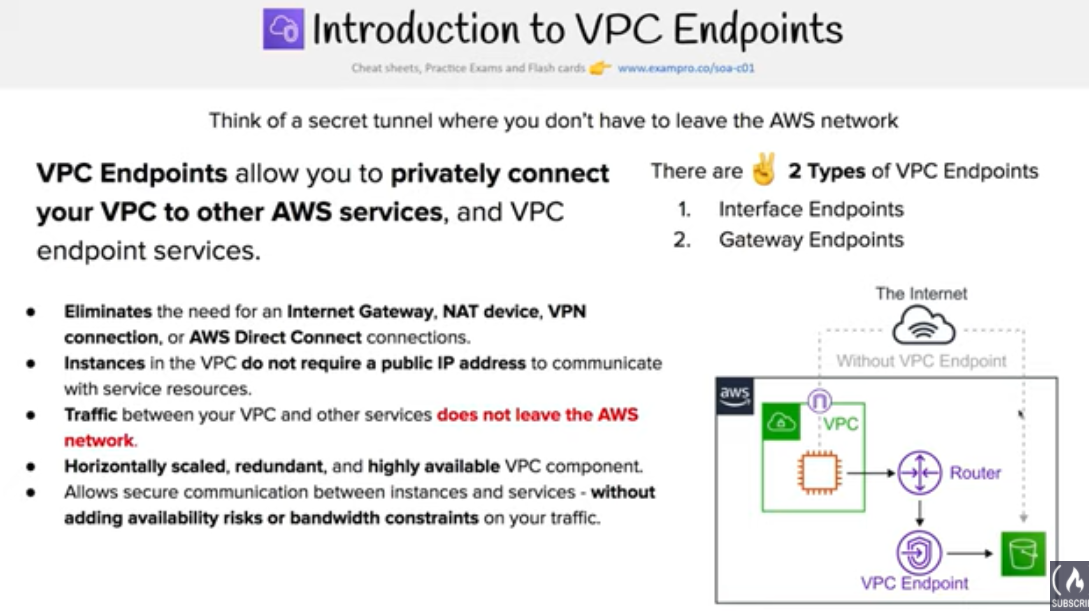
VPC Endpoints Overview

# VPC Endpoints Overview

Timeline

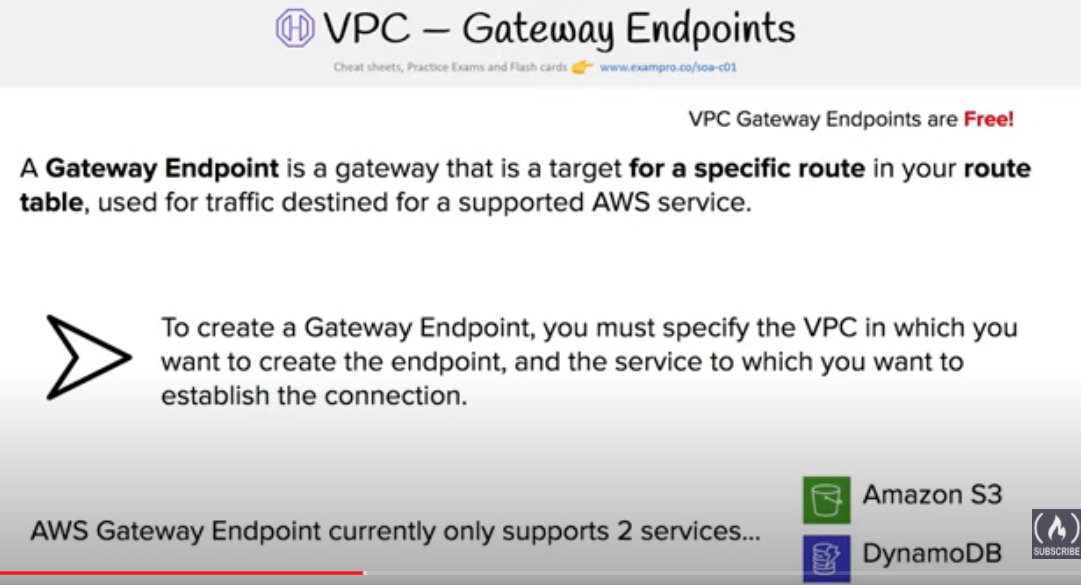
Description automatically generated with medium confidence



