How-To Library

Informatica

Configuring Informatica Encryption for Mappings in Advanced Mode in Amazon S3 V2 Connector

Abstract

This article describes how you can configure Informatica encryption for mappings in advanced mode in Amazon S3 V2 Connector.

Supported Versions

- Informatica Intelligent Cloud Services April 2023

Table of Contents

Overview

Informatica encryption is a mechanism for maintaining the privacy and confidentiality of data developed using the Informatica crypto libraries. Use Informatica encryption to encrypt or decrypt the data of binary and flat files.

You can use Informatica encryption for mappings in advanced mode in Amazon S3 V2 Connector. You must configure AWS and Cloud Data Integration to use Informatica encryption in the advanced cluster.

Prerequisites

Consider the following prerequisites when you configure Informatica encryption for mappings in advanced mode:

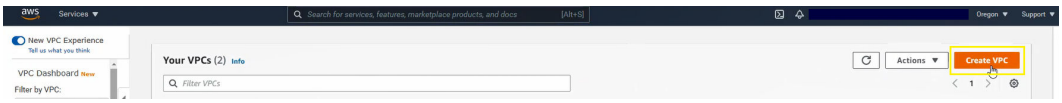
- Install the Secure Agent on an Amazon EC2 machine.
- Enable the Informatica crypto library license.

Configure Informatica Encryption on the AWS Console

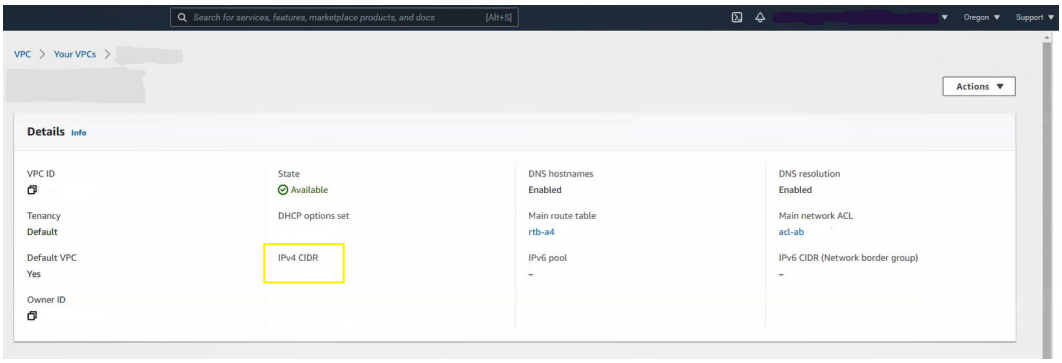
To configure Informatica encryption on the AWS console, create a VPC, create an inbound rule for the security group of the EC2 machine, and add the IPV4 CIDR value for the VPC in the inbound rule.

Perform the following steps on the AWS console to configure Informatica encryption:

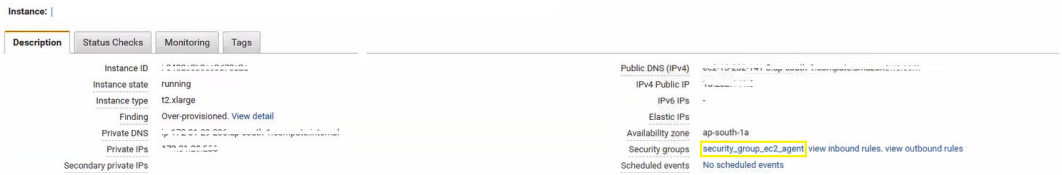
1. Log in to the AWS console.
2. Enter **VPCs** in the `Search` box.
   The **Your VPCs** window appears.
3. Click **Create VPC**.



4. Specify the VPC and subnet details.
5. Copy the IPV4 CIDR value for the VPC that you created.



6. In the **Services** tab, select **EC2**.
7. In the EC2 dashboard, select the EC2 machine where the Secure Agent is installed.
8. Scroll down to the **Description** section for the EC2 machine.
9. In the **Security groups** field, select the security group.



10. Click the **Inbound** tab.
11. Click **Edit** to edit the inbound rule.
    The **Edit inbound rules** window appears.
12. Click **Add Rule**.
13. Select the **Type** as **All traffic** and paste the value for **Source** with the IPV4 CIDR value that you copied in step 5.
14. Click **Save**.

Configure Informatica Encryption in Cloud Data Integration

To configure Informatica encryption in Cloud Data Integration, specify the VPC details in the elastic cluster configuration. Then, select the encryption type as Informatica encryption to encrypt or decrypt the data.

Administrator Service

Perform the following steps in the Administrator service:

1. Log in to Informatica Intelligent Cloud Services.
2. Go to **Administrator**.
3. Click **Advanced Clusters** and select the type of advanced cluster. You can create a new cluster or edit an existing cluster.
4.
5. In the **Advanced Configuration** section, enter the VPC and subnet details that you specified in AWS.

6. Click **Save**.

Data Integration Service

Perform the following steps in the Data Integration service:

1. In Informatica Intelligent Cloud Services, go to **Data Integration**.
2. Click **New** > **Mappings** > **Mapping**.
3. In the Mapping Designer, click **Switch to Advanced**.
4. Under advanced properties in the Source or Target transformations, select **Informatica Encryption** as the encryption type.
5. Specify the rest of the properties in the advanced properties.
6. Click **Save**.
7. Run the mapping.

Note: When you enable Informatica encryption for sources and targets across different regions, then the encryption is not supported for clusters that have S3 gateway endpoint without NAT.

Author

Informatica Intelligent Cloud Services Documentation Team