Informatica

Configuring AssumeRole Authentication for Amazon Redshift V2 Connector

Abstract

You can use the IAM AssumeRole authentication to access Amazon Redshift V2 resources. You can configure the Redshift IAM role ARN with an IAM user or define an EC2 instance to assume a role. This article describes the guidelines to configure Redshift IAM Authentication using AssumeRole to connect to Redshift using Redshift V2 Connector.

Supported Versions

- Informatica Intelligent Cloud Services April 2023

Table of Contents

Overview

You can use the AssumeRole authentication in Amazon Redshift to access the Redshift database without the need to provide the database credentials. You can enable users to connect to the Redshift database using temporary security credentials.

You can use AssumeRole to enable new or existing database users to connect to the Redshift database. You can use an IAM role configured with required trust policies to generate temporary security credentials to access Amazon Redshift. You can enable IAM users or define an EC2 instance to assume an IAM role to access Redshift.

Additionally, you can also enable cross-account access where the Redshift cluster, S3 bucket, and Redshift IAM role ARN are in one account and the IAM users or the EC2 role are in a different account. In this scenario, you need to configure the user accounts to assume the role in the Redshift cluster account.

AssumeRole authentication methods

You can configure the AssumeRole authentication in Amazon Redshift.

Select the **Redshift IAM Authentication via AssumeRole** and use one of the following methods to establish an Amazon Redshift connection:

Assume a role using access key and secret key

> To assume a role, specify the access key and secret key in the connection properties. You can attach the required permission and trust policies to the Redshift IAM Role ARN to assume a role.

Assume a role using an EC2 role

To enable the EC2 role, select the **Use EC2 Role to Assume Role** check box in the connection properties. The Amazon EC2 role can assume another IAM role from the same or different AWS account without a permanent Redshift access key and secret key.

AssumeRole with access key and secret key

You can access the Amazon Redshift database with the access key and secret key using an IAM Role ARN. To access Redshift, you must configure the permission and trust policies.

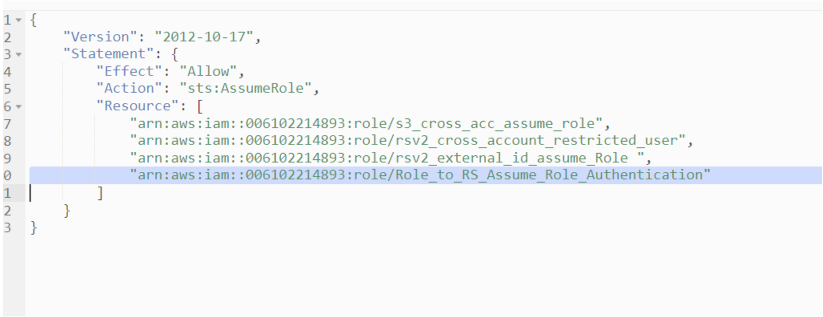
After you define the policies, identify the `Cluster Identifier` and `Database Name` values from the JDBC URL in the connection properties. For example, if the JDBC URL is `<jdbc:redshift://`**`infa-rs-qa-cluster`**`.czf3ijw5fo0z.us-west-2.redshift.amazonaws.com:5439/`**`rsqa`**`>`, `infa-rs-qa-cluster` is the cluster identifier and `<rsqa>` is the database name.

AssumeRole with an existing database user

To connect to Redshift using an existing database user by using an IAM user to assume a role, specify the database user, Redshift access key and secret key, and the Redshift IAM role in the connection properties.

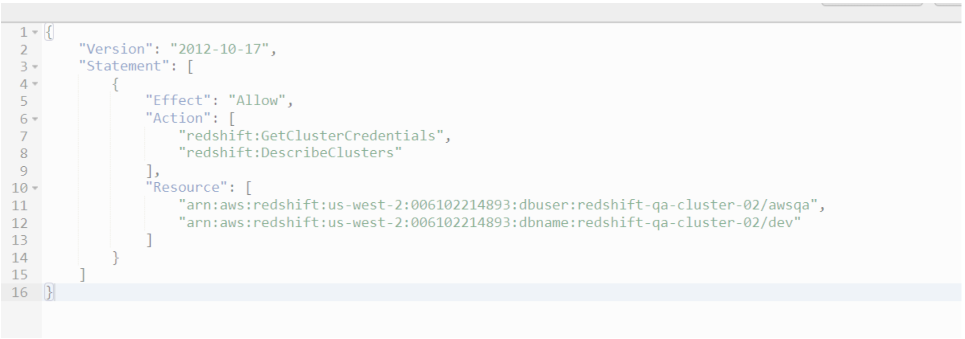
For an IAM user to assume a role, attach the following AWS IAM user policies in the AWS console:

- AWS IAM user policy for the Redshift access key and secret key:



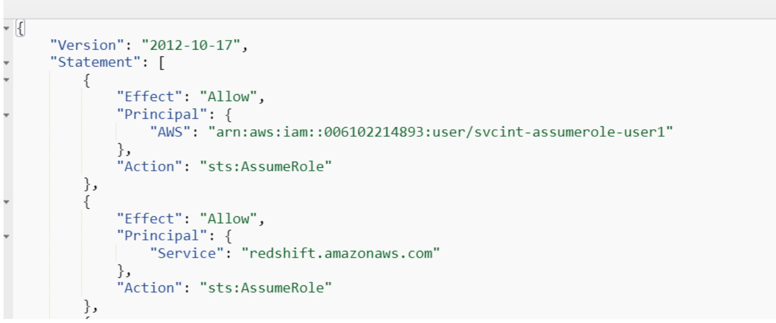
```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": [
            "arn:aws:iam::006102214893:role/s3_cross_acc_assume_role",
            "arn:aws:iam::006102214893:role/rsv2_cross_account_restricted_user",
         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

- AWS IAM role policy of the Redshift IAM role ARN for an existing database user:



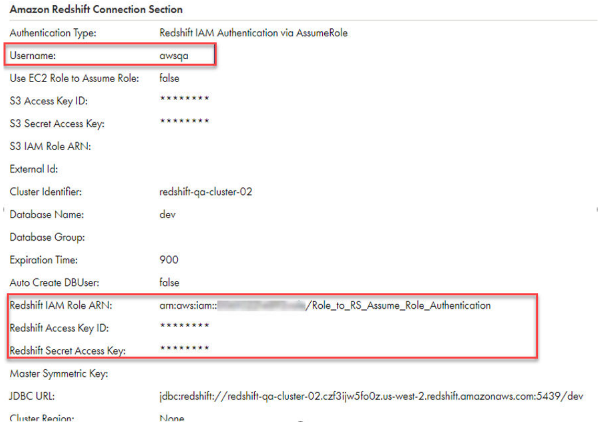
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "redshift:GetClusterCredentials",
                "redshift:DescribeClusters"
            ],
            "Resource": [
                "arn:aws:redshift:us-west-2:006102214893:dbuser:redshift-qa-cluster-02/awsqa",
                "arn:aws:redshift:us-west-2:006102214893:dbname:redshift-qa-cluster-02/dev"
            ]
        }
    ]
}
```

- Trust policy that defines which user can assume the Redshift role:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::006102214893:user/svcint-assumerole-user1"
            },
            "Action": "sts:AssumeRole"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "redshift.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        },
```

After you define the policies, you can specify the following attributes in the connection properties for an existing database user:



Amazon Redshift Connection Section

Authentication Type:	Redshift IAM Authentication via AssumeRole
Username:	awsqa
Use EC2 Role to Assume Role:	false
S3 Access Key ID:	********
S3 Secret Access Key:	********
S3 IAM Role ARN:	
External Id:	
Cluster Identifier:	redshift-qa-cluster-02
Database Name:	dev
Database Group:	
Expiration Time:	900
Auto Create DBUser:	false
Redshift IAM Role ARN:	arn:aws:iam::[redacted]/Role_to_RS_Assume_Role_Authentication
Redshift Access Key ID:	********
Redshift Secret Access Key:	********
Master Symmetric Key:	
JDBC URL:	jdbc:redshift://redshift-qa-cluster-02.czf3ijw5fo0z.us-west-2.redshift.amazonaws.com:5439/dev
Cluster Region:	None

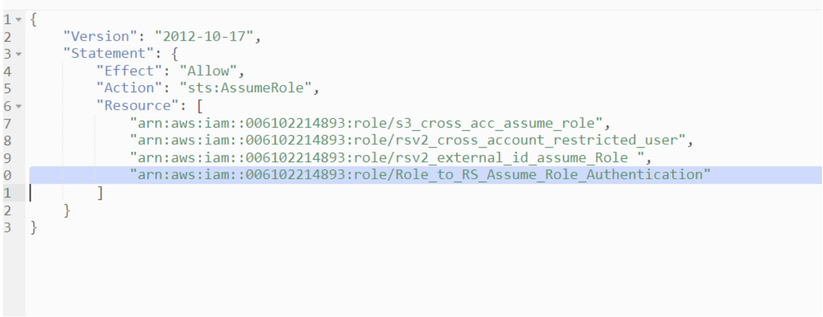
AssumeRole with a new database user

For a new user to connect to Redshift database using the IAM user to assume a role, you must select the **Auto Create DBUser** option in the Amazon Redshift connection section. Specify Redshift access key and secret key of the IAM user and Redshift IAM role in the connection properties.

Also, attach the permission policy in AWS to the Redshift IAM role.

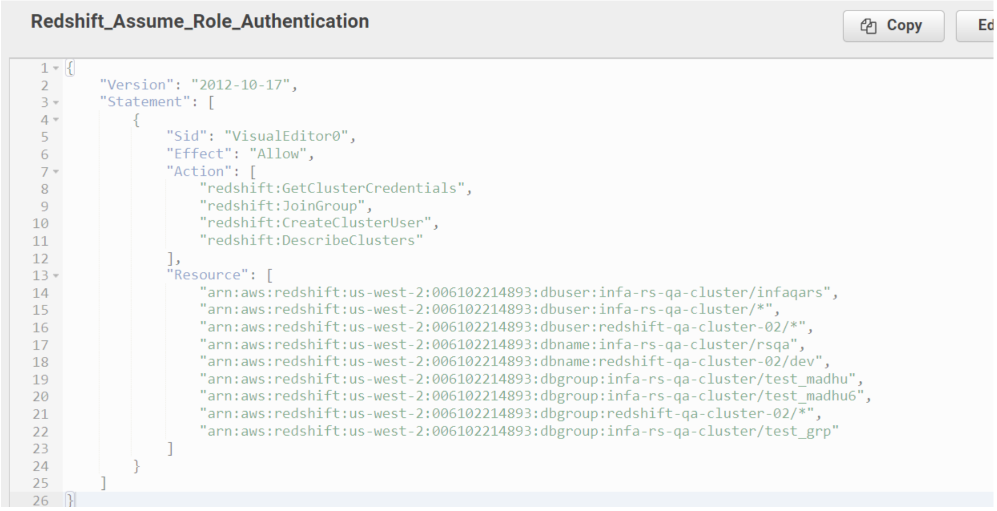
For an IAM user to assume a role, attach the following AWS IAM user policies in the AWS console:

- AWS IAM user policy for the Redshift access key and secret key:



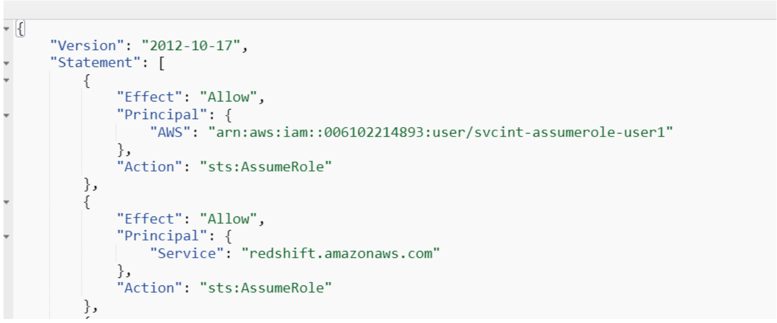
```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": [
            "arn:aws:iam::006102214893:role/s3_cross_acc_assume_role",
            "arn:aws:iam::006102214893:role/rsv2_cross_account_restricted_user",
         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

