**AWS Serverless Services include:**

**Compute:** AWS Lambda, AWS Fargate

**Messaging:** Amazon SNS, Amazon SQS

**Database:** Amazon DynamoDB**,** Amazon Aurora Serverless

**Orchestration:** AWS Step Functions

Server-based services include: Amazon EC2, Amazon RDS, Amazon Redshift and Amazon EMR.

AWS Organizations has five main benefits:

1) Centrally manage access polices across multiple AWS accounts.

2) Automate AWS account creation and management.

3) Control access to AWS services.

4) Consolidate billing across multiple AWS accounts.

5) Configure AWS services across multiple accounts.

When you want to estimate the costs of Amazon EBS you need to consider the following:

1- Volume types.

2- Input/output operations per second(IOPS).

3- Snapshots.

4- Data Transfer.

Well-Architected Framework

General design principles :

1. Stop guessing capacity
2. Test systems at Production scale
3. Automate to make architectural experimentation easier
4. Allow for evolutionary architectures
5. Drive architecture using data
6. Improve through game days

Five pillars of the Framework :

1. Operational Excellence
   1. Perform operations as code
   2. Annotate documentation
   3. Make frequent, small, reversible changes
   4. Refine operations procedures frequently
   5. Anticipate failures
   6. Learn from all operations failures

Key AWS assets

AWS CloudFormation – templates based on best practices

AWS Config and AWS Config rules create standard for workloads and check environments for compliance with standards

Amazon CloudWatch monitors operational health of a workload

Amazon Elasticsearch Service (ES) allows analysis of log data for actionable insights

1. Security
   1. Implement a strong Identity foundation
   2. Enable traceability
   3. Apply security at all layers
   4. Automate security best practices
   5. Protect data in transit and at rest
   6. Keep people away from data
   7. Prepare for security events

Best practices

1. IAM – MFA, AWS Organizations
2. Detective controls – CloudTrail, CloudWatch, GuardDuty
3. Infrastructure protection – VPC, CloudFront with AWS Shield, WAF
4. Data protection – ELB, EBS, S3, RDS , Amazon Macie (sensitive data), KMS
5. Incident response – IAM, CloudWatch, CloudFormation
6. Reliability
   1. Test recovery procedures
   2. Automatically recover from failure
   3. Scale horizontally
   4. Stop guessing capacity
   5. Manage change in Automation

Best practices

1. Foundations – IAM, VPC, Trusted Advisor for visibility into service limits, Shield
2. Change Management – CloudTrail, Config for resource and configuration inventory, Auto Scaling, CloudWatch
3. Failure Management – CloudFormation, S3 for backups, Glacier for Archives, KMS for Key Management
4. Performance Efficiency
   1. Democratize advanced technologies
   2. Go Global in minutes
   3. Use serverless architectures
   4. Experiment more often
   5. Mechanical sympathy – use technology approach that aligns best with objective

Best Practices

1. Selection
   1. Compute – Instances, Containers, Functions
      1. Auto Scaling
   2. Storage – access method (block/file/object), access pattern (random/sequential), throughput required, access frequency (online, offline, archival), update frequency (WORM, dynamic), availability and durability constraints
      1. EBS (SSD, PIOPS)
      2. S3 for serverless content delivery
      3. S3 Transfer Acceleration enables fast, easy, secure transfer of files over large distances
   3. Database – availability, consistency, partition tolerance, latency, durability, scalability, query capability
      1. RDS for optimization (PIOPS, Read replicas)
      2. DynamoDB for single-digit millsecond latency at any scale
   4. Network
      1. Route 53 provides latency-based routing
      2. VPC endpoints and Direct Connect can reduce network jitter
2. Review
   1. AWS Blog
   2. What’s New section on AWS website
3. Monitoring
   1. CloudWatch
4. Trade-off – consistency, durability and space vs time or latency
   1. ElastiCache, CloudFront, Snowball for performance improvement
   2. RDS replicas for scaling read-heavy workloads
5. Cost Optimization
   1. Adopt a Consumption model
   2. Measure overall efficiency
   3. Stop spending money on data center operations
   4. Analyze and attribute expenditure
   5. Use managed and app-level ownership to reduce cost of ownership

