

**ПРОГРАММНАЯ ПЛАТФОРМА ДЛЯ УПРАВЛЕНИЯ
КОРПОРАТИВНЫМИ ЗНАНИЯМИ, AI-
АССИСТЕНТАМИ И ИНТЕЛЛЕКТУАЛЬНЫМИ
АГЕНТАМИ «SEMANTIX»**

Инструкция по установке ПО

Листов 76

АННОТАЦИЯ

Настоящий документ содержит сведения, необходимые для установки, настройки, эксплуатации, контроля состояния, защиты, резервного копирования, обновления и восстановления программного обеспечения Semantix. Документ предназначен для работников, выполняющих обязанности системного администратора, администратора безопасности и администратора организации.

Документ построен с учётом требований Единой системы программной документации к руководству системного программиста и общих требований к текстовым программным документам.

Команды, имена файлов, переменных и служб приводятся в точном виде, необходимом для выполнения операций. Остальные наименования и пояснения приведены на русском языке. Названия разделов экранной формы соответствуют русской локализации программы.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ	6
1.1 Наименование и назначение.....	6
1.2 Условные обозначения	6
1.3 Требования к квалификации	6
1.4 Границы применимости руководства	7
2. СОСТАВ ПОСТАВКИ И ПРОГРАММНЫЕ КОМПОНЕНТЫ	7
2.1 Состав комплекта поставки	7
2.2 Состав после развёртывания	9
2.3 Зависимости, сохраняемые данные и последствия отказа	9
3. УСЛОВИЯ ПРИМЕНЕНИЯ	10
3.1 Поддерживаемые операционные системы и варианты размещения	10
3.2 Минимальные ресурсы для установки на одном сервере	11
3.3 Требования к дискам и времени.....	11
3.4 Матрица совместимости кластерной установки.....	11
3.5 Расчёт ресурсов кластерной установки	12
3.6 Уровни готовности и отказоустойчивости	13
4. ПОДГОТОВКА К УСТАНОВКЕ	13
4.1 Исходные данные.....	13
4.2 Сетевое разграничение	14
4.3 Подготовка узла для установки на одном сервере.....	14
4.4 Подготовка узлов Astra Linux Special Edition 1.7 и 1.8.....	15
4.5 Подготовка узлов РЕД ОС 7.3 и 8.0.....	16
4.6 Подготовка Deckhouse Kubernetes Platform	17
4.7 Подготовка изолированной среды	19
5. УСТАНОВКА ПРОГРАММЫ.....	19
5.1 Общие правила.....	19
5.2 Установка на одном сервере.....	20
5.3 Кластерная установка	23
5.4 Проверка после установки.....	30
6. ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА.....	30
6.1 Создание главного администратора	30
6.2 Настройка русского языка.....	32
6.3 Настройка моделей.....	33
6.4 Создание организации	36

6.5 Активация лицензии.....	37
7. УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ И ДОСТУПОМ	38
7.1 Добавление пользователя	38
7.2 Изменение и отзыв доступа	40
7.3 Удаление пользователя из организации	41
7.4 Просмотр всех пользователей	42
7.5 Удаление организации.....	42
8. УПРАВЛЕНИЕ БАЗАМИ ЗНАНИЙ И ФАЙЛАМИ	44
8.1 Создание базы знаний.....	44
8.2 Состояния обработки	45
8.3 Ограничения загрузки.....	48
8.4 Подключение внешнего источника данных.....	49
8.5 Подключение сервера инструментов.....	51
8.6 Создание помощника	52
9. ЖУРНАЛИРОВАНИЕ И КОНТРОЛЬ СОСТОЯНИЯ.....	53
9.1 События, подлежащие контролю	53
9.2 Ежедневная проверка	53
9.3 Пороговые значения оповещений	55
9.4 Дополнительный контроль операционной системы и кластера.....	56
10. РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ	56
10.1 Состав резервной копии	56
10.2 Рекомендуемая схема	57
10.3 Копирование при установке на одном сервере.....	57
10.4 Копирование кластерной установки	58
10.5 Восстановление	59
11. ОБНОВЛЕНИЕ ПРОГРАММЫ.....	60
11.1 Подготовка обновления.....	60
11.2 Порядок обновления при установке на одном сервере	60
11.3 Порядок обновления кластера	60
11.4 Обновление операционной системы, Kubernetes и Deckhouse.....	61
12. УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ	62
12.1 Сбор диагностических сведений.....	63
12.2 Диагностика кластерной установки	63
13. ЗАЩИТА ИНФОРМАЦИИ.....	64
13.1 Обязательные меры	64

13.2Работа с внешними моделями и подключениями	64
13.3Защита кластерной установки на поддерживаемых операционных системах	65
14. РЕГЛАМЕНТНЫЕ РАБОТЫ	65
15. ЗАВЕРШЕНИЕ РАБОТЫ.....	66
Приложение А (обязательное).....	68
Приложение Б (рекомендуемое)	69
Приложение В (справочное)	71
Приложение Г (обязательное)	72
Приложение Д (рекомендуемое)	74
Приложение Е (справочное)	76

1. ОБЩИЕ СВЕДЕНИЯ

1.1 Наименование и назначение

Полное наименование: Программная платформа для управления корпоративными знаниями, AI-ассистентами и интеллектуальными агентами «Semantix».

Краткое наименование: Программная платформа Semantix (далее – Semantix).

Назначение, функциональные возможности и область применения Semantix установлены в документе «Описание применения Semantix». Настоящее руководство определяет порядок установки, настройки и административного сопровождения программы.

Руководство используется совместно с документами «Описание применения Semantix», «Руководство пользователя Semantix» и эксплуатационной документацией на применяемые системные средства.

1.2 Условные обозначения

Термин	Значение в настоящем руководстве
Комплект поставки	Файлы установки, программные образы, контрольные суммы и эксплуатационные документы, передаваемые для установки Semantix.
Программный компонент	Логически обособленная часть Semantix или системное средство, необходимое для её работы.
Организация	Изолированная область данных и настроек одной организации. В отдельных подписях экранной формы используется слово «тенант».
Главный администратор	Пользователь, управляющий организациями и всеми пользователями системы.
Администратор организации	Пользователь, управляющий участниками и ресурсами своей организации.
Узел	Вычислительная машина, на которой размещаются программные компоненты.
Контейнер	Изолированная среда выполнения программного компонента.
Образ	Неизменяемый комплект файлов для запуска контейнера.
Постоянный том	Область хранения данных, сохраняемая при повторном создании контейнера.
Журнал	Последовательность сообщений о работе программного компонента либо о действиях пользователей.
Резервная копия	Копия данных и настроек, предназначенная для восстановления.

1.3 Требования к квалификации

Администратор должен владеть основами работы с операционными системами семейства Linux, сетями передачи данных, средствами управления контейнерами, реляционными базами данных, объектными хранилищами и

средствами защиты информации. Для промышленного размещения в кластере требуется опыт сопровождения кластеров контейнеров и постоянных томов.

1.4 Границы применимости руководства

Руководство распространяется на поставку Semantix, содержащую элементы, перечисленные в разделе 2. До начала установки администратор проверяет обозначение версии, состав поставки и контрольные суммы. Установка прекращается при отсутствии обязательного элемента либо несовпадении контрольной суммы.

Условие	Обязательное решение до начала работ
Версия Semantix	Записать номер версии из комплекта поставки и контрольные суммы программных образов.
Операционная система	Выбрать одну из операционных систем, перечисленных в разделе 3.1, и установить поддерживаемое обновление.
Вариант размещения	Выбрать установку на одном сервере, стандартный кластер Kubernetes либо Deckhouse Kubernetes Platform.
Режим защиты	Зафиксировать действующие средства разграничения доступа и согласованные исключения. Самовольное отключение защитных механизмов запрещено.
Отказоустойчивость	Утвердить схему базы данных, объектного и поискового хранилищ, временного хранилища, постоянных томов и резервного копирования.
Внешние системы	Определить службы моделей, почты и источники данных, разрешённые сетевые направления и владельцев служебных учётных записей.

Указание совместимости с операционной системой или кластерной платформой означает допустимый вариант размещения Semantix при соблюдении матрицы версий и успешном выполнении приёмочных проверок. Оно не является заявлением о сертификации Semantix как средства защиты информации и не распространяется автоматически на любые сочетания версий системных средств.

2. СОСТАВ ПОСТАВКИ И ПРОГРАММНЫЕ КОМПОНЕНТЫ

2.1 Состав комплекта поставки

До распаковки и запуска администратор сверяет комплект поставки с приведённым перечнем. Контрольные суммы проверяются для каждого архива и программного образа.

Элемент	Состав	Назначение
Каталог установки на одном сервере	docker/	Файлы запуска Semantix и системных компонентов на одном сервере.
Основное описание контейнеров	docker/docker-compose.yml	Запуск серверной части Semantix и обработчика заданий.
Описание системных компонентов	docker/docker-compose-base.yml	Запуск базы данных, поискового, объектного и временного хранилищ.

Элемент	Состав	Назначение
Рабочие параметры	docker/.env	Версии образов, адреса, порты, пароли и режимы работы. Перед запуском создаётся защищённая резервная копия исходного файла.
Шаблон системных настроек	docker/service_conf.yaml.template	Формирование настроек соединений между программными компонентами.
Сценарии запуска и переноса	docker/entrypoint.sh; docker/migration.sh	Запуск серверных процессов, резервное копирование и восстановление для установки на одном сервере.
Настройки поискового хранилища	docker/infinity_conf.toml	Параметры запуска поискового хранилища Infinity.
Настройки входной веб-службы	docker/nginx/	Публикация экранной формы и программного интерфейса по защищённому протоколу.
Кластерный пакет	Архив установки Semantix для Kubernetes; файл значений; описания ресурсов	Установка Semantix в стандартном Kubernetes или Deckhouse Kubernetes Platform.
Перечень образов	Наименования, версии и контрольные суммы образов	Загрузка только неизменяемых и проверенных образов.
Ведомость контрольных сумм	SHA256SUMS	Проверка целостности файлов комплекта поставки.
Документация	Описание применения; руководство администратора; руководство пользователя	Установка, настройка и эксплуатация Semantix.

Проверка контрольных сумм:

Конкретные значения SHA-256 относятся к определённой версии Semantix и поэтому не приводятся в общем тексте руководства. Они содержатся в файле SHA256SUMS и в ведомости контейнерных образов, включённых в комплект поставки. Отсутствие этих файлов или хотя бы одного значения означает, что комплект поставки неполный; начинать установку нельзя.

До распаковки перейти в корневой каталог комплекта поставки и выполнить проверку:

```
sha256sum -c SHA256SUMS
```

Проверка считается успешной, если для каждого файла выведено ОК. При сообщении FAILED, отсутствии файла или строки в ведомости установку остановить и запросить комплект повторно. Редактировать SHA256SUMS вручную запрещается.

Для контейнерных образов дополнительно сверить digest (контрольную сумму) вида sha256:<значение> из ведомости образов с digest образа во внутреннем реестре. Фиксированный тег без digest не подтверждает неизменность образа.

```
docker image inspect <имя_образа:версия> --format '{{json .RepoDigests}}'
```

Для установки на одном сервере обязательны каталог docker, программные образы и ведомость контрольных сумм. Для кластерного размещения дополнительно обязателен кластерный пакет. Отсутствие кластерного пакета означает, что данный комплект предназначен только для установки на одном сервере.

2.2 Состав после развёртывания

Программный компонент	Объект размещения	Назначение	Постоянные данные
Серверная часть Semantix	Контейнер или несколько экземпляров в Kubernetes	Экранные формы, программный интерфейс и прикладные операции.	Настройки и связи объектов сохраняются в PostgreSQL; файлы — в объектном хранилище.
Обработчик заданий Semantix	Отдельный контейнер или несколько экземпляров в Kubernetes	Извлечение содержимого документов, создание фрагментов и выполнение фоновых заданий.	Состояние заданий — в PostgreSQL и временном хранилище; результаты — в постоянных хранилищах.
PostgreSQL 16	Контейнер, постоянный том либо внешняя служба	Учётные записи, организации, настройки, связи объектов и состояние заданий.	Критичные данные, обязательные для резервного копирования.
Infinity 0.6.15	Контейнер, постоянный том либо отдельная служба	Поисковые представления и поиск по документам.	Индексы, подлежащие копированию или повторному построению.
Объектное хранилище MinIO	Контейнер, постоянный том либо внешняя служба	Исходные документы и производные файлы.	Критичные пользовательские файлы.
Временное хранилище Valkey 8	Контейнер, постоянный том либо внешняя служба	Очереди, сеансы и короткоживущее служебное состояние.	Текущее состояние заданий; не заменяет резервную копию постоянных данных.
Входная веб-служба	В составе серверного контейнера либо отдельным компонентом кластера	Приём защищённых соединений и передача запросов серверной части.	Свидетельства и настройки; пользовательские данные не хранит.
Служба моделей	Внешняя служба или отдельная нагрузка в кластере	Смысловое представление, ранжирование и подготовка ответов.	Не входит в стандартный комплект поставки Semantix; параметры подключения сохраняются в Semantix.

2.3 Зависимости, сохраняемые данные и последствия отказа

При проектировании необходимо отделять повторно создаваемые из образов компоненты от компонентов, содержащих постоянные данные. Увеличение числа экземпляров серверной части или обработчиков не устраняет единичную точку отказа в базе данных либо хранилище.

Программный компонент	Последствие отказа	Требование для промышленной среды
Серверная часть Semantix	Новые запросы не принимаются либо завершаются ошибкой; данные в хранилищах сохраняются.	Не менее двух экземпляров при требовании непрерывности, распределение по разным узлам, проверки готовности и ограничения ресурсов.
Обработчики заданий	Новые документы и фоновые задания не обрабатываются; выполнявшееся задание может быть повторено.	Не менее двух экземпляров, управляемое повторение заданий, контроль очереди и блокировка одновременной обработки одного задания.
PostgreSQL	Недоступны вход, настройки, организации и прикладные операции.	Отказоустойчивая внешняя служба либо кластерная схема; согласованная копия и проверенная процедура переключения.
Объектное хранилище	Недоступны исходные файлы и результаты обработки.	Избыточное хранение, контроль целостности, версии объектов и отдельная резервная копия.
Поисковое хранилище	Поиск и обработка документов нарушены.	Поддерживаемая многосоставная схема либо документированное повторное построение из базы данных и исходных файлов.
Временное хранилище	Нарушаются сеансы, очереди и фоновые задания.	Схема с переключением либо утверждённое время восстановления; контроль потери незавершённых заданий.

3. УСЛОВИЯ ПРИМЕНЕНИЯ

3.1 Поддерживаемые операционные системы и варианты размещения

Semantix поддерживает установку на одном сервере и кластерное размещение на следующих российских операционных системах архитектуры x86-64.

Операционная система	Версии	Один сервер	Kubernetes и Deckhouse
Astra Linux Special Edition	1.7; 1.8	Да	Да
РЕД ОС	7.3; 8.0	Да	Да

Примечание — Основные примеры подготовки узла в настоящем руководстве приведены для Astra Linux Special Edition 1.8. Отличия подготовки РЕД ОС приведены в разделе 4.5. После подготовки операционной системы порядок установки Semantix одинаков для любого выбранного варианта размещения.

Deckhouse Kubernetes Platform является платформой на основе Kubernetes. В карточке установки указываются операционная система узлов, её версия, выпуск Deckhouse и фактическая версия Kubernetes.

3.2 Минимальные ресурсы для установки на одном сервере

Ресурс	Минимальное значение	Рекомендация для эксплуатации
Процессор	4 вычислительных ядра	От 8 ядер; увеличить при параллельной обработке документов.
Оперативная память	16 Гбайт	От 32 Гбайт; объём зависит от средств распознавания и моделей.
Дисковое пространство	50 Гбайт	От 200 Гбайт на отдельном надёжном томе с контролем заполнения.
Операционная система	Astra Linux Special Edition 1.7/1.8 или РЕД ОС 7.3/8.0, x86-64	Серверная установка с действующими обновлениями безопасности.
Сеть	Доступ пользователей к адресу программы	Ограничение доступа межсетевым экраном; защищённое соединение.

Указанные значения являются исходным минимумом. Окончательный расчёт выполняется по числу пользователей, объёму документов, скорости получения результата, количеству одновременных заданий, выбранным моделям и требуемому сроку хранения журналов.

3.3 Требования к дискам и времени

- размещать постоянные данные на отказоустойчивых томах;
- не хранить единственную копию на системном разделе;
- обеспечить запас свободного места не менее 20 процентов и оповещение при достижении 70, 80 и 90 процентов заполнения;
- синхронизировать системное время всех узлов с доверенным внутренним источником времени;
- запретить использование сетевой файловой системы без подтверждённой поддержки блокировок и требуемой производительности базы данных.

