**ООО "Генезис АйТи"**

# СИСТЕМА УПРАВЛЕНИЯ СЛУЖБОЙ КАТАЛОГОВ DYNAMIC DIRECTORY

**Версия 4.3**

## Руководство администратора

## Часть 1. Установка и настройка

RU.69838320.02.06-08 32 01

Листов 95

2026

# АННОТАЦИЯ

Настоящий документ представляет собой руководство по установке и настройке системы управления службой каталогов Dynamic Directory (далее – Система).

Руководство определяет порядок установки и настройки Системы.

Перед установкой Системы рекомендуется внимательно ознакомиться с настоящим руководством.

Сведения, необходимые для эксплуатации Системы, приведены в документе "Dynamic Directory. Руководство администратора. Часть 2. Эксплуатация" (индекс RU.69838320.02.06-08 32 02).

Перед установкой Системы рекомендуется внимательно ознакомиться с настоящим руководством.

При разработке документа использованы ссылки на следующие стандарты:

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

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

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

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

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

# СОДЕРЖАНИЕ

**1 Общие положения** . . . . . **5**

1.1 Назначения и условия применения программного обеспечения . . . . . 5
1.2 Уровень подготовки персонала . . . . . 7

1.2.1 Администратор Системы . . . . . 8
1.2.2 Администратор информационной безопасности . . . . . 8
1.2.3 Специалист по техническому обслуживанию . . . . . 8
1.2.4 Пользователи . . . . . 9

1.3 Перечень документации . . . . . 9

**2 Архитектурные решения** . . . . . **11**

2.1 Архитектурные решения Системы . . . . . 11
2.2 Состав программного обеспечения . . . . . 12
2.3 Требования к аппаратным средствам . . . . . 14

2.3.1 Сервер службы каталогов Dynamic Directory . . . . . 14
2.3.2 Сервер групповых политик Puppet . . . . . 19

**3 Установка** . . . . . **20**

3.1 Порядок установки и настройки . . . . . 20
3.2 Установка Dynamic Directory . . . . . 21

3.2.1 Установка ОС на сервер . . . . . 21
3.2.2 Выполнение сценария установки службы каталогов . . . . . 26
3.2.3 Установка с использованием сертификата . . . . . 31
3.2.4 Настройка дополнительного сервера Dynamic Directory . . . . . 32
3.2.5 Вывод из эксплуатации сервера Dynamic Directory . . . . . 37

3.3 Установка сервера Puppet . . . . . 39

3.3.1 Обновление сервера Puppet . . . . . 44

3.4 Обновление Dynamic Directory . . . . . 44

3.4.1 Обновление с версии 4.1 до 4.2 . . . . . 44
3.4.2 Обновление с версии 4.2 до 4.3 . . . . . 47
3.4.3 Обновление через интернет-репозиторий . . . . . 50

3.5 Настройка сервера журналирования Rsyslog . . . . . 51

3.5.1 Настройка пересылки журналов Rsyslog . . . . . 52

3.6 Установка ОС на сервер файлового обмена . . . . . 53
3.6.1 Настройка сетевых ресурсов для групп доменных пользователей . . 61
3.7 Подключение репозитория Dynamic Directory . . . . . 69
3.8 Установка консоли администратора Dynamic Directory . . . . . 71
3.9 Настройка управляемых АРМ . . . . . 72
3.9.1 Обновление пакетов . . . . . 72
3.9.2 Настройка управляемых АРМ с использованием клиента (ОС Linux) 72
3.9.3 Настройка управляемых АРМ с использованием клиента (ОС MS Windows) . . . . . 79
3.9.4 Настройка управляемых АРМ вручную для Astra Linux . . . . . 89
3.9.5 Настройка управляемых АРМ вручную для РЕД ОС и РОСА . . . . . 91
3.10 Установка лицензионного ключа . . . . . 93
3.11 Установка антивирусного ПО . . . . . 94
**Термины и сокращения** . . . . . **95**

# 1 ОБЩИЕ ПОЛОЖЕНИЯ

## 1.1 Назначения и условия применения программного обеспечения

Система предназначена для централизованного управления данными пользователей, персональных компьютеров, общих папок, принтеров и других ресурсов ИТ-инфраструктуры. Также Система обеспечивает механизмы аутентификации и авторизации пользователей при доступе к информационным ресурсам.

Система предназначена для обеспечения следующих функций:

– аутентификация пользователей и компьютеров на основе протокола Kerberos при подключении из любой точки сети передачи данных;

– использование следующих криптоалгоритмов на основе AES и Camellia (при работе входящего в состав FreeIPA MIT Kerberos KDC):

- AES-256 CTS mode with 96-bit SHA-1 HMAC;
- AES-256 CTS mode with 192-bit SHA-384 HMAC;
- Camellia-256 CTS mode with CMAC;
- AES-128 CTS mode with 96-bit SHA-1 HMAC;
- AES-128 CTS mode with 128-bit SHA-256 HMAC;
- Camellia-128 CTS mode with CMAC;

– однозначная идентификация пользователя при доступе к локальным и сетевым ресурсам, которые находятся под управлением Системы;

– авторизация пользователей при доступе к локальным и сетевым ресурсам, которые находятся под управлением Системы;

– централизованное управление объектами службы каталогов, такими как учетные записи пользователей, учетные записи компьютеров, группы безопасности и рассылки, принтеры и т.д.;

– централизованное управление политиками безопасности;

– обеспечение доверительных отношений службы каталогов с существующими доменами службы каталогов Microsoft Active Directory;

– делегирование полномочий по управлению объектами в рамках отдельных организационных подразделений назначенным, ИТ-специалистам;

– централизованное управление настройками АРМ с помощью механизма аналогов групповых политик (далее – политики), аналогичного механизму групповых политик службы каталогов Microsoft Active Directory, через консоль

управления с графическим интерфейсом с возможностью фильтрации применяемых аналогов групповых политик на основе членства пользователей или компьютеров в группах или принадлежности к организационным подразделениям;

– навигация и поиск объектов управления по каталогу, в том числе пользователей, компьютеров, групп, печатающих устройств;

– запись событий службы каталогов в журналы;

– создание, изменение и удаление записей службы каталогов в составе:

  – организационные единицы;
  – учетные записи пользователей;
  – учетные записи компьютеров;
  – группы пользователей;
  – группы компьютеров;
  – общие папки;
  – общие принтеры;
  – права доступа к объектам службы каталогов;
  – шаблоны параметров политик;
  – политики;
  – параметры политик;
  – зоны DNS;

– иерархическое отображение записей службы каталогов;

– навигация и поиск по записям службы каталогов;

– отображение списка доступных политик;

– создание и изменение контейнеров политик;

– назначение политик объектам службы каталогов: домен и организационное подразделение;

– отображение иерархической структуры контейнера политики: политики пользователей и политики компьютера;

– возможность создания подкаталогов в вышеназванных контейнерах политики (например, "Политики пользователей Доступ к съемным запоминающим устройствам");

– возможность добавления параметров политик, созданных в редакторе политик, в подкаталоге контейнера (например, "Политики пользователей Доступ к съемным запоминающим устройствам Запретить доступ ко всем съемным запоминающим устройствам");

– возможность изменения параметров политики, включая, но не ограничиваясь (например, "Политики пользователей Доступ к съемным

запоминающим устройствам  Запретить доступ ко всем съемным запоминающим устройствам" – Политика: Включена"):

  - логический параметр ("Вкл./Выкл.");
  - путь (например, "\\Общая папка\Документы");
  - числовые данные (например, количество попыток подключения к принтеру);
  - списки (например, список доверенных узлов сети);
- редактирование шаблонов политик, включая:
  - описание шаблона политики;
  - имя параметра политики;
  - тип параметра;
  - сценарий, выполняемый на клиентском АРМ при авторизации пользователя;
  - описание параметра политики.

Система обеспечивает следующее информационное взаимодействие:

- с администраторами с целью управления записями службы каталогов и политиками;

- с пользователями с целью идентификации и аутентификации пользователей, применения политик на пользовательских АРМ.

Транзакционная модель работы с данными, реализованная в Системе, обеспечивает репликацию объектов каталога и отсутствие расхождений между одним и тем же объектом на разных узлах Системы.

Интерфейс Системы реализован на русском и английском языке.

Система поддерживает кириллицу, в том числе при выводе предупреждений пользователю и в лог-файлах.

## 1.2 Уровень подготовки персонала

Персонал Системы включает следующие категории:

- системный администратор;
- администратор информационной безопасности;
- специалист по техническому обслуживанию;
- пользователь.

### 1.2.1 Администратор Системы

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

Основными обязанностями администратора Системы являются:

– установка, настройка и мониторинг работоспособности системного и базового программного обеспечения;

– инсталляция и настройка прикладного программного обеспечения;

– создание и изменение объектов службы каталогов;

– создание и изменение объектов политик;

– настройка локальной компьютерной сети и сетевого окружения;

– контроль доступа к сетевым ресурсам.

### 1.2.2 Администратор информационной безопасности

Квалификация администратора безопасности: высокий уровень знаний и наличие практического опыта выполнения работ по организации доступа администраторов и пользователей к функциям информационных систем, а также наличие профессиональных знаний и практического опыта в разработке и назначении ролей пользователей.

Основными обязанностями администратора информационной безопасности являются:

– разработка и назначение ролей пользователям Системы;

– организация доступа и разграничение прав доступа пользователей к информации и функциям;

– проведение работ по выявлению возможных каналов вмешательства в процесс функционирования и осуществления НСД к информации.

### 1.2.3 Специалист по техническому обслуживанию

Квалификация специалиста по техническому обслуживанию: высокий уровень знаний и наличие практического опыта выполнения работ 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:

– модернизация, настройка и мониторинг работоспособности комплекса технических средств (серверов, рабочих станций);

– конфигурирования и настройки программно-технических средств Системы;

– диагностика типовых неисправностей.

### 1.2.4 Пользователи

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.

## 1.3 Перечень документации

Для освоения работы по развертыванию Системы необходимо изучить разделы по установке и настройке этого документа и дополнительную документацию:

– руководство по эксплуатации (https://kb.rosa.ru/dynamic-directory/4.3/ekspluatatsiya);

– документация по FreeIPA (EN - https://www.freeipa.org/page/Documentation);

Примечание — В качестве базового руководства по архитектуре и развертыванию компонентов IPA-домена на русском языке может быть использовано независимое руководство сообщества DevOps Way – https://devopsway.ru/posts/freeipa-setup/.

– документация по Puppet (EN – https://puppet.com/docs/puppet/7/puppet_index.html).

П р и м е ч а н и е — Принципы работы, архитектурные особенности и синтаксис Puppet подробно описаны в русскоязычном переводе книги "Архитектура приложений с открытым исходным кодом" на ресурсе Rus-Linux – https://rus-linux.net/MyLDP/BOOKS/Architecture-Open-Source-Applications/Vol-2/puppet-01.html

# 2 АРХИТЕКТУРНЫЕ РЕШЕНИЯ

## 2.1 Архитектурные решения Системы

Решение в минимальной конфигурации базируется на двух службах: служба каталогов Dynamic Directory и служба управления конфигурациями ПК. В базовой поставке Dynamic Directory используется служба управления конфигурациями ПК Puppet Server. Кроме того, в качестве службы управления может использоваться платформа оркестрации РОСА Центр управления, которая тесно интегрируется со службой каталогов Dynamic Directory, в этом случае развёртывание службы управления конфигурацией ПК Puppet Server не требуется.

На всех управляемых АРМ в домене используются шлюзы ddpo_get и ddlap: первый отвечает за получение значений параметров аналогов групповых политик из службы каталогов и передачу их для применения службе управления конфигурацией ПК, второй предназначен для автоматической смены паролей локальных администраторов на АРМ и безопасной передачи их в службе каталогов Dynamic Directory. Указанные шлюзы и перечень манифестов входят в состав дистрибутива и распространяются на АРМ пользователей автоматически после установки клиента службы каталогов Dynamic Directory (dd-client).

Управление Системой осуществляется при помощи программного обеспечения для управления службой каталогов Dynamic Directory (dd-admin).

Технологическая схема приведена на рисунке 1.

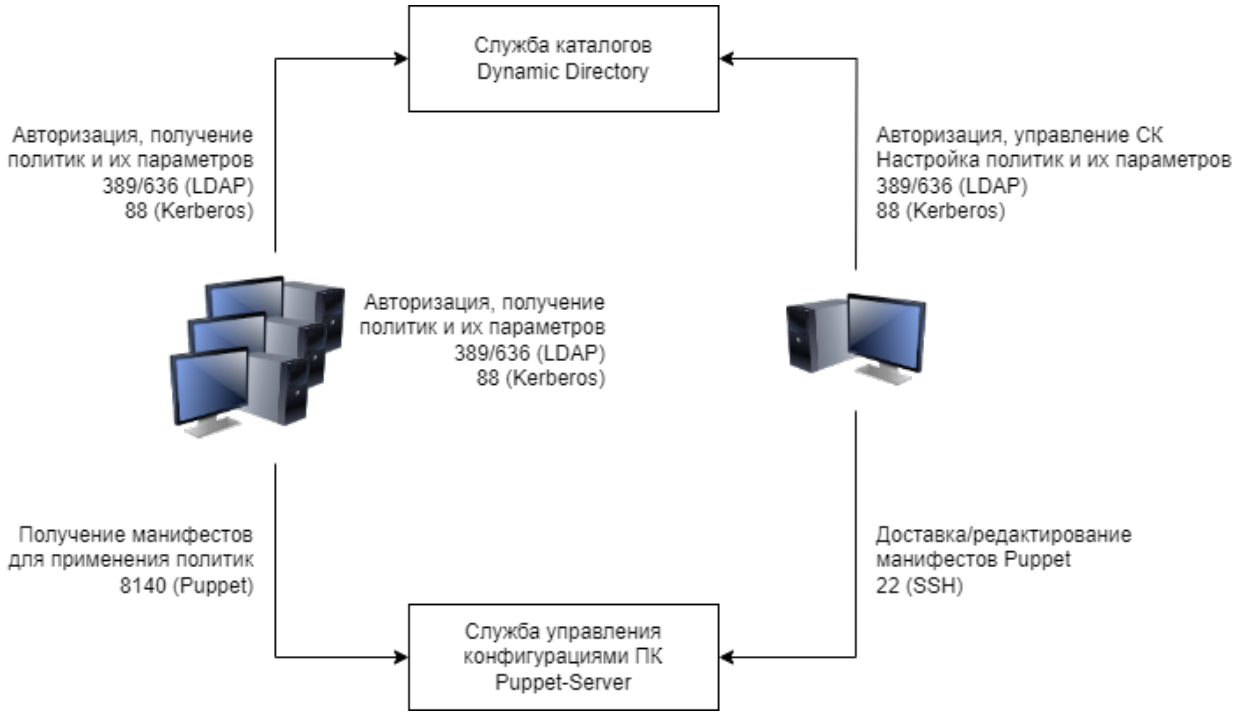


Рисунок 1 – Технологическая схема

## 2.2 Состав программного обеспечения

Программное обеспечение Системы состоит из следующих компонентов:

- служба каталогов Dynamic Directory (dd-server);
- служба управления конфигурациями ПК Puppet Server;
- клиент службы каталогов Dynamic Directory (dd-client);
- управление службой каталогов Dynamic Directory (dd-admin).

Агент управления конфигурацией ПК Puppet Agent, ПО для управления службой каталогов Dynamic Directory и агент dd-client службы каталогов Dynamic Directory могут быть развернуты и функционировать под управлением следующих версий одной из операционных систем на базе Linux:

- Astra Linux 1.7_x86-64 (далее – Astra Linux);
- РЕД ОС 7/8 (далее – РЕД ОС);
- РОСА "Хром" 12/13 Сервер, РОСА "Хром" 12/13 Рабочая станция (далее – РОСА);
- Альт рабочая станция 10 (далее – Альт).

Все серверные компоненты Системы имеют возможность работать в виртуальных средах следующих средств виртуализации:

- ROSA Virtualization;
- VMware vCenter;
- Red Hat Virtualization;
- oVirt;
- РЕД Виртуализация;
- HOSTVM;
- zVirt.

В случае развёртывания Системы в виртуальной среде необходимо использовать виртуальный графический адаптер типа VGA.

Всё необходимое для корректной работы Системы ПО входит в состав дистрибутива. Основные компоненты Системы и компоненты, которые должны присутствовать на клиентских АРМ, перечислены в таблице 1.

Таблица 1 – Программное обеспечение, необходимое для функционирования Системы

| № п/п | Название программного обеспечения | Роль программного обеспечения | Место установки |
|---|---|---|---|
| 1 | Операционная система ROSA Enterprise Linux Server | Операционная система | Контроллеры домена, серверы управления. |
| 2 | Операционная система клиентских АРМ | Операционная система. | АРМ администратора Системы, АРМ администратора информационной безопасности, АРМ пользователя |
| 3 | Dynamic Directory (на базе FreeIPA) | Централизованная система по управлению идентификацией пользователей | Контроллеры домена |
| 4 | Служба управления конфигурациями ПК Puppet Server | Система централизованного управления конфигурацией ОС, программ и персональных компьютеров | Контроллеры домена/ отдельный сервер |

| № п/п | Название программного обеспечения | Роль программного обеспечения | Место установки |
|---|---|---|---|
| 5 | Набор манифестов для Puppet Server, включающий шлюзы ddpo_get и ddlap | Интерпретация групповых политик на клиентских АРМ. | Контроллеры домена/отдельный сервер. Манифесты распространяются на АРМ Системы через службу управления конфигурацией ПК |
| 6 | Клиент службы каталогов Dynamic Directory (dd-client) | Конфигурирование freeipa-client, sssd, puppet-agent. | Все АРМ, входящие в домен |
| 7 | puppet-agent, должен входить в состав ОС клиентских АРМ | Применение манифестов на клиентских АРМ, для реализации групповых политик. | Все АРМ, где требуется применение политик |
| 8 | freeipa-client, должен входить в состав ОС клиентских АРМ | Настройка конфигурации АРМ для работы в домене. | Все АРМ, входящие в домен |
| 9 | Программное обеспечение для управления службой каталогов Dynamic Directory (dd-admin) | ПО для управления службой каталогов | АРМ администратора Службы каталогов |

Функциональные ограничения на применение Системы накладываются только входящими в нее компонентами.

## 2.3 Требования к аппаратным средствам

### 2.3.1 Сервер службы каталогов Dynamic Directory

Требования к аппаратным средствам сервера, предназначенного для установки сервера службы каталогов Dynamic Directory, приведены в таблице 2.

Таблица 2 – Требования к аппаратным средствам сервера службы каталогов Dynamic Directory

| Параметр | Минимальное значение | Рекомендуемое значение |
|---|---|---|
| Количество ядер процессора | 2 | 4 |

| Параметр | Минимальное значение | Рекомендуемое значение |
|---|---|---|
| Объем оперативной памяти, Гбайт | 4 | 16 |
| Свободное дисковое пространство, Гбайт | 20 | 100 |
| Скорость подключения к ЛВС, Мб/с | 100 | 1000 |

### 2.3.1.1 Масштабирование

При увеличении количества объектов в каталоге основным ресурсом, требующим масштабирования, является оперативная память. На каждые 10 000 объектов необходимо добавить 2Гб оперативной памяти.

При увеличении количества обслуживаемых АРМ необходимо добавить количество ядер процессора, которое зависит, в том числе, от производительности этих ядер. При достижении 80% загрузки процессоров в пиковые моменты рекомендуется увеличить количество выделенных ядер.

На один сервер службы каталогов Dynamic Directory в расположении рекомендуется не более 2500 обслуживаемых хостов. При превышении этого количества необходимо добавить дополнительный сервер службы каталогов Dynamic Directory.

### 2.3.1.2 Проектирование топологии реплик

Топология реплик определяет структуру связей между серверами Dynamic Directory в рамках домена и обеспечивает:

- отказоустойчивость системы;
- репликацию данных между серверами;
- балансировку нагрузки при обработке запросов.

#### 2.3.1.2.1 Требования к топологии

При проектировании топологии необходимо соблюдать базовые рекомендации по определению количества и подключению реплик (таблица 3).

Таблица 3 – Требования к топологии реплик

| № | Требование | Обоснование |
|---|---|---|
| 1 | Разворачивать не менее двух реплик в каждом ЦОД | Обеспечение отказоустойчивости: в случае сбоя одного сервера вторая реплика сможет взять на себя управление и обработку запросов |
| 2 | Использовать не более 60 серверов Dynamic Directory в рамках одного домена | Поддержание высокой производительности и управляемости доменом |
| 3 | Подключать каждую реплику как минимум к двум другим репликам | Гарантия того, что информация будет реплицироваться между всеми узлами, а не только между исходной репликой и первым установленным сервером |
| 4 | Использовать не более 4 репликационных связей для каждого из суффиксов (Domain и CA) | Избыточное количество связей не дает существенных преимуществ, но может отрицательно сказаться на общей производительности системы |
| 5 | Подключать реплики в ЦОД друг к другу для репликации домена в пределах ЦОД | Обеспечение быстрой и надежной локальной репликации внутри дата-центра |
| 6 | Подключать каждый ЦОД как минимум к двум другим ЦОД для репликации домена между ЦОД | Обеспечение межцентровой репликации и географической отказоустойчивости |

#### 2.3.1.2.2 Минимальная топология (базовая конфигурация)

Минимальная топология применяется для небольших организаций (до 500 пользователей) и на начальном этапе внедрения (рисунок 2).

