Benefits:

- It automates the creation and renewal of private certificates for on-premises and AWS resources.
- It provides an easy process to create certificates. Just submit a CSR to a Certificate Authority, or upload and install the certificate once received.
- SSL/TLS provides data-in-transit security, and SSL/TLS certificates authorize the identity of sites and connections between browsers and applications.

Price details:

- The certificates created by AWS Certificate Manager for using ACM-integrated services are free.
- With AWS Certificate Manager Private Certificate Authority, monthly charges are applied for the operation of the private CA and the private certificates issued.

AWS Auto Scaling

What is AWS Auto Scaling?

- AWS Auto Scaling keeps on monitoring your Application and automatically adjusts the capacity required for steady and predictable performance.
- By using auto scaling it's very easy to set up the scaling of the application automatically with no manual intervention.
- It allows you to create scaling plans for the resources like EC2 Instances, Amazon EC2 tasks, Amazon DynamoDB, Amazon Aurora Read Replicas.
- It balances Performance Optimization and cost.

Terminologies related to AWS Autoscaling Groups:

Launch Configuration vs Launch Template

- EC2 Auto Scaling uses two types of instance configuration templates: launch configurations and launch templates.
- We recommend that you use launch templates to make sure that you're getting the latest features from Amazon EC2.
- For example, you must use launch templates to use Dedicated Hosts, which enable you to bring your eligible software licenses from vendors, including Microsoft, and use them on EC2.
- If you intend to use a launch configuration with EC2 Auto Scaling, be aware that not all Auto Scaling group features are available.
- If you want to launch on-demand and spot both instances you have to choose a launch template.

Auto Scaling Lifecycle Hooks:

- The Lifecycle hook will pause your EC2 instance.
- The paused instances will remain in the wait state until the action is completed.
- The Wait state will remain active till the timeout period ends.

Monitoring:

- **Health Check:** Keep on checking the health of the instance and remove the unhealthy instance out of Target Group.
- **CloudWatch Events:** AutoScaling can submit events to Cloudwatch for any type of action to perform in the autoscaling group such as a launch or terminate an instance.
- **CloudWatch Metrics:** It shows you the statistics of whether your application is performing as expected.
- **Notification Service:** Autoscaling can send a notification to your email if the autoscaling group launches or the instance gets terminated.

Charges:

- AWS will not charge you additionally for the Autoscaling Group.
- You will be paying for the AWS Resources that you will use.

AWS CloudFormation

What is AWS CloudFormation?
AWS CloudFormation is a service that collects AWS and third-party resources and manages them throughout their life cycles, by launching them together as a stack.

A template is used to create, update, and delete an entire stack as a single unit, without managing resources individually.

It provides the capability to reuse the template to set the resources easily and repeatedly.

It can be integrated with AWS IAM for security. It can be integrated with CloudTail to capture API calls as events.

Templates - A JSON or YAML formatted text file used for building AWS resources.

Stack - It is a single unit of resources.

Change sets - It allows checking how any change to a resource might impact the running resources.

Stacks can be created using the AWS CloudFormation console and AWS Command Line Interface (CLI).

Stack updates: First the changes are submitted and compared with the current state of the stack and only the changed resources get updated.

There are two methods for updating stacks:

- **Direct update** - when there is a need to quickly deploy the updates.
- **Creating and executing change sets** - they are JSON files, providing a preview option for the changes to be applied.

StackSets are responsible for safely provisioning, updating, or deleting stacks.

Nested Stacks are stacks created within another stack by using the AWS::CloudFormation::Stack resource.

When there is a need for common resources in the template, Nested stacks can be used by declaring the same components instead of creating the components multiple times. The main stack is termed as parent stack and other belonging stacks are termed as child stack, which can be implemented by using ref variable '! Ref'.

AWS CloudFormation Registry helps to provision third-party application resources alongside AWS resources. Examples of third-party resources are incident management, version control tools.

Price details:

- AWS does not charge for using AWS CloudFormation, charges are applied for the services that the CloudFormation template comprises.
- AWS CloudFormations supports the following namespaces: AWS::*, Alexa::*, and Custom::*. If anything else is used except these namespaces, charges are applied per handler operation.
- Free tier - 1000 handler operations per month per account
- Handler operation - $0.0009 per handler operation

Example: CloudFormation template for creating EC2 instance

```
EC2Instance:
    Type: AWS::EC2::Instance
    Properties:
        ImageId: 1234xyz
        KeyName: aws-keypair
        InstanceType: t2.micro
        SecurityGroups:
            - !Ref EC2SecurityGroup
BlockDeviceMappings:
    - DeviceName: /dev/sda1
      Ebs:
          VolumeSize: 50
```

AWS CloudTrail

What is AWS CloudTrail?
AWS CloudTrail is defined as a global service that permits users to enable operational and risk auditing of the AWS account.

It allows users to view, search, download, archive, analyze, and respond to account activity across the AWS infrastructure.

It records actions as an event taken by a user, role, or an AWS service in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

AWS CloudTrail mainly integrates with:

- Amazon S3 can be used to retrieve log files.
- Amazon SNS can be used to notify about log file delivery to the bucket with Amazon Simple Queue Service (SQS).
- Amazon CloudWatch for monitoring and AWS Identity and Access Management (IAM) for security.

CloudTrail events of the past 90 days recorded by CloudTrail can be viewed in the CloudTrail console and can be downloaded in CSV or JSON file.

Trail log files can be aggregated from multiple accounts to a single bucket and can be shared between accounts.

AWS CloudTrail Insights enables AWS users to identify and respond to unusual activities of API calls by analyzing CloudTrail management events.

There are three types of CloudTrail events:

- Management events or control plane operations
    - Example - Amazon EC2 *CreateSubnet* API operations and CreateDefaultVpc API operations
- Data events
    - Example - S3 Bucket *GetObject*, *DeleteObject*, and *PutObject* API operations
- CloudTrail Insights events (unusual activity events)
    - Example - Amazon S3 *deleteBucket* API, Amazon EC2 *AuthorizeSecurityGroupIngress* API

Example of CloudTrail log file:
IAM log file -
The below example shows that the IAM user Rohit used the AWS Management Console to call the AddUserToGroup action to add Nayan to the administrator group.

```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "PR_ID",
        "arn": "arn:aws:iam::210123456789:user/Rohit",
        "accountId": "210123456789",
        "accessKeyId": "KEY_ID",
        "userName": "Rohit"
    },
```

"eventTime": "2021-01-24T21:18:50Z",
"eventSource": "iam.amazonaws.com",
"eventName": "CreateUser",
"awsRegion": "ap-south-2",
"sourceIPAddress": "176.1.0.1",
"userAgent": "aws-cli/1.3.2 Python/2.7.5 Windows/7",
"requestParameters": {"userName": "Nayan"},
"responseElements": {"user": {
"createDate": "Jan 24, 2021 9:18:50 PM",
"userName": "Nayan",
"arn": "arn:aws:iam::128x:user/Nayan",
"path": "/",
"userId": "12xyz"
}}
}]}

CloudWatch monitors and manages the activity of AWS services and resources, reporting on their health and performance. Whereas, CloudTrail resembles logs of all actions performed inside the AWS environment.

Price details:

- Charges are applied based on the usage of Amazon S3.
- Charges are applied based on the number of events analyzed in the region.
- The first copy of Management events within a region is free, but charges are applied for additional copies of management events at $2.00 per 100,000 events.
- Data events are charged at $0.10 per 100,000 events.
- CloudTrail Insights events provide visibility into unusual activity and are charged at $0.35 per 100,000 write management events analyzed.

Amazon CloudWatch

What is Amazon CloudWatch?
Amazon CloudWatch is a service that helps to monitor and manage services by providing data and actionable insights for AWS applications and infrastructure resources.

It monitors AWS resources such as Amazon RDS DB instances, Amazon EC2 instances, Amazon DynamoDB tables, and, as well as any log files generated by the applications.

Amazon CloudWatch can be accessed by the following methods:

- Amazon CloudWatch console
- AWS CLI
- CloudWatch API
- AWS SDKs

Amazon CloudWatch is used together with the following services:

- Amazon Simple Notification Service (Amazon SNS)
- Amazon EC2 Auto Scaling
- AWS CloudTrail
- AWS Identity and Access Management (IAM)

It collects monitoring data in the form of logs, metrics, and events from AWS resources, applications, and services that run on AWS and on-premises servers. Some metrics are displayed on the home page of the CloudWatch console. Additional custom dashboards to display metrics can be created by the user.

Alarms can be created using CloudWatch Alarms that monitor metrics and send notifications or make automatic changes to the resources based on actions whenever a threshold is breached.

CloudWatch console provides Cross-account functionality which provides cross-account visibility to the dashboards, alarms, metrics, and dashboards without Sign-in and Sign-out of different accounts. This functionality becomes more useful if the accounts are managed by AWS Organizations.

CloudWatch Container Insights are used to collect and summarize metrics and logs from containerized applications. These Insights are available for Amazon ECS, Amazon EKS, and Kubernetes platforms on Amazon EC2.

