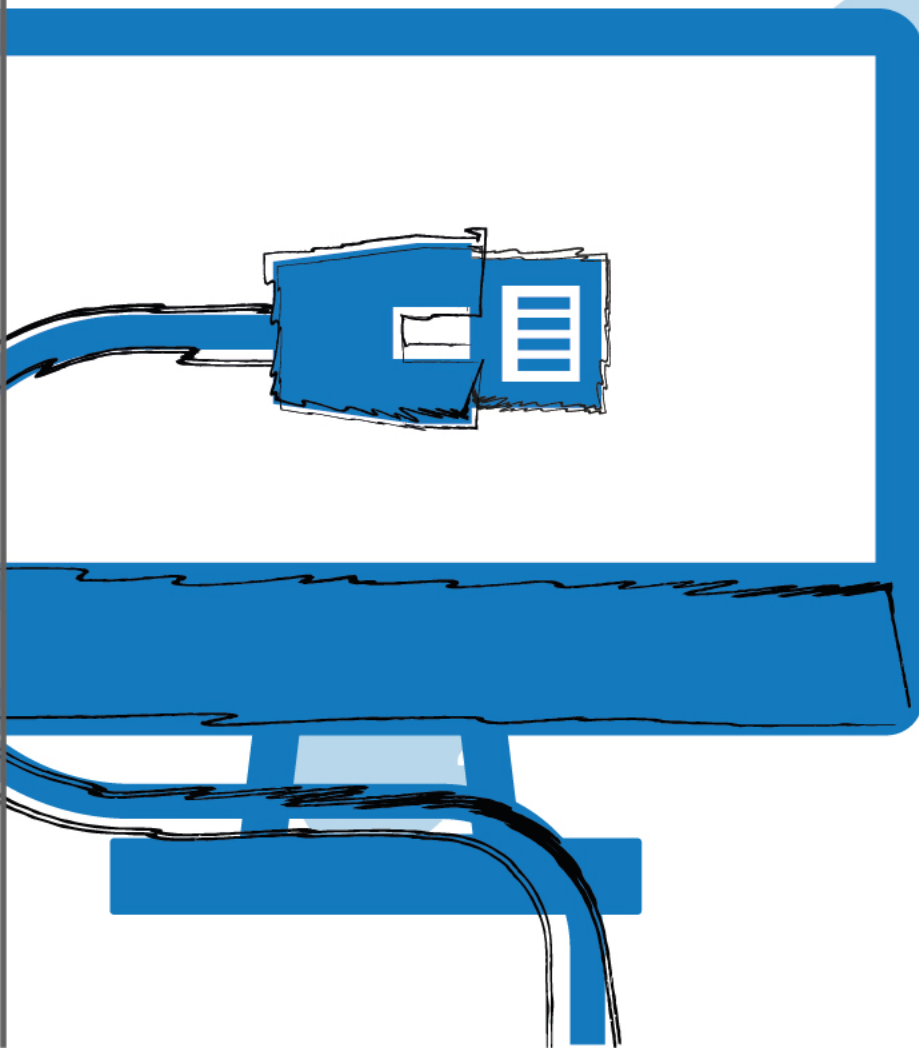




AL-1704

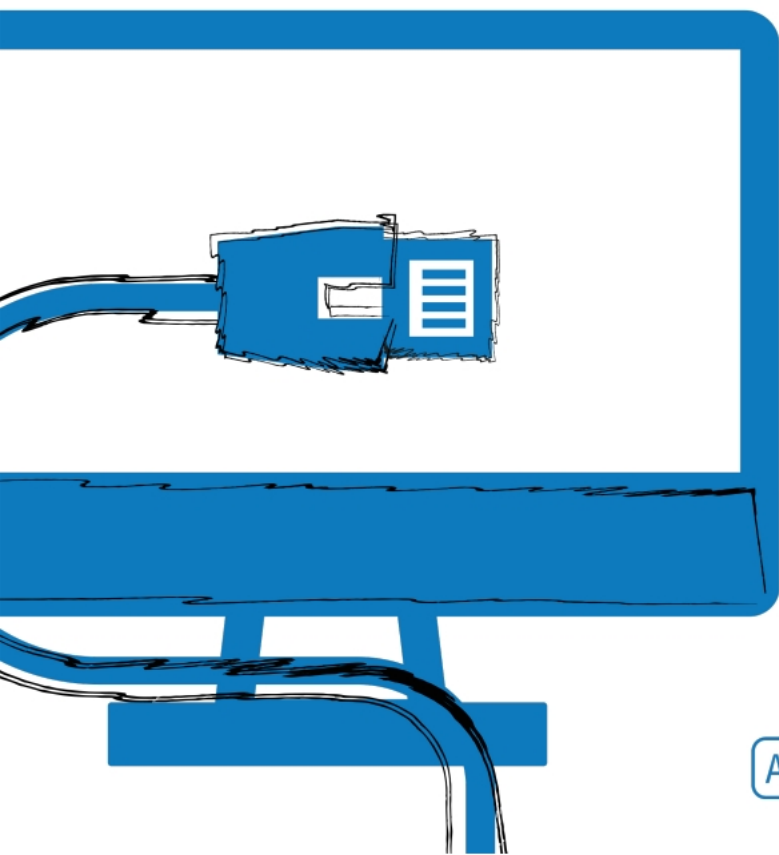
**Сборник
практических
заданий для курса**



Модуль 1

Основы TCP/IP сетей.

Настройка и диагностика сети



Сборник практических заданий для курса «AL-1704. Сетевое администрирование ОС Astra Linux Special Edition 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

Материалы:

- Эталонная виртуальная машина template_1704_3:
 - Процессор — 1.
 - RAM — 2 ГБ.
 - Диск — 30 ГБ.
 - Сетевой адаптер — тип подключения «Сетевой мост».
 - ОС — Astra Linux Special Edition 1.7.3 (максимальный уровень защищенности) с установленными дополнениями VirtualBox для гостевых ОС.

Дополнительная информация:

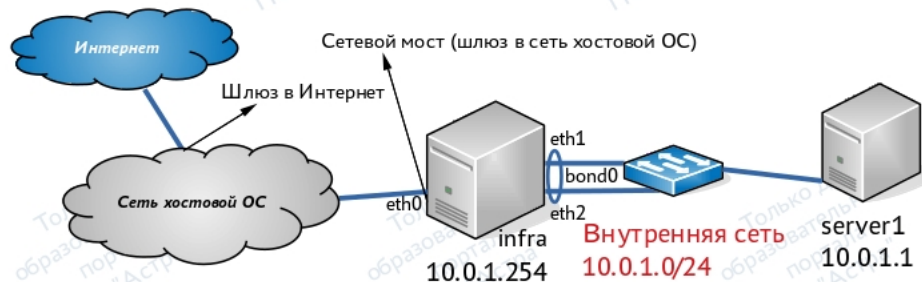
- Настройки эталонной виртуальной машине предполагают, что репозитории Astra Linux 1.7.3 доступны через Интернет.
- В учебном центре репозитории могут располагаться на внутренних ресурсах УЦ. В этом случае в эталонную VM должны быть внесены соответствующие изменения.

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

Описание практического задания

- Настройка сетевых интерфейсов в виртуальной машине (VM) `infra` с помощью Network Manager.
- Настройка сетевого интерфейса в VM `server1` с помощью `ifup/ifdown` команд.
- Агрегирование (объединение) Ethernet интерфейсов на VM `infra`.

Схема сети



Настройка VM `infra`

Задание: Настроить VM `infra`, первоначально изменив имя хоста (`infra`), а затем настроить сетевое подключение, соответствующее интерфейсу `eth0`, с использованием Network Manager. Далее внести информацию об имени и адресе хоста в файл `/etc/hosts` и включить внутреннюю маршрутизацию.

- 1 Клонировать VM `template_1704_3` и назвать новую VM `infra`.
- 2 Не запуская VM `infra`, добавить два сетевых интерфейса (всего три). Один (первый) интерфейс — сетевой мост, два других — внутренняя сеть.
- 3 Запустить VM `infra`.
- 4 Сменить имя хоста на `infra` с помощью команды `hostnamectl`.

```
sudo hostnamectl set-hostname infra
```

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

```
127.0.0.1    localhost
10.0.1.254   infra
```

- 6 Изменить имена соединений в Network Manager на net1, net2, net3 так, чтобы названия сетевых соединений для первого (eth0), второго (eth1) и третьего (eth3) интерфейсов имели вид net1, net2, net3.

```
nmcli con sh
nmcli con mod <старое имя> con-name <новое имя соединения>
```

- 7 Проверить, получил ли внешний интерфейс (сетевой мост) сетевые настройки по DHCP.

```
ip a s eth0
```

- 8 Настроить соединение net2: IP-адрес - 10.0.1.254/24. Проверить, что настройка сетевого соединения произведена успешно.

```
nmcli con mod net2 ipv4.addresses 10.0.1.254/24 ipv4.method
manual
nmcli con up net2
ip a s eth1
```

- 9 Включить внутреннюю маршрутизацию.

```
sudo sysctl -w net.ipv4.ip_forward=1
```

- 10 Настроить автоматическое включение маршрутизации при загрузке системы путем внесения изменений в файл /etc/sysctl.conf.

```
net.ipv4.ip_forward=1
```

Настройка VM server1

Задание: Настроить VM server1, первоначально изменив имя хоста (server1), затем настроить сетевой интерфейс eth0 с использованием файла interfaces и внести информацию об имени и адресе хоста в файл /etc/hosts.

- 1 Клонировать VM template_1704_3 и назвать новую VM — server1.

- 2 Запустить VM.

- 3 Сменить имя хоста на server1 командой hostnamectl

```
sudo hostnamectl set-hostname server1
```

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

```
127.0.0.1    localhost
10.0.1.1    server1
```

- 5 Остановить и запретить запуск Network Manager.

```
sudo systemctl stop NetworkManager
sudo systemctl mask NetworkManager
```

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

- IP-адрес - 10.0.1.1/24;
- шлюз - 10.0.1.254

```
auto eth0
iface eth0 inet static
    address 10.0.1.1/24
    gateway 10.0.1.254
```

7 Перезапустить службу и проверить настройки сетевого интерфейса и доступность шлюза.

```
sudo systemctl restart networking
ip a s eth0
ping 10.0.1.254
```

Настройка агрегации Ethernet интерфейсов

Задание: Настроить агрегацию сетевых интерфейсов eth1 и eth2 в режиме active-backup на хосте infra с использованием Netwotk Manager, затем произвести сетевые настройки агрегированного интерфейса и с помощью утилиты tcpdump проверить работоспособность агрегированного сетевого интерфейса путем отключения/включения интерфейсов.

1 Настройка производится на BM infra.

2 Убрать настройки и отключить сетевое соединение net2.

```
nmcli con mod net2 ipv4.method auto
nmcli con down net2
```

3 Создать (добавить) логический ведущий (master) интерфейс типа bond с именем сетевого интерфейса bond0 с помощью Network Manager.

```
nmcli con add type bond ifname bond0
```

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

```
nmcli con add type ethernet ifname eth1 master bond0
nmcli con add type ethernet ifname eth2 master bond0
```

5 Определить название сетевого соединения типа bond

```
nmcli con sh
```

6 Настроить статический адрес 10.0.1.254 на интерфейсе bond0.

**nmcli con mod bond-bond0 ipv4.addr 10.0.1.254/24
ipv4.method manual**

- 7 Активировать настройки bond0.

nmcli con up bond-bond0

- 8 Проверить, что интерфейс bond0 настроен и server1 доступен.

**ip a s bond0
ping 10.0.1.1**

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

nmcli con mod bond-bond0 bond.options mode=active-backup

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

nmcli con mod bond-bond0 +bond.options fail_over_mac=1

- 11 Активировать изменения на интерфейсе bond0 и проверить, что режимы агрегирования настроены верно.

**nmcli con up bond-bond0
nmcli con sh bond-bond0 | grep bond**

- 12 Установить tcpdump.

sudo apt install tcpdump

- 13 Запустить непрерывную проверку доступности хоста 10.0.1.1.

ping 10.0.1.1

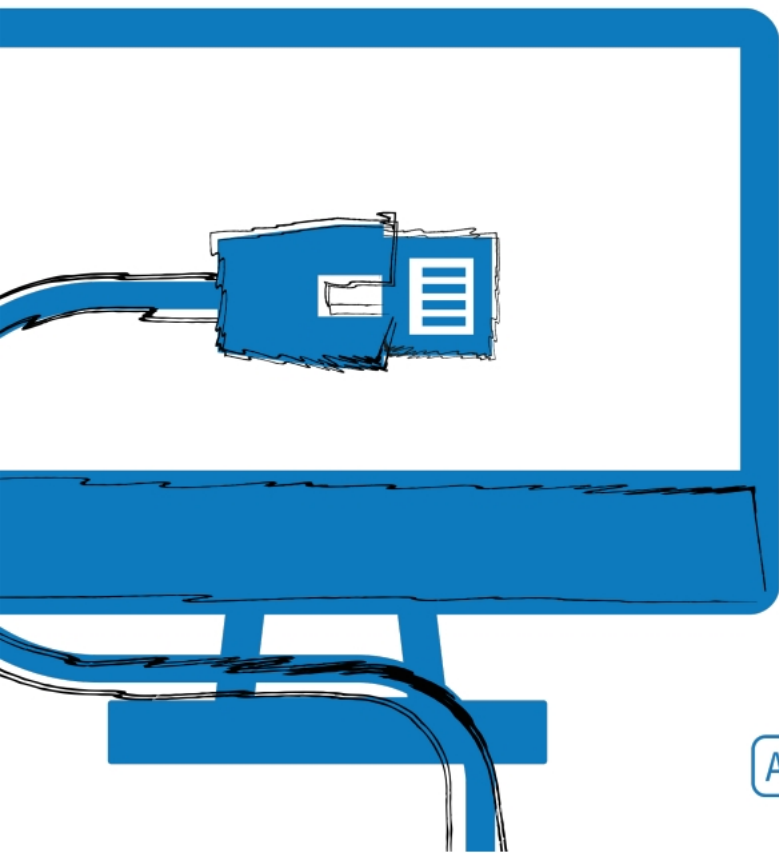
- 14 Запустить еще два терминала, в которых осуществлять перехват ICMP сообщений на интерфейсах eth1 и eth2.

**sudo tcpdump -i eth1 icmp
sudo tcpdump -i eth2 icmp**

- 15 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 (сетевой адаптер 2).

Модуль 2

Настройка удаленного доступа



Сборник практических заданий для курса «AL-1704. Сетевое администрирование ОС Astra Linux Special Edition 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

Материалы:

- Эталонная виртуальная машина template_1704_3:
 - Процессор — 1.
 - RAM — 2 ГБ.
 - Диск — 30 ГБ.
 - Сетевой адаптер — тип подключения «Сетевой мост».
 - ОС — Astra Linux Special Edition 1.7.3 (максимальный уровень защищенности) с установленными дополнениями VirtualBox для гостевых ОС.

Дополнительная информация:

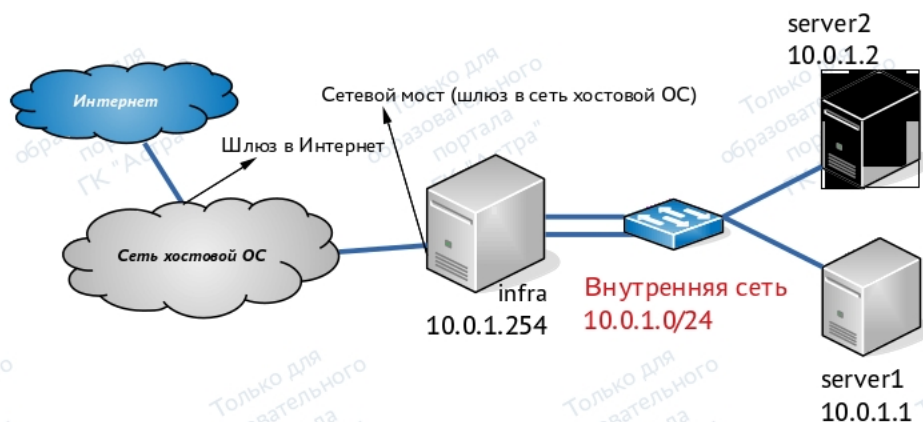
- Настройки эталонной виртуальной машине предполагают, что репозитории Astra Linux 1.7.3 доступны через Интернет.
- В учебном центре репозитории могут располагаться на внутренних ресурсах УЦ. В этом случае в эталонную ВМ должны быть внесены соответствующие изменения.

Модуль 2. Настройка удаленного доступа

Описание практического задания

- Настройка аутентификации по ключам при подключении по SSH с BM infra к BM server1.
- Создание и настройка BM server2.
- Настройка аутентификации по ключам при подключении по SSH с BM infra к BM server2.
- Переадресация портов с помощью SSH:
 - динамическая переадресация и настройка утилиты apt;
 - переадресация локального порта для доступа к сетевым службам.

Схема сети



Настройка аутентификации по ключам

Задание: На хосте infra настроить аутентификацию по ключам при подключении к хосту server1 по SSH. Настроить BM server2:

- изменить имя хоста (server2),
- настроить сетевой интерфейс eth0 на server2 с использованием файла interfaces.

