

Платформа Радар

Руководство по установке и обновлению

Версия 3.6.7

ООО «Пангео Радар»

Оглавление

1.	Γ	Тодгот	овка к установке	4
	1.1	. Фо	рма поставки	4
	1.2	. Oc	новные этапы установки и запуска Платформы Радар	4
	1.3	. По	дготовка оборудования	4
	1	.3.1	Подготовка дисковой системы	4
	1	.3.2	Подготовка аппаратной части	5
	1	.3.3	Настройка сетевой конфигурации	5
	1	.3.4	Настройка NTP	6
	1	.3.5	Подготовка для установки Платформы Радар без доступа к сети Интернет	6
	1	.3.6	Подготовка для развертывания Платформы Радар с доступом к сети Интернет	6
2.	3	стано	вка Платформы Радар	7
	2.1	. По	дготовка установочных файлов	7
	2.2	. 3ar	луск скрипта для установки	7
	2.3	. Пр	одолжение установки в веб-интерфейсе	8
	2.4	. 3ar	іуск установки	12
	2.5	. Пр	оверка работоспособности ПО	13
	2	2.5.1	Первичное конфигурирование Платформы Радар	16
	2	.5.2	Синхронизация с Базой Знаний	16
	2.6	. Bo	зможные проблемы	16
3.	C	Особен	ности распределенной установки	18
	3.1	. Oc	обенности подготовки оборудования	18
	3	8.1.1	Подготовка дисковой системы к распределенной установке	18
	3	8.1.2	Настройка сетевой конфигурации при распределенной установке	18
	3.2	. Pao	спределенная установка	20
	3	3.2.1	Подготовка установочных файлов Платформы Радар	20
	3	3.2.2	Продолжение установки в веб-интерфейсе	21
	3	3.2.3	Запуск установки ролей Платформы Радар	24
	3.3	. Пр	оверка распределенной установки и работоспособности ПОПО	25
	3	3.3.1	Первичное конфигурирование Платформы Радар	28
	3	3.3.2	Синхронизация с Базой Знаний	29
	3	3.3.3	Добавление нового узла кластера	29
	3.4	. Bo	зможные проблемы	31
4.	Γ	Троцед	ура обновления	33
5.	P	ешени	ие проблем	36
	5.1	. Сб	ор диагностической информации при типе установки "Все в одном" (All-in-One)	36
	5.2	. Pex	кимы работы Платформы Радар	36

5.2.1	Штатный режим	.36
5.2.2	Сервисный режим	36
5.2.3	Режим обслуживания компонента LOG-COLLECTOR	36
5.2.4	Режим обслуживания компонента BALANCER	37
5.2.5	Режим обслуживания WORKER	37
5.2.6	Режим обслуживания MASTER	37
5.2.7	Режим обслуживания компонента DATA	37
5.2.8	Режим обслуживания CORRELATOR	37

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 <u>сайте</u>);
- 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:
 - о **по SSH;**
 - физический доступ к серверу с клавиатурой и монитором;
 - о консоль MGMT интерфейса;
 - о 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 «<u>Подготовка для установки Платформы Радар без доступа к сети</u> <u>Интернет»</u> 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 http://mirror.yandex.ru/debian buster-updates main
deb http://mirror.yandex.ru/debian buster-updates main
deb 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
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).

```
a.kurkov@v-stand-25:/var/tmp$ 1s
pgr-3.3.l-rc3.tar.gz
systemd-private-dcb8fd6f7f724cb58a7414e48dab6dac-systemd-timesyncd.service-K8oRb
N
a.kurkov@v-stand-25:/var/tmp$
```

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).

Komaндoй 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 u /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).

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 \rightarrow /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



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).



Мастер установки

Лицензия	Глобальные настройки	Узлы	Установка
Код активации			
eyJwYXNzljoiODgwYTlxNT	lzZDE5ZWZiNWZmNDhjY2Q4MWY5NzA	5NjEiLCJod2kiOiJINHNJ	QUFBQUFBQUEvK3ł
Лицензия			
			1
Активировать			
Назад			Далее

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).