3.4 Матрица совместимости кластерной установки

Составная часть	Поддерживаемое условие	Что фиксируется в карточке установки
Операционная система узлов	Astra Linux Special Edition 1.7/1.8 либо РЕД ОС 7.3/8.0.	Полное обозначение ОС, корректирующее обновление, архитектура, версия ядра и дата установки обновлений безопасности.
Архитектура процессора	x86-64 для описанной в руководстве поставки.	Вывод команды <code>dpkg --print-architecture</code> и архитектура каждого образа. Иная архитектура допускается только при наличии отдельного комплекта поставки.

Составная часть	Поддерживаемое условие	Что фиксируется в карточке установки
Система управления кластером	Kubernetes поддерживаемой версии либо Deckhouse Kubernetes Platform поддерживаемого выпуска.	Версия средства управления кластером; для Deckhouse — версия платформы и фактическая версия Kubernetes.
Средство запуска контейнеров	Средство, поддерживаемое установленной кластерной платформой.	Наименование и версия. В Deckhouse не заменяется вручную в обход порядка сопровождения платформы.
Сетевое средство кластера	Поддерживает сетевые правила, разрешение служебных имён и выбранный входной контроллер.	Наименование, версия, диапазоны адресов, размер пакета и входной класс.
Постоянные тома	Класс томов обеспечивает требуемые режимы доступа, производительность, увеличение и, при необходимости, снимки.	Наименование класса, поставщик, параметры избыточности, режим привязки, возможность снимка и увеличения.

Фактическое сочетание версий операционной системы, Kubernetes и Deckhouse проверяется по действующим матрицам поддержки и записывается в карточку установки. Изменение любого элемента сочетания является изменением конфигурации и требует проверки по разделу 11.

3.5 Расчёт ресурсов кластерной установки

Минимальные требования для установки на одном сервере нельзя применять для кластера. Расчёт выполняется отдельно для прикладных служб и каждого хранилища. Значения из файлов поставки являются начальными и не подтверждают достаточность для промышленной нагрузки.

Исходное значение	Как определить	На что влияет
Пользователи и одновременные запросы	Максимум зарегистрированных, одновременно работающих и выполняющих поиск пользователей.	Число экземпляров прикладной службы, процессор, память, число соединений базы данных.
Поступление документов	Количество и общий объём за час и сутки; доля изображений и отсканированных страниц.	Число обработчиков, память, временное место и длительность очереди.
Объём исходных файлов	Текущий объём плюс прогноз прироста на срок эксплуатации.	Объектное хранилище, сеть и резервные копии.
Объём поисковых данных	Измерение на контрольной загрузке не менее 5–10 процентов ожидаемого массива.	Тома поискового хранилища, память и время повторного построения.
Журналы и аудит	Среднесуточный прирост, срок хранения и пиковая частота событий.	Отдельные тома и внешнее средство сбора журналов.
Резервные копии	Полные копии, изменения, число поколений и место для пробного восстановления.	Внешняя ёмкость, пропускная способность и длительность технологического окна.

Расчётная ёмкость каждого хранилища должна включать полезные данные, служебные данные выбранного средства (запас не менее 20 процентов), объём на перестроение либо слияние данных и резерв на период до расширения. Результат контрольной нагрузки, измеренные задержки и максимальная длина очереди прикладываются к акту ввода в эксплуатацию.

3.6 Уровни готовности и отказоустойчивости

Уровень	Признаки	Допустимое заявление
Работоспособная кластерная установка	Службы запущены в Kubernetes; постоянные данные могут храниться в одном экземпляре.	Подтверждена работоспособность в кластере. Непрерывность при отказе узла не подтверждена.
Установка с избыточными прикладными службами	Веб-служба и обработчики имеют несколько экземпляров на разных узлах; хранилища могут оставаться одиночными.	Подтверждено продолжение обработки при отказе одного прикладного экземпляра. Отказ хранилища остаётся критическим.
Отказоустойчивая установка	Все критические данные имеют согласованную многосоставную схему или внешние отказоустойчивые службы; экземпляры распределены по независимым узлам или зонам; проверено переключение.	Допустимое время простоя и потери данных подтверждены тестированием по проектной методике.

В проверенной конфигурации файлов кластерной установки отдельные хранилища могут по умолчанию создаваться в одном экземпляре. Поэтому установка значений по умолчанию не должна называться отказоустойчивой. Для такого требования применяются внешние отказоустойчивые службы, либо утверждённые многосоставные схемы PostgreSQL, объектного, поискового и временного хранилищ, поддерживаемые эксплуатационной службой.

4. ПОДГОТОВКА К УСТАНОВКЕ

4.1 Исходные данные

Сведение	Что подготовить
Адрес программы	Полное доменное имя и адреса узлов.
Свидетельство защищённого соединения	Свидетельство и закрытый ключ от доверенного удостоверяющего центра.
Хранилище образов	Адрес внутреннего хранилища, учётные данные только на чтение.
Постоянные тома	Классы и размеры томов для базы данных, файлов и поискового хранилища.
Почта	Адрес почтового узла и служебный отправитель — если применяются приглашения и уведомления.
Модели	Адреса служб моделей, их наименования, ограничения и служебные ключи.

Сведение	Что подготовить
Резервное копирование	Место хранения, расписание, срок хранения и ответственные лица.
Наблюдение	Средство сбора журналов, показателей состояния и оповещений.

4.2 Сетевое разграничение

Из пользовательской сети должен быть доступен только входной адрес веб-службы по защищённому протоколу. Порты базы данных, поискового, объектного и временного хранилищ не должны публиковаться во внешние сети. Административный доступ к узлам разрешается только из выделенной сети управления.

Направление	Разрешение
Пользователь → входной адрес программы	Разрешить только защищённый веб-доступ.
Прикладная служба → база данных	Разрешить внутри служебной сети.
Прикладная служба и обработчики → объектное, поисковое и временное хранилища	Разрешить внутри служебной сети.
Прикладная служба → службы моделей	Разрешить только к согласованным адресам.
Службы → средство сбора журналов и времени	Разрешить исходящие соединения к утверждённым адресам.
Внешняя сеть → внутренние хранилища	Запретить.

4.3 Подготовка узла для установки на одном сервере

1. Установить поддерживаемое средство управления контейнерами и средство совместного запуска контейнеров.
2. Создать отдельную служебную учётную запись без возможности обычного входа пользователей.
3. Создать каталог установки и каталог резервных копий с правами только для администратора.
4. Проверить системный параметр количества отображений виртуальной памяти.
5. Настроить межсетевой экран, синхронизацию времени, сбор системных журналов и контроль свободного места.

```
sysctl vm.max_map_count
```

```
sudo sysctl -w vm.max_map_count=262144
```

Постоянное значение следует закрепить в системной настройке операционной системы в соответствии с её эксплуатационной документацией.

4.4 Подготовка узлов Astra Linux Special Edition 1.7 и 1.8

Проверка готовности узла Astra Linux

Элемент процедуры	Содержание
Путь	Командная строка каждого будущего узла кластера.
Кто выполняет	Системный администратор операционной системы. Получены утверждённые обозначения выпуска, ядра, режима защиты, сетевые адреса, внутренние хранилища пакетов и правила обновления.
Ожидаемый результат	Все узлы имеют однородную, зафиксированную и допустимую конфигурацию операционной системы, готовы к включению в кластер.

Порядок выполнения:

1. На каждом узле проверить полное обозначение операционной системы, версию ядра и архитектуру. Для описанной поставки требуется x86-64; смешение архитектур в одной группе узлов не допускается.
2. Установить утверждённое очередное обновление Astra Linux и обновления безопасности. Фактические версии записать в карточку установки.
3. Проверить, что системное время синхронизируется с доверенным источником, имя узла уникально, прямое и обратное разрешение имён дают ожидаемые адреса.
4. Проверить файловые системы системных и прикладных разделов. Для данных, на которые распространяются механизмы мандатного разграничения, не применять файловую систему vfat; использовать согласованный поддерживаемый вариант, например ext4 или xfs.
5. Проверить свободное место, число ядер, память и системный параметр `vm.max_map_count`. Изменять параметр только через утверждённый файл системных настроек с регистрацией изменения.
6. Проверить доверие к внутреннему удостоверяющему центру, доступность внутреннего хранилища образов и пакетов, а также отсутствие прямого обращения к неразрешённым внешним узлам.
7. Проверить действующие механизмы мандатного разграничения и замкнутой программной среды. Не отключать их для ускорения установки. Необходимое исключение оформляется отдельным проектным решением и проверяется администратором безопасности.
8. Если на Astra Linux 1.7 для установки на одном сервере применяется пакет `docker.io`, использовать выпуск ОС не ниже очередного обновления 1.7.3 и проверить поддержку версии пакета по документации Astra Linux.
9. Для Astra Linux 1.8 использовать основное поддерживаемое ядро данного выпуска и не требовать отсутствующего отдельного усиленного ядра; соответствие режима защиты подтверждать средствами самой ОС.

Проверка результата:

- `cat /etc/os-release` содержит ожидаемый выпуск;

- `uname -r` совпадает с утверждённой версией ядра;
- `dpkg --print-architecture` возвращает `amd64`;
- `timedatectl` показывает синхронизацию;
- имена узлов разрешаются верно;
- `vm.max_map_count` не ниже значения, необходимого выбранному поисковому хранилищу;
- защитные механизмы не были самовольно отключены.

Отмена или возврат:

- Если узел не соответствует матрице, не включать его в кластер; вернуть в группу подготовки, исправить выпуск или настройки и повторить все проверки.

Особые указания:

- Поддержка Astra Linux 1.7 и 1.8 относится к кластерной конфигурации Semantix при соблюдении раздела 3.4.
- Для каждого узла сохранить вывод проверок без паролей и ключей в приложении к протоколу установки.

```
cat /etc/os-release
uname -r
dpkg --print-architecture
nproc && free -h && df -h
timedatectl status
sysctl vm.max_map_count
findmnt -o TARGET,FSTYPE,OPTIONS
```

4.5 Подготовка узлов РЕД ОС 7.3 и 8.0

Проверка готовности узла РЕД ОС

Элемент процедуры	Содержание
Путь	Командная строка каждого сервера или будущего узла кластера.
Кто выполняет	Системный администратор операционной системы. Получены утверждённые версии РЕД ОС и ядра, сетевые адреса, внутренние репозитории пакетов и правила обновления.
Ожидаемый результат	Серверы и узлы имеют однородную, зафиксированную и поддерживаемую конфигурацию РЕД ОС; проверки завершены без ошибок.

Порядок выполнения:

1. На каждом узле проверить полное обозначение РЕД ОС, корректирующее обновление, версию ядра и архитектуру. Для поставки Semantix требуется x86-64.
2. Установить поддерживаемое корректирующее обновление РЕД ОС и обновления безопасности. Фактические версии записать в карточку установки.
3. Проверить уникальность имени узла, прямое и обратное разрешение имён, синхронизацию времени и доверие к внутреннему удостоверяющему центру.

4. Проверить доступность утверждённых внутренних хранилищ пакетов и программных образов. В изолированной среде внешние хранилища не использовать.
5. Проверить число вычислительных ядер, оперативную память, свободное место, файловые системы и значение `vm.max_map_count`.
6. Для установки на одном сервере установить средство управления контейнерами из поддерживаемого хранилища РЕД ОС, запустить службу и проверить средство совместного запуска контейнеров.
7. Для кластерного размещения не устанавливать средство запуска контейнеров вручную, если им управляет Kubernetes или Deckhouse Kubernetes Platform.
8. Настроить межсетевой экран, системный аудит, сбор журналов и запрет автоматического обновления компонентов, способного вызвать незапланированный перезапуск узла.

Проверка результата:

- `cat /etc/os-release` содержит РЕД ОС 7.3 либо 8.0;
- `uname -m` возвращает `x86_64`;
- `timedatectl` показывает синхронизацию времени;
- `vm.max_map_count` не ниже значения, необходимого поисковому хранилищу;
- для установки на одном сервере `docker version` и `docker compose version` завершаются без ошибки;
- защитные механизмы и системный аудит включены.

Команды проверки:

```
cat /etc/os-release
uname -r && uname -m
rpm --eval '%{_arch}'
nproc && free -h && df -h
timedatectl status
sysctl vm.max_map_count
findmnt -o TARGET,FSTYPE,OPTIONS
systemctl status docker
docker version
docker compose version
```

4.6 Подготовка Deckhouse Kubernetes Platform

Проверка готовности Deckhouse Kubernetes Platform

Элемент процедуры	Содержание
Путь	Командная строка администратора кластера Deckhouse.
Кто выполняет	Администратор платформы. Кластер Deckhouse уже создан штатным способом; узлы подготовлены по 4.4 или 4.5; известна утверждённая версия Deckhouse.
Ожидаемый результат	Deckhouse предоставляет исправный кластер Kubernetes, классы хранения и входа, необходимые для установки Semantix.

Порядок выполнения:

1. Проверить, что подключение командной строки указывает на требуемый промышленный кластер, а не на тестовую среду.
2. Зафиксировать версию Deckhouse и фактическую версию Kubernetes. Сопоставить обе версии с матрицей совместимости раздела 3.4 и официальной матрицей поддерживаемых операционных систем Deckhouse.
3. Проверить готовность всех узлов и отсутствие давления по памяти, диску и числу процессов. Узлы с состоянием, отличным от Ready, до установки Semantix не использовать.
4. Проверить состояние модулей Deckhouse. Модули сети, постоянных томов, входного контроллера, выпуска свидетельств и наблюдения, используемые проектом, должны быть работоспособны.
5. Получить перечень классов постоянных томов, входных классов и, если нужны снимки, классов снимков. Не подставлять в параметры Semantix имя класса по памяти — скопировать фактическое имя из вывода.
6. Проверить загрузку контрольного образа из внутреннего хранилища на каждой группе рабочих узлов.
7. Проверить сетевые правила организации, размер сетевого пакета, разрешение служебных имён и доступ к внутренним службам времени, моделей, почты и резервного копирования.
8. Определить метки и ограничения узлов для прикладных служб, обработчиков и хранилищ. Если используются выделенные узлы, заранее оформить допускаемые размещения и запреты.

Проверка результата:

- контекст и адрес кластера зафиксированы;
- все требуемые узлы готовы;
- используемые модули Deckhouse работоспособны;
- классы томов и входа существуют;
- контрольный образ загружается;
- версии входят в утверждённую матрицу.

Отмена или возврат:

- При несовместимой версии Semantix не устанавливать. Обновление или возврат Deckhouse выполняется только по документации платформы и отдельному плану изменения.

Особые указания:

- В кластере Deckhouse не устанавливать и не заменять вручную средство запуска контейнеров, сетевые и дисковые модули в обход управления платформы.
- Имена пространств, модулей и классов зависят от конфигурации кластера; в документе установки фиксируются фактические значения.

```
kubectl config current-context
kubectl version
kubectl get nodes -o wide
kubectl get moduleconfig
kubectl get storageclass
kubectl get ingressclass
kubectl get volumesnapshotclass
```

4.7 Подготовка изолированной среды

1. Составить полный перечень образов Semantix и системных образов кластера с неизменяемыми версиями и контрольными суммами.
2. Перенести образы во внутреннее хранилище и проверить их считывание с каждой группы узлов.
3. Подготовить внутренние хранилища пакетов выбранной операционной системы. Пакеты разных операционных систем и основных версий не смешивать.
4. Перенести пакет кластерной установки, вспомогательные средства, файлы моделей и словари распознавания, если они требуются.
5. Настроить внутренние службы доменных имён, времени, удостоверяющего центра, почты, сбора журналов и резервного копирования.
6. Запретить неучтённые исходящие соединения и провести установку при включённом запрете, чтобы выявить скрытые внешние зависимости.
7. Сформировать ведомость переноса: источник, версия, контрольная сумма, дата проверки и ответственный.

Перед включением строгого автономного режима следует протестировать обработку контрольного документа при полностью отключённом внешнем сетевом доступе. Тест считается успешным, если документ загружен, обработан и доступен в поиске, а в журналах нет обращений к внешним ресурсам. Только после этого автономный режим можно вводить в промышленную эксплуатацию. Такая проверка заранее выявляет отсутствующие локальные модели, словари и другие зависимости.

5. УСТАНОВКА ПРОГРАММЫ

5.1 Общие правила

- использовать только утверждённый комплект поставки и зафиксированные версии образов;
- проверить контрольные суммы комплекта до установки;
- не сохранять пароли и ключи в репозитории исходного кода, истории команд и открытых файлах настроек;
- первую установку выполнить в тестовой среде, затем повторить по утверждённому протоколу в промышленной среде;

- зафиксировать дату, версию, перечень образов, значения контрольных сумм и исполнителя.

