

Платформа Радар

Руководство по установке

Версия 3.5.4

Оглавление

Оглавление

1. Подготовка к установке

- 1.1. Форма поставки
- 1.2. Основные этапы установки и запуска **Платформы Радар**
- 1.3. Подготовка оборудования
 - 1.3.1. Подготовка дисковой системы {#disk_prepare}
 - 1.3.2. Подготовка аппаратной части
 - 1.3.3. Настройка сетевой конфигурации
 - 1.3.4. Настройка NTP
 - 1.3.5. Подготовка для установки **Платформы Радар** без доступа к сети Интернет {#noipnt}
 - 1.3.6. Подготовка для развертывания **Платформы Радар** с доступом к сети Интернет

2. Установка Платформы

- 2.1. Подготовка установочных файлов Платформы
- 2.2. Запуск инсталляционного скрипта и первичная установка системы
- 2.3. Продолжение установки и настройки Платформы
- 2.4. Запуск установки
- 2.5. Проверка работоспособности ПО
 - 2.5.1. Первичное конфигурирование Платформы
 - 2.5.2. Синхронизация с Базой Знаний
- 2.6. Возможные проблемы

3. Особенности распределенной установки

- 3.1. Особенности подготовки оборудования
 - 3.1.1. Подготовки дисковой системы к распределенной установке
 - 3.1.2. Настройка сетевой конфигурации при распределенной установке
- 3.2. Особенности распределенной установки Платформы
 - 3.2.1. Подготовка установочных файлов Платформы
 - 3.2.2. Запуск инсталляционного скрипта и первичная установка системы
 - 3.2.3. Продолжение установки и настройки Платформы
 - 3.2.4. Запуск установки ролей Платформы
- 3.3. Проверка распределенной установки и работоспособности ПО
 - 3.3.1. Первичное конфигурирование Платформы
 - 3.3.2. Синхронизация с Базой Знаний
 - 3.3.3. Добавление нового узла кластера
- 3.4. Возможные проблемы

1. Подготовка к установке

1.1. Форма поставки

Платформа Радар может поставляться в следующих вариантах:

- в виде образа виртуальной машины с предустановленным ПО и компонентами;
- в виде защищенного паролем зашифрованного архива с дистрибутивами.

Пароль передаётся отдельно от архива.

1.2. Основные этапы установки и запуска Платформы Радар

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

Перед началом процесса необходимо выбрать наиболее подходящую конфигурацию установки (см. [«Примеры конфигураций»](#)).

В таблице 1 приведен состав действий и роли исполнителей, задействованных в процессе развертывания **Платформы Радар**.

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

Таблица 1 -- Перечень действий

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 {#disk_prepare}

Подготовка к установке и запуску **Платформы Радар** должна осуществляться с учетом требований, представленных в разделах [«Требования к ПО»](#) и [«Требования к ТО»](#), и, в зависимости от выбранного варианта, развертывания.

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, из требований к ресурсам для конкретного модуля **Платформы Радар** (см «Общее описание»);
- тип файловой системы - XFS (при необходимости можно использовать ext4).

Процедура разметки дисковой подсистемы Хранение данных для серверной роли DATA при распределенной инсталляции описана в разделе [«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, удовлетворяющих системным требованиям (см. [«Требования к ТО»](#)).

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 [«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 разделе [«Пример настройки службы синхронизации времени в ОС Debian»](#).

1.3.5. Подготовка для установки Платформы Радар без доступа к сети Интернет {#noint}

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

- доступ к целевой системе по SSH (необходимо для копирования образов системы, файлов конфигурации и настройки системы);
- 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

Для наглядности наши специалисты подготовили видео фрагмент установки SIEM "Платформа Радар"

2.1. Подготовка установочных файлов Платформы

Подключитесь по SSH к Платформе, используя полученный IP-адрес стенда и логин.

Внимание! Для запуска установки необходимо получить права суперпользователя

Перейдите в каталог `/var/tmp`:

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

Далее загрузите установочный архив. Например, командой `curl`. Командой `ls` убедитесь, что установочный архив загружен успешно и находится в каталоге `/var/tmp` (см. рисунок 1):

```
a.kurkov@v-stand-25:/var/tmp$ curl http://releases.pgr.local/3.3.1-rc3/pgr-3.3.1-rc3-online.tar.gz --output pgr-3.3.1-rc3-online.tar.gz
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             %             Dload  Upload   Total   Spent    Left   Speed
100 1550M  100 1550M    0     0  109M      0  0:00:14  0:00:14  --:--:--  105M
a.kurkov@v-stand-25:/var/tmp$ ls
pgr-3.3.1-rc3-online.tar.gz
systemd-private-dcb8fd6f7f724cb58a7414e48dab6dac-systemd-timesyncd.service-K8oRbN
a.kurkov@v-stand-25:/var/tmp$ █
```

Рисунок 1 - Загрузка установочного архива

Если скачан 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 скачан 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 (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.

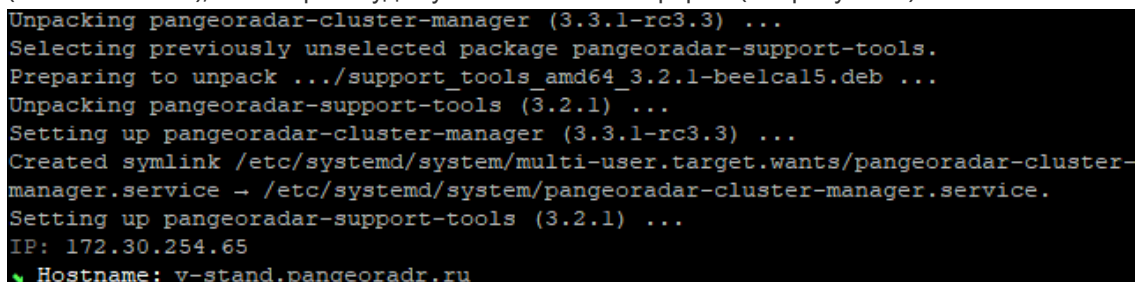
2.2. Запуск инсталляционного скрипта и первичная установка системы

Внимание! Перед запуском установки убедитесь, что сервер, на котором устанавливается Платформа, подключен к сети Интернет.

Для корректной установки Платформы 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.

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. Далее укажите внешний IP-адрес и доменное имя сервера (необязательно), на котором будет установлена Платформа (см. рисунок 2).



```
Unpacking pangeoradar-cluster-manager (3.3.1-rc3.3) ...
Selecting previously unselected package pangeoradar-support-tools.
Preparing to unpack .../support_tools_amd64_3.2.1-beelcal5.deb ...
Unpacking pangeoradar-support-tools (3.2.1) ...
Setting up pangeoradar-cluster-manager (3.3.1-rc3.3) ...
Created symlink /etc/systemd/system/multi-user.target.wants/pangeoradar-cluster-manager.service → /etc/systemd/system/pangeoradar-cluster-manager.service.
Setting up pangeoradar-support-tools (3.2.1) ...
IP: 172.30.254.65
Hostname: v-stand.pangeoradr.ru
```

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 и настройки Платформы

1. После перехода по адресу, указанному в конце работы инсталлятора (см. раздел "Запуск инсталляционного скрипта и первичная установка системы"), необходимо пройти процедуру авторизации (admin\admin) и смены пароля по умолчанию согласно руководству пользователя.

