How-To Library

Informatica

Configuring private communication with Amazon S3 using the Amazon S3 V2 Connector

Abstract

This article describes how you can configure private communication to connect to Amazon S3 using the Amazon S3 V2 Connector.

Supported Versions

- Informatica® Cloud Data Integration Amazon S3 V2 Connector
- Informatica® Cloud Data Integration

Table of Contents

Overview

You can configure a gateway endpoint or interface endpoint on the AWS console and in the Amazon S3 V2 connection to enable private communication to connect to Amazon S3 from Cloud Data Integration.

You can configure Amazon S3 V2 Connector to establish private communication with Amazon S3 without exposing your traffic to the public internet. To establish a private connection with Amazon S3, ensure that the Secure Agent is a part of the subnet in the AWS Virtual Private Cloud (VPC). An S3 endpoint routes an S3 request to the Amazon S3 service. You can create an S3 interface endpoint or an S3 gateway endpoint.

S3 gateway endpoint

A gateway endpoint is a target for a route in your route table that is used to forward S3 traffic to the S3 gateway endpoint.

Route tables control the routing of traffic between the VPC and the AWS service. Each subnet that is associated with one of the route tables has access to the endpoint. The traffic from instances in these subnets is then routed through the endpoint to the AWS service.

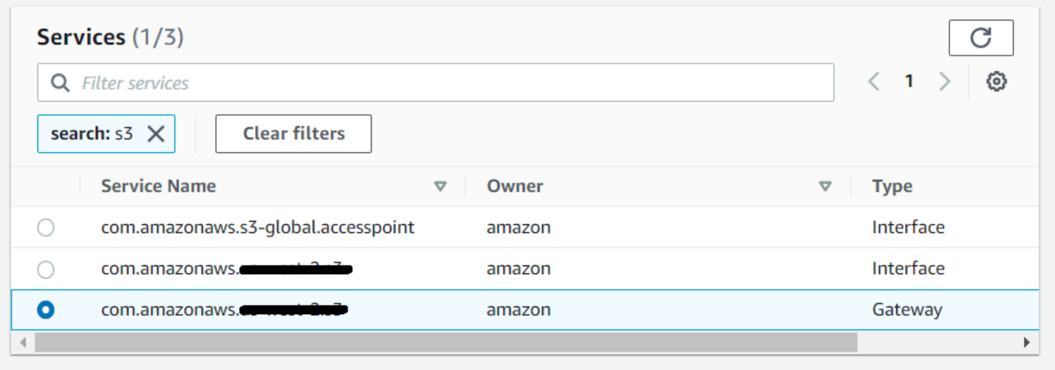
Configure the gateway endpoint on the AWS console

On the AWS console, select a service of the gateway type, select the VPC, the route table, and add a policy for the endpoint.

Perform the following steps on the AWS console to configure a gateway endpoint:

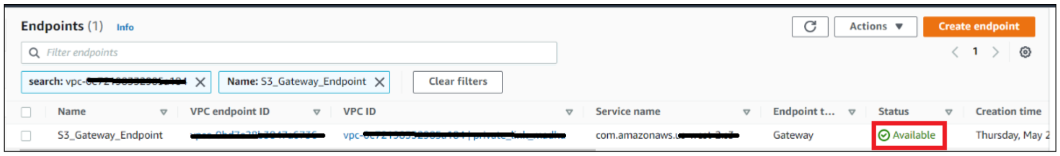
1. Log in to the **AWS Console**, and in the navigation pane, choose the region where you want to create endpoints.
2. On the **Search** tab, search for VPC.
   The VPC dashboard appears.

