LUMENDATA

Data Sheet

Key Pair Authentication Setup for Informatica, Airflow with Snowflake

5201 GREAT AMERICAN PARKWAY, SUITE 320
SANTA CLARA, CA 95054
Tel: (855) 695-8636
E-mail: info@lumendata.com
Website: www.lumendata.com

This guide provides **a step-by-step approach to configuring key pair-based authentication between Informatica, Airflow, and Snowflake**. The process involves:

- Generating a private and public key.
- Associating the public key with a Snowflake user.
- Configuring Informatica and Airflow to authenticate using the private key.

Step 1: Generate the Private Key

The first step is to generate an encrypted private key that will be used for authentication.

Steps:

- **Open Terminal/Command Prompt:** Open the terminal or command prompt on the Secure Agent machine.
- **Generate the Private Key:** Run the following OpenSSL command to generate a 2048-bit RSA private key and encrypt it using DES3 encryption:

"openssl genrsa 2048 | openssl pkcs8 -topk8 -v2 des3 -inform PEM -out rsa_key.p8"

- **Enter a Password:** You will be prompted to enter a password to encrypt the private key. Enter the password twice to confirm and securely encrypt the key.
- **Save the Key:** Once the command executes successfully, a file named rsa_key.p8 will be generated in the following location:

"C:\Users\SecureAgent"
This file contains the encrypted private key.

Step 2: Generate the Public Key

Next, generate a public key corresponding to the private key. The public key will be used for authentication in Snowflake.

Steps:

- **Generate the Public Key:** Execute the following command to generate the public key from the private key file (rsa_key.p8):

"openssl rsa -in rsa_key.p8 -pubout -out rsa_key.pub"

```
AzureAD+PDineshReddy@LDILAADCPDR02 MINGW64 ~
$ openssl rsa -in rsa_key.p8 -pubout -out rsa_key.pub
Enter pass phrase for rsa_key.p8:
writing RSA key
```

- **Save the Public Key:** After running the command, the public key will be stored in a file named:

"C:\Users\SecureAgent\rsa_key.pub"

Step 3: Link the Public Key to the Snowflake User

Now that you have generated the public key, associate it with the appropriate user in Snowflake.

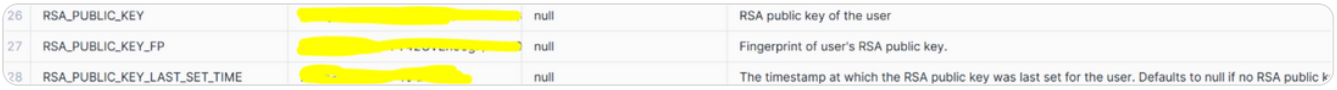
Steps:

- Log in to Snowflake: Access Snowflake using the Web UI or any SQL client.
- Associate the Public Key with the User: Run the following SQL command to link the public key to the desired Snowflake user:

"ALTER USER Infa_Demo SET RSA_PUBLIC_KEY='<Public Key Value>';"

- Replace <Public Key Value> with the actual public key contents generated in rsa_key.pub.
- Verify the Association: Run the following command to confirm that the public key has been successfully associated with the Snowflake user:

"desc user Infa_Demo;"



Step 4: Configure Informatica to Use Key Pair Authentication

With the public key linked to the Snowflake user, configure Informatica to authenticate using the private key.

Prerequisite: Configure Snowflake JDBC Properties File

Before creating the connection in Informatica, perform the following setup:

- Include all the necessary connection details for connector from informatica to snowflake in jdbc.properties file.

```
jdbcUrl = jdbc:snowflake://example.snowflakecomputing.com
user = USer_name
database = Database for connection
schema = Schema to be point out
warehouse = Warehouse for query execution
role = Role Assigned
privateKeyFile = Private key path in secureagent folder
providers=BC
```

Next step place this in informatica secure agent jre folder and try to execute the following command with that path in cmd " java -jar SnowFlake.jar"

