Установка и настройка Indeed Log Server версии 7 с хранилищем в SysLog.

П Информация

Файлы для Indeed Log Server 7 расположены: indeed AM 7.0 \Indeed Log Server \< Homep версии> \

- Indeed.LogServer-v7.0.0.x64.ru-ru.msi Пакет для установки Indeed Log Server 7.
- IndeedEA.Server.EventLog-v7.0.1.x64.ru-ru.msi Пакет для создания необходимой структуры журнала в Windows EvetLog.

Установка

- 1. Выполнить установку Indeed Log Server через запуск инсталлятора Indeed.LogServer-v7. 0.0.x64.ru-ru.msi.
- 2. Добавить привязку https в настройка Default Web Site в IIS Manager.

П Информация

Indeed Log Server 7 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.

- а. Запустите IIS Manager и раскройте пункт Сайты (Sites).
- b. Выберите сайт Default Web Site и нажмите Привязки (Bindings) в разделе Действи я (Actions).
- с. Нажмите **Добавить** (Add):
 - i. **Тип** (Type) https.
 - іі. Порт (Port) 443.
 - ііі. Выберите SSL-сертификат (SSL Certificate).
- d. Сохраните привязку.

Установка sysLog сервера.

П Информация

Indeed Log Server 7 поддерживает формат sys-log, вы можете использовать любой сервер, работающий с данным форматом. В качестве примера далее рассмотрена настройка sys-log cepвера 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.

1	Syslog Watcher 4	_ 🗆 🗙
Window	s Firewall Exception	
Add Wi	indows firewall exception (allow incoming connections)	
	Cancel < Back	Next >

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.
 - а. Выберите пункт "**Network Interfaces"**.
 - b. Проверьте что выбрано использование протокола udp и указан порт.

		Syslog Watcher Settings
	User Interface - Grid View - Processing - Formats - VendorPack - Confirmations Server - Network Interfaces - Advanced Networking - Domain Names - Remote Access - Processing - Formats Storage - Storage Backups Email Alerts Server	Systog Watcher Settings Internet Protocol Image: Show Local Interfaces O Bind to local IPv4 addresses (0.0.0.0) Image: Bind to specified IPv4 addresses: Image: Bind to local IPv6 addresses: Image: Bind to all local IPv6 addresses: Image: Bind to specified IPv6 addresses: Image: Transport Layer
	- Email Account Export to Text - Destination Export to DB - Database	Receive syslags over UDP on part: 514 Show Used Parts Receive syslags over TCP on part: 1468 Accelve
с. Выберите і	пункт " Processing"	. Выберите кодировку UTF-8. Syslog Watcher Settings
	User Interface - Grid View - Processing - Formats - VendorPack - Confirmations Server - Network Interfaces - Advanced Networking - Domain Names - Remote Access - Processing - Formats Storage - Storage Backups Email Alerts - Email Account Export to Text - Destination Export to DB - Database	These settings are used by the server when processing syslogs. Processing Default serverity: Debug Default facility: local 0 Processing Remove trailing CR.LF (Carriage Return /Line Feed) Replace non-printable ASCII characters (codes 0-31) with: Hexadecimal ACSII code of the character Custom printable character: Custom printable char

Редактирование конфигурационного файла.

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



- Откройте конфигурационный файл clientApps.config (C:\inetpub\wwwroot\ils\clientApps. config).
- 4. В тегах Targetid и ReadTargetid указать sampleSyslog.

(j)	Информация	
	В тегах Targetid и ReadTargetid указывается идентификатор выбранного типа хранения лог файлов.	
	Идентификаторы заданы в теге <targets></targets> , конфигурационные файлы для каждого типа находится в папке targetConfigs с соответствующим именем.	



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

2							
St	Constant Server	Stop Serv	er Sta	tus	Reloa	d Fil	ter
Sł	now Any	Severity •	from	All So	ources	+ last	10
ę	Last 1000	Syslogs	Syslogs	for Per	iod S	earch R	esults
Ŗ	Received	-				So	urce l
ind							
<u>P</u>							
ŝ							
lter							

Пример отображения.

