Day 01/100 AWS Date :- 09/12/2021

Amazon EBS encryption ⇒

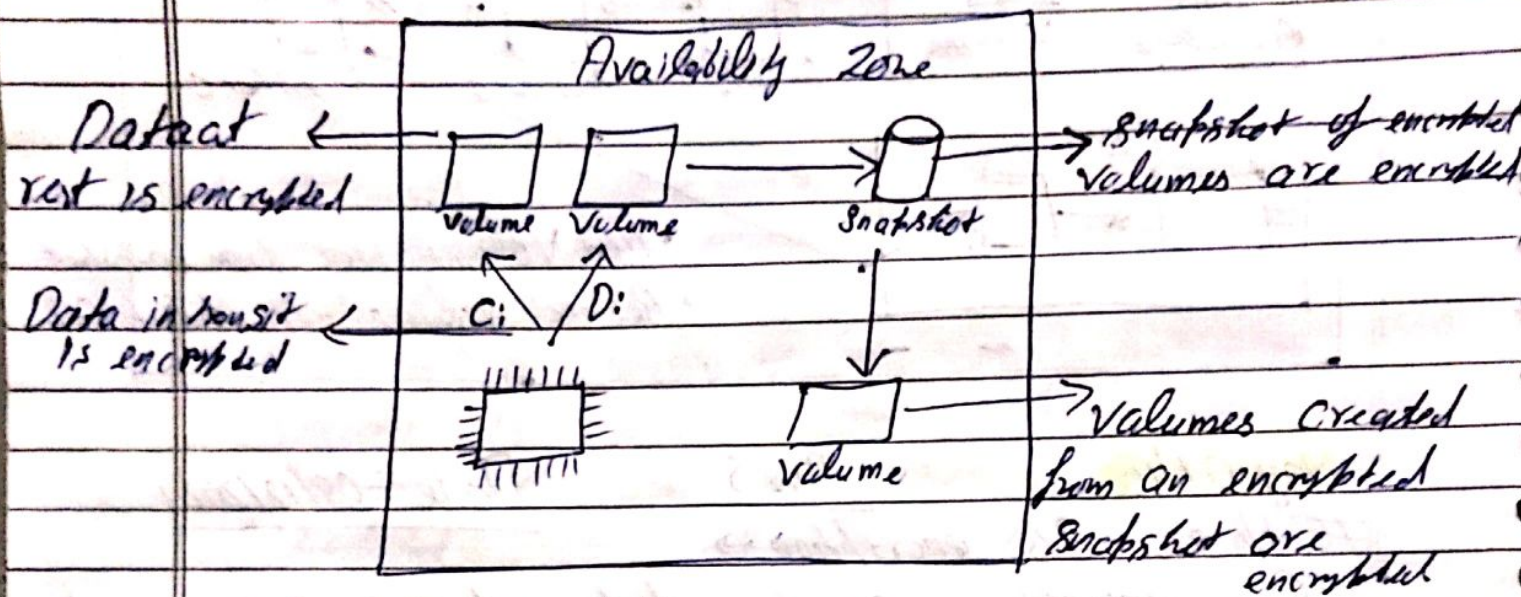
- EBS encryption enables data at rest security by encryption your data volumes, boot volumes and snapshots using Amazon-Managed Keys or keys created using AWS KMS.

- DATA at transit encryption occurs on the servers that host EC2 instance, which encrypts the data as it moves b/w EC2 instance and EBS data and boot volumes.

- EBS encrypts your volume with a data key using the industry-standard AES-256 algorithm

- The following types of data are encrypted :-
  - Data at rest inside the volume
  - All data moving b/w the volume and instance

- All snapshot created from the volume.
- All volumes created from these snapshots.



Amazon EBS Pricing :

