07-02-2023

Azure Key Vault Integration with IICS

Spoorthi Vaidya, Consultant PS

spvaidya@informatica.com

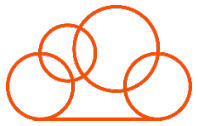
Informatica

Housekeeping Tips

- Today's Webinar is scheduled for 1 hour
- The session will include a webcast and then your questions will be answered live at the end of the presentation
- All dial-in participants will be muted to enable the speakers to present without interruption
- Questions can be submitted to "All Panelists" via the Q&A option and we will respond at the end of the presentation
- The webinar is being recorded and will be available on our INFASupport YouTube channel and Success Portal - where you can download the slide deck for the presentation. The link to the recording will be emailed as well.
- Please take time to complete the post-webinar survey and provide your feedback and suggestions for upcoming topics.

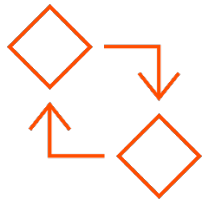
Informatica

Feature Rich Success Portal



Bootstrap trial and POC Customers

Enriched Customer Onboarding experience



Product Learning Paths and Weekly Expert Sessions

Informatica Concierge

Tailored training and content recommendations

Informatica

More Information

Success Portal

https://success.informatica.com

Communities & Support

https://network.informatica.com

Documentation

https://docs.informatica.com

University

https://www.informatica.com/in/services-and-training/informatica-university.html

Informatica

The information being provided today is for informational purposes only. The development, release, and timing of any Informatica product or functionality described today remain at the sole discretion of Informatica and should not be relied upon in making a purchasing decision.

Statements made today are based on currently available information, which is subject to change. Such statements should not be relied upon as a representation, warranty or commitment to deliver specific products or functionality in the future.

Informatica

Agenda

1. Introduction
2. Key Vault Integration Utility - Scope & Purpose
3. Azure Key Vault - Azure portal setup
4. Methodology used for IICS connection update
5. Demo
6. Q&A

Introduction

- This webinar is intended for all IICS developers, administrators, and architects.
- The session will help you learn how to automate the process of updating the IICS connections of any type created in the Administration Service with the secret values in the Azure Key Vault using IICS Cloud Application Integration assets.

Purpose

What is the purpose of Azure Key Vault integration with IICS?

- The credentials/connection parameters for IICS Connections are stored in the Azure Key Vault Secrets.
- Update the IICS connection parameters in the higher IICS environment when imported from lower IICS environment
  - CI/CD Code Promotion
  - Assets Migration
- Update the IICS connections on schedule with password rotation.

Scope

What is the scope of Azure Key Vault integration utility?

- Automate the process of updating the IICS connections in the Administration Service
- IICS Cloud Application Integration Assets are used to automate the process
- This utility integrates the IICS connection with Azure Key Vault

Azure Key Vault

Azure portal settings for Key Vault API permission and Access Policy

Informatica

Azure Key Vault

What is Azure Key Vault?

- Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys.

Informatica

Access secret values from the Azure Key Vault

What are the various ways to access the secret values from Azure Key Vault?

REST API

- Azure REST APIs

Azure Key Vault Secret Client Library

- The Azure Key Vault secret client library allows you to manage secrets
  - Python
  - Node.js
  - Java
  - .NET
  - Go

Informatica

Authenticate Azure Key Vault in Code

How do we authenticate the Azure Key Vault in code?

- Key Vault uses Azure Active Directory (Azure AD) authentication, which requires an Azure AD security principal to grant access.
- An Azure AD security principal
  - User
  - An Application Service Principal
    - ✓ Managed Identity
    - ✓ Registering the application with azure identity platform
  - A group of any of above types
- A service principal's object ID acts like its username, service principal's client secret acts like its password.

