Architecting on AWS – Key Concepts

Module 1 – Architecting Fundamentals

- AWS Infrastructure
  - Data centers
  - Availability Zones
  - Regions
    - Factors impacting Region selection
      - Governance / Latency
      - Service availability / Cost
  - AWS Local Zones
  - Edge locations
- AWS Well-Architected Framework
  - Pillars
    - Security / Cost optimization
    - Reliability / Performance efficiency
    - Operational excellence / Sustainability
  - AWS Well-Architected Tool

Module 2 – Account Security

- Principals and identities
  - AWS account root user
  - IAM – *Authentication / Authorization*
    - user
      - AWS API calls
        - Console Access (AWS Management Console)
          - ID, Password
        - Programmatic Access (AWS CLI, AWS SDKs)
          - Access Key ID, Secret Access Key
      - Setting permissions with IAM policies
    - user group
    - role
      - Assuming a role (+ AWS STS)
        - *by* IAM user
        - *by* AWS services
        - *by* Federated user (Non-AWS)
    - policy (*assigned to* user, group, role)
- Security Policies
  - Set maximum permissions
    - IAM permissions boundaries
    - AWS Organizations service control policies (SCPs)
  - Grant permissions
    - IAM identity-based policies
      - AWS managed
      - Customer managed
    - IAM resource-based policies
    - + Defense in depth
- Managing Multiple Accounts
  - AWS Organizations (+ SCPs)
  - + Using policies for a layered defense

Module 3 – Networking 1

- IP Addressing
  - Classless Inter-Domain Routing (CIDR) (/16 ~ /28)
- VPC(Virtual Private Cloud) Fundamentals
  - Subnets
    - Public
      - Internet gateway + Route table + Public IP
    - Private
  - Internet gateway
  - Route table – *Public / Private*
  - Default Amazon VPCs
  - Elastic IP address (EIP)
  - Elastic network interface (+ *Security Group*)
  - NAT gateway
    - Connecting private subnets to the internet
    - Deploy a VPC across multiple Availability Zones
- VPC Traffic Security
  - Network ACLs (+ rules)
  - Security groups (+ chaining)

Module 4 – Compute

- EC2(Elastic Cloud Compute) Instances
  - Launch considerations
    - Name and tags
    - Application and OS Image – AMI
      - Prebuilt / AWS Marketplace / Custom
    - Instance type and size (+ AWS Compute Optimizer)
    - Key pair
    - Network and security
    - Storage
    - Placement and tenancy
      - Tenancy
        - Shared, Dedicated Instance, Dedicated Host
      - Placement groups
        - Cluster, Spread, Partition
    - Script and metadata
      - User data
      - Instance metadata
- Storage for EC2 instances
  - Amazon Elastic Block Store (Amazon EBS)
    - volume types
      - SSD (gp2, gp3, io1, io2, io2 Block Express)
      - HDD (st1, sc1)
  - Instance store volumes
- Amazon EC2 pricing options
  - On-Demand
  - Savings Plans – Compute / EC2 Instance
  - Spot Instances
- AWS Lambda

Module 5 – Storage

- Overview - Block / File / Object Storage
- Amazon S3(Simple Storage Service)
  - Securing objects
    - Access control
    - Bucket policies
    - Block Public Access
    - Access Points (+ policy)
    - Server-side encryption - SSE-S3 / SSE-KMS / SSE-C
  - Storing objects
    - Storage classes
      - S3 Standard / Standard IA / One Zone IA
      - S3 Glacier Instant / Flexible Retrieval
      - S3 Glacier Deep Archive
      - S3 Intelligent-Tiering
    - Versioning
    - Lifecycle policies
    - Replicating S3 objects
  - Additional Amazon S3 features
    - Multipart upload
    - Transfer Acceleration
    - Event notifications (+ Lambda)
- Shared File Systems
  - Amazon EFS(Elastic File System)
  - Amazon FSx
    - Amazon FSx for Windows File Server
    - Amazon FSx for Lustre
- Data migration tools
  - Offline
    - AWS Snow Family
      - Snowcone / Snowball Edge / Snowmobile
  - Online
    - AWS Storage Gateway
      - Volume gateway – *Cached / Stored*
      - Tape gateway
      - Amazon S3 File gateway
      - Amazon FSx File Gateway
    - DataSync (*to* S3, EFS, FSx)
    - AWS Transfer Family

