

VPC Endpoints S3 Bucket

- ❖ Managing Amazon S3 access with VPC endpoints and S3 Access Points
- ❖ Many customers own multiple Amazon S3 buckets, some of which are accessed by applications running in VPCs.
- ❖ Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you define.
- ❖ This virtual network closely resembles a traditional network that you would operate in your own data center, with the benefits of using the **scalable infrastructure of AWS**.
- ❖ It is often the case that you want to make sure that applications running inside a VPC have access only to **specific S3 buckets**.
- ❖ Furthermore, when you have multiple shared datasets that must be accessed by applications running in **different VPCs, managing access and permissions can quickly become a challenge**.
- ❖ VPC endpoints for Amazon S3 simplify access to S3 from within a VPC by providing configurable and highly reliable secure connections to S3 that do not require an internet gateway or Network Address Translation (NAT) device.
- ❖ When you create a **S3 VPC endpoint**, you can attach an endpoint policy to it that controls access to Amazon S3.
- ❖ S3 Access Points, a feature of Amazon S3, simplifies managing data access at scale for applications using shared datasets on S3.
- ❖ Access Points are unique hostnames that customers create to enforce distinct permissions and network controls for any request made through the Access Point.
- ❖ In this post, I discuss an approach that uses S3 Access Points in combination with VPC endpoint policies to make it easy to manage access to shared Amazon S3 datasets.
- ❖ The idea is to create an Amazon S3 VPC-Only Access Point and use it in the VPC endpoint policy to control access to the S3 bucket.
- ❖ You also have the option to use bucket policies to **firewall S3 bucket access to VPCs only**, which I also cover.

Using Amazon S3 VPC endpoints to control access to S3 buckets

Organizations can specify individual buckets in the Amazon S3 VPC endpoint policy to restrict access to only specific buckets from within the VPC.

Here is a sample VPC endpoint policy to allow access to a specific S3 bucket from within a VPC:

```
{
  "Statement": [
    {
      "Sid": "Access-to-specific-bucket-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::my_secure_bucket",
        "arn:aws:s3:::my_secure_bucket/*"]
    }
  ]
}
```

While this is useful, as the number of buckets owned by the organization grows, it becomes difficult to keep track and manually specify newly created buckets in the Amazon S3 VPC endpoint policy.

For example, when a new S3 bucket is created in a particular account that the application running within a VPC needs access to, you must manually edit the VPC endpoint policy to allow list the newly created S3 bucket.

To make this simpler to manage, we look at Amazon S3 Access Points.

Using S3 Access Points with VPC endpoints

To restrict access optionally further to a shared Amazon S3 bucket, you can use a VPC endpoint policy to require applications use the S3 Access Point through a specified VPC.

S3 Access Points have an AWS ARN that includes the account number and Region identifier, which can be used in the VPC endpoint policy.

Instead of specifying individual buckets in the Amazon S3 VPC endpoint policy, an Access Point prefix can be used to specify all Access Points under an account.