5.2 Установка на одном сервере

Ниже приведён полный порядок установки на подготовленном узле. Команды выполняются из каталога комплекта поставки. Значения в угловых скобках заменяются фактическими значениями без самих скобок.

5.2.1 Проверка узла перед установкой

1. Войти на узел под отдельной административной учётной записью и перейти в каталог комплекта поставки.
2. Проверить выпуск операционной системы, число вычислительных ядер, объём памяти и свободное место.
3. Проверить наличие средств управления контейнерами и совместного запуска контейнеров.
4. Проверить системный параметр `vm.max_map_count`. Значение должно быть не меньше 262144.
5. Проверить, что порты 80 и 443 не заняты другой службой. Внутренние порты хранилищ не должны прослушиваться на внешнем сетевом интерфейсе.
6. Проверить разрешение полного доменного имени в адрес узла и синхронизацию времени.

```
cat /etc/os-release
nproc
free -h
df -h
docker version
docker compose version
sysctl vm.max_map_count
ss -lntup | grep -E ":(80|443) "
getent hosts <полное_доменное_имя>
timedatectl status
```

Проверка	Критерий допуска
Операционная система	Поддерживаемый 64-разрядный выпуск Linux; обновления безопасности установлены.
Контейнеры	Средство управления контейнерами соответствует утверждённому комплекту поставки; служба запущена.
Совместный запуск	Поддерживается команда <code>docker compose</code> ; старая отдельная команда не используется.
Память и диск	Не ниже требований раздела 3; свободно не менее 20 процентов.
Системный параметр	<code>vm.max_map_count</code> не меньше 262144.
Имя и время	Имя разрешается правильно; расхождение времени не превышает допуска организации.

5.2.2 Подготовка рабочих параметров

Перед первым запуском создать рабочую копию файла .env и заменить все стандартные и демонстрационные пароли. Значения не следует вводить прямо в историю команд; предпочтительно подготовить файл в защищённом редакторе с правами доступа 600.

```
cd <каталог_установки>/docker
cp .env .env.initial
chmod 600 .env .env.initial
openssl rand -base64 32
```

Параметр	Что указать	Как проверить
DOC_ENGINE	Выбранное поисковое хранилище: infinity, elasticsearch либо opensearch. Для первой установки использовать вариант, утверждённый в проектном решении.	Значение совпадает с включённым составом контейнеров.
POSTGRES_USER	Отдельное имя пользователя прикладной базы данных.	Не является учётной записью администратора операционной системы.
POSTGRES_DBNAME	Имя прикладной базы данных, например semantix.	Содержит только допустимые для базы данных символы.
POSTGRES_PASSWORD	Случайный пароль не короче 24 знаков.	Не совпадает с другими паролями и не содержит заводского значения.
MINIO_USER	Отдельное имя пользователя объектного хранилища.	Совпадает с параметром пользователя в шаблоне служебной настройки.
MINIO_PASSWORD	Случайный пароль не короче 24 знаков.	Совпадает с параметром пароля в шаблоне служебной настройки.
REDIS_PASSWORD	Случайный пароль временного хранилища.	Не пустой и не совпадает с другими паролями.
TIMEZONE	Europe/Moscow либо иной утверждённый часовой пояс.	Совпадает с часовым поясом журналов организации.
REGISTER_ENABLED	0 для закрытой промышленной установки; 1 только при разрешённой самостоятельной регистрации.	После запуска страница регистрации соответствует принятому решению.
MAX_CONTENT_LENGTH	Предельный размер одного загружаемого файла в байтах.	Значение согласовано с пределом входной веб-службы.
DOC_BULK_SIZE	Начальное значение 4; повышать только после измерения памяти.	При обработке нет завершений из-за нехватки памяти.
EMBEDDING_BATCH_SIZE	Начальное значение 16; уменьшить при нехватке памяти модели.	Контрольный документ обрабатывается устойчиво.

После изменения файла проверить, что в нём не остались демонстрационные значения паролей, адресов и имён образов. Значения секретов в отчёт об установке не включать.

```
grep -E
"^(DOC_ENGINE|POSTGRES_USER|POSTGRES_DBNAME|TIMEZONE|REGISTER_ENABLED|DOC_BULK_SIZE|EMBEDDING_BATCH_SIZE)=" .env
```

5.2.3 Настройка адреса и защищённого соединения

1. Получить свидетельство защищённого соединения и закрытый ключ для полного доменного имени программы.
2. Поместить их в каталог, указанный в настройке входной веб-службы. Закрытый ключ должен читаться только служебной учётной записью.
3. В файле настройки входной службы указать имя узла, пути к свидетельству и ключу, предельный размер тела запроса и время ожидания длительного ответа.
4. Запретить публикацию портов базы данных, поискового, объектного и временного хранилищ на внешнем сетевом интерфейсе. Если комплект поставки публикует их для отладки, удалить соответствующие внешние сопоставления портов.
5. Проверить настройку входной службы до запуска.

```
chmod 600 <путь_к_закрытому_ключу>
```

```
openssl x509 -in <путь_к_свидетельству> -noout -subject -issuer -dates
```

В промышленной среде открытый доступ по незащищённому протоколу должен перенаправляться на защищённый либо быть полностью запрещён.

5.2.4 Запуск и последовательная проверка контейнеров

1. Распаковать утверждённый комплект поставки в каталог установки.
2. Перейти в каталог с описанием состава контейнеров.
3. Проверить рабочий файл .env и права доступа к нему.
4. Задать уникальные стойкие пароли для базы данных, объектного и временного хранилищ.
5. Задать адреса моделей, почтовой службы, службы учётных записей и внешний адрес программы.
6. Запустить службы в фоновом режиме.
7. Проверить состояние всех контейнеров и журналы прикладной службы.
8. Открыть внешний адрес программы и выполнить первичный вход.

```
cd <каталог_установки>/docker
```

```
chmod 600 .env
```

```
docker compose -f docker-compose.yml pull
```

```
docker compose -f docker-compose.yml up -d
```

```
docker compose -f docker-compose.yml ps
```

```
docker compose -f docker-compose.yml logs --tail=200
```

9. После запуска выполнить `docker compose ps` и убедиться, что нет контейнеров в состоянии завершения или циклического перезапуска.
10. Выполнить просмотр последних 200 строк общего журнала. Допустимы сообщения первоначального создания баз данных; повторяющиеся ошибки соединения недопустимы.
11. Подождать не менее двух минут и повторно проверить число перезапусков.

12. Проверить доступность прикладной службы с самого узла, затем с рабочей станции администратора.

13. Перезагрузить страницу входа и убедиться, что ошибки веб-службы отсутствуют.

```
docker compose -f docker-compose.yml ps --all
```

```
docker compose -f docker-compose.yml logs --tail=200 --no-color
```

```
curl -k -I https://<полное_доменное_имя>/
```

Наблюдение	Решение
Контейнер базы данных не готов	Не запускать повторную установку. Проверить том, пароль, права каталога и журнал базы данных.
Прикладная служба ожидает базу данных	Сопоставить POSTGRES_HOST, POSTGRES_PORT, POSTGRES_USER, POSTGRES_DBNAME и POSTGRES_PASSWORD между файлами.
Ошибка объектного хранилища	Сопоставить MINIO_USER, MINIO_PASSWORD и внутреннее имя службы; проверить постоянный том.
Ошибка временного хранилища	Проверить REDIS_PASSWORD и внутреннее имя службы.
Страница открывается, но вход не работает	Проверить службу учётных записей, точность внешнего адреса и синхронизацию времени.

5.3 Кластерная установка

Кластерная установка выполняется в стандартном Kubernetes либо в Deckhouse Kubernetes Platform на узлах одной из операционных систем раздела 3.1. В командах используется пространство имён semantix. Иное согласованное имя необходимо применять одинаково во всех командах и файлах установки.

До начала работ выбрать ровно один вариант кластерной платформы. Для Deckhouse не устанавливать поверх платформы собственные сетевые, дисковые или входные средства, если их функции уже предоставляются модулями Deckhouse. Для стандартного Kubernetes ответственность за совместимость этих средств лежит на эксплуатирующей организации.

5.3.1 Проверка кластера

1. Проверить доступ к требуемому кластеру и текущий контекст командной строки.
2. Зафиксировать версию кластерной платформы и Kubernetes. Для Deckhouse выполнить процедуру 4.6, для стандартного Kubernetes — приложить сведения о средстве создания и сопровождения кластера.
3. Проверить состояние узлов, операционную систему, архитектуру и доступные ресурсы. Узлы Astra Linux должны пройти процедуру 4.4, узлы РЕД ОС — процедуру 4.5.
4. Проверить наличие входного контроллера, класса постоянных томов и средства выпуска свидетельств защищённого соединения, если оно применяется.

5. Проверить класс снимков томов, если резервное копирование будет использовать снимки. Отсутствие класса снимков должно быть компенсировано прикладным копированием каждой службы данных.
6. Проверить возможность загрузки образов из внутреннего хранилища с каждого рабочего узла.
7. Проверить, что полные доменные имена программы и службы учётных записей указывают на входной адрес кластера.
8. Проверить правила сети между пространствами имён и наличие исходящего доступа только к утверждённым службам.
9. Проверить достаточность ресурсов с учётом запросов всех экземпляров и запаса на отказ одного рабочего узла.

```
kubectl config current-context
```

```
kubectl get nodes -o wide
```

```
kubectl get storageclass
```

```
kubectl get ingressclass
```

```
kubectl get volumesnapshotclass
```

```
kubectl get namespace semantix
```

Критерий допуска	Требуемый результат
Версии	Сочетание операционной системы и Kubernetes и при наличии Deckhouse закреплено в утверждённой матрице.
Узлы	Все предназначенные узлы готовы; архитектура amd64; нет давления по памяти и диску; время синхронизировано.
Хранение	Класс томов существует, поддерживает нужный режим доступа и имеет подтверждённую производительность.
Вход	Входной класс существует; адреса разрешаются; свидетельства подготовлены.
Образы	Каждый неизменяемый образ выпуска доступен из внутреннего хранилища; контрольные суммы совпадают.
Ёмкость	После размещения всех запросов ресурсов сохраняется запас для переноса экземпляров при отказе одного узла.

5.3.2 Создание пространства имён и доступа к образам

1. Создать пространство имён `semantix`, если оно отсутствует.
2. Подготовить защищённый файл доступа к внутреннему хранилищу образов. Учётная запись должна иметь только право чтения и область действия только для требуемого раздела хранилища.
3. Создать закрытый объект из защищённого файла. Не вводить действующий пароль как буквальный параметр команды и не сохранять его в журнале команд.
4. Проверить наличие закрытого объекта и отсутствие его содержимого в выводе команд и отчёте установки.

5. Удалить временный файл с рабочей станции утверждённым способом либо оставить только в защищённом хранилище секретов.
6. В рабочем файле `values-production.yaml` указать имя этого закрытого объекта в `imagePullSecrets`.
7. Ограничить создание и чтение закрытых объектов выделенными служебными учётными записями и проверить журнал действий кластера.

```
kubectl create namespace semantix
```

```
umask 077
```

```
kubectl -n semantix create secret generic semantix-registry-pull \
```

```
--type=kubernetes.io/dockerconfigjson \
```

```
--from-file=.dockerconfigjson=<защищённый_файл_доступа>
```

```
kubectl -n semantix get secret semantix-registry-pull
```

Не копировать готовое содержимое закрытого объекта из исходного файла параметров. Для каждой установки создаётся новый доступ; обнаруженные в исходниках действующие ключи подлежат немедленной замене.

5.3.3 Заполнение `values-production.yaml`

Раздел	Обязательные действия администратора
<code>imagePullSecrets</code>	Указать имя созданного закрытого объекта доступа к образам.
<code>dockerRegistrySecret</code>	Для промышленной среды предпочтительно <code>create: false</code> и заранее созданный закрытый объект; не хранить закодированные учётные данные в файле.
<code>env.DOC_ENGINE</code>	Выбрать одно поисковое хранилище. Остальные не должны запускаться.
<code>env.POSTGRES_*</code>	Задать отдельные имя базы, пользователя, пароль и допустимое число соединений.
<code>env.MINIO_*</code> и <code>env.REDIS_PASSWORD</code>	Заменить все значения; не использовать одинаковые пароли.
<code>env.DEFAULT_ADMIN_EMAIL</code>	Указать служебный адрес первого главного администратора.
<code>env.DEFAULT_ADMIN_PASSWORD</code>	Оставить пустым для однократного безопасного создания либо задать через отдельный закрытый файл, не помещаемый в систему контроля версий.
<code>env.TIMEZONE</code>	Указать <code>Europe/Moscow</code> или утверждённый часовой пояс.
<code>backend, taskExecutor, canvasExecutor</code>	Задать число экземпляров, запросы и пределы процессора и памяти.
<code>storage.className</code> и <code>capacity</code>	Указать существующий класс и рассчитанные размеры постоянных томов.
<code>ingress.hosts</code> и <code>ingress.tls</code>	Указать внешнее имя программы и закрытый объект со свидетельством.
<code>zitadel.config</code> и <code>zitadel.ingress</code>	Указать отдельное имя службы учётных записей, защищённый порт и свидетельство.
<code>audit.retentionDays</code>	Указать утверждённый срок хранения журнала; значение 0 означает бессрочное хранение и требует расчёта диска.

Раздел	Обязательные действия администратора
modelCache	Указать постоянный том для моделей. Строгий автономный режим включать только после заполнения тома.

Рабочий файл `values-production.yaml` должен содержать только несекретные значения. Пароли, закрытые ключи, ключи программного доступа и данные доступа к хранилищу образов помещаются в закрытые объекты из внешнего защищённого хранилища. Если пакет текущего выпуска не поддерживает ссылки на заранее созданные закрытые объекты для всех параметров, файл с секретами создаётся только на защищённой рабочей станции с правами 600, используется однократно и не помещается в систему контроля версий или архив обычных параметров.

После заполнения проверить, что в рабочем файле отсутствуют стандартные пароли, действующие ключи доступа, публичные демонстрационные адреса и тег `latest`. Для каждого образа должен быть указан неизменяемый тег выпуска, а при строгих требованиях — контрольная сумма образа. Наличие кодирования `base64` не считается защитой секрета.

```
chmod 600 values-production.yaml
grep -nE 'latest|changeme' values-production.yaml
```

Отдельно проверить число экземпляров хранилищ. Значение `replicaCount: 2` у прикладной службы не делает одиночные PostgreSQL, объектное, поисковое или временное хранилище отказоустойчивыми. Проектное решение должно для каждого из них выбрать внешнюю отказоустойчивую службу, поддерживаемую многосоставную схему либо явно принять время восстановления из резервной копии.

5.3.4 Предварительное построение и установка

1. Создать отдельное пространство имён.
2. Создать закрытые объекты с паролями, ключами и свидетельствами защищённого соединения.
3. Проверить классы постоянных томов и возможность увеличения.
4. Заполнить файл параметров установки: адреса образов, размеры томов, число экземпляров, ограничения ресурсов и внешний адрес.
5. Проверить сформированные описания ресурсов без применения.
6. Установить программный комплект.
7. Дождаться готовности всех экземпляров служб.
8. Проверить входной адрес, журналы, постоянные тома и распределение экземпляров по узлам.

```
kubectl create namespace semantix
```

```
umask 077
```

```
helm template semantix <каталог_пакета> -n semantix -f values-production.yaml > rendered.yaml
```

```
helm upgrade --install semantix <каталог_пакета> -n semantix -f values-production.yaml --wait --timeout 20m
```

```
kubectl -n semantix get pods,svc,pvc
```

```
kubectl -n semantix get events --sort-by=.metadata.creationTimestamp
```

Для промышленной установки следует задать запросы и ограничения ресурсов, проверки готовности и работоспособности, распределение экземпляров по разным узлам или зонам, допустимое число одновременно недоступных экземпляров, запрет запуска от привилегированного пользователя, неизменяемую корневую файловую систему там, где это допускается, и сетевые правила между службами.

