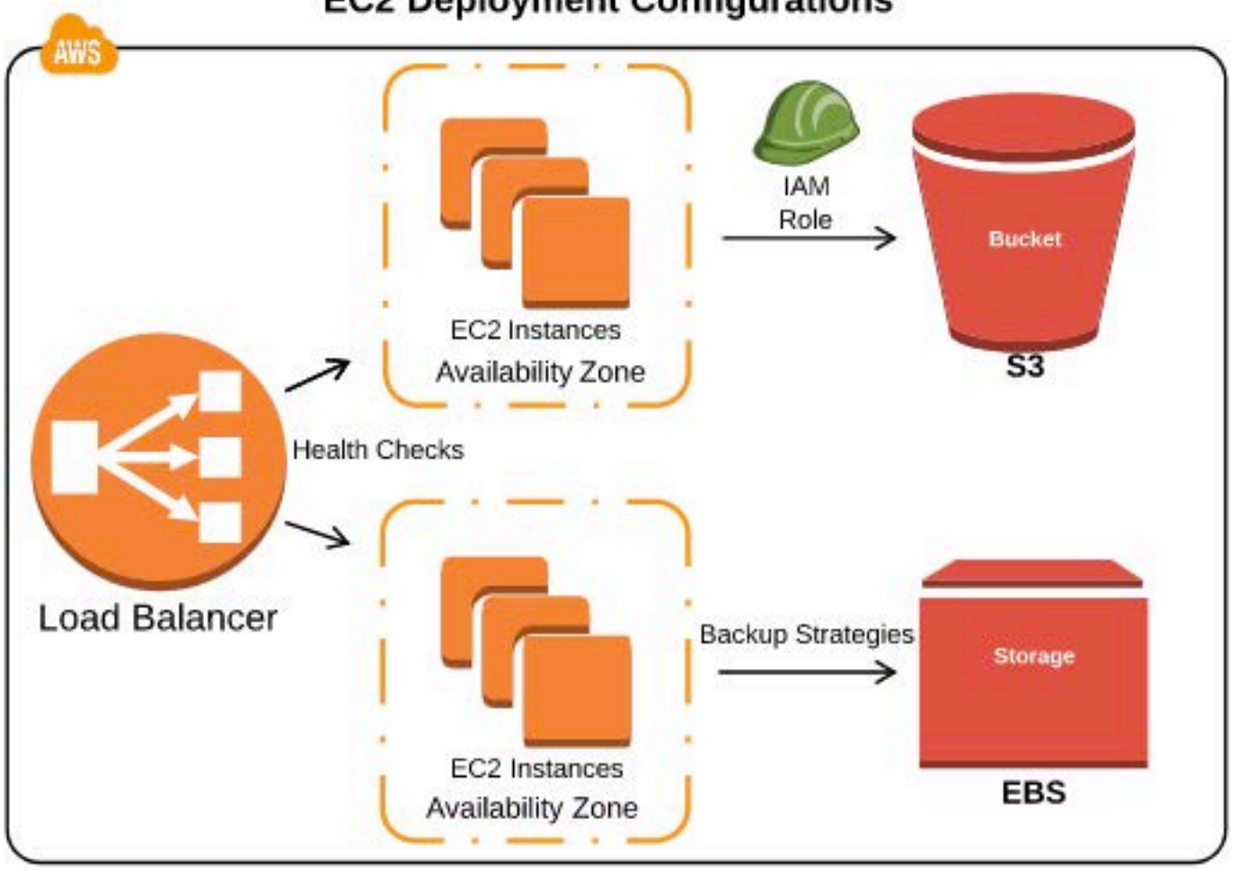
Choose a Topic

Deployment Concepts With EC2

Scenario:

A DevOps Engineer will be required to work with EC2 instances and a key task will be using various techniques to backup EC2 instances. Likewise, Elastic Load Balancers as a part of deployments will be a common tool in the DevOps Engineer's toolset. The ability to configure ELBs securely, with appropriate Health Checks, and to configure logging will be required both professionally and as a demonstrable skill on the DevOps Professional Certification exam.

