ALD Pro

ИНСТРУКЦИИ

РАЗВЕРТЫВАНИЕ ALD PRO В ВИРТУАЛЬНОЙ СРЕДЕ (ЗНАКОМСТВО С ALD PRO)

Версия 2.4.1

Содержание

Аннотация

В настоящей инструкции представлены рекомендации по развертыванию сетевых служб ALD Pro в виртуальной среде VirtualBox для ознакомления с возможностями продукта.

Предварительные требования

Инструкция предназначена для администратора, обладающего знаниями и опытом в следующих областях:

- Администрирование Linux (материалы курсов AL-1702, AL-1703)
- Администрирование компьютерных сетей (материалы курса AL-1704)
- Администрирование LDAP-каталога, использование протокола аутентификации Kerberos

Постановка задачи

Вы отвечаете за управление пользователями/компьютерами в организации ООО «Компани», которая предоставляет консультационные услуги по всему СНГ с штаб-квартирой в Москве. Вам поставили задачу по переносу инфраструктуры на сервера под управлением Astra Linux. При прохождении данной инструкции вы узнаете о базовой структуре доменных служб Astra Linux Directory, их развертыванию, настройке и использованию.

Построение ИТ-инфраструктуры предприятия начинается с планирования структуры домена. Домен – это логическое объединение объектов ИТ инфраструктуры (серверов, компьютеров, пользователей, принтеров и др.), разделяющих общие настройки администрирования, безопасности и репликации. Информация об объектах хранится на выделенных серверах — контроллерах домена — и доступна через службу каталога. Служба каталога работает по LDAP-протоколу и имеет встроенный механизм аутентификации (LDAP Bind, привязка LDAP), но в целях безопасности в пользовательских приложениях рекомендуется использовать Kerberos-аутентификацию, за работу которой отвечает еще одна служба контроллера домена — центр распределения ключей (Key Distribution Center, KDC).

На первом шаге мы проверим работу доменной аутентификации, поэтому нам нужно будет установить один контроллер домена, ввести в домен пользовательский компьютер и проверить механизм доменной аутентификации.

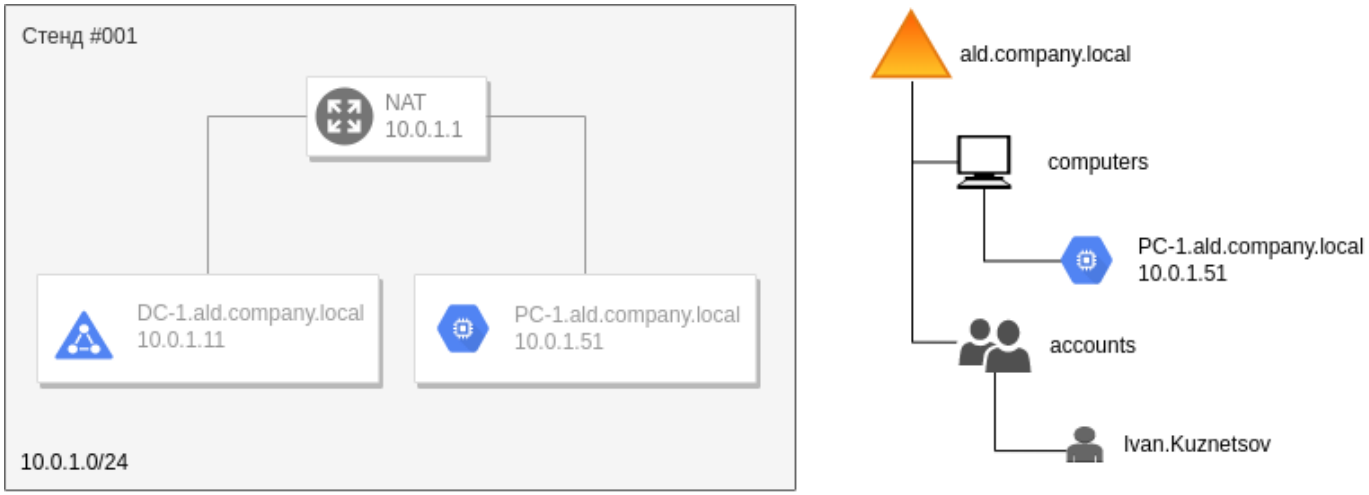

Рисунок 3.1 – Пример топологии домена

Создайте сеть в VirtualBox

Взаимодействие между компьютерами в домене осуществляется через компьютерную сеть по протоколу TCP/IP. Сервера из соображений безопасности обычно выносят в отдельную подсеть, чтобы ограничить к ним доступ правилами межсетевого экрана, но так как аспекты безопасности не являются предметом данной инструкции, то в нашем случае все хосты будут размещены в общей сети 10.0.1.0/24, созданной средствами VirtualBox.

Чтобы создать сеть в VirtualBox, вам нужно:

- 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 (будем использовать собственную службу динамической настройки узлов ALD Pro)

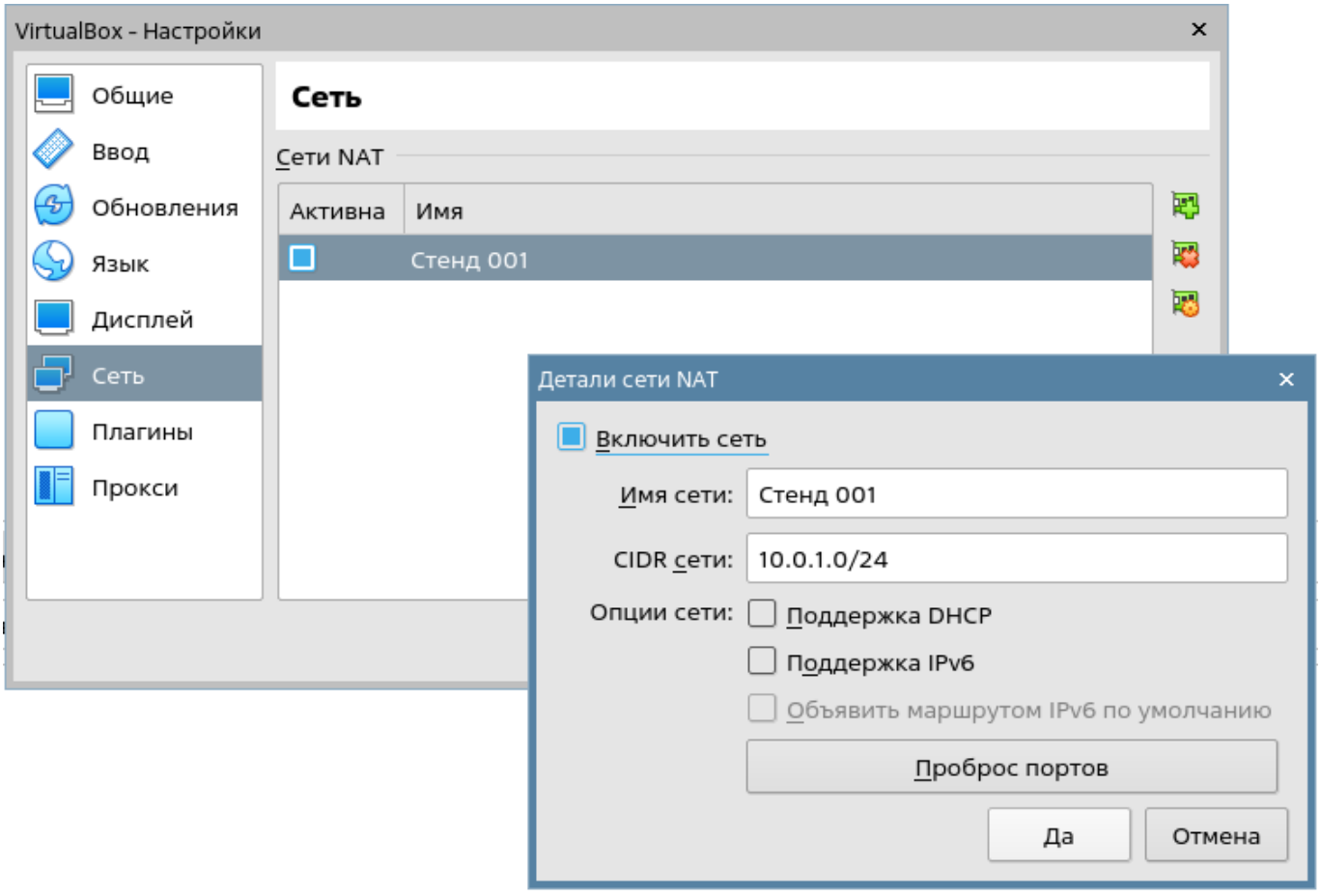

Рисунок 4.1 – Настройки сети virtualbox

В данной сети средствами VirtualBox будет создан NAT-шлюз, через который виртуальные машины смогут выходить в Интернет. 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

