Prashant Lakhera Follow
Mar 21, 2019 · 4 min read · Listen

100 Days of DevOps — Day 39-Introduction to VPC EndPoint

Welcome to Day 39 of 100 Days of DevOps, Focus for today VPC Endpoint

> What is VPC EndPoint?

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic.

There are two types of VPC endpoints:

- ***Interface endpoints**(using private links): An interface endpoint is an elastic network interface with a private IP address that serves as an entry point for traffic destined to a supported service*

```
# Supported Services

Amazon API Gateway

AWS CloudFormation

Amazon CloudWatch

Amazon CloudWatch Events

Amazon CloudWatch Logs

AWS CodeBuild

AWS Config

Amazon EC2 API

Elastic Load Balancing API

Amazon Elastic Container Registry

Amazon Elastic Container Service

AWS Key Management Service

Amazon Kinesis Data Streams

Amazon SageMaker and Amazon SageMaker Runtime

Amazon SageMaker Notebook Instance

AWS Secrets Manager

AWS Security Token Service

AWS Service Catalog

Amazon SNS

Amazon SQS

AWS Systems Manager

Endpoint services hosted by other AWS accounts

Supported AWS Marketplace partner services
```

- ***Gateway endpoints:** A gateway endpoint is a gateway that is a target for a specified route in your route table, used for traffic destined to a supported AWS service*

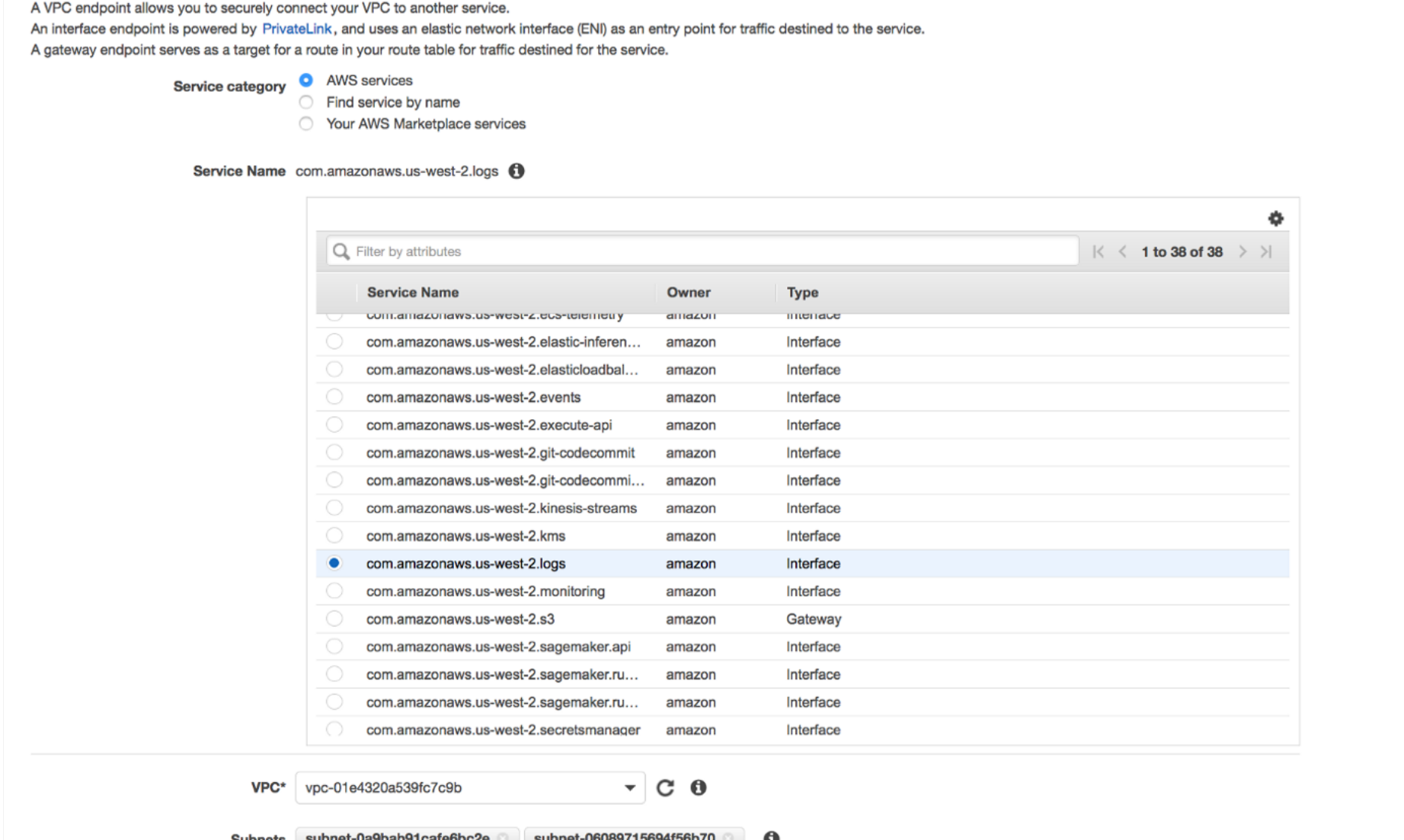
```
# Supported Services

* Amazon S3
* DynamoDB
```

