Инструкция по установке СК-11 11.7.1 и «СК11.Equipment Inspection Logbook» («СК11.Обходы»)

дата редакции: Декабрь, 2023

Авторские, имущественные права и общие положения по использованию документа

Настоящий документ пересматривается на регулярной основе с внесением всех необходимых исправлений и дополнений в следующие выпуски.

Предприняты все меры для того, чтобы содержащаяся здесь информация была максимально актуальной и точной, тем не менее, компания Монитор Электрик не несёт ответственности за ошибки или упущения, а также за любой ущерб, причинённый в результате использования содержащейся здесь информации.

О технических неточностях или опечатках вы можете сообщить в Службу технической поддержки Монитор Электрик. Мы будем рады вашим замечаниям и предложениям.

Содержание данного документа может быть изменено без предварительного уведомления. Перед использованием убедитесь, что это актуальная версия, соответствующая версии использующейся системы. Для получения актуальной версии вы можете обратиться по адресам, указанным на сайте www.monitel.ru.

Названия продуктов и компаний, упомянутые здесь, могут являться торговыми марками соответствующих владельцев.

Продукция, для которой разработана настоящая документация (документ) является сложным прикладным программным обеспечением, которое далее будет именоваться «Программный продукт».

Компания Монитор Электрик оставляет за собой право внесения любых изменений в настоящую документацию.

Гарантия

Компания Монитор Электрик гарантирует устранение выявленных в Программном продукте дефектов. Исправленные версии Программного продукта предоставляются в виде обновления.

Дефектом признаётся отклонение функциональности Программного продукта от соответствующего описания, приведённого в настоящей документации, препятствующее нормальной эксплуатации Программного продукта, при условии соблюдения требований к организации эксплуатации, приведённых в настоящей документации. Допускается несущественное различие фактической функциональности Программного продукта и описания, приведённого в настоящей документации, при условии, что это не влияет значимым образом на процесс эксплуатации.

Правила безопасной эксплуатации и ограничение ответственности

Программный продукт функционирует в составе системы, включающей помимо самого Программного продукта компьютерное аппаратное обеспечение, системное и специальное программное обеспечение, сегменты вычислительной сети – далее совместно именуемые инфраструктурой. Современная инфраструктура, в которой функционирует Программный продукт, включает сложное аппаратное и программное обеспечение, которое может модернизироваться и обновляться независимо от Программного продукта. Поэтому для безопасной и бесперебойной эксплуатации Программного продукта перед вводом его в постоянную эксплуатацию должна быть разработана эксплуатационная документация на систему в целом. Настоящий документ предназначен для облегчения пользователю (эксплуатирующей организации) задачи разработки собственной эксплуатационной документации на систему.

Для повышения безопасности и бесперебойности эксплуатации систем на базе Программного продукта необходимо выполнять следующие основные требования по организации эксплуатации (другие требования и рекомендации могут содержаться в соответствующих разделах документа):

- Реализация и эксплуатация автоматизированных систем, в составе которых функционирует Программный продукт, должны осуществляться на основе проектной документации, при разработке которой проработаны и согласованы с эксплуатирующей организацией все вопросы совместимости и интеграции компонентов, включая Программный продукт.
- Эксплуатация Программного продукта должна проводиться в соответствии с эксплуатационной документацией эксплуатирующей организации, а также рекомендациями Службы технической поддержки Монитор Электрик.
- В эксплуатационной документации должен быть описан механизм взаимодействия специалистов эксплуатирующей организации (администраторы, пользователи) со Службой технической поддержки Монитор Электрик, включая регламент выполнения рекомендаций и подготовки ответов на запросы дополнительной информации Службы технической поддержки Монитор Электрик в ходе штатной эксплуатации и устранения нарушений в работе Программного продукта.
- Запрещено использование нештатных средств, не входящих в состав Программного продукта или не описанных в эксплуатационной документации, в том числе инструментов для внесения изменений в базы данных Программного продукта.
- Аппаратное обеспечение, системное программное обеспечение, внешнее программное обеспечение, взаимодействующее с Программным продуктом или работающее на общей с ним аппаратной платформе, а также другая ИТ-инфраструктура, обеспечивающая работу Программного продукта, должны быть совместимы с эксплуатируемой версией Программного продукта и функционировать без сбоев.
- В соответствии с эксплуатационной документацией и внутренними регламентами эксплуатирующей организации, с определённой периодичностью должны выполняться следующие профилактические мероприятия:
  - перезагрузка серверов и клиентских рабочих станций, на которых установлен Программный продукт;
  - установка критически важных обновлений системного программного обеспечения, внешнего программного обеспечения, взаимодействующего с Программным продуктом или работающего на общей с ним аппаратной платформе;
  - обновление антивирусных БД на серверах и клиентских рабочих станциях, на которых установлен Программный продукт;
  - проверка и обеспечение достаточности аппаратных ресурсов;

- проверка журналов операционной системы и Программного продукта на наличие записей об ошибках и устранение причин их возникновения;
- мониторинг корректной работы сетевого оборудования ЛВС, которое участвует в обмене данными между компонентами Программного продукта, а также между Программным продуктом и внешними системами.

- Регламент (периодичность, условия) выполнения профилактических мероприятий определяется эксплуатирующей организацией самостоятельно в зависимости от условий эксплуатации с учётом рекомендаций, приведённых в настоящей документации, и рекомендаций Службы технической поддержки Монитор Электрик при их наличии.
- При использовании Программного продукта для выполнения важных операций, которые могут привести к возникновению значительных убытков или связаны с рисками для жизни и здоровья людей, пользователь Программного продукта должен убедиться в том, что Программный продукт и инфраструктура функционируют в штатном режиме, без сбоев, а после завершения операции – убедиться в том, что она выполнена корректно.
- Все значимые для обеспечения безопасной эксплуатации Программного продукта регламентные операции и профилактические мероприятия, а также факты проверки готовности системы к выполнению важных операций и факты успешного выполнения важных операций должны фиксироваться в оперативном журнале эксплуатации или подтверждаться другим надёжным способом – на усмотрение эксплуатирующей организации. Эксплуатирующая организация должна предоставлять копии и выписки из оперативного журнала эксплуатации по запросу Службы технической поддержки Монитор Электрик.

Компания Монитор Электрик не несёт ответственности за упущенную экономическую выгоду, убытки или претензии третьих лиц, включая любые прямые, косвенные, случайные, специальные, типичные или вытекающие убытки (включая, но не ограничиваясь, утрату возможности использования, потерю данных или прибыли, прекращение деятельности), произошедшие при любой схеме ответственности, возникшие вследствие использования или невозможности использования Программного продукта, даже если о возможности такого ущерба было заявлено.

Оглавление

1. Установка серверной части на платформе Linux

В процессе установки СК-11 на платформе Linux выполняется развёртывание серверной части Системы, баз данных на подготовленных серверах с созданием домена СК-11.

Домен – группа SCADA/EMS серверов, изолированная от другой группы, которая выполняет определённый набор функций таких как: работа в темпе процесса, тренажёр, испытательный полигон и т.д.

Возможны следующие схемы развёртывания домена СК-11, в зависимости от количества серверных узлов домена СК-11, определяющие разницу в подготовке сертификатов, keytab-файлов и настройки инвентаря *Ansible*:

Перед началом работ по подготовке к установке серверной части Системы рекомендуется ознакомиться с разделом справочной системы "Организация распределения и балансировки серверных ресурсов".

Точки подключения WEB_EP и SCADA_EP необходимы для взаимодействия с доменом СК-11:

- точка доступа SCADA_EP позволяет переадресовывать запросы к веб-сервисам СК-11 на сервере или группе серверов приложений оперативного контура, составляющих группу "Основная группа";
- точка доступа WEB_EP позволяет переадресовывать запросы к веб-сервисам СК-11 на сервере или группе серверов веб-приложений, составляющих группу "Веб-сервисы".

- **Шесть серверных узлов;**

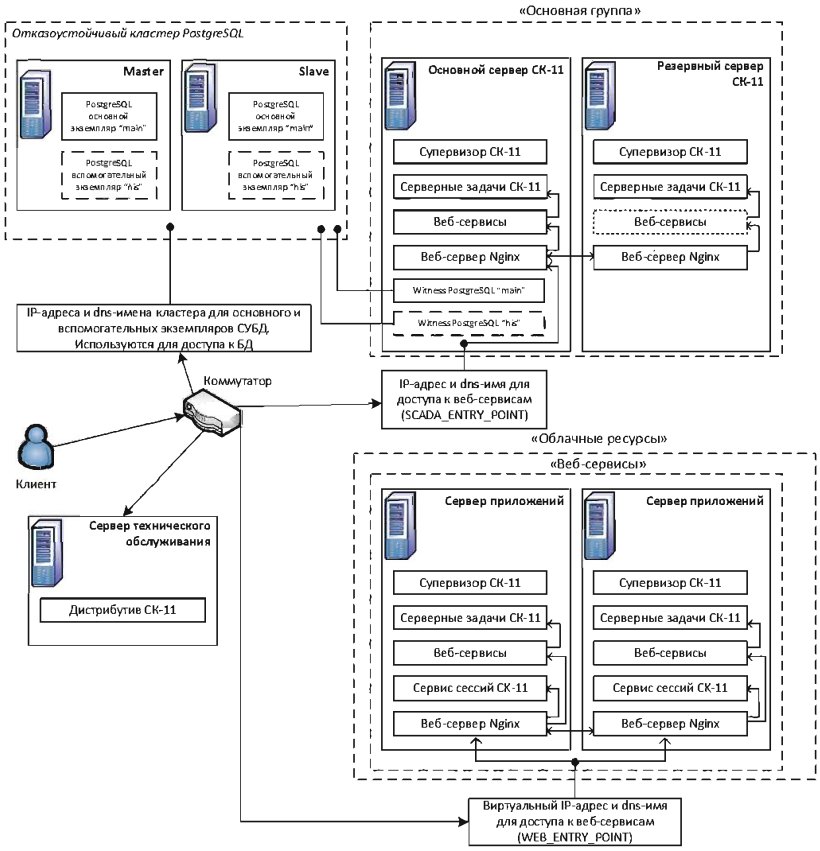


Рис. 1. Схема развёртывания домена СК-11 на шести узлах

Отказоустойчивость группы "Основная группа" реализуется направлением запросов к основному серверному узлу (master) группы по адресу точки доступа SCADA_EP. Управление переадресацией точки доступа выполняется средствами серверного приложения "Служба управления задачами СК-11" (СК-11 Supervisor) за счёт привязки IP точки доступа к сетевому интерфейсу сервера, который в данный момент является основным в домене СК-11;

Отказоустойчивость группы "Веб-сервисы" реализуется использованием программы *HAProxy*.

- **Три серверных узла;**

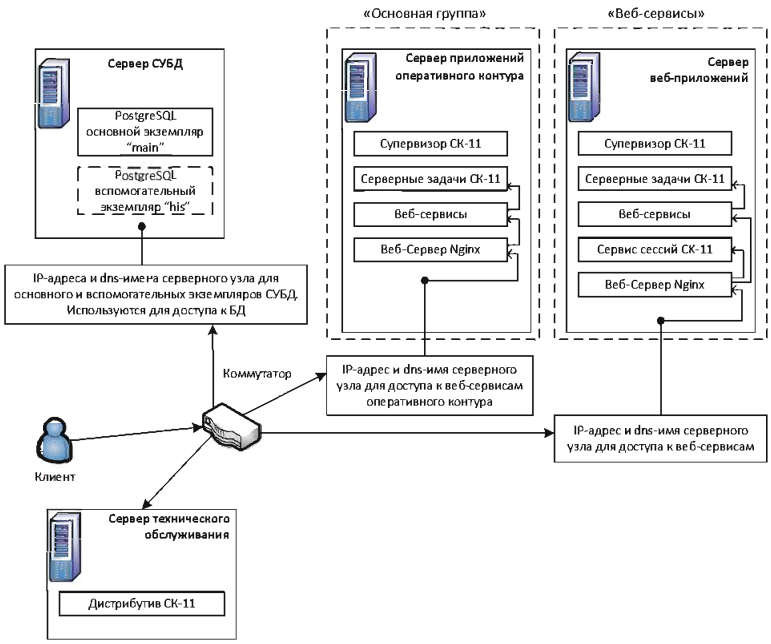


Рис. 2. Схема развёртывания домена СК-11 на трёх узлах

- **Один серверный узел.**

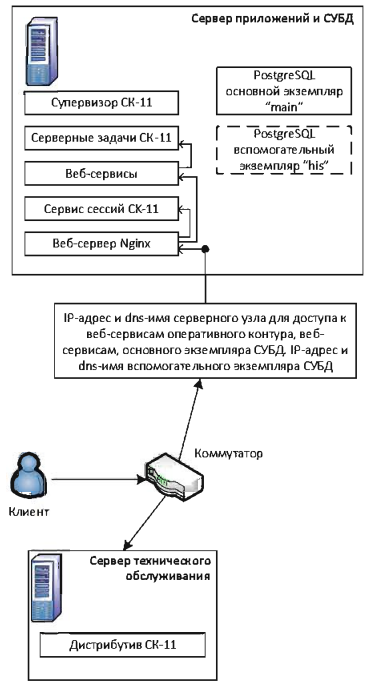


Рис. 3. Схема развёртывания домена СК-11 на одном узле

- **Служба каталогов:**
  - *Microsoft Active Directory (MS AD)*;
  - *FreeIPA*.

При использовании *Службы каталогов FreeIPA* не поддерживается конфигурация развёртывания с клиентскими компьютерами на платформе *Windows*.

В варианте развёртывания домена СК-11 со *Службой каталогов MS AD* предполагается наличие установленного и настроенного контроллера *Службы каталогов* до начала установки Системы.

При использовании *Службы каталогов FreeIPA* возможны следующие варианты конфигурации развёртывания СК-11:

- Контроллер *Службы каталогов FreeIPA* уже установлен и настроен на отдельном серверном узле, выполняется установка только домена СК-11;
- Контроллер *Службы каталогов FreeIPA* и домен СК-11 устанавливаются и настраиваются одновременно дистрибутивом Системы. Контроллер *Службы каталогов* устанавливается на отдельном серверном узле;
- Контроллер *Службы каталогов FreeIPA* и домен СК-11 устанавливаются и настраиваются одновременно дистрибутивом Системы на одном серверном узле. Данная конфигурация применяется только для конфигурации развёртывания домена СК-11 с одним серверным узлом.

Процесс установки СК-11 представляет из себя автоматизированную настройку окружения и развёртывание ПО средствами системы управления конфигурациями Ansible.

Перед началом установки рекомендуется ознакомиться с описанием системы *Ansible* и изучить формат YAML во избежание проблем установки, связанных с ошибками синтаксиса, которые могут быть внесены администратором в процессе описания параметров установки.

Входные параметры установки описываются в так называемом *инвентаре Ansible* – наборе файлов в формате YAML, в которых определяются значения переменных.

Установка разделена на несколько этапов, соответствующих выполнению команды "`make`", которая запускает установку компонентов Системы по сценариям (плейбукам), описанным в формате `YAML`:

`make bootstrap` – выполняет развёртывание репозиториев с вспомогательным ПО, распаковку модулей СК-11 из дистрибутива, первичную настройку ОС и сети на серверах, установку обновлений ОС и средств разработки.

`make play` – выполняет установку серверной части СК-11, копируя модули на серверы, регистрирует службы и т.д. Выполняет развёртывание СУБД *PostgreSQL*, создание кластера при необходимости использования решений высокой доступности БД, развёртывание БД СК-11. Для развёртывания баз данных Системы создаётся два экземпляра (instance) *PostgreSQL*: main и his. Экземпляр main состоит из узлов (одно узла при отсутствии кластера), имена которых соответствуют именами серверов, на которых они развёрнуты. На данном экземпляре хранятся все БД СК-11, кроме БД архива оперативной информации "his". Доступ к БД, развёрнутым на экземпляре main, выполняется по имени прослушивателя данного экземпляра. Экземпляр his состоит из узлов (одно узла при отсутствии кластера), имена которых создаются в службе каталогов отдельно, и которые развёрнуты на тех же серверах, что и узлы экземпляра main. На

данном экземпляре хранится БД архива оперативной информации. Доступ к БД his выполняется по имени прослушивателя экземпляра *PostgreSQL* "his".

Далее последовательно описаны этапы подготовки и установки СК-11 на платформе Linux:

1. Подготовка к установке;
2. Подготовка сервера технического обслуживания;
3. Настройка инвентаря Ansible;
4. Установка программного обеспечения СК-11;
5. Настройка Справочной системы.

Отдельно рассмотрен вариант установки программного обеспечения СК-11 с предустановленной СУБД PostgreSQL.

1.1. Подготовка к установке

При планировании установки Системы необходимо определить целевую архитектуру и количество применяемых серверов, используемую *Службу каталогов* и наличие её контроллера.

В рамках подготовки к установке серверной части Системы на платформе *Linux* необходимо выполнить следующие работы и произвести соответствующую настройку:

- запросить у системных администраторов организации имена и адреса серверов точного времени (ntp);
- создание DNS-записей для имён серверов, групп серверов, а также имён прослушивателей кластера *PostgreSQL*;
- установка и первичная настройка ОС на серверных узлах домена СК-11.

При конфигурации развёртывания с существующим контроллером *Службы каталогов (MS AD/FreeIPA)* дополнительно необходимо выполнить следующие работы:

- запросить у системных администраторов организации имена и адреса контроллеров домена Службы каталогов (dc);
- подготовка сертификатов для обеспечения работоспособности веб-сервисов и служб СК-11 по протоколу HTTPS;
- подготовка keytab-файлов для возможности аутентификации с помощью Kerberos.

Keytab-файл – это файл, содержащий пары Kerberos принципалов и их ключей (полученных с использованием Kerberos пароля). Эти файлы используются для аутентификации в системах, использующих Kerberos, без ввода пароля.

В случае конфигурации развёртывания с установкой контроллера *Службы каталогов FreeIPA* описанные выше действия по подготовке сертификатов и keytab-файлов выполняются инсталлятором в автоматизированном режиме.

В дочерних разделах подробно рассмотрены указанные выше работы:

- Создание DNS-записей.
- Подготовка SSL-сертификатов.
- Подготовка keytab-файлов для аутентификации через Kerberos.
- Установка ОС Astra Linux SE 1.7 на серверные узлы.
- Первичная настройка ОС Astra Linux.

1.1.1. Создание DNS-записей

Для работы платформы СК-11 необходимо выполнить следующую настройку DNS-записей в зависимости от конфигурации развёртывания:

1. Создать DNS-записи серверов приложений СК-11, серверов *PostgreSQL* и сервера технического обслуживания. Рекомендуемые форматы имён серверов соответственно:
    1. `*-scada1` – все конфигурации (узел обозначается в конфигурации *Ansible* псевдонимом – `host-scada-01`);

2. `*-scada2` – конфигурация с шестью серверными узлами (узел обозначается в конфигурации *Ansible* псевдонимом – `host-scada-02`);
3. `*-web1` – конфигурация с тремя и шестью серверными узлами (узел обозначается в конфигурации *Ansible* псевдонимом – `host-web-01`);
4. `*-web2` – конфигурация с шестью серверными узлами (узел обозначается в конфигурации *Ansible* псевдонимом – `host-web-02`);
5. `*-pg1` – конфигурация с тремя и шестью серверными узлами (узел обозначается в конфигурации *Ansible* псевдонимом – `host-pg-01`);
6. `*-pg2` – конфигурация с шестью серверными узлами (узел обозначается в конфигурации *Ansible* псевдонимом – `host-pg-02`);
7. `*-pg-his1` – все конфигурации (узел обозначается в конфигурации *Ansible* псевдонимом – `host-pg-his-01`);
8. `*-pg-his2` – конфигурация с шестью серверными узлами (узел обозначается в конфигурации *Ansible* псевдонимом – `host-pg-his-02`);
9. `*-deployer` – все конфигурации (узел обозначается в конфигурации *Ansible* псевдонимом – `host-deployer`);
10. *-`freeipa` – все конфигурации с установкой контроллера *Службы каталогов FreeIPA* на выделенный серверный узел (узел обозначается в конфигурации *Ansible* псевдонимом – `host-freeipa`).

Необходимость вспомогательного экземпляра "his" *PostgreSQL* для БД "Архив БДРВ" (HIS) определяется наличием опции лицензии "his" в файле лицензии платформы СК-11. Если указанная опция отсутствует, то регистрация DNS-записей pg-his-01, pg-his-02, pg-his-lst не требуется.

2. Создать статическую (static) DNS-запись для группы веб-серверов с IP-адресом из той же сети, что и основные IP-адреса серверов приложений домена СК-11, для конфигурации с шестью серверными узлами. Рекомендуемый формат имени: *-web (группа обозначается в конфигурации *Ansible* псевдонимом – `host-web`).
3. Создать статическую (static) DNS-запись для основной группы серверов приложений с IP-адресом из той же сети, что и основные IP-адреса серверов приложений домена СК-11, для конфигурации с шестью серверными узлами. Рекомендуемый формат имени: *-scada (группа обозначается в конфигурации *Ansible* псевдонимом – `host-scada`).
4. Создать статическую (static) DNS-запись для имени прослушивателя кластера основного *PostgreSQL* экземпляра (main) с IP-адресом из той же сети, что и основные IP-адреса серверов приложений домена СК-11, для конфигурации с шестью серверными узлами. Рекомендуемый формат имени: *-pg-lst (прослушиватель экземпляра main обозначается в конфигурации *Ansible* псевдонимом – `host-pg-lst`).
5. Создать статическую (static) DNS-запись для имени прослушивателя кластера *PostgreSQL* экземпляра "his" с IP-адресом из той же сети, что и основные IP-адреса серверов приложений домена СК-11, для конфигурации с шестью серверными узлами. Рекомендуемый формат имени: *-pg-his-lst (прослушиватель экземпляра his обозначается в конфигурации Ansible псевдонимом – host-pg-his-lst).

6. Обеспечить корректное разрешение созданных DNS-записей всеми используемыми DNS-серверами в прямой и обратной зонах.

DNS-записи имён серверов и точек подключения должны соответствовать правилам (RFC 952, RFC 1123). Они должны начинаться с буквы или цифры, заканчиваться буквой или цифрой и иметь внутри символы только букв, цифр, допускается использования внутри символа дефиса (-). Следует обратить внимание, что символ подчёркивания (_) может использоваться в начале имени и внутри имени в зависимости от спецификации применяемого DNS-сервера, по спецификации RFC 1123 символ подчёркивания может использоваться только в начале имени. Использование символа подчёркивания рекомендуется избегать.

Не допускается использование символов SDDL и зарезервированных имён.

Минимальная длина имени: 2 символа. Максимальная длина имени: 15 символов, в соответствии с ограничениями для протокола NetBIOS (RFC 1002).

1.1.2. Подготовка SSL-сертификатов

Действие SSL-сертификатов ограничено по времени. В случае истечения срока действия сертификатов Система становится неработоспособной по причине отсутствия возможности проверки прав пользователей на работу с приложениями.

В целях недопущения неработоспособности Системы администратору необходимо следить за сроком действия SSL-сертификатов. В случае необходимости следует заранее подготовить новые сертификаты и своевременно выполнить их замену на серверных узлах домена СК-11.

Для обеспечения взаимодействия компонентов Системы с использованием протокола HTTPS необходимы SSL сертификаты, выпущенные доверенным *Удостоверяющим центром* (*Certification authority*).

Условные обозначения:

- `host-depoler.domain.local` – полное имя сервера технического обслуживания;
- `host-scada-01.domain.local` – полное имя первого узла сервера приложений для конфигурации с шестью узлами, полное имя узла сервера приложений для конфигурации с одним или тремя узлами;
- `host-scada-02.domain.local` – полное имя второго узла сервера приложений для конфигурации с шестью узлами;
- `host-web-01.domain.local` – полное имя первого узла веб-приложений для конфигурации с шестью узлами, полное имя узла веб-приложений для конфигурации с тремя узлами;
- `host-web-02.domain.local` – полное имя второго узла веб-приложений для конфигурации с шестью узлами.

В зависимости от конфигурации развёртывания точкой подключения WEB_EP является:

- для конфигурации с шестью узлами имя группы веб-серверов `host-web`;
- для конфигурации с тремя узлами имя сервера `host-web-01.domain.local`;
- для конфигурации с одним узлом имя сервера `host-scada-01.domain.local`.

Состав необходимых сертификатов включает себя:

1. Файлы сертификата для сервера технического обслуживания. Поле Subject должно содержать атрибут Common Name (CN) со значением, соответствующим полному сетевому имени (FQDN) имя сервера технического обслуживания. SSL-сертификат должен быть разделён на два файла:
   - `[host-depoler.domain.local].private_key.pem` – содержит только личный ключ (`private key`);
   - `[host-depoler.domain.local].pem` – содержит сертификат и личный ключ, включая атрибуты.

