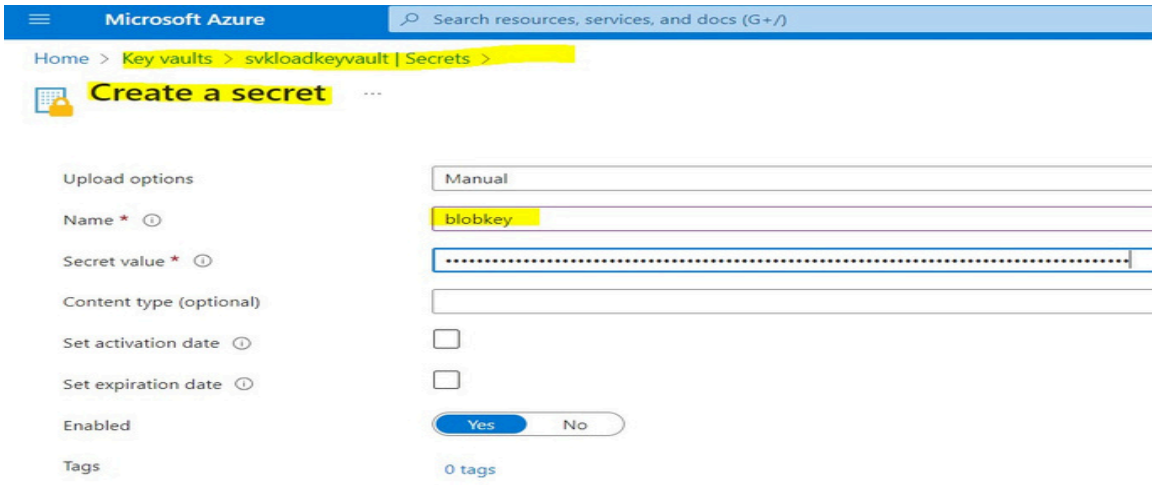
Building a Secure Azure Data Factory Pipeline with Azure Key Vault Integration In today's data-driven world, securing access to your data sources is paramount. Here's a step-by-step guide on how I created a secure Azure Data Factory (ADF) pipeline by integrating Azure Key Vault for managing secrets like storage and database connection strings.

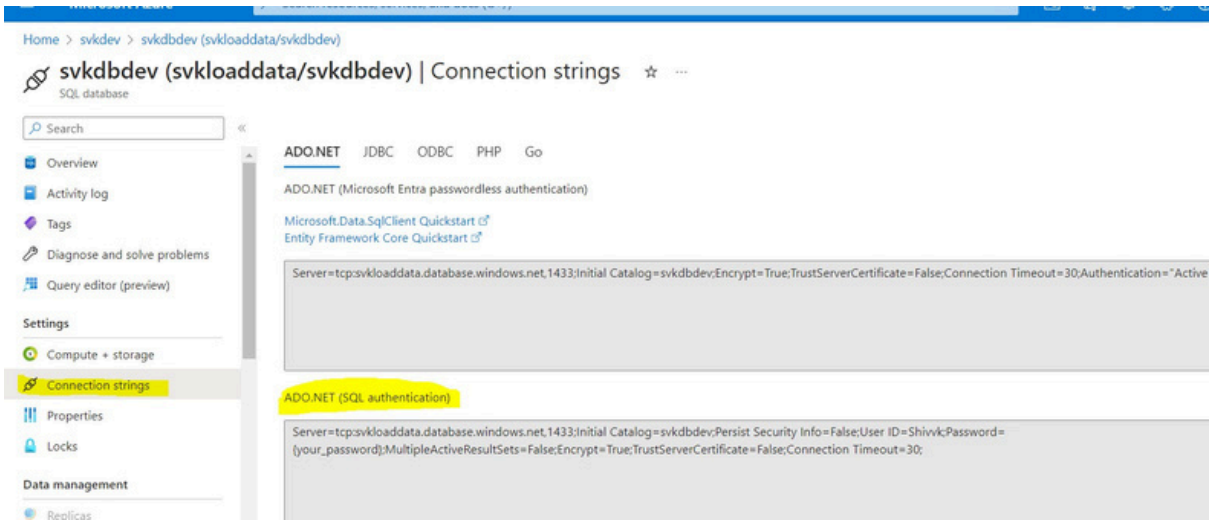
Step 1: Create a Storage Account

1. Set Up the Storage Account: Navigate to the Azure portal and create a new storage account.
2. Access Keys: Under the storage account, go to Security + Networking and select Access keys. Copy the connection string.

