AWS Solution Architect

TECHNOLOGY

VPC, Networking, and Content Delivery

simplilearn

A Day in the Life of a Cloud Architect

You work as a network engineer and are looking for a networking solution that fits the following requirements:

- The company is searching for a domain name service that can connect user requests to AWS-hosted infrastructure.
- The solution should also be capable of routing traffic according to certain policies.

To achieve all of the above along with some additional features, you will be learning a few concepts in this lesson that will help you find solutions for the above-given scenario.

A Day in the Life of a Cloud Architect

You are employed as an administrator in a company. Your company is considering moving its infrastructure to the cloud but is concerned about security. You've been asked to recommend a few security solutions available in AWS that meet the following criteria so that the organization may make a migration decision:

- They'd like an entity that can be attached to any AWS resource and define access permissions for that resource.
- The company doesn't want to give out long-term credentials (such usernames and passwords or access keys) to any server, therefore they'll need a solution that can provide temporary rights for applications to utilize when calling other AWS resources.

A Day in the Life of a Cloud Architect

- They'd also want to look after the AWS account's governance, compliance, operational audits, and risk auditing.
- They also want to ensure that the security and compliance of the applications they've installed on AWS are up to standard.

To achieve all the above along with some additional features, you will be learning a few concepts in this lesson that will help you find solutions for the above-given scenario.

Learning Objectives

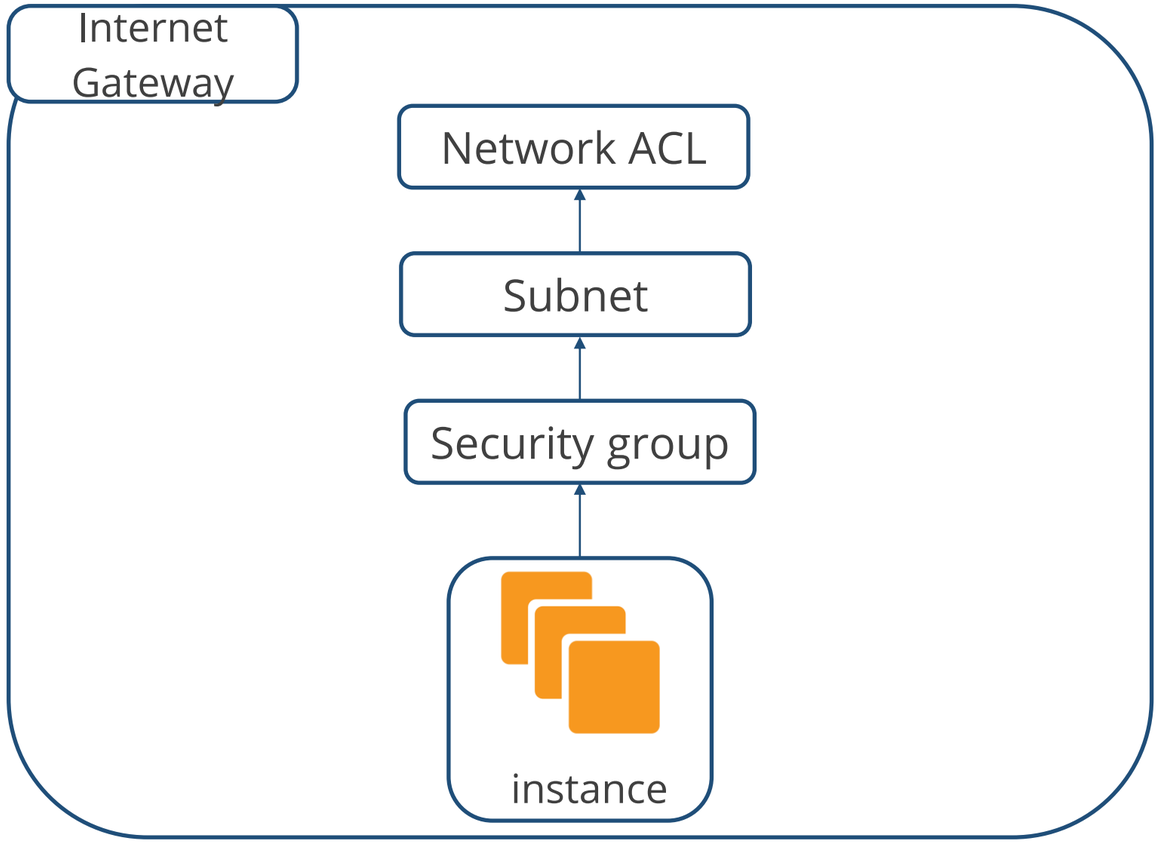
By the end of this lesson, you will be able to:

- Configure IAM and its policies
- Work with CloudFront
- Create a VPC endpoint
- Implement different types of routing

Security Group

Security Group

AWS Security group handles the incoming and outgoing traffic, which serves as the virtual firewall for EC2 instances.



Security Group

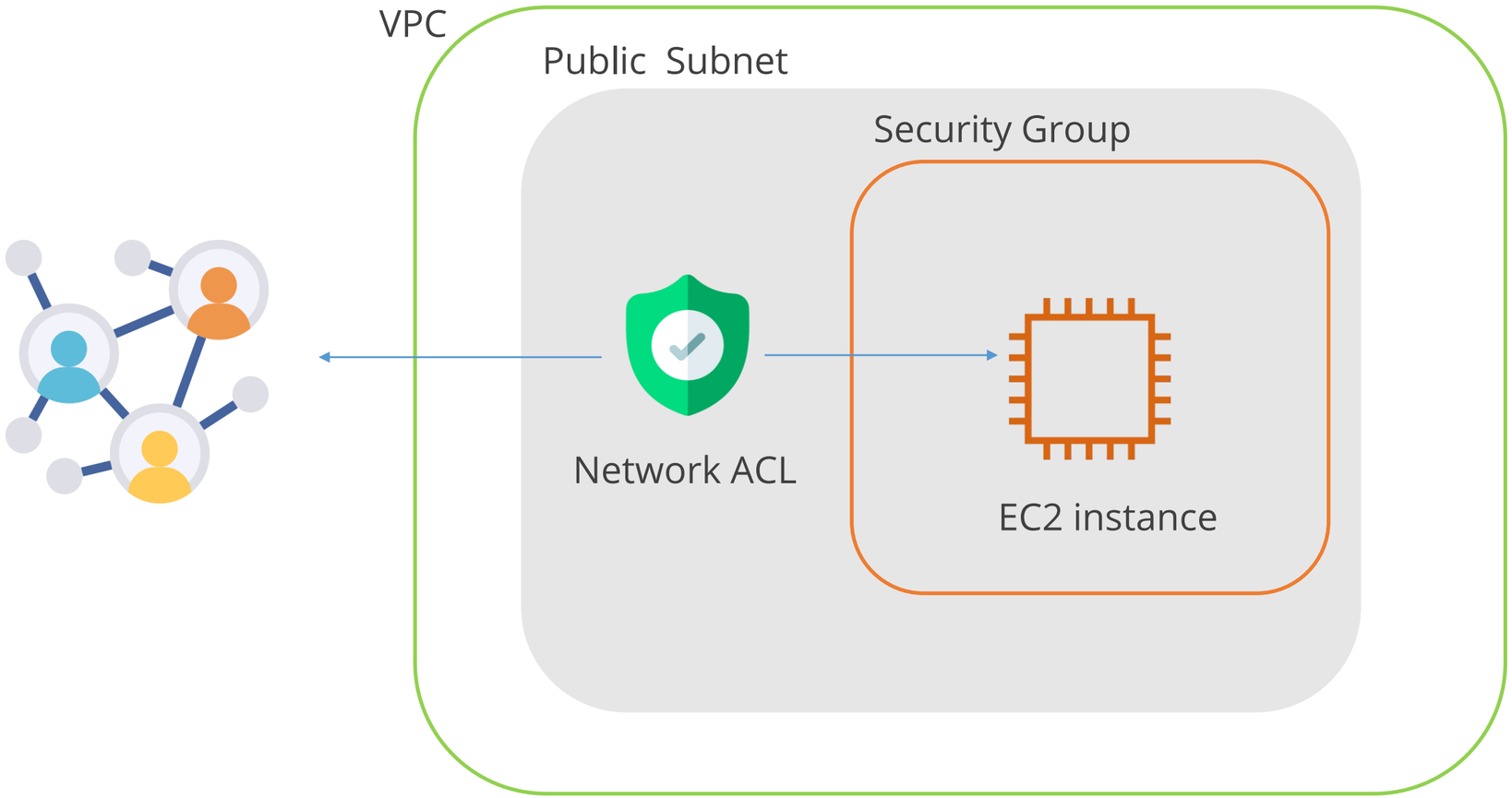
The rules for security groups:

1. Security groups by default include outbound rules that permit all outbound traffic.
2. The traffic can be filled using security group rules based on protocols and ports.
3. There is no way to construct security group rules that restrict access.
4. A security group's rules can be changed at any time and all instances connected will be updated.

Network ACL (NACL)

Network ACL (NACL)

Network ACL acts as an optional safety feature that serves as a firewall to manage the traffic entering and leaving a subnet.



Network ACL (NACL)

The rules for security ACL are as follows:

- **Rule number:** Rules are ranked from lowest to highest according to their number. Any higher-numbered rule that could be in conflict with a rule that matches traffic is ignored
- **Type:** It's possible to define the type of traffic, such as SSH, as well as all traffic or a specific range
- **Protocol:** Any protocol with a standard protocol number can be specified. By choosing ICMP as the protocol, we can check the protocol number and define any or all the ICMP kinds and codes

Network ACL (NACL)

The rules for security ACL are as follows:

- Port reach: The traffic's listening port or set of ports. 80, for HTTP traffic, as an illustration
- Source: [Inbound only rules], the traffic is generated by (CIDR range)
- Destination: [Exit rules only] the traffic's final destination (CIDR range)
- Allow/Deny: Whether to let or block the requested traffic

Network ACL (NACL)

The difference between Network ACL and Security Group are:

Security Group	Network ACL
• In the security group, it operates at the instance level. • Security groups are stateful • Security group supports allow rules only	• In the NACL, it acts as a firewall at the subnet level • Network ACLs are stateless. • It supports allowing rules and denies rules

IP Addresses

IP Addresses

The following are the types of IP Addresses in Amazon VPC:

- Private IP Address
- Public IP Address
- Elastic IP Address

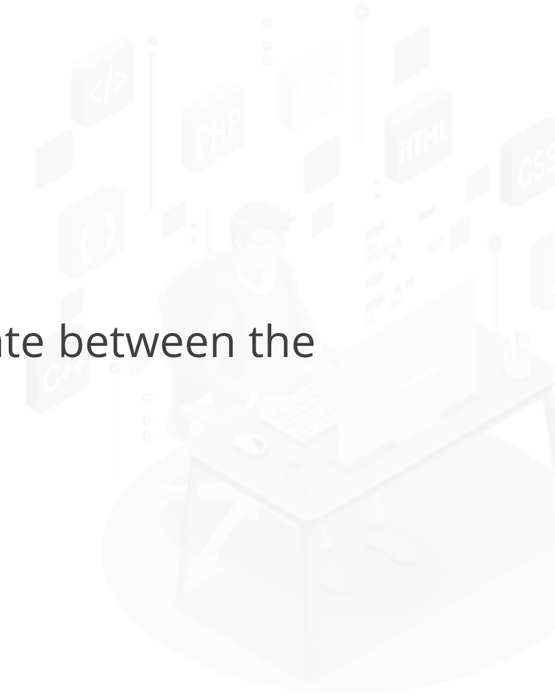
- A private IP address is not reachable over the internet.
- The users can use private IP address to communicate between instances in the same VPC.
- Public IP will get released whenever the user spot and instance.

IP Addresses

The following are the types of IP Addresses in Amazon VPC:

- Private IP Address
- Public IP Address
- Elastic IP Address

- A public IP address is reachable from the internet.
- The users can use public IP address to communicate between the instances and the internet.



IP Addresses

The following are the types of IP Addresses in Amazon VPC:

- Private IP Address
- Public IP Address
- Elastic IP Address

- An Elastic IP address is a public IP address that the users can allocate to their account.
- The users can associate it to and from the instances as they require, and it remains allocated to their account until they choose to release it.

Multiple IP Addresses

It can be useful to assign multiple IP addresses to an instance in the VPC to do the following:

- Host multiple websites on a single server by using multiple SSL certificates on a single server and associating each certificate with a specific IP address
- Operate network appliances, such as firewalls or load balancers, that have multiple IP addresses for each network interface
- Redirect internal traffic to a standby instance in case the instance fails, by reassigning the secondary IP address to the standby instance

Create Key Pair for EC2

Duration: 5 mins

Problem statement:

You have been assigned a task to create a fresh new key pair.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed:

1. Set up the prerequisites for configuring VPC
2. Create a key pair

Default VPC Walk Through

Duration: 13 mins

Problem statement:

You have been assigned a task to create a default VPC.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed:

1. Set up the prerequisites for configuring VPC
2. Create a default VPC

Explore Network ACL Firewall

Duration: 13 mins

Problem statement:

You have been assigned a task to create an NACL.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed:

1. Set up the prerequisites for configuring NACL
2. Create a Network ACL

VPC Flow Logs

VPC Flow Log

A flow log can be created for a VPC, a subnet, or a network interface.

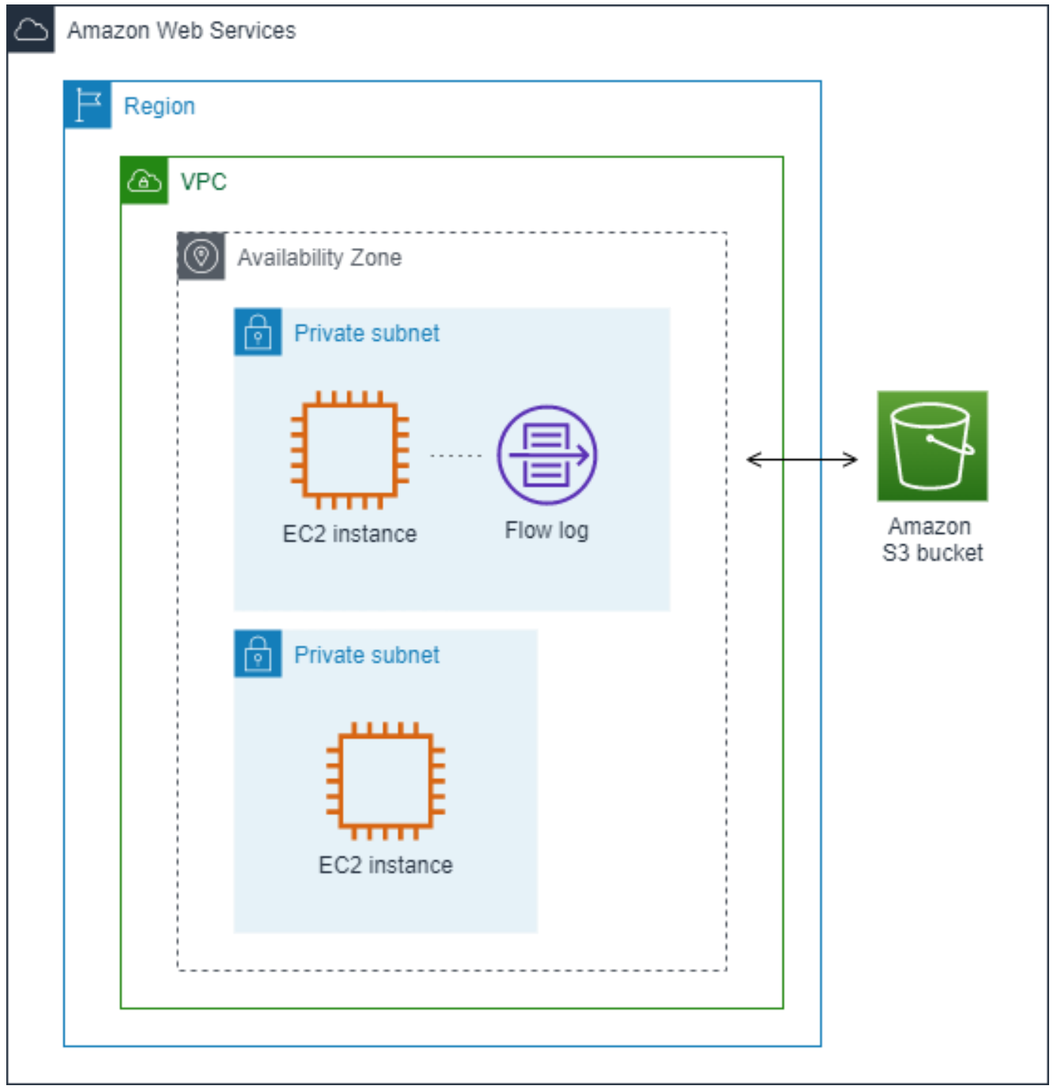
When a flow log is created for a subnet or VPC, it monitors every network interface in that subnet or VPC.

VPC Flow Log

VPC flow log can be published in two destinations, CloudWatch Logs and Amazon S3.

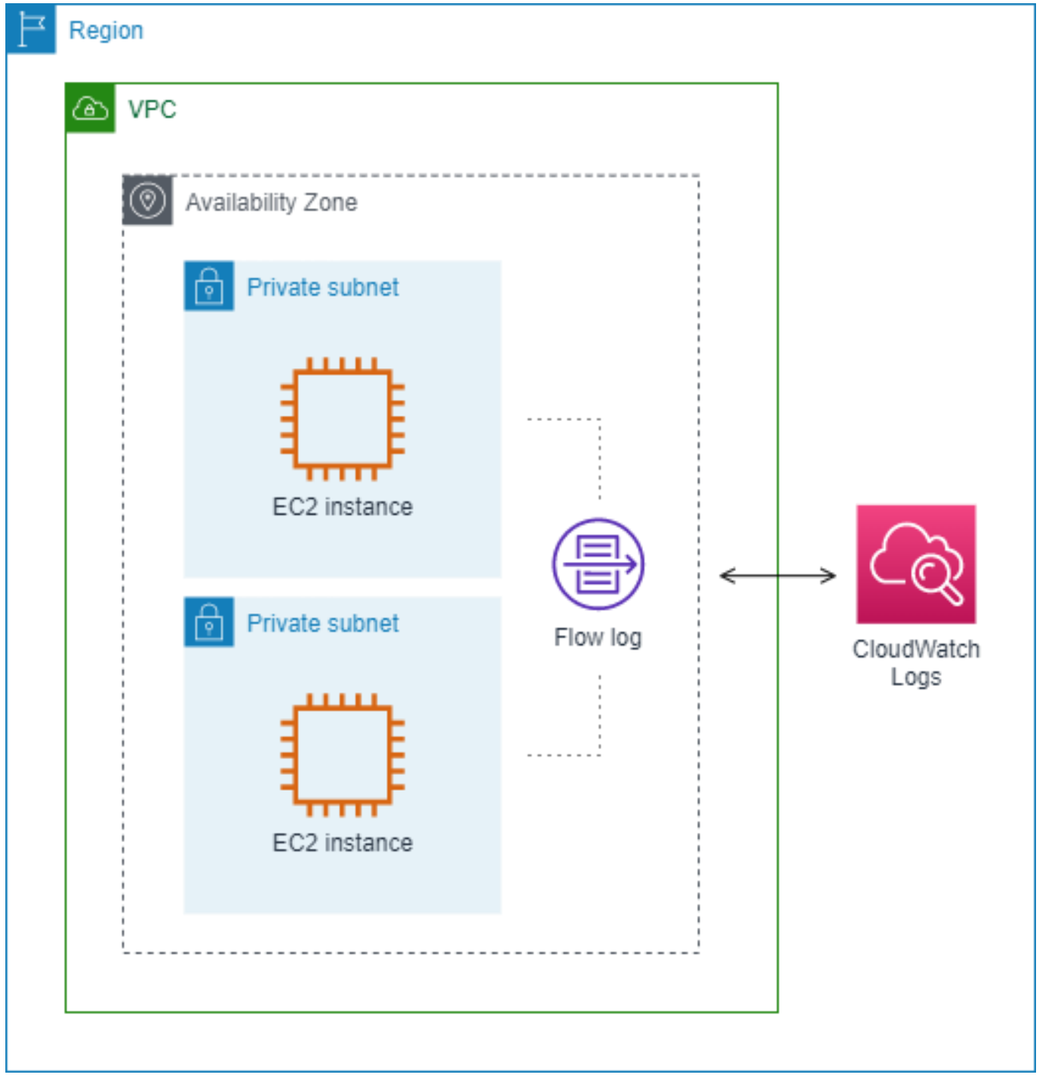
- **Amazon S3**: VPC Flow Logs collects flow log records and consolidates them into log files.
- **CloudWatch Log**: Flow log data is published to a log group when published to CloudWatch Logs.

VPC Flow Log in Amazon S3



VPC flow logs collect flow log records, consolidate them into log files, and then publish the log files at 5-minute intervals to the Amazon S3 bucket and each log file contains flow log records for the last five minutes of IP traffic.

VPC Flow Log in CloudWatch



When publishing to CloudWatch Logs, flow log data is published to a log group, and each network interface has a unique log stream in the log group, and flow log records are stored in log streams.

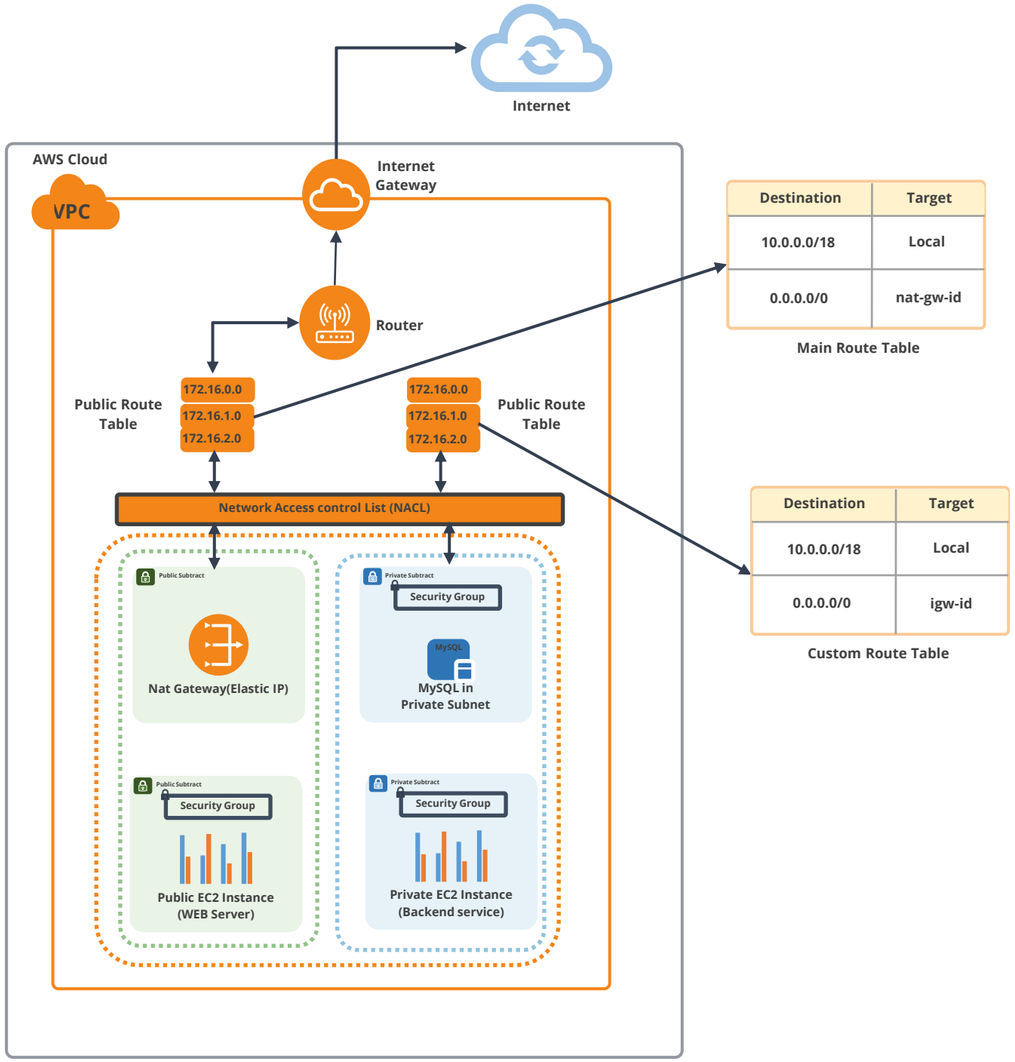
VPC Flow Log

A request in VPC must go through the sequence of steps before reaching an AWS-hosted endpoint, and the endpoint used is an EC2 instance.