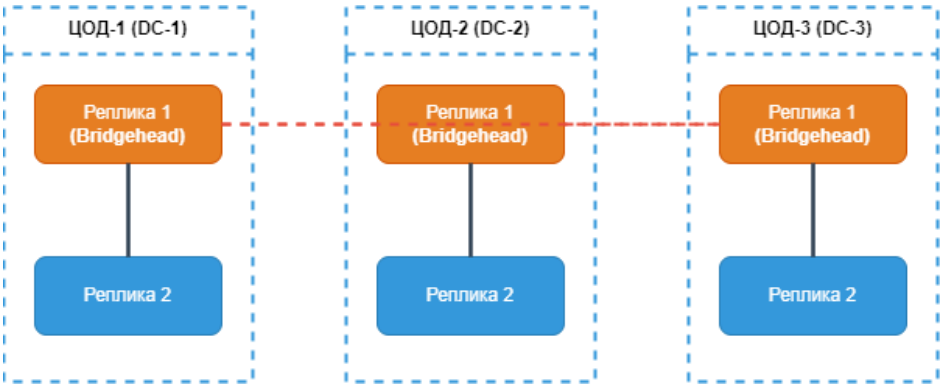


Рисунок 2 – Схема с минимальной топологией реплик

Схема демонстрирует реализацию следующих требований:

- в каждом из трех ЦОД развернуто минимальное количество реплик (по 2 в каждом);
- реализована треугольная топология связей между ЦОД, где каждый ЦОД подключен к двум другим;
- каждая реплика имеет минимум 2 связи для гарантированной доставки данных.

Характеристики минимальной топологии отображены в таблице 4.

Таблица 4 – Параметры минимальной топологии

| Параметр | Значение |
|---|---|
| Количество ЦОД | 3 |
| Всего реплик | 6 |
| Сложность управления | Низкая |
| Отказоустойчивость | Базовая |
| Время развертывания | 1-2 недели |
| Стоимость инфраструктуры | Низкая |

Минимальная топология рекомендуется в следующих случаях:

- небольшие организации (до 500 пользователей);
- начальный этап внедрения Dynamic Directory;
- ограниченный бюджет на инфраструктуру;
- наличие 2-3 географических локаций.

Ключевыми преимуществами данной конфигурации являются простота управления и мониторинга, минимальные требования к сетевой инфраструктуре, а также быстрое развертывание.

#### 2.3.1.2.3 Масштабная топология (замена иерархии MS AD)

Масштабная топология применяется для крупных организаций (1000+ пользователей) и предназначена для полной замены существующей иерархической инфраструктуры MS AD.

На рисунке 3 показана масштабная топология с трехуровневой иерархией, обеспечивающая высокую отказоустойчивость и гибкость.

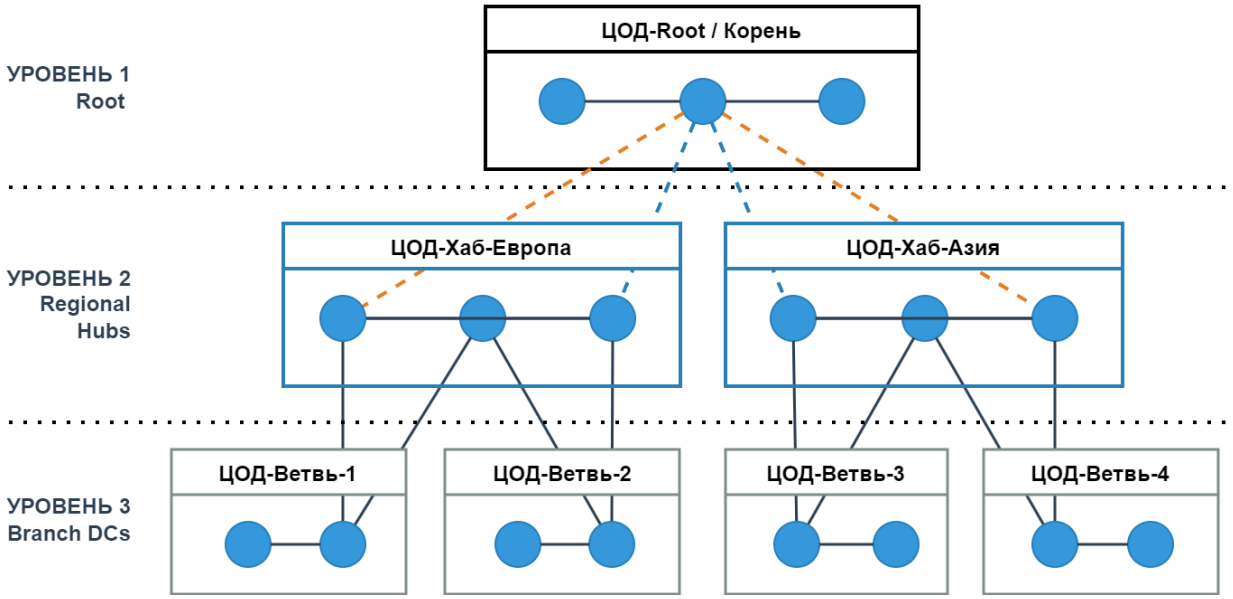


Рисунок 3 – Схема масштабной топологии реплик (замена иерархии MS AD)

Схема демонстрирует реализацию следующих архитектурных решений:

- трехуровневая иерархия: Root -> Regional Hubs -> Branch DCs;
- разделение суффиксов Domain (синие пунктирные линии) и CA (оранжевые пунктирные линии);
- топология hub-and-spoke с избыточными связями;
- масштабирование до 7 и более ЦОД с варьированием количества реплик в зависимости от роли ЦОД.

Характеристики масштабной топологии отображены в таблице 5.

Таблица 5 – Параметры масштабной топологии

| Параметр | Значение |
|---|---|
| Количество ЦОД | 7 и более |
| Всего реплик | 17 и более |
| Сложность управления | Высокая |
| Отказоустойчивость | Высокая |
| Время развертывания | 1-2 месяца |
| Стоимость инфраструктуры | Высокая |

Масштабная топология рекомендуется в следующих случаях:
- крупные организации (1000+ пользователей);
- географически распределенная структура;
- замена существующей инфраструктуры MS AD;
- высокие требования к отказоустойчивости и производительности.

Преимущества перед стандартной иерархией MS AD заключаются в гибкой топологии без жесткой привязки доменов, независимой репликации суффиксов Domain и CA, а также в возможности масштабирования без перестройки всей структуры.

### 2.3.2 Сервер групповых политик Puppet

Требования к аппаратным средствам сервера, предназначенного для установки сервера групповых политик Puppet, приведены в таблице 6.

Таблица 6 – Требования к аппаратным средствам сервера Puppet

| Параметр | Минимальное значение | Рекомендуемое значение |
|---|---|---|
| Количество ядер процессора | 2 | 8 |
| Объем оперативной памяти в ГБ | 2 | 16 |
| Свободное дисковое пространство в ГБ | 20 | 100 |
| Скорость подключения к ЛВС, Мб/с | 100 | 1000 |

# 3 УСТАНОВКА

## 3.1 Порядок установки и настройки

Порядок установки Системы включает следующие этапы:

– установка и настройка службы каталогов Dynamic Directory;

– установка и настройка службы управления конфигурациями ПК Puppet Server;

– подготовка АРМ администратора;

– установка клиента службы каталогов Dynamic Directory на управляемые АРМ.

Установка и настройка службы каталогов Dynamic Directory включает следующие действия:

– установка и конфигурирование службы каталогов Dynamic Directory на все экземпляры серверов в режиме мультимастера;

– настройка топологии репликации между серверами Dynamic Directory (при необходимости её изменения);

– установка и настройка программного обеспечения dd-client на все клиентские рабочие места.

Установка и настройка службы управления конфигурациями ПК Puppet Server включает следующие действия:

– установка и конфигурирование основного сервера Puppet Server;

– установка и конфигурирование дополнительных серверов Puppet Server (при необходимости);

– установка и настройка puppet-agent на все клиентские рабочие места.

Подготовка АРМ администратора включает следующие действия:

– подключение репозиториев Dynamic Directory;

– установка пакета dd-client;

– конфигурирование dd-client в интерактивном режиме;

– установка программного обеспечения для управления службой каталогов Dynamic Directory (dd-admin);

– установка редактора групповых политик (пакет dd-tedit), при необходимости;

– установка, при необходимости, утилиты миграции (пакет dd-migrate).

Установка клиента службы каталогов Dynamic Directory на управляемые АРМ включает следующие работы:

- подключение репозиториев Dynamic Directory;
- установка пакета dd-client;
- конфигурирование dd-client в интерактивном режиме.

Работа с данными Системы допускается только после установки службы каталогов Dynamic Directory, службы управления конфигурациями ПК Puppet Server и всех дополнительных компонентов Системы.

Запуск всех служб, необходимых для корректной работы Системы, после выполнения установок и настроек выполняется автоматически, без дополнительных действий со стороны администратора.

## 3.2 Установка Dynamic Directory

В процессе развертывания сервера службы каталогов администратор должен сначала осуществить установку ОС на физический сервер или ВМ, а затем выполнить консольный интерактивный сценарий установки Dynamic Directory, используя консольную утилиту ipa-server-install.

### 3.2.1 Установка ОС на сервер

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

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

На экране последовательно появятся меню программы установки, интерфейс для выбора языка сопровождения установки и меню "Обзор установки", предназначенное для обзора и последующей настройки параметров установки (рисунок 4).

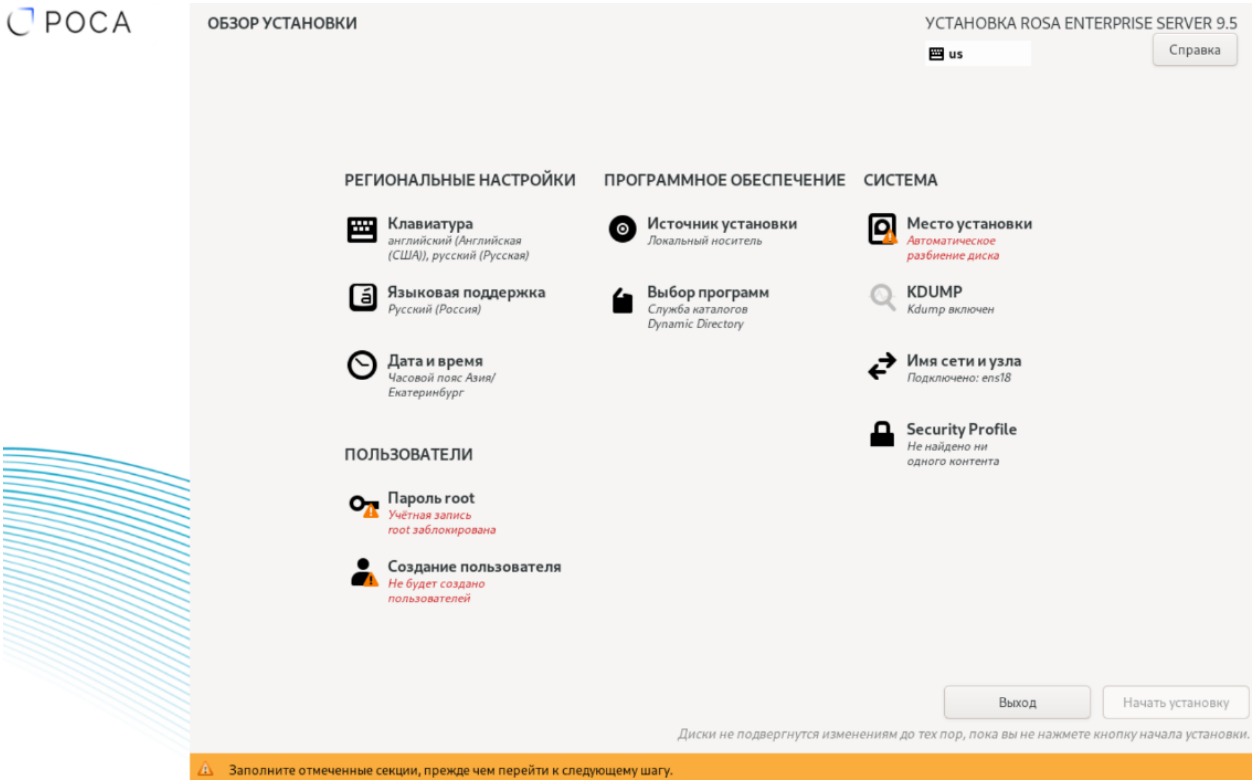


Рисунок 4 – Обзор установки

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

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

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

Для перехода к интерфейсу настройки соответствующих параметров требуется нажать на наименование секции "Выбор программ".

В секции "Выбор программ" нужно установить переключатель "Базовое окружение" в положение "Служба каталогов Dynamic Directory" для установки соответствующего базового ПО на сервер и нажать кнопку Готово (рисунок 5) для возвращения в меню "Обзор установки".

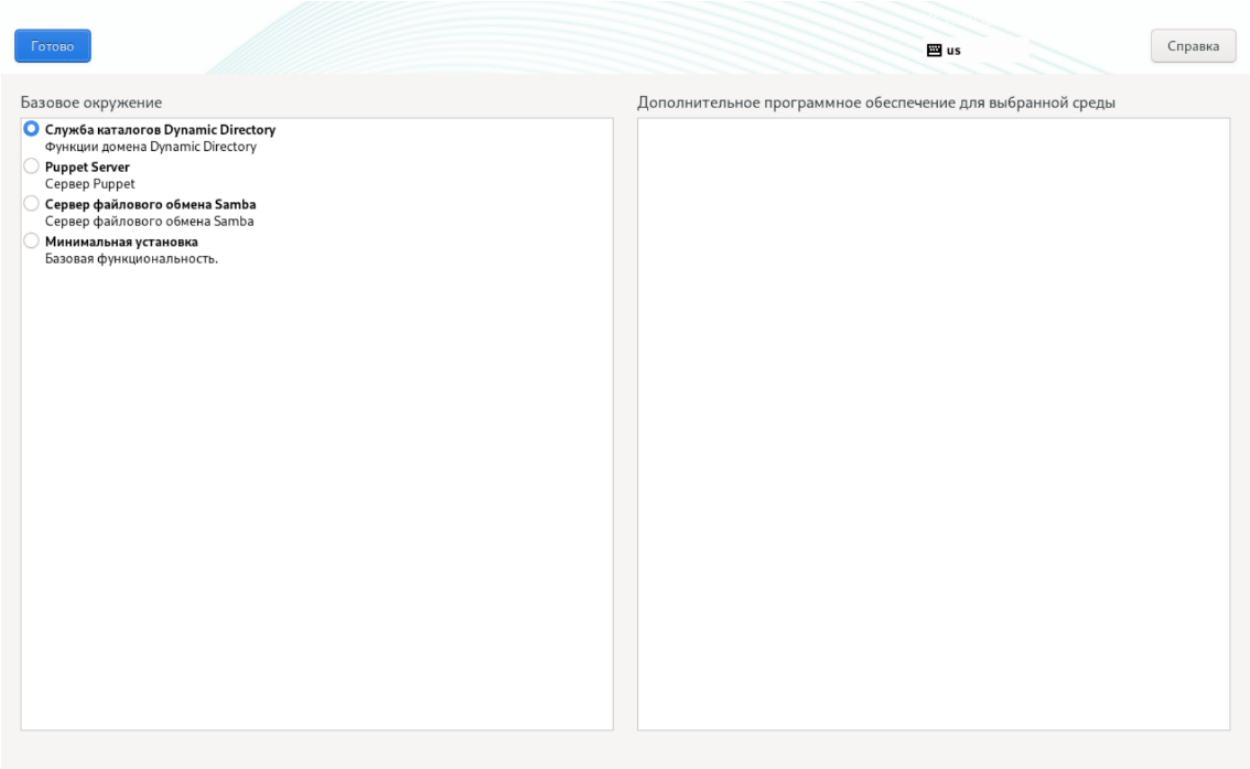


Рисунок 5 – Выбор секции установки

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

В секции "Имя сети и узла" необходимо задать полное доменное имя сервера службы каталогов Dynamic Directory, которое должно быть доменным именем по крайней мере третьего уровня (например, dd.rosa.dev, где dd – краткое имя хоста, а rosa.dev – домен, в котором служба каталогов будет выполнять функции контроллера домена).

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

Для функционирования службы каталогов Dynamic Directory необходим уникальный домен. При выборе домена необходимо избегать использования доменов home.arpa. и local. даже в целях тестирования. Домен home.arpa. выделен IETF для использования в локальных сетях, но глобально обозначен в

DNS как занятый и используемый IANA. Домен local. используется с mDNS, что может приводить к проблемам с загрузкой хостов по сети при использовании этого домена.

Далее нужно подключить необходимый сетевой интерфейс сервера службы каталогов и настроить параметры сетевого соединения – IP-адрес (например, 10.0.0.2), маску сети (например, 255.255.0.0), шлюз по умолчанию (например, 10.0.0.1).

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

В секции "Пароль root" нужно установить пароль для учетной записи суперпользователя root.

После настройки всех обязательных параметров нужно нажать кнопку `Начать установку` для запуска процесса установки ОС сервера службы каталогов Dynamic Directory.

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

После перезагрузки Системы на экране появится строка приглашения командного интерпретатора для входа в ОС сервера службы каталогов Dynamic Directory.

### 3.2.1.1 Миграция сервера с версии 8.7 на 9.x

При переходе работающей Системы, в которой уже существуют созданные ранее подразделения, пользователи, политики, делегирования и введенные в домен АРМы, с ОС ROSA Enterprise Linux Server версии 8.7 на версию 9.x, следует воспользоваться следующим порядком действий:

а) установить сервер Dynamic Directory версии 9.x;

б) обновить на сервере с версией 8.7 службу каталогов 389ds, установив 3 пакета (предоставляются отдельно):

- 389-ds-base-1.4.3.39-8.res8.x86_64.rpm;
- 389-ds-base-libs-1.4.3.39-8.res8.x86_64.rpm;
- python3-lib389-1.4.3.39-8.res8.noarch.rpm;

в) на установленном сервере Dynamic Directory с версией 9.x заменить файл 87-dd-policy-cleaner.update (предоставляется отдельно) в директории /usr/share/ipa/updates/;

г) сделать репликацию с сервера версии 8.7, добавив к параметрам "--setup-ca --setup-adtrust":

```
ipa-replica-install --mkhomedir -w p@$$w0rd --setup-dns
--setup-ca --setup-adtrust --forwarder=11.22.33.1
```

д) выполнить изменение сервера обновления сертификатов:

```
kinit admin
ipa config-mod --ca-renewal-master-server FQDN_Сервера_9.4(9.5)
```

е) на серверах, где IP-адресация указана статичной, нужно изменить DNS на сервер с версией 9.x;

ж) удалить сервер версии 8.7 из топологии:

```
kinit admin
ipa server-del FQDN_Сервера_8.7
```

з) выключить сервер версии 8.7;

и) выполнить скрипт admpc migrate_res9.py (предоставляется отдельно), указав в DNS новый сервер версии 9.x;

к) проверить работоспособность Системы;

л) создать новые политики и проверить корректность их работы;

м) создать новый сервер версии на 9.x (рекомендуется такой же адрес, что был у сервера версии 8.7);

н) провести репликацию нового сервера с уже работающим сервером версии 9.x;

о) убедиться, что Система работоспособна.

#### 3.2.1.2 Обновление службы каталогов Dynamic Directory до версии 9.5

В случае использования службы каталогов на базе Dynamic Directory и ее установки с помощью дистрибутива версии 9.4 необходимо подключить репозиторий ipa-dd, выполнив команды:

```
dnf makecache
dnf install -y rosa-release-ipa-dd
```

В случае использования службы каталогов на базе чистой FreeIPA и ее установки с помощью дистрибутива версии 9.4 необходимо подключить репозиторий ipa, выполнив команду:

```
dnf makecache
dnf install -y rosa-release-ipa
```

Далее обновление выполняется штатным методом командами:

```
dnf makecache
dnf update
```

При обновлении пакетов ipa-server и dd-server также требуется выполнить команду:

```
ipa-server-upgrade
```

### 3.2.2 Выполнение сценария установки службы каталогов

**Следует обратить внимание**, что:

– если планируется использовать двусторонние доверительные отношения с доменами MS AD и общие ресурсы в доменах MS AD пользователями Dynamic Directory, то перед выполнением сценария установки на контроллере домена Dynamic Directory необходимо отключить шифрование SHA-2. Данный вид шифрования не поддерживается операционными системами MS Windows для протокола Kerberos;

– если в качестве перенаправителя указан сервер без DNSSEC-валидации, то на настраиваемом сервере DNSSEC-валидация будет отключена автоматически.