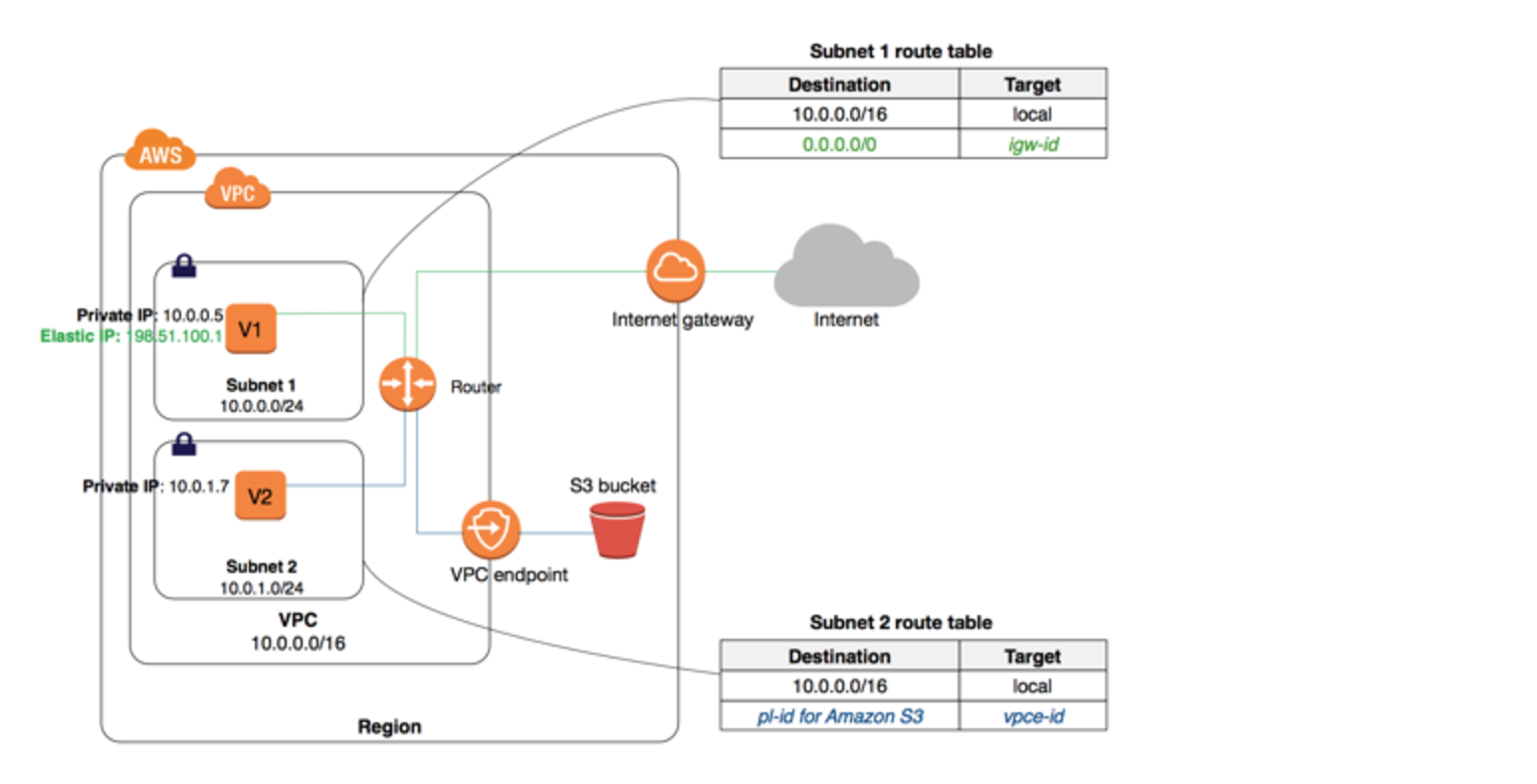
* **VPC endpoint enables creation of a private connection between VPC to supported AWS services and VPC endpoint services powered by PrivateLink using its private IP address**
* **VPC Endpoint does not require a public IP address, access over the Internet, NAT device, a VPN connection or AWS Direct Connect**
* **Traffic between VPC and AWS service does not leave the Amazon network**
* Endpoints are virtual devices, that are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in the VPC and AWS services without imposing availability risks or bandwidth constraints on your network traffic.
* **Endpoints currently do not support cross-region requests, ensure that the endpoint is created in the same region as your bucket**
* **AWS currently supports two types of Endpoints**
  + **VPC Interface Endpoints**
  + **VPC Gateway Endpoints**
* VPC Endpoint policy is an IAM resource policy attached to an endpoint for controlling access from the endpoint to the specified service.. Endpoint policy, by default, allows full access to the service.
* **Endpoint policy does not override or replace IAM user policies or service-specific policies (such as S3 bucket policies).**