3. Click **Endpoints**.
4. Click **Create endpoint**.
   The **Create endpoint page** appears.
5. Enter a name for the S3 gateway endpoint.
6. Select **AWS services** as the service category.
7. In **Services**, search for S3, and select a service of the gateway type.
   The following image shows the service that you need to select:



	Service Name	Owner	Type
○	com.amazonaws.s3-global.accesspoint	amazon	Interface
○	com.amazonaws.[redacted]	amazon	Interface
●	com.amazonaws.[redacted]	amazon	Gateway

8. From the list, select the VPC where you want to create the endpoint.
9. Select the route table that you created for the VPC.
10. Select **Custom** or **Full access** policy based on your requirement, and paste the policy in the text box.
    For the minimal Amazon IAM policy, see the Amazon S3 V2 Connector guide.
11. Click **Create endpoint**.
    The gateway endpoint is created.
12. Go back to the **Endpoints** page to view the details of the gateway endpoint.
    The following image shows the gateway endpoint that you created:



search: vpc-[redacted]

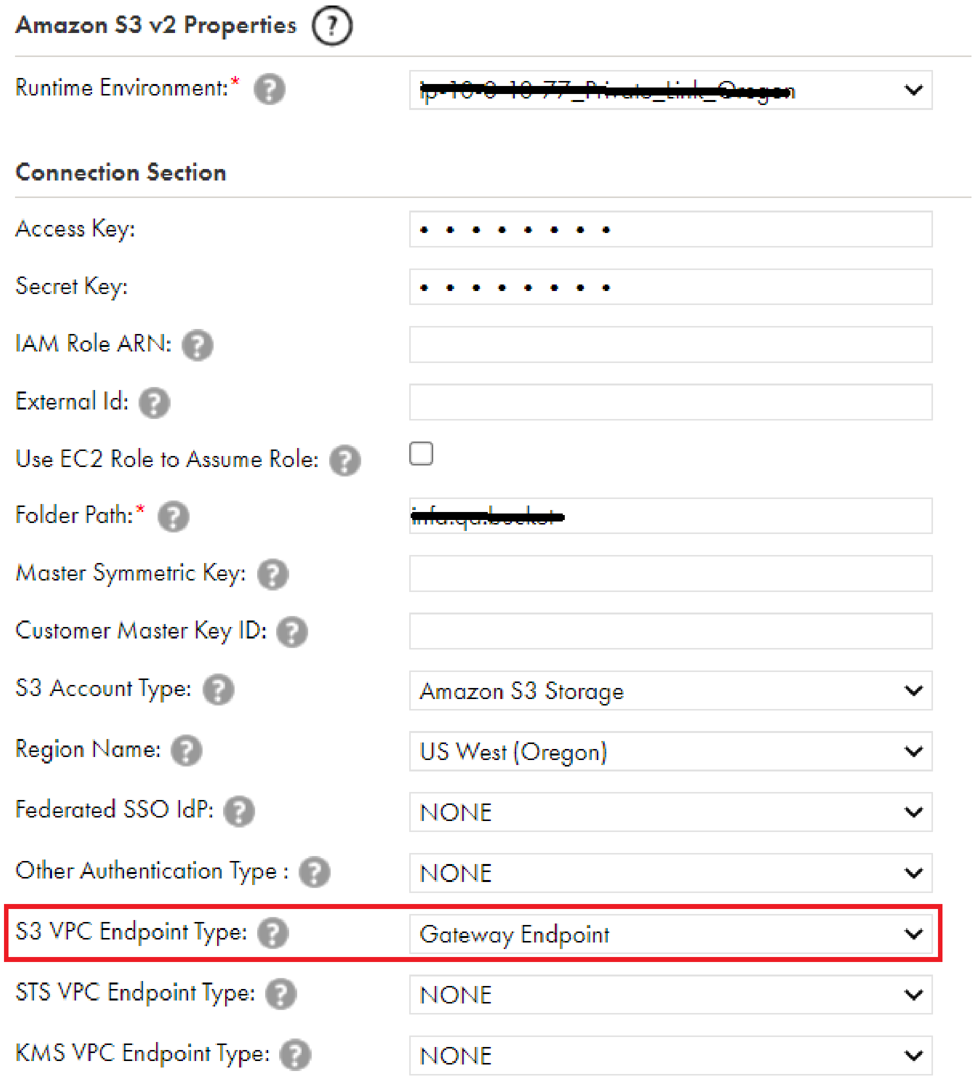
Name: S3_Gateway_Endpoint

□	Name	VPC endpoint ID	VPC ID	Service name	Endpoint t...	Status	Creation time
□	S3_Gateway_Endpoint	[redacted]	vpc-[redacted]	com.amazonaws.[redacted]	Gateway	Available	Thursday, May 2

Configure the gateway endpoint in the connection properties

Select the gateway endpoint connection property in Cloud Data Integration.