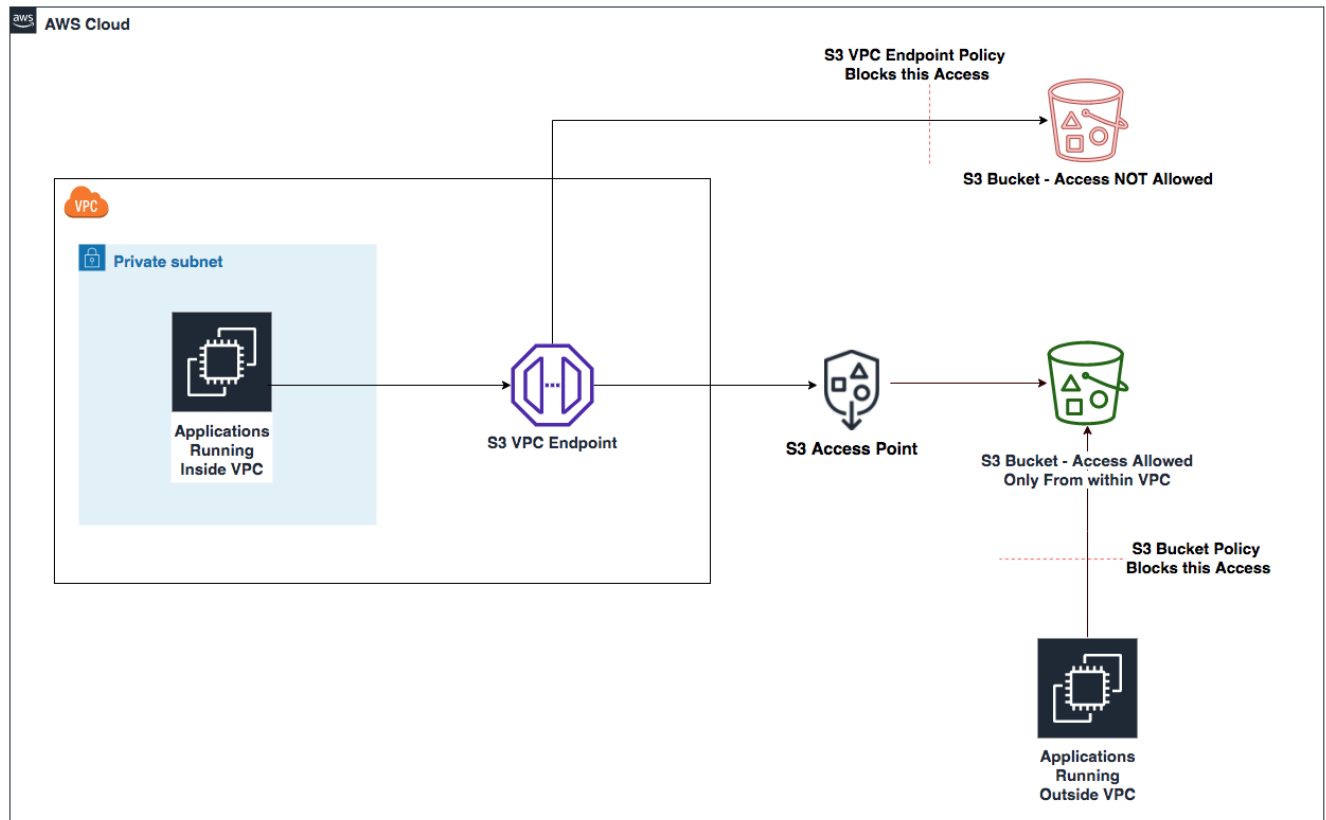
For example, in the VPC endpoint policy, you can add a condition as shown in the following snippet:

```
"Condition": {  
    "ArnNotLikeIfExists": {  
        "s3:DataAccessPointArn": "arn:aws:s3:us-east-1:<Account  
ID>:accesspoint/*"  
    }  
}
```

When a new Amazon S3 bucket is created, to allow access from the VPC, you can create an S3 Access Point on the S3 bucket.

The preceding condition in the VPC endpoint policy would automatically allow access to this new S3 bucket via the Access Point, without having to edit the VPC endpoint policy.

Setup and tutorial



Prerequisites

- AWS Account with a VPC
- A private subnet (no internet access via Internet Gateway, NAT gateway or NAT instance)
- At least one Amazon S3 bucket

Tutorial

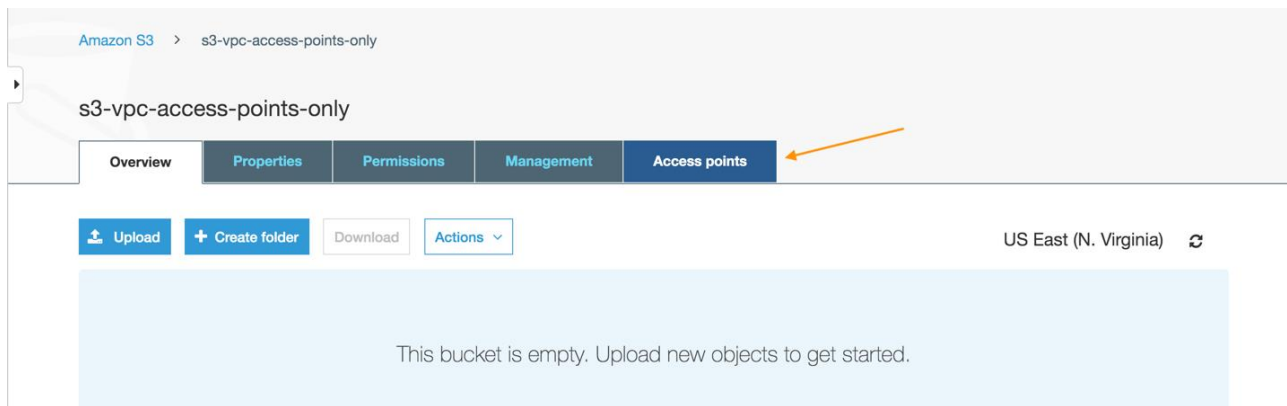
- Create a VPC-only Access Point for the Amazon S3 bucket. This makes sure that this Access Point can only be accessed by resources in a specific VPC.
- Create Amazon S3 gateway endpoint in the VPC and add a VPC endpoint policy. This VPC endpoint policy will have a statement that allows S3 access only via access points owned by the organization. We take advantage of the account ID in the Access Point ARN to make this possible.
- Add a bucket policy on the bucket to allow access only from the VPC: This prevents any access from outside the VPC.

