ООО «НТЦ ИТ РОСА»

УТВЕРЖДЕН
РСЮК.10121-01 91 01-ЛУ

КОМПЛЕКС УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ ГИБРИДНОЙ ИТ-ИНФРАСТРУКТУРЫ «РОСА ЦЕНТР УПРАВЛЕНИЯ»

Руководство по установке

РСЮК.10121-01 91 01

Листов 30

2023

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 «Комплекс управления жизненным циклом гибридной ИТ-инфраструктуры «РОСА Центр Управления»» РСЮК.10121-01 (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.

Дополнительные сведения об администрировании РОСА Центр Управления приведены в документе «Комплекс управления жизненным циклом гибридной ИТ-инфраструктуры «РОСА Центр Управления». Руководство администратора» РСЮК.10121-01 92 01.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

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

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

Сетевая установка ОС на новых хостах выполняется в автоматическом режиме с использованием DHCP и TFTP, а также применением сценария развертывания `Kickstart`. Развертывание контролируемых хостов 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 хостам через DHCP в качестве маршрута по умолчанию.

Примечание – Хосты, находящиеся вне управляемой локальной подсети, не могут быть инициализированы по сети автоматически, т.к. DHCP будет недоступен вне своей подсети. Однако, можно установить ОС на хост с носителя, и в дальнейшем зарегистрировать такой хост в РОСА Центр Управления. В этом случае необходимо настроить сеть и источники пакетов на хосте вручную, и после этого провести процедуру регистрации хоста.

РОСА Центр Управления предоставляет графический веб-интерфейс для централизованного мониторинга и администрирования контролируемых хостов. При этом доступ пользователей к элементам интерфейса комплекса и функциональным возможностям операционного управления хостами реализован с применением ролевой модели.

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.

Обратите 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 (см. подраздел 3.1).

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

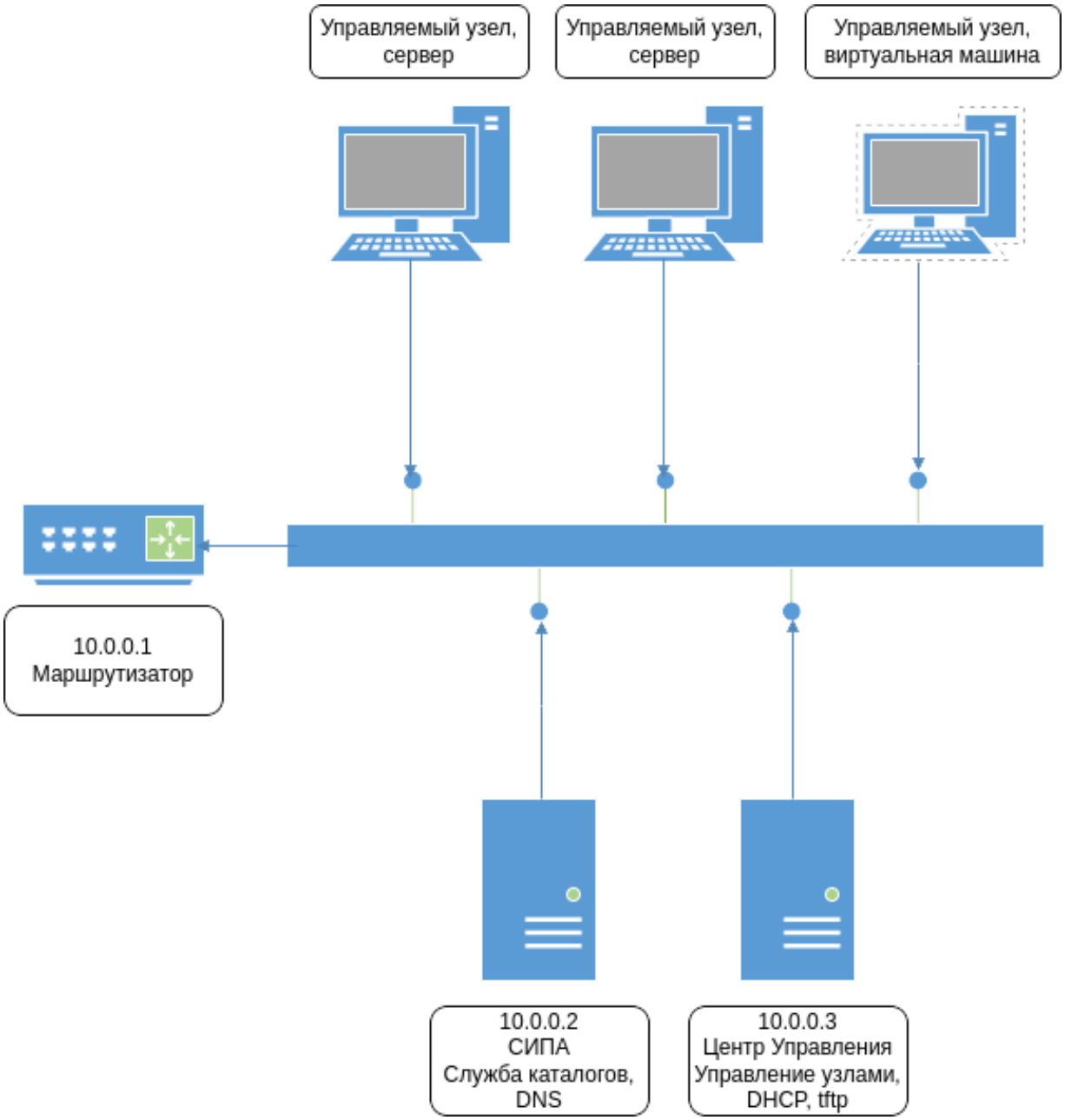

Рисунок 1 – Общая схема конфигурации РОСА Центр Управления

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

Сервер СИПА обеспечивает управляемым хостам 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 хосты в домене и автоматически создавать все необходимые записи для управляемых хостов.

РОСА Центр Управления функционирует в своей локальной подсети в качестве сервера DHCP и TFTP, назначает управляемым хостам IP-адреса, передает сетевые настройки, обеспечивает сетевую загрузку и установку ОС, а в качестве маршрута по

умолчанию РОСА Центр Управления назначает хостам IP-адрес маршрутизатора (например, `10.0.0.1`).

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

Примечание – Для того, чтобы управляемые хосты могли разрешать имена хостов 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.

Собственный IP-адрес (например, `10.0.0.3`) сервер РОСА Центр Управления передает агентам `Puppet` и/или `Salt`, принимает и регистрирует отчеты агентов управления конфигурацией, обеспечивает управление этими агентами, а также предоставляет агентам доступ к классам `Puppet` и к состояниям `Salt`.

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 следующей таблице.

Таблица 1 – Требования к аппаратным средствам сервера РОСА Центр Управления

Параметр	Минимальное значение	Рекомендуемое значение
Количество ядер процессора	2	4
Объем оперативной памяти в Гбайт	4	8
Свободное дисковое пространство в 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.

Обратите внимание, что при увеличении количества управляемых хостов может потребоваться дополнительное дисковое пространство для хранения журналов.

2.1.2. Сервер СИПА

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

Таблица 2 – Требования к аппаратным средствам сервера СИПА

Параметр	Минимальное значение	Рекомендуемое значение
Количество ядер процессора	2	4
Объем оперативной памяти в Гбайт	4	4
Свободное дисковое пространство в Гбайт	20	40

2.2. 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/`**`4505`**, `TCP/`**`4506`** – Salt;
- `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 хостам по протоколу SSH, используя по умолчанию порт `TCP/`**`22`**. Обратите внимание,

что при использовании иного порта необходимо в процессе настройки РОСА Центр Управления добавить параметр `remote_execution_ssh_port`, где указать используемый номер порта для каждого такого хоста.