The following image shows the connection property that you configure in Amazon S3 V2 Connector for the gateway endpoint:



Amazon S3 v2 Properties

Runtime Environment:*	[redacted]

Connection Section

Access Key:	• • • • • • • •
Secret Key:	• • • • • • • •
IAM Role ARN:	
External Id:	
Use EC2 Role to Assume Role:	□
Folder Path:*	[redacted]
Master Symmetric Key:	
Customer Master Key ID:	
S3 Account Type:	Amazon S3 Storage
Region Name:	US West (Oregon)
Federated SSO IdP:	NONE
Other Authentication Type :	NONE
S3 VPC Endpoint Type:	Gateway Endpoint
STS VPC Endpoint Type:	NONE
KMS VPC Endpoint Type:	NONE

S3 interface endpoint

An interface endpoint is a network interface with a private IP address from the IP address range of your subnet. It serves as an entry point for traffic destined to an AWS service.

When you create an interface endpoint, additionally, you can configure an STS VPC endpoint or a KMS VPC endpoint based on your requirement.

Select the **IAM Role ARN** or **Federated SSO IdP** connection property to configure the STS VPC endpoint. Select the **Customer Master Key ID** connection property to configure the KMS VPC endpoint.

Configure the interface endpoint on the AWS console

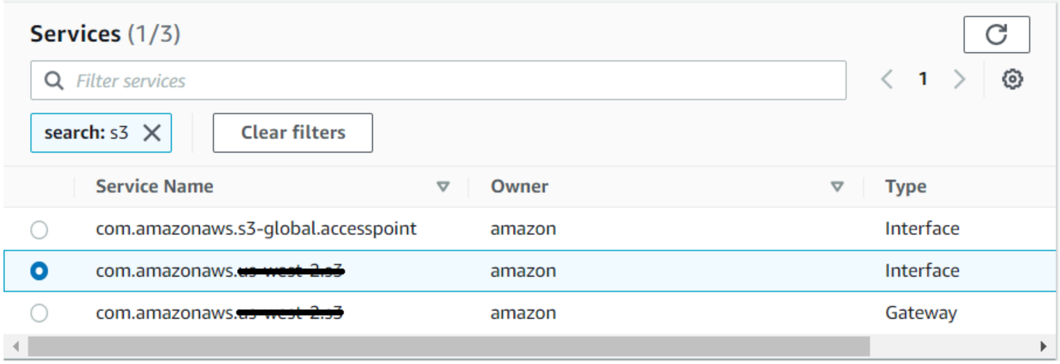
On the AWS console, select a service of the interface type, select the VPC, the private subnet, the security group, and add the policy for the interface endpoint.

Perform the following steps on the AWS console to configure an interface endpoint:

1. Log in to the **AWS Console**, and navigate to the region where you want to create endpoints.

2. On the **Search** tab, search for VPC.
   The VPC dashboard appears.
3. Click **Endpoints**.
4. Click **Create endpoint**.
   The **Create endpoint page** appears.
5. Enter a name for the S3 interface endpoint.
6. Select **AWS services** as the service category.
7. In **Services**, search for S3, and select a service of the interface type.
   To configure the STS VPC endpoint, search for the STS service. To configure the KMS VPC endpoint, search for the KMS service.

   The following image shows the S3 service:



Services (1/3)