≡	ПАНГЕО РАДАР	Клиентский по	ртал				③ Документ	тация 🛛 🔕 test 🗸
۵	Активны	е лицензии				Активн	ые тикеты в поддержку	
Ц	Тип	Приобретена ψ	Техническая поддержка до \downarrow	$EPS \ \Downarrow$		Nº	Тема обращения	
	full	08.02.2023	08.02.2024	10000	Требуется активация		Нет обращений	
							Создать обращения	

Рисунок 4 – Клиентский портал Платформы Радар

 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).

≡	К ПАНГЕО РАДАР	Клиентский по	ртал					③ Документация	\bigotimes test \vee
â	Активн	ые лицензии				Активн	ые тикеты в поддержку		
Ц	Тип	Приобретена ↓	Техническая поддержка до \downarrow	$EPS \ \Downarrow$		№ Тема обращения			
	full	08.02.2023	08.02.2024	10000	Лицензия		Нет обращен	ий	
						Создать обращен		вния	

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**".

Активные лицензии					Активные тикеты в поддержку		
Тип	Приобретена ↓	Техническая поддержка до ↓	$EPS \ \Downarrow$		Nº	Тема обращен	ния
full	08.02.2023	08.02.2024	10000	Лицензия Скачать лицензию ZzpRDss458GXBwWLpeUsPO	tbPRhrwsr7jeie	X eGwxKmd	Нет обращений Создать обращения
				Construction of the constr	KFh20Sk2MuW V63y/wqlc6xm b+kb2aL9mVk, Gab189NrTMct rhZsLab4J1CY +RRofIZEtxfVnl DCB2YCn24+B A4VNUGs2qg: Скопироват	<pre>////////////////////////////////////</pre>	

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).



Мастер установки

	Глобальные настр	ойки	Узлы	Установка					
Осн	Основной сервер								
IP	172	. 30	. 254	. 65					
Haa	зад			Далее					

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).

Мастер установки

Глобальные настройки			Узлы	Установка		
Добавление нового узла						
Название			Порт			
			22			
Введите имя						
Логин			Пароль			
root						
IP	dat mo	a nitor	ing			
Введите ір	wor infr bac	rker a :kup				
Добавление ролей к узлам	cor age But	ance relate ent_w 6epu	r or vin тероль			
172.30.254.65 👕 Добавить во	се Вы	бери	те роль		÷	+
• master						
Роль data не добавлена						
Роль monitoring не добавлена						

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".

Мастер установки

	Глобальные настройки	Узлы	Установка						
	Начать установку								
Назад									

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

L28985 (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).

Управление нодами								
Узлы системы Сервисы Конфиг	лрационные файлы Скрипты API	ключи Учетные записи для сбора данных	Транспорты Планировщик зада	ч Управление конфигурацией				
Карта кластера Глобальные настройки	Вручную 🕈 💋							
Узлы Проверка	172.30.254.65 Настройки							
	rvs				- pangeoradar-rvs_api.service			
	pluto				 pangeoradar-pluto-web.service pangeoradar-pluto-worker.service 			
	logmule				- pangeoradar-logmule.service			
	nginx				- nginx.service			
	kafka-exporter				- kafka-exporter.service			
	mongo				- mongod.service			
	eventant				- pangeoradar-eventant.service			
	postgresql				- postgresql.service			
	redis-exporter				- redis_exporter.service			
	prometheus				- prometheus.service			

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).

Вручную 🗘 🞜	
172.30.254.65	Настройки

Рисунок 14 – Настройка узла (ноды)

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

все сервисы узла		
Sc 🗢 🔁		
rvs	- pangeoradar-rvs_api.service	Действия 🔻
pluto	 pangeoradar-pluto-web.service pangeoradar-pluto-worker.service 	Действия -
logmule	- pangeoradar-logmule.service	Действия 🔻
nginx	- nginx.service	Действия 🔻
kafka-exporter	- kafka-exporter.service	Действия 🕶
mongo	 - mongod.service 	Статус Логи
eventant	 pangeoradar-eventant.service 	Переустановить сервис
postgresql	 postgresql.service 	Перезапустить
redis-exporter	- redis_exporter.service	Действия 👻

