Fetch secret values from the Azure Key Vault

Last Modified on 04/29/2021 8:03 am EDT

V9.6.1

Overview

You can use an Azure Key Vault to securely store tokens, passwords, certificates, and other secret values like connection strings. It also helps you to manage encryption keys and certificates. With Azure Key Vault there are almost no chances that secret values may be accidentally leaked as the values are no longer stored in the Cora SeQuence application configuration files.

Functionality

The Azure Key Vault keeps secure your secret values in the configuration files and prevents them from getting accidentally leaked or stolen.

To apply these configurations, use the Set-CoraSeQuenceApplicationConfiguration PowerShell function.

Prerequisites

You need to have an Azure Key Vault to store the secrets. In addition, you need to create an Azure Active Directory Application and service principal that is used to access the secrets. You also need to create a secret for the application.

For the key vault you have created for the service principal, grant a minimum of “Get” and “List” permissions using the access policy.

Add the following environment variables on the Cora SeQuence machine:

Environment variable	Description
AZURE_TENANT_ID	the ID of the tenant (directory) where the AD application is registered
AZURE_CLIENT_ID	the ID of the application (client) that you created to read the secrets
AZURE_CLIENT_SECRET	the secret for the Azure Active Directory application
SEQ_KEYVAULT_NAME	the name of the key vault that holds the secrets
ENV_PREFIX (Optional)	the prefix for the names of the secrets in the vault

Make sure to follow the exact naming convention for all the environment variables.

Using the Azure Key Vault configurations

You can use the following Azure Key Vault configurations to pull secret information from an Azure Key Vault.

Azure Key Vault configuration name	Parent configuration	Secret
AzureKeyVaultFilesStorageConnection	None	• Credentials: Cora SeQuence encrypted credentials to connect to the database • Connection string: the connection string to the Cora SeQuence database.
AzureKeyVaultPersistence	AddFilesStorageConnection	filesStorage-storageProviders--connection-connection string to the storage provider The Name of the provider must be same as the name configured in the application.
AzureKeyVaultOpenIdConnect	OpenIdConnect	identity-openIdConnect-ClientSecret

The system automatically applies the matching standard configurations for Azure Key Vaults however, you need to provide token values of the standard configuration. Parent configurations indicate that additional transformations will take place. While applying configurations, provide the tokens required by the parent configurations.