Платформа Радар

Руководство по установке и обновлению

Версия 3.6.7

ООО «Пангео Радар»

Оглавление

1. Подготовка к установке

1.1. Форма поставки

Оптический DVD диск, содержащий архив с дистрибутивом системы и документацию по **Платформе Радар**.

1.2. Основные этапы установки и запуска Платформы Радар

В данном разделе приведен поэтапно процесс установки и запуска **Платформы Радар**.

Сервера, на которых разворачивается ПО **Платформы Радар**, далее именуются целевыми системами.

В таблице приведен состав действий и роли исполнителей, задействованных в процессе развертывания **Платформы Радар**:

Действие	**Ответственный за выполнение**
Подготовка оборудования	Системный администратор
Установка ПО **Платформы Радар**	Системный администратор
Проверка работоспособности ПО	Администратор **Платформы Радар**
Конфигурирование функций **Платформы Радар**	Администратор **Платформы Радар**
Конфигурирование взаимодействия **Платформы Радар** с окружением	Администратор **Платформы Радар**

1.3. Подготовка оборудования

1.3.1 Подготовка дисковой системы

При разметке дисковой подсистемы необходимо учитывать следующие требования:

- корневой раздел (/) - все свободное пространство;
- раздел /home - 10 Гб;
- раздел swap - не менее 10% от общего объема оперативной памяти;
- тип файловой системы - XFS (при необходимости можно использовать EXT4).

Процедура разметки дисковой подсистемы для серверной роли DATA при распределенной инсталляции описана в руководстве «**Администратор**» → «**Процессы работы**» → «**Подготовка дисковой подсистемы для реализации роли DATA»**.

1.3.2 Подготовка аппаратной части

Подготовка как физического сервера, так и виртуальной машины выполняются по одинаковому сценарию и включают следующую последовательность операций:

1. Организация доступа к выбранным физическим серверам/виртуальным машинам;
2. На физических серверах должна быть проведена разметка дисков (форматирование);
3. Установка операционной системы Debian версии не ниже 10 (не рассматривается в данном документе, полную информацию по установке можно получить на сайте);
4. Первичная настройка операционной системы (сетевая конфигурация, DNS, NTP).

1.3.3 Настройка сетевой конфигурации

1. Для доступа к веб-интерфейсам управления **Платформой Радар** инсталлятор откроет порты:
    - 9000
    - 8080
    - 8180
2. Между узлами кластера будет разрешено взаимодействие в обе стороны по следующим портам:
    - 9092
    - 9200
    - 5672
    - 15672
    - 5432
    - 2092
    - 8080
    - 8086
    - 9000
    - 8180
    - 6677
    - 6630
    - 22

Подробное описание сетевого взаимодействия приведено в разделе «**Администратор**» → «**Процессы работы**» → «**Перечень используемых Платформой Радар портов**».

1.3.4 Настройка NTP

На всех узлах кластера необходимо настроить службу синхронизации времени. Пример настройки службы времени в ОС Debian приведен в руководстве «**Администратор**» → «**Процессы работы**» → «**Настройка службы синхронизации времени в ОС Debian**».

1.3.5 Подготовка для установки Платформы Радар без доступа к сети Интернет

Подготовка для установки **Платформы Радар** без доступа к сети Интернет включает обеспечение следующих условий:

- должен быть обеспечен доступ к целевой системе одним из следующих способов:
  - по SSH;
  - физический доступ к серверу с клавиатурой и монитором;
  - консоль MGMT интерфейса;
  - консоль виртуальной машины.
- наличие учётной записи с правами привилегированного пользователя (администратора) ОС в целевой системе.

1.3.6 Подготовка для развертывания Платформы Радар с доступом к сети Интернет

Подготовка для установки **Платформы Радар** с доступом к сети Интернет включает выполнение действий, приведенных в разделе «Подготовка для установки Платформы Радар без доступа к сети Интернет» и следующие дополнительные действия:

1. Добавление альтернативных репозиториев в конфигурационный файл: */etc/apt/source.list*:

```
deb http://security.debian.org/debian-security buster/updates main
deb-src http://security.debian.org/ buster/updates main

deb http://mirror.yandex.ru/debian buster main
deb-src http://mirror.yandex.ru/debian buster main

deb http://mirror.yandex.ru/debian buster-updates main
deb-src http://mirror.yandex.ru/debian buster-updates main

deb http://mirror.yandex.ru/debian/ buster-proposed-updates main non-free contrib
deb-src http://mirror.yandex.ru/debian/ buster-proposed-updates main non-free
contrib
```

2. Настройка доступа к репозиториям через Интернет для загрузки недостающих пакетов.

2. Установка Платформы Радар

2.1. Подготовка установочных файлов

Подключитесь к серверу, на который планируется установка **Платформы Радар**.

Внимание! *Для запуска установки необходимо получить права суперпользователя*.

Скопируйте с оптического диска установочный архив и поместите его в каталог `/var/tmp`.

Перейдите в каталог `/var/tmp`:

```
cd /var/tmp/
```

Командой `ls` убедитесь, что установочный архив успешно скопирован и находится в каталоге `/var/tmp` (см. рисунок 1).

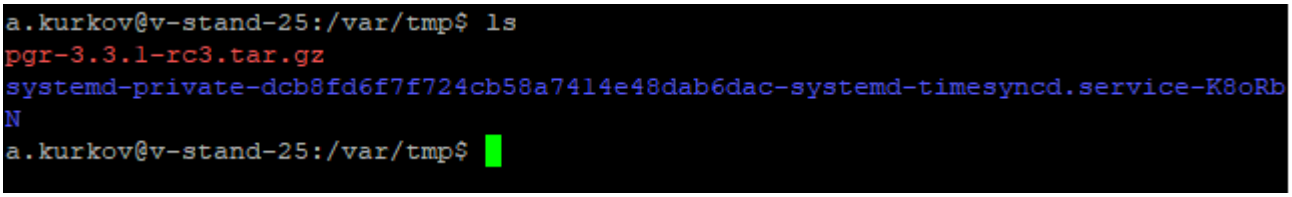

Рисунок 1 – Проверка установочного архива

Если получен зашифрованный архив (файл с расширением `*.enc`), выполните команду для расшифровки:

```
openssl enc -aes-256-cbc -d -in pgr-RELEASE_VERSION-INSTALLATION_TYPE.tar.gz.enc |
tar xz
```

Если получен незашифрованный архив (файл с расширением `*.tar.gz`), выполните команду для разархивирования:

```
tar -zxvf pgr-RELEASE_VERSION-INSTALLATION_TYPE.tar.gz
```

Где название архива **pgr-RELEASE_VERSION-INSTALLATION_TYPE.tar.gz.enc** содержит:

- RELEASE_VERSION - номер версии релиза **Платформы Радар** (например, 3.3.1);
- INSTALLATION_TYPE - тип установки (online или offline).

Командой `ls` убедитесь, что установочный скрипт `install.sh` расположен в директории `/var/tmp/` после распаковки установочного архива.

2.2. Запуск скрипта для установки

Внимание! *Для корректной установки **Платформы Радар** в ОС Debian должна быть задана переменная PATH, содержащая полный список необходимых путей: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin. В случае, если переменная PATH не содержит путей /usr/sbin и /sbin, их следует добавить вручную.*

Выполните следующие действия:

1. Находясь в директории `/var/tmp`, выполните команду `bash install.sh`. Для выполнения команды с правами суперпользователя используйте команду `sudo`. Например, `sudo bash install.sh`.

2. Установка занимает некоторое время, в течение которого загружаются и устанавливаются модули **Платформы Радар**. Далее укажите внешний IP-адрес и доменное имя сервера (необязательно), на котором будет установлена **Платформа Радар** (см. рисунок 2).

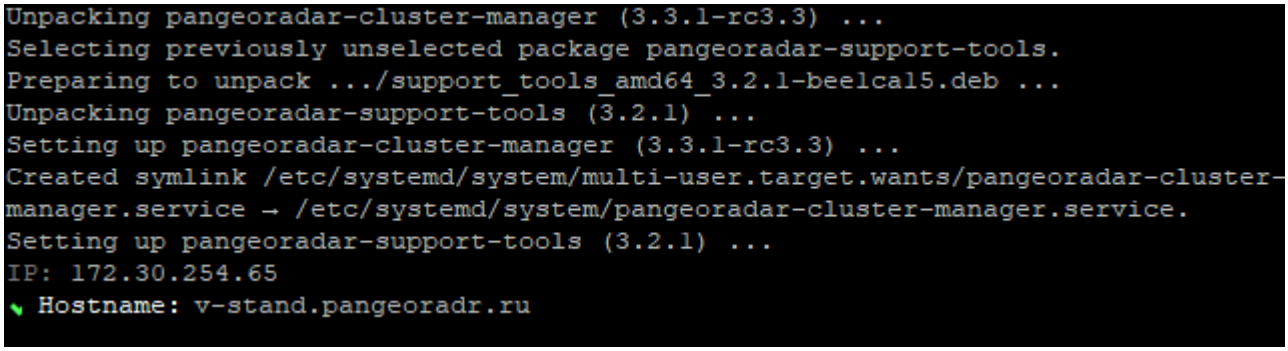

Рисунок 2 - Указание IP-адреса и имени сервера

3. Через некоторое время установка будет закончена на экране появится сообщение об успешном завершении:

   ```
   Продолжите установку по адресу: `http://<УКАЗАННЫЙ ВАМИ IP>/install
   Логин/Пароль по умолчанию - `admin/admin`
   ```

2.3. Продолжение установки в веб-интерфейсе

1. После перехода по адресу, указанному в конце работы инсталлятора, необходимо пройти процедуру авторизации и смены пароля по умолчанию: `admin`/`admin`.

2. После прохождения авторизации станет доступен этап получения лицензии **Платформы Радар** (см. рисунок 3).

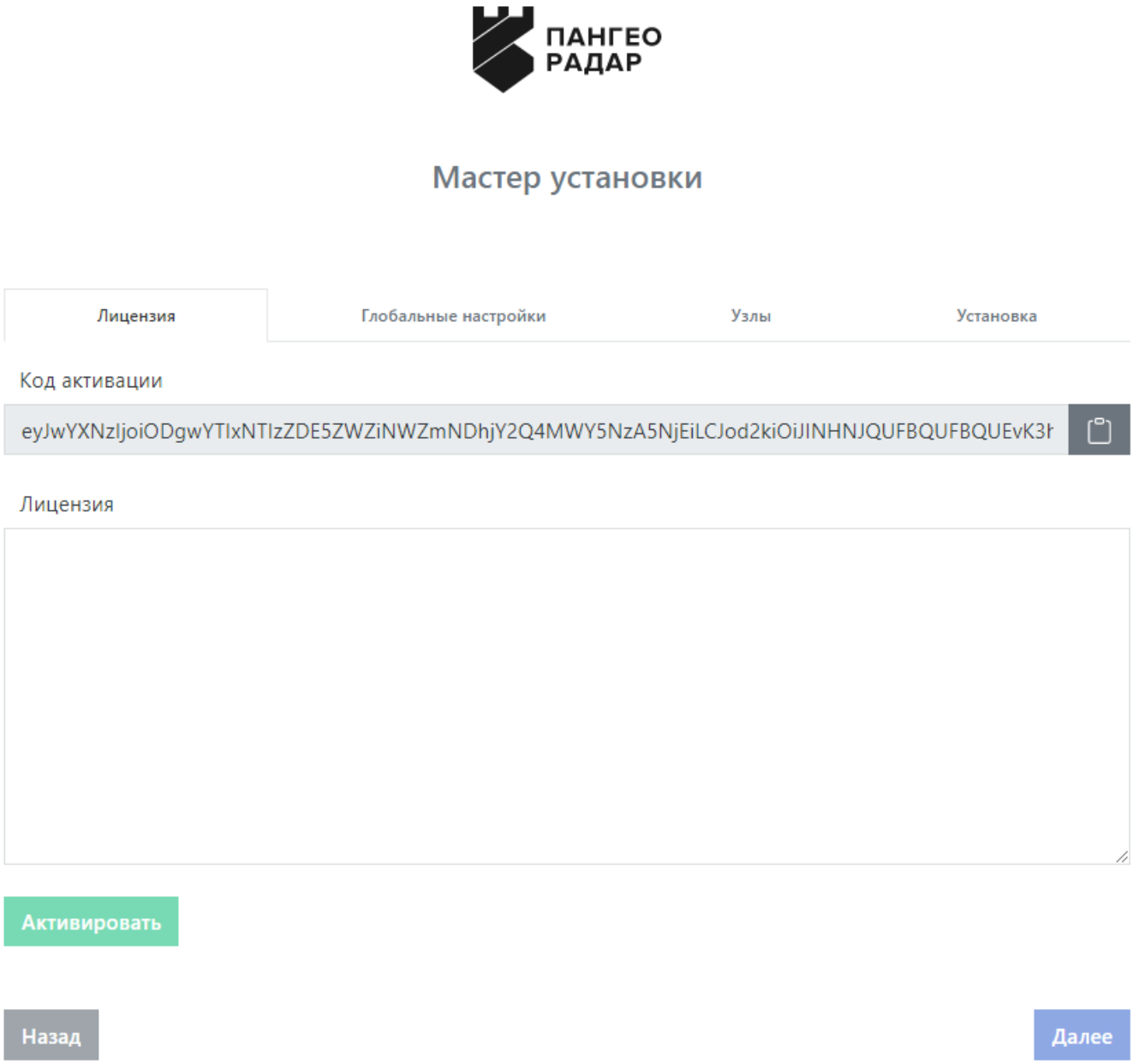

Рисунок 3 – Экран получения лицензии Платформы Радар

3. На вкладке **Лицензия** отображается ваш код активации. Его необходимо указать в личном кабинете клиентского портала **Платформы Радар** (см. рисунок 4).

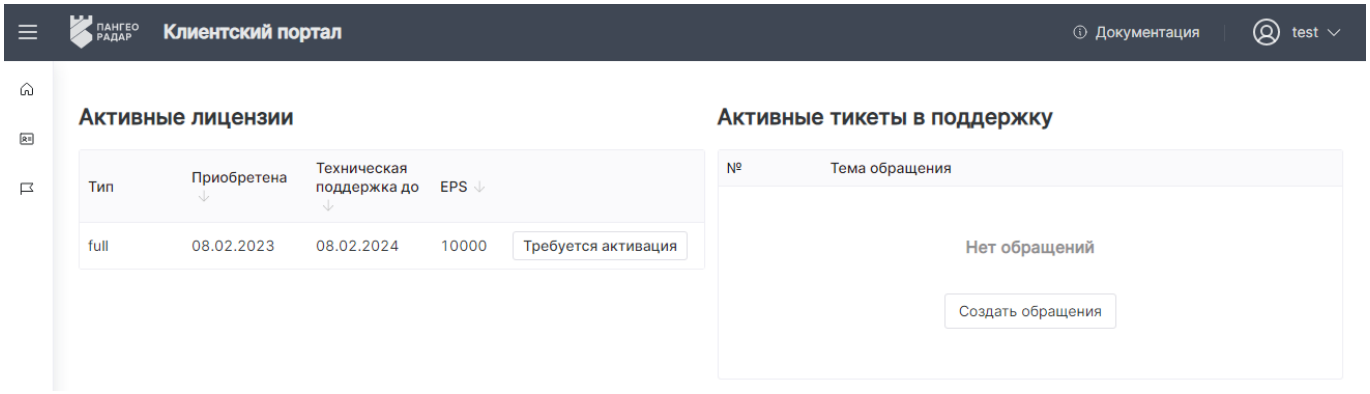

Рисунок 4 – Клиентский портал Платформы Радар

4. Нажмите на кнопку "**Требуется активация**". В появившемся окне укажите код активации и закройте окно. В личном кабинете клиентского портала **Платформы Радар** кнопка "**Требуется активация**" будет заменена на кнопку "**Лицензия**" (см. рисунок 5).