Рисунок 15 – Выбор действий

×

 \times

5. В выпадающем меню выбрать необходимый пункт:

• Статус - выводит информацию о состоянии сервиса (см. рисунок 16);

Статус

 pangeorad 	tar-rvs_api.service - Pangeo Radar rvs_api
Loaded:	loaded (/etc/systemd/system/pangeoradar-rvs_api.service; enabled; vendor preset: enabled)
Active:	active (running) since Tue 2022-08-23 10:59:26 MSK; 3h 37min ago
Main PID:	13592 (python3)
Tasks:	8 (limit: 4915)
Memory:	29.1M
CGroup:	/system.slice/pangeoradar-rvs_api.service
	-13592 /opt/pangeoradar/rvs_api/venv/bin/python3 /opt/pangeoradar/rvs_api/venv/bin/rvs_api -c /opt/pangeoradar/configs/rvs_api/conf.yaml

Рисунок 16 – Окно с информацией о состоянии сервиса

Закрыть

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

Лог ошибок

-- Logs begin at Wed 2021-03-17 08:35:28 MSK, end at Wed 2021-03-17 13:41:23 MSK. --Mar 17 11:20:29 pgr-master systemd[1]: Stopping Pangeo Radar Api Gateway... Mar 17 11:20:29 pgr-master systemd[1]: Stopped Pangeo Radar Api Gateway. Mar 17 11:20:29 pgr-master systemd[1]: Started Pangeo Radar Api Gateway.

Закрыть

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 «<u>Решение проблем</u>».

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).

РАДАР		Поиск	Q		
Рабочий стол	г	Тараметры			
ЦЕНТР УПРАВЛЕНИ	1Я				
Просмотр соб	ытий	Общие Обработка	уязвимостей Синхрониз	ация с Базой Знаний	
• Инциденты	<	Синхронизация типов и	нцидентов Статус синхро	онизации: Завершена в 2	024-06-18 17:27:15
🛱 Активы	< 1				
💧 Оценка соотве	етствия ПО <				
🖮 Отчеты					
📙 Коррелятор	¢				
📽 Параметры	~				

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);



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).

ВСЕ СЕРВИСЫ УЗЛА		
5c 🗢 😫		
rvs	- pangeoradar-rvs_api.service	Действия -
pluto	 pangeoradar-pluto-web.service pangeoradar-pluto-worker.servic 	е Действия -
logmule	- pangeoradar-logmule.service	Действия -
nginx	- nginx.service	Действия 🔻
kafka-exporter	- kafka-exporter.service	Действия -
mongo	- mongod.service	Статус Логи
eventant	- pangeoradar-eventant.service	Переустановить сервис
postgresql	- postgresql.service	Перезапустить
	D	

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 «<u>Подготовка к</u> <u>установке</u>»), 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	162SNMPtrap;4807UDPreceiver;4808TCPreceiver;4809TCPreceiver;4810HTTPreceiver;4811HTTPSreceiver;4812NetFlowreciver	Пассивный сбор событий	

Исходящий	Входящий	Порты	Описание
Пользователи Платформы Радар	Master	8080 9000 6676 6677	Доступ к интерфейсу Платформы Радар, проверка АРІ 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).

```
a.kurkov@v-stand-25:/var/tmp$ ls
pgr-3.3.l-rc3.tar.gz
systemd-private-dcb8fd6f7f724cb58a7414e48dab6dac-systemd-timesyncd.service-K8oRb
N
a.kurkov@v-stand-25:/var/tmp$
```

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 «<u>Продолжение установки в веб-интерфейсе</u>»).
- 3. После активации лицензии нажмите кнопку далее, после чего будет отображен экран глобальных настроек (см. рисунок 22).



Мастер установки

Глобальные настр	оойки	Узлы	Установка
Основной сервер			
IP 172	. 30	. 254	. 65
Назад			Далее

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).

