NTechnology | SIEM

Руководство по установке

НЦОТ

Содержание

1. Общая информация о системе

1.1 О документе

Этот документ содержит информацию для планирования и выполнения развертывания компьютерной программы, предназначенной для сбора и анализа событий информационной безопасности (Security Information and Event Management system) «NTechnology SIEM» (далее – NT SIEM), а также о работе со службами сбора событий с машин Windows.

Комплект документации NT SIEM включает в себя следующие документы:

- Этот документ;
- Руководство по созданию запросов – содержит описание наборов запросов и результаты применения этих запросов;
- Руководство пользователя – содержит справочную информацию и инструкции по настройке и администрированию продукта. Содержит сценарии использования продукта для управления информационными активами организации и событиями информационной безопасности;
- Руководство по написанию правил – содержит рекомендации по созданию правил нормализации, агрегации, корреляции и обогащения событий.

1.2 О NT SIEM

NT SIEM – это система, которая осуществляет сбор, хранение и анализ событий, исходящих от сетевых устройств, средств защиты информации, баз данных, ключевых корпоративных ресурсов, инфраструктуры систем и приложений.

1.3 Краткое описание возможностей системы

Система NT SIEM предоставляет следующие основные функциональные возможности:

- Сбор журналов событий с различных источников;
- Визуализация данных в виде графиков, диаграмм в форме дашбордов;
- Анализ журналов событий в соответствии с правилами нормализации, корреляции, агрегации и обогащения;
- Формирование инцидентов на основе процессов агрегации, обогащения и корреляции;
- Управление инцидентами информационной безопасности;
- Хранение событий и инцидентов информационной безопасности;

- Фильтрация по различным параметрам событий и инцидентов, в том числе с использованием избранных запросов для быстрого доступа к фильтрам по событиям;
- Использование готовой базы правил, а также возможность создания собственных правил и табличных списков;
- Мониторинг состояния системы;
- Отправка уведомлений пользователям в рамках веб-приложения и по электронной почте;
- Формирование и выгрузка отчетов за определенный период времени;
- Осуществление интеграций, в том числе и с SOAR-системами.

2. Схема взаимодействия компонентов

Для обеспечения корректного взаимодействия компонентов системы должны быть доступны для соединения указанные на рисунке 1 порты.

Направленность стрелок указывает сетевые вызовы – от инициатора к получателю.

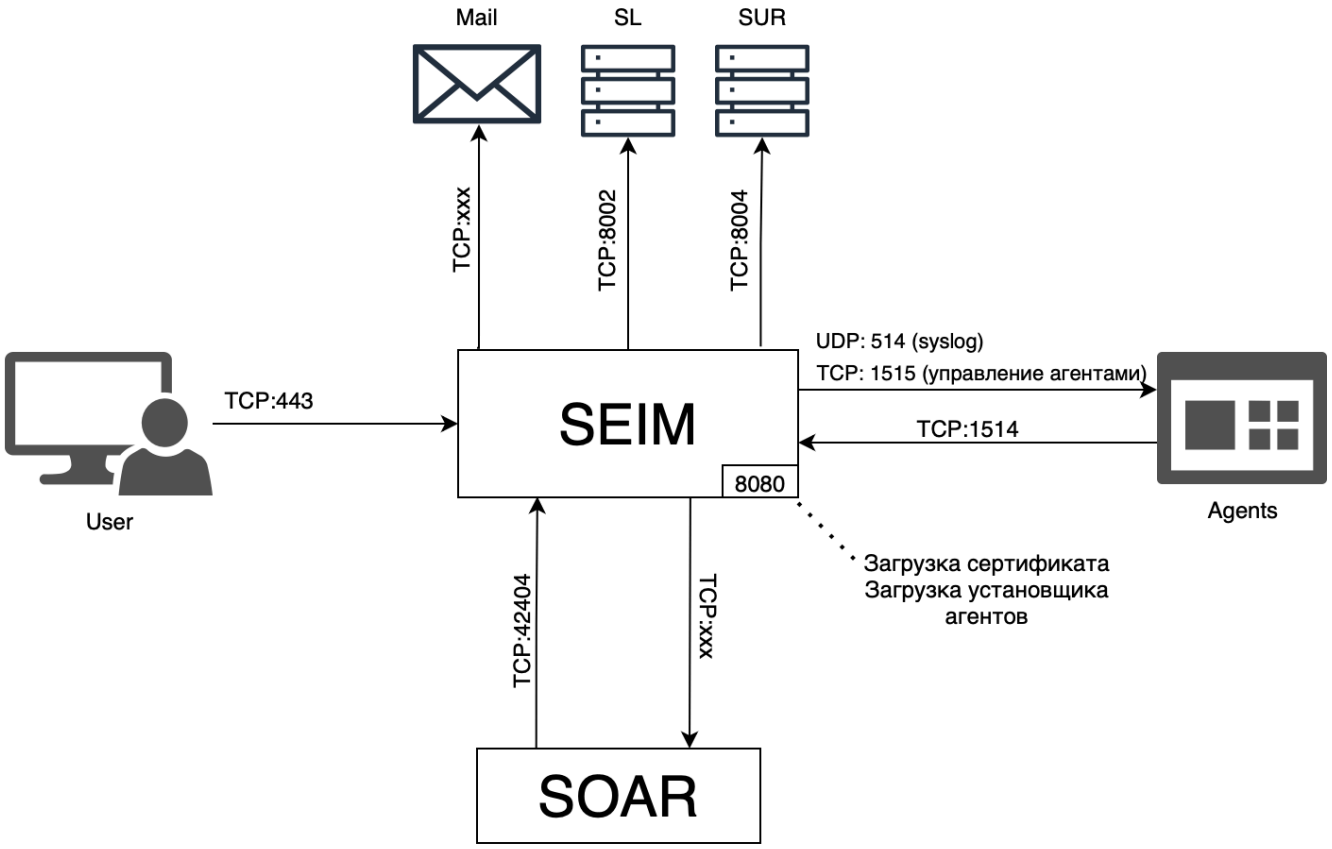

Рисунок 1 – Схема взаимодействия компонентов до версии NT SIEM v1.2.0

TCP:xxx – настраиваемые порты: для взаимодействия системы и почтового сервера для отправки электронных писем; для взаимодействия системы и SOAR для передачи инцидентов и/или событий.