Azure Portal settings

Permissions to be provided for your service principal application

- Assign Azure Key Vault API permission
  - Have full access to Azure Key Vault Services for the Application
- Key Vault Access Policy
  - Access policies enable you to have fine grained control over access to vault items
  - Set the privileges and principal - Application Name

Auto update of IICS Connections

Methodology used for IICS connections update

Informatica

REST APIs usage

REST APIs used in the code for automation

Azure REST APIs

- Get Bearer Access Token
- Get Key Vault Secrets list
- Get Secret Value

IICS REST APIs

- Login V2 /Login V3
- Get Connection Details
- Update Connection

Informatica

IICS REST API

- Login V2 /Login V3
  - ServerURL/BaseAPI URL
  - Session Id
- Get Connection Details
- Update Connection

Details of a particular connection

To request the details of a particular connection, include the connection ID or name in the URI. Use one of the following URIs:

```
/api/v2/connection/<id>
```

```
/api/v2/connection/name/<name>
```

If you use the connection name in the URI and the connection name includes a space, replace the space with `%20`. For example:

```
/api/v2/connection/name/my%20connection
```

POST Request

You can create or update connections. To update a connection, use the connection ID with the following URI. To create a connection, omit the optional connection ID.

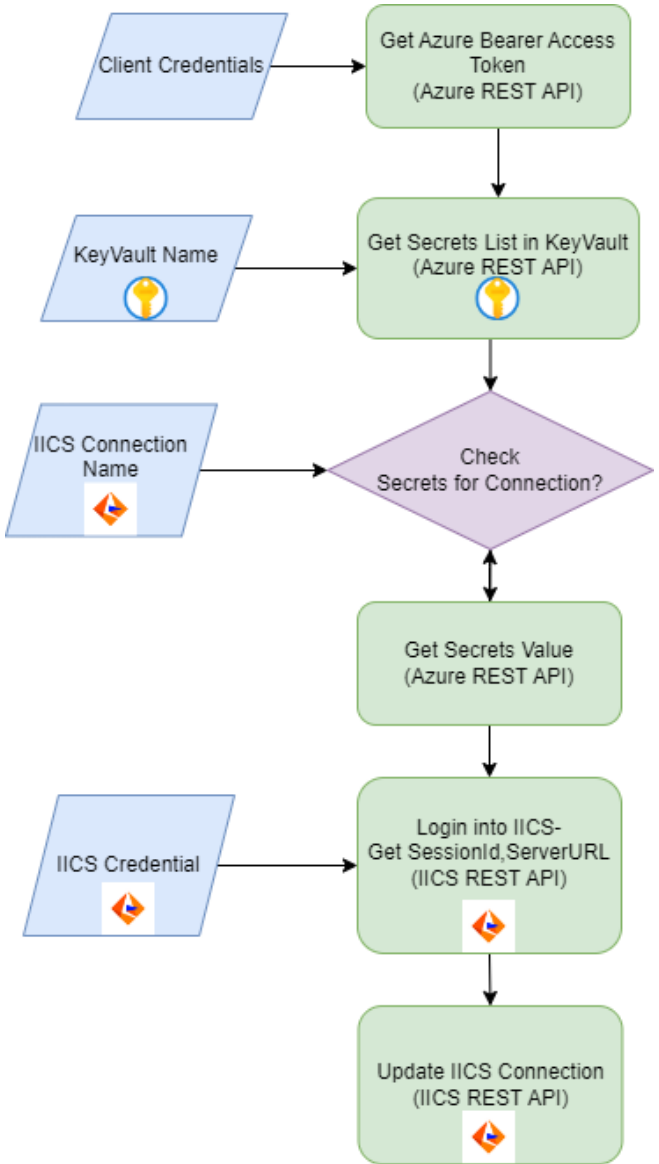
```
/api/v2/connection/<id>
```

You can submit a partial update using partial mode. To submit a request using partial mode, use a JSON request and include the following line in the header:

```
Update-Mode=PARTIAL
```

Methodology Implemented

Flowchart of the Methodology



Informatica

IICS Cloud Application Integration Assets

- Service connectors
  - Connect to the IICS REST API
  - Connect to the Azure API
- App connections
  - App connection on top of the service connector
- Cloud Application Integration process
  - Process to fetch the connection param values from Azure Key Vault and Update the IICS Connections

KeyVaultIntegration (5)

