AWS Cheatsheet - Part 1

Author: Bhaskar S
Version: 1.3
Date: 02/25/2024
Blog: PolarSPARC

AWS Cloud Adoption Fwk

- Is a comprehensive guide designed to help organizations effectively plan and implement their cloud adoption strategies
- Addresses the various aspects of cloud adoption from different perspectives - business, people, governance, platform, operations, and security
- **Business** perspective focuses on ensuring that the cloud investments accelerate the digital transformation ambitions and business outcomes
- **People** perspective focuses on ensuring that the organization has the necessary skills, resources, and organizational structure to support cloud adoption
- **Governance** perspective focuses on establishing policies, controls, and processes to ensure compliance, security, and cost optimization
- **Platform** perspective focuses on accelerating the delivery of cloud workloads via an enterprise-grade, scalable, hybrid cloud environment
- **Operations** perspective focuses on ensuring that cloud services are delivered at a level that is agreed upon with the business stakeholders
- **Security** perspective focuses on achieving the confidentiality, integrity, and availability of data and cloud workloads

AWS Support

- Developer **DOES NOT** get Phone support OR access to Support API OR 3rd Party S/W support
- **ONLY** Enterprise gets Tech Acct Manager, Concierge Support, and online self-paced labs

AWS Partner Network

- **Consulting Partners** are professional services firms that help customers of all sizes design, architect, migrate, or build new applications on AWS
- **Technology Partners** provide software solutions that are either hosted on or integrated with the AWS platform

AWS Well Architected Fwk

- **Operational Excellence** - focuses on running and monitoring systems, and continually improving processes and procedures. Key topics include automating changes, responding to events, and defining standards to manage daily operations
- **Security** - focuses on protecting information and systems. Key topics include confidentiality and integrity of data, managing user permissions, and establishing controls to detect security events

- **Reliability** - focuses on workloads performing their intended functions and how to recover quickly from failure to meet demands. Key topics include distributed system design, recovery planning, and adapting to changing requirements
- **Performance Efficiency** - focuses on structured and streamlined allocation of IT and computing resources. Key topics include selecting resource types and sizes optimized for workload requirements, monitoring performance, and maintaining efficiency as business needs evolve
- **Cost Optimization** - focuses on avoiding unnecessary costs. Key topics include understanding spending over time and controlling fund allocation, selecting resources of the right type and quantity, and scaling to meet business needs without overspending
- **Sustainability** - focuses on minimizing the environmental impacts of running cloud workloads. Key topics include a shared responsibility model for sustainability, understanding impact, and maximizing utilization to minimize required resources and reduce downstream impacts

Shared Responsibility Model

- Security and Compliance are a shared responsibility between AWS and the customer
- AWS is responsible for protecting the infrastructure (hardware, software, networking, and facilities) that runs all of the services offered in the cloud
- For IaaS (EC2), the customer is required to perform all of the necessary security configuration and management tasks (including updates and security patches of the guest OS)
- Customers are responsible for the configuration of the AWS-provided firewall (called a security group) on each instance AND managing their data (including encryption options)

- **Inherited controls** - Physical and Environmental controls
- **Shared controls** - For Patch Management, AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications
- **Shared controls** - For Configuration Management, AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications

- **Customer specific** - Service and Communications Protection or Zone Security which may require a customer to route or zone data within specific security environments

Billing and Cost

- Budgets allows one to set custom budgets to track/forecast costs/usage AND respond to alerts from SNS if one exceeded the budget thresholds

- Cost Explorer allows one to visualize, understand, manage AWS costs/usage over time, forecast future costs/usage, identify trends, pinpoint cost drivers, and detect anomalies

- Cost and Usage Reports is a one-stop shop for accessing the most granular data about AWS costs/usage. One can also load the cost/usage information into various tools of choice - Athena, Redshift, QuickSight
- Cost and Usage Reports also allows one to track the EC2 Reserved Instance (RI) usage and view the discounted RI rate that was charged to the resources

