

AWS CCP Notes

Amazon CloudWatch service (to collect and monitor data metrics) - needed to deploy EC2 auto-scaling feature that automatically scale up/down based on demand

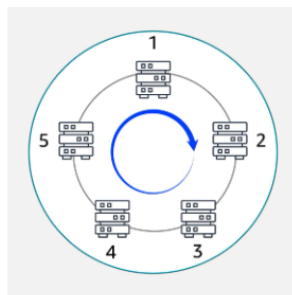
EC2 auto scale adjusts the number of EC2 instances based on the app's demand. 2 types:

1. *Dynamic scaling* adjusts in real time to fluctuations in demand.
2. *Predictive scaling* preemptively schedules the right number of instances based on anticipated demand.

ELB Elastic Load Balancing - ability to scale up or down to distribute traffic according to demand

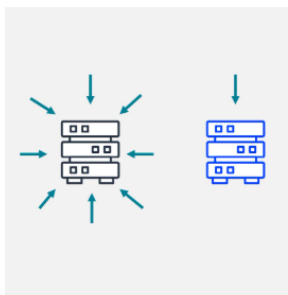
To optimize traffic distribution, ELB uses several **routing methods**:

1. Round Robin
2. Least Connections
3. IP Hash
4. Least Response Time



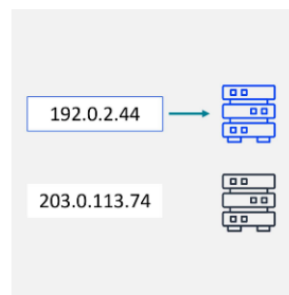
Round Robin

Distributes traffic evenly across all available servers in a cyclic manner.



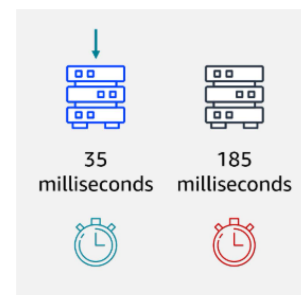
Least Connections

Routes traffic to the server with the fewest active connections, maintaining a balanced load.



IP Hash

Uses the client's IP address to consistently route traffic to the same server.



Least Response Time

Directs traffic to the server with the fastest response time, minimizing latency.

Amazon SQS - simple queue service, a message queuing service, can send, store, and receive messages at any scale ensuring they are not lost

Amazon SNS - simple notification service, a publish-subscribe service that publishers use to send messages to subscribers through SNS topics, tailoring them to their interests and opt-in

Amazon EventBridge- serverless service that routes events from apps like (3rd-party, custom apps, & AWS services) to other apps (like the doordash app, verifies payment, notifies restaurant, confirms inventory, then schedule delivery for pickup)

Amazon Machine Image (AMIs) launch new Amazon EC2 instances with the same software configuration and settings, providing consistency.

AWS LAMBDA - serverless compute service (function-as-a-service) -that runs code in response to events without the need to provision or manage servers. It automatically manages the underlying infrastructure, scaling resources based on the volume of requests

- Set code to trigger from an event source
- Run the code (only when even occurs, ex. File upload or user action)
- Pay only for compute used

3 Components of Lambda

1. Function
2. Triggers
3. Runtime (code)

Containers provide a reliable way to package your application's code and dependencies into a single, portable unit, making them ideal for workflows that require high security, reliability, and scalability.

- Keeps environment/image consistent through deployment (ie. QA, Staging, Production)

Elastic Container Registry ECR - fully managed Docker registry that stores container images

Container Orchestration Services (manages the lifecycle of containers incl. start/stop/run across a cluster)

1. **ECS - Elastic Container Service** - good for streamlining/integrating still can define parameters (such as EC2 types and ELBs) for small-to medium
2. **EKS - Elastic Kubernetes Service** - open source, more complex, offers more control and flexibility (allows Kubernetes clusters to run on AWS good for large scale/hybrid deployments) for enterprises/large

AppStream 2.0 - is a fully managed, secure application streaming service that allows customers to stream desktop applications from AWS to any device with a web browser. It handles provisioning, scaling, patching, and maintenance of the backend infrastructure, delivering high performance and responsive user experience.