Обратите внимание, что с версии NT SIEM v1.0.2 для работы с пользовательским интерфейсом на межсетевом экране должен быть открыт порт 443.

После версии NT SIEM v1.2.0 схема взаимодействия компонентов меняется: компоненты SL, SUR, Agents – не актуальны.

Направленность стрелок указывает сетевые вызовы – от инициатора к получателю.

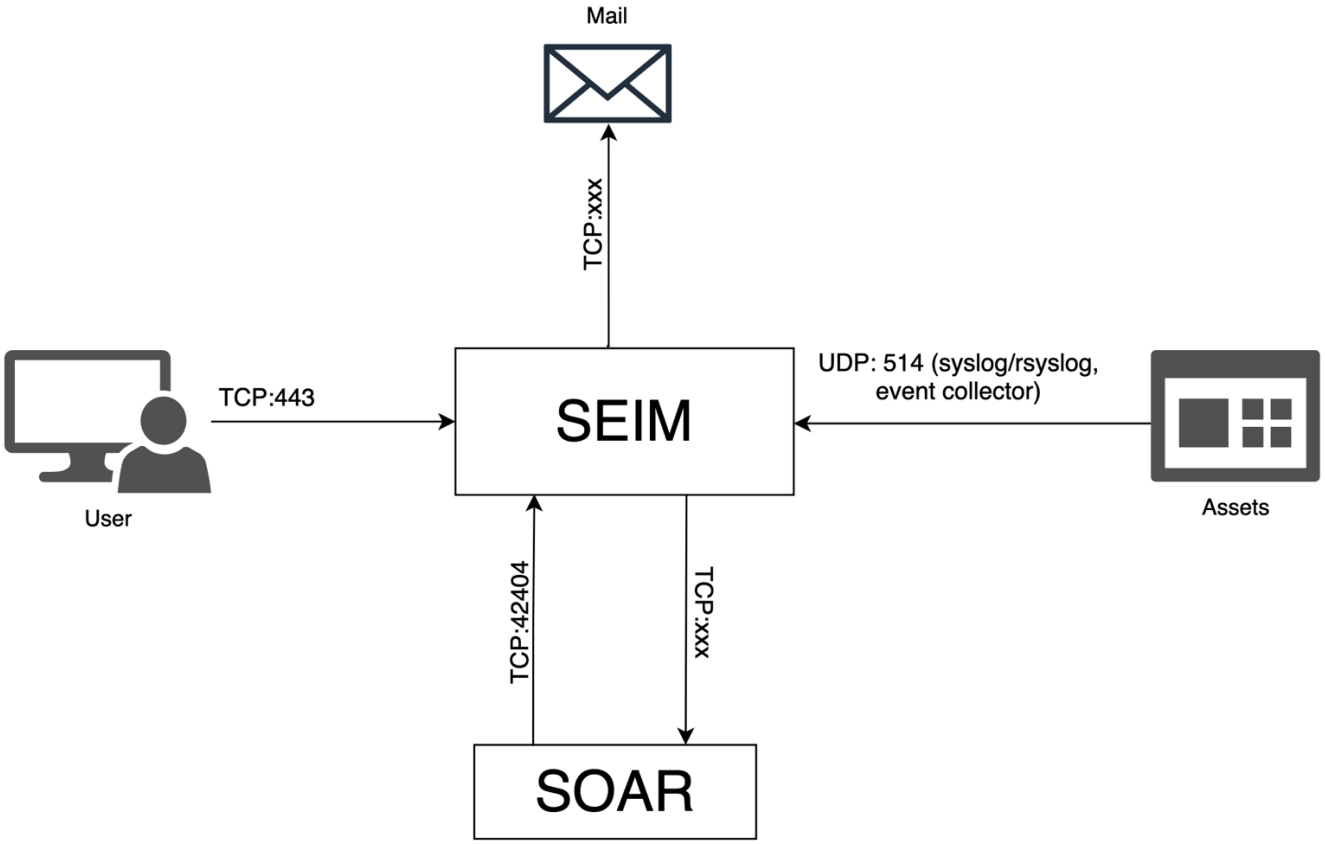

Рисунок 2 – Схема взаимодействия компонентов после версии NT SIEM v1.2.0

3. Сценарий развертывания системы

3.1 Аппаратные и программные требования

Дистрибутив NT SIEM подготовлен для установки на операционную систему (далее – ОС) Ubuntu Server 22.04 (на базе ядра Linux версии 5.19 и выше). При установке Ubuntu Server 22.04 необходимо обратить внимание на следующие шаги:

– Разметка дискового пространства. Необходимо смонтировать все свободное пространство под корневую директорию (рис. 2).