После прохождения авторизации станет доступен этап получения лицензии Платформы (подробнее см. раздел "[Первичная активация лицензии](#)")

2. После активации лицензии нажмите кнопку далее, после чего будет отображен экран глобальных настроек (см. рисунок 3).

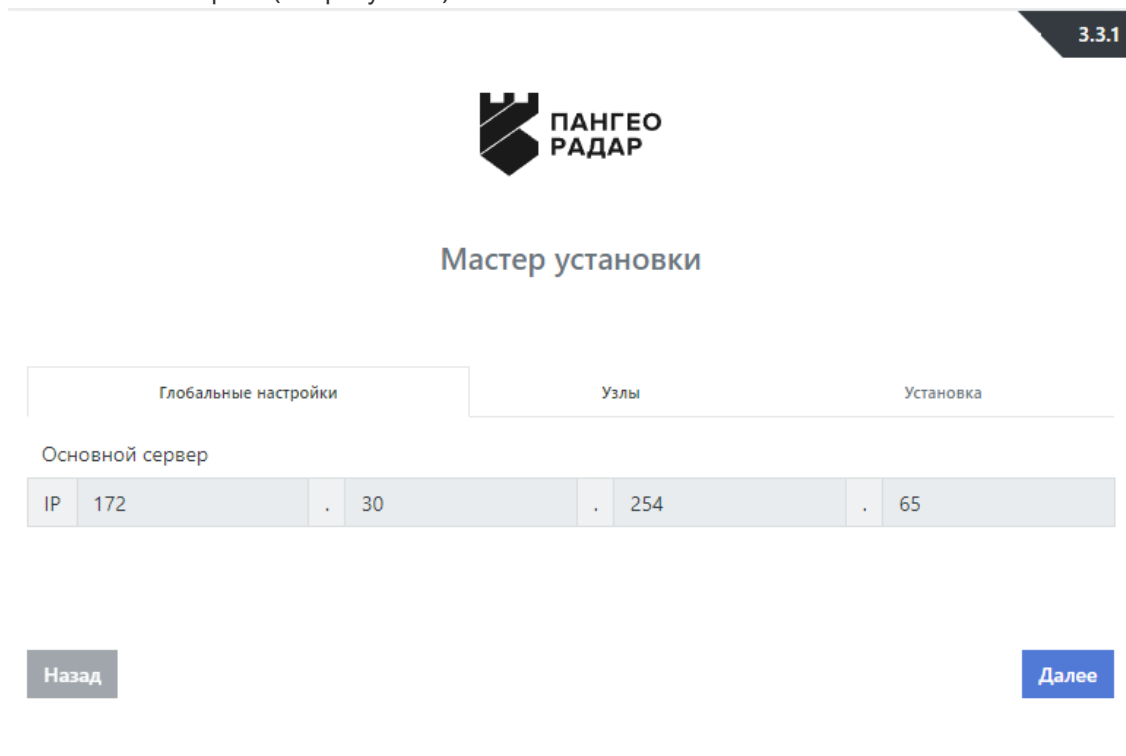


Рисунок 3 - Экран продолжения установки Платформы

3. На данном экране нажмите на кнопку «Далее» и перейдите на экран настройки узлов (см. рисунок 4):



Мастер установки

Глобальные настройки | Узлы | Установка

Добавление нового узла

Название Порт

Введите имя

Логин Пароль

IP

Введите ip

Добавление ролей к узлам

172.30.254.65

- data
- monitoring
- agent
- worker
- infra
- backup
- balancer
- correlator
- agent_win

Выберите роль

Выберите роль

- master

Роль data не добавлена

Роль monitoring не добавлена

Рисунок 4 - Экран настройки узлов Платформы

4. В разделе настройки узлов в случае установки на один сервер необходимо добавить к уже существующему узлу серверные роли (см. рисунок 4):

- data
- monitoring
- worker
- infra
- backup
- balancer
- correlator

Кнопка "Добавить все" позволяет назначить серверу все возможные роли.

5. Далее перейдите к шагу «Установка» нажатием кнопки «Далее».

2.4. Запуск установки

1. На экране старта установки (см. рисунок 5) нажмите на кнопку «Начать установку». После этого станет доступен экран просмотра журнала установки (см. рисунок 6).



Мастер установки

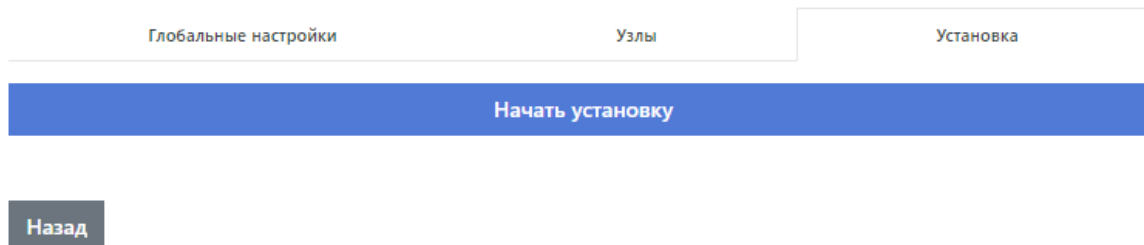


Рисунок 5 - Экран старта установки

```

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 already installed
Warning: apt-key output should not be parsed (stdout is not a terminal)

```

Рисунок 6 - Процесс установки

2. Установка занимает некоторое время. По завершению процесса установки откроется Платформа в меню администрирования "Кластер" - "Узлы системы" - "Проверка"

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

2.5. Проверка работоспособности ПО

Проверка работоспособности ПО включает в себя шаги по проверке на наличие в разделе управления кластером «Кластер» незапущенных сервисов и ошибок в журналах сервисов.

1. Для выполнения проверки необходимо перейти в меню администрирования "Кластер" (см. рисунок 7).

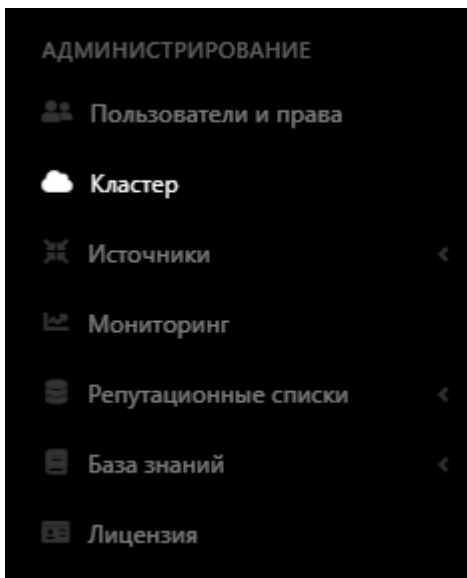


Рисунок 7 - Раздел управления кластером

2. Перейти на вкладку "Узлы системы", выбрать раздел "Проверка" и убедиться, что индикация всех сервисов подсвечена зеленым. Это означает, что все сервисы находятся в рабочем состоянии (см. рисунок 8).

