АО "НТЦ ИТ РОСА"

ПЛАТФОРМА ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ ОПЕРАЦИОННЫХ СИСТЕМ "РОСА ЦЕНТР УПРАВЛЕНИЯ"

Версия 2.4.0

Руководство системного администратора

Часть 1. Установка и настройка

РСЮК.10121-09 32 01

Листов 77

2025

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

АННОТАЦИЯ

Данное руководство предназначено для системных администраторов, осуществляющих развертывание, сопровождение и контроль функционирования программного средства "Платформа централизованного управления жизненным циклом операционных систем "РОСА Центр Управления" РСЮК.10121-09 (далее – РОСА Центр Управления, Комплекс).

В руководстве содержатся сведения о процессе и параметрах установки РОСА Центр Управления, а также информация, необходимая для выполнения первичной настройки Комплекса.

Сведения, необходимые для эксплуатации РОСА Центр Управления, приведены в документе "РОСА Центр Управления. Руководство системного администратора. Часть 2. Эксплуатация" (шифр РСЮК.10121-09 32 02).

Перед установкой РОСА Центр Управления рекомендуется внимательно ознакомиться с настоящим руководством.

При разработке документа использованы ссылки на следующие стандарты:

– ГОСТ Р 2.105-2019 "Единая система конструкторской документации (ЕСКД). Общие требования к текстовым документам";

– ГОСТ 2.601 "Единая система программной документации. Виды программных документов";

– ГОСТ 19.101-77 "Единая система программной документации. Виды программ и программных документов";

– ГОСТ 19.105-78 "Единая система программной документации. Общие требования к программным документам";

– ГОСТ 19.503-79 "Единая система программной документации. Руководство системного программиста".

Настоящий документ подготовлен в соответствии с технологической инструкцией "РОСА. Регламент формирования документации к программным продуктам" (шифр РСЮК.11001-02 90 01).

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

РОСА Центр Управления обеспечивает централизованное управление жизненным циклом гибридной ИТ-инфраструктуры корпоративного уровня, включающей инфраструктуру физической, виртуальной и частной облачной среды организации.

РОСА Центр Управления позволяет осуществлять сетевое развертывание (установку ОС и настройку системной конфигурации) управляемых узлов (физических серверов и ВМ) в автоматическом режиме. При этом сетевое развертывание осуществляется на новых узлах без предустановленной ОС, а уже существующие узлы (ранее развернутые другим способом) могут быть зарегистрированы в РОСА Центр Управления в установленном порядке.

Сетевая установка ОС на новых узлах выполняется в автоматическом режиме с использованием DHCP и TFTP, а также применением сценария развертывания Kickstart. Развертывание управляемых узлов осуществляется в локальной подсети, непосредственно подключенной к маршрутизатору организации и к одному из сетевых интерфейсов сервера РОСА Центр Управления. Поэтому в процессе установки РОСА Центр Управления необходимо указать используемый сетевой интерфейс сервера и IP-адрес маршрутизатора подсети. На указанном сетевом интерфейсе будут развернуты DHCP и TFTP, а IP-адрес маршрутизатора будет передан управляемым узлам через DHCP в качестве маршрута по умолчанию.

Примечание – Узлы, находящиеся вне управляемой локальной подсети, не могут быть инициализированы по сети автоматически, так как DHCP будет недоступен вне своей подсети. Однако, можно установить ОС на узел с носителя и в дальнейшем зарегистрировать такой узел в РОСА Центр Управления. В этом случае необходимо настроить сетевые параметры и источники пакетов на узле вручную и после этого провести процедуру регистрации узла.

РОСА Центр Управления предоставляет графический веб-интерфейс для централизованного мониторинга и конфигурирования управляемых узлов. При этом доступ пользователей к элементам интерфейса Комплекса и к функциональным возможностям операционного управления узлами реализован с применением ролевой модели.

В Комплексе реализованы подсистемы мониторинга, отображения, поиска и аналитики для мониторинга, визуализации и анализа статусов сервисов компьютерной сети, серверов и сетевого оборудования ИТ-инфраструктуры. При наличии в инфраструктуре организации существующих систем мониторинга, отображения, поиска и аналитики добавлена возможность их миграции в Комплекс.

Поддержка доменов службы каталогов для аутентификации и авторизации доменных пользователей обеспечивается за счет интеграции РОСА Центр Управления с внешней системой идентификации, политик и аудита (СИПА).

Примечание – СИПА представляет собой контроллер домена на базе FreeIPA, который обеспечивает управление учетными записями пользователей, доменом и зонами DNS. Механизм управления описан в документации на службу каталогов FreeIPA (https://www.freeipa.org/page/Documentation.html).

Следует обратить внимание, что совместная установка СИПА и РОСА Центр Управления на один сервер не допускается. Поэтому необходимо либо включить РОСА Центр Управления в существующий домен СИПА (при наличии), либо предварительно установить СИПА на отдельный сервер (подраздел 3.1).

Общая схема взаимодействия сервера РОСА Центр Управления с сервером СИПА и управляемыми узлами представлена на рисунке 1.

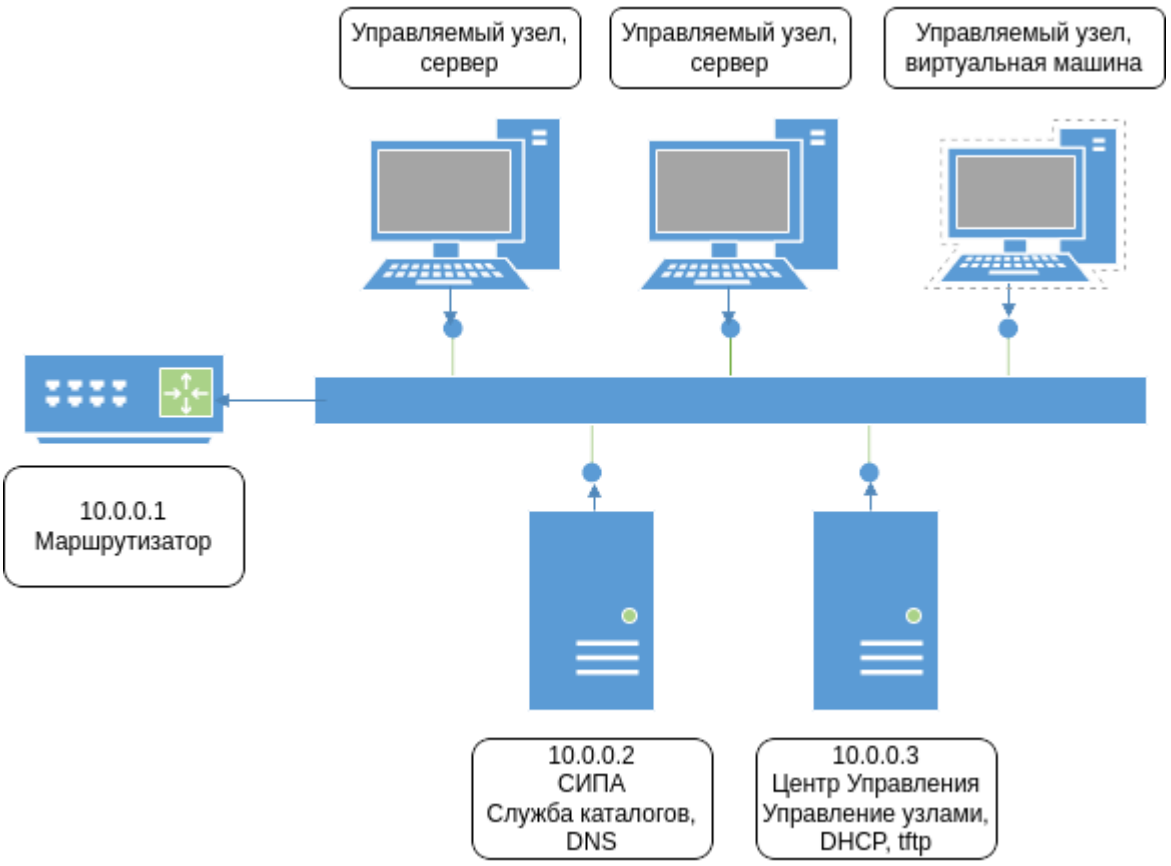

Рисунок 1 – Общая схема конфигурации РОСА Центр Управления

В общей схеме конфигурации сервер СИПА и сервер РОСА Центр Управления находятся в одной локальной подсети с управляемыми узлами и подключены к одному коммутатору.

Сервер СИПА обеспечивает управляемым узлам и серверу РОСА Центр Управления доступ к службам каталогов и DNS.

РОСА Центр Управления в процессе своей установки регистрируется в службе каталогов и создает необходимые принципалы (уникальные имена) Kerberos для управления записями в зоне DNS. Таким образом, РОСА Центр Управления получает возможность регистрировать узлы в домене и автоматически создавать все необходимые записи для управляемых узлов.

РОСА Центр Управления функционирует в своей локальной подсети в качестве сервера DHCP и TFTP, назначает управляемым узлам IP-адреса, передает сетевые настройки, обеспечивает сетевую загрузку и установку ОС, а в качестве маршрута по умолчанию РОСА Центр Управления назначает узлам IP-адрес маршрутизатора (например, 10.0.0.1).

Все управляемые узлы через DHCP настраиваются таким образом, что используют сервер СИПА в качестве своего основного сервера DNS и в дальнейшем могут разрешать доменные имена узлов из своей подсети в IP-адреса.

Примечание – Для того, чтобы управляемые узлы могли разрешать имена узлов из других подсетей организации и/или сети Интернет, на сервере СИПА необходимо настроить перенаправители зон и/или глобальные перенаправители на серверы DNS организации и/или на серверы DNS интернет-провайдера.

Сервер РОСА Центр Управления передает собственный IP-адрес (например, 10.0.0.3) агенту Puppet, принимает и регистрирует отчеты агента управления конфигурацией, обеспечивает управление этим агентом, а также предоставляет агенту доступ к классам Puppet.

2 УСЛОВИЯ ВЫПОЛНЕНИЯ УСТАНОВКИ

2.1 Требования к аппаратным средствам

2.1.1 Сервер РОСА Центр Управления

Требования к аппаратным средствам сервера, предназначенного для установки РОСА Центр Управления, приведены в таблице 1.

Таблица 1 – Требования к аппаратным средствам сервера РОСА Центр Управления

Параметр	Минимальное значение	Установка ОС с управлением содержимым
Количество ядер процессора	4	8
Объем оперативной памяти, Гбайт	8	20
Свободное дисковое пространство, Гбайт	40	80

Примечание – Для повышения производительности РОСА Центр Управления рекомендуется увеличить количество процессоров, а для ускорения работы подсистемы ввода-вывода (осуществление операций чтения-записи базы данных, ведение журналов и индексирование классов Puppet) рекомендуется использовать накопители SSD или иные носители высокой производительности.

Следует обратить внимание, что при увеличении количества управляемых узлов может потребоваться дополнительное дисковое пространство для хранения журналов.

2.1.2 Сервер СИПА

Требования к аппаратным средствам сервера, предназначенного для установки СИПА, приведены в таблице 2.

Таблица 2 – Требования к аппаратным средствам сервера СИПА

Параметр	Минимальное значение	Рекомендуемое значение
Количество ядер процессора	2	4

Параметр	Минимальное значение	Рекомендуемое значение
Объем оперативной памяти в Гбайт	8	16
Свободное дисковое пространство в Гбайт	20	40

2.1.3 Требования к программным средствам

Для функционирования Комплекса следующие порты сервера РОСА Центр Управления должны быть открыты и доступны для входящих соединений, не должны использоваться другими службами или быть заблокированы межсетевым экраном:

– TCP/443 – HTTPS;
– TCP/8140 – Puppet.

Для обеспечения внешней интеграции и обмена информацией серверу РОСА Центр Управления должны быть доступны конечные точки API используемой системы виртуализации (ROSA Virtualization, VMware).

Примечание – Сервер РОСА Центр Управления подключается к контролируемым узлам по протоколу SSH, используя по умолчанию порт TCP/22. Следует обратить внимание, что при использовании иного порта необходимо в процессе настройки РОСА Центр Управления добавить параметр remote_execution_ssh_port, в котором указать используемый номер порта для каждого такого узла.

В случает развёртывания Комплекса в виртуальной среде необходимо использовать виртуальный графический адаптер типа VGA.

Для функционирования Комплекса следующие порты сервера СИПА должны быть открыты и доступны для входящих соединений, не должны использоваться другими службами или быть заблокированы межсетевым экраном:

– TCP/80, TCP/443 – HTTP/HTTPS;
– TCP/389, TCP/636 – LDAP/LDAPS;
– TCP, UDP/88, TCP, UDP/464 – Kerberos;
– TCP, UDP/53 – DNS;
– UDP/123 – NTP.

Примечание – Дополнительно сервер СИПА может анализировать порт 8080 и – в некоторых конфигурациях – порты 8443 и 749. Указанные три порта используются для внутренних подключений и внешний доступ к ним не требуется. Рекомендуется не

открывать порты 8080, 8443, 749 и заблокировать их с помощью межсетевого экрана для входящих соединений.

Доступ к веб-интерфейсу РОСА Центр Управления осуществляется с внешней рабочей станции через один из следующих рекомендуемых браузеров актуальной версии:

– Google Chrome;
– Microsoft Edge;
– Apple Safari;
– Mozilla Firefox, в том числе Mozilla Firefox ESR;
– Яндекс.Браузер.

2.1.4 Требования к персоналу

Системный администратор, осуществляющий процесс установки и первичной настройки РОСА Центр Управления, должен обладать опытом развертывания и сопровождения серверных версий ОС Linux, совместимых с диалектом Red Hat®Enterprise Linux, таких как ROSA Enterprise Linux Server, CentOS и тому подобных.

3 УСТАНОВКА И ПЕРВИЧНАЯ НАСТРОЙКА

В общем случае процесс установки и первичной настройки Комплекса состоит из последовательного выполнения следующих процедур:

– установка СИПА;

– установка РОСА Центр Управления;

– регистрация существующих узлов в РОСА Центр Управления;

– сетевое развертывание новых узлов под контролем РОСА Центр Управления;

– настройка аутентификации пользователей через службу каталогов LDAP сервера СИПА (или иную внешнюю службу каталогов LDAP);

– подключение РОСА Центр Управления к внешней системе виртуализации (ROSA Virtualization, VMware).

3.1 Установка СИПА

В процессе развертывания СИПА системный администратор должен сначала осуществить установку ОС на физический сервер или ВМ, а затем выполнить консольный интерактивный сценарий установки СИПА ipa-server-install.

3.1.1 Установка ОС на сервер СИПА

Установка ОС на сервер СИПА осуществляется системным администратором с использованием носителя с дистрибутивом РОСА Центр Управления из комплекта поставки Комплекса.

Для запуска программы установки ОС требуется провести загрузку сервера СИПА с этого носителя.

На экране последовательно появятся меню программы установки, интерфейс для выбора языка сопровождения установки и меню "Обзор установки", предназначенное для обзора и последующей настройки параметров установки (рисунок 2).

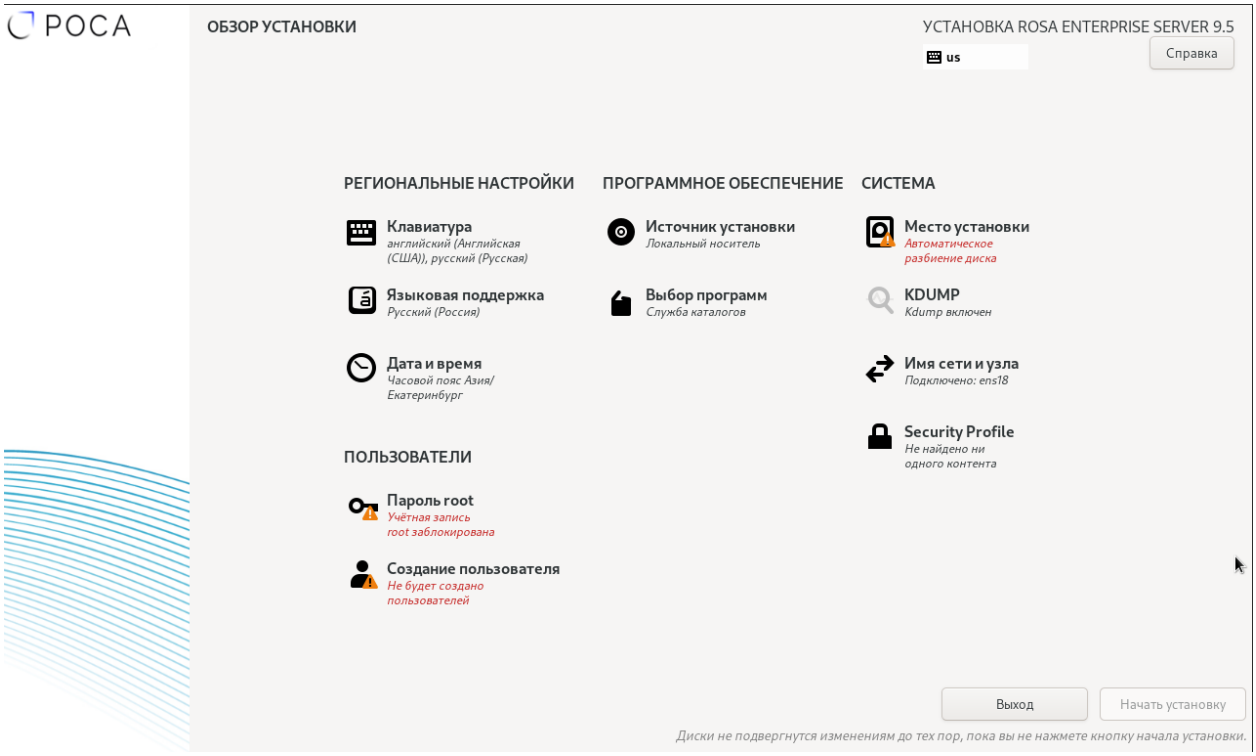

Рисунок 2 – Обзор установки

Панель "Обзор установки" содержит тематические секции, в которые сгруппированы соответствующие параметры установки. Следует обратить внимание, что вместо последовательного определения параметров программа установки дает возможность настроить параметры в произвольном порядке выбором необходимых секций в меню "Обзор установки".

Под наименованием каждой секции приводится информация о текущих параметрах, настроенных автоматически программой установки.

Необходимо убедиться, что в секции "Место установки" автоматически настроен параметр "Локальный носитель".

Для перехода к интерфейсу настройки соответствующих параметров требуется нажать на наименование секции. После настройки параметров нужно нажать кнопку Готово для возвращения в меню "Обзор установки".

В секции "Выбор программ" указывают переключатель "Базовое окружение" в положение "Служба каталогов" для установки соответствующего базового ПО на сервер СИПА.

В секции "Место установки" выбирают необходимый диск и устанавливают переключатель "Конфигурация устройств хранения данных" в положение "Автоматически".

В секции "Имя сети и узла" необходимо задать полное доменное имя сервера СИПА, которое должно быть доменным именем по крайней мере третьего

уровня (например, ipa.rosa.int, где ipa – краткое имя узла, а rosa.int – домен, в котором СИПА будет выполнять функции контроллера домена).

Следует обратить внимание, что СИПА не поддерживает работу с доменом первого уровня. При этом допускается использование домена, начиная с третьего уровня и далее.

Для функционирования СИПА необходим уникальный домен. При выборе домена необходимо избегать использования доменов home.arpa. и local. даже в целях тестирования. Домен home.arpa. выделен IETF для использования в локальных сетях, но глобально обозначен в DNS как занятый и используемый IANA. Домен local. используется с mDNS, что может приводить к проблемам с загрузкой узлов по сети при использовании этого домена.

Далее подключают необходимый сетевой интерфейс сервера СИПА и настраивают параметры сетевого соединения – IP-адрес (например, 10.0.0.2), маску сети (например, 255.255.0.0), шлюз по умолчанию (например, 10.0.0.1).

Необходимо обратить внимание, что IP-адрес сетевого интерфейса сервера СИПА требуется задавать только статическим. Таким образом, заданный IP-адрес контроллера домена не изменится впоследствии, и зарегистрированные в домене узлы не потеряют связь с контроллером.

В секции "Пароль root" устанавливают пароль для учетной записи суперпользователя root.

После настройки всех обязательных параметров нужно нажать кнопку `Начать установку` для запуска процесса установки ОС сервера СИПА.

После завершения процесса установки ОС необходимо нажать кнопку `Перезагрузка системы`.

После перезагрузки системы на экране появится строка приглашения командного интерпретатора для входа в ОС сервера СИПА.

3.1.2 Выполнение сценария установки СИПА

Установка СИПА осуществляется консольной утилитой ipa-server-install.

Примечание – Сценарий установки ipa-server-install создает файл журнала var/log/ipaserver-install.log. В случае неудачной установки СИПА можно просмотреть записи этого журнала для выявления проблемы в процессе установки.

По умолчанию СИПА устанавливается со встроенной службой DNS и со встроенным центром сертификации CA в качестве корневого удостоверяющего центра.

Для запуска интерактивного сценария установки нужно осуществить вход в ОС сервера СИПА от имени учетной записи суперпользователя root и выполнить следующую консольную команду:

```
# ipa-server-install
```

Сценарий установки предложит настроить встроенную службу DNS. Для подтверждения нужно ввести yes:

```
Do you want to configure integrated DNS (BIND)? [no]: yes
```

Далее сценарий установки предложит определенные значения по умолчанию для следующих параметров – имя узла СИПА, имя домена и имя области Kerberos:

```
Server host name [ipa.rosa.int]:
Please confirm the domain name [rosa.int]:
Please provide a realm name [ROSA.INT]:
```

Чтобы принять предложенные значения по умолчанию, нужно нажать клавишу `Enter`.

Для изменения параметра по умолчанию вводят необходимое значение.

Затем требуется установить (ввести и подтвердить) пароли для суперпользователя службы каталогов LDAP (Directory Manager) и для пользовательской административной учетной записи admin СИПА (IPA admin):

```
Directory Manager password:
Password (confirm):

IPA admin password:
Password (confirm):
```

Далее сценарий установки предложит настроить перенаправление DNS:

```
Do you want to configure DNS forwarders? [yes]:
```

Если перенаправление DNS конфигурировать не нужно, вводят no.

Для настройки перенаправления DNS нажимают клавишу `Enter` или вводят yes. Сценарий установки запросит и затем добавит IP-адреса средств перенаправления в файл /etc/named.conf.

После этого сценарий установки предложит проверить, нужно ли настроить какие-либо обратные записи DNS для IP-адресов, связанных с СИПА. Для подтверждения следует нажать клавишу `Enter` или ввести yes:

```
Do you want to search for missing reverse zones? [yes]:
```

Если в результате поиска будут обнаружены отсутствующие обратные зоны, сценарий установки спросит, нужно ли создать обратные зоны для соответствующих обратных записей DNS. Для подтверждения нужно нажать клавишу `Enter`:

```
    Do you want to create reverse zone for IP 10.0.0.2 [yes]:
    Please specify the reverse zone name [0.0.10.in-addr.arpa.]:
    Using reverse zone(s) 0.0.10.in-addr.arpa.
```

Для подтверждения всех сделанных настроек конфигурации СИПА следует ввести yes:

```
    Continue to configure the system with these values? [no]:
yes
```

Сценарий приступит к установке СИПА в соответствии с заданной конфигурацией.

После завершения установки СИПА на экране появится соответствующее сообщение, а также сценарий установки порекомендует сделать резервную копию сертификата корневого центра сертификации CA и убедиться в том, что требуемые сетевые порты сервера СИПА открыты для входящих соединений.