Add Amazon S3 VPC only Access Point on the buckets

We first create an S3 Access Point that's only accessible from a specified VPC. It has a network origin of VPC, and Amazon S3 rejects any request made to the Access Point that doesn't originate from that VPC.

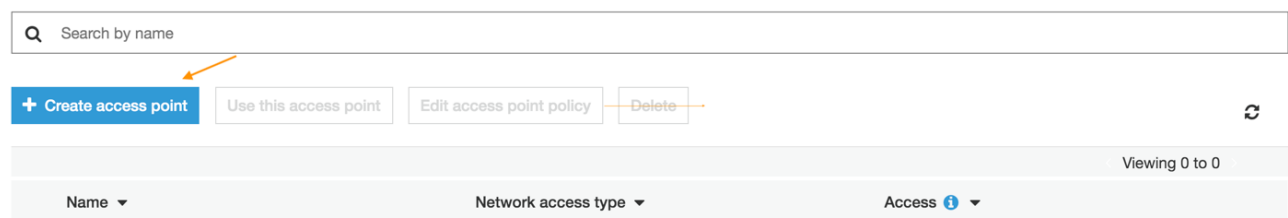
In the Amazon S3 console, navigate to the bucket you want to allow access from your VPCs.

Choose Access points.



Choose **Create access point**.

Access points can be used to provide access to your bucket. The S3 console doesn't support using virtual private cloud (VPC) access points to access bucket resources. To access bucket resources from a VPC access point, you'll need to use the AWS CLI, AWS SDK, or Amazon S3 REST API. [Learn more](#)



On the **Create access point** page:

- Give a name to the Access Point. (You can use any name that is unique to the account. This is not a globally unique name like the S3 bucket name.)
- For the **Network access type**, select **Virtual Private Cloud (VPC)**.

Create access point

Region

US East (N. Virginia)

Region is determined by bucket location

Access point name

vpc-only-access-point

Access point names must be unique within the account for this Region, and comply with the [rules for access point naming](#).

Network access type

☒ Virtual private cloud (VPC)

No internet access. Requests are made over a specified VPC only.

☐ Internet

Select **Block all public access**.

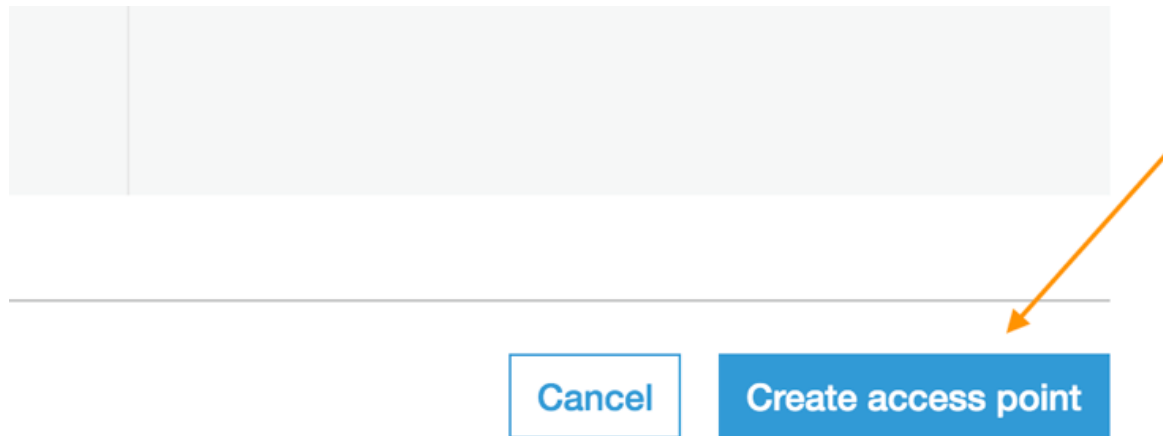
Block public access (access point settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this access point. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

