



Configuring Amazon S3 security settings and access controls

Getting started at an AWS hosted workshop

▼ S3 Security Best Practices

▼ Prepare Your Lab

Attach IAM Role to EC2 Instance

Connect to the EC2 Instance

Bucket Name

▼ Lab 1 - S3 Security Exercises

Require HTTPS

Require SSE-KMS Encryption

Restrict Access to an S3 VPC Endpoint

Use AWS Config Rules to Detect a Public Bucket

Use Amazon Access Analyzer for S3

► Lab 2 - S3 Access Grants

► Lab 3 - Enabling Malware Protection for S3 by using GuardDuty

► Lab 4 - S3 Access Control Lists

Lab Summary

[Configuring Amazon S3 security settings and access controls](#) > [S3 Security Best Practices](#) > [Lab 1 - S3 Security Exercises](#)

Restrict Access to an S3 VPC Endpoint

You can simplify access to S3 resources from within a VPC by using a VPC Endpoint. These endpoints are easy to configure, highly reliable, and provide a secure connection to S3 that does not require a gateway or NAT instance.

In this exercise, we will configure a S3 VPC Endpoint and a bucket policy to limit access to only requests that pass through the VPC Endpoint. This is an easy way to limit access to only clients in your VPC.

From the AWS console in the top search bar, search and select VPC.

- Click Endpoints on the column to the left.
- Click Create Endpoint.
- Name your endpoint SID-endpoint

VPC > Endpoints > Create endpoint

Create endpoint Info

There are three types of VPC endpoints – Interface endpoints, Gateway Load Balancer endpoints, and Gateway endpoints. Interface endpoints and Gateway Load Balancer endpoints are powered by AWS PrivateLink, and use an Elastic Network Interface (ENI) as an entry point for traffic destined to the service. Interface endpoints are typically accessed using the public or private DNS name associated with the service, while Gateway endpoints and Gateway Load Balancer endpoints serve as a target for a route in your route table for traffic destined for the service.

Endpoint settings

Name tag - optional

Creates a tag with a key of 'Name' and a value that you specify.

SID-endpoint

Service category

Select the service category

☒ AWS services

Services provided by Amazon

☐ PrivateLink Ready partner services

Services with an AWS Service Ready designation

☐ AWS Marketplace services

Services that you've purchased through AWS Marketplace

☐ Other endpoint services

Find services shared with you by service name

- Type S3 in the search bar and press enter. This should filter to the S3 Endpoint. Select the Gateway type endpoint.

Services (1/5)

Search

s3 X Clear filters

	Service Name	Owner	Type	Service R
<input type="radio"/>	com.amazonaws.s3-global.accesspoint	amazon	Interface	–
<input type="radio"/>	com.amazonaws.us-west-2.s3	amazon	Interface	–
<input checked="" type="radio"/>	com.amazonaws.us-west-2.s3	amazon	Gateway	–
<input type="radio"/>	com.amazonaws.us-west-2.s3-outposts	amazon	Interface	–
<input type="radio"/>	com.amazonaws.us-west-2.s3express	amazon	Gateway	–

- Under VPC, select the VPC that says SID-vpc.

VPC

Select the VPC in which to create the endpoint

VPC

The VPC in which to create your endpoint.

vpc-05783b297c2d393a9 (SID-vpc)

- Do not configure any route tables. Leave the Policy set to Full Access.

Route tables (2) [Info](#)

Filter route tables

<input type="checkbox"/>	Name	Route Table ID	Main
<input type="checkbox"/>	SID-routes	rtb-028a65669bd37f55e (SID-routes)	No
<input type="checkbox"/>	-	rtb-0849f52f7cec90918	Yes

When you use an endpoint, the source IP addresses from your instances in your affected subnets for accessing the AWS service in the same region will be private IP addresses, not public IP addresses. Existing connections from your affected subnets to the AWS service that use public IP addresses may be dropped. Ensure that you don't have critical tasks running when you create or modify an endpoint.

Policy [Info](#)

VPC endpoint policy controls access to the service.

☒ **Full access**
Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service. All policies — IAM user policies, VPC endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.

☐ **Custom**
Use the [policy creation tool](#) to generate a policy, then paste the generated policy below.

1

- Click Create endpoint.

Copy the VPC Endpoint ID of vpce-xxxxxxx to your text editor.

Endpoints (1/1) [Info](#)

Filter endpoints

VPC endpoint ID: vpce-05d328d6153ecb854 [Clear filters](#)

<input checked="" type="checkbox"/>	Name	VPC endpoint ID	VPC ID	Service name
<input checked="" type="checkbox"/>	SID-endpoint	vpce-05d328d6153ecb854	vpc-05783b297c2d393a9 SID-vpc	com.amazonaws.us-we

From the AWS console in the top search bar, search and select S3.

