How-To Library

Informatica

Using an assume role for Amazon S3 resources in Informatica Cloud Data Integration

Abstract

You can assume an IAM (Identity and Access Management) role in Amazon S3 resources to generate temporary security credentials. The temporary security credentials give you limited access to Amazon resources for a certain period. You can use the IAM role in Amazon Redshift V2 Connector and Amazon S3 V2 Connector to access Amazon S3 resources. This article describes how an IAM user can use an assume role to temporarily gain access to the Amazon S3 resources.

Supported Versions

- Informatica® Cloud Data Integration Amazon S3 V2 and Amazon Redshift Connectors

Table of Contents

Overview

You can use a permanent access key and secret key to access the Amazon S3 resources. Anyone with the keys can access sensitive information from the AWS resources. When you use an assume role, it allows existing Identity and Access Management (IAM) users to access the Amazon S3 resources for a limited period, helping you to securely control access to these resources.

You can use the assume role in Amazon S3 V2 Connector to access Amazon S3 resources. In Amazon Redshift V2 Connector, you can use the assume role to access the Amazon S3 staging bucket to stage the Amazon Redshift data before writing to Amazon Redshift.

You can use IAM roles to delegate access to IAM users managed within your account. IAM users under a different AWS account, IAM users under a different AWS account and using an External ID for enhanced security, or for an EC2 role to access an AWS service such as EC2.

Advantages of an assume role

You can assume an IAM user role and request temporary security credentials to access the Amazon S3 resources.

An assume role offers the following advantages:

Temporary credentials

> You can use an assume role and generate temporary security credentials to access the Amazon S3 resources.

Enhanced security

> You can access Amazon S3 resources by using temporary session credentials. You can request the temporary credentials from the AWS Security Token Service (STS). The process of fetching temporary credentials is secure and transparent.

User Configurations

> You have the option to specify an appropriate session time for the credentials in the Amazon S3 and Amazon Redshift connectors. AWS STS returns the temporary credentials with a default session time. The credentials expire after crossing the time limit.

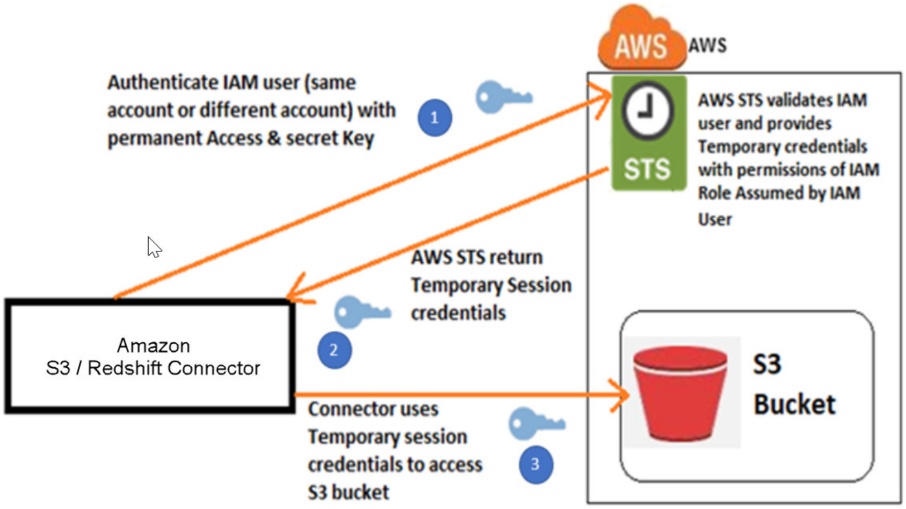
Configure the assume role in the connector

You can gain access to Amazon S3 resources by using an assume role in Amazon S3 and Amazon Redshift connectors.

You can use Amazon S3 and Amazon Redshift connectors to access the Amazon resources by using temporary security credentials generated for an IAM user using an assume role.

Accessing AWS using the connector

The connector uses the following process to interact with the AWS Security Token Service (STS) to generate temporary session credentials by using an assume role:


AWS
AWS
Authenticate IAM user (same account or different account) with permanent Access & secret Key
1
STS
AWS STS validates IAM user and provides Temporary credentials with permissions of IAM Role Assumed by IAM User
AWS STS return Temporary Session credentials
2
Amazon S3 / Redshift Connector
S3 Bucket
Connector uses Temporary session credentials to access S3 bucket
3

1. The connector establishes a connection with the AWS Security Token Service (STS) using the permanent access key and secret key from Cloud Data Integration. These keys have limited permission to create the IAM roles.
2. AWS Security Token Service (STS) validates the IAM user and provides the temporary credentials with permissions of the IAM role assumed by an IAM user. The AWS STS API response to the connector includes the temporary security credentials.
3. The connector uses the temporary security credentials to call the Amazon API operations and gains access to Amazon S3 resources.

Connection properties

To use an assume role, you need to configure certain properties in the Amazon S3 and Amazon Redshift connections.

The connection properties that you configure depend on whether you delegate access to IAM users managed within your account, IAM users under a different AWS account, or an AWS service such as EC2.

For more information about creating an Amazon S3 V2 connection, see Amazon S3 V2 connection properties.

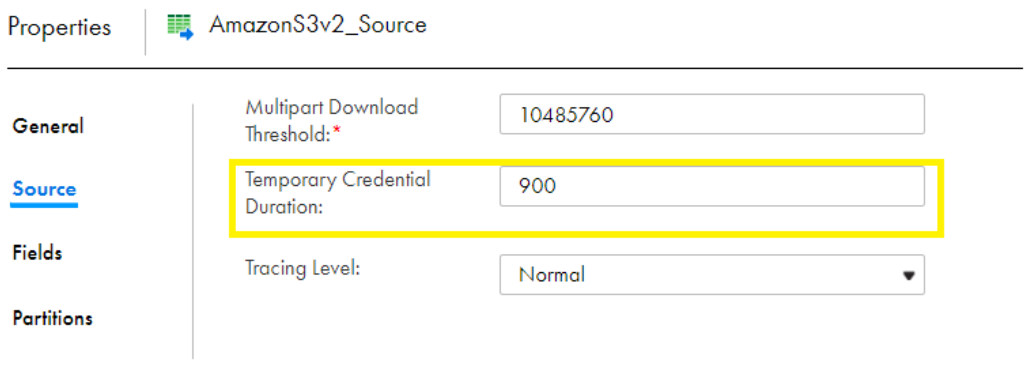
For more information about creating an Amazon Redshift V2 connection, see Amazon Redshift V2 connection properties.

