1 Fundamentals and Accounts

AWS Accounts - basics

AWS Account

- AWS account is container for identities (users) and ressources (services).
- It is a global entity, not bound to a region.
- It is the root of the AWS hierarchy.

Root user

- Root user is the first user created with the account, it uses the email that created the account.
- It has full access to all AWS services and resources and can't be restricted.
- It is recommended to create an IAM user for daily use and keep the root user for emergencies.

IAM

- IAM (Identity and Access Management) is a service that allows to manage users and permissions.
- IAM identites are created in the account and can be used to access AWS services of the account.
- IAM identities can be users, groups or roles.
- IAM identities have no permissions by default, permissions are granted by policies.
- IAM identities can be shared between accounts if needed but has to be specifically allowed.

AWS Fundamentals

Public vs private services

- **Public services** are in the AWS public zone and are accessible from the internet. To access a public service you still need the authentication and authorization to access the service.

- **Private services** are in the AWS private zone and are not accessible from the internet. VPC's are private unless otherwise specified (like the default VPC). To access a private service you need to be in the same VPC or have a VPC peering connection. In case of a hybrid cloud, you can use a VPN or Direct Connect to access the private services. (services a verifier)

AWS Global Infrastructure

- **Region**: A region is a geographical area that consists of two or more availability zones. Each region is a separate geographic area. Each region has multiple, isolated locations known as Availability Zones.

- **Availability Zone**: An Availability Zone is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region. Availability Zones are physically separated by a meaningful distance, many kilometers, from any other Availability Zone, although all are within 100 km of each other.

- **Edge Location**: Edge Locations are endpoints for AWS which are used for caching content. Typically this consists of CloudFront, Amazon's Content Delivery Network (CDN). Requests for content are automatically routed to the nearest edge location, so content is delivered with the best possible performance.

AWS Default VPC

- When you create an AWS account, you get a default VPC in each region. The default VPC is a logically isolated virtual network in the AWS cloud that is automatically created for your AWS account. The default VPC has a default subnet in each Availability Zone. You can create your own VPC and subnets if you want to.

- There can only be one default VPC per region, and they can be deleted and recreated from the console UI .

- The default VPC is a public VPC, meaning that the instances in the default VPC can access the internet. The default VPC has an internet gateway attached to it. The default VPC has a default security group attached to it. (The default security group allows all inbound traffic and all outbound traffic. You can create your own security groups if you want to.(a verifier))

- They always have the same IP range (IPv4 CIDR block: 172.31.0.0/16) and same '1 subnet per AZ' architecture.

EC2

- **Elastic Compute Cloud (EC2)** is AWS's implement of IAAS(Infrastructure as a service).

- It allows you to provision virtual machines known as instances with resources you select and an operating system of your choosing.

AMI

AMI (Amazon Machine Image) is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance.

AMI includes the following:

- One or more Amazon Elastic Block Store (Amazon EBS) snapshots, or, for instance-store-backed AMIs, a template for the root volume of the instance (for example, an operating system, an application server, and applications).
- Launch permissions that control which AWS accounts can use the AMI to launch instances.
- A block device mapping that specifies the volumes to attach to the instance when it's launched.

NOT stored in AMI:

- Instance Settings
- Network Settings

EXAM: What is NOT stored in an AMI? Instance and Network Settings

Root Volume: AMI contains boot volume of instance, boots O/S

S3

EXAM: Bucket name must be Globally Unique. Error where you can't create a bucket? Prolly not a unique name

EXAM: More bucket name restrictions: 3-63 characters, all lowercase, no underscores, not formatted like IP addresses

EXAM: Bucket limits: soft limit of 100 buckets per AWS account, hard limit of 1000 buckets (hard limit increased by connecting with Support). If you have more than 1000 users, you can't use 1 bucket per user, but you can use prefixes within a bucket to let multiple users use one bucket.

EXAM: Unlimited Objects in a bucket, ranging from 0 bytes to 5TB in size

EXAM: Object Structure: Key = Name, Value = Data

S3 Patterns and Anti-Patterns

- S3 is an Object Store system, NOT File System and NOT Block System
- S3 has no File System, it's flat. It's not Block storage, so you can't mount it as K:\ or /images
- Great for 'offload'
- S3 should be your default INPUT and/or OUTPUT to MANY AWS products

EXAM: Where to store data in AWS? S3 should be default answer

QUIZ: What is true of Simple Storage Service (S3)

- S3 is an AWS Public Service
- S3 is an Object Storage System
- Buckets can store an unlimited amount of data

CloudFormation

What makes a template? Components:

- All templates have a list of resources. This is the only mandatory item
- Description. Free text field for the author to provide details on template. (If you have AWSTemplateFormatVersion, Description MUST follow it in YAML/JSON)
- Metadata. Can control the UI (groupings, order, labels, descriptions), as well as other things (to be covered later)
- Parameters. Value parameters, default values, etc.
- Mappings. Create lookup tables.
- Conditions. Allows decision making in the template. Step 1 create condition, Step 2 use condition
- Outputs. Once template is finished it can present outputs like admin or setup adddress, instance ID

EXAM: In a CFN Template, if you have the AWSTemplateFormatVersion item, the Description MUST follow directly after in your YAML/JSON template file

CloudWatch

CloudWatch is a core supporting service within AWS which provides metric, log and event management services. Collects / manages operational data on your behalf.