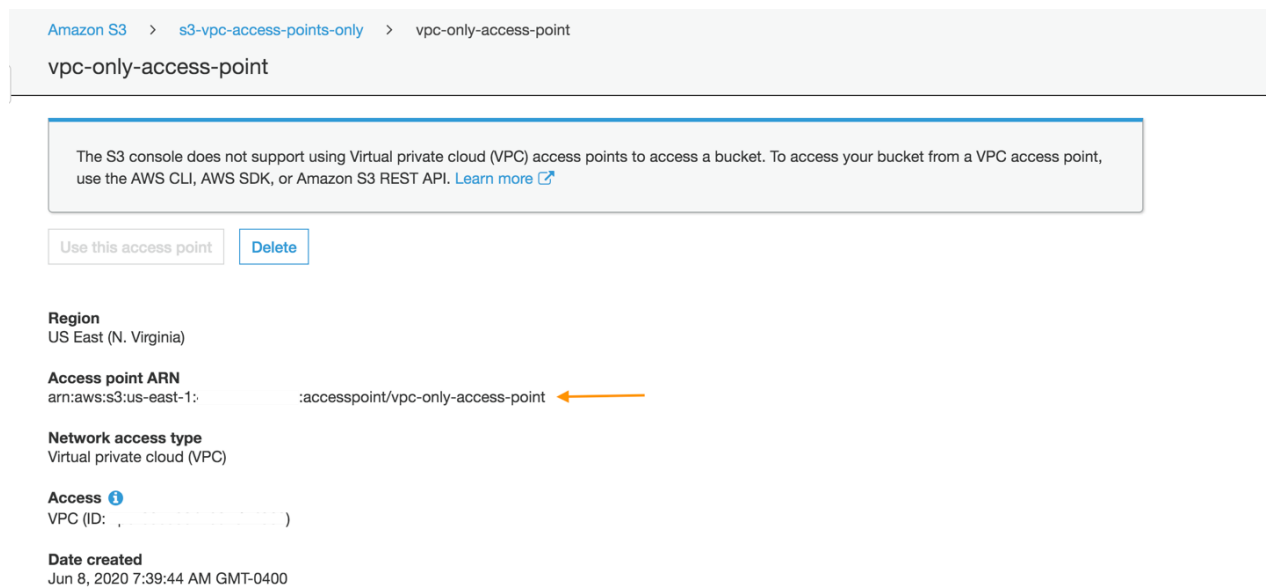
☒ **Block all public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

Choose **Create access point**.

