

# loganalyzer

**LogAnalyzer** – это web приложение, которое предназначено для просмотра логов системных событий, полученных от **syslog**, при помощи веб-браузера.

**Rsyslog** – это приложение, представляющее собой расширение стандартного демона **syslog**, одной из особенностей которого является возможность сохранять события в БД **MySQL**.

## Пакеты

<https://loganalyzer.adiscon.com/download/>

```
1 | wget http://download.adiscon.com/loganalyzer/loganalyzer-[version].tar.gz
```

## Установка

1. Распаковать архив

```
1 | tar zxvf loganalyzer-[version].tar.gz
```

2. Перенести файлы **loganalyzer** в директорию веб-сервера

```
1 | mv loganalyzer-[version]/src/* /var/www/logs.test.local/html/  
2 | mv loganalyzer-[version]/contrib/* /var/www/logs.test.local/html/
```

3. Для файлов-скриптов необходимо добавить атрибут возможности исполнения (**x**) и выполнить скрипт `configure.sh`, который создаст файл **config.php** с возможностью записи (**w**)

```
1 | chmod u+x configure.sh secure.sh  
2 | ./configure.sh
```

## Настройка

1. Установка необходимых пакетов

```
1 | dnf install httpd php mysql php-mysql php-mysqld mysql-server wget  
   rsyslog rsyslog-mysql
```

2. Старт и включение автозапуска **Apache** и **MySQL**

```
1 | systemctl start httpd mysql  
2 | systemctl enable httpd mysql
```

## MySQL/MariaDB (опционально)

1. Установить пароль пользователю **root** (изначально пуст)

```
1 | mysqladmin - u root password NewPassword
```

2. Импорт **схемы** базы данных **rsyslog** в **MySQL**

```
1 | mysql -u root -p < /usr/share/doc/rsyslog/mysql-createdB.sql
```

3. Создадим отдельного пользователя в базе **MySQL** для доступа к данным **rsyslog**, затем назначим ему доступ к базе **Syslog**, которая была создана из ранее импортированной схемы.

```
1 | mysql - u root - p mysql
2 | mysql> CREATE USER 'rsyslog'@'localhost' IDENTIFIED BY 'P@ss';
3 | mysql> GRANT ALL ON Syslog.* TO 'rsyslog'@'localhost';
4 | mysql> flush privileges;
5 | mysql> exit;
```

- Смена пароля: `ALTER USER 'root'@'localhost' IDENTIFIED BY 'новый_пароль';`
- Проверка доступа и работы базы:

```
1 | [root@centos-vm ~]# mysql -u rsyslog -p
2 | Enter password:
3 |
4 | mysql> show databases;
5 | +-----+
6 | | Database |
7 | +-----+
8 | | Syslog   |
9 | | information_schema |
10 | +-----+
11 | 2 rows in set (0.02 sec)
12 |
13 | mysql> use Syslog;
14 | Reading table information for completion of table and column names
15 | You can turn off this feature to get a quicker startup with -A
16 |
17 | Database changed
18 | mysql> show tables;
19 | +-----+
20 | | Tables_in_Syslog |
21 | +-----+
22 | | SystemEvents     |
23 | | SystemEventsProperties |
24 | | logcon_charts     |
25 | | logcon_config     |
26 | | logcon_dbmappings |
27 | | logcon_fields     |
28 | | logcon_groupmembers |
29 | | logcon_groups     |
```

```

30 | logcon_savedreports |
31 | logcon_searches    |
32 | logcon_sources      |
33 | logcon_users        |
34 | logcon_views        |
35 +-----+
36 13 rows in set (0.00 sec)
37
38 mysql> select * from SystemEvents limit 2 \G

```

## Rsyslog

1. Создаем файл **mysql.conf** в директории "кастомных" конфигов для **rsyslog**

```

1 | $ModLoad ommysql
2 | authpriv.* : ommysql:127.0.0.1,Syslog,rsyslog,Password

```

, где -

- `$ModLoad ommysql` - подключение модуля для пересылки логов в базу данных
- `authpriv.* : ommysql:127.0.0.1,Syslog,rsyslog,Password`  
`authpriv` - несистемные авторизационные сообщения. Здесь можно настроить сбор и запись любых сообщений, каждую комбинацию нужно отделять «;» (например, `mail.*; authpriv.* : ommysql...`).
- `127.0.0.1` - адрес на котором слушает сервер
- `Syslog` - имя базы данных
- `rsyslog` и `Password` - пользователь и пароль для доступа к базе

2. Перезапускаем **rsyslog**

```

1 | systemctl reload rsyslog

```

Задался вопросом, как в эту схему с базой данных интегрировать еще логи с удаленных машин. Надо будет копнуть инфу.