AWS Fargate - serverless compute option w/o the infrastructure mgmt leaving you to only worry about your container (a container hosting platform, can be used with both ECS/EKS)

AWS Elastic Beanstalk - simplified provisioning, config mgmt, visibility and control, - A managed service for deploying and scaling web applications

AWS Batch - for heavy duty tasks, massive datasets, running simulations, complex calculations, handles Infra mgmt - scales compute resources for batch jobs

AWS Lightsail - quick and easy to manage, offering Virtual Private Servers VPSs, storage & networking - ideal for small business with basic workloads while still offering the mgmt console

AWS Outpost - designed for hybrid solutions, extends AWS services to on prem - good for low latency and compliance and for migrating legacy systems, and data processing in remote areas

CloudFormation - helps automate deployment of cloud resources, an IaC service, helps achieve consistent reliable setups each time as your business grows

Use cases for CloudFormation include the following:

- Managing infrastructure with DevOps such as continuous integration and delivery (CI/CD) pipelines
- Scaling resources such as Amazon EC2 instances to multi-Region applications in a consistent, repeatable way

Choosing a region considerations:

1. Compliance - subject to local laws, complying to regions, EU compliance to GDPR etc.

2. Proximity - being close to AZs for lower latency and better responsiveness
3. Features - available feature options in each region, varies by location
4. Pricing - some regions have lower operational costs also tax laws/regulations play affect

NETWORKING

VPC Flow Logs - a feature that allows users to capture info about net traffic to and from their VPCs, aiding in troubleshooting connectivity.

AWS Direct Connect - a private dedicated physical line (fiber connection) connecting from your data center to AWS - working with a partner in your area - alternative to VPN.

AWS PrivateLink - allows you to privately connect your VPC to services and resources, other VPCs, and endpoints as though they were in your VPC

Add'l Gateway Services

Network Address Translation (NAT) Gateway - is a NAT service allowing instances in a private subnet to connect to services outside your VPC but external services can't connect.

AWS Transit Gateway - connects your VPCs and on-prem networks through a central hub as cloud infra. Expands globally, inter-Region peering connects transit gateways together

Amazon API Gateway - service for creating, publishing, maintaining, monitoring, and securing APIs at scale.

AWS Edge Services

Amazon CloudFront - a content delivery network (CDN) service designed to serve content close to users as possible like content, images, videos, data, apps, APIs using edge locations

Amazon Route 53 - is a cloud DNS service that provides a reliable and cost-effective way to route end users to internet applications, and also routes users to infra outside of AWS. Can manage all domain names in a single service.

AWS Global Accelerator - a service that uses AWS global network to improve app availability by using intelligent traffic routing. It does this by providing static IP addresses, directing traffic over the AWS global network, and routing to optimal endpoints based on health, user location, and policies.

Feature	Security Groups	Network ACLs
Scope	Instance level (attached to EC2 instances)	Subnet level (associated with subnets)
State	Stateful (remembers state)	Stateless (doesn't remember state)
Rule types	Only allow type rules	Both allow and deny type rules
Return traffic	Return traffic is automatically allowed if inbound traffic is allowed	Return traffic must be implicitly allowed in both directions
Uses	Fine-grained control of traffic for individual EC2 instances	Broad control of traffic in and out of subnets

STORAGE

Block Storage Services

*EBS provides block level storage needed for EC2 instances and databases

Amazon EC2 instance store - An unmanaged non-persistent, high-performance temp block-level storage directly attached to EC2 instances for temporary data.

Amazon Elastic Block Store (EBS) - A managed service that provides persistent block storage volumes for EC2 instances, offering various types for different workloads, ensures data protection through automatic replication within the same Availability Zone

Object Storage

*S3 excels at scalable object storage for web assets, backups, & more

Amazon Simple Storage Service (S3) -A fully managed scalable object storage service for storing and retrieving any amount of data from anywhere. -provides scalable object storage ideal for storing and distributing media files. It includes features like lifecycle policies for cost optimization, bucket organization for client projects, access controls for security, and the ability to generate URLs for easy file sharing.

