



ALDPro

РУКОВОДСТВО АДМИНИСТРАТОРА. БЫСТРЫЙ СТАРТ

РДЦП.10101-01 95 01-01
Версия 3.0.0

Содержание

1 Введение	2
2 Подготовка виртуальной среды	3
2.1 Создание сети в VirtualBox	3
2.2 Создание VM для контроллера домена	5
2.3 Создание VM для клиента	6
3 Развертывание ALD Pro на контроллере домена	7
3.1 Настройка сетевого интерфейса	7
3.2 Указание имени сервера	10
3.3 Настройка доступных репозиториях	11
3.4 Настройка приоритетов пакетов	11
3.5 Установка пакетов	12
3.6 Повышение роли сервера до контроллера домена	13
3.7 Отключение DNSSEC, настройка глобального перенаправления	14
4 Ввод компьютера в домен	16
4.1 Настройка сети для доступа к репозиториям	16
4.2 Настройка доступных репозиториях	17
4.3 Установка пакетов	18
4.4 Ввод компьютера в домен	19
4.5 Проверка работы синхронизации времени	20

Введение

ALD Pro предоставляет возможность тестового развертывания в виртуальной среде для ознакомления с системой, выполнения исследовательских и образовательных задач. Данное руководство описывает процесс настройки виртуального окружения и развертывания ALD Pro.

Подготовка виртуальной среды

2.1. Создание сети в VirtualBox

Чтобы создать сеть в VirtualBox необходимо:

- Открыть «Настройки» из меню «Файл»
- В разделе «Сеть» выполнить команду «Добавить»
- Открыть настройки сети и указать следующее:
 - Имя сети: «Стенд 001»
 - CIDR сети (диапазон адресов): «10.0.1.0/24»
 - Поддержка DHCP: Откл (будет использована статическая адресация)

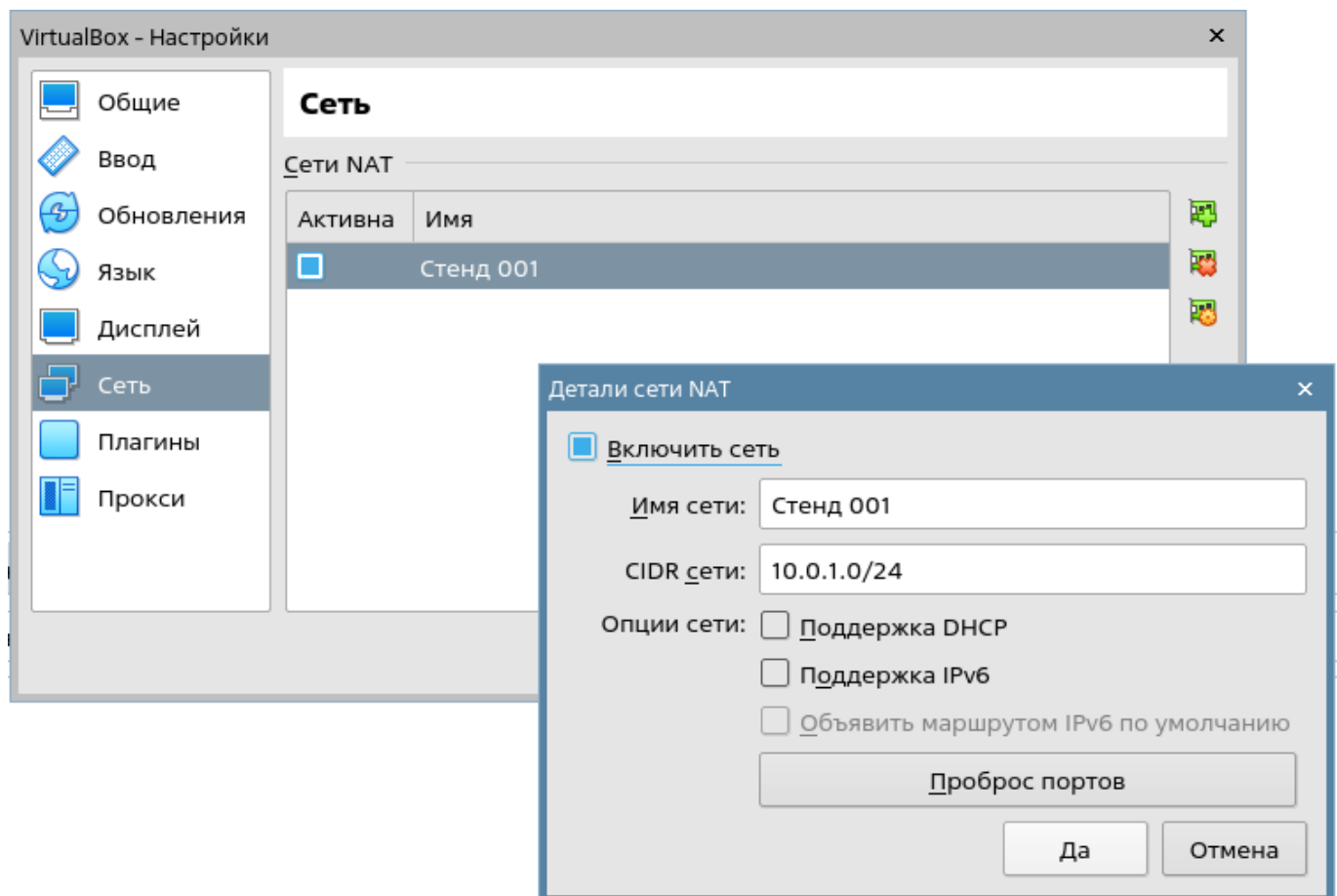


Рисунок 2.1 – Настройки сети virtualbox

В данной сети средствами VirtualBox будет создан NAT-шлюз. IP-адресом шлюза будет является первый адрес в указанной сети 10.0.1.1

