RuDesktop

Документация

Быстрый старт

RuDesktop

Версия 3.1 • сформировано 21.11.2026

Оглавление

1 Описание **4**

2 Карта сценария **5**

3 Шаг 1. Подготовка перед установкой **7**
3.1 Системные требования 7
3.2 Сетевые требования 8
3.3 Подготовка ОС 8
3.4 Выбор сценария установки 9

4 Шаг 2. Установка сервера **10**
4.1 Установка DEB-пакета 10
4.2 Установка RPM-пакета 10
4.3 Проверка установки 11

5 Шаг 3. Создание суперпользователя и первый вход **12**
5.1 Создание суперпользователя 12
5.2 Первый вход в веб-интерфейс 12

6 Шаг 4. Активация лицензии **14**
6.1 Получение ключа 14
6.2 Активация 14

7 Шаг 5. Сетевая настройка **16**
7.1 Замена SSL-сертификата 16
7.2 Изменение IP-адреса сервера 17
7.3 Изменение стандартного порта 17
7.4 Ограничение доступа к веб-интерфейсу 18
7.5 Разделение портов веб и клиентов 18
7.6 Дополнительные сетевые настройки 18

8 Шаг 6. Базовые настройки сервера **19**

8.1 Настройка SMTP . . . 19
8.2 Двухфакторная аутентификация . . . 20
8.3 Защита от подбора пароля . . . 20
8.4 Группы по умолчанию . . . 21
8.5 Длительность сессии и саморегистрация . . . 21
8.6 Настройки мостов . . . 21
8.7 Логирование и Syslog . . . 22
8.8 Прочие блоки . . . 22

9 Шаг 7. Подключение источников пользователей 23
9.1 Создание групп и распределение прав . . . 23
9.2 Локальные пользователи . . . 24
9.3 Подключение Active Directory / LDAP . . . 24
9.4 Подключение Keycloak (SSO) . . . 25
9.5 Подразделения . . . 25

10 Шаг 8. Распределение доступов (ACL) 26

11 Шаг 9. Безопасность подключений 28
11.1 Корневые сертификаты для проверки клиентов . . . 28
11.2 Чёрный список . . . 28
11.3 Белый список . . . 29
11.4 Подсети и геолокация . . . 29
11.5 SSH-доступы . . . 30

12 Шаг 10. Дополнительные компоненты 31
12.1 Мосты для удалённых филиалов . . . 31
12.2 Точки распространения . . . 32
12.3 PXE-сервер для удалённой установки ОС . . . 32
12.4 Модуль аналитики (Apache Superset) . . . 32
12.5 Интеграции с внешними системами . . . 33
12.6 Публикация событий в Syslog . . . 33
12.7 Уведомления пользователям . . . 33
12.8 Kickstart-преднастройка клиента . . . 34

13 Шаг 11. Резервное копирование и эксплуатация 35
13.1 Резервное копирование БД . . . 35
13.2 Логи сервера . . . 36
13.3 Очередь задач . . . 36
13.4 Отказоустойчивый кластер . . . 37

14 Шаг 12. Распространение клиента 38
14.1 Через сканирование сети . . . 38
14.2 Через Kaspersky Security Center или Active Directory . . . 38
14.3 Ручная установка . . . 39
14.4 Преднастроенный клиент через Kickstart . . . 39
14.5 Проверка работы клиента . . . 39

15 Чек-лист безопасности перед прод-запуском 40

16 Диагностика и устранение проблем 42
16.1 Проверка статуса сервера . . . 42
16.2 Перезапуск сервера . . . 42

16.3 Логи сервера 43
16.4 Типовые проблемы 43

17 Завершение **45**
17.1 Куда идти дальше 45

ГЛАВА 1

Описание

Быстрый старт - пошаговый сценарий первичного развёртывания и настройки сервера **RuDesktop** для администратора: от подготовки машины до полностью готового к работе сервера, к которому уже могут подключаться клиенты

Подсказка

Каждый шаг содержит краткое описание действия и ссылки на подробные инструкции в Руководстве администратора и Руководстве пользователя

Важно

Часть шагов (PXE-сервер, отказоустойчивый кластер, Apache Superset) требует лицензии **UEM**

Эти шаги отдельно отмечены меткой **UEM-only**

ГЛАВА 2

Карта сценария

Полный сценарий развёртывания сервера состоит из следующих шагов:

1. *Шаг 1. Подготовка перед установкой* - системные требования, поддерживаемые ОС, сетевые требования, выбор сценария установки
2. *Шаг 2. Установка сервера* - установка DEB- или RPM-пакета, проверка работы сервера
3. *Шаг 3. Создание суперпользователя и первый вход* - создание административной учётной записи и вход в веб-интерфейс
4. *Шаг 4. Активация лицензии* - получение и активация лицензионного ключа
5. *Шаг 5. Сетевая настройка* - замена SSL-сертификата, изменение IP и порта, ограничение доступа
6. *Шаг 6. Базовые настройки сервера* - SMTP, двухфакторная аутентификация, группы по умолчанию, логирование
7. *Шаг 7. Подключение источников пользователей* - Active Directory, Keycloak, локальные пользователи и группы
8. *Шаг 8. Распределение доступов (ACL)* - кто из пользователей и групп может подключаться к каким устройствам и в каком режиме
9. *Шаг 9. Безопасность подключений* - корневые сертификаты, чёрный/белый списки, подсети
10. *Шаг 10. Дополнительные компоненты* - мосты, точки распространения, PXE, Superset, интеграции, Syslog, уведомления, Kickstart
11. *Шаг 11. Резервное копирование и эксплуатация* - бэкап БД, логи, очередь задач, отказоустойчивый кластер

12. *Шаг 12. Распространение клиента* - массовая установка клиента **RuDesktop** на удалённые устройства