For detailed steps on configuring the Snowflake JDBC driver, refer to:
Snowflake Private Key Authentication Documentation

Configure the Connection in Informatica

- **Log in to Informatica Administrator:** Open the Informatica Administrator console. Navigate to the Connections section.
- **Create a New Snowflake Connection:** Click on New Connection to create a new Snowflake connection. Choose Snowflake Data Cloud as the connection type.
- **Configure the Connection Details:**
  Warehouse: Specify the Snowflake warehouse.
  Database: Provide the target Snowflake database.
  Schema: Specify the relevant schema within the database.
- **Enable Key Pair Authentication:** In the connection settings, change the Authentication Type to Key Pair.
- **Private Key File:** Browse and specify the file path to the private key (rsa_key.p8) stored on the Secure Agent machine.

"C:\Users\SecureAgent\rsa_key.p8"

Note: Ensure that the private key file is securely stored and accessible only by the Secure Agent Machine where Informatica is running.

For more information : [Snowflake PrivateKey Authentication for CDI, APPMI and DBMI]

Step 5: Test and Save the Connection

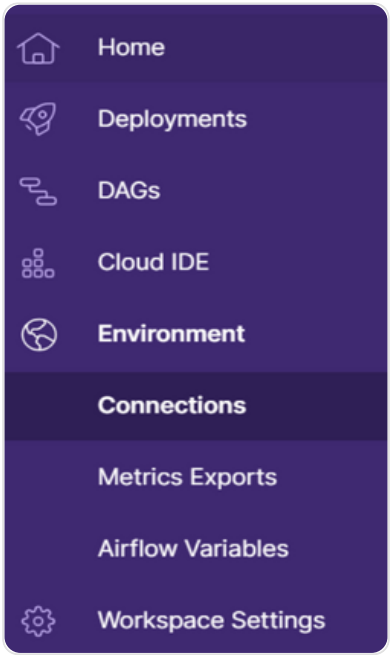
- Test the Connection: After entering all required details, click on the Test Connection button.
- Verify that the connection is successful and that key pair authentication is functioning correctly.
- Save the Connection: If the test is successful, save the connection configuration.

