

Инструкция по установке программного обеспечения СЦУСИБ RuSIEM

ООО «РусИЕМ»

г. Москва, 2023 г.

Порядок установки программного комплекса «Система централизованного управления событиями информационной безопасности RuSIEM»

Важно:

В процессе установки потребуется ввод лицензионного ключа, который необходимо получить у производителя ПО в соответствии с инструкцией, указанной в пункте 3 подпунктах 4-6.

1. Скачайте дистрибутив

Ссылка на скачивание дистрибутива:

<https://files.rusiem.tech/nextcloud/s/jXsZZfr6JRA89ex>

Получите информацию по установке с инструкцией на почту.

2. Выбор места установки системы:

• На виртуальный сервер VmWare esxi или Microsoft Hyper-V

- 1) Формат диска стоит выбрать «Thin provision» с целью экономии дискового пространства хранилища esxi;
- 2) Объем выделенной виртуальной оперативной памяти не менее 16 GB;
- 3) Если имеется вероятность что на гипервизоре может оказаться менее 16 GB свободной оперативной памяти – установить в настройках виртуальной машины резервирование оперативной памяти;
- 4) Выделено не менее 2х процессоров;
- 5) Присутствует виртуальный USB контроллер.

• На физический сервер:

- 1) Перед установкой серверной части системы, необходимо выделить физический сервер соответствующий требованиям к аппаратному обеспечению и установить операционную систему Ubuntu Server 18.04 LTS (Bionic Beaver) x64 - <https://releases.ubuntu.com/18.04> (и там актуальный Server Install image for 64-bit PC, например **ubuntu-18.04.6-live-server-amd64.iso**), а также настроить доступ сервера к сети Интернет.

3. Настройки перед установкой системы

1) Перед установкой системы рекомендуется проверить наличие русской локализации командой:

```
locale -a
```

2) При отсутствии в списке ru_RU и ru_RU.UTF-8 установите их командами:

```
sudo locale-gen ru_RU
```

```
sudo locale-gen ru_RU.UTF-8
```

```
sudo update-locale
```

3) Ввести команду для получения UUID сервера (под root доступом или через sudo):

```
/usr/sbin/dmidecode -s system-uuid | awk '{print toupper($0)}'
```

4) Отправить UUID на электронную почту технической поддержки по адресу support@rusiem.com для получения ключа лицензии.

5) Ключ лицензии генерируется на внутренних серверах RuSIEM. Ключ представляет собой зашифрованную строку.

6) Далее ключ передается ответным письмом по электронной почте заказчику. Лицензионный ключ привязан к аппаратной платформе сервера.

4. Установка системы

1) Запустить скрипт установки:

Создайте директорию `/opt/install/`, выполните следующую команду:

```
mkdir /opt/install/
```

Далее скопируйте файл `rusiem.rfrit.tgz` на сервер, затем скопируйте его в директорию `/opt/install/`, выполнив команду:

```
cp rusiem.rfrit.tgz /opt/install/
```

Затем перейдите в директорию `/opt/install/` и распакуйте архив, выполнив следующие команды:

```
cd /opt/install/
```

`tar xvzf rusiem.rfrit.tgz`

`bash ./install.sh`

2) Выбрать версию установки системы:

- Бесплатная версия RvSIEM;
- Коммерческая версия RuSIEM;
- Коммерческая версия RuSIEM с модулем аналитики RuSIEM Analytics;
- Модуль аналитики RuSIEM Analytics (установка на отдельный сервер);
- Коммерческая версия RuSIEM (без компонентов базы данных);
- Автономный сервер базы данных (без RuSIEM/RvSIEM).

3) Выбрать версию Elasticsearch.

