



---

## Инструкция по установке СК-11 11.6.6

версия: 11.6.6

дата печати: Сентябрь, 2022

## **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 используемой системы. Для получения актуальной версии вы можете обратиться по адресам, указанным на сайте [www.monitel.ru](http://www.monitel.ru).

Данный документ содержит информацию, которая является конфиденциальной и принадлежит Монитор Электрик. Все права защищены. Не допускается копирование, передача, распространение и иное разглашение содержания данного документа, а также, любых выдержек из него третьим лицам без письменного разрешения Монитор Электрик. Нарушители несут ответственность за ущерб в соответствии с законом.

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 незначительное 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.



|  |           |
|--|-----------|
| <b>1. Установка на платформе Linux .....</b>                           | <b>7</b>  |
| <b>1.1. Подготовка к установке.....</b>                                | <b>9</b>  |
| 1.1.1. Создание DNS-записей .....                                      | 10        |
| 1.1.2. Подготовка SSL-сертификата для Apache.....                      | 11        |
| 1.1.3. Подготовка keytab-файлов для аутентификации через Kerberos..... | 13        |
| 1.1.4. Установка ОС Astra Linux SE 1.6 на серверные узлы.....          | 18        |
| 1.1.5. Установка ОС Astra Linux SE 1.7 на серверные узлы.....          | 37        |
| 1.1.6. Первичная настройка ОС Astra Linux .....                        | 56        |
| <b>1.2. Подготовка сервера технического обслуживания.....</b>          | <b>57</b> |
| 1.2.1. Подключение к серверу технического обслуживания .....           | 58        |
| 1.2.2. Создание репозитория из дисков Astra Linux.....                 | 58        |
| 1.2.3. Копирование и подготовка инсталлятора .....                     | 60        |
| <b>1.3. Настройка инвентаря Ansible .....</b>                          | <b>62</b> |
| 1.3.1. Шесть серверных узлов .....                                     | 62        |
| 1.3.1.1. Настройка конфигурации серверных узлов.....                   | 62        |
| 1.3.1.2. Настройка параметров установки.....                           | 68        |
| 1.3.2. Три серверных узла.....   | 71        |
| 1.3.2.1. Настройка конфигурации серверных узлов.....                   | 71        |
| 1.3.2.2. Настройка параметров установки.....                           | 75        |
| 1.3.3. Один серверный узел .....                                       | 78        |
| 1.3.3.1. Настройка конфигурации серверного узла.....                   | 78        |
| 1.3.3.2. Настройка параметров установки.....                           | 82        |
| 1.3.4. Монтирование хранилища для резервных копий БД.....              | 85        |

|  |    |
|--|----|
| 1.4. Установка программного обеспечения СК-11..... | 85 |
| 1.5. Настройка Справочной системы .....            | 86 |

# 1. Установка 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*:

- **Шесть серверных узлов;**

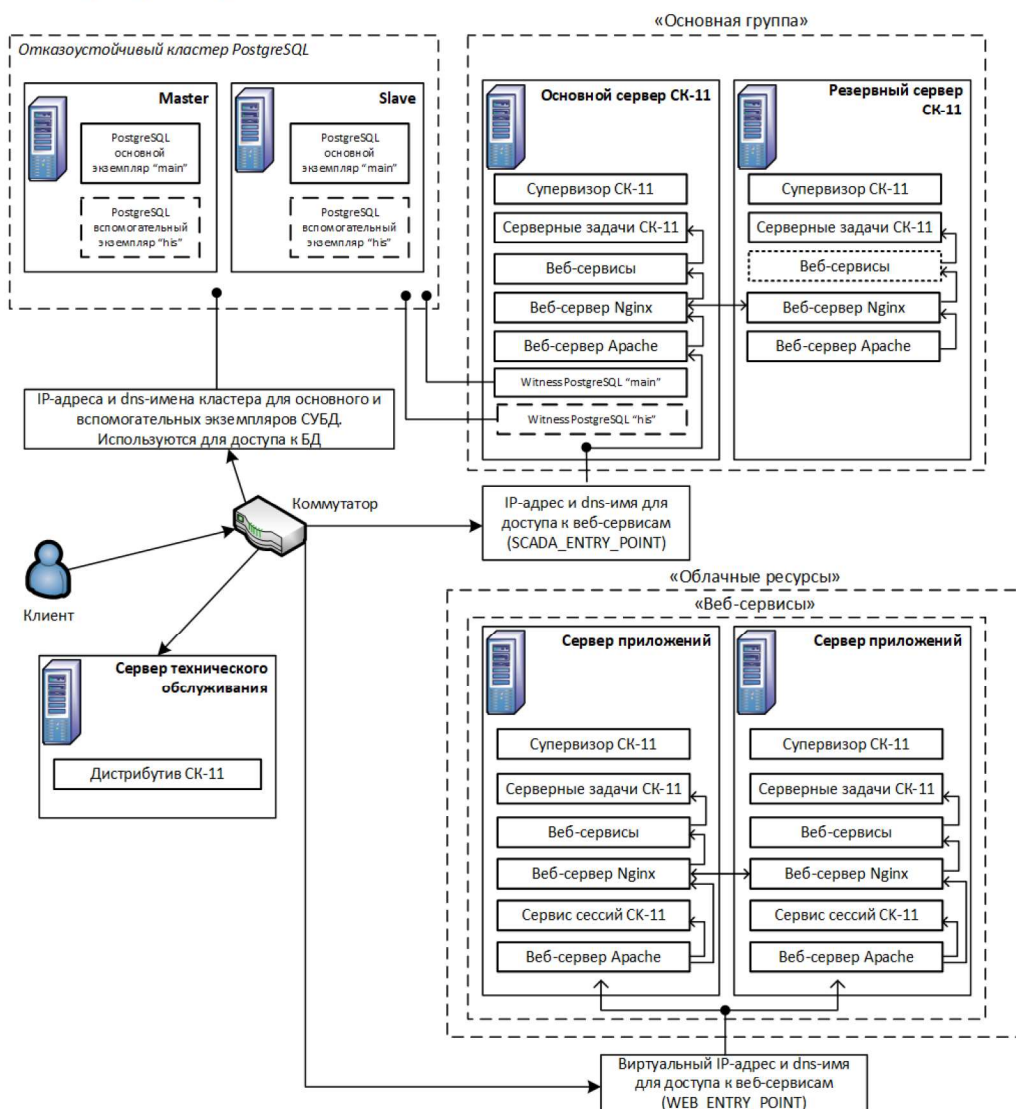


Рис. 1. Схема развёртывания домена СК-11 на шести узлах



- Три серверных узла;

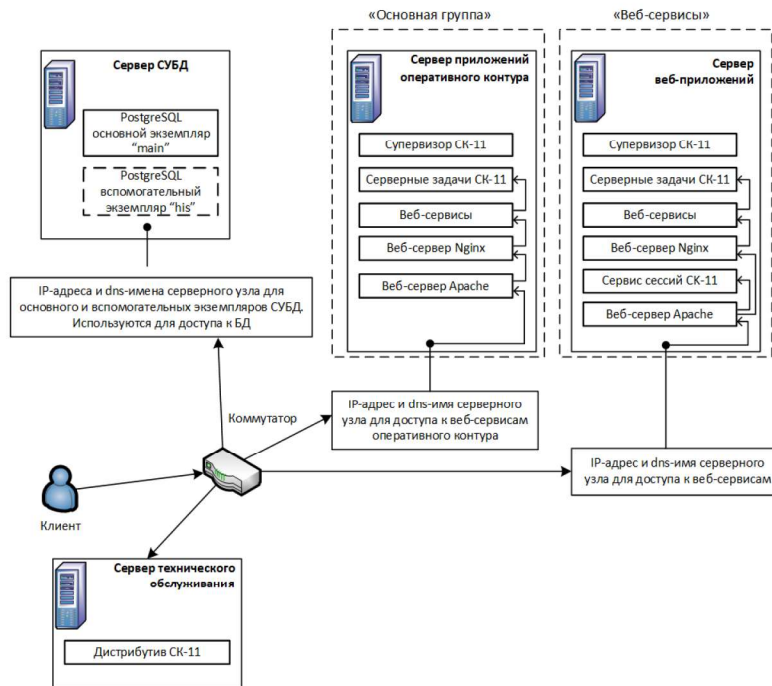


Рис. 2. Схема развёртывания домена СК-11 на трёх узлах

- 
- Один серверный узел.

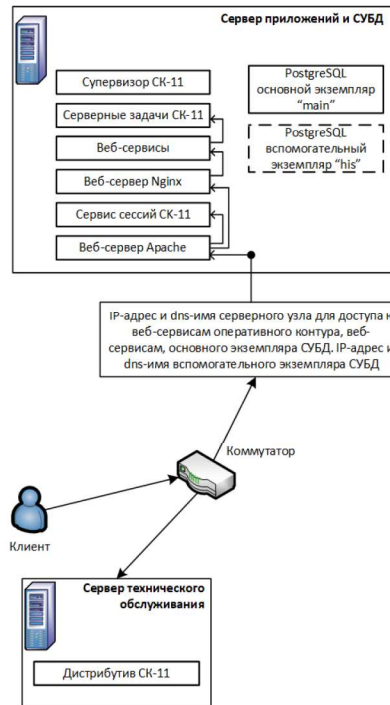


Рис. 3. Схема развёртывания домена СК-11 на одном узле

Установка выполняется в несколько последовательных этапов:

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

## 1.1. Подготовка к установке

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

- создание DNS-записей для имён серверов и точек подключения (entry point) WEB\_EP и SCADA\_EP, а также имени кластера *PostgreSQL*. Точки подключения необходимы для взаимодействия с доменом СК-11 в конфигурации с шестью узлами:
  - точка доступа WEB\_EP позволяет переадресовывать запросы к веб-сервисам СК-11, отказоустойчивость которых реализуется использованием *HAProxy*;
  - точка доступа SCADA\_EP позволяет переадресовывать запросы к веб-сервисам СК-11, работающим на основном сервере (master) Основной группы домена СК-11. 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;
- подготовка сертификата 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.
- установка и первичная настройка ОС на серверных узлах домена СК-11.

При планировании установки Системы необходимо определить целевую архитектуру и количество применяемых серверов.

Для установки необходимы следующие данные, запрашиваемые у системных администраторов организации:

- имена и адреса контроллеров домена Службы каталогов (dc);
- имена и адреса серверов точного времени (ntp).

В дочерних разделах подробно рассмотрены указанные выше работы:

- [Создание DNS-записей.](#)

- [Подготовка SSL-сертификата для Apache.](#)
- [Подготовка keytab-файлов для аутентификации через Kerberos.](#)
- Установка ОС [Astra Linux SE 1.6](#) или [Astra Linux SE 1.7](#) на серверные узлы, в зависимости от приобретённой версии ОС.
- [Первичная настройка ОС Astra Linux.](#)



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

### 1.1.1. Создание DNS-записей

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



Необходимость вспомогательного экземпляра "his" кластера *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-1st* для экземпляра *PostgreSQL* "his" не требуется.

1. Создать DNS-записи серверов приложений СК-11, серверов *PostgreSQL* и сервера технического обслуживания. Рекомендуемые форматы имён серверов соответственно::
  1. \*-scada1 – конфигурация с тремя и шестью серверными узлами;
  2. \*-scada2 – конфигурация с шестью серверными узлами;
  3. \*-web1 – конфигурация с тремя и шестью серверными узлами;
  4. \*-web2 – конфигурация с шестью серверными узлами;
  5. \*-pg1 – все конфигурации;
  6. \*-pg2 – конфигурация с шестью серверными узлами;
  7. \*-pg-his-01 – все конфигурации;
  8. \*-pg-his-02 – конфигурация с шестью серверными узлами;
  9. \*-deployer – все конфигурации.
2. Создать статическую (static) DNS-запись для точки подключения WEB\_ENTRY\_POINT 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.
3. Создать статическую (static) DNS-запись для точки подключения SCADA\_ENTRY\_POINT 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.



4. Создать статическую (static) DNS-запись для имени прослушвателя основного экземпляра (main) кластера *PostgreSQL* 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-1st.
5. Создать статическую (static) DNS-запись для имени прослушвателя экземпляра "his" кластера *PostgreSQL* 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-1st.
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, 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-сертификата для Apache

Для обеспечения работоспособности веб-сервисов и служб СК-11 по протоколу HTTPS необходим SSL сертификат, выпущенный доверенным *Удостоверяющим центром (Certification authority)*. Требования к сертификату различаются в зависимости от целевой конфигурации развёртывания домена СК-11:

#### ▲ Шесть серверных узлов

SSL-сертификат должен быть разделён на два файла:

- [WEB\_EP\_FQDN].private\_key.pem – содержит только личный ключ (private key);
- [WEB\_EP\_FQDN].pem – содержит сертификат и личный ключ, включая атрибуты.