На хосте infra настроить аутентификацию по ключам при подключении к хосту server2 по SSH.

- 1 На server1 проверить работоспособность службы ssh. При необходимости запустить службу ssh и добавить ее в автозагрузку.

```
sudo systemctl status ssh
sudo systemctl start ssh
sudo systemctl enable ssh
```

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

```
ssh-keygen
ssh-copy-id sa@10.0.1.1
```

- 3 Создать VM server2 путём клонирования VM template_1704_3.

- 4 В созданной VM server2 сменить имя хоста на server2.

```
sudo hostnamectl set-hostname server2
```

- 5 Добавить в файл /etc/hosts запись для server2.

```
127.0.0.1    localhost
10.0.1.2     server2
```

- 6 Остановить и запретить запуск Network Manager.

```
sudo systemctl stop NetworkManager
sudo systemctl mask NetworkManager
```

- 7 Настроить сетевой интерфейс eth0 в файле /etc/network/interfaces:

- IP адрес 10.0.1.2/24;
- шлюз 10.0.1.254

```
auto eth0
iface eth0 inet static
    address 10.0.1.2/24
    gateway 10.0.1.254
```

- 8 Перезапустить службу networking. Проверить настройки и доступность шлюза.

```
sudo systemctl restart networking
ip a s eth0
ping 10.0.1.254
```

- 9 На server2 запустить проверить работоспособность службы ssh.

```
sudo systemctl status ssh
```

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

ssh-copy-id sa@10.0.1.2

Переадресация портов.

Задание: В первой части задания на хосте server1 запустить SOCKS-прокси с помощью SSH-туннеля через хост infra и настроить работу утилиты apt через SOCKS-прокси.

Во второй части задания на хосте server1 установить и запустить веб-сервер Apache. Отключить на веб-сервере режим работы AstraMode и обеспечить доступ к веб-серверу только по адресу 127.0.0.1. На хосте infra с помощью SSH настроить переадресацию локального порта для доступа к веб-серверу, работающему на хосте server1.

- 1 На BM server1 настроить динамическую переадресацию (SOCKS-прокси) на хост infra.

```
ssh -fN -D 1080 10.0.1.254
```

- 2 Проверить, что SOCKS-прокси запустился.

```
ss -tln | grep 1080
```

- 3 Настроить работу утилиты apt через SOCKS-прокси:

- создать файл /etc/apt/apt.conf.d/70proxy;
- добавить в файл настройки для прокси;
- проверить, что apt работает через прокси.

```
Acquire::https::Proxy "socks5h://127.0.0.1:1080";  
Acquire::http::Proxy "socks5h://127.0.0.1:1080";  
sudo apt update
```

- 4 На BM server1 установить веб-сервер apache2.

```
sudo apt install apache2
```

- 5 В файл /var/www/html/index.html поместить файл test.txt.

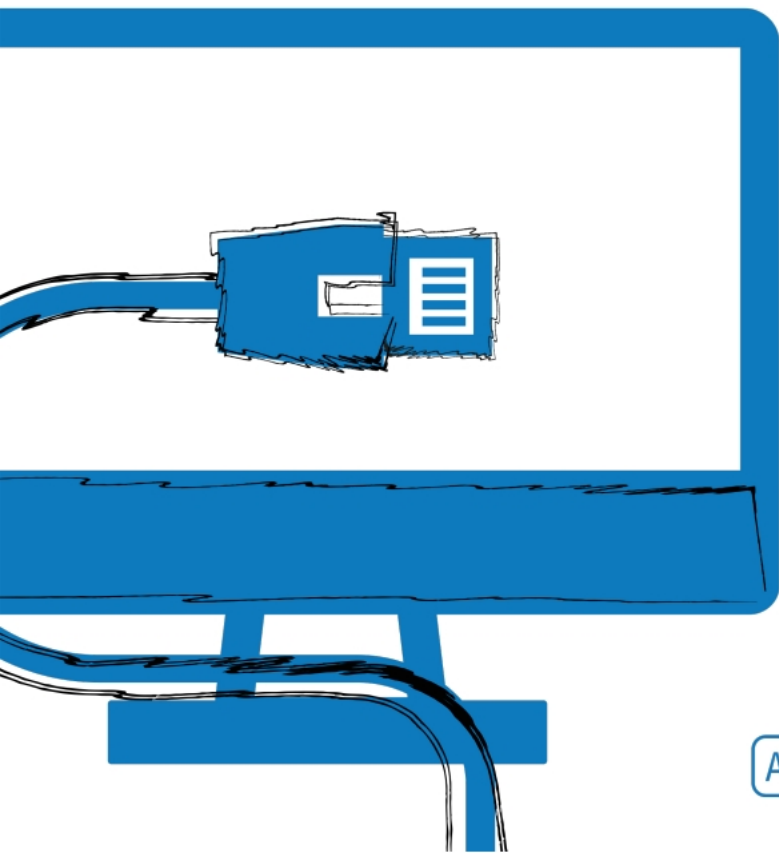
```
sudo bash -c "cat > /var/www/html/index.html"  
<HTML>  
    <BODY>  
    Course AL-1704  
    </BODY>  
</HTML>  
<Ctrl-D>
```

- 6 Произвести следующие настройки apache2:

- в файле `/etc/apache2/apache2.conf` задать параметр `AstraMode off`
 - в файле `/etc/apache2/ports.conf` задать параметр `Listen 127.0.0.1:80`
7. Перезапустить службу `apache2`.
`sudo systemctl restart apache2`
 8. Проверить работоспособность `apache2` сервера и что сервер доступен только локально.
`sudo ss -tlnp | grep 80`
`curl http://localhost`
`curl http://10.0.1.1`
 9. На ВМ `infra` проверить доступ к веб-серверу, установленному на ВМ `server1`, с помощью утилиты `curl`.
`curl http://10.0.1.1`
 10. Настроить локальную переадресацию порта 8080 на ВМ `infra` на порт 80 в ВМ `server1`.
`ssh -fN -L 8080:127.0.0.1:80 sa@10.0.1.1`
 11. Получить файл `test.txt` с FTP сервера с помощью утилиты `curl`:
`curl http://localhost:8080`

Модуль 3

Служба DNS



Сборник практических заданий для курса «AL-1704. Сетевое администрирование ОС Astra Linux Special Edition 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

Материалы:

- Эталонная виртуальная машина template_1704_3:
 - Процессор — 1.
 - RAM — 2 ГБ.
 - Диск — 30 ГБ.
 - Сетевой адаптер — тип подключения «Сетевой мост».
 - ОС — Astra Linux Special Edition 1.7.3 (максимальный уровень защищенности) с установленными дополнениями VirtualBox для гостевых ОС.

Дополнительная информация:

- Настройки эталонной виртуальной машине предполагают, что репозитории Astra Linux 1.7.3 доступны через Интернет.
- В учебном центре репозитории могут располагаться на внутренних ресурсах УЦ. В этом случае в эталонную VM должны быть внесены соответствующие изменения.

Модуль 3. 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

Задание: На хосте server1 установить DNS-сервер bind9. Настроить на хосте server1 ведущий (master) DNS-сервер для зон astra.test и 1.0.10.in-addr.arpa: в файле /etc/bind/named.conf.local создать описание для этих зон и создать файлы с зонной информацией.

Зонная информация должна включать записи типа SOA и NS (DNS-серверы: server1.astra.test и server2.astra.test), а также информацию о хостах infra, server1 и server2. Для имени server1.astra.test требуется определить псевдоним www.astra.test.

1 В BM server1 установить bind9.

Примечание: следует использовать SOCKS-прокси.

sudo apt install bind9

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

```
zone "astra.test"{
    type master;
    file "master/astra.test";
};
```

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

```
zone "1.0.10.in-addr.arpa"{
    type master;
    file "master/10.0.1";
};
```

- 4 Проверить правильность внесенных изменений в настройки сервера DNS.

```
sudo named-checkconf
```

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

```
sudo mkdir /var/cache/bind/master
sudo chgrp bind /var/cache/bind/master
sudo chmod g+s /var/cache/bind/master
```

- 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`);
- А – для `server1.astra.test`, `server2.astra.test`, `infra.astra.test` (внутренний интерфейс);
- CNAME `www` → `server1`.

```
$TTL 1h
@ IN SOA server1.astra.test. dnsmaster.astra.test. (
2022032201 ; задать текущие значения ууууmmddnn
10800
3600
604800
86400 )
```

```
IN NS server1
IN NS server2.astra.test.
```

```
server1 IN A 10.0.1.1
server2 IN A 10.0.1.2
infra IN A 10.0.1.254
www IN CNAME server1
```

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

```
sudo named-checkzone astra.test
/var/cache/bind/master/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).

```
$TTL 1h
@ IN SOA server1.astra.test. dnsmaster.astra.test. (
2022032201 ; задать текущие значения ууууmmddnn
10800
3600
604800
86400 )
```

```
IN NS server1.astra.test.
IN NS server2.astra.test.
```

```
1 IN PTR server1.astra.test.
2 IN PTR server2.astra.test.
254 IN PTR infra.astra.test.
```

- 9 Проверить правильность внесения зонной информации в файл 10.0.1.

```
sudo named-checkzone 1.0.10.in-addr.arpa
/var/cache/bind/master/10.0.1
```

- 10 Перезапустить сервер DNS и проверить, что служба DNS работает.

```
sudo systemctl restart bind9  
systemctl status bind9
```

Настройка подчиненного сервера DNS для зон astra.test и

1.0.10.in-addr.arpa

Задание: На хосте server2 установить DNS-сервер bind9. Настроить на хосте server2 подчиненный (slave) DNS-сервер для зон astra.test и 1.0.10.in-addr.arpa. Для этого в файле /etc/bind/named.conf.local нужно создать описание для этих зон, указав в качестве ведущего DNS-сервера server1. Убедиться, что трансфер зонной информации прошел успешно.

- 1 В ВМ server2 установить bind9.

Примечание: использовать SOCKS-прокси и настроить работу apt через прокси.

```
sudo apt install bind9
```

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

```
systemctl status bind9
```

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

```
sudo mkdir /var/cache/bind/slave  
sudo chgrp bind /var/cache/bind/slave  
sudo chmod g+s /var/cache/bind/slave
```

- 4 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.

```
zone "astra.test" {  
    type slave;  
    file "slave/astra.test";  
    masters {10.0.1.1};  
};
```

- 5 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.

```
zone "1.0.10.in-addr.arpa" {
    type slave;
    file "slave/10.0.1";
    masters {10.0.1.1;};
};
```

- 6 Проверить правильность внесенных изменений в настройки сервера DNS.

```
sudo named-checkconf
```

- 7 Перезапустить сервер DNS и проверить, что служба DNS работает.

```
sudo systemctl restart bind9
systemctl status bind9
```

- 8 Настроить 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 server2.

```
forwarders {
    10.0.1.254;
};
```

Настройка кэширующего сервера DNS

Задание: На хосте infra настроить кэширующий DNS-сервер. На DNS-серверах server1 и server2 настроить ретрансляцию запросов на DNS-сервер infra.

- 1 Настройка производится на VM infra.

- 2 В VM infra установить bind9.

```
sudo apt install bind9
```

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

```
systemctl status bind9
```

- 4 На DNS-серверах server1 и server2 настроить ретрансляцию DNS-запросов на кэширующий DNS-сервер infra. Для этого внести соответствующие изменения в файлы /etc/bind/named.conf.options.

```
forwarders {
    10.0.1.254;
};
```

Настройка клиентской части DNS

Задание: На хостах server1 и server2 настроить DNS-клиент, внося изменения в файл resolv.conf. Для хостов server1 и server2 в качестве DNS-сервера указать адрес локального хоста. Настроить DNS-клиент на хосте infra с помощью Network Manager. В качестве DNS-серверов указать адреса хостов server1 и server2.

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

- на server1 — DNS-сервер - localhost;
В файл /etc/resolv.conf внести запись.

```
nameserver 127.0.0.1
```

- на server2 — DNS-сервер localhost;
В файл /etc/resolv.conf внести запись.

```
nameserver 127.0.0.1
```

- на infra — server1 и server2.

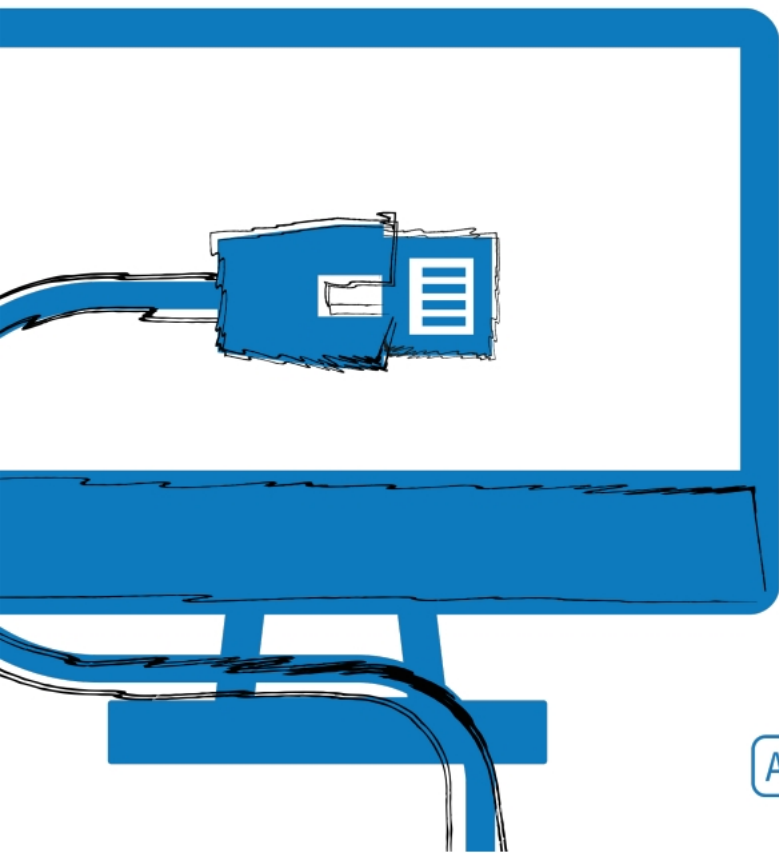
```
nmcli con mod net1 ipv4.dns "10.0.1.1, 10.0.1.2" \
  ipv4.ignore-auto-dns yes
nmcli con up net1
```

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

```
sudo apt install dnsutils
nslookup infra.astra.test
nslookup www.astralinux.ru
```

Модуль 4

Служба DHCP и настройка динамического DNS



Сборник практических заданий для курса «AL-1704. Сетевое администрирование ОС Astra Linux Special Edition 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

Материалы:

- Эталонная виртуальная машина template_1704_3:
 - Процессор — 1.
 - RAM — 2 ГБ.
 - Диск — 30 ГБ.
 - Сетевой адаптер — тип подключения «Сетевой мост».
 - ОС — Astra Linux Special Edition 1.7.3 (максимальный уровень защищенности) с установленными дополнениями VirtualBox для гостевых ОС.

Дополнительная информация:

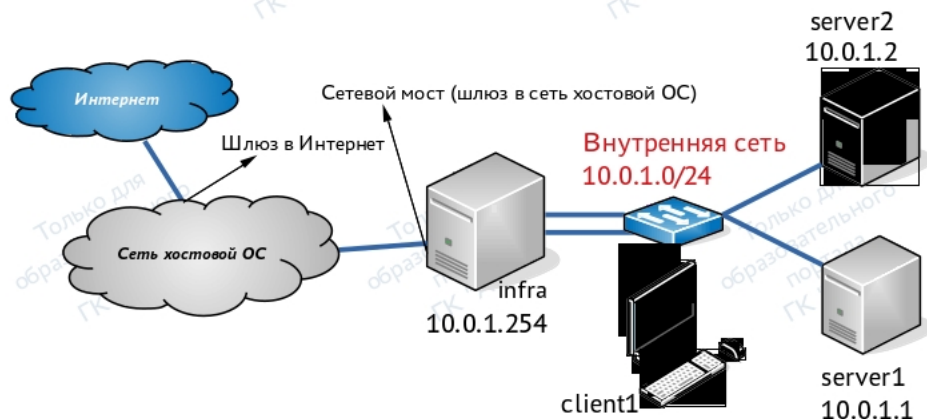
- Настройки эталонной виртуальной машине предполагают, что репозитории Astra Linux 1.7.3 доступны через Интернет.
- В учебном центре репозитории могут располагаться на внутренних ресурсах УЦ. В этом случае в эталонную VM должны быть внесены соответствующие изменения.

Модуль 4. 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

Задание: На хосте server1 установить DHCP-сервер. Настроить DHCP-сервер для выдачи динамических IP-адресов из диапазона 10.0.1.101-10.0.1.199, передавая клиентам сетевые настройки (адреса DNS-серверов и шлюза). Создать и настроить VM client1. Убедиться, что хост client1 получил IP-адрес и сетевые настройки от DHCP-сервера. На хосте server1 получить информацию о выданных в аренду адресах.

- 3 На server1 установить сервер DHCP.

```
sudo apt install isc-dhcp-server
```

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

INTERFACESv4="eth0"

- 5 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.

```
subnet 10.0.1.0 netmask 255.255.255.0 {  
    range 10.0.1.101 10.0.1.199;  
    option routers 10.0.1.254;  
    option domain-name-servers 10.0.1.1, 10.0.1.2;  
}
```

- 6 Запустить службу DHCP и проверить, что служба запущена.

