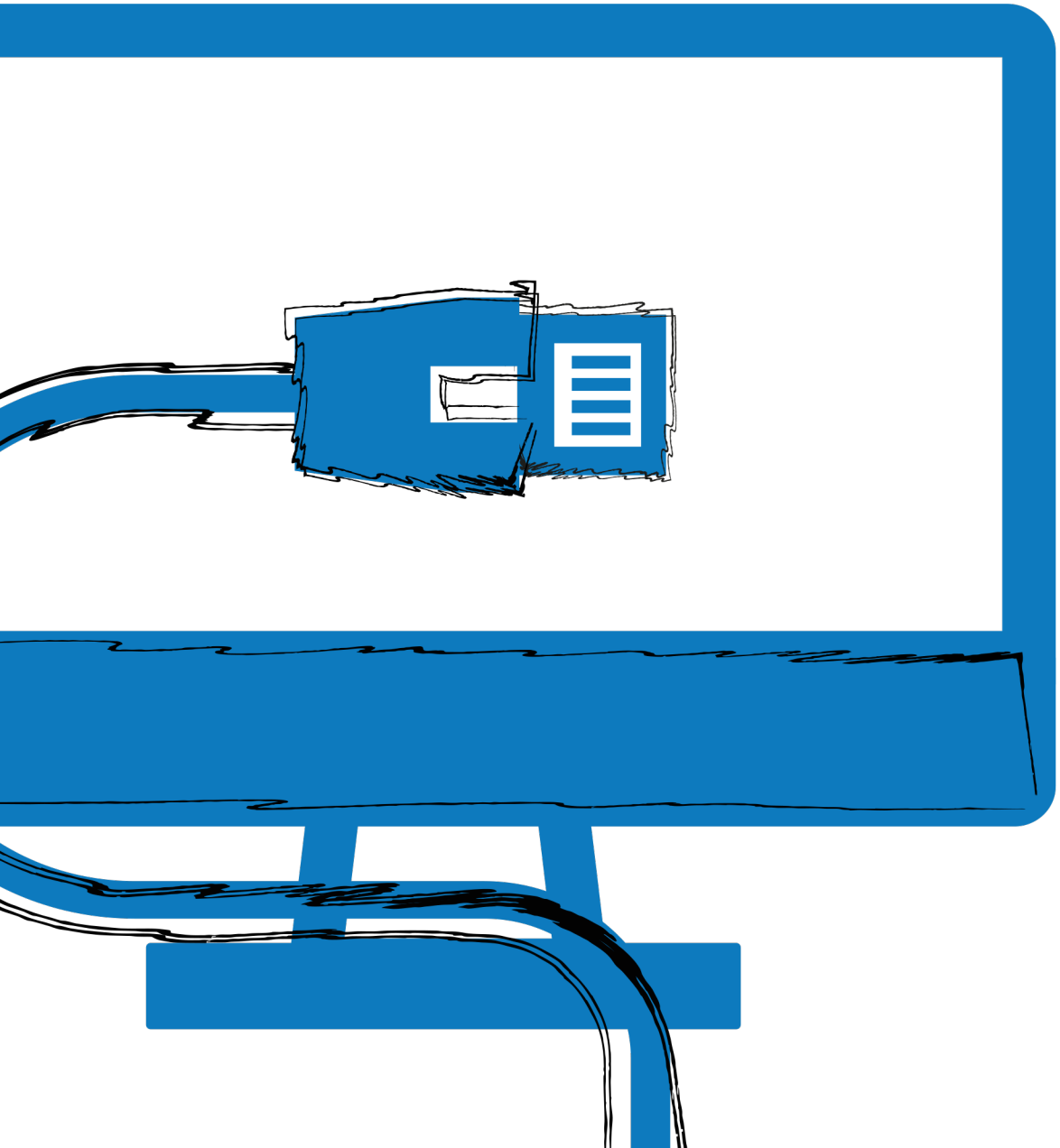
Курс AL-1704

Сборник практических заданий для курса



Оглавление

Сборник практических заданий для курса «ALSE-1704. Сетевое администрирование Astra Linux 1.7»....3
Модуль 1. Основы TCP/IP сетей. Настройка и диагностика сети....4
Модуль 2. IPv6....8
Модуль 3. Настройка удаленного доступа....11
Модуль 4. Служба DNS....13
Модуль 5. Служба DHCP и настройка динамического DNS....16
Модуль 6. Прокси-сервер SQUID....19
Модуль 7. Синхронизация времени по сети....21
Модуль 8. Управление конфигурациями с помощью Ansible....22
Модуль 9. Служба каталогов на базе решения FreeIPA....25
Модуль 10. Веб-сервер на основе Apache....32
Модуль 11. Система электронной почты на базе Exim и Dovecot....37
Модуль 12. Защищенный комплекс программ для печати и маркировки документов....42
Модуль 13. Установка Astra Linux по сети....49

Сборник практических заданий для курса «ALSE-1704. Сетевое администрирование Astra Linux 1.7»

Требования:

- Компьютер со следующими характеристиками:
  - процессор архитектуры AMD64 (x86_64) не менее 8 ядер;
  - RAM не менее 32 ГБ;
  - NVME или SATA SSD диски, не менее 300ГБ свободного места.
- ОС GNU/Linux или Windows 10 (или более новые версии).
- VirtualBox 6.1 или новее.

Материалы:

- Эталонная виртуальная машина template_1704:
  - Процессор — 1.
  - RAM — 2 ГБ.
  - Диск — 30 ГБ.
  - Сетевой адаптер — внутренняя сеть.
  - ОС — Astra Linux Special Edition с установленными дополнениями VirtualBox для гостевых ОС.

Дополнительная информация:

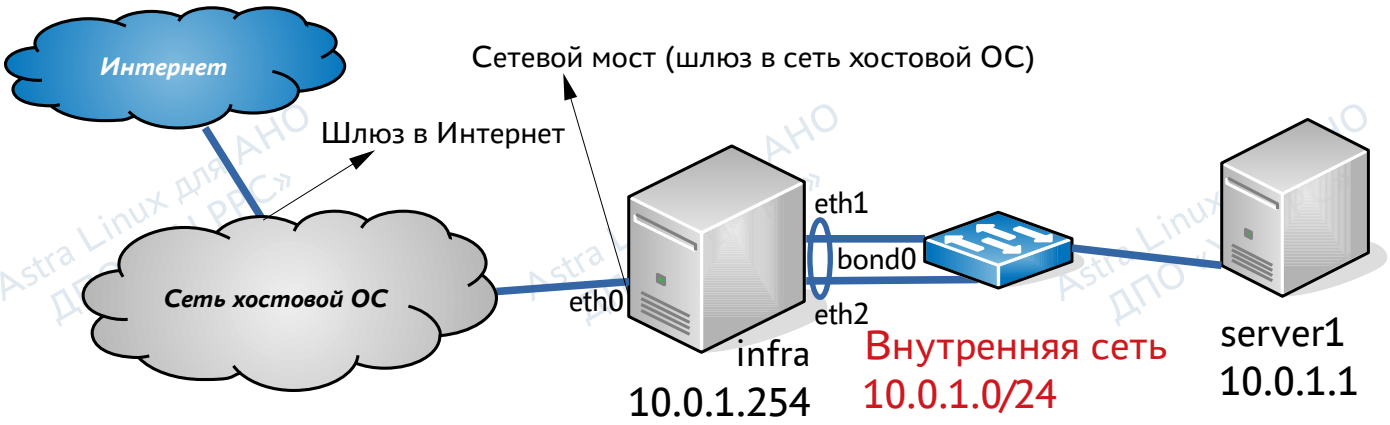
- В сборнике практических заданий используются:
  - имена доменов: astra.test, edu.test;
  - номера сетей 10.0.1.0/24, 10.0.2.0/24;
  - имя учетной записи администратора sa;
  - имена виртуальный машин: infra, server1, server2, client1, s1, s2, c1, mail.
- Преподаватель, на свое усмотрение, может изменить имена доменов, номера сетей, имена учетных записей и имена машин.
- Могут быть использованы другие системы виртуализации для проведения учебных занятий.

Модуль 1. Основы TCP/IP сетей. Настройка и диагностика сети

Описание практического задания

- Установка сетевых настроек на виртуальной машине (ВМ) infra с помощью Network Manager.
- Создание репозитория программного обеспечения на ВМ infra.
- Установка сетевых настроек на ВМ server1 с помощью ifup/ifdown команд.
- Подключение ВМ server1 к репозиторию на ВМ infra.
- Агрегирование (объединение) Ethernet интерфейсов на ВМ infra.

Схема сети



Настройка ВМ infra

1 Клонировать ВМ template_1604 и назвать новую ВМ infra.

2 Не запуская ВМ infra, добавить диск размером 25 Гб и два сетевых интерфейса (всего три). Один (первый) интерфейс — сетевой мост, два других — внутренняя сеть.

3 Запустить ВМ infra.

4 Сменить имя хоста на infra с помощью команды hostnamectl.

5 Создать запись для infra в файле /etc/hosts.

6 Изменить имя соединений в Network Manager на net1, net2, net3.

7 Настроить один из интерфейсов внутренней сети (net2).

8 Проверить, получил ли внешний интерфейс (сетевой мост) IP адрес и сетевые настройки автоматически по DHCP.

9 Если внешний интерфейс (сетевой мост) не получает IP адрес, то настроить интерфейс eth0 (сетевые настройки сообщит Ваш преподаватель).

10 Включить внутреннюю маршрутизацию.

11 Настроить автоматическое включение маршрутизации при загрузке системы в файле /etc/sysctl.conf.

12 Отформатировать новый (второй) диск.

13 Создать каталог /iso.

14 Добавить в /etc/fstab строку для монтирования второго диска.

15 Смонтировать второй диск.

16 Создать в /iso образ установочного компакт-диска 1.7.1 (включающего репозиторий main и обновления update).

17 Установить ftp сервер.

18 Поправить настройки ftp сервера в /etc/vsftpd.conf, разрешив анонимный доступ и включив режим автономной работы (standalone):

listen=YES
anonymous_enable=YES

19 Перезапустить ftp сервер.

20 Создать каталоги /srv/ftp/pub, /srv/ftp/pub/, /srv/ftp/pub/1.7.1-update, /srv/ftp/pub/1.7.1-base.

21 Настроить монтирование образа компакт-диска в каталог /srv/ftp/pub/1.7.1-main в файле /etc/fstab.

22 Смонтировать образы компакт-дисков.

23 Скачать архив devel-1.7.1-22.11.2021_10.50.tgz (дата в названии файла может измениться), например, используя браузер b hfcgfr:

```
tar xvfz devel-1.7.1-22.11.2021_10.50.tgz -C  /srv/ftp/pub/1.7.1/base
```

24 Подключить репозитории, изменив файл /etc/apt/sources.list.

25 При необходимости использования extended репозитория требуется доступ в Интернет:

```
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/ 1.7_x86-64 main contrib non-free
```

26 Либо, как вариант, можно использовать онлайн репозитории, раскомментировав соответствующие строки в /etc/apt/sources.list:

```
#deb cdrom:[OS Astra Linux 1.7.1 1.7_x86-64 DVD ]/ 1.7_x86-64 contrib main non-free
```

```
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-main/ 1.7_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-update/ 1.7_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-base/ 1.7_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/ 1.7_x86-64 main contrib non-free
```

27 Обновить локальный кэш с метаданными репозиториев.

Настройка ВМ server1

1 Клонировать ВМ template_1604 и назвать новую ВМ — server1.

2 Запустить виртуалку.

3 Сменить имя хоста на server1 командой hostnamectl.

4 Добавить в файл /etc/hosts запись о server1.

5 Остановить и запретить запуск Network Manager.

6 Настроить сетевой интерфейс eth0 в файле /etc/network/interfaces.

7 Перезапустить службу и проверить настройки и доступность шлюза.

8 Подключить репозитории в /etc/apt/sources.list.

9 Либо воспользоваться репозиторием в сети Интернет:

```
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-main/ 1.7_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-update/ 1.7_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-base/ 1.7_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/ 1.7_x86-64 main contrib non-free
```

10 Обновить локальный кэш с метаданными репозиториев.

Настройка агрегации Ethernet интерфейсов

1 Настройка производится на ВМ infra.

2 Отключить сетевое соединение net2.

3 Создать логический ведущий (master) интерфейс bond0 с помощью Network Manager.

4 Настроить Ethernet интерфейсы eth1 и eth2 как подчиненные (slave) интерфейсы.

5 Настроить статический адрес 10.0.1.254 на интерфейсе bond0.

6 Активировать настройки bond0.

7 Проверить, что интерфейс bond0 настроен и server1 доступен.

8 Включить на интерфейсе bond0 режим «активный-резервный».

9 Включить на интерфейсе bond0 режим переназначения MAC адреса на активный интерфейс (параметр fail_over_mac).

10 Активировать изменения на интерфейсе bond0.

11 Установить tcpdump.

12 Запустить непрерывную проверку доступности хоста 10.0.1.1.

13 В двух других терминалах осуществлять перехват ICMP сообщений на интерфейсах eth1 и eth2.

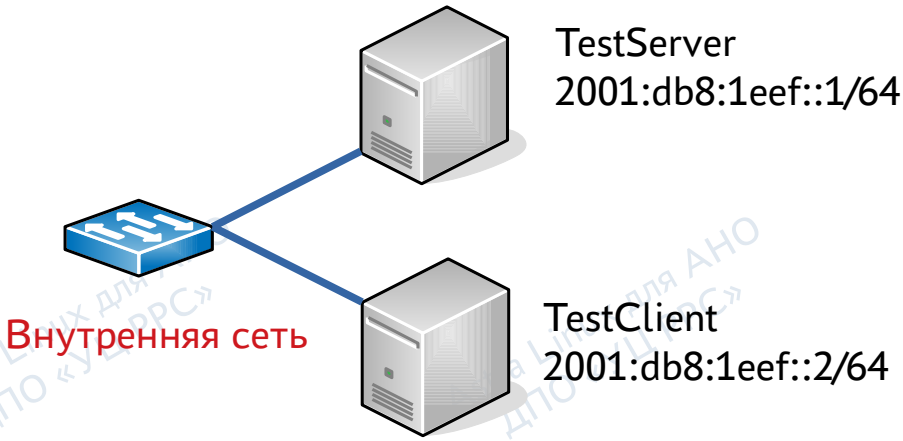
14 В VirtualBox отключить сетевую карту (Устройства→Сеть→Подключить сетевой адаптер 2), по которой передаются данные, и проверить, что передача данных производится по резервному каналу. Снова включить сетевую карту.