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 слушать 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.

2.3. 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 РОСА “Кобальт” Сервер, CentOS и т.п.

3. УСТАНОВКА И ПЕРВИЧНАЯ НАСТРОЙКА КОМПЛЕКСА

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

- установка СИПА;

- установка РОСА Центр Управления;

- регистрация существующих хостов в РОСА Центр Управления;

- сетевое развертывание новых хостов 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 администратор сначала осуществляет установку ОС на физический сервер или ВМ, а затем выполняет консольный интерактивный сценарий установки СИПА `ipa-server-install`.

3.1.1. Установка ОС на сервер СИПА

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

Для запуска программы установки ОС загрузите сервер СИПА с этого носителя.

На экране последовательно появятся меню программы установки, интерфейс для выбора языка сопровождения установки и меню “`Сводка установки`”, предназначенное для обзора и последующей настройки параметров установки.

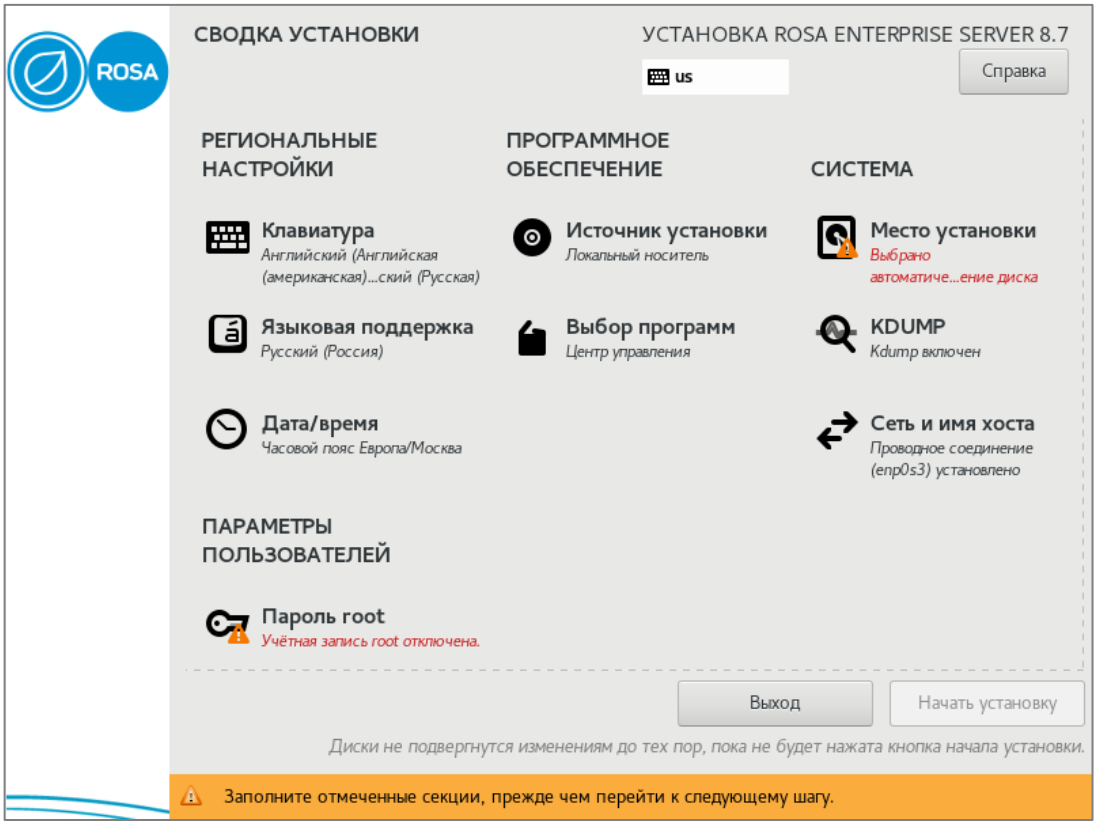

Рисунок 2 – Сводка установки

Меню “Сводка установки” содержит тематические секции, в которые сгруппированы соответствующие параметры установки. Обратите внимание, что вместо последовательного определения параметров программа установки дает возможность настроить параметры в произвольном порядке, выбирая необходимые секции в меню “Сводка установки”.

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

Примечание – Убедитесь, что в секции “Источник установки” автоматически настроен параметр “Локальный носитель”.

Нажмите на наименование секции для перехода к интерфейсу настройки соответствующих параметров. После настройки параметров нажмите кнопку Готово для возвращения в меню “Сводка установки”.

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

В секции “Место установки” выберите необходимый диск и установите переключатель “Конфигурация устройств хранения данных” в положение “Автоматически”.

В секции “Сеть и имя хоста” задайте полное доменное имя сервера СИПА, которое должно быть доменным именем по крайней мере третьего уровня (например, ipa.company.ru, где ipa – краткое имя хоста, а company.ru – домен, в котором СИПА будет выполнять функции контроллера домена).

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

Примечание – Для функционирования СИПА необходим уникальный домен. При выборе домена избегайте 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 хостов по сети при использовании этого домена.

Далее, подключите необходимый сетевой интерфейс сервера СИПА и настройте параметры сетевого соединения – IP-адрес (например, 10.0.0.2), маску сети (например, 255.255.255.0), шлюз по умолчанию (например, 10.0.0.1).

Обратите 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 хосты не потеряют связь с контроллером.

В секции “Пароль root” установите пароль для учетной записи суперпользователя root.

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

После завершения процесса установки ОС нажмите 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 осуществите вход в ОС сервера СИПА от имени учетной записи суперпользователя `root` и выполните следующую консольную команду:

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

Сценарий установки предложит настроить встроенную службу DNS. Для подтверждения введите `yes`:

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

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

```
Server host name [ipa.company.ru]:
Please confirm the domain name [company.ru]:
Please provide a realm name [COMPANY.RU]:
```

Чтобы принять предложенные значения по умолчанию, нажмите клавишу `Enter`.

Для изменения параметра по умолчанию введите необходимое значение.

Установите (введите и подтвердите) 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, введите `no`.

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

Далее, сценарий установки предложит проверить, нужно ли настроить какие-либо обратные записи DNS для IP-адресов, связанных с СИПА. Для подтверждения нажмите клавишу `Enter` или введите `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 нажмите 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 введите `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`) выполните 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 перезагрузите конфигурацию межсетевого экрана. Для этого выполните 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 введите в адресной строке браузера (на внешней рабочей станции) доменное имя сервера СИПА.

Например:

```
https://ipa.company.ru
```

На экране появится страница авторизации веб-интерфейса.

