Designing Applications and Architectures in AWS

(Aligned with AWS Solution Architect Associate Certification)

©Simplilearn. All rights reserved.

simplilearn

TECHNOLOGY

VPC, Networking, and Content Delivery

©Simplilearn. All rights reserved.

A Day in the Life of a Cloud Architect

John is a cloud architect in an organization and has been asked to address security concerns about moving the company's infrastructure to the AWS cloud.

The company has outlined specific requirements:

- They seek an entity that can attach to any AWS resource, defining its access permissions.
- Instead of distributing long-term credentials, like usernames, passwords, or access keys, the company requires a solution offering temporary rights to applications when interacting with AWS resources.

©Simplilearn. All rights reserved.

A Day in the Life of a Cloud Architect

- They aim to manage governance, compliance, operational audits, and risk assessments within the AWS account.
- The security and compliance of applications on AWS should align with the company's standards.

John’s responsibilities include setting up an AWS account and utilizing the AWS Command Line Interface (CLI) to engage with AWS services and resources. He must also master using AWS Identity and Access Management (IAM) to ensure secure access to AWS resources.

To achieve these, he will learn a few concepts in this lesson to help him find a solution for the given scenario.

©Simplilearn. All rights reserved.

Learning Objectives

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

- Configure IAM and its policies to ensure secure access management
- Create and configure a CloudFront distribution to distribute content globally
- Create and configure VPC endpoints to privately connect to AWS services without public internet exposure
- Implement a range of routing methods to manage network traffic efficiently

©Simplilearn. All rights reserved.

Security Group and NACL

©Simplilearn. All rights reserved.

Security Group

An AWS security group acts as a virtual firewall for EC2 instances, controlling both incoming and outgoing traffic.

©Simplilearn. All rights reserved.

Security Group

These are the following rules for security groups:

- By default, security groups include outbound rules that permit all outbound traffic.
- A user can filter traffic using security group rules based on protocols and ports.
- A user cannot construct security group rules that restrict access.
- A user can change a security group's rules, and all connected instances will be updated.

©Simplilearn. All rights reserved.

Network ACL (NACL)

A Network ACL (NACL) is an optional security feature. It acts as a firewall, controlling traffic that enters and leaves a subnet.

©Simplilearn. All rights reserved.

Network ACL (NACL)

The rules for Network ACL include:

- **Rule number:** Rules rank from the lowest to the highest number. If traffic matches a lower-numbered rule, the system ignores any conflicting higher-numbered rule.
- **Type:** This category defines the traffic type, like SSH. Users can select a specific range or all traffic types.
- **Protocol:** Users can select any protocol with a standard number. For example, when using ICMP, they can identify its number and specify any or all its types and codes.

©Simplilearn. All rights reserved.

Network ACL (NACL)

The rules for Network ACL include:

- **Port reach:** This specifies the port or range of ports that the network traffic uses. For example, HTTP traffic uses port **80** by default.
- **Source:** For inbound rules, this factor indicates the traffic's origin using the CIDR range.
- **Destination:** For outbound rules, this defines the traffic's destination, also specified using the CIDR range.
- **Allow or Deny:** This rule determines if the system should allow or deny the traffic.

©Simplilearn. All rights reserved.

Network ACL vs. Security Group

The differences between Network ACL and Security Group are as follows:

Security Group	Network ACL
• Operates at the instance level • Is stateful • Supports only allow rules	• Acts as a firewall at the subnet level • Is stateless • Supports both allow and deny rules

©Simplilearn. All rights reserved.

IP Addresses

The types of IP addresses in Amazon VPC are as follows:

Private IP Address

Public IP Address

Elastic IP Address

- A private IP address is unreachable over the internet.
- Users can use it to communicate between instances within the same VPC.
- When users stop an instance, the public IP associated with it is released.

©Simplilearn. All rights reserved.

IP Addresses

The types of IP addresses in Amazon VPC are as follows:

Private IP Address

Public IP Address

Elastic IP Address

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

©Simplilearn. All rights reserved.

IP Addresses

The types of IP addresses in Amazon VPC are as follows:

Private IP Address

Public IP Address

Elastic IP Address

- An Elastic IP address is a public IP address that users can allocate to their accounts.
- Users can associate or disassociate it with instances as needed.
- It stays with the user's account until they decide to release it.

©Simplilearn. All rights reserved.