- AWS IAM role policy of the Redshift IAM role ARN for a new database user:



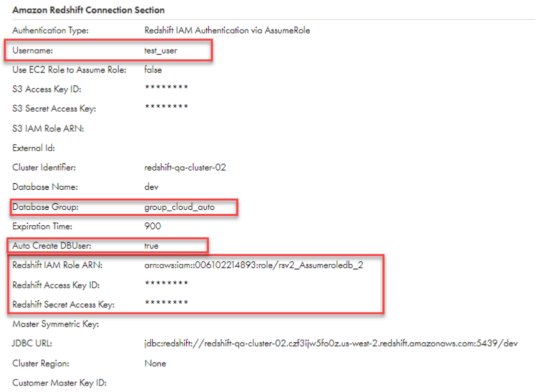
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "redshift:GetClusterCredentials",
                "redshift:JoinGroup",
                "redshift:CreateClusterUser",
                "redshift:DescribeClusters"
            ],
            "Resource": [
                "arn:aws:redshift:us-west-2:006102214893:dbuser:infa-rs-qa-cluster/infaqars",
                "arn:aws:redshift:us-west-2:006102214893:dbuser:infa-rs-qa-cluster/*",
                "arn:aws:redshift:us-west-2:006102214893:dbuser:redshift-qa-cluster-02/*",
                "arn:aws:redshift:us-west-2:006102214893:dbname:infa-rs-qa-cluster/rsqa",
                "arn:aws:redshift:us-west-2:006102214893:dbname:redshift-qa-cluster-02/dev",
                "arn:aws:redshift:us-west-2:006102214893:dbgroup:infa-rs-qa-cluster/test_madhu",
                "arn:aws:redshift:us-west-2:006102214893:dbgroup:infa-rs-qa-cluster/test_madhu6",
                "arn:aws:redshift:us-west-2:006102214893:dbgroup:redshift-qa-cluster-02/*",
                "arn:aws:redshift:us-west-2:006102214893:dbgroup:infa-rs-qa-cluster/test_grp"
            ]
        }
    ]
}
```

- Trust policy that defines which user can assume the Redshift role:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::006102214893:user/svcint-assumerole-user1"
            },
            "Action": "sts:AssumeRole"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "redshift.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        },
```

After you define the policies, you can specify the following attributes in the connection properties for a new database user:



Amazon Redshift Connection Section

Authentication Type:	Redshift IAM Authentication via AssumeRole
Username:	test_user
Use EC2 Role to Assume Role:	false
S3 Access Key ID:	********
S3 Secret Access Key:	********
S3 IAM Role ARN:	
External Id:	
Cluster Identifier:	redshift-qa-cluster-02
Database Name:	dev
Database Group:	group_cloud_auto
Expiration Time:	900
Auto Create DBUser:	true
Redshift IAM Role ARN:	arn:aws:iam::006102214893:role/rsv2_Assumeroledb_2
Redshift Access Key ID:	********
Redshift Secret Access Key:	********
Master Symmetric Key:	
JDBC URL:	jdbc:redshift://redshift-qa-cluster-02.czf3ijw5fo0z.us-west-2.redshift.amazonaws.com:5439/dev
Cluster Region:	None
Customer Master Key ID:	

You can also add the new user to a database group where the user can inherit all the permissions that are associated to the group. Additionally, you can set the **AutoCreateDBUser** to true to create new users at runtime.

AssumeRole with Cross-account access in Redshift

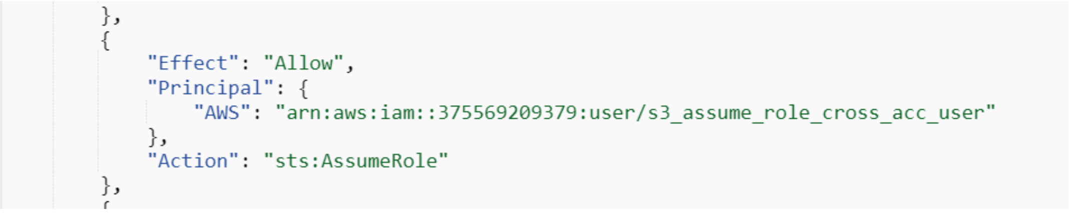
You can enable cross-account access for AssumeRole authentication. Attach the AWS IAM user policies for access key and secret key and trust policy to define which user can assume the Redshift role. Based on the use case, you can define the policy either for a new user or an existing user in Redshift database.

Enabling trust and permission policies for cross-account access

Let's consider a use case where the Redshift cluster, S3 bucket, and Redshift IAM Role ARN are in the same account, for example Account A. The IAM user whose access key and secret key you configure in the connection properties resides in Account B.

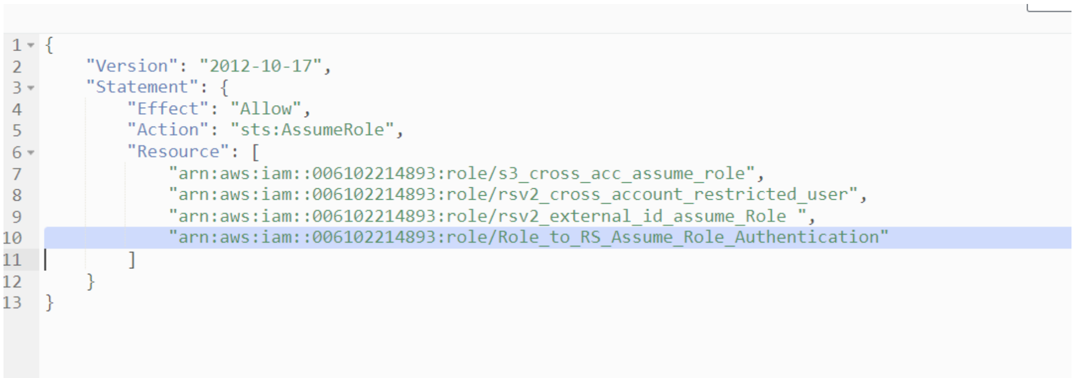
Enable the following policies for cross-account access:

- Trust policy of the Redshift IAM Role ARN in Account A:



```
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::375569209379:user/s3_assume_role_cross_acc_user"
            },
            "Action": "sts:AssumeRole"
        },
        {
```

- Permission policy of the IAM user in Account B:



```
{
    "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 ",
            "arn:aws:iam::006102214893:role/Role_to_RS_Assume_Role_Authentication"
        ]
    }
}
```

AssumeRole with EC2 role

You can access the Amazon Redshift database by defining an EC2 role, where the EC2 instance can assume a role. To access Redshift, you must enable the **Use EC2 to Assume Role** check box in the connection properties and configure the permission and trust policies.

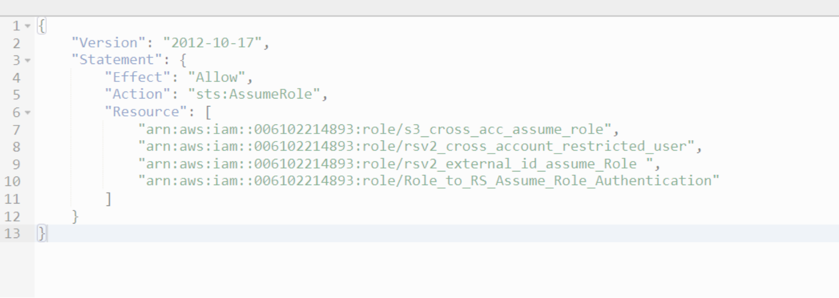
When you define the policies, identify the `Cluster Identifier` and `Database Name` values from the JDBC URL in the connection properties. For example, if the JDBC URL is `<jdbc:redshift://`**`infa-rs-qa-cluster`**`.czf3ijw5fo0z.us-west-2.redshift.amazonaws.com:5439/`**`rsqa`**`>`, `infa-rs-qa-cluster` is the cluster identifier and `<rsqa>` is the database name.