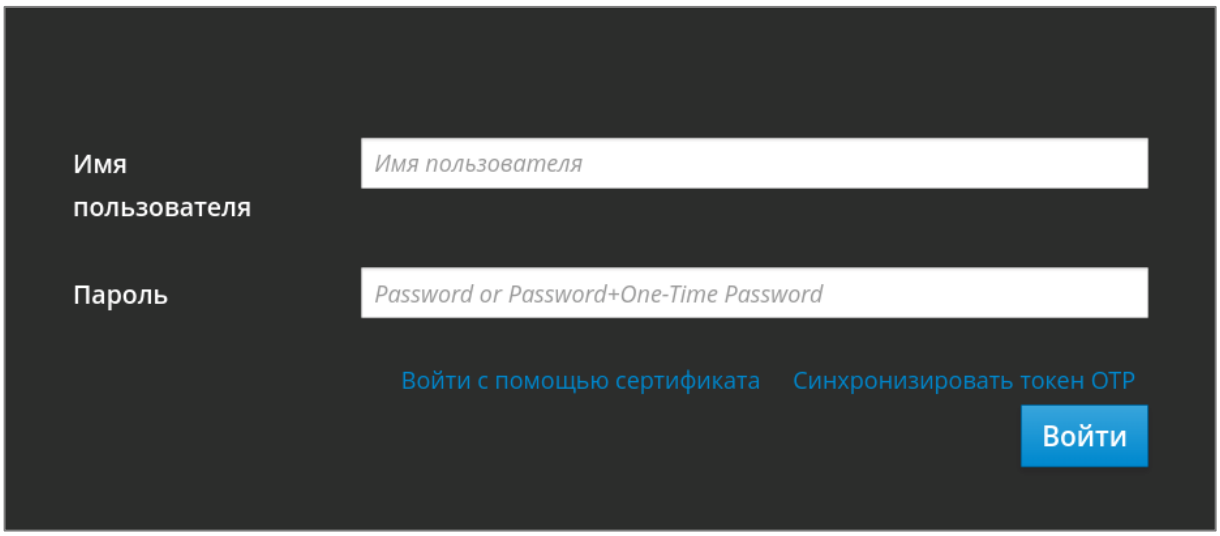

Рисунок 3 – Страница авторизации СИПА

Для входа в интерфейс введите имя и пароль пользователя в соответствующие поля, после чего нажмите кнопку `Войти`.

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

3.2. Установка РОСА Центр Управления

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

- установка ОС на физический сервер или ВМ;

- добавление сертификата SSL;

- выполнение интерактивного сценария установки РОСА Центр Управления `controlcenter-install`.

3.2.1. Установка ОС на сервер РОСА Центр Управления

Для запуска программы установки ОС загрузите 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 “`Сводка установки`”, предназначенное для обзора и последующей настройки параметров установки.

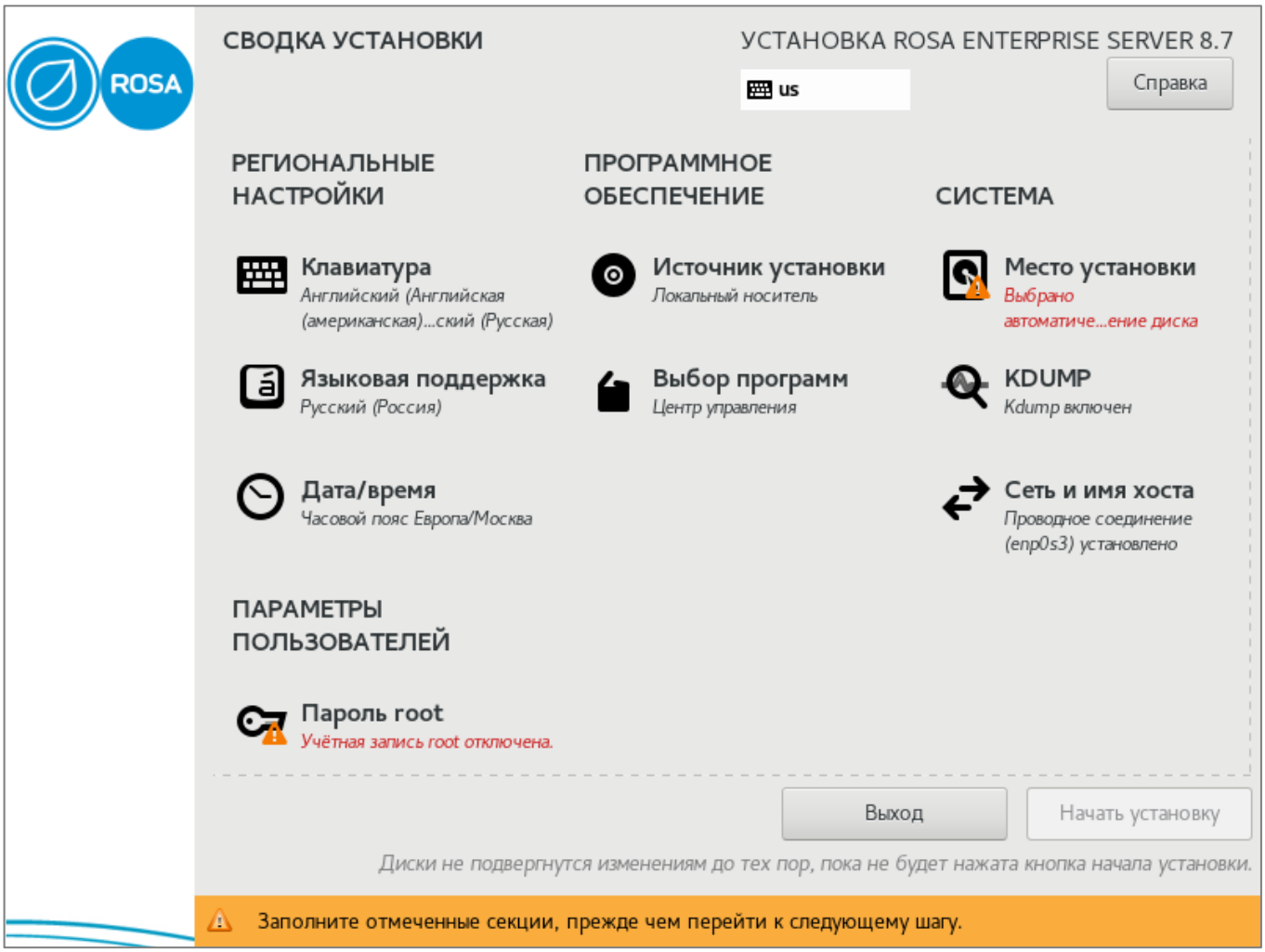

Рисунок 4 – Сводка установки

Меню “Сводка установки” содержит тематические секции, в которые сгруппированы соответствующие параметры установки. Обратите внимание, что вместо последовательного определения параметров программа установки дает возможность настроить параметры в произвольном порядке, выбирая необходимые секции в меню “Сводка установки”.

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

Примечание – Убедитесь, что в секции “Источник установки” автоматически настроен параметр “Локальный носитель”, а в секции “Выбор программ” настроен параметр “Центр управления”.

Нажмите на наименование секции для перехода к интерфейсу настройки соответствующих параметров. После настройки параметров нажмите кнопку Готово для возвращения в меню “Сводка установки”.

В секции “Место установки” выберите необходимый диск и установите переключатель “Конфигурация устройств хранения данных” в положение “Автоматически”.

В секции “Сеть и имя хоста” задайте полное имя сервера РОСА Центр Управления в домене СИПА, что позволит автоматически зарегистрировать хост в домене (например, cc.company.ru, где cc – краткое имя хоста, а company.ru – домен, в котором СИПА является контроллером домена).

Далее, подключите необходимый сетевой интерфейс сервера РОСА Центр Управления и настройте параметры сетевого соединения – IP-адрес (например, 10.0.0.3), маску сети (например, 255.255.255.0), шлюз по умолчанию (например, 10.0.0.1), сервер DNS (например, 10.0.0.2).

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

В секции “Пароль root” установите пароль для учетной записи суперпользователя root.

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

После завершения процесса установки нажмите кнопку Перезагрузка системы.

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

3.2.2. Добавление сертификата SSL

Сертификат SSL используется веб-интерфейсом РОСА Центр Управления для обеспечения безопасного сетевого соединения, а соответствующий сертификат CA (сертификат корневого доверенного ЦС) используется в процессе установки и функционирования РОСА Центр Управления.

Примечание – Для веб-интерфейса РОСА Центр Управления может использоваться самоподписанный сертификат ЦС Puppet, однако рекомендуется установить и использовать сертификат доверенного центра сертификации.