Multiple IP Addresses

Assigning multiple IP addresses to an instance in the VPC can be beneficial to:

- Host multiple websites on one server using different SSL certificates. Each certificate can be associated with a unique IP address.
- Operate network appliances like firewalls or load balancers that need multiple IP addresses for each network interface.
- Redirect internal traffic to a standby instance if the primary one fails. This is done by reassigning the secondary IP address to the standby instance.

©Simplilearn. All rights reserved.

Creating Key Pair for EC2

Duration:10 min

Problem Statement:

You have been assigned a task to create a key pair for an EC2 instance to be used as a security credential for user authorization.

ASSISTED PRACTICE

©Simplilearn. All rights reserved.

Assisted Practice: Guidelines

Steps to be followed are:

1. Create a key pair for an EC2 instance

©Simplilearn. All rights reserved.

Creating a Default VPC

Duration:10 min

Problem Statement:

You have been assigned a task to set up a secure and isolated network environment that forms the basis for hosting AWS resources, gaining practical skills in essential networking configuration within the AWS ecosystem.

ASSISTED PRACTICE

©Simplilearn. All rights reserved.

Assisted Practice: Guidelines

Steps to be followed are:

1. Create a default VPC

©Simplilearn. All rights reserved.

Exploring Network ACL Firewall

Duration:10 min

Problem Statement:

You have been assigned a task to set up the prerequisites for and explore the network ACL firewall.

ASSISTED PRACTICE

©Simplilearn. All rights reserved.

Assisted Practice: Guidelines

Steps to be followed are:

1. Create a network ACL

©Simplilearn. All rights reserved.

VPC Flow Logs

©Simplilearn. All rights reserved.

VPC Flow Logs

VPC Flow Logs is a feature that captures information about the IP traffic going to and from network interfaces in a VPC.

When a user creates a flow log for a subnet or VPC, it monitors all network interfaces within that subnet or VPC.

©Simplilearn. All rights reserved.

VPC Flow Logs

VPC flow logs can be published to two destinations: CloudWatch Logs and Amazon S3.

- **Amazon S3:** VPC Flow Logs collects and consolidates flow log records into log files.
- **CloudWatch Logs:** When flow log data is published to CloudWatch Logs, it populates a specific log group.

©Simplilearn. All rights reserved.

VPC Flow Logs in Amazon S3

- VPC Flow Logs gathers flow log records, consolidates them into log files, and then publishes these files every five minutes to an Amazon S3 bucket.
- Each of these log files captures the IP traffic data from the previous five minutes.

©Simplilearn. All rights reserved.

VPC Flow Logs in CloudWatch

- When a user publishes to CloudWatch Logs, the flow log data goes into a specific log group.
- Within this group, each network interface gets its unique log stream.
- Flow log records are then stored within these log streams.

©Simplilearn. All rights reserved.

VPC Flow Logs

Before a request in a VPC reaches an AWS-hosted EC2 instance endpoint, it must follow a sequence of steps.

The VPC flow is typically explained using two components:

1. The external request
2. The private instance

©Simplilearn. All rights reserved.

VPC Flow Logs

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 illustrates the workflow of components within a private instance. The following components are involved in processing an external request:

- Internet Gateway
- Router or Route Table
- Network ACL (associated with the subnet)
- Security Group (linked to the instance)
- Public Instance

©Simplilearn. All rights reserved.

IAM Roles for Publishing Flow Logs to CloudWatch Logs

To publish flow logs to a specific log group in CloudWatch Logs, users must ensure:

- The IAM role associated with the flow log has the required permissions.
- This IAM role resides within the AWS account.

©Simplilearn. All rights reserved.

IAM Roles for Publishing Flow Logs to CloudWatch Logs

For the user's IAM role, the attached policy must grant the following permissions:

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

©Simplilearn. All rights reserved.

IAM Roles for Publishing Flow Logs to CloudWatch Logs

Ensure a trust relationship is set for the VPC Flow Logs service to assume the relevant IAM role.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-
logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

©Simplilearn. All rights reserved.

IAM Roles for Publishing Flow Logs to CloudWatch Logs

Users are advised to use the **aws:SourceAccount** and **aws:SourceArn** condition keys to guard against the confused deputy problem.

©Simplilearn. All rights reserved.

Enhancing Trust Policy for Flow Logs

To improve security, users can append this condition block to their existing trust policy:

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

©Simplilearn. All rights reserved.

Using Flow Log ARN in IAM Roles

The source account refers to the owner of the flow log, while the source ARN identifies the flow log's ARN.

If a user is unsure of the flow log ID, they can substitute that segment of the ARN with a wildcard. Later, they can update the policy after creating the flow log.

©Simplilearn. All rights reserved.