Advanced source and target properties

You need to set the time duration during which an IAM user can use the dynamically generated temporary credentials to access the AWS resource. Enter the temporary credentials duration in seconds in the advanced source and target properties for the Amazon S3 and Amazon Redshift connectors in a mapping. The default is 900 seconds.

If you require more than 900 seconds, you can set the time duration to a maximum of 12 hours in the AWS console and then enter the same time duration in this property.

The following image shows an example of the configured **temporary credential duration** in the source properties in an Amazon S3 connection:



Multipart Download Threshold:* 10485760

Temporary Credential Duration: 900

Tracing Level: Normal

For more information about the advanced properties, see Amazon Redshift V2 advanced properties and Amazon S3 V2 advanced properties.

Assume role support for Amazon Web Services

You can use an assume role for existing Identity and Access Management (IAM) users to access AWS resources that they don't already have access to or to access resources in another AWS account. To configure an assume IAM role and enable the same account or cross-account API access, you need to establish a trust relationship between the two accounts.

You can use the following process to establish a trust relationship between an existing IAM user account and other AWS accounts:

1. Create a trusting entity. A trusting entity is an account that owns the Amazon S3 bucket and has an IAM Role to be assumed.
2. Create a trusted entity. A trusted entity is an account where the IAM user is managed.
3. Use the AWS Security Token Services (STS) to generate the temporary session credentials through assume role.

AWS Security Token Services

AWS Security Token Services (STS) enables you to request session tokens from the global STS endpoint which works in all AWS regions. You can use the AWS Identity and Access Management (IAM) roles and configure the global STS endpoint to generate session tokens that are compatible with all AWS regions.

The following specifications make the temporary security credentials different from the long-term access key credentials used by the IAM users:

- Temporary security credentials are short-term credentials. You cannot use them after the credentials expire.
- Temporary security credentials are generated dynamically on request and you cannot store the temporary security credentials. You can request for new temporary credentials before or after the session expires.
- By default, the temporary security credentials last for an hour. However, you can use the optional **DurationSeconds** parameter to specify the duration of your session. You can enter a value from 900 seconds (15 minutes) to the maximum session duration setting for a role. You can enter a value from 1 hour to 12 hours.

Case 1. IAM user and IAM role are in the same account

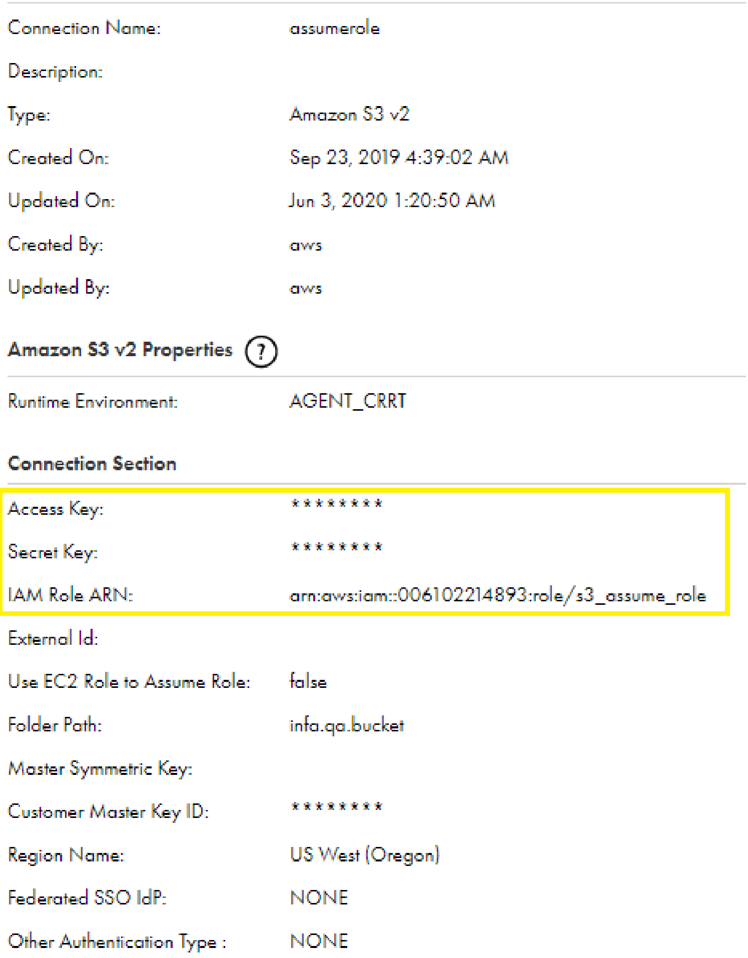
You can configure an assume role for an IAM user when the IAM user and the IAM role are in the same account. The IAM user has permission only to assume the role.

You must configure Cloud Data Integration and AWS to use the assume role.

Configure the connection properties in Cloud Data Integration

Specify the access key, secret key, and the IAM Role ARN in the connection properties in Cloud Data Integration.

The following image shows the properties that you configure for an assume role with an IAM user in the Amazon S3 V2 connection:



Connection Name:	assumerole
Description:	
Type:	Amazon S3 v2
Created On:	Sep 23, 2019 4:39:02 AM
Updated On:	Jun 3, 2020 1:20:50 AM
Created By:	aws
Updated By:	aws