Модуль 2. IPv6

Описание практического задания

- Проверка связи по IPv6 с использованием Link-Local адресов.
- Проверка связи по IPv6 с использованием статически назначенных адресов.
- Настройка клиента для получения адреса с помощью RA.
- Настройка клиента для получения адреса с помощью DHCPv6.

Схема сети



Проверка связи с использованием Link Local адресов

1 На TestServer посмотреть ipv6 адрес.

2 На TestClient осуществить ping на полученный адрес.

Назначение статических IPv6 адресов

1 На обеих машинах отключить и замаскировать NetworkManager.

2 На TestServer прописать статический IPv6 адрес 2001:db8:1eef::1.

3 Поднять сетевой интерфейс и проверить, что сетевой интерфейс подтянулся.

4 На TestClient прописать статический IPv6 адрес 2001:db8:1eef::2.

5 Проверить пинг с TestClient на TestServer, используя назначенный статический адрес.

6 Назначить TestClient произвольный статический IPv6-адрес в той же сети.

7 Обновить сетевой интерфейс eth0, убедиться, что адрес принялся.

8 Проверить пинг с TestServer на TestClient по новому адресу.

Настройка radvd для имитации маршрутизатора на сервере TestServer

1 На TestServer установить radvd.

2 На TestServer сконфигурировать radvd для объявления префикса 2001:db8:1eef::/64.

3 Запустить службу radvd.

Настройка получения IPv6 адресов на TestClient с применением RA

1 Настроить на TestClient в /etc/network/interfaces получение IPv6 по RA. Статические настройки удалить.

2 На TestClient применить настройки IPv6, проверить получение IPv6. адреса

3 На TestServer проверить пинг полученного из EUI-64 Global Unicast-адреса, и пинг до временного адреса.

```
ping 2001:db8:1eef:0:a00:27ff:fe91:8f3e
ping 2001:db8:1eef:0:ac11:56a7:8c95:d482
```

4 Посмотреть таблицу маршрутизации:

```
ip -6 r
```

Настройка на TestServer isc-dhcp-server для выдачи IPv6-адресов по dhcpv6

1 Установить isc-dhcp-server.

2 Включить в файле /etc/default/isc-dhcp-server.

3 Добавить настройку префикса сети для выдачи по DHCPv6 в файле /etc/dchp/dhcpd6.conf.

```
subnet6 2001:db8:1eef::/64 {
        range6 2001:db8:1eef::dfc5:d0
2001:db8:1eef::dfc5:ff;
}
```

4 Запустить isc-dhcp-server, при необходимости активировать.

Настройка получения IPv6 адресов на TestClient с применением по DHCPv6

1 Настроить на TestClient в /etc/network/interfaces получение IPv6 по DHCPv6.

2 На TestClient применить настройки IPv6, проверить получение IPv6 адреса.

3 На TestServer проверить пинг полученного из EUI-64 Global Unicast-адреса, и пинг до временного адреса:

```
ping 2001:db8:1eef::dfc5:f9
```

4 Посмотреть таблицу маршрутизации:

```
ip -6 r
```

5 Если нет пинга или default-маршрута то необходимо проверить состояние radvd (так как default gateway получается с помощью RA, а не DHCPv6), при необходимости включить, а также активировать:

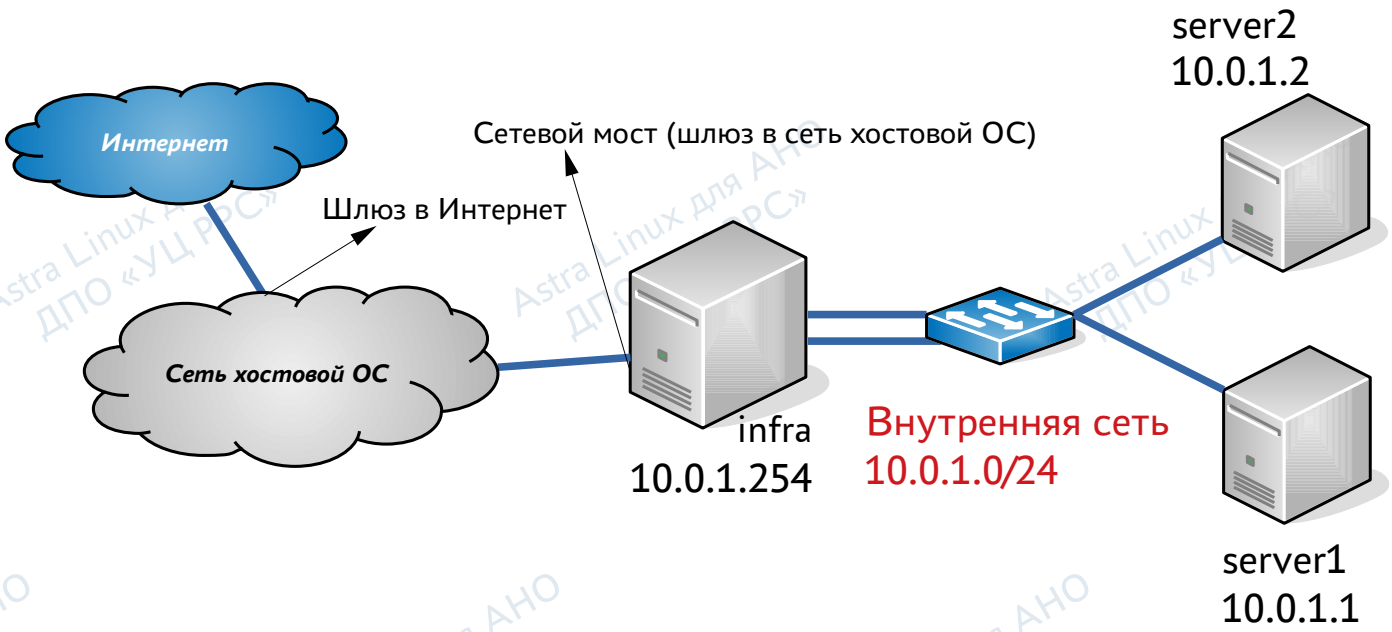
```
systemctl status radvd
systemctl start radvd
systemctl enable radvd
```

Модуль 3. Настройка удаленного доступа

Описание практического задания

- Настройка аутентификации по ключам при подключении по SSH с ВМ infra к ВМ server1.
- Создание и настройка ВМ server2.
- Настройка аутентификации по ключам при подключении по SSH с ВМ infra к ВМ server2.
- Перенаправление портов с помощью SSH для доступа к сетевым сервисам, запущенных на интерфейсе localhost.

Схема сети



Настройка аутентификации по ключам

1 На server1 запустить службу ssh и добавить ее в автозагрузку.

2 На infra настроить аутентификацию по ключам с server1 под учетными записями sa на клиенте и сервере.

3 Клонировать ВМ template_1604 и назвать ее server2.

4 Сменить имя хоста на server2.

5 Добавить в файл /etc/hosts запись о server2.

6 Остановить и запретить запуск Network Manager.

7 Настроить сетевой интерфейс eth0 в файле /etc/network/interfaces.

8 Перезапустить службу networking и проверить настройки и доступность шлюза.

9 Скопировать на server2 с server1 (командой scp) файл /etc/apt/sources.list.

10 Обновить локальный кэш с метаданными подключенных репозиториев.

11 На server2 запустить службу ssh и добавить ее в автозагрузку.

12 На infra настроить аутентификацию по ключам с server2 под учетными записями sa на клиенте и сервере.

Перенаправление портов (дополнительное задание)

1 На ВМ server1 установить FTP сервер vsftpd.

2 Создать каталог /srv/ftp/pub.

3 В каталог /srv/ftp/pub поместить файл test.txt.

4 Внести изменения в файл /etc/vsftpd.conf для настройки анонимного доступа к FTP серверу и запуска сервера на интерфейсе 127.0.0.1 в режиме автономной работы (standalone).

5 Перезапустить службу vsftpd.

6 Проверить работоспособность FTP сервера и что сервер доступен только локально.

7 На ВМ infra проверить доступ к FTP серверу, установленному на ВМ server1, с помощью утилиты curl.

8 Настроить динамическое перенаправление портов на ВМ infra.

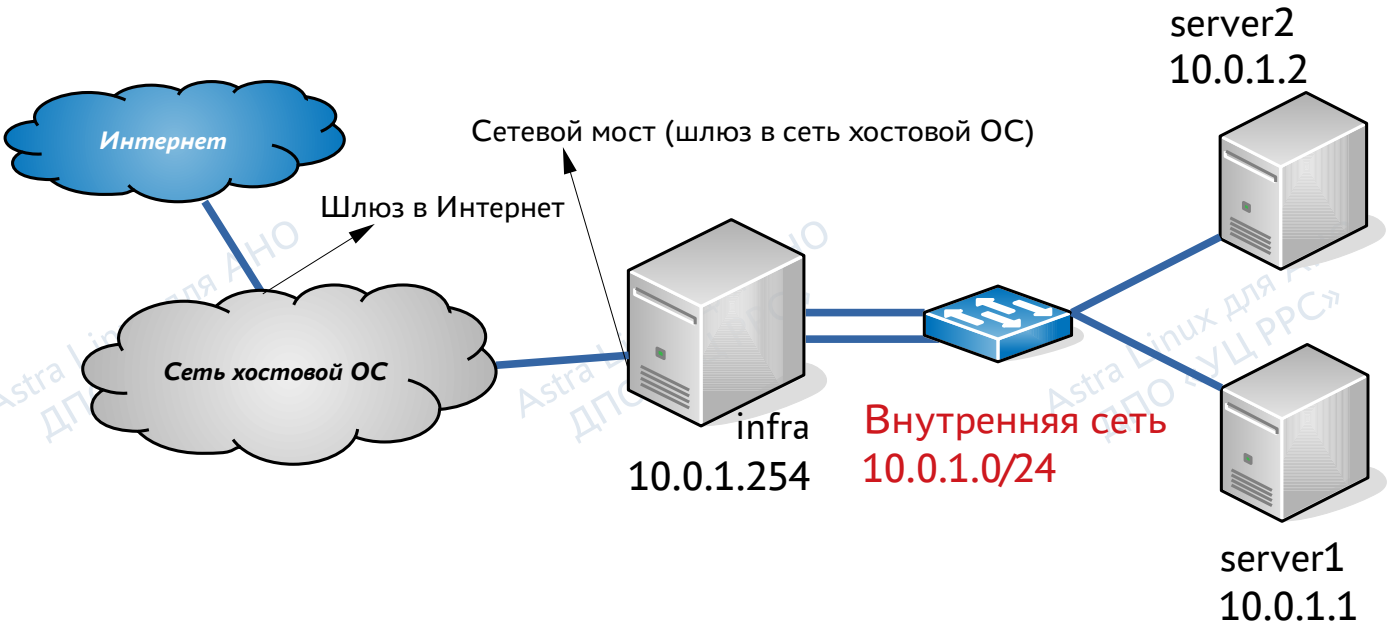
9 Получить файл test.txt с FTP сервера с помощью утилиты curl.

Модуль 4. Служба DNS

Описание практического задания

- Настройка ведущего DNS сервера.
- Настройка подчиненного DNS сервера.
- Настройка кэширующего сервера.
- Настройка клиентской части DNS.

Схема сети



Настройка ведущего сервера DNS для зон astra.test и 1.0.10.in-addr.arpa

1 В ВМ server1 установить bind9.

2 В файле /etc/bind/named.conf.local описать зону astra.test, для которой server1 является ведущим сервером DNS.

3 В файле /etc/bind/named.conf.local описать зону 1.0.10.in-addr.arpa, для которой server1 является ведущим сервером DNS.

4 Проверить правильность внесенных изменений в настройки сервера DNS.

5 Создать каталог /var/cache/bind/master. Назначить группу bind группой — владельцем созданного каталога и установить бит защиты sgid.

6 Создать файл astra.test в каталоге /var/cache/bind/master с ресурсными записями для зоны astra.test:

- SOA;
- NS (server1.astra.test и server2.astra.test);
- A - для server1.astra.test, server2.astra.test, infra.astra.test (внутренний интерфейс);
- CNAME www→server1.

7 Проверить правильность внесения зонной информации в файл astra.test.

8 Создать файл 10.0.1 в каталоге /var/cache/bind/master с ресурсными записями для зоны 1.0.10.in-addr.arpa:

- SOA;
- NS (server1.astra.test и server2.astra.test);
- PTR (для адресов 10.0.1.1, 10.0.1.2, 10.0.1.254).

9 Проверить правильность внесения зонной информации в файл 10.0.1.

10 Настроить перенаправление запросов о доменных именах других зон на ВМ infra. Для этого внести изменения в файл /etc/bind/named.conf.options.

11 Перезапустить сервер DNS и проверить, что служба DNS работает.

Настройка подчиненного сервера DNS для зон astra.test и 1.0.10.in-addr.arpa

1 Убедиться, что на server2 настроена сеть. Если это не было сделано ранее, то настроить аналогично, как это было сделано ранее.

2 В ВМ server2 установить bind9.

3 Проверить запущена ли служба bind9. Если не служба не работает, то запустить.

4 Создать каталог /var/cache/bind/slave. Назначить группу bind группой — владельцем созданного каталога и установить на каталог бит защиты sgid.

5 Настроить server2 как подчиненный (slave) сервер для зоны astra.test. Для этого внести соответствующие изменения в файл /etc/bind/named.conf.local. Зонную информацию хранить в файле /var/cache/bind/slave/astra.test.

6 Настроить server2 как подчиненный (slave) сервер для зоны 1.0.10.in-addr.arpa. Для этого внести соответствующие изменения в файл /etc/bind/named.conf.local. Зонную информацию хранить в файле /var/cache/bind/slave/10.0.1.

7 Проверить правильность внесенных изменений в настройки сервера DNS.

8 Перезапустить сервер DNS и проверить, что служба DNS работает.

Настройка кэширующего сервера DNS

1 Настройка производится на ВМ infra.

2 В ВМ infra установить bind9.

3 Проверить запущена ли служба bind9. Если не служба не работает, то запустить.

4 Настроить на server1 и server2 перенаправление DNS запросов по разрешению имен внешних (Интернет) DNS имен на кэширующий сервер (infra).
Для этого внести изменения в файл /etc/bind/named.conf.options на server1 и server2.

Настройка клиентской части DNS

1 Настроить клиентскую часть DNS, указав в качестве DNS серверов:

- на server1 — localhost;
  В файл /etc/resolv.conf внести запись:
- на server2 — localhost;
  В файл /etc/resolv.conf внести запись:
- на infra — server1 и server2.

