Log Server

Indeed Log Server поддерживает работу с:

- **СУБД Microsoft SQL Server**
- **СУБД PostgreSQL, PostgreSQL Pro**
- **Syslog сервером** (вывод в форматах Plain, CEF и LEEF)

Чтение событий поддерживается только из одного хранилища (<ReadTargetId>), запись событий возможна одновременно в несколько хранилищ (<WriteTargets>).

Настройка чтения и записи событий в СУБД

Microsoft SQL Server

1. Перейдите в каталог **C:\inetpub\wwwroot\ls\targetConfigs**, создайте копию файла sampleDb.config и переименуйте её в **mssqlDb.config**, затем отредактируйте файл **mssqlDb.config** в соответствии с настройками ниже:
   <Settings> … </Settings>:
   - **Data Source** - имя сервера Microsoft SQL Server или именованного экземпляра Microsoft SQL Server
   - **Initial Catalog** - имя базы данных (ILS)
   - **User ID** - сервисная учётная запись для работы с базами данных Indeed PAM
   - **Password** - пароль сервисной учётной записи

   ```
   <Settings>
       <ConnectionString>Server=sql.domain.local; Initial Catalog=ILS; Integrated Security=False; User ID=IPAMSQLServiceOps; Password=Password</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>
   ```

2. В файле **C:\inetpub\wwwroot\ls\clientApps.config** отредактируйте секцию **pam** для работы с файлом mssqlDb.config:

   ```
   <Application Id="pam" SchemaId="Pam.Schema">
    <ReadTargetId>mssqlDb</ReadTargetId>
    <WriteTargets>
     <TargetId>mssqlDb</TargetId>
    </WriteTargets>
    <AccessControl>
     <!--<CertificateAccessControl CertificateThumbprint="001122...AA11" Rights="Read" />-->
    </AccessControl>
   </Application>
   ```

3. Далее в этом же файле в секции **Targets** добавьте новый элемент:

   ```
   <Targets>
    ...
    <Target Id="mssqlDb" Type="mssql"/>
   </Targets>
   ```

PostgreSQL, PostgreSQL Pro

1. Перейдите в каталог **C:\inetpub\wwwroot\ls\targetConfigs**, создайте копию файла sampleDb.config и переименуйте её в **postgresDb.config**, затем отредактируйте файл **postgresDb.config** в соответствии с настройками ниже:
   <Settings> ... </Settings>:
   - **Host** - имя сервера PostgreSQL / PostgreSQL Pro или именованного экземпляра PostgreSQL
   - **Database** - имя базы данных (ILS)
   - **Username** - сервисная учётная запись для работы с базами данных Indeed PAM
   - **Password** - пароль сервисной учётной записи

   ```
   <Settings>
       <ConnectionString>Server=sql.domain.local; Database=ILS; Integrated Security=False;
   Username=IPAMSQL; Password=Password</ConnectionString>
   </Settings>
   ```

2. В файле **C:\inetpub\wwwroot\ls\clientApps.config** отредактируйте секцию **pam** для работы с файлом postgresDb.config:

   ```
   <Application Id="pam" SchemaId="Pam.Schema">
    <ReadTargetId>postgresDb</ReadTargetId>
    <WriteTargets>
     <TargetId>postgresDb</TargetId>
    </WriteTargets>
    <AccessControl>
     <!--<CertificateAccessControl CertificateThumbprint="001122...AA11" Rights="Read" />-->
    </AccessControl>
   </Application>
   ```

3. Далее в этом же файле в секции **Targets** добавьте новый элемент:

   ```
   <Targets>
    ...
    <Target Id="postgresDb" Type="pgsql"/>
   </Targets>
   ```

Настройка записи событий в Syslog

1. Перейдите в каталог **C:\inetpub\wwwroot\ls\targetConfigs**, создайте копию файла sampleSyslog.config и переименуйте её в **Syslog.config**, затем отредактируйте в соответствии с настройками ниже:
   <Settings> … </Settings>:
   - **HostName** - имя Syslog сервера
   - **Port** - порт Syslog сервера
   - **Protocol** - тип подключения к Syslog серверу: TCPoverTLS, TCP, UDP
   - **Format** - формат логов: Plain, CEF, LEEF
   - **SyslogVersion** - спецификация протокола: RFC3164, RFC5424

   ```
   <Settings HostName="localhost" Port="5081" Protocol="TCP" Format="CEF"
   SyslogVersion="RFC3164" />
   ```

2. В файле **C:\inetpub\wwwroot\ls\clientApps.config** отредактируйте секцию **pam** для работы с файлом Syslog.config - добавьте новый TargetId для WriteTarget:

   ```
   <Application Id="pam" SchemaId="Pam.Schema">
    <ReadTargetId>mssqlDB</ReadTargetId>
    <WriteTargets>
     <TargetId>mssqlDB</TargetId>
     <TargetId>Syslog</TargetId>
    </WriteTargets>
    <AccessControl>
     <!--<CertificateAccessControl CertificateThumbprint="001122...AA11" Rights="Read" />-->
    </AccessControl>
   </Application>
   ```

3. Далее в этом же файле в секции **Targets** добавьте новый элемент:

   ```
   <Targets>
    ...
      <Target Id="mssqlDb" Type="mssql"/>
    <Target Id="Syslog" Type="syslog"/>
   </Targets>
   ```

Пример настройки записи событий одновременно в СУБД PostgreSQL и Sy

1. Перейдите в каталог **C:\inetpub\wwwroot\ls\targetConfigs** и создайте файлы **postgresDb.config**, **Syslog.config** как было описано выше.
2. В файле **C:\inetpub\wwwroot\ls\clientApps.config** отредактируйте секцию **pam**:

```
<Application Id="pam" SchemaId="Pam.Schema">
 <ReadTargetId>postgresDb</ReadTargetId>
 <WriteTargets>
  <TargetId>postgresDb</TargetId>
  <TargetId>Syslog</TargetId>
 </WriteTargets>
 <AccessControl>
  <!--<CertificateAccessControl CertificateThumbprint="001122...AA11" Rights="Read" />-->
 </AccessControl>
</Application>
```

3. Далее в этом же файле в секции **Targets** добавьте строки для **postgresDB** и **Syslog**:

```
<Targets>
    ...
 <Target Id="postgresDb" Type="pgsql"/>
 <Target Id="Syslog" Type="syslog"/>
</Targets>
```

После сохранения изменений в файлах необходимо перезапустить IIS.