ALD Pro

# РУКОВОДСТВО АДМИНИСТРАТОРА. ЧАСТЬ 1

РДЦП.10101-01 95 01-02
Версия 3.0.0

# Содержание


**1 Общие сведения** **3**

1.1 Требования к квалификации администратора . . . . . 3

1.2 Функциональное назначение . . . . . 3

1.3 Технологический стек . . . . . 4

1.4 Планирование ресурсов . . . . . 6

1.4.1 Вертикальное масштабирование . . . . . 6

1.4.2 Горизонтальное масштабирование . . . . . 12

1.4.3 Результаты нагрузочного тестирования . . . . . 15

1.4.4 Практический кейс по планированию ресурсов . . . . . 18

1.5 Рекомендации по именованию домена . . . . . 23

**2 Развертывание контроллеров домена и подсистем** **25**

2.1 Развертывание первого контроллера домена . . . . . 25

2.1.1 Подготовка окружения сервера к установке контроллера домена . . . 25

2.1.2 Установка пакетов . . . . . 31

2.1.3 Повышение роли сервера до контроллера домена . . . . . 32

2.1.4 Дополнительные настройки DNS . . . . . 35

2.1.5 Глобальный каталог . . . . . 36

2.1.6 Модуль синхронизации . . . . . 37

2.1.7 Проверка работы портала управления . . . . . 38

2.2 Ввод компьютера в домен . . . . . 39

2.2.1 Настройка сети на клиентских компьютерах . . . . . 40

2.2.2 Ввод компьютера в домен . . . . . 48

2.3 Вывод компьютера из домена . . . . . 50

2.3.1 Действия на рабочей станции под управлением Astra Linux Special Edition . . . . . 50

2.3.2 Действия на рабочей станции под управлением Альт Рабочая станция 10.4 и Альт СП 10 . . . . . 52

2.3.3 Действия на рабочей станции под управлением РЕД ОС 7.3.5 и РЕД ОС 8 . . . . . 53

2.3.4 Действия на контроллере домена . . . . . 55

2.4 Установка резервного контроллера домена . . . . . 56

2.4.1 Подготовка к установке резервного контроллера . . . 56
2.4.2 Повышение роли сервера до резервного контроллера домена . . . 59
2.5 Установка подсистемы сетевого репозитория . . . 61
2.5.1 Установка сервера репозиториев . . . 61
2.6 Установка подсистемы общего доступа к файлам . . . 63
2.6.1 Установка сервера общего доступа к файлам . . . 63
2.7 Установка подсистемы сервера печати . . . 66
2.8 Установка подсистемы «Динамическая настройка узла» DHCP . . . 68
2.9 Установка подсистемы «Установка ОС по сети» TFTP + PXE . . . 70
2.10 Установка подсистемы мониторинга . . . 72
2.11 Установка подсистемы журналирования . . . 74
2.12 Установка модуля инвентаризации . . . 76

**3 Обновление подсистем 79**
3.1 Обновление первого контроллера домена . . . 79
3.1.1 Подготовка к обновлению . . . 80
3.1.2 Обновление . . . 83
3.1.3 Обновление с установкой Глобального Каталога . . . 86
3.1.4 Обновление с установкой Модуля Синхронизации . . . 87
3.2 Обновление клиентов домена . . . 87
3.2.1 Подготовка к обновлению . . . 88
3.2.2 Обновление . . . 88
3.3 Обновление репликаций контроллера домена . . . 89
3.3.1 Подготовка к обновлению . . . 89
3.3.2 Обновление . . . 91
3.4 Обновление подсистем . . . 92
3.4.1 Обновление подсистемы сетевого репозитория . . . 92
3.4.2 Обновление подсистемы общего доступа к файлам . . . 93
3.4.3 Обновление подсистемы сервера печати . . . 95
3.4.4 Обновление подсистемы «Динамическая настройка узла» DHCP . . . 96
3.4.5 Обновление подсистемы «Установка ОС по сети» TFTP + PXE . . . 97
3.4.6 Обновление подсистемы мониторинга . . . 99
3.4.7 Обновление подсистемы журналирования . . . 101
3.5 Централизованное обновление менеджера политик программного обеспечения 103

**4 Матрицы совместимости и обновлений 105**
4.1 Матрица совместимости ПК ALD Pro . . . 105
4.2 Матрица обновлений ПК ALD Pro . . . 108

# Общие сведения

## 1.1. Требования к квалификации администратора

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

- Администрирование Linux, основной курс AL-1702
- Администрирование Linux, расширенный курс AL-1703
- Администрирование компьютерных сетей (материалы курса AL-1704)

Администратору важно обладать базовыми навыками администрирования **LDAP**-каталога и использования протокола аутентификации **Kerberos**.

## 1.2. Функциональное назначение

ALD Pro (**Astra Linux Directory Pro**) – это набор сетевых служб сервера **Astra Linux** для организации централизованного управления ИТ-инфраструктурой. Система построена на хорошо известных компонентах с открытым исходным кодом, использующих стандартные протоколы обмена информацией: FreeIPA, 389 Directory Server, MIT Kerberos, Bind9, ISC DHCP, NTP, SSSD, CUPS, Samba, Zabbix, Syslog-NG, RabbitMQ, SaltStack.

В основе лежит служба каталога, которая обеспечивает централизованное хранение данных о пользователях, хостах, сервисных учетных записях и обеспечивает доступ к этой информации по открытым протоколам. Управление системой можно осуществлять из веб-интерфейса, командной строки или через REST API.

Система ALD Pro расширяет возможности по администрированию серверов и рабочих станций следующими функциями:

- централизованное управление учетными записями пользователей и компьютеров, организационной структурой предприятия, конфигурациями доменных компьютеров с помощью применения групповых политик, включая установку и удаление программного обеспечения;

- синхронизация времени на всех компьютерах предприятия;
- автоматизированная установка операционных систем по локальной сети;
- управление печатью и общим доступом к файлам в компьютерной сети предприятия;
- мониторинг серверной группировки и журналирование событий.

## 1.3. Технологический стек

Система ALD Pro использует клиент-серверную архитектуру и состоит из следующих компонентов:

- Серверные подсистемы устанавливаются на выделенный или виртуальный сервер:
  - Контроллер Домена (Портал Управления, FreeIPA, 389 Directory Server, MIT Kerberos, Bind9, Samba, Chrony, SSSD, SaltStack, RabbitMQ)
  - Подсистема Печати (CUPS)
  - Подсистема Общий Доступ к Файлам (Samba)
  - Подсистема Мониторинг (Zabbix)
  - Подсистема Журналирования (Сбора Логов) (Syslog-NG)
  - Подсистема Репозитория ПО (Reprepro)
  - Подсистема Установка ОС по Сети (TFTP + PXE)
  - Подсистема Динамической Настройки Узла (ISC DHCP)
- Клиентская часть — реализована в виде агентов, которые устанавливаются на все компьютеры домена:
  - `aldpro-client` — клиентская часть ALD Pro, через которую устанавливаются и настраиваются остальные клиентские приложения и сервисы;
  - `astra-freeipa-client` — утилита от **Astra Linux** для внесения дополнительных настроек в конфигурацию `sssd` и других служб в соответствии с требованиями операционной системы;
  - `freeipa-client` — клиентская часть подсистемы FreeIPA, настраивает службу `sssd`;
  - `krb5-user` — поддержка работы с **Kerberos**, утилиты `kinit` и др.;
  - `sssd` — набор служб для работы машины в домене;
  - `sssd-ldap` — **LDAP** бэкенд службы `sssd`;

- `ldap-utils` — утилиты `ldapsearch` и др.;
- `freeipa-admintools` — набор утилит администрирования `ipa CLI`;
- `aldpro-salt-minion` — клиентская часть групповых политик;
- `zabbix-agent` — клиентская часть подсистемы мониторинга;
- `syslog-ng` — клиентская часть подсистемы журналирования;

Для обеспечения базовой функциональности ALD Pro необходимо установить один контроллер домена. Для обеспечения отказоустойчивости и возможности обслуживать систему без прерывания доступа к сервисам аутентификации и авторизации рекомендуется устанавливать не менее двух контроллеров. Минимальную конфигурацию оборудования для развертывания подсистем, см. table_1.

| Компонент | CPU Ядер | RAM | SSD | Кол-во |
|---|---|---|---|---|
| Контроллер Домена до 3 тыс. пользователей | 4 | 8 ГБ | >= 50 ГБ | 2 шт. |
| Дополнительные ресурсы на 10 тыс. пользователей | 10 | 0.5 ГБ | 0.5 ГБ | |
| Подсистема Мониторинга | 2 | 2 ГБ | >= 30 ГБ | 1 шт. |
| Подсистема «Динамическая Настройка Узла» (DHCP) | 2 | 2 ГБ | >= 30 ГБ | 1 шт. |
| Подсистема «Репозитории ПО» | 2 | 2 ГБ | >= 100 ГБ | 1 шт. |
| Подсистема «Установка ОС по сети» (PXE) | 2 | 2 ГБ | >= 30 ГБ | 1 шт. |
| Подсистема «Служба Печати» | 2 | 2 ГБ | >= 30 ГБ | 1 шт. |
| Подсистема «Общий Доступ к Файлам» | 2 | 2 ГБ | >= 30 ГБ | 1 шт. |

Таблица 1 — Минимальные характеристики для установки подсистем ALD Pro

**Внимание:** Запрещено устанавливать в одной операционной системе сразу несколько подсистем ALD Pro, т.к. это может привести к некорректной работе продукта и нежелательной конкуренции за ресурсы **CPU** и **RAM**.

## 1.4. Планирование ресурсов

От работы доменных служб зависит надежность работы всей ИТ инфраструктуры, поэтому при планировании домена администраторы должны действовать проактивно и применять различные способы вертикального и горизонтального масштабирования, чтобы исключить проблемы недостаточной производительности. Ниже представлены рекомендации, которые помогут в решении указанной задачи.

### 1.4.1. Вертикальное масштабирование

Вертикальным масштабированием называют повышение производительности системы за счет повышения производительности отдельного узла путем выделения серверу дополнительных вычислительных ресурсов — оперативной памяти, потоков центрального процессора и т.п.

#### 1.4.1.1. Объем памяти

В работе службы каталога преобладают операции чтения, поэтому в производительности контроллера решающую роль играет достаточный объем оперативной памяти, чтобы контроллер мог обрабатывать запросы без обращения к медленным дискам.

Файлы каталога расположены в папке */var/lib/dirsrv*, после развертывания первого контроллера размер базы составляет не менее 45 Мб и увеличивается по мере создания объектов, в среднем по 50 КБ на каждую дополнительную учетную запись пользователя. Таким образом, объем памяти диска рассчитывается: для нужд самой операционной системы контроллеру следует выделить не менее 50 ГБ, а под хранение каталога для упрощения расчетов выделяется по 1 ГБ на каждые 20 тысяч объектов. Расчетное значение должно составлять не более 40% от доступного пространства.

$$HDD,\ GB = 50 + N\ objects/20\,000$$

**Внимание:** Производительность файловой подсистемы влияет на скорость записи, поэтому рекомендуется использовать SSD или RAID с высокой производительностью чтения/записи. Скорость произвольного чтения у современных твердотельных дисков составляет порядка 50-100 тысяч операций в секунду (IOPS).

Ещё одним вариантом увеличения производительности LDAP может быть использование разных устройств для корня файловой системы (/) и каталога с БД (*/var/lib/dirsrv/*). Смотрите руководство администратора ОС, раздел монтирования дисков.

Для загрузки каталога требуется больше оперативной памяти, т.к. для ускорения операций поиска служба **ns-slapd** индексирует данные каталога. Пустая база данных занимает в памяти не менее 65 Мб, и это значение растет по мере увеличения числа объектов, на каждую дополнительную учетную запись в среднем добавляется 50 КБ. Таким образом, минимально необходимый объем оперативной памяти можно рассчитать математически: для нужд самой операционной системы контроллеру следует выделить порядка 2-3 ГБ, а для работы с каталогом в целях упрощения расчетов возьмем по 1ГБ на каждые 20 тысяч объектов:

$$RAM,\ GB = 3 + N\ objects/20\ 000$$

Ниже приведено несколько примеров:

- Для работы с каталогом, в котором содержится 10 000 пользователей и 100 групп, контроллеру нужно выделить порядка 4 ГБ ОЗУ:

$$RAM,\ GB = 3 + 10\ 100\ objects/20\ 000 \approx 4\ GB\ RAM$$

- Для работы с каталогом, в котором 100 000 пользователей и 30 000 групп, контроллеру нужно выделить до 10 ГБ ОЗУ:

$$RAM,\ GB = 3 + 130\ 000\ objects/20\ 000 \approx 10\ GB\ RAM$$

---

**Примечание:** При создании учетных записей контроллер домена потребляет в два раза больше оперативной памяти, т.е. примерно 100 КБ на каждую новую запись, которая высвобождается после перезапуска службы **dirsrv**. Эта особенность работы не проявляется в сценарии репликации, но ее следует учитывать при планировании начальной миграции.

---

Несмотря на возможность работы с ограниченным объёмом оперативной памяти (см. пример расчёта выше) на контроллере домена, это может вызвать высокую интенсивность чтения данных с диска, что приведёт к общему замедлению системы и сервиса **LDAP**

(**ns-slapd**) в частности. Для обеспечения надёжной работы контроллера домена и сопутствующих сервисов, а также для исключения увеличения времени репликации из-за дополнительных операций чтения данных с диска, рекомендуется на контроллерах домена не уменьшать объём оперативной памяти ниже 8 ГБ.

---

**Примечание:** Рекомендуемый минимальный размер оперативной памяти одного контроллера домена — 8 ГБ.

---

#### 1.4.1.2. Количество потоков центрального процессора

Если требуемый объем оперативной памяти зависит от размера базы данных, то количество ресурсов центрального процессора определяется тем, сколько пользователей должен обслуживать конкретный контроллер. Например, в базе может быть 100 тысяч пользователей, но нагрузка по их обслуживанию может распределяться между 20 репликами, тогда на каждый контроллер будет приходиться не более 5 тысяч обслуживаемых пользователей.

Приложения имеют разный сценарий взаимодействия с каталогом, что влияет на его нагрузку. Таким образом, у каждой организации получается свой уникальный профиль использования ресурсов этой службы. Поэтому администраторам следует рассчитать данный показатель для своей организации самостоятельно, достигая использования ЦПУ на уровне 40% от максимума в пиковые периоды, а отправной точкой может быть выделение одного потока для работы операционной системы и еще по одному потоку на каждую тысячу пользователей.

$$CPUs = (1 + N\ users/1\,000)$$

Ниже приведено несколько примеров:

- Для обслуживания 2-3 тысяч пользователей контроллеру домена нужно выделить не менее 4 потоков.

$$CPUs = (1 + 3\,000/1\,000) = 4$$

---

**Примечание:** Компания **RedHat** в своей документации рекомендует использовать контроллеры домена именно такой производительности, но эта рекомендация не подойдет

крупным организациям, в штате которых работает несколько сотен тысяч сотрудников, т.к. контроллер, обслуживающий 10 тысяч сотрудников, будет в три раза эффективнее использовать оперативную память в пересчете на активного пользователя, чем контроллер, обслуживающий 3 тысячи сотрудников.

---

- Для обслуживания 10 тысяч пользователей контроллеру домена нужно выделить 11 потоков.

$$CPUs = (1 + 1\ 0000/1\ 000) = 11$$

Следует отметить, что данные оценки сильно зависят от сценария использования службы каталога, поэтому на такое количество пользователей рекомендуется выделять порядка 8-12 потоков.

- Если под контроллер домена выделить физический сервер с двумя процессорами Xeon Silver (48 потоков), то теоретически он сможет обслуживать 47 тысяч пользователей.

$$CPUs = (1 + 47\ 000/1\ 000) = 48$$

При планировании таких контроллеров следует принимать во внимание ограничения по пропускной способности сети. Для обслуживания такого числа пользователей потребуется использование сетевого интерфейса со скоростью передачи данных не менее 1 Гбит/с.

При выборе процессора следует учитывать, что LDAP-запросы в большей степени зависят от скорости дисковой подсистемы, а Kerberos-аутентификация использует сложные криптографические алгоритмы, поэтому в большей степени зависит от вычислительной производительности контроллера. Увеличивать вычислительные мощности контроллера можно как за счет добавления дополнительных ядер, так и за счет увеличения их частоты, при этом следует учитывать, что, если нагрузка на ядра не превышает 40%, то дополнительный прирост производительности можно получить только за счет увеличения частоты ядер.

- Не рекомендуется использовать процессоры с базовой тактовой частотой ниже 1,8 ГГц. Это может негативно сказаться на общей скорости работы контроллера домена, как части информационной системы.

---

**Примечание:** При изменении количества потоков процессора (замена процессора или изменение настроек виртуальной машины) необходимо обновить переменную

DAEMON_ARGS в файле */etc/default/krb5-kdc* и перезапустить службу **krb5-kdc**.