В именах файлов [WEB\_EP\_FQDN] следует заменить на полное [имя \(FQDN\) точки подключения WEB\\_EP](#);

- поле Subject должно содержать атрибут Common Name (CN) со значением, соответствующим полному сетевому имени (FQDN) точки подключения WEB\_EP;
- поле Subject Alternative Name (SAN) должно содержать все краткие и полные DNS-имена серверов \*-scada1, \*-scada2, \*-web1, \*-web2 и объединяющих их кластеров точек подключения WEB\_EP, SCADA\_EP.

#### ▲ Три серверных узла

SSL-сертификат должен быть разделён на два файла:

- [\*-web1].private\_key.pem – содержит только личный ключ (private key);
- [\*-web1].pem – содержит сертификат и личный ключ, включая атрибуты.

В именах файлов [\*-web1] следует заменить на полное имя (FQDN) серверного узла для веб-приложений Системы;

- 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 \*-scada1, \*-web1.

#### ▲ Один серверный узел

SSL-сертификат должен быть разделён на два файла:

- [\*-pg1].private\_key.pem – содержит только личный ключ (private key);
- [\*-pg1].pem – содержит сертификат и личный ключ, включая атрибуты.

В именах файлов [\*-pg1] следует заменить на полное имя (FQDN) серверного узла приложений и СУБД Системы;

- 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 все краткое и полное DNS-имя сервера \*-pg1.

#### **Общие требования к файлам сертификата**

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

К файлам SSL-сертификата должен прилагаться файл корневого сертификата домена Службы каталогов root.##domain.local##.crt, где ##domain.local## – полное имя домена Службы каталогов.

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 целевой конфигурации развёртывания домена СК-11:

Условные обозначения:

- `host-pg-01.domain.local` – полное имя первого узла основного (main) экземпляра кластера *PostgreSQL*. Для конфигурации с одним узлом имя используется для узла сервера приложений и СУБД;
- `host-pg-02.domain.local` – полное имя второго узла основного (main) экземпляра кластера *PostgreSQL*;
- `host-pg-1st.domain.local` – полное имя прослушивателя основного (main) экземпляра кластера *PostgreSQL*;
- `host-pg-his-01.domain.local` – полное имя первого узла экземпляра "his" кластера *PostgreSQL*. Для конфигурации с одним или тремя узлами используется для виртуального имени экземпляра "his" *PostgreSQL*;
- `host-pg-his-02.domain.local` – полное имя первого узла экземпляра "his" кластера *PostgreSQL*;
- `host-pg-his-1st.domain.local` – полное имя прослушивателя экземпляра "his" кластера *PostgreSQL*;
- `host-web1.domain.local` – полное имя узла веб-приложений для конфигурации с тремя узлами;
- `web_ep.domain.local` – полное имя точки подключения [WEB EP](#) к службам СК-11;
- `scada_ep.domain.local` – полное имя точки подключения [SCADA EP](#) к службам СК-11.



Необходимость вспомогательного экземпляра "his" кластера *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 домена MS AD создать отдельные учётные записи пользователя для использования службами *postgres* и *http*, например:



```
domain.local\httpservice
domain.local\postgresservice
```

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

```
HTTP/web_ep.domain.local
HTTP/scada_ep.domain.local
postgres/host-pg-1st.domain.local, postgres/host-pg-01.domain.local,
postgres/host-pg-02.domain.local
postgres/host-pg-his-1st.domain.local, postgres/host-pg-his-
01.domain.local, postgres/host-pg-his-02.domain.local
```

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

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

```
apache2.web_ep.domain.local.keytab
apache2.scada_ep.domain.local.keytab
postgres.host-pg-1st.domain.local.keytab
postgres.host-pg-his-1st.domain.local.keytab
```

|             |                                    |               |
|-------------|------------------------------------|---------------|
| Keytab-файл | apache2.web_ep.domain.local.keytab | соответствует |
| принципалу  | HTTP/web_ep.domain.local           | и             |
|             | domain.local\httpservice           | пользователю  |

|             |                                      |               |
|-------------|--------------------------------------|---------------|
| Keytab-файл | apache2.scada_ep.domain.local.keytab | соответствует |
| принципалу  | HTTP/scada_ep.domain.local           | и             |
|             | domain.local\httpservice             | пользователю  |

|             |                             |  |                           |   |   |              |
|-------------|-----------------------------|--|---------------------------|---|---|--------------|
| Keytab-файл | (multiple principal keytab) | postgres.host-pg-1st.domain.local.keytab | соответствует принципалам | postgres/host-pg-1st.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-1st.domain.local.keytab | соответствует принципалам | postgres/host-pg-his-1st.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:

```
web_ep.domain.local
scada_ep.domain.local
host-pg-1st.domain.local
host-pg-01.domain.local
host-pg-02.domain.local
host-pg-his-1st.domain.local
host-pg-his-01.domain.local
host-pg-his-02.domain.local
```

2. Далее создаются учётные записи служб:

```
HTTP/web_ep.domain.local
HTTP/scada_ep.domain.local
postgres/host-pg-1st.domain.local
postgres/host-pg-01.domain.local
postgres/host-pg-02.domain.local
postgres/host-pg-his-1st.domain.local
postgres/host-pg-his-01.domain.local
postgres/host-pg-his-02.domain.local
```

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

```
apache2.web_ep.domain.local.keytab, соответствующий принципу
HTTP/web_ep.domain.local

apache2.scada_ep.domain.local.keytab, соответствующий принципу
HTTP/scada_ep.domain.local

postgres.host-pg-1st.domain.local.keytab, (multiple principal keytab)
соответствующий принципалам postgres/host-pg-1st.domain.local,
postgres/host-pg-01.domain.local, postgres/host-pg-02.domain.local

postgres.host-pg-his-1st.domain.local.keytab, (multiple principal keytab)
соответствующий принципалам postgres/host-pg-his-1st.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*, например:

```
domain.local\httpservice
```

```
domain.local\postgresservice
```

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

```
HTTP/host-web1.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:

```
apache2.host-web1.domain.local.keytab
```

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

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

Keytab-файл `apache2.host-web1.domain.local.local.keytab` соответствует принципалу `HTTP/host-web1.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-web1.domain.local
```

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

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

2. Далее создаются учётные записи служб:

```
HTTP/host-web1.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:



apache2.host-web1.domain.local.keytab, соответствующий принципалу  
HTTP/host-web1.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*, например:

domain.local\httpservice

domain.local\postgresservice

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

HTTP/host-pg-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:

apache2.host-pg-01.domain.local.keytab

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

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

Keytab-файл apache2.host-pg-01.domain.local.local.keytab  
соответствует принципалу HTTP/host-pg-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-pg-01.domain.local`

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

2. Далее создаются учётные записи служб:

`HTTP/host-pg-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:

`apache2.host-pg-01.domain.local.keytab`, соответствующий принципу  
`HTTP/host-pg-01.domain.local`

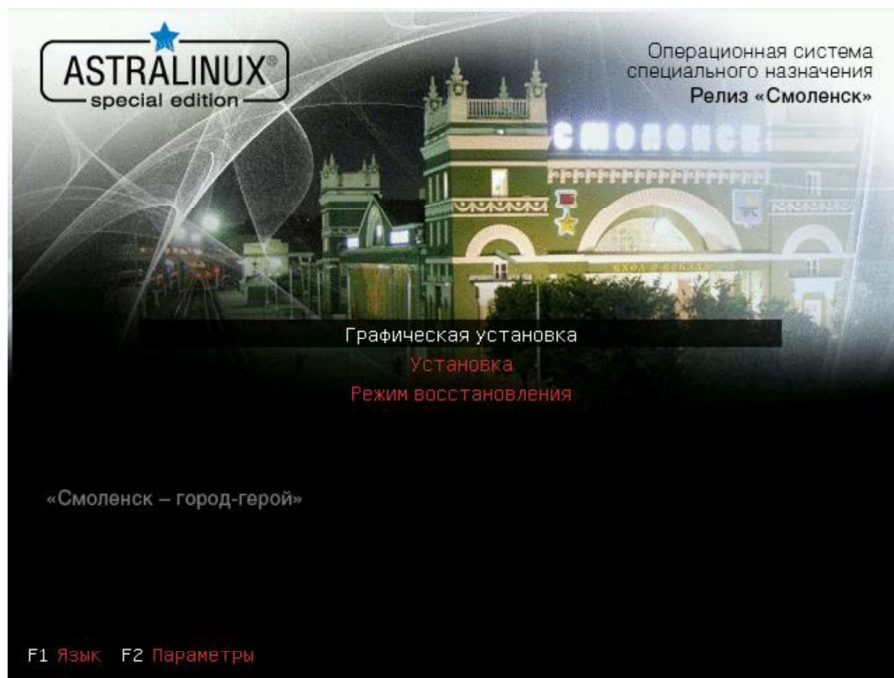
`postgres.host-pg-01.domain.local.keytab`, соответствующий принципу  
`postgres/host-pg-01.domain.local`

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

#### 1.1.4. Установка ОС Astra Linux SE 1.6 на серверные узлы

При установке ОС "*Astra Linux Special Edition*" РУСБ.10015-01 (очередное обновление 1.6, релиз Смоленск) 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](#).

**Лицензия**

4.1. Настоящее СОГЛАШЕНИЕ вступает в силу с момента установки или копирования ПРОГРАММНОГО ПРОДУКТА.

4.2. По инициативе ПРАВООБЛАДАТЕЛЯ СОГЛАШЕНИЕ может быть расторгнуто в случае нарушения ПОЛЬЗОВАТЕЛЕМ условий настоящего СОГЛАШЕНИЯ.

**5. ПРАВА НА ИНТЕЛЛЕКТУАЛЬНУЮ СОБСТВЕННОСТЬ**

5.1. Правовой титул и все права интеллектуальной собственности на ПРОГРАММНЫЙ ПРОДУКТ, включая (но не ограничиваясь только этим) любые входящие в его состав элементы мультимедиа, текст и программы, а также содержание сопровождающих его печатных материалов и любые копии ПРОГРАММНОГО ПРОДУКТА принадлежат ПРАВООБЛАДАТЕЛЮ, за исключением случаев, указанных в 5.2 настоящего СОГЛАШЕНИЯ.

5.2. Правовой титул и все права на объекты интеллектуальной собственности, которые не являются разработкой ПРАВООБЛАДАТЕЛЯ, но входят в состав ПРОГРАММНОГО ПРОДУКТА, включая (но не ограничиваясь только этим) любые входящие в его состав элементы мультимедиа, текст и программы, и доступ к которым предоставляет ПРОГРАММНЫЙ ПРОДУКТ, принадлежат владельцам прав на такие элементы и защищены международными соглашениями и законодательством Российской Федерации о защите интеллектуальной собственности. Настоящее СОГЛАШЕНИЕ не предоставляет ПОЛЬЗОВАТЕЛЮ никаких прав на использование такого содержания ПРОГРАММНОГО ПРОДУКТА. Права на такое содержание ПРОГРАММНОГО ПРОДУКТА, в т.ч. (но не ограничиваясь только этим) право на получение его исходного кода по отдельному запросу, определяются отдельными лицензионными соглашениями правообладателей данных объектов интеллектуальной собственности.

5.3. За нарушение авторских прав ПРАВООБЛАДАТЕЛЯ на ПРОГРАММНЫЙ ПРОДУКТ ПОЛЬЗОВАТЕЛЬ несет гражданскую, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

**6. ГАРАНТИИ**

6.1. ПРАВООБЛАДАТЕЛЬ гарантирует, что:

6.1.1. ПРОГРАММНЫЙ ПРОДУКТ содержится в полном объеме, соответствующем описанию, представленному в печатных материалах или электронной документации, которые входят в состав ПРОГРАММНОГО ПРОДУКТА.

6.1.2. Функции, которые выполняет ПРОГРАММНЫЙ ПРОДУКТ, соответствуют функциям, указанным в печатных и электронных материалах и (или) документации к ПРОГРАММНОМУ ПРОДУКТУ, либо превосходят их.

6.2. Настоящая гарантия недействительна, если сбой в работе ПРОГРАММНОГО ПРОДУКТА возник в результате неосторожности, неправильного обращения или применения, а также в случаях, перечисленных в 3.4 настоящего СОГЛАШЕНИЯ.

**7. ПРИМЕНИМОЕ ЗАКОНОДАТЕЛЬСТВО**

7.1. При использовании ПРОГРАММНОГО ПРОДУКТА применяются международные соглашения Российской Федерации и действующее законодательство Российской Федерации, регулирующее отношения в области интеллектуальной собственности.

Принимаете ли Вы условия настоящей лицензии?