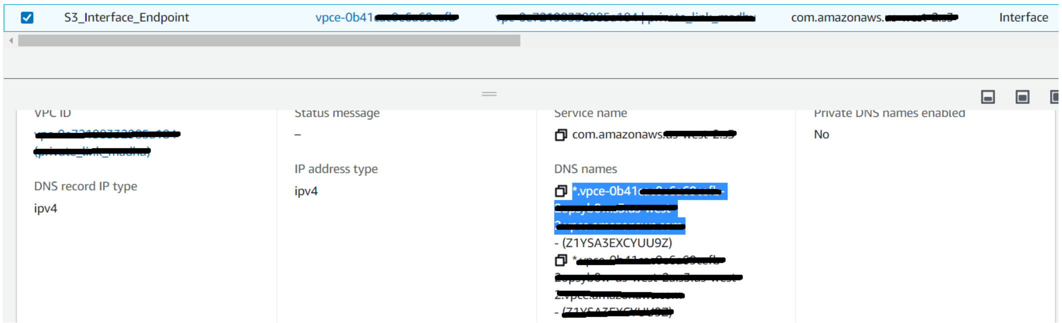
	Service Name	Owner	Type
○	com.amazonaws.s3-global.accesspoint	amazon	Interface
●	com.amazonaws.[redacted]	amazon	Interface
○	com.amazonaws.[redacted]	amazon	Gateway

8. From the list, select the VPC where you want to create the endpoint.
9. Click **Additional settings**, and clear the **Enable DNS name** check box.
10. Select the private subnet that you created.
11. Select the security group.
12. Select **Custom** or **Full access** policy based on your requirement, and paste the policy in the text box.
    For the minimal Amazon IAM policy, see the Amazon S3 V2 Connector guide.
13. Click **Create endpoint**.
    The interface endpoint is created.
14. Go back to the **Endpoints** page to view the details of the interface endpoint.

15. Copy the DNS name of the interface endpoint.
You need to enter the DNS name in the **Endpoint DNS Name for Amazon S3** connection property in Cloud Data Integration in the following format:

```
bucket.<DNS name of the interface endpoint>
```

The following image shows the DNS name of the interface endpoint:



☑ S3_Interface_Endpoint | vpce-0b41[redacted] | [redacted] | com.amazonaws.[redacted] | Interface

VPC ID
[redacted]

DNS record IP type
ipv4

Status message
–

IP address type
ipv4

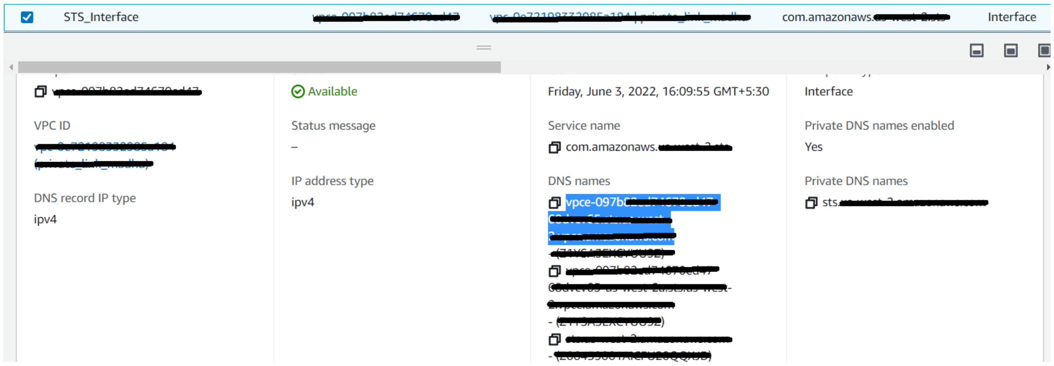
Service name
com.amazonaws[redacted]

DNS names
*.vpce-0b41[redacted]
- (Z1YSA3EXCYUU9Z)
*[redacted]

Private DNS names enabled
No

If you configure the STS VPC interface endpoint, you need to enter the DNS name in the **Endpoint DNS Name for AWS STS service** connection property in Cloud Data Integration.

The following image shows the DNS name of the STS VPC interface endpoint:



☑ STS_Interface | [redacted] | [redacted] | com.amazonaws.[redacted] | Interface

[redacted]

VPC ID
[redacted]

DNS record IP type
ipv4

✓ Available

Status message
–

IP address type
ipv4

Friday, June 3, 2022, 16:09:55 GMT+5:30

Service name
com.amazonaws.[redacted]

DNS names
vpce-097b[redacted]
[redacted]