Мастер установки

Глобальные настройки		Узлы	Установка	
Добавление нового узла				
Название		Порт		
		22		
Введите имя				
Логин		Пароль		
root				
IP	data moi age wor	a nitoring nt ker		
^{Введите ір} Добавление ролей к узлам	infra bac bala corr age Bac	а kup ancer relator nt_win берите роль		
172.30.254.65 📋 Добавить во	се Выб	берите роль	÷	+
• master				
Роль data не добавлена				
Роль monitoring не добавлена				

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):

Глобальные настройки	Узлы	Установка
Добавление нового узла		
Название	Порт	
balancer01	22	
Логин	Пароль	
root		
IP		
172.30.254.81	Добавить	
Successfully /opt/pangeoradar/distrs director (Reading database 28160 files and direct Preparing to unpack/pangeoradar-cluster- Unpacking pangeoradar-cluster-agent (3.0.10. Setting up pangeoradar-cluster-agent (3.0.10) Created symlink /etc/systemd/system/multi-us Successfully generate remote ssh key/nSucces Successfully /opt/pangeoradar/distrs director (Reading database 28160 files and direct Preparing to unpack/pangeoradar-cluster- Unpacking pangeoradar-cluster-agent (3.0.10. Setting up pangeoradar-cluster-agent (3.0.10) Created symlink /etc/systemd/system/multi-us	<pre>ory create/nFile Copy success/ns cories currently installed.) agent_amd64.deb 3) 3) cer.target.wants/pangeoradar-clu ssfully get remote ssh key/nSuccess/ns cories currently installed.) agent_amd64.deb 3) 0.3) cer.target.wants/pangeoradar-clu</pre>	Selecting previously unselected pa uster-agent.service → /etc/systemc cessfully add master ip to hosts f Selecting previously unselected pa uster-agent.service → /etc/systemc

Рисунок 24 – Добавление нового узла

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

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	ŧ	+
• worker				-
172.30.254.84 👕	Добавить все	Выберите роль	\$	+
• data				-
172.30.254.85 👕	Добавить все	Выберите роль	\$	+
correlator				-
Назад			Да	лее

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"...

Мастер установки

Глобальные настройки	Узлы	Установка
	Начать установку	
Назад		



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

L28985 (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).

 Рабочий стол 	Управление нодами		
	Узлы системы Сервисы Конфі	игурационные файлы Скрипты АРІ ключи Учетные записи для сбора данных	Транспорты Планировщик задач Управление конфигурацией
О, Просмотр событий	Управление мультиарендностью		
Инциденты <			
	Карта кластера	Добавление нового узла	
🖥 Оценка соответствия ПО 🧹	Узлы	Название	Πορτ
	Проверка		22
📙 Коррелятор <		Введите имя	
🕫 Параметры 🧹			
алминистрирование		Логин	Пароль
Пользователи и права		root	
Kracran		IP	
T Meronautra			Добавить
ы источники		ведите ір	
Мониторинг			
Репутационные списки <		Добавление ролей к узлам	
База знаний <			
💷 Лицензия		Добавить все Выберите роль	÷ +
		• master	
		• data	
		monitoring	
		worker	

Рисунок 28 – Раздел управления кластером

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

Управление			Управление нод						
Узлы системы Сервисы Конф	ригурационные файлы Скрипты	АРі ключи Учетные записи для сбора данных Транспорты Планировщик задач							
Карта кластера Глобальные настройки	Добавление новог	го узла							
Узлы	Название	Порт							
Проверка		22							
	Введите имя								
	Логин	Пароль							
	root								
	IP								
		Добавить							
	Введите ір								
	Добавление ролей к узлам								
	*	Добавить все Выберите роль	÷ +						
	master								
	 monitoring 								
	• infra								
		Добавить все Выберите роль	¢ +						
	balancer								
	1	добавить все Выберите роль	¢ +						
	worker								
		Добавить все Выберите роль	•						
	 correlator 								
		Добавить все Выберите роль	¢ •						
	• data								
		Добавить все Выберите роль	÷ •						
	correlator								

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.

Управление											Управление нодами
Узлы системы	Сервисы	Конфиг	урационные файлы	Скрипты	API ключи	Учетные записи для сбора данных	Транспорты	Планировщик задач			
Карта класт Глобальны	тера е настройки		Вручную 🗢 足								
Проверка		ה		Настро	йки				_	_	
			prometheus						•	- prometheus.service	
			knowledgebase			5			:	- pangeoradar-kb.service - pangeoradar-kb-sidekiq.service	
			rmca						:	- pangeoradar-rmca.service - pangeoradar-rmca-sidekiq.service	
			grafana						•	- grafana-server.service	
			toller							pangeoradar-toller service	

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).