#### 1.4.1.3. Пропускная способность сети

При планировании домена следует учитывать два основных вида трафика:

- трафик клиентских запросов (**Kerberos** и **LDAP** запросы к каталогу);
- трафик репликации (по стандартному **LDAPS** протоколу).

#### 1.4.1.4. Клиентский трафик

В процессе обслуживания клиентов контроллеры домена, как правило, получают небольшие входящие запросы на предоставление относительно больших объемов данных, поэтому на контроллерах обычно преобладает исходящий трафик.

Любые оценки являются субъективными, однако, в качестве общих рекомендаций следует исходить из того, что при количестве пользователей до 5 000 будет достаточно интерфейса с пропускной способностью в 100 Мбит/с, а если предполагается обслуживать больше пользователей, нужно установить на контроллере интерфейс с пропускной способностью в 1 Гбит/с. В результате оптимизации нужно добиться, чтобы показатель использования сети не выходил за пределы 40% от максимума в пиковые периоды.

Учитывая то, что внешние каналы связи редко достигают гигабитных скоростей и активно используются пользователями для выхода в интернет, в каждом офисе рекомендуется создавать отдельный сайт и размещать в нем один-два контроллера для локальной обработки клиентских запросов. Такой подход к организации домена позволит разгрузить VPN туннели между офисами и использовать эти каналы связи только для репликации.

#### 1.4.1.5. Трафик репликации

В ходе репликации контроллеры обмениваются только новыми и измененными данными, поэтому объем трафика оказывается небольшим, и его довольно просто прогнозировать, например:

- при добавлении 1000 пользователей трафик репликации окажется в два раза больше, чем при добавлении 500 пользователей;

- если устанавливается новый контроллер в удаленном офисе с подключением в 5 Мбит/с, то ожидается, что на репликацию базы данных размером 1,5 ГБ потребуется не менее часа.

**Внимание:** Крайне важно исключить долгую работу контроллера в автономном режиме, т.к. после этого может потребоваться повторная инициализация контроллера с загрузкой всего каталога.

#### 1.4.1.6. Сервис Глобального каталога

Глобальный каталог представляет из себя ещё одну базу данных (экземпляр **dirsrv**), который содержит частичную копию (часть атрибутов) некоторых объектов службы каталога. Он необходим для корректной работы доверительных отношений и устанавливается на контроллере домена, выделенном под него. На контроллер домена, где будет установлен глобальный каталог, необходимо выделить дополнительно 15-20% дискового пространства и такой же объем ОЗУ. Дополнительным потреблением процессорного времени можно пренебречь, т.к. чтение объектов из памяти достаточно малозатратная операция для ЦПУ.

#### 1.4.1.7. Модуль синхронизации

Основные ресурсы, потребляемые при работе модуля синхронизации — это дисковое пространство, размер которого будет прямо пропорционален количеству синхронизируемых объектов. Дисковое пространство потребляется БД **PostgreSQL**, где хранятся метаданные всех синхронизированных объектов. Для корректной работы модуля синхронизации необходимо выделить дополнительно 15-20% дискового пространства от расчётного.

С настройками по умолчанию **PostgreSQL** хранит кеш объектов в оперативной памяти. Учитывая, что около 80% обрабатываемых запросов являются запросами на чтение, будет достаточно выделить дополнительно 10-15% от расчетного объёма ОЗУ.

#### 1.4.1.8. Расчет отдельных технических пакетов

> **Внимание:** В разделе описаны рекомендации только для части используемых технологий. Остальные рекомендации находятся в разработке. Если возникли сложности с работой **RabbitMQ**, рекомендации по расчету ресурсов для этих технических пакетов представлены ниже.

#### 1.4.1.9. Планирование ресурсов RabbitMQ

Начиная с версии ALD Pro 2.3.0, для **RabbitMQ** отключена кластеризация между контроллерами домена, поэтому брокер сообщений обеспечивает только транзакционность Портала управления ALD Pro и его накладными расходами можно пренебречь, отнеся их к базовым потребностям операционной системы.

#### 1.4.1.10. Планирование ресурсов Salt

Начиная с версии ALD Pro 2.4.0, для управления хостами используется только автономная служба **Salt Minion**, которой не требуется **Salt Master** на сервере, поэтому на контроллерах домена дополнительные ресурсы для работы системы конфигурирования выделять не требуется.

### 1.4.2. Горизонтальное масштабирование

Горизонтальным масштабированием называют повышение производительности системы за счет увеличения количества вычислительных узлов, обслуживающих клиентов, без изменения их производительности. Например, если предполагается использовать контроллеры с 8-12 потоками ЦПУ, которые могут обслуживать по 10 тысяч пользователей, то в организации со штатом в 30 тысяч сотрудников потребуется не менее 3 контроллеров такой производительности:

$$N\ controllers = 30\ 000\ users / 10\ 000\ per\ controller = 3\ controllers.$$

Синхронизация данных между контроллерами обеспечивается процессом репликации, во **FreeIPA** она происходит в мультимастер-режиме, т.е. изменения можно вносить на любом контроллере. Балансировка нагрузки и отказоустойчивость обеспечивается через DNS —

клиентам выдается до трех DNS-серверов, каждый из которых может принадлежать определенному сайту и выдавать SRV-записи в соответствии принадлежностью служб к соответствующим сайтам.

#### 1.4.2.1. Топология соглашений о репликации

В качестве примера обычно приводят топологию из четырех сайтов, см. *Топология из четырех сайтов*, в каждом из которых по четыре контроллера, в результате чего полученная схема вводит администраторов в заблуждение, что в сайте может быть не более четырех контроллеров.

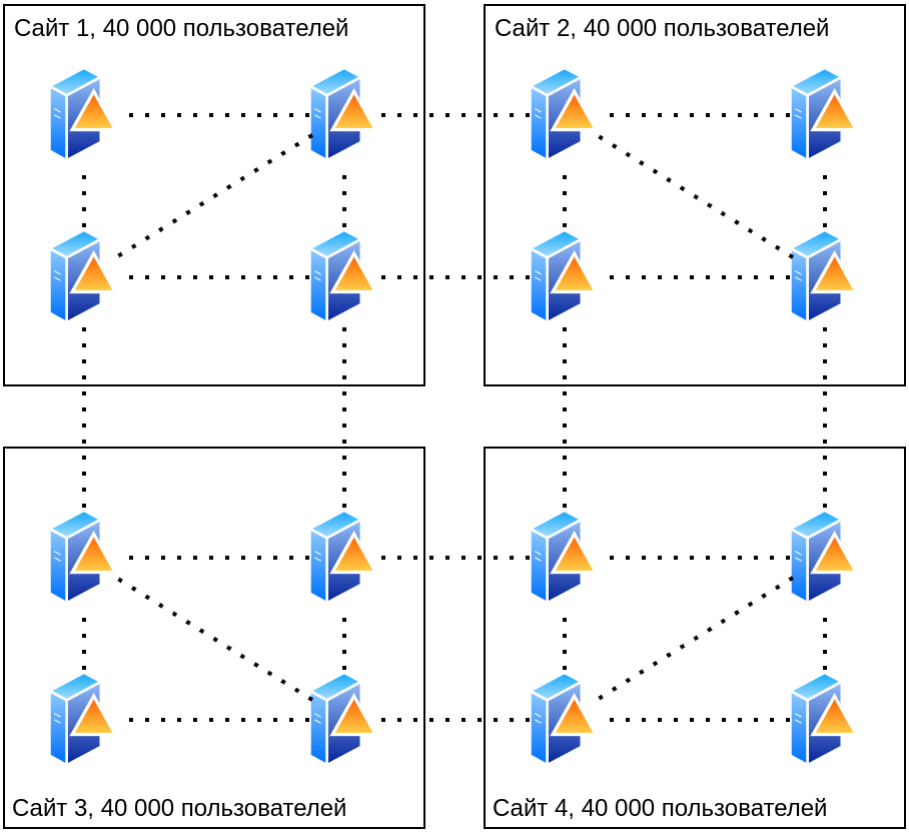


Рисунок 1.1 – Топология из четырех сайтов

В реальной жизни редко бывает, чтобы численность сотрудников в каждой локации была одинаковой, поэтому количество контроллеров может быть, как больше, так и меньше. Ниже приведен пример с тремя сайтами численностью 20, 30 и 80 тысяч человек, см. *Топология из трех сайтов*.

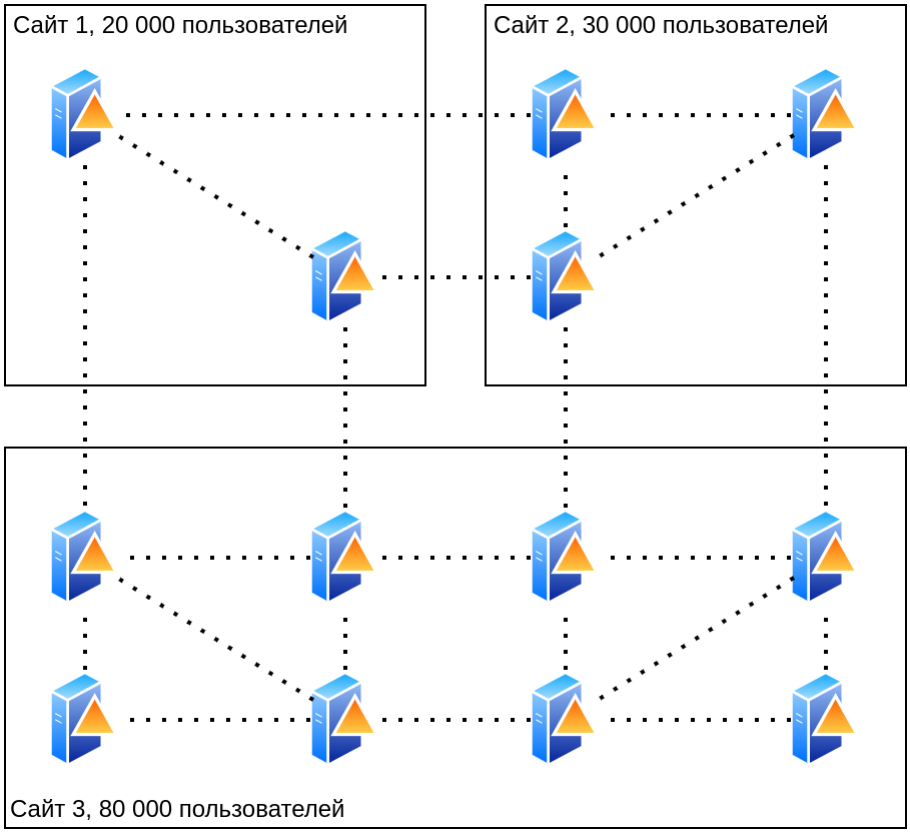


Рисунок 1.2 – Топология из трех сайтов

#### 1.4.2.2. Рекомендации по построению топологии

При планировании топологии следует учитывать несколько рекомендаций:

- Для обеспечения надежности на уровне **0,99** следует установить в каждом сайте не менее двух контроллеров домена.

Если предположить, что сервер работает с надежностью в 90%, тогда при добавлении еще одного такого сервера получается, что в 90% случаев от оставшихся 10% система будет оставаться все так же работоспособной. Итоговая надежность повысится до **0.9 + 0.1 * 0.9 = 0.99**

Максимальное количество контроллеров на сайт не лимитируется, но в настройках рабочих станций можно задать только три DNS-сервера, поэтому стандартными средствами можно обеспечить надежность до **0,999**, а дополнительные контроллеры будут использоваться только для распределения нагрузки.

- Для обеспечения надежности репликации контроллеров домена на уровне 0,99 у каждого из них должно быть не менее 2 соглашений о репликации с другими

контроллерами домена. Для обеспечения надежности межсайтовой репликации на том же уровне у каждого сайта должно быть не менее 2 соглашений о репликации с контроллерами из других сайтов.

- Не рекомендуется создавать более четырех соглашений о репликации на одном контроллере домена, т.к. при недоступности каких-то из серверов алгоритм репликации будет останавливаться на каждом из них, ожидая ответа, что будет приводить к значительному снижению скорости репликации. По этой же причине рекомендуется удалять из домена контроллеры, которые более не используются, а число временно выключенных серверов сводить к минимуму.
- При планировании топологии нужно стремиться к тому, чтобы между любыми двумя контроллерами в домене было не более 5-10 промежуточных узлов, но при этом количество контроллеров, у которых сразу более 4 соглашений о репликации, нужно стараться сводить к минимуму. Такая оптимизация необходима для уменьшения количества прыжков (hops), за которые изменения могут быть распространены в домене.

При этом вне зависимости от топологии домена работу ИТ-службы нужно организовать таким образом, чтобы изменения в домен вносились как можно ближе к потребителю. Например, если потребуется сбросить пароль сотруднику из Новосибирска, то эти изменения должен внести местный администратор с контроллера из своего сегмента сети. В этом случае такие изменения будут максимально быстро реплицированы на все контроллеры, которые обслуживают сотрудника непосредственно, а когда изменения станут доступны на серверах московского региона — это уже не принципиально.

- Для максимальной производительности репликации под эту функцию можно выделить отдельные контроллеры и снять с них обслуживание обычных пользователей путем переключения в режим скрытой реплики (hidden replica).

### 1.4.3. Результаты нагрузочного тестирования

В части горизонтального масштабирования:

- В один домен можно ввести >400 контроллеров, и это не нарушит работу механизма репликации. Не наблюдается технических ограничений для создания доменов на 2-3 тысячи контроллеров, а с выходом функции доверительных отношений между доменами ALD Pro в версии 2.3.0 большую ИТ-инфраструктуру можно разбить на несколько доменов и вопрос горизонтального масштабирования снимается полностью.

- Согласно лабораторным испытаниям, на одном контроллере домена может быть создано более 150 соглашений о репликации сразу, но при планировании топологии домена на практике рекомендуется создавать не более четырех. Важно учитывать, что при недоступности партнера по репликации контроллер домена будет пытаться установить с ним связь несколько раз, что может приводить к значительным задержкам, если таких серверов окажется много. Поэтому для обеспечения надежной репликации на контроллере домена рекомендуется создавать не менее двух соглашений, а для исключения задержек в работе этого механизма избегать более четырех.

В части вертикального масштабирования:

- Контроллер может держать нагрузку >10 тысяч рабочих станций. При увеличении количества ядер производительность возрастает линейно с коэффициентом 0.9 в широком диапазоне (проверяли до 48 ядер), т.е. увеличение числа ядер в 2 раза повышает производительность на 80%.

Использование технологии гиперпоточности добавляет 50-75%, но ее эффективность снижается, если нагрузка на ядра становится выше 80%.

В дополнение к сказанному текущая архитектура групповых политик ALD Pro переносит всю нагрузку по суммированию параметров на рабочие станции, поэтому обслуживание тысяч хостов не создает ощутимой нагрузки на сервер.

- В домене можно создать >30 млн. объектов, и это не нарушит работу контроллеров. Увеличение количества объектов приведет к увеличению размера базы данных и объема потребляемой оперативной памяти. В больших инфраструктурах настоятельно рекомендуется отключать плагин **Schema Compatibility**, т.к. построение виртуального дерева объектов каталога создает существенную задержку в запуске служб (на базе в 30 млн. объектов задержка составляла чуть более 30 минут).

Пример производительности в пересчете на один контроллер домена, полученный на каталоге размером 30 млн. объектов (более 100 ГБ на диске). Характеристики каждого контроллера 16 ЦПУ, 128 ГБ ОЗУ. (рис.1.3-1.5)

- LDAP Search - 5 040 чтений в секунду
- LDAP Bind - 126 аутентификаций в секунду
- LDAP Modify - 126 изменений в секунду
- Kerberos TGT - 180 аутентификаций в секунду

Рисунок 1.3 – Результаты нагрузочного тестирования

Рисунок 1.4 – Результаты нагрузочного тестирования

Рисунок 1.5 – Результаты нагрузочного тестирования

### 1.4.4. Практический кейс по планированию ресурсов

Исходные требования:

- Объектов в каталоге: 1 млн. (650 тыс. пользователей, 350 тыс. групп).
- Обслуживаемых пользователей: 2 тыс.

Расчеты:

Для размещения файлов операционной системы и каталога на жестком диске потребуется не менее 60 ГБ HDD:

$$HDD = 50 + 1\ 000\ 000/20\ 000 \approx 100\ GB$$

Для того, чтобы контроллер домена (КД) смог разместить каталог с 1 млн. объектов в оперативной памяти, ему потребуется не менее 100 ГБ ОЗУ:

$$RAM = 3 + 1\ 000\ 000/20\ 000 \approx 66\ GB$$

Если к контроллеру будут обращаться 2 тысячи пользователей, то ему потребуется не

менее 3 потоков:

$$CPUs = 1 + 2\,000/1\,000 = 3$$

Конкретно к этому серверу будет обращаться 2 тыс. пользователей, поэтому достаточно одной виртуальной машины. Но если нужно будет обеспечить единовременную работу всех 600 тысяч пользователей, то потребуется не менее 300 таких контроллеров и более целесообразным будет увеличить производительности контроллеров до 10 тысяч пользователей (8-12 потоков ЦПУ), тогда количество контроллеров можно будет сократить до 60 единиц.