The VPC flow is explained using:

- The External Request
- The Private Instance

VPC Flow Log



Destination	Target
10.0.0.0/18	Local
0.0.0.0/0	nat-gw-id

Main Route Table

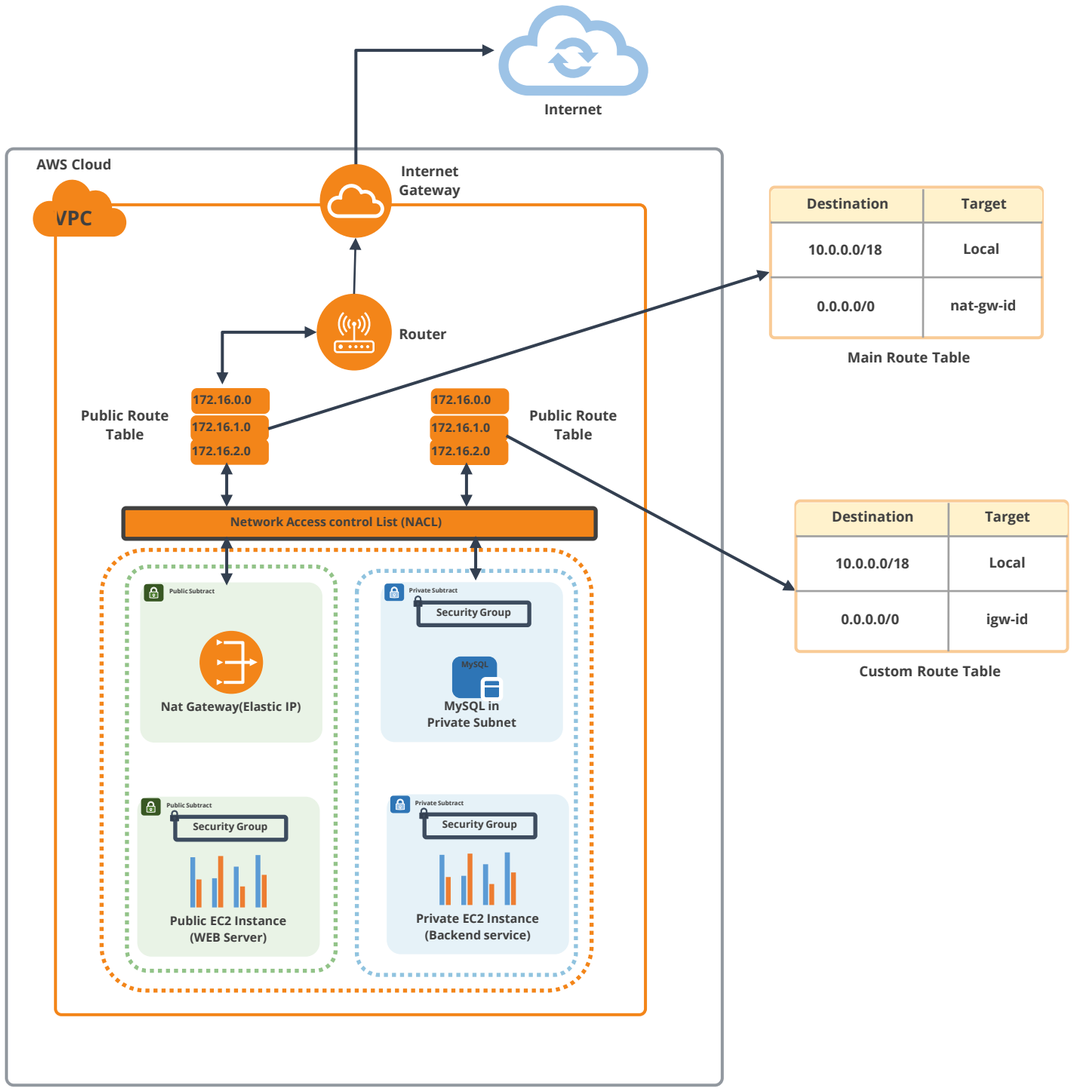
Destination	Target
10.0.0.0/18	Local
0.0.0.0/0	igw-id

Custom Route Table

The image represents the working of the components in a private instance.
It includes the following components:
External Request:

- Internet Gateway
- Router or Route Table
- Network ACL (attached to subnet)
- Security Group (attached to instance)
- Public Instance

VPC Flow Log



Destination	Target
10.0.0.0/18	Local
0.0.0.0/0	nat-gw-id

Main Route Table

Destination	Target
10.0.0.0/18	Local
0.0.0.0/0	igw-id

Custom Route Table

The image represents the working of the components in a private instance.
It includes the following components:

1. Security Group (Outbound rule)
2. Network ACL (for private subnet)
3. Router / Route Table
4. Network ACL
5. NAT (in the public subnet)
6. Router / Route Table
7. Internet Gateway
8. External Destination

TECHNOLOGY

IAM Role for VPC Flow Capture

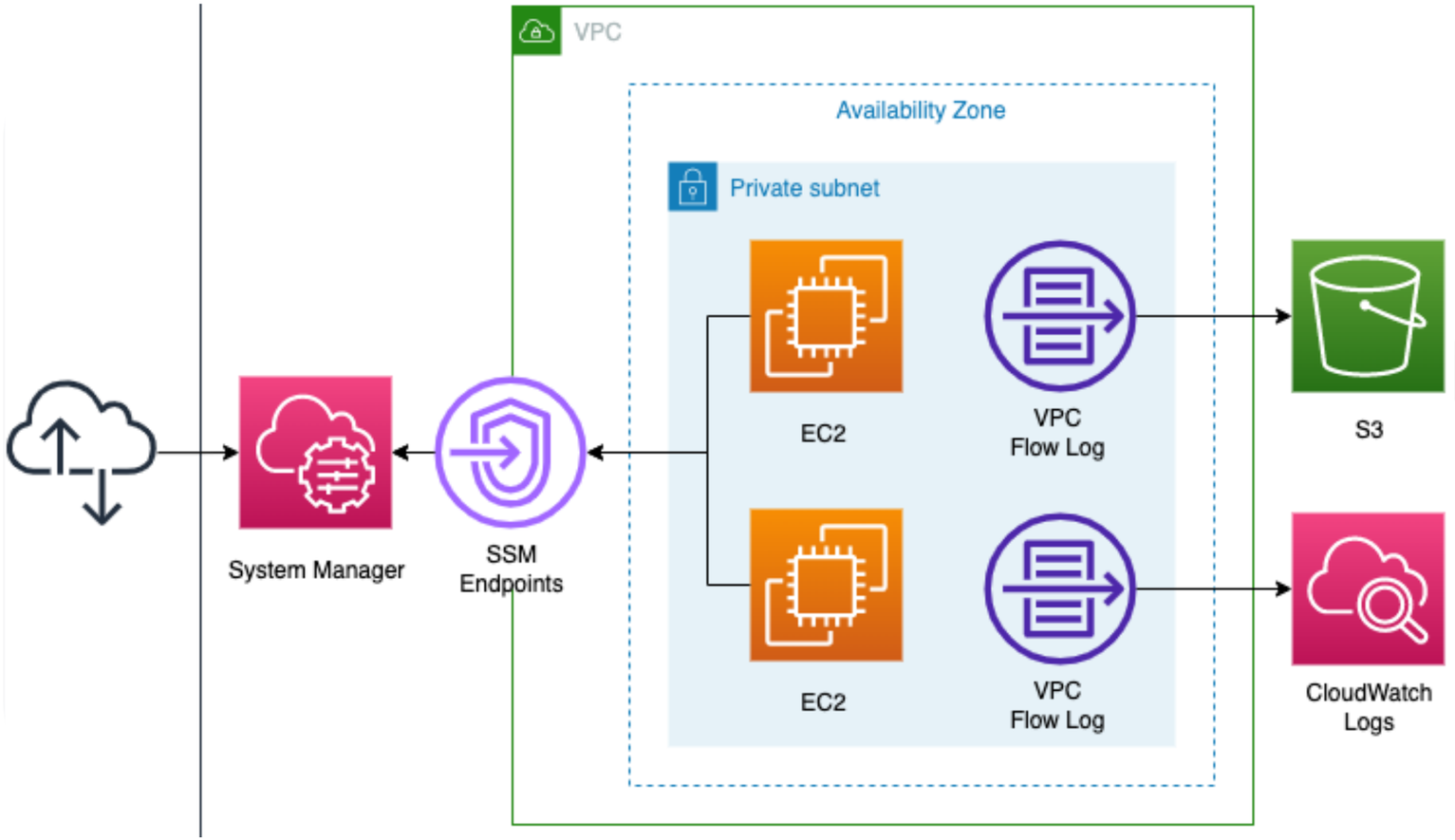
Overview: VPC Flow Logs

Virtual Private Cloud (VPC) flow logs provides built-in power to monitor information about how a user's network resources are operated in Amazon Web Services.

- Flow logs can monitor the traffic that is reaching a user's instance.
- Flow logs can enable a user to capture information about the IP traffic going to and from network interfaces in the user's VPC.

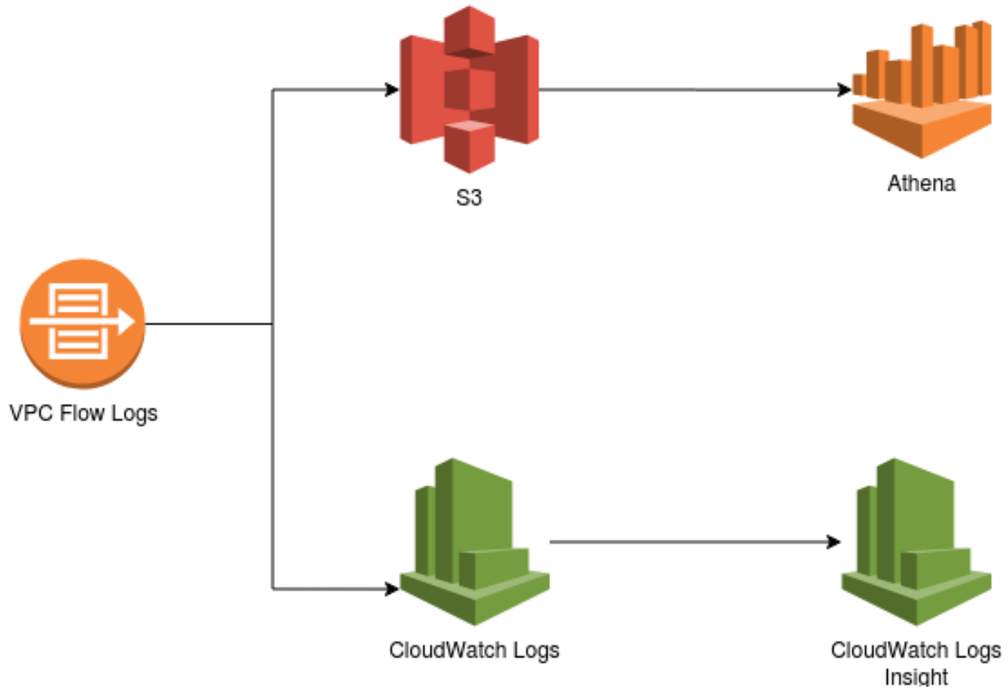
Publishing of Flow Logs to CloudWatch Logs

The data from flow logs can be easily published to Amazon CloudWatch.



Publishing of Flow Logs to CloudWatch Logs

Flow log data is published to a log group when publishing to CloudWatch Logs, and each network interface has a distinct log stream in the log group.



Log streams contain flow log records.

Publishing of Flow Logs to CloudWatch Logs

Users can create multiple flow logs that publish data to the same log group.

A single integrated log stream is present if the same network interface appears in one or more flow logs belonging to the same log group.

Publishing of Flow Logs to CloudWatch Logs

If a user specifies that one flow log should capture rejected traffic and the other flow log should capture accepted traffic, then the combined log stream captures all traffic.

Publishing of Flow Logs to CloudWatch Logs

Users who submit flow logs to CloudWatch Logs are subjected to data ingestion and archival charges for vended logs.

Publishing of Flow Logs to CloudWatch Logs

The **timestamp** field in CloudWatch Logs refers to the start time that is recorded in the flow log record.

Publishing of Flow Logs to CloudWatch Logs

The **ingestionTime** field indicates the date and time when the flow log record was received by CloudWatch Logs.

This timestamp is later than the end time that's captured in the flow log record.

IAM Roles for Publishing Flow Logs to CloudWatch Logs

To publish flow logs to the designated log group in CloudWatch Logs, the IAM role that is linked to the user's flow log must have the necessary rights.

The IAM role must belong to the user’s AWS account.

IAM Roles for Publishing Flow Logs to CloudWatch Logs

The IAM policy that's attached to the user's IAM role must include at least the following permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

IAM Roles for Publishing Flow Logs to CloudWatch Logs

It should be ensured that the role has a trust relationship that allows the flow logs service to assume the role.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
"Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

IAM Roles for Publishing Flow Logs to CloudWatch Logs

It is recommended that the user should use the **aws:SourceAccount** and **aws:SourceArn** condition keys to protect against the confused deputy problem.

Scenario: IAM Roles for Publishing Flow Logs

A user can add the following condition block to the previous trust policy:

```
 "Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:region:account_id:vpc-flow-log/flow-log-id"
    }
}
```

Scenario: IAM Roles for Publishing Flow Logs

The source account would be the owner of the flow log, and the source ARN would be the flow log ARN.

If the user doesn't know the flow log ID, the user can replace that portion of the ARN with a wildcard and then update the policy after creating the flow log.

Create or Update an IAM Role for Flow Logs

Users can update an existing role or can use a recommended procedure to create a new role for using with flow logs.

Creating an IAM Role for Flow Logs

The below process should be followed to create an IAM role for flow logs:

- Open the IAM console at HTTPS.
- In the navigation pane, choose **Roles** and then **Create role**.
- For **Select type of trusted entity**, choose **AWS service**.
- For **Use case**, choose **EC2** and choose **Next: Permissions**.

Creating an IAM Role for Flow Logs

The below process should be followed to create an IAM role for flow logs:

- On the **Attach permissions policies** page, choose **Next: Tags** and optionally add tags, choose **Next: Review**.
- Enter a name for your role and optionally provide a description, then select **Create role**.
- Select the name of your role. For **Permissions**, choose **Add inline policy**, **JSON**.

Creating an IAM Role for Flow Logs

The below process should be followed to create an IAM role for flow logs:

- Copy the policy from IAM roles for publishing flow logs to CloudWatch Logs and paste it into the window. Choose **Review policy**.
- Enter a name for the policy and choose to **Create policy**.
- Select the name of the role. For **Trust relationships**, choose **Edit trust relationship**. Choose **Update Trust Policy**.
- On the **Summary** page, note the ARN for the role. The user will need this ARN while creating the flow log.

