

Установка и настройка Indeed AM Log Server с хранилищем в SysLog

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.

Информация

Indeed AM Admin Console не позволяет читать события из sysLog сервера. Для отображения журнала в Admin Console необходимо наличие своей БД (SQL-сервер или EventLog) для хранения событий Indeed AM LogServer.

Установка

1. Выполнить установку Indeed AM Log Server через запуск инсталлятора **Indeed.LogServer-x64.ru-ru.msi**.

2. Добавить привязку **https** в настройка **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.

Установка sysLog сервера.

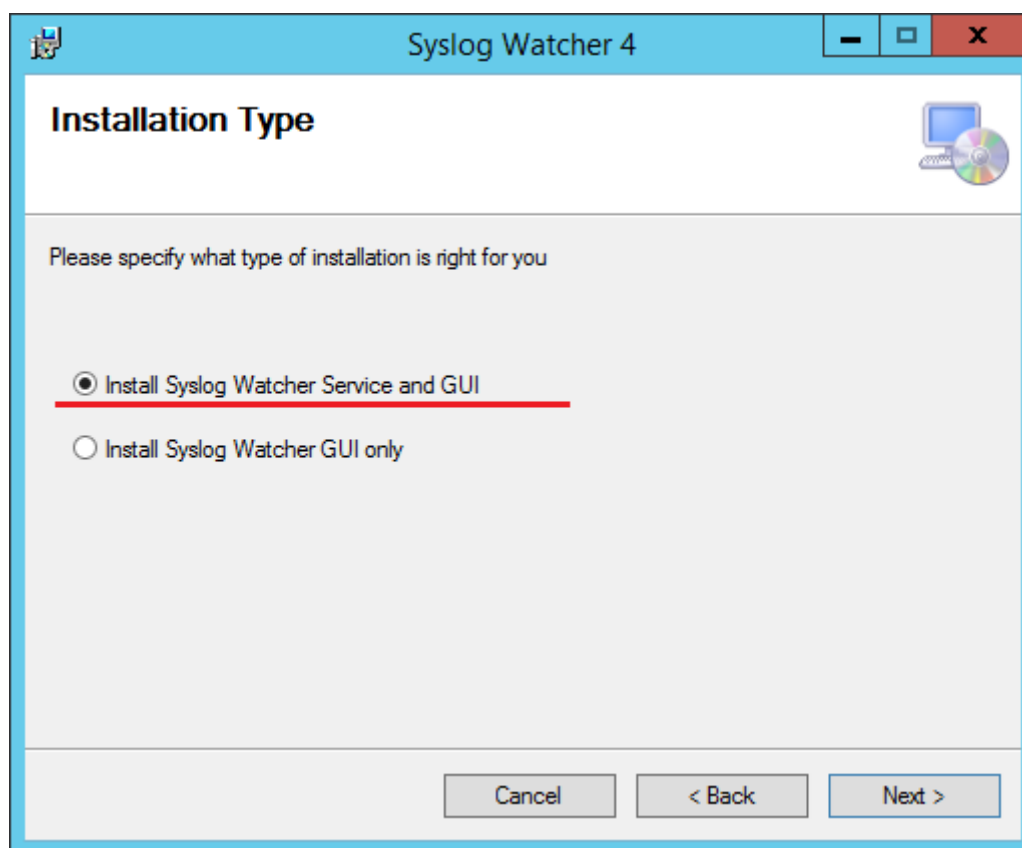
 Информация

Indeed AM Log Server поддерживает формат sys-log, вы можете использовать любой сервер, работающий с данным форматом. В качестве примера далее рассмотрена настройка sys-log сервера **Syslog Watcher v4.8.6**.