ГЛАВА 3

Шаг 1. Подготовка перед установкой

Перед установкой сервера убедитесь, что машина соответствует системным требованиям и сети открыты необходимые порты

3.1 Системные требования

Минимальные требования для сервера **Удаленный доступ** (УД):

- **Процессор (CPU):** 4 ядра
- **Оперативная память (RAM):** 8 ГБ
- **Место на жёстком диске:** 20 ГБ свободного места
- **PostgreSQL:** версия 14 или выше

Для сервера с **УД и UEM** (на 2000 АРМ):

- **Процессор (CPU):** 8 ядер или выше
- **Оперативная память (RAM):** 16 ГБ или выше
- **Место на жёстком диске:** 100 ГБ + пространство для образов ОС и установочных пакетов
- **Сетевое подключение:** 1 Гбит/с

Полный список поддерживаемых ОС, требования к дисковой подсистеме (IOPS) и каналам до общих сервисов - на странице Системные требования

3.2 Сетевые требования

- Настроенный SSL/TLS-сертификат (по умолчанию - самоподписанный, рекомендуется заменить на доверенный, см. *Шаг 5. Сетевая настройка*)
- Настроенный межсетевой экран с ограничением доступа к административному веб-интерфейсу

Сводная таблица портов, которые могут потребоваться:

Порт	Протокол	Назначение	Когда нужен
443	TCP	Подключение клиентов **RuDesktop** и веб-интерфейс	Всегда
80	TCP	HTTP-редирект на HTTPS	При использовании Let's Encrypt
22	TCP	SSH к удалённым устройствам	Если используются SSH-доступы
67	UDP	DHCP-сервер PXE	При использовании PXE (UEM-only)
4011	UDP	ProxyDHCP-сервер PXE	При использовании PXE (UEM-only)
69	UDP	TFTP-сервер PXE	При использовании PXE (UEM-only)
445	TCP	SMB для установки Windows по PXE	При установке Windows через PXE (UEM-only)
5432	TCP	PostgreSQL	При вынесении БД на отдельный сервер или для точек распространения/кластера
6379	TCP	Redis	При вынесении Redis на отдельный сервер или для точек распространения/кластера
514	TCP/UI	Syslog	При публикации событий аудита во внешний SIEM

3.3 Подготовка ОС

Важно

Если вы используете **Astra Linux** (1.7 Воронеж или 1.8 Смоленск), перед установкой сервера временно отключите **МКЦ** и **МРД** - иначе при создании пользователя возникнет ошибка `PAM account manager`

Подробная инструкция: Установка сервера на Astra с МКЦ

Важно

Перед обновлением до версии 2.9 убедитесь, что у вас установлена **PostgreSQL 14** или выше

При необходимости выполните миграцию на новую версию PostgreSQL

3.4 Выбор сценария установки

Выберите подходящий способ развёртывания:

Стандартная установка

DEB- или RPM-пакет на уже установленную ОС - подходит для большинства случаев
Описано в *Шаге 2*

Установка из ISO-образа

Готовый ISO-образ с Ubuntu Server 24.04, PostgreSQL 16, Nginx и сервером **RuDesktop** - для развёртывания «с нуля»

Установка в закрытый контур

Установка без доступа в интернет (через локальный репозиторий или ручную загрузку пакетов)

Отказоустойчивый кластер

Несколько узлов сервера с общими **PostgreSQL** и **Redis**, **UEM-only**

ГЛАВА 4

Шаг 2. Установка сервера

Стандартная установка одной командой работает для **Ubuntu**, **Debian**, **Astra**, **ОСнова** (DEB) и для **РЕД ОС**, **AlterOS**, **МСВСфера** (RPM)

4.1 Установка DEB-пакета

Для **Ubuntu**, **Debian**, **Astra**, **ОСнова**:

```
bash -c "$(wget -O - https://storage.rudesktop.ru/repos/stable3.1/
↪install-rudesktop-server-stable3.1-deb.sh)"
```

4.2 Установка RPM-пакета

Для **РЕД ОС**, **AlterOS**, **МСВСфера**:

```
bash -c "$(wget -O - https://storage.rudesktop.ru/repos/stable3.1/
↪install-rudesktop-server-stable3.1-rpm.sh)"
```

Важно

Для остальных RPM-дистрибутивов (**ALT Linux**, **РОСА**, **CentOS**, **Fedora**, **AlmaLinux**) скачайте `.rpm` -пакет и установите его вручную через пакетный менеджер

После установки `.rpm` -пакета обязательно выполните команду rude reinstall

Подробные инструкции для всех способов: Установка/обновление сервера

4.3 Проверка установки

После успешной установки в выводе появятся строки об успешном запуске сервисов:

```
Install server
    Enable web socket ... OK
    Enable web service ... OK
    Enable relay ... OK
    Enable executor ... OK
Starting services
    Start web socket ... OK
    Start web service ... OK
    Start relay ... OK
    Start executor ... OK
    Start smbd ... OK
    Enable nginx ... OK
    Start nginx ... OK
    Set local connect to 192.168.10.15:443 ... OK
Сервер rudesktop успешно установлен.
```

Подсказка

Проверьте, что веб-интерфейс открывается по адресу `https://[адрес_сервера]/` - на этом этапе вы увидите страницу входа с самоподписанным сертификатом

ГЛАВА 5

Шаг 3. Создание суперпользователя и первый вход

После установки серверной части необходимо создать суперпользователя для доступа к веб-интерфейсу

5.1 Создание суперпользователя

Выполните команду на сервере:

```
rude createsuperuser
```

После выполнения команды введите следующие данные:

```
Логин: [ввести_имя_пользователя]
Электронная почта: [ввести_email_пользователя]
Password: [ввести_пароль]
Password (again): [повторить_пароль]
Superuser created successfully
```