Еще интересно как заниматься ротацией тех логов, что лежат в бд. Туда ведь лапы **logrotate** уже не дотянутся

## Apache

1. Создаем директорию для сайта **Loganalyzer**.

```

1 | mkdir -p /var/www/logs.test.local/html
2 | mkdir -p /var/www/logs.test.local/log

```

2. Проверка разрешений на корневую директорию.

```
1 | chmod -R 755 /var/www
```

3. Согласно инструкции по установке, перемещаем содержимое директорий **src** и **contrib** в корень директории сайта. Затем делаем скрипт **configure.sh** исполняемым и выполняем его. Назначаем владельцем директории сайта - **apache**, чтобы не возникло проблем с доступом.

```
1 | mv loganalyzer-[version]/src/* /var/www/html/loganalyzer
2 | mv loganalyzer-[version]/contrib/* /var/www/html/loganalyzer/
3
4 | chmod u+x configure.sh secure.sh
5 | ./configure.sh
```

4. Затем в директории сервера **apache** создаем еще две директории: **sites-available** (конфигурации виртуальных хостов) и **sites-enabled** (доступные для обслуживания, символические ссылки на конфиги виртуальных хостов)

```
1 | mkdir /etc/httpd/sites-available /etc/httpd/sites-enabled
```

5. В главный файл конфигурации вносим дополнение, для того, чтобы поиск виртуальных хостов проходил в директории **sites-enabled**

```
1 | nano /etc/httpd/conf/httpd.conf
2
3 | # добавить в конец файла
4 | IncludeOptional sites-enabled/*.conf
```

6. Создаем новый виртуальный хост для **loganalyzer**

```
1 | cp /usr/share/doc/httpd/httpd-vhosts.conf /etc/httpd/sites-
  | available/loganalyzer.conf
2 | nano sites-available/loganalyzer.conf
3
4 | <VirtualHost *:80>
5 |     ServerName www.example.com
6 |     ServerAlias example.com
7 |     DocumentRoot /var/www/example.com/html
8 |     ErrorLog /var/www/example.com/log/error.log
9 |     CustomLog /var/www/example.com/log/requests.log combined
10 | </VirtualHost>
```

7. После сохранения конфигурации виртуального хоста, создаем символическую ссылку для получения доступа к сайту

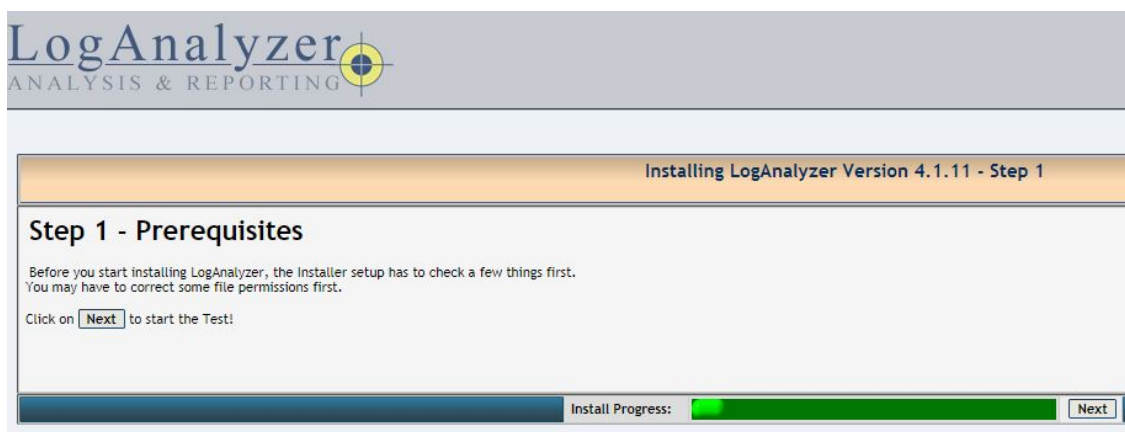
```
1 | ln -s /etc/httpd/sites-available/example.com.conf /etc/httpd/sites-
  | enabled/example.com.conf
```

