Документ

Черновик

2024-01-01

СОДЕРЖАНИЕ

1

НАЗНАЧЕНИЕ КОМПЛЕКСА

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 предоставляет пользователю следующие возможности для автоматизированного развертывания и конфигурирования управляемых узлов:

- осуществлять сетевое развертывание (установку ОС и настройку системной конфигурации управляемых узлов (физических серверов и рабочих станций, ВМ) в автоматическом режиме с применением сценариев развертывания Kickstart. При этом сетевое развертывание осуществляется на новых узлах без предустановленной ОС, а уже существующие узлы (ранее развернутые другим способом) могут быть зарегистрированы пользователем в РОСА Центр Управления в установленном порядке;
- осуществлять управление конфигурациями развернутых узлов. При этом состояние конфигурации узла автоматически корректируется согласно заданным параметрам. Кроме того, формируется соответствующая отчетность и сохраняется история изменений;
- использовать графический веб-интерфейс для централизованного мониторинга и конфигурирования управляемых узлов. При этом доступ пользователей к элементам интерфейса РОСА Центр Управления и к функциональным возможностям операционного управления узлами реализован с применением ролевой модели. Кроме того, Комплекс может быть интегрирован с внешней системой аутентификации пользователей

2

ФУНКЦИИ КОМПЛЕКСА

РОСА Центр Управления выполняет следующие функции:

- сбор сведений о первоначальной конфигурации аппаратной части узлов на момент установки клиентов;
- периодический опрос аппаратной части узлов с целью выявления изменений в составе и параметрах их аппаратной части;
- фиксация сведений об аппаратной части узлов в виде сохраняемых отчётов на дату опроса;
- хранение данных инвентаризации в течение не менее трех месяцев;
- настройка перечня инвентаризируемых аппаратных компонентов, а также их атрибутов;
- сбор перечня программного обеспечения;
- отображение сведений о программной части в виде отчётов с возможностью составления индивидуальных отчетов;
- сбор информации о файлах на локальных дисках узлов, подключенных к Комплексу;
- оценка соответствия параметров узлов заданным шаблонам конфигурации;
- отображение результатов оценки в консоли администрирования в виде отчетов;
- управление содержимым, включая базовую ОС, службы промежуточного ПО и приложения конечных пользователей;
- управление различными типами содержимого на каждом этапе жизненного цикла ПО;
- управление подписками для поиска, доступа и загрузки содержимого из соответствующи репозиториев;
- сбор информации об использовании программного обеспечения на основе информации о времени запуска и продолжительности работы исполняемых файлов приложений;
- хранение информации об использовании программного обеспечения;
- отображение собранной информации об использовании программного обеспечения в консоли администрирования в виде отчетов;
- доставка приложений или пакетов программного обеспечения до рабочих станций;
- запуск на рабочих станциях соответствующей программы установки для доставленного приложения или пакета программного обеспечения согласно заданному расписанию;
- отображение пользователям уведомлений об установке программного обеспечения и скрытие таких уведомлений при выполнении системных задач обслуживания;
- отображение и хранение сведений о процессе распространения программного обеспечения в виде отчётов с возможностью составления индивидуальных отчетов;
- установка операционной системы на узлы и серверы Комплекса;
- выполнение сценариев развертывания операционной системы на новых и используемых рабочих станциях;
- миграция узлов на отечественную операционную систему;
- контроль процесса выполнения сценария в виде отчётов;
- установка обновлений как на все узлы, так и отдельно для заданной группы узлов;
- отображение пользователям уведомлений об установке обновлений программного обеспечения и своевременного предупреждения о необходимости перезагрузки узла для завершения процесса установки;

— контроль процесса распространения обновлений в виде отчётов с возможностью составления индивидуальных отчетов;
— мониторинг и визуализация статусов сервисов компьютерной сети, серверов и сетевого оборудования ИТ-инфраструктуры;
— обеспечение работы подсистемы мониторинга;
— обеспечение работы подсистемы отображения;
— обеспечение работы подсистемы поиска и аналитики;
— управление мобильными устройствами на ОС “РОСА Мобайл”.

3

ОБЛАСТЬ ПРИМЕНЕНИЯ

РОСА Центр Управления может быть использован государственными и коммерческими средними предприятиями в первую очередь для централизованного управление жизненным циклом гибридной ИТ-инфраструктуры корпоративного уровня, включающей инфраструктуру физической, виртуальной и частной облачной среды.

Настоящее руководство предназначено для использования системным администратором, пользователем и специалистом по техническому обслуживанию.

Квалификация системного администратора: высокий уровень знаний и наличие практическо опыта выполнения работ по установке, настройке и администрированию программных средств, применяемых в Комплексе, а также наличие профессиональных знаний и практического опыта в области системного администрирования.

Основными обязанностями системного администратора являются:

1. установка, настройка и мониторинг работоспособности системного и базового программного обеспечения;
2. инсталляция и настройка прикладного программного обеспечения;
3. создание и изменение объектов службы каталогов;
4. создание и изменение объектов политик;
5. настройка локальной компьютерной сети и сетевого окружения;
6. контроль доступа к сетевым ресурсам.

Квалификация специалиста по техническому обслуживанию: высокий уровень знаний и наличие практического опыта выполнения работ по установке, настройке и подключению компьютерного и серверного оборудования, применяемого в Системе, а также наличие профессиональных знаний и практического опыта в области технического обслуживания.

Основными обязанностями специалиста по техническому обслуживанию являются:

1. модернизация, настройка и мониторинг работоспособности Комплекса технических средств (серверов, рабочих станций);
2. конфигурирование и настройка программно-технических средств Комплекса;
3. диагностика типовых неисправностей.

Пользователи должны обладать знаниями и навыками работы в качестве пользователя персональных компьютеров в соответствии с Приложением к приказу Мининформсвязи России от 27.12.2005 г. № 147 “Об утверждении квалификационных требований к федеральным государственным гражданским служащим и государственным гражданским служащим субъектов Российской Федерации в области использования информационных технологий”. Дополнительных требований к пользователям не предъявляется.

4

УСЛОВИЯ ПРИМЕНЕНИЯ

РОСА Центр Управления представляет собой клиент-серверное приложение и имеет взаимосвязанн модульную структуру, объединенную под единым графическим веб-интерфейсом.

Функциональная архитектура Комплекса состоит из сервера и как минимум одного агента.

Сервер является центральным компонентом РОСА Центр Управления, который обеспечивает функционирование веб-интерфейса Комплекса и управление конфигурациями развернутых узлов.

Агент является исполнительным компонентом РОСА Центр Управления, который реализует функции управления TFTP, DHCP, DNS, Puppet, Puppet CA и Ansible.

Таким образом, агент помогает серверу оркестрировать процессы сетевого развертывания управляемых узлов. При этом агент функционирует только в своей выделенной локальной подсети.

Примечание – В процессе типовой установки Комплекса осуществляется развертывание сервера и одного агента с полным набором функций управления непосредственно на узле РОСА Центр Управления.

Взаимодействие Комплекса со службой каталогов осуществляется на уровне доменных пользователей и групп.

5

ПЕРЕЧЕНЬ ДОКУМЕНТАЦИИ

Для эксплуатации структурных компонентов Комплекса следует ознакомиться со следующей документацией, относящейся к программному обеспечению:

- официальная документация по продуктам РОСА;
- официальная документация по FreeIPA;
- официальная документация по Ansible;
- официальная документация по Puppet;
- официальная документация по Zabbix;
- официальная документация по Grafana;
- официальная документация по OpenSearch.

6

СТРУКТУРА КОМПЛЕКСА

Комплекс включает в себя следующие основные структурные компоненты:

- подсеть;
- домен;
- настроенная и подготовленная к сетевой установке на управляемых узлах операционная система РОСА “Хром” (или ROSA Enterprise Linux Server);
- примеры групп узлов;
- настроенные ассоциации шаблонов развертывания;
- сервер Puppet;
- Ansible;
- плагин Katello;
- плагины управления вычислительными ресурсами систем виртуализации ROSA Virtualization, VMWare и Libvirt.

7

УСТАНОВКА И НАСТРОЙКА КОМПЛЕКСА

Установка и настройка РОСА Центр Управления описаны в документе “Платформа централизованно управления жизненным циклом операционных систем”РОСА Центр Управления”. Руководство системного администратора. Часть 1. Установка и настройка” (шифр РСЮК.10121-09 32 01).

8

ИНТЕРФЕЙС КОМПЛЕКСА

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

9

ДОСТУП ПОЛЬЗОВАТЕЛЕЙ И НАВИГАЦИЯ ПО ИНТЕРФЕЙСУ

Доступ к веб-интерфейсу РОСА Центр Управления осуществляется пользователем 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.

Для доступа к веб-интерфейсу РОСА Центр Управления необходимо ввести в адресной строке браузера доменное имя сервера РОСА Центр Управления, например:

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

На экране появится страница авторизации веб-интерфейса (рисунок 1).

9.1 ::sign-image

src: /image2.png sign: Рисунок 1 — Страница авторизации РОСА Центр Управления — ::

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

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 пользовател 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 2).

Схематичное расположение панелей интерфейса:

1 – Панель навигации;

2 – Панель быстрого доступа;

3 – Рабочая область.

9.2 ::sign-image

src: /image3.png sign: Рисунок 2 — Интерфейс РОСА Центр Управления — ::

Для последующего перемещения по страницам интерфейса РОСА Центр Управления используются требуемые пункты меню панели навигации (рисунок 3).

9.3 ::sign-image

src: /image4.png sign: Рисунок 3 — Панель навигации — ::

Пользовательский интерфейс выбранного пункта панели навигации отображается в рабочей области.

> Примечание – Для увеличения размера отображаемой рабочей области интерфейса можно свернуть панель навигации нажатием на пиктограмму в левом верхнем углу страницы.

Для удобной навигации по пунктам меню можно воспользоваться механизмом быстрого поиска “Найти и перейти” в верхней части панели навигации. При наборе текста в поле появляется перечень пунктов меню по найденному контексту, при нажатии на которые осуществляется быстрый переход к соответствующей рабочей области (рисунок 4).

9.4 ::sign-image

src: /image5.png sign: Рисунок 4 — Поиск пунктов меню — ::

Панель быстрого доступа содержит функциональные пиктограммы (звонок) и (пользовател которые при нажатии обеспечивают просмотр полученных оповещений о контролируемых событиях РОСА Центр Управления (пункт Оповещения о событиях) и доступ в меню учетной записи текущего пользователя Комплекса соответственно.

Для управления содержанием рабочей области используется кнопка , с помощью которой можно задавать перечень колонок таблицы для отображения данных.

10

ПОИСК ОБЪЕКТОВ

Интерфейс РОСА Центр Управления предоставляет пользователю возможность осуществления точного и гибкого поиска различных объектов.

Поле “Поиск” доступно на каждой странице интерфейса, при этом атрибуты поиска варьируются в зависимости от контекста этой страницы (рисунок 5).

10.1 ::sign-image

src: /image8.png sign: Рисунок 5 — Поле “Поиск” — ::

Поисковый запрос в РОСА Центр Управления может представлять собой как простой текстовый запрос, так и сложный запрос, созданный с использованием специальных операторов и символов.

Для выполнения процедуры поиска необходимо ввести текст запроса в поле “Поиск”, после чего нажать клавишу `Enter`.

> Примечание – Интерфейс РОСА Центр Управления поддерживает функцию автодополнения поисковых запросов, когда при вводе текущего запроса отображается список возможных вариантов его продолжения. При этом пользователь может выбрать предложенный вариант запроса из списка или продолжить вводить собственный запрос вручную.

Например, простой текстовый запрос rosa, выполненный в поисковом поле вкладки “Узлы”, вернет список всех узлов, содержащих указанное значение в наименовании узла или ОС, а также в комментарии (кратком описании узла).

В сложных поисковых запросах могут использоваться операторы сравнения = (равно), != (не равно), > (больше), < (меньше), а также операторы AND (логическое И) и OR (логическое ИЛИ) для выполнения поиска сразу по нескольким критериям.

Например, запрос “Группа узлов = Puppet AND Владелец != Администратор” вернет список всех узлов из группы Puppet, владельцем которых не является администратор.

Также в запросах может использоваться маска подстановки *, которая предназначена для замены последующих символов.

Например, запрос cob* вернет в качестве результата поиска варианты cobra, cobalt, cobain и тому подобные.

Кроме того, в поисковых запросах допускается указывать различные форматы даты и времени: 20 минут назад, 4 часа назад, вчера, сегодня, 3 недели назад, 8 месяцев назад, 17 июня и тому подобные.

Для типовых и часто используемых запросов интерфейс РОСА Центр Управления предоставляет пользователю возможность создания и применения закладок. При применении закладки осуществляется быстрый переход к выполнению предопределенных условий поиска.

Для сохранения текущего поискового запроса в качестве закладки нажимают пиктограмму (закладка) справа от поля “Поиск”.

Для использования закладки, ранее созданной пользователем, или закладки, предоставляем в РОСА Центр Управления по умолчанию, следует нажать на пиктограмму (раскрыть) справа от поля “Поиск”, после чего выбрать из раскрывающегося списка необходимую закладку.

Примечание – Дополнительное управление закладками осуществляется в меню “Управление Закладки” панели навигации.

11

АВТОРИЗАЦИЯ В КОМПЛЕКСЕ

Авторизация в Комплексе осуществляется с использованием механизмов службы каталогов, для чего существует возможность сопоставления группам пользователей Комплекса доменных групп пользователей службы каталогов, используя механизм внешних источников аутентификации и внешних групп пользователей. При этом для внешних источников аутентификации возможно назначение выбранных организаций и местоположений, а для внешних групп пользователей – настройка ролей.

Перед началом интеграции со службой каталогов рекомендуется создать в интерфейсе Комплекса локального пользователя с именем, несовпадающим ни с одним из имен пользователей службы каталогов, и сложным паролем, назначив при этом ему максимальные права администрато Данный шаг позволит произвести отмену изменений в случае некорректной настройки источника аутентификации.

Для создания локального пользователя необходимо перейти в пункт основного меню “Управление Пользователи” и в рабочей области нажать кнопку . Далее в соответствии с рисунком 6:

1. заполнить поля “Имя пользователя” и “Почта” на вкладке “Пользователь”;
2. выбрать тип авторизации в выпадающем списке “Авторизован” – “INTERNAL” – и задать пароль, введя его дважды в полях “Пароль” и “Подтверждение”;
3. включить параметр в поле “Почта включена” на вкладке “Настройки электронной почты”;
4. на вкладке “Роли” добавить роль “Управление” в поле “Выбранные элементы”, нажав пиктограмму (плюс);
5. нажать кнопку .

11.1 ::sign-image

src: /image12.png sign: Рисунок 6 — Создание локального пользователя с правами администратора — ::

12

ПРАВИЛА ВЫПОЛНЕНИЯ ОПЕРАЦИЙ

В разделах начиная с “Администрирование” по “Наблюдение и оповещение” приведены операции, обеспечивающие функционал Комплекса в соответствии с правами пользователей, предоставленными ролевой моделью.

Администратор Комплекса обладает полными правами на выполнение операций.

Условиями, при соблюдении которых возможно выполнение операции, являются наличие соответствующих прав пользователя на операцию.

Подготовительным действием для выполнения всех операций является авторизация пользователя в домене.

Основные действия при выполнении операций описаны в требуемой для корректного результата последовательности.

Заключительным действием для каждой операции является закрытие интерфейсного окна рабочей области операции с сохранением или без сохранения данных.

В результате выполнения операций появляются всплывающие сообщения зеленого цвета, например, как на рисунке 7, в случае успешного завершения или красного – при возникновении ошибки. Сообщение можно закрыть, нажав на пиктограмму (крест).

12.1 ::sign-image

src: /image14.png sign: Рисунок 7 — Сообщение о результате операции — ::

13

ОРГАНИЗАЦИИ

Организации разделяют ресурсы РОСА Центр Управления на логические группы на основе владения, назначения, содержимого, уровня безопасности или подразделений. Пользователю предоставлена возможность создавать несколько организаций и управлять ими с помощью Комплекса, а затем разделять и назначать подписки каждой отдельной организации. Это обеспечивает метод управления содержимым для нескольких отдельных организаций в рамках одной системы управления. Возможные варианты использования Комплекса для организаций:

- Единая организация – Использование одной организации хорошо подходит для малого бизнеса с простой цепочкой системного администрирования. В этом случае создается единая организация для бизнеса и ей назначается содержимое. Для этой цели также можно использовать “Организацию по умолчанию”.
- Несколько организаций – Использование нескольких организаций хорошо подходит для крупной компании, которая владеет несколькими небольшими бизнес-единицами, например, компания с отдельными группами системного администрирования и разработки ПО. В этом случае создается одна организация для компании, а затем по одной организации для каждой из принадлежащих ей бизнес-единиц. Затем назначается содержимое каждой организации в зависимости от ее потребностей.
- Внешние организации – Использование внешних организаций хорошо подходит для компании, которая управляет внешними системами для других организаций, например, компания, предлагающая клиентам ресурсы облачных вычислений и веб-хостинга. В этом случае создается организация для собственной системной инфраструктуры компании, а затем организация для каждого внешнего бизнеса. Затем назначается содержимое каждой организации, где это необходимо.

Для создания новой организации нужно перейти в меню “Управление Организации” и нажать кнопку . Далее необходимо в полях ввода задать наименование и описание организации. Нажать кнопку и перейти к редактированию для задания содержимого (рисунок 8).

13.1 ::sign-image

src: /image15.png sign: Рисунок 8 — Изменение организации — ::

14

МЕСТОПОЛОЖЕНИЯ

В РОСА Центр Управления местоположения функционируют аналогично организациям, но местоположения предоставляют метод группировки ресурсов и назначения узлов. Местоположени имеют следующие концептуальные различия от организаций:

— основаны на физических или географических условиях;
— имеют иерархическую структуру.

Для создания нового местоположения нужно перейти в меню “Управление Местоположени и нажать кнопку . Далее необходимо в полях ввода задать наименование и описание нового местоположения, а также выбрать в списке “Родитель” вышестоящее местоположе в иерархической структуре. Нажать кнопку и перейти к редактированию для задания содержимого (рисунок 9).

14.1 ::sign-image

src: /image16.png sign: Рисунок 9 — Изменение местоположения — ::

15

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 У через внешнюю службу каталогов.

Для настройки подключения к службе каталогов LDAP нужно перейти в меню “Управление Источники аутентификации” панели навигации и нажать кнопку LDAP.

На экране появится интерфейс настройки, в котором параметры подключения распределены по вкладкам (рисунок 10).

15.1 ::sign-image

src: /image17.png sign: Рисунок 10 — Параметры подключения службы каталогов LDAP — ::

Во вкладке “LDAP-сервер” 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 требуется нажать кнопку . 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. Пользователь с этой учетной записью может подключаться к службе каталогов и выполнять запросы поиска учетных записей требуемых пользователей в каталоге в процессе аутентификации. В качестве значения указывают отличительное имя для этой учетной записи (например, uid=ldapsearch, cn=users, cn=accounts, dc=rosa, dc=int);
- Пароль – пароль пользователя, используемый для первоначального подключения к службе каталогов;
- Базовое DN – отличительное имя для записи каталога, которая содержит учетные записи пользователей (например, dc=rosa, dc=int);

— Базовый DN группы – отличительное имя для записи каталога, которая содержит информацию о группах пользователей (например, cn=groups, cn=accounts, dc=rosa, dc=int);
— Использовать сетевые группы – при активации будут использованы сетевые группы NIS вместо групп Posix;
— Фильтр LDAP – правило фильтрации учетных записей пользователей службы каталогов (при необходимости);
— 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 – для синхронизации групп пользователей РОСА Центр Управления и групп службы каталогов LDAP этот параметр активируется в обязательном порядке.

Во вкладке “Атрибуты” не требуется дополнительная настройка параметров при подключени 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 нажимают кнопку .

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 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 11).

15.2 ::sign-image

src: /image18.png sign: Рисунок 11 — 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 следует нажать кнопку и ввести наименование нужной группы службы LDAP без атрибутов и в символьном виде (например, admins или users), после чего выбрать из списка “Источник аутентификации LDAP” ранее подключенную службу каталогов.

После завершения настройки параметров группы пользователей нужно нажать кнопку .

С целью проверки выполняют вход в веб-интерфейс РОСА Центр Управления с реквизитами учетной записи внешнего пользователя из ранее выбранной и добавленной группы службы каталогов LDAP для того, чтобы 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.