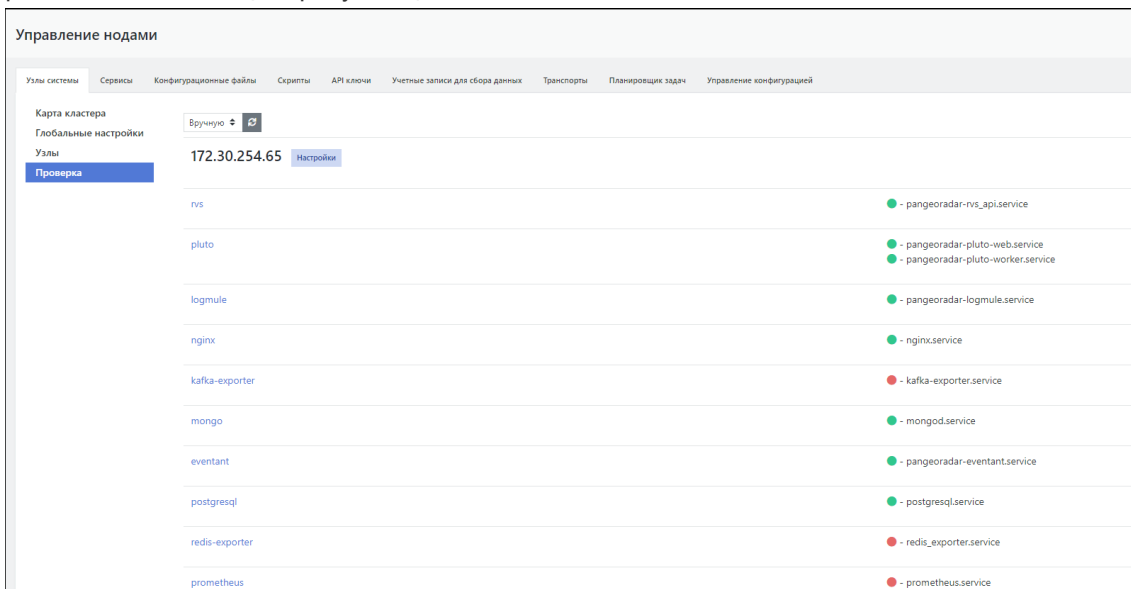


Рисунок 8 - Проверка сервисов

3. Для проверки состояния и просмотра событий сервиса необходимо нажать кнопку «Настройки» рядом с ip адресом-узла, на котором развернуты сервисы (см. рисунок 9).

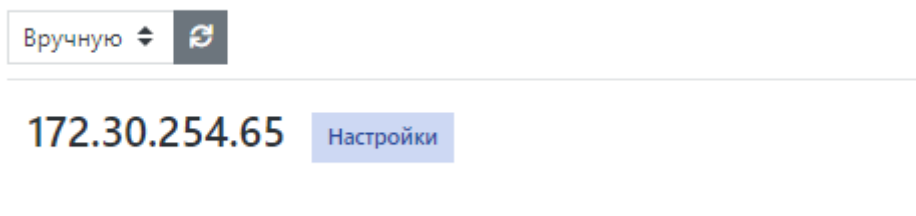


Рисунок 9 - Настройка ноды

4. На странице Управление хостом выбрать интересующий сервис и нажать кнопку «Действия» (см. рисунок 10).

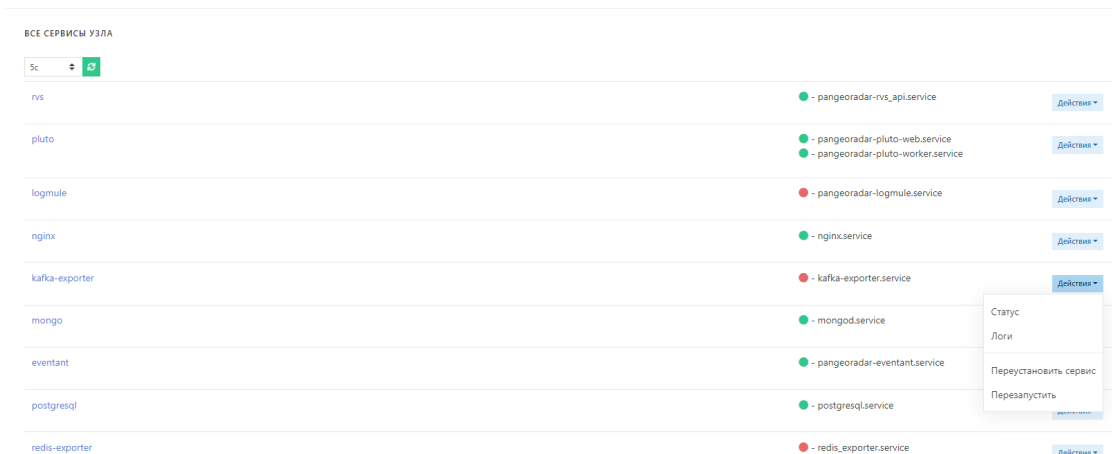


Рисунок 10 - Выбор действий

5. В выпадающем меню выбрать необходимый пункт:

- Статус - выводит информацию о состоянии сервиса (см. рисунок 11).

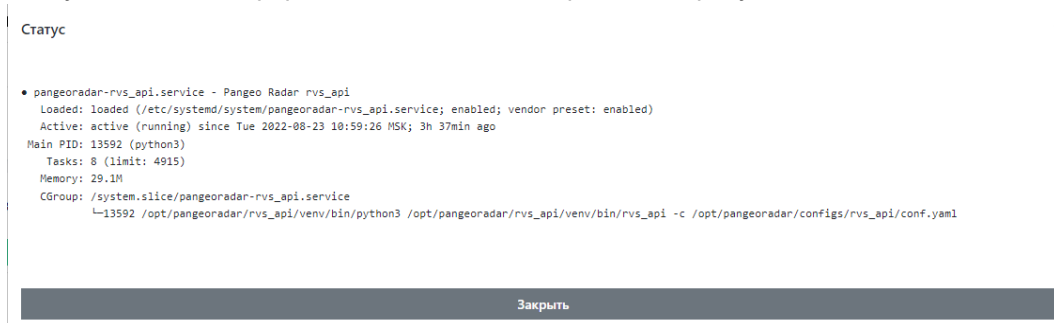


Рисунок 11 - Окно с информацией о состоянии сервиса

- Логи - выводит журнал событий сервиса (см. рисунок 12).



Рисунок 12 - 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, обратитесь к [Руководству по сбору информации и устранения неисправностей](#)

2.5.1. Первичное конфигурирование Платформы

Первичное конфигурирование платформы 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

При выполнении операций по синхронизации с Базой Знаний необходимо выполнить следующие действия:

- синхронизировать типы инцидентов;
 - синхронизировать правила для Коррелятора.
1. Для этого перейдите в раздел «Центр управления» - «Параметры» - "Параметры" и выберите вкладку «Синхронизация с Базой Знаний».
 2. Нажмите на кнопки «Синхронизация типов инцидентов» и «Синхронизация коррелятора» (см. рисунок 13).

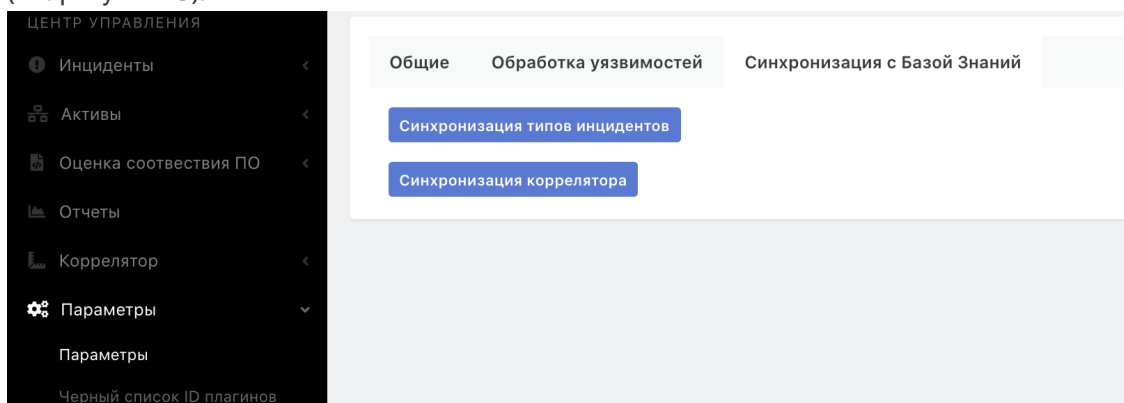


Рисунок 13 - Вкладка синхронизации с Базой Знаний

Синхронизация правил для коррелятора может занимать некоторое время.