Для открытия необходимых портов сервера СИПА (в зоне default службы межсетевого экрана firewalld) выполняют следующую консольную команду:

```
    # firewall-cmd --permanent --add-
port={80/tcp,443/tcp,389/tcp,
636/tcp,88/tcp,88/udp,464/tcp,464/udp,53/tcp,53/udp,123/udp}
```

Для применения изменений необходимо перезагрузить конфигурацию межсетевого экрана, выполнив следующую консольную команду:

```
    # firewall-cmd --reload
```

После установки СИПА и настройки межсетевого экрана станет доступным вход в веб-интерфейс управления СИПА.

3.1.3 Доступ к веб-интерфейсу СИПА

Для доступа к веб-интерфейсу управления СИПА нужно ввести в адресной строке браузера (на внешней рабочей станции) доменное имя сервера СИПА, например:

```
    https://ipa.rosa.int
```

На экране появится страница авторизации веб-интерфейса (рисунок 3).

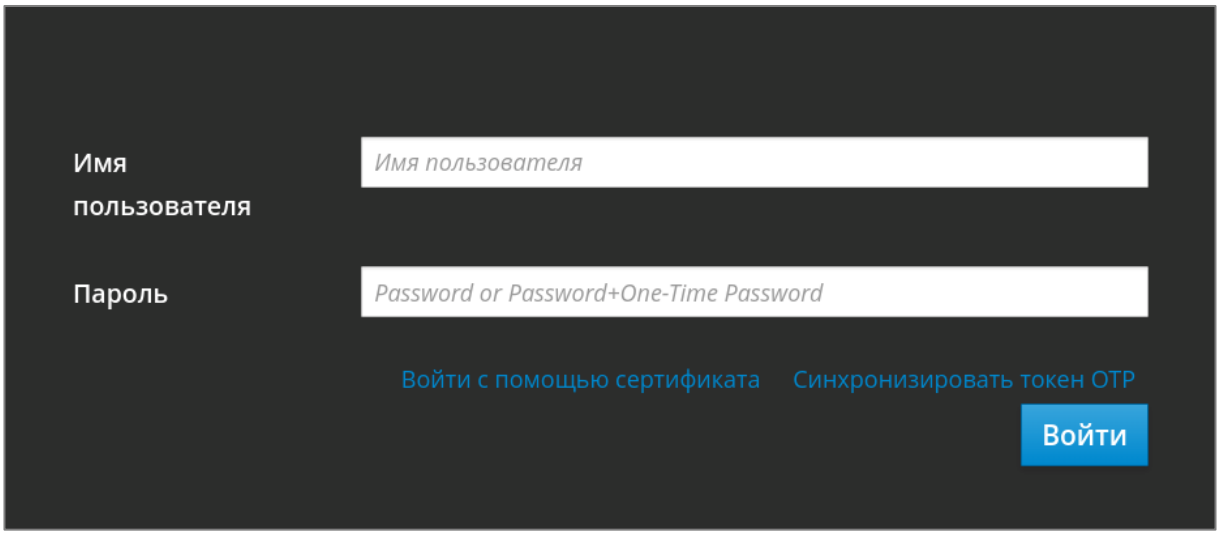

Рисунок 3 – Страница авторизации СИПА

Для входа в интерфейс требуется ввести имя и пароль пользователя в соответствующие поля, после чего нажать кнопку Войти.

Примечание – Первичный вход в веб-интерфейс управления СИПА осуществляется от имени учетной записи администратора admin.

3.2 Установка РОСА Центр Управления

Установка РОСА Центр Управления предполагает развертывание "с нуля" (см. п.3.2.1) или обновление с предыдущих версий (см. п.3.2.2).

3.2.1 Установка Комплекса

Процесс первоначальной установки РОСА Центр Управления состоит из последовательного выполнения следующих процедур:

– установка ОС на физический сервер или ВМ;

– выполнение интерактивного сценария установки controlcenter-install.sh.

3.2.1.1 Установка ОС на сервер

Для запуска программы установки ОС необходимо загрузить физический сервер или ВМ с носителя с дистрибутивом РОСА Центр Управления из комплекта поставки Комплекса.

На экране последовательно появятся меню программы установки, интерфейс для выбора языка сопровождения установки и меню "Обзор

установки", предназначенное для обзора и последующей настройки параметров установки (рисунок 4).

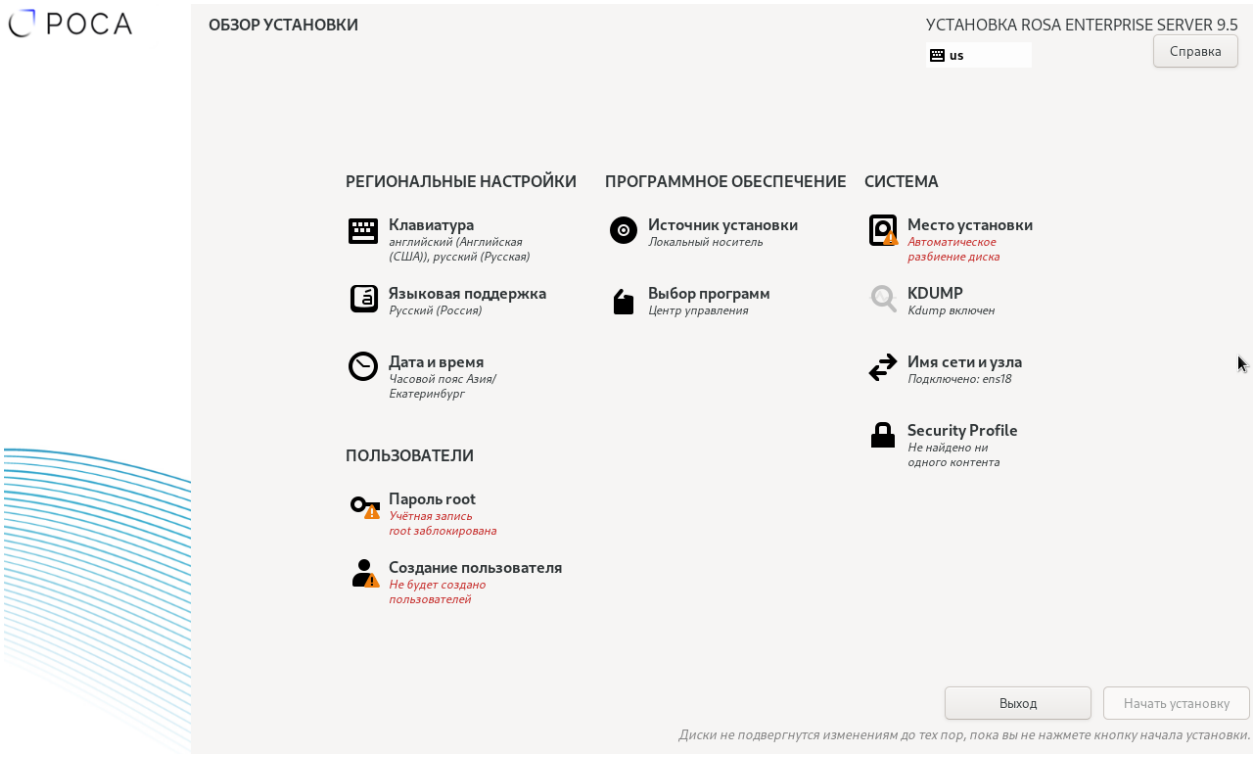

Рисунок 4 – Обзор установки

Панель "Обзор установки" содержит тематические секции, в которые сгруппированы соответствующие параметры установки. Следует обратить внимание, что вместо последовательного определения параметров программа установки дает возможность настроить параметры в произвольном порядке с помощью выбора необходимых секций в меню "Обзор установки".

Под наименованием каждой секции приводится информация о текущих параметрах, настроенных автоматически программой установки.

Необходимо убедиться, что в секции "Место установки" автоматически настроен параметр "Локальный носитель", а в секции "Выбор программ" для управления репозиториями и содержимым выбрать вариант "Центр управления (с поддержкой управления содержимым)" (рисунок 5).

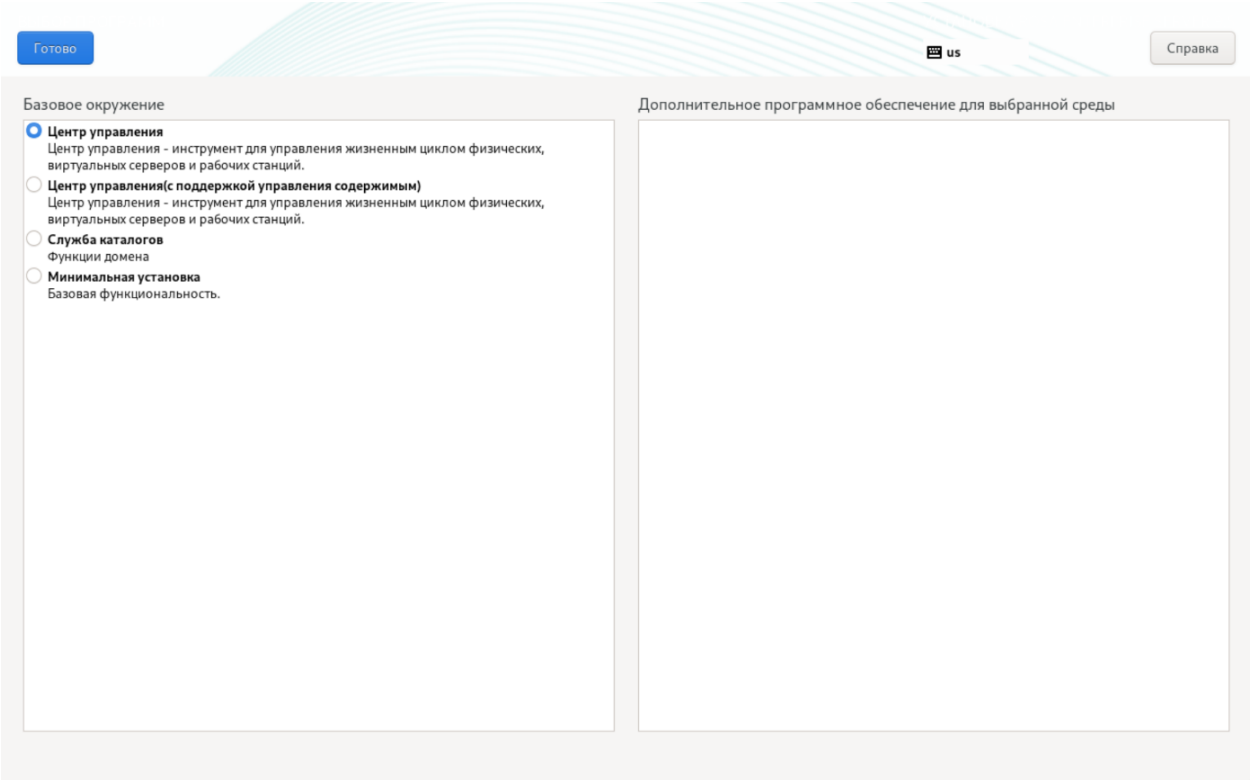

Рисунок 5 – Выбор варианта установки

Для перехода к интерфейсу настройки соответствующих параметров нужно нажать на наименование секции, после настройки параметров – кнопку Готово для возвращения в меню "Обзор установки".

В секции "Место установки" требуется выбрать необходимый диск и установить переключатель "Конфигурация устройств хранения данных" в положение "Автоматически".

В секции "Имя сети и узла" задают полное имя сервера РОСА Центр Управления в домене СИПА, что позволит автоматически зарегистрировать узел в домене (например, cc.rosa.int, где cc – краткое имя узла, а rosa.int – домен, в котором СИПА является контроллером).

Далее подключают необходимый сетевой интерфейс сервера РОСА Центр Управления и настраивают параметры сетевого соединения – IP-адрес (например, 10.0.0.3), маску сети (например, 255.255.0.0), шлюз по умолчанию (например, 10.0.0.1), сервер DNS (например, 10.0.0.2) (рисунок 6). Соединение по протоколу IPv6 рекомендуется отключить.

Примечание – Если Комплекс используется в инфраструктуре с Dynamic Directory или СИПА указывается DNS-сервер службы каталогов.

Следует обратить внимание, что IP-адрес сетевого интерфейса сервера РОСА Центр Управления требуется задавать только статическим.

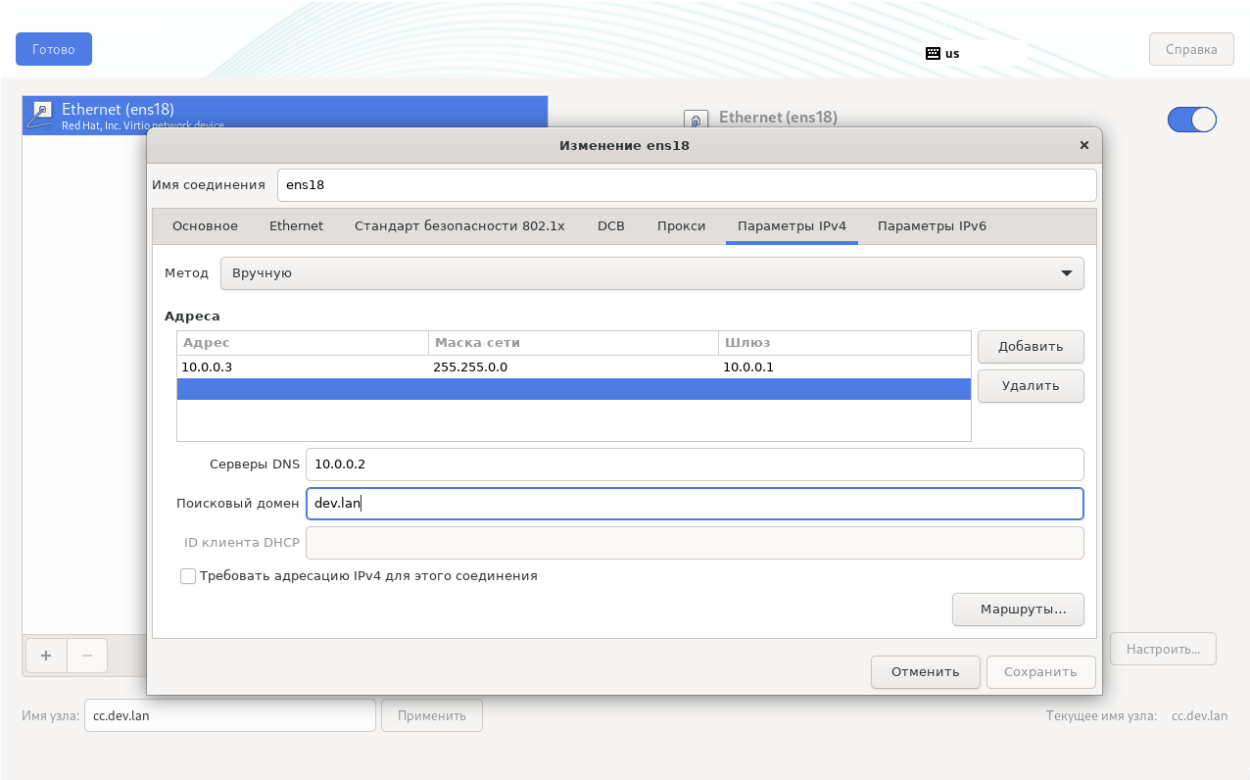

Рисунок 6 – Настройка сетевого соединения

В секции "Пароль root" необходимо установить пароль для учетной записи суперпользователя root. При необходимости можно создать локального пользователя с правами локального администратора, входящего в группу пользователей wheel.

После настройки всех обязательных параметров нужно нажать кнопку `Начать установку` для запуска процесса установки РОСА Центр Управления.

После завершения процесса установки требуется нажать кнопку `Перезагрузка системы`.

После перезагрузки системы на экране появится строка приглашения командного интерпретатора для входа в ОС сервера РОСА Центр Управления.

3.2.1.2 Выполнение сценария установки

Установка РОСА Центр Управления осуществляется с помощью скрипта controlcenter-install.sh.

Для запуска интерактивного сценария установки требуется выполнить следующую команду в терминале ОС сервера РОСА Центр Управления от имени учетной записи суперпользователя root:

```
# controlcenter-install.sh
```

На экране появится текстовый интерфейс сценария установки. Для сопровождения процесса необходимо следовать инструкциям этого интерфейса, выбрав вариант установки (рисунок 7). Варианты установки описаны в пп.3.2.1.2.1-3.2.1.2.2.

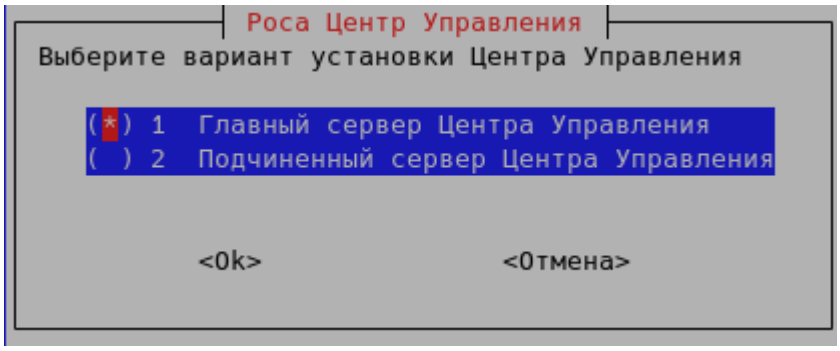

Рисунок 7 – Выбор варианта установки

3.2.1.2.1. Установка главного сервера

После выбора варианта установки главного сервера выполняют следующие шаги:

а) Выбрать вариант подключения к службе каталогов (рисунок 8):

– Без подключения к службе каталогов;
– Служба каталогов Dynamic Directory;
– Служба каталогов СИПА.

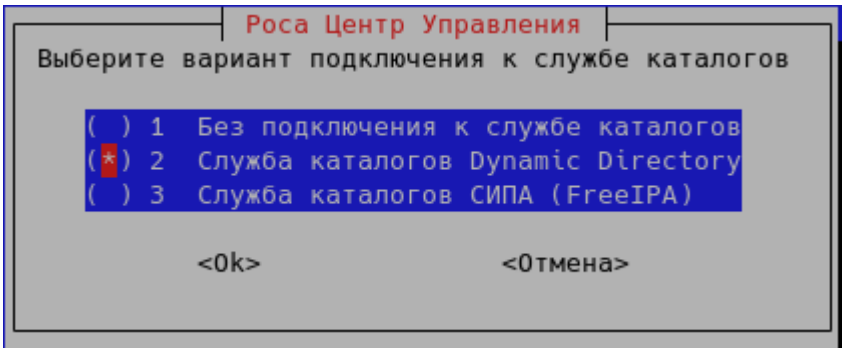

Рисунок 8 – Выбор варианта подключения к службе каталогов

Для варианта установки без подключения к службе каталогов необходимо следовать следующим условиям:

– В конфигурации сети указать действующий DNS-сервер, на котором в прямой и обратной зонах должны быть записи для Комплекса.

– В случае отсутствия DNS-сервера сделать запись в файле /etc/hosts для Комплекса.

б) Указать учётные данные пользователя с правом добавления узлов в домен службы каталогов, создания служб, добавления правил ролевой модели (пользователь Комплекса по умолчанию – admin) (рисунок 9).

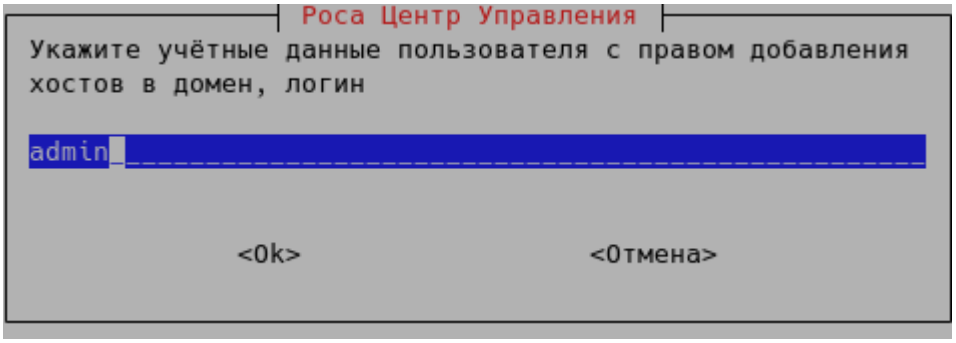

Рисунок 9 – Ввод учетных данных пользователя

в) задать пароль пользователя с правом добавления узлов в домен (рисунок 10).

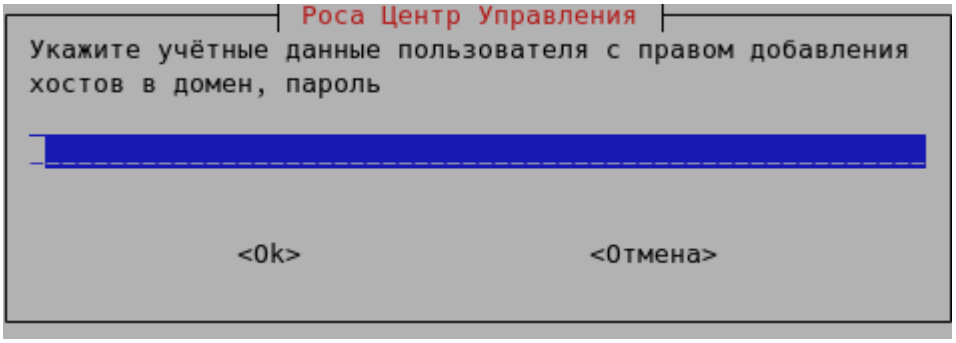

Рисунок 10 – Ввод пароля пользователя

г) Выбрать вариант использования SSO (рисунок 11).

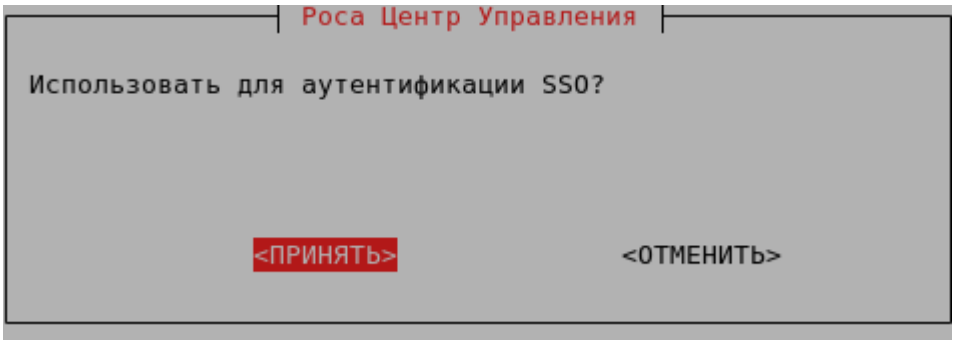

Рисунок 11 – Выбор использования SSO

д) Указать имя принципала для управления записями DNS (по умолчанию – имя узла) (рисунок 12).