Setting Up an IAM Role for Flow Logs

Users can either update an existing role or follow a recommended procedure to create a new role specifically for flow logs.

©Simplilearn. All rights reserved.

Creating an IAM Role for Flow Logs

To create an IAM role for VPC flow logging, follow these steps:

- Go to the IAM console at: https://console.aws.amazon.com/iam
- In the navigation pane, select **Roles**
- Click **Create role**
- On the **Select role type** page, select **AWS service**

©Simplilearn. All rights reserved.

Creating an IAM Role for Flow Logs

To create an IAM role for VPC flow logging, follow these steps:

- In the **Choose a service that will use this role** list, select **VPC Flow Logs**
- Click **Next: Permissions**
- On the **Permissions** page, select the permission **AmazonVPCFullAccess**
- Click **Next: Tags**

©Simplilearn. All rights reserved.

Creating an IAM Role for Flow Logs

To create an IAM role for VPC flow logging, follow these steps:

- (Optional) To add tags to your role, select **Add tags** and enter the tag key and value
- Click **Next: Review**
- On the **Review** page, enter a name for the role and a description
- Click **Create role**

©Simplilearn. All rights reserved.

Permissions for IAM Users to Pass a Role

To allow users to pass a role in IAM for VPC flow log capture, they need specific permissions.

Below is the IAM policy for such permission:

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

©Simplilearn. All rights reserved.

Creating a Flow Log in the VPC

Duration:10 min

Problem Statement:

You have been assigned a task to create a VPC flow log within the AWS framework and configure the logging settings, setting filter criteria, and specifying an Amazon S3 bucket.

ASSISTED PRACTICE

©Simplilearn. All rights reserved.

Assisted Practice: Guidelines

Steps to be followed are:

1. Create a flow log in the default VPC

©Simplilearn. All rights reserved.

NAT and Internet Gateways

©Simplilearn. All rights reserved.

Internet Gateways

An Internet gateway is a VPC component that scales horizontally, is redundant, and offers high availability. This gateway enables communication between the VPC and the Internet.

It serves two main purposes:

- It acts as a target in the VPC route tables for traffic that is routable on the internet.
- It handles network address translation (NAT) for instances with public IPv4 addresses.

©Simplilearn. All rights reserved.

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*

©Simplilearn. All rights reserved.

Egress-only Internet Gateways

An egress-only Internet gateway is an internet gateway that users cannot associate with a security group.

- Users can employ security groups for their instances within a private subnet to manage traffic in and out of those instances.
- To control the traffic entering and leaving the subnet, users can apply a network ACL.

©Simplilearn. All rights reserved.

Network Address Translation (NAT)

A NAT device allows instances in a private subnet to connect to the Internet or other AWS services. However, it prevents the Internet from initiating connections in these instances.

There are two main types of NAT devices:

NAT gateway

NAT instance

©Simplilearn. All rights reserved.

NAT Gateway

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

Custom route table

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

Main rout table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*nat-gateway-id*

©Simplilearn. All rights reserved.

NAT Gateway: Characteristics

The NAT Gateway possesses the following key characteristics:

- Bandwidth and scalability
- Protocol support
- Network ACL control
- Concurrent connections

©Simplilearn. All rights reserved.

NAT Gateway: Limitations

While the NAT Gateway is a powerful tool, it does come with certain limitations:

- Single Elastic IP
- No security group association
- ClassicLink inaccessibility
- Routing constraints

©Simplilearn. All rights reserved.

VPC Endpoints: Overview

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.

©Simplilearn. All rights reserved.

Interface VPC Endpoint

An interface VPC endpoint provides users with the capability to establish connections to services powered by AWS PrivateLink, which encompasses a variety of AWS services.

For each specified subnet within a user's VPC, the creation of an interface VPC endpoint results in the generation of an endpoint network interface in that subnet.

©Simplilearn. All rights reserved.

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 themselves.
- Users are billed according to their hourly usage and data processing charges.

©Simplilearn. All rights reserved.

Interface Endpoint: Features

Interface VPC endpoints offer the following key features:

01

TCP traffic support: Interface VPC endpoints facilitate communication over the TCP protocol.

02

Selective response: Endpoints respond exclusively to traffic initiated by resources within the user's VPC.

03

Publicly resolvable DNS names: The DNS names assigned to interface VPC endpoints can be resolved publicly.

04

Scalable bandwidth: Each interface endpoint boasts substantial bandwidth capabilities.

©Simplilearn. All rights reserved.

