RuSIEM

Руководство по экспулатации администратора

2023

Содержание

1. Общие сведения

1.1 Назначение системы

Полная версия системы предназначена как для сбора и анализа информации, так и для обнаружения атак и различных аномалий в организации, проведения глубокого анализа и проактивного поиска угроз, а также оперативного реагирования на инциденты и их дальнейшего расследования. Система способна выявить угрозу, когда обычные средства детектирования по отдельности её не видят, но она может быть обнаружена при тщательном анализе и корреляции информации из различных источников.

Полная версия системы предоставляет следующие функциональные возможности:

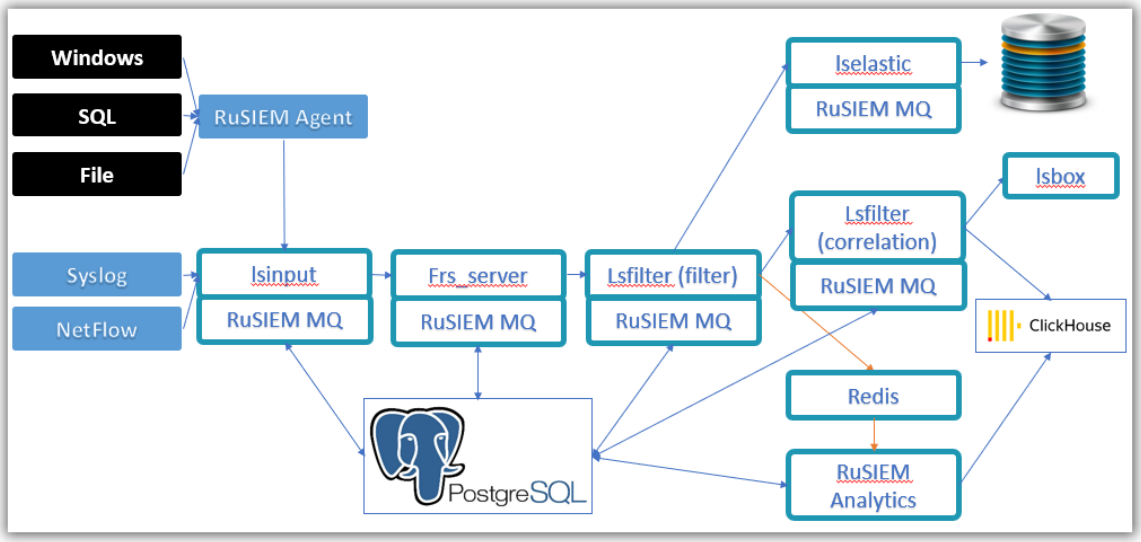
- сбор с помощью собственного агента и пассивный прием событий;
- нормализация событий с долгосрочным хранением и оперативным поиском;
- обогащение событий мета-информацией, описывающей о чем событие в понятном для пользователя формате;
- поиск по событиям без знания типов и состава событий на основе симптоматики;
- приоритезация событий посредством весов симптоматики, в том числе составным весом;
- корреляция на последовательных событиях (счетчик);
- триггерная корреляция фактов различных событий;
- агрегация весов по объектной модели для обнаружения угроз без применения сигнатур;
- проверка ip, fqdn, md5/sha1 file, url, email по фид-листам с угрозами;
- встроенный инцидент-менеджмент для реагирования и фиксации угроз;

- автоматическое обновление продукта, правил корреляции, симптоматики и фидов;
- ролевая модель доступа в систему.

Бесплатная версия системы является системой класса Log Management и предназначена для сбора информации, ее нормализации и обогащения, без возможности проводить анализ.

1.2 Архитектура системы

Архитектура системы представлена ниже.



Система состоит из набора микросервисов выполняющие определенные задачи:

- **RuSIEM Agent** - отвечает за сбор событий с Windows систем, SQL серверов, файловых логов;
- **lsinput** - отвечает за прием событий от различных источников (Syslog, NetFlow, RuSIEM Agent). Isinput принимает события, ставит их в очередь и передает дальше по цепочке;
- **Frs_server** - отвечает за нормализацию событий (разделение событий по полям на основе встроенных правил (по таксономии));
- **Lsfilter (filter)** - отвечает за функционал симптоматики (обогащения событий полезной информацией - добавление описания и критичности событий);

- **lselastic** - отвечает за запись событий в elasticsearch для дальнейшей работы с событиями (поиск, просмотр, анализ, отчеты, ретроспективный анализ);
- **Lsfilter (correlation)** - отвечает за корреляцию событий по инцидентам генерируемых системой в процессе работы; **(доступно в платной версии)**
- **RuSIEM Analytics** - отвечает за поиск аномалий. **(доступно в платной версии, по отдельной лицензии)**

1.3 Требования к программному обеспечению

Требования к программному обеспечению:

Требования к операционной системе серверных компонентов (ОС)	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) Ubuntu Server 22.04 LTS (Jammy Jellyfish) x64 - https://releases.ubuntu.com/22.04 (и там актуальный Server Install image for 64-bit PC, например ubuntu-22.04.2-live-server-amd64.iso) Astra Linux Special Edition РУСБ.10015-01 (версия не ниже обновления 1.7).
Требования к операционной системе (ОС) для программного компонента «Агент»	Microsoft Windows 7 SP1 или выше с установленными компонентами программного обеспечения Microsoft Windows Imaging Component и Microsoft .NET Framework 4.5
Требования к браузерам для доступа к интерфейсу RuSIEM	• Google Chrome, версии не менее чем 9.0; • Safari, версии не менее чем 5.0.5; • Mozilla Firefox, версии не менее чем 3.0; • Internet Explorer, версии не менее чем 7.0;

	• Opera, версии не менее чем 10.5

1.4 Требования к аппаратному обеспечению

Минимальные требования к аппаратному обеспечению для 1000 событий в секунду (EPS)	• vCPU: не менее 16 потоков, работающих на частоте не менее 2.4 ГГц; • RAM: не менее 32 ГБ; • HDD (системные данные): не менее 200 ГБ; • HDD (Хранение данных): не менее 500 ГБ; • Сетевой интерфейс: Ethernet 100/1000 Мбит/с.
Гипервизор среды виртуализации	• VMWare Esxi версии 5.1 или выше; • Microsoft Hyper-V. • ProxMox VE

2. Установка системы

2.1 Важная информация перед установкой системы

2.1.1 Факторы при планировании

При планировании следует учитывать:

- Детализация аудита на источниках – важный фактор. Включать абсолютно весь имеющийся аудит на источниках бессмысленно. Необходимо совместно с вендором или интегратором выбрать источники и уровень детализации аудита исходя из решаемых кейсов, критичности актива, информативности событий;

- Загруженность имеющихся гипервизоров. Большой поток событий не просто принимается и сохраняется в базы данных, но также осуществляется детальная обработка событий по множеству условий;

- Аналитика – это не просто скоуп условий. Это поиск взаимосвязей по миллионам возможных комбинаций что требует довольно мощных ресурсов;

- Учитывайте, что вы желаете собирать, с каких источников, нужны ли все события сохранять (к примеру – нужно ли сохранить события о разрешенных соединениях и как долго требуется хранить);

- Учитывайте каналы связи между удаленными объектами. Возможно стоит поставить выделенный отдельный сервер или виртуальную машину вместо передачи событий;

- Учитывайте разрешенные зоны соединений. Возможно, если политикой запрещены соединения по сети – стоит пересмотреть расположение агентов/серверов или организовать выделенные vlan;

- Обеспечение непрерывности/резервирования/архивного хранения.

2.1.2 Планирование дискового пространства

При планировании развертывания RUSIEM следует корректно учитывать выделение ресурсов, так как источники могут быстро заполнить дисковое пространство.

Нельзя использовать авторасширение дисков. Следует выделять статичные ресурсы.

Можно воспользоваться следующей примерной оценкой, приведенной в таблице ниже.

Источник	**Минимальный аудит, EPS**	**Полный аудит, EPS**	**~ Минимальный объем за сутки, Kb**	**~ объем за сутки с полным аудитом, Kb**
Рабочая станция Windows	10	50	320	22400
Файловый сервер	20	До 2700	640	86400
Контроллер домена	20	До 800	640	32000
Сетевое оборудование с передачей syslog	5	До 3000	160	96000
Прокси-сервер	100	До 8000	3200	256000

Примечание. Система позволяет гибкое вертикальное и горизонтальное наращивание производительности и позволяет гибко масштабировать компоненты системы без прерывания процесса обработки событий.

2.1.3 Синхронизация времени и NTP

Для корректной работы системы необходимо чтобы сервер и источники работали с точным временем. Разброс в несколько секунд и минут может губительно повлиять на работу аналитических модулей системы. Рекомендуется поднять локальный сервер точного времени в сети и синхронизировать его с периодичностью не менее чем один раз в сутки. Также, рекомендуется настроить синхронизацию источников с локальным NTP сервером. В случае необходимости, в роли NTP сервера может выступить RuSIEM.

Важно! Гипервизоры и системы виртуализации могут привносить существенные отклонения на дату и время на виртуальных машинах.

2.1.4 Список портов и протоколов, используемых серверами системы

Важно! Если вы используете на прокси серверах sslstrip и планируете обновление RuSIEM через подобный сервер – система не будет обновляться! Ни автоматически, ни вручную инженерами.

1. Подготовить ресурсы по ранее согласованным параметрам.
2. Организовать доступ к системе:

Источник	**Назначение**	**Порт**	**Описание**
Рабочие места операторов/аналитиков	Rusiem Web	443 TCP	Доступ к интерфейсу системы
Источники syslog	RuSIEM ls_input	5014, 514 TCP/UDP	Syslog события
Windows рабочие места/сервера	RuSIEM ls_input	3515 TCP	События RuSIEM Agent

	RuSIEM IoC	открытый 443https	Индикатор компроментации IoC агента

3. Обеспечить полный доступ между компонентами SIEM-системы с каналом не менее 1Gbps.

4. Организовать доступ по ssh на сервера для установки компонентов RuSIEM (порт 22 TCP).

5. Организовать прямой доступ от серверов RuSIEM по портам 80, 443 к данным узлам.

Узлы для получения скрипта установки	**Узлы для установки и обновления системы**
files.rusiem.tech	ru.archive.ubuntu.com perseus.rusiem.com apt.postgresql.org archive.ubuntu.com keyserver.ubuntu.com ppa.launchpad.net rstc.rusiem.tech files.rusiem.tech orion.rusiem.com www.postgresql.org sierra.rusiem.com standards-oui.ieee.org pypi.org files.pythonhosted.org

	*.ru.pool.ntp.org

6. Список адресов для Astra

Узлы для получения скрипта установки	**Узлы для установки и обновления системы**
files.rusiem.tech	orion.rusiem.com download.astralinux.ru

2.1.5 Список портов и протоколов, используемых для получения событий

Протокол	**Порт**	**Направление**	**Описание**
Tcp	3515	Агент → Управляющий сервер	Передача событий с модулей RuSIEM агента
Tcp/udp	5014/514	Источники событий → Коллектор	Tcp/udp syslog
tcp	443	Агент → Удаленный windows event log	Удаленный сбор событий без установки агента с MS Windows OS
tcp	445	Агент → Удаленный windows event log	Удаленный сбор событий без установки агента с MS Windows OS
Oracle	1521	Агент → Удаленный сервер Oracle DB	Коннектор для сбора событий с БД Oracle
Ftp	21	Агент → Удаленный FTP сервер	Коннектор для сбора событий в виде текстовых файлов с ftp, sftp, ftps серверов
TCP/UDP	1433	Агент → Удаленный сервер MS SQL	Коннектор для сбора событий с MS SQL
TCP/UDP	3306	Агент → Удаленный сервер MySql	Коннектор для сбора событий с MySQL
TCP/UDP	5432	Агент → Удаленный сервер PostgreSQL DB	Коннектор для сбора событий с PostgreSQL

Протокол	Порт	Направление	Описание
TCP/UDP	135	Агент → Удаленной Windows EventLog	Удаленный сбор событий журналов WMI посредством DCOM соединения
TCP/UDP	9999	Источники событий → Коллектор	Tcp/udp Netflow v5/v9

2.2 Подготовка к установке

Система может быть установлена:

На виртуальном сервере VmWare esxi или Microsoft Hyper-V

В процессе установки шаблона следует ответить на ряд вопросов о размещении виртуальной машины и параметрах. При выборе формата диска стоит выбрать «Thin provision» с целью экономии дискового пространства хранилища esxi.

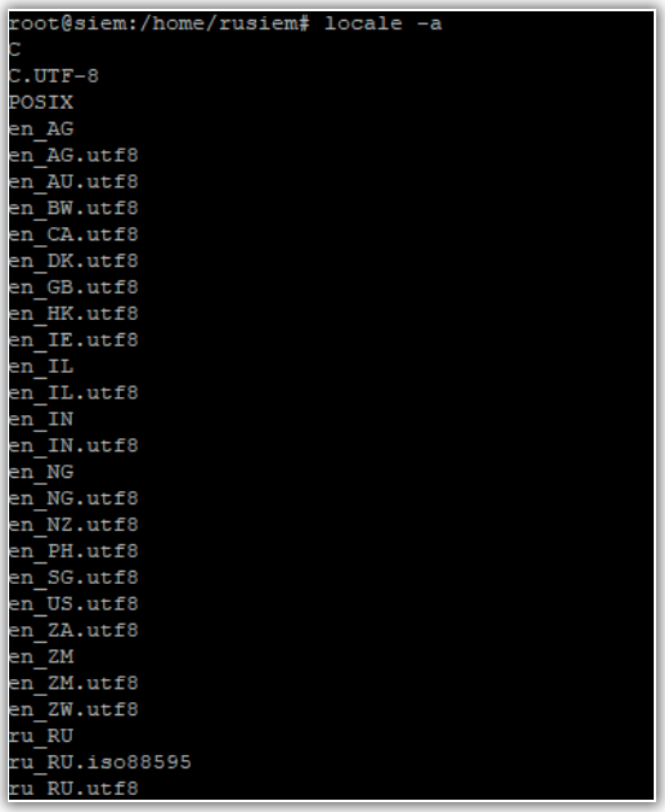
Перед запуском виртуальной машины следует убедиться, что выделенные ресурсы соответствуют аппаратным требованиям, рекомендуемым для планируемой нагрузки (EPS).

На физическом сервере

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**) или Ubuntu Server 22.04 LTS (Jammy Jellyfish) x64 - https://releases.ubuntu.com/22.04 (и там актуальный Server Install image for 64-bit PC, например **ubuntu-22.04.2-live-server-amd64.iso**), а также настроить доступ сервера к сети Интернет.

Перед установкой системы рекомендуется проверить наличие русской локализации командой:

locale -a



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

Получение UUID

Для бесплатной версии (RvSIEM) получение лицензии не требуется!

После установки ОС для открытия доступа к репозиториям RuSIEM необходимо сообщить system UUID.

Команда получения UUID сервера

Данную команду необходимо выполнять под root доступом, или через sudo.

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

К UUID будет также привязан ключ лицензии.

UUID может смениться при смене оборудования, в том числе при миграции виртуальной машины на другой сервер.

После получения подтверждения, что доступ к репозиториям открыт, можно запускать установочный скрипт.

2.3 Установка RuSIEM на Ubuntu

2.3.1 Установка RuSIEM на Ubuntu 18.04

Все действия производятся с правами root.

Необходимо получить архив rusiem.rfrit.tgz с deb-пакетами и скриптом 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 xvf rusiem.rfrit.tgz

Запуск скрипта установки

bash ./install.sh

```
Check OS (Ubuntu: bionic 18.04 required)
OS PASSED: OK
PASSED: running as bash ./install.sh
This utility will help you to install RuSIEM commercial version, RvSIEM free version or RuSIEM Analytics (also will be installed commercial version RuSIEM)
More information you can find on the website:
https://rusiem.com/en (English version)
https://rusiem.com/ru (Russian version)
 ATTENTION!
 RuSIEM commercial version REQUIRES A LICENSE and previously accepted access to a private repository BEFORE install!
 RvSIEM free does not require any licenses and access, is distributed freely

At any time you can switch between versions.
For example, set RvSIEM free first. And then - for a commercial version of RuSIEM. And back.
Approximate installation time: ~20-30 min
Will be downloaded: ~200-400 Mb
Proxy don't used (detected by /etc/environment)
Press 1 for install RuSIEM commercial version (kernel + database) (Subscription access required!)
Press 2 for install RuSIEM and RuSIEM analytics (kernel + database + analytics) (Subscription access required!)


For all installations of RuSIEM/RvSIEM with a database on a single server - after installation, you can transfer the database to a separate server.
Select the version to install:2
Your choice - RuSIEM Analytics version
Before starting the installation - write a corporate letter to support@rusiem.com with a request to provide access to the commercial version.
Specify the following Server ID: C0DF6D63-817A-4470-A813-AF2C2B0FA25B
Before continuing the installation, you must wait for a response that you have been granted access and issued a license for this Server ID!

If you received a response from support@rusiem.com, press Y to continue or N to cancel the installation.:Y
```

Скрипт предложит несколько вариантов установки:

- Коммерческая версия RuSIEM;

- Коммерческая версия RuSIEM с модулем аналитики RuSIEM Analytics;

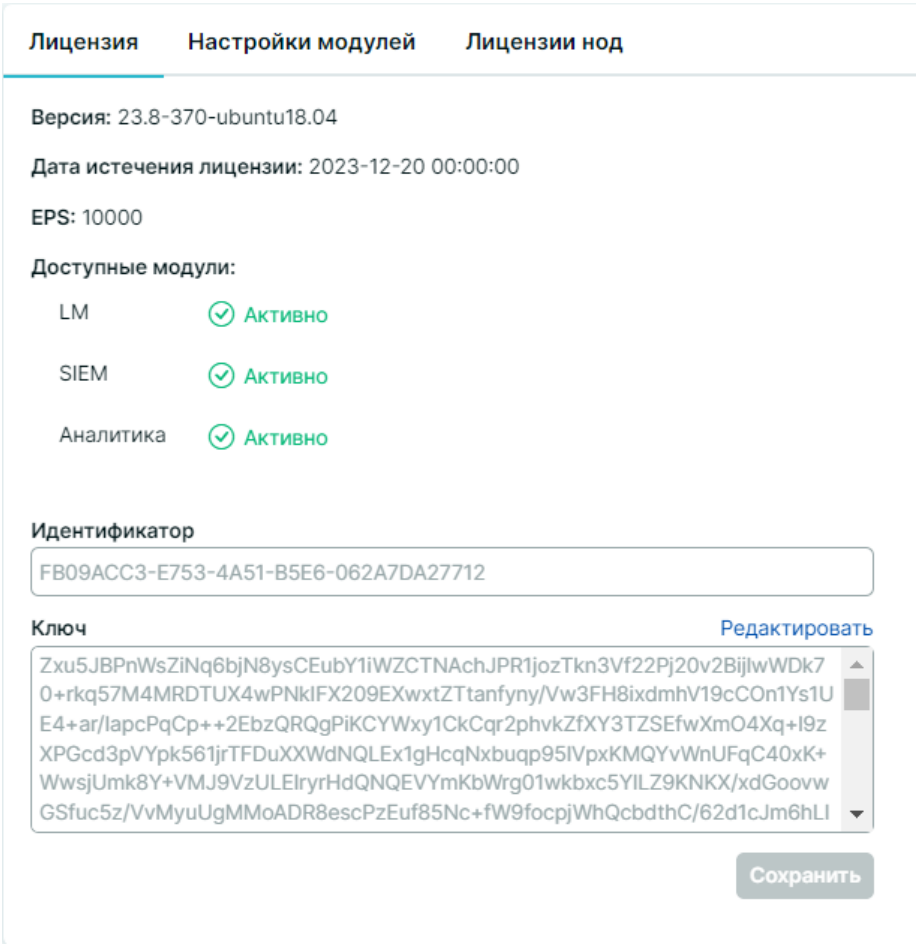
Выбирайте коммерческую версию или коммерческую версию с аналитикой в зависимости от имеющейся лицензии.

Активация системы

После установки зайдите на веб-консоль (https://<IP RuSIEM>):

- Имя пользователя по умолчанию: admin;
- Пароль по умолчанию: admin.

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



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

- Язык по умолчанию: любой;
- 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;

- URL сервера: https://адрес_сервера (вспомогательный параметр, используется при формировании ссылок на инциденты в email-уведомлениях);
- Наименование организации: любое.

Дополнительные настройки:

- Host для подключения Elasticsearch: 127.0.0.1:9200;
- 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;

После установки и активации лицензии

Установите оптимальный (равный половине ОЗУ) размер памяти для Elasticsearch (в примере параметры для 16 Гб ОЗУ), но не более 32 GB.

Выделите не менее 1 Гб ОЗУ под данные операционной системы.

Настройка сервиса elasticsearch.

1. nano /etc/elasticsearch/jvm.options

   Раскомментировать и изменить:

   (Рекомендованное значение 1/3 ОЗУ если устанавливается аналитика и 1/2 если не устанавливалась)

   -Xms10g

   -Xmx10g

2. nano /etc/default/elasticsearch

   Раскомментировать:

MAX_LOCKED_MEMORY=unlimited

3. nano /etc/security/limits.conf

Добавить перед строкой # End of file:

elasticsearch soft memlock unlimited

elasticsearch hard memlock unlimited

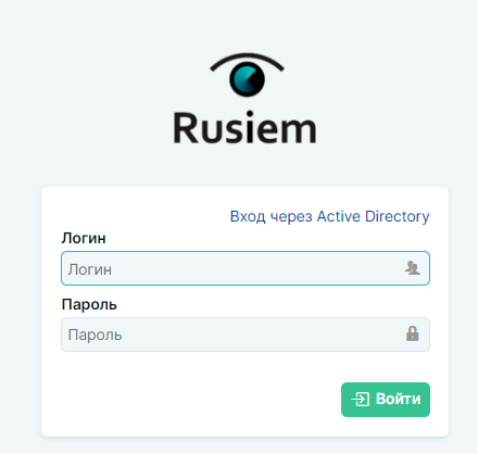
4. nano /usr/lib/systemd/system/elasticsearch.service

Вставить в блок [Service]

LimitMEMLOCK=infinity

После всех настроек systemctl daemon-reload и systemctl restart elasticsearch

Откройте браузер и перейдите по адресу: https://IP-адрес_VM1 должна отобразиться страница входа в систему:



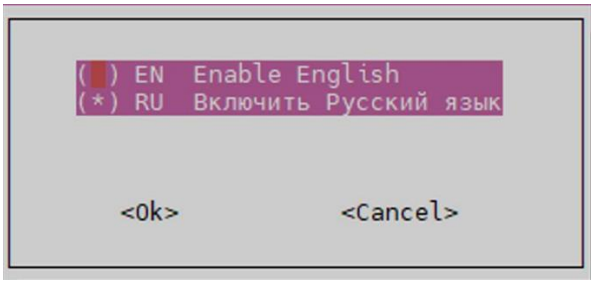
2.3.2 Установка RuSIEM на Ubuntu 22.04

Все действия производятся с правами root.

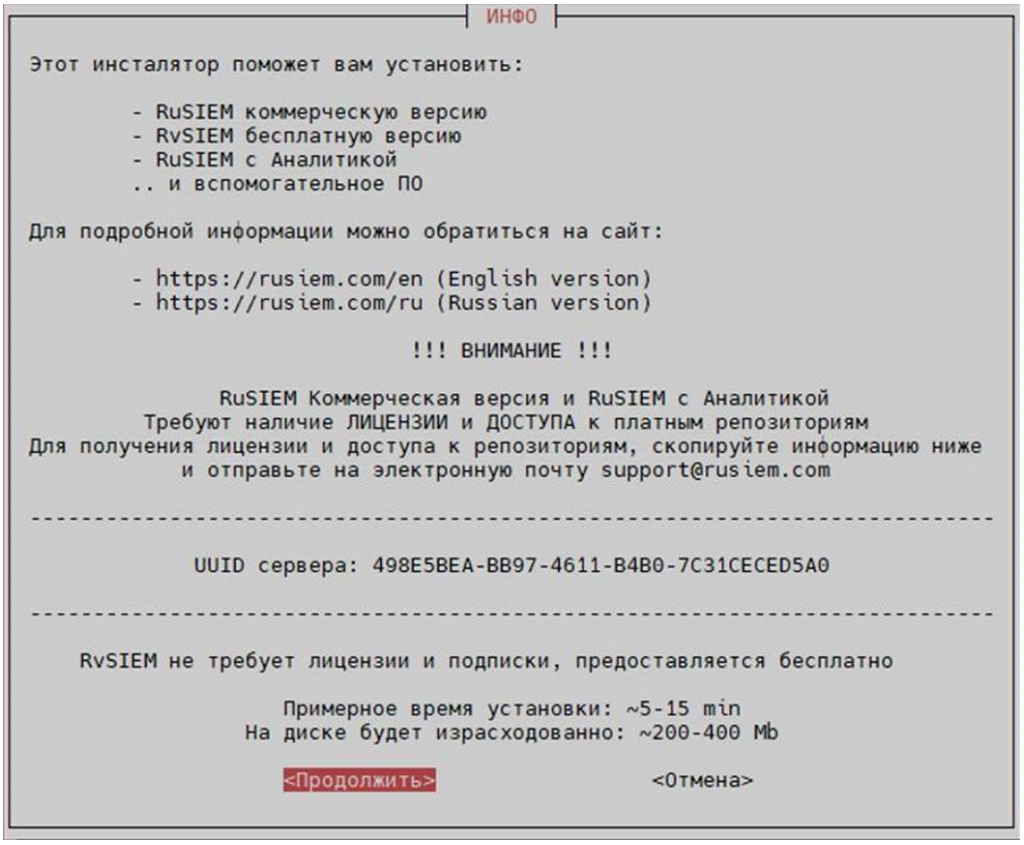
Запуск скрипта установки:

wget https://files.rusiem.tech/nextcloud/s/mgAtFZJwdRj9rax/download -O install.sh; bash ./install.sh

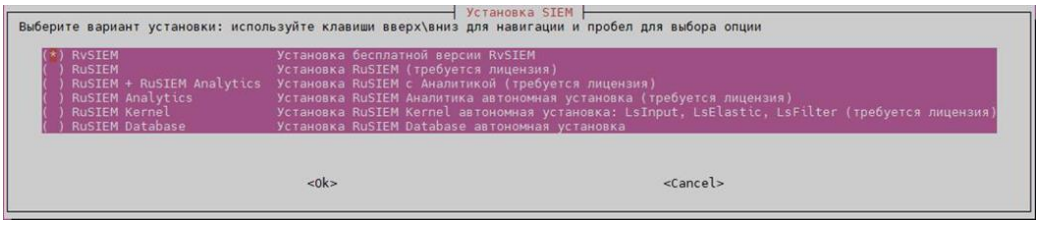
1.Выбрать необходимый язык



2. Внимательно прочитать и нажать <Продолжить>



3. Выбрать пункт соответствующий вашей лицензии

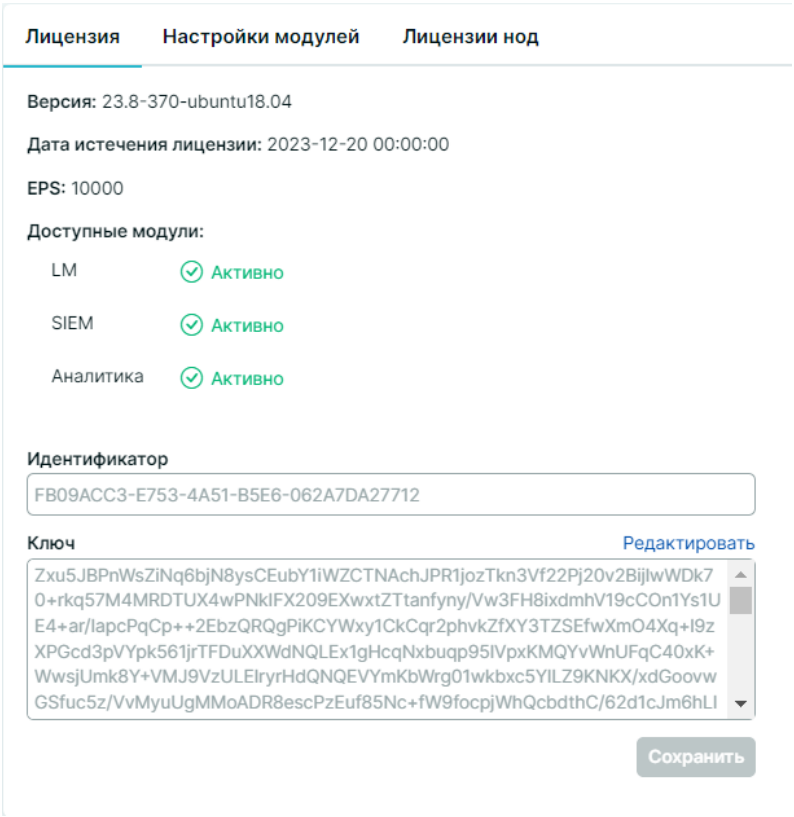


Активация системы

После установки зайдите на веб-консоль (https://<IP RuSIEM>):

- Имя пользователя по умолчанию: admin;
- Пароль по умолчанию: admin.

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



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

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

Дополнительные настройки:

- Host для подключения Elasticsearch: 127.0.0.1:9200;
- Версия Elasticsearch: проверить установленную версию в системе (dpkg -l | grep elasticsearch) и выбрать соответствующий вариант (По умолчанию: 7.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;

После установки и активации лицензии

Установите оптимальный (равный половине ОЗУ) размер памяти для Elasticsearch (в примере параметры для 16 Гб ОЗУ), но не более 32 GB.

Выделите не менее 1 Гб ОЗУ под данные операционной системы.

Настройка сервиса elasticsearch.

1. nano /etc/elasticsearch/jvm.options

   Раскомментировать и изменить:

   (Рекомендованное значение 1/3 ОЗУ если устанавливается аналитика и 1/2 если не устанавливалась)

   -Xms10g

   -Xmx10g

2. nano /etc/default/elasticsearch

   Раскомментировать:

   MAX_LOCKED_MEMORY=unlimited

3. nano /etc/security/limits.conf

   Добавить перед строкой # End of file:

   elasticsearch soft memlock unlimited

   elasticsearch hard memlock unlimited

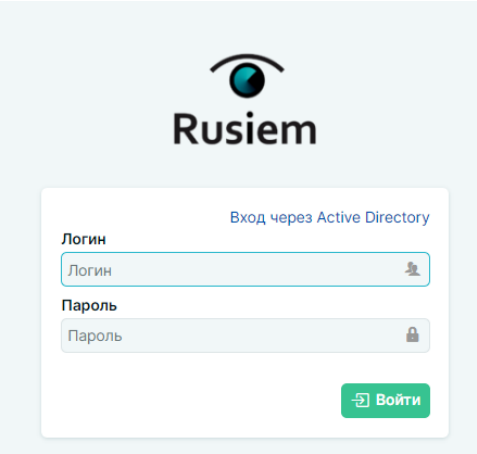
4. nano /usr/lib/systemd/system/elasticsearch.service

   Вставить в блок [Service]

   LimitMEMLOCK=infinity

   После всех настроек systemctl daemon-reload и systemctl restart elasticsearch

   Откройте браузер и перейдите по адресу: https://IP-адрес_VM1 должна отобразиться страница входа в систему:



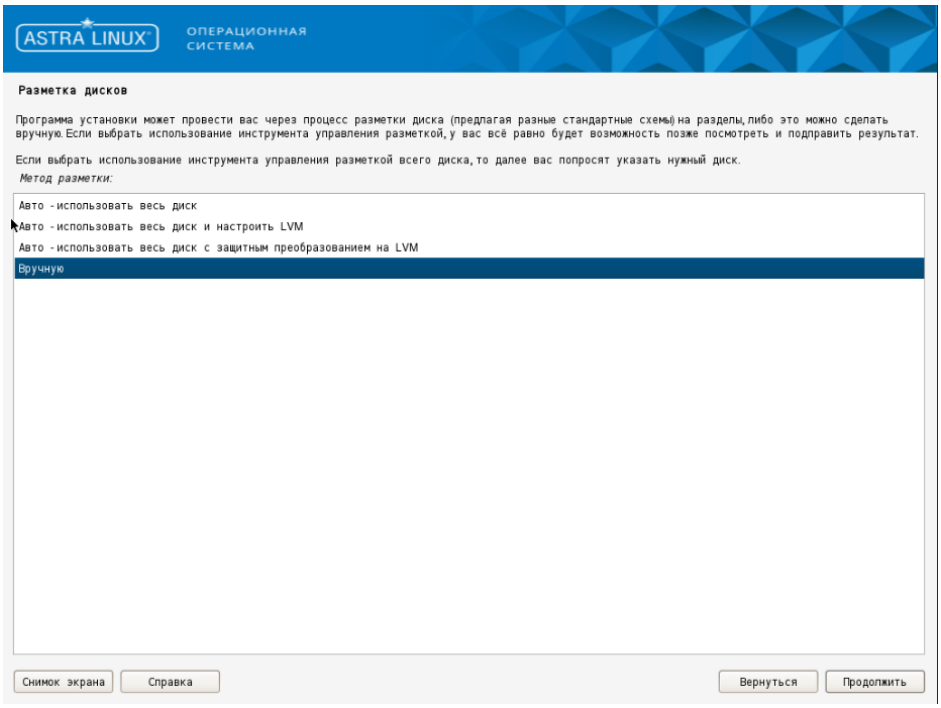
2.4 Установка RuSIEM на Astra

2.4.1 Создание LVM раздела

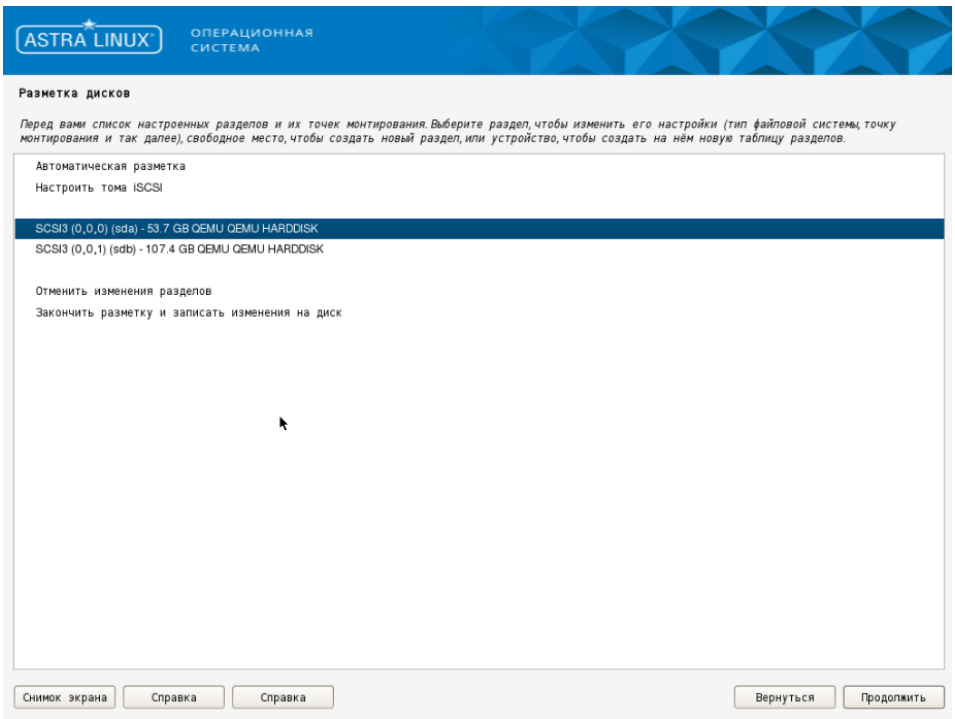
Рекомендуемая версия для установки: Astra Linux Special Edition РУСБ.10015-01 (версия не ниже обновления 1.7).

Создание LVM раздела

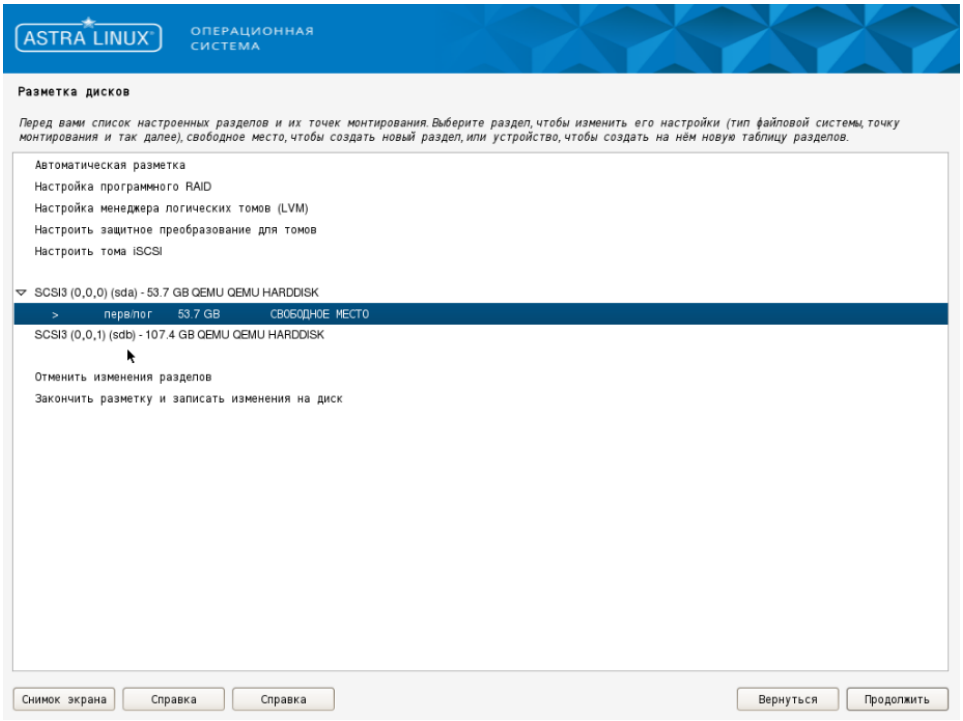
- Выбираем ручную разметку.



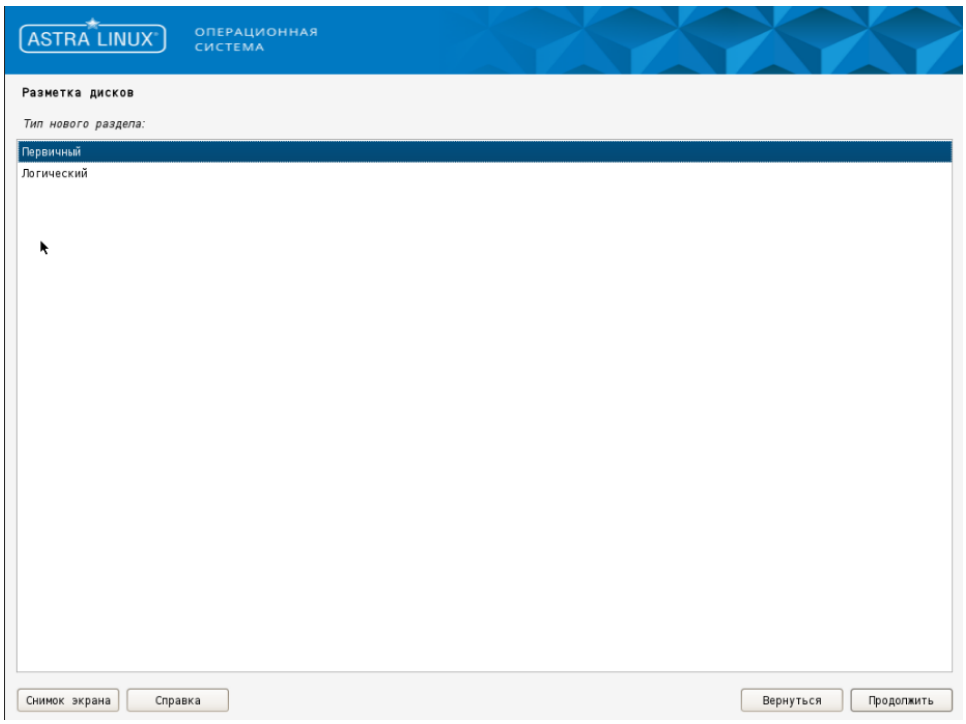
- Выбираем жёсткий диск и нажимаем "Продолжить".



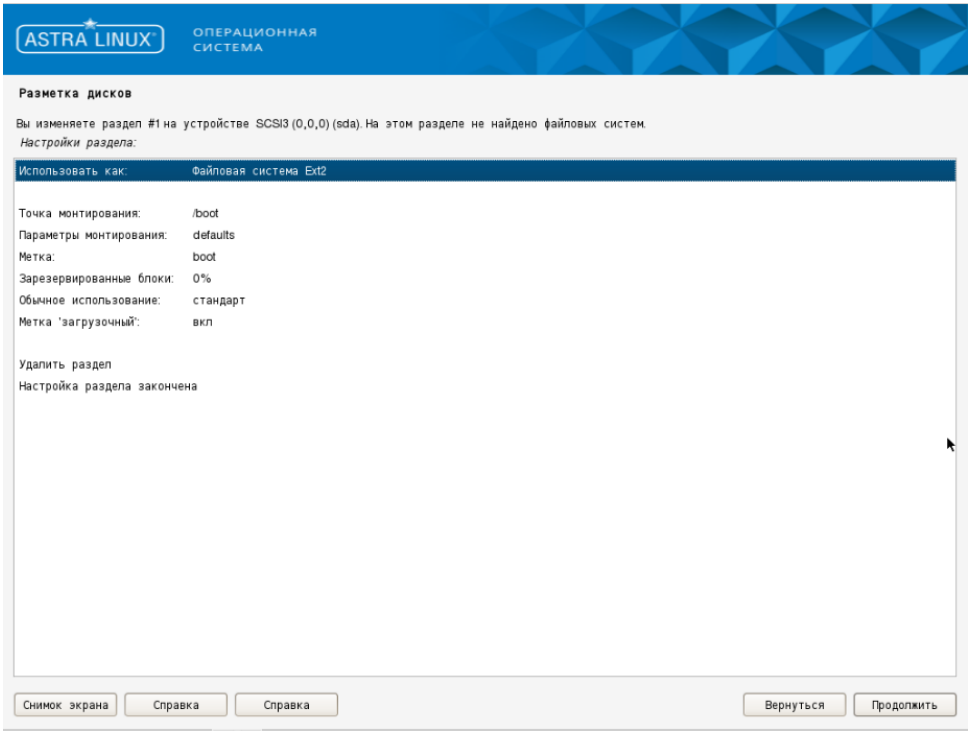
- Создаём новую таблицу разделов, выбрав "Да" и нажав "Продолжить".
- Выбираем СВОБОДНОЕ МЕСТО и нажимаем "Продолжить".



- Создаем новый раздел размером 500МБ.

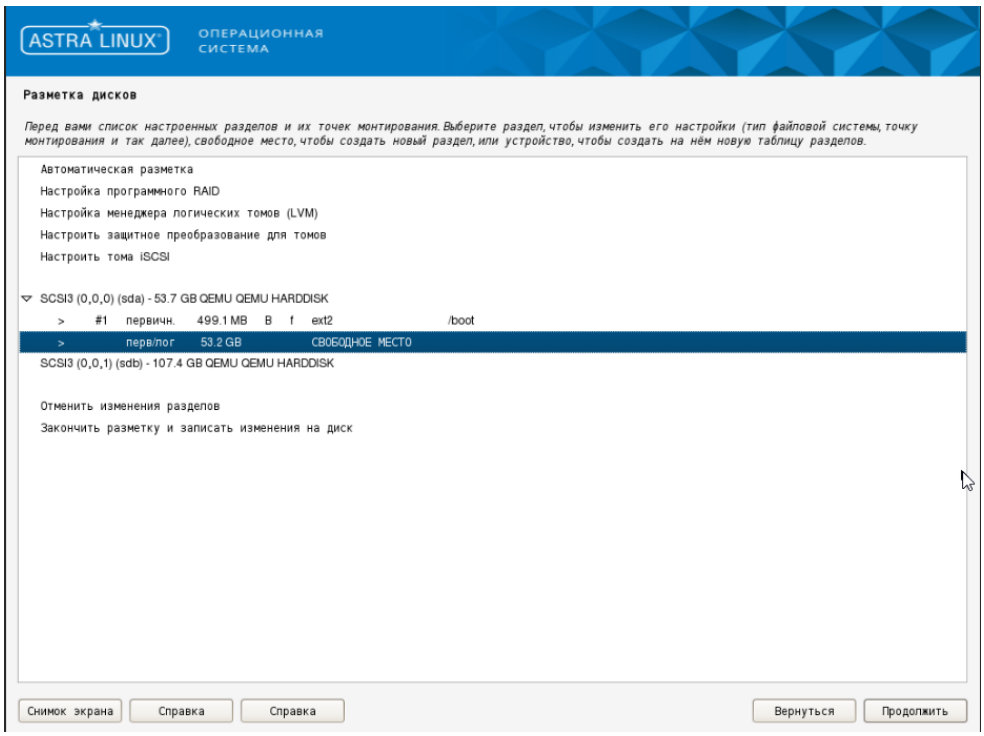


- Выбираем "Первичный" и размещаем новый раздел в начале свободного места. После этого делаем аналогичные настройки для boot раздела.

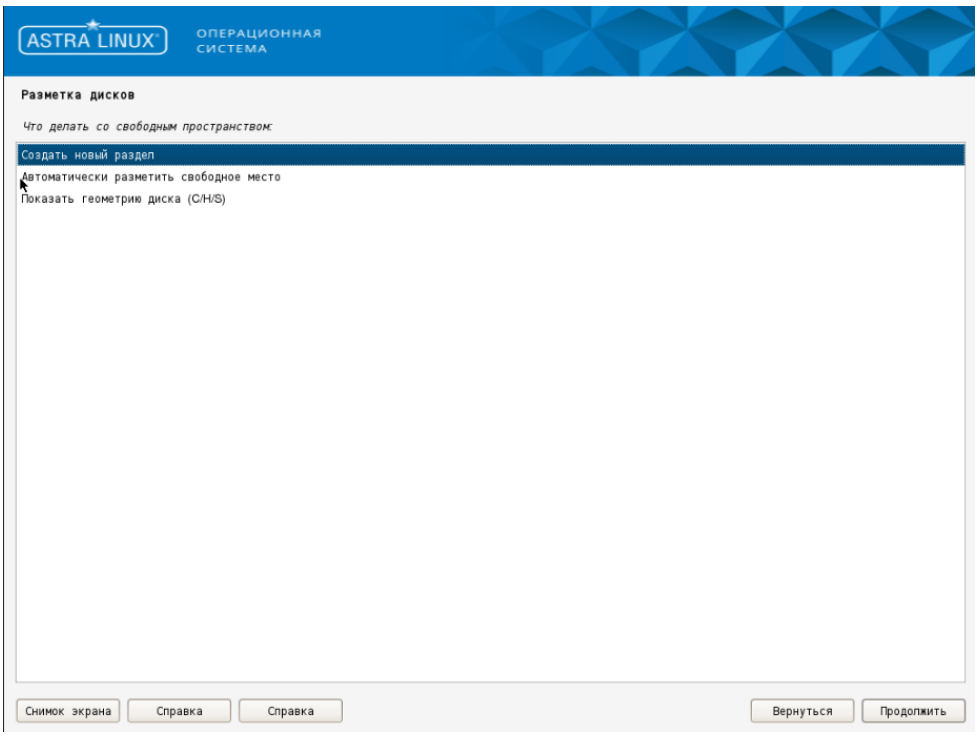


- Выбираем "Настройка раздела закончена" и нажимаем "Продолжить".