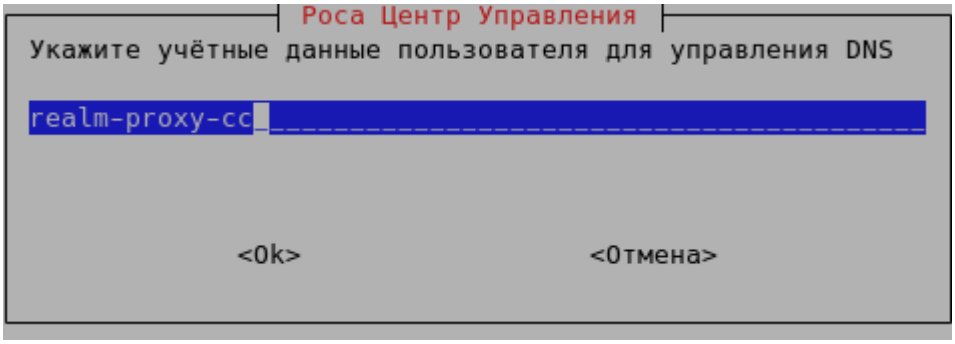

Рисунок 12 – Ввод имени принципала

е) Выбрать вариант конфигурирования DHCP (рисунок 13).

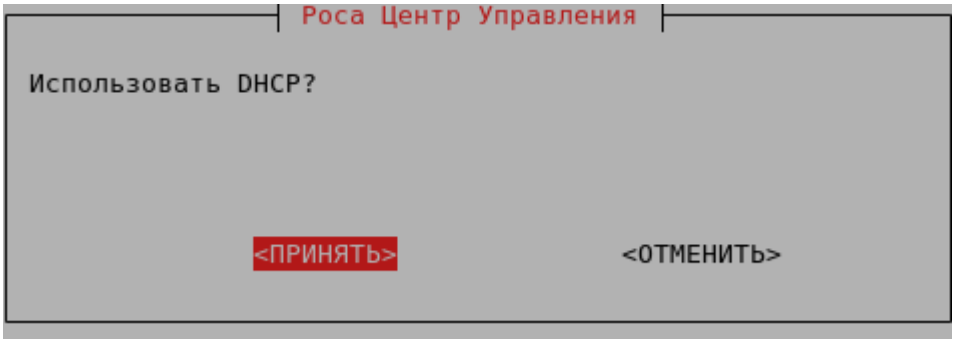

Рисунок 13 – Выбор конфигурирования DHCP

ж) Указать на каком интерфейсе будет использоваться DHCP (рисунок 14);

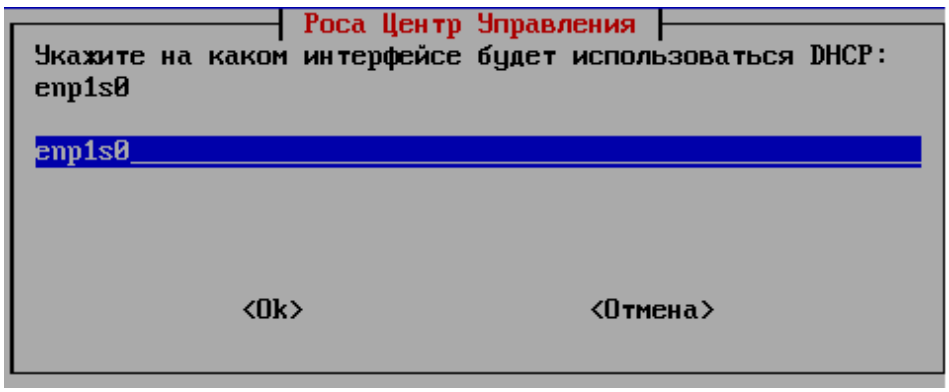

Рисунок 14 – Указание интерфейса

з) Указать адрес маршрутизатора (рисунок 15).

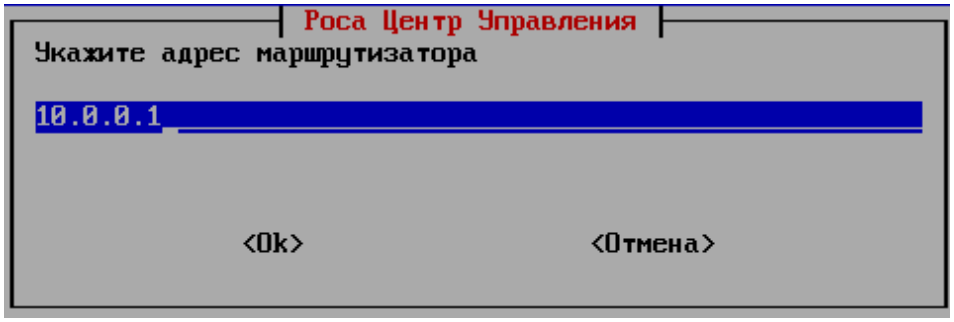

Рисунок 15 – Указание адреса маршрутизатора

Рекомендуется явно указать IP-адрес маршрутизатора в локальной подсети, который будет передаваться управляемым узлам по DHCP. В случае если этот IP-адрес не будет указан, сценарием установки используется маршрутизатор по умолчанию сервера РОСА Центр Управления.

Примечание – Впоследствии IP-адрес маршрутизатора можно указать (или изменить) как значение в поле "Маршрут по умолчанию", доступном в меню "Инфраструктура → Подсети" панели навигации веб-интерфейса РОСА Центр Управления.

и) Выбрать настройку диапазона DHCP, необходимого для сетевой установки ОС (рисунок 16).

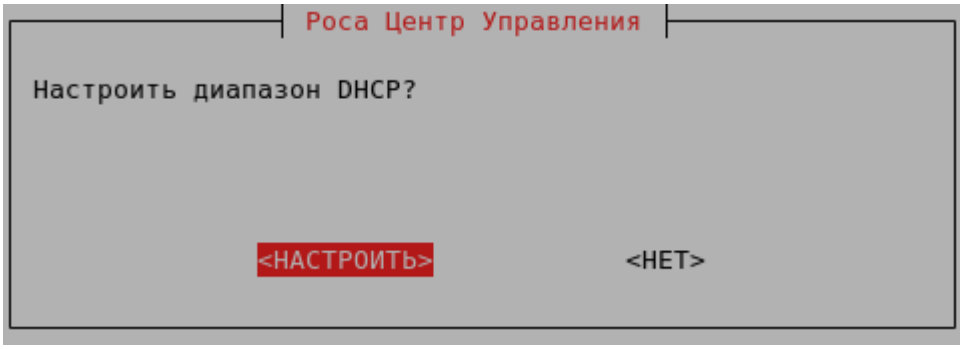

Рисунок 16 – Выбор настройки диапазона DHCP

к) Указать начало диапазона [10.0.0.5] (рисунок 17).

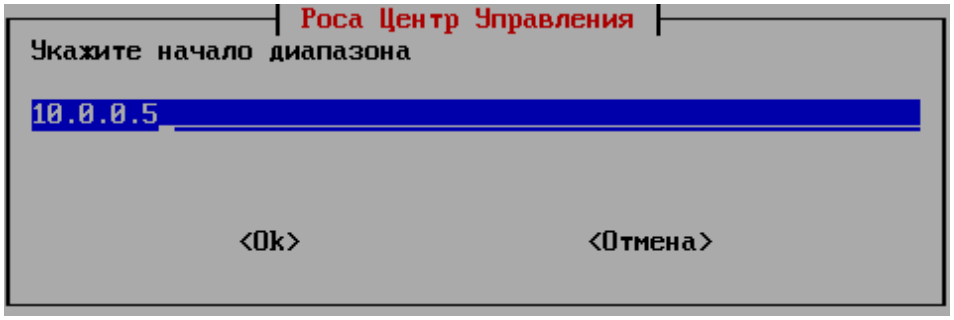

Рисунок 17 – Начало диапазона

л) Указать конец диапазона [10.0.0.64] (рисунок 18);

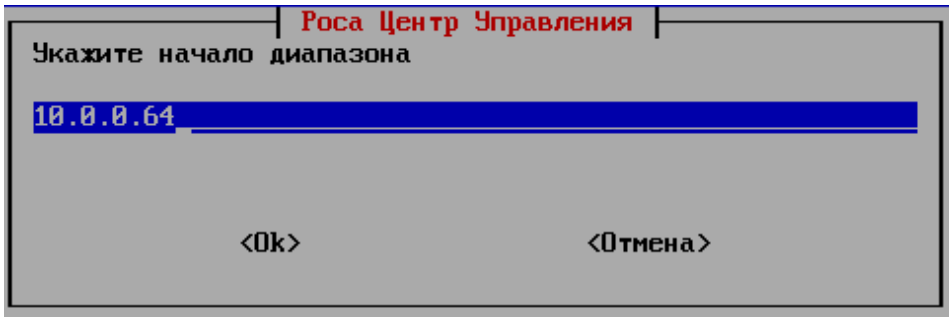

Рисунок 18 – Конец диапазона

Примечание – Диапазон IP-адресов DHCP, находящихся вне контроля РОСА Центр Управления, может быть полезен в том случае, если в локальной подсети предполагается использовать сетевые принтеры и/или другое оборудование, функционирующее не под управлением Комплекса. Для настройки нужно указать начальный и конечный IP-адреса диапазона DHCP таким образом, чтобы два этих диапазона (под управлением Комплекса и вне контроля РОСА Центр Управления) не пересекались между собой.

м) Указать пароль администратора Комплекса (рисунок 19).

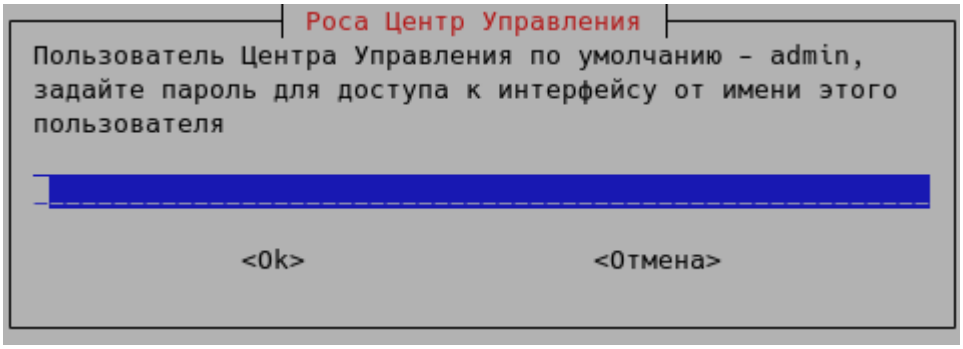

Рисунок 19 – Ввод пароля администратора

н) Запустить установку РОСА Центр Управления, нажав кнопку <Ок> (рисунок 20).

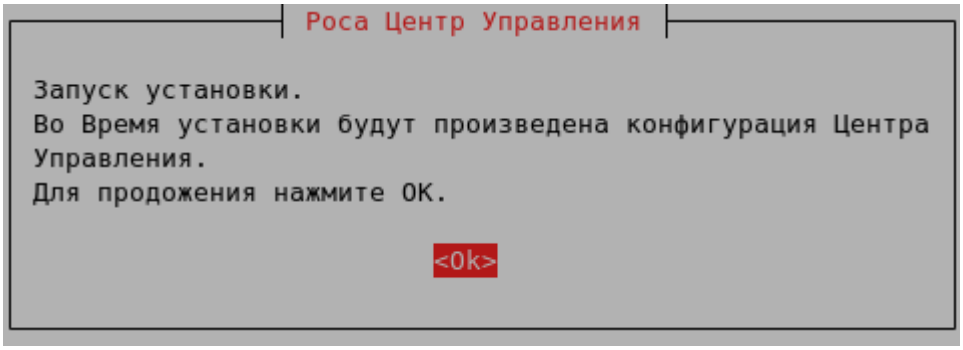

Рисунок 20 – Запуск установки

Сценарий приступит к установке РОСА Центр Управления в соответствии с заданной конфигурацией.

В результате выполненных действий по установке развернутый РОСА Центр Управления будет содержать следующие структурные элементы:

– подсеть;

– домен;

– настроенные и подготовленные к сетевой установке шаблоны ОС на управляемых узлах, такие как ROSA Chrome, Astra Linux; РЕД ОС, ALT Linux;

– примеры групп узлов;

– сервер Puppet;

– Ansible;

– плагин Katello (при установке с управлением содержимым);

– плагины управления вычислительными ресурсами систем виртуализации ROSA Virtualization, VMWare и Libvirt.

3.2.1.2.2. Установка подчиненного сервера

После выбора варианта установки подчиненного сервера выполняют следующие шаги:

а) Указать главный сервер (рисунок 21).

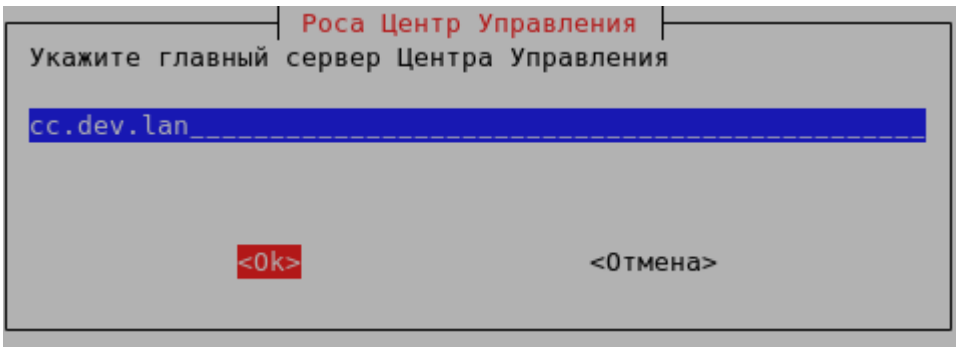

Рисунок 21 – Ввод данных главного сервера

б) Указать ключ клиента OAuth (рисунок 22).

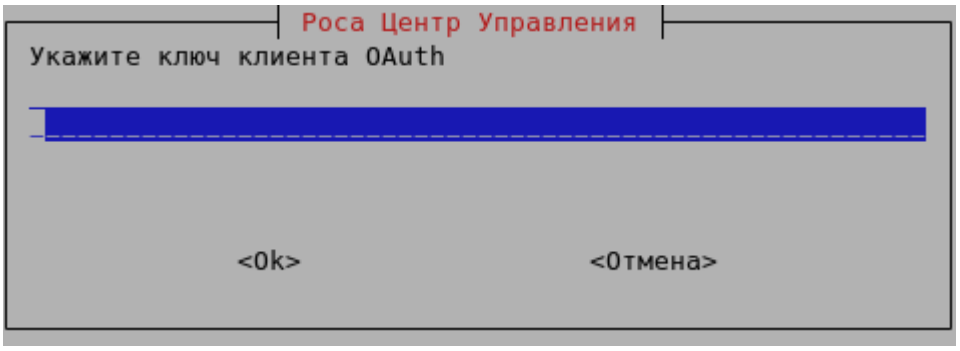

Рисунок 22 – Ввод ключа клиента OAuth

Для получения ключа клиента OAuth на главном сервере необходимо выполнить команду от имени пользователя root:

```
# cat /etc/foreman/settings.yaml | grep oauth_consumer_key | awk '{print $2}'
```

в) Указать секретный ключ клиента OAuth (рисунок 23)

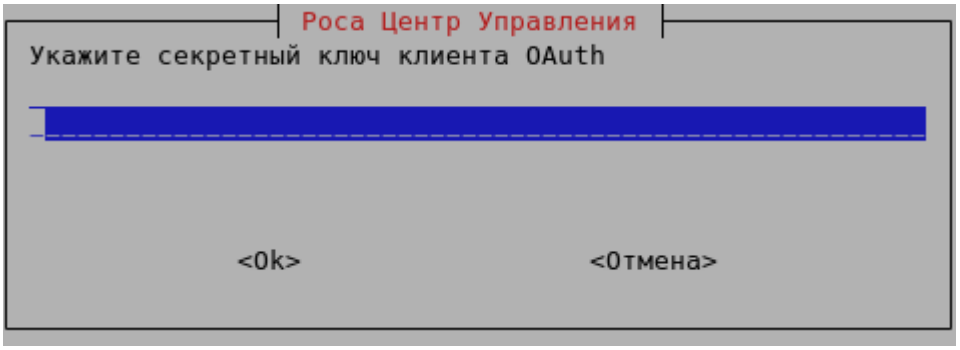

Рисунок 23 – Ввод секретного ключа

Для получения секретного ключа клиента OAuth на главном сервере необходимо выполнить команду от имени пользователя root:

```
# cat /etc/foreman/settings.yaml | grep oauth_consumer_secret | awk '{print $2}'
```

г) Выбрать вариант среды, в которой будет происходить установка (рисунок 24).

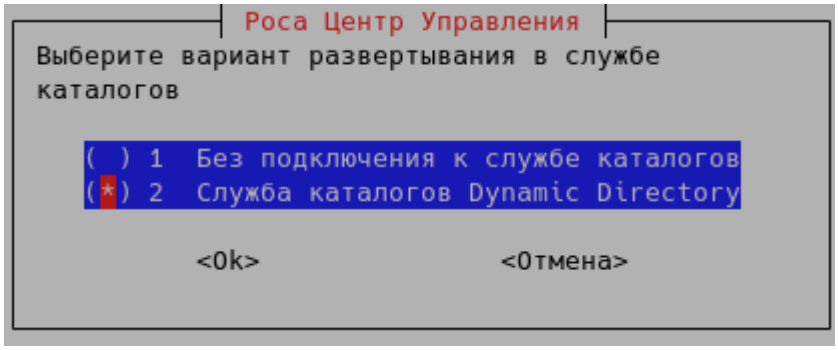

Рисунок 24 – Выбор варианта развертывания

д) Выбрать вариант использования DHCP для сетевой установки ОС (рисунок 25).

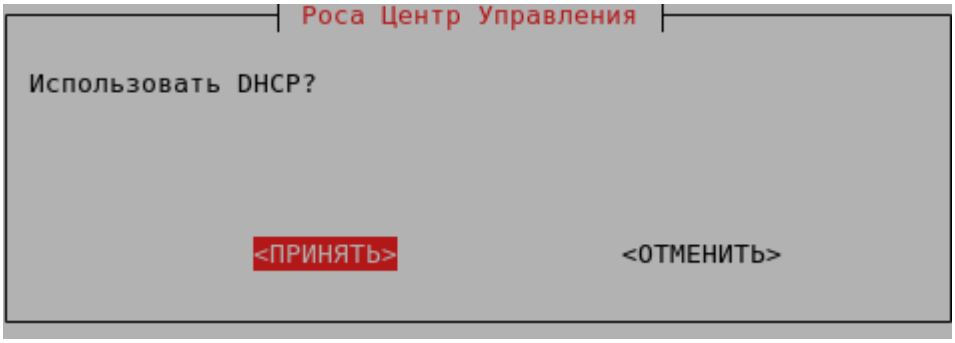

Рисунок 25 – Выбор использования DHCP

е) Указать на каком интерфейсе будет использоваться DHCP (рисунок 26).

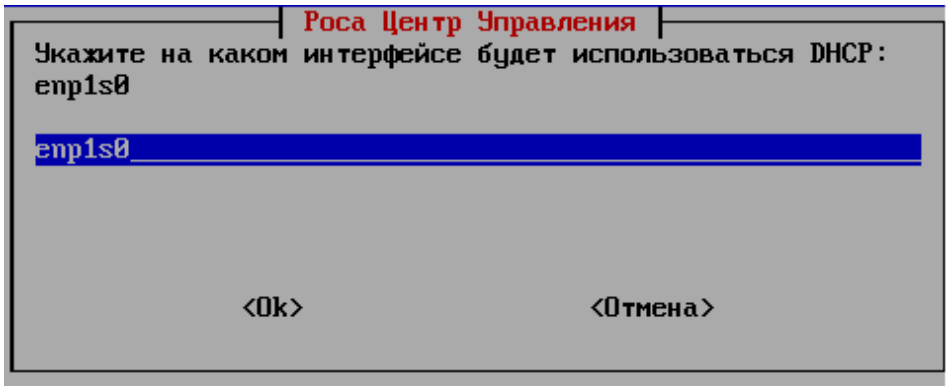

Рисунок 26 – Указание интерфейса

ж) Указать адрес маршрутизатора (рисунок 27).

а

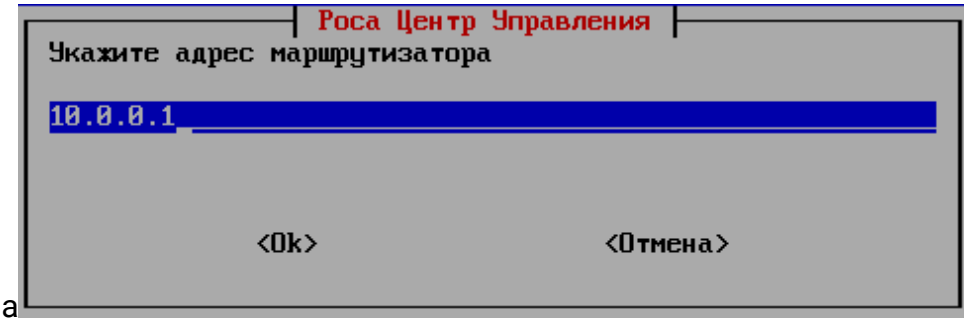

Рисунок 27 – Указание адреса маршрутизатора

Рекомендуется явно указать IP-адрес маршрутизатора в локальной подсети, который будет передаваться управляемым узлам по DHCP. В случае если этот IP-адрес не будет указан, сценарием установки используется маршрутизатор по умолчанию сервера РОСА Центр Управления.

Примечание – Впоследствии IP-адрес маршрутизатора можно указать (или изменить) как значение в поле "Маршрут по умолчанию", доступном в меню "Инфраструктура → Подсети" панели навигации веб-интерфейса РОСА Центр Управления.

з) Выбрать необходимость настройки диапазона DHCP (рисунок 28).

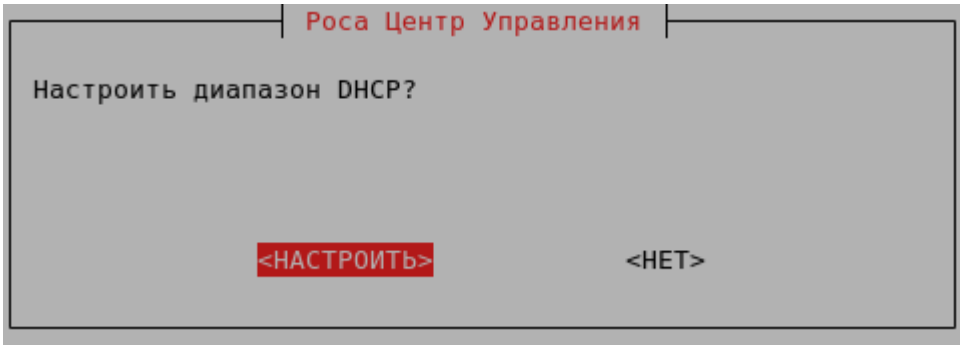

Рисунок 28 – Выбор настройки диапазона DHCP

и) Указать начало диапазона [10.0.0.5] (рисунок 29).