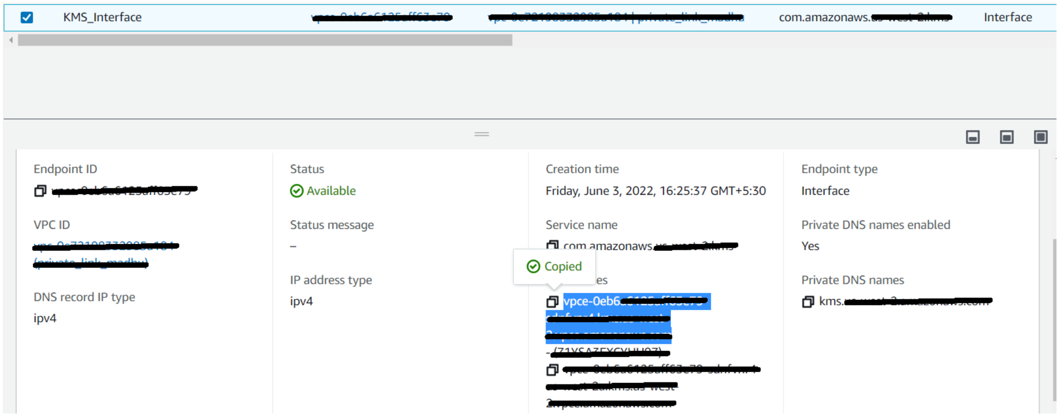
Interface

Private DNS names enabled
Yes

Private DNS names
sts.[redacted]

If you configure the KMS VPC interface endpoint, you need to enter the DNS name in the **Endpoint DNS Name for AWS KMS service** connection property in Cloud Data Integration.

The following image shows the DNS name of the KMS VPC interface endpoint:



☑ KMS_Interface | [redacted] | [redacted] | com.amazonaws.[redacted] | Interface

Endpoint ID
[redacted]

VPC ID
[redacted]

DNS record IP type
ipv4

Status
✓ Available

Status message
–

IP address type
ipv4

Creation time
Friday, June 3, 2022, 16:25:37 GMT+5:30

Service name
com.amazonaws.[redacted]

✓ Copied

DNS names
vpce-0eb6[redacted]
[redacted]

Endpoint type
Interface

Private DNS names enabled
Yes

Private DNS names
kms.[redacted]

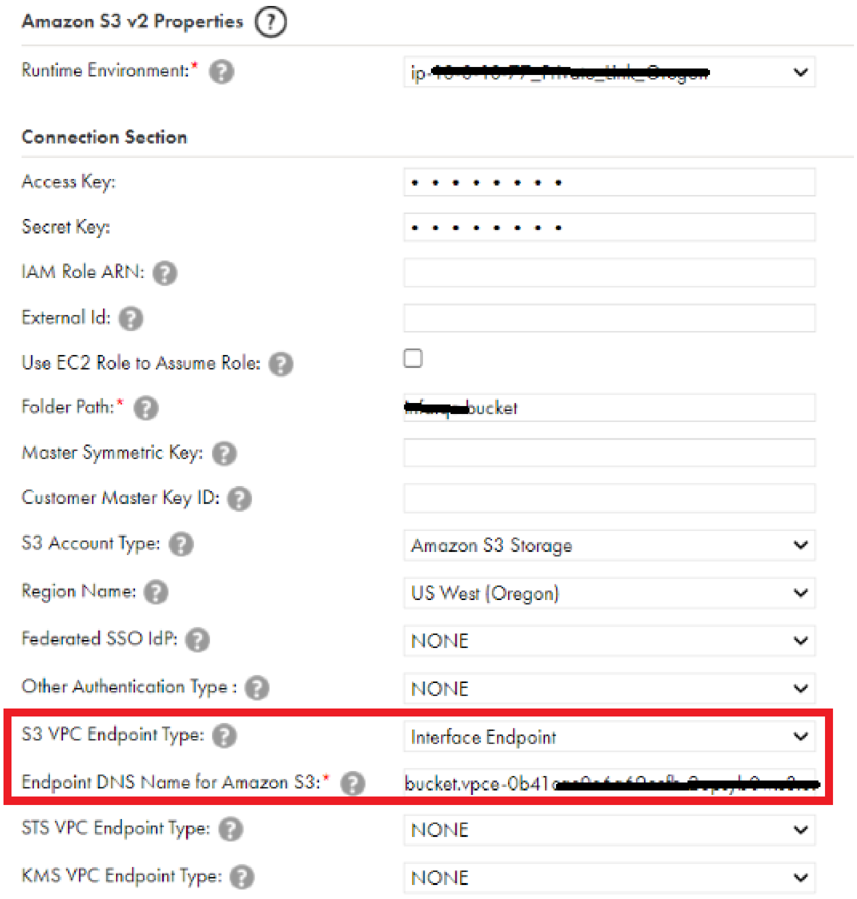
Configure the interface endpoint in the connection properties