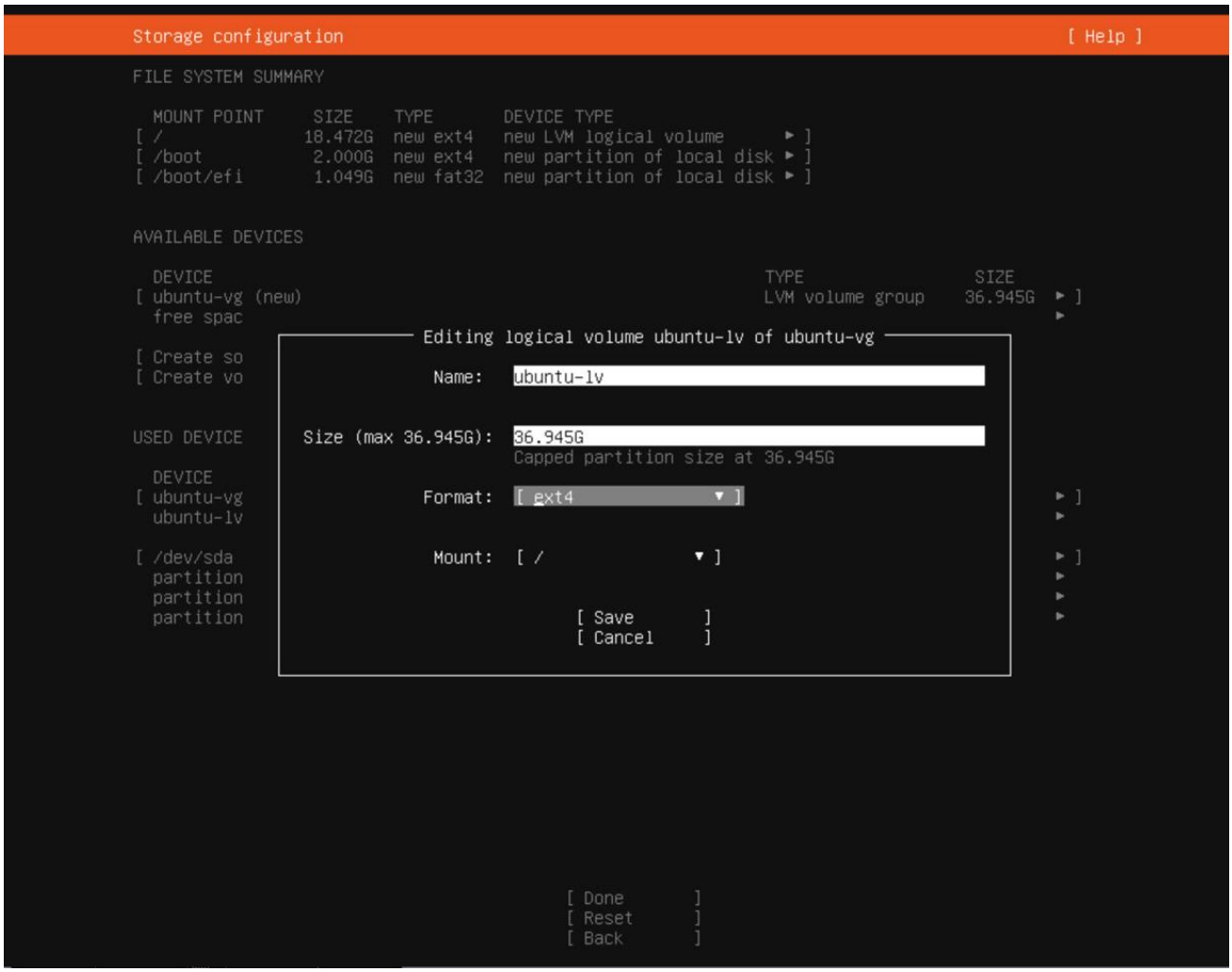

Рисунок 3 – Разметка дискового пространства

– Выбор наборов пакетов. На данном этапе не следует выбирать ни один из наборов пакетов. В противном случае дальнейшая установка может быть выполнена некорректно.

Кроме того, для своей работы NT SIEM использует данные, поставляемые сторонними программными продуктами – агентами, которые могут быть установлены на операционных системах семейств Linux, Windows.

Перед развертыванием NT SIEM необходимо настроить на Firewall правила для корректной работы в пользовательском интерфейсе.

Для работы в интерфейсе NT SIEM рекомендуется использовать последние версии браузеров Google Chrome, Microsoft Chromium Edge, Mozilla Firefox.

Для расчета необходимого дискового пространства следует использовать следующую формулу с учетом количества событий, генерируемых в секунды (EPS):

Объем данных (ГБ) = EPS × Размер события (байт) × Время хранения (секунды)

Далее предлагается рассмотреть пример расчета необходимого дискового пространства для 1000 EPS.

Таблица 1 – Данные для расчета

Показатель	**Значение**
EPS	1000
Средний размер события	1 КБ (1024 байта).
Время хранения	30 дней (2 592 000 секунд).

Подставив данные в формулу, получим:

Объем данных = 1000 × 1024 × 2 592 000 ≈ 2.59 ТБ.

Таким образом, для хранения данных за 30 дней потребуется около 2.6 ТБ дискового пространства.

Аналогично можно посчитать, что для 1000 EPS требуется пространство в 25 ТБ с расчетом на то, что данные должны хранится год. Пример конфигурации системы для 1000 EPS отражен в таблице 2.

Таблица 2 – Примеры конфигурации для 1000 EPS

Компонент	**CPU min (ядра)**	**CPU rec (ядра)**	**RAM min (Гб)**	**RAM rec (Гб)**
Manager	4	6	8	16
Indexer	6	8	16	32
Остальные сервисы	2	4	8	16
Всего	12	18	32	64

3.2 Установка системы NT SIEM

Для того, чтобы начать процесс установки NT SIEM необходимо скачать и распаковать исходные файлы из дистрибутива, предоставляемого производителями NT SIEM.

Для того, чтобы распаковать исходные файлы следует переключиться на пользователя `root`, имеющего администраторский доступ к вашей системе, и выполнить команду для создания временной директории:

```
mkdir temp/
```

```
tar -zxvf NtechnologySiem_v1.2.0.tar.gz -C temp/
```

После распаковки архива необходимо перейти в директорию, где будут находиться два файла `1.2.0.tar.gz`, `new_install.sh` и папки с документацией, базой правил и инсталлятором служб сборки событий. Для перехода следует выполнить команду:

```
cd temp/
```

Далее необходимо поменять права доступа для файла `new_install.sh`, который уже входит в состав дистрибутива. Для этого необходимо ввести в консоли следующую команду:

```
chmod u+x new_install.sh
```

После изменения прав доступа ввести в консоли команду для запуска скрипта установки:

```
./ new_install.sh
```

После произведенных команд необходимо ввести значения в интерактивной меню для файла-шаблона `project_variables`, который уже входит в состав дистрибутива.