Permissions for IAM Users to Pass a Role

Users must also have permission to use the **iam: PassRole** action for the IAM role that is associated with the flow log.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "iam:PassRole"
        ]
        "Resource": [
            "arn:aws:iam::account-id:role/flow-log-role-name"
        ]
     }
   ]
}
```

Creating a VPC Flow Log

Duration: 13 mins

Problem statement:

You have been assigned a task to create an VPC flow log.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed:

1. Setting up the prerequisites for configuring VPC flow log
2. Creating a VPC flow log

Internet Gateways

Internet Gateways

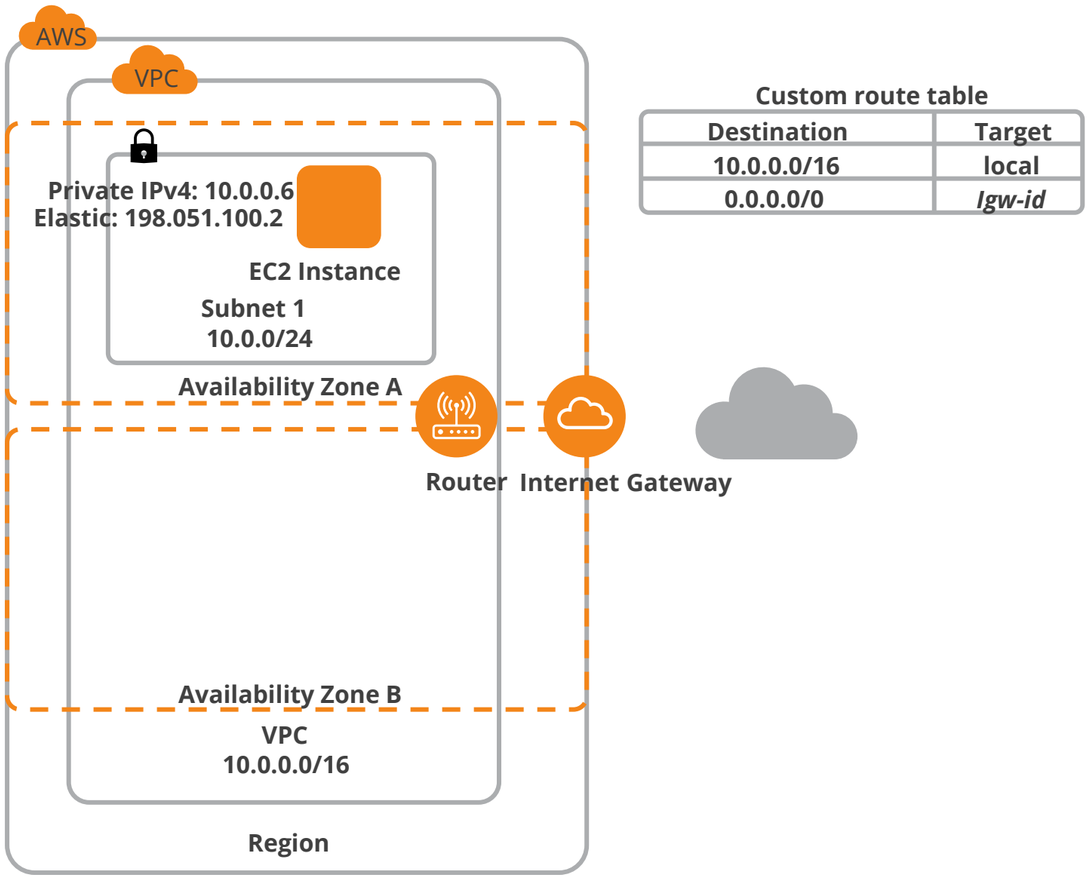
An Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between the VPC and the Internet.

An Internet gateway serves two purposes:

- It provides a target in the VPC route tables for internet-routable traffic.
- It performs network address translation (NAT) for instances that have been assigned public IPv4 addresses.

Internet Gateways

The following diagram shows the communication between the Elastic IP address and the Internet:



Custom route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*Igw-id*

Source: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

Egress-only Internet Gateways

An Internet gateway where the users cannot associate with a security group is known as an egress-only Internet gateway.

- Users can use security groups for their instances in the private subnet to control the traffic to and from those instances.
- Users can use a network ACL to control the traffic to and from the subnet for which it routes the traffic.

TECHNOLOGY

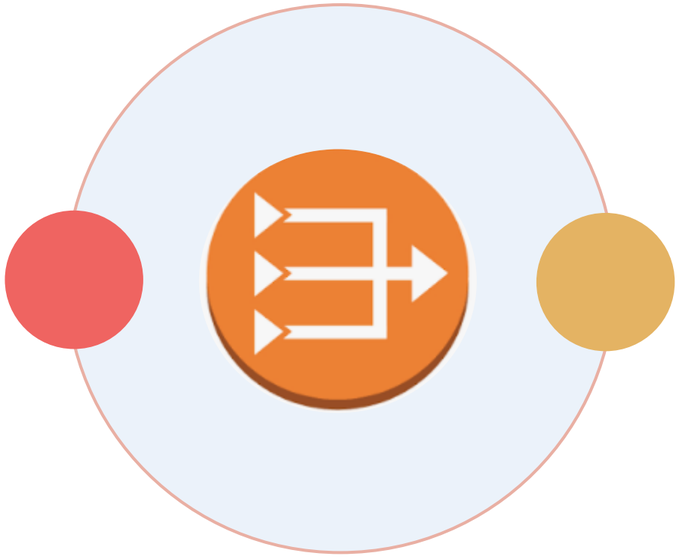
Network Address Translation (NAT) Gateway

Network Address Translation (NAT)

A NAT device is used to enable instances in a private subnet to connect to the internet or other AWS services, preventing the Internet from initiating connections with those instances.

There are two types of NAT devices:

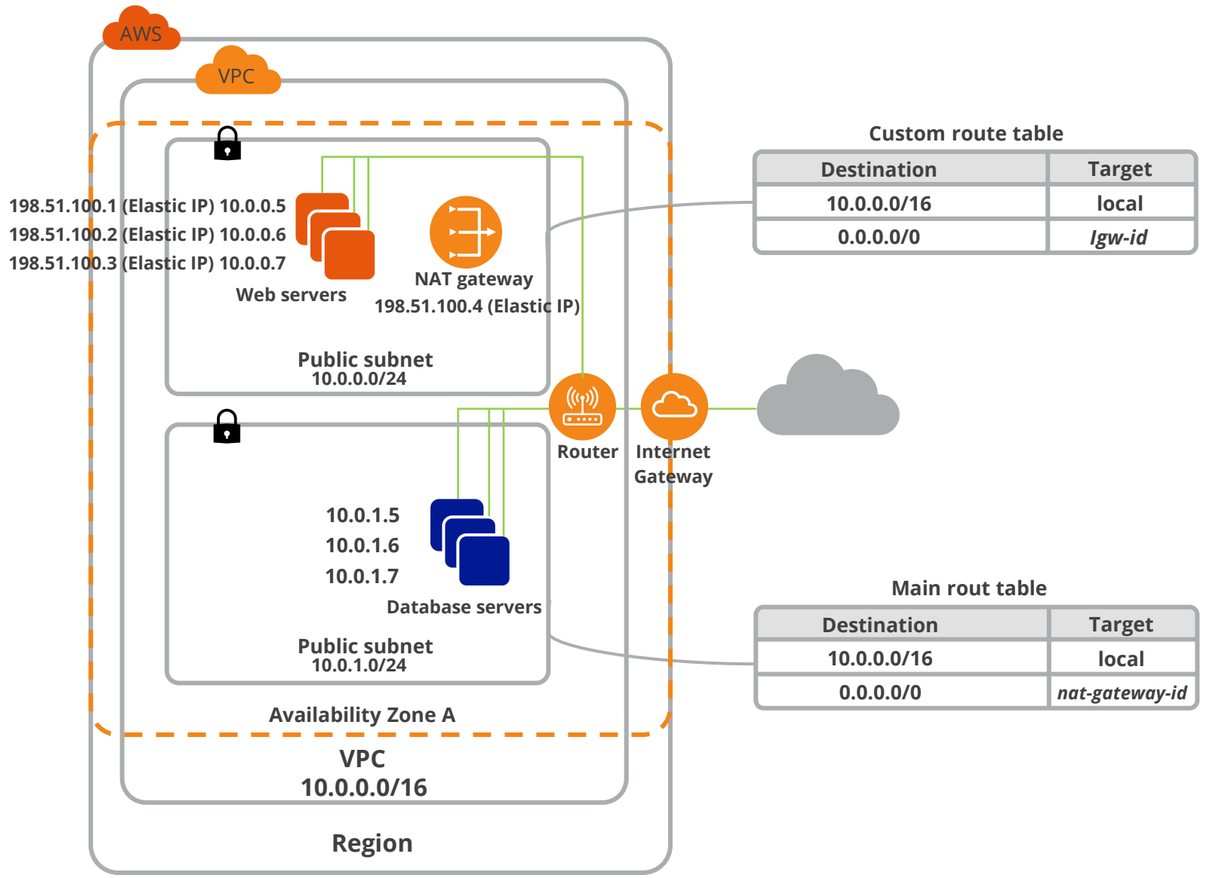
NAT gateway



NAT instance

NAT Gateway

The following diagram illustrates the architecture of a VPC with a NAT gateway:



Source: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

Characteristics of NAT Gateway

- It supports 5 Gbps of bandwidth and automatically scales up to 45 Gbps.
- It supports the TCP, UDP, and ICMP protocols.
- Users can use a network ACL to control the traffic to and from the subnet in which the NAT gateway is located.
- It can support up to 55,000 simultaneous connections to each unique destination.

Limitations of NAT Gateway

- Users can associate exactly one Elastic IP address with a NAT gateway.
- Users cannot associate a security group with a NAT gateway.
- A NAT gateway cannot be accessed by a ClassicLink connection that is associated with the VPC.
- Users cannot route traffic to a NAT gateway through a VPC peering connection, a Site-to-Site VPN connection, or AWS Direct Connect.

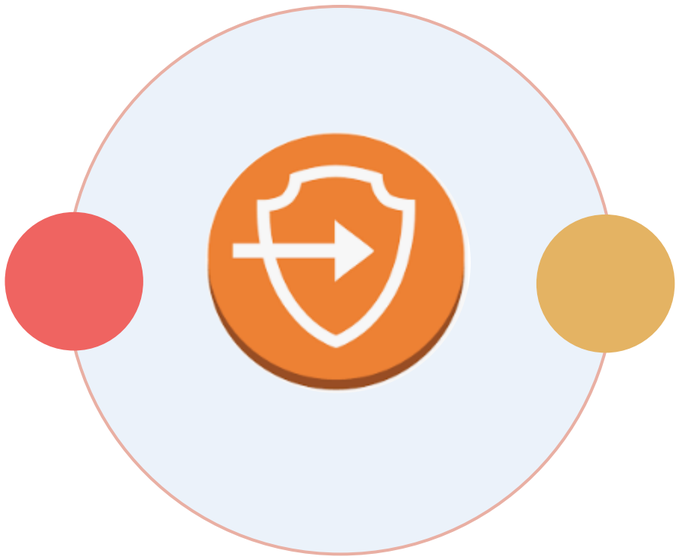
Interface Endpoints

Overview of VPC Endpoints

A VPC endpoint enables users to connect the VPC to their AWS services without requiring an Internet Gateway, NAT device, VPN, or an AWS Direct Connect connection.

There are two types of VPC endpoints:

Interface endpoints



Gateway endpoints

Amazon S3 supports both gateway endpoints and interface endpoints.

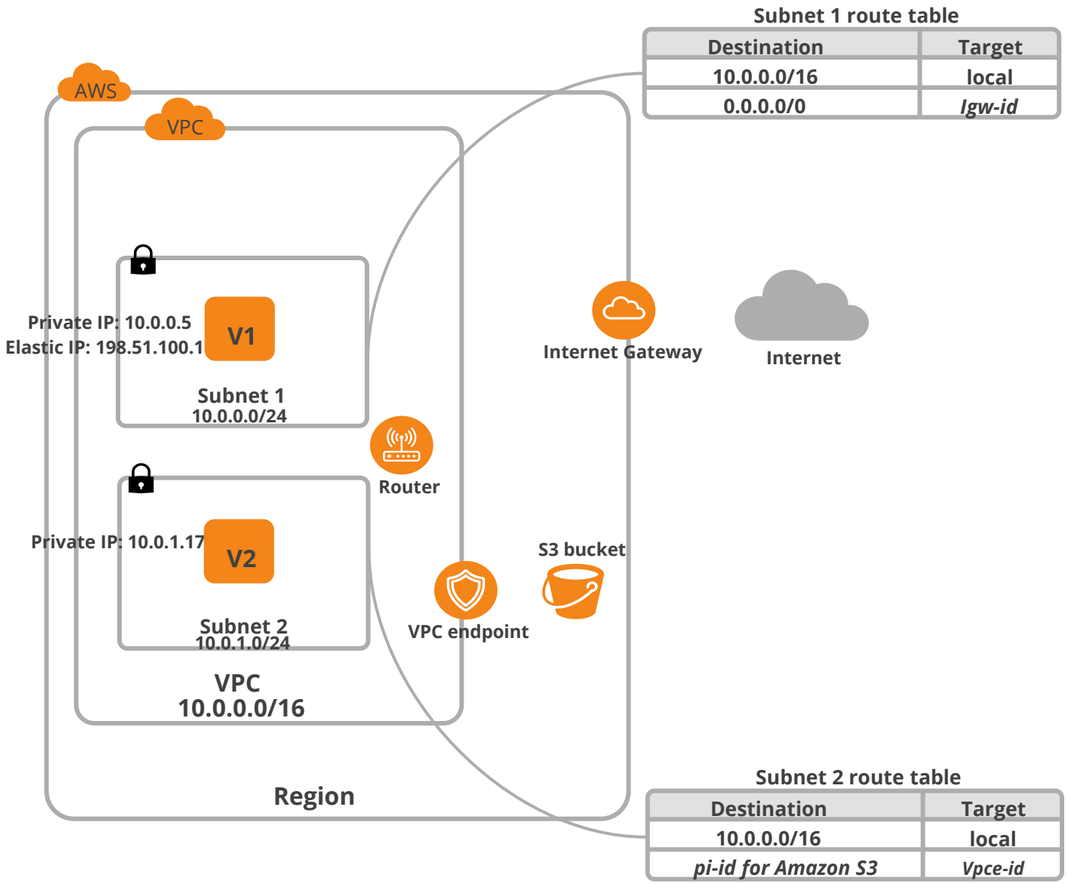
Interface VPC Endpoint

Users can create an interface VPC endpoint to connect to services powered by AWS PrivateLink, including various AWS services.

Each subnet that a user specifies from their VPC creates an endpoint network interface in the subnet and assigns a private IP address from the subnet address range.

Accessing an AWS Service Using an Interface VPC Endpoint

An endpoint network interface is a requester-managed network interface.



- Users can view the VPC endpoint interface in their AWS account but cannot manage it by themselves.
- Users are billed according to their hourly usage and data processing charges.

Features of Interface Endpoint

01 Interface VPC endpoints support traffic over TCP.

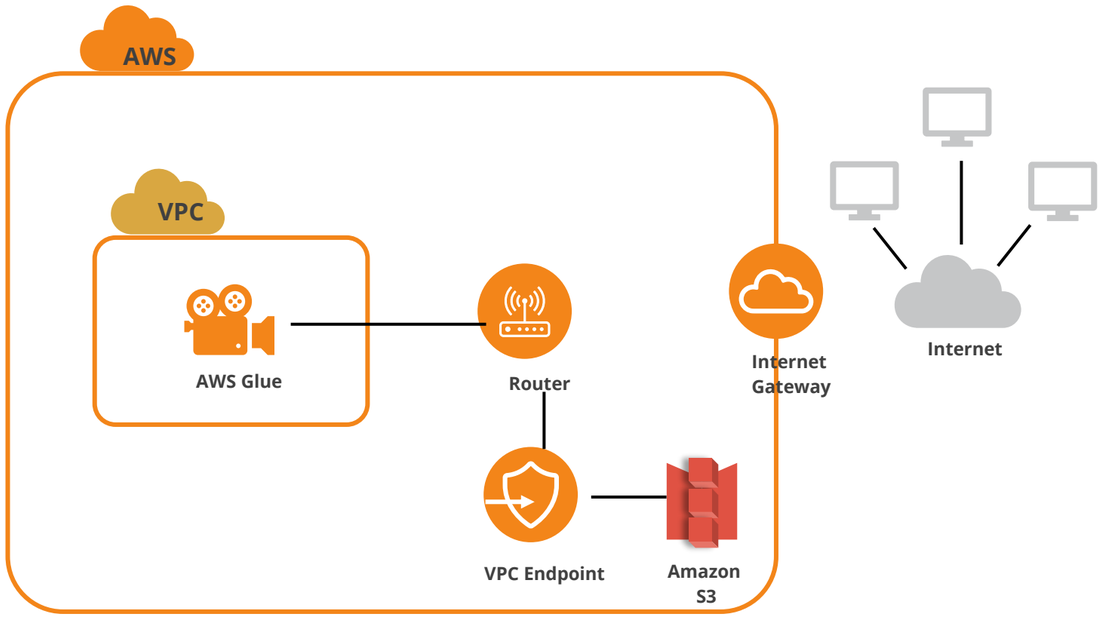
02 An endpoint only returns responses to traffic that are initiated by resources in the user's VPC.

03 The DNS names created for VPC endpoints can be resolved publicly.

04 Each interface endpoint can support a bandwidth of 10 Gbps for each Availability Zone and can scale up to 40 Gbps.

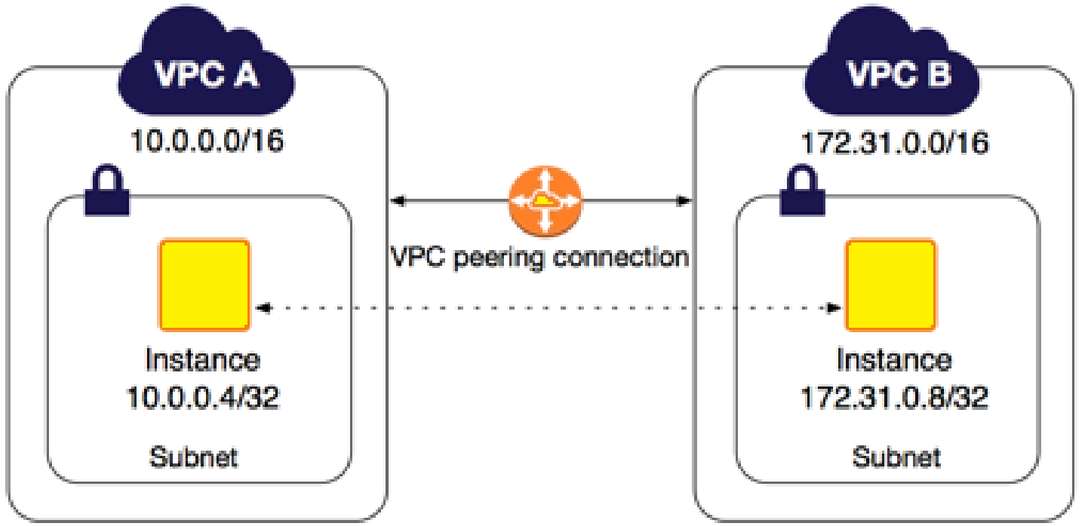
Gateway Endpoints

Gateway endpoints provide reliable connectivity to Amazon S3 and DynamoDB without requiring an Internet gateway or NAT device for the user's VPC.



- Gateway endpoints do not enable AWS PrivateLink.
- There is no additional charge for using gateway endpoints.

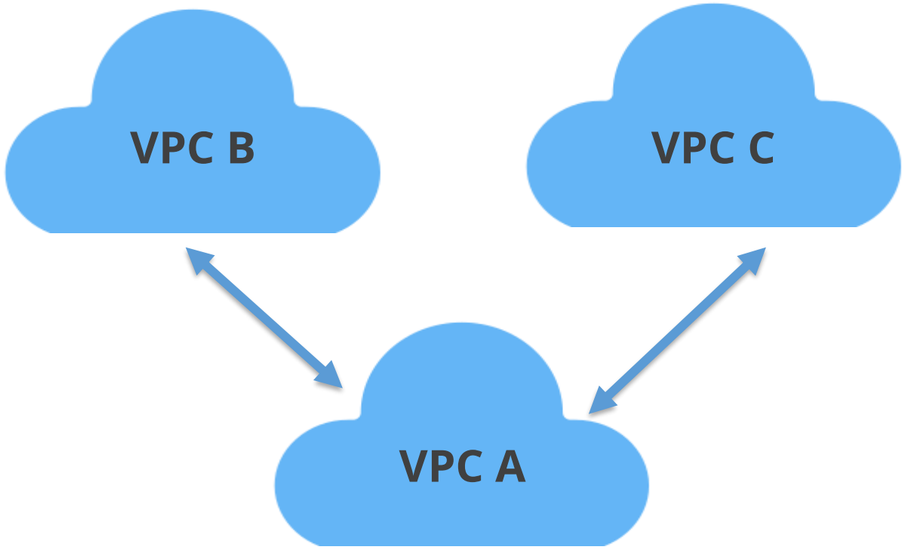
Peering Connection



A VPC peering connection is a networking link that allows users to route traffic between two VPCs using private IPv4 or IPv6 addresses.

Multiple Peering Connection

A VPC peering connection is a direct connection between two VPCs. Multiple VPC peering connections can be created for each VPC that users own. However, transitive peering relationships are not supported.

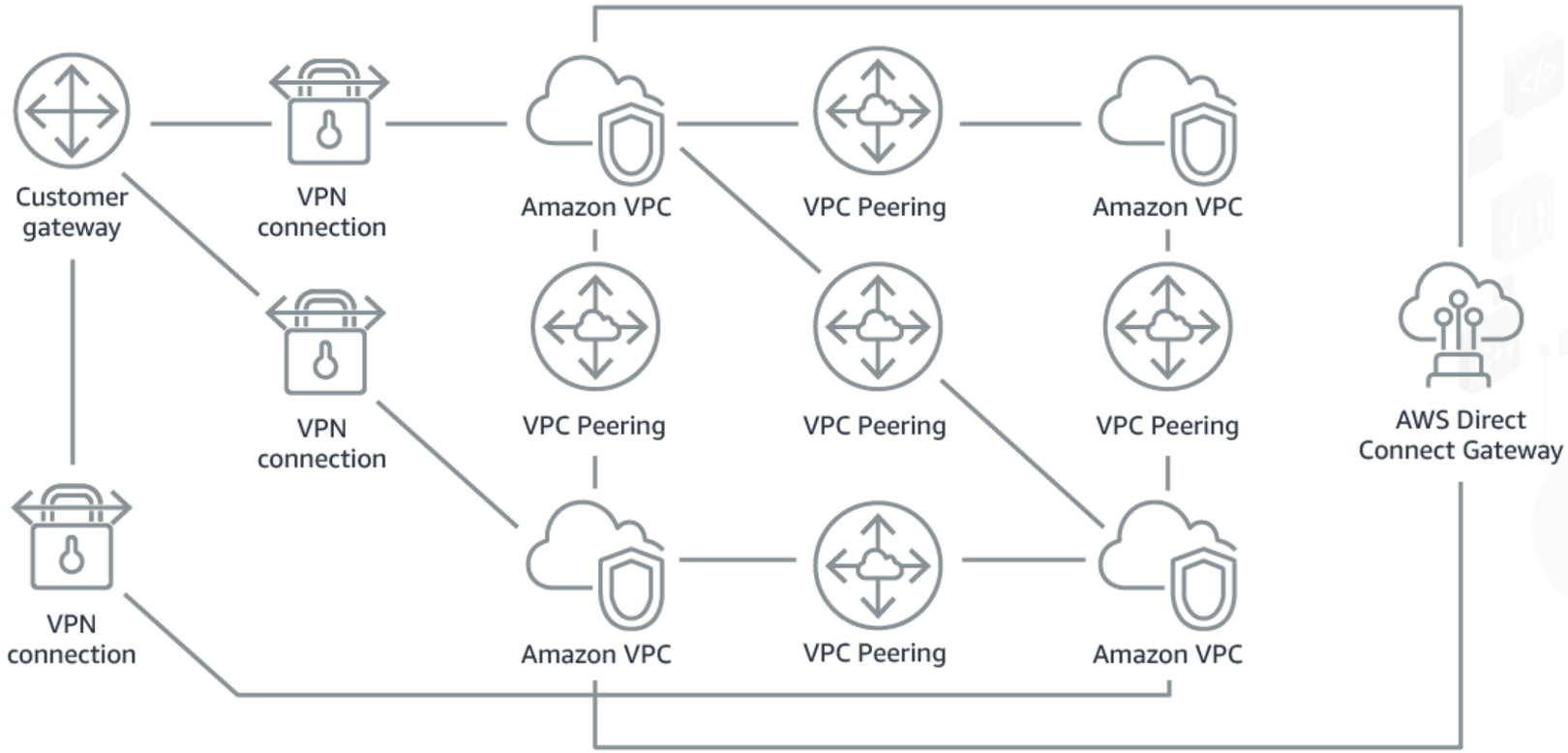


Transit Gateway

The AWS Transit Gateway is a central hub that connects users with Amazon Virtual Private Clouds (VPCs) and on-premises networks. It simplifies user networks and eliminates complicated peering relationships.

Transit Gateway

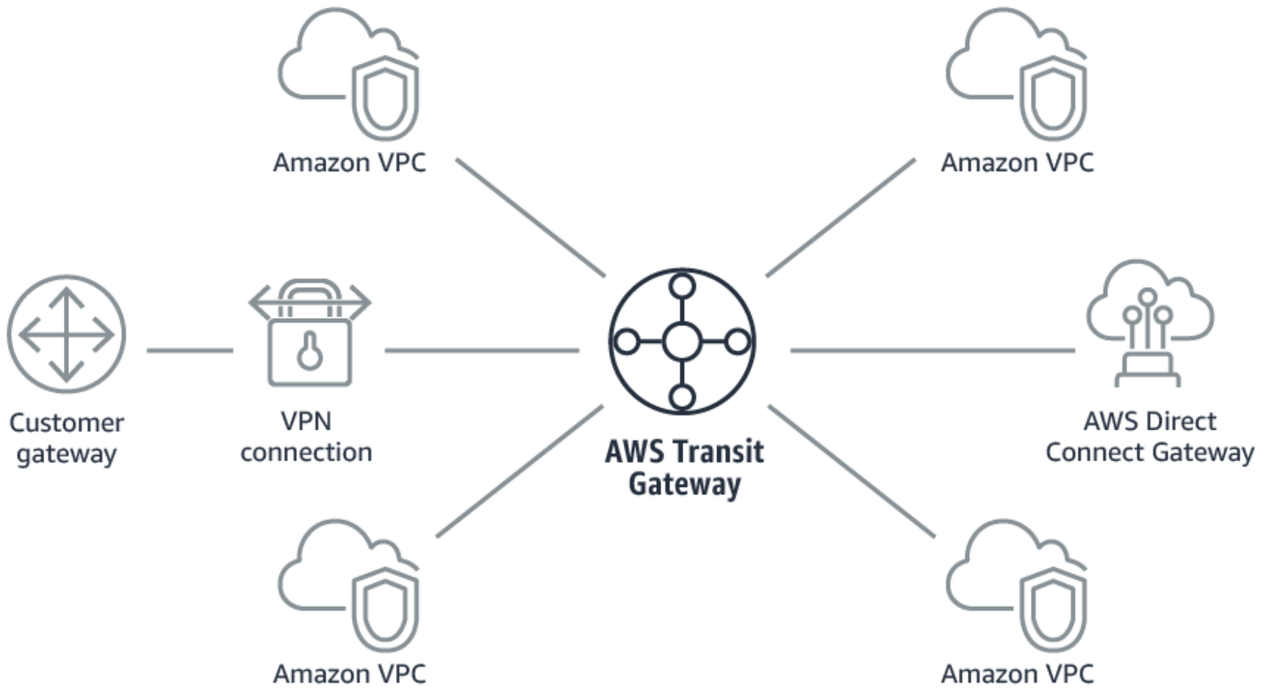