В настройках виртуальной машины, на вкладке «Сеть»

- Адаптер 1
 - Тип подключения: Сеть NAT
 - Имя из списка: «Стенд 001»
- Адаптер 2-4: Откл

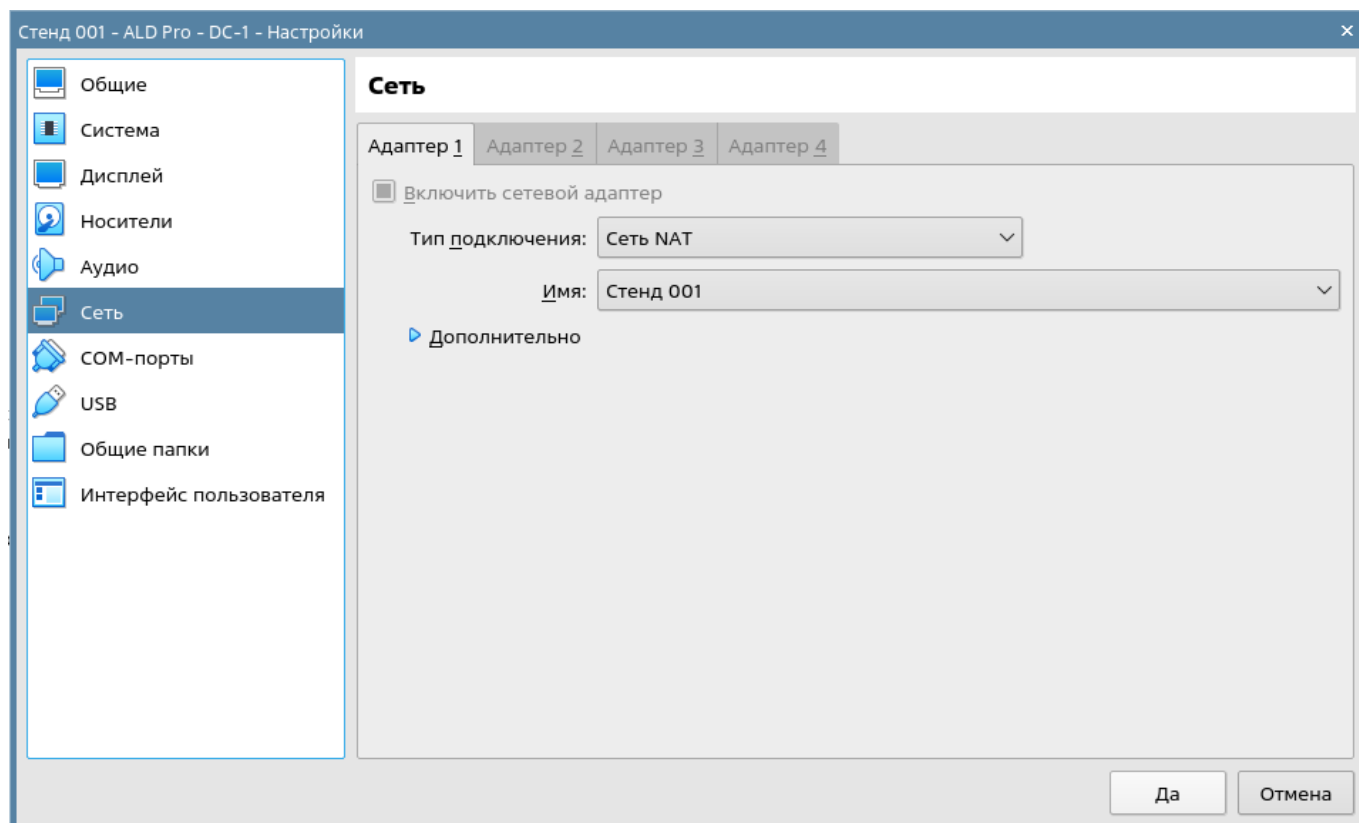


Рисунок 2.2 – Настройки сети виртуальной машины

Так как DHCP от VirtualBox в выбранной сети отключен, серверу не будет автоматически назначен адрес и это следует сделать вручную далее.

2.2. Создание VM для контроллера домена

Тестовый стенд будет работать без реальной нагрузки, поэтому указанная конфигурация оборудования может не соответствовать минимальным требованиям к производительности виртуальных машин.

В окне VirtualBox Manager выполнить команду «Машина → Создать» и указать следующие параметры:

- Указать имя и тип:
 - Имя: «Стенд 001 — dc-1.ald.company.lan»
 - Папка машины: по умолчанию
 - Тип: Linux
 - Версия: Other Linux (64-bit)
- Объем памяти: 4096 МБ
- Жесткий диск: создать новый виртуальный жесткий диск
- Тип файла: VDI (VirtualBox Disk Image)
- Формат хранения: Динамический виртуальный жесткий диск
- Указать имя и размер файла:
 - Путь: по умолчанию
 - Размер: 32 ГБ

После создания виртуальной машины в ее настройках:

- на вкладке «Система Процессор» указать:
 - Процессоры: 4 ЦП
- на вкладке «Носители» для компакт-диска указать установочный файл ALSE «1.7.7.9-24.04.25_19.28.iso» на вкладке «Сеть» выбрать:
 - тип подключения: Сеть NAT
 - имя: Стенда 001

Загрузить виртуальную машину с диска и установить операционную систему с графическим окружением и уровнем безопасности «Смоленск». На серверах должна быть установлена система, поддерживающая мандатный контроль целостности и конфиденциальности, на клиентах может быть любой уровень безопасности.