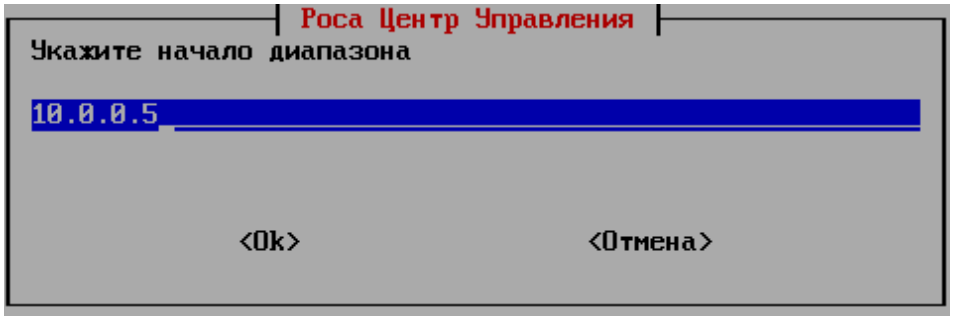

Рисунок 29 – Начало диапазона

к) Указать конец диапазона [10.0.0.64] (рисунок 30);

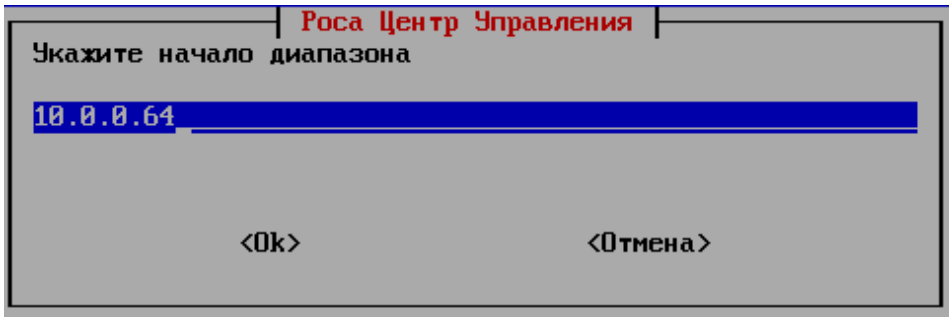

Рисунок 30 – Конец диапазона

Примечание – Диапазон IP-адресов DHCP, находящихся вне контроля РОСА Центр Управления, может быть полезен в том случае, если в локальной подсети предполагается использовать сетевые принтеры и/или другое оборудование, функционирующее не под управлением Комплекса. Для настройки нужно указать начальный и конечный IP-адреса диапазона DHCP таким образом, чтобы два этих диапазона (под управлением Комплекса и вне контроля РОСА Центр Управления) не пересекались между собой.

л) Задать пароль администратора Комплекса (рисунок 31).

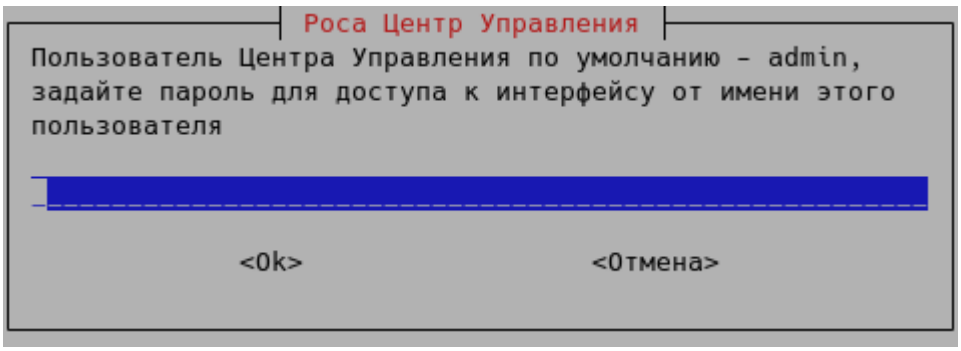

Рисунок 31 – Ввод пароля администратора

м) Запустить установку РОСА Центр Управления, нажав кнопку <Ок> (рисунок 32).

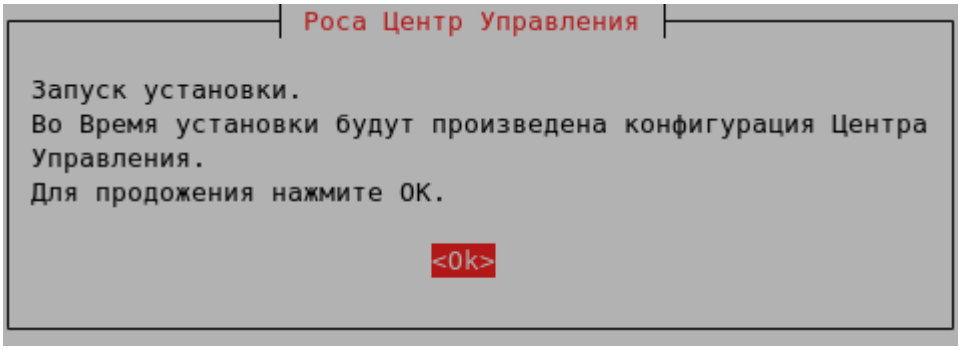

Рисунок 32 – Запуск установки

3.2.2 Обновление с предыдущих версий

3.2.2.1 Обновление до версии 2.2.0

В случае установленной ранее версии 2.0.0 или 2.1.0 для перехода на новую версию 2.2.0 Комплекса требуется выполнить следующие команды:

а) установить пакет, который добавит новые репозитории:

```
# dnf install -y https://ddynamic.ru/repo/res9/base/rosa-release-9.4-3.res9.noarch.rpm
```

б) переустановить пакет syslinux:

```
# dnf reinstall syslinux
```

в) обновить системные пакеты (во время обновления сервисы Комплекса будут недоступны):

```
# dnf -y update
```

г) установить новый пакет rosa-control-center:

```
# dnf -y install rosa-control-center
```

д) обновить Комплекс, ответить на вопросы; в процессе появится поддержка аутентификации с использованием SSO (сценарий установки описан в п.3.2.1.2):

```
# controlcenter-update.sh
```

После обновления в интерфейсе Комплекса нужно выполнить импорт классов Puppet ENC.

3.2.2.2 Обновление до версии 2.3.0

Для обновления с версии 2.2.0 до версии 2.3.0 необходимо выполнить следующие действия:

а) установить пакет с добавленными репозиториями:

```
# dnf install https://ddynamic.ru/repo/res9/base/rosa-release-rcc-2.3-9.5-1.res9.noarch.rpm
```

б) обновить кеш менеджера пакетов:

```
# dnf makecache
```

в) обновить системные пакеты (во время обновления сервисы Комплекса будут недоступны):

```
# dnf -y update
```

г) выполнить обновление базы данных Комплекса:

```
# foreman-rake db:migrate
```

д) перезапустить службы Комплекса:

```
# foreman-maintain service restart
```

3.2.2.3 Обновление до версии 2.4.0

Для обновления с версии 2.3.0 до версии 2.4.0 необходимо выполнить следующие команды:

а) установить пакет с добавленными репозиториями:

```
# dnf install https://ddynamic.ru/repo/res9/base/rosa-release-rcc-2.4-9.5-1.res9.noarch.rpm
```

б) обновить кеш менеджера пакетов:

```
# dnf makecache
```

в) обновить системные пакеты (во время обновления сервисы Комплекса будут недоступны):

```
# dnf -y update
```

г) выполнить обновление Комплекса:

```
# controlcenter-install.sh
```

После запуска скрипта обновления будет выведено диалоговое, что найден установленный экземпляр Комплекса (рисунок 33), с предложением о дальнейших действиях. Следует нажать кнопку `<ПРОДОЛЖИТЬ>`.

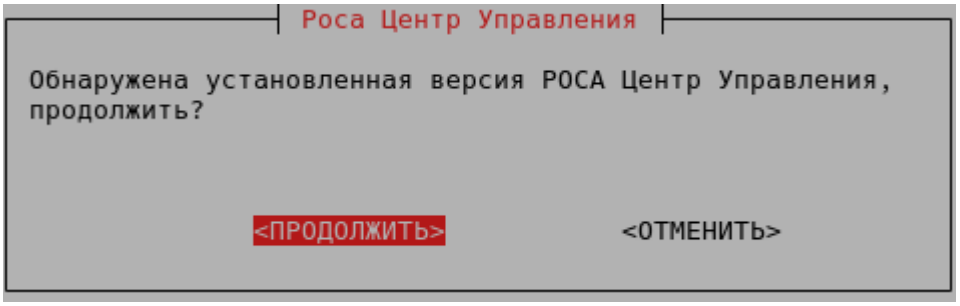

Рисунок 33 – Сообщение об обнаружении

Далее появится диалоговое окно с запросом об обновлении конфигурации РОСА Центр Управления (рисунок 34). В это окне нужно нажать кнопку `<ОТМЕНИТЬ>`.

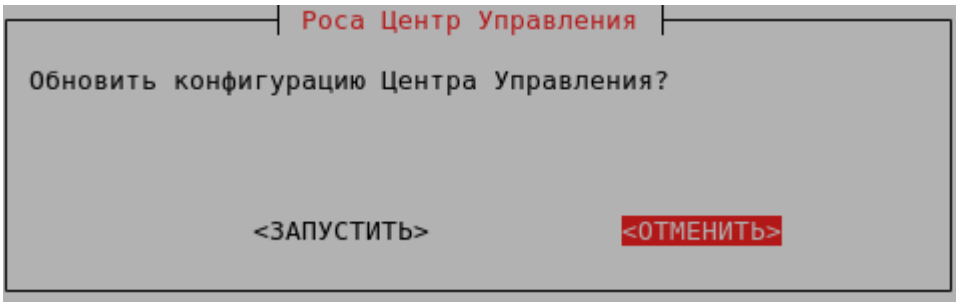

Рисунок 34 – Запрос на обновление

Примечание – Нажатие кнопки `<ЗАПУСТИТЬ>` предполагает, что найденный экземпляр установлен с ошибками, и нужна корректировка установленного Комплекса. Этот вариант следует использовать в исключительных случаях. Дальнейшие ответы на запросы в мастере обновления должны совпадать с начальной установкой Комплекса.

3.2.3 Доступ к веб-интерфейсу РОСА Центр Управления

Для доступа к веб-интерфейсу РОСА Центр Управления нужно ввести в адресной строке браузера (на внешней рабочей станции) доменное имя сервера РОСА Центр Управления, например:

```
https://cc.rosa.int
```

На экране появится страница авторизации веб-интерфейса (рисунок 35).

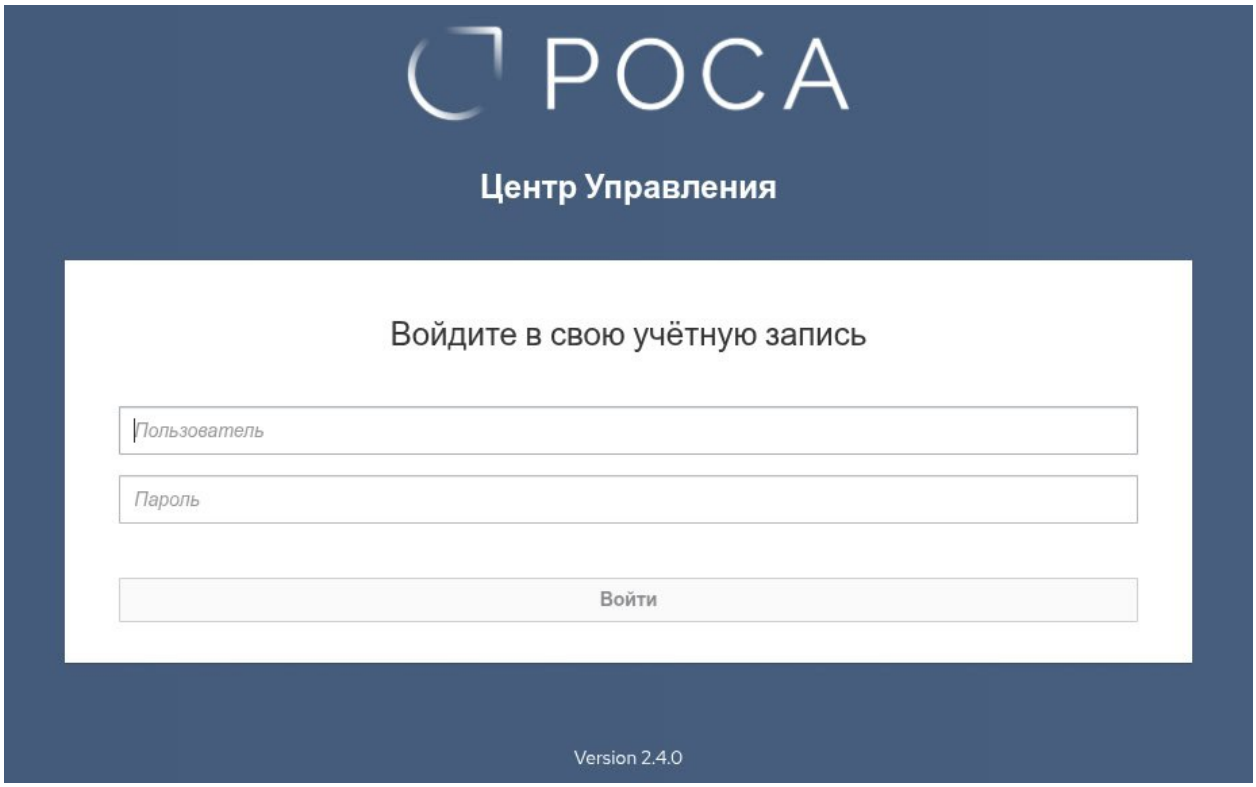

Рисунок 35 – Страница авторизации РОСА Центр Управления

Для входа в РОСА Центр Управления необходимо ввести имя и пароль пользователя, после чего нажать кнопку Вход.

Примечание – Первичный вход в веб-интерфейс РОСА Центр Управления осуществляется от имени учетной записи администратора admin.

В случае успешной авторизации на экране появится пользовательский интерфейс РОСА Центр Управления.

Интерфейс РОСА Центр Управления состоит из панели навигации с доступными пользователю вкладками, панели быстрого доступа с функциональными пиктограммами, а также рабочей области, в которой по умолчанию (при входе пользователя в систему) отображается интерфейс вкладки "Узлы" с перечнем узлов и краткой информацией об управляемых узлах (рисунок 36).

Схематичное расположение панелей интерфейса:

1 – Панель навигации

2 – Панель быстрого доступа

3 – Рабочая область

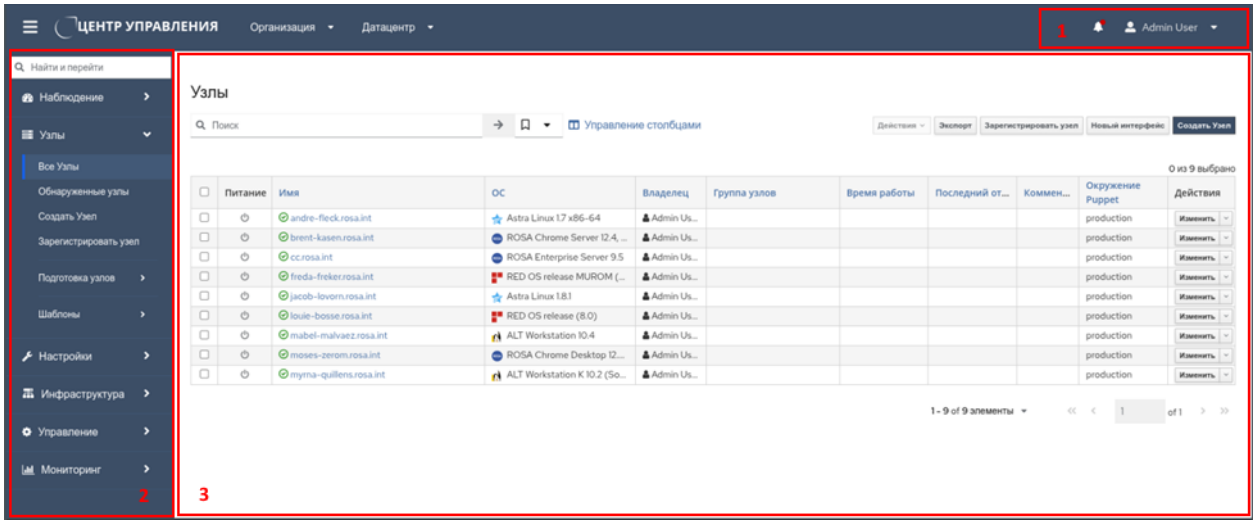

Рисунок 36 – Интерфейс РОСА Центр Управления

Для перемещения по страницам интерфейса РОСА Центр Управления используют необходимые вкладки и пункты меню панели навигации (рисунок 37).

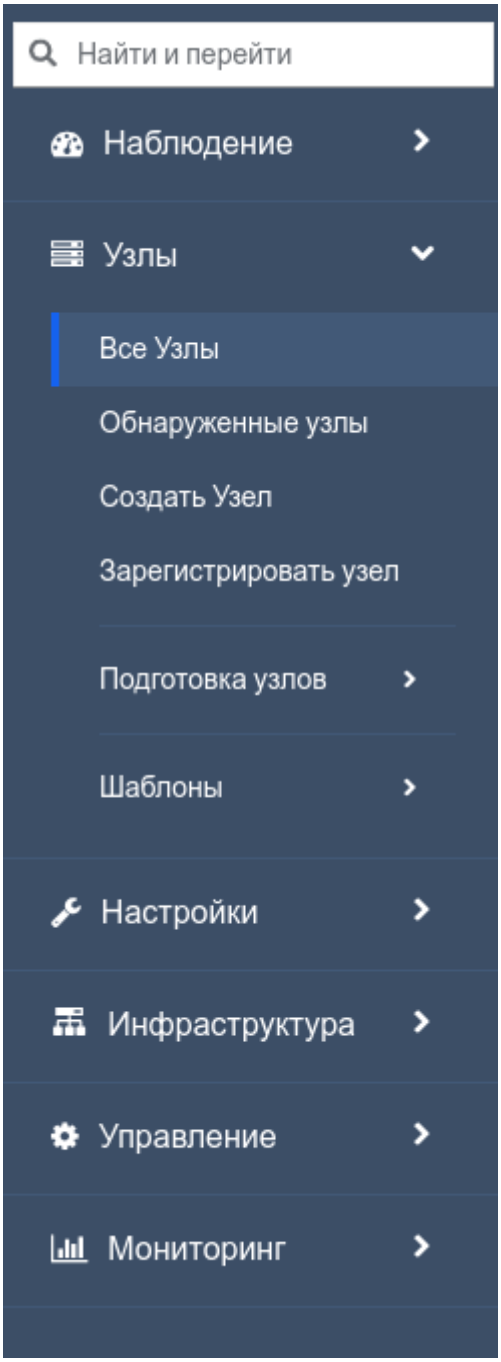

Рисунок 37 – Панель навигации

3.3 Установка и настройка подсистем

3.3.1 Установка подсистем мониторинга, отображения, поиска и аналитики

Сервер мониторинга и отображения должен устанавливаться на отдельный сервер с установленной ROSA Enterprise Linux Server 9.* в минимальной конфигурации. Для установки всех требуемых пакетов нужно использовать класс

rcc_zabbix_srv. Для этого следует сначала зарегистрировать сервер в Комплексе, установив пакет puppet-agent:

```
# dnf install puppet-agent
```

После этого необходимо изменить настройки puppet-agent, указав в качестве переменной server сервер Комплекса в файле /etc/puppetlabs/puppet/puppet.conf:

```
[agent]
ca_server = cc.rosa.int
server = cc.rosa.int
```

Затем нужно выполнить команду обновления:

```
puppet agent -t
```

После выполнения этой команды сервер мониторинга будет успешно зарегистрирован на сервере РОСА Центр управления.

Установка подсистем отображения, мониторинга, поиска и аналитики может быть произведена в автоматическом режиме на отдельный сервер с использованием модуля rcc_srv_monlog_install.

Примечание – По умолчанию для подсистемы мониторинга будет использоваться PostgreSQL 13-й версии. В случае необходимости можно использовать PostgreSQL 16-й версии, подключив соответствующий репозиторий на будущем сервере мониторинга, выполнив команду:

```
# dnf install -y rosa-release-postgres-16
```

Для корректной установки необходимо задать параметры классов, указанные в таблице 3. Описание работы с классами приведено в п.7.3 документа "Платформа централизованного управления жизненным циклом операционных систем "РОСА Центр Управления". Руководство системного администратора. Часть 2. Эксплуатация" (шифр РСЮК.10121-09 32 02).

Таблица 3 – Параметры класса

Имя класса	Имя параметра	Тип параметра	Значение
rcc_srv_monlog_install::grafana_configure			
	grafana_adm_pwd	строка	Пароль администратора подсистемы отображения
	grafana_rcc_viewer_pwd	строка	Пароль пользователя с правами на просмотр графиков

Имя класса	Имя параметра	Тип параметра	Значение
rcc_srv_monlog_install::opensearch_configure			
	opensearch_pwd	строка	Пароль администратора подсистемы поиска и аналитики
rcc_srv_monlog_install::zabbix_configure			
	zabbix_db_pwd	строка	Пароль администратора БД подсистемы мониторинга
	zabbix_rcc_pwd	строка	пароль пользователя подсистемы мониторинга

Данный модуль выполняет следующие операции:

– устанавливает необходимые пакеты;

– настраивает межсетевой экран;

– устанавливает плагины сопряжения подсистемы отображения;

– настраивает подсистему мониторинга в качестве источника данных для подсистемы отображения;

– настраивает подсистему поиска и аналитики в качестве источника данных для подсистемы отображения;

– обеспечивает настройку взаимодействия подсистем через SSL/HTTPS;

– создает учетные записи подсистем согласно заданным параметрам классов.

Результатом работы модуля является настроенный сервер с установленными подсистемами отображения, мониторинга, поиска и аналитики. Интерфейсы управления подсистемами доступны по следующим адресам:

– подсистема отображения – https://<fqdn_имя_сервера>:3000;

– подсистема мониторинга – https://<fqdn_имя_сервера>/zabbix;

– подсистема поиска и аналитики – https://<fqdn_имя_сервера>:5601.

3.3.2 Установка клиентской части подсистемы мониторинга

Для установки агента подсистемы мониторинга используется класс rcc_zabbix_agent:

а) в настройках класса rcc_zabbix_agent включить возможность переопределения параметров zabbix_server (строка), zabbix_server_active (строка) и is_it_dirsrv (логическое значение), установить значения по умолчанию:

– zabbix_server – адрес используемого сервера мониторинга;
– zabbix_server_active – адрес используемого сервера активных проверок (в большинстве случаев устанавливается то же значение, что и для zabbix_server);
– is_it_dirsrv – логическое значение; переопределяется в true только при установке на сервера службы каталогов Dynamic Directory;

б) назначить класс на отдельные APM или группу APM, при необходимости переопределить значения по умолчанию (например, в частном случае – задание is_it_dirsrv в true для установки на сервер каталогов Dynamic Directory);

в) при следующем запуске агента Комплекса для выбранных узлов будут сформированы задания на установку агентов подсистемы мониторинга и первоначальное конфигурирование.

3.3.3 Настройка плагина мониторинга

Конфигурация плагина мониторинга в Комплексе осуществляется из общих настроек, доступных по адресу https://cc.rosa.int/settings, на вкладке "Плагин Мониторинга" или через основное меню Комплекса "Управление → Параметры → Плагин Мониторинга".

Конфигурация плагина определяется следующими параметрами:

– "Ссылки на страницы в Grafana" – URL-ссылка на панели мониторинга сервера отображения. Для ее определения в интерфейсе сервера отображения в основном меню перейти в "Dashboards" и выбрать нужную панель мониторинга. Справа вверху нажать на кнопку `Share (Поделиться)`. На вкладке "Link" нажать `Copy` (рисунок 38).