Вопросы для заполнения:

- Ввести IP-адрес хоста машины, где будет произведена установка системы;
- Ввести Network Syslog. В данной опции следует указывать из каких ip-сетей осуществлять сбор событий. По умолчанию, NETWORK=0.0.0.0, что означает, что сбор событий происходит из всех подсетей;
- Ввести маску сети. По умолчанию, MASK=0;
- Указать, сколько выделить оперативной памяти, но не более 50 % от общей оперативной памяти. Обратить внимание, что необходимо выбрать цифру, под которой указана нужная вам оперативная память:

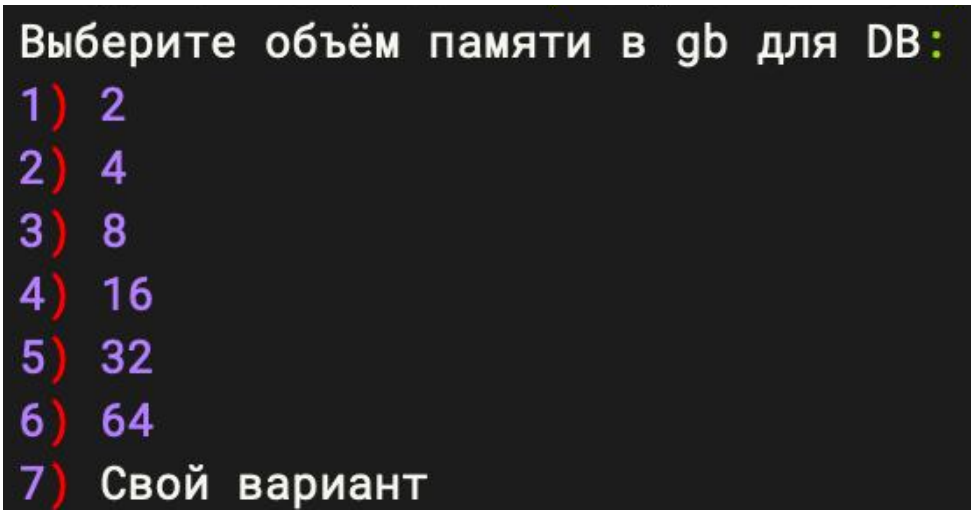

Рисунок 4 – Варианты объема оперативной памяти

Если вам необходимо написать свою величину, то пишете цифру 7 и следующей командой вводите значение в ГБ.

Процесс установки занимает несколько минут. Управление NT SIEM осуществляется через веб-интерфейс. Для этого следует открыть браузер Google Chrome и ввести в адресной строке IP-адрес (`https://IP_Address`, где IP_Address – IP-адрес сервера, где производилась инсталляция NT SIEM). Первая загрузка веб-интерфейса может занять несколько минут.

При необходимости можно изменить настройки по умолчанию сети `Docker (172.17.0.1)`, для этого необходимо:

1. Создать или отредактировать файл `/etc/docker/daemon.json`

```
sudo nano /etc/docker/daemon.json
```

2. Добавить или заменить содержимое, где `bip` — это IP-адрес и подсеть для интерфейса `docker0`:

```
{
  "bip": "100.100.1.1/16"
}
```

Следует убедиться, что выбранная сеть **не конфликтует** с локальной или VPN-сетью.

3. Перезапустить `Docker`

```
sudo systemctl restart docker
```

После загрузки веб-интерфейс будет выглядеть на как рисунке 5.

Рисунок 5 – Страница авторизации системы NT SEIM

В ходе установки системы также подгружаются системные правила, используемые для обработки и анализа данных в NT SIEM.

Учетная запись администратора по умолчанию имеет атрибуты:

- имя пользователя: admin;
- пароль: sTr0n&gg.

Рекомендуется изменить пароль сразу после входа в веб-интерфейс. В дальнейшем можно создать и другие учетные записи, например, с ролью администратора или оператора.

Для смены пароля у учетной записи администратора следует:

- Выбрать в боковом меню страницу «Настройки системы» (рис.5).
- На вкладке «Пользователи» выбрать пользователя с ролью «Супер Администратор».
- Нажать на кнопку «Редактировать».
- Ввести новый пароль.
- Нажать на кнопку «Сохранить».

Как результат, пароль учетной записи администратора изменится. Если Пользователь не подтверждает свое действие или при нажатии на кнопку «Отмена», все данные остаются неизменными.