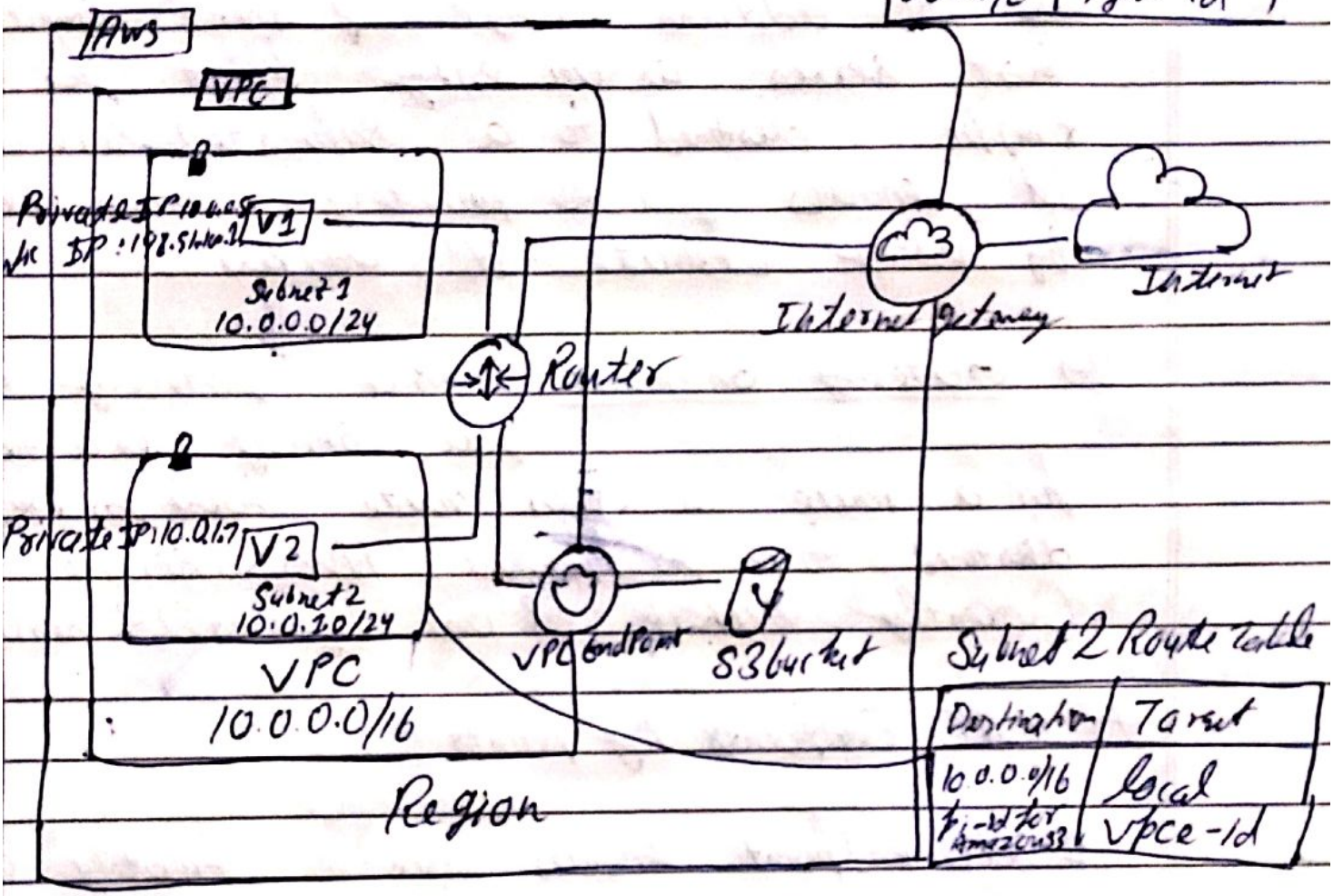
- With EBS, you pay for only what you provision.
- Volume Storage is charged for the amount of ~~EBS~~ GB provisioned per month, until the volume is released.
- Amazon EBS snapshot are a point in time copy of your block data. EBS snapshot are stored incrementally, which means you are billed only for the changed block stored.
- AWS Pricing Calculator can be used estimate the price to provision any EC2 instance

DATE 09/12/2021

AWS - VPC

Subnet 1 Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id



Subnet 2 Route Table

Destination	Target
10.0.0.0/16	local
pl-id for Amazon S3	VPCE-id

→ VPC endpoint enables creation of a private connection b/w VPC to supported AWS service and VPC endpoint service powered by PrivateLink using its private IP address. Traffic b/w VPC and AWS service does not leave the Amazon network.

There are two types of VPC endpoints.

-1-> Interface endpoint is an elastic network interface [ENI] with private IP address from the IP address range of user's subnet that serves as an entry point for traffic destined to a supported service. It enables you to privately access services by using private IP address.

2-> Gateway Endpoint is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service. Currently supports S3 and DynamoDB services.

VPC Endpoints Key points

1. VPC endpoint enables users to privately connect their VPC to supported AWS service.

2. VPC Endpoint does not require a public IP address, access over the Internet, NAT device, a ~~VPN~~ VPN Connection or AWS Direct Connect to communicate with resource in the service.