- Each object includes data itself, metadata, & a unique identifier/key.
- Stored in a S3 bucket - (a container) with a unique name across all of AWS

Storage Class Types

1. S3 Standard - default for general purpose storage
2. S3 Intelligent-Tiering - for unknown/changing access patterns to most cost effective.
3. S3 Standard-IA - good for infrequently accessed data but requires rapid access
4. S3 One Zone-IA - stores data in 1 AZ reduces costs, good for secondary backups
5. S3 Express 1 Zone - stores in 1 AZ for most frequently accessed data w/faster access
6. S3 Glacier Instant Retrieval - archiving data rarely accessed with quick retrieval
7. S3 Glacier Flexible Retrieval - for archived data accessed 1-2x/year retrieved in 1-5 min
8. S3 Glacier Deep Archive -lowest cost for 7-10 year retention with retrievals of 12 hours
9. S3 Outposts - delivers on-prem obj storage using S3 APIs, serves local workloads

S3 Storage Analysis - looks at your data access patterns and decides when to move data to a more cost-effective storage class

File Storage

*EFS offers managed shared file systems from workloads that require rapid, simultaneous access to files.

Amazon Elastic File System (EFS) - A fully managed, scalable Network File System (NFS) for use with AWS Cloud services and on-premises resources. Regional resource.

1. Good for redundancy setup across multiple AZs
2. Allows thousands of NFS connections to EC2s simultaneously
3. Elastic storage, grows and shrinks as you add/remove files

Amazon Athena - service that the dev team should use to write a simple query that can read all the .csv files stored in an Amazon S3 bucket and generate a summary report. Allows users to analyze data in S3 using standard SQL, requires no setup or mgmt of servers. Can handle multiple data formats including .csv

Amazon FSx - A fully managed file storage service for popular file systems like Windows, Lustre, and NetApp ONTAP.

1. **Windows File Server** - delivers a wide range of data access, data mgmt, & admin capabilities. - provides SMB support, Active Directory integration, and Windows features like data deduplication, while delivering consistent sub-millisecond latencies as a fully managed service.
 - a. Migrate Windows file servers to AWS, Accelerate hybrid workload
 - b. Reduce SQL server deployment cost, streamline virtual desktops & streaming
2. For **NetApp ONTAP** - fully managed shared storage with the popular data access and mgmt capabilities of ONTAP
 - a. Migrate workloads to AWS seamlessly, build modern apps
 - b. Modernize data mgmt, streamline business continuity
3. For **OpenZFS** - built on the OpenZFS file system and accessible through the NFS protocol (v3, v4, v4.1, and v4.2).
 - a. Migrate workloads to AWS, deliver insights faster for data analytics workloads
 - b. Accelerate content mgmt, increase dev/test velocity
4. For **Lustre** - shared storage with the scalability and performance of the popular Lustre file system.

- a. Accelare ML, enable high perf computing (HPC)
- b. Unlock big data analytics, increase media workload agility

Add'l Storage Services

AWS Storage Gateway - fully managed, hybrid-cloud storage service that provides on-premises access to virtually unlimited cloud storage. There are 3 gateway types:

1. **S3 File Gateway** - bridges on-prem env with S3 appears as standard file server
2. **Volume Gateway** - you create virtual storage vols while maintaining local access to your data - bridge between on-prem infra and AWS Cloud storage - presents cloud storage as iSCSI *block storage volumes* rather than file shares.
 - a. **Vol Gateway in Cached mode** - stores primary data/complete dataset in cloud while frequent access data is cached locally for low-latency access
 - b. **Vol Gateway in Stored mode** - locally keeps your complete dataset while asynchronously backing it up to the cloud as EBS snapshots
3. **Tape Gateway** - replaces physical tape with virtual tape making the transition to cloud seamless - can manage the lifecycle as well, moving less frequent access to more cost effective storage class for long-term retention

AWS Elastic Disaster Recovery - fully managed service that streamlines the recovery of your physical, virtual, and cloud-based servers into AWS - minimizes downtime and data loss by providing fast, reliable recovery of on-premises and cloud-based applications using affordable storage, minimal compute, and point-in-time recovery

DATABASES

Amazon Relational Database Services (RDS) - service that organizes collections of data into tables with rows and columns, where relationships exist between different tables.