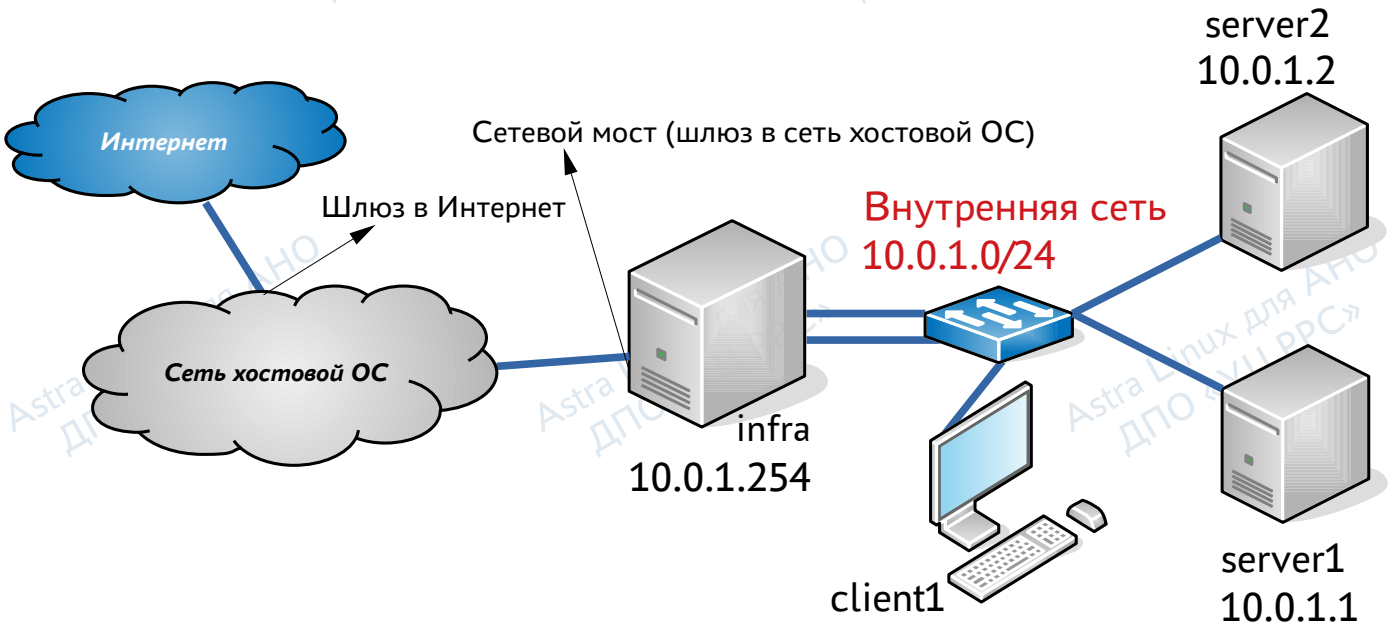
2 Убедиться, что разрешаются имена и адреса как во внутренней сети, так и в Интернет во всех трех ВМ: server1, server2, infra.

Модуль 5. Служба DHCP и настройка динамического DNS

Описание практического задания

- Настройка службы DHCP для выдачи и получения динамического IP адреса.
- Настройка службы DHCP для выдачи и получения фиксированного IP адреса.
- Настройка динамического DNS.

Схема сети



Настройка выдачи и получения динамических IP адресов

1 На server1 установить сервер DHCP.

2 В файле /etc/default/isc-dhcp-server определить, на каком сетевом интерфейсе будет работать сервер DHCP.

3 Выделить диапазон 10.0.1.101-10.0.1.199 для выдачи динамических IP адресов. Сервер DHCP должен передавать адрес шлюза (10.0.1.254) и адреса серверов DNS (10.0.1.1, 10.0.1.2). Внести соответствующие изменения в файл /etc/dhcp/dhcpd.conf.

4 Запустить службу DHCP и проверить, что служба запущена:

5 Путем клонирования ВМ template_1604 создать и запустить ВМ client1.

6 Изменить имя хоста на client1.

7 Удалить из файла /etc/hosts строку:
127.0.1.1 astra

8 Настроить на client1 получение динамического адреса. Для настройки использовать Network Manager и dhclient. Внести изменения в файл /etc/NetworkManager/NetworkManager.conf.

9 Проверить, что IP адрес был получен.

10 Определить продолжительность аренды IP адреса и адрес DHCP сервера, с которого были получены сетевые реквизиты. Воспользуйтесь командой nmcli.

11 На сервере DHCP (ВМ server1) с помощью команды dhcp-lease-list получить информацию о выданных IP-адресах.

Настройка выдачи и получения фиксированного IP адреса

1 В ВМ server2 настроить получение адреса по DHCP. Внести соответствующие изменения в файл /etc/network/interfaces.

2 Деактивировать сетевой интерфейс.

3 Перезапустить службу networking и проверить, что IP адрес получен с сервера DHCP.

4 В ВМ server1 настроить службу DHCP для выдачи фиксированного IP адреса (10.0.1.2/24) хосту server2. Внести соответствующие изменения в файл /etc/dhcp/dhcpd.conf, указав в параметрах шлюз по умолчанию, а в качестве сервера DNS — localhost.
Примечание: узнать MAC адрес сетевого интерфейса хоста server2 можно, например, командой dhcp-lease-list.

5 Перезапустить службу DHCP:

6 На хосте server2 деактивировать сетевой интерфейс, перезапустить службу networking и проверить получение IP адреса, маршрут по умолчанию и разрешение имен DNS.

Настройка динамического обновления зонной информации на DNS сервере

1 Настроить службу DNS (server1):

- С помощью утилиты dnssec-keygen создать ключ с именем dhcp-dns, используя алгоритм хеширования MD5 для формирования кода аутентификации сообщений (HMAC-MD5). Длина ключа — 128 бит.

- Значение ключа сохраняется в файл в текущем каталоге с суффиксом .private.
- В файл /etc/bind/named.conf.local добавить секцию типа key, в которой описываются параметры созданного ключа.
- В секции типа zone добавить разрешение обновлять зонную информацию с помощью созданного ключа.
- Перезапустить службу DNS и проверить ее статус.

2 Настроить службу DHCP (server1):

- В файл /etc/dhcp/dhcpd.conf внести следующие изменения:
  - Определить параметр domain-name.
  - Определить параметры ddns-update-style и ddns-updates.
  - Добавить секцию типа key с описанием параметров созданного ранее ключа (такую же, как в настройках службы DNS).
  - Создать секции типа zone для зон astra.test и 1.0.10.in-addr.arpa, в которых определяются ведущий сервер DNS и используемый для обновления ключ.
- Перезапустить службу DHCP и проверить статус службы:

3 Настроить клиент DHCP (client1):

- Добавить в файл /etc/dhcp/dhclient.conf следующие настройки:
  send fqdn.fqdn "client1.astra.test.";
  send fqdn.encoded on;
  send fqdn.server-update on;
  request fqdn;
- Выключить и включить "Проводное соединение 1".

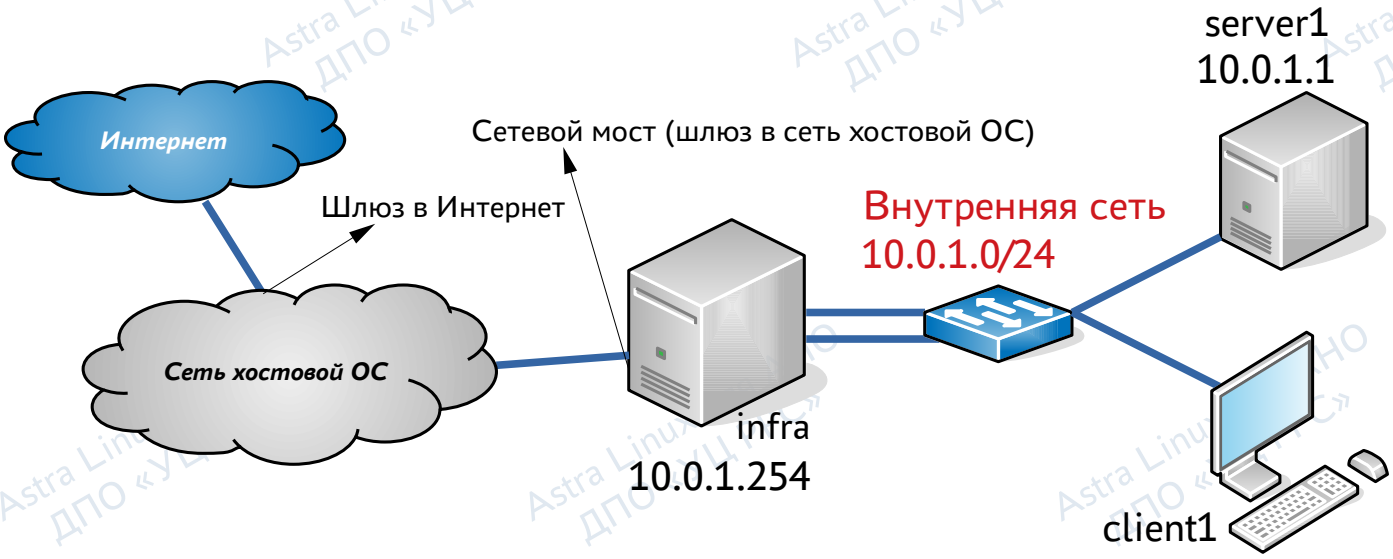
4 Проверить, что зонная информация обновилась на обоих серверах DNS (server1 и server2) и включает ресурсные записи для хоста client1 и в зоне astra.test и в зоне 1.0.10.in-addr.arpa.

Модуль 6. Прокси-сервер SQUID

Описание практического задания

- Установка и первоначальная настройка SQUID.
- Настройка базовой аутентификации в SQUID.
- Настройка ограничения доступа пользователей к web-ресурсам по времени.

Схема сети



Установка и первоначальная настройка SQUID

1 Установить SQUID на ВМ infra.

2 Сохранить исходный вариант конфигурационного файла SQUID.

3 На основе исходного конфигурационного файла SQUID создать новый конфигурационный файл, исключив комментарии и пустые строки, содержащиеся в исходном файле.

4 Создать в конфигурационном файле /etc/squid/squid.conf список управления доступом типа src с именем localnet, добавив в этот список управления доступом все хосты из сети 10.0.1.0/24.

5 Включить в /etc/squid/squid.conf правило разрешающее хостам, определенным в списке управление доступом localnet, обращаться к прокси-серверу.
Примечание: правило должно быть размещено до запрещающего правила http_access deny all.

6 Выполнить команду, которая позволяет перечитать измененный конфигурационный файл.

7 Проверить доступность сервера SQUID и возможность доступа к Интернет ресурсам на ВМ client1 (используйте браузер Firefox).

Настройка базовой аутентификацию NCSA

1 Установить программный пакет apache2-utils на infra.

2 Командой htpasswd создать пользователя iuser на infra.
Примечание: используйте параметр -c имя_файла_с_паролями, когда первый раз выполняете команду htpasswd.

3 Установить владельцев proxy:proxy и права 640 на файл с паролями.

4 Внести изменения в конфигурационный файл SQUID:

- Настроить схему аутентификации NCSA с помощью директивы auth_param.
- Определить список управления доступом типа proxy_auth с именем authusers, который содержит всех валидных пользователей.
- Добавить правило, запрещающее доступ пользователям, не указанным в списке управления доступом authusers, и правило, разрешающее доступ валидным пользователям.
  Примечание: правила должны быть размещены до последнего правила, запрещающего доступ всем, и до правила localnet.

5 Выполнить перечитывание конфигурационного файла сервером SQUID.

6 Проверить, работает ли аутентификация для SQUID с ВМ client1.

Настройка запрета доступа к веб-ресурсам в указанный временной диапазон (запретить доступ к youtube в рабочее время)

1 Создать список управления доступом типа dstdomain, который включает домен youtube.com.

2 Создать список управления доступом типа time, который определяет рабочее время.

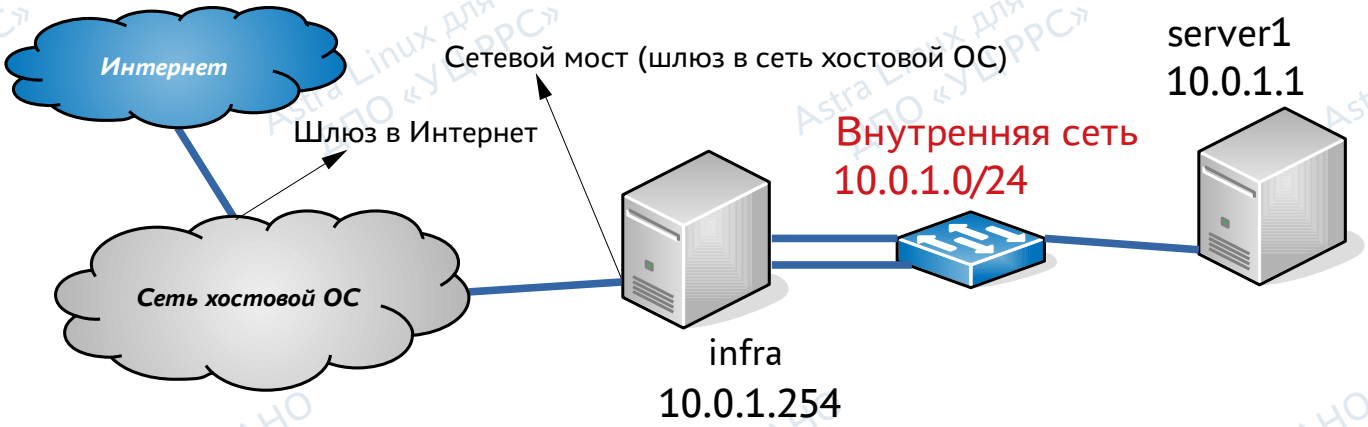
3 Добавить правило, которое запрещает доступ к сайтам в домене youtube.com в рабочее время, указав одновременно оба списка управления доступом.
Примечание: поместите правило в нужно место в файле /etc/squid/squid.conf, чтобы оно сработало.

Модуль 7. Синхронизация времени по сети

Описание практического задания

- Настройка службы chronycd.
- Настройка встроенной в systemd службы синхронизации времени.

Схема сети



Настройка синхронизации времени с помощью службы ntpd

1 Настроить службу chrony на ВМ infra:
   - В качестве источника времени выбрать пул ru.pool.ntp.org.
   - Остальные источники времени из конфигурационного файла удалить.
2 С помощью утилиты chronyc проверить, что синхронизация времени производится.

