



**Защищенный программный
комплекс «Платформа
Галактика»**

**Инструкция по установке
и настройке системы**

galaktika.ru
galaktika.ru/zpk/

2020

Требования к инфраструктуре

Перед установкой системы необходимо

проверить инфраструктуру по следующей инструкции

[Требования к инфраструктуре](#)

Настройка подключения по SSH

На АРМ с которого будет производиться развертывание ЗПК

необходимо настроить подключение по SSH при помощи сертификатов

по следующей инструкции

[Настройка подключения по SSH](#)

Установка системы

На АРМ с которого будет производиться развертывание ЗПК

необходимо выполнить развертывание ЗПК

по следующей инструкции

[Установка системы \(без пакетов\)](#)

Деинсталляция системы

Необходимо выполнить деинсталляцию ЗПК

по следующей инструкции

[Деинсталляция системы](#)

Установка Astra Linux SE 1.6

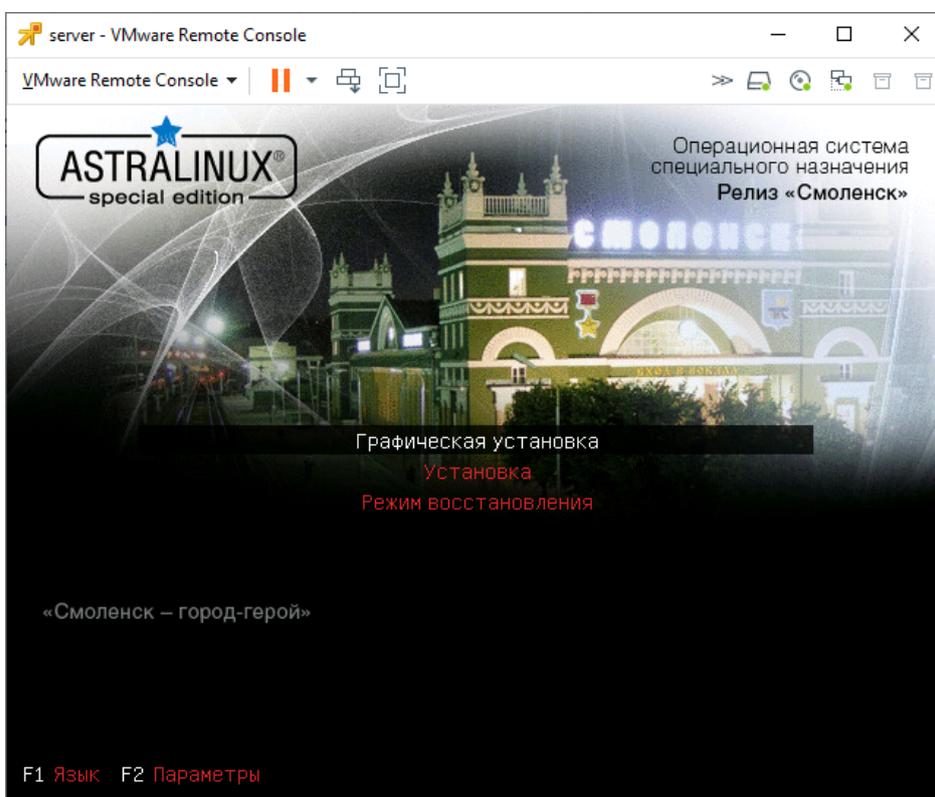
Настройка механизмов защиты Astra Linux SE за рамками данного документа

Типовой список настройки опубликован в Astra Linux Red Book по адресу

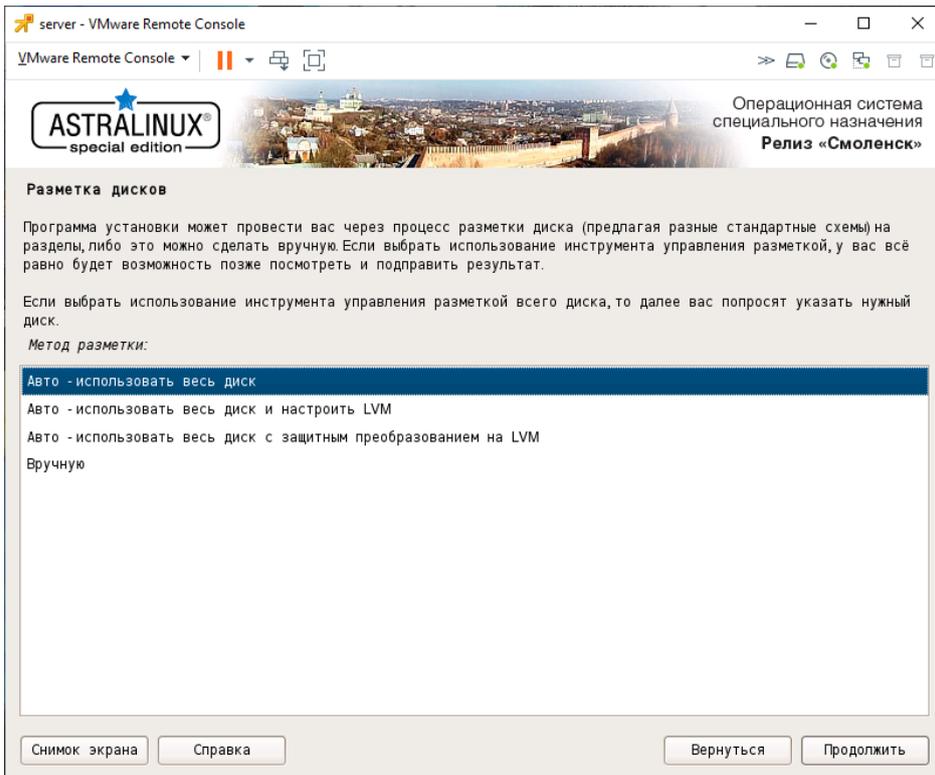
<https://wiki.astralinux.ru/pages/viewpage.action?pageId=57444116>