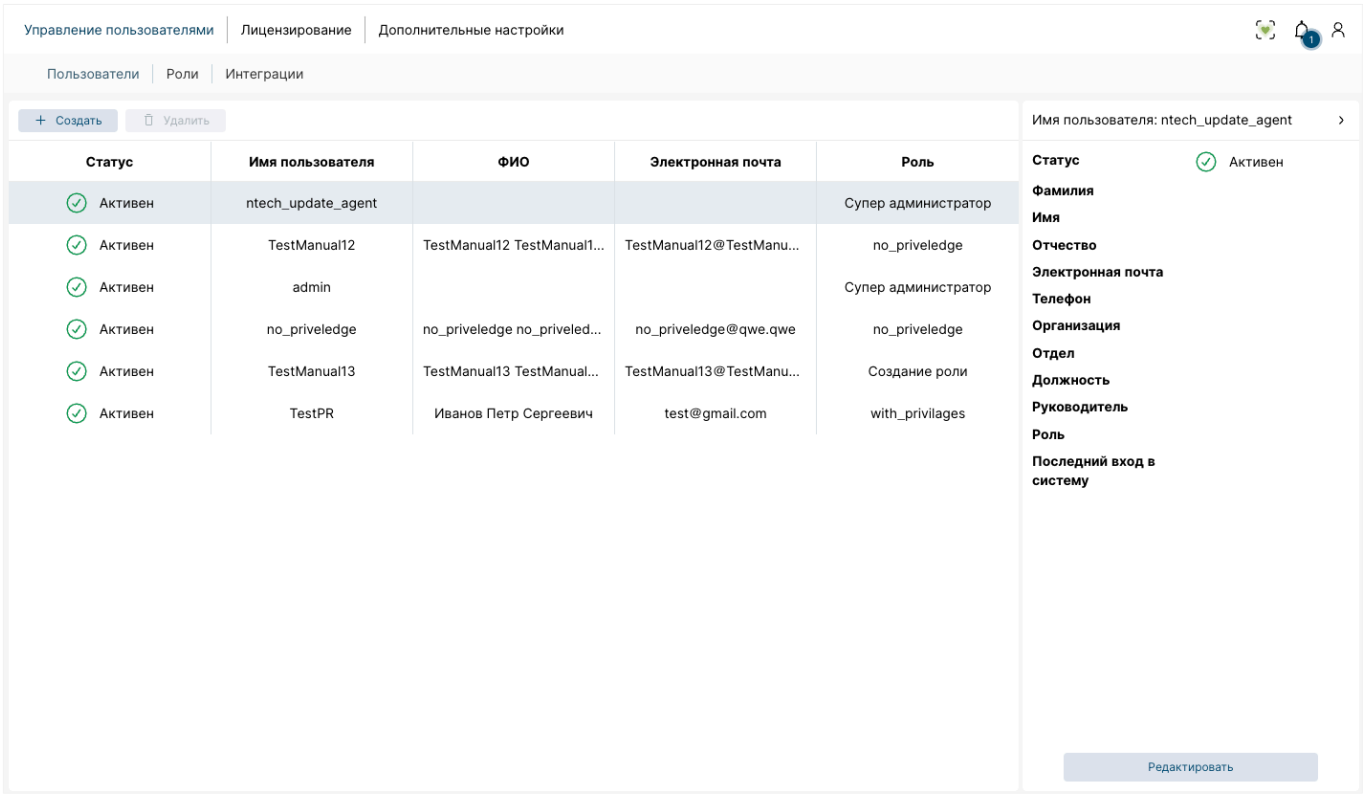

Рисунок 6 – Страница «Настройки системы»

3.3 Синхронизация времени на серверах

Для корректной работы системы необходимо настроить синхронизацию времени.

Первым шагом, необходимо установить «chrony» с помощью следующей команды:

```
sudo apt install chrony
```

Далее, необходимо убедиться, что виртуальная машина имеет доступ в интернет. Если доступ в Интернет отсутствует, то необходимо отредактировать файл `/etc/chrony/chrony.conf`, заменив значение NTP-сервера на имя или IP-адрес внутреннего NTP-сервера вашей организации.

Затем необходимо запустить сервис синхронизации системного времени, выполнив команду:

```
sudo systemctl enable --now chrony
```

Через несколько секунд выполнить команду:

```
sudo timedatectl | grep 'System clock synchronized'
```

При успешной синхронизации системного времени, вывод будет содержать строку:

```
System clock synchronized: yes.
```

3.4 Добавление лицензии

После установки системы, для получения полного функционала системы, необходимо загрузить ключ лицензии: с/без подключения к серверу лицензирования.

Для этого сначала необходимо перейти на группу страниц «Настройки системы», а затем на страницу «Лицензирование» (рис.7), скопировать данные из поля «Хэш» с помощью и передать его поставщику системы.

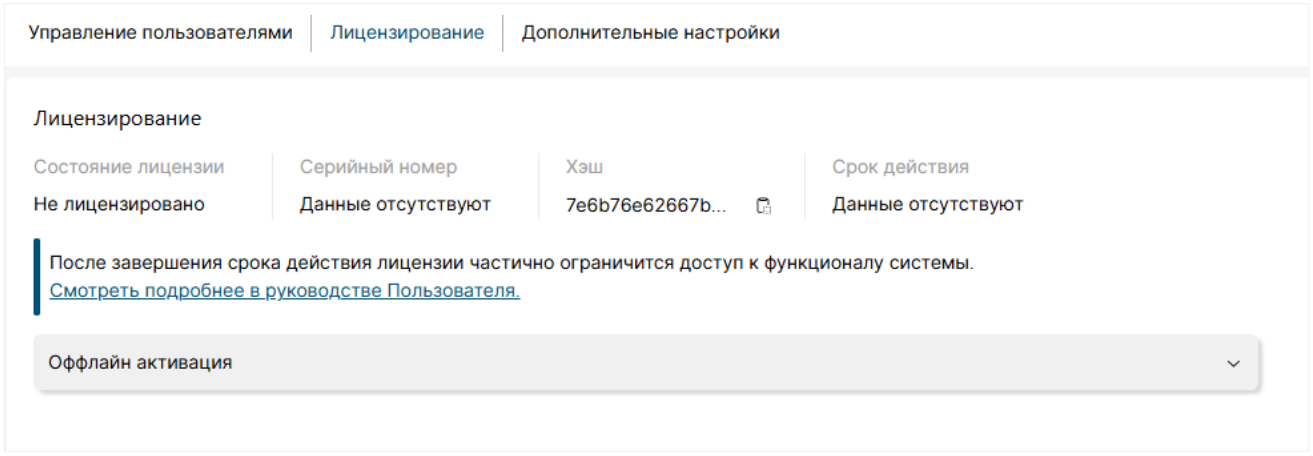

Рисунок 7 – Страница «Лицензирование» без активной лицензии»

После чего поставщиком системы будет выдан файл с расширением `.dat`, который необходимо будет загрузить вручную. Для этого необходимо перетащить файл в поле (рис.8) для загрузки или нажатием на данное поле, открыть проводник и выбрать файл. В случае продления лицензии, весь процесс необходимо будет повторить.