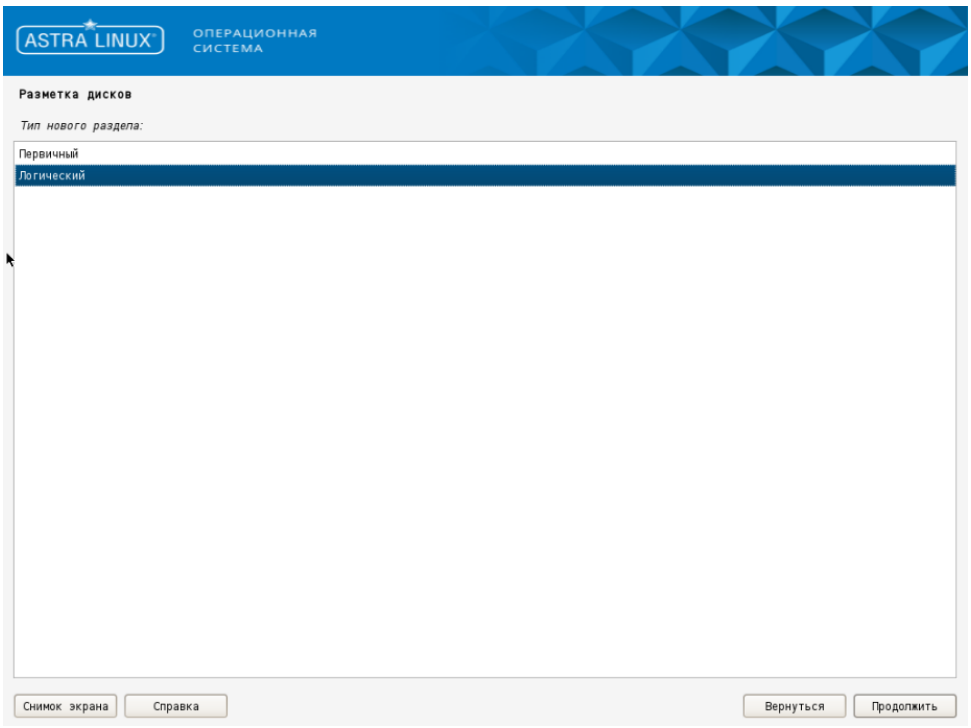
- Разметка загрузочного раздела закончена. Далее создаём раздел LVM. Для этого выбираем СВОБОДНОЕ МЕСТО и нажимаем кнопку "Продолжить".



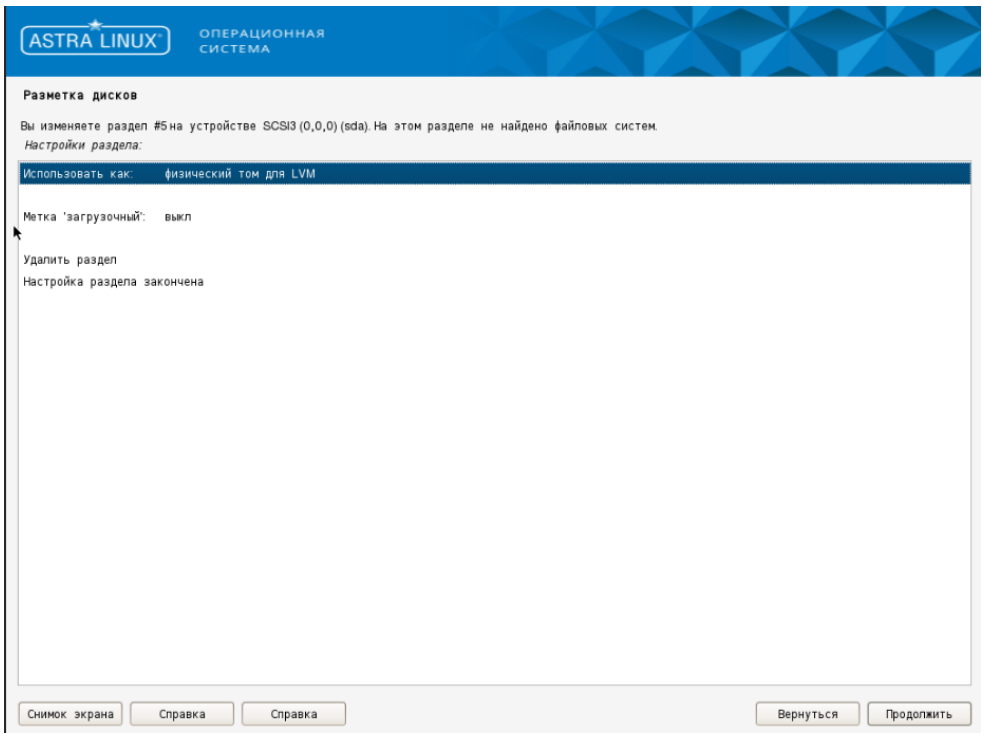
- Выбираем "Создать новый раздел".



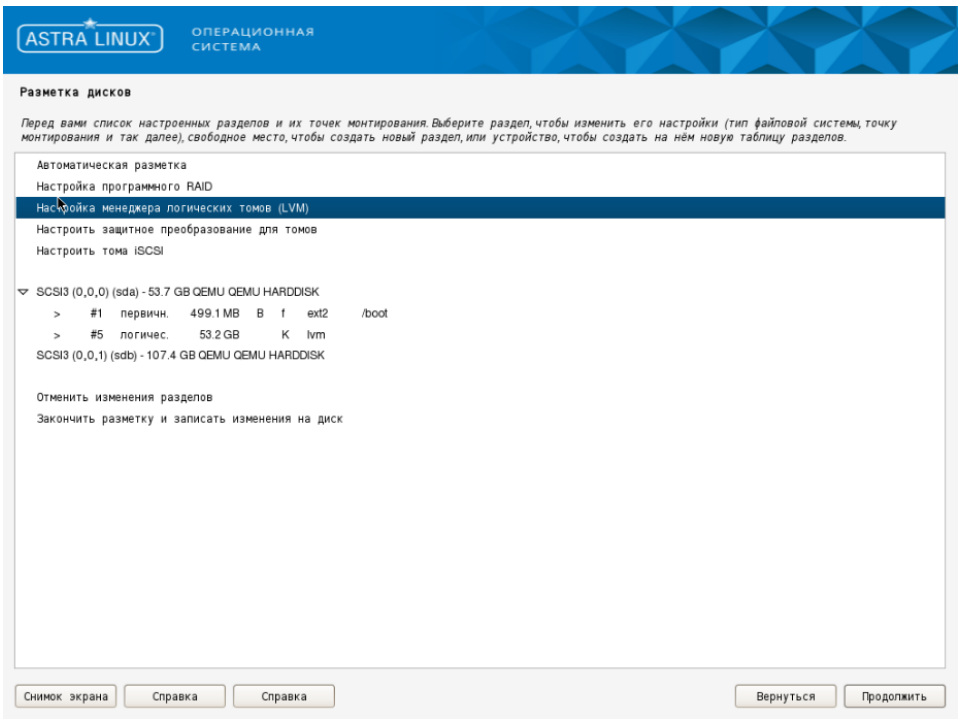
- Выделяем необходимое место под корневой раздел, а далее выбираем "Логический".



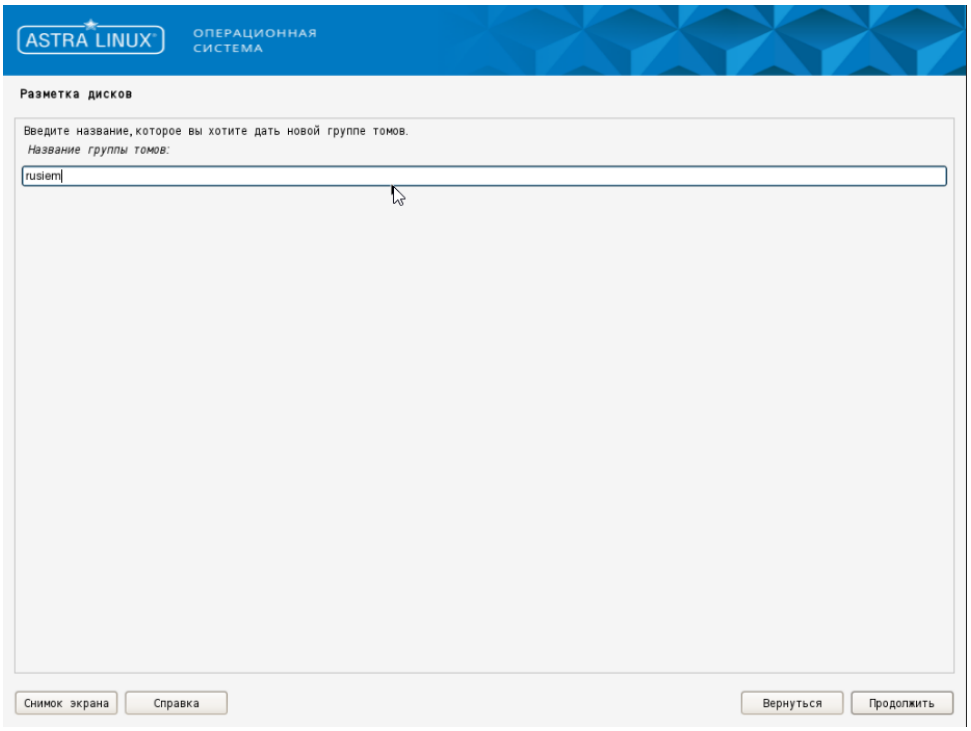
- Выбираем “Физический том для LVM”.



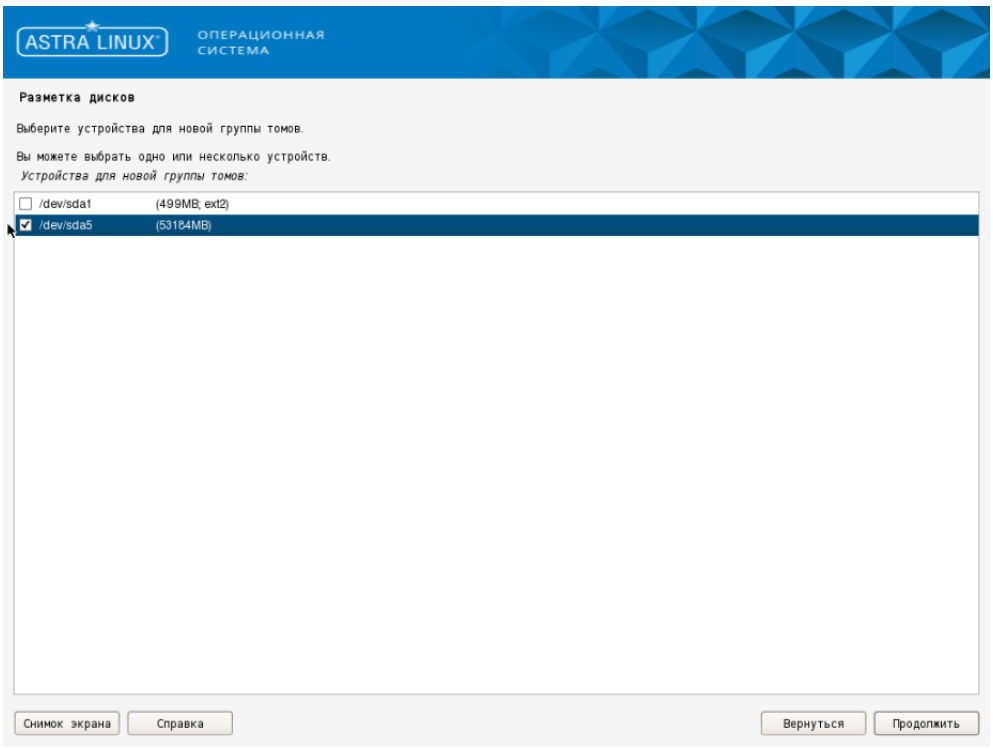
- Выбираем "Настройка раздела закончена".
- Выбираем "Настройка менеджера логических томов (LVM)".



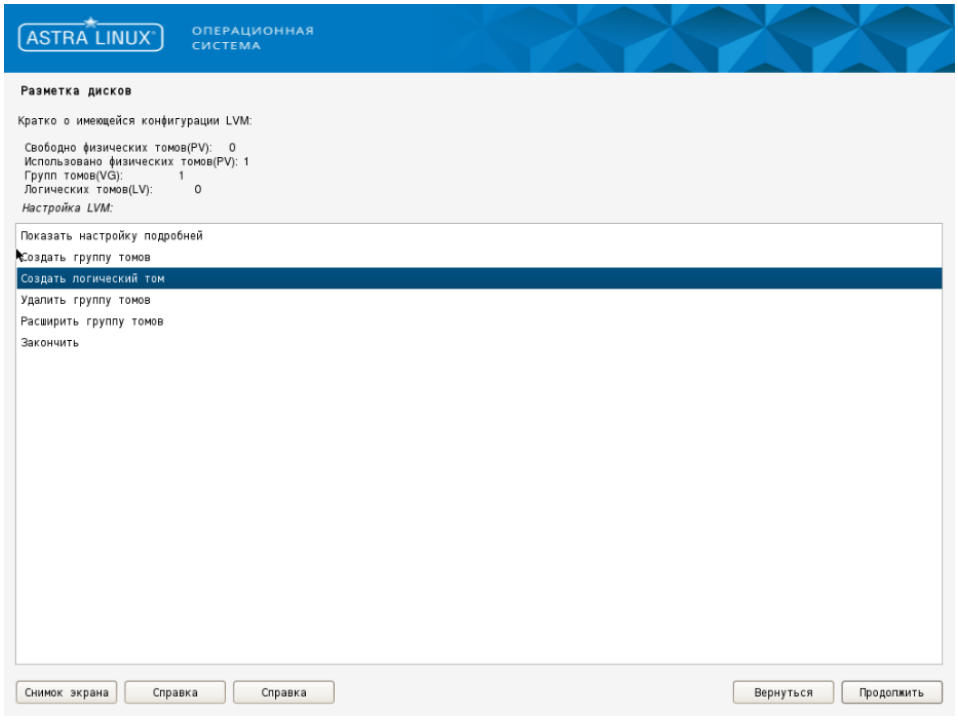
- Далее выбираем "Создать группу томов".
- Назовём группу томов любым именем.



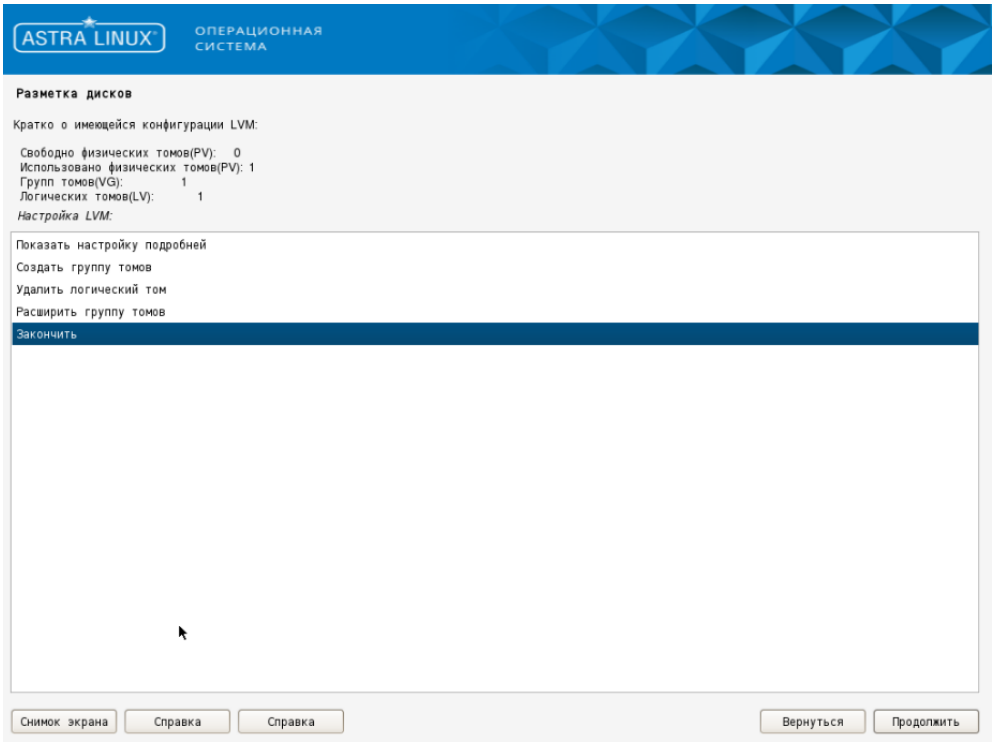
- Выбираем место для корневого раздела.



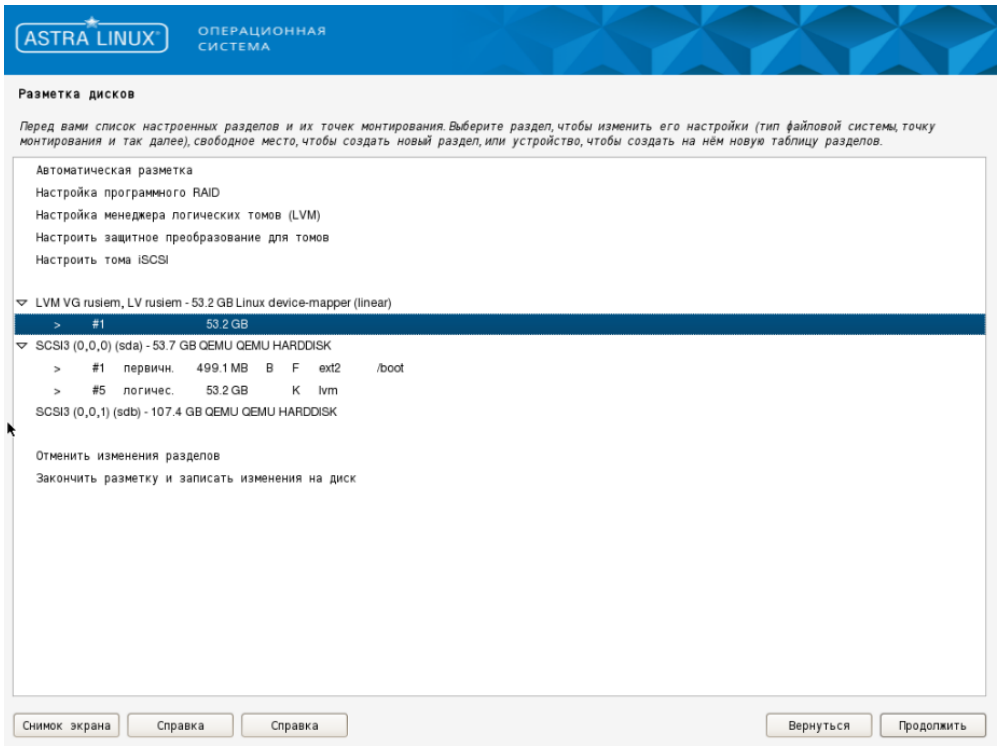
- Далее начнём создавать логические тома. Выбираем "Создать логический том".



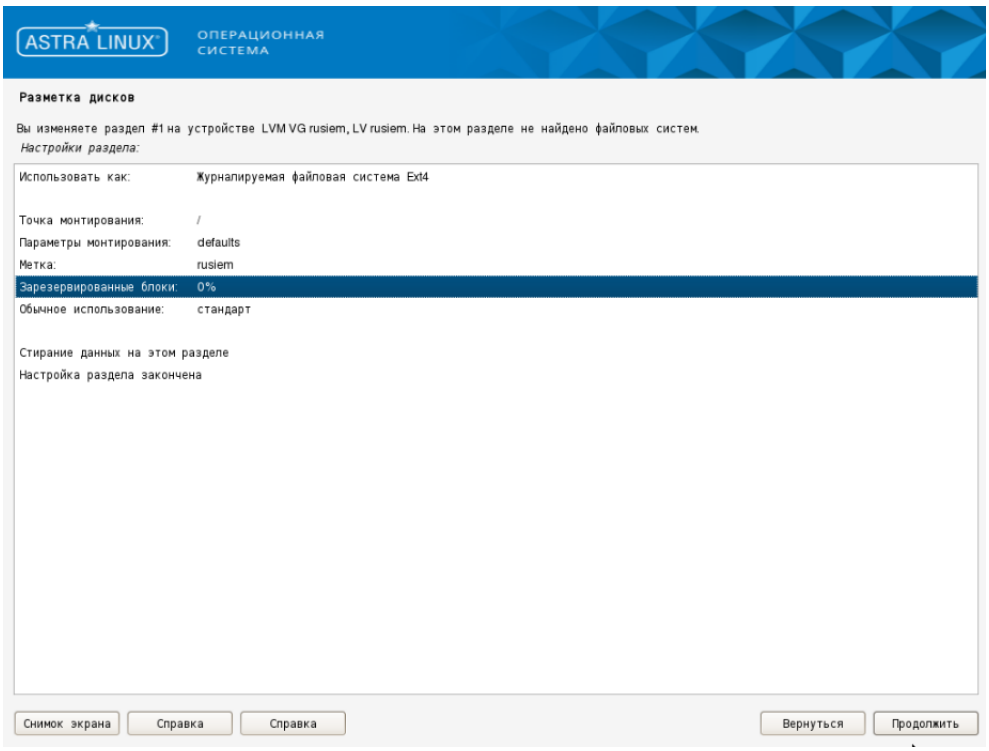
- Создаем логический том, даем ему любое название, выделяем необходимое количество места.



- Заканчиваем разметку логических томов, выбрав "Закончить" и нажав "Продолжить".
- Теперь необходимо разметить наши логические тома. Для этого выбираем логический том "rusiem" и нажимаем "Продолжить".



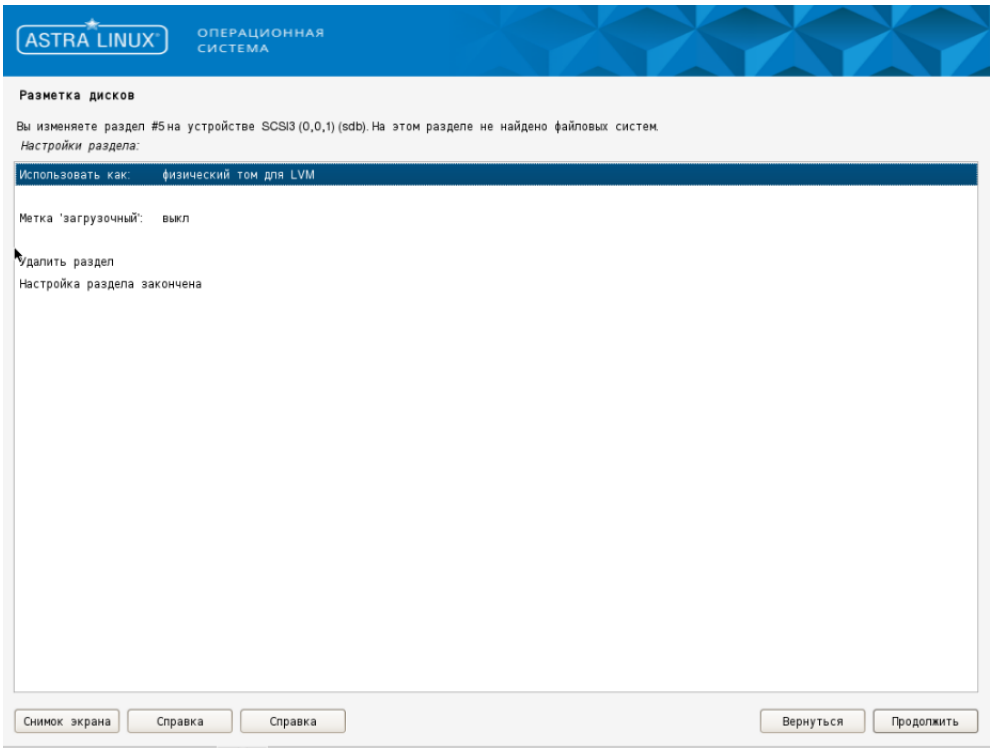
- Выбираем "Использовать как:".
- И делаем аналогичные настройки.



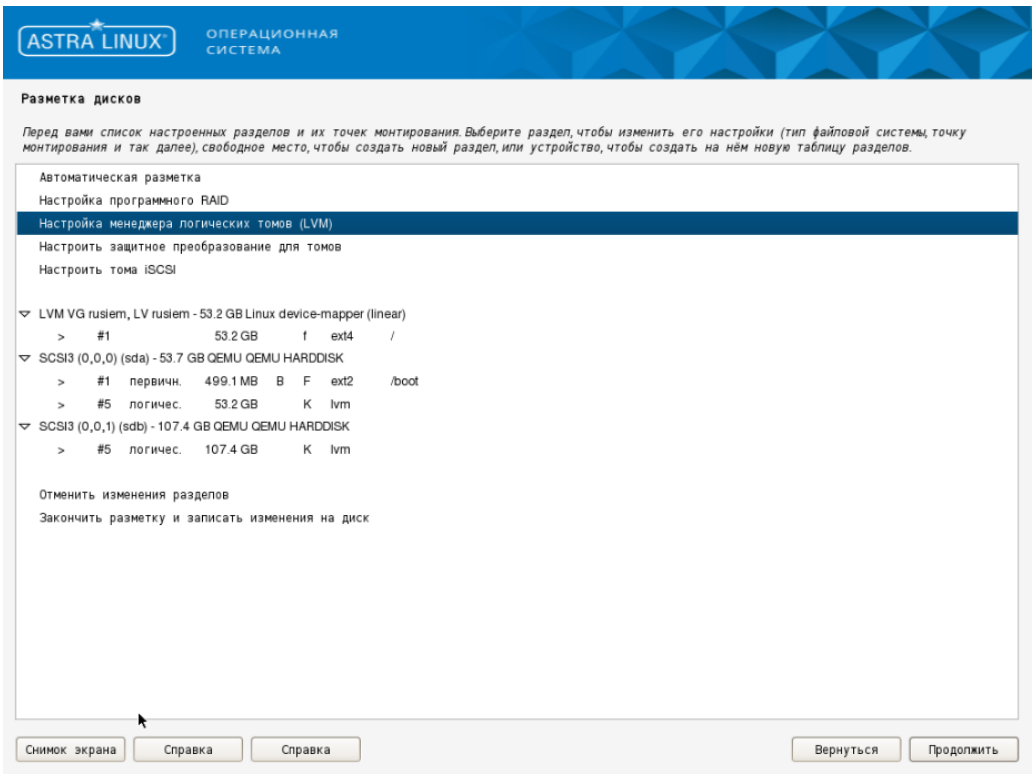
- Выбираем "Настройка раздела закончена".

Создание /data раздела

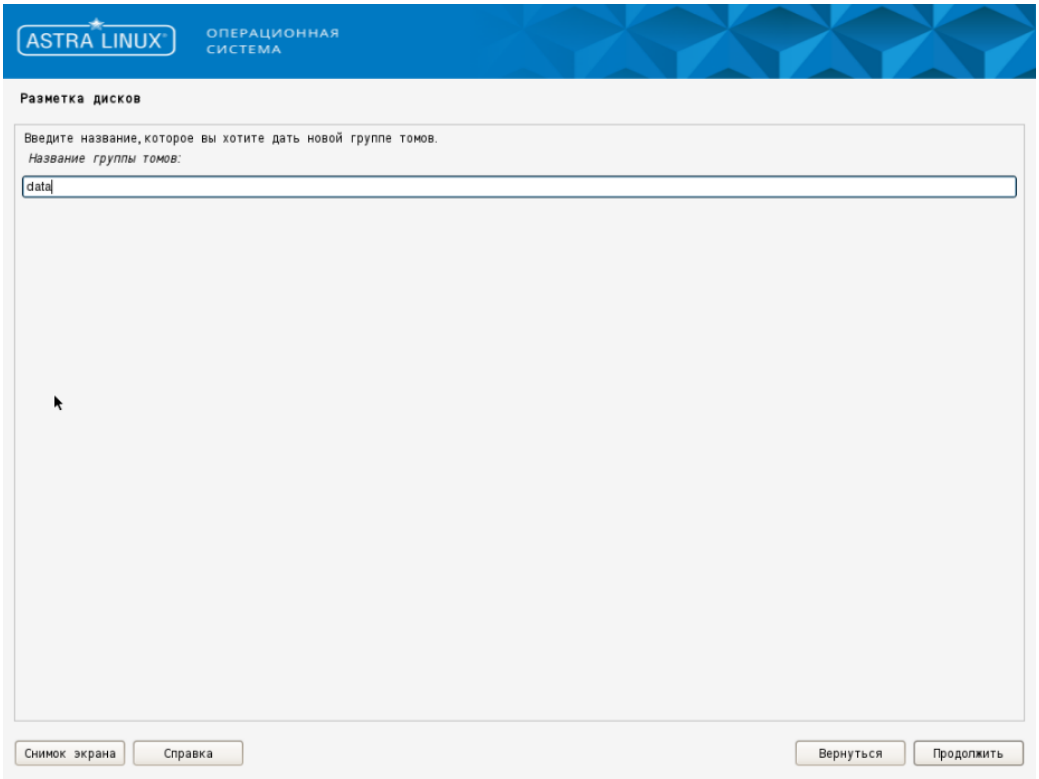
- Создаем физический том LVM.



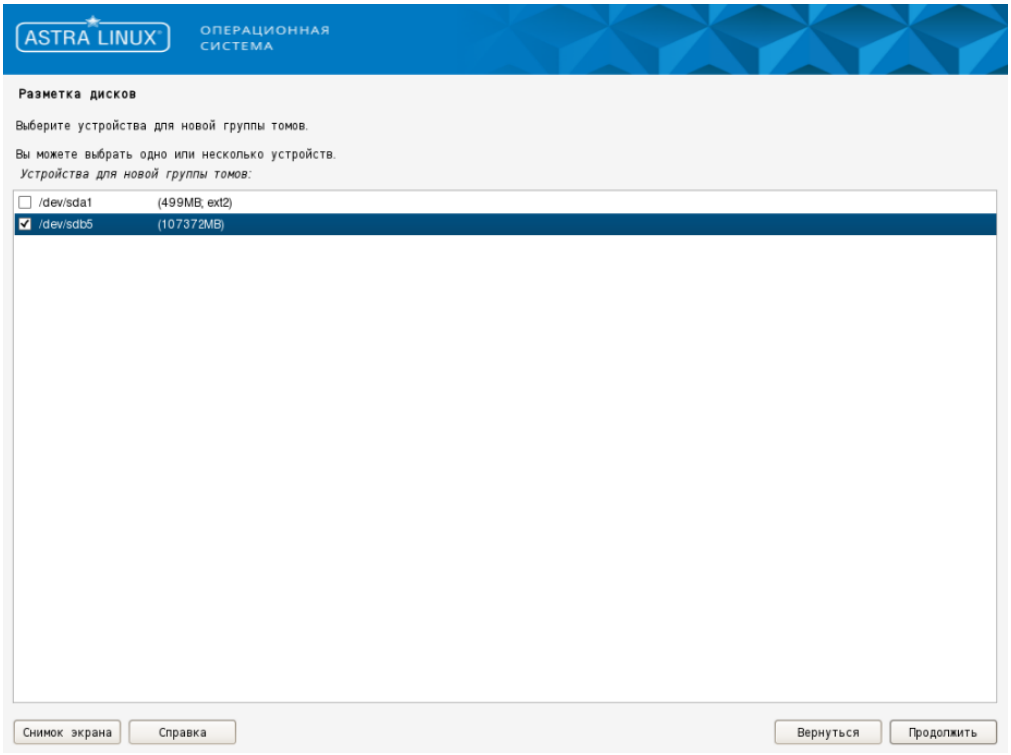
- Выбираем "Настройка менеджера логических томов (LVM)".



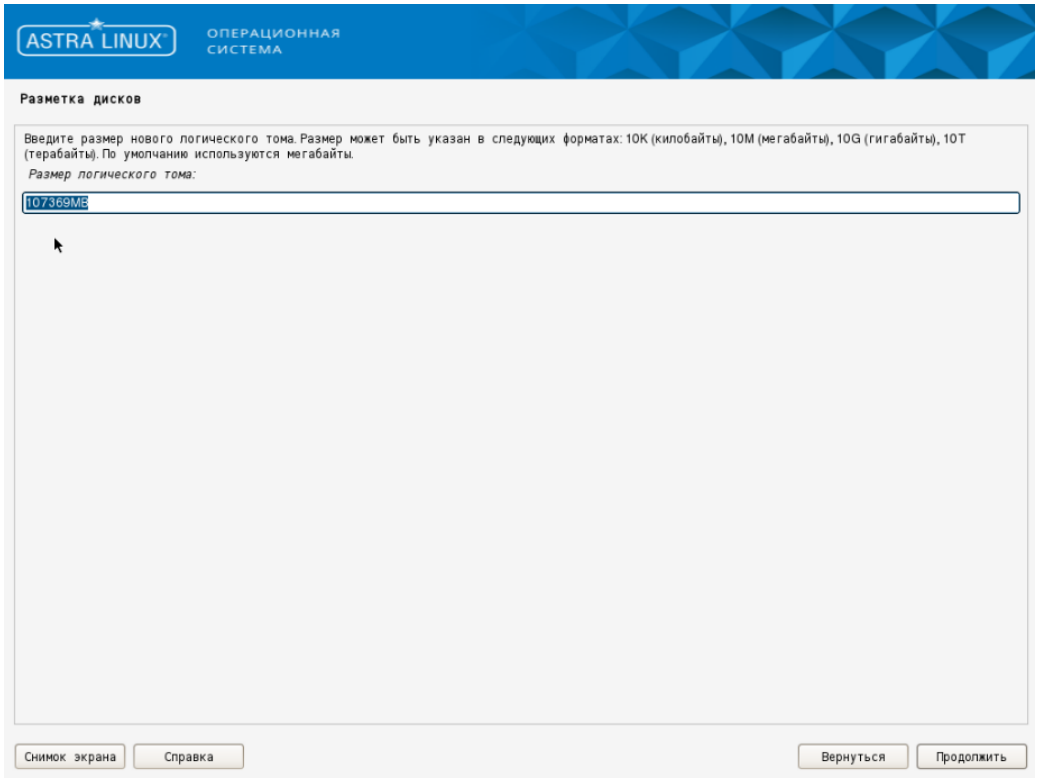
- Выбираем “Создать группу томов” и вписываем название data.



- Выделяем необходимое устройство.

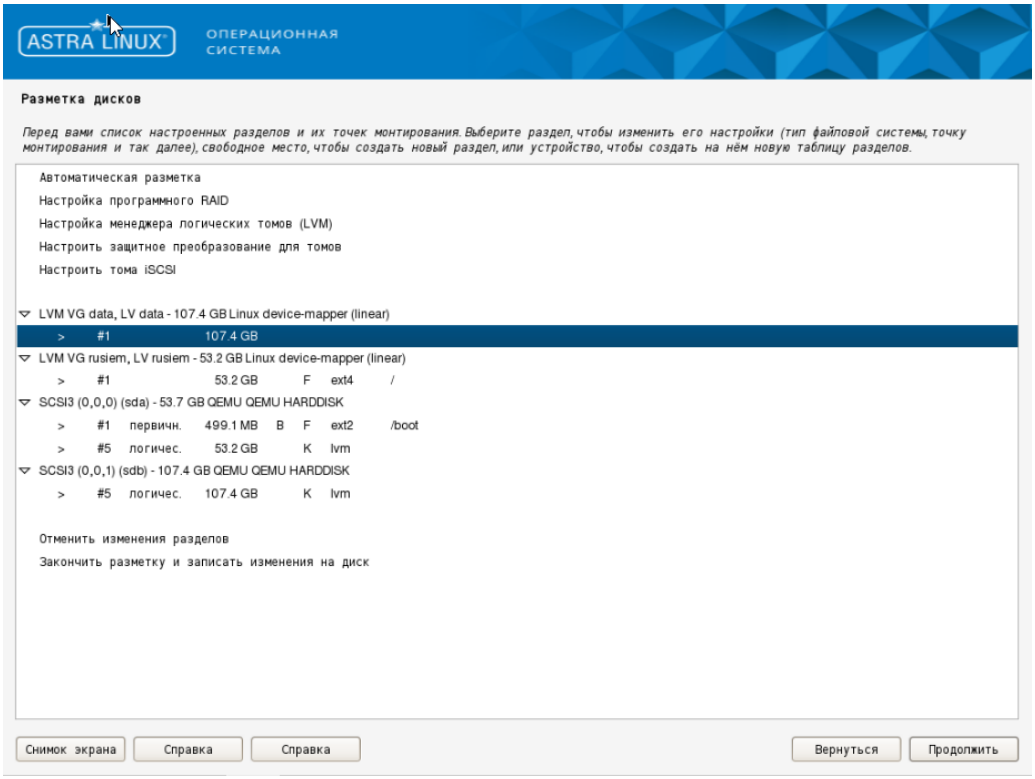


- Выбираем "Создать логический том". Используем только что созданный том, даем ему название data и выделяем необходимое количество памяти.

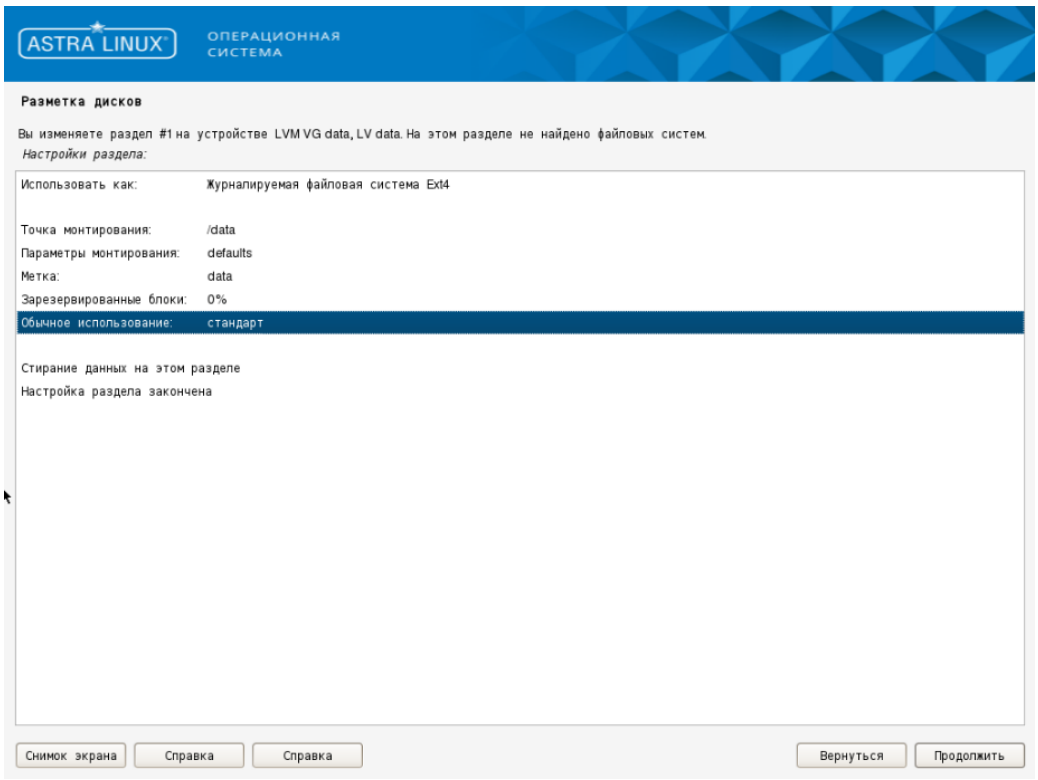


- Заканчиваем разметку логических томов, выбрав "Закончить" и нажав "Продолжить".

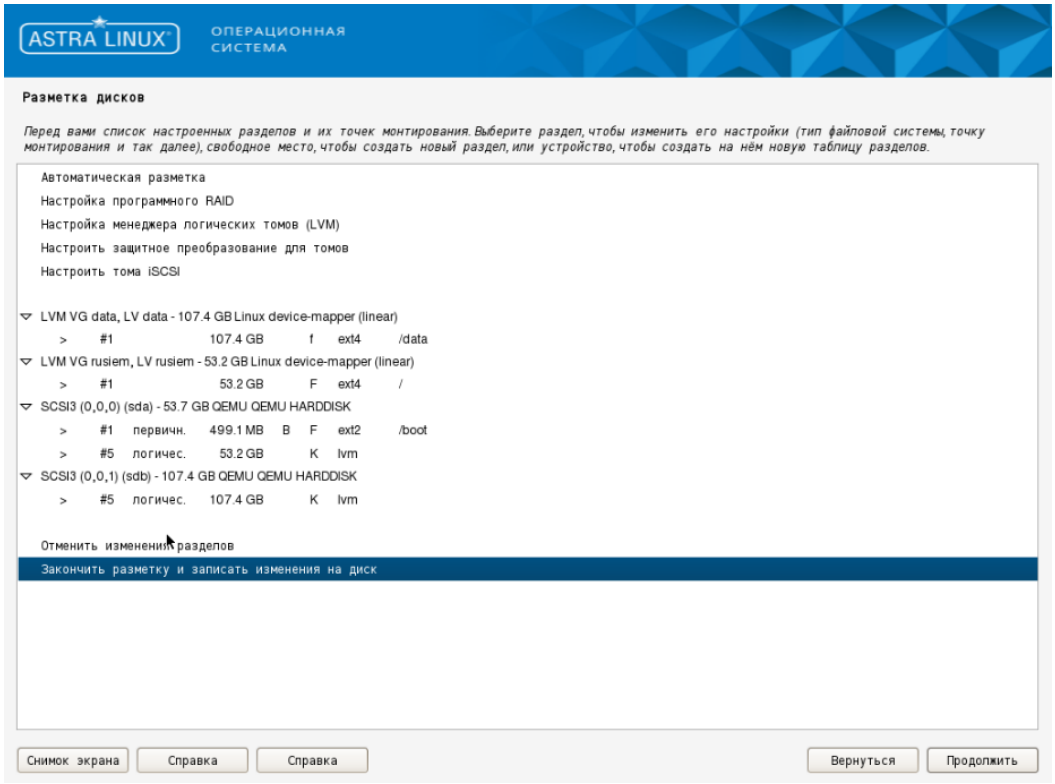
- Теперь необходимо разметить наши логические тома. Для этого выбираем логический том "data".



- Выполняем аналогичные настройки и выбираем "Настройка раздела закончена".



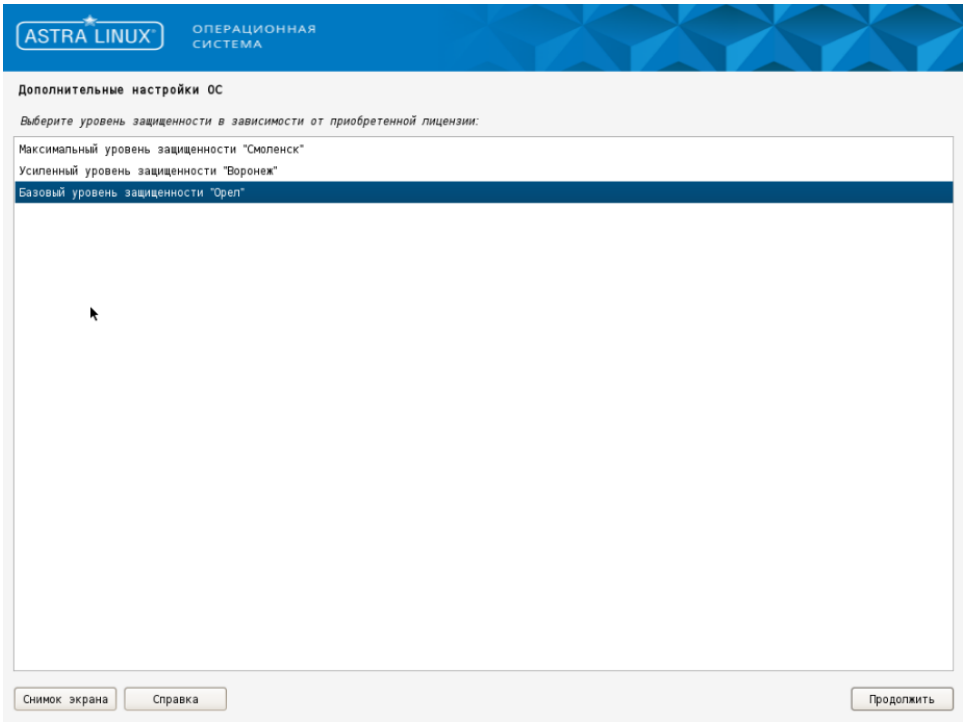
- Разметка закончена. Выбираем "Закончить разметку и записать изменения на диск" и нажимаем "Продолжить".



2.4.2 Установка Astra

Рекомендуемая версия для установки: Astra Linux Special Edition РУСБ.10015-01 (версия не ниже обновления 1.7).