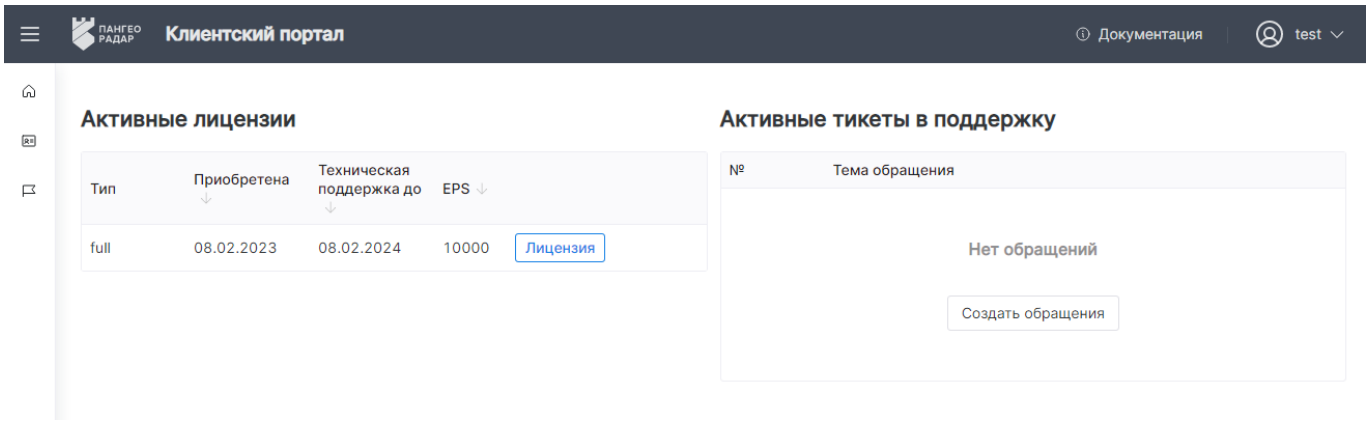

Рисунок 5 – Кнопка получения лицензии

5. Нажмите на кнопку "**Лицензия**", после чего откроется окно с кодом лицензии (см. рисунок 6). Скопируйте код лицензии в буфер обмена кнопкой "**Скопировать в буфер**".

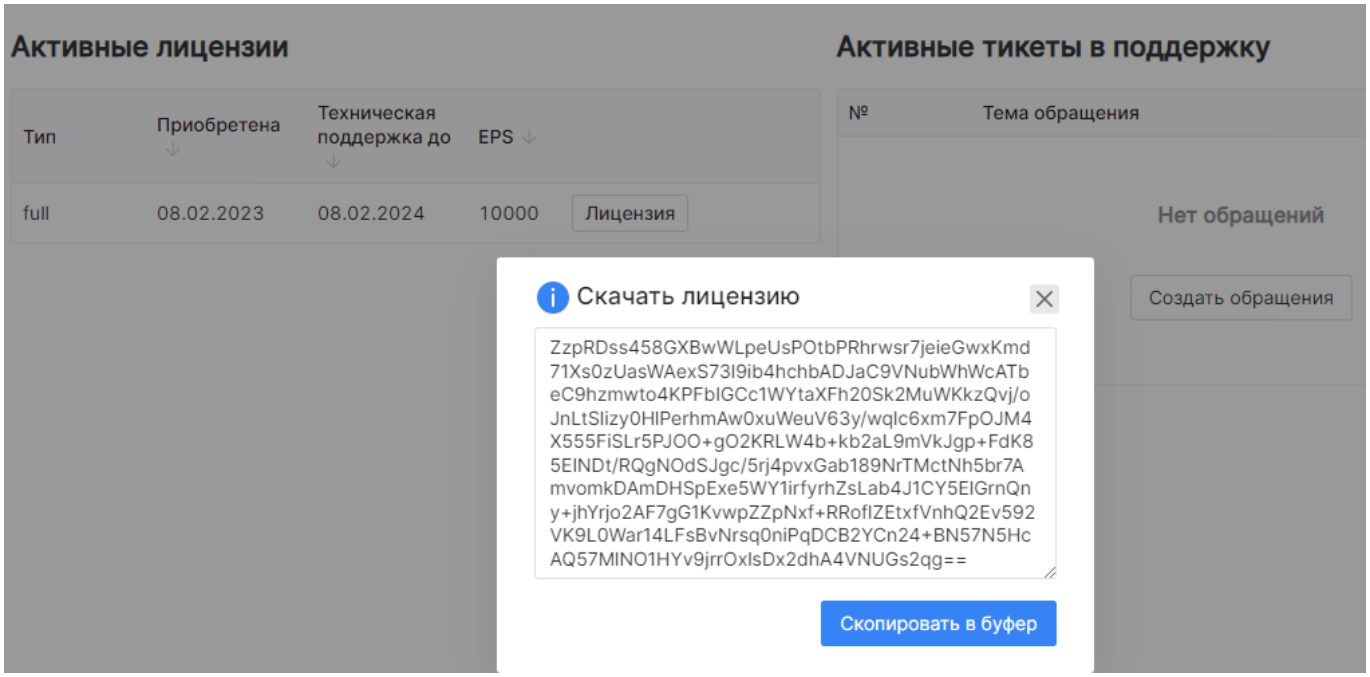

Рисунок 6 – Скачивание лицензии

6. Вернитесь к окну установки (см. рисунок 3). Вставьте код лицензии в окно "**Лицензия**" и нажмите кнопку "**Активировать**". Лицензия будет активирована, а на экране будут отображены ее параметры (см. рисунок 7).

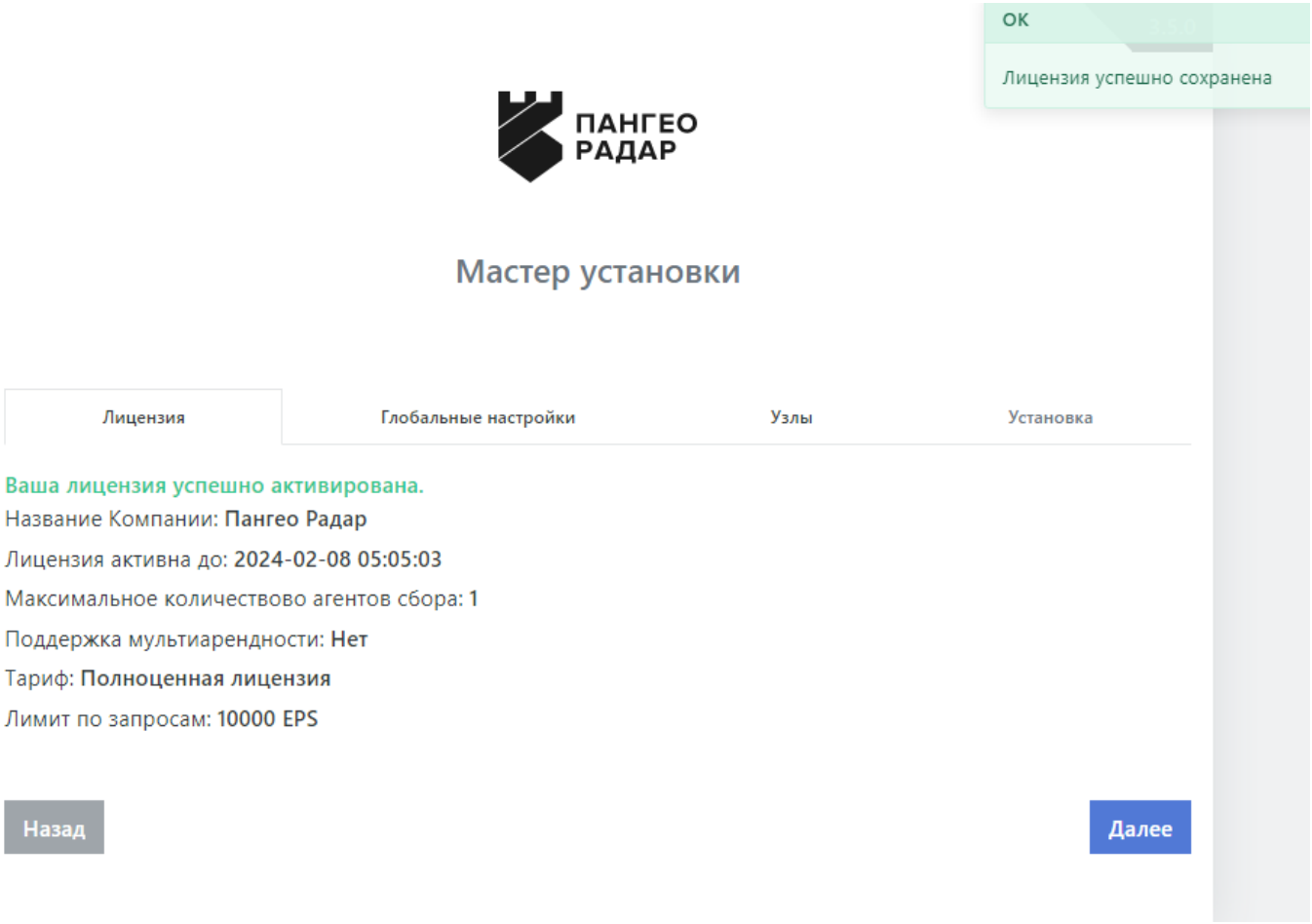

Рисунок 7 - Параметры лицензии

7. После активации лицензии нажмите кнопку далее, после чего будет отображен экран глобальных настроек (см. рисунок 8).

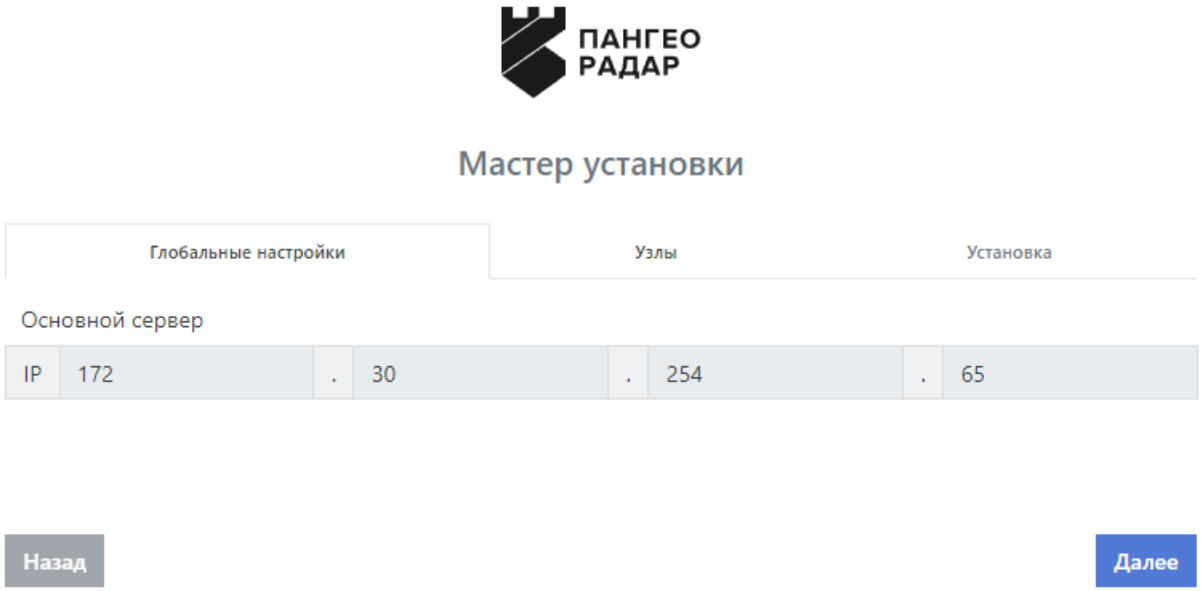

Рисунок 8 – Мастер установки платформы в веб-интерфейсе

8. На данном экране нажмите на кнопку "**Далее**" и перейдите на экран настройки узлов (см. рисунок 9).

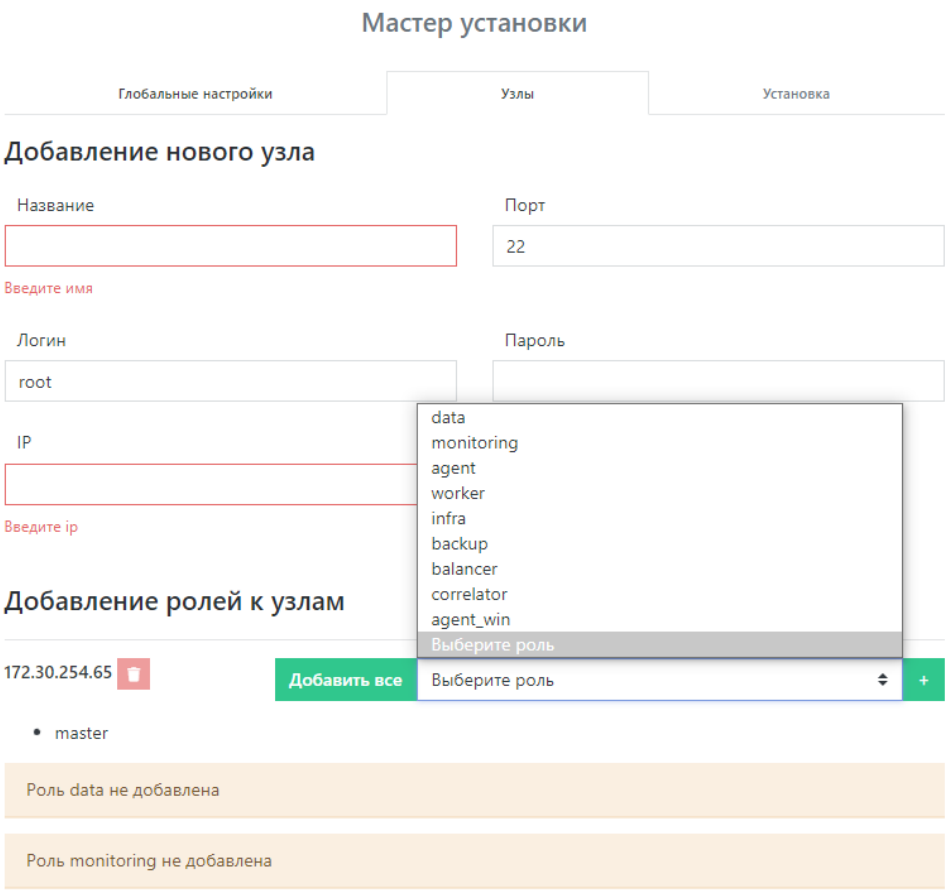

Рисунок 9 – Мастер установки. Настройка узлов платформы

9. В разделе настройки узлов в случае установки на один сервер необходимо назначить все возможные серверные роли с помощью кнопки "**Добавить все**".
10. Далее перейдите к шагу "**Установка**" нажатием кнопки "**Далее**".

