aws Cloud Practitioner Notes

Please distribute or share this information with relevant individuals as needed.

Hussein Al Sayed

24-10-2024

Advantages and Benefits of Cloud Computing

- **1. Trade capital expense for variable expense**
  - No upfront-cost Instead of paying for data centers and servers
  - Pay On-Demand Pay only when you consume computing resources
- **2. Benefit from massive economies of scale**
  - Usage from hundreds of thousands of customers aggregated in the cloud.
  - You are sharing the cost with other customers to get unbeatable savings
- **3. Stop guessing capacity**
  - Eliminate guesswork about infrastructure capacity needs. Instead of paying for idle or underutilized servers, you can scale up or

down to meet the current need.

- **4. Increase speed and agility**
  - Launch resources within a few clicks in minutes instead of waiting days or weeks
- **5. Stop spending money on running and maintaining data centers**
  - Focus on your own customers, rather than on the heavy lifting of racking, stacking, and powering servers
- **6. Go global in minutes**
  - Deploy your app in multiple regions around the world with a few clicks.
  - Provide lower latency and a better experience for your customers at minimal cost.

https://docs.aws.amazon.com/whitepapers/latest/aws-overview/six-advantages-of-cloud-computing.html

Types of Cloud Computing

SaaS (Software as a Service) For Customers

- A completed product that is run and managed by the service provider

PaaS (Platform as a Service) For Developers

- Removes the need for your organization to manage the underlying infrastructure. Focus on the deployment and management of your applications

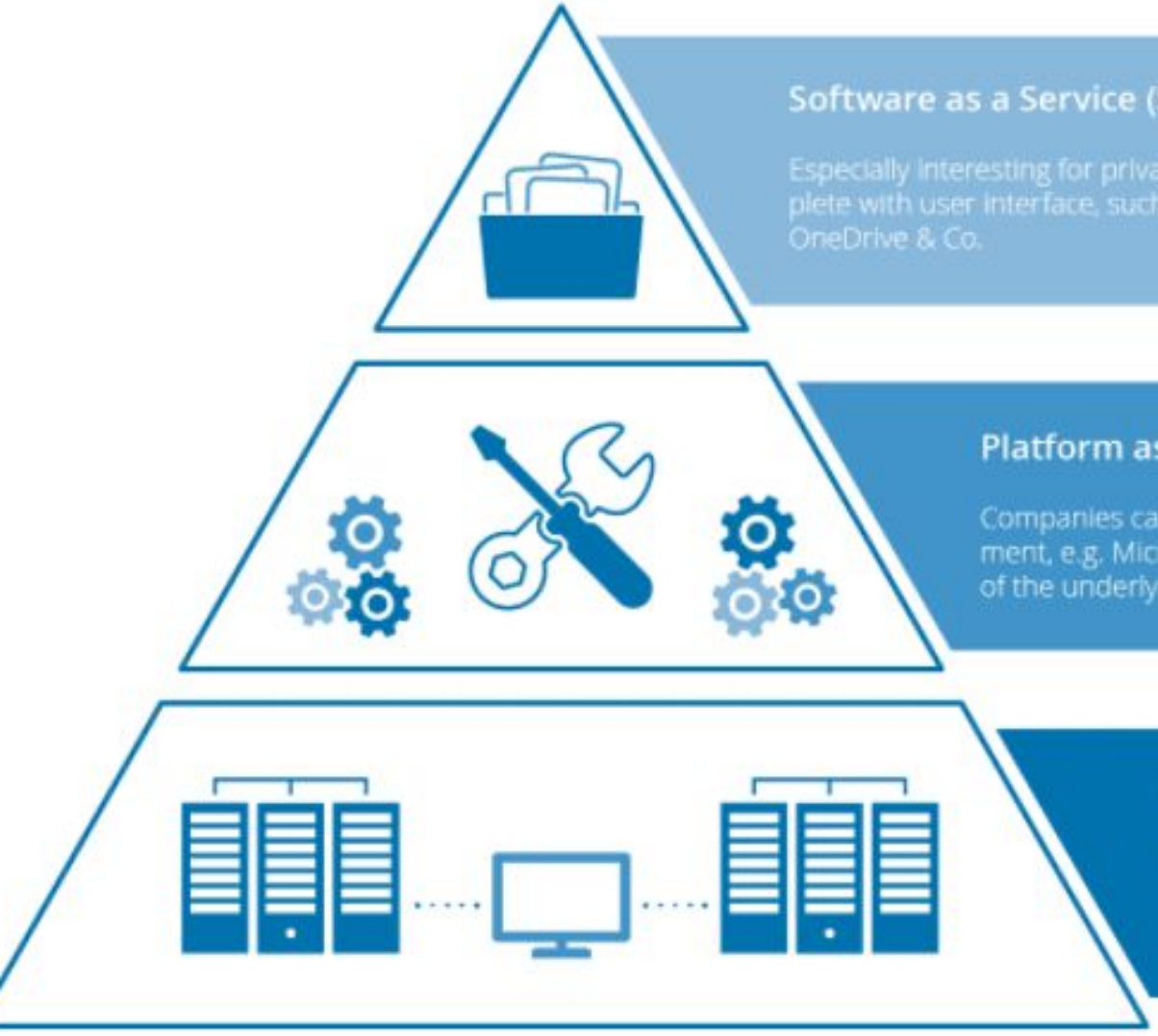
IaaS (Infrastructure as a Service) For Admins