4) Выбрать сохранение данных ClickHouse:

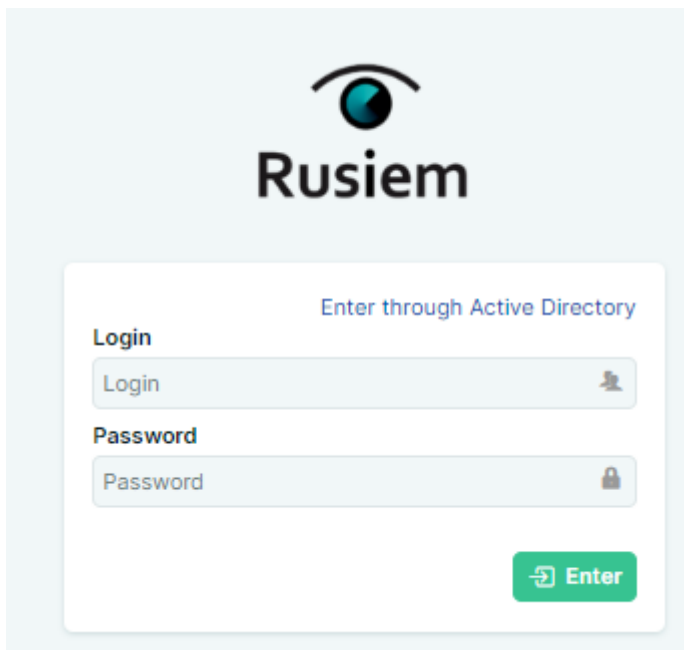
- 1 - сохранение данных будет произведено в `data/clickhouse`;
- 0 - сохранение данных в `var/lib/clickhouse`

5) Далее установка будет выполнена автоматически.

5. Активация системы

1) Откройте браузер и перейдите по адресу: https://IP-адрес_VM1

Должна отобразиться страница входа в систему:



Enter through Active Directory

Login

Login

Password

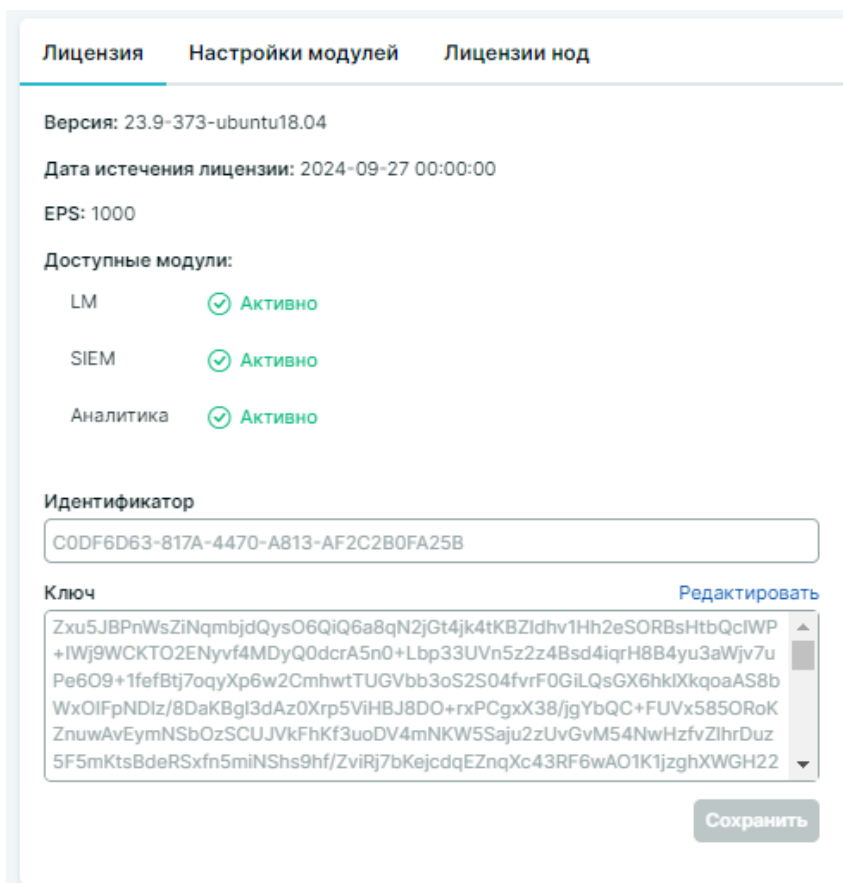
Password

Enter

Имя пользователя по умолчанию: admin;

Пароль по умолчанию: admin.