AssumeRole with an existing database user

To connect to the Amazon Redshift database for an existing database user using the EC2 role to assume a role, specify the user name in the Amazon Redshift connection section and select the **Use EC2 Role to AssumeRole** checkbox.

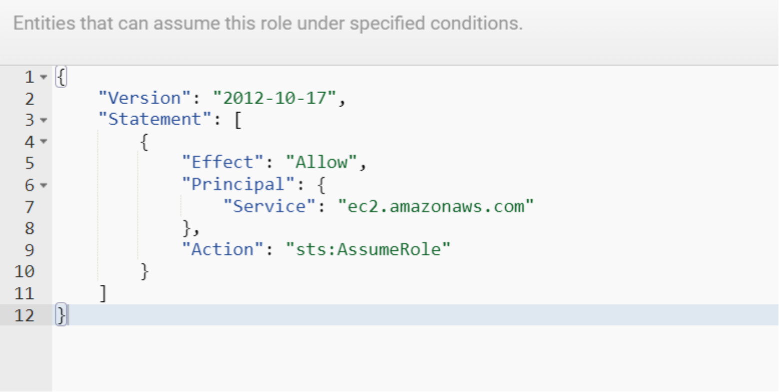
To assume a role using the EC2 role, attach the following policies to an EC2 role in the AWS console:

- AWS IAM EC2 policy that enables you to assume a role:



```
{
    "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 ",
            "arn:aws:iam::006102214893:role/Role_to_RS_Assume_Role_Authentication"
        ]
    }
}
```

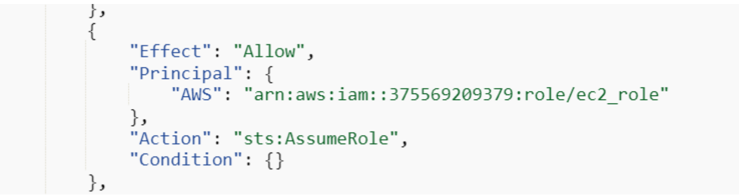
- The trust relationship of the EC2 role to assume a role:



Entities that can assume this role under specified conditions.

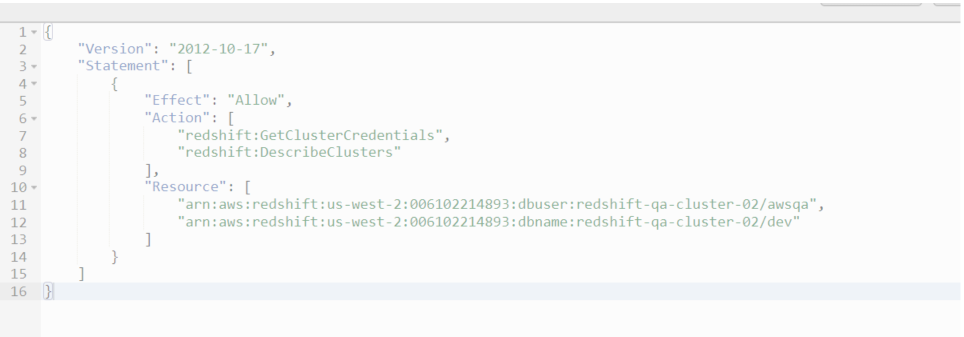
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

- Trust relationship of the Redshift role to enable the EC2 role to assume a role:



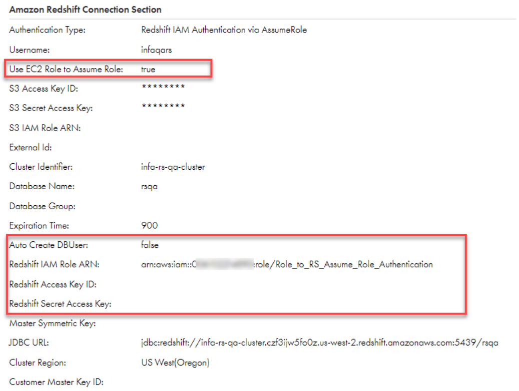
```
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::375569209379:role/ec2_role"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        },
```