Уг	правление хостом -				У	правление нодами 🗦	Управление хостом
	роли узла			дополнительные сервисы узла	ι.		
			\$				\$
	Добавить			Добавить			
	balancer	Раскатить роль	Удалить				
	1 ²						
	все сервисы узла						
	5c 🗢 💋						
	kafka				 pangeoradar-kafka.service 		Действия *
	node-exporter				- node_exporter.service		Действия 🔻
	kafka-exporter				 kafka-exporter.service 		Действия 🔻
	rsyslog				- rsyslog.service		Действия 🔻
	nginx				- nginx.service		Действия 👻

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).

	Добавить			Добавить	
	balancer	Раскатить роль	Удалить		
В	СЕ СЕРВИСЫ УЗЛА				
	5c 🔶 💋				
	kafka			 pangeoradar-kafka.service 	Действия
	node-exporter			- node_exporter.service	Статус Логи
	kafka-exporter			- kafka-exporter.service	Переустановить сервис
	rsyslog			- rsyslog.service	Обновить конфиг Перезапустить
	nginx			- nginx.service	Действия 🔻

Рисунок 32 – Выбор действия с компонентом

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

Craryc x • pangeoradar <u>(afka.service</u> Apache Kafka Server Loaded: loaded (/etc/system/system/pangeoradar-kafka.service; enabled; vendor preset: enabled) Active: active (running) since Tue 2022-02-01 15:06:55 MSK; 4h 36min ago Docs: http://kafka.apache.org/documentation.html Main PID: 29211 (java) Tasks: 80 (limit: 4915) Memory: 1011.2% CGroup: /system.slice/pangeoradar-kafka.service _29211 /usr/lib/jvm/java-1.11.0-openjdk-amd64/bin/java -xmx1G -xms1G -server -xX:+UseGIGC -XX:MaxGCPauseMillis=20 -XX:InitiatingHeapOccupancyPercent=35 -: Действия Закрыть			🔁 Назад	
<pre> • pangeoradar kafka.service Apache Kafka Server Loaded: loaded (/etc/system/pangeoradar-kafka.service; enabled; vendor preset: enabled) Active: active (running) since Tue 2022-02-01 15:06:55 MSK; 4h 36min ago Docs: http://kafka.apache.org/documentation.html Main PID: 20211 (java) Tasks: 80 (limit: 4915) Memory: 1011.2M CGroup: /system.slice/pangeoradar-kafka.service</pre>	Статус	X		
 pangeoradar <u>kafka.servic</u> Apache Kafka Server Loaded: loaded (/etc/system/system/pangeoradar-kafka.service; enabled; vendor preset: enabled) Active: active (running) since Tue 2022-02-01 15:06:55 MSK; 4h 36min ago Docs: http://kafka.apache.org/documentation.html Main PID: 29211 (java) Tasks: 80 (limit: 4915) Memory: 1011.2M CGroup: /system.slice/pangeoradar-kafka.service 29211 /usr/lib/jvm/java-1.11.0-openjdk-amd64/bin/java -Xmx1G -Xms1G -server -XX:+UseGIGC -XX:MaxGCPauseMillis=20 -XX:InitiatingHeapOccupancyPercent=35 -: Действия Закрыть Kafka-exporter 				