Настройка синхронизации времени с помощью systemd

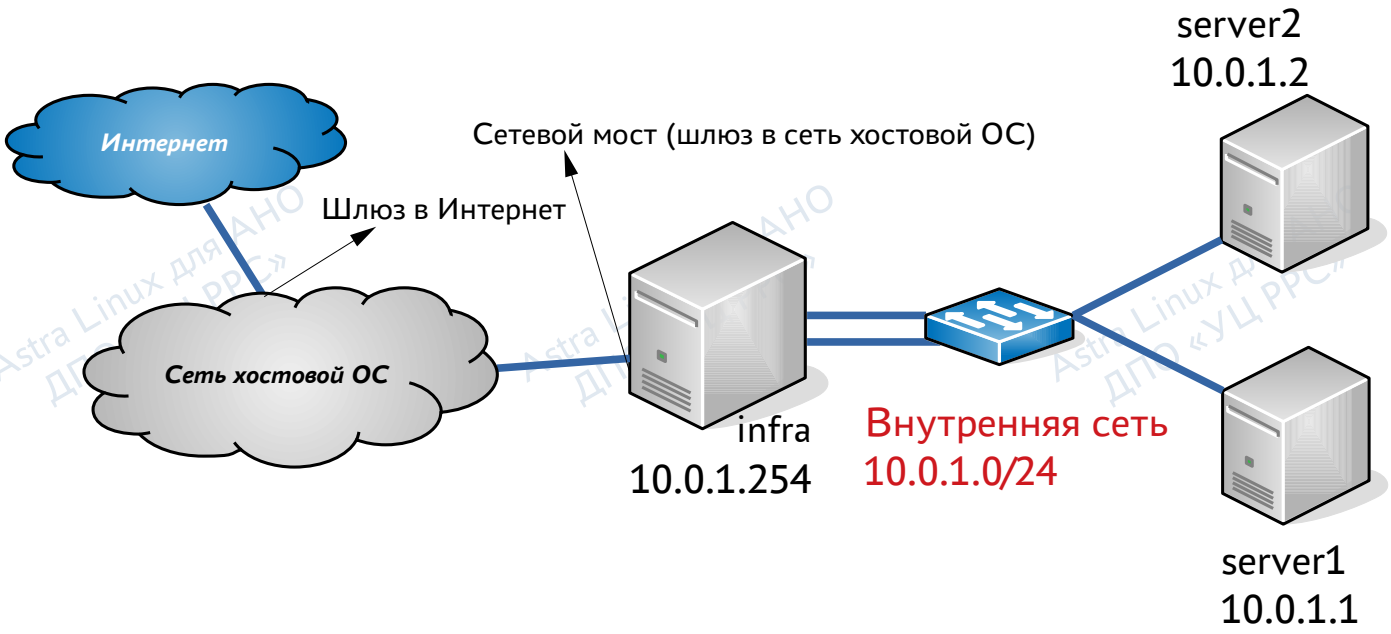
1 Удалить службу ntpd.
2 Настроить синхронизацию времени для ВМ server1, используя встроенную в systemd NTP службу. Источник времени — infra.

Модуль 8. Управление конфигурациями с помощью Ansible

Описание практического задания

- Установка Ansible.
- Создание инвентаризационного файла.
- Использование ansible в командной строке.
- Автоматизация установки и настройки веб-сервера Apache.

Схема сети



Установка ansible, использование ansible в командной строке и создание файла инвентаризации

1 Установить ansible на ВМ infra.

2 Настроить на ВМ infra SSH-аутентификацию по ключам с хостами server1 и server2.
Примечание: это должно было сделано ранее в Модуле 2 «Настройка удаленного доступа».

3 Дальнейшие действия осуществлять под учетной записью администратора системы (sa).

4 Создать в домашнем каталоге подкаталог ansible и перейти в него. Дальнейшие действия осуществлять в созданном каталоге.

5 Создать файл hosts, в который добавить:

- записи для хостов server1, server2 и infra;
- группу servers для хостов server1 и server2;
- переменные ansible_host для каждого хоста.

6 Настроить так, чтобы созданный файл инвентаризации использовался в командах и Ansible по умолчанию. Создать и поместить настройки в файл ~/.ansible.cfg.

7 Получить информацию («факты») о хосте server1 с помощью команды ansible и узнать объем RAM на этом хосте.

8 С помощью команды ansible получить значения текущих дат и времени на server1 и server2.

9 (Дополнительное задание) Изменить информацию в файлах /etc/hosts, используя команду ansible:

- Просмотреть содержимое файлов /etc/hosts.
- Заменить строки вида:
  IP_адрес имя_хоста
  на
  IP_адрес имя_хоста.astra.test имя_хоста.
  Использовать модуль replace.
- Проверить новое содержимое файлов /etc/hosts.

Установка, запуск и проверка работоспособности веб-сервера apache на хостах из группы servers

1 Создать плейбук apache.yml, в который включить следующие задания (tasks):

- Установить последнею версии Apache. Обновить кэш репозитория, если кэш не обновлялся больше часа (модуль apt).
- Копировать файлы index.html на продуктивный веб-сервер server1 и на тестовый веб-сервер server2:
  - создать два index-prod.html и index-test.html для продуктивного веб сервера server1 и тестового веб сервера server2, соответственно, следующего содержания (точки заменить на текст, в котором упоминается информация о типе веб-сервера):

```
<body>
 <h1> .....</h1>
</body>
```

- Файлы разместить в подкаталоге files, предварительно создав этот каталог.
- С помощью модуля copy настроить копирование этих файлов в каталог /var/www/html на оба сервера под именами index.html. Примечание: использовать переменную для хостов, задать этой переменной разные значения для разных серверов (prod для server1 и test для server2) и сформировать имена файлов-источников с использованием значений этой переменной.

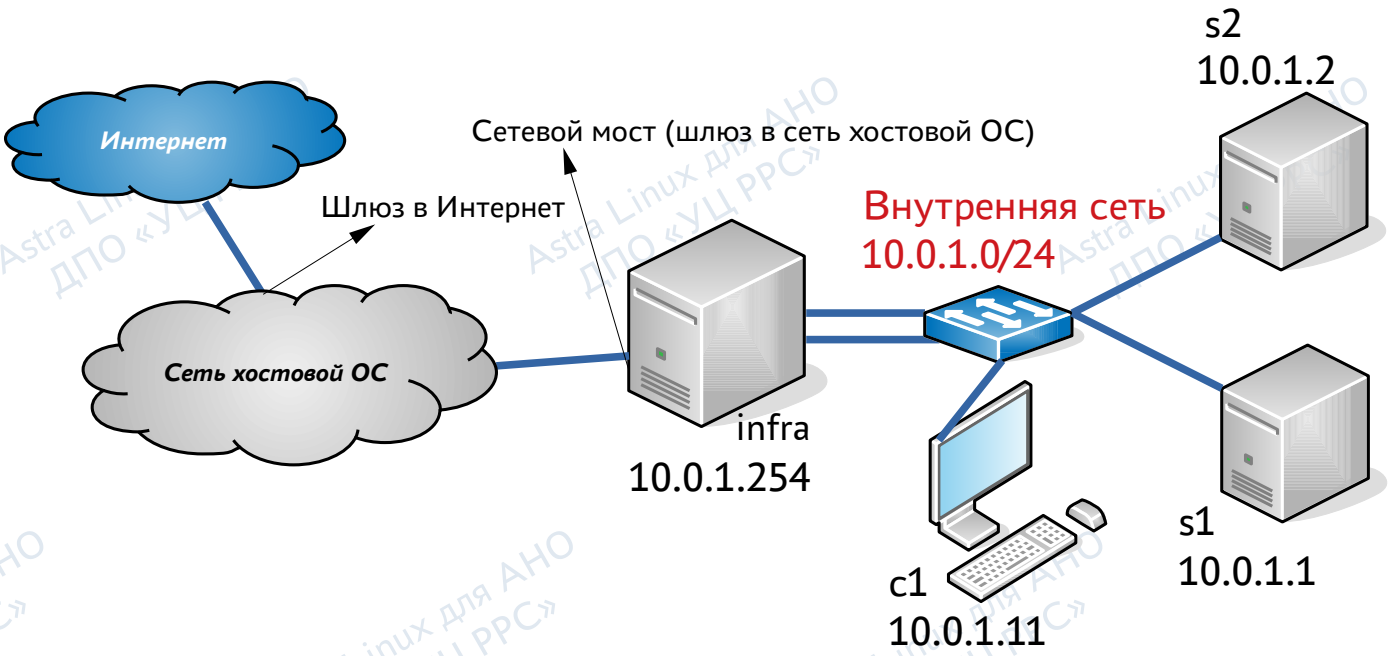
- Отключить параметр AstraMode в Apache (файл /etc/apache2/apache2.conf). Вставить строку
  AstraMode off
  после
  # AstraMode on
- Перезапустить службу apache2 на обоих серверах. Сделать так, чтобы служба Apache2 автоматически запускался при загрузке обоих серверов.
- Проверить содержимое стартовых страниц веб-серверов (index.html).
- Использовать модуль uri с параметром return_content=yes.
- С помощью register поместить веб-страницу в переменную и вывести ее на экран с помощью модуля debug.

Модуль 9. Служба каталогов на базе решения FreeIPA

Описание практического задания

- Установка и запуск сервера FreeIPA.
- Установка клиента FreeIPA и ввод клиента в домен.
- Управление доменными учетными записями.
- Управление доступом на базе узла.
- Регистрация сетевых служб в домене FreeIPA на примере прокси-сервера SQUID.
- Установка и запуск реплики FreeIPA.

Схема сети



Установка сервера

1 Остановить ВМ server1, server2, client1. В дальнейших заданиях эти ВМ не используются.

2 ВМ infra используется в задании по настройке FreeIPA и в дальнейших заданиях.

3 Создать ВМ s1 путем клонирования ВМ template_1604. Увеличить количество процессоров до 3х. Увеличить объем RAM до 3ГБ. Сетевая карта - одна, подключена к внутренней сети. Запустить ВМ.

4 Изменить имя хоста на s1.astra.test.

5 Настроить сетевой интерфейс через Network Manager (IP — 10.0.1.1/24; DNS сервер — localhost, шлюз — 10.0.1.254):

6 Добавить в /etc/hosts запись о s1.astra.test:

```
127.0.0.1 localhost localhost.localdomain
10.0.1.1 s1.astra.test s1
```

7 Проверить доступность ВМ infra.

8 Подключить репозитории. В файле /etc/apt/sources.list должно быть:

```
deb file:///srv/ftp/pub/1.7.1-main 1.7_x86-64 contrib main non-free
deb file:///srv/ftp/pub/1.7.1-base 1.7_x86-64 contrib main non-free
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-
extended/ 1.7_x86-64 main contrib non-free
```

9 Либо воспользоваться репозиторием в сети Интернет:

```
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-main/
1.7_x86-64 main contrib non-free

deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-
update/ 1.7_x86-64 main contrib non-free

deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-base/
1.7_x86-64 main contrib non-free

deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-
extended/ 1.7_x86-64 main contrib non-free
```

10 Обновить кэш с метаданными репозиториев.

11 Установить серверное программное обеспечение FreeIPA.

12 Установить клиентское программное обеспечение FreeIPA.

13 Запустить сервер FreeIPA (все по умолчанию и задать пароль для доменной учетной записи admin).

14 Проверить статус служб FreeIPA командой ipactl.

15 Проверить доступность административной веб-консоли FreeIPA через браузер Firefox (пользователь: admin, пароль был введен во время запуска сервера FreeIPA)
https://s1.astra.test

16 Запустить службу ssh и включить службу ssh в автозагрузку.

Установка клиента и ввод клиента в домен

1 Создать ВМ c1 путем клонирования template_1604 и запустить ее.

2 Задать имя хоста c1.astra.test.

3 Настроить сетевой интерфейс (IP адрес 10.0.1.11/24; dns сервер — s1.astra.test, шлюз — 10.0.1.254).

4 Проверить доступность сервера FreeIPA s1.astra.test.

5 Настроить доступ к репозиториям, скопировав файл sources.list с сервера FreeIPA s1.astra.test.

6 Обновить кэш с метаданными репозиториев.

7 Установить пакет dnsutils.

8 Проверить разрешение имени сервера в DNS.

9 Внести изменения в файл /etc/hosts:
```
127.0.0.1       localhost
10.0.1.11       c1.astra.test c1
```

10 Установить клиент FreeIPA.

11 Запустить клиент FreeIPA.

12 Перезагрузить хост c1.astra.test.

13 На сервере FreeIPA s1.astra.test проверить, что хост c1.astra.test добавлен в домен.

Управление учетными записями

1 Создать учетную запись доменного пользователя ipauser1 из веб-консоли https://s1.astra.test (мин. уровень конфиденциальности — 0, макс. — 1):

- Идентификация→Пользователи→+Добавить (заполнить обязательный поля и задать пароль).
- Щелкнуть по имени добавленной учетной записи.
- В Параметрах идентификации задать минимальный (0) и максимальные уровни конфиденциальности (1).

2 Создать учетную запись пользователя ipauser2 и задать пароль из командной строки с помощью утилиты ipa (мин. уровень конфиденциальности — 0, макс. — 2).

3 На клиенте c1.astra.test зайдите под учетными записями ipauser1 и ipauser2 с разными уровнями конфиденциальности.

Управление доступом на основе узла

1 Выполняется с помощью утилиты ipa в командной строке на сервере FreeIPA s1.astra.test. (может быть также выполнено в веб-консоли).

2 Просмотреть информацию о всех настроенных службах из командной строки и проверить, есть ли в списке служба fly-dm.

3 Создать правило, которое разрешает доменному пользователю ipauser2 графический вход в систему на хосте c1.astra.test:

- На сервере FreeIPA добавить службу fly-dm.
- Создать «пустое» правило с именем flydm.
- Добавить в правило flydm учетную запись пользователя ipauser2.
- Добавить в правило flydm хост c1.astra.test.
- Добавить в правило flydm службу fly-dm.

4 Просмотреть правило flydm.

5 Протестировать правило flydm для пользователей ipauser1 и ipauser2 с помощью утилиты ipa hbactest.

6 Отключить правило allow_all и снова протестировать правило flydm.

7 Зайти под учетными записями ipauser1 и ipauser2 на хостах s1.astra.test и c1.astra.test через графический вход.

8 Попробуйте зайти пользователем ipauser2 в c1.astra.test через виртуальный терминал.

9 Включите правило allow_all.

Регистрация сетевых служб во FreeIPA (SQUID)

1 Настроить перенаправление DNS запросов с сервера FreeIPA s1.astra.test на кэширующий «пограничный» DNS сервер infra:

- Перейти в веб-консоль https://s1.astra.test.
- Выбрать Сетевые службы→DNS→Глобальная конфигурация DNS→Глобальные перенаправители→ввести 10.0.1.254->Сохранить.

