**Secure Hybrid Access to S3 using VPC Endpoint**

[Access S3 From VPC]

**Introduction**

VPC endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components. They allow communication between your compute resources and AWS services without imposing availability risks.

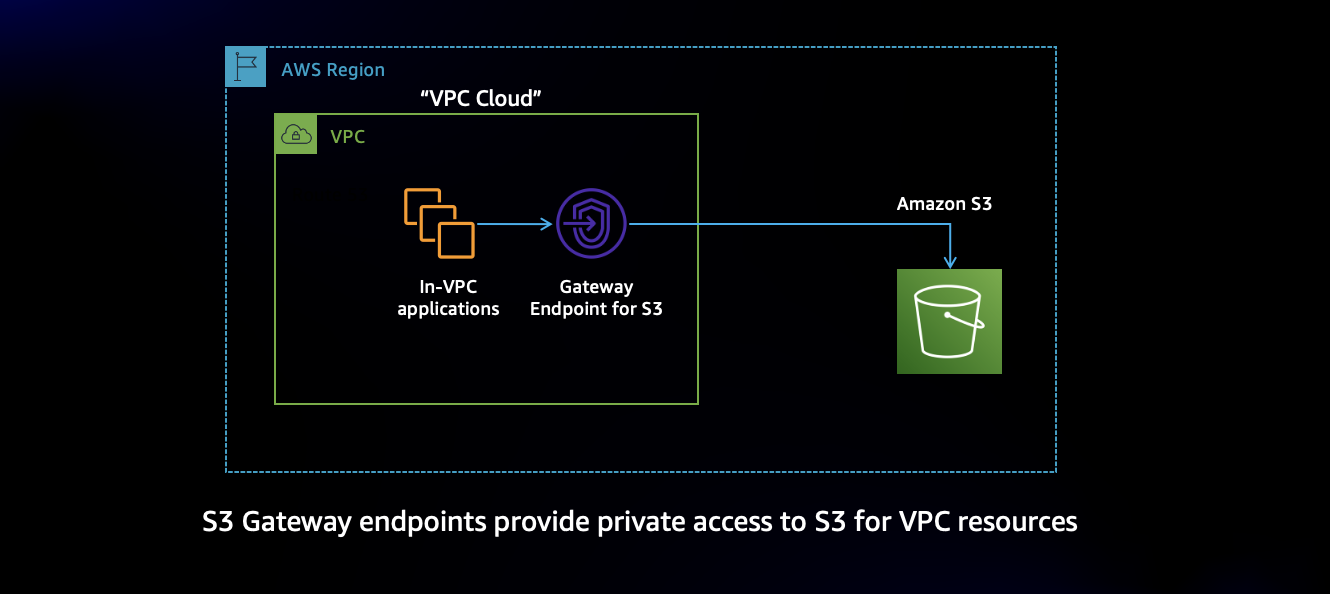
**Project Description – Scenario**

In this project, I will use VPC Cloud for cloud resources such as a Gateway endpoint and an EC2 instance to test with.

The Intention of this project is to demonstrate, how you can create, configure, and test VPC endpoints that enable your workloads to reach AWS services without traversing the Public Internet.

I will create a Gateway endpoint to access Amazon S3:

**Architecture – Overview**



Gateway VPC endpoint, and an Interface VPC endpoint. These two types of VPC endpoints offer different benefits depending on if you are accessing Amazon S3 from the cloud or you’re on-premises location.

**Access S3 from VPC**

In this section, I will create a Gateway endpoint to access Amazon S3 from an EC2 instance. The Gateway endpoint will allow me to create an S3 bucket and upload an object without using the Public Internet.

Note: To create an endpoint, you must specify the VPC in which you want to create the endpoint, and the service to which you want to establish the connection.

You can use both Gateway endpoints and Interface endpoints in the same VPC.