Below is the image of an AWS transit gateway when it is not in use:



https://d1.awsstatic.com/product-marketing/transit-gateway/tgw-before.7f287b3bf00bbc4fbdeadef3c8d5910374aec963.png

Transit Gateway

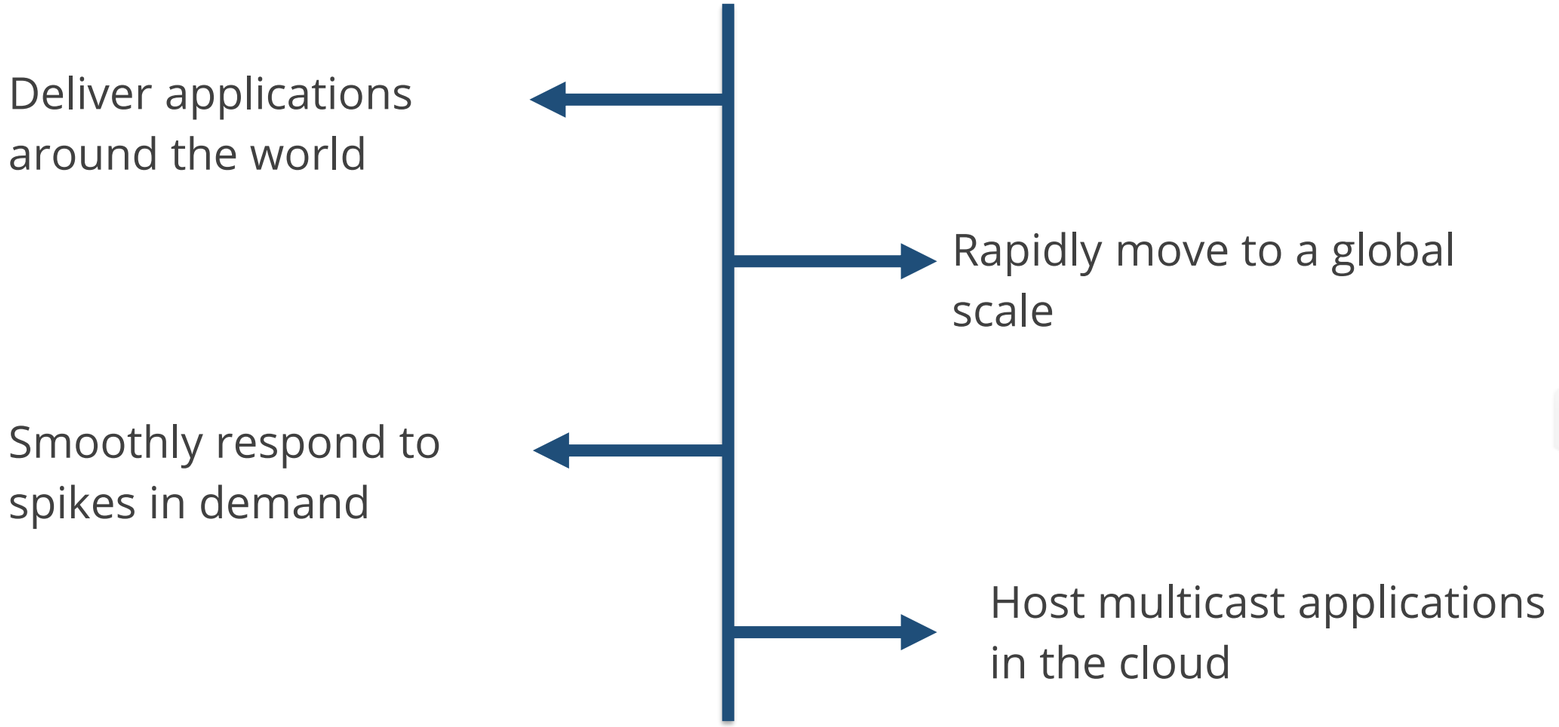
Below is the image of an AWS transit gateway when it is in use:



https://d1.awsstatic.com/product-marketing/transit-gateway/tgw-after.d85d3e2cb67fd2ed1a3be645d443e9f5910409fd.png

Use Cases

Following are the use cases for AWS Transit Gateway:



Public and Private Subnet, Route Table, and NAT

Duration: 20 mins

Problem Statement:

You have been asked to create a public and private subnet, route table and nat.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed:

1. Set up the prerequisites to create public and private subnets
2. Create a route table and NAT

Origin Access Identity (OAI)

Duration: 10 mins

Problem Statement:

You have been asked to block S3 access for the public restrict access only through the CloudFront using OAI .

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed:

1. Set up the prerequisites to create a VPC Flow Log
2. Create a resource access manager, NAT source and destination check

Creating a VPC Endpoint

Duration: 13 mins

Problem statement:

You have been assigned a task to create an VPC Endpoint.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed:

1. Setting up the prerequisites for configuring VPC
2. Creating a VPC Endpoint

VPC Peering Connections

Duration: 10 mins

Problem Statement:

You have been asked to create and connect two VPCs with different regions using a peering connection.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed:

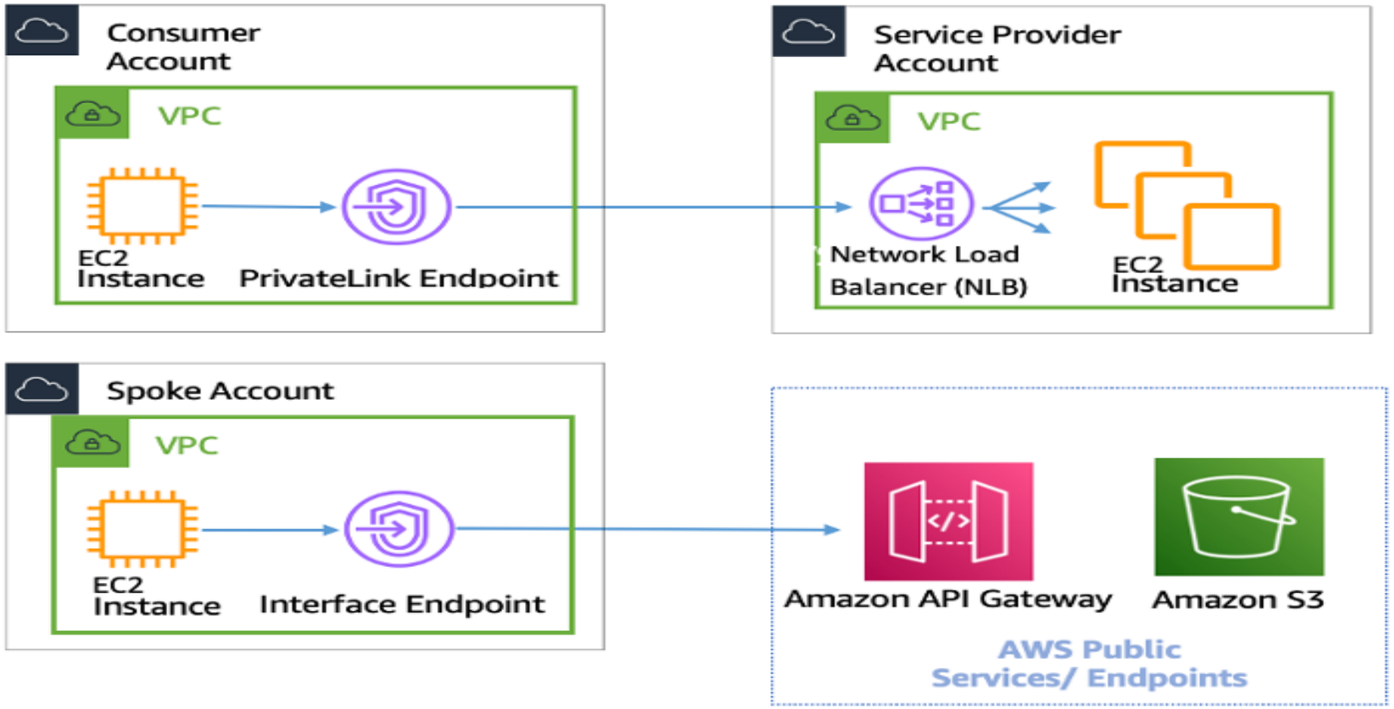
1. Create two VPCs with different regions
2. Establish a peering connection between the VPCs

Private Link and Bastion Host

Private Link

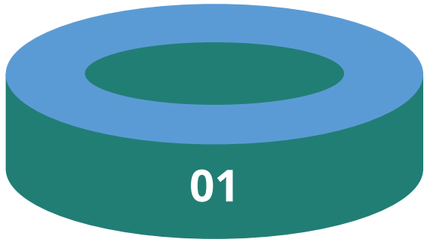
AWS private link provides private connectivity between VPCs, AWS services, and users on-premises networks without exposing the traffic to the public internet.

AWS private link makes it easy to connect services across different accounts and VPCs to significantly simplify your network architecture.

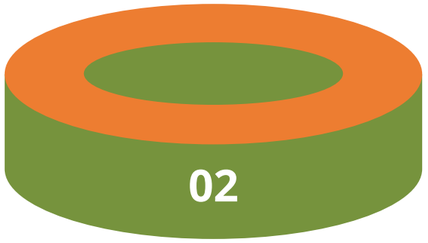


Benefits of Private Link

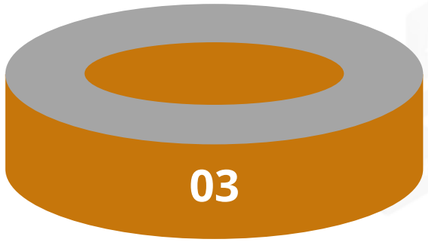
The benefits of private link are as follows:



Private link secures your traffic.



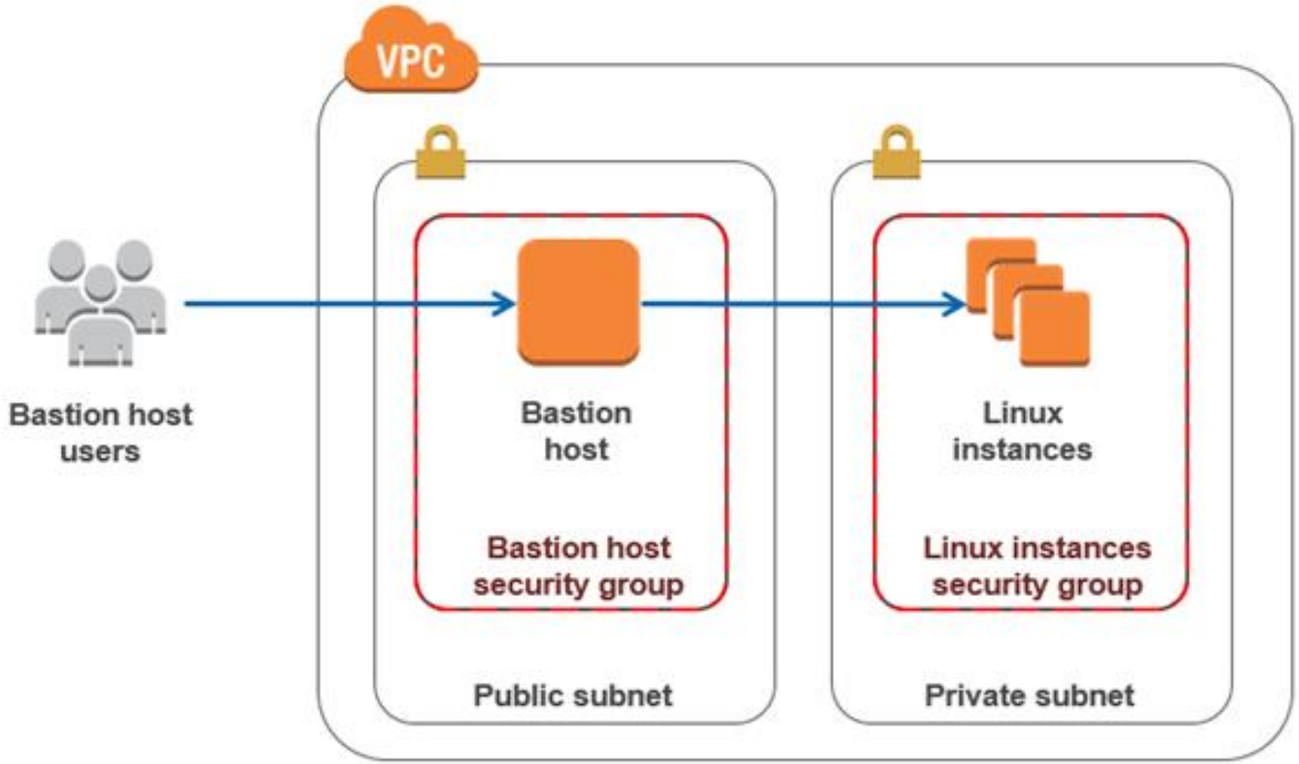
It simplifies network management.



It helps in accelerating your cloud migration.

Bastion Host

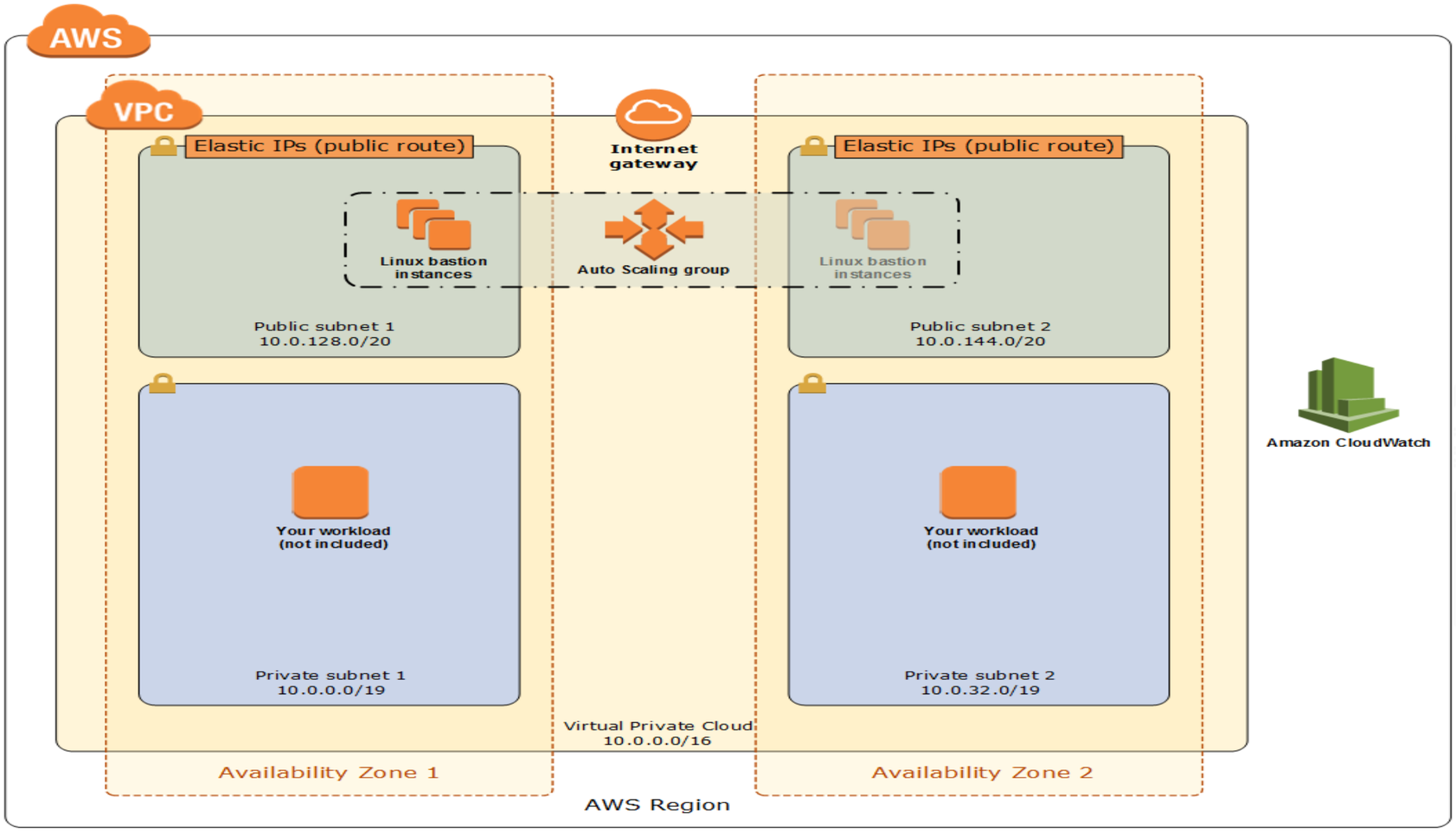
A bastion host is a server whose purpose is to provide access to a private network from an external network, such as the Internet.



Source: https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-established-through-a-bastion-host/

Bastion Host: Architecture

The following diagram shows the Linux bastion host architecture on AWS:

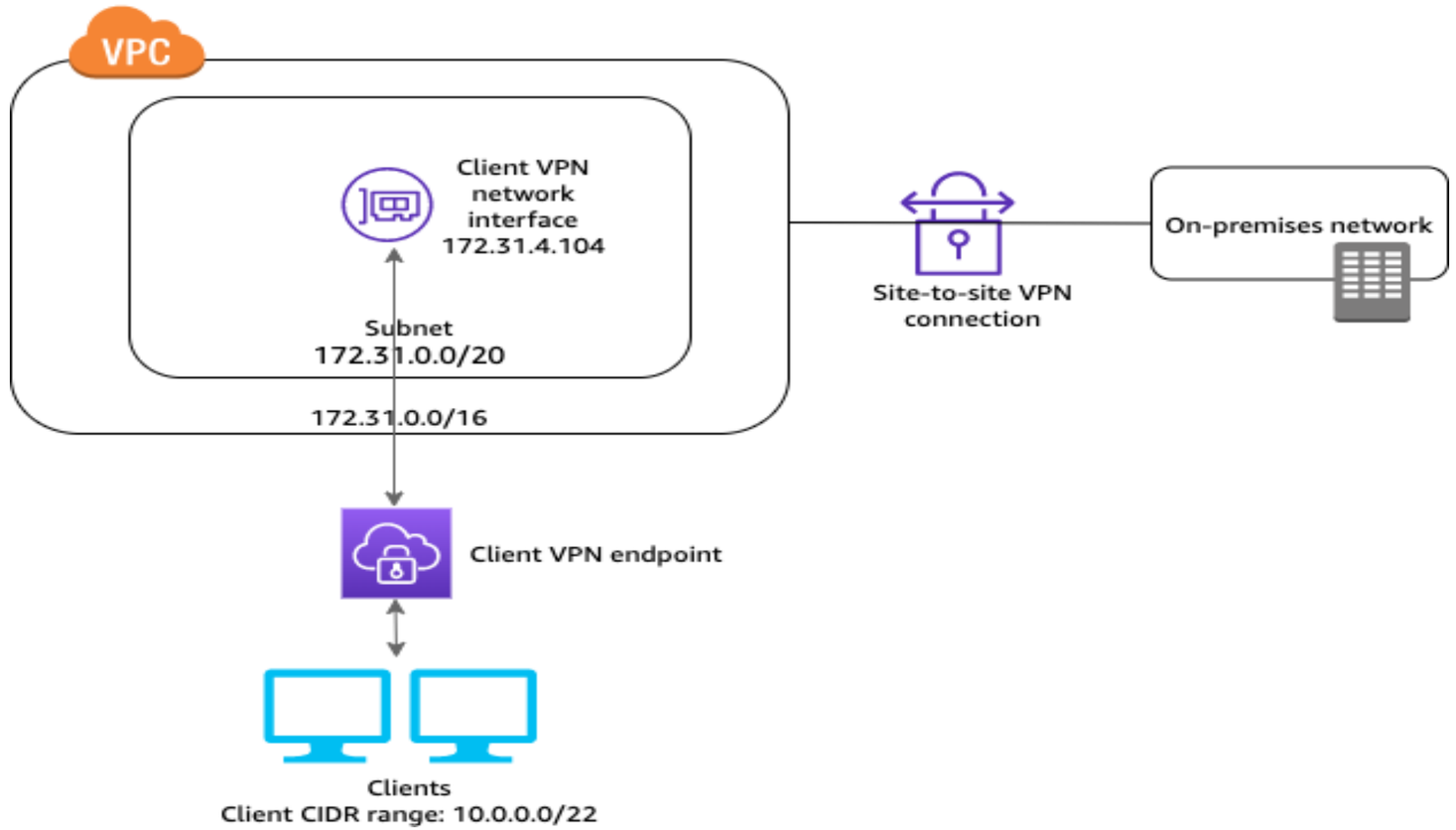


Source: https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html

External Clients

External Clients

The configuration for this scenario includes access to an on-premises network only. We recommend this configuration if users need to give clients access to the resources within an on-premises network.



Steps to Access an On-premises Network

The steps are as follows:

Create a VPC with at least one subnet. Identify the subnet in the VPC that user want to associate with the Client VPN endpoint and note its IPv4 CIDR ranges.

Identify a suitable CIDR range of the client IP addresses that do not overlap with the VPC CIDR.

Review the rules and limitations for client VPN endpoints.

Steps to Implement the Configuration

These are the steps to implement the configuration of Client VPN:

01 Get started with the Client VPN

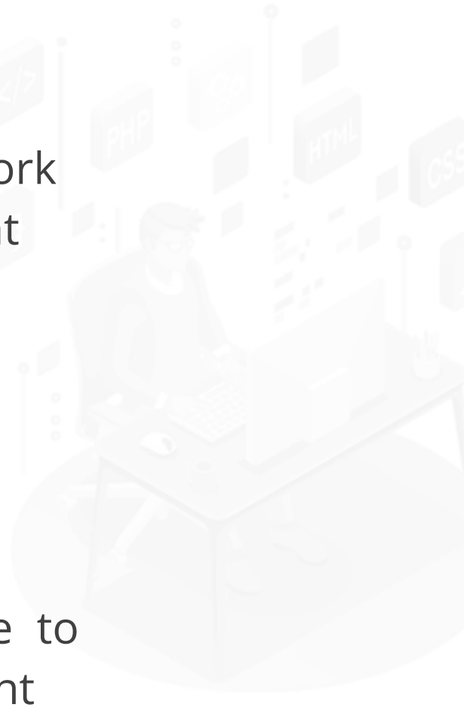
02 Testing the site-to-site VPN connection

03 Create a Client VPN point

04 Associate a target network with a Client VPN point

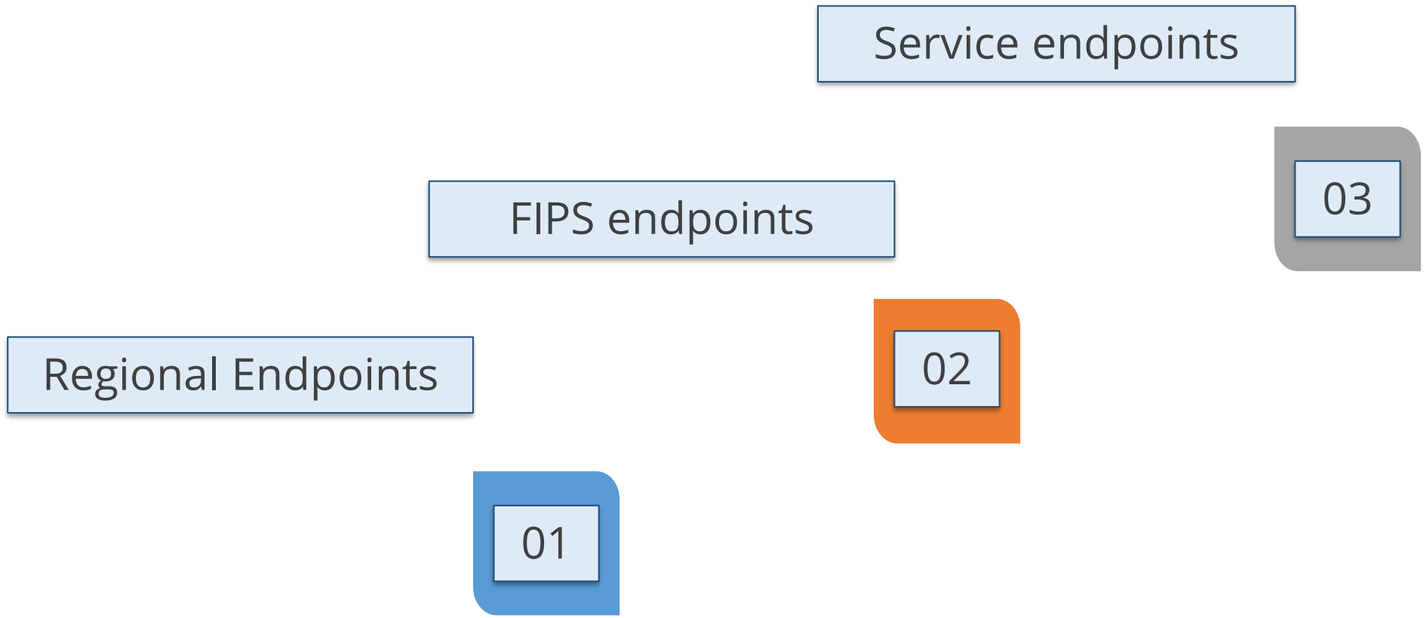
05 Create an endpoint route

06 Add an authorized rule to a Client VPN endpoint



Public Endpoints

To connect programmatically to an AWS service, users use an endpoint. An endpoint is the URL of the entry point for an AWS web service. The different types of endpoints are as follows:



AWS Systems Manager

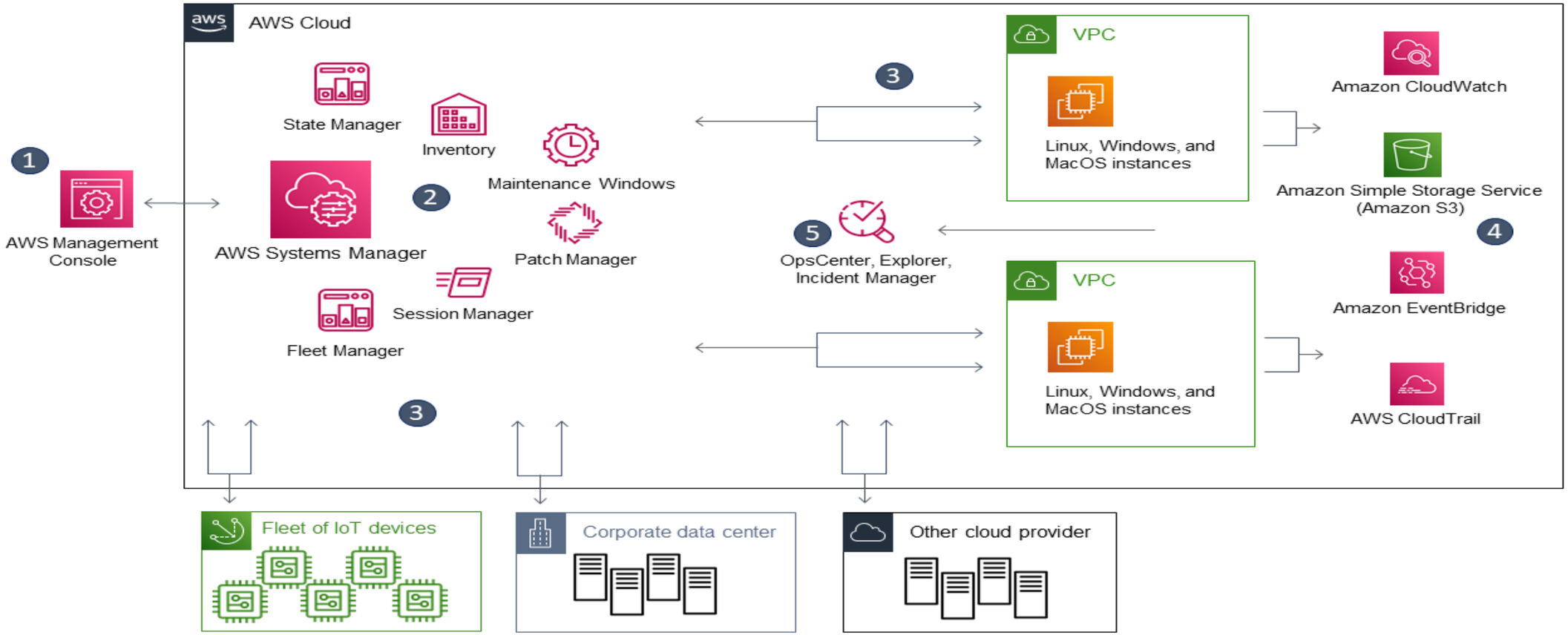
Systems Manager

AWS Systems Manager is a tool that provides visibility and control of the entire AWS infrastructure to the user.

- It integrates with CloudWatch, which allows users to view the dashboard, and operational data, or report bugs.
- It also includes the run command to automate operational tasks such as security patching.
- It also organizes the inventory by grouping resources by application or environment.

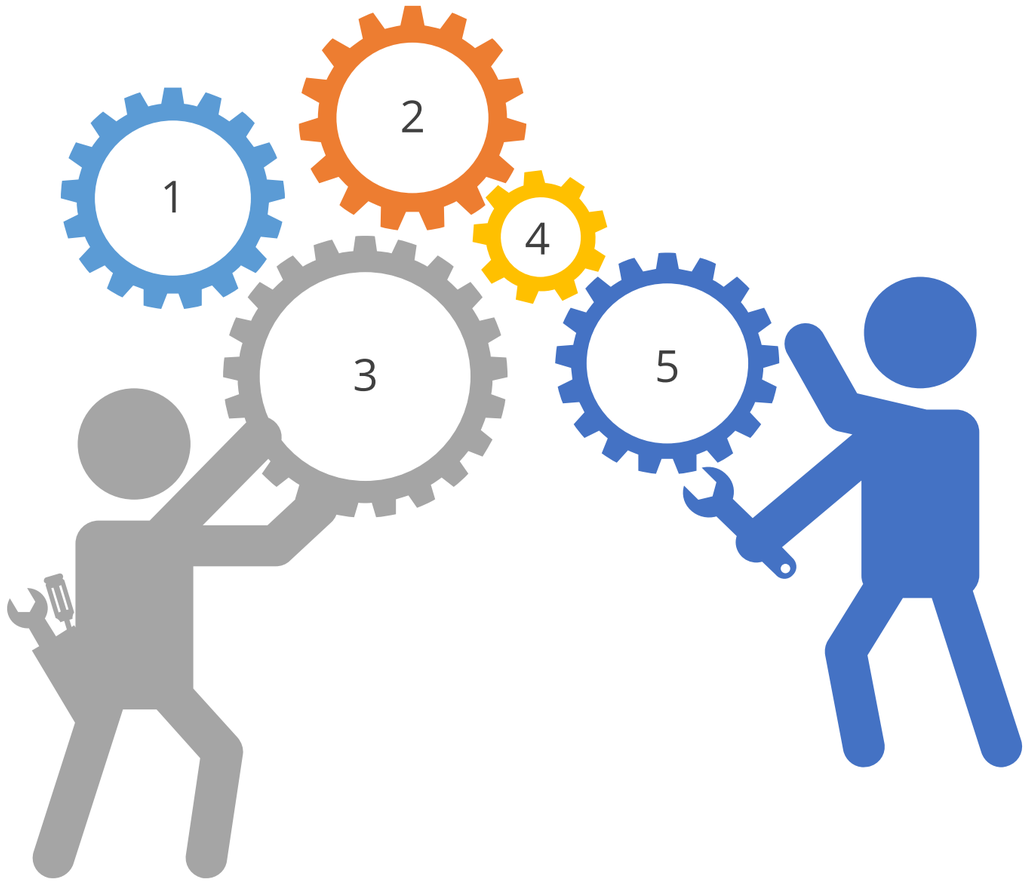
System Manager Process Flow

The general example of System Manager process flow:



System Manager Works in Details

The main points are as follows:

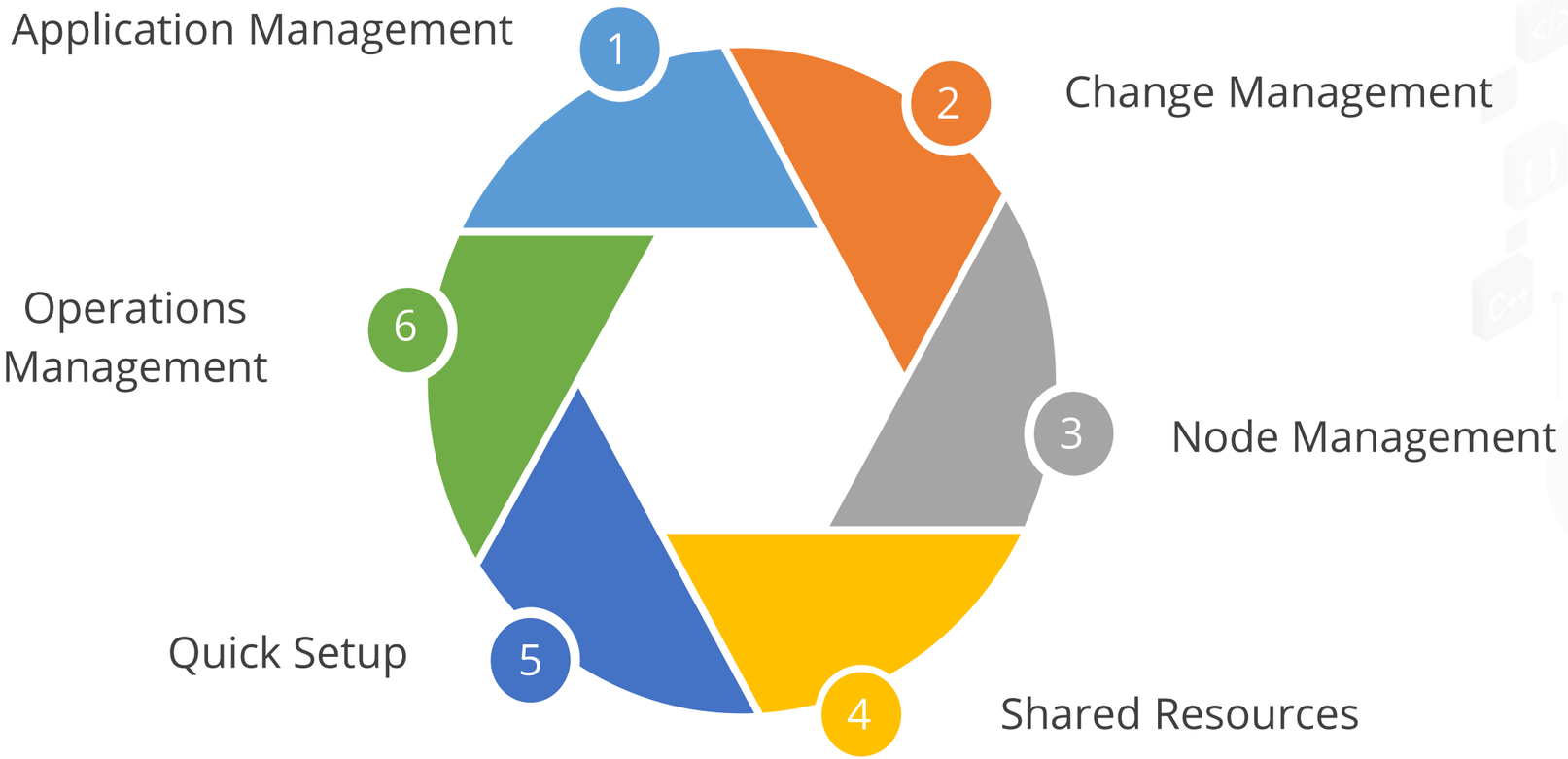


- Access System Manager
- Choose a System Manager
- Verification and processing
- Reporting
- System Manager operations management capabilities

System Manager Capabilities

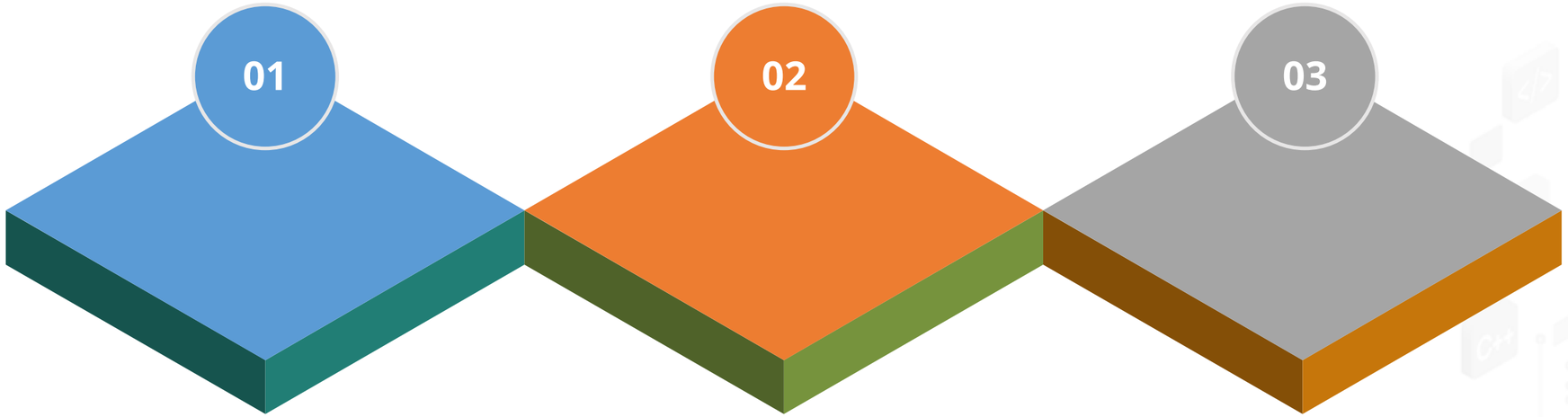
System Manager Capabilities

Systems Manager groups capabilities are divided into the following categories:



Application Management

The Application Management capabilities are as follows:



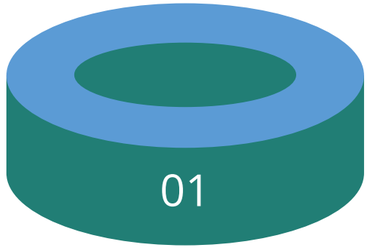
Application Management: An application is a logical group of AWS resources that you want to operate as a unit.