- При установке рекомендуется выполнять установку Astra linux в качестве серверного решения. Не стоит устанавливать офисные, мультимедийные и прочие приложения.
- При установке системы нужно выбрать уровень защиты 0 (Базовый уровень защиты “Орел”) или же после установки: /etc/parsec/mswitch.conf, параметр zero_if_notfound установить в yes



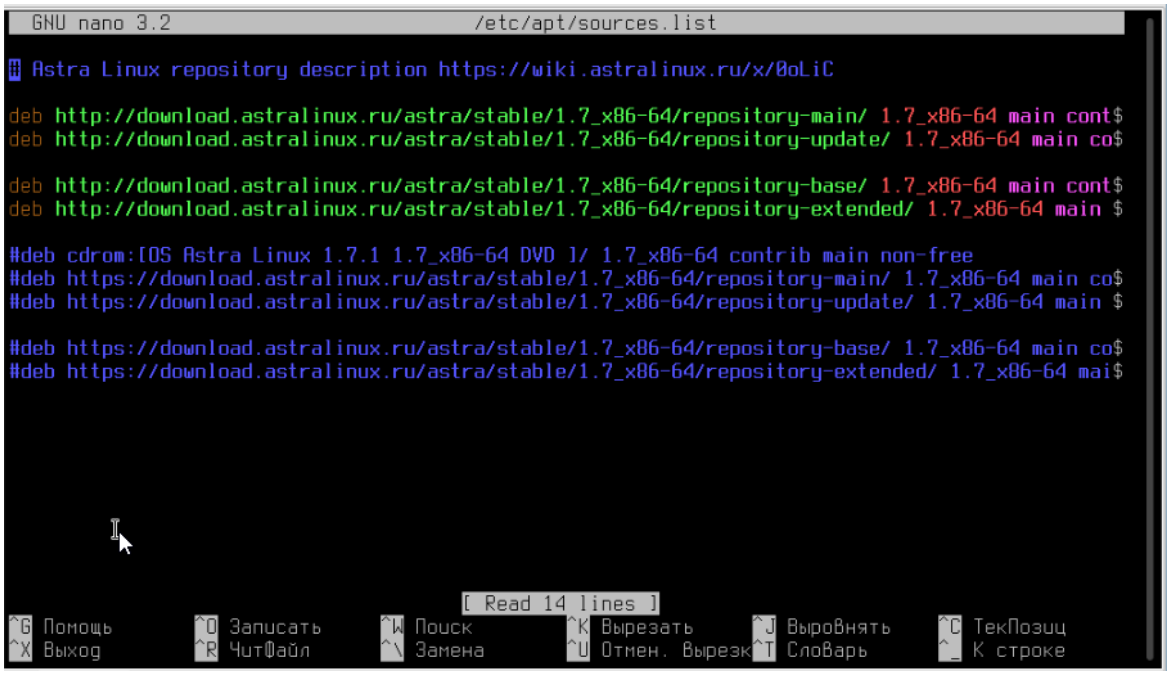
- Перейти в файл /etc/apt/sources.list.Отключить репозитории и оставить только следующие (Допускается замена download на dl):
    - Для Astra Linux Special Edition версии 1.7.0 :

deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-main/ 1.7_x86-64 main contrib non-free

deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-update/ 1.7_x86-64 main contrib non-free

deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-base/ 1.7_x86-64 main contrib non-free

deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/ 1.7_x86-64 main contrib non-free



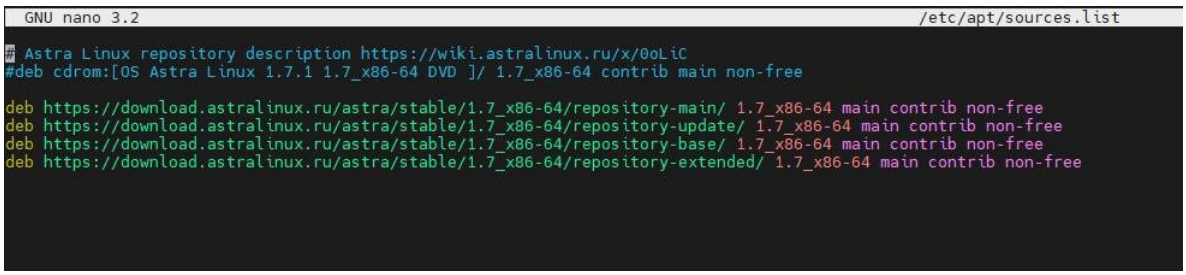
- Для Astra Linux Special Edition версии не ниже 1.7.1:

deb http://download.astralinux.ru/astra/stable/1.7_x86-64/repository-main/ 1.7_x86-64 main contrib non-free

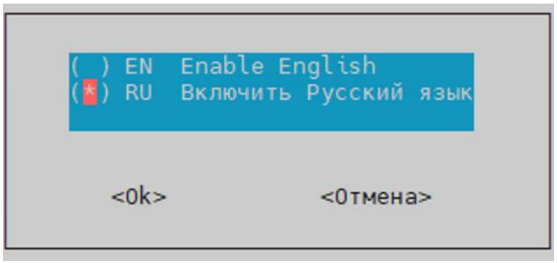
deb http://download.astralinux.ru/astra/stable/1.7_x86-64/repository-update/ 1.7_x86-64 main contrib non-free

deb http://download.astralinux.ru/astra/stable/1.7_x86-64/repository-base/ 1.7_x86-64 main contrib non-free

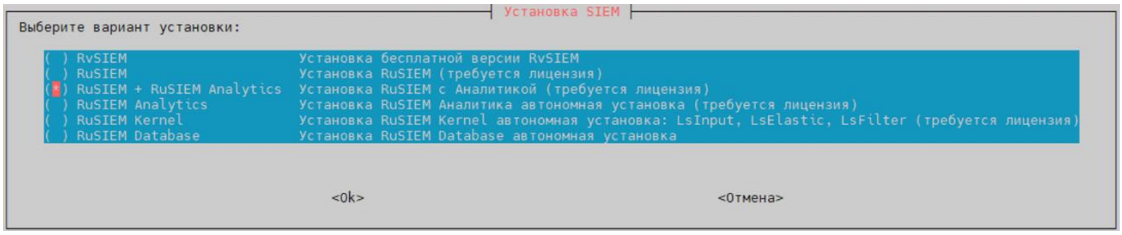
deb http://download.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/ 1.7_x86-64 main contrib non-free



- Выполнить apt update и apt upgrade. После обновления системы ее необходимо перезагрузить
- Скачайте и запустите скрипт установки командой: wget https://files.rusiem.tech/nextcloud/s/gnoSndywnN8oBwe/download -O install.sh; bash ./install.sh
- Выбираем необходимый язык



- Выбираем необходимую версию SIEM



Конфигурация Elasticsearch

1. nano /etc/elasticsearch/jvm.options

   Раскомментировать и изменить:

   (Рекомендованное значение 1/3 ОЗУ если устанавливается аналитика и 1/2 если не устанавливалась)

   -Xms10g

   -Xmx10g

2. nano /etc/default/elasticsearch

   Раскомментировать:

   MAX_LOCKED_MEMORY=unlimited

3. nano /etc/security/limits.conf

   Добавить перед строкой # End of file:

   elasticsearch soft memlock unlimited

   elasticsearch hard memlock unlimited

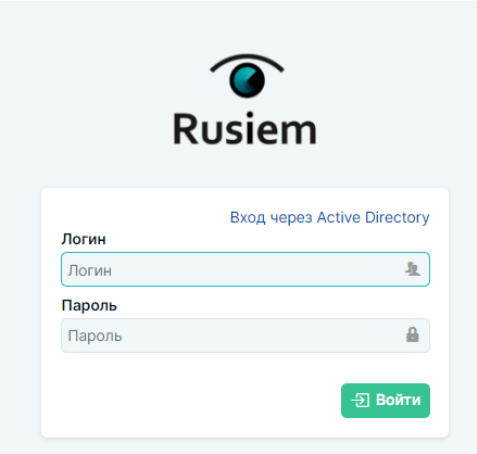
4. nano /usr/lib/systemd/system/elasticsearch.service

   Вставить в блок [Service]

   LimitMEMLOCK=infinity

   После всех настроек systemctl daemon-reload и systemctl restart elasticsearch

   Откройте браузер и перейдите по адресу: https://IP-адрес_VM1 должна отобразиться страница входа в систему:



2.4.3 Установка коллектора событий RuSIEM на Astra Linux

1) После установки системы необходимо в файле /etc/parsec/mswitch.conf изменить параметр zero_if_notfound на yes.

```
# Return zero data instead of ENOENT/ENODATA in the absence of record
zero_if_notfound: yes
```

2) Необходимо получить UUID сервера и направить его на support@rusiem.com

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

3) В файле /etc/apt/sources.list прописать записи и отключить другие:

deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-main/ 1.7_x86-64 main contrib non-free

deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-update/ 1.7_x86-64 main contrib non-free

deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-base/ 1.7_x86-64 main contrib non-free

deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/ 1.7_x86-64 main contrib non-free

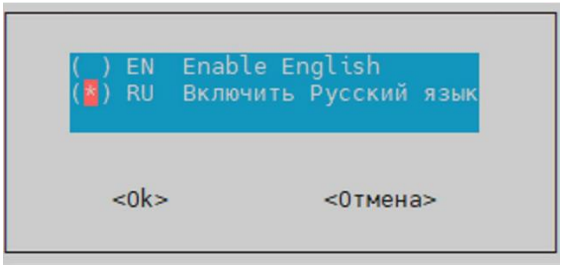
```
 GNU nano 3.2                                    /etc/apt/sources.list

# Astra Linux repository description https://wiki.astralinux.ru/x/0oLiC

#deb cdrom:[OS Astra Linux 1.7.1 1.7_x86-64 DVD ]/ 1.7_x86-64 contrib main non-free
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-main/ 1.7_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-update/ 1.7_x86-64 main contrib non-free

deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-base/ 1.7_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/ 1.7_x86-64 main contrib non-free
```

4) Выполнить apt update и apt upgrade. После обновления системы ее необходимо перезагрузить

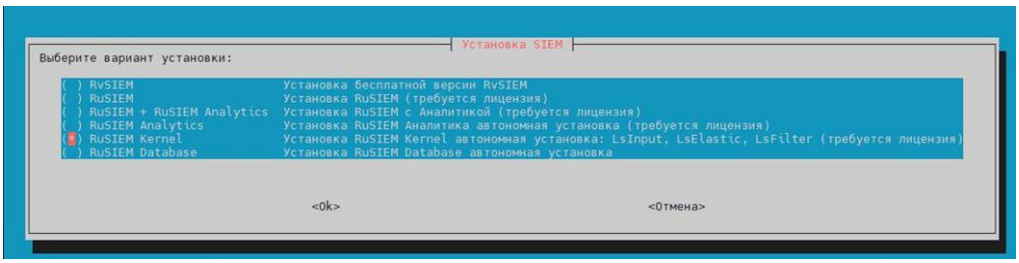
5) Скачать и запустить скрипт установки командой:

wget https://files.rusiem.tech/nextcloud/s/gnoSndywnN8oBwe/download -O install.sh; bash ./install.sh

6) Выбрать язык



7) Вариант RuSIEM Kernel



8) После установки остановить лишние сервисы:

systemctl stop lselastic

systemctl stop postgresql

systemctl stop frs_server

systemctl stop lsfilter

systemctl stop redis

systemctl disable lselastic

systemctl disable frs_server

systemctl disable postgresql

systemctl disable lsfilter

systemctl disable redis

9) Привести crontab в соответствие, выполнить команду EDITOR=nano crontab -e и закомментировать в соответствии с записями ниже лишние строки:

#Ansible: PAID backup user data

#50 23 * * * PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin" /bin/bash /opt/rusiem/support/backup_user_data.sh

#Ansible: PAID rst update

#* * * * * cd /var/www/html;sudo -u www-data php artisan rusiem-ioc:update

#Ansible: PAID clear list referencies

5 1 * * * cd /var/www/html;sudo -u www-data php artisan clear:clear-reference-list-ttl-expired

#Ansible: PAID gossopka update comment

*/3 * * * * cd /var/www/html;sudo -u www-data php artisan gossopka:comments

#Ansible: PAID sender

* * * * * cd /var/www/html;sudo -u www-data php artisan sender:run

#Ansible: PAID esarchive task scheduler

#* * * * * cd /var/www/html;sudo -u www-data php artisan esarchive:scheduler

#Ansible: PAID scheduler correlation

*/5 * * * * cd /var/www/html/;sudo -u www-data php artisan scheduler:correlation

#Ansible: PAID delete unused events

#0 * * * * cd /var/www/html;sudo -u www-data php artisan incidents:delete-unused-events

#Ansible: PAID delete old incidents

#1 1 * * * cd /var/www/html;sudo -u www-data php artisan incidents:delete-old

#Ansible: PAID multitenancy

*/1 * * * * cd /var/www/html;sudo -u www-data php artisan multitenancy

#Ansible: PAID Clear Sessions

*/1 * * * * cd /var/www/html;sudo -u www-data php artisan sessions:clear

#Ansible: PAID Export incidents-history

5 7 * * * cd /var/www/html;sudo -u www-data php artisan export:incidents-history

#Ansible: PAID Check updates

5 6 * * * cd /var/www/html;sudo -u www-data php artisan updates:check

#Ansible: PAID ESarchive delete-old

#5 5 * * * cd /var/www/html;sudo -u www-data php artisan esarchive:delete-old

#Ansible: PAID Sender

*/1 * * * * cd /var/www/html;sudo -u www-data php artisan sender:run

#Ansible: PAID ESarchive sched

#*/1 * * * * cd /var/www/html;sudo -u www-data php artisan esarchive:scheduler

#Ansible: PAID Telegram notifications

*/1 * * * * cd /var/www/html;sudo -u www-data php artisan notification:telegram

10) В конце файла /etc/init.d/firewall.sh дописать правила:

iptables -A INPUT -p tcp -s ip_коллектора --sport 5432 -j ACCEPT

iptables -A OUTPUT -p tcp -d ip_коллектора --dport 5432 -j ACCEPT

iptables -A INPUT -p tcp -s ip_коллектора --sport 260 -j ACCEPT

iptables -A OUTPUT -p tcp -d ip_коллектора --dport 260 -j ACCEPT

iptables -A INPUT -p tcp -s ip_коллектора --sport 240 -j ACCEPT

iptables -A OUTPUT -p tcp -d ip_коллектора --dport 240 -j ACCEPT

iptables -A INPUT -p tcp -s ip_коллектора --sport 231 -j ACCEPT

iptables -A OUTPUT -p tcp -d ip_коллектора --dport 231 -j ACCEPT

iptables -A INPUT -p tcp -s ip_основной_ноды --sport 5432 -j ACCEPT

iptables -A OUTPUT -p tcp -d ip_основной_ноды --dport 5432 -j ACCEPT

iptables -A INPUT -p tcp -s ip_основной_ноды --sport 260 -j ACCEPT

iptables -A OUTPUT -p tcp -d ip_основной_ноды --dport 260 -j ACCEPT

iptables -A INPUT -p tcp -s ip_основной_ноды --sport 240 -j ACCEPT

iptables -A OUTPUT -p tcp -d ip_основной_ноды --dport 240 -j ACCEPT

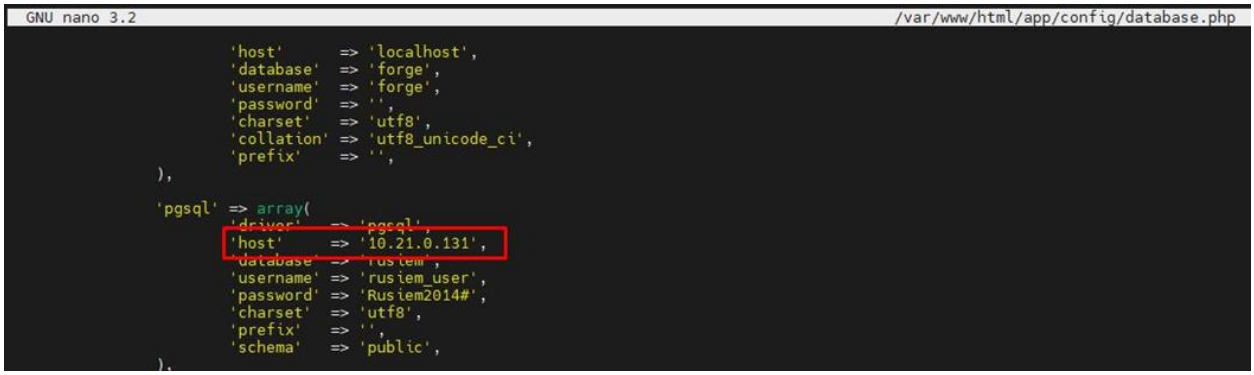
iptables -A INPUT -p tcp -s ip_основной_ноды --sport 231 -j ACCEPT

iptables -A OUTPUT -p tcp -d ip_основной_ноды --dport 231 -j ACCEPT

11) Выполнить /etc/init.d/firewall.sh start

12) Открыть файл /var/www/html/app/config/database.php и изменить у pgsql параметр

'host' => '172.16.0.102' тут указать IP основной ноды RuSIEM, куда должны поступать события.



13) На основной ноде RuSIEM, куда должны поступать события, открыть файл /opt/rusiem/modules_user.yaml и поменять параметр analytics_sa на 1

14) Выполнить на основной ноде /bin/bash /opt/rusiem/tools/provisioner/bin/update.sh

15) В конце файла /etc/init.d/firewall.sh дописать правила на основной ноде:

iptables -A INPUT -p tcp -s ip_коллектора --sport 5432 -j ACCEPT

iptables -A OUTPUT -p tcp -d ip_коллектора --dport 5432 -j ACCEPT

iptables -A INPUT -p tcp -s ip_коллектора --sport 260 -j ACCEPT

iptables -A OUTPUT -p tcp -d ip_коллектора --dport 260 -j ACCEPT

iptables -A INPUT -p tcp -s ip_коллектора --sport 240 -j ACCEPT

iptables -A OUTPUT -p tcp -d ip_коллектора --dport 240 -j ACCEPT

iptables -A INPUT -p tcp -s ip_коллектора --sport 231 -j ACCEPT

iptables -A OUTPUT -p tcp -d ip_коллектора --dport 231 -j ACCEPT

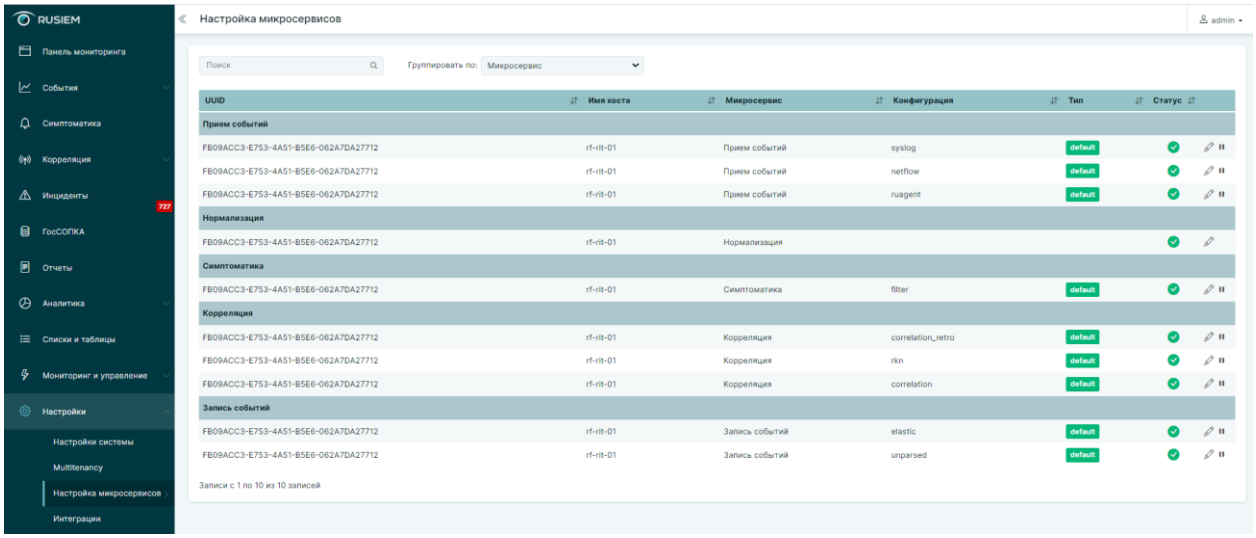
iptables -A INPUT -p tcp -s ip_основной_ноды --sport 5432 -j ACCEPT
iptables -A OUTPUT -p tcp -d ip_основной_ноды --dport 5432 -j ACCEPT
iptables -A INPUT -p tcp -s ip_основной_ноды --sport 260 -j ACCEPT
iptables -A OUTPUT -p tcp -d ip_основной_ноды --dport 260 -j ACCEPT
iptables -A INPUT -p tcp -s ip_основной_ноды --sport 240 -j ACCEPT
iptables -A OUTPUT -p tcp -d ip_основной_ноды --dport 240 -j ACCEPT
iptables -A INPUT -p tcp -s ip_основной_ноды --sport 231 -j ACCEPT
iptables -A OUTPUT -p tcp -d ip_основной_ноды --dport 231 -j ACCEPT

16) Выполнить /etc/init.d/firewall.sh start

17) Выполнить на основной ноде команду systemctl restart postgresql

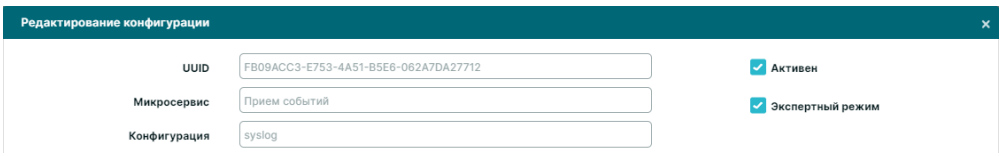
18) На коллекторе выполнить команду systemctl restart lsinput

19) Перейти в веб интерфейс основной ноды на вкладку «Настройки» -> «Настройки микросервисов»

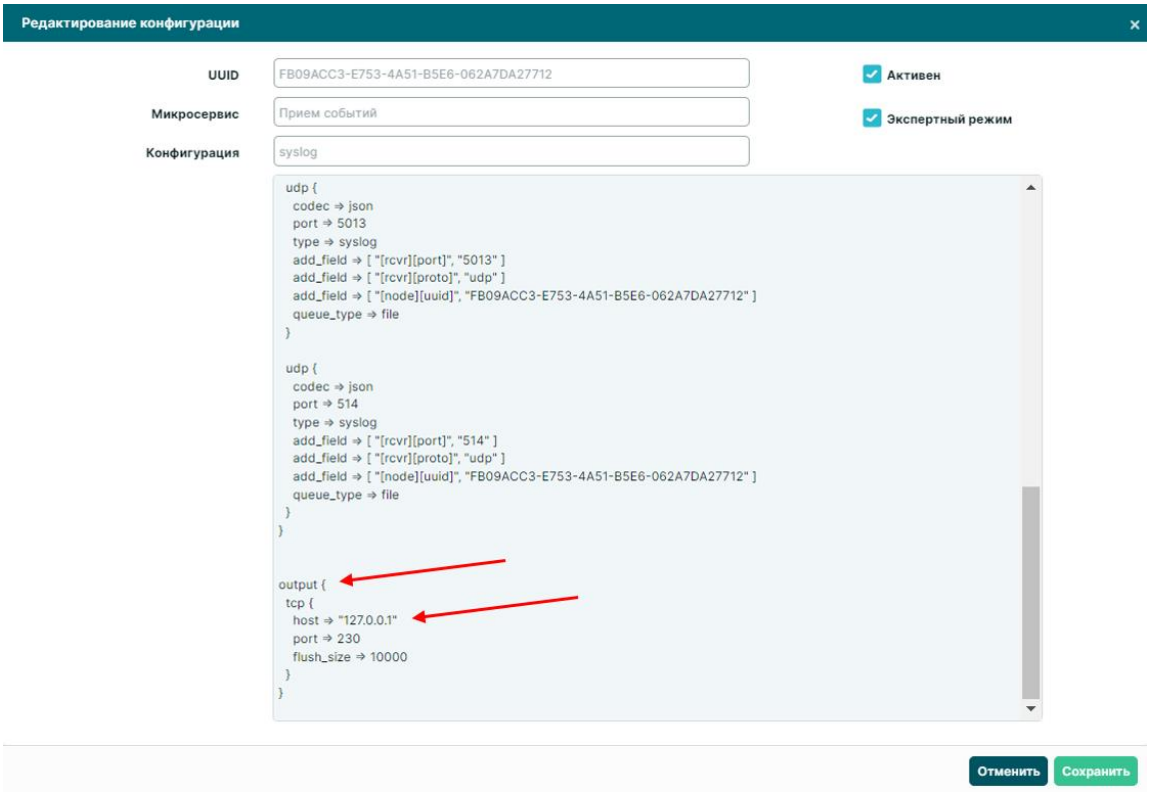


20) Нажать вверху таблицы «UUID» чтобы отсортировать по UUID. У ноды коллектора оставить включенными только микросервисы «Приема событий», другие останавить, если они есть. (нажав на значок в виде кнопки паузы – «деактивировать»)

21) Напротив микросервисов «приема событий» ноды коллектора жмем, по одной за раз, значок карандаша, ставим галочку «экспертный режим»



22) В самом низу списка, в элементе output прописать параметр host, меняя его на IP основной ноды RuSIEM.



23) Повторить это действие для всех микросервисов «приема событий» ноды коллектора.

24) Настройка завершена!

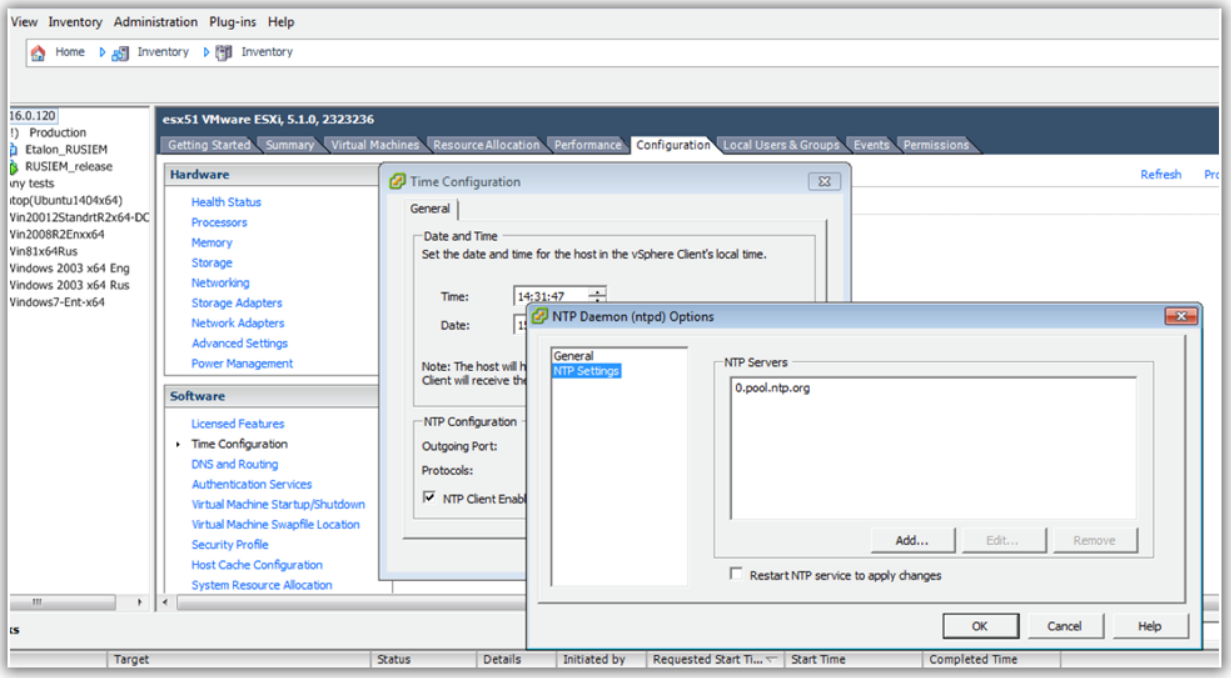
2.5 Конфигурация RuSIEM

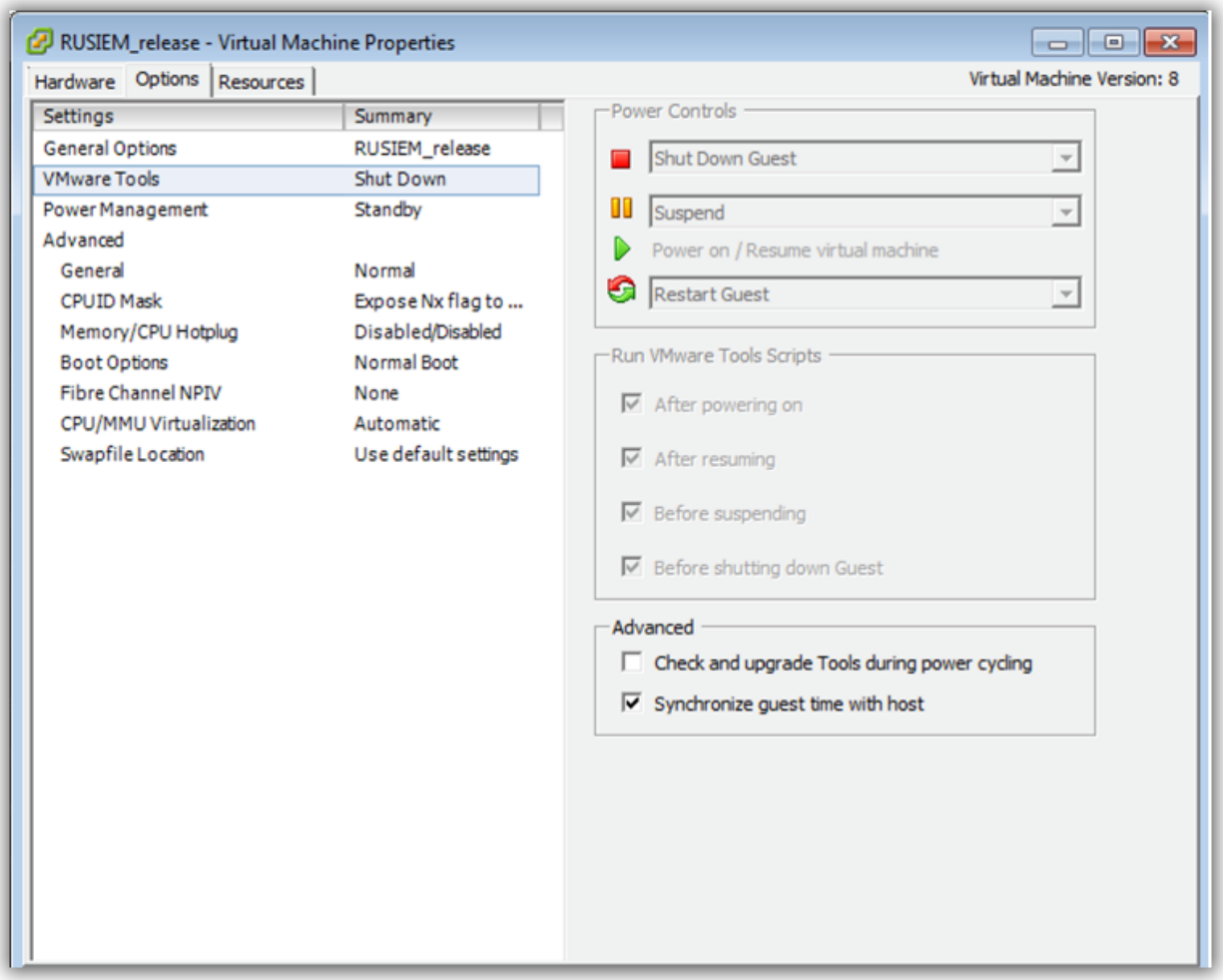
2.5.1 Настройка NTP синхронизации VmWare Esxi

Перед запуском Rusiem необходимо настроить синхронизацию самого сервера ESXi и самой гостевой машины. Пропишите NTP сервер в настройках ESXi как указано на рисунке ниже и установите галку в настройках самой виртуалки. Если у вас имеется NTP сервер внутри корпоративной сети – можете указать его IP адрес или DNS имя.

Для изменения часового пояса в системе прописать:

dpkg-reconfigure tzdata





2.5.2 Доступ к системе по доменному имени

Рекомендуется использовать статические IP адреса для RuSIEM. В случае DHCP это можно настроить в исключениях или увеличив время высвобождения IP адреса.

Для доступа к веб-консоли можно также прописать полученный IP адрес на корпоративном DNS сервере.

2.5.3 Настройка статического IP адреса

Используя клиент ssh или консоль гипервизора залогиньтесь используя индивидуальный пароль/логин для Rusiem (отличается в каждой инсталляции и отличен от используемого для web консоли).

Используя команду:

nano /etc/network/interfaces

пропишите в конфигурационном файле следующие строки, заменив параметры своими:

- auto lo
- iface lo inet loopback
- auto eth0
- iface eth0 inet static
- address 172.16.0.124
- netmask 255.255.255.0
- gateway 172.16.0.1

Подключение дополнительного сетевого интерфейса

Подключение второго интерфейса производится в следующем порядке:

- Для HyperV/ESX серверов добавляется дополнительный виртуальный адаптер;
- Сервер rusiem перезагружается;
- С помощью команды ifconfig выясняется имя интерфейса (для второго и последующего, как правило, eth1, eth2, ethN);
- Используя команду nano /etc/network/interfaces прописывается статический адрес путем добавления в конфигурационный файл строк:

- auto eth1;
- iface eth1 inet static;
- address 172.16.0.125;
- netmask 255.255.255.0;
- gateway 172.16.0.1.

Конфигурация для DHCP

Конфигурация для DHCP:

- auto eth1;
- iface eth1 inet dhcp.

Правила для файервола

Добавьте правила для файервола:

- nano /etc/init.d/firewall.sh;
- найти раздел «# web» и добавить службы, доступные на данном интерфейсе;
- Скопировать сохраненный измененный firewall.sh в /home/rusiem/.

2.5.4 Настройка DNS

Используя команду:

nano /etc/resolvconf/resolv.conf.d/tail

укажите вторичный сервер DNS или оставьте 8.8.8.8. В качестве первого обязательно должен остаться локальный кэширующий сервер с именно этими параметрами:

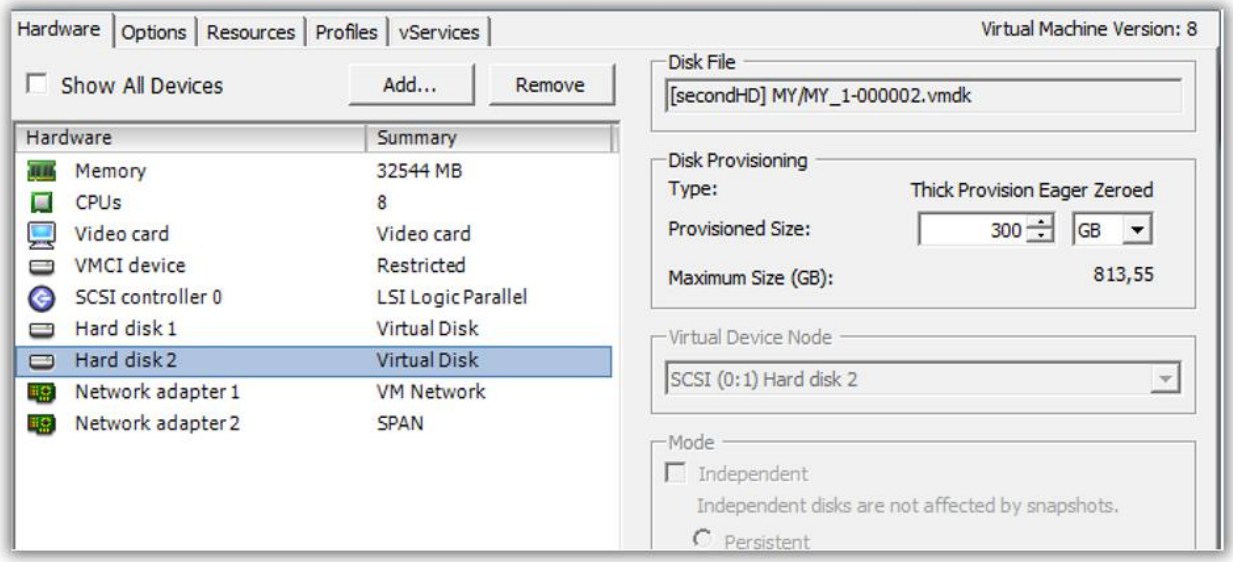
- domain rusiem.local;
- search rusiem.local;
- nameserver 127.0.0.1;
- nameserver 8.8.8.8.

2.5.5 Подключение дополнительного жесткого диска для данных

По умолчанию, на системном диске недостаточно места для хранения поступающих событий. Хранение данных осуществляется в разделе /data/. Наилучшим методом является создание дополнительного диска под хранение данных. С учетом технологии LVM – дисковое пространство может быть

увеличено в дальнейшем. Рекомендуется для тестирования добавлять диск размером не менее 300 GB.

В консоли гипервизора при выключенной виртуальной машине с RuSIEM добавьте новый жесткий диск.

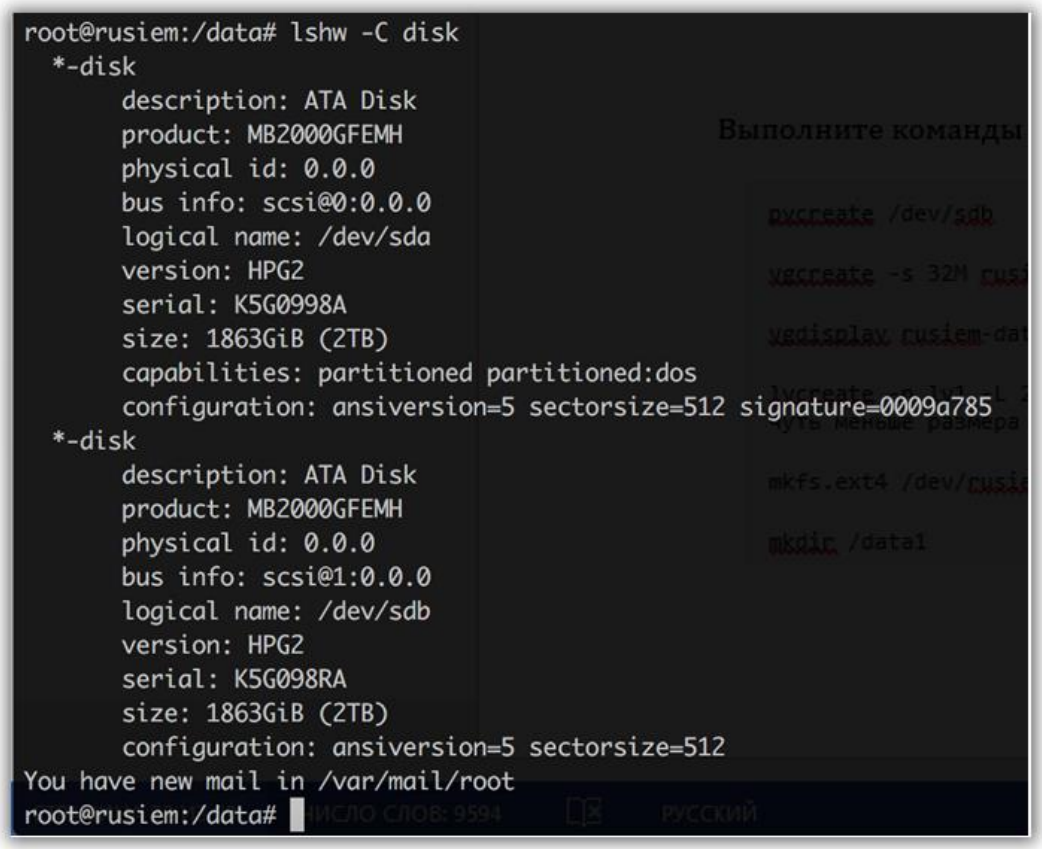


Запустите виртуальную машину, залогиньтесь в консоль с правами root.

Остановите все сервисы RuSIEM командой:

/opt/rusiem/support/stopall.sh

Для проверки какие диски подключены выполните команду lshw -C disk.



Выполните команды ниже для подключения нового диска (здесь sdb – второй жесткий диск):

- pvcreate /dev/sdb;
- vgcreate -s 32M rusiem-data /dev/sdb #ничего здесь не изменять;
- vgdisplay rusiem-data #покажет информацию о созданном диске;
- lvcreate -n lv1 -L 280GB rusiem-data #вместо 280GB указать размер диска. Он всегда чуть меньше размера реального подмапленного нового диска на предыдущих этапах;
- mkfs.ext4 /dev/rusiem-data/lv1;
- mkdir /data1;
- mount /dev/rusiem-data/lv1 /data1/.

Выполните команду:

rsync -a /data/ /data1/

дождитесь выполнения команды (после отработки подождать от 3х минут в зависимости от количества данных)

umount /data

mv data1 data

Если при последних командах возникла ошибка «Device or resource busy» - вы не выполнили команду stopall.sh

Какие процессы держат директорию – можно посмотреть командой:

lsof -n | grep \/data\/

Открыть файл /etc/fstab командой:

nano /etc/fstab и добавьте строчку ниже

/dev/mapper/rusiem--data-lv1 /data ext4 errors=remount-ro 0 1

Сохранить файл.

Перезагрузить сервер командой:

reboot now

После перезагрузки выполнить команды для проверки корректности конфигурации дисковых разделов:

df -h

ls /data

Команда ls /data/ должна показать примерно следующее:

backup clickhouse frs_server lost+found lselastic lsfilter lsinput

2.5.6 Настройка пересылки событий RuSIEM\RvSIEM в другие системы

В системе возможна настройка пересылки событий в другие системы SIEM:

1. Всех событий в исходном формате;
2. Всех событий в rusiem-формате;
3. Событий в rusiem-формате с весом выше указанного;
4. Всех событий в CEF формате;
5. Событий в CEF формате с весом выше указанного;
6. Инцидентов в CEF формате.

Настройка пересылки событий осуществляется через конфигурационные файлы.

2.5.6.1 Настройка пересылки в CEF формате

Скопируйте системный конфигурационный файл /opt/rusiem/frs_server/etc/cef_output командой:

```
cp /opt/rusiem/frs_server/etc/cef_output  /opt/rusiem/frs_server/etc/cef_myout_user.conf
```

Внимание! Постфикс user.conf обязателен

Отредактируйте файл /opt/rusiem/frs_server/etc/cef_myout_user.conf заменив в конфигурации значения:

- host => "172.16.0.36" # ip хоста куда будет осуществляться пересылка;
- port => 1999 # порт назначения пересылки.

Внимание! Остальные параметры следует оставить без изменений.

Если необходимо отключить SSL (TLS) – следует изменить параметр:

ssl_enable => true на ssl_enable => false и закомментировать строки ниже, начинающиеся с ssl_ префикса.

2.5.6.2 Настройка пересылки в формате plain text

Данным способом могут пересылаться события с любого модуля (очереди) обработки. Для пересылки необходимо:

А) Создать конфигурацию /opt/rusiem/frs_server/etc/имя_user.conf

Внимание! Постфикс user.conf обязательно должен присутствовать.

В конфигурации задать следующие строки:

```
input {
internal {
        key => "classified"
```

```
        }
}

filter {
}

output {
tcp {
        codec => line
        host => "172.16.0.125" #ip хоста приемника
        port => 5014 #порт назначения приемника
}
}
```

Для udp трафика (если необходимо) секция output будет выглядеть так:

```
output {
udp {
        codec => plain
        host => "172.16.0.125"
        port => 5014
}
}
```

Б) В конфигурации межсетевого экрана /etc/init.d/firewall.sh добавить при необходимости строки разрешающие исходящий данный тип трафика.

В) Перезагрузить сервер frs командой: service frs_server restart и убедиться, что события поступают на хост приемника.

2.5.6.3 Настройка пересылки с добавлением кастомных меток

```
input {
tcp {
   codec => json
   host => "0.0.0.0"
```

```
    port => 5018
    type => syslog
    add_field => [ "[rcvr][port]", "5018" ]
    add_field => [ "[rcvr][proto]", "tcp" ]
    queue_type => file
  }
}

output {
tcp {
    port => 261
    codec => json
    flush_size => 500
  }
}


input {
internal {    # pickup events from rusiem-mq internal
key => "classified"
}
}

filter {
  mutate {
    add_field => {
      "[soc][db][id]" => "UUID"
            }
                }
}
```

```
output {
tcp {
        codec => json
        host => "192.168.0.1" # change this for “server region B” IP
        port => 5018
#       queue_type => file # this options can be work only in commercial version RuSIEM
}
}

input {
tcp {
    port => 5555
    codec => json
    queue_type => file
  }
}
output {
  tcp {
    port => 262
    host => "127.0.0.1"
  }
}
```

2.5.6.4 Настройка пересылки с применением шифрования TLS

Для TLS следует сгенерировать сертификаты и разместить в /opt/rusiem/frs_server/ssl/ директории. Для отправки – требуется открытый ключ, для приема – закрытый. Сертификаты самоподписанные можно сгенерировать командами:

- openssl genrsa 2048 > ca-key.pem;

- openssl req -new -x509 -nodes -days 3600 -key ca-key.pem -out ca-cert.pem;
- openssl req -newkey rsa:2048 -days 3600 -nodes -keyout server-key.pem -out server-req.pem;
- openssl rsa -in server-key.pem -out server-key.pem;
- openssl x509 -req -in server-req.pem -days 3600 -CA ca-cert.pem -CAkey ca-key.pem -set_serial 01 -out server-cert.pem.

Для пересылки следует воспользоваться конфигурацией /opt/rusiem/frs_server/etc/cef_output и директивами:

```
output {
   tcp {
      codec => cef_lines

      host => "172.16.0.36"
      port => 1999

      ssl_enable => true
      ssl_cacert => "/opt/rusiem/frs_server/ssl/"
      ssl_cert => "/opt/rusiem/frs_server/ssl/cacert.pem"
#       ssl_key => "/opt/rusiem/frs_server/ssl/server-key.pem"
#       ssl_key_passphrase => "P@ssw0rd"
}}
```

Для plain tls без CEF необходимо установить параметр: codec => line.

2.5.6.5 Пересылка событий по условию или паттерну

Для фильтра пересылки можно использовать паттерн или условие. Например, для фильтрации по весу можно использовать if условие:

```
output {
if [symptoms][sweight] > 8 {
   tcp {
```

```
        codec => line
        host => "172.16.0.36"
        port => 5014
    }}
```

Можно использовать строгое условие:

```
if [type] == "syslog" { оператор }
```

Или паттерн:

```
if [message] =~ /monit:/ { оператор }
```

Внимание! Json поля идут без двойных кавычек, с обрамлением скобками []. Не вложенные поля (плоские) – в [имя_поля].

2.5.7 Переназначение портов для приема событий

Возможно переназначение, добавление дополнительных портов для коммуникации с источниками событий. Для агента возможно переназначение портов в настройках системы с изменением для каждого агента в разделе «Источники». Применительно для остальных протоколов – посредством изменения конфигурационных файлов с расширением .conf в каталоге /opt/rusiem/lsinput/etc.

2.5.8 Переключение версий системы

2.5.8.1 Переключение с свободно распространяемой версии RvSIEM на коммерческую RuSIEM

Доступ к репозиторию с коммерческой версии ограничен. Перед переключением необходимо связаться со службой поддержки и получить положительный ответ о предоставленном доступе.

Отредактируйте файл /opt/rusiem/modules_user.dat. Например, командой nano /opt/rusiem/modules_user.dat изменив параметры:

- lm=1;
- siem=1;
- free_rvsiem=0;

- allow_update=1;
- binary_update=1.

и при наличии подключения сервера к сети Интернет - запустите скрипт /opt/rusiem/update/bin/update-hourly.sh.

2.5.8.2 Переключение с коммерческой версии RuSIEM на RuSIEM Analytics

Доступ к репозиторию с коммерческой версии ограничен. Перед переключением необходимо связаться со службой поддержки и получить положительный ответ о предоставленном доступе.

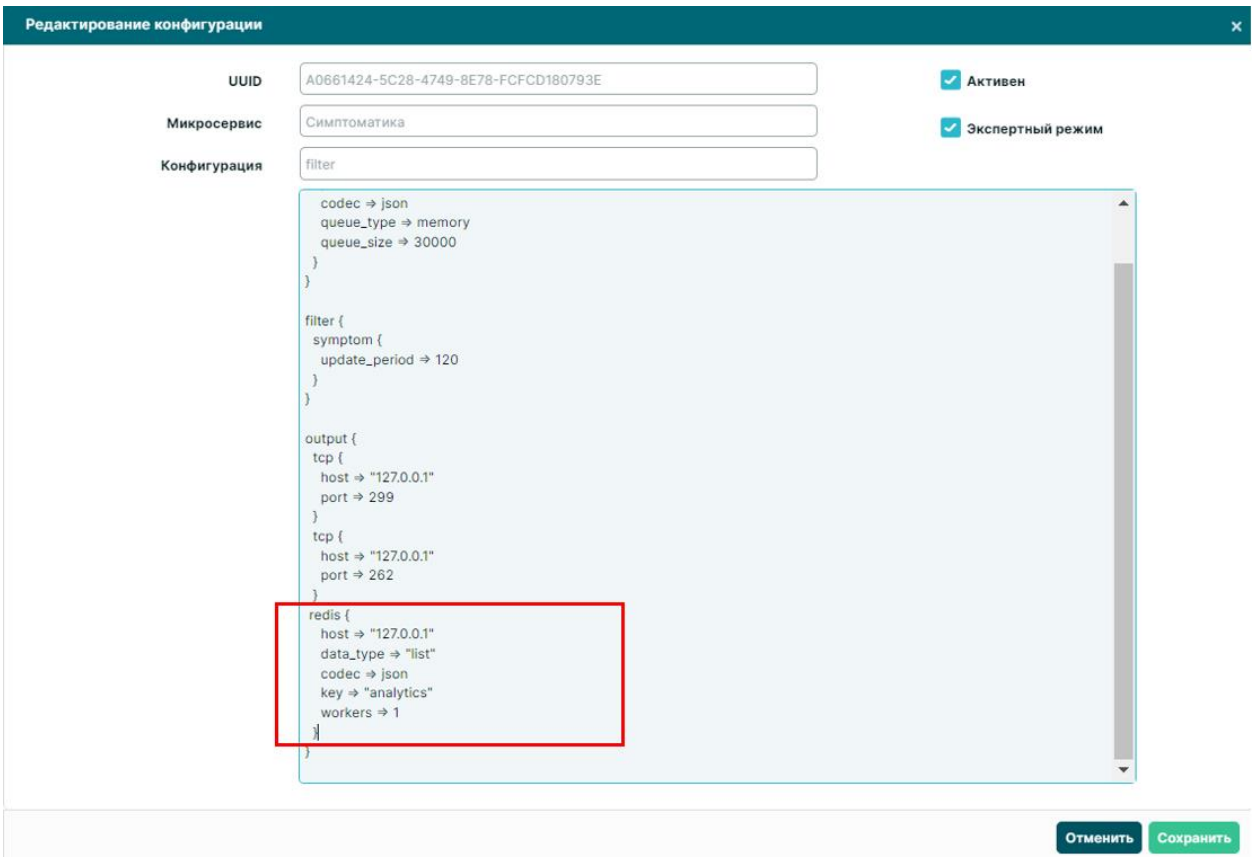
Отредактируйте файл /opt/rusiem/modules_user.dat. Например, командой nano /opt/rusiem/modules_user.dat изменив параметры:

- lm=1;
- siem=1;
- free_rvsiem=0;
- analytics=1;
- allow_update=1;
- binary_update=1.