1. До применения просмотреть `rendered.yaml` и убедиться, что в нём нет открытых паролей и ошибочных внешних служб.
2. Выполнить проверку установки с параметром `--dry-run`.
3. Применить пакет с ожиданием готовности.
4. Проверить все экземпляры служб. Особое внимание уделить службе учётных записей, прикладной базе, поисковому и объектному хранилищам, обработчикам и журналу действий.
5. Проверить постоянные тома: все должны быть связаны; случайно созданные тома неправильного класса до загрузки данных удалить и создать заново по согласованной заявке.
6. Проверить входные правила и соответствие их адресов свидетельствам защищённого соединения.
7. Проверить события пространства имён от старых к новым.
8. Проверить фактическое распределение нескольких экземпляров одной службы по разным узлам. Если они размещены на одном узле, настроить правила разнесения и повторить проверку.
9. Проверить, что файл `rendered.yaml` имеет права 600, не передаётся в заявку без очистки и уничтожается после оформления обезличенного протокола.

```
helm upgrade --install semantix <каталог_пакета> -n semantix -f values-production.yaml --dry-run
```

```
kubectl -n semantix get pods -o wide
```

```
kubectl -n semantix get pvc
```

```
kubectl -n semantix get ingress
```

```
kubectl -n semantix get events --sort-by=.metadata.creationTimestamp
```

5.3.5 Получение данных первого входа

Если пароль главного администратора создавался автоматически, получить его из закрытого объекта только на защищённой рабочей станции. Имя закрытого объекта формируется из имени установки: `<имя_установки>-env-config`.

```
kubectl -n semantix get secret <имя_установки>-env-config -o jsonpath='{.data.DEFAULT_ADMIN_EMAIL}' | base64 -d
```

```
kubectl -n semantix get secret <имя_установки>-env-config -o jsonpath='{.data.DEFAULT_ADMIN_PASSWORD}' | base64 -d
```

- не сохранять полученный пароль в протокол команд, снимок экрана или заявку;
- выполнить первый вход и заменить временный пароль, если способ входа это допускает;

- сохранить аварийные данные доступа в утверждённом защищённом хранилище;
- проверить, что повторное обновление пакета не изменяет созданный пароль и ключ сеанса.

5.3.6 Распределение служб и постоянных данных

Объект	Минимальная настройка для распределения	Как проверить
Веб-служба	Не менее двух экземпляров; разнесение по именам узлов; проверка готовности.	kubectl get pods -o wide показывает разные узлы; удаление одного экземпляра не прерывает контрольный запрос.
Обработчики задач	Не менее двух экземпляров; ограничение параллельности по реальным ресурсам; разнесение по узлам.	После вывода одного узла новые задания продолжают выполняться, зависшее задание обнаруживается и обрабатывается по регламенту.
PostgreSQL	Внешняя отказоустойчивая служба или утверждённая многосоставная схема с проверенным переключением.	Роль основного экземпляра меняется по тестированию; приложение восстанавливает соединения; потери данных укладываются в норматив.
Объектное хранилище	Данные распределены по нескольким независимым носителям или узлам; единственный постоянный том не используется как единственная копия.	При отказе одного носителя контрольный файл доступен и его контрольная сумма совпадает.
Поисковое хранилище	Многосоставная схема либо измеренное повторное построение из исходных файлов и базы.	Контрольный поиск доступен после отказа либо восстановлен за допустимое время.
Временное хранилище	Схема с переключением либо утверждённый порядок восстановления очередей и сеансов.	После тестирования новые задания принимаются; потерянные задания перечислены и повторены управляемо.
Постоянные тома	Избыточность предоставляется системой хранения; снимок не заменяет избыточность.	Документация класса хранения и тестирования отказа подтверждают требуемое поведение.

Правила разнесения, запреты размещения на неподходящих узлах и допустимое число одновременно недоступных экземпляров должны входить в пакет промышленной установки. Жёсткое требование разнесения применяют с учётом числа узлов: ошибочная настройка может оставить службу в ожидании при недостатке подходящих узлов.

5.3.7 Приёмочные испытания отказа узла

1. Согласовать технологическое окно, точный целевой узел, допустимое время простоя и критерий прекращения тестирования.

2. Создать и проверить резервную копию; убедиться, что на целевом узле нет единственного экземпляра данных без иной копии.
3. Зафиксировать размещение экземпляров, состояние томов, число незавершённых заданий и время начала.
4. Без удаления данных вывести один рабочий узел из обслуживания штатным способом кластерной платформы.
5. Проверить повторное размещение прикладных экземпляров, вход пользователя, контрольный поиск и постановку нового документа в обработку.
6. Проверить базу данных, объектное, поисковое и временное хранилища по критериям проектного решения.
7. Вернуть узел в работу, дождаться устойчивого состояния и проверить отсутствие потерянных или дублированных заданий.
8. Зафиксировать фактическое время прерывания, потерю данных, предупреждения, отклонения и решение о допустимости схемы.

Тестирование запрещено выполнять путём удаления постоянных томов, принудительного удаления объектов данных или выключения нескольких узлов без отдельной методики. Для Deckhouse вывод узла и возврат выполняются штатными средствами платформы, с учётом её текущей документации.

5.3.8 Размещение локальных моделей

Если Semantix обращается к внешней службе моделей, графические ускорители на узлах Semantix не требуются. Если локальная служба моделей включается в тот же кластер, она проектируется как отдельная нагрузка: выделяются совместимые с выбранной операционной системой узлы с графическими ускорителями, утверждённые драйверы и средство распределения устройств, отдельные метки и ограничения размещения, постоянный кэш моделей и расчёт электропитания, охлаждения и памяти устройств.

1. Проверить совместимость драйвера и ядра выбранной операционной системы на тестовом узле.
2. Запретить размещение обычных хранилищ на узлах моделей, если это следует из проектного решения.
3. Загрузить модели во внутренний кэш и сверить контрольные суммы.
4. Выполнить контрольный запрос при отключённом внешнем доступе.
5. Проверить поведение при занятости всех устройств: запрос должен ожидать или завершаться управляемой ошибкой, а не приводить к перезапуску прикладных служб.

5.4 Проверка после установки

Проверка	Ожидаемый результат
Матрица версий	В карточке установки указаны поддерживаемая операционная система, ядро, Kubernetes и при наличии Deckhouse; сочетание утверждено.
Состояние служб	Все обязательные службы работают и не перезапускаются циклически.
Веб-доступ	Открывается страница «Вход» на русском языке.
Защищённое соединение	Свидетельство действительно, имя узла совпадает, цепочка доверия полна.
Вход администратора	Открывается «Консоль администратора».
Раздел организаций	Раздел «Управление тенантами» открывается; создание организации выполняется по 6.4.
Загрузка документа	Файл загружается, обработка завершается состоянием «УСПЕШНО».
Поиск	По контрольному вопросу возвращается ожидаемый фрагмент.
Журнал действий	В журнале отражается тестовое событие входа; создание организации проверяется после выполнения 6.4.
Перезапуск	После управляемого перезапуска данные и настройки сохраняются.
Отказ узла	Если заявлена отказоустойчивость, тестирование по 5.3.7 пройдено; фактическое время простоя и потеря данных не превышают норматива.

Проверка считается завершённой только при наличии записи исполнителя, времени, фактического результата и ссылки на диагностические сведения при отклонении. Формулировка «проверено без замечаний» без измеримых результатов для приёмки не используется.

6. ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА

6.1 Создание главного администратора

Способ создания первой учётной записи определяется комплектом поставки и принятой службой управления учётными записями. Временный пароль должен быть заменён при первом входе. После проверки работы следует отключить саморегистрацию, если она не предусмотрена правилами организации, и сохранить аварийную учётную запись в защищённом хранилище секретов.

6.1.1 Первый вход главного администратора

Элемент процедуры	Содержание
Путь	Браузер → <a href="https://<полное_доменное_имя>/">https://<полное_доменное_имя>/ → «Войти».

Элемент процедуры	Содержание
Кто выполняет	Работник, назначенный главным администратором. Получены адрес и временные данные доступа по процедуре 5.3.5 либо из акта установки.
Ожидаемый результат	Главный администратор может открыть общесистемную консоль и список организаций.

Порядок выполнения:

1. Открыть программу только по полному защищённому адресу. Не продолжать работу при предупреждении браузера о свидетельстве.
2. На странице «Вход» указать служебный адрес электронной почты главного администратора.
3. Ввести временный пароль вручную либо из защищённого хранилища и нажать «Войти».
4. Если служба учётных записей требует сменить пароль, задать новый уникальный пароль и подтвердить его.
5. Открыть меню учётной записи и убедиться, что доступен пункт «Консоль администратора».
6. Открыть «Консоль администратора» и затем «Управление тенантами». Отсутствие сообщения «У вас нет доступа к этой странице» подтверждает полномочия.
7. Выйти из программы и повторно войти новым паролем.

Проверка результата:

- адрес в строке браузера совпадает с утверждённым;
- язык страницы установлен на русский;
- в журнале есть успешный вход;
- временный пароль больше не используется.

Особые указания:

- Не использовать первую главную учётную запись для повседневной работы с документами.
- Создать вторую аварийную административную учётную запись по правилам организации и хранить её отдельно.

6.1.2 Отключение самостоятельной регистрации

Элемент процедуры	Содержание
Путь	Файл .env для установки на одном сервере, либо env в values-production.yaml кластерной установки.
Кто выполняет	Системный администратор с доступом к файлам установки. Операция выполняется после создания необходимых администраторов.
Ожидаемый результат	Новые пользователи создаются только администратором либо принятой службой учётных записей.

Порядок выполнения:

1. Остановить приём изменений на время короткого технологического окна.
2. В варианте с одним сервером в файле .env установить REGISTER_ENABLED=0. В кластерном файле параметров установить равнозначное значение выпуска, если оно поддерживается поставкой.
3. Применить настройку перезапуском контейнеров либо обновлением пакетной установки.
4. Открыть страницу входа в отдельном закрытом окне браузера.
5. Убедиться, что самостоятельное создание учётной записи недоступно, а обычный вход работает.

Проверка результата:

- страница «Регистрация» отсутствует или отклоняет создание;
- существующие пользователи входят без ошибок;
- изменение зафиксировано в журнале работ.

Отмена или возврат:

- вернуть REGISTER_ENABLED=1 только по письменному решению владельца системы и повторно применить настройки.

6.2 Настройка русского языка

1. Войти в программу.
2. Открыть «Настройки пользователя».
3. В поле «Язык» выбрать «Русский».
4. Сохранить настройку.
5. Повторно открыть основные разделы и убедиться, что отображаются «База знаний», «Ассистенты», «Управление файлами», «Агент», «Поиск» и «Консоль администратора».

Шаг проверки	Ожидаемая подпись
Верхняя панель	«База знаний», «Ассистенты», «Управление файлами», «Агент», «Поиск».
Меню учётной записи	«Настройки пользователя», «Выйти».
Общие кнопки	«Создать», «Сохранить», «Удалить», «Назад», «Далее», «Заккрыть».
Управление организациями	«Управление тенантами», «Создать тенант», «Управление пользователями».
Обработка документа	«ОЖИДАЕТ», «ОБРАБАТЫВАЕТ», «ОТМЕНЕНО», «УСПЕШНО», «ОШИБКА».

Если отдельные подписи остаются на другом языке, записать адрес страницы, текст подписи и версию программы. До исправления в руководстве использовать русское функциональное название и, при необходимости, привести видимую подпись в кавычках, как элемент экранной формы.

6.3 Настройка моделей

В разделе настроек моделей администратор задаёт доступные организации службы формирования текста, смыслового представления, повторного упорядочивания (реранкер), распознавания речи и описания изображений. Для каждой службы указываются адрес, точное имя модели, служебный ключ, предельное время ожидания и допустимое число одновременных обращений.

- служебные ключи хранить только в закрытом хранилище секретов;
- не направлять документы во внешнюю службу без правового основания и утверждённой модели угроз;
- зафиксировать версию каждой модели; изменение модели смыслового представления после создания фрагментов требует повторной обработки базы знаний;
- проверить обработку русского текста, таблиц, изображений и сканированных документов на контрольном наборе.

6.3.1 Добавление поставщика моделей через экранную форму

Элемент процедуры	Содержание
Путь	Меню учётной записи → «Настройки пользователя» → «Провайдеры моделей» → «Добавить провайдера».
Кто выполняет	Администратор организации. Подготовлены базовый адрес службы, служебный ключ при необходимости, точное имя модели и её предельный размер контекста.
Ожидаемый результат	Модель доступна для выбора в системных настройках и соответствующих объектах.

Порядок выполнения:

1. Открыть «Настройки пользователя» и выбрать «Провайдеры моделей».
2. Нажать «Добавить провайдера». Если список пуст, можно нажать одноимённую кнопку в центре страницы.
3. На шаге «О провайдере» выбрать поставщика. Для собственной совместимой службы выбрать вариант совместимого программного интерфейса.
4. Нажать «Далее».
5. В поле «Базовый URL» указать полный адрес программного интерфейса службы. Адрес должен быть доступен из прикладного контейнера, а не только с рабочей станции.
6. В поле «API-Ключ» указать служебный ключ. Для локальной службы без проверки ключа оставить поле пустым только при изолированной сети и утверждённом решении.
7. В поле «Название модели» указать точное имя, которое возвращает служба моделей.

8. В поле «Тип модели» выбрать фактическое назначение: модель чата, смыслового представления, повторного упорядочивания (реранкер), преобразования речи либо изображения.
9. Указать «Макс. токенов» согласно настройке службы, а не рекламному пределу модели.
10. Нажать «Сохранить».
11. Нажать «Обновить» на странице поставщиков и убедиться, что добавленная карточка отображается.

Проверка результата:

- карточка поставщика отображается после обновления;
- имя и тип модели указаны правильно;
- контрольный короткий запрос завершается без ошибки доступа;
- ключ не отображается полностью после сохранения.

Отмена или возврат:

- открыть карточку поставщика, выбрать изменение или удаление модели; перед удалением убедиться, что модель не выбрана в существующих базах знаний и помощниках.

Особые указания:

- базовый адрес должен заканчиваться на путь, требуемый конкретной совместимой службой;
- для одной службы допускается добавить несколько моделей разных типов, но имена и назначения фиксируются отдельно.

6.3.2 Назначение моделей по умолчанию

Элемент процедуры	Содержание
Путь	«Настройки пользователя» → «Провайдеры моделей» → «Установить модели по умолчанию».
Кто выполняет	Администратор организации. Требуемые модели уже добавлены и проверены.
Ожидаемый результат	Новые базы знаний и фоновые задачи получают утверждённые модели по умолчанию.

Порядок выполнения:

1. Нажать «Установить модели по умолчанию».
2. В поле «Модель чата» выбрать основную модель формирования ответов.
3. В поле «Сервисная модель» выбрать отдельную экономичную модель для фоновых задач либо оставить использование основной модели.
4. В поле «Модель эмбединга» выбрать модель смыслового представления русского текста.
5. При наличии выбрать «Модель реранкинга» для повторного упорядочивания найденных фрагментов.

6. При обработке изображений выбрать модель описания изображений; при работе с аудио — модель распознавания речи.
7. Нажать «Сохранить».
8. Создать временную тестовую базу знаний и проверить, что новые значения подставляются автоматически.

Проверка результата:

- все обязательные поля заполнены;
- тестовая база получает ожидаемую модель смыслового представления;
- русский контрольный текст обрабатывается без искажения;
- изменение занесено в журнал работ.

Особые указания:

- Изменение значений по умолчанию не обязано менять уже созданные объекты.
- Модель смыслового представления существующей базы нельзя заменять после создания фрагментов без повторной обработки документов.

6.3.3 Проверка доступности модели с прикладного узла

Элемент процедуры	Содержание
Путь	Командная строка внутри прикладного контейнера или временного диагностического контейнера в служебной сети.
Кто выполняет	Системный администратор. Известен базовый адрес модели; служебный ключ передаётся через защищённую переменную и не выводится на экран.
Ожидаемый результат	Прикладная служба может обратиться к модели по настроенному адресу.

Порядок выполнения:

1. Проверить разрешение имени службы модели.
2. Проверить установление соединения на требуемый порт.
3. Выполнить предусмотренный поставщиком безопасный запрос списка моделей либо проверки состояния.
4. Сопоставить возвращённое имя модели со значением экранной формы.
5. Проверить время ответа и отсутствие ошибок свидетельства защищённого соединения.

Проверка результата:

- имя разрешается в правильный адрес;
- соединение устанавливается;
- служба возвращает ожидаемую модель;
- ключ не попал в журнал и историю команд.

6.4 Создание организации

6.4.1 Создание организации через экранную форму

Элемент процедуры	Содержание
Путь	Верхняя панель → «Консоль администратора» → «Управление тенантами» → «Создать тенант».
Кто выполняет	Главный администратор. Подготовлены уникальное наименование организации и адрес её ответственного администратора.
Ожидаемый результат	В таблице появилась новая организация; созданы её начальные настройки и корневая папка.

Порядок выполнения:

1. Войти под учётной записью главного администратора.
2. Открыть «Консоль администратора» и выбрать «Управление тенантами».
3. Проверить отсутствие организации с таким же полным наименованием.
4. В правой верхней части страницы нажать «Создать тенант».
5. В окне «Создать тенант» в поле «Введите название тенанта» ввести утверждённое наименование организации.
6. Нажать «Создать» один раз и дождаться сообщения «Тенант успешно создан».
7. Найти организацию в таблице и открыть «Управление пользователями».
8. Записать наименование и дату создания в карточку установки.