5.2 Первый вход в веб-интерфейс

Откройте в браузере адрес `https://[адрес_сервера]/` и войдите под созданной учётной записью

Подсказка

Для смены пароля суперпользователя используйте команду rude changepassword

ГЛАВА 6

Шаг 4. Активация лицензии

Без активной лицензии часть функций сервера будет недоступна - на всех страницах будет отображаться уведомление с просьбой выполнить активацию

6.1 Получение ключа

Запросите лицензионный ключ:

- По адресу `sales@rudesktop.ru`
- Через персонального менеджера компании **RuDesktop**

Лицензия определяет:

- Максимальное количество подключаемых устройств
- Максимальное количество одновременных подключений
- Максимальное количество учётных записей пользователей
- Доступность модулей **UEM** и **MDM**
- Срок действия

6.2 Активация

Активация выполняется на странице **Администрирование → Лицензия** одним из двух способов:

- **Онлайн** - сервер обращается к серверу активации **RuDesktop** напрямую, требуется доступ в интернет
- **Офлайн** - администратор отправляет запрос активации в письме, получает ответный лицензионный текст и вставляет его в форму на сервере

Подробная инструкция: Лицензия

Важно

При активации лицензии без модуля **UEM** все фоновые задачи UEM-политик автоматически отключаются

Это нужно учитывать при переходе с UEM-лицензии на лицензию без UEM

Важно

При обновлении сервера с предыдущей минорной версии (например, 2.8 → 2.9) сначала запросите новый ключ, обновите его на странице **Лицензия**, и только потом запускайте обновление сервера

Иначе обновление завершится с ошибкой и откатом на предыдущую версию

Примечание

На этом этапе сервер уже запущен, лицензирован и принимает подключения

Дальнейшие шаги (5-11) - это последовательная настройка сервера для продуктивной эксплуатации

Часть из них опциональна и выполняется по необходимости

ГЛАВА 7

Шаг 5. Сетевая настройка

После первого входа рекомендуется настроить сетевые параметры сервера: заменить самоподписанный SSL-сертификат, при необходимости изменить IP-адрес или порт, ограничить доступ к веб-интерфейсу

Подсказка

Все шаги ниже опциональны и выполняются по необходимости

Если стандартные настройки (порт 443, самоподписанный сертификат, единый адрес) подходят - можно перейти к *Шагу 6*

7.1 Замена SSL-сертификата

По умолчанию сервер использует самоподписанный сертификат - клиенты и браузеры будут показывать предупреждение о недоверенном соединении

Рекомендуется заменить его на доверенный (корпоративный или Let’s Encrypt). Доступны два сценария замены:

- **Прямое подключение через rudesktop/ca/CA** - стандартный сценарий, когда не используется мост-балансировщик
- **Через конфигурацию nginx** - сценарий, когда в инфраструктуре используется мост **RuDesktop** для балансировки нагрузки

Подробная инструкция: Добавление собственных SSL-сертификатов

Важно

Перед заменой сертификатов сделайте резервную копию каталога `/var/lib/rudesktop/ca/` - команда `rude reinstall` удаляет файлы CA, и они не сохраняются автоматически

7.2 Изменение IP-адреса сервера

Чтобы изменить IP-адрес или доменное имя, под которым сервер публикуется для клиентов:

```
rude install [СЕРВЕР]:[ПОРТ]
```

Подсказка

Указывать порт необязательно - по умолчанию используется 443

Если нужно сбросить локальную конфигурацию и корневой CA при смене адреса (после этого клиенты потеряют доверие к серверу):

```
rude reinstall [СЕРВЕР]:[ПОРТ]
```

Важно

Команда `rude reinstall` **деструктивная** - удаляет `/etc/default/rudesktop`, `/etc/rudesktop/`, конфиги nginx и корневой CA

Подробнее, включая режим **двух IP-адресов** (для разных сетевых интерфейсов): Смена и установка IP

7.3 Изменение стандартного порта

Если порт 443 занят или требуется нестандартный порт, отредактируйте `/etc/nginx/sites-enabled/rudesktop`, замените значение `listen 443 ssl;` на нужный порт и перезагрузите сервер:

```
rude restart
```

Важно

Не забудьте открыть выбранный порт в межсетевом экране сервера и в правилах сетевого периметра

Подробная инструкция: Смена стандартного порта

7.4 Ограничение доступа к веб-интерфейсу

Если административный веб-интерфейс должен быть доступен только из определённых подсетей (при этом клиентский трафик **RuDesktop** продолжает обслуживаться), настройте в конфигурации `nginx` директивы `allow` /`deny` для блока `location / {`

Подробная инструкция: Ограничение доступа к веб-интерфейсу

7.5 Разделение портов веб и клиентов

Если требуется разнести административный веб-интерфейс и клиентский endpoint по разным портам (например, веб только во внутренней сети, клиентский endpoint наружу), создайте отдельный server-блок `nginx` для клиентов

Подробная инструкция: Разделение портов

7.6 Дополнительные сетевые настройки

- Смена адреса для модуля аналитики - для **Apache Superset** (UEM-only)
- Настройка подключения и SSL для сторонней БД - подключение к внешней **PostgreSQL** с защищённым каналом
- Настройка unix-socket - перевод сервера на работу через unix-socket вместо TCP

ГЛАВА 8

Шаг 6. Базовые настройки сервера

Базовые настройки задаются в веб-интерфейсе на странице **Администрирование → Настройки**

Ниже перечислены блоки, которые рекомендуется настроить при первичном развёртывании. Полное описание всех блоков и параметров - на странице Настройки

Подсказка

После внесения изменений в любом блоке нажмите кнопку Сохранить внизу страницы - без сохранения настройки не применятся

8.1 Настройка SMTP

Настройка SMTP-сервера обязательна для отправки приглашений, писем со сбросом пароля, системных уведомлений и одноразовых кодов **Email (OTP)** при двухфакторной аутентификации