Управление учетными записями внешних пользователей осуществляется в домене службы каталогов. Механизм управления описан в документации на службу каталогов (пункт Перечень документации настоящего руководства).

16

РОЛЕВАЯ МОДЕЛЬ ПОЛЬЗОВАТЕЛЕЙ

В РОСА Центр Управления реализована ролевая модель пользователей.

Роли можно создавать, удалять и редактировать на странице “Управление Роли”. Каждая роль содержит фильтры разрешений, которые определяют действия, разрешенные для пользователя (рисунок 12).

16.1 ::sign-image

src: /image19.png sign: Рисунок 12 — Настройка ролей пользователей — ::

При создании роли можно привязать ее к местонахождению и организации, определить фильтры, а после создания роли – с одним или несколькими пользователями, а также группами пользователей.

Встроенная системная роль “Default role” (“Роль по умолчанию”) представляет собой набор разрешений, который будет предоставлен каждому пользователю в дополнение к уже имеющимся у него ролям.

Кроме того, имеется возможность создания собственных ролей на основе уже имеющихся посредством их клонирования и редактирования.

Интерфейс содержит набор базовых ролей, которые распределяются между пользователями но не могут быть изменены. Базовые роли включают в себя достаточный набор настроек по умолчанию и в большинстве случаев удовлетворяют требованиям пользователя Комплекса с правами:

- “System admin (системный администратор)” – это базовая роль с широкими возможностя на управление организациями, местоположениями, пользователями, группами пользователей, источниками авторизации, ролями, фильтрами и настройками с доступом ко всем ресурсам. Цель этой роли – настроить среду для использования другими пользователями. Администратор может создавать организации/местоположен но не имеет доступа к ресурсам внутри них. Системный администратор может создавать новых пользователей, назначать их местоположениям/организациям и добавлять пользователям роли. Системный администратор может просматривать и редактировать настройки. Также пользователи с этой ролью могут делегировать роли, которыми они сами не владеют;
- “Ansible Roles Manager (менеджер ролей Ansible)” – на управление ролями Ansible;
- “Ansible Tower Inventory Reader (проверка инвенторий Ansible Tower)” – на проверку позиций динамических инвенторий Ansible Tower;
- “Auditor (аудитор)” – на просмотр только журнала аудита и ничего больше;
- “Bookmarks manager (менеджер закладок)” – на управление закладками поиска и на обновление всех общедоступных закладок;
- “Content Exporter (экспортер содержимого) – на экспорт представлений содержимого в организации;
- “Content Importer (импортер содержимого)” – на импорт представлений содержимого в организации;

— Discovery Manager (менеджер обнаружения) – на проведение обнаружения хостов;
— Discovery Reader (просмотр обнаружения) – на просмотр обнаруженных хостов;
— “Edit hosts (редактирование роли узлов)” – на обновление узлов;
— “Edit partition tables (редактирование таблиц разделов)” – на редактирование таблиц разделов;
— “Manager (менеджер)” – на все доступные разрешения (аналогично администратору, но за исключением изменения настроек);
— “Organization admin (администратор организации)” – на все разрешения, за исключением управления организациями;
— “Remote Execution Manager (менеджер удаленного выполнения)” – на управление шаблонами заданий, функциями удаленного выполнения, отмену заданий и просмотр журналов аудита;
— “Remote Execution User Роль (пользователь удаленного выполнения)” – на выполнение заданий удаленного выполнения на узлах;
— “Site manager (менеджер сайта)” – на просмотр и для управления узлами в инфраструктуре
— “Tasks Manager (диспетчер процессов)” – на проверку, отмену, возобновление и разблокировку процессов;
— “Tasks Reader (проверка процессов)” – на проверку процессов;
— “Viewer (просмотр)” – только на чтение;
— “View hosts (просмотр узлов)” – только на просмотр узлов.

17

ЗАКЛАДКИ

Редактирование и удаление ранее созданных закладок в рабочих областях интерфейса Комплекса осуществляется в меню “Управление Закладки” (рисунок 13)

17.1 ::sign-image

src: /image20.png sign: Рисунок 13 — Работа с закладками — ::

По нажатии на имени закладку можно провести ее редактирование, а при нажатии на кнопку в столбце “Действия” – ее удаление после подтверждения.

18

ФУНКЦИИ УДАЛЕННОГО ВЫПОЛНЕНИЯ

В РОСА Центр Управления реализованы функции удаленного выполнения заданий на узлах, которые привязаны к шаблонам заданий.

Привязка осуществляется в меню “Управление Функции удаленного выполнения”. Для редактирования функции необходимо выбрать ее из перечня и в поле “Шаблон задания” определить соответствующее задание (рисунок 14). Далее нажимают кнопку для сохранения функции.

18.1 ::sign-image

src: /image21.png sign: Рисунок 14 — Редактирование функции удаленного выполнения — ::

Работа с шаблонами заданий осуществляется через меню “Узлы Шаблоны Шаблоны заданий” (рисунок 15).

18.2 ::sign-image

src: /image22.png sign: Рисунок 15 — Шаблоны заданий — ::

В рабочей области для создания нового шаблона нужно нажать кнопку . Аналогичное окно редактирования уже существующего шаблона открывают нажатием на имени шаблона. В окне редактирования на вкладках “Шаблон”, “Входные параметры”, “Задание” и “Тип” необходимо ввести скрипт сценария и значения полей для формирования задания. Запуск задания на выполнение осуществляется кнопкой в столбце “Действия” перечня шаблонов заданий.

19

ПОДКЛЮЧЕНИЕ КОМПЛЕКСА 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.

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

Для настройки подключения к внешней системе виртуализации надо перейти в меню “Инфраструктура Вычислительные ресурсы” панели навигации и нажать кнопку

.

На экране появится интерфейс настройки, в котором параметры подключения распределены по вкладкам (рисунок 16).

19.1 ::sign-image

src: /image23.png sign: Рисунок 16 — 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 .

20

НАСТРОЙКА ИСХОДЯЩЕЙ ПОЧТЫ

Для рассылки сообщений пользователям по электронной почте сервер РОСА Центр Управления должен быть интегрирован с внешним почтовым SMTP-сервером или настроен в качестве локального почтового агента MTA (например, sendmail).

> Примечание – Используемые адреса электронной почты должны быть указаны в учетных записях пользователей Комплекса.

20.1 Подключение Комплекса к внешнему почтовому серверу

Для подключения РОСА Центр Управления к внешнему почтовому SMTP-серверу необходимо перейти в меню “Управление Параметры” панели навигации и во вкладке “Email” указать необходимые значения для следующих параметров (рисунок 17):

- Способ доставки – способ рассылки исходящих сообщений по электронной почте. Возможные значения: sendmail (значение по умолчанию) или SMTP. В случае подключения к внешнему почтовому серверу указывают значение SMTP;
- Адрес SMTP – доменное имя или IP-адрес узла SMTP-сервера;
- Порт SMTP – номер порта SMTP-сервера;
- Аутентификация SMTP – протокол аутентификации, используемый при внешних соединениях с SMTP-сервером в процессе отправки сообщений. Возможные значения: plain, login, cram-md5 или none (не использовать протокол аутентификации). Значение none является значением по умолчанию. В случае использования протокола аутентификации указывают необходимые значения для следующих параметров:
- Имя пользователя SMTP – имя пользователя для идентификации на SMTP-сервере;
- Пароль SMTP – пароль пользователя для аутентификации на SMTP-сервере;
- Префикс темы сообщений – префикс для отображения в поле “Тема” у исходящих сообщений. Рекомендуемое значение: РОСА Центр Управления.

20.2 ::sign-image

src: /image24.png sign: Рисунок 17 — Настройка почты SMTP — ::

20.3 Настройка локального почтового агента

Для настройки локального почтового агента MTA нужно перейти в меню “Управление Параметры” панели навигации и во вкладке “Email” указать необходимые значения для следующих параметров (рисунок 18):

- Метод доставки – способ рассылки исходящих сообщений по электронной почте. Возможные значения: sendmail (значение по умолчанию) или smtp. В случае настройки локального почтового агента используют значение sendmail;

— Расположение Sendmail – путь к программе (исполняемому файлу) локального почтового агента MTA. Значение по умолчанию: `/usr/sbin/sendmail`;
— Аргументы Sendmail – аргументы (опции), которые используются при запуске локального почтового агента MTA. Значение по умолчанию: `-i`;
— Префикс темы сообщений – префикс (приставка) для отображения в поле “Тема” у исходящих сообщений. Рекомендуемое значение: РОСА Центр Управления.

20.4 ::sign-image

src: /image25.png sign: Рисунок 18 — Настройка почты локального агента — ::

21

УПРАВЛЕНИЕ УЗЛАМИ

Управление узлами осуществляется пользователем Комплекса через пункт меню “Узлы Все Узлы” панели навигации (рисунок 19).

21.1 ::sign-image

src: /image26.png sign: Рисунок 19 — Вкладка “Узлы” — ::

В рабочей области “Узлы” отображается перечень узлов, которые уже находятся под контролем РОСА Центр Управления. Каждый управляемый узел представлен в виде отдельной строки в общем перечне.

Краткая информационная сводка по каждому узлу содержит индикатор общего статуса узла, доменное имя узла, наименование окружения Puppet, тип ОС, имя владельца и группы узла, время последнего отчета.

Общий статус узла определяется суммарным состоянием процессов первичного развертыва и последующего конфигурирования узла, при этом индикатор общего статуса может принимать следующие значения:

- узел функционирует под контролем РОСА Центр Управления в штатном режиме и какие-либо предупреждения отсутствуют - {pictogram}
- узел функционирует под контролем РОСА Центр Управления в штатном режиме, но есть предупреждения от отдельных модулей Комплекса - {pictogram}
- узел функционирует под контролем РОСА Центр Управления, произошел сбой (ошибка) - {pictogram}

При наведении курсора “мыши” на этот индикатор появится всплывающее сообщение с дополнительными сведениями о причинах, которые вызвали сбой (ошибку) или появление предупреждения.

Для получения дополнительной информации об узле нужно нажать наименование (доменное имя) узла, чтобы перейти на отдельную страницу с подробными параметрами узла, на которой эти параметры представлены в текстовом и графическом виде и распределены по различным блокам и вкладкам (рисунок 20).

Настройка длительности тайм-аута обновления статуса узла осуществляется в окне основного меню “Управление Параметры” через параметр “Интервал потери синхронизации”, значение которого задается в минутах.

21.2 ::sign-image

src: /image30.png sign: Рисунок 20 — Параметры узла — ::

> Примечание – 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 Комплекса добавить параметр remote_execution_ssh_port, в значении которого указать используемый номер порта для каждого такого узла.

22

РАЗВЕРТЫВАНИЕ НОВЫХ УЗЛОВ

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.

22.1 Подготовка установочного носителя

Дополнительная подготовка источников установки для ОС проводится по следующим сценариям:

1. ROSA Chrome/Fresh;

   Источники установки формируются аналогично для дистрибутивов:

   — ROSA Chrome Desktop 12.4, platform 2021.1;
   — ROSA Chrome Server 12.4, platform 2021.1;
   — ROSA Fresh Desktop 12.4, platform 2021.1;
   — ROSA Fresh Server 12.4, platform 2021.1.

   Необходимо скачать и распаковать полученный образ дистрибутива. В распакованном каталоге образа создать каталог для файлов загрузки:

   ```
   bash Terminal mkdir -p ./images/pxeboot
   ```

   Далее скопировать файлы для загрузки:

   ```
   bash Terminal cp ./initrd0.img ./images/pxeboot/initrd.img cp ./vmlinuz0 ./images/p
   ```

2. Astra Linux 1.7;

   Необходимо скачать и распаковать полученный образ дистрибутива. В распакованном каталоге образа создать каталог для файлов загрузки:

   ```
   bash Terminal mkdir -p ./dists/stable/main/installer-amd64/current/images/netboot/d
   ```

   Затем скопировать файлы для загрузки:

   ```
   bash Terminal cp ./netinst/initrd.gz ./dists/stable/main/installer-amd64/current/im
cp ./netinst/linux ./dists/stable/main/installer-amd64/current/images/netboot/debian-inst
   ```

3. ALT Linux P10;

   Источники установки формируются аналогично для дистрибутивов:

   — ALT Workstation 10.1 (Autolycus);
   — ALT Workstation K 10.2 (Sorbaronia Mitschurinii).

   Необходимо скачать и распаковать полученный образ дистрибутива. В распакованном каталоге образа создать каталог для файлов загрузки:

```
bash Terminal mkdir -p ./syslinux/alt0
```

Затем скопировать файлы для загрузки:

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

Перейти в каталог для установки:

```
bash Terminal cd ./Metadata
```

Создать каталоги для скриптов установки:

```
bash Terminal mkdir -p ./install-scripts/postinstall.d mkdir -p ./install-scripts/p
```

Создать файл ./install-scripts/postinstall.d/99_grub_install.sh для установки загрузчика:

```
bash Terminal #!/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.dev
cat > /mnt/destination/tmp/grub_install.sh << EOF #!/bin/bash device=\`cat /tmp/grub_inst
LC_ALL=C /usr/sbin/grub-install --boot-directory=/boot \${device} LC_ALL=C /usr/sbin/upda
systemctl enable sshd systemctl enable puppet EOF chmod +x /mnt/destination/tmp/grub_inst
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
```

Создать права на исполнение скрипта:

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

Создать архив с установочными скриптами:

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

После создания архива удалить каталог подготовки скриптов:

```
bash Terminal rm -rf ./install-scripts
```

22.2 Подготовка к сетевому развертыванию узла на других ОС

22.2.1 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 PXE в верхнем правом углу в появившемся модальном окне нажать на кнопку .

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 21).

22.3 ::sign-image

src: /image31.png sign: Рисунок 21 — Изменение параметра — ::

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 22).

22.4 ::sign-image

src: /image32.jpg sign: Рисунок 22 — Меню загрузки ВМ — ::

После успешной загрузки по сети на экран будет выведено окно (рисунок 23).

22.5 ::sign-image

src: /image33.png sign: Рисунок 23 — Результат успешной загрузки — ::

Далее в меню “Узлы Обнаруженные узлы” в рабочей панели должен появиться обнаруженный узел (рисунок 24).

Для процедуры сетевой установки следует нажать кнопку .

22.6 ::sign-image

src: /image34.png sign: Рисунок 24 — Обнаруженные узлы — ::

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

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

22.6.1 Установка ОС на узле с автоматическим развертыванием

Для включения в процедуру 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 25), указать “Местоположение обнаружения”, “Организация обнаружения”. Для отмены авторазвертывания параметру присваивают значение “Нет”.

22.7 ::sign-image

src: /image35.png sign: Рисунок 25 — Параметры авторазвертывания — ::

Для всех обнаруженных узлов необходимо провести процедуру включения в группы узлов, задания правил и параметров сетевой установки в соответствии с п. Параметры сетевого развертывания узла 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 (рисунок 26).

22.8 ::sign-image

src: /image36.png sign: Рисунок 26 — Правила обнаружения — ::

В рабочей области на вкладке “Основной” необходимо ввести значения полей (рисунок 27):

- 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 .

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

- – просмотреть обнаруженные узлы по этому правилу;
- – просмотреть управляемые узлы по этому правилу;
- – отключить правило;
- – удалить правило.

22.9 ::sign-image

src: /image37.png sign: Рисунок 27 — 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.

22.10 Параметры сетевого развертывания узла

После регистрации лицензии и подготовки установочного носителя ОС требуется выполнить настройку параметров сетевого развертывания узла. Для этого следует перейти в меню “Узлы Создать узел” панели навигации.

На экране появится интерфейс настройки, в котором параметры развертывания нового узла распределены по вкладкам (рисунок 28).

22.11 ::sign-image

src: /image38.png sign: Рисунок 28 — Параметры сетевого развертывания узла — ::

Во вкладке “Узел” интерфейса настройки указывают имя узла.

Примечание – Указывается не полное доменное имя, а только непосредственно символьное имя узла (например, backup или monitoring).

Затем из раскрывающегося списка “Область” нужно выбрать 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 (в общем случае 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.

Примечание – 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 требуется указать 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 РОСА “Хром” (или ROSA Enterprise Linux Server), поэтому рекомендуется оставить существующие значения без изменений. Параметры из секции “Глобальные параметры” можно переопределять или удалять, нажав соответствующую кнопку в строке параметра. Кроме того, есть возможность добавлять параметры конкретного узла в секции “Параметры Узла”, для чего нужно нажать кнопку + и ввести его имя, тип и значение.

При создании узла имеется возможность указания пользователя, добавившего узел, и пользователя, который будет этим узлом управлять. Операция осуществляется на вкладке “Дополнительно” выбором пользователя из списка “Владелец” в меню “Узлы” при создании или редактировании узла.

После завершения настройки параметров развертывания нужно нажать кнопку .

В результате РОСА Центр Управления автоматически подготовит необходимые конфигурацио 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.

Далее необходимо включить узел, установить приоритет загрузки узла по сети и дождаться окончания процесса развертывания.

Для просмотра списка узлов выбирают пункт основного меню “Узлы Все Узлы”. Для просмотра информации об узле нужно нажать на его имя. Для редактирования информации об узле следует нажать на кнопку в колонке “Действия” в строке с его именем в списке. Для удаления узла нужно выбрать действие “Удалить” в строке записи или выбрать пункт “Удалить узлы” в общем списке “Действия” для выбранных узлов.

22.12 Указание сетевого адреса подсети

Для заведения в РОСА Центр Управления подсетей, используемых в организации и/или их местоположении, необходимо перейти в пункт основного меню “Инфраструктура ® Подсети”, в окне которого можно завести новую подсеть, нажав кнопку , или изменить параметры существующей, нажав на её имени (рисунок 29).

Для удаления подсети нужно выбрать действие “Удалить” в строке записи домена.

22.13 ::sign-image

src: /image39.png sign: Рисунок 29 — Работа с подсетями — ::

При создании или изменении подсети указываются имя подсети, ее параметры, отнесение к доменам, организация и местоположение (рисунок 30). Для сохранения введенных данных необходимо нажать кнопку .

22.14 ::sign-image

src: /image40.png sign: Рисунок 30 — Изменение данных о подсети — ::

Для того чтобы у узла была задана подсеть, необходимо отнести узел к группе, а уже для группы узлов задать эти параметры в основном меню “Настройка Группы узлов” на вкладке “Сеть” (рисунок 31). Здесь же на вкладках “Местоположения” и “Организации” можно задать местоположение и организацию группы соответственно.

22.15 ::sign-image

src: /image41.png sign: Рисунок 31 — Параметры сети для группы узлов — ::

22.16 Указание серверов прокси HTTP

Для обеспечения работы РОСА Центр Управления без прямого доступа к сети Интернет необходимо указать серверы прокси HTTP. Для этого в пункте меню навигации выбрать “Инфраструктура HTTP Прокси” и в рабочей области нажать кнопку HTTP- .

На вкладке “HTTP-прокси” вводят имя сервера и его URL с указанием порта. Проверить подключение можно нажатием кнопки с идентичным названием (рисунок 32). Для сохранения данных нажимают кнопку .

22.17 ::sign-image

src: /image42.png sign: Рисунок 32 — Добавление прокси HTTP — ::

22.18 Вычислительные ресурсы

Для создания узлов на базе ВМ необходимо завести виртуальные вычислительные ресурсы. Работа с ресурсами обеспечивается в меню “Инфраструктура Вычислительные ресурсы” (рисунок 33). Для добавления нового ресурса нажимают кнопку и вводят его наименование, описание и выбирают среду виртуализации в раскрывающемся списке “Сервис”: EC2, Libvirt, OpenStack, VMware или oVirt. В зависимости от выбранной среды необходимо ввести параметры для подключения и конфигурирования ресурса. Здесь же на вкладках “Местоположения” и “Организации” можно задать местоположение и организацию соответственно. Для сохранения данных нажимают кнопку . В появившемся списке в столбце действия можно выбрать изменение или удаление существующего вычислительного ресурса.

22.19 ::sign-image

src: /image43.png sign: Рисунок 33 — Вычислительные ресурсы — ::

Вычислительные ресурсы используются при создании новых ВМ в качестве альтернативы узлам, работающим на физическом оборудовании. Профили ВМ привязывают к вычислительным ресурсам и создают на их основе образы ВМ и сами ВМ на базе образов (рисунок 34). Вычислительный ресурс указывают при создании ВМ на вкладке “Узел” выбором в поле “Развертывание” наименования ресурса.