Конфигурационный файл /etc/crypto-policies/back-ends/krb5.config должен иметь вид:

```
[libdefaults]
permitted_enctypes = aes256-cts-hmac-sha1-96
aes128-cts-hmac-sha1-96
```

После изменений в файле /etc/crypto-policies/back-ends/krb5.config обязательно должна быть выполнена перезагрузка.

Установка службы каталогов осуществляется консольной утилитой ipa-server-install.

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

По умолчанию служба каталогов устанавливается со встроенной службой DNS и со встроенным центром сертификации CA в качестве корневого удостоверяющего центра. Для установки сервера сертификации используется самоподписанный сертификат. Описание установки с использованием сертификата, выпущенного сторонним сервером сертификации, приведено в п. 3.2.3. В этом случае устанавливаемый центр сертификации будет подчинённым по отношению к серверу, выпустившему для него сертификат.

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

```
ipa-server-install --setup-dns --mkhomedir
```

Если планируется создание сервера с именем DNS-зоны (прямой или обратной), которая разрешается настроенным в Системе сервером DNS (уже делегирована другому серверу), также необходимо использовать параметр "--allow-zone-overlap":

```
ipa-server-install --setup-dns --mkhomedir --allow-zone-overlap
```

Далее сценарий установки предложит задать значения параметров сервера – имя хоста службы каталогов, имя домена и имя области Kerberos:

```
Server host name [dd.rosa.dev]:
Please confirm the domain name [rosa.dev]:
Please provide a realm name [ROSA.DEV]:
```

Чтобы принять значения, нужно нажать клавишу `Enter`.

Для изменения параметра по умолчанию можно ввести требуемое значение.

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

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

Далее сценарий установки предложит настроить перенаправление DNS:

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

Указанные перенаправители должны быть доступны во время установки Системы, так как при указании недоступных перенаправителей установка будет прервана. Если на момент конфигурирования сервера перенаправители по какой-либо причине недоступны, можно их не указывать, а добавить позже.

Если перенаправление DNS конфигурировать не нужно, следует ввести no.

Для настройки перенаправления DNS нужно нажать клавишу `Enter` или ввести yes. **Следует обратить внимание**, что если в качестве перенаправителя указан сервер без DNSSEC валидации, то на настраиваемом сервере DNSSEC-валидация будет отключена автоматически.

Если на перенаправителях включено подписание зон с помощью DNSSEC, что типично для общедоступных DNS-серверов, но в настраиваемой системе необходимо отключить именно валидацию (например, при построении доверия с доменом Active Directory, в котором подписание зон DNSSEC не используется), следует указать опцию `--no-dnssec-validation` при выполнении команды `ipa-server-install`.

После этого сценарий установки предложит проверить, нужно ли настроить какие-либо обратные записи DNS для IP-адресов, связанных со службой каталогов. **Следует обратить внимание**, что для установки и функционирования реплик Системы необходимо наличие PTR-записи о них в обратной зоне. Для подтверждения следует нажать клавишу `Enter` или ввести yes:

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

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

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

Для настройки NetBIOS нужно ввести имя или, если устраивает значение по умолчанию, нажать клавишу `Enter`.

При необходимости редактирования NTP-сервера следует набрать символ "y". Если можно оставить значение по умолчанию, то нажать клавишу `Enter` (рисунок 6).

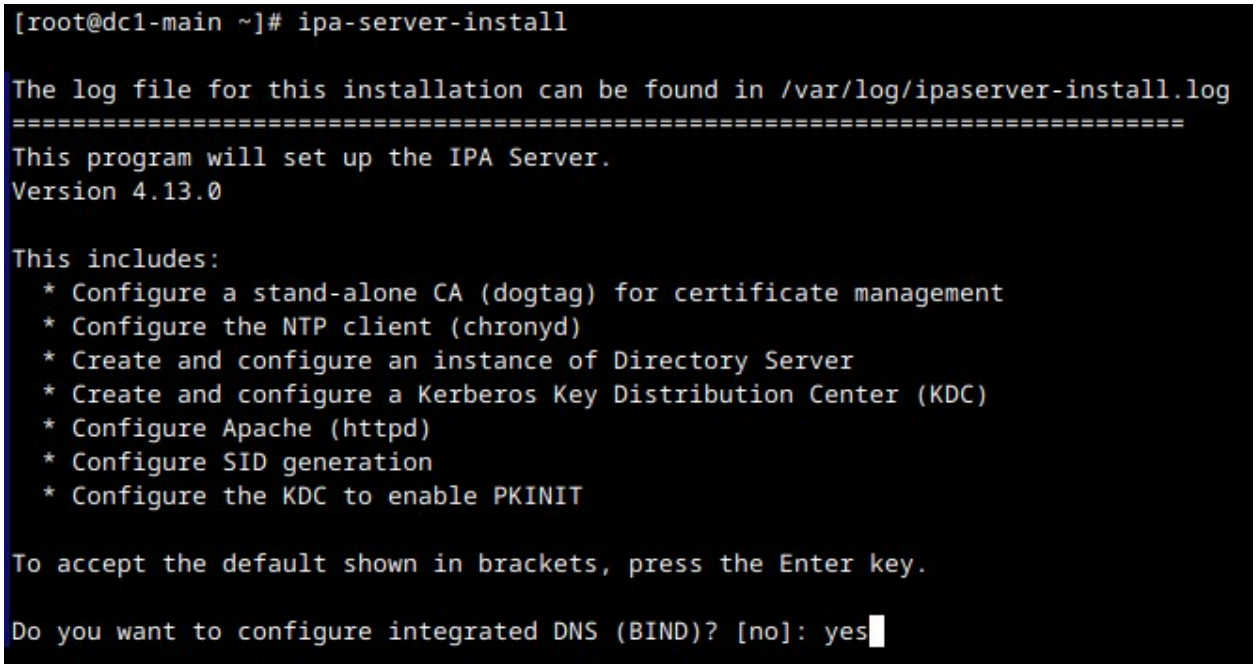


Рисунок 6 – Сценарий установки

Для подтверждения всех сделанных настроек конфигурации службы каталогов следует ввести yes:

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

Сценарий приступит к установке службы каталогов в соответствии с заданной конфигурацией.

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

Далее на сервере необходимо отключить или настроить брандмауэр:

- команда отключения брандмауэра:

```
systemctl stop firewalld
```

- команда настройки брандмауэра:

```
firewall-cmd --add-service=freeipa-4 --add-service=dns
--add-service=ntp --add-service=freeipa-replication --permanent
&& firewall-cmd –
reload
```

- вариант команды настройки брандмауэра, в том числе для организации доверительных отношений с лесом MS AD:

```
firewall-cmd --add-service=freeipa-4 --add-service=dns
--add-service=ntp --add-service=freeipa-replication
--add-service=freeipa-trust –
permanent && firewall-cmd --reload
```

После выполнения конфигурации сервера нужно выполнить команду `dd-sssd-config`, которая настроит SSSD для возможности входа на сервер пользователями, находящимися в расположениях отличных от стандартного:

```
dd-sssd-config
```

На этом установка основных служб Системы на сервере завершена.

Если планируется использование доверительных отношений с MS AD, необходимо также выполнить настройку компонента ipa-server-trust-ad, описанную в пункте 8.1.1 документа "Dynamic Directory. Руководство администратора. Часть 2. Эксплуатация".

После установки службы каталогов и настройки межсетевого экрана станет доступным вход в перспективы Dynamic Directory.

### 3.2.3 Установка с использованием сертификата

Для использования центром сертификации CA сертификата, выпущенного сторонним сервером сертификации, необходимо добавить опцию --external-ca, если сервер сертификации является сервером Microsoft; также необходимо указать его тип опцией --external-ca-type=ms-cs и OID профиля сертификата опцией --external-ca-profile.

Команда установки выглядит следующим образом:

```
ipa-server-install --setup-dns --mkhomedir --external-ca
```

Основные шаги установки аналогичны тем, что описаны в п. 3.2.2, но установка разделена на два этапа.

На первом этапе требуется создать файл запроса сертификата *.csr, который оканчивается текстом:

```
The next step is to get /root/ipa.csr signed by your CA and
re-run /usr/sbin/ipa-server-install as:
/usr/sbin/ipa-server-install
--external-cert-file=/path/to/signed_certificate
--external-cert-file=
/path/to/external_ca_certificate
```

После этого необходимо, используя файл /root/ipa.csr, выпустить сертификат для сервера, применив сторонний центр сертификации. Далее скопировать полученный сертификат и CA-сертификат центра сертификации на настраиваемый сервер, например, под именами /root/ipa.cer и /root/ca.cer.

На втором этапе необходимо повторно выполнить команду ipa-server-install, дополнительно указав в опции --external-cert-file путь до сертификата сервера и CA-сертификата сервера сертификации, его выпустившего, например:

```
ipa-server-install --setup-dns --mkhomedir --external-cert-file
/root/ipa.cer --external-cert-file /root/ext-ca.cer
```

### 3.2.4 Настройка дополнительного сервера Dynamic Directory

**Следует обратить внимание**, что если планируется использовать двусторонние доверительные отношения с доменами MS AD и общие ресурсы в доменах MS AD пользователями Dynamic Directory, то перед выполнением сценария установки на контроллере домена Dynamic Directory необходимо отключить шифрование SHA-2. Данный вид шифрования не поддерживается операционными системами MS Windows для протокола Kerberos. Отключение шифрования SHA-2 должно быть произведено на каждом контроллере домена Dynamic Directory.

В конфигурационный файл /etc/crypto-policies/back-ends/krb5.config необходимо внести следующие правки:

```
[libdefaults]
permitted_enctypes = aes256-cts-hmac-sha1-96
aes128-cts-hmac-sha1-96
```

После изменений в файле /etc/crypto-policies/back-ends/krb5.config необходимо выполнить перезагрузку.

Для настройки дополнительного сервера (реплики) Dynamic Directory нужно выполнить следующие шаги:

а) создать обратную запись DNS для нового сервера на установленном контроллере домена:

– получить билет Kerberos от пользователя, имеющего права на обратную зону DNS, к которой принадлежит добавляемый сервер (или от имени пользователя admin), выполнив команду вида "kinit ЛОГИН_ПОЛЬЗОВАТЕЛЯ", например:

```
kinit admin
```

– добавить PTR-запись в обратную зону, выполнив команду:

```
ipa dnsrecord-add ИМЯ_ОБРАТНОЙ_ЗОНЫ. ИМЯ_ЗАПИСИ --ptr-rec
FQDN_СЕРВЕРА.
```

Например, для сервера с FQDN dc2-main.lin.rosa и IP-адресом 11.22.33.44 команда для добавления в зону 33.22.11.in-addr.arpa будет выглядеть так:

```
ipa dnsrecord-add 33.22.11.in-addr.arpa. 44 --ptr-rec
dc2-main.lin.rosa.
```

б) задать имя сервера в формате FQDN, используя команду hostnamectl или отредактировав файл /etc/hostname (при редактировании файла напрямую после внесения изменений необходимо перезапустить сервер), например, для сервера dc2-main и домена lin.rosa:

```
hostnamectl set-hostname dc2-main.lin.rosa
```

в) в качестве DNS указать работающий сервер службы каталогов Dynamic Directory:

```
nmtui
```

г) на создаваемой реплике отключить или настроить брандмауэр:

- отключить брандмауэр:

```
systemctl stop firewalld
```

- настроить брандмауэр:

```
firewall-cmd --add-service=freeipa-4 --add-service=dns
--add-service=ntp --add-service=freeipa-replication --permanent
&& firewall-cmd –
reload
```

- настроить брандмауэр, в том числе для организации доверительных отношений с лесом MS AD:

```
firewall-cmd --add-service=freeipa-4 --add-service=dns
--add-service=ntp --add-service=freeipa-replication
--add-service=freeipa-trust –
permanent && firewall-cmd --reload
```

д) выполнить команду создания реплики:

```
ipa-replica-install --mkhomedir -w password --setup-dns
--setup-ca --forwarder=11.22.33.1
```

При доверии с MS AD:

```
ipa-replica-install --mkhomedir -w password --setup-dns
--setup-ca --setup-adtrust --forwarder=11.22.33.1
```

где:

– "--mkhomedir" – создание домашних директорий при входе доменных пользователей;

– "-w password" – пароль пользователя admin;

– "--setup-dns" – установка реплики с DNS;

– "--setup-ca" – установка реплики с интегрированным CA;

– "--setup-adtrust" – установка доверительных отношений с MS AD;

– "--forwarder=11.22.33.1" – установка сервера с IP-адресом 11.22.33.1 в качестве сервера перенаправления DNS.

**Следует учитывать**, что:

– Параметр --forwarder может использоваться несколько раз для указания нескольких серверов перенаправления.

– Вместо указания серверов перенаправления (параметр --forwarder) можно использовать --no-forwarders, тогда будет использоваться глобальная политика перенаправления DNS, если она настроена, либо перенаправление DNS использоваться не будет, если глобальная политика не настроена, или --auto-forwarders – серверы перенаправления DNS будут взяты из файла /etc/reslov.conf настраиваемого сервера.

– Если для подключения реплики используется пользователь, отличный от admin, необходимо указать его параметром -p, например "-p otheradmin".

После выполнения конфигурации сервера нужно выполнить команду dd-sssd-config, которая настроит SSSD для возможности входа на сервер пользователями, находящимися в расположениях, отличных от стандартного:

```
dd-sssd-config
```

### 3.2.4.1 Настройка сегментов репликации (топологии)

По умолчанию при вводе реплики командой `ipa-replica-install` создаётся один сегмент репликации между новым сервером и тем сервером, с которого выполнялась установка. Для обеспечения отказоустойчивости и соответствия рекомендациям, изложенным в п. 2.3.1.2 настоящего Руководства,

необходимо настроить дополнительные (перекрёстные) сегменты репликации между серверами.

Для просмотра существующих сегментов репликации необходимо получить билет Kerberos и выполнить команды:

```
kinit admin
ipa topologysuffix-find
ipa topologysegment-find
```

Для просмотра топологии конкретного суффикса (например, domain или ca) выполнить команды:

```
ipa topologysegment-find domain
ipa topologysegment-find ca
```

Для создания перекрёстного сегмента репликации между двумя существующими серверами необходимо выполнить команду:

```
ipa topologysegment-add domain --left FQDN_СЕРВЕРА_1 --right
FQDN_СЕРВЕРА_2
```

где:

– domain – суффикс репликации (допустимые значения: domain, ca, adtrust);

– --left – полное доменное имя первого сервера сегмента;

– --right – полное доменное имя второго сервера сегмента.

Пример создания перекрёстного сегмента между серверами dc1-main.lin.rosa и dc3-main.lin.rosa для суффикса домена:

```
ipa topologysegment-add domain --left dc1-main.lin.rosa --right
dc3-main.lin.rosa
```

При необходимости одновременного создания сегментов для суффиксов domain и ca команду следует выполнить для каждого суффикса отдельно:

```
ipa topologysegment-add domain --left dc1-main.lin.rosa --right
dc3-main.lin.rosa
ipa topologysegment-add ca --left dc1-main.lin.rosa --right
dc3-main.lin.rosa
```

Для удаления сегмента репликации необходимо выполнить команду:

```
ipa topologysegment-del domain ИМЯ_СЕГМЕНТА
```

Имя сегмента формируется автоматически в формате FQDN_-СЕРВЕРА_1-to-FQDN_СЕРВЕРА_2 и может быть уточнено командой `ipa topologysegment-find`.

После добавления сегментов рекомендуется проверить состояние репликации:

```
ipa-replica-manage list FQDN_СЕРВЕРА
```

Для принудительной инициализации репликации по конкретному сегменту (при необходимости) выполнить:

```
ipa topologysegment-reinitialize domain ИМЯ_СЕГМЕНТА
--direction left-right
```

где параметр --direction принимает значения left-right или right-left и определяет направление инициализации данных.

**Рекомендации по построению топологии**

При настройке сегментов репликации необходимо соблюдать следующие правила (п. 2.3.1.2):

– каждый сервер должен быть связан сегментами репликации как минимум с двумя другими серверами;

– количество сегментов репликации для каждого суффикса на одном сервере не должно превышать четырёх;

– в рамках одного ЦОД все серверы должны быть связаны друг с другом для обеспечения репликации домена в пределах ЦОД;

– каждый ЦОД должен быть связан как минимум с двумя другими ЦОД для обеспечения межплощадочной репликации;

– общее количество серверов Dynamic Directory в рамках одного домена не должно превышать 60.

Пример топологии для трёх серверов в одном ЦОД (полносвязная схема):

```
dc1-main.lin.rosa ←→ dc2-main.lin.rosa
dc1-main.lin.rosa ←→ dc3-main.lin.rosa
dc2-main.lin.rosa ←→ dc3-main.lin.rosa
```

П р и м е ч а н и е — Изменение топологии репликации вступает в силу немедленно. Специальная перезагрузка серверов не требуется.

### 3.2.5 Вывод из эксплуатации сервера Dynamic Directory

#### 3.2.5.1 Подготовка к выводу из эксплуатации

Для вывода сервера из эксплуатации необходимо соблюдение следующих условий:

– доступ к удаляемому серверу с root-привилегиями;

– наличие учётных данных администратора Dynamic Directory;

– удаление сервера не должно привести к отключению топологии, т. е. не нарушить связь между другими серверами в топологии;

– выводимый из эксплуатации сервер не должен быть единственным сервером DNS, единственным сервером CA или единственным сервером KRA, не должен быть сервером обновления сертификатов и сервером генерации списка отзыва сертификатов. Роли сервера обновления сертификатов и сервера генерации списка отзыва сертификатов обычно имеет сервер, который был развёрнут первым (если роли не переназначались).

Для подготовки к выводу из эксплуатации требуется выполнение следующих шагов:

а) проверить сервер на роли единственного сервера DNS, единственного сервера CA или единственного сервера KRA можно, выполнив на любом из контроллеров домена от имени администратора домена, команды:

```
$ ipa server-role-find --role 'CA server'
$ ipa server-role-find --role 'DNS server'
$ ipa server-role-find --role 'KRA server'
```

П р и м е ч а н и е — Роль KRA не настраивается в установке по умолчанию и может отсутствовать.

б) проверить при необходимости сервер на роль сервера обновления сертификатов, выполнив на любом из контроллеров домена от имени администратора домена команду:

```
$ ipa config-show |grep "Главный сервер обновления CA IPA"
```

в) назначить новый сервер обновления сертификатов:

```
$ ipa config-mod --ca-renewal-master-server
<FQDN_НОВОГО_СЕРВЕР>A
```

в) проверить, не является ли сервер сервером генерации списка отзыва сертификатов, выполнив на нём команду:

```
$ ipa-crlgen-manage status
```

Если в выводе указано "Enable", выполнить на выводимом из эксплуатации сервере команду:

```
$ ipa-crlgen-manage disable
```

А на другом сервере с ролью CA:

```
$ ipa-crlgen-manage enable
```

Если выводимый сервер недоступен, и неизвестно является ли он сервером генерации списка отзыва сертификатов, следует выполнить на всех серверах в инфраструктуре команду:

```
$ ipa-crlgen-manage status
```

и, если на всех серверах получен ответ "Disable", на одном из остающихся серверов нужно выполнить:

```
$ ipa-crlgen-manage enable
```

г) на одном из серверов выполнить от имени администратора домена команду:

```
$ ipa-replica-manage dnarange-show
```

Диапазон DNA ID должен присутствовать на серверах, остающихся в топологии.

Если диапазон DNA ID присутствует только на выводимом из эксплуатации сервере, необходимо на другом сервере создать тестового пользователя и снова проверить диапазоны DNA ID, выполнив:

```
$ ipa-replica-manage dnarange-show
```

#### 3.2.5.2 Вывод из эксплуатации

Для вывода из эксплуатации сервера Dynamic Directory на одном из серверов, остающихся в топологии, от имени администратора домена нужно выполнить команду:

```
$ ipa server-del <FQDN_УДАЛЯЕМОГО_СЕРВЕРА>
```

Если это приведёт к нарушению топологии или если сервер имеет уникальную роль, в выводе будет выдано соответствующее предупреждение. В этом случае следует отказаться от операции, добавить другим серверам уникальные роли и/или создать связи между серверами, которые остаются в эксплуатации, и затем повторить операцию.

Далее на сервере, выводимом из эксплуатации, выполнить команду:

```
$ ipa-server-install --uninstall
```

Для проверки необходимо убедиться, что в служебных DNS-записях типа SRV отсутствует выведенный из эксплуатации сервер. В случае наличия сервера в таких записях, нужно удалить данные о нём вручную.

### 3.3 Установка сервера Puppet

Для функционирования Системы необходимо установить серверное программное обеспечение Puppet Server на сервер управления, работающий в домене.

Для установки сервера Puppet в окне "Обзор установки" нужно нажать на наименование секции "Выбор программ" (рисунок 7).