2 На ВМ infra выполнить следующее:

- Изменить имя хоста.
- Внести изменения в /etc/hosts:
  127.0.0.1 localhost
  10.0.1.254 infra.astra.test infra

- Установить на обоих сетевых интерфейсах BM infra (net1, bond-bond0) в качестве DNS сервера 10.0.1.1 (s1.astra.test).
- На кэширующем DNS сервере (BM infra) перенаправить запросы на внешний DNS (в случае, если запросы кэширующего сервера в Интернет заблокированы). Внести соответствующие изменения в файле /etc/bind/named.conf.options:
- Убедиться, что разрешаются как внешние DNS имена, так и имена в домене astra.test.
- Проверить, что по умолчанию вызывается python 2.7 (если не так, то переопределить символическую ссылку /usr/bin/python).
- Установить клиент FreeIPA.
- Запустить клиент FreeIPA (ввести хост infra в домен astra.test).

3 На контроллере FreeIPA s1.astra.test выполнить следующее:

- Проверить, что хост infra введен в домен astra.test.
- Зарегистрировать службу squid в домене.

4 На прокси-сервере infra.astra.test выполнить следующие действия (SQUID должен был установлен в предыдущей практической работе Модуль 5 «Прокси-сервер SQUID»):

- Создать файл /etc/squid/krb5.keytab с ключом для службы squid.
- Назначить на файл /etc/squid/krb5.keytab владельца proxy и группу-владельца proxy, задать права доступа 640.
- Внести информацию о keytab-файле в сценарий, запускающий службу SQUID. Для этого в файл /etc/init.d/squid добавить строки после DESC="Squid HTTP Proxy":
  KRB5_KTNAME=/etc/squid/krb5.keytab
  export KRB5_KTNAME
- В файле /etc/squid/squid.conf настроить аутентификацию SQUID через Kerberos:
  - Закомментировать строки, содержащие разрешающие правила для localnet.
  - Закомментировать или удалить строки с настройками других видов аутентификации (например, аутентификации NCSA, которая настраивалась в предыдущей практической работе Модуль 5 «Прокси-сервер SQUID»).

- Перед последним правилом http_access deny all добавить строки, которые разрешают использовать SQUID только доменным пользователям (настроить аутентификацию SQUID через Kerberos).
- Перезапустить systemd и службу squid (может занять продолжительное время) и убедиться, что служба squid была запущена успешно.

5 На хосте c1.astra.test выполнить следующие действия:

- Зайти администратором (под локальной учетной записью sa).
- Проверить, что внешние DNS имена и имена из домена astra.test разрешаются.
- В браузере Firefox настроить прокси для доступа в Интернет (ручная настройка прокси): infra.astra.test, порт 3128, установить параметр «Также использовать этот прокси для FTP и HTTPS».
- В адресной строке браузер Firefox ввести www.astralinux.ru и зайти на сайт. Можно одновременно на хосте infra.astra.test ввести команду tail -f /var/log/squid/access.log
  и отслеживать процесс обращения к Интернет-ресурсам через прокси.
- Зайти под доменной учетной записью ipauser1 с нулевым уровнем конфиденциальности.
- Настроить в браузере Firefox прокси и зайти на сайт www.astralinux.ru. На хосте infra.astra.test проверить поступающую в файл /var/log/squid/access.log информацию.

Установка реплики FreeIPA

1 Создать новую ВМ s2 с помощью клонирования template_1604. Увеличить количество процессоров до 3х. Увеличить объем RAM до 3ГБ. Сетевая карта - одна, подключена к внутренней сети. Запустить ВМ.

2 Изменить имя хоста на s2.astra.test.

3 Настроить сетевой интерфейс через Network Manager (IP - 10.0.1.2/24; DNS сервер - 10.0.1.1 (s1.astra.test), шлюз - 10.0.1.254).

4 Добавить в /etc/hosts запись о s1.astra.test.

5 Проверить доступность ВМ s1.astra.test.

6 Настроить доступ к репозиториям, скопировав файл sources.list с сервера FreeIPA s1.astra.test.

7 Обновить кэш с метаданными репозиториев.

8 Установить пакет dnsutils.

9 Проверить разрешение имени сервера s1.astra.test в DNS.

10 Установить клиент FreeIPA.

11 Запустить клиент FreeIPA.

12 Перезагрузить хост s2.astra.test.

13 На сервере FreeIPA s1.astra.test проверить, что хост s2.astra.test добавлен в домен.

14 На хосте s2.astra.test запустить службу ssh:

sudo systemctl start ssh

15 На сервере FreeIPA s1.astra.test с помощью утилиты astra-freeipa-server-crt создать сертификат для s2.astra.test и передать его на s2.astra.test.

16 На сервере FreeIPA s1.astra.test создать PTR запись для s2.astra.test, или из веб-консоли, или с помощью команды ipa dnsrecord-add.

17 На хосте s2.astra.test установить серверное программное обеспечение FreeIPA.

18 На хосте s2.astra.test запустить реплику FreeIPA, указав имя файла с сертификатом.

19 На s2.astra.test изменить DNS сервер на 127.0.0.1:

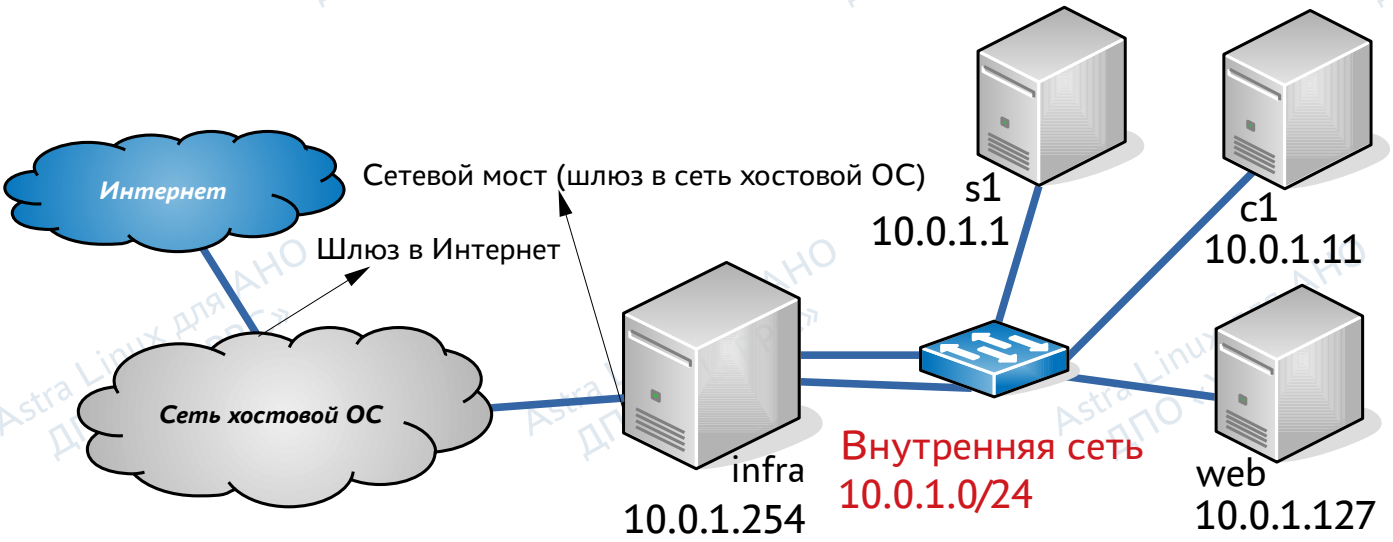
20 На s2.astra.test проверить, что реплика работает путем выполнения команды ipactl status
и входа в администраторскую веб-консоль hhtps://s2.astra.test (IPA-сервер→Топология→IPA-сервер, IPA-сервер→Топология→Topology Graph).

Модуль 10. Веб-сервер на основе Apache

Описание практического задания

- Установка веб-сервера «доступного из Интернет» на виртуальной машине (ВМ) infra.
- Установка веб-сервера для локального доступа на ВМ server1.
- Настройка авторизации с применением FreeIPA.
- Работа со страницами с мандатными метками.

Схема сети



Настройка Apache2 на ВМ infra

1 Установить apache2 на ВМ infra.

2 Выключить режим AstraMode в /etc/apache2/apache2.conf.

3 Создать /etc/apache2/conf-available/fqdn.conf с содержимым:

ServerName localhost

4 Активировать конфигурационный файл fqdn, перечитать конфигурацию веб-сервера и проверить его состояние.

5 Создать файл конфигурации виртуального хоста в /etc/apache2/sites-available.

6 Отредактировать файл конфигурации виртуального хоста, указав доменное имя сервера в параметре ServerName и путь к каталогу с веб-страницами.

7 Создать каталог для размещения веб-страниц.

8 Разместить в созданном каталоге веб-страницу index.html, например, со следующим содержимым:

```
<html>
<head>
<title>Welcome to infra</title>
</head>
<body>
<h1>Welcome to infra</h1>
<p>Hello!</p>
</body>
</html>
```

9 Активировать сайт, описанный в конфигурации виртуального хоста, и перечитать конфигурацию веб-сервера.

10 Проверить созданную страницу в браузере.

11 Установить php7.0 в качестве модуля Apache2.

12 Проверить версию php:

```
php -v
```

13 Создать в каталоге виртуального хоста файл info.php с содержимым:

```
<?php
phpinfo();
?>
```

14 Проверить отображение страницы, сгенерированной info.php в браузере.

Настройка самоподписанных сертификатов

1 Создать удостоверяющий центр – CA (Certification Authority):

```
cd /etc/apache2/
sudo mkdir ssl
sudo chmod 700 ssl
cd ssl
sudo openssl genrsa -des3 -out my-ca.key
```

2 Создать сертификат для удостоверяющего центра:

```
sudo openssl req -new -x509 -days 3650 -sha256 \
```

-key my-ca.key -out my-ca.crt

3 В конфигурационном файле /etc/ssl/openssl.cnf найти и раскомментировать строку:
req_extensions = v3_req

4 В секции [v3_req] после строк:

basicConstraints = CA:FALSE

keyUsage = nonRepudiation, digitalSignature, keyEncipherment

следует добавить строку:
`subjectAltName = @alt_names`
после которой создать новую секцию [alt_names].

5 В новую секцию [alt_names] добавить строки вида DNS.X = домен, указав домены, для которых выпускается сертификат, где X=1,2,3 и т. д. Можно указать несколько доменов/поддоменов.

6 Создать файл ключа для веб-сервера:

sudo openssl genrsa -des3 -out my-apache.key 1024

7 Удалить пароль из файла ключа веб-сервера:

sudo openssl rsa -in my-apache.key -out new.my-apache.key
sudo mv new.my-apache.key my-apache.key

8 Создать запрос на подпись сертификата Certificate Signature Request (csr) в удостоверяющем центре:

openssl req -new -key my-apache.key -out my-apache.csr

9 Подписать сертификат Apache в удостоверяющем центре:

sudo openssl x509 -req -in my-apache.csr \
-out my-apache.crt -sha256 -CA my-ca.crt \
-CAkey my-ca.key -CAcreateserial -days 366

10 Назначить права только на чтение только для владельца на файлы ключей.

11 Отредактировать файл default-ssl.conf:
```
SSLCertificateFile /etc/apache2/ssl/my-apache.crt
SSLCertificateKeyFile /etc/apache2/ssl/my-apache.key
SSLCACertificateFile /etc/apache2/ssl/my-ca.crt
```

12 Включить mod_ssl.

13 Перезапустить веб-сервер.

14 Проверить работы – зайти в браузере на сайт с использованием https.

Настройка ВМ web

1. Клонировать ВМ template_1604 и назвать новую виртуалку web.
2. Запустить виртуалку.
3. Сменить имя хоста на web.
4. Поправить /etc/hosts, добавив соответствие доменного имени машины и ее IP-адреса.
5. Остановить и запретить запуск Network Manager.
6. Настроить сетевой интерфейс eth0 с IP-адресом 10.0.1.127 в файле /etc/network/interfaces.
7. Указать IP-адрес DNS-сервера 10.0.1.1 в файле /etc/resolv.conf.
8. Перезапустить службу и проверить настройки и доступность шлюза.
9. Скопировать эталонный sources.list в /etc/apt/sources.list с ВМ infra.
10. Обновить локальный кэш с метаданными репозиториев.
11. Установить клиент FreeIPA.
12. Ввести ВМ web в домен.
13. Перезапустить ВМ web.
14. Проверить из графического интерфейса администратора или в терминале на контроллере домена s1.

Настройка Kerberos авторизации веб-сервера Apache в домене FreeIPA

1. На ВМ web установить apache2 и модуль авторизации через Kerberos.
2. На контроллере домена s1 зарегистрировать веб-службу web.
3. В ВМ web создать ключи и сохранить их в файле /etc/apache2/keytab.
4. Установить права и владельца на файл keytab.
5. Настроить Kerberos авторизацию на веб-сервере, включив секцию <Directory> в настройку виртуального хоста.
6. Перезапустить веб-сервер.

Создание страниц с разными уровнями конфиденциальности на ВМ web

1. Зайти на ВМ web.

2 Установить на каталоги /var/www, /var/www/html атрибут ccnr и уровень конфиденциальности 2.

3 Перейти в каталог /var/www/html.

4 Создать файлы для проверки доступа на уровнях конфиденциальности 1 и 2 с названиями level1.html и level2.html с содержимым, явно указывающим на уровень конфиденциальности файла (например, выводящих текст Level1 и Level2).

5 Назначить созданным файлам соответствующие уровни конфиденциальности.

6 Изменить владельца и группу-владельца файлов .html на www-data.

```
sudo chown www-data:www-data *.html
```

Настройка клиента для работы с локальным веб-сервером Apache2

1 Зайти на c1 по очереди: локальным пользователем sa, пользователями в домене eudser1, eduser2 (с уровнями конфиденциальности 0,1,2).