Рисунок 38 – Получение ссылки

Вставить скопированную ссылку в поле редактирования значения в Комплексе и нажать кнопку Сохранить (рисунок 39);

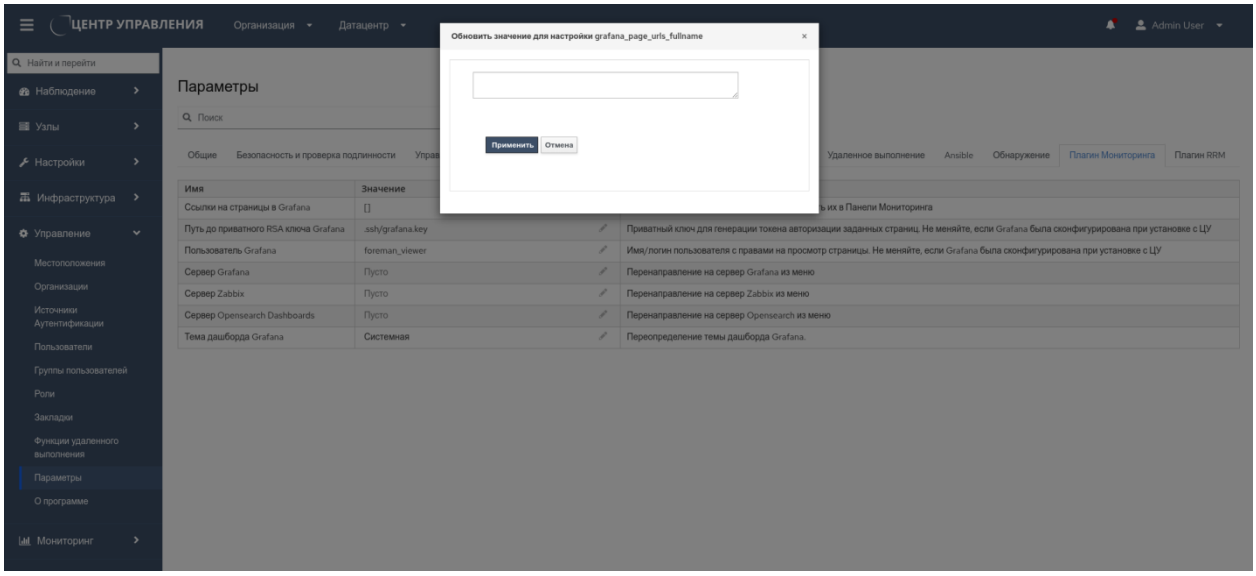

Рисунок 39 – Сохранение ссылки

– "Путь до приватного RSA ключа Grafana" – значение по умолчанию ".ssh/grafana.key". В случае если приватный ключ хранится в другом месте в Комплексе, то значение следует изменить. Следует убедиться, чтобы у процесса Комплекса был доступ к файлу приватного ключа;

– "Пользователь Grafana" – логин пользователя, под которым будет происходить авторизация с использованием JWT из Комплекса в подсистеме отображения. Значение по умолчанию – foreman_viewer. Если при создании УЗ для просмотра был создан пользователь с другим логином, следует отредактировать данное значение;

– "Сервер Grafana" – URL-ссылка на переход в сервер отображения из главного меню интерфейса Комплекса;

– "Сервер Zabbix" – URL-ссылка на переход в сервер мониторинга из главного меню интерфейса Комплекса;

– "Сервер OpenSearch Dashboards" – URL-ссылка на переход в сервер поиска и аналитики из главного меню интерфейса Комплекса.

Параметры сервера подсистемы отображения и сервера подсистемы мониторинга можно задать как в параметрах плагина, так и в соответствующих конфигурационных файлах:

– /opt/grafana_server.txt;

– /opt/zabbix_server.txt.

Значения заданные через параметры плагина мониторинга имеют более высокий приоритет, а значения заданные в конфигурационных файлах в этом случае будут игнорированы (рисунок 40).

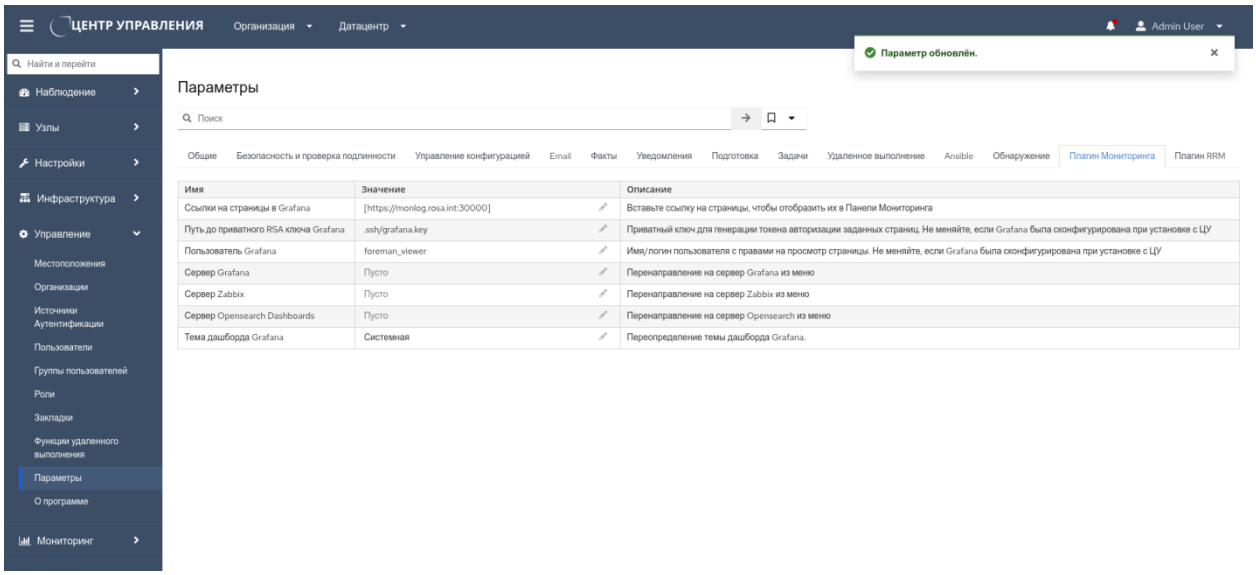

Рисунок 40 – Настройка плагина мониторинга

3.3.4 Импортирование файлов шаблонов мониторинга серверов Dynamic Directory

Для корректного отображения данных, передаваемых сервером службы каталогов необходимо произвести следующие операции в веб-интерфейсе подсистемы мониторинга:

а) в главном меню подсистемы в разделе "Сбор данных" выбрать пункт "Шаблоны" (рисунок 41);

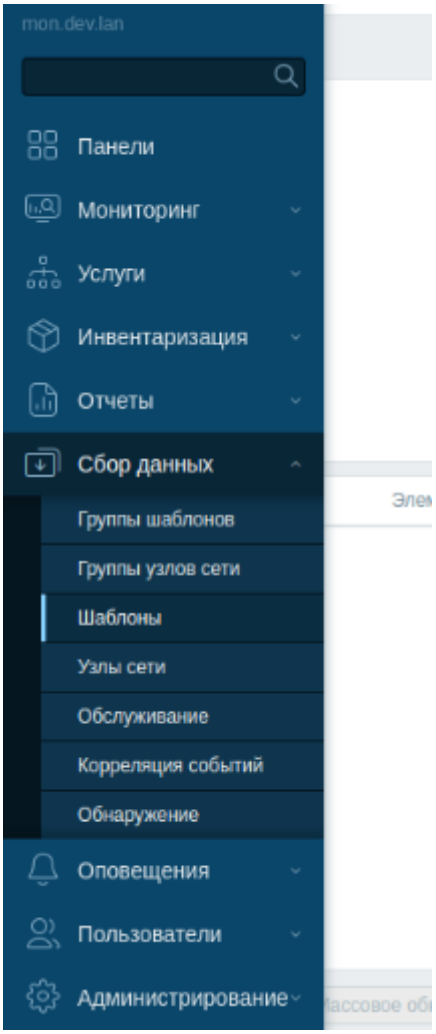

Рисунок 41 – Меню подсистемы мониторинга

б) с помощью кнопки Импорт в верхнем правом углу интерфейса выбрать в появившемся диалоговом окне файл шаблона 389ds_templates.xml и подтвердить действие кнопкой с одноименным названием (рисунок 42).

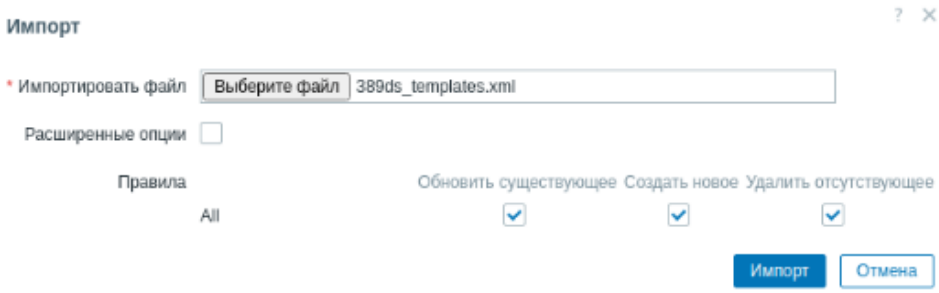

Рисунок 42 – Импорт шаблона

3.4 Интеграция с мобильными устройствами

Начиная с версии 2.2, РОСА Центр управления поддерживает интеграцию с мобильными устройствами (далее – МУ) на ОС "РОСА Мобайл". Функционал управления МУ предоставляется в формате отдельного образа установочного диска (дистрибутива).

Реализованные функции:

– автоматизированное подключение к серверу Комплекса;
– управление пакетной базой МУ (установка, обновление и удаление ПО);
– настройка интервала синхронизации МУ;
– управление блокировкой камеры МУ;
– управление ПИН-кодом, блокировка МУ;
– удаление пользовательских данных;
– сброс настроек МУ до заводских;
– управление работой GPS-приемника;
– управление работой GSM-модема;
– получение информации о местоположении МУ по данным системы глобального позиционирования;
– получение информации о ближайших Wi-Fi-сетях;
– получение информации об используемом GSM-соединении;
– получение информации о списке установленных пакетов и их версиях;
– получении информации о состоянии заряда аккумулятора МУ.

3.4.1 Автоматизированное подключение

Для корректной работы автоматизированной регистрации МУ необходимо в пункте меню "Управление → Параметры → Подготовка" установить параметр "Шаблон глобальной регистрации по умолчанию" в значение "r_mob_onboarding".

Регистрация МУ производится в пункте меню "Узлы → Зарегистрировать узел" (рисунок 43).

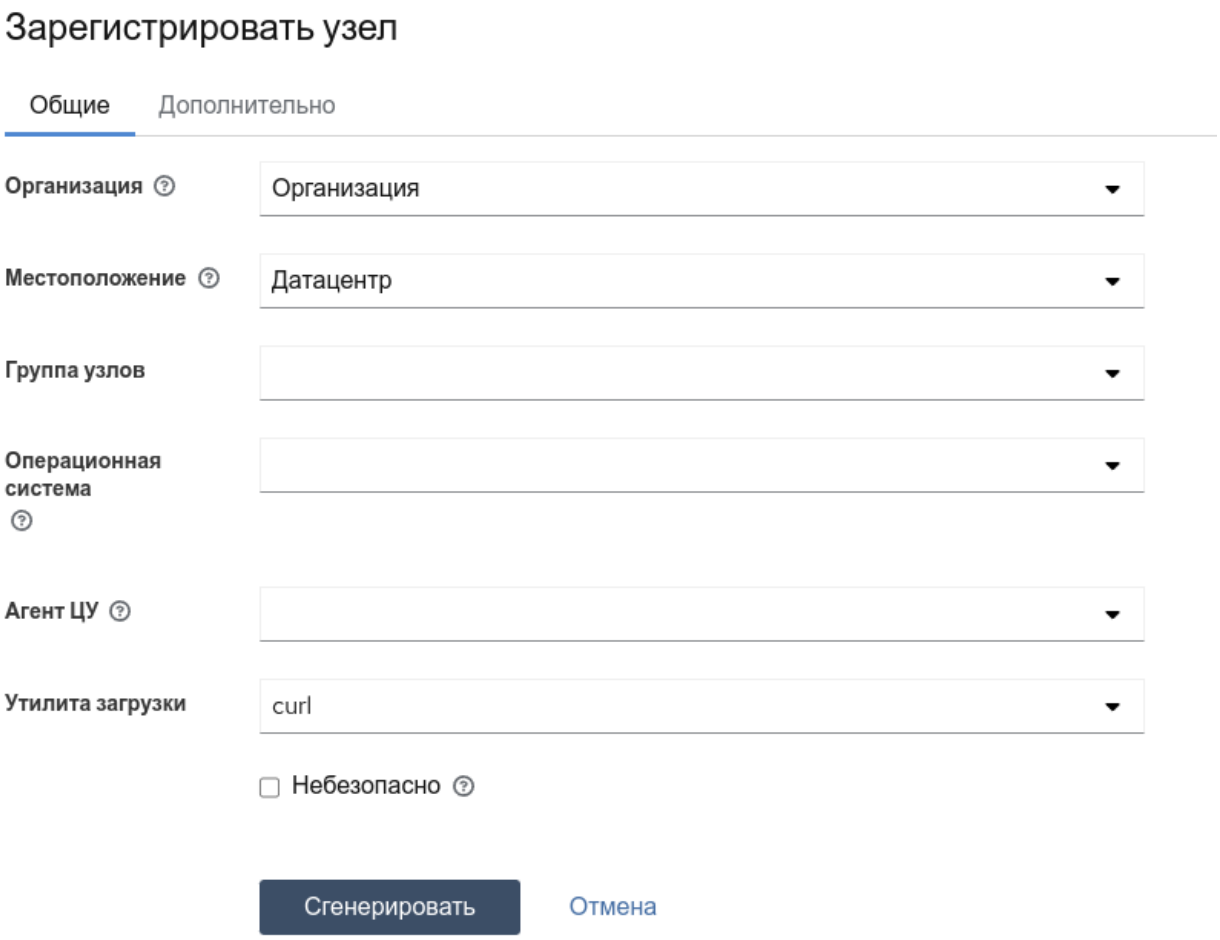

Рисунок 43 – Регистрация МУ

В форме необходимо заполнить сведения об организации и местоположении МУ, а так же группе узлов.

При нажатии на кнопку `Сгенерировать` содержание окна обновляется и появляется строка, содержащая команду подключения МУ к Комплексу, и QR-код (рисунок 44). При выполнении данной команды на конечном МУ (клиенте) от имени пользователя с административными правами или сканировании QR-кода приложением "РОСА Контроль", будет произведена автоматическая настройка клиента на работу с Комплексом.

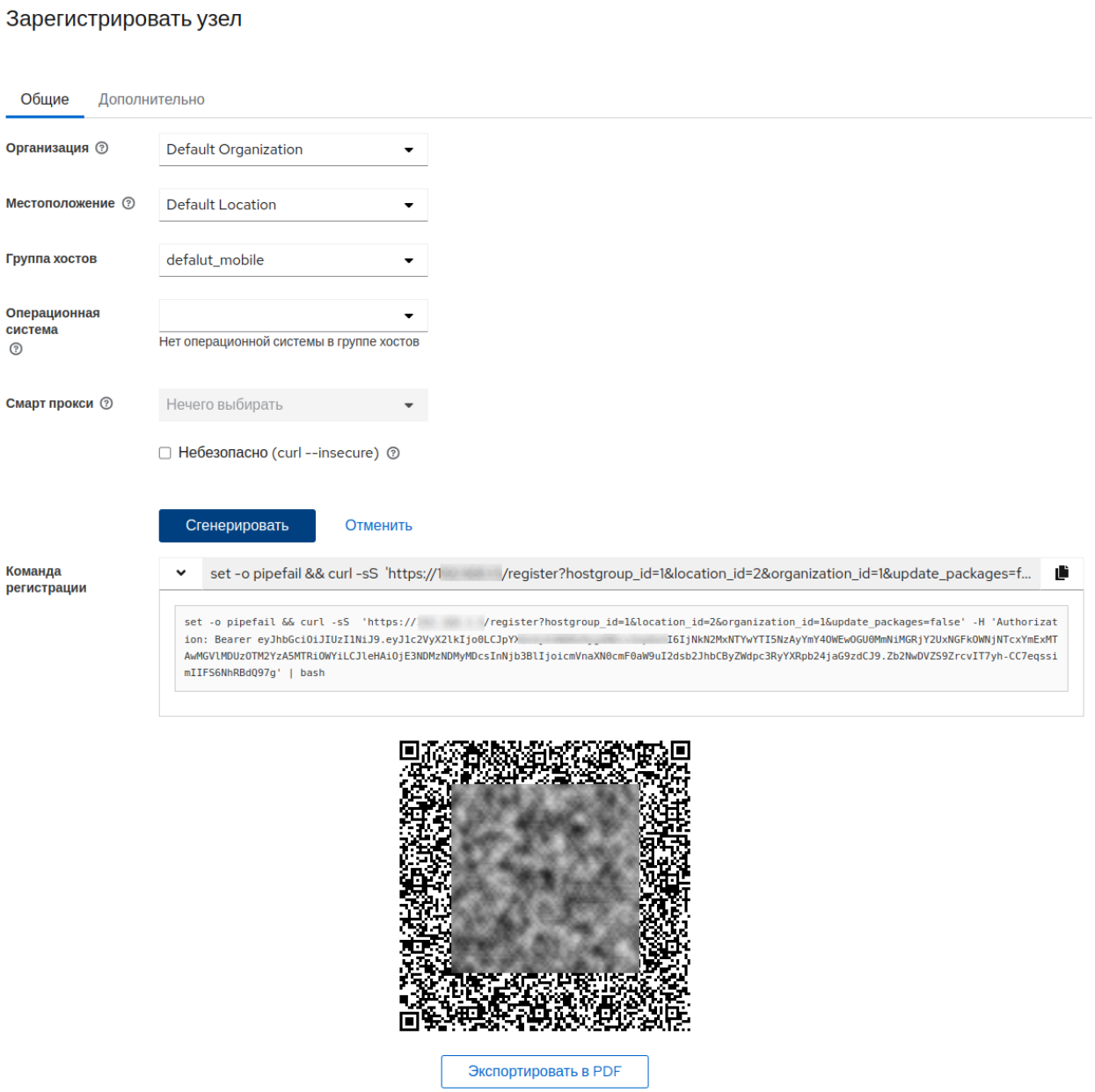

Рисунок 44 – Данные о регистрации и подключении

При необходимости можно экспортировать QR-код в PDF-документ нажатием кнопки `Экспортировать в PDF` под QR-кодом.

Настройки шаблона экспортируемого PDF-документа доступны по пункту меню "Управление → Параметры → QR Онбординг" (рисунок 45).

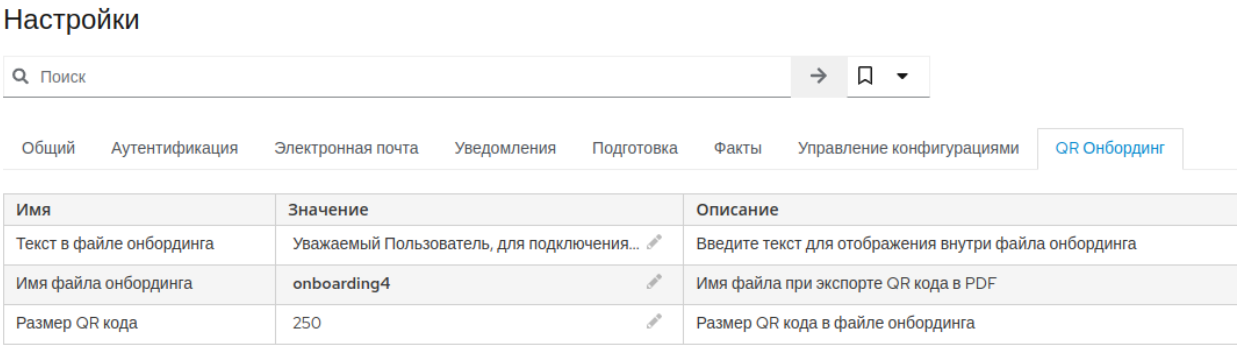

Рисунок 45 – Настройки шаблона PDF-документа

Изменение поля "Текст в файле онбординга" позволяет добавить произвольный текст в экспортируемый PDF-документ, например, как показано на рисунке 46.

Рисунок 46 – Пример текста при онбординге

3.4.2 Подписание сертификата

После успешного выполнения на МУ автоматизированного подключения и регистрации будет сформирован запрос на подписание сертификата Комплекса.

Подписание сертификата осуществляется в меню "Инфраструктура → Агенты ЦУ → <имя сервера сертификации> → Центр сертификации Puppet → Сертификаты".

В интерфейсе будет отображена таблица имен сертификатов, их состояния, сроки действия и отпечатки (fingerprint). Для выборки запросов на подписание сертификатов следует установить фильтр отображения состояния в верхней правой части интерфейса в "ожидание". После проведенных действий в интерфейсе отобразятся все устройства, сертификаты которых не подписаны. Подписание производится в меню "Действия", расположенном в правой части строки с именем устройства.

Следует отметить, что уникальным идентификатором устройства является его IMEI-код.

3.4.3 Функции управления

3.4.3.1 Управление пакетной базой

Модуль управления пакетной базой предназначен для централизованной установки, обновления или удаления пакета (или их перечня) на конечном МУ. Параметры класса приведены в таблице 4.

Таблица 4 – Параметры класса

Имя класса	Имя параметра	Тип параметра	Пример значения	Описание
r_mob_package_manager				
	pkgs_to_install	массив	["app1","app2"]	Перечень пакетов для установки
	pkgs_to_remove	массив	["app3","app4"]	Перечень пакетов для удаления
	pkgs_to_update	массив	["app5","app6"]	Перечень пакетов для обновления

3.4.3.2 Настройка интервала синхронизации

Модуль управления интервалом синхронизации предназначен для централизованной настройки частоты обращения клиентского МУ к серверу Комплекса. Использование параметров rand_min и rand_max позволяет настроить минимальную и максимальную границы произвольного приращения к задаваемому параметру во избежание пиковых нагрузок. Параметры класса приведены в таблице 5.

Таблица 5 – Параметры класса

Имя класса	Имя параметра	Тип параметра	Пример значения	Описание
r_mob_runinterval				
	runinteval	целое число	15	Частота синхронизации в минутах
	rand_min	целое число	0	Минимальное приращение в минутах
	rand_max	целое число	4	Максимальное приращение в минутах

3.4.3.3 Управление блокировкой камеры

Модуль управления блокировкой камеры позволяет централизованно отключать (или включать) возможность использования камеры на МУ. Параметры класса приведены в таблице 6.

Таблица 6 – Параметры класса

Имя класса	Имя параметра	Тип параметра	Пример значения	Описание
r_mob_camera_control				
	camera_enable	логическое значение	true	Возможность запуска приложения камеры: true – разрешить; false – запретить

3.4.3.4 Управление ПИН-кодом

Модуль позволяет принудительно задать ПИН-код блокировки. При следующей синхронизации ПИН-код будет заменен. Если на момент выполнения сессия пользователя активна, то экран будет принудительно погашен, а сессия заблокирована. Разблокировка возможна только заново установленным паролем. Параметры класса приведены в таблице 7.

Таблица 7 – Параметры класса

Имя класса	Имя параметра	Тип параметра	Пример значения	Описание
r_mob_ch_pwd				
	password	строка	1234	ПИН-код блокировки МУ

3.4.3.5 Удаление пользовательских данных

Модуль позволяет осуществить удаление пользовательских данных из МУ в двух режимах:

Сброс к заводским настройкам – При выборе сброса к заводским настройкам МУ перезапустится, будет произведено полное удаление всех ранее произведенных настроек и пользовательских данных. Связь с Комплексом будет прервана и для повторного подключения необходимо будет произвести процедуру регистрации устройства.