2.3. Создание VM для клиента

В окне VirtualBox Manager выполните команду «Машина → Создать» и указать следующие параметры:

- Указать имя и тип:
 - Имя: «Стенд 001 - ALD Pro — PC-1»
 - Папка машины: по умолчанию
 - Тип: Linux
 - Версия: Other Linux (64-bit)
- Объем памяти: 2048 МБ
- Жесткий диск: создать новый виртуальный жесткий диск
- Тип файла: VDI (VirtualBox Disk Image)
- Формат хранения: Динамический виртуальный жесткий диск
- Указать имя и размер файла:
 - Путь: по умолчанию
 - Размер: 32 ГБ

После создания виртуальной машины в ее настройках

- на вкладке «Система:raw-latex:Процессор» указать:
 - Процессоры: 2 ЦП
- на вкладке «Носители» для компакт-диска указать установочный файл
ALSE «1.7.7.9-24.04.25_19.28.iso», md5 диска
de1e72c271497a2b27909ea148f93f1f
- на вкладке «Сеть» выбрать:
 - тип подключения: Сеть NAT
 - имя: Стенда 001

Загрузить VM с диска и установить ОС с графическим окружением через мастер. Уровень безопасности ПК может быть любым.

Развертывание ALD Pro на контроллере домена

3.1. Настройка сетевого интерфейса

Для установки пакетов серверу нужно иметь доступ к репозиториям, расположенным в сети Интернет по адресу <https://dl.astralinux.ru>

При установке ALSE с графической оболочкой fly-wm управление сетевыми соединениями осуществляется через службу NetworkManager и одноименный апплет.

Так как была отключена DHCP служба, для настройки сети необходимо сделать следующее:

- Щелкнуть правой кнопкой мыши по иконке «Сетевые соединения» в правом нижнем углу экрана (в области уведомлений).
- В контекстном меню выбрать пункт **Изменить соединения**

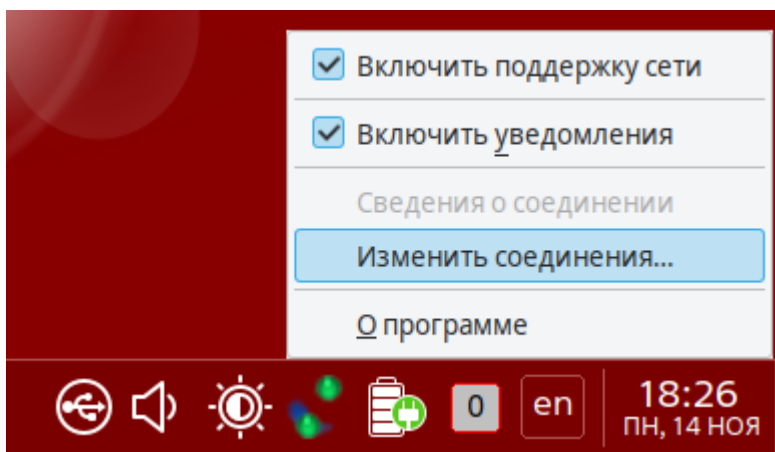


Рисунок 3.1 – Настройка сети для доступа к репозиториям 1

- Сделать двойной клик по заголовку «Проводное соединение 1»