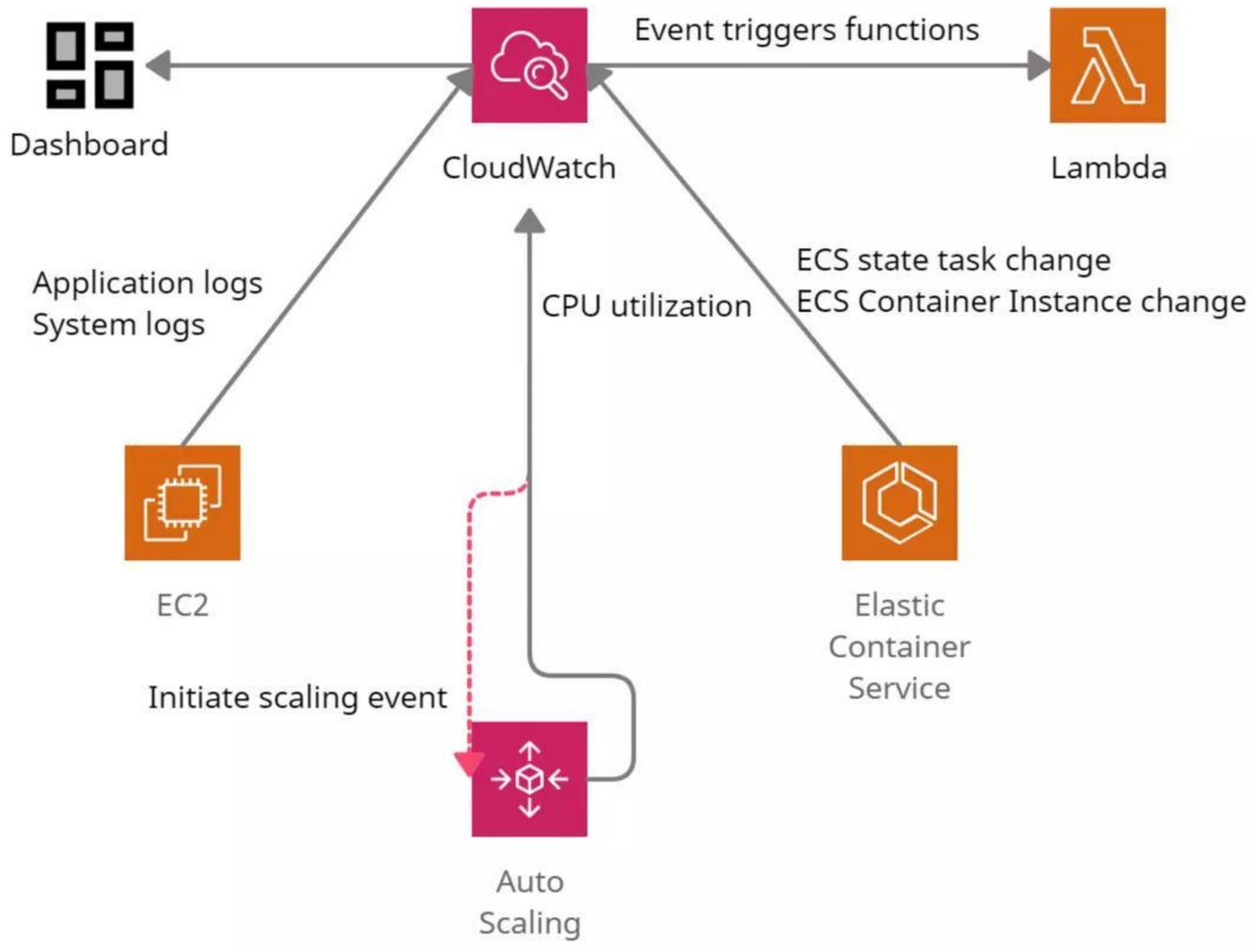
CloudWatch Lambda Insights are used to collect and summarize system-level metrics including CPU time, memory, disk, and network for serverless applications running on AWS Lambda.

CloudWatch agent is installed on the EC2 instance to provide the following features:

- It collects system-level metrics from Amazon EC2 instances or on-premises servers across operating systems.
- It collects custom metrics from the applications using the StatsD and collectd protocols.

StatsD - supported on both Linux servers and Windows Server
collectd - supported only on Linux servers.

- The metrics from the CloudWatch agent can be collected and stored in CloudWatch just like any other CloudWatch metrics.
- The default namespace for the CloudWatch agent metrics is CWAgent, and can be changed while configuring the agent.



Amazon CloudWatch in action

AWS Config

What is AWS Config?
AWS Config is a service that continuously monitors and evaluates the configurations of the AWS resources (services).

It helps to view configuration changes performed over a specific period of time using AWS Config console and AWS CLI.

It evaluates AWS resource configurations based on specific settings and creates a snapshot of the configurations to provide a complete inventory of resources in the account.

It retrieves previous configurations of resources and generates notifications whenever a resource is created, modified, or deleted.

It uses Config rules to evaluate configuration settings of the AWS resources. AWS Config also checks any condition violation in the rules. There can be 150 AWS Config rules per region.

- Managed Rules
- Custom Rules

It is integrated with AWS IAM, to create permission policies attached to the IAM role, Amazon S3 buckets, and Amazon Simple Notification Service (Amazon SNS) topics.

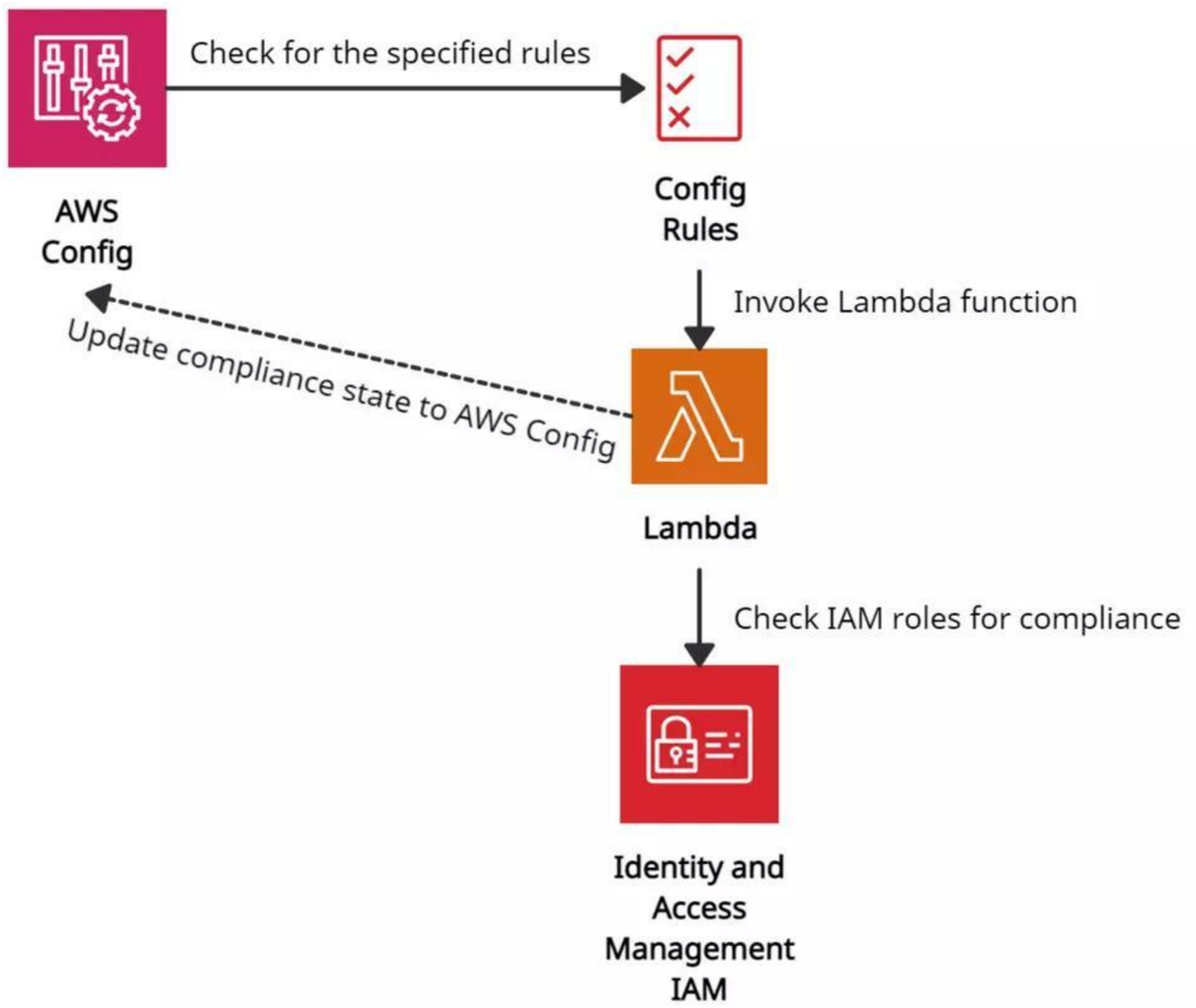
It is also integrated with AWS CloudTrail, which provides a record of user actions or an AWS Service by capturing all API calls as events in AWS Config.

AWS Config provides an aggregator (a resource) to collect AWS Config configuration and compliance data from:

- Multiple accounts and multiple regions.
- Single account and multiple regions.
- An organization in AWS Organizations
- The Accounts in the organization which have AWS Config enabled.

Use Cases:

- It enables the user to code custom rules in AWS Lambda that define the best guidelines for resource configurations. Users can also automate the assessment of the resource configuration changes to ensure compliance and self-governance across your AWS infrastructure.
- Data from AWS Config allows users to continuously monitor the configurations for potential security weaknesses. After any security alert, Config allows the user to review the configuration history and understand the risk factor.



AWS Config in action

Price details:

- Charges are applied based on the total number of configuration items recorded at the rate of $0.003 per configuration item recorded per AWS Region in the AWS account.
- For Config rules, charges are applied based on the number of AWS Config rules evaluated.
- Additional charges are applied if AWS Config integrates with other AWS Services at a standard rate.

AWS License Manager

What is AWS License Manager?