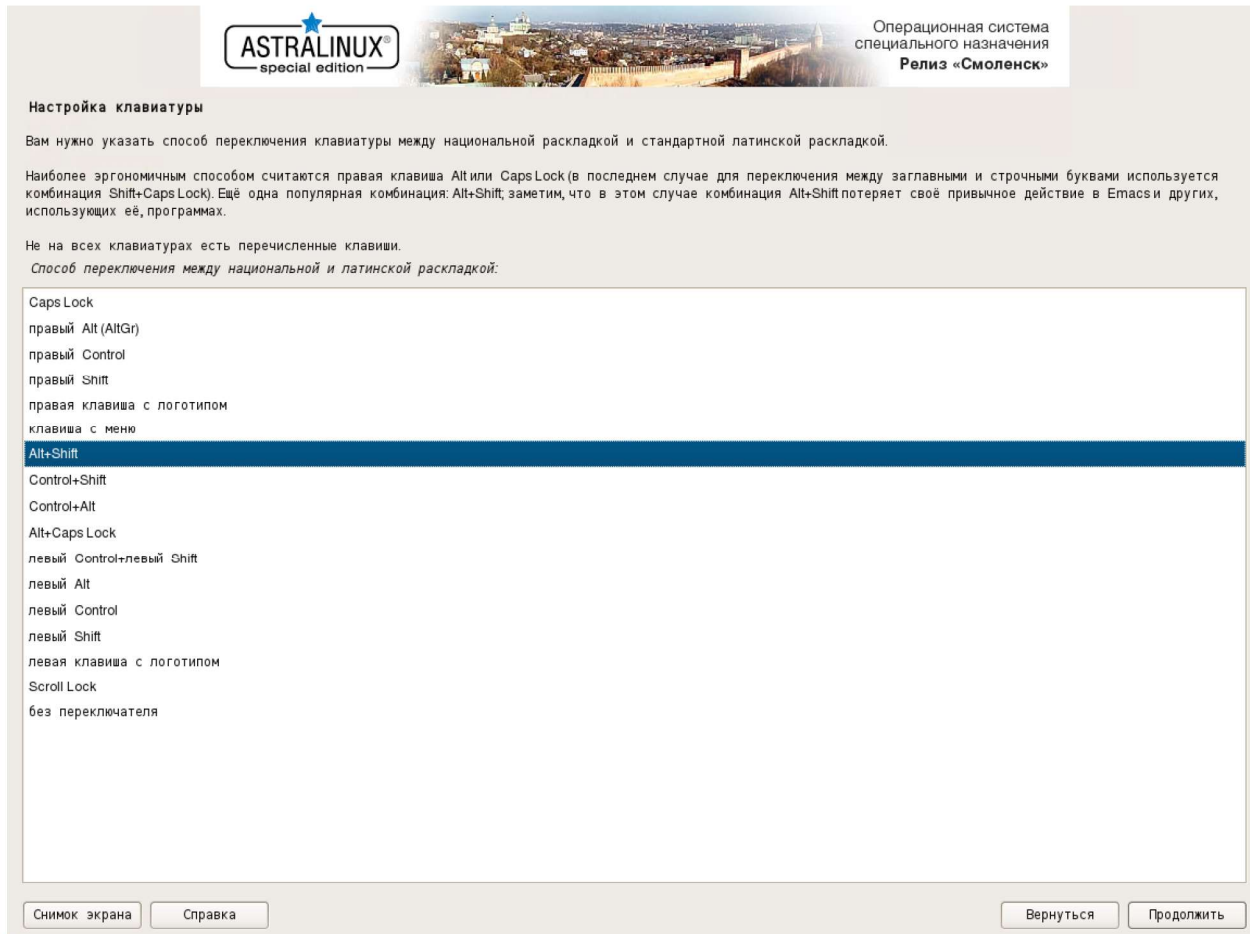
Нет

Да

Снимок экрана    Справка    [Продолжить](#)



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



**ASTRALINUX®**  
special edition

Операционная система  
специального назначения  
**Релиз «Смоленск»**

### Настройка клавиатуры

Вам нужно указать способ переключения клавиатуры между национальной раскладкой и стандартной латинской раскладкой.

Наиболее эргономичным способом считаются правая клавиша Alt или CapsLock (в последнем случае для переключения между заглавными и строчными буквами используется комбинация Shift+CapsLock). Ещё одна популярная комбинация: Alt+Shift, заметим, что в этом случае комбинация Alt+Shift потеряет своё привычное действие в Emacs и других, использующих её, программах.

Не на всех клавиатурах есть перечисленные клавиши.  
*Способ переключения между национальной и латинской раскладкой:*

- Caps Lock
- правый Alt (AltGr)
- правый Control
- правый Shift
- правая клавиша с логотипом
- клавиша с меню
- Alt+Shift**
- Control+Shift
- Control+Alt
- Alt+Caps Lock
- левый Control+левый Shift
- левый Alt
- левый Control
- левый Shift
- левая клавиша с логотипом
- Scroll Lock
- без переключателя

Снимок экрана    Справка    Вернуться    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**.



#### Настройка сети

Введите имя этого компьютера.

Имя компьютера – это одно слово, которое идентифицирует вашу систему в сети. Если вы не знаете каким должно быть имя вашей системы, то посоветуйтесь с администратором вашей сети. Если вы устанавливаете вашу собственную домашнюю сеть, можете выбрать любое имя.

Имя компьютера:

Снимок экрана

Справка

Вернуться

Продолжить

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



#### Настройка учётных записей пользователей и паролей

Выберите имя учётной записи администратора. Учётная запись должна начинаться со строчной латинской буквы, за которой может следовать любое количество строчных латинских букв или цифр.

Имя учётной записи администратора:

Снимок экрана

Справка

Вернуться

Продолжить

7. Дважды ввести пароль для администратора серверного узла. Нажать на кнопку **Продолжить**.





#### Настройка учётных записей пользователей и паролей

Хороший пароль представляет из себя смесь букв, цифр и знаков препинания, и должен периодически меняться.

Введите пароль для нового администратора:

●●●●●●●●

Проверка правильности ввода осуществляется путём повторного ввода пароля и сравнения результатов.

Введите пароль ещё раз:

●●●●●●●●

Снимок экрана

Справка

Вернуться

Продолжить

8. Выбрать необходимый часовой пояс, в котором будет работать система. Нажать на кнопку **Продолжить**.



#### Настройка времени

Если нужного часового пояса нет в списке, то вернитесь к шагу "Выбор языка" и выберите страну, в которой используется требуемый часовой пояс (страну, в которой вы живёте или сейчас находитесь).

Выберите часовой пояс:

Москва-01 - Калининград  
**Москва+00 - Москва**  
 Москва+01 - Самара  
 Москва+02 - Екатеринбург  
 Москва+03 - Омск  
 Москва+04 - Красноярск  
 Москва+05 - Иркутск  
 Москва+06 - Якутск  
 Москва+07 - Владивосток  
 Москва+08 - Магадан  
 Москва+09 - Камчатка

Снимок экрана

Справка

Вернуться

Продолжить

- Выбрать режим разметки разделов диска "Авто – использовать весь диск и настроить LVM". Нажать на кнопку [Продолжить](#).



**Разметка дисков**

Программа установки может провести вас через процесс разметки диска (предлагая разные стандартные схемы) на разделы, либо это можно сделать вручную. Если выбрать использование инструмента управления разметкой, у вас всё равно будет возможность позже посмотреть и подправить результат.

Если выбрать использование инструмента управления разметкой всего диска, то далее вас попросят указать нужный диск.

*Метод разметки:*

Авто - использовать весь диск

**Авто - использовать весь диск и настроить LVM**

Авто - использовать весь диск с защитным преобразованием на LVM

Вручную

Снимок экрана    Справка

Вернуться    Продолжить

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





#### Разметка дисков

Заметим, что все данные на выбранном диске будут стёрты, но не ранее чем вы подтвердите, что действительно хотите сделать изменения.

Выберите диск для разметки:

SCSI3 (0,0,0) (sda) - 136.4 GB Msft Virtual Disk

Снимок экрана

Справка

Вернуться

Продолжить

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



**Разметка дисков**

Выбрано для разметки:

SCSI3 (0,0,0) (sda) - Msft Virtual Disk: 136.4 GB

Диск может быть размечен по одной из следующих схем. Если вы не знаете, что выбрать -- выберите первую схему.

Схема разметки:

Все файлы в одном разделе (рекомендуется новичкам)

Отдельный раздел для /home

Снимок экрана

Справка

Вернуться

Продолжить

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



#### Разметка дисков

Перед настройкой логических томов нужно записать информацию о разделах на диск. Эти изменения будет невозможно отменить.

После настройки с помощью менеджера логических томов больше нельзя изменять разметку дисков, содержащих физические тома. Прежде чем продолжить настройку, убедитесь, что вы удовлетворены текущей разметкой дисков.

На этих устройствах изменены таблицы разделов:  
SCSI3 (0,0,0) (sda)

Записать изменения на диск и настроить LVM?

Нет

Да

Снимок экрана

Справка

Продолжить

13. Выбрать пункт "Закончить разметку и записать изменения на диск". Нажать на кнопку **Продолжить**.



#### Разметка дисков

Перед вами список настроенных разделов и их точек монтирования. Выберите раздел, чтобы изменить его настройки (тип файловой системы, точку монтирования и так далее), свободное место, чтобы создать новый раздел, или устройство, чтобы создать на нём новую таблицу разделов.

Автоматическая разметка  
 Настройка программного RAID  
 Настройка менеджера логических томов (LVM)  
 Настроить защитное преобразование для томов  
 Настроить тома iSCSI

▾ LVM VG astra-vg, LV root - 131.8 GB Linux device-mapper (linear)
 

- > #1 131.8 GB f ext4 /

▾ LVM VG astra-vg, LV swap\_1 - 4.3 GB Linux device-mapper (linear)
 

- > #1 4.3 GB f подк подк

▾ SCSI3 (0,0,0) (sda) - 136.4 GB Msft Virtual Disk
 

- > #1 первичн. 254.8 MB B f ext2 /boot
- > #5 логичес. 136.1 GB K lvm

Отменить изменения разделов

Закончить разметку и записать изменения на диск

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





**Разметка дисков**

Если вы продолжите, то изменения, перечисленные ниже, будут записаны на диски. Или же вы можете сделать все изменения вручную.

На этих устройствах изменены таблицы разделов:

LVM VG astra-vg, LV root  
LVM VG astra-vg, LV swap\_1  
SCSI3 (0,0,0) (sda)

Следующие разделы будут отформатированы:

LVM VG astra-vg, LV root как ext4  
LVM VG astra-vg, LV swap\_1 как подк  
раздел #1 на устройстве SCSI3 (0,0,0) (sda) как ext2

Записать изменения на диск?

Нет

Да

Снимок экрана

Справка

Продолжить

15. На шаге "Выбор программного обеспечения" выбрать пункты "Базовые средства", "Средства удалённого доступа SSH". Нажать на кнопку **Продолжить**.



#### Выбор программного обеспечения

В данный момент установлена только основа системы. Исходя из ваших потребностей, можете выбрать один и более из готовых наборов программного обеспечения.  
 Выберите устанавливаемое программное обеспечение:

- Базовые средства
- Рабочий стол Fly
- Приложения для работы с сенсорным экраном
- Средства работы в сети
- Офисные средства
- СУБД
- Средства удаленного доступа SSH
- Защищенный WEB сервер
- Средства Виртуализации
- Средства Мультимедиа

16. На шаге "Выбор установка программного обеспечения" ничего выбирать не требуется.  
 Нажать на кнопку [Продолжить](#).



Выбор и установка программного обеспечения

Выберите дополнительные функции устанавливаемой ОС.

Служба ALD

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



#### Дополнительные настройки ОС

Вы можете настроить параметры безопасности ОС и отключить автоматическую настройку сети. Мандатный контроль целостности процессов ОС по умолчанию включен и после настройки ОС администратором необходимо включить мандатный контроль целостности ОС и режим ЗПС. Для управления МКЦ могут использоваться программы `lu-admin-smc`, `astra-misc-control`, `set-fs-ilev`, `unset-fs-ilev`.

Дополнительные настройки ОС

|                                     |  |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | Включить режим замкнутой программной среды               |
| <input type="checkbox"/>            | Запретить установку бита исполнения                      |
| <input type="checkbox"/>            | Использовать по умолчанию ядро Hardened                  |
| <input type="checkbox"/>            | Запретить вывод меню загрузчика                          |
| <input type="checkbox"/>            | Включить очистку разделов страничного обмена             |
| <input type="checkbox"/>            | Включить очистку освобождаемых областей для EХТ-разделов |
| <input type="checkbox"/>            | Включить блокировку консоли                              |
| <input type="checkbox"/>            | Включить блокировку интерпретаторов                      |
| <input type="checkbox"/>            | Включить межсетевой экран <code>ufw</code>               |
| <input type="checkbox"/>            | Включить системные ограничения <code>ulimits</code>      |
| <input type="checkbox"/>            | Отключить возможность трассировки <code>ptrace</code>    |
| <input type="checkbox"/>            | Отключить автоматическую настройку сети                  |
| <input type="checkbox"/>            | Установить 32-битный загрузчик                           |

Снимок экрана    Справка

Продолжить

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





**Установка системного загрузчика GRUB на жёсткий диск**

Похоже, что данная система будет единственной на этом компьютере. Если это действительно так, то можно спокойно устанавливать системный загрузчик GRUB в основную загрузочную запись первого жёсткого диска.

