Содержание

Настройка хранения строк подключения в Hashicorp Vault

Начиная с версии системы 3.30, чтобы повысить безопасность хранения секретов (паролей, токенов/маркеров-доступа, API-ключей, закрытых криптографических ключей и т.п.) можно настроить подключение системы ADVANTA к СУБД или сервису Active Directory через сервис хранения секретов HashiCorp Vault.

В этом случае в системе или файлах конфигурации не будут храниться пароли к сервисам и службам компании.

Для этого в настройках конфигурационного файла системы `client.config` необходимо:

1. Добавить раздел с указанием использования сервиса хранения секретов.
2. Добавить раздел с перечнем ключей, получаемых из сервиса хранения секретов для строк соединения с СУБД.
3. Добавить раздел для получения секрета для сервисов Active Directory (если используется).
4. После получения секретов, добавить алгоритм замены паролей - выполняется получение всех секретов и их перечень интерпретируется как набор именованных ключей, после чего, выполняется подстановка значений найденных ключей на их значение.

Изменения в конфигурационном файле

Необходимые изменения в конфигурационном файле `client.config` для запуска системы через получение паролей из сервиса хранения секретов HashiCorp Vault:

1. В разделе `<configSections>` добавить обработку наличия секции `<section name=″hashiCorpVault″ type=″Config.HashiCorpVaultConfigurationSection, SL.App.Config″/>`, которая будет использоваться как индикатор необходимости использовать Hashicorp Vault.
2. В разделе `<configuration>` добавить проверку и обработку секций: `<hashiCorpVault address=″″ roleId=″″ secretId=″″ version=″″ mountPoint=″″ path=″″/>`.

Секция `hashiCorpVault` содержит обязательные атрибуты:

- `address` – адрес сервера Vault, обязательный;
- `roleId` – идентификатор (GUID) роли, обязательный;
- `secretId` – идентификатор (GUID) секрета, обязательный;
- `version` – обязательный параметр, версия контейнера. Возможные варианты: V1, V2.
- `mountPoint` – обязательный параметр, точка монтирования контейнера секретов;
- `path` - обязательный параметр, путь к секретам.

Примеры фрагментов из конфигурационного файла

В конфигурационном файле `client.config` выполняется поиск ключей вида `{$key$}` и

замена их на значения keyValue, полученные из Vault.

При наличии в секции <configuration> секции <hashiCorpVault address="" roleId="" secretId="" version="" mountPoint="" path=""/>, пароли будут считаны из хранилища секретов как названия ключей и их значений (пары key, keyValue), для последующей замены.

> Названия ключей в хранилище секретов должны соответствовать всем {key} в заменяемых фрагментах.

Проверяются на наличие строк шаблона разделы файла конфигурации:

- настройки приложения - секция <appSettings>, атрибут value;
- настройки Active Directory - секция <adDomains>/<domains>, атрибуты: login, password, ldappath;
- настройки openIdConnect - секция <openIdConnect>/<providers>, атрибут clientSecret.

Пример фрагмента из client.config:

```
<configuration>
  <hashiCorpVault address="https://vault.yourcompany.ru:8200"
roleId="roleId" secretId="secretId" version="V2" mountPoint="kv-v2"
path="dbPasswords"/>
.....
</configuration>

.....
  <connectionStrings>
    <add name="db" providerName="System.Data.SqlClient"
connectionString="Server=localhost;Database=b-stable;User
ID=SL_APP;Password={$db$};Pooling=true;Max Pool Size=4000;
TrustServerCertificate=True" />
    <add name="dbCubes" providerName="System.Data.SqlClient"
connectionString="Server=localhost;Database=b-stable;User
ID={$busDB$};Password={$dbCubes$};Pooling=true;Max Pool Size=4000;
TrustServerCertificate=True" />
  </connectionStrings>
```

> В примере для двух connectionString name="db" и "dbCubes", размещены ключи: {db}, {$busDB$}, {$dbCubes$} - они будут заменены на их значения из хранилища секретов.