Запустить загрузку Astra Linux SE с установочного диска

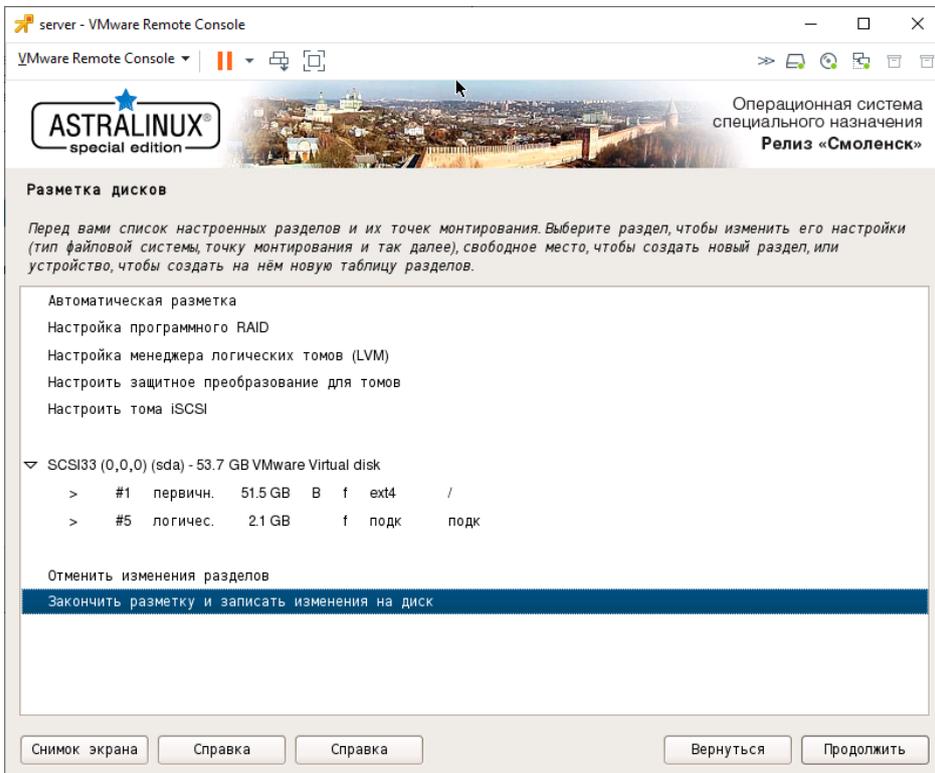
На диалоге выбора типа установки выбрать установку в графическом режиме



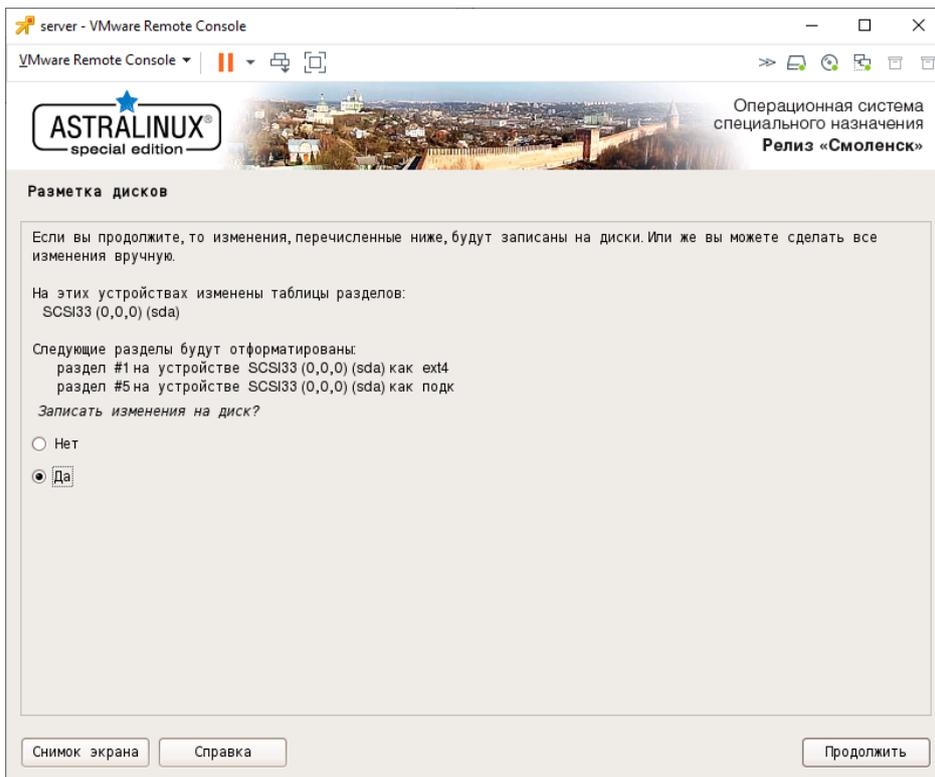
На диалоге разметки дисков необходимо выбрать требуемый тип разметки диска