- AWS License Manager is a service that manages software licenses in AWS and on-premises environments from vendors such as Microsoft, SAP, Oracle, and IBM.
- It supports Bring-Your-Own-License (BYOL) feature which means that users can manage their existing licenses for third-party workloads (Microsoft Windows Server, SQL Server) to AWS.
- It enables administrators to create customized licensing rules that help to prevent licensing violations (using more licenses than the agreement).
- The rules operate by stopping the instance from launching or by notifying administrators about the infringement (violation of a law).
- Administrators use rule-based controls on the consumption of licenses, to set limits on new and existing cloud deployments.
- **Hard limit** - does not allow the launch of non-compliant instances
- **Soft limit** - allow the launch of non-compliant instance but sends an alert to the administrators
- It provides control and visibility of all the licenses to the administrators with the help of the AWS License Manager dashboard.
- It allows administrators to specify Dedicated Host management preferences for allocation and capacity utilization.
- AWS License Manager's managed entitlements provide built-in controls to software vendors (ISVs) and administrators so that they can assign licenses to approved users and workloads.
- AWS Systems Manager can manage licenses on physical or virtual servers hosted outside of AWS using AWS License Manager.
- AWS Systems Manager helps to discover software running on existing EC2 instances and then rules can be attached and validated in EC2 instances allowing the licenses to be tracked using the License Manager's dashboard.
- AWS Organizations along with AWS License Manager helps to allow cross-account disclosure of computing resources in the organization by using service-linked roles and enabling trusted access between License Manager and Organizations.

AWS License Manager is integrated with the following services:

- AWS Marketplace
- Amazon EC2
- Amazon RDS
- AWS Systems Manager
- AWS Identity and Access Management (IAM)
- AWS Organizations
- AWS CloudFormation
- AWS X-Ray

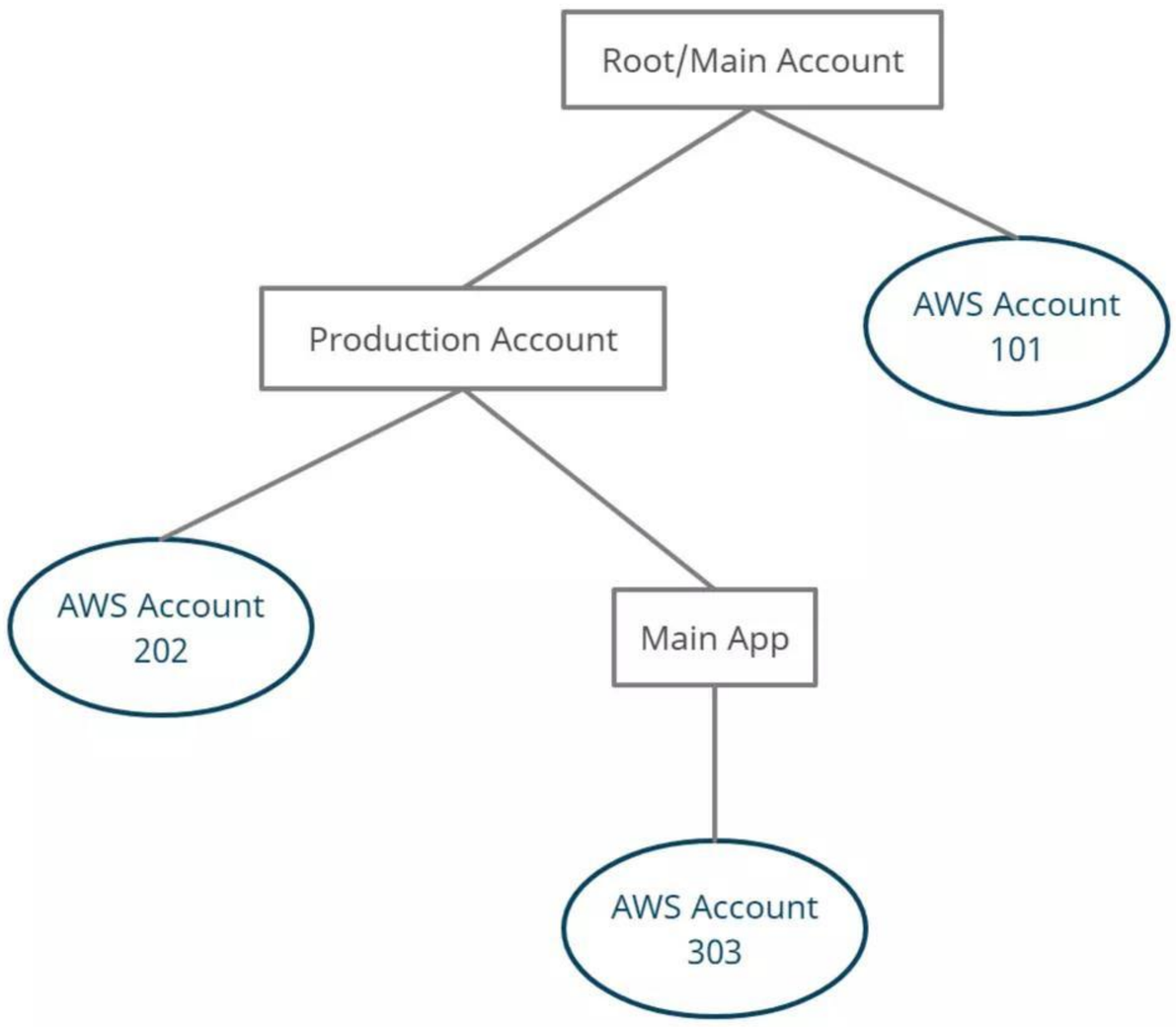
Price details:

- Charges are applied at normal AWS rates only for the AWS resources integrated with AWS License Manager.

AWS Organizations

What are AWS Organizations?
AWS Organizations is a global service that enables users to consolidate and manage multiple AWS accounts into an organization.
It includes account management and combined billing capabilities that help to meet the budgetary, and security needs of the business better.

- The main account is the management account – it cannot be changed.
- Other accounts are member accounts that can only be part of a single organization.



AWS Organizations flow

AWS Organizations can be accessed in the following ways:

- AWS Management Console
- AWS Command Line Tools
    - AWS Command Line Interface (AWS CLI)
    - AWS Tools for Windows PowerShell.
- AWS SDKs
- AWS Organizations HTTPS Query API

Features:

- AWS Organizations provides security boundaries using multiple member accounts.
- It makes it easy to share critical common resources across the accounts.
- It organizes accounts into organizational units (OUs), which are groups of accounts that serve specified applications.
- Service Control Policies (SCPs) can be created to provide governance boundaries for the OUs. SCPs ensure that users in the accounts only perform actions that meet security requirements.

- Cost allocation tags can be used in individual AWS accounts to categorize and track the AWS costs.
- It integrates with the following services:
    - AWS CloudTrail - Manages auditing and logs all events from accounts.
    - AWS Backup - Monitor backup requirements.
    - AWS Control Tower - to establish cross-account security audits and view policies applied across accounts.
    - Amazon GuardDuty - Managed security services, such as detecting threats.
    - AWS Resource Access Manager (RAM) - Can reduce resource duplication by sharing critical resources within the organization.
- Steps to be followed for migrating a member account:
    - Remove the member account from the old Organization.
    - Send an invitation to the member account from the new Organization.
    - Accept the invitation to the new Organization from the member account.

Price details:

- AWS Organizations is free. Charges are applied to the usage of other AWS resources.
- The management account is responsible for paying charges of all resources used by the accounts in the organization.
- AWS Organizations provides consolidated billing that combines the usage of resources from all accounts, and AWS allocates each member account a portion of the overall volume discount based on the account's usage.

AWS Systems Manager

What is AWS Systems manager?

AWS Systems Manager is a service which helps users to manage EC2 and on-premises systems at scale. It not only detects the insights about the state of the infrastructure but also easily detects problems as well.

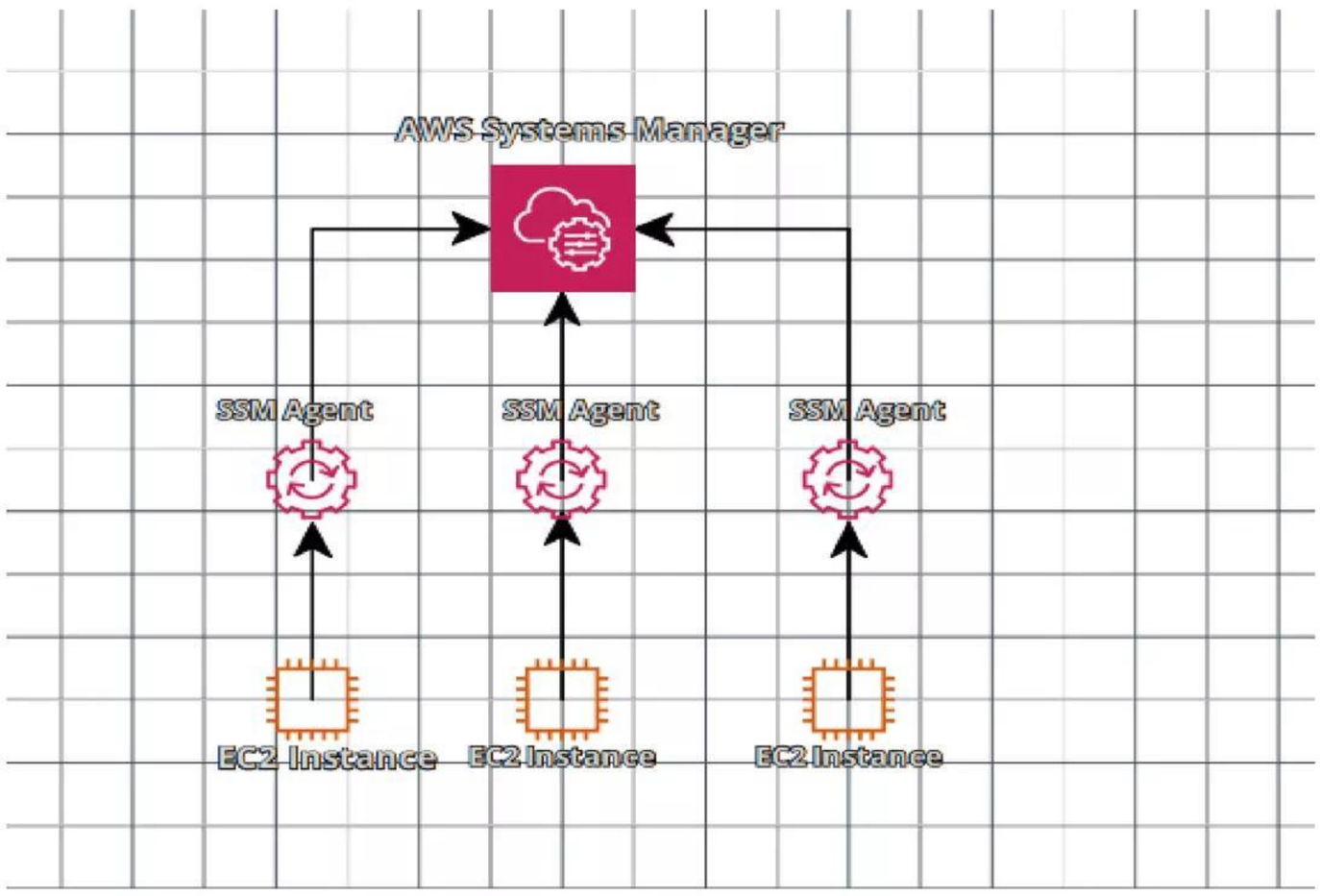
Additionally, we can patch automation for enhanced compliance. This AWS service works for both Windows and Linux operating systems.