2 Настроить поддержку Kerberos авторизации в Firefox:

- в адресной строке набрать about:config;
- найти параметры, содержащие negotiate;
- параметрам network.negotiate-auth.delegation-uris и network.negotiate-auth.trusted-uris задать значение http://, https://

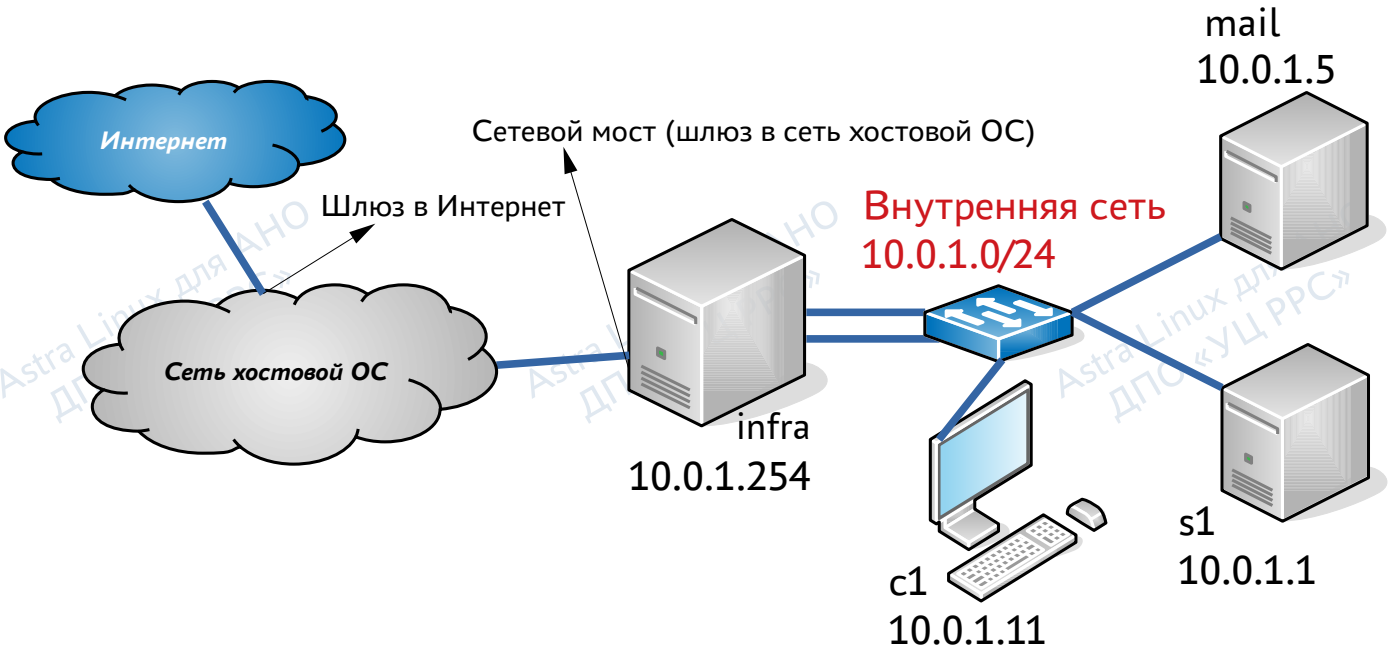
3 Зайти в браузере на страницы http://web.edu.test, http://web.edu.test/level1.html, http://web.edu.test/level2.html. Сравнить результаты при входе разными пользователями с разными уровнями конфиденциальности.

Модуль 11. Система электронной почты на базе Exim и Dovecot

Описание практического задания

- Установка и первоначальная настройка защищенного программного почтового комплекса.
- Настройка аутентификации почтовых служб через Kerberos.
- Настройка почтового клиента Thunderbird.

Схема сети



Создание и настройка ВМ для почтового сервера

1 Создать ВМ mail путем клонирования ВМ template_1604. Запустить ВМ и зайти под учетной записью локального администратора (sa).

2 Изменить имя хоста на mail.astra.test:

3 Настроить сетевой интерфейс через Network Manager (IP — 10.0.1.5/24; DNS сервер — s1.astra.test (10.0.1.1), шлюз — 10.0.1.254).

4 Проверить доступность сервера FreeIPA s1.astra.test.

5 Настроить доступ к репозиториям: скопировать файл sources.list с сервера FreeIPA s1.astra.test.

6 Обновить кэш с метаданными репозиториев.

7 Установить пакет dnsutils.

8 Проверить разрешение имени сервера в DNS.

9 Внести изменения в файл /etc/hosts:
```
127.0.0.1       localhost
10.0.1.5        mail.astra.test mail
```

10 Установить клиент FreeIPA.

11 Запустить клиент FreeIPA.

12 Перезагрузить mail.astra.test.

13 На сервере FreeIPA s1.astra.test проверить, что хост mail.astra.test добавлен в домен.

Установка программного обеспечения и первоначальная настройка

1 На хосте mail.astra.test установить защищенный комплекс программ электронной почты.

2 Произвести первоначальную настройку exim4.

3 Ввести следующие ответы на вопросы во время первоначальной настройки (результаты запомнятся в файле /etc/exim4/update-exim4.conf.conf):

- Тип почтовой конфигурации: **Интернет сайт; ...**
- Почтовое имя системы: **astra.test**
- IP адреса, с которых ожидаются входящие SMTP соединения: **10.0.1.5**
- Места назначения, для которых должна приниматься почта: **astra.test**
- Домены для релейной передачи почты: **пусто**
- Хосты для релейной передачи почты: **пусто**
- Сокращать количество DNS-запросов: **нет**
- Метод доставки локальной почты: **Maildir формат в /var/mail**
- Разделить конфигурацию на маленькие файлы: **Да**

Настройка аутентификации СЭП через Kerberos

1 На контроллере домена зарегистрировать почтовые службы smtp (exim4) и imap (dovecot), которые будут работать на хосте mail.astra.test.

2 Используя веб-консоль freeIPA, добавить ресурсные записи DNS:

- MX запись для зоны astra.test, почтовый сервер mail.astra.test.

- PTR запись для хоста mail.astra.test.

3 На сервере mail.astra.test создать ключи для почтовых служб и добавить ключи в keytab-файл:

4 Используя списки управления доступом назначить право доступа x на каталог /var/lib/dovecot и право доступа r на keytab-файл для пользователя dovecot.

5 На почтовом сервере mail.astra.test настроить dovecot для обеспечения аутентификации через Kerberos:

- В файле /etc/dovecot/conf.d/10-auth.conf:
  - Раскомментировать строку:
    disable_plaintext_auth = yes
  - Раскомментировать строку и задать значение - имя почтового сервера:
    auth_gssapi_hostname = mail.astra.test
  - Раскомментировать строку и задать значение - абсолютное имя keytab-файла:
    auth_krb5_keytab = /var/lib/dovecot/dovecot.keytab
  - Изменить значение параметра на gssapi
    auth_mechanisms = gssapi
- В файле /etc/dovecot/conf.d/10-master.conf внутри секции service auth { ... } внести следующую подсекцию (exim будет использовать сокет службы dovecot для аутентификации через Kerberos - даем соответствующие права доступа):

```
unix_listener auth-client {
 mode = 0600
 user = Debian-exim
}
```

6 Перезапустить службу dovecot и проверить статус службы.

7 Настроить exim4 для аутентификации через Kerberos. На почтовом сервере mail.astra.test создать файл /etc/exim4/conf.d/auth/22_exim4-dovecot-kerberos-ipa со следующим содержимым:

```
dovecot_gssapi:
driver = dovecot
public_name = GSSAPI
server_socket = /var/run/dovecot/auth-client
server_set_id = $auth1
```

8 Перезапустить службу exim4 и проверить статус.

Настройка почтового клиента «Почта Thunderbird»

1 Зайти на хосте c1.astra.test под доменной учетной записью ipauser2 с разными уровнями конфиденциальности: 0, 1 и 2.

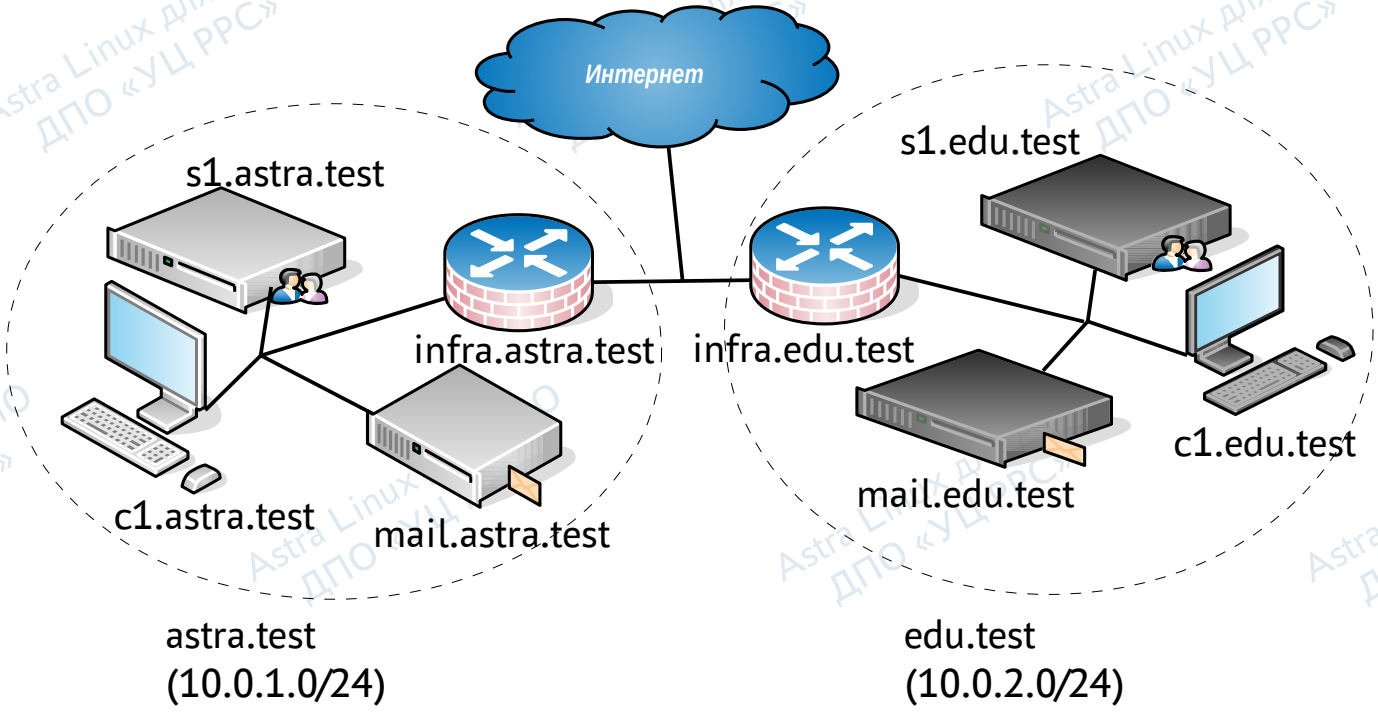
2 Настроить почтовый клиент «Почта Thunderbird» для учетной записи ipauser2 на каждом уровне конфиденциальности и отправить письма пользователю ipauser1.

3 Зайти на хосте c1.astra.test под доменной учетной записью ipauser1 с разными уровнями конфиденциальности: 0 и 1.

4 Настроить почтовый клиент «Почта Thunderbird» для учетной записи ipauser1 на каждом уровне конфиденциальности и прочитать полученные письма.

Настройка взаимодействия двух СЭП (опционально)

Схема стенда

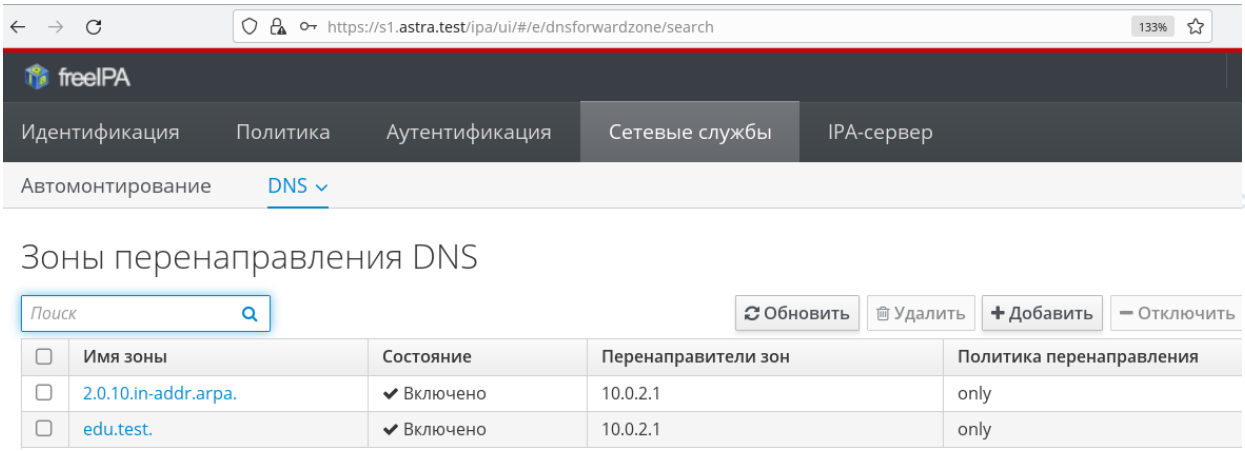


1 Данное задание предполагает, что:

- Имеется два набора по 4 виртуальных машины в каждой.
- В домене edu.test ВМ настроены аналогично, как и в astra.test.

- Между сетями 10.0.1.0/24 и 10.0.2.0/24 настроена маршрутизация. Статические маршруты определены на infra.astra.test и infra.edu.test.

2 На DNS сервере s1. astra.test (10.0.1.1) настроить перенаправление (forwarding) зон edu.test. и 2.0.10.in-addr.arpa. на DNS сервер s1.edu.test (10.0.2.1). Аналогичные действия сделать на DNS сервере s1.edu.test (10.0.2.1) для зон astra.test. и 1.0.10.in-addr.arpa. (воспользуйтесь веб-консолью freeIPA).



3 Проверить на mail.astra.test и mail.edu.test разрешаются ли ресурсные записи DNS типа MX для доменов astra.test и edu.test. Используйте команду nslookup или dig.

4 На mail.astra.test разрешить отправку почты (relay) в домен edu.test. Это можно сделать, установив параметр dc_relay_domains='edu.test' в файле /etc/exim4/update-exim4.conf.conf или с помощью dpkg-reconfigure exim4-config

5 Аналогичные действия произведите на mail.edu.test.