EC2 Deployment Configurations



Choose a Topic

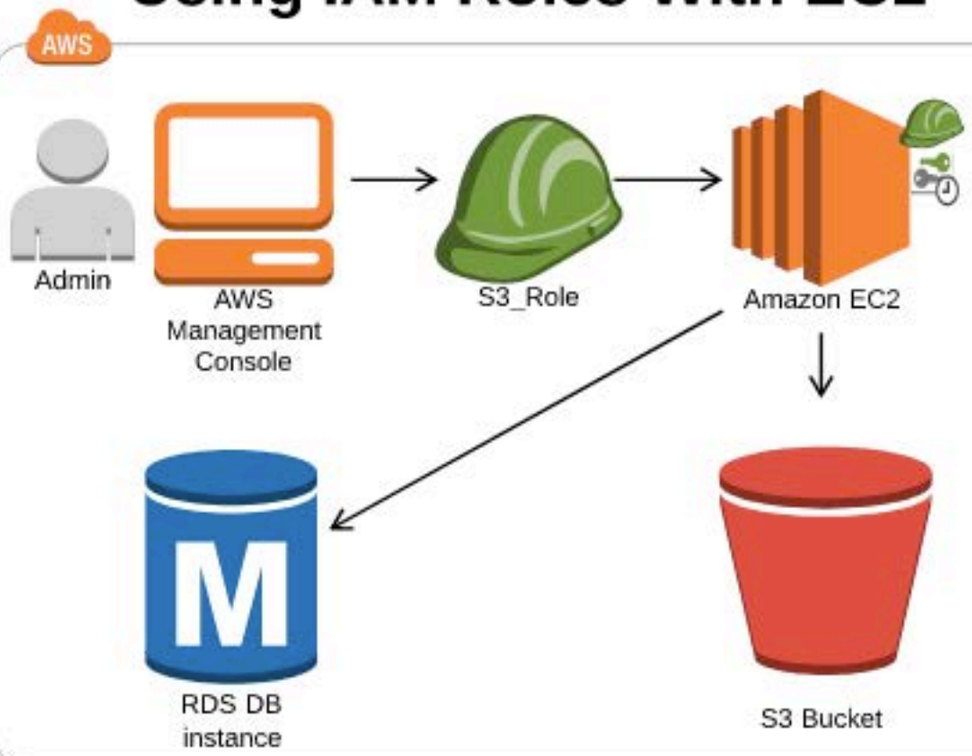
Deployment Concepts With EC2

Key Concepts

X

AWS

Using IAM Roles With EC2



IAM Roles For EC2

- Applications must sign their API requests with AWS credentials.
- Need a strategy for managing credentials for your applications that run on EC2 instances.
- IAM roles allow your applications to securely make API requests from your instances.

Steps To Configure IAM Roles For EC2

1. Create an IAM role.
2. Define which accounts or AWS services can assume the role.
3. Define which API actions and resources the application can use after assuming the role.
4. Specify the role when you launch your instance, or attach the role to a running or stopped instance.
5. Have the application retrieve a set of temporary credentials and use them.

Choose a Topic

Deployment Concepts With EC2

X

AWS

IAM Roles For EC2 Key Concepts

- Applications must sign their API requests with AWS credentials.
- Securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests.
- Protect your credentials from other users.
- You must also be able to update the credentials on each instance when you rotate your AWS credentials.
- IAM roles allow you to securely make API requests from your instances, without requiring you to manage the security credentials that the applications use.
- Use IAM roles to grant permissions to applications running on your instances that need to use a bucket in Amazon S3.
- Specify permissions for IAM roles by creating a policy in JSON format.
- If you change a role, the change is propagated to all instances.
- You cannot attach multiple IAM roles to a single instance, but you can attach a single IAM role to multiple instances.
- Amazon EC2 uses an *instance profile* as a container for an IAM role.
- When you create an IAM role using the IAM console, the console creates an instance profile automatically and gives it the same name as the role to which it corresponds.
- If you use the AWS CLI, API, or an AWS SDK to create a role, you create the role and instance profile as separate actions, with potentially different names.
- An application on the instance retrieves the security credentials provided by the role from the instance metadata item iam/security-credentials/*role-name*.
- These security credentials are temporary and are rotated automatically.
- To enable an IAM user to launch an instance with an IAM role or to attach or replace an IAM role for an existing instance, you must grant the user permission to pass the role to the instance:

  { "Effect": "Allow", "Action": "iam:PassRole", "Resource": "*" }

Common Use Cases:

- Store database credentials in S3. Use an IAM Role on an EC2 instance to retrieve the Database Credentials.
- Store temporary credentials in an S3 Bucket and utilize an IAM Role on EC2 to retrieve thos credentials.
- Storage of access keys in S3 and retrieval utilizing IAM Roles.
- Store configuration files for bootstrapping EC2 instances in S3. Retrieve the configuration files during bootstrapping using an IAM Role.