Features:

- Easily integrated with CloudWatch metrics/dashboards and AWS Config.
- It helps to discover and audit the software installed.
- Compliance management
- We can group more than 100 resource types into applications, business units, and environments.
- It helps to view instance information such as operating system patch levels, install software and see the compliance with the desired state.
- Act associate and configurations with resources and find out the discrepancies.
- Distribute multiple software versions safely across the instances.
- Increase the security area by running a command or maintaining scripts.
- Patch your instances of schedule to keep them compliant.
- Helps managers to automate workflows.
- It helps to reduce errors by securely applying configurable parameters into centralized service.

How does the System Manager work?

Firstly, User needs to install the SSM agent on the system they control. If an instance can’t be controlled with SSM, it’s probably an issue with the SSM agent. Also, we need to make sure all the EC2 instances have a proper IAM role to allow SSM actions.



Pricing:

- App Config:
    - Get Configuration API Calls: $0.2 per 1M Get Configuration calls
    - Configurations Received: $0.0008 per configuration received
- Parameter Store:
    - Standard: No additional charge.
    - Advanced: $0.05 per advance parameter per month.
- Change Manager:
    - Number of change requests: $0.296 per change request.
    - Get, described, Update, and GetoptsSummary API requests: $0.039 per 1000 requests.

AWS CodeBuild

What is AWS CodeBuild?

Amazon codeBuild is a fully managed continuous integration service that helps developers to build and run test code rapidly. This service also provides test artifacts with great efficiency.

This gives an advantage to developers/DevOps engineers not to wait in long build queues, scaling, configuring, and maintaining build service. AWS CodeBuild runs continuously and avoids the wait time for concurrent jobs. Additionally, users pay only for the build time they use. In other words, the ideal time won't be counted in billing time for the user.

Features:

1. Easy to Set up – Amazon CodeBuild is easy to set up for the developers. Either they can build their code build environment or use one of the preconfigured environments.
2. It works with existing tools such as Jenkins plugin, GIT, etc.
3. It can scale automatically with several concurrent builds.
4. Automated Build: Developers need to configure builds once and whenever there is a code change, CodeBuild service will automatically run and generate the test results.
5. Pay as you go which means developers are only charged for the time it takes to complete the build, idle time won't be considered in billing.

Pricing:

Pricing will be computed based on the build minutes. The first 100 minutes of the build are free and then the rest will be charged based on each instance type usage.

AWS CodeCommit

What Is AWS CodeCommit?
AWS CodeCommit is a version control service hosted by Amazon Web Services that users can use privately to store and manage assets (such as documents, source code, and binary files) in the cloud.

In other words, AWS provides the service which allows you to just store the code or any assets without worrying about the version control like other version control tools such as Bitbucket, GitHub, etc. AWS manages everything on its own and takes full responsibility for scaling its infrastructure.

Features:

- Ensures High secure code (encrypted) with any type of code.
- Collaborative work (users can access the same piece of code with different IAM users and different security groups).
- Easy scalability.
- Easy to integrate with third-party groups.

Pricing:
AWS CodeCommit provides free tier term for the first 5 active users for the below configurations:
First 5 active user receives:

- Unlimited repositories
- 50 GB storage
- 10K Git requests/month

Additional active user beyond the first 5 users:

- Unlimited repositories
- 10 GB storage
- 2K Git requests/month

There will be additional charges for additional storage or an increase in GIT requests if increased.

AWS CodeDeploy

What is AWS CodeDeploy?
AWS CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances, on-premises instances, serverless Lambda functions, or Amazon ECS services.

Below type of deployments can be done using AWS CodeDeploy service:

- Code, Serverless Lambda Functions.
- Web & Configuration Files
- Executables and Packages.
- Scripts and Multimedia.

Following are components that concerns AWS CodeDeploy Service:

- Compute Platform
- Deployment Types & Groups.
- IAM & Service Roles
- Applications.

How does AWS CodeDeploy work?
It is divided into 3 parts. There might be multiple versions available for your application. First, the developer has to finalize the application revision which needs to be deployed. Then deployment configuration needs to be finalized. This is an app specification file(YML extension) that contains information such as source/destination location etc. and the last part is, deploy the appropriate revision to cloud location which is called deployment group.

Features:

- Help to release new features rapidly.
- It supports avoiding downtime during application deployment by maximizing application availability and handles all application complexity.
- It allows easy launch and tracking of application status.

Pricing:

- Free code deployment to Amazon EC2 or AWS Lambda.
- $0.02 charges per on-premises instance deployment.

AWS X-Ray

What is AWS X-Ray?
AWS X-Ray helps to analyze and debug production systems in distributed environments. AWS X-Ray is a method used to profile and monitor applications, mostly built using microservice architecture.

Using X-Ray service features, it's very easy for a user to troubleshoot and find the root cause of slowness of the system, including other performance-related errors.

X-Ray components:

- Daemon: a unique application that collects related segment data.
- Segments: provides resource names, requests information.
- Subsegments: This provides granular details about downstream calls.
- Service Graph: Visual representation of micro-service response or failure.
- Traces: Collects all segments created from a single request.
- Sampling: Algorithm which decides which request needs to be traced.
- Filter Expressions: easier to deep dive to understand the particular path.

Features:

- Supports all language (Go, NodeJS, Ruby, Java, Phyton, ASP.NET, PHP)
- It supports AWS service integration with Lambda, API Gateway, App Mesh, CloudTrail, CloudWatch, AWS Config, EB, ELB, SNS, SQS, EC2, ECS, Fargate.
- Helps in improving application performance.
- Easy to discover application issues with insights provided by X-Ray.
- It helps in tracking user requests as they travel through the entire application.

Pricing:

- Traces recorded/retrieved/scanned will cost $.50 per 1 million requests beyond the free tier.

AWS Database Migration Service

What is AWS Database Migration Service?
AWS Database Migration Service is a cloud service used to migrate relational databases from on-premises, Amazon EC2, or Amazon RDS to AWS securely. It does not stop the running application while performing the migration of databases, resulting in downtime minimization.

It performs homogeneous as well as heterogeneous migrations between different database platforms.

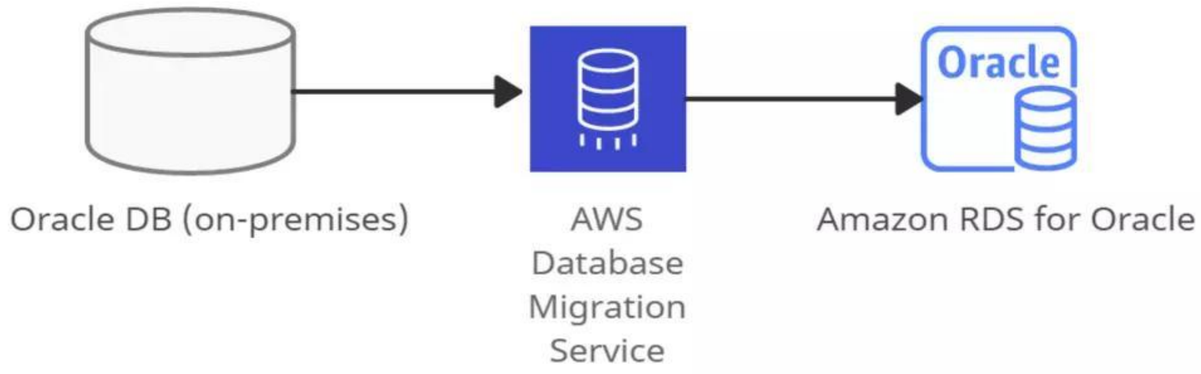
MySQL - MySQL (homogeneous migration)
MySQL - Amazon Aurora (heterogeneous migration)

AWS DMS supports the following data sources and targets engines for migration:

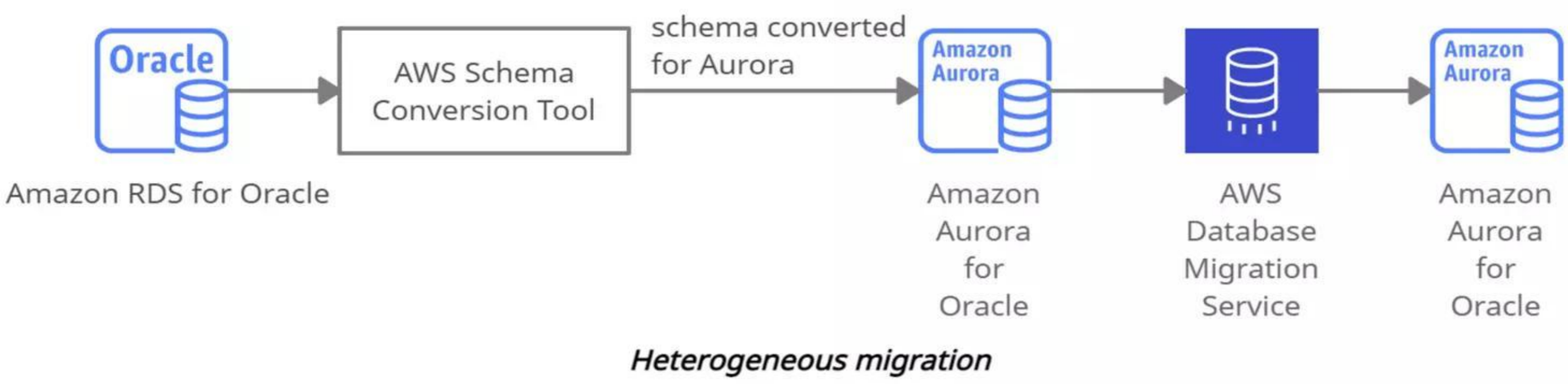
- **Sources**: Oracle, Microsoft SQL Server, PostgreSQL, Db2 LUW, SAP, MySQL, MariaDB, MongoDB, and Amazon Aurora.
- **Targets**: Oracle, Microsoft SQL Server, PostgreSQL, SAP ASE, MySQL, Amazon Redshift, Amazon S3, and Amazon DynamoDB.

It performs all the management steps required during the migration, such as monitoring, scaling, error handling, network connectivity, replicating during failure, and software patching.

AWS DMS with AWS Schema Conversion Tool (AWS SCT) helps to perform heterogeneous migration.



Homogeneous migration



Heterogeneous migration

Amazon API Gateway

What is Amazon API Gateway?

Amazon API Gateway is a service which creates, publishes, maintains, monitors and secures APIs at any scale.

- It helps to create Synchronous microservices with Load Balancers and forms the app-facing part of the AWS serverless infrastructure with AWS Lambda.
- It handles the tasks involved in processing concurrent API calls.
- It combines with Amazon EC2, AWS Lambda or any web application (public or private endpoints) to work as back-end services.

API Gateway creates RESTful APIs that:

- Are HTTP-based.
- Enable stateless and client-server communication.
- Create standard HTTP methods such as GET, POST, PUT, PATCH and DELETE.

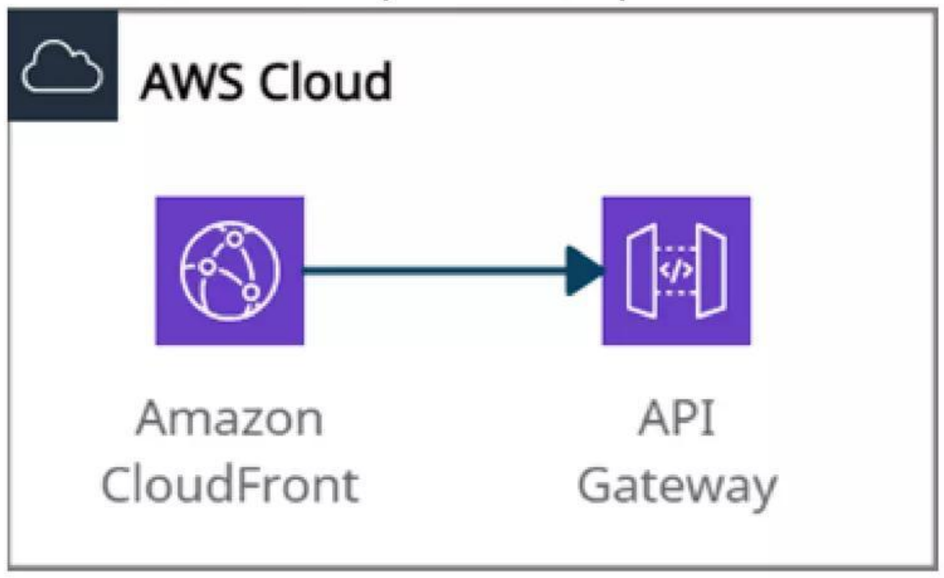
API Gateway creates WebSocket APIs that:

- Follow WebSocket protocol and enable stateful, full-duplex communication between client and server.
- Route incoming messages to the destination based on message content.

Endpoint Type**s** for API Gateway:

Edge-optimized endpoint:

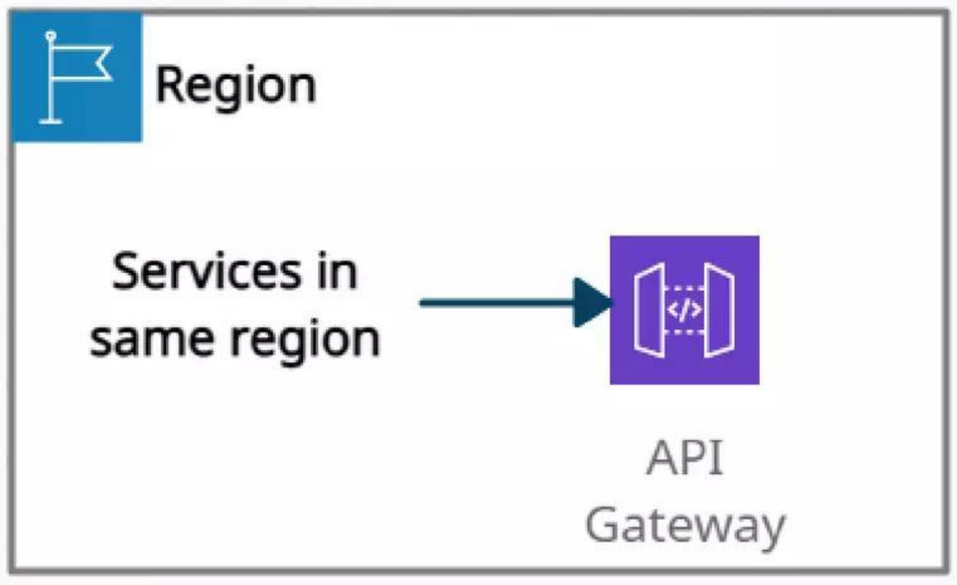
- It signifies reduced latency for requests all around the world.
- CloudFront is also used as the public endpoint.



Edge-optimized endpoint

Regional endpoint:

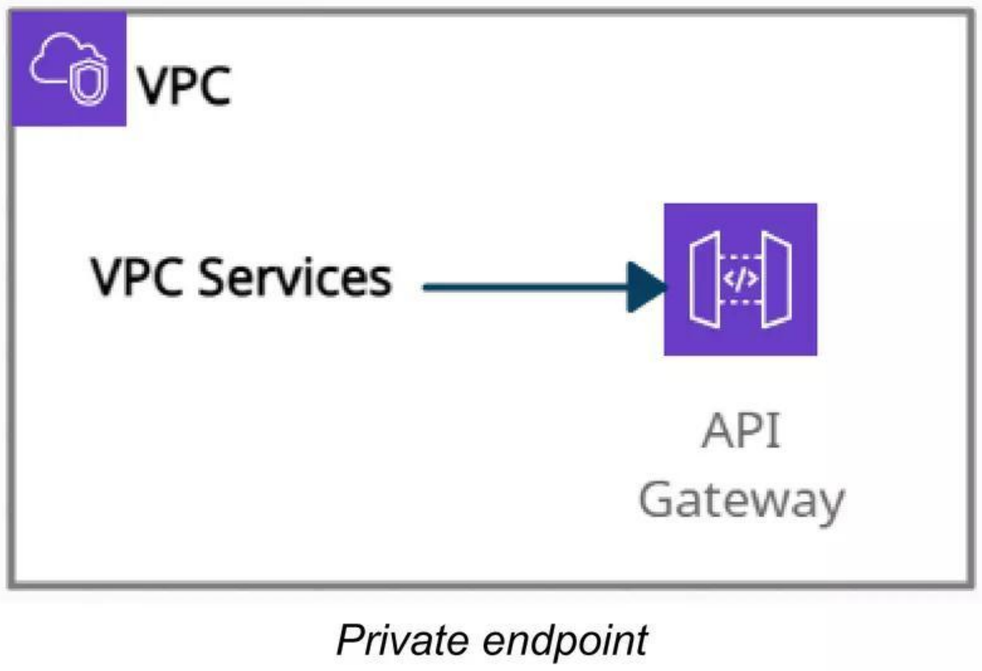
- It signifies reduced latency for requests that originate in the same region. It can also configure the CDN and protect WAF.



Regional endpoint

Private endpoint:

- It securely exposes the REST APIs to other services only within the VPC.



Private endpoint

API Gateway - Securities:

- Resource-based policies
- IAM Permissions
- Lambda Authorizer (formerly Custom Authorizers)
- Cognito user pools

Features:

- It helps to create stateful (WebSocket) and stateless (HTTP and REST) APIs.
- It integrates with CloudTrail for logging and monitoring API usage and API changes.
- It integrates with CloudWatch metrics to monitor REST API execution and WebSocket API execution.
- It integrates with AWS WAF to protect APIs against common web exploits.
- It integrates with AWS X-Ray for understanding and triaging performance latencies.

Price details:

- You pay for API Caching as it is not eligible for the AWS Free Tier.
- API requests are not charged for authorization and authentication failures.
- Method calls which consist of API keys are not charged if API keys are missing or invalid.
- API Gateway-throttled and plan-throttled requests are not charged if the request rate exceeds the predefined limits.

AWS Cloud Map

What is AWS Cloud Map?