2) В разделе «Лицензия» пропишите ключ лицензии, дождитесь проверки ключа и подтверждения, что лицензия активна.



Лицензия Настройки модулей Лицензии нод

Версия: 23.9-373-ubuntu18.04

Дата истечения лицензии: 2024-09-27 00:00:00

EPS: 1000

Доступные модули:

LM	Активно
SIEM	Активно
Аналитика	Активно

Идентификатор

C0DF6D63-817A-4470-A813-AF2C2B0FA25B

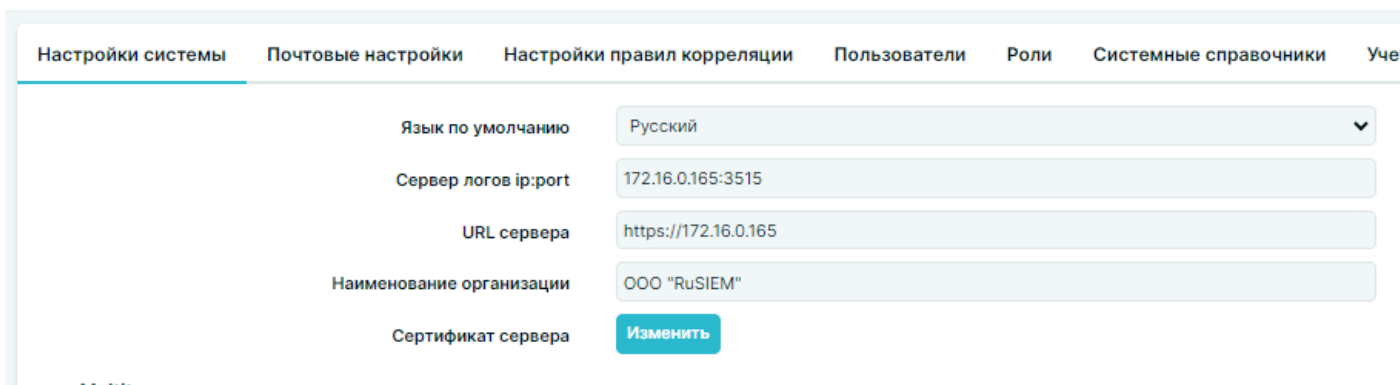
Ключ [Редактировать](#)

Zxu5JBPnWsZiNqmbjdQysO6QiQ6a8qN2jGt4jk4tKBZidhv1Hh2eSORBsHtbQcIWP
+IWj9WCKTO2ENyvf4MDyQ0dcrA5n0+Lbp33UVn5z2z4Bsd4iqrH8B4yu3aWjv7u
Pe6O9+1fefBtj7oqyXp6w2CmhwTUGVbb3oS2S04fvrF0GiLQsGX6hkiXkqoaAS8b
WxOIFpNDIz/8DaKBgl3dAz0Xrp5ViHBJ8DO+rxPCgxX38/jgYbQC+FUvX585ORoK
ZnuwAvEymNSbOzSCUJVkFhKf3uoDV4mNKW5Saju2zUvGvM54NwHzfvZlhrDuz
5F5mKtsBdeRSxfn5miNShs9hf/ZviRj7bKejcdqEZnqXc43RF6wAO1K1jzghXWGH22

Сохранить

3) В настройках системы пропишите следующие параметры (остальные настройки кроме указанных оставьте по умолчанию):

- Язык по умолчанию: любой;
- Host для подключения Elasticsearch: 127.0.0.1:9200;
- URL сервера: `https://адрес_сервера` (вспомогательный параметр, используется при формировании ссылок на инциденты в email-уведомлениях);
- Наименование организации: любое.



