

Cloud Computing

Sunday, March 6, 2022 10:38 AM

Computer - EC2, Lambda
Networking - VPC, Direct Connect
Storage - S3, EBS
Analytics - Athena, Redshift
Dev - Cloud9, CodeCommit
Security - IAM, Macie
DBs - RDS, DynamoDB

Usage - On Demand; Pay as you go

6 Advantages of Cloud Computing

1. Go Global In minutes
2. Stop spending money running and maintaining data centers
3. Benefit from massive economies of scale
4. Increase speed, agility
5. Stop guessing capacity
6. Capital expense to variable expense
 - a. Capital expenses (CapEx) = **upfront** purchases toward fixed assets
 - b. Operating expenses (OpEx) = funds used to run **day-to-day** operations

High Availability - operate continuously without failure

Elasticity - no need to plan ahead or plan capacity; provision what you need; grow and shrink based on demand

Agility - increased speed, innovate faster

Durability - long-term data protection; data will remain intact

Cloud Computing Models

1. IaaS - building blocks of IT; web hosting
2. SaaS - Complete App; personal email accessed through web
3. PaaS - For Devs; develop software without worrying infrastructure; storefront website

Cloud Deployment Models

1. Private Cloud - on-prem; internal data center; no advantages of cloud computing
2. Public Cloud - AWS; no physical hardware; cloud computing
3. Hybrid Cloud - sensitive data locally; web app on AWS; benefits of both

AWS Global Infrastructure

Sunday, March 6, 2022 10:51 AM

Regions - **geographically** isolated locations

- **2 or more AZs**
- Fully independent
- Resource specific and service specific

Availability Zones - one or more physically separated data centers, each with redundant power, networking, and connectivity, separate facilities

- Separated
- **Low-latency connections**
- **Fault tolerant**
- **High availability**

Edge Locations - **cache** content for **fast delivery** to users

AWS Account

Sunday, March 6, 2022 10:55 AM

AWS Management Console - access AWS account and manage apps running in account via web browser

- New to cloud
- Non-tech roles
- Tech roles
- Easy to use and search

Root user- made with every AWS account

- Make sure to MFA
- Certain things only root can do

AWS CLI - access AWS account through terminal

- Devs

Programmatic Access - provides access to your AWS resources through an app or a tool like CLI

1. CLI
2. App Code
 - a. Using SDKs and programmatic calls
3. SDKs

Compute Services: EC2

Sunday, March 6, 2022 11:28 AM

Elastic Cloud Compute EC2 - allows you to rent and manage virtual servers in cloud

- Elastic compute power
- Virtual servers in cloud
 - a. Provision at click of button
 - b. Preconfigured AMI - Amazon Machine Image
 - c. Deploy apps directly to EC2
 - d. Receive 750 compute hours/mo. On free tier plan
- Real world?
 - Deploy a Database
 - Deploy a web app
 - Deploy to multiple AZ's to make app highly-available
- Methods to access EC2
 - AWS management console
 - EC2 Instance Connect (EIC)
 - Use IAM policies to control SSH access to your instances, removing need to manage SSH keys
 - SSH - Secure Shell - establish secure connection to instance from local device
 - AWS Systems Manager - manage your EC2 instances via web browser or CLI
 - Most common way to connect Linux EC2 instances is via SSH
 - Generate Key pair
 - ◻ Key pair - consists of private and public key
 - ◆ Proves identity when connecting to EC2
 - Connect via SSH
 - ◻ User --> SSH Client on Laptop (use private key) --> EC2 Instance (use public key)

EC2 Pricing Options

- On-Demand
 - Fixed price billed down to the second based on instance type. No contract, pay for what you use
 - Use cases:
 1. Care about low cost without upfront payment or long-term commitment
 2. Your apps have unpredictable workloads that can't be interrupted
 3. Apps under development
 4. Workloads < 1 year
- Spot
 - Use unused capacity. Request fulfilled only if capacity available
 - Cheapest option
 - Use cases:
 1. Not concerned about start or stop
 2. Workloads can be interrupted
 3. App is only feasible at very low compute prices
 - Fun facts:
 - Save up to 90% off on-demand
 - Pay spot price that is in effect at beginning of each hour
- Reserved Instances
 - Commit to a specific instance type 1 or 3 years in a particular region
 - Use cases:
 1. App has steady state usage, and can commit to 1 or 3 years
 2. Pay money upfront in order to receive a discount on On-Demand prices
 3. App requires capacity reservation
 - Fun facts:

- 75% off on-demand
- Sign contract
- Reserve capacity in availability zone for any duration
- All upfront, partial upfront, no upfront
- Convertible type 54% off
- Dedicated Hosts
 - Physical server dedicated to running your instances
 - Use cases:
 1. Want to bring your own ser-bound software license from vendors like Microsoft, Oracle
 2. Regulatory or corporate compliance reqs around tenancy model
 - Fun Facts:
 - 70% off
 - Bring existing per-socket, per-core, per-VM software licenses
 - No multi-tenancy - server not shared with other customers
 - Dedicated host is a physical server, dedicated instance - runs on the host
- Savings Plans
 - Commit to compute usage measured per hour for 1 or 3 years
 - Use cases:
 - Want to lower your bills across multiple compute services
 - Flexibility to change compute services, instance types, OS, regions
 - Fun facts:
 - 72% off on-demand
 - Not making commitment to dedicated, just want compute usage
 - Savings shared across compute services i.e. EC2, Fargate, Lambda
 - No capacity reservation

