AWS SysOps Cheat Sheet

V2020.10.31

(Dr Yan Xu)

Monitoring and Reporting

CloudWatch

1. Metrics:
   EC2, ELB, EBS, S3, RDS, Custom Metrics
2. Logstream:
   - Application (SDK), Load Balancer, AWS Lambda, ...
   - Expiration policies
   - S3 or ElasticSearch
3. Alarm:
   - fun(Metrics) -> ALARM?
   - Auto Scaling, EC2 Actions, SNS notifications
   - Evaluation period: 10 sec? 60 sec? 300 sec?
4. Events:
   - Source: AWS Resource, Crontab
   - Action: AWS Lambda, SQS/SNS/Kinesis
5. Dashboard (global)

Alternative 1: Grafana (open-source)
Alternative 2: Splunk

High Availability

Scalability

1. Vertical Scalability
2. Horizontal Scalability (critical)

Auto Scaling

1. Load Balancer (ALB - HTTP level, NLB - TCP/IP level)
2. Target Group
3. Auto Scaling Group (Minimum/Maximum/Desired/ScaleUp/ScaleDown)
4. Instance Launch Configuration (or template)
5. Health Check (ALB/NLB health check, EC2 health check)

1: ASG is not a must-have, instances could be attached to TG directly
2: ASG is attached to TG, not part of TG
3: ALB could enforce stickiness with cookies
4: ALB could direct traffic to *multiple* TGs based on rules (e.g. routes)
5: ELB needs a warming up in case of sudden spike of traffic
6: ELB provides SSL termination (HTTPS)
7: ELB metrics: Latency, Health Check, SurgeQueueLength, SpilloverCount
8: Each HTTP request has an added custom header: X-Amzn-Trace-Id

CloudFormation: Infrastructure as Code

Building Blocks

1. Resources (Type: AWS::aws-product-name::data-type-name)
2. Parameters
3. Mappings
4. Outputs
5. Conditionals

Grammar

1. Key value Pairs
2. Nested objects
3. Support Arrays, multi line strings and comments

Special Functions

- Fn::Ref, Fn::FindInMap , Fn::ImportValue
- Fn::GetAtt, Fn::Join, Fn::Sub
- Condition Functions (e.g. Fn::If, Fn::Not, Fn::Equals)

1: CFN-INIT could customize instance initialization script (e.g. install httpd), and its log is located /var/log/cfn-init.log and /var/log/cfn-init-cmd.log
2: CFN-SIGNAL could block CloudFormation until it receives a signal
3: For CFN changes, failures will trigger rollback to the last success stage

Storage

S3 (Simple Storage Service)

1. Buckets must have a globally unique name
2. Storage Classes:
   - Standard - General Purpose
   - Standard-Infrequent Access (IA)
   - Glacier (Vaults & Archive), etc
3. Lifecycle Rules: Transition & Expiration
4. Encryption:
   - SSE-S3, (AES-256)
   - SSE-KMS,
   - SSE-C, (HTTPS + the encryption key)
   - Client Side Encryption
5. Security (any one allow & no deny):
   - IAM policies (for user)
   - Bucket Policies
   - Bucket/Object Access Control List
6. Eventual Consistency Model
7. Versioning and MFA-Delete
8. Pre-signed URLs: default valid for 3600 seconds
9. AWS Storage Gateway

EBS (Elastic Block Store)

1. network drive
2. provisioned capacity (GB and IOPS)
3. Volume Types: GP2 (boot volumes), IO1 (boot volumes), ST1 and SC1
4. GP2: Max IOPS is 16,000, 3 IOPS per GB, means at 5,334GB we are at the max IOPS
5. EBS Snapshots and Migration
6. EBS Snapshots and Encryption

EFS (Elastic File System)

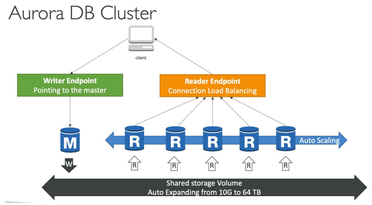
1. Highly available, scalable, expensive, pay per use

DataBase

RDS

1. Read Replicas (<=5)
2. Multi AZ replication (Disaster Recovery)
3. Backup and Snapshots
4. Security:
   - private subnet
   - security group
   - IAM policies
   - Username and password
5. Conditionals

Aurora



In-Memory DB

- ElastiCache (Redis or Memcached)

EC2 (Elastic Compute Cloud)