2.6. Возможные проблемы

После первичной установки некоторые компоненты могут иметь отрицательное состояние доступности.

Для устранения проблем с сервисом RADAR TERMITE включите типы источников (см. раздел ["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» перейдите в раздел "Узлы" и кликните на IP-адрес узла, на котором располагается неработающий сервис (см. рисунок 14).

Добавление ролей к узлам

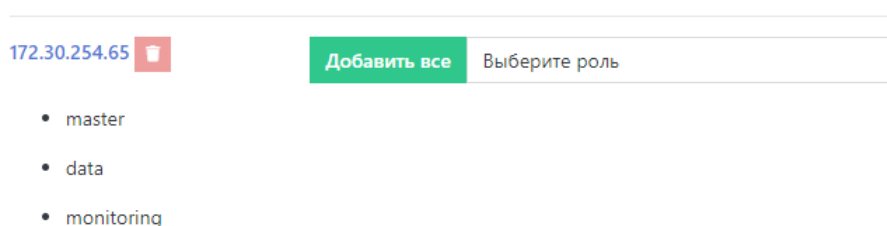


Рисунок 14 - Выбор узла

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 15).

Сервис	Статус	Действия
rvs	● - pangeoradar-rvs_api.service	Действия ▾
pluto	● - pangeoradar-pluto-web.service ● - pangeoradar-pluto-workers.service	Действия ▾
logmule	● - pangeoradar-logmule.service	Действия ▾
nginx	● - nginx.service	Действия ▾
kafka-exporter	● - kafka-exporter.service	Действия ▾ Статус Логи Переустановить сервис Перезапустить
mongo	● - mongod.service	Действия ▾
eventant	● - pangeoradar-eventant.service	Действия ▾
postgresql	● - postgresql.service	Действия ▾

Рисунок 15 - Панель "Все сервисы узла"

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

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

3. Особенности распределенной установки

3.1. Особенности подготовки оборудования

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

3.1.1. Подготовки 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 swar - не менее 10% от общего объема оперативной памяти, из требований к ресурсам для конкретного модуля Платформы (см. раздел [«Требования к ТО»](#));
- тип файловой системы - XFS (при необходимости можно использовать ext4).

Для серверной роли DATA необходимо провести процедуру разметки дисковой подсистемы Хранение данных, которая приведена в разделе [«Подготовка дисковой подсистемы для реализации роли DATA»](#).

3.1.2. Настройка сетевой конфигурации при распределенной установке

1. Для доступа к веб-интерфейсам управления Платформой 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 1 приведены необходимые сетевые настройки при распределенной установке Платформы Радар (независимо от вариантов распределенной установки).

Таблица 1 -- Сетевые настройки для распределенной установки Платформы Радар

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

Исходящий	Входящий	Порты	Описание
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 receiver	Пассивный сбор событий
Пользователи Платформы	Master	8080 9000 6676 6677	Доступ к интерфейсу платформы, 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 разделе [«Сетевое взаимодействие»](#).

3.2. Особенности распределенной установки Платформы

3.2.1. Подготовка установочных файлов Платформы

Подключитесь по SSH к Платформе, используя полученный IP-адрес станда и логин.

Внимание! Для запуска установки необходимо получить права суперпользователя

Перейдите в каталог `/var/tmp`:

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

Далее загрузите установочный архив. Например, командой `curl`. Командой `ls` убедитесь, что установочный архив загружен успешно и находится в каталоге `/var/tmp` (см. рисунок 16):

```
a.kurkov@v-stand-25:/var/tmp$ curl http://releases.pgr.local/3.3.1-rc3/pgr-3.3.1-rc3-online.tar.gz --output pgr-3.3.1-rc3-online.tar.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 1550M  100 1550M    0     0  109M      0  0:00:14  0:00:14 --:--:-- 105M
a.kurkov@v-stand-25:/var/tmp$ ls
pgr-3.3.1-rc3-online.tar.gz
systemd-private-dcb8fd6f7f724cb58a7414e48dab6dac-systemd-timesyncd.service-K8oRbN
a.kurkov@v-stand-25:/var/tmp$
```

Рисунок 16 - Загрузка установочного архива

Если скачан 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 скачан 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 (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. Запуск инсталляционного скрипта и первичная установка системы

Внимание! Перед запуском установки убедитесь, что сервер, на котором устанавливается Платформа, подключен к сети Интернет.

Для корректной установки Платформы 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.

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. Далее укажите внешний IP-адрес и доменное имя сервера (необязательно), на котором будет установлена Платформа (см. рисунок 17).

```
Unpacking pangeoradar-cluster-manager (3.3.1-rc3.3) ...
Selecting previously unselected package pangeoradar-support-tools.
Preparing to unpack ../support_tools_amd64_3.2.1-beelcal5.deb ...
Unpacking pangeoradar-support-tools (3.2.1) ...
Setting up pangeoradar-cluster-manager (3.3.1-rc3.3) ...
Created symlink /etc/systemd/system/multi-user.target.wants/pangeoradar-cluster-
manager.service → /etc/systemd/system/pangeoradar-cluster-manager.service.
Setting up pangeoradar-support-tools (3.2.1) ...
IP: 172.30.254.65
▼ Hostname: v-stand.pangeoradr.ru
```

Рисунок 17 - 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`
```

3.2.3. Продолжение установки и настройки Платформы

1. После перехода по адресу, указанному в конце работы инсталлятора (см. раздел "Запуск инсталляционного скрипта и первичная установка системы"), необходимо пройти процедуру авторизации (`admin\admin`) и смены пароля по умолчанию согласно руководству пользователя.
После прохождения авторизации станет доступен этап получения лицензии Платформы (подробнее см. раздел "[Первичная активация лицензии](#)")
2. После активации лицензии Нажмите кнопку далее, после чего будет отображен экран глобальных настроек (см. рисунок 18).



Мастер установки

Глобальные настройки	Узлы	Установка
----------------------	------	-----------

Основной сервер

IP	172	.	30	.	254	.	65
----	-----	---	----	---	-----	---	----

[Назад](#) [Далее](#)

Рисунок 18 - Экран продолжения установки Платформы

7. На данном экране нажмите на кнопку «Далее» и перейдите на экран настройки узлов (см. рисунок 19):



Мастер установки

Глобальные настройки Узлы Установка

Добавление нового узла

Название Порт

Введите имя

Логин Пароль

IP

Введите ip

Добавление ролей к узлам

172.30.254.65

- master

Роль data не добавлена

Роль monitoring не добавлена

Рисунок 19 - Экран настройки узлов Платформы

8. При выполнении распределенной инсталляции Платформы сначала необходимо добавить все узлы кластера через форму Добавления нового узла (см. рисунок 20):

Глобальные настройки Узлы Установка

Добавление нового узла

Название: balancer01 Порт: 22

Логин: root Пароль:






IP: 172.30.254.81 **Добавить**