EC2 instances offer load balancing and Auto Scaling

1. ELB auto distributes your incoming app traffic across multiple EC2 instances
 - a. Classic Load Balancer, Application Load Balancer, Gateway Load Balancer, Network Load Balancer
2. Auto Scaling adds or replaces EC2 instances auto across AZs, based on need and changing demand
 - **Auto Scaling** reduces the impact of system failures and **improves the availability of your applications.**
 - **HORIZONTAL SCALING OR SCALING OUT**
 - Do not confuse horizontal scaling with vertical scaling (or scaling up), which upgrades an EC2 instance by adding more power (CPU, RAM) to an existing serve

Compute Service: Lambda

Sunday, March 6, 2022 1:41 PM

AWS Lambda - serverless compute that lets you run code without managing servers

- You author app code, called **functions**, using many popular languages
- **Scales automatically**
- **Serverless**
- **Real world?**
 - Real-time file processing
 - Sending email notifications
 - Backend business logic
- **Features**
 1. Supports Java, Go, PowerShell, Node, C#, Python, Ruby
 2. You author code using your favorite development environment or via the console
 3. Lambda can execute your code in response to events
 4. 15-minute timeout
- **Pricing Model:**
 1. Compute time
 - i. Pay only for the time your code is running
 2. Request count
 3. Always free
 - i. 1 million free requests/month even after Free tier expires

Exploring Compute Services: Additional Compute Services

Sunday, March 6, 2022 1:50 PM

AWS Fargate - Serverless compute engine for containers

- Manage containers i.e. Docker
- Scales automatically
- Serverless

Amazon Lightsail - quickly launch all resources you need for small projects

- Deploy preconfigured apps i.e. WordPress with a click
- Simple screens
- Includes virtual machine, SSD-based storage, data transfer, DNS management, static IP
- Low monthly free, as low as \$3.50

AWS Outposts - run cloud services in your internal data center

- Support workloads that need to remain on-prem due to latency or data sovereignty needs
- AWS delivers and installs servers in your internal data center
- Hybrid
- Access to cloud services and APIs to develop apps on-prem

AWS Batch - process large workloads into smaller chunks or batches

- Run hundreds, thousands of smaller batch processing jobs
- Dynamically provisions instances based on volume

Leveraging Storage Services: S3

Sunday, March 6, 2022 2:02 PM







Amazon Simple Storage Service (Amazon S3) - object storage service for cloud that is highly-available

- Objects stored in buckets
- Unlimited storage
- Public or private
- Upload objects via console, CLI, programmatically from within code using SDKs
 - Set security at the bucket level or individual object level using access control lists, bucket policies, or access point policies
 - Enable versioning to create multiple versions
 - Use S3 access logs to track access to buckets
 - S3 is a regional services, name is globally unique

Data Accessibility

- Durability
 - 11 9's durability
 - Objects are never lost or compromised
- Availability
 - Access your data quickly when needed
 - S3 standard is 99.99% available

S3 Storage Classes

					
S3 Standard	S3 Intelligent-Tiering	S3 Standard-IA	S3 One Zone-IA	S3 Glacier	S3 Glacier Deep Archive
Frequent	Access frequency			Archive	
<ul style="list-style-type: none">• Active, frequently accessed data• Milliseconds access• ≥ 3 AZ• \$0.0210/GB	<ul style="list-style-type: none">• Data with changing access patterns• Milliseconds access• ≥ 3 AZ• \$0.0210 to \$0.0125/GB• Monitoring fee per object• Min storage duration	<ul style="list-style-type: none">• Infrequently accessed data• Milliseconds access• ≥ 3 AZ• \$0.0125/GB• Retrieval fee per GB• Min storage duration• Min object size	<ul style="list-style-type: none">• Re-creatable, less accessed data• Milliseconds access• 1 AZ• \$0.0100/GB• Retrieval fee per GB• Min storage duration• Min object size	<ul style="list-style-type: none">• Archive data• Select minutes or hours• ≥ 3 AZ• \$0.0040/GB• Retrieval fee per GB• Min storage duration	<ul style="list-style-type: none">• Long-term archive-data• Select hours• ≥ 3 AZ• \$0.00099/GB• Retrieval fee per GB• Min storage duration


S3 Outposts

- Provides object storage on-premises
- A single storage class
- Store data across multiple devices and servers

Recommended for:

- Data that needs to be kept local
- Demanding application performance needs

Amazon S3 Outposts



S3 In Real World

1. Static websites
 - a. Use CloudFront for distribution
2. Data Archive
 - a. Archive data infrequently accessed
3. Analytics System
 - a. Use with Redshift and Athena
4. Mobile apps
 - a. Mobile users upload files to S3 bucket

Additional Storage Services

Sunday, March 6, 2022 2:13 PM

Amazon Elastic Block Store (EBS) - storage device, or volume - can be attached or removed from EC2

- Data persists when instance is not running
- Tied to 1 AZ
- Tied to 1 instance in same AZ
- Recommended for:
 - Quickly accessible data
 - Running a DB on an instance
 - Long-term data storage

EC2 Instance Store - local storage physically attached to host computer and cannot be removed

- Physically attached
- Ephemeral or temporary - loss of storage when EC2 is stopped
- Faster with higher I/O speeds
- Recommended for:
 - Temporary storage needs
 - Data replicated across multiple instances

Amazon Elastic File System (EFS) - serverless network file system for sharing files

- Supports linux only
- More expensive than EBS
- Accessible across different AZ's in same region
- Recommended for:
 - Main directories for business-critical apps
 - Lift and shift existing enterprise apps

Storage Gateway - hybrid storage service

- Connect on-prem and cloud data
- Supports hybrid model
- Recommended for:
 - Moving backups to cloud
 - Reducing costs for hybrid cloud storage
 - Low latency access to data

AWS Backup - manage data backups across multiple AWS Services

- Integrates w/ EC2, EBS, EFS, and more
- Create backup plan that includes frequency and retention

Understanding Content Delivery Services

Sunday, March 6, 2022 2:23 PM

What is a CDN?