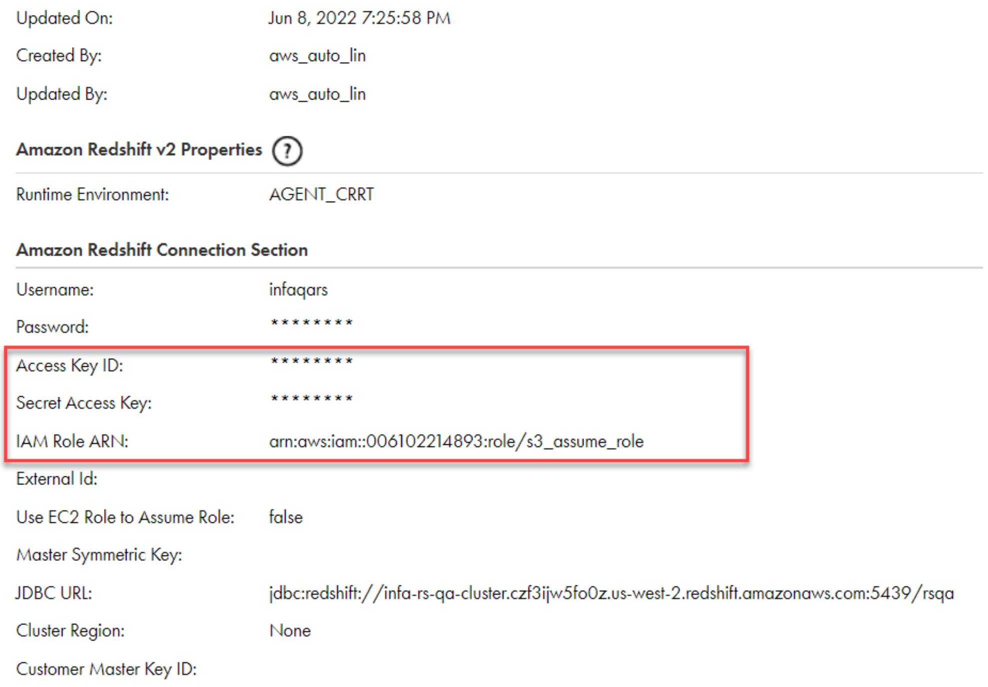
Amazon S3 v2 Properties

Runtime Environment:	AGENT_CRRT

Connection Section

Access Key:	********
Secret Key:	********
IAM Role ARN:	arn:aws:iam::006102214893:role/s3_assume_role
External Id:	
Use EC2 Role to Assume Role:	false
Folder Path:	infa.qa.bucket
Master Symmetric Key:	
Customer Master Key ID:	********
Region Name:	US West (Oregon)
Federated SSO IdP:	NONE
Other Authentication Type :	NONE

The following image shows the properties that you configure for an assume role with an IAM user in the Amazon Redshift V2 connection:



Updated On: Jun 8, 2022 7:25:58 PM

Created By: aws_auto_lin

Updated By: aws_auto_lin

Amazon Redshift v2 Properties

Runtime Environment: AGENT_CRRT

Amazon Redshift Connection Section

Username: infaqars

Password: ********

Access Key ID: ********

Secret Access Key: ********

IAM Role ARN: arn:aws:iam::006102214893:role/s3_assume_role

External Id:

Use EC2 Role to Assume Role: false

Master Symmetric Key:

JDBC URL: jdbc:redshift://infa-rs-qa-cluster.czf3ijw5fo0z.us-west-2.redshift.amazonaws.com:5439/rsqa

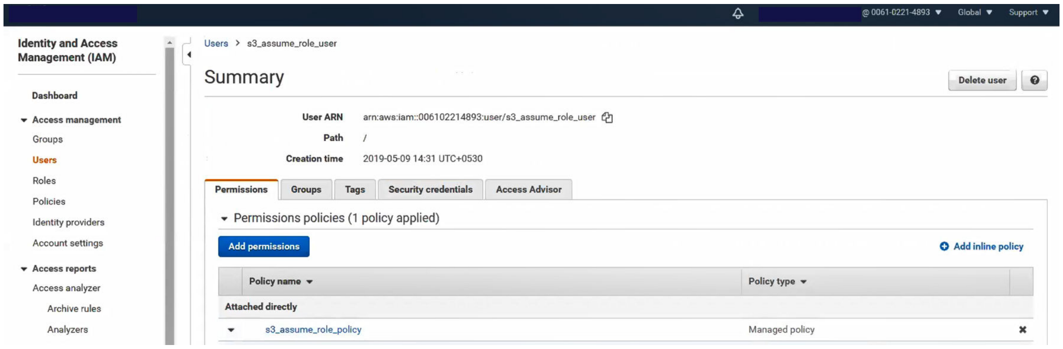
Cluster Region: None

Customer Master Key ID:

Configure assume role on the AWS console

Perform the following steps on the AWS console to configure assume role when the IAM user and the IAM role are in the same account:

1. Log in to the **AWS Console**.
2. Click **Dashboard** from the left panel.
   The **AWS Service** dashboard page appears.
3. Click **IAM**.
   The **Welcome to Identity and Access Management** page appears.
4. Click **Users** from the left panel.
   Create an IAM user and attach a policy to the IAM user.



[redacted] [redacted] @ 0061-0221-4893

Users > s3_assume_role_user

Summary

User ARN: arn:aws:iam::006102214893:user/s3_assume_role_user

Path: /

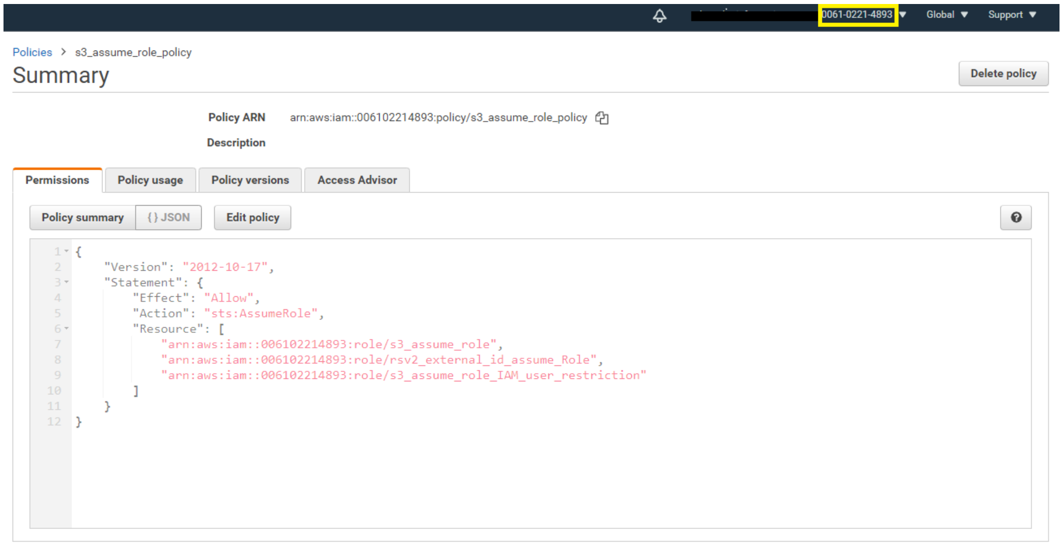
Creation time: 2019-05-09 14:31 UTC+0530

Permissions policies (1 policy applied)

Policy name	Policy type
Attached directly	
s3_assume_role_policy	Managed policy

5. Click **Policies** from the left panel.
   The **Policies** page appears.

The following image shows a sample policy attached to the IAM user in account 0061-0221-4893 (account A):