22.20 ::sign-image

src: /image44.png sign: Рисунок 34 — Работа с вычислительным ресурсом — ::

22.21 Профили виртуальных машин

В случае создания узлов на базе ВМ необходимо завести возможные профили их технических характеристик для развертывания. Работа с профилями ВМ обеспечивается в меню “Инфраструкту Профили вычислений” (рисунок 35). Для добавления нового профиля нажимают кнопку и вводят его наименование. Для сохранения данных нажимают кнопку . В столбце действия можно выбрать изменение или удаление существующего профиля ВМ.

Профили ВМ используются при создании новых узлов в качестве альтернативы узлам, работающим на физическом оборудовании. Профили указывают при создании узла на вкладке “Узел” выбором в поле “Развертывание”

22.22 ::sign-image

src: /image45.png sign: Рисунок 35 — Вычислительные профили — ::

22.23 Создание подготовленных образов конфигураций узлов

Для оперативного управления конфигурациями узлов предусмотрена возможность создания подготовленных образов конфигураций, которые могут быть развёрнуты на узлах в автоматизирова режиме.

Для подготовки таких образов используется раздел “Узлы” основного меню и группы пунктов меню с данными для конфигурирования узлов (рисунок 36):

1. группа “Подготовка узлов”:
    - “Архитектура” – перечень применяемых архитектур узлов;
    - “Модели оборудования” – типы применяемых классов центрального процессора узла;
    - “Установочный носитель” – перечень источников устанавливаемых операционных систем с указанием пути для скачивания;
    - “Операционные системы” – перечень операционных систем со спецификацией всех применяемых параметров установки: версии ОС, семейства ОС, архитектуры рабочих станций, таблицы разделов, установочного носителя и шаблона подготовки;

Примечание – Для ОС может применяться набор настраиваемых шаблонов (начальный и постустановочный сценарии, установщик ОС и загрузчик PXE).

2. группа “Шаблоны”:
    - “Таблицы разделов” – инструкции в виде скриптов для создания таблиц разделов на накопителях рабочих станций в зависимости от семейства операционной системы;
    - “Шаблоны подготовки” – инструкции в виде скриптов, описывающие все этапы подготовки конфигурации узла, начиная с подготовительного и заканчивая завершающим шаблонами;
    - “Шаблоны заданий” – инструкции в виде скриптов, описывающие задания на всех этапах подготовки конфигурации узла.

22.24 ::sign-image

src: /image46.png sign: Рисунок 36 — Подготовка образов конфигураций узлов — ::

На основании этих данных каждый узел может быть сконфигурирован как отдельно, так и в составе групп с подобными конфигурациями. Выбор и применение конфигураций узлов в составе групп осуществляется на вкладке “Операционная система” при редактировании группы по пункту меню “Настройка Группы узлов”.

22.25 Конфигурирование шаблонов установки ОС

Для конфигурирования шаблонов установки ОС нужно перейти в меню “Узлы Подготовка узлов Операционные системы” и нажать кнопку или выбрать существующую ОС из списка (рисунок 37).

22.26 ::sign-image

src: /image47.png sign: Рисунок 37 — Создание новой или выбор настроенной ОС — ::

На вкладке “Шаблоны” выбираются шаблоны для каждого этапа загрузки ОС (рисунок 38).

Для сохранения следует нажать кнопку .

22.27 ::sign-image

src: /image48.png sign: Рисунок 38 — Настройка шаблонов для ОС — ::

22.28 Установочные носители

Для указания источников устанавливаемых ОС с указанием пути для скачивания используется функционал меню “Узлы Подготовка узлов Установочный носитель” (рисунок 39).

22.29 ::sign-image

src: /image49.png sign: Рисунок 39 — Перечень установочных носителей — ::

Для создания нового установочного носителя нужно нажать кнопку и в рабочей области на вкладке “Носитель” задать значения полей (рисунок 40):

- Имя – имя установочного носителя;
- Путь – путь до установочного носителя в виде URL;
- Семейство ОС – тип ОС.

22.30 ::sign-image

src: /image50.png sign: Рисунок 40 — Создание установочного носителя — ::

Для сохранения нажать кнопку .

Для работы с установочными носителями нужно внести изменения в соответствующие классы Puppet rcc_typical_arm_bux и rcc_typical_arm_bux, отвечающие за установку пакетов на узлы.

Для внесения изменений нужно перейти в меню “Настройки Классификатор узлов Puppet Классы”, в рабочей области выбрать имя класса и на вкладке “Параметр Smart Class” выбрать для редактирования параметр по маске с постфиксом и внести изменения в раздел “Поведение по умолчанию”:

- *_enable – включить параметр в поле “Изменить”, в поле “Значение по умолчанию” задать “true” для установки пакетов, “false” для удаления;
- *_packages – для задания списков пакетов включить параметр в поле “Изменить”, задать строку перечня пакетов, разделенных запятыми, в поле “Значение по умолчанию”. Для сохранения нажать кнопку .

23

СОЗДАНИЕ УЗЛОВ

Пользователь Комплекса может создавать дополнительные узлы (в дополнение к узлам, развернутым через сетевую инфраструктуру) для последующего включения в группы управляемых узлов.

Для создания узлов можно воспользоваться двумя вариантами:

1. перейти в меню “Узлы Создать Узел” панели навигации;
2. перейти в меню “Узлы Все Узлы” панели навигации и нажать кнопку в верхнем правом углу рабочей области

Далее в появившейся рабочей области на вкладке “Узел” необходимо присвоить имя узлу и заполнить поля, относящие узел к месторасположению, организации, группе узлов, домену и настройкам систем оркестрации. Также требуется заполнить всю информацию, относящуюся к узлу, на вкладках “Роли Ansible”, “Операционная система”, “Интерфейсы”, “Puppet ENC”, “Параметры”, “Дополнительно” (рисунок 41). На вкладке “Puppet ENC” при необходимости выбирают классы, относящиеся к создаваемому узлу, нажав на пиктограмму (плюс) рядом с названием класса.

23.1 ::sign-image

src: /image51.png sign: Рисунок 41 — Создание узла — ::

Для сохранения настроек параметров узла необходимо нажать кнопку .

24

РЕГИСТРАЦИЯ СУЩЕСТВУЮЩИХ УЗЛОВ

Для успешной регистрации в РОСА Центр Управления существующий узел (ранее развернутый не под управлением Комплекса) 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 Управл 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 следующие сетевые порты сервера РОСА Центр Управления:
  - `TCP/443` – HTTPS;
  - `TCP/8140` – Puppet;
- узлу должны быть доступны следующие сетевые порты сервера СИПА:
  - `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 – При необходимости можно настроить для регистрируемых узлов правила автоподписывания сертификатов Puppet (п.3.4 документа “Платформа централизованного управления жизненным циклом операционных систем”РОСА Центр Управ Руководство системного администратора. Часть 1. Установка и настройка” (шифр РСЮК.10121-08 32 01)).

Для подключения агента puppet требуется:

- открыть сессию от имени суперпользователя root на узле, который необходимо подключить к серверу РОСА Центр Управления;
- открыть в текстовом редакторе файл конфигурации (в зависимости от версии ОС) `/etc/puppet/puppet.conf` с помощью команды:

`bash Terminal mcedit /etc/puppet/puppet.conf` - создать или изменить секцию конфигурац файла [agent] со следующим содержанием:

`bash Terminal [agent] ca_server = cc.rosa.int certname = host.rosa.int server = cc.rosa.int`

где: - ca_server – FQDN сервера сертификации РОСА Центр Управления; - certname – FQDN подключаемого узла; - server – FQDN сервера РОСА Центр Управления;

- включить и запустить системный агент puppet, выполнив команду:

```
bash Terminal systemctl enable --now puppet
```

— для проверки запуска агента выполнить команду:

```
bash Terminal puppet agent -t
```

После подготовки узла необходимо перейти в меню “Узлы Зарегистрировать узел” панели навигации для настройки параметров регистрации узла (рисунок 42).

24.1 ::sign-image

src: /image52.png sign: Рисунок 42 — Параметры регистрации узла — ::

В списке “Группа узлов” выбирают группу, в которую будет включен узел, затем выбирают ОС, указывают или создают ключ активации, а остальные параметры регистрации узла можно оставить со значениями по умолчанию.

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 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 надо нажать кнопку . В результате в текстовом поле под этой кнопкой появится созданная команда (скрипт регистрации).

Далее копируют эту команду и выполняют в терминале ОС регистрируемого узла.

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

25

СОЗДАНИЕ ГРУППЫ УЗЛОВ

Пользователь Комплекса может создавать собственные группы узлов (в дополнение к группам, созданным в РОСА Центр Управления по умолчанию) для группировки управляемых узлов по различным признакам с целью единовременного применения конфигурационных настроек сразу к группе однотипных узлов.

Для создания группы рабочих станций (или узлов – в нотации интерфейса Комплекса) нужно перейти в меню “Настройки Группы узлов” панели навигации и нажать кнопку в верхнем правом углу рабочей области (рисунок 43).

25.1 ::sign-image

src: /image53.png sign: Рисунок 43 — Работа с группами узлов — ::

Далее в появившейся рабочей области на вкладке “Группа узлов” необходимо присвоить имя создаваемой группе. При необходимости можно выбрать в поле “Родитель” вышестоящую группу узлов. При наличии родительской группы узлов для создаваемой группы будут применяться в том числе классы, назначенные на все вышестоящие группы (рисунок 44).

25.2 ::sign-image

src: /image54.png sign: Рисунок 44 — Создание группы узлов — ::

Также заполняют всю информацию, относящуюся к группе, на вкладках “Роли Ansible”, “Сеть”, “Операционная система”, “Параметры”, “Puppet ENC”, “Местоположения”, “Организации”, “Ключи активации”.

На вкладке “Puppet ENC” выбирают классы, относящиеся к создаваемой группе узлов, нажав на пиктограмму (плюс) рядом с названием класса.

Для раздельного управления серверным и пользовательским сегментами удобно использовать функционал организаций и местоположений, задать которые можно в соответствующ вкладках “Организации” и “Местоположения”. В случае построения иерархии организации с разделением объектов управления по функциональному назначению (например, серверы и рабочие станции) на одном из верхних уровней разделенное управление может сводиться к выбору нужной организации в фильтре.

Для сохранения настроек параметров группы узлов необходимо нажать кнопку .

С помощью действия “Вложить” в строке текущей группы возможно организовать наследование применимости классов от вышестоящих (родительских) к нижестоящим (дочерним) группам узлов.

26

ДОБАВЛЕНИЕ УЗЛА В ГРУППУ

При необходимости управляемый узел может быть добавлен в одну из существующих групп узлов.

Для добавления узла в группу нужно перейти в меню “Узлы Все Узлы” панели навигации и нажать наименование (доменное имя) необходимого узла.

На экране появится интерфейс с подробными параметрами выбранного узла, в котором нажимают кнопку , затем во вкладке “Узел” из раскрывающегося списка “Группа узлов” выбирают необходимую группу и нажимают кнопку для сохранения настройки (рисунок 45).

Примечание – Изменение ранее выбранной группы для узла осуществляется аналогичным способом.

26.1 ::sign-image

src: /image55.png sign: Рисунок 45 — Выбор узла для отнесения к группе — ::

Другим способом изменения группы для узла является возможность перейти в меню “Узлы Все Узлы”, выбрать все или некоторые узлы, проставив “флажки” в крайний левый столбец списка, и, нажав кнопку в верхнем правом углу, выбрать пункт “Изменить группу” (рисунок 46).

Далее в появившемся окне нужно назначить группу для выбранных ранее узлов и нажать кнопку .

26.2 ::sign-image

src: /image56.png sign: Рисунок 46 — Выбор группы узлов — ::

После изменения группы для выбранных узлов будут назначены классы как выбранной, так и вышестоящих групп.

27

ПРИСВОЕНИЕ ГРУППЫ НЕРАСПРЕДЕЛЕННЫМ УЗЛАМ

Модуль RCC_default_group предназначен для присвоения заданной группы нераспределенным узлам на сервере РОСА Центр Управления.

Принцип работы модуля состоит в добавлении или удалении из расписания планировщика cron скрипта распределения узлов в зависимости от бинарного параметра enable_default_hostgroup.

Скрипт в модуле представлен в виде erb-шаблона с возможностью переопределения имени группы.

Управление в скрипте реализовано с помощью утилиты командной строки hammer от имени администратора.

Следует обратить внимание, что для правильной работы необходимо наличие корректно заполненного файла /root/.hammer/cli.modules.d/foreman.yml следующего вида:

```
bash Terminal :foreman: Credentials. You'll be asked for them interactively if you leave them blank here :username: 'admin' :password: '<            admin>'
```

Данный файл создается автоматически при установке Комплекса, но требует внесения изменений при последующей смене пароля пользователя admin.

Для автоматического распределения в группу по умолчанию необходимо назначить модуль RCC_default_group на группу “Rosa Control Center Server” в меню “Настройка Группы узлов”. После выполнения Puppet-агента создается расписание cron для скрипта, который назначает группу по умолчанию для всех узлов без назначенной группы.

Параметры модуля приведены в таблице 1.

27.1 ::app-collapsible

27.2 label: “Таблица 1 - Параметры модуля RCC_default_group”

#content

Имя

Тип

Значение по умолчанию

Описание

enable_default_group

Boolean

true

true – включение автоматического присвоения группыfalse – выключение автоматического присвоения группы

default_group_name

String

Default

Имя группы для автоматического присвоения нераспределенным узлам

::

28

СОСТОЯНИЕ УЗЛА

Для получения информации о состоянии конкретного узла и развернутых на нем конфигураций необходимо перейти в пункт основного меню “Узлы Все Узлы” и нажать на имени узла.

В рабочей панели отображается вся актуальная информация о состоянии узла на вкладках “Обзор”, “Сведения”, “Параметры”, “Ansible”, “Puppet”, “Отчеты” и на виджетах в соответствии с размещенными на них легендами. Для получения более подробной информации о текущем состоянии узла можно воспользоваться ссылками (рисунок 47).

28.1 ::sign-image

src: /image57.png sign: Рисунок 47 — Состояние узла — ::

29

УПРАВЛЕНИЕ АРМ С ОС WINDOWS

В Комплексе для управления АРМ с ОС Windows используются классы и факты Puppet.

Для обеспечения такого управления на АРМ с ОС Windows должен быть установлен и настроен puppet-agent.

С помощью Комплекса можно выполнить операции, описанные в п. Управление АРМ с ОС Windows.

Следует обратить внимание, что операции будет выполняться каждый раз при отработке puppet-agent на АРМ. Для отключения операции нужно отвязать АРМ от группы узлов.

29.1 Копирование файлов

Для копирования файлов из одной папки в другую как по сети, так и в файловой системе ПК нужно создать группу узлов и привязать к ней класс `rcc_win:copy_file`.

Для этого нужно выполнить следующие действия:

1. создать группу узлов (описано в п. Создание группы узлов);
2. перейти на вкладку “Puppet ENC” созданной группы и в доступных классах выбрать `rcc_win:copy_file`, который должен появиться в секции “Включенные классы” (рисунок 48);

29.2 ::sign-image

src: /image58.png sign: Рисунок 48 — Выбор класса — ::

3. в параметрах выбранного класса задать значения (рисунок 49):

   — `rcc_win_copy_from` – директория, из которой нужно выполнить копирование;
   — `rcc_win_copy_to` – директория, в которую нужно выполнить копирование;

29.3 ::sign-image

src: /image59.png sign: Рисунок 49 — Параметры копирования — ::

4. нажать кнопку , класс будет привязан к группе;
5. добавить в эту группу те АРМ, для которых операция копирования актуальна, и при следующей отработке puppet-agent такая операция будет выполнена.

29.4 Запуск исполняемого файла.

Для запуска какого-либо исполняемого файла необходимо выполнить следующие действия:

1. создать группу узлов (описано в п. Создание группы узлов);
2. перейти в пункт меню “Настройка Группы узлов” и на вкладке “Классификатор узлов Puppet” в созданную группу добавить класс rcc_win:exec;
3. задать значение параметра rcc_win_exec_command – полный путь до исполняемого файла (рисунок 50);

29.5 ::sign-image

src: /image60.png sign: Рисунок 50 — Параметр rcc_win_exec_command — ::

3. нажать кнопку , класс будет привязан к группе;
4. добавить в эту группу те АРМ, для которых операция запуска актуальна, и при следующей отработке puppet-agent такая операция будет выполнена.

29.6 Подключение сетевого диска

Для подключения сетевого диска к АРМ необходимо выполнить следующие действия:

1. создать группу узлов (описано в п. Создание группы узлов);
2. перейти в пункт меню “Настройка Группы узлов” и на вкладке “Puppet ENC” в созданную группу добавить класс rcc_win:net_use (рисунок 51);

29.7 ::sign-image

src: /image61.png sign: Рисунок 51 — Выбор класса — ::

3. в параметрах выбранного класса задать значения (рисунок 52):
   - rcc_win_net_disk_letter – имя подключаемого сетевого диска;
   - rcc_win_net_disk_passwd – пароль локального администратора;
   - rcc_win_net_disk_user – логин локального администратора;
   - rcc_win_net_path – полный путь подключаемой сетевой директории;

29.8 ::sign-image

src: /image62.png sign: Рисунок 52 — Параметры класса — ::

4. нажать кнопку , класс будет привязан к группе;
5. добавить в эту группу те АРМ, для которых операция подключения сетевого диска актуальна, и при следующей отработке puppet-agent такая операция будет выполнена.

Следует обратить внимание, что операция подключения сетевого диска будет выполнена под УЗ локального администратора, и подключенный диск не будет виден пользователям. Это действие используется только для обслуживания АРМ, например, для подключения

диска администратором, а затем копирования файлов или папки на АРМ, чтобы в дальнейшем установить программу.

29.9 Обзор установленного ПО

В Комплексе можно посмотреть установленное на АРМ программное обеспечение.

Для этого нужно открыть пункт меню “Наблюдение Факты”, найти и выбрать факт rcc_win_software, после чего отобразится список узлов с установленным на них ПО (рисунок 53).

29.10 ::sign-image

src: /image63.png sign: Рисунок 53 — Значение факта rcc_win_software — ::

Например, чтобы посмотреть узлы, на которых установлена программа WinRAR, в строке поиска нужно ввести `! ~ WinRar` и получить отфильтрованный список узлов (рисунок 54).

29.11 ::sign-image

src: /image64.png sign: Рисунок 54 — Список узлов с установленным WinRAR — ::

29.12 Обзор установленных обновлений Windows

Для того чтобы посмотреть установленные на АРМ обновления Windows, нужно зайти в пункт меню “Наблюдение Факты”, найти и выбрать факт rcc_win_update, после чего отобразится список АРМ с установленными на них обновлениями ОС Windows (рисунок 55).

29.13 ::sign-image

src: /image65.png sign: Рисунок 55 — Список узлов с установленными обновлениями ОС Windows — ::

30

МИГРАЦИЯ УЗЛОВ НА РОСА “ХРОМ”

30.1 Миграция с ОС Windows

30.1.1 Развертывание сервера обеспечения миграции

Требования к аппаратным средствам сервера, предназначенного для обеспечения миграции, приведены в таблице 2.

30.2 ::app-collapsible

30.3 label: “Таблица 2 - Требования к аппаратным средствам сервера обеспечения миграции”

#content

Параметр

Минимальное значение

Рекомендуемое значение

Количество ядер процессора

2

4

Объем оперативной памяти, Гбайт

4

8

Свободное дисковое пространство, Гбайт

2000

4000

::

Для миграции узлов, подключенных к Комплексу, необходимо осуществить предварительное развертывание сервера обеспечения процедуры миграции. Сервер служит временным хранилищем мигрируемых пользовательских данных и резервной копией локальных разделов мигрируемого АРМ.

Благодаря сохраненной резервной копии разделов в случае возникновения необходимости существует возможность отката АРМ в состояние “до миграции” с использованием стандартных утилит ОС Windows.

Для автоматизированного развертывания сервера предусмотрено использование класса rcc_migrator_create_backup_server.

Данный класс имеет два параметра:

- backup_server – IP-адрес или FQDN-имя сервера, выбранного в качестве сервера обеспечения миграции (например, 10.0.0.17);
- backup_folder – расположение каталога на сервере, в котором будет хранится резервная копия разделов мигрируемого АРМ, а также переносимая информация профилей пользователей (например, /srv/migrate).