- Mechanism to deliver content quickly and efficiently based on geographical location
- Low latency

Amazon CloudFront - CDN that delivers data and apps globally with low latency

- Content available globally or restrict it based on location
- Speeds up delivery of static and dynamic web content
- Uses edge locations to cache content
- Real world?
 - S3 static websites
 - Prevent attacks
 - Can stop DDoS and certain web attacks
 - IP address blocking
 - Geo-restriction to prevent users accessing content in certain countries

Amazon Global Accelerator - sends your users through the AWS global network when accessing your content, speeding up delivery

- Improves latency and availability of single-region apps
- Sends traffic through AWS global network
- 60% performance boost
- Auto re-routes traffic to health available regional endpoints

Amazon S3 Transfer Accelerator - improves content uploads and downloads to and from s3 buckets over long distances

- Fast TRANSFER OF FILES OVER LONG DISTANCES
- Uses CloudFront's globally distributed edge locations
- Customers around world can upload to central bucket

Network Cloud Services

Tuesday, February 15, 2022 11:30 AM

Amazon Virtual Private Cloud (VPC)

VPC is a foundational service that allows you to create a secure private network in the AWS cloud where you launch your resources.



VPC

- Don't forget internet gateway allows traffic to the public internet and peering connects 2 VPC's together

DNS - Domain Name System - connects IP address to Domain name like acloud.guru

- Directs internet traffic by connecting domain names with web servers

Amazon Route 53 - DNS service that routes users to apps

- Highly available and scalable
- Domain name registration
- **Health checks** on AWS resources
- Supports **hybrid** cloud architectures

AWS Direct Connect - **dedicated physical** network connection from on-premises data center to AWS

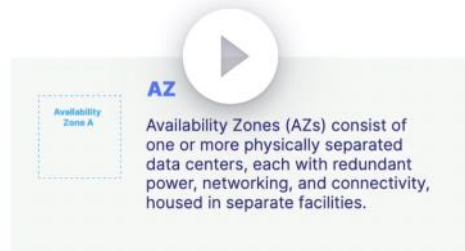
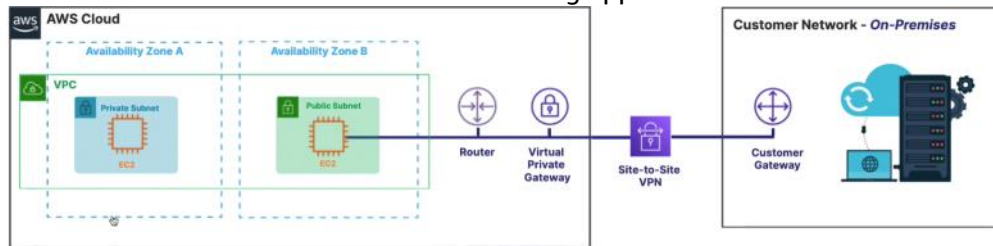
- Dedicated physical connection
- Connects on-premises data center to AWS
- *Data travels over private network*
- Hybrid model support
- Uses in real world:
 - o Large data sets
 - o Business critical data
 - o Hybrid models

Hybrid cloud is combo of public and private clouds

AWS VPN

- Site-to-site VPN creates a secure connection b/w your internal networks and your AWS VPCs
- Similar to Direct Connect, but *data travels over the public internet*
- Data auto encrypted
- Connects your on-premises data center to AWS
- Supports a hybrid environment
- Option is slightly cheaper than direct connect

Site-to-Site VPN in the real world makes moving apps to cloud easier.



- Virtual Private Gateway - VPN connector on the **AWS side**
- Customer Gateway - VPN connector on the **customer side**

API Gateway - allows you to build and manage APIs.

- Share data b/w systems
- Integrates with **AWS Lambda**
- Client <-> API Gateway <-> Lambda <-> RDS

Utilizing Databases

Tuesday, February 15, 2022 11:45 AM

Databases allow us to collect, store, retrieve, sort, graph, manipulate data

- Organized collection of various data
- Web, mobile, etc
- Access by querying it

RDS, Aurora, DynamoDB, DocumentDB, ElastiCache, Neptune

Amazon RDS (Relational Database Service)

- Easy to launch and manage relational databases
- Aurora, PostgreSQL, MySQL, MariaDB, Oracle, SQL Server
- High availability and fault tolerance using multi-AZ deployment option
- AWS manages with auto software patching, auto backups, operating system maintenance, etc.
- Read replicas -- increase performance and durability (read-only copies of database)

Amazon Aurora - Relational; supports MySQL and PostgreSQL

- 5x faster MySQL; 3x faster PostgreSQL
- Scales auto while providing durability and high availability
- Managed by RDS

DynamoDB - NoSQL key-value and document database

- Key-value
- Fully managed; serverless
- Non-relational
- Scales auto; fast performance