Установка сертификата SSL осуществляется в терминале ОС сервера РОСА Центр Управления от имени учетной записи суперпользователя root в соответствии со следующей инструкцией.

1. Выполните следующую команду для создания каталога `/etc/httpd/cc_ssl/`:

```
# mkdir /etc/httpd/cc_ssl
```

2. Скопируйте сертификат хоста в файл `/etc/httpd/cc_ssl/cert.pem`.

3. Скопируйте сертификат промежуточного центра сертификации в файл `/etc/httpd/cc_ssl/chain.pem`.

4. Скопируйте ключ в файл `/etc/httpd/cc_ssl/key.pem`.

5. Выполните следующие команды, чтобы сделать ключ доступным на чтение только веб-серверу:

```
# chgrp apache /etc/httpd/cc_ssl/key.pem
# chmod 0640 /etc/httpd/cc_ssl/key.pem
```

6. Скопируйте сертификат CA в файл `/etc/foreman/ca.pem`.

Обратите внимание, что в систему необходимо добавить все требуемые файлы – `cert.pem`, `chain.pem`, `key.pem`, `ca.pem`. В противном случае для веб-интерфейса РОСА Центр Управления будет использоваться самоподписанный сертификат ЦС Puppet.

После добавления в систему необходимых сертификатов выполните сценарий установки РОСА Центр Управления.

3.2.3. Выполнение сценария установки РОСА Центр Управления

Установка РОСА Центр Управления осуществляется консольной утилитой `controlcenter-install`.

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

```
# controlcenter-install
```

На экране появится текстовый интерфейс сценария установки. Для сопровождения процесса следуйте инструкциям этого интерфейса.

```
Обнаружены следующие сетевые интерфейсы:
enp7s0: 10.0.0.3/16
Укажите на каком интерфейсе будет использоваться DHCP: (enp7s0) [enp7s0]:
Укажите адрес маршрутизатора [10.0.0.1]:
```

Рекомендуется явно указать IP-адрес маршрутизатора в локальной подсети, который будет передаваться управляемым хостам 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.

```
...
```

```
Вы можете настроить диапазон DHCP, в котором IP адреса будут
выдаваться безусловно.

Хосты, получившие такой IP адрес, не контролируются и не учитываются
Центром Управления.

Желаете настроить диапазон DHCP? [y/N]: y

Укажите начало диапазона [10.0.0.5]:

Укажите конец диапазона [10.0.64.0]:
```

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 укажите 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.

```
...
Укажите учётные данные пользователя с правом добавления хостов в
домен СИПА.

логин: admin

пароль: ********

повтор: ********
```

Примечание – Здесь необходимо указать реквизиты учетной записи администратора СИПА.

```
...
Пользователь Центра Управления по умолчанию - admin,

задайте пароль для доступа к интерфейсу от имени этого пользователя.

пароль: ********

повтор: ********
```

Далее, для подтверждения всех сделанных настроек конфигурации РОСА Центр Управления введите `y`:

```
Выбранные параметры:
 интерфейс: enp7s0
 подсеть: 10.0.0.0/16
 маршрутизатор: 10.0.0.1
 диапазон DHCP: 10.0.0.5 - 10.0.64.0
Принять и продолжить? [y/N]: y
```

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

```
PLAY [Set up Foreman] **********************************************

TASK [Gathering Facts] *********************************************

...
```

```
TASK [Report] ******************************************************
ok: [foreman] => {}
```

После завершения работы сценария установки необходимо разрешить РОСА Центр Управления вносить изменения в прямую и обратную зоны DNS. Для этого сценарий установки автоматически сгенерирует правило следующего вида:

```
grant DNS\047cc.company.ru@COMPANY.RU wildcard * ANY;
```

Скопируйте созданное правило, после чего выполните вход в веб-интерфейс СИПА, где перейдите в меню “Сетевые службы → DNS → Зоны DNS” панели навигации.

Далее, в параметрах прямой и обратной зоны DNS просмотрите существующие правила в поле “Политика обновления BIND” и добавьте правило, сгенерированное сценарием установки, а также убедитесь, что разрешено динамическое обновление.

Примечание – В случае, если требуется ограничить права РОСА Центр Управления, измените параметры созданного правила соответствующим образом.

В результате выполненных действий по установке комплекса, развернутый РОСА Центр Управления содержит следующие структурные элементы:

- подсеть;
- домен;
- настроенные и подготовленные к сетевой установке на управляемых хостах операционные системы РОСА “Кобальт” и ROSA Enterprise Server;
- примеры групп хостов;
- настроенные ассоциации шаблонов развертывания;
- сервер Puppet;
- сервер Salt;
- Ansible;
- плагины управления вычислительными ресурсами систем виртуализации ROSA Virtualization, VMWare и Libvirt.

3.2.4. Доступ к веб-интерфейсу РОСА Центр Управления

Для доступа к веб-интерфейсу РОСА Центр Управления введите в адресной строке браузера (на внешней рабочей станции) доменное имя сервера РОСА Центр Управления.

Например:

```
https://cc.company.ru
```

На экране появится страница авторизации веб-интерфейса.

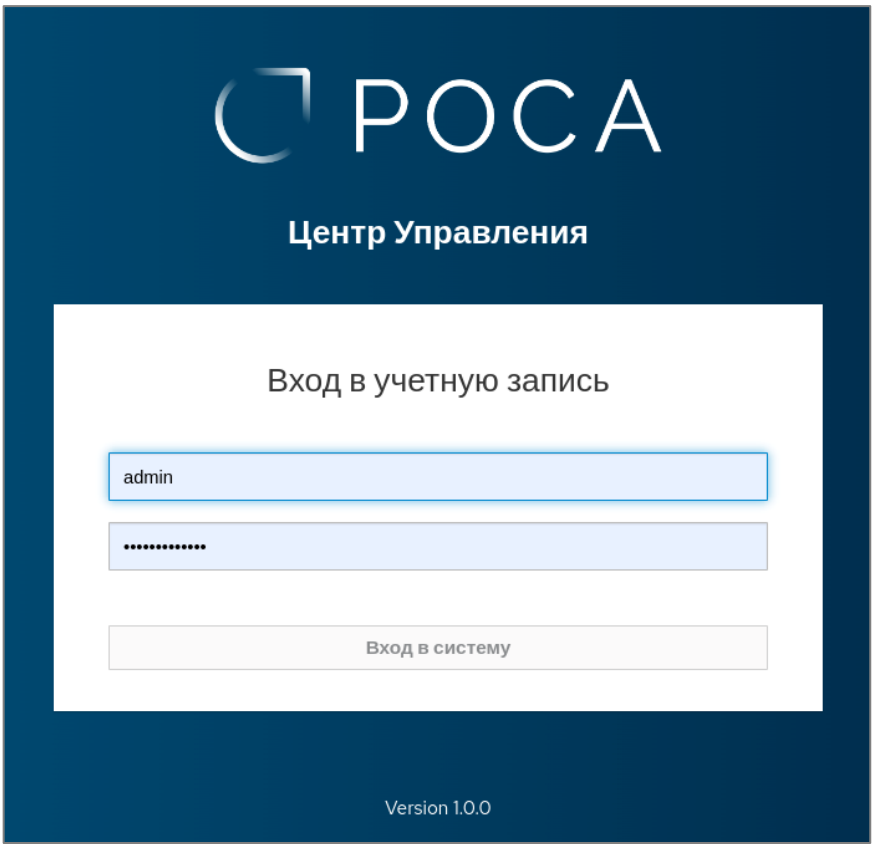

Рисунок 5 – Страница авторизации РОСА Центр Управления

Для входа в интерфейс введите имя и пароль пользователя, после чего нажмите кнопку `Вход в систему`.

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.