Внимание! Если программе установки не удалось обнаружить другую операционную систему, имеющуюся на компьютере, то изменение основной загрузочной записи приведёт к тому, что эту операционную систему некоторое время нельзя будет загрузить. Позднее можно будет настроить GRUB для её загрузки.

*Установить системный загрузчик GRUB в главную загрузочную запись?*

Нет

Да

Снимок экрана

Справка

Вернуться

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](#).



#### Установка системного загрузчика GRUB на жёсткий диск

Системный загрузчик GRUB обладает многими мощными интерактивными свойствами, которые могут быть использованы для несанкционированного доступа к системе, если неизвестный пользователь получит доступ к машине перед загрузкой. Чтобы защититься от этого, вы можете задать пароль, который нужно будет ввести для редактирования меню или для входа в режим командной строки GRUB. По умолчанию, любому пользователю разрешено запускать любой пункт меню без пароля.

Введите пароль для GRUB.

Пароль для GRUB:

Снимок экрана

Справка

Вернуться

Продолжить

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



Операционная система  
специального назначения  
**Релиз «Смоленск»**

**Установка системного загрузчика GRUB на жёсткий диск**

Введите тот же самый пароль для GRUB ещё раз, чтобы убедиться в правильности ввода.

*Введите пароль ещё раз:*

●●●●●●

Снимок экрана

Справка

Вернуться

Продолжить

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



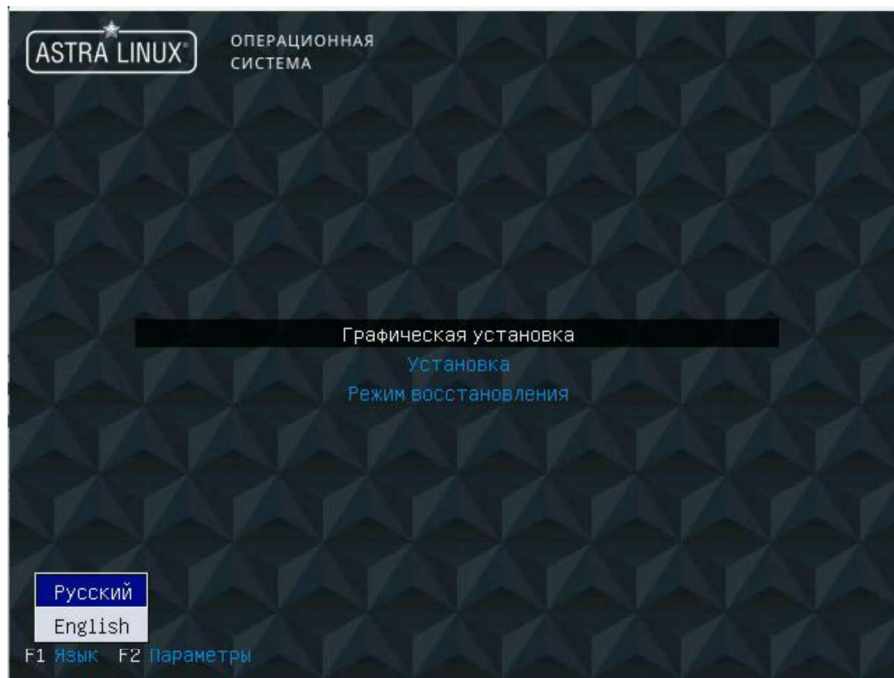
22. После установки нужно изменить порядок загрузки виртуальной машины с cdrom на hdd и оставить установочный диск *Astra Linux* в cdrom.

### 1.1.5. Установка ОС Astra Linux SE 1.7 на серверные узлы

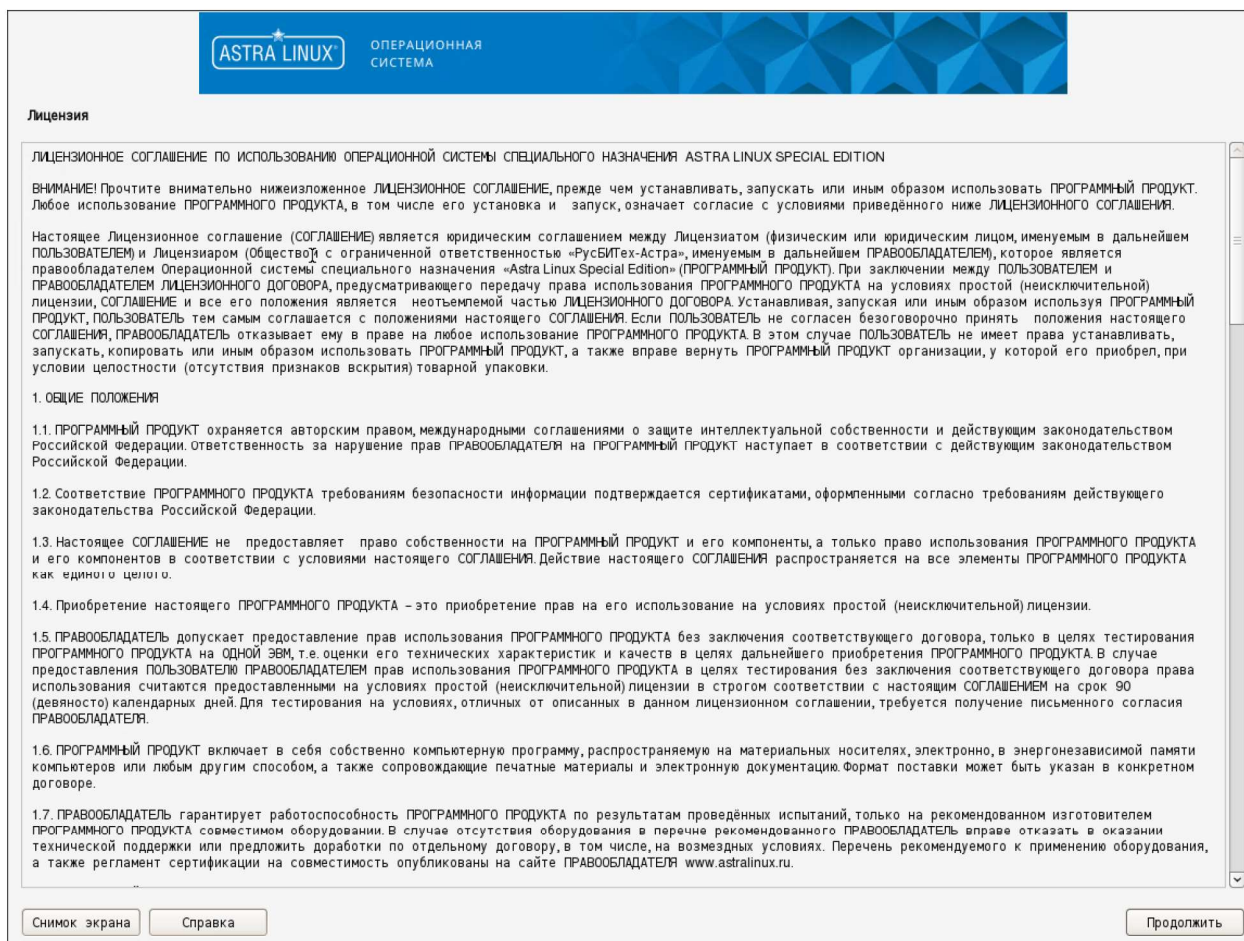
При установке ОС "*Astra Linux Special Edition*" РУСБ.10015-01 (очередное обновление 1.7) на серверные узлы выполняются следующие шаги:

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

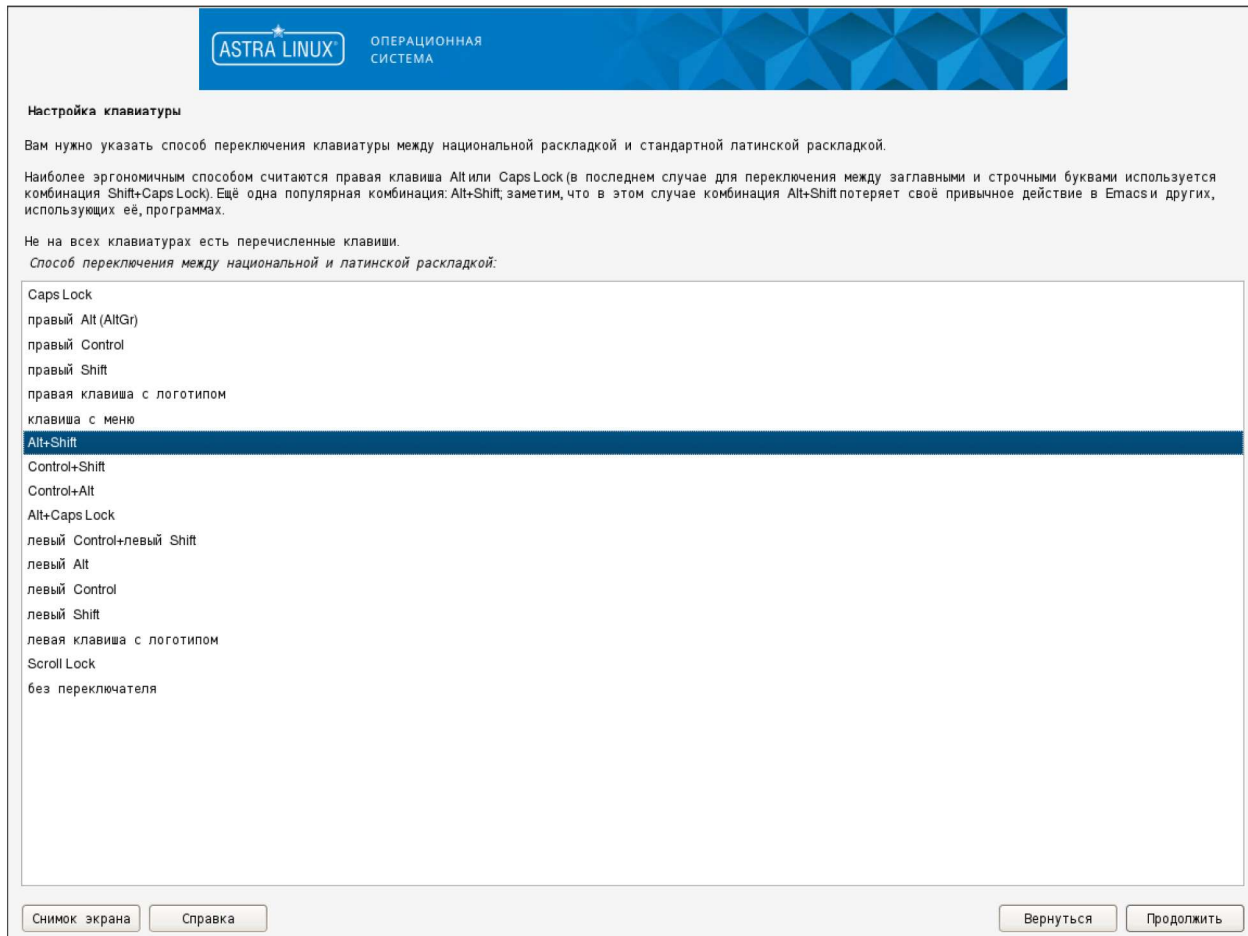




3. Ознакомьтесь с условиями лицензии, установить значение "Да" для пункта "Принимаете ли Вы условия настоящей лицензии?". Нажать на кнопку **Продолжить**.



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**.

**ASTRA LINUX** ОПЕРАЦИОННАЯ СИСТЕМА

### Настройка сети

Введите имя этого компьютера.

Имя компьютера -- это одно слово, которое идентифицирует вашу систему в сети. Если вы не знаете каким должно быть имя вашей системы, то посоветуйтесь с администратором вашей сети. Если вы устанавливаете вашу собственную домашнюю сеть, можете выбрать любое имя.

Имя компьютера:

Снимок экрана Справка Вернуться Продолжить

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

**ASTRA LINUX** ОПЕРАЦИОННАЯ СИСТЕМА

**Настройка учётных записей пользователей и паролей**

Выберите имя учётной записи администратора. Учётная запись должна начинаться со строчной латинской буквы, за которой может следовать любое количество строчных латинских букв или цифр.

*Имя учётной записи администратора:*

Снимок экрана Справка Вернуться Продолжить

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



## Настройка учётных записей пользователей и паролей

Хороший пароль представляет из себя смесь букв, цифр и знаков препинания, и должен периодически меняться.

Введите пароль для нового администратора:

●●●●●●●●

Проверка правильности ввода осуществляется путём повторного ввода пароля и сравнения результатов.

Введите пароль ещё раз:

●●●●●●●●

Снимок экрана

Справка

Вернуться

Продолжить

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

**Настройка времени**

Если нужного часового пояса нет в списке, то вернитесь к шагу "Выбор языка" и выберите страну, в которой используется требуемый часовой пояс (страну, в которой вы живёте или сейчас находитесь).