DocumentDB - fully managed; MongoDB

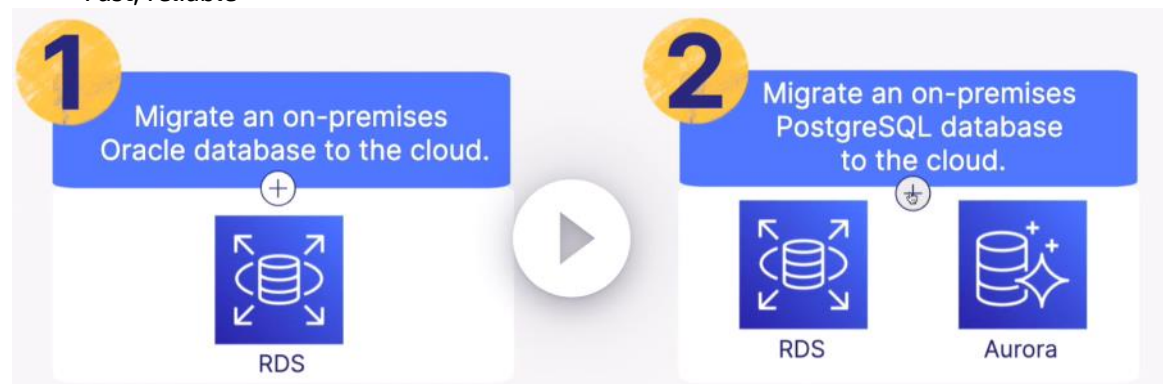
- Document database
- MongoDB
- Fully managed; serverless
- Non-relational

ElastiCache - fully managed in-memory datastore compatible with Redis or Memcached

- In-memory datastore
- Redis; Memcached
- Data can be lost b/c stored in-memory
- High performance; low latency

Neptune - fully managed graph DB; highly connected datasets

- Graph database
- Support highly-connected datasets like social media networks
- Fully managed; serverless
- Fast; reliable



3

Alleviate database load for data that is accessed often.



ElastiCache

4

Process large sets of user profiles and social interactions.



Neptune

5

NoSQL database fast enough to handle millions of requests per second.



DynamoDB

6

Operate MongoDB workloads at scale.



DocumentDB



Exploring Migration and Transfer Services

Sunday, March 6, 2022 2:35 PM

Database Migration Service (DMS) - migrate DBs to or within AWS

- Migrate on-prem DBs to AWS
- Continuous data replication
- Supports homogeneous and heterogeneous migrations
- Virtually no downtime
- Real world?
 - Oracle to Aurora MySQL
 - On-prem oracle to Aurora MySQL
 - Oracle to Oracle
 - On-prem oracle to oracle on EC2
 - RDS Oracle to Aurora MySQL
 - Migrate RDS oracle to Aurora MySQL

Server Migration Service (SMS) - migrate on-prem servers to AWS

- On-prem to AWS
- Server saved as a new AMI
- Use AMI to launch servers as EC2

Snow Family - allows you to transfer large amounts of on-prem data to AWS using physical device

- Snowcone
 - Smallest member
 - 8 terabytes
 - Offline shipping
 - Online w/ DataSync
- Snowball and Snowball Edge
 - Petabyte-scale
 - Transfer data in and out
 - Cheaper than internet transfer
 - Snowball Edge supports EC2 and Lambda
- Snowmobile
 - Multi-petabyte or exabyte scale
 - Data loaded to S3
 - Securely transported

DataSync - allows for online data transfer from on-prem to AWS storage services like S3 or EFS

- Migrates data from on-prem to AWS
- Copy data over Direct Connect or the internet
- Copy data between AWS storage services
- Replicate data cross-region or cross-account

Leveraging Analytics Services

Tuesday, February 15, 2022 3:38 PM

Data Warehouses - data storage solution that aggregates massive amounts of historical data from disparate sources

- Support querying, reporting, analytics; not used for transaction processing
 - o RDS is for transaction processing
- Redshift - scalable data warehouse solution
 - o **Data warehousing** solution
 - o Speed; efficiency
 - o Exabyte-scale data
 - o In the real world:
 - Data consolidation
 - Relational database that does not require real-time transaction processing (insert, update, delete)
 - o Analytics - act of querying or processing your data
 - Athena - query service for Amazon S3
 - Query service
 - Analyze **S3** data using **SQL**
 - Pay per query
 - Considered **serverless**
 - Glue - prepares your data for analytics
 - Extract, Transform, Load service (**ETL**)
 - **Prepare** and **load** data
 - Helps you better understand your data
 - Kinesis - allows you to analyze data and video streams in **real-time**
 - Real time streaming data
 - Video, audio, application logs
 - Website clickstreams, IoT
 - Elastic MapReduce (EMR) - helps *process large amounts of data*
 - Process **big data**
 - Analyze data with **Hadoop**
 - Works with big data frameworks
 - Data Pipeline - helps you move data b/w **compute** and **storage** services running either on AWS or on-premises
 - Moves data at specific **intervals**
 - Moves data based on **conditions**
 - Sends **notifications** on success or failure
 - ◆ i.e. use data pipeline to move data from S3 to Redshift
 - QuickSight - helps you visualize your data
 - Interactive **dashboards**
 - **Embed** dashboards into your apps
 - Analytics in real world scenarios:
 - Search data in S3?
 - ◆ Athena
 - Log Analytics?
 - ◆ Kinesis

Leveraging Machine Learning Services

Tuesday, February 15, 2022 3:53 PM

Rekognition - allows you to automate image and video analysis.

- Image and video analysis
- Identify custom labels in images and videos
- Face and text detection in images and videos
 - o i.e. recognize pizza toppings, ensure food quality

Comprehend - **natural-language processing** service that finds **relationships** in text

- NLP
- Insights and relationships
- Analyzes text
- i.e. review social media posts

Polly - text into speech

- Mimics natural-sounding human speech
- Several voices and languages
- Create custom voice

SageMaker - helps you build, train and deploy machine learning models quickly

- Prepare data for models
- Train and deploy models
- Provides Deep Learning AMIs
- i.e. recommend movies and products to buy on e-commerce

Translate - language translation

- Real-time batch language translation
- Many languages
- Translates many content formats

Lex - helps you build conversational interfaces like **chatbots**.