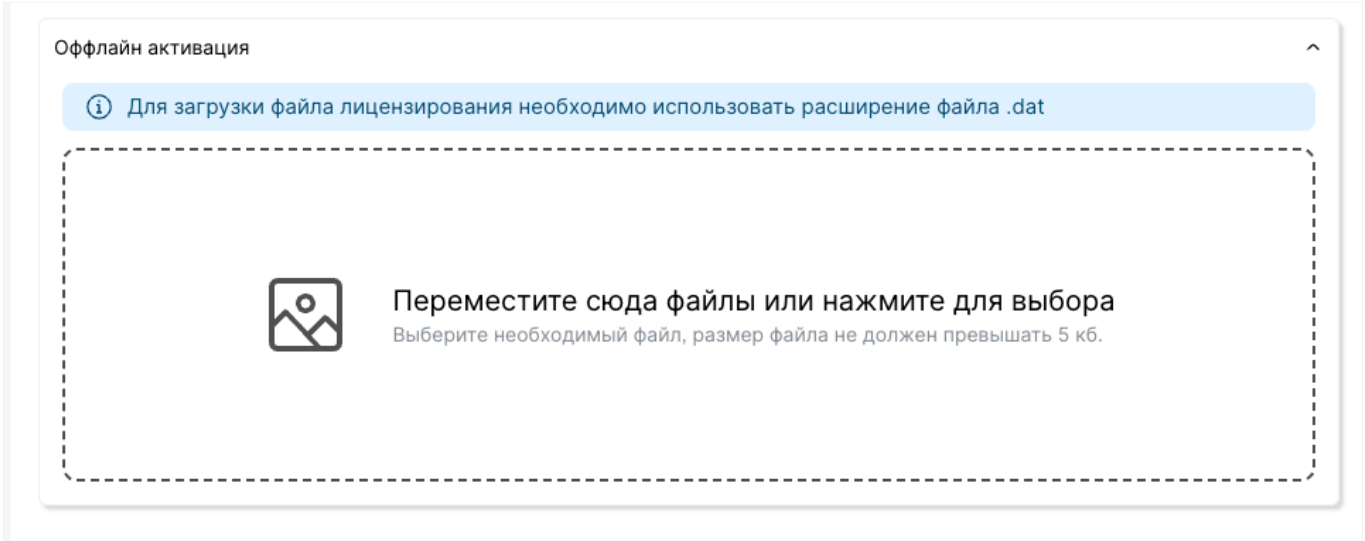

Рисунок 8 – Блок «Оффлайн активация»

При успешной установке лицензии поля «Серийный номер лицензии» и «Срок действия» будут заполнены данными о текущей лицензии, и состояние лицензии изменится на «Активна» (рис.9).

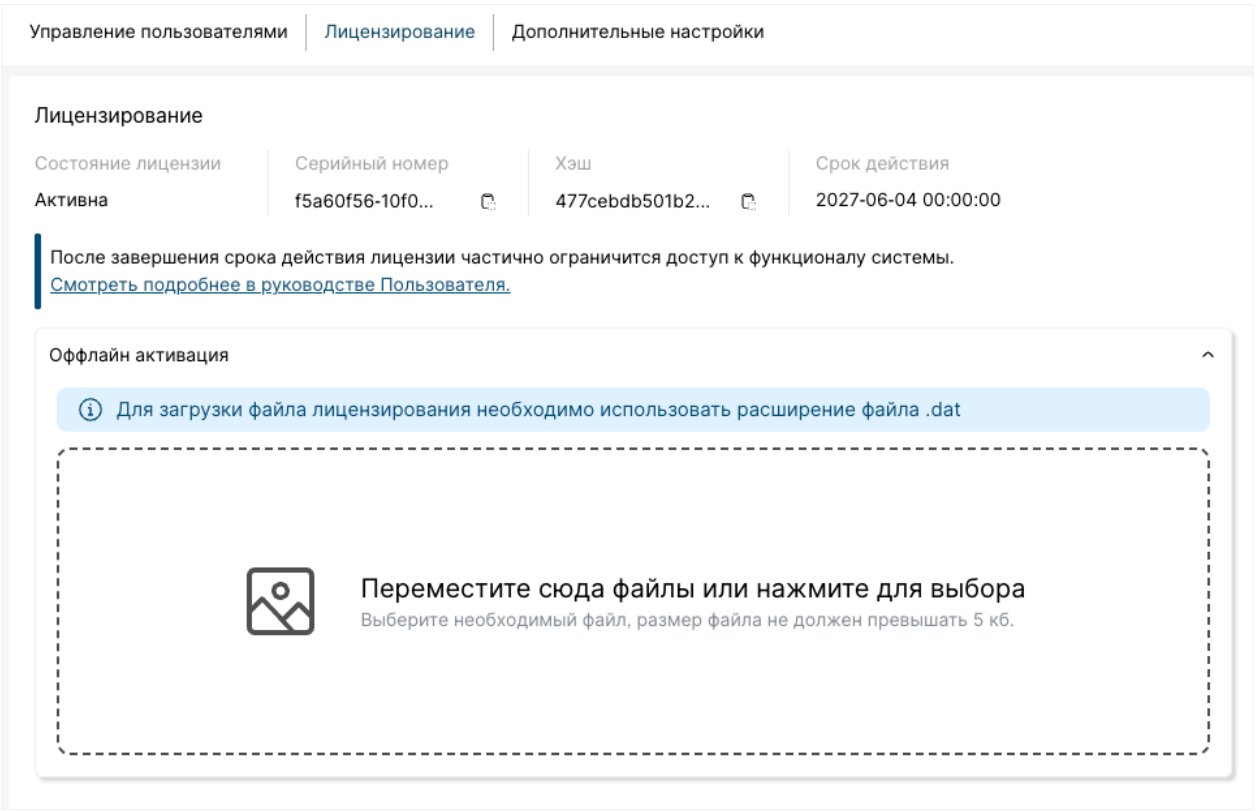

Рисунок 9 – Страница «Лицензирование» с активной лицензией

Следует обратить внимание, что при изменении конфигурации, необходимо обновление лицензии, для этого следует обратиться к поставщику программного обеспечения.