Подтвердить выбранные настройки



Запустить разметку диска

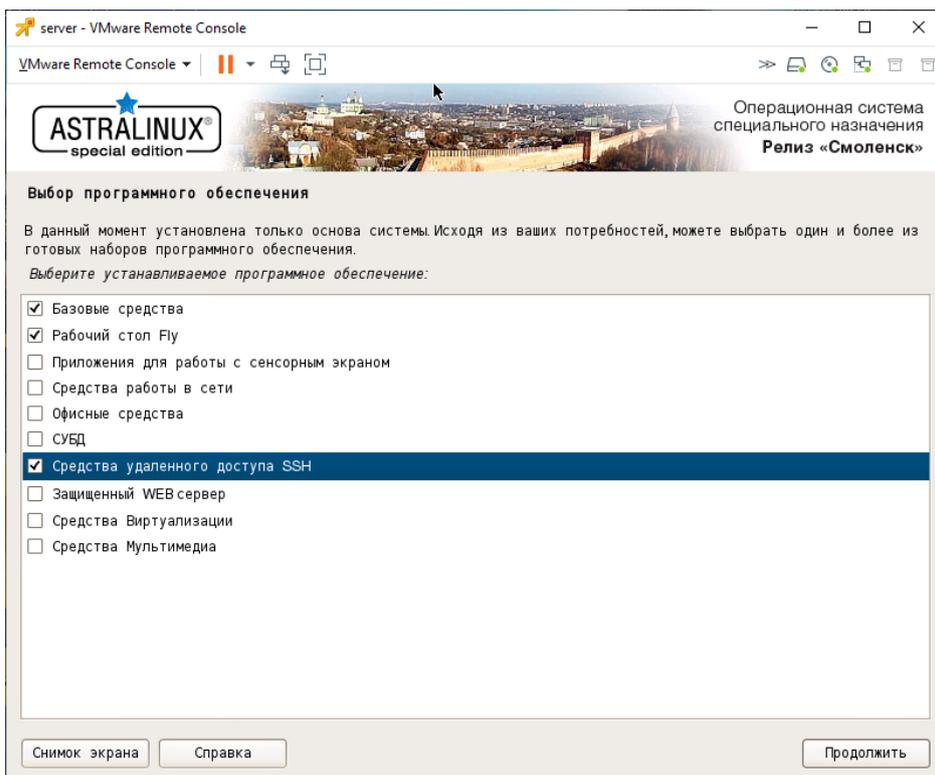


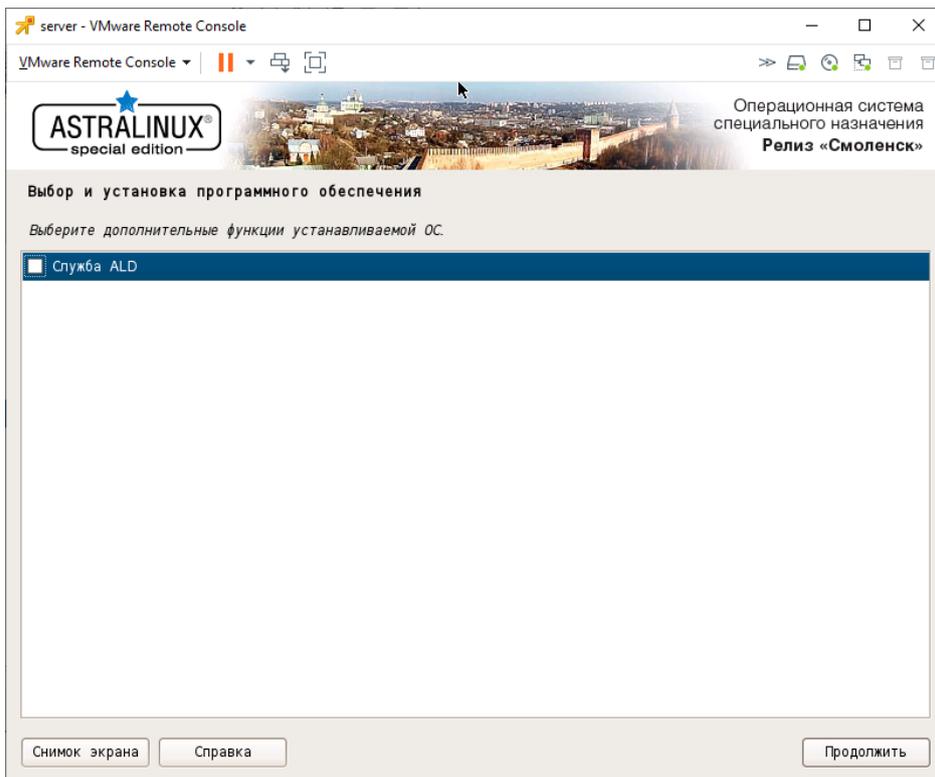
На диалогах выбора программного обеспечения необходимо отметить пункты:

"Базовые средства",

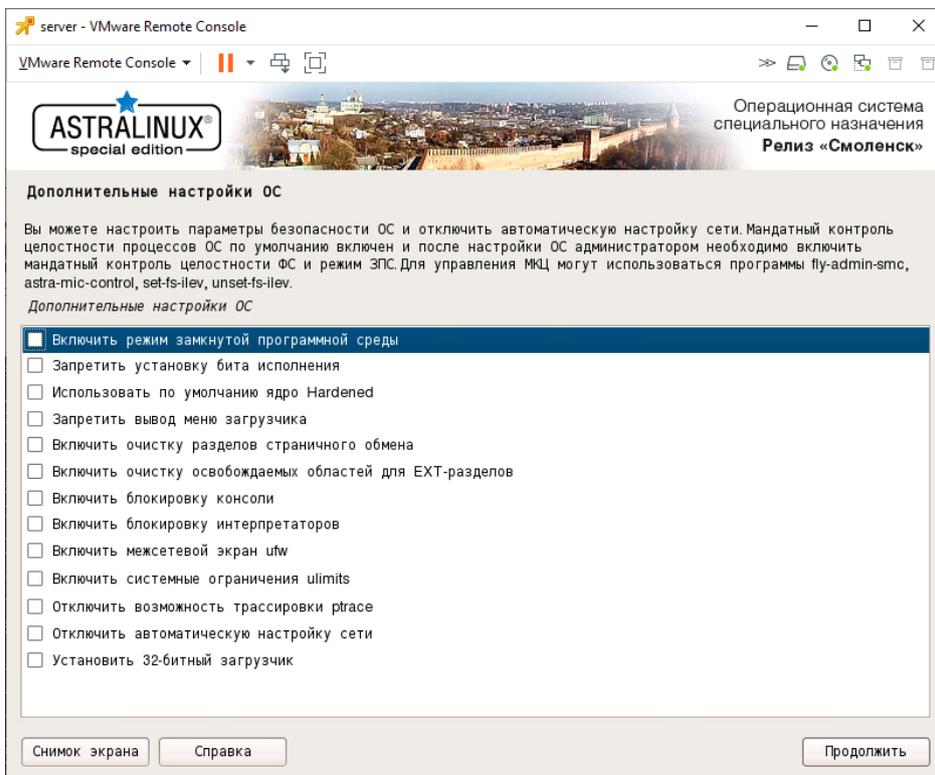
"Рабочий стол Fly"