- Recognize speech and understand language
- Build highly engaging chatbots
- Amazon Alexa

Understanding Developer Tools

Tuesday, February 15, 2022 4:50 PM

Cloud9 - allows you to **write code within an integrated development environment (IDE) from within your web browser.**

- Integrated development environment (IDE)
- **Write** and **debug** code
- Supports several popular languages
- Build **serverless** apps - cloud9 preconfigures the development environment with the needed SDKs and libraries. You can easily write code for your Lambda function directly in your web browser.

CodeCommit - source control system or private Git repos.

- Create repos to store code
- Commit, branch, merge code
- Collaborate with other software developers
- Manage source code – similar to github

CodeBuild – allows you to **build** and **test** your application source code.

- Compiles source code and **runs tests**
- Enables **continuous integration and delivery**
- Produces build artifacts ready to be deployed
- Run tests before deploying a new version of an application to production

CodeDeploy – manages the **deployment** of code to compute services in cloud or on-premises

- Deploys code to **EC2, Fargate, Lambda, and on-prem**
- Maintains application uptime
- Real world?
 - o Maintain application uptime when rolling out a new version
 - **Eliminates the downtime** of your app when deploying a new version due to its rolling deployments.

CodePipeline - **automates** the software release process.

- Quickly deliver new features and updates
- Integrates with **CodeBuild** to run builds and unit tests
- Integrates with **CodeCommit** to retrieve source code
- Integrates with **CodeDeploy** to deploy your changes
- Real World?
 - o Add **automation** to the building, testing, and deployment of your app
 - When combined with other dev tools, CodePipeline helps dev teams implement DevOps practices that *automate testing and movement of code into production.*

X-Ray - **debug** production apps

- Analyze and debug
- Map application components
- View requests end-to-end
- Real world?
 - o Trace calls to an RDS Database
 - Help you map requests made to your RDS DB from within your app. Track info about SQL queries generated and more.

CodeStar - helps devs **collaboratively work** on development projects

- Developers connect their development environment
- Integrates with **CodeCommit, CodeBuild and CodeDeploy**
- Contains issue tracking dashboard
- Real world?
 - o Manage the development pipeline
 - Integrate with CodeCommit, CodeBuild, CodeDeploy

Exploring Deployment and Infrastructure Management

Wednesday, February 16, 2022 12:57 PM

These services help you quickly stand up new apps, automate management of infrastructure, provide real-time visibility into system health

Infrastructure as Code (IaC)

- Allows you to write a script to provision AWS resources. The benefit is that you **provision resources** in a **reproducible manner** that saves time.

- o **JSON** Script
 - "MyBucket" : {
 "Type": "AWS::S3::Bucket"
 }
- o **YAML** Script
 - MyBucket:
 Type: AWS::S3::Bucket

CloudFormation - allows you to provision AWS resources using **Infrastructure as Code (IaC)**

- o Provides a repeatable process for provisioning resources
- o Works with most AWS resources
- o Create **templates** for the resources you want to implement
- o Real world?
 - Automate the infrastructure provisioning process for EC2 services
 - CloudFormation Template -> Stack created based on template

Elastic Beanstalk - **Compute** services that allows you to **deploy your web apps** and web services to AWS

- o Orchestration service that provisions resources
- o **Auto** handles the deployment
- o Monitors application health via a health dashboard
- o Not used to deploy apps on-prem
- o Real world?
 - Quickly deploy a scalable java-based web app to AWS
 - Deploys your Java code and handles **capacity provisioning, load balancing, and auto-scaling.**
 - Elastic Beanstalk even monitors the health of your app

OpsWorks - allows you to use **Chef** or **Puppet** to automate the configuration of your servers and **deploy** code

- o Deploy code and manage apps
- o Manage on-prem servers or EC2 instances in AWS cloud
- o Works with Chef and Puppet automation platforms
- o Real world?
 - Allows you to define software installation scripts and automate configuration for your application servers

Messaging Services and Use

Thursday, March 3, 2022 8:26 PM

SQS - Simple message queuing system that allows you build loosely-coupled systems

- FIFO - First in First Out

SNS - Simple Notification Service - allows you to send emails and text messages from your apps

- Pub/Sub service
- Plain text email
- Real world?
 - Send email when EC2 instance utilization > 80%
 - Works with CloudWatch Alarm

SES - Simple Email Service - SES is an email service that allows you to sent rich HTML emails

- Marketing, professional looking

Exploring Auditing, Monitoring, and Logging Services

Thursday, March 3, 2022 8:55 PM

Uses for auditing, monitoring, and logging services:

- Who signed in and made changes via AWS Mgmt. Console?
- Current load on this EC2 instance?
- Root cause of application error?
- Which execution path resulting in the error?

CloudWatch - collection of services that help you monitor and observe cloud resources

- Metrics, logs, events
- Detect anomalies in environment
- Alarms
- Visualize logs
- CloudWatch Alarms - high resolution alarms
 - Notification if EC2 instance goes into stopped state or usage goes above a certain utilization
- CloudWatch Logs - monitor application logs
- CloudWatch Metrics - visualize time-series data
- CloudWatch Events - trigger an event
 - Notification when root user API calls are detected in your account indicating root user activity.