Select the interface endpoint connection property and enter the endpoint DNS name for the interface endpoint in Cloud Data Integration.

Enter the endpoint DNS name for Amazon S3 in the following format:

```
bucket.<DNS name of the interface endpoint>
```

The following image shows the Amazon S3 V2 connection property that you configure for the interface endpoint in Cloud Data Integration:



Amazon S3 v2 Properties

Runtime Environment:*	ip-[redacted]

Connection Section

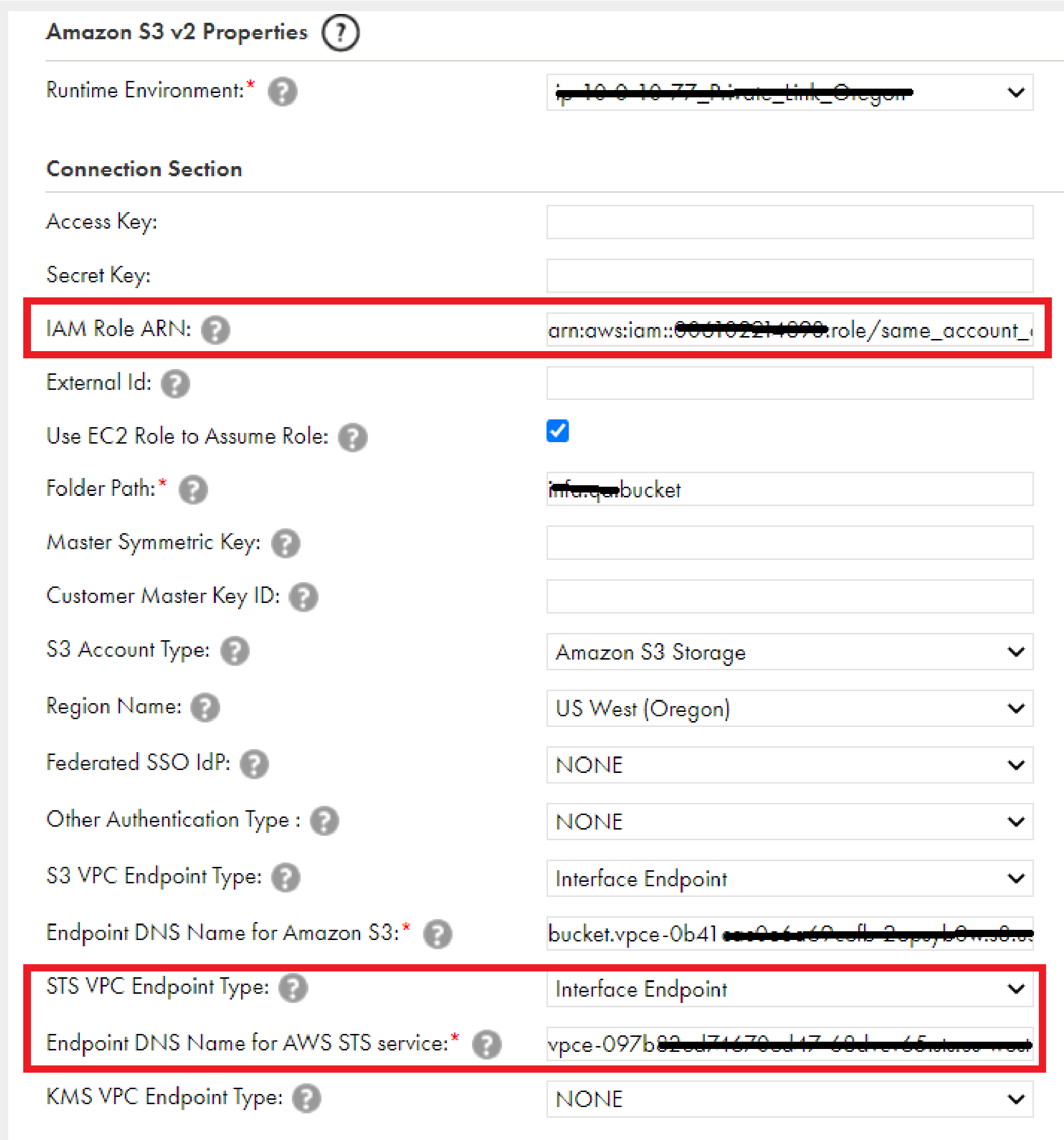
Access Key:	• • • • • • • • •
Secret Key:	• • • • • • • • •
IAM Role ARN:	
External Id:	
Use EC2 Role to Assume Role:	☐
Folder Path:*	[redacted]bucket
Master Symmetric Key:	
Customer Master Key ID:	
S3 Account Type:	Amazon S3 Storage
Region Name:	US West (Oregon)
Federated SSO IdP:	NONE
Other Authentication Type :	NONE
S3 VPC Endpoint Type:	Interface Endpoint
Endpoint DNS Name for Amazon S3:*	bucket.vpce-0b41[redacted]
STS VPC Endpoint Type:	NONE
KMS VPC Endpoint Type:	NONE

