Using External Secret Manager

Using an external secret manager allows you to store all data warehouse passwords in one place, and point AtScale to use it instead of typing the credentials manually. You can also store LDAP credentials in a secret manager.

About

Secret managers can be used with AtScale as follows:

- Supported products are Vault and AWS Secret Manager
- For storing passwords for data warehouses and file systems.

Prerequisites

- You should have Vault or AWS Secret Manager account already created and configured.
- Your AtScale account should be Super User.
- You know how to configure and restart the AtScale engine. For details, see Changing Engine Settings.

Enabling Secret Managers

1. In AtScale, go to Settings > Organization Settings > Engine
2. Enable and configure secret managers as follows:

   - For Vault, enable the `secret.vault.enabled` setting.

     Then enter the corresponding values for the `secret.vault.address`, `secret.vault.kvsecretsenginepath`, and `secret.vault.token` settings.

   - For AWS Secret Manager, enable the `secret.aws.enabled` setting.

     Then enter the corresponding values for the `secret.aws.accesskey`, `secret.aws.accesskeyid`, and `secret.aws.region` settings.

3. Save the settings and restart the Engine.

Configuring Connections

1. Make sure the steps in the Enabling secret managers section above are completed.
2. In AtScale, go to Settings > Organization Settings > Data Warehouses.
3. Choose a data warehouse, locate the connection you need, and choose the Edit button.
4. In the Edit Connection dialog, locate the Authorization section and enter the path and key (when using Vault), or the ARN and key (when using AWS).

5. Save your changes.

For more information, see Adding Data Warehouses.

Configuring LDAP Directories

1. Make sure the steps in the Enabling secret managers section above are completed.

2. In AtScale, go to Security > Directory > Setup.

3. Select Custom Directory.

4. Locate the Vault Credentials (or AWS Credentials) section, and enter the credentials.

5. Save your changes.

For more information, see Connecting to an LDAP Server or Microsoft Active Directory and Azure AD.