AWS Cloud Map is a service that keeps track of application components, location dependencies, attributes and health status, and also allows dynamic scaling and responsiveness of the application.

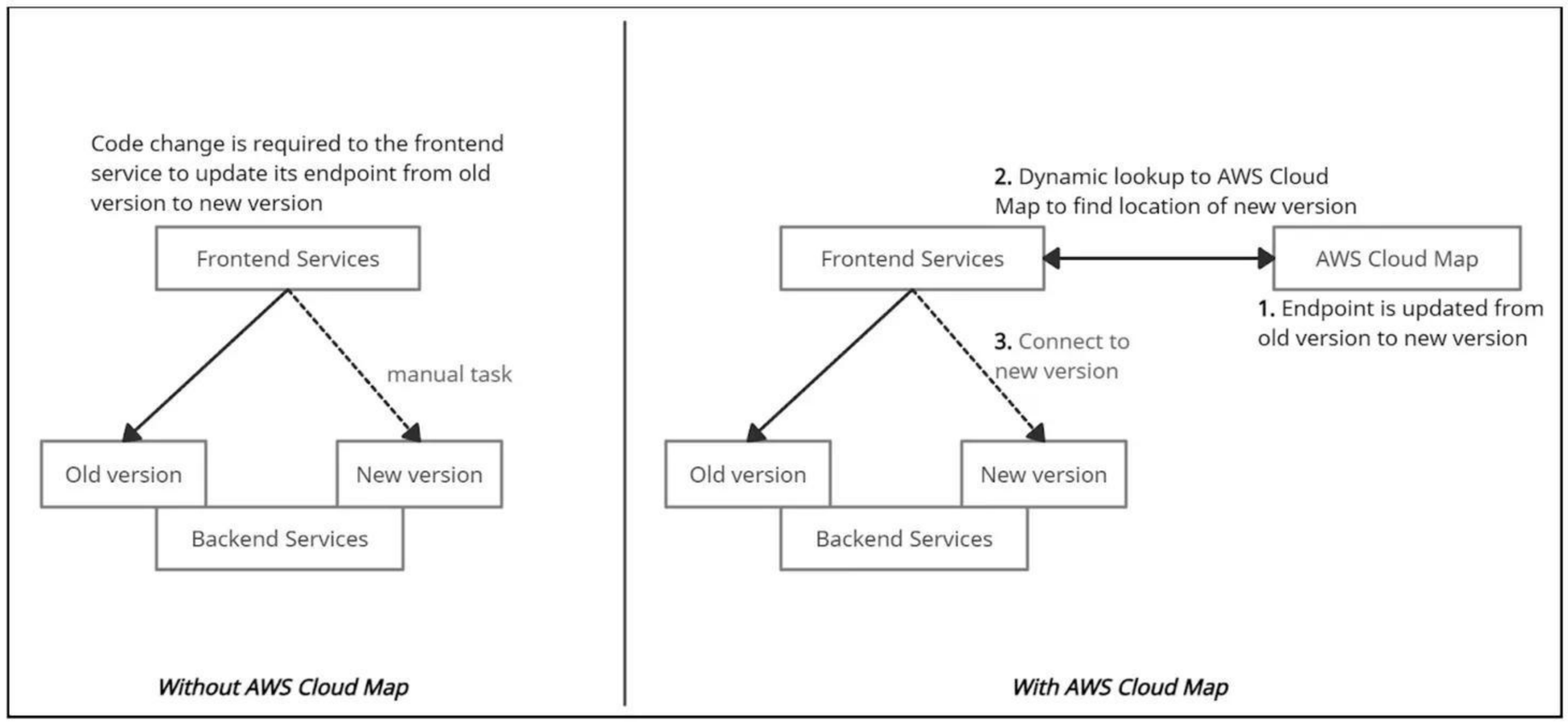
It uses AWS Cloud Map DiscoverInstances API calls, DNS queries in a VPC, or public DNS queries to locate resources in the backend.

A service is a template that is used by AWS Cloud Map when an application adds another resource, such as database servers.

When the application needs to connect to a resource, AWS Cloud Map calls API DiscoverInstances and specifies the namespace and service that are associated with the resource. AWS Cloud Map only returns healthy instances if health checking is specified while creating the service.

When an application adds a resource, a service instance is created by calling the AWS Cloud Map *RegisterInstance* API action. The service instance helps to locate the resource, by using DNS or using the AWS Cloud Map DiscoverInstances API action.

It can be used to register and locate any cloud resources, such as Amazon EC2 instances, Amazon Simple Queue Service (Amazon SQS) queues, Amazon DynamoDB tables, Amazon S3 buckets, or APIs deployed on top of Amazon API Gateway, among others.



AWS Cloud Map

Features:

- It decreases time consumption as it restricts the user to manage all the resource names and their locations manually within the application code.
- It is strongly integrated with Amazon Elastic Container Service (Amazon ECS).
- It constantly checks the health of the resources and allows users to choose whether to use Amazon Route 53 health checks or a third-party health checker.

- It provides a registry for the application services defined by namespaces and restricts developers to store, track, and update resource name and location information within the application code.

Price details:

- Extra charges related to Amazon Route 53 DNS and health check usage.
- Service registry charge - $0.10 per registered resource per month.
- Lookup requests charge - $1.00 per million discovery API calls.

Amazon CloudFront

What is Amazon CloudFront?
Amazon CloudFront is a content delivery network (CDN) service that securely delivers any kind of data to customers worldwide with low latency, low network and high transfer speeds.

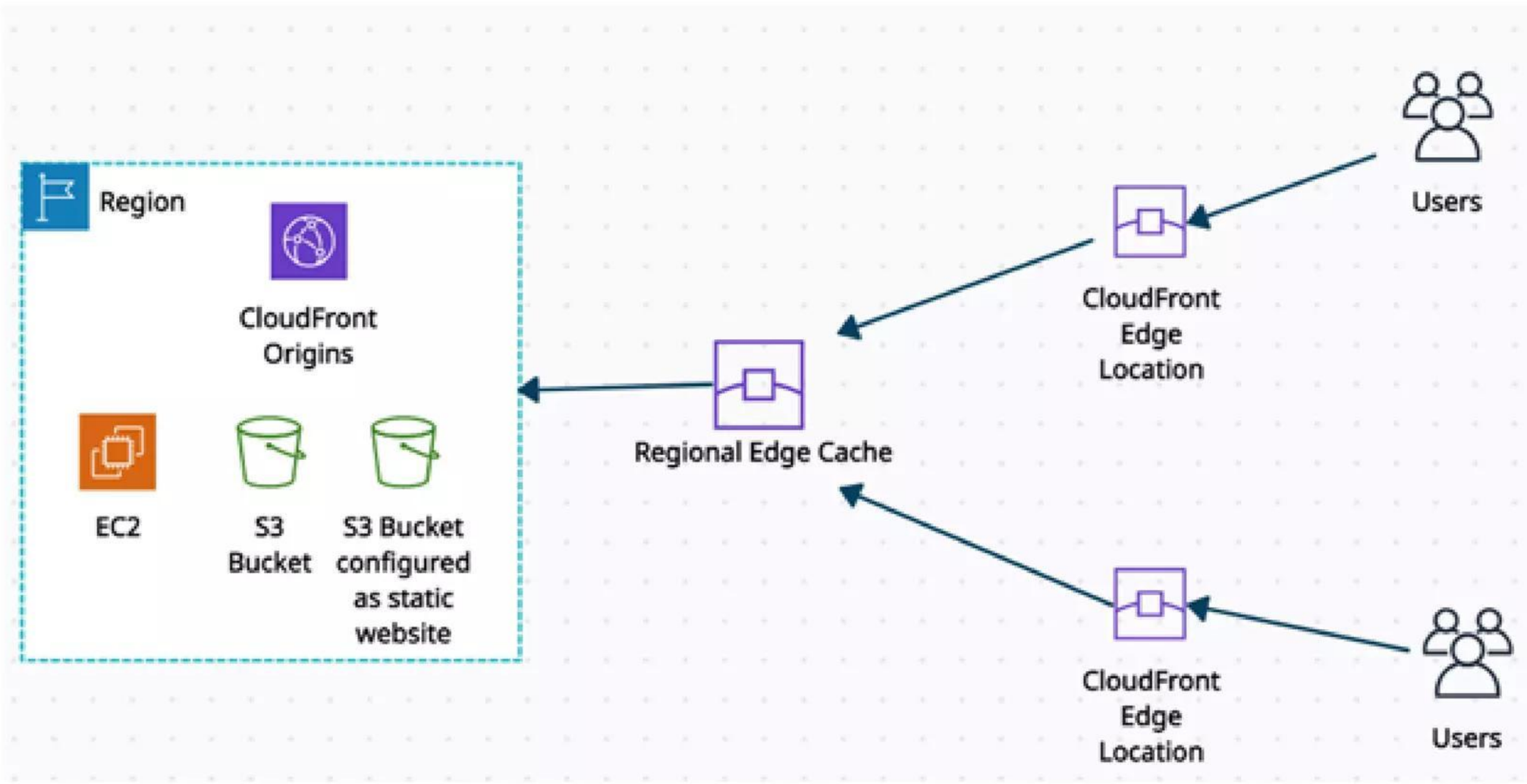
It uses edge locations (a network of small data centers) to cache copies of the data for the lowest latency. If the data is not present at edge locations, the request is sent to the source server, and data gets transferred from there.

It is integrated with AWS services such as

- Amazon S3,
- Amazon EC2,
- Elastic Load Balancing,
- Amazon Route 53,
- AWS Elemental Media Services.

The AWS origins from where CloudFront gets its traffic or requests are:

- Amazon S3
- Amazon EC2
- Elastic Load Balancing
- Customized HTTP origin



CloudFront Overview

It provides the programmable and secure edge CDN computing feature through AWS Lambda@Edge.