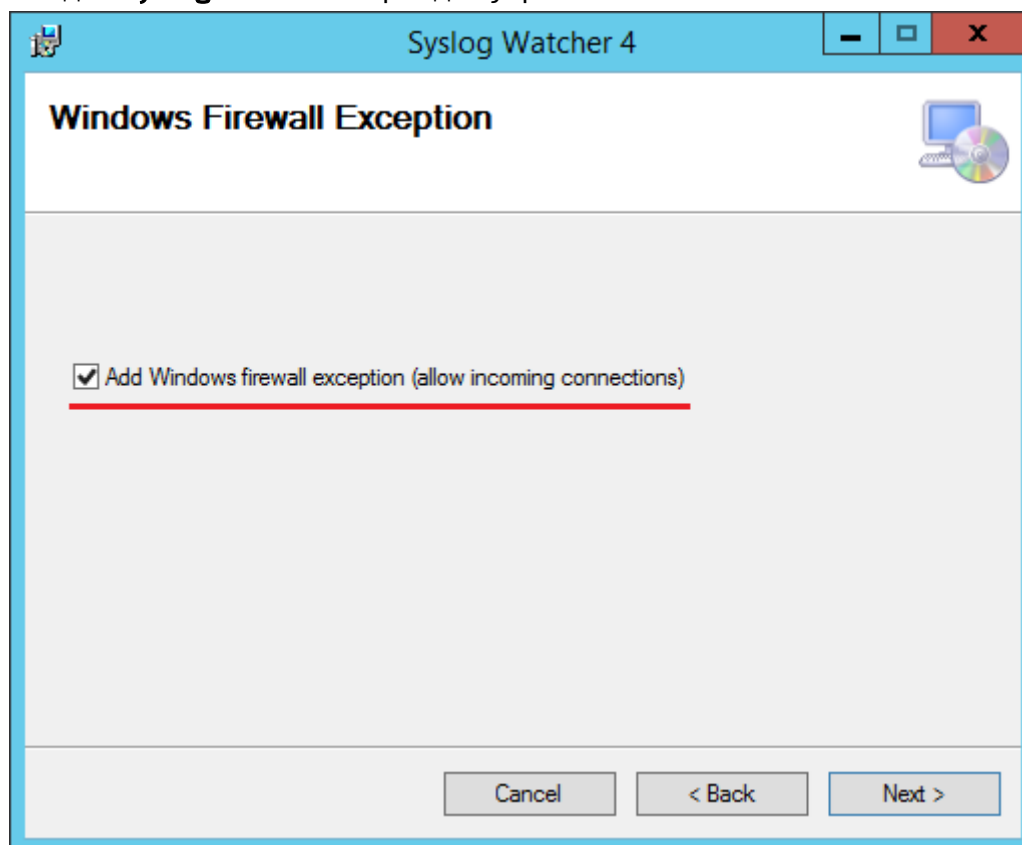
Вы можете скачать утилиту на официальном сайте <https://syslogwatcher.com>

1. Запустите установочный файл **SyslogWatcherSetup-*.*.win32.msi**.
2. В окне "**License Agreement**" примите лицензионное соглашение.

3. В окне "Installation Type" выбрать тип установки "Install Syslog Watcher Service and GUI".



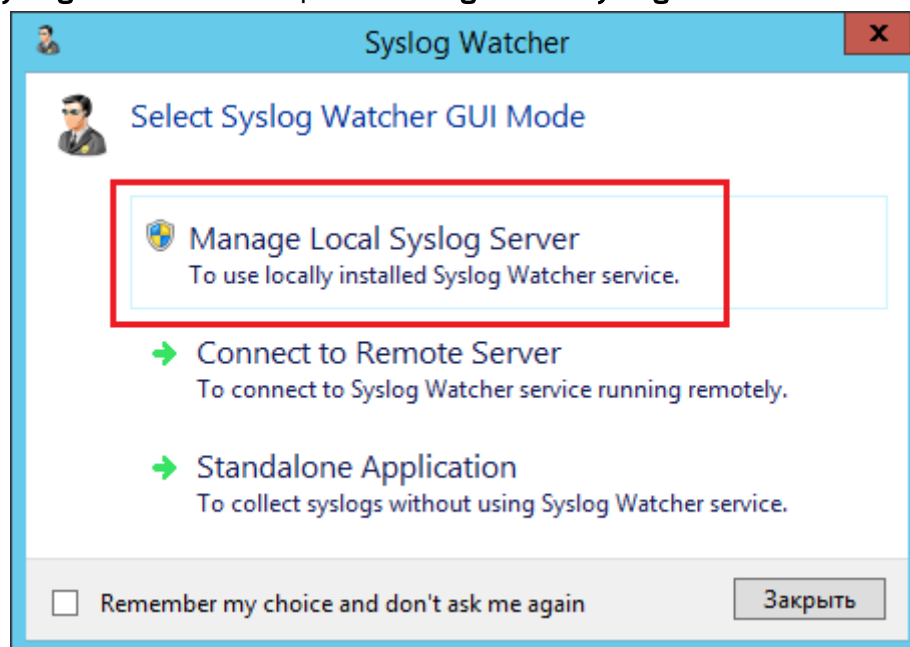
4. В окне "Select installation Folder" выбрать путь установки для **sys-log сервера**.
5. В окне "Windows Firewall Exception" разрешить добавление правила на все входящие соединения для **Syslog Watcher** в брандмауэр **Windows**.



6. В окне "Confirm Installation" нажать "Next" для подтверждения установки.
7. Дождаться завершения установки сервера.

Настройка sysLog сервера.

1. Запустите Syslog Watcher и выберите "Manage Local Syslog Server".



2. Нажмите "**Settings**" в верхнем меню программы.

a. Выберите пункт "**Network Interfaces**".

b. Проверьте что выбрано использование протокола udp и указан порт.

The screenshot shows the 'Syslog Watcher Settings' dialog box with the 'Network Interfaces' tab selected in the left sidebar. The 'Internet Protocol' section has the following settings: 'Bind to local IPv4 interfaces' is checked with a link to 'Show Local Interfaces'; 'Bind to specified IPv4 address' is selected with the value '192.168.1.4'; 'Bind to local IPv6 interfaces' is checked; 'Bind to all local IPv6 addresses (:::)' is selected. The 'Transport Layer' section has 'Receive syslogs over UDP on port: 514' checked and underlined in red, with a link to 'Show Used Ports'; 'Receive syslogs over TCP on port: 1468' is unchecked. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

c. Выберите пункт "**Processing**". Выберите кодировку **UTF-8**.

