Log Server

Компонент **Indeed Log Server** позволяет записывать события со всех серверов Рутокен KeyBox в единый журнал Windows Event Log, СУБД Microsoft SQL Server, PostgreSQL Server, SysLog Server.

Компонент устанавливается на одном из серверов Рутокен KeyBox или на отдельной рабочей станции (в домене или вне его). Системные требования для установки компонента совпадают с требованиями к серверу Рутокен KeyBox.

Установка Indeed Log Server

1. Выполните вход на рабочую станцию с правами локального администратора.
2. Запустите **Indeed.LogServer.msi** из дистрибутива (каталог Indeed.Log.Server) и выполните его установку следуя указаниям Мастера.
3. Из каталога **Indeed.Log.Server** скопируйте файлы:
    - В каталог **C:\inetpub\wwwroot\ls** скопируйте **cmSchema.config.**
    - В каталог **C:\inetpub\wwwroot\ls\targetConfigs** скопируйте **cmEventLogTarget.config**, **cmMsSqlTarget.config**, **cmPgSqlTarget.config** и **cmSysLogTarget.config**.

Indeed Log Server поддерживает чтение событий только из одного хранилища (<ReadTargetId>), запись событий возможна одновременно в несколько хранилищ (<WriteTargets>).
Для применения настроек после сохранения изменений в файлах необходимо перезапустить IIS.

Настройка чтения и записи событий в Windows Event Log

1. Перейдите в каталог **C:\inetpub\wwwroot\ls** и отредактируйте файл **clientApps.config** следующим образом:

    - В секции **Applications** добавьте:

    ```
    <Application Id="cm" SchemaId="cmSchema">
        <ReadTargetId>cmEventLogTarget</ReadTargetId>
        <WriteTargets>
            <TargetId>cmEventLogTarget</TargetId>
        </WriteTargets>
        <AccessControl>
            <!--<CertificateAccessControl CertificateThumbprint="001122...AA11" Rights="Read" />-->
        </AccessControl>
    </Application>
    ```

    - В секции **Targets** добавьте новый элемент:

    ```
    <Targets>
        <Target Id="cmEventLogTarget" Type="eventlog"/>
    </Targets>
    ```

2. Сохраните изменения и закройте файл конфигурации.

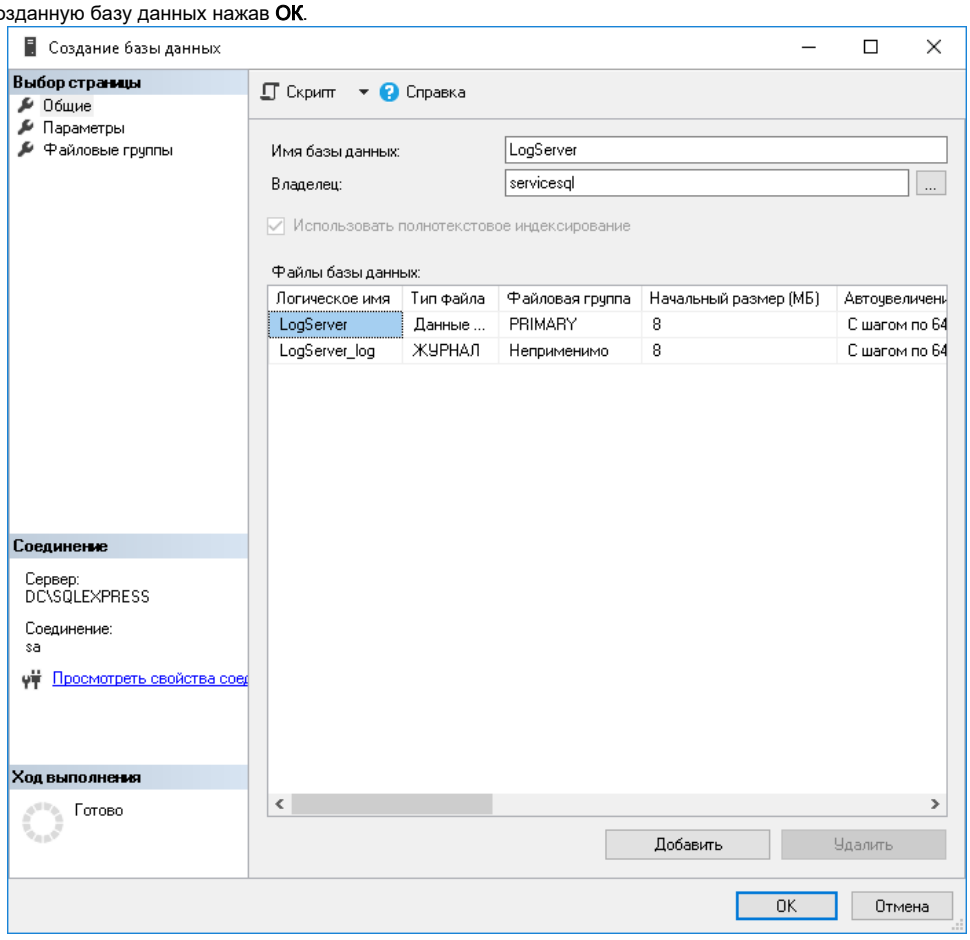
Настройка чтения и записи событий в СУБД MS SQL