Для перемещения по страницам интерфейса РОСА Центр Управления используйте необходимые вкладки и пункты меню панели навигации.

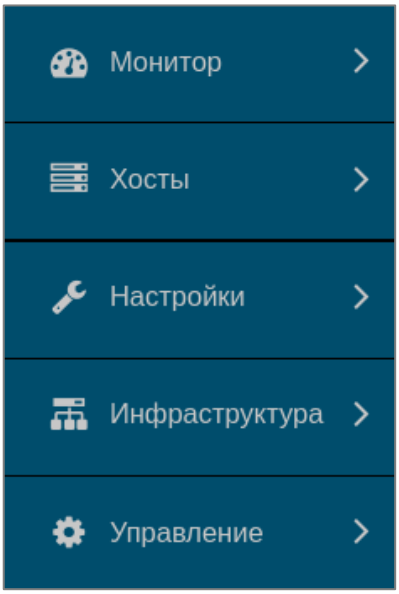

Рисунок 6 – Панель навигации

3.3. Регистрация существующих хостов в РОСА Центр Управления

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

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

- на хосте должны быть настроены источники пакетов, которые содержат пакеты `puppet-agent` и `salt-minion`;

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

- хосту должны быть доступны сетевые порты сервера РОСА Центр Управления и сервера СИПА, указанные в подразделе 2.2.

Примечание – При необходимости настройте для регистрируемых хостов правила автоподписывания сертификатов Puppet и Salt.

После подготовки хоста выполните вход в веб-интерфейс РОСА Центр Управления, где перейдите в меню “`Хосты → Зарегистрировать хост`” панели навигации для настройки параметров регистрации хоста.

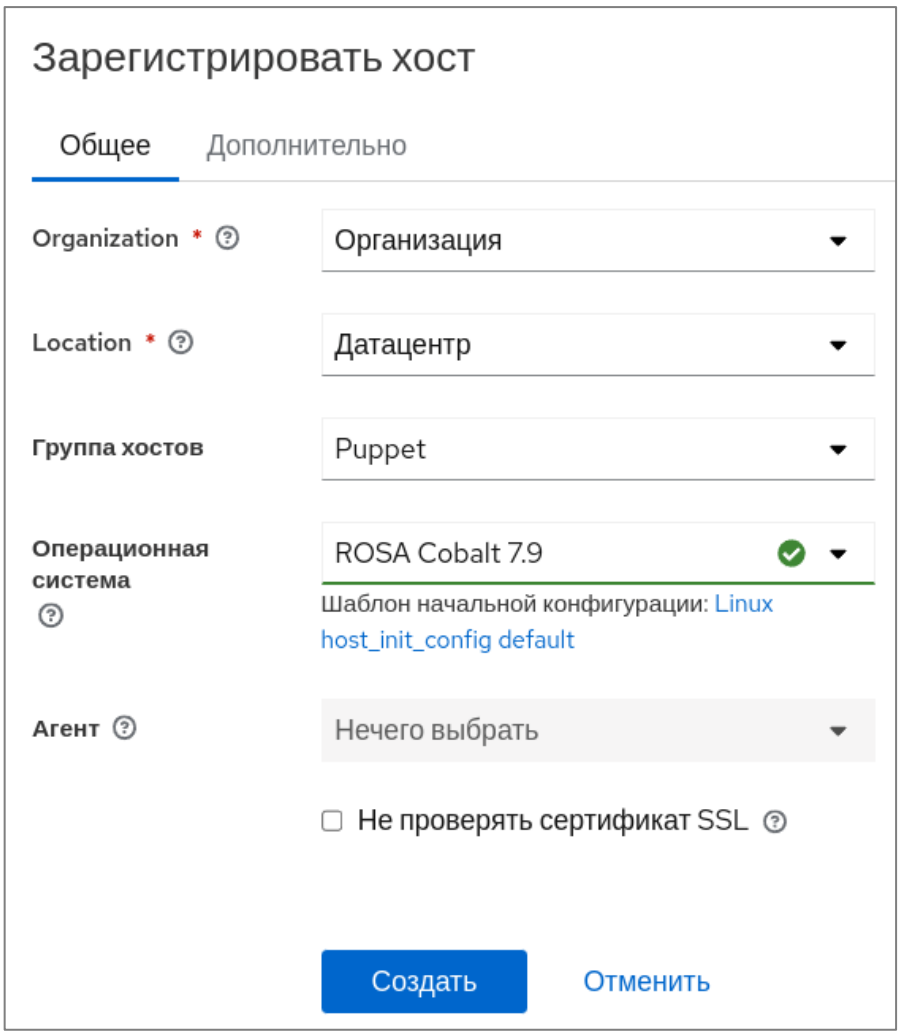

Рисунок 7 – Параметры регистрации хоста

В соответствующих списках выберите группу, в которую будет включен хост, затем выберите ОС, а остальные параметры регистрации хоста можно оставить со значениями по умолчанию.

Примечание – В случае использования самоподписанного сертификата ЦС Puppet установите флажок “Не проверять сертификат SSL”.

Обратите внимание, что выбор группы определяет конфигурацию хоста и настройки, которые будут применены к ОС. По умолчанию в РОСА Центр Управления доступны следующие группы хостов:

- Generic – содержит преднастроенные параметры сети, предоставляет функции дистанционного выполнения команд, скриптов, а также плейбуков (исполняемых сценариев) Ansible;

- Puppet – дополнительно устанавливает и настраивает Puppet на регистрируемом хосте;

- Salt – дополнительно устанавливает и настраивает Salt на регистрируемом хосте.

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 хост операционной системе, т.к. 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 нажмите кнопку Создать. В результате в текстовом поле под этой кнопкой появится созданная команда (скрипт регистрации).

Скопируйте эту команду и выполните в терминале ОС регистрируемого хоста.

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

Обратите внимание, что при выборе группы Puppet или Salt, и невыполненной настройке правила автоподписывания сертификата, процесс регистрации хоста прервется с сообщением о том, что клиентский сертификат был отправлен, но не был подписан. В этом случае, для завершения регистрации хоста выполните подписание сертификата вручную.

Для подписания сертификата Puppet перейдите в меню “Инфраструктура → Агенты Центра Управления” панели навигации веб-интерфейса РОСА Центр Управления, где нажмите наименование агента, которое соответствует доменному имени сервера РОСА Центр Управления, а затем перейдите на вкладку “ЦС Puppet → Сертификаты”. Найдите в появившемся списке наименование сертификата, которое соответствует доменному имени регистрируемого хоста, и нажмите кнопку Подписать напротив необходимого сертификата.

Подписание сертификата Salt осуществляется в терминале ОС сервера РОСА Центр Управления.

Для просмотра списка сертификатов выполните следующую команду:

```
salt-key -L
```

Для подписания сертификата выполните следующую команду, где укажите наименование необходимого сертификата:

```
salt-key -a <сертификат>
```

После подписания сертификата повторите выполнение скрипта регистрации в терминале ОС хоста.

3.4. Развертывание новых хостов под контролем РОСА Центр Управления

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

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

3.4.1. Подготовка к сетевому развертыванию хоста

Основная часть подготовки к сетевому развертыванию хоста выполняется автоматически программой установки РОСА Центр Управления. Тем не менее администратору комплекса необходимо выполнить следующие предварительные действия:

- зарегистрировать лицензионный ключ ОС РОСА “Кобальт”;

- подготовить установочный носитель ОС.

3.4.1.1. Регистрация лицензии ОС РОСА "Кобальт"

Лицензионный ключ ОС РОСА “Кобальт” вводится в глобальные параметры комплекса.