Step 2: Create a Key Vault

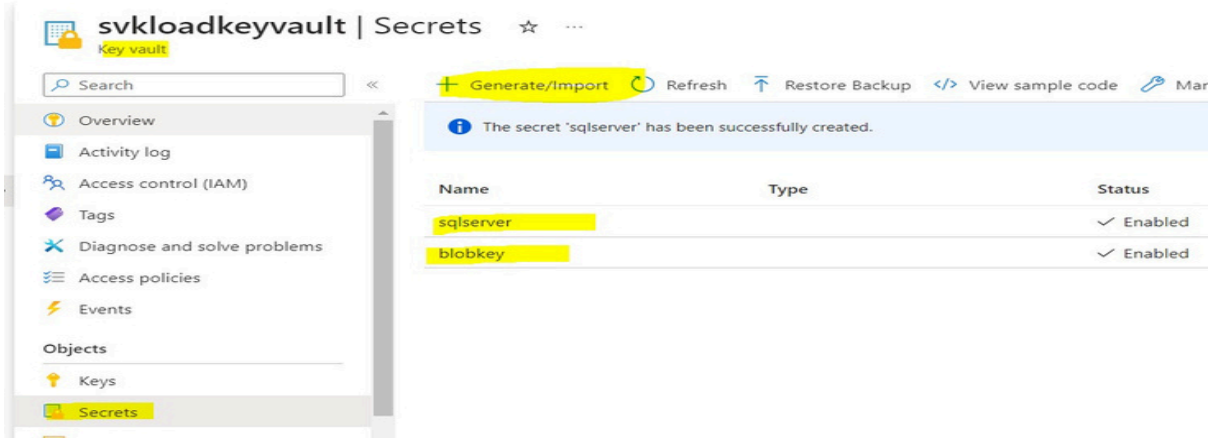
1. Set Up Key Vault : Create a new Key Vault service.
2. Generate Secrets:
   - Go to Secrets and select Generate/Import.
   - For the storage account, paste the copied connection string from the storage account's access keys. Similarly, generate a secret for your SQL server
   - connection string. Go to the SQL database, copy the ADO.NET connection string (SQL Authentication), and replace it in the Key Vault.

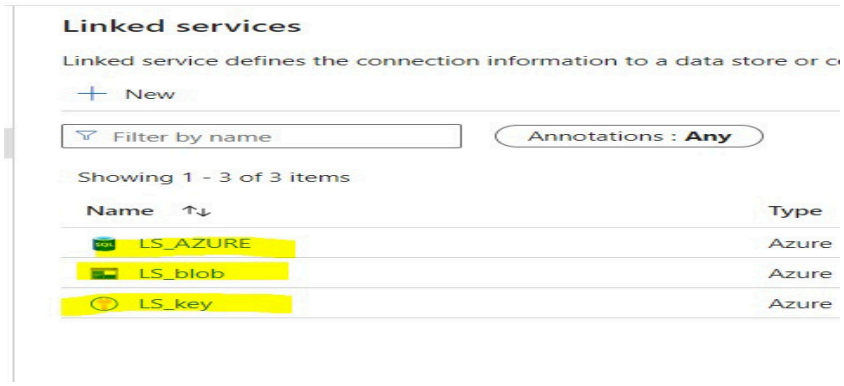




Step 3: Create Linked Services in ADF

1. Linked Service for Key Vault:
    - In ADF, create a linked service for Azure Key Vault.
    - Pass the subscription and Key Vault details created earlier.
    - Test the connection and create the linked service.
2. Linked Service for Azure SQL Database:
    - Create a linked service for the Azure SQL database in ADF.
    - Instead of a direct connection string, select Key Vault to fetch the connection string securely.

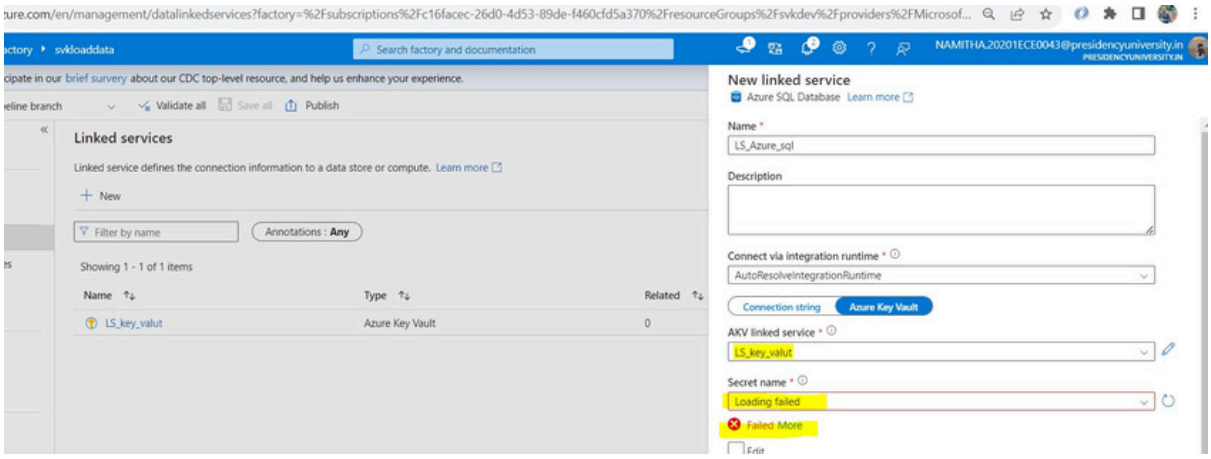




Troubleshooting Secret Access

If the secret key is not loading, follow these steps:

1. Access Policies: Go to your Key Vault and select Access Policies.
2. Create Access Policy:
   - o Click + Add Access Policy.
   - o Select Secret Permissions and add your Data Factory's managed identity as the principal.
   - o Save and create the access policy.



For more details, you can refer to the official Microsoft document .

Benefits:

Enhanced Security: By using Azure Key Vault, sensitive connection strings and secrets are securely managed.

Simplified Management: Centralized secret management simplifies configuration and reduces the risk of credential leakage.

Scalability: Easily scale your data operations with secure and efficient credential management.