База для хранения данных Indeed Log Server создается вручную, а её наполнение происходит автоматически.

1. Создайте базу данных в среде SQL Management Studio с произвольным именем:
    - В окне **Обозреватель объектов** (Object Explorer) нажмите правой кнопкой мыши по вкладке **Базы данных** (Databases).
    - Выберите **Создать базу данных...** (New Database...).
    - Укажите **Имя базы данных:** (Database name:) например, **LogServer**.
    - В поле **Владелец:** (Owner:) определите владельца создаваемой базы.

    Создайте (например, **servicesql**) или выберите любую внутреннюю учетную запись SQL, или учетную запись Active Directory (например, сервисную учетную запись для работы RutokenKeyBox: **servicecm**). Указанная учетная запись после создания базы будет обладать правами **db_owner, public** и будет использоваться системой для выполнения операций записи/чтения в базу данных.

- Сохраните созданную базу данных нажав **OK**.



2. Перейдите в каталог **C:\inetpub\wwwroot\ls\targetConfigs** и отредактируйте файл **cmMsSqlTarget.config** в соответствии с настройками ниже: **<Settings> … </Settings>**:
   - **Data Source** - имя сервера Microsoft SQL Server или именованного экземпляра Microsoft SQL Server
   - **Database** - имя базы данных (ILS)
   - **User Id** - сервисная учётная запись для работы с базами данных Рутокен KeyBox
   - **Password** - пароль сервисной учётной записи

   ```
   <Settings>
       <ConnectionString>Data Source=MSSQL\SQLEXPRESS;Database=LogServer;User Id=servicesql;
   Password=P@ssw0rd</ConnectionString>
   </Settings>
   ```

   В случае использования именованного экземпляра Microsoft SQL Server значение параметра **Server** необходимо задавать в формате **<имя сервера>\<имя экземпляра>**.

   ```
   <Settings>
       <ConnectionString>Server=sql\Named instance; ... </ConnectionString>
   </Settings>
   ```

3. Отредактируйте **C:\inetpub\wwwroot\ls\clientApps.config** для работы с файлом **cmMsSqlTarget.config**:

   - В секции **Application** добавьте:

```
<Application Id="cm" SchemaId="cmSchema">
    <ReadTargetId>cmMsSqlTarget</ReadTargetId>

    <WriteTargets>
        <TargetId>cmMsSqlTarget</TargetId>
    </WriteTargets>

    <AccessControl>
        <!--<CertificateAccessControl CertificateThumbprint="001122...AA11" Rights="Read" />-->
    </AccessControl>
</Application>
```

- В секции **Targets** добавьте новый элемент:

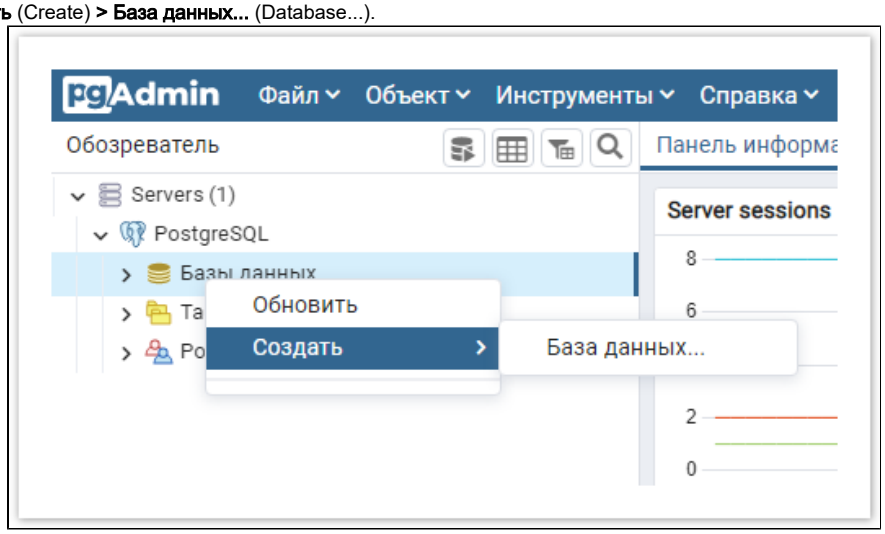
```
<Targets>
    <Target Id="cmMsSqlTarget" Type="mssql"/>
</Targets>
```