Gateway Endpoints

Gateway endpoints offer dependable connectivity to Amazon S3 and DynamoDB, eliminating the need for an Internet gateway or NAT device within the user's VPC.

- However, it's important to note that gateway endpoints do not support AWS PrivateLink integration.
- The usage of gateway endpoints does not incur any additional charges.

©Simplilearn. All rights reserved.

VPC Peering Connection

A VPC peering connection establishes a direct and secure link between two VPCs. Users can create multiple VPC peering connections for each VPC they own.

©Simplilearn. All rights reserved.

Multiple VPC Peering Connections

A VPC peering connection establishes a direct and secure link between two VPCs. Users have the ability to create multiple VPC peering connections for each VPC they own.

However, it's important to note that transitive peering relationships are not supported.

©Simplilearn. All rights reserved.

AWS Transit Gateway

The AWS Transit Gateway serves as a central hub, seamlessly connecting users with both Amazon Virtual Private Clouds (VPCs) and on-premises networks.

Simplifying network configurations and streamlining connectivity eradicate the need for complex peering relationships.

©Simplilearn. All rights reserved.

AWS Transit Gateway

Below is a visual representation of an AWS Transit Gateway in an idle state:

Source: https://aws.amazon.com/blogs/aws/new-use-an-aws-transit-gateway-to-simplify-your-network-architecture/

©Simplilearn. All rights reserved.

AWS Transit Gateway

Below is a visual representation of an operational AWS Transit Gateway:

Source: https://aws.amazon.com/blogs/aws/new-use-an-aws-transit-gateway-to-simplify-your-network-architecture/

©Simplilearn. All rights reserved.

AWS Transit Gateway: Use Cases

The following are the use cases for the AWS Transit Gateway:

- Deliver applications around the world
- Rapidly move to a global scale
- Smoothly respond to spikes in demand
- Host multicast applications in the cloud

©Simplilearn. All rights reserved.

Configuring Subnets, Route Table, and NAT

Duration:10 min

Problem Statement:

You have been assigned a task to create a Virtual Private Cloud (VPC) on AWS, set up subnets, configure route tables, and create a Network Address Translation (NAT) gateway.

ASSISTED PRACTICE

©Simplilearn. All rights reserved.

Assisted Practice: Guidelines

Steps to be followed are:

1. Create a VPC
2. Create Internet gateways
3. Create Subnets
4. Create a route table and NAT

©Simplilearn. All rights reserved.

Creating a VPC Endpoint

Duration:10 min

Problem Statement:

You have been assigned a task to create a VPC Endpoint to establish a secure connection between a Virtual Private Cloud (VPC) and an Amazon S3 bucket.

ASSISTED PRACTICE

©Simplilearn. All rights reserved.

Assisted Practice: Guidelines

Steps to be followed are:

1. Create a VPC Endpoint

©Simplilearn. All rights reserved.

Configuring VPC Peering Connections

Duration:10 min

Problem Statement:

You have been assigned a task to connect two VPCs with different regions using peering connection.

ASSISTED PRACTICE

©Simplilearn. All rights reserved.

Assisted Practice: Guidelines

Steps to be followed are:

1. Create two VPCs with different regions
2. Configure Peer connection

©Simplilearn. All rights reserved.

Private Link and Bastion Host

©Simplilearn. All rights reserved.

AWS PrivateLink

- AWS PrivateLink establishes secure and private connections between VPCs, AWS services, and on-premises networks.
- AWS PrivateLink simplifies the process of connecting services across diverse accounts and VPCs, offering a streamlined approach to enhancing the network architecture.

©Simplilearn. All rights reserved.

AWS PrivateLink

The benefits of private link are as follows:

Enhanced data security

Streamlined network management

Smooth cloud migration

©Simplilearn. All rights reserved.

Bastion Host

A bastion host is a specialized server designed to facilitate secure access between a private and an external network, such as the Internet.

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

©Simplilearn. All rights reserved.

Linux Bastion Host Architecture

The diagram below illustrates the architecture of a Linux bastion host on AWS:

©Simplilearn. All rights reserved.

External Clients

The configuration for this scenario includes access to an on-premises network only.

The configuration mentioned above is advisable when users require clients to have access to resources within an on-premises network.

©Simplilearn. All rights reserved.

Steps for Accessing an On-Premises Network

The steps are as follows:

Step 1

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

Step 2

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

Step 3

Review the rules and limitations for client VPN endpoints.

©Simplilearn. All rights reserved.