Проверка результата:

- организация присутствует в списке после обновления страницы;
- кнопка «Управление пользователями» открывает список участников;
- в журнале действий имеется событие создания организации.

Отмена или возврат:

- Если наименование введено ошибочно и данные ещё не загружались, удалить организацию по процедуре 7.5.1 и создать заново.

Особые указания:

- В экранной форме используется слово «тенант»; в руководстве ему соответствует термин «организация».

6.4.2 Переключение между организациями

Порядок выполнения:

1. Открыть меню учётной записи в верхней панели.
2. В списке рабочих пространств выбрать требуемую организацию.
3. Дождаться обновления страницы.
4. Проверить название активного рабочего пространства перед созданием базы знаний, загрузкой файла или настройкой подключения.

Проверка результата:

- отображаются ресурсы выбранной организации;

- в разделе «Команда» отображаются участники выбранной организации.
Администратор организации назначается по процедуре 7.1.1 или 7.1.2.

6.5 Активация лицензии

Лицензию активирует главный администратор. Для активации требуется токен, выданный Semantix. В зависимости от сетевого доступа применяется активация через интернет или автономная активация.

Перед началом:

- получить токен активации по официальному каналу поддержки support@semantix.pro;
- для активации через интернет разрешить защищённое соединение с <https://license.semantix.pro>;
- для автономной активации подготовить компьютер с доступом в интернет и разрешённый способ переноса файлов между контурами.

Активация через интернет:

1. Войти в Semantix под учётной записью главного администратора.
2. Открыть «Консоль администратора» и выбрать «Лицензия».
3. В поле «Токен активации» вставить полученный токен.
4. Нажать «Активировать» и дождаться сообщения «Лицензия активирована».
5. В блоке «Активированная лицензия» проверить редакцию, срок действия, доступные функции и лимиты.

Автономная активация:

1. На странице «Лицензия» вставить полученный токен в поле «Токен активации».
2. Нажать «Активировать офлайн» и сохранить файл `semantix-activation.smxreq`.
3. Перенести файл запроса на компьютер с доступом в интернет и открыть <https://license.semantix.pro/activate>.
4. Загрузить файл `.smxreq` и нажать «Активировать и скачать лицензию».
5. Сохранить полученный файл `.smxlic` и перенести его в контур Semantix.
6. В Semantix открыть «Консоль администратора» → «Лицензия», нажать «Загрузить файл лицензии» и выбрать файл `.smxlic`.
7. Дождаться сообщения «Лицензия установлена» и проверить сведения в блоке «Активированная лицензия».

Проверка результата:

- на странице «Лицензия» отображаются редакция, срок действия, функции и лимиты;
- рабочие функции Semantix доступны в пределах установленной лицензии;
- перезапуск сервера или контейнеров после активации не требуется.

Действия при ошибке:

- если центр лицензирования недоступен, повторить попытку позднее или выполнить автономную активацию; ранее установленная действующая лицензия при этом не изменяется;
- если токен отклонён, проверить правильность копирования и обратиться в поддержку; токен привязывается к установке, на которой был впервые активирован;
- если файл лицензии не принят, не редактировать его содержимое, повторно сформировать запрос и передать сведения об ошибке в поддержку.

Особые указания:

- файл .smxreq содержит токен активации; хранить и передавать его как пароль, а после завершения активации удалить временные копии;
- сведения об оборудовании в файл .smxreq не включаются;
- адрес центра лицензирования задан в программе и в интерфейсе администратора не изменяется.

7. УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ И ДОСТУПОМ

Полномочия назначаются в пределах выбранной организации. Перед добавлением участника главный администратор проверяет основание и требуемую роль.

Роль	Основные полномочия	Ограничения
Главный администратор	Создание и удаление организаций; просмотр пользователей; назначение пользователей организациям.	Назначается минимальному числу доверенных работников.
Владелец организации	Управление участниками и ресурсами организации; назначение администратора организации.	Не назначается обычной операцией добавления участника.
Администратор организации	Управление участниками и ресурсами своей организации.	Не управляет другими организациями и главным администратором.
Пользователь	Работа с разрешёнными базами знаний, файлами, помощниками и поиском.	Не выполняет общесистемные административные операции.
Приглашённый	Ожидание принятия приглашения в организацию.	До принятия приглашения полномочия ограничены.

7.1 Добавление пользователя

Форма поддерживает два варианта: включение уже существующей учётной записи и одновременное создание новой записи. Выбирать следует только вариант.

7.1.1 Включение существующего пользователя в организацию

Элемент процедуры	Содержание
Путь	«Консоль администратора» → «Управление тенантами» → нужная строка → «Управление пользователями» → «Добавить пользователя» → «Выбрать существующего».
Кто выполняет	Главный администратор. Пользователь уже существует в системе, но ещё не включён в выбранную организацию.
Ожидаемый результат	Существующая учётная запись получила доступ к выбранной организации.

Порядок выполнения:

1. Проверить название организации в исходном списке.
2. Нажать «Управление пользователями» в её строке.
3. Нажать «Добавить пользователя».
4. Выбрать вкладку «Выбрать существующего».
5. Открыть поле «Выберите пользователя...» и найти запись по полному адресу электронной почты. Сверить имя и фамилию.
6. В поле «Выбрать роль» выбрать «Пользователь» либо «Администратор тенанта».
7. Нажать «Добавить».
8. Дождаться сообщения об успешном добавлении и проверить строку пользователя.

Проверка результата:

- адрес и имя совпадают с заявкой;
- роль отображается верно;
- дата изменения соответствует текущей;
- пользователь видит рабочее пространство после повторного входа.

Отмена или возврат:

- Удалить участника из организации по процедуре 7.3. Учётная запись при наличии других организаций сохранится.

7.1.2 Создание нового пользователя

Элемент процедуры	Содержание
Путь	«Консоль администратора» → «Управление тенантами» → нужная строка → «Управление пользователями» → «Добавить пользователя» → «Создать нового».
Кто выполняет	Главный администратор. Получена заявка с именем, фамилией, служебным адресом и требуемой ролью.
Ожидаемый результат	Создана новая учётная запись, сразу включённая в выбранную организацию.

Порядок выполнения:

1. До создания нажать «Назад» и кнопку «Пользователи» в верхней части списка организаций; убедиться, что адрес ещё не зарегистрирован.
2. Вернуться в нужную организацию и открыть «Управление пользователями».
3. Нажать «Добавить пользователя» и выбрать «Создать нового».
4. В поле «Имя» ввести имя без сокращений, в поле «Фамилия» — фамилию.
5. Ввести служебный адрес электронной почты. Личные адреса для административных ролей не использовать.
6. Создать временный пароль по правилам службы учётных записей. Не использовать один пароль для нескольких пользователей.
7. Выбрать роль. По умолчанию оставлять «Пользователь».
8. Нажать «Добавить».
9. Передать временный пароль отдельным защищённым каналом и потребовать смену при первом входе.
10. После первого входа проверить доступ пользователя и закрыть заявку.

Проверка результата:

- в общем списке пользователей имеется одна запись;
- участник имеется в выбранной организации;
- вход выполняется временным, затем новым паролем;
- административные разделы соответствуют назначенной роли.

Отмена или возврат:

- Если пользователь создан ошибочно и не состоит в других организациях, удалить его из текущей организации; исходный код предусматривает удаление локальной записи после успешного удаления во внешней службе учётных записей.

7.2 Изменение и отзыв доступа

Полномочия должны пересматриваться не реже одного раза в квартал и при каждом изменении должностных обязанностей. При увольнении доступ прекращается до окончания последнего рабочего дня. Удаление пользователя из организации выполняется после проверки, не владеет ли он единственными экземплярами необходимых ресурсов.

- запретить общие учётные записи, кроме документированной аварийной записи;
- назначать административную роль на ограниченный срок, если это возможно;
- разделить повседневную и административную учётные записи;
- не передавать пароли по открытой почте и в общих чатах;
- проверять журнал после каждого массового изменения доступа.

7.3 Удаление пользователя из организации

Отзыв доступа участника

Элемент процедуры	Содержание
Путь	«Консоль администратора» → «Управление тенантами» → организация → «Управление пользователями» → строка пользователя → «Удалить».
Кто выполняет	Главный администратор. Имеется основание на отзыв доступа; проверено, что удаляется правильный пользователь. Владелец организации этой кнопкой не удаляется.
Ожидаемый результат	Доступ пользователя к выбранной организации отозван.

Порядок выполнения:

1. Открыть список участников организации.
2. Найти пользователя по адресу электронной почты, а не только по имени.
3. Проверить роль и принадлежность к другим организациям через общий список «Пользователи».
4. В строке пользователя нажать «Удалить».
5. В предупреждении «Вы уверены, что хотите удалить этого пользователя из тенанта?» проверить организацию и подтвердить действие.
6. Дождаться сообщения «Пользователь успешно удален».
7. Обновить страницу и убедиться, что строка исчезла.
8. Проверить журнал действий и закрыть заявку.

Проверка результата:

- пользователь отсутствует в списке организации;
- при наличии других организаций его учётная запись сохранена;
- при отсутствии других организаций вход прекращён, если это предусмотрено связанной службой учётных записей;
- событие удаления участника записано.

Отмена или возврат:

- Повторно добавить существующего пользователя по процедуре 7.1.1. Если учётная запись была полностью удалена, создать новую по процедуре 7.1.2.

Особые указания:

- Удаление из организации не является передачей принадлежащих пользователю материалов. До удаления проверить ответственных за базы знаний и подключения.

7.4 Просмотр всех пользователей

Сверка пользователей и ролей

Элемент процедуры	Содержание
Путь	«Консоль администратора» → «Управление тенантами» → кнопка «Пользователи».
Кто выполняет	Главный администратор.
Ожидаемый результат	Получен актуальный перечень пользователей и их членства в организациях.

Порядок выполнения:

1. Открыть страницу «Управление тенантами».
2. В правой верхней части нажать «Пользователи».
3. Для каждой записи проверить адрес электронной почты, организацию и роль.
4. Сопоставить список с кадровыми данными и действующими заявками.
5. Отдельно выписать главных администраторов и администраторов организаций.
6. Устранить лишние полномочия отдельными заявками, не выполняя массовое удаление без резервной копии.

Проверка результата:

- нет пользователей без владельца заявки;
- нет административных ролей с истёкшим основанием;
- один адрес не представлен несколькими ошибочными записями.

7.5 Удаление организации

Операция «Удалить тенант» удаляет связанные базы знаний, диалоги, файлы, задания, подключения и настройки. Перед подтверждением обязательно выполнить резервное копирование, получить письменное основание, проверить состав организации и назначить срок хранения копии. Восстановление средствами экранной формы не предусмотрено.

Безвозвратное удаление организации

Элемент процедуры	Содержание
Путь	«Консоль администратора» → «Управление тенантами» → строка организации → кнопка с изображением корзины.
Кто выполняет	Главный администратор и второй проверяющий. Получено письменное основание; создана и проверена резервная копия.
Ожидаемый результат	Организация и все связанные объекты удалены; пользователи других организаций сохранены.

Порядок выполнения:

1. Открыть организацию и составить перечень пользователей, баз знаний, файлов, помощников, поисковых приложений, подключений и ключей программного доступа.
2. Остановить автоматическую синхронизацию всех подключений организации.
3. Создать согласованную резервную копию и выполнить контроль чтения архивов.
4. Вернуться в «Управление тенантами». Найти организацию по полному наименованию.
5. Попросить второго проверяющего сверить наименование, число пользователей и основание.
6. Нажать кнопку с изображением корзины.
7. Прочитать предупреждение с фактическим названием организации. Если название не совпадает, нажать «Нет».
8. Подтвердить удаление.
9. Дождаться сообщения «Тенант успешно удален». Не перезапускать службы во время удаления.
10. Проверить отсутствие организации в списке, отсутствие её ресурсов и наличие записи в журнале.

Проверка результата:

- организация отсутствует после обновления страницы;
- её входные подключения остановлены;
- в журнале есть завершённое событие удаления;
- резервная копия зарегистрирована и защищена от досрочного удаления.

Отмена или возврат:

- Экранного восстановления нет. Развернуть совместимую версию в изолированной среде и восстановить полную согласованную резервную копию по разделу 10.

Особые указания:

- Если удаление внешней организации в службе учётных записей завершается ошибкой, локальное удаление не должно продолжаться; устранить внешнюю ошибку и повторить операцию.

8. УПРАВЛЕНИЕ БАЗАМИ ЗНАНИЙ И ФАЙЛАМИ

8.1 Создание базы знаний

8.1.1 Создание и первоначальная настройка базы знаний

Элемент процедуры	Содержание
Путь	Верхняя панель → «База знаний» → «Создать базу знаний».
Кто выполняет	Администратор организации. По процедуре 6.3.2 назначена модель смыслового представления. Известны владелец данных, язык и требуемый способ доступа.
Ожидаемый результат	Создана пустая база знаний с утверждённым языком, доступом, моделью и способом фрагментации.

Порядок выполнения:

1. Переключиться в нужную организацию и открыть «База знаний».
2. Нажать «Создать базу знаний».
3. В поле «Название базы знаний» ввести понятное уникальное название, отражающее предметную область и при необходимости подразделение.
4. В поле «Описание» указать назначение, владельца данных, состав документов и ограничения использования.
5. В поле «Язык документов» выбрать русский язык для преимущественно русскоязычного набора.
6. В поле «Права доступа» выбрать «Только я» для подготовки либо «Команда» для совместного управления участниками организации.
7. В поле «Модель эмбединга» выбрать утверждённую модель смыслового представления. После создания фрагментов эта модель не меняется без полной повторной обработки.
8. В поле «Метод фрагментации» выбрать способ по типу документов: «Законы» для нормативных актов, «Руководство» для структурированных руководств, «Простой» для смешанных документов, «Таблица» для построчных таблиц, «Вопросы и ответы» для пар вопрос–ответ.
9. В поле «Рекомендуемый размер фрагмента» указать начальное значение из методики испытаний. Для обычного связного текста начать с 512–800 токенов, затем проверить качеством поиска.
10. Нажать «Сохранить».
11. Открыть созданную базу и проверить вкладки «Основное», «Документы», «Метод фрагментации», «Тестирование поиска» и при включении «Граф знаний».

Проверка результата:

- название отображается в общем списке;
- описание и права сохранены;

- модель смыслового представления совпадает с актом настройки;
- вкладка документов пуста и готова к загрузке.

Отмена или возврат:

- Пока документы не загружены, удалить ошибочную базу через меню её карточки и создать заново.
- После загрузки сначала удалить документы и проверить отсутствие нужных помощников, затем удалить базу.

Особые указания:

- Не создавать несколько баз с одинаковыми названиями.
- Параметры фрагментации утверждать на контрольном наборе, а не сразу на полном массиве.

8.1.2 Выбор метода фрагментации

Тип исходных материалов	Рекомендуемый выбор	Что проверить после обработки
Нормативные правовые акты	«Законы»	Границы статей и пунктов не смешаны; номер и заголовок статьи сохранены.
Технические руководства в PDF	«Руководство»	Разделы выделены по заголовкам; таблицы не отделены от пояснений.
Разнородные документы	«Простой»	Фрагменты не слишком короткие и не соединяют разные темы.
Презентации	«Презентация»	Один слайд образует отдельный осмысленный фрагмент.
Табличный справочник	«Таблица»	Первая строка распознана как заголовки; каждая строка отдельна.
Перечень вопросов и ответов	«Вопросы и ответы»	В каждой записи ровно одна пара вопрос–ответ.
Один короткий документ	«Один»	Весь документ помещается в допустимый контекст и не требует частичного поиска.

После выбора перейти к процедуре 8.2.1, обработать не менее трёх документов разных видов и выполнить не менее десяти контрольных запросов по процедуре 8.3.1.

8.2 Состояния обработки

Состояние в программе	Действие администратора
ОЖИДАЕТ	Проверить доступность очереди и наличие свободных обработчиков, если ожидание превышает установленный срок.
ОБРАБАТЫВАЕТ	Наблюдать за временем и потреблением ресурсов; не перезапускать службу без необходимости.
ОТМЕНЕНО	Установить причину отмены; при необходимости запустить обработку повторно.
УСПЕШНО	Проверить число фрагментов и выполнить контрольный поиск.

Состояние в программе	Действие администратора
ОШИБКА	Открыть сообщение о ходе обработки, сопоставить время с журналами обработчика и устранить первопричину.