Удаление пользовательских данных – Предполагает удаление только данных в домашнем каталоге пользователя с сохранением системных настроек и подключения к Комплексу.

Параметры класса приведены в таблице 8.

Таблица 8 – Параметры класса

Имя класса	Имя параметра	Тип параметра	Пример значения	Описание
r_mob_delete_user_data				
	hard_reset_to_defaults	логическое значение	false	Сброс устройства к заводским настройкам
	delete_user_data	логическое значение	false	Удаление данных в каталоге профиля пользователя

Следует обратить внимание, что удаление пользовательских данных будет происходить при каждом запуске агента Комплекса, пока класс r_mob_delete_user_data назначен устройству, а параметр delete_user_data установлен в значение true.

3.4.3.6 Управление GPS-приемником

Модуль позволяет управлять функционированием приемника глобальной системы позиционирования и функционалом отслеживания местоположения. Параметры класса приведены в таблице 9.

Таблица 9 – Параметры класса

Имя класса	Имя параметра	Тип параметра	Пример значения	Описание
r_mob_gps_control				
	gps_enable	логическое значение	true	Управление состоянием GPS-приемника: true – приемник включен; false – приемник выключен
r_mob_gps_control::gps_data				
	gps_location	логическое значение	true	Управление состоянием отслеживания местоположения: true – включено; false – выключено

Следует отметить, что корректная работа GPS-приемника зависит от многих факторов, основным из которых является отсутствие препятствий и/или помех прохождения сигнала.

3.4.3.7 Управление работой GSM-модема

Модуль позволяет управлять функционированием приемо-передатчика сигнала сотовой связи. Параметры класса приведены в таблице 10.

Таблица 10 – Параметры класса

Имя класса	Имя параметра	Тип параметра	Пример значения	Описание
r_mob_gsm_control				
	gsm_enable	логическое значение	true	Управление состоянием GSM-модема: true – включен;

Имя класса	Имя параметра	Тип параметра	Пример значения	Описание
				false – выключен

Следует обратить внимание, что при отсутствии Wi-Fi-подключений выключение GSM-модема может привезти к невозможности установления связи между МУ и сервером Комплекса

3.4.3.8 Получение информации о текущем состоянии

Получения информации о текущем состоянии МУ обеспечивается механизмом фактов. Подробно об использовании фактов описано в п.9.3 документа "Платформа централизованного управления жизненным циклом операционных систем "РОСА Центр Управления". Руководство системного администратора. Часть 2. Эксплуатация" (шифр РСЮК.10121-09 32 02). Параметры фактов приведены в таблице 11.

Таблица 11 – Параметры фактов

Основное имя факта	Имя параметра	Пример значения	Описание
r_mob_battery_capacity		68	Заряд АКБ в процентах
r_mob_battery_status	pkgs_to_install	Discharging	АКБ в режиме разряда
	pkgs_to_remove	Charging	АКБ заряжается
r_mob_camera	pkgs_to_update	true	Пользователю доступно использование камеры
r_mob_gps_data			Структурированный факт - местоположение
	timestamp	1742345601	Временная отметка полученных данных в формате UNIX
	altitude	122	Высота над уровнем моря
	accuracy	2.6	Оценочная точность полученных координат
	heading	273	Направление движения в градусах

Основное имя факта	Имя параметра	Пример значения	Описание
	latitude	68.545321	Широта
	longtitude	153.169764	Долгота
	osm_link	https://www.openstreetmap.org/?mlat=68.545321&mlon=153.169746&zoom=15	Сформированная ссылка просмотра местоположения на карте OpenStreetMap
r_mob_gsm_connection			Структурированный факт - данные о сотовой сети
	cell_id	0A092152	Идентификатор используемой базовой станции в 16-ричном формате
	registration_status	1	Код состояния регистрации в сети
	network_mode	2	Режим работы сети
	access_technology	7	Код используемой технологии связи
	location_area_code	87AF	LAC –код местоположения базовой станции в 16-ричном формате
	network_mode_description	Enabled (status + LAC and network type)	Расшифровка режима работы сети
	access_technology_description	LTE	Расшифровка используемой технологии связи
	registration_status_description	Registered, home network	Расшифровка состояния регистрации в сети
r_mob_wifi_networks			Структурированный факт
	wlan0	[{"essid"=>"KVA", "bssid"=>"D4:DA:21:73:2E:12", "signal_level"=>-33},	Информация о ближайших сетях в диапазоне 2.4 ГГц. Представлена в виде

Основное имя факта	Имя параметра	Пример значения	Описание
		{"essid"=>"CorpWIFI", "bssid"=>"08:43:F1:F6:35:2A", "signal_level"=>-81}]	хеша с отображением имени сети, аппаратного адреса и уровня сигнала
	wlan1	[{"essid"=>"KVA5", "bssid"=>"D4:DA:21:73:2E:13", "signal_level"=>-54}, {"essid"=>"CorpWIFI", "bssid"=>"08:43:F1:F6:35:2B", "signal_level"=>-60}]	Информация о ближайших сетях в диапазоне 5 ГГц. Представлена в виде хеша с отображением имени сети, аппаратного адреса и уровня сигнала
r_mob_packages	list::installed::<имя пакета>	<версия пакета>	Информация об установленных пакетах. Имя пакета является частью имени факта, значение факта – версия установленного пакета

3.5 Регистрация существующих узлов в РОСА Центр Управления

Для успешной регистрации в РОСА Центр Управления существующий узел должен соответствовать следующим предварительным условиям:

– основным сервером DNS регистрируемого узла должен быть сервер СИПА либо сервер DNS, который настроен так, что позволяет разрешать записи DNS сервера СИПА;

– на узле должны быть настроены источники пакетов, которые содержат пакеты puppet-agent;

– в случае использования стороннего сертификата для веб-интерфейса РОСА Центр Управления вместо самоподписанного сертификата ЦС Puppet на регистрируемый узел должен быть добавлен соответствующий сертификат CA (сертификат корневого доверенного ЦС) – файл /etc/foreman/ca.pem;

– узлу должны быть доступны сетевые порты сервера РОСА Центр Управления и сервера СИПА, указанные в подразделе 2.1.3.

Примечание – При необходимости настраивают для регистрируемых узлов правила автоподписывания сертификатов Puppet.

После подготовки узла нужно выполнить вход в веб-интерфейс РОСА Центр Управления и перейти в меню "Узлы → Зарегистрировать узел" панели навигации для настройки параметров регистрации узла (рисунок 47).

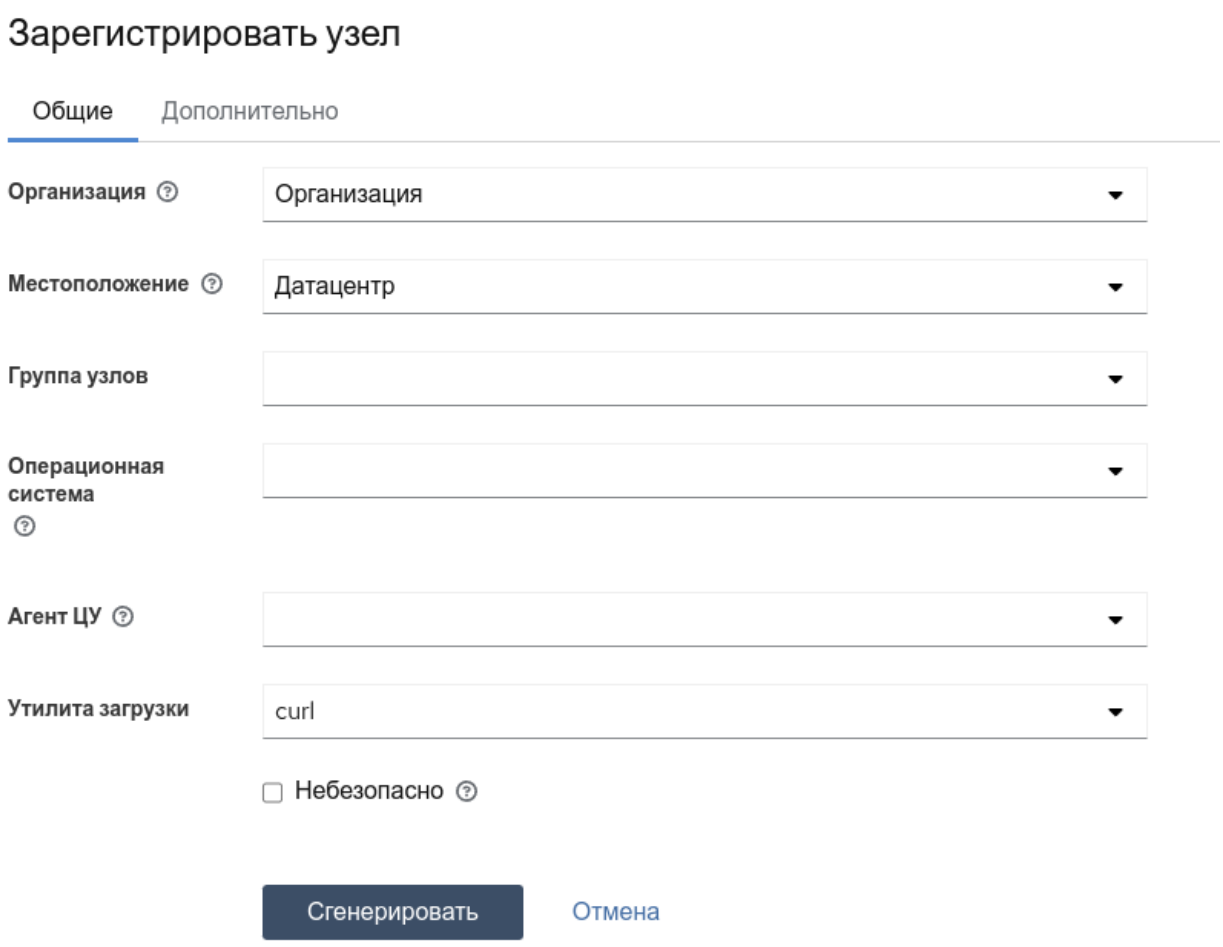

Рисунок 47 – Параметры регистрации узла

В соответствующих списках выбирают группу, в которую будет включен узел, затем выбирают ОС, а остальные параметры регистрации узла можно оставить со значениями по умолчанию.

В случае использования самоподписанного сертификата ЦС Puppet нужно включить параметр "Небезопасно".

Следует обратить внимание, что выбор группы определяет конфигурацию узла и настройки, которые будут применены к ОС. По умолчанию в РОСА Центр Управления доступны следующие группы узлов:

– Generic – при выборе этой группы применяются преднастроенные параметры сети, а также предоставляются функции дистанционного выполнения команд, скриптов и плейбуков (исполняемых сценариев) Ansible на регистрируемом узле;

– Puppet – при выборе этой группы дополнительно устанавливается и настраивается агент Puppet на регистрируемом узле.

Примечание – В процессе эксплуатации Комплекса необходимые пользовательские настройки могут быть внесены напрямую в параметры исходных групп, однако рекомендуется сделать копии групп и вносить изменения только в эти копии, а исходные группы использовать в качестве шаблонов.

Выбор ОС должен соответствовать фактически установленной на узел операционной системе, так как в зависимости от указанной версии ОС шаблоны подготовки генерируют различные скрипты регистрации, учитывающие доступные репозитории, версии пакетов программ и прочие специфические аспекты. Таким образом, скрипты регистрации, сгенерированные для одной ОС, в общем случае не могут быть использованы для другой ОС.

После настройки параметров регистрации нужно нажать кнопку Сгенерировать. В результате в текстовом поле под этой кнопкой появится созданная команда (скрипт регистрации).

Необходимо скопировать эту команду и выполнить в терминале ОС регистрируемого узла.

В случае успешной конфигурации и регистрации узла на экране появится соответствующее сообщение.

3.6 Развертывание новых узлов под контролем РОСА Центр Управления

Сетевое развертывание новых узлов под контролем РОСА Центр Управления выполняется в автоматическом режиме с применением стандартизированного сценария развертывания Kickstart.

В процессе развертывания узла осуществляется установка ОС и первичная настройка системной конфигурации узла (автоматически настраиваются имя узла, параметры сети и репозитории), а также выполняется регистрация узла в РОСА Центр Управления, при этом правила автоподписывания сертификатов не требуют какой-либо специальной подготовки.

3.6.1 Подготовка установочного носителя для ОС

Установочные носители для сетевой установки необходимо подготавливать на отдельном сервере, отличного от сервера РОСА Центр Управления.

Установочный носитель представляет собой копию установочного ISO-образа.

3.6.1.1 Настройка сервера репозиториев установочных носителей

Для установки ОС для сервера репозиториев установочных носителей рекомендуется использовать ROSA Enterprise Server.

Установка ОС производится в минимальной конфигурации.

При установке ОС необходимо задать статический адрес IPV4, который впоследствии будет использоваться в настройках Комплекса. Протокол IPV6 рекомендуется отключить.

После установки ОС необходимо установить дополнительное программное обеспечение apache, для чего выполнить команду от имени пользователя root:

```
# dnf -y install httpd
```

Установленный сервис нужно запустить и включить автоматический запуск при загрузке ОС. Для этого следует выполнить команду от имени пользователя root:

```
# systemctl enable --now httpd
```

В случае установленной и активной службы firewalld необходимо разрешить доступ на 80 порт TCP, либо отключить, выполнив команду:

```
# systemctl disable --now firewalld
```

По умолчанию корневой каталог сервера расположен по пути /var/www/html.

Для установки сервера подготавливаются установочные диски для одной из следующих ОС:

– ROSA Enterprise Server 9.x;
– ROSA Chrome/Fresh;
– Astra Linux 1.7;
– РЕД ОС 8;
– ALT Linux P10.

Далее нужно создать корневой каталог для установочных носителей, для чего выполнить команду от имени пользователя root:

```
# mkdir -p /var/www/html/media
```

Затем требуется создать каталоги для размещения установочных носителей, выполнив команду от имени пользователя root:

```
# mkdir -p /var/www/html/media/res
# mkdir -p /var/www/html/media/rosa
```

```
# mkdir -p /var/www/html/media/astra
# mkdir -p /var/www/html/media/redos
# mkdir -p /var/www/html/media/alt
```

Для получения ISO-образов рекомендуется использовать программу wget. В минимальной установке сервера она отсутствует, поэтому ее необходимо установить с помощью команды от имени пользователя root:

```
# dnf -y install wget
```

Затем необходимо скачать установочные образы ОС в каталог /tmp, например

```
# wget -O /tmp/res.iso [путь для установочного образа Rosa Enterprise Server 9]
# wget -O /tmp/rosa.iso [путь для установочного образа RosaLinux]
# wget -O /tmp/astra.iso [путь для установочного образа Astra Linux]
# wget -O /tmp/redos.iso [путь для установочного образа Redos Linux]
# wget -O /tmp/alt.iso [путь для установочного образа AltLinux]
```

После этого следует создать каталоги для монтирования установочных ISO-образов командой от имени пользователя root:

```
# mkdir -p /tmp/res
# mkdir -p /tmp/rosa
# mkdir -p /tmp/astra
# mkdir -p /tmp/redos
# mkdir -p /tmp/alt
```

Далее требуется смонтировать установочные ISO-образы в созданные каталоги, для чего выполнить команду от имени пользователя root:

```
# mount -o loop /tmp/res.iso /tmp/res
# mount -o loop /tmp/rosa.iso /tmp/rosa
# mount -o loop /tmp/astra.iso /tmp/astra
# mount -o loop /tmp/redos.iso /tmp/redos
# mount -o loop /tmp/alt.iso /tmp/alt
```

И, наконец, необходимо скопировать файлы из смонтированных ISO-образов ОС в каталоги установочных носителей, выполнив команды:

```
# cp -r /tmp/res/* /var/www/html/media/res
# cp -r /tmp/rosa/* /var/www/html/media/rosa
# cp -r /tmp/astra/* /var/www/html/media/astra
# cp -r /tmp/redos/* /var/www/html/media/redos
# cp -r /tmp/alt/* /var/www/html/media/alt
```

3.6.1.2 Подготовка установочного носителя ROSA Chrome/Fresh

Для подготовки установочного носителя ROSA Chrome/Fresh в каталоге установочного носителя /var/www/html/media/rosa нужно создать подкаталог для файлов загрузки командой:

```
# mkdir -p ./images/pxeboot
```

Далее необходимо скопировать файлы для загрузки:

```
# cp ./initrd0.img ./images/pxeboot/initrd.img
# cp ./vmlinuz0 ./images/pxeboot/vmlinuz
```

3.6.1.3 Подготовка установочного носителя Astra Linux 1.7

Для подготовки установочного носителя Astra Linux 1.7 в каталоге установочного носителя /var/www/html/media/astra нужно создать подкаталог для файлов загрузки:

```
# mkdir -p ./dists/stable/main/installer-
amd64/current/images/netboot/debian-installer/amd64
```

Затем требуется скопировать файлы для загрузки:

```
# cp ./netinst/initrd.gz ./dists/stable/main/installer-
amd64/current/images/netboot/debian-installer/amd64/initrd.gz
# cp ./netinst/linux ./dists/stable/main/installer-
amd64/current/images/netboot/debian-installer/amd64/linux
```

3.6.1.4 Подготовка установочного носителя ALT Linux P10

Для подготовки установочного носителя ALT Linux P10 нужно выполнить следующие действия:

а) в каталоге установочного носителя /var/www/html/media/alt создать подкаталог для файлов загрузки:

```
# mkdir -p ./syslinux/alt0
```

б) скопировать файлы для загрузки:

```
# cp ./boot/initrd.img ./syslinux/alt0/full.cz
# cp ./boot/vmlinuz ./syslinux/alt0/vmlinuz
```

в) перейти в каталог для установки:

```
# cd ./Metadata
```

г) создать каталог для скриптов установки:

```
# mkdir -p ./install-scripts/postinstall.d
# mkdir -p ./install-scripts/preinstall.d
```

д) создать файл ./install-scripts/postinstall.d/99_grub_install.sh для установки загрузчика:

```
#!/bin/bash
if [ "$(lsblk | grep /mnt/destination/boot/efi)" != ""
];then
 exit
fi
if [ "$(lsblk | grep /mnt/destination | grep nvme)" != "" ];
then
 bootdevice='/dev/nvme'
elif [ "$(lsblk | grep /mnt/destination | grep vda)" != ""
]; then
 bootdevice='/dev/vda'
elif [ "$(lsblk | grep /mnt/destination | grep sda)" != ""
]; then
 bootdevice='/dev/sda'
else
 bootdevice='notfound'
fi
if [ ${bootdevice} == "notfound" ]; then
 exit 1
fi
echo "${bootdevice}" >
/mnt/destination/tmp/grub_install.device
cat > /mnt/destination/tmp/grub_install.sh << EOF
#!/bin/bash
device=\`cat /tmp/grub_install.device\`
LC_ALL=C /usr/sbin/grub-install --boot-directory=/boot
\${device}
```

```
    LC_ALL=C /usr/sbin/update-grub
    fi
    EOF
    chmod +x /mnt/destination/tmp/grub_install.sh
    mount --bind /dev /mnt/destination/dev
    mount --bind /proc /mnt/destination/proc
    mount --bind /sys /mnt/destination/sys
    chroot /mnt/destination /tmp/grub_install.sh
    exit 0
```

е) создать права на исполнение скрипта:

```
    # chmod +x ./install-
scripts/postinstall.d/99_grub_install.sh
```

ж) создать архив с установочными скриптами:

```
    # rm -f ./install-scripts.tar && cd ./install-scripts && tar
-cf ../install-scripts.tar ./* && cd ..
```

з) удалить каталог подготовки скриптов:

```
    # rm -rf ./install-scripts
```

3.6.2 Подготовка к сетевому развертыванию узла на других ОС

3.6.2.1 Установка ОС на узле без автоматического развертывания

Процедура развертывания ОС на узле осуществляется по сценариям в виде скриптов "Шаблонов подготовки".

Перед сетевой установкой необходимо создать конфигурационные файлы для загрузки по сети. Для этого необходимо перейти в "Узлы → Шаблоны → Шаблоны подготовки", нажать на кнопку `Создать PXE по умолчанию` в верхнем правом углу и в появившемся модальном окне нажать на кнопку `Подтвердить`.

В случае развертывания ОС Альт Linux для подготовки в меню "Управление → Параметры" во вкладке "Подготовка" необходимо изменить значение параметра "Рендеринг в безопасном режиме" на "Да" (рисунок 48).

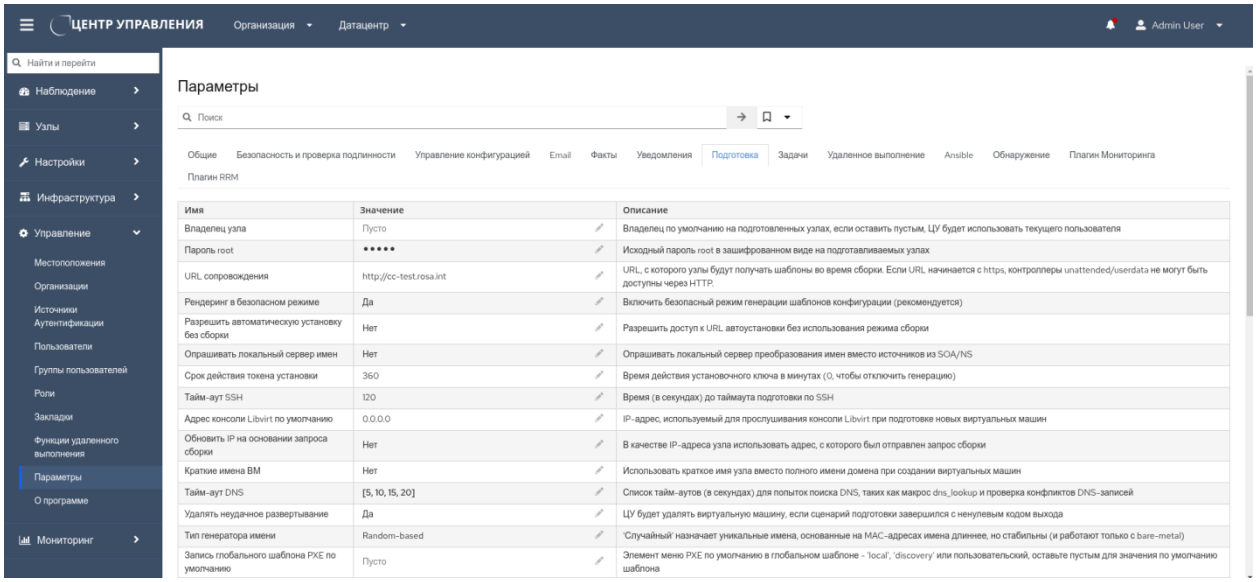

Рисунок 48 – Изменение параметров подготовки сетевой установки

Для подготовки установки ОС на узле без настройки автоматического развертывания необходимо настроить ВМ для загрузки по сети.

Затем следует перейти к загрузке ВМ, на которой предполагается развертывание, и на экране выбрать плагин "Control Center Discovery Image" (рисунок 49).