• Пример отображения в Syslog Watcher.

Start Steve Start Reised Per
Operation Operation Security Operation Security Operation Security
Show Any Severity - from LOG - last 1000 : messages Update every 10 : seconds Updated at 26.11.2018 12:01:26 AutoStorell © AutoStorell : 0 System I = 1 Second = 1 Seco
Image: Constraint of the standard of th
Openantic Source 10 Source 10 <t< td=""></t<>
Bit Diameter Source: Fisiality Serving Onit. Message 26.11.2018 10.30: 11 LOG local 7 Info 2018-11-2 as unit. server Logon@yAthenticatorSucceeded [indeed 2018-11-2 26.11.2018 10.30: 11 LOG local 7 Info 2018-11-2 as unit server Logon@yAthenticatorSucceeded [indeed 30.47] 26.11.2018 12.00: 11 LOG local 7 Info 2018-11-2 as unit server Acquire@ersonall.comes [indeed 30.47] 26.11.2018 12.00: 11 LOG local 7 Info 2018-11-2 as unitserver Acquire@ersonall.comes [indeed 30.47] 26.11.2018 12.00: 11 LOG local 7 Info 2018-11-2 as unitserver Acquire@ersonall.comes [indeed 30.47] 26.11.2018 12.00: 11 LOG local 7 Info 2018-11-2 as unitserver Acquire@ersonall.comes [indeed 30.47] 26.11.2018 12.00: 11 LOG local 7 Info 2018-11-2 as <td< td=""></td<>
Open Text Display LOG local 7 Infe 2018-111-2ex unit
Open Processing Control Status Contro Status Control Status Control
En L12018 12:00 L0.G local 7 Infla 2018-11-2 en unk
20/20 25.11/2018 12:00
2 26.11.2018 12:00::1 L.O.G local7 Info 2018-11-2ea unk server RelassPersonallicense [indeed]32:47 26.11.2018 12:00::1 L.O.G local7 Info 2018-11-2ea unk server AcquirePersonallicense [indeed]32:47 26.11.2018 12:00::1 L.O.G local7 Info 2018-11-2ea unk server AcquirePersonallicense [indeed]32:47 26.11.2018 12:00::1 L.O.G local7 Info 2018-11-2ea unk server AcquirePersonallicense [indeed]32:47
26.11.2018 12:00: ::1 LOG local 7 Info 2018-11-2 ea unk server AcquirePersonalLicense [indeed@32473 26.11.2018 12:00: ::1 LOG local 7 Info 2018-11-2 ea unk server AcquirePersonalLicense [indeed@32473
26.11.2018 12:00: ::1 LOG local 7 Info 2018-11-2 ea unk server AcquirePersonalLicense [indeed@32473
26.11.2018 12:00: ::1 LOG local 7 Info 2018-11-2 ea unk server ReleasePersonalLicense [indeed@32473
26.11.2018 12:00: ::1 LOG local 7 Info 2018-11-2 ea unk server ReleasePersonalLicense [indeed@32473
26.11.2018 12:00: ::1 LOG local 7 Info 2018-11-2 ea unk server AcquirePersonalLicense [indeed@32473
Message View
Info / local 7 LOG (::1) 26 ноября 2018 г. 11:00:31.963
ятик (доров)/и/directotor5/socceeded (indexe)822,473 нециска/points/action="thintprine Management Conceller requestLiser="Admin Indexel" requestComputer="192,158.1.3" logonhode= Windows Toker" authComments ¹¹ Пользователь был услешно аутентифицирован по предоставленному зитентификатору.Пригожение: Enterprine Management Concell. Пользователь: Admin Indeed.Конпьютер: 192,158.1.3.Cnoco6 входа: Windows Token.Коннентврий аутентификатора: .