Выберите часовой пояс:

Москва-01 - Калининград  
Москва+00 - Москва  
Москва+01 - Самара  
Москва+02 - Екатеринбург  
Москва+03 - Омск  
Москва+04 - Красноярск  
Москва+05 - Иркутск  
Москва+06 - Якутск  
Москва+07 - Владивосток  
Москва+08 - Магадан  
Москва+09 - Камчатка

Снимок экрана

Справка

Вернуться

Продолжить

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

**Разметка дисков**

Программа установки может провести вас через процесс разметки диска (предлагая разные стандартные схемы) на разделы, либо это можно сделать вручную. Если выбрать использование инструмента управления разметкой, у вас всё равно будет возможность позже посмотреть и подправить результат.

Если выбрать использование инструмента управления разметкой всего диска, то далее вас попросят указать нужный диск.

*Метод разметки:*

Авто - использовать весь диск

Авто - использовать весь диск и настроить LVM

Авто - использовать весь диск с защитным преобразованием на LVM

Вручную

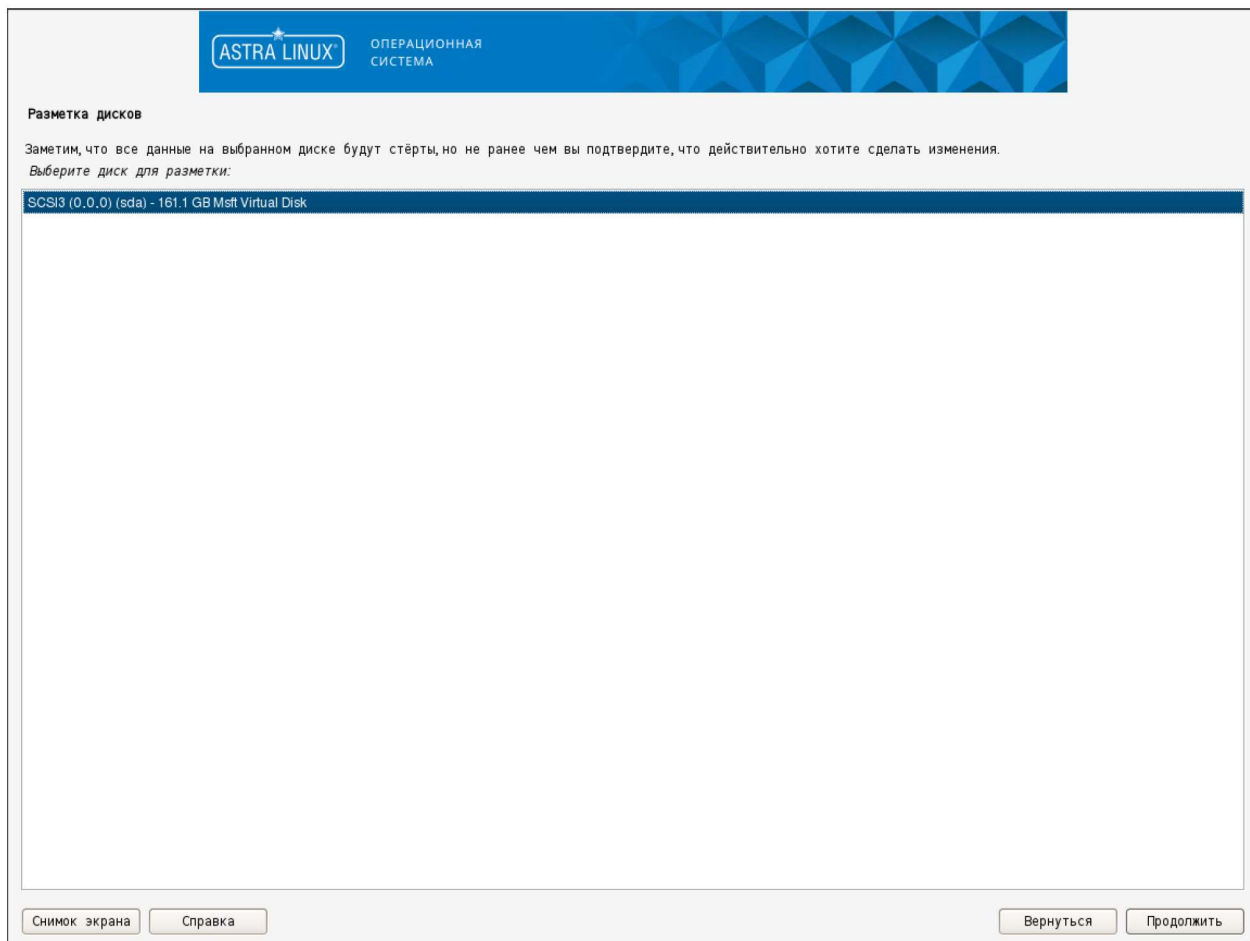
Снимок экрана

Справка

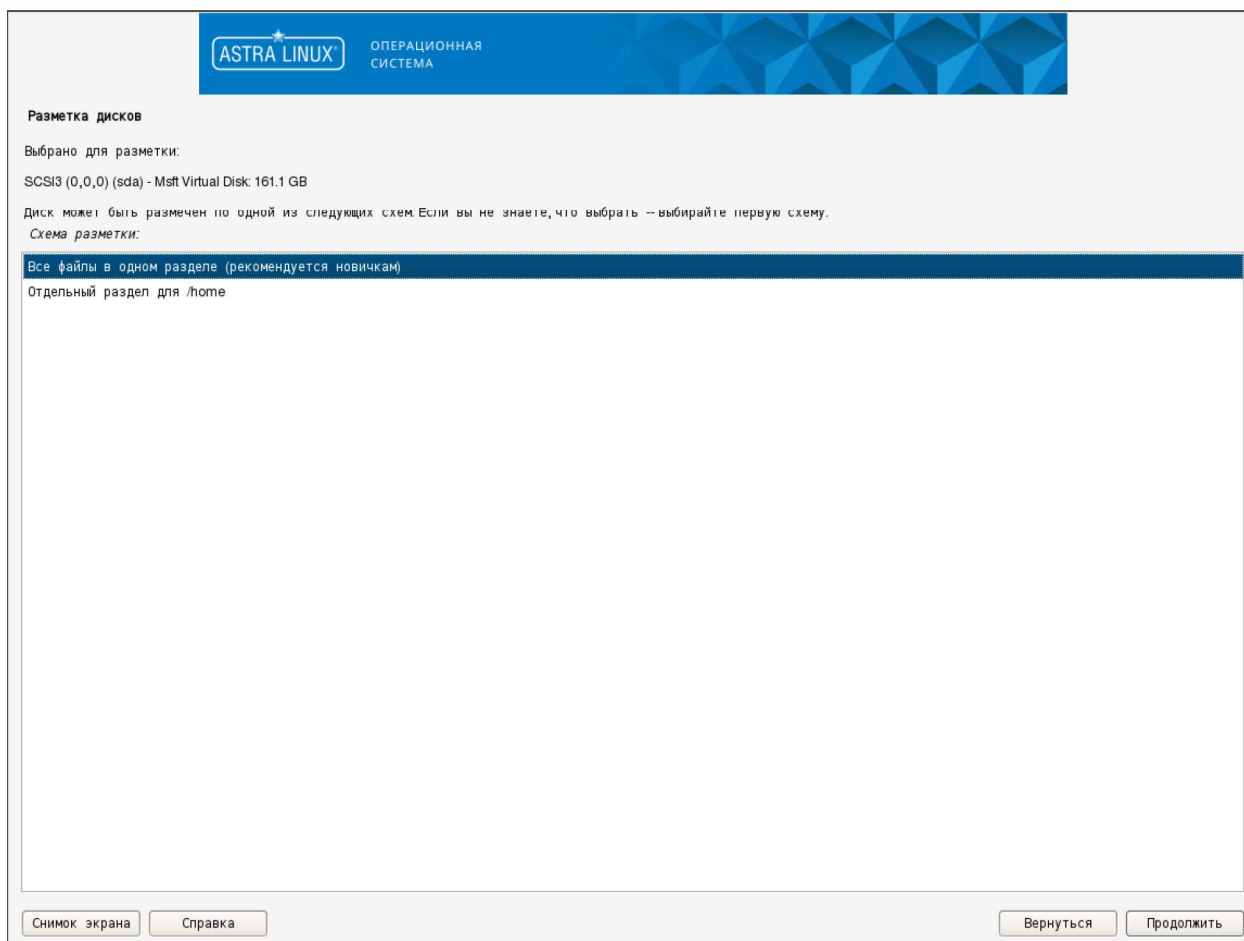
Вернуться

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**.



## Разметка дисков

Перед настройкой логических томов нужно записать информацию о разделах на диск. Эти изменения будет невозможно отменить.

После настройки с помощью менеджера логических томов больше нельзя изменять разметку дисков, содержащих физические тома. Прежде чем продолжить настройку, убедитесь, что вы удовлетворены текущей разметкой дисков.

На этих устройствах изменены таблицы разделов:

SCSI3 (0,0,0) (sda)

Записать изменения на диск и настроить LVM?

Нет

Да

Снимок экрана

Справка

Продолжить

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

## Разметка дисков

Для установки можно использовать как всю группу томов, так и часть её. При использовании части, либо если вы добавите другие диски после разбивки, позднее вы сможете увеличить размер логических дисков, используя утилиты LVM, а значит, использование малой части группы томов во время установки может быть более гибким решением.

Минимальный размер для выбранного способа установки — 11.0 GB (или 6%); однако учтите, что установка выбранных вами пакетов может потребовать большего места. Максимально доступный размер — 160.5 GB.

На заметку: чтобы задать максимальный размер можно ввести "max", а также можно задавать процентное значение (например, "20%"), которое считается от максимального размера.

Размер группы томов, используемый для установки:

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

## Разметка дисков

Если вы продолжите, то изменения, перечисленные ниже, будут записаны на диски. Или же вы можете сделать все изменения вручную.

На этих устройствах изменены таблицы разделов:

LVM VG astra-linux-1-7-vg, LV root  
LVM VG astra-linux-1-7-vg, LV swap\_1  
SCSI3 (0,0,0) (sda)

Следующие разделы будут отформатированы:

LVM VG astra-linux-1-7-vg, LV root как ext4  
LVM VG astra-linux-1-7-vg, LV swap\_1 как подк  
раздел #1 на устройстве SCSI3 (0,0,0) (sda) как ext2

Записать изменения на диск?

Нет

Да

Снимок экрана

Справка

Продолжить

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

**ASTRA LINUX** ОПЕРАЦИОННАЯ СИСТЕМА

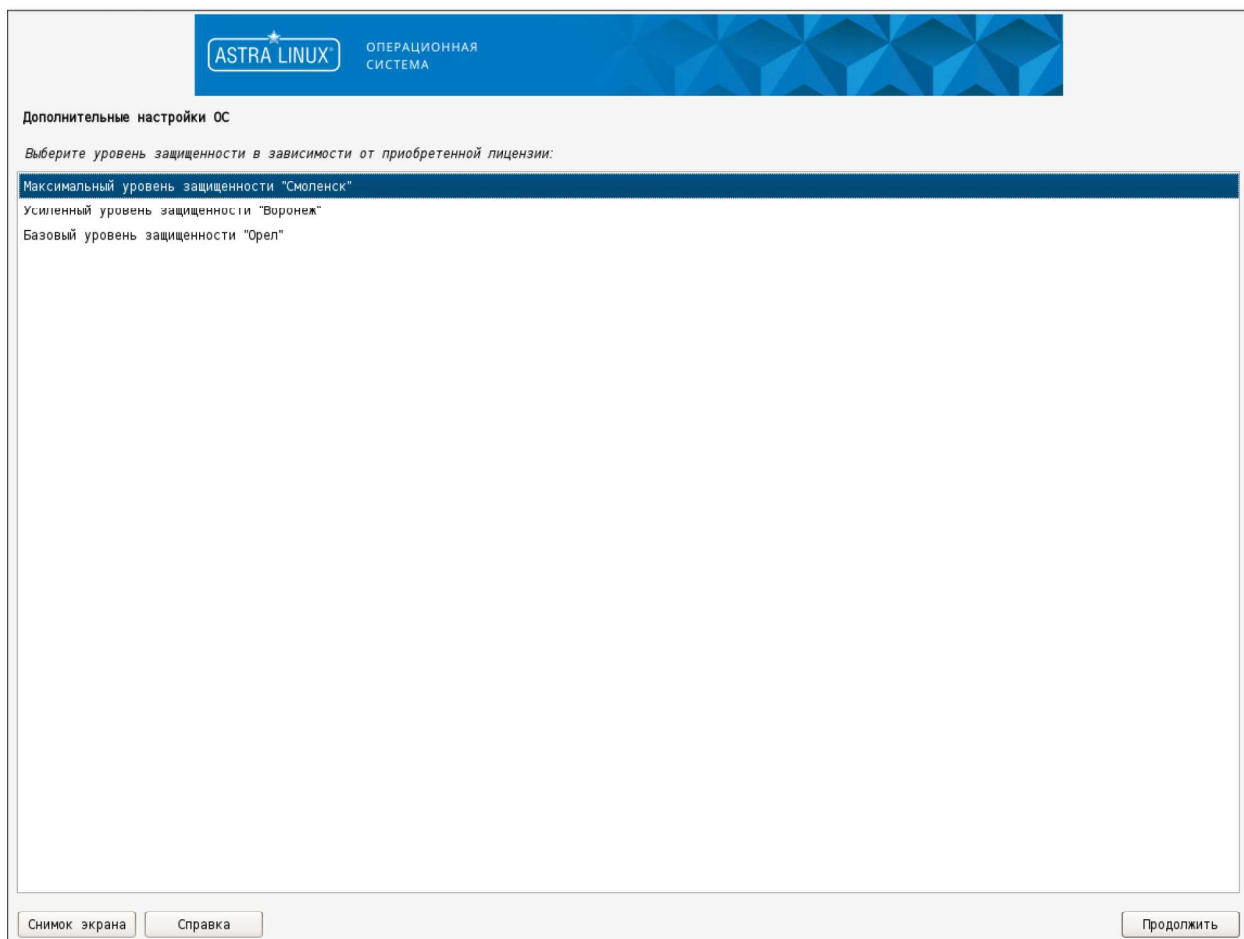
### Выбор программного обеспечения

В данный момент установлена только основа системы. Исходя из ваших потребностей, можете выбрать один и более из готовых наборов программного обеспечения.  
Выберите устанавливаемое программное обеспечение:

- Графический интерфейс Fly
- Средства работы с Интернет
- Офисные приложения
- Средства работы с графикой
- Средства мультимедиа
- Средства Виртуализации
- Игры
- Консольные утилиты
- Средства фильтрации сетевых пакетов ipt
- Расширенные средства для работы с сенсорным экраном
- Средства удаленного подключения SSH
- Ядро hardened

Снимок экрана    Справка    **Продолжить**

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



17. На шаге "Дополнительные настройки ОС" требуется выбрать следующие опции, после чего нажать на кнопку **Продолжить**:

- a. Мандатный контроль целостности (при наличии опции),
- b. Мандатное управление доступом (при наличии опции),
- c. Запрет трассировки ptrace,
- d. Запрос пароля для команды sudo,
- e. Системные ограничения ulimits.



Дополнительные настройки ОС

Вы можете настроить параметры безопасности ОС в зависимости от выбранного режима работы, отключить автоматическую настройку сети и настроить системные часы.

Дополнительные настройки ОС

- Мандатный контроль целостности
- Мандатное управление доступом
- Замкнутая программная среда
- Очистка освобождаемой внешней памяти
- Запрет вывода меню загрузчика
- Запрет трассировки ptrace
- Запрос пароля для команды sudo
- Запрет установки бита исполнения
- Запрет исполнения скриптов пользователя
- Запрет исполнения макросов пользователя
- Запрет консоли
- Системные ограничения ulimits
- Запрет автонастройки сети
- Местное время для системных часов

Снимок экрана

Справка

Продолжить

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

## Установка системного загрузчика GRUB на жёсткий диск

Похоже, что данная система будет единственной на этом компьютере. Если это действительно так, то можно спокойно устанавливать системный загрузчик GRUB в основную загрузочную запись первого жёсткого диска.

Внимание! Если программе установки не удалось обнаружить другую операционную систему, имеющуюся на компьютере, то изменение основной загрузочной записи приведёт к тому, что эту операционную систему некоторое время нельзя будет загрузить. Позднее можно будет настроить GRUB для её загрузки.

Установить системный загрузчик GRUB в главную загрузочную запись?