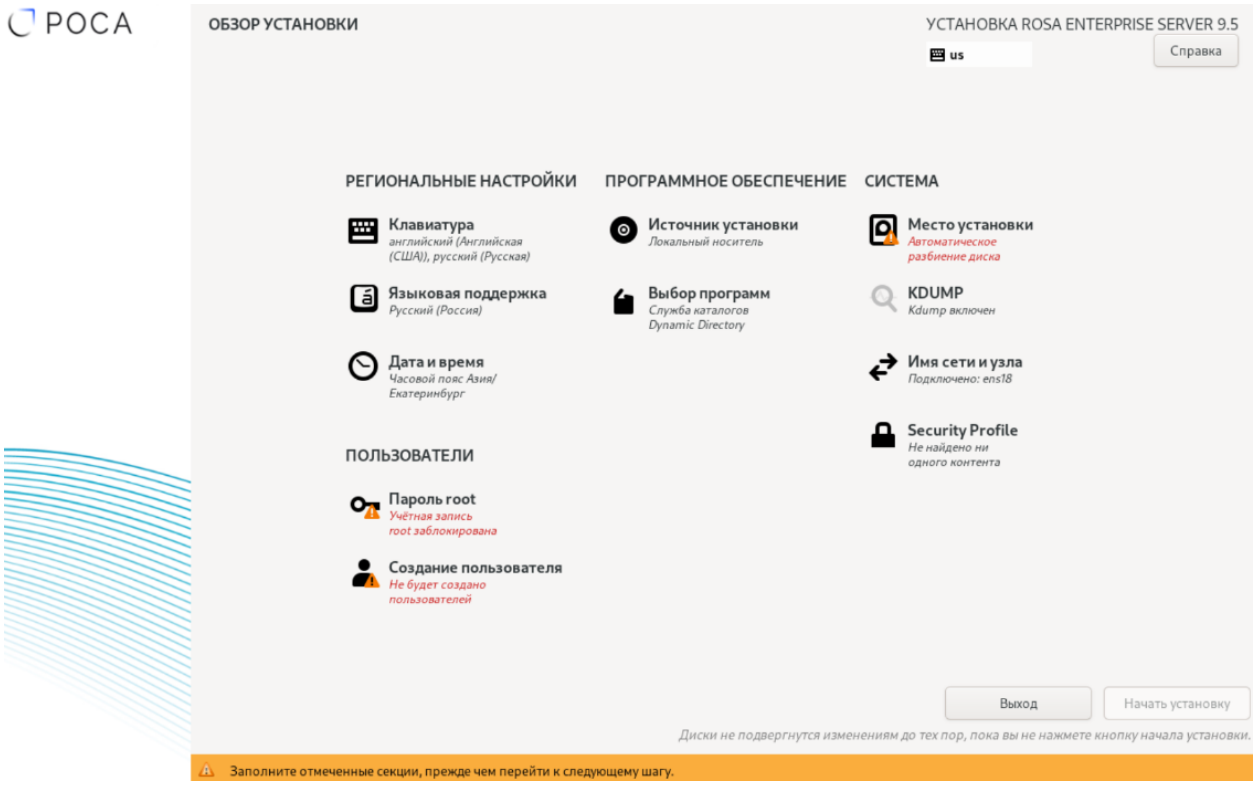


Рисунок 7 – Обзор установки

В секции "Выбор программ" нужно указать переключатель "Базовое окружение" в положение "Puppet Server для Dynamic Directory" для установки соответствующего базового ПО на сервер и нажать кнопку `Готово` (рисунок 8) для возвращения в меню "Обзор установки".

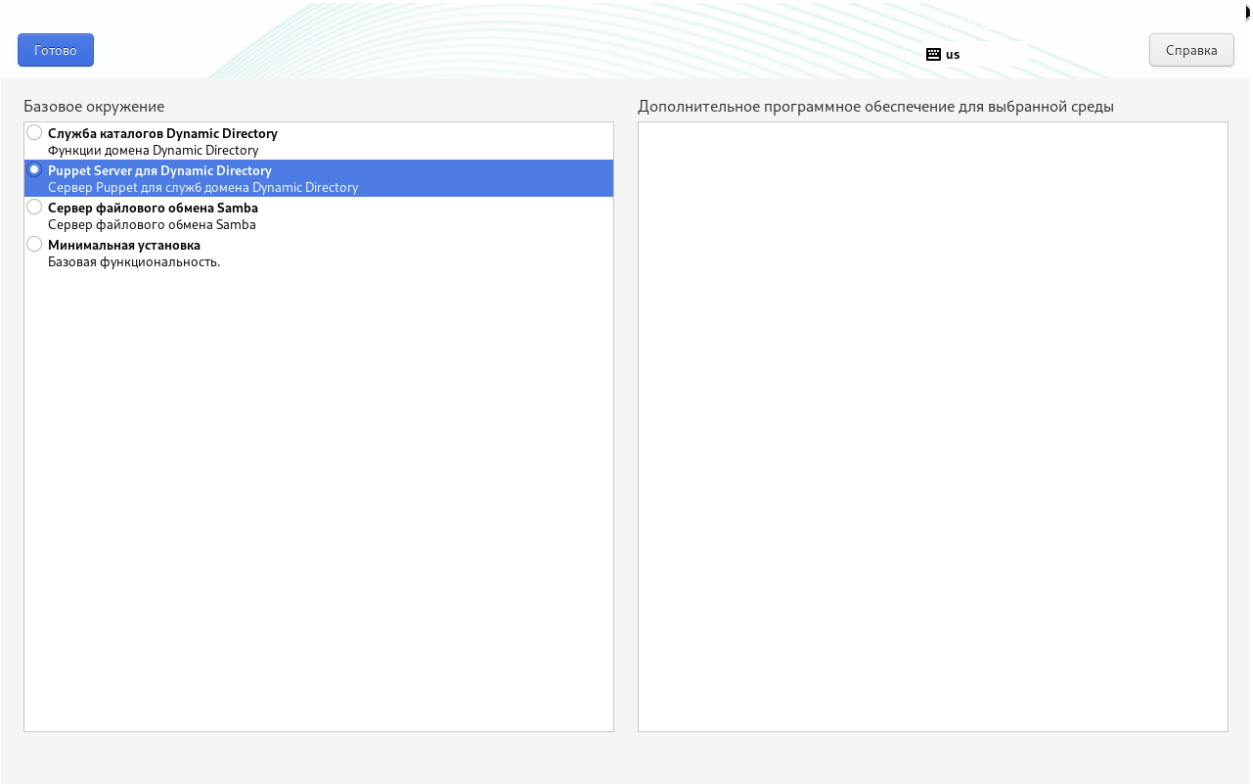


Рисунок 8 – Выбор секции установки

Далее необходимо задать имя сервера в формате FQDN с указанием домена под управлением Dynamic Directory (рисунок 9).

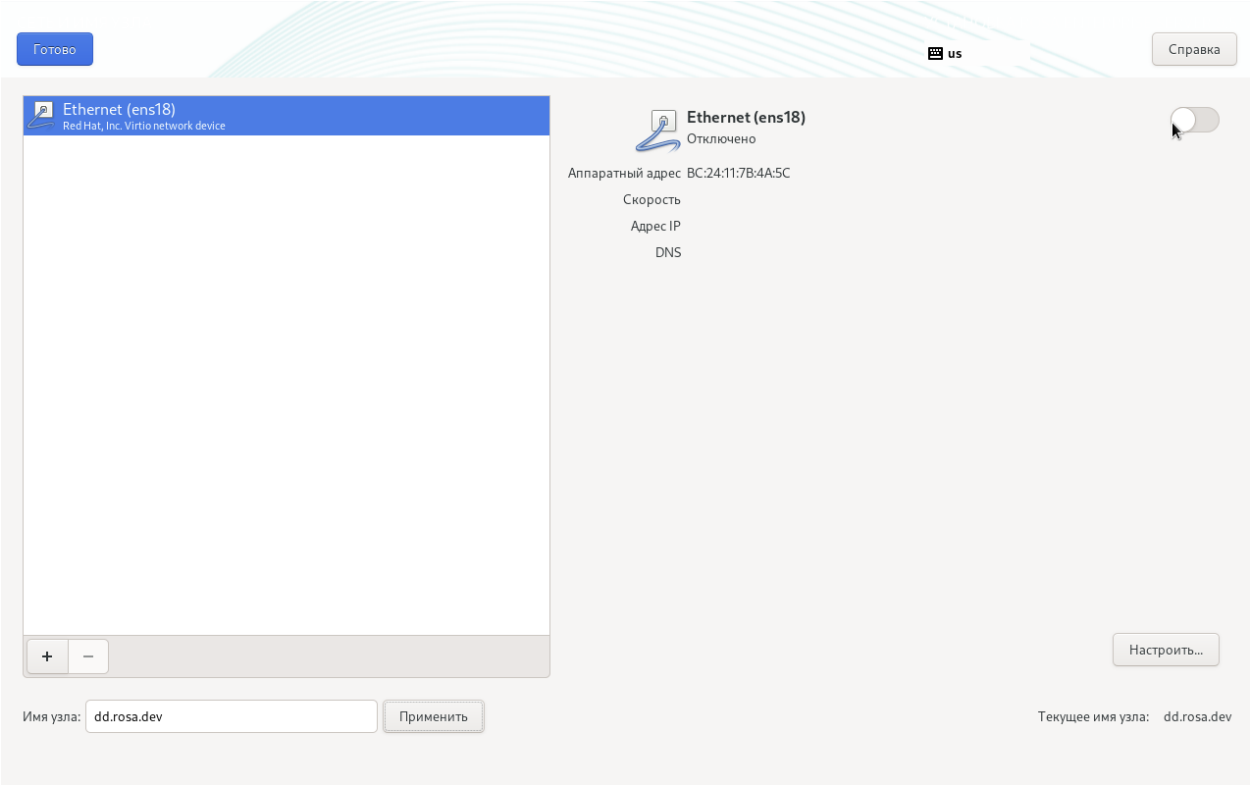


Рисунок 9 – Настройка сервера

Затем в настройках сети нужно указать серверы Dynamic Directory в качестве DNS-серверов. В качестве домена поиска следует указать имя домена Dynamic Directory (рисунок 10).

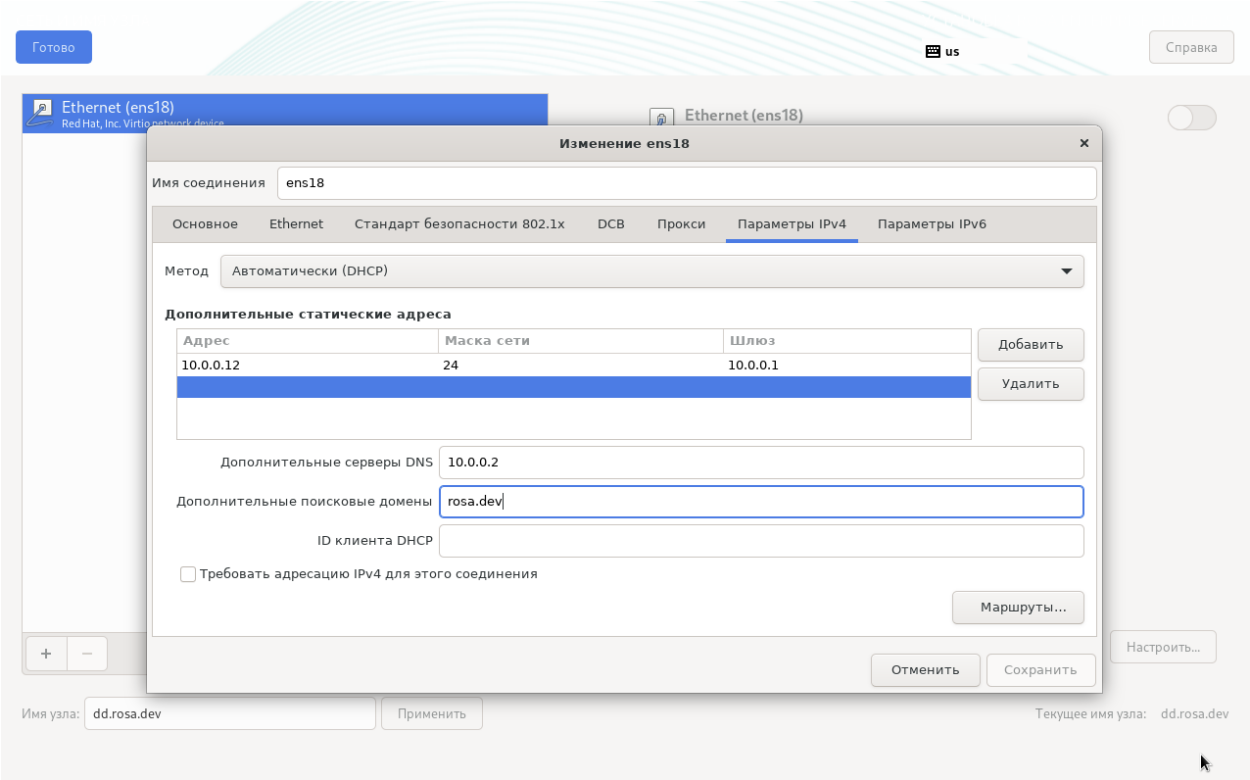


Рисунок 10 – Настройка сети

После установки сервера необходимо выполнить его ввод в домен командой:

```
ipa-client-install --mkhomedir
```

После установки клиента нужно выполнить дополнительное конфигурирование SSSD командой:

```
dd-sssd-config
```

После этого необходимо сконфигурировать брандмауэр, выполнив команды:

```
firewall-cmd --permanent --add-service=puppetmaster
firewall-cmd --reload
```

### 3.3.1 Обновление сервера Puppet

Для обновления сервера Puppet необходимо выполнить следующие шаги:

а) Подключить репозиторий, выполнив команду:

```
dnf install rosa-release-dd-4.3
```

б) Выполнить команды:

```
dnf makecache
dnf update
```

в) Выполнить команду для обновления сервера Puppet:

```
systemctl restart puppetserver
```

## 3.4 Обновление Dynamic Directory

### 3.4.1 Обновление с версии 4.1 до 4.2

Для обновления Dynamic Directory с версии 4.1 до версии 4.2 необходимо выполнить следующее:

На сервере:

а) смонтировать ISO-образ Dynamic Directory 4.2:

```
mount /dev/sr0 /mnt
```

б) в файле /etc/yum.repos.d/ROSA-res9.repo найти группу параметров DVD и изменить параметр enabled на "1" (рисунок 11)

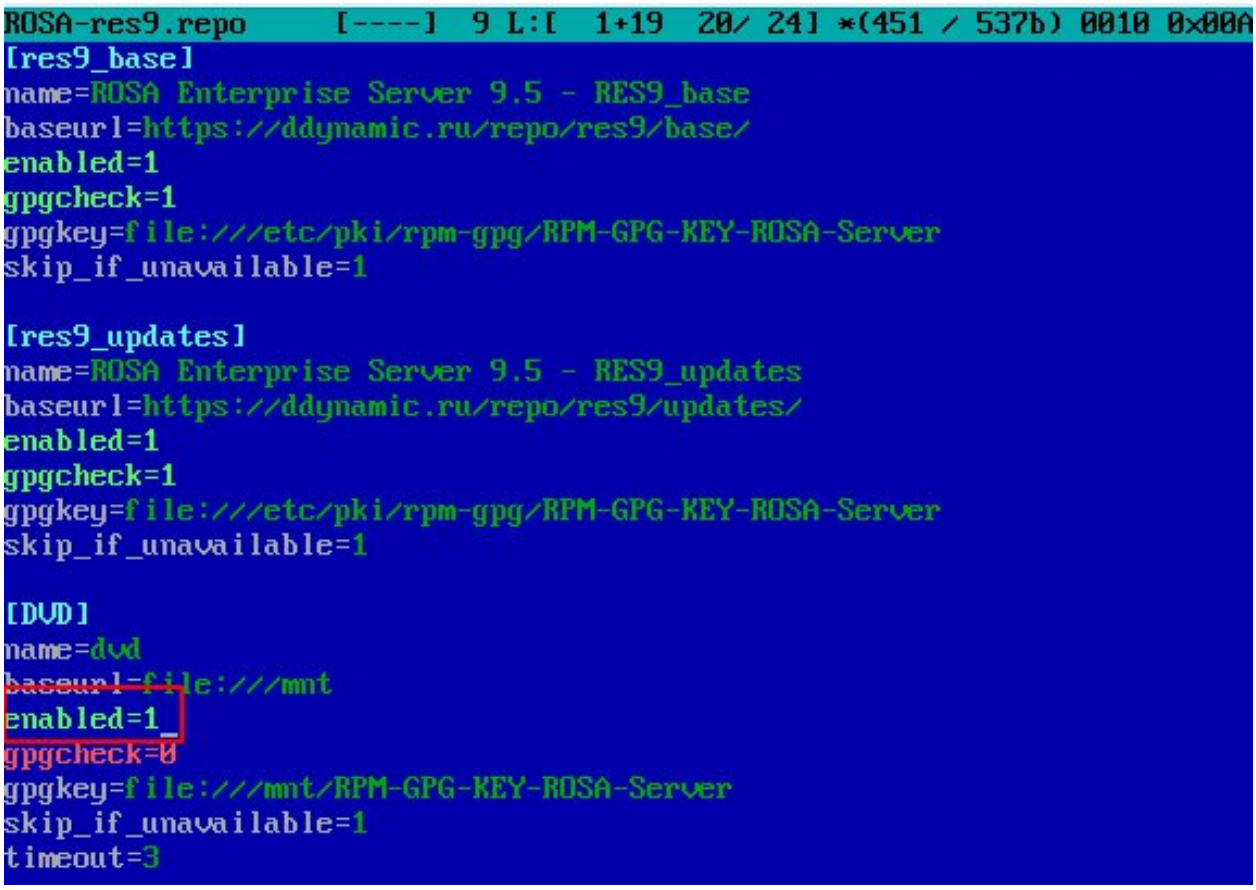


Рисунок 11 – Редактирование файла ROSA-res9.repo

в) выполнить команды:

```
dnf makecache
dnf update
```

г) после окончания процедуры обновления пакетов выполнить команду:

```
ipa-server-upgrade
```

На стороне клиентских АРМ, включая АРМ Администратора, необходимо установить пакеты для подключения репозиториев Dynamic Directory 4.2:

– Для ОС Alt Linux p10:

```
apt-get install https://ddynamic.ru/dd/4.2/alt/noarch/RPMS.clas⌋
sic/dd-release-4.2-1.0.
0-1.alt.noarch.rpm
apt-get update
```

- Для ОС Astra 1.7.x:

```
wget https://ddynamic.ru/dd/4.2/astra/pool/non-free/d/dd-releas⌋
e-4.2/dd-release-4.
2_1.0.0-1.astra_all.deb -O /tmp/dd-release-4.2.deb
apt-get install /tmp/dd-release-4.2.deb
apt-get update
```

- Для ОС RedOS 7:

```
dnf install https://ddynamic.ru/dd/4.2/redos/7/dd-release-4.2-1⌋
.0.0-1.redos7.
noarch.rpm
dnf makecache
dnf update
```

- Для ОС RedOS 8:

```
dnf install https://ddynamic.ru/dd/4.2/redos/8/dd-release-4.2-1⌋
.0.0-1.redos8.
noarch.rpm
dnf makecache
dnf update
```

- Для ОС РОСА "ХРОМ":

```
dnf install https://ddynamic.ru/dd/4.2/rosa/chrome/dd-release-4⌋
.2-1.0.0-1.chrome.
noarch.rpm
dnf makecache
dnf update
```

- Для ОС РОСА "КОБАЛЬТ":

```
yum install https://ddynamic.ru/dd/4.2/rosa/res7/dd-release-4.2-
1.0.0-1.res7.
noarch.rpm
yum makecache
yum update
```

### 3.4.2 Обновление с версии 4.2 до 4.3

Для обновления Dynamic Directory с версии 4.2 до версии 4.3 необходимо выполнить **на сервере** следующее:

а) смонтировать ISO-образ Dynamic Directory 4.3:

```
mount /dev/sr0 /mnt
```

б) в файле /etc/yum.repos.d/ROSA-res9.repo найти группу параметров DVD и изменить параметр enabled на "1" (рисунок 12)

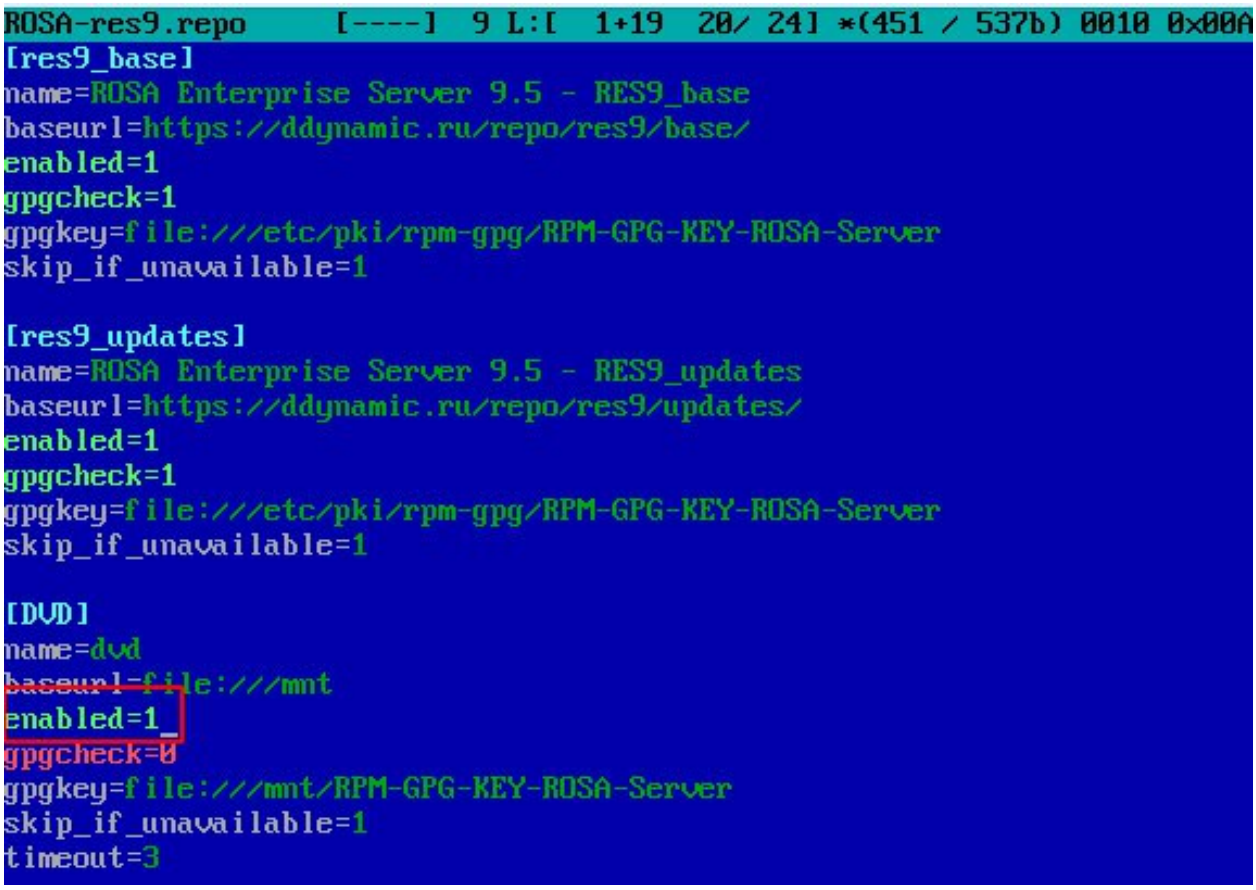


Рисунок 12 – Редактирование файла ROSA-res9.repo

в) выполнить команды:

```
dnf makecache
dnf update --allowerasing
```

Либо предварительно удалить пакет rsyslog-logrotate:

```
dnf remove -y rsyslog-logrotate
dnf update
```

П р и м е ч а н и е — В Dynamic Directory 4.3 функционал rsyslog-logrotate включён в основной пакет.