Choose a Topic

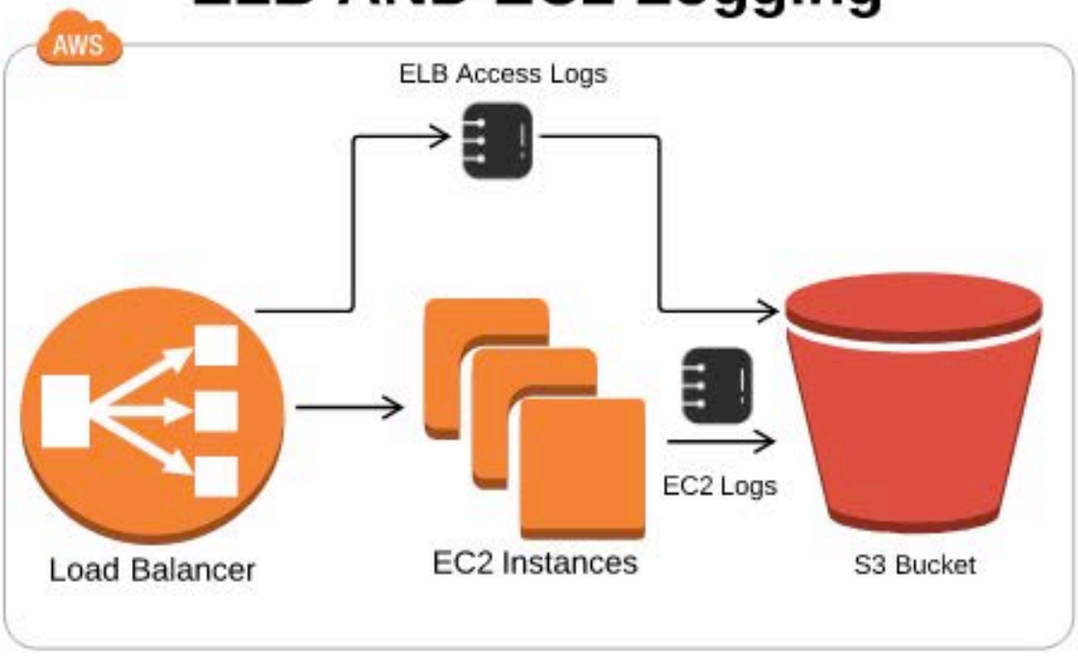
Deployment Concepts With EC2

Key Concepts

X

AWS

ELB AND EC2 Logging



Elastic Load Balancer Access Logs

- Access logs capture detailed information about requests sent to your load balancer.
- You can use these access logs to analyze traffic patterns and to troubleshoot issues.
- Access logging is an optional feature of ELB that is disabled by default.
- The logs are stored in an S3 bucket that you specify.
- There is no additional charge for access logs.

Steps To Enable Access Logs For Your Classic Load Balancer

1. Create an S3 Bucket.
2. Attach a Policy to Your S3 Bucket.
3. Enable Access Logs.
4. Verify that the Load Balancer Created a Test File in the S3 Bucket.

Choose a Topic

Deployment Concepts With EC2

X

AWS

ELB Logging Key Concepts

- Access Logs give detailed information about requests sent to the Load Balancer like:
  - Time the request was received
  - The client's IP Address
  - Request Paths
  - Server Responses
  - Latencies
- Access Logs turned off by Default
- Logs can be taken in intervals of 5 and 60 minutes
- Look at data from requests going to our applications such as:
  - Timestamp - when the Load Balancer received the request.
  - Client:port - IP Address and port of the requesting client.
  - Backend:port - IP Address and port of the instance that processed the request.
- Request Processing Time
  - HTTP - Total time it took from the ELB receiving the request until the request is sent to an instance.
  - TPC - Total time from the Load Balancer accepting a TCP/SSL connection to when it sent the first byte of data to an instance.
- Responsce Processing Time
- How to use Logging Data:
  - Process the data with Elastic Map Reduce or 3rd party tools
  - Feed the data into those tools and receive data back out