- The basic building blocks for cloud IT. Provides access to networking features, computers and data storage

Cloud Computing Deployment Models

- Cloud Fully utilizing cloud computing
- Hybrid Using both Cloud and On-Premise
- On-Premise Deploying resources on-premises, using virtualization and resource management tools, is sometimes called “private Cloud”

https://aws.amazon.com/types-of-cloud-computing/



Software as a Service (SaaS)

Especially interesting for private users is cloud-based application software complete with user interface, such as Microsoft Office 365 or Dropbox, Google Drive, OneDrive & Co.

Platform as a Service (PaaS)

Companies can rent predefined platforms for software development, e.g. Microsoft Azure. The provider deals with administration of the underlying servers.

Infrastructure as a Service (IaaS)

Providers like Amazon Web Services (AWS) rent out storage and computing capacities on their servers.

AWS Global Infrastructure

- **Regions** physical location in the world with multiple Availability Zones
  - Every region is physically isolated from and independent of every other region in terms of location, power, water supply
  - Each region has at least 2 AZs (most have 3 AZs)
  - US-EAST is the largest region. Majority of new AWS Services become available here first
  - Not all services are available in all regions
  - US-EAST-1 is the region where you see all your billing information
- **Availability Zones (AZs)** one or more discrete data centers
  - An AZ is a datacenter owned and operated by AWS in which AWS services run
  - AZs are represented by a Region Code, followed by a letter identifier eg. us-east-1a
  - Multi-AZ is when you run instances across multiple AZs. If an AZ goes down you can route traffic to another Azs
  - AZs in the same region have sub 10ms latency between each other.
- **Edge Location** datacenter owned by a trusted partner of AWS
  - An Edge Location is a datacenter owned by a trusted partner of AWS which has a direct connection to the AWS network.
  - This allows for low latency no matter where the end user is geographically located.
  - Fast downloads from AWS with CloudFront and fast uploads to AWS with API Gateway
  - Points of Presences (PoPs) internet access points to the AWS network
  -

https://aws.amazon.com/about-aws/global-infrastructure/

Regions in Mexico, New Zealand, the Kingdom of Saudi Arabia, Thailand, Taiwan, and the AWS European Sovereign Cloud.

Security

The Shared Responsibility Model describes who is responsible for what:

- **Customer Responsibility "In" the Cloud**
  - Data you store on AWS services eg. turning on encryption,
  - Code you run on AWS Service
  - Configuration of Services eg. IAM roles, choosing OS on EC2 instance, configuring Security Groups.
- **AWS Responsibility "Of" the Cloud**
  - Underlying Physical Hardware
  - Global Infrastructure eg. Data Centers
  - Operation of Managed Services

AWS Compliance Programs

A set of internal policies and procedures of a company to comply with laws, rules, and regulations or to uphold business reputation.

Well known compliance programs:

- **HIPAA** (Health Insurance Portability and Accountability Act)
  - United States legislation that provides data privacy and security provisions for safeguarding medical information.
- **PCI DSS** (The Payment Card Industry Data Security Standard)
  - When you want to sell things online and you need to handle credit card information.
- **FIPS** (The Federal Information Processing Standard)
  - standard that specifies the security requirements for cryptographic modules that protect sensitive information
- **NIST 800-53** (National Institute of Standards and Technology)
  - recommended security controls for federal information systems and organizations and documents for all federal information systems, except those designed for national security.