Configure the STS VPC interface endpoint in the connection properties

After you select the S3 interface endpoint connection property and enter the DNS name of the S3 interface endpoint, you can additionally configure the STS VPC interface endpoint.

When you select the **IAM Role ARN** or **Federated SSO IdP** connection property, select the STS VPC interface endpoint and enter the endpoint DNS name for the STS VPC interface endpoint in Cloud Data Integration.

The following image shows the Amazon S3 V2 connection property that you configure for the STS VPC interface endpoint in Cloud Data Integration:



Amazon S3 v2 Properties

Runtime Environment:*	[redacted]

Connection Section

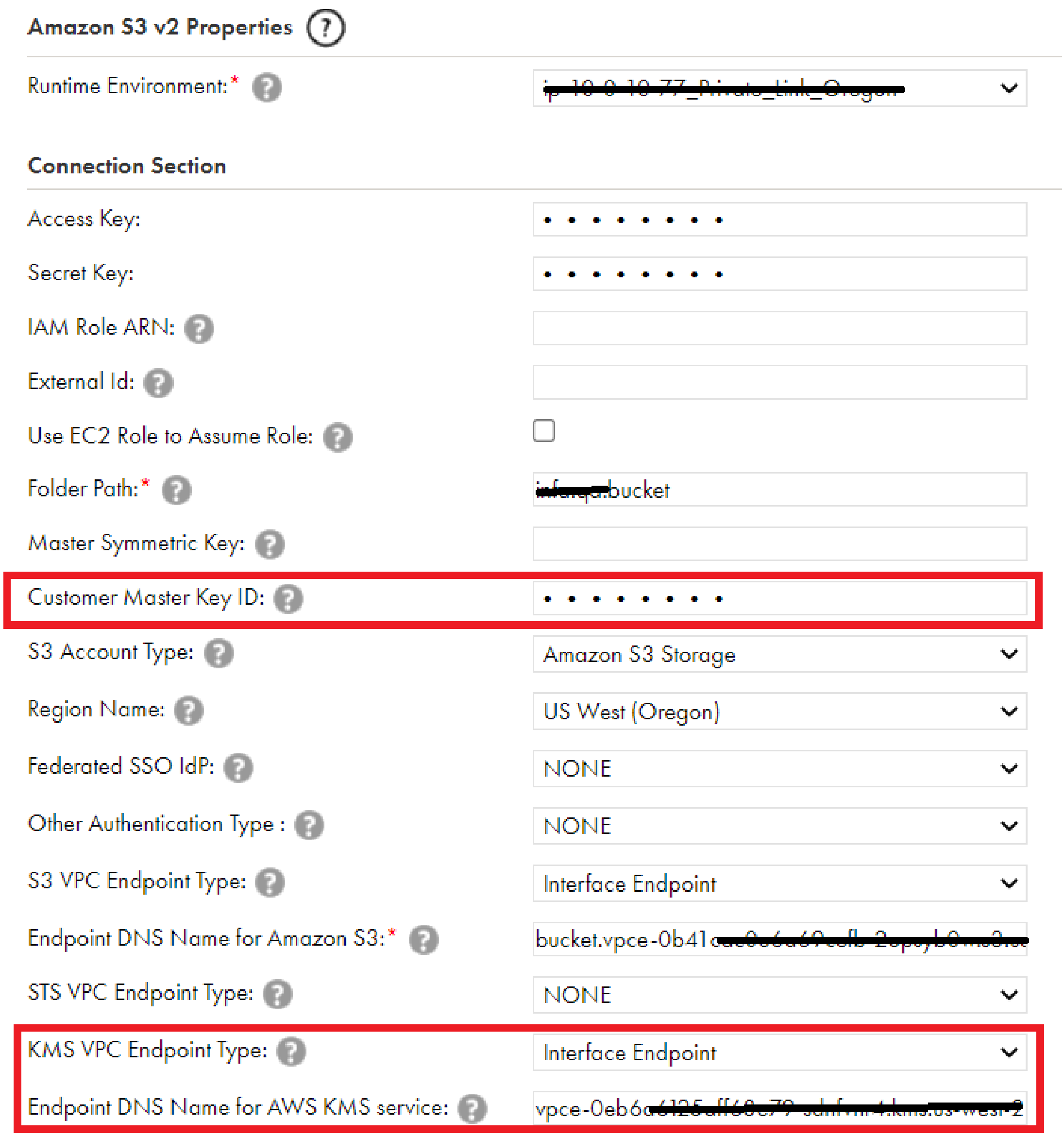
Access Key:	
Secret Key:	
IAM Role ARN:	arn:aws:iam::[redacted]:role/same_account_
External Id:	
Use EC2 Role to Assume Role:	☑
Folder Path:*	[redacted]bucket
Master Symmetric Key:	
Customer Master Key ID:	
S3 Account Type:	Amazon S3 Storage
Region Name:	US West (Oregon)
Federated SSO IdP:	NONE
Other Authentication Type :	NONE
S3 VPC Endpoint Type:	Interface Endpoint
Endpoint DNS Name for Amazon S3:*	bucket.vpce-0b41[redacted]
STS VPC Endpoint Type:	Interface Endpoint
Endpoint DNS Name for AWS STS service:*	vpce-097b[redacted]