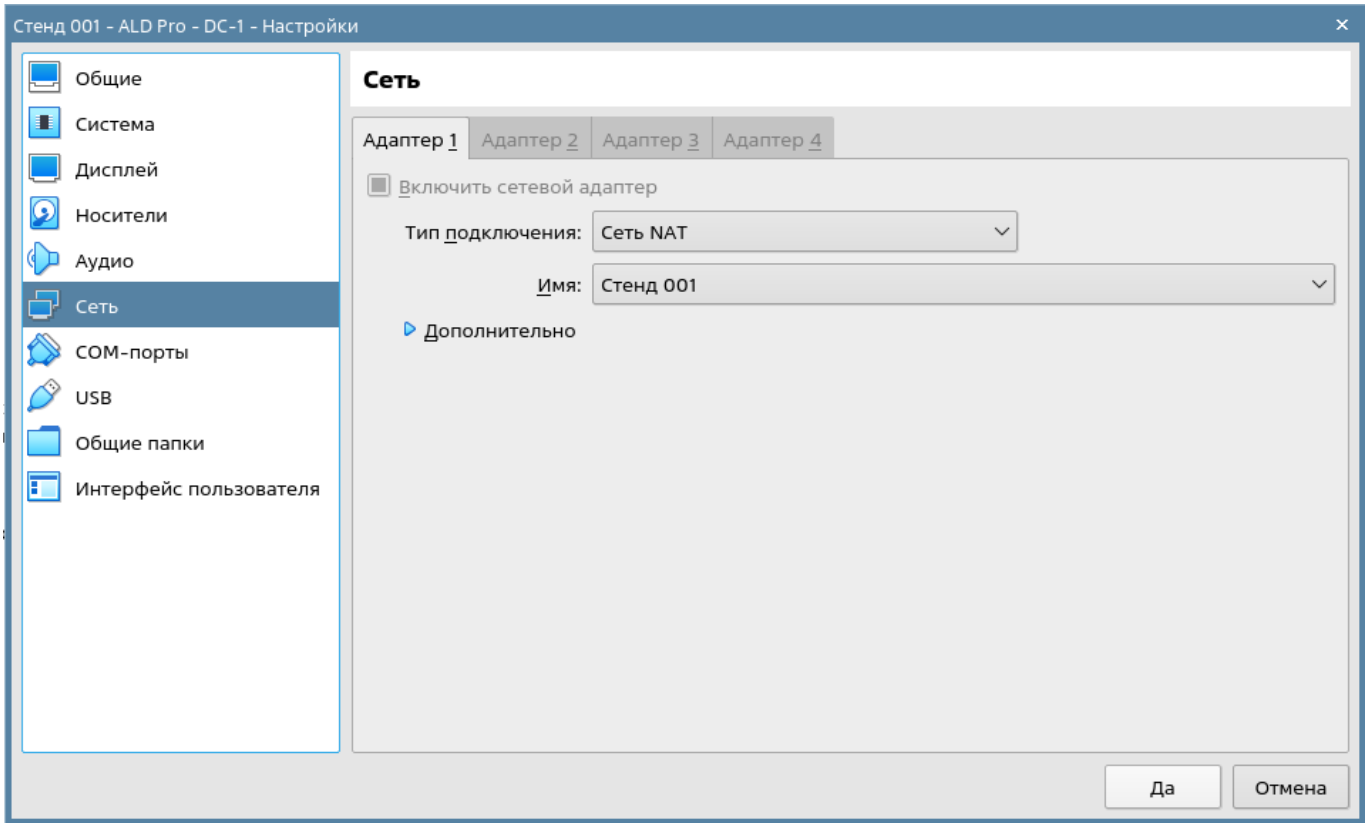

Рисунок 4.2 – Настройки сети виртуальной машины

Учитывая тот факт, что DHCP от VirtualBox в выбранной сети отключен, серверу не будет автоматически назначен адрес и это следует сделать вручную далее.

Создайте VM для контроллера (dc-1.ald.company.local)

В окне VirtualBox Manager выполните команду «Машина:raw-latex:*Создать*» и укажите следующие параметры:

•Укажите имя и тип:

- Имя: «Стенд 001 — dc-1.ald.company.local»
- 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

•Укажите имя и размер файла:

- Путь: по умолчанию
- Размер: 32 ГБ

После создания виртуальной машины в ее настройках:

•на вкладке «Система Процессор» укажите:

- Процессоры: 4 ЦП

•на вкладке «Носители» для компакт-диска укажите установочный файл ALSE «1.7.2-11.08.2022_15.28.iso» на вкладке «Сеть» выберите:

- тип подключения: Сеть NAT
- имя: Стенда 001

Загрузите виртуальную машину с диска и установите 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.

Установите пакеты ALD Pro на DC-1

6.1. Настройте сеть для доступа к репозиториям

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 управление сетевыми соединениями осуществляется через службу NetworkManager и одноименный апплет. Эта служба предоставляет удобный графический интерфейс, и автоматически перенастраивает сеть при подключении к Wi-Fi, что очень удобно при работе на персональных компьютерах, но на серверах ее рекомендуется отключать, т. к. используемые этой службой алгоритмы управления сетью могут создать проблемы в работе служб каталога и центра распределения ключей контроллера домена. Чуть позже мы так и сделаем, но сейчас для установки пакетов воспользуемся возможностями этой службы для быстрой настройки сети.

Так как мы отключили DHCP службу, для настройки сети сделайте следующее:

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

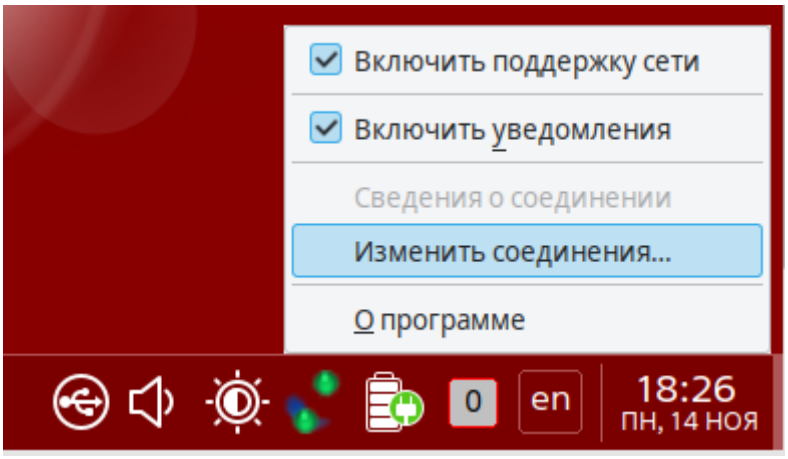

Рисунок 6.1 – Настройка сети для доступа к репозиториям 1

- Сделайте двойной клик по заголовку «Проводное соединение 1»

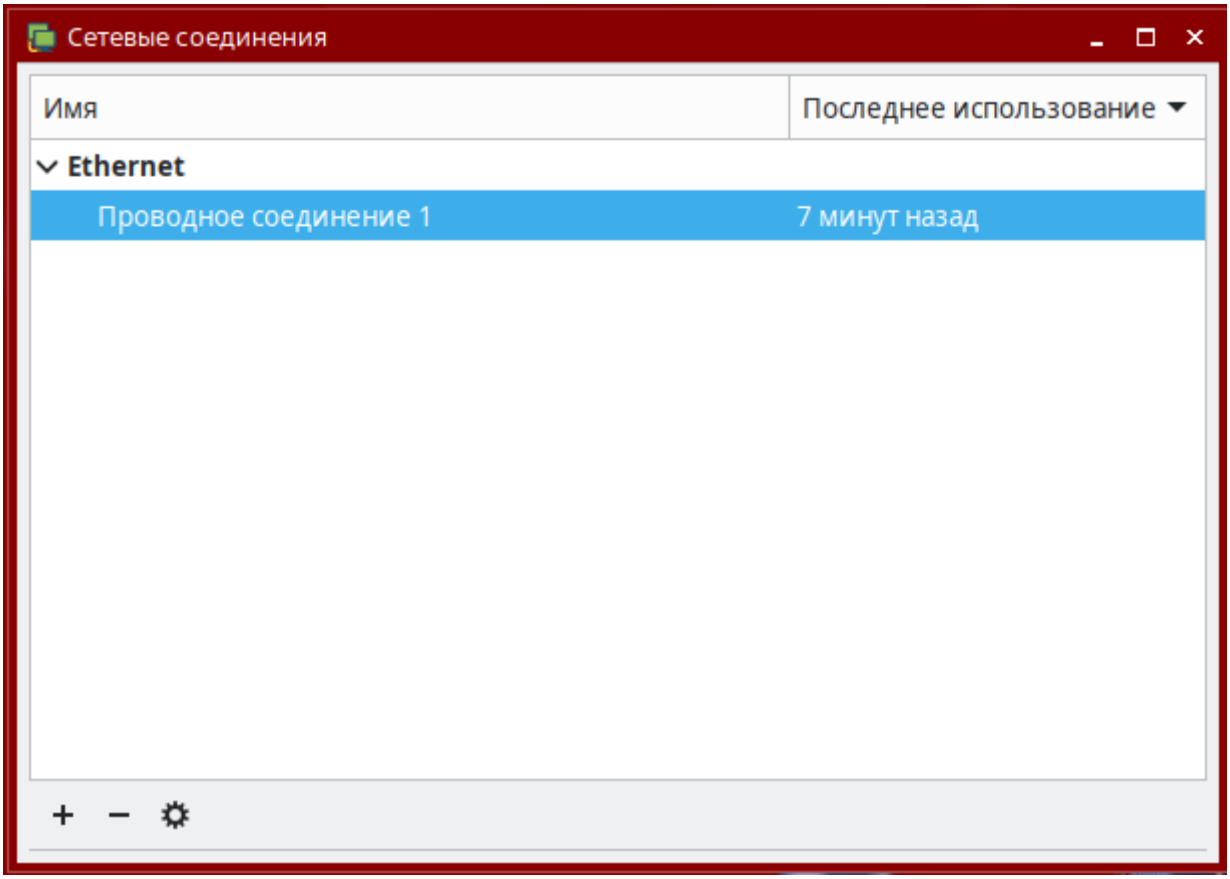

Рисунок 6.2 – Настройка сети для доступа к репозиториям 2

•На закладке Параметры IPv4 укажите 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).