4. Сохраните изменения и закройте файл конфигурации.

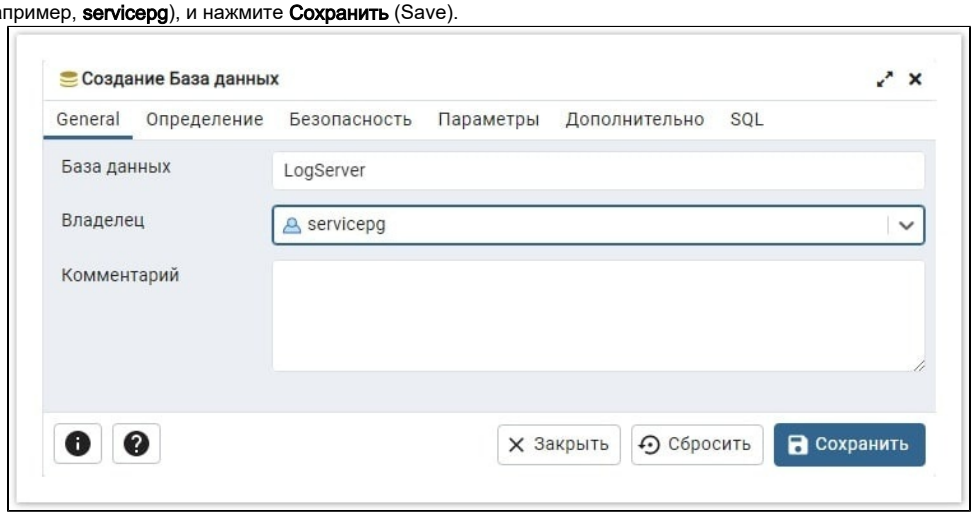
Настройка чтения и записи событий в СУБД PostgreSQL

База для хранения данных Indeed Log Server создается вручную, а её наполнение происходит автоматически.

1. В СУБД PostgreSQL (например, в среде **pgAdmin)** создайте базу данных:
   - В окне **Обозреватель** (Browser) нажмите правой кнопкой мыши по пункту **Базы данных** (Databases).
   - Выберите **Создать** (Create) **> База данных...** (Database...).



   - На вкладке **Общие** (General) укажите произвольное название базы данных в поле **База данных** (Database), например, **LogServer**, выберите из списка **Владелец** (Owner) сервисную учетную запись, которая будет использоваться для подключения к базе данных (например, **servicepg**), и нажмите **Сохранить** (Save).



2. Предоставление привилегий сервисной учётной записи на таблицы базы данных:

- Выделите созданную базу данных в списке и перейдите в меню **Запросник** (Query Tool) (нажатием на кнопку  или комбинацией клавиш ALT+SHIFT+Q)
- Введите текст запроса, указав в запросе имя учётной записи:

```
GRANT ALL PRIVILEGES ON ALL TABLES  IN SCHEMA public TO "     ";
```

- В меню **Запросник** нажмите на кнопку **Выполнить** (Execute/Refresh)  .