г) после окончания процедуры обновления пакетов выполнить команду:

```
ipa-server-upgrade
```

При обновлении до версии 4.3 с помощью утилиты ipa-server-upgrade групповые политики обновляются автоматически. Для использования нового функционала политик необходимо обновить консоль управления Dynamic Directory (dd-admin) до версии 4.3 или выше.

На стороне **клиентских АРМ**, включая АРМ Администратора, необходимо установить пакеты для подключения репозиториев Dynamic Directory 4.3:

- для ОС Alt Linux p10:

```
apt-get install https://ddynamic.ru/dd/4.3/alt/noarch/RPMS.clas⌋
sic/dd-release-4.3-1.0.
0-1.alt.noarch.rpm
```

- для Alt Linux SP:

```
apt-get install https://ddynamic.ru/dd/4.3/alt-sp/noarch/RPMS.c⌋
lassic/dd-release-4.3-1.
0.0-1.alt_sp.noarch.rpm
```

- для ОС Astra 1.7.x:

```
wget https://ddynamic.ru/dd/4.3/astra/pool/non-free/d/dd-releas⌋
e-4.3/dd-release-4.
3_1.0.0-1.astra_all.deb -O /tmp/dd-release-4.3.deb
apt-get install /tmp/dd-release-4.3.deb
apt-get update
```

- для ОС RedOS 7:

```
dnf install https://ddynamic.ru/dd/4.3/redos/7/dd-release-4.3-1⌋
.0.0-1.redos7.
noarch.rpm
dnf makecache
```

- для ОС RedOS 8:

```
dnf install https://ddynamic.ru/dd/4.3/redos/8/dd-release-4.3-1
.0.0-1.redos8.
noarch.rpm
dnf makecache
```

- для ОС РОСА "ХРОМ" 12:

```
dnf install https://ddynamic.ru/dd/4.3/rosa/chrome/dd-release-4
.3-1.0.0-1.chrome.
noarch.rpm
dnf makecache
```

- для ОС РОСА "ХРОМ" 13:

```
dnf install https://ddynamic.ru/dd/4.3/rosa/chrome_13/dd-releas
e-4.3-1.0.0-1.
chrome13.noarch.rpm
dnf makecache
```

- для ОС РОСА "КОБАЛЬТ":

```
yum install https://ddynamic.ru/dd/4.3/rosa/res7/dd-release-4.3-
1.0.0-1.res7.
noarch.rpm
yum makecache
```

### 3.4.3 Обновление через интернет-репозиторий

Для обновления через интернет-репозиторий необходимо выполнить следующее:

а) перейти на основной контроллер домена Комплекса под учетной записью root или через sudo поднять права до root (если root не был использован при установке) и выполнить команду подключения серверного репозитория Dynamic Directory 4.3:

```
dnf install rosa-release-dd-4.3
```

б) выполнить команды:

```
dnf makecache
dnf update --allowerasing
```

в) после окончания процедуры обновления пакетов выполнить команду:

```
ipa-server-upgrade
```

г) дождаться завершения обновления.

После обновления на основном контроллере домена если есть реплики, то необходимо последовательно выполнить аналогичные команды обновления и на них.

**Следует обратить внимание**, что обновление одного сервера IdM может занимать от 10 минут и дольше. Точное время зависит от топологии сети, задержки связи и объема изменений. Если серверы обновляются параллельно или с короткими интервалами, возникает риск конфликтов репликации. Системе требуется время, чтобы синхронизировать данные между всеми узлами.

Необходимо также обновить утилиту управления Dynamic Directory – dd-admin. Для этого нужно подключить репозиторий Dynamic Directory 4.3 для используемой системы (п. 3.4.2)

После подключения нужно выполнить команду обновления для конкретной системы.

Для ОС РОСА "XPOM" (12/13) нужно выполнить команду:

```
dnf update
```

## 3.5 Настройка сервера журналирования Rsyslog

Для настройки сервера журналирования необходимо установить минимальную конфигурацию REL.

Затем в файле /etc/rsyslog.conf нужно раскомментировать следующие строки:

```
Для получения журналов по протоколу UDP
module(load="imudp") # needs to be done just once
input(type="imudp" port="514")
```

```
Для получения журналов по протоколу TCP
module(load="imtcp") # needs to be done just once
input(type="imtcp" port="514")
```

После этого следует добавить в /etc/rsyslog.conf или создать файл /etc/rsyslog.d/01-remotelogs.conf со следующим содержанием:

```
$template
RemoteLogs,"/var/log/remote-logs/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& ~=
```

Затем перезапустить службу журналирования командой:

```
systemctl restart rsyslog
```

Добавить правило в Firwalld для UDP:

```
firewall-cmd --add-service syslog --permanent
```

Добавить правило в Firwalld для TCP:

```
firewall-cmd --add-port=514/tcp --permanent
```

Перезапустить Firewalld:

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

### 3.5.1 Настройка пересылки журналов Rsyslog

Для настройки пересылки всех журналов необходимо в /etc/rsyslog.d создать файл 01-remote-all.conf со следующим содержанием:

```
*.* @@11.22.33.44
```

где 11.22.33.44 – IP--адрес сервера журналирования.

Затем нужно перезапустить службу журналирования командой:

```
systemctl restart rsyslog
```

### 3.6 Установка ОС на сервер файлового обмена

Установка ОС на сервер файлового обмена осуществляется системным администратором с использованием носителя с дистрибутивом из комплекта поставки Комплекса.

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

На экране последовательно появятся меню программы установки, интерфейс для выбора языка сопровождения установки и меню "Обзор установки", предназначенное для обзора и последующей настройки параметров установки (рисунок 13).

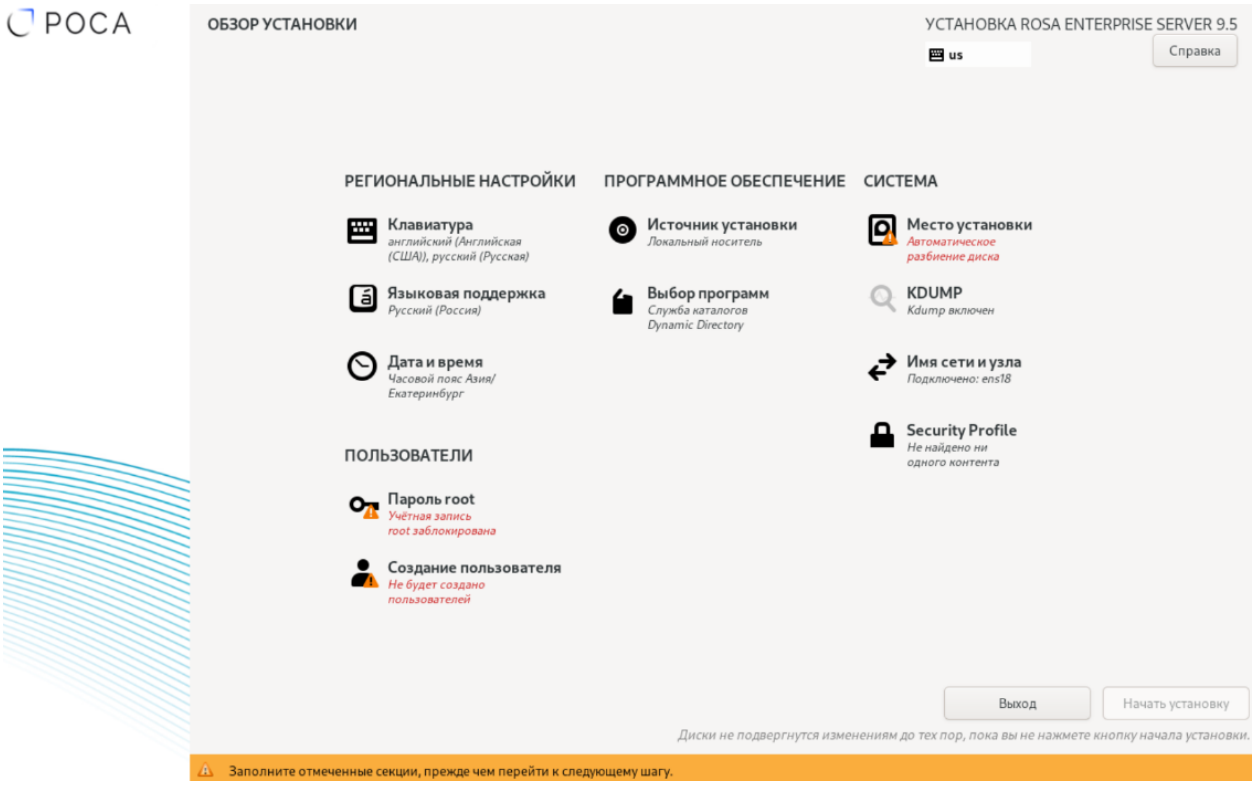


Рисунок 13 – Обзор установки

Меню "Обзор установки" содержит тематические секции, в которые сгруппированы соответствующие параметры установки. Следует обратить

внимание, что вместо последовательного определения параметров программа установки дает возможность настроить параметры в произвольном порядке выбором необходимых секций в меню "Обзор установки".

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

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

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

В секции "Выбор программ" устанавливают переключатель "Базовое окружение" в положение "Сервер файлового обмена Samba" для установки соответствующего базового ПО на сервер файлового обмена (рисунок 14).

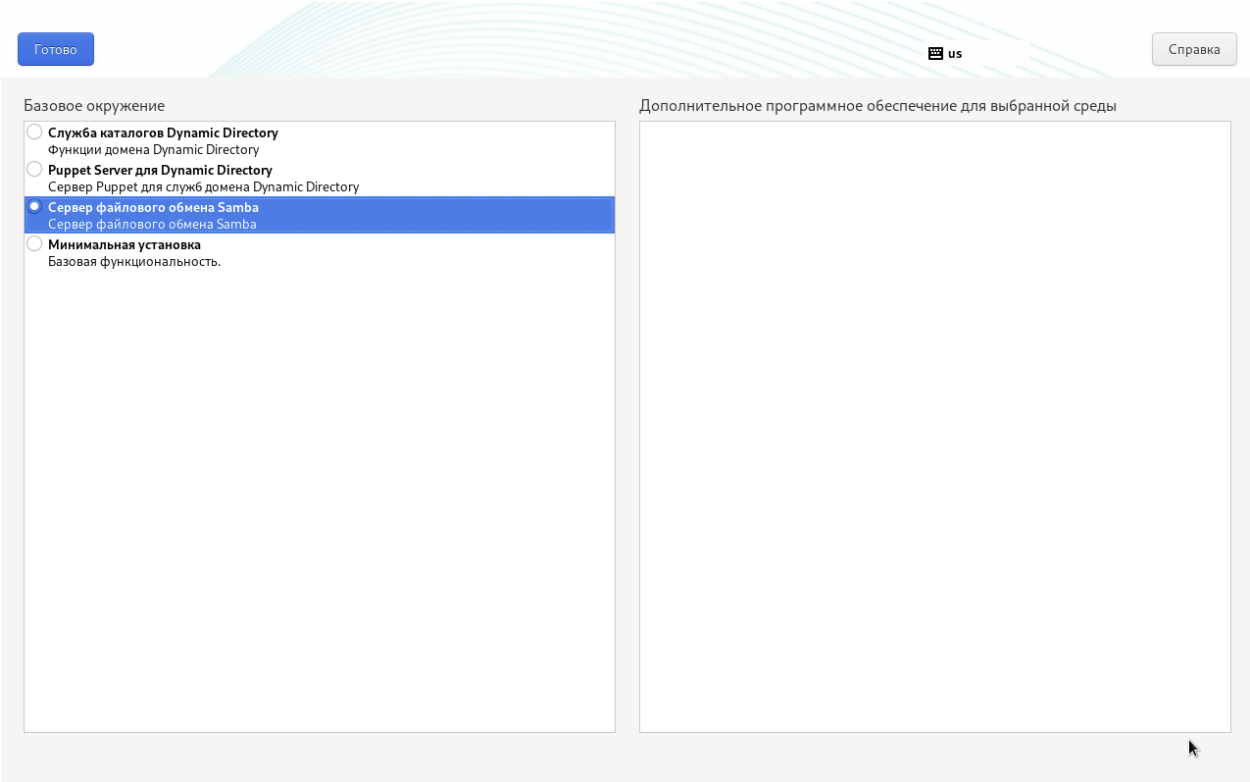


Рисунок 14 – Выбор базового ПО

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

В секции "Имя сети и узла" необходимо задать полное доменное имя файлового сервера, которое должно быть доменным именем по крайней мере третьего уровня (например, smb.rosa.dev, где smb – краткое имя узла, а rosa.dev – домен, в котором сервер будет выполнять функции сервера файлового обмена).

Далее подключают необходимый сетевой интерфейс файлового сервера и настраивают параметры сетевого соединения – IP-адрес (например, 10.0.0.4), маску сети (например, 255.255.0.0) и шлюз по умолчанию (например, 10.0.0.1).

**Необходимо обратить внимание**, что IP-адрес сетевого интерфейса сервера файлового обмена требуется задавать только статическим.

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

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

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

После перезагрузки системы на экране появится строка приглашения командного интерпретатора, в котором нужно выполнить следующие действия:

а) войти в систему под пользователем root;

б) отключить selinux, для чего выполнить команду:

```
setenforce 0
```

в) открыть в редакторе файлов, например в mcedit, файл конфигурации:

```
mcedit /etc/selinux/config
```

г) изменить параметр SELINUX на disabled (рисунок 15);

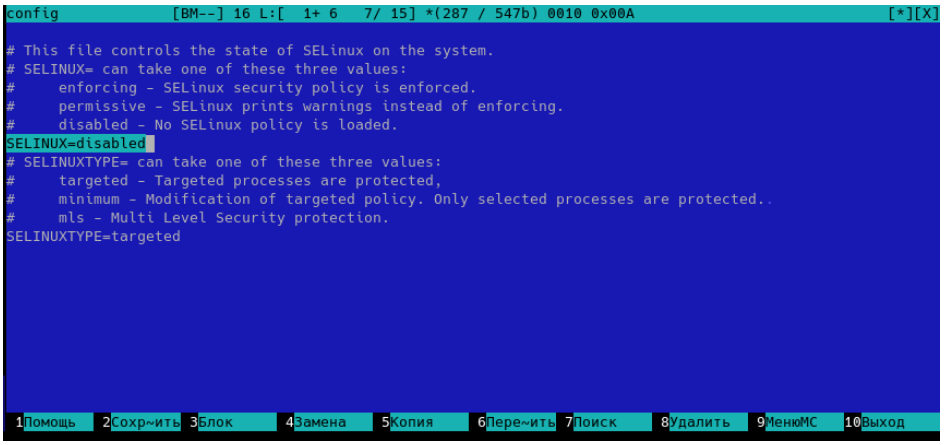


Рисунок 15 – Редактирование файла конфигурации

д) перегрузить компьютер командой:

```
reboot
```

После перезагрузки нужно войти в ОС под пользователем root.

Далее требуется произвести ввод сервера в домен, выполнив команду:

```
ipa-client-install
```

В результате должен быть получен примерно такой вывод команды:

```
This program will set up IPA client.
Version 4.9.10
Discovery was successful!
Do you want to configure chrony with NTP server or pool
address? [no]:
Client hostname: smb.rosa.dev
Realm: ROSA.DEV
DNS Domain: rosa.dev
IPA Server: dc.rosa.dev
BaseDN: dc=rosa,dc=dev
Continue to configure the system with these values? [no]: yes
Synchronizing time
```

```
No SRV records of NTP servers found and no NTP server or pool
address was provided.
Using default chrony configuration.
Attempting to sync time with chronyc.
Time synchronization was successful.
User authorized to enroll computers: admin
Password for admin@END.POINT:
Successfully retrieved CA cert
Subject: CN=Certificate Authority,O=END.POINT
Issuer: CN=Certificate Authority,O=END.POINT
Valid From: 2024-03-18 05:49:50
Valid Until: 2044-03-18 05:49:50
Enrolled in IPA realm ROSA.DEV
Created /etc/ipa/default.conf
Configured /etc/sssd/sssd.conf
Systemwide CA database updated.
Hostname (smb.end.point) does not have A/AAAA record.
Missing reverse record(s) for address(es): 10.0.0.4.
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Configuring end.point as NIS domain.
Configured /etc/krb5.conf for IPA realm ROSA.DEV
Client configuration complete.
The ipa-client-install command was successful
```

Затем следует перегрузить компьютер командой:

```
reboot
```

После перезагрузки нужно вновь войти в ОС под пользователем root.

Далее нужно получить действительный билет Kerberos пользователя, имеющего права на добавление служб в службе каталогов, для чего выполнить команду:

```
kinit admin
```

Затем требуется ввести пароль для заданного пользователя.

После успешного получения билета Kerberos можно произвести установку и настройку сервера файлового обмена, выполнив команду:

```
ipa-client-samba
```

Для подтверждения заданных параметров следует ввести ответ на вопрос yes.

Примерный вывод команды:

```
Searching for IPA server...
IPA server: DNS discovery
Chosen IPA master: dc.rosa.dev
SMB principal to be created: cifs/smb.rosa.dev@ROSA.DEV
NetBIOS name to be used: SMB
Discovered domains to use:
Domain name: rosa.dev
NetBIOS name: DEV
SID: S-1-5-21-867572240-1235709901-3344055872
ID range: 1412000000 - 1412199999
Continue to configure the system with these values? [no]: yes
Samba domain member is configured. Please check configuration
at /etc/samba/smb.conf and start smb and winbind services
```

Далее необходимо включить системные службы файлового сервера, выполнив команду:

```
systemctl enable --now smb winbind
```

После выполнения этих действий файловый сервер установлен и настроен.