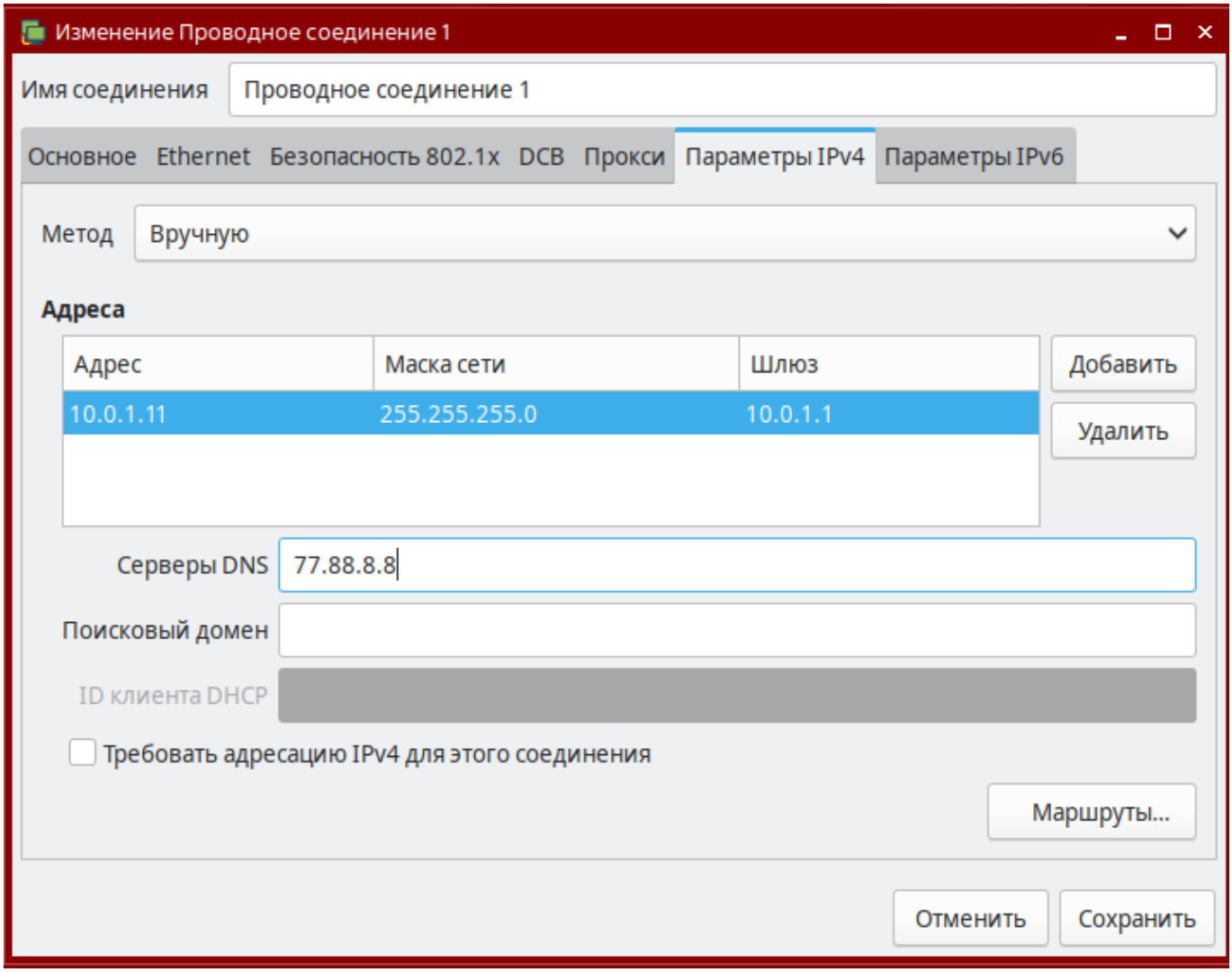

Рисунок 6.3 – Настройка сети для доступа к репозиториям 3

- Проверьте, что у вас есть доступ к репозиториям:

```
ping dl.astralinux.ru
```

6.2. Настройте доступные репозитории

Файлы программ Linux объединяются в пакеты и распространяются через специальные хранилища, называемые репозиториями. Основным файлом для хранения списка доступных репозиториев является `/etc/apt/sources.list`, дополнительные списки могут храниться в файлах `\*.list` в директории `/etc/apt/sources.list.d/`

Для установки на сервере под управлением Astra Linux 1.7.2 программного продукта ALD Pro версии 1.2.0 из официальных интернет-репозиториев РусБИТех-Астра содержание этого файла должно быть следующим:

```
# vi /etc/apt/sources.list
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.2/repository-base/ 1.
↪7_x86-64 main contrib non-free
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.2/repository-
↪extended/ 1.7_x86-64 main contrib non-free
deb https://dl.astralinux.ru/aldpro/stable/repository-main/ 1.2.0 main
deb https://dl.astralinux.ru/aldpro/stable/repository-extended/ generic main
```

Для сохранения изменений в файле `sources.list` программа vi должна быть запущена с привилегиями root-пользователя, на что указывает символ # в начале строки. Запуская программу из-под обычного пользователя, можно добавить «sudo»:

```
sudo vi /etc/apt/sources.list
```

При первом выполнении команды «sudo» система потребует ввести пароль, а после успешной аутентификации внесет необходимую информацию в кеш и будет хранить ее следующие 15 минут в соответствии со значением параметра timestamp_timeout в файле `/etc/sudoers`.

Чтобы расширить ограничение в 15 минут вы можете запустить новую сессию оболочки от имени супер пользователя командой «sudo -i». Выйти из привилегированной сессии можно будет позднее командой «exit».

```
localadmin@astra:~$ sudo -i
[sudo] пароль для localadmin: **********
root@astra:~# exit
Выход
localadmin@astra:~$
```

Редактор vi является крайне специфичным. После открытия документа вы находитесь в режиме ввода команд. Например, вы можете ввести команду «:q» и нажать клавишу Enter, чтобы закрыть программу. Редактирование документа возможно в режимах вставки и замены, для переключения между которыми используется клавиша Insert. Для возврата в режим команд вам нужно будет нажать клавишу Esc. Чтобы сохранить и закрыть документ используйте команды «:wq». Если нужно закрыть документ без сохранения «:q!».

Каждая строка файла sources.list соответствует одному из четырех репозиториев (ALSE base & extended, ALD Pro main & extended) и имеет следующий формат:

```
deb <путь_корневому_каталогу_репозитория> <код_дистрибутива> <компонент1>
↪<компонент2> <компонент3>``
```

Комментарии по использованным инструкциям:

deb — указывает на то, что репозиторий соответствует репозиторию бинарных файлов с предварительно скомпилированными пакетами. Для репозиториев с исходными кодами используют «deb-src»

uri — задает адрес репозитория, у интернет-репозиториев адрес начинается с «http(s)://», адреса локальных репозиториев начинаются с «file:/». При добавлении репозитория с диска командой «apt-cdrom add» в файле появится строка «cdrom:[]/»

дистрибутив — дополняет uri, уточняя необходимый релиз продукта. В одном репозитории могут находиться пакеты сразу для нескольких релизов.

компонент — это группа пакетов, объединенная по условиям использования:

non-free — группа содержит пакеты, которые не соответствуют принципам свободного ПО, имеют патенты или другие юридические ограничения;

contrib — группа содержит пакеты, которые сами по себе соответствуют принципам свободного ПО, но зависят от пакетов из группы «non-free» (т. е. не могут без них работать);

main — группа содержит пакеты свободного ПО, которые не зависят от пакетов из групп «contrib» и «non-free».

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

```
apt update
```

Информацию о пакетах для обновления индекса менеджер возьмет из файла Release или InRelease, ссылки на которые формируются по следующей схеме:

Рисунок 6.4 – Формирование ссылки репозитория

Попробуйте скачать этот файл в браузере, и вы увидите ссылки на Packages-файлы для

разных компонентов и архитектур.

Файлы InRelease отличаются от файлов Release тем, что они содержат PGP-подписи. Содержание Packages-файлов после выполнения apt-get update кешируется на локальном диске в папке `/var/lib/apt/lists`

6.3. Настройте приоритеты пакетов

Пакетному менеджеру APT может быть доступно сразу несколько версий одного и того же приложения из разных репозиториев, поэтому он выбирает наиболее подходящего кандидата для установки в соответствии с приоритетами 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 конфигурационны 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
```

Это правило позволяет избежать установки и обновления пакетов из сторонних репозиториев, если компанией РусБИТех-Астра для операционной системы под релиз 1.7_x86-64 была разработана специальная версия.

Такой же подход следует использовать для пакетов ALD Pro — создайте конфигурационный файл `/etc/apt/preferences.d/aldpro` со следующим содержимым:

```
### vi /etc/apt/preferences.d/aldpro
Package: *
Pin: release n=generic
Pin-Priority: 900
```

Следует учитывать, что приоритет 900 не позволит понизить версию уже установленного в системе пакета, т. к. для выполнения даунгрейда приоритет кандидата должен быть P >

1000. Поэтому рекомендуется не выполнять обновление операционной системы из интернет-репозиториев, отличных от frozen, во избежание установки конфликтующих версий пакетов.

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

```
apt list --upgradable
apt upgrade -y
```

6.4. Установите пакеты

Теперь система готова к установке ALD Pro, для этого выполните команду

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

Комментарии по использованным инструкциям и параметрам:

DEBIAN_FRONTEND — переменная окружения, которая позволяет изменить режим взаимодействия с пользователем при установке пакетов менеджером APT. Многие приложения на стадии установки уточняют необходимые настройки для последующей работы, что станет помехой для автоматического развертывания. Переключение менеджера пакетов в режим noninteractive позволяет избежать уведомлений от Kerberos, OpenDNSSec и PAM.

-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

aldpro-mp - инсталляционный пакет портала управления (management portal) продукта ALD Pro

Ознакомьтесь с журналом установки и выполните перезагрузку системы

```
reboot
```

Во время перезагрузки в сообщениях ядра появятся ошибки запуска некоторых только что установленных служб. Это нормальное поведение продукта, которое происходит по

причине того, что эти службы еще не настроены должным образом.

Выполните продвижение DC-1 до контроллера домена

Продвижением называют процедуру, в ходе которой выполняется настройка служб сервера для его использования в качестве контроллера домена. Для корректной работы контроллера ему требуется несколько условий:

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

7.1. Настройте сеть для работы контроллера домена

Как уже было упомянуто выше, служба NetworkManager создает дополнительные накладные расходы, поэтому на серверах ее рекомендуется отключить:

```
systemctl stop network-manager.service
systemctl disable network-manager.service
systemctl status network-manager.service
```

После отключения NetworkManager сетевые настройки нужно задавать в файлах `interfaces` и `resolv.conf`.

Файл `/etc/network/interfaces` используется командами `ifup/ifdown` для конфигурирования сетевых интерфейсов. Служба каталога тесно интегрирована со службой разрешения имен, поэтому контроллер домена выступает еще и в роли DNS-сервера. Адреса DNS-серверов через DHCP или даже вручную распространяются по всей сети, поэтому на контроллере домена настоятельно рекомендуют устанавливать статический адрес. По нашей схеме IP должен быть 10.0.1.11, для этого укажите в файле `interfaces` следующее:

```
### vi /etc/network/interfaces
source /etc/network/interfaces.d/*
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
    address 10.0.1.11
    netmask 255.255.255.0
    gateway 10.0.1.1
```

Комментарии по использованным инструкциям:

auto eth0 — строка, начинающаяся со слова «auto», указывает интерфейс, который будет подниматься при вызове команды «ifup -a». Посмотреть список доступных интерфейсов можно командой «ip a», первый сетевой интерфейс VirtualBox имеет идентификатор eth0

iface eth0 inet static — строка со словом «iface», начинает группу строк, отвечающих за настройку указанного интерфейса. Следующее слово «inet/inet6» указывает, какой протокол будет использоваться — IPv4 или IPv6 соответственно. Следующее слово «static/dhcp» указывает способ назначения настроек — вручную, или динамически.

address, netmask, gateway — задают IP адрес, маску и шлюз по умолчанию для интерфейса, указанного в предшествующей ей строке «iface», если для него выбран способ назначения настроек «static»

В некоторых инструкциях вы можете встретить указание в файле `interfaces` таких параметров, как `dns-nameservers` и `dns-search`, но они имеют силу, только в том случае, если в системе работает служба `resolvconf`, которая переносит эти настройки соответствующим образом в файл `/etc/resolv.conf` Для получения развернутой информации о допустимом синтаксисе файла `interfaces` выполните команду `man interfaces`.

Чтобы применить новые настройки, следует перезапустить службу Networking. Теперь вы можете проверить доступ к публичным серверам по IP

```
systemctl restart networking.service
ping 77.88.8.8
```

Файл `/etc/resolv.conf` определяет настройки для процедур разрешения имен из

библиотеки `glibc`, которая используется в сетевых утилитах ping, dig и т.д. В этом файле следует следует указать:

```
### vi /etc/resolv.conf
search ald.company.local
nameserver 127.0.0.1
```

Комментарии по использованным инструкциям:

search — строка, начинающаяся со слова «search», задает DNS-суффикс, используемый при разрешении имен. Если указан суффикс «ald.company.local», то при обращении к хосту «dc-1» будет также предпринята попытка обращения к «dc-1.ald.company.local».

nameserver — строка, начинающаяся со слова «nameserver», задает адрес DNS-сервера для преобразования имен. Библиотека glibc поддерживает до трех строк nameserver, используя дополнительные сервера в качестве резервных.

Если до установки пакетов ALD Pro перенаправление DNS-запросов на localhost (127.0.0.1) привело бы к отказу в работе механизма разрешения имен, то сейчас этого не произойдет, т. к. в системе работает сервис bind9, который выполняет функцию рекурсивного разрешителя имен. Bind9 сам находит запрашиваемые DNS-записи, последовательно обращаясь ко всем DNS серверам, обслуживающим зону, начиная с корневой (см. файлы `/etc/bind/named.conf.default-zones` и `/usr/share/dns/root.hints`). Единственно, по умолчанию bind9 может использовать механизм DNSSEC для проверки ответов, но его лучше отключить в файле `ipa-options-ext.conf`, т. к. технология еще не получила широкого распространения. Если установлено значение “auto” (проверять для всех зон) или “yes” (проверять только для тех зон, для которых задан публичный ключ), измените его на “no” (не проверять): `dnssec-validation no;`

В папке bind есть так же файл `named.conf.options`, но при установке FreeIPA в файле настроек указана загрузка именно `ipa-options-ext.conf`. Проверить, что ваши изменения были внесены в правильном файле можно утилитой named-checkconf с ключом p:

```
named-checkconf -p
```

Перезапустите службу разрешения имен и проверьте, что у вас есть доступ к серверам времени:

```
systemctl start bind9.service
nslookup ntp.org
```

Отметим, что после продвижения сервера до контроллера домена DNS-служба будет запускаться как `bind9-pkcs11.service` с аутентификацией в домене по keytab файлу.

7.2. Задайте имя сервера

При продвижении сервера до контроллера домена используется значение HOSTNAME, которое должно быть задано в формате «имя_сервера.полное_имя_домена», поэтому для будущего контроллера с именем «dc-1» в домене «ald.company.local» следует указать «dc-1.ald.company.local». Сделать это можно редактированием файла `/etc/hostname` напрямую или с помощью утилиты `hostnamectl`. После смены имени для проверки следует также перезапустить bash.

```
hostnamectl set-hostname dc-1.ald.company.local
exec bash
hostnamectl
echo $HOSTNAME
```

Чтобы имена dc-1 и dc-1.ald.company.local всегда разрешались в localhost, в файле `/etc/hosts` нужно изменить содержание второй строки:

```
### vi /etc/hosts
127.0.0.1   localhost
127.0.1.1   dc-1 dc-1.ald.company.local
```

Проверить можно командой ping:

```
ping dc-1
ping dc-1.ald.company.local
```

7.3. Выполните скрипт продвижения

Для продвижения сервера выполните скрипт `aldpro-server-install.sh`.

```
set +o history
/opt/rbta/aldpro/mp/bin/aldpro-server-install.sh -d ald.company.local -n dc-
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
↪1 -p 'AstraLinux_172' --no-reboot
set -o history
```

Так как команда содержит пароль в открытом виде, перед ее вызовом рекомендуется отключать запись истории команд. Если вы забыли это сделать, удалите последнюю команду из истории с помощью `history -d $(history 1)` или напрямую отредактируйте файл `/root/.bash_history`

Комментарии по использованным ключам:

d — имя домена

n — имя сервера

p — пароль администратора домена

no-reboot — отменяет перезагрузку после завершения процедуры настройки. Выполнение скрипта занимает некоторое время, поэтому мы рекомендуем выполнить перезагрузку вручную после ознакомления с журналом.

Описание параметров скрипта можно получить с помощью ключа -h

> **Предупреждение:** Имя хоста, которое вы передаете в параметр -d должно быть таким же, какое возвращает команда hostname, иначе служба каталога не сможет получить доступ к собственному keytab файлу.

Пароль должен быть не менее 8 символов. Для использования специальных символов в пароле, например знака доллара, заключите пароль в одинарные кавычки.

Скрипт является неинтерактивным, вам следует определить все указанные параметры для корректного продвижения сервера

Для применения всех настроек выполните перезагрузку сервера:

```
reboot
```

После загрузки войдите в систему, используя доменную учетную запись администратора с паролем из строки продвижения сервера:

```
login: admin

password: ********** (пароль администратора домена)
```

Так как в кеше SSSD службы нет учетных данных администратора, то первый вход возможен будет только при доступности Центра распределения ключей и Службы каталога. Для запуска этих служб может потребоваться чуть больше времени, чем появится окно приветствия, поэтому, если у вас не получилось войти на сервер под доменной учетной записью сразу, подождите пару минут и попробуйте еще раз. И вы всегда можете войти локальным пользователем, чтобы проверить состояние этих служб через утилиту `ipactl`:

```
### ipactl status
Directory Service: RUNNING
krb5kdc Service: RUNNING
kadmin Service: RUNNING
named Service: RUNNING
httpd Service: RUNNING
ipa-custodia Service: RUNNING
smb Service: RUNNING
winbind Service: RUNNING
ipa-otpd Service: RUNNING
ipa-dnskeysyncd Service: RUNNING
ipa: INFO: The ipactl command was successful
```

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.local`

Для проверки работы портала добавьте настройку глобального перенаправления, чтобы BIND9 использовал внешний резолвер, 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». И не забудьте нажать кнопку «Сохранить» в правом верхнем углу.

7.4. Отключите DNSSEC, настройте глобальное перенаправление

После установки FreeIPA отключите DNSSEC, теперь уже в файле `/etc/bind/ipa-options-ext.conf`, и перезапустите DNS службу еще раз, см. выше.

Для завершения настройки портала добавьте 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». И не забудьте нажать кнопку «Сохранить» в правом верхнем углу.

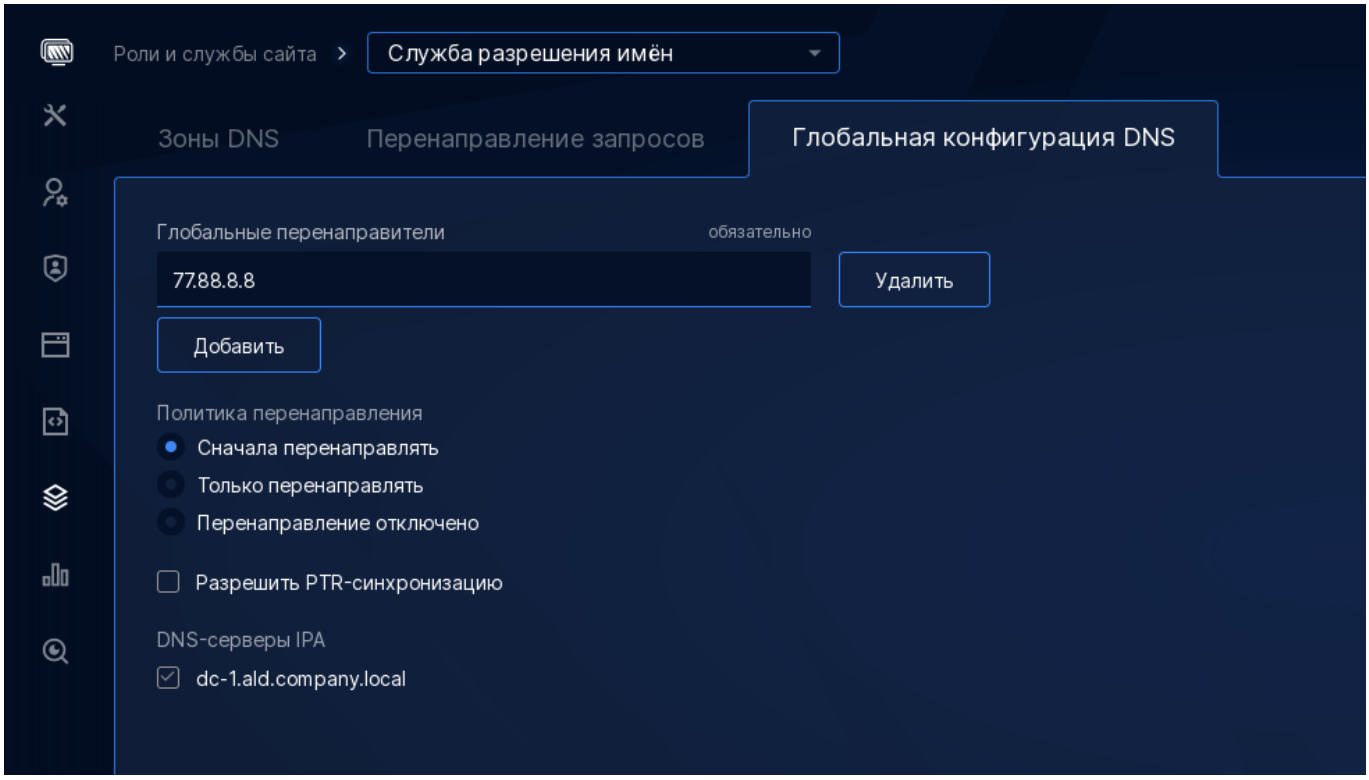

Рисунок 7.1 – Настройка глобального перенаправления

Проверить настройки DNS службы можно из командной строки:

```
ipa dnsconfig-show
```

В некоторых инструкциях для проверки DNS предлагают использовать утилиту dig с ключом +trace, но в этом случае dig вместо того, чтобы обратиться к внешнему резолверу, станет выполнять рекурсивные запросы, начиная с зоны верхнего уровня. Поэтому, если вы все же хотите увидеть подтверждение, что при разрешении имен запросы пошли к

внешнему резолверу, запустите в отдельном окне tcpdump для прослушивания пакетов, отправляемых на 53 порт:

```
apt-get install tcpdump
tcpdump port 53
```

Создайте VM для пользовательского компьютера (pc-1.ald.company.local)

Ввод пользовательского компьютера в домен «ALD Pro» можно осуществить двумя способами: вручную и автоматически при установке ОС по сети. В данной инструкции выполним ввод компьютера в домен вручную.

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

- **Укажите 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
- **Укажите имя и размер файла:**
  - Путь: по умолчанию
  - Размер: 32 ГБ

После создания виртуальной машины в ее настройках

- **на вкладке «Система:raw-latex:Процессор» укажите**
  - Процессоры: 2 ЦП
- **на вкладке «Носители» для компакт-диска укажите установочный файл** ALSE «1.7.1-22.11.2021_10.50.iso», md5 диска de1e72c271497a2b27909ea148f93f1f
- **на вкладке «Сеть» выберите:**

- тип подключения: Сеть NAT
- имя: Стенда 001

Загрузите виртуальную машину с диска и с помощью мастера установите операционную систему с графическим окружением, уровень безопасности пользовательского компьютера может быть любым.

Установите клиентские пакеты ALD Pro на PC-1

9.1. Настройте сеть 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, но в рамках данной инструкции с целью 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.local (см. про DNS-суффикс выше)

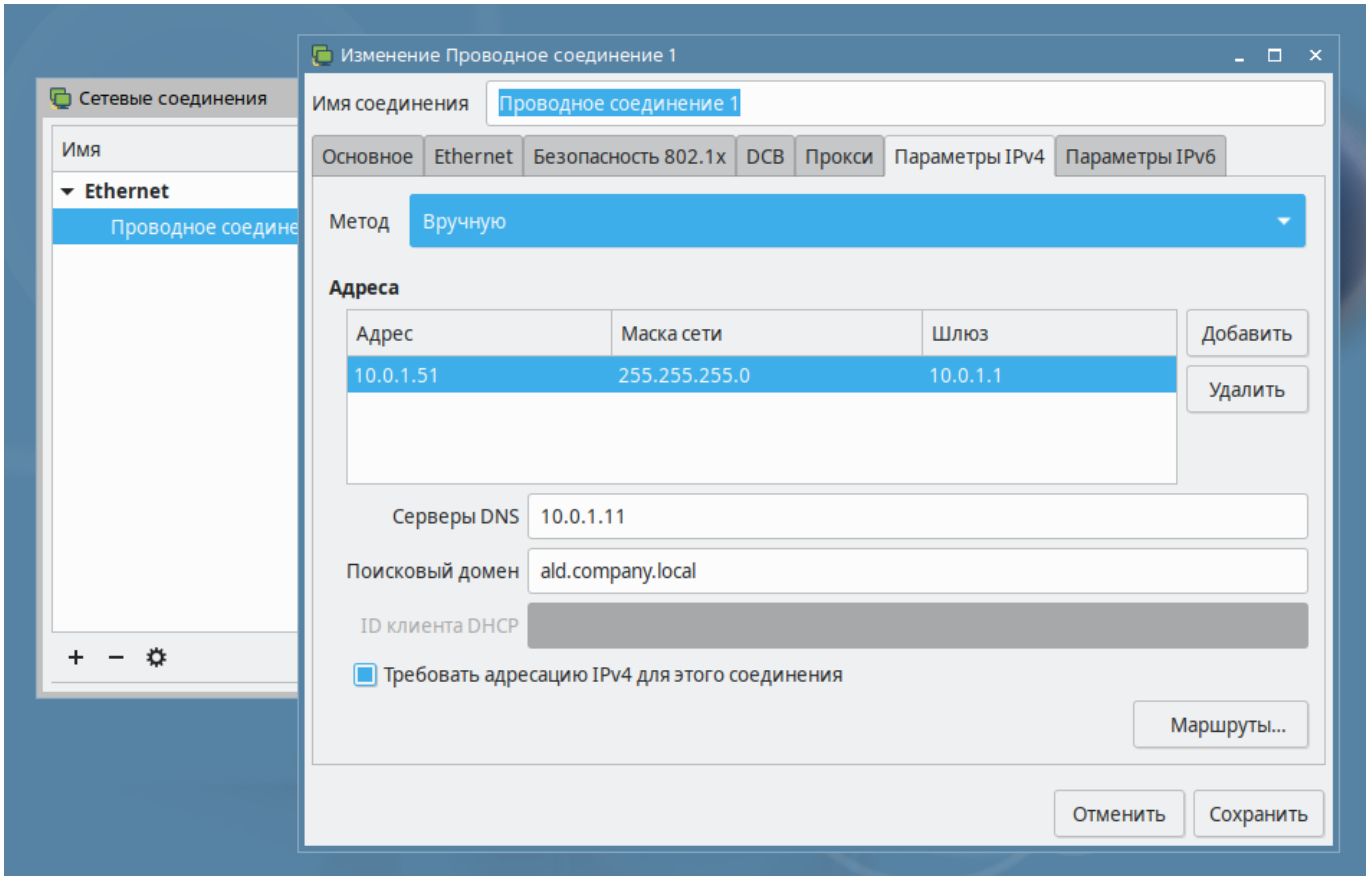

Рисунок 9.1 – Настройка параметров IPv4

Можете проверить результат ваших действий командами:

```
ip a
ping 77.88.8.8
ping dl.astralinux.ru
ping dc-1.ald.company.local
ping dc-1
```

9.2. Настройте доступные репозитории

Для установки клиентской части ALD Pro версии 1.2 на ALSE 1.7.2 из официальных интернет-репозиториев РусБИТех-Астра содержание файла `/etc/apt/soureces.list` должно быть таким же, как при установке серверной части:

```
### vi /etc/apt/sources.list
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.2/repository-base/ 1.
↪7_x86-64 main contrib non-free
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.2/repository-
↪extended/ 1.7_x86-64 main contrib non-free
deb https://dl.astralinux.ru/aldpro/stable/repository-main/ 1.2.0 main
deb https://dl.astralinux.ru/aldpro/stable/repository-extended/ generic main
```

Настройте приоритеты, так же как делали на сервере

```
### vi /etc/apt/preferences.d/aldpro
Package: *
Pin: release n=generic
Pin-Priority: 900
```

Обновите индекс и проверьте, нет ли пакетов, доступных для обновления. Обновите систему, если таковые будут обнаружены:

```
apt update
apt list --upgradable
apt upgrade -y
```

9.3. Установите пакеты

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

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

Комментарии к использованным ключам можно найти в разделе инструкции по установке пакетов на сервере.

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/sssd/sssd.log`)

Выполните 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.

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

```
nslookup pc-1
```

Данная команда проверит не только имя «pc-1», но и «pc-1.ald.company.local», т. к. в настройках NetworkManager на предыдущем шаге мы указали DNS-суффикс «ald.company.local». Данная команда должна подтвердить, что хост с указанным именем не найден на DNS сервере.

Установить имя хоста нужно в формате «имя_сервера.полное_имя_домена», поэтому для пользовательского компьютера с именем «pc-1» в домене «ald.company.local» следует указать значение «pc-1.ald.company.local»

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

Вы также можете сгенерировать случайное имя хосту следующей командой:

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

Все готово для ввода компьютера в домен:

```
set +o history
/opt/rbta/aldpro/client/bin/aldpro-client-installer -c ald.company.local -u
↪admin -p 'AstraLinux_172' -d pc-1 -i -f
```

Комментарии по использованным ключам:

c — имя домена

u — логин администратора домена

p — пароль администратора домена

d — имя компьютера

i — использовать интерактивный режим

f — продолжает ввод компьютера в домен, даже если возникнут какие-либо ошибки в ходе этого процесса

Для применения всех настроек выполните перезагрузку компьютера:

```
reboot
```

После перезагрузки войдите в систему, используя доменную учетную запись администратора с паролем из строки продвижения сервера:

```
login: admin

password: ********** (пароль администратора домена)
```

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

Проверка работы синхронизации времени

Вопрос синхронизации времени требует отдельного рассмотрения, так как для работы протокола проверки подлинности Kerberos необходимо, чтобы время на клиенте и на сервере расходилось не более, чем на 5 минут.

По умолчанию в Astra Linux синхронизация времени отключена, но виртуальные машины VirtualBox берут время из хостовой операционной системы во время загрузки после полного выключения, поэтому отсутствие синхронизации времени можно заметить только при работе с горячими снимками, которые были сделаны во время работы операционной системы.

При установке ALD Pro (как клиентской, так и серверной части) в системе появляется служба `chrony`, содержание конфигурационного файла которой автоматически редактируется через механизм групповых политик в соответствии с текущими настройками домена «Роли и службы сайта Служба синхронизации времени». Пользовательские компьютеры синхронизируют время с контроллером, а контроллер берет его у публичных серверов.

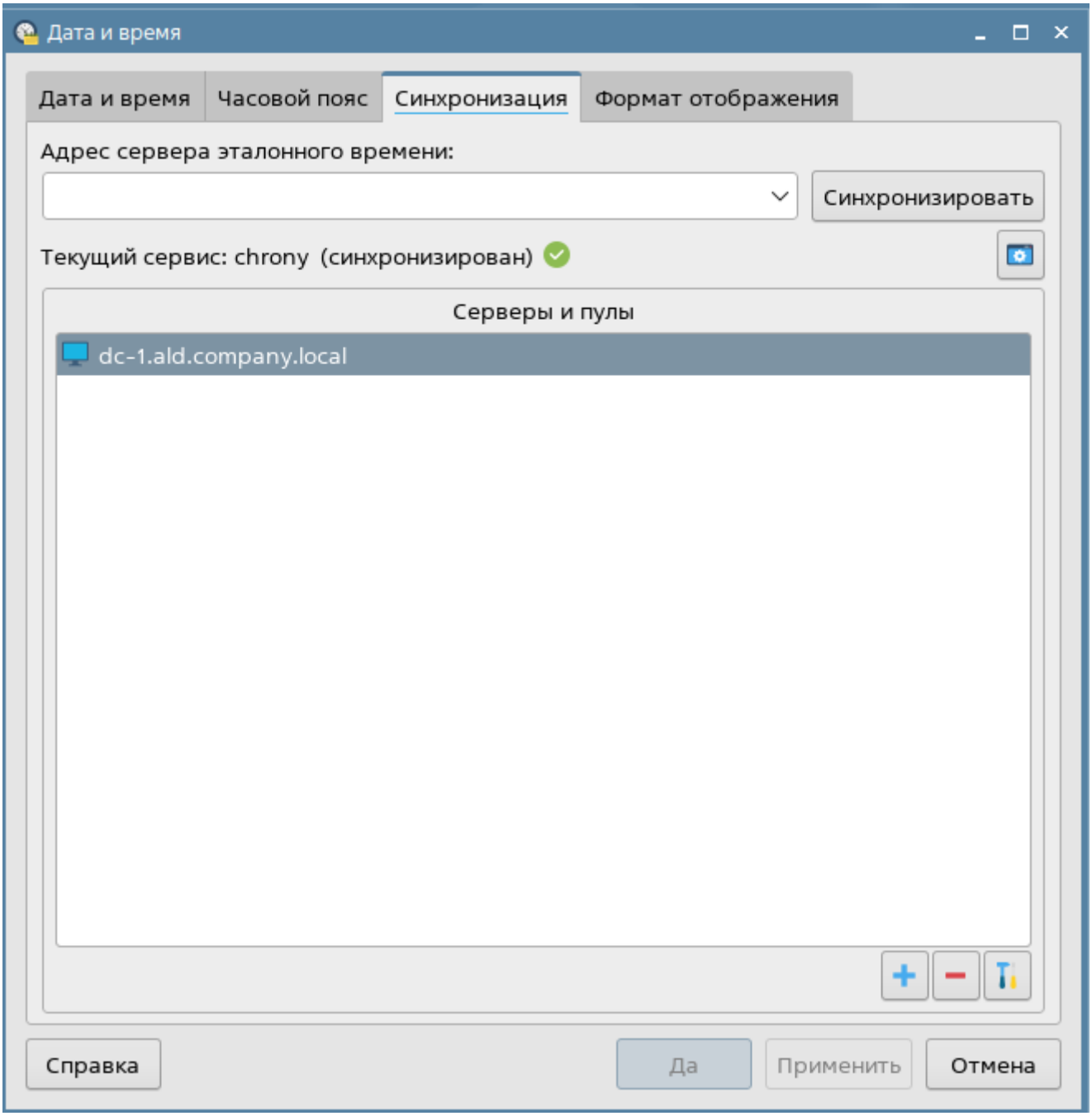

Рисунок 11.1 – Синхронизация даты и времени 1

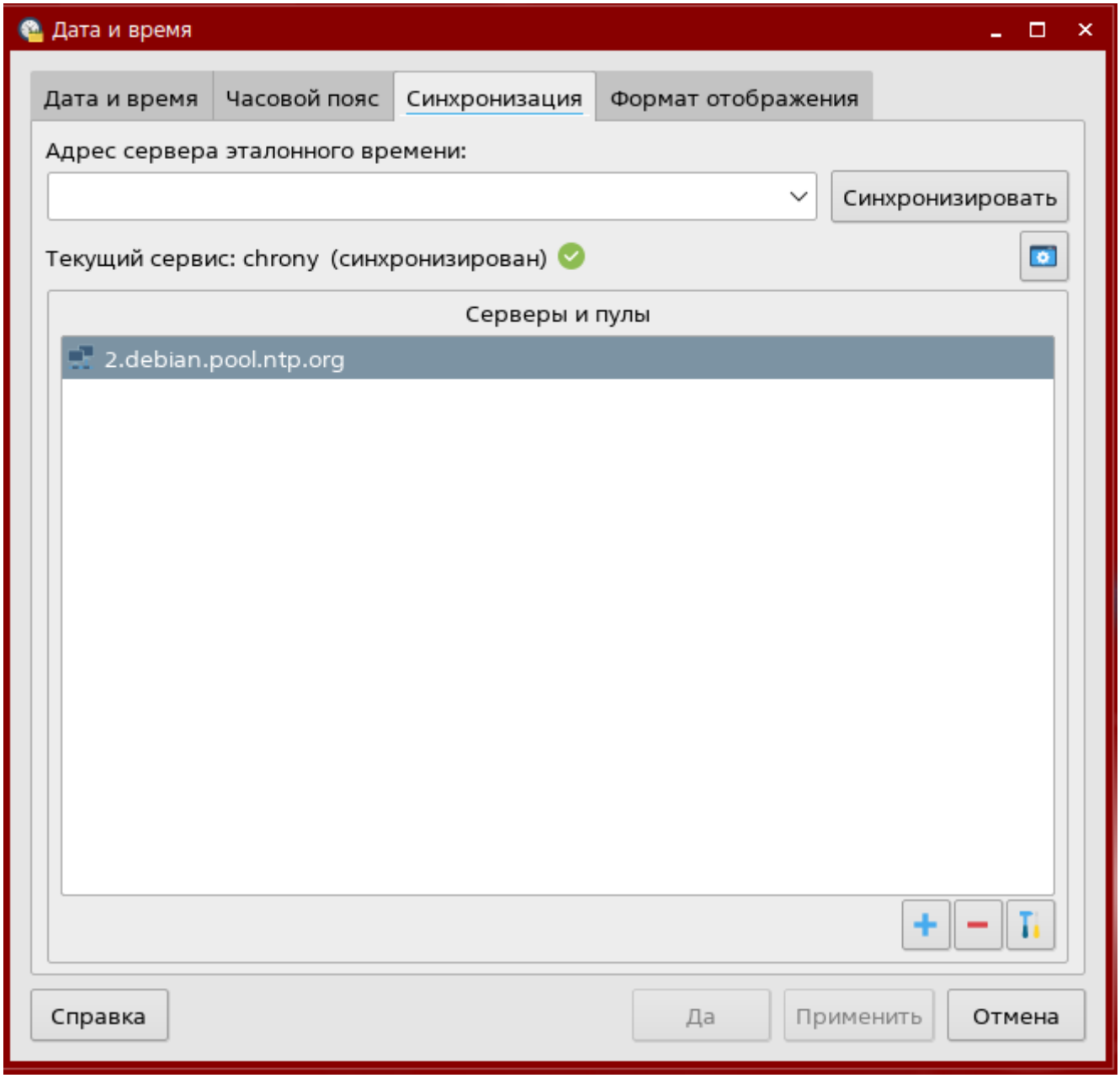

Рисунок 11.2 – Синхронизация даты и времени 2

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

```
systectl 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.local        2   6   377    51  +4571ns[  -48us] +/-
 ↪19ms
...
```

В настройках `chrony`, которые использует ALD Pro, указан параметр makestep, поэтому при выполнении синхронизации компьютер сразу устанавливает требуемое значение. Если у вас будет отсутствовать параметр makestep, то служба будет крайне медленно «подтягивать» время к требуемом значению (по несколько секунд в минуту), и вам будет казаться, что синхронизация времени не работает. Форсировать переход к целевому значению в этом случае вы можете вызовом команды makestep через chornyc:

```
chronyc makestep
```

В настройках `chrony`, которые использует ALD Pro, указан параметр rtcsync, поэтому клиенты сверяют часы каждые 11 минут. Параметр rtcsync так же необходим для того, чтобы служба chrony при синхронизации времени сбрасывала флаг STA_UNSYNC, иначе в приложении «Дата и время» у вас будет оставаться предупреждение об отсутствии синхронизации.

Если требуется проверить работу NTP-сервера, вы можете воспользоваться командой `ntpdate` с ключом q (query only, отправить только запрос без изменения времени). Крайне полезными являются также ключи v и d, включающие подробный вывод (verbose) и отладку (debugging) соответственно.