- It provides operations such as dynamic origin load-balancing, custom bot-management computationally, or building serverless origins.
- It has a built-in security feature to protect data from side-channel attacks such as Spectre and Meltdown.
- Field-level encryption with HTTPS - data remains encrypted throughout starting from the upload of sensitive data.

- AWS Shield Standard - against DDoS attacks.
- AWS Shield Standard + AWS WAF + Amazon Route53 - against more complex attacks than DDoS.

Amazon CloudFront Access Controls:
Signed URLs:
- Use this to restrict access to individual files.

Signed Cookies:
- Use this to provide access to multiple restricted files.
- Use this if the user does not want to change current URLs.

Geo Restriction:
- Use this to restrict access to the data based on the geographic location of the website viewers.

Origin Access Identity (OAI):
- Outside access is restricted using signed URLs and signed cookies, but what if someone tries to access objects using Amazon S3 URL, bypassing CloudFront signed URL and signed cookies. To restrict that, OAI is used.
- Use OAI as a special CloudFront user, and associate it with your Cloudfront distribution to secure Amazon S3 content.

Pricing Details:
- You pay for:
  - Data Transfer Out to Internet / Origin
  - A number of HTTP/HTTPS Requests.
  - Each custom SSL certificate associated with CloudFront distributions
  - Field-level encryption requests.
  - Execution of Lambda@Edge
- You do not pay for:
  - Data transfer between AWS regions and CloudFront.
  - AWS ACM SSL/TLS certificates and Shared CloudFront certificates.

AWS PrivateLink

What is AWS PrivateLink?

AWS PrivateLink is a network service used to connect to AWS services hosted by other AWS accounts (referred to as endpoint services) or AWS Marketplace. Whenever an interface VPC endpoint (interface endpoint) is created for service in the VPC, an Elastic Network Interface (ENI) in the required subnet with a private IP address is also created that serves as an entry point for traffic destined to the service.

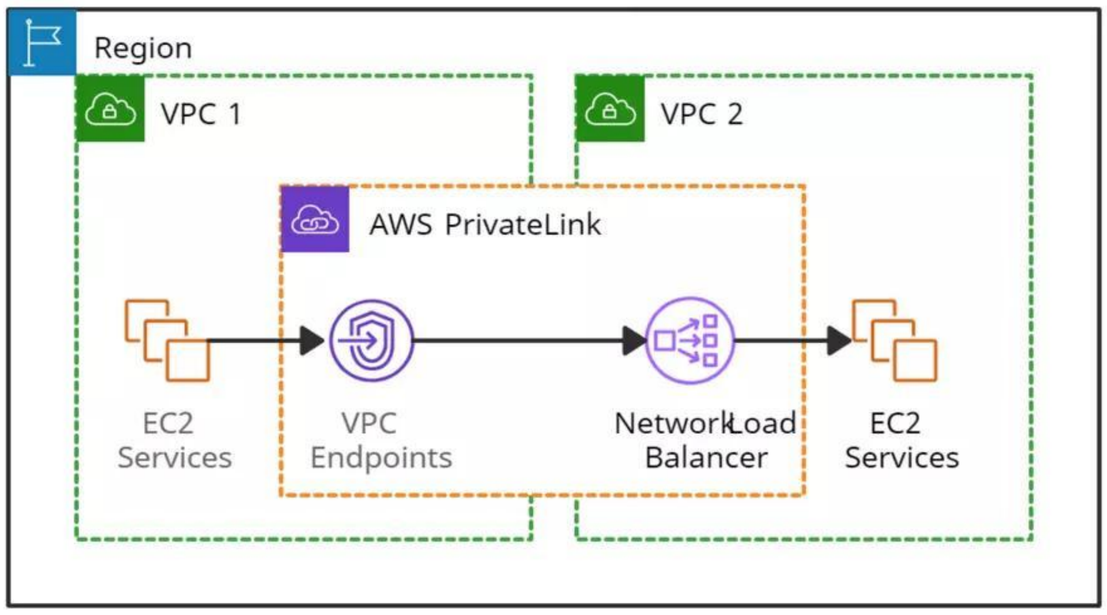
Interface endpoints

- It serves as an entry point for traffic destined to an AWS service or a VPC endpoint service.

Gateway endpoints

- It is a gateway in the route-table that routes traffic only to Amazon S3 and DynamoDB.

PrivateLink is used for scenarios where the source VPC acts as a service provider, and the destination VPC acts as a service consumer. So service consumers use an interface endpoint to access the services running in the service provider.	But Direct Connect is something different. It only creates a connection between an interface endpoint and your on-premises data center. It can be used with AWS PrivateLink.



AWS PrivateLink

Features:

- It is integrated with AWS Marketplace services so that the services can be directly attached to the endpoint.
- It provides security by not allowing the public internet and reducing the exposure to threats, such as brute force and DDoS attacks.
- It helps to connect services across different accounts and Amazon VPCs without any firewall rules, VPC peering connection, or managing VPC Classless Inter-Domain Routing (CIDRs).
- It helps to migrate on-premise applications to the AWS cloud more securely. Services can be securely accessible from the cloud and on-premises via AWS Direct Connect and AWS VPN.

Pricing details:

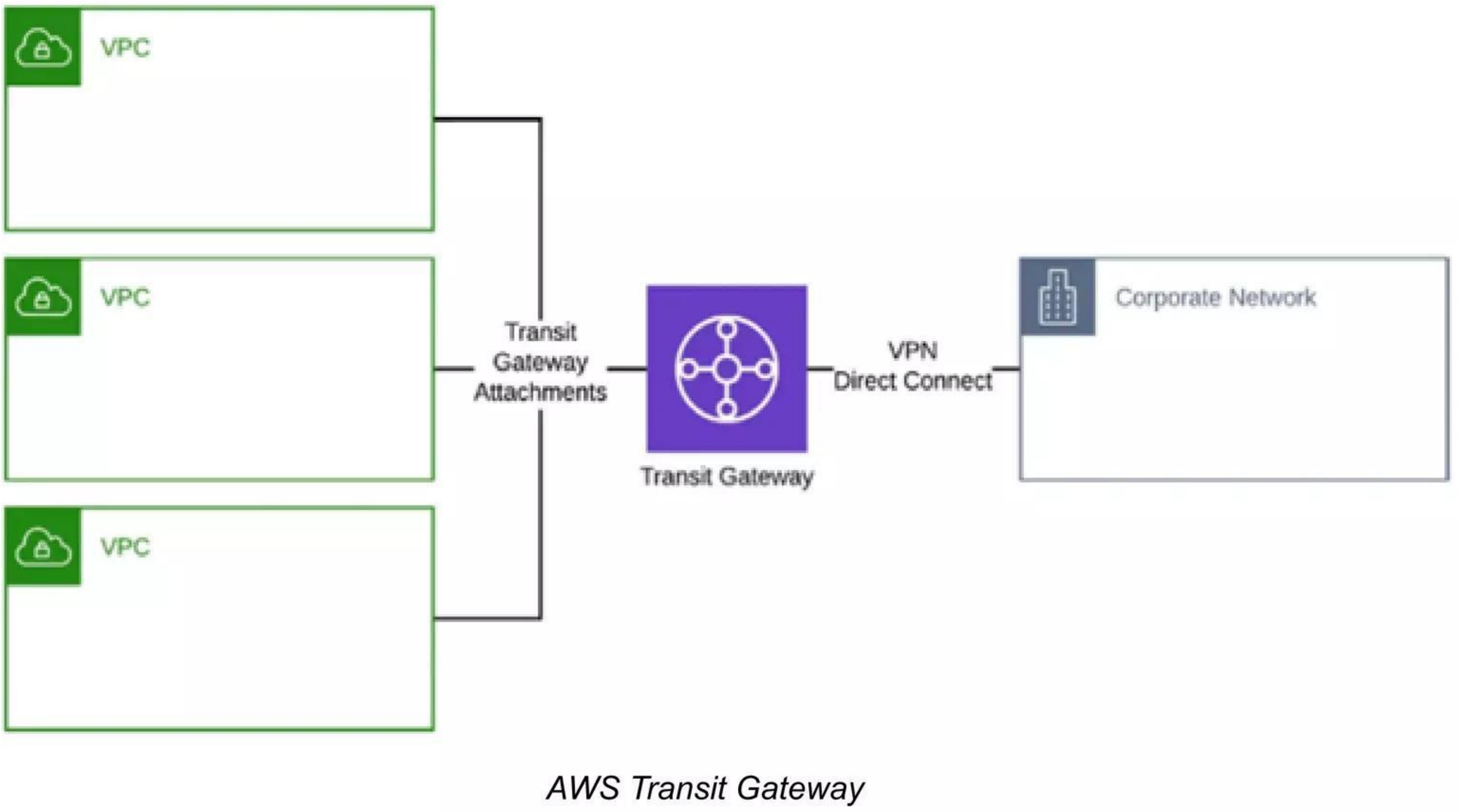
- PrivateLink is charged based on the use of endpoints.