8. Перезагружаем **apache** и приступаем к установке **loganalyzer**

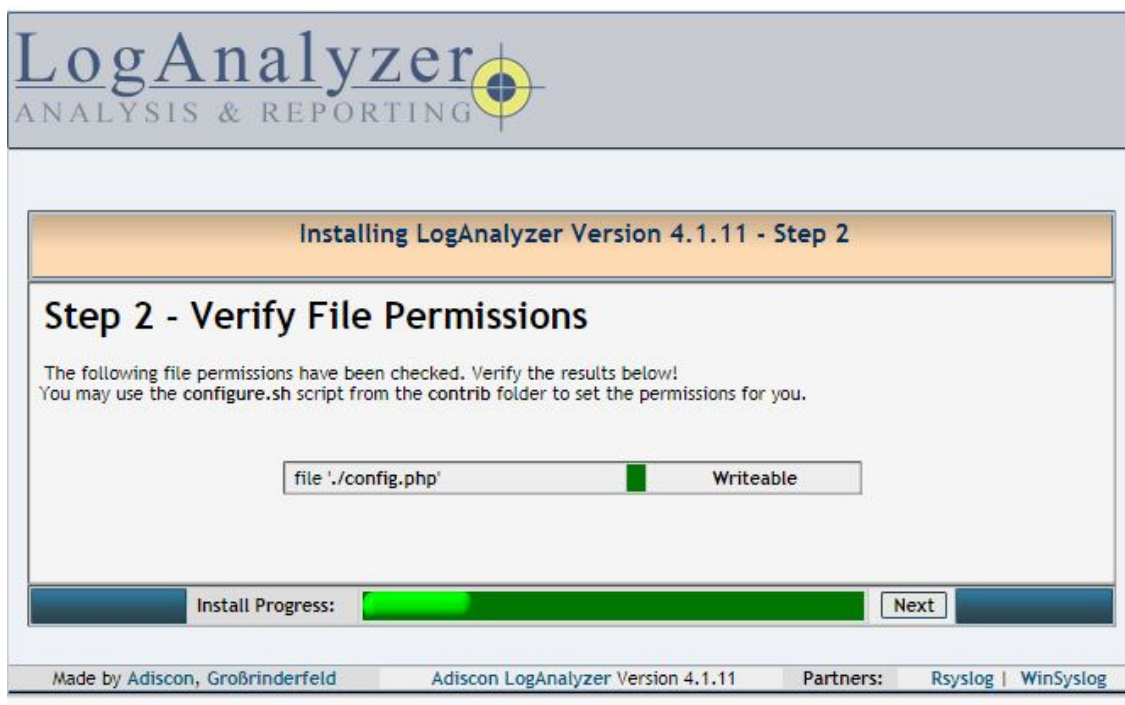
```
1 | systemctl reload apache
```

## WEB

1. Через браузер получаем доступ к нашему сайту **logalyzer-mysql.ip/install.php**



2. Проверка прав доступа к директориям



3. Конфигурация пользователя для базы и некоторых дополнительных опций. Вписываем сюда значения из конфигурационного файла **/etc/rsyslog.d/mysql.conf**

Installing LogAnalyzer Version 4.1.11 - Step 3

## Step 3 - Basic Configuration

In this step, you configure the basic configurations for LogAnalyzer.

Frontend Options	
Number of syslog messages per page	<input type="text" value="50"/>
Message character limit for the main view	<input type="text" value="80"/>
Character display limit for all string type fields	<input type="text" value="30"/>
Show message details popup	<input checked="" type="radio"/> Yes <input type="radio"/> No
Automatically resolved IP Addresses (inline)	<input checked="" type="radio"/> Yes <input type="radio"/> No

User Database Options	
Enable User Database	<input checked="" type="radio"/> Yes <input type="radio"/> No
A MYSQL database Server is required for this feature. Other database engines are not supported for the User Database System. However for logsources, there is support for other database systems.	
Database Host	<input type="text" value="localhost"/>
Database Port	<input type="text" value="3306"/>
Database Name	<input type="text" value="Syslog"/>
Table prefix	<input type="text" value="logcon_"/>
Database User	<input type="text" value="rsyslog"/>
Database Password	<input type="password" value="...."/>
Require user to be logged in	<input checked="" type="radio"/> Yes <input type="radio"/> No
Authentication method	<div style="border: 1px solid black; padding: 2px;">Internal authentication ▼</div>

Install Progress: 
Next

4. Проверка доступов к базе по предоставленному логину/паролю и заливка структуры таблиц, с которыми будет работать **LogAnalyzer**.

Installing LogAnalyzer Version 4.1.11 - Step 4

## Step 4 - Create Tables

If you reached this step, the database connection has been successfully verified!