App Configuration: Helps you create, manage, and deploy application configurations and feature flag.

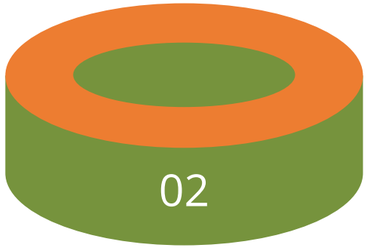
Parameter store: provides secure, hierarchical storage for configuration data and remote management.

Change Management

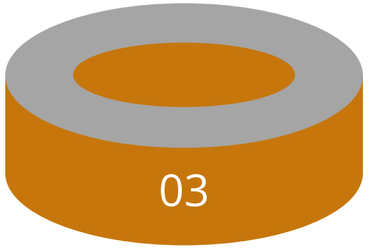
The Change Management capabilities are as follows:



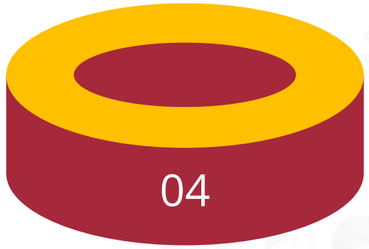
Change Manager: It is an enterprise change management framework for requesting, approving, implementing, and reporting the operational changes to users' application configuration and infrastructure.



Automation: Use automation to automate common maintenance and deployment tasks.



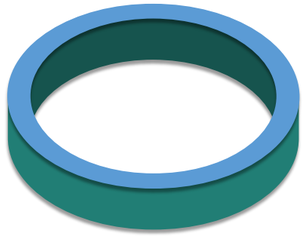
Change Calendar: It helps user set up date and time ranges during the actions you specify.



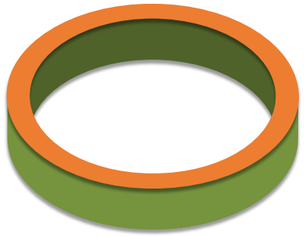
Maintenance Windows: To set up recurring schedules for managed instances to run administrative tasks.

Node Management

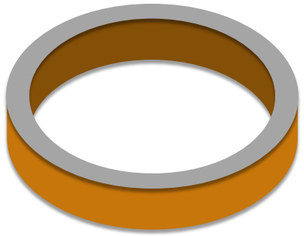
The Node Management capabilities are as follows:



Use Compliance: To scan users' fleet of managed nodes for patch compliance and configuration inconsistencies.



Fleet Manager: is a unified user interface (UI) experience that helps user remotely manage the nodes.



Inventory: Automates the process of collecting software inventory from the managed nodes. You can use inventory to gather metadata about applications, files, components, patches, and more.

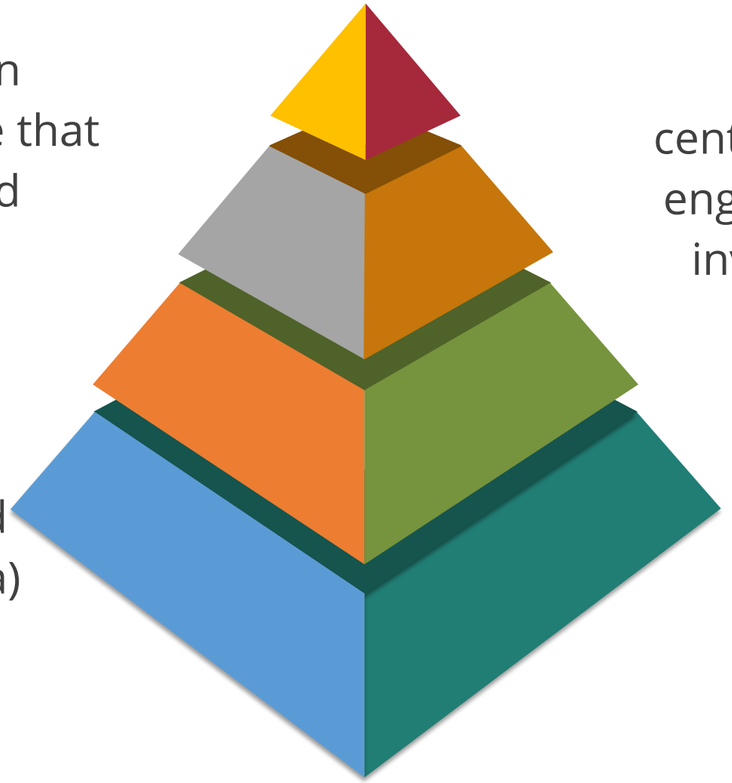
Session Manager: Provides secure and auditable edge device and instance management without needing to open inbound ports, maintain bastion hosts, or manage SSH keys.

Operations Management

The Operations Management are as follows:

Incident Manager: It is an incident management console that helps users to mitigate and recover from incidents.

Explorer: Displays an aggregated view of operations data (Ops Data) for the AWS accounts and across AWS Regions.

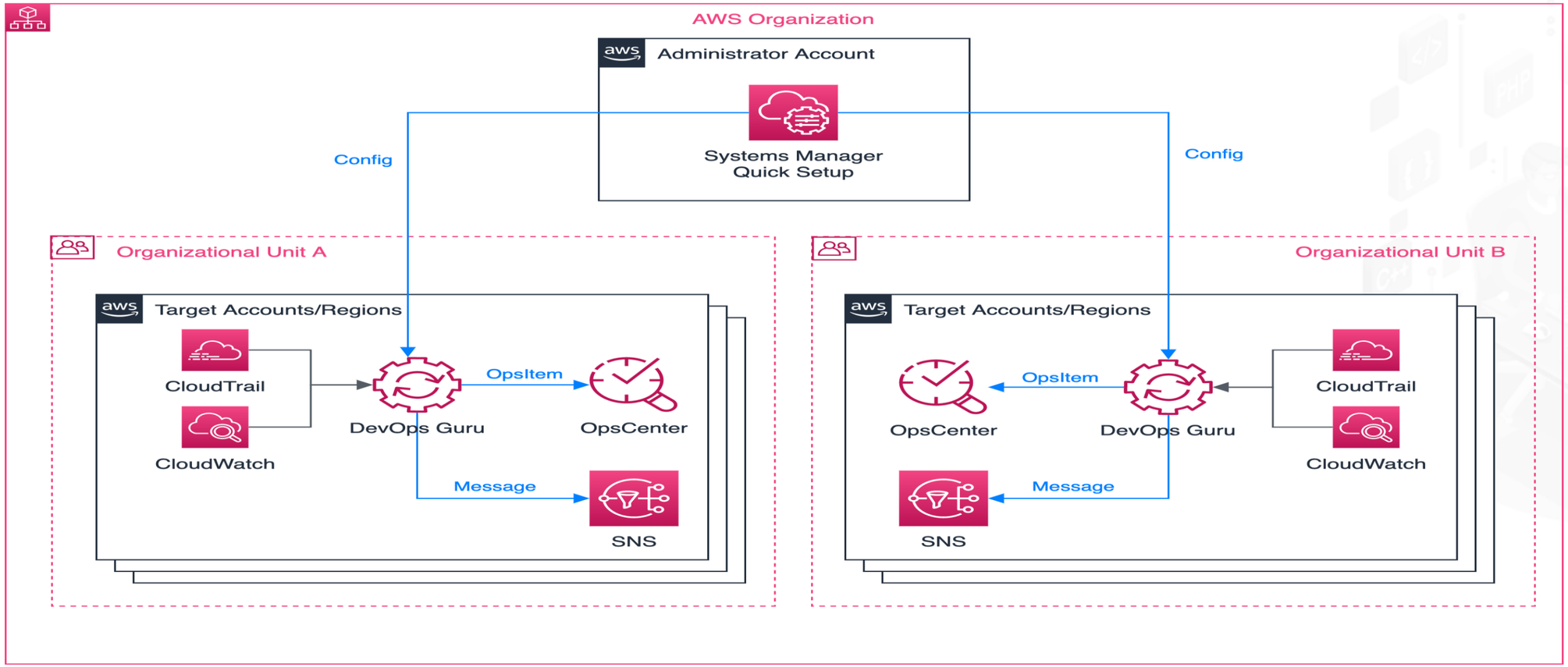


OpsCenter: Provides a central location where operation engineers can view, resolve and investigate operational items related to AWS resources

Amazon CloudWatch: Dashboards are customizable pages in the CloudWatch console that users can use to monitor the resources in a single view.

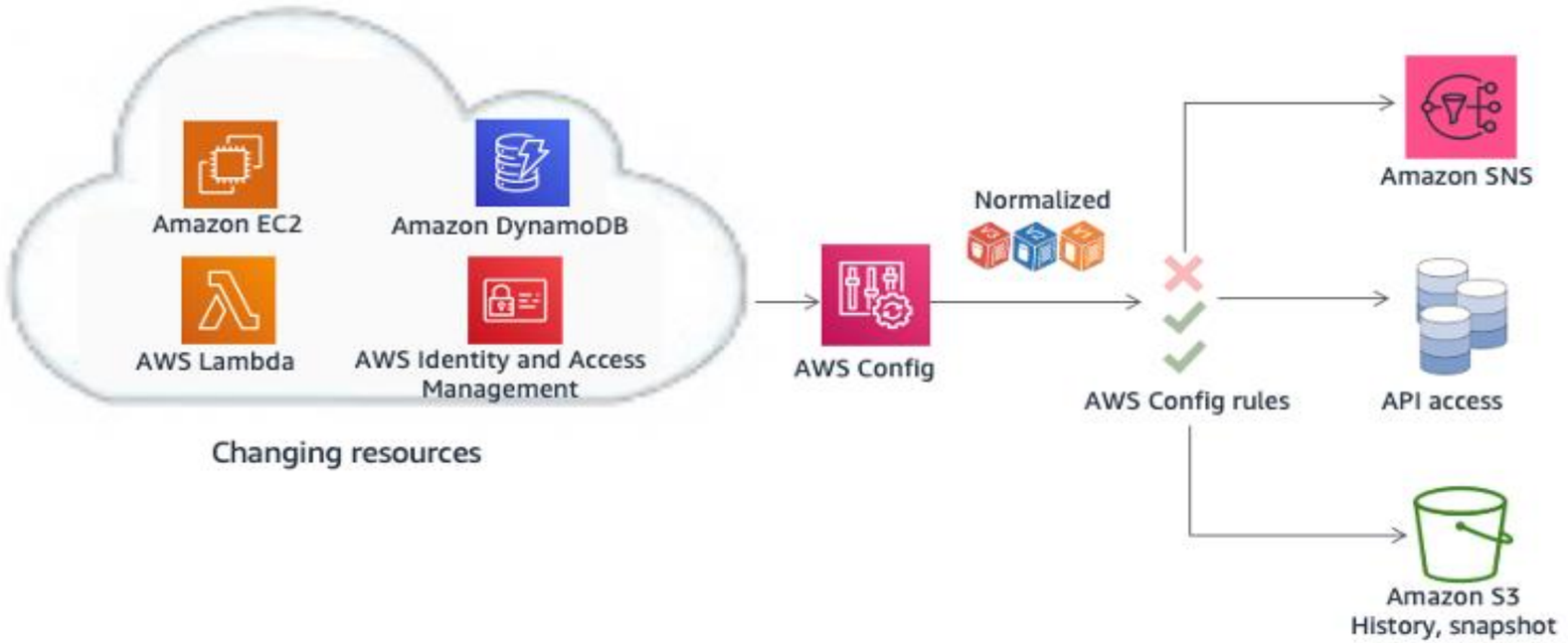
Quick Setup

Quick Setup simplifies setting up services, including Systems Manager, by automating common or recommended tasks. These tasks include, for example, creating the required AWS Identity and Access Management (IAM) instance profile role.



Shared Resources

A Systems Manager document (SSM document) defines the actions that the Systems Manager performs.



SSM document types include the Command documents, which are used by the state manager, Run Command, and Automation runbooks, which are used by Systems Manager Automation.

Accessing Systems Manager

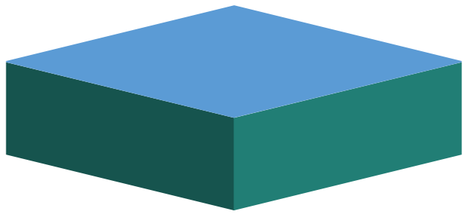
Accessing Systems Manager

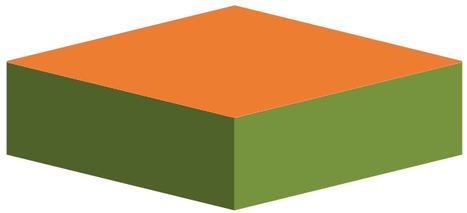
Users can work with the Systems Manager in any of the following ways:

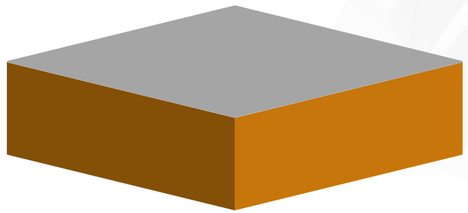
The Systems Manager console is a browser-based interface to access and use the Systems Manager.

AWS IoT Greengrass V2 console - Users can view and manage edge devices that are configured for AWS IoT Greengrass in the Greengrass console.

AWS command line tools- The tools are supported on Linux, macOS, and Windows. Using the AWS Command Line Interface can be faster and more convenient than using the console.







TECHNOLOGY

Virtual Private Network (VPN) Connections

VPN Connections

AWS Virtual Private Network (VPN) solutions establish secure connections between the user's on-premises networks, remote offices, client devices, and the AWS global network.

The following VPN connectivity options help the user to connect the Amazon VPC to remote networks:

01	AWS Site-to-Site VPN
02	AWS Client VPN

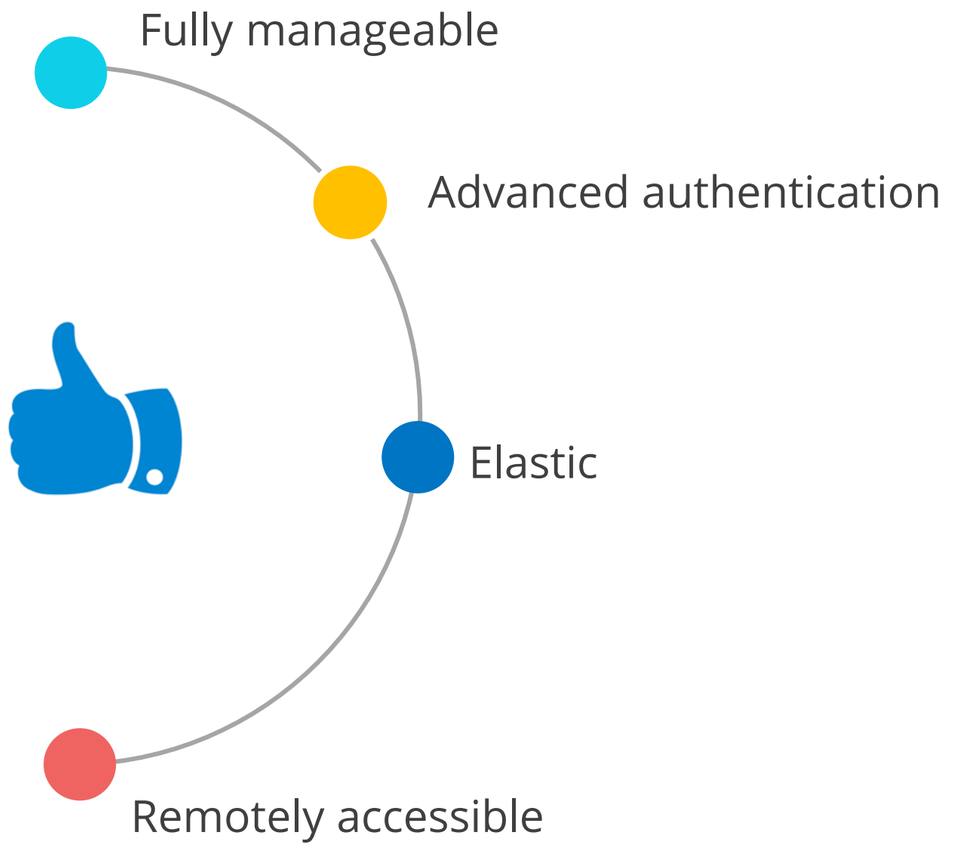
VPN Connections

The following VPN connectivity options help the user to connect the Amazon VPC to remote networks:

03	AWS VPN CloudHub
04	Third party software VPN appliance

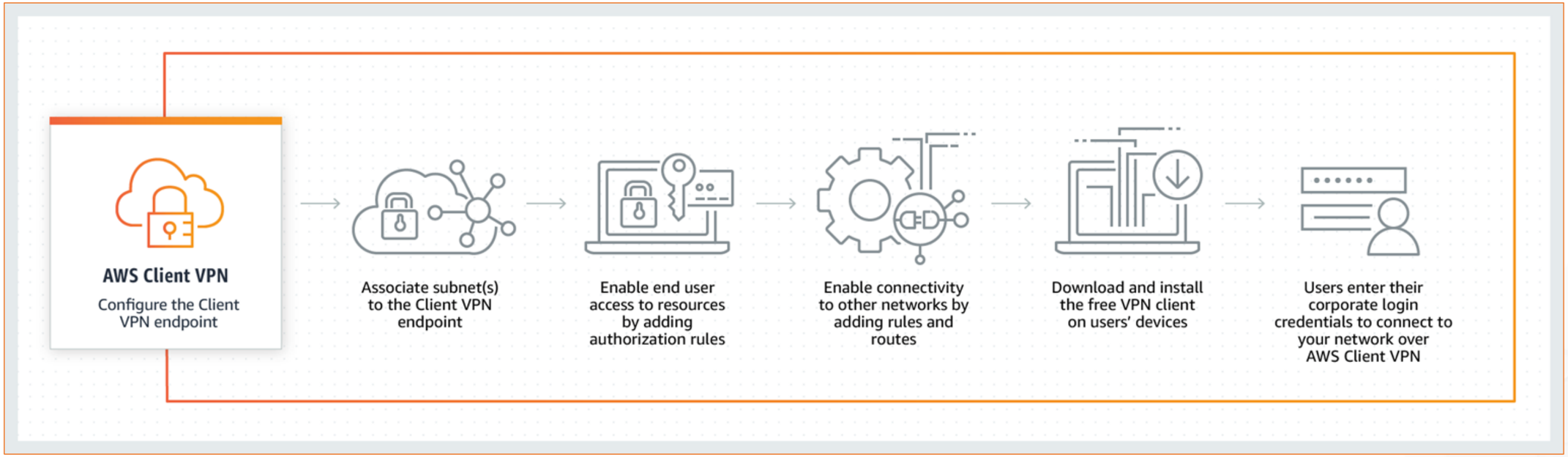
Benefits of VPN Connections

Some of the benefits of VPN connections are as follows:



Working of VPN Connections

The following diagram shows the working of VPN connections:

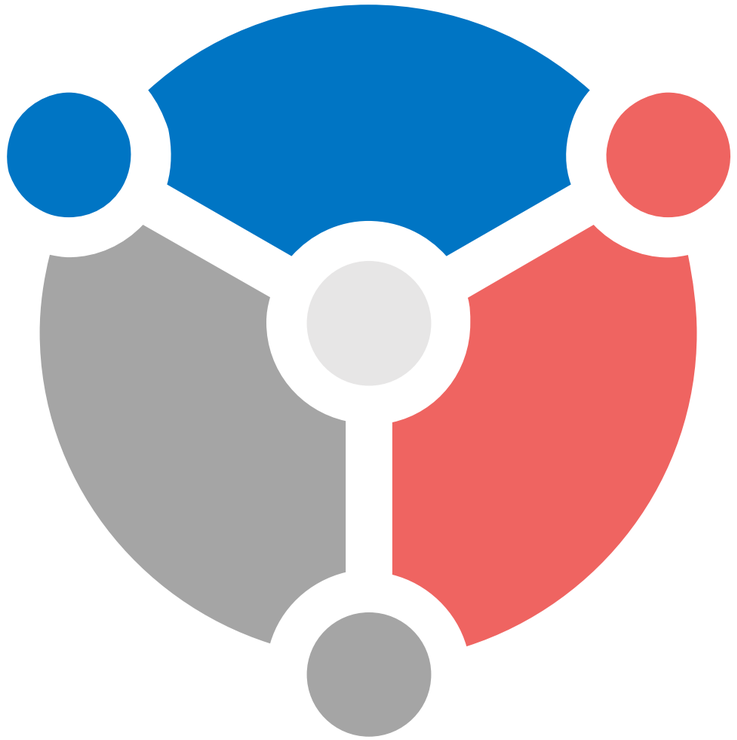


Source: https://aws.amazon.com/vpn/

Use Cases of VPN Connections

The following are the use cases of VPN connections:

Easily access applications in the cloud or on-premises



Easily deploy and remove VPN access for temporary workers

Quickly scale remote access

Direct Connect

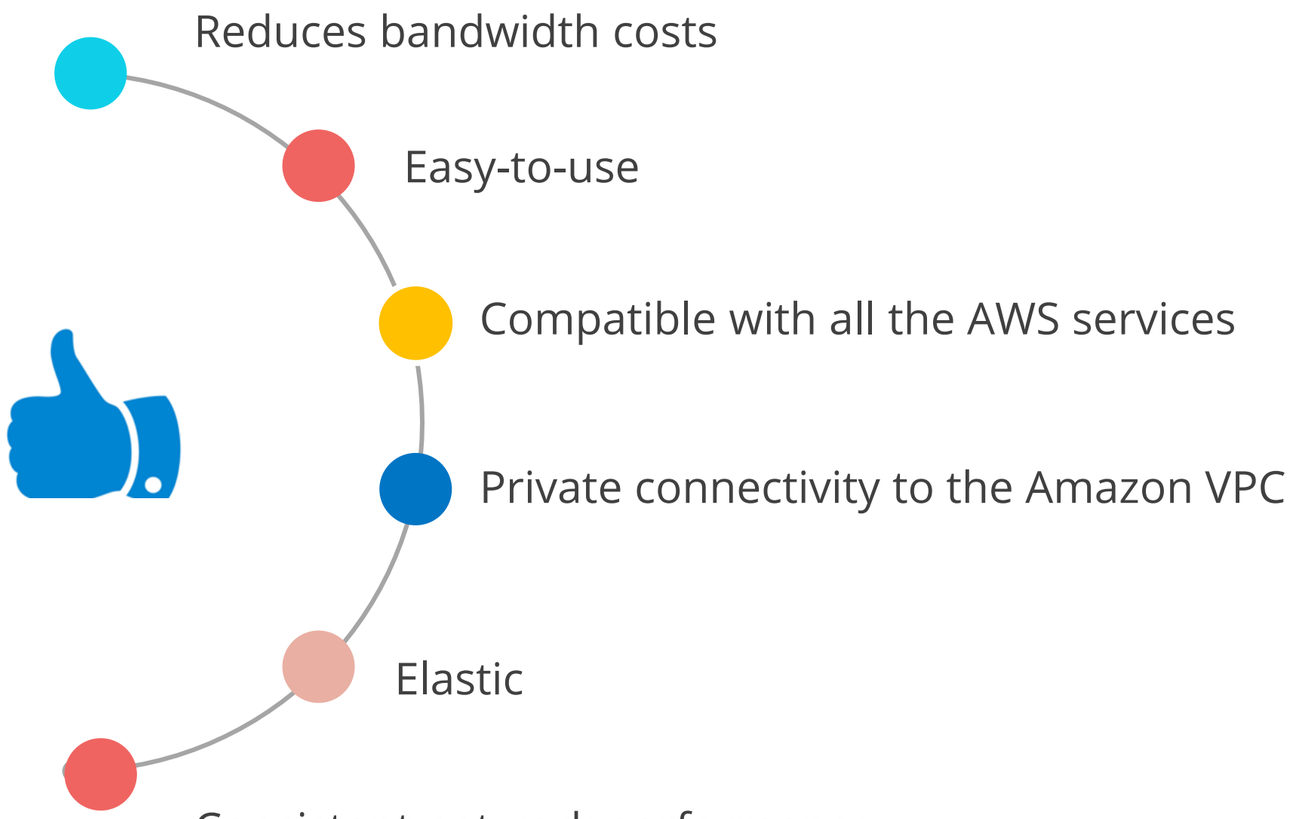
Direct Connect

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from the user's premises to AWS.

More about Direct Connect:

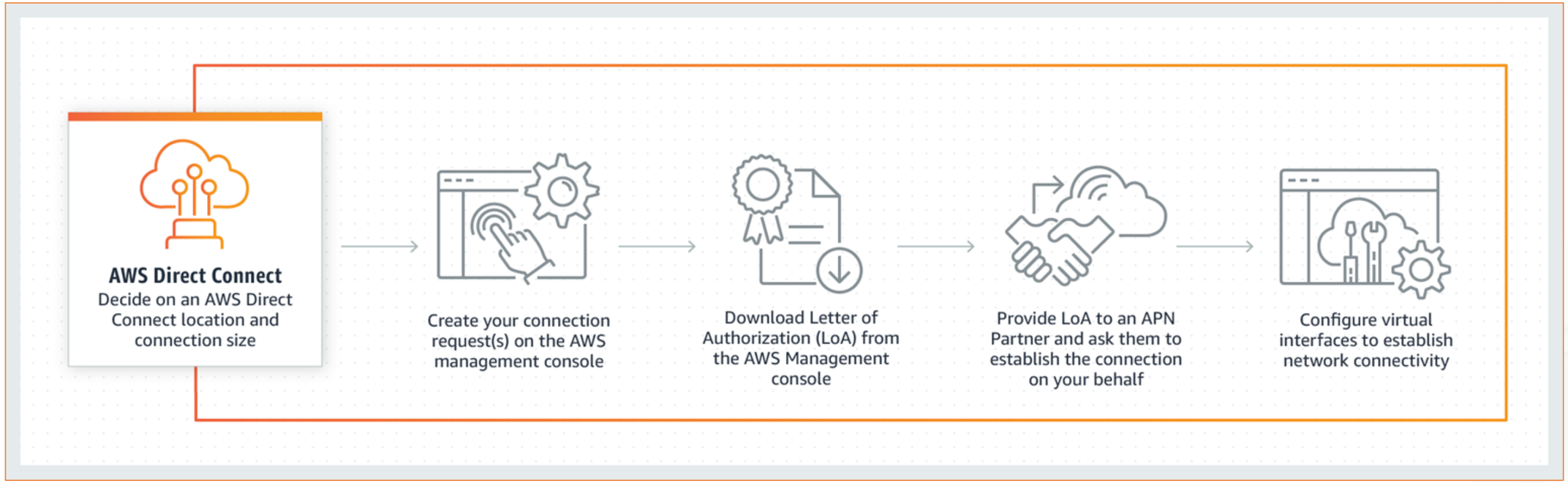
01	It helps to establish private connectivity between AWS and the data center, office, or colocation environment.
02	It helps to establish a dedicated connection between the network and one of the AWS Direct Connect locations.

Benefits of Direct Connect



Working of Direct Connect

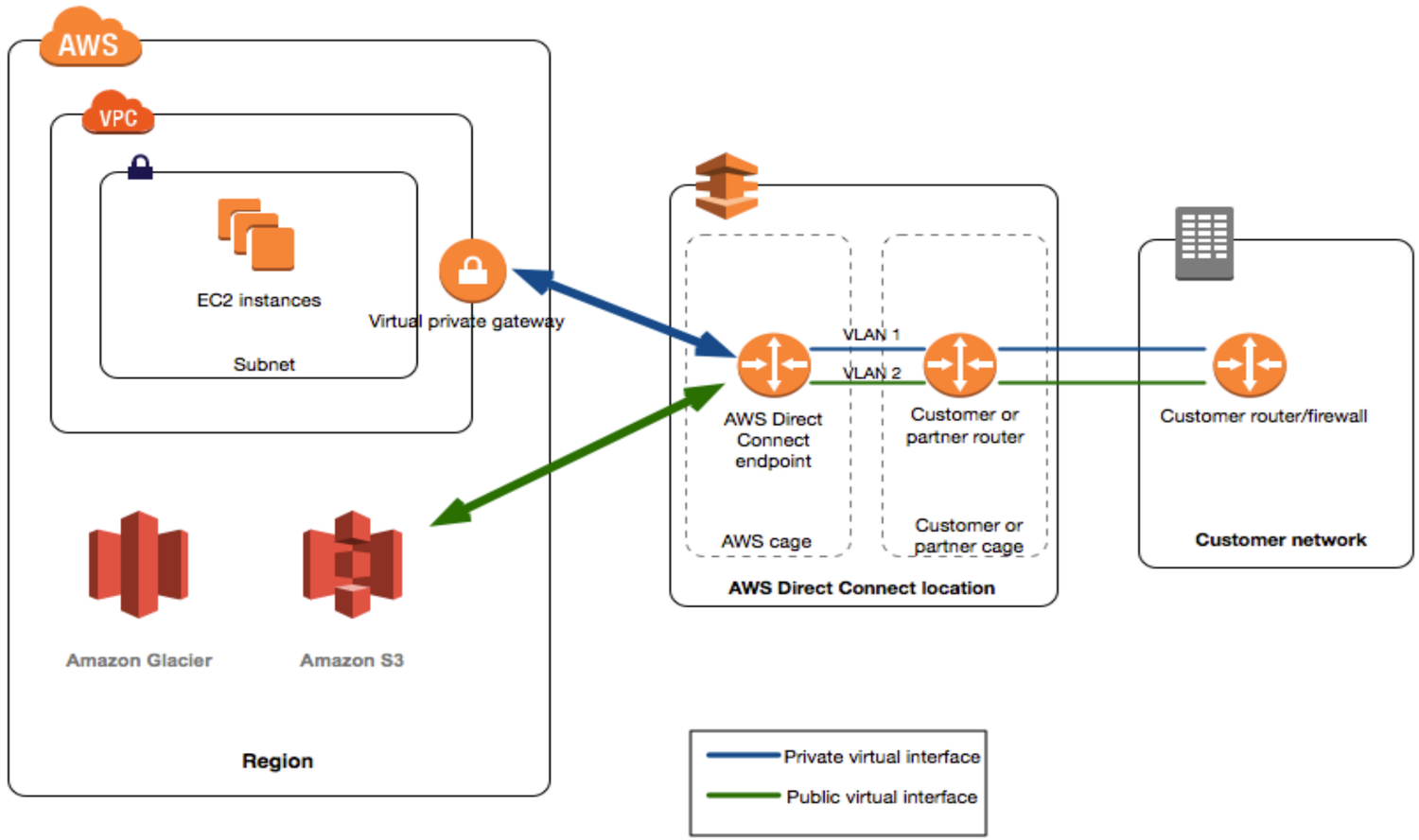
The following diagram shows the working of Direct Connect:



Source: https://aws.amazon.com/directconnect/?nc=sn&loc=1

Working of Direct Connect

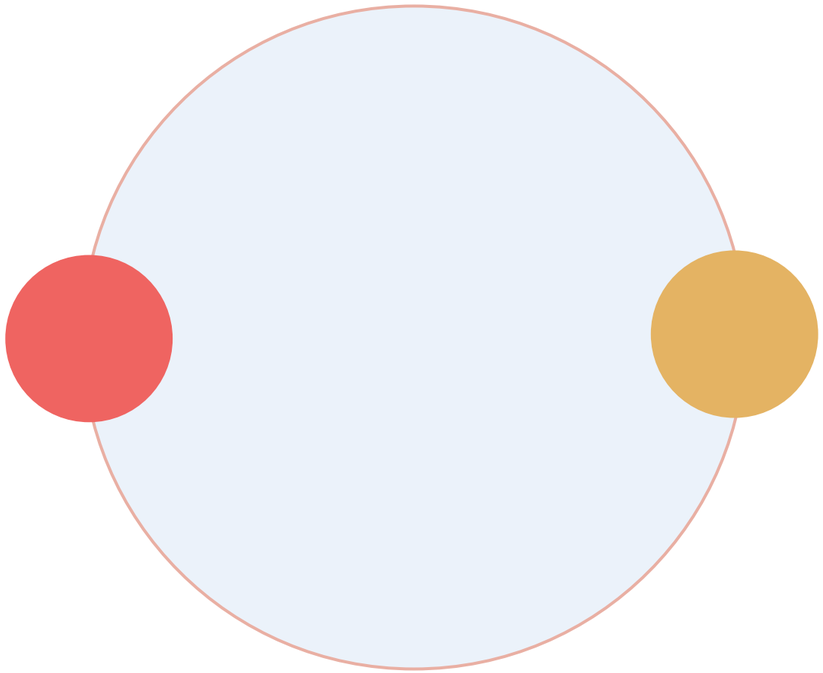
The following diagram shows how AWS Direct Connect interfaces with the network:



Source: https://aws.amazon.com/directconnect/?nc=sn&loc=1