"Средства удаленного доступа SSH"

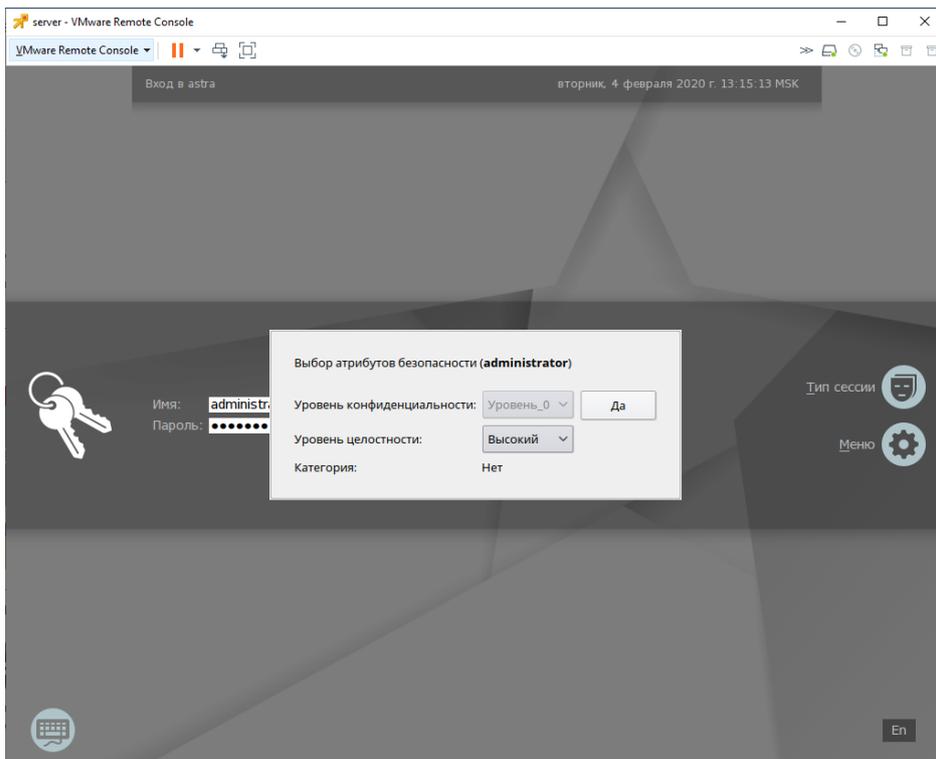




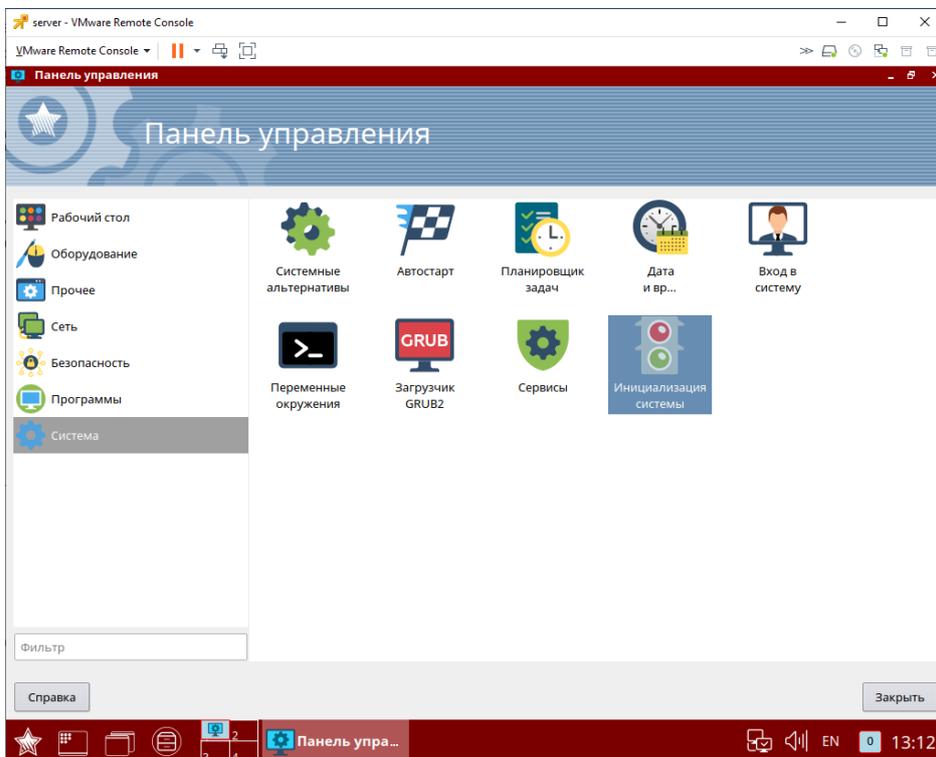
На диалоге дополнительных настроек, оставить параметры выключенными