***Scenario1:** I want to push logs from EC2 private instance(running on Private IP)to CloudWatch Logs.*

- *To setup VPC Endpoint*

```
Go to https://us-west-2.console.aws.amazon.com/vpc --> EndPoints
```



- *Once the endpoint is created you will see an elastic network interface with a private IP address which acts as an entry point for traffic destined to a supported service*

Terraform Code

```
resource "aws_vpc_endpoint" "ec2logs"{
  vpc_id            ="${var.vpc_id}"
  service_name      = "com.amazonaws.us-west-2.logs"
  subnet_ids = ["${var.subnet_id}"]
  vpc_endpoint_type = "Interface"

  security_group_ids = [
    "${var.security_group}"
  ]
  policy = <<POLICY
{
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        }
    ]
}
POLICY
  private_dns_enabled = true
}
```

vpc_logs_endpoint.tf hosted with ❤ by GitHub view raw

***Scenario2:** I want to push logs from EC2 private instance(running on Private IP)to AWS S3.*

- *In the case of gateway endpoint, you will see the entry in the route table, used for traffic destined to a supported AWS service*

Terraform Code

```
resource "aws_vpc_endpoint" "s3" {
  vpc_id       = "${var.vpc_id}"
  service_name = "com.amazonaws.us-west-2.s3"
  route_table_ids = ["${var.route_table}"]
      policy = <<POLICY
{
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        }
    ]
}
POLICY
}
```

s3_endpoint.tf hosted with ❤ by GitHub view raw

GitHub Link

100daysofdevops/100daysofdevops
Contribute to 100daysofdevops/100daysofdevops development by creating an account on GitHub.
github.com

> Limitations

- *Only Support IPv4*
- *Support only for the same region*
- *Interface endpoint cannot only be accessible via VPC Peering or VPN connection only via Direct Connect.*
- *You cannot use an IAM policy or bucket policy to allow access from a VPC IPv4 CIDR range (the private IPv4 address range). VPC CIDR blocks can be overlapping or identical, which may lead to unexpected results. Therefore, you cannot use the `aws:SourceIp` condition in your IAM policies for requests to Amazon S3 through a VPC endpoint. This applies to IAM policies for users and roles, and any bucket policies.If a statement includes the `aws:SourceIp` condition, the value fails to match any provided IP address or range*

Restricting Access to a Specific VPC Endpoint

```
{
   "Version": "2012-10-17",
   "Id": "Policy1415115909152",
   "Statement": [
     {
       "Sid": "Access-to-specific-VPCE-only",
       "Principal": "*",
       "Action": "s3:*",
       "Effect": "Deny",
       "Resource": ["arn:aws:s3:::examplebucket",
                    "arn:aws:s3:::examplebucket/*"],
       "Condition": {
         "StringNotEquals": {
           "aws:sourceVpce": "vpce-1a2b3c4d"
         }
       }
     }
   ]
}
```

restriction_access_to_specific_vpc_endpoint hosted with ❤ by GitHub view raw

Restricting Access to a Specific VPC

```
{
   "Version": "2012-10-17",
   "Id": "Policy1415115909153",
   "Statement": [
     {
       "Sid": "Access-to-specific-VPC-only",
       "Principal": "*",
       "Action": "s3:*",
       "Effect": "Deny",
       "Resource": ["arn:aws:s3:::examplebucket",
                    "arn:aws:s3:::examplebucket/*"],
       "Condition": {
         "StringNotEquals": {
           "aws:sourceVpc": "vpc-111bbb22"
         }
       }
     }
   ]
}
```

restriction_access_to_specific_vpc hosted with ❤ by GitHub view raw

Looking forward from you guys to join this journey and spend a minimum an hour every day for the next 100 days on DevOps work and post your progress using any of the below medium.

- *Twitter: @100daysofdevops OR @lakhera2015*
- *Facebook: https://www.facebook.com/groups/795382630808645/*
- *Medium: https://medium.com/@devopslearning*
- *Slack: https://devops-myworld.slack.com/messages/CF41EFG49/*
- *GitHub Link:https://github.com/100daysofdevops*

Reference

100 Days of DevOps — Day 0
D-day is just one day away and finally, this is a continuation of the post(I posted a month earlier)
medium.com