Components of Direct Connect

These are the two key components of Direct Connect:



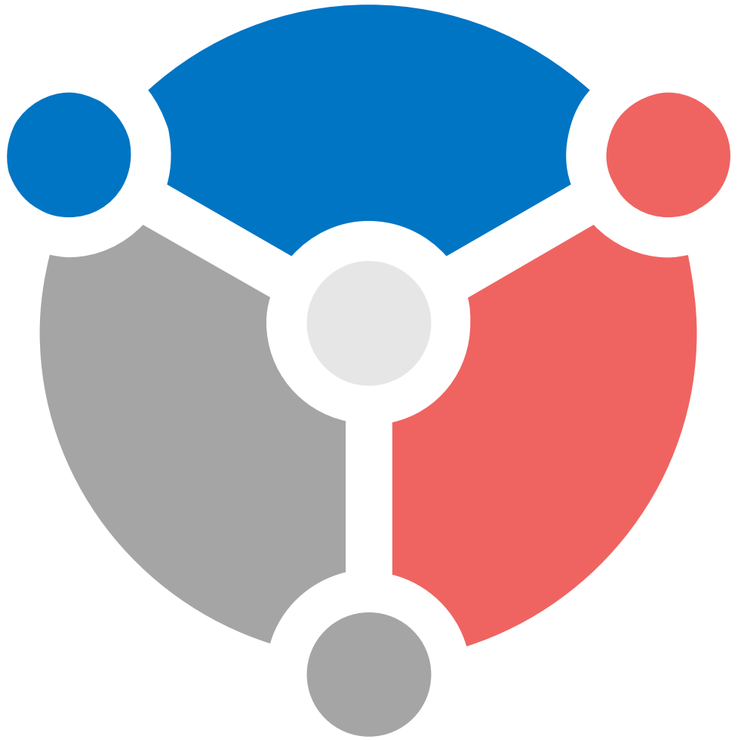
Connections

Virtual interfaces

Use Cases of Direct Connect

The following are the use cases of Direct Connect:

Working with large data sets



Real-time data feeds

Hybrid environments

Direct Connect Costs

The following are the costs associated with Direct Connect:

01	Dedicated connections
02	Hosted connections
03	Data transfer

Direct Connect Costs

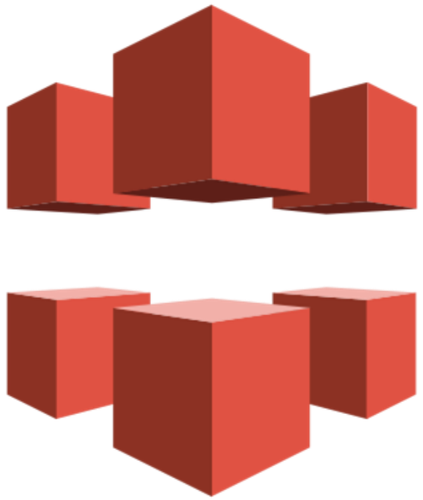
The following are the costs associated with Direct Connect:

04	TCO calculator
05	AWS pricing calculator
06	Economics resource center

Why CloudFront?

Why CloudFront?

Amazon CloudFront is a global content delivery network (CDN) service that securely delivers content to the end users with low latency and high transfer speeds.

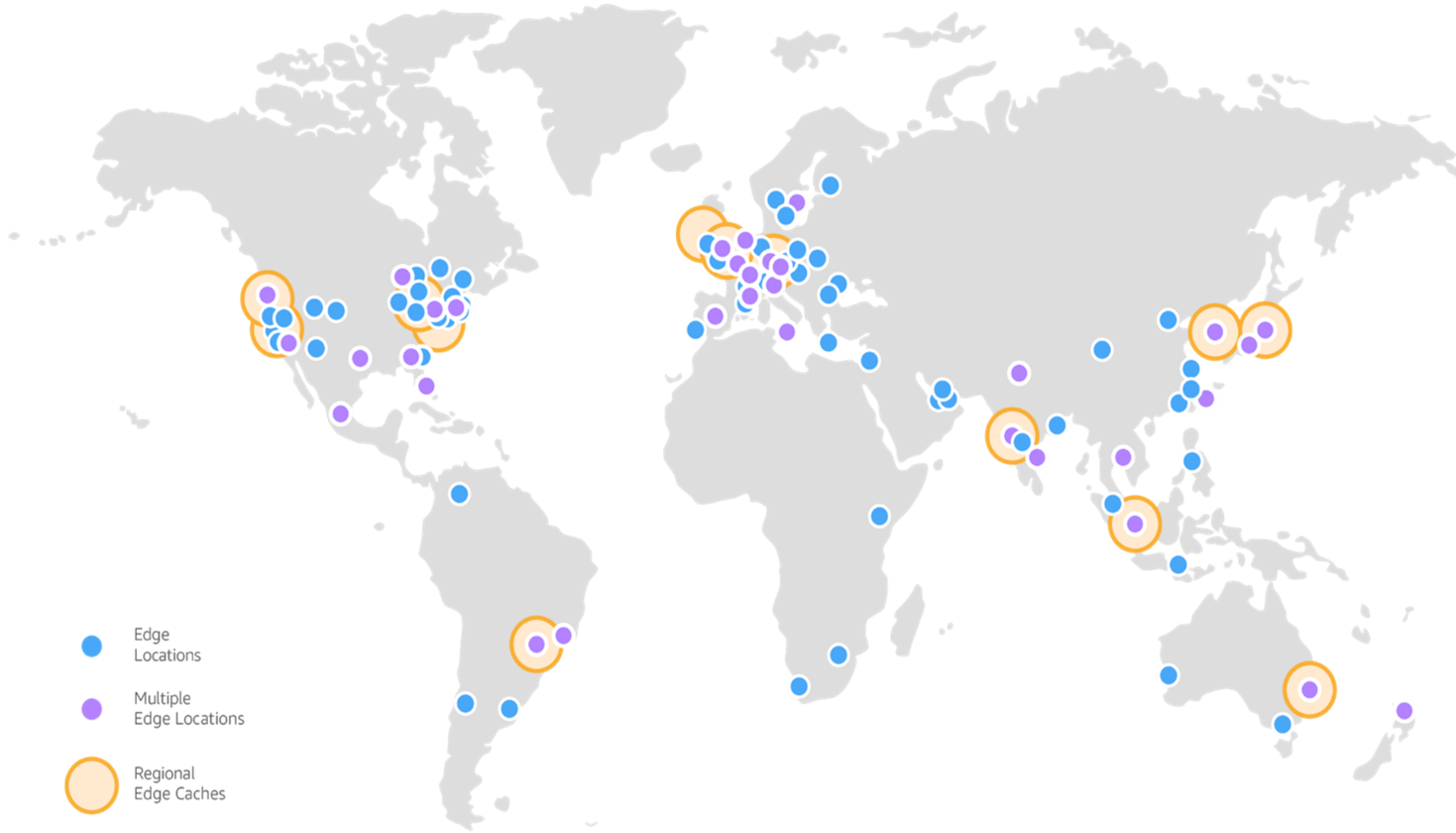


Amazon CloudFront

Source: aws.amazon.com

Points of Presence

Amazon CloudFront Points of Presence (POPs)



Source: aws.amazon.com

Points of Presence

Points of Presence is a single data center.

They speed up website loading by caching web pages and images.

Content Delivery Using CloudFront

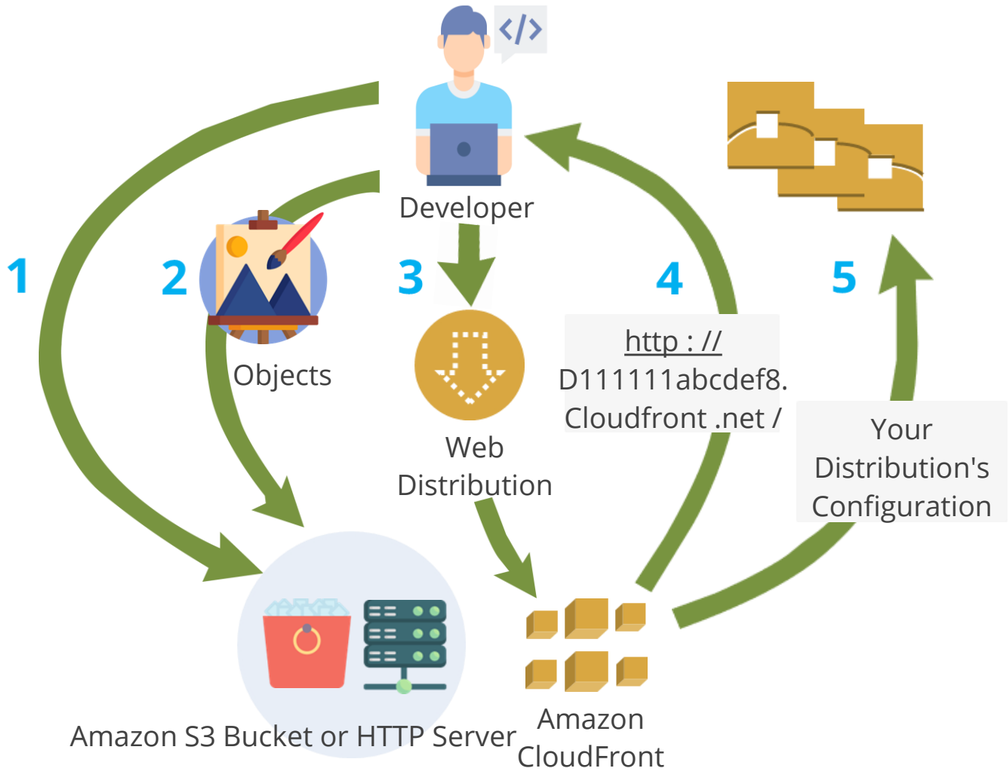
The steps to set up a CloudFront distribution to deliver content are:

1. Specify origin servers
2. Upload data files to the origin servers
3. Create a CloudFront distribution

CloudFront assigns a domain name to the new distribution and sends the distribution's configuration to all its edge locations.

Content Delivery Using CloudFront

A picture representation to set up a CloudFront distribution to deliver content:



Source: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html

Lambda@Edge

What Is Lambda@Edge?

Lambda@Edge is an Amazon CloudFront feature that allows users to access code closer to the application's users, improving speed and lowering latency.

Benefits

Following are the benefits of Lambda@Edge:

1. Makes the apps more responsive
2. Does not have servers to administer
3. Personalizes the content distribution

Working of Lambda@Edge

Lambda@Edge simply runs during the request cycle and makes logical judgments that affect CloudFront content delivery.

Source: https://aws.amazon.com/lambda/edge/

Use Cases

Following are a few important use cases which you can build with Lambda@Edge:

Simplify and reduce origin infrastructure:

Lambda@Edge can be used as an extension or replacement for your origin.

Website security and privacy:

The users can trigger a Lambda function to add HTTP security headers on all origin responses without having to modify the application code on the origin.

Use Cases

Following are a few important use cases which you can build with Lambda@Edge:

Dynamic web application at the edge:

Lambda@edge can be combined with other AWS services to build powerful web applications.

Search Engine Optimization (SEO):

Lambda@Edge can be used to improve search engine optimization for a user's website.

Use Cases

Following are a few important use cases which you can build with Lambda@Edge:

Intelligently route across origins and data centers :

The Load on the origins can be balanced while improving the performance for the users.

Bot mitigation at the edge:

Lambda@Edge can a help user by blocking unwanted bots at the edge and let the authorized traffic go through.

Use Cases

Following are a few important use cases which you can build with Lambda@Edge:

Improved user experience :

Website and web application contents can be personalized without sacrificing the performance .

Real-time image transformation:

A user can customize their experience by transforming images on the fly based on the user characteristics.

CloudFront Security

Security of the Cloud

AWS is responsible for securing the infrastructure that powers AWS services in the AWS Cloud. AWS also offers services that may be used securely. As a part of the AWS compliance process, third-party auditors examine and verify the efficacy of our security on a regular basis.

Source: https://aws.amazon.com/s3/features/replication/

Security in the Cloud

The AWS service determines the obligation. Users are also responsible for additional aspects such as the sensitivity of the data, the requirements of the company, and relevant laws and regulations.

Source: https://aws.amazon.com/s3/features/replication/

Cache Configuration and Invalidation

Duration: 13 mins

Problem statement:

You have been assigned a task to configure a cache and invalidate it.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed:

1. Setting up the prerequisites for configuring cache
2. To configure cache and invalidate it

Origin Access Identity (OAI)

Duration: 10 mins

Problem Statement:

You have been asked to block S3 access for the public restrict access only through the CloudFront using OAI.

ASSISTED PRACTICE

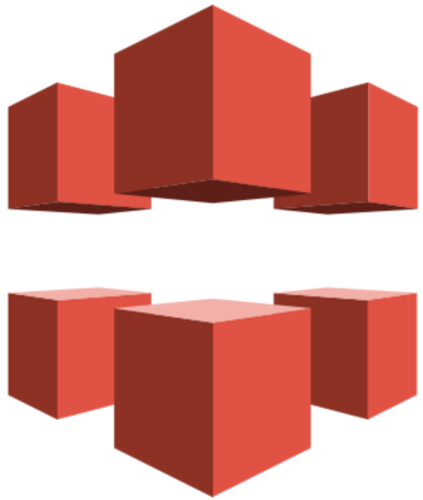
Assisted Practice: Guidelines

Steps to be followed:

1. Create an S3 bucket
2. Restrict the access only through the CloudFront using OAI

CloudFront with S3 origin

S3 bucket access can be secured using CloudFront Origin Access Identity (OAI) when using S3 origin with CloudFront.



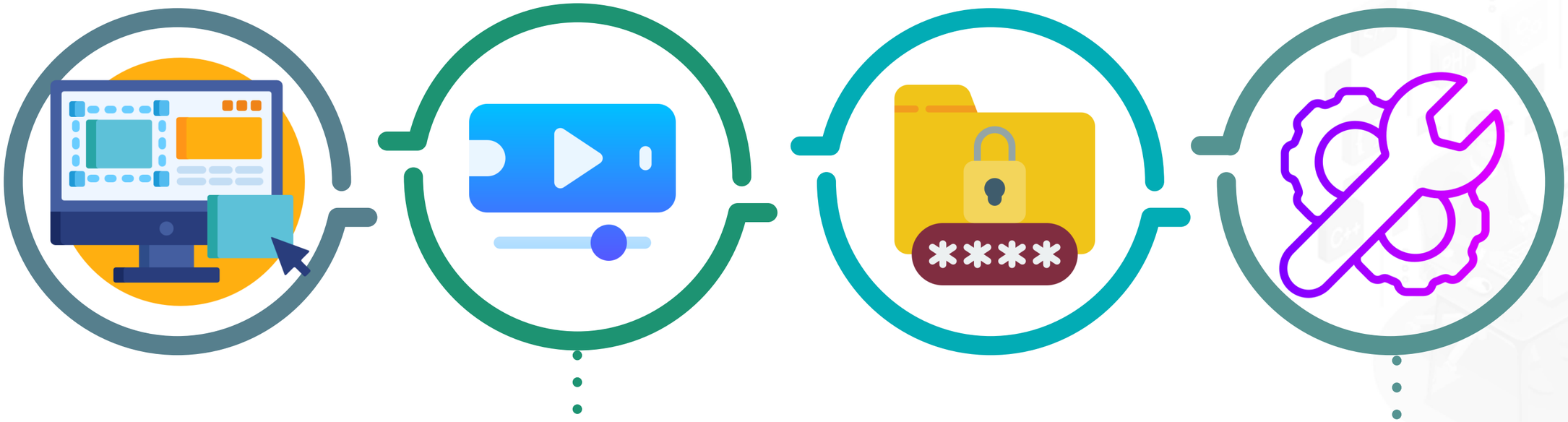
CloudFront with S3 origin

A CloudFront distribution uses the principle that OAI provides so that S3 can authenticate with it and S3 permits CloudFront distribution access to the content by granting this OAI principal permission to perform the s3:GetObject action in the bucket policy.