В блоке Настройки SMTP укажите:

- SMTP сервер - например, `smtp.yandex.ru`
- SMTP порт - `25` (без шифрования), `465` (SSL) или `587` (STARTTLS)
- SMTP имя пользователя и SMTP пароль - учётные данные
- SMTP использовать TLS - включение шифрования
- Отправитель по умолчанию - адрес в поле `From` отправляемых писем

- Получатель по умолчанию - адрес для тестового сообщения и системных уведомлений

После сохранения проверьте настройки кнопкой Отправка тестового сообщения

8.2 Двухфакторная аутентификация

В блоке Аутентификация выберите второй фактор для входа в веб-интерфейс и клиент **RuDesktop**:

- **Email (OTP)** - требует настроенного *SMTP*
- **Телефон (OTP)** - требует настроенного SMS-шлюза (поддерживается `sms.ru`)
- **Telegram (OTP)** - требует настроенного Telegram-бота
- **MAX (OTP)** - требует настроенного MAX-бота
- **Аутентификатор (TOTP)** - Google Authenticator, Яндекс Ключ и аналоги, не требует SMTP/SMS/мессенджеров
- **Электронный ключ (FIDO2)** - аппаратный USB-токен
- **ЭЦП Рутокен (PKI)** - электронная подпись на устройстве **Рутокен**

Важно

Для способов **Email**, **Телефон**, **Telegram**, **MAX**: если в профиле пользователя не указаны соответствующие контактные данные, одноразовый пароль не отправится и пользователь не сможет войти

8.3 Защита от подбора пароля

В блоке Аутентификация рекомендуется настроить:

- Включить Captcha при входе в админ панель - активация **Yandex SmartCaptcha** для защиты входа
- Попытки входа до появления капчи - после скольких неудачных попыток показывается Captcha
- Попытки входа до блокировки IP - после скольких неудачных попыток IP блокируется

  Значение по умолчанию - `10`
- Время блокировки IP (в часах) - длительность блокировки

  По умолчанию - `0.5` (30 минут)

Подсказка

Чтобы вручную сбросить блокировку IP, выполните rude axes_reset_ip

8.4 Группы по умолчанию

В блоке Безопасность выберите группы, в которые автоматически попадают новые пользователи и устройства при первом подключении или регистрации:

- Группа по умолчанию для новых компьютеров
- Группа по умолчанию для новых пользователей

Важно

Список групп подгружается со страницы Группы

Создайте необходимые группы и распределите права **до** того, как разрешать саморегистрацию или импорт из домена

8.5 Длительность сессии и саморегистрация

В блоке Безопасность:

- Максимальная длительность сессии (в минутах) - время автоматического выхода

  По умолчанию - `20160` минут (14 дней)

- Разрешить самостоятельную регистрацию пользователей - активирует форму саморегистрации

Важно

При включении саморегистрации убедитесь, что у группы по умолчанию заданы минимально необходимые права - иначе зарегистрировавшийся пользователь не сможет работать в системе

8.6 Настройки мостов

В блоке Настройки мостов задайте правила подключения клиентов:

- Адрес основного моста - по умолчанию указывается адрес главного сервера
- Порт подключения клиентов - порт, прописываемый клиентам в установочных скриптах и пакетах

  По умолчанию совпадает с портом сервера (443); меняется при разделении портов

- Тип подключения - **Авто**, **Мост** или **NAT**
- Использовать hostname в качестве ID устройства - вместо числового ID устройству присваивается hostname

Важно

При использовании hostname в качестве ID имена хостов должны быть уникальными - иначе при подключении устройств с одинаковым hostname возникнет конфликт идентификаторов

8.7 Логирование и Syslog

В блоке Настройки логов включите дублирование событий аудита во внешний Syslog согласно политике безопасности вашей организации:

- Записывать статус подключений в syslog
- Записывать результаты запуска политик в syslog
- Записывать события аутентификации админ панели в syslog
- Записывать события HTTP запросов в syslog
- Записывать события CRUD (изменения объектов) в syslog
- Записывать события Экспорта в syslog

Подсказка

По умолчанию все настройки логов в Syslog выключены - включайте только те события, которые требуются по политике аудита

8.8 Прочие блоки

По мере необходимости настройте остальные блоки:

- Настройки Ansible - количество потоков и таймаут выполнения задач (политики UEM)
- Настройки клиента - таймауты сессий удалённого доступа
- Видеозаписи - путь хранения и качество видеозаписей сессий
- Настройки HelpDesk - перенаправление пользователей на внешнюю страницу техподдержки
- Карты - API-ключ **Яндекс.Карт** для отображения устройств
- Настройки баннера - баннер в клиенте и в веб-интерфейсе
- Обновления - уведомления о новых версиях сервера

Полное описание всех параметров: Настройки

ГЛАВА 9

Шаг 7. Подключение источников пользователей

На свежем сервере есть только один пользователь - суперпользователь, созданный на *Шаге 3*

Перед массовым внедрением необходимо создать структуру групп и подключить источники пользователей: локальных, **Active Directory** или **Keycloak**

Подсказка

Учётные записи в **RuDesktop** появляются пятью способами: ручное создание, саморегистрация, приглашение, импорт из домена, `rude createsuperuser`

Подробнее: Пользователи

9.1 Создание групп и распределение прав

Группа объединяет пользователей и устройства и определяет их права в системе

Перед добавлением пользователей создайте необходимые группы на странице **Организация → Группы** и назначьте им права доступа

Примечание

На сервере есть предустановленные группы: **Администратор**, **Без доступа**, **Гость**, **Мои группы**, **Права доступа**, **Руководитель подразделения**, **Сотрудник поддержки**

Их нельзя удалить, но можно редактировать

Группы используются для:

- разграничения прав доступа к устройствам между командами и ролями
- объединения устройств для применения политик и уведомлений
- включения принудительной записи удалённых сессий и передач файлов
- связывания со внешними источниками - доменными группами LDAP и группами **Keycloak**

Подробная инструкция: Группы

Важно

После создания групп вернитесь в **Администрирование → Настройки** и укажите их в полях Группа по умолчанию для новых пользователей и Группа по умолчанию для новых компьютеров (см. *Группы по умолчанию*)

9.2 Локальные пользователи

Локальные пользователи создаются вручную на странице **Организация → Пользователи** или приходят:

- через Приглашения - отправка ссылки приглашения на e-mail
- через Саморегистрацию - если в настройках включена опция Разрешить самостоятельную регистрацию пользователей

Подробная инструкция: Пользователи

9.3 Подключение Active Directory / LDAP

Интеграция с **LDAP** позволяет:

- авторизовать доменных пользователей в **RuDesktop** по их учётным данным
- формировать динамические группы на основе LDAP-групп
- распределять устройства и пользователей на основании LDAP-групп

Поддерживаются два режима интеграции:

- **Только авторизация** - учётная запись создаётся в **RuDesktop** при первом входе пользователя, периодическая синхронизация не нужна

- **Авторизация и периодическая синхронизация** - списки пользователей, групп и устройств заранее переносятся в локальную базу через политику Синхронизация со службой каталогов

Конфигурация выполняется на странице **Организация → Домены**. Можно подключить несколько доменов одновременно - пользователи разных доменов не пересекаются благодаря суффиксу `@<domain>` в логине

Подробная инструкция: Домены

9.4 Подключение Keycloak (SSO)

Интеграция с **Keycloak** позволяет настроить единый вход (SSO) и/или периодическую синхронизацию пользователей и групп

Поддерживаются три режима:

- **Только SSO авторизация** - пользователь входит через форму **Keycloak**, учётная запись создаётся при первом входе
- **Только синхронизация** - пользователи и группы переносятся по расписанию, вход выполняется по локальным учётным данным
- **SSO авторизация и синхронизация одновременно**

Группы из **Keycloak** можно связать с локальными группами **RuDesktop** для назначения прав на основании членства. Конфигурация выполняется на странице **Администрирование → Keycloak**. После настройки **Keycloak** можно выбрать как Авторизацию по умолчанию

Подробная инструкция: Keycloak

9.5 Подразделения

Если в организации несколько зон ответственности администраторов (например, филиалы или отделы), используйте Подразделения - это группы пользователей и устройств с отдельным администратором, управляющим только своими ресурсами

ГЛАВА 10

Шаг 8. Распределение доступов (ACL)

После создания групп и подключения источников пользователей нужно распределить права на конкретные устройства - кому из пользователей или групп разрешено подключаться к каким устройствам и в каком режиме

В **RuDesktop** этим управляют **Доступы** (ACL) - правила вида «кто и как может подключаться к каким устройствам». Каждое правило состоит из четырёх частей:

- **Подключаемые устройства** - кто инициирует подключение (пользователь, устройство, группа, динамическая группа или «все»)
- **Устройства для подключения** - к чему разрешено подключаться (устройство, группа, динамическая группа или «все»)
- **Права подключения** - что разрешено в рамках сессии (мастер-пароль, скрытое подключение, без подтверждения, удалённый терминал администратором и т.д.)
- **Разрешения** - типы подключений (Удалённый рабочий стол, Передача файлов, Терминал, RDP, TCP-туннелирование, Проброс USB)

При подключении сервер проверяет совпадения по всем активным правилам и собирает итоговый набор прав. Если для пары «оператор → клиент» нет ни одного активного правила, подключение **запрещено**. Управление выполняется на странице **Удалённый доступ → Доступы** в веб-интерфейсе

Подсказка

Если уже выстроены группы пользователей и устройств (см. **Шаг 7**), задавайте правила на уровне групп - новые устройства, попадающие в группу, автоматически получают одинаковые права

Это сильно проще, чем индивидуальные правила на каждое устройство

Важно

- Суперпользователь имеет полный доступ независимо от настроенных правил
- Правило с выключенным флагом Включено сохраняется, но не учитывается - его можно вернуть в работу позднее
- Правила **Чёрного и Белого списков** (см. *Шаг 9*) проверяются **до** ACL и могут блокировать подключение независимо от настроенных доступов

Подробная инструкция: Доступы

ГЛАВА 11

Шаг 9. Безопасность подключений

После подключения источников пользователей рекомендуется ограничить, кто и откуда может подключаться к серверу

11.1 Корневые сертификаты для проверки клиентов

На странице **Администрирование → Сертификаты** управляются корневые сертификаты в формате PEM, которые используются для проверки подлинности подключений - например, при настройке мостов, когда мост использует собственный центр сертификации

Важно
После установки сервера автоматически создаётся основной сертификат
Он помечается как защищённый и не может быть изменён или удалён

Подробная инструкция: Сертификаты

11.2 Чёрный список

Чёрный список запрещает подключение устройств к серверу по следующим признакам:

- **IP-адрес**
- **Адрес сети** (CIDR-подсеть, например `192.168.1.0/24`)

- **Уникальный код** (UUID устройства)
- **Имя пользователя**
- **Название хоста**

Правила настраиваются на странице **Администрирование → Чёрный список**

Важно

Правила **Чёрного списка** имеют приоритет над Белым списком: если устройство одновременно подходит под обе категории, подключение запрещается

Подробная инструкция: Чёрный список

11.3 Белый список

Белый список разрешает подключение устройств по тем же признакам (IP, подсеть, UUID, имя пользователя, hostname)

Используется, когда нужно явно перечислить разрешённые устройства. Правила настраиваются на странице **Администрирование → Белый список**