1. Virtualization
   - Hypervisor: Xen
2. Placement Groups
   - Cluster: low-latency
   - Spread: availability
   - Partition:
3. Instance Types:
   - R (RAM), C (CPU), M (balanced), I(I/O), G(GPU), T2/T3
4. Instance Launch Types:
   - On Demand Instances
   - Reserved (Reserved Instances, Convertible Reserved Instances, Scheduled Reserved Instances, etc)
   - Spot Instances
   - Dedicated Instances/Hosts
5. Burstable Instances (T2/T3)
6. Key Pair
7. Elastic IPs
8. Fleet Management: AWS Systems Manager
   - SSM Inventory - software list
   - Run Command
   - Session Manager (not use SSH access)
   - Patch Manager

Networking

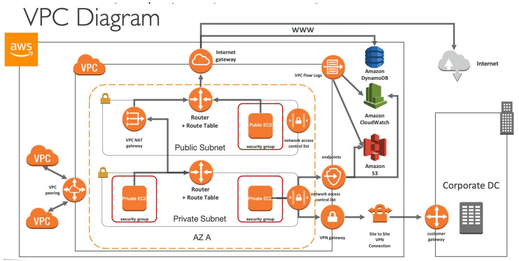
Route 53 (a Managed DNS)

1. common records
   - A: hostname to IPv4
   - AAAA: hostname to IPv6
   - CNAME: hostname to hostname
   - Alias: hostname to AWS resource
2. TTL (Time to Live)
3. Routing Policy
   - Simple Routing Policy
   - Multi Value Routing Policy (<=8)
   - Weighted Routing Policy (A/B Test)
   - Latency Routing Policy
   - Failover Routing Policy
   - Geolocation Routing Policy (require "default")

VPC (Virtual Private Cloud)

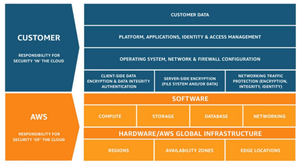
1. CIDR - IPv4 (Classless Inter-Domain Routing)
2. Private IP
   a. 10.0.0.0/8 <= in big networks
   b. 172.16.0.0/12 <= default AWS one
   c. 192.168.0.0/16 <= example: home networks
3. Default VPC
   a. all instances have public IP
   b. have internet connectivity
4. Internet Gateways & Route tables
5. NAT Instances & NAT Gateway
6. AWS DNS Server: 169.254.169.253
7. Network ACL (subnet) v.s. Security Group (instance)
   a. Default Network ACL allows all outbound and inbound
8. VPC Peering
9. VPC Endpoints
10. VPC Flow Log
11. Site to Site VPN
    a. a Customer Gateway on DC
    b. a Virtual Private Gateway on VPC
    c. a site-to-site VPN over public internet
12. Direct Connect

VPC Diagram



Security and Compliance

Shared Responsibility Model



Security

1. DDOS Attack
   - AWS Shield Standard
   - AWS Shield Advanced
2. AWS Web Application Firewall
   - E.g. IP addresses, HTTP headers
   - Deployed on CloudFront, ALB or API Gateway
3. AWS Inspector
   - Vulnerability analysis only for EC2 instances
4. Guard Duty (Protect AWS Account)
   - Using CloudTrail Logs, VPC Flow Logs and DNS Logs
5. Trusted Advisor
   - Cost Optimization, Performance, Service Limits, etc
6. KMS
7. Cloud HSM (FIPS 140-2 Level 3 compliance)
8. Multi Factor Authentication
9. STS – Security Token Service
   - to grant limited and temporary access to AWS resources
   - Cross Account Access
   - SAML Federation
   - AWS Cognito (for Public Applications)

Compliance

1. AWS Config: Track config changes and compliance against rules
2. AWS CloudTrail: Track API calls made by users within account
3. AWS Artifact: AWS compliance reports

Cost Management

1. AWS Billing Alarms (CloudWatch us-east-1)
2. AWS Cost Explorer and Cost Allocation Tags
3. AWS Organization and Service Control Policies
4. AWS Service Catalog
5. Pricing Model (selected service):
   - EC2 - instance running time
   - S3 - size & time
   - DynamoDB - data reads and writes
   - Route53 - Hosted Zones, DNS queries, Domain name
   - RDS (e.g. Postgres) - DB instance running time
   - CloudWatch - log size (e.g. $0.53 per GB)
   - Athena - data scanned (e.g. $5.00 per TB of data scanned)
   - QuickSight - per user/month
   - EMR - instances & EBS volumes
   - SQS - per request (e.g. $0.40 per million requests)