- Use cases: web apps, enterprise workloads and product inv for e-commerce platforms

Benefits of RDS:

- Automated patching
- Backups
- Redundancy
- Failover
- Disaster recovery

Amazon Aurora - a managed relational database designed to help reduce unnecessary input/output (I/O) operations, compatible with MySQL and PostgreSQL, provides high performance and availability and auto-scales alongside your workloads.

5x the throughput of MySQL and 3x of PostgreSQL

- Use cases: gaming apps, media, and content mgmt

Amazon DynamoDB - a fully managed NoSQL database (*based on key value pairs*) service that provides fast and predictable performance for both document and key-value data structures. It's a powerful and incredibly fast database option for use cases that require a flexible schema, and is ideal for applications that require high performance and seamless scaling.

- Use cases: gaming platforms, financial service apps, and mobile apps with global user bases
1. Provides data encryption for both data at rest and in transit
 2. High availability by replicating data across 3 facilities within each AWS Region maintaining multiple copies
 3. Consistent high performance brings **single digit millisecond response times at any scale**
 4. Auto-scales throughput based on actual usage, can set target utilization level and will auto provision capacity to maintain those levels.

Amazon Redshift - data warehousing service, specifically designed for analytics of large volumes of data and ideal for feeding analytics dashboards with large datasets.

Amazon ElastiCache -An in-memory caching service that supports Redis, Valkey, or Memcached to improve application performance through faster data retrieval

Amazon DocumentDB (with MongoDB compatibility) is a fully managed service designed to handle semistructured data, which is information that doesn't conform to rigid relational schemas. Amazon DocumentDB is a MongoDB-compatible database, so it manages JSON-like documents with dynamic schemas. For mission-critical workloads with auto scaling

AWS Backup streamlines data protection across various AWS resources and on-premises deployments by providing a single dashboard for monitoring and managing backups.

Amazon Neptune - a fully managed, purpose-built graph database service that manages highly connected data sets, like those used in social networking applications. It excels at understanding complex relationships that are difficult to identify in traditional relational databases like user connections, friend networks, and interaction patterns.

AI/ML

Generative AI on AWS

Amazon SageMaker JumpStart—An ML hub with FMs and pre-built ML solutions deployable with a few clicks

Amazon Bedrock—A fully managed service for adapting and deploying FMs from Amazon and other leading AI companies

Amazon Q—An interactive AI assistant that can be integrated with a company's information repositories

ETL Process - Extract, Transform, Load data

SECURITY

AWS IAM Identity Center - designed to help orgs implement single sign on for AWS resources using their existing identity providers.

Server-side encryption - an encryption option that S3 provides to encrypt data at rest in S3. S3 encrypts an object before saving it to disk in its data centers and decrypts it when you download the objects.

AWS WAF (Web Application Firewall) is designed to protect web-facing applications and APIs from common web exploits and abusive traffic. Common web attacks:

- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Command injection
- Path traversal
- Bad bots and scrapers

Amazon Cognito - provides user identity & authentication for mobile and web apps, allowing users to sign up, sign in, and access AWS resources with different identity providers.

Amazon Macie - used to monitor data at rest using ML can be used to assess security posture. Certify that sensitive data is discovered and protected in Amazon S3.

AWS Shield Standard- a managed DDoS protection service that safeguards applications running on AWS from common, frequently occurring types of DDoS attacks at no cost.