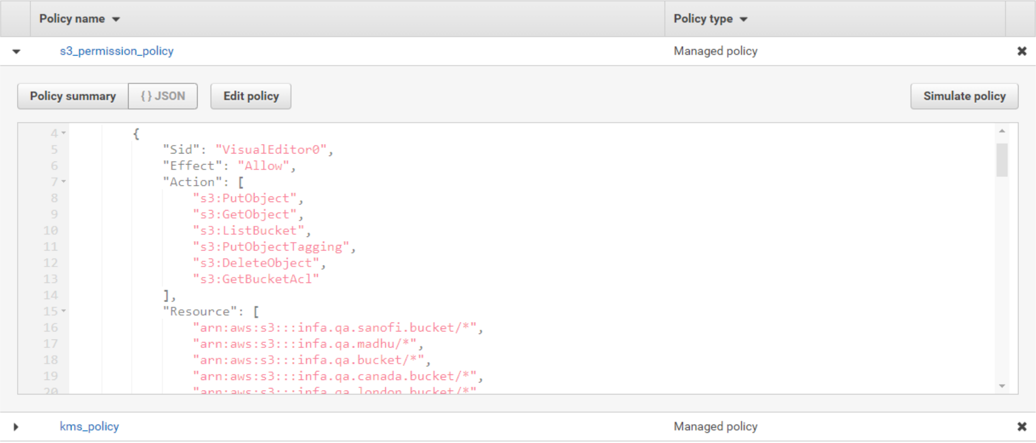
Summary

Policy ARN arn:aws:iam::006102214893:policy/s3_assume_role_policy

Description

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": [
            "arn:aws:iam::006102214893:role/s3_assume_role",
            "arn:aws:iam::006102214893:role/rsv2_external_id_assume_Role",
            "arn:aws:iam::006102214893:role/s3_assume_role_IAM_user_restriction"
        ]
    }
}
```

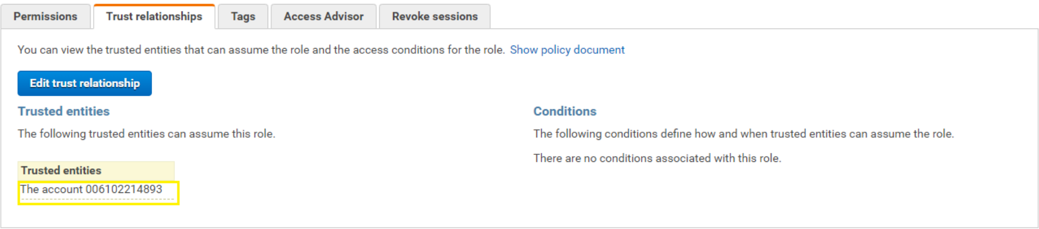
6. Click **Roles** from the left panel.
   The following image shows the policies attached to the IAM role:



Policy name ▼	Policy type ▼
s3_permission_policy	Managed policy
kms_policy	Managed policy