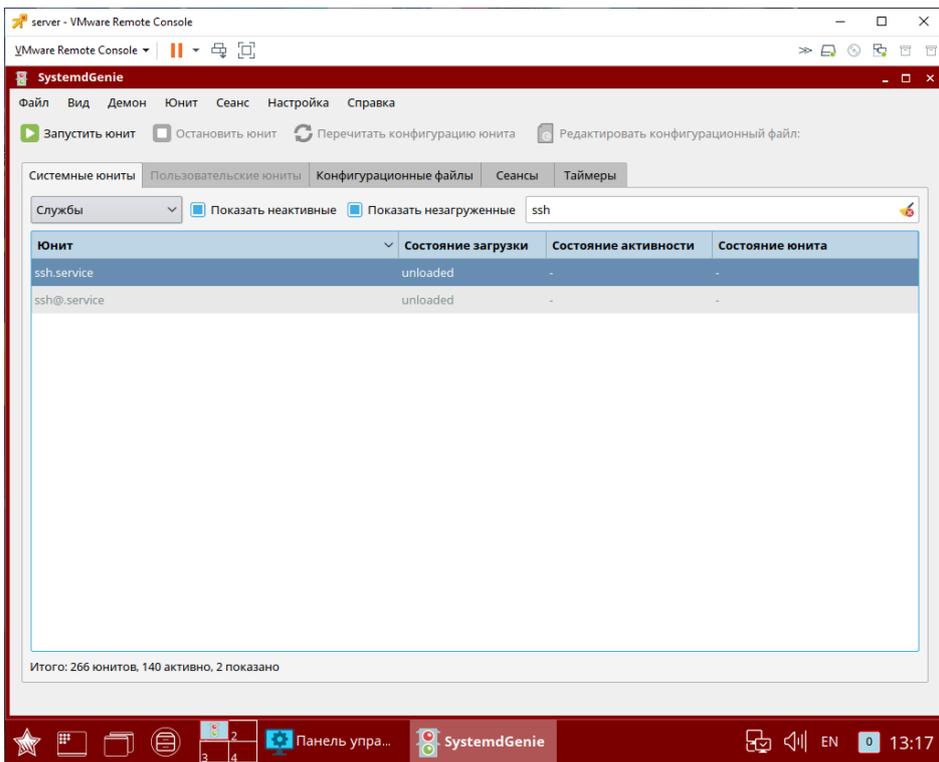
После завершения установки системы войти под учетной записью администратора с высоким уровнем целостности



Открыть панель управления и запустить "Инициализация системы"



Найти в списке служб "ssh.service". В контекстном меню выполнить команды "включить юнит" и "запустить юнит"



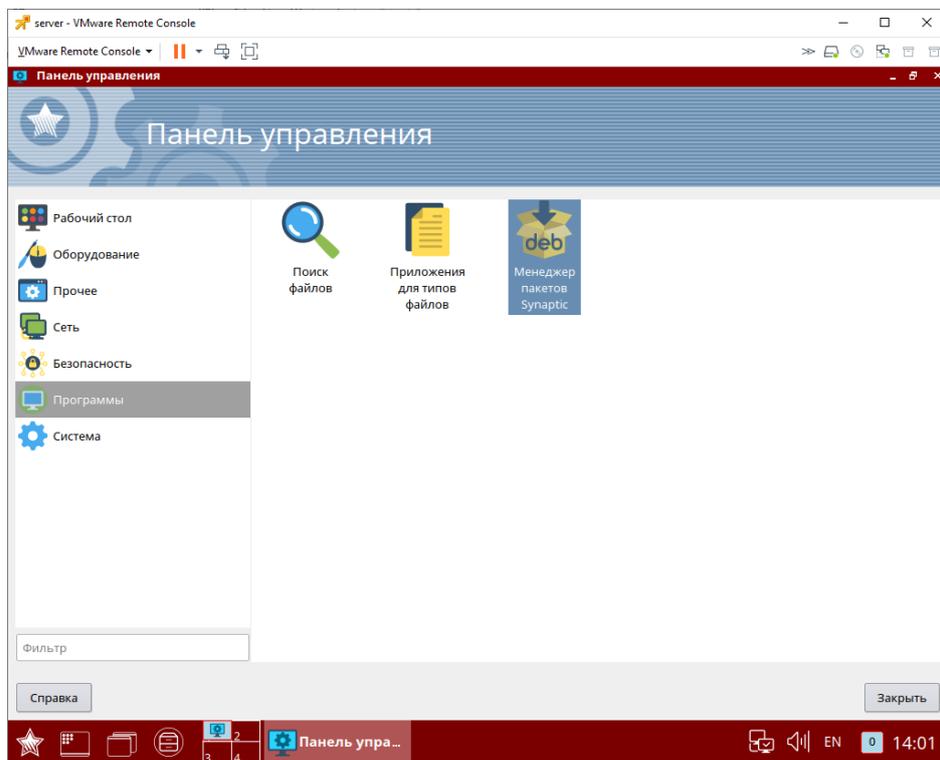
Подробнее ознакомиться с настройками службы SSH можно в статье опубликованной по адресу