   В именах файлов [`host-depoler.domain.local`] следует заменить на полное имя (FQDN) сервера технического обслуживания. Требования к заполнению реквизитов сертификата:
   - поле Subject должно содержать атрибут Common Name (CN) со значением, соответствующим полному сетевому имени (FQDN) сервера технического обслуживания;
   - поле Subject Alternative Name (SAN) должно содержать краткое и полное DNS-имя сервера `host-depoler`.
2. Файл корневого сертификата домена *Службы каталогов* `root.##domain.local##.crt`, где `##domain.local##` – полное имя домена *Службы каталогов*.
3. Файлы сертификата для веб-сервисов и служб СК-11. Требования к сертификату различаются в зависимости от целевой конфигурации развёртывания домена СК-11:

Шесть серверных узлов

SSL-сертификат должен быть разделён на два файла:

- `[host-web.domain.local].private_key.pem` – содержит только личный ключ (`private key`);
- `[host-web.domain.local].pem` – содержит сертификат и личный ключ, включая атрибуты.

В именах файлов [`host-web.domain.local`] следует заменить на полное имя (FQDN) имя основной группы. Требования к заполнению реквизитов сертификата:

- поле Subject должно содержать атрибут Common Name (CN) со значением, соответствующим полному сетевому имени (FQDN) основной группы;

- поле Subject Alternative Name (SAN) должно содержать все краткие и полные DNS-имена серверов `host-scada-01`, `host-scada-02`, `host-web-01`, `host-web-02` и объединяющих их имена групп `host-scada`, `host-web`.

Три серверных узла

SSL-сертификат должен быть разделён на два файла:

- `[host-web-01.domain.local].private_key.pem` – содержит только личный ключ (`private key`);
- `[host-web-01.domain.local].pem` – содержит сертификат и личный ключ, включая атрибуты.

В именах файлов [`host-web-01.domain.local`] следует заменить на полное имя (FQDN) серверного узла для веб-приложений Системы. Требования к заполнению реквизитов сертификата:

- поле Subject должно содержать атрибут Common Name (CN) со значением, соответствующим полному сетевому имени (FQDN) серверного узла для веб-приложений Системы;
- поле Subject Alternative Name (SAN) должно содержать все краткие и полные DNS-имена серверов `host-scada-01`, `host-web-01`.

Один серверный узел

SSL-сертификат должен быть разделён на два файла:

- `[host-scada-01.domain.local].private_key.pem` – содержит только личный ключ (`private key`);
- `[host-scada-01.domain.local].pem` – содержит сертификат и личный ключ, включая атрибуты.

В именах файлов [`host-scada1.domain.local`] следует заменить на полное имя (FQDN) серверного узла приложений и СУБД Системы. Требования к заполнению реквизитов сертификата:

- поле Subject должно содержать атрибут Common Name (CN) со значением, соответствующим полному сетевому имени (FQDN) серверного узла приложений и СУБД Системы;
- поле Subject Alternative Name (SAN) должно содержать краткое и полное DNS-имя сервера `host-scada-01`.

Общие требования к файлам сертификата

SSL-сертификат должен быть выпущен с использованием алгоритмов семейства SHA-2 или SHA-3. Например, SHA256.

Сертификат *Удостоверяющего центра* (*Certification authority*), с помощью которого были выпущены SSL-сертификаты для серверов СК-11, должен быть в списке доверенных корневых центров сертификации (Trusted Root Certification Authorities) на всех серверах домена СК-11 и на всех клиентских компьютерах.

1.1.3. Подготовка keytab-файлов для аутентификации через Kerberos

Процесс подготовки keytab-файлов для аутентификации через Kerberos отличается в зависимости от целевой конфигурации развёртывания домена СК-11:

Условные обозначения:

- `host-scada-01.domain.local` – полное имя первого узла сервера приложений для конфигурации с шестью узлами, полное имя узла сервера приложений для конфигурации с тремя узлами. Для конфигурации с одним узлом имя используется для узла сервера приложений и СУБД;
- `host-web-01.domain.local` – полное имя первого узла веб-приложений для конфигурации с шестью узлами, полное имя узла веб-приложений для конфигурации тремя узлами;
- `host-web-02.domain.local` – полное имя второго узла веб-приложений для конфигурации с шестью узлами
- `host-pg-01.domain.local` – полное имя узла (первого узла кластера) основного (main) экземпляра *PostgreSQL*, полное имя сервера СУБД для конфигурации с тремя узлами;
- `host-pg-02.domain.local` – полное имя второго узла основного (main) экземпляра *PostgreSQL* для конфигурации с шестью узлами;
- `host-pg-lst.domain.local` – полное имя прослушивателя кластера *PostgreSQL* основного экземпляра "main" для конфигурации с шестью узлами;
- `host-pg-his-01.domain.local` – полное имя узла (первого узла кластера) экземпляра "his" *PostgreSQL*. Для конфигурации с одним или тремя узлами используется для виртуального имени экземпляра "his" *PostgreSQL*;
- `host-pg-his-02.domain.local` – полное имя второго узла экземпляра "his" для кластера *PostgreSQL* для конфигурации с шестью узлами;
- `host-pg-his-lst.domain.local` – полное имя прослушивателя кластера *PostgreSQL* экземпляра "his" для конфигурации с шестью узлами.

Необходимость вспомогательного экземпляра "his" *PostgreSQL* для БД "Архив БДРВ" (HIS) определяется наличием опции лицензии "his" в файле лицензии платформы СК-11. Если указанная опция отсутствует, то генерация keytab-файла для экземпляра *PostgreSQL* "his" не требуется.

Шесть серверных узлов

Процесс подготовки keytab-файлов для аутентификации через Kerberos отличается в зависимости от используемой *Службы каталогов*:

Microsoft Active Directory

1. В *Службе каталогов MS AD* создать отдельные учётные записи пользователя для использования службами *postgres* и *http*:

   `domain.local\httpservice`

   `domain.local\postgresservice`

2. Зарегистрировать SPN для служб postgres и HTTP на соответствующие учётные записи пользователей:

   `HTTP/host-web.domain.local, HTTP/host-web-01.domain.local, HTTP/host-web-02.domain.local`

   `postgres/host-pg-lst.domain.local, postgres/host-pg-01.domain.local, postgres/host-pg-02.domain.local`

   `postgres/host-pg-his-lst.domain.local, postgres/host-pg-his-01.domain.local, postgres/host-pg-his-02.domain.local`

   a. Для служб *postgres* и *http* следует регистрировать SPN для каждого узла и для кластерного имени на одну и ту же учётную запись пользователя (`domain.local\postgresservice`, `domain.local\httpservice`).

3. Сформировать три (два, при отсутствии экземпляра "his" *PostgreSQL*) keytab-файла:

   `HTTP@host-web.domain.local.keytab`

   `postgres@host-pg-lst.domain.local.keytab`

   `postgres@host-pg-his-lst.domain.local.keytab`

   Keytab-файл `HTTP@host-web.domain.local.keytab` соответствует принципалу `HTTP/host-web.domain.local, HTTP/host-web-01.domain.local, HTTP/host-web-02.domain.local` и пользователю `domain.local\httpservice`

   Keytab-файл (multiple principal keytab) `postgres@host-pg-lst.domain.local.keytab` соответствует принципалам `postgres/host-pg-lst.domain.local, postgres/host-pg-01.domain.local, postgres/host-pg-02.domain.local` и пользователю `domain.local\postgresservice`

   Keytab-файл (multiple principal keytab) `postgres@host-pg-his-lst.domain.local.keytab` соответствует принципалам `postgres/host-pg-his-lst.domain.local, postgres/host-pg-his-01.domain.local, postgres/host-pg-his-02.domain.local` и пользователю `domain.local\postgresservice`

MIB Kerberos

1. В случае использования в качестве каталога *MIB Kerberos*, например, на *FreeIPA* (*Astra Linux*), в каталоге создаются учётные записи узлов:

```
host-web.domain.local
host-web-01.domain.local
host-web-02.domain.local
host-pg-lst.domain.local
host-pg-01.domain.local
host-pg-02.domain.local
host-pg-his-lst.domain.local
host-pg-his-01.domain.local
host-pg-his-02.domain.local
```

2. Далее создаются учётные записи служб:

```
HTTP/host-web.domain.local
HTTP/host-web-01.domain.local
HTTP/host-web-02.domain.local
postgres/host-pg-lst.domain.local
postgres/host-pg-01.domain.local
postgres/host-pg-02.domain.local
postgres/host-pg-his-lst.domain.local
postgres/host-pg-his-01.domain.local
postgres/host-pg-his-02.domain.local
```

3. Для перечисленных служб генерируются три (два, при отсутствии экземпляра "his" *PostgreSQL*) keytab-файла:

   `HTTP@host-web.domain.local.keytab`, (multiple principal keytab), соответствующий принципалам `HTTP/host-web.domain.local`, `HTTP/host-web-01.domain.local`, `HTTP/host-web-02.domain.local`

   `postgres@host-pg-lst.domain.local.keytab`, (multiple principal keytab), соответствующий принципалам `postgres/host-pg-lst.domain.local`, `postgres/host-pg-01.domain.local`, `postgres/host-pg-02.domain.local`

   `postgres@host-pg-his-lst.domain.local.keytab`, (multiple principal keytab), соответствующий принципалам `postgres/host-pg-his-lst.domain.local`, `postgres/host-pg-his-01.domain.local`, `postgres/host-pg-his-02.domain.local`

Три серверных узла

Процесс подготовки keytab-файлов для аутентификации через Kerberos отличается в зависимости от используемой *Службы каталогов*:

Microsoft Active Directory

1. В Службе каталогов домена MS AD создать отдельные учётные записи пользователя для использования службами *postgres* и *http*:

   `domain.local\httpservice`

   `domain.local\postgresservice`

2. Зарегистрировать SPN для служб postgres и HTTP на соответствующие учётные записи пользователей:

   `HTTP/host-web-01.domain.local`

   `postgres/host-pg-01.domain.local`

   `postgres/host-pg-his-01.domain.local`

3. Сформировать три (два, при отсутствии экземпляра "his" *PostgreSQL*) keytab-файла:

   `HTTP@host-web-01.domain.local.keytab`

   `postgres@host-pg-01.domain.local.keytab`

   `postgres@host-pg-his-01.domain.local.keytab`

   Keytab-файл `HTTP@host-web-01.domain.local.keytab` соответствует принципалу `HTTP/host-web-01.domain.local` и пользователю `domain.local\httpservice`.

   Keytab-файл `postgres@host-pg-01.domain.local.keytab` соответствует принципалу `postgres/host-pg-01.domain.local` и пользователю `domain.local\postgresservice`.

   Keytab-файл `postgres@host-pg-his-01.domain.local.keytab` соответствует принципалу `postgres/host-pg-his-01.domain.local` и пользователю `domain.local\postgresservice`.

MIB Kerberos

1. В случае использования в качестве каталога *MIB Kerberos*, например, на *FreeIPA* (*Astra Linux*), в каталоге создаются учётные записи узлов:

   `host-web-01.domain.local`

   `host-pg-01.domain.local`

   `host-pg-his-01.domain.local`

2. Далее создаются учётные записи служб:

   `HTTP/host-web-01.domain.local`

   `postgres/host-pg-01.domain.local`

   `postgres/host-pg-his-01.domain.local`

3. Для перечисленных служб генерируются три (два, при отсутствии экземпляра "his" *PostgreSQL*) keytab-файла:

`HTTP@host-web-01.domain.local.keytab`, соответствующий принципалу `HTTP/host-web-01.domain.local`

`postgres@host-pg-01.domain.local.keytab`, соответствующий принципалу `postgres/host-pg-01.domain.local`

`postgres@host-pg-his-01.domain.local.keytab`, соответствующий принципалу `postgres/host-pg-his-01.domain.local`

Один серверный узел

Процесс подготовки keytab-файлов для аутентификации через Kerberos отличается в зависимости от используемой *Службы каталогов*:

Microsoft Active Directory

1. В Службе каталогов домена MS AD создать отдельные учётные записи пользователя для использования службами *postgres* и *http*:

   `domain.local\httpservice`

   `domain.local\postgresservice`

2. Зарегистрировать SPN для служб postgres и HTTP на соответствующие учётные записи пользователей:

   `HTTP/host-scada-01.domain.local`

   `postgres/host-scada-01.domain.local`

   `postgres/host-pg-his-01.domain.local`

3. Сформировать три (два, при отсутствии экземпляра "his" *PostgreSQL*) keytab-файла:

   `HTTP@host-scada-01.domain.local.keytab`

   `postgres@host-scada-01.domain.local.keytab`

   `postgres@host-pg-his-01.domain.local.keytab`

   Keytab-файл `HTTP@host-scada-01.domain.local.keytab` соответствует принципалу `HTTP/host-scada-01.domain.local` и пользователю `domain.local\httpservice`.

   Keytab-файл `postgres@host-scada-01.domain.local.keytab` соответствует принципалу `postgres/host-scada-01.domain.local` и пользователю `domain.local\postgresservice`.

   Keytab-файл `postgres@host-pg-his-01.domain.local.keytab` соответствует принципалу `postgres/host-pg-his-01.domain.local` и пользователю `domain.local\postgresservice`.

MIB Kerberos

1. В случае использования в качестве каталога *MIB Kerberos*, например, на *FreeIPA* (*Astra Linux*), в каталоге создаются учётные записи узлов:

`host-scada-01.domain.local`

`host-pg-his-01.domain.local`

2. Далее создаются учётные записи служб:

   `HTTP/host-scada-01.domain.local`

   `postgres/host-scada-01.domain.local`

   `postgres/host-pg-his-01.domain.local`

3. Для перечисленных служб генерируются три (два, при отсутствии экземпляра "his" *PostgreSQL*) keytab-файла:

   `HTTP@host-scada-01.domain.local.keytab`, соответствующий принципалу `HTTP/host-scada-01.domain.local`

   `postgres@host-scada-01.domain.local.keytab`, соответствующий принципалу `postgres/host-scada-01.domain.local`

   `postgres@host-pg-his-01.domain.local.keytab`, соответствующий принципалу `postgres/host-pg-his-01.domain.local`

Общим для всех вариантов конфигурации развёртывания домена СК-11 является подготовка keytab-файлов для аутентификации через Kerberos служебных пользователей Системы с псевдонимами [ck11_server_services_user] и [ck11_deploy_user]. Процесс подготовки keytab-файлов для аутентификации через Kerberos отличается в зависимости от используемой *Службы каталогов*:

- Microsoft Active Directory

1. В Службе каталогов домена *MS AD* создать отдельные учётные записи пользователя для использования служебными пользователями:

   `domain.local\ck11_server_services_user`

   `domain.local\ck11_deploy_user`

2. Сформировать два keytab-файла:

   `ck11_server_services_user@domain.local.keytab`

   `ck11_deploy_user@domain.local.keytab`

   Keytab-файл `ck11_server_services_user@domain.local.keytab` соответствует пользователю `domain.local\ck11_server_services_user`.

   Keytab-файл `ck11_deploy_user@domain.local.keytab` соответствует пользователю `ck11_deploy_user@domain.local.keytab`.

- MIB Kerberos

1. В случае использования в качестве каталога *MIB Kerberos*, например, на *FreeIPA* (*Astra Linux*), в каталоге создаются учётные записи служебных пользователей:

   `ck11_server_services_user.domain.local`

   `ck11_deploy_user.domain.local`

2. Для перечисленных пользователей генерируются два keytab-файла:

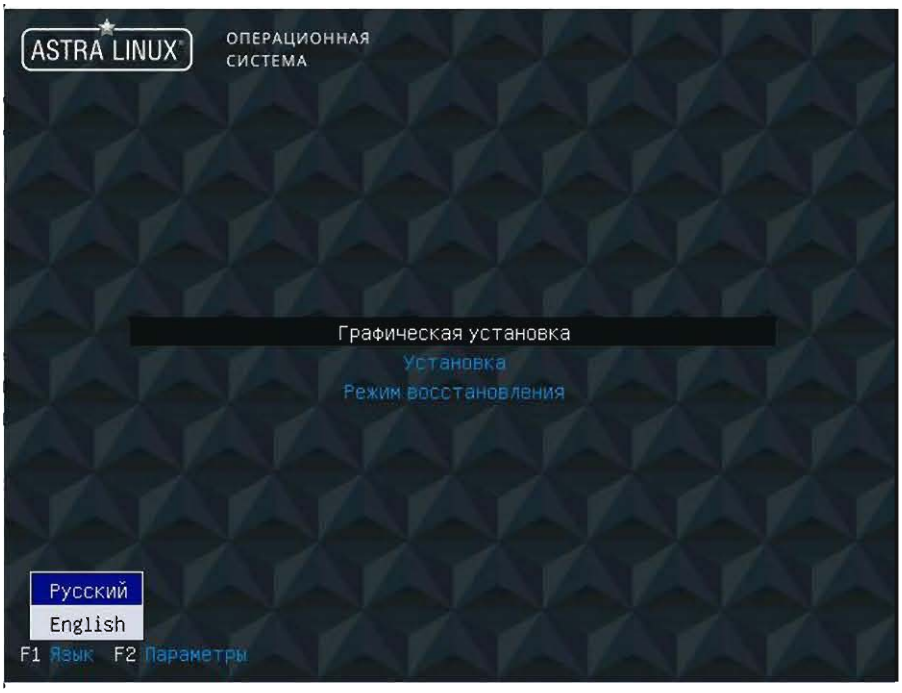
   `ck11_server_services_user@domain.local.keytab`, соответствующий пользователю `ck11_server_services_user.domain.local`

   `ck11_deploy_user@domain.local.keytab`, соответствующий пользователю `ck11_deploy_user.domain.local`

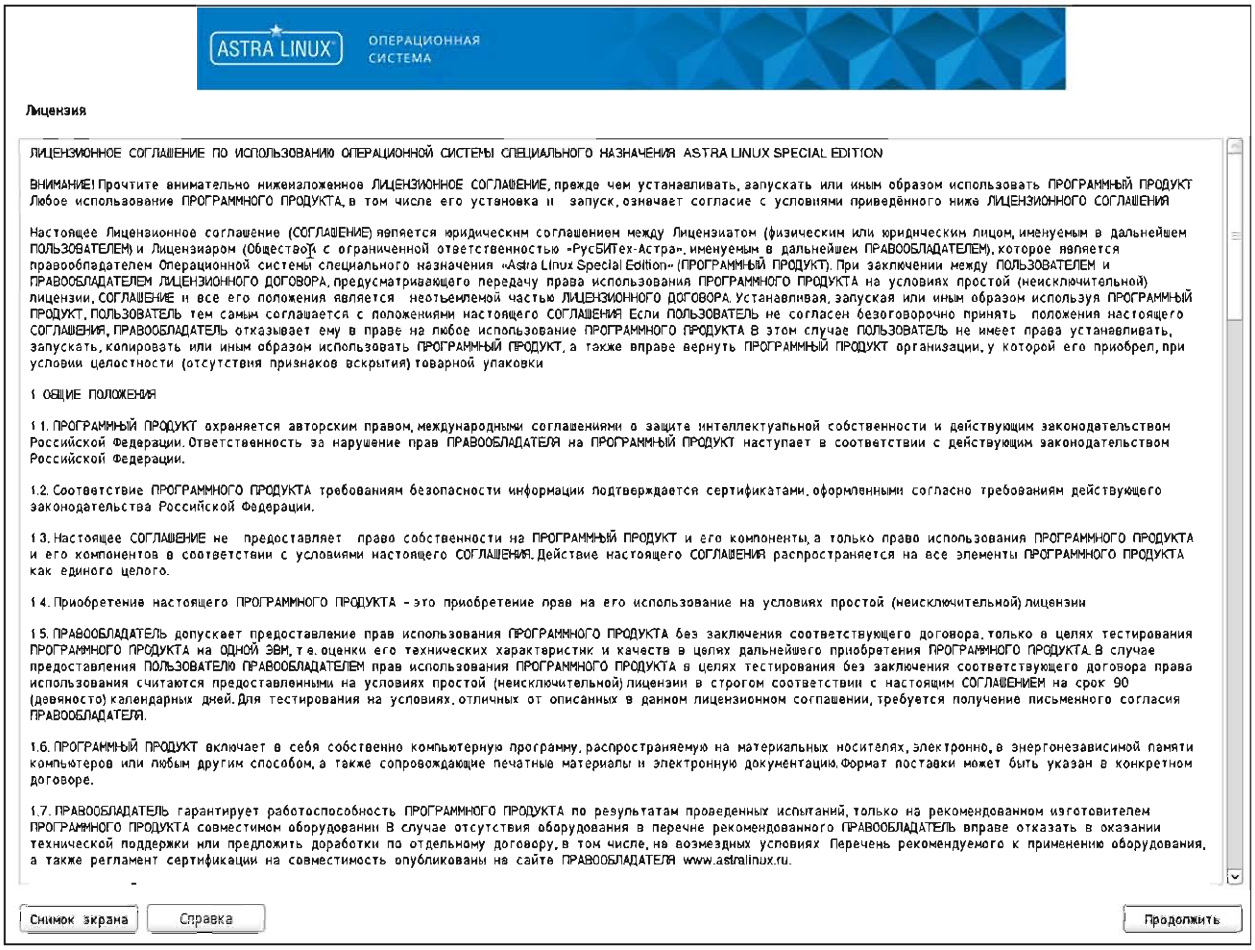
1.1.4. Установка ОС Astra Linux SE 1.7 на серверные узлы

При установке ОС *"Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7.3)* на серверные узлы выполняются следующие шаги:

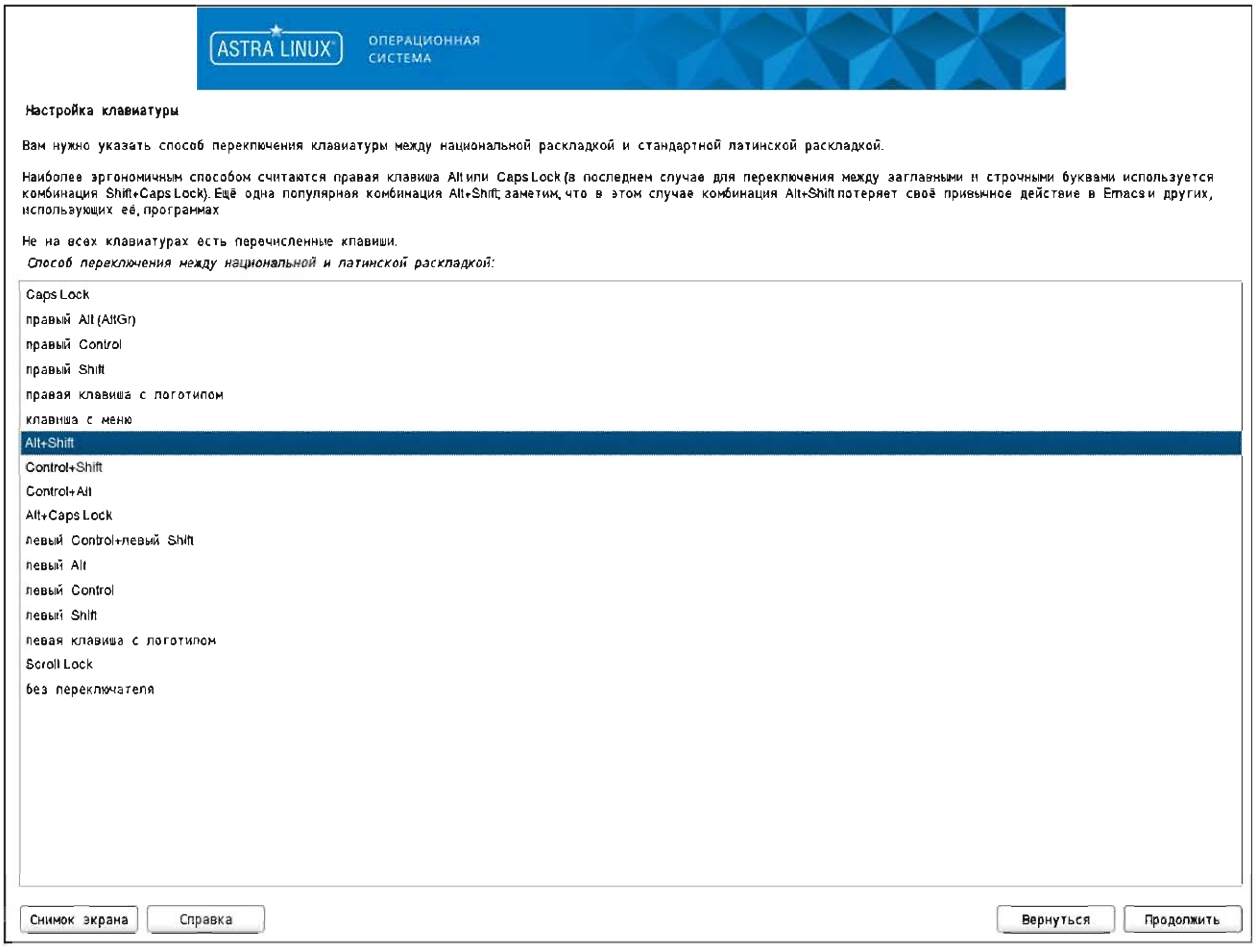
1. Смонтировать на сервере диск с дистрибутивом *Astra Linux Special Edition* в cdrom. Загрузиться с носителя дистрибутива ОС.
2. Выбрать режим установки "Графическая установка".