2.4. Запуск установки

1. На экране старта установки (см. рисунок 10) нажмите на кнопку "**Начать установку**".

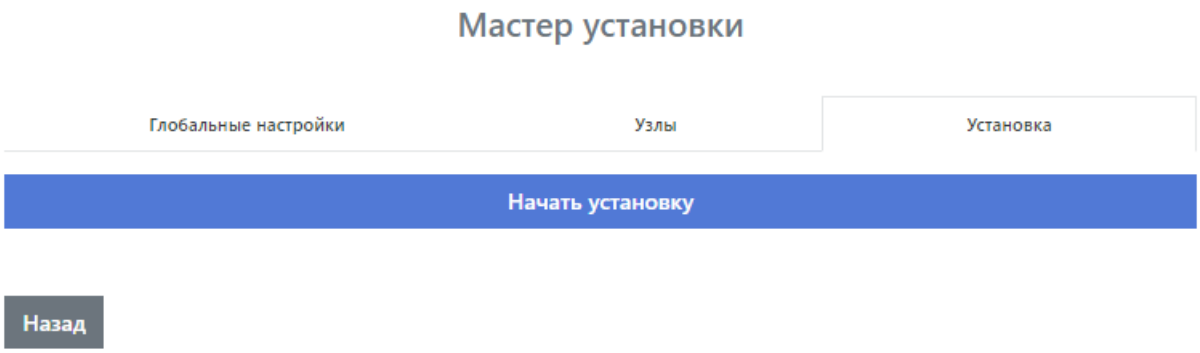

Рисунок 10 - Мастер установки. Экран старта установки

2. После этого станет доступен экран просмотра журнала установки (см. рисунок 11).

```
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2021-03-16 17:49:06 MSK; 55ms ago
     Docs: http://www.elastic.co
 Main PID: 28985 ((icsearch))
    Tasks: 0 (limit: 4915)
   CGroup: /system.slice/elasticsearch.service
           └─28985 (icsearch)

Mar 16 17:49:06 platform11.test.pgr.local systemd[1]: Started Elasticsearch.
done
wget alredy installed
Warning: apt-key output should not be parsed (stdout is not a terminal)
```

Рисунок 11 – Журнал установки

3. Установка занимает некоторое время. По завершению процесса установки откроется **Платформа Радар** в меню администрирования ***Кластер - Узлы системы - Проверка***.

На этом установка **Платформы Радар** завершена, можно переходить к этапу проверки работоспособности ПО.

2.5. Проверка работоспособности ПО

1. Для выполнения проверки необходимо перейти в меню администрирования "**Кластер**" (см. рисунок 12).

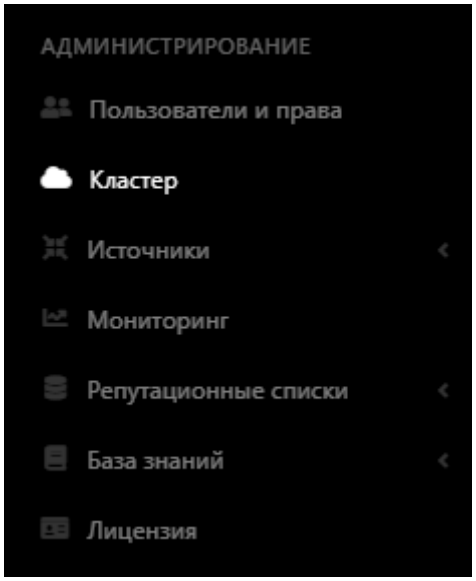

Рисунок 12 – Раздел управления кластером

2. Перейти на вкладку **Узлы системы - Проверка** и убедиться, что индикация всех сервисов подсвечена зеленым. Это означает, что все сервисы находятся в рабочем состоянии (см. рисунок 13).

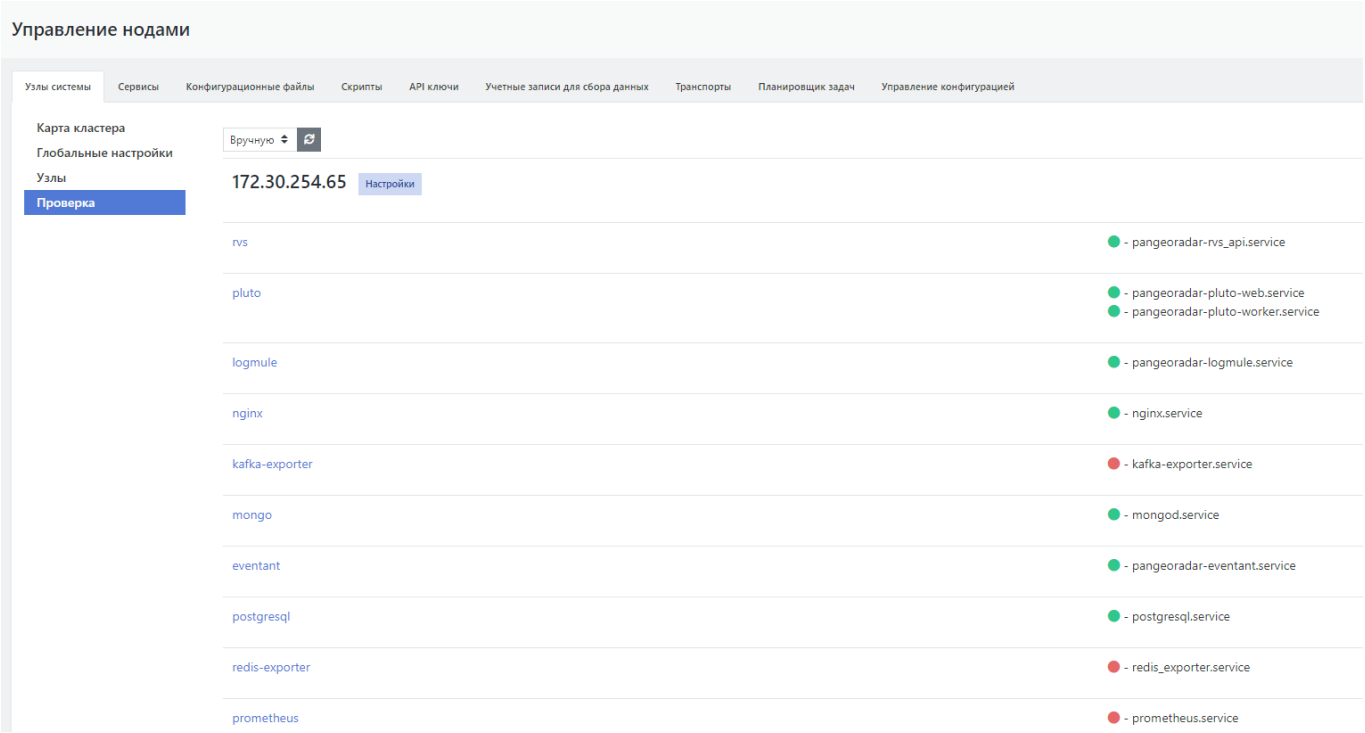

Рисунок 13 – Проверка сервисов

3. Для проверки состояния и просмотра событий сервиса необходимо нажать кнопку "**Настройки**" рядом с IP-адресом узла, на котором развернуты сервисы (см. рисунок 14).

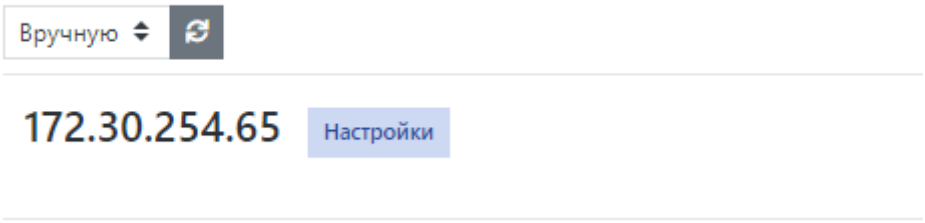

Рисунок 14 – Настройка узла (ноды)

4. На странице "**Управление хостом**" выбрать интересующий сервис и нажать кнопку "**Действия**" (см. рисунок 15).

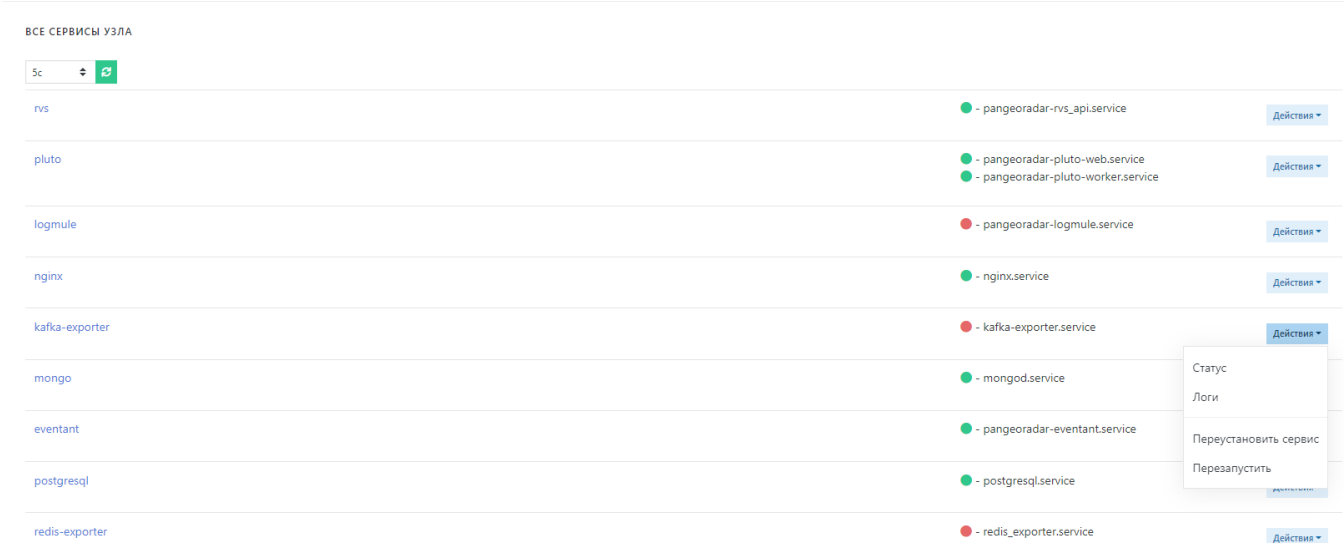

Рисунок 15 – Выбор действий

5. В выпадающем меню выбрать необходимый пункт:
   - Статус - выводит информацию о состоянии сервиса (см. рисунок 16);

Рисунок 16 – Окно с информацией о состоянии сервиса

   - Логи - выводит журнал событий сервиса (см. рисунок 17).

Рисунок 17 – Окно вывода событий сервиса

Если сервис подсвечен красным цветом, то это означает, что сервис не работает. Попробуйте выбрать пункт меню "**Перезапустить**" для перезапуска сервиса. Если это не помогает, выберите пункт "**Переустановить сервис**" для его переустановки.

Для получения подробной информации по решению проблем, связанных с работоспособностью **Платформы Радар** см. раздел «Решение проблем».

2.5.1 Первичное конфигурирование Платформы Радар

Первичное конфигурирование **Платформы Радар** включает создание и настройку следующих объектов:

- пользователи;
- группы пользователей;
- группы активов.

Подробное описание по созданию и настройке объектов приведено в документе «Руководство администратора».

2.5.2 Синхронизация с Базой Знаний

Для синхронизации с Базой Знаний выполните следующие действия:

1. Перейдите в раздел ***Центр управления - Параметры - Параметры*** и выберите вкладку "**Синхронизация с Базой Знаний**".
2. Нажмите на кнопку "**Синхронизация типов инцидентов**" (см. рисунок 18).

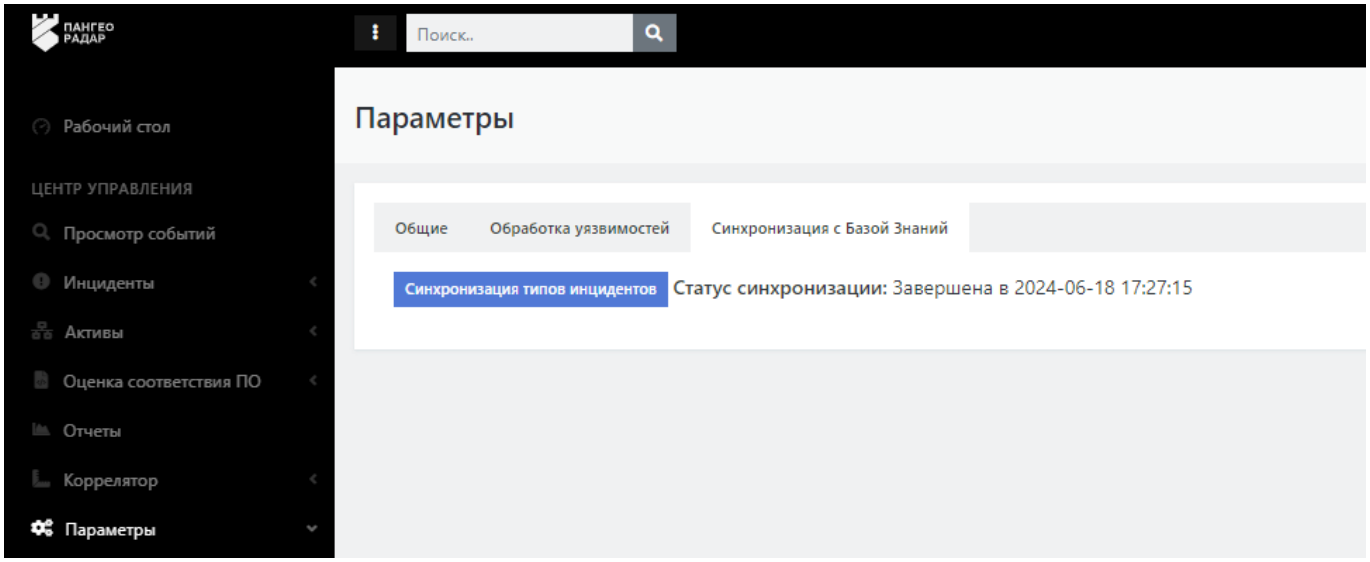

Рисунок 18 – Вкладка "Синхронизации с Базой Знаний"

2.6. Возможные проблемы

После первичной установки некоторые компоненты могут иметь отрицательное состояние доступности.