Amazon Inspector - runs automated security assessments, bring vulnerabilities to your attention with recommendations

Amazon GuardDuty - to identify threats, an IDS, monitors streams of your account metadata and net activity

Amazon Detective - treat visualizations and insights gen AI powered, further investigates the root cause once a threat is detected

Amazon Security Hub - SIEM - can accelerate time to resolution (TTR) with automated remediation.

MONITORING

Amazon CloudWatch - monitors your AWS resources and the applications that you run on AWS in real time. You gain system wide visibility into resource utilization, app performance, and operational health.

1. Metrics
 2. Alarms
 3. Dashboards
 4. Automate scaling
- Use cases: to monitor and troubleshoot infrastructure. Helps visualize/analyze your resources, operate efficiently with automation.

AWS CloudTrail - tracks user activity and API usage in the cloud and on prem, and with other cloud providers. Details history of API calls to track changes and identify who made them and when. Record of past 90 days.

- Use cases: It can be used for compliance and auditing, identifying security incidents, troubleshooting operational issues.

AWS Artifact -free service for on-demand access to AWS security and compliance reports and select online agreements.

- Use cases: It can be used to manage select online agreements and assess third-party security and compliance.

AWS Config - service to assess, audit and evaluate the config of your AWS resources.

- Use cases: It can be used to continually audit security monitoring and analysis and to streamline operational troubleshooting and change management.

AWS Audit Manager - continually audits your AWS usage to simplify risk and compliance assessment, helps collect evidence and manage audit data.

- Use case: It can be used to automate evidence collection, continually audit to assess compliance, and deploy internal risk assessments.

(SCP) Service Control Policies - a policy that lets you place restrictions on the AWS services, resources, and individual API actions that users and roles in each account can access. SCPs can be applied to either OUs or individual member accounts.

AWS Control Tower - a service to enforce and manage governance rules for security, operations and compliance at scale across all your orgs & account in the cloud

- Use cases: deploy apps and provision compliant AWS accounts
 1. **Account Factory** - configurable template that standardizes the provisioning of new accounts
 2. **Controls** - aka guardrails, high level rules that provide governance for your overall AWS env.
 3. **Landing Zone** - multi-account env that's based on security and compliance, its the enterprise wide container that holds all of the OUs accounts, users, and resources you want to regulate for compliance.

AWS Service Catalog - a curated catalog of AWS resources, easily deploy baseline networking resources & security tools to govern consistently

- Use cases: Use it to provision resources across AWS accounts, apply access controls, and accelerate provisioning of continuous integration and continuous delivery (CI/CD) pipelines.

AWS License Manager - helps manage and govern your software licenses and fine-tune your licensing costs.

AWS Health Dashboard - view account specific health info, plan for lifecycle events or troubleshoot an incident

Pricing & Support

There are 3 fundamental drivers of cost with AWS:

1. Compute - pay-as-you use EC2, Lambda, ECS
2. Storage
3. Outbound Data Transfer

AWS Billing and Cost Management Dashboard - centralizes cost mgmt, showing current charges, usage, forecasts, and detailed breakdowns.

AWS Budgets - set up alerts for projects where costs exceed predefined thresholds and forecast future expenses based on current usage trends.

AWS Cost Explorer - visualizes, analyzes and manages costs and usage with graphs/reports/forecasts.