Нет

Да

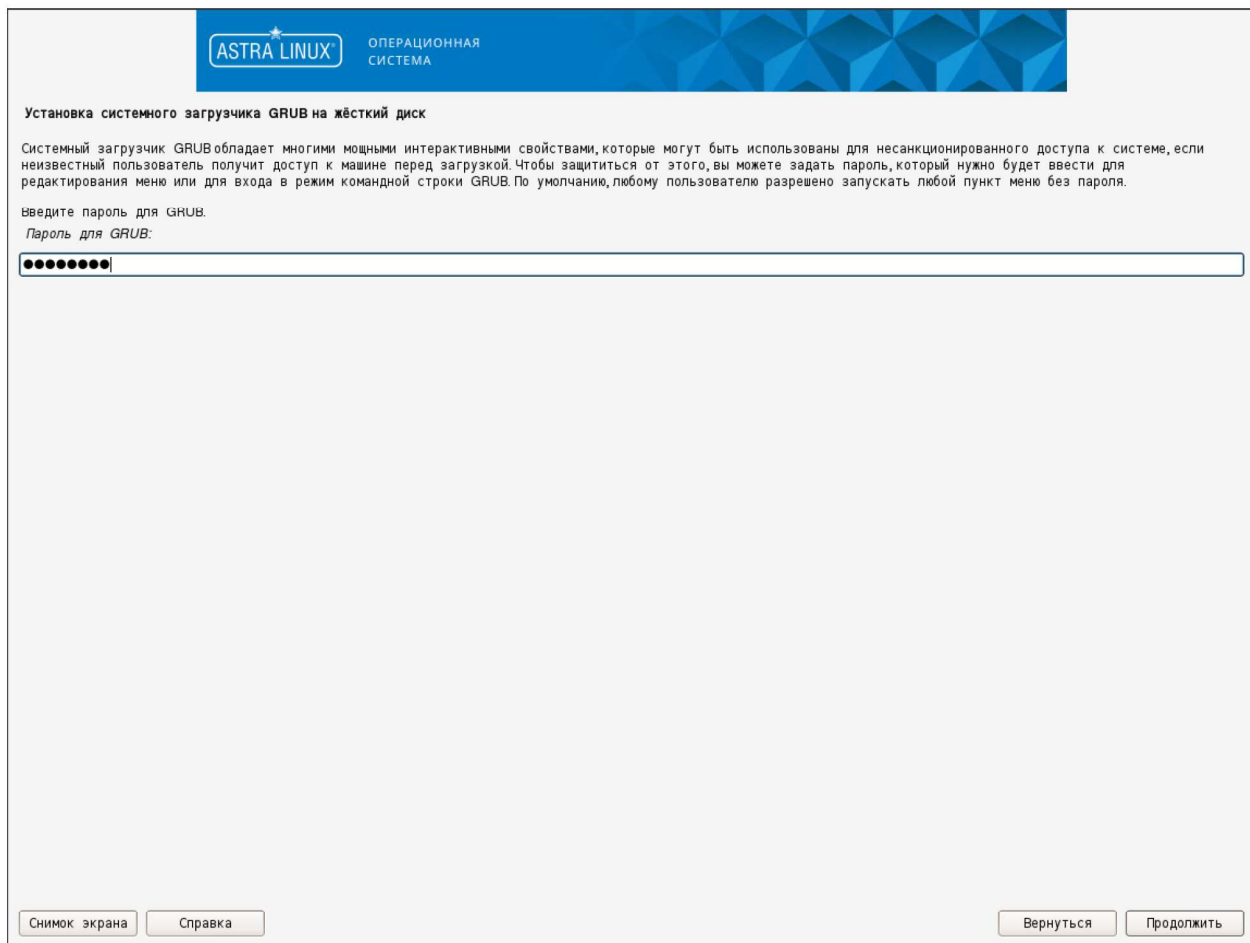
Снимок экрана

Справка

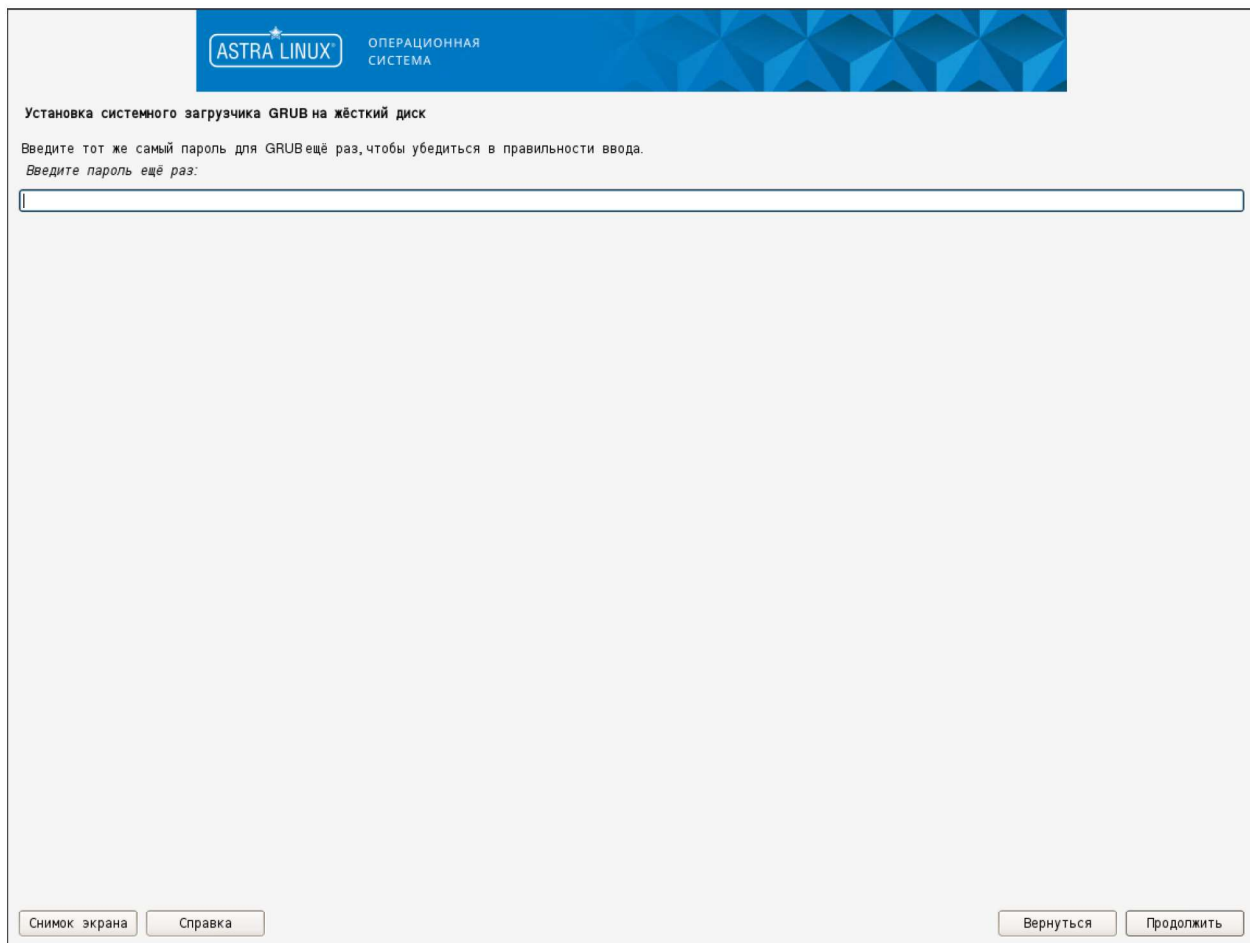
Вернуться

Продолжить

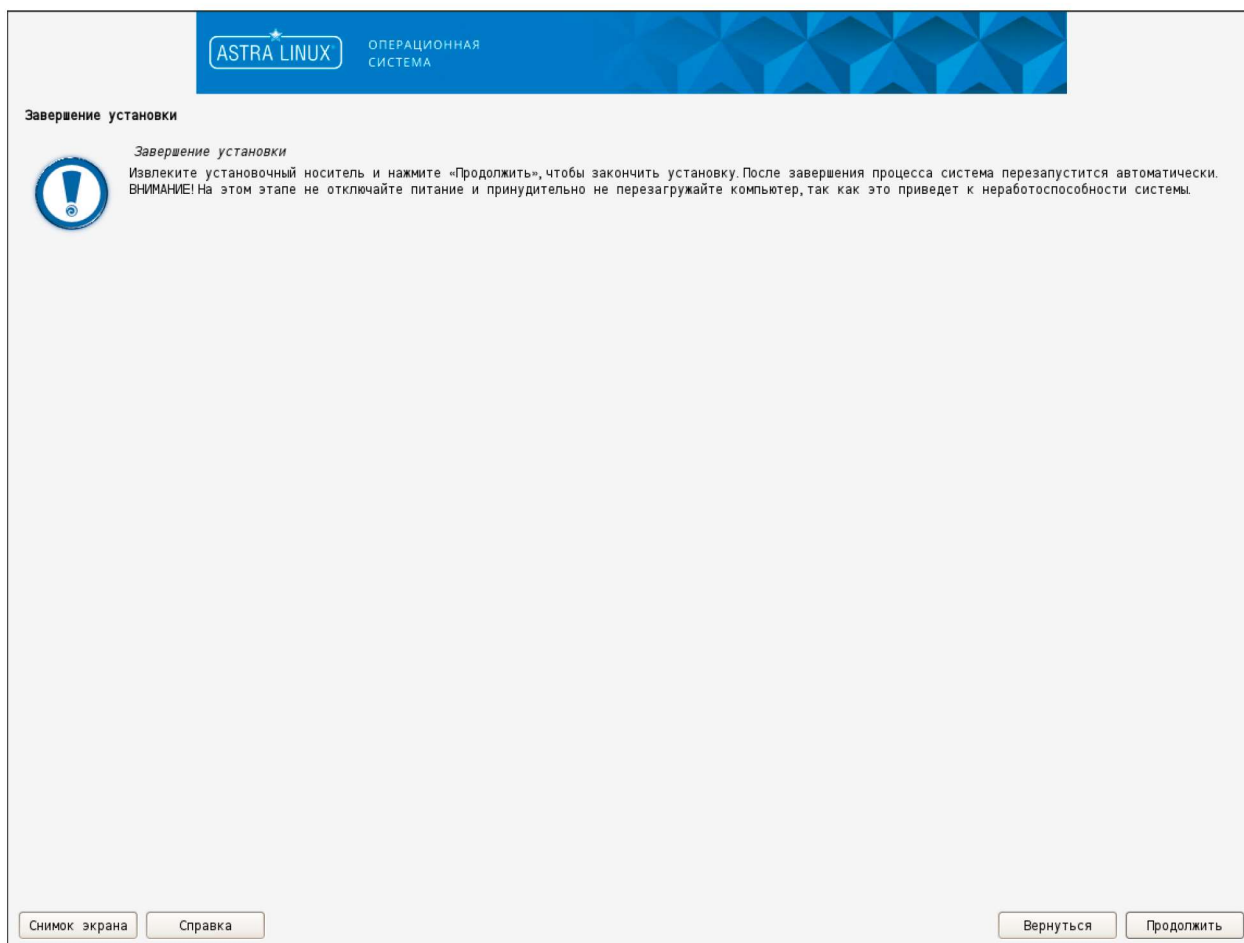
19. Ввести пароль для доступа к редактированию GRUB при загрузке (рекомендуется использовать такой же пароль, как для учётной записи администратора). Нажать на кнопку [Продолжить](#).



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 cdrom на hdd и оставить установочный диск *Astra Linux SE* в cdrom.

### 1.1.6. 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: у.у.у

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

2. 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
```

3. Выполнить следующие команды:

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

4. После перезагрузки проверить доступность сервера, подключившись к нему командной оболочкой с использованием протокола Secure Shell (SSH).

5. 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](#)), обновления, исправления

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 инсталлятора;
- /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/sessionsservice – 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. Вставить диск с *Astra Linux Special Edition* на сервер технического обслуживания и смонтировать в cdrom командой:

```
sudo mount /dev/cdrom
```

3. Создать каталог для публикации репозитория командой:

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

4. Установить *apache2* командой:

```
sudo apt install apache2
```

5. Создать файл конфигурации репозитория командой:

```
sudo touch /etc/apache2/sites-enabled/000-repo.conf
```

6. Открыть файл в текстовом редакторе:

```
sudo mcedit /etc/apache2/sites-enabled/000-repo.conf
```

7. Задать следующее содержимое файла:

```
DocumentRoot /repository/publish
<Directory "/repository/publish">
Options +Indexes
AllowOverride None
Require all granted
</Directory>
```

8. Выполнить команду:

```
sudo rm -f /etc/apache2/sites-enabled/000-default.conf
```

9. В файле */etc/apache2/apache2.conf* раскомментировать параметр *AstraMode* и задать значение *'off'*.

10. Перезапустить приложение *apache2* для применения изменений:

```
sudo systemctl restart apache2
```

11. Создать в */repository/publish* каталоги репозитория для установки стороннего ПО и средств разработки:

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

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

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

13. Смонтировать в *cdrom* диск со средствами разработки для соответствующей версии ОС, который можно загрузить с сайта производителя ОС. Скопировать с диска каталоги *dists* и *pool* в каталог:

```
/repository/publish/smolensk_devel
```

14. Загрузить с сайта производителя ОС диски, включающие актуальные обновления для соответствующей версии ОС (каталоги с дисками имеют имена, начинающиеся с даты, в формате *ууууММдд*). Скопировать с дисков каталоги *dists* и *pool* в соответствующие



каталоги `/repository/publish/smolensk_main_updates_yyyyMMdd`, предварительно создав их. Ознакомиться со списком обновлений можно по ссылке:

- для ОС Astra Linux (очередное обновление 1.6) – <https://wiki.astralinux.ru/pages/viewpage.action?pagelid=41192827>
- для ОС Astra Linux (очередное обновление 1.7) – <https://wiki.astralinux.ru/pages/viewpage.action?pagelid=158612043>

15. Загрузить с сайта производителя ОС диск с последними обновлениями средств разработки для соответствующей версии ОС. Скопировать с диска каталоги `dists` и `pool` в каталог `/repository/publish/smolensk_devel_updates_yyyyMMdd`, предварительно создав его.

16. Создать файл со списком репозитория по умолчанию:

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

17. 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_devel stable main contrib non-free  
deb http://##DEPLOYER_IP##:80/smolensk_main_updates_yyyyMMdd stable main contrib non-free  
deb http://##DEPLOYER_IP##:80/smolensk_devel_updates_yyyyMMdd stable main contrib non-free  
#---end setup repos
```

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

Состав строк может отличаться в зависимости от количества созданных репозитория с обновлениями ОС с именами в формате: `smolensk_main_updates_yyyyMMdd`.

18. Закомментировать все строки символом `#` в следующих файлах:

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

19. Выполнить обновление репозитория командой:

```
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 инсталляционными файлами.

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.com](mailto:market@monitel.com), 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/##CONF_NAME## -C ansible
ansible/bootstrap.sh
```

где `##CONF_NAME##` – имя архива конфигурации инвентаря *Ansible*, указывается в зависимости от [конфигурации развёртывания Системы](#) (количества серверных узлов):  
`ansible.ck11.tar.bz2`, `ansible.ck11.3hosts.tar.bz2`,  
`ansible.ck11.onehost.tar.bz2`.



Для конфигурации развёртывания Системы с шестью серверными узлами используется файл архива `ansible.ck11.tar.bz2`.

5. В каталог `/home/administrator/ansible/files/keytabs` скопировать [keytab-файлы](#) для *Apache* и *PostgreSQL*, созданные ранее. Имена keytab-файлов должны быть следующими:

```
postgres.##PG_CLUSTER_FQDN##.keytab
apache2.##WEB_EP_FQDN##.keytab
```

где `##PG_CLUSTER_FQDN#` – полное доменное имя основного экземпляра кластера PostgreSQL/экземпляра "his" кластера PostgreSQL;

`##WEB_EP_FQDN##` – полное доменное имя WEB\_ENTRY\_POINT.



Необходимость вспомогательного экземпляра "his" кластера *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.

6. В каталог `/home/administrator/ansible/files/certificates` скопировать файлы [SSL-сертификатов](#):

```
root.##domain.local##.crt – корневой сертификат Службы каталогов;
[WEB_EP_FQDN].private_key.pem – содержит только личный ключ (private key);
```



[WEB\_EP\_FQDN].pem – содержит сертификат и личный ключ, включая атрибуты.  
где ##domain.local## – полное имя домена Службы каталогов.

7. Выполнить команды:

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

## 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. [Настройка параметров установки](#).
3. [Монтирование хранилища для резервных копий БД](#).

### 1.3.1. Шесть серверных узлов

- [Настройка конфигурации серверных узлов](#)
- [Настройка 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 псевдонимы 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" кластера *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 точки подключения `WEB_ENTRY_POINT` (`WEB_EP`) к балансировщику нагрузки `WebApi`;

**host-scada** – имя точки подключения `SCADA_ENTRY_POINT` (`SCADA EP`) к балансировщику нагрузки `SCADA`.



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

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

```
host-pg-his-01 ansible_host=10.81.169.147 ansible_user=administrator
postgres_instance=his primary_hostname=host-pg-01
```

```
host-pg-his-02 ansible_host=10.81.169.148 ansible_user=administrator
postgres_instance=his primary_hostname=host-pg-02
```

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

```
host-pg-lst ansible_host=10.81.169.150 postgresql_instance=main
postgresql_entrypoint=yes
```

```
host-pg-his-lst ansible_host=10.81.169.149 postgresql_instance=his
postgresql_entrypoint=yes
```

Для адреса точки подключения `WEB_EP` необходимо добавить атрибут `ck11_web_entrypoint=yes`. Например:

```
host-web ansible_host=10.81.169.158 ck11_web_entrypoint=yes
```

Для адреса точки подключения `SCADA_EP` необходимо добавить атрибут `ck11_scada_entrypoint=yes`. Например:

```
host-scada ansible_host=10.81.169.159 ck11_scada_entrypoint=yes
```

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 развертывания ПО.

#### ▪ [ck11]

##### **Определение**

Серверы приложений СК-11.

##### **Состав**

Узлы, на которых будет установлена серверная часть СК-11. На узлах данной группы будет развернута "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.

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 задачи, доступ к которым выполняется по протоколу HTTPS, используя имя 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 первых двух списка разворачивается сервис *PostgreSQL* и БД с настроенной репликацией между ними. На всех трёх будут развёрнуты компоненты *Corosync+Pacemaker*, обеспечивающие кластеризацию *PostgreSQL*. 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 "Userld | 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

### ▪ [virtual]

#### Определение

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

### Состав

Список необходим при развертывании компонентов для распознавания системой *Ansible* виртуальных имен. По умолчанию:

```
host-pg
host-pg-his
host-web
host-scada
```

#### ▀ Пример заполненного файла конфигурации

```
otikk-deploy ansible_host=10.81.169.157 ansible_user=administrator

otikk-le-scada1 ansible_host=10.81.169.151 ansible_user=administrator
otikk-le-scada2 ansible_host=10.81.169.152 ansible_user=administrator
otikk-le-web1  ansible_host=10.81.169.153 ansible_user=administrator
otikk-le-web2  ansible_host=10.81.169.154 ansible_user=administrator

otikk-le-pg1   ansible_host=10.81.169.155 ansible_user=administrator postgresql_instance=main
otikk-le-pg2   ansible_host=10.81.169.156 ansible_user=administrator postgresql_instance=main
otikk-le-pg    ansible_host=10.81.169.150                postgresql_instance=main
postgresql_entrpoint=yes

otikk-le-his1  ansible_host=10.81.169.147 ansible_user=administrator postgresql_instance=his
primary_hostname=otikk-le-pg1
otikk-le-his2  ansible_host=10.81.169.148 ansible_user=administrator postgresql_instance=his
primary_hostname=otikk-le-pg2
otikk-le-his   ansible_host=10.81.169.149                postgresql_instance=his
postgresql_entrpoint=yes

otikk-le-web   ansible_host=10.81.169.158 ck11_web_entrpoint=yes
otikk-le-scada ansible_host=10.81.169.159 ck11_scada_entrpoint=yes

[manager]
otikk-deploy

[ck11]
otikk-le-scada1
otikk-le-scada2
otikk-le-web1
otikk-le-web2

[ck11_scada]
otikk-le-scada1
otikk-le-scada2

[ck11_web]
otikk-le-web1 keepalived_master=yes
otikk-le-web2

[jsreport]
otikk-le-web1
otikk-le-web2

[cluster]
otikk-le-pg1
otikk-le-pg2
otikk-le-scada1

[postgresql]
otikk-le-pg1
otikk-le-pg2
```



```
otikk-le-his1
otikk-le-his2

[rabbitmq]
otikk-le-scada1
otikk-le-scada2

[etcd]
otikk-le-scada1
otikk-le-web1
otikk-le-web2

[virtual]
otikk-le-pg
otikk-le-his
otikk-le-web
otikk-le-scada
```

### 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 "\_";

**default\_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"
```

**ck11\_energycanonicalmodel\_path:** путь к XML-файлу собственной версии канонической модели энергосистемы. Для использования пользовательской версии канонической модели параметр требуется раскомментировать, после чего указать путь к расположению XML-файла.



Если не требуется использовать пользовательскую версию канонической модели, то параметр `ckll_energycanonicalmodel_path` необходимо оставить закомментированным или указать значение "none".

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**: список IP-адресов 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/repstoryes.yaml` задать значение параметра инвентаря *Ansible*:

**repstoryes\_advanced**: список строк подключения к репозиториям ПО, создание которых описано в разделе "[Создание репозитория из дисков Astra Linux](#)" и добавленных в файл `/etc/apt/sources.list.d/default.list`. Пример заполнения параметра:

`repstoryes_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;

**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 развернута БД модели "Конфигурации системы" (odb\_sysconfig);

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 развертывании СК-11. Необходимо указать одного из пользователей, входящих в список **[postgresql\_su\_users]** файла **users.yaml**.

**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".

---

### 1.3.2. Три серверных узла

- [Настройка конфигурации серверных узлов](#)
- [Настройка 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 псевдонимы 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" кластера *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).



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

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

```
host-pg-his-01 ansible_host=10.81.169.147 ansible_user=administrator
postgres_instance=his primary_hostname=host-pg-01
```

Для адресов прослушивателей экземпляров *PostgreSQL* необходимо добавить атрибут **postgresql\_entrypoint=yes**.