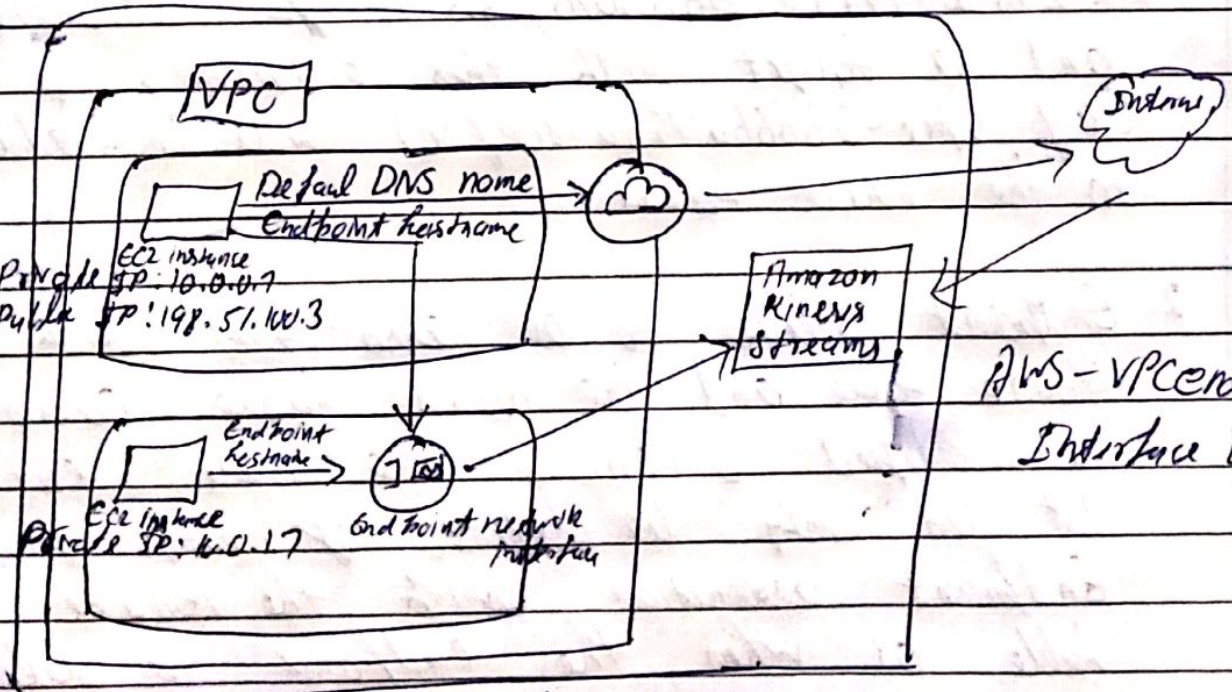
3) Endpoints are virtual devices, that are horizontally scaled, redundant, and highly available VPC Component that allow communication b/w instance in the VPC.

4) Access to the resource in other service can be controlled by endpoint policies.

5) By default, Endpoint policy, allows full access to services. Endpoint policies must be written in JSON format.

6) Endpoint policy does not override or replace IAM user policies or service-specific policies (such as

Interface Endpoints:



Default name: Kinesis.us-east-1.amazon.com
Endpoint-specific DNS hostname: vpce-123-ab.kinesis.us-east-1.vpce.amazonaws.com

DATE 09/11/2021

2. When you create an interface endpoint, AWS generate a static DNS hostname (Private) that you can use to communicate with the service. This is optional.

2. Network ACL for the subnet can restrict traffic and needs to be configured seperately.

Gateway Endpoints:

1. A route is automatically added to the Route table with a destination that specifies the prefix list of services and the target with the endpoint id.
e.g. - A rule with destination S3 service (pl-63a5400a (com.amazonaws.us-east-1.s3, 54.231.00/17, 52.216.0.0/15, 3.5.16.0/21, 3.5.0.0/20)) and a target with this endpoint's id (e.g. vpce-0666ba758a38cef8c) will be added to the route table.

2. 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 or when the endpoint is deleted.

BKS

DATE 09/12/2021

3. Security groups needs to be modified to allow outbound tcp traffic from the VPC to the service that specified in the endpoint. Use the service prefix list ID (e.g. com.amazonaws.us-east-1.s3) as the destination in the outbound rule.

4. Multiple endpoints can be created in a single VPC, for multiple services.

5. Multiple endpoints to the same service cannot be specified in a single route table.

6. You can create multiple endpoints in a single VPC for a single service but different Route Tables used to enforce different access policies from different subnets to the same services.

7. You can modify the endpoint policy that's attached to your endpoint and add or remove the route tables that are used by the endpoint.

VPC Endpoint Limitations:

1. VPC endpoint support IPv4 traffic only.
2. End point are supported within the same Region only. You cannot create an endpoint b/w a VPC and a service in a different Regions.
3. Endpoints could transfer an endpoint from one VPC to another or from one service to another.