## 

## VPC Gateway Endpoints

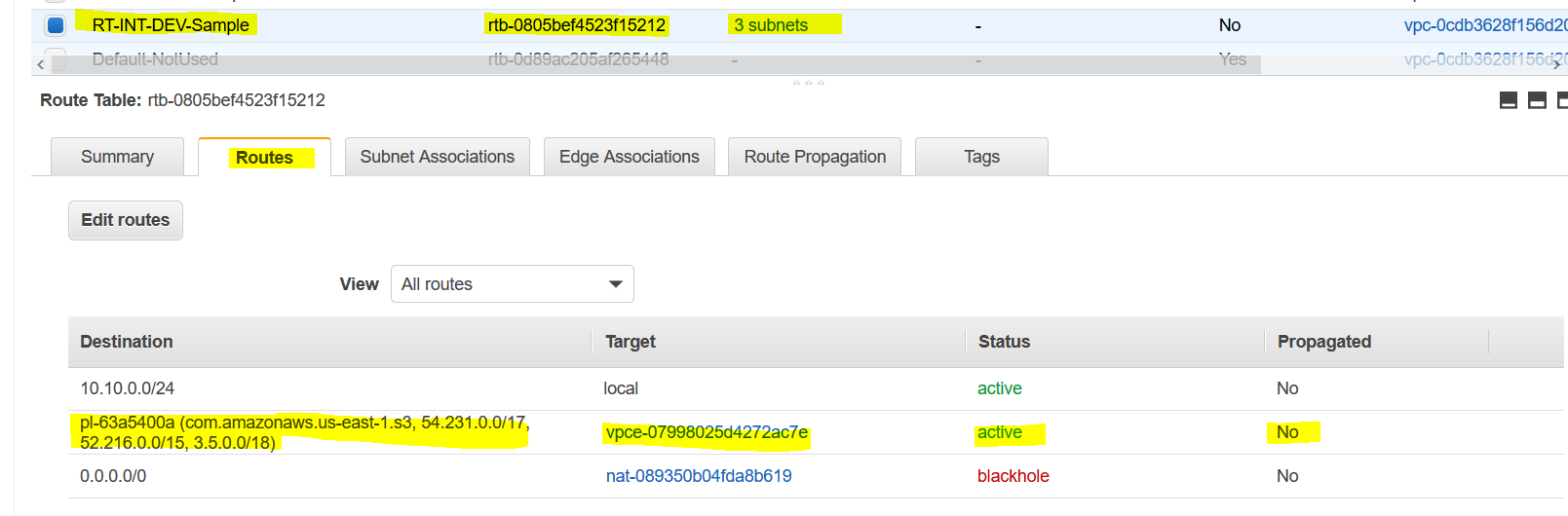


* A VPC Gateway Endpoint is a gateway that is a target for a specified route in the route table, used for traffic destined to a supported AWS service.
* **VPC Gateway Endpoint currently supports S3 and DynamoDB services**