4. Установка обновлений

Обратите внимание, что установка версий выполняется последовательно. Например, перед установкой версии NT SIEM v1.0.2 сначала необходимо установить NT SIEM v1.0.1 и только потом начинать процесс установки NT SIEM v1.0.2, иначе процесс установки будет завершен неудачно.

4.1 Установка обновления NT SIEM v1.0.1

В период установки новой версии могут происходить потери событий, следовательно для их минимизации, рекомендуется проводить обновления в периоды низкой нагрузки.

Для установки версии NT SIEM v1.0.1 необходимо распаковать архив с расширением .tar в директорию, в которой установлен NT SIEM.

```
tar -xzvf 1.0.1.tar.gz -C siem-docker/
```

Далее необходимо перейти в директорию `siem-docker`:

```
cd siem-docker/
```

После перехода в директорию следует выполнить команды:

```
chmod u+x 1.0.1.sh
./1.0.1.sh
```

4.2 Установка обновления NT SIEM v1.0.2

Перед установкой версии NT SIEM v1.0.2 необходимо удостовериться, что версия NT SIEM v1.0.1 уже установлена. Иначе, процесс установки NT SIEM v1.0.2 будет завершен неудачно.

В период установки новой версии могут происходить потери событий, следовательно для их минимизации, рекомендуется проводить обновления в периоды низкой нагрузки.

Далее необходимо распаковать архив с расширением .tar в директорию, в которой установлен NT SIEM.

```
tar -xzvf 1.0.2.tar.gz -C siem-docker/
```

Далее необходимо перейти в директорию `siem-docker`:

```
cd siem-docker/
```

После перехода в директорию следует выполнить команды:

```
chmod u+x 1.0.2.sh
./1.0.2.sh
```

4.3 Установка обновления NT SIEM v1.1.0

Перед установкой версии NT SIEM v1.1.0 необходимо удостовериться, что версия NT SIEM v1.0.2 уже установлена. Иначе, процесс установки NT SIEM v1.1.0 будет завершен неудачно.

Далее необходимо распаковать архив с расширением .tar в директорию, в которой установлен NT SIEM.

```
tar -xzvf 1.1.0.tar.gz -C siem-docker/
```

Далее необходимо перейти в директорию `siem-docker`:

```
cd siem-docker/
```

После перехода в директорию следует выполнить команды:

```
chmod u+x 1.1.0.sh
./1.1.0.sh
```

4.4 Установка обновления NT SIEM v1.1.1

Перед установкой версии NT SIEM v1.1.1 необходимо удостовериться, что версия NT SIEM v1.1.0 уже установлена. Иначе, процесс установки NT SIEM v1.1.1 будет завершен неудачно.

Далее необходимо распаковать архив с расширением .tar в директорию, в которой установлен NT SIEM.

```
tar -xzvf 1.1.1.tar.gz -C siem-docker/
```

Далее необходимо перейти в директорию `siem-docker`:

```
cd siem-docker/
```

После перехода в директорию следует выполнить команды:

```
chmod u+x 1.1.1.sh
./1.1.1.sh
```

4.5 Установка обновления NT SIEM v1.1.2

Перед установкой версии NT SIEM v1.1.2 необходимо удостовериться, что версия NT SIEM v1.1.1 уже установлена. Иначе, процесс установки NT SIEM v1.1.2 будет завершен неудачно.

Далее необходимо распаковать архив с расширением .tar в директорию, в которой установлен NT SIEM.

```
tar -xzvf 1.1.2.tar.gz -C siem-docker/
```

Далее необходимо перейти в директорию `siem-docker`:

```
cd siem-docker/
```

После перехода в директорию следует выполнить команды:

```
chmod u+x 1.1.2.sh
./1.1.2.sh
```

4.6 Установка обновления NT SIEM v1.2.0

Перед установкой версии NT SIEM v1.2.0 необходимо удостовериться, что версия NT SIEM v1.1.2 уже установлена. Иначе, процесс установки NT SIEM v1.2.0 будет завершен неудачно. Либо необходимо сразу ставить систему с версией v1.2.0.

Для того, чтобы распаковать исходные файлы следует переключиться на пользователя `root`, имеющего администраторский доступ к вашей системе, и выполнить команду для создания временной директории:

```
mkdir temp/
tar -zxvf NtechnologySiem_v1.2.0.tar.gz -C temp/
```

После распаковки архива необходимо перейти в директорию, выполнив команду, где будут находиться два файла `1.2.0.tar.gz, new_install.sh`:

```
cd temp/
```

Далее необходимо поменять права доступа для файла `new_install.sh`, который уже входит в состав дистрибутива. Для этого необходимо ввести в консоли следующую команду:

```
chmod u+x new_install.sh
```

После изменения прав доступа ввести в консоли команду для запуска скрипта установки:

```
./ new_install.sh
```

5. Работа с сервисами для сбора событий с Windows

5.1 Установка, удаление, остановка работы сервиса

Перед установкой сервиса необходимо заполнить файл конфигурации (п.5.2). Для того чтобы установить сервис, необходимо запустить файл инсталлятор `ntechnology-events-collector-x32.exe` или `ntechnology-events-collector-x64.exe` с параметром `install`, которые находятся в директории `NtechnologyEventsCollector` в распакованном при установке архиве.

После запуска инсталлятор запускает службу сбора событий и создает файл конфигурации в папке `C:\Program Files \NEC`. Там же будут хранить логи по работе сервиса. Можно запустить с параметром `start`, удалить с параметром `uninstall` или остановить работу сервиса с параметром `stop`.