- **AWS Identity and Access Management (IAM)** manage access to AWS services and resources eg. users, groups and roles
- **AWS Artifact** self-service portal for on-demand access to AWS' compliance reports
- **AWS Inspector** runs a security benchmark against specific EC2 instances.
- **AWS Shield** protect against DDoS attacks (stops flooding a website a large amount of fake traffic)
- **AWS Web Application Firewall (WAF)** protect your web applications from common web exploits
- **Amazon Guard Duty** threat detection service that monitors for malicious, suspicious activity and unauthorized behavior.
- **AWS Key Management Service (KMS)** create and control the encryption keys used to encrypt your data.
- **Amazon Macie** monitors S3 data access for anomalies, generates alerts when detects risk of unauthorized access or data leaks.
- **AWS Virtual Private Network (VPN)** establish secure and private tunnel from your network or device to the AWS global network
- **AWS Site-to-Site VPN** securely connect on-premises network or branch office site to VPC
- **AWS Client VPN** securely connect users to AWS or on-premises networks
- **Security Groups (SGs)** Acts as a firewall at the instance level Implicitly denies all traffic. You create only Allow rules.
- **Network Access Control Lists (NACLs)** Acts as a firewall at the subnet level You create Allow and Deny rules.
- **Private Subnets** a slice of the Virtual Private Network that has no direct route to the internet
- **Private subnets** do not assign public IP addresses to EC2 instances
- **AWS Security Hub** a comprehensive view of your high-priority security alerts and security posture across your AWS accounts, consolidation of security logging information into a report based on security compliance frameworks eg. CIS, PCI-DSS
- **IAM Access Analyzer** helps you identify resources in your organization and accounts, such as Amazon S3 buckets or IAM roles,that are shared with an external entity. identify unintended access to your resources and data, which is a security risk.

Technology

Databases Services

- **DynamoDB**- NoSQL key/value database
- **DocumentDB**- NoSQL Document database that is MongoDB compatible
- **RDS**- Relational Database Service that supports multiple engines
    - ENGINES: MySQL, Postgres, Maria DB, Oracle, Microsoft SQL Server, Aurora
    - Aurora MySQL (5x faster) and PSQL (3x faster) database fully managed
- **Aurora Serverless**- only runs when you need it, like AWS Lambda
- **Neptune**- Managed Graph Database
- **Redshift**- Columnar database, petabyte warehouse
- **ElastiCache**- Redis or, Memcached database