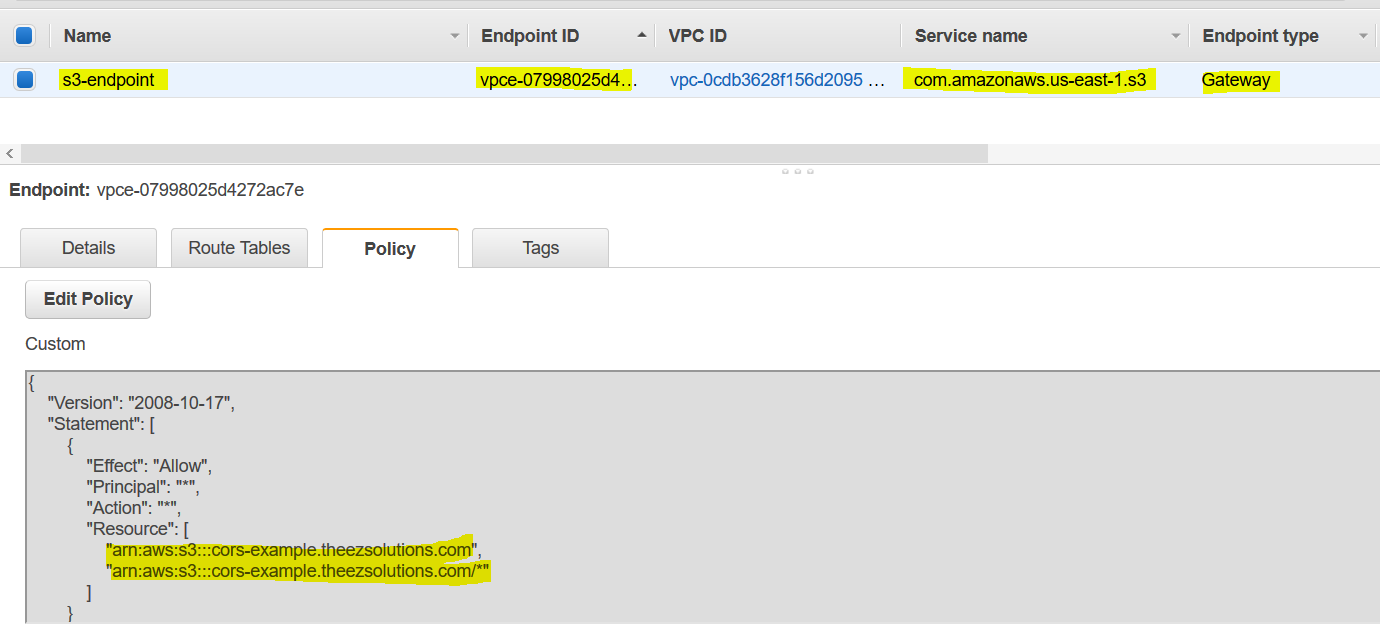


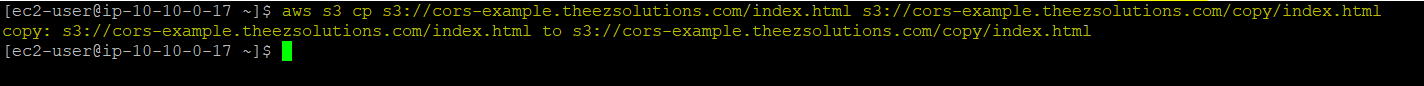
### Configuration

* Endpoint requires the VPC and the service to be accessed via the endpoint
* Endpoint needs to be associated with the Route table and the route table cannot be modified to remove the route entry. It can only be deleted by removing the Endpoint association with the Route table
* A route is automatically added to the Route table with a destination that specifies the prefix list of service and the target with the endpoint id. for e.g. A rule with destination **pl-68a54001 (com.amazonaws.us-west-2.s3)** and a target with this endpoints’ ID (e.g. vpce-12345678) will be added to the route tables