Для регистрации лицензии ОС выполните вход в веб-интерфейс РОСА Центр Управления, где перейдите в меню “`Настроить → Глобальные параметры`” панели навигации и выберите параметр “`rels 7 support id server`”. Затем введите лицензионный ключ в поле “`Значение`”, после чего нажмите кнопку `Принять` для сохранения настройки.

3.4.1.2. Подготовка установочного носителя ОС

Во время сетевой установки ОС используется копия установочного диска. Поэтому необходимо сделать содержимое этого диска доступным по протоколу HTTP. Для этого используйте любой имеющийся внутренний веб-сервер и скопируйте содержимое установочного диска в каталог, к которому веб-сервер имеет доступ на чтение. Далее, настройте виртуальный хост, разрешите строить и отображать автоматический индекс каталога. Проверьте при помощи браузера, что по адресу настроенного виртуального хоста отображается содержимое диска и файлы доступны для скачивания, после чего скопируйте URL из адресной строки браузера вместе с заголовком протокола (например, `http://files.company.ru/rosa_cobalt/`).

Для подготовки установочного носителя ОС выполните вход в веб-интерфейс РОСА Центр Управления, где перейдите в меню “`Хосты → Установочный носитель`” панели навигации и нажмите кнопку `Создать носитель`. Вставьте ранее скопированный URL в поле “`Путь`”. Затем введите краткое наименование носителя в поле “`Имя`” (например, `ROSA`

Enterprise Linux 7.9), в раскрывающемся списке “Семейство ОС” выберите значение “Red Hat”, после чего нажмите кнопку Принять.

Для завершения подготовки носителя перейдите в меню “Хосты → Операционные системы” панели навигации, чтобы настроить соответствие между носителем и типом используемой ОС. Выберите соответствующую ОС из списка (в данном случае, ROSA Enterprise Linux 7.9). Затем во вкладке “Установочный носитель” выберите в левом списке ранее созданный носитель ОС, который при этом будет перенесен в правый список, после чего нажмите кнопку Принять для сохранения настройки.

3.4.2. Параметры сетевого развертывания хоста

После регистрации лицензии и подготовки установочного носителя ОС выполните настройку параметров сетевого развертывания хоста. Для этого в веб-интерфейсе РОСА Центр Управления перейдите в меню “Хосты → Создать хост” панели навигации.

На экране появится интерфейс настройки, в котором параметры развертывания нового хоста распределены по вкладкам.

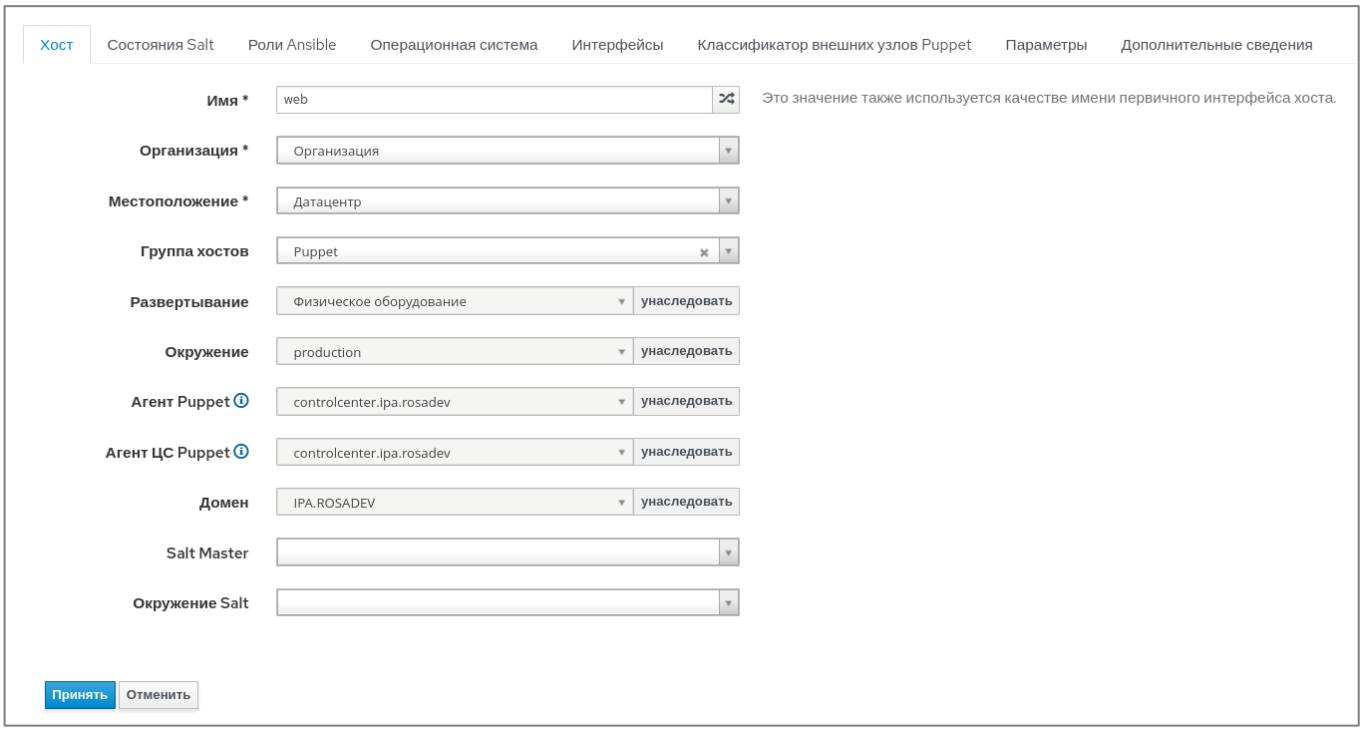

Рисунок 8 – Параметры сетевого развертывания хоста

Во вкладке “Хост” интерфейса настройки укажите имя хоста. Обратите внимание, что здесь указывается не полное доменное имя, а только непосредственно символьное имя хоста (например, backup или monitoring). Затем из раскрывающегося списка “Домен” выберите домен СИПА, в который РОСА Центр Управления может вводить хосты. В итоге полное доменное имя хоста будет составлено автоматически из символьного имени хоста и имени домена.

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

Следующие две вкладки предоставляют возможность задать состояния Salt и присвоить роли Ansible соответственно. Перед установкой ОС допускается оставить для этих параметров значения по умолчанию, так как настройки этих параметров можно изменить впоследствии.

Во вкладке “Операционная система” укажите значения для следующих обязательных параметров настройки:

- архитектура;

- ОС;

- установочный носитель;

- таблица разделов;

- пароль суперпользователя root.

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

Вкладка “Классификатор внешних узлов Puppet” позволяет назначить список модулей Puppet для выполнения на хосте. 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, т.е. параметры, которые влияют на генерируемые скрипты установки и настройки. При этом значения по умолчанию этих параметров согласованы с ОС РОСА “Кобальт” (или ОС ROSA Enterprise Server), поэтому рекомендуется оставить существующие значения без изменений.

После завершения настройки параметров развертывания нажмите кнопку Принять.

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

Включите хост, установите приоритет загрузки хоста по сети и дождитесь окончания процесса развертывания.

3.5. 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 выполните вход в веб-интерфейс РОСА Центр Управления, где перейдите в меню “Администрирование → Источники аутентификации” панели навигации, после чего нажмите кнопку Создать источник аутентификации LDAP.

На экране появится интерфейс настройки, в котором параметры подключения распределены по вкладкам.