<https://wiki.astralinux.ru/display/doc/SSH>

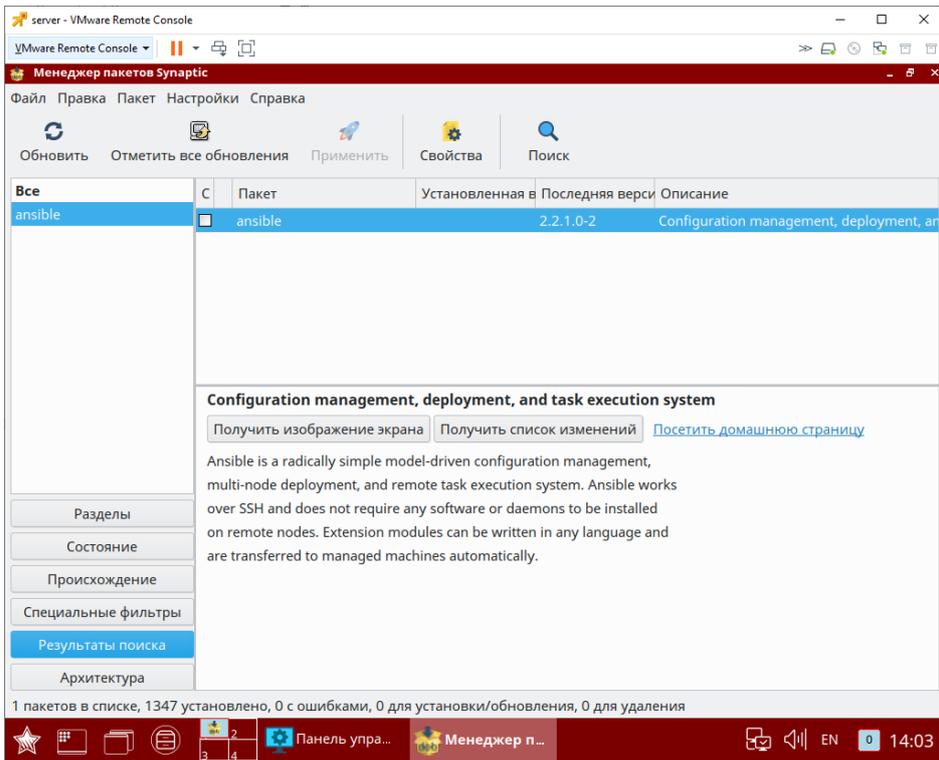
Установка Ansible

Необходимо войти под учетной записью администратора с высоким уровнем целостности

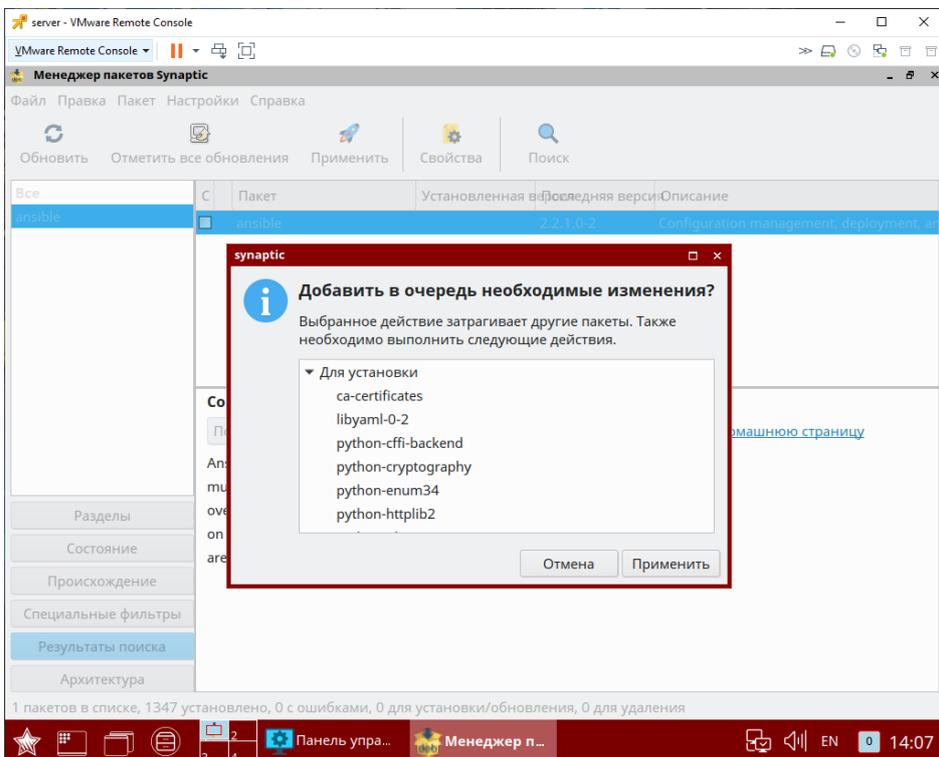
Открыть панель управления и запустить "Менеджер пакетов Synaptic"



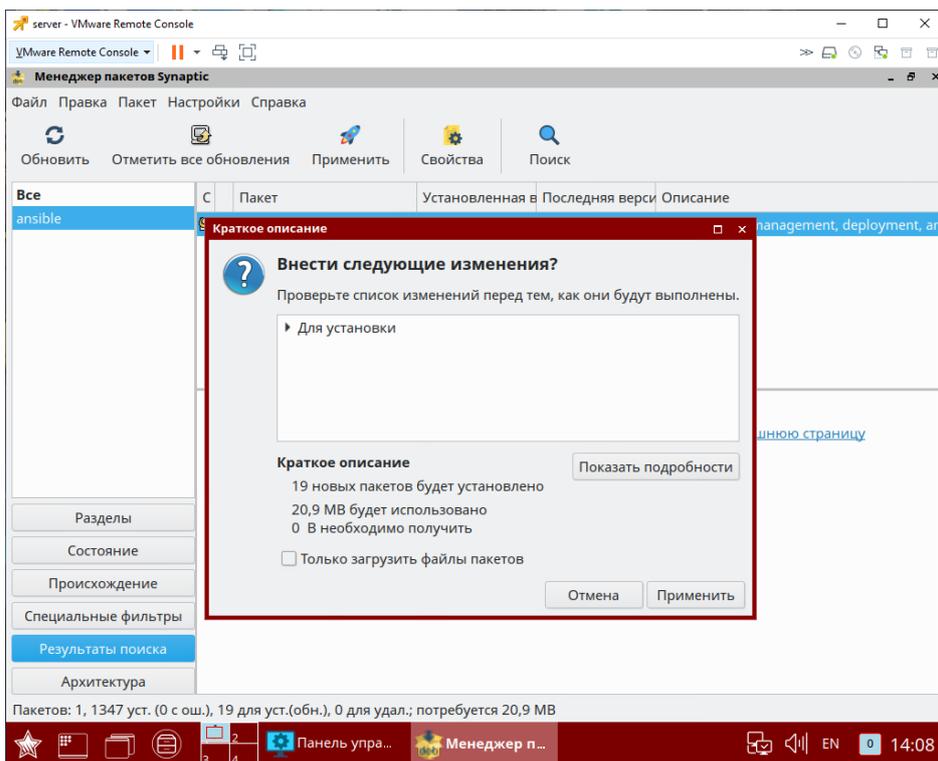
Выбрать пакет "ansible" и в контекстном меню выбрать команду "Отметить для установки"



