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).

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

При наличии секции <add id=″dbPasswords« version=″″ mountPoint=″″ path=″″/> пароли будут считаны из хранилища секретов. При этом названия ключей в хранилище должны соответствовать параметру name в секции connectionStrings.

При отсутствии ключа какой-либо connectionString, пароль для этой строки подключения считан из хранилища не будет. Пароль, указанный в connectionString, будет заменен паролем из хранилища. Если пароль в connectionString не задан, то он будет добавлен в строку подключения.

Пример фрагмента из client.config:

```
<add id="dbPasswords" version="V2" mountPoint="kv-v2" path="dbPasswords"/>
……..
<connectionStrings>

        <add name="db" providerName="System.Data.SqlClient"
connectionString="Server=localhost;Database=b-stable;User
ID=SL_APP;Password=123;Pooling=true;Max Pool Size=4000;
TrustServerCertificate=True"/>

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

```
  </connectionStrings>
```

> В примере для connectionString name=″db″, пароль '123', указанный в конфигурации, будет заменен на пароль из хранилища секретов.
> К остальным строкам подключения будет добавлен пароль из хранилища секретов.

При наличии секции <add id=″adDomainPasswords″ version=″″ mountPoint=″″ path=″″/> пароли будут считаны из хранилища секретов, но выполняется она не при старте приложения, а при действиях, для которых необходима учетная запись Active Directory. При этом названия ключей в хранилище должны соответствовать параметру name в секции domains.

Пример фрагмента из client.config:

```
<add id="adDomainPasswords" version="V2" mountPoint="kv-v2"
path="adDomainPasswords"/>
…….
<adDomains>

    <domains>

      <add name="DOMAIN_NAME" login="login" password="password"
ldappath="LDAP://DC=domain_name,DC=local"/>;

    </domains>

  </adDomains>
```

> В примере для domain name=″DOMAIN_NAME″, пароль 'password' указанный в конфигурации будет заменен на пароль из хранилища секретов.

From:
https://wiki.a2nta.ru/ - **Wiki [3.x]**

Permanent link:
https://wiki.a2nta.ru/doku.php/product/settings/system/vault?rev=1727093695

Last update: **23.09.2024 12:14**