```
sudo systemctl start isc-dhcp-server.service  
systemctl status isc-dhcp-server.service
```

- 7 Путем клонирования VM template_1704_3 создать и запустить VM client1.

- 8 Изменить имя хоста на client1.

```
sudo hostnamectl set-hostname client1
```

- 9 В файла /etc/hosts заменить astra на client1:

```
127.0.1.1 client1
```

- 10 Подумать, какой dhcp клиент используется в VM client1 и почему?

```
ps -ef | grep NetworkManager
```

В файле /etc/NetworkManager/NetworkManager.conf отсутствует параметр dhcp. По умолчанию используется dhclient

- 11 Проверить, что IP адрес и другие настройки в VM client1 были получены от DHCP-сервера server1. Определить срок аренды.

```
ip a s
```

```
nmcli con sh Проводное\ соединение\ 2 | grep dhcp
```

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

Настройка выдачи и получения фиксированного IP адреса

Задание: На хосте server2 настроить получение IP-адреса по DHCP и узнать MAC-адрес сетевого интерфейса.

Настроить DHCP сервер на хосте server1 для выдачи адреса 10.0.1.2 хосту server2 и передачи сетевых настроек (адрес DNS-сервера - 127.0.0.1 и адрес шлюза).

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

```
auto eth0
iface eth0 inet dhcp
```
- 2 Деактивировать сетевой интерфейс.

```
sudo ifdown eth0
```
- 3 Перезапустить службу `networking` и проверить, что IP адрес получен с сервера DHCP.

```
sudo systemctl restart networking
ip a s
```
- 4 В VM 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`.

```
host server2 {
    hardware ethernet MAC_адрес_server2;
    fixed-address 10.0.1.2;
    option routers 10.0.1.254;
    option domain-name-servers 127.0.0.1;
}
```

- 5 Перезапустить службу DHCP:

```
sudo systemctl restart isc-dhcp-server.service
sudo systemctl status isc-dhcp-server.service
```
- 6 На хосте server2 деактивировать сетевой интерфейс, перезапустить службу `networking` и проверить получение IP адреса, маршрут по умолчанию и разрешение имен DNS.

```
sudo ifdown eth0
sudo systemctl restart networking
ip a s
ip route
nslookup server1.astra.test
```

Настройка динамического обновления зонной информации на DNS сервере

Задание: На хосте server1 создать ключ (алгоритм MD5, длина ключа 128 бит) и добавить описание ключа в настройки ведущего DNS-сервера (файл /etc/bind/named.conf.local). В настройках ведущего DNS-сервера разрешить обновление зонной информации с использованием созданного ключа.

Далее в настройках DHCP-сервера включить возможность передачи данных о хостах, которым выданы динамические IP-адреса, DNS-серверу. Определить параметр, задающий имя домена, добавить информацию о ключе и зонах, в которых должна обновляться информация, указав адрес ведущего DNS-сервера. В заключении убедиться, что информация об имени и IP-адресе хоста client1 добавилась в зоны astra.test и 1.0.10.in-addr.arpa.

1 Настроить службу DNS (server1):

- Убедиться, что пользователь bind имеет право создавать файлы в каталоге, в котором хранятся файлы с зонной информацией.

```
sudo chown bind /var/cache/bind/master
```

- 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.

```
sudo dnssec-keygen -a HMAC-MD5 -b 128 -n HOST dhcp-dns
```

- Значение ключа сохраняется в файл в текущем каталоге с суффиксом .private.

```
sudo cat *.private
```

```
...
Algorithm: 157 (HMAC_MD5)
Key: sHkZg3jICvLS+rJV5HDDiA==
...
```

- В файл /etc/bind/named.conf.local добавить секцию типа key, в которой описываются параметры созданного ключа.

```
key dhcp-dns {
    algorithm HMAC-MD5;
    secret "sHkZg3jICvLS+rJV5HDDiA==";
};
```

- В секции типа zone добавить разрешение обновлять зонную информацию с помощью созданного ключа.


```
zone "astra.test"{
    type master;
    file "master/astra.test";
    allow-update{ key dhcp-dns; };
};
```

```
zone "1.0.10.in-addr.arpa"{
    type master;
    file "master/10.0.1";
    allow-update{ key dhcp-dns; };
};
```

- Перезапустить службу DNS и проверить ее статус.

```
sudo systemctl restart bind9
systemctl status bind9
```

2 Настроить службу DHCP (server1):

- В файл /etc/dhcp/dhcpd.conf внести следующие изменения:
 - Определить параметр domain-name.

```
option domain-name "astra.test";
```

- Определить параметры ddns-update-style и ddns-updates.

```
ddns-update-style interim;
ddns-updates on;
```

- Добавить секцию типа key с описанием параметров созданного ранее ключа (такую же, как в настройках службы DNS).

```
key dhcp-dns {
    algorithm HMAC-MD5;
    secret "sHkZg3jICvLS+rJV5HDDiA==";
}
```

- 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.

```
zone astra.test {
    primary 10.0.1.1;
    key dhcp-dns;
}
```

```
zone 1.0.10.in-addr.arpa {
    primary 10.0.1.1;
    key dhcp-dns;
}
```


- Перезапустить службу DHCP и проверить статус службы:

```
sudo systemctl restart isc-dhcp-server.service  
systemctl status isc-dhcp-server.service
```

- 3 В VM client1 активировать сетевое соединение командой nmcli.

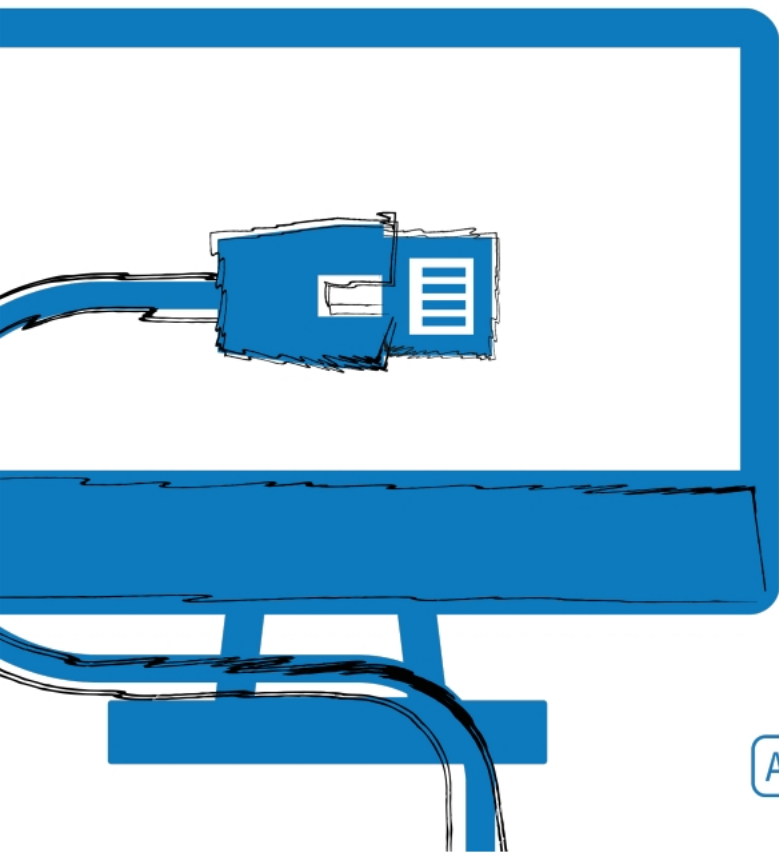
```
nmcli con up Проводное\ соединение\ 2
```

- 4 Проверить, что зонная информация обновилась на обоих серверах DNS (server1 и server2) и включает ресурсные записи для хоста client1 в зонах astra.test и 10.0.10.in-addr.arpa.

```
nslookup client1.astra.test 10.0.1.1  
nslookup client1.astra.test 10.0.1.2  
nslookup IP_адрес_client1 10.0.1.1  
nslookup IP_адрес_client1 10.0.1.2
```

Модуль 5

Прокси-сервер SQUID



Модуль 5. 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

Задание: На хосте infra установить прокси-сервер SQUID и разрешить доступ к прокси-серверу для хостов из сети 10.0.1.0/24.

1. Установить SQUID на BM infra.

```
sudo apt install squid
```

2. Сохранить исходный вариант конфигурационного файла SQUID.

```
cd /etc/squid  
sudo cp squid.conf squid.conf.orig
```

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

```
sudo -i
cd /etc/squid
cat squid.conf.orig | grep -v '^#' | grep -v '^$' >
squid.conf
exit
```

- 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.

```
acl localnet src 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.

```
http_access allow localnet
```

- 6 Выполнить команду, которая позволяет пересчитать измененный конфигурационный файл.

```
sudo squid -k reconfigure
```

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

Настройка базовой аутентификацию NCSA

Задание: На хосте infra установить программный пакет apache2-util. С помощью команды htpasswd создать учетную запись пользователя iuser, при этом пароли пользователей хранить в файле /etc/squid/passwd. Настроить на прокси-сервере SQUID NCSA аутентификацию пользователей. Убедиться, что аутентификация пользователей на прокси-сервере работает правильно.

- 1 Установить программный пакет apache2-utils на infra.

```
sudo apt install apache2-utils
```

- 2 Командой htpasswd создать пользователя iuser на infra.

Примечание: используйте параметр -s имя_файла_с_паролями, когда первый раз выполняете команду htpasswd.

```
sudo htpasswd -s /etc/squid/passwd iuser
```

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

```
sudo chown proxy:proxy /etc/squid/passwd
sudo chmod 640 /etc/squid/passwd
```

4 Внести изменения в конфигурационный файл SQUID:

- Настроить схему аутентификации NCSA с помощью директивы `auth_param`.

```
auth_param basic program
```

```
/usr/lib/squid/basic_ncsa_auth /etc/squid/passwd
```

- Определить список управления доступом типа `proxy_auth` с именем `authusers`, который содержит всех валидных пользователей.

```
acl authusers proxy_auth REQUIRED
```

- 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`.

```
http_access deny !authusers
```

```
http_access allow authusers
```

5 Выполнить перечитывание конфигурационного файла сервером SQUID.

```
sudo squid -k reconfigure
```

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

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

Задание: Добавить в настройки прокси-сервера два списка управления доступом: один соответствует домену назначения `youtube.com`, другой – диапазону рабочего времени (с 9 до 18 часов). Создать на прокси-сервере правило, запрещающее доступ к ресурсам из домена `youtube.com` в рабочее время. Убедиться, что правило работает.

- 1 На хосте `client1` проверить доступность `youtube.com`.

- 2 Создать список управления доступом типа `dstdomain`, который включает домен `youtube.com`.

```
acl youtube_site dstdomain .youtube.com
```

- 3 Создать список управления доступом типа `time`, который определяет рабочее время.

```
acl work_time time 9:00-18:00
```

- 4 Добавить правило, которое запрещает доступ к сайтам в домене youtube.com в рабочее время, указав одновременно оба списка управления доступом.

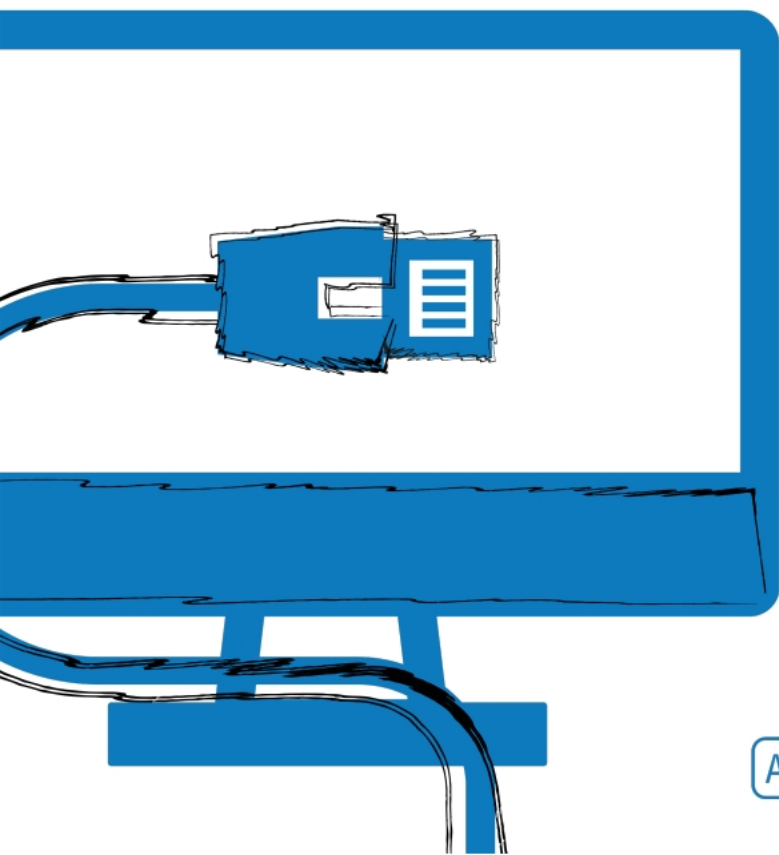
Примечание: поместите правило в нужное место в файле /etc/squid/squid.conf, чтобы оно сработало.

http_access deny youtube_site work_time

- 5 На хосте client1 проверить доступность youtube.com.

Модуль 6

Синхронизация времени по сети



Сборник практических заданий для курса «AL-1704. Сетевое администрирование ОС Astra Linux Special Edition 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

Материалы:

- Эталонная виртуальная машина template_1704_3:
 - Процессор — 1.
 - RAM — 2 ГБ.
 - Диск — 30 ГБ.
 - Сетевой адаптер — тип подключения «Сетевой мост».
 - ОС — Astra Linux Special Edition 1.7.3 (максимальный уровень защищенности) с установленными дополнениями VirtualBox для гостевых ОС.

Дополнительная информация:

- Настройки эталонной виртуальной машине предполагают, что репозитории Astra Linux 1.7.3 доступны через Интернет.
- В учебном центре репозитории могут располагаться на внутренних ресурсах УЦ. В этом случае в эталонную VM должны быть внесены соответствующие изменения.

Модуль 6. Синхронизация времени по сети

Описание практического задания

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

Схема сети



Настройка синхронизации времени с помощью службы chrony

Задание: На хосте infra настроить службу chrony, указав в качестве источников времени публичные NTP-серверы. Разрешить только хостам из сети 10.0.1.0/24 использовать сервер infra в качестве источника времени. Убедиться, что синхронизация времени на хосте infra происходит успешно.

6 Настроить службу chrony на VM infra:

- В качестве источников времени выбрать сервер ntp1.vniiftri.ru и пул [pool.ntp.org](https://www.pool.ntp.org/). Убрать все лишние источники времени.
- Разрешить доступ к серверу infra только хостам из сети 10.0.1.0/24.
- Для параметра `maxupdateskew` установить значение, характерное для надежного быстрого сетевого соединения.

```
cat /etc/chrony/chrony.conf
server ntp1.vniiftri.ru iburst
pool ru.pool.ntp.org iburst
keyfile /etc/chrony/chrony.keys
driftfile /var/lib/chrony/chrony.drift
logdir /var/log/chrony
maxupdateskew 10.0
rtcsync
makestep 1 3
allow 10.0.1.0/24
```

- 7 С помощью утилиты `chronyc` проверить, что синхронизация времени производится.

```
sudo chronyc sources
sudo chronyc tracking
```

Настройка синхронизации времени с помощью `systemd`

Задание: На хосте `server1` настроить синхронизацию, используя службу `systemd-timesyncd`. В качестве источника времени использовать сервер `infra`.

- 1 Удалить службу `ntp`.

```
sudo apt purge ntp
```

- 2 Настроить синхронизацию времени для ВМ `server1`, используя встроенную в `systemd` NTP службу. Источник времени — `infra`.