Важно

- Если **Белый список** пуст, подключение разрешено всем устройствам
- Если в **Белом списке** есть записи, подключение разрешено только устройствам, соответствующим хотя бы одному правилу
- Правила **Чёрного списка** имеют приоритет над **Белым списком**

Подробная инструкция: Белый список

11.4 Подсети и геолокация

Если в инфраструктуре используются устройства с приватными IP-адресами (внутренняя корпоративная сеть), их геопозиция не определяется автоматически

Чтобы устройства корректно отображались на карте и подключались к ближайшему мосту, зарегистрируйте подсети на странице **Администрирование → Подсети**. Каждое правило сопоставляет диапазон IP-адресов (CIDR-подсеть) с городом и координатами

Подробная инструкция: Подсети

11.5 SSH-доступы

Для подключения сервера **RuDesktop** к удалённым устройствам по SSH (например, для запуска политик на Linux-устройствах без агента) на странице **Администрирование → SSH доступы** заведите учётные записи с логином, паролем или ключом

Подробная инструкция: SSH доступы

ГЛАВА 12

Шаг 10. Дополнительные компоненты

Этот шаг охватывает компоненты, которые подключаются по необходимости - для распределённой инфраструктуры, аналитики, удалённой установки ОС и интеграции с внешними системами

12.1 Мосты для удалённых филиалов

Мост - это отдельный сервер **RuDesktop**, развёрнутый в географически удалённой точке

Главный сервер по координатам подбирает ближайший к клиенту мост и направляет через него подключение, что сокращает сетевую задержку для удалённых филиалов. Подключение моста выполняется в два этапа:

1. **Развёртывание сервера-моста** - установка пакета с переменной `INSTALL_MODE=relay` на отдельной машине

   Подробная инструкция: Настройка мостов

2. **Регистрация моста на главном сервере** - создание записи на странице **Администрирование → Мосты**

   Подробная инструкция: Мосты

Подсказка

Чтобы устройства с приватными IP корректно подбирались к ближайшему мосту, заранее зарегистрируйте Подсети (см. *Подсети и геолокация*)

12.2 Точки распространения

Точка распространения - отдельный узел в режиме исполнителя (`INSTALL_MODE=executor`)

Узел подключается к общим **Redis** и **PostgreSQL** главного сервера, забирает оттуда задачи и выполняет их у себя - это снимает нагрузку с главного сервера и позволяет распараллелить выполнение задач. Подключение точки распространения:

1. Создать запись на странице **Администрирование → Точки распространения** в веб-интерфейсе главного сервера
2. Открыть сетевой доступ к **Redis** и **PostgreSQL** с узла-исполнителя
3. Установить пакет с переменной `INSTALL_MODE=executor` на узле-исполнителе

Предупреждение

Версии сервера на главном узле и точке распространения должны совпадать

После обновления главного сервера точку распространения необходимо обновить до той же версии

Подробная инструкция: Настройка точек распространения и Точки распространения

12.3 PXE-сервер для удалённой установки ОС

Доступно только в UEM версии

Встроенный **PXE-сервер RuDesktop** позволяет удалённо устанавливать ОС в локальной сети. Реализован как systemd-сервис `rudesktop-pxe.service` и включает DHCP-сервер на порту 67, ProxyDHCP на порту 4011, TFTP-сервер и SMB-сервер для **Windows**. Сервис автоматически запускается и останавливается при публикации образа ОС

Подробная инструкция: Настройка PXE, включая примеры конфигурации **MikroTik** и **DHCPD**

12.4 Модуль аналитики (Apache Superset)

Доступно только в UEM версии

Модуль `rudesktop-superset` (встроенный **Apache Superset**) служит для организации, обработки и визуализации данных из базы сервера **RuDesktop** - построения отчётов и аналитических дашбордов

Установка и обновление модуля выполняется отдельным пакетом, после установки модуль управляется командами rude superset start, `stop`, `restart`, `status`, `backup`, `restore`

Подробная инструкция: Установка модуля аналитики

Подсказка

Если используется только лицензия **Удаленный доступ** (без UEM), модуль аналитики устанавливать не нужно

12.5 Интеграции с внешними системами

На странице Интеграции описаны подключения сервера к внешним системам:

- Jatoba - российская СУБД как замена **PostgreSQL**
- Kaspersky Security Center - двусторонняя интеграция: импорт устройств из KSC и распространение клиента **RuDesktop** через KSC
- Multifactor - многофакторная аутентификация через сервис **Multifactor**
- RuSIEM - отправка событий аудита в SIEM-систему **RuSIEM**

12.6 Публикация событий в Syslog

Дублирование событий аудита (подключения, политики, входы, HTTP-запросы, изменения объектов, экспорт) во внешний **Syslog** или SIEM-систему

Сообщения отправляются в формате **CEF (Common Event Format)** в кодировке UTF-8. Включение состоит из трёх шагов:

1. Настроить локальный syslog-демон (`rsyslog` или `syslog-ng`) на приём по TCP и пересылку в SIEM
2. Указать адрес приёмника в `/etc/rudesktop/settings` через параметры `SYSLOG_HOST` и `SYSLOG_PORT`, перезапустить сервер
3. В веб-интерфейсе на странице **Администрирование → Настройки** в блоке Настройки логов включить тумблеры для нужных групп событий (см. *Логирование и Syslog*)

Подробная инструкция: Публикация событий в Syslog

12.7 Уведомления пользователям

Доступно только в UEM версии

Уведомления - рассылка оповещений пользователям и группам о событиях сервера: завершении задач (политик, отчётов, синхронизаций), готовности отчётов, изменениях конфигурации устройств после инвентаризации, поступлении новых обращений в поддержку. Поддерживаемые каналы доставки:

- **Email** - на адрес пользователя или общий адрес из настроек сервера (требует настроенного *SMTP*)

- **Телефон (SMS)** - на номер пользователя (требует настроенного SMS-шлюза)
- **Telegram** - личный чат пользователя и/или общий чат из настроек сервера
- **MAX** - личный чат пользователя в мессенджере **MAX** и/или общий чат из настроек сервера

Правила настраиваются на странице **Организация → Уведомления** - каждое правило задаёт «кому, по какому каналу, по какому событию» отправлять оповещения, одно правило может покрывать сразу несколько событий

Важно

- Чтобы пользователь получал уведомления, в его профиле должны быть заполнены контактные данные для выбранного канала (телефон, Email, Telegram, MAX)
- Для отправки в **общий чат** соответствующие поля должны быть заполнены в Настройках сервера
- Уведомления общего чата по **Телефону (SMS)** не предусмотрены

Подробная инструкция: Уведомления

12.8 Kickstart-преднастройка клиента

Конфигурационные файлы **Kickstart** применяются к клиенту **RuDesktop** при первой установке или по политике

Используются для централизованной преднастройки клиента - указания адреса сервера, группы по умолчанию, параметров подключения. Файлы расположены на сервере в каталогах:

```
/var/lib/rudesktop/kickstart/windows
/var/lib/rudesktop/kickstart/linux
/var/lib/rudesktop/kickstart/macos
```

Профили преднастройки управляются на странице Kickstart, формат файлов и порядок применения описаны в разделе Настройка Kickstart

ГЛАВА 13

Шаг 11. Резервное копирование и эксплуатация

Перед запуском сервера в продуктив настройте регулярное резервное копирование, ознакомьтесь с расположением логов и при необходимости разверните отказоустойчивый кластер

13.1 Резервное копирование БД

Команда `rude backup` сохраняет базу данных **PostgreSQL** в gzip-сжатый файл:

```
rude backup /path/to/file.gz
```

Подсказка

Рекомендуется выполнять резервное копирование перед каждым обновлением сервера

При обновлении на минорную версию (например, 2.8 → 2.9) бэкап создаётся автоматически в `/var/lib/rudesktop/`

Восстановление из резервной копии - командой rude restore

Важно

Команда `rude backup` сохраняет **только базу данных**

Для полного восстановления сервера на чистой инсталляции дополнительно сохраните:

- `/etc/default/rudesktop` - параметры запуска и переменные окружения
- `/etc/rudesktop/settings` - настройки веб/backend
- `/etc/rudesktop-relay.toml` - конфигурация relay (если используется)
- `/var/lib/rudesktop/media/` - загруженные файлы (репозитории, отчёты)
- `/var/lib/rudesktop/user/` - пользовательские override-конфиги (PXE, Ansible)
- `/var/lib/rudesktop/kickstart/` - kickstart-сценарии
- `/var/lib/rudesktop/ca/` - сертификаты CA сервера

Подробная инструкция: Резервное копирование

13.2 Логи сервера

Все логи находятся в каталоге `/var/log/rudesktop/` (права `700`, владелец `rudesktop` - для просмотра требуются `sudo`)

Основные файлы:

- `rudesktop.log` - Django-часть: веб-интерфейс, API, фоновые задачи, синхронизация LDAP/AD
- `execution.log` - модуль выполнения политик и задач (executor)
- `server.log` - нативные компоненты `relay` / `rz`: подключения клиентов, маршрутизация
- `updater.log` - служба обновления сервера
- `redis.log` - встроенный Redis
- `domains/job_<domain_id>.log` - подробные логи синхронизации с доменом

Подробная инструкция: Логи сервера

13.3 Очередь задач

Просмотр и остановка фоновых задач - на странице **Администрирование → Очередь задач**

Задачи попадают в очередь автоматически: выполнение политик UEM, синхронизация с доменами и **Keycloak**, фоновый экспорт, массовые действия

Подробная инструкция: Очередь задач

13.4 Отказоустойчивый кластер

Доступно только в UEM версии

Для непрерывной работы сервера при отказе одного узла или целой площадки разверните несколько узлов **RuDesktop** в режиме высокой доступности (HA) с общими **PostgreSQL** и **Redis**:

- 2, 3 или более узлов
- Поддерживаются схемы **Active-Active** и **Active-Passive**
- Балансировка нагрузки и автоматическое переключение при отказе

Подробная инструкция: Развертывание отказоустойчивого кластера

Важно

Каналы между узлами и общими сервисами должны обеспечивать пропускную способность не менее **1 Гбит/с** и задержку менее **1 мс** - **Redis** критически чувствителен к задержкам

ГЛАВА 14

Шаг 12. Распространение клиента

Финальный шаг - распространение клиента **RuDesktop** на удалённые устройства

Доступны несколько способов

14.1 Через сканирование сети

В разделе Сканирование сети создайте профиль обнаружения и запустите поиск устройств. Подготовьте учётные данные для установки клиента, проверьте установку на одном устройстве, затем настройте правила авто-установки для остальных устройств

14.2 Через Kaspersky Security Center или Active Directory

Массовое распространение клиента средствами **KSC** или **Active Directory**

Примечание

Подробная инструкция Kaspersky: https://support.kaspersky.ru/ksc-linux/15/6383

14.3 Ручная установка

Установочные пакеты находятся в веб-интерфейсе сервера на странице Панель управления

Поддерживаются клиенты для **Windows**, **Linux**, **macOS**, **Android**, **iOS**

Подсказка

Чтобы открыть страницу загрузки пакетов без авторизации, включите в **Администрирование → Настройки** опцию Доступ к пакетам клиента неавторизованными пользователями

Страница будет доступна по адресу `https://[АДРЕС_СЕРВЕРА]/dashboard/distr/`

14.4 Преднастроенный клиент через Kickstart

Через Kickstart можно сразу указать адрес сервера, группу по умолчанию и параметры подключения - клиент применит эти настройки при первой установке без участия пользователя