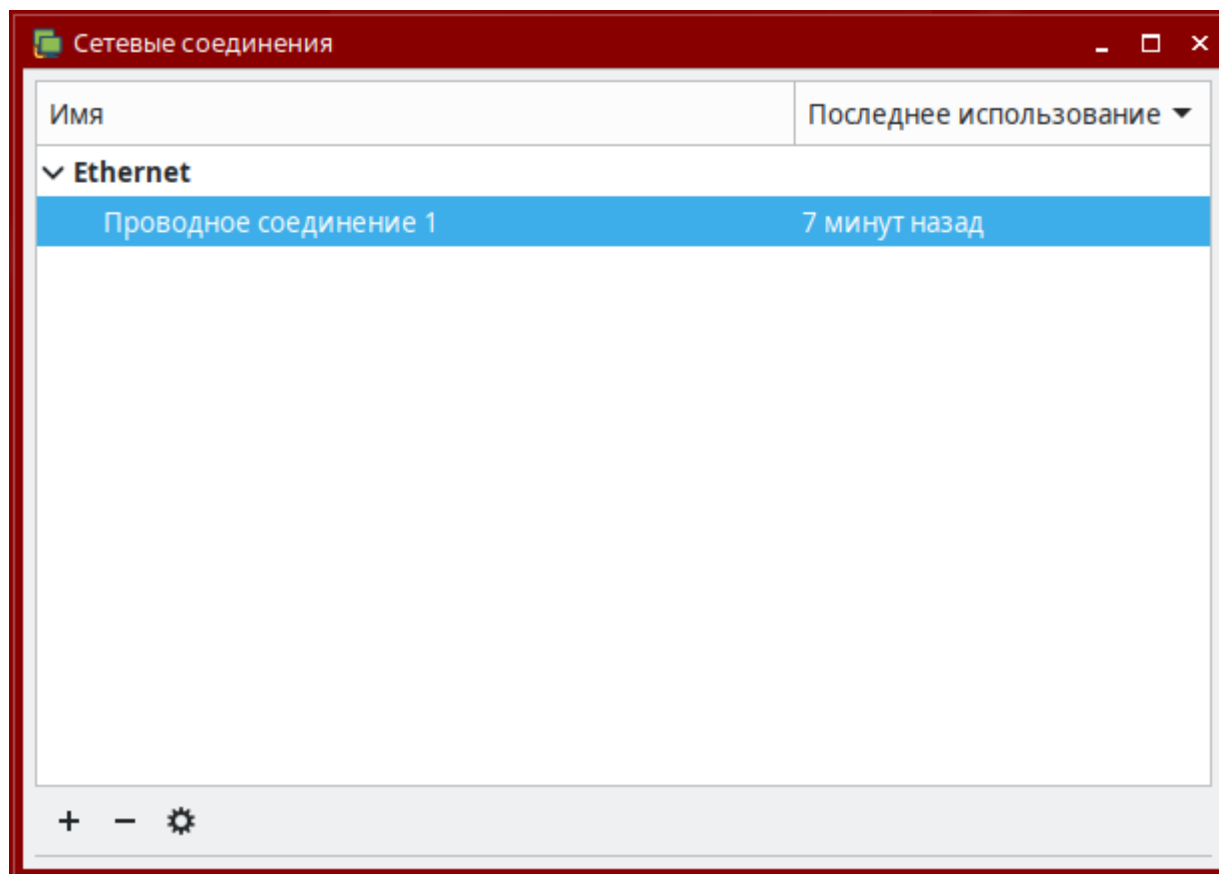


Рисунок 3.2 – Настройка сети для доступа к репозиториям 2

- На закладке Параметры IPv4 указать следующее:
 - Метод: Вручную
 - Адрес: 10.0.1.11
 - Маска: 255.255.255.0
 - Шлюз: 10.0.1.1
 - Серверы DNS: 77.88.8.8 (бесплатная служба разрешения имен от Яндекс).

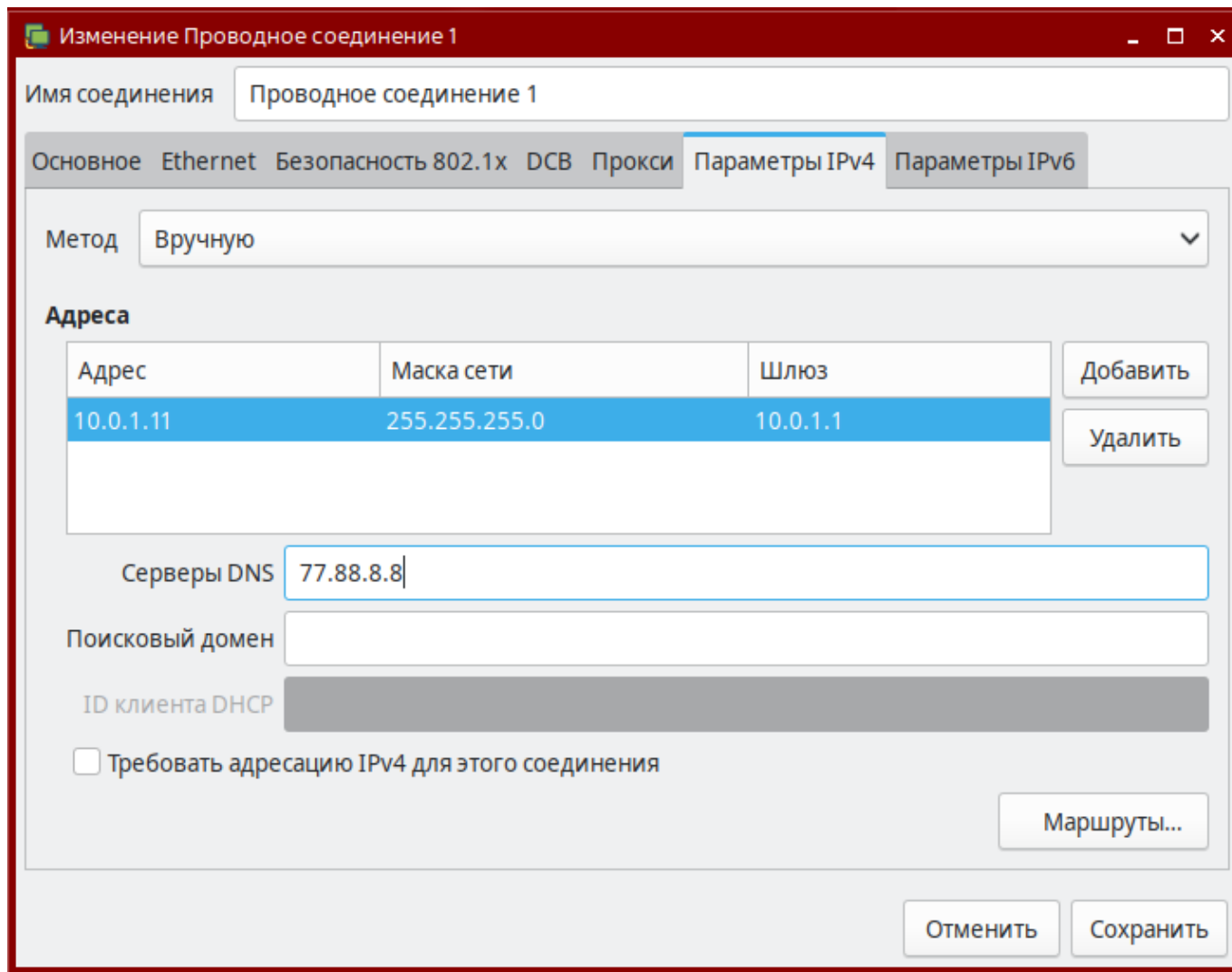


Рисунок 3.3 – Настройка сети для доступа к репозиториям 3

- После установки настроек необходимо проверить подключение к репозиториям ALSE:

```
ping -c 4 dl.astralinux.ru
```