Three jobs:

1. Metrics. AWS Products, Apps, on-premises. Some metrics require extra installed CloudWatch Agent
2. CloudWatch Logs. AWS Products, Apps, on-premises. Almost anything logged can be ingested by Logs
3. CloudWatch Events. AWS Services & Schedules. If an AWS service does something, this will generate an event that can perform another action. Or you can set up a chrono-repeating event through here.

Core Concepts

- Namespace: Container for monitoring data. There is a naming ruleset for naming. All AWS data foes into a special namespace AWS/[service]
- Metric: Collection of related data points in a time-ordered structure
- Datapoints: A single unit of a metric; consists of timestamp and a value
- Dimensions: Generally, a metric is a collection (Eg. CPU utilization comes from all EC2 instances, not just one). You can use dimensions to single out resources to see their individual metrics. "Separate datapoints for different things or perspectives within the same metric"
- Alarms: Taking actions based on metrics. States: OK or ALARM (ALARM can be SNS Notification or Action), and INSUFFICIENT DATA (when there's not yet enough data)

Route 53 Fundamentals

AWS's managed DNS product. Global service, single database; no need to pick region in console UI. Globally resilient.

R53: Two main services:

1. Register Domains
2. Host Zones... managed nameservers

R53: Architecture

Register domains. To do this, it has relationships with all major domain registries (.com, .io, .net, etc)

1. Check if domain available 2. Zone File created for registering domain (DNS DB for domain) 3. Allocates managed nameservers for this zone (usually 4). get nameserver records added to top level domain zone

R53: Zones

DNS Zones and Hosting for those zones. Hosted zone created if domain available (and allocates 4 NS's to host zone). HZ can be Public or Private (linked to VPCs, for sensitive DNS records). Hosted Zones stores records (recordsets).

DEMO: R53 Register Domain - animals4life.org

Search / Nav to R53 console > Registered Domains > click "Register Domains" > Search for domain > Select domain you want > Proceed to Checkout (choose duration, auto-renew) > fill out Contact Info > Pricing (up front cost + monthly hosted fee) > click "Submit" > await domain registry

- Transfer Lock: Security feature, domain can't be transferred away from R53 without disabling this lock
- If you delete and recreate HZ, you'll be allocated 4 new Name Servers (would need to update some stuff if you weren't using R5#)

DNS Record Types

- Nameserver Records (NS). Allows delegation to occur in DNS. Eg. .com zone
- A Records / AAAA Records. Map host names to IP addresses. A record = IPv4, AAAA = IPv6
- CNAME Record. Canonical name. Let's you create equivalent of DNS shortcuts; host-to-host records. CNAMEs reduce admin overhead.
- MX Record. For email. How a server can find the mail server (SMTP) for a specific domain.
- TXT Records. Add arbitrary text to a domain; add additional functionality. Eg. Prove domain ownership.

EXAM: CNAMEs cannot point directly at an IP address, only other names.

- QUIZ: What is a CloudFormation Logical Resource? A resource defined in a CFN Template
- QUIZ: How many DNS Root Servers Exist? 13
- QUIZ: Who manages DNS Root Servers? 12 Large Organizations
- QUIZ: Who manages DNS Root Zone? IANA
- QUIZ: A Record = IPv4, AAAA Record = IPv6
- QUIZ: DNS Record type is how the root zone delegates control of .org to the .org registry
- QUIZ: Which type of organization maintains the zones for a TLD (e.g .ORG)? Registry
- QUIZ: Which type of organization has relationships with the .org TLD zone manager allowing domain registration? - Registrar
- QUIZ: How many subnets in a default VPC? Equal to the number of Availability Zones in the region the VPC in located in

TTL - Time To Live

Numeric value that can be set on DNS records. Getting result from authoritative source is an authoritative answer. If a 3600 TTL value is set, results of query are stored in resolver server for 3600 seconds (1 hour), creating a non-authoritative answer for delivery -- during this time, another query would receive this cached non-authoritative answer.

- Low value means more queries against your server. High value less queries but less control
- TIP: If doing any work to change DNS values, it's recommended that you lower the TTL value in advance (days/weeks in advance)