CloudTrail - tracks **user activity** and **API calls** within your account

- Log and retain account activity
- Track activity through console, SDK, CLI
- Identify which user made changes
- Detect unusual activity in your account
 - You can troubleshoot events over the past 90 days using the CloudTrail event history log to find the specific time an event occurred on a per-Region basis. You can create a custom trail to extend past 90 days.
- Things you can track with CloudTrail:
 - Username
 - Event time and name
 - IP Address
 - Access key
 - Region
 - Error code

Exploring Additional Services

Thursday, March 3, 2022 9:13 PM

Amazon Workspaces - allows you to host virtual desktops cloud

- Virtualize windows, linux
- Work-from-home

Amazon Connect - cloud contact center

- Customer service functionality
- Improved productivity of help desk agents

Shared Responsibility Model

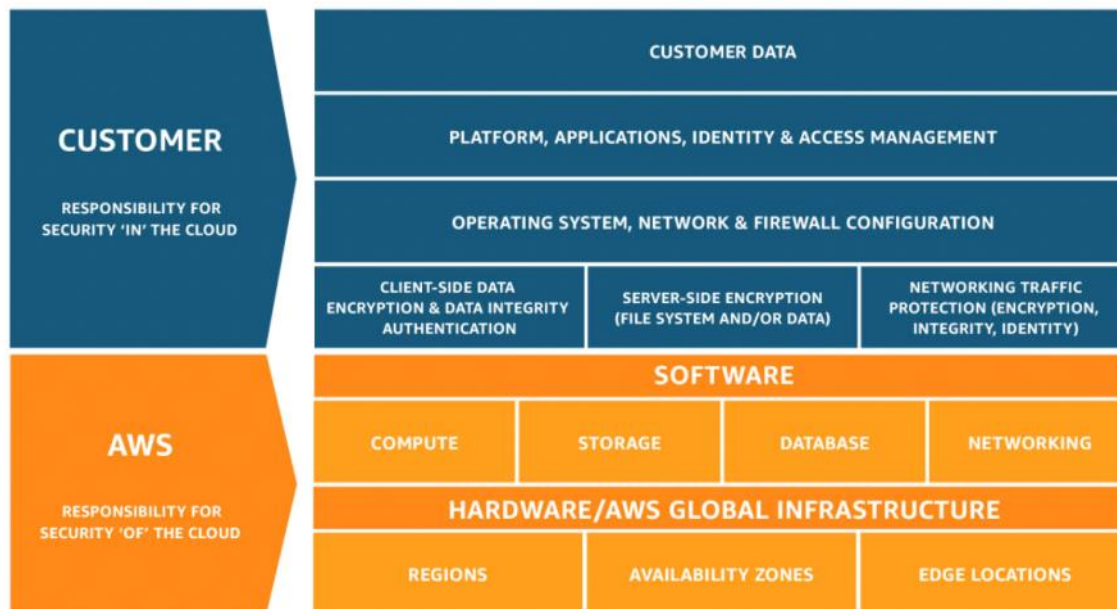
Thursday, February 17, 2022 2:18 PM

AWS Responsibility

- Security of the cloud
- AWS is responsible for protecting and securing their infrastructure
 - o Global infrastructure; regions, edge locations, AZs
 - o Building Security; AWS controls access to its data centers where your data resides
 - o Networking Components; generators, power supply, computer room A/C, fire systems, etc.
 - o Software; RDS, S3, ECS, Lambda, patching of host operating systems, data access endpoints

YOUR Responsibility

- Security in the cloud
- You are responsible for how the services are implemented and managing your app data
 - o App Data; app data and encryption options
 - o Security config; securing account, API calls, rotating credentials, restricting internet access from your VPCs, etc.
 - o Patching; guest OS incl. updates and security patches
 - o Identity and Access Management; You are responsible for app security and identity and access mgmt.
 - o Network Traffic; you are responsible for network traffic protection, which includes security group firewall config
 - o Installed Software; app code, installed software, etc. you must patch vulnerabilities often



Well-Architected Framework

Monday, February 21, 2022 4:25 PM

5 Pillars of Well-Architected Framework

- Operational Excellence
 - i.e. AWS CodeCommit version control - enable tracking of code changes and to version control CloudFormation templates
- Security
 - CloudTrail - central logging of all actions performed in your account
- Reliability
 - Multi-AZ deployment of RDS DBs
- Performance Efficiency
 - AWS Lambda run code, zero administration
- Cost Optimization
 - S3 Intelligent-Tiering

Understanding IAM Users

Monday, February 21, 2022 4:30 PM

IAM - Control access to your AWS services and resources

- Global service - free
- Identities - **who** can access your resources
 - o Root user, individ. Users, groups, roles
- Access - **what** resources they can access
 - o Policies, aws managed policies, customer managed policies, permissions boundaries
- Principle of Least Privilege
 - o Giving a user the min access required to get the job done
- Roles - define access permissions; temporarily assumed by an IAM user or service
- Policies - manage permissions for IAM users, groups and roles by creating a policy document in JSON and attaching it
- Best practices:
 - o Enable MFA for privileged users
 - Root and Administrative
 - o Strong passwords
 - o Create individual users instead of using root
 - o Use roles for EC2 instances
 - Use roles over long-term credentials i.e. access keys
- IAM Credential Report - lists all users in account and status of credentials
 - o Status of pw's, access keys, MFA
 - o Used for auditing, compliance

Exploring Application Security Services

Tuesday, February 22, 2022 8:54 AM

Firewall - prevent unauthorized access to your network by inspecting incoming and outgoing traffic against rules you've defined

Web Application Firewall (WAF) - protects web apps against common web attacks

- Protects apps against common attack patterns
- Protects against SQL injection
- Protects against cross-site scripting



- WAF can stand in front of CloudFront and Elastic Load Balancers for your EC2 instances

DDoS - Distributed Denial of Service

- Causes traffic jam on a website or app in attempt to crash it
 - Bots - attack requests
 - Overwhelms application and crashes
- AWS Shield - managed DDoS protection service
 - Always ON
 - FREE (*Shield Standard*)
 - Protects against common and freq. occurring attacks
 - *Shield Advanced* = paid service
 - Enhanced; 24/7 access to AWS experts
 - **CloudFront, Route 53, ELB, AWS Global Accelerator** support
 - Receive real-time notification of suspected DDoS incidents and 24/7 assistance for the attack
- Macie - helps you discover and protect sensitive data
 - Uses **Machine Learning**
 - Evaluates **S3** Environment
 - Uncovers **personally identifiable info (PII)**
 - C.C. #'s or S.S #'s