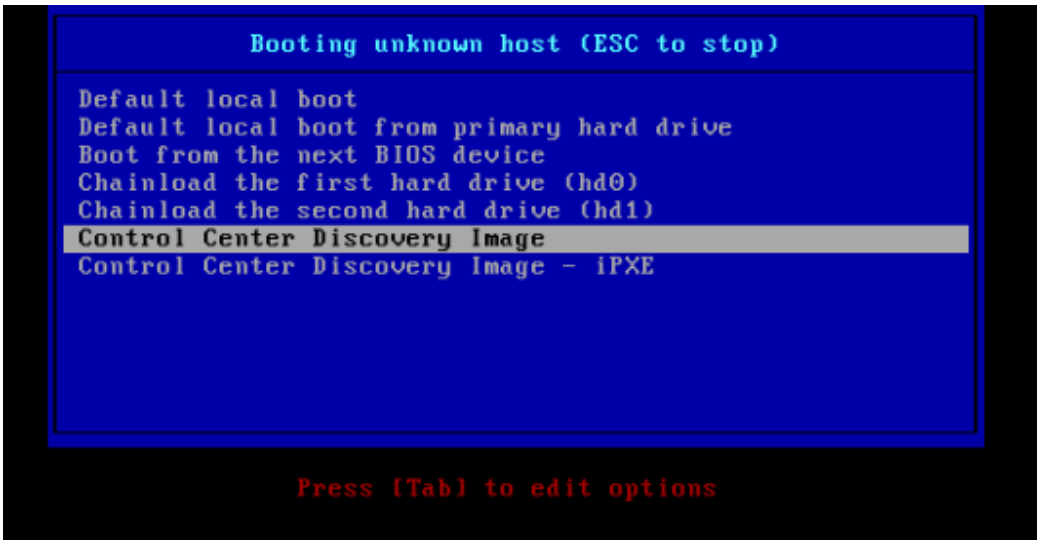

Рисунок 49 – Меню загрузки ВМ

После успешной загрузки по сети на экран будет выведено окно (рисунок 50).

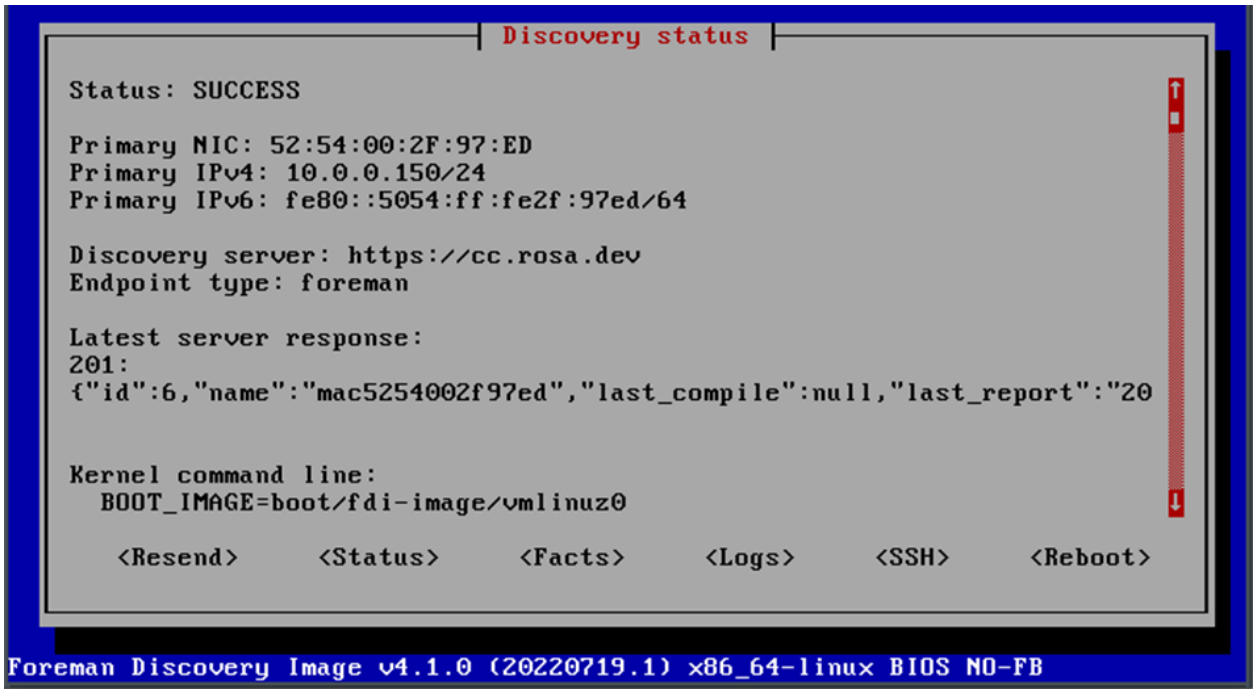

Рисунок 50 – Результат успешной загрузки

Далее в меню "Узлы → Обнаруженные узлы" в рабочей панели должен появиться обнаруженный узел (рисунок 51).

Для процедуры сетевой установки следует нажать кнопку Сетевая установка.

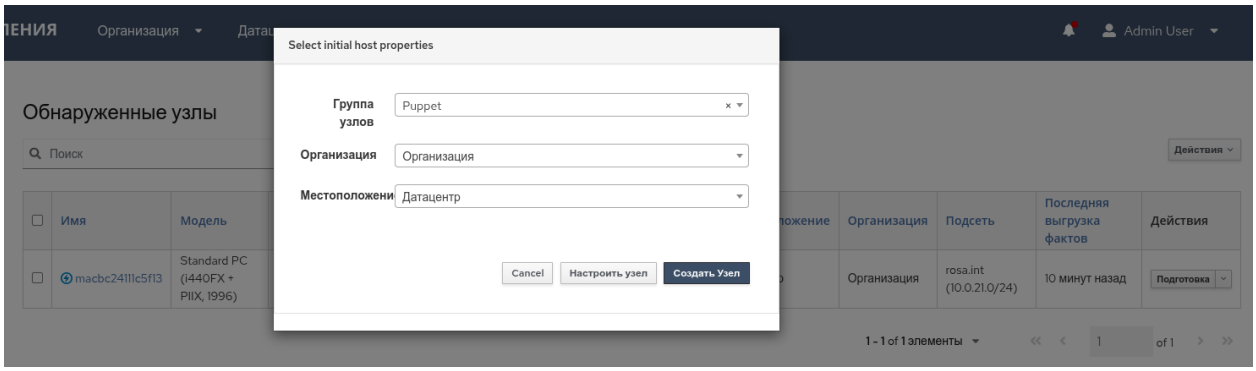

Рисунок 51 – Обнаруженные узлы

Далее в появившемся модальном окне нужно выбрать группу узлов "Puppet", организацию и местоположение, затем нажать кнопку Создать узел. Затем указать параметры для операционной системы, которая предполагается к установке и нажать кнопку Применить.

После этого будет создана конфигурация и ВМ перезагрузится автоматически в соответствии с параметрами развертывания.

В случае необходимости можно зарегистрировать отдельный узел в Комплексе, выполнив следующие действия:

а) установить пакет puppet-agent:

```
# dnf install puppet-agent
```

б) изменить настройки puppet-agent, указав в качестве переменной server сервер Комплекса в файле /etc/puppetlabs/puppet/puppet.conf:

```
[agent]
ca_server = cc.rosa.int
server = cc.rosa.int
```

в) выполнить команду обновления puppet:

```
puppet agent -t
```

В результате узел будет успешно зарегистрирован на сервере Комплекса.

3.6.2.2 Установка ОС на узле с автоматическим развертыванием

Для включения автоматического развертывания вновь обнаруженных узлов или групп узлов по заданным правилам требуется в меню "Управление → Параметры" на вкладке "Обнаружение" рабочей области задать значение "Да" параметру "Автоматическая подготовка" (рисунок 52), указать " Местоположение обнаружения", "Организация обнаружения". Для отмены авторазвертывания параметру присваивают значение "Нет".

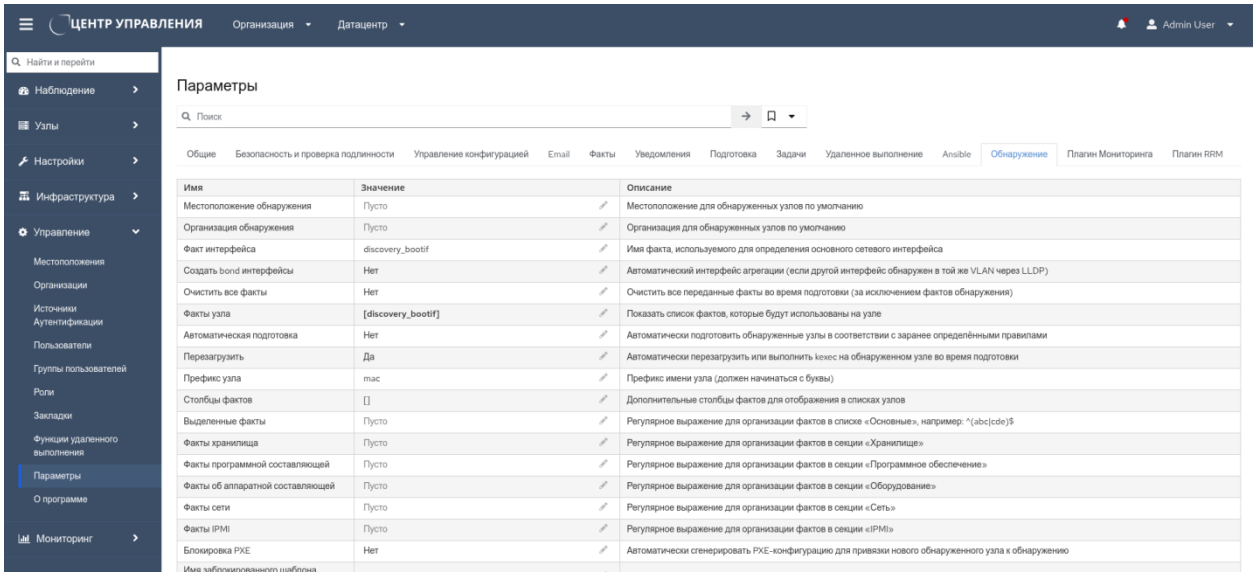

Рисунок 52 – Параметры авторазвертывания

Для всех обнаруженных узлов необходимо провести процедуру включения в группы узлов, задания правил и параметров сетевой установки в соответствии с п.5.1.3 в меню "Настройки → Группы узлов":

– на вкладке "Группа узлов" определить параметры для агента Puppet;
– на вкладке "Операционная система" назначить целевую ОС.

Для подготовки процедуры автоматического развертывания используется функционал правил обнаружения узлов.

Для создания правила обнаружения в меню "Настройка → Правила обнаружения" требуется нажать кнопку Создать правило (рисунок 53).

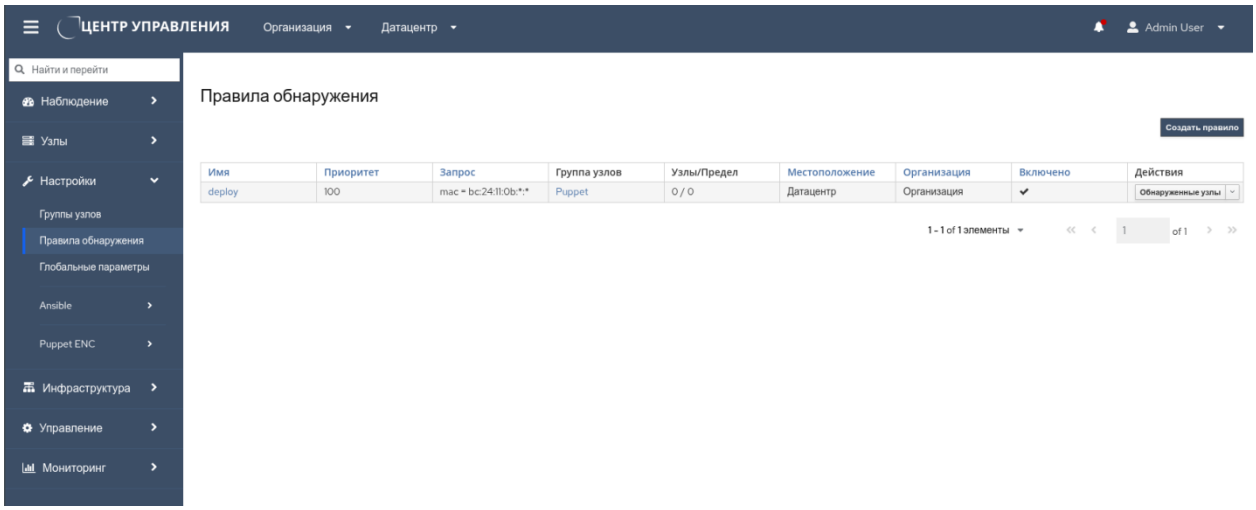

Рисунок 53 – Правила обнаружения

В рабочей области на вкладке "Основной" необходимо ввести значения полей (рисунок 54):

– Имя – имя правила;
– Search – условие для поиска узлов по их характеристикам;
– Hostname – имя узла;
– Ограничение узлов – максимальное инициализируемых число в соответствии с правилами (0 – без ограничений);
– Группа узлов – группа узлов, к которой будет применено правило с настроенными параметрами;
– Приоритет – приоритет применения правила (тем выше, чем ниже число).
– Включено – можно отключить параметр, чтобы правило не использовалось.

Для сохранения правила нажать кнопку Применить.

В рабочей области отобразится созданное правило автоматического развертывания, в строке которого можно выбором из столбца "Действия" нажать кнопки:

– Обнаруженные узлы – просмотреть обнаруженные по этому правилу узлы;

– Сопоставленные узлы – просмотреть управляемые узлы по этому правилу;

– Отключить – отключить правило;

– Удалить – удалить правило.

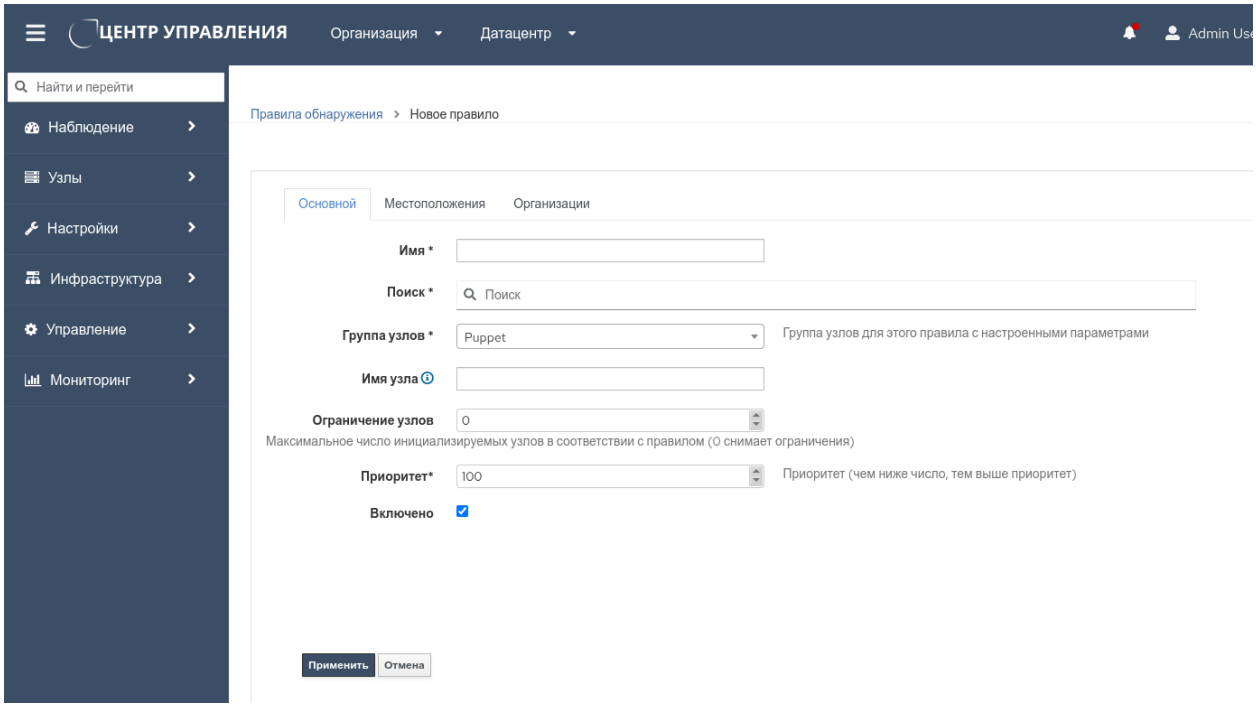

Рисунок 54 – Редактирование правила обнаружения

В результате на всех обнаруженных узлах будет автоматически создана конфигурация, узел перезагрузится и осуществится развертывание назначенной ОС в соответствии с заданными ранее правилами и параметрами.

3.6.3 Параметры сетевого развертывания узла

После регистрации лицензии и подготовки установочного носителя ОС необходимо выполнить настройку параметров сетевого развертывания узла. Для этого в веб-интерфейсе РОСА Центр Управления переходят в меню "Узлы → Создать узел" панели навигации.

На экране появится интерфейс настройки, в котором параметры развертывания нового узла распределены по вкладкам (рисунок 55).

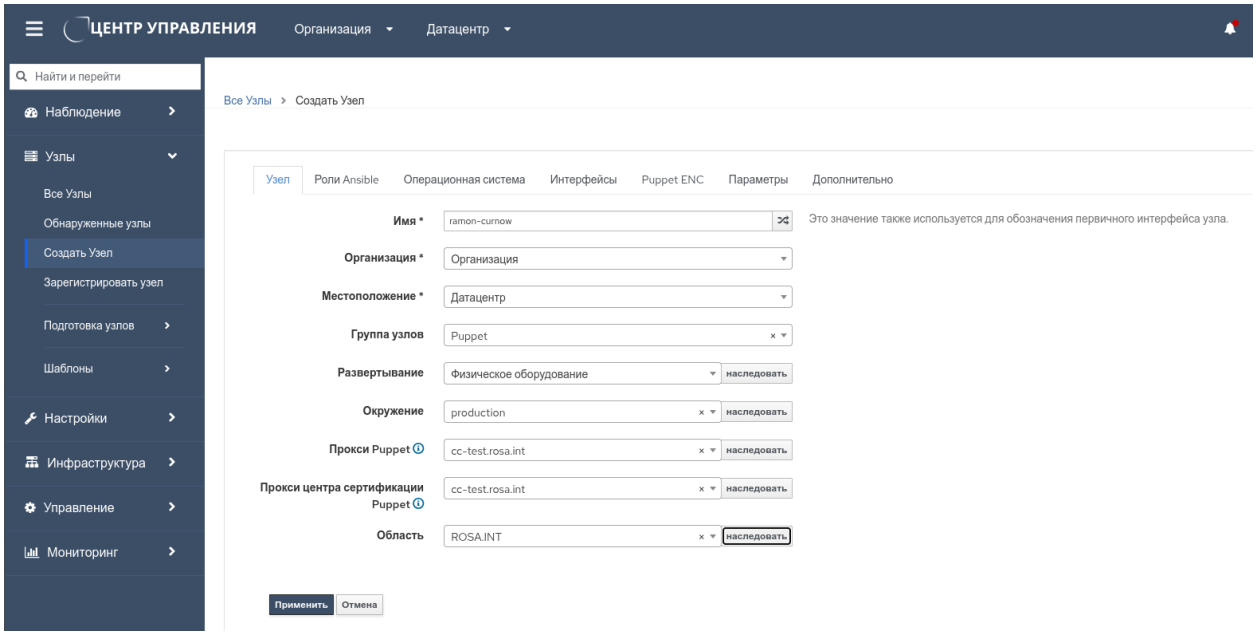

Рисунок 55 – Параметры сетевого развертывания узла

Во вкладке "Узел" интерфейса настройки указывают имя узла. Следует обратить внимание, что здесь указывается не полное доменное имя, а только непосредственно символьное имя узла (например, backup или monitoring). Затем из раскрывающегося списка "Область" выбирают домен СИПА, в который РОСА Центр Управления может вводить узлы. В итоге полное доменное имя узла будет составлено автоматически из символьного имени узла и имени домена.

При необходимости в первой вкладке можно выбрать группу, в которую будет включен узел (впрочем, узел может быть и вне группы). При этом соответствующие поля настроек Puppet будут автоматически заполнены в соответствии с настройками выбранной группы. Также здесь можно настроить параметры Puppet вручную. Необходимо обратить внимание, что изменить значения этих параметров после установки ОС будет невозможно. Для этого потребуется переустановка ОС.

Вкладка "Роли Ansible" предоставляют возможность присвоить роли Ansible. Перед установкой ОС допускается оставить для этих параметров значения по умолчанию, так как настройки этих параметров можно изменить впоследствии.

Во вкладке "Операционная система" указывают значения для следующих обязательных параметров настройки:

– архитектура;
– ОС;
– установочный носитель;
– таблица разделов;

– пароль суперпользователя root.

Во вкладке "Интерфейсы" настраивают параметры как минимум для одного (первичного) сетевого интерфейса. Обязательно указывают IP-адрес и MAC-адрес. При этом указанный MAC-адрес интерфейса должен соответствовать фактическому, так как по MAC-адресу первичного сетевого интерфейса узел идентифицируется во время первой загрузки и получает настройки через DHCP.

Вкладка "Puppet ENC" позволяет назначить список модулей Puppet для выполнения на узле. Перед установкой ОС допускается оставить для этих параметров значения по умолчанию, так как настройки этих параметров можно изменить впоследствии.

Вкладка "Параметры" содержит параметры управления поведением шаблонов подготовки, то есть параметры, которые влияют на генерируемые скрипты установки и настройки. При этом значения по умолчанию этих параметров согласованы с ROSA Enterprise Server, поэтому рекомендуется оставить существующие значения без изменений.

После завершения настройки параметров развертывания нужно нажать кнопку Применить.

В результате РОСА Центр Управления автоматически подготовит необходимые конфигурационные файлы pxelinux и kickstart, разместит ядро ОС и файл initrd в корневом каталоге TFTP, после чего на экране появится сообщение о готовности к сетевому развертыванию узла.

Затем требуется включить узел, установить приоритет загрузки узла по сети и дождаться окончания процесса развертывания.

3.7 Настройка аутентификации пользователей через внешнюю службу LDAP

Интеграция Комплекса со службой каталогов LDAP сервера СИПА (или иной внешней службой каталогов LDAP) позволяет осуществлять аутентификацию пользователей по протоколу LDAP/LDAPS в РОСА Центр Управления. Кроме того, при наличии политики периодической смены паролей обеспечивается стойкость и регулярная смена паролей пользователей РОСА Центр Управления через внешнюю службу каталогов.

Для настройки подключения к службе каталогов LDAP нужно выполнить вход в веб-интерфейс РОСА Центр Управления, перейти в меню "Администратор → Источники Аутентификации" панели навигации и нажать кнопку Создать источник аутентификации LDAP.

На экране появится интерфейс настройки, в котором параметры подключения распределены по вкладкам (рисунок 56).