Best practices

1. Expenditure awareness
   1. Cost Explorer to track spend and gain insights into exactly where you spend
   2. AWS Budgets to send notifications if cost/usage are not in line with forecast
   3. Tagging
   4. CloudWatch billing alerts
   5. Simple Monthly Calculator to calculate data transfer costs
2. Cost-effective resources
   1. On-Demand Instances – pay for compute capacity by the hr, no minimum commitments
   2. Reserved Instances – reserve capacity, Upto 75% off on-demand pricing
   3. Spot Instances – leverage unused EC2 capacity, upto 90% off on-demand pricing, for situations which can have interruption
3. Matching supply and demand
4. Optimizing over time

Architecting for Cloud

* Applications that are migrated, maintain existing traditional operating models, leverage the ability to manage Infrastructure as Code through APIs enabling robust and repeatable build processes, improving reliability.
* Solutions that are refactored leverage higher levels of automation of the operational processes as the supporting services, e.g. AWS Auto Scaling and self-healing architectures.
* Solutions that are rearchitected and designed for cloud operations are typically fully automated through DevOps processes for delivery pipeline and management.

Stateless Applications : stateless application is an application that does not need knowledge of previous interactions and does not store session information. Stateless applications can scale horizontally because any of the available compute resources (such as EC2 instances and AWS Lambda functions) can service any request. Without stored session data, you can simply add more compute resources as needed.

Distribute load to multiple nodes :

Push - you can use Elastic Load Balancing (ELB) to distribute a workload. ELB routes incoming application requests across multiple EC2 instances. Network Load Balancer – Layer 4 of OSI and handles TCP. Application Load Balancer – Layer 7 of OSI and supports content-based routing – HTTP/HTTPS. Route 53 – DNS round robin.

Pull – for asynchronous and event-driven workload. tasks that need to be performed or data that needs to be processed can be stored as messages in a queue using Amazon Simple Queue Service (Amazon SQS) or as a streaming Amazon Web Services data solution such as Amazon Kinesis. Multiple compute resources can then pull and consume those messages, processing them in a distributed fashion.

Stateless – no session data preserved. To prevent stateless - Option can be to use DynamoDB to store session data, or store large files in S3 or EFS.

Disposable resources instead of fixed servers

Configuration drift can be addressed by creating immutable architecture where a problem server is replaced with a new server – possible in stateless architecture

Bootsrapping to instantiate compute resources.

When compared to the bootstrapping approach, a golden image results in faster start times and removes dependencies to configuration services or third-party repositories.

While golden images are most commonly used when you launch new EC2 instances, they can also be applied to resources such as Amazon RDS DB instances or Amazon EBS volumes.

Hybrid - Items that do not change often or that introduce external dependencies will typically be part of your golden image. Items that change often or differ between your various environments can be set up dynamically through bootstrapping actions.

Alarms and Events

Amazon CloudWatch alarms: You can create a CloudWatch alarm that sends an Amazon Simple Notification Service (Amazon SNS) message when a particular metric goes beyond a specified threshold for a specified number of periods. Those Amazon SNS messages can automatically kick off the execution of a subscribed Lambda function, enqueue a notification message to an Amazon SQS queue, or perform a POST request to an HTTP or HTTPS endpoint.

Amazon CloudWatch Events: Delivers a near real-time stream of system events that describe changes in AWS resources.22 Using simple rules, you can route each type of event to one or more targets, such as Lambda functions, Kinesis streams, and SNS topics.

AWS Lambda scheduled events: You can create a Lambda function and configure AWS Lambda to execute it on a regular schedule.

AWS WAF security automations: AWS WAF is a web application firewall that enables you to create custom, application-specific rules that block common attack patterns that can affect application availability, compromise security, or consume excessive resources. You can administer AWS WAF completely through APIs, which makes security automation easy, enabling rapid rule propagation and fast incident response.

Managed Services

Amazon SQS you can offload the administrative burden of operating and scaling a highly available messaging cluster, while paying a low price for only what you use.

The same applies to Amazon S3, which enables you to store as much data as you want and access it when you need it, without having to think about capacity, hard disk configurations, replication, and other related issues.