Exploring Additional Security Services

Thursday, March 3, 2022 10:23 PM

Config - **assess, audit, evaluate** configs of resources

- Track **config changes over time**
- Config history file to **S3**
- **Notifications** via **SNS** of every config change

GuardDuty - intelligent threat detection system that uncovers unauthorized behavior

- **Machine learning**
- Built-in detection: **EC2, S3, IAM**
- Reviews CloudTrail, VPC Flow Logs, DNS **Logs**
- Real world?
 - Detect **unusual API call events** commonly used by attackers

Inspector - works with **EC2 instances** to uncover and **report vulnerabilities**

- Agent installed on **EC2**
- **Reports** vulnerabilities
- **Checks** access from the internet, remote root login, vulnerable software versions, etc.
- Real world?
 - Identify unintended network access to an EC2 instance via detailed report of security findings

Artifact - on-demand access to AWS security and **compliance** reports

- Central repo for **compliance reports** from third-party
- SOC - Service Organization Controls
- PCI - Payment Card Industry

Cognito - control access to mobile and web apps

- Provides **authentication and authorization**
- User **sign-up and sign-in**
- Real world?
 - Social media sign-in to web app

Utilizing Data Encryption and Secrets Management Services

Friday, March 4, 2022 12:23 PM

Key Management Service (KMS) - allows you to **generate and store** encryption keys

- Key gen
- Store and control keys - **AWS manages** encryption keys
- **Automatically** enabled for some services
- Real world?
 - Encrypt Amazon EBS volumes

CloudHSM - **hardware security module** used to generate encryption keys

- **Dedicated hardware**
- Generate and manage **your own keys** - AWS does NOT have access
- Real world?
 - Meet corporate, contractual and regulatory compliance requirements for data security by using dedicated hardware in cloud

Secrets Manager - allows you to manage and retrieve **secrets** (passwords or keys)

- **Rotate, manage, retrieve**
- **Encrypt** at rest
- Integration w/ **RDS, Redshift, DocumentDB**
- **Real world?**
 - Secrets Manager allows you to retrieve database credentials with a call to Secrets Manager APIs, removing the need to hardcode sensitive information in plain text within your application code

Understanding AWS Pricing

Friday, March 4, 2022 12:32 PM

3 fundamental drivers of cost:

1. Compute
 - a. Hourly - start to termination
2. Storage
 - a. data
3. Outbound data transfer
 - a. Data in flight

Free Offer Types

1. 12 mo. Free
 - a. Initial sign-up with AWS
2. Always free
 - a. Non-expiration
3. Trials
 - a. Short-term

EC2 Pricing

- On-Demand
 - Hour or by second; **no pre-pay**
- Savings Plan
 - **Commit** hourly 1-or-3-year-term
- RIs
 - **Commit** 1-or-3; pay no matter if used or unused
- Spot Instances
 - **Spare** capacity
- Dedicated Hosts
 - **Physical** server

Lambda Pricing

- Number of Requests
- Code Execution Time
- 1,000,000 req. for free/mo.

S3 Pricing - pay for the storage you use

- Storage class
- Storage
 - # and size of objects
- Data Transfer
 - Transferred out
- Request and Data Retrieval

RDS Pricing

- Running clock hours
- Type of DB
- Storage
- Purchase type
- DB count
- API Requests
- Deployment type
- Data Transfer

TCO - Total Cost of Ownership - financial estimate that helps you understand direct and indirect costs of AWS

Application Discovery Service - **plan** migration projects to the AWS cloud

- planning
- **Estimate TCO**
- Used w/ **other Migration services**

Pricing Calculator - provides an estimate of AWS fees and charges i.e. **TCO**

AWS Price List API - allows you to query price of AWS Services

- Query with JSON or HTML
- Receive **price alerts** when prices change
- One way to determine costs of services

Ways to Reduce TCO w/ AWS?

1. Minimize capital expenditures
2. Utilize Ris
3. Right size your resources w/ provisioning

Understanding Billing Services

Friday, March 4, 2022 2:24 PM

These are tools to help you track your ongoing spending

Budgets - allows you to set custom budgets that **alert** you when your costs or usage **exceed** your budgeted amount

- Improve **planning & cost control**
- **Cost, usage, reservation** budgets
 - Cost- plan how much you want to spend
 - Usage - plan how much you want to use
 - Reservation - set RIs or savings plan utilization or coverage targets
- Budget **alerts**
- Real world?
 - Monitor free tier usage

Cost and Usage Report - most comprehensive set of cost usage and data

- Aggregate usage data daily, hourly, monthly
- Real world?
 - View most granular data

Cost Explorer - visualize and forecast costs and usage over time

- Visualize
- Past 12 mo.
- Forecast up to 3 mo.
- Real world?
 - Analyze EC2 usage over 7,30,60 days

Cost Allocation Tags - useful for tracking spend

- Allow labeling using a key and value pair
- Allow you to track costs via cost allocation report

Exploring Governance Services

Friday, March 4, 2022 2:41 PM

Organizations - centrally manage multiple AWS accounts under one umbrella

- Group multiple accounts
- Single payment
- Automate account creation
- Allocate resources and apply policies across accounts
 - SCP - service control policies
 - Used to enforce permissions that you want everyone in organization to follow
 - OU - Organization Units - grouping of AWS accounts that are similar
- Benefits?
 - Consolidated Billing
 - One bill
 - Cost Savings
 - Volume discounts for combined accounts usage
 - Account Governance
 - Automate way to create accounts or invite existing accounts
- Real world?
 - Organizations allows you to save money using Reserved Instance (RI) sharing. RI sharing allows all accounts in the organization to receive the hourly cost-benefit of RIs purchased by any other account. You can always turn off RI sharing using the master payer (or root) organization.