```
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:PutObjectTagging",
                "s3:DeleteObject",
                "s3:GetBucketAcl"
            ],
            "Resource": [
                "arn:aws:s3:::infa.qa.sanofi.bucket/*",
                "arn:aws:s3:::infa.qa.madhu/*",
                "arn:aws:s3:::infa.qa.bucket/*",
                "arn:aws:s3:::infa.qa.canada.bucket/*",
                "arn:aws:s3:::infa.qa.london.bucket/*"
```

7. Click **Trust relationships** tab to define the trust relationship within the AWS account.
   The following image shows that the user in account A is trusted to assume the role that you defined:



You can view the trusted entities that can assume the role and the access conditions for the role. Show policy document

Trusted entities

The following trusted entities can assume this role.

Trusted entities
The account 006102214893

Conditions

The following conditions define how and when trusted entities can assume the role.

There are no conditions associated with this role.

Case 2. IAM user and IAM role are in different accounts

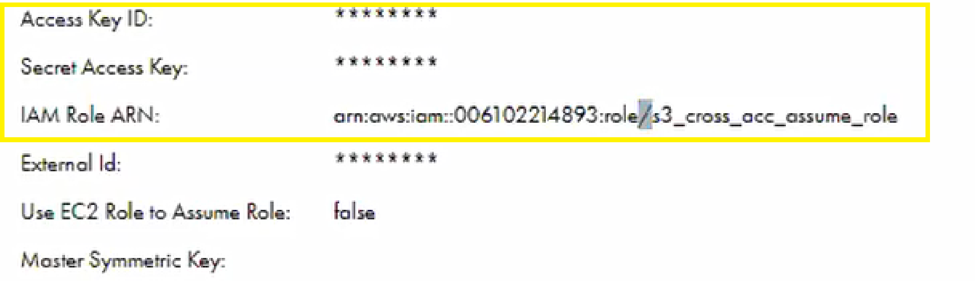
You can configure assume role for an IAM user when the IAM user and the IAM role are in different accounts.

You must configure Cloud Data Integration and AWS to use the assume role.

Configure the connection properties in Cloud Data Integration

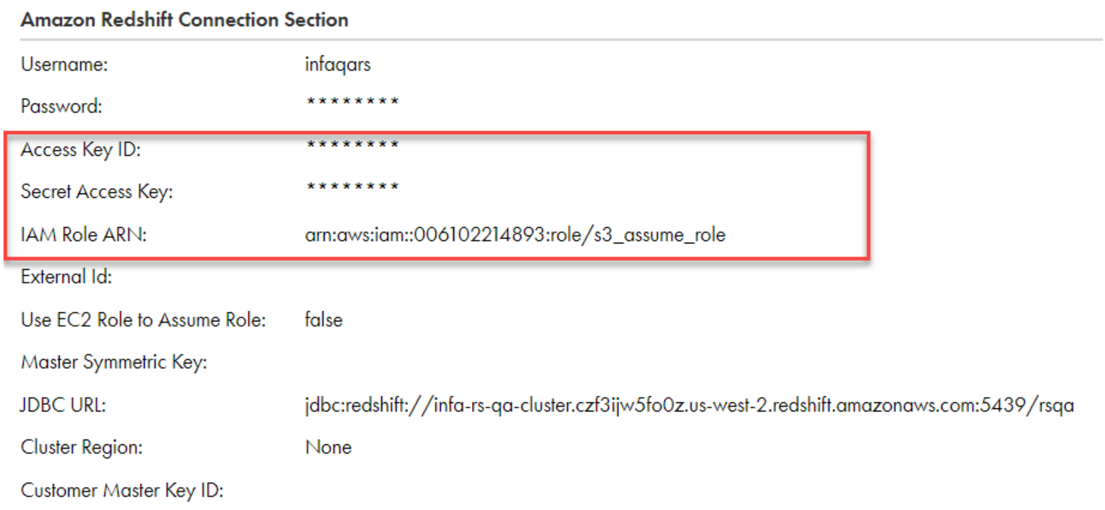
Specify the access key, secret key, and the IAM Role ARN in the connection properties in Cloud Data Integration.

The following image shows the properties that you configure for an IAM user and IAM role in the Amazon S3 V2 connection:



Access Key ID:	********
Secret Access Key:	********
IAM Role ARN:	arn:aws:iam::006102214893:role/s3_cross_acc_assume_role
External Id:	********
Use EC2 Role to Assume Role:	false
Master Symmetric Key:	

The following image shows the properties that you configure for an IAM user and IAM role in the Amazon Redshift V2 connection:



Amazon Redshift Connection Section

Username:	infaqars
Password:	********
Access Key ID:	********
Secret Access Key:	********
IAM Role ARN:	arn:aws:iam::006102214893:role/s3_assume_role
External Id:	
Use EC2 Role to Assume Role:	false
Master Symmetric Key:	
JDBC URL:	jdbc:redshift://infa-rs-qa-cluster.czf3ijw5fo0z.us-west-2.redshift.amazonaws.com:5439/rsqa
Cluster Region:	None
Customer Master Key ID:	

Configure assume role on the AWS console

A user in account `3755-6920-9379` (account A) can assume a role in account `0061-0221-4893` (account B) to access specific resources of account B.

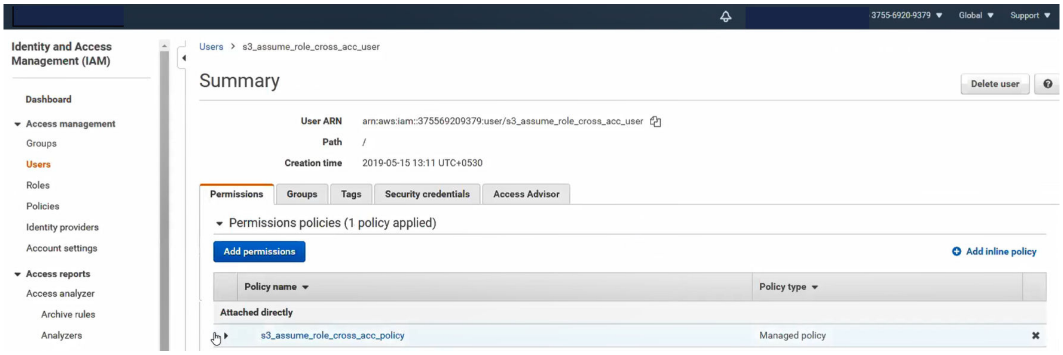
Perform the following steps on the AWS console to configure assume role when the IAM user and the IAM role are in different accounts:

1. Log in to the **AWS Console**.

2. Click **Dashboard** from the left panel.
   The **AWS Service** dashboard page appears.

3. Click **IAM**.
   The **Welcome to Identity and Access Management** page appears.

4. Click **Users** from the left panel.
   Create an IAM user and attach a policy to the IAM user.



[redacted] [redacted] 3755-6920-9379 ▼ Global ▼ Support ▼

Identity and Access Management (IAM)

- Dashboard
- ▾ Access management
  - Groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
- ▾ Access reports
  - Access analyzer
    - Archive rules
    - Analyzers

Users > s3_assume_role_cross_acc_user

Summary

Delete user

User ARN	arn:aws:iam::375569209379:user/s3_assume_role_cross_acc_user
Path	/
Creation time	2019-05-15 13:11 UTC+0530

Permissions | Groups | Tags | Security credentials | Access Advisor

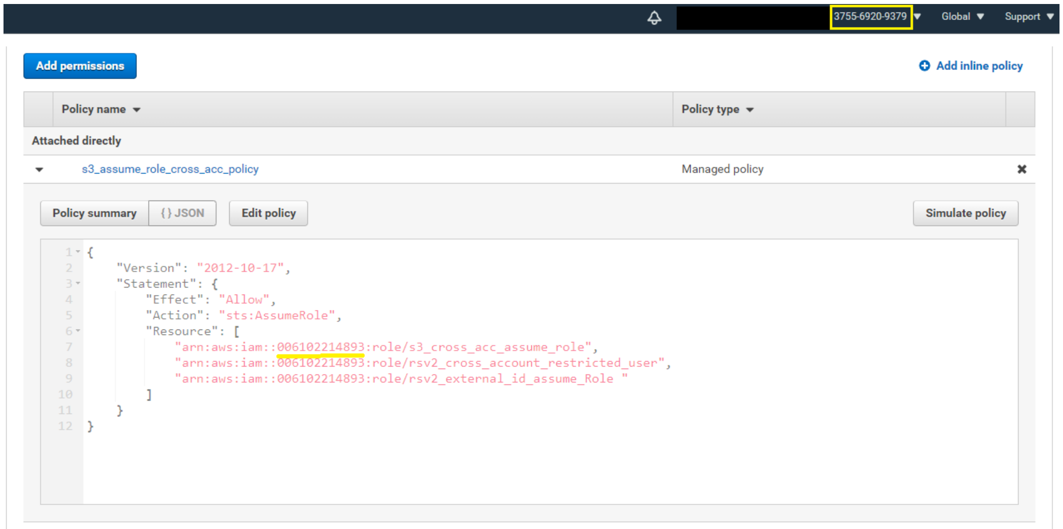
▾ Permissions policies (1 policy applied)

Add permissions | Add inline policy

Policy name	Policy type
Attached directly	
s3_assume_role_cross_acc_policy	Managed policy

5. Click **Policies** from the left panel.
   The **Policies** page appears.

   The following image shows a sample policy attached to the IAM user in account A:



[redacted] 3755-6920-9379 ▼ Global ▼ Support ▼

Add permissions | Add inline policy

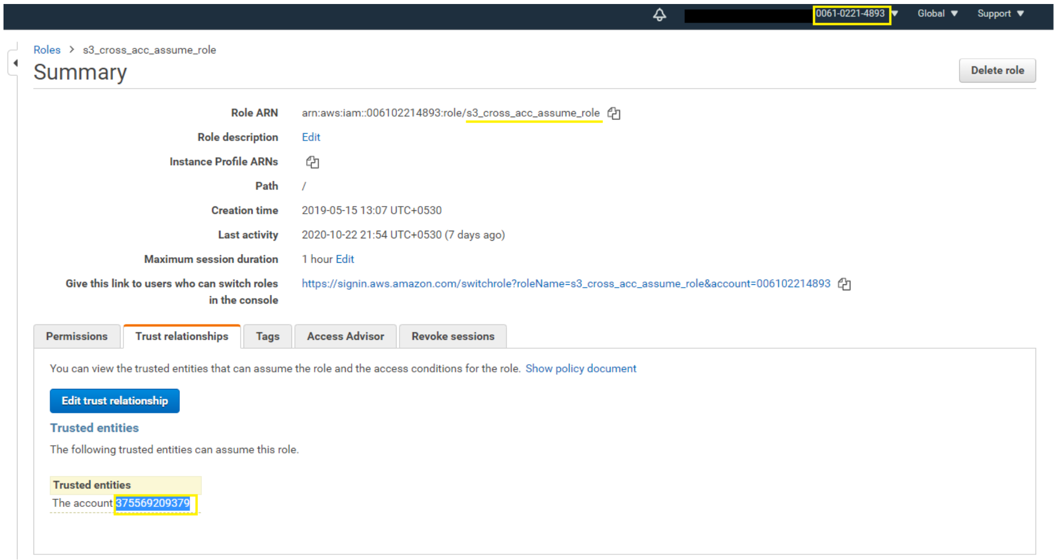
Policy name	Policy type
Attached directly	
s3_assume_role_cross_acc_policy	Managed policy

Policy summary | { } JSON | Edit policy | Simulate policy

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": [
            "arn:aws:iam::006102214893:role/s3_cross_acc_assume_role",
            "arn:aws:iam::006102214893:role/rsv2_cross_account_restricted_user",
            "arn:aws:iam::006102214893:role/rsv2_external_id_assume_Role "
        ]
    }
}
```