Следует учесть, что объекты в каталоге создаются в среднем со скоростью один объект в секунду и это значение растет по мере увеличения количества объектов в каталоге, поэтому на создание 1 млн. объектов уйдет не менее 11 дней. Ускорить процесс можно увеличением числа потоков, но зависимость будет нелинейной, т.к. потоки будут конкурировать за общие ресурсы.

Дополнительного ускорения процедуры можно достичь путем создания пользователей на нескольких контроллерах одновременно, т.к. при репликации вычислительных ресурсов требуется меньше, чем при создании объектов.

Для тестирования остальных подсистем в соответствии с типовой схемой, см. *Типовая схема инфраструктуры*, нужно дополнительно 8 виртуальных машин: 2 ЦПУ, 4 ГБ ОЗУ, 100 ГБ HDD (DHCP, установка ОС по сети, сервер печати, сервер общего доступа к файлам, сервер аудита, сервер мониторинга, сервер репозиториев, клиентская машина).

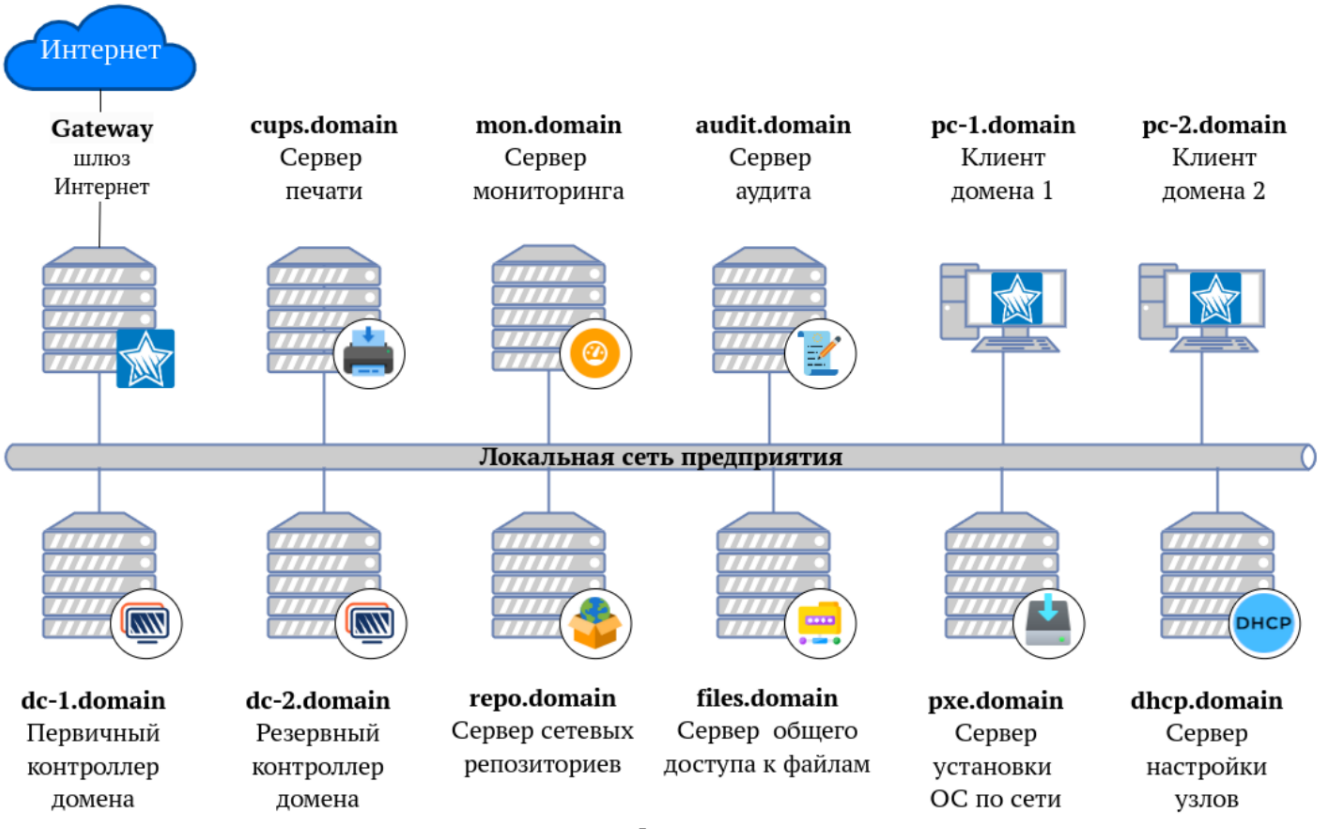


Рисунок 1.6 – Типовая схема инфраструктуры

Для упрощения предварительного расчёта ресурсов можно воспользоваться двумя таблицами:

| На один КД | RAM | HDD |
|---|---|---|
| Базовые требования | 3 | 50 |
| Кол-во объектов | | |
| 3 000 | 8,0 | 50,2 |
| 5 000 | 8,0 | 50,3 |
| 10 000 | 8,0 | 50,5 |
| 50 000 | 8,0 | 52,5 |
| 100 000 | 8,0 | 55,0 |

продолжение на следующей странице

Таблица 1.2 – продолжение с предыдущей страницы

| На один КД | RAM | HDD |
|---|---|---|
| 150 000 | 10,5 | 57,5 |
| 200 000 | 13,0 | 60,0 |
| 250 000 | 15,5 | 62,5 |
| 300 000 | 18,0 | 65,0 |
| 400 000 | 23,0 | 70,0 |
| 500 000 | 28,0 | 75,0 |
| 700 000 | 38,0 | 85,0 |
| 800 000 | 43,0 | 90,0 |
| 1 000 000 | 53,0 | 100,0 |
| 1 500 000 | 78,0 | 125,0 |
| 2 000 000 | 103,0 | 150,0 |

Таблица 2 — Расчёт дискового пространства и количество оперативной памяти на один контроллер домена

| На домен, сайт | CPU | Кол-во КД |
|---|---|---|
| Базовые требования | 1 | |
| коэффициент | 1000 | 32 |
| Активные объекты | | |
| 3 000 | 8,0 | 1,0 |
| 5 000 | 8,0 | 1,0 |
| 10 000 | 11,0 | 1,0 |
| 50 000 | 51,0 | 2,0 |

продолжение на следующей странице

Таблица 1.3 – продолжение с предыдущей страницы

| На домен, сайт | CPU | Кол-во КД |
|---|---|---|
| 100 000 | 101,0 | 4,0 |
| 150 000 | 151,0 | 5,0 |
| 200 000 | 201,0 | 7,0 |
| 250 000 | 251,0 | 8,0 |
| 300 000 | 301,0 | 10,0 |
| 400 000 | 401,0 | 13,0 |
| 500 000 | 501,0 | 16,0 |
| 700 000 | 701,0 | 22,0 |
| 800 000 | 801,0 | 26,0 |
| 1 000 000 | 1001,0 | 32,0 |
| 1 500 000 | 1501,0 | 47,0 |
| 2 000 000 | 2001,0 | 63,0 |

Таблица 3 — Расчёт необходимого количества процессорных ядер и количества контроллеров домена для обработки запросов от активных пользователей

## 1.5. Рекомендации по именованию домена

В документации и обучающих курсах применяются домены **contoso.com** или **ad.example.test**, которые используют для обучающих целей, но не приемлемы для развёртывания продуктивных сред. Поэтому рекомендуется придерживаться следующих правил:

- Лучший вариант - это использовать свой домен третьего уровня. Например, если организация приобрела домен **mycompany.ru** для своего Web-сайта и почты, то для **ALD Pro** можно использовать доменное имя третьего уровня **ald.mycompany.ru**. Если в группе компаний планируется несколько юридических лиц, то каждому юр. лицу можно создать домен четвертого уровня. Таким образом будет гарантироваться отсутствие конфликтов с публичными DNS-именами.
- Если публичный домен не используется, то можно задействовать зоны **.lan** или **.internal**, например, **ald.company.lan**. Во многих инструкциях упоминается возможность использования зоны **.local** в качестве частного домена верхнего уровня для внутренних нужд предприятия, но в этом случае возникают конфликты Multicast DNS (RFC6762) и невозможность использования протокола **zeroconf**, который реализован в Linux службой **Avahi**, поэтому данная зона не рекомендуется.

---

**Важно:** Предложенные зоны **.lan** и **.internal** не зарегистрированы в глобальном списке Top-Level Domains, но всегда будет оставаться вероятность, что их ведут в эксплуатацию в будущем. Соответственно, следует использовать зоны **.lan**, **.internal** и **.local** учитывая эти риски.

---

Выбор префикса для домена:

- Следует выбирать префикс, который вряд ли устареет, т.е. избегать имен, таких как линейка продуктов или операционная система, которые могут измениться в будущем. Рекомендуется использовать универсальные имена, такие как **corp**, **ent** или **ald**.
- Следует выбирать префикс, содержащий только стандартные символы Интернета **a–z**, **0–9** и (**-**), но не полностью числовые.
- Следует выбирать префикс длиной не более 15 символов, потому что первый компонент доменного имени будет использован в качестве NetBIOS-имени.
- При выборе префикса следует учитывать, что два домена не смогут работать в доверительных отношениях, если у них будут совпадать NetBIOS-имена и имена контроллеров домена, например, если текущий домен AD DS имеет имя

**corp.mycompany.com**, то не стоит для домена **ALD Pro** использовать имя **corp.mycompany.ru**. Иначе не получится создать между этими доменами доверительные отношения.

---

**Важно:** В стандарте доменных имен (RFC1034) разрешается использовать заглавные буквы латинского алфавита **A-Z**, но служба каталога **FreeIPA** налагает дополнительные требования и обязует использовать только нижний регистр символов.

Если в команде ввода в домен указать имя хоста заглавными буквами, то процедура завершиться ошибкой. Если поменять имя хоста на заглавные (например, **FS-01.ald.company.lan**) после ввода в домен, то появится ошибка при установке подсистем на такие хосты.

Перед созданием имени ознакомьтесь с 2.1.1.3. *Настройка имени хоста*

---

На предприятии принято называть сервера и персональные компьютеры по заданной конвенции наименований, например, конвенция для серверов **<location>-<type>-<number>.<domain>** разрешает такой вариант наименования **msk-dc-1.ald.company.lan**. Во-первых, это нужно для стандартизации и общего понимания архитектуры системы, а во-вторых позволит качественно управлять узлами с помощью автоматизации. Например, имя узла **dc-1** с легкостью разделяется на части по разделителю «**-**» с помощью команды **cut**:

```
echo "dc-1.ald.company.lan" | cut -d"." -f 1 | cut -d"-" -f 1
```

Результат выполнения покажет, что выбранный узел является контроллером, а не мониторингом:

```
dc
```

# Развертывание контроллеров домена и подсистем

Для установки серверной части **ALD Pro** (контроллер домена, подсистема) важно использовать операционную систему без предварительных настроек.

При переустановке ALD Pro на сервер/компьютер (контроллер домена, подсистема, клиентская рабочая станция) с тем же именем `hostname` необходимо предварительно убедиться, что этот хост полностью выведен из домена, а записи о нем отсутствуют в LDAP-каталоге. Подробнее в разделах *Вывод компьютера из домена* и backup-controller-delete.

## 2.1. Развертывание первого контроллера домена

### 2.1.1. Подготовка окружения сервера к установке контроллера домена

#### 2.1.1.1. Требования к ОС

Продукт **ALD Pro** можно установить на хостах под управлением операционной системы **Astra Linux Special Edition** (**ALSE**). Для установки контроллеров домена и других подсистем требуется максимальный уровень защищенности «Смоленск». Клиентская часть может быть установлена в системе с любым уровнем защищённости.

При установке продукта необходимо учитывать список поддерживаемых версий системы - см. **Руководство администратора. Часть 1** → **Матрицы совместимости и обновлений** → **Матрица совместимости**. Версия ОС в командах и примерах ниже указана в формате `1.7.xxx` - актуального оперативного обновления.

Для проверки версии и уровня защищенности операционной системы **ALSE** используются следующие команды:

```
cat /etc/astra/build_version
sudo astra-modeswitch getname
```

Результат выполнения команд:

```
<номер версии ОС>
maximum(smolensk)
```

Для увеличения уровня защищённости операционной системы **Astra Linux** до максимального уровня («Смоленск») необходимо ввести следующую команду:

```
sudo astra-modeswitch set 2
```

---

**Примечание:** Стоит учитывать, что при увеличении уровня защищенности состояние опций (МРД и МКЦ) автоматически не изменяется, но опции, доступные в новом режиме, становятся доступными для включения.

---

#### 2.1.1.2. Настройка сетевого интерфейса

Если операционная система установлена с графическим интерфейсом **fly-wm**, то в качестве менеджера сетевых подключений устанавливается служба **NetworkManager**. На серверах ее нужно отключить:

```
sudo systemctl stop NetworkManager
sudo systemctl disable NetworkManager
sudo systemctl mask NetworkManager
sudo systemctl status NetworkManager
```

После выполнения последней команды в терминале должна отобразиться информация о маскировке службы **NetworkManager**:

```
o NetworkManager.service
  Loaded: masked (Reason: Unit NetworkManager.service is masked.)
  Active: inactive (dead) since Tue 2024-10-29 18:16:15 MSK; 3min 35s ago
Main PID: 493 (code=exited, status=0/SUCCESS)
...
```

После отключения службы **NetworkManager** сетевые настройки задаются в файлах `/etc/network/interfaces` и `/etc/resolv.conf`. Файл `resolv.conf` используется **DNS**-клиентом, а файл `interfaces` – утилитами `ifup` и `ifdown` для конфигурирования

сетевых интерфейсов.

Так как служба каталога интегрирована со службой разрешения имен, то контроллер домена выступает еще и в роли **DNS**-сервера. Адреса **DNS**-серверов устанавливаются на доменных компьютерах вручную или через **DHCP**. Поэтому на контроллерах домена рекомендуется использовать только статические IP-адреса. Отредактировать файл конфигурации можно с помощью редактора `nano`:

```
sudo nano /etc/network/interfaces
```

Пример настройки сетевого интерфейса на контроллере домена для использования статического IP-адреса:

```
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
```

где:

- `auto eth0` — указывает, что интерфейс `eth0` включается автоматически при выполнении команды `ifup -a`. Список доступных интерфейсов можно посмотреть командой `ip a`, интерфейс сетевой карты обычно имеет идентификатор `eth0`.
- `iface eth0 inet static` — строка, начинающаяся с директивы `iface`, объединяет группу строк, отвечающих за настройку указанного сетевого интерфейса:
  - `eth0` - определяет имя интерфейса;
  - `inet` - указывает, что следует использовать `IPv4`. Также может принимать значение `inet6` для `IPv6` соответственно;
  - `static` - указывает, что настройки интерфейса задаются вручную. Также может принимать значение `dhcp` для динамической настройки с помощью **DHCP**-сервера.
- `address`, `netmask`, `gateway` — задают IP-адрес, маску и шлюз по умолчанию для интерфейса, указанного в строке `iface`.

Для применения новых настроек, необходимо перезапустить службу `Networking` и

очистить старое соединение командой `flush` утилиты `ip`:

> **Внимание:** Если доступ к компьютеру осуществляется исключительно удалённо, например, посредством протоколов SSH или RDP, то чтобы избежать возможной утраты соединения, вместо команды **flush** рекомендуется выполнить простую перезагрузку системы при помощи команды **sudo reboot**.

```
sudo ip addr flush dev eth0
sudo systemctl restart networking
```

Для возможности обращения к публичным репозиториям следует настроить функцию разрешения имен. В файле `/etc/resolv.conf` рекомендуется указать бесплатный сервер разрешения имен от Яндекс:

```
sudo nano /etc/resolv.conf
```

Изменить содержимое файла:

```
nameserver 77.88.8.8
```

После установки настроек необходимо проверить подключение к репозиториям **ALSE**:

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

---

**Примечание:** Если продукт нужно установить в закрытом контуре без доступа в Интернет, необходимо воспользоваться установочным диском или локальным репозиторием (см. *Подключение репозиториев*).

---

#### 2.1.1.3. Настройка имени хоста

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.

#### 2.1.1.4. Подключение репозиториев

**Установка через интернет-репозитории**

Для установки продукта из официальных интернет-репозиториев **РусБИТех-Астра** на операционной системе **ALSE** 1.7.xxx содержимое файла `/etc/apt/sources.list` должно быть следующим:

```
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
```

---

**Примечание:** Разработчики операционной системы **Astra Linux** рекомендуют использовать репозитории из ветки `stable`, которые соответствуют последней версии системы, но для корректной работы продукта **ALD Pro** требуется использовать репозитории `frozen`, чтобы гарантировать полную совместимость пакетов. Информация о поддержке очередных обновлений и возможности обновления операционной системы публикуется в **release notes**.