8.2.1 Загрузка и обработка документов

Элемент процедуры	Содержание
Путь	«База знаний» → нужная база → «Документы» → «Добавить файл» → «Локальные файлы».
Кто выполняет	Администратор организации либо уполномоченный пользователь. Файлы проверены антивирусным средством, не защищены неизвестным паролем и соответствуют назначению базы.
Ожидаемый результат	Документы загружены, обработаны и представлены поисковыми фрагментами.

Порядок выполнения:

1. Открыть требуемую базу знаний и убедиться по названию и описанию, что выбрана правильная база.
2. Нажать «Добавить файл».
3. Выбрать «Локальные файлы». Для создания пустого текстового файла использовать отдельный пункт «Создать пустой файл»; веб-сканирование применять только по согласованным адресам.
4. Перетащить файлы в область загрузки либо нажать выбор файлов. За одну операцию выбирать не более 32 файлов и не превышать установленный предел размера.
5. Дождаться завершения передачи. Не закрывать страницу, пока для каждого файла не появилась строка в списке.
6. Для PDF при необходимости открыть настройки файла и задать «Диапазон страниц»: поле «от» включается, поле «до» задаёт конечную границу согласно подсказке текущего выпуска.
7. Выбрать «Анализатор PDF». Для текстового PDF без сложной разметки допустим «Простой»; для таблиц и сложной структуры использовать визуальный анализатор, проверенный тестированием.
8. Для сканированных страниц включить распознавание текста. Для обычного текстового PDF отключить его, если это подтверждено контрольным просмотром.
9. Для сложных таблиц выбрать точное качество; при нехватке памяти — быстрое. Установить число страниц в одной группе обработки с учётом памяти обработчика.
10. Выделить загруженные файлы и нажать «Обработать».
11. Наблюдать переход «ОЖИДАЕТ» → «ОБРАБАТЫВАЕТ» → «УСПЕШНО».

12. Открыть «Просмотр» и выборочно сравнить полученные фрагменты с исходными страницами.

Проверка результата:

- все файлы имеют состояние «УСПЕШНО»;
- число фрагментов больше нуля;
- русские буквы, даты и числа распознаны правильно;
- таблицы не потеряли соответствие строк и заголовков;
- в просмотре есть ссылка на исходный документ и номер страницы, если он доступен.

Отмена или возврат:

- Для ошибочного файла нажать «Удалить» в его строке и подтвердить операцию, затем загрузить исправленную копию.
- При ошибочных настройках изменить параметры и выполнить повторную обработку только после подтверждения удаления прежних фрагментов.

Особые указания:

- Не запускать одновременно массовую обработку и резервное копирование без протестированного согласованного режима.
- Состояние «УСПЕШНО» подтверждает техническую обработку, но не качество распознавания; нужен просмотр и контрольный поиск.

8.2.2 Повторная обработка документа

Элемент процедуры	Содержание
Путь	«База знаний» → база → «Документы» → строка документа → настройки/«Обработать».
Кто выполняет	Администратор организации. Зафиксирована причина повторной обработки и подготовлены контрольные запросы.
Ожидаемый результат	Фрагменты документа полностью пересозданы с новыми параметрами.

Порядок выполнения:

1. Открыть документ и записать текущее число фрагментов, способ обработки и результаты контрольных запросов.
2. Изменить только один проверяемый параметр: распознавание, качество таблиц, диапазон страниц, размер группы или способ фрагментации.
3. Нажать «Обработать». Если программа предупреждает об очистке существующих фрагментов, проверить имя файла и подтвердить.
4. Дождаться состояния «УСПЕШНО».
5. Сравнить число и содержимое фрагментов с предыдущим результатом.
6. Повторить прежние контрольные запросы и зафиксировать улучшение либо ухудшение.

Проверка результата:

- нет одновременно старых и новых дублирующихся фрагментов;
- контрольные числа и таблицы распознаны;
- качество поиска не ухудшилось.

Отмена или возврат:

- Вернуть прежнее значение параметра и повторно обработать документ. Исходный файл должен сохраняться неизменным.

8.3 Ограничения загрузки

Текущая локализация указывает для локального размещения предел одной загрузки до 1 Гбайт и до 32 файлов. Эти значения должны быть сверены с параметрами входной службы, объектного хранилища и конкретного выпуска. Администратор вправе устанавливать меньшие пределы исходя из ресурсов и требований безопасности.

Проверка качества поиска

Элемент процедуры	Содержание
Путь	«База знаний» → нужная база → «Тестирование поиска».
Кто выполняет	Администратор организации либо владелец данных. Документы имеют состояние «УСПЕШНО». Подготовлены вопросы с заранее известными правильными документами и фрагментами.
Ожидаемый результат	Подтверждено, что база находит правильные источники по контрольному набору запросов.

Порядок выполнения:

1. Открыть вкладку «Тестирование поиска».
2. В поле «Тестовый текст» ввести первый контрольный вопрос на русском языке.
3. Оставить начальный «Порог сходства» 0,2, если методикой испытаний не установлено иное.
4. Установить вес сходства ключевых слов и смыслового сходства так, чтобы их сумма соответствовала требованию формы. Начать со сбалансированного значения.
5. Если настроена модель повторного упорядочивания (реранкер), выбрать её и задать число фрагментов для повторной оценки.
6. Нажать «Тестирование».
7. В разделе «Найденные результаты» проверить первые результаты, «Комбинированное сходство», «Сходство терминов» и «Векторное сходство».
8. Нажать «Просмотр» и убедиться, что найден правильный фрагмент и источник.
9. Повторить проверку для точного вопроса, вопроса с синонимами, вопроса с номером документа, вопроса по таблице и отрицательного вопроса, ответа на который в базе нет.

10. Зафиксировать значения, при которых правильные фрагменты устойчиво входят в первые результаты.
11. Перенести проверенные значения в настройки помощника или поискового приложения: значения на вкладке тестирования автоматически не сохраняются для них.

Проверка результата:

- для положительных вопросов правильный источник присутствует в согласованном числе первых результатов;
- для отрицательного вопроса нерелевантные результаты не превышают порог;
- номера, даты и названия совпадают с источником;
- результаты и параметры внесены в протокол испытаний.

Отмена или возврат:

- Вернуть прежние параметры; при плохом результате проверить фрагментацию и распознавание, а не только снижать порог.

Особые указания:

- Слишком низкий порог увеличивает шум; слишком высокий скрывает полезные фрагменты.
- Проверка поиска не равна проверке окончательного ответа помощника.

8.4 Подключение внешнего источника данных

8.4.1 Создание подключения

Элемент процедуры	Содержание
Путь	«Настройки пользователя» → «Коннекторы» → «Новый коннектор».
Кто выполняет	Администратор организации. Создана отдельная учётная запись во внешней системе с минимальными правами; определены разрешённые области данных и расписание.
Ожидаемый результат	Создано работоспособное подключение, которое загружает только разрешённые данные.

Порядок выполнения:

1. Открыть «Настройки пользователя», выбрать «Коннекторы».
2. Нажать «Новый коннектор».
3. Выбрать тип внешней системы из каталога. Доступный состав зависит от выпуска.
4. На шаге общих параметров указать уникальное название подключения и целевую базу знаний либо создание отдельной базы, если форма это предлагает.
5. На шаге соединения указать адрес внешней системы и служебные учётные данные.

6. На шаге состава данных выбрать только разрешённые пространства, папки, проекты, потоки или сущности. Исключить личные и закрытые области, не входящие в основание.
7. На шаге синхронизации указать период, начальную дату и правила обработки вложений.
8. Нажать «Проверить». Не сохранять подключение, если проверка завершилась ошибкой.
9. После успешной проверки нажать «Создать коннектор» либо «Подключить и начать синхронизацию» в зависимости от типа.
10. Открыть карточку подключения и наблюдать состояния «Активен» или «Синхронизация».
11. После первой загрузки открыть целевую базу знаний, проверить документы и выполнить контрольный поиск.

Проверка результата:

- состояние не содержит ошибки;
- время «Последняя синхронизация» обновляется;
- в целевой базе появляются ожидаемые документы;
- неразрешённые области отсутствуют;
- служебный пароль не отображается открыто.

Отмена или возврат:

- Нажать «Пауза», дождаться остановки текущей синхронизации, затем удалить ошибочно загруженные документы и само подключение.
- При утечке ключа немедленно отозвать его во внешней системе и создать новый.

Особые указания:

- Кнопка «Полная загрузка» повторно обходит исходный массив и может создать значительную нагрузку; выполнять в технологическое окно.
- Удаление подключения не всегда означает удаление уже загруженных документов; проверить базу отдельно.

8.4.2 Приостановка, возобновление и повторная загрузка

Элемент процедуры	Содержание
Путь	«Настройки пользователя» → «Коннекторы» → карточка подключения.
Кто выполняет	Администратор организации.
Ожидаемый результат	Синхронизация управляемо остановлена, возобновлена либо выполнена заново.

Порядок выполнения:

1. Открыть карточку и проверить текущее состояние, последнюю синхронизацию и последнюю ошибку.

2. Для временной остановки нажать «Пауза» и дождаться состояния «Приостановлен».
3. После устранения причины нажать «Продолжить» и проверить переход в состояние «Активен».
4. Для полного повторного обхода сначала оценить объём и создать резервную копию целевой базы.
5. Нажать «Полная загрузка» и подтвердить действие.
6. Наблюдать прогресс; после завершения проверить число новых, обновлённых и ошибочных объектов.

Проверка результата:

- состояние соответствует выбранному действию;
- нет необъяснимых дубликатов;
- последняя ошибка очищена либо документирована.

8.5 Подключение сервера инструментов

Добавление сервера инструментов

Элемент процедуры	Содержание
Путь	«Настройки пользователя» → раздел серверов инструментов → «Добавить».
Кто выполняет	Администратор организации. Известны имя, тип соединения, полный адрес и признак необходимости токена. Определён разрешённый перечень инструментов.
Ожидаемый результат	Сервер зарегистрирован в текущей организации, перечень инструментов сохранён.

Порядок выполнения:

1. Открыть раздел серверов инструментов в настройках.
2. Нажать «Добавить».
3. В поле названия ввести уникальное имя длиной не более 255 байт.
4. Выбрать тип соединения, поддерживаемый сервером.
5. Ввести полный адрес. Для внутренней шлюзовой службы использовать её внутренний адрес, доступный прикладной службе.
6. Если требуется, ввести токен авторизации. Не помещать токен в адрес.
7. Нажать «Проверить». Система должна получить перечень инструментов.
8. Просмотреть названия и описания найденных инструментов. Отключить все изменяющие инструменты, не одобренные владельцем системы.
9. Нажать «Сохранить».
10. Повторно открыть карточку и обновить перечень инструментов.

Проверка результата:

- проверка соединения успешна;
- перечень инструментов соответствует ожидаемому;

- неразрешённые инструменты выключены;
- создание отражено в журнале действий.

Отмена или возврат:

- Удалить сервер через карточку. Перед удалением проверить помощников и последовательности, которые его используют.

Особые указания:

- Имя сервера должно быть уникальным в организации.
- Проверка и сохранение выполняют сетевое обращение; неверный адрес или недоступный токен приводят к отказу создания.

8.6 Создание помощника

Создание и проверка помощника

Элемент процедуры	Содержание
Путь	Верхняя панель → «Ассистенты» → «Создать ассистента».
Кто выполняет	Администратор организации. База знаний обработана и прошла процедуру 8.3.1; модель чата добавлена.
Ожидаемый результат	Создан помощник, отвечающий по выбранным базам и утверждённым правилам.

Порядок выполнения:

1. Открыть «Ассистенты» и нажать «Создать ассистента».
2. В поле «Имя ассистента» указать уникальное назначение, например «Помощник по внутренним регламентам».
3. Выбрать русский язык и при необходимости загрузить изображение.
4. В поле «Базы знаний» выбрать только проверенные базы. Пустые базы в списке не отображаются.
5. В поле «Модель» выбрать утверждённую модель чата.
6. В поле «Системный промпт» на русском языке задать роль, допустимые источники, требование ссылаться на источник, запрет выдумывать сведения и поведение при отсутствии ответа.
7. Указать «Пустой ответ» для случая, когда подходящие сведения не найдены.
8. Установить число первых фрагментов, порог сходства и иные параметры согласно результатам процедуры 8.3.1.
9. Для справочного помощника установить температуру 0–0,2. Если модель использует другую шкалу, выбрать минимальное доступное значение. Повышать температуру только после тестирования на утверждённом наборе запросов и проверки точности и воспроизводимости ответов.
10. Если модель поддерживает инструменты, включить только одобренные инструменты.
11. Нажать «Сохранить» и открыть «Новый чат».

12. Выполнить положительный, отрицательный и провокационный контрольные вопросы. Проверить текст ответа и источники.

Проверка результата:

- правильный вопрос получает подтверждённый источником ответ;
- при отсутствии сведений используется заданный пустой ответ;
- ответ не раскрывает документы, недоступные пользователю;
- неразрешённые инструменты не вызываются.

Отмена или возврат:

- Вернуться в «Настройки ассистента», исправить один параметр и повторить полный контрольный набор.
- При критической ошибке снять публикацию или удалить помощника после сохранения журнала испытаний.

9. ЖУРНАЛИРОВАНИЕ И КОНТРОЛЬ СОСТОЯНИЯ

9.1 События, подлежащие контролю

Группа	Примеры
Вход и доступ	успешный и неуспешный вход, выход, изменение пароля, выдача административной роли;
Организации	создание, удаление, добавление и удаление участника;
Данные	создание и удаление базы знаний, загрузка и удаление документа, изменение прав;
Подключения	создание, изменение и удаление подключения к внешней системе;
Система	запуск и остановка служб, ошибка базы данных, нехватка места, повторный запуск контейнера;
Резервные копии	начало, завершение, ошибка, результат проверки восстановления.

9.2 Ежедневная проверка

- доступность внешнего адреса и срок действия свидетельства защищённого соединения;
- состояние и число перезапусков служб;
- заполнение постоянных томов и системного раздела;
- ошибки прикладной службы и обработчиков за последние сутки;
- длина очереди и число зависших заданий;
- успешность последней резервной копии;
- необычные административные действия и повторяющиеся ошибки входа.

```
docker compose -f docker-compose.yml ps
```

```
docker compose -f docker-compose.yml logs --since=24h --no-color
```

```
df -h
```

```
kubecttl -n semantix get pods,pvc
```

```
kubecttl -n semantix get events --sort-by=.lastTimestamp
```

9.2.1 Проверка состояния через экранную форму

Элемент процедуры	Содержание
Путь	«Консоль администратора» → «Настройки» либо «Настройки пользователя» → «Система».
Кто выполняет	Администратор организации или главный администратор.
Ожидаемый результат	Все обязательные внутренние службы доступны приложению.

Порядок выполнения:

1. Открыть раздел «Система».
2. Дождаться завершения загрузки карточек состояния.
3. Проверить карточку поискового хранилища: индикатор должен быть зелёным, время ответа — в пределах обычного значения.
4. Проверить карточку объектного хранилища.
5. Проверить карточку временного хранилища.
6. Проверить карточку базы данных.
7. Проверить карточку обработчиков задач. Должны отображаться сердечбиения ожидаемого числа обработчиков.
8. При жёлтом или красном индикаторе записать точное время, название карточки и текст ошибки, затем перейти к командной проверке соответствующей службы.
9. После устранения обновить страницу и убедиться, что индикатор стал зелёным.

Проверка результата:

- все карточки зелёные;
- число обработчиков совпадает с установленным;
- время ответа не выросло резко относительно обычного;
- ошибки отсутствуют.

Особые указания:

- Зелёный индикатор подтверждает доступность, но не заменяет проверку свободного места, резервной копии и контрольного поиска.

9.2.2 Просмотр журнала контейнера при ошибке

Элемент процедуры	Содержание
Путь	Командная строка узла либо кластера.
Кто выполняет	Системный администратор. Известны время ошибки и имя службы.
Ожидаемый результат	Установлена первичная причина либо собраны достаточные сведения для передачи разработчику.

Порядок выполнения:

1. Установить временной интервал: не менее пяти минут до события и десяти минут после.
2. Сохранить состояние контейнеров до перезапуска.
3. Получить журнал только нужной службы за установленный интервал.
4. Найти первую ошибку, а не только последующие сообщения о недоступности.
5. Сопоставить идентификатор задания, организации или документа без раскрытия содержимого.
6. Сохранить обезличенный фрагмент журнала в заявке.
7. После устранения повторить действие пользователя и убедиться, что ошибка не появляется.