Добавить в очередь установку зависимых компонентов



Подтвердить установку



Настройка подключения по SSH

Необходимо войти под учетной записью администратора с высоким уровнем целостности

и открыть терминал

Создать ключи для подключения

Для этого выполнить в терминале команду

```
ssh-keygen
```

Можно указать команду без параметров.

Согласиться с предложением записать создаваемый ключ в файл по умолчанию: `~/.ssh/id_rsa`

Пара из открытого и закрытого ключей будет автоматически создана в подкаталоге `.ssh` домашнего каталога пользователя:

```
~/.ssh/id_rsa
```

```
~/.ssh/id_rsa.pub
```

Копирование открытого ключа на сервера

Далее, открытый ключ `~/.ssh/id_rsa.pub` нужно передать на сервера, к которым нужно подключаться.

При этом нужно указать имя пользователя, от имени которого будет производиться подключение

(пользователь должен обладать высоким уровнем целостности и правами администратора через `sudo`)

Для этого выполнить в терминале команду

```
ssh-copy-id -i ~/.ssh/id_rsa.pub имя_пользователя@имя_сервера
```

На запрос пароля необходимо ввести пароль пользователя удалённого компьютера, и ключ будет передан и установлен.

Проверить результат можно подключением, которое должно выполняться без запроса пароля

Для этого выполнить в терминале команду

```
ssh имя_пользователя@имя_сервера
```

Установка системы

Копирование и подготовка пакета установки

Необходимо скопировать установочный пакет ZPK.Platforma.Galaktika-1.0.tgz

на АРМ с которого будет производиться развертывание системы (произведена установка Ansible и настроено подключение по ssh)

Необходимо войти под учетной записью администратора с высоким уровнем целостности и открыть терминал

В терминале перейти в папку с установочным пакетом и выполнить команду

```
tar xzf ZPK.Platforma.Galaktika-1.0.tgz
```

Установочный пакет будет извлечен в папку ZPK

Настройка инвентаря

Необходимо открыть в текстовом редакторе (например nano, mcedit, kate) файл ZPK\inv\hosts

и произвести настройку в соответствии с IP адресами серверов, рабочих станций, и схемой развертывания

Параметры и их назначение:

all: vars: install_packages (true/false) - установка необходимых пакетов. для этого apt должен быть настроен на неинтерактивную установку пакетов с установочного диска Astra Linux SE 1.6

all: vars: setup_dns (true/false) - настройка DNS сервера Bind 9

all: vars: dns_servers - адрес DNS сервера. если параметр setup_dns установлен в true, адрес должен соответствовать серверу из all: children: group_dns: hosts

all: vars: ald_init (true/false) - инициализация домена ALD

all: vars: ald_join (true/false) - подключение серверов и рабочих станций к домену ALD

all: vars: ald_users (true/false) - создание учетных записей пользователей

all: vars: ald_services (true/false) - создание служб kerberos для Web-сервера и сервера СУБД

all: vars: ald_domain - название создаваемого домена ALD и прямой зоны DNS

all: vars: admin_password - пароль учетной записи администратора ALD (admin/admin)

all: vars: ald_server - FQDN имя сервера ЕПП

all: vars: setup_web (true/false) - установка и настройка Web-сервера

all: vars: web_server - FQDN имя сервера приложений

all: vars: auth_realm - название Kerberos realm используемого при аутентификации на сервере приложений

all: vars: database_server - FQDN имя сервера СУБД

all: vars: database_port - номер TCP порта кластера PostgreSQL

all: vars: database_name - название базы данных

all: children: group_dns: vars: zone_fwd - название прямой DNS зоны

all: children: group_dns: vars: zone_rev - название обратной DNS зоны

all: children: group_dns: vars: zone_ns - имя DNS сервера прямой и обратной зоны

all: children: group_dns: vars: zone_fwd_records - A записи прямой зоны

all: children: group_dns: vars: zone_rev_records - PTR записи обратной зоны

all: children: group_dns: vars: hosts - сервер, на который будет установлена роль DNS сервер

all: children: group_ald: vars: kdc_password - Пароль для kerberos master key

all: children: group_ald: vars: hosts - сервер, на который будет установлена роль сервер ЕПП

all: children: group_web: vars: wsgi_path - путь для установки WSGI приложения

all: children: group_web: vars: site_path - путь для установки SPA приложения

all: children: group_web: vars: hosts - сервер, на который будет установлена роль сервер приложений

all: children: group_db: vars: dba_password - пароль для учетной записи postgres кластера PostgreSQL

all: children: group_db: vars: hosts - сервер, на который будет установлена роль сервер СУБД

all: children: group_arm: vars: hosts - рабочие станции, на которые будет установлена роль APM

Настройка учетных записей

Необходимо открыть в текстовом редакторе (например nano, mcedit, kate) файл ZPK\install\passfile2.j2

и настроить список учетных записей ЕПП и их паролей которые будут созданы при установке системы

Проверка доступности

Необходимо войти под учетной записью администратора с высоким уровнем целостности