Loaded: loaded (/etc/system/pageoradar-kafka.service; enabled; vendor preset: enabled) Active: active (running) since Tue 2022-02-01 15:06:55 MSK; 4h 36min ago Docs: http://kafka.apache.org/documentation.html Main PID: 29211 (java) Tasks: 80 (limit: 4915) Memory: 1011.2M CGroup: /system.slice/pangeoradar-kafka.service L29211 /usr/lib/jvm/java-1.11.0-openjdk-amd64/bin/java -Xmx16 -server -XX:+UseG16C -XX:MaxGCPauseMillis=20 -XX:InitiatingHeapOccupancyPercent=35 -: Aekcraw Bakpurb Kafka-exporter Kafka-exporter	 pangeorad 	ar <mark>kafka.service -</mark> Apache Kafka Server		
Active: active (running) since Tue 2022-02-01 15:06:55 M5K; 4h 36min ago Docs: http://kafka.apache.org/documentation.html Main PID: 29211 (java) Tasks: 80 (limit: 4915) Memory: 1011.2M CGroup: /system.slice/pangeoradar-kafka.service CGroup: /system.slice/pangeoradar-kafka.service /kmsiG -server -xX:+UseGiGC -XX:MaxGCPauseMillis=20 -XX:InitiatingHeapOccupancyPercent=35 -: Aewcrount Закрыть kafka-exporter	Loaded:	loaded (/etc/systemd/system/pangeoradar-kafka.service; enabled; vendor preset: enabled)		
Docs: http://kafka.apache.org/documentation.html Main PID: 29211 (java) Tasks: 80 (linit: 4915) Memory: 1011.2M GGroup: /system.slice/pangeoradar-kafka.service	Active:	active (running) since Tue 2022-02-01 15:06:55 MSK; 4h 36min ago		
Main PID: 29211 (java) Tasks: 80 (limit: 4915) Memory: 1011.2M CGroup: /system.slice/pangeoradar-kafka.service 	Docs:	nttp://kafka.apache.org/documentation.html		
Tasks: 80 (Limit: 4915) Memory: 1011.2M CGroup: /system.slice/pangeoradar-kafka.service 	Main PID:	29211 (java)		
Memory: 1911.2M CGroup: /system.slice/pangeoradar-kafka.service /usr/lib/jvm/java-1.11.0-openjdk-amd64/bin/java -XmxIG -XmsIG -server -XX:+UseGIGC -XX:MaxGCPauseMillis=20 -XX:InitiatingHeapOccupancyPercent=35 -: Дейстил Каfka-exporter kafka-exporter	Tasks:	30 (limit: 4915)		
CGroup: /system.slice/pangeoradar-kafka.service	Memory:	1811.2M		
29211 /usr/lib/jvm/java-1.11.0-openjdk-amd64/bin/java -Xmx1G -Xms1G -server -XX:+UseGIGC -XX:MaxGCPauseMillis=20 -XX:InitiatingHeapOccupancyPercent=35 -: Действия Закрыть Каfka-exporter Каfka-exporter	CGroup:	/system.slice/pangeoradar-kafka.service		
Аейстан Закрыть kafka-exporter kafka-exporter		└─29211 /usr/lib/jvm/java-1.11.0-openjdk-amd64/bin/java -Xmx1G -Xms1G -server -XX:+UseG1GC -XX:MaxGCPauseMillis=20 -XX:InitiatingHeapOccupancyPercent=35 -:		
Аейстаи Закрыть kafka-exporter kafka-exporter				
Аействи Закрыть kafka-exporter kafka-exporter.service				
Закрыть Действи kafka-exporter	4		Дейст	твия 🔻
Закрыть Дейстии kafka-exporter				
Aeitravi kafka-exporter • kafka-exporter.service		Закирыть		
kafka-exporter • kafka-exporter.service		закроти	Дейст	твия 🔻
kafka-exporter				
kafka-exporter 🖉 – kafka-exporter.service				
ва деистви	ава	kafka-exporter • kafka-exporter.service	Дейст	твия 👻

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).