```
{
    "Sid": "StmtCFOAI",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity <OAI ID>"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::<s3 bucket name>/*"
}
```

CloudFront

The use cases for Amazon CloudFront are as follows:



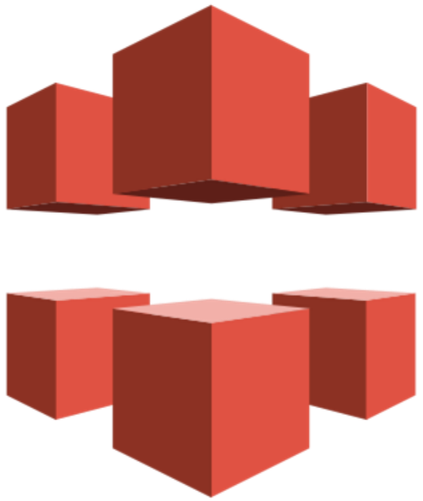
Accelerate static website content delivery

Serve video on demand or live streaming video

Encrypt specific fields throughout system processing

Customize the edge

Benefits of CloudFront



- It will reduce the burden and cache users' content in edge locations, resulting in excellent application availability.
- It guarantees increased productivity and is easy to use.
- It makes it easier to send content to specified end users via GEO targeting services.
- It utilizes HTTP or HTTPS protocols for rapid content delivery.

CloudFront Distribution with S3 Origin

Duration: 10 mins

Problem Statement:

You have been asked to host a static web content in an Amazon S3 bucket that is protected and accelerated by Amazon CloudFront.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed:

1. Create an S3 bucket
2. Upload a file
3. Configure Amazon CloudFront

Global Accelerator

Amazon Global Accelerator

Amazon Global Accelerator is used to improve the performance of an application for local and global users.

Amazon Global Accelerator

Depending on the type, the application can gain additional benefits from the accelerator.

- Standard accelerator improves the availability of your internet application that is used by the global audience. It directs traffic over the AWS global network to the nearest region to the client.

- You can map one or more users to a particular destination by utilizing a custom routing accelerator.

Amazon Global Accelerator

There are two static Anycast IPv4 addresses offered by the Global Accelerator.

The supported endpoints have included the following:

- Internet-facing Application Load Balancer (ALB)
- Internal Application Load Balancer (ALB)
- Internet-facing Network Load Balancer (NLB)
- Elastic IP
- EC2 Instance (with or without Public IP)

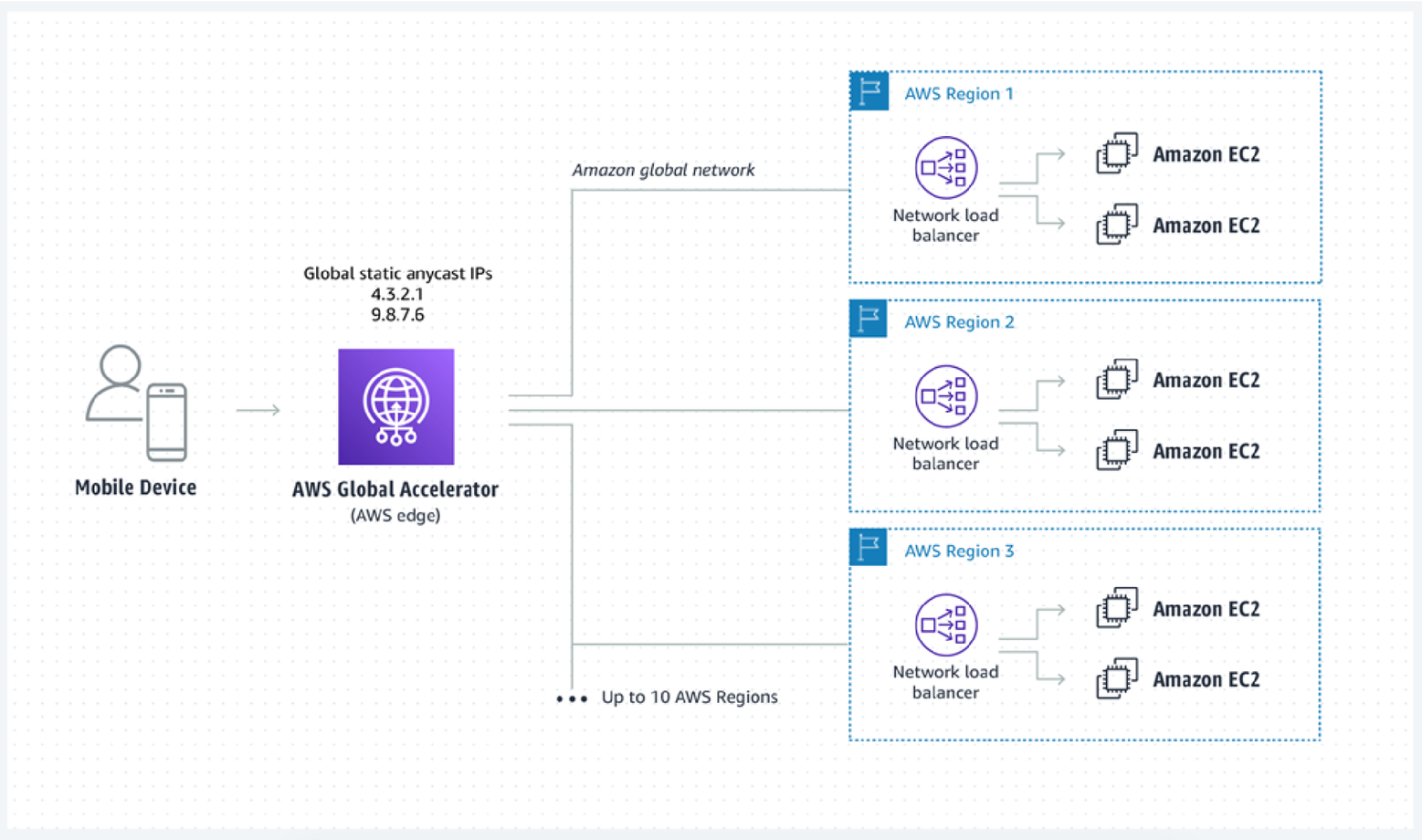
How Amazon Global Accelerator Works

For clients, the static IP addresses offered by AWS Global Accelerator act as a single fixed entry point and using Global Accelerator linking the static IP addresses to local endpoints in one or more AWS Regions when configuring the accelerator.

- **Standard accelerators**, traffic is forwarded to the fastest AWS endpoint based on the user's location, the endpoint's state, and the endpoint weights you define.
- **Custom routing accelerators**, based on the external static IP address and listener port that you give, each client is routed to a specific Amazon EC2 instance and port in a VPC subnet.

Amazon Global Accelerator

The Global Accelerator decreases the number of hops required before a TPC or UDP package enters Amazon's network, optimizing the route for each client and lowering latencies.



Create a Global Accelerator

Duration: 13 mins

Problem statement:

You have been assigned a task to create a global accelerator.

ASSISTED PRACTICE

Assisted Practice: Guidelines

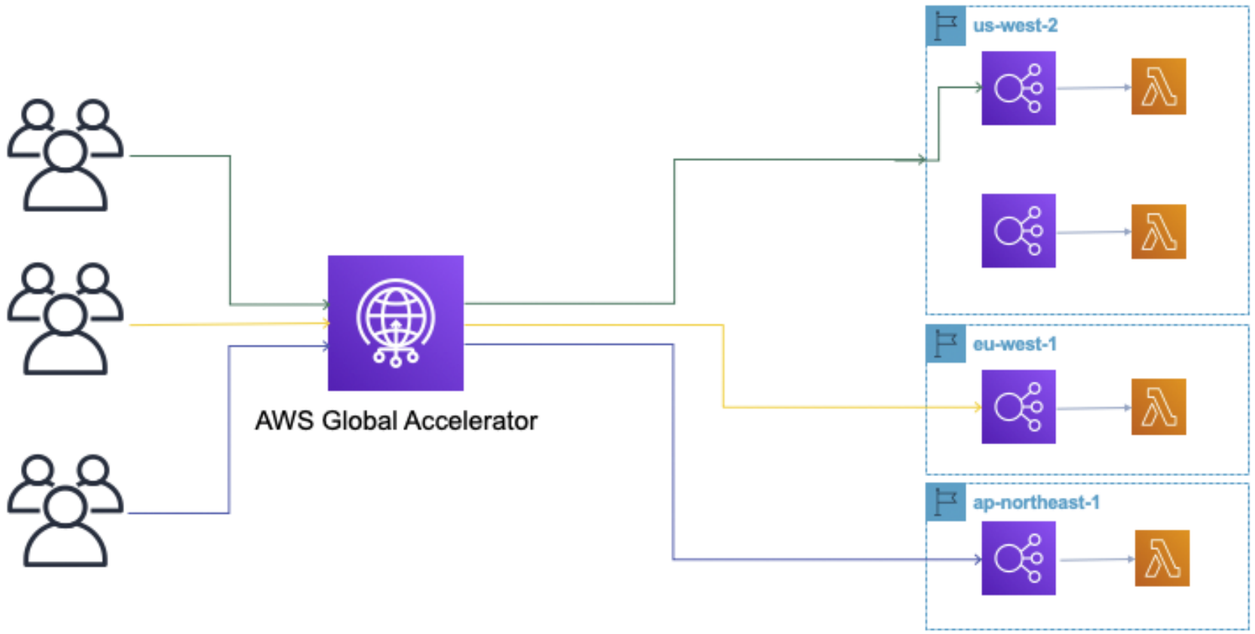
Steps to be followed:

1. Set up an EC2 instance for configuring the global accelerator
2. Create a global accelerator

Three AWS Options to Global Audience

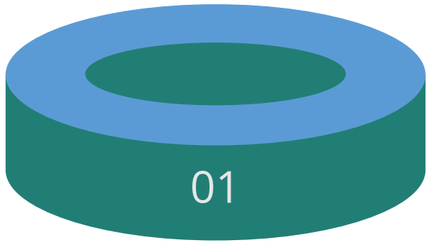
AWS Global Audience

The AWS Global Accelerator optimizes the path to your application to keep packet loss, jitter, and latency consistently low.

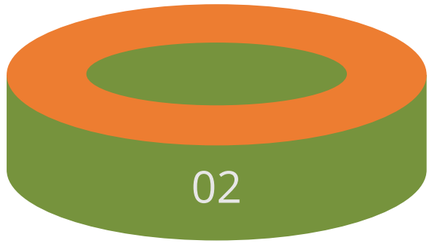


AWS Global Audience

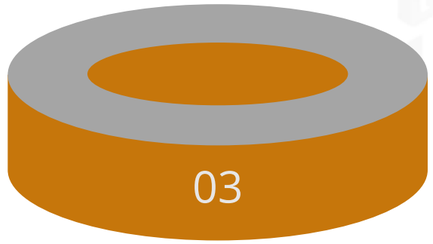
The three examples of AWS Global Audience are as follows:



CloudFront



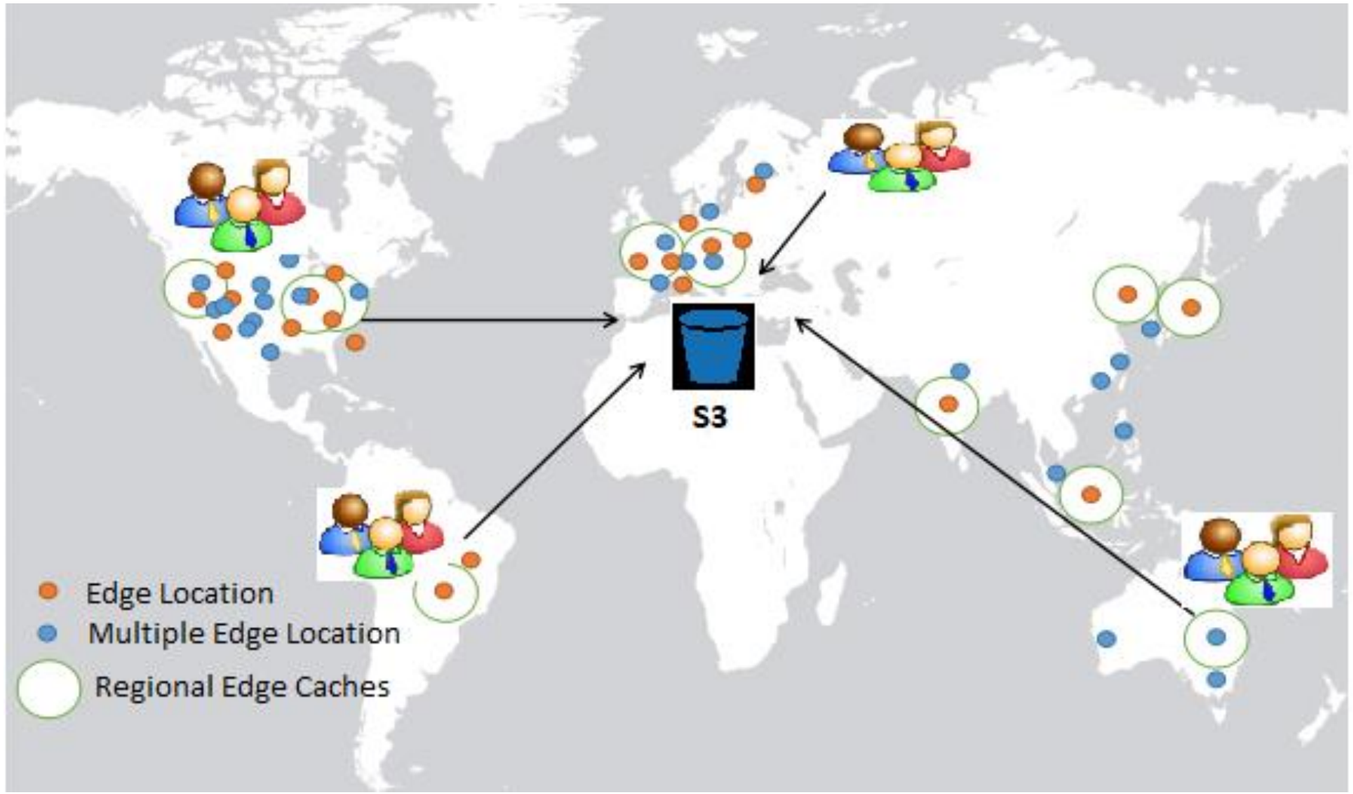
Global Accelerate



Route S3

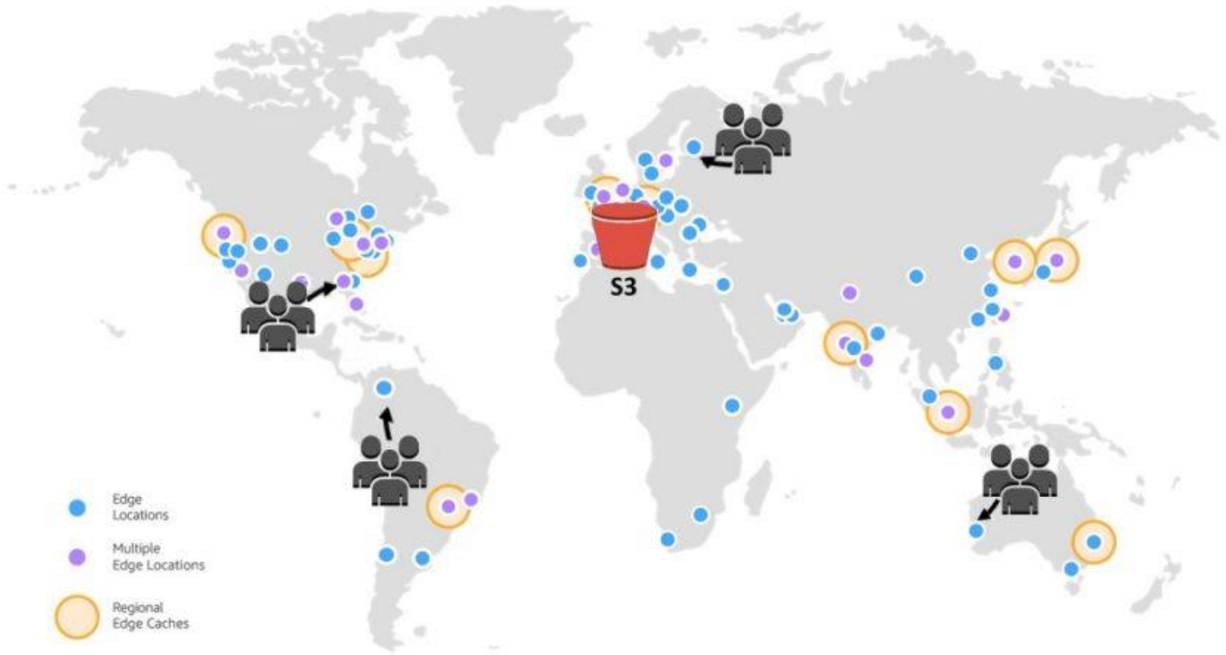
AWS Global Audience - CloudFront

Amazon CloudFront peers with thousands of tier carriers globally. It is well connected with all major access networks for optimal performance and has hundreds of terabits of deployed capacity.



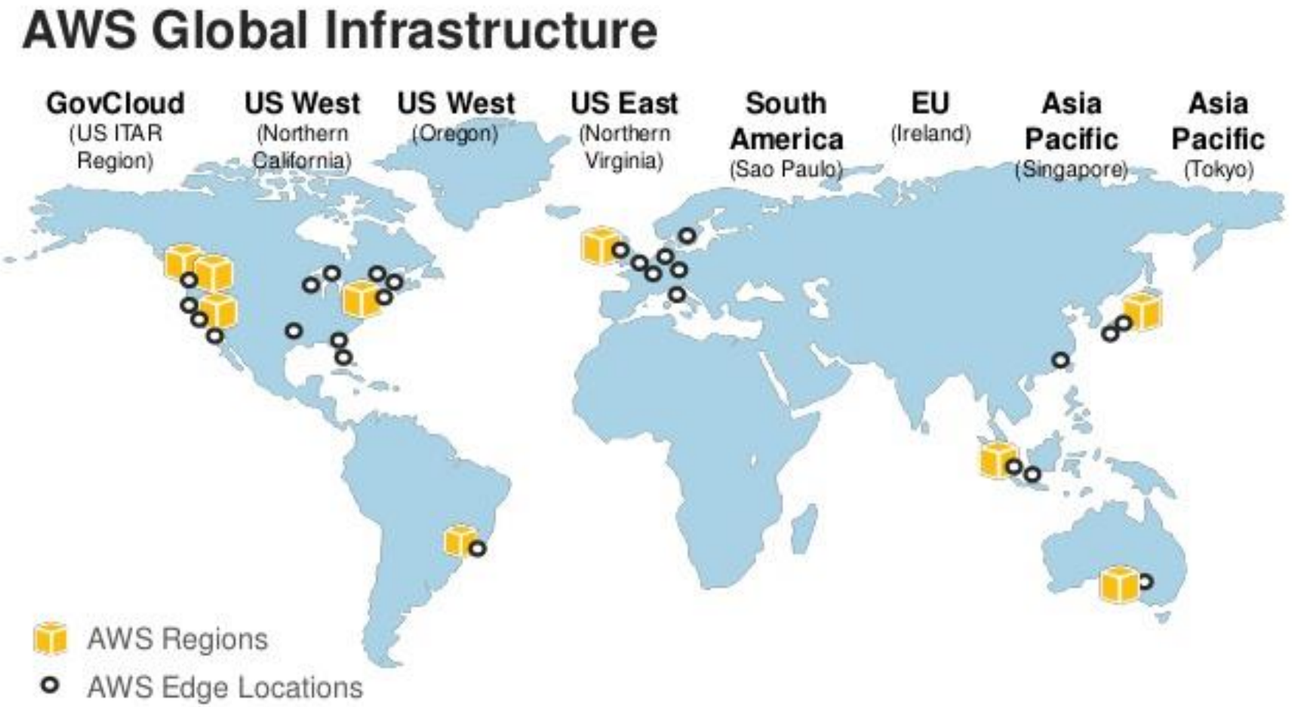
AWS Global Audience - Route S3

Route end users to your site reliably with globally-dispersed Domain Name System (DNS) servers and automatic scaling. Set up your DNS routing in minutes with domain name registration and straightforward visual traffic flow tools.



AWS Global Audience - Global Accelerator

In the Global Accelerator, you are provided two global static public IPs that act as a fixed entry point to your application, improving availability. On the back end, add or remove your AWS application endpoints, such as Application Load Balancers, Network Load Balancers, EC2 Instances, and Elastic IPs without making user-facing changes.



TECHNOLOGY

Amazon Route 53

Amazon Route 53

Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service.

Amazon Route 53

Features of Amazon Route 53

The following are the features of Amazon Route 53:

01 Resolver

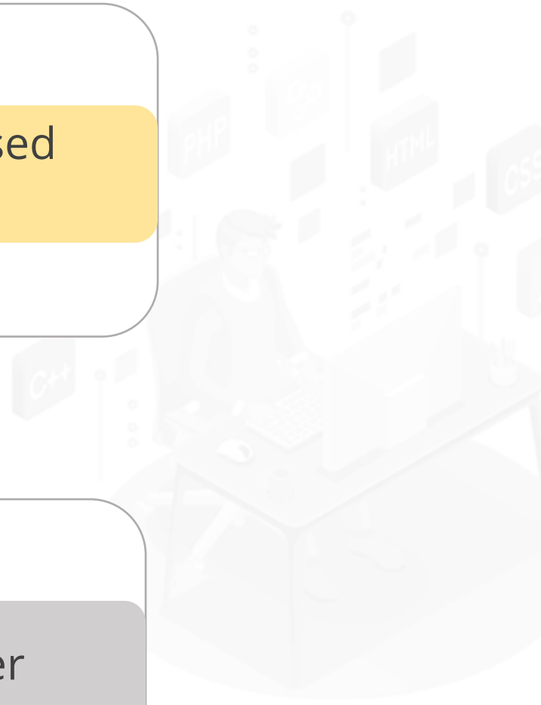
02 Traffic flow

03 Latency based routing

04 Geo DNS

05 Private DNS for VPC

06 DNS failover



Features of Amazon Route 53

The following are the features of Amazon Route 53:

07 Health Checks and monitoring

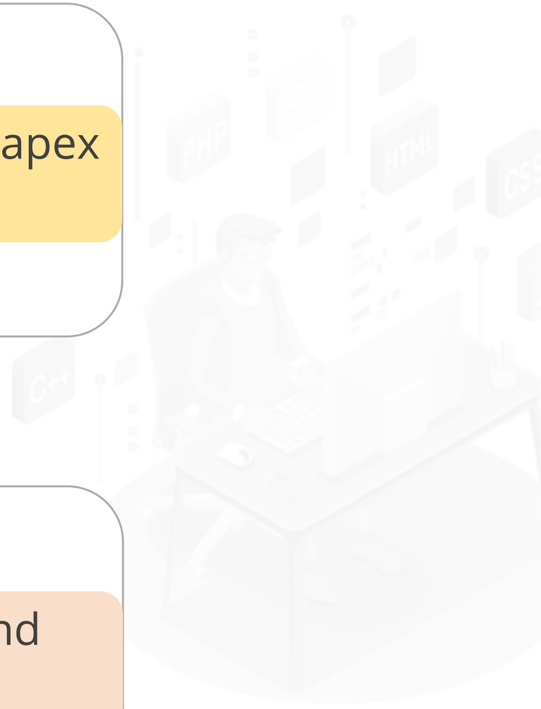
08 Domain Registration

09 CloudFront zone apex support

10 Amazon ELB integration

11 Management console

12 Weighted round robin



Benefits of Amazon Route 53

Some of the benefits of Amazon Route 53 are:

01	Highly available and reliable
02	Flexible
03	Well designed
04	Easy-to-use
05	Fast performance

Benefits of Amazon Route 53

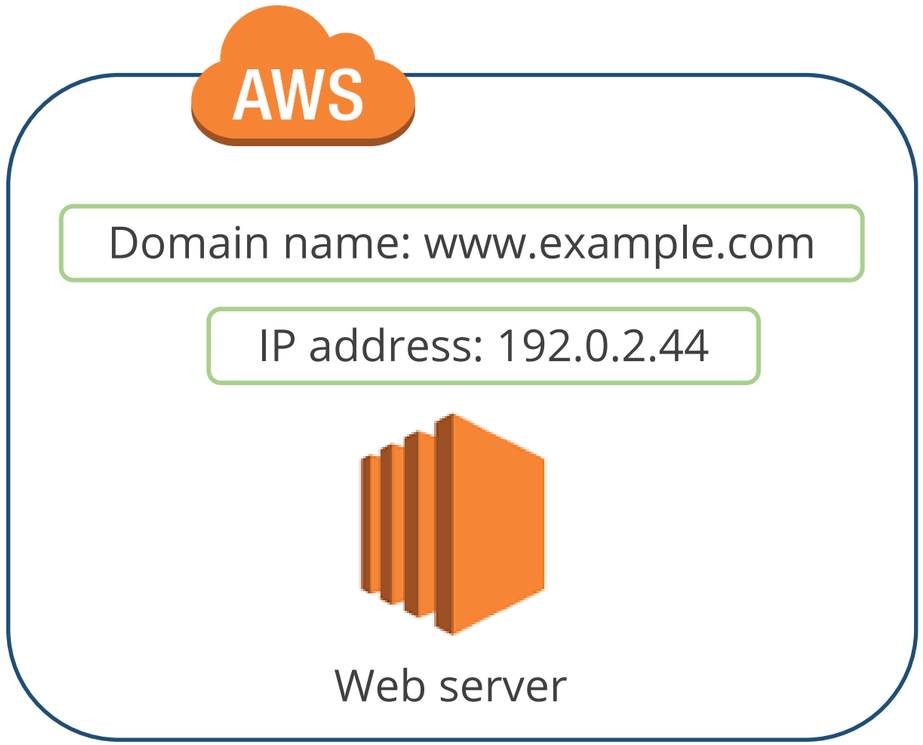
Some of the benefits of Amazon Route 53 are:

06	Cost-effective
07	Secure
08	Scalable
09	Simplifies the hybrid cloud

Domain Name System (DNS)

Domain Name System (DNS)

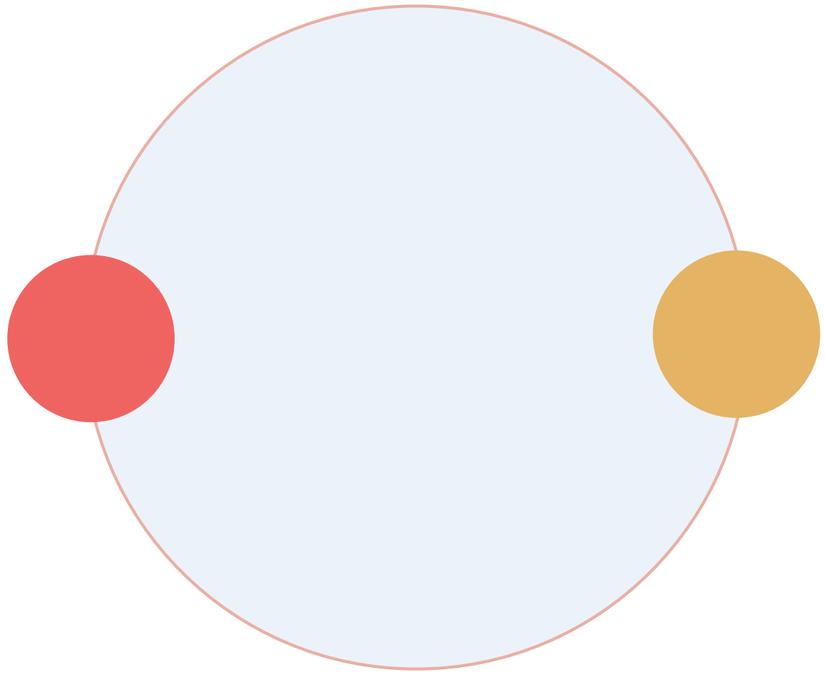
Domain Name System (DNS) translates human-readable domain names (www.example.com) to machine-readable IP addresses (192.0.2.44).



Domain Name System

Domain Name System Services

These are the two types of DNS services:

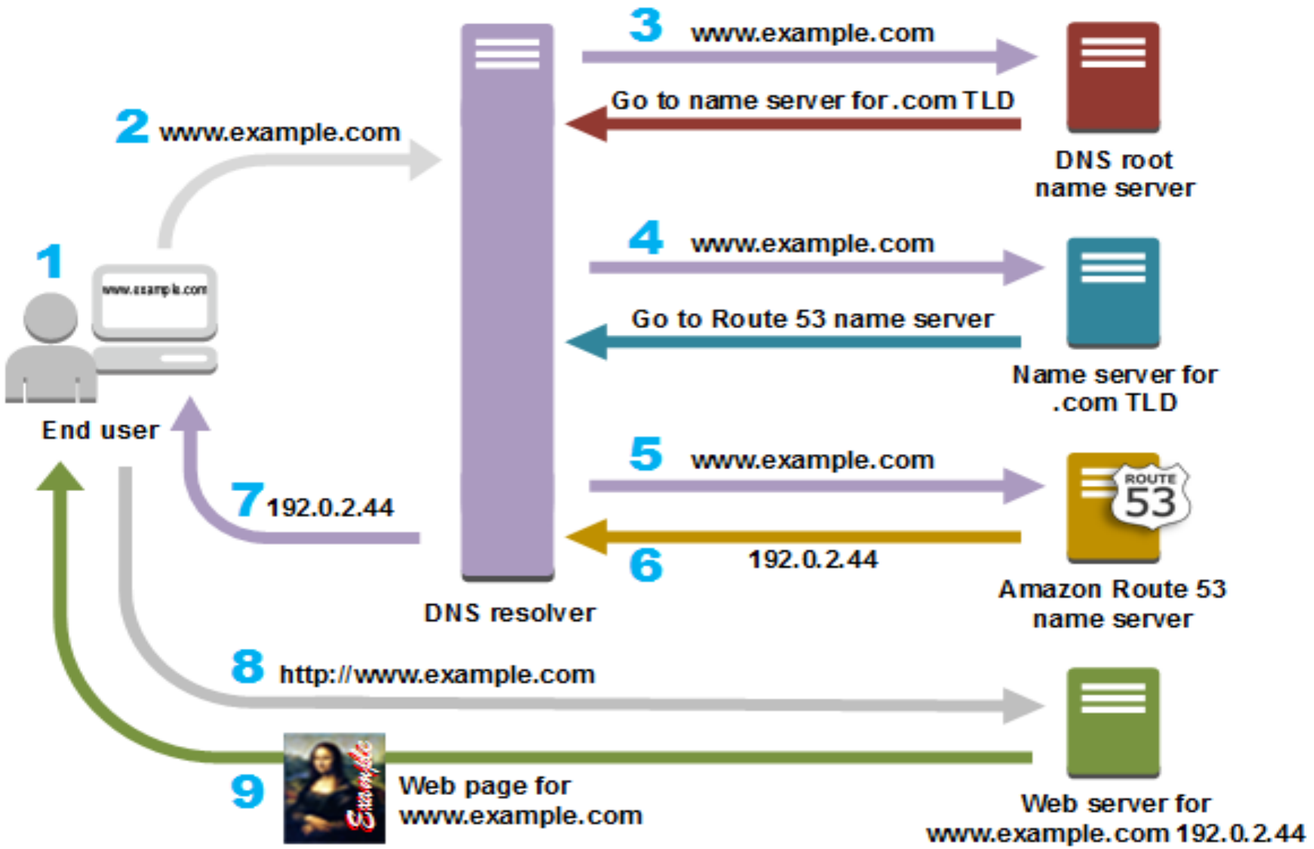


Authoritative DNS

Recursive DNS

Domain Name System Workflow

The following diagram gives an overview of how recursive and authoritative DNS services work together to route an end-user to the website or application:



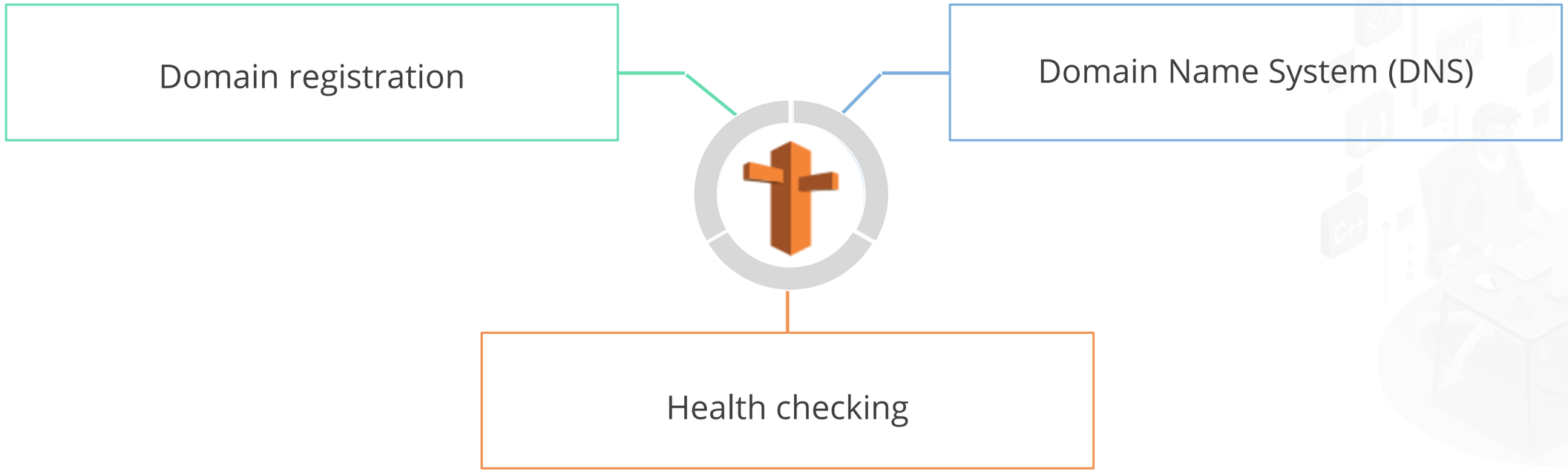
Source: https://aws.amazon.com/route53/what-is-dns/#:~:text=DNS%2C%20or%20the%20Domain%20Name,addresses%20(for%20example%2C%20192.0.

TECHNOLOGY

Amazon Route 53 Concepts and Terminologies

Amazon Route 53 Concepts

The following are the concepts of Amazon Route 53:



Amazon Route 53 Concepts

The following concepts are related to domain registration:

01	Domain name
02	Domain registrar
03	Domain registry
04	Domain reseller
05	Top-level domain (TLD)

Amazon Route 53 Concepts

The following concepts are related to Domain Name System (DNS):

01	Authoritative name server
02	DNS query
03	DNS resolver
04	IP address
05	Private DNS

Amazon Route 53 Concepts

The following concepts are related to Domain Name System (DNS):

06	Recursive name servers
07	Reusable delegation set
08	Routing policy
09	Subdomain
10	Time to live (TTL)

Amazon Route 53 Concepts

The following concepts are related to health checking:

01	DNS failover
02	Endpoint
03	Health check

Amazon Route 53 Terminologies

The following terminologies are used in Amazon Route 53:

01	02	03	04
Name servers	**Alias record**	**Hosted zone**	**DNS record**

It helps to translate domain names into the IP addresses that computers use to communicate with one another.

Amazon Route 53 Terminologies

The following terminologies are used in Amazon Route 53:

01	02	03	04
Name servers	Alias record	Hosted zone	DNS record