AWS Transit Gateway

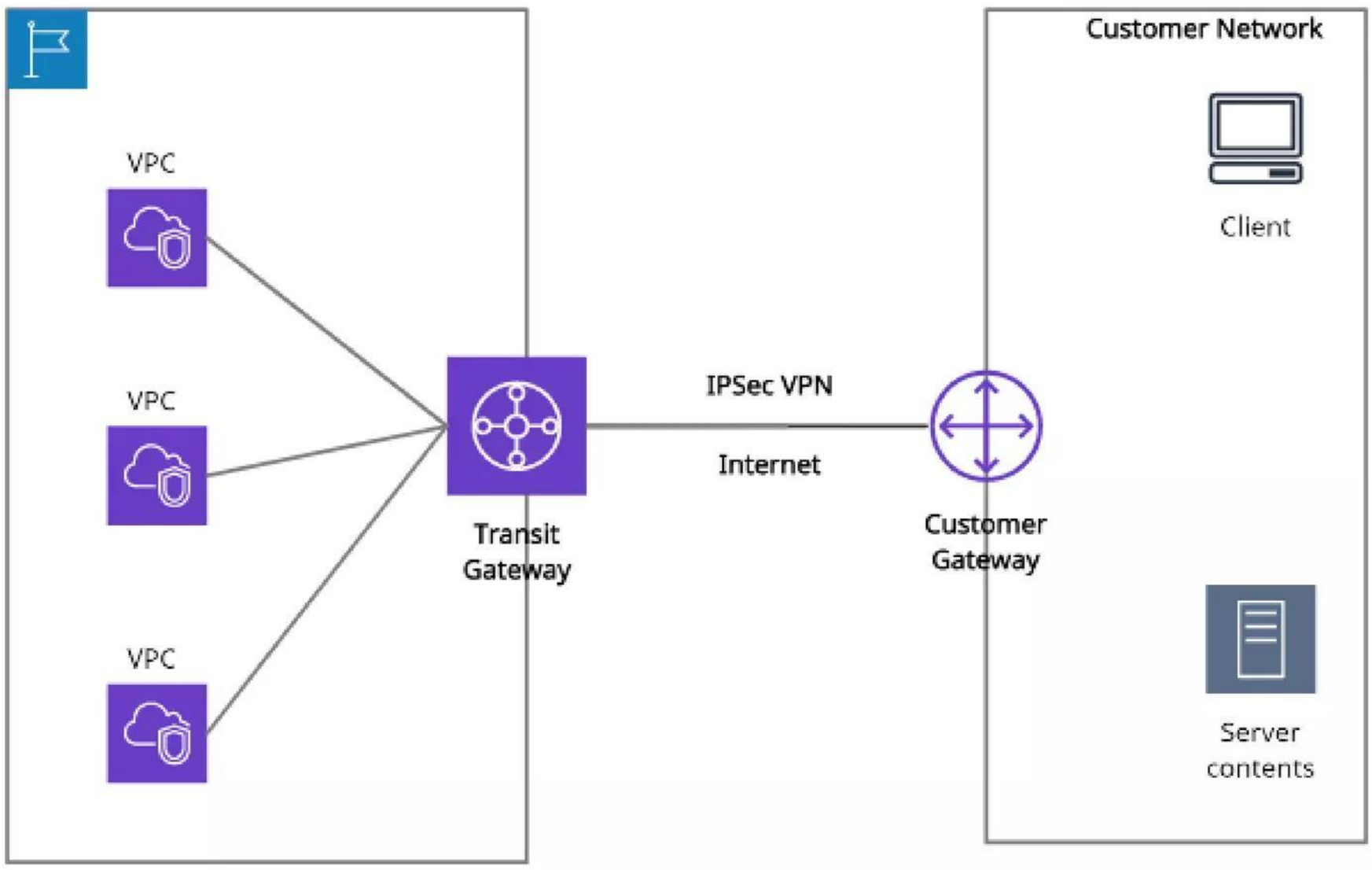
What is AWS Transit Gateway?

AWS Transit Gateway is a network hub used to interconnect multiple VPCs. It can be used to attach all hybrid connectivity by controlling your organization's entire AWS routing configuration in one place.

- It can be more than one per region but can not be peered within a single region.
- It helps to solve the problem of complex VPC peering connections.
- It can be connected with an AWS Direct Connect gateway from a different AWS account.
- Resource Access Manager (RAM) cannot integrate AWS Transit Gateway with Direct Connect gateway.
- To implement redundancy, Transit Gateway also allows multi-user gateway connections.
- Transit Gateway VPN attachment is a feature to create an IPsec VPN connection between your remote network and the Transit Gateway.
- Transit Gateway Network Manager is used to manage and monitor networking resources and connections to remote branch locations.
- It reduces the complexity of maintaining VPN connections with hundreds of VPCs, which become very useful for large enterprises.
- It supports attaching Amazon VPCs with IPv6 CIDRs.



AWS Transit Gateway



AWS Transit Gateway + VPN

Transit Gateway vs. VPC peering:

Transit Gateway	VPC peering
It has an hourly charge per attachment in addition to the data transfer fees.	It does not charge for data transfer.
Multicast traffic can be routed between VPC attachments to a Transit Gateway.	Multicast traffic cannot be routed to peering connections.
It provides Maximum bandwidth (burst) of 50 Gbps per Availability Zone per VPC connection.	It provides no aggregate bandwidth.
Security groups feature does not currently work with Transit Gateway.	Security groups feature works with intra-Region VPC peering.

Transit Gateway can be created using the following ways

- AWS CLI
- AWS Management Console
- AWS CloudFormation

Price details:

- Users will be charged for your AWS Transit Gateway on an hourly basis.

AWS Direct Connect

What is AWS Direct Connect?

AWS Direct Connect is a cloud service that helps to establish a dedicated connection from an on-premises network to one or more VPCs in the same region.

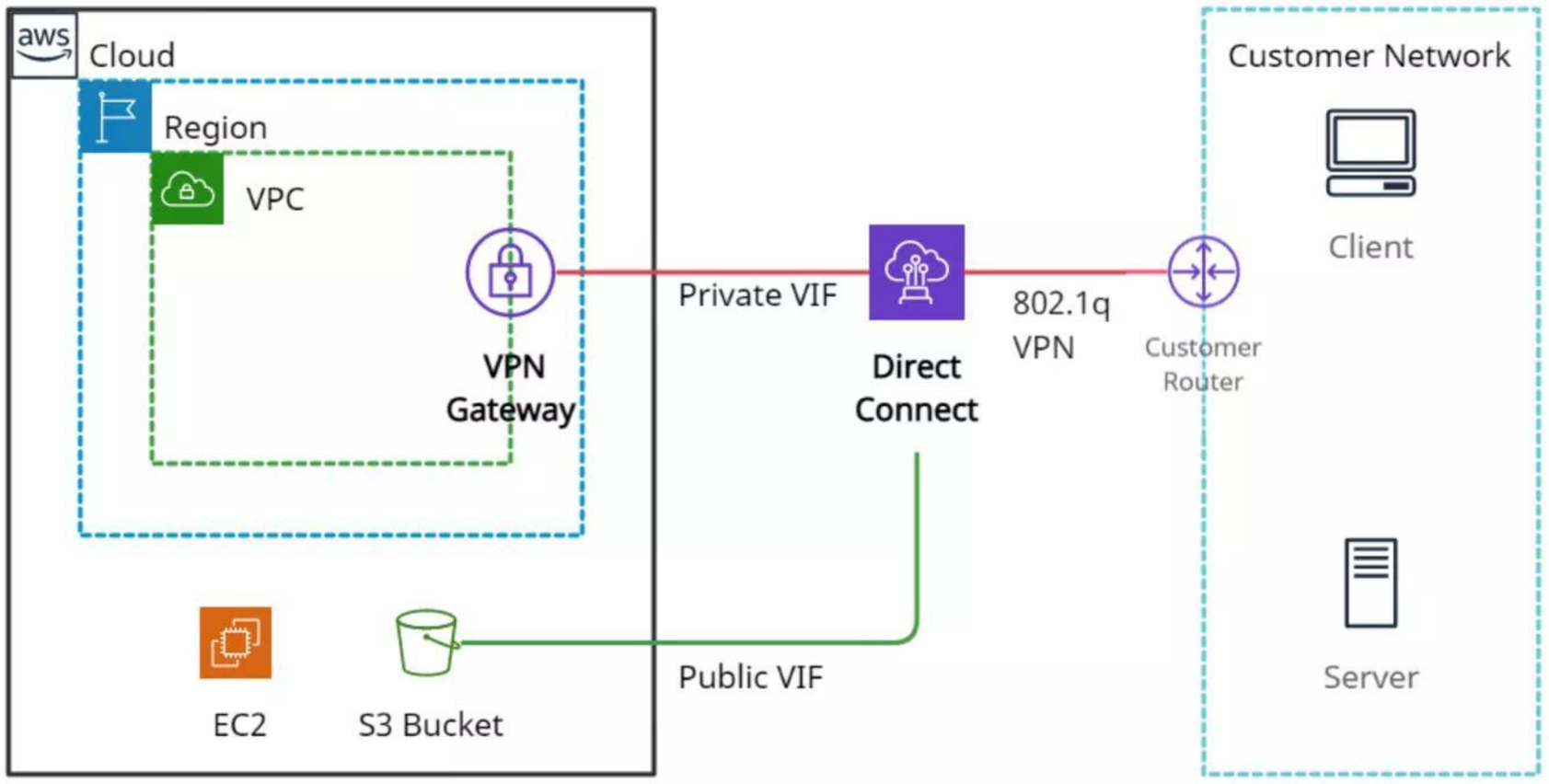
Private VIF with AWS Direct Connect helps to transfer business-critical data from the data-center, office or colocation environment into AWS, bypassing your Internet service provider and removing network traffic.

Private virtual interface: It helps to connect an Amazon VPC using private IP addresses.

Public virtual interface: It helps to connect AWS services located in any AWS region (except China) from your on-premises data center using public IP addresses.

Methods of connecting to a VPC:

- AWS Managed VPN.
- AWS Direct Connect.
- AWS Direct Connect plus a VPN.
- AWS VPN CloudHub.
- Transit VPC.
- VPC Peering.
- AWS PrivateLink.
- VPC Endpoints.



Amazon Direct Connect

Direct Connect gateway:

It is a globally available service used to connect multiple Amazon VPCs across different regions or AWS accounts. It can be integrated with either of the following gateways:

- Transit gateway - it is a network hub used to connect multiple VPCs to an on-premise network in the same region.
- Virtual private gateway - It is a distributed edge routing function on the edges of VPC.