Configure Airflow to Use Key Pair Authentication with Snowflake

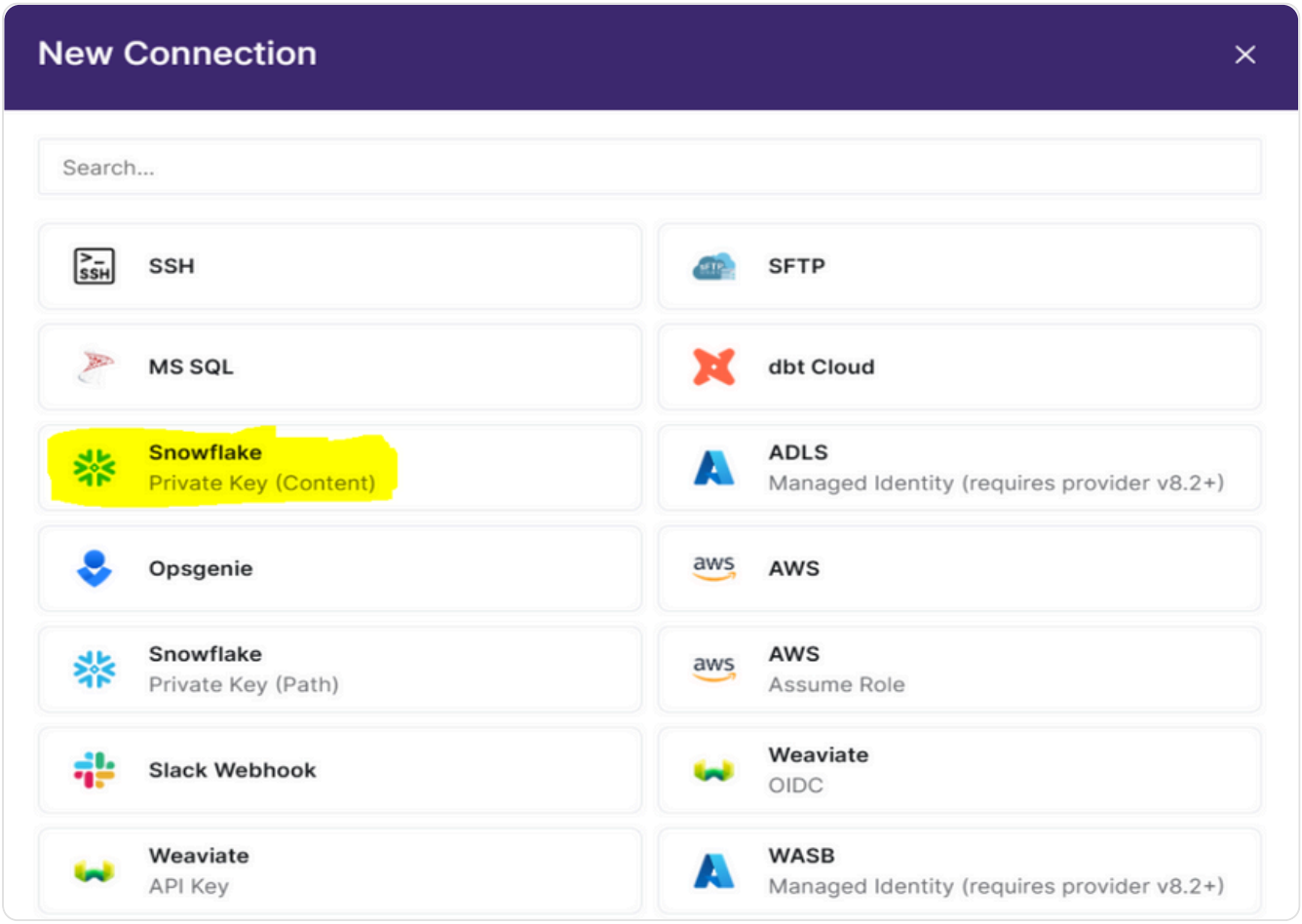
Airflow can also be configured to connect with Snowflake using private key authentication. This approach ensures secure authentication without requiring a password.

Steps:

- **Open Astronomer UI**: Log in to the Astronomer Web UI.



- **Navigate to Environments:** Click on Connection. Select Snowflake(Private Key(Content)).



- **Create a New Snowflake Connection**: Configure the following details
  Connection ID: snowflake_key_auth (or any relevant name)
  User Name: <user-name>
  Account: <account_name>
  Private Key:(content)
- Copy the contents of the rsa_key.p8 file and paste it directly into the Private Key field.
- **Test and Save the Connection**: Click on create connection.

Conclusion

By following these steps, you have successfully configured key pair-based authentication between Informatica, Airflow, and Snowflake.

This setup enhances security by eliminating the need to store passwords, ensuring that only authorized Service accounts can access Snowflake using the generated private key.

- **Private Key Encryption**: Encrypted private key ensures secure storage.
- **Public Key Association**: Ensures authentication with linked Snowflake user.
- **Informatica and Airflow Configuration**: Secure connection using private key.

For any troubleshooting or further assistance, refer to the official documentation of Informatica, Airflow, and Snowflake.

Authors

Abhishek Gaur
Technical Lead - Level 1

P Dinesh Reddy
Junior Data Analyst

About LumenData

LumenData is a leading provider of **Enterprise Data Management, Cloud & Analytics** solutions. We help businesses navigate their data visualization and analytics anxieties and enable them to accelerate their innovation journeys.

Founded in 2008, with locations in multiple countries, LumenData is privileged to serve over 100 leading companies. LumenData is **SOC2 certified** and has instituted extensive controls to protect client data, including adherence to GDPR and CCPA regulations.

LUMENDATA

Get in touch with us:
info@lumendata.com

Let us know what you need:
lumendata.com/contact-us