```
ntpdate -qvd dc-1.ald.company.local
```

После синхронизации времени указанная выше команда `timedatectl` может показать расхождение между системным временем ALSE (Universal time) и значением времени в BIOS (RTC time, real time clock), так как запись в BIOS происходит только при выключении компьютера. 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`:

```
admin@dc-1:~$ kinit
Password for admin@ALD.COMPANY.LOCAL: *********
```

Информацию о выданных билетах можно увидеть командой `klist`:

```
admin@dc-1:~$ klist Ticket cache:
KEYRING:persistent:1194600000:krb_ccache_Y1bhW3f Default principal:
admin@ALD.COMPANY.LOCAL valid starting Expires Service principal
16.10.2022 14:40:20 17.10.2022 14:40:18
krbtgt/ALD.COMPANY.LOCAL@ALD.COMPANY.LOCAL
```

Как работает вход в доменный компьютер

При входе пользователя в доменный компьютер аутентификация осуществляется по протоколу Kerberos.

Протокол назван так по имени трехголовой собаки Цербера, охраняющей выход из царства мёртвых по древнегреческой мифологии. Каждая голова этой собаки соответствует одному из трех участников процедуры аутентификации:

Клиент (Client) — субъект, желающий получить доступ к ресурсу.

Сервер приложения (Application Server, AP) — служба, к ресурсу которой клиент хочет получить доступ.

Центр распределения ключей (Key Distribution Center, KDC) — доверенная третья сторона, отвечающая за аутентификацию (Authentication Servicec, AS) пользователей и выпуск билетов для доступа к сетевым службам в домене (Ticket Granting Server, TGS).

Рассмотрим процесс аутентификации пользователя. Просим учесть, что описание является упрощенным для понимания принципиальных аспектов работы протокола. Например, мы упускаем детали предварительной аутентификации, не рассматриваем использование случайных чисел (nonce) и др.

1. Пользователь Алиса через приложение графического входа (Fly Display Manager Greet) передает логин и пароль в открытом виде клиенту Керберос, в роли которого выступает System Security Services Daemon (SSSD). Учетные данные пользователя обрабатываются стеком модулей аутентификации (Pluggable Authentication Modules, PAM).

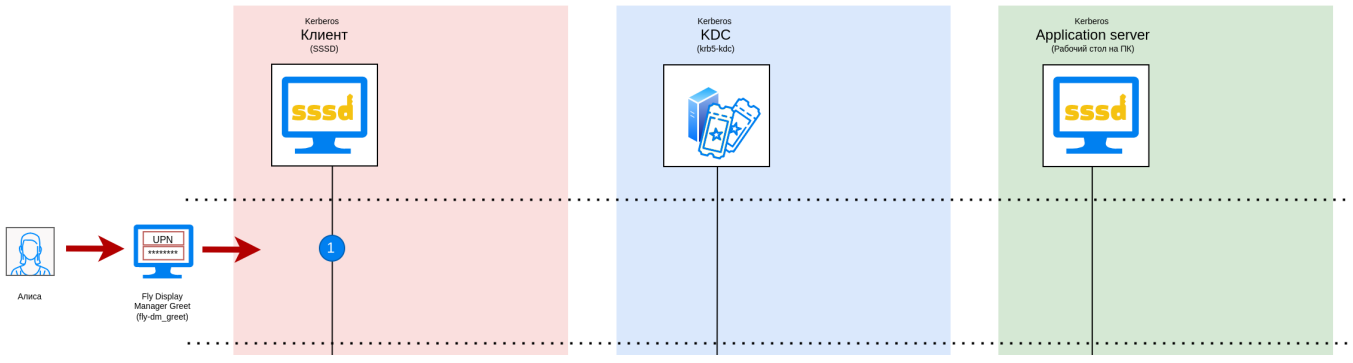

Рисунок 12.1 – Как работает вход в доменный компьютер 1

2. Клиент Керберос рассчитывает долгосрочный мастер ключ Алисы (UPN long-term key или Master key), как хэш от введенного пароля, и может удалить из памяти компьютера пароль в открытом виде для повышения устойчивости системы к взлому.

Рисунок 12.2 – Как работает вход в доменный компьютер 2

3. Клиент отправляет запрос службе аутентификации Центра распределения ключей (Key Distribution Center, KDC).

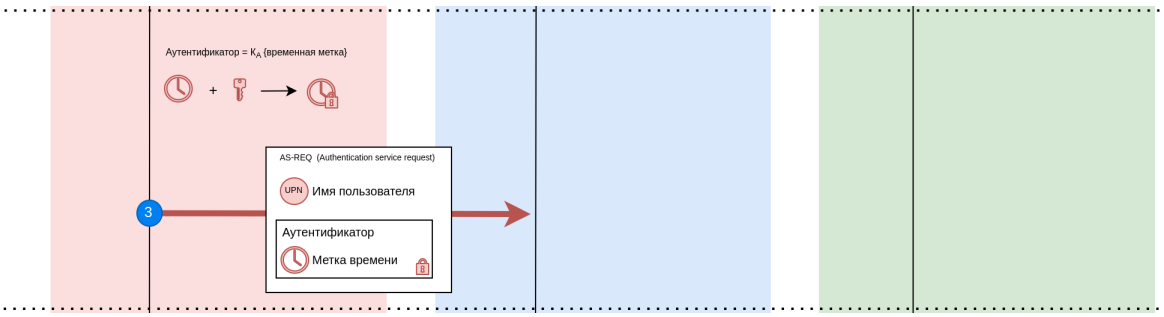

Рисунок 12.3 – Как работает вход в доменный компьютер 3

4. KDC расшифровывает аутентификатор, используя хэш пароля Алисы из LDAP-каталога. Ключи для аутентификации по протоколу керберос хранятся в атрибуте krbPrincipalKey, который представляет из себя бинарный объект, зашифрованный мастер-ключом KDC.

Если процедура расшифровки завершилась успешно и полученная временная метка расходится с временем сервера не более, чем на 5 минут, то считается, что предварительная аутентификация пройдена успешно. По этой причине для корректной работы kerberos-протокола так важна синхронизация времени между всеми участниками.

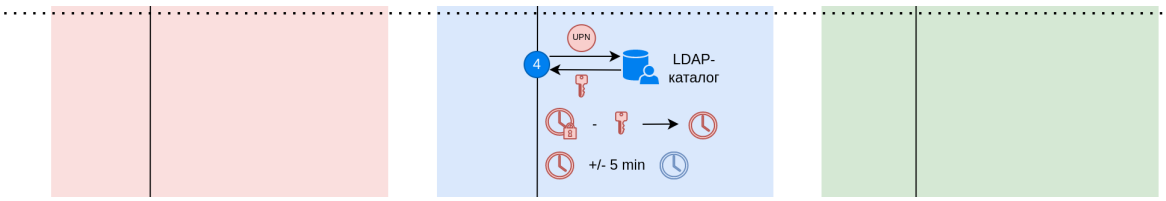

Рисунок 12.4 – Как работает вход в доменный компьютер 4

5. Для повышения безопасности системы KDC генерирует временный сессионный ключ (S1) и передает его клиенту, чтобы использовать в дальнейшем для шифрования сообщений между клиентом и KDC вместо хэша пароля пользователя.

Рисунок 12.5 – Как работает вход в доменный компьютер 5

6. Не смотря на то, что сессионный ключ был сгенерирован сервером, в домене может быть несколько контроллеров, и Клиент вправе обратиться с последующим запросом к любому из них. Клиенту выдается билет на выдачу билетов (Ticket-granting ticket, TGT), который он должен предъявлять в KDC при последующих обращениях.

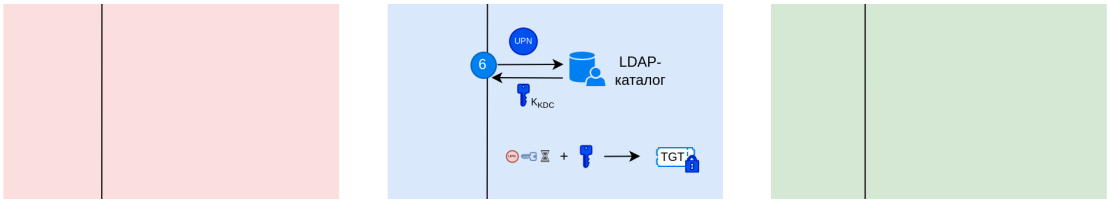

Рисунок 12.6 – Как работает вход в доменный компьютер 6

7. Сессионный ключ и билет шифруются симметричным алгоритмом с помощью долгосрочного ключа клиента, поэтому только клиент сможет расшифровать сообщение, подтверждая этим фактом, что является тем, за кого себя выдает. Данная проверка аутентичности считается основной.

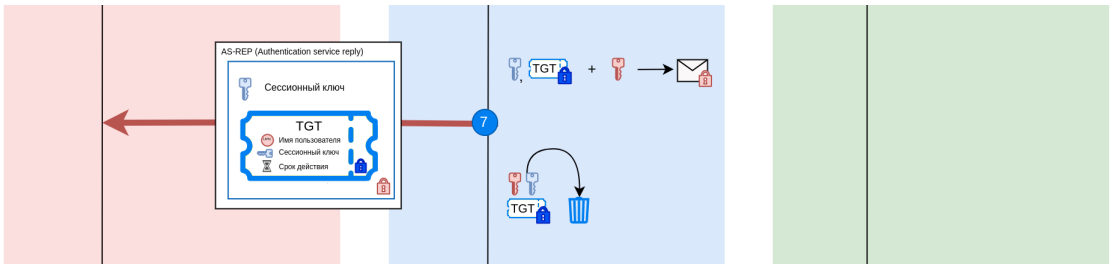

Рисунок 12.7 – Как работает вход в доменный компьютер 7

8. Клиент расшифровывает сессионный ключ и TGT билет своим долгосрочным ключом. Возможность использования этих данных в последующих запросах означает, что Клиент является тем, за кого себя выдает.

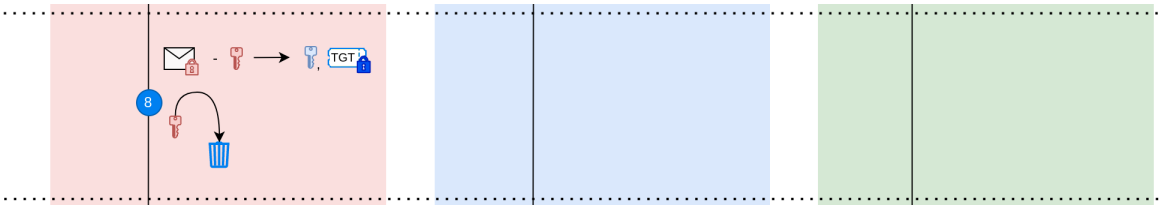