---

#### Установка с помощью iso-образов

Для установки продукта с использованием **iso**-файлов эти образы нужно сначала примонтировать к системе, например, с помощью следующих команд (на примере ОС 1.7.6):

```
sudo mkdir /mnt/alse_1.7.6
sudo mount -o loop /distr/base-1.7.6.iso /mnt/alse_1.7.6

sudo mkdir /mnt/ald_pro_3.0.0
sudo mount -o loop /distr/ALDPro-3.0.0-1.7_x86-64.iso /mnt/ald_pro_3.0.0/
```

Где:

- `mount` – утилита обеспечивает монтирование файловой системы;
- `-o loop` – ключ позволяет связать свободное петлевое устройство (`/dev/loopN`) с указанным **iso**-образом;
- `/distr/base-1.7.6.iso` – параметр определяет абсолютный путь к **iso**-образу;
- `/mnt/alse_1.7.6` – параметр определяет точку монтирования.

При установке продукта с использованием смонтированного **iso**-образа содержимое файла `/etc/apt/sources.list` должно быть следующим:

```
deb file:///mnt/alse_1.7.6 1.7_x86-64 main non-free contrib
```

Содержимое файла `/etc/apt/sources.list.d/aldpro.list` должно быть следующим:

```
deb file:///mnt/ald_pro_3.0.0/ 1.7_x86-64 main base
```

#### 2.1.1.5. Обновление программных пакетов

Необходимо проверить наличие доступных для обновления пакетов и выполнить обновление пакетов в случае их наличия:

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

### 2.1.2. Установка пакетов

Для установки пакетов продукта необходимо выполнить следующую команду:

```
sudo DEBIAN_FRONTEND=noninteractive apt-get install -y -q aldpro-mp aldpro-
↪gc aldpro-syncer aldpro-syncer-pwdsync
```

где:

- `DEBIAN_FRONTEND` — переменная окружения, которая позволяет изменить режим взаимодействия с пользователем при установке пакетов менеджером APT. Переключение менеджера пакетов в режим `noninteractive` позволяет избежать уточнений о настройках для последующей работы от **Kerberos**, **OpenDNSSec** и **PAM**;
- `-y` — ключ позволяет автоматически ответить **Да** на все возможные вопросы в ходе установки;
- `-q` — ключ позволяет скрыть сообщения о прогрессе установки, делая журнал более читаемым;
- `aldpro-mp` — основной инсталляционный пакет **ALD Pro**, который позволяет через зависимости установить все остальные пакеты продукта, за исключением пакетов глобального каталога и модуля синхронизации;
- `aldpro-gc` — инсталляционный пакет глобального каталога. Модуль обеспечивает возможность поиска объектов из доверенного домена **ALD Pro** при назначении прав доступа в стандартных приложениях **Microsoft Windows**. Не используется, если установка доверительных отношений не требуется;
- `aldpro-syncer` — инсталляционный пакет модуля синхронизации. Модуль позволяет синхронизировать организационные подразделения, группы и пользователей, включая их пароли, чтобы обеспечить доступ пользователей по логину/паролю к любым информационным системам вне зависимости от того, к

какому домену подключены эти системы. Не используется, если не требуется гибридное развертывание;

- `aldpro-syncer-pwdsync` - вспомогательный пакет модуля синхронизации `aldpro-syncer`, отвечающий за взаимную синхронизацию паролей пользователей из контроллера MS AD в ALD Pro. Пакет можно не устанавливать, если функционал синхронизации паролей между MS AD и ALD Pro не будет использоваться.

При возникновении ошибок, информация о них записывается в журнал пакетного менеджера в файле `/var/log/apt/term.log`. Для просмотра используется следующая команда:

```
sudo grep 'error:' /var/log/apt/term.log
```

### 2.1.3. Повышение роли сервера до контроллера домена

**Внимание:** При установке контроллера домена на сервер, на котором включен режим замкнутой программной среды, перед запуском скрипта продвижения домена необходимо выполнить перезагрузку сервера.

**Внимание:** В версии 3.0.0 был введен механизм валидации параметров для утилиты `aldpro-server-install`.

При обновлении первого КД с помощью утилиты `aldpro-server-install` следует пропустить пункты 2, 6, 9, 10 из списка проверок ниже. Обновление резервных КД выполняется через портал управления. Поэтому необходимо выполнить все пункты из списка проверок ниже.

Подробное описание механизма валидации параметров см. в **Руководство администратора. Часть 2 → Инструкция по валидации параметров установки/обновления ALD Pro** .

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 --setup_
↪gc --setup_syncer --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.

Параметры утилиты `aldpro-server-install`:

- `-d` (`--domain`) — имя домена;
- `-n` (`--name`) — имя сервера. В параметре нужно передать короткое имя сервера без указания домена, т.е. первый компонент от полного **FQDN**-имени, которое выдает команда `hostname -f`;
- `-p` (`--admin_pwd`) — получить пароль администратора домена из командной строки (небезопасно). Для возможности использования в пароле специальных символов значение следует заключить в одинарные кавычки, например: **„pa_s$w0rd“**.
- `--ip` — IP-адрес контроллера домена, на котором предполагается обслуживать клиентов домена.
- `--setup_gc` — ключ указывает, что нужно настроить установленный ранее модуль глобального каталога.
- `--setup_syncer` — ключ указывает, что нужно настроить установленный ранее модуль синхронизации.
- `--no-reboot` — ключ отключает автоматическую перезагрузку после завершения процедуры настройки. Мы рекомендуем запускать перезагрузку вручную после ознакомления с журналом установки.

Для вступления изменений в силу необходимо перезагрузить сервер:

```
sudo reboot
```

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

- login: `admin`
- password: `*****` (пароль администратора домена из строки продвижения сервера)

**Внимание:** Важно помнить, что корректный вход в систему возможен только после полной загрузки всех служб. Если после перезагрузки сервера не удалось войти в операционную систему контроллера под доменной учетной записью, стоит повторить попытку через пару минут. Если доступ для доменного пользователя так и не появится, необходимо войти в систему с помощью локальной учетной записи и проверить содержимое журналов `/var/log/auth.log` и `/var/log/messages`.

После загрузки сервера проверить статус доменных служб можно с помощью команды `status` утилиты `aldproctl`:

```
sudo aldproctl status
```

Результат выполнения команды:

```
.....Сервисы ALD Pro.....
Сервис aldpro-mp-services: ЗАПУЩЕН
Сервис globalcatalog: ЗАПУЩЕН
Сервис ipa-gcsyncd: ЗАПУЩЕН
.....Сервисы FreeIPA.....
Сервис Directory Service: ЗАПУЩЕН
Сервис krb5kdc: ЗАПУЩЕН
Сервис kadmin: ЗАПУЩЕН
Сервис named: ЗАПУЩЕН
Сервис httpd: ЗАПУЩЕН
Сервис ipa-custodia: ЗАПУЩЕН
Сервис smb: ЗАПУЩЕН
Сервис winbind: ЗАПУЩЕН
Сервис ipa-otpd: ЗАПУЩЕН
Сервис ipa-dnskeysyncd: ЗАПУЩЕН
.....Другие сервисы.....
Сервис celery: ЗАПУЩЕН
Сервис celerybeat: ЗАПУЩЕН
```

Утилита поддерживает такой же набор команд `start/stop/restart/status`.

### 2.1.4. Дополнительные настройки DNS

Для корректной работы сервера необходимо отключить **DNSSEC**. Для его отключения 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
```

Несмотря на то, что **bind9-pkcs11** может успешно выступать в роли распознавателя, для снижения нагрузки с **DNS**-сервера эту функцию рекомендуется передать стороннему сервису, например, публичным **DNS**-серверам от **Яндекс**, которые доступны по IP-адресу `77.88.8.8`.

Для настройки перенаправления **DNS**-запросов на портале управления **Роли и службы сайта** → **Служба разрешения имен** → **Глобальная конфигурация DNS** нужно добавить запись с политикой **Только перенаправлять** или **Сначала перенаправлять**, см. *Глобальная конфигурация DNS*.

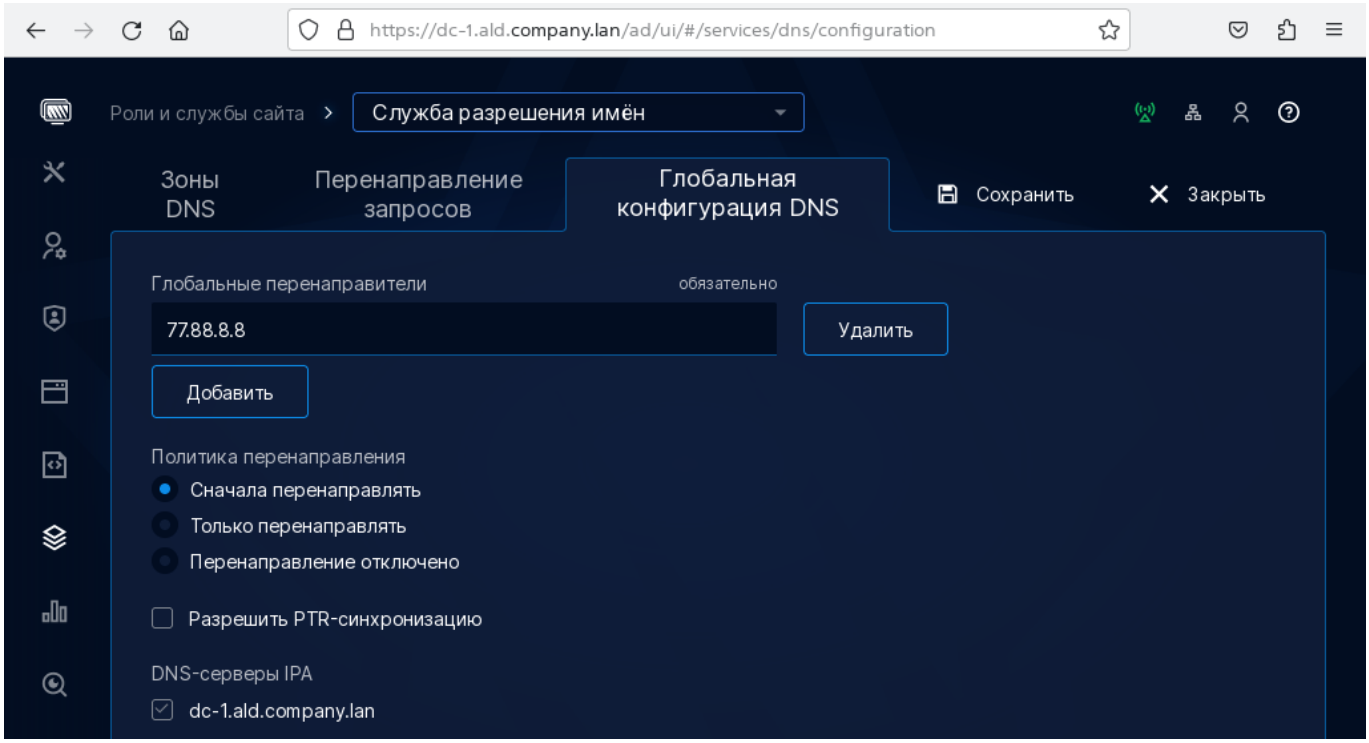


Рисунок 2.1 – Глобальная конфигурация DNS

Создание обратной **DNS**-зоны подробно описано в разделе **Роли и службы сайта → Служба разрешения имен → Зоны DNS → Создание зоны DNS Руководства администратора. Часть 2**. Важно помнить, что по умолчанию обратная зона создается с маской с размерностью `/24`, игнорируя настройки сетевого адаптера. Если подсеть отличается от размерности `/24`, то необходимо вручную создать обратную зону нужной размерности, а созданную по умолчанию - выключить.

## 2.1.5. Глобальный каталог

### 2.1.5.1. Установка глобального каталога

Модуль глобального каталога может быть установлен во время продвижения первого контроллера домена.

Для этого достаточно установить пакет `aldpro-gc` и добавить ключ `--setup_gc` при вызове утилиты `aldpro-server-install`.

Важно помнить, что для установки необходима роль глобального каталога. Если роль глобального каталога не была установлена сразу, то ее можно добавить позднее на любой контроллер домена через портал управления на странице **Роли и службы сайта →**

**Служба глобального каталога**. В противном случае, при очередном обновлении конфигурации сервер автоматически удалит модуль глобального каталога. Контроллер, которому будет назначена новая роль, автоматически обновит свою конфигурацию через полчаса.

Для форсирования установки роли на сервере необходимо использовать команды:

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

Проверить работу глобального каталога после его установки можно командой:

```
sudo aldproctl status --service=globalcatalog
```

## 2.1.6. Модуль синхронизации

### 2.1.6.1. Установка модуля синхронизации

Если планируется использовать расширенные функции интеграции с доменом **Microsoft Active Directory** (**MS AD**), то нужно будет дополнительно установить модуль синхронизации, который обеспечивает целостность информации между доменами **ALD Pro** и **MS AD**.

В этом случае в двух доменах используется один и тот же состав пользователей и групп, а синхронизировать можно будет не только обычные атрибуты, но и пароли. Это позволит обеспечить доступ пользователей к любым информационным системам по логину/паролю вне зависимости от того, через контроллер какого домена информационная система проверяет аутентичность пользователей.

Для установки модуля синхронизации необходимо установить следующие deb-пакеты:

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

Затем требуется выполнить обновление системы командой `aldpro-server-install --update` со всеми необходимыми ключами:

```
sudo aldpro-server-install --update -d ald.company.lan -n dc-1 --ip 10.0.1.
↪11 --setup_syncer --no-reboot
```

После ввода команды система запросит ввести пароль администратора домена.

Если на контроллере домена был установлен также модуль глобального каталога, то при обновлении сервера вам нужно будет добавить ключ `--setup_gc`, иначе подсистема обновления удалит этот модуль с сервера.

### 2.1.7. Проверка работы портала управления

Чтобы открыть портал управления с контроллера домена, необходимо запустить браузер **Mozilla Firefox**: адрес сайта `https://dc-1.ald.company.lan` будет являться домашней странице, а приложение будет автоматически доверять сертификату этого веб-ресурса и разрешать **Kerberos**-аутентификацию.

Если браузер разрешает прозрачную **Kerberos**-аутентификацию, то можно использовать ссылку **Вход с Kerberos**.

**Kerberos**-аутентификация работать не будет при обращении к порталу управления:

- с браузера, отличного от **Mozilla Firefox**;
- с компьютера, который не входит в домен;
- под любым, не входящим в домен, пользователем.

Поэтому потребуется вводить логин и пароль вручную, и также согласиться с риском использования самоподписанного сертификата. Однако, при необходимости можно настроить любую рабочую станцию так же как контроллер домена, следуя рекомендациям из раздела **Отладка подсистем ALD Pro → Безопасный обмен данными с применением SSL/TLS Руководство администратора. Часть 2**.

## 2.2. Ввод компьютера в домен

Для ввода компьютера в домен необходимо обладать привилегиями, см. **Руководство администратора. Часть 2 → Необходимые привилегии для ввода компьютера в домен**.

Существует возможность ввода в домен клиентов под управлением операционных систем, отличных от **Astra Linux**:

- **Альт Рабочая станция 10.4**
- **Альт СП 10**
- **РЕД ОС 7.3.5**
- **РЕД ОС 8**

Для каждого клиента с указанными выше операционными системами доступны функции:

- возможность ввода в домен через терминал и графическую утилиту (`aldpro-client-installer`);
- удаленное подключение к клиенту (`aldpro-client-rdm`);
- политики доступа к узлу (HBAC-правила);
- политики повышения привилегий (SUDO-правила);
- политики обновления ALD Pro;
- получение файлов `aldpro-policy-manager` из службы каталогов (`aldpro-gpupdate --pm`);
- получение параметров групповых политик (`aldpro-gpupdate --gp`);
- доверительные отношения с **MS AD**;
- задания автоматизации;
- параметры групповых политик, в описании которых указана совместимость с альтернативными ОС:

  Параметры компьютеров → Оборудование → Установить принтеры Параметры компьютеров → Дата и время → Настройки сервиса сетевого времени Chrony Параметры компьютеров → Дата и время → Параметры сервера или пула сетевого времени Параметры компьютеров → Загрузчик GRUB2 → Автоматическая загрузка Параметры пользователей → Приложения для типов файлов → Приложение для типов файлов Параметры пользователей → Приложения для типов файлов → Сетевые

приложения

- дополнительные параметры групповых политик.

### 2.2.1. Настройка сети на клиентских компьютерах

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** необходимо установить следующие значения, см. *Настройки сети с помощью графической утилиты NetworkManager*:

- Метод: Вручную
- Адрес: 10.0.1.51
- Маска: 255.255.255.0
- Шлюз: 10.0.1.1 шлюз маршрутизатора или gateway
- Серверы DNS: 10.0.1.11 (адрес dc-1)
- Поисковый домен: ald.company.lan

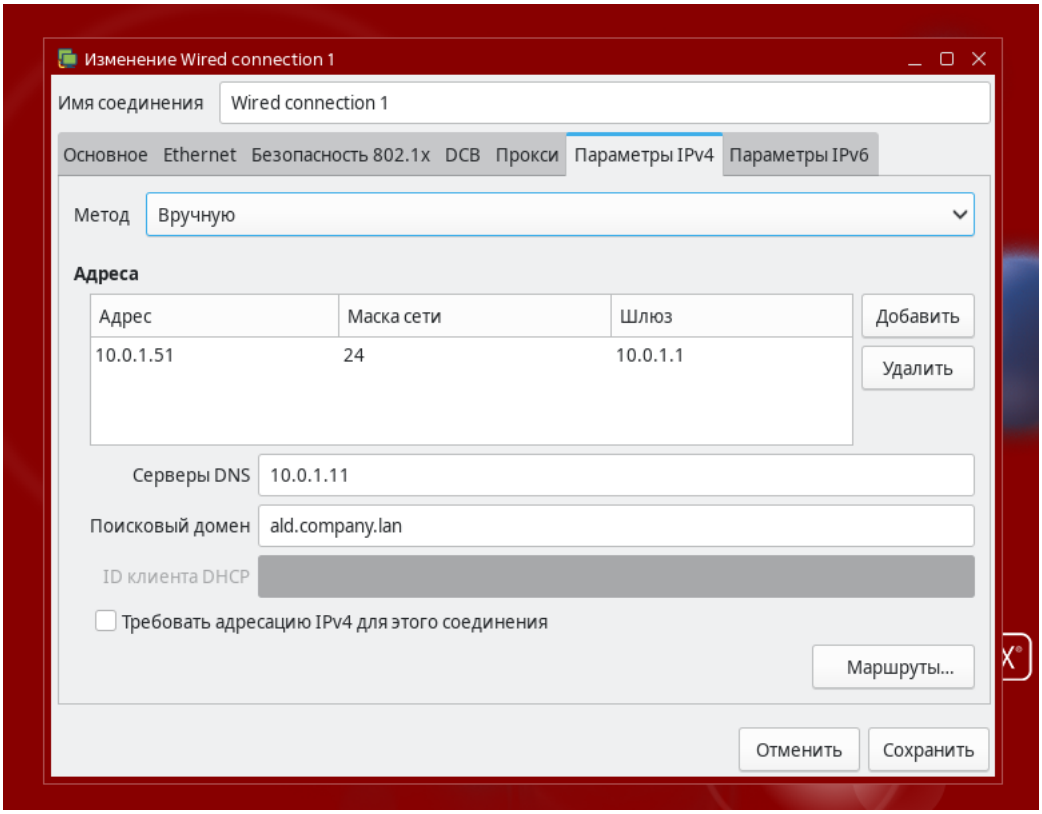


Рисунок 2.2 – Настройки сети с помощью графической утилиты NetworkManager

Для применения новых настроек необходимо выключить и повторно включить поддержку сети через панель задач, кликнув по апплету **NetworkManager**.

Для установки пакетов компьютеру нужно иметь доступ к репозиториям, расположенным по адресу https://dl.astralinux.ru. Для проверки применения IP-адреса и доступности сайта и хостов сети используются команды:

```
ip a
ping -c 4 dl.astralinux.ru
ping -c 4 dc-1.ald.company.lan
ping -c 4 dc-1
```

#### 2.2.1.1. Настройка доступных репозиториев и установка пакетов на клиенте с Astra Linux Special Edition 1.7.xxx

Для установки клиентской части **ALD Pro** версии 3.0.0 на **ALSE** 1.7.xxx из официальных интернет-репозиториев **РусБИТех-Астра** содержание файла `/etc/apt/sources.list` должно быть таким же, как при установке серверной части:

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

где файл `sources.list` содержит:

```
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
```

Для установки клиентской части **ALD Pro** необходимо выполнить команду:

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

Информация об использованных ключах расположена в разделе по установке пакетов на контроллере домена.

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`).

#### 2.2.1.2. Настройка доступных репозиториев и установка пакетов на клиенте с Astra Linux Special Edition 1.8.xxx

Для установки клиентской части **ALD Pro** версии 3.0.0 на **ALSE** 1.8.xxx из официальных интернет-репозиториев **РусБИТех-Астра** содержание файла `/etc/apt/sources.list` должно быть таким же, как при установке серверной части:

```
deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.xxx/repository-main/
 ↪ 1.8_x86-64 main contrib non-free
```

или:

```
deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.xxx/repository-main/
 ↪ 1.8_x86-64 main contrib non-free
deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.xxx/repository-
 ↪extended/ 1.8_x86-64 main contrib non-free
```

Для просмотра содержимого файла использовать команду:

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

Для установки 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 1.8_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
```

Для установки клиентской части **ALD Pro** необходимо выполнить команду:

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

Информация об использованных ключах расположена в разделе по установке пакетов на контроллере домена.

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`).

#### 2.2.1.3. Настройка доступных репозиториев и установка пакетов на клиенте с Astra Linux Special Edition 4.7.6

Для установки клиентской части **ALD Pro** версии 3.0.0 на **ALSE** 4.7.6 из официальных интернет-репозиториев **РусБИТех-Астра** содержание файла `/etc/apt/sources.list` должно быть следующим:

```
deb https://dl.astralinux.ru/astra/frozen/4.7_arm/4.7.6/repository-main/ 4.7_
↪arm main contrib non-free
deb https://dl.astralinux.ru/astra/frozen/4.7_arm/4.7.6/repository-update/ 4.
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
↪7_arm main contrib non-free
```

Для просмотра содержимого файла использовать команду:

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

Для установки 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/ 4.7_arm 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
```

Для установки клиентской части **ALD Pro** необходимо выполнить команду:

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

Информация об использованных ключах расположена в разделе по установке пакетов на контроллере домена.

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`).

#### 2.2.1.4. Настройка доступных репозиториев и установка пакетов на клиенте с Альт Рабочая станция 10.4 и Альт СП 10

Для управления пакетами в **Альт Рабочая станция 10.4** и **Альт СП 10** рекомендуется использовать консольную утилиту APT.

Для установки клиентской части **ALD Pro** версии 3.0.0 на **Альт Рабочая станция 10.4** и **Альт СП 10** из официальных интернет-репозиториев РусБИТех-Астра требуется создать отдельный файл `/etc/apt/sources.list.d/aldpro.list`:

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

Вставить в этот файл содержимое и сохранить:

```
rpm https://download.astralinux.ru/aldpro/frozen/01/3.0.0/alt/p10/ 3.0.0 main
```

Повысить приоритет пакетов для данного репозитория. Для этого необходимо создать файл `/etc/apt/preferences.d/aldpro-client`:

```
sudo nano /etc/apt/preferences.d/aldpro-client
```

Внести следующее содержимое в файл:

```
Package: *
Pin: release n=x86-64
Pin-Priority: 900
```

Обновить индекс пакетов нового репозитория командой:

```
sudo apt-get update
```

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

```
sudo apt-get install -y -q aldpro-client
```

- -y — ключ позволяет автоматически ответить «Да» на все возможные вопросы в ходе установки.
- -q — ключ позволяет скрыть сообщения о прогрессе установки.

Если после этого перезагрузить пользовательский компьютер, в сообщениях ядра

появятся ошибки запуска SSSD и зависящих от нее служб (журнал загрузки можно найти в файле `/var/log/boot.log`). Это происходит потому что служба еще не настроена соответствующим образом (журнал службы SSSD можно найти в файле `/var/log/sssd/sssd.log`).

#### 2.2.1.5. Настройка доступных репозиториев и установка пакетов на клиенте с РЕД ОС 7.3.5 и РЕД ОС 8

Для управления пакетами в **РЕД ОС** рекомендуется использовать консольную утилиту DNF. Для установки клиентской части **ALD Pro** версии 3.0.0 на **РЕД ОС** из официальных интернет-репозиториев РусБИТех-Астра требуется создать отдельный список для `/etc/yum.repos.d/aldpro.repo`:

```
sudo nano /etc/yum.repos.d/aldpro.repo
```

Вставить в файл для **РЕД ОС 7.3.5**:

```
[aldpro-main]

name=aldpro

baseurl=https://download.astralinux.ru/aldpro/frozen/01/3.0.0/redos/3.0.0/7/
↪x86_64/

enabled=1

gpgcheck=1

repo_gpgcheck=0 # Параметр может понадобиться для проверки метаданных самого
↪репозитория

gpgkey=https://путь/до/файла/сертификата

priority=98 # Так как default 99 (аналог preferences в apt)
```

Вставить в файл для **РЕД ОС 8**:

```
[aldpro-main]

```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
name=aldpro

baseurl=https://download.astralinux.ru/aldpro/frozen/01/3.0.0/redos/3.0.0/8/
↪x86_64/

enabled=1

gpgcheck=1

repo_gpgcheck=0 # Параметр может понадобиться для проверки метаданных самого
↪репозитория

gpgkey=https://путь/до/файла/сертификата

priority=98 # Так как default 99 (аналог preferences в apt)
```

Обновить индекс пакетов нового репозитория командой:

```
sudo dnf makecache
```

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

```
sudo dnf install -y aldpro-client
```

- -y — ключ позволяет автоматически ответить «Да» на все возможные вопросы в ходе установки.

Если после этого перезагрузить пользовательский компьютер, в сообщениях ядра появятся ошибки запуска SSSD и зависящих от нее служб (журнал загрузки можно найти в файле `/var/log/boot.log`). Это происходит потому что служба еще не настроена соответствующим образом (журнал службы SSSD можно найти в файле `/var/log/sssd/sssd.log`).

### 2.2.2. Ввод компьютера в домен

Независимо от операционной системы, ввод компьютера в домен выполняется одинаково.

> **Внимание:** При вводе в домен компьютера, на котором включен режим замкнутой программной среды, перед запуском скрипта ввода в домен необходимо выполнить перезагрузку компьютера.

Компьютер может быть введен в домен:

- с помощью набора команд через командную строку;
- с помощью графической утилиты `aldpro-client-installer`.

Ниже описан способ с использованием командной строки. Использование графической утилиты подробно описано в **Руководстве администратора. Часть2**.

Для успешного ввода компьютера в домен 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`.

Проверить уникальность имени компьютера **pc-1** в домене **ald.company.lan** можно командой `nslookup`:

```
nslookup pc-1
```

С помощью данной команды проверяется, что хост с указанным именем не найден на **DNS**-сервере. Данная команда проверит не только имя **pc-1**, но и **pc-1.ald.company.lan**, т.к. в настройках **NetworkManager** на предыдущем шаге указан **DNS**-суффикс **ald.company.lan**.

Выполнить ввод компьютера **pc-1** можно с помощью команд:

```
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 необходимо выполнить перезагрузку компьютера:

```
sudo reboot
```

После перезагрузки необходимо войти 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. Дальнейшая аутентификация пользователя возможна через кэш **SSSD** службы.

## 2.3. Вывод компьютера из домена

Вывод компьютера из домена предполагает приведение его операционной системы в исходное состояние и удаление всех записей о хосте из каталога. Это может потребоваться, например, в случаях:

- администратор допустил опечатку в названии имени хоста;
- оборудование устарело и нужно его вывести из эксплуатации.

### 2.3.1. Действия на рабочей станции под управлением Astra Linux Special Edition

На рабочей станции сначала следует сделать откат настройки клиента **FreeIPA**, чтобы привести содержание общих конфигурационных файлов, включая настройки **PAM** стека, в исходное состояние. Для этого нужно войти в систему учетной записью локального администратора, например, **localadmin** и выполнить команду **astra-freeipa-client** с ключом `-U`:

```
sudo astra-freeipa-client -U
```

Результат выполнения команды:

```
Unenrolling client from IPA server
...
Client uninstall complete.
```

Удалить пакеты приложений, указав явно **aldpro**, **freeipa**, **sssd** и **krb5**. Все другие пакеты будут удалены через зависимости.

```
sudo apt purge 'aldpro*' 'freeipa*' 'sssd*' 'krb5*'
sudo apt autoremove --purge
```

Установить сетевые настройки с учетом нового сценария использования рабочей станции.

Проверить список профилей в домашней папке:

```
cd /home/ && ls
```

В результате отображаются профили нескольких пользователей, один из которых

локальный администратор, например, **localadmin**, который был указан при установке:

```
admin localadmin ivani ppetr
```

Удалить домашние директории доменных пользователей и оставшиеся в системе артефакты.

```
sudo rm -rf /home/admin
```

Удалить каталоги клиентских приложений подсистем **ALD Pro**:

```
sudo rm -rf /var/lib/sss/pubconf/krb5.include.d/
sudo rm -rf /etc/krb5.conf.d/
sudo rm -rf /var/lib/sss/
sudo rm -rf /etc/sssd/
sudo rm -rf /opt/rbta/aldpro/
sudo rm -rf /etc/syslog-ng/aldpro/
sudo rm -rf /srv/aldpro-salt/minion.d/
sudo rm -rf /srv/aldpro-salt/config/
sudo rm -rf /var/lib/certmonger/
```

Для удаления корневого сертификата домена из файла `/etc/ssl/certs/ca-certificates.crt` следует вызвать утилиту `update-ca-certificates`:

```
sudo update-ca-certificates
```

В завершение действий над выводимым компьютером необходимо вернуть компьютеру исходное имя хоста, например, **astra**, и перезагрузить его:

```
sudo hostnamectl set-hostname astra
sudo reboot
```

### 2.3.2. Действия на рабочей станции под управлением Альт Рабочая станция 10.4 и Альт СП 10

На рабочей станции сначала следует сделать откат настройки клиента **FreeIPA**, чтобы привести содержание общих конфигурационных файлов, включая настройки **PAM** стека, в исходное состояние.

```
sudo ipa-client-install --uninstall --unattended
```

При выполнении команды в системе происходят следующие действия:

- в службе каталога снимается отметка о том, что хост зарегистрирован в домене;
- ключи хоста удаляются из файла `/etc/krb5.keytab`;
- содержимое конфигурационных файлов, например, `/etc/krb5.conf`, `/etc/ldap/ldap.conf` приводится в исходное состояние;
- к имени файла конфигурации `/etc/sssd/sssd.conf` добавляется суффикс `.deleted`.

Удалить пакеты приложений, указав явно **aldpro**, **freeipa**, **sssd**. Все другие пакеты будут удалены через зависимости.

```
sudo apt-get remove -y --purge '^aldpro*' '^freeipa*' '^sssd*'
sudo apt-get autoremove --purge
```

Удалить домашние директории доменных пользователей:

```
sudo rm -rf /home/<логин_доменного_пользователя>
```

Удалить каталоги клиентских приложений подсистем **ALD Pro**:

```
sudo rm -rf /var/lib/sss/pubconf/krb5.include.d/
sudo rm -rf /etc/krb5.conf.d/
sudo rm -rf /var/lib/sss/
sudo rm -rf /etc/sssd/
sudo rm -rf /opt/rbta/aldpro/
sudo rm -rf /etc/syslog-ng/aldpro/
sudo rm -rf /srv/aldpro-salt/
sudo rm -rf /var/lib/certmonger/
```

Удалить репозиторий клиента **ALD Pro**:

```
sudo rm -rf /etc/apt/sources.list.d/aldpro.list
sudo rm -rf /etc/apt/preferences.d/aldpro-client
sudo apt-get update
```

Для удаления корневого сертификата домена следует вызвать утилиту `update-ca-trust`:

```
sudo update-ca-trust
```

В завершение действий над выводимым компьютером можно установить сетевые настройки и имя хоста с учетом нового сценария использования рабочей станции и перезагрузить его:

```
sudo reboot
```

### 2.3.3. Действия на рабочей станции под управлением РЕД ОС 7.3.5 и РЕД ОС 8

На рабочей станции сначала следует сделать откат настройки клиента **FreeIPA**, чтобы привести содержание общих конфигурационных файлов, включая настройки **PAM** стека, в исходное состояние.

```
sudo ipa-client-install --uninstall --unattended
```

**Внимание:** В результате выполнения команды появится сообщение об успешности вывода клиента из домена `Client uninstall complete.`, но также появится и сообщение об ошибке `The ipa-client-install command failed.`. В логе `/var/log/ipaclient-uninstall.log` при этом отобразится ошибка:

```
2025-06-06T08:47:49Z ERROR Some installation state for domainname has not
↪been restored, see /var/lib/ipa/sysrestore/sysrestore.state
```

Данная ошибка не критична и вызвана особенностями IPA-клиента в **РЕД ОС**. Чтобы она не возникала можно предварительно удалить неиспользуему секцию [domainname] из файла конфигурации для восстановления /var/lib/ipa-client/sysrestore/sysrestore.state. Это можно сделать вручную или воспользоваться командой:

```
sudo sed -i '/\[domainname\]/,/enabled = False/ d' /var/lib/ipa-client/
↪sysrestore/sysrestore.state
```

При выполнении команды в системе происходят следующие действия:

- в службе каталога снимается отметка о том, что хост зарегистрирован в домене;
- ключи хоста удаляются из файла `/etc/krb5.keytab`;
- содержимое конфигурационных файлов, например, `/etc/krb5.conf`, `/etc/ldap/ldap.conf` приводится в исходное состояние;
- к имени файла конфигурации `/etc/sssd/sssd.conf` добавляется суффикс `.deleted`.

Удалить пакеты приложений, указав явно **aldpro**, **freeipa**, **sssd** и **krb5**. Все другие пакеты будут удалены через зависимости.