- Policy to enable a Redshift role for an existing database user:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "redshift:GetClusterCredentials",
                "redshift:DescribeClusters"
            ],
            "Resource": [
                "arn:aws:redshift:us-west-2:006102214893:dbuser:redshift-qa-cluster-02/awsqa",
                "arn:aws:redshift:us-west-2:006102214893:dbname:redshift-qa-cluster-02/dev"
            ]
        }
    ]
}
```

After you define the policies, you can specify the following attributes in the connection properties for an existing database user:



Amazon Redshift Connection Section

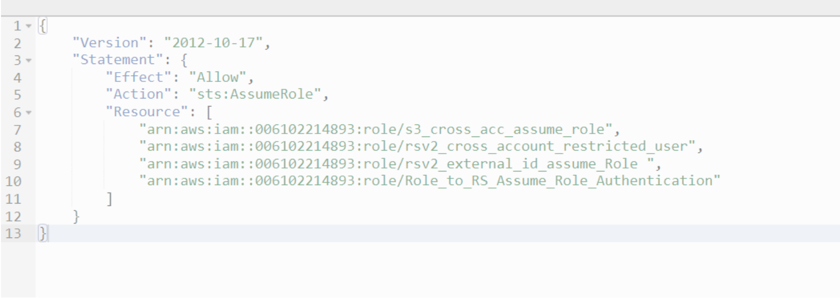
Authentication Type:	Redshift IAM Authentication via AssumeRole
Username:	infaqars
Use EC2 Role to Assume Role:	true
S3 Access Key ID:	********
S3 Secret Access Key:	********
S3 IAM Role ARN:	
External Id:	
Cluster Identifier:	infa-rs-qa-cluster
Database Name:	rsqa
Database Group:	
Expiration Time:	900
Auto Create DBUser:	false
Redshift IAM Role ARN:	arn:aws:iam::0[redacted]:role/Role_to_RS_Assume_Role_Authentication
Redshift Access Key ID:	
Redshift Secret Access Key:	
Master Symmetric Key:	
JDBC URL:	jdbc:redshift://infa-rs-qa-cluster.czf3ijw5fo0z.us-west-2.redshift.amazonaws.com:5439/rsqa
Cluster Region:	US West(Oregon)
Customer Master Key ID:	

AssumeRole with a new database user

To connect to the Amazon Redshift database using the EC2 role to assume a role, specify the user name in the Amazon Redshift connection properties and select the **Use EC2 Role to AssumeRole** checkbox.

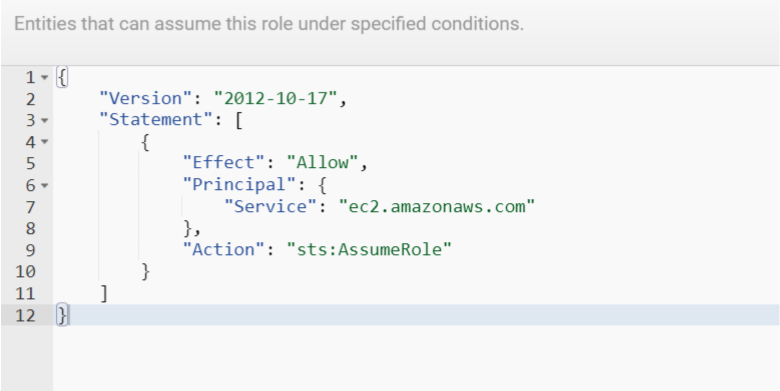
To assume a role using the EC2 role, you must attach the following policies to the EC2 role in the AWS console:

- AWS IAM EC2 policy that enables you to assume a role:



```
{
    "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 ",
            "arn:aws:iam::006102214893:role/Role_to_RS_Assume_Role_Authentication"
        ]
    }
}
```

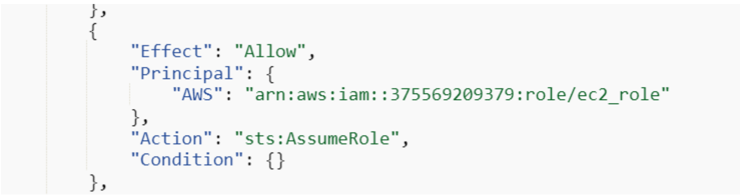
- The trust relationship of the EC2 role to assume a role:



Entities that can assume this role under specified conditions.

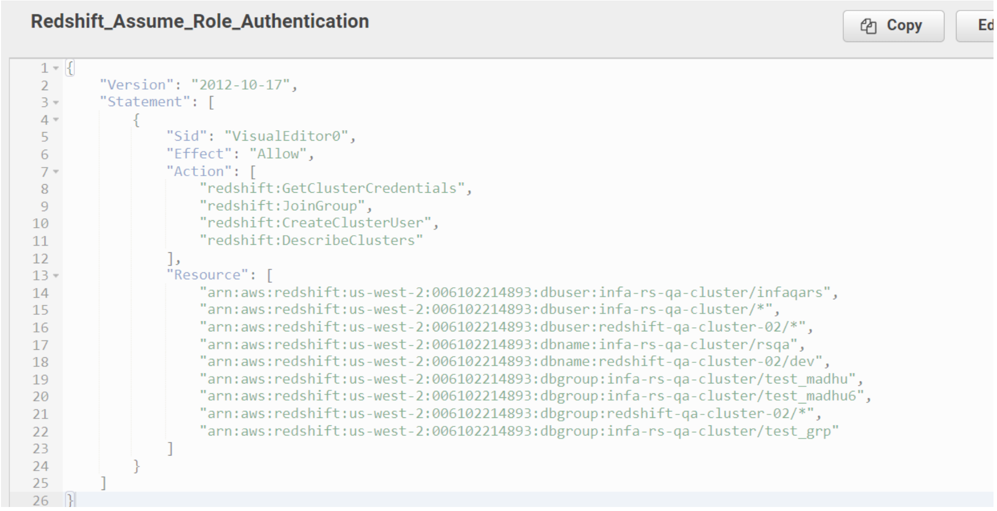
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

- Trust relationship of the Redshift role to enable the EC2 role to assume a role:



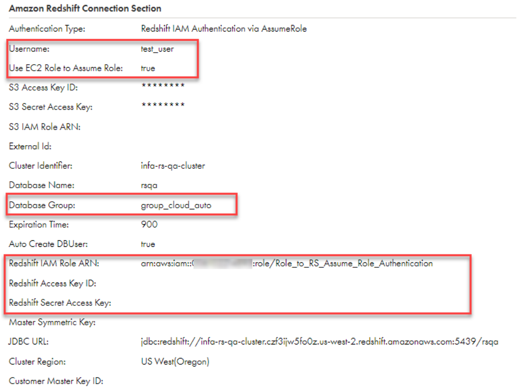
```
    },
    {
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::375569209379:role/ec2_role"
        },
        "Action": "sts:AssumeRole",
        "Condition": {}
    },
```

- You can attach the following policy in AWS to a Redshift role for a new database user:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "redshift:GetClusterCredentials",
                "redshift:JoinGroup",
                "redshift:CreateClusterUser",
                "redshift:DescribeClusters"
            ],
            "Resource": [
                "arn:aws:redshift:us-west-2:006102214893:dbuser:infa-rs-qa-cluster/infaqars",
                "arn:aws:redshift:us-west-2:006102214893:dbuser:infa-rs-qa-cluster/*",
                "arn:aws:redshift:us-west-2:006102214893:dbuser:redshift-qa-cluster-02/*",
                "arn:aws:redshift:us-west-2:006102214893:dbname:infa-rs-qa-cluster/rsqa",
                "arn:aws:redshift:us-west-2:006102214893:dbname:redshift-qa-cluster-02/dev",
                "arn:aws:redshift:us-west-2:006102214893:dbgroup:infa-rs-qa-cluster/test_madhu",
                "arn:aws:redshift:us-west-2:006102214893:dbgroup:infa-rs-qa-cluster/test_madhu6",
                "arn:aws:redshift:us-west-2:006102214893:dbgroup:redshift-qa-cluster-02/*",
                "arn:aws:redshift:us-west-2:006102214893:dbgroup:infa-rs-qa-cluster/test_grp"
            ]
        }
    ]
}
```

The following image shows an example of the configured connection properties:



Amazon Redshift Connection Section

Authentication Type:	Redshift IAM Authentication via AssumeRole
Username:	test_user
Use EC2 Role to Assume Role:	true
S3 Access Key ID:	********
S3 Secret Access Key:	********
S3 IAM Role ARN:	
External Id:	
Cluster Identifier:	infa-rs-qa-cluster
Database Name:	rsqa
Database Group:	group_cloud_auto
Expiration Time:	900
Auto Create DBUser:	true
Redshift IAM Role ARN:	arn:aws:iam::[redacted]:role/Role_to_RS_Assume_Role_Authentication
Redshift Access Key ID:	
Redshift Secret Access Key:	
Master Symmetric Key:	
JDBC URL:	jdbc:redshift://infa-rs-qa-cluster.czf3ijw5fo0z.us-west-2.redshift.amazonaws.com:5439/rsqa
Cluster Region:	US West(Oregon)
Customer Master Key ID:	

AssumeRole with Cross-account access in Redshift

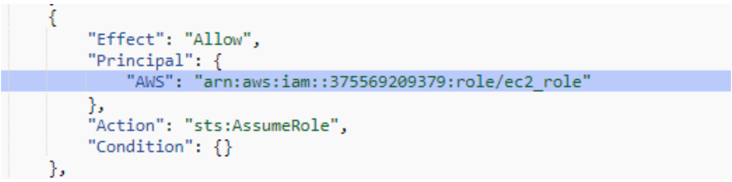
You can enable cross-account access for AssumeRole authentication.

Enabling trust and permission policies for cross-account access

Let's consider a use case where the Redshift cluster, S3 bucket, Redshift IAM Role ARN are in the same account, for example Account A. The EC2 instance that assumes a role is in a different account, Account B.

