

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.

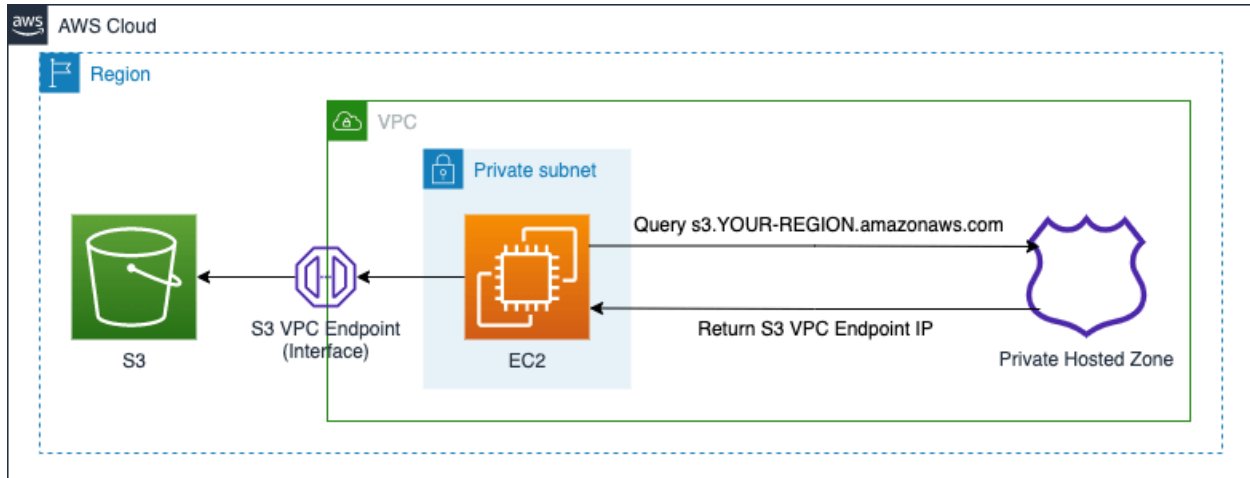
Table of Contents

- Overview
- Confirmation of S3 Access
- Creation of S3 Interface VPC Endpoint
- Access to S3 Using VPC Endpoint
- Creation of Route 53 Private Hosted Zone
- Addition of DNS Record
- Access to S3 without `-endpoint-url`
- Conclusion

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-xxxxxxxxxxxxxxxx-
xxxxxxxx.s3.ap-northeast-1.vpce.amazonaws.com",
      "HostedZoneId": "xxxxxxxxxxxxxx"
    },
    {
      "DnsName": "/*.vpce-xxxxxxxxxxxxxxxx-xxxxxxx-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-xxxxxxxxxxxxxxxx-xxxxxxx.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.

The screenshot shows the AWS Route 53 console interface for a private hosted zone named `s3.ap-northeast-1.amazonaws.com`. The breadcrumb navigation at the top indicates the path: `Route 53 > Hosted zones > s3.ap-northeast-1.amazonaws.com`. Below the zone name, there are buttons for `Delete zone`, `Test record`, and `Configure query logging`. A section titled `Hosted zone details` includes an `Edit hosted zone` button. The `Records (2)` tab is selected, showing a table of existing records. A red arrow points to the `Create record` button in the top action bar of the records section.

Route 53 > Hosted zones > s3.ap-northeast-1.amazonaws.com

Private s3.ap-northeast-1.amazonaws.com Info

Delete zone Test record Configure query logging

► Hosted zone details Edit hosted zone

Records (2) Hosted zone tags (0)

Records (2) Info

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

Refresh Delete record Import zone file Create record

Filter records by property or value Type Routing policy Alias < 1 > ⚙

<input type="checkbox"/>	Record name ▼	Type ▼	Routin... ▼	Differ... ▼	Value/Route traffic to ▼
<input type="checkbox"/>	s3.ap-northeast-1.a...	NS	Simple	-	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.
<input type="checkbox"/>	s3.ap-northeast-1.a...	SOA	Simple	-	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.ama...

Create record [Info](#)

Quick create record [Switch to wizard](#)

▼ Record 1 [Delete](#)

Record name [Info](#)

s3.ap-northeast-1.amazonaws.com

Keep blank to create a record for the root domain.

Record type [Info](#)

A – Routes traffic to an IPv4 address and some AWS resources ▼

☒ Alias

Route traffic to [Info](#)

Alias to VPC endpoint ▼

Asia Pacific (Tokyo) [ap-northeast-1] ▼

Alias hosted zone ID:

Routing policy [Info](#)

Simple routing ▼

Evaluate target health ☒ Yes

[Add another record](#)

Cancel

Create records

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.