Для устранения проблем с сервисом **RADAR-TERMITE** включите необходимые типы источников (см. «**Руководство по подключению источников**» → «**Работа с пассивными источниками событий**»).

Для устранения проблем с неработающим сервисом (такой сервис выделен красным) выполните следующие действия:

1. Перейдите в раздел "**Кластер**";
2. На вкладке ***Узлы системы - Узлы*** кликните на IP-адрес узла, на котором располагается неработающий сервис (см. рисунок 19);

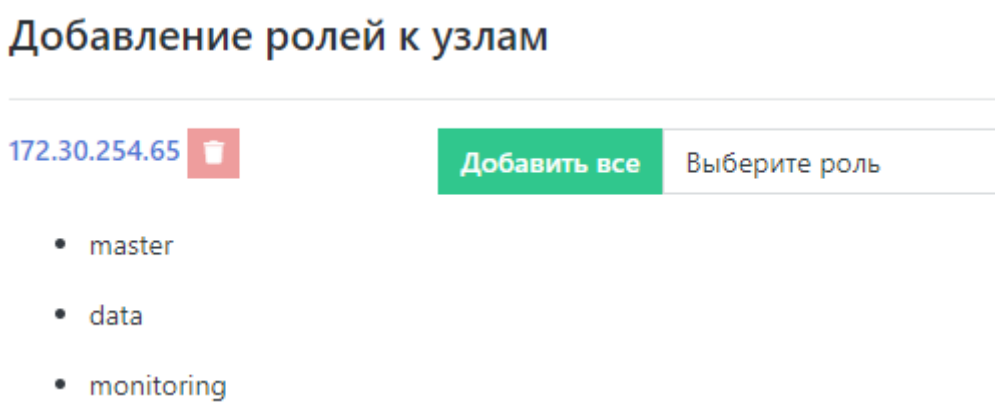

Рисунок 19 – Выбор узла

3. На панели "**Все сервисы узла**" найти неработающий сервис и нажать кнопку "**Действия**". В выпадающем меню выбрать пункт "**Перезапустить**". Если перезапуск сервиса не помог, выберите пункт "**Переустановить сервис**" (см. рисунок 20).

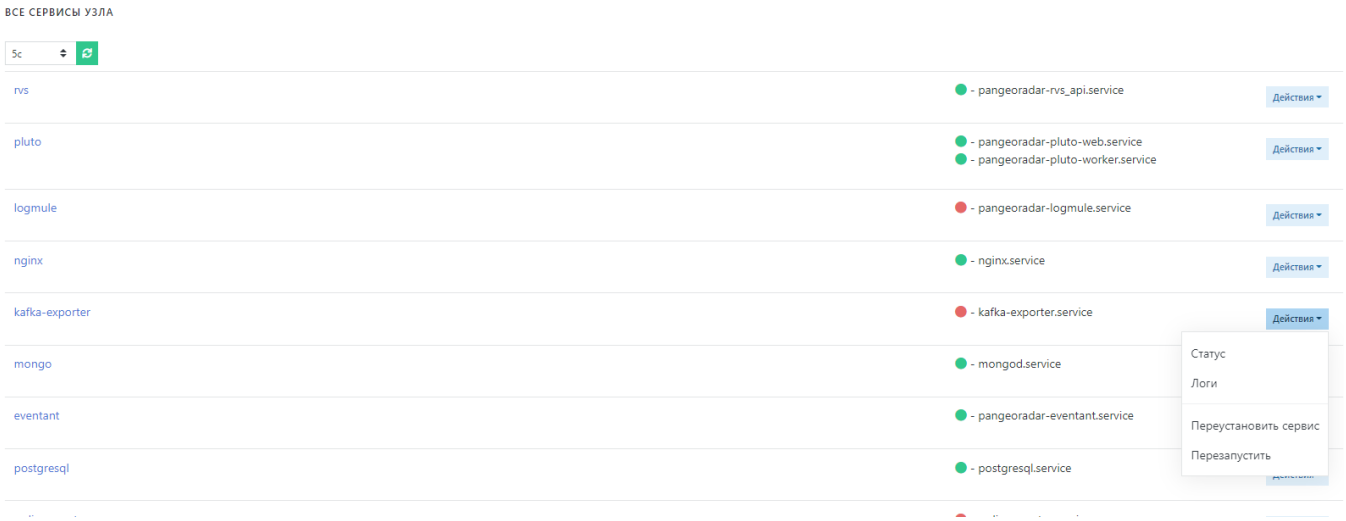

Рисунок 20 – Все сервисы узла

Успешное завершение процесса развертывания, выполнение проверочных мероприятий, конфигурирование **Платформы Радар** и синхронизация с Базой Знаний позволят начать целевую эксплуатацию функционала **Платформы Радар**.

В ходе эксплуатации **Платформы Радар** необходимо руководствоваться документами «**Руководство администратора**» и «**Руководство оператора**».

3. Особенности распределенной установки

3.1. Особенности подготовки оборудования

Подготовка оборудования для распределенной установки **Платформы Радар** производится аналогично подготовке оборудования для централизованной установки (см. раздел «Подготовка к установке»), кроме задач подготовки дисковой системы и настройки сетевых конфигураций.

3.1.1 Подготовка дисковой системы к распределенной установке

Для распределенной установки при разметке дисковой подсистемы для всех серверных ролей, кроме серверной роли DATA, необходимо учитывать следующие (стандартные) требования:

- корневой раздел (/) - все свободное пространство;
- раздел /home - 10 Гб;
- раздел swap - не менее 10% от общего объема оперативной памяти;
- тип файловой системы - XFS (при необходимости можно использовать EXT4).

Для серверной роли DATA необходимо провести процедуру разметки дисковой подсистемы Хранение данных, которая приведена в «**Администратор**» → «**Процессы работы**» → «**Подготовка дисковой подсистемы для реализации роли DATA»**.

3.1.2 Настройка сетевой конфигурации при распределенной установке

1. Для доступа к веб-интерфейсам управления **Платформой Радар** нужно открыть порты:
    - 9000
    - 8080
    - 8180
2. Между узлами кластера необходимо разрешить взаимодействие в обе стороны по следующим портам:
    - 9092
    - 9200
    - 5672
    - 15672
    - 5432
    - 2092
    - 8080
    - 8086
    - 9000
    - 8180
    - 6677

- 6630
- 22

Ниже в таблице приведены необходимые сетевые настройки при распределенной установке **Платформы Радар** (независимо от вариантов распределенной установки):

Исходящий	**Входящий**	**Порты**	**Описание**
Correlator	Master	5672	Чтение нормализованных событий из очереди для корреляции
Correlator	Master	8086	Передача результатов корреляции
Log-Collector	Balancer	1500-5000, 9997-9999, 15403, 15404TCP/UDP	Передача данных от сборщика в балансировщик и менеджер очередей
Log-Collector	Источники событий	21, 22, 135, 445, 1443, 3306, 5432, 5601	Активный сбор событий
Log-Collector	Log-Collector	4813	Взаимодействие между двумя сборщиками
Log-Collector	Master	9000	Запрос конфигурационных данных
Master	Data	9200	Работа с сырыми событиями
Master	Correlator	2092	Управление правилами корреляции
Master	Log-Collector	4805 4806	Мониторинг и сбор статистики. Управление сборщиком событий API
Master	Balancer Correlator Data Worker	6676	Управление агентами кластера
Master	Balancer Correlator Data Worker	9100	Мониторинг и сбор статистики
Master	Balancer	9292, 9308	Мониторинг и сбор статистики
Master	Data	9114	Мониторинг и сбор статистики
Worker	Balancer	9092	Чтения событий из менеджера очередей для их обработки
Worker	Master	5672	Передача нормализованных событий в очередь на корреляцию
Worker	Data	9200	Передача событий на хранение
Источники событий	Log-Collector	162 SNMP trap; 4807 UDP receiver; 4808 TCP receiver; 4809 TCP receiver SSL/TLS; 4810 HTTP receiver; 4811 HTTPS receiver; 4812 NetFlow reciever	Пассивный сбор событий

Исходящий	Входящий	Порты	Описание
Пользователи Платформы Радар	Master	8080 9000 6676 6677	Доступ к интерфейсу Платформы Радар, проверка API ключей
Data (с ролью Master)	Data (с ролью Data)	9300	Взаимодействие между нодами в кластере хранилища данных

Также подробное описание сетевого взаимодействия для различных вариантов установки приведено в руководстве «**Администратор**» → «**Процессы работы**» → «**Перечень используемых Платформой Радар портов**».

3.2. Распределенная установка

3.2.1 Подготовка установочных файлов Платформы Радар

Подключитесь к серверу, на который планируется установка **Платформы Радар**.

Внимание! *Для запуска установки необходимо получить права суперпользователя*.

Скопируйте с оптического диска установочный архив и поместите его в каталог `/var/tmp`.

Перейдите в каталог `/var/tmp`:

```
cd /var/tmp/
```

Командой `ls` убедитесь, что установочный архив успешно загружен и находится в каталоге `/var/tmp` (см. рисунок 21).

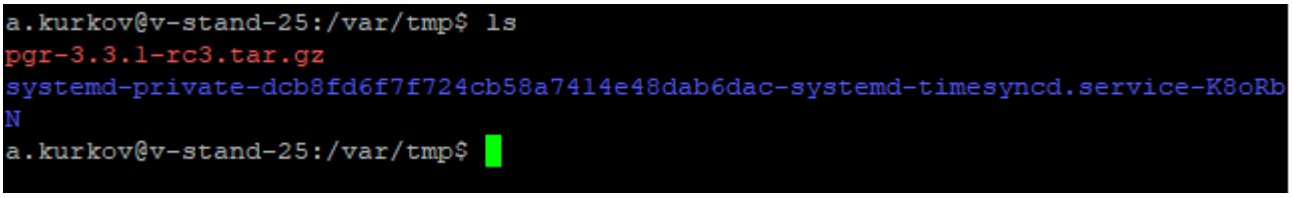

Рисунок 21 – Проверка установочного архива

Если получен зашифрованный архив (файл с расширением `*.enc`), выполните команду для расшифровки:

```
openssl enc -aes-256-cbc -d -in pgr-RELEASE_VERSION-INSTALLATION_TYPE.tar.gz.enc |
tar xz
```

Если получен незашифрованный архив (файл с расширением `*.tar.gz`), выполните команду для разархивирования:

```
tar -zxvf pgr-RELEASE_VERSION-INSTALLATION_TYPE.tar.gz
```

Где название архива **pgr-RELEASE_VERSION-INSTALLATION_TYPE.tar.gz.enc** содержит:

- RELEASE_VERSION - номер версии релиза **Платформы Радар** (например, 3.3.1);
- INSTALLATION_TYPE - тип установки (online или offline).

Командой `ls` убедитесь, что установочный скрипт `install.sh` расположен в директории `/var/tmp/` после распаковки установочного архива.

3.2.2 Продолжение установки в веб-интерфейсе

1. После перехода по адресу, указанному в конце работы инсталлятора, необходимо пройти процедуру авторизации и смены пароля по умолчанию: `admin`/`admin`.
2. После прохождения авторизации станет доступен этап получения лицензии (см. пункты 2-6 раздела «Продолжение установки в веб-интерфейсе»).
3. После активации лицензии нажмите кнопку далее, после чего будет отображен экран глобальных настроек (см. рисунок 22).

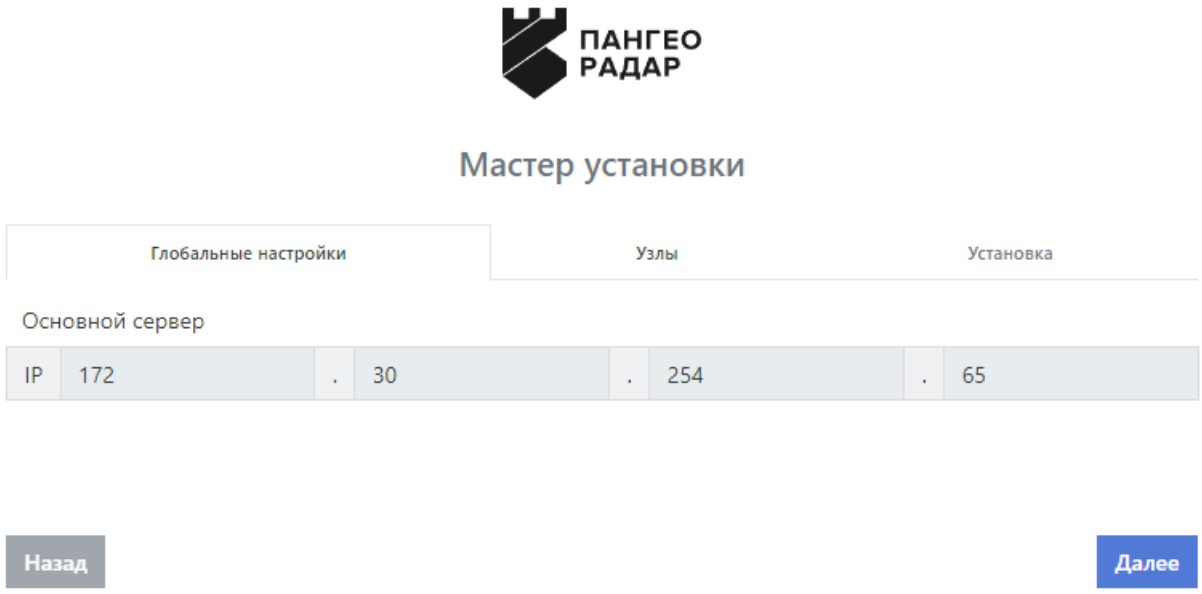

Рисунок 22 – Мастер установки платформы в веб-интерфейсе

4. На данном экране нажмите на кнопку "**Далее**" и перейдите на экран настройки узлов (см. рисунок 23).