Для проверки соединения следует выполнить команду:

```
smbclient -kL //$(hostname)/
```

Команда должна вывести доступные ресурсы на файловом сервере:

```
Sharename Type Comment
--------- ---- -------
homes Disk
IPC$ IPC IPC Service (Samba 4.16.4)
admin Disk Home directory of admin
SMB1 disabled — no workgroup available
```

Для создания тестового ресурса нужно выполнить следующие действия в командной строке:

а) создать каталог для тестирования:

```
mkdir -p /srv/share
```

б) задать права на созданный каталог:

```
chmod 755 /srv/share
```

в) создать каталог для пользователей:

```
mkdir -p /srv/share/private
```

г) задать права на созданный каталог:

```
chmod 755 /srv/share/private
```

д) создать каталог для групп пользователей:

```
mkdir -p /srv/share/groups
```

е) задать права на созданный каталог:

```
chmod 755 /srv/share/groups
```

ж) создать каталог "только для чтения" для всех пользователей:

```
mkdir -p /srv/share/readonly
```

з) задать права на созданный каталог:

```
chmod 755 /srv/share/readonly
```

и) создать каталог для "чтения-записи" для всех пользователей:

```
mkdir -p /srv/share/read-write
```

к) задать права на созданный каталог:

```
chmod 777 /srv/share/read-write
```

л) добавить в конфигурационный файл /etc/samba/smb.conf секцию конфигурации данного сетевого ресурса:

```
[share]
comment = test right
path = /srv/share
public = yes
writable = yes
read only = no
hide unreadable = yes
create mask = 0666
directory mask = 0777
force create mode = 0666
force directory mode = 0777
```

Для проверки созданного тестового ресурса следует выполнить команду:

```
smbclient -kL //$(hostname)/
```

Команда должна вывести доступные ресурсы, в том числе тестовый share, на файловом сервере:

```
Sharename       Type      Comment
---------       ----      -------
homes           Disk
share           Disk      test right
IPC$            IPC       IPC Service (Samba 4.16.4)
admin           Disk      Home directory of admin
SMB1 disabled — no workgroup available
```

### 3.6.1 Настройка сетевых ресурсов для групп доменных пользователей

Для организации работы с общими папками необходимо создать структуру каталогов и настроить права доступа для различных групп доменных пользователей. Ниже приведён порядок настройки **примерной** инфраструктуры, обеспечивающий разграничение доступа на уровне файловой системы и на уровне конфигурации Samba.

**Следует обратить внимание**, что перед настройкой необходимо создать новые группы или использовать названия, фактически присутствующие в инфраструктуре.

#### 3.6.1.1 Создание групп в службе каталогов

Перед настройкой файлового сервера **необходимо убедиться**, что в службе каталогов Dynamic Directory созданы соответствующие группы пользователей. Создание групп выполняется с АРМ администратора через консоль dd-admin либо консольной командой:

```
kinit admin
ipa group-add grp_accounting --desc="Бухгалтерия"
ipa group-add grp_engineering --desc="Инженерный отдел"
ipa group-add grp_management --desc="Руководство"
```

где:

– имя группы (например, grp_accounting) – уникальное имя создаваемой группы в службе каталогов;

– --desc – текстовое описание группы, отображаемое в консоли dd-admin и в атрибутах группы в каталоге. Параметр необязательный, но рекомендуется для удобства администрирования.

Добавление пользователей в группы:

```
ipa group-add-member grp_accounting --users=ivanov,petrova
ipa group-add-member grp_engineering --users=sidorov,kuznetsov
ipa group-add-member grp_management --users=director,cfo
```

где:

– имя группы (например, grp_accounting) – имя существующей группы, в которую добавляются пользователи;

– --users – список имён доменных пользователей, перечисленных через запятую без пробелов, которые необходимо добавить в группу.

### 3.6.1.2 Создание структуры каталогов на файловом сервере

На файловом сервере необходимо войти под учётной записью root и выполнить:

```
mkdir -p /srv/smb/accounting
mkdir -p /srv/smb/engineering
mkdir -p /srv/smb/management
mkdir -p /srv/smb/common
mkdir -p /srv/smb/common/read-only
```

где: - -p – создание всех промежуточных каталогов в указанном пути, если они ещё не существуют, а также подавление ошибки, если каталог уже создан; - путь (например, /srv/smb/accounting) – полный путь к создаваемому каталогу на файловом сервере.

### 3.6.1.3 Назначение владельца и групповых прав

Для каждого каталога необходимо задать владельцем пользователя root и соответствующую доменную группу. Имена групп в файловой системе определяются через SSSD и, как правило, совпадают с именами групп в службе каталогов:

```
chown root:grp_accounting /srv/smb/accounting
chown root:grp_engineering /srv/smb/engineering
chown root:grp_management /srv/smb/management
chown root:grp_management /srv/smb/common
```

где:

– root – имя пользователя-владельца каталога. В данном случае владельцем назначается суперпользователь;

– имя после двоеточия (например, grp_accounting) – доменная группа, которой назначается групповое владение каталогом;

– путь (например, /srv/smb/accounting) – путь к каталогу, для которого изменяются владелец и группа.

Примечание — Если имя группы не распознаётся, необходимо убедиться, что служба SSSD запущена и доменная группа кеширована. Для принудительного обновления кеша выполняется команда `sss_cache -E`.

### 3.6.1.4 Установка прав доступа (POSIX-права)

Права доступа задаются в соответствии с требуемой моделью разграничения:

– /srv/smb/accounting – устанавливаются права 2770, обеспечивающие полный доступ (чтение, запись, выполнение) для членов группы grp_accounting и полный запрет доступа для всех остальных пользователей. Бит setgid обеспечивает наследование группы для новых файлов;

– /srv/smb/engineering – устанавливаются права 2770, обеспечивающие полный доступ для членов группы grp_engineering и полный запрет доступа для всех остальных пользователей;

– /srv/smb/management – устанавливаются права 2770, обеспечивающие полный доступ для членов группы grp_management и полный запрет доступа для всех остальных пользователей;

– /srv/smb/common – устанавливаются права 2775, обеспечивающие чтение и запись для членов группы grp_management, а также чтение и выполнение для всех остальных доменных пользователей;

– /srv/smb/common/read-only – устанавливаются права 2775, обеспечивающие чтение для всех доменных пользователей и запись только для членов группы grp_management.

Примечание — Бит setgid (значение 2 в первой цифре) гарантирует, что все вновь создаваемые файлы и подкаталоги будут наследовать группу родительского каталога, а не первичную группу создавшего пользователя.

Команды установки прав:

```
chmod 2770 /srv/smb/accounting
chmod 2770 /srv/smb/engineering
chmod 2770 /srv/smb/management
chmod 2775 /srv/smb/common
chmod 2775 /srv/smb/common/read-only
```

где:

– первая цифра (например, 2 в 2770) – специальные биты: значение 2 означает установку бита setgid (наследование группы родительского каталога для создаваемых файлов и подкаталогов);

– вторая цифра (например, 7 в 2770) – права владельца каталога: 7 – чтение, запись и выполнение; 5 – чтение и выполнение;

– третья цифра (например, 7 в 2770) – права группы-владельца: 7 – чтение, запись и выполнение; 5 – чтение и выполнение; 0 – отсутствие доступа;

– четвёртая цифра (например, 0 в 2770) – права всех остальных пользователей: 0 – отсутствие доступа; 5 – чтение и выполнение;

– путь (например, /srv/smb/accounting) – путь к каталогу, для которого устанавливаются права доступа.

### 3.6.1.5 Конфигурирование ресурсов в /etc/samba/smb.conf

Для конфигурирование ресурсов в /etc/samba/smb.conf нужно:

а) открыть файл конфигурации Samba:

```
mcedit /etc/samba/smb.conf
```

б) добавить следующие секции в конец файла:

```
[accounting]
comment = Общий ресурс бухгалтерии
path = /srv/smb/accounting
valid users = @grp_accounting
read only = no
writable = yes
create mask = 0660
directory mask = 2770
force create mode = 0660
force directory mode = 2770
hide unreadable = yes
browseable = yes

[engineering]
comment = Общий ресурс инженерного отдела
path = /srv/smb/engineering
```

```
valid users = @grp_engineering
read only = no
writable = yes
create mask = 0660
directory mask = 2770
force create mode = 0660
force directory mode = 2770
hide unreadable = yes
browseable = yes

[management]
comment = Общий ресурс руководства
path = /srv/smb/management
valid users = @grp_management
read only = no
writable = yes
create mask = 0660
directory mask = 2770
force create mode = 0660
force directory mode = 2770
hide unreadable = yes
browseable = yes

[common]
comment = Общий ресурс для всех подразделений
path = /srv/smb/common
valid users = @"Domain Users"
read only = no
writable = yes
create mask = 0664
directory mask = 2775
force create mode = 0664
force directory mode = 2775
hide unreadable = no
browseable = yes

[common-ro]
comment = Ресурс только для чтения
```

```
path = /srv/smb/common/read-only
valid users = @"Domain Users"
read only = yes
browseable = yes
```

Описание ключевых параметров секции ресурса:

– valid users – список пользователей и/или групп, которым разрешён доступ к ресурсу. Символ @ перед именем означает группу. При указании нескольких групп они перечисляются через запятую, например "@grp_accounting, @grp_management";

– read only – запрещает запись в ресурс при значении yes;

– writable – разрешает запись в ресурс при значении yes. Является обратной альтернативой параметру read only;

– create mask – определяет максимальные права, назначаемые создаваемым файлам;

– directory mask – определяет максимальные права, назначаемые создаваемым каталогам;

– force create mode – определяет права, которые будут принудительно установлены на создаваемых файлах независимо от запроса клиента;

– force directory mode – определяет права, которые будут принудительно установлены на создаваемых каталогах;

– hide unreadable – скрывает файлы и каталоги, недоступные для чтения текущему пользователю;

– browseable – определяет, отображается ли ресурс в списке общих ресурсов при просмотре сервера.

Примечание — Для ограничения доступа к ресурсу несколькими конкретными группами используется перечисление:

```
valid users = @grp_accounting, @grp_management
```

Для полного запрета доступа определённым пользователям или группам используется параметр invalid users:

```
invalid users = @grp_engineering
```

### 3.6.1.6 Проверка конфигурации и перезапуск служб

Для проверки корректности файла конфигурации нужно выполнить команду:

```
testparm -s
```

где: - -s – подавление интерактивного запроса подтверждения и вывод итогового конфигурационного файла без пауз. При наличии синтаксических ошибок в файле /etc/samba/smb.conf они будут отображены в выводе команды.

При отсутствии ошибок необходимо перезапустить службы Samba:

```
systemctl restart smb winbind
```

### 3.6.1.7 Проверка доступа

Для проверки доступности ресурсов нужно выполнить команду:

```
smbclient -kL //$(hostname)/
```

где:

– //$(hostname)/accounting – сетевой путь к проверяемому ресурсу на текущем сервере;

– -k – использование аутентификации Kerberos (требуется предварительно полученный билет Kerberos пользователя, чей доступ проверяется);

– -c "ls" – выполнение команды ls (вывод списка файлов) на удалённом ресурсе и завершение сеанса.

Далее проверить доступ конкретного доменного пользователя к определённому ресурсу, выполнив команду:

```
smbclient //$(hostname)/accounting -k -c "ls"
```

Затем следует проверить права конкретного пользователя на ресурс (эмуляция доступа), выполнив команду:

П р и м е ч а н и е — Перед выполнением необходимо получить билет пользователя Kerberos для пользователя admin, либо указать пароль через % (user%password).

```
smbcacls //$(hostname)/accounting "" -U admin
```

где:

– //$(hostname)/accounting – сетевой путь к ресурсу, права на который проверяются;

– "" – имя файла или каталога внутри ресурса, для которого выводятся ACL. Пустая строка означает корневой каталог ресурса;

– -U admin – имя пользователя для аутентификации. В реальной среде рекомендуется заменить на конкретную доменную учётную запись, права которой проверяются, либо использовать аутентификацию Kerberos через параметр -k вместо -U.

### 3.6.1.8 Подключение ресурсов на клиентских АРМ

На клиентских АРМ под управлением ОС Linux доменный пользователь может подключить ресурс командой:

```
mkdir -p /mnt/accounting
mount -t cifs //smb.rosa.dev/accounting /mnt/accounting -o
sec=krb5,uid=$(id -u),gid=$(id -g)
```

где:

– -t cifs – тип файловой системы удалённого ресурса (протокол SMB/CIFS);

– //smb.rosa.dev/accounting – сетевой путь к общему ресурсу на файловом сервере;

– /mnt/accounting – локальная точка монтирования, в которой содержимое ресурса будет доступно пользователю;

– sec=krb5 – использование аутентификации Kerberos для подключения к ресурсу;

– uid=$(id -u) – идентификатор локального пользователя, от имени которого будет выполняться доступ к файлам на смонтированном ресурсе;

– gid=$(id -g) – идентификатор локальной группы, от имени которой будет выполняться доступ к файлам на смонтированном ресурсе.

Для автоматического монтирования при входе пользователя рекомендуется настроить соответствующую политику через консоль dd-admin или добавить запись в /etc/fstab:

```
//smb.rosa.dev/accounting /mnt/accounting cifs
sec=krb5,user,uid=0,gid=0 0 0
```

где:

- //smb.rosa.dev/accounting – сетевой путь к общему ресурсу;
- /mnt/accounting – локальная точка монтирования;
- cifs – тип файловой системы;
- sec=krb5 – аутентификация Kerberos;
- user – разрешение на монтирование ресурса непривилегированным пользователем;
- uid=0, gid=0 – владелец и группа смонтированных файлов (в данном примере – root). Для реальной среды рекомендуется заменить на реальные UID и GID целевой группы пользователей либо убрать данные параметры и управлять доступом через POSIX-права на сервере;
- первые 0 – отключение резервного копирования утилитой dump;
- вторые 0 – отключение проверки файловой системы утилитой fsck при загрузке.

На клиентских АРМ под управлением ОС MS Windows ресурс подключается через проводник: "Сетевое окружение → переход по адресу <!-- Serif_-start -->\\smb.rosa.dev\accounting<!-- Serif_end -->" либо командой:

```
net use Z: \\smb.rosa.dev\accounting /persistent:yes
```

где:

- Z: – буква сетевого диска, которая будет назначена ресурсу в проводнике MS Windows. Допускается любая свободная буква латинского алфавита;
- \\smb.rosa.dev\accounting – сетевой путь к общему ресурсу на файловом сервере;
- /persistent:yes – сохранение подключения к ресурсу после перезагрузки компьютера. Для отключения автоматического подключения используется значение /persistent:no.

## 3.7 Подключение репозитория Dynamic Directory

Репозитории с клиентской частью размещены по следующим ссылкам в зависимости от типа ОС:

- Astra Linux 1.7.x – https://ddynamic.ru/dd/4.3/astra/
- ALT Linux P10 – https://ddynamic.ru/dd/4.3/alt/
- РОСА "ХРОМ" 12 – https://ddynamic.ru/dd/4.3/rosa/chrome/
- РОСА "ХРОМ" 13 – https://ddynamic.ru/dd/4.3/rosa/chrome_13/
- РОСА "КОБАЛЬТ" – https://ddynamic.ru/dd/4.3/rosa/res7/
- РЕД ОС 7 – https://ddynamic.ru/dd/4.3/redos/7/
- РЕД ОС 8 – https://ddynamic.ru/dd/4.3/redos/8/

Подключение репозитория Dynamic Directory для последующей установки пакета dd-client осуществляется следующими консольными командами в зависимости от типа ОС:

- для ОС Astra Linux 1.7.x выполнить последовательно три команды:

```
wget https://ddynamic.ru/dd/4.3/astra/pool/non-free/d/dd-releas⌋
e-4.3/dd-release-4.
3_1.0.0-1.astra_all.deb -O /tmp/dd-release-4.3.deb
apt-get install /tmp/dd-release-4.3.deb
apt-get update
```

- для ОС ALT Linux P10:

```
apt-get install https://ddynamic.ru/dd/4.3/alt/noarch/RPMS.clas⌋
sic/dd-release-4.3-1.0.
0-1.alt.noarch.rpm
```

- для ОС РОСА "ХРОМ" 12:

```
dnf install https://ddynamic.ru/dd/4.3/rosa/chrome/dd-release-4⌋
.3-1.0.0-1.chrome.
noarch.rpm
dnf makecache
```

- для ОС РОСА "ХРОМ" 13 (рисунок 16):

```
dnf install https://ddynamic.ru/dd/4.3/rosa/chrome_13/dd-releas⌋
e-4.3-1.0.0-1.
chrome13.noarch.rpm
dnf makecache
```

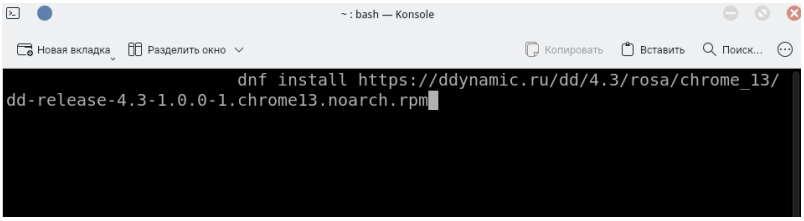


Рисунок 16 – Вид команды wget

- для РОСА "КОБАЛЬТ":

```
yum install https://ddynamic.ru/dd/4.3/rosa/res7/dd-release-4.3-
1.0.0-1.res7.
noarch.rpm
yum makecache
```

- для РЕД ОС 7:

```
dnf install https://ddynamic.ru/dd/4.3/redos/7/dd-release-4.3-1
.0.0-1.redos7.
noarch.rpm
dnf makecache
```

- для РЕД ОС 8:

```
dnf install https://ddynamic.ru/dd/4.3/redos/8/dd-release-4.3-1
.0.0-1.redos8.
noarch.rpm
dnf makecache
```

### 3.8 Установка консоли администратора Dynamic Directory

Для доступа к графическому интерфейсу Dynamic Directory необходимо установить консоль администратора Dynamic Directory в зависимости от используемой ОС:

- для Astra Linux выполнить установку из подключенного репозитория:

```
$ sudo apt install dd-admin
```

- для РЕД ОС и РОСА выполнить установку из подключенного репозитория:

```
$ sudo dnf install dd-admin
```

## 3.9 Настройка управляемых АРМ

Для функционирования управляемых АРМ в дистрибутиве ОС должен быть сконфигурирован клиент службы каталогов Dynamic Directory (dd-client).

Настройка управляемых АРМ производится в зависимости от используемой ОС.

По результатам настройки клиентские ПК должны быть установлены и настроены следующим образом:

а) АРМ введён в домен под управлением службы каталогов Dynamic Directory, настроенной согласно п. 3.2 настоящего Руководства;

б) АРМ управляется сервером Puppet, настроенным согласно п. 3.3 настоящего Руководства.

### 3.9.1 Обновление пакетов

Для обновления пакетной базы после подключения репозитория Dynamic Directory и обновления кэша метаданных нужно выполнить команду:

```
dnf -y update
```

### 3.9.2 Настройка управляемых АРМ с использованием клиента (ОС Linux)

Для настройки управляемого АРМ необходимо произвести установку пакета dd-client для соответствующей ОС и выполнить скрипт конфигурации dd-client-install.

**Следует обратить внимание**, что перед настройкой управляемых АРМ на ОС Astra Linux необходимо включить сетевой репозиторий и отключить DVD-репозиторий.

Установка пакета dd-client из подключенного репозитория для ОС Astra Linux выполняется командой:

```
sudo apt install dd-client
```

Установка пакета dd-client из подключенного репозитория для РЕД ОС, РОСА "Хром" и ROSA Fresh выполняется командой:

```
sudo dnf install dd-client
```

Для установки и конфигурирования клиента необходимо выполнить команду dd-client-install от имени привилегированного пользователя:

```
dd-client-install
```

Далее нужно следовать инструкциям установщика, вводя данные на запросы или нажимая клавишу `Enter` по умолчанию:

```
Введите имя домена:rosa.dev
Подготовка АРМ к вводу в домен rosa.dev
Введите имя АРМ в формате FQDN (dev-main.rosa.dev):
Введите имя пользователя с правами на ввод АРМ в домен (admin):
Введите пароль (не менее 8 символов):
Введите пароль (не менее 8 символов) ещё раз:
ПАРАМЕТРЫ ПОДКЮЧЕНИЯ К ДОМЕНУ:
ИМЯ ДОМЕНА: rosa.dev
ИМЯ АРМ: dev-main.rosa.dev
Пользователь для ввода в домен: admin
Подтвердить заданные опции и выполнить ввод в домен? [y/n]: y
y
This program will set up FreeIPA client.
Version 4.8.10
Discovery was successful!
Client hostname: dev-main.rosa.dev
Realm: ROSA.DEV
DNS Domain: rosa.dev
IPA Server: dc1-main.rosa.dev
BaseDN: dc=rosa,dc=dev
Synchronizing time
```

```
No SRV records of NTP servers found and no NTP server or pool
address was provided.
Using default chrony configuration.
Attempting to sync time with chronyc.
Time synchronization was successful.
Successfully retrieved CA cert
Subject: CN=Certificate Authority,O=ALL-DEMO.ROSA
Issuer: CN=Certificate Authority,O=ALL-DEMO.ROSA
Valid From: 2024-04-22 21:15:24
Valid Until: 2044-04-22 21:15:24
Enrolled in IPA realm ALL-DEMO.ROSA
Created /etc/ipa/default.conf
Configured sudoers in /etc/authselect/user-nsswitch.conf
Configured /etc/sssd/sssd.conf
Configured /etc/krb5.conf for IPA realm ALL-DEMO.ROSA
Systemwide CA database updated.
Extra A/AAAA record(s) for host dev-main.rosa.dev:
fe80::b85d:f070:a27c:b6cb.
Incorrect reverse record(s):
10.125.22.200 is pointing to dev-main. instead of
dev-main.rosa.dev.
10.125.22.200 is pointing to dev-main.local. instead of
dev-main.rosa.dev.
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config.d/04-ipa.conf
Configuring rosa.dev as NIS domain.
Client configuration complete.
The ipa-client-install command was successful
```

На этом ввод клиента в домен завершен.