The next step will be to create the necessary database tables used by the LogAnalyzer User System. This might take a while!

**WARNING:** If you have an existing LogAnalyzer installation in this database with the same tableprefix, all your data will be **OVERWRITTEN!** Make sure you are using a fresh database, or you want to overwrite your old LogAnalyzer database.

Click on Next to start the creation of the tables

Install Progress: 
Next

5. Проверка наличия таблиц.

Installing LogAnalyzer Version 4.1.11 - Step 5

## Step 5 - Check SQL Results

Tables have been created. Check the List below for possible Error's

- Successfully executed statements: 24
- Failed statements: 0

You can now proceed to the next step adding the first LogAnalyzer Admin User!

Install Progress: 
Next

Made by Adiscon, Großbründerfeld
Adiscon LogAnalyzer Version 4.1.11

6. Создание администратора к web-интерфейсу **LogAnalyzer**.

The screenshot shows the LogAnalyzer web interface during installation. At the top, the logo reads "LogAnalyzer ANALYSIS & REPORTING". Below it, a header bar says "Installing LogAnalyzer Version 4.1.11 - Step 6". The main heading is "Step 6 - Creating the Main Useraccount". A message states: "You are now about to create the initial LogAnalyzer User Account. This will be the first administrative user, which will be needed to login into LogAnalyzer and access the Admin Center!". Below this is a form titled "Create User Account" with three input fields: "Username" (containing "root"), "Password" (containing "\*\*\*\*\*"), and "Repeat Password" (containing "\*\*\*\*\*"). At the bottom of the form is a progress bar labeled "Install Progress:" which is nearly full, and a "Next" button. The footer contains the text: "Made by Adiscon, Großbrinderfeld", "Adiscon LogAnalyzer Version 4.1.11", and "Partners: Rsyslog | WinSyslog".

7. Добавляем источник логов для отображения. **LogAnalyzer** умеет показывать записи из текстового файла, базы данных **MongoDB** или **MySQL**. Описываем опции доступа к базе.

The screenshot shows the "First Syslog Source" configuration screen. It has a form with several sections. The top section has three fields: "Name of the Source" (containing "Mysql Source"), "Source Type" (a dropdown menu set to "MYSQL Native"), and "Select View" (a dropdown menu set to "Syslog Fields"). Below this is a section titled "Database Type Options" with a dropdown menu set to "MonitorWare". Under this section are several fields: "Table type", "Database Host" (containing "localhost"), "Database Name" (containing "Syslog"), "Database Tablename" (containing "SystemEvents"), "Database User" (containing "rsyslog"), and "Database Password" (containing "\*\*\*\*\*"). At the bottom right of this section are two radio buttons labeled "Yes" and "No", with "No" being selected. At the bottom of the screen is a progress bar labeled "Install Progress:" which is nearly full, and a "Next" button.

8. Завершение установки



# LogAnalyzer

ANALYSIS & REPORTING

## Installing LogAnalyzer Version 4.1.11 - Step 8

### Step 8 - Done

Congratulations! You have successfully installed LogAnalyzer :)

Click [here](#) to go to your installation.

Install Progress:

Finish!

Made by [Adiscon](#), [Großbrunderfeld](#)

**Adiscon LogAnalyzer**  
Version 4.1.11

Partners: [Rsyslog](#) [WinSyslog](#)

Page rendered in: 0.0624 seconds | DB queries: 91 | GZIP enabled: yes | Script Timeout: 30 seconds

# LogAnalyzer

ANALYSIS & REPORTING

Select Language

English

Select a Style

Default

Select Source

Mysql Source

Select View

Syslog Fields

Search

Show Events

Statistics

Reports

Help

Search in Knowledge Base

Admin Center

Logoff

Logged in as "root"

Maximize View

Search (filter):

Search

I'd like to feel sad

Reset search

Highlight >>

Advanced Search (sample: facility:local0 severity:warning)

Recent syslog messages

Set auto reload:

Auto reload disabled

Records per page:

Preconfigured (50)

Pagers:

1

2

3

4

5

6

7

8

9

10

Date	Facility	Severity	Host	Syslogtag	ProcessID	Message
Today 20:11:13	DAEMON	INFO	centos-vm	systemd[1]:	Syslog	Started The PHP FastCGI Process Manager.
Today 20:11:12	DAEMON	INFO	centos-vm	systemd[1]:	Syslog	Starting The PHP FastCGI Process Manager...
Today 20:11:12	DAEMON	INFO	centos-vm	systemd[1]:	Syslog	Stopped The PHP FastCGI Process Manager.
Today 20:11:12	DAEMON	INFO	centos-vm	systemd[1]:	Syslog	Stopping The PHP FastCGI Process Manager...
Today 20:04:25	SECURITY	INFO	centos-vm	sshd[1804]:	Syslog	pam_unix(sshd:session): session opened for user root by (uid=0)
Today 20:04:25	AUTH	INFO	centos-vm	systemd-logind[1039]:	Syslog	New session 5 of user root.
Today 20:04:25	DAEMON	INFO	centos-vm	systemd[1]:	Syslog	Started Session 5 of user root.
Today 20:04:25	SECURITY	INFO	centos-vm	sshd[1804]:	Syslog	Accepted password for root from 192.168.100.101 port 51816 ssh2
Today 20:02:50	DAEMON	WARNING	centos-vm	systemd[1]:	Syslog	iscsi.service: Unit cannot be reloaded because it is inactive.
Today 20:02:50	DAEMON	INFO	centos-vm	NetworkManager[921]:	Syslog	<info> [1614603770.4506] manager: NetworkManager state is now CONNECTED_GLOBAL
Today 20:02:50	DAEMON	INFO	centos-vm	NetworkManager[921]:	Syslog	<info> [1614603770.4500] device (ens33): Activation: successful, device activat ...
Today 20:02:50	DAEMON	INFO	centos-vm	NetworkManager[921]:	Syslog	<info> [1614603770.4428] policy: set 'ens33' (ens33) as default for IPv4 routin ...
Today 20:02:50	DAEMON	INFO	centos-vm	NetworkManager[921]:	Syslog	<info> [1614603770.4427] manager: NetworkManager state is now CONNECTED_SITE
Today 20:02:50	DAEMON	INFO	centos-vm	NetworkManager[921]:	Syslog	<info> [1614603770.4416] manager: NetworkManager state is now CONNECTED_LOCAL
Today 20:02:50	DAEMON	INFO	centos-vm	NetworkManager[921]:	Syslog	<info> [1614603770.4411] device (ens33): state change: secondaries -> activated ...
Today 20:02:50	DAEMON	INFO	centos-vm	NetworkManager[921]:	Syslog	<info> [1614603770.4408] device (ens33): state change: ip-check -> secondaries ...
Today 20:02:50	DAEMON	INFO	centos-vm	NetworkManager[921]:	Syslog	<info> [1614603770.4334] device (ens33): state change: ip-config -> ip-check (r ...

## WEB-конфигурация

- Добавление новых источников: **Admin Center -> Sources**

Для добавления отдельного текстового лог-файла, необходимо выдать ему права на чтение либо изменить владельца или группу, для доступа к нему **apache**

# LogAnalyzer

ANALYSIS & REPORTING

Satisfied with Adiscon LogAnalyzer?

Donate

Donate and help keep the project alive!

Select Language

English

Select a Style

Default

Search

Show Events

Statistics

Reports

Help

Search in Knowledge Base

Admin Center

Logoff

Logged in as "root"

Maximize View

Preferences

Sources

Fields

Views

Searches

Charts

Message Parsers

Report Modules

DBMappings

Users

Groups

Sources Options

ID	Source Name	Source Type	Assigned To	Available Actions
5	messages	Diskfile	Global	<div> <div></div> <div></div> </div>
6	secure	Diskfile	Global	<div> <div></div> <div></div> </div>





Add new Source

Так же, при добавлении первого источника, база данных теряется из списка. Появляется только после удаления всех новых источников. У них так же отличается пункт о назначении



Assigned To				
			Global	
			Global	
Source				

ID	Source Name	Source Type	Assigned To	Available Actions
Source1	Mysql Source	MySQL Database	Configuration File	  
 Add new Source				

## Источники

<https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-centos-7-ru>

<https://logalyzer.adiscon.com/doc/install.html>

<https://logalyzer.adiscon.com/doc/>

<https://habr.com/ru/post/213519/>

<http://feanor184.ru/linux/rsyslog-i-loganalyzer-podnimaem-server-logirovaniya-na-linux.html>

<https://voxlink.ru/kb/linux/nastrojka-logirovaniya-s-pomoshhju-rsyslog-i-loganalyzer/>

<https://yallalabs.com/monitoring-tools/how-to-install-loganalyzer-adiscon-centos-8/>

<https://qiwichupa.net/t/foss>

<https://www.ekzorchik.ru/2018/09/how-to-deploy-loganalyzer-on-ubuntu-18-04/>