14.5 Проверка работы клиента

После установки клиента на тестовое устройство проверьте, что оно появилось в веб-интерфейсе и доступно для подключения:

1. Откройте страницу Устройства - устройство должно появиться в списке со статусом **Онлайн**
2. Откройте свойства устройства и проверьте корректность данных: hostname, IP-адрес, версия клиента, ОС, группа
3. Запустите тестовое подключение через действие Подключиться - должна открыться сессия удалённого доступа
4. После завершения сессии проверьте запись в Журнале сессий

Подсказка

Если устройство не появляется в списке - проверьте *Шаг 9* (чёрный/белый списки), доступность порта 443 с устройства до сервера и логи клиента (вкладка **Поддержка → Логи** в клиенте)

ГЛАВА 15

Чек-лист безопасности перед прод-запуском

Перед вводом сервера в продуктивную эксплуатацию пройдитесь по чек-листу:

Сеть и шифрование

- Самоподписанный SSL-сертификат заменён на доверенный (см. *Шаг 5*)
- Открыты только необходимые порты, веб-интерфейс ограничен по IP/подсетям
- Веб-интерфейс и клиентский endpoint при необходимости разнесены по разным портам

Аутентификация

- Включена двухфакторная аутентификация для входа в веб-интерфейс
- Включена Captcha и блокировка IP при подборе пароля
- Изменены пароли стандартных учётных записей, выданы индивидуальные пароли
- Если разрешена саморегистрация - у группы по умолчанию заданы минимально необходимые права

Группы и права

- Созданы группы по ролям (администраторы, операторы, пользователи), у каждой настроены минимально необходимые права
- Указаны группы по умолчанию для новых пользователей и устройств

- Подключены источники пользователей (AD/LDAP, Keycloak) или заведены локальные учётки

Защита подключений

- Настроены чёрный и/или белый список устройств
- Загружены корпоративные корневые сертификаты

Эксплуатация

- Настроено регулярное резервное копирование БД (по cron или systemd-timer)
- Включена публикация событий в Syslog согласно политике аудита
- Настроен мониторинг свободного места в `/var/lib/rudesktop/` и `/var/log/rudesktop/`
- Установлен источник бесперебойного питания (UPS)

ГЛАВА 16

Диагностика и устранение проблем

Если после развёртывания что-то не работает - начинайте с этих команд

16.1 Проверка статуса сервера

```
rude status
```

Команда покажет состояние всех компонентов: `nginx`, `relay`, `executor`, `web`, `redis`, `postgresql`, `pxe`

16.2 Перезапуск сервера

```
rude restart
```

Подсказка

После изменения SSL-сертификата, IP-адреса, порта или конфигурации `nginx` сервер нужно перезапустить вручную

После сохранения настроек в веб-интерфейсе перезапуск, как правило, не требуется

16.3 Логи сервера

Все логи находятся в `/var/log/rudesktop/` (см. *Шаг 10 → Логи сервера*)

Типичные команды диагностики:

```
sudo tail -f /var/log/rudesktop/rudesktop.log    # веб-интерфейс, API, синхронизация
sudo tail -f /var/log/rudesktop/server.log       # подключения клиентов, relay
sudo tail -f /var/log/rudesktop/execution.log    # политики и задачи UEM
```

16.4 Типовые проблемы

Проблема	Что проверить
Веб-интерфейс не открывается	Доступность порта 443 с клиента; статус `nginx` (`rude status`); запись `listen` в `/etc/nginx/sites-enabled/rudesktop`
Клиент не подключается к серверу	IP/доменное имя сервера в клиенте совпадает с тем, что указан при `rude install`; правила чёрного и белого списка; логи `server.log`
«Pam account manager» при `createsuperuser` на Astra	Не отключён МКЦ/МРД
Не приходят OTP по Email	Заполнен *блок SMTP* и пройден тест отправки; в профиле пользователя указан e-mail
Не отрабатывает синхронизация с AD	Подробные логи в `/var/log/rudesktop/domains/job_<id>.log`; включить Подробные логи синхронизации AD для диагностики
Не выполняются политики UEM	Очередь задач в **Администрирование → Очередь задач**; статус `executor` (`rude status`); логи `execution.log`
Заблокирован вход после неудачных попыток	Сбросить блокировку IP - rude axes_reset_ip; сбросить пароль - rude changepassword

Подсказка

Если не удаётся диагностировать проблему самостоятельно, выполните команду rude diag - она автоматически соберёт логи, конфигурации и состояние сервисов в один архив

Полученный файл приложите к обращению в техническую поддержку **RuDesktop** - это быстрее и надёжнее, чем собирать данные вручную

ГЛАВА 17

Завершение

На этом этапе сервер **RuDesktop** полностью развёрнут и готов к работе:

- ✓ Установлен и проверен сервер
- ✓ Создан суперпользователь и активирована лицензия
- ✓ Настроена сеть (SSL, IP, порт)
- ✓ Настроены SMTP, 2FA и базовые параметры безопасности
- ✓ Подключены источники пользователей (локальные, AD, Keycloak)
- ✓ Настроены правила доступа (чёрный/белый списки, подсети, сертификаты)
- ✓ Подключены дополнительные компоненты (по необходимости)
- ✓ Настроено резервное копирование
- ✓ Распространён клиент на удалённые устройства

17.1 Куда идти дальше

Руководство пользователя
Работа в веб-интерфейсе: удалённый доступ, политики, задачи, инвентаризация, отчёты

Руководство администратора
Расширенная настройка сервера, CLI-команды `rude`, REST API, диагностика

Сценарии использования
Готовые сценарии для типовых задач

FAQ
Часто задаваемые вопросы и решения типовых проблем