Steps to Implement the Configuration

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

01	Generate server and client certificates and keys
02	Create a Client VPN endpoint
03	Associate a target network
04	Add an authorization rule for the VPC
05	Provide access to the internet
06	Verify security group requirements
07	Download the Client VPN endpoint configuration file
08	Connect to the Client VPN endpoint

©Simplilearn. All rights reserved.

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:

01 Regional endpoints

02 FIPS endpoints

03 Service endpoints

©Simplilearn. All rights reserved.

Systems Manager

AWS Systems Manager is a powerful tool that grants users comprehensive visibility and control over their entire AWS infrastructure.

- 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.

©Simplilearn. All rights reserved.

Systems Manager

AWS Systems Manager is a robust and secure end-to-end management solution tailored for hybrid cloud environments.

©Simplilearn. All rights reserved.

System Manager Process Flow

Here is an example of the process flow within AWS Systems Manager:

©Simplilearn. All rights reserved.

System Manager Works in Details

The key aspects are as follows:

1. Accessing System Manager
2. Choosing a System Manager
3. Verification and processing
4. Reporting
5. Leveraging System Manager's operations management capabilities

©Simplilearn. All rights reserved.

System Manager Capabilities

Systems Manager capabilities are divided into the following categories:

©Simplilearn. All rights reserved.

Application Management

The Application Management capabilities are as follows:

Application management: This feature allows you to logically group AWS resources that you want to operate as a unit within your application.

App Ccnfiguration: It assists in creating, managing, and deploying application configurations and feature flags.

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

©Simplilearn. All rights reserved.

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 user's application configuration and infrastructure.

Automation:
You can utilize automation to streamline and automate common maintenance and deployment tasks.

©Simplilearn. All rights reserved.

Change Management

The Change Management capabilities are as follows:

Change calendar:
This feature assists users in configuring date and time ranges during specified actions.

Maintenance windows:
These windows enable users to establish recurring schedules for managed instances to perform administrative tasks.

©Simplilearn. All rights reserved.

Node Management

The Node Management capabilities are as follows:

Use compliance:
This capability allows users to scan their fleet of managed nodes for patch compliance and configuration inconsistencies.

Fleet manager:
Fleet Manager provides a unified user interface (UI) experience that assists users in remotely managing the nodes.

©Simplilearn. All rights reserved.

simplilearn

Node Management

The Node Management capabilities are as follows:

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

Session Manager:
This feature provides secure and auditable edge device and instance management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys.

©Simplilearn. All rights reserved.

Operations Management

The Operations Management are as follows:

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

Explorer: This feature displays an aggregated view of operations data (Ops Data) for AWS accounts and across AWS Regions.

OpsCenter: It provides a central location where operations 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 utilize to monitor resources in a single view.

©Simplilearn. All rights reserved.

Quick Setup

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

©Simplilearn. All rights reserved.

Understanding SSM Documents

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

SSM document types include:

- **Command Documents:** Used by the State Manager for Run Commands
- **Automation Runbooks:** Used by Systems Manager Automation

©Simplilearn. All rights reserved.

VPN Connections

©Simplilearn. All rights reserved.

VPN Connections

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

The following VPN connectivity options facilitate the connection of Amazon Virtual Private Cloud (VPC) to remote networks:

01	AWS Site-to-Site VPN
02	AWS Client VPN
03	AWS VPN CloudHub
04	Third-Party Software VPN Appliance

©Simplilearn. All rights reserved.

VPN Connections: Benefits

The benefits of the VPN connections are as follows:

©Simplilearn. All rights reserved.

Working of VPN Connections

The following diagram shows the working of VPN connections:

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

©Simplilearn. All rights reserved.

Use Cases of VPN Connections

VPN connections offer versatile solutions that address several practical scenarios, such as:

Effortless application access

Rapid remote access scaling

Effortless deployment and removal for temporary workers

©Simplilearn. All rights reserved.

Direct Connect

AWS Direct Connect is a cloud service solution that simplifies the establishment of a dedicated network connection from the user's premises to AWS.

More about AWS Direct Connect:

01	It facilitates the creation of private connectivity between AWS and data centers, offices, or colocation environments.
02	It establishes a dedicated connection between the user's network and one of the AWS Direct Connect locations.

©Simplilearn. All rights reserved.

Direct Connect: Benefits

Direct Connect

- Reduces bandwidth costs
- Easy-to-use
- Compatible with all the AWS services
- Private connectivity to the Amazon VPC
- Elastic
- Consistent network performance

©Simplilearn. All rights reserved.

Working of Direct Connect

The following diagram shows the working of Direct Connect:

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

©Simplilearn. All rights reserved.