```
-----
Successfully /opt/pangeoradar/distrs directory create/nFile Copy success/nSelecting previously unselected pa
(Reading database ... 28160 files and directories currently installed.)
Preparing to unpack .../pangeoradar-cluster-agent_amd64.deb ...
Unpacking pangeoradar-cluster-agent (3.0.10.3) ...
Setting up pangeoradar-cluster-agent (3.0.10.3) ...
Created symlink /etc/systemd/system/multi-user.target.wants/pangeoradar-cluster-agent.service → /etc/systemd
Successfully generate remote ssh key/nSuccessfully get remote ssh key/nSuccessfully add master ip to hosts f
-----
Successfully /opt/pangeoradar/distrs directory create/nFile Copy success/nSelecting previously unselected pa
(Reading database ... 28160 files and directories currently installed.)
Preparing to unpack .../pangeoradar-cluster-agent_amd64.deb ...
Unpacking pangeoradar-cluster-agent (3.0.10.3) ...
Setting up pangeoradar-cluster-agent (3.0.10.3) ...
Created symlink /etc/systemd/system/multi-user.target.wants/pangeoradar-cluster-agent.service → /etc/systemd
```

Рисунок 20 - Добавление нового узла

9. После чего назначьте серверные роли согласно архитектуре проектного решения (см. рисунок 21):

Добавление ролей к узлам

172.30.254.86 	Добавить все	Выберите роль	⌵	+
• master				-
• monitoring				-
• infra				-
• backup				-
172.30.254.82 	Добавить все	Выберите роль	⌵	+
• balancer				-
172.30.254.83 	Добавить все	Выберите роль	⌵	+
• worker				-
172.30.254.84 	Добавить все	Выберите роль	⌵	+
• data				-
172.30.254.85 	Добавить все	Выберите роль	⌵	+
• correlator				-

Назад **Далее**

Рисунок 21 - Добавление ролей к узлам

10. Далее перейдите к шагу «Установка» нажатием кнопки «Далее».

3.2.4. Запуск установки ролей Платформы

1. На экране старта установки (см. рисунок 22) нажмите на кнопку «Начать установку». После этого станет доступен экран просмотра журнала установки (см. рисунок 23).

3.3.1



Мастер установки

Глобальные настройки

Узлы

Установка

Начать установку

Назад

Рисунок 22 - Экран старта установки