```
host-pg-01 ansible_host=10.81.169.158 postgresql_instance=main
postgresql_entrypoint=yes
```

```
host-pg-his-01 ansible_host=10.81.169.147 postgresql_instance=his
postgresql_entrypoint=yes
```

Для адреса точки подключения `WEB_EP` необходимо добавить атрибут **ck11\_web\_entrypoint=yes**. Например:

```
host-pg-01 ansible_host=10.81.169.158 ck11_web_entrypoint=yes
```

Для адреса точки подключения `SCADA_EP` необходимо добавить атрибут **ck11\_scada\_entrypoint=yes**. Например:

```
host-pg-01 ansible_host=10.81.169.158 ck11_scada_entrypoint=yes
```

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 развертывания 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.

По умолчанию:

```
host-scada-01
```

### ▪ [ck11\_web]

#### **Определение**

Сервер группы горячего резерва "Веб-сервисы".

#### **Состав**

Узел, на котором будут запущены задачи, доступ к которым выполняется по протоколу HTTPS.

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

#### ▪ Пример заполненного файла конфигурации

```

otikk-deploy ansible_host=10.81.169.157 ansible_user=administrator

otikk-le-scada1 ansible_host=10.81.169.151 ansible_user=administrator ck11_scada_entrypoint=yes
otikk-le-web1   ansible_host=10.81.169.153 ansible_user=administrator ck11_web_entrypoint=yes

otikk-le-pg1    ansible_host=10.81.169.155 ansible_user=administrator postgresql_instance=main
postgresql_entrypoint=yes
otikk-le-his1   ansible_host=10.81.169.147 ansible_user=administrator postgresql_instance=his
primary_hostname=otikk-le-pg1 postgresql_entrypoint=yes

[manager]
otikk-deploy

[ck11]
otikk-le-scada1
otikk-le-scada2
otikk-le-web1

[ck11_scada]
otikk-le-scada1

[ck11_web]
otikk-le-web1

[jsreport]
otikk-le-web1

[postgresql]
otikk-le-pg1
otikk-le-his1

[rabbitmq]
otikk-le-scada1

[etcd]
otikk-le-scada1

```

### 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 "\_";

**default\_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"
```

**ck11\_energycanonicalmodel\_path**: путь к ХМИ-файлу собственной версии канонической модели энергосистемы. Для использования пользовательской версии канонической модели параметр требуется раскомментировать, после чего указать путь к расположению ХМИ-файла.



Если не требуется использовать пользовательскую версию канонической модели, то параметр **ck11\_energycanonicalmodel\_path** необходимо оставить закомментированным или указать значение "none".

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**: список IP-адресов 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/reposytoryes.yaml** задать значение параметра инвентаря *Ansible*:

**reposytoryes\_advanced**: список строк подключения к репозиториям ПО, создание которых описано в разделе "[Создание репозитория 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**: учетная запись пользователя, от имени которого будет выполняться аутентификация Kerberos всех серверных задач СК-11;

**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 развернута БД модели "Конфигурации системы" (odb\_sysconfig).

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 развертывании СК-11. Необходимо указать одного из пользователей, входящих в список **[postgres\_su\_users]** файла **users.yaml**.

**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

- [Настройка конфигурации серверного узла](#)
- [Настройка 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 псевдонимы 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-pg-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" кластера *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).



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

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

```
host-pg-his-01 ansible_host=10.81.169.147 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=10.81.169.158 postgresql_instance=main
postgresql_entrypoint=yes

host-pg-his-01 ansible_host=10.81.169.147 postgresql_instance=his
postgresql_entrypoint=yes
```

Для адреса точки подключения `WEB_EP` необходимо добавить атрибут **ck11\_web\_entrypoint=yes**. Например:

```
host-pg-01 ansible_host=10.81.169.158 ck11_web_entrypoint=yes
```

Для адреса точки подключения `SCADA_EP` необходимо добавить атрибут **ck11\_scada\_entrypoint=yes**. Например:

```
host-pg-01 ansible_host=10.81.169.158 ck11_scada_entrypoint=yes
```

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 развертывания ПО.

#### ▪ [ck11]

##### **Определение**

Серверы приложений СК-11.

##### **Состав**

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

host-pg-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.

По умолчанию:

host-pg-01

#### ▪ [ck11\_web]

##### **Определение**

Сервер группы горячего резерва "Веб-сервисы".

##### **Состав**

Узел, на котором будут запущены задачи, доступ к которым выполняется по протоколу HTTPS, используя имя сервера ГР "Веб-сервисы".

По умолчанию:

host-pg-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-pg-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:

host-pg-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-pg-01

#### ▪ Пример заполненного файла конфигурации

```
otikk-deploy ansible_host=10.81.169.157 ansible_user=administrator
```

```
otikk-le-pg1    ansible_host=10.81.169.155 ansible_user=administrator postgresql_instance=main  
ck11_scada_entrypoint=yes ck11_web_entrypoint=yes postgresql_entrypoint=yes  
otikk-le-his1  ansible_host=10.81.169.147 ansible_user=administrator postgresql_instance=his  
primary_hostname=otikk-le-pg1 postgresql_entrypoint=yes
```



```
[manager]
otikk-deploy

[ck11]
otikk-le-pg1

[ck11_scada]
otikk-le-pg1

[ck11_web]
otikk-le-pg1

[jsreport]
otikk-le-pg1

[postgresql]
otikk-le-pg1
otikk-le-his1

[rabbitmq]
otikk-le-pg1

[etcd]
otikk-le-pg1
```

### 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 "\_";

**default\_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"
```

**ck11\_energycanonicalmodel\_path:** путь к XMI-файлу собственной версии канонической модели энергосистемы. Для использования пользовательской версии канонической модели параметр требуется раскомментировать, после чего указать путь к расположению XMI-файла.



Если не требуется использовать пользовательскую версию канонической модели, то параметр `ck11_energycanonicalmodel_path` необходимо оставить закомментированным или указать значение "none".

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:** список IP-адресов 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/reposytoryes.yaml` задать значение параметра инвентаря *Ansible*:

**reposytoryes\_advanced:** список строк подключения к репозиториям ПО, создание которых описано в разделе "[Создание репозитория 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;

**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, на котором будет развернута БД модели "Конфигурации системы" (odb\_sysconfig).

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 развертывании СК-11. Необходимо указать одного из пользователей, входящих в список **[postgresql\_su\_users]** файла **users.yaml**.

**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. 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`

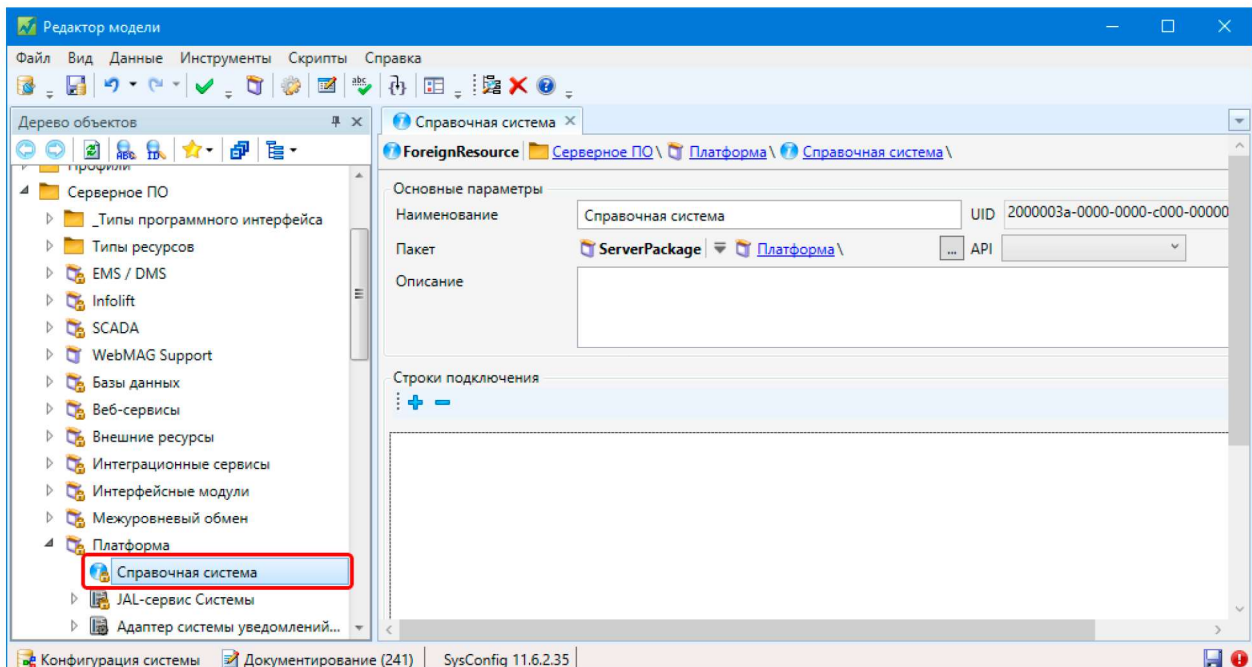



Развёртывание и настройка отказоустойчивого кластера СУБД PostgreSQL выполняется автоматизированно.

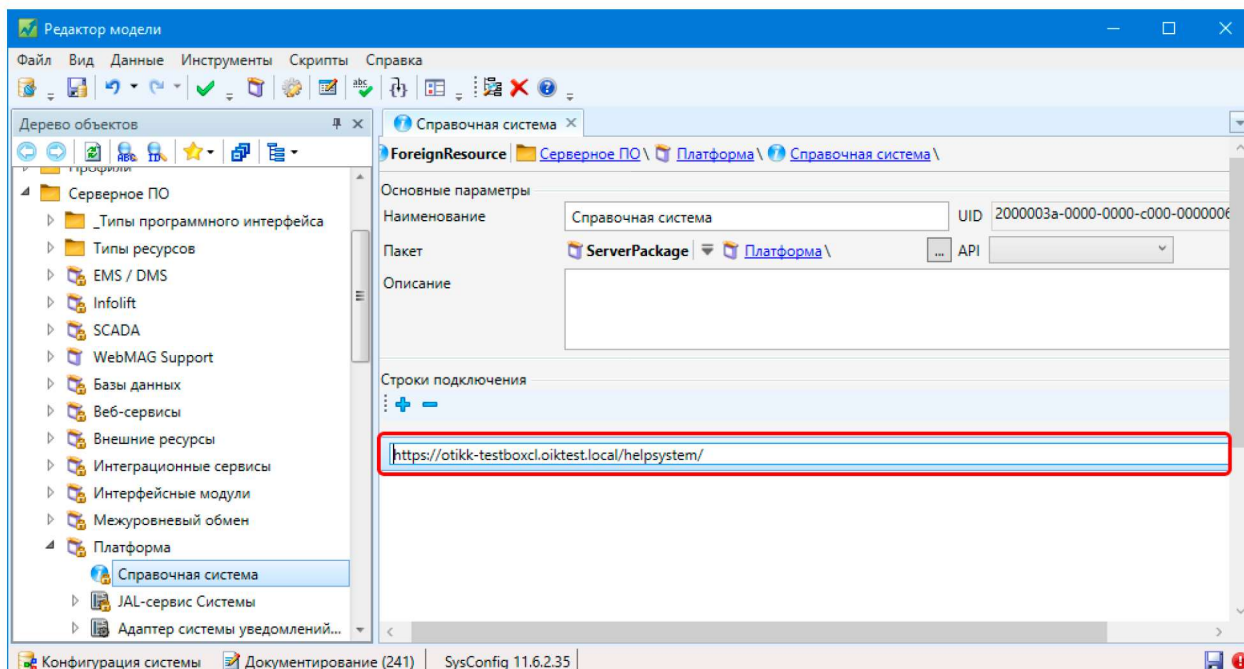
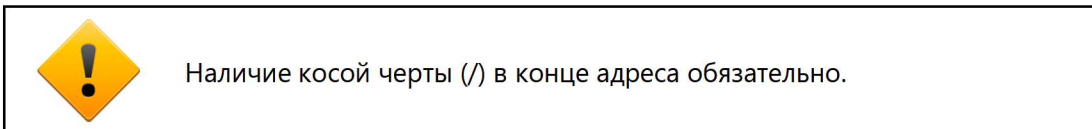
## 1.5. Настройка Справочной системы

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).



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.