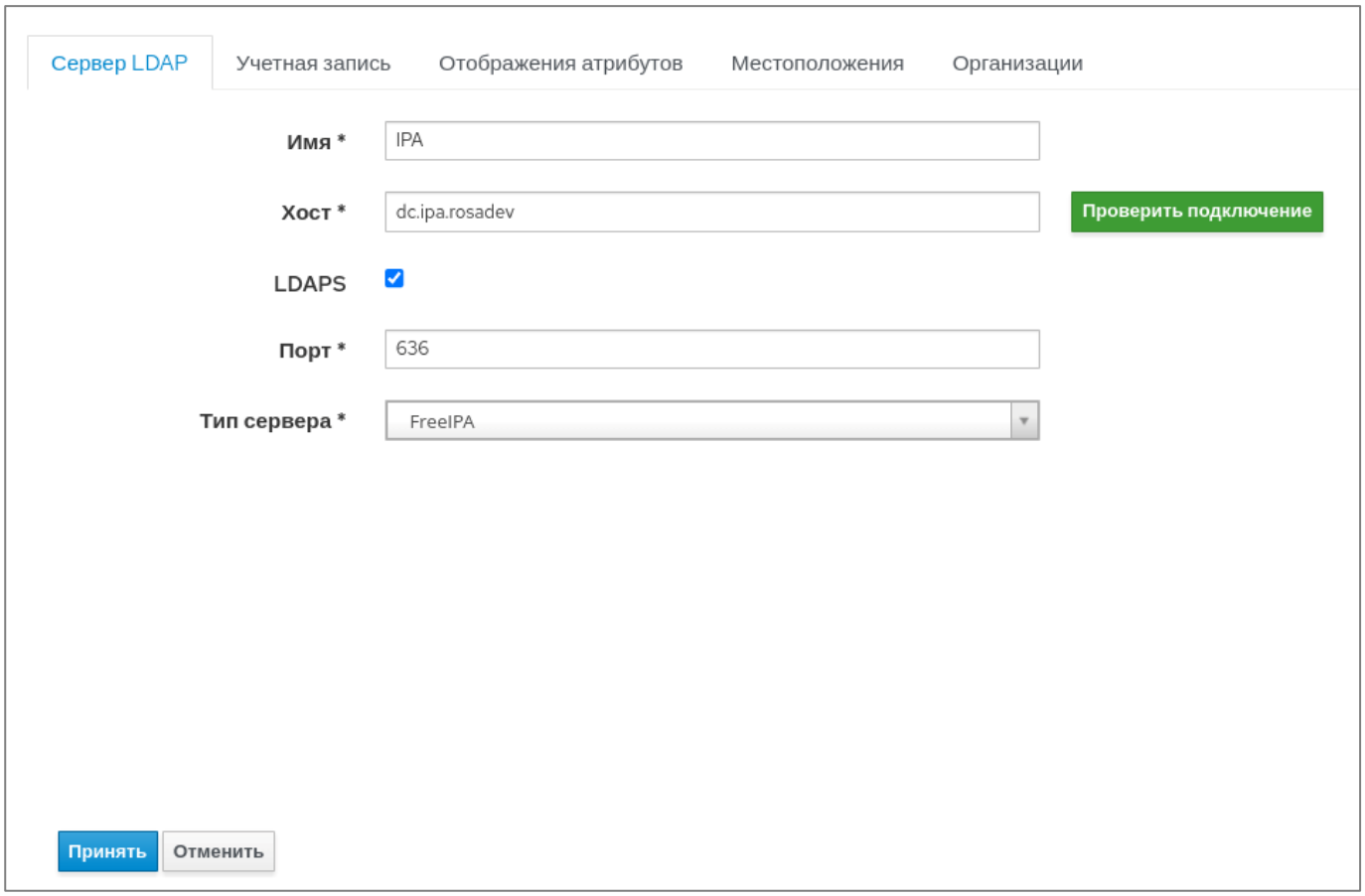

Рисунок 9 – Параметры подключения службы каталогов LDAP

Во вкладке “Сервер LDAP” интерфейса настройки укажите необходимые значения для следующих параметров подключения:

- Имя – краткое наименование подключаемой службы каталогов;

- Хост – 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 укажите значение FreeIPA.

После настройки этих параметров нажмите кнопку Проверить подключение. Если параметры сервера LDAP были указаны корректно, то проверка пройдет успешно. В противном случае внесите необходимые изменения в указанные значения этих параметров.

Во вкладке “Учетная запись” укажите 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 укажите отличительное имя для этой учетной записи (например, uid=ldapsearch, cn=users,cn=accounts,dc=company,dc=ru);

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

- Базовое отличительное имя – отличительное имя для записи каталога, которая содержит учетные записи пользователей (например, dc=company,dc=ru);

- Базовое отличительное имя групп – отличительное имя для записи каталога, которая содержит информацию о группах пользователей (например, cn=groups, cn=accounts,dc=company,dc=ru);

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

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

- Синхр. Usergroup – обязательно активируйте этот параметр, чтобы осуществлялась синхронизация групп пользователей РОСА Центр Управления и групп службы каталогов LDAP.

Во вкладке “Отображения атрибутов” не требуется дополнительная настройка параметров при подключении службы каталогов LDAP сервера СИПА.

Вкладки “Местоположения” и “Организации” позволяют ограничить доступ пользователей подключаемой службы каталогов только указанными местоположениями и организациями.

После завершения настройки параметров подключения нажмите кнопку Принять.

Обратите 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, перейдите в меню “Администрирование → Группы пользователей” панели навигации и нажмите 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.