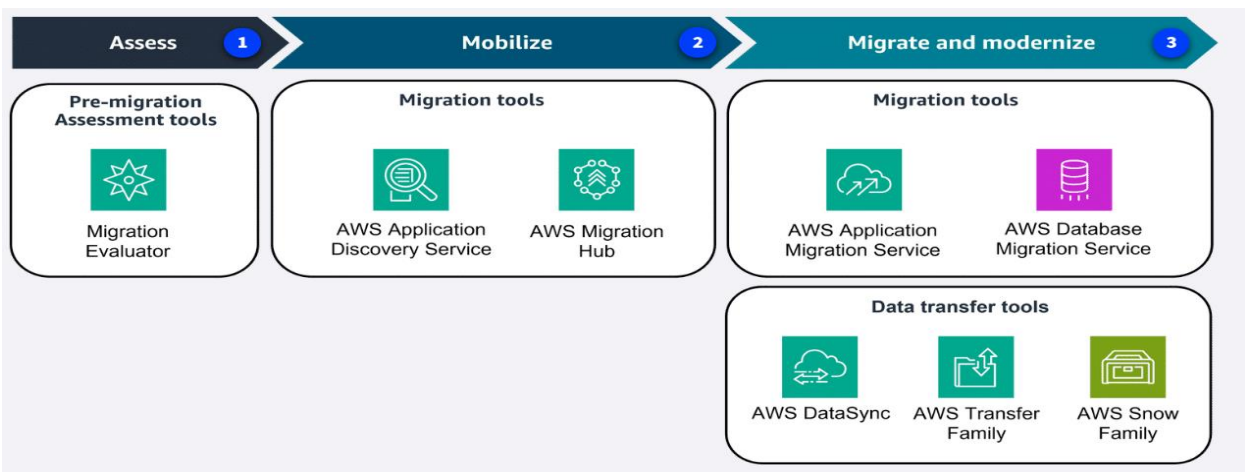
AWS Pricing Calculator -web-based tool to create estimates, input configs, such as instance types, storage options, and data transfer volumes, and receive a detailed cost breakdown.

Basic Support	Developer Support	Business Support	Enterprise On-Ramp Support	Enterprise Support
Included for all AWS customers	Recommended for experimenting or testing in AWS	Recommended minimum tier for production workloads in AWS	Recommended for production and business critical workloads in AWS	Recommended for business critical and mission critical workloads in AWS
Includes access to documentation, whitepapers, and AWS re:Post	Response times: <ul style="list-style-type: none"> • < 24 hours for general guidance • < 12 hours when systems impaired 	Response times: <ul style="list-style-type: none"> • <i>Includes previous plan response times</i> • < 4 hours when production system impaired • < 1 hour when production system is down 	Response times: <ul style="list-style-type: none"> • <i>Includes previous plan response times</i> • < 30 minutes when business-critical system is down 	Response times: <ul style="list-style-type: none"> • <i>Includes previous plan response times</i> • < 15 minutes when business- or mission-critical system is down

Core AWS Trusted Advisor checks	Core AWS Trusted Advisor checks	Full set of AWS Trusted Advisor checks	Full set of AWS Trusted Advisor checks	Full set of AWS Trusted Advisor checks and prioritized recommendations by AWS account team
Technical Account Management not included	Technical Account Management not included	Technical Account Management not included	A pool of technical account managers (TAMs) provide proactive guidance	A designated TAM provides consultative architectural and operational guidance

Welcome to AWS Documentation	The AWS Documentation page provides comprehensive technical resources, including guides, API references, tutorials, and best practices across AWS services.
--	---