Рисунок 12.8 – Как работает вход в доменный компьютер 8

9. Клиент отправляет контроллеру запрос на доступ к серверу приложению, в котором содержится имя пользователя, имя сервера приложения, билет на выдачу билетов

(TGT) и аутентификатор. В качестве аутентификатора выступает метка времени, зашифрованная симметричным алгоритмом с помощью сессионного ключа S1.

Рисунок 12.9 – Как работает вход в доменный компьютер 9

10. KDC расшифровывает информацию из TGT билета, используя долгосрочный ключ KDC из LDAP-каталога, после чего ему становится доступна следующая информация: имя пользователя, сессионный ключ и срок действия билета. Сервер расшифровывает аутентификатор, используя сессионный ключ из TGT билета, и, если полученное значение расходится с временем сервера не более, чем на 5 минут, то считается, что аутентификация пройдена успешно.

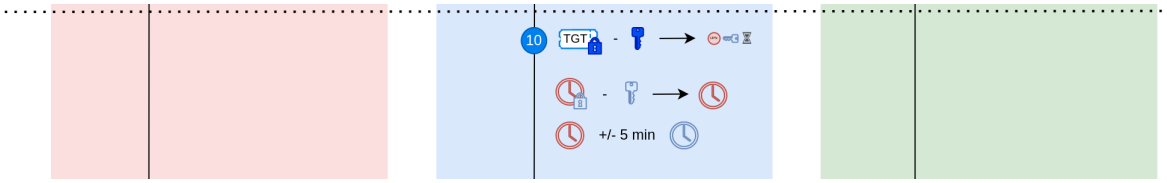

Рисунок 12.10 – Как работает вход в доменный компьютер 10

11. Для повышения безопасности протокола KDC генерирует новый сессионный ключ (S2) и передает его клиенту, чтобы использовать в дальнейшем для шифрования сообщений между клиентом и сервером приложения вместо сессионного ключа S1.

Рисунок 12.11 – Как работает вход в доменный компьютер 11

12. Ключ S2 был сгенерирован сервером KDC и его следует передать Серверу приложения. Клиенту выдается зашифрованный сервисный билет (Service ticket, ST), который он должен предъявлять серверу приложения.

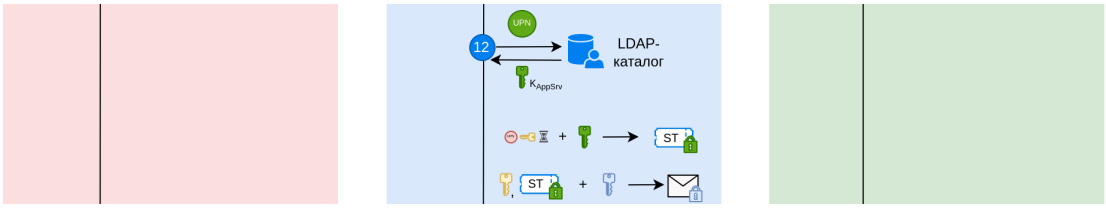

Рисунок 12.12 – Как работает вход в доменный компьютер 12

13. После передачи сервисного билета Клиенту информация о ключах больше не требуется и может быть удалена для повышения безопасности системы.

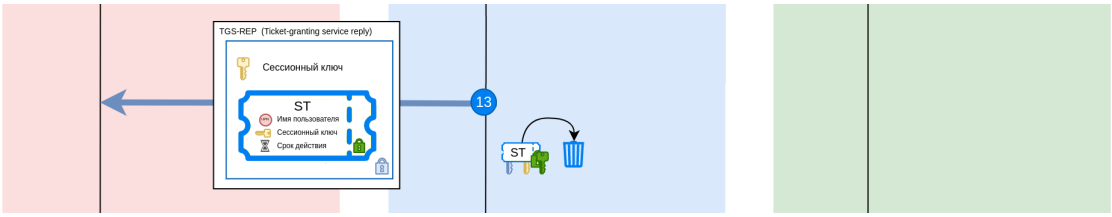

Рисунок 12.13 – Как работает вход в доменный компьютер 13

14. Клиент расшифровывает сессионный ключ S2 и сервисный билет ST известным ему сессионным ключом S1. Возможность использования этих данных в последующих запросах означает, что Клиент является тем, за кого себя выдает.

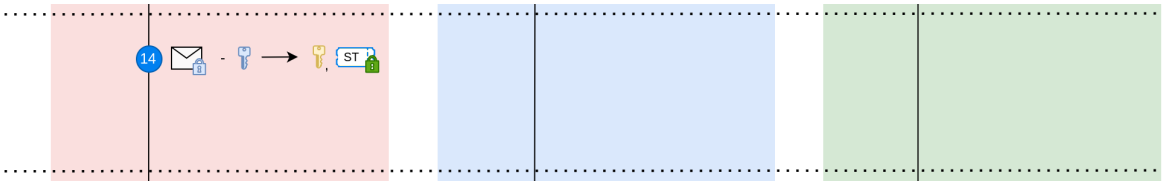

Рисунок 12.14 – Как работает вход в доменный компьютер 14

15. Клиент отправляет серверу приложения запрос на аутентификацию, в котором содержится имя пользователя, сервисный билет (ST) и аутентификатор. В качестве аутентификатора выступает метка времени, зашифрованная симметричным алгоритмом с помощью сессионного ключа S2.

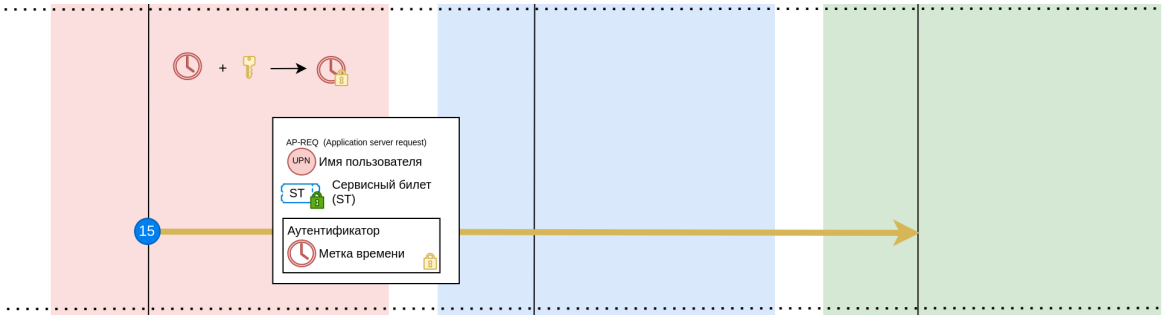

Рисунок 12.15 – Как работает вход в доменный компьютер 15

16. Сервер приложения, в роли которого выступает служба SSSD на пользовательском компьютере расшифровывает ответ. Используя этот долгосрочный ключ, служба

SSSD может расшифровать информацию из сервисного билета (ST), после чего ей становится доступна следующая информация: имя пользователя, сессионный ключ S2 и срок действия билета. SSSD расшифровывает аутентификатор, используя сессионный ключ S2 из сервисного билета, и, если полученное значение расходится с временем компьютера не более, чем на 5 минут, то считается, что аутентификация пройдена успешно.

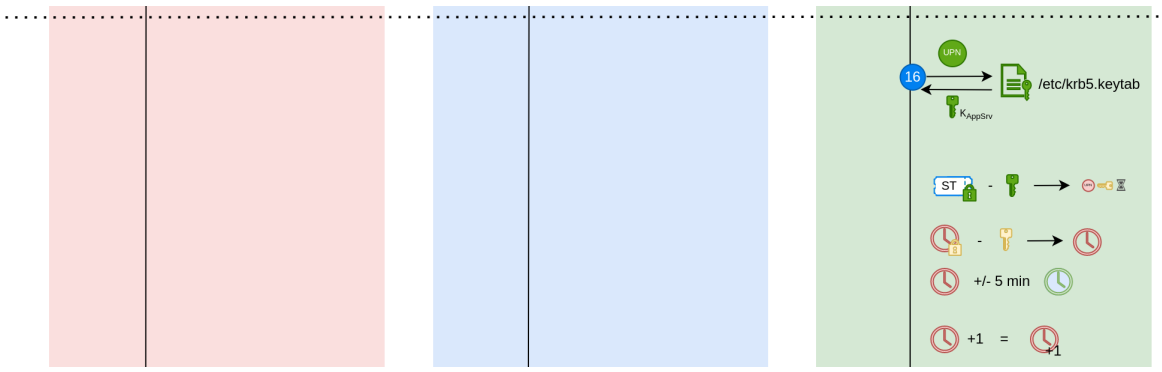

Рисунок 12.16 – Как работает вход в доменный компьютер 16

17. Для подтверждения сервером приложения своей аутентичности он увеличивает полученную метку времени на 1, шифрует симметричным алгоритмом, используя сессионный ключ S2, и возвращает клиенту. Данное подтверждение актуально при аутентификации в сетевых приложения, когда клиент и сервер приложения являются разными субъектами.

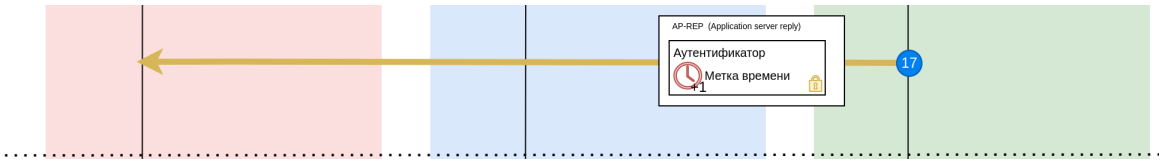

Рисунок 12.17 – Как работает вход в доменный компьютер 17

18. Клиент расшифровывает аутентификатор, используя сессионный ключ S2. Если полученное значение можно получить, прибавляя 1 к ранее отправленному значению, то взаимная аутентификация считается пройденной успешно. Получив подтверждение, что вход в компьютер действительно хочет выполнить Алиса, приложение DM запускает приложение рабочий стол (Fly Windows Manager, fly-wm) от ее имени.

Рисунок 12.18 – Как работает вход в доменный компьютер 18

Как управлять билетами Kerberos из командной строки

Информацию о выданных билетах можно увидеть командой `klist`:

```
admin@dc-1:~$ klist
Ticket cache: KEYRING:persistent:1194600000:krb_ccache_Y1bhW3f
Default principal: admin@ALD.COMPANY.LOCAL
valid starting  Expires Service principal
16.10.2022 14:40:20 17.10.2022 14:40:18 krbtgt/ALD.COMPANY.LOCAL@ALD.COMPANY.
 ↪LOCAL
```

Очистить кэш можно командой `kdestroy`:

```
admin@dc-1:~$ kdestroy
```

Пройти аутентификацию в домене можно командой kinit:

```
admin@dc-1:~$ kinit Password for admin@ALD.COMPANY.LOCAL: *********
```

Сменить пароль текущего пользователя можно командой kpasswd:

```
admin@dc-1:~$ kpasswd Password for admin@ALD.COMPANY.LOCAL: *********
```