Для назначения класса Puppet необходимо выполнение следующих шагов:

1. перейти в пункт основного меню “Узлы Все Узлы” и выбрать сервер;
2. перейти к редактированию сервера, нажав кнопку в столбце “Действия”;
3. на вкладке “Puppet ENC” из перечня “Доступные классы” перенести класс rcc_migrator_create_
во “Включенные классы” (рисунок 56);
4. нажать кнопку .

30.4 ::sign-image

src: /image66.png sign: Рисунок 56 — Параметры класса — ::

После назначения класса на сервер обеспечения миграции и задания параметров (backup_server и backup_folder) произойдет автоматическая установка и настройка необходимых сервисов.

Во время первого запуска класса возможен автоматический перезапуск сервера для изменения настроек безопасности selinux.

30.4.1 Требования к аппаратному и программному обеспечению узлов

Процедура миграции применяется к физическим узлам в соответствии со следующими требованиями конфигурации:

1. Минимальная конфигурация ПК:
   - ЦП архитектуры x86-64, 2 ядра 1,2 ГГц;
   - ОЗУ 2 ГБ;
   - 20 ГБ свободного дискового пространства на основном накопителе.
2. Рекомендуемая конфигурация ПК:
   - ЦП архитектуры x86-64, 2 ядра 1,2 ГГц;
   - ОЗУ 4 ГБ;
   - 50 ГБ свободного дискового пространства на основном накопителе.
3. Оборудование должно быть совместимо с дистрибутивом развёртываемой отечественной ОС и отвечать его системным требованиям.
4. На узлах в настройках микропрограммы EFI должен быть отключен протокол Secure Boot.

5. На диске, содержащем системный раздел, не должно содержаться динамических и шифрованных разделов.
6. Недопустимы блокировки доступа к информации на диске со стороны систем безопасности. Каталоги пользователей должны быть открыты на чтение и запись.

30.4.2 Сценарий миграции

Сценарий миграции узлов с Windows-подобной на отечественную ОС включает подготовительные действия оператора миграции и автоматизированные процедуры, выполняемые Комплексом:

1. Проверка средствами ОС Windows готовности узла к миграции на наличие необходимых прав доступа и версий клиентского программного обеспечения. Очистка пользовательских данных от ненужных программ и файлов. Проверка наличия и/или установка на узле Puppet-агента. Это позволяет минимизировать количество сбоев в процессе миграции и сэкономить дисковое пространство на backup-сервере.
2. Включение мигрируемого узла в группу узлов с классами Puppet для миграции или подключение к узлу классов Puppet для миграции с последующим запуском агента Puppet на узле для начала процедуры.
3. Сохранение на backup-сервере данных и настроек пользователей узла. Сохраняются следующие папки пользователей:
   - Загрузки;
   - Документы;
   - Изображения;
   - Рабочий стол.

   Примечание – Папки пользователей сохраняются независимо от месторасположения на дисках и в каталогах.

4. Доставка и установка на системный диск “образа” целевой отечественной операционной системы. По завершении этапа производится запуск целевой ОС.
5. Настройка ОС и программного обеспечения. Завершающий этап, на котором осуществляется ряд процессов, необходимых для ввода узла в эксплуатацию: ввод в домен, подключение к системному прокси-серверу, установка дополнительного ПО, подключение периферийного оборудования, настройка прикладного ПО и информационных систем.

30.4.3 Процедура миграции

Процедура миграции производится с помощью использования предустановленных классов Puppet (п. Puppet настоящего Руководства).

Для миграции нескольких узлов можно создать отдельную группу, в которую следует добавить все классы Puppet, применяемые ниже.

Для осуществления подготовки к процедуре миграции необходимо выполнение следующих шагов:

1. перейти в пункт основного меню “Узлы ® Все Узлы” и выбрать узел с установленной Windows-подобной ОС и предустановленным Puppet-агентом;
2. перейти к редактированию узла, нажав кнопку в столбце Действия;
3. на вкладке “Puppet ENC” из перечня “Доступные классы” перенести класс rcc_migrator_win_sid во “Включенные классы”, в котором можно настроить параметры для Windows-части миграции (рисунок 57):

   — backup_letter – задать букву подключаемого сетевого диска резервных копий;
   — backup_server – назначить FQDN-имя или IP-адрес сервера обеспечения миграции;
   — delay_after_backup – задать задержку в секундах по окончании этапа резервного копирования;
   — delay_after_cleaning – задать задержку в секундах по окончании этапа очистки;

30.5 ::sign-image

src: /image67.png sign: Рисунок 57 — Назначение Puppet-класса узлу — ::

4. нажать кнопку .
5. запустить Puppet-агент на узле по одному из вариантов:

   — выполнение команды:

```
bash Terminal puppet agent -t
```

- перезагрузка ОС; - перезапуск Windows-службы “Puppet Agent”.

Далее производятся следующие действия:

1. автоматизированная очистка дискового пространства узла от вспомогательных, системных и других файлов для оптимизации скорости миграции и размера при создании “образа” сохраняемых данных, по окончании которого будет выдано сообщение “Внимание! Для завершения подготовительного этапа миграции ОС необходимо перезагрузить компьютер. Автоматический перезапуск через 240 секунд” (можно инициировать перезагрузку вручную) (рисунок 58);

30.6 ::sign-image

src: /image68.png sign: Рисунок 58 — Сообщение после этапа очистки — ::

2. после перезагрузки автоматизированное сохранение пользовательских данных и снимка “образа” ОС узла, по окончании которого будет выдано сообщение “Внимание! Ваш АРМ готов к проведению миграции. Перезапустите ПК и выберите пункт меню загрузки ‘Control Center Discovery Image’. Автоматический перезапуск через 120 секунд” (можно инициировать перезагрузку вручную) (рисунок 59);

30.7 ::sign-image

src: /image69.png sign: Рисунок 59 — Сообщение после этапа сохранения данных — ::

> Примечание – Получить статус выполнения заданий по очистке и резервному копированию АРМ под управлением Windows возможно обратившись к факту fact=rcc_migrator_win_status (рисунок 60), воспользовавшись веб-интерфейсом Комплекса.

30.8 ::sign-image

src: /image70.png sign: Рисунок 60 — Факт о статусе выполнения заданий — ::

3. после перезагрузки необходимо выбрать из меню загрузки (рисунок 61) пункт “Control Center Discovery Image” для перехода к процедуре миграции;

30.9 ::sign-image

src: /image71.png sign: Рисунок 61 — Меню загрузки — ::

4. в процессе загрузки узла появится сообщение (рисунок 62); необходимо дождаться окончания времени обратного отсчета, не нажимая никакие клавиши;

30.10 ::sign-image

src: /image72.png sign: Рисунок 62 — Сообщение о процессе обнаружения узла — ::

5. после успешной загрузки узла появится сообщение (рисунок 63)

30.11 ::sign-image

src: /image73.png sign: Рисунок 63 — Сообщение об успешной загрузке — ::

6. данные об обновленном узле передаются в Комплекс; нужно перейти в меню “Узлы Обнаруженные узлы” и убедиться, что появился новый узел (рисунок 64), который необходимо в дальнейшем мигрировать;

30.12 ::sign-image

src: /image74.png sign: Рисунок 64 — Новый обнаруженный узел — ::

7. в строке узла в колонке “Действия” нажать ; в появившемся модальном окне “Выбор параметров инициализации узла” выбрать из раскрывающихся списков “Группу узлов”, для которой заданы параметры установки ОС, “Организацию”, “Месторасполо и нажать кнопку (рисунок 65);

30.13 ::sign-image

src: /image75.png sign: Рисунок 65 — Параметры узла — ::

8. в рабочей области редактирования узла на вкладке “Puppet ENC” из перечня “Доступные классы” добавить класс rcc_migrator_lin_side во “Включенные классы” в котором можно настроить параметр backup_server – FQDN-имя или IP-адрес сервера восстановления узла к исходному состоянию (рисунок 66);

30.14 ::sign-image

src: /image76.png sign: Рисунок 66 — Назначение Puppet-класса узлу — ::

9. нажать кнопку ;
10. новый узел автоматически перезагрузится и в меню PXE-загрузки теперь нужно выбрать пункт “Kickstart Rosa PXELinux” для миграции на целевую ОС (рисунок);

30.15 ::sign-image

src: /image77.png sign: Рисунок 67 — Выбор процедуры миграции на новую ОС — ::

11. далее производится автоматизированная установка новой ОС;
12. после установки появится меню (рисунок 67), в котором для локальной загрузки нужно выбрать пункт “Default local boot” для работы с мигрированным узлом;

30.16 ::sign-image

src: /image78.png sign: Рисунок 68 — Выбор локальной загрузки для начала работы — ::

13. при первом входе в домен после миграции сохраненные данные и настройки переносятся в новую целевую ОС.

30.16.1 Результаты миграции

В результате миграции в конфигурации новой отечественной ОС присутствуют следующие данные и настройки:

— данные всех пользователей узла;

— файлы *.pst почтовой программы;
— сетевые папки общего доступа.

Применение миграции с использованием РОСА Центр Управления имеет следующие преимущества:

— проверка и исправление файловой системы средствами ОС Windows, что снижает риск сбоев в процессе создания образа ВМ в дальнейшем;
— уменьшение объема дисковой информации;
— сокращение времени миграции;
— отсутствие необходимости подготовки дополнительных шаблонов развертывания миграции, так как можно использовать существующие шаблоны развертывания ОС;
— максимальная полнота данных и настроек пользователей узла по сравнению с мигрируемой ОС.

30.17 Установка и миграция с ОС Windows с использованием “золотого образа”

30.17.1 Требования к оператору миграции

Пользователь Комплекса (оператор миграции) должен иметь следующий опыт:

— Администрирование ОС Windows для установки и настройки программного обеспечения (агент системы оркестрации puppet);
— Установка ОС в Комплексе с использованием PXE;
— Установки ОС в Комплексе с обнаружением узлов;
— Создание/изменение групп узлов;
— Управление АРМ с использование классов Puppet ENC;
— Переопределение классов Puppet ENC;
— Назначение запланированных заданий;
— Знание работы с системами виртуализации для создания образов установленной ОС.

30.17.2 Подготовка “золотого образа”

При подготовке “золотого образа” необходимо соблюдать следующие условия:

— предусмотреть, чтобы корневой раздел был последним;
— рекомендуется использовать для SWAP размещение в файле;
— рекомендуется предустановить необходимые репозитории, используемые в инфраструкт
— рекомендуется предустановить необходимое программное обеспечение, используемое в инфраструктуре;
— обратить внимание при создании образов на режим загрузки MBR/UEFI;
— форматом “золотого образа” должен быть QCOW2;

— для подготовки “золотого образа” должна использоваться система виртуализации, поддерживающая формат дисковой подсистемы QCOW2;
— при использовании физического АРМ необходимо использовать утилиту qemu-img для снятия “золотого образа”.

30.17.3 Подготовка сервера хранения

Сервер хранения предназначен для хранения “золотых образов” и данных с АРМ.

Данные с АРМ включают:

— образ блочного устройства с мигрируемой ОС;
— архивы данных пользователей.

Для подготовки сервера необходимо провести следующие действия:

1. при установке ОС необходимо предусмотреть достаточное свободное дисковое пространств для хранения данных;
2. создать локального пользователя (например, migrator);
3. создать SSH-ключ для данного пользователя; созданный приватный ключ будет использоваться для подключения;
4. настроить конфигурацию SSH-сервера, для подключения созданного пользователя;
5. создать каталог для хранения “золотых образов”;
6. владельцем файлов “золотых образов” назначить созданного пользователя;
7. создать каталог для хранения данных с АРМ;
8. владельцем каталога данных с АРМ назначить созданного пользователя.

После подготовки сервера хранения можно проводить процедуры установки (п. Установка ОС) или миграции с ОС Windows (п. Миграция ОС).

30.17.4 Установка ОС

Для установки используется механизм Комплекса: PXE-сервер в режиме обнаружения узлов.

Для установки ОС из “золотого образа” необходимо преднастроить группу узлов. В качестве эталонной группы в Комплексе создана группа Gold_Deploy.

В свойствах группы Gold_Deploy необходимо определить следующие параметры:

— во вкладке “Группа узлов”:
  – Окружение – “production”;
  – Прокси Puppet;
  – Прокси центра сертификации Puppet;
— во вкладке “Сеть” установить параметры для домена;
— во вкладке “Операционная система”:
  – Архитектура – x86_64;
  – Операционная система – ROSA Enterprise Server Migration Image 9.5.2;

- Носитель – ROSA Enterprise Server Migration Image 9.5.2;
- Таблица Разделов – Kickstart default;
- PXE-загрузчик– выбирается в соответствие с загрузчиком “золотого образа”;
- Пароль пользователя root;

— во вкладке “Параметры”:

- gold_image_name – тип “строка”; задает имя “золотого образа”;
- gold_server_key – тип “строка”; приватный ключ пользователя, от имени которого будет осуществляться подключение;
- gold_server_name – тип “строка”; IP-адрес сервера хранения;
- gold_server_path – тип “строка”; путь на сервере хранения для размещения “золотых образов”;
- gold_server_user – тип “строка”; имя пользователя на сервере хранения.

Далее следует установить для группы узлов “Местоположение” и “Организации”.

После установки параметров группы узлов необходимо загрузить АРМ в режиме PXE.

Затем требуется в меню загрузки выбрать “Control Center Discovery Image”.

После обнаружения узла нужно назначить на него созданную группу узлов.

В результате будет произведена автоматическая перезагрузка и установка новой ОС на АРМ.

30.17.5 Миграция ОС

Для миграции ОС используется дополнительное окружение “migration”.

При миграции ОС поддерживается подключение к домену Dynamic Directory с некоторыми ограничениями к доменам, основанными на FreeIPA: не поддерживается перемещение компьютера в организационное подразделение в связи с отсутствием делегирования прав и реальной иерархии организационных подразделений.

Служебное доменное имя для миграции rosa.migration предназначено для подключения промежуточного образа ОС к Комплексу с автоматическим подписанием сертификата.

Описание классов для миграции Класс подготовки миграции для ОС Windows rcc_migration_windov параметры класса и описание:

— default_route – тип “строка”; шлюз для промежуточного образа;
— dns_server – тип “строка”; DNS-сервер для промежуточного образа;
— grub_timeout – тип “строка”; время для загрузки для двойной загрузки в промежуточный образ
— reboot_timeout – тип “строка”; время перезагрузки после установки целевой ОС;
— uefi_letter – тип “строка”; имя диска в Windows для монтирования раздела UEFI;

Класс установки ОС rcc_migration_install_gold_image, параметры класса и описание:

- create_disk_img – тип “логическое значение”; флаг, определяющий создание образа блочного устройства с установленной ОС Windows;
- image_name – тип “строка”; имя файла золотого образа;
- ipa_domain – тип “строка”; имя домена;
- ipa_parentou – тип “строка”; DN организационного подразделения, в которое должен быть помещено АРМ после миграции и ввода в домен;
- ipa_realm_proxy – тип “строка”; имя служебной учетной записи Комплекса для управления учетными записями;
- reboot_timeout – тип “строка”; время перезагрузки после проведения миграции;
- root_password – тип “строка”; пароль пользователя root для промежуточной ОС, который необходим для подключения в случае возникновения возможных ошибок;
- server_data – тип “строка”; каталог на сервере хранения для данных с АРМ;
- server_key – тип “строка”; приватный SSH-ключ пользователя, от имени которого осуществляется подключение к серверу хранения;
- server_name – тип “строка”; IP-адрес сервера хранения;
- server_path – тип “строка”; каталог на сервере хранения для “золотых образов”;
- server_user – тип “строка”; пользователь, от имени которого осуществляется подключение к серверу хранения.

Для оптимальной процедуры миграции ОС рекомендуется использование групп хостов с переопределением параметров классов Puppet ENC.

Подготовка ОС Windows для проведения миграции Для подготовки ОС Windows для проведения миграции необходимо соблюдать следующие условия:

- Имя компьютера под управлением MS Windows не должно содержать символы верхнего регистра;
- ОС Windows должна быть подключена к Комплексу. Для подключения к Комплексу с рекомендуемым пакетом для установки puppet-agent-6.28.0-x64.msi нужно создать и выполнить скрипт с необходимыми действиями и параметрами:

```
bash Terminal hostname > myhostname.txt set /p certname=<myhostname.txt msiexec.exe
/qn /norestart /package puppet-agent-6.28.0 -x64.msi PUPPET_CA_SERVER="FQDN          "
PUPPET_MASTER_SERVER="FQDN          " PUPPET_AGENT_ENVIRONMENT="migration" PUPPET_AGENT_C
```

- При подключении АРМ с ОС Windows следует обратить внимание на установленное время, особенно в среде виртуализации;
- После подключения АРМ с MS Windows хосту нужно назначить группу хостов подготовки миграции для ОС Windows;
- Для ускорения процесса подготовки на мигрируемом АРМ нужно выполнить из командной строки запуск агента от имени администратора командой:

```
bash Terminal puppet agent -t
```

Выполнение агента необходимо провести в два этапа:

- первый запуск – подготавливает ОС, происходит очистка установленной ОС;
- второй запуск – производит установку загрузчика, создает архивы данных пользователей выводит сообщение, что ОС готова к перезагрузке, происходит перезагрузка в промежуточный образ.

Процедура миграции ОС Миграция происходит с использованием промежуточного образа ОС, в функции которого входит:

- подключение к Комплекса;
- определение раздела/диска, на котором установлена ОС Windows;
- монтирование ресурсов сервера хранения;
- создание образа блочного устройства, на котором установлена ОС Windows;
- копирование данных пользователей;
- копирование “золотого образа” на целевое блочное устройство;
- расширение корневого раздела;
- обновление initramfs;
- установка/обновление агента системы оркестрации Puppet;
- установка/обновление клиента FreeIPA;
- ввод АРМ в домен;
- перемещение АРМ в заданное организационное подразделение;
- конфигурация агента системы оркестрации Puppet;
- копирование данных пользователей на мигрируемый АРМ;
- автоматическая перезагрузка.

После перезагрузки в промежуточный образ АРМ автоматически подключается к Комплексу с именем mig[MAC адрес].rosa.migration.

На данный узел назначается группа узлов установки ОС.

После назначения класса необходимо для данного узла в Комплексе назначить удаленное задание выполнения “Puppet Run Once”.

После выполнения задания начнется процесс миграции.

По завершении процесса миграции АРМ автоматически будет введен в домен с заданным организационным подразделением, подключенным к РОСА Центр Управления.

30.18 Миграция с РОСА “Кобальт” с использованием backup-сервера

В качестве исходного состояния при миграции на РОСА “Хром” рассматривается АРМ под управлением ОС РОСА “Кобальт”, введенный в домен и с локальным пользователем.

Процедура миграции осуществляется выполнением следующих шагов:

1. в Комплексе создать группу узлов (например, cobalt4migrate), к которой привязать класс rcc_cobalt2chrome (рисунок 69);

30.19 ::sign-image

src: /image79.png sign: Рисунок 69 — Включение класса rcc_cobalt2chrome — ::

2. в группу узлов добавить АРМ, который подлежит миграции (на АРМ должен быть установлен и настроен puppet-agent), для чего на вкладке “Узлы” отметить строку с АРМ и по кнопке выбрать “Изменить группу” (рисунок 70);

30.20 ::sign-image

src: /image80.png sign: Рисунок 70 — Изменение группы — ::

3. выбрать нужную группу и нажать кнопку (рисунок 71);

30.21 ::sign-image

src: /image81.jpg sign: Рисунок 71 — Включение в группу миграции — ::

3. после включения в группу для миграции на АРМ будет выполнен манифест, по результатам которого осуществятся настройки для начала миграции:
   - резервное копирование всех данных пользователей;
   - создание полного зашифрованного образа для отката в случае непредвиденной ситуации;

   Примечание – Все данные с АРМ передаются на backup-сервер в зашифрованном виде, при этом данные пользователей после миграции будут восстановлены на новой ОС. В зашифрованном архиве data_tar_gz.gpg сохраняются данные пользователей, а в файле sda_img.tar.gz.gpg – зашифрованный образ ОС.