и открыть терминал

В терминале перейти в папку ZPK с извлеченным установочным пакетом и выполнить команду

```
ansible -i ./hosts all -a 'hostname -f'
```

В выводе выполнения команды не должно быть ошибок подключения к серверам и рабочим станциям

Установка системы

Перед запуском процесса установки, сервера и рабочие станции должны быть настроены на неинтерактивный режим установки пакетов с инсталляционного диска Astra Linux SE 1.6

Необходимо войти под учетной записью администратора с высоким уровнем целостности

и открыть терминал

В терминале перейти в папку ZPK с извлеченным установочным пакетом и выполнить команду

```
./install.sh
```

Деинсталляция системы

Деинсталляция системы на АРМ

Удалить пакеты Astra Linux

- firefox
- firefox-astra
- firefox-l10n-ru

Деинсталляция системы на сервере СУБД

Удалить базу данных указанную в инвентаре в параметре all: vars: database_name

В конфигурационном файле /etc/postgresql/9.6/main/pg_hba.conf удалить строку

аутентификации по gssapi (в колонке peer указан тип gss)

В конфигурационном файле /etc/postgresql/9.6/main/postgresql.conf закомментировать

параметр krb_server_keyfile

Удалить файл /etc/postgresql/9.6/main/krb5.keytab

Удалить кластер PostgreSQL командой pg_dropcluster 9.6 main

Удалить пакеты Astra Linux

- postgresql-astra
- postgresql-contrib

Деинсталляция системы на Web сервере

Удалить содержимое каталога указанного в инвентаре в параметре all: children: web: vars: wsgi_path

Удалить содержимое каталога указанного в инвентаре в параметре all: children: web: vars: site_path

В конфигурационном файле /etc/apache2/mods-enabled/wsgi.conf закомментировать параметр WSGIPythonPath

В конфигурационном файле /etc/apache2/sites-enabled/000-default.conf закомментировать параметр WSGIScriptAlias

и удалить блок <Location /> ... </Location>

Удалить файл /etc/apache2/keytab

Удалить содержимое каталога /usr/local/lib/python2.7/dist-packages

Удалить пакеты Astra Linux

- apache2
- libapache2-mod-auth-kerb
- libapache2-mod-wsgi
- python-jinja2
- python-werkzeug
- python-psycopg2
- python-gssapi

Деинсталляция системы на сервере ЕПП

Удалить из домена ALD службу HTTP/имя web сервера

Удалить из домена ALD службу postgres/имя сервера СУБД

Установка системы (без пакетов)

Копирование и подготовка пакета установки

Необходимо скопировать установочный пакет ZPK.Platforma.Galaktika-1.0.tgz

на АРМ с которого будет производиться развертывание системы

Необходимо войти под учетной записью администратора с высоким уровнем целостности и открыть терминал

В терминале перейти в папку с установочным пакетом и выполнить команду

```
tar xzf ZPK.Platforma.Galaktika-1.0.tgz
```

Установочный пакет будет извлечен в папку install

Настройка инвентаря

Необходимо открыть в текстовом редакторе (например nano, mcedit, kate) файл

install\hosts

и произвести настройку в соответствии с IP адресами серверов, рабочих станций и схемой развертывания

Параметры и их назначение:

all: vars: ald_domain - название домена ALD

all: vars: admin_password - пароль учетной записи администратора ALD (admin/admin)

all: vars: web_server - FQDN имя сервера приложений

all: vars: database_server - FQDN имя сервера СУБД

all: vars: database_port - номер TCP порта кластера PostgreSQL

all: vars: database_name - название базы данных

all: vars: auth_realm - название Kerberos realm используемого при аутентификации на сервере приложений

all: children: web: vars: wsgi_path - путь для установки WSGI приложения

all: children: web: vars: site_path - путь для установки SPA приложения

all: children: web: vars: hosts - сервер, на который будет установлена роль сервер приложений

all: children: database: vars: dba_password - пароль учетной записи postgres кластера PostgreSQL

all: children: database: vars: hosts - сервер, на который будет установлена роль сервер СУБД

Проверка доступности

Необходимо войти под учетной записью администратора с высоким уровнем целостности и открыть терминал

В терминале перейти в папку install с извлеченным установочным пакетом и выполнить команду

```
ansible -i ./hosts all -a 'hostname -f'
```

В выводе выполнения команды не должно быть ошибок подключения к серверам и рабочим станциям

Установка системы

Необходимо войти под учетной записью администратора с высоким уровнем целостности и открыть терминал

В терминале перейти в папку install с извлеченным установочным пакетом и выполнить команду

```
ansible-playbook -i ./hosts ./setup.yml
```

Требования к инфраструктуре

Установка может быть произведена как на базе уже развернутой инфраструктуры так и с разворачиванием ее в процессе установки

Если в инвентаре параметр `install_packages` установлен в `false`, то на серверах и рабочих станциях должны быть предустановлены пакеты описанные с соответствующих разделах

Требования к серверу ЕПП

На сервере организации ЕПП должен быть установлен и настроен домен Astra Linux Directory

Требования к Web серверу

Сервер должен быть подключен к домену развернутому на сервере ЕПП

На сервере должны быть установлены следующие пакеты из состава Astra Linux

- apache2
- libapache2-mod-auth-kerb
- libapache2-mod-wsgi
- python-jinja2
- python-werkzeug
- python-psycopg2
- python-gssapi

Требования к серверу СУБД

Сервер должен быть подключен к домену развернутому на сервере ЕПП

На сервере должны быть установлены следующие пакеты из состава Astra Linux

- postgresql-astra
- postgresql-contrib

Требования к АРМ

АРМ должен быть подключен к домену развернутому на сервере ЕПП

На АРМ должны быть установлены следующие пакеты из состава Astra Linux

- firefox
- firefox-astra
- firefox-l10n-ru