6. Define an IAM role in account B. Click **Roles** from the left panel.
   Configure the policies for the IAM role that you configured when the IAM user and the IAM role were in the same account.

7. Click **Trust relationships** tab to define the trust relationship within the AWS account.
   The following image shows that a user from account A is trusted to assume the role that you defined in account B:



Summary

Role ARN	arn:aws:iam::006102214893:role/s3_cross_acc_assume_role
Role description	Edit
Instance Profile ARNs	
Path	/
Creation time	2019-05-15 13:07 UTC+0530
Last activity	2020-10-22 21:54 UTC+0530 (7 days ago)
Maximum session duration	1 hour Edit
Give this link to users who can switch roles in the console	https://signin.aws.amazon.com/switchrole?roleName=s3_cross_acc_assume_role&account=006102214893

You can view the trusted entities that can assume the role and the access conditions for the role. Show policy document

Trusted entities

The following trusted entities can assume this role.

Trusted entities
The account 375569209379

Case 3. External ID for cross-account access

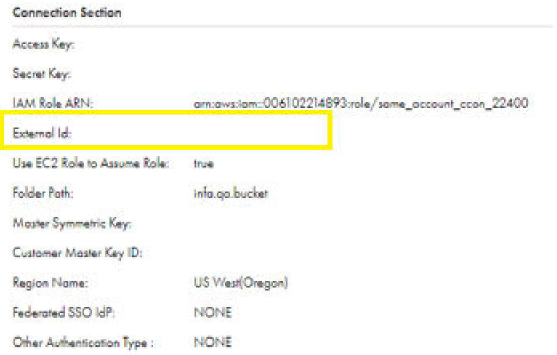
You can specify the external ID for a secure cross-account access to the Amazon connector bucket when the Amazon connector bucket is in a different AWS account.

You must configure Cloud Data Integration and AWS to use the assume role.

Configure the connection properties in Cloud Data Integration

Specify the IAM role ARN and the external ID in the connection properties in Cloud Data Integration.

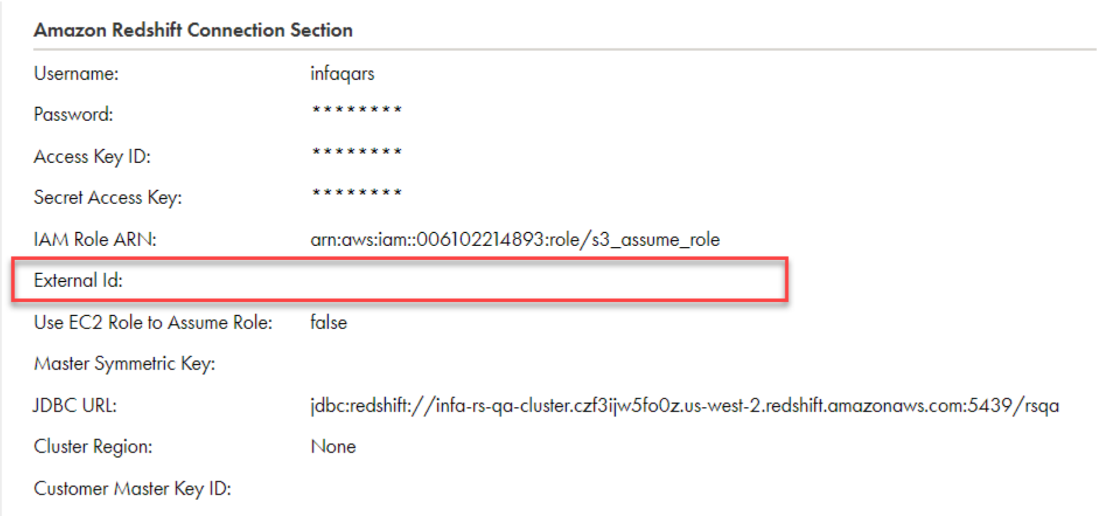
The following image shows the shows the configured IAM role ARN and external ID in an Amazon S3 V2 connection:



Connection Section

Access Key:	
Secret Key:	
IAM Role ARN:	arn:aws:iam::006102214893:role/same_account_ccon_22400
External Id:	
Use EC2 Role to Assume Role:	true
Folder Path:	info.qa.bucket
Master Symmetric Key:	
Customer Master Key ID:	
Region Name:	US West(Oregon)
Federated SSO IdP:	NONE
Other Authentication Type :	NONE

The following image shows the properties that you need to configure in an Amazon Redshift V2 connection:



Amazon Redshift Connection Section

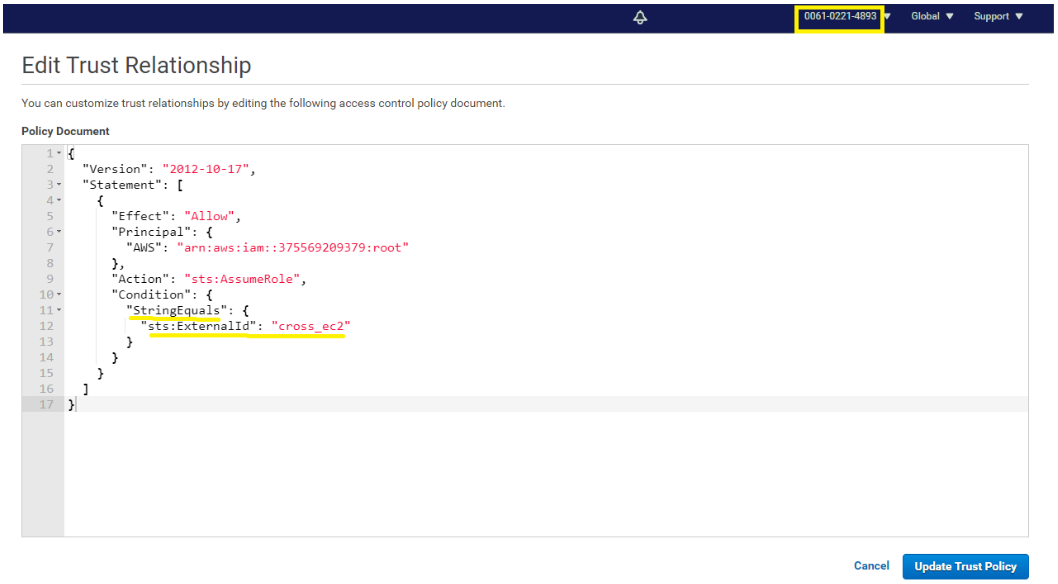
Username:	infaqars
Password:	********
Access Key ID:	********
Secret Access Key:	********
IAM Role ARN:	arn:aws:iam::006102214893:role/s3_assume_role
External Id:	
Use EC2 Role to Assume Role:	false
Master Symmetric Key:	
JDBC URL:	jdbc:redshift://infa-rs-qa-cluster.czf3ijw5fo0z.us-west-2.redshift.amazonaws.com:5439/rsqa
Cluster Region:	None
Customer Master Key ID:	

Configure assume role on the AWS console

When an IAM user from account A tries to assume a role in account B, the IAM user needs to specify an external ID to be authenticated to assume this role even though you have defined the rules and policies for the IAM user and IAM role.

Perform the following steps on the AWS console to configure the assume role:

1. Log in to the **AWS Console**.
2. Click **Dashboard** from the left panel.
   The **AWS Service** dashboard page appears.
3. Click **IAM**.
   The **Welcome to Identity and Access Management** page appears.
4. Click **Policies** from the left panel.
   Configure the policies for the IAM user that you configure when the IAM user and the IAM role are in different accounts.
5. Click **Roles** from the left panel.
   Configure the policies for the IAM role that you configure when the IAM user and the IAM role are in different accounts.
6. Click **Trust relationships** tab to view the trust relationship for the AWS account.
7. Click **Edit trust relationship** to define the trust relationship.
   The **Edit Trust Relationship** window opens.
8. Edit the policy and specify the conditions for the external ID.
   The following image shows the condition that you defined for the external ID:



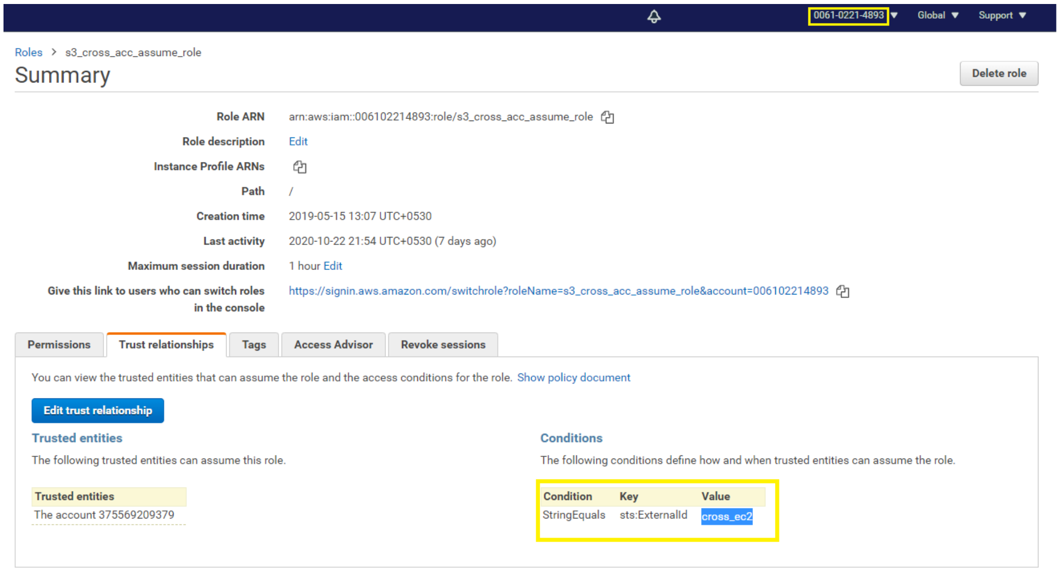
Edit Trust Relationship

You can customize trust relationships by editing the following access control policy document.