It is a type of record that users can create with Amazon Route 53 to route traffic to AWS resources such as Amazon CloudFront distributions and Amazon S3 buckets.

Amazon Route 53 Terminologies

The following terminologies are used in Amazon Route 53:

01	02	03	04
Name servers	Alias record	Hosted zone	DNS record

It is a container for records, which includes information about how the users want to route traffic for a domain and all of its subdomains.

Amazon Route 53 Terminologies

The following terminologies are used in Amazon Route 53:

01	02	03	04
Name servers	Alias record	Hosted zone	DNS record

It is an object in a hosted zone that the users use to define how they want to route traffic for the domain or a subdomain.

TECHNOLOGY

Amazon Route 53 Policies

Amazon Route 53 Policies

Amazon Route 53 supports the following routing policies:

01	02	03	04
Simple routing policy	**Failover routing policy**	**Geolocation routing policy**	**Geoproximity routing policy**

It is used to route internet traffic to a single resource that performs a given function for the domain, for example, a web server that serves content for the example.com website.

Amazon Route 53 Policies

Amazon Route 53 supports the following routing policies:

01	02	03	04
Simple routing policy	Failover routing policy	Geolocation routing policy	Geoproximity routing policy

It is used when the users want to configure the active-passive failover.

Amazon Route 53 Policies

Amazon Route 53 supports the following routing policies:

01	02	03	04
Simple routing policy	Failover routing policy	Geolocation routing policy	Geoproximity routing policy

It is used when the users want to route the internet traffic to the resources based on the location of the users.

Amazon Route 53 Policies

Amazon Route 53 supports the following routing policies:

01	02	03	04
Simple routing policy	**Failover routing policy**	**Geolocation routing policy**	**Geoproximity routing policy**

It is used when the users want to route traffic based on the location of the resources and, optionally, shift traffic from resources in one location to resources in another.

Amazon Route 53 Policies

Amazon Route 53 supports the following routing policies:

05	06	07
Latency routing policy	**Multivalue answer routing policy**	**Weighted routing policy**

It is used when the users want to route the traffic based on the location of the resources and, optionally, shift the traffic from the resources in one location to the resources in another.

Amazon Route 53 Policies

Amazon Route 53 supports the following routing policies:

05	06	07
Latency routing policy	Multivalue answer routing policy	Weighted routing policy

It helps the users to check the health of each resource, so Amazon Route 53 returns only values for healthy resources.

Amazon Route 53 Policies

Amazon Route 53 supports the following routing policies:

05	06	07
Latency routing policy	**Multivalue answer routing policy**	**Weighted routing policy**

It is used to route traffic to multiple resources in proportions that the users specify.

Route 53 Health Checks

Route 53 Health Checks

Amazon Route 53 health checks keep track of the status and performance of your web applications, web servers, and other services.

Every health check can monitor one or more of the following:

- The health of a specified resource, such as a web server
- The status of other health checks
- The status of an Amazon CloudWatch alarm
- Amazon Route 53 Application Recovery Controller helps the user to set up routing control health checks with DNS failover records

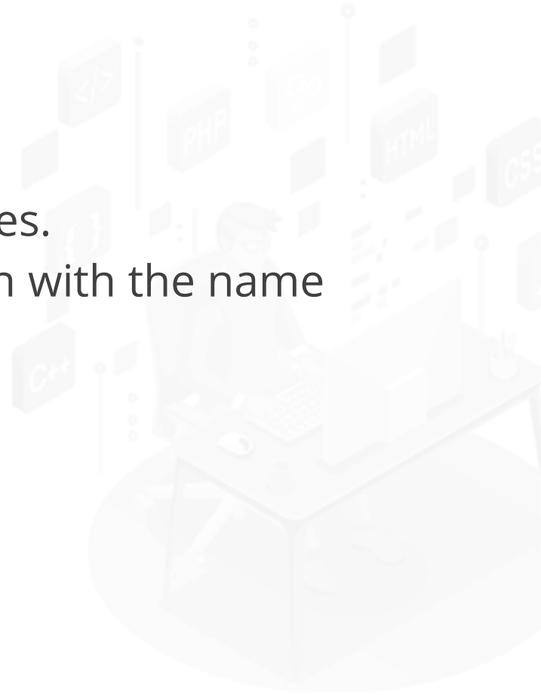
Amazon Route 53 Best Practices

Amazon Route 53 Best Practices

The following are the best practices for Amazon Route 53:

- Name server delegation
- TTL resource record sets
- Alias record
- Minimize latency

- It helps to translate domain names into IP addresses.
- It updates the registrar's name server configuration with the name servers to provide maximum availability.

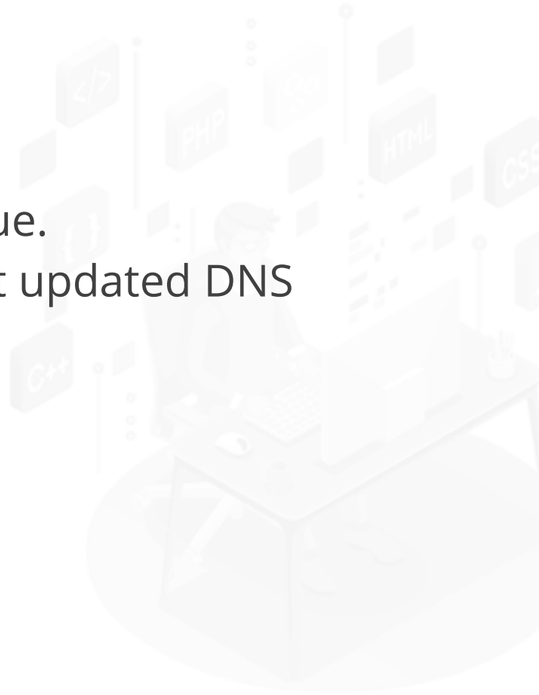


Amazon Route 53 Best Practices

The following are the best practices for Amazon Route 53:

- Name server delegation
- TTL resource record sets
- Alias record
- Minimize latency

- Resource records can benefit from a lower TTL value.
- For long TTLs, DNS resolvers take longer to request updated DNS records.

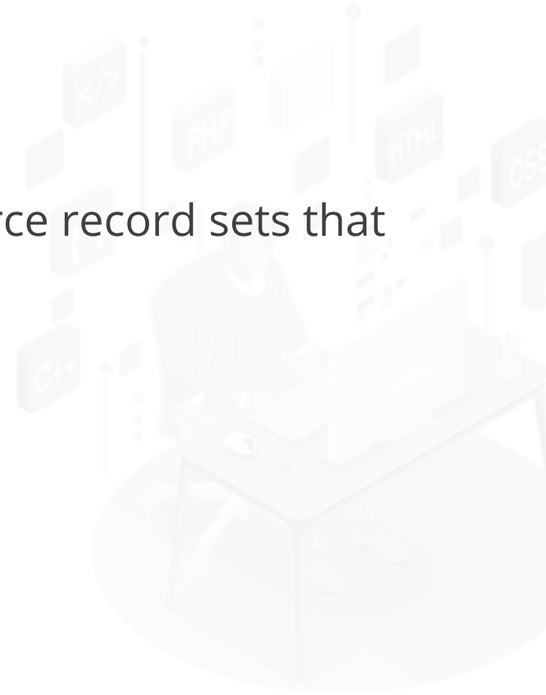


Amazon Route 53 Best Practices

The following are the best practices for Amazon Route 53:

- Name server delegation
- TTL resource record sets
- Alias record
- Minimize latency

- Alias record sets are used while configuring resource record sets that route DNS queries to AWS resources.
- These are available at free of cost.

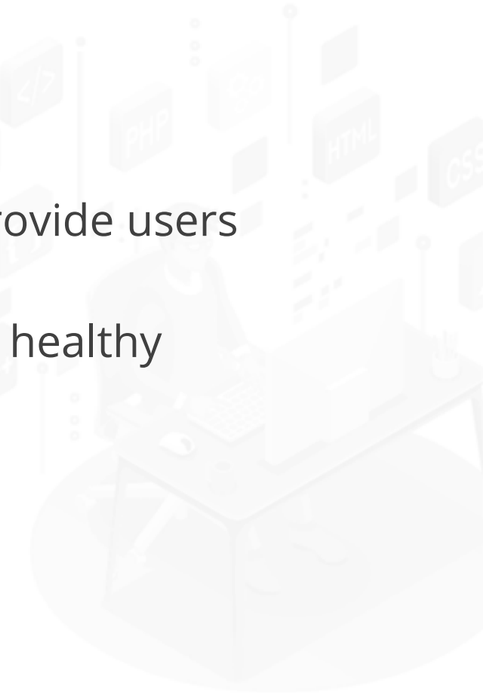


Amazon Route 53 Best Practices

The following are the best practices for Amazon Route 53:

- Name server delegation
- TTL resource record sets
- Alias record
- Minimize latency

- Latency or Geolocation routing policies are used to provide users with the best response times.
- A health check ensures that the users are rerouted to healthy instances during an outage.



Limitations of Amazon Route 53

Limitations of Amazon Route 53

The following are the limitations of Amazon Route 53:

1. Amazon Route 53 private endpoints are not available in VPN or Direct Connect.
2. It provides no forwarding or conditional forwarding options for domains used on an on-premise network.
3. It does not support private zone transfers.

Pricing

Pricing

To allow testing, a Route 53 hosted zone that is deleted within 12 hours of creation is not charged.

- The first 50 AWS endpoint health checks that are linked to an AWS account or paid to the same AWS account as the health check are free.
- Free DNS queries can be made to other AWS services' alias records.

Pricing

Each domain name is registered through or transferred into Route 53 is subject to an annual fee. Per AWS account, a maximum of 20 domain names may be registered.

Pricing

The price for the Hosted Zone depends on:

- Charges for a hosted zone are made at the time of creation and on the first of each succeeding month.
- A hosted zone that is deleted within 12 hours after creation is not charged to facilitate testing.

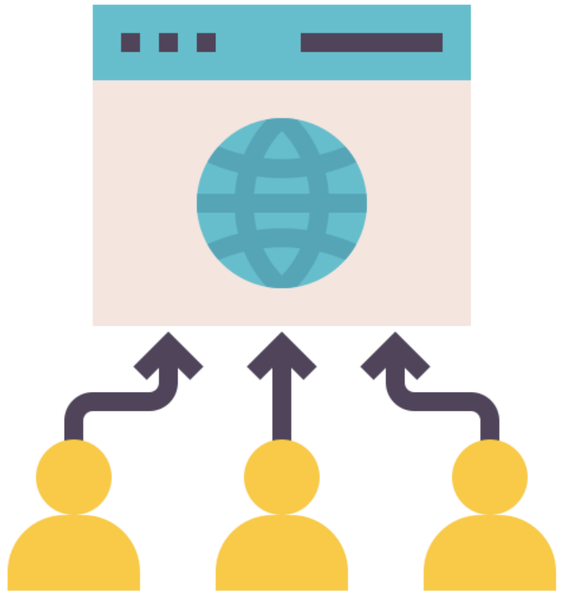
Pricing

Depending on the routing strategy selected when establishing a new record for the hosted zone, the user will be charged for certain query types:

- Alias queries
- Standard DNS
- Geolocation-based queries
- Latency-based queries

Pricing

Traffic Flow policies and records:



- Make sure there are no deny statements that restrict public read access to S3:GetObject operation by reviewing the bucket policy.
- Make sure there is no competing explicit refuse statement even if the bucket policy contains an explicit allow statement.

Key Takeaways

- AWS Identity and Access Management (IAM) is a web service that allows the user to control the authorization of AWS resources.
- Amazon VPC is a service that helps users launch AWS resources into a defined virtual network.
- Amazon Route 53 automatically creates a name server (NS) record that has the same as your hosted zone.
- VPC flow logs are used to capture information about the IP traffic going to and from the network interfaces in your VPC.

Customizing EC2 Instance with VPCs, Subnets, Gateway, and Route Table

Duration: 30 mins

Project agenda: To create VPC and launch a web instance

Description:

You are required to create a custom VPC and create a subnet and attach the subnet to VPC. Create an internet gateway, route table and then launch an EC2 instance.

Perform the following:

- Create a web instance
- Create an internet gateway and attach it to VPC
- Create a subnet and a route table

LESSON-END PROJECT

TECHNOLOGY

Thank You

simplilearn