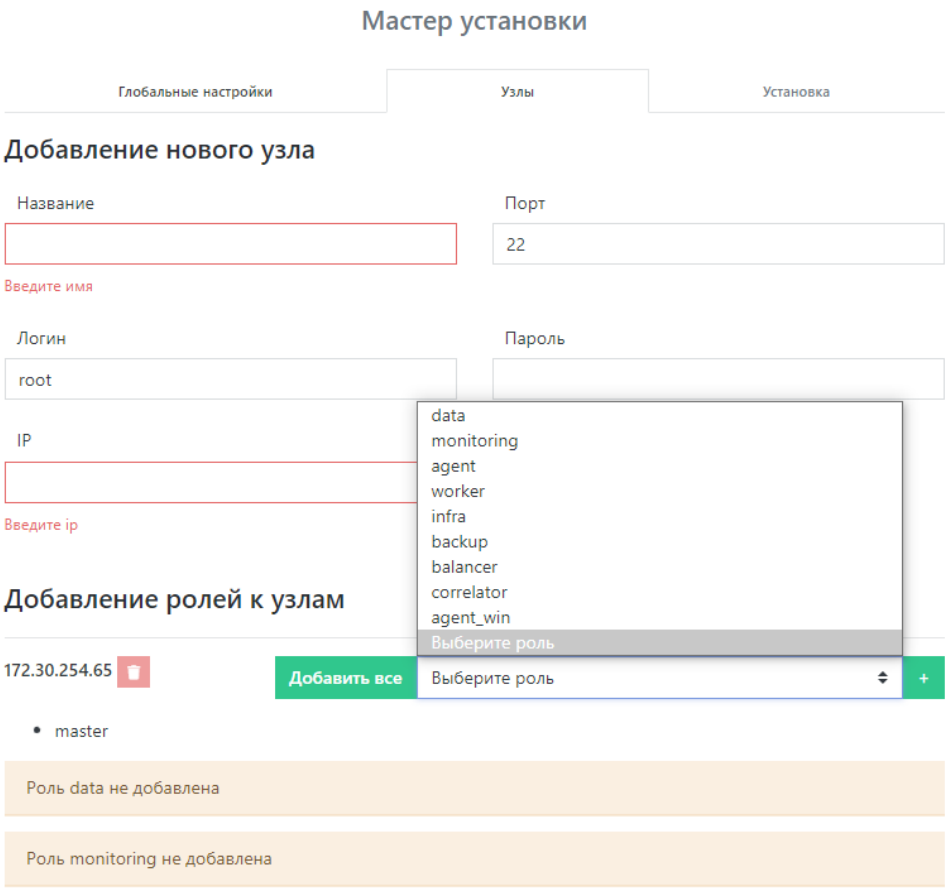

Рисунок 23 – Мастер установки. Настройка узлов платформы

5. При выполнении распределенной инсталляции **Платформы Радар** сначала необходимо добавить все узлы кластера через форму "**Добавления нового узла**" (см. рисунок 24):

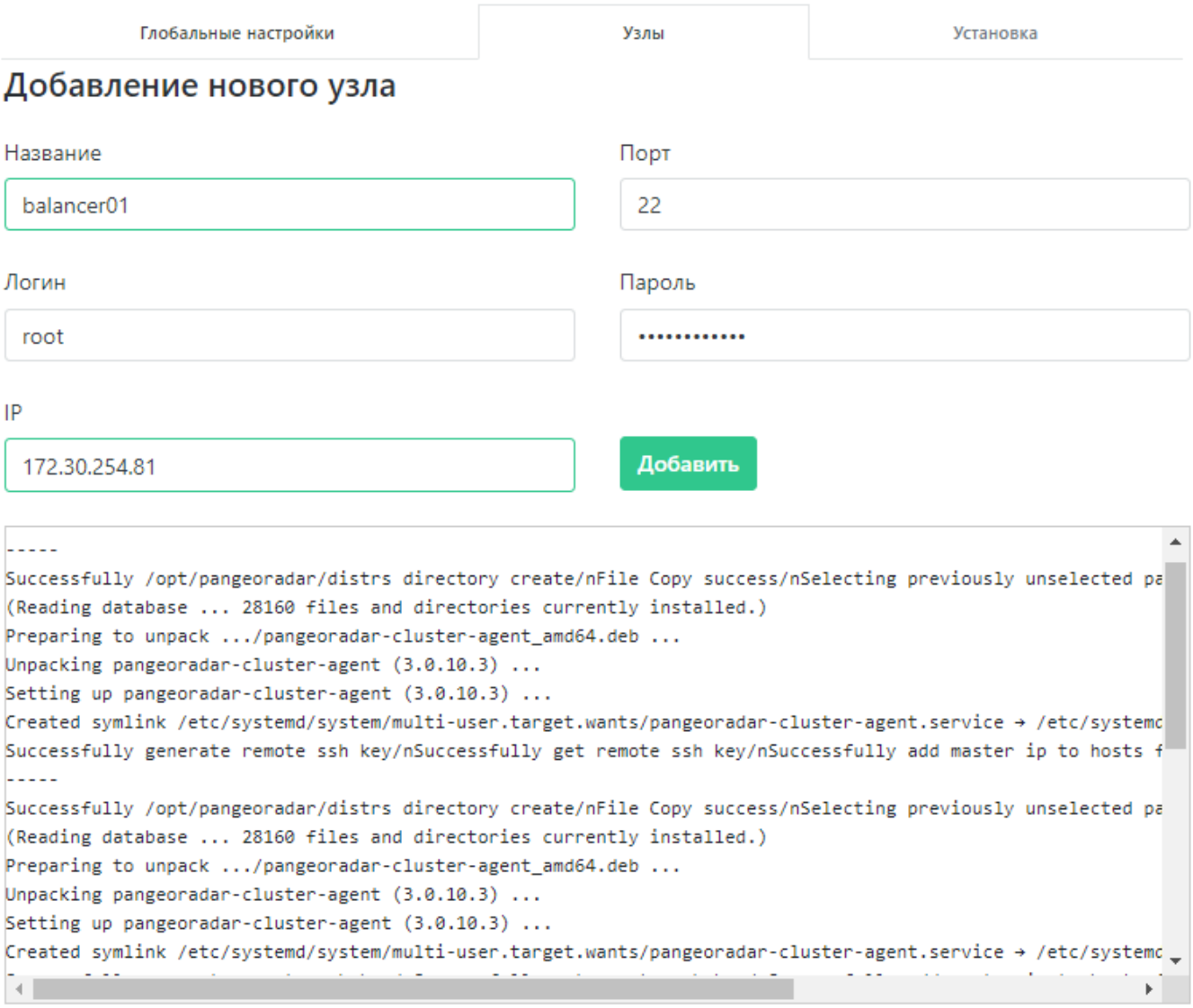

Рисунок 24 – Добавление нового узла

6. После чего назначьте серверные роли согласно архитектуре проектного решения (см. рисунок 25).

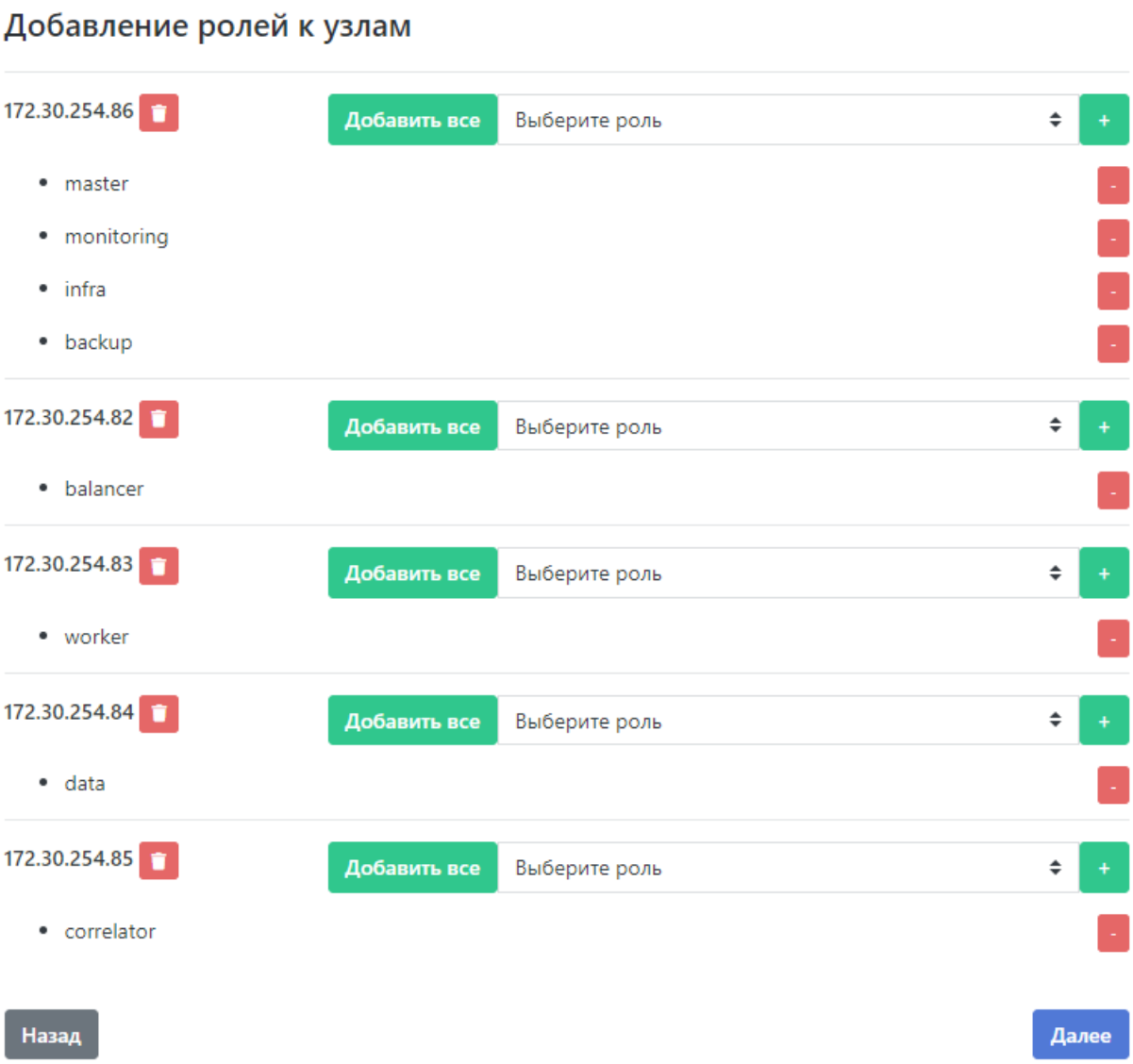

Рисунок 25 – Добавление ролей к узлам

7. Далее перейдите к шагу "**Установка**" нажатием кнопки "**Далее**".

3.2.3 Запуск установки ролей Платформы Радар

1. На экране старта установки (см. рисунок 26) нажмите на кнопку "**Начать установку**"..

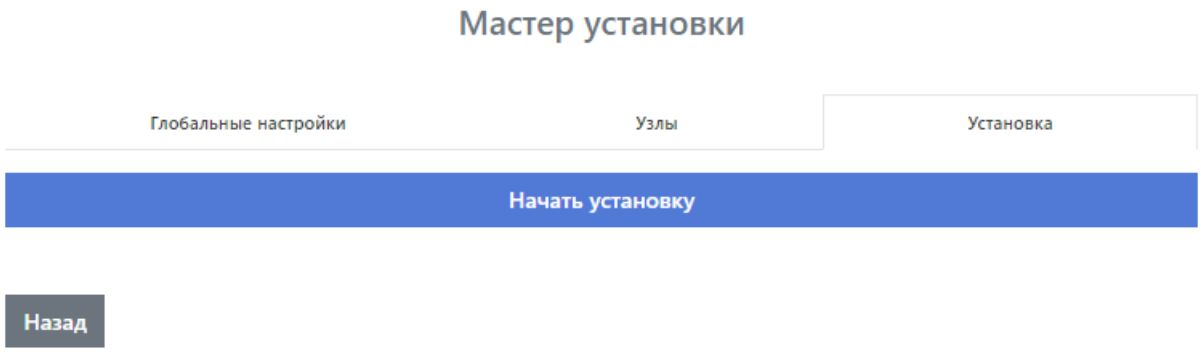

Рисунок 26 - Мастер установки. Экран старта установки

2. После этого станет доступен экран просмотра журнала установки (см. рисунок 27).

```
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2021-03-16 17:49:06 MSK; 55ms ago
     Docs: http://www.elastic.co
 Main PID: 28985 ((icsearch))
    Tasks: 0 (limit: 4915)
   CGroup: /system.slice/elasticsearch.service
           └─28985 (icsearch)

Mar 16 17:49:06 platform11.test.pgr.local systemd[1]: Started Elasticsearch.
done
wget alredy installed
Warning: apt-key output should not be parsed (stdout is not a terminal)
```

Рисунок 27 – Журнал установки

3. Установка занимает некоторое время. По завершению процесса установки откроется **Платформа Радар** в меню администрирования ***Кластер - Узлы системы - Проверка***.

На этом установка **Платформы Радар** завершена, далее идет этап проверки работоспособности.

3.3. Проверка распределенной установки и работоспособности ПО

Для проверки наличия распределенной установки и работоспособности ПО выполните следующие действия:

1. Зайдите в графический интерфейс **Платформы Радар** с правами администратора.
2. Перейдите в раздел ***Администрирование - Кластер - Узлы системы - Узлы*** (см. рисунок 28).

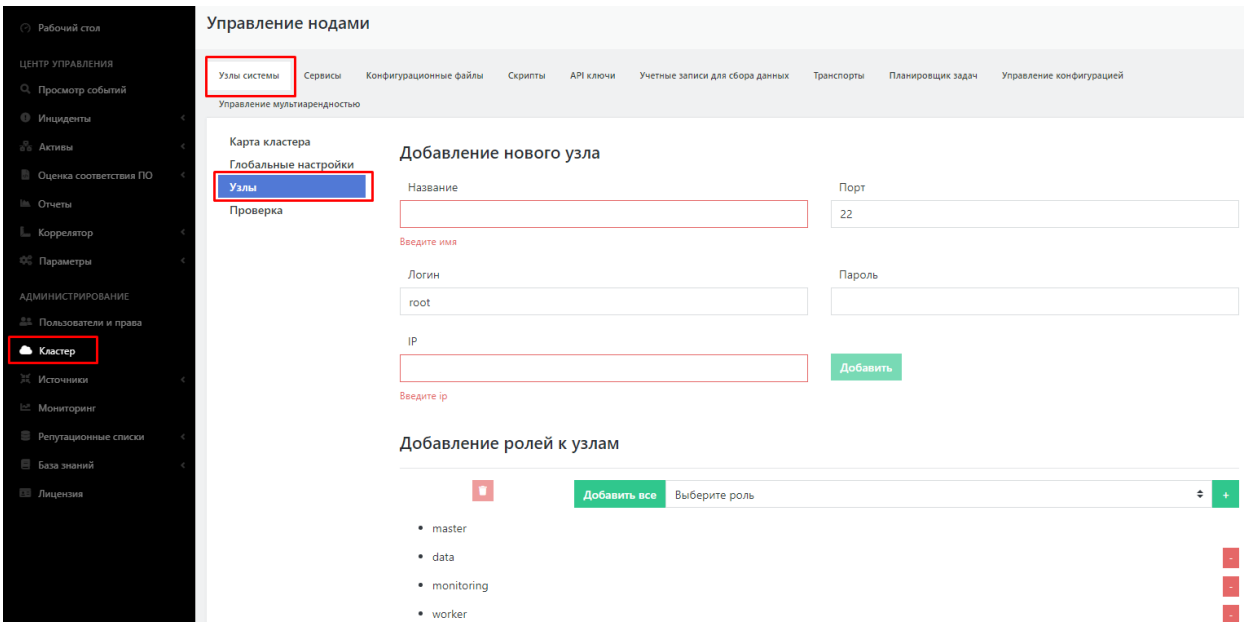

Рисунок 28 – Раздел управления кластером

3. Убедитесь, что узлов в составе **Платформы Радар** больше одного, роли распределены по узлам (см. рисунок 29).