Other examples of managed services that power your applications include:

* Amazon CloudFront for content delivery
* ELB for load balancing
* Amazon DynamoDB for NoSQL databases
* Amazon CloudSearch for search workloads

Relational database workloads that need to scale their write capacity beyond the constraints of a single DB instance require a different approach called *data partitioning* or *sharding*. With this model, data is split across multiple database schemas each running in its own autonomous primary DB instance.

Last-minute read :

* + - 1. Difference between CodeCommit and CodeDeploy ?
      2. Difference among SQS, SWF, SNS, SES ?
      3. Difference between NAT gateway and NAT Instance ?
      4. Difference between Security Group and NACL ?
      5. IAM : Policy/Group/User/Role ?
      6. Difference – Cost Explorer, Budgets, Simple Monthly Calculator?
      7. AMI vs Golden Image ?
      8. Difference between CloudSearch and ElasticSearch ?
* IAM Policies are documents that define permissions and can be applied to users, groups and roles
* IAM policies can be written to grant access to Amazon S3 buckets
* IAM Roles are created and then “assumed” by trusted entities and define a set of permissions for making AWS service requests
* IAM Groups are collections of users and have policies attached to them
* An IAM user is an entity that represents a person or service
* Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS
* CloudWatch is for performance monitoring (CloudTrail is for auditing)
* CloudWatch is used to collect and track metrics, collect and monitor log files, and set alarms
* AWS CloudTrail is a web service that records activity made on your account and delivers log files to an Amazon S3 bucket
* CloudTrail is for auditing (CloudWatch is for performance monitoring)
* CloudTrail is about logging and saves a history of API calls for your AWS account
* CloudTrail records account activity and service events from most AWS services
* The AWS Storage Gateway service enables hybrid storage between on-premises environments and the AWS Cloud. It provides low-latency performance by caching frequently accessed data on premises, while storing data securely and durably in Amazon cloud storage services. AWS Storage Gateway supports three storage interfaces: file, volume, and tape
* File gateway provides a virtual on-premises file server, which enables you to store and retrieve files as objects in Amazon S3
* The volume gateway represents the family of gateways that support block-based volumes, previously referred to as gateway-cached and gateway-stored modes
* Tape Gateway (formerly known as Gateway Virtual Tape Library) is used for backup with popular backup software
* DNS names are used for service discovery. In loose coupling disparate resources must have a way of discovering each other without prior knowledge of the network topology
* Reservations apply to various services, including: EC2, DynamoDB, ElastiCache, RDS and RedShift
* Two of the components you need to connect to your VPC with a VPN connection are a virtual private gateway on the VPC side and a customer gateway on the on-premise network side
* The only storage options for a root volume that can be booted from are EBS volumes and Instance Stores

Route 53 features include domain registration, DNS, traffic flow, health checking, and failover.

* The Amazon S3 notification feature enables you to receive notifications when certain events happen in your bucket
* Notifications can be sent to: SNS Topics, SWS Queues, and Lambda functions
* Amazon Simple Workflow Service (SWF) is a web service that makes it easy to coordinate work across distributed application components. SWF enables applications for a range of use cases, including media processing, web application back-ends, business process workflows, and analytics pipelines, to be designed as a coordination of tasks
* Amazon Security Token Service (STS) is used for requesting temporary credentials
* Amazon Simple Queue Service (SQS) is a message queue used for decoupling application components
* Amazon Simple Notification Service (SNS) is a web service that makes it easy to set up, operate, and send notifications from the cloud
* SNS supports notifications over multiple transports including HTTP/HTTPS, Email/Email-JSON, SQS and SMS
* For operational analytics such as application monitoring, log analytics and clickstream analytics,Amazon Elasticsearch Service allows you to search, explore, filter, aggregate, and visualize your data in near real-time
* For big data processing using the Spark and Hadoop frameworks,Amazon EMR provides a managed service that makes it easy, fast, and cost-effective to process vast amounts data
* For interactive analysis,Amazon Athena makes it easy to analyze data directly in S3 and Glacier using standard SQL queries
* For dashboards and visualizations,Amazon QuickSight provides you a fast, cloud-powered business analytics service, that that makes it easy to build stunning visualizations and rich dashboards that can be accessed from any browser or mobile device