Architecting on AWS – Key Concepts

Module 6 – Database Services

- Relational vs. Nonrelational databases
- Amazon RDS
  - Multi-AZ deployments
  - Read replicas
  - Data encryption at rest (+ AWS KMS)
- Aurora DB clusters
  - Aurora Serverless for PostgreSQL and MySQL
- DynamoDB
  - Tables – Item / Attribute / Partition key / Sort key
  - Capacity and scaling – Provisioned / On-Demand
  - Consistency options – Eventually / Strongly
  - Global tables
- Database caching
  - Caching strategies - Lazy loading / Write-through
  - Managing your cache
    - Cache validity (+ TTL) / Managing memory
  - ElastiCache – Memcached vs. Redis
  - DynamoDB Accelerator
- Database migration tools
  - AWS Database Migration Service (DMS)
  - AWS Schema Conversion Tool (SCT)

Module 7 – Monitoring and Scaling

- Monitoring
  - CloudWatch - Metric
  - Types of logs
    - Amazon CloudWatch Logs
    - AWS CloudTrail
    - VPC Flow Logs (*to* S3, CloudWatch Logs)
- Alarms and events
  - CloudWatch Alarms – OK / Alarm / Insufficient Data
  - Amazon EventBridge
- Load balancing
  - Types of load balancers – ALB / NLB / GWLB
  - Components – Target Group / Listener (+ *Rule*)
- Auto scaling
  - Types of auto scaling
    - AWS Auto Scaling – *EC2, DynamoDB, Aurora, etc*
    - Amazon EC2 Auto Scaling – *EC2*
      - Components
        - Launch templates
        - Auto Scaling group – Min / Max / Desired
        - Auto scaling policy
          - Invoke scaling with CloudWatch alarms
          - Ways to scale
            - Scheduled / Dynamic / Predictive
      - Optimize cost – On-Demand, Savings Plan / Spot

Module 8 – Automation

- CloudFormation (IaC)
  - Templates (JSON/YAML)- Using multiple templates
  - Stacks
- Infrastructure management
  - Elastic Beanstalk
  - AWS Solutions Library
  - AWS Cloud Development Kit (AWS CDK)
  - Systems Manager

Module 9 – Containers

- Microservices (vs. Monolithic)
- Containers (vs. virtual machines)
- Container services
  - Amazon ECR
  - Amazon ECS (+ EC2 or Fargate)
  - Amazon EKS (+ EC2 or Fargate)

Module 10 – Networking 2

- VPC endpoints (*without* IGW, NAT, public IP)
  - Gateway endpoint – *S3, DynamoDB*
  - Interface endpoint – *Access from on premises*
- VPC peering (No transitive)
- Hybrid networking
  - AWS Site-to-Site VPN (static / dynamic)
  - AWS Direct Connect(DX) (*only* dynamic)
- Transit Gateway
  - Components
    - Attachment
      - VPC / VPN connection
      - Direct Connect gateway
      - Transit Gateway Connect / Peering
    - Route table
  - + Full / Partial connectivity, Isolation

Module 11 – Serverless

- API Gateway
- Amazon SQS
  - Queue types - Standard / FIFO
  - Optimizing queue configurations
    - Visibility timeout
    - Polling type - Short polling / long polling
- Amazon SNS – Standard / FIFO
- Amazon Kinesis
  - Kinesis Data Streams
  - Kinesis Data Firehose
    - *to* Redshift, S3, OpenSearch
    - *to* HTTP endpoint, 3rd party service provider
  - Kinesis Data Analytics
- Step Functions
  - State machine (+ *Amazon States Language*)

Module 12 – Edge Services

- Amazon Route 53
  - public and private DNS
  - Routing policies
    - Failover / Geolocation / Geoproximity
    - Latency-based / Multivalue answer / Weighted
- Amazon CloudFront (+ AWS WAF / Shield)
  - Static or dynamic content
  - Components
    - Origins – S3 Bucket / ELB / Custom origin
    - Behaviors – Path pattern / TTL etc.
- DDoS protection
  - Shield Standard (*vs. Advanced*)
  - AWS WAF (+ WebACLs, Rule statements)
    - *to* CloudFront / ALB / API Gateway / AppSync
  - AWS Firewall Manager
    - + WAF / VPC SG / Shield / Network Firewall
- Outposts (42U rack, 1U/2U servers)

Module 13 – Backup and Recovery

- Disaster planning - RTO / RPO
  - Duplicate your storage – *S3, EBS, DataSync*
  - Configuring AMIs for recovery *(or Container Image)*
  - Failover network design – *Route 53, ELB, VPC, DX*
  - Database backup and replicas – *RDS, DynamoDB*
  - Templates and scripts – *CloudFormation, Scripts*
- AWS Backup
- Recovery strategies
  - Backup and restore
  - Pilot light
  - Fully working low-capacity standby
  - Multi-site active-active