Working of Direct Connect

The diagram below illustrates the interaction of AWS Direct Connect with the network:

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

©Simplilearn. All rights reserved.

Components of Direct Connect

AWS Direct Connect comprises two essential components:

©Simplilearn. All rights reserved.

Use Cases of Direct Connect

AWS Direct Connect offers versatile solutions that address several practical scenarios, enhancing data transfer, performance, and operational efficiency.

Efficient handling of large data sets

Real-time data feeds and exchanges

Hybrid environments integration

©Simplilearn. All rights reserved.

Direct Connect: Costs

The following are the costs associated with Direct Connect:

01 Dedicated connections

02 Hosted connections

03 Data transfer

©Simplilearn. All rights reserved.

Direct Connect: Costs

The following are the costs associated with Direct Connect:

04	TCO calculator
05	AWS pricing calculator
06	Economics resource center

©Simplilearn. All rights reserved.

CloudFront

©Simplilearn. All rights reserved.

CloudFront

Amazon CloudFront is a global content delivery network (CDN) service designed to securely and efficiently distribute content to end users, ensuring low latency and high transfer speeds.

Amazon CloudFront

©Simplilearn. All rights reserved.

Amazon CloudFront Points of Presence (POPs)

Amazon CloudFront operates through a network of strategically located Points of Presence (POPs) to optimize content delivery, enhance user experiences, and ensure high availability.

Source: https://aws.amazon.com/blogs/networking-and-content-delivery/400-amazon-cloudfront-points-of-presence/

©Simplilearn. All rights reserved.

Amazon CloudFront Points of Presence (POPs)

Points of Presence is a single data center.

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

©Simplilearn. All rights reserved.

Content Delivery Using CloudFront

The process of establishing a CloudFront distribution to efficiently deliver content involves the following steps:

- Specify origin servers
- Upload data files to the origin servers
- Create a CloudFront distribution

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

©Simplilearn. All rights reserved.

Content Delivery Using CloudFront

Here is a visual representation of setting up a CloudFront distribution to deliver content:

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

©Simplilearn. All rights reserved.

CloudFront With S3 origin

CloudFront provides seamless integration with Amazon S3, bolstering the security of S3 bucket access by utilizing CloudFront Origin Access Identity (OAI).

©Simplilearn. All rights reserved.

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

©Simplilearn. All rights reserved.

CloudFront: Benefits

- CloudFront alleviates the load on the origin servers by caching content at its edge locations.
- It enables targeted content delivery based on user locations through its GEO targeting services.
- It utilizes HTTP and HTTPS protocols to ensure secure and rapid content delivery to end users.

©Simplilearn. All rights reserved.

Configuring CloudFront Distribution with S3 Origin

Duration:10 min

Problem Statement:

You have been assigned a task to host static web content in an Amazon S3 bucket, protected and accelerated by Amazon CloudFront.

ASSISTED PRACTICE

©Simplilearn. All rights reserved.

Assisted Practice: Guidelines

Steps to be followed are:

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

©Simplilearn. All rights reserved.

Creating Cache Configuration and Invalidation

Duration:10 min

Problem Statement:

You have been assigned a task to configure CloudFront distributions and perform cache invalidation to ensure timely updates of content served through Amazon CloudFront.

ASSISTED PRACTICE

©Simplilearn. All rights reserved.

Assisted Practice: Guidelines

Steps to be followed are:

1. Create Distributions
2. Create Invalidation

©Simplilearn. All rights reserved.

Configuring Origin Access Identity (OAI)

Duration:10 min

Problem Statement:

You have been assigned a task to block S3 access for the public and restrict access only through the CloudFront using OAI.

ASSISTED PRACTICE

©Simplilearn. All rights reserved.

Assisted Practice: Guidelines

Steps to be followed are:

1. CloudFront access with OAI

©Simplilearn. All rights reserved.

Lambda@Edge

©Simplilearn. All rights reserved.

What Is Lambda@Edge?

Lambda@Edge, an Amazon CloudFront feature, empowers users to access code closer to their application's end users, resulting in improved speed and reduced latency.

©Simplilearn. All rights reserved.

Lambda@Edge: Benefits

1. Makes the apps more responsive
2. Eliminates the need for server administration
3. Personalizes the content distribution

©Simplilearn. All rights reserved.

Working of Lambda@Edge

It operates seamlessly within the request cycle, making informed decisions that directly impact the delivery of CloudFront content.

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

©Simplilearn. All rights reserved.