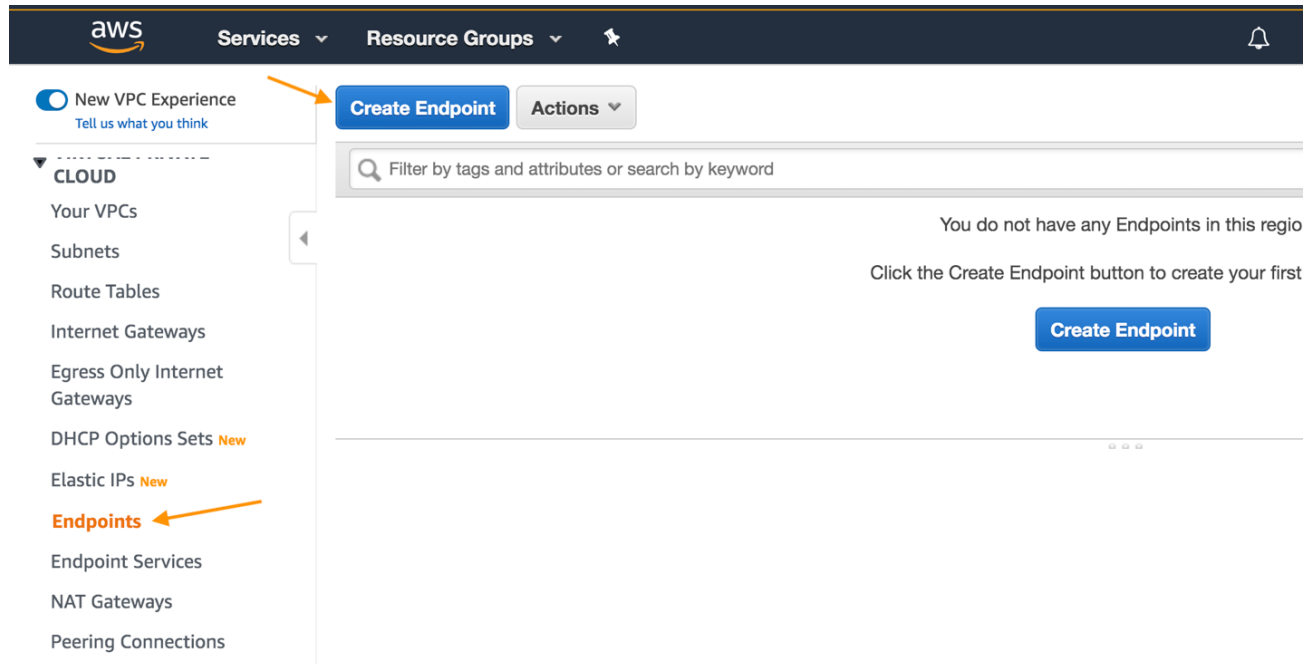


Navigate back to Access Point and note the ARN of the Access Point.



Create an Amazon S3 gateway endpoint in your VPC

We then create an Amazon S3 VPC Gateway endpoint to make sure that all S3 traffic is routed via this S3 VPC endpoint. Navigate to the Amazon VPC console and click Endpoints from the left navigation menu. Choose Create Endpoint.



Search and select endpoints for S3

[Endpoints](#) > Create Endpoint

Create Endpoint



A VPC endpoint allows you to securely connect your VPC to another service.
An interface endpoint is powered by [PrivateLink](#), and uses an elastic network interface (ENI) as an entry point for traffic destined to the service.
A gateway endpoint serves as a target for a route in your route table for traffic destined for the service.

- Service category**
- ☒ AWS services
 - ☐ Find service by name
 - ☐ Your AWS Marketplace services

Service Name com.amazonaws.us-east-1.s3 ⓘ

search : s3 Add filter			1 to 1 of 1	
Service Name	Owner	Type		
<input checked="" type="radio"/> com.amazonaws.us-east-1.s3	amazon	Gateway		

Select the VPC and subnet where you want the endpoint to be created. Only resources in the selected subnets are able to access the Amazon S3 endpoint.

VPC*  

Configure route tables A rule with destination **pl-63a5400a (com.amazonaws.us-east-1.s3)** and a target with this endpoints' ID (e.g. vpce-12345678) will be added to the route tables you select below.

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

	Route Table ID	Main	Associated With
<input checked="" type="checkbox"/>	rtb-	Yes	subnet-

Under the **Policy** section, select **custom** and paste the following policy into the text-area. Make sure you replace the *<Account ID>* with the ID of the account of your account.

Note that we use a wild card “” to specify the Access Point ARN. This allows access to any new Amazon S3 access points created under the account and eliminates the process of manually editing VPC endpoint policies*

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "AllowUseOfS3",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "*"
    },
    {
      "Sid": "OnlyIfAccessedViaAccessPoints",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "ArnNotLikeIfExists": {
```

```

        "s3:DataAccessPointArn": "arn:aws:s3:us-east-1:<Account
ID>:accesspoint/*"
    }
}
]
}

```

- Click **Create Endpoint**.

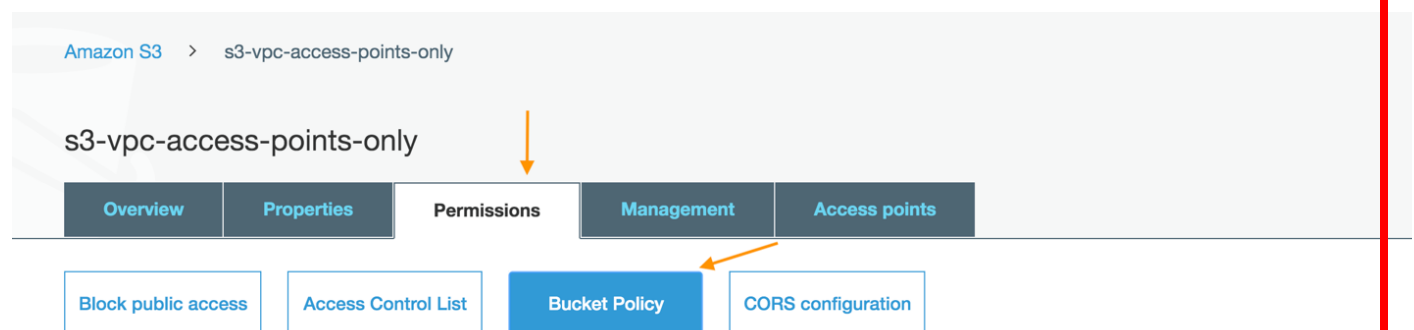
Locking down Amazon S3 bucket to VPC access only

You may want to ensure that Amazon S3 buckets can be accessed from within VPC only. This can be achieved using a bucket policy on the S3 bucket that restricts access only to specified VPCs.

Complete the following steps to set up a bucket policy and a Service Control Policy (SCP).

First, we create an Amazon S3 bucket policy to make sure that the S3 bucket can be accessed only from a specific VPC.

- Navigate back to the S3 bucket main page.
- Click **Permissions**, then click **Bucket Policy**.



Copy and paste the following bucket policy. Make sure you replace *<bucket name>* with the name of the bucket and *<vpc id>* with the VPC that is allowed to access the bucket.