и при наличии подключения сервера к сети Интернет - запустите скрипт /opt/rusiem/update/bin/update-hourly.sh.

Если аналитика расположена локально, то необходимо перейти в раздел "Настройки" -> "Настройка микросервисов". Напротив микросервиса симптоматики нажать на кнопку редактирования. Далее в открывшемся окне активировать чекбокс ☑ "Экспертный режим" и вписать следующее:

```
redis {
  host => "127.0.0.1"
  data_type => "list"
  codec => json
  key => "analytics"
  workers => 1
 }
```



2.5.8.3 Переключение с коммерческой версии RuSIEM на свободно распространяемую RvSIEM

Отредактируйте файл /opt/rusiem/modules_user.dat. Например, командой nano /opt/rusiem/modules_user.dat изменив параметры:

- lm=1;
- siem=0;
- free_rvsiem=1;
- allow_update=1;
- binary_update=1.

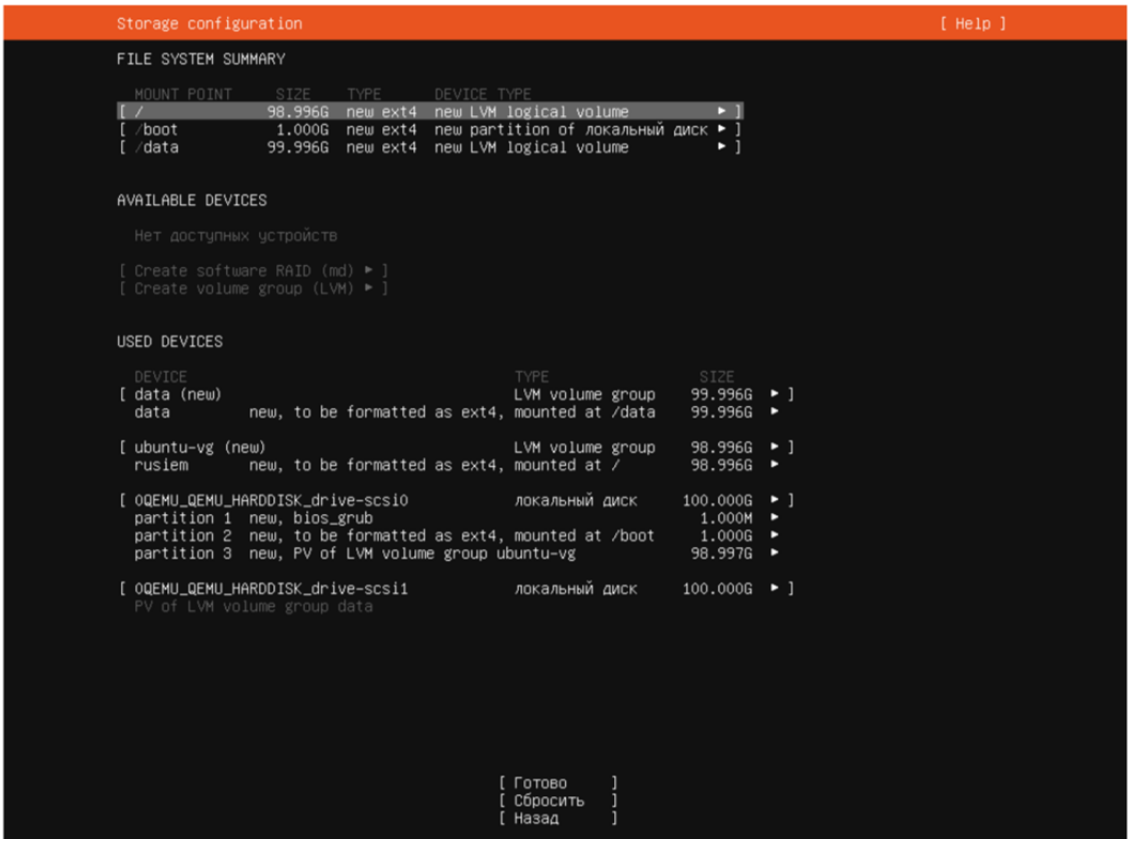
и при наличии подключения сервера к сети Интернет - запустите скрипт /opt/rusiem/update/bin/update-hourly.sh.

2.5.9 Кластер ElasticSearch с переносом данных

Rusiem-Elastic-hot*

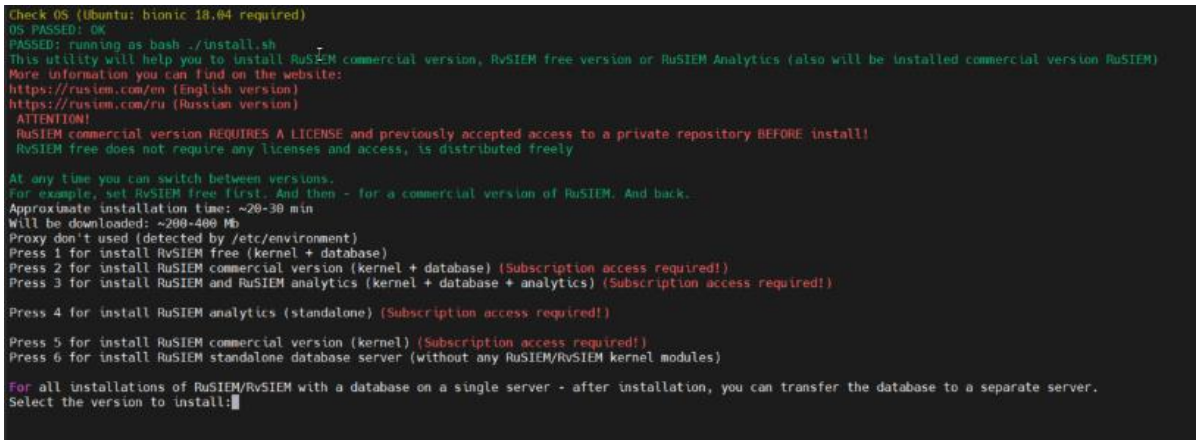
Диск 1 монтируется в корневой раздел /

Диск 2 монтируется в /data раздел

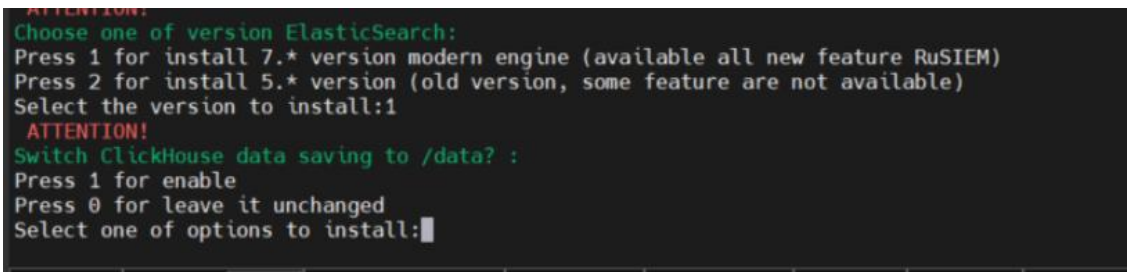


После установки запускаем скрипт:

wget https://files.rusiem.tech/nextcloud/s/j6wcHzzaqT8w5wc/download -O install.sh; bash ./install.sh



Выбираем 6 вариант установки.



После установки изменяем. Устанавливаем значение равное половине ОЗУ.

nano /etc/elasticsearch/jvm.options

-Xms10g

-Xmx10g

В nano /etc/default/elasticsearch необходимо прописать следующую строчку

MAX_LOCKED_MEMORY=unlimited

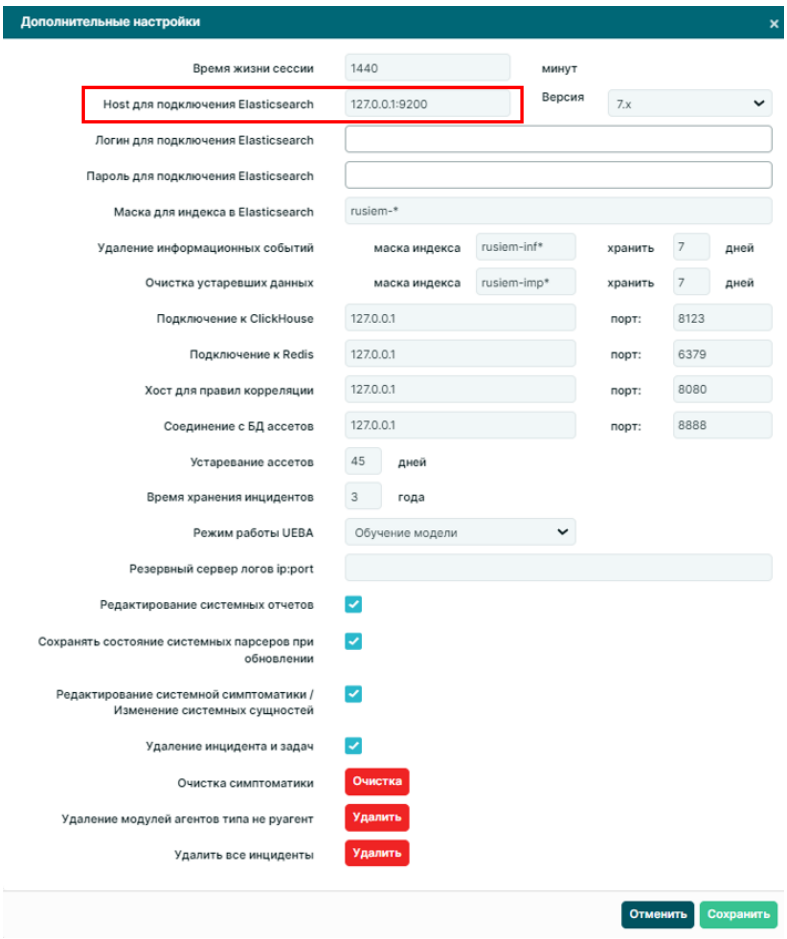
Прописываем настройку hot ноды

nano /etc/elasticsearch/elasticsearch.yml

```
cluster.name: rusiem
node.name: hot_0
node.roles: [data, data_hot, master]
node.attr.box_type: "hot"
cluster.initial_master_nodes: [hot_0]
path.data: /data/elasticsearch
path.logs: /var/log/elasticsearch
bootstrap.memory_lock: true
network.host: 0.0.0.0
http.port: 9200
discovery.zen.ping.unicast.hosts: ["172.16.0.141"]
action.destructive_requires_name: false
```

В discovery.zen.ping.unicast.hosts указываем ip всех нод кроме настраиваемой

Указываем адрес elasticsearch в веб интерфейсе



Измените параметры файла конфигурации modules_user.dat:

nano /opt/rusiem/modules_user.dat

data_node=1 > data_node=0

data_host="127.0.0.1" > data_host="<ElasticSearch IP>"

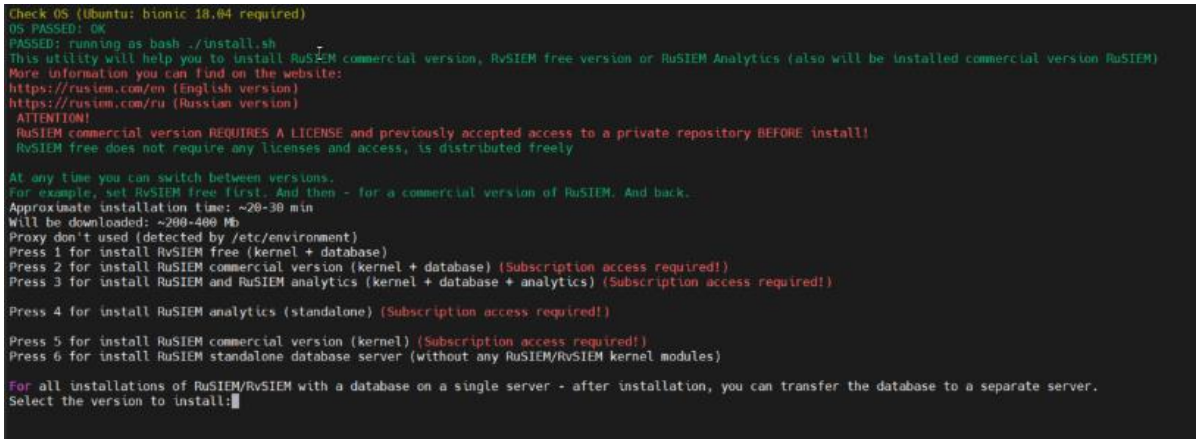
Rusiem-Elastic-cold*

Диск 1 монтируется в корневой раздел /

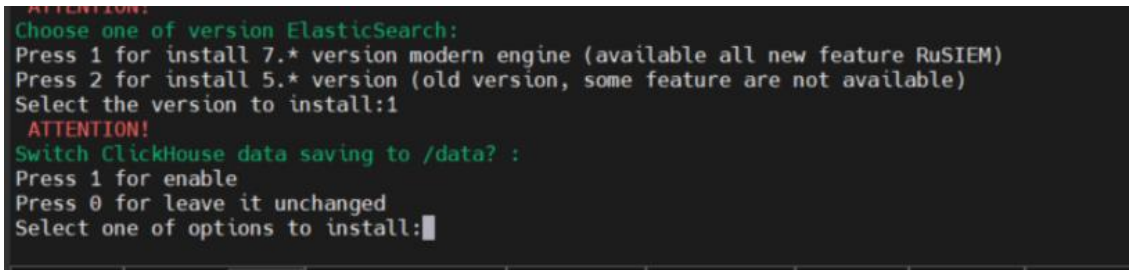
Диск 2 монтируется в /data раздел

После установки запускаем скрипт:

wget https://files.rusiem.tech/nextcloud/s/j6wcHzzaqT8w5wc/download -O install.sh; bash ./install.sh



Выбираем 6 вариант установки.



После установки изменяем. Устанавливаем значение равное половине ОЗУ.

nano /etc/elasticsearch/jvm.options

-Xms10g

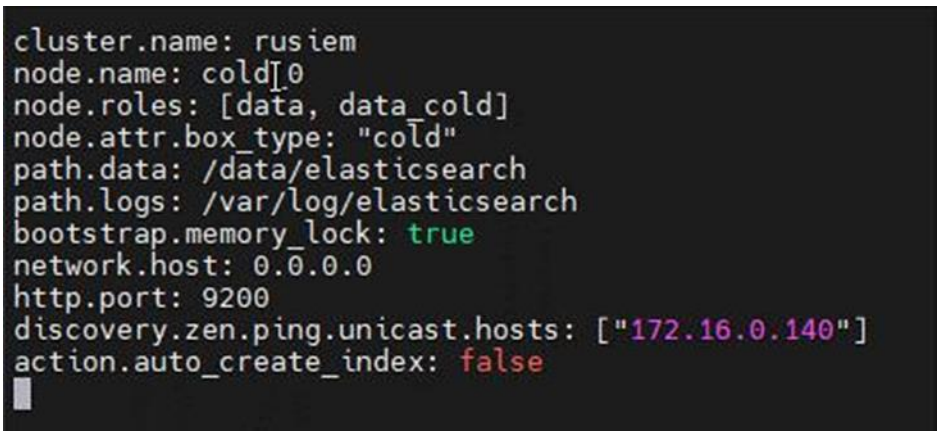
-Xmx10g

В nano /etc/default/elasticsearch необходимо прописать следующую строчку

MAX_LOCKED_MEMORY=unlimited

Прописываем настройку hot ноды

nano /etc/elasticsearch/elasticsearch.yml



В discovery.zen.ping.unicast.hosts указываем ip всех нод кроме настраиваемой

Выполняем:

rm -rf /data/elasticsearch/nodes/*

systemctl restart elasticsearch

на всех нодах elasticsearch (В том числе горячие)

Перенос на холодные ноды:

На головной ноде (LM) необходимо создать файл hot2cold.sh:

touch /opt/rusiem/elastic_template/hot2cold.sh

```
/!#bin/bash

data_host="IP_Hot_node" #Тут необходимо указать ip HOT ноды
data_port="9200"
N=2

cd /opt/rusiem/elastic_template/

while [ "$N" != 1 ]; do
        d=$(date "+%Y.%m.%d" -d "$N days ago")
        echo "$d"
        curl -XPUT -H 'Content-Type:application/json'
http://$data_host:$data_port/rusiem-inf-unparsed$d/_settings -d
@template_cold.json
        curl -XPUT -H 'Content-Type:application/json'
http://$data_host:$data_port/rusiem-imp$d/_settings -d @template_cold.json
        curl -XPUT -H 'Content-Type:application/json'
http://$data_host:$data_port/rusiem-inf$d/_settings -d @template_cold.json
        #curl -H 'Content-Type:application/json' -XPOST
"http://$data_host:$data_port/rusiem-inf-unparsed$d/_close"
        #curl -H 'Content-Type:application/json' -XPOST
"http://$data_host:$data_port/rusiem-inf$d/_close"
        #curl -H 'Content-Type:application/json' -XPOST
"http://$data_host:$data_port/rusiem-imp$d/_close"
        : $((N = $N - 1))
done
```

Добавляем в crontab данный файл:

crontab -e

15 0 * * * PATH='/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin' bash /opt/rusiem/elastic_template/hot2cold.sh

2.6 Установка отдельного сервера баз данных

2.6.1 Установка

Все действия производятся с правами root.

Для установки компонентов базы данных - лицензия не требуется.

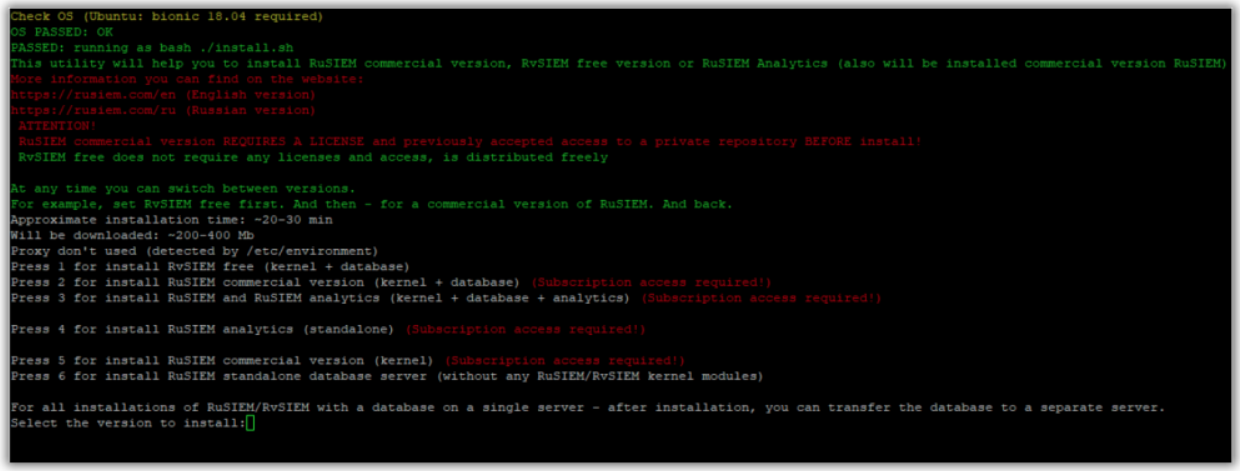
Запуск скрипта установки:

Скрипт под Ubuntu 22.04:

wget https://files.rusiem.tech/nextcloud/s/mgAtFZJwdRj9rax/download -O install.sh; bash ./install.sh

Скрипт под Astra Linux Special Edition (версией не ниже обновления 1.7):

wget https://files.rusiem.tech/nextcloud/s/ktZ4r4daGTGTTs4/download -O install.sh; bash ./install.sh



Выбрать вариант установки RuSIEM standalone database (вариант 6).

2.6.2 Конфигурация Elasticsearch

1. nano /etc/elasticsearch/jvm.options

   Раскомментировать и изменить:

   (Рекомендованное значение 1/3 ОЗУ если устанавливается аналитика и 1/2 если не устанавливалась)

   -Xms10g

   -Xmx10g

2. nano /etc/default/elasticsearch

   Раскомментировать:

   MAX_LOCKED_MEMORY=unlimited

3. nano /etc/security/limits.conf

   Добавить перед строкой # End of file:

   elasticsearch soft memlock unlimited

elasticsearch hard memlock unlimited

4. nano /usr/lib/systemd/system/elasticsearch.service

Вставить в блок [Service]

LimitMEMLOCK=infinity

После всех настроек systemctl daemon-reload и systemctl restart elasticsearch

2.6.3 Настройки межсетевого экрана для взаимодействия с нодой

RuSIEM IP - сетевой адрес RuSIEM

ElasticSearch IP - сетевой адрес дата ноды

На сервере RuSIEM

В файле /etc/init.d/firewall.sh в секцию #elasticsearch добавьте следующие настройки:

iptables --append OUTPUT --protocol tcp --src $EXTIP --dst <ElasticSearch IP> --dport 9200 --jump ACCEPT

iptables --append INPUT --protocol tcp --src <ElasticSearch IP> --sport 9200 --dst $EXTIP --jump ACCEPT

Примените настройки командой:

/etc/init.d/firewall.sh start

2.6.4 Конфигурация сервера RuSIEM

Измените параметры файла конфигурации modules_user.dat:

nano /opt/rusiem/modules_user.dat

data_node=1 > data_node=0

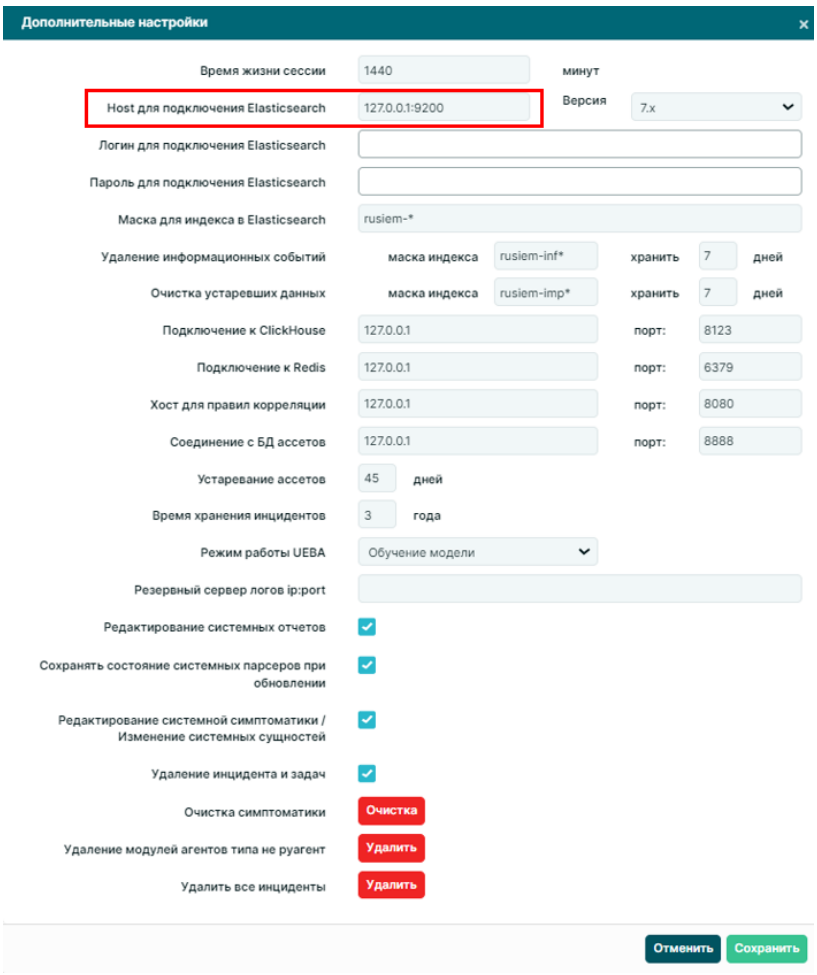
data_host="127.0.0.1" > data_host="<ElasticSearch IP>"

Запустите скрипт:

/opt/rusiem/elastic_template/template.sh

В веб интерфейсе измените параметр - Host for ElasticSearch:

127.0.0.1:9200 > <ElasticSearch IP>:9200



Сохраните изменения.

2.7 Установка модуля Аналитики на отдельный сервер (standalone)

Конфигурация сервера RuSIEM

Запустите install.sh для Ubuntu 18 или Запустите install.sh для Ubuntu 22.04, или Запустите install.sh для Astra.

Установите коммерческую версию (выберите пункт “2”) без модуля аналитики.

Если Rusiem установлен до 25.11.2020, то необходимо обновить firewall.sh командой:

```
cp /opt/rusiem/update/content/init/firewall.sh /etc/init.d/firewall.sh
```

После установки откройте на редактирование файл /opt/rusiem/modules_user.dat.

Укажите в нем следующие опции:

- feeds=1;
- assets=1;

- feeds_update=1;
- vulns_update=1;
- analytics_sa=1;
- analytics=0.

Запустите скрипт /opt/rusiem/update/bin/update-hourly.sh для применения настроек.

Настройка PostgreSQL.

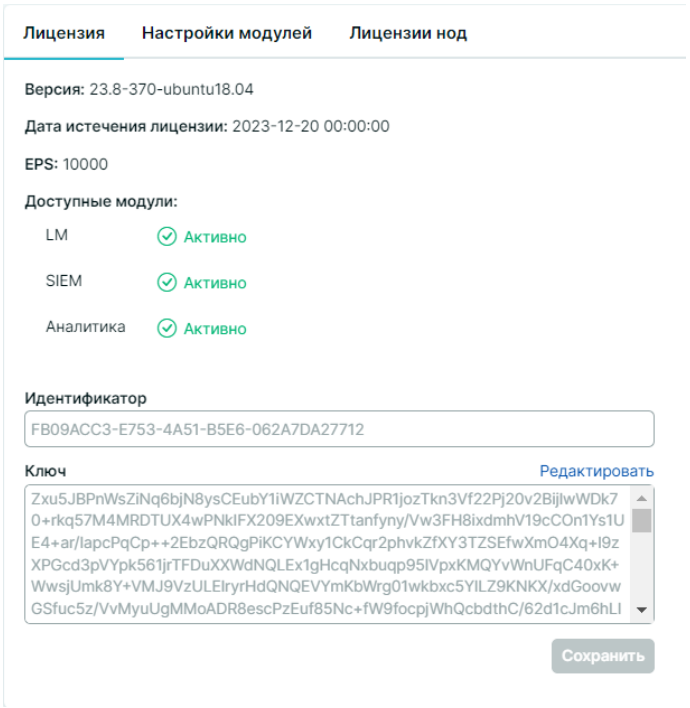
Добавьте ip аналитики следующим образом:

```
echo "host all all <IP>/32 md5" >> /etc/postgresql/10/main/pg_hba.conf
service postgresql reload
```

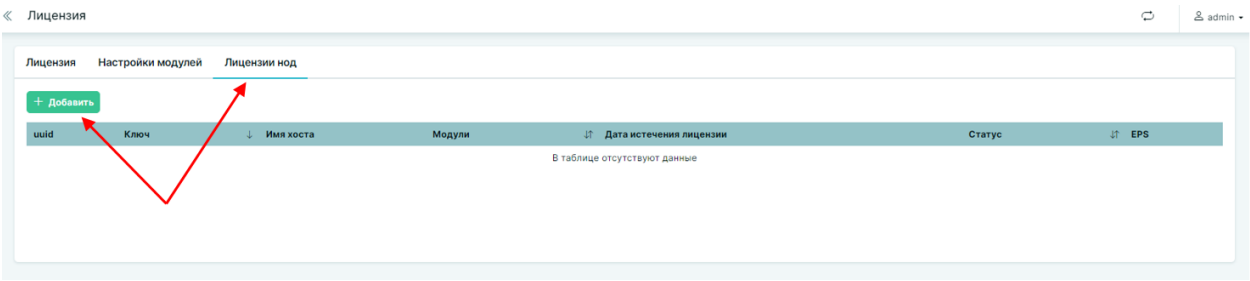
где IP - адрес сервера аналитики.

- Добавьте лицензию на SIEM и аналитику.

  Лицензия на модуль аналитики находится на сервере RuSIEM.

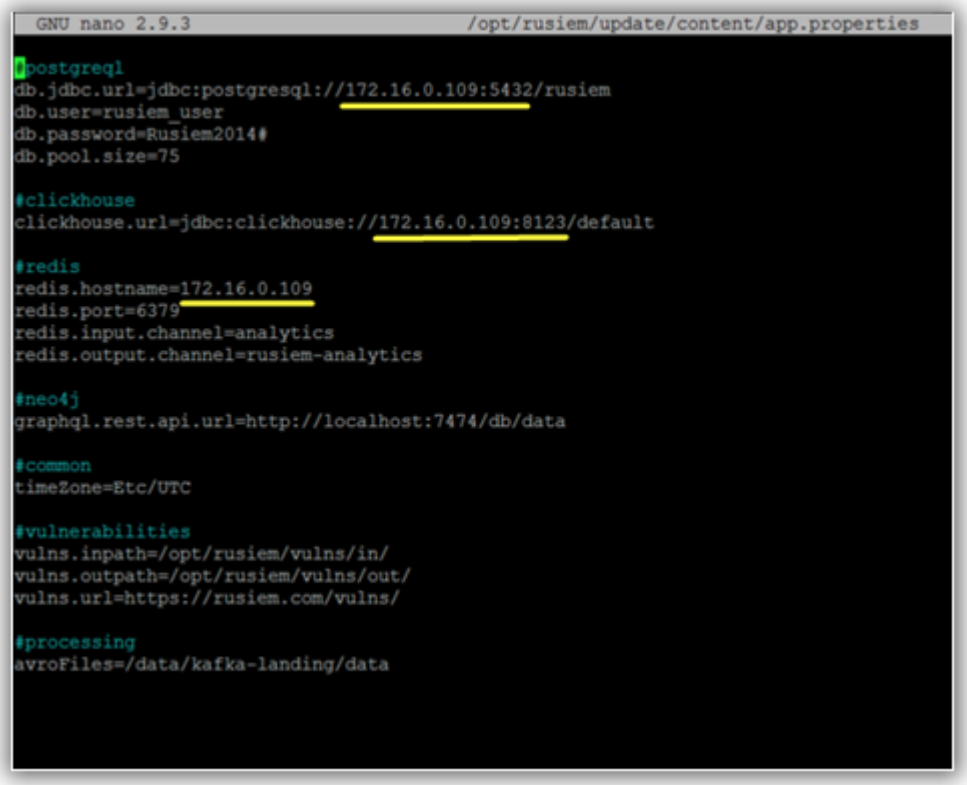


- В лицензиях нод добавьте UUID и ключ для сервера аналитики.



Установка и настройка аналитики версии standalone

- Запустите install.sh для Ubuntu 18 или Запустите install.sh для Ubuntu 22.04, или Запустите install.sh для Astra.
- Запустите установку аналитики (выберите пункт "4").
- Дождитесь окончания установки.
- Откройте на редактирование файл /opt/rusiem/update/content/app.properties и замените ip для подключений к postgresql, clickhouse, redis. В качестве ip указываем ip сервера, где установлен rusiem.



- Для применения настроек необходимо перезапустить сервис аналитики командой:

systemctl restart rusiem-processing.service

Открытые порты

На сервере SIEM и аналитики должны быть открыты порты: 5432, 8123, 6379, 7015 - в обе стороны.

3. Настройка системы

3.1 Настройки proxy

В файле **/etc/environment** должны присутствовать настройки proxy.

Пример:

https_proxy="http://192.168.124.142:3128"

http_proxy="http://192.168.124.142:3128"

ftp_proxy="http://192.168.124.142:3128"

socks_proxy="http://192.168.124.142:3128"

no_proxy=localhost,127.0.0.0, 127.0.0.1, 127.0.1.1, **172.16.0.111**

где **172.16.0.111** – сервер эластик.

а также в файл **/etc/apt/apt.conf** добавлены настройки

Пример:

Acquire::http::proxy "http://192.168.124.142:3128";

Acquire::https::proxy "http://192.168.124.142:3128";

Acquire::ftp::proxy "http://192.168.124.142:3128";

Acquire::socks::proxy "http://192.168.124.142:3128";

Acquire::::proxy "true".

3.2 Настройки modules_user.dat

Все настройки производятся в файле:

/opt/rusiem/modules_user.dat

siem=1 – Опция активирует функционал **SIEM**.

analytics=1 – Опция активирует функционал **Аналитики**.

analytics_sa=1 – Опция активирует функционал **Standalone (отдельно стоящей) Аналитики**.

free_rvsiem=0 – Опция активирует функционал **RvSIEM**.

update_method="deb“– Опция указывает метод обновления. По умолчанию deb. Метод git более не используется.

web=1 – Опция активирует функционал **Веб-Интерфейса**.

lm=1 – Опция активирует функционал **Лог менеджмента** (работы с событиями).

data_node=1 – Опция активирует функционал **Локальной дата ноды**.

data_host="127.0.0.1" – Опция указывает (хост) адрес расположения дата ноды.

data_port="9200" – Опция указывает порт подключения Дата ноды (по умолчанию 9200).

system_syslog=1 – Опция включает опции локального логирования событий сервера SIEM (аудит логов, логи событий демонов и т.д.).

allow_update=1 – Опция включает автоматическое обновление компонентов системы.

os_update=1 – Опция включает обновление компонентов операционной системы.

binary_update=1 – Опция разрешает установку пакетов Rv/RuSIEM.

kb_update=1 – Опция разрешает обновление КБ пакетов (правила нормализации, корреляции, симптоматика и т.д.).

fw_update=0 – Опция разрешает обновления firewall.sh (По умолчанию 0).

web_update=1 – Опция развешает обновление пакета **WEB**.

kernel_update=1 – Опция разрешает обновление **KERNEL** пакета.

arp_scan=1 – Опция активирует **ARP сканирование** (каждые 30 минут).

auto_clean=1 – Опция активирует автоматическую очистку (в настоящее время не используется).

rkn_monitor=1 – Опция активирует **РКН монитор**.

nmap_scan=1 – Опция активирует возможность использования встроенного **сканера NMAP** (в настоящее время не используется).

feeds=1 – Опция активирует **ФИДЫ** (Функционал и отображение в интерфейсе).

assets=1 – Опция активирует функционал **Ассетов (Активы)**.

feeds_update=1 – Опция активирует функционал обновления **Фидов**.

vulns_update=1 – Опция активирует функционал обновления **Уязвимостей**.

custom_config=0 – Опция позволяет использовать собственные конфиги демонов и настроек системы. (защита от перезаписи).

send_incident_tcp=1 – Опция позволяет отправлять инциденты в виде событий, потом привязывать сопровождающие события и отправлять следом.

Для отключения в RuSIEM/RvSIEM локального логирования

Измените параметр system_syslog в значение 0.

system_syslog=0

/opt/rusiem/update/bin/update-hourly.sh

3.3 Настройка межсетевого экрана

Все настройки производятся в файле: /etc/init.d/firewall.sh

Запустить/Применить настройки: /etc/init.d/firewall.sh start

Остановить/Разрешить все: /etc/init.d/firewall.sh stop

Переменные:

$EXTIP – IP адрес внешнего интерфейса

$EXTIF – Имя внешнего интерфейса

Внимание! Все что не разрешено – запрещено.

Документация: http://ipset.netfilter.org/iptables.man.html

Помощь: https://www.perturb.org/content/iptables-rules.html

3.4 Настройка сбора статистики по количеству событий (lsinput)

Перед началом настройки сбора статистики оцените поток событий, без их пост обработки.

Настройка сбора статистики

1) Определите порт и протокол отправки событий от источника.

К примеру TCP/514 или UDP/514.

2) В файле конфигурации lsinput внесите изменения, в зависимости порта и протокола:

- В секции input изменить queue_type на memory

Пример конфигурации для 514 UDP

```
udp {
  codec => json
  port => 514
  type => syslog
  add_field => [ "[rcvr][port]", "514" ]
  add_field => [ "[rcvr][proto]", "udp" ]
  queue_type => memory
}
```

- В секции output измените направление пересылки событий на null, указав размер пакета (flush_size) не менее 25000:

```
null {
  flush_size => 25000
}
```

Пример конфигурации

```
output {
#  redis {
#    host => "127.0.0.1"
#    data_type => "list"
#    key => "lsinputs"
#    codec => json
#  }
#  tcp {
#    host => "127.0.0.1"
#    port => 231
#    flush_size => 10000
#  }

    null {
      flush_size => 25000
    }

}
```

3) Перезапустите lsinput, для приенения файла конфигурации:

```
service lsinput restart
```

4) В файл /opt/rusiem/modules_user.dat добавьте параметр custom_config=1 для защиты файла конфигурации от изменений.

5) Статистика работы собирается в соотвествующие журналы, в зависимости порта и протокола

- 514/UPD - /opt/rusiem/lsinput/log/lsinput.udp_514.syslog.conf.log
- 514/TCP - /opt/rusiem/lsinput/log/lsinput.tcp_514.syslog.conf.log

6) Сбор статистики необходимо собирать за период не менее 2 минут.

7) Входящий поток событий можно получить в сообщении вида:

Tcp/UdpInput [0x7f90c74439d8]: queue size: 0, request per time: 139 {"sec":60,"usec":0},

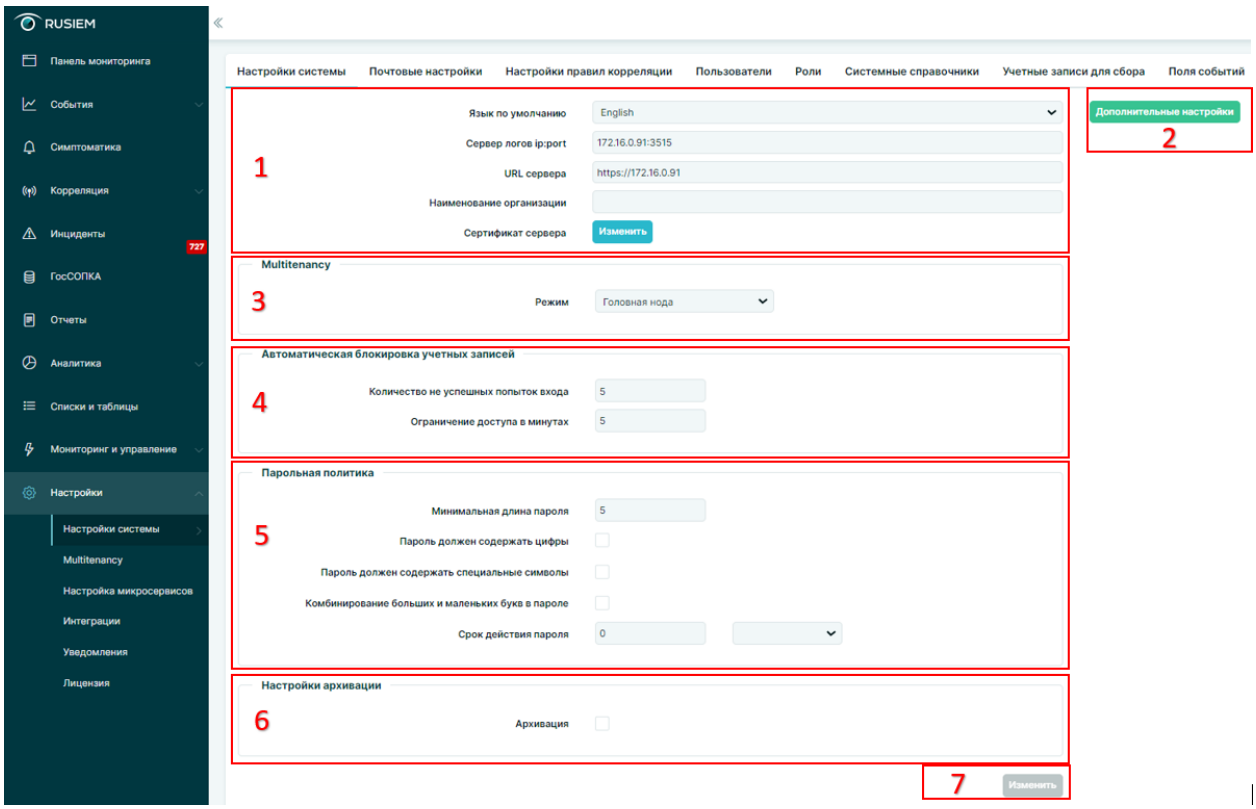
где request per time - количество событий поступивших в систему за одну минуту, для расчета среднего количества событий в секунду (EPS)

Пример журнала для ~21 000 UDP/514

```
2021-05-04 13:43:38 siem [INFO]: CheckerLicenseThread: UUID=A926FE48-6E64-4D26-B0D9-BCDA445BAEE3: license check status: success, eps=90000
2021-05-04 13:43:38 siem [INFO]: CheckerLicenseThread: set_eps_limit=90000
2021-05-04 13:44:33 siem [INFO]: Tcp/UdpInput [0x7f90c74439d8]: queue size: 54, request per time: 1315349 {"sec":60,"usec":0}
2021-05-04 13:44:33 siem [INFO]: NullClientOutput: [0x55d5e0ea2810]: queue size: 212, request per time: 1315019 {"sec":60,"usec":6367}
2021-05-04 13:45:33 siem [INFO]: Tcp/UdpInput [0x7f90c74439d8]: queue size: 183, request per time: 1311153 {"sec":60,"usec":0}
2021-05-04 13:45:33 siem [INFO]: NullClientOutput: [0x55d5e0ea2810]: queue size: 251, request per time: 1311481 {"sec":60,"usec":3838}
2021-05-04 13:46:33 siem [INFO]: Tcp/UdpInput [0x7f90c74439d8]: queue size: 28, request per time: 1322016 {"sec":60,"usec":0}
2021-05-04 13:46:33 siem [INFO]: NullClientOutput: [0x55d5e0ea2810]: queue size: 227, request per time: 1322428 {"sec":60,"usec":3659}
2021-05-04 13:47:33 siem [INFO]: Tcp/UdpInput [0x7f90c74439d8]: queue size: 31, request per time: 1337551 {"sec":60,"usec":0}
2021-05-04 13:47:33 siem [INFO]: NullClientOutput: [0x55d5e0ea2810]: queue size: 242, request per time: 1336768 {"sec":60,"usec":2823}
```

3.5 Раздел "Настройки"

3.5.1 Вкладка "Настройки системы"



№ поля	Наименование
1	"Настройки системы"
2	"Дополнительные настройки"
3	"Multitenancy"
4	"Автоматическая блокировка учетных записей"

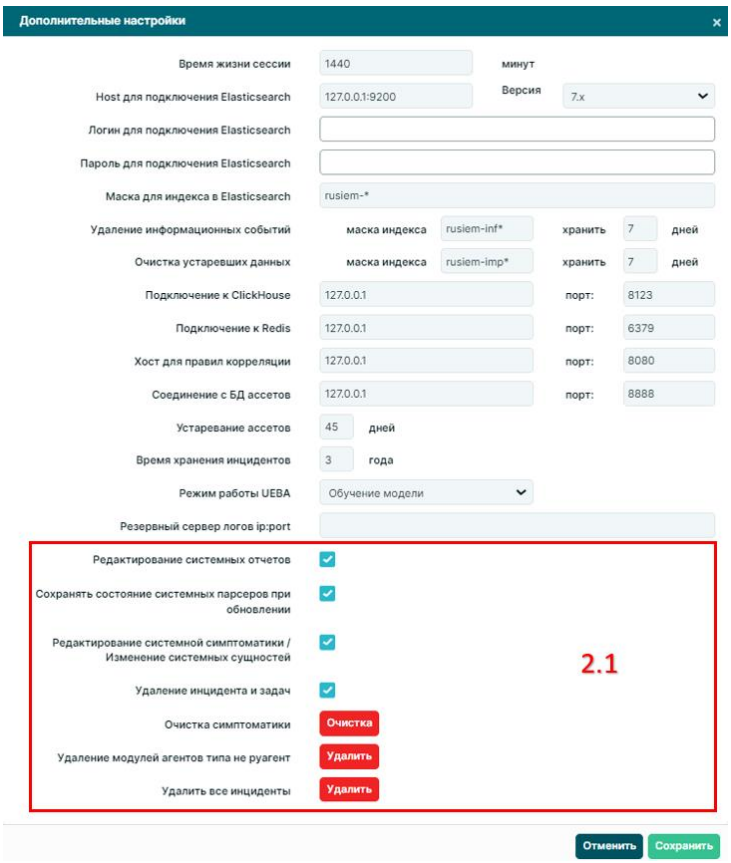
5	"Парольная политика"
6	"Настройки архивации"
7	"Изменить"

В поле "**1**" пропишите следующие параметры:

- Язык по умолчанию: любой;
- 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;
- URL сервера: https://адрес_сервера (вспомогательный параметр, используется при формировании ссылок на инциденты в email-уведомлениях);
- Наименование организации: любое;
- сертификат сервера (п.3.8)

Поле "**3**" описано в п.3.6

Нажмите на кнопку "Дополнительные настройки". Откроется окно, показанное ниже.



Пропишите следующие параметры (остальные настройки кроме указанных оставьте по умолчанию):

- Host для подключения Elasticsearch: 127.0.0.1:9200;
- Версия Elasticsearch: проверьте установленную версию в системе (dpkg -l | grep elasticsearch) и выберите соответствующий вариант (По умолчанию: 5.x);
- В полях "Удаление информационных событий" и "Очистка устаревших данных" пропишите: маска – по умолчанию, время хранения – установите требуемое (рекомендуется оставить значение по умолчанию, впоследствии при наличии места на диске время хранения можно будет увеличить);

Поле "**2-1**" содержит системные настройки, которые предназначены для разработчиков системы и по умолчанию будут недоступны.

В поле "**4**" "Автоматическая блокировка учетных записей" при необходимости введите:

- Количество неуспешных попыток входа - число допустимых неуспешных попыток входа до включения ограничения доступа.
- Ограничение доступа в минутах - временной интервал ограничения доступа после превышения установленного числа неуспешных попыток входа.

В поле "**5**" "Парольная политика" при необходимости введите правила парольной политики.

Поле "**6**" "Настройки архивации" описаны в п. 3.5.1.2

После ввода всех необходимых настроек нажмите "Изменить".

3.5.1.1 Настройка Multitenancy

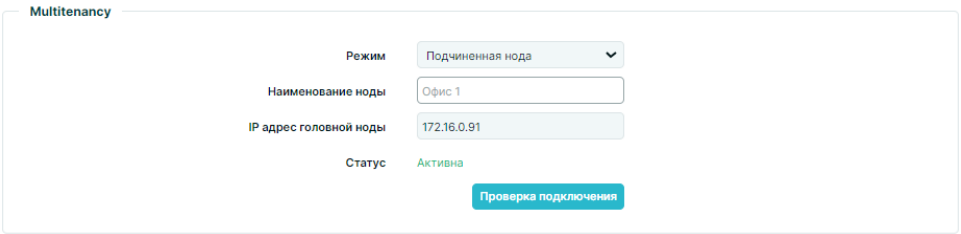
Перейти в раздел "Настройки" на вкладку "Настройки системы". В поле "Multitenancy" выбрать режим Ноды из выпадающего списка:

- Выключен;
- Головная нода;
- Подчиненная нода.

При выборе режима "Головная нода" появится раздел "Multitenancy", описанный в п.3.6.3.