При настроенном сервере РОСА Центр управления или Puppet/Saltstack можно также выполнить подключение АРМ к серверу управления, для чего

необходимо подтвердить подключение к серверу управления, введя "y" и следуя дальнейшим инструкциям:

Примечание — При настройке так же будет загружен клиент Puppet или Saltstack (должны быть доступны соответствующие репозитории ОС).

```
Вы хотите настроить подключение к серверу управления сейчас
[y/n]: y
y
Введите тип сервера управления puppet|saltstack: puppet
Введите fqdn сервера управления puppet: cc.rosa.dev
read_config_server
Connection to cc.rosa.dev (10.125.22.12) 8140 port [tcp/puppet]
succeeded!
APM будет настроен на использование сервера конфигурации
puppet: cc.rosa.dev
ROSA 2021.1 - x86_64 - Contrib 69 kB/s | 3.4 kB 00:00
ROSA 2021.1 - x86_64 - Main 68 kB/s | 3.4 kB 00:00
ROSA 2021.1 - x86_64 - Non-free 68 kB/s | 3.3 kB 00:00
ROSA 2021.1 - i686 - Contrib 70 kB/s | 3.4 kB 00:00
ROSA 2021.1 - i686 - Main 68 kB/s | 3.4 kB 00:00
ROSA 2021.1 - i686 - Non-free 67 kB/s | 3.3 kB 00:00
Создан кэш метаданных.
Зависимости разрешены.
================================================================⌋
================================================
Пакет Архитектура Версия Репозиторий Размер
================================================================⌋
================================================
Установка:
puppet noarch 7.25.0-1 mirror-rosa-x86_64-main 1.3 M
Установка зависимостей:
facter noarch 4.4.0-1 mirror-rosa-x86_64-main 279 k
hiera noarch 3.6.0-3 mirror-rosa-x86_64-main 31 k
lib64ruby2.7 x86_64 2.7.8-9 mirror-rosa-x86_64-main 2.8 M
ruby x86_64 2.7.8-9 mirror-rosa-x86_64-main 35 k
rubygem-concurrent-ruby noarch 1.1.5-3 mirror-rosa-x86_64-main
242 k
rubygem-deep_merge noarch 1.2.1-6 mirror-rosa-x86_64-main 12 k
```

```
rubygem-hocon noarch 1.3.1-1 mirror-rosa-x86_64-main 88 k
rubygem-irb noarch 1.2.6-9 mirror-rosa-x86_64-main 63 k
rubygem-json x86_64 2.6.3-1 mirror-rosa-x86_64-contrib 177 k
rubygem-openssl x86_64 2.1.4-9 mirror-rosa-x86_64-main 140 k
rubygem-psych x86_64 3.1.0-9 mirror-rosa-x86_64-main 44 k
rubygem-semantic_puppet noarch 1.0.2-1 mirror-rosa-x86_64-main
20 k
rubygem-thor noarch 1.0.1-1 mirror-rosa-x86_64-main 58 k
rubygems noarch 3.1.6-9 mirror-rosa-x86_64-main 234 k
Установка слабых зависимостей:
ruby-default-gems noarch 2.7.8-9 mirror-rosa-x86_64-main 23 k
rubygem-bigdecimal x86_64 2.0.0-9 mirror-rosa-x86_64-main 47 k
rubygem-bundler noarch 2.3.26-1 mirror-rosa-x86_64-main 380 k
rubygem-io-console x86_64 0.5.6-9 mirror-rosa-x86_64-main 20 k
rubygem-rdoc noarch 6.2.1.1-9 mirror-rosa-x86_64-main 374 k
Результат транзакции
================================================================
================================================
Установка 20 Пакетов
Объем загрузки: 6.4 M
Объем изменений: 26 M
Загрузка пакетов:
(1/20): hiera-3.6.0-3-rosa2021.1.noarch.rpm 245 kB/s | 31 kB
00:00
(2/20): rubygem-json-2.6.3-1-rosa2021.1.x86_64.rpm 720 kB/s |
177 kB 00:00
(3/20): facter-4.4.0-1-rosa2021.1.noarch.rpm 805 kB/s | 279 kB
00:00
(4/20): ruby-2.7.8-9-rosa2021.1.x86_64.rpm 1.3 MB/s | 35 kB
00:00
(5/20): ruby-default-gems-2.7.8-9-rosa2021.1.noarch.rpm 874
kB/s | 23 kB 00:00
(6/20): rubygem-bigdecimal-2.0.0-9-rosa2021.1.x86_64.rpm 1.8
MB/s | 47 kB 00:00
(7/20): rubygem-bundler-2.3.26-1-rosa2021.1.noarch.rpm 2.7 MB/s
| 380 kB 00:00
(8/20): puppet-7.25.0-1-rosa2021.1.noarch.rpm 3.4 MB/s | 1.3 MB
00:00
```

```
(9/20): rubygem-concurrent-ruby-1.1.5-3-rosa2021.1.noarch.rpm
2.8 MB/s | 242 kB 00:00
(10/20): rubygem-deep_merge-1.2.1-6-rosa2021.1.noarch.rpm 494
kB/s | 12 kB 00:00
(11/20): rubygem-hocon-1.3.1-1-rosa2021.1.noarch.rpm 2.9 MB/s |
88 kB 00:00
(12/20): rubygem-io-console-0.5.6-9-rosa2021.1.x86_64.rpm 755
kB/s | 20 kB 00:00
(13/20): rubygem-irb-1.2.6-9-rosa2021.1.noarch.rpm 2.3 MB/s |
63 kB 00:00
(14/20): rubygem-openssl-2.1.4-9-rosa2021.1.x86_64.rpm 5.1 MB/s
| 140 kB 00:00
(15/20): rubygem-psych-3.1.0-9-rosa2021.1.x86_64.rpm 1.6 MB/s |
44 kB 00:00
(16/20): rubygem-semantic_puppet-1.0.2-1-rosa2021.1.noarch.rpm
767 kB/s | 20 kB 00:00
(17/20): rubygem-thor-1.0.1-1-rosa2021.1.noarch.rpm 2.1 MB/s |
58 kB 00:00
(18/20): rubygem-rdoc-6.2.1.1-9-rosa2021.1.noarch.rpm 4.8 MB/s
| 374 kB 00:00
(19/20): rubygems-3.1.6-9-rosa2021.1.noarch.rpm 2.7 MB/s | 234
kB 00:00
(20/20): lib64ruby2.7-2.7.8-9-rosa2021.1.x86_64.rpm 3.4 MB/s |
2.8 MB 00:00
--------------------------------------------------------------
----------------------------------------------
Общий размер 6.7 MB/s | 6.4 MB 00:00
Проверка транзакции
Проверка транзакции успешно завершена.
Идет проверка транзакции
Тест транзакции проведен успешно.
Выполнение транзакции
Подготовка : 1/1
Установка : lib64ruby2.7-2.7.8-9.x86_64 1/20
Установка : ruby-default-gems-2.7.8-9.noarch 2/20
Установка : rubygem-bigdecimal-2.0.0-9.x86_64 3/20
Установка : rubygem-io-console-0.5.6-9.x86_64 4/20
Установка : rubygem-bundler-2.3.26-1.noarch 5/20
```

```
Установка : rubygem-irb-1.2.6-9.noarch 6/20
Установка : ruby-2.7.8-9.x86_64 7/20
Установка : rubygem-openssl-2.1.4-9.x86_64 8/20
Установка : rubygem-psych-3.1.0-9.x86_64 9/20
Установка : rubygems-3.1.6-9.noarch 10/20
Установка : rubygem-json-2.6.3-1.x86_64 11/20
Установка : rubygem-rdoc-6.2.1.1-9.noarch 12/20
Установка : rubygem-concurrent-ruby-1.1.5-3.noarch 13/20
Установка : rubygem-deep_merge-1.2.1-6.noarch 14/20
Установка : rubygem-hocon-1.3.1-1.noarch 15/20
Установка : rubygem-semantic_puppet-1.0.2-1.noarch 16/20
Установка : rubygem-thor-1.0.1-1.noarch 17/20
Установка : facter-4.4.0-1.noarch 18/20
Установка : hiera-3.6.0-3.noarch 19/20
Запуск скриптлета: puppet-7.25.0-1.noarch 20/20
Установка : puppet-7.25.0-1.noarch 20/20
Запуск скриптлета: puppet-7.25.0-1.noarch 20/20
Failed to open 'puppet': No such file or directory
Cannot set file attributes for '/var/log/journal', maybe due to
incompatibility in specified attributes, previous=0x00080000,
current=
0x00080000, expected=0x00880000, ignoring.
Cannot set file attributes for
'/var/log/journal/6570b00422d3482496625e15ba107cf2', maybe due
to incompatibility in
specified attributes, previous=0x00080000, current=0x00080000,
expected=0x00880000, ignoring.
Проверка : rubygem-json-2.6.3-1.x86_64 1/20
Проверка : facter-4.4.0-1.noarch 2/20
Проверка : hiera-3.6.0-3.noarch 3/20
Проверка : lib64ruby2.7-2.7.8-9.x86_64 4/20
Проверка : puppet-7.25.0-1.noarch 5/20
Проверка : ruby-2.7.8-9.x86_64 6/20
Проверка : ruby-default-gems-2.7.8-9.noarch 7/20
Проверка : rubygem-bigdecimal-2.0.0-9.x86_64 8/20
Проверка : rubygem-bundler-2.3.26-1.noarch 9/20
Проверка : rubygem-concurrent-ruby-1.1.5-3.noarch 10/20
Проверка : rubygem-deep_merge-1.2.1-6.noarch 11/20
```

```
Проверка : rubygem-hocon-1.3.1-1.noarch 12/20
Проверка : rubygem-io-console-0.5.6-9.x86_64 13/20
Проверка : rubygem-irb-1.2.6-9.noarch 14/20
Проверка : rubygem-openssl-2.1.4-9.x86_64 15/20
Проверка : rubygem-psych-3.1.0-9.x86_64 16/20
Проверка : rubygem-rdoc-6.2.1.1-9.noarch 17/20
Проверка : rubygem-semantic_puppet-1.0.2-1.noarch 18/20
Проверка : rubygem-thor-1.0.1-1.noarch 19/20
Проверка : rubygems-3.1.6-9.noarch 20/20
Установлен:
facter-4.4.0-1.noarch hiera-3.6.0-3.noarch
lib64ruby2.7-2.7.8-9.x86_64
puppet-7.25.0-1.noarch ruby-2.7.8-9.x86_64
ruby-default-gems-2.7.8-9.noarch
rubygem-bigdecimal-2.0.0-9.x86_64
rubygem-bundler-2.3.26-1.noarch
rubygem-concurrent-ruby-1.1.5-3.noarch
rubygem-deep_merge-1.2.1-6.noarch rubygem-hocon-1.3.1-1.noarch
rubygem-io-console-0.5.6-9.x86_64
rubygem-irb-1.2.6-9.noarch rubygem-json-2.6.3-1.x86_64
rubygem-openssl-2.1.4-9.x86_64
rubygem-psych-3.1.0-9.x86_64 rubygem-rdoc-6.2.1.1-9.noarch
rubygem-semantic_puppet-1.0.2-1.noarch
rubygem-thor-1.0.1-1.noarch rubygems-3.1.6-9.noarch
Выполнено!
```

На этом подключение к серверу управления завершено.

### 3.9.3 Настройка управляемых АРМ с использованием клиента (ОС MS Windows)

**Следует обратить внимание**, что работоспособность клиента Dynamic Directory для MS Windows была протестирована на совместимость с ОС MS Windows 10 и Windows 11.

Возможности клиента Dynamic Directory для MS Windows:

– Подключение АРМ с совместимыми операционными системами к сфере Kerberos домена Dynamic Directory.

– Создание учётной записи компьютера в домене.

– Аутентификация пользователей на АРМ с использованием учётных записей домена Dynamic Directory через протокол Kerberos.

### 3.9.3.1 Установка приложения DD-client

Для ввода в домен Dynamic Directory ПК под управлением ОС MS Windows 10 и Windows 11 необходимо следующее:

а) Скачать и установить приложение DD-client (https://ddynamic.ru/dd/4.2/win/DD-client.exe);

Примечание — Для установки приложения необходимы права администратора компьютера.

б) После запуска установки нажать кнопку `Да` во всплывающем окне (рисунок 17);

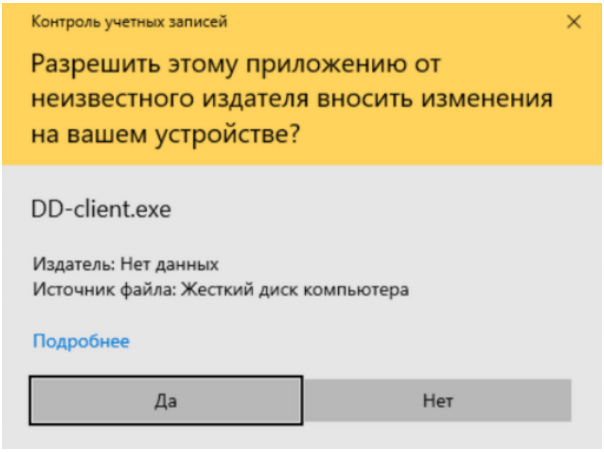


Рисунок 17 – Всплывающее окно с разрешением DD-client вносить изменения в системе

в) Поставить флажки "Установить .NET Runtime" и "Отключить NetBIOS", нажать кнопку `Далее` (рисунок 18);

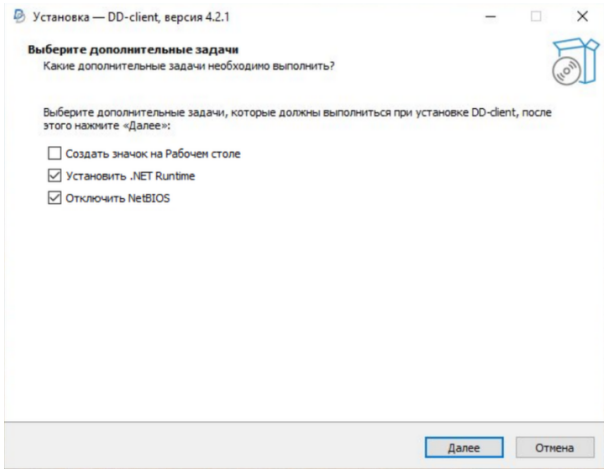


Рисунок 18 – Параметр ".NET Runtime" в окне мастера установки

Примечания:

– Отключение NetBIOS ускоряет вход (аутентификацию) доменных пользователей Dynamic Directory на рабочих станциях с ОС Windows.

– Отключение NetBIOS в рамках работы на автоматизированном рабочем месте (АРМ) под управлением Windows 10 или Windows 11 может повлиять на несколько аспектов сетевого взаимодействия, особенно в устаревших или гибридных ИТ-средах. Однако в современных сетях, построенных на основе DNS и протоколов, не зависящих от NetBIOS, это отключение часто безопасно и даже рекомендуется с точки зрения безопасности.

– В случае необходимости, NetBIOS можно снова включить в свойствах сетевого подключения (Свойства протокола IPv4 – Дополнительно – Вкладка WINS – Параметр NetBIOS "По умолчанию").

г) На этапе готовности к установке нажать кнопку Установить (рисунок 19);

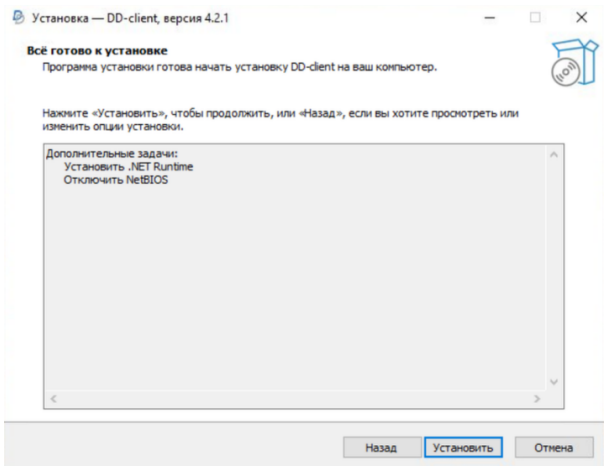


Рисунок 19 – Этап готовности к установке

д) В окне установки компонента ".NET Runtime" нажать кнопку Установить (рисунок 20);

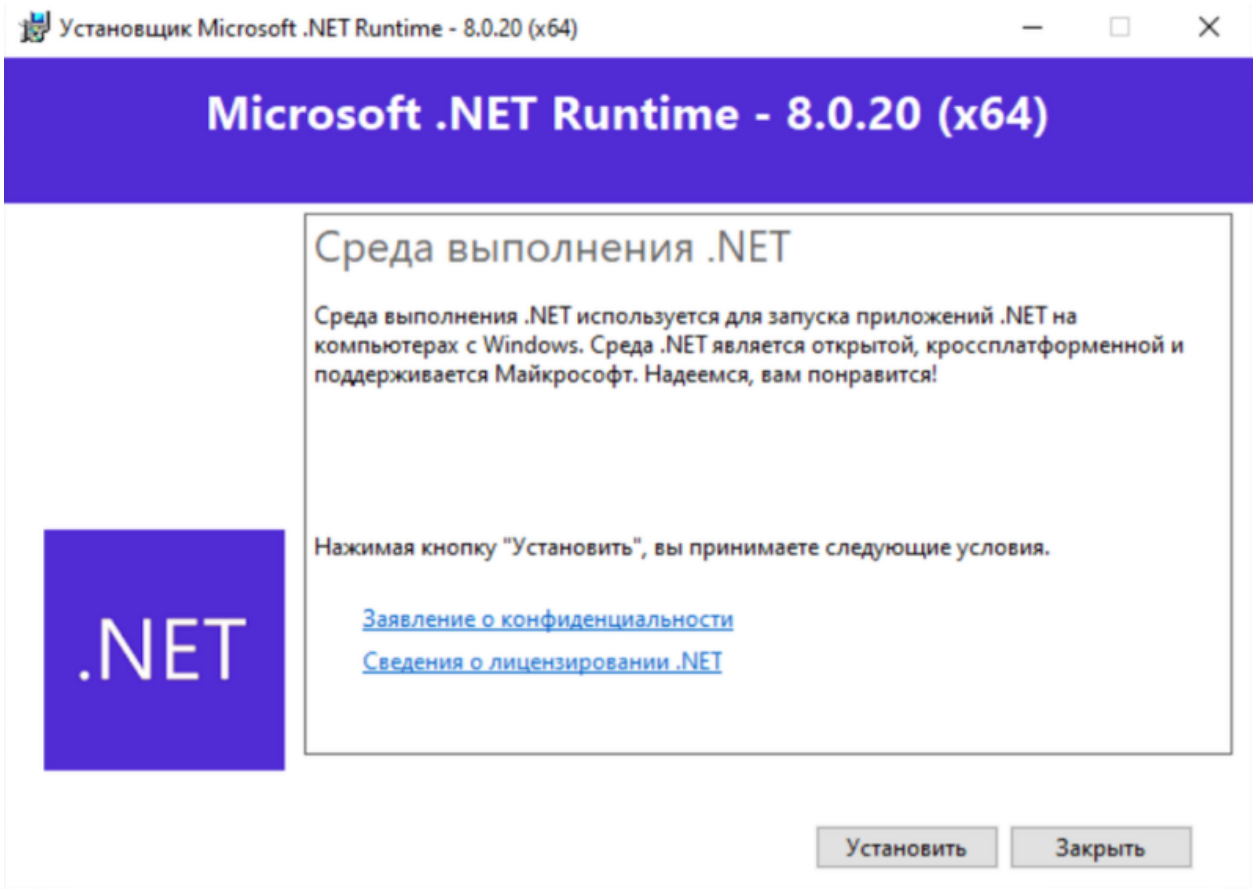


Рисунок 20 – Окно установки Microsoft .NET Runtime 8.0.20 (x64)

е) После завершения установки нажать кнопку Закрыть (рисунок 21).