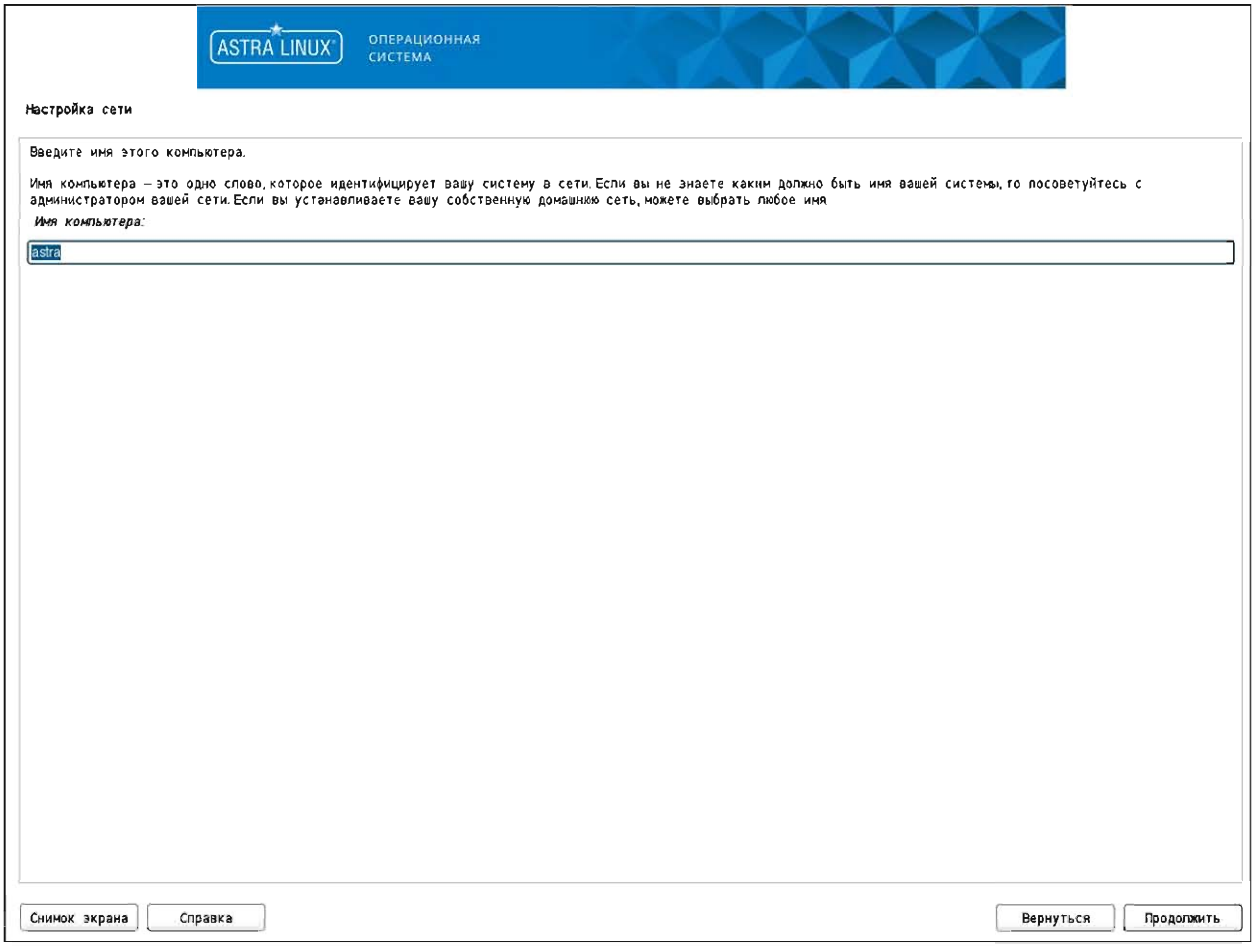
3. Ознакомиться с условиями лицензии, установить значение "Да" для пункта "Принимаете ли Вы условия настоящей лицензии?". Нажать на кнопку Продолжить.



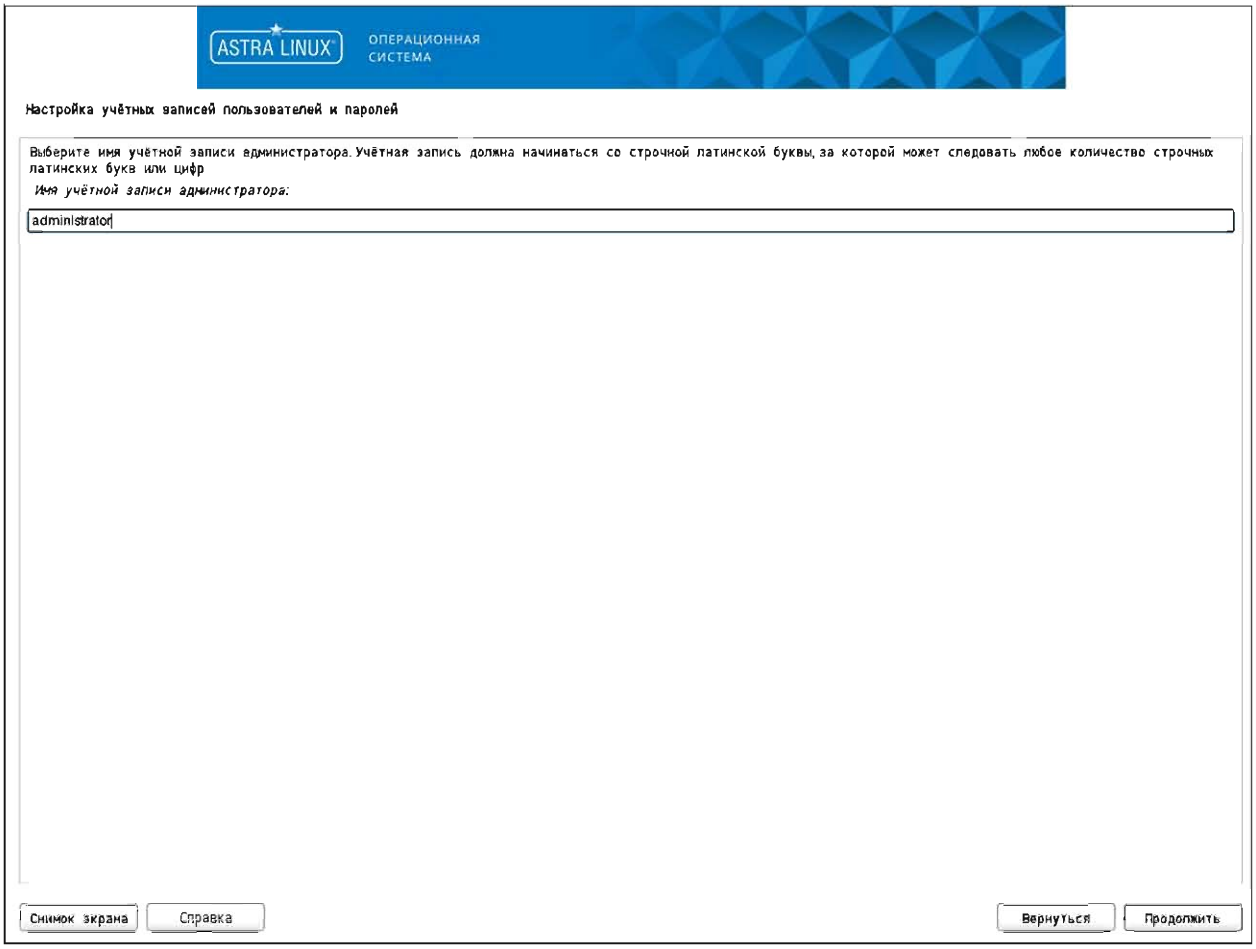
4. Выбрать предпочитаемое сочетание клавиш для изменения раскладки клавиатуры. Нажать на кнопку Продолжить.



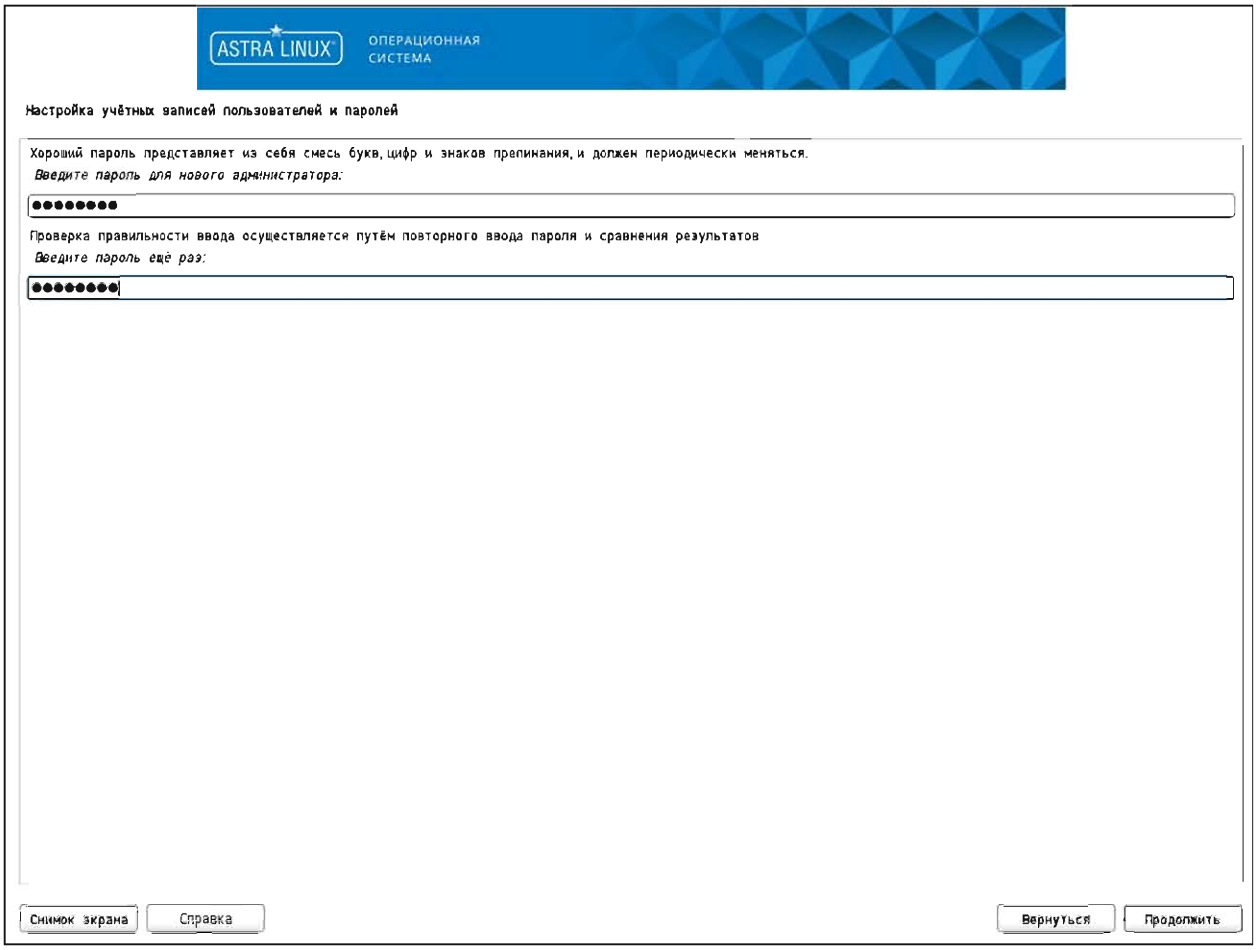
5. После загрузки компонентов программы установки ввести необходимое имя серверного узла (hostname), по которому будет доступен данный узел по сети. Нажать на кнопку Продолжить.



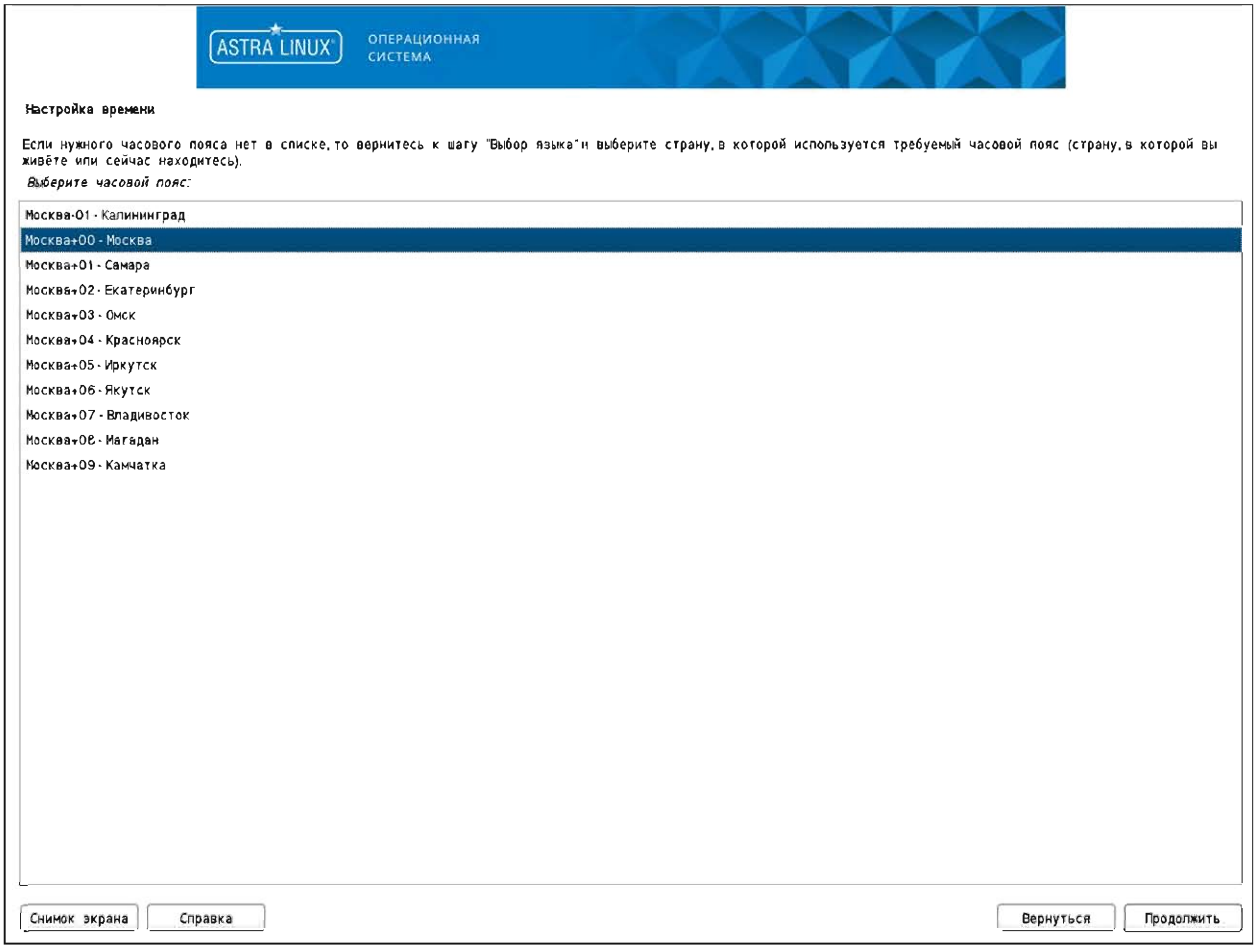
6. Указать имя учётной записи администратора, от имени которой будет выполняться первичная настройка ОС. Требуемое имя – **administrator**. Нажать на кнопку Продолжить.



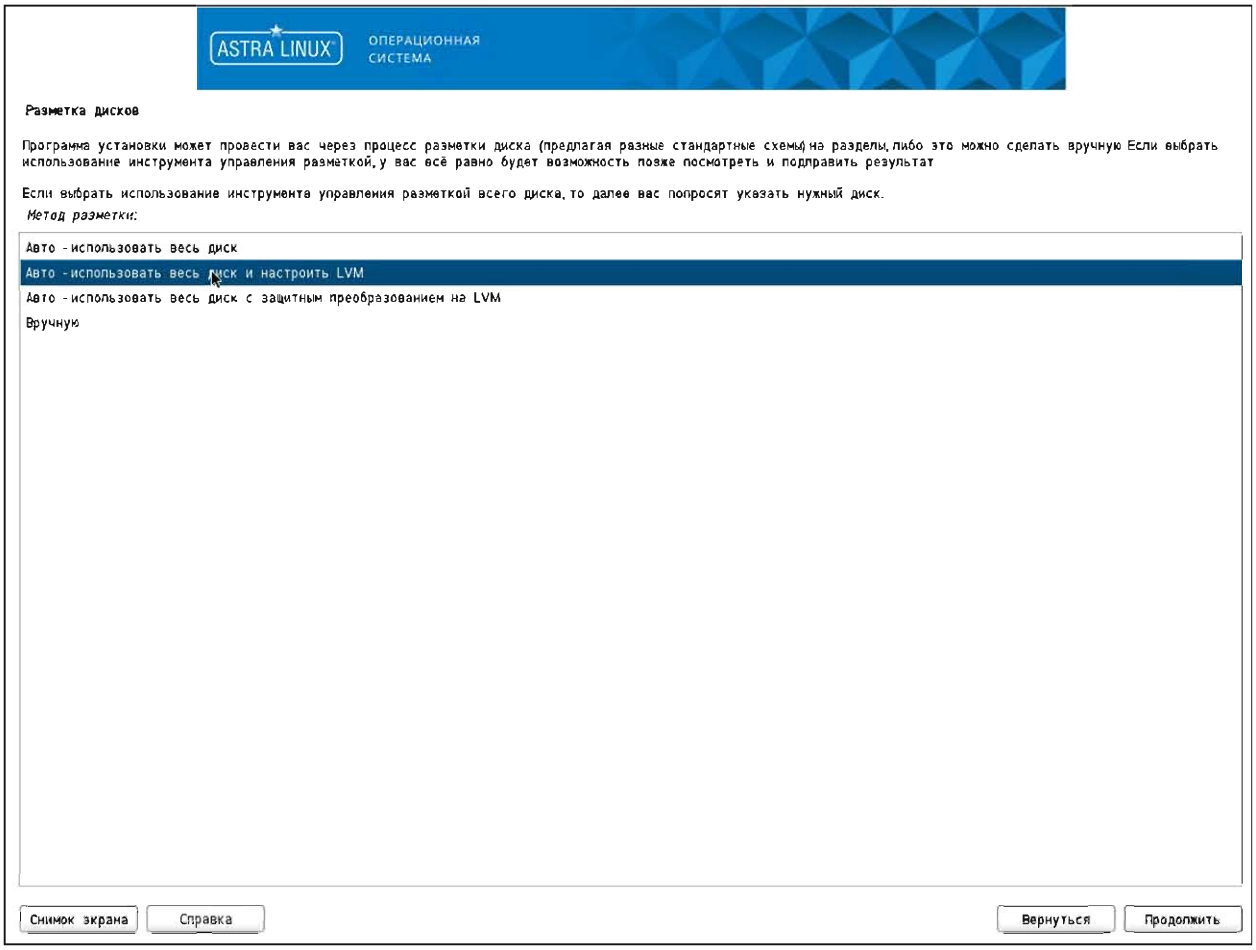
7. Ввести пароль для администратора серверного узла и продублировать его с целью проверки правильности ввода. Нажать на кнопку Продолжить.



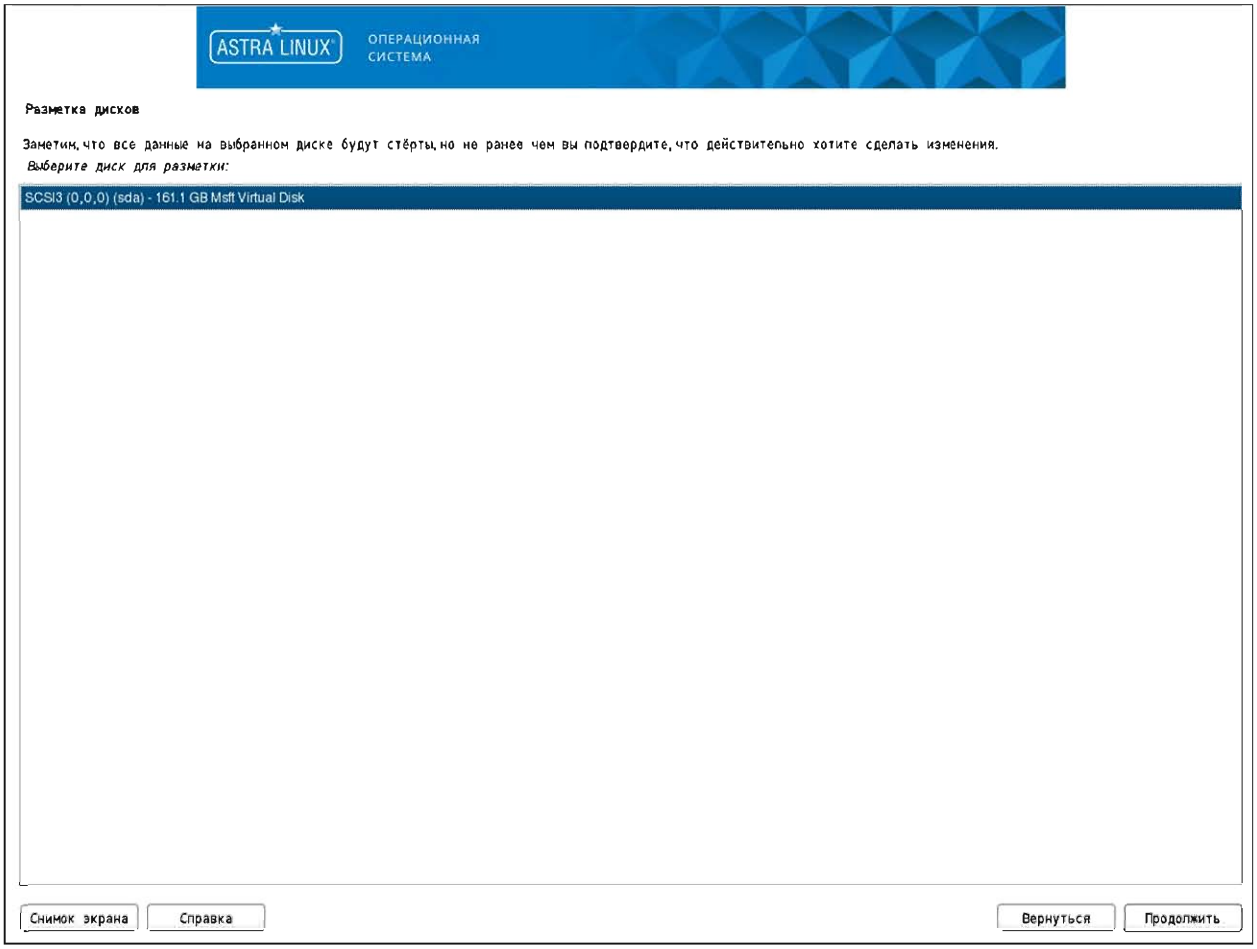
8. Выбрать необходимый часовой пояс. Нажать на кнопку Продолжить.



