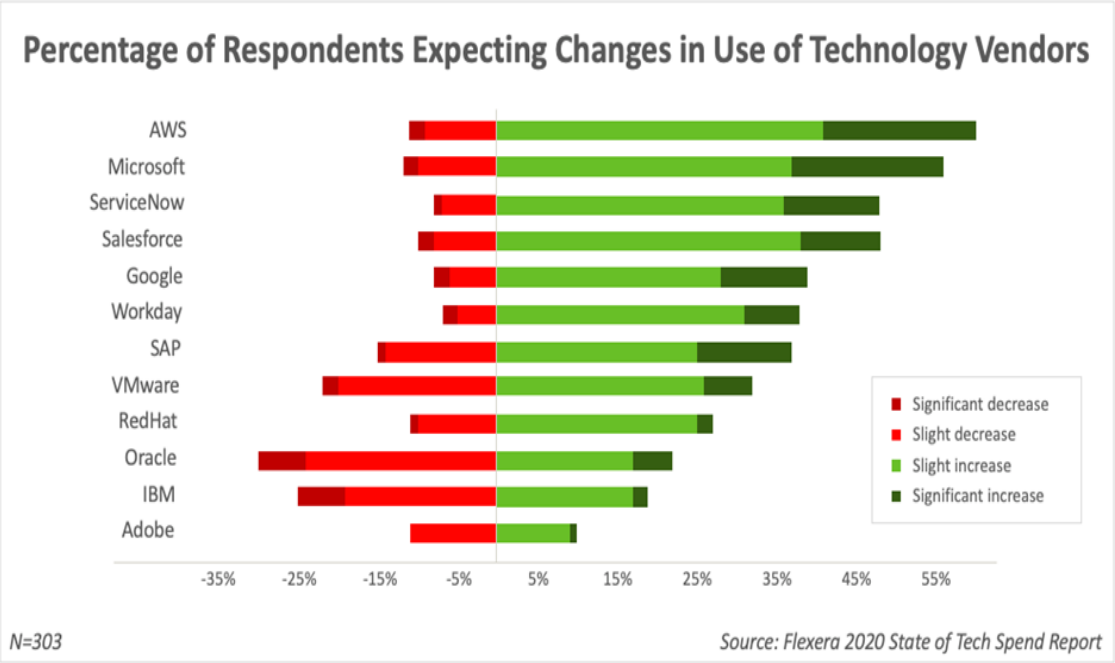
Brief History

- 2003 – Chris pinkham and Benjamin Black present a paper on what Amazon's own internal infrastructure should look like. They suggested selling it as a service and prepared a business case.
- SQS officially launched in 2004
- AWS officially launched in 2006
- 2007 – over 180,000 developers on the platform
- 2010 all of amazon.com moved over to AWS
- 2012 – first re-invent conference
- 2013 – Certifications Launched
- 2017 – AWS re-invent releases a host of Artificial Intelligent services
- 2018 – AWS launch ML Specialty Certs
- 2019 – New AWS Deep Learning containers, AWS IOT Device Tester and more
- 2020 - Amazon Connect supports speaking styles with neural Text-to-Speech voices, New classroom course: AWS Cloud Financial Management for Builders

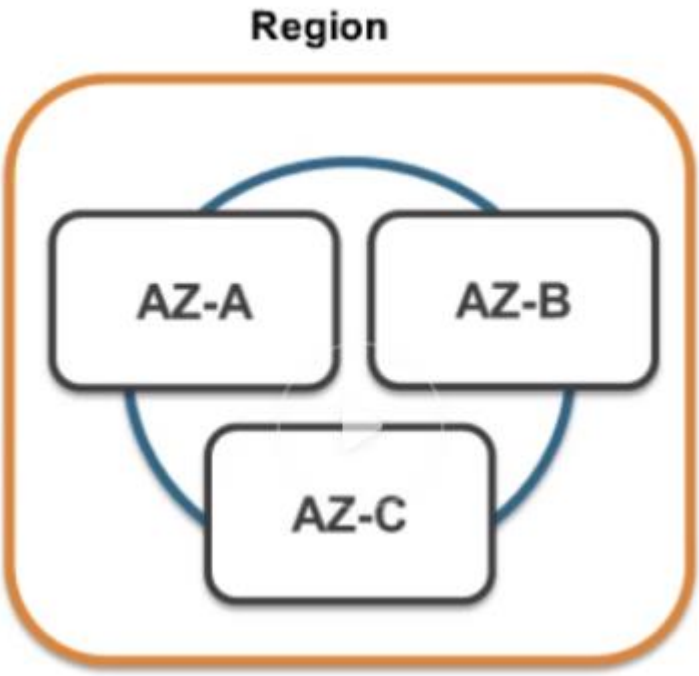
Cloud Spend As Predicted By Goldman Sachs





AWS Global Infrastructure

- 19 Regions & 57 Availability Zone – December 2018
- 22 Regions & 69 AZ's
- Availability Zone is a Data Center(is a building filled with servers)
- A Region is a geographical area (Physical Location).
- Each Region consists of 2 (or more) Availability Zones.



US East (Northern Virginia) Region
EC2 Availability Zones: 6
Launched 2006

US East (Ohio) Region
EC2 Availability Zones: 3
Launched 2016

US West (Oregon) Region
EC2 Availability Zones: 3
Launched 2011

US West (Northern California) Region
EC2 Availability Zones: 3*
Launched 2009

GovCloud (US-West) Region
EC2 Availability Zones: 3
Launched 2011

GovCloud (US-East) Region
EC2 Availability Zones: 3
Launched 2018

Canada (Central) Region
EC2 Availability Zones: 2
Launched 2016
Learn more at AWS Canada

Edge Locations:

- Edge Locations are endpoints for AWS which are used for caching content. Typically this consists of CloudFront, Amazon;s Content Delivery Network (CDN)
- There are many more Edge Locations than Regions.
- Currently there are over 150 Edge Locations.

Identity and Access Management (IAM)

- IAM allows you to manage users and their level of access to the AWS Console.
- IAM is universal.it does not apply to regions at this time.
- Features
    - Centralized control of your AWS Account
    - Shared access to your AWS account
    - Granular Permissions
    - Identity Federation (including Active Directory, Facebook, Linkedin etc)
    - Multifactor authentication
    - Provide Temporary access for users/devices and services where necessary
    - Allows you to setup your own password rotation policy

- Integrates with many different AWS services
- Supports PCI DSS Compliance

Key Terminology For IAM

Users

End users such as people, employees of an organization etc.

Groups

A collection of users. Each user in the group will inherit the permissions of the group

-

Policies

Policies are made up of documents, called policy documents. These documents are in a format called JSON and they give permissions as to what a user/Group/Role is able to do.

Roles

You create roles and then assign them to AWS Resources.

- The root account is simply the account created when first setup your AWS account.it has complete Admin access.
- New users have No permissions when first created.
- New Users are assigned Access Key ID & Secret Access Keys when first created. You can use this to access AWS via the APIs and Command Line

- You only get to view these once. If you loose them, you have to regenerate them. So save them in a secure location.
- You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources.
- For example, you might want to grant users in your AWS account access to resources they don't usually have, or grant users in one AWS account access to resources in another account.