Logs	; begin a	t Sun 20	21-12-19	19:11:13 MSK,	end at Tue 20	22-02-01	19:50:	13 MSK							
Feb 01	15:07:00	v-study	-balancer	kafka-server	-start.sh[2921	1]: [202	2-02-01	15:07:00,360	INFO	Static member Member	Metadata(memb	erId=rdkafka	a-e41d	7e7e-434e-4e	e76-9eb5-5
Feb 01	15:07:00	v-study	-balancer	kafka-server	-start.sh[2921	1]: [202	2-02-01	15:07:00,360]	INFO	[GroupCoordinator 0]	: Loading gro	up metadata	for 99	999-Radar-IO	CS with ge
Feb 01	15:07:00	v-study	-balancer	kafka-server	-start.sh[2921	1]: [202	2-02-01	15:07:00,361]	INFO	[GroupMetadataManage	r brokerId=0]	Finished lo	oading	offsets and	d group me
Feb 01	15:07:00	v-study	-balancer	kafka-server	-start.sh[2921	1]: [202	2-02-01	15:07:00,361]	INFO	[GroupMetadataManage	r brokerId=0]	Finished lo	oading	offsets and	d group me
Feb 01	15:07:02	v-study	-balancer	kafka-server	-start.sh[2921	1]: [202	2-02-01	15:07:02,212	INFO	[GroupCoordinator 0]	: Preparing t	o rebalance	group	2570-Fortig	gate-Firew
Feb 01	15:07:02	v-study	-balancer	kafka-server	-start.sh[2921	1]: [202	2-02-01	15:07:02,471	INFO	[GroupCoordinator 0]	: Preparing t	o rebalance	group	2604-Kasper	rsky-Secur
Feb 01	15:07:04	v-study	-balancer	kafka-server	-start.sh[2921	1]: [202	2-02-01	15:07:04,563	INFO	[GroupCoordinator 0]	: Preparing t	o rebalance	group	9999-Radar	ICS in st
Feb 01	15:07:04	v-study	-balancer	kafka-server	-start.sh[2921	1]: [202	2-02-01	15:07:04,746	INFO	[GroupCoordinator 0]	: Preparing t	o rebalance	group	3300-ft20_>	kml in sta
Feb 01	15:07:05	v-study	-balancer	kafka-server	-start.sh[2921	1]: [202	2-02-01	15:07:05,093]	INFO	[GroupCoordinator 0]	: Preparing t	o rebalance	group	2162-Cisco-	NetFlow i
Feb 01	15:07:05	v-study	-balancer	kafka-server	-start.sh[2921	1]: [202	2-02-01	15:07:05,850	INFO	[GroupCoordinator 0]	: Preparing t	o rebalance	group	1515-Micros	soft-Windo
Feb 01	15:07:06	v-study	-balancer	kafka-server	-start.sh[2921	1]: [202	2-02-01	15:07:06,361]	INFO	[GroupCoordinator 0]	: Preparing t	o rebalance	group	15405-NIDS-	suricata-
Feb 01	15:07:06	v-study	-balancer	kafka-server	-start.sh[2921	1]: [202	2-02-01	15:07:06,423	INFO	[GroupCoordinator 0]	: Preparing t	o rebalance	group	1514-Micros	soft-Windo
Feb 01	15:07:06	v-study	-balancer	kafka-server	-start.sh[2921	1]: [202	2-02-01	15:07:06,770	INFO	[GroupCoordinator 0]	: Preparing t	o rebalance	group	5552-Audit[) in state

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 вебинтерфейсе.

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).

\mathbf{i}	ПАНГЕО РАДАР	! По	иск Q		
	Рабочий стол	Парам	іетры		
	ТР УПРАВЛЕНИЯ				
Q,	Просмотр событий	Общи	е Обработка уязвимостей	Синхронизация с Базой Знаний	
	Инциденты <	Синх	ронизация типов инцидентов	т атус синхронизации: Заверш	ена в 2024-06-18 17:27:15
	Активы				
	Оценка соответствия ПО 🤇				
	Отчеты				
	Коррелятор <				
¢°	Параметры 🗸				

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).

управление нодами								
Узлы системы Сервисы Конф	игурационные файлы Скрипты АРІ ключи Учетные записи для сбора данных Транспорты Планировци	к задач Управление конфигурацией						
Карта кластера Глобальные настройки	Добавление нового узла							
Узлы	Название	Πορτ						
Проверка		22						
	Введите имя							
	Логин	Пароль						
	root							
	10							
	II	Лобавит						
	Влелите ір	Accession 1997						
	Добавление ролей к узлам							
	172.30.254.65 💼 Добавить все Выберите роль	÷ •						

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).