3.2. Указание имени сервера

Изменение имени хоста рекомендуется делать с помощью утилиты `hostnamectl`:

```
sudo hostnamectl set-hostname dc-1.ald.company.lan
```

В имени хоста можно использовать буквы латинского алфавита [a-z] **в нижнем регистре**, цифры [0-9], точку [.] и дефис [-]. Имя хоста задается в формате полного имени **FQDN** (от **Fully Qualified Domain Name**), например, **dc-1.ald.company.lan**, поэтому команда `hostname` без параметров должна выдавать полное имя. Данное правило касается имен всех машин домена.

Для того чтобы имя контроллера всегда могло быть преобразовано в IP-адрес вне зависимости от доступности **DNS**-службы, содержимое файла `/etc/hosts` должно быть:

```
10.0.1.11 dc-1.ald.company.lan dc-1
127.0.0.1 localhost.localdomain localhost
#127.0.1.1 dc-1 - закомментировать или удалить строку с адресом локальной
↪петли
...
```

В начало файла нужно добавить строку со статическим IP-адресом контроллера, полным и коротким именем хоста. Полное имя должно быть указано перед коротким, чтобы оно считалось каноническим и возвращалось командой `hostname -f`, что требуется для корректной работы скриптов автоматизации.

3.3. Настройка доступных репозиториев

Для установки ALD Pro 3.0.0 на Astra Linux 1.7.xxx содержание файла должно быть следующим:

```
# /etc/apt/sources.list
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.xxx/repository-main 1.
↳7_x86-64 main non-free contrib
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.xxx/repository-
↳update 1.7_x86-64 main contrib non-free
# 1.7.xxx - должно соответствовать оперативному обновлению ОС, установленной
↳на машине
```

Для установки продукта ALD Pro 3.0.0 из официальных интернет-репозиториев РусБИТех-Астра нужно создать дополнительный файл `/etc/apt/sources.list.d/aldpro.list` и добавить в него следующую строку:

```
deb https://dl.astralinux.ru/aldpro/frozen/01/3.0.0/ 1.7_x86-64 main base
```

После изменения состава репозиториев следует обновить индекс доступных пакетов с помощью команды:

```
apt update
```

3.4. Настройка приоритетов пакетов

По умолчанию для всех пакетов, находящихся в репозиториях, приоритет $P=500$. Переопределить приоритет по умолчанию можно с помощью конфигурационных файлов в директории `/etc/apt/preferences.d`

В системе Astra Linux уже есть один такой конфигурационный файл, устанавливающий приоритет 900 для пакетов релиза 1.7_x86-64:

```
### cat /etc/apt/preferences.d/smolensk
Package: *
Pin: release n=1.7_x86-64
Pin-Priority: 900
```

Для пакетов ALD Pro — создать конфигурационный файл
/etc/apt/preferences.d/aldpro со следующим содержимым:

```
Package: *  
Pin: release n=generic  
Pin-Priority: 900
```

Перестраивать индекс после настройки приоритетов не требуется. Необходимо проверить, нет ли пакетов, доступных для обновления, и обновить систему, если таковые будут обнаружены:

```
sudo apt update  
sudo apt list --upgradable  
sudo apt dist-upgrade -y -o Dpkg::Options::=--force-confold
```

3.5. Установка пакетов

Теперь система готова к установке ALD Pro, для этого выполнить команду:

```
sudo DEBIAN_FRONTEND=noninteractive apt-get install -y -q aldpro-mp
```

- -y — параметр позволяет автоматически ответить «Да» на все возможные вопросы в ходе установки;
- -q — параметр позволяет скрыть сообщения о прогрессе установки, делая журнал более читаемым.

Ознакомиться с журналом установки и выполнить перезагрузку системы:

```
reboot
```

Во время перезагрузки в сообщениях ядра появятся ошибки запуска некоторых только что установленных служб. Ошибки служб при загрузке - это нормально.

3.6. Повышение роли сервера до контроллера домена

Требования к продвижению:

- Статичный IP адрес
- Разрешение имен через собственный DNS-сервер
- Имя хоста в соответствии с именем сервера в домене

Повышение роли сервера до контроллера домена выполняется с помощью следующей команды:

```
sudo aldpro-server-install -d ald.company.lan -n dc-1 --ip 10.0.1.11 --no-  
↪reboot
```

После ввода команды система запросит пароль администратора домена, который будет установлен для доменного пользователя `admin` и суперпользователя LDAP-каталога `cn=Directory Manager`. Пароль должен быть не менее 8 символов.

Для вступления изменений в силу необходимо перезагрузить сервер:

```
sudo reboot
```

После повышения роли сервера до контроллера домена необходимо убедиться, что содержимое файла `/etc/resolv.conf` соответствует следующим строкам:

```
nameserver 127.0.0.1  
search ald.company.lan
```

Если нет, то необходимо самостоятельно привести его к такому содержанию.

После перезагрузки сервера войти в систему можно, используя доменную учетную запись администратора:

- login: admin;
- password: ***** (пароль администратора домена).