```
{
  "Version": "2012-10-17",
  "Id": "S3BukcetPolicyVPCAccessOnly",
  "Statement": [
    {
      "Sid": "DenyIfNotFromAllowedVPC",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::<bucket name>",
        "arn:aws:s3:::<bucket name>/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:SourceVpc": "<vpc id>"
        }
      }
    }
  ]
}
```

Restricting S3 Access Points to VPC-Only type

You can set up AWS SCPs to require any new Access Point in the organization to be restricted to VPC-Only type. This makes sure that any Access Point created in

your organization provides access only from within the VPCs and there by firewalling your data to within your private networks.

Here is a sample SCP that can be applied at root, organizational unit, or account level:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "Action": [
        "s3:CreateAccessPoint"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEqualsIfExists": {
          "s3:AccessPointNetworkOrigin": [
            "vpc"
          ]
        }
      }
    }
  ]
}
```

Automation of S3 Access Point Creation with AWS CloudFormation

You may seek to deploy multiple S3 Access Points with a consistent configuration.

In that case, an AWS CloudFormation template can be used to create, update, and delete an entire S3 Access Point stack as a single unit, instead of creating S3 Access Points individually. The CloudFormation template describes your desired

S3 Access Point resources and their dependencies. This enables you to automate the management and provisioning of S3 Access Points across multiple AWS accounts and AWS Regions consistently.

Here is a sample AWS CloudFormation template for S3 Access Point deployment.

Please note that the following parameters can be changed depending on preference.

Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

pAccessPointName
Access Point Name.

pAuditAccountID
Account ID requiring access.

pAuditAdminEmail
audit admin email.

pFoldertoAccess
Folder to Access Name.

pFunctionName
lambda function name.

pRoleName
S3 Access Point role Name.

pSNSTopicName
SNS Topic Name.

Cleaning up

If you completed the steps in this post to test S3 Access Points and VPC endpoints, you may want to delete the resources to avoid incurring unwanted charges.

To delete an S3 Access Point:

1. Open the [Amazon S3 console](#).
2. Navigate to the **Access points** tab for your bucket.
3. Select the option button next to the name of the Access Point that you want to delete.
4. Choose **Delete**.
5. Confirm that you want to delete your Access Point by entering its name in the text field that appears and choosing **Confirm**.

To delete an endpoint:

- Open the [Amazon VPC console](#).
- In the navigation pane, choose **Endpoints** and select your endpoint.
- Choose **Actions, Delete Endpoint**.
- In the confirmation screen, choose **Yes, Delete**.

Conclusion

Managing data access at scale for shared datasets in Amazon S3 can be challenging when you have large number of applications with different access requirements.

Furthermore, you would need to make sure that access to sensitive data is firewalled to within your private networks.

In this post, I discussed how you can use Amazon S3 VPC endpoints and S3 Access Points to manage permissions to shared datasets on S3.

I also discussed how you can firewall data access to within your VPC to ensure that your sensitive data is protected from any unintended access from outside your VPCs.

S3 Access Points can be used with VPC endpoints to provide secure access to multi-tenant S3 buckets while making it easy to manage permissions.

Having secure access to multi-tenant S3 buckets while easily managing permissions enables you to scale seamlessly with minimal manual intervention while ensuring that your sensitive data is protected.