Cloud Architect, Cloud Network Engineer

Compute, Networking

**Lab Details**

1. This lab walks you through the steps to create an endpoint for Amazon S3 and access with EC2 Instance in Private subnet.
2. EC2 instances of private subnet will be accessible from a bastion host or so-called an EC2 instance in a public subnet.
3. Duration: **90 minutes**
4. AWS Region: **US East (N. Virginia) us-east-1**

**Introduction**

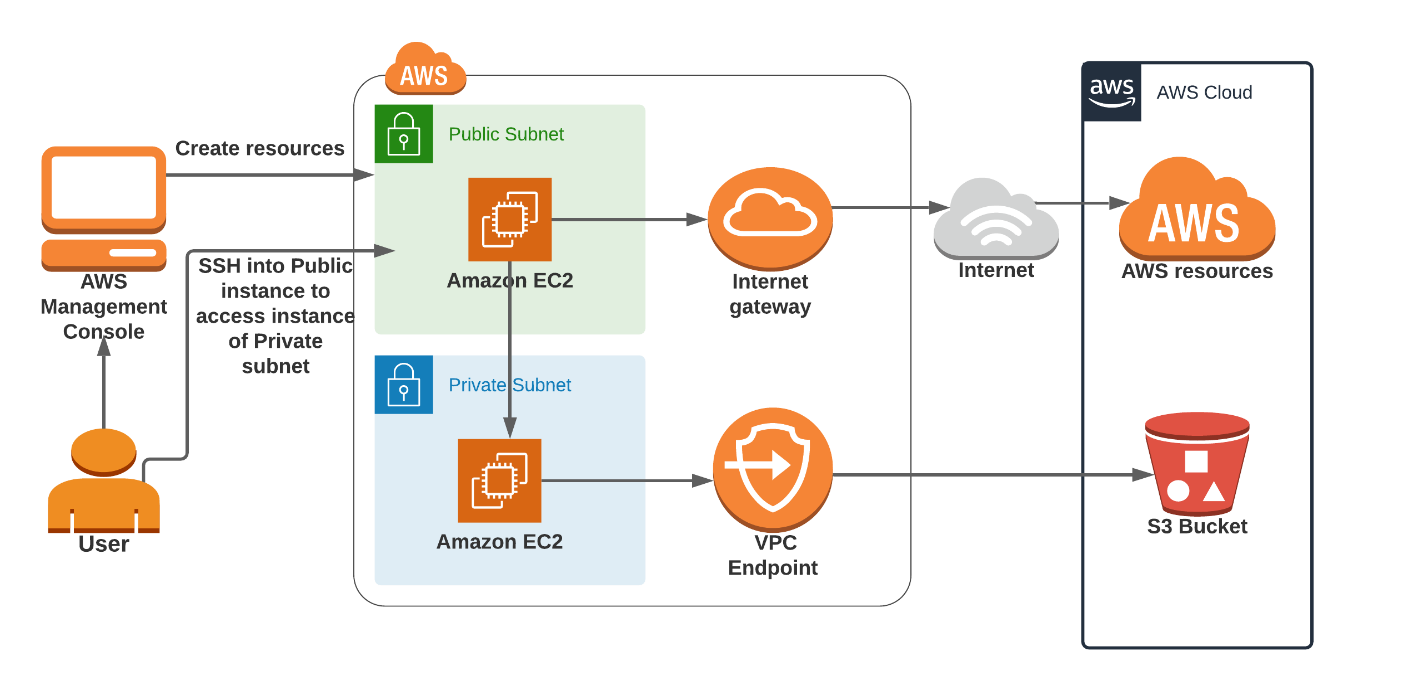
Bastion Instance

* **A bastion host is a system**that is exposed to the internet.
* In terms of security, Bastion is the only server that is exposed to the internet and should be highly protective of malicious attacks.
* **A Bastion host** is also **known as a Jump Box**. It is a computer that acts like a proxy server and that allows the client machine to connect to the remote server.
* It usually resides outside the firewall.
* In this lab, we are using Bastion instance as a Public instance to SSH into a Private instance.

VPC endpoint for S3

* VPC Endpoint allows us to securely connect your VPC and supported AWS services powered by AWS PrivateLink. AWS PrivateLink is a service that allows you to access AWS services by using private IP addresses. In this case, traffic does not leave Amazon’s network.
* VPC endpoint does not require a NAT Gateway, NAT instance, Internet Gateway, or any VPN services to access AWS Services.
* There are two types of VPC endpoints: Gateway and Interface.
* VPC endpoint for S3 comes under Gateway endpoint.
* When you create a VPC endpoint for S3, it asks for the Route table, then it adds the Prefix list to that route table. You can’t modify/delete the entry present in the route table, created by Endpoint.

**Architecture Diagram**



**Task Details**

1. Sign into AWS Management Console
2. Create a VPC
3. Create and attach an Internet Gateway with custom VPC
4. Create a Public and Private Subnet
5. Configure the Public subnet to enable auto-assign public IPv4 address
6. Add an entry to the Internet (0.0.0.0/0) in the Main Route table.
7. Create a Route Table for the Private subnet
8. Associate the Private subnet with the custom Route table i.e. RT for Private subnet
9. Create security groups
10. Create a Bastion Host (Publicly accessible EC2 Instance)
11. Create an Endpoint instance (Privately accessible EC2 instance)
12. SSH into Endpoint instance (Privately accessible) through Bastion host
13. Create a VPC endpoint for S3, attach it to the Private subnet's Route table.
14. List all the S3 Bucket and its objects
15. Validation of the lab.
16. Deleting AWS Resources.

**Launching Lab Environment**

     1. To launch the lab environment, Click on the  button.

     2. Please wait until the cloud environment is provisioned. It will take less than a minute to provision.

     3. Once the Lab is started, you will be provided with **IAM user name**, **Password**, **Access** **Key**, and **Secret** **Access** **Key**.

**Note** : You can only start one lab at any given time