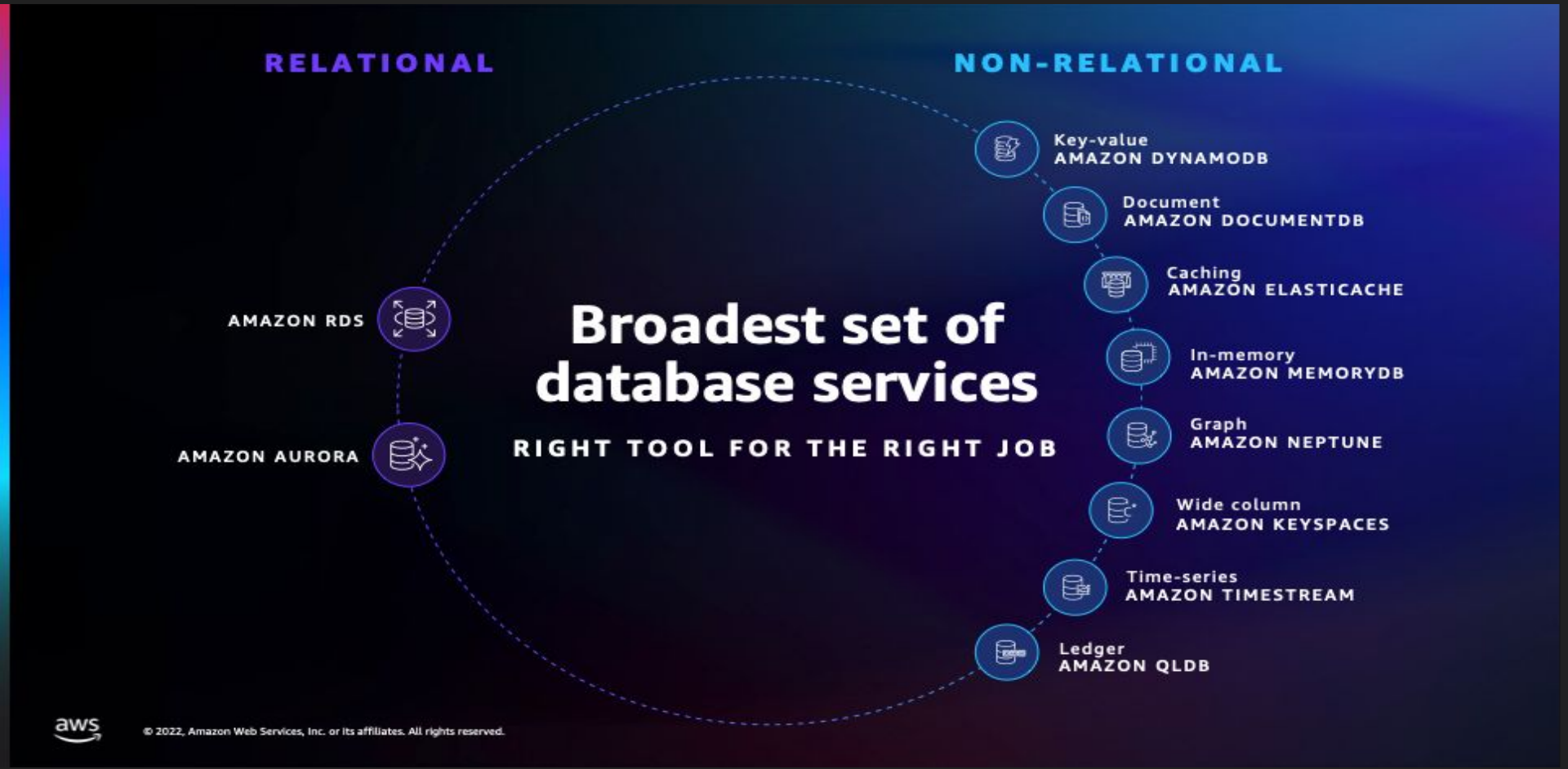
https://docs.aws.amazon.com/whitepapers/latest/aws-overview/database.html

Networking Services

- **Region** the geographical location of your network
- **AZ** the data center of your AWS resources
- **VPC** a logically isolated section of the AWS Cloud where you can launch AWS resources
- **Internet Gateway (IGW)** Enable access to the Internet
- **Route Tables** determine where network traffic from your subnets are directed
- **NACLs** Acts as a firewalls at the subnet level
- **Security Groups (SGs)** Acts as firewall at the instance level
- **Subnets** a logical partition of an IP network into multiple, smaller network segments
    - Public subnets have direct access to the internet eg. public and private IP addresses are assigned to EC2 Instances
    - Private subnets have no direct access to internet eg. only private IP addresses are assigned to EC2 Instances

https://docs.aws.amazon.com/whitepapers/latest/aws-overview/networking-services.html

Databases Services



Networking and content delivery

Cloud networking from AWS

NETWORKING SERVICES FOR EVERY APPLICATION AND WORKLOAD

Networking foundations	Global & hybrid connectivity	Edge networking & content delivery	Application Networking	Network security and remote access
Amazon VPC	AWS Direct Connect	AWS CloudFront	Elastic Load Balancing	AWS Network Firewall
AWS Transit Gateway	AWS Direct Connect SiteLink	AWS Global Accelerator	Amazon VPC Lattice	AWS Verified Access
AWS PrivateLink	AWS Cloud WAN	AWS Route 53		AWS Client VPN
	AWS Site to Site VPN			

AWS **Global Network Infrastructure**, **silicon** innovation, and centralized **network operations**

Organizations and Accounts

- **Organizations** allow you to centrally manage billing, control access, compliance, security, and share resources across your AWS accounts.
- **Root Account User** is a single sign-in identity that has complete access to all AWS services and resources in an account
- Each account has a Root Account User
- **Organization Units** are a group of AWS accounts within an organization which can also contain other organizational units - creating a hierarchy
- **Service Control Policies (SCPs)** give central control over the allowed permissions for all accounts in your organization, helping to ensure your accounts stay within your organization's guidelines.

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html

Provisioning Services

- **Elastic Beanstalk**- service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker
- **AWS OpsWorks**- configuration management service that provides managed instances of Chef and Puppet.
- **AWS CloudFormation**- infrastructure as code, JSON or YAML
- **AWS QuickStart**- pre-made packages that can launch and configure your AWS compute, network, storage, and other services required to deploy a workload on AWS
- **AWS Marketplace**- a digital catalogue of thousands of software listings from independent software vendors you can use to find, buy, test, and deploy software.