The screenshot shows the 'Syslog Watcher Settings' dialog box with the 'Processing' tab selected in the left sidebar. The 'Processing' section has the following settings: 'Default severity: Debug' and 'Default facility: local 0'; 'Remove trailing CR/LF (Carriage Return / Line Feed)' is checked; 'Replace non-printable ASCII characters (codes 0-31) with:' is checked, with 'Hexadecimal ACSII code of the character' selected; 'Force codepage: 65001 (UTF-8)' is checked and underlined in red; 'Insert domain name after IP address within message body' is checked. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Редактирование конфигурационного файла.

1. Откройте конфигурационный файл **sampleSyslog.config** (C:\inetpub\wwwroot\ils\targetConfigs\sampleSyslog.config).
2. Для тега **"Settings"** укажите данные для подключения к **sys-log**.

Пример настройки для Syslog Watcher

```
<Settings HostName="localhost" Port="514" Protocol="udp" />
```

3. Откройте конфигурационный файл **clientApps.config** (C:\inetpub\wwwroot\ils\clientApps.config).
4. Для блока с **"Application Id="ea"** в тегах **TargetId** и **ReadTargetId** указать **sampleSyslog**.



Информация

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

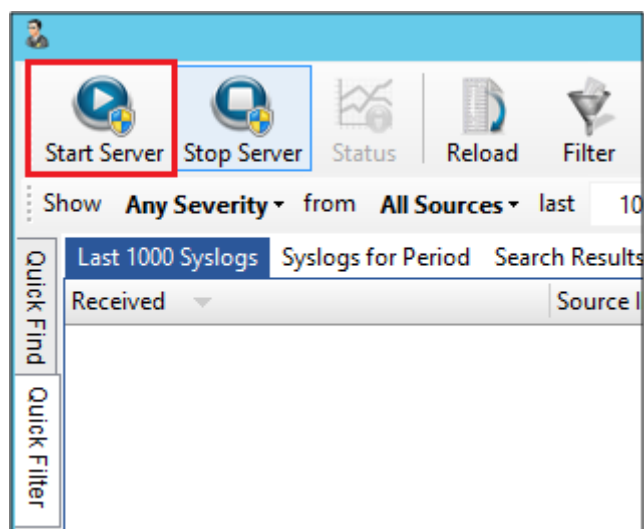
В блоке **WriteTargets**, в тегах **TargetId**, указывается идентификатор хранилища куда будет осуществляться запись событий.

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

5. Нажмите "**Start Server**" в верхнем левом углу программы **Syslog Watcher**.



Пример отображения.

- Пример отображения в Syslog Watcher.

The screenshot displays the Syslog Watcher - Local Syslog Server application. The interface includes a top toolbar with buttons for Start Server, Stop Server, Status, Reload, Filter, Find, Search, Import, Export, Delete, Reports, Storage, and Settings. Below the toolbar is a status bar showing 'Show Any Severity' from LOG last 1000 messages, updated every 10 seconds on 26.11.2018 12:01:26. The main area shows a table of the last 1000 syslogs. The table has columns: Received, Source IP, Source, Facility, Severity, Timestamp, Tag, Ori..., and Message. The messages are filtered by 'LOG' facility and 'Info' severity. The 'Message View' pane at the bottom shows a detailed view of a selected message.

Received	Source IP	Source	Facility	Severity	Timestamp	Tag	Ori...	Message
26.11.2018 10:52:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server LogonByAuthenticatorSucceeded [indee...
26.11.2018 11:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server LogonByAuthenticatorSucceeded [indee...
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server AcquirePersonalLicense [indeed@32473 r...
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server ReleasePersonalLicense [indeed@32473 li...
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server ReleasePersonalLicense [indeed@32473 li...
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server AcquirePersonalLicense [indeed@32473 r...
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server AcquirePersonalLicense [indeed@32473 r...
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server ReleasePersonalLicense [indeed@32473 li...
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server ReleasePersonalLicense [indeed@32473 li...
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server AcquirePersonalLicense [indeed@32473 r...

Message View

Info / local 7 LOG (::1) 26 ноября 2018 г. 11:00:31.963

server LogonByAuthenticatorSucceeded [indeed@32473
requestApplication="Enterprise Management Console" requestUser="Admin Indeed" requestComputer="192.168.1.3"
logonMode="Windows Token" authComment=""] Пользователь был успешно аутентифицирован по предоставленному
аутентификатору.Приложение: Enterprise Management Console.Пользователь: Admin Indeed.Компьютер:
192.168.1.3.Способ входа: Windows Token.Комментарий аутентификатора: .