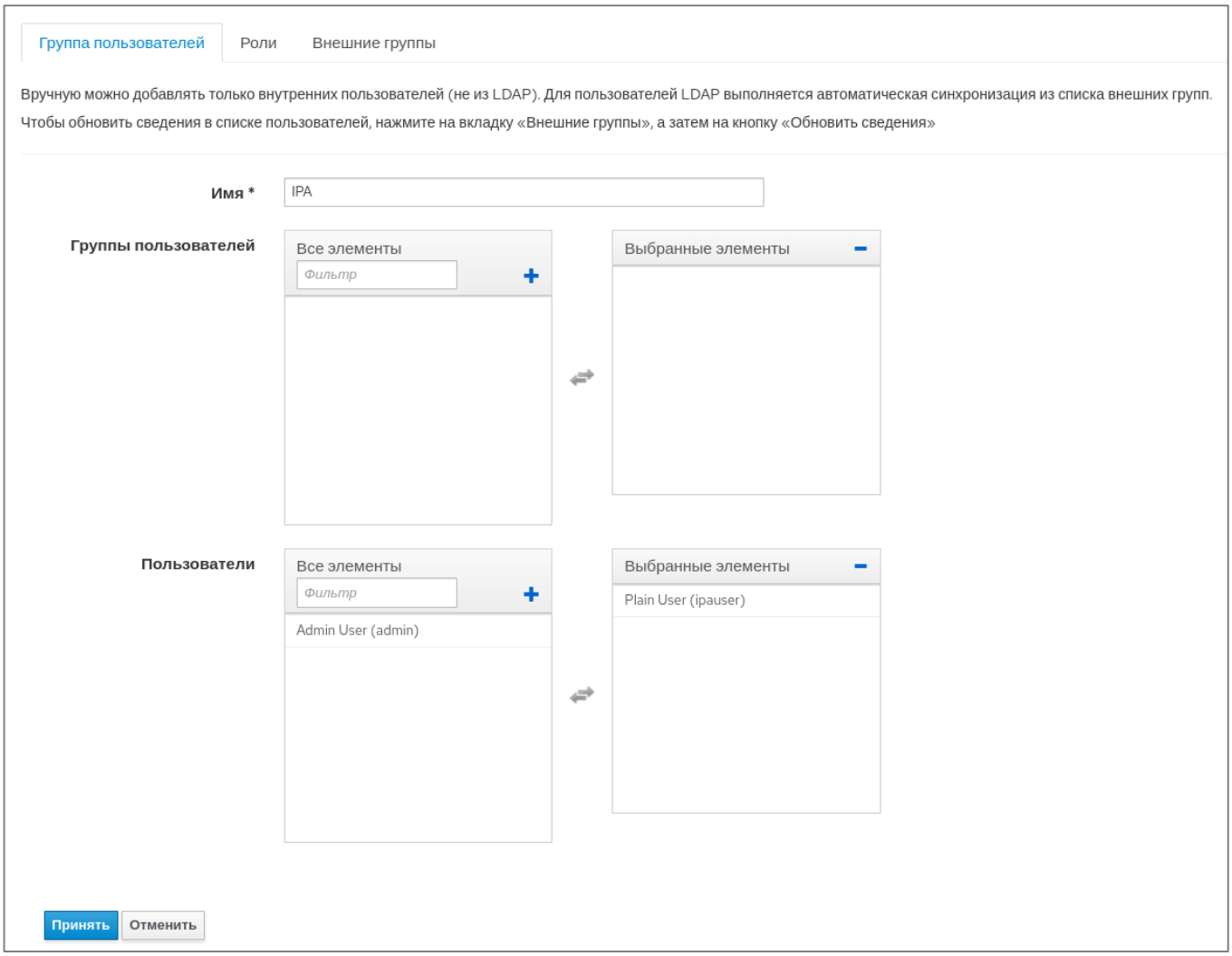

Рисунок 10 – Параметры группы пользователей

Во вкладке “Группа пользователей” интерфейса настройки укажите краткое наименование группы.

Во вкладке “Роли” присвойте этой группе пользователей необходимые роли в РОСА Центр Управления.

Во вкладке “Внешние группы” настройте 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, ранее присвоенными группе пользователей РОСА Центр Управления.

Для настройки необходимого соответствия между этими группами нажмите кнопку Добавить внешнюю группу пользователей и введите наименование нужной группы службы LDAP без атрибутов и в символьном виде (например, admins или users), после чего выберите из списка “Источник аутентификации LDAP” ранее подключенную службу каталогов.

После завершения настройки параметров группы пользователей нажмите кнопку Принять.

С целью проверки выполните вход в веб-интерфейс РОСА Центр Управления с реквизитами учетной записи внешнего пользователя из ранее выбранной и добавленной

группы службы каталогов LDAP и убедитесь, 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.

3.6. Подключение РОСА Центр Управления к внешней системе виртуализации

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

Для настройки подключения к внешней системе виртуализации выполните вход в веб-интерфейс РОСА Центр Управления, где перейдите в меню “Инфраструктура → Вычислительные ресурсы” панели навигации, после чего нажмите кнопку Создать вычислительный ресурс.

На экране появится интерфейс настройки, в котором параметры подключения распределены по вкладкам.

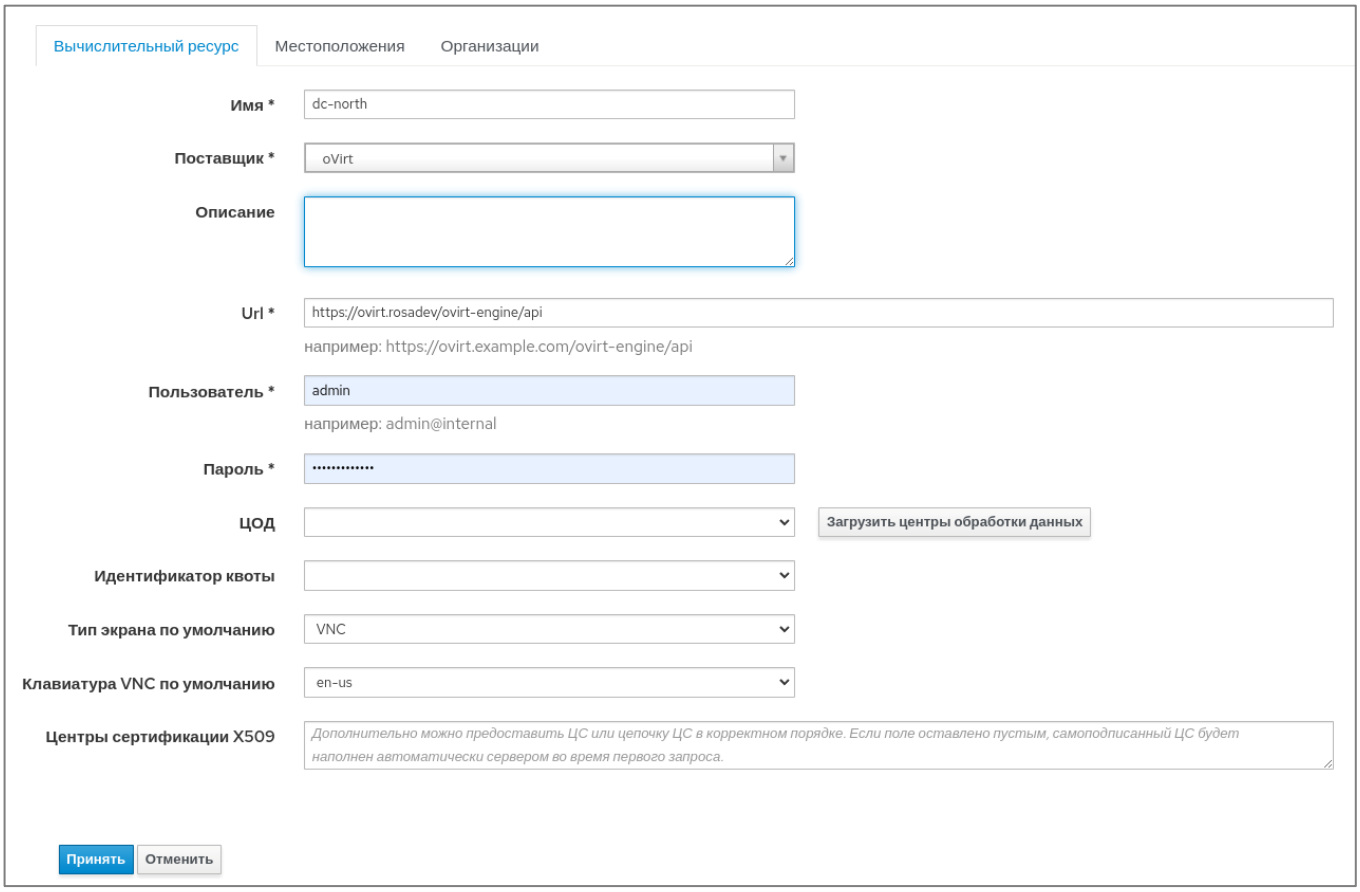

Рисунок 11 – Параметры подключения системы виртуализации

Во вкладке “Вычислительный ресурс” интерфейса настройки укажите необходимые значения для следующих параметров подключения:

- Имя – наименование подключаемой системы виртуализации;

- Поставщик – платформа виртуализации (ROSA Virtualization, VMware). В случае подключения к системе виртуализации ROSA Virtualization укажите значение oVirt;

- Описание – краткое описание подключаемой системы виртуализации;

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

- Пользователь – имя пользователя, имеющего права для управления ВМ, с указанием источника аутентификации (например, controlcenter@internal);

- Пароль – пароль пользователя.

После завершения настройки параметров подключения системы виртуализации нажмите кнопку Принять.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Определение
ВМ	Виртуальная машина
ИТ	Информационные технологии
ОС	Операционная система
ПО	Программное обеспечение
СИПА	Система идентификации, политик и аудита
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 хоста
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)
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

Лист регистрации изменений									
Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводит. докум. и дата	Подп.	Дата
Изм.	измененных	замененных	новых	аннулированных					