s3-via-endpoint-private-zone

At present, you can access AWS S3 via your VPC's private network using an S3 Interface VPC endpoint. For more information, please refer to the following documentation:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html

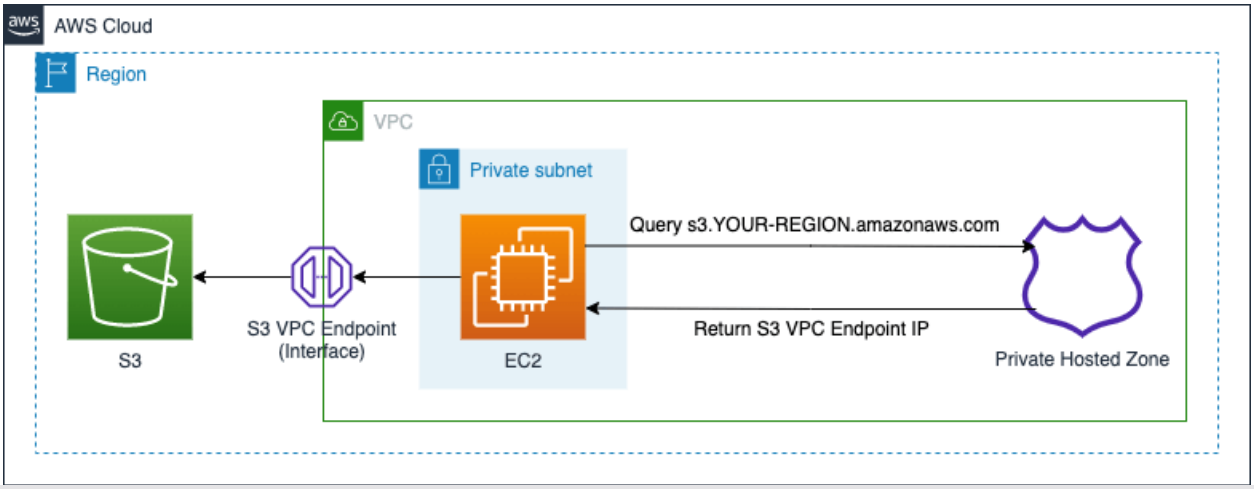
Please note that using an S3 Interface VPC endpoint requires specifying the `--endpoint-url` option, and you cannot access the default S3 endpoint (`your-region.s3.amazonaws.com`). If you need to access the default endpoint, you can use a Route 53 private hosted zone.

Table of Contents

Overview

If you need to access S3 from your on-premise network that is peered to a VPC, you may need to use a Route 53 inbound resolver (DNS Forwarder) depending on your network configuration. This post

provides instructions for accessing S3 from an EC2 instance in a private subnet.



Confirmation of S3 Access

You can confirm that you cannot access S3 without a provisioned S3 VPC endpoint.

```
$ aws s3 ls --region $YOUR_REGION --cli-read-timeout 1 --cli-connect-timeout 1

Connect timeout on endpoint URL: "https://s3.ap-northeast-1.amazonaws.com/"
```

Copy

Creation of S3 Interface VPC Endpoint

To create an S3 Interface VPC Endpoint, use the following commands.

Please note that Interface VPC Endpoints will continue to incur charges until they are deleted.

```
$ aws ec2 create-vpc-endpoint \
  --vpc-id $YOUR_VPC_ID \
  --vpc-endpoint-type Interface \
  --service-name com.amazonaws.$YOUR_REGION.s3 \
```

```
  --subnet-ids $YOUR_PRIVATE_SUBNET_IDS \
  --security-group-ids $YOUR_SECURITY_GROUP_IDS

$ aws ec2 describe-vpc-endpoints \
  --filters Name=service-
name,Values=com.amazonaws.$YOUR_REGION.s3 \
  --query "VpcEndpoints[*].DnsEntries"
[
    [
        {
            "DnsName": "*.vpce-xxxxxxxxxxxxxxxxx-
xxxxxxxx.s3.ap-northeast-1.vpce.amazonaws.com",
            "HostedZoneId": "xxxxxxxxxxxxxx"
        },
        {
            "DnsName": "*.vpce-xxxxxxxxxxxxxxxxx-xxxxxxxx-ap-
northeast-1a.s3.ap-northeast-1.vpce.amazonaws.com",
            "HostedZoneId": "xxxxxxxxxxxxxx"
        }
    ]
]
```

Copy

Access to S3 Using VPC Endpoint

You can now access S3 through the VPC endpoint using the following command.