Control Tower - ensure you accounts conform to company-wide policies

- Set up new accounts using multi-account strategy
- Works directly w/ AWS Organizations
- Enforce best use of services in accounts
- Provides dashboard to manage accounts
- Real world?
 - Disallow public write access to all S3 buckets across accounts
 - Control Tower allows you to govern your multi-account environment by enabling cross-account security audits or preventing or detecting security issues through mandatory or optional guardrails.

System Manager - gives visibility and control over your AWS resources

- **Automate** operational **tasks** on resources
- **Group resources** and take **action**
- **Patch and run commands** on EC2 and RDS instances
- Real world?
 - Deploy OS and software patches automatically across large group of instances according to a schedule

Trusted Advisor - real-time guidance to help you provision resources following AWS best practices

- Best practices
- Recommendations?
 - Checks for unrestricted access for specific ports on EC2 instances * FREE
 - Checks S3 bucket permissions to determine if public access * FREE
 - Checks MFA on root * FREE
 - Checks IAM password policy * Enterprise or Business
 - Checks for RDS snapshots * FREE
 - Checks for usage of services over 80% over service limit * Enterprise or Business
 - Checks exposed access keys * Enterprise or Business
 - CloudFront delivery optimization * Enterprise or Business

License Manager - manage software licenses

- Manage on-prem AWS licenses
- Track licenses for Oracle, Microsoft, SAP, and more

Certificate Manager - provision and manage SSL/TLS certificates

- Public and private cert. for free
- Integrates: ELB, API Gateway, more

Utilizing Management Services

Monday, March 7, 2022 1:01 PM

Services that help you migrate to and build faster in the cloud

Managed Services - helps you efficiently operate your AWS infrastructure

- **Augments** your internal staff
- Provides ongoing management of your infrastructure
- Reduces operational risks and overhead
- Real world?
 - **Increase operational efficiency** by helping you develop app-specific health monitoring using CloudWatch

Professional Services - helps enterprise customers move to a cloud-based operating model

- Implements solutions
- Real world?
 - Help w/ evaluating an app for migration to the cloud
 - Quickly move **on-prem apps to cloud**

AWS Partner Network (APN) - global community of **approved partners** that offer software solutions and consulting services for AWS

- Offers **tech partners** that provide software solutions
- Provides **consulting partners** that offer professional services
- Find approved vendors w/ deep AWS expertise
- Real world?
 - If your team lacks tech expertise to build and deploy, APN could help you get up and running

Marketplace - **digital catalog** of prebuilt solutions you can purchase or license. You may also sell your own solutions to others via Marketplace

- Buy third-party software
- Sell solutions to AWS customers
- Search catalog for software listings and purchase w/ a click
- Real world?
 - Try out app w/ free-trial before making commitment

Personal Health Dashboard - alerts you to events that might impact your AWS environment

- Troubleshoot guidance
- Feedback tailored to your **specific** environment

Exploring Support Plans

Monday, March 7, 2022 1:09 PM

Support Plans

1. Basic
 - a. Included for free all AWS accounts
 - i. Account and billing
 - ii. Service limit increases
 - iii. Customer service
 - 1) 24/7 access via **email only**
2. Developer
 - a. \$29/mo. - testing and development
 - i. Account and billing
 - ii. Service limit increases
 - iii. Tech support
 - iv. **1 primary contact**
 - v. **Unlimited cases**
 - 1) Cloud Support Associate
 - a) Business-hours; access via email only
 - 2) Response times
 - a) General guidance < 24 hours
 - b) System impaired < 12 hours
3. Business
 - a. \$100/mo. - production workloads
 - i. Account and billing
 - ii. Service limit increases
 - iii. Tech support
 - iv. **Unlimited contacts**
 - v. **Unlimited cases**
 - vi. **Full set of Trusted Advisor Checks**
 - 1) Cloud Support Engineers
 - a) 24/7 via email, phone, chat
 - 2) Response Times
 - a) General guidance < 24 hours
 - b) System impaired < 12 hours
 - c) Production system impaired < 4 hours
 - d) Production system down < 1 hour
4. Enterprise
 - a. \$15,000/mo. - business or mission-critical production workloads
 - i. Account and billing
 - ii. Service limit increases
 - iii. Tech support
 - iv. **Unlimited contacts**
 - v. **Unlimited cases**
 - vi. **Technical Account Manager (TAM)**
 - vii. **Concierge Support Team**
 - viii. **Infrastructure Event Management**
 - ix. **Full set of Trusted Advisor Checks**
 - 1) Cloud Support Engineers
 - a) 24/7 via email, phone, chat
 - 2) Response Times
 - a) General guidance < 24 hours
 - b) System impaired < 12 hours

- c) Production system impaired < 4 hours
- d) Production system down < 1 hour
- e) **Business-critical system down** < 15 minutes

Support Case Types

- There are 3 types of support cases you can open w/ **AWS Support**
 - 1. **Account and billing**
 - i. Account-related and billing cases can be opened by all customers
 - 2. **Service limit increases**
 - i. Default service quote (or limit) increases can be opened by all customers
 - 3. **Technical support**
 - i. Tech support cases can only be opened by **Developer, Business, or Enterprise** plans
- AWS support does NOT allow cases for code dev, debugging custom software, or performing system admin tasks