Lambda@Edge: Use Cases

Following are a few important use cases of Lambda@Edge:

Simplify and reduce origin infrastructure:

Lambda@Edge can be employed as an extension or replacement for the origin.

Website security and privacy:

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

©Simplilearn. All rights reserved.

Lambda@Edge: Use Cases

Following are a few important use cases of Lambda@Edge:

Dynamic web application:

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

Search Engine Optimization (SEO):

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

©Simplilearn. All rights reserved.

Lambda@Edge: Use Cases

Following are a few important use cases of Lambda@Edge:

Intelligently route across origins and data centers :

The load on the origins can be balanced while improving user performance.

Bot mitigation at the edge:

Lambda@Edge can help users by blocking unwanted bots at the edge and letting authorized traffic go through.

©Simplilearn. All rights reserved.

Lambda@Edge: Use Cases

Following are a few important use cases of Lambda@Edge:

Improved user experience :

Website and web application content can be personalized without sacrificing performance.

Real-time image transformation:

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

©Simplilearn. All rights reserved.

Global Accelerator

©Simplilearn. All rights reserved.

AWS Global Accelerator

Amazon Global Accelerator is a powerful solution designed to enhance application performance and availability for local and global users.

By utilizing a network of AWS Edge Locations, Global Accelerator ensures that the application delivers a seamless and optimized experience to users globally.

©Simplilearn. All rights reserved.

AWS Global Accelerator

Amazon Global Accelerator offers versatile solutions that provide substantial benefits to applications based on their type and requirements.

The types of Amazon Global Accelerator are:

- Standard accelerator
- Custom routing accelerator

©Simplilearn. All rights reserved.

AWS Global Accelerator

AWS Global Accelerator provides static Anycast IPv4 addresses for enhanced global application availability and performance.

The supported endpoints include 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 a Public IP)

©Simplilearn. All rights reserved.

How Global Accelerator Works

Amazon Global Accelerator operates by providing clients with static IP addresses that serve as a consistent and fixed entry point to the application.

- For standard accelerators, the traffic is directed to the fastest AWS endpoint based on various factors, such as the user's geographical location, the state of the endpoint, and the weights assigned to each endpoint.
- In the case of custom routing accelerators, clients are directed to specific Amazon EC2 instances and ports within a VPC subnet.

©Simplilearn. All rights reserved.

AWS Global Accelerator

Amazon Global Accelerator streamlines the path that TCP or UDP packets take when entering Amazon's network, effectively reducing the number of hops required.

This optimization of the route for each client results in lower latencies and improved application performance.

©Simplilearn. All rights reserved.

AWS Global Accelerator

The key benefits of utilizing the AWS Global Accelerator are as follows:

Global anycast network: Leverages the extensive, high-performance AWS global network.

Static IP addresses: Provide consistent entry points.

Accelerated traffic routing: Routes traffic dynamically based on latency, health checks, and user-defined policies.

©Simplilearn. All rights reserved.

AWS Global Accelerator

The key benefits of utilizing the AWS Global Accelerator are as follows:

Health checks and endpoint monitoring: Monitor endpoint health continuously.

Global failover and disaster recovery: Redirect traffic to healthy endpoints in another region during failures.

Flexible port mapping: Supports TCP and UDP protocols and maps multiple ports to a single endpoint.

©Simplilearn. All rights reserved.

AWS Global Accelerator: Use Cases

AWS Global Accelerator is valuable for a range of use cases:

Content delivery
accelerates media and video delivery via the nearest edge location.

Multi-region applications
elevate performance with high availability and low latency.

IoT applications
optimize real-time communication and rapid responses.

Gaming
improves multiplayer experiences through reduced lag.

Web applications
ensure fast and consistent web experiences by intelligently routing traffic.

©Simplilearn. All rights reserved.

AWS Global Accelerator

To begin using AWS Global Accelerator, follow these simple steps:

©Simplilearn. All rights reserved.

Creating a Global Accelerator

Problem Statement:

You have been assigned a task to create a Global Accelerator on AWS, that enhances the availability and performance of your applications by intelligently routing traffic across multiple regions and endpoints.

ASSISTED PRACTICE

©Simplilearn. All rights reserved.

Assisted Practice: Guidelines

Steps to be followed are:

1. Create an EC2 web instance
2. Create a Global Accelerator

©Simplilearn. All rights reserved.

Amazon Route 53

©Simplilearn. All rights reserved.

Amazon Route 53

Amazon Route 53 is a scalable and highly available DNS web service provided by Amazon Web Services (AWS).

Its primary function is to translate user-friendly domain names into corresponding IP addresses, enabling users to access websites and applications effortlessly.