Примечание: для выполнения данного задания требуется снять запрет на запуск службы `systemd-timesyncd` путем комментирования в файле `/lib/systemd/system/systemd-timesyncd.service.d/disable-with-time-daemon.conf` строки

```
ConditionFileIsExecutable=!/usr/sbin/VboxService
```

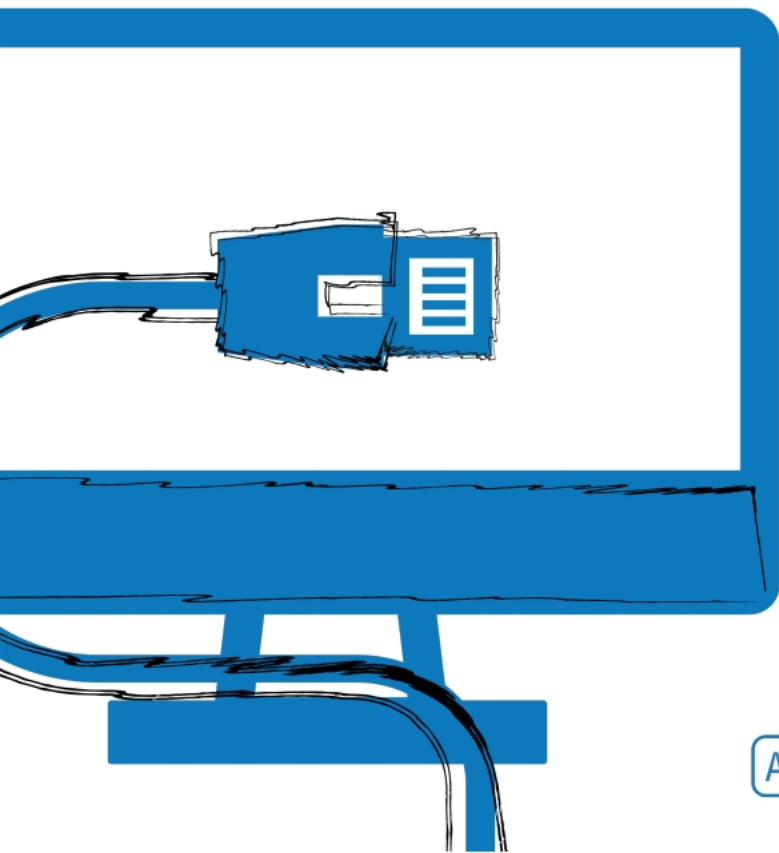
```
cat /etc/systemd/timesyncd.conf | grep '^NTP'
NTP=10.0.1.254
```

- 3 Убедиться, что синхронизация времени проходит успешно.

```
timedatectl timesync-status
```

Модуль 7

Управление конфигурациями с помощью Ansible

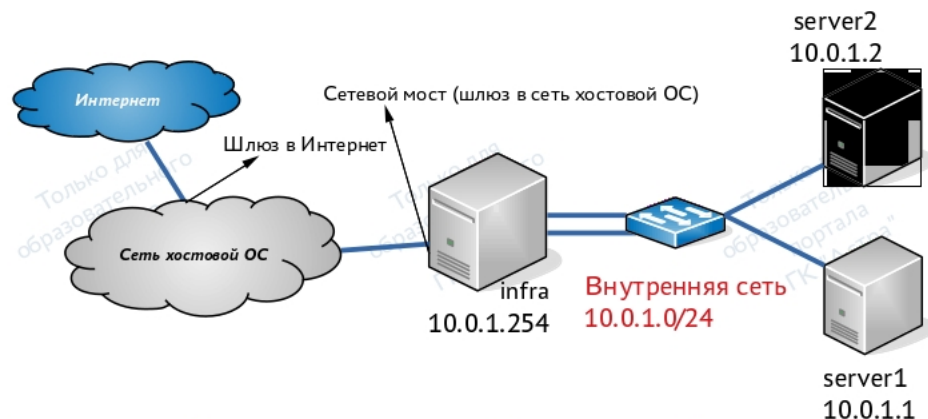


Модуль 7. Управление конфигурациями с помощью Ansible

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

Задание: На хосте infra. Создать каталог ansible, в котором будут размещаться все файлы проекта. В этом каталоге создать файл инвентаризации hosts, в котором описать хосты server1, server2, infra и группу хостов servers, состоящую из server1 и server2.

Создать конфигурационный файл ansible.cfg, в котором произвести настройки, позволяющие использовать файл инвентаризации по умолчанию. С помощью команды ansible получить текущие даты и время всех хостов. В качестве дополнительного задания, используя команду ansible и модуль replace, привести строку в файле /etc/hosts, содержащую адрес и имя хоста к виду: IP_адрес имя_хоста.astra.test имя_хоста.

- 1 Установить ansible на BM infra.
`sudo apt install ansible`
- 2 Настроить на BM 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.
`mkdir ~/ansible`
`cd ~/ansible`
- 5 Создать файл hosts, в который добавить:
 - записи для хостов server1, server2 и infra;
 - группы servers для хостов server1 и server2;
 - переменные ansible_host для каждого хоста.`infra ansible_host=10.0.1.254`
`[servers]`
`server1 ansible_host=10.0.1.1`
`server2 ansible_host=10.0.1.2`
- 6 Настроить так, чтобы созданный файл инвентаризации использовался в командах Ansible по умолчанию. Для этого создать файл ~/ansible/ansible.cfg и внести в него соответствующие настройки.
Примечание: можно посмотреть содержимое файла /etc/ansible/ansible.cfg и сделать по аналогии.
`[defaults]`
`inventory = ../ansible/host`
- 7 С помощью команды ansible получить значения текущих дат и времени на server1 и server2.
`ansible -a "date" servers`
- 8 (Дополнительное задание) Изменить информацию в файлах /etc/hosts, используя команду ansible:
 - Просмотреть содержимое файлов /etc/hosts.

`ansible -a "cat /etc/hosts" servers`

- Заменить строки вида:

IP_адрес имя_хоста

на

IP_адрес имя_хоста.astra.test имя_хоста.

Использовать модуль replace.

```
ansible -m replace -a "path=/etc/hosts \
regexp='(.+)[ \t]+(server[1-9])$' \
replace='\1 \2.astra.test \2'" servers -b
```

- Проверить новое содержимое файлов /etc/hosts.

```
ansible -a "cat /etc/hosts" servers
```

Работа с переменными, создание плейбука (playbook)

Задание: С помощью сбора фактов получить информацию об использовании оперативной памяти на хосте server1. Создать плейбук, который на группы хостов servers:

- устанавливает веб-сервер Apache;
- отключает режим AstraMode;
- копирует разные файлы index.html на рабочий веб-сервер (server1) и тестовый веб-сервер (server2);
- перезапускает веб-серверы;
- получает содержимое веб-страниц index.html и выводит их на экран.

1. Получить информацию («факты») о хосте server1 с помощью команды ansible и узнать информацию об объеме и использовании оперативной памяти.

Примечание: используйте параметр filter модуля сбора фактов.

```
ansible -m setup -a 'filter=*mem*' server1
```

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

- Установить последнюю версию 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 сору 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). Для этого 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.

Содержимое файла инвентаризации hosts:
infra ansible_host=10.0.1.254

```
[servers]
server1 ansible_host=10.0.1.1 stadiya=prod
server2 ansible_host=10.0.1.2 stadiya=test
```

Содержимое файла apache.yml:

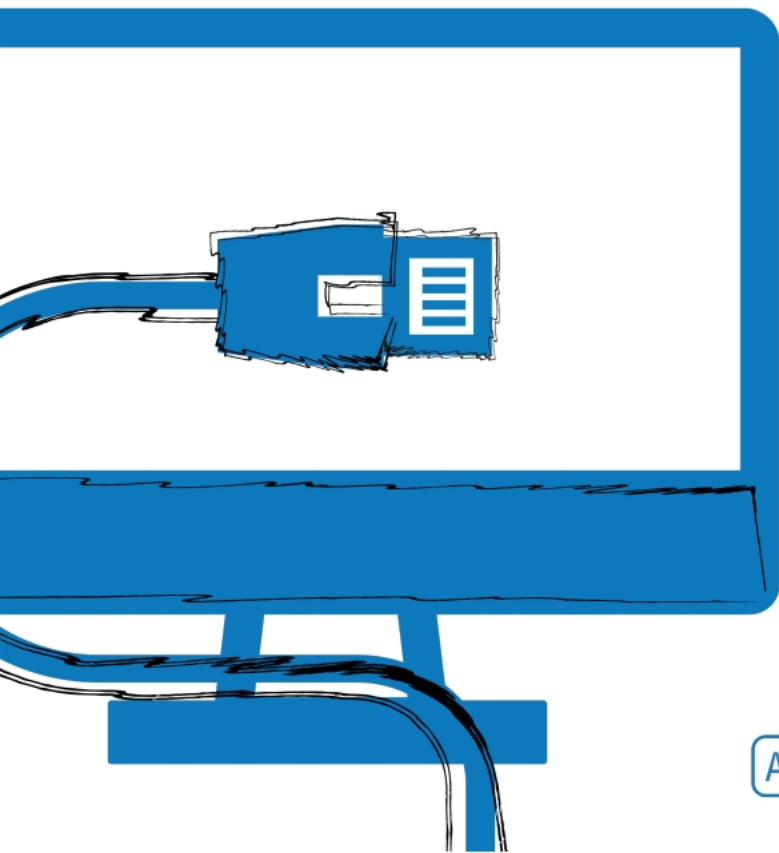
```
---
- name: Установка, запуск и проверка apache
  hosts: servers
  become: yes
```

tasks:

- name: Установка последней версии apache2
apt:
 - name: "apache2"
 - state: latest
 - update_cache: yes
 - cache_valid_time: 3600
- name: Отключаем AstraMode
lineinfile:
 - path: /etc/apache2/apache2.conf
 - insertafter: '^# AstraMode'
 - line: 'AstraMode off'
- name: Копируем индексные файлы
copy:
 - src: "index-{{ stadiya }}.html"
 - dest: "/var/www/html/index.html"
- name: Запускаем apache2
service:
 - name: apache2
 - state: restarted
 - enabled: yes
- name: Проверка работы веб-серверов
uri:
 - url: http://{{ ansible_host }}
 - return_content: yesregister: page
- name: Вывод содержимого веб-страницы
debug:
 - var: page.content

Модуль 8

Служба каталогов на базе решения FreeIPA



Сборник практических заданий для курса «AL-1704. Сетевое администрирование ОС Astra Linux Special Edition 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

Материалы:

- Эталонная виртуальная машина template_1704_3:
 - Процессор — 1.
 - RAM — 2 ГБ.
 - Диск — 30 ГБ.
 - Сетевой адаптер — тип подключения «Сетевой мост».
 - ОС — Astra Linux Special Edition 1.7.3 (максимальный уровень защищенности) с установленными дополнениями VirtualBox для гостевых ОС.

Дополнительная информация:

- Настройки эталонной виртуальной машине предполагают, что репозитории Astra Linux 1.7.3 доступны через Интернет.
- В учебном центре репозитории могут располагаться на внутренних ресурсах УЦ. В этом случае в эталонную ВМ должны быть внесены соответствующие изменения.

Модуль 8. 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



Действия, которые следует выполнить перед началом выполнения заданий

- 1 Остановить VM server1, server2, client1. В дальнейших заданиях эти VM не используются.
- 2 В VM infra :
 - отключить базовую аутентификацию в SQUID-прокси, настроенную ранее.

- сетевой интерфейс net1 настроить на автоматическое получение по DHCP адресов DNS-серверов.
nmcli con mod net1 ipv4.ignore-auto-dns no ipv4.dns ""
nmcli con up net1
- выключить режим проверки DNSSEC и перезапустить DNS-сервер.
файл /etc/bind/named.conf.options
dnssec-validation no;
sudo systemctl restart bind9

Развертывание первого сервера FreeIPA

Задание: Создать VM s1 и увеличить RAM до 3Гб, а количество ядер до 3х. Настроить имя хоста (s1.astra.test) и сетевые параметры интерфейса (10.0.1.1/24, шлюз и DNS-сервер 10.0.1.254). Внести информацию об имени адресе хоста s1.astra.test в файл /etc/hosts.

Настроить доступ к репозиториям ПО с помощью прокси-сервера infra. Установить серверное ПО FreeIPA. Изменить DNS-сервер на локальный хост. Развернуть первый сервер FreeIPA. Настроить ретрансляцию DNS-запросов на DNS-сервер infra.

- 1 Создать VM s1 путем клонирования VM template_1704_3. Увеличить количество процессоров до 3х. Увеличить объем RAM до 3ГБ. Сетевая карта одна, подключена к внутренней сети. Запустить VM.
- 2 Изменить имя хоста на s1.astra.test.

```
sudo hostnamectl set-hostname s1.astra.test
```

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

```
nmcli con mod Проводное\ соединение\ 2 con-name net1
nmcli con mod net1 ipv4.addresses 10.0.1.1/24 ipv4.dns
10.0.1.254 \ipv4.gateway 10.0.1.254 ipv4.method manual
nmcli con up net1
```

- 4 Добавить в /etc/hosts запись о s1.astra.test:
127.0.0.1 localhost localhost.localdomain
10.0.1.1 s1.astra.test s1

- 5 Проверить доступность VM infra.

```
ping 10.0.1.254
```

- 6 Настроить доступ к репозиториям Astra Linux, используя прокси SQUID, развернутый на хосте infra.

Файл `/etc/apt/apt.conf.d/70proxy`
`Acquire::http::proxy "http://10.0.1.254:3128";`

- 7 Обновить кэш с метаданными репозиториями.
`sudo apt update`
- 8 Установить серверное программное обеспечение FreeIPA.
`sudo apt install astra-freeipa-server`
- 9 Установить клиентское программное обеспечение FreeIPA.
`sudo apt install astra-freeipa-client`
- 10 Изменить DNS сервер на 127.0.0.1
`nmcli con mod net1 ipv4.dns 127.0.0.1`
`nmcli con up net1`
- 11 Развернуть сервер FreeIPA (все по умолчанию и задать пароль для доменной учетной записи admin).
`sudo astra-freeipa-server -d astra.test -n s1 -o`
- 12 Проверить статус служб FreeIPA командой `ipactl`.
`ipactl status`
- 13 Проверить доступность административной веб-консоли FreeIPA через браузер Firefox (пользователь: admin, пароль был введен во время запуска сервера FreeIPA)
<https://s1.astra.test>
- 14 Настроить ретрансляцию DNS запросов с сервера FreeIPA s1.astra.test на кэширующий 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.

Установка клиента и ввод клиента в домен

Задание: Создать ВМ c1. Настроить имя хоста (c1.astra.test) и сетевые параметры интерфейса (10.0.1.11/24, шлюз 10.0.1.254 и DNS-сервер 10.0.1.1). Внести информацию об имени адресе хоста c1.astra.test в файл `/etc/hosts`. Настроить доступ к репозиториям ПО с помощью прокси-сервера infra. Установить клиентское ПО FreeIPA. Ввести хост c1.astra.test в домен.

- 1 Создать ВМ c1 путем клонирования `template_1704_3` и запустить ее.
- 2 Задать имя хоста c1.astra.test.

```
sudo hostnamectl set-hostname c1.astra.test
```

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

```
nmcli con mod Проводное\ соединение\ 2 con-name net1  
nmcli con mod net1 ipv4.addresses 10.0.1.11/24 ipv4.dns  
10.0.1.1 \  
ipv4.gateway 10.0.1.254 ipv4.method manual  
nmcli con up net1
```

- 4 Проверить доступность сервера FreeIPA s1.astra.test.

```
ping 10.0.1.1
```

- 5 Настроить доступ к репозиториям Astra Linux, используя прокси SQUID, развернутый на хосте infra.

- 6 Обновить кэш с метаданными репозиториями.

```
sudo apt update
```

- 7 Установить пакет dnsutils.

```
sudo apt install dnsutils
```

- 8 Проверить разрешение имени сервера в DNS.

```
nslookup s1.astra.test
```

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

- 10 Установить клиент FreeIPA.

```
sudo apt install astra-freeipa-client
```

- 11 Запустить клиент FreeIPA.

```
sudo astra-freeipa-client -d astra.test
```

- 12 Перезагрузить хост c1.astra.test.

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

```
kinit admin
```

```
ipa host-show c1.astra.test
```

или

в веб-консоли <https://s1.astra.test> Идентификация → Узлы.

Управление учетными записями

Задание: Создать учетную запись `ipauser1` (минимальный уровень конфиденциальности – 0, максимальный – 1) из веб-консоли и `ipauser2` (минимальный уровень конфиденциальности – 0, максимальный – 2) с помощью консольных утилит.

- 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).

```
ipa user-add --first=IPA --last=User2 ipauser2
ipa user-mod ipauser2 --macmin=0 --macmax=2
ipa passwd ipauser2
```
- 3 На клиенте `s1.astra.test` зайдите под учетными записями `ipauser1` и `ipauser2` с разными уровнями конфиденциальности.

Управление доступом на основе узла

Задание: Создать правило, которое разрешает доступ пользователю `admin` ко всем службам на всех хостах. Создать правило, которое разрешает пользователю `ipauser2` осуществлять графический вход в систему на хосте `s1.astra.test`. Отключить правило, разрешающее доступ любым пользователям к любым службам на любых хостах. Задание можно выполнять как с помощью консольных утилит, так и через веб-консоль.

- 1 Создать правило `admin_rule`, разрешающее пользователю `admin` доступ ко всем службам на всех хостах.

```
ipa hbacrule-add --hostcat='all' --servicecat='all' \
admin_rule
ipa hbacrule-add-user --users=admin admin_rule
```
- 2 Просмотреть информацию о всех настроенных службах из командной строки и проверить, есть ли в списке служба `fly-dm`.

```
ipa hbacsvc-find
```


- 3 Создать правило, которое разрешает доменному пользователю `ipauser2` графический вход в систему на хосте `c1.astra.test`:
 - На сервере FreeIPA добавить службу `fly-dm`.
`ipa hbacsvc-add fly-dm --desc="Fly Display Manager"`
 - Создать «пустое» правило `ipauser2_flydm` с именем `ipauser2_flydm`.
`ipa hbacrule-add ipauser2_flydm`
 - Добавить в правило `flydm` учетную запись пользователя `ipauser2`.
`ipa hbacrule-add-user ipauser2_flydm --users=ipauser2`
 - Добавить в правило `flydm` хост `c1.astra.test`.
`ipa hbacrule-add-host ipauser2_flydm \`
`--hosts=c1.astra.test`
 - Добавить в правило `flydm` службу `fly-dm`.
`ipa hbacrule-add-service ipauser2_flydm --hbacsvcs=fly-dm`
- 4 Просмотреть правило `flydm`.
`ipa hbacrule-show ipauser2_flydm`
- 5 Отключить правило `allow_all`.
`ipa hbacrule-disable allow_all`
- 6 Зайти под учетными записями `ipauser1` и `ipauser2` на хостах `s1.astra.test` и `c1.astra.test` через графический вход.
- 7 Сделать попытку зайти пользователем `ipauser2` в `c1.astra.test` через виртуальный терминал.