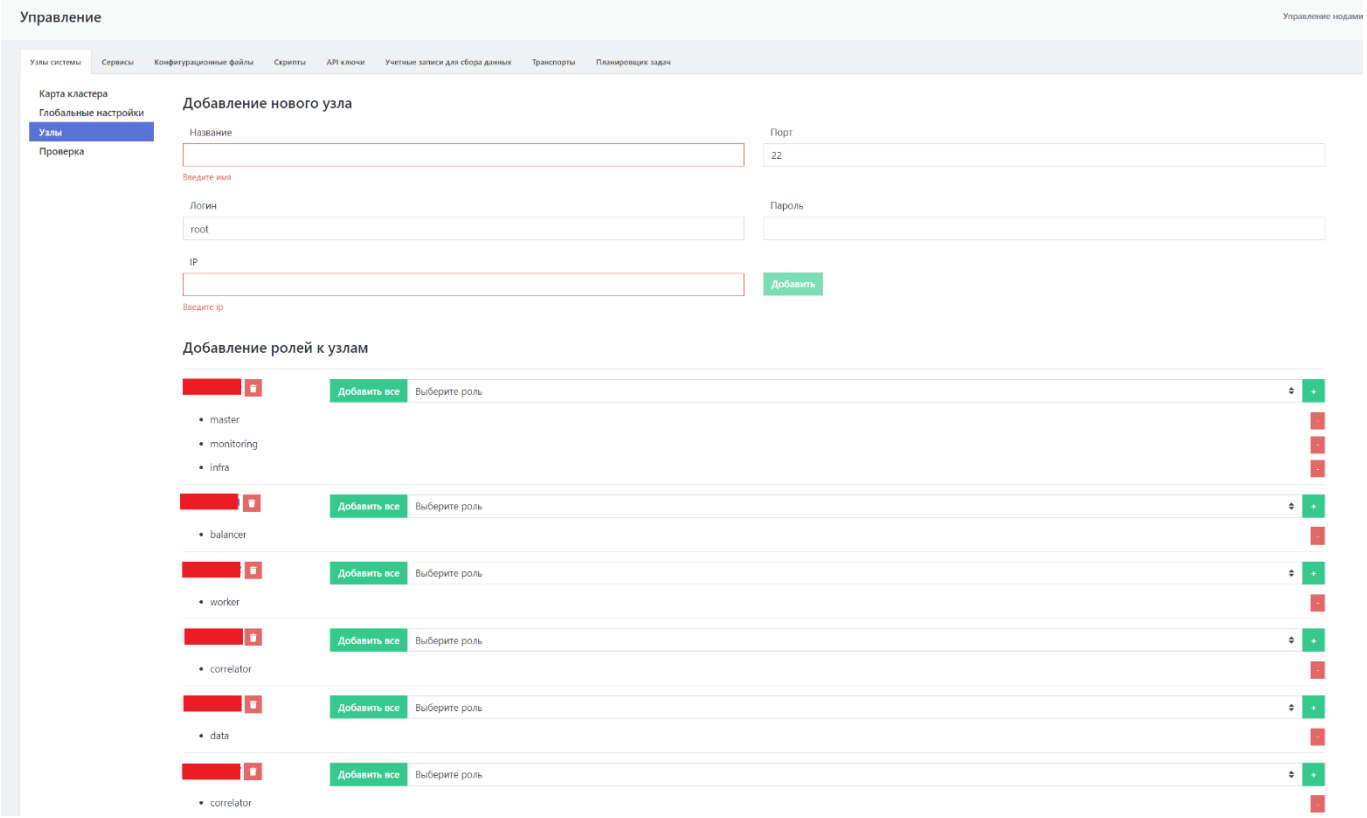

Рисунок 29 – Список узлов платформы с указанием ролей

4. Перейдите на вкладку ***Узлы системы - Проверка*** (см. рисунок 30). Убедитесь, что список узлов и их ролей, совпадает с тем, что было задано при распределенной установке и настройке **Платформы Радар**, и на всех узлах индикация всех сервисов подсвечена зеленым, т.е. все сервисы находятся в рабочем состоянии.

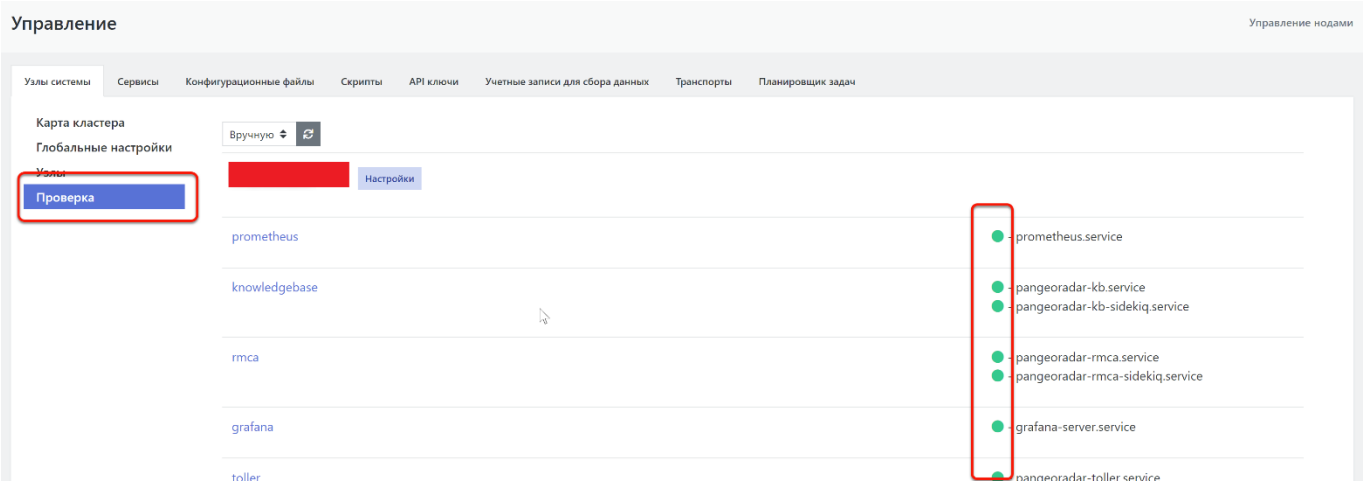

Рисунок 30 - Проведение проверки сервисов, установленных на узлах Платформы Радар

5. Выберите один из узлов, например *balancer*, и нажмите кнопку "**Настройки**", расположенную справа от названия узла. Откроется страница управления узлом и списком всех сервисов, установленных на данном узле (см. рисунок 31).

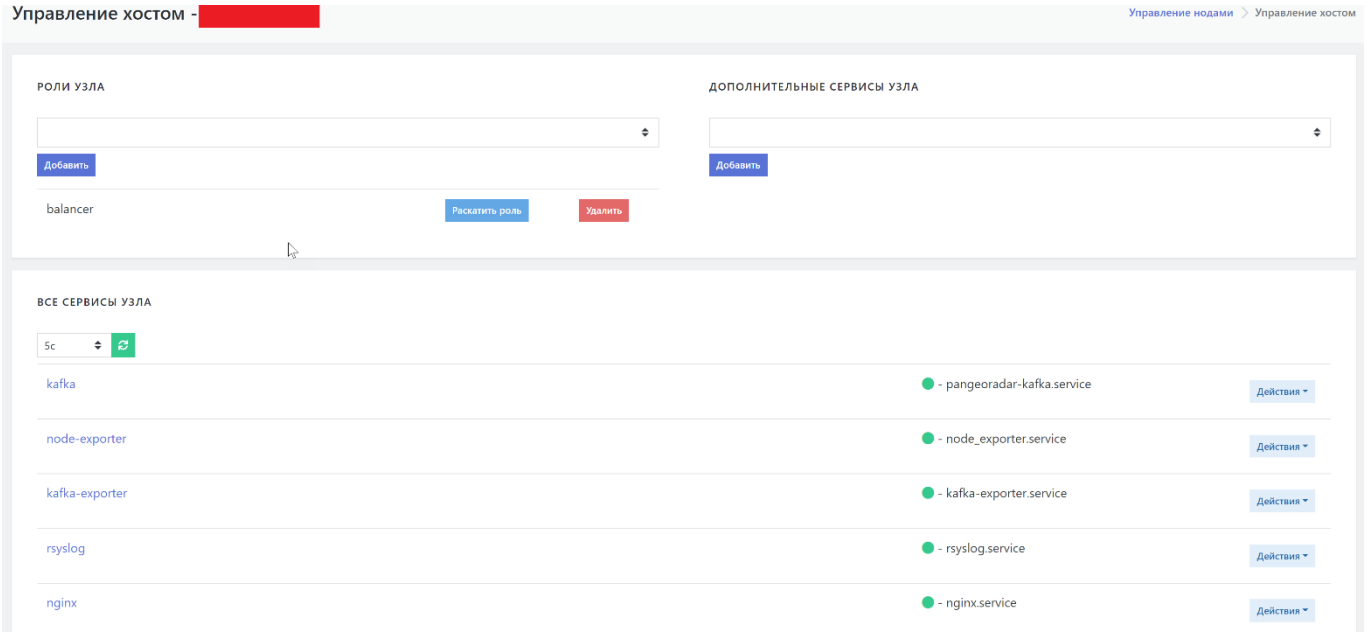

Рисунок 31 – Страница «Управление хостом»

6. На странице "**Управление хостом**" выберите интересующий сервис, например, kafka, и нажмите кнопку "**Действия**". В раскрывшемся списке выберите "**Статус**" (см. рисунок 32).

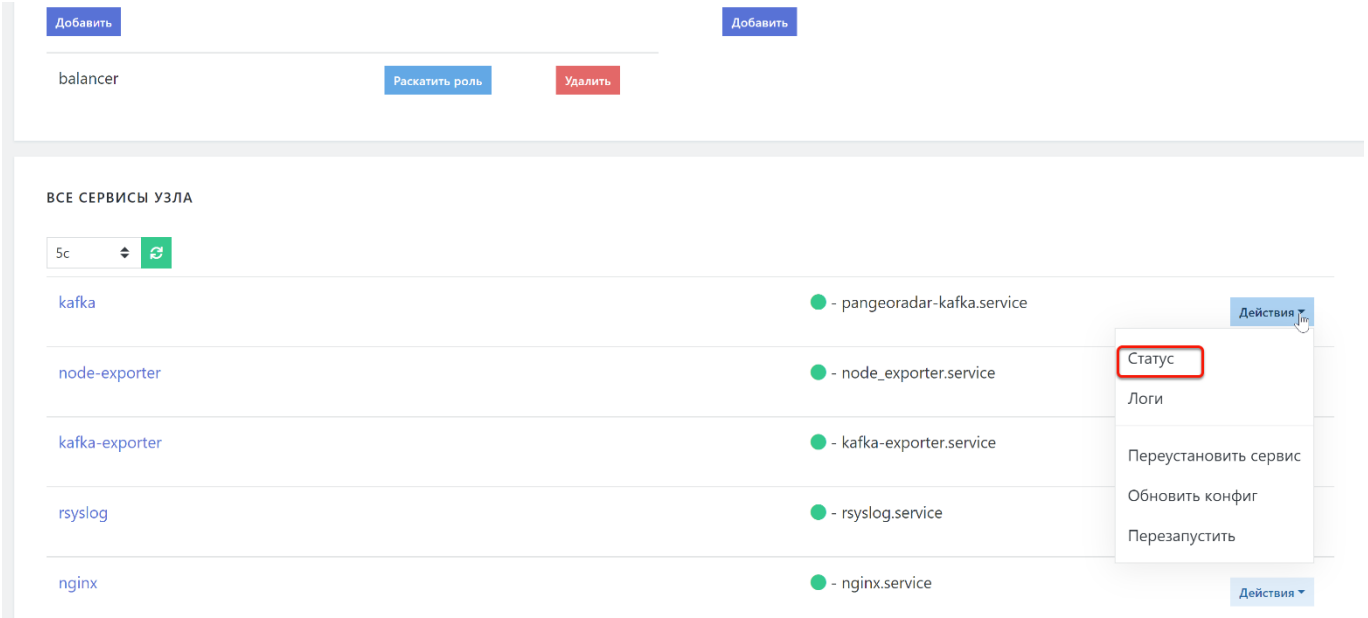

Рисунок 32 – Выбор действия с компонентом

При выборе действия "**Статус**" на экран выводится информация о состоянии сервиса (см. рисунок 33).

Рисунок 33 – Информация о состоянии сервиса

7. В раскрывшемся списке "**Действия**" выберите "**Логи**" (см. рисунок 32).

   При выборе действия "**Логи**" на экран выводится журнал событий сервиса (см. рисунок 34).

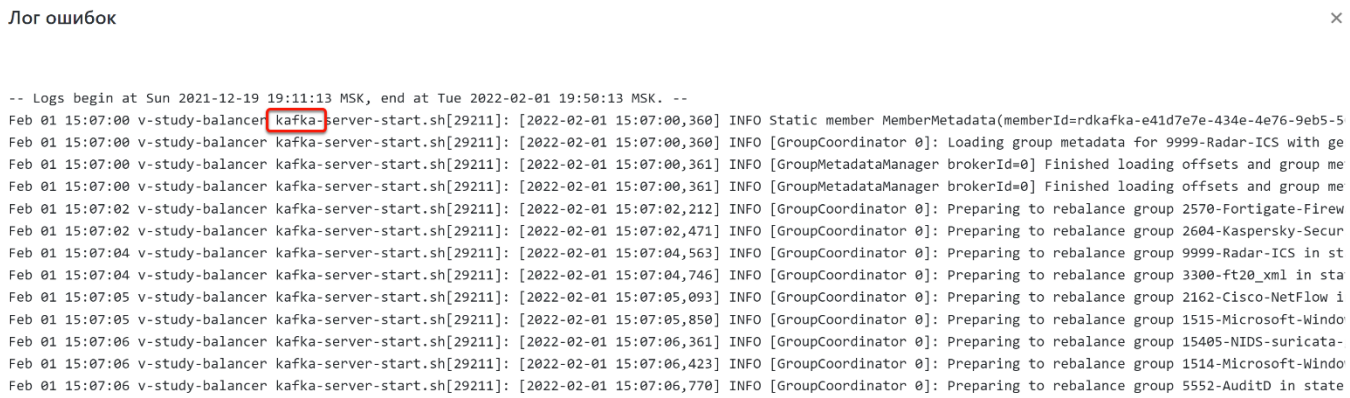

Рисунок 34 – Журнал событий сервиса

Для подтверждения достоверности информации, полученной через веб-интерфейс **Платформы Радар**, можно подключиться удаленно по SSH к выбранному ранее для проверки узлу (*balancer*) и выполнить команду:

`service pangeoradar-kafka status` (указать сервис, который был выбран в ГПИ для проверки, в данном случае kafka)

В результате выполнения команды в окне терминала должна отобразиться та же информация о сервисе, что и в окне веб-интерфейса при выборе действия "Статус".