Please note that the `--region` option must be specified.

```
$ aws s3 ls \
  --region $YOUR_REGION \
  --endpoint-url http://vpce-xxxxxxxxxxxxxxxxx-xxxxxxxx.s3.ap-
northeast-1.vpce.amazonaws.com
2022-11-26 06:28:36 sample-bucket-of-s3-through-private-network
```

Copy

Creation of Route 53 Private Hosted Zone

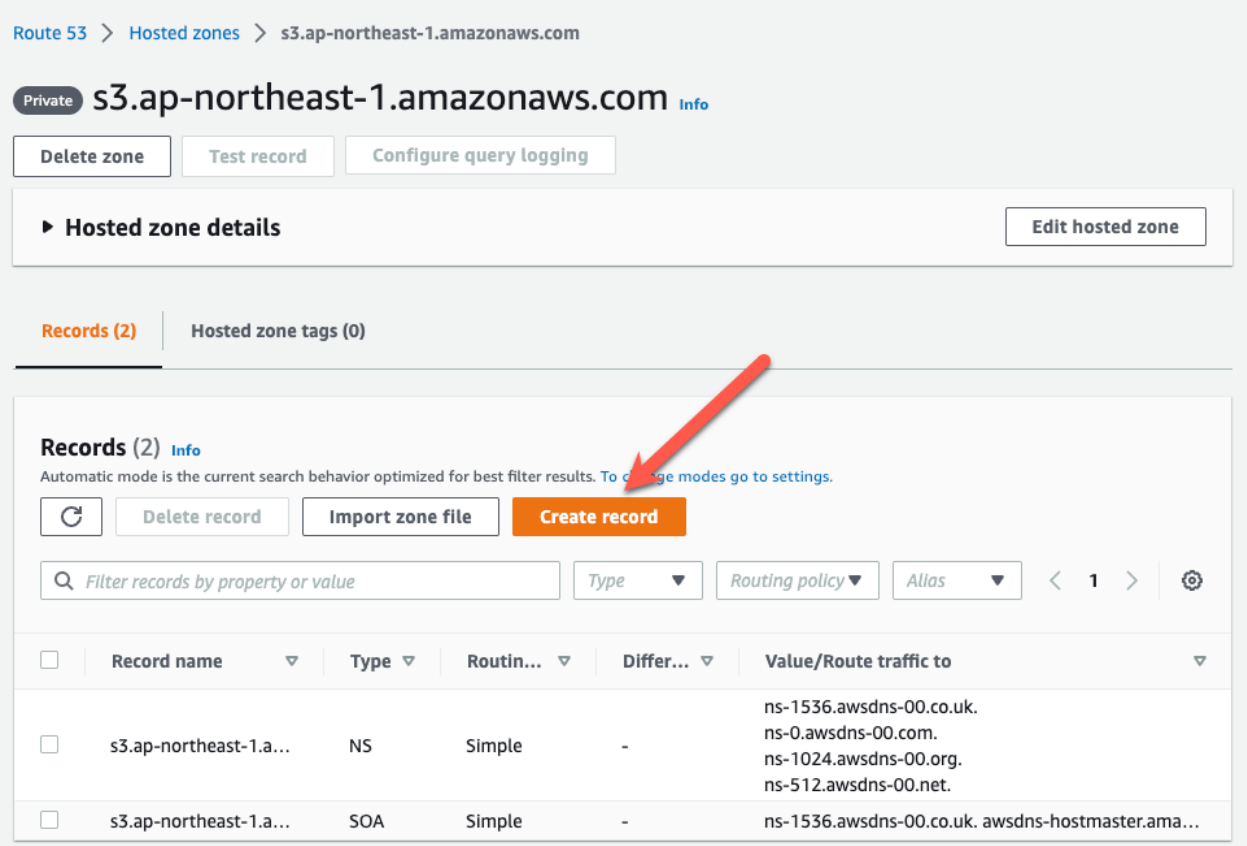
To create a Route 53 private hosted zone, use the following command.