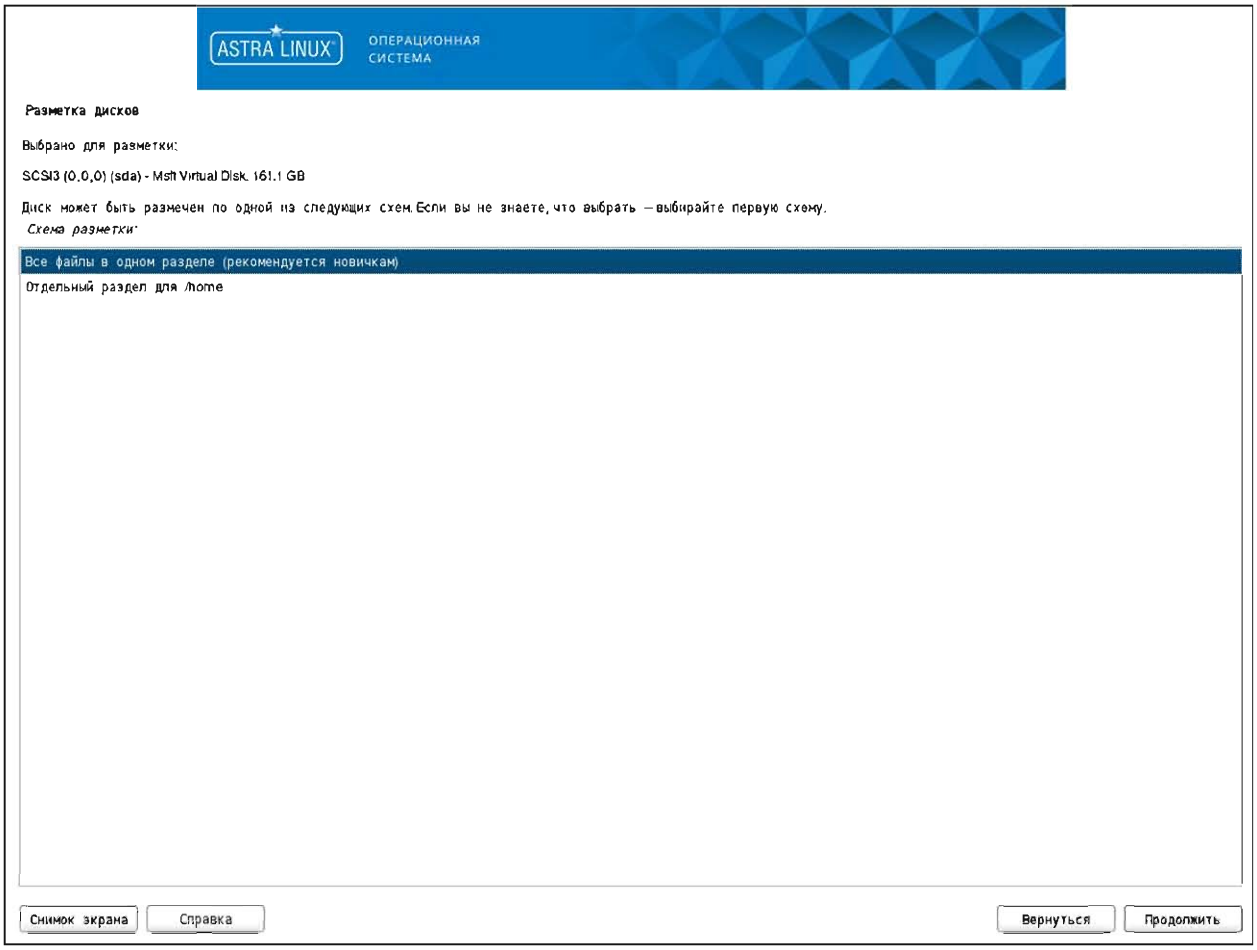
9. Выбрать режим разметки разделов диска "Авто – использовать весь диск и настроить LVM". Нажать на кнопку Продолжить.



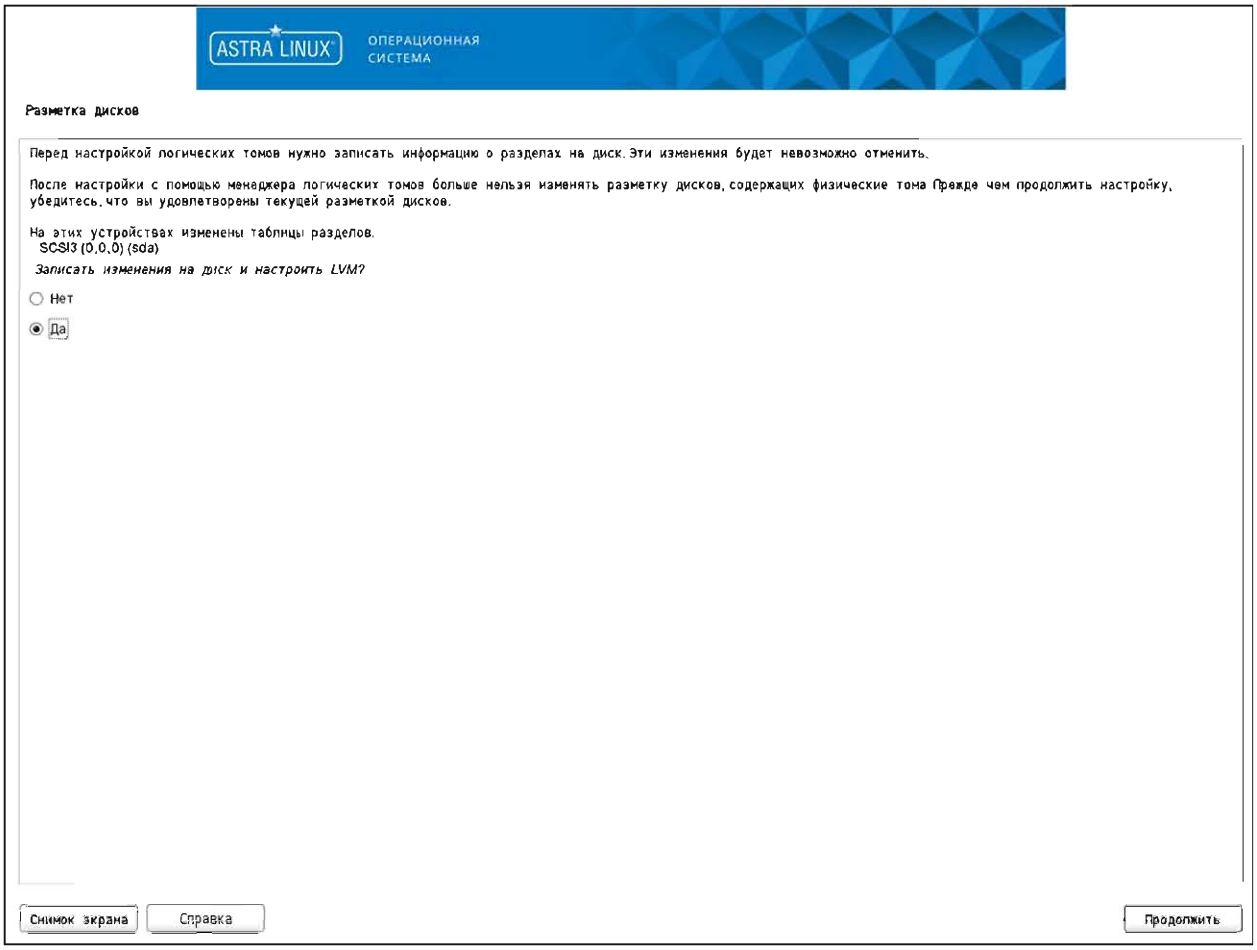
10. Выбрать диск для разметки разделов файловой системы. Нажать на кнопку Продолжить.



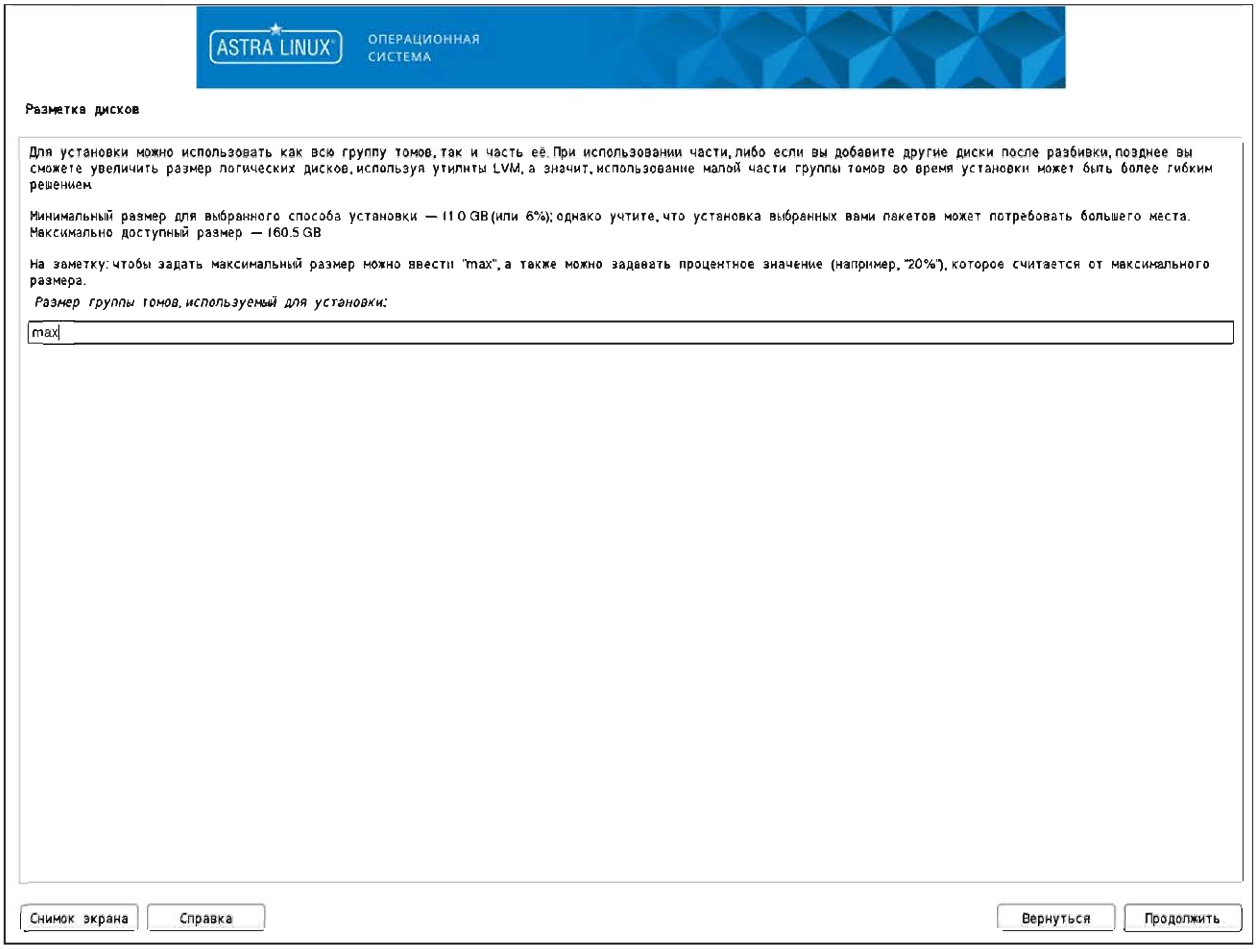
11. Выбрать схему разметки "Все файлы в одном разделе (рекомендуется новичкам)". Нажать на кнопку Продолжить.



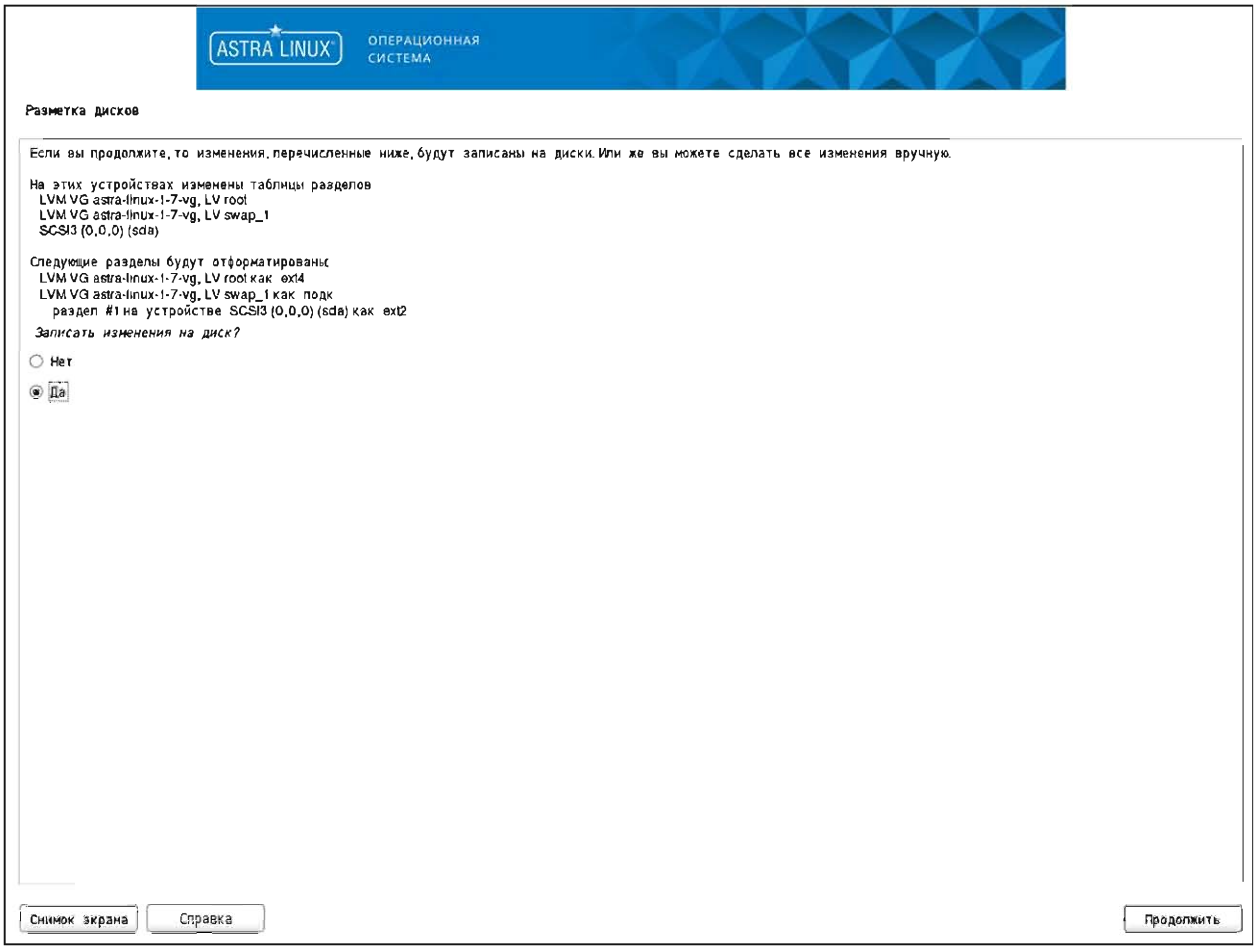
12. Подтвердить запись изменений разметки на диск, выбрав пункт "Да". Нажать на кнопку Продолжить.



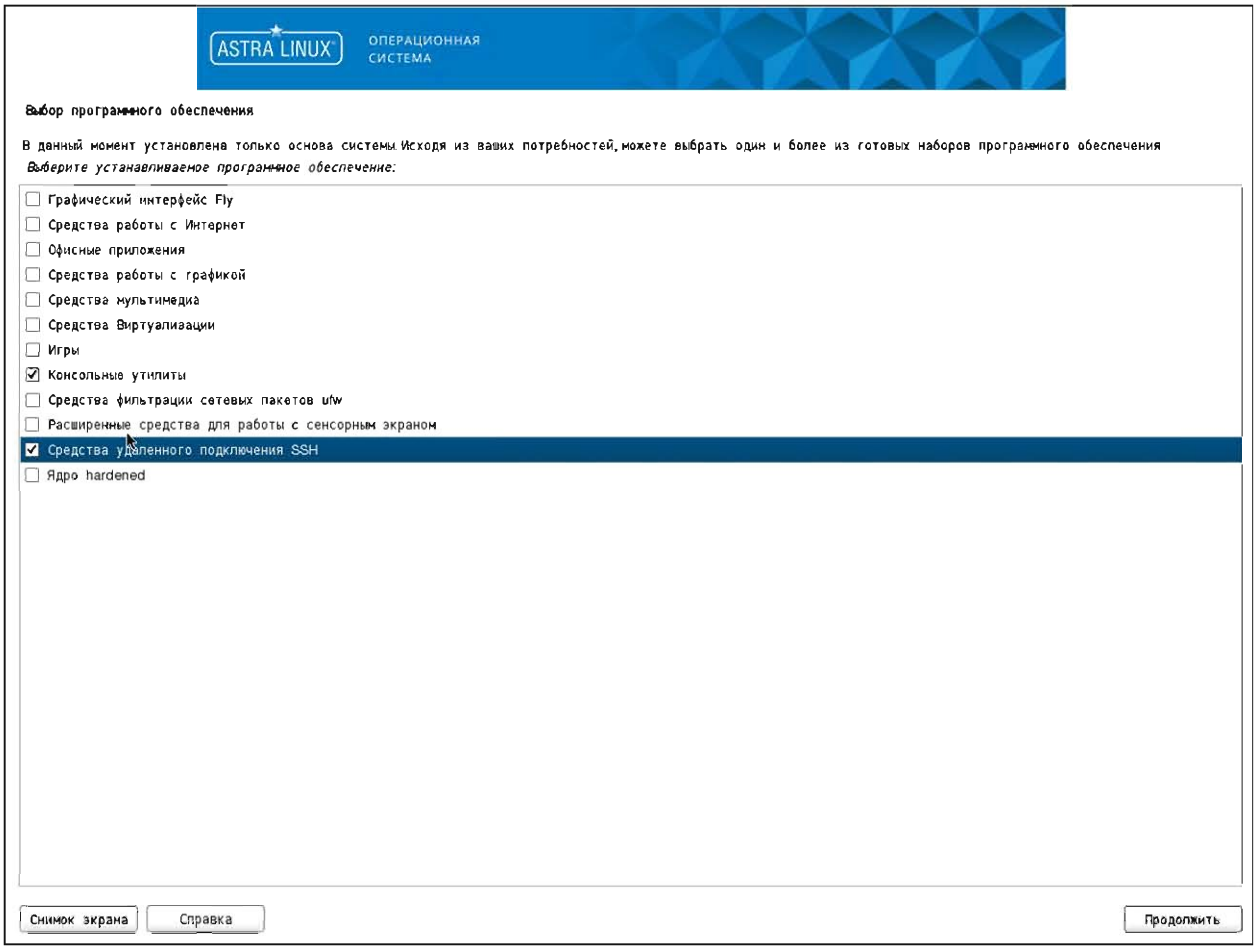
13. Указать максимально доступный размер группы томов. Нажать на кнопку Продолжить.



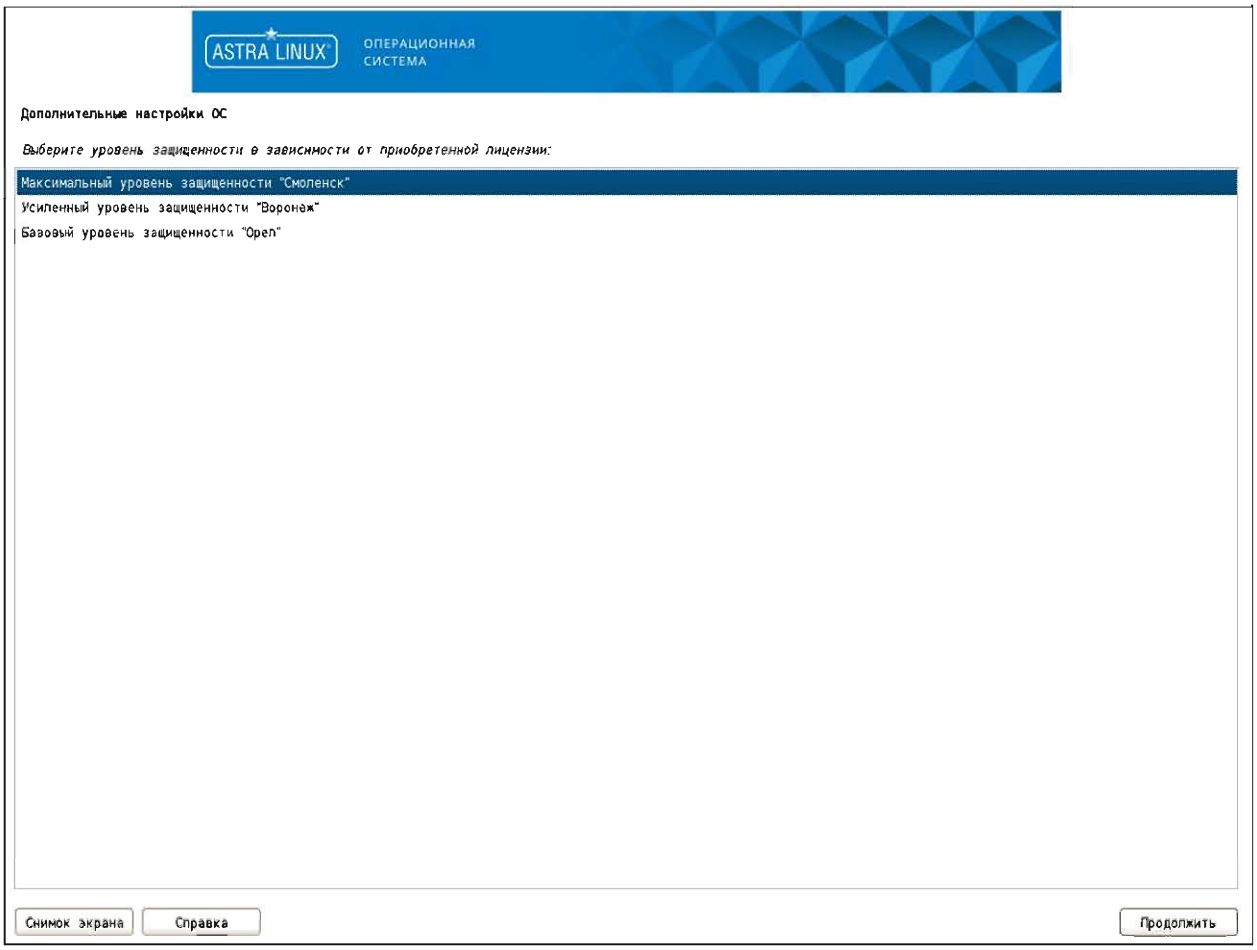
14. Подтвердить запись изменений разметки на диск, выбрав пункт "Да". Нажать на кнопку Продолжить.



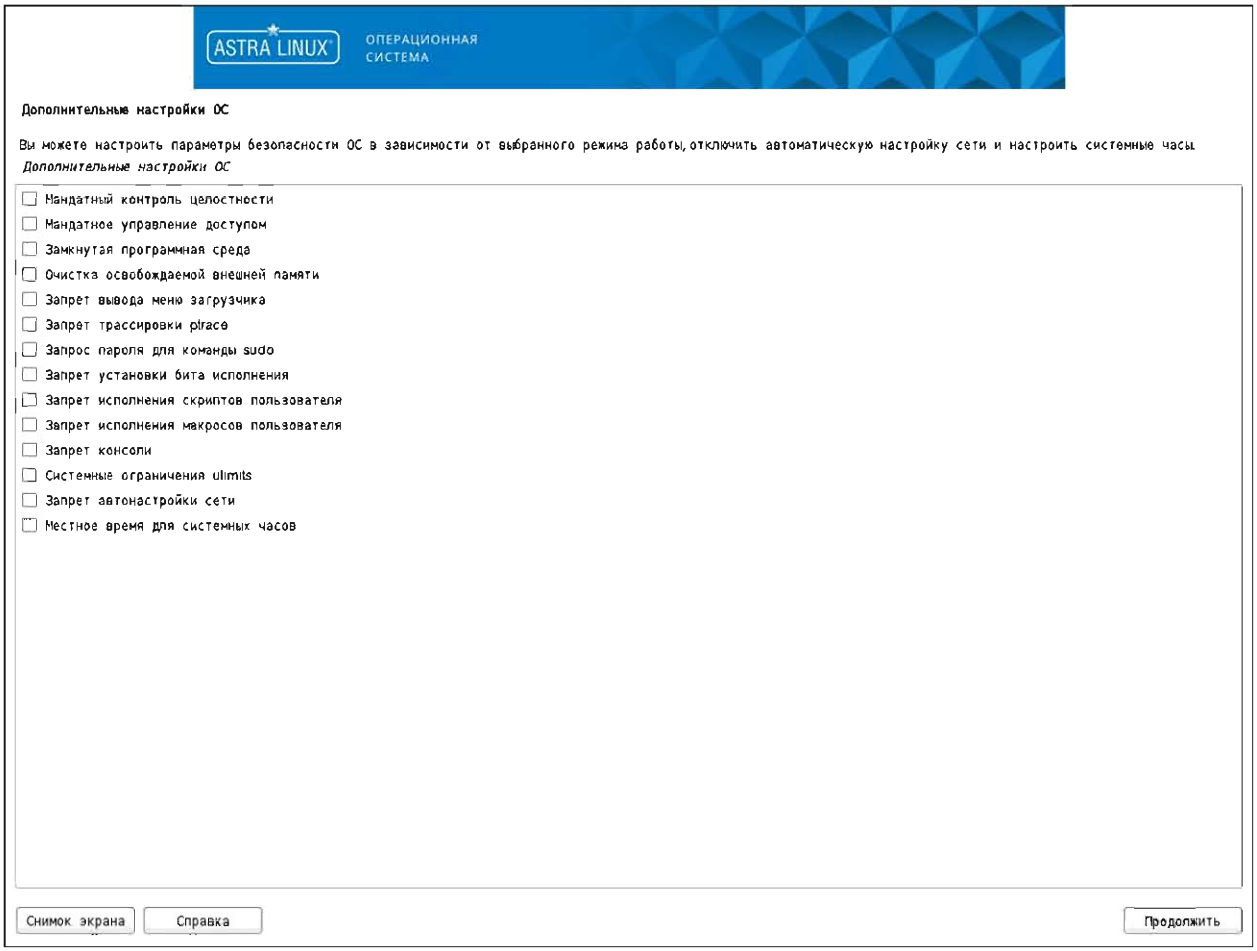
15. На шаге "Выбор программного обеспечения" выбрать пункты "Консольные утилиты", "Средства удалённого доступа SSH". Нажать на кнопку Продолжить.