После загрузки сервера проверить статус доменных служб можно с помощью команды:

```
sudo aldproctl status
```

Для доступа на портал управления откройте на контроллере домена браузер Mozilla

Firefox, адрес портала будет установлен страницей по умолчанию, авторизация должна пройти прозрачно без запроса пароля.

URL: `https://dc-1.ald.company.lan`

3.7. Отключение DNSSEC, настройка глобального перенаправления

После установки FreeIPA необходимо отключить DNSSEC в файле `/etc/bind/ipa-options-ext.conf`. Параметру `dnssec-validation` нужно присвоить значение `no`.

Особенностью настроек службы `bind9-pkcs11` по умолчанию является запрет на обработку рекурсивных DNS-запросов от клиентов, находящихся за пределами той же подсети, в которой находится сам DNS-сервер. Сделано это для предотвращения DDoS-атак с DNS-усилением, но эта защита не актуальна для контроллеров домена, которые работают в закрытом периметре, поэтому в файле `ipa-options-ext.conf` рекомендуется задать также значение `any` для параметров `allow-recursion` и `allow-query-cache` или определить в файле `/etc/bind/ipa-ext.conf` список доверенных сетей.

После внесения изменений содержимое файла `/etc/bind/ipa-options-ext.conf` должно быть следующим:

```
allow-recursion { any; };  
allow-query-cache { any; };  
dnssec-validation no;
```

Для проверки конфигурационного файла `bind9` после изменений использовать команду:

```
sudo named-checkconf /etc/bind/named.conf
```

Для применения изменений требуется перезапустить DNS-службу:

```
sudo systemctl restart bind9-pkcs11.service
```

Для завершения настройки портала добавить настройку глобального перенаправления, чтобы BIND9 использовал внешний DNS сервер, а не обходил все DNS сервера, начиная с

корневых, каждый раз. На вкладке «Роли и службы сайта — Служба разрешения имен — Глобальная конфигурация DNS» рекомендуется установить адрес публичного DNS, например от Яндекс 77.88.8.8, с политикой перенаправления «Сначала перенаправлять».

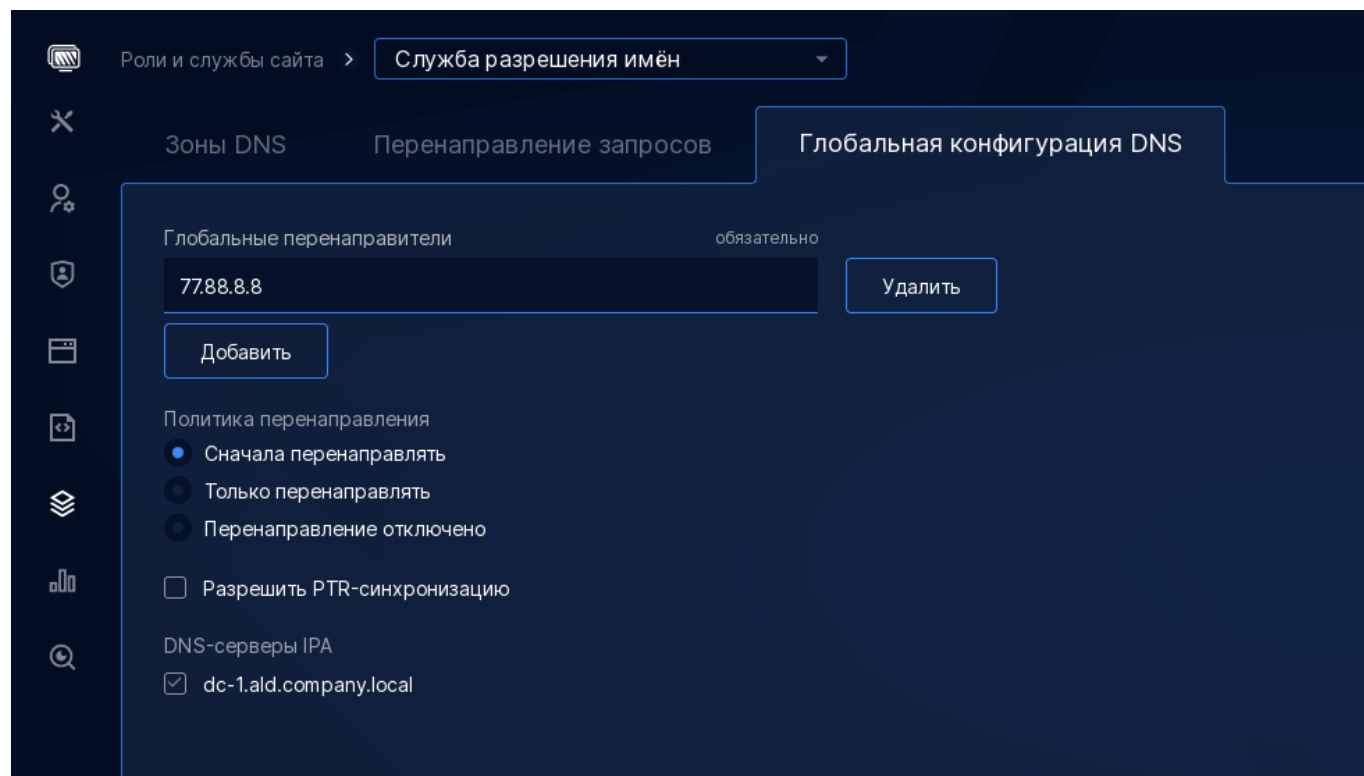


Рисунок 3.4 – Настройка глобального перенаправления

Ввод компьютера в домен

4.1. Настройка сети для доступа к репозиториям

Для установки пакетов серверу нужно иметь доступ к репозиториям, расположенным в сети Интернет по адресу <https://dl.astralinux.ru>

На пользовательских компьютерах настройка сети выполняется через стандартную службу NetworkManager. В реальной инфраструктуре для настройки пользовательских компьютеров используется DHCP. Для упрощения компьютеру будет назначен статический адрес.