- Trusted Advisor helps one optimize costs, increase performance, improve security/resilience by continuously evaluating the AWS environment against best practice checks across broad categories (cost optimization, performance, resilience, security, operational excellence, and service limits) AND makes recommendations to remediate any deviations from best practices

- Compute Optimizer uses ML to analyze historical utilization metrics to recommend optimal AWS resources (EC2, EBS, Lambda) for workloads to reduce costs and improve performance

Disaster Recovery

- **Recovery Point Objective** (RPO)
    - Measurement of the amount of data that can be acceptably lost (how often one does backup - in secs, mins, or hours)
    - Patterns:
        1. Synchronous Replication (millisecs to secs)
        2. Asynchronous Replication (secs to mins)
        3. Snapshots (mins to hours)
    - Example: one can acceptably lose 2 hours of data in a database (2hr RPO) means backup **MUST** be taken every 2 hours

- **Recovery Time Objective** (RTO)
    - Measurement of the amount of time it takes to restore after a disaster event (how quickly can one recover - in secs, mins, or hours)
    - Patterns:
        1. Fault Tolerance (millisecs to secs)
        2. High Availability, Load Balancing, Auto Scaling (secs to mins)
        3. Automated Cross-Region Recovery (mins to hours)
    - Example: if the IT dept expects to 4 hours to bring apps online after a disaster (4hrs RTO)

- **Disaster Recovery Strategies**
    - Backup and Restore - for low priority workloads, provision and restore after the event, costs the least
    - Pilot Light - in another region, data is replicated, services in idle/off state, resources activated after the event
    - Warm Standby - in another region, minimum resources always running, for business critical workloads, can scale up/down
    - Multi-Site Active-Active - in another region, zero downtime, near zero data loss, mission critical workloads

Miscellaneous

- Elastic Beanstalk is PaaS for web/worker apps developed using modern programming languages (Go, Java, .NET, Node.js, PHP, Python, Ruby) with load balancing, auto scaling, and monitoring
- Elastic Beanstalk app version is the deployable code (zip, war, etc) in S3 AND environment is the instance of a running app version

- Elastic Beanstalk environment config is all the parameters and settings of the environment

- App Runner is PaaS service platform that lets one build/deploy/run web apps and API services without prior infrastructure or container experience, one can start with either the source code or a container image, for rapid production deployment of web apps and microservices

- Systems Manager allows one to manage servers running on AWS AS WELL AS in on-prem data center through a single interface

- Transfer Family is a fully managed, highly available, scalable service that enables one to use the FTP (FTP, FTPS, SFTP) protocol to transfer files to AWS S3 or EFS

- Amplify is a set of tools and features for building full-stack apps (with web and mobile backends and frontend UIs) on AWS

- AppSync is a fully managed service that makes it easy to develop apps using GraphQL APIs
- AppSync apps can securely access, manipulate, and receive real-time updates from multiple data sources

- DeviceFarm is an automated app testing service for web and mobile apps

- License Manager is used for managing licenses from software vendors AND provides a centralized management option for both AWS and on-prem resources
- License Manager allows one to track license usage based on vCPUs, cores, sockets, or no of machines

- X-Ray enables developers to conduct performance analysis and debug distributed microservice-based apps that span multiple AWS accounts, regions and AZs, offering an end-to-end visibility

- Health provides ongoing visibility into the resource performance and the availability of AWS services and accounts

- Artifact provides on-demand access to security and compliance reports and select online agreements AND all accounts have access to it

- Resource Access Manager is a service that enables one to easily and securely share resources with any account or within an organization, one can share Transit Gateways, subnets, License Manager configurations, and Route 53 resolver rules

- CodeCommit is a version control service that enables one to privately store and manage Git repositories

- CodeBuild is a fully managed build service that compiles source code, runs unit tests, and produces artifacts that are ready to deploy

- CodePipeline is a continuous delivery service that enables one to model, visualize, and automate the steps required to release app software

- CodeDeploy automates code deployments to any instance, including EC2 instances and instances running on-prem

- Pinpoint is a Digital User Engagement Service that enables AWS customers to effectively communicate with their end-users and measure user engagement across multiple channels including email, Text Messaging (SMS) and Mobile Push Notifications

---