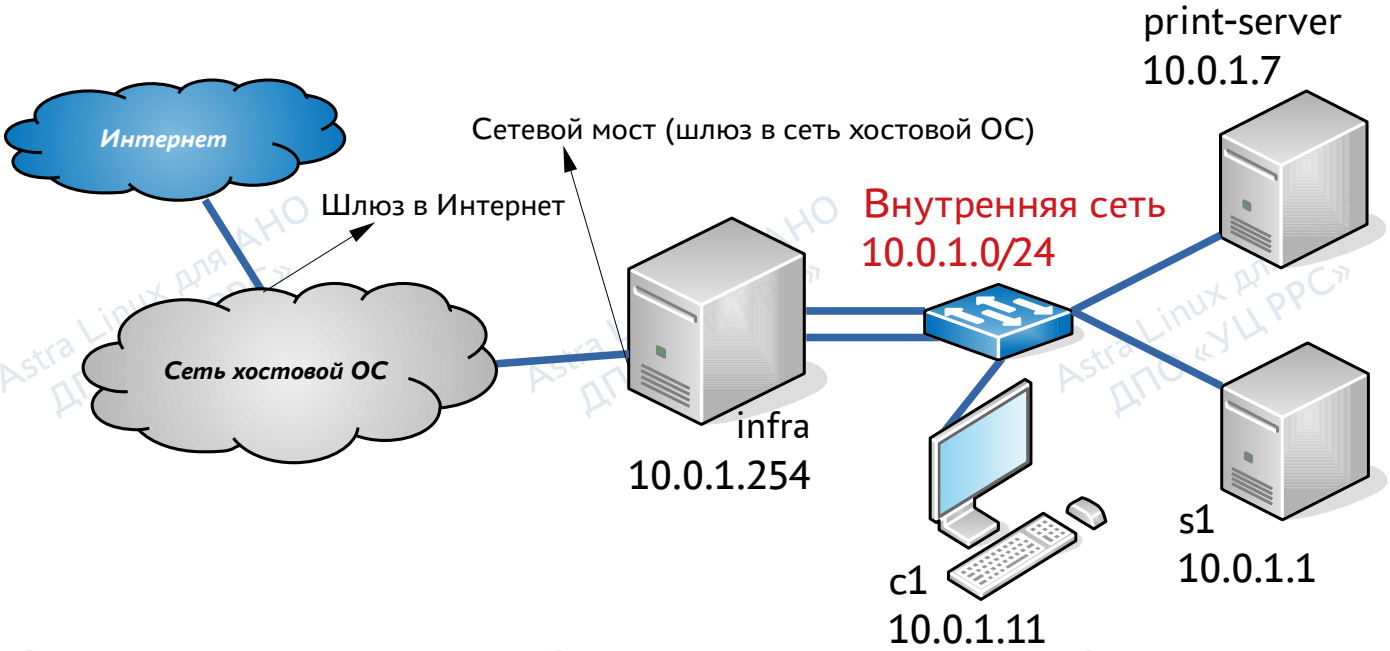
6 На c1.astra.test и c1.edu.test проверьте, что можно отправлять почтовые сообщения пользователям доменов astra.test и edu.test с различными мандатными уровнями.

Модуль 12. Защищенный комплекс программ для печати и маркировки документов

Описание практического задания

- Настройка сервера печати.
- Настройка клиента печати.
- Интеграция службы печати и FreeIPA.
- Маркировка документов.

Схема сети



Создание и настройка ВМ print-server

1 Создать ВМ print-server путем клонирования ВМ template_1604. Запустить ВМ и зайти под учетной записью локального администратора (sa).

2 Изменить имя хоста на print-server.astra.test:

3 Настроить сетевой интерфейс через Network Manager (IP — 10.0.1.7/24; DNS сервер — s1.astra.test (10.0.1.1), шлюз — 10.0.1.254):

4 Проверить доступность сервера FreeIPA s1.astra.test.

5 Внести изменения в файл /etc/hosts:
127.0.0.1 localhost
10.0.1.7 print-server.astra.test print-server

6 Настроить доступ к репозиториям: скопировать файл sources.list с сервера FreeIPA s1.astra.test.

7 Обновить кэш с метаданными репозиториев.

8 Установить пакет dnsutils.

9 Проверить разрешение имени сервера FreeIPA в DNS.

Установка драйвера принтера для печати в PDF-файл

Примечание: данный драйвер печати используется исключительно в целях демонстрации.

1 Настроить работу apt через прокси сервер. Внести изменения в файл /etc/apt/apt.conf.d/70debconf
Примечание: на прокси-сервере SQUID (ВМ infra) разрешить доступ всем хостам из сети 10.0.1.0/24. Раскомментировать список доступа localnet и разрешающее правило для localnet. Правило должно находиться до правила, разрешающего доступ только аутентифицированным в Kerberos пользователям.

2 Убедиться, что в /etc/apt/sources.list добавлен extended репозиторий (при необходимости добавить его):

```
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/ 1.7_x86-64 main contrib non-free
```

3 Обновить кэш репозиториев.

4 Установить программный пакет cups-pdf.

Настройка сервера печати и аутентификации службы печати

1 Установить на ВМ print-server клиента FreeIPA и ввести данных хост в домен FreeIPA.

2 Перезагрузить ВМ print-server.

3 На сервере FreeIPA (s1.astra.test) создать доменную учетную запись cups_admin (с помощью утилиты ipa или веб-консоли).

4 На сервере FreeIPA зарегистрировать службу печати cups, которая использует протокол IPP.

5 Зайти в ВМ print-server под учетной записью локального администратора (sa) создать в каталоге /tmp keytab-файл с ключом для службы CUPS.

6 С помощью утилиты ktutil перенести созданные ключи в файл /etc/krb5.keytab.

7 Включить доменного пользователя cups_admin в локальные группы lpadmin и lpmac и проверить успешность выполнения этих действий.

8 Разрешить службе CUPS принимать задания и команды с удаленных хостов, а также установить значение * для параметра ServerAlias и задать имя сервера печати в параметре ServerName.

9 Настроить аутентификацию службы CUPS через Kerberos. Внесите следующие изменения в настройки CUPS:
sudo cupsctl DefaultPolicy=parsec
sudo cupsctl MacEnable=On
sudo cupsctl DefaultAuthtype=Negotiate

10 В файле /etc/cups/cupsd.conf заменить строку
Port 631
на
Listen 0.0.0.0:631

11 Командой cupsctl параметр MarkerUser установить в значение ipp.

12 Создайте каталог /opt/cups-pdf.

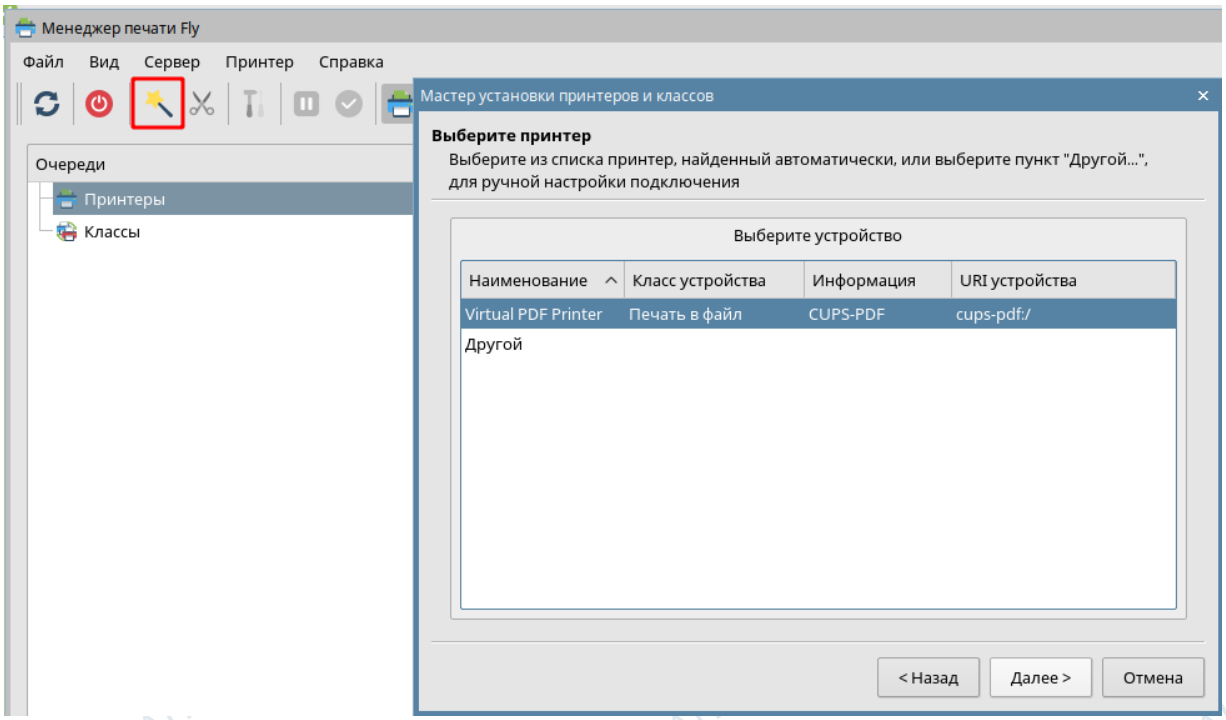
13 В файле /etc/cups/cups-pdf.conf изменить значения параметра Out (каталог, куда будут помещаться pdf файлы) на /opt/cups-pdf/${USER}.

14 Перезапустить службу CUPS.

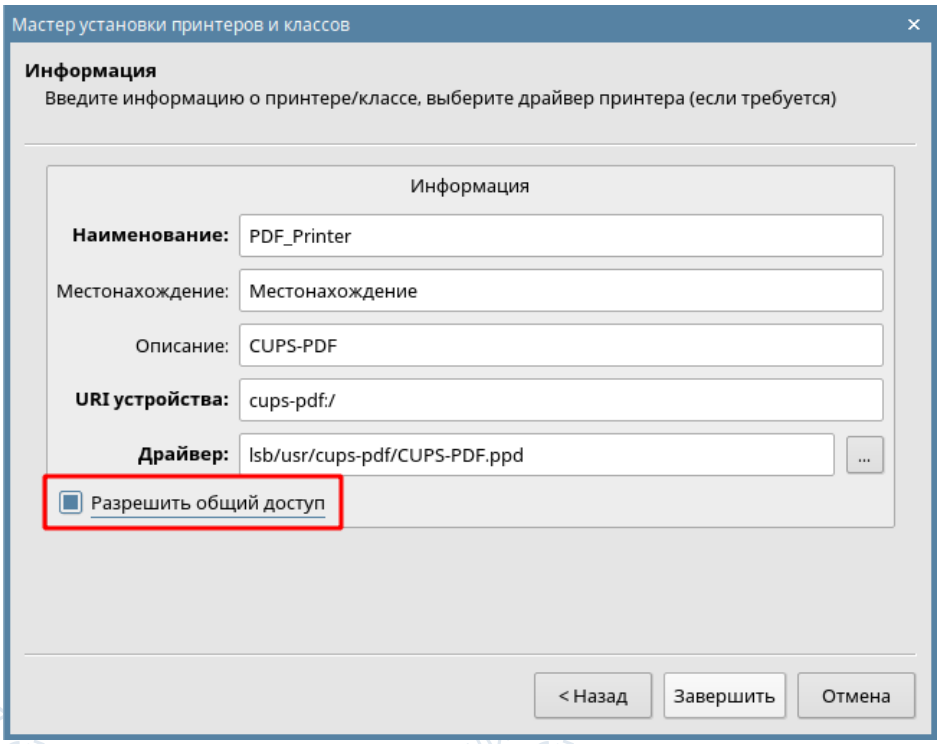
15 Зайти в ВМ print-server под доменной учетной записью cups_admin.

16 Вызвать «Менеджер печати Fly» командой fly-admin-printer.

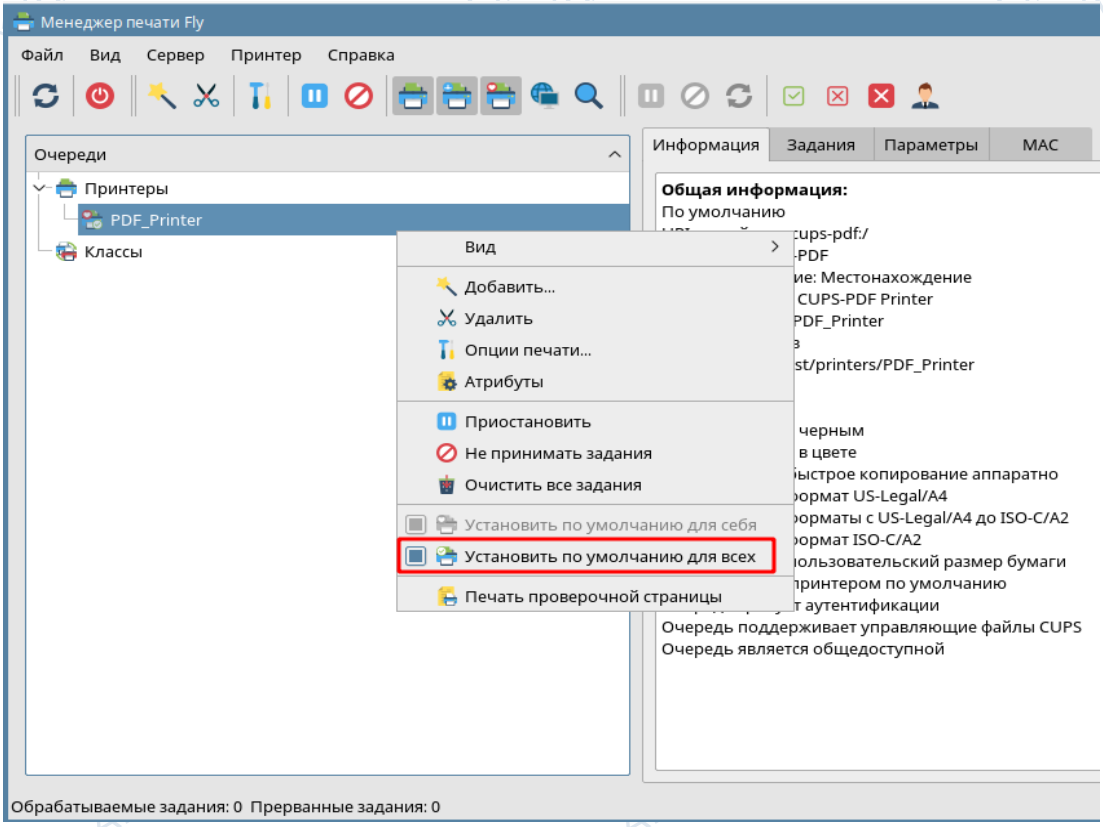
17 Нажать кнопку «Добавить ...» на панели инструментов. В появившемся окне «Мастера установки принтеров и классов» выбрать обнаруженный принтер и нажать кнопку «Далее».