MIGRATION



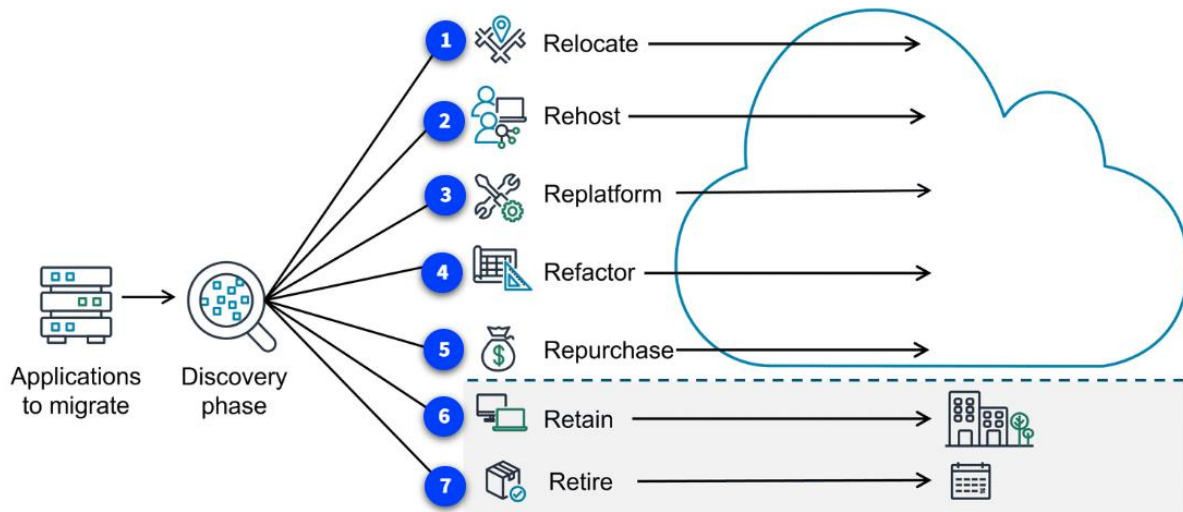
3 Phases of Migration

1. **Assess** - assess current readiness, identify business outcomes and the need to migrate, build a business case.
2. **Mobilize** - create migration plan and address any gaps your readiness, deep understanding of the interdependencies between apps in your env, evaluate migration strategies to meet your business objectives.
3. **Migrate & Modernize** - execute, each app is architected, validated, and migrated, take adv. of migration specialists.

AWS Cloud Adoption Framework (AWS CAF) - framework that brings AWS experience & best practice to companies preparing to migrate to the AWS cloud. Provides tools to help accelerate the migration journey.



7 Migration Strategies to consider when migrating apps to the cloud - each strategy depends on factors such as the complexity of existing apps, business goals, time constraints, and available resources.



AWS App Discovery - a migration detective, explores on-premises server inventory and connections. taking notes, how they work together and what resources they need, and providing detailed reports

AWS Cloud9 - AWS service that enables users to run their existing custom and non-production workloads on the cloud quickly and cost-effectively. A cloud-based Integrated Development Environment (**IDE**) that lets users write, run, and debug code from a web browser.

AWS App Migrations Service - helps pack up your apps and smoothly moves them to the cloud, can make small adjustments to ensure it fits with the move. It helps the agency simplify, expedite, and reduce the cost of migrating and modernizing applications.

Migration Evaluator - a moving consultant, detailed cost estimates, understanding savings and planning a budget, for data driven decisions

AWS Migration Hub - command center for the entire moving process, unified view of all tasks and progress tracking, to keep everything organized.

AWS Database Migration Service (AWS DMS) - to move your databases to AWS, relational, data warehouses, noSQL databases, and analytics workloads - a vm that runs replication software. It

provides a way to plan, assess, convert, and migrate databases even with data warehouses in one central tool and can be used when converting databases.

Heterogenous conversion - when you need to change your database to a different type of database service

AWS Schema Conversion Tool (AWS SCT) - converts the source database schema and code into a format compatible with the target database. Any code that can't be converted auto is marked for manual conversion for you to review before migration proceeds.

AWS DataSync - for automating and accelerating data transfer - The benefits include streamlining and accelerating secure data migrations. DataSync manages data movement workloads with bandwidth throttling, migration scheduling, task filtering, and task reporting. It also provides rapid data replication.

AWS Transfer Family - makes it easy to manage and share data with simple secure and scalable file transfers, secure file transfers over FTP, SFTP & FTPS. Simplifies the process.

AWS SnowBall Edge (physical device) - devices deliver high performance NVMe storage, making it possible to simplify multi-petabyte data migrations from on-prem locations to AWS. For OFFLINE MIGRATIONS.

WELL-ARCHITECTED SOLUTIONS

Well-Architected Framework (6 pillars)

1. Operational excellence - running and monitoring to deliver business value, auto pipelines
2. Security - building security into solutions, protects systems & data through best practices
3. Reliability - recovery planning, system withstand failure, emphasizes system adaptability auto scales to meet demand

4. Performance efficiency - using resources efficiently like scaling EC2 instances
5. Cost optimization - controlling/reducing expenses by optimizing resource allocation
6. Sustainability- minimalizes environmental impact, promotes energy efficient systems