```
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 already installed
```

```
Warning: apt-key output should not be parsed (stdout is not a terminal)
```

Рисунок 23 - Процесс установки

2. Установка занимает некоторое время. По завершению процесса установки откроется Платформа в меню администрирования "Кластер" - "Узлы системы" - "Проверка"

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

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 24). Убедитесь что узлов в составе Платформы больше одного, роли распределены по узлам (см. рисунок 25).

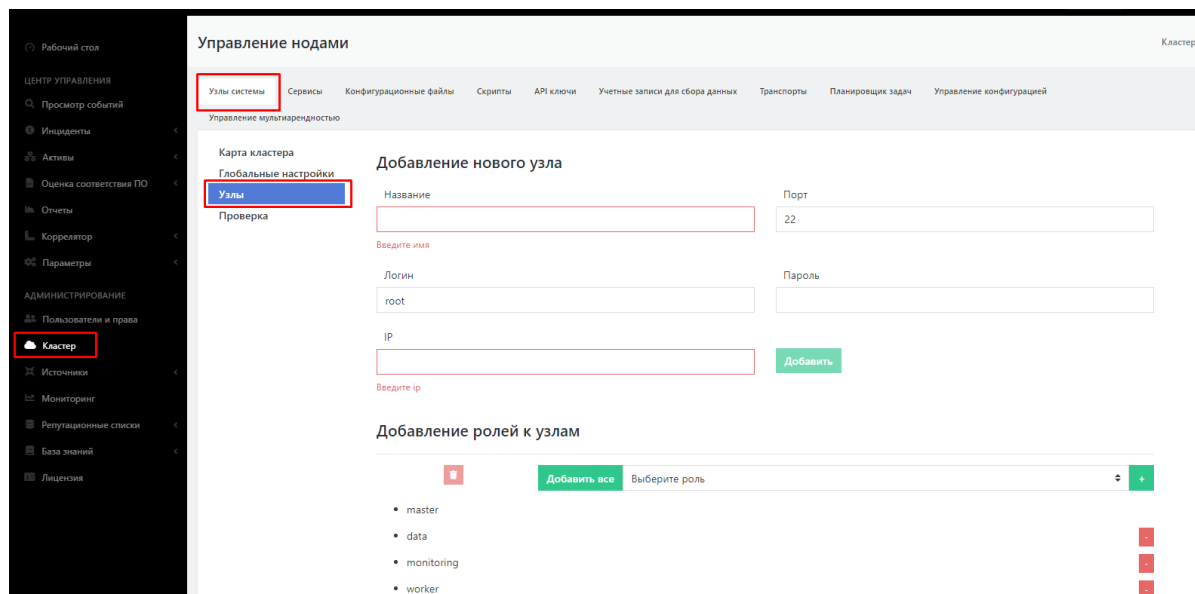


Рисунок 24 - Раздел управления кластером

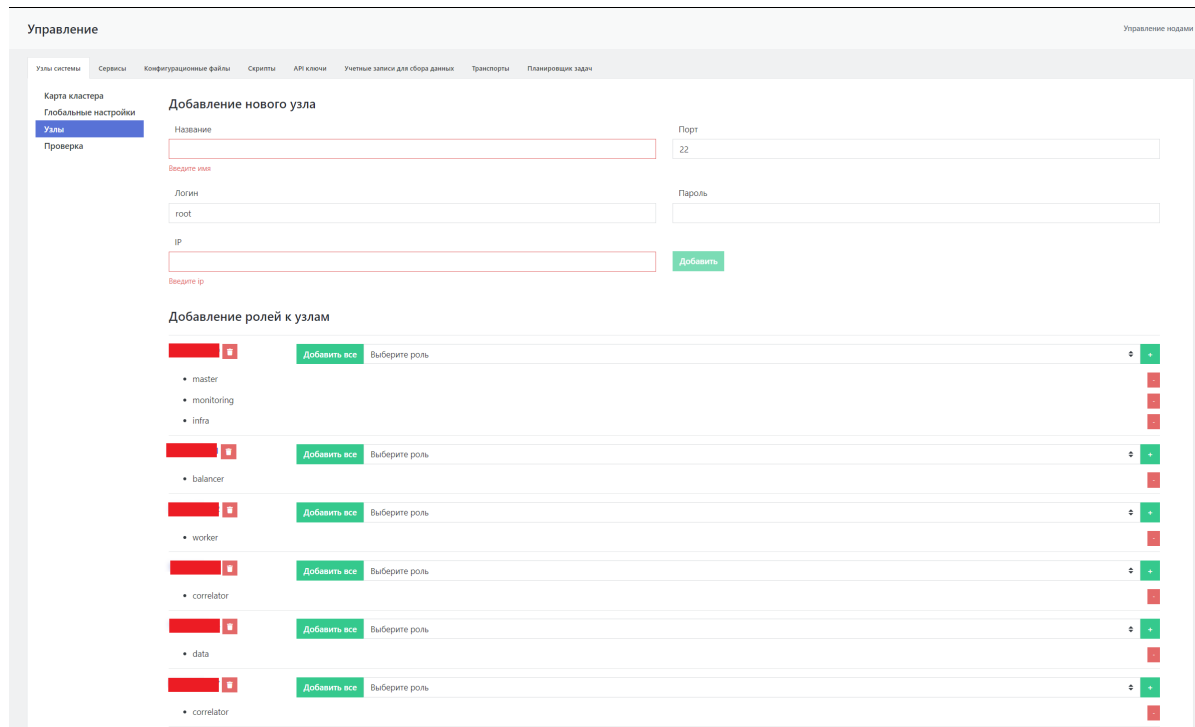


Рисунок 25 - Список узлов Платформы с указанием ролей

3. На вкладке "Узлы системы" перейдите в подраздел "Проверка" (см. рисунок 26). Убедитесь, что список узлов и их ролей, совпадает с тем, что было задано при распределенной установке и настройке Платформы. Убедитесь что на всех узлах индикация всех сервисов подсвечена зеленым, т.е. все сервисы находятся в рабочем состоянии.

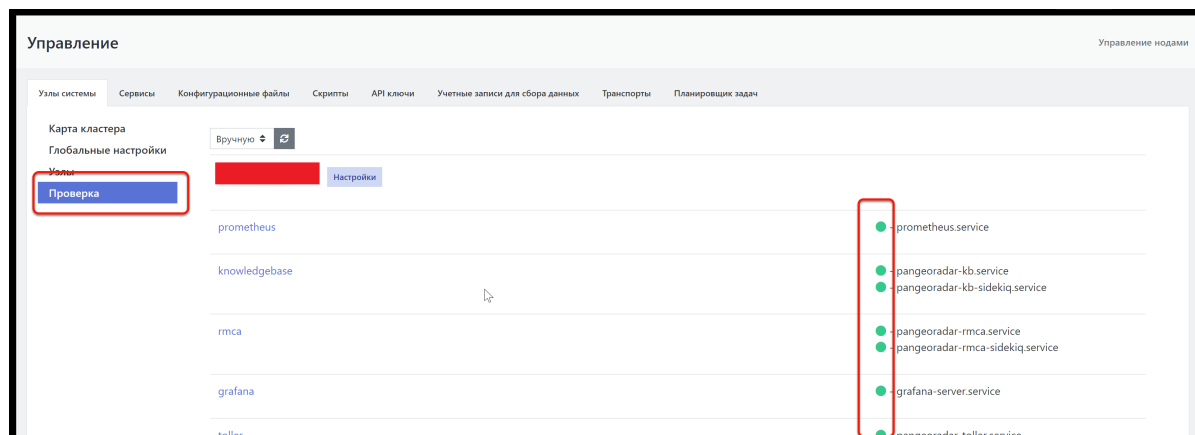


Рисунок 26 - Проведение проверки сервисов, установленных на узлах Платформы

4. Выберите один из узлов, например Balancer, и нажмите кнопку **Настройки**, расположенную справа от названия узла (см. рисунок 26). Откроется страница управления узлом и списком всех сервисов, установленных на данном узле (см. рисунок 27).

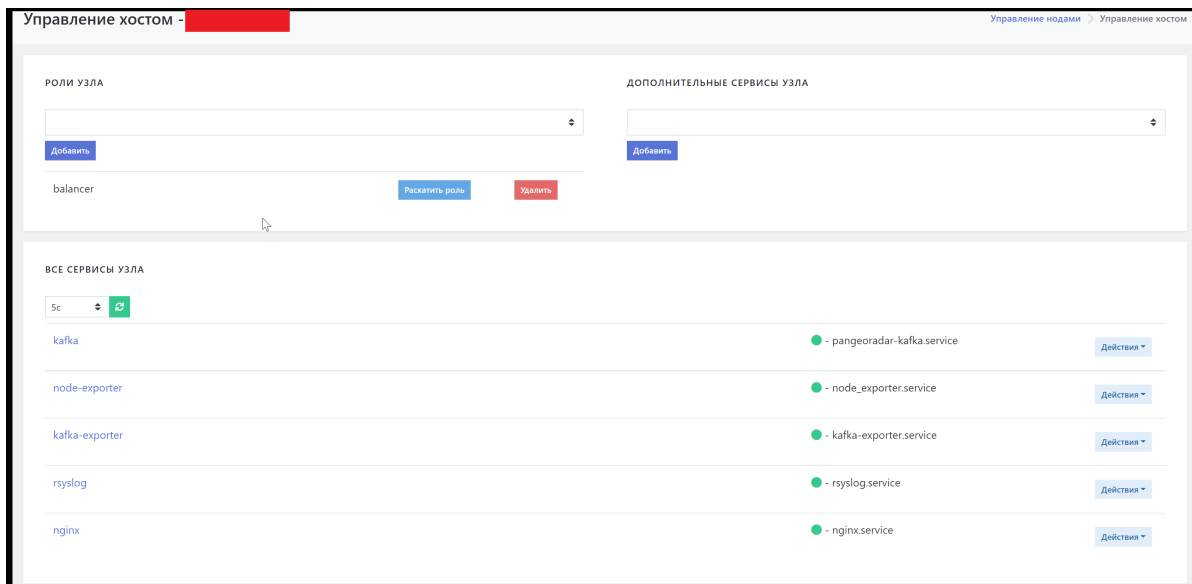


Рисунок 27 - Страница с функциями управления хостом