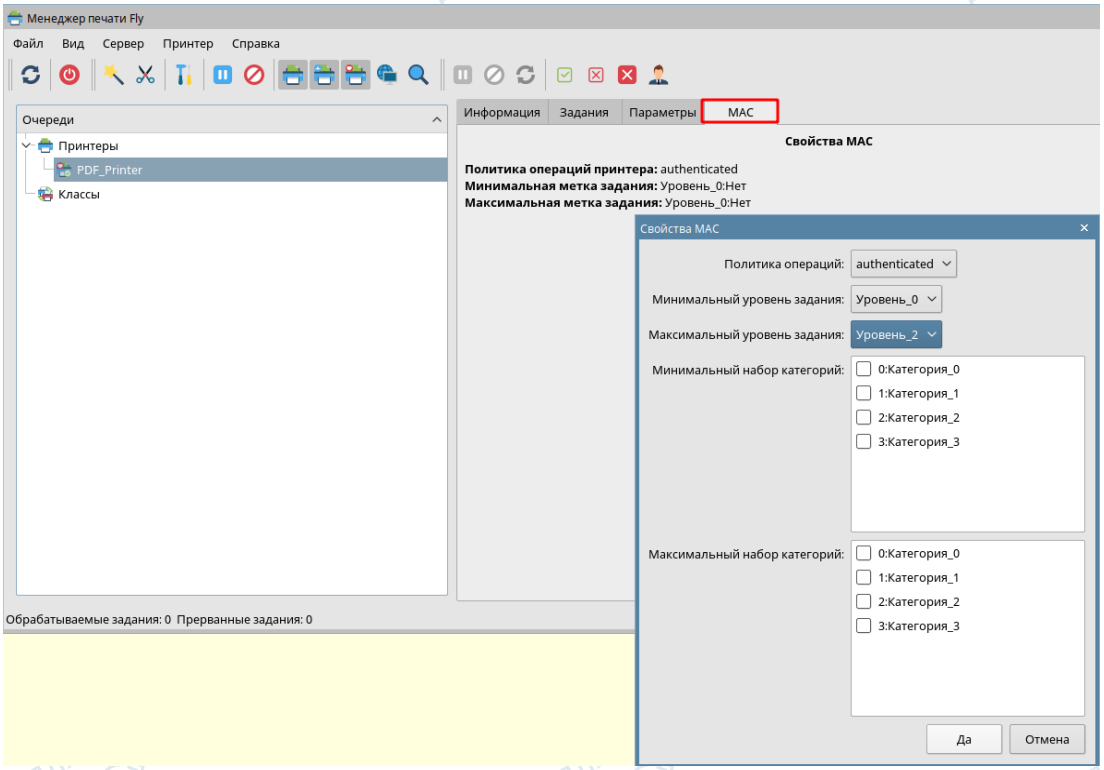
18 В следующем окне «Мастера установки принтеров и классов» установить параметр «Разрешить общий доступ». Также можно изменить название принтера (поле «Наименование»). Нажать кнопку «Завершить».



19 Назначить установленный принтер как принтер по умолчанию для всех.



20 На вкладке «MAC» ввести минимальную и максимальную метки для заданий. Установить минимальный уровень — 0, максимальный — 2.



21 В главном меню выбрать пункт «Принтер», в выпадающем меню выбрать пункт «Опции печати ...». В появившемся окне перейти на вкладку «Задания» и установить значение параметра «Политика операция» равным «parsec».

Настройка клиента службы печати, печать файлов

1 Зайти под учетной записью локального администратора (sa) на ВМ c1.astra.test.

2 В файле /etc/cups/client.conf определить параметр ServerName, присвоив значение равное DNS имени сервера печати.

3 В командной строке проверить доступность сетевого принтера.

4 С помощью утилиты командной строки отправить на печать файл /etc/cups/client.conf.

5 Зайти на ВМ c1.astra.test под доменной учетной записью пользователя ipauser1 с уровнем конфиденциальности 0.

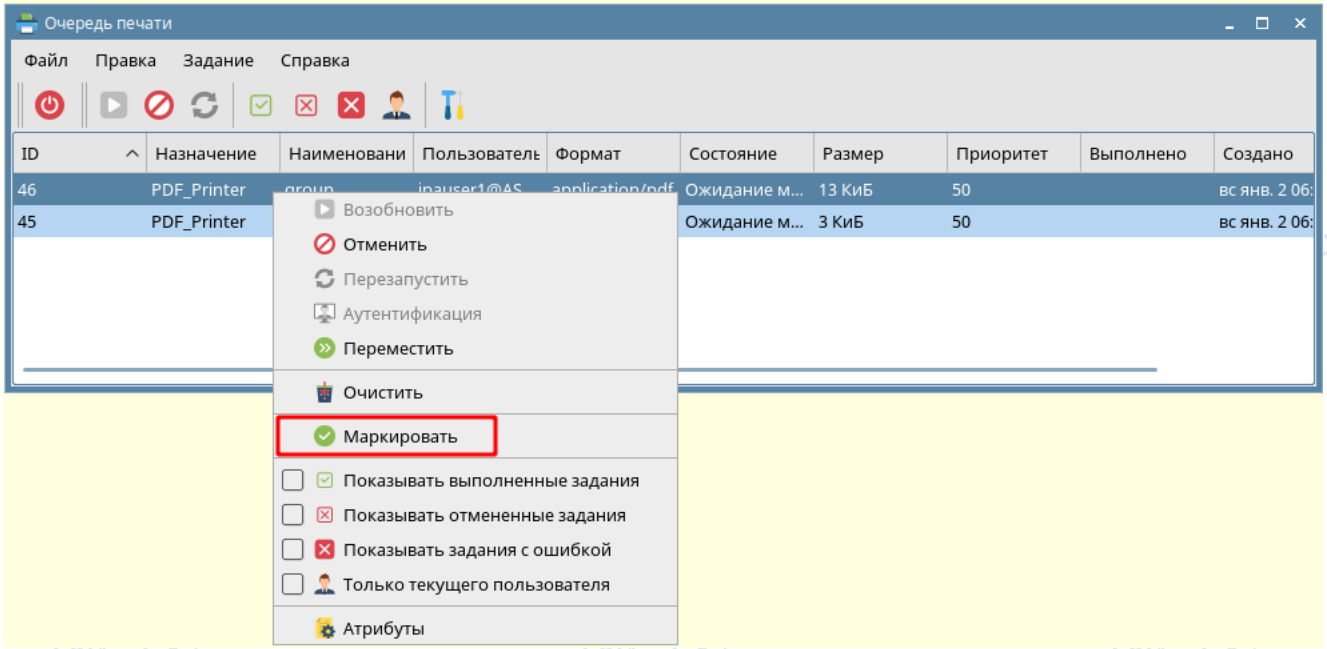
6 В редакторе kate открыть файл /etc/hosts и отправить его на печать.

7 Зайти на ВМ c1.astra.test под доменной учетной записью пользователя ipauser1 с уровнем конфиденциальности 1.

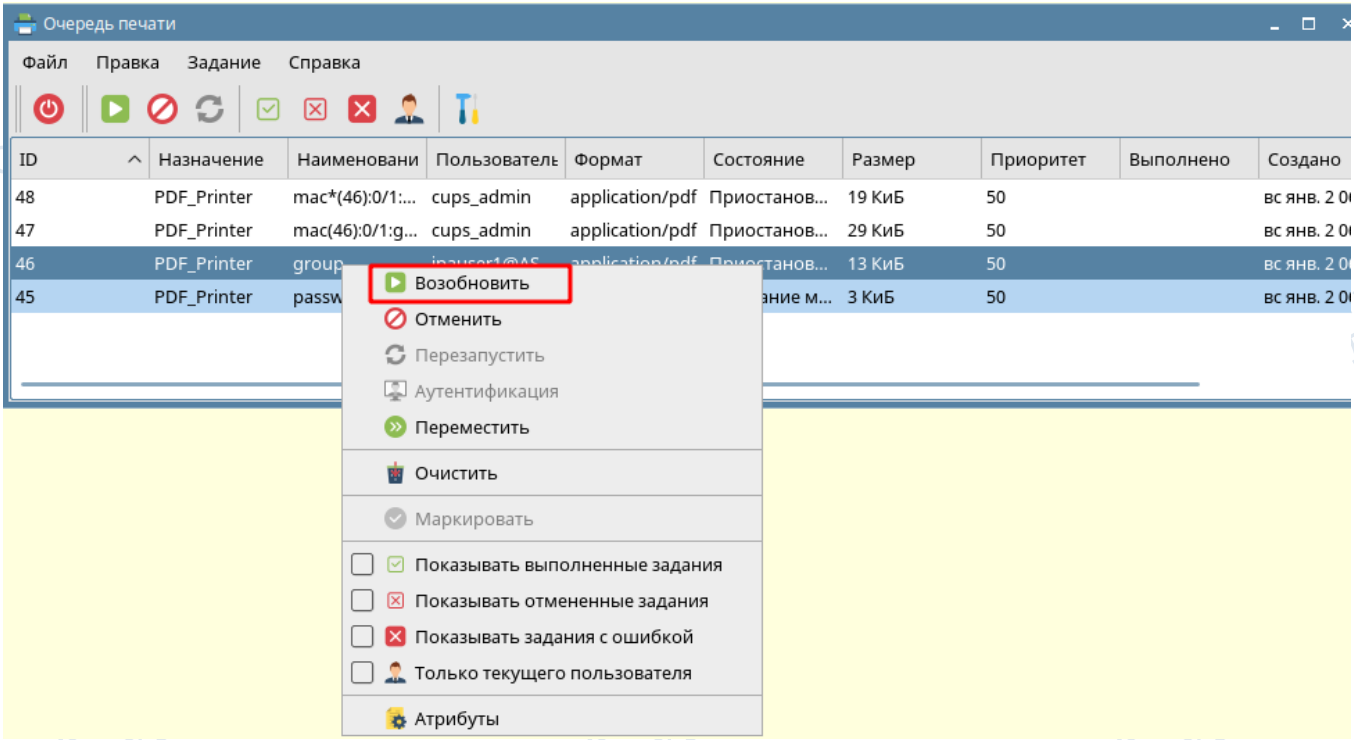
8 Напечатать с помощью утилиты командной строки файл /etc/passwd.

9 Открыть в редакторе kate файл /etc/group и отправить его на печать.

10 На ВМ print-server.astra.test под учетной записью cups_admin произвести маркировку с помощью утилиты fly-jobviewer.



11 После выполнения маркировки задания в контекстном меню задания выбрать пункт «Возобновить», чтобы распечатать документ.
Примечание: кроме основного задания маркировка создаст еще два дополнительных задания. Для возобновления печати следует выбрать основное задание.

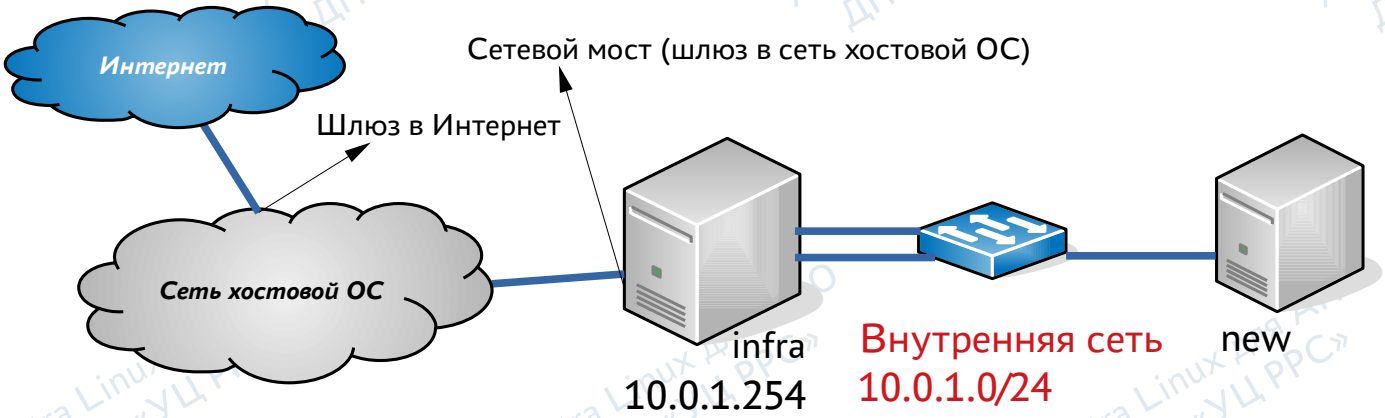


Модуль 13. Установка Astra Linux по сети

Описание практического задания

- Создание сетевого репозитория.
- Установка TFTP-сервера.
- Настройка DHCP-сервера.
- Выполнение автоматической удаленной установки.

Схема сети



Создание репозитория на ВМ infra

1 Предполагается, что веб-сервер Apache2 уже установлен. Режим AstraMode выключен.

2 Добавить строку в файл /etc/fstab для постоянного монтирования образа дистрибутива в /var/www/html/.

3 Выполнить монтирование до перезагрузки.

4 Установить TFTP-сервер.

5 Изменить параметр TFTP_OPTIONS в файле /etc/default/tftpd-hpa, добавив необходимые параметры.

6 Скопировать файлы, необходимые для сетевой установки, в каталог tftp.

7 Создать каталог для конфигурации `/srv/tftp/pxelinux.cfg`.

8 Создать файл `/srv/tftp/pxelinux.cfg/default`.

9 Файл /srv/tftp/pxelinux.cfg/default можно взять из статьи wiki.astralinux.ru «Установка ОС Astra Linux по сети» по адресу: https://wiki.astralinux.ru/pages/viewpage.action?pageId=3277939.

10 Указать в файле /srv/tftp/pxelinux.cfg/default корректные схему и адрес сервера — http://10.0.1.254.

11 В файле /etc/dhcp/dhcpd.conf добавить в раздел subnet параметр filename.

12 Перезапустить DHCP-сервер.

13 В каталоге /var/www/html создать файл с ответами для автоматической установки preseed.cfg .

14 Файл можно скачать по адресу https://wiki.astralinux.ru/download/attachments/68914051/preseed_smol.cfg?version=1&modificationDate=1581576351839&api=v2.

15 В файле preseed.cfg нужно указать имя протокола, адрес сервера и каталог, в котором находится дистрибутив.

16 Указать учетную запись пользователя sa и задать для него пароль.

17 Создать новую виртуальную машину new:

- Процессор — 1;
- RAM — 2 ГБ;
- Диск — 30 ГБ;
- Сетевой адаптер — внутренняя сеть;
- Операционную систему вручную не устанавливать, виртуальный компакт-диск в виртуальный привод не вставлять.

18 При запуске машины new следует выбрать установку по сети.
Примечание: для VirtualBox следует нажать F12 и появится меню. В меню выбираем загрузку по сети путем нажатия на клавишу l — LAN.

19 Установка будет выполнена автоматически. Если же возникнет ошибка, то это означает, что один из разобранных выше шагов был выполнен некорректно. Тогда следует вернуться, обнаружить и исправить ошибки.

20 В случае, если все было верно, установка будет произведена без участия человека, ВМ будет перезагружена, и будет открыто окно входа в систему.