KMS VPC Endpoint Type:	NONE

Configure the KMS VPC interface endpoint in the connection properties

After you select the S3 interface endpoint connection property and enter the DNS name of the S3 interface endpoint, you can additionally configure the KMS VPC interface endpoint.

When you enter the **Customer Master Key ID** connection property, select the KMS VPC interface endpoint and enter the endpoint DNS name for the KMS VPC interface endpoint in Cloud Data Integration.

The following image shows the Amazon S3 V2 connection property that you configure for the KMS VPC interface endpoint in Cloud Data Integration:



Amazon S3 v2 Properties

Runtime Environment:*	[redacted]

Connection Section

Access Key:	••••••••
Secret Key:	••••••••
IAM Role ARN:	
External Id:	
Use EC2 Role to Assume Role:	☐
Folder Path:*	[redacted]bucket
Master Symmetric Key:	
Customer Master Key ID:	••••••••
S3 Account Type:	Amazon S3 Storage
Region Name:	US West (Oregon)
Federated SSO IdP:	NONE
Other Authentication Type :	NONE
S3 VPC Endpoint Type:	Interface Endpoint
Endpoint DNS Name for Amazon S3:*	bucket.vpce-0b41[redacted]
STS VPC Endpoint Type:	NONE
KMS VPC Endpoint Type:	Interface Endpoint
Endpoint DNS Name for AWS KMS service:	vpce-0eb6[redacted]

Authors

Wilson Fernandes

Sakshi Bansal