На вкладке «Параметры IPv4» установите следующие значения:

- Метод: Вручную
- Адрес: 10.0.1.51
- Маска: 255.255.255.0
- Шлюз: 10.0.1.1 (шлюз от VirtualBox)
- Серверы DNS: 10.0.1.11 (адрес DC-1)
- Поисковый домен: ald.company.lan (см. про DNS-суффикс выше)

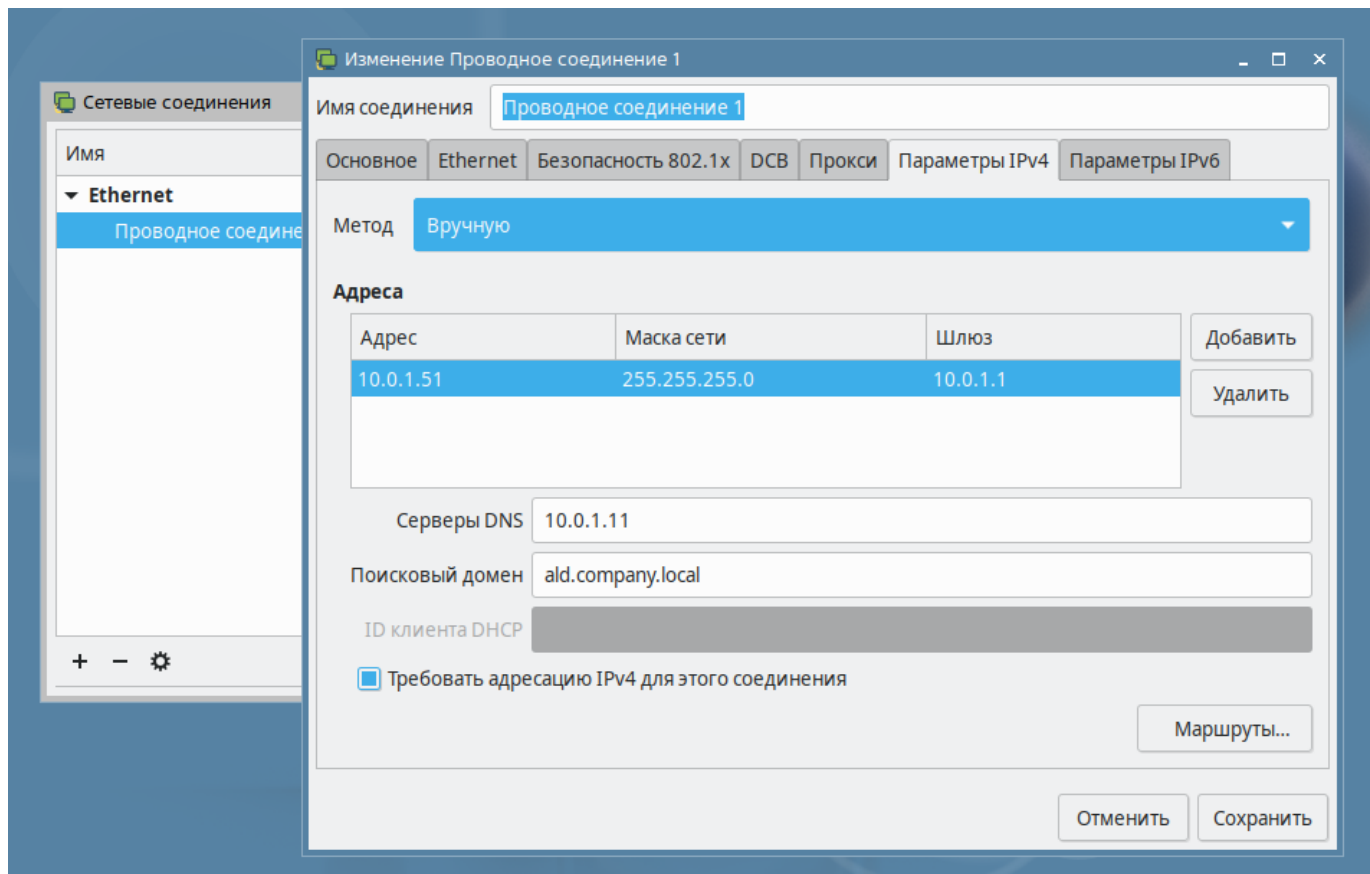


Рисунок 4.1 – Настройка параметров IPv4

4.2. Настройка доступных репозиториев

Содержание файла `/etc/apt/sources.list` должно быть таким же, как при установке серверной части:

```
# /etc/apt/sources.list
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.xxx/repository-main/
↪1.7_x86-64 main contrib non-free
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.xxx/repository-
↪update/ 1.7_x86-64 main contrib non-free
# 1.7.xxx - должно соответствовать оперативному обновлению ОС, установленной
↪на машине
```

Также необходимо создать отдельный список для `/etc/apt/sources.list.d/aldpro.list`:

```
sudo nano /etc/apt/sources.list.d/aldpro.list
```

Вставить в этот файл содержимое:

```
deb https://dl.astralinux.ru/aldpro/frozen/01/3.0.0 1.7_x86-64 main base
```

Обновить индекс и проверить, нет ли пакетов, доступных для обновления. Обновить систему, если таковые будут обнаружены, командами:

```
sudo apt update
sudo apt list --upgradable
sudo apt dist-upgrade -y -o Dpkg::Options::=--force-confnew
```

Настроить приоритеты, так же как делали на сервере

```
Package: *
Pin: release n=generic
Pin-Priority: 900
```

4.3. Установка пакетов

Теперь система готова к установке клиентской части ALD Pro, для этого выполнить команду:

```
sudo DEBIAN_FRONTEND=noninteractive apt-get install -y -q aldpro-client
```

Комментарии к использованным ключам можно найти в разделе [Установка пакетов](#).