4. по окончании резервного копирования на экране АРМ появится примерно такое сообщение, как на рисунке 72;

30.22 ::sign-image

src: /image82.jpg sign: Рисунок 72 — Сообщение после резервного копирования — ::

5. нажать кнопку и перезагрузить компьютер с последующей загрузкой по сети и выбором пункта меню “Control Center Discovery Image EFI” (если только ОС до этого была в EFI) (рисунок 73);

30.23 ::sign-image

src: /image83.png sign: Рисунок 73 — Выбор типа загрузки — ::

6. в процессе загрузки узла появится сообщение (рисунок 74); необходимо дождаться окончания времени обратного отсчета, не нажимая никакие клавиши;

30.24 ::sign-image

src: /image84.png sign: Рисунок 74 — Сообщение о процессе обнаружения узла — ::

7. после успешной загрузки узла появится сообщение об успешной отправке данных на сервер (рисунок 75);

30.25 ::sign-image

src: /image85.jpg sign: Рисунок 75 — Сообщение об успешной загрузке — ::

8. в Комплексе перейти в пункт меню “Узлы Обнаруженные узлы”, выбрать в рабочей области требуемый АРМ и нажать кнопку (рисунок 76);

30.26 ::sign-image

src: /image86.png sign: Рисунок 76 — Выбор сетевой установки для АРМ — ::

9. в окне (рисунок 77) выбрать ранее настроенную группу узлов “Rosa Chrome/c2c” и нажать кнопку (переименовывать не нужно, так как мигрированному АРМ будет присвоено то же имя, что было до миграции);

30.27 ::sign-image

src: /image87.jpg sign: Рисунок 77 — Включение АРМ в преднастроенную группу — ::

В настройках узла на вкладке “Операционная система” выбрать параметр в списке “Загрузчик PXE” (рисунок 78):

— для UEFI – “Grub2 UEFI”;
— для MBR – “PXELinux BIOS”;

30.28 ::sign-image

src: /image88.png sign: Рисунок 78 — Выбор параметра загрузки — ::

10. после этого на мигрируемом АРМ начнется перезагрузка (по сети), в процессе которой выбрать пункт меню “Kickstart Rosa PXEGrub2”, после чего начнется установка, занимающая определенное время;
11. после перезагрузки АРМ уже начнет запускаться под управлением ОС РОСА “Хром” (рисунок 79);

30.29 ::sign-image

src: /image89.jpg sign: Рисунок 79 — Загрузка РОСА “Хром” — ::

Следует обратить внимание, что после первой загрузки РОСА “Хром” не нужно входить под УЗ пользователя, так как в это время копируются пользовательские данные, а по окончании будет выполнена перезагрузка в автоматическом режиме. На экране входа отобразятся локальные пользователи, которые были ранее в ОС РОСА “Кобальт” (рисунок 80);

30.30 ::sign-image

src: /image90.jpg sign: Рисунок 80 — Окно входа — ::

После выполненных шагов АРМ включен в домен, и можно входить как под доменной УЗ, так и под УЗ локального пользователя. Клиент puppet-agent уже настроен и работает с ключами от АРМ до миграции, на сервере Комплекса он будет присутствовать в списке узлов под старым именем (рисунок 81).

30.31 ::sign-image

src: /image91.png sign: Рисунок 81 — АРМ под новой ОС в списке узлов — ::

Ввиду того, что узел после окончания процедуры остался в группе миграции, его необходимо удалить из нее, как это показано на рисунке 82.

30.32 ::sign-image

src: /image92.jpg sign: Рисунок 82 — Удаление узла из группы миграции — ::

Кроме того, на вкладке “Узлы” в перечне узлов присутствует промежуточный узел, используемый при миграции и который следует удалить, выбрав из списка действие “Удалить” в соответствующем столбце (рисунок 83).

30.33 ::sign-image

src: /image93.png sign: Рисунок 83 — Удаление промежуточного АРМ — ::

В результате проделанных действий АРМ мигрирован, введен в домен, присутствует в Комплексе (puppet-agent настроен) и готов к работе.

30.34 Миграция с РОСА “Кобальт” с использованием USB

В качестве исходного состояния при миграции на РОСА “Хром” рассматривается АРМ под управлением ОС РОСА “Кобальт” с локальной УЗ и доменной УЗ. У всех пользователей есть данные, которые размещены в домашней директории в стандартных папках (Рабочий стол, Загрузки и др.).

Для начала миграции дополнительно нужно выполнить несколько предварительных действий:

1. на АРМ установить и настроить клиент puppet_agent;
2. в Комплексе настроить шаблон для миграции (рисунок 84);

30.35 ::sign-image

src: /image94.png sign: Рисунок 84 — Настройка шаблона подготовки — ::

3. в Комплексе настроить группу узлов с включенными классами (рисунок 85);

30.36 ::sign-image

src: /image95.png sign: Рисунок 85 — Настройка группы узлов — ::

4. к АРМ подключить накопитель USB (желательно более 500 Гб свободного пространства) с обязательным наименованием метки тома “usb-migrator”, который должен оставаться подключенным до конца миграции;

Примечание – На накопитель USB копируется зашифрованная резервная копия пользовательских данных и настроек системы, из которой после миграции проводится обратная распаковка. Также по требованию (по умолчанию включено) создается зашифрованный полный образ системы, на который можно откатиться в случае необходимости. Файлы на накопителе USB хранятся в папке с MAC-адресом мигрируемого АРМ. Содержимое накопителя USB рекомендуется хранить до тех пор, пока оно больше не понадобится для восстановления данных. После успешной миграции содержимое накопителя USB рекомендуется удалить для обеспечения безопасности.

5. в Комплексе настроить puppet-класс `rcc_cobalt2chrome_usb`, для чего выбрать пункт меню “Настройки Puppet ENC Классы”, найти и выбрать этот класс, перейти на вкладку “Параметр класса” для настройки смарт-класса (рисунок 86);

30.37 ::sign-image

src: /image96.png sign: Рисунок 86 — Параметры для настройки — ::

6. настроить два смарт-класса, для чего в секции “Поведение по умолчанию” включить флажок “Переопределить”, ввести значения и нажать кнопку :

   — rcc c2c create full image – параметр съемки полного образа системы (true – снять полный образ, false – не создавать образ) (рисунок 87);

30.38 ::sign-image

src: /image97.png sign: Рисунок 87 — Параметр rcc c2c create full image — ::

- rcc c2c saving sources – параметр, задающий дополнительные папки (указываются через пробел), которые нужно скопировать в зашифрованный архив и перенести в новую систему (рисунок 88);

30.39 ::sign-image

src: /image98.png sign: Рисунок 88 — Параметр rcc c2c saving sources — ::

7. изменить параметры класса для самой группы, для чего открыть пункт меню “Настройки Группы узлов”, выбрать нужную группу (в данном случае c2cUSB), перейти на вкладку “Puppet ENC”, перейти к секции “Параметры класса Puppet” внизу страницы для изменения, внести изменения и нажать кнопку ;

30.40 ::sign-image

src: /image99.png sign: Рисунок 89 — Изменение параметров для группы — ::

На рисунке 89 цифрой 1 обозначено значение параметра, которое задает необходимость сохранения полного образа системы, а цифрой 2 – значение параметра, которое задает дополнительные папки (через пробел) для сохранения в образе. Для этой настройки не следует указывать папки пользователя в /home/username, т.к. они уже включены в резервную копию. Настройка предназначена для переноса каких-либо нестандартных пользовательских и системных папок (настроек), но следует учитывать, что, если задать, например, папку /etc, то она будет сохранена, а затем распакована поверх /etc в установленной системе, что приведет к неработоспособности ОС, поэтому рекомендуется с осторожностью включать в образ дополнительные папки.

После выполнения всех действий можно осуществить процедуру миграции, состоящую из следующих шагов:

1. в Комплексе найти имя подлежащего миграции АРМ, включить рядом с его именем параметр, нажать кнопку и выбрать из выпадающего меню “Изменить группу”;
2. в открывшемся модальном окне выбрать в выпадающем списке “Группа узлов” группу c2cUSB, после этого нажать на ставшую активной кнопку (рисунок 90); выбранный АРМ будет включен в группу c2cUSB для миграции;

30.41 ::sign-image

src: /image100.jpg sign: Рисунок 90 — Выбор группы — ::

3. дождаться окончания выполнения манифеста на выбранном АРМ (запустится по времени или вручную), в процессе которого будут сохранены в зашифрованном виде все данные пользователей, настройки puppet-agent и создан полный образ системы на подключенный к АРМ внешний накопитель USB; по окончании будет выведено сообщение о завершении резервного копирования, как на рисунке 91;

30.42 ::sign-image

src: /image101.jpg sign: Рисунок 91 — Сообщение после резервного копирования — ::

4. нажать кнопку и перезагрузить компьютер;
5. в процессе перезагрузки войти в BIOS/UEFI и выставить загрузку по сети (PXE) или нажать комбинацию клавиш (зависит от производителя материнской платы) и в BOOT MENU выбрать загрузку по сети; начнется загрузка вспомогательного образа с сервера PXE;
6. после загрузки по сети выбрать пункт меню “Control Center Discovery Image” (рисунок 92);

30.43 ::sign-image

src: /image102.jpg sign: Рисунок 92 — Выбор типа загрузки — ::

7. после успешной загрузки узла и регистрации на сервере появится сообщение об успешной отправке данных на сервер Комплекса (рисунок);

30.44 ::sign-image

src: /image103.jpg sign: Рисунок 93 — Сообщение об успешной загрузке — ::

8. в Комплексе перейти в пункт меню “Узлы Обнаруженные узлы”, выбрать в рабочей области требуемый АРМ и нажать кнопку (рисунок 94);

30.45 ::sign-image

src: /image104.png sign: Рисунок 94 — Выбор сетевой установки для АРМ — ::

9. в открывшемся окне (рисунок 95) выбрать ранее настроенную группу узлов c2cUSB и нажать кнопку ; сервер Комплекса передаст АРМ все нужные настройки для загрузки и установки системы РОСА “Хром” по сети;

30.46 ::sign-image

src: /image105.jpg sign: Рисунок 95 — Включение АРМ в преднастроенную группу — ::

10. АРМ начнет перезагрузку, после чего опять должен загрузиться по сети (PXE); для дальнейшей установки ОС выбрать пункт “Kickstart Rosa PXElinux” (для режима MBR/Legacy BIOS) (рисунок 96);

30.47 ::sign-image

src: /image106.jpg sign: Рисунок 96 — Выбор варианта загрузки — ::

11. после этого на мигрируемом АРМ начнется загрузка и установка ОС РОСА “Хром”, занимающая определенное время (рисунок 97);

30.48 ::sign-image

src: /image107.jpg sign: Рисунок 97 — Установка ОС РОСА “Хром” — ::

12. после окончания установки АРМ будет перезагружен, можно убрать загрузку в BIOS по сети (PXE) и выставить загрузку с жесткого диска, после чего должна загрузиться ОС РОСА “Хром” (рисунок 98);

30.49 ::sign-image

src: /image108.jpg sign: Рисунок 98 — Загрузка РОСА “Хром” — ::

Следует обратить внимание, что после первой загрузки РОСА “Хром” не нужно входить под УЗ пользователя, так как в это время копируются пользовательские данные, а по окончании будет выполнена перезагрузка в автоматическом режиме. На экране входа отобразятся локальные пользователи, которые были ранее в ОС РОСА “Кобальт” (рисунок 99);

30.50 ::sign-image

src: /image90.png sign: Рисунок 99 — Окно входа — ::

После выполненных шагов АРМ включен в домен, и можно входить как под доменной УЗ, так и под УЗ локального пользователя. Клиент puppet-agent уже настроен и работает с ключами от АРМ до миграции. На сервере Комплекса он будет присутствовать в списке узлов под старым именем (рисунок 100).

30.51 ::sign-image

src: /image109.png sign: Рисунок 100 — АРМ под новой ОС в списке узлов — ::

Теперь USB-накопитель можно извлечь из компьютера.

Ввиду того, что узел после окончания процедуры остался в группе миграции, его необходимо удалить из группы, как это показано на рисунке 101.

30.52 ::sign-image

src: /image92.png sign: Рисунок 101 — Удаление узла из группы миграции — ::

Кроме того, на вкладке “Узлы” в перечне узлов присутствует промежуточный узел, используемый при миграции и который следует удалить, выбрав из списка действие “Удалить” в соответствующем столбце. Для подтверждения удаления необходимо нажать кнопку в появившемся модальном окне.

В результате проделанных действий АРМ мигрирован, введен в домен, присутствует в Комплексе (puppet-agent настроен) и готов к работе.

31

ГЛОБАЛЬНЫЕ ПАРАМЕТРЫ

РОСА Центр Управления может использовать два типа параметров – глобальные параметры (доступные из любого манифеста) и параметры класса (ограниченные одним классом Puppet). Они могут быть добавлены через Комплекс несколькими способами.

Рекомендуется использовать параметры классов там, где это возможно, так как это упрощает разработку, использование и совместное использование модулей и классов Puppet. Класс может четко указывать, какие параметры он ожидает, предоставлять разумные значения по умолчанию и позволять пользователям переопределять их. Комплекс также может автоматически импортировать информацию о параметрах класса, что упрощает использова новых классов без необходимости знать и вводить точные имена глобальных параметров.

Работа с глобальными параметрами осуществляется через пункт меню “Настройки Глобальные параметры”. Для редактирования параметра нужно нажать на его имя, а для создания нового глобального параметра – кнопку (рисунок 102). Для глобального параметра необходимо задать имя, тип, значение и, при необходимости, скрыть значение, установив соответствующий флажок.

31.1 ::sign-image

src: /image110.png sign: Рисунок 102 — Глобальные параметры — ::

32

ANSIBLE

Модуль Ansible позволяет осуществлять автоматизированное управление конфигурациями контролируемых узлов РОСА Центр Управления путем дистанционного запуска плейбуков на этих узлах.

> Примечание – По умолчанию Ansible подключается к управляемым узлам по протоколу SSH.

В общем случае плейбук, запущенный на управляемом узле, выполняет по очереди заданный набор всех ролей Ansible, которые были выбраны пользователем для этого узла. При этом каждая роль Ansible представляет собой отдельный исполняемый командный сценарий, осуществляющий определенную настройку конфигурации узла.

32.1 Общие параметры Ansible

Интерфейс РОСА Центр Управления предоставляет пользователю возможность для настройки следующих основных параметров Ansible:

- Тай-маут отчета timeout – временной интервал (в минутах), предназначенный для формирования отчета Ansible с результатами выполнения плейбука. Значение по умолчанию: 30;
- Тип подключения – тип (протокол) подключения Ansible к управляемым узлам для дистанционного запуска плейбуков. Значение по умолчанию: SSH;
- Уровень детализации по умолчанию – уровень детализации записей в журнале о процессе выполнения плейбука Ansible;
- Тайм-аут после подготовки – временной интервал (в секундах) после развертывания нового узла, предназначенный для первичного выполнения заданных ролей Ansible на новом узле. Значение по умолчанию: 360;
- Путь до приватного ключа – путь к файлу с закрытым ключом SSH.

Значения общих параметров Ansible доступны пользователю для просмотра и редактирован
во вкладке “Ansible” в меню “Управление Параметры” панели навигации (рисунок 103).

32.2 ::sign-image

src: /image111.png sign: Рисунок 103 — Общие параметры Ansible — ::

Для редактирования определенного параметра надо нажать соответствующую пиктограмму
(карандаш), после чего указать необходимое значение.

32.3 Импорт ролей и переменных Ansible

Перечень импортированных ролей Ansible отображается в меню “Настройки Ansible Роли” панели навигации (рисунок 104), а список используемых переменных – в меню “Настройки Ansible Переменные”.

32.4 ::sign-image

src: /image113.png sign: Рисунок 104 — Роли Ansible — ::

Для импорта дополнительной роли или переменной требуется нажать кнопку … на соответствующей странице интерфейса и выбрать необходимый источник.

> Примечание – При импорте переменных Ansible дополнительно автоматически будут импортированы все роли, связанные с этими переменными и при этом отсутствующие в перечне ранее импортированных ролей.

Для создания переменной Ansible в рабочей области по меню “Настройки Ansible Переменные” нужно нажать кнопку `Ansible`.

Далее следует ввести параметры переменной в полях “Ключ”, “Описание”, выбрать “Роль Ansible”, а также переопределить параметры по умолчанию и задать валидаторы ввода (рисунок 105).

Нажать кнопку .

32.5 ::sign-image

src: /image114.png sign: Рисунок 105 — Параметры новой переменной Ansible — ::

32.6 Присвоение ролей Ansible

Выполняемые роли Ansible могут быть присвоены пользователем как отдельному управляемому узлу, так и группе узлов.

Следует обратить внимание, что роли Ansible, присвоенные группе узлов, также будут автоматически присвоены каждому отдельному узлу в этой группе. При этом изменение группы узла приведет к изменению набора ролей Ansible, ранее присвоенных узлу через группу.

32.7 Присвоение ролей Ansible отдельному узлу

Для присвоения ролей Ansible узлу необходимо перейти в меню “Узлы Все Узлы” панели навигации и нажать наименование (доменное имя) необходимого узла.

На экране появится интерфейс с подробными параметрами выбранного узла, в котором нужно нажать кнопку и затем перейти на вкладку “Роли Ansible” (рисунок 106).

32.8 ::sign-image

src: /image115.png sign: Рисунок 106 — Присвоение ролей Ansible узлу — ::

В списке доступных ролей Ansible последовательно нажимают соответствующую пиктограмму (плюс) для присвоения всех необходимых ролей узлу. При этом добавленные роли отобразятся в списке присвоенных ролей Ansible.

Для удаления определенной роли из списка присвоенных ролей Ansible нажимают соответствующую пиктограмму (минус). При этом роли, присвоенные узлу через группу узлов, удалить из этого списка нельзя.

После присвоения всех необходимых ролей Ansible узлу нужно нажать кнопку .

32.9 Выполнение ролей Ansible

Выполнение ролей Ansible на управляемых узлах осуществляется путем дистанционного запуска плейбуков на этих узлах.

Плейбук Ansible может запускаться как пользователем Комплекса вручную, так и в автоматическом режиме по заданному расписанию. При этом процесс запуска плейбука может осуществляться на отдельном узле или одновременно на нескольких узлах, входящих в определенную группу.

33

PUPPET

33.1 Классы

С помощью модуля управления конфигурациями Puppet производится назначение предустановлен
классов для узлов, реализуемых через классы Puppet.

Для назначения классов разработанных модулей с использованием веб-интерфейса РОСА Центр Управления необходимо в меню “Настройки ® Puppet ENC Классы” нажать кнопку …. В результате отобразится перечень классов (рисунок 107).

33.2 ::sign-image

src: /image117.png sign: Рисунок 107 — Импортированные классы Puppet — ::

Для определения файла с описанием действий, которые нужно выполнить на узле или группе узлов, и его определения для дальнейшего выполнения необходимо воспользоваться меню “Узлы Все Узлы” или “Настройка Группы узлов” в режиме редактирования узла или группы соответственно и на вкладке “Puppet ENC” выбрать классы во “Включенные классы” из перечня “Доступных классов”, используя пиктограммы (плюс) и (минус) (рисунок 108).

33.3 ::sign-image

src: /image118.png sign: Рисунок 108 — Выбор классов Puppet — ::

33.4 Окружения

Для просмотра и редактирования окружений Puppet следует перейти в меню “Настройки Puppet ENC Окружения”. Для создания нового окружения нажимают кнопку Puppet. Далее в открывшейся рабочей области вводят имя окружения, выбирают из соответствующ вкладок местоположение и организацию и нажимают кнопку для сохранения. Чтобы удалить окружение, в строке списка выбирают действие и в модальном окне подтверждения действия нажимают кнопку . В этой же рабочей области можно перейти сразу к работе с классами Puppet, описанной в п. Применение классов настоящего документа.

33.5 Применение классов

Для определения классов Puppet требуется перейти в меню “Настройки Puppet ENC Классы” и выбором класса из списка просматривать и редактировать его с использованием параметров класса (п. Параметры класса). В этой же рабочей области можно привязать

класс к группам узлов, используя пиктограммы (плюс) и (минус). Для сохранения изменений нажимают кнопку .

Перед применением классов Puppet следует убедиться, что разрешена их активация в настройках группы узлов. Глобальный статус класса Puppet можно отследить на вкладке “Параметр класса” (п. Параметры класса). Необходимо включить флажок “Переопределить” в разделе “Поведение по умолчанию”. Этот параметр отвечает за доступ к настройкам (включению) класса Puppet в рамках группы узлов.

Проверить включение класса Puppet можно в свойствах выбранной группы узлов на вкладке “Puppet ENC” (п. Параметры класса). В разделе “Параметры классов Puppet” должно быть указано значение True для выбранного класса Puppet.