Storage Services 

- **S3**- Simple Storage Service - object storage
- **S3 Glacier**- low cost storage for archiving and long-term backup
- **Storage Gateway**- hybrid cloud storage with local caching eg. File Gateway, Volume Gateway, Tape Gateway
- **EBS**- Elastic Block Storage - hard drive in the cloud you attach to EC2 instances
    - SSD, IOPS SSD, Throughput HHD, Cold HHD
- **EFS**- Elastic File Storage - file storage mountable to multiple EC2 instances at the same time
- **Snowball**- Physically migrate lots of data via a computer suitcase 50-80 TB
- **Snowball Edge**- A better version of Snowball - 100 TB
- **Snowmobile**- Shipping container, pulled by a semi-trailer truck - 100 PB

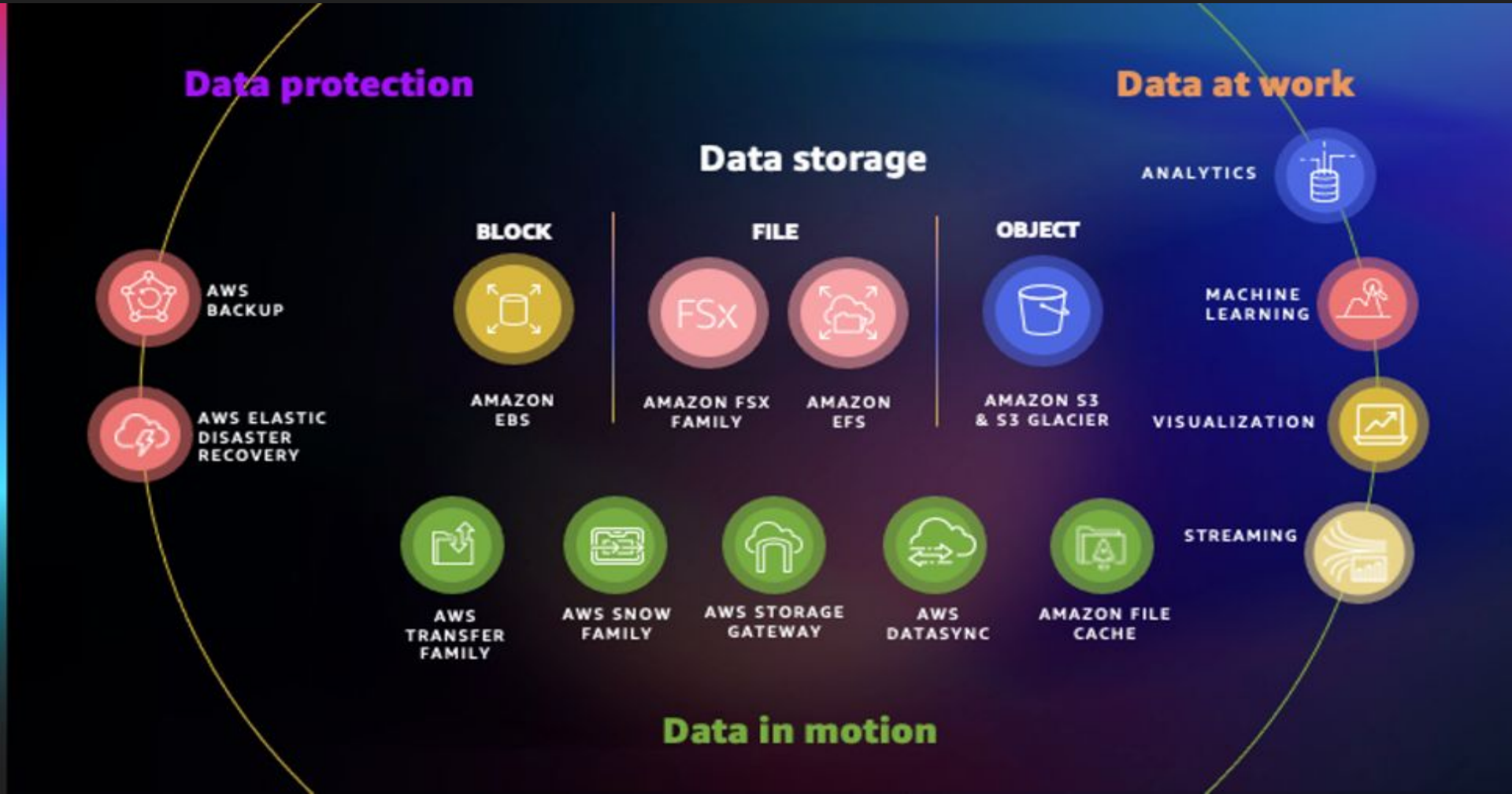
Logging Services

- logs all (SDK, CLI) between (who can we blame)
- is a collection of multiple services
    - CloudWatch Performance data about AWS Services eg. CPU Utilization, Memory, Network I
    - CloudWatch Represents a time-ordered set of data points. A variable to monitor
    - CloudWatch Trigger an event based on a condition eg. ever hour take snapshot of server

■ Also Known As

- CloudWatch Triggers notifications based on metrics
- CloudWatch Create visualizations based on metrics

Storage Services



Enterprise Integration Services

- **Direct Connect** dedicated Gigabit network connection from your premises to AWS Imagine having a direct fibre optic cable running straight to AWS
- **AWS VPN** establish a secure connection to your AWS network
    - **Site-to-Site VPN**- Connecting your on-premise to your AWS network
    - **Client VPN**- Connecting a Client (a laptop) to your AWS network
- **Storage Gateway** A hybrid storage service that enables your on-premises applications to use AWS cloud storage. You can use this for backup and archiving, disaster recovery, cloud data processing, storage tiering, and migration.
- **Active Directory** The AWS Directory Service for Microsoft Active Directory also known as AWS Managed Microsoft AD - enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud.

Computing Services

- **EC2** Elastic Compute Cloud, highly configurable server eg. CPU, Memory, Network, OS
- **ECS** Elastic Container Service **Docker as a Service** highly scalable, high-performance container orchestration service that
supports Docker containers, pay for EC2 instances
- **Fargate** Microservices where you don't think about the infrastructure. Play per task
- **EKS Kubernetes as a Service** easy to deploy, manage, and scale containerized applications using Kubernetes
- **Lambda serverless functions** run code without provisioning or managing servers. pay only for the compute time consume
- **Elastic Beanstalk** orchestrates various AWS services, including EC2, S3, SNS, CloudWatch, ASGs, and ELBs