Настройка правил SUDO

Задание: Создать SUDO-правила, которое разрешает пользователю `ipauser2` просматривать журнальный файл `/var/log/auth.log` с помощью команды `cat` на хосте `c1.astra.test`. Задание можно выполнить как из веб-консоли, так и с помощью консольных утилит.

- 1 Проверить, что пользователь `ipauser2` не может просмотреть файл `/var/log/auth.log` на хосте `c1.astra.test`.
- 2 Добавить команду для просмотра файла `/var/log/auth.log` в список SUDO-команд.
`ipa sudocmd-add "/usr/bin/cat /var/log/auth.log"`
- 3 Создать «пустое» правило `ipauser2_sudo`

- ipa sudorule-add ipauser2_sudo**
4. Добавить в SUDO-правило пользователя ipauser2.
- ipa sudorule-add-user ipauser2_sudo --users=ipauser2**
5. Добавить в SUDO-правило хост c1.astra.test
- ipa sudorule-add-host ipauser2_sudo --hosts=c1.astra.test**
6. Добавить в SUDO-правило команду
- ipa sudorule-add-allow-command ipauser2_sudo **
--sudocmds='/usr/bin/cat /var/log/auth.log'
7. Добавить в SUDO-правило имя учетной записи пользователя (root), от имени которого будет выполняться команда.
- ipa sudorule-add-runasuser ipauser2_sudo --users=root**
8. Добавить в SUDO-правило параметр, который позволяет выполнять команду без ввода пароля.
- ipa sudorule-add-option ipauser2_sudo **
--sdooption='!authenticate'
9. Проверить, что созданное правило позволяет пользователю ipauser2 на хосте c1.astra.test просматривать файл /var/log/auth.log
- sudo cat /var/log/auth.log**

Регистрация сетевых служб во FreeIPA (SQUID) (опциональное)

Задание: Ввести хост infra в домен astra.test. Настроить Kerberos-аутентификацию на прокси-сервере infra.astra.test, которая позволяет получать доступ к прокси-серверу только доменным пользователям.

1. На VM infra выполнить следующее:
- Изменить имя хоста.
- sudo hostnamectl set-hostname infra.astra.test**
- Внести изменения в /etc/hosts:
- ```
127.0.0.1 localhost
10.0.1.254 infra.astra.test infra
```
- На сетевом интерфейсе net1 запретить автоматическое получение адреса DNS-сервера по DHCP и добавить DNS-сервер 10.0.1.1 (s1.astra.test).

```
nmccli con mod net1 ipv4.ignore-auto-dns yes \
 ipv4.dns 10.0.1.1
nmccli con up net1
```

- На кэширующем DNS сервере (BM infra) настроить ретрансляцию запросов на внешний DNS 8.8.8.8. Внести соответствующие изменения в файле /etc/bind/named.conf.options:

```
forwarders {
 8.8.8.8;
};
sudo systemctl restart bind9
```

- Убедиться, что разрешаются как внешние DNS имена, так и имена в домене astra.test.

```
nslookup www.astralinux.ru
nslookup s1.astra.test
```

- Установить клиент FreeIPA.

```
sudo apt install astra-freeipa-client
```

- Запустить клиент FreeIPA (ввести хост infra в домен astra.test).

```
sudo astra-freeipa-client -d astra.test
sudo reboot
```

- 2 Проверить, что хост infra введен в домен astra.test.

```
ipa host-show infra.astra.test
```

- 3 Зарегистрировать службу squid в домене.

```
ipa service-add HTTP/infra.astra.test
```

- 4 На прокси-сервере infra.astra.test выполнить следующие действия:

- Создать файл /etc/squid/squid.keytab с ключом для службы squid.

```
sudo ipa-getkeytab -s s1.astra.test \
 -p HTTP/infra.astra.test -k /etc/squid/squid.keytab
```

- Назначить на файл /etc/squid/krb5.keytab владельца проху и группу-владельца проху, задать права доступа 640.

```
sudo chown proxy:proxy /etc/squid/squid.keytab
sudo chmod 640 /etc/squid/squid.keytab
```

- В файле /etc/squid/squid.conf настроить аутентификацию SQUID через Kerberos:

- Закомментировать строку, содержащую разрешающее правило для localnet.

**#http\_access allow 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 доменным пользователям (настроить аутентификацию SQUID через Kerberos).

```
auth_param negotiate program
/usr/lib/squid/negotiate_kerberos_auth -s } → Одна строка
HTTP/infra.astra.test -k
/etc/squid/squid.keytab
auth_param negotiate children 10
auth_param negotiate keep_alive on
acl kerb_users proxy_auth REQUIRED
http_access allow kerb_users
```

- Перезапустить `systemd` и службу `squid` (может занять продолжительное время) и убедиться, что служба `squid` была запущена успешно.

```
sudo systemctl daemon-reload
sudo systemctl restart squid
sudo systemctl status squid
```

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

- Зайти под локальной учетной записью администратора (`sa`).
- Проверить, что внешние DNS имена и имена из домена `astra.test` разрешаются.

```
nslookup www.astralinux.ru
nslookup infra.astra.test
```

- В браузере Firefox настроить прокси для доступа в Интернет (ручная настройка прокси): `infra.astra.test`, порт 3128, установить параметр «Также использовать этот прокси для HTTPS», в поле «Не использовать прокси для» указать `10.0.1.0/24`.
- В адресной строке браузер Firefox ввести `www.astralinux.ru` и сделать попытку зайти на сайт.

- Зайти под доменной учетной записью `iprauser2` с нулевым уровнем конфиденциальности.
  - Настроить в браузере Firefox прокси таким же образом, как и для локального пользователя `sa`, и зайти на сайт `www.astralinux.ru`.
- 6 После выполнения задания отключить на прокси-сервере Kerberos-аутентификацию и разрешить всем хостам их сети `10.0.1.0/24` получать доступ к прокси-серверу.

## Установка реплики FreeIPA

Задание: Создать VM `s2` и увеличить RAM до 3ГБ, а количество ядер до 3х. Настроить имя хоста (`s2.astra.test`) и сетевые параметры интерфейса (`10.0.1.2/24`, шлюз `10.0.1.254` и DNS-сервер `10.0.1.1`). Внести информацию об имени адресе хоста `s2.astra.test` в файл `/etc/hosts`. Настроить доступ к репозиториям ПО с помощью прокси-сервера `infra`. Установить серверное ПО FreeIPA. Изменить DNS-сервер на локальный хост. Развернуть реплику FreeIPA.

- 1 Создать новую VM `s2` с помощью клонирования `template_1704_3`. Увеличить количество процессоров до 3х. Увеличить объем RAM до 3ГБ. Сетевая карта - одна, подключена к внутренней сети. Запустить VM.

- 2 Изменить имя хоста на `s2.astra.test`.

```
sudo hostnamectl set-hostname 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`).

```
nmcli con mod Проводное\ соединение\ 2 con-name net1
nmcli con mod net1 ipv4.addresses 10.0.1.2/24 ipv4.dns
10.0.1.1 \ipv4.gateway 10.0.1.254 ipv4.method manual
nmcli con up net1
```

- 4 Добавить в `/etc/hosts` запись о `s2.astra.test`.

```
127.0.0.1 localhost localhost.localdomain
10.0.1.2 s2.astra.test s2
```

- 5 Проверить доступность VM `s1.astra.test`.

```
ping 10.0.1.1
```

- 6 Настроить доступ к репозиториям Astra Linux, используя прокси-сервер, развернутый на хосте `infra`.

- 7 Обновить кэш с метаданными репозиториями.

```
sudo apt update
```

- 8 Установить пакет dnstools.
- ```
sudo apt install dnstools
```
- 9 Проверить разрешение имени сервера s1.astra.test в DNS.
- ```
nslookup s1.astra.test
```
- 10 Установить клиент FreeIPA.
- ```
sudo apt install astra-freeipa-client
```
- 11 Запустить клиент FreeIPA.
- ```
sudo astra-freeipa-client -d astra.test
```
- 12 Перезагрузить хост s2.astra.test.
- 13 На сервере FreeIPA s1.astra.test проверить, что хост s2.astra.test добавлен в домен.
- ```
ipa host-show s2.astra.test
```
- или
- в веб-консоли <https://s1.astra.test> Идентификация→Узлы.
- 14 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.
- ```
sudo astra-freeipa-server-crt --host s2.astra.test \
--export --push admin@10.0.1.2 --pin пароль --48
```
- 15 На сервере FreeIPA s1.astra.test создать PTR запись для s2.astra.test, или из веб-консоли, или с помощью команды ipa dnsrecord-add.
- ```
ipa dnsrecord-add 1.0.10.in-addr.arpa 2 \
--ptr-rec s2.astra.test.
```
- 16 На хосте s2.astra.test установить серверное программное обеспечение FreeIPA.
- ```
sudo apt install astra-freeipa-server
```
- 17 На хосте s2.astra.test запустить реплику FreeIPA, указав имя файла с сертификатом.
- ```
sudo astra-freeipa-replica -a ~admin/s2.astra.test.p12 \
--pin пароль
```
- 18 На s2.astra.test изменить DNS сервер на 127.0.0.1:
- ```
nmcli con mod net1 ipv4.dns 127.0.0.1
nmcli con up net1
```



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

### Настройка синхронизации времени в домене (опционально).

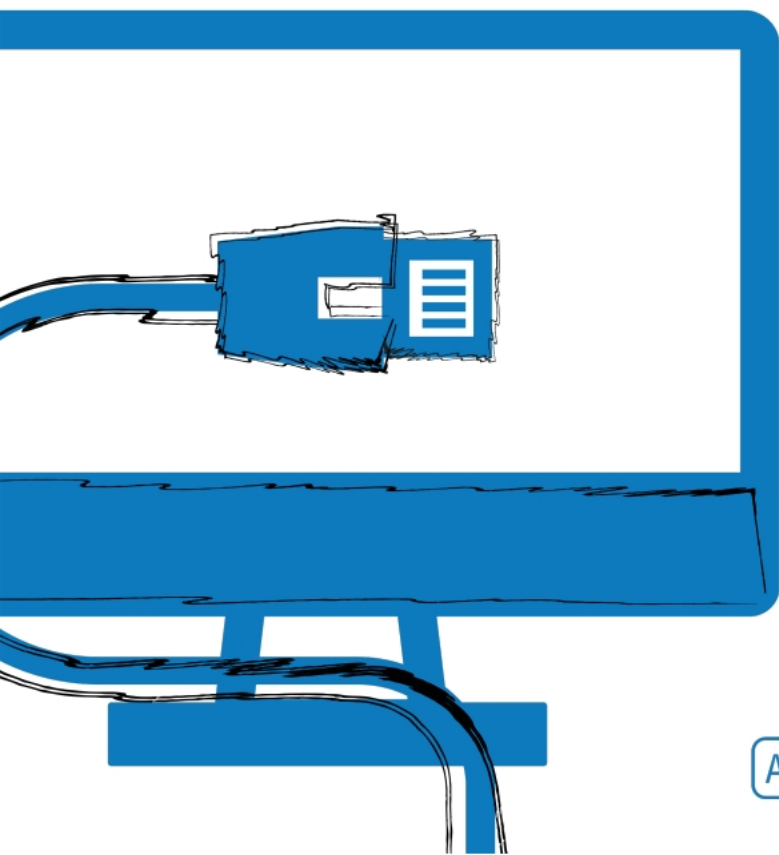
Задание: Используя ВМ `infra` как управляющий хост, написать и выполнить `playbook`, который передает на все хосты домена конфигурационный файл для службы `chrony`. В качестве источника времени использовать хост `infra.astra.test`.

- 1 На ВМ `infra` зайти под учетной записью локального или доменного администратора.
- 2 Настроить аутентификацию по ключам для SSH-серверов `s1.astra.test`, `s2.astra.test`, `c1.astra.test`.
- 3 Создать конфигурационный файл для службы `chrony`, в котором в качестве источника времени указать сервер `infra.astra.test` (10.0.1.254).
- 4 Создать и выполнить плейбук, который скопирует созданный конфигурационный файл на хосты `s1`, `s2`, `c1` и перезапустит на них службу `chrony`.



## Модуль 9

### Веб-сервер на основе Apache



# Сборник практических заданий для курса «AL-1704. Сетевое администрирование ОС Astra Linux Special Edition 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

## Материалы:

- Эталонная виртуальная машина template\_1704\_3:
  - Процессор — 1.
  - RAM — 2 ГБ.
  - Диск — 30 ГБ.
  - Сетевой адаптер — тип подключения «Сетевой мост».
  - ОС — Astra Linux Special Edition 1.7.3 (максимальный уровень защищенности) с установленными дополнениями VirtualBox для гостевых ОС.

## Дополнительная информация:

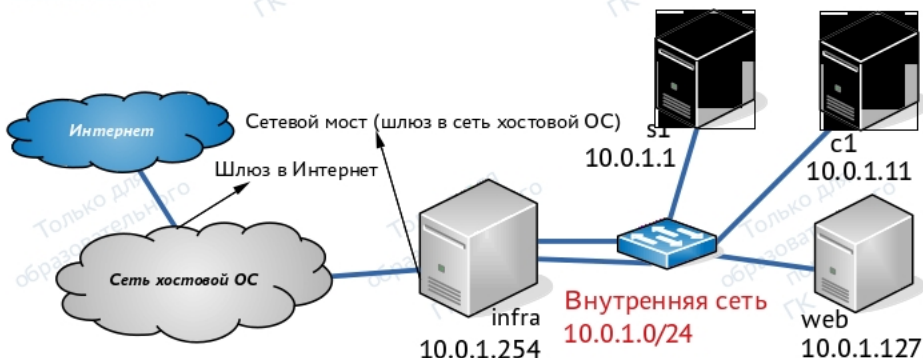
- Настройки эталонной виртуальной машине предполагают, что репозитории Astra Linux 1.7.3 доступны через Интернет.
- В учебном центре репозитории могут располагаться на внутренних ресурсах УЦ. В этом случае в эталонную ВМ должны быть внесены соответствующие изменения.

## Модуль 9. Веб-сервер на основе Apache

### Описание практического задания

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

### Схема сети



### Действия, которые следует выполнить перед началом выполнения заданий

Если в практической работе по модулю 8 не было выполнено опциональное задание, в котором хост infra вводился как клиент в домен, то следует на хосте infra:

- 5 Указать в сетевом соединении net1 в качестве DNS-сервера s1.astra.test (10.0.1.1) и сделать A-запись для infra.astra.test.

```
nmcli con mod net1 ipv4.ignore-auto-dns yes \
 ipv4.dns 10.0.1.1
nmcli con up net1
```

- 6 На кэширующем DNS сервере (BM infra) настроить ретрансляцию запросов на внешний DNS 8.8.8.8. Внести соответствующие изменения в файле /etc/bind/named.conf.options:

```
forwarders {
 8.8.8.8;
};
sudo systemctl restart bind9
```

## Настройка Apache2 на VM infra

**Задание:** Установить Apache2. Создать и активировать конфигурационный файл для отключения режима AstraMode. Настроить виртуальный веб-сервер infra.astra.test. Файлы виртуального веб-сервера infra.astra.test разместить в каталоге /var/www/infra. Отключить виртуальный веб-сервер, активированный по умолчанию во время установки Apache2. Установить модуль Apache для поддержки PHP.

- 1 Установить apache2 на VM infra.

```
sudo apt install apache2
```

- 2 Создать конфигурационный файл astramode\_off.conf в каталоге /etc/apache2/conf-available, в котором настроить отключение режима AstraMode.

```
AstraMode off
```

- 3 Отключить режим AstraMode, активировав настройку из файла astramode\_off.conf.

```
sudo a2enconf astramode_off
sudo systemctl reload apache2
```

- 4 В конфигурационный файл виртуального веб-сервера по умолчанию /etc/apache2/sites-available/000-default.conf добавить параметр:  
ServerName 10.0.1.254

- 5 Создать конфигурационный файл виртуального веб-сервера infra.astra.test в /etc/apache2/sites-available путем копирования файла 000-default.conf в файл infra.conf.

```
cd /etc/apache2/sites-available
sudo cp 000-default.conf infra.conf
```

- 6 Отредактировать конфигурационный файл и виртуального веб-сервера infra.astra.test, указав доменное имя сервера infra.astra.test в параметре ServerName и путь к каталогу с веб-страницами /var/www/infra.