Choose a Topic

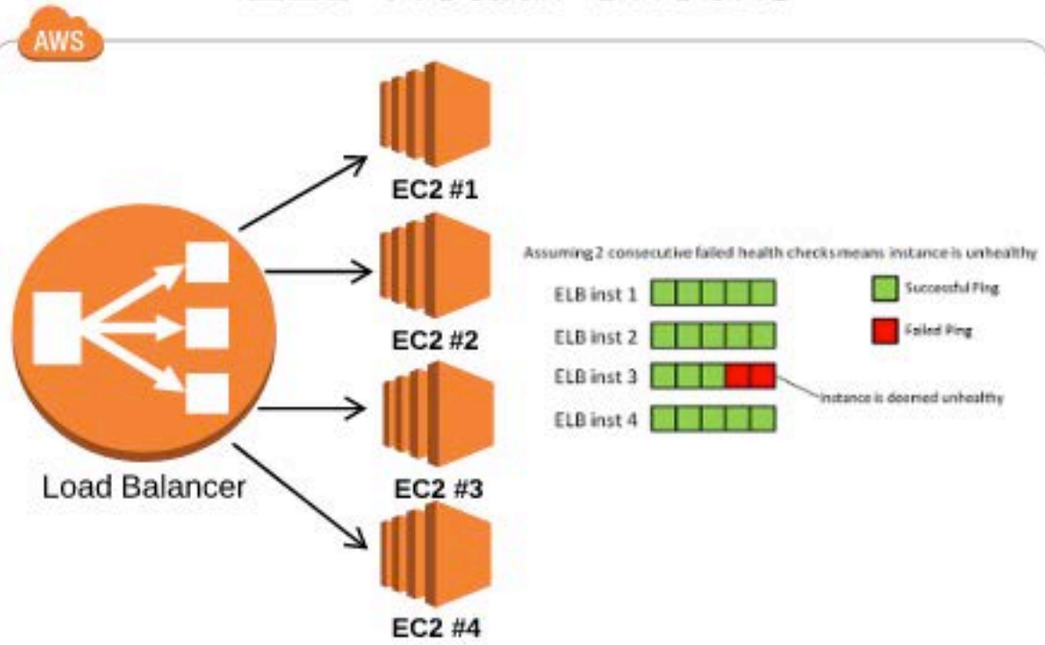
Deployment Concepts With EC2

Key Concepts

X

AWS

ELB Health Checks



Elastic Load Balancer Health Checks

- To discover the availability of your EC2 instances, an ELB periodically sends pings, attempts connections, sends requests to test EC2 instances.
- The status of the instances that are healthy at the time of the health check is InService.
- The status of any instances that are unhealthy at the time of the health check is OutOfService.
- The load balancer performs health checks on all registered instances, whether the instance is in a healthy state or an unhealthy state.

Steps To Use ELB Health Checks With Auto Scaling

1. Select your Auto Scaling Group
2. For Health Check Type, select ELB.
3. For Health Check Grace Period, enter 300.
4. Choose Save.
5. On the Instances tab, the Health Status column displays the results of the newly added health checks.

Choose a Topic

Deployment Concepts With EC2

X

AWS

ELB Health Check Key Concepts

- ELB periodically sends pings, attempts connections, or sends requests (Health Checks) to test the EC2 instances.
- Healthy instances have a status of InService, unhealthy instances have a status of OutOfService.
- The ELB performs Health Checks on ALL registered instances, but routes requests only to healthy instances. If an unhealthy instance is restored to a healthy state, the ELB will again route traffic to it.
- The load balancer checks the health of the registered instances using either the default health check configuration provided by ELB or a health check configuration that you configure.
- If you have associated your Auto Scaling group with a Classic load balancer, you can use the load balancer health check to determine the health state of instances in your Auto Scaling group.