172.30.254.83	Добавить все	Выберите роль	¢	+
• worker				-

Рисунок 37 – Созданный узел кластера

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

Уп	равление хостом - 172.30.254.83		
	роли узла		
			\$
	Добавить		
	worker	Раскатить роль	Удалить

Рисунок 38 – Установка роли на новый узел кластера

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

Лог установки \times { "finished": true, "started": false } status) Delete Kadar Platform normalized indices older than 14 days * # options: # ignore_empty_list: True # disable_action: False # filters: # - filtertype: pattern # # # # kind: prefix value: normalized_ - filtertype: age source: name direction: older # timestring: '%Y.%m.%d' # unit: days # unit_count: 14 done Закончен скрипт - curator-config -----• Установка завершена, закрыть окно

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).

Управлени	Управление нодами										
Узлы системы	Сервисы	Конфигурационные файлы	Скрипты АРІ ключи	Учетные записи для сбора данных	Транспорты	Планировщик задач	Управление конфигурацией				
Карта клас	тера	Основной серве	p								
Узлы		IP 172		. 30			254	. 65			
Проверка		Обновить конф	игурационные файлы								



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);



 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).

все сервисы узла			
Sc + Ø			
rvs	 pangeoradar-rvs_api.service 		Действия 👻
pluto	 pangeoradar-pluto-web.service pangeoradar-pluto-worker.service 		Действия 👻
logmule	- pangeoradar-logmule.service		Действия 👻
nginx	- nginx.service		Действия 👻
kafka-exporter	- kafka-exporter.service		Действия 🕶
mongo	- mongod.service	Статус Логи	
eventant	 pangeoradar-eventant.service 	Переустанов	ить сервис
postgresql	 postgresql.service 	Перезапустит	допольни
	· · · · · · · ·		

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:

- 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 <u>https://portal.pangeoradar.ru/login</u> или направить письмо на электронный адрес <u>support@pangeoradar.ru</u>.
- 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: <u>https://192.168.1.10:8180</u>
 - Проверить работоспособность каждого обновляемого инстанса.
- мастер-ноду 4. С клиентского портала скачать 3.6.* на версию релиза 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:

 Рабочий стол 	Управле	ние муль	ьтиарендностью							
центр управления С. Просмотр событий Инциденты <	Узлы систен Управление	ны Сервисы мультиаренднос	Конфигурационные фай. тъю	ты Скрипты	АРІ ключи	Учетные записи для сб	ора данных	Транспорты	Планировщик задач	Управление конфигурацией
а Активы <	списо	ИНСТАНСОВ								РЕДАКТИРОВАНИЕ ИНСТАНСА
Оценка соответствия ПО	Id			Название	Адрес		Версия			Название
Коррелятор <	and the	a dia art	-f2ca7245fe70	.62	https://	62:9000	3.5.3	Редактироват	ь Удалить	.62
🕸 Параметры <	4		-4a137f398194	.51	https://	.51:9000	3.3.2	Редактироват	ь Удалить	Адрес
АДМИНИСТРИРОВАНИЕ 🌲 Пользователи и права										Версия релиза
📥 Кластер 🚹										3.5.3
∷ Источники <										Сортировка
🗠 Мониторинг										0
 Репутационные списки База знаний 										Отмена Сохранить

Рисунок 43 – Управление мультиарендностью. Редактирование основной ноды

Для подчинённой:

Рабочий стол	Управление мультиаре	ндностью				
ентр управления Просмотр событий	Узлы системы Сервисы Конфи	гурационные файлы Скрипты	АРІ ключи Учетные запис	и для сбора данных Трансп	орты Планировщик задач	Управление конфигура.
Инциденты <	2					
а Активы «	список инстансов					редактирование
Оценка соответствия ПО						Название
	Id	Название	Адрес	Версия		.51
Коррелятор <	f2ca	7245fe70 .62	https:// 62:90	00 3.5.3 Редан	тировать Удалить	
6 Параметры <	-4a1	37f398194 .51	https:// .51:90	00 3.3.2 Редан	тировать Удалить	Адрес
					3	https://*
Пользователи и права						Версия релиза
Кластер						3.3.2
Источники «						Сортировка
Мониторинг						1
Репутационные списки «						
База знаний 🕔						Отмена Сохра

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 OC от администратора не требуется дополнительных действий. Если в рамках проводимых работ не требовалась перезагрузка OC, 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.