```
ServerName infra.astra.test
ServerAdmin webmaster@localhost
DocumentRoot /var/www/infra
```

- 7 Создать каталог для размещения веб-страниц сайта `infra.astra.test`.  
**`sudo mkdir /var/www/infra`**
- 8 Разместить в созданном каталоге веб-страницу `index.html` 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 `infra.astra.test`.
`sudo a2ensite infra`
`sudo systemctl reload apache2`
- 10 В браузере получить доступ к настроенным сайтам, набрав в адресной строке браузера <http://infra.astra.test> и <http://10.0.1.254>.
- 11 Деактивировать виртуальный веб-сервер по умолчанию и снова в адресной строке браузера набрать <http://infra.astra.test> и <http://10.0.1.254>
`sudo a2dissite 000-default.conf`
`sudo systemctl reload apache2`
- 12 Установить php и модуль php для Apache2.
`sudo apt install php libapache2-mod-php`
- 13 Проверить версию php:
`php -v`
- 14 Создать в каталоге виртуального хоста `infra.astra.test` файл `info.php` с содержимым:
- ```
<?php
phpinfo();
?>
```
- 15 Проверить в браузере отображение страницы, сгенерированной `info.php`.

## Настройка самоподписанных сертификатов (опциональное задание)

**Задание:** Создать самоподписанный сертификат для веб-сайта `infra.astra.test`. Настроить веб-сайт `infra.astra.test` для работы с использованием протокола TLS (SSL).

- 1 Создать удостоверяющий центр – CA (Certification Authority):  

```
sudo -i
cd /etc/apache2/
mkdir ssl
chmod 700 ssl
cd ssl
openssl genrsa -des3 -out my-ca.key
```
- 2 Создать сертификат для удостоверяющего центра:  

```
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.  

```
DNS.1 = infra.astra.test
DNS.2 = www.infra.astra.test
DNS.3 = *.infra.astra.test
```
- 6 Создать файл ключа для веб-сервера (размер ключа - 2048 бита):  

```
openssl genrsa -des3 -out my-apache.key 2048
```
- 7 Удалить пароль из файла ключа веб-сервера:  

```
openssl rsa -in my-apache.key -out new.my-apache.key
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:  
`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.  
`sudo chmod 400 *.key`
- 11 Назначить каталогу /etc/apache2/ssl и файла внутри этого каталога владельца www-data и группу-владельца www-data.  
`sudo chown -R www-data:www-data /etc/apache2/ssl`
- 12 Отредактировать файл /etc/apache2/sites-available/default-ssl.conf:  
`SSLCertificateFile /etc/apache2/ssl/my-apache.crt`  
`SSLCertificateKeyFile /etc/apache2/ssl/my-apache.key`  
`SSLCACertificateFile /etc/apache2/ssl/my-ca.crt`
- 13 Активировать модуль mod\_ssl.  
`sudo a2enmod ssl`
- 14 Активировать сайт, настройки которого хранятся в конфигурационном файле default-ssl.conf.  
`sudo a2ensite default-ssl.conf`
- 15 Перезапустить службу apache2.  
`sudo systemctl restart apache2`
- 16 Проверить работоспособность сайта – ввести в адресную строку браузера `https://infra.astra.test`.

## Настройка VM web

**Задание:** Создать VM web. Настроить VM web: имя хоста – `web.astra.test`, IP адрес – `10.0.1.127/24`, шлюз – `10.0.1.254`, DNS-сервер – `10.0.1.1`. Внести информацию об имени и адресе хоста в /etc/hosts. Ввести хост `web.astra.test` в домен.

- 1 Клонировать VM template\_1704\_3 и назвать новую виртуалку web.
- 2 Запустить виртуалку.

- 3 Сменить имя хоста на web.

```
sudo hostnamectl set-hostname web.astra.test
```

- 4 Поправить /etc/hosts, добавив соответствие доменного имени машины и ее IP-адреса.

```
127.0.0.1 localhost
10.0.1.127 web.astra.test web
```

- 5 Остановить и запретить запуск Network Manager.

```
sudo systemctl stop NetworkManager
sudo systemctl mask NetworkManager
```

- 6 Настроить сетевой интерфейс eth0 с IP-адресом 10.0.1.127 в файле /etc/network/interfaces.

```
auto eth0
iface eth0 inet static
address 10.0.1.127/24
gateway 10.0.1.254
```

- 7 Указать IP-адрес DNS-сервера 10.0.1.1 в файле /etc/resolv.conf.

```
nameserver 10.0.1.1
```

- 8 Перезапустить службу и проверить настройки и доступность шлюза.

```
sudo systemctl restart networking
ip a
ping 10.0.1.254
```

- 9 Настроить работу apt через прокси-сервер infra.astra.test.

- 10 Обновить локальный кэш с метаданными репозиторияев.

```
sudo apt update
```

- 11 Установить клиент FreeIPA.

```
sudo apt install astra-freeipa-client
```

- 12 Ввести BM web в домен.

```
sudo astra-freeipa-client -d astra.test
```

- 13 Перезагрузить BM web.

```
sudo systemctl reboot
```

- 14 Проверить, что хост web.astra.test введен в домен.

```
ipa host-show web.astra.test
```

## Настройка Kerberos авторизации веб-сервера Apache в домене FreeIPA

Задание: Установить Apache и модуль Kerberos-аутентификации для Apache на хосте web.astra.test. Зарегистрировать веб-службу, работающую на хосте web.astra.test, в домене. Разместить файл с ключом для веб-службы на хосте web.astra.test. Настроить Kerberos-аутентификацию для сайта по умолчанию ().

- 1 Зайти на ВМ web под учетной записью доменного администратора.
- 2 На ВМ web установить apache2 и модуль аутентификации через Kerberos.

```
sudo apt install apache2 libapache2-mod-auth-gssapi
```

- 3 Зарегистрировать веб-службу web.

```
ipa service-add HTTP/web.astra.test@ASTRA.TEST
```

- 4 В ВМ web записать ключи для веб-службы в файл /etc/apache2/keytab.

```
sudo ipa-getkeytab -p HTTP/web.astra.test@ASTRA.TEST \
-k /etc/apache2/keytab
```

- 5 Установить права и владельца на файл keytab.

```
sudo chown www-data:www-data /etc/apache2/keytab
sudo chmod 640 /etc/apache2/keytab
```

- 6 Настроить Kerberos-аутентификацию на веб-сервере, включив секцию <Directory> в конфигурационный файл виртуального веб-сервера /etc/apache2/sites-enabled/000-default.conf.

```
<Directory /var/www/html>
AuthType Kerberos
KrbAuthRealms ASTRA.TEST
KrbServiceName HTTP/web.astra.test@ASTRA.TEST
Krb5Keytab /etc/apache2/keytab
KrbMethodNegotiate on
KrbMethodK5Passwd off
require valid-user
KrbSaveCredentials on
</Directory>
```

- 7 Перезапустить веб-сервер.

```
sudo systemctl restart apache2
```

## Создание веб-страниц с разными уровнями конфиденциальности в BM web

**Задание:** На хосте web.astra.test назначить метку безопасности на каталоги /var/www и /var/www/html: уровень конфиденциальности – 2, все категории, уровень мандатной целостности – 63, дополнительный атрибут – 63.

В каталоге /var/www/html создать две веб-страницы с разными уровнями конфиденциальности level1.html – уровень конфиденциальности 1 и level2.html – уровень конфиденциальности – 2.

- 1 В BM web установить уровень конфиденциальности 2 и атрибут ccnr на каталоги /var/www, /var/www/html

```
sudo pdpl-file 2:63:-1:ccnr /var/www
sudo pdpl-file 2:63:-1:ccnr /var/www/html
```

- 2 Перейти в каталог /var/www/html.

```
cd /var/www/html
```

- 3 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).

```
sudo -i
echo '<h1>LEVEL1</h1>' > level1.html
echo '<h1>LEVEL TWO</h1>' > level2.html
exit
```

- 4 Назначить созданным файлам соответствующие уровни конфиденциальности.

```
sudo pdpl-file 1:0:0 level1.html
sudo pdpl-file 2:0:0 level2.html
```

- 5 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

**Задание:** Зайти под учетными записями ipauser1 и ipauser2 с разными уровнями конфиденциальности, настроить браузер Firefox для поддержки Kerberos-аутентификации и вывести содержимое страниц level1.html и level2.html.

- 1 Зайти на c1 по очереди: локальным пользователем sa, доменными пользователями ipaser1, ipauser2 (с уровнями конфиденциальности 0,1,2).

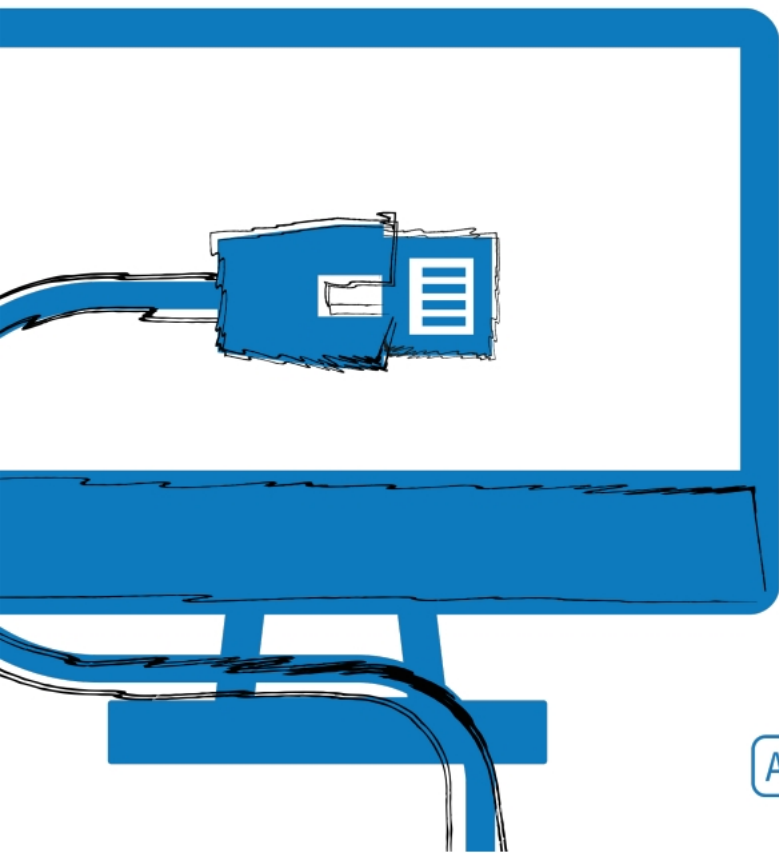
## 2 Настроить поддержку Kerberos-аутентификацию в Firefox:

- 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 браузер на страницы <http://web.astra.test>, <http://web.edu.test/level1.html>, <http://web.astra.test/level2.html>. Сравнить результаты при входе разными пользователями с разными уровнями конфиденциальности.

## Модуль 10

### Система электронной почты на базе Exim и Dovecot



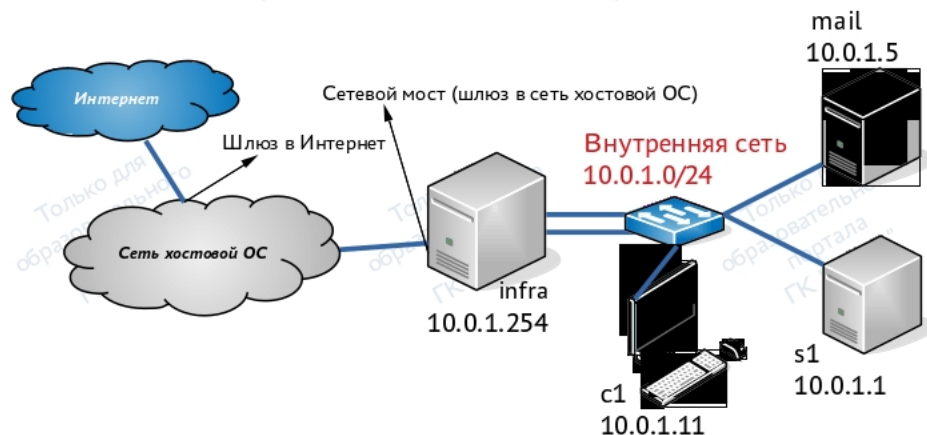


## Модуль 10. Система электронной почты на базе Exim и Dovecot

### 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

**Задание:** Создать ВМ mail. Настроить ВМ mail: имя хоста - mail.astra.test, IP адрес - 10.0.1.5/24, шлюз - 10.0.1.254, DNS-сервер - 10.0.1.1. Внести информацию об имени и адресе хоста в /etc/hosts. Ввести хост mail.astra.test в домен.

- 4 Создать ВМ mail путем клонирования ВМ template\_1704\_3. Запустить ВМ и зайти под учетной записью локального администратора (sa).
- 5 Изменить имя хоста на mail.astra.test.

```
sudo hostnamectl set-hostname mail.astra.test
```

- 6 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).

```
nmcli con mod Проводное\ соединение\ 2 con-name net1
nmcli con mod net1 ipv4.addresses 10.0.1.5/24 ipv4.dns
10.0.1.1 \
 ipv4.gateway 10.0.1.254 ipv4.method manual
nmcli con up net1
```

- 7 Проверить доступность сервера FreeIPA s1.astra.test.

```
ping 10.0.1.1
```

- 8 Настроить доступ к репозиториям через прокси-сервер infra.astra.test.

- 9 Обновить кэш с метаданными репозитория.

```
sudo apt update
```

- 10 Установить пакет dnsutils.

```
sudo apt install dnsutils
```

- 11 Проверить разрешение имени сервера в DNS.

```
nslookup s1.astra.test
```

- 12 Внести изменения в файл /etc/hosts:

```
127.0.0.1 localhost
10.0.1.5 mail.astra.test mail
```

- 13 Установить клиент FreeIPA.

```
sudo apt install -yq astra-freeipa-client
```

- 14 Запустить клиент FreeIPA.

```
sudo astra-freeipa-client -d astra.test
```

- 15 Перезагрузить mail.astra.test.

- 16 Проверить, что хост mail.astra.test введен в домен.

```
ipa host-show mail.astra.test
```

или в веб-консоли <https://s1.astra.test> Идентификация–Узлы

## Установка программного обеспечения и первоначальная настройка

Задание: Установить exim4 и dovecot. Произвести первоначальную настройку exim4 (метод доставки локальной почты - maildir).

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

```
sudo apt install exim4-daemon-heavy dovecot-imapd dovecot-gssapi
```

- 2 Произвести первоначальную настройку exim4.

```
sudo dpkg-reconfigure exim4-config
```

- 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

**Задание:** зарегистрировать в домене службы exim4 (smtp) и dovecot (imap). На почтовом сервере mailastra.test создать keytab-файл с ключами для smtp и imap служб. Добавить MX-запись в зону DNS astra.test. Настроить Kerberos-аутентификацию для служб smtp и imap.

- 1 Зарегистрировать почтовые службы smtp (exim4) и imap (dovecot), которые будут работать на хосте mail.astra.test.

```
ipa service-add imap/mail.astra.test@ASTRA.TEST
ipa service-add smtp/mail.astra.test@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 файл с ключами для почтовых служб /var/lib/dovecot/dovecot.keytab.

```
sudo ipa-getkeytab -p imap/mail.astra.test@ASTRA.TEST \
-k /var/lib/dovecot/dovecot.keytab
sudo ipa-getkeytab -p smtp/mail.astra.test@ASTRA.TEST \
-k /var/lib/dovecot/dovecot.keytab
```

4 Дать пользователю dovecot право на чтение для keytab-файла.  
**sudo setfacl -m u:dovecot:r /var/lib/dovecot/dovecot.keytab**

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.

**sudo systemctl restart dovecot**  
**systemctl status dovecot**

7 Настроить exim4 для аутентификации через Kerberos. На почтовом сервере mail.astra.test создать файл

/etc/exim4/conf.d/auth/22\_exim4-dovecot-kerberos-ips 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.

**sudo systemctl restart exim4**  
**systemctl status exim4**

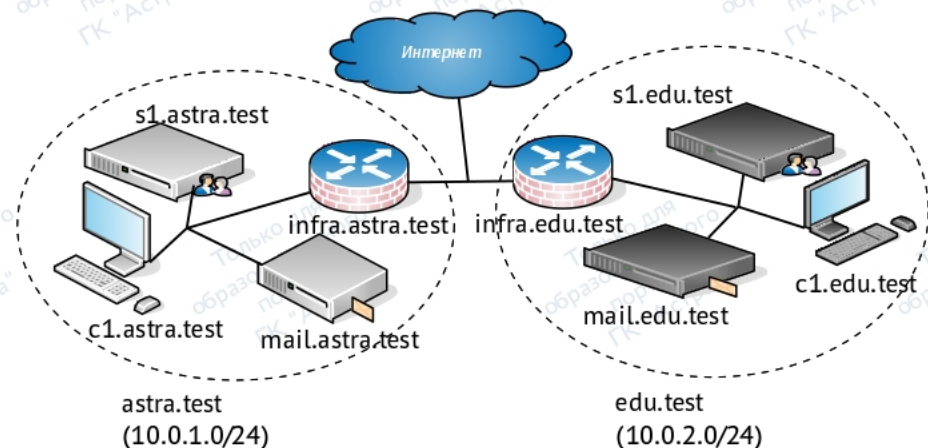
## Настройка почтового клиента «Почта Thunderbird»

**Задание:** зайти под учетными записями пользователей `ipauser1` и `ipauser2` с разными уровнями конфиденциальности, настроить Thunderbird и отправить друг другу почтовые сообщения.

