Содержание

Настройка хранения строк подключения в Hashicorp Vault

Начиная с версии системы 3.29, 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).

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 `<section name= ″hashiCorpVault″ type=″Config.HashiCorpVaultConfigurationSection, smcorelib″/>`, параметр будет использоваться как индикатор необходимости использовать Hashicorp Vault.
2. В разделе `<configuration>` добавить следующие секции:

- `<hashiCorpVault address=″″ roleId=″″ secretId=″″>` с закрывающим тэгом `</hashiCorpVault>`;
- внутри секции `hashiCorpVault` добавить список контейнеров `<containers>.....</containers>` в которой будет располагаться список контейнеров для заполнения из Hashicorp.

> Формат описания одного контейнера: `<add id=″″ version=″″ mountPoint=″″ path=″″/>`, где id – название контейнера.
>
> Доступны названия:
>
> - `adDomainPasswords` – для Active Directory;
> - `dbPasswords` – для `connectionString` в СУБД.

Параметры для обращения к серверу Hashicorp Vault:

- `address` – адрес сервера Vault, обязательный;
- `roleId` – идентификатор (GUID) роли, обязательный;
- `secretId` – идентификатор (GUID) секрета, обязательный.

Параметры для контейнеров, их может быть 2 вида:

1. `dbPasswords` – контейнер для хранения паролей для подключения к БД, в нем указываются параметры доступа в Hashicorp Vault, где размещен список хранимых секретов для СУБД. Перечень названий параметров, которые могут быть размещены в контейнер совпадает с набором `connectionString` из файла конфигурации:

- `db` – основная база системы;
- `dbCubes` – база для хранения вынесенных кубов;
- `busDb` – база хранения данных для шины;
- `sqlServerCacheDb` – база хранения кэша.

2. `adDomainPasswords` – контейнер для хранения паролей учетных записей Active Directory. В этом контейнере обрабатывается один параметр: `DOMAIN_NAME`.

Общие параметры:

1. `version` – обязательный параметр, версия контейнера. Возможные варианты: V1, V2.
2. `mountPoint` – обязательный параметр, точка монтирования контейнера секретов.
3. `path` - обязательный параметр, путь к секретам.

Примеры фрагментов из конфигурационного файла