При выборе режима "Подчиненная нода" необходимо заполнить дополнительные поля:

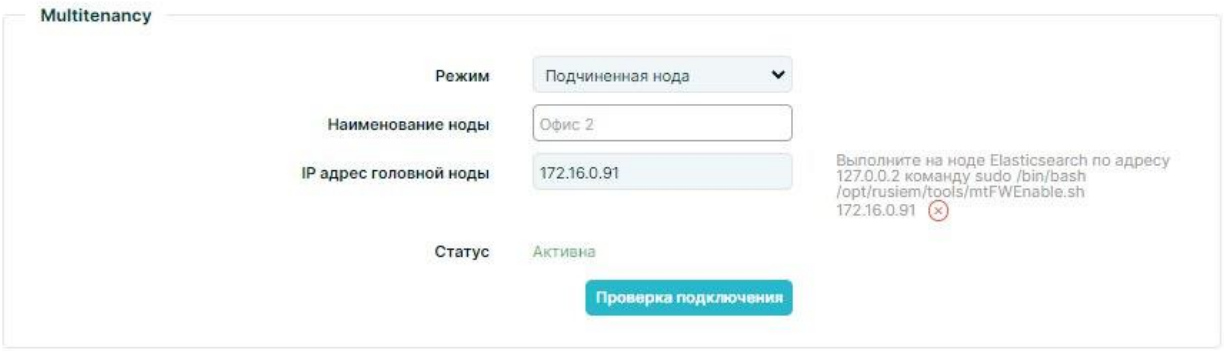
- "Наименование ноды" - ввести наименование подчиненной ноды;
- "IP адрес головной ноды" - указать адрес веб сервера головной ноды;
- Нажать кнопку "Проверка подключения" - проверка соединения с головной нодой. Над кнопкой выводится текст статуса соединения с головной нодой: "Неактивна/Активна".



Последовательность действий с мультитенантностью описана в п.3.6.2.

ВАЖНО:

Для функционирования мультипоиска в случае, если на подчиненной ноде эластик вынесен необходимо подключиться по ssh на ноду с эластиком и выполнить там скрипт, о чем пишется подсказка при включении режима: "подчиненная нода"

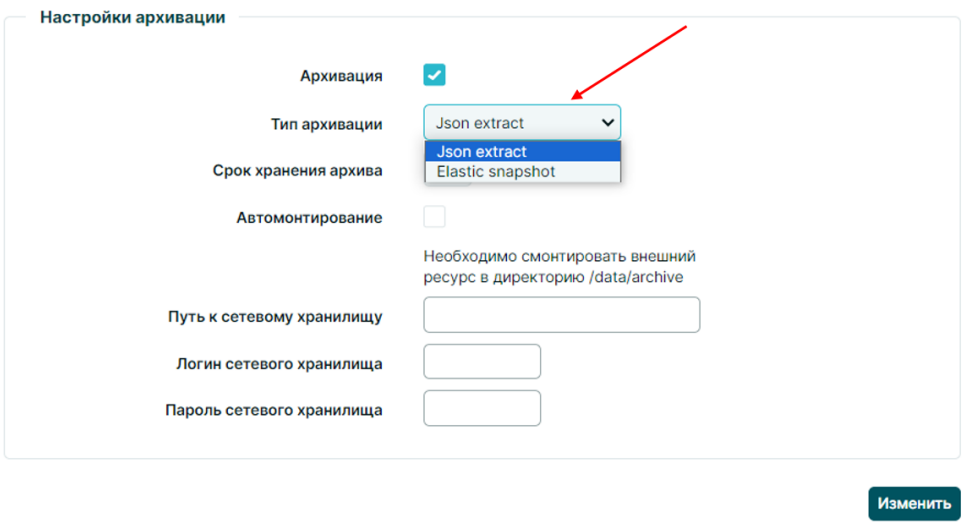


3.5.1.2 Настройка архивации

Для включения архивации событий безопасности, необходимо выделить сетевое хранилище и настроить функционал в RuSIEM:

Настройки - > Настройки архивации - > Архивация. По умолчанию архивация выключена.

Далее произвести настройки:



Необходимо выбрать тип архивации

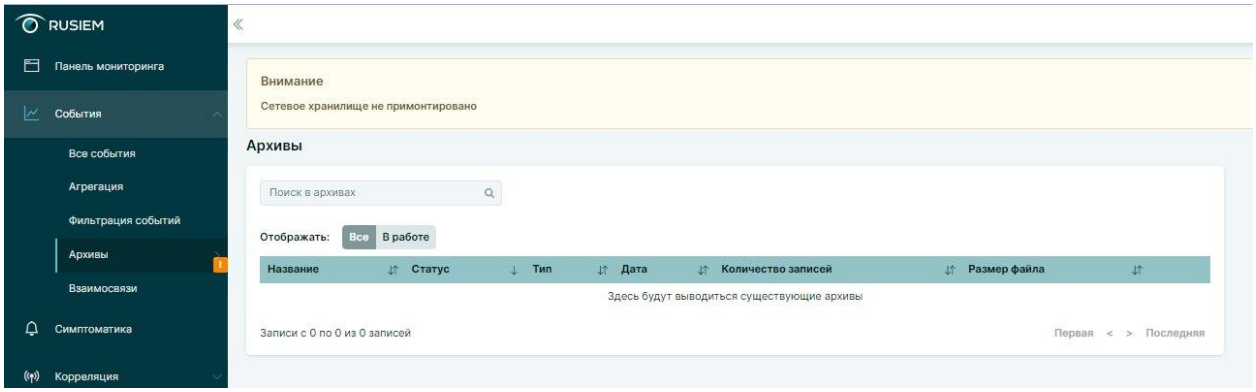
- **Jsonexstract**– индексы ужимаются в 9 раз, однако процесс архивации и разархивации занимает продолжительное время. Использование до 2-3k EPS (верхнее ограничение строго - 3k EPS).
- **Elastic snapshot**- Индексы занимают столько-же места, сколько и в Эластике. Архивация и разархивация происходит очень быстро. Можно использовать когда угодно.

Важно! При изменении типа архивации в списке архивов отобразятся только архивы данного типа.

Автомонтирование – при активации происходит автоматическое соединение с хранилищем и проводится мониторинг соединения.

Если автомонтирование не доступно то необходимо вручную смонтировать внешнее хранилище на сервере RuSIEM в папку **/data/archive**.

Если хранилище не примонтировано, система выведет восклицательный знак в разделе Архивы и сообщение «Сетевое хранилище не примонтировано»



Далее нужно указать **путь** к сетевому хранилищу.

При необходимости указать **логин** и **пароль** сетевого хранилища.

Elastic Snapshot при вынесенном ElasticSearch

Если Elasticsearch вынесен на отдельный сервер, для архивации в режиме "ElasticSnapshot" необходимо выполнить следующие действия:

На каждом сервере с ElasticSearch:

1) В консоле прописать

/opt/rusiem/modules_user.dat

На всех нодах кластера указать адрес веб-интерфейса системы

web_url="ip_addrr"

```
siem=0
analytics=0
free_rvsiem=0
update_method="deb"
whitelabel=0
web=0
lm=0
data_node=1
data_host="127.0.0.1"
data_port="9200"
system_syslog=1
allow_update=1
os_update=1
binary_update=1
kb_update=1
fw_update=0
web_update=0
kernel_update=1
arp_scan=0
auto_clean=1
rkn_monitor=0
nmap_scan=0
update_grub=1
es_version=7
analytics_ext=1
web_url="172.16.0.103"
```

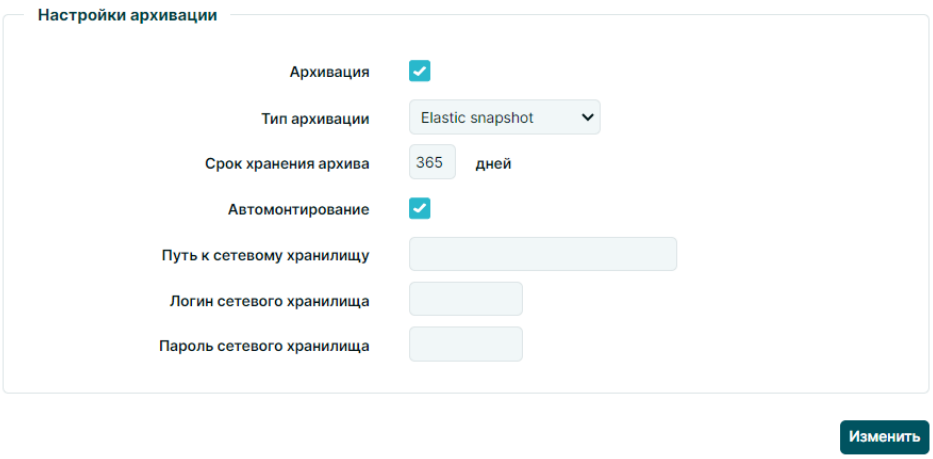
2) На всех нодах запустить этот скрипт, он возьмет публичный ключ вебки для дальнейшей авторизации

/opt/rusiem/tools/get_key.sh

3) На всех нодах проверить в **/etc/elasticsearch/elasticsearch.yml** настройку **path.repo: /data/archive**

4) В вебке включить архивацию.

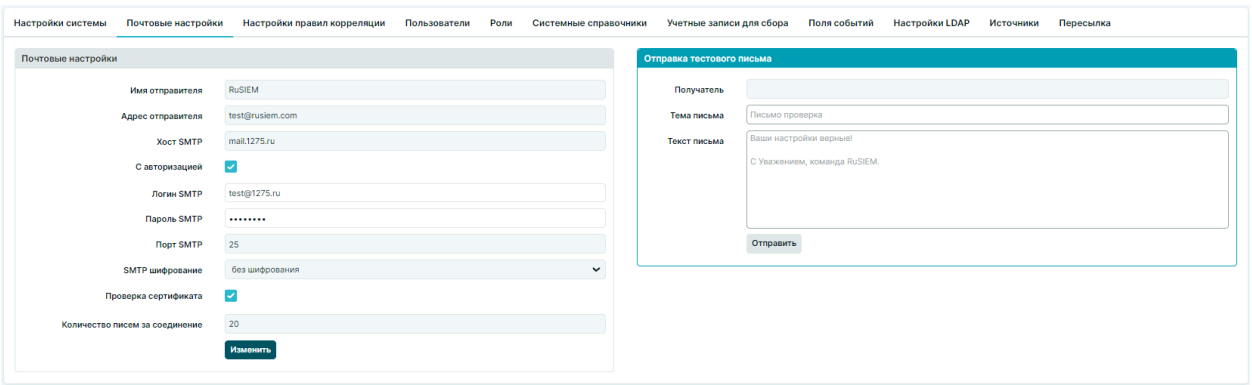
Перейти в раздел "Настройки", в поле "Настройки архивации" установить галочку ☑ Архивация.



3.5.2 Вкладка "Почтовые настройки"

Для подключения внешнего почтового сервера выполните следующие настройки:

- в поле "Адрес отправителя" укажите адрес отправителя вида: имя_отправителя@имя_домена_сети;
- в поле "Хост SMTP" укажите адрес почтового сервера.



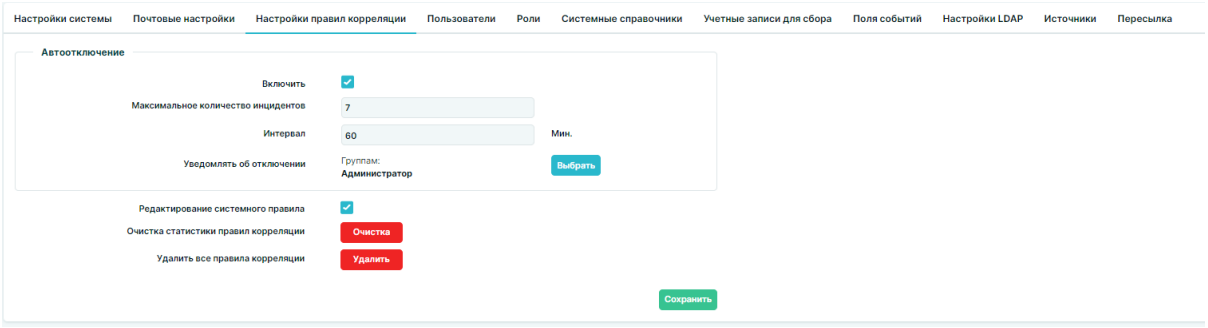
При выборе функционала авторизации укажите логин и пароль STMP, порт передачи данных и выберите тип шифрования данных: "без шифрования", "tls" или "ssl".

После заполнения необходимых полей нажмите на кнопку "Изменить".

3.5.3 Настройки правил корреляци

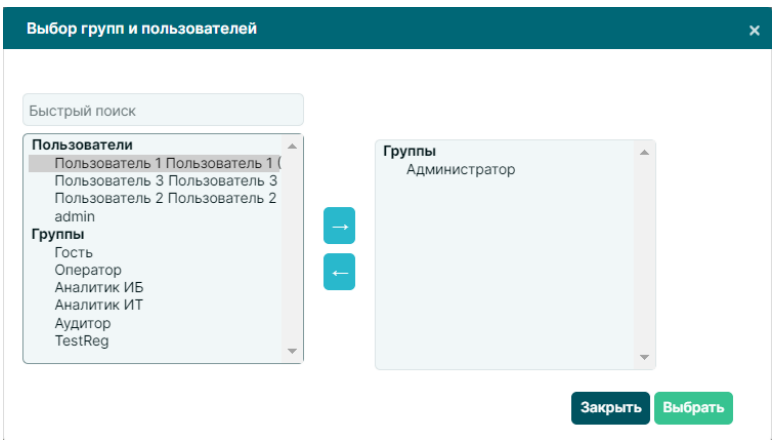
Настройка автоотключения правил корреляции

Автоотключение можно настроить на все правила или на каждое отдельно.



Для **общих настроек на все правила** корреляции необходимо активировать чекбокс **Включить** в блоке "Автоотключение" и заполнить появившиеся поля:

- **Максимальное количество инцидентов** - указать количество инцидентов, после превышения которого в течение указанного интервала, правила автоматически отключаются;
- **Интервал** - указать интервал в минутах, в течении которого выявляется превышение порогового значения;
- **Уведомлять об отключении**:
  - нажать на кнопку **Выбрать**;



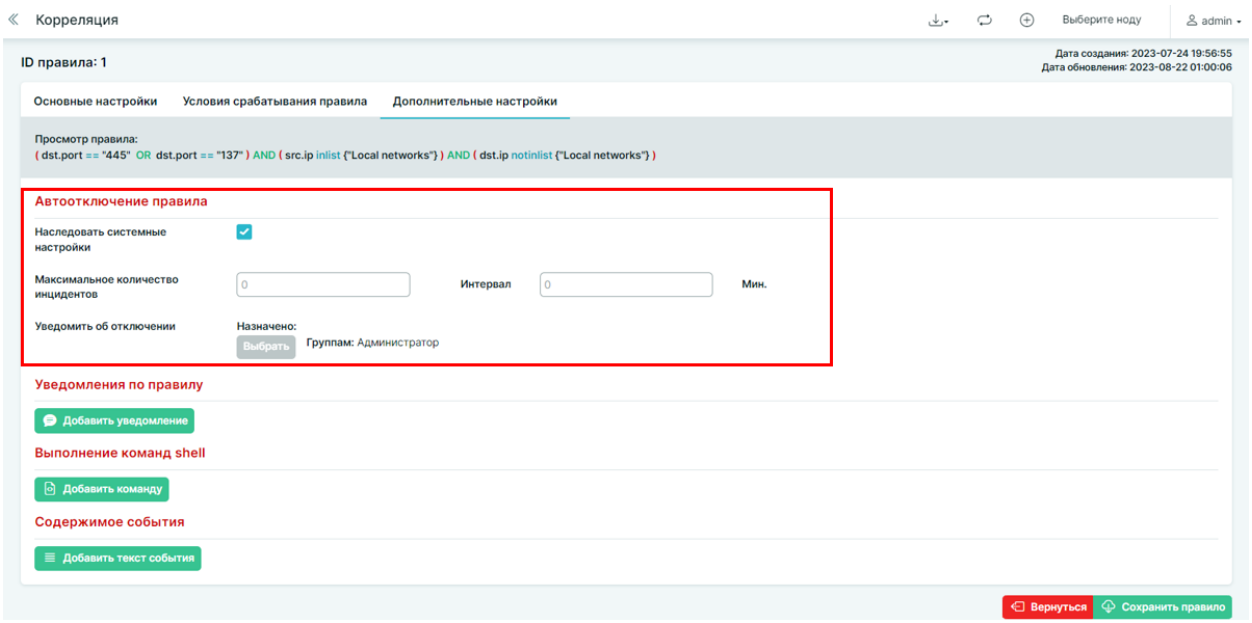
  - В открывшемся окне выбрать необходимых пользователей или группы, которым будет поступать уведомление об отключении правил.

После блока "Автоотключение":

- Чекбокс ☑ "**Редактирование системного правила**" - данная опция необходима для выдачи доступа управления системными правилами;
- **Очистка статистики правил корреляции** - при нажатии на кнопку "**Очистка**" происходит обнуление статистики сработки правил корреляции;
- **Удаление всех правил корреляции** - при нажатии на кнопку "**Удалить**" происходит удаление всех правил корреляции.

При включенном автоотключении

В окне создания/редактирования правил корреляции перейти на вкладку «Дополнительные настройки» появится блок "Автоотключение правила". Автоматически в каждом блоке будут наследоваться системные настройки.



Для **индивидуальной настройки** автоотключения правила корреляции необходимо:

- Снять галочку чекбокса ☐ "**Наследовать системные настройки**".
- Указать **максимальное количество инцидентов.**
- Указать **интервал** работы правила.

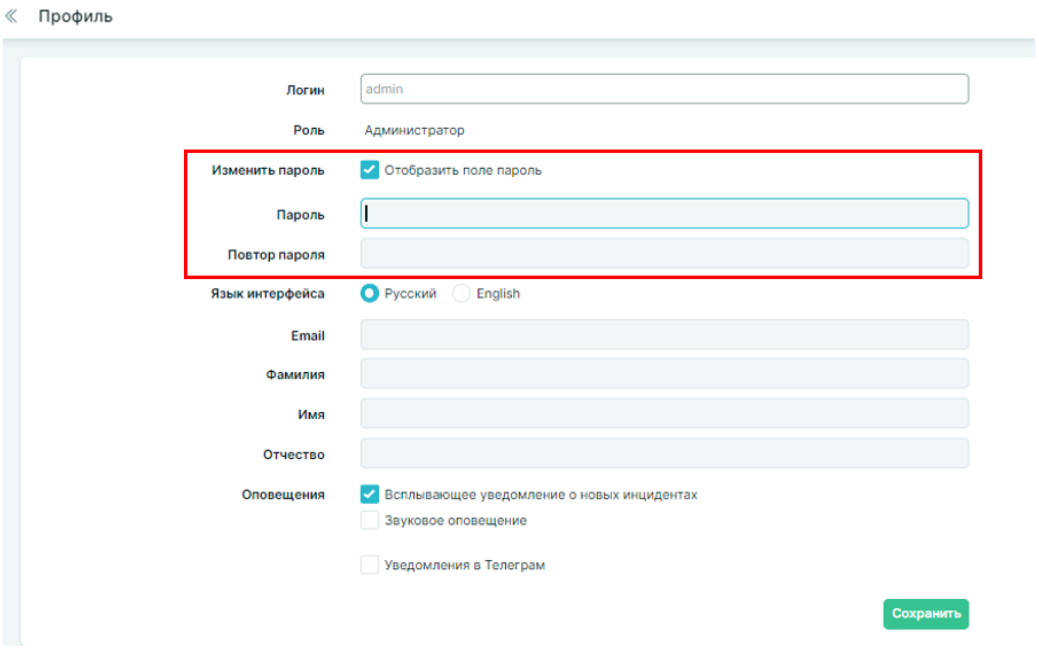
- **Выбрать пользователей или группы**, которым будут отправлены уведомления об отключении данного правила.
- Нажать кнопку "Сохранить правило".

Для использования данных настроек автоотключения необходимо для выбранных пользователей установить права доступа в блоке "Корреляция" (подробнее 3.5.5 Вкладка "Роли").

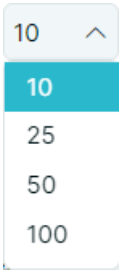
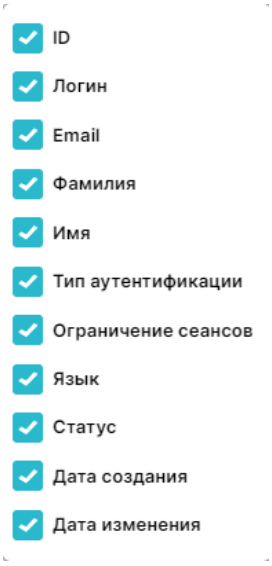
3.5.4 "Изменить пароль"

Для изменения пароля перейти в профиль в правом верхнем углу и установить галочку «Изменить пароль»:

- В поле "Пароль" введите свой новый пароль;
- Введите новый пароль в поле "Повтор пароля" и нажмите на кнопку "Сохранить".



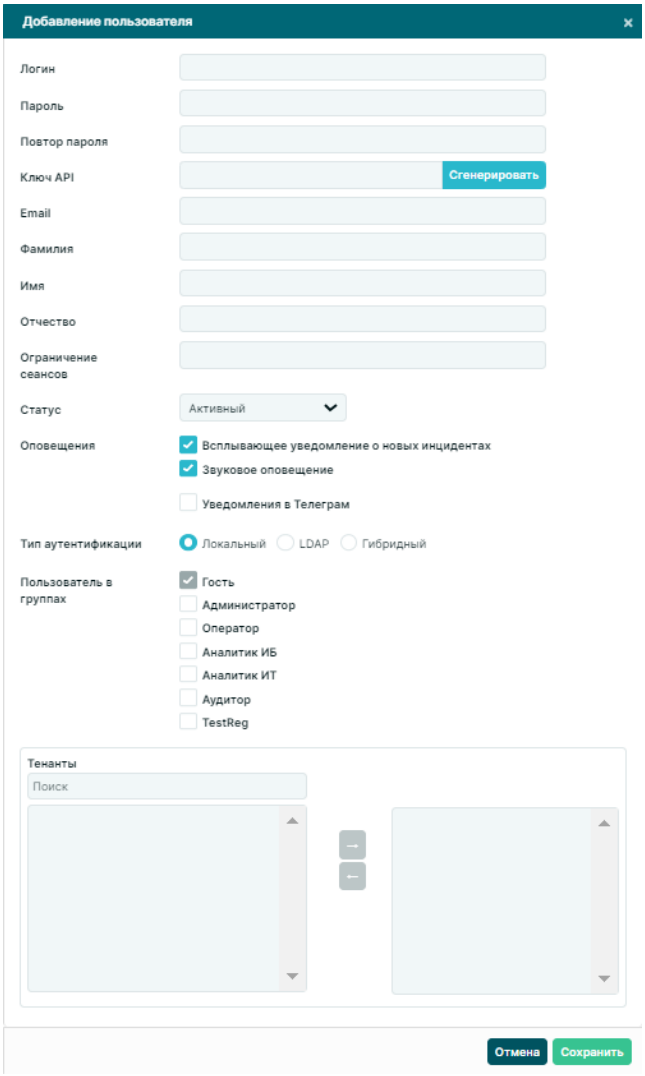
3.5.5 Вкладка "Пользователи"

№ Кнопки/ элемента управления	Наименование	Описание
1	"Добавить"	Добавление пользователя
2	"Поиск пользователей"	Поиск пользователей по введенному критерию
3	"Показать"	Выбор в выпадающем списке количества отображаемых на одной странице пользователей в списке 
4	"Показать/Скрыть колонки"	Выбор в выпадающем меню отображаения/скрытия колонок в списке пользователей 
5	"Редактировать"	Редактирование выбранного пользователя
6	"Удалить"	Удаление выбранного пользователя

Добавление пользователя

Для добавления нового пользователя нажмите на кнопку  .

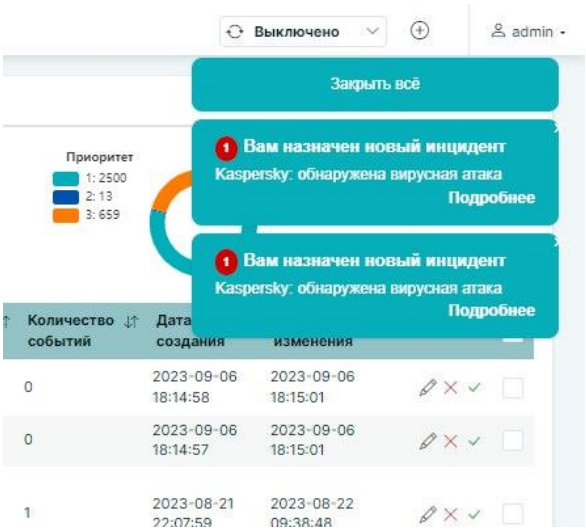
Блок **"Тенанты"** отображается **только при наличии головной и подчиненных нодах,** которые настраиваются на вкладке "Настройки системы" в блоке "Multitenancy".



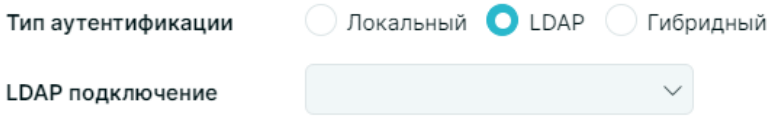
В отобразившемся окне "Добавление пользователя" заполните поля:

- Логин: Введите логин пользователя;
- Пароль: Задайте временный пароль для аутентификации пользователя, в соответствии с заданной парольной политикой в настройке системы;
- Повтор пароля: Введите пароль еще раз;
- Фамилия: Введите фамилию пользователя;
- Имя: Введите имя пользователя;

- Ограничение сеансов: Введите количество активных сеансов для данного пользователя;
- Статус: Выберите в выпадающем списке - "Активный" или "Заблокированный";
- Оповещения: чекбоксы "Всплывающие уведомления о новых инцидентах" и чекбокс "Звуковое оповещение";



- Тип аутентификации: Выберите необходимый метод аутентификации - "Локальный", "LDAP" или "Гибридный";
    - LDAP подключение: Выберите в выпадающем списке домен к которому привязана учетная запись пользователя (при выбранных типах аутентификации - "LDAP" или "Гибридный");



    - Пользователь AD: Введите логин пользователя, прописанный в настройках LDAP (при выбранных типах аутентификации - "LDAP" или "Гибридный");
- Пользователь в группах: Выберите роль или роли пользователя с необходимыми правами;
- Тенанты: Выберите тенант, который будет привязан к пользователю, переместив его из левого поля в правое при помощи стрелок. Он необходим для копирования на ноды правил, симптомов,

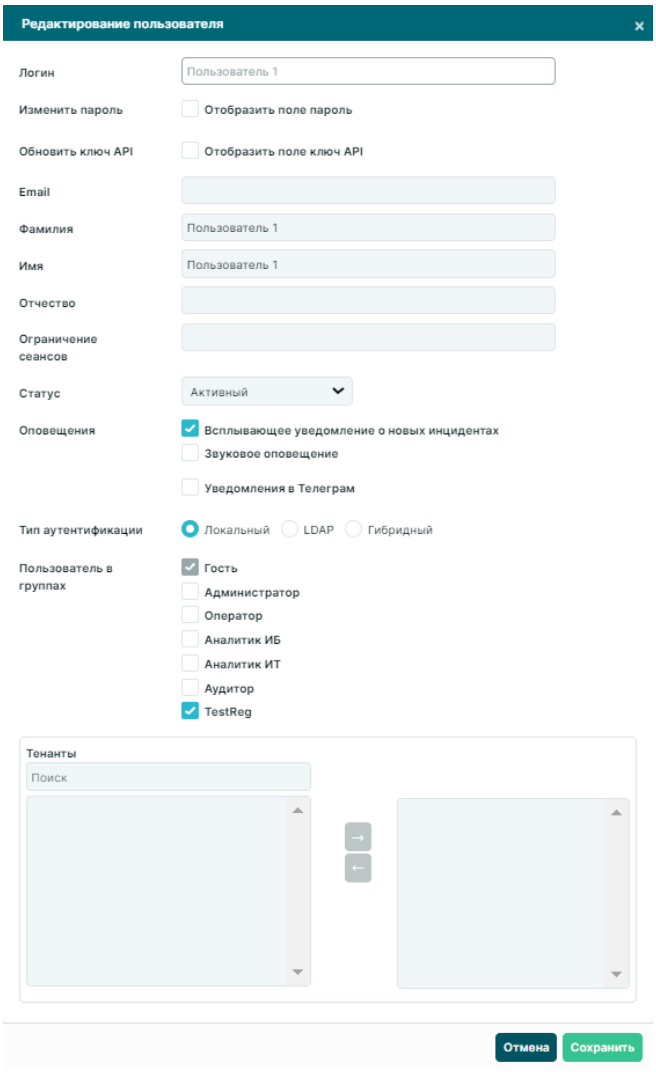
парсеров и мультипоиска по нескольким нодам. Если тенант не указан для пользователя, то данный пользователь будет видеть все созданные тенанты в системе.

- Email, Отчество, Оповещения: Заполняются пользователем.

Нажмите на кнопку "Сохранить".

Редактирование и удаление пользователя

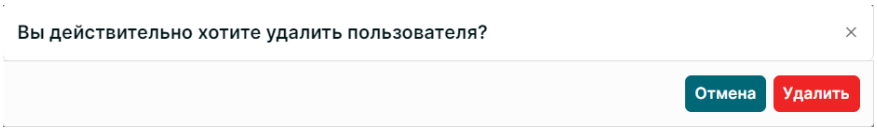
Для редактирования пользователя нажмите на кнопку  .



В отобразившемся окне "Редактирование пользователя" внесите необходимые изменения и нажмите на кнопку "Сохранить".

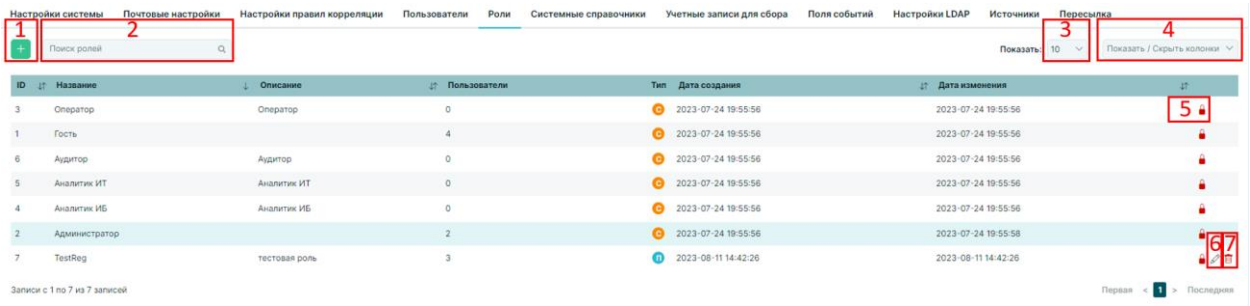
Примечание - Логин пользователя изменить нельзя.

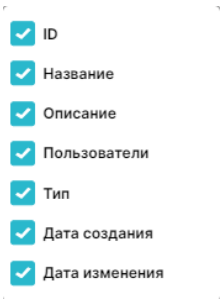
Для удаления пользователя нажмите на кнопку  .



Подтвердите или отмените действие, нажав на соответствующую кнопку.

3.5.6 Вкладка "Роли"



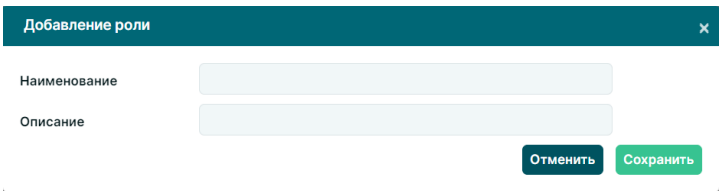
№ Кнопки/элемента управления	Наименование	Описание
1	"Добавить"	Добавление пользовательской роли
2	"Поиск ролей"	Поиск ролей по заданному критерию
3	"Показать"	Выбор в выпадающем списке количества отображаемых на одной странице ролей в списке 
4	"Показать/Скрыть колонки"	Выбор в выпадающем меню отображения/скрытия колонок в списке ролей 

№ Кнопки/элемента управления	Наименование	Описание
5	"Права доступа"	Просмотр назначенных прав доступа выбранной системной роли, просмотр/редактирование назначенных прав доступа выбранной пользовательской роли
6	"Редактировать"	Редактирование выбранной пользовательской роли
7	"Удалить"	Удаление выбранной пользовательской роли

Создание пользовательской роли

Для создания пользовательской роли нажмите на кнопку  .

В отобразившемся окне "Добавление роли" введите наименование роли, ее описание и нажмите на кнопку "Сохранить" .



Созданная роль отобразится в списке ролей и будет доступна для редактирования и удаления.

Назначение прав доступа пользовательской роли

Для назначения прав пользовательской роли нажмите на кнопку  .

В отобразившемся окне "Права доступа" задайте необходимые права для созданной пользовательской роли.

Наименование раздела	**Устанавливаемые права доступа**		
Учетные записи для сбора	☐ Доступ к разделу		
СКУД справочники	☐ Все права	☐ Управление	☐ Просмотр
Все модули	☐ Все права		
Аналитика	☐ Все права ☐ Редактировать ☐ Доступ к уязвимостям	☐ Доступ к baseline ☐ Сохранять	☐ Удалять ☐ Просмотр
Архивы	☐ Все права ☐ Редактировать ☐ Доступ к уязвимостям	☐ Доступ к baseline ☐ Сохранять	☐ Удалять ☐ Просмотр
Ассеты	☐ Доступ к разделу		
Отслеживание аутентификации	☐ Полный доступ		
Категории	☐ Все права ☐ Экспорт ☐ Удаление системные	☐ Удаление ☐ Импорт ☐ Управление системные	☐ Управление ☐ Просмотр
Стандарты	☐ Все права ☐ Импорт	☐ Управление ☐ Просмотр	☐ Экспорт ☐ Управление системные
Взаимосвязи	☐ Доступ к разделу		
Корреляция	☐ Все права ☐ Просмотр	☐ Удаление ☐ Настройки	☐ Загрузка ☐ Управление
Дашборд	☐ Удаление ☐ Загрузка	☐ Управление	☐ Просмотр
Обогащение	☐ Все права ☐ Управление	☐ Удаление	☐ Удаления системные

Наименование раздела	**Устанавливаемые права доступа**		
	☐ Импорт	☐ Управление системные ☐ Просмотр	☐ Экспорт ☐
Агрегация событий	☐ Все права ☐ Редактирование	☐ Создание ☐ Просмотр	☐ Удаление ☐ Импорт
Фильтрация событий	☐ Все ☐ Редактирование	☐ Создание ☐ Импорт	☐ Удаление ☐ Просмотр
События	☐ Все права ☐ Настройки	☐ Управление ☐ Загрузка	☐ Просмотр
Фиды	☐ Доступ к разделу		
Поля событий	☐ Доступ к разделу		
Инциденты	☐ Все права ☐ Свои инциденты	☐ Все инциденты	☐ Удаление
Интеграция	☐ Доступ к разделу		
Лицензия	☐ Доступ к разделу		
Списки	☐ Все права ☐ Управление ☐ Импорт	☐ Удаление ☐ Управление системные ☐ Просмотр	☐ Удаление системные ☐ Экспорт
Multitenancy	☐ Все права ☐ Передача парсеров на ноды ☐ Просмотр информации по нодам	☐ Управление нодами ☐ Передача симптомов на ноды	☐ Передача правил корреляции на ноды ☐ Выбор нод
Уведомления	☐ Все права		
Парсеры	☐ Все права ☐ Просмотр	☐ Удаление	☐ Редактирование

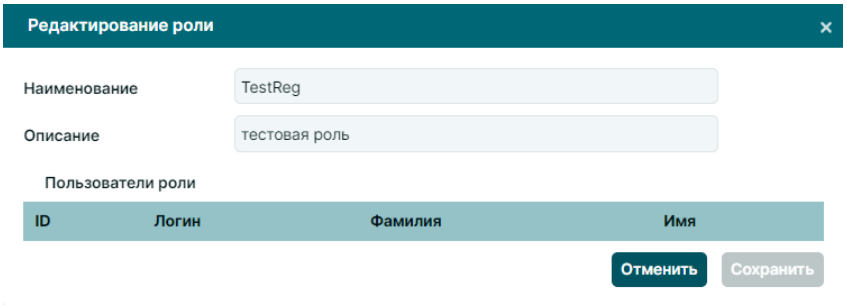
Наименование раздела	**Устанавливаемые права доступа**		
Настройки системы	☐ Все права		
Справочники	☐ Все права ☐ Экспорт	☐ Удаление ☐ Импорт	☐ Управление ☐ Просмотр
Отчеты	☐ Все права ☐ Сохранять	☐ Удалять ☐ Загружать	☐ Редактировать ☐ Просмотр
Ограничение ресурсов	☐ Черный список	☐ Белый список	
Роли	☐ Все права ☐ Просмотр	☐ Удаление	☐ Управление
Источники	☐ Все права	☐ Просмотр	
Симптомы	☐ Все права ☐ Экспорт ☐ Удаление системные	☐ Удаление ☐ Импорт ☐ Управление системные	☐ Управление ☐ Просмотр
Система	☐ Все права		
Пользовательские источники	☐ Все права ☐ Просмотр	☐ Удаление	☐ Редактирование
Пользователи	☐ Все права ☐ Просмотр	☐ Удаление	☐ Управление

Редактирование и удаление пользовательской роли

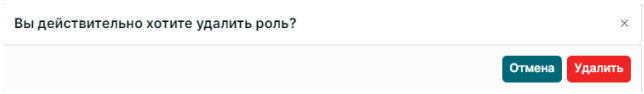
Внимание! Функции редактирования и удаления доступны только для пользовательских ролей.

Для редактирования пользовательской роли нажмите на кнопку  .

В отобразившемся окне "Редактирование роли" введите новое наименование и описание роли и нажмите на кнопку "Сохранить".

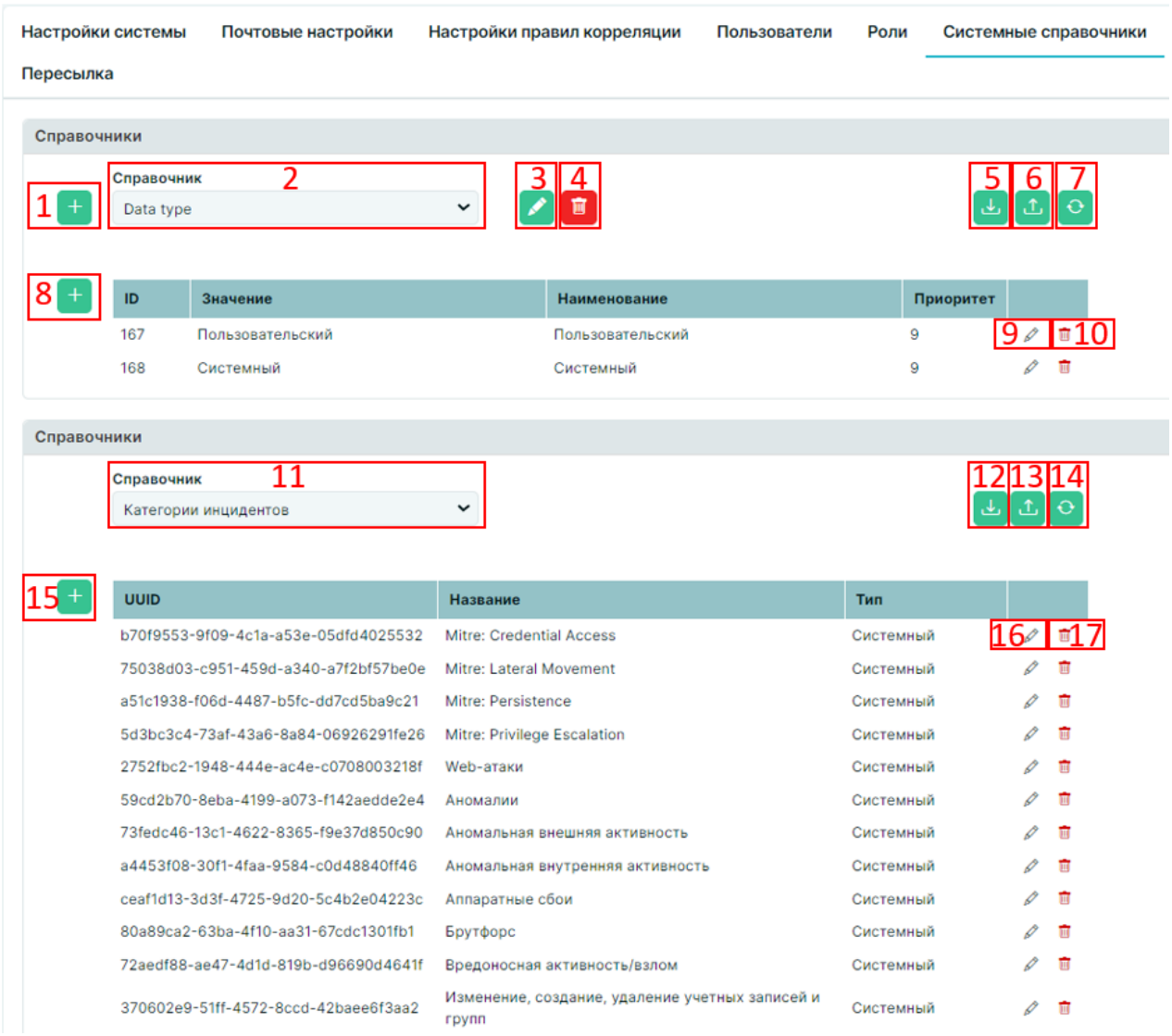


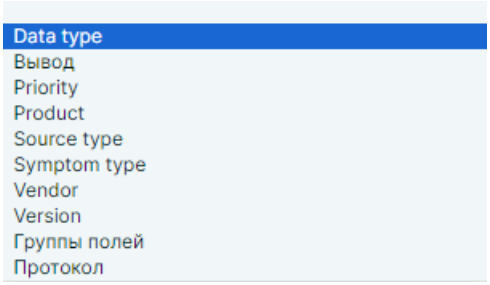
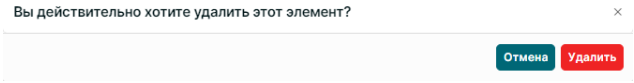
Для удаления пользовательской роли нажмите на кнопку .



В отобразившемся окне подтвердите или отмените удаление нажав на соответствующую кнопку.

3.5.7 Вкладка "Системные справочники"

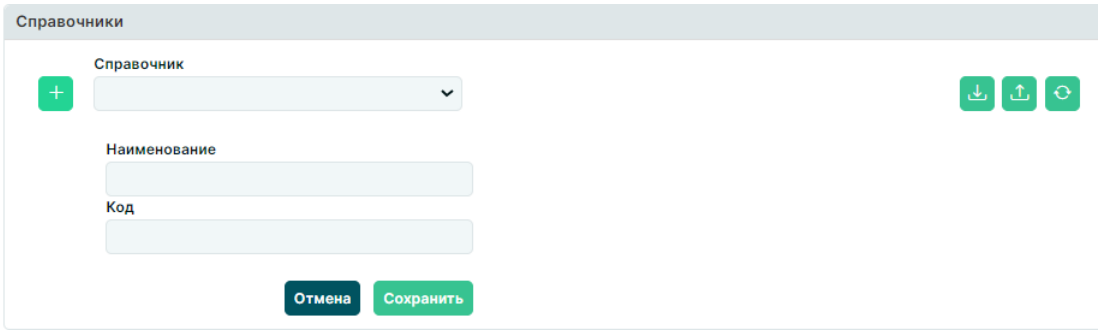


№ Кнопки/Поля	Наименование	Описание
1	"Добавление нового справочника"	-
2	"Справочник"	Выбор справочника в выпадающем списке 
3	"Редактирование справочника"	-
4	"Удаление справочника"	-
5	"Экспорт справочников"	-
6	"Импорт справочников"	-
7	"Обновить"	Обновление страницы
8	"Добавление нового элемента справочника"	-
9	"Редактировать"	Редактирование элемента справочника
10	"Удалить"	Удаление элемента справочника 
11	"Справочник"	Выбор справочника "Категории инцидентов"

№ Кнопки/Поля	Наименование	Описание
12	"Экспорт справочников"	-
13	"Импорт справочников"	-
14	"Обновить"	Обновление страницы
15	"Добавление нового элемента справочника"	-
16	"Редактировать"	Редактирование элемента справочника

Работа со справочниками

Для добавления/редактирования справочника нажмите на кнопку  .



Для редактирования справочника:

- Выберите справочник в выпадающем списке поля "Справочник" (см. поле "**2**");
    - Data type - справочник по типу данных (системные/пользовательские);
    - Вывод - справочник
    - Priority - справочник приоритетов;
    - Product - справочник имеющихся продуктов;
    - Source type - справочник типов событий;
    - Symptom type - справочник типов симптомов;

- Vendor - справочник имеющихся вендоров;
- Version - справочник имеющихся версий;
- Группы полей - справочник группы полей (Источник/Назначение/Геоданные источника/Геоданные назначения/Симптомы/Данные хоста/Служебные). Отображается при подробном развертывании просмотра событий.
- Протокол - справочник имеющихся протоколов.

- Введите новое наименование и Code в соответствующих полях и нажмите на кнопку "Сохранить".

Для добавления нового справочника:

- Введите наименование справочника и Code в соответствующих полях и нажмите на кнопку "Сохранить".

Для редактирования справочника нажмите на кнопку .

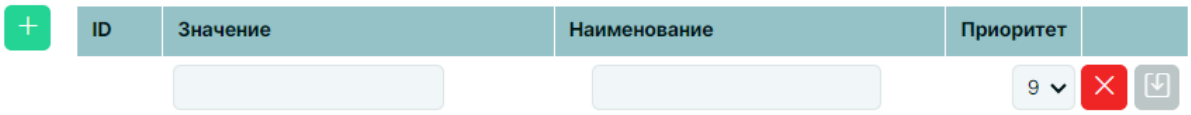
Для удаления справочника нажмите на кнопку .

Для экспорта справочника нажмите на кнопку .

Для импорта справочника нажмите на кнопку .

Работа с элементами справочника

Для добавления нового элемента справочника нажмите на кнопку .



Введите значение, наименование, выберите приоритет в выпадающем списке - от 0 до 9 и нажмите на кнопку "Сохранить".

Для редактирования элемента справочника нажмите на кнопку .

Для удаления элемента справочника нажмите на кнопку .

Работа со справочником "Категории инцидентов"

Для добавления нового элемента справочника нажмите на кнопку .

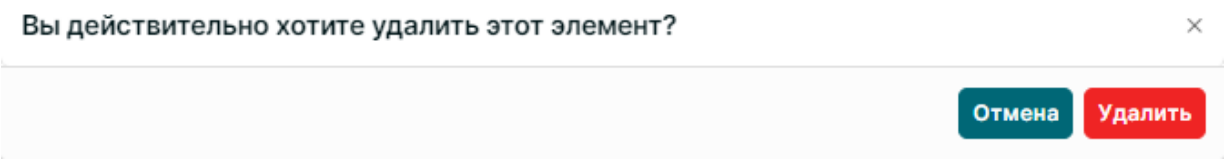
Введите наименование элемента справочника.

- сохранить новый элемент справочника;

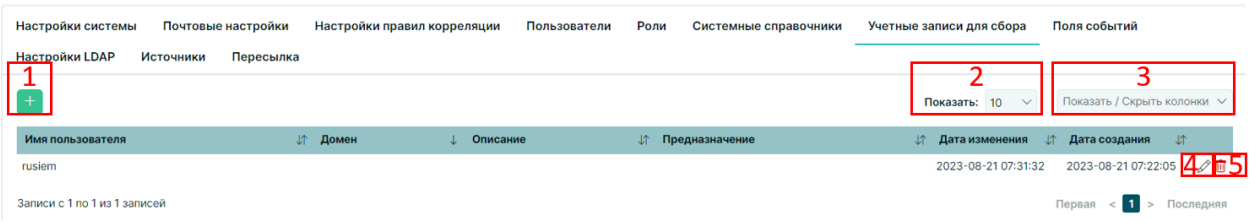
- отменить добавление нового элемента справочника.

Для редактирования элемента справочника нажмите на кнопку .