Policy Document

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::375569209379:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "cross_ec2"
        }
      }
    }
  ]
}
```

9. Click **Update Trust Policy**.
   The **Trust relationships** tab shows the external ID condition and the value that you specified.



Summary

Role ARN	arn:aws:iam::006102214893:role/s3_cross_acc_assume_role
Role description	Edit
Instance Profile ARNs	
Path	/
Creation time	2019-05-15 13:07 UTC+0530
Last activity	2020-10-22 21:54 UTC+0530 (7 days ago)
Maximum session duration	1 hour Edit
Give this link to users who can switch roles in the console	https://signin.aws.amazon.com/switchrole?roleName=s3_cross_acc_assume_role&account=006102214893

You can view the trusted entities that can assume the role and the access conditions for the role. Show policy document

Trusted entities

The following trusted entities can assume this role.

Trusted entities
The account 375569209379

Conditions

The following conditions define how and when trusted entities can assume the role.

Condition	Key	Value
StringEquals	sts:ExternalId	cross_ec2

Case 4. EC2 role for the same or different AWS accounts

You can use an assume role for an Amazon EC2 role to access the AWS resources from the same or different AWS accounts. When you use an assume role with EC2, the Secure Agent must be on an EC2 box.

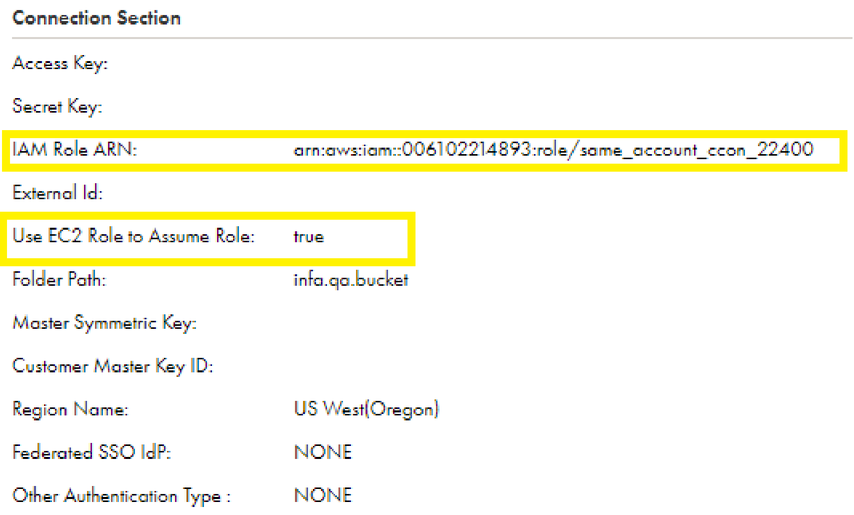
The Amazon EC2 role would be able to assume another IAM role from the same or different AWS account without requiring a permanent access key and secret key.

You must configure Cloud Data Integration and AWS to use the assume role.

Configure the connection properties in Cloud Data Integration

Specify **IAM Role ARN** and set the **Use EC2 Role to Assume Role** property to **true** in the connection properties in Cloud Data Integration.

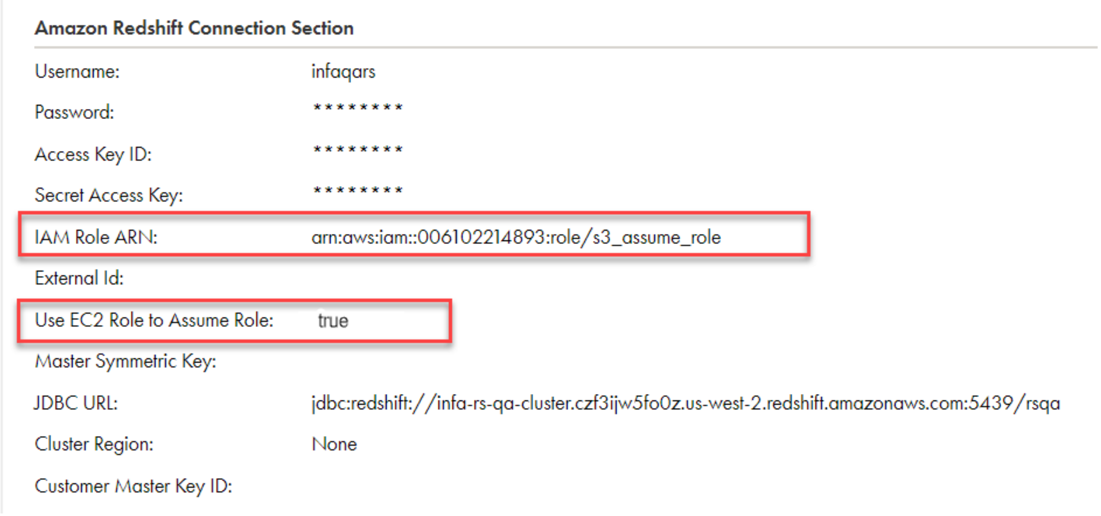
The following image shows the configured property in the Amazon S3 V2 connection:



Connection Section

Access Key:	
Secret Key:	
IAM Role ARN:	arn:aws:iam::006102214893:role/same_account_ccon_22400
External Id:	
Use EC2 Role to Assume Role:	true
Folder Path:	infa.qa.bucket
Master Symmetric Key:	
Customer Master Key ID:	
Region Name:	US West(Oregon)
Federated SSO IdP:	NONE
Other Authentication Type :	NONE

The following image shows the configured property in the Amazon Redshift V2 connection:



Amazon Redshift Connection Section

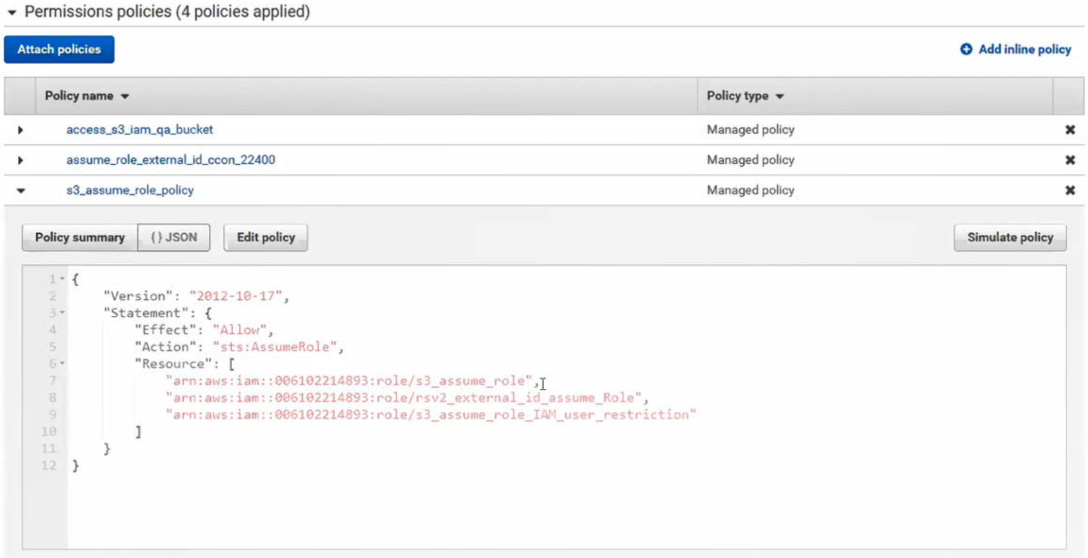
Username:	infaqars
Password:	********
Access Key ID:	********
Secret Access Key:	********
IAM Role ARN:	arn:aws:iam::006102214893:role/s3_assume_role
External Id:	
Use EC2 Role to Assume Role:	true
Master Symmetric Key:	
JDBC URL:	jdbc:redshift://infa-rs-qa-cluster.czf3ijw5fo0z.us-west-2.redshift.amazonaws.com:5439/rsqa
Cluster Region:	None
Customer Master Key ID:	

Configure assume role on the AWS console

The EC2 role assumes a role that an IAM user assumes when the IAM user and the IAM role are in the same account.

Create an EC2 instance and assign a policy to an EC2 role, which in turn has an assume role. Then install the Secure Agent.

The following image shows the sample policies attached to an EC2 role:



Policy name	Policy type
access_s3_iam_qa_bucket	Managed policy
assume_role_external_id_ccon_22400	Managed policy
s3_assume_role_policy	Managed policy

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": [
            "arn:aws:iam::006102214893:role/s3_assume_role",
            "arn:aws:iam::006102214893:role/rsv2_external_id_assume_Role",
            "arn:aws:iam::006102214893:role/s3_assume_role_IAM_user_restriction"
        ]
    }
}
```

Authors

Sumit Kumar Mishra

Abhishek Kumar Dayal

Anush Shetty