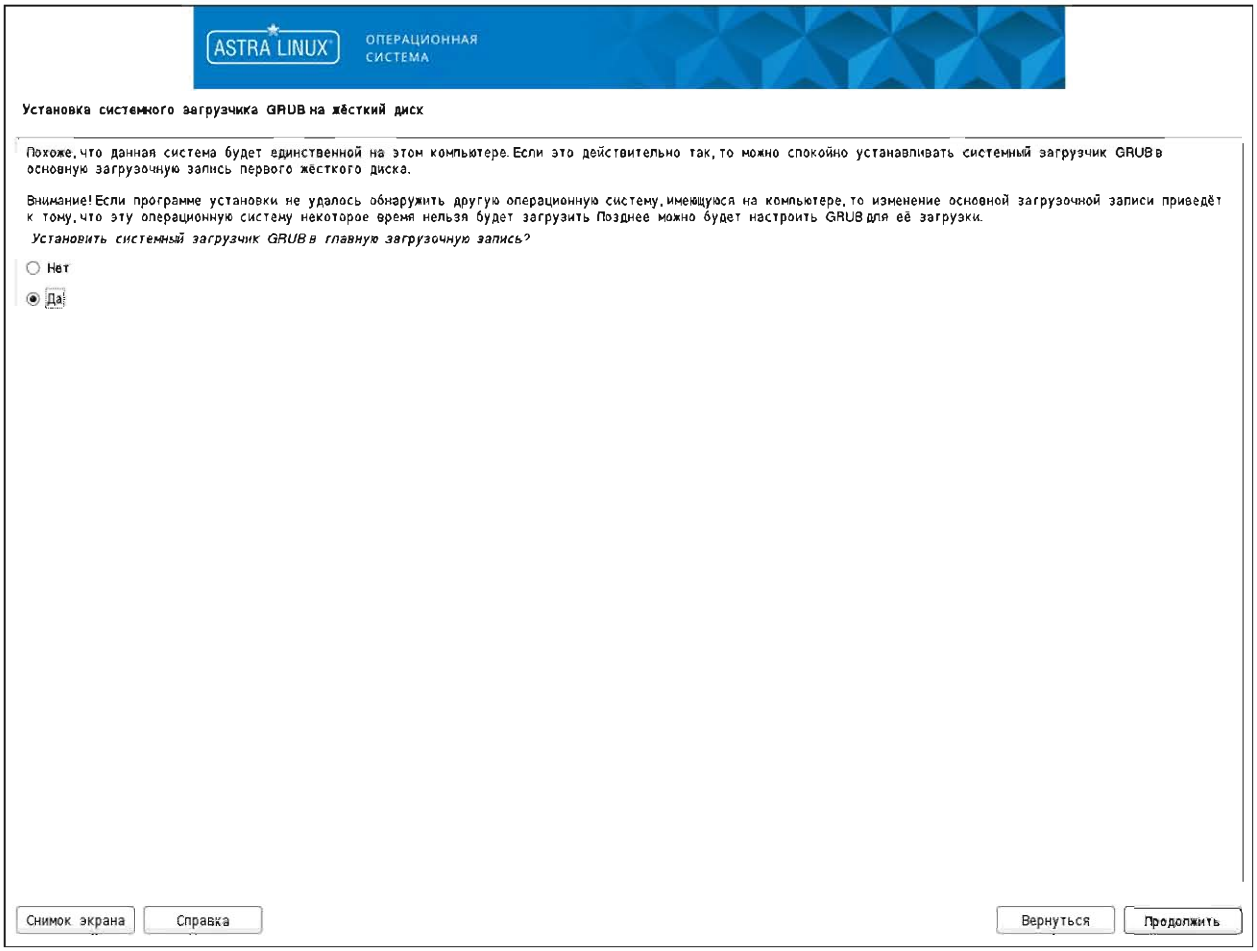
16. Выбрать уровень защищённости в зависимости от приобретённой лицензии. Нажать на кнопку Продолжить.



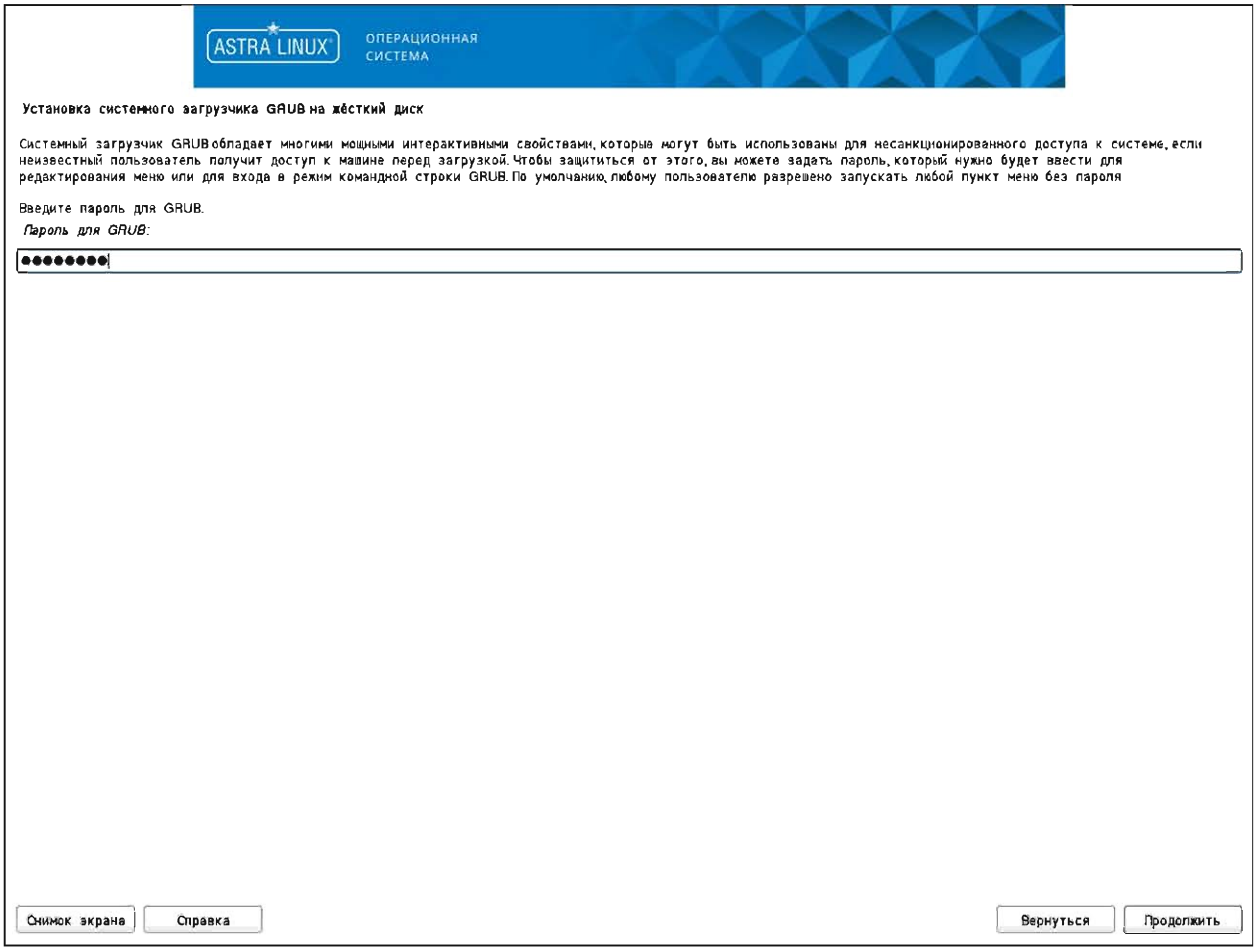
17. На шаге "Дополнительные настройки ОС" ничего выбирать не требуется. Нажать на кнопку Продолжить.



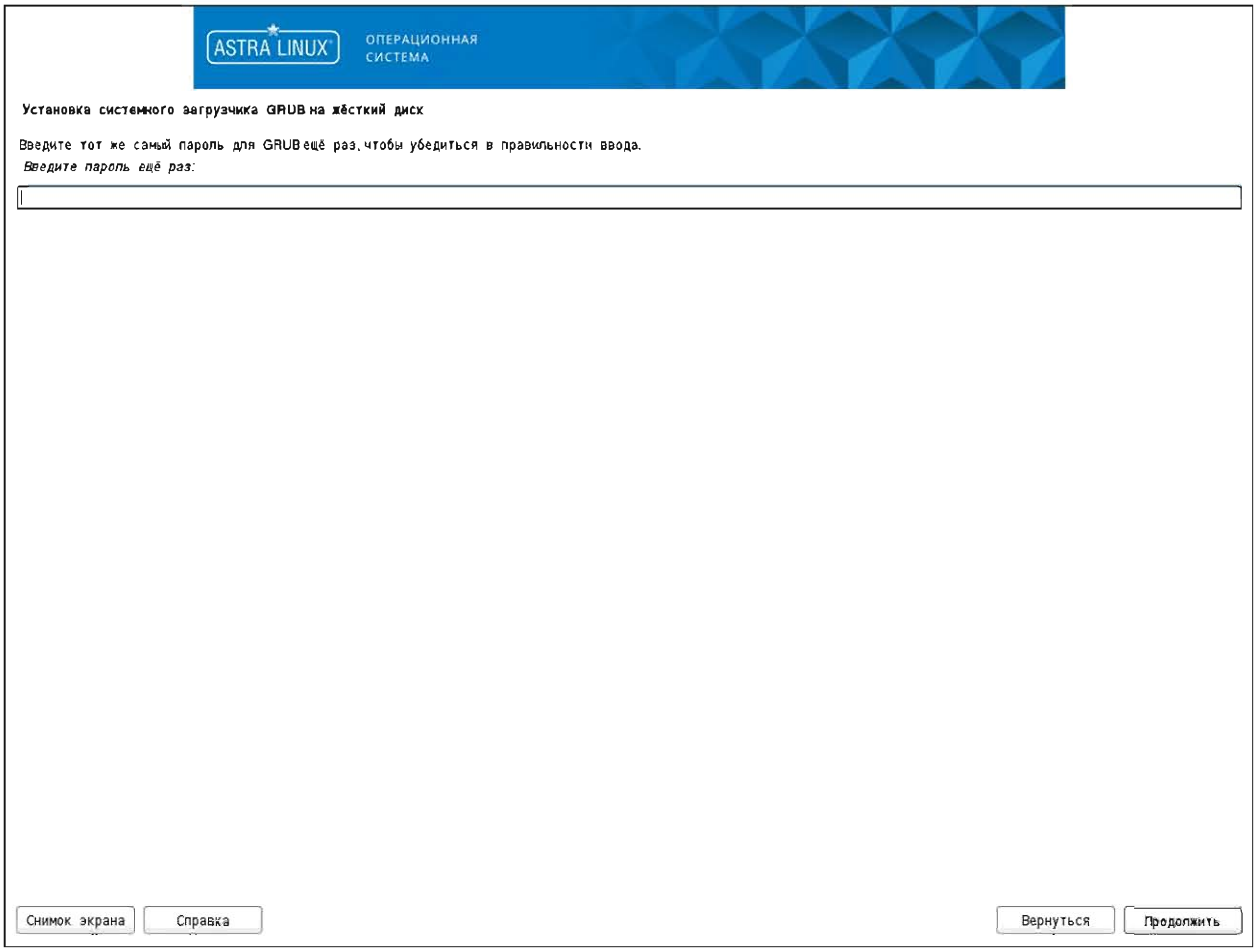
18. Подтвердить установку системного загрузчика GRUB на жёсткий диск, выбрав пункт "Да". Нажать на кнопку Продолжить.



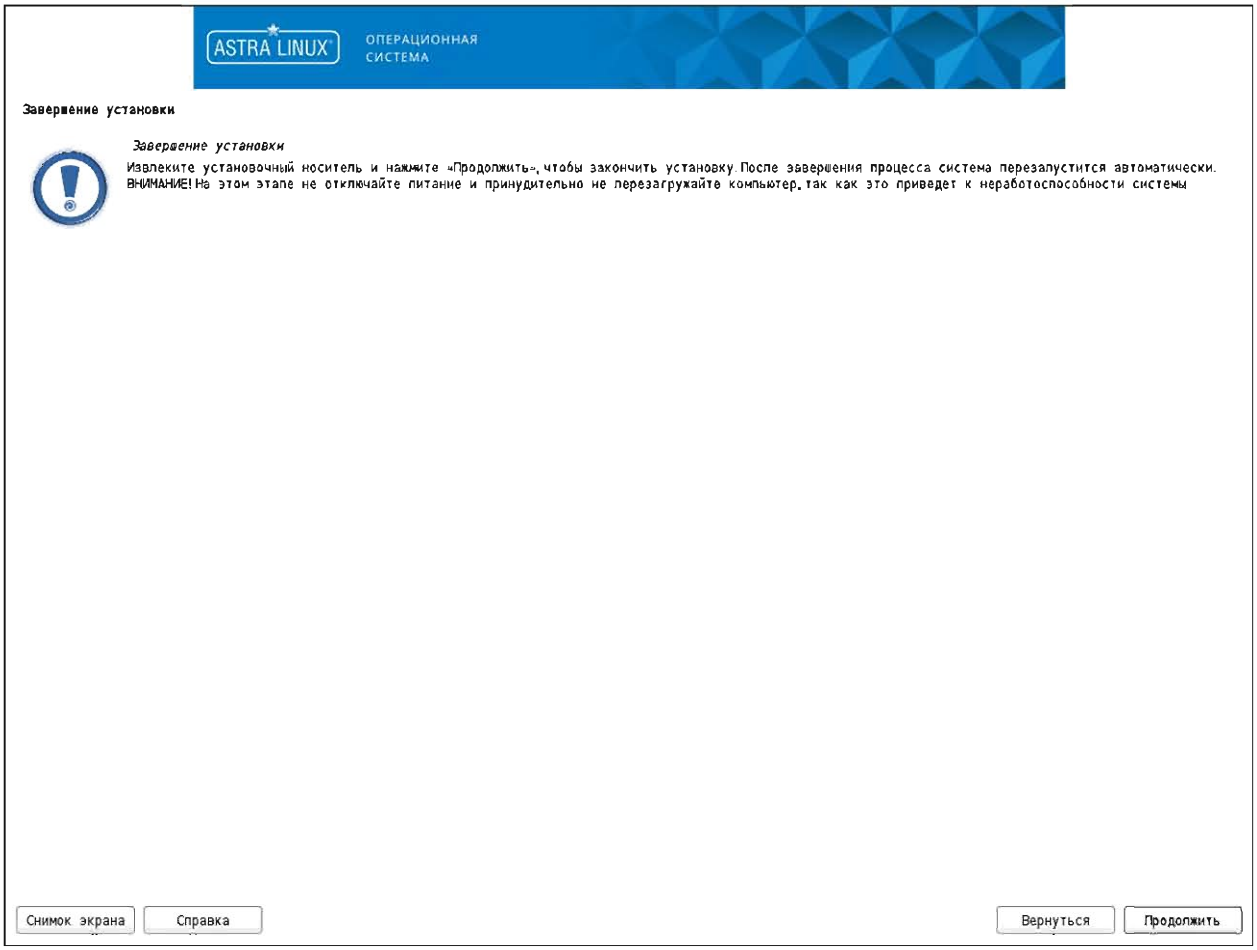
19. Ввести пароль для доступа к редактированию GRUB при загрузке (рекомендуется использовать такой же пароль, как для учётной записи администратора). Нажать на кнопку Продолжить.



20. Повторно ввести пароль для доступа к редактированию GRUB при загрузке. Нажать на кнопку Продолжить.



21. На шаге "Завершение установки" нажать на кнопку Продолжить для завершения установки



22. Изменить порядок загрузки виртуальной машины с компакт-диска на жёсткий и оставить установочный диск *Astra Linux SE* в приводе.

1.1.5. Первичная настройка ОС Astra Linux

После установки ОС *Astra Linux* необходимо выполнить первичную настройку:

1. Открыть файл `/etc/network/interfaces` в текстовом редакторе и задать следующее содержимое:

> Если файла нет, его можно создать командой:
> `touch /etc/network/interfaces`

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
#
```

```
allow-hotplug eth0
iface eth0 inet static
address ##HOST_IP##
netmask ##SUBNET_MASK##
gateway ##GATEWAY##
```

где заменить макропеременные:

`##HOST_IP##` – на IP адрес в формате: x.x.x.x

`##SUBNET_MASK##` – на маску подсети хоста в формате: y.y.y.y

`##GATEWAY##` – на IP-адрес шлюза по умолчанию в формате: x.x.x.z

2. Проверить, что размер SWAP равен размеру ОЗУ. При этом значение может быть изменено, исходя из особенностей эксплуатируемой системы, но только в следующих пределах: от 16 Гб до ОЗУ*3. Подробности по настройке приведены ниже:
   - Настройка файла подкачки в Astra Linux

Перед тем как перейти к настройке необходимо проверить не подключены ли разделы подкачки к системе. Для этого необходимо выполнить команду:

```
sudo swapon —show
```

```
administrator@len-web-02:~$ sudo swapon --show
NAME      TYPE      SIZE   USED PRIO
/dev/dm-1 partition   4G 333.5M   -2
```

Если команда вернёт строчку: `TYPE = partition`, то раздел подкачки в системе уже присутствует и следует проверить, что он соответствует условиям из пункта 2 (см. выше). Если ничего не будет выведено, значит в системе swap не настроен.

Создание и подключение файла подкачки, а также отключение раздела подкачки.

Перед созданием файла подкачки необходимо убедиться, что на жёстком диске имеется достаточно свободного места.

Для создания файла подкачки следует выполнить команду:

```
sudo fallocate -l 30G /swapfile
```

Далее, необходимо убедиться действительно ли зарезервировано нужное количество памяти.

Для проверки следует выполнить команду:

```
ls -lh /swapfile
```

```
administrator@len-web-02:~$ sudo fallocate -l 30G /swapfile
administrator@len-web-02:~$ ls -lh /swapfile
-rw-r--r-- 1 root root 30G Feb  8 10:38 /swapfile
```

Когда файл готов, необходимо преобразовать его в файл swap, для чего надо заблокировать доступ к нему всем кроме суперпользователя.

Для этого необходимо выполнить команду:

```
sudo chmod 600 /swapfile
```

После этого только пользователь root может читать и изменять данный файл:

```
ls -lh /swapfile
```

```
administrator@len-web-02:~$ sudo chmod 600 /swapfile
administrator@len-web-02:~$ ls -lh /swapfile
-rw------- 1 root root 30G Feb  8 10:38 /swapfile
```

Далее необходимо создать файловую систему swap командой:

```
sudo mkswap /swapfile
```

```
administrator@len-web-02:~$ sudo mkswap /swapfile
Setting up swapspace version 1, size = 30 GiB (32212250624 bytes)
no label, UUID=a0e2cd80-42f0-4a75-879a-4815b0b49f0a
```

Когда файл будет размещён и промаркирован, необходимо включить файл подкачки, чтобы начать его использовать:

```
sudo swapon /swapfile
```

После этого можно убедиться, что swap включён, выполнив команду:

```
sudo swapon –show
```

```
administrator@len-web-02:~$ sudo swapon --show
NAME      TYPE      SIZE   USED PRIO
/dev/dm-1 partition   4G 333.5M   -2
/swapfile file       30G     0B   -3
```

Для отключения раздела подкачки следует выполнить команду:

```
sudo swapoff /dev/dm-1
```

Чтобы настройка swap сохранялась после перезагрузки, необходимо отредактировать файл `/etc/fstab`. Можно вручную добавить строку в файл, либо использовать следующую команду:

```
echo '/swapfile none swap sw 0 0' | sudo tee -a /etc/fstab
```

а также закомментировать строку с подключением раздела подкачки:

```
/etc/fstab         [----]  0 L:[  1+14  15/ 15] *(782 / 782b) <EOF>
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
/dev/mapper/astra--vg-root /               ext4    errors=remount-ro 0       1
# /boot was on /dev/sda1 during installation
UUID=505c54ac-7f00-49c0-af72-5e305dfdca60 /boot           ext2    defaults        0       2
#/dev/mapper/astra--vg-swap_1 none            swap    sw              0       0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0
/dev/fd0        /media/floppy0  auto    rw,user,noauto  0       0
/swapfile none swap sw 0 0
```

3. Отредактировать файл `/etc/resolv.conf` в текстовом редакторе:

Если файла нет, его можно создать командой:
`touch /etc/resolv.conf`

a. Перечислить в файле IP-адреса серверов DNS в формате:

```
nameserver ##IP##
```

b. Указать полное имя домена в формате:

```
domain ##DOMAIN_FQDN##
```

где заменить макропеременные:

`##IP##` – на соответствующий адрес сервера DNS

`##DOMAIN_FQDN##` – на полное имя домена

Например:

```
nameserver 10.11.222.11
nameserver 10.11.222.12
domain oikdev.local
```

4. Выполнить следующие команды:

```
sudo systemctl enable ssh
sudo reboot
```

5. После перезагрузки проверить доступность сервера, подключившись к нему командной оболочкой с использованием протокола Secure Shell (SSH).
6. Повторить действия данного раздела на всех серверах для СК-11.

1.2. Подготовка сервера технического обслуживания

Сервер технического обслуживания – выделенный серверный узел, предназначенный для обеспечения операций по установке (создания домена СК-11), обновлению, исправлению серверной части Системы на платформе *Linux*. Настройка сервера технического обслуживания осуществляется в следующем порядке:

1. Подключение к серверу технического обслуживания,
2. Создание репозитория из дисков Astra Linux,
3. Копирование и подготовка инсталлятора.

Для корректной работы сервера технического обслуживания требуется размещение следующих файлов в указанных каталогах:

- `/home/administrator/setup` – эталонный пакет дистрибутива Системы;
- `/home/administrator/ansible/files/keytabs` – место хранения keytab-файлов;
- `/home/administrator/ansible/files/certificates` – место хранения сертификатов;
- `/home/administrator/setup/License.ck11` – файл лицензии СК-11.

В процессе установки стартового окружения создаются следующие пути размещения эталонных данных и средств установки Системы:

- `/home/administrator/ansible` – размещение данных системы управления конфигурациями;
- `/opt/creator` – установленный экземпляр утилиты настройки Системы;
- `/opt/creator/output/` – исходные данные для создания БД;
- `/data/client` – эталонные клиентские модули;
- `/data/documentation` –эталонная документация;
- `/data/frontends` – эталонные веб-приложения;
- `/data/libs` – эталонные библиотеки;
- `/data/server` – эталонные серверные модули;
- `/data/sessionservice` – эталонный Сервис сессий СК-11.

1.2.1. Подключение к серверу технического обслуживания

Подключение к серверу технического обслуживания осуществляется командной оболочкой с использованием протокола Secure Shell (SSH). Для аутентификации необходимо использовать данные учётной записи пользователя: administrator.

1.2.2. Создание репозитория из дисков Astra Linux

1. Выполнить подключение по SSH к серверу технического обслуживания от имени administrator.
2. Создать каталог для публикации репозиториев:

```
sudo mkdir -p /repository/publish
```

3. Установить nginx из дистрибутива СК-11:

```
sudo -E dpkg -i <путь к каталогу с
дистрибутивом>/setup/astra/packages/nginx_1.25.1_monitel-1.1.3_amd64.deb
```

4. Открыть в редакторе файл конфигурации репозиториев:

```
sudo mcedit /etc/nginx/nginx.conf
```

и в блок http{} добавить:

```
server {
  listen ##DEPLOYER_IP##:80 default_server;
  location / {
  root /repository/publish;
  autoindex on;
  }
  }
```

где `##DEPLOYER_IP##` необходимо заменить на IP-адрес текущего сервера технического обслуживания.

5. Создать в `/repository/publish` каталоги репозиториев для установки стороннего ПО и средств разработки:

```
sudo mkdir -p /repository/publish/smolensk_main
sudo mkdir -p /repository/publish/smolensk_base
```

6. Скопировать с установочного диска *Astra Linux* каталоги `dists` и `pool` в каталог:

```
/repository/publish/smolensk_main
```

7. Смонтировать в `cdrom` диск дистрибутив base. Загрузить архив базового (base) репозитория ОС Astra Linux Special Edition можно в новой версии Личного кабинета. Для этого следует перейти на вкладку "Лицензии и сертификаты", выбрать лицензию на ОС Astra Linux Special Edition 1.7, затем в нижнем меню выбрать пункт Обновление | Оперативные обновление | <требуемое оперативное обновление> и загрузить архив репозитория. Версия репозитория base должна соответствовать версии установочного диска Astra Linux. Скопировать с него каталоги `dists` и `pool` в каталог:

```
/repository/publish/smolensk_base
```

8. Создать файл со списком репозиториев по умолчанию:

```
sudo touch /etc/apt/sources.list.d/default.list
```

9. Добавить в файл `/etc/apt/sources.list.d/default.list` строки подключения к созданным репозиториям:

```
#---start setup repos
deb http://##DEPLOYER_IP##:80/smolensk_main stable main contrib non-free
deb http://##DEPLOYER_IP##:80/smolensk_base stable main contrib non-free
#---end setup repos
```

где `##DEPLOYER_IP##` заменить на IP-адрес текущего сервера технического обслуживания.

10. Закомментировать все строки символом # в следующих файлах:

```
/etc/apt/sources.list
/etc/apt/sources.list_astra
```

11. Перезапустить nginx и выполнить обновление репозиториев:

```
sudo systemctl restart nginx
sudo apt update
```

1.2.3. Копирование и подготовка инсталлятора

1. Скопировать на сервер технического обслуживания в домашний каталог администратора (`/home/administrator`) каталог "`setup`" с дистрибутивом Системы.

2. Для установки вам потребуется файл лицензии, по параметрам которого будет сформирована многосерверная система с необходимым набором функциональных модулей.

   С целью защиты программного обеспечения от промышленного шпионажа, в том числе от иностранных конкурентов, файл лицензии для членов Экспертного совета Реестра Российского программного обеспечения при Минкомсвязи России предоставляется по запросу, направленному на электронный адрес: market@monitel.ru, в течение 30 минут.

   Скопировать файл лицензии License.ck11 в каталог `/home/administrator/setup/`;

3. Подключиться к серверу технического обслуживания.

4. Последовательно выполнить следующие команды в домашнем каталоге администратора:

```
cp -rf setup/ansible ~
tar -xvf setup/ansible/ansible.tar.bz2 -C ansible
ansible/bootstrap.sh
```

> `ansible.tar.bz2` – архив конфигурации инвентаря *Ansible*.

5. Распаковать шаблоны *инвентаря Ansible* командой:

```
tar -xvf ansible/inventory_examples.tar.bz2 -C ansible/inventory
```

6. Для конфигурации развёртывания с имеющейся *Службой каталогов* (*MS AD/FreeIPA*) в каталог `/home/administrator/ansible/files/keytabs` скопировать keytab-файлы для *Nginx*, *PostgreSQL* и служебных пользователей, созданные ранее.

> Необходимость вспомогательного экземпляра "his" *PostgreSQL* для БД "Архив БДРВ" (HIS) определяется наличием опции лицензии "his" в файле лицензии платформы СК-11. Если указанная опция отсутствует, то keytab-файл для экземпляра *PostgreSQL* "his" не создаётся.

7. Для конфигурации развёртывания с имеющейся *Службой каталогов* (*MS AD/FreeIPA*) в каталог `/home/administrator/ansible/files/certificates` скопировать ранее подготовленные файлы SSL-сертификатов.

   a. Выполнить команды:

```
cd ~/ansible/files/certificates
openssl x509 -in ##HTTP##.pem -out ##HTTP##.crt
openssl x509 -in ##host-deployer##.pem -out ##host-deployer##.crt
cd ~/ansible
```

   где `##HTTP##` – имя сертификата для веб-сервисов и служб СК-11,
   `##host-deployer##` – имя сертификата для сервера технического обслуживания.

1.3. Настройка инвентаря Ansible

Настройка инвентаря *Ansible* выполняется в несколько последовательных этапов:

1. Настройка конфигурации серверных узлов и параметров установки в зависимости от целевой схемы развёртывания Системы:
   a. Шесть серверных узлов;
   b. Три серверных узла;
   c. Один серверный узел.
2. Если целевая схема развёртывания предусматривает использование/установку *Службы каталогов FreeIPA*, то выполняется настройка её конфигурации.
3. Монтирование хранилища для резервных копий БД.

В зависимости от конфигурации развёртывания точкой подключения SCADA_EP является:

- для конфигурации с шестью узлами имя основной группы `host-scada`;
- для конфигураций с одним или тремя узлами имя сервера `host-scada-01.domain.local`.

В зависимости от конфигурации развёртывания точкой подключения WEB_EP является:

- для конфигурации с шестью узлами имя группы веб-серверов `host-web`;
- для конфигурации с тремя узлами имя сервера `host-web-01.domain.local`;
- для конфигурации с одним узлом имя сервера `host-scada-01.domain.local`.

1.3.1. Шесть серверных узлов

1. Подключиться к серверу технического обслуживания;
2. Перейти в каталог /`home/administrator/ansible/inventory/ck11.6hosts/`:

```
cd ~/ansible/inventory/ck11.6hosts/
```

3. Выбрать каталог шаблона конфигурации развёртывания в зависимости от запланированной *Службы каталогов* и наличия её контролёра:
   a. `ad.exists` – используется установленный и настроенный контролёр *Службы каталогов MS AD,*
   b. `freeipa.exists` – используется установленный и настроенный контролёр *Службы каталогов FreeIPA,*
   c. `freeipa.install` – контроллер *Службы каталогов FreeIPA* (на выделенном узле) и домен СК-11 устанавливаются и настраиваются одновременно.
4. Скопировать содержимое выбранного каталога шаблона конфигурации развёртывания в корень каталога /`home/administrator/ansible/inventory`:

```
cp -RTv ##template directory## ~/ansible/inventory
```

где `##template directory##` – имя выбранного каталога шаблона конфигурации.

5. Удалить каталоги шаблонов конфигурации для всех вариантов развёртывания домена СК-11 в каталоге /`home/administrator/ansible/inventory`, оставить файл `hosts` и каталог `group_vars`, выполнив команды:

```
cd ~/ansible/inventory/
rm -r ck11.1host ck11.3hosts ck11.6hosts
```

6. Выполнить настройку конфигурации серверных узлов;
7. Выполнить настройку параметров установки.

1.3.1.1. Настройка конфигурации серверных узлов

1. Подключиться к серверу технического обслуживания;
2. Перейти в каталог `home/administrator/ansible/inventory/`;
3. Отредактировать файл `hosts` – установить имена и адреса серверных узлов, а также распределить их по группам в зависимости от роли.

   По умолчанию в шаблоне используются следующие обозначения, псевдонимы серверных узлов:

   host-deployer – сервер технического обслуживания, на котором развёрнута система *Ansible* для установки/обновления СК-11 и сопутствующих компонентов;

   host-scada-01 – основной сервер (master) оперативного контура (ОК);

   host-scada-02 – резервный сервер (slave) оперативного контура (ОК);

   host-web-01 – основной сервер (master) группы горячего резерва "Веб-сервисы";

   host-web-02 – резервный сервер (slave) группы горячего резерва "Веб-сервисы";

   host-pg-01 – первый узел основного экземпляра "main" кластера *PostgreSQL*, на котором хранятся БД СК-11, кроме БД "Архив БДРВ" (HIS);

   host-pg-02 – второй хост основного экземпляра "main" кластера *PostgreSQL*, на котором хранятся БД СК-11, кроме БД "Архив БДРВ" (HIS);

   host-pg-lst – имя (прослушиватель) основного экземпляра (main) кластера *PostgreSQL*, на котором хранятся БД СК-11, кроме БД "Архив БДРВ" (HIS);

   Необходимость вспомогательного экземпляра "his" *PostgreSQL* для БД "Архив БДРВ" (HIS) определяется наличием опции лицензии "his" в файле лицензии платформы СК-11.

   host-pg-his-01 – первый узел экземпляра "his" кластера PostgreSQL, на котором хранится БД "Архив ТМ" (HIS);

   host-pg-his-02 – второй узел экземпляра "his" кластера PostgreSQL, на котором хранится БД "Архив ТМ" (HIS);

   host-pg-his-lst – имя (прослушиватель) экземпляра "his" кластера PostgreSQL, на котором хранится БД "Архив ТМ" (HIS);

   host-web – имя группы веб-серверов;

host-scada – имя основной группы серверов приложений;

host-freeipa – имя сервера Службы каталогов FreeIPA, для конфигурации развёртывания с использованием/установкой *Службы каталогов FreeIPA*.

В файле `hosts` необходимо заменить псевдонимы на реальные имена серверов, которые будут использоваться в дальнейшей эксплуатации.

При определении узлов экземпляра "his" необходимо задать `hostname` сервера в переменной **`primary_hostname`**. Например:

```
 host-pg-his-01  ansible_host=10.10.10.147 ansible_user=administrator
postgresql_instance=his primary_hostname=host-pg-01

 host-pg-his-02  ansible_host=10.10.10.148 ansible_user=administrator
postgresql_instance=his primary_hostname=host-pg-02
```

Для адресов прослушивателей кластера *PostgreSQL* необходимо добавить атрибут **`postgresql_entrypoint=yes`**.

```
 host-pg-lst  ansible_host=10.10.10.150 postgresql_instance=main
postgresql_entrypoint=yes

 host-pg-his-lst  ansible_host=10.10.10.149 postgresql_instance=his
postgresql_entrypoint=yes
```

Для адреса точки подключения WEB_ENTRY_POINT (WEB_EP) необходимо добавить атрибут **`ck11_web_entrypoint=yes`**. Например:

```
 host-web  ansible_host=10.10.10.158 ck11_web_entrypoint=yes
```

Для адреса точки подключения SCADA_ENTRY_POINT (SCADA EP) необходимо добавить атрибут **`ck11_scada_entrypoint=yes`**. Например:

```
 host-scada  ansible_host=10.10.10.159 ck11_scada_entrypoint=yes
```

Для серверных узлов указывается атрибут с учётной записью пользователя для использование инструментарием *Ansible*:

```
 ansible_user=administrator
```

Группы узлов, имена которых заключены в квадратные скобки, позволяют распределить узлы в зависимости от их ролей. Описание групп представлено ниже.

- [manager]

  Определение

  Сервер технического обслуживания.

  Состав

  Сервер, на котором развернут *Ansible* для выполнения операций автоматизированного развёртывания ПО.

- [ck11]

  Определение

  Серверы приложений СК-11.

  Состав

  Узлы, на которых будет установлена серверная часть СК-11. На узлах данной группы будет развёрнута "Служба управления задачами СК-11", которая запустит задачи, определяемые описанием сервера в модели "Конфигурация системы". По умолчанию:

  host-scada-01

  host-scada-02

  host-web-01

  host-web-02

- [ck11_scada]

  Определение

  Серверы Основной группы горячего резерва.

  Состав

  Узлы, на которых будут запущены задачи, выполняющие обработку оперативной информации. Например, "БДРВ", "Обработка телеметрии", "Процессор топологии" и т.д. Отказоустойчивость ресурсов обеспечивается за счёт службы СК-11 Supervisor. Для доступа к веб-сервисам оперативного контура используется точка подключения SCADA_EP.

  Должно быть указано не более двух серверов. По умолчанию:

  host-scada-01

  host-scada-02

- [ck11_web]

  Определение

  Серверы группы горячего резерва "Веб-сервисы".

  Состав

  Узлы, на которых будут запущены веб-сервисы, доступ к которым выполняется по протоколу HTTPS, с использованием имени точки подключения WEB_EP.

  Должно быть указано не более двух серверов. По умолчанию:

  host-web-01

  host-web-02

- [jsreport]

  Определение

  Серверы размещения компонентов *jsreport*.

  Состав

  Узлы, на которых будут размещены компоненты *jsreport*, включая специализированную БД, для обеспечения работы веб-сервисов СК-11. Должно быть указано не более двух серверов. По умолчанию:

  host-web-01

  host-web-02

- [cluster]

  Определение

  Серверы кластера *PostgreSQL*.

  Состав

  В группу должны входить три узла. На всех трёх узлах будут развёрнуты компоненты *Corosync+Pacemaker*, обеспечивающие кластеризацию PostgreSQL. На первых двух узлах списка разворачивается сервис *PostgreSQL* и БД с настроенной репликацией между ними. Третий узел в данной группе играет роль голосующей ноды при определении основного (master) сервера кластера. При использовании конфигурации Системы с количеством узлов более двух в качестве голосующей ноды используется один из серверов приложений СК-11. По умолчанию в шаблоне задан второй сервер Основной группы – host-scada-02. По умолчанию:

  host-pg-01

  host-pg-02

  host-scada-02

- [postgresql]

Определение

Серверы с СУБД *PostgreSQL*, включая виртуальные имена узлов вспомогательного экземпляра *PostgreSQL* "his".

Состав

Узлы, на которых будет развёрнут сервис *PostgreSQL* и БД СК-11. По умолчанию:

host-pg-01

host-pg-02

host-pg-his-01

host-pg-his-02

- [rabbitmq]

Определение

Серверы для развёртывания брокера сообщений *RabbitMq*.

Состав

Узлы, на которых будет развёрнут компонент *RabbitMq*, реализующий коммуникацию между некоторыми клиентскими и серверными приложениями. В качестве узлов *RabbitMq* выбираются два сервера приложений СК-11, на которых будет запущена задача СК-11 "Мониторинг RabbitMq", предоставляющая точки подключения к брокеру для приложений СК-11. По умолчанию в модели "Конфигурация системы" данная задача запускается на основном и резервном серверах Основной группы host-scada-01, host-scada-02. По умолчанию:

host-scada-01

host-scada-02

- [etcd]

Определение

Серверы для развёртывания компонента *ETCD*.

Состав

Узлы, на которых будет развёрнуты службы *ETCD*. Для хранения конфигурации пар "UserId | Guid", используемых для аутентификации пользователей платформы СК-11, применяется высоконадёжное распределённое хранилище данных *ETCD*.

Должно быть указано три узла. По умолчанию первым используемым узлом указывается основной сервер host-scada-01. В качестве двух других рекомендуется использовать серверы host-web-01, host-web-02, на которых также будет развёрнут "Сервис сессий СК-11", использующий *ETCD*. По умолчанию:

host-scada-01

host-web-01

host-web-02

- [linux_dc]

Определение

Серверный узел *Службы каталогов FreeIPA*. Группа используется в конфигурациях развёртывания с использованием/установкой *Службы каталогов FreeIPA*.

Состав

По умолчанию указывается узел host-freeipa с атрибутом роли контроллера домена *Службы каталогов*:

host-freeipa freeipa_host_is_pdc=yes

- [virtual]

Определение

Контейнеры DNS-сервера, использующиеся в качестве точек подключения (прослушивателей) к отказоустойчивым ресурсам.

Состав

Список необходим при развёртывании компонентов для распознавания системой *Ansible* виртуальных имён. По умолчанию:

host-pg

host-pg-his

host-web

host-scada

- [other]

Определение

Сторонние узлы, связь с которыми требуется для обеспечения работы домена СК-11.

Состав

По умолчанию представлен пример с узлом для размещения внешних репозиториев ОС:

hostname_3

- Пример заполненного файла конфигурации

```
qa-i2-6h-depl ansible_host=10.10.10.87 ansible_user=administrator

qa-i2-6h-op1 ansible_host=10.10.10.85 ansible_user=administrator
qa-i2-6h-op2 ansible_host=10.10.10.88 ansible_user=administrator
qa-i2-6h-web1   ansible_host=10.10.10.86 ansible_user=administrator
qa-i2-6h-web2   ansible_host=10.10.10.98 ansible_user=administrator

qa-i2-6h-pg1    ansible_host=10.10.10.92 ansible_user=administrator postgresql_instance=main
qa-i2-6h-pg2    ansible_host=10.10.10.96 ansible_user=administrator postgresql_instance=main
qa-i2-6h-pg     ansible_host=10.10.10.206                           postgresql_instance=main
postgresql_entrypoint=yes

qa-i2-6h-his1   ansible_host=10.10.10.203 ansible_user=administrator postgresql_instance=his
primary_hostname=qa-i2-6h-pg1
```

```
qa-i2-6h-his2   ansible_host=10.10.10.204 ansible_user=administrator postgresql_instance=his
primary_hostname=qa-i2-6h-pg2
qa-i2-6h-his    ansible_host=10.10.10.208                            postgresql_instance=his
postgresql_entrypoint=yes

qa-i2-6h-web    ansible_host=10.10.10.207 ckll_web_entrypoint=yes
qa-i2-6h-sep  ansible_host=10.10.10.205 ckll_scada_entrypoint=yes

# Группа хостов-деплоеров (всегда один хост)
[manager]
qa-i2-6h-depl

# Группа хостов, на которые устанавливается комплекс
[ckll]
qa-i2-6h-op1
qa-i2-6h-op2
qa-i2-6h-web1
qa-i2-6h-web2

# Группа scada хостов комплекса
[ckll_scada]
qa-i2-6h-op1
qa-i2-6h-op2

# Группа web хостов комплекса
[ckll_web]
qa-i2-6h-web1 keepalived_master=yes
qa-i2-6h-web2

# Группа jsreport хостов
[jsreport]
qa-i2-6h-web1
qa-i2-6h-web2

# Группа хостов кластера postgresql
[cluster]
qa-i2-6h-pg1
qa-i2-6h-pg2
qa-i2-6h-op1

# Группа серверов postgresql
[postgresql]
qa-i2-6h-pg1
qa-i2-6h-pg2
qa-i2-6h-his1
qa-i2-6h-his2

# Группа серверов rabbitmq
[rabbitmq]
qa-i2-6h-op1
qa-i2-6h-op2

[etcd]
qa-i2-6h-op1
qa-i2-6h-web1
qa-i2-6h-web2

# Группа динамических ip, плавающих между хостами
[virtual]
qa-i2-6h-pg
qa-i2-6h-his
qa-i2-6h-web
qa-i2-6h-sep
```

1.3.1.2. Настройка параметров установки

Если параметр не требуется, устанавливается символ: [] после двоеточия (например, dns_servers_primary: []).

Строка password_changeme означает необходимость замены строки на пароль для родительского атрибута.

Атрибуты, отсутствующие в документации, менять не рекомендуется.

1. Подключиться к серверу технического обслуживания.
2. Перейти в каталог `/home/administrator/ansible/inventory/group_vars/`
3. В файле **`all/all.yaml`** задать значения следующих параметров инвентаря *Ansible*:

   `responsible_person:` ФИО и телефон для связи администратора;

   `target_instance:` псевдоним текущего экземпляра СК-11. Рекомендуется использовать в качестве псевдонима аббревиатуру названия организации. Данный псевдоним будет использоваться в информационных сообщениях CLI. Может состоять из букв латинского алфавита, цифр, символа "_";

   `deafult_timezone:` часовой пояс серверов, который будет указан при настройке СУБД *PostgreSQL*. При заполнении данного поля необходимо убедиться, что на всех серверах СК-11 используется один и тот же часовой пояс.

   Посмотреть список всех возможных часовых поясов возможно, выполнив команду:

   ```
   timedatectl list-timezones
   ```

   Смена часового пояса выполняется командой:

   ```
   sudo timedatectl set-timezone "Europe/Moscow"
   ```

   Дополнительно можно указать параметр "**`ck11_energycanonicalmodel_path`**:". Параметр указывает путь к XMI–файлу канонической модели энергосистемы, для использования пользовательской версии канонической модели.

   Если не требуется использовать пользовательскую версию канонической модели, то параметр `ck11_energycanonicalmodel_path` добавлять не следует.

4. В файле **`all/backup.yaml`** задать значения параметров резервного копирования БД *PostgreSQL*;
5. В файле **`all/network.yaml`** заполнить настройки сети, серверов синхронизации времени, DNS-серверов для параметров инвентаря *Ansible*:

   `network_mask:` короткая и полная маска подсети;

   `network_default_gateway:` адрес сетевого шлюза, используемого по умолчанию;

   `timesync_primary_servers:` список первичных ntp серверов;

   `timesync_fallback_servers:` список fallback ntp серверов;

   `dns_servers_primary:` IP-адрес первичного DNS сервера;

   `dns_servers_fallback`: список IP-адресов fallback DNS серверов;

Задать параметры домена Службы каталогов:

primary_domain: полное имя домена Службы каталогов;

primary_domain_controller: имя (hostname) контроллера домена Службы каталогов;

friend_realms: список дружественных доменов Служб каталогов.

6. Если в файле лицензии Системы отсутствует опция "HIS", удалить описание экземпляра "his" в файле **all/postgresql_cluster.yaml**.
7. В файле **all/reposytories.yaml** задать значение параметра инвентаря *Ansible*:

   reposytories_advanced: список строк подключения к репозиториям ПО, создание которых описано в разделе "Создание репозиториев из дисков Astra Linux" и добавленных в файл `/etc/apt/sources.list.d/default.list`. Пример заполнения параметра:

   ```
   reposytories_advanced:
     - deb http://10.81.169.157:80/smolensk_main stable main contrib non-free
     - deb http://10.81.169.157:80/smolensk_devel stable main contrib non-free
     - deb http://10.81.169.157:80/smolensk_main_updates_20200327 stable main contrib non-free
     - deb http://10.81.169.157:80/smolensk_devel_updates_20200327 stable main contrib non-free
   ```

8. В файле **all/users.yaml** задать значения следующих параметров инвентаря *Ansible*:

   administrator_user: имя администратора, данное при установке ОС *Astra Linux*. По умолчанию – administrator;

   administrator_password: пароль администратора, заданный при установке ОС *Astra Linux*;

   ck11_pw: пароль учётной записи 'monitel', от имени которой будут запускаться службы СК-11;

   jsreport_database: параметры подключения к БД JsReport. Необходимо изменить только пароль пользователя jsruser;

   administrators: список администраторов серверов. По умолчанию указаны администратор, заданный при установке ОС, и root;

   users: список пользователей, для которых будет разрешено подключение к серверам СК-11 по SSH. Для каждого пользователя в список ключей `ssh_keys` необходимо добавить персональные публичные SSH-ключи;

   postgresql_su_users: доменные учётные записи администраторов СК-11, которые будут иметь привилегии `superuser` в СУБД *PostgreSQL*. Данные привилегии необходимы для работы с приложениями, в которых выполняется создание новых баз данных, например, OdbCreator и "Управление рабочими моделями";

   postgresql_worker_users: доменные учётные записи, которым разрешено чтение и запись в базы данных Системы. В данный список должны быть включены учётные

записи, от имени которых проходит аутентификация сервиса "Служба управления задачами СК-11" (СК-11 Supervisor) на серверах и клиентских компьютерах. При аутентификация данных пользователей через Kerberos доступ к БД будет выполняться от имени `[postgresql_worker_user]` (по умолчанию – "ck11_krb"), являющегося владельцем всех БД Системы;

`postgresql_replication_user:` пользователь repluser, от имени которого будет выполняться репликация в *PostgreSQL*. Необходимо изменить только пароль;

`postgresql_worker_user:` пользователь *PostgreSQL*, от имени которого выполняются операции в СУБД сервисами СК-11 на серверах и клиентских компьютерах. Требуется изменить только пароль;

`postgresql_su_user:` учётная запись *PostgreSQL*, обладающая правами суперпользователя. Требуется изменить только пароль;

`postgresql_su_pwd_user:` учётная запись *PostgreSQL*, обладающая правами суперпользователя с правом подключения по логину и паролю. Требуется изменить только пароль;

`postgresql_superuser_pw:` пароль суперпользователя "*postgres*";

`ck11_server_services_user:` учётная запись пользователя, от имени которого будет выполняться аутентификация Kerberos всех серверных задач СК-11, с подготовленным keytab-файлом;

`ck11_client_services_users:` доменные пользователи, от имени которых выполняется аутентификация службы СК-11 Supervisor на клиентских компьютерах;

`ck11_admin_users:` доменные пользователи, которым будут назначены привилегии Администратора СК-11 в модели "Конфигурация системы";

`ck11_admin_hosts:` компьютеры пользователей, обладающих привилегиями Администратора СК-11 в модели "Конфигурация системы";

`ck11_sessionservice_allowed_users:` список пользователей домена, от имени которых будет проходить аутентификацию "Служба управления задачами СК-11" (СК-11 Supervisor) на серверах и клиентских компьютерах. Домен и имя пользователя указываются в нижнем регистре;

Изменить пароли пользователей **`hacluster_auth`**, **`haproxy_admin_user`**, **`rabbitmq_administrator_user`**.

9. В файле **`ck11.yaml`** задать значения следующих параметров инвентаря *Ansible*:

   `ck11_configuration_server:` полное имя (FQDN) прослушивателя основного экземпляра (main) кластера *PostgreSQL*, на котором будет развёрнута БД модели "Конфигурации системы" (odb_sysconfig);

   `ck11_smb_shares:` пути к сетевым ресурсам для монтирования к серверам СК-11. Для указания пути должны использоваться только латинские символы, а также путь не должен содержать пробелов и символов пунктуации, спецсимволов.

10. В файле **`ck11_web.yaml`** задать значения следующих параметров инвентаря *Ansible*:

    `keepalived_address:`

    `ip:` IP-адрес точки подключения WEB_EP;

mask: короткая маска подсети, из которой этот адрес;

multicast: широковещательный адрес для discovery, например, 224.0.0.32.

11. В файле **manager.yaml** задать значения следующих параметров инвентаря *Ansible*:

    ck11_deploy_user: пользователь, от имени которого будет выполняться аутентификация в *PostgreSQL* на сервере технического обслуживания при развёртывании СК-11. Необходимо указать одного из пользователей, входящих в список **[postgresql_su_users]** файла `users.yaml` с подготовленным keytab-файлом;

    ck11_init_disable_energy_schedule: запрет на поддержку расписания выпусков в объектных моделях БД, указывается всегда, когда не требуется работа в регламенте выпусков модели;

    ck11_cut_cm_by_license: при включённом параметре происходит усечение канонической модели энергетических БД в соответствии с опциями лицензии Системы. По умолчанию значение "no".

1.3.2. Три серверных узла

1. Подключиться к серверу технического обслуживания;
2. Перейти в каталог /`home/administrator/ansible/inventory/ck11.3hosts/`:

   ```
   cd ~/ansible/inventory/ck11.3hosts/
   ```

3. Выбрать каталог шаблона конфигурации развёртывания в зависимости от запланированной *Службы каталогов* и наличия её контролёра:
   a. `ad.exists` – используется установленный и настроенный контролёр *Службы каталогов MS AD*,
   b. `freeipa.exists` – используется установленный и настроенный контролёр *Службы каталогов FreeIPA*,
   c. `freeipa.install` – контроллер *Службы каталогов FreeIPA* (на выделенном узле) и домен СК-11 устанавливаются и настраиваются одновременно.
4. Скопировать содержимое выбранного каталога шаблона конфигурации развёртывания в корень каталога /`home/administrator/ansible/inventory`:

   ```
   cp -RTv ##template directory## ~/ansible/inventory
   ```

   где `##template directory##` – имя выбранного каталога шаблона конфигурации.
5. Удалить каталоги шаблонов конфигурации для всех вариантов развёртывания домена СК-11 в каталоге /`home/administrator/ansible/inventory`, оставить файл `hosts` и каталог `group_vars`, выполнив команды:

   ```
   cd ~/ansible/inventory/
   rm -r ck11.1host ck11.3hosts ck11.6hosts
   ```

6. Выполнить настройку конфигурации серверных узлов;
7. Выполнить настройку параметров установки.

1.3.2.1. Настройка конфигурации серверных узлов

1. Подключиться к серверу технического обслуживания;
2. Перейти в каталог `home/administrator/ansible/inventory/`;
3. Отредактировать файл `hosts` – установить имена и адреса серверных узлов, а также распределить их по группам в зависимости от роли.

   По умолчанию в шаблоне используются следующие обозначения, псевдонимы серверных узлов:

   host-deployer – сервер технического обслуживания, на котором развёрнута система *Ansible* для установки/обновления СК-11 и сопутствующих компонентов;

   host-scada-01 – сервер приложений оперативного контура (ОК);

   host-web-01 – сервер веб-приложений;

   host-pg-01 – узел основного экземпляра "main" *PostgreSQL*, на котором хранятся БД СК-11, кроме БД "Архив БДРВ" (HIS);

   Необходимость вспомогательного экземпляра "his" *PostgreSQL* для БД "Архив БДРВ" (HIS) определяется наличием опции лицензии "his" в файле лицензии платформы СК-11.

   host-pg-his-01 – виртуальное имя для вспомогательного экземпляра "his" PostgreSQL для хранения БД "Архив БДРВ" (HIS).

   host-freeipa – имя сервера Службы каталогов FreeIPA, для конфигурации развёртывания с использованием/установкой *Службы каталогов FreeIPA*.

   В файле `hosts` необходимо заменить псевдонимы на реальные имена серверов, которые будут использоваться в дальнейшей эксплуатации.

   При определении узлов экземпляра "his" необходимо задать `hostname` сервера в переменной **`primary_hostname`**. Например:

```
 host-pg-his-01 ansible_host=10.10.10.147 ansible_user=administrator
postgresql_instance=his primary_hostname=host-pg-01
```

   Для адресов прослушивателей экземпляров *PostgreSQL* необходимо добавить атрибут **`postgresql_entrypoint=yes`**.