Проверка результата:

- указан точный интервал;
- зафиксирована версия;
- секреты и персональные данные удалены;
- есть результат повторной проверки.

```
docker compose -f docker-compose.yml logs --since="2026-01-01T10:00:00" --until="2026-01-01T10:20:00"
<служба>
```

```
kubectrl -n semantix logs <экземпляр_службы> --since=20m
```

```
kubectrl -n semantix logs <экземпляр_службы> --previous --since=20m
```

9.3 Пороговые значения оповещений

Показатель	Предупреждение	Критическое состояние
Свободное место	менее 30 %	менее 10 %
Использование памяти	более 80 % в течение 15 минут	более 90 % в течение 5 минут
Перезапуски службы	более 1 за час	циклический перезапуск
Очередь заданий	рост 30 минут	нет обработки 15 минут
Возраст резервной копии	превышает расписание на 25 %	нет успешной копии более двух расписаний
Срок свидетельства	менее 30 суток	менее 7 суток

Пороговые значения проверяются в течение первого месяца эксплуатации и затем закрепляются в регламенте наблюдения.

9.4 Дополнительный контроль операционной системы и кластера

Объект	Что контролировать	Когда требуется вмешательство
Узлы операционной системы	Состояние файловых систем, свободное место и индексные дескрипторы, ошибки ядра, синхронизация времени, срок установки обновлений безопасности.	Ошибки ввода-вывода, переход файловой системы только в чтение, рассинхронизация времени, окончание поддержки установленного обновления.
Kubernetes	Готовность узлов, давление по памяти и диску, число незапланированных выселений, ошибки планирования и загрузки образов.	Узел не готов дольше согласованного времени, экземпляры не размещаются, повторяются ошибки доступа к образам.
Deckhouse	Состояние используемых модулей, доступность служебных компонентов, предупреждения о несовместимости и предстоящем обновлении.	Используемый модуль неработоспособен, версия выходит из поддержки, автоматическое изменение может затронуть Semantix.
Постоянные тома	Состояние привязки, заполнение, задержки операций, ошибки системы хранения и успешность снимков.	Том не связан, заполнен более порога, задержки превышают базовое значение, снимок не создаётся.
Распределение экземпляров	Фактическое размещение по узлам и зонам, соблюдение запретов и правил разнесения.	Все экземпляры критической службы оказались на одном узле либо в одной зоне.
Свидетельства и закрытые объекты	Срок действия, событие обновления, успешное чтение только разрешёнными службами.	До окончания менее порога, обновление не применилось, обнаружено неразрешённое чтение.

```
kubectl get nodes
```

```
kubectl -n semantix get pods -o wide
```

```
kubectl -n semantix get pvc
```

```
kubectl -n semantix get events --sort-by=.metadata.creationTimestamp
```

Обновление Deckhouse или операционной системы не выполняется автоматически без согласованного окна, если оно может перезапустить узел либо изменить сетевое, дисковое или входное средство. Оповещение должно поступить до начала изменения.

10. РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ

10.1 Состав резервной копии

- реляционная база данных;
- объектное хранилище с исходными документами;
- поисковое хранилище либо документированная возможность полного повторного построения;

- данные службы управления учётными записями;
- файлы параметров без открытого раскрытия секретов;
- закрытые объекты и свидетельства в зашифрованном виде;
- перечень версий образов и контрольные суммы комплекта поставки.

Копирование только файлов документов недостаточно. Для согласованного восстановления необходимо сохранить базу данных, файлы, поисковые сведения и настройки одного момента времени.

10.2 Рекомендуемая схема

Вид копии	Периодичность	Хранение
Полная	еженедельно	не менее 4 недель;
Изменения	ежедневно	не менее 14 суток;
Перед обновлением	перед каждым изменением версии	до успешного завершения приёмочных проверок;
Долговременная	ежемесячно	по правилам организации;

Не менее одной копии хранится вне основного узла или кластера. Копии шифруются, доступ к ним журналируется. Не реже одного раза в квартал выполняется пробное восстановление в изолированной среде.

До выбора расписания владелец системы утверждает два измеримых значения: максимально допустимый интервал потери данных и максимально допустимую продолжительность восстановления. Период копирования должен быть короче допустимого интервала потери, а пробное восстановление должно укладываться в допустимую продолжительность. Если эти условия не выполняются, расписание и способ копирования пересматриваются.

10.3 Копирование при установке на одном сервере

1. Оповестить пользователей о технологическом окне.
2. Дождаться завершения обработки документов или остановить приём новых заданий.
3. Остановить прикладные службы без удаления постоянных томов.
4. Создать копии всех постоянных томов и рабочего файла параметров.
5. Рассчитать контрольные суммы архивов.
6. Зашифровать и переместить копию в утверждённое хранилище.
7. Запустить службы и выполнить проверку доступности.

```
docker compose -f docker-compose.yml down
```

```
bash docker/migration.sh backup <каталог_копии>
```

```
sha256sum <каталог_копии>/* > <каталог_копии>/SHA256SUMS
```

Запрещается применять параметр удаления томов при остановке. Команда с параметром `-v` удаляет постоянные данные и не должна использоваться в обычной эксплуатации.

Проверка созданной копии

1. Проверить код завершения сценария копирования; наличие каталога само по себе не означает успех.
2. Проверить, что архивы базы данных, объектного, поискового и временного хранилищ имеют ненулевой размер.
3. Проверить контрольные суммы всех файлов.
4. Скопировать комплект в утверждённое внешнее хранилище.
5. На отдельном тестовом узле восстановить копию под другим адресом.
6. Выполнить вход, открыть контрольную организацию, скачать исходный файл и выполнить контрольный поиск.
7. Зафиксировать время создания, время восстановления, объём и результат.

```
sha256sum -c <каталог_копии>/SHA256SUMS
```

```
du -sh <каталог_копии>
```

10.4 Копирование кластерной установки

Для кластера предпочтительно использовать согласованные снимки постоянных томов вместе с прикладной копией базы данных. Нельзя считать набор несогласованных снимков разных моментов полноценной копией. В Deckhouse применяется класс снимков, фактически предоставляемый настроенным модулем хранения; имя класса не переносится из примера другой установки.

1. Остановить постановку новых заданий и автоматическую синхронизацию подключений.
2. Дождаться завершения выполняемых заданий; записать оставшиеся идентификаторы.
3. Создать логическую копию прикладной базы PostgreSQL и отдельной базы журнала действий.
4. Создать копию объектного хранилища средствами, обеспечивающими версии и целостность объектов.
5. Создать снимок поискового хранилища его штатным способом либо сохранить возможность полного повторного построения из базы и файлов.
6. Сохранить описание установленного выпуска, рабочий файл параметров без открытых секретов и перечень закрытых объектов.
7. Создать снимки постоянных томов, если их поддерживает класс хранения.
8. Проверить состояние каждого снимка и возможность создать из него новый постоянный том в отдельном тестовом пространстве имён.

9. Рассчитать контрольные суммы выгрузок и перенести их во внешнее защищённое хранилище.
10. Возобновить синхронизацию и постановку заданий.
11. Выполнить пробное восстановление в отдельном пространстве имён.

```
helm get values semantix -n semantix -o yaml > values-installed.yaml
```

```
kubectl -n semantix get pvc -o wide
```

```
kubectl -n semantix get deployment,statefulset,service,ingress -o yaml > resources-installed.yaml
```

Файлы `values-installed.yaml` и `resources-installed.yaml` перед сохранением проверить на наличие секретов. Закрытые объекты выгружаются только утверждённым средством резервного копирования в зашифрованном виде; обычная команда просмотра в текстовый файл не применяется.

Снимок тома, находящийся в той же системе хранения, не является внешней резервной копией. Отказ или ошибочное удаление системы хранения может уничтожить и рабочий том, и снимок. Как минимум одна проверенная копия данных и описания конфигурации переносится в независимое защищённое хранилище.

10.5 Восстановление

1. Развернуть совместимую версию программного комплекта.
2. Остановить все службы.
3. Проверить контрольные суммы и расшифровать копию.
4. Восстановить постоянные тома либо данные каждой внешней службы.
5. Проверить права на каталоги и соответствие адресов в настройках.
6. Запустить сначала хранилища, затем прикладную службу и обработчики.
7. Выполнить вход, открыть контрольную организацию, проверить документы, поиск и журнал.
8. Зафиксировать фактическую потерю данных по времени и продолжительность восстановления.

```
bash docker/migration.sh restore <каталог_копии>
```

```
docker compose -f docker-compose.yml up -d
```

Приёмка после восстановления

Объект проверки	Действие	Критерий
Учётные записи	Войти главным администратором и обычным пользователем.	Роли и организации совпадают с состоянием копии.
Организации	Открыть список организаций и число участников.	Контрольные значения совпадают.
Файлы	Скачать не менее трёх контрольных файлов разных форматов.	Контрольные суммы совпадают с исходными.
Поиск	Выполнить утверждённые контрольные запросы.	Найдены ожидаемые источники.

Объект проверки	Действие	Критерий
Помощник	Выполнить положительный и отрицательный вопрос.	Ответ и поведение при отсутствии данных верны.
Подключения	Открыть карточки, не запуская массовую загрузку.	Настройки восстановлены; секреты действуют либо заменены.
Журнал	Найти события до момента копии и новое событие входа.	История доступна, новые события добавляются.

Промышленный адрес переключается на восстановленную среду только после выполнения всех обязательных проверок и подписания протокола восстановления.

11. ОБНОВЛЕНИЕ ПРОГРАММЫ

11.1 Подготовка обновления

- изучить перечень изменений и несовместимостей;
- зафиксировать текущую версию и значения параметров;
- создать и проверить резервную копию;
- проверить обновление на копии промышленных данных в тестовой среде;
- подготовить план возврата и критерии остановки;
- назначить технологическое окно и уведомить пользователей.

11.2 Порядок обновления при установке на одном сервере

1. Остановить приём новых заданий и дождаться завершения выполняемых.
2. Создать резервную копию.
3. Получить утверждённые образы и проверить их контрольные суммы.
4. Обновить файл состава контейнеров и параметры только по инструкции выпуска.
5. Запустить обновление.
6. Проверить преобразование структуры данных, состояние служб и журналы.
7. Выполнить приёмочные проверки из подраздела 5.4.
8. Снять ограничение на работу пользователей.

```
docker compose -f docker-compose.yml pull
docker compose -f docker-compose.yml up -d
docker compose -f docker-compose.yml ps
```

11.3 Порядок обновления кластера

1. Проверить новую версию пакета установки и всех образов по контрольным суммам; не использовать тег latest.
2. Сопоставить требования новой версии с фактическими версиями операционной системы, Kubernetes, Deckhouse, входного компонента и классов хранения.

3. Получить текущие несекретные значения установки и подготовить сравнение с новыми значениями. Не заменять рабочий файл примером из нового пакета целиком.
4. Создать согласованную резервную копию и пробно восстановить её на совместимой версии.
5. Выполнить построение описаний ресурсов и предварительную проверку обновления в тестовом пространстве имён.
6. Остановить новые длительные задания, выполнить обновление и дождаться завершения преобразований структуры данных.
7. Проверить состояние каждого развёртывания, хранилищ, событий и журнала приложения.
8. Выполнить проверки 5.4, включая русский интерфейс, вход, организацию, документ, поиск и журнал.
9. Наблюдать среду установленный срок; только после этого закрыть изменение и разрешить удаление прежних образов.

```
helm upgrade semantix <каталог_пакета> -n semantix -f values-production.yaml --wait --timeout 20m
```

```
kubectl -n semantix rollout status deployment --timeout=20m
```

После обновления запрещается удалять предыдущие образы и резервную копию до завершения установленного срока наблюдения. Возврат к предыдущей версии выполняется только при подтверждённой совместимости структуры данных либо с восстановлением полной резервной копии.

11.4 Обновление операционной системы, Kubernetes и Deckhouse

Обновление системной основы выполняется отдельно от обновления Semantix. Одновременное изменение операционной системы, Kubernetes или Deckhouse и версии Semantix запрещается, поскольку при отказе невозможно однозначно определить причину.

1. Проверить целевую версию в разделе 3.1 и в официальной матрице поддерживаемых операционных систем кластерной платформы.
2. Создать и проверить резервные копии Semantix, службы учётных записей и системных описаний кластера.
3. Повторить обновление на тестовом кластере с той же операционной системой и теми же средствами хранения и сети.
4. Зафиксировать порядок обновления управляющих и рабочих узлов, допустимое число одновременно недоступных узлов и критерий остановки.
5. Выводить рабочие узлы по одному, проверяя перенос экземпляров и доступность данных после каждого узла.
6. Для Deckhouse применять только штатный порядок и утверждённый режим обновления платформы; не заменять её компоненты вручную.
7. После каждого этапа проверять узлы, модули, постоянные тома, входной адрес и контрольный запрос Semantix.

8. После полного обновления повторить тестирование резервного восстановления и при заявленной отказоустойчивости — управляемое тестирование отказа узла.

Переход между основными версиями Astra Linux или РЕД ОС рассматривается как смена основного выпуска операционной системы, а не как обычное пакетное обновление. Для него подготавливается отдельный план переноса или последовательной замены узлов, проверяется совместимость ядра, средства запуска контейнеров, сетевых и дисковых компонентов. Изменение на месте без протестированной процедуры не допускается.

12. УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

Проявление	Вероятная причина	Действия
Страница не открывается	Не работает входная или прикладная служба; ошибка разрешения имени; межсетевой экран.	Проверить имя узла, порт, состояние контейнера, последние сообщения и свидетельство защищённого соединения.
Вход отклоняется	Неверный пароль; учётная запись отключена; недоступна служба учётных записей; рассинхронизация времени.	Проверить время, состояние службы, журнал входа и членство пользователя в организации.
Документ остаётся в состоянии «ОЖИДАЕТ»	Нет свободного обработчика; недоступно временное хранилище; очередь остановлена.	Проверить обработчики, очередь, память и сообщения за время постановки задания.
Состояние «ОШИБКА»	Неподдерживаемый или повреждённый файл; недостаток памяти; ошибка распознавания или модели.	Скачать исходный файл, проверить формат, сообщение о ходе обработки и журнал обработчика; повторить на контрольном файле.
Поиск не возвращает документ	Обработка не завершена; неверные права; высокий порог сходства; ошибочная модель.	Проверить состояние, права, число фрагментов и «Тестирование поиска»; сравнить с контрольным запросом.
Не загружается файл	Превышен размер; заполнен диск; недоступно объектное хранилище.	Проверить предел входной службы, свободное место, доступность хранилища и права записи.
Служба постоянно перезапускается	Ошибка параметров; нехватка памяти; недоступна зависимая служба.	Изучить предыдущее завершение, причину остановки и журнал; не увеличивать пределы до установления причины.
Не создаётся организация	Нет прав главного администратора; ошибка службы учётных записей или базы данных.	Проверить роль, доступность зависимых служб и запись события создания.
Экземпляр остаётся в состоянии Pending	Не хватает ресурсов; правила размещения исключают все узлы; постоянный том не создаётся.	Просмотреть события экземпляра, доступные ресурсы, метки и ограничения узлов, затем состояние заявки на том.

Проявление	Вероятная причина	Действия
Состояние ImagePullBackOff	Нет доступа к внутреннему хранилищу; неверное имя образа; отсутствует закрытый объект; архитектура образа не подходит.	Сверить полный адрес и неизменяемую версию образа, закрытый объект, доверие к свидетельству хранилища и архитектуру узла.
Заявка на постоянный том остаётся Pending	Неверный класс, нет ёмкости, несовместим режим доступа или модуль хранения неработоспособен.	Просмотреть событие заявки, фактический класс и состояние средства хранения; не удалять рабочие тома других служб.
После обновления Deckhouse пропал вход	Изменился входной модуль, адрес, класс или свидетельство.	Проверить состояние модулей, входной объект, адрес службы и свидетельство; сопоставить с протоколом изменения платформы.
На узле операционной системы отказ в доступе к файлу	Права владельца, обычные права или мандатное разграничение не разрешают операцию.	Зафиксировать отказ в системном журнале; проверить владельца, права и метки. Не отключать защитный механизм целиком.

12.1 Сбор диагностических сведений

- точное время и часовой пояс;
- версия программы и контрольные суммы образов;
- имя организации и обезличенный идентификатор пользователя;
- последовательность действий до ошибки;
- снимок состояния служб и число перезапусков;
- журналы за ограниченный промежуток времени;
- сведения о ресурсах узла и заполнении томов;
- идентификатор задания или документа без передачи самого документа, если он содержит ограниченные сведения.

Перед передачей диагностических сведений необходимо удалить пароли, ключи, файлы сеансов, персональные данные и содержимое документов, не требуемое для анализа.

12.2 Диагностика кластерной установки

1. Зафиксировать точное время, текущий контекст кластера, версии Semantix, Kubernetes, Deckhouse при наличии, операционной системы и ядра затронутого узла.
2. Получить состояние экземпляра и его события до перезапуска. Сообщение события обычно точнее общего состояния.
3. Если экземпляр перезапускался, получить журнал предыдущего экземпляра и причину завершения.
4. Проверить зависимые службы по направлению от приложения к базе данных, объектному, поисковому и временному хранилищам.
5. Проверить заявку и постоянный том. Не удалять заявку только ради повторного создания, пока не установлено, есть ли на томе единственная копия данных.