5. На странице "Управление хостом" выберите интересующий сервис, например, kafka, и нажмите кнопку **Действия**. В раскрывшемся списке выберите **Статус** (см. рисунок 28).

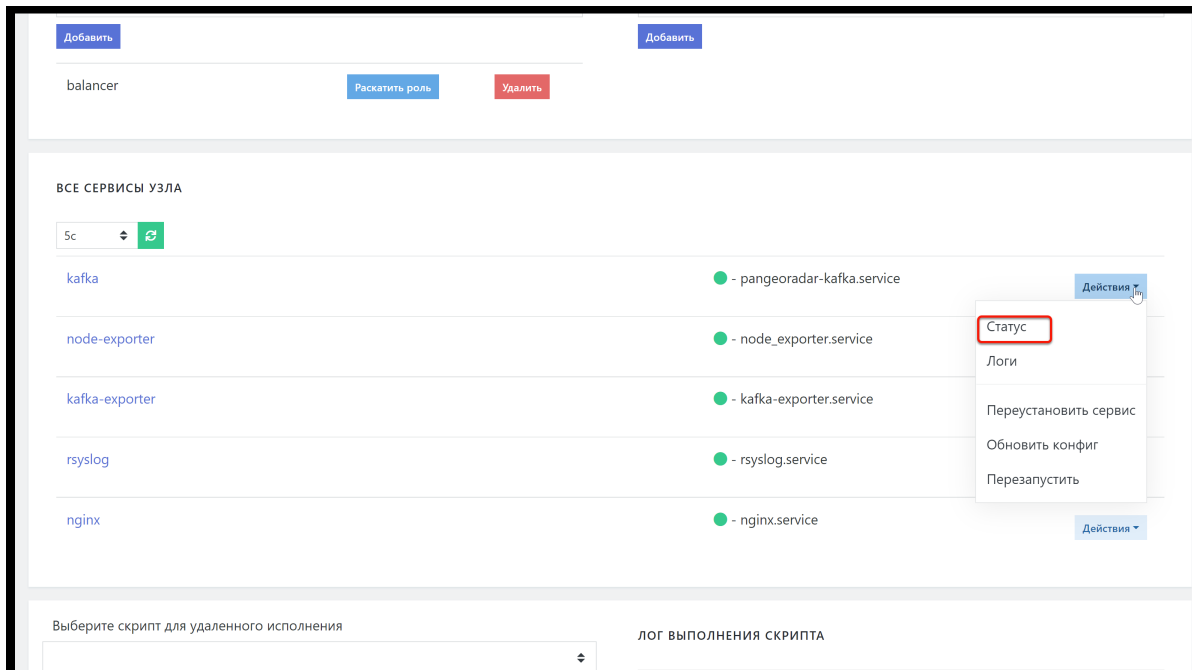


Рисунок 28 - Выбор действий с компонентом

При выборе действия ****Статус**** на экран выводится информация о состоянии сервиса (см. рисунок 29).



Рисунок 29 - Окно с информацией о состоянии сервиса

б. В раскрывшемся списке **Действия** выберите **Логи** (см. рисунок 28).

При выборе действия **Логи** на экран выводится журнал событий сервиса (см. рисунок 30).

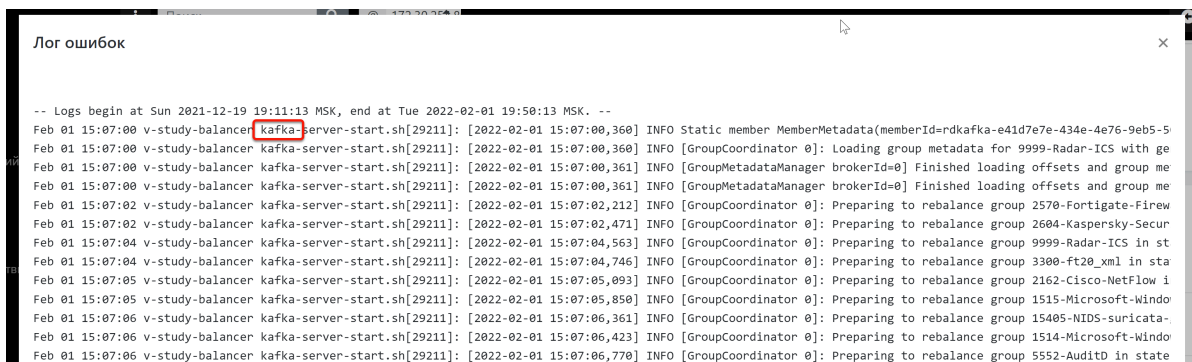


Рисунок 30 - Окно вывода событий сервиса

Для подтверждения достоверности информации, полученной через веб-интерфейс Платформы, 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 по команде **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

Первичное конфигурирование платформы 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

При выполнении операций по синхронизации с Базой Знаний необходимо выполнить следующие действия:

- синхронизировать типы инцидентов;
 - синхронизировать правила для Коррелятора.
1. Для этого перейдите в раздел «Центр управления» - «Параметры» - "Параметры" и выберите вкладку «Синхронизация с Базой Знаний».
 2. Нажмите на кнопки «Синхронизация типов инцидентов» и «Синхронизация коррелятора» (см. рисунок 31).

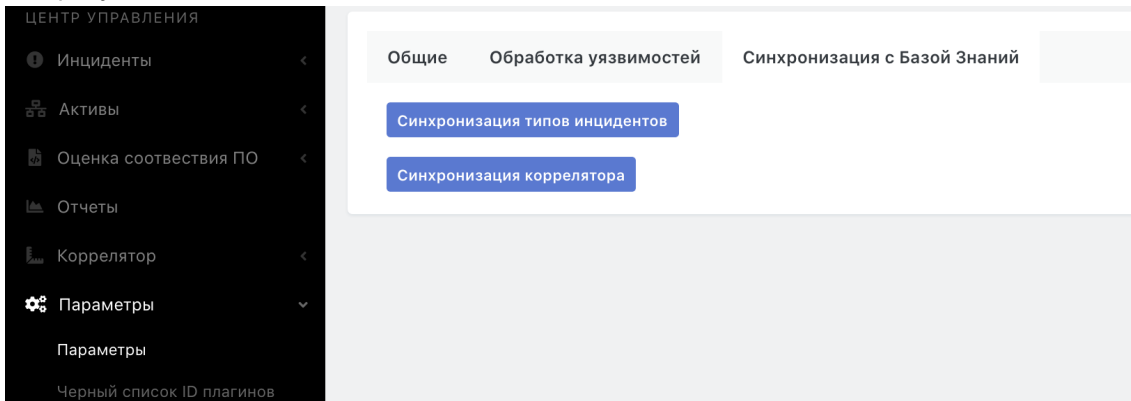


Рисунок 31 - Вкладка синхронизации с Базой Знаний

Синхронизация правил для коррелятора может занимать некоторое время.

3.3.3. Добавление нового узла кластера

При необходимости расширения производительных возможностей Платформы 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 32):