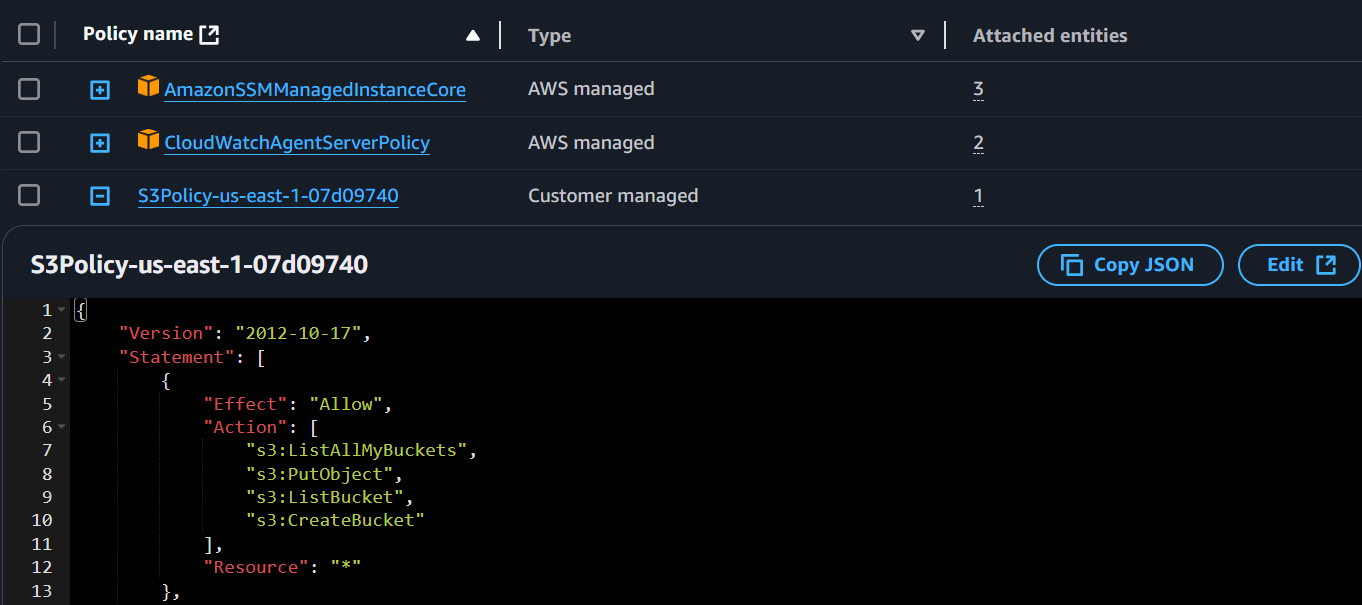
**Creating the Gateway endpoint**

**A screenshot of a computer

Description automatically generated**

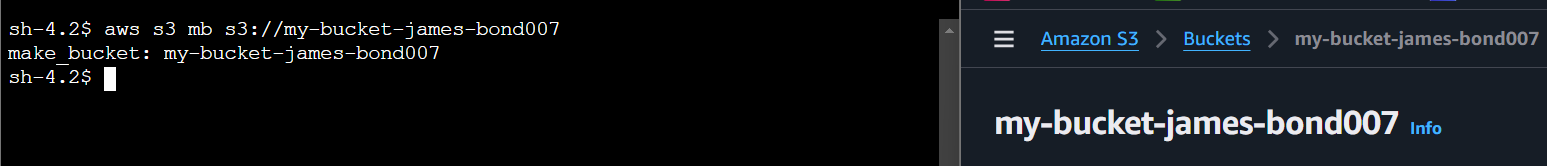
**Note:** AWS automatically adds a route that points traffic destined for the service to the endpoint to the selected route tables.

An IAM Role and Policy has been attached to the EC2 instance, the role grants s3 permissions to perform various actions.



**Test the Gateway Endpoint**

I will use AWS Session Manager to access EC2 instances and test connectivity to Amazon S3 through the Gateway endpoint



Testing the Gateway endpoint by uploading a file to Amazon S3

A screen shot of a computer code

Description automatically generated

A screenshot of a computer

Description automatically generated

**Summary | Re-cap**

* created a Gateway endpoint for Amazon S3, and used the AWS CLI to upload an object.
* The upload worked because the Gateway endpoint allowed communication to S3, without needing an Internet Gateway attached to "VPC Cloud".
* This demonstrates the functionality of the Gateway endpoint as a secure path to S3 without traversing the Public Internet.

**Done!**