3. По умолчанию в PostgreSQL разрешены только локальные подключения к базам данных, поэтому для работы между различными серверами требуется настройка удалённого подключения к БД:

- В каталоге PostgreSQL откройте конфигурационный файл **pg_hba.conf.**

Расположение файла pg_hba.conf

Для Windows — `C:\Program Files\PostgreSQL\< >\data`

Для *nix — `/etc/postgresql/< >/main`

- В конце файла добавьте строку следующего типа:

```
CONNECTIONTYPE DATABASE USER ADDRESS METHOD
```

Где:

- **CONNECTIONTYPE** - Тип подключения. Указывается "host" - будет использоваться подключение по TCP/IP.
- **DATABASE** - Имя базы данных, для которой предоставляется доступ (ALL для доступа ко всем базам данных).
- **USER** - Имя пользователя, для которого будет доступно подключение (ALL для доступа всех пользователей).
- **ADDRESS** - IP-адрес удалённого сервера RutokenKeyBox (0.0.0.0/0 для доступа с любых адресов).
- **METHOD** - Метод аутентификации пользователя (например, md5, scram-sha-256).
  Примеры:

```
host LogServer servicepg 192.200.1.0/24 md5
host ALL servicepg 10.0.0.0/8 md5
host ALL ALL 0.0.0.0/0 scram-sha-256
```

4. В каталоге **C:\inetpub\wwwroot\ls\targetConfigs** отредактируйте файл **cmPgSqlTarget.config** в соответствии с настройками ниже: **<ConnectionString> … </ConnectionString>**:
   - **Host** - имя сервера PostgreSQL Server
   - **Port** - порт для подключения к СУБД PostgreSQL (5432 — значение по умолчанию)
   - **Database** - имя созданной в п.1 базы данных
   - **Username** - сервисная учётная запись для подключения к указанной базе данных
   - **Password** - пароль сервисной учётной записи

```
<Settings>
  <ConnectionString>Host=SRV-POSTGRESQL;Port=5432;Database=LogServer;Username=servicepg;
Password=P@ssw0rd</ConnectionString>
</Settings>
```

5. В файле **C:\inetpub\wwwroot\ls\clientApps.config** отредактируйте секцию **<Application>** для работы с файлом **cmPgSqlTarget.config** – добавьте новый TargetId для ReadTarget, WriteTarget:

```
<Application Id="cm" SchemaId="cmSchema">
    <ReadTargetId>cmPgSqlTarget</ReadTargetId>

    <WriteTargets>
        <TargetId>cmPgSqlTarget</TargetId>
    </WriteTargets>

    <AccessControl>
        <!-- <CertificateAccessControl CertificateThumbprint="001122...AA11" Rights="Read" /> -->
    </AccessControl>
</Application>
```

В том же файле отредактируйте секцию **<Target>** для работы с файлом **cmPgSqlTarget.config**

```
<Targets>
    <Target Id="cmPgSqlTarget" Type="pgsql"/>
</Targets>
```

Настройка записи событий в Syslog

Возможности Syslog ограничены только записью событий (<WriteTargets>). В данном примере дополняется конфигурация из предыдущего примера с PostgreSQL.

1. В каталоге **C:\inetpub\wwwroot\ls\targetConfigs** отредактируйте файл **cmSysLogTarget.config** в соответствии с настройками ниже: **<ConnectionString> … </ConnectionString>**:
    - **HostName** - имя или IP-адрес Syslog сервера.
    - **Port** - порт Syslog сервера (514 — порт по умолчанию).
    - **Protocol** - тип подключения к Syslog серверу: UDP, TCP, TCPoverTLS.
    - **Format** - опциональный параметр, определяет формат логов: Plain, CEF, LEEF.
    - **SyslogVersion** - опциональный параметр, спецификация протокола: RFC3164, RFC5424.

    ```
    <Settings HostName="SRV-SYSLOG" Port="514" Protocol="UDP"/>
    ```
2. В файле **C:\inetpub\wwwroot\ls\clientApps.config** отредактируйте секцию **<Application>** для работы с файлом **cmSysLogTarget.config** – добавьте новый TargetId для WriteTarget:

```
<Applications>
    <Application Id="cm" SchemaId="cmSchema">
        <ReadTargetId>cmPgSqlTarget</ReadTargetId>

        <WriteTargets>
            <TargetId>cmPgSqlTarget</TargetId>
            <TargetId>cmSysLogTarget</TargetId>
        </WriteTargets>

        <AccessControl>
            <!-- <CertificateAccessControl CertificateThumbprint="001122...AA11" Rights="Read" /> -->
        </AccessControl>
    </Application>
</Applications>
```

В том же файле отредактируйте секцию **<Target>** для работы с файлом **cmSysLogTarget.config**

```
<Targets>
    <Target Id="cmPgSqlTarget" Type="pgsql"/>
    <Target Id="cmSysLogTarget" Type="syslog"/>
</Targets>
```

Файлы

cmEventLogTarget.config
cmMsSqlTarget.config
cmPgSqlTarget.config
cmSchema.config
cmSysLogTarget.config