5.2 Заполнение файла конфигурации

Для корректной работы необходимо заполнить файл конфигурации. Файл конфигурации должен быть в формате `.toml`. Шаблон представлен ниже:

```
# # Service is enabled, can be started manually (Required).
# service_start_type = "OnDemand"
# # Disabled service (Required).
# service_start_type = "Disabled"
# # Autostart on system startup (Required).
service_start_type = "AutoStart"
# # Start delay in secs (Required).
start_delay = 10

[nec_config]
# Log level. One of ["info", "debug","error", "warn", "trace"].
# Default = "info"
log_level = "info"

# Win Event Wmi section.
# Can connect to local machines.
# Describes by set (must be uniq) of [[nec_config.win_event_wmi]] sections.
```

```
# Local 1
[[nec_config.win_event_wmi]]

[nec_config.win_event_wmi.local]
# Namespace path (Optional, default = "ROOT\\\\CIMV2").
# namespace_path = "local1"

[nec_config.win_event_wmi.local.poll_config]
# Polling interval in secs (Required).
interval = 5
# List of log files (Required).
log_files = ["Application"]



# # Local 2
# [[nec_config.win_event_wmi]]

# [nec_config.win_event_wmi.local]
# # Namespace path (Optional, default = "ROOT\\\\CIMV2").
# namespace_path = "local2"

# [nec_config.win_event_wmi.local.poll_config]
# # Polling interval in secs (Required).
# interval = 5
# # List of log files (Required).
# log_files = ["Application", "Windows Powershell"]



# # Win Event Subscriber section (enable only for Windows.Client >= Vista &
Windows.Server >= 2008).
# [nec_config.win_event_subscriber]
# # A query that specifies the types of events that you want the
subscription service to return.
# x_query = '''
# <QueryList>
#   <Query Id="0">
#     <Select Path="Windows PowerShell">*</Select>
```

```
#     <Select Path="Application">*</Select>
#   </Query>
# </QueryList>
# '''



# File Watcher section.
[nec_config.file_watcher]
# Paths for watch (Required).
paths = ['D:\path.txt']
# # Retrys to send event to inner channel (Optional, default = 3).
# send_to_channel_retrys = 3

# Poll watcher kind.
[nec_config.file_watcher.watcher_kind.poll]
# Polling interval in secs (Required).
interval = 5

# # Recommended watcher (get notification from system, maybe not work in
some cases).
# [nec_config.file_watcher.watcher_kind.recommended]



# Event Sender section.

# Udp section.
[nec_config.event_sender_config.udp]
local_addr = "0.0.0.0"
local_port = 8081
remote_addr = "127.0.0.1"
remote_port = 514
# # Bound of inner channel for events (Optional, default = 10000).
# channel_bound = 10000

# # Tcp section.
# [nec_config.event_sender_config.tcp]
# remote_addr = "127.0.0.1"
# remote_port = 8888
```

Описание файла конфигурации и его составляющий представлена в таблице 3:

Таблица 3– Параметры файла конфигурации

Параметр	**Описание**
Конфигурация сервиса	
`service_start_type`	Допустимые значения: `OnDemand` – сервис включен, но необходим ручной запуск; `Disabled` – сервис выключен; `AutoStart` – сервис включен и запускается автоматически; `start_delay = 10` – время ожидания запуска после поднятия системы в секундах, используется при `service_start_type = "AutoStart"` .
Конфигурация коллектора `[nec_config]`	
`log_level`	По умолчанию, `log_level = "info"` Допустимые значения: `info` – минимально необходимая информация; `debug` – подробная информация необходимая для отладки приложения; `error` – ситуация которая не должна была случиться в приложении (ошибка); `warn` – предупреждение; `trace` – полное логирование всех входящих и исходящих сообщений.
Блок `[nec_config.win_event_wmi]`	
`namespace_path`	Путь до возможного пространства имен. По умолчанию, `default = "ROOT\\\\CIMV2"`
`[nec_config.win_event_wmi.local.poll_config]`	

Параметр	Описание
log_files	Массив названий каналов, откуда будут собираться события.
interval	Частота сбора событий, в секундах.
Блок [nec_config.win_event_subscriber]	
x_query	Обязательно поле для указания каналов сбора событий.
<Select Path="Windows PowerShell">*</Select>	* – используется для задания фильтра поиска событий.
Блок [nec_config.file_watcher]	
paths	Массив путей до файлов, с которых необходимо совершать сбор событий.
send_to_channel_retrys	Количество попыток для отправки данных по каналу channel_bound.
[nec_config.file_watcher.watcher_kind.poll]	
interval	Частота сбора событий, в секундах.
Блок [nec_config.event_sender_config.udp]	
local_addr	По умолчанию, local_addr = "0.0.0.0" IP-адрес, откуда будет совершаться сбор данных.
local_port	Порт, откуда будет совершаться сбор данных.
remote_addr	IP-адрес, где стоит SIEM-система для передачи собранных событий.
remote_port	Порт, где стоит SIEM-система для передачи собранных событий.
channel_bound	По умолчанию, channel_bound = 10000. Размер очереди событий.
Блок [nec_config.event_sender_config.tcp]	
remote_addr	IP-адрес, где стоит SIEM-система для передачи собранных событий.

Параметр	Описание
remote_port	Порт, где стоит SIEM-система для передачи собранных событий.

Блоки `Win Event Wmi` и `Win Event Subscriber` собирают события из `Windows Event Log`.

Блок `Win Event Subscriber` рекомендуется для использования, так как данные Windows машина передает сама, и нет необходимости в постоянном опросе. Однако есть ограничения. Блок `Win Event Subscriber` недоступен для `Windows.Client >= Vista & Windows.Server >= 2008`.

Блок `File Watcher` используется для подключения к файлам с целью мониторинга и сбора событий.

Блок `Poll watcher kind` используется для указания интервала опроса.

Блок `Event Sender` используется для указания параметров, определяющих, куда направлять собранные данные.