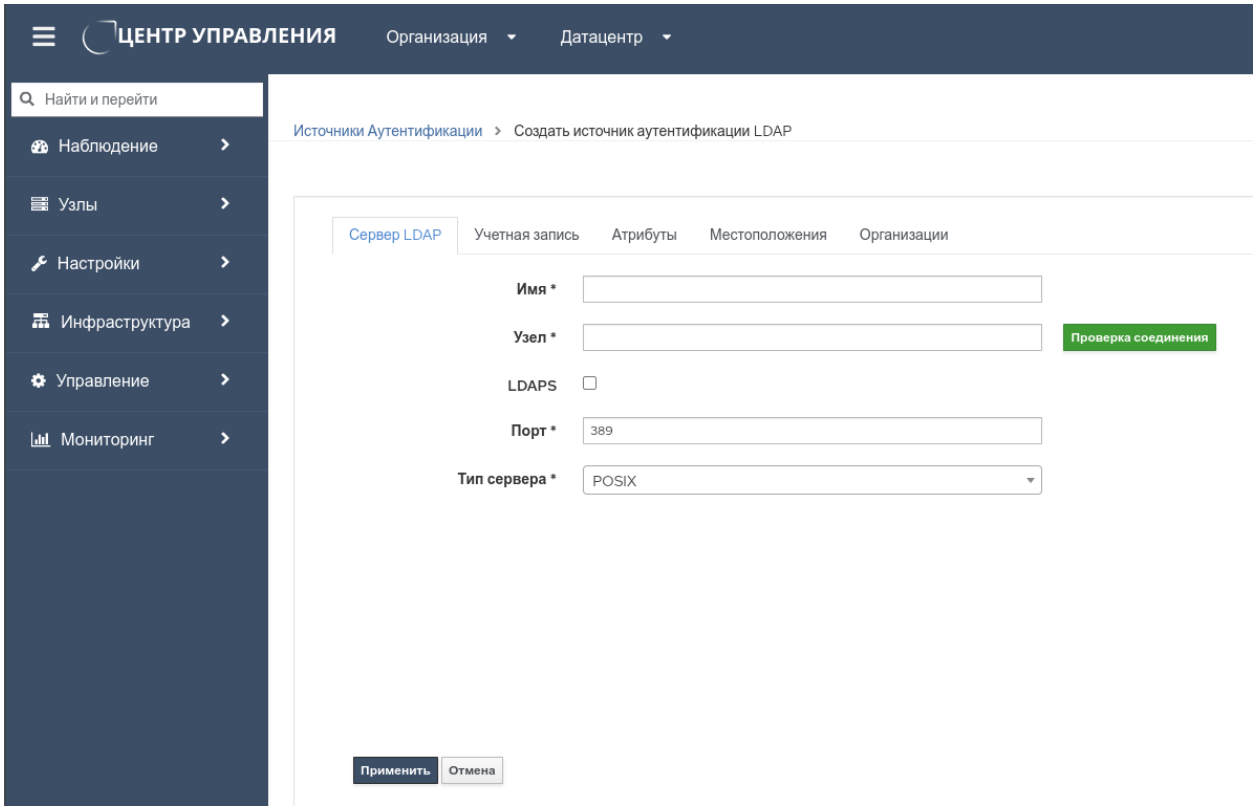

Рисунок 56 – Параметры подключения службы каталогов LDAP

Во вкладке "Сервер LDAP" интерфейса настройки указывают необходимые значения для следующих параметров подключения:

– Имя – краткое наименование подключаемой службы каталогов;

– Узел – имя или IP-адрес сервера LDAP (без указания протокола подключения);

– LDAPS – при активации этого параметра будет использоваться зашифрованное подключение;

– Порт – порт сервера LDAP;

– Тип сервера – категория (разновидность) сервера каталогов LDAP. В случае подключения к серверу СИПА указывают значение FreeIPA.

После настройки этих параметров следует нажать кнопку Проверка соединения. Если параметры сервера LDAP были указаны корректно, то проверка пройдет успешно. В противном случае нужно внести необходимые изменения в указанные значения этих параметров.

Во вкладке "Учетная запись" указывают необходимые значения для следующих параметров подключения:

– Учетная запись – учетная запись службы каталогов LDAP, имеющая право на чтение в каталоге. Этот пользователь используется для подключения к службе каталогов и выполнения запросов поиска учетных записей необходимых пользователей в каталоге в процессе аутентификации. В качестве значения следует указать отличительное имя для этой учетной записи (например, uid=ldapsearch,cn=users,cn=accounts,dc=dev,dc=lan);

– Пароль учетной записи – пароль пользователя, используемого для первоначального подключения к службе каталогов;

– Базовый DN – отличительное имя для записи каталога, которая содержит учетные записи пользователей (например, dc=dev,dc=lan);

– Базовый DN групп – отличительное имя для записи каталога, которая содержит информацию о группах пользователей (например, cn=groups,cn=accounts,dc=dev,dc=lan);

– Использовать сетевые группы – при активации будут использованы сетевые группы NIS вместо групп Posix;

– LDAP-фильтр – при необходимости задайте правила фильтрации учетных записей пользователей службы каталогов;

– Автоматическая регистрация – при активации параметра и в случае успешной авторизации пользователей службы каталогов будут автоматически создаваться соответствующие учетные записи пользователей РОСА Центр Управления;

– Синхронизация пользовательских групп – обязательно активируют этот параметр, чтобы осуществлялась синхронизация групп пользователей РОСА Центр Управления и групп службы каталогов LDAP.

Во вкладке "Атрибуты" не требуется дополнительная настройка параметров при подключении службы каталогов LDAP сервера СИПА.

Вкладки "Местоположения" и "Организации" содержат параметры, которые позволяют ограничить доступ пользователей подключаемой службы каталогов только указанными местоположениями и организациями (например, отдельными подразделениями и филиалами) в структуре предприятия.

После завершения настройки параметров подключения нужно нажать кнопку Применить.

Следует обратить внимание, что успешная аутентификация внешних пользователей службы каталогов LDAP не означает предоставление этим пользователям каких-либо прав по умолчанию в РОСА Центр Управления. Поэтому после настройки подключения к службе каталогов необходимо перейти в меню "Управление → Группы пользователей" панели навигации и нажать кнопку Создать группу пользователей для настройки необходимых прав

(ролей) и взаимосвязи между группой пользователей РОСА Центр Управления и группами службы каталогов LDAP.

На экране появится интерфейс настройки, в котором параметры группы пользователей РОСА Центр Управления распределены по вкладкам (рисунок 57).

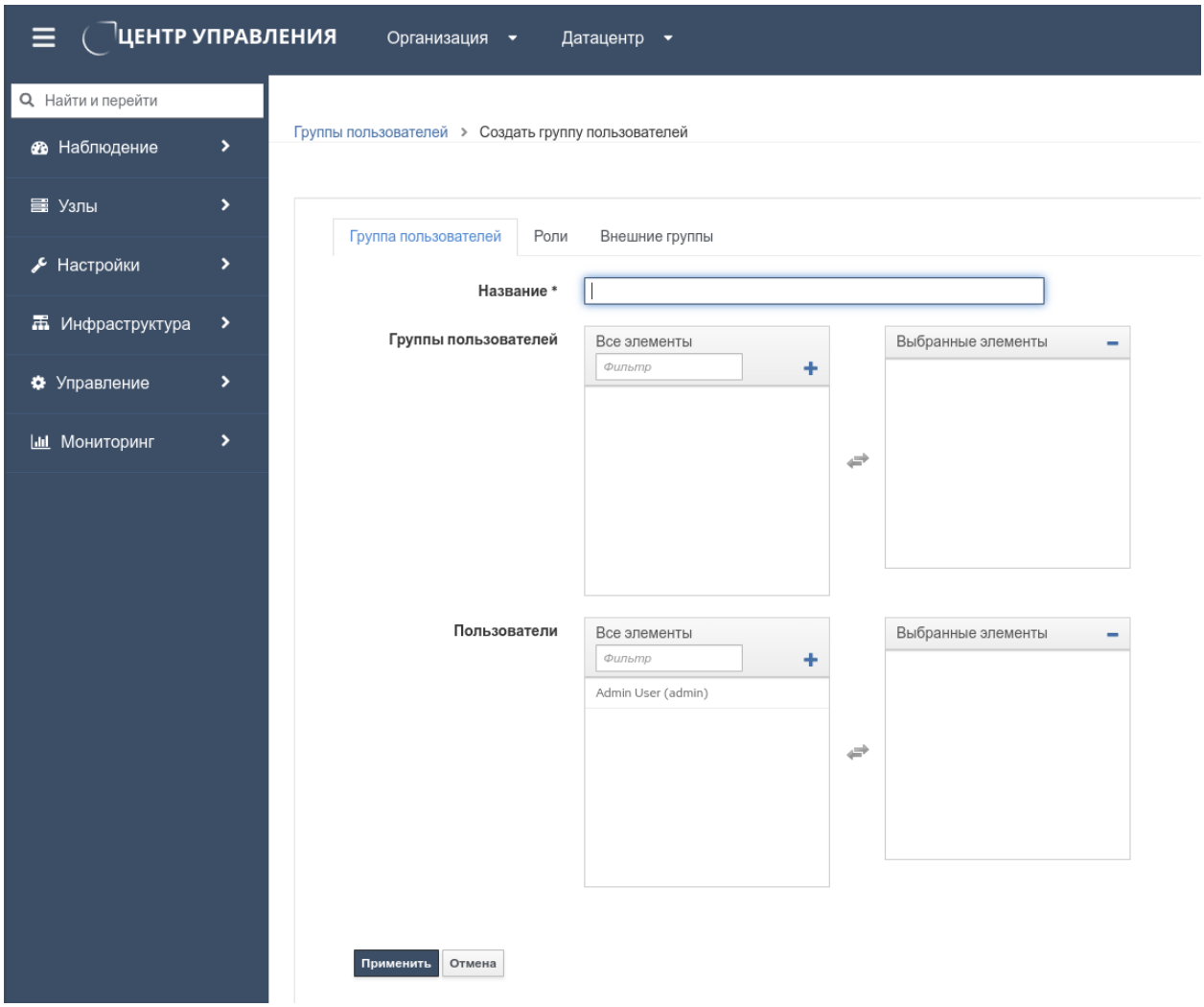

Рисунок 57 – Параметры группы пользователей

Во вкладке "Группа пользователей" интерфейса настройки указывают краткое наименование группы.

Во вкладке "Роли" присваивают этой группе пользователей необходимые роли в РОСА Центр Управления.

Во вкладке "Внешние группы" настраивают соответствие между внутренней группой пользователей РОСА Центр Управления и одной или несколькими внешними группами службы каталогов LDAP. При этом каждая из выбранных групп службы LDAP будет наделять своих пользователей правами в

соответствии с ролями, которые были ранее присвоены группе пользователей РОСА Центр Управления.

Для настройки необходимого соответствия между этими группами нужно нажать кнопку +Добавить внешнюю группу пользователей и ввести наименование нужной группы службы LDAP без атрибутов и в символьном виде (например, admins или users), после чего выбрать из списка "Источник аутентификации" ранее подключенную службу каталогов.

После завершения настройки параметров группы пользователей нужно нажать кнопку Применить.

С целью проверки следует выполнить вход в веб-интерфейс РОСА Центр Управления с реквизитами учетной записи внешнего пользователя из ранее выбранной и добавленной группы службы каталогов LDAP и убедиться, что права этого пользователя соответствуют ролям, присвоенным взаимосвязанным группам.

Примечание – Для внутренних пользователей, проходящих локальную аутентификацию при доступе к РОСА Центр Управления, рекомендуется создавать собственные отдельные (невзаимосвязанные) группы и присваивать необходимые роли аналогичным образом.

3.8 Подключение РОСА Центр Управления к внешней системе виртуализации

Интеграция Комплекса с внешней системой виртуализации (ROSA Virtualization, VMware) позволяет в процессе развертывания новых узлов создавать ВМ напрямую через веб-интерфейс РОСА Центр Управления.

Для настройки подключения к внешней системе виртуализации нужно выполнить вход в веб-интерфейс РОСА Центр Управления, перейти в меню "Инфраструктура → Вычислительные ресурсы" панели навигации и нажать кнопку Создать вычислительный ресурс.

На экране появится интерфейс настройки, в котором параметры подключения распределены по вкладкам (рисунок 58).

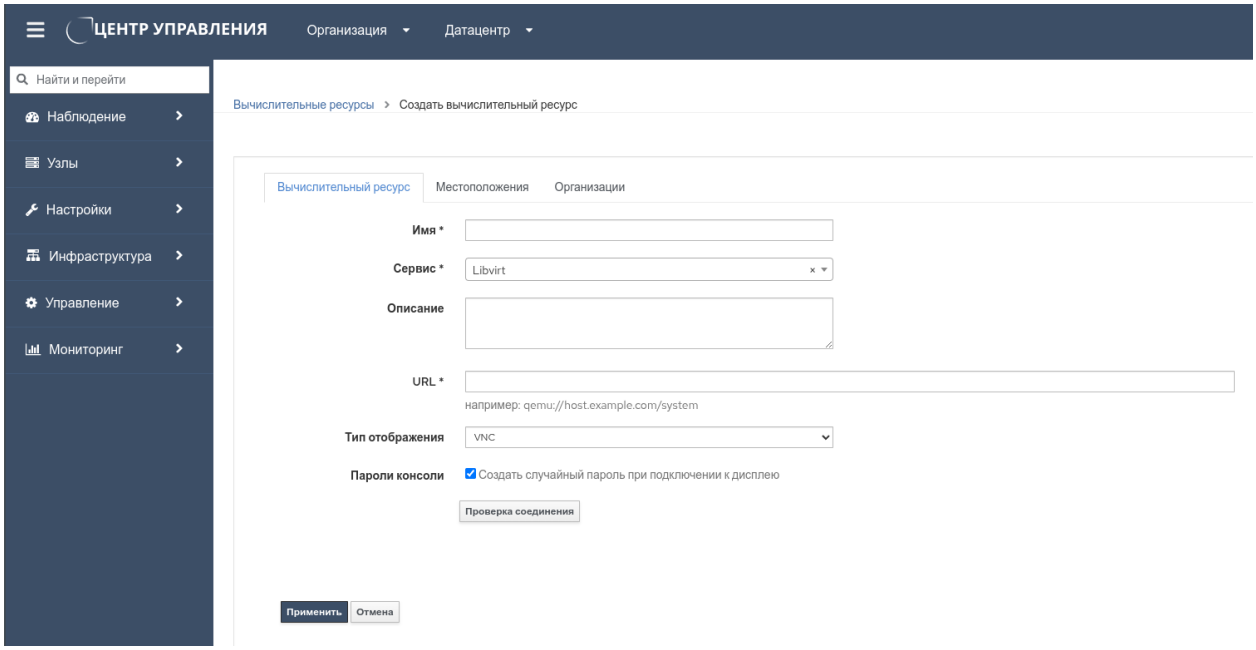

Рисунок 58 – Параметры подключения системы виртуализации

Во вкладке "Вычислительный ресурс" интерфейса настройки указывают необходимые значения для следующих параметров подключения:

– Имя – наименование подключаемой системы виртуализации;

– Сервис – платформа виртуализации (EC2, Libvirt, Openstack, VMware и Ovirt). В случае подключения к системе виртуализации ROSA Virtualization необходимо указать значение oVirt;

– Описание – краткое описание подключаемой системы виртуализации;

Далее в зависимости от выбранной системы виртуализации задать значения параметров:

– EC2:

  – HTTP прокси – прокси сервер для подключения к серверам поставщика;
  – Ключ доступа – публичный ключ SHH для доступа;
  – Секретный ключ – приватный ключ SSH для доступа;
  – Gov Cloud – использование в рамках правительственных сетей (не применяется);
  – Регион – выбор региона;

– Libvirt:

  – URL – сетевой адрес конечных точек API подключаемой системы виртуализации (например, https://virt.rosa.int/libvirt-engine/api);
  – Тип отображения – выбор типа отображаемого дисплея по умолчанию;

– Пароли консоли – включение случайного пароля для консоли;

– Openstack:

– URL – сетевой адрес конечных точек API подключаемой системы виртуализации (например, https://virt.rosa.int/openstack-engine/api);
– Пользователь – имя пользователя, имеющего права на управление ВМ, с указанием источника аутентификации (например, controlcenter@internal);
– Пароль – пароль пользователя.
– Название проекта (арендатора) – имя проекта (V3) или имя арендатора (V2) из CLI или файла RC;
– Домен пользователя – значение домена пользователя из CLI или файла RC (только для типа авторизации V3);
– Имя домена проекта – значение доменного имени проекта из CLI или файла RC (только для типа авторизации V3);
– ID домена проекта – значение ID домена проекта из CLI или файла RC (только для типа авторизации V3);
– Разрешить использование внешней сети в качестве главной сети – разрешает включение внешней сети провайдера в качестве основной сети Openstack;

– VMware:

– VCenter/Сервер – выбор сервера для подключения;
– Пользователь – имя пользователя, имеющего права на управление ВМ, с указанием источника аутентификации (например, controlcenter@internal);
– Пароль – пароль пользователя;
– Центр данных – выбор ЦОД для сеанса;
– Отпечаток – уникальный отпечаток сертификата VWware;
– Тип отображения – выбор типа отображаемого дисплея по умолчанию;
– Включить кэширование – включение кэширования вызовов провайдера VWware;
– Пароли для консоли VNC – включение случайного пароля для консоли;

– oVirt:

– URL – сетевой адрес конечных точек API подключаемой системы виртуализации (например, https://virt.rosa.int/ovirt-engine/api);

– Пользователь – имя пользователя, имеющего права на управление ВМ, с указанием источника аутентификации (например, controlcenter@internal);
– Пароль – пароль пользователя.
– Центр данных – выбор ЦОД для сеанса Ovirt;
– ID квоты – выбор установленной квоты провайдера Ovirt;
– Тип отображения по умолчанию – выбор типа отображаемого дисплея по умолчанию;
– Клавиатура VNC по умолчанию – выбор клавиатуры по умолчанию для сеанса VNC;
– Сертификация X509 – указывается центр сертификации или цепочка центров сертификации (оставляется пустым для автоматического заполнения).

Вкладки "Местоположения" и "Организации" содержат параметры, которые позволяют ограничить подключение системы виртуализации только указанными местоположениями и организациями (например, отдельными подразделениями и филиалами) в структуре предприятия.

После завершения настройки параметров подключения системы виртуализации нужно нажать кнопку Применить.

3.9 Интеграция с РОСА Менеджер ресурсов

Настоящий раздел описывает интеграцию Комплекса с программным средством "Платформа управления гибридной ИТ-инфраструктурой "РОСА Менеджер ресурсов" (далее — РОСА Менеджер ресурсов).

3.9.1 Сквозная авторизация через SSO (Kerberos)

Оба программных продукта поддерживают внешнюю аутентификацию пользователей с использованием службы каталогов на базе FreeIPA/СИПА, включая реализацию механизма единого входа (SSO) на основе протокола Kerberos.

Для обеспечения сквозной авторизации необходимо выполнить следующие условия:

а) Оба продукта должны быть настроены на работу с одним и тем же доменом СИПА.

В РОСА Центр Управления настройка внешней аутентификации выполняется в разделе "Управление → Источники аутентификации" с типом FreeIPA (подробнее в п. 5.3 документа "Платформа централизованного

управления жизненным циклом операционных систем "РОСА Центр Управления". Руководство системного администратора. Часть 2. Эксплуатация" (шифр РСЮК.10121-09 32 02).

В РОСА Менеджер ресурсов настройка внешней аутентификации выполняется в разделе "Параметры → Параметры приложения → Сервер → Аутентификация", где выбирается режим "Внешняя (httpd)" (подробнее в п. 4.2.1 документа "РОСА Менеджер ресурсов. Руководство системного администратора. Часть 2. Эксплуатация" (шифр – РСЮК.10111-04 32 02).

б) Веб-серверы обоих продуктов должны быть корректно интегрированы с Kerberos, для чего требуется:

– настроить доверенные SPN (Service Principal Names) для HTTP-сервисов;

– развернуть на серверах обоих продуктов сертификаты и ключи Kerberos в соответствии с требованиями домена СИПА;

– обеспечить синхронизацию времени на всех узлах с NTP-сервером домена.

в) Группы пользователей должны быть сопоставлены между продуктами.

Рекомендуется использовать одинаковые имена групп и ролей в обоих продуктах. Группы из СИПА должны быть привязаны к соответствующим ролям:

– в РОСА Центр Управления — через механизм внешних групп пользователей (подробнее в п. 5.3 документа "Платформа централизованного управления жизненным циклом операционных систем "РОСА Центр Управления". Руководство системного администратора. Часть 2. Эксплуатация" (шифр РСЮК.10121-09 32 02);

– в РОСА Менеджер ресурсов — через раздел "Параметры → Управление доступом → Группы" (подробнее в п. 4.2.2.2 документа "РОСА Менеджер ресурсов. Руководство системного администратора. Часть 2. Эксплуатация" (шифр – РСЮК.10111-04 32 02).

После выполнения указанных условий пользователь, прошедший аутентификацию в одном из продуктов, получает доступ к другому продукту без повторного ввода учетных данных при условии, что его браузер поддерживает передачу билетов Kerberos (например, настроена доверенная зона в браузере).

3.9.2 Переход между интерфейсами

При корректной настройке SSO обеспечивается возможность прямого перехода между веб-интерфейсами РОСА Центр Управления и РОСА Менеджер ресурсов:

– из интерфейса РОСА Центр Управления можно перейти к информации о соответствующем узле или виртуальной машине в РОСА Менеджер ресурсов, если объект зарегистрирован в обоих продуктах;

– из интерфейса РОСА Менеджер ресурсов можно перейти к странице управления узлом в РОСА Центр Управления, если узел введён в домен СИПА и известен Комплексу.

Для корректной работы переходов необходимо, чтобы:

– оба продукта были доступны по FQDN-именам из браузера пользователя;

– в настройках обоих продуктов были указаны корректные URL-адреса друг друга:

- в РОСА Менеджер ресурсов — через параметр "Настраиваемый URL поддержки" (подробнее в п. 4.2.1.3 документа "РОСА Менеджер ресурсов. Руководство системного администратора. Часть 2. Эксплуатация" (шифр – РСЮК.10111-04 32 02);

- в РОСА Центр Управления — через параметры внешних ссылок в шаблонах или профилях.

Таким образом, при соблюдении указанных требований достигается единый контур управления, позволяющий администратору использовать оба продукта как интегрированное решение для управления гибридной ИТ-инфраструктурой.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Определение
БД	База данных
ВМ	Виртуальная машина
ИТ	Информационные технологии
МУ	Мобильное устройство – смартфон или планшет на базе ОС "РОСА Мобайл"
ОС	Операционная система
ПО	Программное обеспечение
СИПА	Система идентификации, политик и аудита
УЗ	Учетная запись
ЦС	Центр сертификации
API	Application programming interface – программный интерфейс приложения
CA	Certification authority – центр сертификации (удостоверяющий центр)
DHCP	Dynamic host configuration protocol – протокол динамической настройки сетевой конфигурации узла
DNS	Domain name system – система доменных имен
ESR	Extended support release – релиз с расширенной (долговременной) поддержкой
HTTP	Hypertext transfer protocol – протокол передачи гипертекста
HTTPS	Hypertext transfer protocol secure – защищенная версия протокола передачи гипертекста
IANA	Internet assigned numbers authority – организация по управлению адресами в сети Интернет
IETF	Internet engineering task force – инженерный совет сети Интернет
IP	Internet protocol – протокол межсетевого взаимодействия
IPA	Identity, policy and audit – система идентификации, политик и аудита (СИПА)

Сокращение	Определение
LDAP	Lightweight directory access protocol – протокол доступа к каталогам
LDAPS	Lightweight directory access protocol secure – защищенная версия протокола доступа к каталогам
MAC	Media access control – уникальный идентификатор сетевого оборудования
mDNS	Multicast DNS – многоадресный DNS
NTP	Network time protocol – протокол сетевого времени
SSD	Solid state drive – твердотельный накопитель
SSH	Secure shell – защищенная оболочка
SSL	Secure sockets layer – уровень защищенных сокетов
TCP	Transmission control protocol – протокол управления передачей данных
TFTP	Trivial file transfer protocol – протокол передачи файлов
UDP	User datagram protocol – протокол пользовательских датаграмм
URL	Uniform resource locator – сетевой адрес ресурса