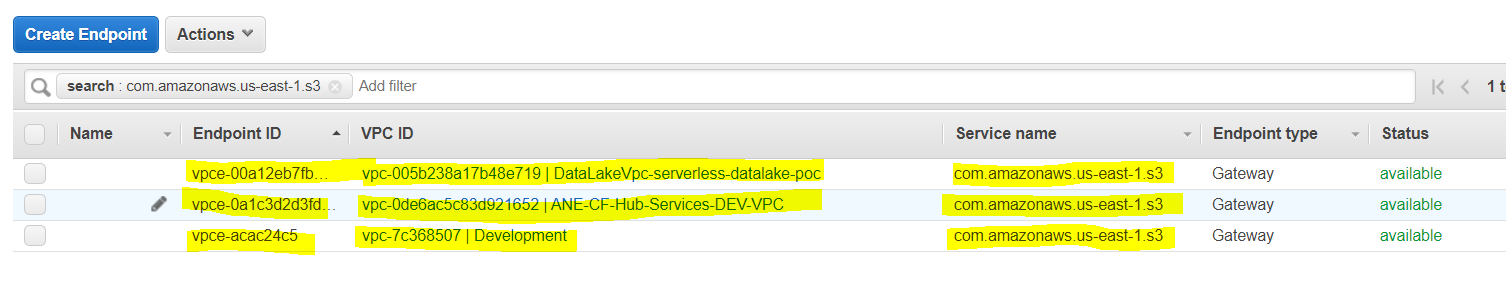


* Access to the resources in other services can be controlled by endpoint policies.





* Security groups needs to be modified to allow Outbound traffic from the VPC to the service thats specified in the endpoint. Use the service prefix list ID for e.g. com.amazonaws.us-east-1.s3  as the destination in the outbound rule
* **Multiple endpoints can be created in a single VPC, for e.g., to multiple services.**
* Multiple endpoints can be created for a single service, and different route tables used to enforce different access policies from different subnets to the same service.



* **Multiple endpoints to the same service CANNOT be specified in a single route table**