33.6 Группы конфигураций

В меню “Настройка Puppet ENC Группы конфигураций” предоставляется возможность одноэтапного метода привязки нескольких классов Puppet к узлу или к группе узлов. Для этого требуется нажать кнопку , ввести имя группы, выбрать классы во “Включенные классы” из перечня “Доступных классов”, используя пиктограммы (плюс) и (минус). Далее нажимают кнопку для сохранения изменений (рисунок 109).

33.7 ::sign-image

src: /image119.png sign: Рисунок 109 — Редактирование группы конфигураций — ::

Для привязки группы конфигураций в меню “Узлы Все Узлы” или “Настройка Группы узлов” в режиме редактирования узла или группы соответственно и на вкладке “Puppet ENC” выбрать группы конфигураций во “Включенные группы конфигураций” из перечня “Доступных групп конфигураций”, используя пиктограммы (плюс) и (минус).

33.8 Параметры класса

Параметры класса, привязанные к классам Puppet (п. Применение классов), переопределяются в меню “Настройки Puppet ENC Параметры класса”.

В блоке данных “Детали параметра” вводят требуемые данные о параметрах:

— в поле “Описание” – краткое описание параметра;

В блоке данных “Поведение по умолчанию” – признак переопределения по умолчанию, тип, значение по умолчанию, признак исключения из классификации, признак скрытой переменной;

В блоке “Дополнительный валидатор входных данных”:

— признак обязательности, тип и правило валидатора;

— при выборе признака переопределения по умолчанию предоставляется возможность настроить порядок разрешения значений в блоке данных “Приоритет порядка атрибутов”, а также указать конкретные сопоставители в блоке с одноименным названием.

Для сохранения переменной нажимают кнопку .

33.9 Локальные репозитории

Для обеспечения оперативной установки и обновления ПО групп узлов создаются локальные репозитории на базе интернет-репозиториев посредством следующих классов Puppet:

— rcc_srv_repo – для конфигурации сервера локального репозитория;
— rcc_srv_repo_alt_10 – для ОС Альт Рабочая станция 10;
— rcc_srv_repo_astra_17 – для ОС Astra Linux SE 1.7;
— rcc_srv_repo_redos_73 – для ОС РЕД ОС 7.3;
— rcc_srv_repo_rosa_2021_1 – для ОС РОСА версии 2021.1.

Для привязки классов при создании или редактировании групп узлов (п. Создание группы узлов) на вкладке “Классификатор узлов Puppet” включают класс rcc_srv_repo и один из классов для ОС из списка “Доступные классы” во “Включенные классы” и нажимают кнопку .

Чтобы задать параметры классов для работы с репозиториями, нужно перейти в меню “Настройки Puppet ENC Классы”, в рабочей области выбрать имя класса и на вкладке “Параметр класса” выбрать для редактирования параметр по маске с постфиксом и внести изменения в раздел “Поведение по умолчанию”:

— *_enable – для включения класса включить параметр в поле “Изменить”, задать логическое значение “true” в поле “Значение по умолчанию”;
— *_cron_d – для задания периода синхронизации в днях включить параметр в поле “Изменить”, задать число дней в поле “Значение по умолчанию” в виде строки;
— *_cron_h – для задания периода синхронизации в часах включить параметр в поле “Изменить”, задать число часов в поле “Значение по умолчанию” в виде строки;
— *_cron_m – для задания периода синхронизации в минутах включить параметр в поле “Изменить”, задать число дней в поле “Значение по умолчанию” в виде строки.
— Для сохранения нажать кнопку .

Для подключения узлов к локальным репозиториям и работы с ними используются следующие классы Puppet:

— rcc_client_repo_alt_10 – для ОС Альт Рабочая станция 10;
— rcc_ client_repo_astra_17 – для ОС Astra Linux SE 1.7;
— rcc_ client_repo_redos_73 – для ОС РЕД ОС 7.3;
— rcc_ client_repo_rosa_2021_1 – для ОС РОСА версии 2021.1.

Для включения классов необходимо перейти в меню “Настройки Puppet ENC Классы”, в рабочей области выбрать имя класса и на вкладке “Параметр класса” выбрать для редактирования параметр с постфиксами *_enable или *_url и внести изменения в раздел “Поведение по умолчанию” соответственно:

— *_enable – для включения класса включить параметр в поле “Изменить”, задать логическое значение “true” в поле “Значение по умолчанию”;
— *_url – для задания адреса локального репозитория включить параметр в поле “Изменить”, задать, например, строку “http://repo.rosa.int/alt” в поле “Значение по умолчанию”.

Для сохранения нажать кнопку .

33.10 Управление пакетами

Для управления установкой, обновлением и удалением отдельных сторонних пакетов в Комплексе используется класс rcc_package_manager.

В этом классе применяются три параметра:

— pkgs_to_install - массив пакетов для установки, например [“htop”, “mc”, “nmap”];
— pkgs_to_remove - массив пакетов для удаления, например [“jag”, “curl”];
— pkgs_to_update - массив пакетов для обновления, например [“openssl”, “sshfs”].

Массивы могут состоять как из одного, так и из множества элементов. Также массив может быть пустым, если нет необходимости в каких-либо из трех действий, – в этом случае заполняется как `[""]`.

На основе элементов массивов при следующем запуске агента Комплекса формируются соответствующие задания по установке/обновлению/удалению пакетов. При этом, в зависимости от типа используемой ОС, автоматически применяется соответствующий пакетный менеджер (dnf/apt/aptrpm).

Следует обратить внимание, что массивы должны представлять собой непересекающиеся множества. Иначе, интерпретатор декларативного языка описания состояний не сможет определить в каком состоянии должен находиться пакет (например, одновременно в разных массивах пакет должен быть в последней версии, но при этом должен отсутствовать).

Глобальное переопределение параметров класса rcc_package_manager по умолчанию проводится в меню “Настройки Puppet ENC Параметры класса” (рисунок 110).

33.11 ::sign-image

src: /image120.png sign: Рисунок 110 — Переопределение параметров класса rcc_package_manager — ::

Переопределение параметров для группы узлов или отдельного узла осуществляется в соответствующих настройках групп или узлов (рисунок 111).

33.12 ::sign-image

src: /image121.png sign: Рисунок 111 — Параметры класса для группы или узла — ::

34

УПРАВЛЕНИЕ СОДЕРЖИМЫМ

В контексте РОСА Центр Управления содержимое определяется как программное обеспечение, установленное в ОС. Это включает, помимо прочего, базовую ОС, службы промежуточного ПО и приложения конечных пользователей. С помощью Комплекса можно управлять различными типами содержимого на каждом этапе жизненного цикла ПО.

> Примечание – Функции управления содержимым Комплексу предоставляет плагин Katello. Настоящее руководство может быть использовано только в том случае, если установлен плагин Katello.

35

УПРАВЛЕНИЕ ПОДПИСКАМИ

Комплекс управляет содержимым, позволяет хранить содержимое Red Hat, Deb, Yum и организовывать их различными способами через механизм управления подписками.

Импорт манифеста подписки для предоставления доступа узлам к содержимому Red Hat осуществляется через пункт меню “Содержимое Подписки” нажатием на кнопку .

В появившемся модальном окне необходимо на вкладке “Манифест” задать имя файла манифеста подписки и нажать кнопку (рисунок 112).

35.1 ::sign-image

src: /image122.png sign: Рисунок 112 — Импорт манифеста подписки — ::

После процедуры импорта на вкладке “Журнал манифеста” будут отображены данные об импорте.

На вкладке “Конфигурация CDN” через географически распределенную серию статических веб-серверов можно получить доступ к содержимому и исправлениям Red Hat, предназначенным для использования ОС. Доступное подмножество CDN настраивается с помощью содержимого, доступного с помощью указания в поле URL сервера `https://cdn.redhat.com`.

Red Hat CDN защищена сертификатом проверки подлинности X.509, что гарантирует, что доступ к ней имеют только действительные пользователи.

Для удаления подписки Red Hat из манифеста подписки требуется нажать кнопку в рабочей области, в появившемся одноименном модальном окне нажать и подтвердить удаление.

Примечание – Если удалить манифест с клиентского портала Red Hat или в веб-интерфейсе Комплекса, все права для всех узлов содержимого будут удалены.

Добавление прочих подписок осуществляется с помощью кнопки в рабочей области окна “Подписки”.

Для массового удаления в строке каждой подписки, которую требуется удалить, нужно установить соответствующий параметр, нажать кнопку , а затем подтвердите удаление.

36

ТИПЫ СОДЕРЖИМОГО

С помощью РОСА Центр Управления можно импортировать и управлять многими типами контента.

Например, Комплекс поддерживает следующие типы контента:

- пакеты RPM – импорт из любого репозитория, например Red Hat, SUSE и пользовательских репозиториев. Сервер Комплекса загружает пакеты RPM и сохраняет их локально. Эти репозитории и их пакеты RPM можно использовать в представлениях содержимого;
- пакеты Deb – импорт из репозиториев, например, для Debian или Ubuntu. Также можно импортировать отдельные пакеты Deb или синхронизировать пользовательские репозитории и использовать их в представлениях содержимого;
- деревья Kickstart – импорт для подготовки узла сети. Новые ОС получают доступ к этим деревьям Kickstart по сети для использования в качестве базового содержимого для их установки. Комплекс содержит предопределенные шаблоны Kickstart, но можно создавать и собственные шаблоны.
- шаблоны подготовки – для подготовки узлов под управлением EL на основе синхронизиро содержимого и Debian, Ubuntu или SUSE Linux Enterprise Server на основе локального установочного носителя. Комплекс содержит предопределенные шаблоны AutoYaST, Kickstart и Preseed, а также возможность создания собственных шаблонов, которые используются для подготовки ОС и настройки установки.
- ISO- и KVM-образы – загрузка носителей и управление ими для установки и подготовки. Например, Комплекс загружает, хранит и управляет ISO-образами и гостевыми образами для Red Hat Enterprise Linux и других ОС.
- пользовательский тип файла – любой тип файлов, таких как сертификаты SSL, ISO-образы и файлы OVAL.

Просмотр различных типов содержимого доступен через аккордеон меню панели навигации “Подписки Типы содержимого ” выбором пункта требуемого типа.

37

ПРОДУКТЫ

Содержимое из различных источников и пользовательское содержимое в Комплексе имеют сходство:

- связь между продуктом и его репозиториями остается прежней, и репозитории по-прежнему требуют синхронизации;
- для доступа узлов к продуктам требуется подписка, аналогичная подписке на продукты Red Hat. В Комплексе создается подписка для каждого создаваемого продукта.

Содержимое Red Hat уже организовано в продукты. Например, Red Hat Enterprise Linux Server является продуктом в РОСА Центр Управления. Репозитории для этого продукта состоят из различных версий, архитектур и надстроек. Для репозиториев Red Hat продукты создаются автоматически после включения репозитория.

Другое содержимое может быть организовано в продукты по усмотрению пользователя.

Для создания нового продукта нужно перейти в меню панели навигации “Содержимое Продукты” и нажать кнопку (Create product).

В рабочем окне “Создание продукта (Create product)” необходимо:

1. ввести имя продукта в поле “Название”
2. Комплекс автоматически заполняет поле “Метка” на основе того, что введено в поле “Название”;
3. (необязательно) в списке “Ключ GPG” выбрать ключ GPG для продукта;
4. (необязательно) в списке “SSL CA Cert” выбрать сертификат SSL CA для продукта;
5. (необязательно) в списке “SSL Client Cert” выбрать сертификат клиента SSL для продукта;
6. (необязательно) в списке “SSL Client Cert” выбрать ключ клиента SSL для продукта;
7. (необязательно) в списке “План синхронизации” выбрать существующий план синхронизаци или нажать для нового плана синхронизации в соответствии с требованиями продукта;
8. в поле “Описание” ввести описание продукта;
9. нажать кнопку (рисунок 113).

37.1 ::sign-image

src: /image123.png sign: Рисунок 113 — Создание продукта — ::

После создания продукта можно в окне просмотра продукта добавить репозитории, перейдя на вкладку “Репозитории”, или создать репозиторий для продукта, нажав кнопу (рисунок 114).

37.2 ::sign-image

src: /image124.png sign: Рисунок 114 — обавление репозитория к продукту — ::

38

УЧЕТНЫЕ ДАННЫЕ СОДЕРЖИМОГО

Прежде чем синхронизировать содержимое из внешнего источника, может потребоваться импортировать SSL-сертификаты или ключи в продукт. Это могут быть клиентские сертификаты и ключи или сертификаты ЦС для вышестоящих репозиториев, которые требуется синхронизироват

Если необходимы SSL-сертификаты и ключи для скачивания пакетов, можно добавить их в Комплекс.

Для добавления SSL-сертификатов и ключей нужно перейти в раздел “Содержимое Учетные данные содержимого”. В окне “Учетные данные содержимого (Content Credentials)” нажать кнопку (Create Content Credentials).

Далее необходимо задать параметры (рисунок 115):

1. в поле “Название” ввести имя;
2. в списке “Тип” выбрать “Сертификат SSL”;
3. в поле “Содержание учетных данных” вставить SSL-сертификат или нажать кнопку , чтобы загрузить SSL-сертификат.
4. нажать кнопку .

38.1 ::sign-image

src: /image125.png sign: Рисунок 115 — Создание учетных данных содержимого — ::

38.2 Импорт ключа GPG

В случае если источники используют подписанное содержимое, следует убедиться, что проведена настройка на проверку установки пакетов с помощью соответствующего ключа GPG. Это помогает гарантировать, что могут быть установлены только пакеты из авторизованных источников.

Большинство поставщиков услуг распространения RPM предоставляют свой ключ GPG на своем веб-сайте. Также можно извлечь ключ вручную из RPM, например:

1. загрузить копию пакета репозитория для конкретной версии на локальный компьютер:

   ```
   bash Terminal $ wget http://www.example.com/9.5/example-9.5-2.noarch.rpm
   ```

2. распаковать файл RPM без его установки:

   ```
   bash Terminal $ rpm2cpio example-9.5-2.noarch.rpm | cpio -idmv
   ```

3. ключ GPG расположен относительно извлечения в точке .etc/pki/rpm-gpg/RPM-GPG-KEY-EXAMPLE-95.

В Комплексе по аналогии с п. Учетные данные содержимого нужно перейти в раздел “Содержимое Учетные данные содержимого (Content Credentials)”. В окне “Учетные данные

содержимого (Content Credentials)” нажать кнопку (Create Content Credentials).

Далее необходимо задать параметры:

1. в поле “Название” ввести имя;
2. в списке “Тип” выбрать “Ключ GPG”;
3. в поле “Содержание учетных данных” вставить GPG-ключ или нажмите кнопку , чтобы загрузить GPG-ключ.
4. нажать кнопку .

Если репозиторий содержит содержимое, подписанное несколькими ключами GPG, необходимо ввести все необходимые ключи GPG в поле “Содержимое учетных данных содержимого с новыми строками между каждым ключом, например:

```
bash Terminal -----BEGIN PGP PUBLIC KEY BLOCK----- mQINBFy/HE4BEADttv2TCPzVrre+aJ9f
4aTUR/g+K1S0aqCU+ZS3Rnxb+6fnBxD+COH9kMqXHi3M5UNzbp5WhCdUpISXjjpU XIFFWBPuBfyr/FKRknFH15P+
=F6VG -----END PGP PUBLIC KEY BLOCK----- -----BEGIN PGP PUBLIC KEY BLOCK----- mQINBFw467U
OTFDlKuLkJx99ZYG5xMnBG47C7ByoMec1j94YeXczuBbynOyyPlvduma/zf8oB9e Wl5GnzcLGAnUSRamfqGUWcyM
=WPpI -----END PGP PUBLIC KEY BLOCK-----
```

39

АЛЬТЕРНАТИВНЫЕ ИСТОЧНИКИ СОДЕРЖИМОГО

Альтернативные источники содержимого определяют альтернативные пути для загрузки содержимого во время синхронизации. Само содержимое загружается из альтернативного источника, в то время как метаданные загружаются с сервера Комплекса. Альтернативный источник содержимого обычно используется для ускорения синхронизации, если содержимое находится в локальной файловой системе или в ближайшей сети. Альтернативные источники можно настроить для сервера Комплекса и смарт-прокси (Smart Proxy). Альтернативные источники необходимо обновлять после создания или после внесения изменений. Еженедельное задание cron обновляет все альтернативные источники содержимого. Также можно обновлять альтернативные источники содержимого вручную с помощью веб-интерфейса Комплекса. Альтернативные источники содержимого, связанные с сервером Комплекса или смарт-прокси (Smart Proxy), подключенные к нескольким организациям, влияют на все организации.

Существует три типа альтернативных источников содержимого:

- Пользовательский – загружают из любого вышестоящего репозитория в сети или файловой системе;
- Упрощенный – позволяют копировать информацию из вышестоящего репозитория с сервера Комплекса для выбранных продуктов; идеально подходят для ситуаций, когда подключение от Smart Proxy к вышестоящему репозиторию происходит быстрее, чем с сервера Комплекса;
- RHUI – загружают контент с сервера Red Hat Update Infrastructure.

Пользователи, не являющиеся администраторами, должны иметь следующие разрешения для управления альтернативными источниками содержимого:

- view_smart_proxies;
- view_content_credentials;
- view_organizations;
- view_products.

В дополнение к указанным выше разрешениям следует назначить разрешения, специфичные для альтернативных источников, в зависимости от действий, которые могут выполнять пользователи:

- view_alternate_content_sources;
- create_alternate_content_sources;
- edit_alternate_content_sources;
- destroy_alternate_content_sources.

Для создания нового альтернативного источника содержимого нужно перейти в меню панели навигации “Содержимое Альтернативные источники содержимого” и нажать кнопку

.

В рабочем окне “Добавить альтернативного источника содержимого” нужно по шагам, следуя кнопкам `Next` и `Back`, выбрать тип источника, тип содержимого, ввести имя и описание, выбрать смарт-прокси, ввести базовый путь, выбрать вариант аутентификации, проверить указанные параметры и нажать кнопку (рисунок 116).

39.1 ::sign-image

src: /image126.png sign: Рисунок 116 — Создание альтернативного источника содержимого — ::

40

УЗЛЫ СОДЕРЖИМОГО

Узлы содержимого управляют задачами, связанными с содержимым и подписками. Работа с узлами содержимого осуществляется через меню “Узлы Узлы содержимого” (рисунок 117). Для регистрации узла содержимого нужно нажать кнопку и далее действовать в соответствии с п. Регистрация существующих узлов.

40.1 ::sign-image

src: /image127.png sign: Рисунок 117 — Узлы содержимого — ::

41

КОЛЛЕКЦИИ УЗЛОВ

Коллекции узлов — это определяемые пользователем узлы, используемые для массовых действий, например таких как установка исправлений.

Для создания коллекции через меню “Узлы Коллекция узлов” в рабочей области нужно нажать кнопку `Create Host Collection (  )` и ввести в соответствующие поля название и описание коллекции, а также задать и снять ограничение на количество узлов коллекции с помощью параметра “Unlimited Hosts” (рисунок 118). После создания коллекции при дальнейшем редактировании на вкладке “Узлы” можно добавлять узлы.

41.1 ::sign-image

src: /image128.png sign: Рисунок 118 — Создание коллекции узлов — ::

42

ПЛАН СИНХРОНИЗАЦИИ

План синхронизации проверяет и обновляет содержимое в запланированные дату и время. В РОСА Центр Управления можно создать план синхронизации и назначить продукты этому плану.

Для создания плана нужно перейти в меню “Содержимое План синхронизации” и нажать кнопку .

Далее необходимо задать параметры плана (рисунок 119):

1. в полях “Название” и “Описание” ввести соответственно имя и краткое описание плана;
2. в списке “Интервал” выбрать интервал, с которым должен выполняться план;
3. в списках “Дата начала” и “Время начала” выбрать, когда следует начать выполнение плана;
4. нажать кнопку .

42.1 ::sign-image

src: /image129.png sign: Рисунок 119 — Создание плана синхронизации — ::

Для того чтобы план синхронизации выполнялся регулярно, необходимо его запустить, нажав кнопку и выбрав действие “Запустить”. Для удаления плана выбирают действие “Удалить”.

43

НАЗНАЧЕНИЕ ПЛАНА СИНХРОНИЗАЦИИ ПРОДУКТУ

План синхронизации проверяет и обновляет содержимое в запланированную дату и время. В РОСА Центр Управления можно назначить план синхронизации продуктам для регулярного обновления содержимого.

Для этого нужно перейти в меню “Содержимое План синхронизации”, выбрать план, перейти на вкладку “Продукты” и добавить один или несколько продуктов, которые будут синхронизироваться в соответствии с этим планом (рисунок 120).