- 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 (опциональное задание)

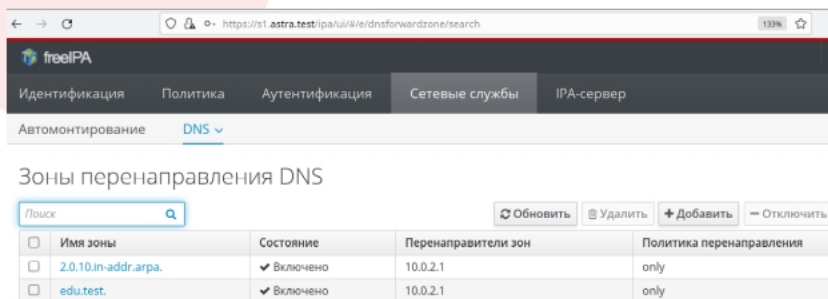
### Схема стенда



- 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).

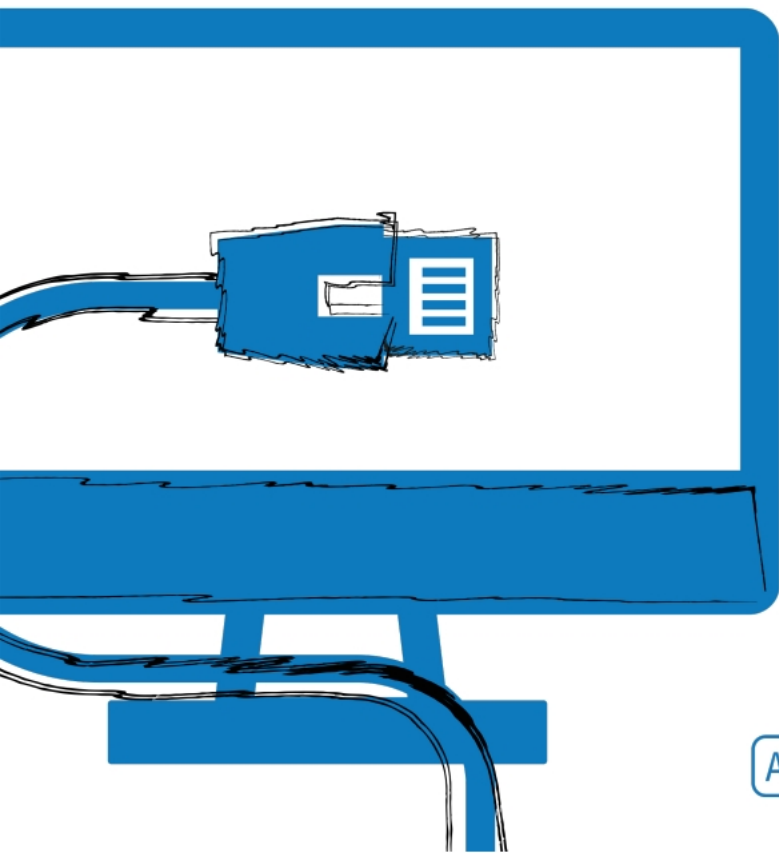


- 3 Проверить на mail.astra.test и mail.edu.test разрешаются ли ресурсные записи DNS типа MX для доменов astra.test и edu.test. Используйте команду nslookup или dig.
- 4 На mail.astra.test разрешить отправку почты (relay) в домен edu.test. Это можно сделать, установив параметр dc\_relay\_domains='edu.test' 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 уровнями конфиденциальности.



## Модуль 11

**Защищенный комплекс  
программ для печати  
и маркировки документов**

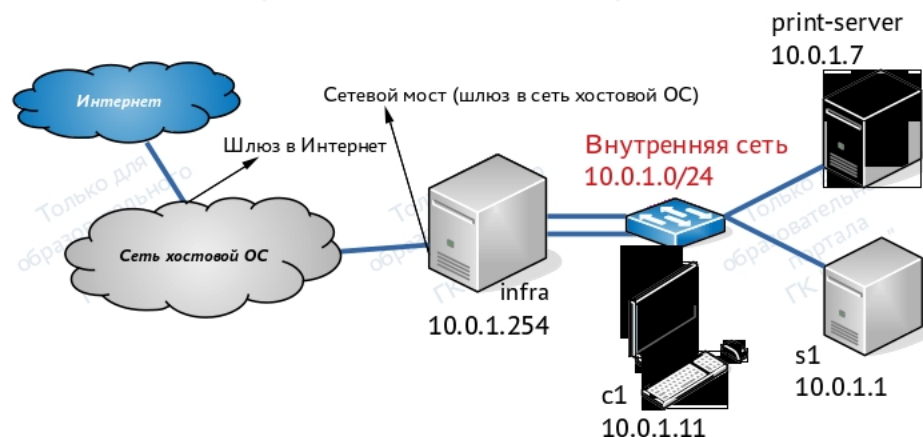


## Модуль 11. Защищенный комплекс программ для печати и маркировки документов

### Описание практического задания

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

### Схема сети



### Создание и настройка VM print-server

**Задание:** Создать VM print-server. Настроить VM print-server: имя хоста – print-server.astra.test, IP адрес – 10.0.1.7/24, шлюз - 10.0.1.254, DNS-сервер – 10.0.1.1. Внести информацию об имени и адресе хоста в /etc/hosts. Настроить доступ к репозиториям через прокси infra.astra.test. Установить драйвер принтера, выводящего документы в pdf-файл.

- 7 Создать VM print-server путем клонирования VM template\_1704\_3. Запустить VM и зайти под учетной записью локального администратора (sa).
- 8 Изменить имя хоста на print-server.astra.test:

```
sudo hostnamectl set-hostname print-server.astra.test
```

- 9 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):

```
nmcli con mod Проводное\ соединение\ 2 con-name net1
nmcli con mod net1 ipv4.addresses 10.0.1.7/24 ipv4.dns
10.0.1.1 \ipv4.gateway 10.0.1.254 ipv4.method manual
nmcli con up net1
```

- 10 Проверить доступность сервера FreeIPA s1.astra.test.

```
ping 10.0.1.1
```

- 11 Внести изменения в файл /etc/hosts:

```
127.0.0.1 localhost
10.0.1.7 print-server.astra.test print-server
```

- 12 Настроить доступ к репозиториям через прокси-сервер infra.astra.test.

- 13 Обновить кэш с метаданными репозиторияев.

```
sudo apt update
```

- 14 Установить пакет dnsutils.

```
sudo apt install dnsutils
```

- 15 Проверить разрешение имени сервера FreeIPA в DNS.

```
nslookup s1.astra.test
```

- 16 Установить драйвер принтера для печати в PDF-файл.

```
sudo apt install printer-driver-cups-pdf
```

## Настройка сервера печати и аутентификации службы печати

**Задание:** Ввести хост print-server в домен astra.test. Создать учетную запись администратора службы печати cups\_admin и включить ее в локальные группы ldapmin и lpnasc. Зарегистрировать службу печати в домене. На сервере печати добавить ключи для службы cups (протокол IPP) в keytab-файл /etc/krb5.keytab. Разрешить службе cups принимать задания от удаленных хостов. Настроить Kerberos-аутентификацию для службы печати и включить поддержку мандатного управления доступом. Настроить принтер так, чтобы pdf-файлы создавались в каталоге /opt/cups-pdf. Разрешить общий доступ к принтеру. Установить принтер для печати в pdf-файл по умолчанию для всех, настроить минимальные и максимальные классификационные метки.

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

```
sudo apt install astra-freeipa-client
sudo astra-freeipa-client -d astra.test
```

- 2 Перезагрузить VM print-server.

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

```
ipa user-add --first "CUPS" --last "Admin" cups_admin
ipa passwd cups_admin
```

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

```
ipa service-add ipp/print-server.astra.test@ASTRA.TEST
```

- 5 Зайти в VM print-server под учетной записью локального администратора (sa) добавить ключ для службы CUPS в keytab-файл /etc/krb5.keytab.

```
sudo ipa-getkeytab \
-p ipp/print-server.astra.test@ASTRA.TEST \
-k /etc/krb5.keytab
```

- 6 Включить доменного пользователя cups\_admin в локальные группы lpadmin и lpmac и проверить успешность выполнения этих действий.

```
sudo usermod -aG lpadmin cups_admin
sudo usermod -aG lpmac cups_admin
id cups_admin
```

- 7 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.

```
sudo cupsctl --remote-admin --share-printers --remote-any
sudo cupsctl ServerAlias=*
sudo cupsctl ServerName=print-server.astra.test
```

- 8 Настроить аутентификацию службы CUPS через Kerberos и включить поддержку мандатного управления доступом. Внесите следующие изменения в настройки CUPS:

```
sudo cupsctl DefaultPolicy=parsec
sudo cupsctl MacEnable=On
sudo cupsctl DefaultAuthType=Negotiate
```

- 9 В файле /etc/cups/cupsd.conf заменить строку Port 631

```
на
Listen 0.0.0.0:631
```

- 10 Командой `cupscctl` параметр `MarkerUser` установить в значение `ipp`.

**`sudo cupscctl MarkerUser=ipp`**

- 11 Создайте каталог `/opt/cups-pdf`.

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

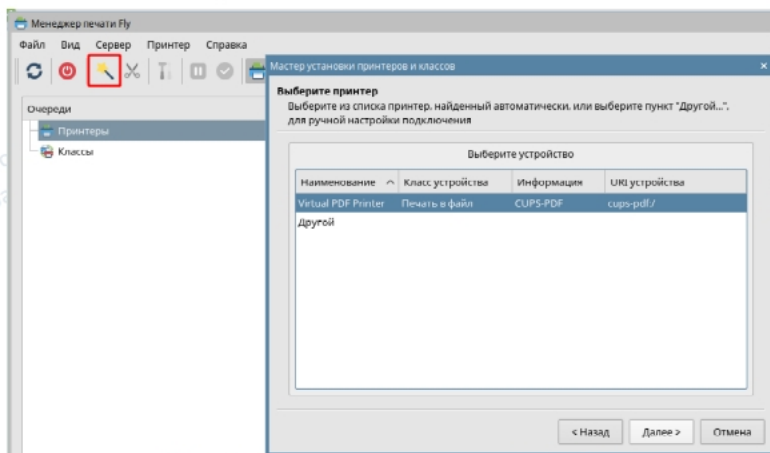
- 13 Перезапустить службу CUPS.

**`sudo systemctl restart cups`**

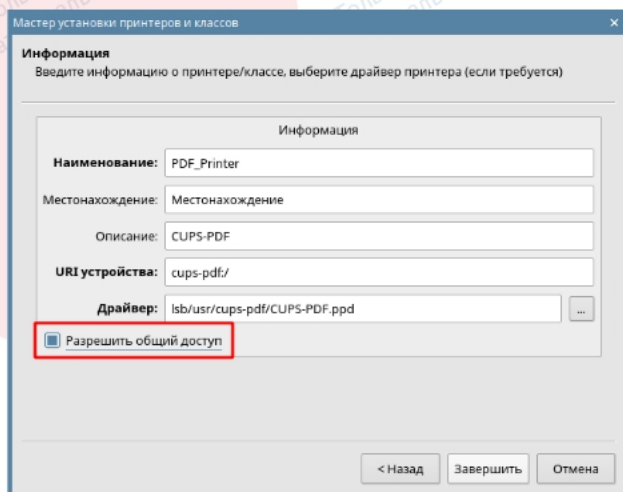
- 14 Зайти в VM `print-server` под доменной учетной записью `cups_admin`.

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

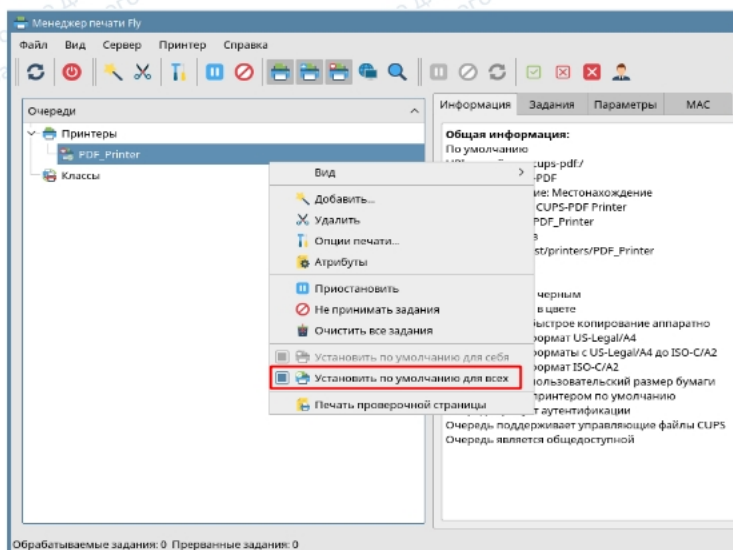
- 16 Нажать кнопку «Добавить ...» на панели инструментов. В появившемся окне «Мастера установки принтеров и классов» выбрать обнаруженный принтер и нажать кнопку «Далее».



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

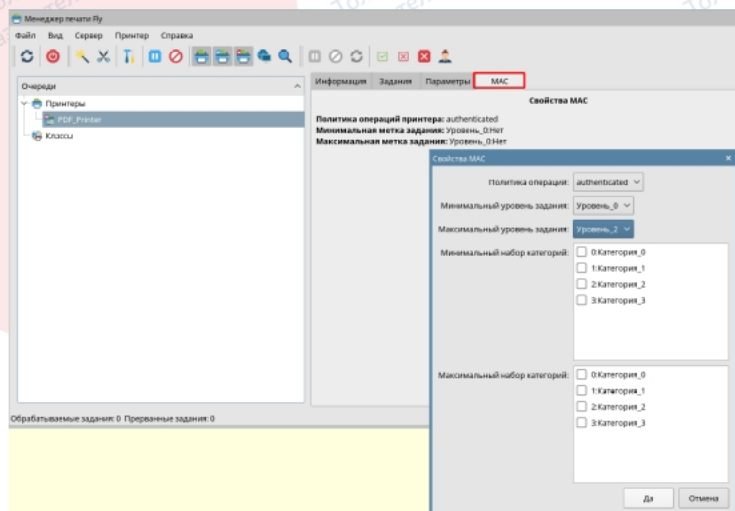


18 Назначить установленный принтер как принтер по умолчанию для всех.

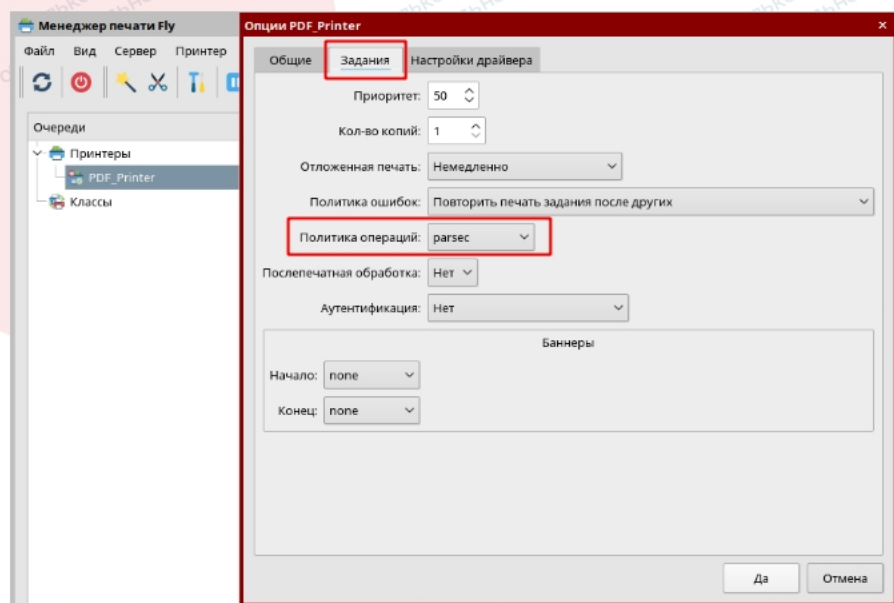


19 На вкладке «MAC» ввести минимальную и максимальную метки для заданий. Установить минимальный уровень — 0, максимальный — 2.





- 20 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 «pagesec».



## Настройка клиента службы печати, печать файлов

**Задание:** Настроить на хосте c1.astra.test клиентскую часть службы печати. Отправить несколько заданий, входя в сеанс под учетной записью доменного пользователя ipauser2 с нулевой и ненулевыми метками безопасности. Зайти на сервер печати под учетной записью cups-admin и произвести маркировку заданий на печать с помощью программы fly-print-station.

- 1 Зайти под учетной записью локального администратора (sa) на VM c1.astra.test.
- 2 В файле /etc/cups/client.conf определить параметр ServerName, присвоив значение равное DNS имени сервера печати.

**ServerName print-server.astra.test**

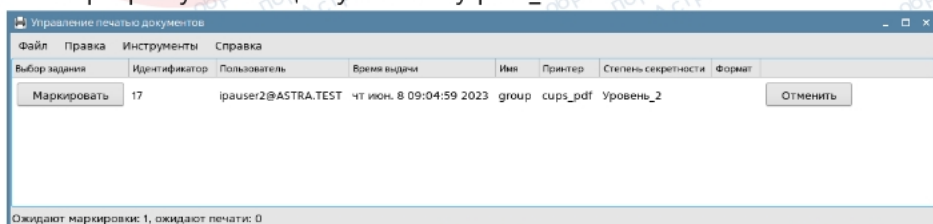
- 3 В командной строке проверить доступность сетевого принтера.