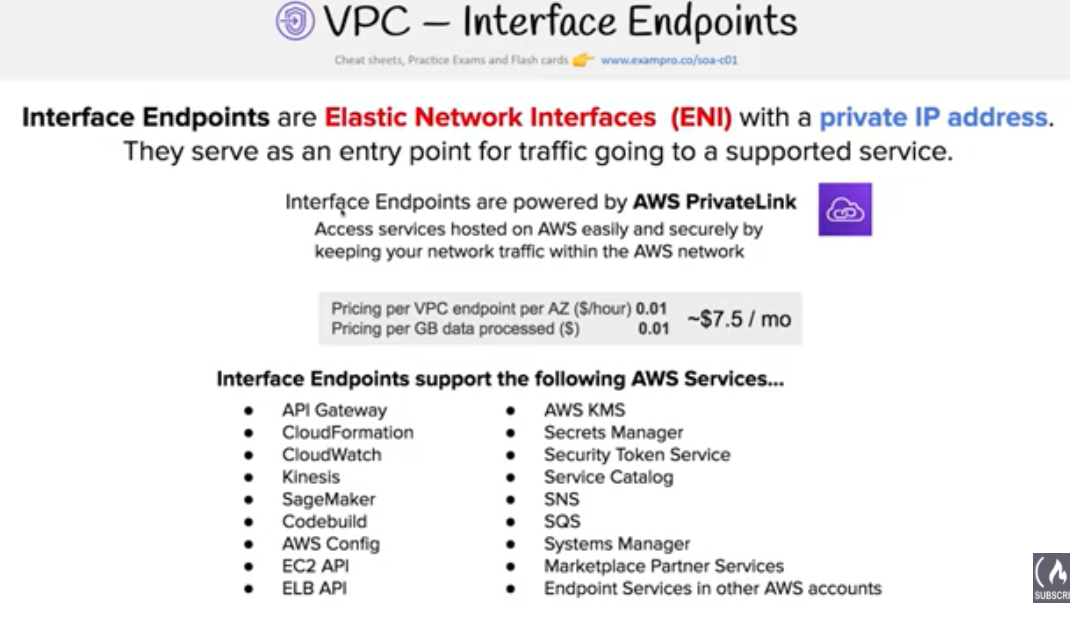
### Limitations

* **Endpoint cannot be created between a VPC and an AWS service in a different region.**
* **Endpoints support IPv4 traffic only.**
* **Endpoint cannot be transferred from one VPC to another, or from one service to another**
* Endpoint connections cannot be extended out of a VPC i.e. resources across the VPN connection, VPC peering connection, AWS Direct Connect connection cannot use the endpoint