ELB Health Check with Auto Scaling Groups

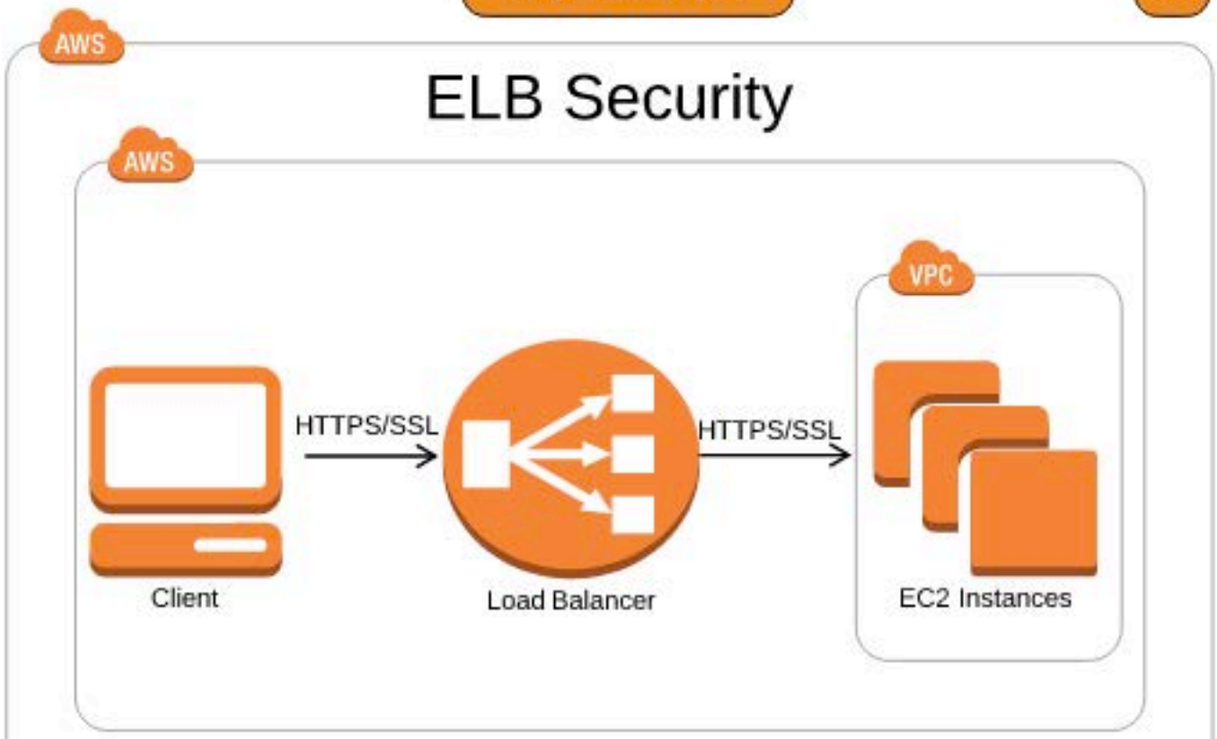
- An Auto Scaling group periodically checks the health status of each instance.
- It can use EC2 status checks only, or EC2 status checks plus Elastic Load Balancing health checks. If it determines that an instance is unhealthy, it replaces the instance.
- Using only EC2 status checks is the default for Auto Scaling Groups
- If you have attached one or more load balancers or target groups to the Auto Scaling group and a load balancer reports that an instance is unhealthy, it does not consider the instance unhealthy and therefore it does not replace it.
- If You configure your Auto Scaling group to determine health status using both EC2 status checks and Elastic Load Balancing health checks, it considers the instance unhealthy if it fails either the status checks or the health check.

Choose a Topic

Deployment Concepts With EC2

Key Concepts

X



Elastic Load Balancer Security

- ELB Listeners
  - Listeners check for connection requests.
  - Need to configure listeners for front-end clients to connect to, and for back-end clients to connect to.
  - Options are: HTTP or HTTPS, TCP or SSL
- HTTP /HTTPS and TCP/SSL differences
  - HTTP/HTTPS
    - Layer 7
    - Can analyze headers from requests
    - Use X-Forwarded-for header to get client IP Address
    - Can enable sticky sessions
  - TCP/SSL
    - Layer 4 (Transport Layer)
    - Proxy Protocol can be used to get client IP Address
    - Sticky Sessions can not be enabled
- If using HTTPS or SSL need to deploy an X.509 SSL certificate and also specify a Security Policy.

Choose a Topic

Deployment Concepts With EC2

X

AWS

ELB Security Key Concepts

- Can configure an ELB to have secure communications with front-end clients and back-end instances.
- ELB listeners check for connection requests. Options:
  - HTTP or HTTPS (Layer 7)
  - TCP or SSL (Layer 4)
  - Port 80 or 443 (typically)
- Configuring back-end authentication
  a. create a public key policy
  b. create a back-end instance authentication policy
  c. set the back-end instance authentication policy with the instance port and protocol
- Once configured, the ELB only communicates with an instance if it has a matching public key.