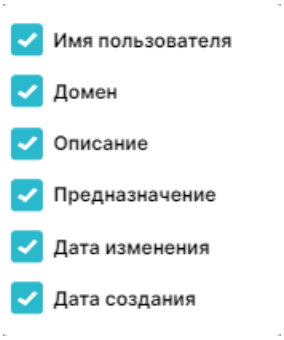
Для удаления элемента справочника нажмите на кнопку . После нажатия появится окно подтверждения удаления элемента справочника.



3.5.8 Вкладка "Учетные записи для сбора"

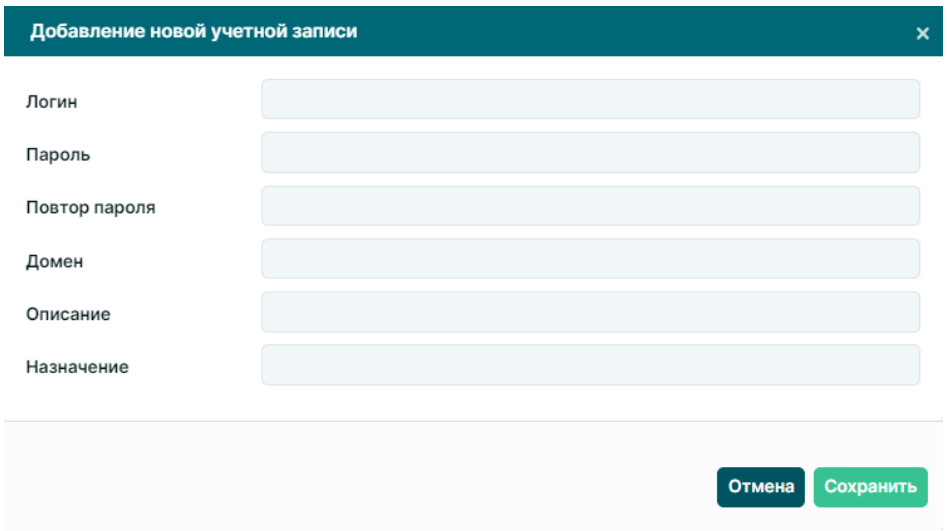


№ Кнопки/элемента управления	Наименование	Описание
1	"Добавить"	Добавление новой учетной записи
2	"Показать"	Выбор в выпадающем списке количества отображаемых на одной странице учетных записей в списке 

3	"Показать/Скрыть колонки"	Выбор в выпадающем меню отображаения/скрытия колонок в списке учетных записей 
4	"Редактировать"	Редактирование выбранной учетной записи
5	"Удалить"	Удаление выбранной учетной записи

Добавление учетной записи

Для добавления учетной записи нажмите на кнопку  .



В отобразившемся окне "Добавление новой учетной записи" введите требуемые данные создаваемой учетной записи:

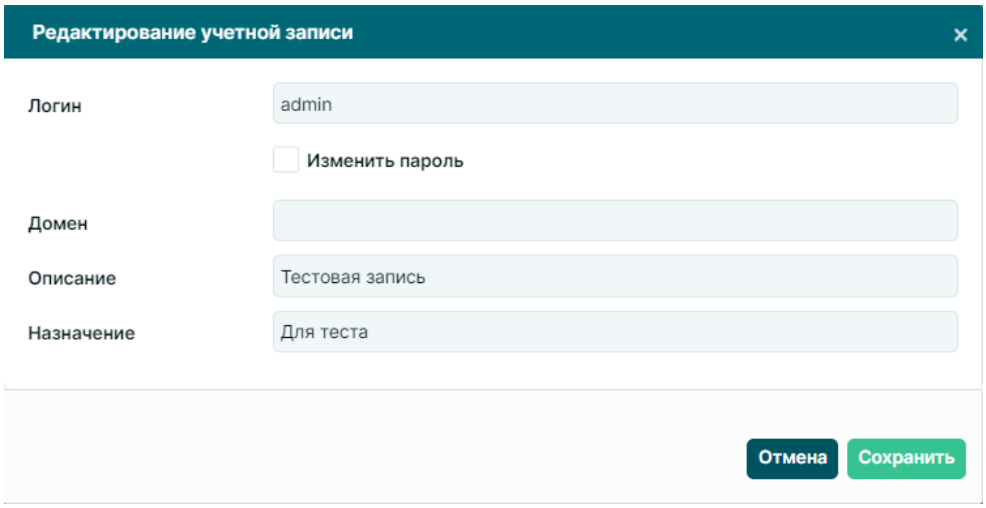
- Логин;
- Пароль
- Повтор пароля;

- Домен;
- Описание;
- Назначение.

Нажмите на кнопку "Сохранить".

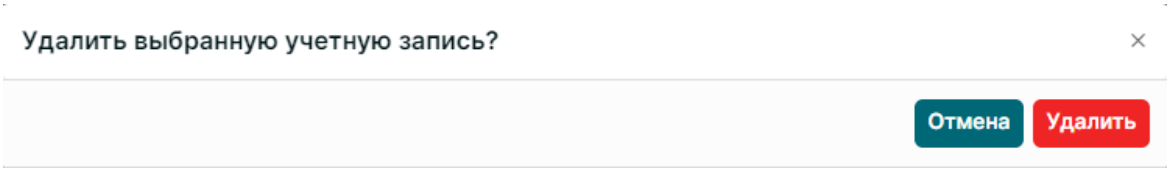
Редактирование и удаление учетной записи

Для редактирования учетной записи нажмите на кнопку .



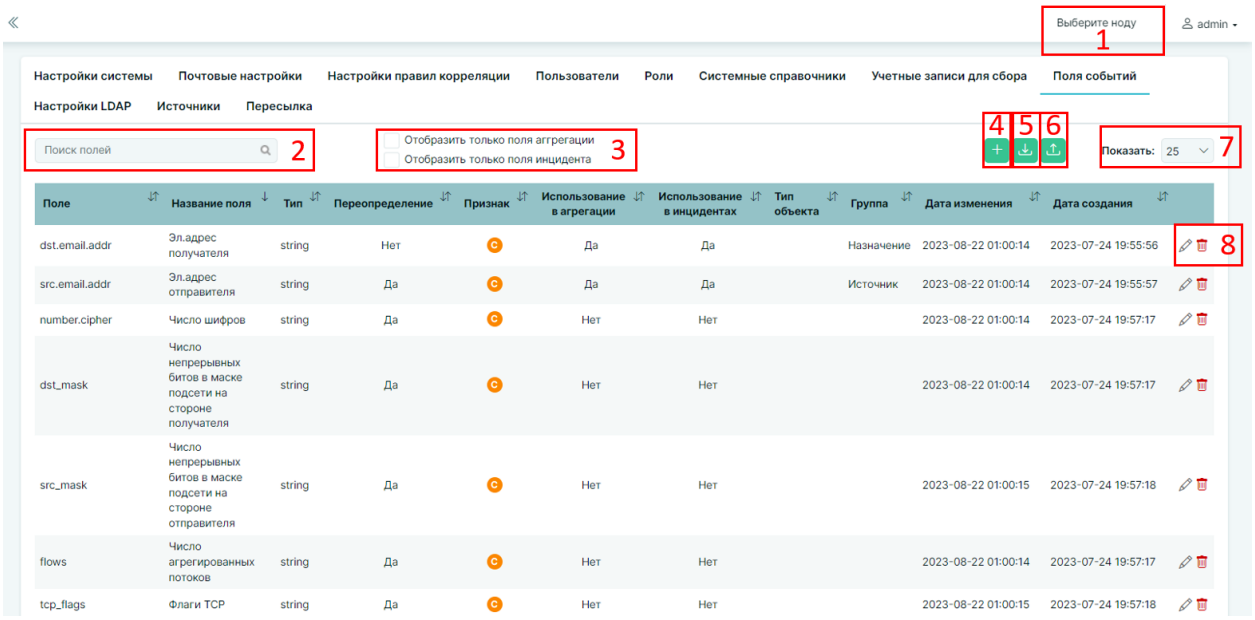
В отобразившемся окне "Редактирование учетной записи" измените требуемые данные учетной записи и нажмите на кнопку "Сохранить".

Для удаления учетной записи нажмите на кнопку .

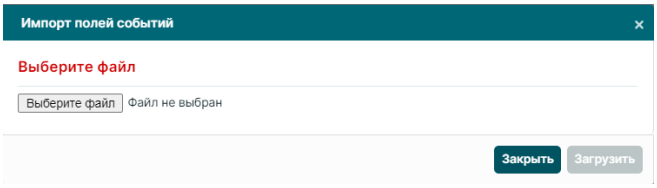
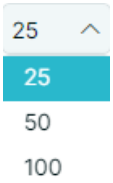


Подтвердите или отмените действие нажав на соответствующую кнопку.

3.5.9 Вкладка "Поля событий"

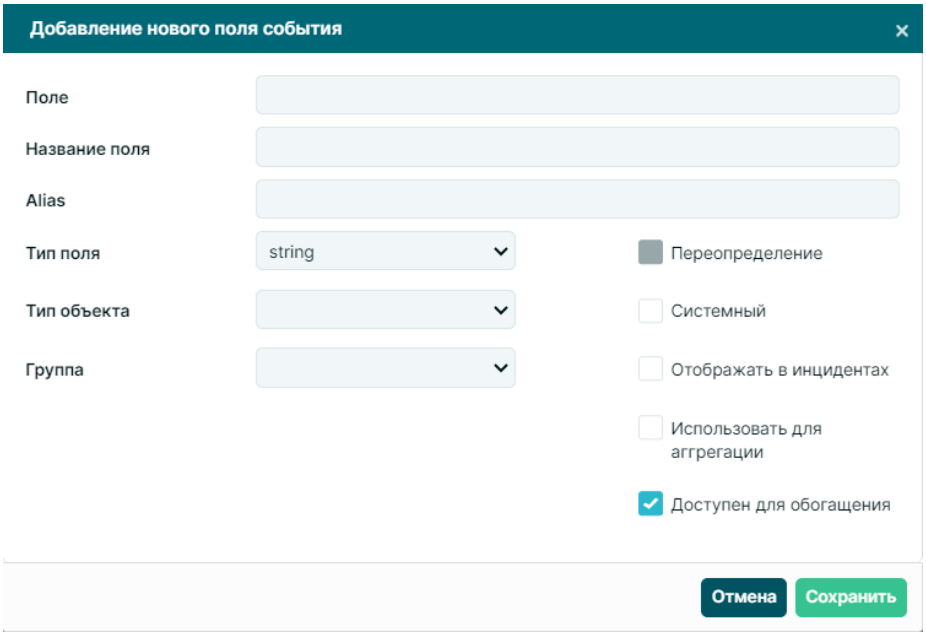


№ Кнопки/Поля/ Элемента управления	Наименование	Описание
1	"Выберите ноду"	Поиск и выбор ноды
2	"Поиск полей"	Поиск полей событий по введенному критерию
3	"Отобразить только поля"	Включение/отключение функции отображения полей событий: ☑ Отобразить только поля агрегации или ☑ Отобразить только поля инцидента При отключенной функции отображаются все поля событий
4	"Добавить"	Добавление нового поля события
5	"Экспорт"	Экспорт полей в JSON-формате Экспорт системных полей Экспорт пользовательских полей

6	"Импорт"	Импорт полей событий 
7	"Показать"	Выбор в выпадающем списке количества отображаемых на одной странице полей событий в списке 
8	"Элементы управления"	- Редактирование выбранного поля события
		- "Удаление". Удаление с обязательным подтверждением действий (Удалить выбранный автозагрузчик? Удалить/Отмена)

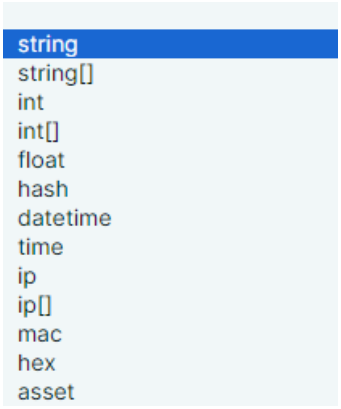
Добавление нового поля события

Для добавления нового поля события нажмите на кнопку .

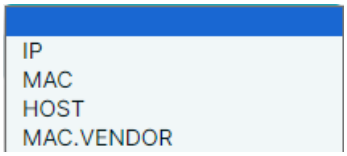


В отобразившемся окне "Добавление нового поля события":

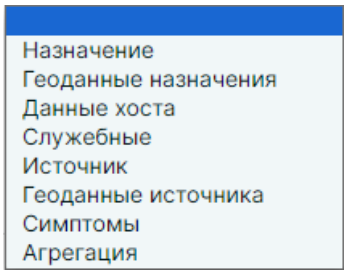
- Введите обозначение поля события (например - src.ip), наименование поля, краткое имя поля (Alias);
- Выберите тип поля из выпадающего списка;



- Выберите тип объекта из выпадающего списка;



- Выберите группу в выпадающем списке;



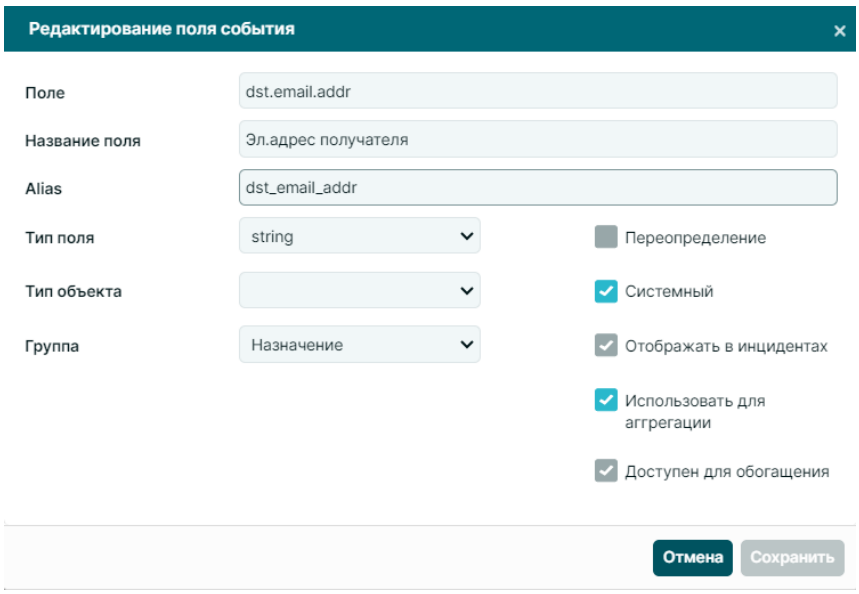
- Включите/отключите функционал:
  - ☐ Системный
  - ☐ Отображать в инцидентах
  - ☐ Использовать для агрегации
  - ☐ Доступен для обогащения

При установке галочки ☑ "Доступен для обогащения" становится возможным выбор этих полей для заполнения в поле "Симптоматика".

- Нажмите на кнопку "Сохранить".

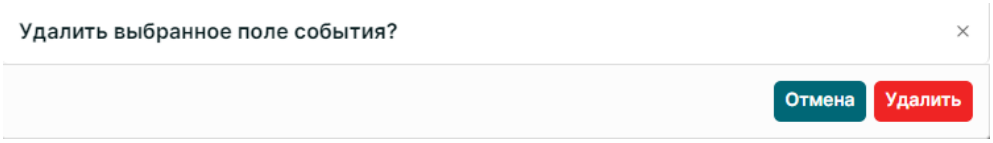
Редактирование и удаление поля события

Для редактирования выбранного поля события нажмите на кнопку  .



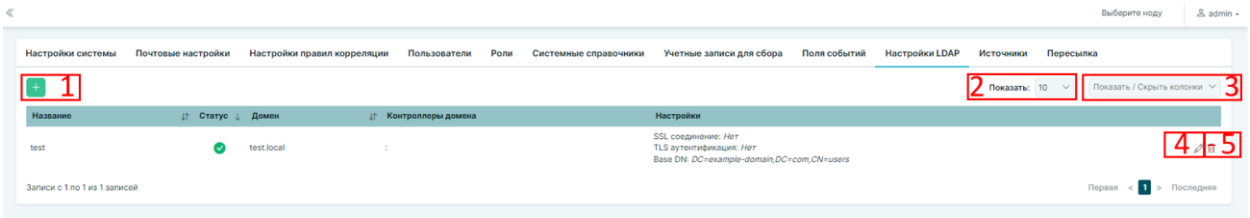
Внесите необходимые изменения и нажмите на кнопку "Сохранить"

Для удаления выбранного поля события нажмите на кнопку .

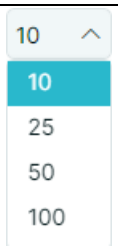
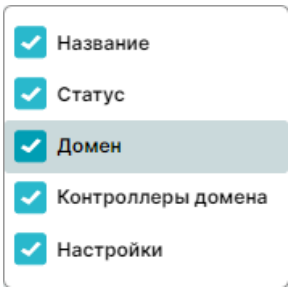


Подтвердите или отмените действие нажатием на соответствующую кнопку.

3.5.10 Вкладка "Настройки LDAP"



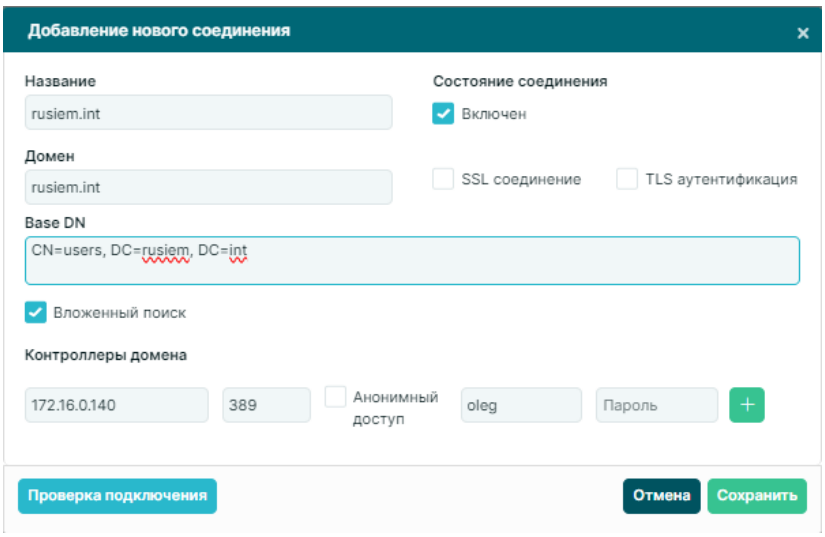
№ Кнопки/ элемента управления	Наименование	Описание
1	"Добавить"	Добавление нового соединения
2	"Показать"	Выбор в выпадающем списке количества отображаемых на одной странице подключений в списке

№ Кнопки/ элемента управления	Наименование	Описание
		
3	"Показать/Скрыть колонки"	Выбор в выпадающем меню отображения/скрытия колонок в списке подключений 
4	"Редактировать"	Редактирование выбранного подключения
5	"Удалить"	Удаление выбранного подключения

Добавление нового соединения

Для добавления нового соединения:

- Нажмите на кнопку  ;
- В отобразившемся окне "Добавление нового подключения" создайте подключение к LDAP как на рисунке ниже, устанавливая параметры для подключения, типичные для вашей инфраструктуры. В качестве поля «контроллер домена» можно указывать fqdn если с rusiem хост резолвится успешно;

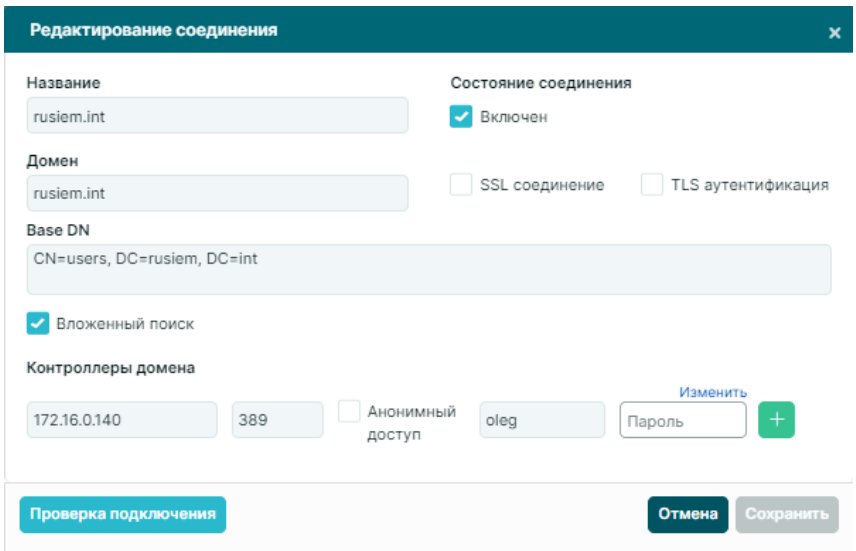


- Нажмите на кнопку «Проверить подключение» и убедитесь, что подключение прошло успешно;
- Нажмите на кнопку "Сохранить".

Редактирование соединения

Для редактирования соединения:

- Нажмите на кнопку  напротив выбранного соединения;
- В отобразившемся окне "Редактирование соединения" отредактируйте подключение к LDAP, устанавливая необходимые для подключения параметры;



- Нажмите на кнопку «Проверить подключение» и убедитесь, что подключение прошло успешно.
- При неудачном подключении на экране появиться сообщение «Ошибка подключения».

Причинами неудачного подключения могут быть:

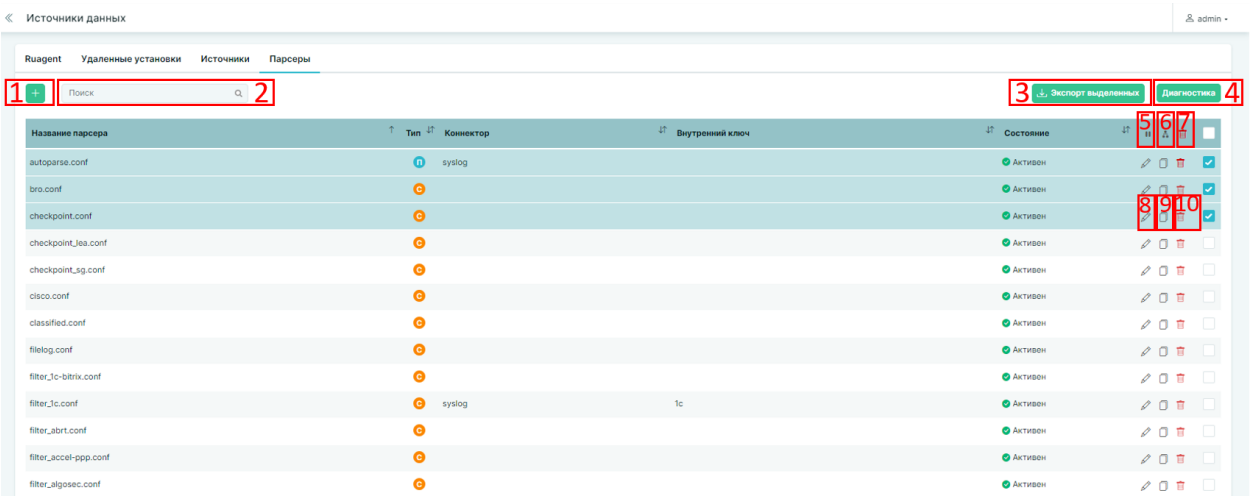
- фильтрация iptables на хосте rusiem (изменить в modules_user.dat параметр обновления файервола fw_update=1, запустить update_hourly.sh);
- некорректно выбранные параметры для подключения;
- некорректный логин/пользователь.
- Нажмите на кнопку "Сохранить".

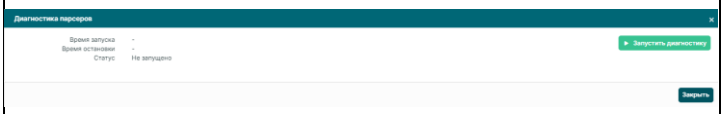
Структура настроек

Название поля	Описание	Значения
Название	Индивидуальное название	Мое подключение
Домен	Домен, к которому нужно присоеденить	mydomain.local
Base DN	База для поиска	DC=example-domain,DC=com,CN=users
Контроллер домена Хост	Hostname или IP контроллера домена	generalAD или 192.168.10.10
Контроллер домена Порт	Порт для подключения по LDAP (Если пусто используются стандартные порты для LDAP или LDAPS)	389 или 636 или пусто
Логин	Логин пользователя домена (Без домена!)	a.antonov
Пароль	Пароль пользователя в домене	Pass1234

3.5.11 "Парсеры"

Перейти в раздел «Мониторинг и управление» - «Источники данных» на вкладку «Парсеры».

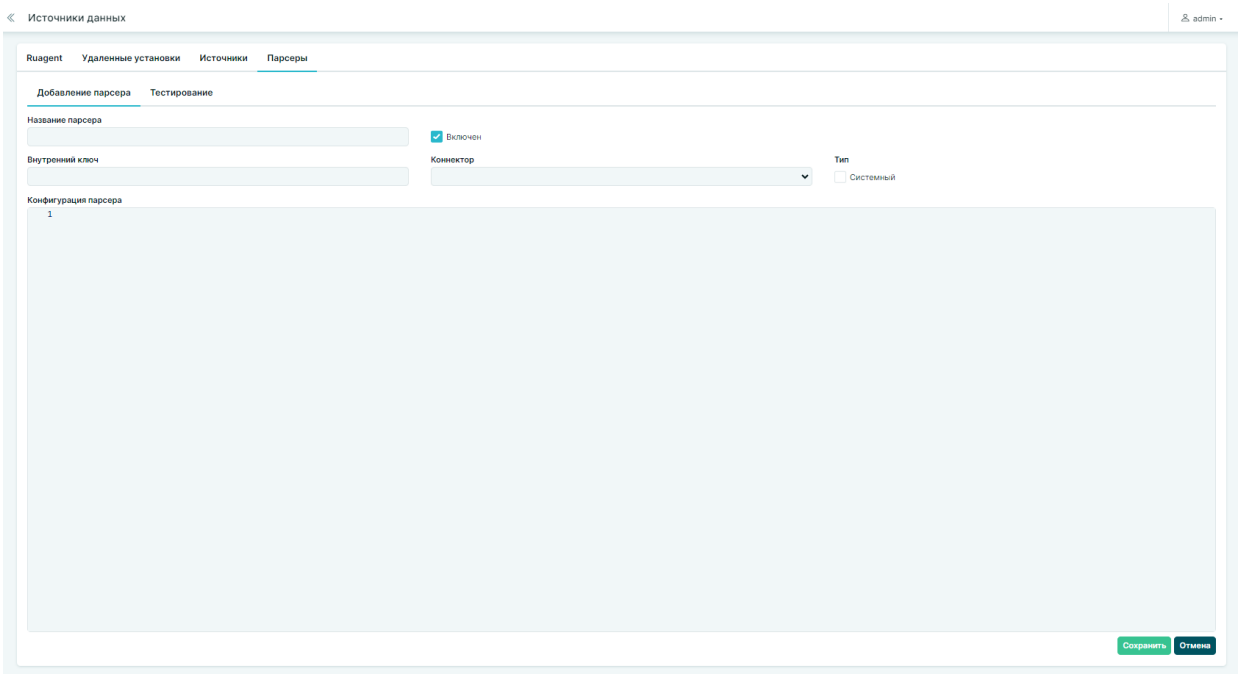


№ Кнопки/ Поля	Наименование	Описание
1	"Добавить"	Добавление/редактирование парсера
2	"Поиск"	Поиск парсера по введенному критерию
3	"Экспорт выделенных"	Экспорт выделенных парсеров
4	"Диагностика"	Диагностика парсеров 
5	"Управление статусом парсеров"	Управление статусом выделенных парсеров:  - Активировать выделенные  - Деактивировать выделенные
6	"Копировать на ноды"	Копирование выделенных парсеров на выбранные ноды
7	"Удалить выделенные"	Удаление выделенных парсеров
8	"Редактировать"	Редактирование выбранного пользовательского парсера Включение/отключение выбранного системного парсера

9	"Создать копию"	Копирование конфигурации выбранного парсера
10	"Удалить"	Удаление выбранного пользовательского парсера

Добавление/редактирование парсера

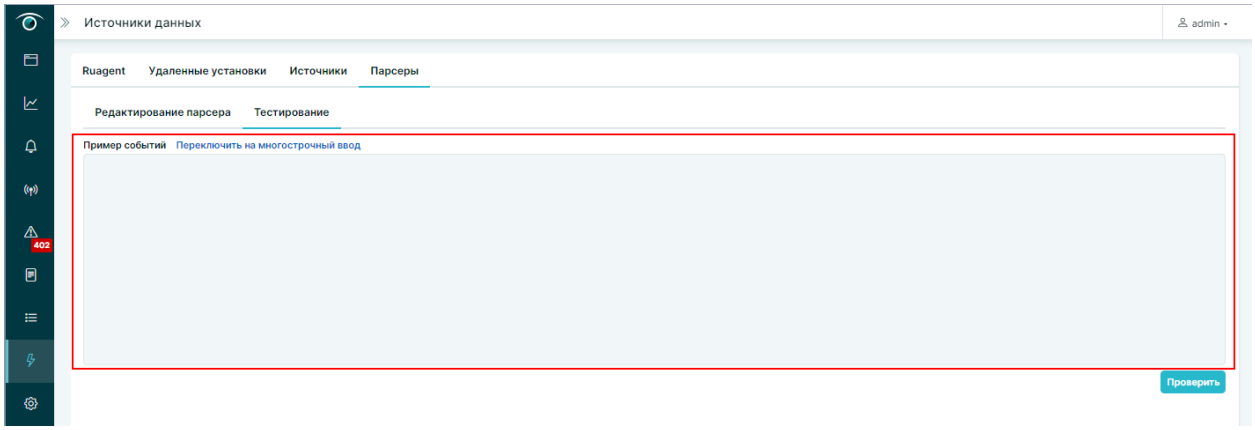
Для добавления парсера нажмите на кнопку  .



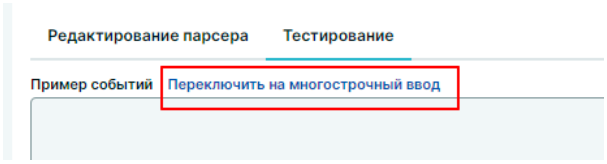
В отобразившемся окне:

- в поле **Название парсера** - введите название;
- в поле **Внутренний ключ** – впишите внутренний ключ, по которому осуществляется поиск данного парсера;
- в поле **Коннектор** - выберите из выпадающего списка коннектор (syslog или ruagent);
- чекбокс **Системный**: включен - системный тип парсера, выключен - пользовательский тип парсера;
- чекбокс **Включен** - выберите включение или выключение парсера;
- в поле **Конфигурация парсера** - введите конфигурационное описание парсера.

Для проверки работы парсера перейдите на вкладку «Тестирование» В область «Пример события» вставьте событие и нажмите на кнопку "Проверить".



Для переключения ввода многострочного события, нажать «переключить на многострочный ввод»



Копирование парсера

Для создания нового пользовательского парсера на основе конфигурации другого парсера выберите необходимый и нажмите на кнопку .

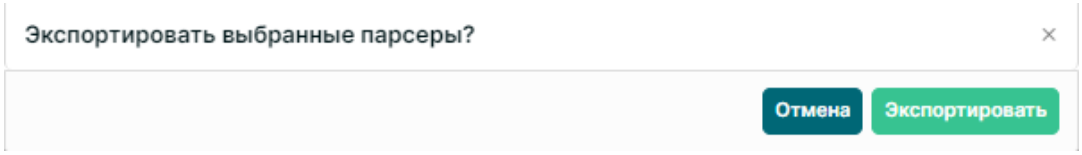
Отобразится окно "Добавление/редактирование парсера" с выбранным парсером для редактирования в названии которого будет стоять постфикс - копия.

Введите необходимые изменения в пользовательский парсер и нажмите на кнопку "Сохранить".

Работа с парсерами

Для экспорта парсеров:

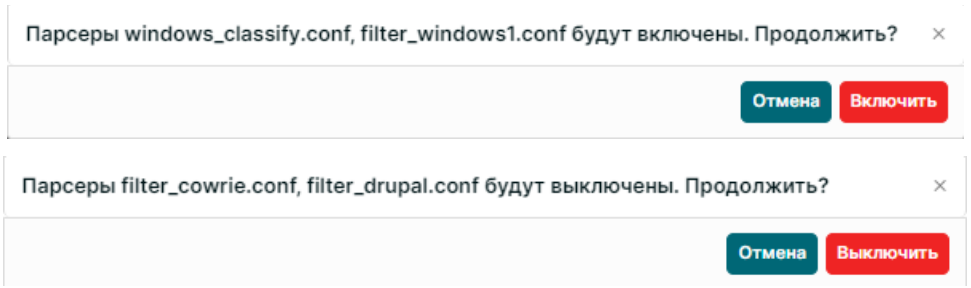
- Выделите необходимые парсеры и нажмите на кнопку "Экспорт выделенных";



- Нажмите кнопку "Экспортировать", выбранные парсеры сохраняться в директории загрузки (download) в формате - SelectedParsers_гггг-мм-дд.json.

Для активации/деактивации парсеров:

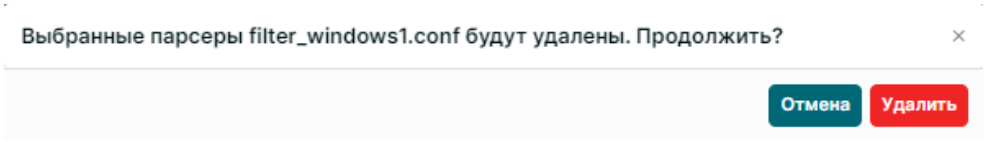
- Выделите необходимые парсеры и нажмите на кнопку ▶ или ⏸;



- Подтвердите выбор действия, нажав на соответствующую кнопку.

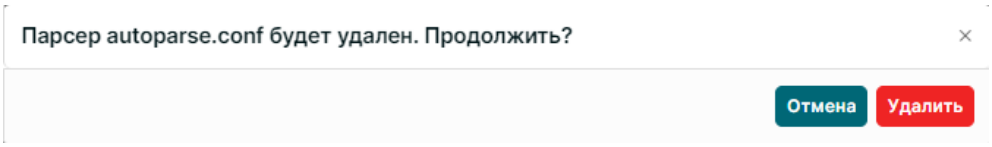
Для удаления парсеров:

- Выделите необходимые парсеры и нажмите на кнопку 🗑



или

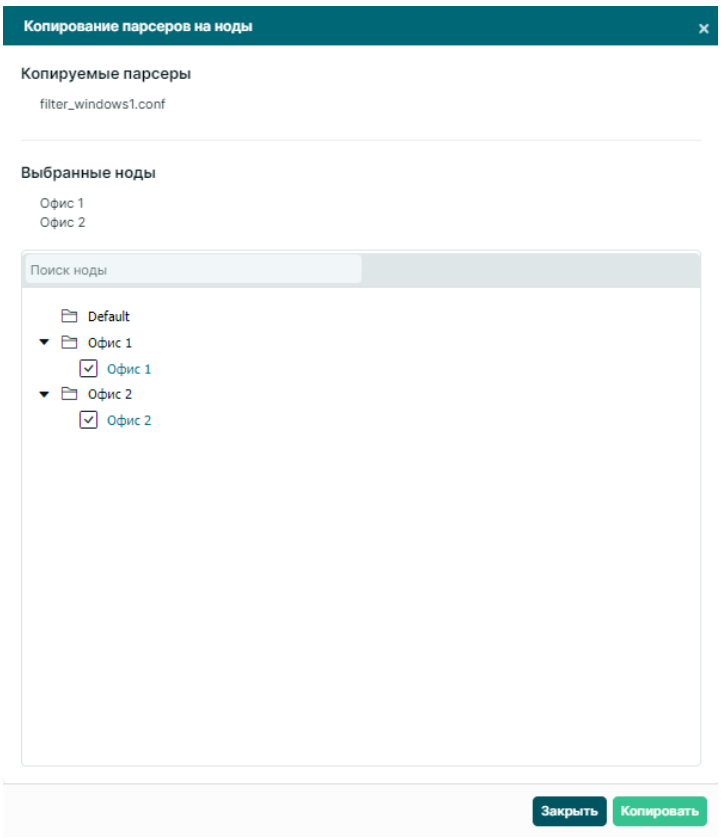
- Нажмите на кнопку 🗑 напротив парсера, который хотите удалить



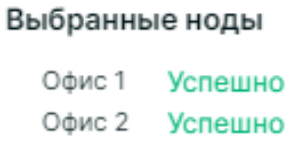
- Подтвердите выбор действия нажав на соответствующую кнопку.

Копирование парсеров на ноды

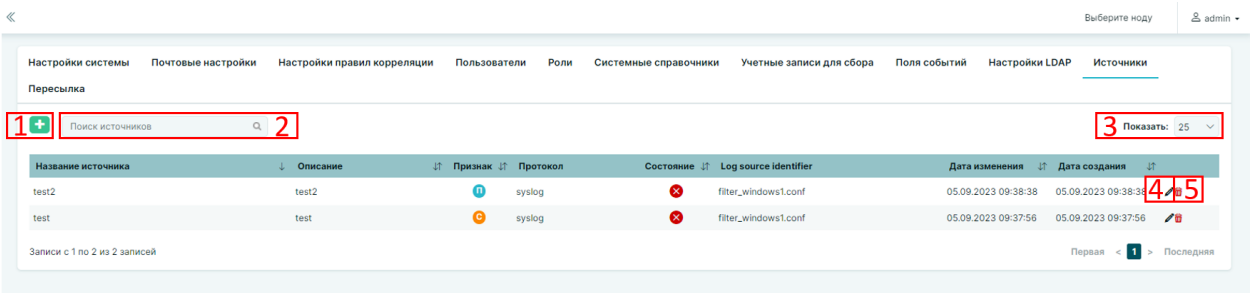
Выделите необходимые пользовательские парсеры и нажмите на кнопку . Откроется окно, показанное ниже:



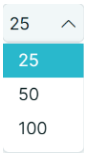
В окне "Копирование парсеров на ноды" выберите необходимые ноды и нажмите на кнопку "Копировать". В поле "Выбранные ноды" отобразится статус копирования.



3.5.12 Вкладка "Источники"

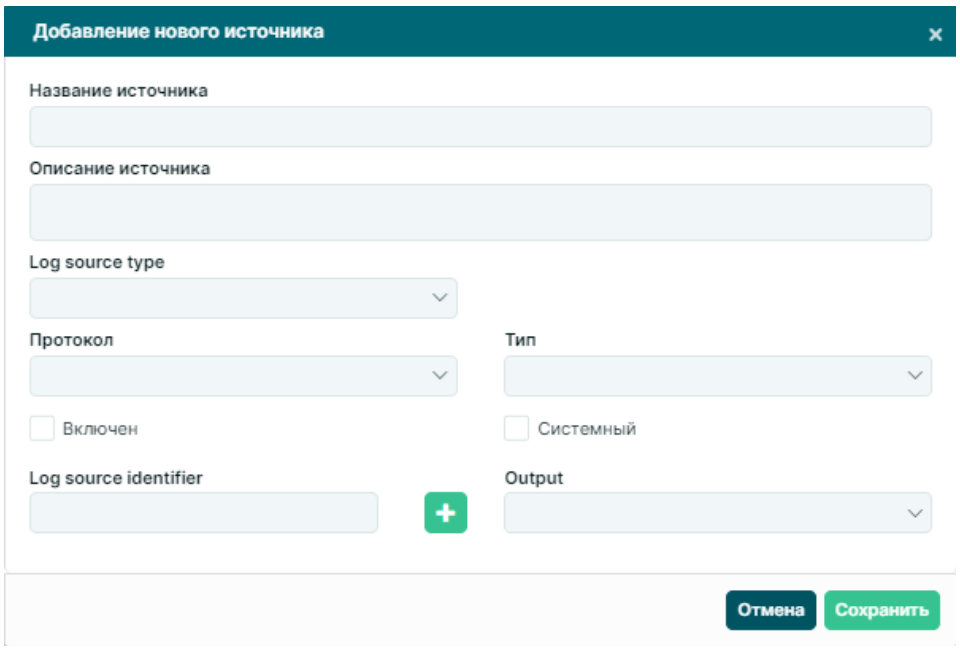


№ Кнопки/Поля/ Элемента управления	Наименование	Описание
1	"Добавить"	Добавление нового источника

2	"Поиск источников"	Поиск источников по введенному критерию
3	"Показать"	Выбор в выпадающем списке количества отображаемых на одной странице источников в списке 
4	"Редактировать"	Редактирование выбранного источника
5	"Удалить"	Удаление выбранного источника

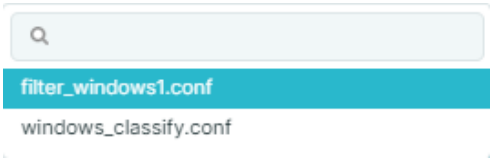
Добавление нового источника

Для добавления нового источника нажмите на кнопку  .

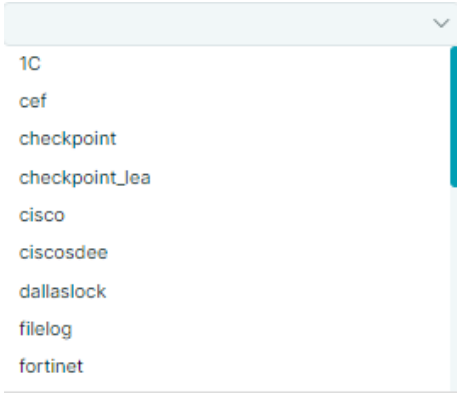


В отобразившемся окне "Добавление нового источника":

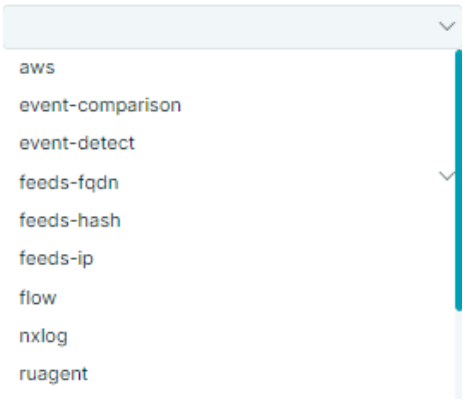
- в поле **Название источника** - введите название;
- в поле **Описание источника** - введите описание;
- в поле **Log source type** - выберите в выпадающем списке тип источника журнала



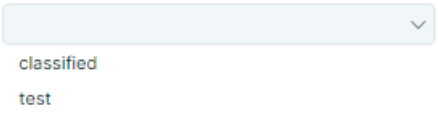
- в поле **Протокол** - выберите в выпадающем списке тип протокола данных



- в поле **Тип** - выберите в выпадающем списке тип данных



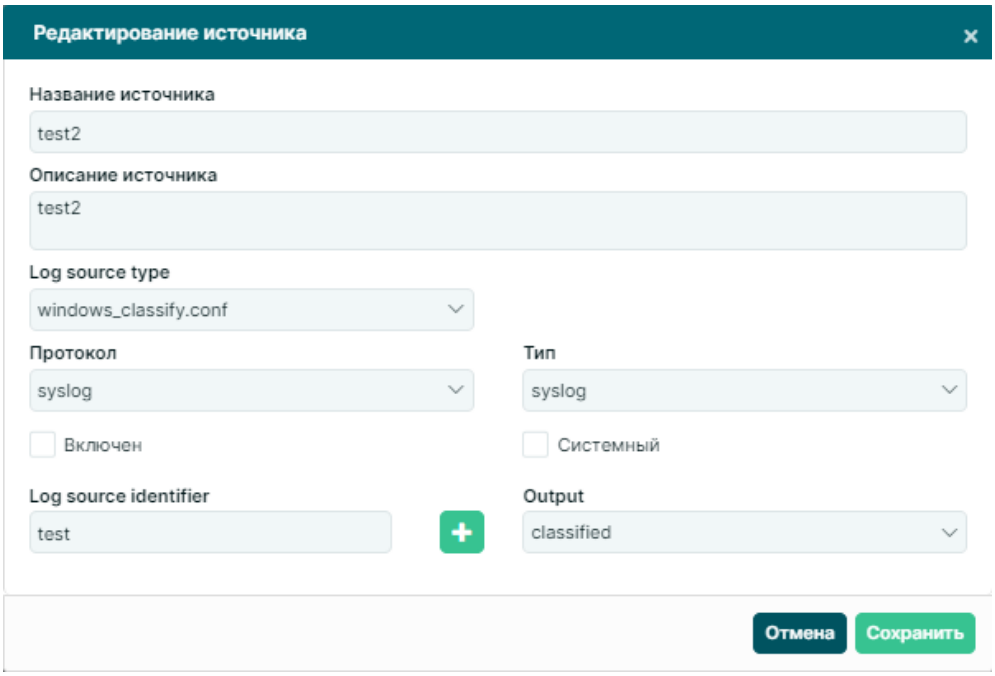
- чекбокс **Включен** - выберите включение/отключение источника;
- чекбокс **Системный** - выберите системный/пользовательский источник;
- в поле **Log source identifier** - введите идентификатор источника журнала, для добавления дополнительного идентификатора нажмите на кнопку  и введите дополнительный идентификатор источника 

- в поле **Output** - выберите в выпадающем списке тип выходных данных 

.

Редактирование источника

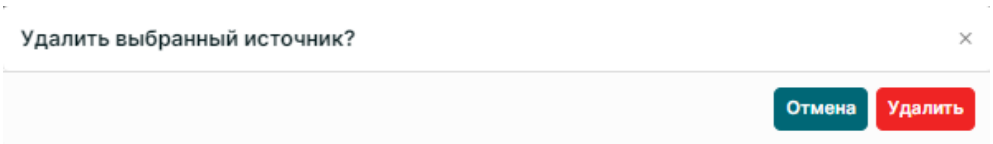
Для редактирования источника нажмите на кнопку .



В отобразившемся окне "Редактирование источника" внесите необходимые изменения и нажмите на кнопку "Сохранить".

Удаление источника

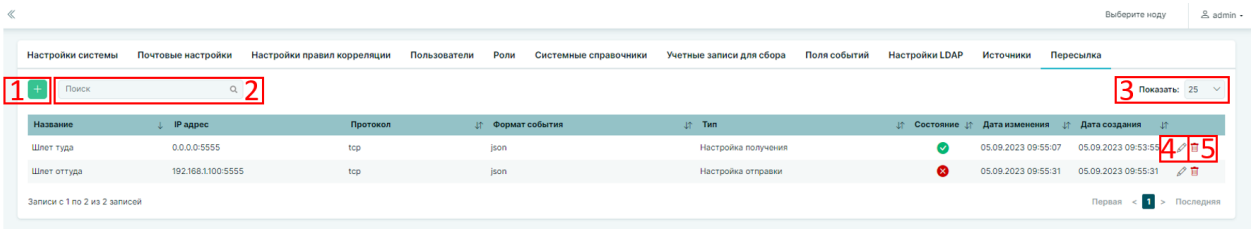
Для удаления источника нажмите на кнопку .

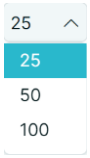


Подтвердите удаление нажатием на кнопку "Удалить".

3.5.13 Вкладка "Пересылка"

Используется при пересылки событий с RvSIEM на RuSIEM.



№ Кнопки/Поля/ Элемента управления	Наименование	Описание
1	"Добавить"	Добавление новой настройки пересылки
2	"Поиск"	Поиск созданных настроек пересылки по введенному критерию
3	"Показать"	Выбор в выпадающем списке количества отображаемых на одной странице созданных настроек пересылки в списке 
4	"Редактировать"	Редактирование выбранной настройки пересылки
5	"Удалить"	Удаление выбранной настройки пересылки

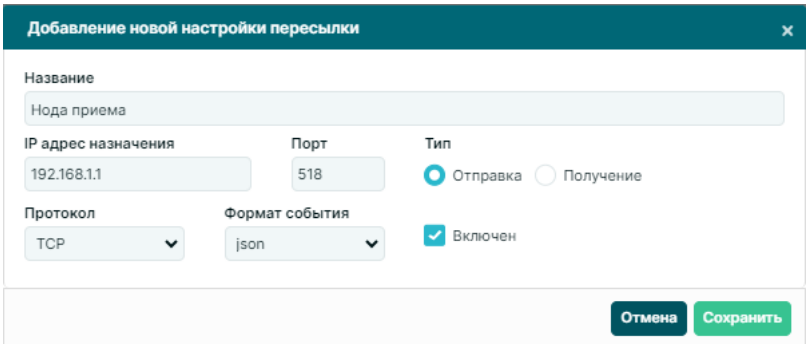
Добавление новой настройки пересылки

Нажмите на кнопку  .