```
 host-pg-01 ansible_host=10.10.10.158 postgresql_instance=main
postgresql_entrypoint=yes

 host-pg-his-01 ansible_host=10.10.10.147 postgresql_instance=his
postgresql_entrypoint=yes
```

   Для адреса точки подключения WEB_ENTRY_POINT (WEB_EP) необходимо добавить атрибут **`ck11_web_entrypoint=yes`**. Например:

```
 host-web-01 ansible_host=10.10.10.158 ck11_web_entrypoint=yes
```

   Для адреса точки подключения SCADA_ENTRY_POINT (SCADA EP) необходимо добавить атрибут **`ck11_scada_entrypoint=yes`**. Например:

```
 host-scada-01 ansible_host=10.10.10.158 ck11_scada_entrypoint=yes
```

Для серверных узлов указывается атрибут с учётной записью пользователя для использование инструментарием *Ansible*:

```
ansible_user=administrator
```

Группы узлов, имена которых заключены в квадратные скобки, позволяют распределить узлы в зависимости от их ролей. Описание групп представлено ниже.

- [manager]

Определение

Сервер технического обслуживания.

Состав

Сервер, на котором развёрнут *Ansible* для выполнения операций автоматизированного развёртывания ПО.

- [ck11]

Определение

Серверы приложений СК-11.

Состав

Узлы, на которых будет установлена серверная часть СК-11. На узлах данной группы будет развёрнута "Служба управления задачами СК-11", которая запустит задачи, определяемые описанием сервера в модели "Конфигурация системы". По умолчанию:

host-scada-01

host-web-01

- [ck11_scada]

Определение

Сервер Основной группы горячего резерва.

Состав

Узел, на котором будут запущены задачи, выполняющие обработку оперативной информации. Например, "БДРВ", "Обработка телеметрии", "Процессор топологии" и т.д. Для доступа к веб-сервисам оперативного контура используется точка подключения SCADA_EP.

По умолчанию:

host-scada-01

- [ck11_web]

Определение

Сервер группы горячего резерва "Веб-сервисы".

Состав

Узел, на котором будут запущены веб-сервисы, доступ к которым выполняется по протоколу HTTPS, с использованием имени точки подключения WEB_EP.

По умолчанию:

host-web-01

- [jsreport]

Определение

Сервер размещения компонентов *jsreport*.

Состав

Узел, на котором будут размещены компоненты *jsreport*, включая специализированную БД, для обеспечения работы веб-сервисов СК-11. Должно быть указано не более двух серверов. По умолчанию:

host-web-01

- [postgresql]

Определение

Сервер с СУБД *PostgreSQL,* включая виртуальное имя узла вспомогательного экземпляра *PostgreSQL* "his".

Состав

Узел, на котором будет развёрнут сервис *PostgreSQL* и БД СК-11. По умолчанию:

host-pg-01

host-pg-his-01

- [rabbitmq]

Определение

Сервер для развёртывания брокера сообщений *RabbitMq*.

Состав

Узел, на котором будет развёрнут компонент *RabbitMq*, реализующий коммуникацию между некоторыми клиентскими и серверными приложениями. В качестве узла *RabbitMq* выбираются сервер приложений СК-11, на котором будет запущена задача СК-11 "Мониторинг RabbitMq", предоставляющая точки подключения к брокеру для приложений СК-11. По умолчанию в модели "Конфигурация системы" данная задача запускается на основном сервере Основной группы host-scada-01. По умолчанию:

host-scada-01

- [etcd]

Определение

Сервер для развёртывания компонента *ETCD*.

Состав

Узел, на который будет развёрнута служба *ETCD*. Для хранения конфигурации пар "UserId | Guid", используемых для аутентификации пользователей платформы СК-11, применяется высоконадёжное распределённое хранилище данных *ETCD*. В случае конфигурации с тремя серверными узлами не используется механизм резервирования хранилища.

По умолчанию:

host-scada-01

- [linux_dc]

Определение

Серверный узел *Службы каталогов FreeIPA*. Группа используется в конфигурациях развёртывания с использованием/установкой *Службы каталогов FreeIPA*.

Состав

По умолчанию указывается узел host-freeipa с атрибутом роли контроллера домена *Службы каталогов*:

host-freeipa freeipa_host_is_pdc=yes

- [other]

Определение

Сторонние узлы, связь с которыми требуется для обеспечения работы домена СК-11.

Состав

По умолчанию представлен пример с узлом для размещения внешних репозиториев ОС:

hostname_3

- Пример заполненного файла конфигурации

```
qa-i2-3h-depl   ansible_host=10.10.10.95 ansible_user=administrator

qa-i2-3h-op1  ansible_host=10.10.10.94 ansible_user=administrator ck11_scada_entrypoint=yes
qa-i2-3h-web1    ansible_host=10.10.10.93 ansible_user=administrator ck11_web_entrypoint=yes

qa-i2-3h-pg1     ansible_host=10.10.10.97 ansible_user=administrator postgresql_instance=main
postgresql_entrypoint=yes
qa-i2-3h-his    ansible_host=10.10.10.202 ansible_user=administrator postgresql_instance=his
primary_hostname=qa-i2-3h-pg1 postgresql_entrypoint=yes

# Группа хостов-деплоеров (всегда один хост)
[manager]
qa-i2-3h-depl

# Группа хостов, на которые устанавливается комплекс
[ck11]
qa-i2-3h-op1
qa-i2-3h-web1

# Группа scada хостов комплекса
[ck11_scada]
qa-i2-3h-op1
```

```
# Группа web хостов комплекса
[ck11_web]
qa-i2-3h-web1

# Группа серверов postgresql
[postgresql]
qa-i2-3h-pg1
qa-i2-3h-his

# Группа серверов rabbitmq
[rabbitmq]
qa-i2-3h-op1

[etcd]
qa-i2-3h-op1
qa-i2-3h-web1
```

1.3.2.2. Настройка параметров установки

Если параметр не требуется, устанавливается символ: [] после двоеточия (например, dns_servers_primary: []).

Строка password_changeme означает необходимость замены строки на пароль для родительского атрибута.

Атрибуты, отсутствующие в документации, менять не рекомендуется.

1. Подключиться к серверу технического обслуживания.
2. Перейти в каталог `/home/administrator/ansible/inventory/group_vars/`
3. В файле **`all/all.yaml`** задать значения следующих параметров инвентаря *Ansible*:

   `responsible_person:` ФИО и телефон для связи администратора;

   `target_instance:` псевдоним текущего экземпляра СК-11. Рекомендуется использовать в качестве псевдонима аббревиатуру названия организации. Данный псевдоним будет использоваться в информационных сообщениях CLI. Может состоять из букв латинского алфавита, цифр, символа "_";

   `deafult_timezone:` часовой пояс серверов, который будет указан при настройке СУБД *PostgreSQL*. При заполнении данного поля необходимо убедиться, что на всех серверах СК-11 используется один и тот же часовой пояс.

Посмотреть список всех возможных часовых поясов возможно, выполнив команду:

```
timedatectl list-timezones
```

Смена часового пояса выполняется командой:

```
sudo timedatectl set-timezone "Europe/Moscow"
```

   Дополнительно можно указать параметр "**`ck11_energycanonicalmodel_path`**:". Параметр указывает путь к XMI–файлу канонической модели энергосистемы, для использования пользовательской версии канонической модели.

Если не требуется использовать пользовательскую версию канонической модели, то параметр `ck11_energycanonicalmodel_path` добавлять не следует.

4. В файле **all/backup.yaml** задать значения параметров резервного копирования БД *PostgreSQL*;
5. В файле **all/network.yaml** заполнить настройки сети, серверов синхронизации времени, DNS-серверов для параметров инвентаря *Ansible*:

   network_mask: короткая и полная маска подсети;

   network_default_gateway: адрес сетевого шлюза, используемого по умолчанию;

   timesync_primary_servers: список первичных ntp серверов;

   timesync_fallback_servers: список fallback ntp серверов;

   dns_servers_primary: IP-адрес первичного DNS сервера;

   dns_servers_fallback: список IP-адресов fallback DNS серверов;

   Задать параметры домена Службы каталогов:

   primary_domain: полное имя домена Службы каталогов;

   primary_domain_controller: имя (hostname) контроллера домена Службы каталогов;

   friend_realms: список дружественных доменов Служб каталогов.
6. Если в файле лицензии Системы отсутствует опция "HIS", удалить описание экземпляра "his" в файле **all/postgresql.yaml**.
7. В файле **all/repsytoryes.yaml** задать значение параметра инвентаря *Ansible*:

   reposytoryes_advanced: список строк подключения к репозиториям ПО, создание которых описано в разделе "Создание репозиториев из дисков Astra Linux" и добавленных в файл `/etc/apt/sources.list.d/default.list`. Пример заполнения параметра:

```
reposytoryes_advanced:
  - deb http://10.81.169.157:80/smolensk_main stable main contrib non-free
  - deb http://10.81.169.157:80/smolensk_devel stable main contrib non-free
  - deb http://10.81.169.157:80/smolensk_main_updates_20200327 stable main contrib non-free
  - deb http://10.81.169.157:80/smolensk_devel_updates_20200327 stable main contrib non-free
```

8. В файле **all/users.yaml** задать значения следующих параметров инвентаря *Ansible*:

   administrator_user: имя администратора, данное при установке ОС *Astra Linux*. По умолчанию – administrator;

   administrator_password: пароль администратора, заданный при установке ОС *Astra Linux;*

   ck11_pw: пароль учётной записи 'monitel', от имени которой будут запускаться службы СК-11;

   jsreport_database: параметры подключения к БД JsReport. Необходимо изменить только пароль пользователя jsruser;

administrators: список администраторов серверов. По умолчанию указаны администратор, заданный при установке ОС, и root;

users: список пользователей, для которых будет разрешено подключение к серверам СК-11 по SSH. Для каждого пользователя в список ключей `ssh_keys` необходимо добавить персональные публичные SSH-ключи;

postgresql_su_users: доменные учётные записи администраторов СК-11, которые будут иметь привилегии `superuser` в СУБД *PostgreSQL*. Данные привилегии необходимы для работы с приложениями, в которых выполняется создание новых баз данных, например, OdbCreator и "Управление рабочими моделями";

postgresql_worker_users: доменные учётные записи, которым разрешено чтение и запись в базы данных Системы. В данный список должны быть включены учётные записи, от имени которых проходит аутентификация сервиса "Служба управления задачами СК-11" (СК-11 Supervisor) на серверах и клиентских компьютерах. При аутентификации данных пользователей через Kerberos доступ к БД будет выполняться от имени `[postgresql_worker_user]` (по умолчанию – "ck11_krb"), являющегося владельцем всех БД Системы;

postgresql_replication_user: пользователь repluser, от имени которого будет выполняться репликация в *PostgreSQL*. Необходимо изменить только пароль;

postgresql_worker_user: пользователь *PostgreSQL*, от имени которого выполняются операции в СУБД сервисами СК-11 на серверах и клиентских компьютерах. Требуется изменить только пароль;

postgresql_su_user: учётная запись *PostgreSQL*, обладающая правами суперпользователя. Требуется изменить только пароль;

postgresql_su_pwd_user: учётная запись *PostgreSQL*, обладающая правами суперпользователя с правом подключения по логину и паролю. Требуется изменить только пароль;

postgresql_superuser_pw: пароль суперпользователя "*postgres*";

ck11_server_services_user: учётная запись пользователя, от имени которого будет выполняться аутентификация Kerberos всех серверных задач СК-11, с подготовленным keytab-файлом

ck11_client_services_users: доменные пользователи, от имени которых выполняется аутентификация службы СК-11 Supervisor на клиентских компьютерах;

ck11_admin_users: доменные пользователи, которым будут назначены привилегии Администратора СК-11 в модели "Конфигурация системы";

ck11_admin_hosts: компьютеры пользователей, обладающих привилегиями Администратора СК-11 в модели "Конфигурация системы";

ck11_sessionservice_allowed_users: список пользователей домена, от имени которых будет проходить аутентификацию "Служба управления задачами СК-11" (СК-11 Supervisor) на серверах и клиентских компьютерах. Домен и имя пользователя указываются в нижнем регистре;

Изменить пароль пользователя **rabbitmq_administrator_user**.

9. В файле **ck11.yaml** задать значения следующих параметров инвентаря *Ansible*:

   ck11_configuration_server: полное имя (FQDN) узла host-pg-01 СУБД *PostgreSQL*, на котором будет развёрнута БД модели "Конфигурации системы" (odb_sysconfig);

   ck11_smb_shares: пути к сетевым ресурсам для монтирования к серверам СК-11. Для указания пути должны использоваться только латинские символы, а также путь не должен содержать пробелов и символов пунктуации, спецсимволов.

10. В файле **manager.yaml** задать значения следующих параметров инвентаря *Ansible*:

    ck11_deploy_user: пользователь, от имени которого будет выполняться аутентификация в *PostgreSQL* на сервере технического обслуживания при развёртывании СК-11. Необходимо указать одного из пользователей, входящих в список **[postgresql_su_users]** файла `users.yaml`, с подготовленным keytab-файлом;

    ck11_init_disable_energy_schedule: запрет на поддержку расписания выпусков в объектных моделях БД, указывается всегда, когда не требуется работа в регламенте выпусков модели;

    ck11_cut_cm_by_license: при включённом параметре происходит усечение канонической модели энергетических БД в соответствии с опциями лицензии Системы. По умолчанию должно быть "yes".

1.3.3. Один серверный узел

1. Подключиться к серверу технического обслуживания;
2. Перейти в каталог /home/administrator/ansible/inventory/ck11.1host/:

   ```
   cd ~/ansible/inventory/ck11.1host/
   ```

3. Выбрать каталог шаблона конфигурации развёртывания в зависимости от запланированной *Службы каталогов* и наличия её контролёра:
   a. `ad.exists` – используется установленный и настроенный контролёр *Службы каталогов MS AD,*
   b. `freeipa.exists` – используется установленный и настроенный контролёр *Службы каталогов FreeIPA,*
   c. `freeipa.install` – контроллер *Службы каталогов FreeIPA* (на выделенном узле) и домен СК-11 устанавливаются и настраиваются одновременно;
   d. `freeipa.onehost` – контроллер *Службы каталогов FreeIPA* и домен СК-11 устанавливаются и настраиваются одновременно на одном узле.
4. Скопировать содержимое выбранного каталога шаблона конфигурации развёртывания в корень каталога /home/administrator/ansible/inventory:

   ```
   cp -RTv ##template directory## ~/ansible/inventory
   ```

   где `##template directory##` – имя выбранного каталога шаблона конфигурации.
5. Удалить каталоги шаблонов конфигурации для всех вариантов развёртывания домена СК-11 в каталоге /home/administrator/ansible/inventory, оставить файл `hosts` и каталог `group_vars`, выполнив команды:

   ```
   cd ~/ansible/inventory/
   rm -r ck11.1host ck11.3hosts ck11.6hosts
   ```

6. Выполнить настройку конфигурации серверных узлов;
7. Выполнить настройку параметров установки.

1.3.3.1. Настройка конфигурации серверного узла

1. Подключиться к серверу технического обслуживания;
2. Перейти в каталог `home/administrator/ansible/inventory/`;
3. Отредактировать файл `hosts` – установить имена и адреса серверных узлов, а также распределить их по группам в зависимости от роли.

   По умолчанию в шаблоне используются следующие обозначения, псевдонимы серверных узлов:

   host-deployer – сервер технического обслуживания, на котором развёрнута система *Ansible* для установки/обновления СК-11 и сопутствующих компонентов;

   host-scada-01 – сервер оперативного контура (ОК), сервер группы горячего резерва "Веб-сервисы", узел основного экземпляра "main" *PostgreSQL*, на котором хранятся БД СК-11, кроме БД "Архив БДРВ" (HIS);

Необходимость вспомогательного экземпляра "his" *PostgreSQL* для БД "Архив БДРВ" (HIS) определяется наличием опции лицензии "his" в файле лицензии платформы СК-11.

host-pg-his-01 – виртуальное имя для вспомогательного экземпляра "his" PostgreSQL для хранения БД "Архив БДРВ" (HIS).

host-freeipa – имя сервера *Службы каталогов FreeIPA*, для конфигурации развёртывания с использованием/установкой *Службы каталогов FreeIPA*.

ck11-proxywin10 – для конфигурации развёртывания с установкой *Службы каталогов FreeIPA* на одном узле с Системой может быть задан узел на ОС *Windows*, который требуется связать с доменом.

В файле `hosts` необходимо заменить псевдонимы на реальные имена серверов, которые будут использоваться в дальнейшей эксплуатации.

При определении узлов экземпляра "his" необходимо задать `hostname` сервера в переменной **`primary_hostname`**. Например:

```
host-pg-his-01 ansible_host=10.10.10.147 ansible_user=administrator
postgresql_instance=his primary_hostname=host-pg-01
```

Для адресов прослушивателей экземпляров *PostgreSQL* необходимо добавить атрибут **`postgresql_entrypoint=yes`**.

```
host-scada-01 ansible_host=10.10.10.158 postgresql_instance=main
postgresql_entrypoint=yes
```

```
host-pg-his-01 ansible_host=10.10.10.147 postgresql_instance=his
postgresql_entrypoint=yes
```

Для адреса точки подключения WEB_ENTRY_POINT (WEB_EP) необходимо добавить атрибут **`ck11_web_entrypoint=yes`**. Например:

```
host-scada-01 ansible_host=10.10.10.158 ck11_web_entrypoint=yes
```

Для адреса точки подключения SCADA_ENTRY_POINT (SCADA EP) необходимо добавить атрибут **`ck11_scada_entrypoint=yes`**. Например:

```
host-scada-01 ansible_host=10.10.10.158 ck11_scada_entrypoint=yes
```

Для серверных узлов указывается атрибут с учётной записью пользователя для использование инструментарием *Ansible*:

```
ansible_user=administrator
```

Группы узлов, имена которых заключены в квадратные скобки, позволяют распределить узлы в зависимости от их ролей. Описание групп представлено ниже.

- [manager]

Определение

Сервер технического обслуживания.

Состав

Сервер, на котором развёрнут *Ansible* для выполнения операций автоматизированного развёртывания ПО.

- [ck11]

Определение

Серверы приложений СК-11.

Состав

Узел, на котором будет установлена серверная часть СК-11. На узле данной группы будет развёрнута "Служба управления задачами СК-11", которая запустит задачи, определяемые описанием сервера в модели "Конфигурация системы". По умолчанию:

host-scada-01

- [ck11_scada]

Определение

Сервер Основной группы горячего резерва.

Состав

Узел, на котором будут запущены задачи, выполняющие обработку оперативной информации. Например, "БДРВ", "Обработка телеметрии", "Процессор топологии" и т.д. Для доступа к веб-сервисам оперативного контура используется точка подключения SCADA_EP.

По умолчанию:

host-scada-01

- [ck11_web]

Определение

Сервер группы горячего резерва "Веб-сервисы".

Состав

Узел, на которых будут запущены веб-сервисы, доступ к которым выполняется по протоколу HTTPS, с использованием имени точки подключения WEB_EP.

По умолчанию:

host-scada-01

- [jsreport]

Определение

Сервер размещения компонентов *jsreport*.

Состав

Узел, на котором будут размещены компоненты *jsreport*, включая специализированную БД, для обеспечения работы веб-сервисов СК-11. Должно быть указано не более двух серверов. По умолчанию:

host-scada-01

- [postgresql]

Определение

Сервер с СУБД *PostgreSQL*, включая виртуальное имя узла вспомогательного экземпляра *PostgreSQL* "his".

Состав

Узел, на котором будет развёрнут сервис *PostgreSQL* и БД СК-11. По умолчанию:

host-scada-01

host-pg-his-01

- [rabbitmq]

Определение

Сервер для развёртывания брокера сообщений *RabbitMq*.

Состав

Узел, на котором будет развёрнут компонент *RabbitMq*, реализующий коммуникацию между некоторыми клиентскими и серверными приложениями. В качестве узла *RabbitMq* выбирается сервер приложений СК-11, на котором будет запущена задача СК-11 "Мониторинг RabbitMq", предоставляющая точки подключения к брокеру для приложений СК-11. По умолчанию:

host-scada-01

- [etcd]

Определение

Сервер для развёртывания компонента *ETCD*.

Состав

Узел, на который будет развёрнута служба *ETCD*. Для хранения конфигурации пар "UserId | Guid", используемых для аутентификации пользователей платформы СК-11, применяется высоконадёжное распределённое хранилище данных *ETCD*. В случае конфигурации с одним серверным узлом не используется механизм резервирования хранилища.

По умолчанию:

host-scada-01

- [linux_dc]

  Определение

  Серверный узел *Службы каталогов FreeIPA*. Группа используется в конфигурациях развёртывания с использованием/установкой *Службы каталогов FreeIPA*.

  Состав

  По умолчанию указывается узел host-freeipa с атрибутом роли контроллера домена *Службы каталогов*:

  host-freeipa freeipa_host_is_pdc=yes

  Для конфигурации развёртывания с установкой *Службы каталогов FreeIPA* на одном узле с Системой по умолчанию:

  host-scada-01 freeipa_host_is_pdc=yes

- [windows]

  Определение

  Группа для узлов на ОС Windows, для которых необходимо сгенерировать скрипты подключения к домену

  Состав

  По умолчанию:

  ck11-proxywin10

- [other]

  Определение

  Сторонние узлы, связь с которыми требуется для обеспечения работы домена СК-11.

  Состав

  По умолчанию представлен пример с узлом для размещения внешних репозиториев ОС:

  hostname_3

- Пример заполненного файла конфигурации