**lpstat -t**

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

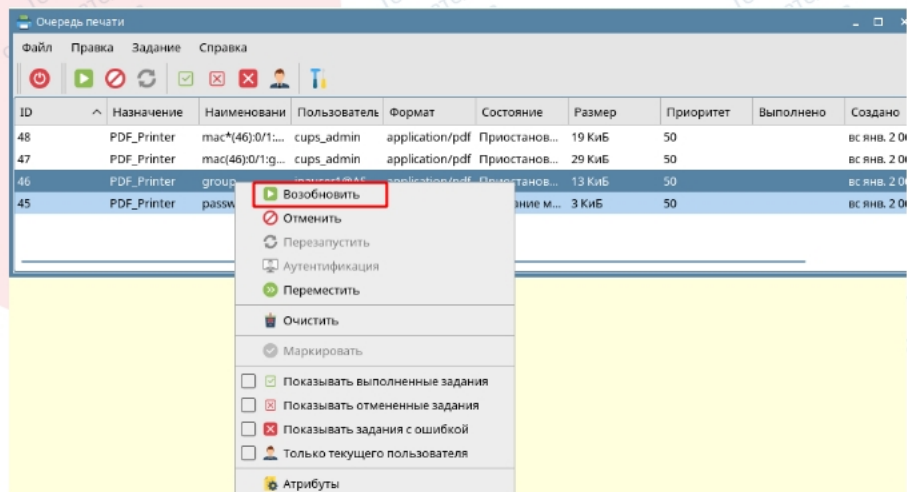
**lp /etc/cups/client.conf**

- 5 Зайти на ВМ c1.astra.test под доменной учетной записью пользователя ipauser2 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 ipauser2 с уровнем конфиденциальности 1.
- 8 Напечатать с помощью утилиты командной строки файл /etc/passwd.  
**lp /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-print\_station.



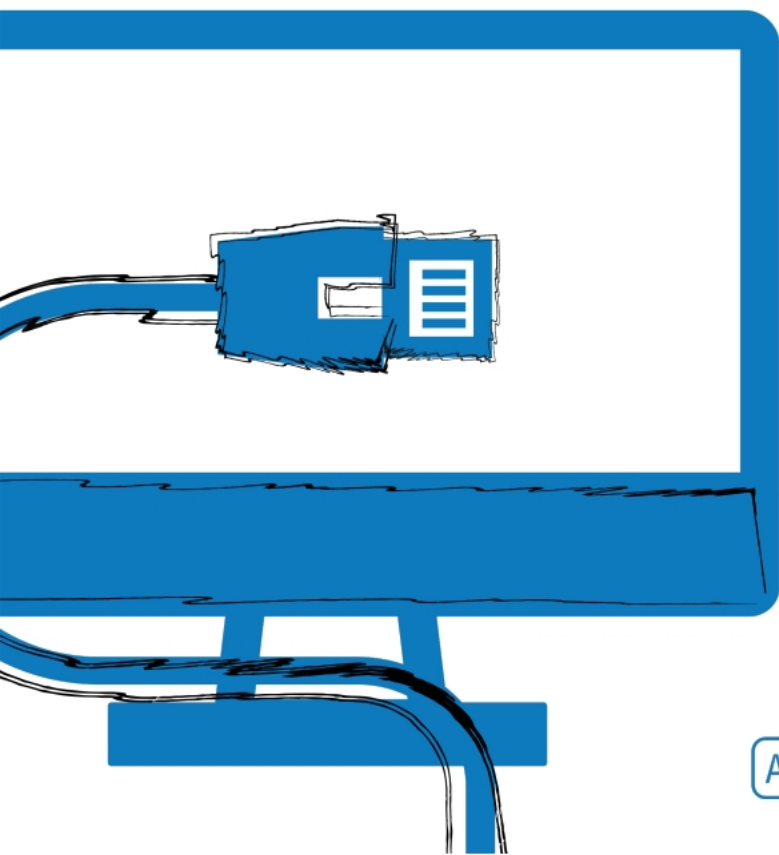
- 11 После выполнения маркировки задания в контекстном меню задания выбрать пункт «Возобновить», чтобы распечатать документ.

**Примечание:** кроме основного задания, маркировка создаст еще два дополнительных задания. Для возобновления печати следует выбрать основное задание.



## Модуль 12

### Установка Astra Linux по сети



# Сборник практических заданий для курса «AL-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

## Материалы:

- Эталонная виртуальная машина template\_1704\_3:
  - Процессор — 1.
  - RAM — 2 ГБ.
  - Диск — 30 ГБ.
  - Сетевой адаптер — тип подключения «Сетевой мост».
  - ОС — Astra Linux Special Edition 1.7.3 (максимальный уровень защищенности) с установленными дополнениями VirtualBox для гостевых ОС.

## Дополнительная информация:

- Настройки эталонной виртуальной машине предполагают, что репозитории Astra Linux 1.7.3 доступны через Интернет.
- В учебном центре репозитории могут располагаться на внутренних ресурсах УЦ. В этом случае в эталонную ВМ должны быть внесены соответствующие изменения.



## Модуль 12. 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 Astra Linux

**Задание:** На VM **infra** создать образ загрузочного компакт-диска с ОС Astra Linux. Настроить автоматическое монтирование образа загрузочного диска в каталог `/var/www/infra/astra`.

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

13 Создать образ загрузочного компакт-диска с именем `/iso/1.7.3.iso`.

```
sudo mkdir /iso
sudo dd if=/dev/sr0 of=/iso/1.7.3.iso status=progress
```

14 Добавить строку в файл `/etc/fstab` для постоянного монтирования образа дистрибутива в `/var/www/infra/astra`.

```
sudo mkdir /var/www/infra/astra
/iso/1.7.3.iso /var/www/infra/astra udf,iso9660
ro,loop,auto 0 0
```

15 Выполнить монтирование до перезагрузки.

**sudo mount -a**

## Установка и настройка TFTP-сервера

**Задание:** Установить TFTP-сервер. Настроить параметры для запуска TFTP-сервера в конфигурационном файле /etc/default/tftpd-hpa. Скопировать в каталог /srv/tftp файлы с установочного диска, необходимые для сетевой установки ОС. Создать конфигурационный файл для PXE-загрузчика /srv/tftp/pxelinux.cfg/default, взяв за основу пример файла с wiki.astralinux.ru

- 1 Установить TFTP-сервер.

**sudo apt install tftpd-hpa**

- 2 Изменить параметр TFTP\_OPTIONS в файле /etc/default/tftpd-hpa, добавив необходимые параметры.

**TFTP\_OPTIONS="--ipv4 --secure --create --umask 027 --permissive"**

- 3 Скопировать файлы, необходимые для сетевой установки, в каталог /srv/tftp.

**sudo cp /var/www/infra/astra/netinst/\* /srv/tftp/  
sudo cp /var/www/infra/astra/isolinux/ldlinux.c32 /srv/tftp/**

- 4 Создать каталог /srv/tftp/pxelinux.cfg.

**sudo mkdir /srv/tftp/pxelinux.cfg**

- 5 В этом каталоге создать конфигурационный файл PXE-загрузчика с именем default. 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>.

- 6 Указать в файле /srv/tftp/pxelinux.cfg/default используемые протокол и адрес сервера, на котором будет размещен файл с ответами на вопросы установщика ОС. В данной практической работе файл будет находиться на веб-сервере, запущенном в ВМ infra – http://10.0.1.254.

```
DEFAULT astra
LABEL astra
kernel linux
append initrd=initrd.gz vga=788 auto=true priority=critical
debian-installer/locale=en_US console-keymaps-at/keymap=ru
hostname=test2 domain=astra.test astra-license/license=true
url=http://10.0.1.254/preseed.cfg interface=auto
netcfg/dhcp_timeout=60
```

## TIMEOUT 5

Примечание: `append ...` – одна длинная строка

## Установка и настройка DHCP-сервера

**Задание:** На ВМ infra установить DHCP-сервер. Указать имя сетевого интерфейса (bond0) в конфигурационном файле /etc/default/isc-dhcp-server. Настроить пул динамических адресов 10.0.1.100-10.0.1.120, указав адреса шлюза и DNS-сервера и имя файла с PXE-загрузчиком.

- 1 Установить DHCP-сервер.

```
sudo apt install isc-dhcp-server
```

- 2 В файле /etc/default/isc-dhcp-server указать имя интерфейса bond0.

```
INTERFACESv4="bond0"
```

- 3 В файле /etc/dhcp/dhcpd.conf добавить описание топологии сети 10.0.1.0/24:

- диапазон адресов 10.0.1.100-10.0.1.120;
- адрес DNS серверов- 10.0.1.254;
- адрес шлюза - 10.0.1.254;
- указать имя файла с PXE-загрузчиком.

```
subnet 10.0.1.0 netmask 255.255.255.0 {
 range 10.0.1.100 10.0.1.120;
 option domain-name-servers 10.0.1.254;
 option domain-name "astra.test";
 option routers 10.0.1.254;
 filename "pxelinux.0";
}
```

- 4 Перезапустить DHCP-сервер.

```
sudo systemctl restart isc-dhcp-server
```

## Создание файла с ответами и установка ОС по сети

**Задание:** Создать файл с ответами /var/www/infra/preseed.cfg, используя пример из wiki.astralinux.ru. Изменить в файле строки, относящиеся к описанию репозитория Astra Linux. Изменить имя учетной записи, создаваемой в процессе установки. Указать метод автоматической разметки диска, который помещает все файлы в один раздел и создает область подкачки. Выполнить установку ОС по сети.

- 1 В каталоге /var/www/infra создать файл с ответами для автоматической установки preseed.cfg .

Пример файла можно скачать по адресу:

<https://wiki.astralinux.ru/pages/viewpage.action?pageId=263031386>

- 2 В файле preseed.cfg нужно указать:

- имя протокола, адрес сервера и каталог, в котором находится дистрибутив.

```
d-i mirror/protocol string http
d-i mirror/http/hostname string 10.0.1.254
d-i mirror/http/directory string /astra
```

- Указать учетную запись пользователя sa и задать для него пароль (12345678).

```
d-i passwd/user-fullname string "System Administrator"
d-i passwd/username string sa
```

- схему разметки диска с одним разделом под все файлы.

```
d-i partman-auto/method string regular
d-i partman-auto/choose_recipe select atomic
d-i partman/confirm_write_new_label boolean true
d-i partman/choose_partition select finish
d-i partman/confirm boolean true
d-i partman/confirm_nooverwrite boolean true
```

- (опционально) убрать или закомментировать все лишние строки.

С помощью команды

```
sudo debconf-set-selections -c preseed.cfg
```

проверить корректность формата файла.

- 3 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.

4 При запуске машины new следует выбрать установку по сети.

Примечание: для VirtualBox следует нажать F12 и появится меню. В меню выбирать загрузку по сети путем нажатия на клавишу I — LAN.

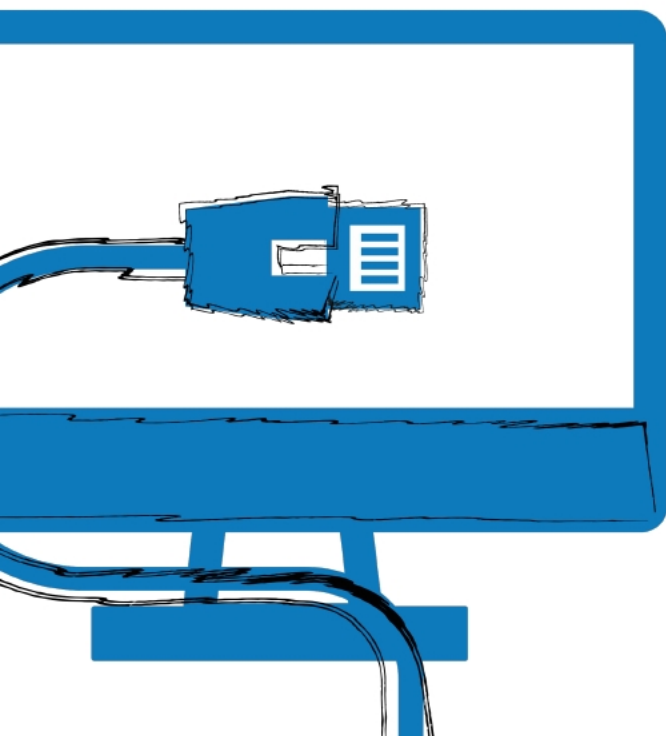
5 Установка будет выполнена автоматически:

- Если возникнет ошибка или появится сообщение, требующее ответа, то это означает, что один из разобранных выше шагов был выполнен некорректно. Тогда следует вернуться, обнаружить и исправить ошибки.

В случае, если все было настроено верно, то установка будет произведена без участия человека, VM будет перезагружена, и будет доступно окно входа в систему.

## Модуль 13

### Основы IPv6 (опциональный)



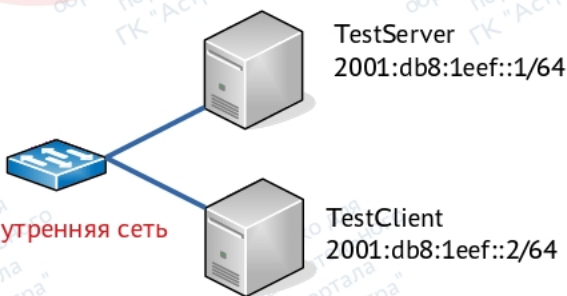


## Модуль 13. Основы IPv6

### 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 Создать VM TestServer и TestClient путем клонирования VM template\_1704\_3.
- 2 На TestServer посмотреть IPv6 адрес.  
**ip -6 a | grep fe80**
- 3 На TestClient выполнить ping хоста TestServer, используя IPv6 адрес TestServer.  
**ping fe80::f793:6823:6cff:c268**

### Назначение статических IPv6 адресов

- 1 На обеих VM отключить и замаскировать NetworkManager.

```
sudo systemctl stop NetworkManager
sudo systemctl mask NetworkManager
```

- 2 На TestServer настроить статический IPv6 адрес 2001:db8:1eef::1 путем внесения изменений в файл /etc/network/interfaces.

```
sudo vi /etc/network/interfaces
auto eth0
iface eth0 inet6 static
 address 2001:db8:1eef::1
 netmask 64
```

- 3 Активировать сетевой интерфейс eth0 на TestServer и проверить, что требуемый IPv6 адрес назначен.

```
sudo ifup eth0
ip -6 a
```

- 4 На TestClient настроить статический IPv6 адрес 2001:db8:1eef::2 путем внесения изменений в файл /etc/network/interfaces.

```
sudo vi /etc/network/interfaces
auto eth0
iface eth0 inet6 static
 address 2001:db8:1eef::2
 netmask 64
```

- 5 Активировать сетевой интерфейс eth0 на TestClient и проверить, что требуемый IPv6 адрес назначен.

```
sudo ifup eth0
ip -6 a
```

- 6 На TestClient проверить доступность TestServer командой ping, используя назначенный статический адрес.

```
ping 2001:db8:1eef::1
```

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

```
vi /etc/network/interfaces
auto eth0
iface eth0 inet6 static
 address 2001:db8:1eef::2
 netmask 64
iface eth0 inet6 static
 address 2001:db8:1eef::dead:1ead
 netmask 64
```

- 8 Обновить сетевой интерфейс eth0, убедиться, что адрес назначен.

```
sudo ifdown eth0
sudo ifup eth0
```

**ip -6 a**

- 9 На TestServer с помощью команды ping проверить доступность TestClient по новому адресу.

**ping 2001:db8:1eef::dead:lead**

## Настройка radvd для имитации маршрутизатора на сервере TestServer

- 1 На TestServer установить radvd.

**Примечание:** следует вставить образ установочного компакт-диска с Astra Linux 1.7.3 в привод ВМ и настроить компакт-диск в качестве репозитория ПО.

**sudo apt install radvd**

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

```
sudo vi /etc/radvd.conf
interface eth0 {
 IgnoreIfMissing on;
 AdvManagedFlag off;
 AdvReachableTime 0;
 AdvSendAdvert on;
 AdvOtherConfigFlag off;
 prefix 2001:db8:1eef::/64 {
 AdvOnLink on;
 AdvAutonomous on;
 };
};
```

- 3 Запустить службу radvd.

```
sudo systemctl start radvd
sudo systemctl enable 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.

```
sudo vi /etc/network/interfaces
auto eth0
iface eth0 inet6 auto
privext 2
```

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

**Примечание:** если назначение адресов не произошло, перезагрузите VM TestClient.

```
sudo ifdown eth0
sudo ifup eth0
ip -6 a
```

- 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.

```
INTERFACESv6="eth0"
```

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

```
sudo vi /etc/dhcp/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 установить автоматический запуск службы.

```
sudo systemctl start isc-dhcp-server
sudo systemctl enable isc-dhcp-server
```

## Настройка получения IPv6 адресов на TestClient с применением по DHCPv6

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

```
sudo vi /etc/network/interfaces
auto eth0
iface eth0 inet6 dhcp
```

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

```
sudo ifdown eth0
sudo ifup eth0
ip -6 a
```

- 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 и добавить в автозапуск.

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