

Установка и настройка Indeed AM Log Server с хранилищем в EventLog

Информация

Файлы для **Indeed AM Log Server** расположены: *indeed AM\Indeed AM Log Server*
\<Номер версии>

- **IndeedAM.LogServer-x64.ru-ru.msi** - Пакет для установки Indeed Log Server.
- **IndeedAM.Server.EventLog-x64.ru-ru.msi** - Пакет для создания необходимой структуры журнала в Windows EventLog.

Установка

1. Выполнить установку Indeed AM Log Server через запуск инсталлятора **Indeed.LogServer-x64.ru-ru.msi**.
2. Добавить привязку **https** в настройках **Default Web Site** в IIS Manager.

Информация

Indeed Log Server является Web приложением, которое работает на базе IIS, в процессе установки для него по умолчанию включается обязательно требование SSL в настройках, что в свою очередь требует включенной привязки https.

Если вы не намерены использовать протокол https, необходимо отключить требование SSL в настройках IIS для logserver.

- a. Запустите **IIS Manager** и раскройте пункт **Сайты (Sites)**.
 - b. Выберите сайт **Default Web Site** и нажмите **Привязки (Bindings)** в разделе **Действия (Actions)**.
 - c. Нажмите **Добавить (Add)**:
 - i. **Тип (Type)** - https.
 - ii. **Порт (Port)** - 443.
 - iii. Выберите **SSL-сертификат (SSL Certificate)**.
 - d. Сохраните привязку.
3. Выполнить установку Indeed EventLog через запуск инсталлятора **IndeedAM.Server.EventLog-x64.ru-ru.msi**.

Редактирование конфигурационного файла.

1. Откройте конфигурационный файл сервера **clientApps.config** (C:\inetpub\wwwroot\ils\clientApps.config).
2. Для блока с "**Application Id**='ea'" в тегах **TargetId** и **ReadTargetId** указать **sampleEventLog**.

Информация

В тегах **ReadTargetId** указывается идентификатор хранилища откуда будет осуществляться чтение событий.

В блоке **WriteTargets**, в тегах **TargetId**, указывается идентификатор хранилища куда будет осуществляться запись событий.

Идентификаторы заданы в теге **<Targets>...</Targets>**, конфигурационные файлы для каждого типа находится в папке **targetConfigs** с соответствующим именем.

Пример

```
<Application Id="ea" SchemaId="eaSchema">
  <ReadTargetId>sampleEventLog</ReadTargetId>
  <WriteTargets>
    <TargetId>sampleEventLog</TargetId>
  </WriteTargets>
  <AccessControl>
    <!--<CertificateAccessControl CertificateThumbprint="001122...AA11" Rights="Read" />-->
  </AccessControl>
</Application>
```

Пример отображения.

- Отображения журнала в Indeed AM Admin Console.

Журнал

Тип события

Не задано

С

02.10.2018 00:00

До

06.10.2018 00:00

Пользователь

Имя учетной записи

Описание содержит

Сервис

Не задано

Пользователь / Инициатор

Имя учетной записи

Событие

Q

Событие	Описание	Время	Сервис	Инициатор	Пользователь
1033	Пользователь Admin Indeed чер...	05.10.2018 11:10:48	Authenticator Management	Admin Indeed	Admin Indeed
1033	Пользователь Admin Indeed чер...	05.10.2018 11:10:34	Authenticator Management	Admin Indeed	Admin Indeed
1028	Пользователь Admin Indeed чер...	05.10.2018 11:10:34	User Access Control Management	Admin Indeed	Admin Indeed
1000	Пользователь был успешно ауте...	05.10.2018 11:10:33	User Access Control Management	Admin Indeed	None
1028	Пользователь Admin Indeed чер...	05.10.2018 11:10:33	User Access Control Management	Admin Indeed	Admin Indeed
1028	Пользователь Admin Indeed чер...	05.10.2018 11:10:33	User Access Control Management	Admin Indeed	Admin Indeed
1028	Пользователь Admin Indeed чер...	05.10.2018 11:10:33	User Access Control Management	Admin Indeed	Admin Indeed
1000	Пользователь был успешно ауте...	05.10.2018 11:10:33	Enterprise Management Console	Admin Indeed	None
1020	Пользователь Admin Indeed выд...	05.10.2018 11:10:33	None	Admin Indeed	Admin Indeed
1021	Пользователем Admin Indeed до...	05.10.2018 11:10:33	None	Admin Indeed	None

- Отображения журнала в событиях Windows.

Просмотр событий (Локальный)

Настройка представления

Журналы Windows

Журналы приложений и служб

Indeed EA

Operational

Microsoft

ThinPrint Diagnostics

Windows PowerShell

Служба управления ключами

События оборудования

Подписки

Operational Событий 27

Уровень	Дата и время	Источник	Код события	Категория задачи
Сведения	05.10.2018 11:32:04	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:32:04	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:32:04	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:10:48	Indeed EA	1033	EA Сервер
Сведения	05.10.2018 11:10:34	Indeed EA	1033	EA Сервер
Сведения	05.10.2018 11:10:34	Indeed EA	1028	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1028	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1028	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1028	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1020	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1021	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1005	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1028	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1028	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1028	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1008	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1007	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1032	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1032	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1000	EA Сервер