6. Для Deckhouse проверить состояние используемого модуля, не изменяя его конфигурацию во время сбора сведений.
7. На узле проверить свободное место, ошибки файловой системы и ядра, время и сетевое разрешение. Не выполнять перезагрузку до сохранения диагностических сведений, если нет угрозы повреждения данных.
8. После устранения причины повторить исходную операцию и контрольный поиск, а не ограничиваться зелёным состоянием экземпляра.

```
kubecttl -n semantix describe pod <имя_экземпляра>
```

```
kubecttl -n semantix logs <имя_экземпляра> --previous --since=30m
```

```
kubecttl -n semantix describe pvc <имя_заявки_на_том>
```

```
kubecttl get events -A --sort-by=.metadata.creationTimestamp
```

```
journalctl -p warning --since "30 minutes ago"
```

13. ЗАЩИТА ИНФОРМАЦИИ

13.1 Обязательные меры

- использовать защищённое соединение для пользовательского и административного доступа;
- ограничить административный доступ выделенной сетью и многофакторной проверкой;
- хранить секреты вне файлов состава контейнеров и исходного кода;
- регулярно менять служебные ключи и немедленно менять их при подозрении на раскрытие;
- применять принцип минимальных полномочий к пользователям и службам;
- устанавливать обновления безопасности операционной системы и системных средств по утверждённому порядку;
- собирать журналы на отдельном защищённом узле;
- проверять образы на известные уязвимости до допуска в промышленную среду;
- запретить непосредственный доступ пользователей к внутренним хранилищам.

13.2 Работа с внешними моделями и подключениями

Перед включением внешней службы администратор совместно с владельцем данных определяет состав передаваемых сведений, место обработки, срок хранения, порядок удаления, правовое основание и допустимые действия. Подключение с правом изменения внешней системы создаётся отдельной служебной учётной записью с минимальными полномочиями. Каждое изменяющее действие должно быть ограничено разрешённым перечнем и отражаться в журнале.

13.3 Защита кластерной установки на поддерживаемых операционных системах

Мера	Требование
Механизмы операционной системы	Мандатное разграничение доступа, контроль целостности и иные включённые механизмы не отключаются общесистемно ради запуска контейнеров. Необходимые разрешения оформляются точно и проверяются администратором безопасности.
Права в кластере	Для установки, наблюдения, резервного копирования и приложения используются разные служебные учётные записи. Постоянные права администратора всего кластера приложению не выдаются.
Закрытые объекты	Секреты шифруются в хранилище кластерной платформы или управляются внешним защищённым средством; чтение ограничивается нужными службами; обращения журналируются; base64 не считается шифрованием.
Сетевые правила	По умолчанию запрещаются неразрешённые входящие и исходящие соединения. Явно разрешаются только связи между перечисленными службами, доступ к моделям, почте, времени, журналам и резервному хранилищу.
Запуск контейнеров	Запрещаются привилегированный режим, повышение полномочий, запись в корневую файловую систему и лишние возможности ядра, если конкретная служба не имеет документированной необходимости.
Образы	Разрешаются только образы из внутреннего хранилища с неизменяемой версией и проверенной контрольной суммой. Перед допуском выполняются проверка состава и известных уязвимостей.
Узлы	Административный вход разрешён из выделенной сети; обычные пользователи на узлы не входят; обновления и изменения системных настроек выполняются по заявке.
Журналы	События операционной системы, Kubernetes, Deckhouse и Semantix передаются на отдельное защищённое средство с единым временем и защитой от изменения.

После изменения защитных настроек выполняется не только проверка запуска, но и отрицательная проверка: пользователь не должен видеть другую организацию, контейнер не должен обращаться к запрещённому адресу, а служебная учётная запись не должна читать чужой закрытый объект.

14. РЕГЛАМЕНТНЫЕ РАБОТЫ

Периодичность	Работы
Ежедневно	Проверка доступности, ошибок, очередей, свободного места, резервной копии и необычных входов.
Еженедельно	Просмотр роста данных и журналов; проверка просроченных заданий; проверка доступных обновлений безопасности операционной системы и системных средств без их автоматического применения.

Периодичность	Работы
Ежемесячно	Проверка полномочий администраторов, срока свидетельств, объёма копий, прогноза ёмкости, распределения экземпляров по узлам и состояния модулей Deckhouse при его использовании.
Ежеквартально	Пробное восстановление; пересмотр прав пользователей; проверка аварийных контактов и инструкции; сверка фактических версий операционной системы, Kubernetes и Deckhouse с матрицами поддержки.
Не реже одного раза в год	Тестирование проектного сценария отказа узла или зоны в непроизводственной среде либо в согласованное окно; пересчёт ресурсов и времени полного восстановления.
Перед изменением	Резервная копия, тестирование, план возврата, согласование окна.
После изменения	Приёмочная проверка, наблюдение, запись результата и обновление документации.

15. ЗАВЕРШЕНИЕ РАБОТЫ

Обычная эксплуатация не требует ежедневной остановки. Плановая остановка выполняется только в технологическое окно.

1. Оповестить пользователей.
2. Запретить постановку новых заданий.
3. Дождаться завершения обработки или зафиксировать незавершённые задания.
4. Создать резервную копию при длительной остановке.
5. Остановить сначала прикладную службу и обработчики, затем хранилища.
6. Проверить отсутствие работающих контейнеров и записать время остановки.

```
docker compose -f docker-compose.yml down
```

Параметр удаления постоянных томов не применять.

Плановая остановка кластерной установки:

1. Оповестить пользователей и владельцев подключений; зафиксировать начало технологического окна.
2. Приостановить автоматическую синхронизацию и запретить постановку новых документов и длительных заданий.
3. Дождаться завершения выполняемых заданий либо записать идентификаторы тех, которые будут повторены.
4. Создать согласованную резервную копию и проверить её состояние.
5. Уменьшить число экземпляров прикладных служб и обработчиков до нуля утверждённым изменением параметров установки. Не удалять пакет, если требуется только остановка.

6. Штатно остановить или переключить внешние хранилища по их собственным инструкциям. Встроенные одиночные хранилища останавливать только после прикладных служб.
7. Проверить отсутствие незавершённых операций записи и состояние постоянных томов.
8. Если останавливается весь кластер, передать управление администратору Kubernetes или Deckhouse; порядок остановки управляющих и рабочих узлов определяется документацией платформы.
9. После запуска кластера сначала проверить хранилища, затем прикладные службы, выполнить вход, контрольный документ и поиск.

Команды удаления пространства имён, Helm-релиза и заявок на постоянные тома не являются командами остановки и для плановой паузы не применяются.

Приложение А (обязательное)

Контрольный лист ввода в эксплуатацию

№	Проверка	Результат	Дата, подпись
1	Комплект поставки и контрольные суммы проверены	☐ Да ☐ Нет	
2	Зафиксированы точные версии Semantix, операционной системы, ядра, Kubernetes и при наличии Deckhouse	☐ Да ☐ Нет	
3	Сочетание версий входит в утверждённую матрицу совместимости	☐ Да ☐ Нет	
4	Сетевые правила и защищённое соединение настроены	☐ Да ☐ Нет	
5	Классы томов, входа и снимков проверены на фактическом кластере	☐ Да ☐ Нет	
6	Секреты размещены в защищённом хранилище; в рабочих файлах их нет	☐ Да ☐ Нет	
7	Ресурсы рассчитаны по контрольной нагрузке с запасом на отказ узла	☐ Да ☐ Нет	
8	Все обязательные службы работают и распределены по проектной схеме	☐ Да ☐ Нет	
9	Для каждого хранилища указано: отказоустойчивая схема либо допустимое время восстановления	☐ Да ☐ Нет	
10	Русский язык интерфейса проверен	☐ Да ☐ Нет	
11	Роли и организации проверены	☐ Да ☐ Нет	
12	Контрольный документ обработан	☐ Да ☐ Нет	
13	Контрольный поиск выполнен	☐ Да ☐ Нет	
14	Журнал действий, журналы операционной системы и кластера поступают во внешнее хранилище	☐ Да ☐ Нет	
15	Резервная копия создана и пробно восстановлена	☐ Да ☐ Нет	
16	Если заявлена отказоустойчивость, управляемый отказ узла протестирован	☐ Да ☐ Нет ☐ Не требуется	
17	Оповещения о месте, памяти, сроке свидетельств и отказах проверены	☐ Да ☐ Нет	
18	Эксплуатационные ответственные и порядок изменения платформы назначены	☐ Да ☐ Нет	

Приложение Б (рекомендуемое)

Карточка установки

Поле	Значение
Наименование среды	
Версия Semantix и идентификатор исходного кода	
Дата установки	
Внешний адрес	
Способ размещения: один сервер / Kubernetes / Deckhouse	
Операционная система: наименование, версия, корректирующее обновление, архитектура	
Версия ядра операционной системы	
Версия Kubernetes	
Версия Deckhouse, если применяется	
Средство запуска контейнеров	
Сетевое средство кластера и размер пакета	
Входной класс	
Класс постоянных томов и параметры избыточности	
Класс снимков	
Перечень и контрольные суммы образов	
Число экземпляров каждой службы	
Схема PostgreSQL	
Схема объектного хранилища	
Схема поискового хранилища	
Схема временного хранилища	
Размеры постоянных томов	
Допустимый интервал потери данных	
Допустимая продолжительность восстановления	
Место резервных копий	
Срок хранения журналов	
Ответственный администратор Semantix	
Ответственный за операционную систему	

Поле	Значение
Ответственный за Kubernetes или Deckhouse	
Ответственный за безопасность	
Номер заявки на изменение	

Приложение В (справочное)**Соответствие экранных разделов**

Подпись в программе	Назначение
Консоль администратора	Общесистемное управление.
Управление тенантами	Управление организациями и их участниками.
Пользователи	Просмотр пользователей системы.
База знаний	Создание и настройка наборов документов.
Управление файлами	Загрузка и организация файлов.
Ассистенты	Управление интеллектуальными помощниками.
Агент	Настройка последовательностей выполнения действий.
Поиск	Управление поисковыми приложениями и выполнение поиска.
Настройки пользователя	Язык и личные параметры.
Тестирование поиска	Проверка нахождения фрагментов по контрольному запросу.

Приложение Г (обязательное)

Маршрут первого ввода в эксплуатацию

Таблица применяется как сквозной маршрут. Переход к следующему этапу допускается только после выполнения критерия предыдущего этапа.

Этап	Раздел	Действие	Критерий перехода
1	3–4	Выбрать вариант размещения, утвердить матрицу версий, рассчитать ресурсы, адреса, тома, сетевые правила и ответственных.	Заполнена карточка установки; сочетание версий утверждено; ресурсы выделены.
2	4.4–4.6, 5.2.1 или 5.3.1	Проверить узел либо кластер и фактические версии операционной системы, Kubernetes и Deckhouse.	Все критерии допуска выполнены; вывод проверок приложен к протоколу.
3	5.2.2–5.2.3 или 5.3.2–5.3.3	Подготовить параметры, секреты, адреса и свидетельства.	Нет стандартных секретов; имена разрешаются.
4	5.2.4 или 5.3.4	Установить и запустить службы.	Все обязательные службы готовы.
5	5.3.5 и 6.1.1	Получить данные и выполнить первый вход.	Доступна «Консоль администратора».
6	6.2	Выбрать русский язык.	Основные разделы отображаются по-русски.
7	6.4.1	Создать организацию.	Организация присутствует после обновления.
8	7.1.1–7.1.2	Создать администратора организации и пользователей.	Роли совпадают с заявками.
9	6.3.1–6.3.3	Подключить и назначить модели.	Контрольный запрос к моделям успешен.
10	8.1.1	Создать тестовую базу знаний.	Язык, доступ, модель и метод сохранены.
11	8.2.1	Загрузить и обработать контрольные документы.	Состояние «УСПЕШНО», фрагменты проверены.
12	8.3.1	Выполнить контрольный поиск.	Правильные источники входят в первые результаты.
13	8.6.1	Создать и протестировать помощника.	Положительный и отрицательный вопросы пройдены.
14	9.2.1	Проверить наблюдение и журналы.	Карточки зелёные, события поступают.
15	10	Создать и пробно восстановить копию.	Подписан протокол восстановления; достигнуты нормативы потери данных и времени восстановления.
16	5.3.6–5.3.7	Если заявлена отказоустойчивость, проверить распределение и управляемый отказ узла.	Простой и потеря данных не превышают утверждённых значений.

Этап	Раздел	Действие	Критерий перехода
17	Приложение А	Заполнить контрольный лист.	Получено решение о вводе в эксплуатацию.

Приложение Д (рекомендуемое)

Безопасные образцы параметров

Образцы показывают обязательные группы параметров и не заменяют файл конкретного выпуска. Значения в угловых скобках должны быть заменены. Пароли из документа не копируются; для каждой среды создаются новые.

Д.1 Образец основных параметров при установке на одном сервере

```
DOC_ENGINE=infinity
POSTGRES_USER=semantix_app
POSTGRES_DBNAME=semantix
POSTGRES_PASSWORD=<создать_уникальный_секрет>
MINIO_USER=semantix_storage
MINIO_PASSWORD=<создать_другой_уникальный_секрет>
REDIS_PASSWORD=<создать_третий_уникальный_секрет>
TIMEZONE=Europe/Moscow
REGISTER_ENABLED=0
DOC_BULK_SIZE=4
EMBEDDING_BATCH_SIZE=16
MAX_CONTENT_LENGTH=1073741824
```

Пароли и ключи не должны совпадать. Если значение содержит специальные символы, способ экранирования сверяется с правилами файла текущего выпуска. Файл должен иметь права 600.

Д.2 Образец ключевых параметров кластерной установки

```
imagePullSecrets:
  - name: semantix-registry-pull
dockerRegistrySecret:
  create: false
env:
  DOC_ENGINE: infinity
  DB_TYPE: postgres
  POSTGRES_USER: semantix_app
  POSTGRES_DBNAME: semantix
  POSTGRES_PASSWORD: <получить_из_закрытого_файла>
  MINIO_ROOT_USER: semantix_storage
  MINIO_PASSWORD: <получить_из_закрытого_файла>
  REDIS_PASSWORD: <получить_из_закрытого_файла>
  DEFAULT_ADMIN_EMAIL: admin@<домен_организации>
  DEFAULT_ADMIN_PASSWORD: ""
  TIMEZONE: Europe/Moscow
backend:
```

```

replicaCount: 2
resources:
  requests: {cpu: "1", memory: "2Gi"}
  limits: {cpu: "4", memory: "8Gi"}
taskExecutor:
  enabled: true
  replicaCount: 2
  workers: 1
ingress:
  enabled: true
  className: nginx
  hosts: [{host: <полное_доменное_имя>}]
  tls: [{secretName: semantix-tls, hosts: [<полное_доменное_имя>]}]
audit:
  enabled: true
  retentionDays: <утверждённый_срок_в_сутках>

```

Запись `DEFAULT_ADMIN_PASSWORD: ""` означает однократное автоматическое создание пароля пакетной установкой. Получить его следует по процедуре 5.3.5. В промышленной среде запросы и пределы ресурсов назначаются всем службам, а не только прикладной службе.

Приложение Е (справочное)

Нормативные документы и сведения о совместимости

Документ или источник	Использование в руководстве
Описание применения Semantix	Наименование, назначение, область применения и термины предметной области.
ГОСТ 19.105-78. Общие требования к программным документам	Правила построения и оформления текстового программного документа.
ГОСТ 19.503-79. Руководство системного программиста	Состав сведений об установке, проверке, настройке и эксплуатации системной части программы.
Deckhouse Kubernetes Platform. Поддерживаемые версии	Поддерживаемые версии Astra Linux Special Edition и РЕД ОС: https://deckhouse.ru/products/kubernetes-platform/documentation/v1/reference/supported_versions.html
Astra Linux. Администрирование средств контейнеризации	Подготовка Astra Linux Special Edition 1.7 и 1.8 к запуску контейнеров: https://wiki.astralinux.ru/pages/viewpage.action?pageId=158601444
РЕД ОС 8. Установка и настройка Docker	Подготовка установки на одном сервере на РЕД ОС: https://redos.red-soft.ru/base/redos-8_0/8_0-administration/8_0-containers/8_0-docker-install/
РЕД ОС 8. Kubernetes	Подготовка стандартного кластера Kubernetes на РЕД ОС: https://redos.red-soft.ru/base/redos-8_0/8_0-administration/8_0-containers/8_0-kubernetes/8_0-kuber/