На отправляющей ноде:

Укажите следующие параметры:

- Тип: Отправка;
- IP адрес принимающей ноды, порт и название;
- Активируйте правило ( Включен).



Порт необходимо указывать не используемый SIEM для приема событий. К примеру 5018

- Внесите изменения в настройки межсетевого экрана в файле /etc/init.d/firewall.sh добавьте строчки:

  iptables -A OUTPUT -p tcp -s $EXTIP --dport 5018 -j ACCEPT

  iptables -A INPUT -p tcp -d $EXTIP --sport 5018 -j ACCEPT

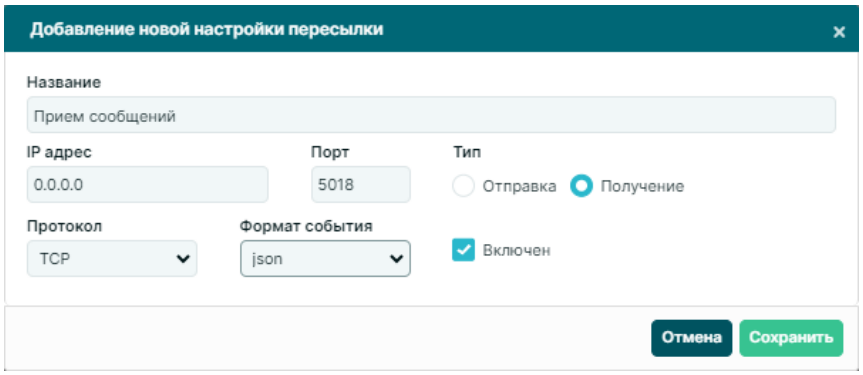
- Примените настройки командой:

  /etc/init.d/firewall.sh start

На принимающей ноде:

Укажите следующие параметры:

- Тип: Получение;
- IP адрес интерфейса, если необходимо слушать на всех доступных интерфейсах, укажите "0.0.0.0";
- Порт приема сообщений;
- Активируйте правило (Включен).



- Внесите изменения в настройки межсетевого экрана в файле /etc/init.d/firewall.sh добавьте строчки:

  iptables -A INPUT -p tcp -d $EXTIP --dport 5018 -j ACCEPT

  iptables -A OUTPUT -p tcp -s $EXTIP --sport 5018 -j ACCEPT

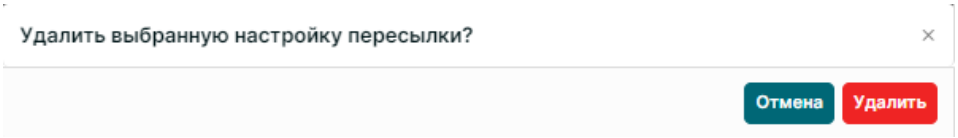
- Примените настройки командой:

  /etc/init.d/firewall.sh start

Редактирование и удаление настройки пересылки

Для редактирования настройки пересылки нажмите на кнопку . Внесите необходимые изменения и нажмите на кнопку "Сохранить".

Для удаления настройки пересылки нажмите на кнопку .



Подтвердите или отмените действие, нажав на соответствующую кнопку.

3.6 Раздел Multitenancy

3.6.1 Описание multitenancy

Мультитенантность(Мультиарендность) - особенность архитектуры ПО, где единый экземпляр приложения обслуживает множество организаций-клиентов.

Простыми словами мультитенантность - это возможность изолированно обслуживать пользователей из разных организаций в рамках одного сервиса (одной инсталляции или развертывания). Основным здесь является соблюдение изолированности клиентов друг от друга. Также это возможность централизованно управлять всеми компонентами такой мультиарендной установки.

Основное полнятие мультитенантности - Нода. Нода это как-раз экземпляр установки RuSIEM(RvSIEM).

Существует несколько видов нод:

- **Подчиненная нода** - это инсталляция у клиента, в которую приходят события. Данная инсталляция может служить только для приема событий, либо для приема, полной обработки и даже хранения, в этом случае в центр будут переданы только инциденты. Архитектурно все события, поступающие с подчиненной ноды на головную имеют идентификатор ноды: node_uuid - который как раз и позволяет определить к какому теннанту данная нода относится.
- **Головная нода** - это как-раз централизованная установка, к которой подключаются подчиненные ноды. В рамках головной ноды может происзодить обработка событий, их хранение, настройка

подчиненных нод, а также доступ пользователей к информации по конкретным теннантам.

В головной ноде несколько подчиненных нод как раз объединяются в Теннант, События одного теннанта обрабатываются друг с другом, а пользователи как раз видят сущности, относящиеся к теннантам, к которым у них есть доступ.

В рамках мультитенантности создается головная нода, с которой осуществляется управление подключенными подчиненными нодами, а также дальнейшее редактирование конфигураций микросервисов нод, их настроек, парсеров, правил корреляции, симптомов, а также отслеживание состояний подключенных нод.

Подключенные подчиненные ноды объединяются в Тенанты, где каждый тенант как раз и представляет собой отдельную "Организацию" или Арендатора. В рамках одного Тенанта может быть несколько нод, также можно организрвать различный режим работы:

- **Подчиненная нода(RuSIEM/RvSIEM)** может только принимать события, их парсить а дальше отправлять на центральную ноду, где будет происходить корреляция в рамках тенанта (то есть с событиями, приходящими с Нод данного тенанта). Также видеть такие события и инциденты будут только пользователи, у которых назначена возможность видеть данный тенант.
- **Подчиненная нода(RuSIEM)** может принимать события, их парсить и коррелировать на своих микросервисах, и дальше передавать на головную ноду только инциденты, которые будут видеть пользователи, имеющие доступ к данному Тенанту. Правилами корреляции подчиненной ноды можно управлять с головной ноды.

  Все взаимодействие с нодами в системе RuSIEM(RvSIEM):

  - Выбор режима ноды в настройках (п.3.5.1.1);
  - Выбор ноды в разделе "Корреляция";
  - Выбор ноды в разделе "Симптоматика";

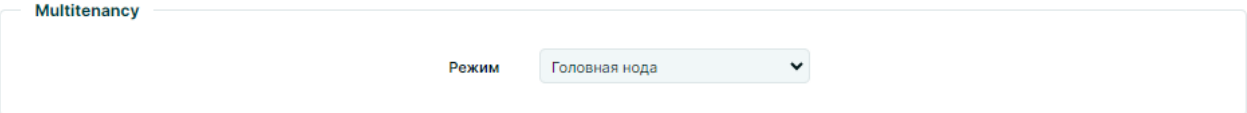
- Выбор ноды в разделе "Инциденты";
- Выбор ноды в разделе "Настройки";
- Поиск событий по нескольким нодам (мультипоиск) (п.3.1.7);
- Копирование пользовательских правил корреляции на подчиненные ноды (п.3.7);
- Копирование пользовательских симптомов на подчиненные ноды (п.4.4);
- Копирование пользовательских парсеров на подчиненные ноды (п.3.5.10);
- Просмотр состояния подчиненных нод (п.4.4.3);
- Возможность передачи инцидентов с подчиненной ноды на главную (п.3.6.5);
- Создание тенантов и распределение нод по ним (п.3.6.4).

О том как создавать головную и подчиненные ноды и работать с ними описано в п.3.6.2.

3.6.2 Работа с multitenancy

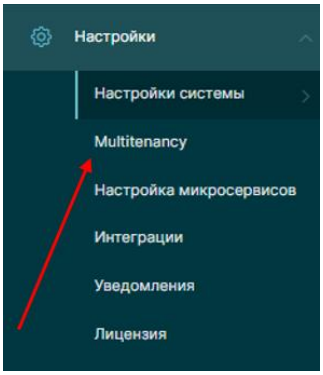
1) Создать головную ноду.

Перейти в раздел "Настройки". В поле "Multitenancy" выбрать режим "Головная нода".



2) На головной ноде создать тенанты.

Перейти в раздел "Multitenancy".

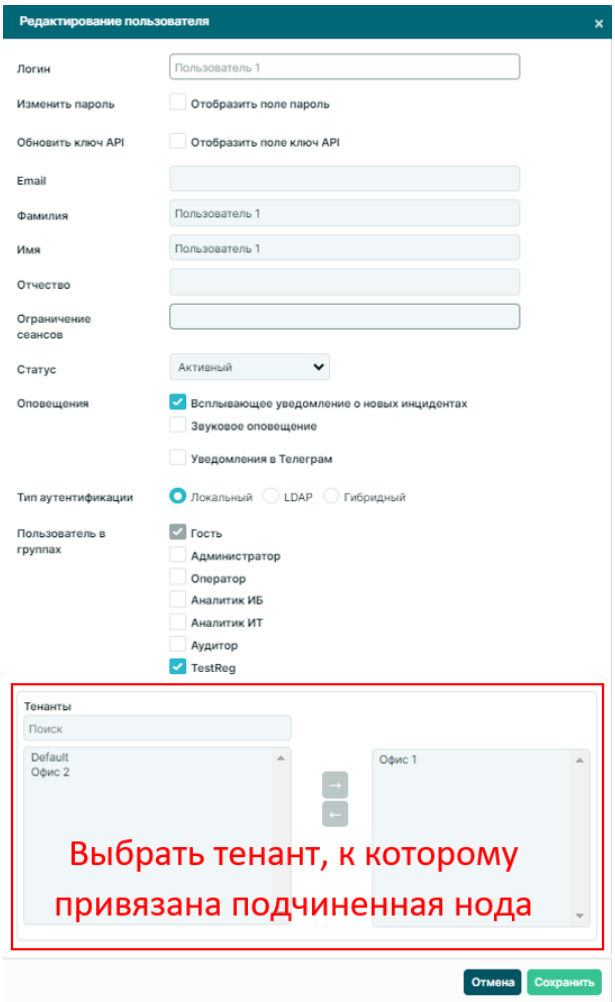


Нажать на кнопку  добавления тенанта. Заполнить необходимые поля и нажать на кнопку "Сохранить". Подробнее описано в п.3.6.4.

3) Создать пользователей ля каждого тенанта и одного общего.

Перейти в раздел "Настройки" на вкладку "Пользователи". Нажать кнопку  добавления пользователя. Запонить необходимые поля и выбрать тенант, который будет привязан к пользователю. Нажать кнопку "Сохранить".

При построении мультитенантной архитектуры "Тенант 1" **не сможет увидеть события** "Тенант 2", "Тенант 3" ... "Тенант N".

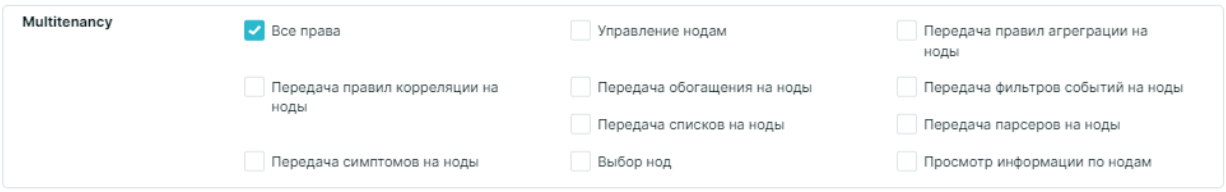


Также создать пользователя и привязать к нему все имеющиеся тенанты. (п.3.5.4)

Если к пользователю не привязывать тенант и нажать на кнопку "Сохранить", то данный пользователь будет видеть все созданные тенанты в системе.

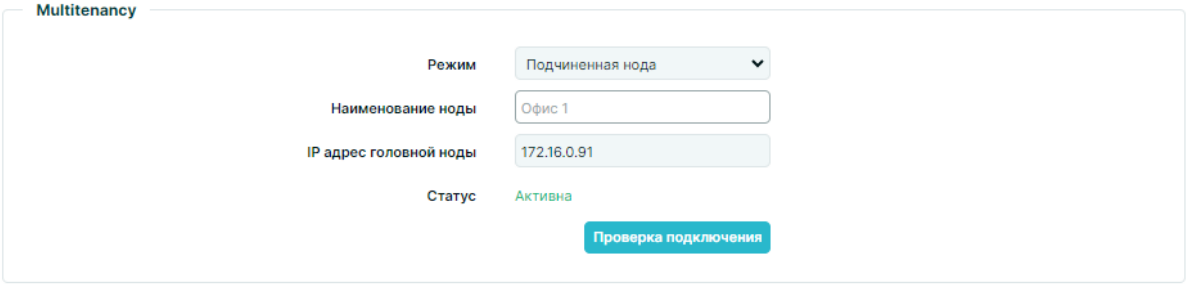
4) Проверить, что у созданных пользователей достаточно ролей.

Перейти в раздел "Настройки" на вкладку "Роли". Напротив созданных пользователей нажать на кнопку - права доступа и проверить достаточно ли ролей у пользователя. (п.3.5.5)



5) Настроить подчиненную ноду.

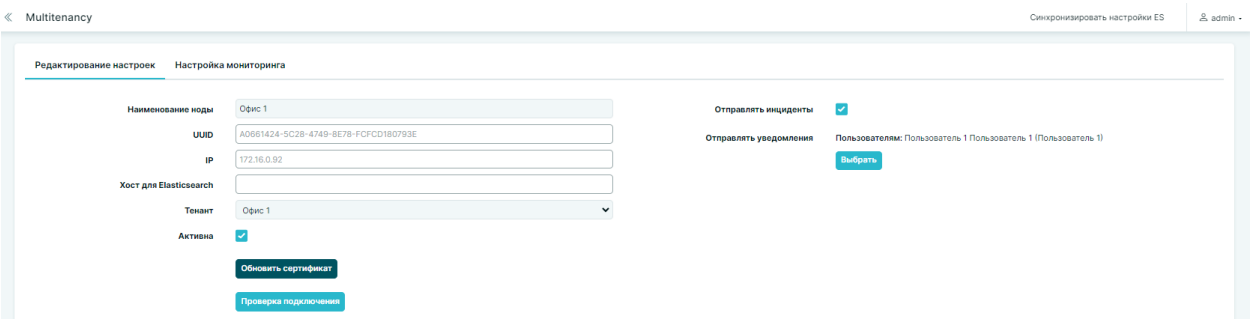
На другом сервере перейти в раздел "Настройки". В поле "Multitenancy" выбрать режим "Подчиненная нода" и заполнить дополнительные поля.



6) На головной ноде отнести подчиненную к определенному тенанту.

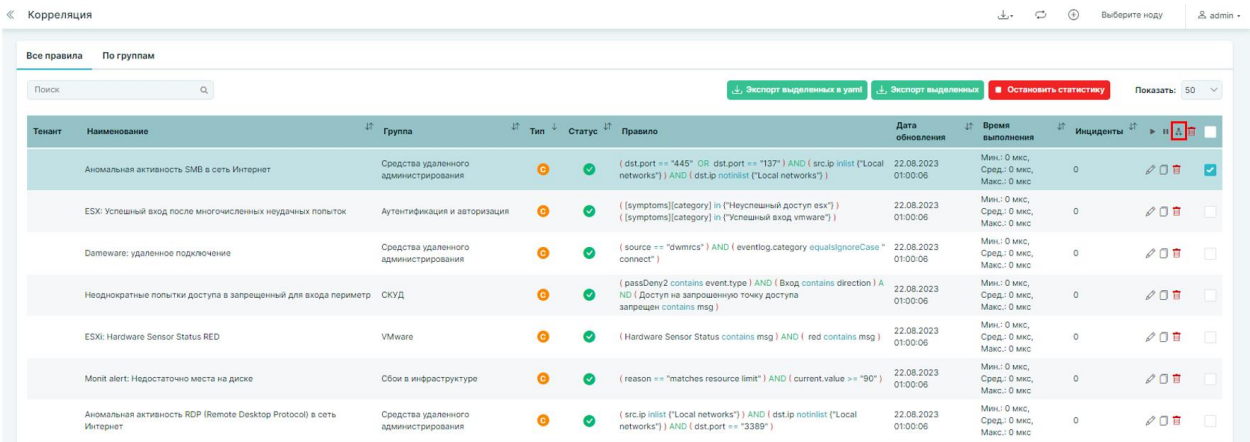
На головной ноде перейти в раздел "Multitenancy". Нажатием на кнопку перетащить ноду к определенному тенанту.

Перейти в настройки ноды, нажав кнопку редактирования ноды. Проверить все настройки ноды, установить галочку на отправку инцидента и выбрать пользователя, которому будет отправляться уведомление. Нажать кнопку "Сохранить". (п.3.6.5)



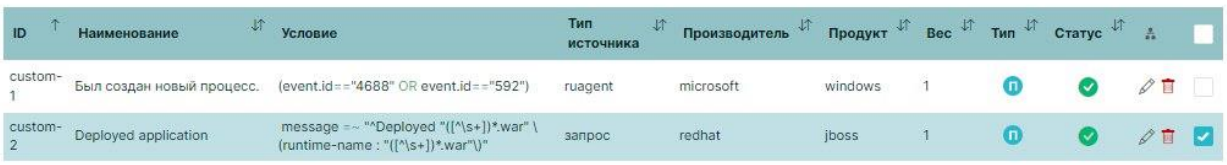
7) Пользователь может отправлять правила корреляции на подчиненные ноды.

Перейти в раздел "Корреляция". Выделить пользовательские правила и нажать кнопку - копировать на ноды. Дальнейшие действия описаны в п.3.7.



8) Пользователь может отправлять пользовательские симптомы и парсеры на подчиненные ноды.

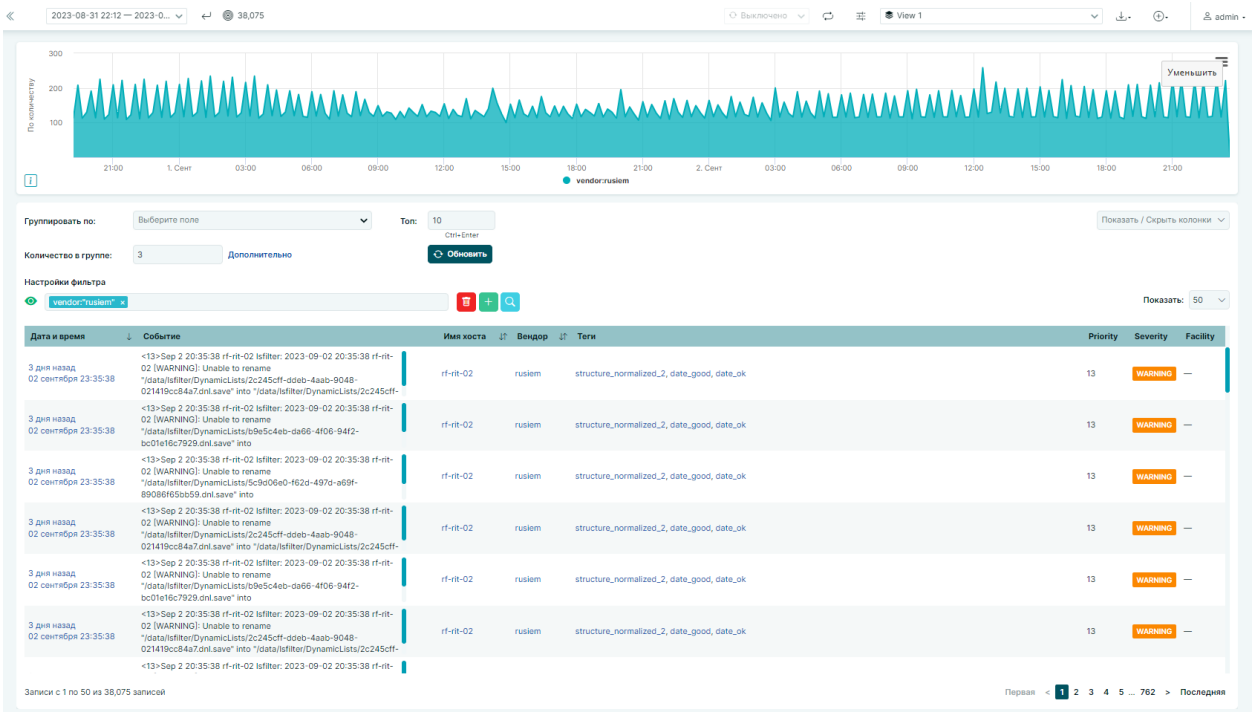
Перейти в раздел "Симптоматика". Выделить пользовательские симптомы и нажать кнопку - копировать на ноды. Дальнейшие действия описаны в п.4.4.



Перейти в раздел "Настройки" на вкладку "Парсеры". Выделить пользовательские парсеры и нажать кнопку - копировать на ноды. Дальнейшие действия описаны в конце п.3.5.10.

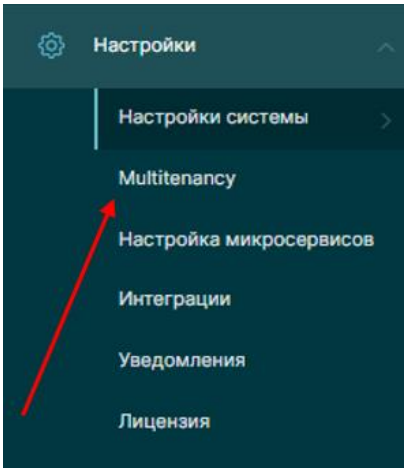
9) Пользователь может выбрать несколько нод для мультипоиска по событиям.

Перейти в раздел "События". Убедиться, что события привязаны к определенному тенату. Действия для осуществления мультипоиска по нескольким нодам описаны п.3.1.7.

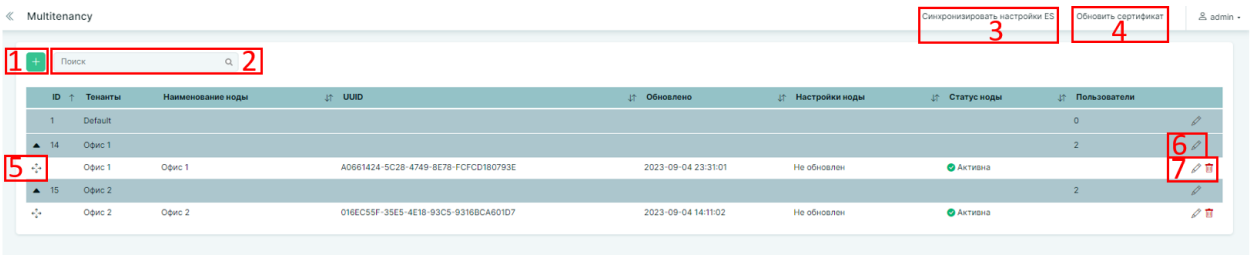


3.6.3 Раздел Multitenancy

На головной ноде перейти в раздел "Multitenancy".



Откроется страница, показанная ниже.



На старнице отобразится таблица с полями:

- **ID**;
- **Тенанты**;
- **Наименование ноды**;
- **UUID ноды**;
- **Обновлено** - дата (ГГ.ММ.ДД) и время обновления;
- **Настройки ноды** - статус настроек подчиненной ноды (обновлен/не обновлен);
- **Статус** ноды - активна/не активна;
- **Пользователи**, которые могут управлять подчиненной нодой.

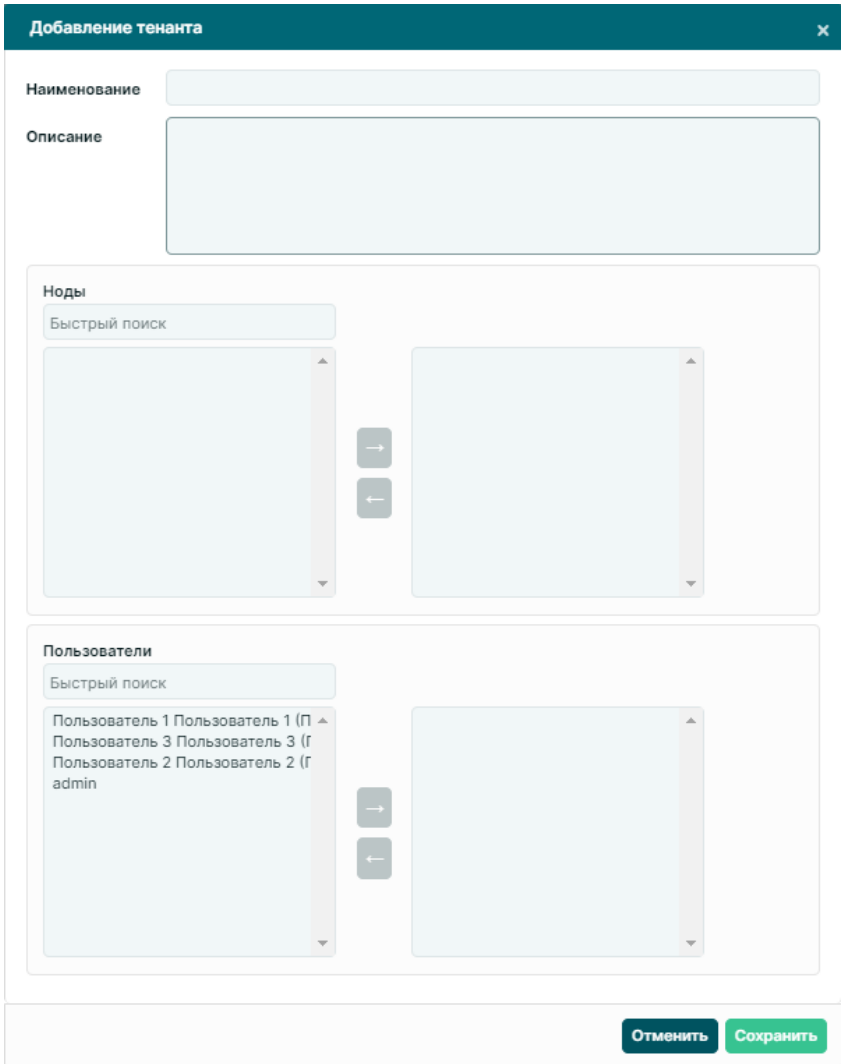
№ Кнопки/ элемента управления	Наименование	Описание
1	"Добавить"	Добавление тенанта, описано в п.3.6.4
2	"Поиск тенантов"	Поиск тенантов по введенному критерию
3	"Синхронизировать настройки ES"	Синхронизация настройки ES
4	"Обновить сертификат"	Обновление сертификата
5	"Переместить"	- перемещение ноды под тенант
6	"Редактировать"	Редактирование тенанта, описано в п.3.6.4

№ Кнопки/ элемента управления	Наименование	Описание
7	"Элементы управления"	- редактирование ноды, описано в п.3.6.5
		- удаление ноды

3.6.4 Добавление/Редактирование тенанта

Окна добавления и редактирования тенаната аналогичные, поэтому рассмотрим добавление тенанта.

В разделе "Multitenancy" нажать на кнопку . Откроется окно, показанное ниже.



В окне заполнить поля:

- "Наименование" - вписать наименование тенанта;
- "Описание" - описать тенант: заполнение необязательно;
- "Ноды" - выбрать ноду, к которой будет привязан тенант, и нажатием на стрелку перенести выбранный элемент из левого поля в правое;
- "Пользователи" - выбрать пользователей, к которым будет привязан тенант, и нажатием на стрелку перенести выбранные элементы из левого поля в правое.

После заполнения нажать на кнопку "Сохранить".

При нажатии на кнопку "Отмена" вернетесь на страницу Multitanancy без сохранения изменений.

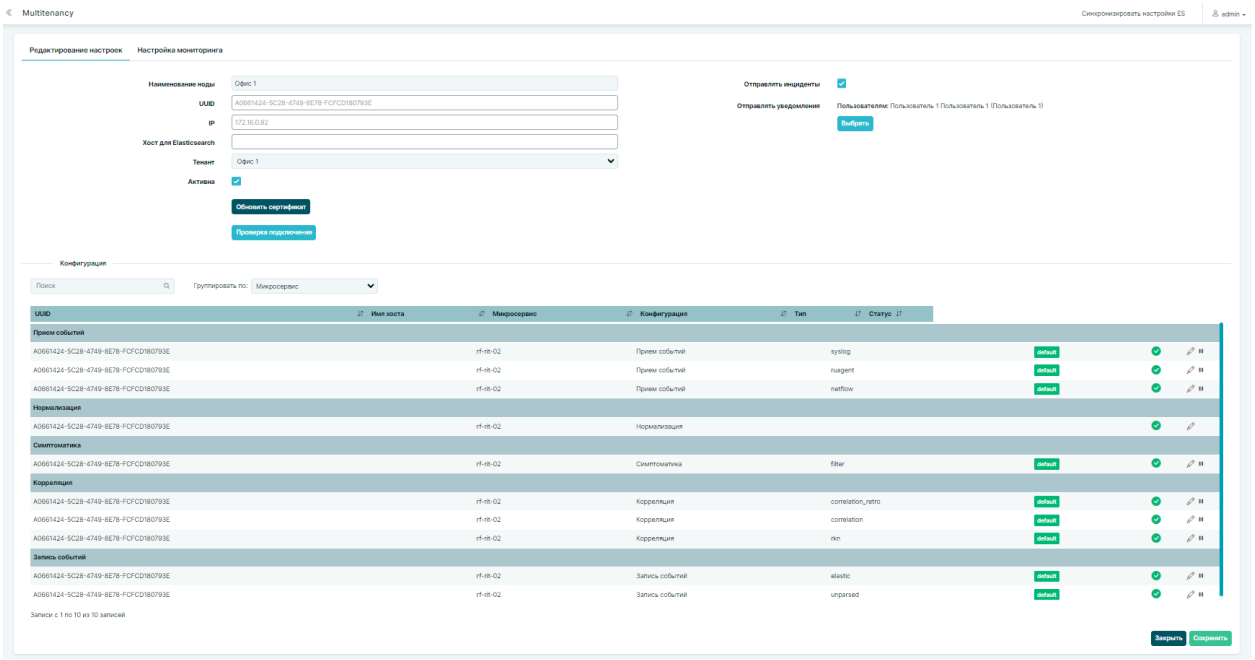
3.6.5 Редактирование ноды

На странице "Multitenancy" нажать на кнопку редактирования  ноды.

Откроется страница редактирования настроек ноды, которая имеет две вкладки:

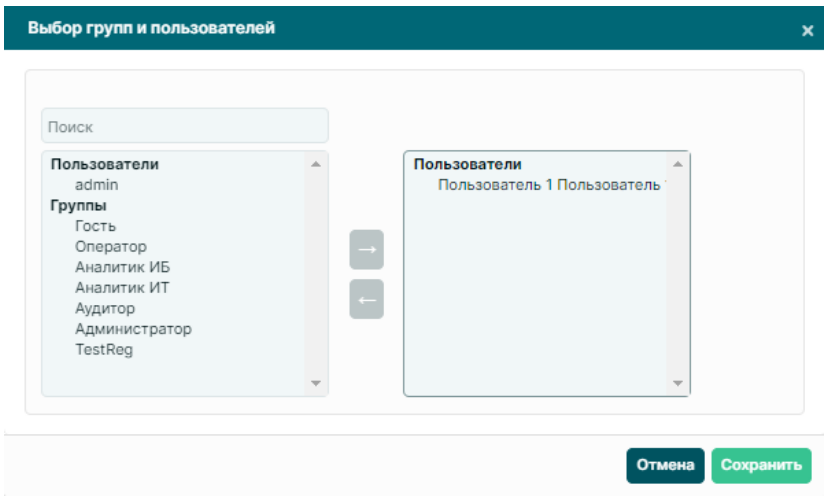
- «Редактирование настроек»
- «Настройка мониторинга»

Вкладка "Редактирование настроек"



На вкладке расположены следующие поля:

- **Наименование ноды** – значение приходит из подчиненной ноды: поле не редактируемое;
- **UUID** – значение приходит из подчиненной ноды, поле не редактируемое;
- **IP** - поле для ввода IP, значение приходит из подчиненной ноды, поле не редактируемое;
- **Тенант** – выбрать из выпадающего списка имеющийся в системе тенант (по умолчанию Default);
- **Активна** - чекбокс, для настройки статуса ноды - ☑ активна нода или ☐ неактивна;
- **Отправлять инциденты** - чекбокс:
  - ☑ - выбрать. Откроется страница, показанная ниже, на которой с помощью стрелок необходимо выбрать кому будет отправлен инцидент и нажать на кнопку "Сохранить";



  - ☐ - не будут отправляться инциденты.
- Поле **Конфигурация**, в которое входят:
  - поле поиска;
  - поле для группировки по всем полям;
  - таблица с перечнем всех микросервисов данной ноды и их данными.

При клике на кнопку редактирования напротив микросервиса открывается модальное окно редактирования конфигурации, описанное в п.3.7.

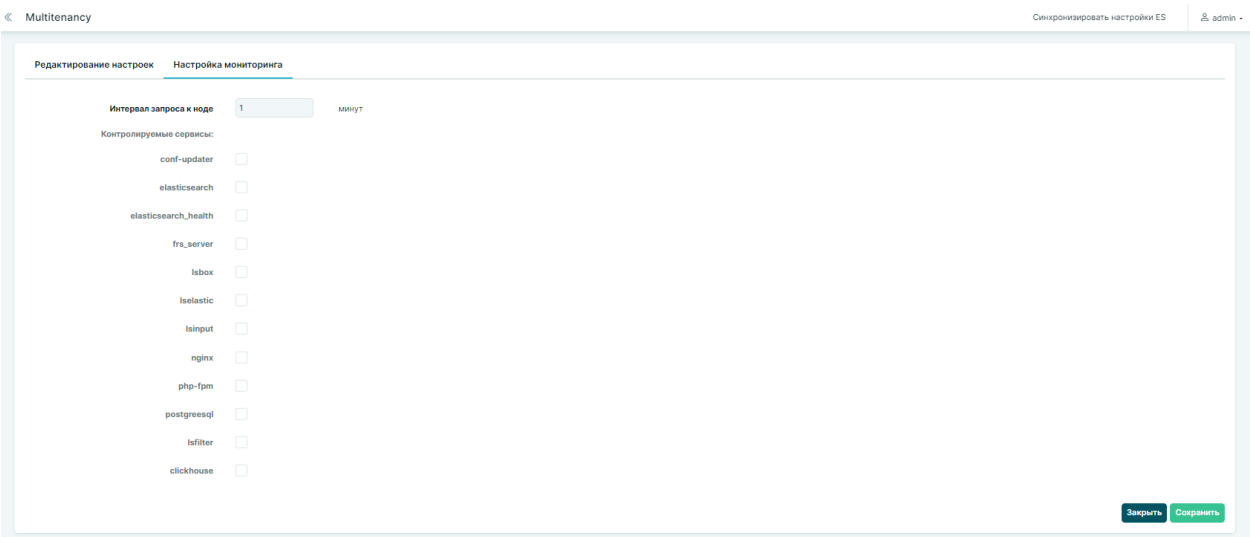
Кнопка активирует конфиг.

Кнопка деактивирует конфиг.

Кнопка "Сохранить" - сохранение всех настроек, после нажатия появляется сообщение о успешном сохранении и открывается главная страница, с таблицей тенантов и нод, где видим данные изменения.

Кнопка "Отмена" - отмена редактирования, при клике изменения не сохраняются и открывается главная страница с таблицей тенантов и нод.

Вкладка "Настройка мониторинга"



На вкладке настройки мониторинга нод заполнить:

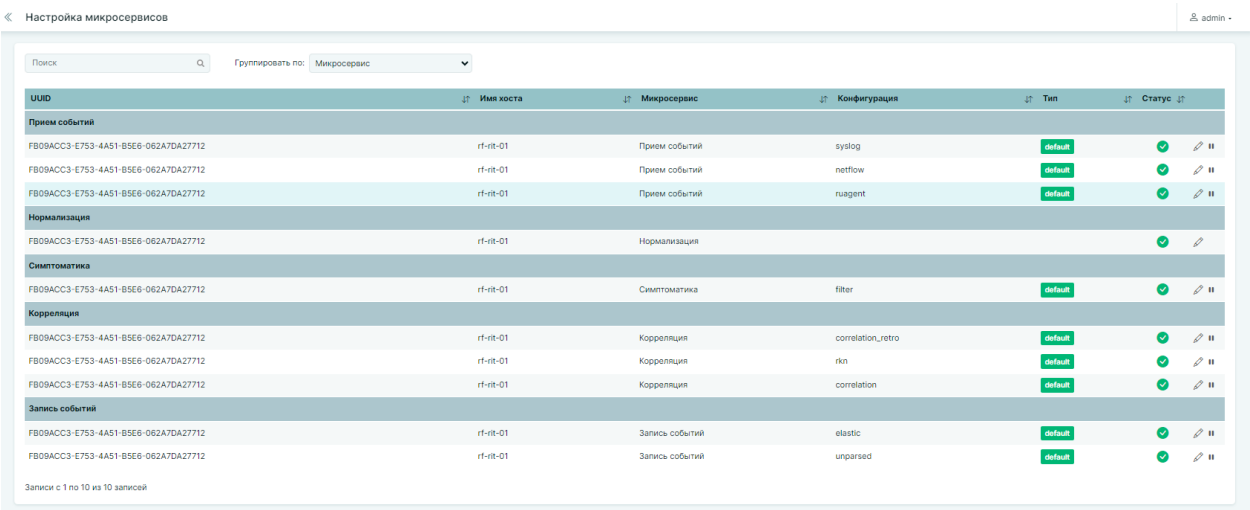
- Интервал запроса к ноде – числовое поле в минутах. Прописывается значение, как часто обращаться к подчиненной ноде.
- Контролируемые сервисы - перечень всех сервисов, напротив необходимых устанавливается галочка.

Нажать кнопку "Сохранить".

В случае если какой-то сервис не работает генерируется событие.

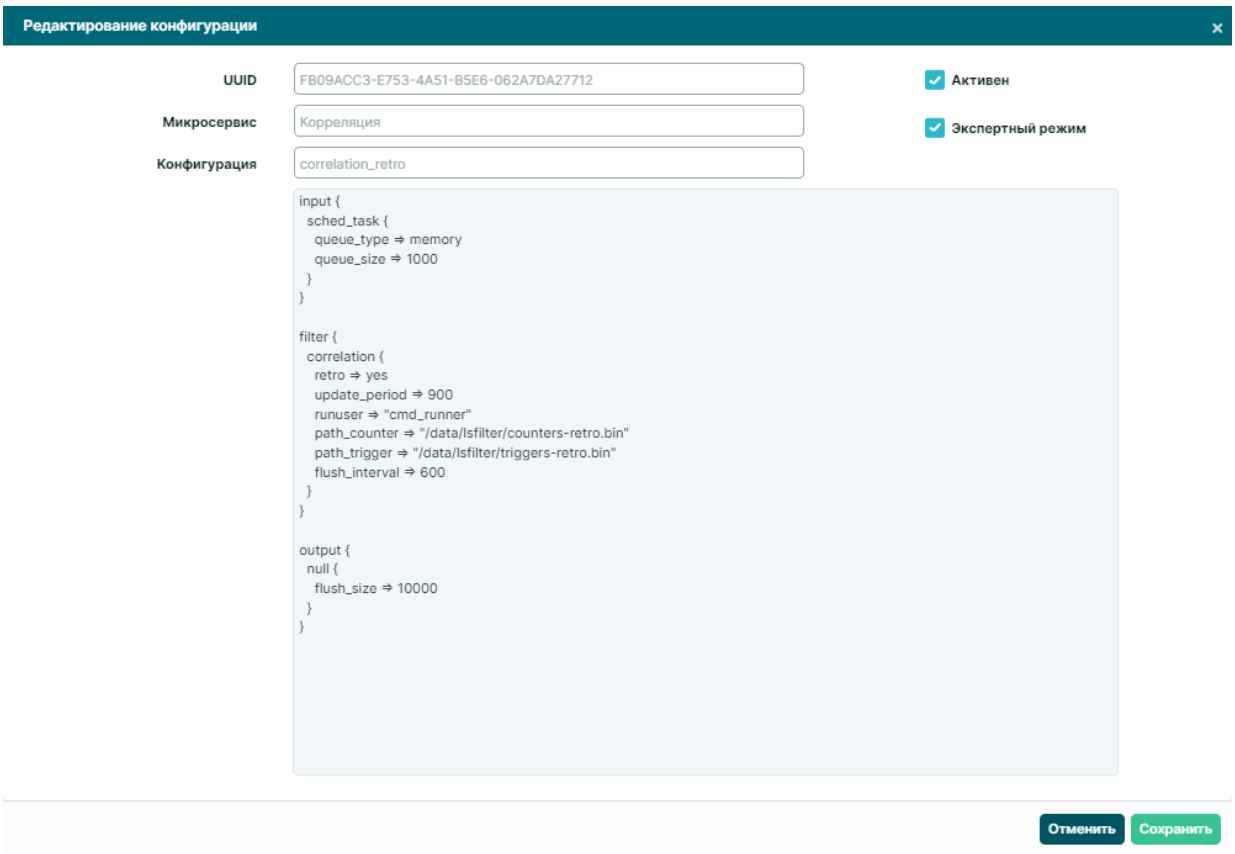
3.7 Редактирование микросервисов

Перейти в раздел "Настройка микросервисов" и нажать кнопку редактирования конфигурации напротив выбранного микросервиса.



Окно "Редактирование конфигурации"

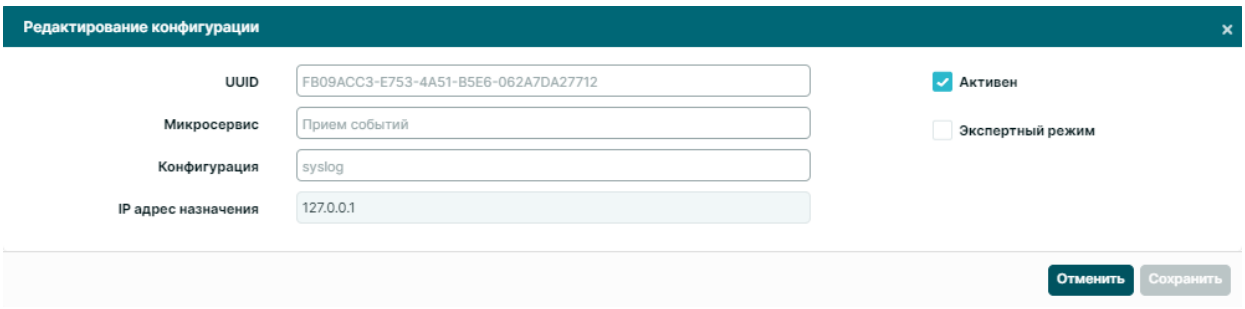
При установке галочки на чекбокс "Экспертный режим" разворачивается код, который можно редактировать.



После внесенных изменения нажать кнопку "Сохранить".

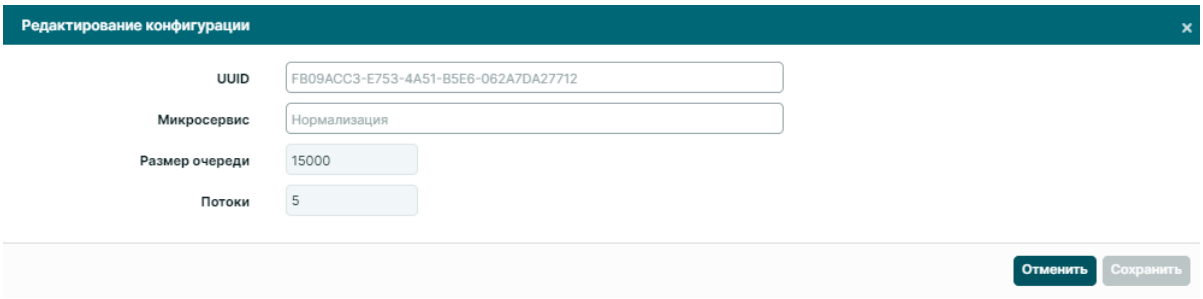
При нажатии на кнопку "Отменить" окно редактирования конфигурации закроется без сохранения внесенных изменений.

1. Редактирование конфигурации микросериса "Прием событий"



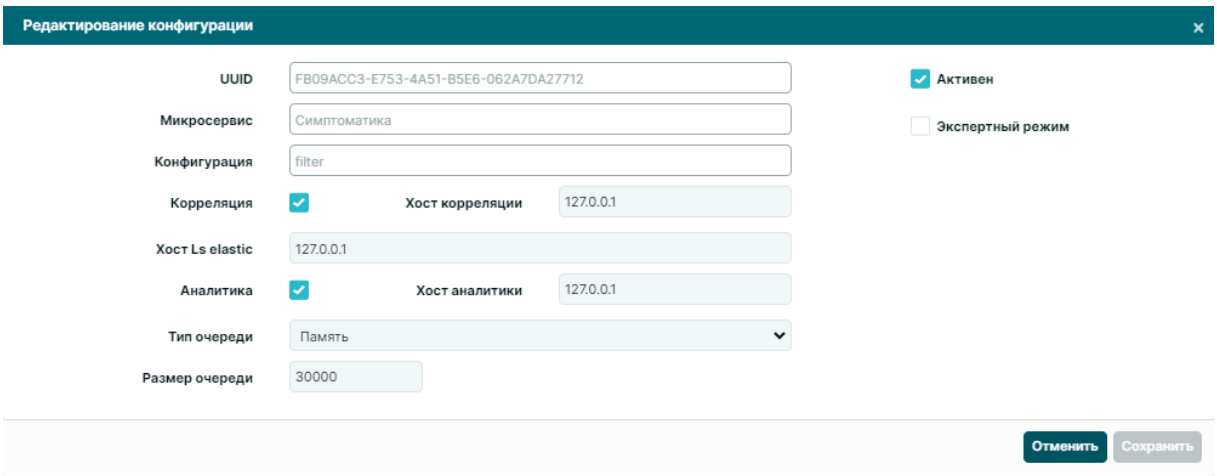
В открывшемся окне установить чекбокс "Активен" и вписать IP адрес назначения. Нажать кнопку "Сохранить" для сохранения изменений или кнопку "Отмена" без сохранения внесенных изменений.

2. Редактирование конфигурации микросервиса "Нормализация"



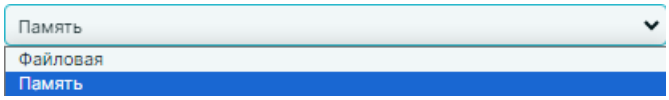
В открывшемся окне вписать размер очереди и количество поток. После заполнения нажать кнопку "Сохранить". При нажатии на кнопку "Отмена" вернетесь на страницу "Редактирования настроек" без сохранения изменений.

3. Редактирование конфигурации микросервиса "Симптоматика"



В окне установить галочку на чекбоксе ☑ "Корреляция" и вписать хост корреляции, хост Ls elastic.

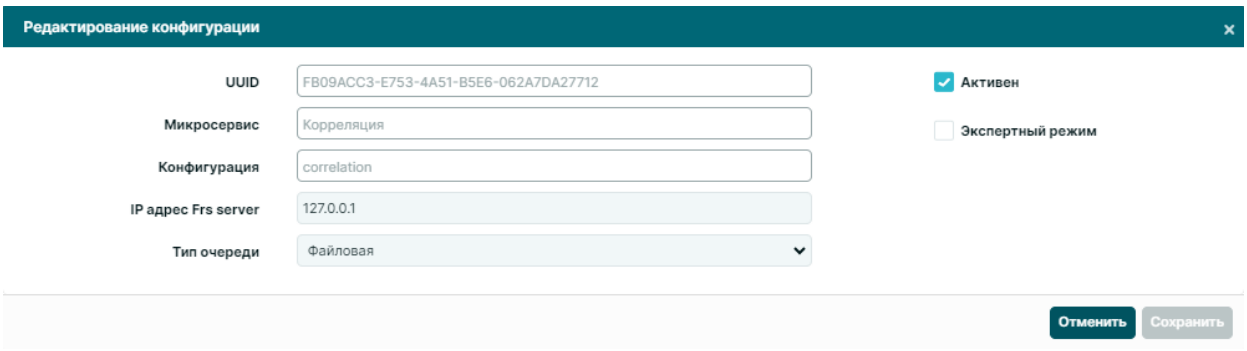
Установить галочку на чекбоксе ☑ "Аналитика" и вписать хост аналитики.