```
qa-i2-1h-depl ansible_host=10.10.10.91 ansible_user=administrator

qa-i2-1h-op1     ansible_host=10.10.10.84  ansible_user=administrator postgresql_instance=main
ck11_scada_entrypoint=yes ck11_web_entrypoint=yes postgresql_entrypoint=yes
qa-i2-1h-his ansible_host=10.10.10.201 ansible_user=administrator postgresql_instance=his
primary_hostname=qa-i2-1h-op1 postgresql_entrypoint=yes

# Группа хостов-деплоеров (всегда один хост)
[manager]
qa-i2-1h-depl

# Группа хостов, на которые устанавливается комплекс
[ck11]
qa-i2-1h-op1

# Группа scada хостов комплекса
[ck11_scada]
qa-i2-1h-op1
```

```
# Группа web хостов комплекса
[ck11_web]
qa-i2-1h-op1

# Группа серверов postgresql
[postgresql]
qa-i2-1h-op1
qa-i2-1h-his

# Группа серверов rabbitmq
[rabbitmq]
qa-i2-1h-op1

[etcd]
qa-i2-1h-op1
```

1.3.3.2. Настройка параметров установки

Если параметр не требуется, устанавливается символ: [] после двоеточия (например, dns_servers_primary: []).

Строка password_changeme означает необходимость замены строки на пароль для родительского атрибута.

Атрибуты, отсутствующие в документации, менять не рекомендуется.

1. Подключиться к серверу технического обслуживания.
2. Перейти в каталог `/home/administrator/ansible/inventory/group_vars/`
3. В файле **`all/all.yaml`** задать значения следующих параметров инвентаря *Ansible*:

   `responsible_person:` ФИО и телефон для связи администратора;

   `target_instance:` псевдоним текущего экземпляра СК-11. Рекомендуется использовать в качестве псевдонима аббревиатуру названия организации. Данный псевдоним будет использоваться в информационных сообщениях CLI. Может состоять из букв латинского алфавита, цифр, символа "_";

   `deafult_timezone:` часовой пояс серверов, который будет указан при настройке СУБД *PostgreSQL*. При заполнении данного поля необходимо убедиться, что на всех серверах СК-11 используется один и тот же часовой пояс.

Посмотреть список всех возможных часовых поясов возможно, выполнив команду:

```
timedatectl list-timezones
```

Смена часового пояса выполняется командой:

```
sudo timedatectl set-timezone "Europe/Moscow"
```

Дополнительно можно указать параметр "**`ck11_energycanonicalmodel_path`**:". Параметр указывает путь к XMI–файлу канонической модели энергосистемы, для использования пользовательской версии канонической модели.

Если не требуется использовать пользовательскую версию канонической модели, то параметр `ck11_energycanonicalmodel_path` добавлять не следует.

4. В файле **all/backup.yaml** задать значения параметров резервного копирования БД *PostgreSQL*;
5. В файле **all/network.yaml** заполнить настройки сети, серверов синхронизации времени, DNS-серверов для параметров инвентаря *Ansible*:

   network_mask: короткая и полная маска подсети;

   network_default_gateway: адрес сетевого шлюза, используемого по умолчанию;

   timesync_primary_servers: список первичных ntp серверов;

   timesync_fallback_servers: список fallback ntp серверов;

   dns_servers_primary: IP-адрес первичного DNS сервера;

   dns_servers_fallback: список IP-адресов fallback DNS серверов;

   Задать параметры домена Службы каталогов:

   primary_domain: полное имя домена Службы каталогов;

   primary_domain_controller: имя (hostname) контроллера домена Службы каталогов;

   friend_realms: список дружественных доменов Служб каталогов.
6. Если в файле лицензии Системы отсутствует опция "HIS", удалить описание экземпляра "his" в файле **all/postgresql.yaml**.
7. В файле **all/repsytoryes.yaml** задать значение параметра инвентаря *Ansible*:

   reposytoryes_advanced: список строк подключения к репозиториям ПО, создание которых описано в разделе "Создание репозиториев из дисков Astra Linux" и добавленных в файл `/etc/apt/sources.list.d/default.list`. Пример заполнения параметра:

```
reposytoryes_advanced:
  - deb http://10.81.169.157:80/smolensk_main stable main contrib non-free
  - deb http://10.81.169.157:80/smolensk_devel stable main contrib non-free
  - deb http://10.81.169.157:80/smolensk_main_updates_20200327 stable main contrib non-free
  - deb http://10.81.169.157:80/smolensk_devel_updates_20200327 stable main contrib non-free
```

8. В файле **all/users.yaml** задать значения следующих параметров инвентаря *Ansible*:

   administrator_user: имя администратора, данное при установке ОС *Astra Linux*. По умолчанию – administrator;

   administrator_password: пароль администратора, заданный при установке ОС *Astra Linux*;

   ck11_pw: пароль учётной записи 'monitel', от имени которой будут запускаться службы СК-11;

   jsreport_database: параметры подключения к БД JsReport. Необходимо изменить только пароль пользователя jsruser;

administrators: список администраторов серверов. По умолчанию указаны администратор, заданный при установке ОС, и root;

users: список пользователей, для которых будет разрешено подключение к серверам СК-11 по SSH. Для каждого пользователя в список ключей `ssh_keys` необходимо добавить персональные публичные SSH-ключи;

postgresql_su_users: доменные учётные записи администраторов СК-11, которые будут иметь привилегии `superuser` в СУБД *PostgreSQL*. Данные привилегии необходимы для работы с приложениями, в которых выполняется создание новых баз данных, например, OdbCreator и "Управление рабочими моделями";

postgresql_worker_users: доменные учётные записи, которым разрешено чтение и запись в базы данных Системы. В данный список должны быть включены учётные записи, от имени которых проходит аутентификация сервиса "Служба управления задачами СК-11" (СК-11 Supervisor) на серверах и клиентских компьютерах. При аутентификация данных пользователей через Kerberos доступ к БД будет выполняться от имени `[postgresql_worker_user]` (по умолчанию – "ck11_krb"), являющегося владельцем всех БД Системы;

postgresql_replication_user: пользователь repluser, от имени которого будет выполняться репликация в *PostgreSQL*. Необходимо изменить только пароль;

postgresql_worker_user: пользователь *PostgreSQL*, от имени которого выполняются операции в СУБД сервисами СК-11 на серверах и клиентских компьютерах. Требуется изменить только пароль;

postgresql_su_user: учётная запись *PostgreSQL*, обладающая правами суперпользователя. Требуется изменить только пароль;

postgresql_su_pwd_user: учётная запись *PostgreSQL*, обладающая правами суперпользователя с правом подключения по логину и паролю. Требуется изменить только пароль;

postgresql_superuser_pw: пароль суперпользователя "*postgres*";

ck11_server_services_user: учётная запись пользователя, от имени которого будет выполняться аутентификация Kerberos всех серверных задач СК-11, с подготовленным keytab-файлом;

ck11_client_services_users: доменные пользователи, от имени которых выполняется аутентификация службы СК-11 Supervisor на клиентских компьютерах;

ck11_admin_users: доменные пользователи, которым будут назначены привилегии Администратора СК-11 в модели "Конфигурация системы";

ck11_admin_hosts: компьютеры пользователей, обладающих привилегиями Администратора СК-11 в модели "Конфигурация системы";

ck11_sessionservice_allowed_users: список пользователей домена, от имени которых будет проходить аутентификацию "Служба управления задачами СК-11" (СК-11 Supervisor) на серверах и клиентских компьютерах. Домен и имя пользователя указываются в нижнем регистре;

Изменить пароль пользователя **rabbitmq_administrator_user**.

9. В файле **ck11.yaml** задать значения следующих параметров инвентаря *Ansible*:

   ck11_configuration_server: полное имя (FQDN) узла host-scada-01, на котором будет развёрнута БД модели "Конфигурации системы" (odb_sysconfig);

   ck11_smb_shares: пути к сетевым ресурсам для монтирования к серверам СК-11. Для указания пути должны использоваться только латинские символы, а также путь не должен содержать пробелов и символов пунктуации, спецсимволов.

10. В файле **manager.yaml** задать значения следующих параметров инвентаря *Ansible*:

    ck11_deploy_user: пользователь, от имени которого будет выполняться аутентификация в *PostgreSQL* на сервере технического обслуживания при развёртывании СК-11. Необходимо указать одного из пользователей, входящих в список **[postgresql_su_users]** файла `users.yaml`, с подготовленным keytab-файлом

    ck11_init_disable_energy_schedule: запрет на поддержку расписания выпусков в объектных моделях БД, указывается всегда, когда не требуется работа в регламенте выпусков модели;

    ck11_cut_cm_by_license: при включённом параметре происходит усечение канонической модели энергетических БД в соответствии с опциями лицензии Системы. По умолчанию должно быть "yes".

1.3.4. Настройка конфигурации Службы каталогов FreeIPA

Если параметр не требуется, устанавливается символ: [] после двоеточия (например, dns_servers_primary: []).

Строка password_changeme означает необходимость замены строки на пароль для родительского атрибута.

Атрибуты, отсутствующие в документации, менять не рекомендуется.

1. Подключиться к серверу технического обслуживания;
2. Перейти в каталог `home/administrator/ansible/inventory/`;
3. Отредактировать файл `hosts`, задать значения псевдонимов, установив имена и адреса серверных узлов:

   host-freeipa – имя сервера *Службы каталогов FreeIPA*, для конфигурации развёртывания с использованием/установкой *Службы каталогов FreeIPA;*

   ck11-proxywin10 – для конфигурации развёртывания с установкой *Службы каталогов FreeIPA* на одном узле с Системой может быть задан узел на ОС *Windows*, который требуется связать с доменом;

   Заполнить значения псевдонимов узлов для групп [linux_dc], [windows].

4. Перейти в каталог `/home/administrator/ansible/inventory/group_vars/`
5. В файле **all/all.yaml** задать значения следующих параметров инвентаря *Ansible:*

   freeipa_domain_controller: в зависимости от конфигурации развёртывания указывается использование контроллера *Службы каталогов FreeIPA;*

freeipa_already_installed: определяет необходимость установки контроллера *Службы каталогов FreeIPA*. В случае использования имеющегося контроллера *Службы каталогов FreeIPA* указывается значение "yes";

ca_certificate_passphrase: для конфигурации развёртывания с установкой контроллера *Службы каталогов FreeIPA* указывается парольная фраза для генерации SSL-сертификатов.

6. В файле **all/users.yaml** задать значения следующих параметров инвентаря *Ansible* для секции "freeipa users":

   freeipa_admin_pw: пароль администратора для домена *FreeIPA*, в случае конфигурации развёртывания с использованием/установкой контроллера *Службы каталогов FreeIPA*;

   domain_users: список пользователей для домена *FreeIPA*;

7. Для случая конфигурации развёртывания с установкой контроллера *Службы каталогов FreeIPA в* файле **all/network.yaml** задать значения следующих параметров инвентаря *Ansible*:

   domain_network: указывается подсеть домена;

   target_freeipa_host: указывается имя (hostname) контроллера *Службы каталогов FreeIPA*, для его установки.

8. Для конфигурации развёртывания с установкой контроллера *Службы каталогов FreeIPA* в файле **all/dc.yaml** задать значения следующих параметров инвентаря *Ansible:*

   domain_members: указываю узлы на ОС *Windows*, которые требуется связать с доменом;

   domain_services: указываются параметры по образцу для подготовки keytab-файлов аутентификации через Kerberos.

1.3.5. Монтирование хранилища для резервных копий БД

На серверах, указанных в группе `[postgresql]` файла `hosts` инвентаря *Ansible*, смонтировать в каталог `/backup` внешнее хранилище для экземпляров *PostgreSQL*, имеющее достаточное количество свободного места для хранения резервных копий БД.

1.4. Установка программного обеспечения СК-11

1. Выполнить подключение к серверу технического обслуживания;
2. Создать терминальную сессию командой:

   ```
   tmux
   ```

3. Перейти в `/home/administrator/`;
4. Выполнить команды:

   ```
   cd ansible
   make play
   ```

Если во время выполнения команд `make` прервалась сессия SSH, после переподключения можно открыть сессию с установкой, выполнив команду:

```
tmux a
```

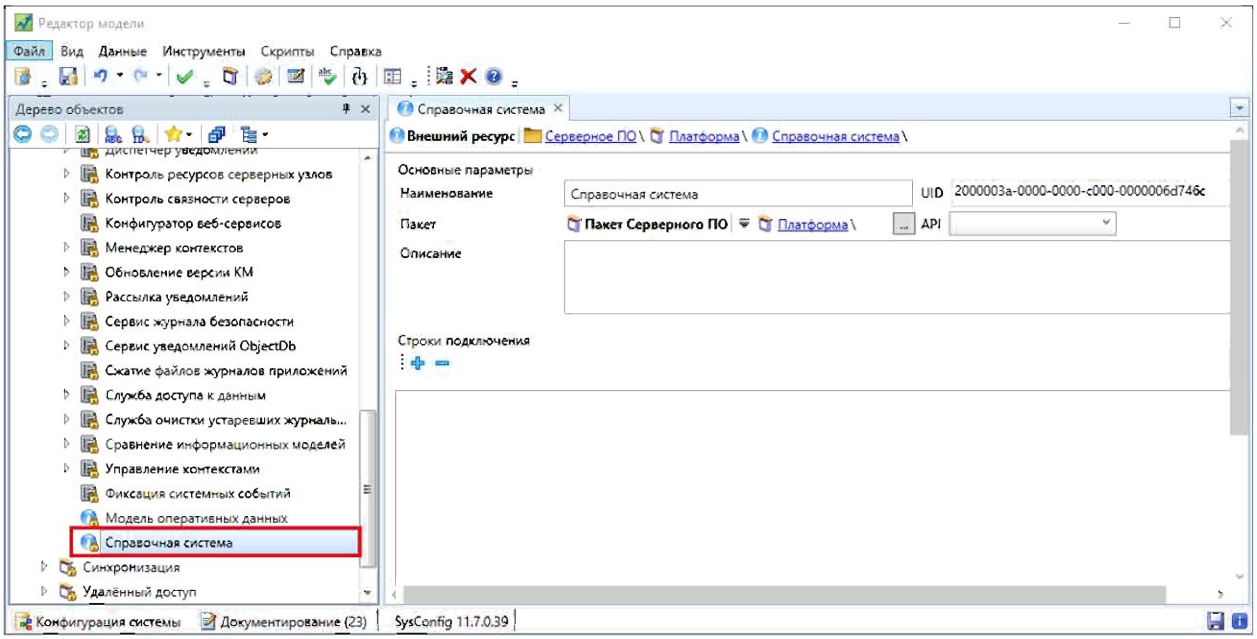
Развёртывание и настройка отказоустойчивого кластера СУБД *PostgreSQL*, если его использование предусмотрено конфигурацией, выполняется автоматизированно.

После завершения установки серверной части СК-11 можно подключиться по SSH к серверам приложений домена СК-11 и с помощью точки входа в управление процессами СК-11 ck11ctl проверить работоспособность серверной части.

1.5. Настройка Справочной системы

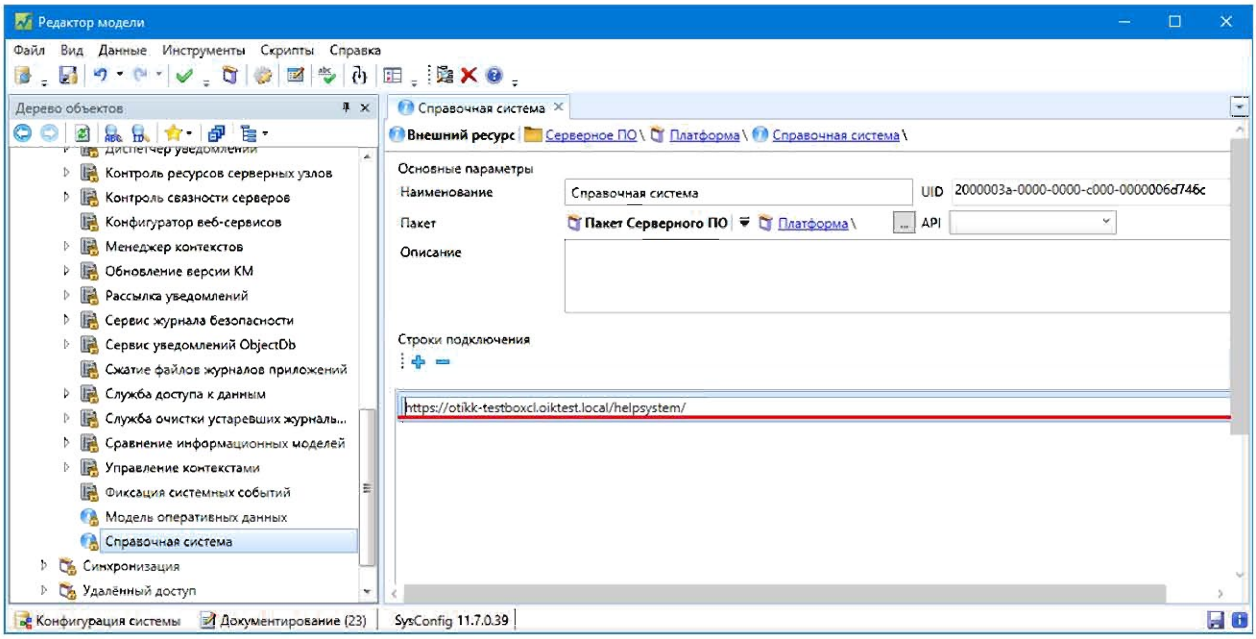
На платформе Linux **Справочная система** для установки поставляется совместно с дистрибутивом платформы СК-11. Установка Справочной системы выполняется совместно с платформой СК-11. После установки требуется выполнить следующие шаги по настройке Справочной системы:

1. Запустить приложение "Редактор модели". Создать новую версию от актуальной в информационной модели "Конфигурация системы".
2. Перейти в базовом дереве по пути: Серверное ПО ⇨ Платформа. Открыть для редактирования экземпляр объекта внешнего ресурса "Справочная система" (UID 2000003A-0000-0000-C000-0000006D746C):



3. Добавить строку подключения для ресурса с помощью кнопки ✚ в области "Строки подключения". Ввести адрес сайта Справочной системы в добавленную строку в формате: `https://[FQDN_WEB_ENTRY_POINT]/helpsystem/`, где [FQDN_WEB_ENTRY_POINT] – полное сетевое имя балансировщика нагрузки WebAPI (UID 20001445-0000-0000-C000-0000006D746C).

> ⚠ Наличие слеша (/) в конце адреса обязательно.



4. Сохранить изменения в БД.
5. Актуализировать отредактированную версию модели "Конфигурация системы".
6. Проверить работоспособность Справочной системы СК-11 по следующему URL (косая черта / в конце обязательна) – `https://[FQDN_WEB_ENTRY_POINT]/helpsystem/`, где `[FQDN_WEB_ENTRY_POINT]` – полное сетевое имя балансировщика нагрузки WebAPI домена СК-11.

> Сайт Справочной системы будет доступен пользователям по адресу: `https://[FQDN_WEB_ENTRY_POINT]/helpsystem/`.

1.6. Установка программного обеспечения СК-11 с предустановленной СУБД PostgreSQL

Доступен вариант установки программного обеспечения СК-11 с предустановленной СУБД *PostgreSQL* на целевых серверах домена СК-11. Данный вариант установки отличается от обычного только тем, что программа установки не выполняет установку и настройку СУБД *PostgreSQL*, а только создаёт базы данных Системы.

Перед установкой СК-11 необходимо последовательно выполнить следующие этапы:

1. Подготовка к установке.
2. Подготовка сервера технического обслуживания.
3. Установить и настроить СУБД *PostgreSQL* на целевые серверы. При необходимости самостоятельно настроить отказоустойчивый кластер *PostgreSQL*. Создать два экземпляра (instance) *PostgreSQL*: main и his. Экземпляр "main" будет использован для хранения всех БД СК-11, кроме БД архива оперативной информации "his". Соответственно, экземпляр "his" будет использован для хранения БД "Архив БДРВ".

Наименование создаваемых экземпляров (instance) *PostgreSQL* должно соответствовать используемым по умолчанию (main, his).

Необходимость вспомогательного экземпляра "his" *PostgreSQL* для БД "Архив БДРВ" (HIS) определяется наличием опции лицензии "his" в файле лицензии платформы СК-11.

4. Настройка инвентаря Ansible. При заполнении инвентаря *Ansible* требуется учесть следующие особенности данного варианта развёртывания СК-11:
   a. в конфигурации серверных узлов указать соответствующие серверные узлы с установленной СУБД *PostgreSQL*. Указать значения соответствующих псевдонимов для экземпляров (instance) *PostgreSQL* "main" и "his";
   b. в файле `all/users.yaml` для параметра `postgresql_su_user` указать имеющуюся учётную запись *PostgreSQL*, обладающую правами суперпользователя. При заполнении параметра `postgresql_su_users`, соответствующие учётные записи пользователей *PostgreSQL* будут созданы при установке Системы.

Для установки программного обеспечения СК-11 с предустановленной СУБД *PostgreSQL* выполнить следующие действия:

1. Выполнить подключение к серверу технического обслуживания.
2. Создать терминальную сессию командой: `tmux`
3. Перейти в: `/home/administrator/`
4. Выполнить команды:

```
cd ansible

make without_postgresql play
```

Если во время выполнения команд `make` прервалась сессия SSH, после переподключения можно открыть сессию с установкой, выполнив команду: `tmux a`

2. Установка «СК11.Equipment Inspection Logbook» («СК11.Обходы»)

2.1. Распаковать архив дистрибутива. На Deployer-сервер домена СК-11 скопировать дистрибутив пакета ПО *СК11.Обходы* («`EquipmentInspections_1.0`»).

2.2. Открыть терминал командной строки от имени сервисного пользователя СК-11 в каталоге «`EquipmentInspections_1.0`».

2.3. Запустить в терминале приложение *PkgInstall*, заменив макроподстановки:

- `##WEB_EP_FQDN##` – полное имя точки подключения WEB_EP;
- `##Private_Key##` - приватный ключ сервисного пользователя СК-11
- ##Administrator_name## - логин сервисного пользователя

CMD	Запуск PkgInstall
`dotnet PkgInstall.dll /malmemory:4096 /sshkeypath:/home/##Administrator_name##/.ssh/##Private_Key## /sshuser: ##Administrator_name## /createbackup:false /webep: ##WEB_EP_FQDN##`	

2.4. В процессе установки в терминале будут возникать сообщения, требующие реакции пользователя путем нажатия определенных клавиш:

Сообщение	Корректная реакция
Вы хотите установить пакет 'EquipmentInspections' для СК-11?	Да (клавиша Y)
Всё готово к установке пакета EquipmentInspections. Установить пакет EquipmentInspections?	Да (клавиша Y)
В процессе выполнения операции 'Создание БД EF_EquipmentInspections на FQDN_SQL_SERVER@PgSQL' произошла ошибка. Ошибка при создании БД Вы можете повторить выполнение операции, проигнорировать ошибку или прервать установку. Выберите требуемое действие.	Проверить ошибку в журнале установки (`PkgInstall.yyyyMMdd.usrlog`), устранить ее и выбрать вариант Повторить (клавиша R)

2.5. Дождаться окончания установки и проверить, что журнал установки (`PkgInstall.yyyyMMdd.usrlog`) не содержит записей об ошибках.

3. Настройка «СК11.Equipment Inspection Logbook» («СК11.Обходы») и смежных подсистем СК-11 при начальной установке

3.1. В модели *Права доступа* присвоить права для работы с ПО *СК11.Обходы*:

- для пользователей, которым необходимо работать с *ЖВК*, присвоить функции «*Обходы. Работа*» или «*Обходы. Администрирование*» для необходимых ролей;

3.2. На Web-серверах домена СК-11 настроить параметры серверной задачи *Веб-сервис Публичного API* для обеспечения работы СК11.Обходы:

- если на сервере отсутствует конфигурационный файл «opt\CK-11\bin\WS_PublicApiGateway.config.Production.json», то создать его путем копирования файла «opt\CK-11\bin\WS_PublicApiGateway.config.json» и последующего переименования полученной копии. Если файл присутствует, то сопоставить его с файлом «WS_PublicApiGateway.config.json» и добавить отсутствующие строки;
- в полученный конфигурационный файл добавить текст, выделенный зеленым:

JSON	WS_PublicApiGateway.config.Production.json

```
...
    "ObjectModels": {
      "Models": {
        // ENERGY_MAIN_MODEL
        "2000001C-0000-0000-C000-0000006D746C": true,
        // SCADA_MODEL
        "20000f1d-0000-0000-c000-0000006d746c": true,
        // ACCESS_MODEL
        "20001CBC-0000-0000-C000-0000006D746C": true
      },

      "Scripting": {
...
```

- с помощью приложения *Управление узлами СК* **поочередно** перезапустить все экземпляры серверной задачи *Веб-сервис Публичного API*.

Веб-интерфейс *СК11.Обходы* доступен по URL https://WEB_EP_FQDN/equipmentinspections/ , где `WEB_EP_FQDN` – полное имя точки подключения WEB_EP.