- Click the bucket name starting with sid-security-xxxxxxx.
- Click on the Permissions tab.
- Under Bucket Policy click Edit

Delete the existing bucket policy. Copy the bucket policy below and paste into the Bucket Policy Editor.

```
{
  "Id": "S3-Security-Deny-unless-VPC-endpoint",
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:*",
    "Effect": "Deny",
    "Resource": "arn:aws:s3:::BUCKET_NAME/*",
    "Condition": {
      "StringNotEquals": {
        "aws:sourceVpce": "VPC_ENDPOINT_ID"
      }
    }
  },
  {
    "Principal": "*"
  }
]
```

Replace BUCKET_NAME with the bucket name and VPC_ENDPOINT_ID with the Endpoint ID.

Make sure you keep the /* at the end of the bucket name.

Your policy should look similar to the below policy.


Edit bucket policy [Info](#)

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts.

[Policy examples](#)
[Policy generator](#)

Bucket ARN

 arn:aws:s3:::sid-security-900ed8e0-6a30-11ed-961c-0a7f8723e72d

Policy

```

1 {
2   "Id": "S3-Security-Deny-unless-VPC-endpoint",
3   "Version": "2012-10-17",
4   "Statement": [{
5     "Action": "s3:*",
6     "Effect": "Deny",
7     "Resource": "arn:aws:s3:::sid-security-900ed8e0-6a30-11ed-961c-0a7f8723e72d/*",
8     "Condition": {
9       "StringNotEquals": {
10        "aws:sourceVpce": "vpce-0d35fe0a40ad750ff"
11      }
12    },
13    "Principal": "*"
14  }]
15 }
16

```

Click **Save Changes**.

From your SSH session run the following command.

```
aws s3api head-object --key app1/file1 --bucket ${bucket}
```



Curious, even though we've created our VPC endpoint and updated our S3 bucket policy to allow requests from the VPC endpoint `vpce-xxxxxxx` the S3 head request fails.

```

[ec2-user@storage-workshop ~]$
[ec2-user@storage-workshop ~]$ aws s3api head-object --key app1/file1 --bucket ${bucket}

An error occurred (403) when calling the HeadObject operation: Forbidden
[ec2-user@storage-workshop ~]$

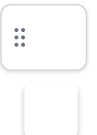
```

Why is this so?

The reason for this is because our EC2 instance is accessing S3 via the internet gateway. This is because the VPC endpoint does not yet have a route table association. We will need to associate a route table to our newly created VPC endpoint so our EC2 instance can access S3 via the VPC endpoint instead of the internet gateway.

From the AWS console in the top search bar, search and select **VPC**.

- Click **Endpoints** on the column to the left.
- Select the VPC Endpoint `SID-endpoint` we created early. Click **Actions** and select **Manage Route Tables**.
- Select the Route Table ID named `SID-routes`.



VPC > Endpoints > vpce-05d328d6153ecb854 > Manage route tables

Manage route tables [info](#)

Subnets associated with selected route tables will be able to access this endpoint.

Route tables (1/2)

Filter route tables

	Name	Route Table ID	Main	Associated Id
<input checked="" type="checkbox"/>	SID-routes	rtb-028a65669bd37f55e (SID-routes)	No	subnet-0d0f8a74b89062c69 (SID-subnet1)
<input type="checkbox"/>	-	rtb-0849f52f7cec90918	Yes	-

When you use an endpoint, the source IP addresses from your instances in your affected subnets for accessing the AWS service in the same region will be private IP addresses, not public IP addresses. Existing connections from your affected subnets to the AWS service that use public IP addresses may be dropped. Ensure that you don't have critical tasks running when you create or modify an endpoint.

Cancel **Modify route tables**

Click Modify Route Tables.

From you SSH session run the following command.

```
aws s3api head-object --key app1/file1 --bucket ${bucket}
```



The request succeeds because the EC2 instance is able to find a route its S3 request via the VPC Endpoint and because our S3 bucket policy permits requests via the VPC endpoint.

```
[ec2-user@storage-workshop ~]$ aws s3api head-object --key app1/file1 --bucket ${bucket}
{
  "AcceptRanges": "bytes",
  "ContentType": "binary/octet-stream",
  "LastModified": "Sun, 08 Oct 2023 21:10:16 GMT",
  "ContentLength": 1048576,
  "ETag": "\"b6d81b360a5672d80c27430f39153e2c\"",
  "ServerSideEncryption": "AES256",
  "Metadata": {}
}
[ec2-user@storage-workshop ~]$
```

[Previous](#)
[Next](#)