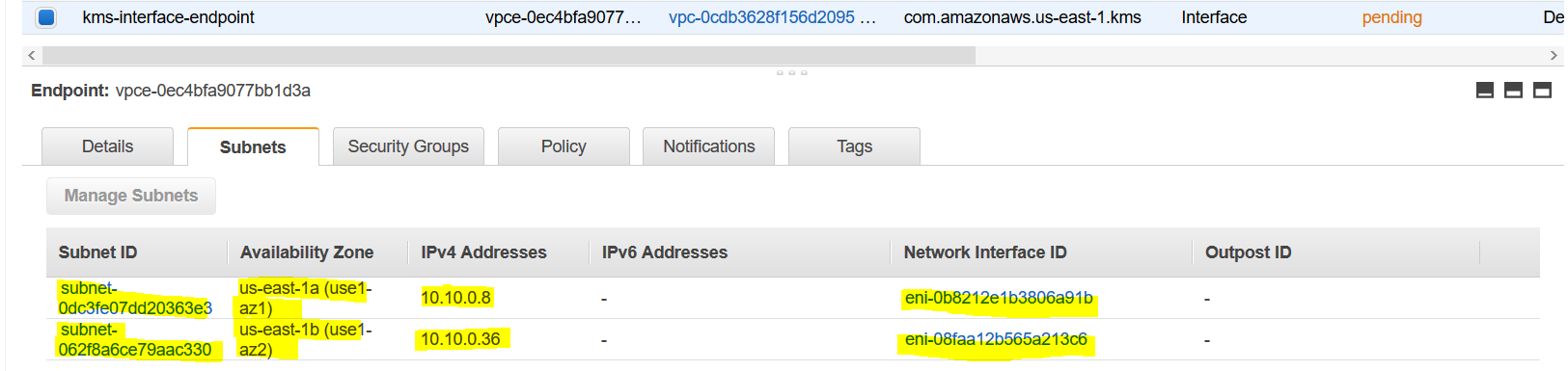
## VPC Interface Endpoints

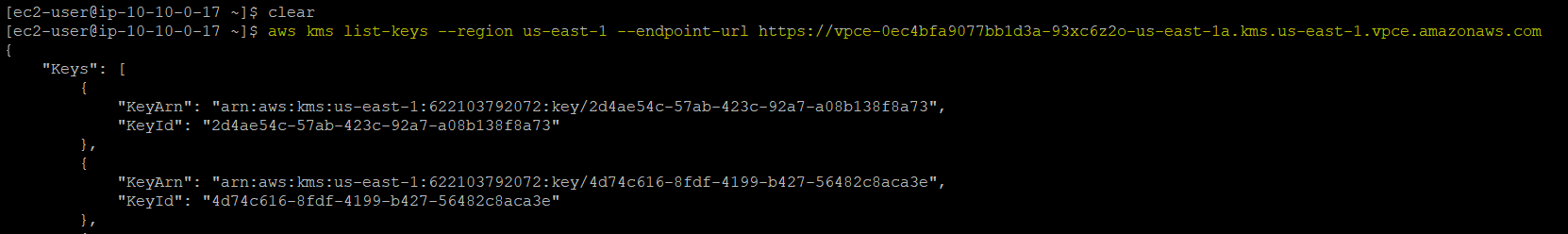
Diagram

Description automatically generated with low confidence



* **VPC Interface endpoint enables connectivity to services powered by AWS PrivateLink.**
* **Services include some AWS services for e.g. CloudTrail, CloudWatch, KMS, etc., services hosted by other AWS customers and partners in their own VPCs (referred to as endpoint services), and supported AWS Marketplace partner services.**
* **It creates a network interface in each subnet which is entry point for the AWS Service.**





### Limitations

* For each interface endpoint, only one subnet per Availability Zone can be selected.
* Each interface endpoint can support a **bandwidth of up to 10 Gbps per Availability Zone by default**. Additional capacity may be added automatically based on your usage.
* **Network ACL for the subnet can restrict traffic, and needs to be configured properly**
* **Interface Endpoint supports TCP traffic only.**
* **Endpoints are supported within the same region only.**
* **Endpoints support IPv4 traffic only.**
* Endpoints cannot be transferred from one VPC to another, or from one service to another.

sVPC Endpoint Services:

**VPC endpoint services can be used to expose an internal service running inside an VPC to internal application running in other VPC. This can be useful where there is no VPN connectivity & peering between VPCs.**

A screenshot of a computer

Description automatically generated with medium confidence

Graphical user interface, text, application

Description automatically generated

Diagram

Description automatically generated

## AWS Certification Exam Practice Questions

1. You have an application running on an Amazon EC2 instance that uploads 10 GB video objects to amazon S3. Video uploads are taking longer than expected inspite of using multipart upload cause of internet bandwidth, resulting in poor application performance. Which action can help improve the upload performance?
   1. Apply an Amazon S3 bucket policy
   2. Use Amazon EBS provisioned IOPS
   3. **Use VPC endpoints for S3**
   4. Request a service limit increase
2. What are the services supported by VPC endpoints, using Gateway endpoint type? Choose 2 answers
   1. **Amazon S3**
   2. Amazon EFS
   3. **Amazon DynamoDB**
   4. Amazon GlacierAmazon SQS
3. What are the different types of endpoint types supported by VPC endpoints? Choose 2answers
   1. **Gateway**
   2. Classic
   3. **Interface**
   4. Virtual
   5. Network
4. An application running on EC2 instances processes sensitive information stored on Amazon S3. The information is accessed over the Internet. The security team is concerned that the Internet connectivity to Amazon S3 is a security risk. Which solution will resolve the security concern?
   1. Access the data through an Internet Gateway.
   2. Access the data through a VPN connection.
   3. Access the data through a NAT Gateway.
   4. **Access the data through a VPC endpoint for Amazon S3.**
5. You need to design a VPC for a three-tier architecture, web-application consisting of an Elastic Load Balancer (ELB), a fleet of web/application servers, and backend consisting of an RDS database. The entire Infrastructure must be distributed over 2 availability zones. Which VPC configuration works while assuring the least components are exposed to Internet?
   1. Two public subnets for ELB, two private subnets for the web-servers, two private subnets for RDS and DynamoDB
   2. Two public subnets for ELB and web-servers, two private subnets for RDS and DynamoDB
   3. **Two public subnets for ELB, two private subnets for the web-servers, two private subnets for RDS and VPC Endpoints for DynamoDB**
   4. Two public subnets for ELB and web-servers, two private subnets for RDS and VPC Endpoints for DynamoDB