Далее выполните команду: `ip a`.

Полученный в результате выполнения команды IP-адрес должен совпадать с IP-адресом в веб-интерфейсе.

3.3.1 Первичное конфигурирование Платформы Радар

Первичное конфигурирование **Платформы Радар** включает создание и настройку следующих объектов:

- пользователи;
- группы пользователей;

- группы активов.

Подробное описание по созданию и настройке объектов приведено в документе «Руководство администратора».

3.3.2 Синхронизация с Базой Знаний

Для синхронизации с Базой Знаний выполните следующие действия:

1. Перейдите в раздел ***Центр управления - Параметры - Параметры*** и выберите вкладку "**Синхронизация с Базой Знаний**".
2. Нажмите на кнопку "**Синхронизация типов инцидентов**"см. рисунок 35).

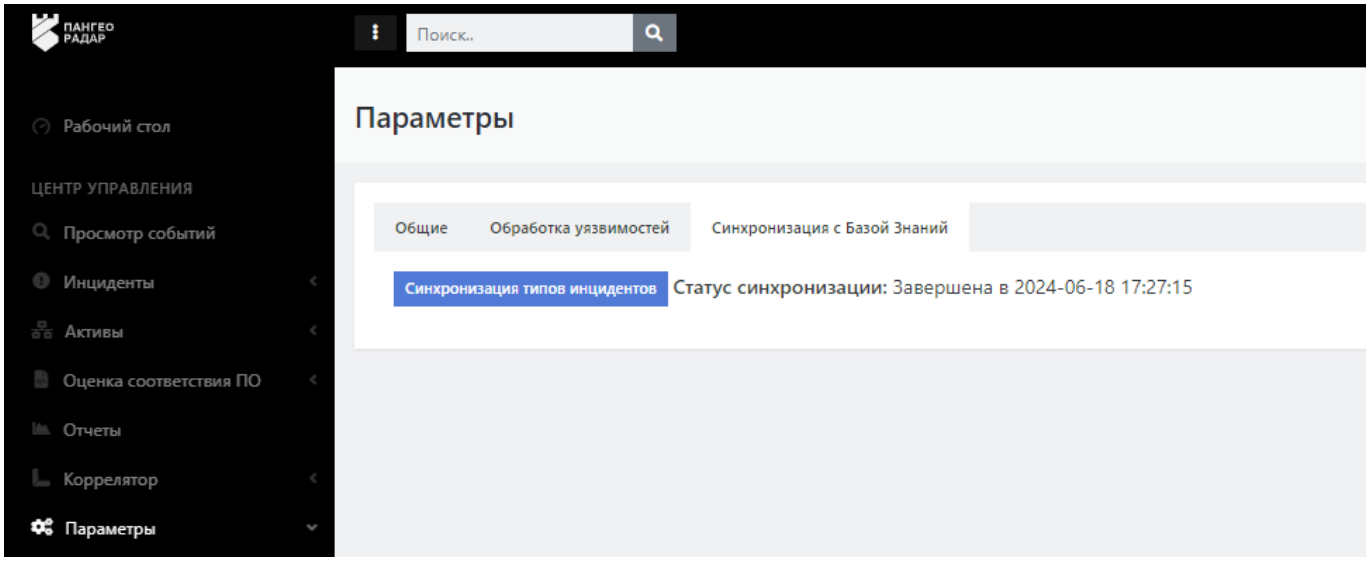

Рисунок 35 – Синхронизация с базой знаний

3.3.3 Добавление нового узла кластера

При необходимости расширения производительных возможностей **Платформы Радар** существует возможность добавить дополнительный экземпляр узла с той или иной ролью.

1. Для этого перейдите в меню администрирования ***Кластер - Узлы системы - Узлы***, заполните форму добавления узла и добавьте к узлу необходимую роль (см. рисунок 36).

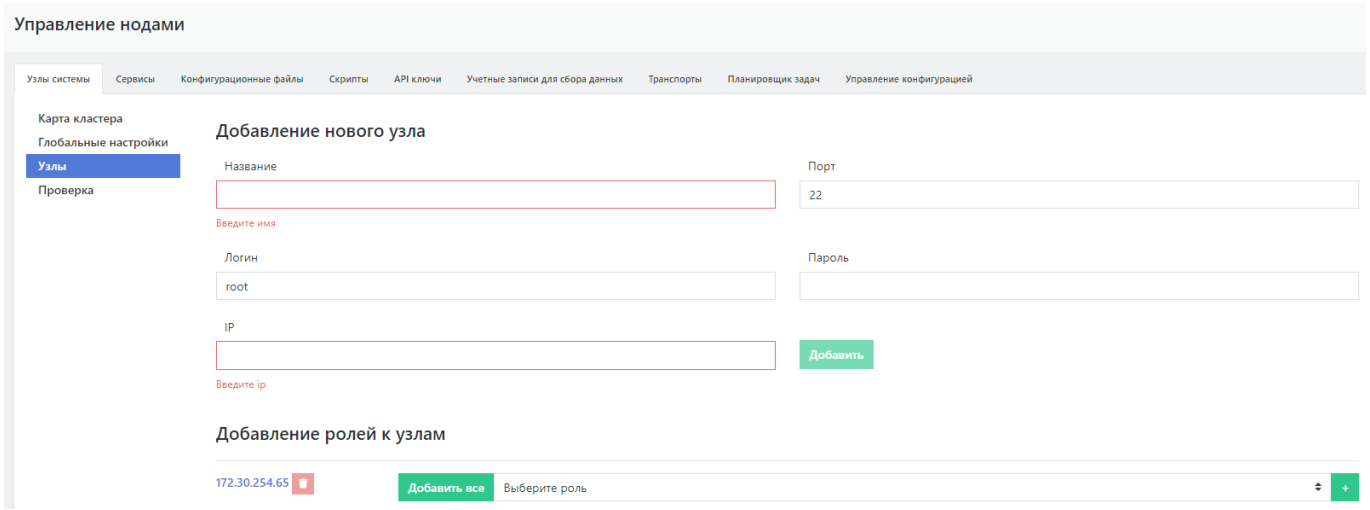

Рисунок 36 – Добавление нового узла кластера

2. Далее - перейдите в настройки созданного узла кластера, для этого необходимо нажать на IP-адрес этого узла (см. рисунок 37).

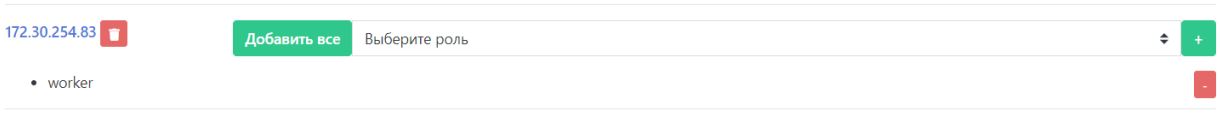

Рисунок 37 – Созданный узел кластера

3. В настройках созданного узла нажмите на кнопку "**Раскатить роль**" напротив добавленной роли (см. рисунок 38).

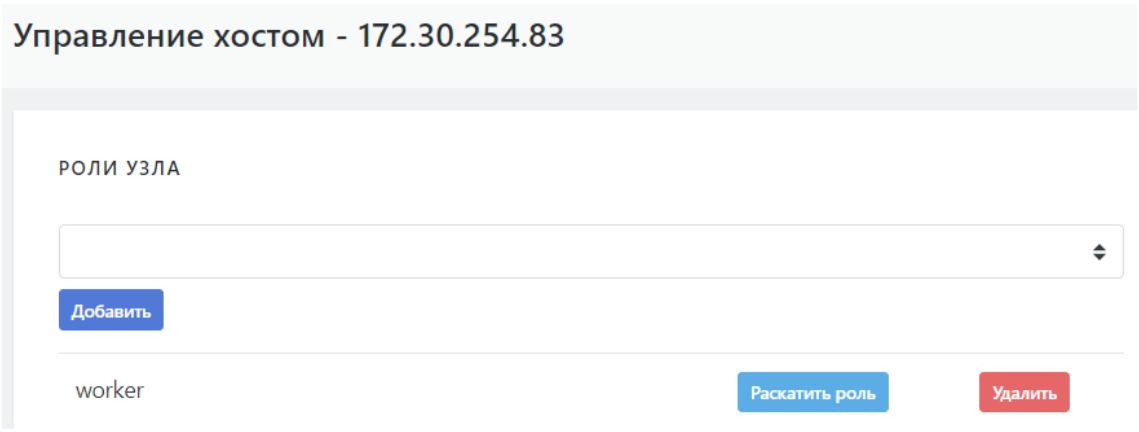

Рисунок 38 – Установка роли на новый узел кластера

4. После чего начнется установка сервисов роли с отображением журнала установки (см. рисунок 39).

Рисунок 39 – Процесс установки роли

5. По завершению установки нажмите кнопку "**Установка завершена, закрыть окно**", перейдите в раздел ***Кластер - Узлы системы - Глобальные настройки*** и нажмите кнопку "**Обновить конфигурационные файлы**" (см. рисунок 40).

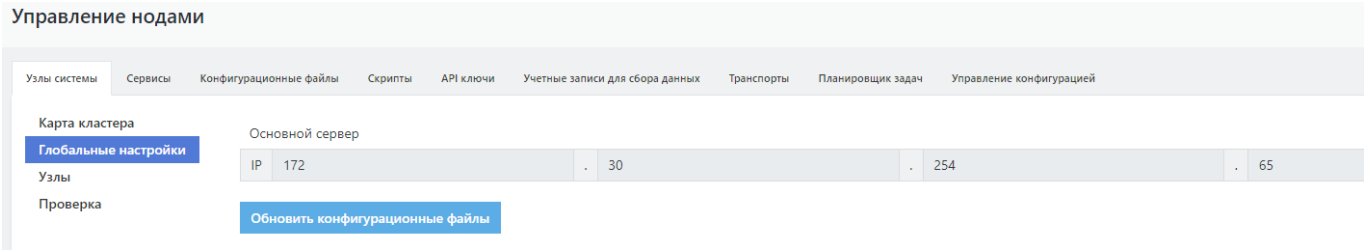

Рисунок 40 – Синхронизация конфигурационных файлов

6. На этом процесс добавления нового узла кластера можно считать завершенным.

3.4. Возможные проблемы

После первичной установки некоторые компоненты могут иметь отрицательное состояние доступности.

Для устранения проблем с сервисом **RADAR-TERMITE** включите необходимые типы источников (см. «**Руководство по подключению источников**» → «**Работа с пассивными источниками событий**»).

Для устранения проблем с неработающим сервисом (такой сервис выделен красным) выполните следующие действия:

1. Перейдите в раздел "**Кластер**";
2. На вкладке ***Узлы системы - Узлы*** кликните на IP-адрес узла, на котором располагается неработающий сервис (см. рисунок 41);

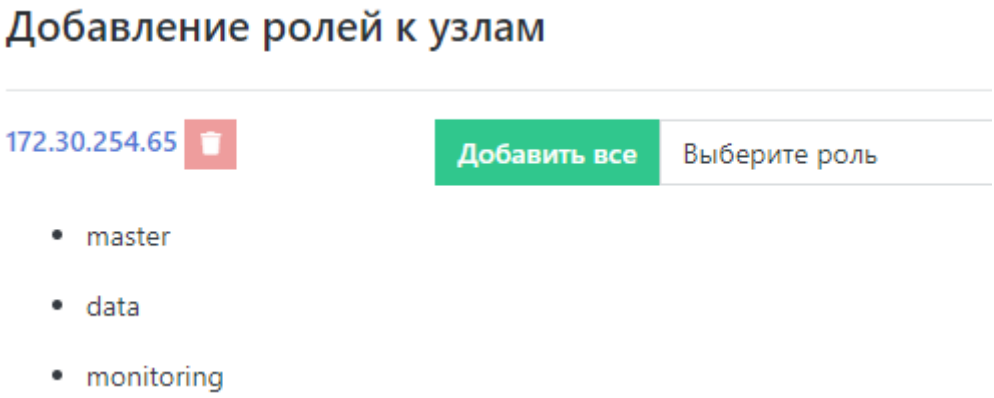

Рисунок 41 – Выбор узла

3. На панели "**Все сервисы узла**" найти неработающий сервис и нажать кнопку "**Действия**". В выпадающем меню выбрать пункт "**Перезапустить**". Если перезапуск сервиса не помог, выберите пункт "**Переустановить сервис**" (см. рисунок 42).

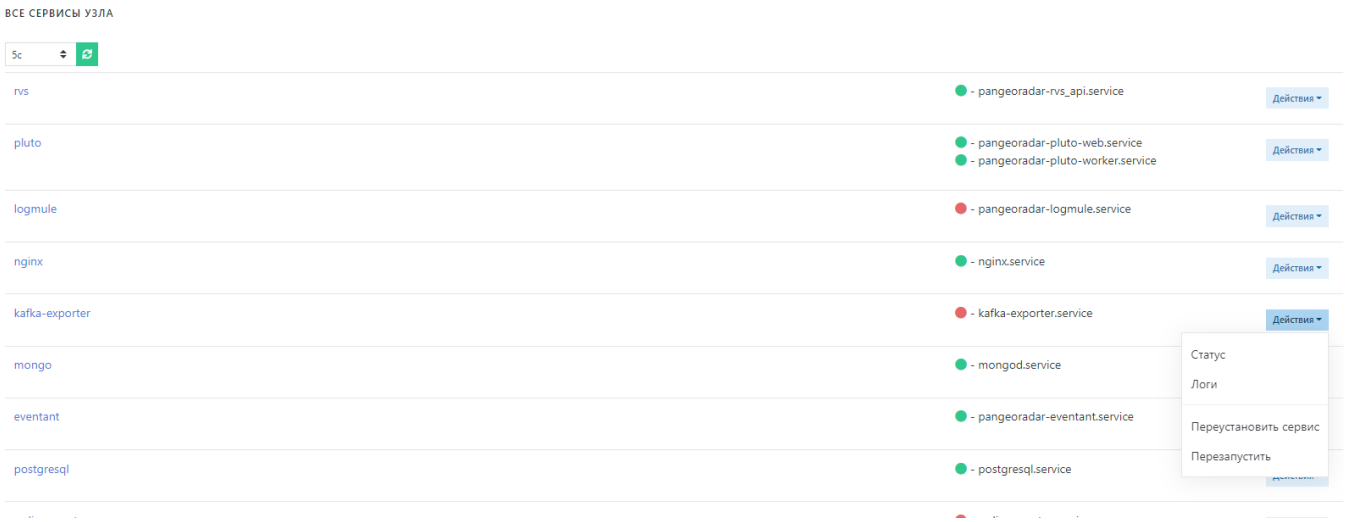

Рисунок 42 – Все сервисы узла

Успешное завершение процесса развертывания, выполнение проверочных мероприятий, конфигурирование **Платформы Радар** и синхронизация с Базой Знаний позволят начать целевую эксплуатацию функционала **Платформы Радар**.