Выбрать из выпадающего списка тип очереди 

и заполнить поле размер очереди. Установить галочку ☑ Активен.

После чего нажать кнопку "Сохранить" или кнопку "Отменить" без сохранения изменений.

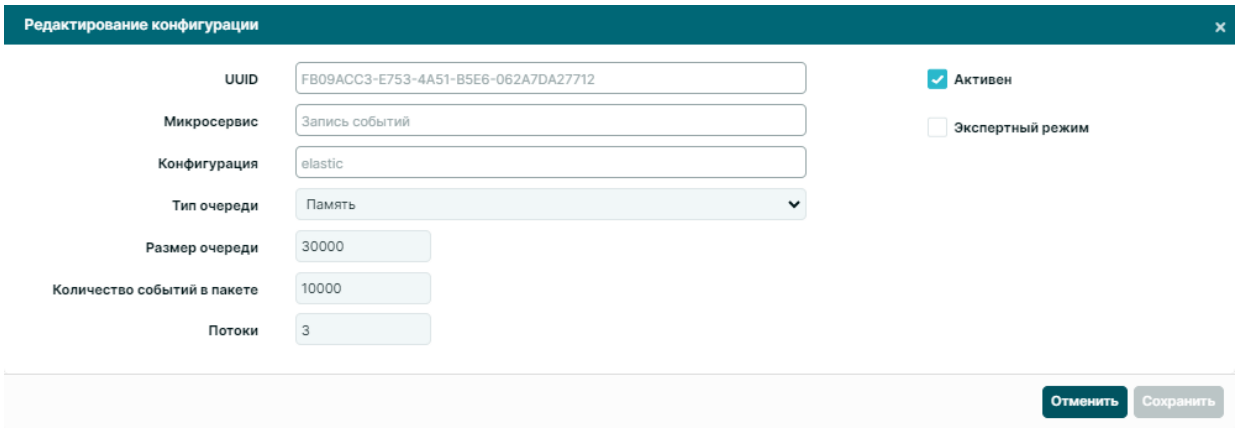
4. Редактирование конфигурации микросервиса "Корреляция"



Заполнить поле IP адрес Frs server, выбрать из выпадающего списка тип очереди, вписать размер очереди и установить галочку ☑ Активен.

После чего нажать кнопку "Сохранить". При нажатии на кнопку "Отменить" производится выход на вкладку "Редактирование настроек" без сохранения изменений.

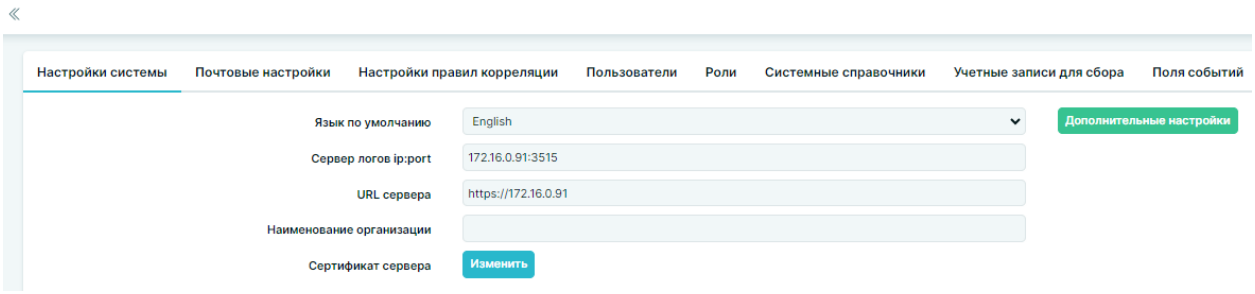
5. Редактирование конфигурации микросервиса "Запись событий"



Выбрать из выпадающего списка тип очереди, вписать размер очереди, количество событий в пакете и количество потоков. Нажать кнопку "Сохранить".

3.8 Настройки сертификата

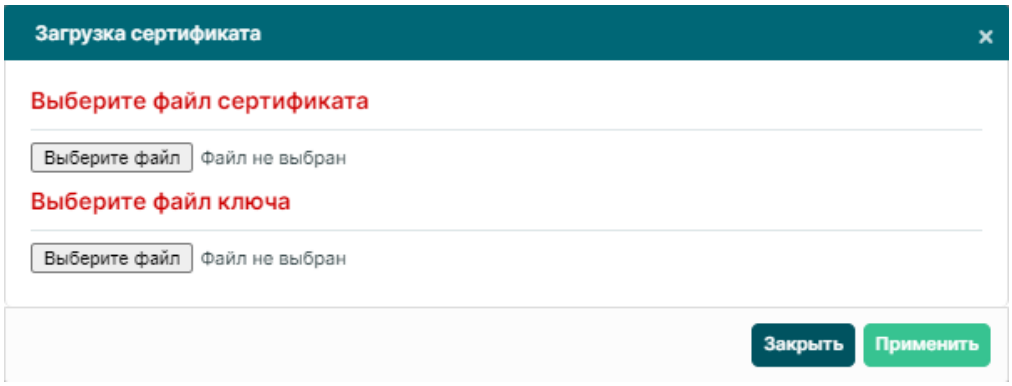
Перейти в раздел "Настройки" в поле "Сертификат сервера" нажать на кнопку "Изменить".



Откроется окно "Загрузка сертификата", в котором необходимо выбрать:

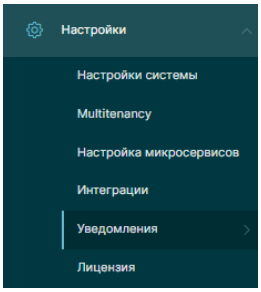
- файл сертификата (.pem, .crt);
- файл ключа (.cer, .key).

Нажать на кнопку "Применить", окно закроется с сохранением изменений. При нажатии на кнопку "Закрыть" окно закроется без сохранения внесенных изменений.

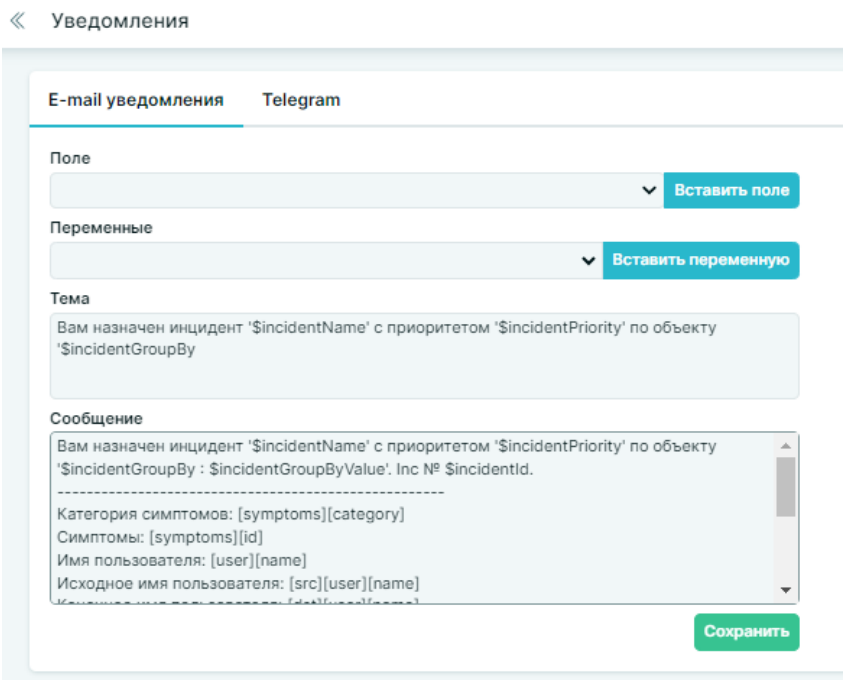


3.9 Раздел «Уведомления»

3.9.1 E-mail уведомления

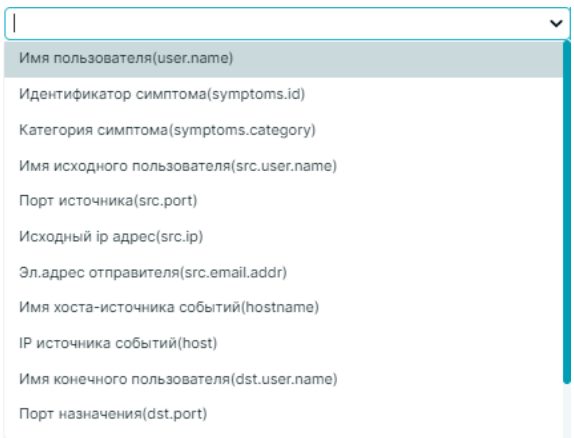
Перейти в раздел "Уведомления" 

на вкладку "E-mail уведомления".

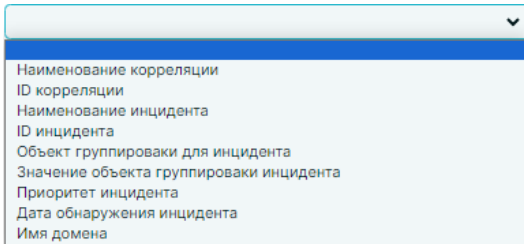


На вкладке заполнить следующие поля:

- Поле - выбрать из выпадающего списка и нажать на кнопку "Добавить поле"



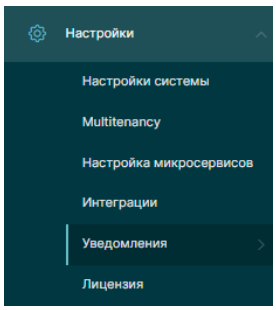
- Переменные - выбрать из выпадающего списка и нажать на кнопку "Вставить переменную"



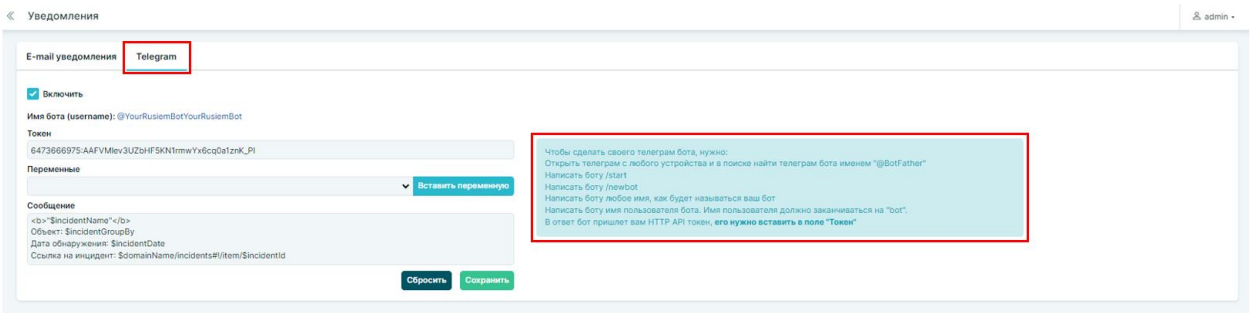
- Создать шаблон темы письма или оставить по умолчанию.
- Создать шаблон самого сообщения или оставить по умолчанию.

3.9.2 Telegram

Настройки бота в Telegram

Перейти в раздел "Уведомления" 

на вкладку "Telegram".



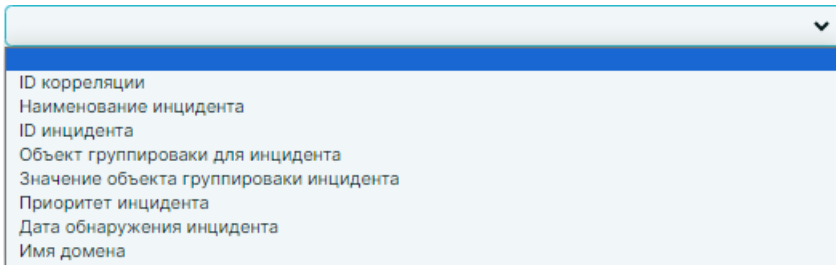
Для использования уведомлений в Telegram установить галочку ☑ Включить.

Необходимо проследовать действиям, указанным в подсказке:

Чтобы сделать своего телеграм бота, нужно:
Открыть телеграм с любого устройства и в поиске найти телеграм бота именем "@BotFather"
Написать боту /start
Написать боту /newbot

Написать боту любое имя, как будет называться ваш бот
Написать боту имя пользователя бота. Имя пользователя должно заканчиваться на "bot".
В ответ бот пришлет вам HTTP API токен, **его нужно вставить в поле "Токен"**

В строке "Переменные" можно выбрать переменную из выпадающего списка, которая будет указана в приходящем уведомлении (заполняется по желанию):

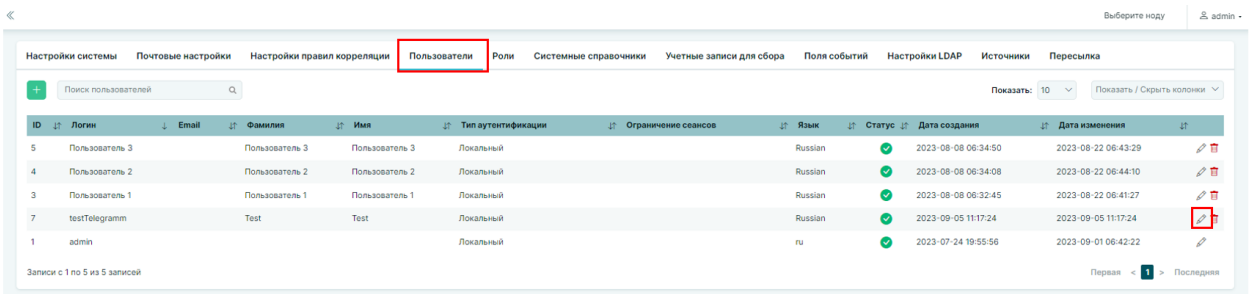


В поле "Сообщение" указан шаблон приходящего уведомления об инциденте.

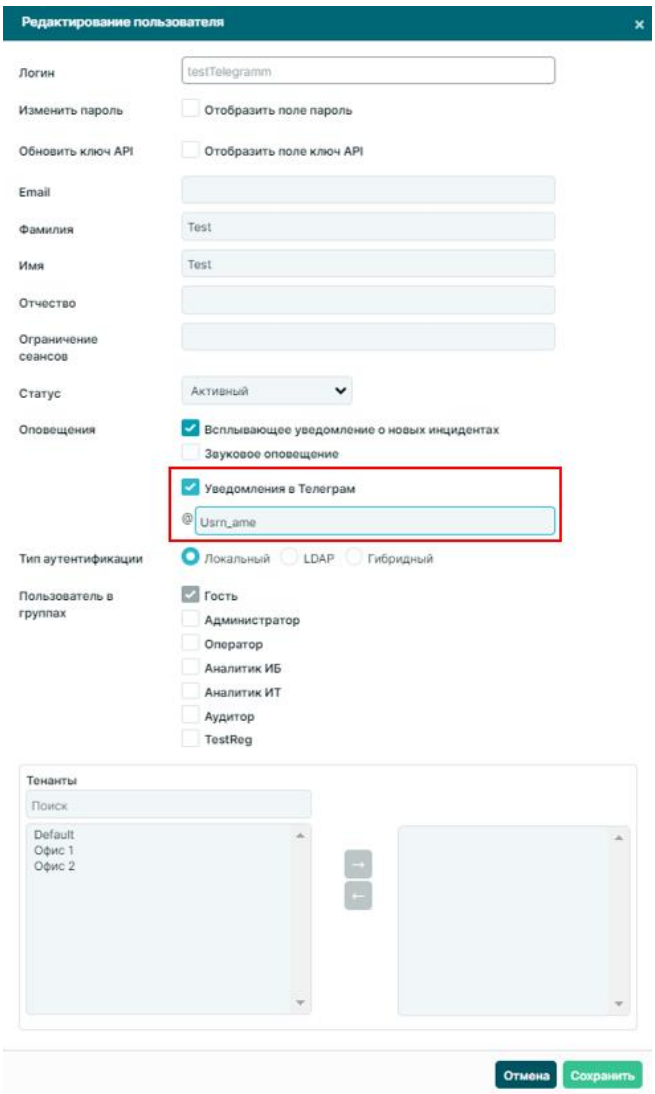
После выполненных условий нажать на кнопку "Сохранить" и в строке "Имя бота (username)" будет указано имя, выбранное вами в Telegram.

Настройки пользователя, которому будут приходить уведомления в Telegram

Далее перейти в раздел "Настройки" на вкладку "Пользователи".



Нажать на кнопку редактирования напротив необходимого пользователя.



Установить галочку ☑ "Уведомления в Телеграм" и вписать имя пользователя **без @** , которому будут приходить уведомления.

Нажать на кнопку "Сохранить".

После проделанных действий отправьте боту команду "/start", чтобы получать уведомления.

4. Диагностика и исправление проблем

4.1 Диагностика проблем

Нет событий

tcpdump -i *en* src host *.*.*.* -vvv

..*.* - IP адрес.

en - имя сетевого интерфейса.

Пример: tcpdump -i ens18 src host **10.80.180.11** and dst port **5014** -vvv

Проверки состояния работы сервисов

/opt/rusiem/support/syschecker.sh

Автоматическое исправление типовых проблем

/opt/rusiem/support/syschecker.sh -r

Сбор журналов для обращения в техническую поддержку.

/opt/rusiem/support/syschecker.sh -o /tmp/report.txt –m

Расширенный сбор журналов для обращения в техническую поддержку

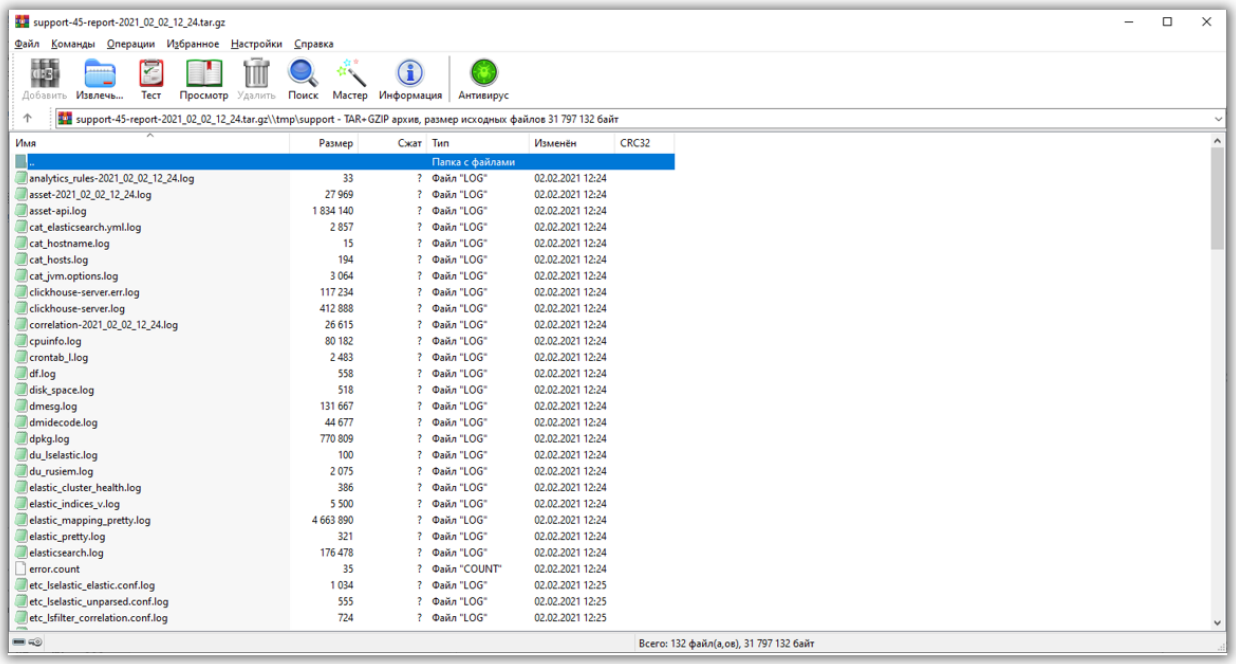
/opt/rusiem/support/rusiem_support.sh

4.2 Диагностика: rusiem_support.sh

Скрипт собирает наибольшее количество данных, необходимых для диагностики

Пример: support-45-report-2021_02_02_12_24.tar.gz

support-**версия**-report-**дата_время**.tar.gz



4.3 Диагностика ноды Elasticsearch

Основной лог для диагностики ноды:

/var/log/elasticsearch/rusiem.log

Посмотреть все доступные индексы и их размер:

curl -H 'Content-Type:application/json' http://127.0.0.1:9200/_cat/indices?v

Удалить определённый индекс:

curl -XDELETE http://127.0.0.1:9200/rusiem-inf-unparsed2021.01.29

Удалить все данные:

curl -XDELETE http://127.0.0.1:9200/*

Закрытие индексов:

curl -XPOST http://127.0.0.1:9200/rusiem-inf-unparsed2021.01.29/_close

Открытие индексов:

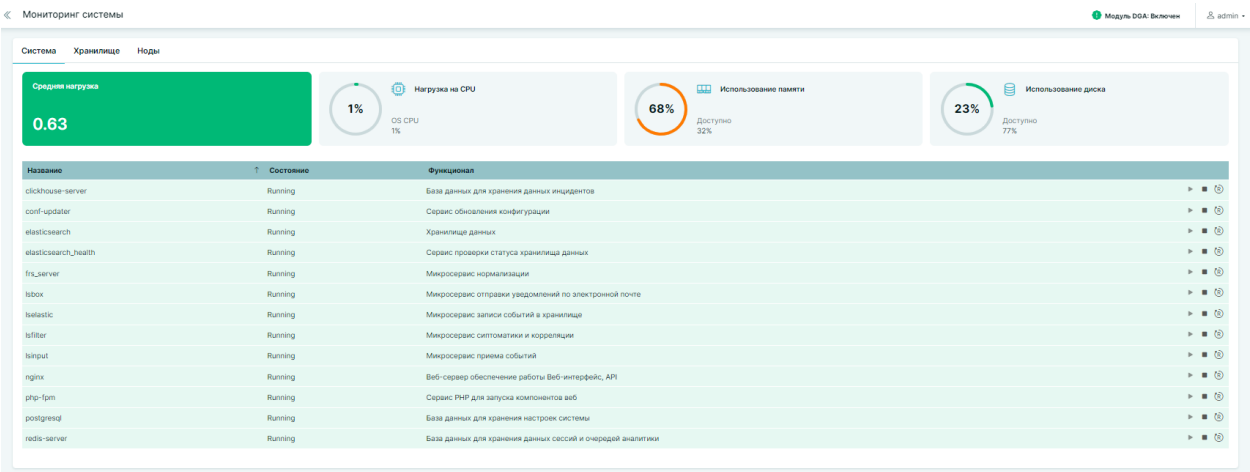
curl -XPOST http://127.0.0.1:9200/rusiem-inf-unparsed2021.01.29/_open

4.4 Раздел "Система"

4.4.1 Вкладка "Система"

Вкладка "Система" состоит из двух полей:

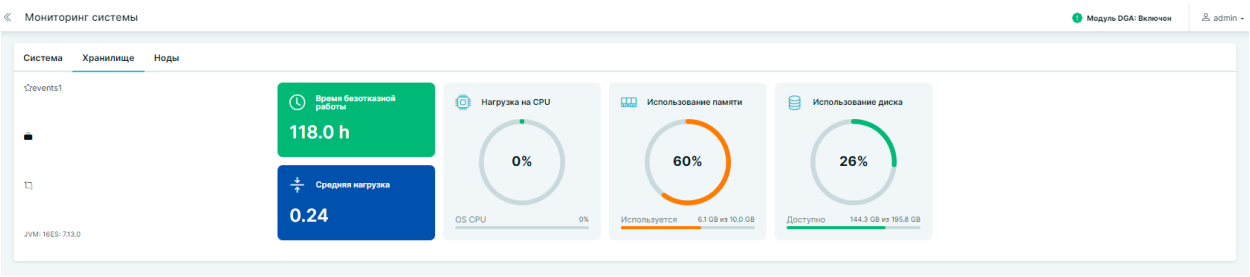
1. Монитор ресурсов системы:
   - Средняя нагрузка;
   - Нагрузка на CPU;
   - Использование памяти;
   - Использованипе диска.
2. Сервисы:
   - Название сервиса;
   - Состояние сервиса;
   - Функионал
   -  - запуск сервиса;
   -  - остановка сервиса;
   -  - перезапуск сервиса.



4.4.2 Вкладка "Хранилище"

Вкладка "Хранилище" состоит из монитора ресурсов:

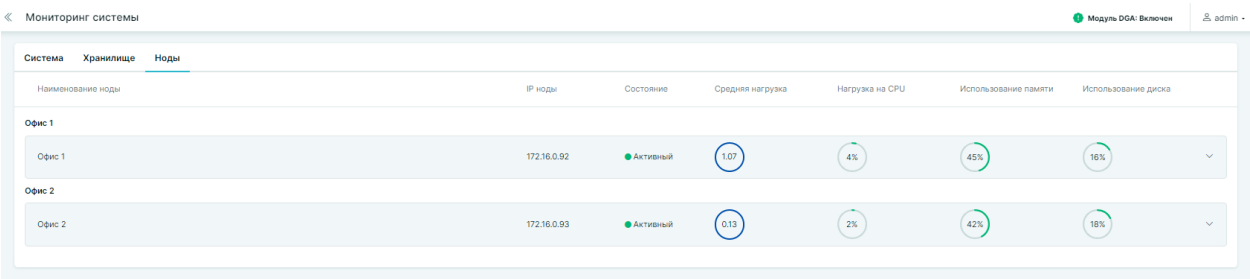
- Наименование ресурса;
- Нагрузка;
- Процесс CPU;
- Использование кучи;
- Использование диска;
- Время безотказной работы.



4.4.3 Вкладка "Ноды"

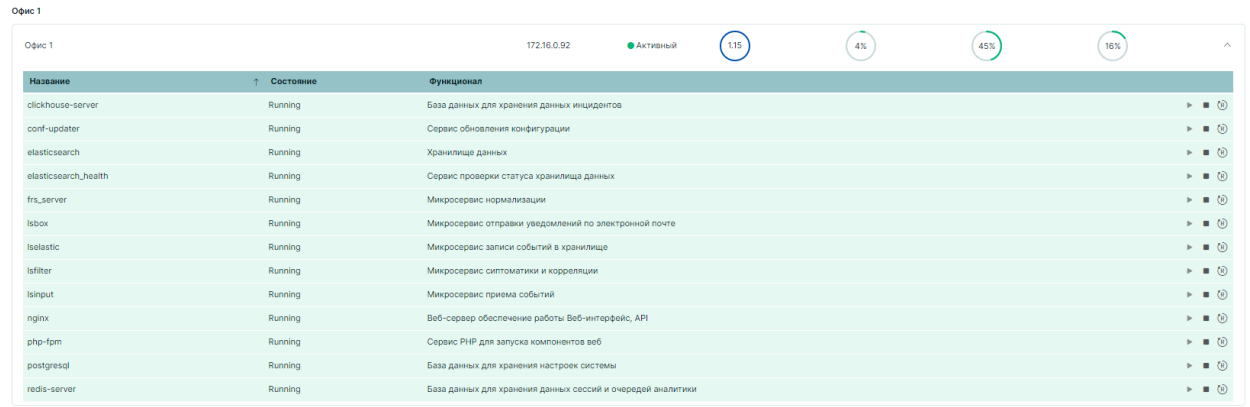
Вкладка "Ноды":

- id;
- Тенанты;
- Наименование ноды;
- IP адрес;
- Состояние;
- Монитор ресурсов



После нажатия на активную ноду откроется список сервисов, который состоит из:

- Названия;
- Состояния;
- Функционала;
-  - запуск сервиса;
-  - остановка сервиса;
-  - перезапуск сервиса.



5. Инструкция по демонам

5.1 Оптимизации демонов

systemctl daemon-reload - (для 18 ubuntu, после изменения настроек демона)

nano /etc/init.d/lsinput

DAEMON_ARGS="-d **-t 4** -p $PIDFILE -f $file -l $WORK_DIR/log -q $QUEUE"

nano /etc/init.d/frs_server

prog_args="**-t 5** -q 15000 -l ${LS_LOG_DIR} $ls_configs -s $DATA"

nano /etc/init.d/lsfilter

DAEMON_ARGS="-d **-t 4** -p $PIDFILE -f $file -l $WORK_DIR/log -q $QUEUE"

nano /etc/init.d/lselastic

DAEMON_ARGS="-d **-t 4** -p $PIDFILE -f $file -l $WORK_DIR/log -q $QUEUE"

Внимание! Если на демоне нет очередей – трогать не надо!

flush_size – максимальное количество данных передаваемые в единицу времени

workers – количество модулей передающих данные

Пример:

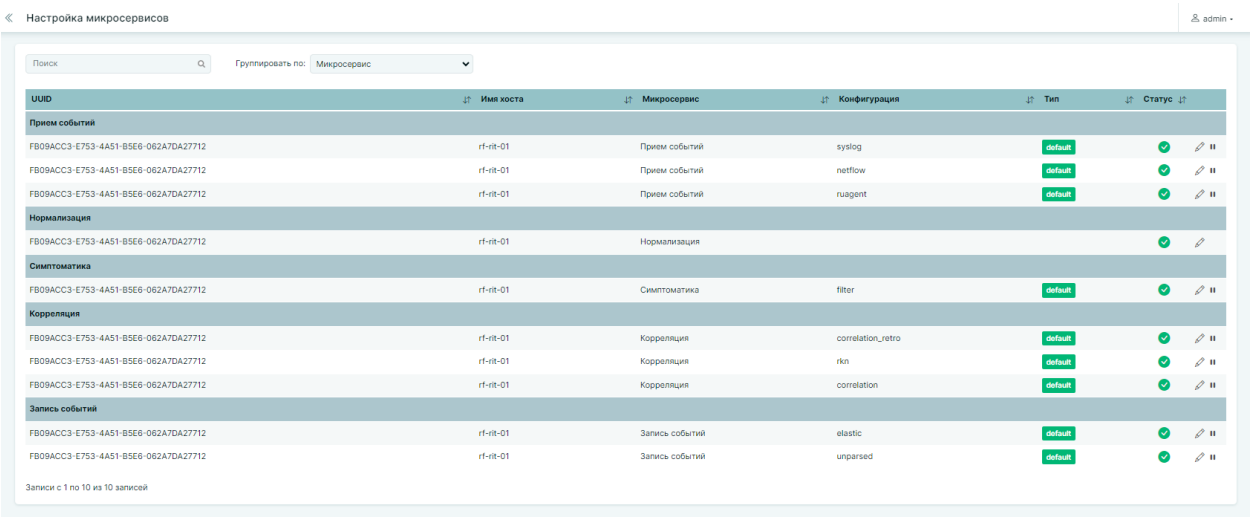
```
output {
 tcp {
        host => "127.0.0.1"
        port => 231
        flush_size => 10000
        workers => 3
    }
}
```

5.2 Структура демонов

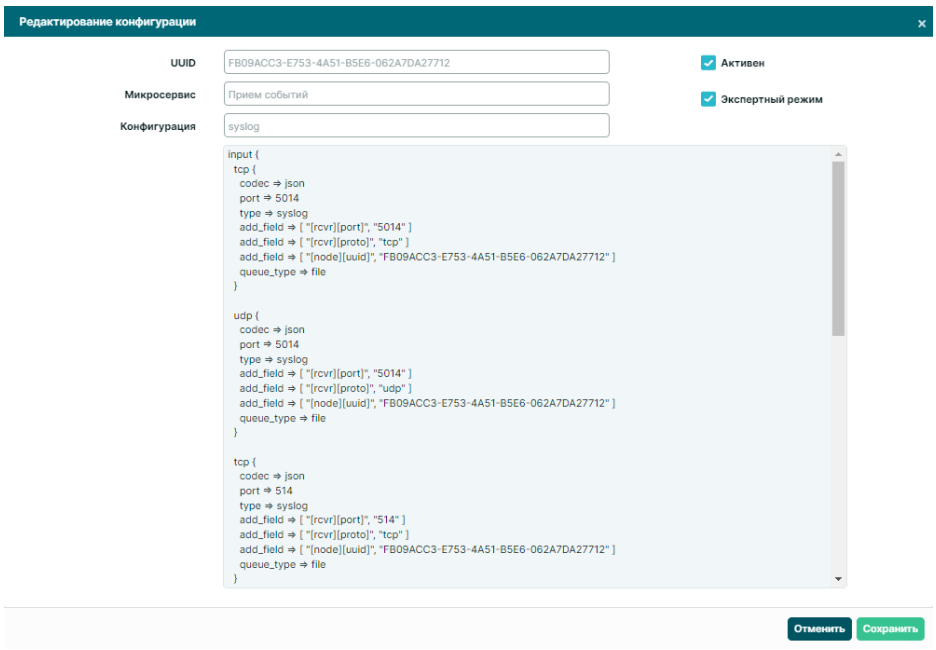
Демон:

/opt/rusiem/*демон*/etc – Файлы конфигурации демона: устаревшая версия;

В данный момент все настройки демонов перемещены в БД и доступны из веб-интерфейса во вкладке "Настройки микросервисов"



При нажатии на кнопку редактирования открывается окно настройки микросервисов, в котором следует выбрать "Экспертный режим"



/opt/rusiem/*демон*/bin – Исполняемый файл демона;

/opt/rusiem/*демон*/log – Журналы работы демона;

/opt/rusiem/*демон*/var - PID файлы потоков демона;

/data/*демон*/ - Очереди, счетчики.

Полезные данные находятся в папках etc и log.

5.3 Структура конфиг файлов демонов

/opt/rusiem/*демон*/etc

Секции:

Input – отвечает за прием данных на демон;

Output – отвечает за передачу данных из демона.

Input

tcp/udp:

- codec => json
- port => 514
- type => syslog/cipher
- add_field => ["[rcvr][port]", "514"]
- queue_type => file/memory

Output

tcp/udp/file/redis/elasticsearch:

- host => "127.0.0.1“
- port => 231
- data_type => "channel“
- key => "unparsed"
- file { path => "/data/ruagent.txt"}

5.4 Описание консольных команд

Экспорт правил корреляции

cd /var/www/html;php artisan export:correlation --file=/path/to/file/filename.json --type=all/user

Параметры:

- **file** (обязательный параметр) - путь к файлу, в который будет выгружаться экспорт.
- **type** [all,user,system] (необязательный параметр) - тип экспортируемых правил. Где all - все, user - только пользовательские, system - только системные.

Импорт правил корреляции

cd /var/www/html;php artisan import:correlation --file=/path/to/file/filename.json

Параметры:

- **file** (обязательный параметр) - путь к импортируемому файлу с правилами корреляции

cd /var/www/html;php artisan export:symptoms --file=/data/backup/userdata/symptoms-$today.json --type=user

cd /var/www/html;php artisan export:reports --file=/data/backup/userdata/reports-$today.json --type=user

cd /var/www/html;php artisan export:eventrules --file=/data/backup/userdata/analytics_rules-$today.json

cd /var/www/html;php artisan export:correlation --file=/data/backup/userdata/correlation-$today.json --type=user

cd /var/www/html;php artisan export:asset-template --file=/data/backup/userdata/asset-$today.json

6. Обновление системы

Система может обновляться:

- в автоматическом режиме ежечасно по расписанию (отключаемо инженером) с подключением к сети Интернет по протоколу https к серверу support.rusiem.com;
- инженером RuSIEM с инициализацией обновления самим инженером с подключением к сети Интернет по протоколу https к серверу support.rusiem.com;
- оффлайн с заменой виртуальной машины с сохранением данных.

Внимание! Для доступа к обновлению необходима действующая лицензия на техническую поддержку.

Список соединений с внешними серверами для обновления

Сервера системы используют следующие ресурсы для обновления.

Имя ресурса	**IP**
Сервера для обновления компонентов SIEM, для всех порт 443	
https://support.rusiem.com	104.131.77.206
https://orion.rusiem.com	88.212.250.212
https://rusiem.com	185.209.115.28
https://packagecloud.io/	52.9.87.203

Имя ресурса	**IP**
https://dl.bintray.com	52.28.1.196 52.28.146.70
Сервера для обновления компонентов ОС, для всех порт 80	
http://us.archive.ubuntu.com/ubuntu/	2001:67c:1562::16 2001:67c:1562::19 91.189.91.26 91.189.91.23
http://packages.erlang-solutions.com	13.224.95.127 13.33.243.90
http://ppa.launchpad.net/webupd8team	91.189.95.83 2001:67c:1560:8008::15
http://packages.elasticsearch.org	151.101.2.217 2a04:4e42::729 2a04:4e42:200::729 2a04:4e42:400::729 2a04:4e42:600::729
http://security.ubuntu.com	2001:67c:1560:8001::11 2001:67c:1360:8001::17 2001:67c:1562::19 2001:67c:1360:8001::21 2001:67c:1562::16 2001:67c:1560:8001::14 91.189.88.149 91.189.88.152 91.189.91.26 91.189.88.161 91.189.91.23

Имя ресурса	**IP**
	91.189.88.162
http://ru.archive.ubuntu.com	213.180.204.183 2a02:6b8::183
http://esm.ubuntu.com	2001:67c:1562::21 2001:67c:1562::22 2001:67c:1360:8001::2e 2001:67c:1360:8001::2d 91.189.91.47 91.189.88.182 91.189.91.46 91.189.88.183 91.189.95.83
http://download.oracle.com	23.211.96.11 23.4.251.166
http://mirrors.kernel.org	2001:4f8:4:6f:0:1994:3:14 149.20.37.36
http://mirrors.edge.kernel.org	2604:1380:3000:1500::1 147.75.95.133
http://standards-oui.ieee.org	140.98.223.27
http://artifacts.elastic.co	2a04:4e42::734 2a04:4e42:200::734 2a04:4e42:400::734 2a04:4e42:600::734 151.101.2.222 151.101.66.222 151.101.130.222

Имя ресурса	IP
	151.101.194.222

Состав обновлений

Ежечасное обновление включает в себя:

- обновление бинарных файлов системы;
- обновление конфигурационных файлов системы;
- обновление парсеров событий;
- критические обновления безопасности;
- обновление системной симптоматики;
- обновление фид-лент (дифференциальные и полные);
- обновление системных правил корреляции;
- обновление функциональности продукта, новые возможности.

При обновлении системы допускается что будет пропущено одно или серия почасовых обновлений.

Рекомендуется (!) периодическое обновление самой операционной системы. По умолчанию, производится перед установкой новых релизных компонентов системы.

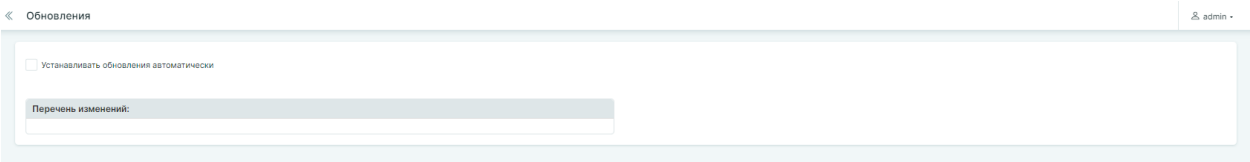
Обновление системы

Обновление системы производится автоматически, по расписанию cron. По умолчанию, обновления:

- глобальное, в 7 утра;
- обновление фидов – каждые полчаса;
- обновление Knowledge Base (правила корреляции, шаблоны, симптоматика, отчеты и т.д.) – каждые полчаса;
- обновление парсеров – каждые полчаса;
- критическое обновление, касающееся стабильности работы системы – каждые полчаса.

При доступном обновлении, система сообщит об этом красным знаком в разделе «Мониторинг и управление» и всплывающим окном «Доступны новые обновления» в правом верхнем углу.

При ручном обновлении необходимо перейти в раздел «Мониторинг и управление» - «Обновления» отображается перечень изменений и кнопка «Установить обновления».

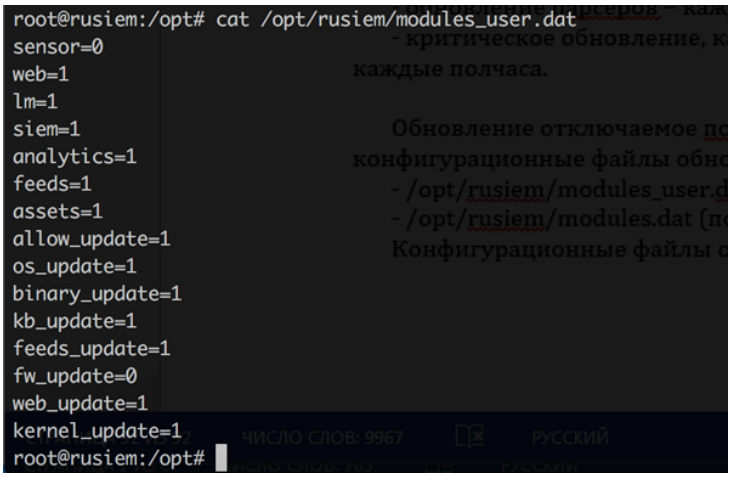


Обновление отключаемое покомпонентно

Основные конфигурационные файлы обновления:

- /opt/rusiem/modules_user.dat (не перезаписываемое, приоритетное);
- /opt/rusiem/modules.dat (по умолчанию).

Конфигурационные файлы обновления имеют синтаксис:



- sensor – сетевой сенсор RuSIEM (отключен по умолчанию);
- web – веб-интерфейс (включен по умолчанию);
- lm – Log management (включен по умолчанию);
- siem – siem-модули (включен для SIEM по умолчанию);
- analytics – компонент аналитики (отключен по умолчанию);
- feeds – фиды (отключен по умолчанию);
- assets – ассеты (отключены по умолчанию);

- allow_update – включает/отключает полностью обновление (включено по умолчанию);
- os_update – обновление операционной системы и компонентов (включено по умолчанию);
- binary_update – обновление бинарных файлов RuSIEM (включено по умолчанию для несертифицированных версий);
- kb_update – обновление базы знаний RuSIEM (включено по умолчанию);
- feeds_update – обновление фидов (отключено по умолчанию);
- Fw_update – обновление правил межсетевого экрана (iptables, по умолчанию отключено);
- web_update – обновление веб-фронтенда (включено по умолчанию);
- kernel_update – обновление ядра операционной системы (включено по умолчанию для несертифицированных версий).

где:

- 1 – компонент/возможность включена;
- 0 – компонент/возможность выключена.

Конфигурационный файл влияет так же на компоненты RuSIEM, которые отображаются в интерфейсе. Например, для отключения раздела аналитики устанавливается analytics=0 в /opt/rusiem/modules_user.dat (а при его отсутствии в файле по умолчанию /opt/rusiem/modules.dat – **Внимание!** Он будет перезаписан с обновлением!).

Обновление производится с помощью bash скриптов (намеренно сделано прозрачным):

- /opt/rusiem/update/bin/update-hourly.sh;
- /opt/rusiem/update/bin/install_analytics.sh;
- /opt/rusiem/update/bin/critical_fix.sh;
- /opt/rusiem/update/bin/update-kb.sh.

Для форсированного обновления на уже работающей системе допускается запуск вручную только update-hourly.sh !!!

Обновление производится через систему apt пакетов с сервера support.rusiem.com по протоколу https. Типовыми командами для обновления служат:

- apt-get update #обновляется локальный репозиторий (список) пакетов;
- apt-get upgrade или apt-get upgrade имя_пакета #обновляется выбранный пакет или все пакеты. С опцией “-y” – производится обновление без подтверждения запроса на обновление;
- apt-get install имя_пакета #устанавливается выбранный пакет;
- apt-get install –reinstall имя_пакета #форсированная установка выбранного пакета из репозитория с переустановкой всех зависимостей и файлов.

Список источников репозиториев, с которых производится установка находится в файле /etc/apt/sources.list.

Обновление системы через прокси-сервер

Допускается настройка доступа в сеть Интернет для обновлений через прокси-сервер.

Настроить прокси на системном уровне можно и через конфигурационные файлы (True UNIX-way). Для этого нужно открыть на редактирования с правами root файл /etc/environment (например sudo vim /etc/environment). В конец файла добавим строки:

- https_proxy="https://user:pass@proxy:port/";
- http_proxy="http://user:pass@proxy:port/";
- ftp_proxy="ftp://user:pass@proxy:port/";
- socks_proxy="socks://user:pass@proxy:port/";
- no_proxy=localhost,127.0.0.0,127.0.1.1,127.0.0.1.

Для примера:

- https_proxy="https://rusiem:pass123@10.0.0.1:3128/";
- http_proxy="http://rusiem:pass123@10.0.0.1:3128/";
- ftp_proxy="ftp://rusiem:pass123@10.0.0.1:3128/";
- socks_proxy="socks://rusiem:pass123@10.0.0.1:3128/".

В новых версиях APT умеет работать с глобальными настройками, но в более старых мог работать только с персональными настройками. Сообщенные настройки: в файле /etc/apt/apt.conf нужно указать:

- Acquire::http::proxy "http://rusiem:pass@localhost:3128/";
- Acquire::https::proxy "http://rusiem:pass@localhost:3128/";
- Acquire::ftp::proxy "http://rusiem:pass@localhost:3128/";
- Acquire::socks::proxy "http://rusiem:pass@localhost:3128/";
- Acquire::::Proxy "true".

7. Резервное копирование и восстановление

Резервное копирование

Резервные копии создаются ежедневно в 23:50 и хранятся 15 дней.

Пользовательские данные помещаются в:

/data/backup/userdata

Пользовательские симптомы:

/data/backup/userdata/symptoms-$today.json

Пользовательские отчеты:

/data/backup/userdata/reports-$today.json

Пользовательские правила аналитики:

/data/backup/userdata/analytics_rules-$today.json

Пользовательские корреляции:

/data/backup/userdata/correlation-$today.json

Пользовательские настройки ассетов:

/data/backup/userdata/asset-$today.json

Резервная копия базы данных PostgreSQL:

/data/backup/userdata/pg-$today.dump

где **$today** - текущая дата

Восстановление данных

Полное автоматическое восстановление выполняется скриптом:

/opt/rusiem/support/restore_user_data.sh

Восстановить Пользовательские симптомы:

cd /var/www/html;php artisan import:symptoms --file=/data/backup/userdata/symptoms-$today.json --type=user

Восстановить Пользовательские отчеты:

cd /var/www/html;php artisan import:reports --file=/data/backup/userdata/reports-$today.json

Восстановить Пользовательские правила аналитики:

cd /var/www/html;php artisan import:eventrules --file=/data/backup/userdata/analytics_rules-$today.json

Восстановить Пользовательские корреляции:

cd /var/www/html;php artisan import:correlation --file=/data/backup/userdata/correlation-$today.json

Восстановить Пользовательские настройки ассетов:

cd /var/www/html;php artisan import:asset-template --file=/data/backup/userdata/asset-$today.json

cd /tmp/

echo 'local all all trust' > /etc/postgresql/10/main/pg_hba.conf

service postgresql restart;sleep 5

sudo -u postgres psql -c "DROP DATABASE rusiem"

sudo -u postgres psql -c "CREATE DATABASE rusiem"

sudo -u postgres psql -c "ALTER DATABASE rusiem OWNER TO rusiem_user;"

sudo -u postgres pg_restore -d rusiem /data/backup/userdata/pg-$today.dump

где **$today** - необходимая дата

Внимание! Перед восстановлением рекомендуется остановить все сервисы /opt/rusiem/support/stopall.sh

По завершению процесса восстановления запустить:

/opt/rusiem/support/start_all.sh