- **AWS Batch** plans, schedules, and executes your batch computing workloads such as **Amazon EC2** and **Spot Instances**

Business Centric Services

- **Amazon Connect**- **Call Center**- Cloud-based call center service you can setup in just a few clicks - based on the same proven system used by the Amazon customer service teams.
- **WorkSpaces**- **Virtual Remote Desktop**- Secure managed service for provisioning either Windows or Linux desktops in just a few minutes which quickly scales up to thousands of desktops
- **WorkDocs -** A content creation and collaboration service - easily create, edit, and share content saved centrally in AWS. **(the AWS version of Sharepoint)**
- **Chime**- AWS Platform for **online meetings, video conferencing**, and business calling which elastically scales to meet your capacity needs
- **WorkMail**- Managed **business email**, contacts, and calendar service with support for existing desktop and mobile email client applications. (IMAP)
- **Pinpoint**- Marketing campaign management system you can **use for sending targeted email,** SMS, push notifications, and voice messages
- **SES - Simple Email Service**- A cloud-based email sending service designed for marketers and application developers to **send marketing, notification, and emails**
- **QuickSight** - A Business Intelligence (BI) service. Connect multiple datasource and quickly visualize data in the form of graphs with little to no programming knowledge.

Application Integration Services

- **Simple Notification Service (SNS)**- A PubSub messaging system. Sends notifications via various formats such as Plain-text **Email**, HTTP/s (**webhooks**) SMS (**text messages**), **SQS** and **Lambda**. Push messages which then are sent to subscribers
- **Simple Queue Service (SQS)** A queueing messaging system. Send events to a queue. Other applications pull the queue for messages. Commonly used for background jobs.
- **Step Functions** coordinate multiple AWS services into serverless workflows. Easily share data among Lambdas. Have a group of lambdas wait for each other. Create logical steps. Also works with Fargate Tasks.
- **EventBridge (CloudWatch Events)** serverless event bus that makes it easy to connect applications together from your own application, third-party services and AWS services.
- **Kinesis**- Real-time streaming data. Create **Producers** which send data to a stream. **Multiple Consumers** can consume data within a stream. Use for real-time analytics, click streams, ingesting data from a fleet of IOT Devices
- **Amazon MQ** A managed message broker service for **Apache ActiveMQ**
- **Managed Kafka Service (MKS)** A managed **Apache Kafka**