Choose a Topic

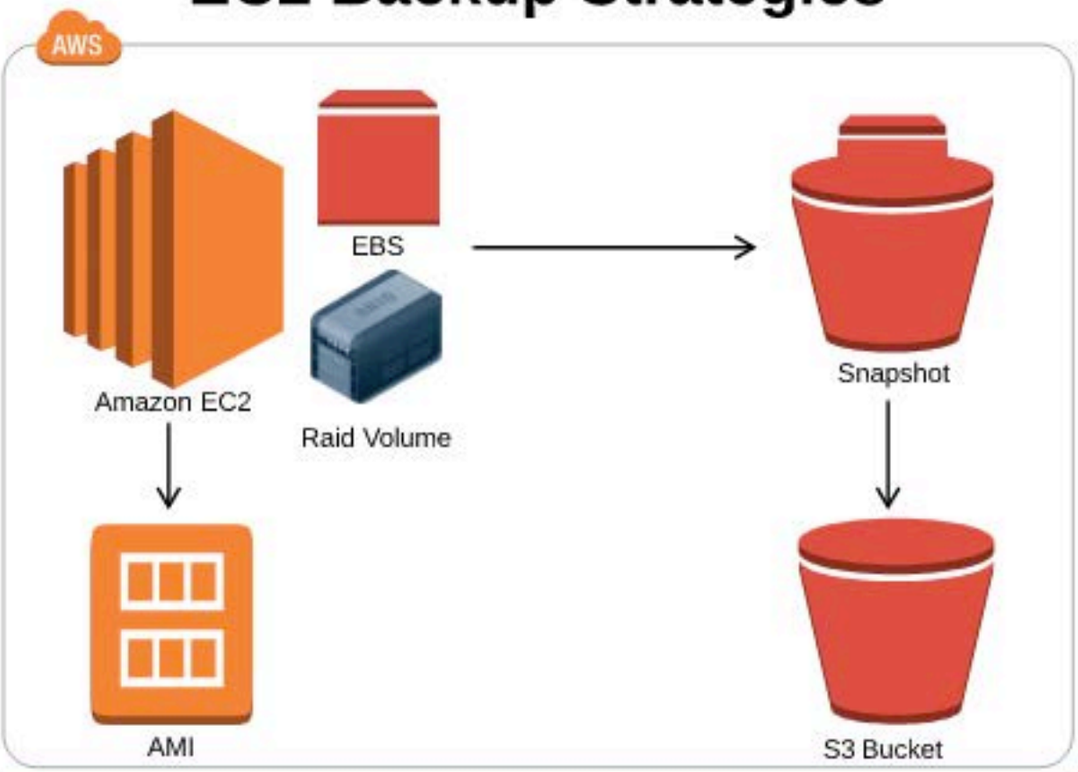
Deployment Concepts With EC2

Key Concepts

X

AWS

EC2 Backup Strategies



Backing Up EC2

- Considerations:
  - Backing up data on EBS volumes reliably and securely.
  - Backing up data on I/O intensive instances (Hot Backups).
  - Backing up data when using RAID volumes.
- EBS Volumes - Snapshots
  - Take point in time snapshots of EBS volumes.
  - Snapshots are stored on S3 making them very reliable.
  - Can also copy snapshots to other regions.
  - Snapshots can be create from API calls including SDKs,CLI, or Console.
  - The first snapshot copies the entire volume to S3, but subsequent snapshots are incremental and only stores block level changes since the last snapshot.
  - "Hot Backups" occur while the volume is performing I/O operations. When taking "Hot Backups" it is recommended to flush the cache and temporarily pause I/O operations.
- AMIs give us a baseline image from which we can build new instances.

Choose a Topic

Deployment Concepts With EC2

X

AWS

EC2 Backups - CLI Commands

- aws ec2 create-snapshot --volume-id vol-1234567890abcdef0 --description "This is my root volume snapshot."
- aws ec2 describe-snapshots --owner-ids 012345678910 --filters Name=status,Values=pending
- aws ec2 delete-snapshot --snapshot-id snap-1234567890abcdef0

Choose a Topic

CloudWatch For DevOps

Scenario: CloudWatch is an essential tool for the DevOps Engineer. CloudWatch supports the DevOps concepts of automation, communication, and collaboration, by giving access to monitoring and logging. CloudWatch metrics can be used to work with Elastic Load Balancers and determine the scaling actions of Auto Scaling Groups. Custom Metrics are a very powerful tool which allow the DevOps Engineer to leverage CloudWatch monitoring in a wide range of scenarios.

CloudWatch Deployment Configurations