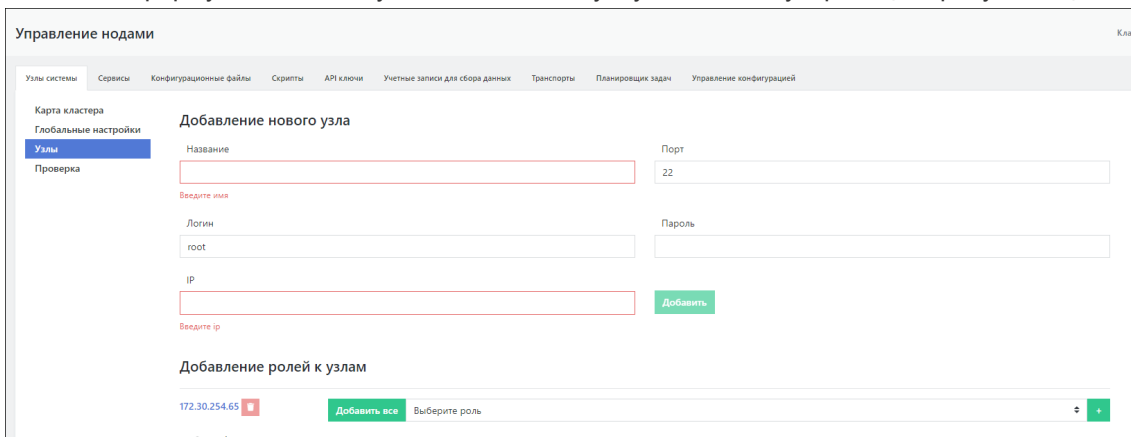


Рисунок 32 - Добавление нового узла кластера

2. Далее - перейдите в настройки созданного узла кластера, для этого необходимо нажать на IP-адрес этого узла (см. рисунок 33):

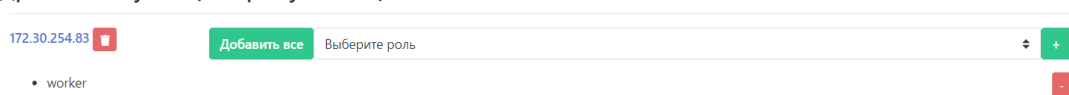


Рисунок 33 - Созданный узел кластера

3. В настройках созданного узла нажмите на кнопку "Раскатить роль" напротив добавленной роли (см. рисунок 34):

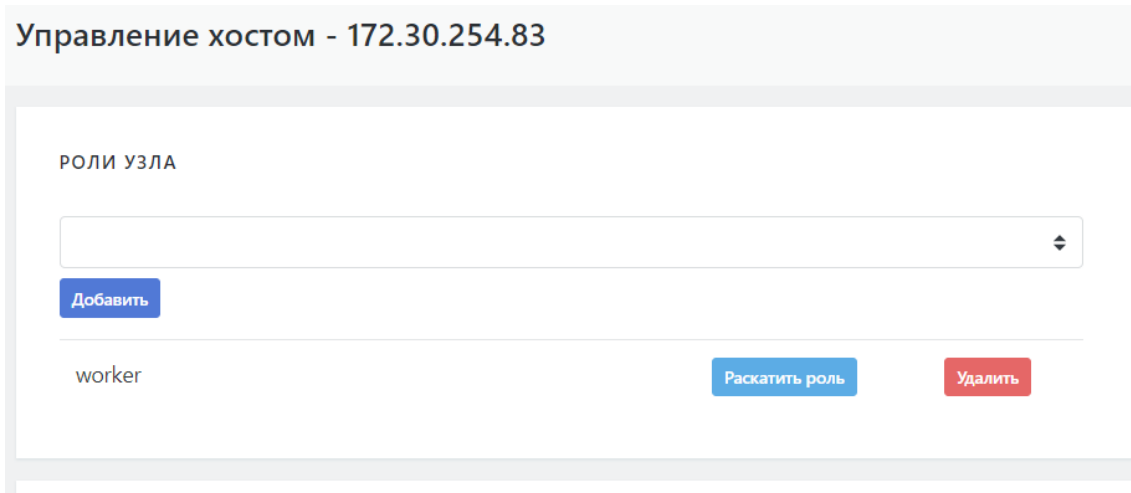


Рисунок 34 - Установка роли на новый узел кластера

4. После чего начнется установка сервисов роли с отображением журнала установки (см. рисунок 35):

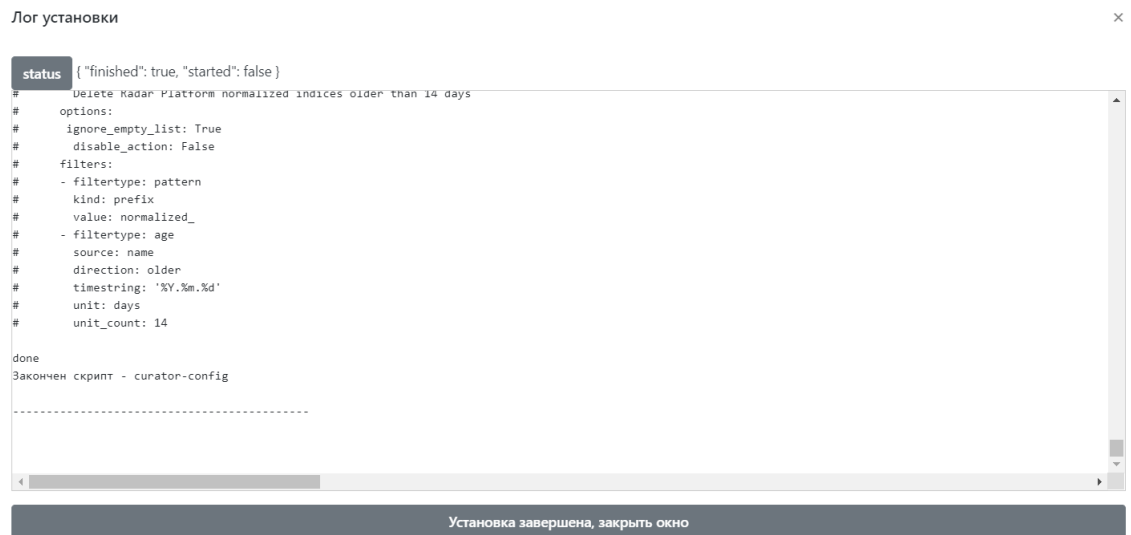


Рисунок 35 - Процесс установки роли

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 36):

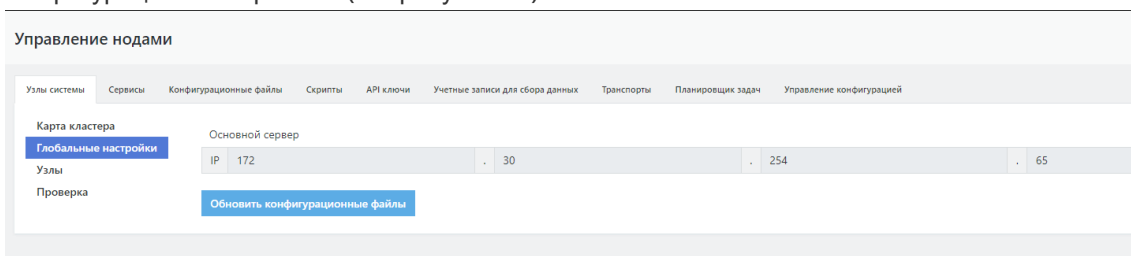


Рисунок 36 - Синхронизация конфигурационных файлов

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 типы источников (Приложение Г: "Включение источников").

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

1. Перейдите в раздел «Кластер».
2. На вкладке «Узлы системы» перейдите в раздел "Узлы" и кликните на IP-адрес узла, на котором располагается неработающий сервис (см. рисунок 37).

Добавление ролей к узлам

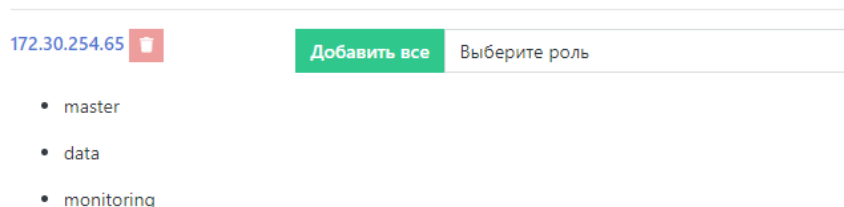


Рисунок 37 - Выбор узла

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 38).

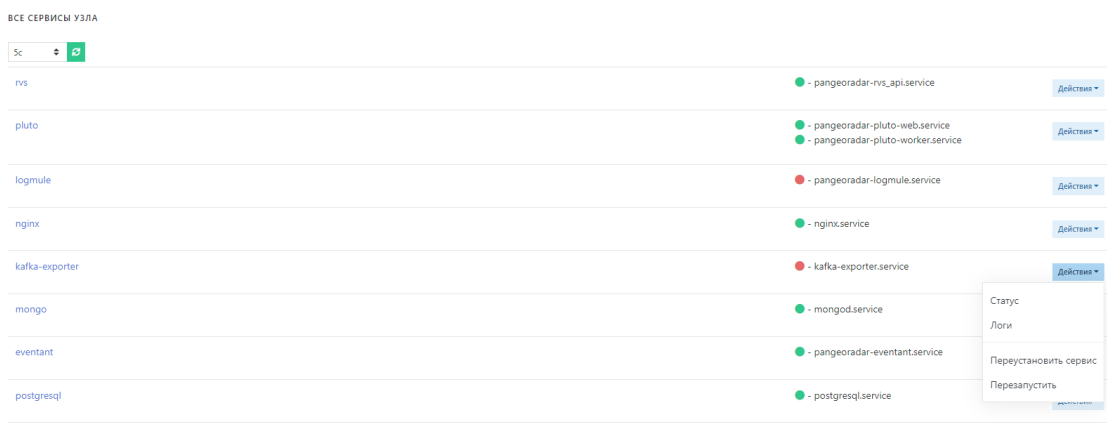


Рисунок 38 - Панель "Все сервисы узла"

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

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