Если перезагружать пользовательский компьютер сейчас, то в сообщениях ядра можно будет увидеть ошибки запуска SSSD и зависящих от нее служб (журнал загрузки можно найти в файле `/var/log/boot.log`) Это происходит по причине того, что служба еще не настроена соответствующим образом (журнал службы sssd можно найти в файле `/var/log/sss/sssd.log`)

4.4. Ввод компьютера в домен

Для ввода компьютера в домена требуется несколько условий:

- у компьютера должно быть задано уникальное имя, которое еще не используется в домене;
- в качестве DNS-сервера должен быть указан IP адрес контроллера домена;
- установлен пакет клиентского программного обеспечения `aldpro-client`.

По данной схеме имя компьютера будет PC-1. Проверить уникальность можно командой `nslookup`:

```
nslookup pc-1
```

В домене «ald.company.lan» следует указать значение «pc-1.ald.company.lan»

```
hostnamectl set-hostname pc-1.ald.company.lan
exec bash
hostnamectl
echo $HOSTNAME
```

Также можно сгенерировать случайное имя хосту следующей командой:

```
hostnamectl set-hostname "pc-$(expr $RANDOM | md5sum | head -c 11).ald.
↪company.lan"
```

Все готово для ввода компьютера в домен:

```
sudo /opt/rbta/aldpro/client/bin/aldpro-client-installer --domain ald.company.
↪lan --account admin --host pc-1 --gui --force --orgunits "ou=ald.company.
↪lan,cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan"
```

После ввода команды система запросит ввести пароль администратора домена.

Параметры утилиты `aldpro-client-installer`:

- `--domain` — имя домена, которое выбрано на основе третьего уровня приобретённого домена, например, ald.company.lan;
- `--account` — логин администратора домена;
- `--password` — получить пароль администратора домена из командной строки

(небезопасно);

- `--host` — имя компьютера в нижнем регистре;
- `--gui` — использовать интерактивный режим;
- `--force` — продолжить ввод компьютера в домен, даже если в домене для его имени уже есть учетная запись. Требуется в тех случаях, когда администратор переустанавливает операционную систему и хочет ввести компьютер в домен с тем же именем;
- `--orgunits` — подразделение компьютера. При выполнении без указанного параметра, компьютеру присваивается корневое подразделение. При вводе некорректного или несуществующего DN, компьютер будет привязан к корневому подразделению.

Для применения всех настроек выполнить перезагрузку компьютера:

```
reboot
```

После перезагрузки войти в систему, используя доменную учетную запись администратора.

Для первого входа в систему доменной учетной записью требуется доступ к контроллеру домена.

4.5. Проверка работы синхронизации времени

Текущие настройки службы синхронизации времени на хосте можно посмотреть в файле `chrony.conf`:

```
cat /etc/chrony/chrony.conf
```

Принудительно обновить содержание конфигурационного файла через механизм групповых политик можно перезапуском службы `aldpro-salt-minion.service`:

```
systemctl restart aldpro-salt-minion.service
```

Принудительно запустить синхронизацию времени можно перезапуском службы

```
systemctl restart chrony
```

Текущее состояние синхронизации можно узнать в приложении «Дата и Время» или командой `timedatectl`:

```
timedatectl
```

Для взаимодействия со службой `chronyd` во время ее работы предназначен интерфейс командной строки `chronyc`. Чтобы увидеть, с какими серверами служба устанавливает соединение, можно отправить через него команду `sources`. Символом звездочки отмечен сервер, время которого установлено в системе.

```
### chronyc sources -v
...
^* dc-1.ald.company.lan      2   6   377   51  +4571ns[  -48us] +/-  19ms
...
```

Форсировать переход к целевому значению вы можете вызовом команды `makestep` через `chronyc`:

```
chronyc makestep
```

Если требуется проверить работу NTP-сервера, вы можете воспользоваться командой `ntptime` с ключом `q` (`query only`, отправить только запрос без изменения времени):

```
ntptime -qvdc dc-1.ald.company.lan
```

Записать текущее время системы в BIOS можно утилитой `hwclock` с параметром `systohc`:

```
hwclock --systohc
```

При значительном изменении времени ранее выданные билеты `kerberos` могут оказаться недействительными, поэтому может потребоваться повторно пройти аутентификацию в домене командой `kinit`:

```
kinit
Password for admin@ALD.COMPANY.LAN: *****
```

Информацию о выданных билетах можно увидеть командой `klist`:

```
klist Ticket cache:
KEYRING:persistent:1194600000:krb_ccache_Y1bhw3f Default principal:
admin@ALD.COMPANY.LAN valid starting Expires Service principal
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

16.10.2022 14:40:20 17.10.2022 14:40:18
krbtgt/ALD.COMPANY.LAN@ALD.COMPANY.LAN