В ходе эксплуатации **Платформы Радар** необходимо руководствоваться документами «**Руководство администратора**» и «**Руководство оператора**».

4. Процедура обновления

Обновление **Платформы Радар** не приводит к потере накопленной информации из баз данных. При обновлении сохраняются собранные события, инциденты, база активов и база знаний со всеми пользовательскими изменениями.

Пакеты обновлений могут быть доставлены на серверы **Платформы Радар** как на съёмных носителях информации (оптические диски, флеш-карты, переносные HDD/SSD накопители), так и с помощью сетевого хранилища при наличии сетевого доступа с серверов **Платформы Радар**.

Обновления базы знаний с пополнением правил корреляции, правил разбора и нормализации без обновления основных пакетов **Платформы Радар** могут быть предоставлены отдельно по запросу Заказчика.

Для обновления **Платформы Радар** с версий 3.3.* и 3.5.* до версии 3.6.* необходимо последовательно выполнить следующие шаги на каждой мастер-ноде каждого инстанса:

1. Перед началом обновления необходимо связаться с вендором для генерации новых лицензий для версии 3.5.*. Без генерации лицензии обновление завершить будет невозможно. Для генерации лицензии можно воспользоваться порталом https://portal.pangeoradar.ru/login или направить письмо на электронный адрес support@pangeoradar.ru.
2. Обязательно выполнить резервное копирование виртуальных машин с установленными компонентами **Платформы Радар**.
3. Перед выполнением обновления подчиненных инстансов необходимо:
   - Проверить корректное значение параметра "**DNS.Auth**" на каждом инстансе. Посмотреть параметр можно в ***Кластер - Управлении конфигурацией - DNS - Адрес сервиса авторизации - DNS.Auth***, переключаясь между каждым инстансом. Адрес сервиса авторизации DNS.Auth должен соответствовать IP-адресу мастер-ноды мастер-инстанса. Например: https://192.168.1.10:8180
   - Проверить работоспособность каждого обновляемого инстанса.
4. С клиентского портала скачать на мастер-ноду версию релиза 3.6.* в директорию `/var/tmp/36\*/`, например `/var/tmp/367/`. Для перехода в нужную директорию и скачивания дистрибутива выполните следующие команды. Например, для версии 3.6.7:

   ```
   mkdir /var/tmp/367/
   cd /var/tmp/367/
   wget https://portal.pangeoradar.ru/pgr-3.6.7.tar.gz
   ```

5. Распаковать скачанный релиз 3.6.7: `tar -xvzf pgr-3.6.5.tar.gz`
6. Находясь в директории `/var/tmp/367/`, выполнить скрипт обновления. Для обновления с версий **Платформы Радар** 3.3.2, 3.5.0 или 3.5.4 необходимо выполнить обновление командой: `bash update_3.6.5_3.3.2.sh`, и дождаться завершения обновления. Скрипт update_3.6.5_3.3.2.sh передается отдельно сотрудниками вендора.

7. После обновления зайти в веб-интерфейс **Платформы Радар**, где должно появится окно для активации лицензии.
    - Для активации лицензии необходимо скопировать **Код активации** из веб-интерфейса;
    - Зайти на клиентский портал в раздел лицензии;
    - В блоке Активные лицензии в действующей лицензии нажать кнопку "**Требуется активация**", вставить код активации и нажать кнопку «Активировать»;
    - Скопировать ключ лицензии и активировать его в веб-интерфейсе **Платформы Радар**;
    - После успешной активации весь функционал **Платформы Радар** будет снова доступен;
8. На основной ноде перейти в ***Кластер - Управление мультиарендностью***. Здесь необходимо задать версию для основной и подчинённой ноды. Для этого напротив основной ноды нажмите "**Редактировать**" и в поле "**Версия релиза**" вставьте значение текущей версии, например: 3.6.5.
9. Затем напротив подчинённой ноды нажмите "**Редактировать**" и в поле «Версия релиза» вставьте значение текущей версии подчиненной ноды, например: 3.3.2. Нажмите кнопку "**Сохранить**".

    Для основной:

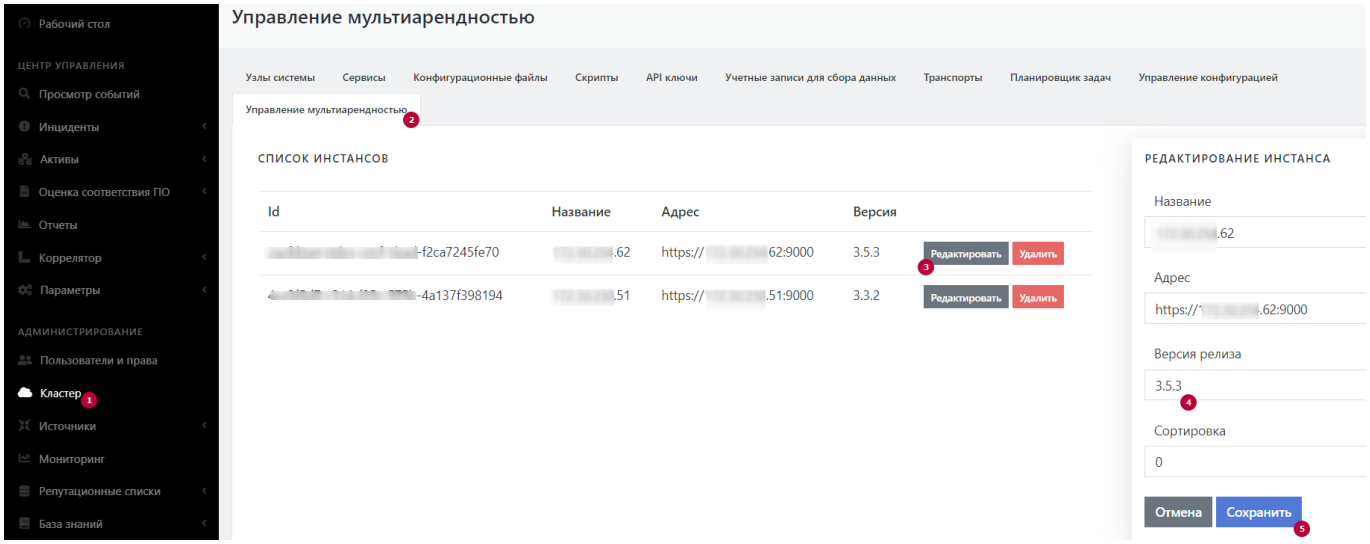

Рисунок 43 – Управление мультиарендностью. Редактирование основной ноды

Для подчинённой:

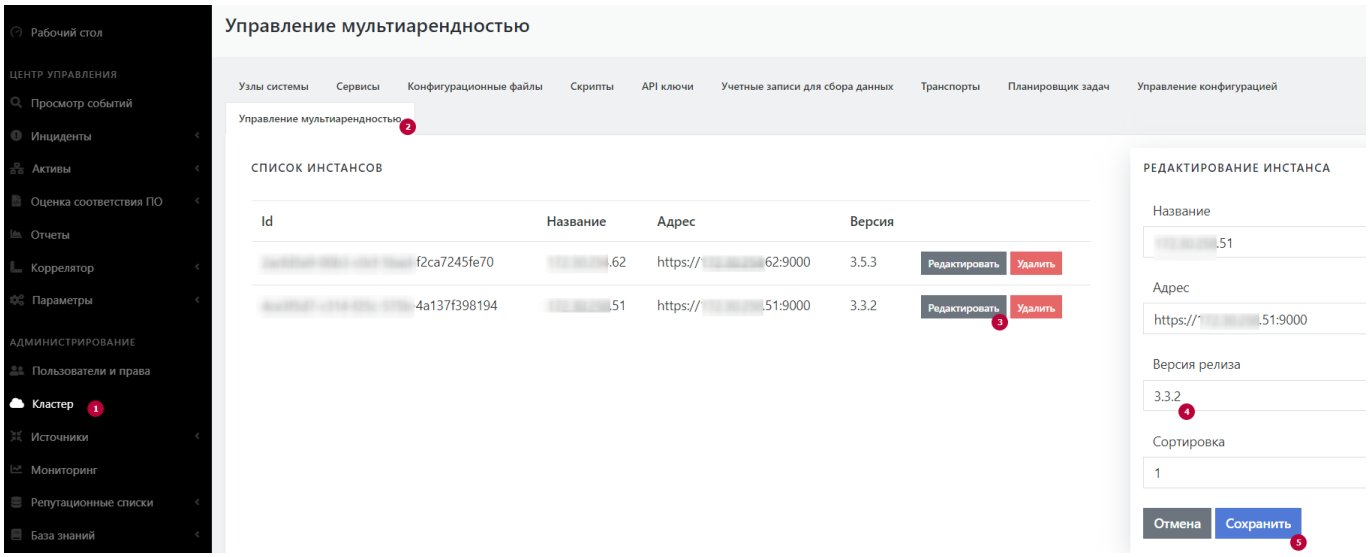

Рисунок 44 – Управление мультиарендностью. Редактирование подчиненной ноды

10. На основной ноде в веб-интерфейсе перейдите в ***Кластер*** - ***Узлы системы*** - ***Узлы*** и выполните следующие действия:
    - Выберите ноду Data(hot), нажав по ip-адресу ноды, добавьте роль eventsrouter и нажмите кнопку "**Раскатить роль**" напротив роли eventsrouter.
    - Выберите ноду Correlator, нажав по ip-адресу ноды, добавьте роль flow-balancer и нажмите кнопку "**Раскатить роль**" напротив роли flow-balancer.
    - Выберите ноду/ноды Correlator, нажав по ip-адресу ноды, добавьте роль logmule2 и нажмите кнопку "**Раскатить роль**" напротив роли logmule2;
    - Выберите ноду/ноды Worker, нажав по ip-адресу ноды и нажмите кнопку «Раскатить роль» напротив роли termite.
11. После выполнения вышеописанных пунктов в веб-интерфейсе **Платформы Радар** перейдите в ***Источники*** - ***Управление источниками*** и нажмите кнопку "**Синхронизировать**".
12. Проверьте работоспособность пайплайна:
    - Проверьте наличие новых событий на странице "**Просмотр событий**";
    - Проверьте отсутствие ошибок в сервисах termite и beaver.
13. **Платформа Радар** обновлена и может быть использована в штатном режиме.

5. Решение проблем

5.1. Сбор диагностической информации при типе установки "Все в одном" (All-in-One)

Для сбора диагностической информации необходимо выполнить следующие действия:

1. Подключиться удаленно к **Платформе Радар** по SSH.
2. Выполнить команду.

```
/opt/pangeoradar/support_tools/diagnostics/aio_diagnostic.sh --diag
```

По окончанию выполнения данной команды на экран будет выведена информация об имени архива и его месторасположении.

5.2. Режимы работы Платформы Радар

5.2.1 Штатный режим

Данный режим используется **Платформой Радар** по умолчанию. В данном режиме все подсистемы работают, события собираются со всех подключенных источников.

5.2.2 Сервисный режим

В случае, если требуется провести работы по обновлению или обслуживанию компонентов, требуется использовать один из сервисных режимов обслуживания для соответствующего компонента.
Данный режим применяется в следующих случаях:

- Обновление ПО компонентов **Платформы Радар**
- Обновление ОС и её компонентов
- Другие работы, требующие перезагрузки ОС или выключения сервера с последующим длительным периодом недоступности

5.2.3 Режим обслуживания компонента LOG-COLLECTOR

Для перевода Платформы Радар в режим обслуживания LOG-COLLECTOR требуется остановить службу PangeoRadarLogCollector.

Если к обслуживаемому компоненту LOG-COLLECTOR подключены источники с пассивным методом сбора, использующие транспорт TCP, то рекомендуется остановить на таких источниках отправку событий на время проведения работ.

Для перехода в штатный режим после перезагрузки ОС от администратора не требуется дополнительных действий. Если в рамках проводимых работ не требовалась перезагрузка ОС, то после проведения работ требуется включить службу PangeoRadarLogCollector в ручном режиме.

5.2.4 Режим обслуживания компонента BALANCER

Для перевода Платформы Радар в режим обслуживания BALANCER требуется остановить службу rsyslog на сервере балансировщика нагрузки.

В случаях, когда планируемое время обслуживания превышает период в 1 час, то также рекомендуется перевести в режим обслуживания компоненты LOG-COLLECTOR.

После завершения работ по обслуживанию требуется запустить службу rsyslog.

5.2.5 Режим обслуживания WORKER

Для перевода Платформы Радар в режим обслуживания WORKER требуется остановить службу termite на обслуживаемом сервере обработки событий.

В случаях, когда сервер обработки событий в кластере один и планируемое время обслуживания превышает период в 1 час рекомендуется также перевести в режим обслуживания сервер BALANCER.

После завершения работ по обслуживанию требуется запустить службу termite.

5.2.6 Режим обслуживания MASTER

Для перевода Платформы Радар в режим обслуживания MASTER требуется приостановить сбор событий со всех источников.

После проведения обслуживания необходимо запустить остановленный ранее сбор событий с источников.

5.2.7 Режим обслуживания компонента DATA

Для перевода Платформы Радар в режим обслуживания DATA требуется остановить службу `elasticsearch` на сервере хранения, а также остановить сбор событий с источников.

После завершения работ по обслуживанию требуется запустить службу `elasticsearch`.

5.2.8 Режим обслуживания CORRELATOR

Для перевода Платформы Радар в режим обслуживания CORRELATOR требуется остановить службу `logmule` на обслуживаемом сервере корреляции событий.

В случаях, когда сервер корреляции событий в кластере один и планируемое время обслуживания превышает период в 1 час рекомендуется также перевести в режим обслуживания сервер MASTER.

После завершения работ по обслуживанию требуется запустить службу `logmule`.