Billing and Pricing

- **AWS Marketplace** curated digital catalogue with of software listings from independent software vendors.
- **Savings Plans** a flexible pricing model that provides savings of up to 72% on your AWS compute usage
    - You can save both for EC2 instances and managed services compute such as Fargate
- **Consolidated Billing** billing and payment methods **across** multiple AWS accounts into **one bill**
- **Volume Discounts** The more you use, the more you save.
- **AWS Cost Explorer** lets you , , and your AWS costs and usage over time.
    - multiple AWS accounts within an AWS Organization costs will be consolidated in the .
- **AWS Budgets** give you the ability to setup alerts if you **exceed** or are **approaching** your defined budget
- **AWS Pricing Calculator** Provides you a detailed set of reports that can be used in executive presentations
- **AWS Resource Groups and Tagging** Helps you organize and consolidate information based on your project and the resources that you use.
    - **Tags** are words or phrases that act as metadata for organizing your AWS resources
    - **Resource Groups** are a collection of resources that share one or more **tags**
- AWS Cost and Usage Reports
- Generate a **detailed spreadsheet**, enabling you to better **analyze** and understand your AWS costs
    - Places the reports into S3
    - Use Athena to turn the report into a queryable database
    - Use QuickSight to visualize your billing data as graphs
- Notable AWS Services that are **Free**
    - AutoScaling, IAM, VPC, Cost Explorer, Organizations and Consolidated Billing
    - Some services are free themselves but the underlying services they preivions are not eg:
        - CloudFormation, Elastic Beanstalk, OpsWorks, CodeStar

Support Plan On AWS

Plan	Cost	Support	Other Details
Basic	$0 USD/month	- No third-party support - Email support for billing and account inquiries only	Minimal support, primarily for basic users
Developer	$29 USD/month	- No third-party support - Email support for technical and account issues	Designed for individual developers
Business	$100 USD/month	- Personal concierge support - Email support for technical issues	Ideal for small to medium-sized businesses
Enterprise	$15,000 USD/month	- Technical Account Manager (TAM) - Full support, possibly including third-party services	Comprehensive, tailored for large enterprises

https://aws.amazon.com/premiumsupport/plans/

EC2 Pricing

On-Demand (least commitment)

- **Key Features**:
  - Low cost and flexible
  - Pay per hour
  - Ideal for short-term, spiky, or unpredictable workloads, and first-time apps
  - Suitable when workloads cannot be interrupted

Reserved Instances (up to 75% off, best long-term value)

- **Key Features**:
  - Best for steady-state or predictable usage
  - Can resell unused reserved instances through the Reserved Instance Marketplace
  - Offers significant savings based on **commitment** and **payment options**:
    - **Commitment**: 1 year or 3 years
    - **Payment Options**: All Upfront, Partial Upfront, and No Upfront
- **Types of Reserved Instances**:
  - **Standard Reserved Instances**:
    - Up to 75% reduced pricing compared to on-demand
    - Cannot change RI attributes
  - **Convertible Reserved Instances**:
    - Up to 54% reduced pricing compared to on-demand
    - Allows you to change RI attributes, provided the new attributes are of equal or greater value
  - **Scheduled Reserved Instances**:
    - Reserve instances for specific time periods (e.g., once a week for a few hours)
    - Savings vary depending on the time and usage pattern

Spot Instances (up to 90% off, biggest savings)

- **Key Features**:
  - Request spare computing capacity at a significant discount
  - Flexible start and end times
  - Can handle interruptions, as instances can be stopped or terminated by AWS at any time
  - Best suited for non-critical background jobs
  - **Pricing**:
    - If your instance is terminated by AWS, you are not charged for the partial hour of usage
    - If you terminate the instance, you are charged for the full hour

Dedicated Hosts (most expensive)

- **Key Features**:
  - Dedicated physical servers for your exclusive use
  - Can be used on-demand or reserved (with up to 70% savings on reserved instances)
  - Ideal for workloads that require isolated hardware for compliance or enterprise-level needs

https://aws.amazon.com/ec2/pricing/