43.1 ::sign-image

src: /image130.png sign: Рисунок 120 — Привязка продуктов к плану синхронизации — ::

> Примечания – Для работы с планами синхронизации рекомендуется: - добавлять планы синхронизации к продуктам и регулярно синхронизировать содержимое таким образом, чтобы снизить нагрузку на комплекс во время синхронизации, например, синхронизировать содержимое чаще, чем реже; - автоматизировать создание и обновление планов синхронизации с помощью Ansible Playbook; - распределить задачи синхронизации на несколько часов, чтобы снизить нагрузку на задачу, создав несколько планов синхронизации с помощью инструмента Custom Cron; - ограничивать параллелизм синхронизации: по умолчанию каждое задание синхронизации репозитория может получать до десяти файлов одновременно, что может быть скорректировано для каждого репозитория; увеличение лимита может повысить производительность, но может привести к перегрузке вышестоящего сервера или отказу от запросов.

44

СТАТУС СИНХРОНИЗАЦИИ

Для наблюдения за выполнением планов синхронизации можно воспользоваться пунктом меню “Содержимое Статус синхронизации”, в рабочей области которого в табличном виде перечислены все продукты, по которым проводилась или проводится в текущий момент синхронизация, с указанием времени начала, продолжительности, сведений о статусе и результатов (рисунок 121).

Для просмотра только текущих синхронизаций следует включить параметр в поле “Активный”.

44.1 ::sign-image

src: /image131.png sign: Рисунок 121 — Статус синхронизации — ::

45

ЖИЗНЕННЫЙ ЦИКЛ ПРИЛОЖЕНИЙ

45.1 Окружения жизненного цикла

Жизненный цикл приложений — это концепция, занимающая центральное место в функциях управления содержимым РОСА Центр Управления. Жизненный цикл приложения определяет, как конкретная ОС и ее программное обеспечение выглядят на определенном этапе.

Например, жизненный цикл приложения может быть простым: только стадия разработки и стадия производства.

Более сложный жизненный цикл приложения может состоять из дополнительных этапов, таких как этап тестирования или бета-версия. Это добавляет дополнительные этапы к жизненному циклу приложения:

- развитие;
- тестирование;
- бета-версия;
- производство.

РОСА Центр Управления предоставляет методы для настройки каждого этапа жизненного цикла приложения в соответствии с требуемыми спецификациями.

Каждый этап жизненного цикла приложения в Комплексе называется окружением. В каждом окружении используется определенный набор содержимого. Комплекс определяет эти коллекции содержимого как представление содержимого. Каждое представление содержимого действует как фильтр, в котором можно определить, какие репозитории и пакеты следует включить в определенное окружение. Это позволяет определить определенные наборы содержимого для каждого окружения.

Например, для почтового сервера может потребоваться только простой жизненный цикл приложения, в котором есть сервер производственного уровня для реального использования и тестовый сервер для опробования новейших пакетов почтового сервера. Когда тестовый сервер пройдет начальную фазу, можно настроить сервер производственного уровня для использования новых пакетов.

Другой пример — жизненный цикл разработки программного продукта. Чтобы разработать новое программное обеспечение в окружении разработки, нужно протестировать его в окружении контроля качества, предварительно выпустив его в виде бета-версии, а затем выпустить ПО в качестве приложения производственного уровня.

Для создания окружения жизненного цикла следует перейти в меню “Содержимое Жизненный цикл Окружения жизненного цикла” и нажать кнопку `Create Environment Path (  )`.

Для нового окружения нужно ввести параметры в поля (рисунок 122):

- Название – имя окружения;
- Метка – генерируется автоматически в зависимости от содержания “Названия”;
- Описание – описания окружения.

Нажать кнопку .

45.2 ::sign-image

src: /image132.png sign: Рисунок 122 — Создание окружения — ::

45.3 Представления

РОСА Центр Управления использует представления содержимого, чтобы предоставить узлам доступ к специально подобранному подмножеству содержимого. Для этого необходимо определить, какие репозитории требуется использовать, а затем применить к содержимому определенные фильтры.

Общая схема создания представлений содержимого для фильтрации и создания снимков выглядит следующим образом:

1. создать представление содержимого;
2. добавить один или несколько репозиториев, необходимые в представлении содержимого;
3. (необязательно) создать один или несколько фильтров для уточнения содержимого представления содержимого;
4. (необязательно) устранить все зависимости пакетов для представления содержимого;
5. опубликовать представление содержимого;
6. (необязательно) привязать представление содержимого в другое окружение.
7. присоединить узел содержимого к представлению содержимого.

Если репозиторий не связан с представлением содержимого, данные не будут переданы, и ОС, зарегистрированные в нем, не смогут получать обновления.

Узел может быть связан только с одним представлением содержимого. Чтобы связать узел с несколькими представлениями содержимого, необходимо создать составное представление содержимого.

Представление содержимого — это специально подобранное подмножество содержимого, к которому могут получить доступ узлы. Создав представление содержимого, можно определить версии программного обеспечения, используемые конкретным окружением или сервером Smart Proxy.

Каждое представление содержимого имеет набор репозиториев в каждом окружении. Сервер Комплекса хранит эти репозитории и управляет ими. Например, можно создать представления содержимого следующими способами:

- представление содержимого со старыми версиями пакетов для рабочего окружения и другое представление содержимого с более новыми версиями пакетов для окружения разработки;
- представление содержимого с репозиторием пакетов, необходимым для ОС, и другое представление содержимого с репозиторием пакетов, необходимым для приложения;
- составное представление содержимого для модульного подхода к управлению представлениями содержимого, т.е. использовать одно представление для управления ОС и другое для управления приложением. При создании составного представления содержимого, объединяющего оба представления содержимого, создается новый

репозиторий, объединяющий репозитории из каждого представления содержимого. Тем не менее, репозитории для представлений содержимого по-прежнему существуют, и ими можно управлять отдельно.

Представление Организации по умолчанию — это управляемое приложением представление содержимого для всего содержимого, синхронизированного с Комплексом. Возможно зарегистрир узел в окружении Library в Комплексе, чтобы использовать представление Организации по умолчанию без настройки представлений содержимого и окружений жизненного цикла.

Продвижение представления содержимого в разных окружениях позволяет при преобразова представления содержимого из одного окружения среды в следующее окружение в жизненном цикле приложения Комплекса обновлять репозиторий и публиковать пакеты.

Для создания представления окружения необходимо перейти в меню панели навигации “ “Содержимое Жизненный цикл Представления” и нажать кнопку .

В появившемся модальном окне для нового представления нужно задать параметры в полях (рисунок 123):

— Имя – имя окружения;
— Метка – генерируется автоматически в зависимости от содержания “Названия”;
— Описание – описания окружения;
— Тип – выбрать представление содержимого или представление составного содержимого;
— (необязательно) если требуется автоматически разрешать зависимости при каждой публикации этого представления содержимого, нужно установить параметр “Решить зависимости”;

Примечание – Решение зависимостей замедляет время публикации и может игнорировать все используемые фильтры представления содержимого. Это также может привести к ошибкам при разрешении зависимостей для исправлений.

Нажать кнопку .

45.4 ::sign-image

src: /image133.png sign: Рисунок 123 — Создание представления содержимого — ::

После создания представления можно перейти к заданию публикации версий, репозиториев и фильтров.

В списке представлений в меню панели навигации “Жизненный цикл Представления” нажать на имя представления (рисунок 124).

45.5 ::sign-image

src: /image134.png sign: Рисунок 124 — Просмотр представления содержимого — ::

На вкладке “Сведения” приведены параметры представления, которые можно редактироват нажатием на пиктограмму (карандаш).

На вкладке “Версия” по кнопке задают публикацию и продвижение версии представления по шагам, используя кнопки `Back` и `Next`. Для публикации нажать `Finish`.

На вкладке “Репозитории” подключают пользовательские репозитории или репозитории Red Hat.

На вкладке “Фильтры” создаются фильтры нажатием на кнопку .

В появившемся модальном окне (рисунок 125) нужно задать параметры фильтра в соответствующих полях:

- имя фильтра;
- тип содержимого;
- тип включения: исключить или включить;
- описание фильтра.

Нажать кнопку .

После создания фильтра дополнительно необходимо задать правила фильтра в зависимости от выбранного типа содержимого при помощи кнопки `RPM`.

45.6 ::sign-image

src: /image136.png sign: Рисунок 125 — Создание фильтра — ::

На вкладке “Журнал” отображаются данные об истории публикации или продвижения представления окружения.

46

ОБЗОР

РОСА Центр Управления осуществляет в автоматическом режиме постоянный сбор данных о значениях разнородных элементов информации (параметров, статусов, событий и тому подобных), связанных с функционированием Комплекса. При этом каждый контролируемый элемент информации является отдельной метрикой наблюдения, а визуализация полученных данных осуществляется для пользователя на специально предназначенной панели наблюдения.

Наблюдение РОСА Центр Управления доступно пользователю Комплекса в меню “Наблюдение Обзор” панели навигации (рисунок 126).

46.1 ::sign-image

src: /image137.png sign: Рисунок 126 — Обзор — ::

Обзор содержит настраиваемый набор виджетов (модулей), отображающих информацию в графическом (диаграмма) и текстовом (таблица с данными) виде о состоянии управляемых узлов и иных объектов наблюдения РОСА Центр Управления.

Для просмотра подробной визуальной статистической информации об отдельных метриках мониторинга можно воспользоваться меню “Наблюдение Состояние узлов” панели навигации (рисунок 127).

46.2 ::sign-image

src: /image138.png sign: Рисунок 127 — Обзор состояний узлов — ::

47

ОПОВЕЩЕНИЯ О СОБЫТИЯХ

Оповещения (сообщения, предупреждения) о контролируемых событиях РОСА Центр Управления отображаются в интерфейсе Комплекса, а также (при необходимости и соответствующих настройках) могут быть отправлены пользователю по электронной почте.

Для просмотра списка полученных оповещений нужно нажать пиктограмму (колокол) на панели быстрого доступа, после чего для просмотра детальной информации о конкретном событии выбрать необходимое оповещение из общего перечня.

Следует обратить внимание, что в случае наличия сформированных и непрочитанных оповещений будет отображаться специальный индикатор красного цвета, который появится в правом верхнем углу пиктограммы (колокол).

Для автоматической рассылки оповещений по электронной почте сервер РОСА Центр Управл должен быть интегрирован с внешним почтовым SMTP-сервером или настроен в качестве локального почтового агента MTA (например, sendmail) во вкладке “Email”, доступной в меню “Управление Параметры” панели навигации. При этом используемые адреса электронной почты должны быть указаны в учетных записях пользователей Комплекса.

В свою очередь, в меню “Управление Пользователи” на вкладке “Почтовые предпочтения” каждый пользователь может выбрать только необходимые типы оповещений на основе событий (например, переход общего статуса узла в состояние сбоя (ошибки)), а для оповещений по расписанию (например, сводка аудита) указать частоту их получения по электронной почте. Кроме того, при необходимости пользователь вообще может отключить почтовую рассылку.

В общем случае управление оповещениями, связанными с событиями на узлах, осуществляе отдельно для каждого узла во вкладке “Дополнительно” (на странице с параметрами узла) через включение или отключение параметра “Узел|Включено”. При этом в момент возникновения контролируемого события на узле оповещается только владелец узла, который может быть как отдельным пользователем, так и группой пользователей.

48

ВЫЗОВЫ ЗАДАНИЙ

В РОСА Центр Управления реализован механизм вызова заданий в соответствии с выбранными шаблонами заданий, поисковым запросами, расписанием запуска и прочими параметрами, позволяющими получать данные о конфигурациях и состояниях.

В меню навигации “Наблюдение Задания” можно получить список выполненных, ранее запущенных или запланированных заданий с указанием статусов и статистики выполнения (рисунок 128). При нажатии на имя задания в рабочей области выдается подробный обзор о результатах выполнения и варианты дальнейших действий.

48.1 ::sign-image

src: /image142.png sign: Рисунок 128 — Вызовы заданий — ::

Для вызова или планирования нового задания необходимо нажать кнопку и в рабочей области определить его параметры, перемещаясь по вкладкам с помощью кнопок и (рисунок 129):

- категория задания;
- шаблон задания;
- целевые узлы, коллекции или группы узлов;
- фильтры и запросы;
- расписание;
- другие дополнительные параметры.

Затем нажать кнопку .

48.2 ::sign-image

src: /image143.png sign: Рисунок 129 — Параметры вызова задания — ::

49

ПРОЦЕССЫ

В РОСА Центр Управления реализована возможность управления процессами, касающимися непосредственно работы Комплекса.

Для получения статистических данных о процессах и возможности управления ими следует выбрать в меню навигации пункт “Наблюдение Задачи ЦУ Задачи” (рисунок 130). Выбрав один или несколько процессов, можно с помощью кнопки завершить, приостановить или принудительно завершить процесс. В столбце “Операция” списка процессов операции можно отметить и принудительно завершить в зависимости от их статуса.

49.1 ::sign-image

src: /image144.png sign: Рисунок 130 — Задачи РОСА Центр Управления — ::

Для просмотра данных о повторяющихся задачах РОСА Центр Управления нужно перейти в меню “Наблюдение Задачи ЦУ Повторяющиеся задачи”. Все ID процессов с описанием параметров показываются в табличном виде.

50

ФОРМИРОВАНИЕ ОТЧЕТА ИЗ ШАБЛОНА

РОСА Центр Управления предоставляет пользователю комплект предустановленных шаблонов отчетов, расположенных в меню “Наблюдение Отчеты Шаблоны отчетов” панели навигации.

Шаблон отчета представляет собой предопределенную структуру, которая предназначена для формирования итогового текстового отчета. Сформированный отчет будет содержать информацию, отображаемую в виде таблицы с данными.

При нажатии на имя шаблона отчета осуществляется переход к редактированию шаблона.

Запуск процесса формирования отчета из шаблона может осуществляться пользователем как вручную в текущий момент времени, так и в автоматическом режиме по заданному расписанию.

Следует обратить внимание, что сформированный отчет будет доступен для скачивания в браузере как файл в форматах CSV, JSON, YAML, HTML, а также (при необходимости и соответствующих настройках) отчет может быть отправлен указанным пользователям по электронной почте.

Для формирования отчета из шаблона нужно перейти в меню “Наблюдение Отчеты Шаблоны отчетов” панели навигации и нажать в строке требуемого шаблона отчета из общего перечня кнопку .

На экране появится интерфейс настройки параметров, в котором можно задать дату и время формирования отчета, в качестве опции установить флажок в поле “Отправить отчет по электронной почте” с указанием адресов электронной почты получателей отчета, задать “Выходной формат” файла и другие параметры фильтрации содержимого отчета.

Также для применения фильтров к отображаемым данным отчета вводят необходимый поисковый запрос (подраздел Поиск объектов), иначе в отчет будут включены все имеющиеся данные (рисунок 131).

50.1 ::sign-image

src: /image145.png sign: Рисунок 131 — Параметры формирования отчета — ::

После завершения настройки параметров формирования отчета нажимают кнопку . В результате на экране отобразится окно, предлагающее открыть (или сохранить) файл отчета в выбранном формате для удобства дальнейшей обработки в соответствующих редакторах. Пример сформированного отчета в CSV-формате приведен на рисунке 132.

Примечание – Процесс формирования отчета выполняется в фоновом режиме и в некоторых случаях может занимать продолжительное время.

50.2 ::sign-image

src: /image146.png sign: Рисунок 132 — Пример текстового отчета — ::

Сформированные отчеты о конфигурации узлов можно просматривать в меню “Наблюдение
 Отчеты Управление конфигурацией”.

51

АУДИТ ИЗМЕНЕНИЙ

Интерфейс РОСА Центр Управления предоставляет пользователю возможность для проведения аудита событий (изменений), произошедших в процессе функционирования Комплекса за определенный период времени. При этом регистрация отслеживаемых изменений осуществляется в журнале аудита согласно предустановленным системным правилам аудита.

Журнал аудита предназначен для просмотра и анализа произошедших изменений в РОСА Центр Управления и доступен пользователю Комплекса в меню “Наблюдение Аудит” панели навигации (рисунок 133).

51.1 ::sign-image

src: /image147.png sign: Рисунок 133 — Журнал аудита — ::

Журнал аудита содержит упорядоченный перечень произошедших изменений. При этом каждое событие аудита представлено в виде отдельной строки в общем перечне и содержит следующие сведения об изменении:

- тип изменения;
- объект изменения;
- имя пользователя, совершившего изменение;
- дата и время изменения.

При необходимости используют значения типа или объекта изменения для фильтрации общего перечня событий в журнале аудита.

Следует обратить внимание, что по умолчанию срок хранения событий аудита не указан, и, соответственно, никакие события из журнала аудита РОСА Центр Управления не будут автоматически удалены.

Тем не менее пользователь может установить произвольное количество дней, предназначен для хранения событий аудита, в качестве значения для параметра “Интервал сохраненных аудитов” во вкладке “Общие”, доступной в меню “Управление Параметры” панели навигации.

Кроме того, при необходимости и соответствующих настройках пользователь может получать от РОСА Центр Управления регулярные письма (оповещения) с подробными сводками аудита по электронной почте.

52

СБОР ФАКТОВ О КОНФИГУРАЦИИ

Автоматизированный сбор информации о программной и аппаратной конфигурациях узлов производится с использованием классов Puppet, при этом существует возможность дополнять собранную информацию записями на языке системы управления YAML.

Информация о конфигурации собирается на момент подключения узлов к Комплексу и содержит информацию о характеристиках аппаратного обеспечения узлов.

Перечень хранимых параметров аппаратного обеспечения может включать, например:

- BIOS: производитель, версия, дата;
- система: производитель, имя продукта, версия, серийный номер, уникальный идентификатор;
- материнская плата: производитель, имя продукта, серийный номер;
- платформа: производитель, тип, версия, серийный номер;
- процессор: семейство, производитель, версия, частота;
- оперативная память: максимальный объем, количество слотов, форм-фактор, скорость, производитель, серийный номер;
- диск: количество дисков в системе, съемный, модель, серийный номер, объем, тип диска, производитель;
- устройства PCI-шины: адрес, наименование для каждого из устройств;
- устройства USB-шины: адрес, наименование для каждого из устройств.

Непосредственно для просмотра всех фактов о конфигурациях необходимо воспользоваться пунктом меню “Наблюдение Факты”. При обращении к этому пункту отобразится список всех узлов со всеми собранными фактами. При нажатии на строку с именем составного факта для каждого из узлов отобразится информация о собранной первоначальной конфигурации (рисунок 134).

52.1 ::sign-image

src: /image148.png sign: Рисунок 134 — Перечень собранных фактов обо всех узлах — ::

Для получения всех фактов о конкретном узле нажимают на его имя (рисунок 135).

52.2 ::sign-image

src: /image149.png sign: Рисунок 135 — Перечень фактов об узле — ::

53

ОТСЛЕЖИВАНИЕ ИЗМЕНЕНИЙ АППАРАТНОЙ КОНФИГУРАЦИИ

Для отслеживания изменений аппаратной конфигурации на АРМ нужно назначить класс rcc_hardware_inventory группе узлов:

1. перейти в меню “Настройки Группы узлов”;
2. нажать кнопку ;
3. заполнить поле “Имя” (например, servers) и выбрать значение в списке “Окружение”;
4. нажать кнопку .

Будет создана группа узлов servers.

Далее необходимо перейти в созданную группу узлов servers и добавить на вкладке “Puppet ENC” два класса: rcc_hardware_inventory и rcc_software_inventory. Перед сохранением настроек классов следует убедиться, что они включены для группы узлов. Раздел для включения классов находится в нижней части текущего окна (рисунок 136).

Нажать кнопку .

53.1 ::sign-image

src: /image150.png sign: Рисунок 136 — Добавление классов в группу узлов — ::

Затем нужно перейти в меню “Узлы Все Узлы” и указать АРМ, который будет добавлен в созданную группу для отслеживания изменений в аппаратной конфигурации. В списке “Действия” требуется выбрать пункт “Изменить группу” (рисунок 137).

53.2 ::sign-image

src: /image151.png sign: Рисунок 137 — Смена группы для выбранных АРМ — ::

Далее следует нажать на выпадающий список “Группа узлов”, выбрать группу servers и нажать кнопку (рисунок 138).

53.3 ::sign-image

src: /image152.png sign: Рисунок 138 — Выбор группы узлов — ::

После этого АРМ будет добавлен в группу servers.