		Name	Type
☐		Conn-Azure-RESTAPI	App Connection
☐		Conn-IICS-RESTAPI	App Connection
☐		ProcessKeyVaultIntegration	Process
☐		SC_Azure_RESTAPI	Service Connector
☐		SC_IICS_RESTAPI	Service Connector

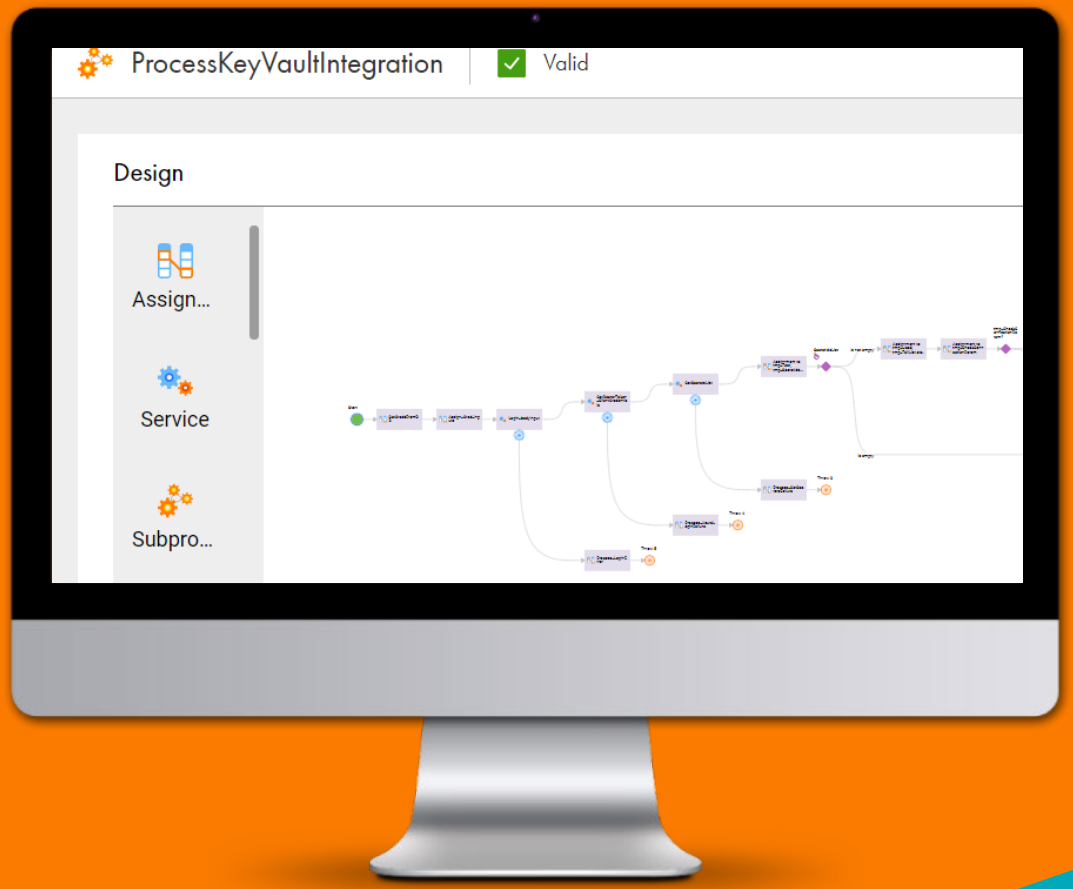
Prerequisites

- Azure Portal Key Vault Access permissions set
- Secrets in the Azure Key Vault need to be named in the following pattern - **<IICSConnectionName><ConnParamValue>**
  - **Example**- Below are the IICS Connection name and secret name for the username connection parameter.
    - IICS ConnectionName: AzureSQLServer
    - Secret name: AzureSQLServerusername
    - <ConnParamValue> need to match the parameter in the IICS REST API **GET Connection Detail** response.
- IICS Connection names should contain only alphanumeric character and dashes “-“.
- Publish the IICS Cloud Application service connectors, App connections, CAI process.

DEMO

1. Azure Portal Key Vault Permission Settings

2. IICS Cloud Application Integration Assets walkthrough, their execution



Informatica

Q&A

Informatica®

Thank you

Email: spvaidya@informatica.com