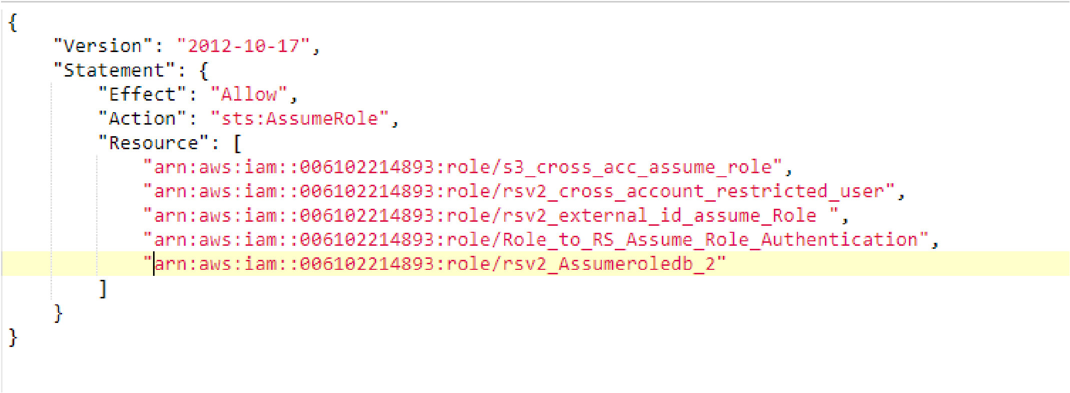
Enable the following policies for cross-account access:

- Trust policy of the Redshift IAM Role ARN in Account A, to let the EC2 in Account B to assume a role:



```
    {
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::375569209379:role/ec2_role"
        },
        "Action": "sts:AssumeRole",
        "Condition": {}
    },
```

- Permission policy of the EC2 role in Account B that you can configure to assume a role in Account A:

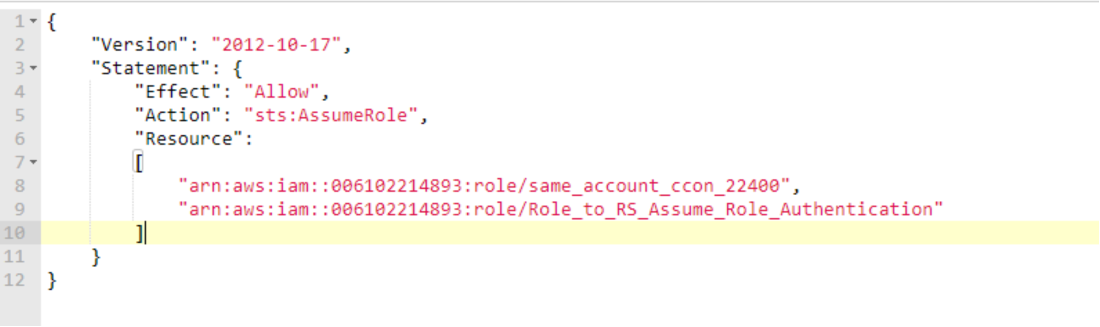


```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": [
            "arn:aws:iam::006102214893:role/s3_cross_acc_assume_role",
            "arn:aws:iam::006102214893:role/rsv2_cross_account_restricted_user",
            "arn:aws:iam::006102214893:role/rsv2_external_id_assume_Role ",
            "arn:aws:iam::006102214893:role/Role_to_RS_Assume_Role_Authentication",
            "arn:aws:iam::006102214893:role/rsv2_Assumeroledb_2"
        ]
    }
}
```

AssumeRole authentication for mappings in advanced mode

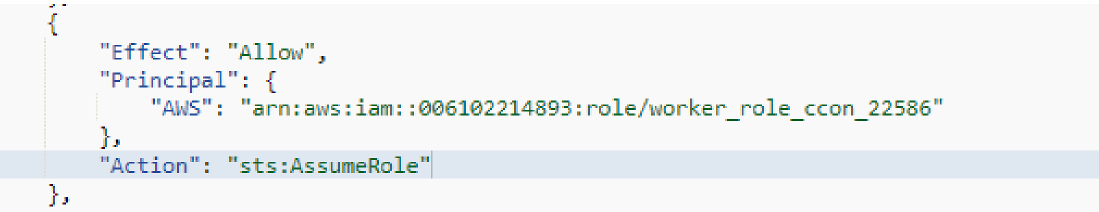
To enable AssumeRole authentication for mappings in advanced mode, you need to attach the AssumeRole permission and trust policies to the worker node role in addition to the existing user policies.

Attach the following permission policy to the worker node in AWS:



```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource":
        [
            "arn:aws:iam::006102214893:role/same_account_ccon_22400",
            "arn:aws:iam::006102214893:role/Role_to_RS_Assume_Role_Authentication"
        ]
    }
}
```

Attach the following trust policy of the Redshift role that allows the worker role to assume it:



```
    {
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::006102214893:role/worker_role_ccon_22586"
        },
        "Action": "sts:AssumeRole"
    },
```

Author

Informatica Intelligent Cloud Services Documentation Team