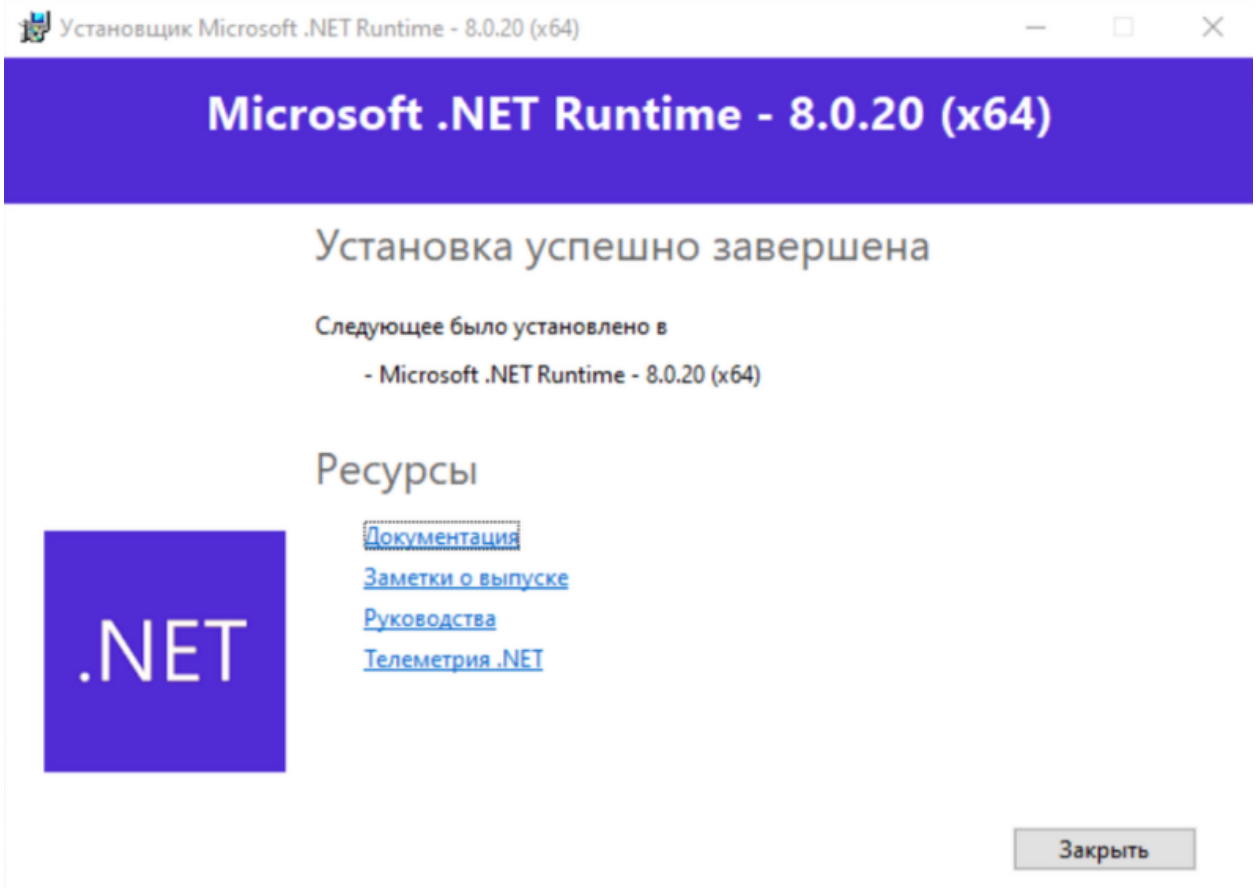


Рисунок 21 – Окно успешного завершения установки .NET Runtime

ж) Если на завершающем этапе мастера не будет снят флажок "Запустить DD-client" (рисунок 22), после нажатия кнопки Завершить откроется окно командной строки в каталоге, содержащем утилиту dd_enroll_host.

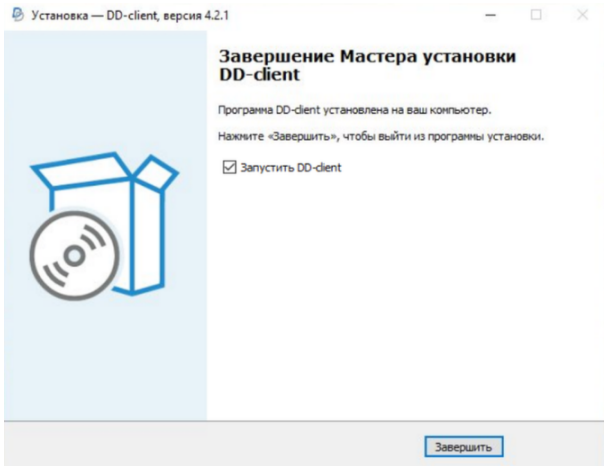


Рисунок 22 – Окно завершения мастера установки DD-client с флажком "Запустить DD-client"

### 3.9.3.2 Ввод в домен

Утилита dd_enroll_host выполняет подключение АРМ к домену Dynamic Directory и может быть запущена со следующими параметрами:

– -s, --server – полное доменное имя контроллера службы каталогов Dynamic Directory;

– -u, --username – имя пользователя, с правами ввода компьютеров в домен;

– -p, --password – пароль пользователя.

Пример команды для подключения к домену:

```
dd_enroll_host -s <FQDN_DC_Server> -u <admin_domain> -p
<user_password>
```

Пример успешного выполнения команды представлен на рисунке 23.

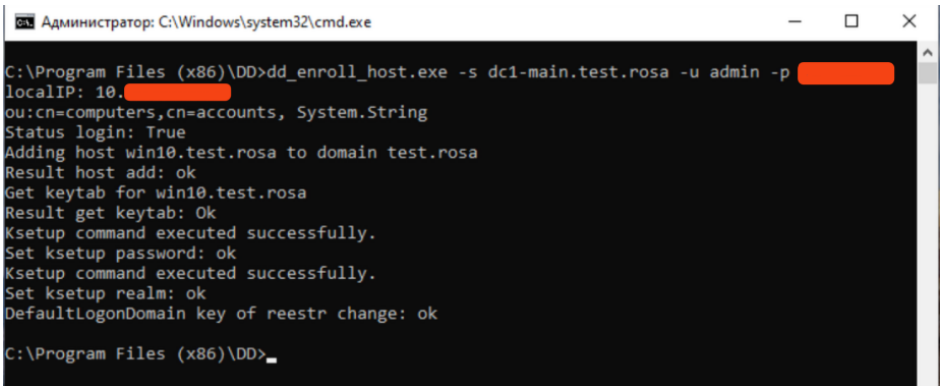


Рисунок 23 – Результат выполнения команды подключения к домену

После ввода в домен Dynamic Directory необходимо перезагрузить компьютер и авторизоваться с учётными данными доменного пользователя (рисунок 24).

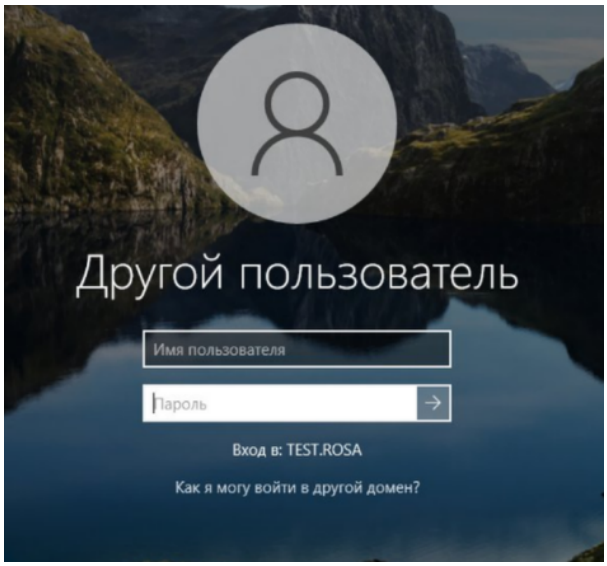


Рисунок 24 – Экран авторизации доменного пользователя

### 3.9.3.3 Вывод из домена

Для вывода из домена Dynamic Directory АРМ с ОС Windows 10 или 11 нужно выполнить следующие действия:

а) Войти под локальным администратором на АРМ.

б) Открыть свойства компьютера, выбрать "Дополнительные параметры системы".

в) Открыть вкладку "Имя компьютера" и нажать на кнопку Изменить (рисунок 25).

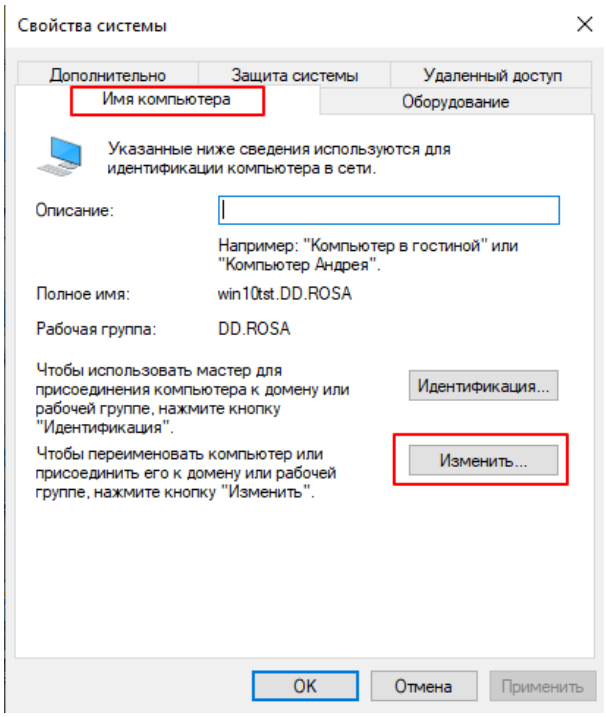


Рисунок 25 – Вкладка "Имя компьютера"

г) Изменить рабочую группу на "WORKGROUP" и нажать OK (рисунок 26).

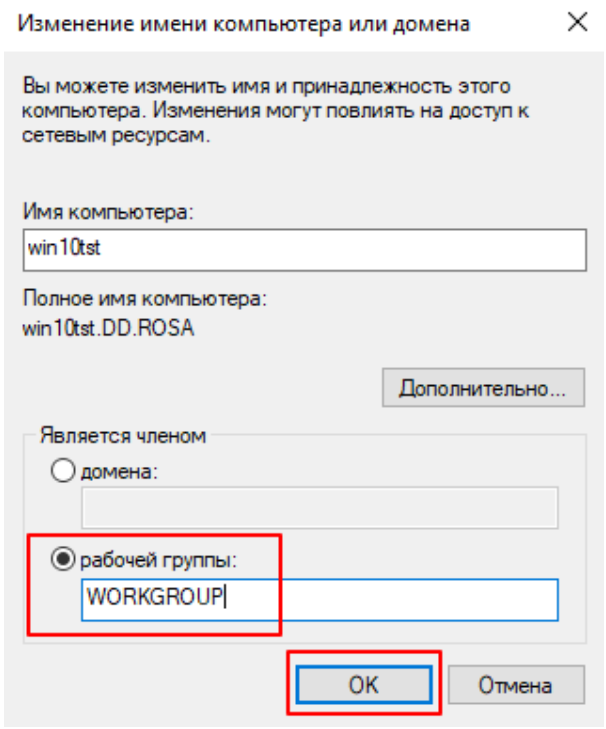


Рисунок 26 – Окно "Изменение имени компьютера или домена"

д) После приветствия "Добро пожаловать в рабочую группу WORKGROUP." нажать OK и перезагрузить компьютер (рисунок 27).

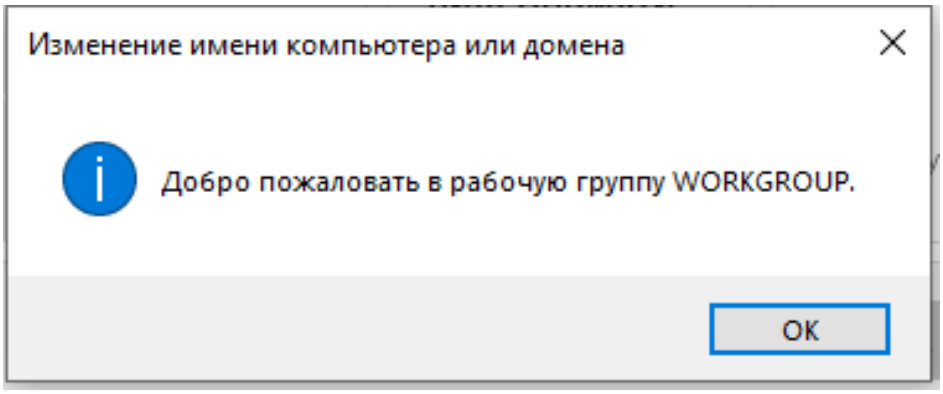


Рисунок 27 – Уведомление об изменении рабочей группы

е) Также требуется удалить АРМ с контроллера домена Dynamic Directory. Для этого нужно зайти на компьютер admpc и запустить графическую утилиту dd-admin. Выбрать в системной папке "Компьютеры" (или в том OU, в котором он находился) выведенный АРМ, вызвать контекстное меню и выбрать "Удалить".

Записи DNS, относящиеся к данному АРМ, будут удалены автоматически. Удаление АРМ с ОС Windows, выведенного из домена Dynamic Directory, успешно завершено.

**Следует обратить внимание**, что после вывода АРМ из домена необходимо удалить на нём приложение dd-client, если не планируется его дальнейшее использование, так как будет продолжен сбор и накопление журналов работы, а также запуск задач при старте системы.

### 3.9.4 Настройка управляемых АРМ вручную для Astra Linux

Для установки агента нужно выполнить на клиентском ПК следующие команды (при этом будет установлен агент и сервер SSH для удалённого управления агентом):

```
sudo apt update
sudo apt install puppet-agent astra-freeipa-client
```

Далее следует задать имя АРМ в формате FQDN:

```
hostnamectl set-hostname ${hostname}.${domain.name}
```

где:
- ${hostname} – имя АРМ в нижнем регистре;
- ${domain.name} – имя домена в нижнем регистре.

Затем необходимо ввести АРМ в домен, выполнив команду:

```
astra-freeipa-client -d ${domain.name} -p ${password}
```

где:
- ${domain.name} – имя домена в нижнем регистре;
- ${password} – пароль пользователя admin.

Если необходимо выполнить ввод в домен от имени другого пользователя, имеющего на это права, можно задать имя пользователя, используя опцию "-u ${username}" (более подробную информацию можно получить из вывода на экран команды "astra-freeipa-client -h").

После ввода в домен следует отредактировать файл /etc/sssd/sssd.conf, добавив в секцию "[domain/${domain.name}" строки:

```
ldap_search_base =
cn=accounts,${base_dn}???cn=ou,cn=dynamicdirectory, ${base_dn}??
ldap_user_search_base = cn=users,cn=accounts,${base_dn}cn=ou,cn
=dynamicdirectory,${base_dn}??
ldap_group_search_base = cn=groups,cn=accounts,${base_dn}???cn=
ou,cn=dynamicdirectory,${base_dn}??
```

Значение ${base_dn} можно посмотреть в файле /etc/ipa/default.conf:

```
cat /etc/ipa/default.conf
```

Отредактировать файл /etc/sssd/sssd.conf можно, используя редактор nano:

```
nano /etc/sssd/sssd.conf
```

Например, для [domain/rosa.dev] добавляемые строки будут выглядеть так:

```
ldap_search_base = cn=accounts,dc=rosa,dc=dev???cn=ou,cn=dynami
cdirectory,dc=rosa,dc=dev??
ldap_user_search_base = cn=users,cn=accounts,dc=rosa,dc=dev???c
n=ou,cn=dynamicdirectory,dc=rosa,dc=dev??
ldap_group_search_base = cn=groups,cn=accounts,dc=rosa,dc=dev??
?cn=ou,cn=dynamicdirectory,dc=rosa,dc=dev??
```

После изменения конфигурационного файла /etc/sssd/sssd.conf необходимо перезапустить сервис SSSD, выполнив команду:

```
systemctl restart sssd.service
```

Далее необходимо отредактировать файл /etc/puppetlabs/puppet/puppet.conf, добавив параметры:

```
[agent]
ca_server = config.rosa.dev
server = config.rosa.dev
certname = user01.rosa.dev
runinterval = 90m
```

Для соединения агент использует IP-порт 8140. Если включен межсетевой экран, то нужно разрешить коммуникации через этот порт, выполнив для сетевого экрана ufw-команду:

```
sudo ufw allow 8140
```

Затем необходимо добавить службу Puppet Agent в автозагрузку и запустить её командами:

```
sudo systemctl enable puppet
sudo systemctl start puppet
```

### 3.9.5 Настройка управляемых АРМ вручную для РЕД ОС и РОСА

Для установки агента надо выполнить на клиентском ПК следующие команды (при этом будет установлен агент и сервер SSH для удалённого управления агентом):

```
dnf update
dnf install puppet-agent ipa-client
```

Далее следует задать имя АРМ в формате FQDN:

```
hostnamectl set-hostname ${hostname}.${domain.name}
```

где:

- ${hostname} – имя АРМ в нижнем регистре;
- ${domain.name} – имя домена в нижнем регистре.

Затем нужно скорректировать файл constant.py командой:

```
sed -i 's|_a-z0-9|_a-z0-9\\-|'
/usr/lib/python3.8/site-packages/ipalib/constants.py
```

После этого необходимо ввести АРМ в домен, выполнив команду:

```
ipa-client-install --hostname=`hostname -f` --domain=`hostname
-d` --realm=`hostname -d | tr 'a-z' 'A-Z'`
--server=ds01.rosa.dev --ntp-
server=ds01.rosa.dev --mkhomedir -p admin -w password
--force-ntpd
```

После ввода в домен следует отредактировать файл /etc/sssd/sssd.conf, добавив в секцию [domain/${domain.name} строки:

```
ldap_search_base =
cn=accounts,${base_dn}???cn=ou,cn=dynamicdirectory, ${base_dn}??
ldap_user_search_base =
cn=users,cn=accounts,${base_dn}???cn=ou,cn=dynamicdirectory,
${base_dn}??
ldap_group_search_base =
cn=groups,cn=accounts,${base_dn}???cn=ou,cn=dynamicdirectory,
${base_dn}??
```

Значение ${base_dn} можно посмотреть в файле /etc/ipa/default.conf:

```
cat /etc/ipa/default.conf
```

Отредактировать файл /etc/sssd/sssd.conf можно, используя редактор nano:

```
nano /etc/sssd/sssd.conf
```

Например, для [domain/rosa.dev] добавляемые строки будут выглядеть так:

```
ldap_search_base = cn=accounts,dc=rosa,dc=dev???cn=ou,cn=dynami⌋
cdirectory,dc=rosa,dc=dev??
ldap_user_search_base = cn=users,cn=accounts,dc=rosa,dc=dev???c⌋
n=ou,cn=dynamicdirectory,dc=rosa,dc=dev??
ldap_group_search_base = cn=groups,cn=accounts,dc=rosa,dc=dev??⌋
?cn=ou,cn=dynamicdirectory,dc=rosa,dc=dev??
```

После изменения конфигурационного файла /etc/sssd/sssd.conf необходимо перезапустить сервис SSSD, выполнив команду:

```
systemctl restart sssd.service
```

Далее необходимо отредактировать файл /etc/puppetlabs/puppet/puppet.conf, добавив параметры:

```
[agent]
ca_server = config.rosa.dev
server = config.rosa.dev
certname = user01.rosa.dev
runinterval = 90m
```

Для соединения агент использует IP-порт 8140. Если включен межсетевой экран, то надо разрешить коммуникации через этот порт, выполнив для сетевого экрана ufw-команду:

```
ufw allow 8140
```

Затем необходимо добавить службу Puppet Agent в автозагрузку и запустить её командой:

```
systemctl enable puppet --now
```

Перезагрузить ПК командой:

```
reboot
```

### 3.10 Установка лицензионного ключа

Установка лицензионного ключа в Систему лицензирует консоль администратора Dynamic Directory.

**Следует обратить внимание**, что файл ключа устанавливается на все АРМ с установленной графической консолью администрирования.

Для установки необходимо:

а) поместить в каталог /usr/share/dd/ файл dd.key (если имя файла отличается от dd.key, то необходимо переименовать файл в dd.key);

б) проверить права на файл, используя команду:

```
ls -la /usr/share/dd/dd.key
```

в) если права отличаются от "-rw-r--r--", выполнить команду:

```
chmod 644 /usr/share/dd/dd.key
```

г) проверить права на файл, используя команду:

```
ls -la /usr/share/dd/dd.key
```

Если права по-прежнему отличаются от "-rw-r--r--" следует обратиться в службу технической поддержки.

### 3.11 Установка антивирусного ПО

Установка антивирусного программного обеспечения Антивирус Касперского проводится следующим образом:

- скачать пакет и записать его в каталог /tmp;
- установить пакет, выполнив команду:

```
dnf -y install /tmp/kesl-XX.X.X-YYYY.x86_64.rpm
```

- запустить скрипт для конфигурирования приложения командой:

```
/opt/kaspersky/kesl/bin/kesl-setup.pl
```

- произвести настройку приложения в соответствии с текущей инфраструктурой.

# ТЕРМИНЫ И СОКРАЩЕНИЯ

| Термин/Сокращение | Определение |
|---|---|
| АРМ | Автоматизированное рабочее место |
| Dynamic Directory | Система управления службой каталогов |
| Веб-сервис | (Web service) Идентифицируемая уникальным веб-адресом (URL-адресом) программная система со стандартизированными интерфейсами |
| НСД | Несанкционированный доступ к информации |
| ОП | Организационные подразделение |
| ОС | Операционная система |
| ПО | Программное обеспечение |
| ПК | Персональный компьютер |
| СК | Служба каталогов |
| СПД | Сеть передачи данных |
| УЗП | Учетная запись пользователя |
| ЦОД | Центр обработки данных |
| AD | (Active Directory) Служба каталогов корпорации Microsoft для операционных систем семейства Windows Server |
| SSSD | (System Security Services Daemon) Пакет приложений для управления аутентификацией и авторизацией в ОС на базе Linux |