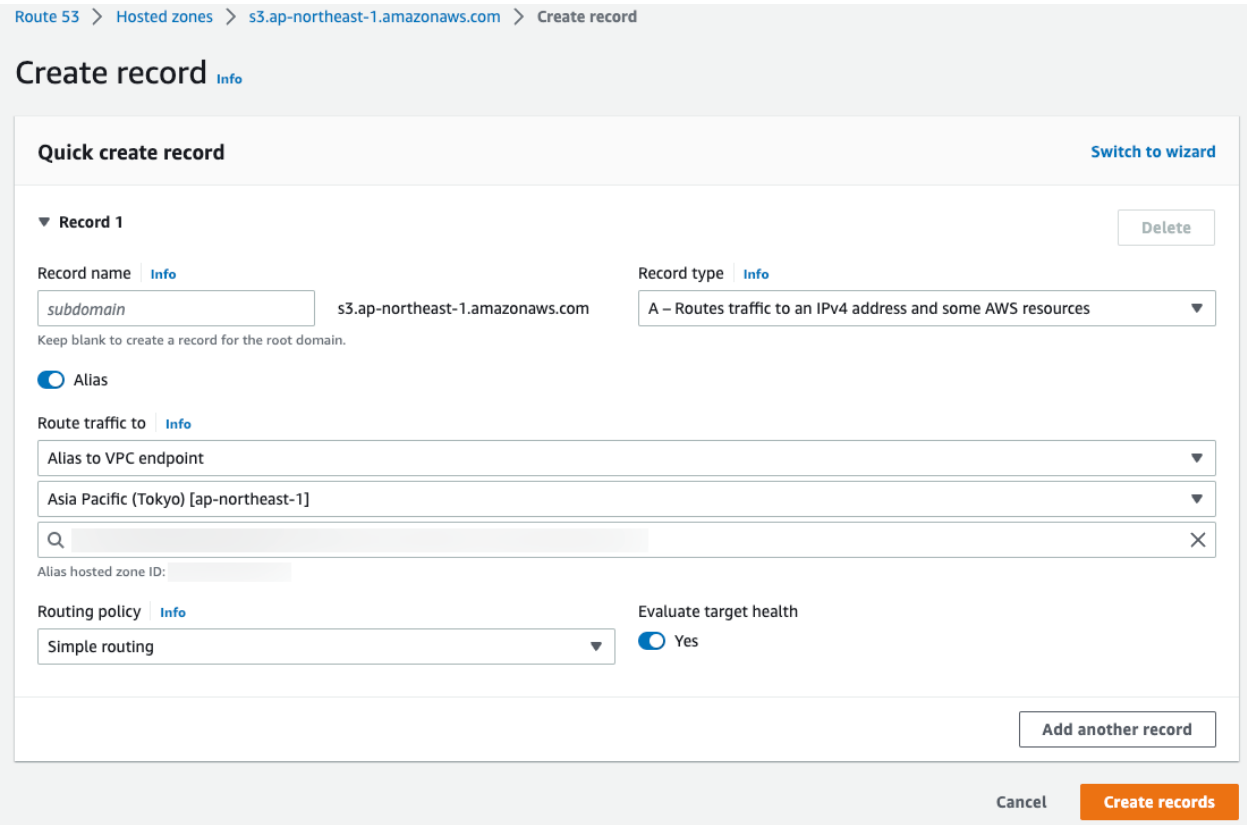
```
$ aws route53 create-hosted-zone \
  --name s3.$YOUR_REGION.amazonaws.com \
  --vpc VPCRegion=$YOUR_REGION,VPCId=$YOUR_VPC_ID \
  --caller-reference "$(date)"
```

Copy

Addition of DNS Record

To add an A (ALIAS) record, follow these steps.





Access to S3 without –endpoint-url

You can now access S3 without using the `--endpoint-url` option. Please note that the `--region` option must still be specified.

```
aws s3 ls --region ap-northeast-1
2022-11-26 06:28:36 sample-bucket-of-s3-through-private-network
```

Copy

Conclusion

In general, an S3 gateway VPC endpoint is only necessary if you need to access S3 exclusively from your VPC's private subnets. The use case presented in this post is useful when you need to access S3 without specifying the `--endpoint-url` option for any reason, such as when application code cannot be changed.