После запуска Puppet-агента на выбранных АРМ будет создана первоначальная конфигураци оборудования и установленного ПО на текущий момент.

Для проверки работы классов rcc_hardware_inventory и rcc_software_inventory нужно:

1. отключить ПК и добавить оперативную память (например, с 4 Гб до 8 Гб);

2. перезапустить ПК и войти под учетной записью пользователя;
3. после входа пользователя будет запущен Puppet-агент и изменения конфигурации АРМ отобразятся в Комплексе.

Для просмотра изменений можно войти в меню “Узлы Все Узлы”, выбрать ПК, на котором был изменен объем оперативной памяти, и выбрать пункт меню “Факты” через пиктограмму (три точки) (рисунок 139).

53.4 ::sign-image

src: /image154.png sign: Рисунок 139 — Переход в пункт меню “Факты” — ::

Далее с помощью строки поиска нужно найти класс rcc_hardware и нажать на changes_log.

На экран будут выведены параметры add и del, нажав на которые можно посмотреть журнал подключения или отключения оборудования на выбранном узле.

54

ИНВЕНТАРИЗАЦИЯ УЗЛОВ

Автоматизированная инвентаризация программной и аппаратной конфигураций узлов производит
с использованием соответствующих классов Puppet, при этом существует возможность дополнять собранную информацию записями на языке системы управления YAML.

Информация о конфигурации собирается на момент подключения узлов к Комплексу и содержит данные о характеристиках программного и аппаратного обеспечения узлов, которые можно посмотреть в одной рабочей области.

Для получения результатов инвентаризации узлов нужно перейти в панели меню “Наблюдение Факты”, в рабочей области отобразится перечень узлов с соответствующими фактами (рисунок 140).

54.1 ::sign-image

src: /image155.png sign: Рисунок 140 — Значения фактов — ::

Результаты инвентаризации аппаратного обеспечения узла содержатся в классе rcc_hardwar нажатием на который можно вывести на экран все факты о параметрах узла, перечисленные в п. Сбор фактов о конфигурации, и нажатием на параметры – их значения.

Результаты инвентаризации программного обеспечения узла содержатся в классе rcc_software, нажатием на который можно вывести на экран все факты о программном обеспечении, установленном на узле.

Факты о ПО содержат следующие параметры:

- installed – установленное ПО со значениями list (список ПО), last_update (время последнего обновления), num (количество ПО);
- recent – последнее установленное ПО со значениями list (список ПО), num (количество ПО);
- updates – подлежащее обновлению ПО со значениями list (список ПО), num (количество ПО).

55

УЧЕТ ЛИЦЕНЗИЙ

Модуль учета лицензий RCC_lic представляет собой набор фактов для сбора информации об используемых лицензиях, который может быть представлен в виде как shell-скрипта, так и в виде ruby-факта.

К факту предъявляются следующие требования:

- в имени факта должно быть уникальное имя (ключ) для лицензионного ПО;
- для удобства и поддержания единого подхода к организации кодовой базы факты предлагается располагать в каталоге rcc_lic используемого окружения;
- факт должен возвращать значения, перечисленные в таблице 3.

55.1 ::app-collapsible

55.2 label: “Таблица 3 - Значения факта RCC_lic”

#content

Имя

Значение

application::<app_code>::license::key

Ключ лицензии

application::<app_code>::license::start_time

Начало действия лицензии в формате ГГГГ-ММ-ДД

application::<app_code>::license::expiry_time

Окончание действия лицензии в формате ГГГГ-ММ-ДД

application::<app_code>::license::vendor

Производитель ПО

application::<app_code>::version::major

Мажорная версия лицензионного ПО

application::<app_code>::version::minor

Минорная версия лицензионного ПО

application::<app_code>::description

Описание ПО

application::<app_code>::name

Отображаемое имя лицензионного ПО

::

В поставке Комплекса представлены факты сбора информации о лицензиях для ОС РОСА “ХРОМ” и Kaspersky Endpoint Security для Linux.

56

РАБОТА С ПОДСИСТЕМАМИ

В Комплексе реализованы подсистемы, расширяющие работу Комплекса с ИТ-инфраструктурой организации:

- подсистема мониторинга;
- подсистема отображения;
- подсистема поиска и аналитики;
- управление мобильными устройствами.

Интеграция и настройка подсистем для работы в связке с интерфейсом РОСА Центр управлен описана в п.3.3 документа “РОСА Центр Управления”. Руководство системного администратора. Часть 1. Установка и настройка” (шифр РСЮК.10121-09 32 01).

57

ПОДСИСТЕМА МОНИТОРИНГА

Подсистема мониторинга РОСА Центр управления обеспечивает мониторинг ИТ-инфраструктуры организации, включающей большое число параметров сети, работоспособности и целостности серверов, виртуальных машин, приложений, сервисов, баз данных, веб-сайтов, облачных сред и многого другого.

Функционал подсистемы мониторинга реализуется через пункт главного меню “Мониторинг Панель мониторинга”.

Сведения, необходимые для эксплуатации подсистемы мониторинга РОСА Центр Управлени приведены в документе “РОСА Центр Управления. Руководство системного администратора. Часть 3-1. Эксплуатация. Подсистема мониторинга” (шифр РСЮК.10121-09 32 03-1).

58

ПОДСИСТЕМА ОТОБРАЖЕНИЯ

Подсистема отображения РОСА Центр управления позволяет запрашивать, отображать, оповещать о событиях и анализировать метрики, журналы и трассировки независимо от места их хранения.

Функционал подсистемы отображения реализуется через пункт главного меню “Мониторинг Настройка отображения”.

Сведения, необходимые для эксплуатации подсистемы отображения РОСА Центр Управлени приведены в документе “РОСА Центр Управления. Руководство системного администратора. Часть 4. Эксплуатация. Подсистема отображения” (шифр РСЮК.10121-09 32 04).

59

ПОДСИСТЕМА ПОИСКА И АНАЛИТИКИ

Подсистема поиска и аналитики РОСА Центр управления является распределенным механизмом поиска и аналитики, который поддерживает различные сценарии использования.

Функционал подсистемы поиска и аналитики реализуется через пункт главного меню “Мониторинг Настройка мониторинга Поиск и аналитика”.

Сведения, необходимые для эксплуатации подсистемы поиска и аналитики РОСА Центр Упра приведены в документе “РОСА Центр Управления. Руководство системного администратора. Часть 5. Эксплуатация. Подсистема поиска и аналитики” (шифр РСЮК.10121-09 32 05).

60

УПРАВЛЕНИЕ 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 классы Puppet функций и фактов описаны в пп. Управление пакетной базой-Получение информации о текущем состоянии:

- 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.

Описание интеграции РОСА Центр Управления с МУ приведено в п. 3.4 документа “РОСА Центр Управления. Руководство системного администратора. Часть 2. Эксплуатация” (шифр РСЮК.10121-09 32 02).

60.1 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.

60.2 ::app-collapsible

60.3 label: “Таблица 4 - Параметры класса”

#content

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

::

60.4 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.

60.5 ::app-collapsible

60.6 label: “Таблица 5 - Параметры класса”

#content

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

::

60.7 Управление блокировкой камеры

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

60.8 ::app-collapsible

60.9 label: “Таблица 6 - Параметры класса”

#content

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

::

60.10 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.

60.11 ::app-collapsible

60.12 label: “Таблица 7 - Параметры класса”

#content

Имя класса

Имя параметра

Тип параметра

Пример значения

Описание

r_mob_ch_pwd

password

строка

1234

ПИН-код блокировки МУ

::

60.13 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.

60.14 ::app-collapsible

60.15 label: “Таблица 8 - Параметры класса”

#content

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.

60.16 Управление GPS-приемником

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

60.17 ::app-collapsible

60.18 label: “Таблица 9 - Параметры класса”

#content

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.

60.19 Управление работой GSM-модема

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

60.20 ::app-collapsible

60.21 label: “Таблица 10 - Параметры класса”

#content

Имя класса

Имя параметра

Тип параметра

Пример значения

Описание

r_mob_gsm_control

gsm_enable

логическое значение

true

Управление состоянием GSM-модема:true – включен;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

60.22 Получение информации о текущем состоянии

Получение 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.

60.23 ::app-collapsible

60.24 label: “Таблица 11 - Параметры фактов”

#content

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

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}, {”essid”=>”CorpWIFI”, ”bssid”=>”08:43:F1:F6:35:2A”, ”signal_level”=>-81}]

Информация о ближайших сетях в диапазоне 2.4 ГГц. Представлена в виде 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

::

61

РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ

Периодическое создание резервной копии данных позволяет сохранять актуальную конфигурацию и различные типы данных РОСА Центр Управления, и в случае возникновения внештатной ситуации (в том числе при повреждении файлов ПО Комплекса) осуществлять восстановление необходимых данных из резервной копии.

Процедуры создания резервной копии и восстановления данных осуществляются пользователем Комплекса в терминальном окне узла РОСА Центр Управления.

61.1 Создание резервной копии данных

Резервная копия РОСА Центр Управления должна содержать следующие типы данных:

- дамп БД – файл, содержащий структуру и содержимое таблиц БД Комплекса;
- конфигурационные настройки Комплекса;
- сертификаты SSL сервера Puppet.

Для различных типов данных должны использоваться отдельные процедуры резервного копирования и восстановления.

Для создания дампа БД выполняют следующую команду:

```
bash Terminal foreman-rake db:dump
```

В результате выполнения этой команды будет создан файл с текущим дампом БД и будет указано расположение этого файла относительно каталога /etc/foreman. При необходимости отдельно копируют файл дампа БД на внешний носитель.

Для создания архива с конфигурацией РОСА Центр Управления выполняют следующую команду:

```
bash Terminal tar --selinux -czvf etc_foreman_dir.tar.gz /etc/foreman
```

где etc_foreman_dir.tar.gz – наименование файла для сохранения архива.

Для создания архива с сертификатами SSL сервера Puppet выполняют следующую команду:

```
bash Terminal tar --selinux -czvf var_lib_puppet_dir.tar.gz /etc/puppetlabs/
puppet/ssl
```

где var_lib_puppet_dir.tar.gz – наименование файла для сохранения архива.

Кроме того, при необходимости выполняют резервное копирование данных и конфигурацион файлов для сетевых сервисов DHCP и TFTP, а также систем оркестрации:

- для сервиса DHCP – каталог /etc/dhcp;
- для сервиса TFTP – каталог /var/lib/tftpboot;
- каталог с классами Puppet /etc/puppetlabs/code;
- каталог с плейбуками Ansible /usr/share/ansible/collections/ansible_collections.

61.2 Восстановление данных из резервной копии

В общем случае процедура восстановления данных осуществляется на том же узле, на котором была создана резервная копия.

В случае миграции РОСА Центр Управления на другой узел учитывают возможные различия в конфигурации между этими двумя узлами (например, использование различных IP-адресов и других сетевых параметров, изменение доменного имени узла и тому подобные).

Следует обратить внимание, что перед выполнением процедуры восстановления данных необходимо остановить работу сервера РОСА Центр Управления.

Для восстановления структуры и содержимого таблиц БД Комплекса выполняют следующую команду:

```
bash Terminal foreman-rake db:import_dump file=<                >
```

Для восстановления конфигурации РОСА Центр Управления выполняют команду:

```
bash Terminal tar --selinux -xzvf etc_foreman_dir.tar.gz -C
```

где etc_foreman_dir.tar.gz – наименование файла с архивом резервной копии.

Для восстановления сертификатов SSL сервера Puppet выполняют команду:

```
bash Terminal tar --selinux -xzvf var_lib_puppet_dir.tar.gz -C
```

где var_lib_puppet_dir.tar.gz – наименование файла с архивом резервной копии.

Кроме того, при необходимости выполняют восстановление данных и конфигурационных файлов для сетевых сервисов DHCP и TFTP, а также систем оркестрации:

- для сервиса DHCP – каталог /etc/dhcp;
- для сервиса TFTP – каталог /var/lib/tftpboot;
- каталог с классами Puppet /etc/puppetlabs/code;
- каталог с плейбуками Ansible
- /usr/share/ansible/collections/ansible_collections.

62

ТИПОВЫЕ ОШИБКИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

В таблице 12 приведен перечень типовых ошибок и способов их устранения в процессе эксплуатации Комплекса.

62.1 ::app-collapsible

62.2 label: “Таблица 12 - Типовые ошибки”

#content

Сообщение об ошибке

Действия администратора

При выполнении puppet-agent на клиентском АРМ или сервере puppet:Error: /File[/var/lib/pupp
Could not evaluate: Could not retrieve information from environment $yourenvironment source(s)
puppet://localhost/pluginfacts

На сервере Комплекса создать папку в каталоге модуля

При выполнении puppet-agent на клиентском АРМ или сервере puppet:Error: Could not retrieve catalog from remote server: Error 400 on SERVER: Failed when searching for node $nodename: No such file or directory @ dir_s_rmdir – /etc/puppetlabs/hiera/node/$nodename.yaml201508
5415-1802nxn.lock.

На сервере Комплекса выполнить в терминале команду:chown -R puppet:puppet /etc/puppetlab

При выполнении puppet-agent на клиентском АРМ или сервере puppet:SSL_connect returned=1 errno=0 state=SSLv3 read server session ticket A: sslv3 alert certificate revoked.

На клиентском АРМ выполнить в терминале команду:sudo rm -r /etc/puppetlabs/puppet/sslНа сервере Комплекса удалить сертификат проблемного узла.

При выполнении puppet-agent на клиентском АРМ или сервере puppet:Wrapped exception:SSL_
returned=1 errno=0 state=unknown state: certificate verify failed: [self signed certificate in certificate chain for /CN=Puppet CA: puppetmaster.example.com].

При выполнении puppet-agent на клиентском АРМ или сервере puppet:ERF12-0104 Общие ошибки подключения или SSL-соединения.

На сервере Комплекса:– если полагаться на групповую запись, то нужно убедиться, что foreman-proxy является членом группы puppet, и перезапустить foreman-proxy;– может потребоваться добавление строки в puppet.conf, чтобы убедиться, что она остается 0664:autosign = $ confdir / autosign.conf {mode = 664}

В веб-интерфейсе Комплекса:ERF12-0735 Невозможно удалить запись DHCP для% s

В веб-интерфейсе Комплекса:– убедиться, что следующие настройки (”Управление Параметры Аутентификация”) правильно установлены на экземпляре Комплекса: Сертификат SSL, Файл центр сертификации SSL, Закрытый ключ SSL;– убедиться, что имя узла прокси совпадает с тем, для которого был выдан сертификат (Общее имя), и, что время синхронизировано

с NTP на обоих серверах.– если в соединении отказано, то это значит, что Комплекс пытается открыть HTTP-соединение с прокси-сервером (обычно через порт 8443).1)Сначала проверить, что прокси действительно запущен:# service foreman-proxy status foreman-proxy (pid 10025) is running …2)Проверить наличие запрещающих правил межсетевых экранов между Комплексом и прокси-узлом, включая iptables или аналогичные, работающие на самом прокси;3) Попробовать выполнить тестовое подключение от сервера Комплекса к прокси, например,telnet proxy.example.co 8443.[Errno :: ECONNRESET]: сброс соединения одноранговым узлом обычно указывает, что интеллектуальный прокси-сервер работает по одному протоколу (например, HTTPS), а Комплекс пытается использовать другой (например, HTTP);4) Отредактировать смарт-прокси через интерфейс Комплекса и изменить протокол в поле URL. Если параметры ssl_* в /etc/foreman-proxy/settings.yml раскомментированы, то прокси – HTTPS, поэтому URL-адрес должен начинаться с "https://".[RestClient :: ResourceNotFound]: 404 Resource Not Found. – это может зависеть от контекста (прокси может возвращать 404, потому что некоторая запись не найдена), но может означать, что функция, которая, как ожидается, будет доступна на прокси (например, Puppet, DNS) фактически не включена в файле конфигурации или запущенном экземпляре.[RestClien :: RequestTimeout]: Тайм-аут запроса. – в этом случае нужно убедиться, что сервер Комплекса имеет сетевой доступ к интеллектуальному прокси-серверу:1) Попробовать использовать команды "telnet proxy.example.com 8443" или "curl -k https://proxy.example.com:8443/features".2) Проверить журналы. В /etc/foreman-proxy/settings.yml можно найти путь к файлу журнала прокси-сервера, обычно это: /var/log/foreman-proxy/proxy.log

В веб-интерфейсе Комплекса:ERF12-0735 Невозможно удалить запись DHCP. Общие ошибки подключения или SSL-соединения.

В веб-интерфейсе Комплекса:ERF12-2357 Невозможно установить запись DNS.

На сервере Комплекса:ERF12-4115 Общие ошибки или ошибки SSL-соединения.

На сервере Комплекса убедиться, что для всех файлов и родительских каталогов установлены достаточные права (например, чтение / выполнение).

В веб-интерфейсе Комплекса:ERF42-1994 Невозможно найти правильный метод аутентифика

В веб-интерфейсе Комплекса необходимо задать пароль, т.к., если получена эта ошибка, вероятно, что пароль отсутствует в определении пользовательского интерфейса Комплекса

В веб-интерфейсе Комплекса:ERF42-3305 Невозможно найти шаблон …

На сервере Комплекса проверить правильность с помощью "ls -l PATH" и, возможно, потребуется обновить представления, доступные в libvirt, с помощью "virsh pool-refresh"

В веб-интерфейсе Комплекса:ERF42-4505 Недопустимый путь.

В веб-интерфейсе Комплекса проверить параметр Default_variables_Lookup_Path в разделе "Дополнительно Настройки Puppet". Он должен быть определен как массив (например, [домен ОС группы узлов fqdn]). Если он определен с помощью начального скрипта, то надо убедиться, что он сохранен как массив, а не как строка

В веб-интерфейсе Комплекса:ERF42-4516 В методе отсутствуют необходимые параметры для перенаправления.

На сервере Комплекса это говорит об ошибке разработки, например, указано process_succes вместо process_success: success_redirect => host_path (@host): redirect_xhr => request.xhr?

В веб-интерфейсе Комплекса:ERF42-7495 ”Не удается найти пользователя foreman_admin при переключении контекста” или ”Не удается найти пользователя foreman_api_admin при переключении контекста”.

На сервере Комплекса восстановить пользователей, запустив в терминале команду:Foreman rake db: seed

В веб-интерфейсе Комплекса:ERF42-9958 ”Неизвестная поддержка управления питанием – невозможно продолжить”.

На сервере Комплекса отредактировать узел и создать новый сетевой интерфейс BMC, который должен указывать на интерфейс управления на узле с правильным IP-адресом и учетными данными. Требуется интеллектуальный прокси с включенной функцией BMC – это служба, с которой Комплекс свяжется для выполнения команд IPMI

В веб-интерфейсе Комплекса:ERF42-9972 Невозможно создать конфигурацию LDAP для …

На сервере Комплекса достаточно создать служебную учетную запись с правами поиска и чтения записей пользователей и групп. Изменить учетные данные нужно в разделе ”Управление Параметры Аутентификация”

В веб-интерфейсе Комплекса:ERF50-1006 Невозможно подключиться к серверу LDAP

На сервере Комплекса убедиться, что сертификат TLS для сервера LDAPS действителен и соответствует имени узла сервера

В веб-интерфейсе Комплекса:ERF50-5345 Убедитесь, что SSL включен в foreman-proxy:: enabled: https

В веб-интерфейсе Комплекса убедиться, что SSL включен в Комплексе:proxy:: enabled: https

В веб-интерфейсе Комплекса:ERF42-9666: для загрузки HTTP требуется прокси с функцией httpboot, а выставленная настройка http_port

На сервере Комплекса существует расширенный параметр, который по умолчанию скрыт и включен. Нужно проверить, не был ли он отключен по ошибке:foreman-installer –foreman-proxy-http true –foreman-proxy-https true –foreman-proxy-httpboot true –foreman-proxy-tftp true

В журнале ошибок сервиса dynflow-sidekiq (запрашивается выводом команды journalctl -fu dynflow-sidekiq@worker.service) появляются сообщения вида:dynflow-sidekiq@worker[36703]: 2022-01-17T11:22:57.078Z 36703 TID-gpkfjfkoj ERROR: Heartbeat thread error: Connection lost (ECONNRESET)При этом наблюдается замедление работы веб-интерфейса

На сервере Комплекса:– отключить сервис network threat protection для Kaspersky Endpoint Security for Linux (KESL);– перезапустить службы foreman и puppetserver

::