©Simplilearn. All rights reserved.

Amazon Route 53: Features

01 Resolver

02 Traffic flow

03 Latency based routing

04 Geo DNS

05 Private DNS for VPC

06 DNS failover

©Simplilearn. All rights reserved.

simplilearn

Amazon Route 53: Features

07

Health checks and monitoring

08

Domain registration

09

CloudFront zone apex support

10

Amazon ELB integration

11

Management console

12

Weighted round robin

©Simplilearn. All rights reserved.

Amazon Route 53: Features

Some of the benefits of Amazon Route 53 are as follows:

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

©Simplilearn. All rights reserved.

Amazon Route 53: Features

Some of the benefits of Amazon Route 53 are as follows:

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

©Simplilearn. All rights reserved.

Route 53 Routing Policies

©Simplilearn. All rights reserved.

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**).

©Simplilearn. All rights reserved.

Domain Name System Services

These are the two types of DNS services:

Authoritative DNS

Recursive DNS

©Simplilearn. All rights reserved.

Domain Name System Workflow

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

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

©Simplilearn. All rights reserved.

Amazon Route 53 Concepts

These concepts are fundamental to understanding Amazon Route 53:

- Domain registration
- Domain Name System (DNS)
- Health checking

©Simplilearn. All rights reserved.

Amazon Route 53 Concepts

The following are the fundamental concepts associated with domain registration:

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

©Simplilearn. All rights reserved.

Amazon Route 53 Concepts

The following are the fundamental concepts associated with Domain Name System (DNS):

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

©Simplilearn. All rights reserved.

simplilearn

Amazon Route 53 Concepts

The following are the fundamental concepts associated with Domain Name System (DNS):

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

©Simplilearn. All rights reserved.

Amazon Route 53 Concepts

The following concepts are related to health checking:

01	DNS failover
02	Endpoint
03	Health check

©Simplilearn. All rights reserved.

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.

©Simplilearn. All rights reserved.

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.

©Simplilearn. All rights reserved.

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 its subdomains.

©Simplilearn. All rights reserved.

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.

©Simplilearn. All rights reserved.

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.

©Simplilearn. All rights reserved.

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 users want to configure active-passive failover.

©Simplilearn. All rights reserved.

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 users want to route internet traffic to resources based on their location.

©Simplilearn. All rights reserved.

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.

©Simplilearn. All rights reserved.

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.

©Simplilearn. All rights reserved.

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

©Simplilearn. All rights reserved.

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.

©Simplilearn. All rights reserved.

Route 53 Health Checks

Amazon Route 53 health checks keep track of the status and performance of the 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

©Simplilearn. All rights reserved.

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.

©Simplilearn. All rights reserved.

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.

©Simplilearn. All rights reserved.

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.

©Simplilearn. All rights reserved.

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.

©Simplilearn. All rights reserved.

Limitations of Amazon Route 53

While Amazon Route 53 offers powerful features, it's essential to be aware of its limitations for effective usage.

1. Amazon Route 53 private endpoints are not available via 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.

©Simplilearn. All rights reserved.

Pricing

Hosted zones deleted within 12 hours of creation are not charged, allowing for testing and experimentation.

- The first 50 AWS endpoint health 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.

©Simplilearn. All rights reserved.

Pricing

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

©Simplilearn. All rights reserved.

Pricing

The price for the Hosted Zone depends on the following:

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

©Simplilearn. All rights reserved.

Pricing

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

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

©Simplilearn. All rights reserved.

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 name as the hosted zone.
- VPC flow logs capture information about the IP traffic going to and from the network interfaces in the VPC.

©Simplilearn. All rights reserved.

Key Takeaways

- Amazon Global Accelerator is a powerful solution designed to enhance application performance and availability for local and global users.
- VPC flow logs can be published to two destinations: CloudWatch Logs and Amazon S3.
- CloudFront provides seamless integration with Amazon S3, bolstering the security of S3 bucket access by utilizing CloudFront Origin Access Identity (OAI).

©Simplilearn. All rights reserved.

Customizing EC2 Instance for Web Instance

Duration: 30 mins

Project agenda: To create a VPC and launch a web instance

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

Perform the following:

1. Create a custom VPC and enable DNS hostname
2. Create an internet gateway and attach it to VPC
3. Create a subnet and a route table
4. Configure a route table
5. Launch the EC2 instance

LESSON-END PROJECT

©Simplilearn. All rights reserved.

TECHNOLOGY

Thank You

©Simplilearn. All rights reserved.

simplilearn