Настройки системы	Почтовые настройки	Настройки правил корреляции	Пользователи	Роли	Системные справочники	Уче
Язык по умолчанию	Русский					
Сервер логов ip:port	172.16.0.165:3515					
URL сервера	https://172.16.0.165					
Наименование организации	ООО "RuSIEM"					
Сертификат сервера	Изменить					

«Дополнительные настройки»:

- Версия Elasticsearch: проверить установленную версию в системе (`dpkg -l | grep elasticsearch`) и выбрать соответствующий вариант (По умолчанию: 5.x);
- Удаление информационных событий и Очистка устаревших данных: маска – по умолчанию, время хранения – установить требуемое; для начала рекомендуется оставить значения по умолчанию, впоследствии при наличии места на диске можно будет увеличить;
- Сервер логов ip:port: адрес и порт, по которым агент для Windows будет отправлять на сервер события; порт всегда 3515, адрес –адрес сервера SIEM (если отсутствует NAT между сервером и агентом), например: 10.10.10.123:3515;

Дополнительные настройки

Время жизни сессии	<input type="text" value="1440"/>	минут	
Host для подключения Elasticsearch	<input type="text" value="127.0.0.1:9200"/>	Версия	<input type="text" value="7.x"/>
Логин для подключения Elasticsearch	<input type="text"/>		
Пароль для подключения Elasticsearch	<input type="text"/>		
Маска для индекса в Elasticsearch	<input type="text" value="rusiem-*"/>		
Удаление информационных событий	маска индекса <input type="text" value="rusiem-inf*"/>	хранить	<input type="text" value="3"/> дней
Очистка устаревших данных	маска индекса <input type="text" value="rusiem-imp*"/>	хранить	<input type="text" value="7"/> дней
Подключение к ClickHouse	<input type="text" value="127.0.0.1"/>	порт:	<input type="text" value="8123"/>
Подключение к Redis	<input type="text" value="127.0.0.1"/>	порт:	<input type="text" value="6379"/>
Хост для правил корреляции	<input type="text" value="127.0.0.1"/>	порт:	<input type="text" value="8080"/>
Соединение с БД активов	<input type="text" value="127.0.0.1"/>	порт:	<input type="text" value="8888"/>
Устаревание активов	<input type="text" value="45"/> дней		
Время хранения инцидентов	<input type="text" value="3"/> года		

3. Установить оптимальный (равный половине ОЗУ) размер памяти для Elasticsearch

- 1) Выделите не менее 1 Гб ОЗУ под данные операционной системы.

`nano /etc/elasticsearch/jvm.options`

- 2) Раскомментируйте и измените значения:

`-Xms10g`

`-Xmx10g`

- 3) Перезапустить Elasticsearch командой:

`systemctl restart elasticsearch`

- 4) В `nano /etc/default/elasticsearch`

Раскомментировать:

`MAX_LOCKED_MEMORY=unlimited`

- 5) В `nano /etc/security/limits.conf`

Добавить перед строкой # End of file:

```
elasticsearch soft memlock unlimited
```

```
elasticsearch hard memlock unlimited
```

6) В `nano /usr/lib/systemd/system/elasticsearch.service`

Вставить в блок [Service]

```
LimitMEMLOCK=infinity
```

4. Проверить базы данных

1) Elasticsearch - на вкладке события должен отображаться график и список событий. Если последние события были более минуты назад, система неисправна.

2) PostgreSQL - вы сможете попасть в web интерфейс и залогиниться.

3) Clickhouse - должна открываться вкладка инцидентов без ошибок.

Также статус баз данных можно проверить из консоли:

```
systemctl status elasticsearch
```

```
systemctl status clickhouse
```

```
systemctl status PostgreSQL
```

Статус должен быть active.

5. Установка агента Rusiem

Установите агент RuSIEM на Windows (если вы планируете собирать события из других источников, кроме syslog). Один установленный агент может собирать из многих других источников удаленно безагентным методом.