```
sudo dnf remove --exclude=krb5-libs -y 'aldpro*' 'freeipa*' 'sssd*' 'krb5*'
sudo dnf -y autoremove
```

Удалить домашние директории доменных пользователей.

```
sudo ls -l /home
sudo rm -rf /home/<логин_доменного_пользователя>
```

Удалить каталоги клиентских приложений подсистем **ALD Pro**:

```
sudo rm -rf /var/lib/sss/pubconf/krb5.include.d/
sudo rm -rf /etc/krb5.conf.d/
sudo rm -rf /var/lib/sss/
sudo rm -rf /etc/sssd/
sudo rm -rf /opt/rbta/aldpro/
sudo rm -rf /etc/syslog-ng/aldpro/
sudo rm -rf /srv/aldpro-salt/
sudo rm -rf /var/lib/certmonger/
```

Удалить репозиторий клиента **ALD Pro**:

```
sudo rm -rf /etc/yum.repos.d/aldpro.repo
sudo dnf makecache
```

Для удаления корневого сертификата домена следует вызвать утилиту `update-ca-trust`:

```
sudo update-ca-trust
```

В завершение действий над выводимым компьютером можно установить сетевые настройки и имя хоста с учетом нового сценария использования рабочей станции и перезагрузить его:

```
sudo reboot
```

### 2.3.4. Действия на контроллере домена

На сервере **dc-1** нужно удалить **DNS**-записи хоста, а затем и сам хост.

```
kinit admin
ipa dnsrecord-del ald.company.lan. pc-1 --del-all
```

Результат удаления записей **DNS**:

```
----------------------
Удалена запись "pc-1"
----------------------
```

Удалить выводимый компьютер из базы системы **FreeIPA**:

```
ipa host-del pc-1.ald.company.lan
```

Результат удаления компьютера:

```
---------------------------------
Удалён узел "pc-1.ald.company.lan"
---------------------------------
```

## 2.4. Установка резервного контроллера домена

Установка резервного контроллера домена выполняется в два этапа:

- подготовка сервера к установке и вводу в домен как обычной рабочей станции.
- назначение серверу роли контроллера домена на портале управления, повышение роли сервера происходит автоматически благодаря системе автоматизации.

### 2.4.1. Подготовка к установке резервного контроллера

Для установки резервного контроллера **dc-2.ald.company.lan** нужно подготовить сервер с такими же техническими характеристиками, как и первый контроллер домена, т.к. реплика будет содержать в базе данных полную копию каталога и должна принять на себя всю нагрузку при отключении основного сервера.

Необходимо убедиться, что на сервере установлена совместимая ОС **Astra Linux Special Edition** версии 1.7.xxx с максимальным уровнем защищенности «Смоленск». Сделать это можно с помощью следующих команд:

```
cat /etc/astra/build_version
sudo astra-modeswitch getname
```

Отключите службу **NetworkManager** на сервере:

```
sudo systemctl stop NetworkManager
sudo systemctl disable NetworkManager
sudo systemctl mask NetworkManager
sudo systemctl status NetworkManager
```

Назначьте сетевому интерфейсу статический адрес и другие параметры в файле `/etc/network/interfaces`:

```
auto lo
iface lo inet loopback

auto eth0
    iface eth0 inet static
    address 10.0.1.12
```

(продолжение на следующей странице)

```
    netmask 255.255.255.0
    gateway 10.0.1.1
```

На момент установки резервного контроллера разрешение имен должно выполняться через первый контроллер домена, поэтому содержимое файла `/etc/resolv.conf` должно быть следующим:

```
search ald.company.lan
nameserver 10.0.1.11
```

Чтобы применить новые настройки, следует перезапустить службу `\Networking`. Может потребоваться также очистить старое соединение командой `flush` утилиты `ip`:

```
sudo ip addr flush dev eth0
sudo systemctl restart networking
```

Если IP-адрес реплики будет находиться не в той же подсети, что и первый контроллер домена, то администратору нужно будет вручную добавить соответствующую обратную зону, т.к. автоматическое создание обратных зон отключено по соображениям безопасности (см. **Руководство пользователя → Роли и службы сайта → Служба разрешения имен → Перенаправление запросов** - добавление зоны).

Далее необходимо установить имя хоста:

```
sudo hostnamectl set-hostname dc-2.ald.company.lan
```

Содержимое файла `/etc/hosts` на **dc-2** должно выглядеть следующим образом:

```
10.0.1.12 dc-2.ald.company.lan dc-2
127.0.0.1 localhost.localdomain localhost
#127.0.1.1 dc-2 - закомментировать или удалить строку с адресом локальной
 ↪петли
```

Проверить доступность контроллера домена **dc-1** и сервера репозиториев **dl.astralinux.ru** можно следующими командами:

```
ping -c 4 dc-1
ping -c 4 dl.astralinux.ru
```

Подключение репозиториев операционной системы **Astra Linux Special Edition** 1.7.xxx и

продукта **ALD Pro** описано подробно в *Развертывание первого контроллера домена*.

Содержание файла `/etc/apt/sources.list` должно быть следующим:

```
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
```

Содержимое файла `/etc/apt/sources.list.d/aldpro.list` должно быть следующим:

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

Обновить списки пакетов и программное обеспечение можно следующими командами:

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

Установить клиентскую часть продукта **ALD Pro**:

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

Ввод хоста **dc-2** в домен **ald.company.lan** выполняется следующими командами:

```
sudo /opt/rbta/aldpro/client/bin/aldpro-client-installer --domain ald.company.
 ↪lan --account admin --host dc-2 --gui --force
```

После ввода команды система запросит ввести пароль администратора домена.

Для применения новых параметров требуется перезагрузить сервер:

```
sudo reboot
```

### 2.4.2. Повышение роли сервера до резервного контроллера домена

Повышение роли сервера до резервного контроллера домена выполняется через портал управления на странице **Управление доменом → Сайты и службы → Контроллеры домена**. Необходимо нажать кнопку **Новый контроллер домена** и установить следующие параметры:

- Имя контроллера - выберите целевой хост из списка.
- Имя сайта - определите сайт, который нужно назначить контроллеру домена.
- Назначить роль глобального контроллера - установите флажок, чтобы автоматически установить на сервере модуль глобального каталога.
- Назначить роль `pkiproxy` - установите флажок, чтобы будущий контроллер мог обрабатывать запросы на выпуск сертификатов. Для успешного назначения этой роли на целевом хосте нужно заранее создать файл `/etc/ssl/freeipa/ca.key` и поместить в него закрытый ключ от доменного сертификата.

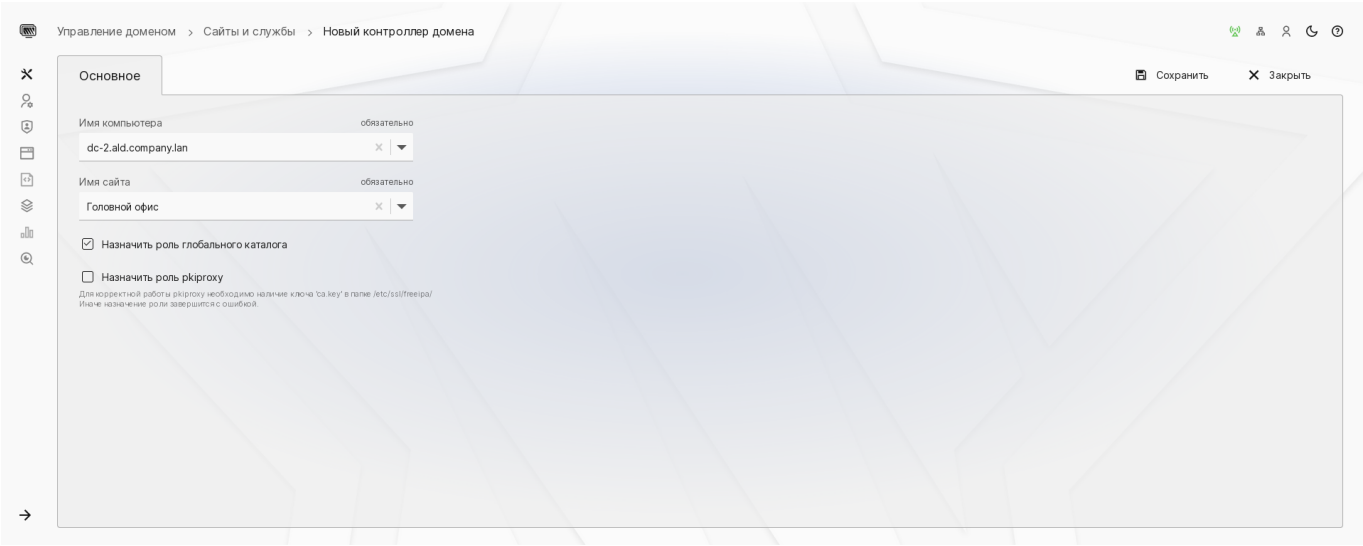


Рисунок 2.3 – Повышение роли сервера до контроллера домена

Роль автоматически применится в течение 30 минут.

Результат установки роли можно увидеть в карточке хоста.

Дополнительную информацию о процессе установки можно получить на целевом хосте в журналах `term.log` и `minion` или воспользоваться утилитой `journalctl` с ключом `-f`, которая позволяет получить информацию напрямую из `systemd`:

```
sudo tail /var/log/apt/term.log
sudo tail /var/log/aldpro-salt/minion
sudo journalctl -f
```

Для форсирования установки подсистемы можно использовать следующую команду:

```
sudo aldpro-roles --iud
```

Процесс установки виден в выводе команды форсирования, результат установки отображается в карточке сервера на портале управления.

Если установка подсистемы завершится ошибкой, то повторную установку можно будет запустить следующей командой:

```
sudo aldpro-roles --iud --action install
```

После установки резервного контроллера домена начнется репликация данных, которая займет некоторое время. Информацию о завершении репликации можно будет увидеть в файле `/var/log/dirsrv/slapd-ALD-COMPANY-LAN/errors`.

```
sudo cat /var/log/dirsrv/slapd-ALD-COMPANY-LAN/errors | grep 'import userRoot
↪'

[25/Nov/2024:09:40:09.407239382 +0300] - INFO - bdb_import_monitor_threads -
↪import userRoot: Workers finished; cleaning up...
[25/Nov/2024:09:40:09.641808546 +0300] - INFO - bdb_import_monitor_threads -
↪import userRoot: Workers cleaned up.
[25/Nov/2024:09:40:09.668458995 +0300] - INFO - bdb_public_bdb_import_main -
↪import userRoot: Indexing complete.  Post-processing...
[25/Nov/2024:09:40:09.684394481 +0300] - INFO - bdb_public_bdb_import_main -
↪import userRoot: Generating numsubordinates (this may take several minutes
↪to complete)...
[25/Nov/2024:09:40:09.756181641 +0300] - INFO - bdb_public_bdb_import_main -
↪import userRoot: Generating numSubordinates complete.
[25/Nov/2024:09:40:09.770676960 +0300] - INFO - bdb_get_nonleaf_ids - import
↪userRoot: Gathering ancestorid non-leaf IDs...
[25/Nov/2024:09:40:09.784493153 +0300] - INFO - bdb_get_nonleaf_ids - import
↪userRoot: Finished gathering ancestorid non-leaf IDs.
[25/Nov/2024:09:40:09.799225688 +0300] - INFO - ldbm_get_nonleaf_ids -
↪import userRoot: Starting sort of ancestorid non-leaf IDs...
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
[25/Nov/2024:09:40:09.815333717 +0300] - INFO - ldbm_get_nonleaf_ids -
↪import userRoot: Finished sort of ancestorid non-leaf IDs.
[25/Nov/2024:09:40:09.846484631 +0300] - INFO - bdb_ancestorid_new_idl_create_
↪index - import userRoot: Creating ancestorid index (new idl)...
[25/Nov/2024:09:40:09.893268580 +0300] - INFO - bdb_ancestorid_new_idl_create_
↪index - import userRoot: Created ancestorid index (new idl).
[25/Nov/2024:09:40:09.907374703 +0300] - INFO - bdb_public_bdb_import_main -
↪import userRoot: Flushing caches...
[25/Nov/2024:09:40:09.921178776 +0300] - INFO - bdb_public_bdb_import_main -
↪import userRoot: Closing files...
[25/Nov/2024:09:40:10.723980460 +0300] - INFO - bdb_public_bdb_import_main -
↪import userRoot: Import complete.  Processed 3616 entries in 7 seconds.
↪(516.57 entries/sec)
```

## 2.5. Установка подсистемы сетевого репозитория

Установка сервера подсистемы сетевого репозитория выполняется в два этапа:

1. ввод сервера в домен как обычной рабочей станции.
2. назначение серверу роли **Сервера репозиториев ПО** на портале управления, установка и настройка происходит автоматически благодаря системе автоматизации.

### 2.5.1. Установка сервера репозиториев

Подготовить сервер репозиториев для установки и обновления программного обеспечения по сети с учетом минимальных требований.

Выполнить настройку сетевого интерфейса согласно *Настройка сетевого интерфейса* и *Настройка сети на клиентских компьютерах*.

Проверить доступность репозиториев **dl.astralinux.ru** и ответ от контроллера домена **dc-1**:

```
ip a
ping -c 4 dl.astralinux.ru
ping -c 4 dc-1.ald.company.lan
ping -c 4 dc-1
```

Настроить репозитории (см. *Настройка доступных репозиториев и установка пакетов на клиенте с Astra Linux Special Edition 1.7.xxx*) и обновить программное обеспечение согласно **Руководство администратора. Часть 1 → Матрицы совместимости и обновлений → Матрица совместимости**.

Установить клиентский пакет программ **ALD Pro**:

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

Ввести сервер репозиториев **repo** в домен **dc-1**:

```
sudo /opt/rbta/aldpro/client/bin/aldpro-client-installer --domain ald.company.
↪lan --account admin  --host repo --gui --force
```

После ввода команды система запросит ввести пароль администратора домена.

Перезагрузить сервер **repo**, чтобы настройки вступили в силу:

```
sudo reboot
```

В портале управления в разделе **Установка и обновление ПО → Репозитории ПО** на вкладке **Серверы репозиториев ПО** развернуть сервер репозиториев нажав на кнопку [**Новый сервер репозиториев ПО**], привязав его к сайту **Головной офис**, см. *Добавление сервера репозиториев*.

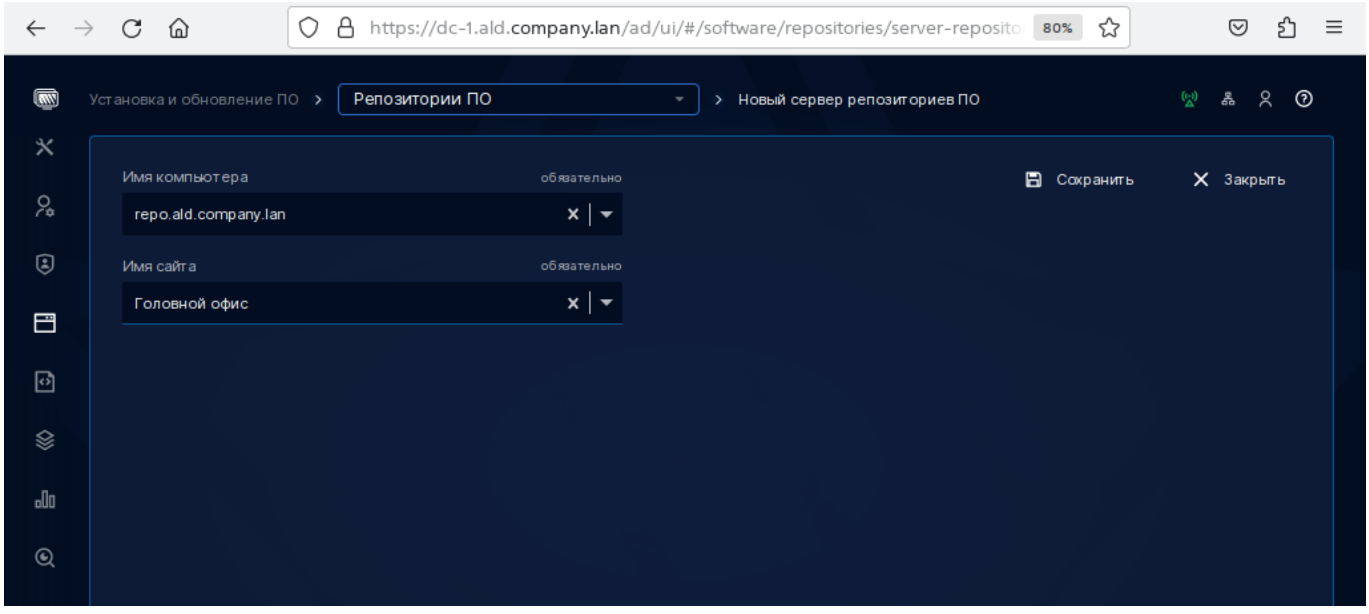


Рисунок 2.4 – Добавление сервера репозиториев

Роль автоматически примениться через 30 минут.

Начало и окончание установки можно посмотреть на карточке хоста на портале управления в журналах `term.log` и `minion` или воспользоваться утилитой `journalctl` с ключом `-f`.

Форсировать применение роли можно командой:

```
sudo aldpro-roles --iud
```

Подробнее о применения форсирования описано в разделе **Утилиты для работы с групповыми политиками, подсистемами и заданиями автоматизации** в **Руководство администратора. Часть 2**.

## 2.6. Установка подсистемы общего доступа к файлам

Установка сервера подсистемы общего доступа к файлам выполняется в два этапа:

1. ввод сервера в домен как обычную рабочую станцию с именем **files**.
2. назначение серверу роли **Сервер общего доступа к файлам** на портале управления, установка и настройка происходит автоматически благодаря системе автоматизации.

### 2.6.1. Установка сервера общего доступа к файлам

Подготовить сервер общего доступа к файлам (минимальные характеристики см. **Общая информация** → **Технологический стек** → таблица → пункт **Подсистема общего доступа к файлам**).

Выполнить настройку сетевого интерфейса согласно *Настройка сетевого интерфейса* и *Настройка сети на клиентских компьютерах*.

Проверить доступность репозиториев **dl.astralinux.ru** и ответ от контроллера домена **dc-1**:

```
ip a
ping -c 4 dl.astralinux.ru
ping -c 4 dc-1.ald.company.lan
ping -c 4 dc-1
```

Настроить репозитории (см. *Настройка доступных репозиториев и установка пакетов*

*на клиенте с Astra Linux Special Edition 1.7.xxx*) и обновить программное обеспечение согласно **Матрице совместимости Руководство администратора. Часть 2**.

Установить клиентский пакет программ **ALD Pro**:

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

Ввести сервер общего доступа к файлам **files** в домен **dc-1**:

```
sudo /opt/rbta/aldpro/client/bin/aldpro-client-installer --domain ald.company.
↪lan --account admin --host files --gui --force
```

После ввода команды система запросит ввести пароль администратора домена.

Перезагрузить сервер **files**, чтобы настройки вступили в силу:

```
sudo reboot
```

В портале управления в разделе **Роли и службы сайта → Общий доступ к файлам** на вкладке **Перечень серверов** развернуть сервер общего доступа, нажав на кнопку [**Новый сервер**]. В окне нового сервера выбрать **files.ald.company.lan**, привязав его к сайту **Головной офис**, см. *Добавление сервера общего доступа к к файлам*.

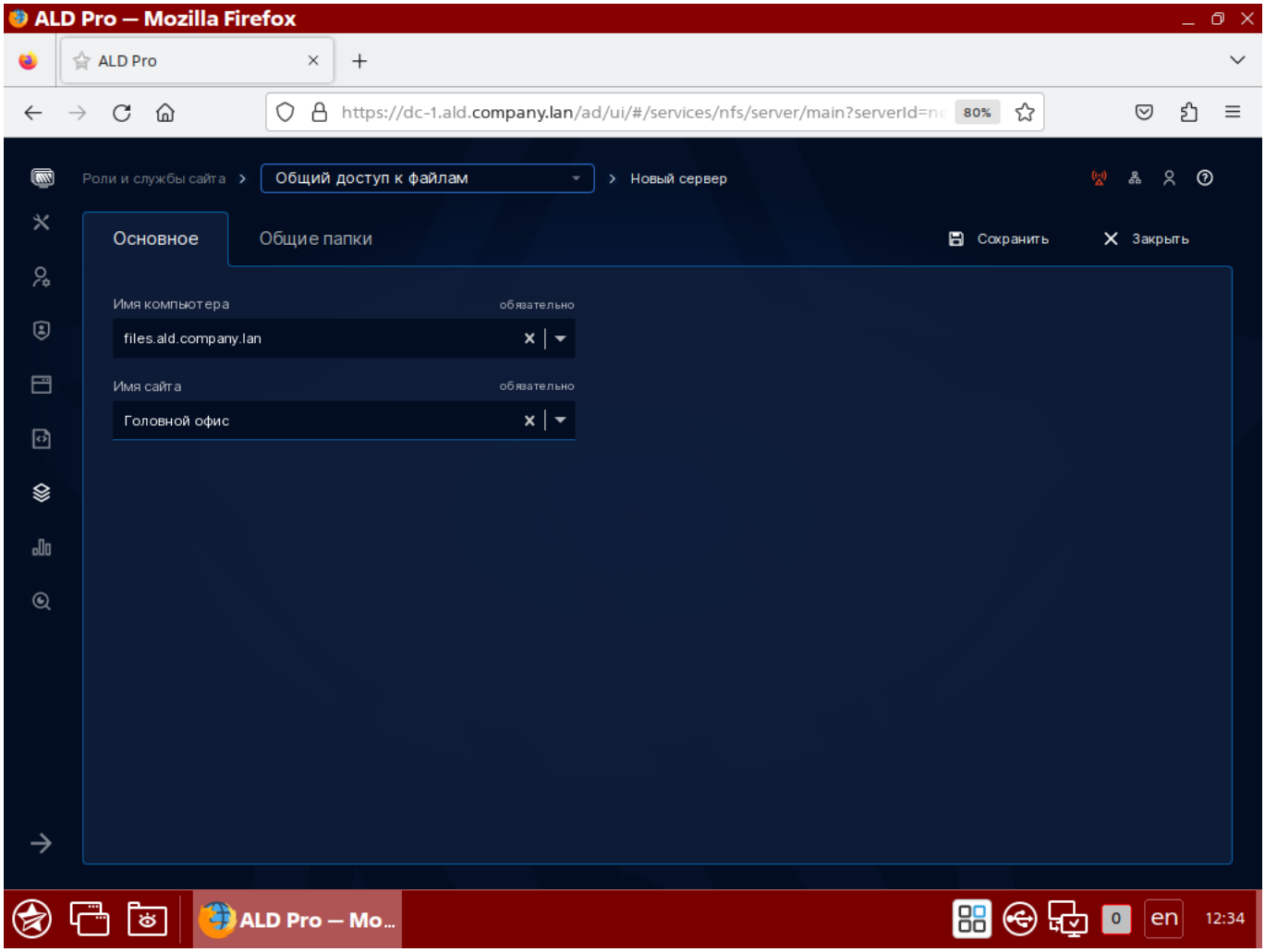


Рисунок 2.5 – Добавление сервера общего доступа к к файлам

Роль автоматически примениться через 30 минут.

Начало и окончание установки можно посмотреть на карточке хоста на портале управления в журналах `term.log` и `minion` или воспользоваться утилитой `journalctl` с ключом `-f`.

Форсировать применение роли можно командой:

```
sudo aldpro-roles --iud
```

Подробнее о применения форсирования описано в разделе **Утилиты для работы с групповыми политиками, подсистемами и заданиями автоматизации** в **Руководство администратора. Часть 2**.

После успешной установки сервера общего доступа к файлам, пользователь, при наличии соответствующих ролей и привилегий, может самостоятельно создавать общие папки и давать доступ к файлам.

## 2.7. Установка подсистемы сервера печати

Подготовить сервер печати в соответствии с минимальными требованиями **Общая информация** → **Технологический стек** → таблица → пункт **Подсистема службы печати**.

Выполнить настройку сетевого интерфейса согласно *Настройка сетевого интерфейса* и *Настройка сети на клиентских компьютерах*.

Проверить доступность репозиториев **dl.astralinux.ru** и ответ от контроллера домена **dc-1**:

```
ip a
ping -c 4 dl.astralinux.ru
ping -c 4 dc-1.ald.company.lan
ping -c 4 dc-1
```

Настроить репозитории (см. *Настройка доступных репозиториев и установка пакетов на клиенте с Astra Linux Special Edition 1.7.xxx*) и обновить программное обеспечение согласно **Руководство администратора. Часть 1** → **Матрицы совместимости и обновлений** → **Матрица совместимости**.

Установить клиентский пакет программ **ALD Pro**:

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

Ввести сервер печати **cups** в домен **dc-1**:

```
sudo /opt/rbta/aldpro/client/bin/aldpro-client-installer --domain ald.company.
↪lan --account admin --host cups --gui --force
```

После ввода команды система запросит ввести пароль администратора домена.

Перезагрузить сервер **cups**, чтобы настройки вступили в силу:

```
sudo reboot
```

В портале управления в разделе **Роли и службы сайта** → **Служба печати** на вкладке **Серверы печати** развернуть сервер общего доступа **cups**, нажав на кнопку [**Новый сервер печати**], привязать его к сайту **Головной офис** см. *Добавление сервера печати*.

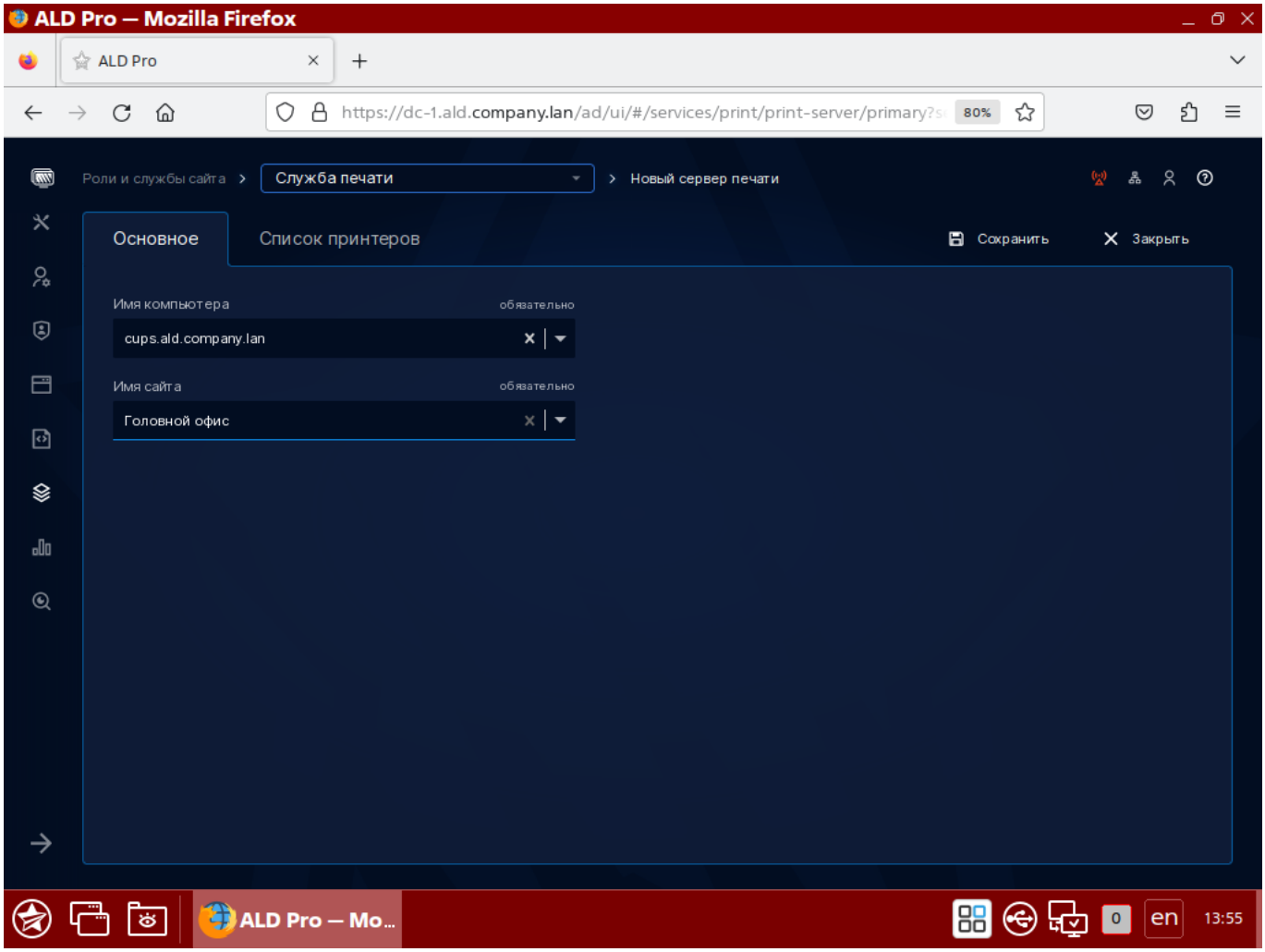


Рисунок 2.6 – Добавление сервера печати

Роль автоматически примениться через 30 минут.

Начало и окончание установки можно посмотреть на карточке хоста на портале управления в журналах `term.log` и `minion` или воспользоваться утилитой `journalctl` с ключом `-f`.

Форсировать применение роли можно командой:

```
sudo aldpro-roles --iud
```

Подробнее о применения форсирования описано в разделе **Утилиты для работы с групповыми политиками, подсистемами и заданиями автоматизации** в **Руководство администратора. Часть 2**.

## 2.8. Установка подсистемы «Динамическая настройка узла» DHCP

Подготовить сервер динамической настройки узлов в соответствии с минимальными требованиями, **Общая информация** → **Технологический стек** → таблица → пункт **Подсистема динамической настройки узла**.

Выполнить настройку сетевого интерфейса согласно *Настройка сетевого интерфейса* и *Настройка сети на клиентских компьютерах*.

Проверить доступность репозиториев **dl.astralinux.ru** и ответ от контроллера домена **dc-1**:

```
ip a
ping -c 4 dl.astralinux.ru
ping -c 4 dc-1.ald.company.lan
ping -c 4 dc-1
```

Настроить репозитории (см. *Настройка доступных репозиториев и установка пакетов на клиенте с Astra Linux Special Edition 1.7.xxx*) и обновить программное обеспечение согласно **Руководство администратора. Часть 1** → **Матрицы совместимости и обновлений** → **Матрица совместимости**.

Установить клиентский пакет программ **ALD Pro**:

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

Ввести сервер **dhcp** в домен **dc-1**:

```
sudo /opt/rbta/aldpro/client/bin/aldpro-client-installer --domain ald.company.
↪lan --account admin --host dhcp --gui --force
```

После ввода команды система запросит ввести пароль администратора домена.

Перезагрузить сервер **dhcp**, чтобы настройки вступили в силу:

```
sudo reboot
```

В портале управления в разделе **Роли и службы сайта** → **Служба динамической настройки узла** на вкладке **Перечень серверов** развернуть сервер **DHCP**, нажав на кнопку [**Новый сервер**]. Выбрать сервер **dhcp.ald.company.lan** и привязать его к сайту

**Головной офис** см. *Добавление сервера DHCP*.

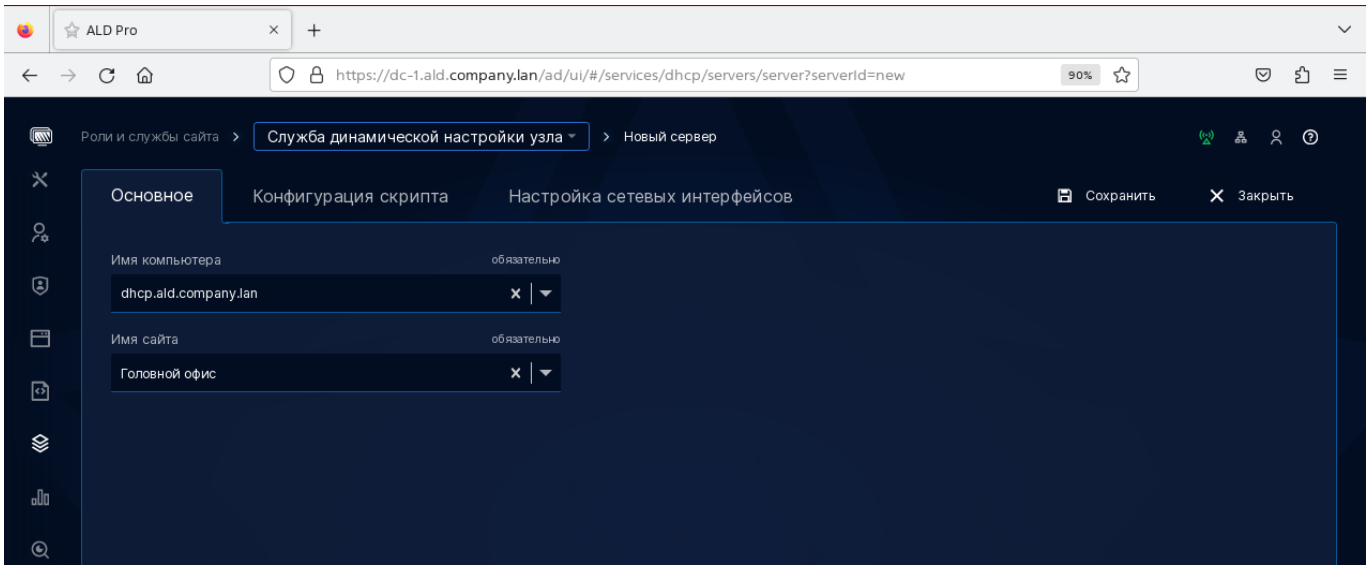


Рисунок 2.7 – Добавление сервера DHCP

Роль автоматически примениться через 30 минут.

Начало и окончание установки можно посмотреть на карточке хоста на портале управления в журналах `term.log` и `minion` или воспользоваться утилитой `journalctl` с ключом `-f`.

Форсировать применение роли можно командой:

```
sudo aldpro-roles --iud
```

Подробнее о применения форсирования описано в разделе **Утилиты для работы с групповыми политиками, подсистемами и заданиями автоматизации** в **Руководство администратора. Часть 2**.

## 2.9. Установка подсистемы «Установка ОС по сети» TFTP + PXE

Подготовить сервер подсистемы установки ОС по сети в соответствии с минимальными требованиями, см. **Общая информация** → **Технологический стек** → таблица → пункт **Подсистема установки ОС по сети**.

Выполнить настройку сетевого интерфейса согласно *Настройка сетевого интерфейса* и *Настройка сети на клиентских компьютерах*.

Проверить доступность репозиториев **dl.astralinux.ru** и ответ от контроллера домена **dc-1**:

```
ip a
ping -c 4 dl.astralinux.ru
ping -c 4 dc-1.ald.company.lan
ping -c 4 dc-1
```

Настроить репозитории (см. *Настройка доступных репозиториев и установка пакетов на клиенте с Astra Linux Special Edition 1.7.xxx*) и обновить программное обеспечение согласно **Руководство администратора. Часть 1** → **Матрицы совместимости и обновлений** → **Матрица совместимости**.

Установить клиентский пакет программ **ALD Pro**:

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

Ввести сервер установки ОС по сети **pxe** в домен **dc-1**:

```
sudo /opt/rbta/aldpro/client/bin/aldpro-client-installer --domain ald.company.
↪lan --account admin --host pxe --gui --force
```

После ввода команды система запросит ввести пароль администратора домена.

Перезагрузить сервер **pxe**, чтобы настройки вступили в силу:

```
sudo reboot
```

В портале управления в разделе **Автоматизация** → **Установка ОС по сети** на вкладке **Серверы установки ОС** развернуть сервер **pxe**, нажав на кнопку [**Новый сервер**]. Выбрать сервер **pxe.ald.company.lan**, привязав его к сайту **Головной офис**. А также

выбрать DHCP-сервер **dhcp.ald.company.lan**, который будет настраивать параметры новым сетевым устройствам. см. *Добавление нового сервера установки ОС по сети PXE*.

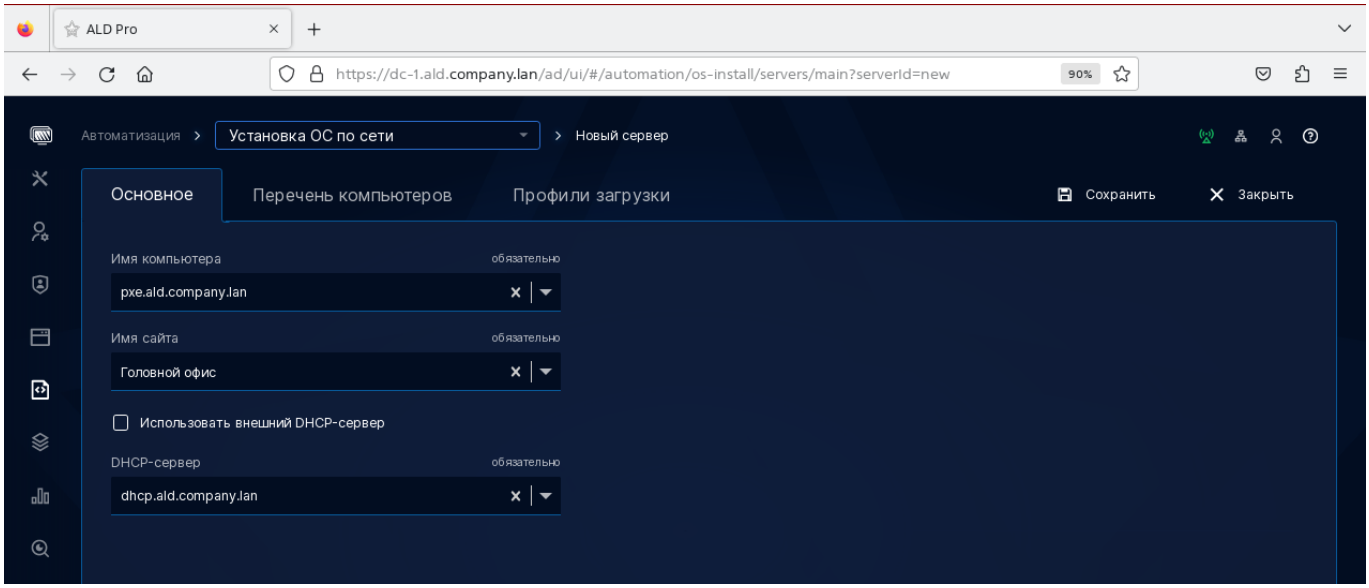


Рисунок 2.8 – Добавление нового сервера установки ОС по сети PXE

Роль автоматически примениться через 30 минут.

Начало и окончание установки можно посмотреть на карточке хоста на портале управления в журналах `term.log` и `minion` или воспользоваться утилитой `journalctl` с ключом `-f`.

Форсировать применение роли можно командой:

```
sudo aldpro-roles --iud
```

Подробнее о применения форсирования описано в разделе **Утилиты для работы с групповыми политиками, подсистемами и заданиями автоматизации** в **Руководство администратора. Часть 2**.

## 2.10. Установка подсистемы мониторинга

Подготовить сервер подсистемы мониторинга в соответствии с минимальными требованиями, см. **Общая информация** → **Технологический стек** → таблица → пункт **Подсистема мониторинга**.

Выполнить настройку сетевого интерфейса согласно *Настройка сетевого интерфейса* и *Настройка сети на клиентских компьютерах*.

Проверить доступность репозиториев **dl.astralinux.ru** и ответ от контроллера домена **dc-1**:

```
ip a
ping -c 4 dl.astralinux.ru
ping -c 4 dc-1.ald.company.lan
ping -c 4 dc-1
```

Настроить репозитории (см. *Настройка доступных репозиториев и установка пакетов на клиенте с Astra Linux Special Edition 1.7.xxx*) и обновить программное обеспечение согласно **Руководство администратора. Часть 1** → **Матрицы совместимости и обновлений** → **Матрица совместимости**.

Установить клиентский пакет программ **ALD Pro**:

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

Ввести сервер мониторинга **mon** в домен **dc-1**:

```
sudo /opt/rbta/aldpro/client/bin/aldpro-client-installer --domain ald.company.
↪lan --account admin --host mon --gui --force
```

После ввода команды система запросит ввести пароль администратора домена.

Перезагрузить сервер **mon**, чтобы настройки вступили в силу:

```
sudo reboot
```

На портале управления в разделе **Мониторинг** → **Журнал событий мониторинга** на вкладке **Серверы мониторинга** развернуть сервер мониторинга **mon**, нажав на кнопку [**Развернуть сервер мониторинга**]. В окне нового сервера выбрать **mon.ald.company.lan**, привязав его к сайту **Головной офис**, см. *Добавление нового сервера мониторинга*.

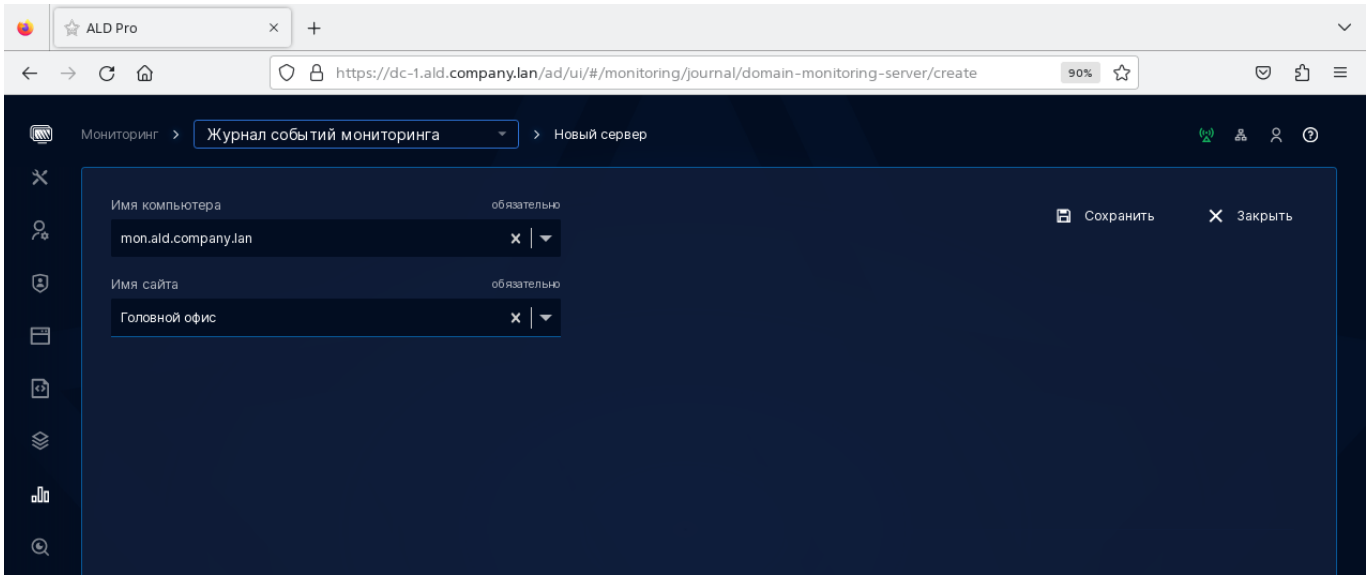


Рисунок 2.9 – Добавление нового сервера мониторинга

Роль автоматически примениться через 30 минут.

Начало и окончание установки можно посмотреть на карточке хоста на портале управления в журналах `term.log` и `minion` или воспользоваться утилитой `journalctl` с ключом `-f`.

Форсировать применение роли можно командой:

```
sudo aldpro-roles --iud
```

Подробнее о применения форсирования описано в разделе **Утилиты для работы с групповыми политиками, подсистемами и заданиями автоматизации** в **Руководство администратора. Часть 2**.

## 2.11. Установка подсистемы журналирования

Подготовить сервер подсистемы мониторинга в соответствии с минимальными требованиями, см. **Общая информация** → **Технологический стек** → таблица → пункт **Подсистема журналирования**.

Выполнить настройку сетевого интерфейса согласно *Настройка сетевого интерфейса* и *Настройка сети на клиентских компьютерах*.

Проверить доступность репозиториев **dl.astralinux.ru** и ответ от контроллера домена **dc-1**:

```
ip a
ping -c 4 dl.astralinux.ru
ping -c 4 dc-1.ald.company.lan
ping -c 4 dc-1
```

Настроить репозитории (см. *Настройка доступных репозиториев и установка пакетов на клиенте с Astra Linux Special Edition 1.7.xxx*) и обновить программное обеспечение согласно **Руководство администратора. Часть 1** → **Матрицы совместимости и обновлений** → **Матрица совместимости**.

Установить клиентский пакет программ **ALD Pro**:

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

Ввести сервер журналирования **audit** в домен **dc-1**:

```
sudo /opt/rbta/aldpro/client/bin/aldpro-client-installer --domain ald.company.
↪lan --account admin --host audit --gui --force
```

После ввода команды система запросит ввести пароль администратора домена.

Перезагрузить сервер **audit**, чтобы настройки вступили в силу:

```
sudo reboot
```

В портале управления в разделе **Журнал событий** → **Серверы журнала событий** на вкладке **Серверы журнала событий** развернуть сервер журналирования **audit**, нажав на кнопку [**Развернуть сервер журнала событий**]. В окне нового сервера выбрать **audit.ald.company.lan**, привязав его к сайту **Головной офис**, см. *Добавление нового сервера журналирования*.

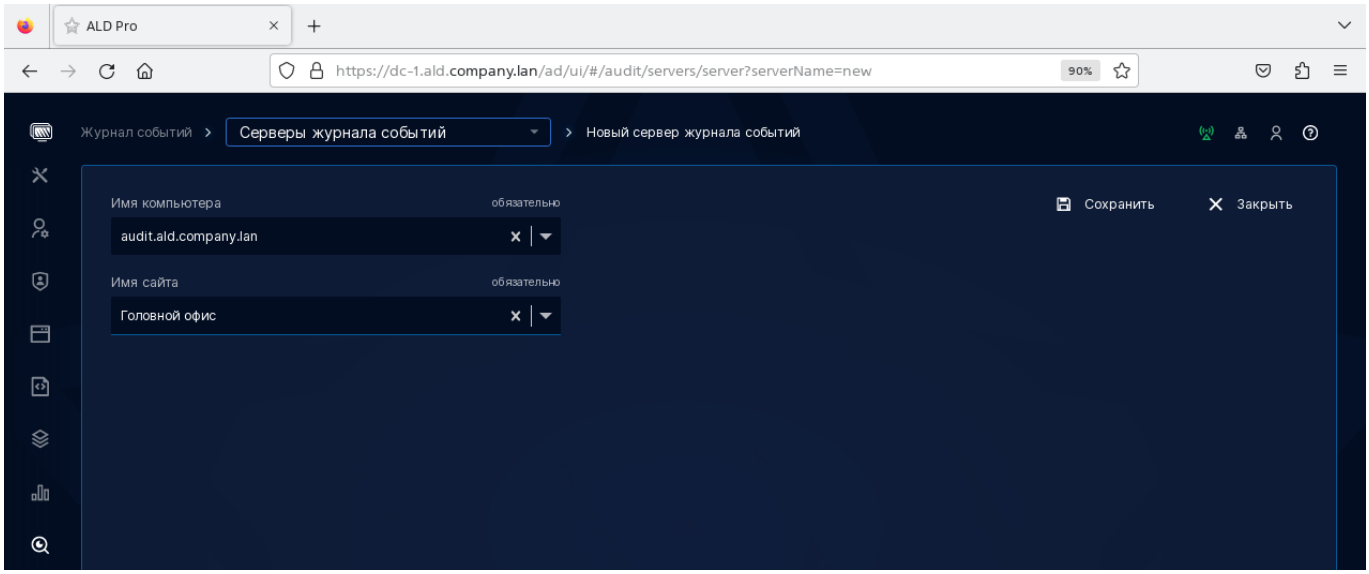


Рисунок 2.10 – Добавление нового сервера журналирования

Роль автоматически примениться через 30 минут.

Начало и окончание установки можно посмотреть на карточке хоста на портале управления в журналах `term.log` и `minion` или воспользоваться утилитой `journalctl` с ключом `-f`.

Форсировать применение роли можно командой:

```
sudo aldpro-roles --iud
```

Подробнее о применения форсирования описано в разделе **Утилиты для работы с групповыми политиками, подсистемами и заданиями автоматизации** в **Руководство администратора. Часть 2**.

## 2.12. Установка модуля инвентаризации

В составе программного комплекса **ALD Pro** предоставляется возможность установки и использования **ACM 1.3.0** как модуля инвентаризация со следующими ограничениями по функциональности:

1. Управление инфраструктурой Системы:

- создание, редактирование и удаление сегментов управления;
- создание, редактирование и удаление серверов агентов.

2. Управление пользователями и их возможностями:

- ведение списка пользователей;
- разграничение возможностей пользователей;
- управление наборами возможностей пользователей.

3. Управление организационной структурой (директориями) компьютеров:

- создание, редактирование и удаление подразделений (директорий) компьютеров;
- ведение списка подразделений (директорий) компьютеров;
- возможность настройки организационной структуры подразделений (директорий) компьютеров в иерархическом виде;
- возможность управления составом компьютеров в директории.

4. Управление компьютерами:

- установка агента и подключение управляемого компьютера к системе;
- создание, редактирование и удаление записей компьютеров;
- ведение списка компьютеров;
- возможность экспорта отчета по списку компьютеров в файл;
- возможность экспорта отчета по инвентарным данным компьютера в файл.

5. Аппаратная инвентаризация:

- возможность сбора инвентарных данных об аппаратной части управляемых компьютеров;
- возможность просмотра собранных сведений об аппаратной части управляемых компьютеров.

6. Инвентаризация установленного ПО:

- возможность сбора инвентарных данных по программной части управляемых компьютеров;
- управление (создание, изменение, удаление) правилами обнаружения ПО на управляемых компьютерах;
- предоставление предустановленных правил обнаружения ПО;
- возможность просмотра собранных сведений о программной части управляемых компьютеров;
- возможность просмотра собранных сведений о пакетах ПО на управляемых компьютерах.

7. Учет лицензий:

- выполнение учета лицензий **ОС Astra Linux** на основе собранных инвентарных данных с управляемых компьютеров;
- возможность экспорта отчета по списку лицензий **ОС Astra Linux** в файл;
- возможность экспорта отчета по данным отдельной выбранной лицензии **ОС Astra Linux** в файл.

8. Управление пользовательской сессией в веб-браузере:

- возможность входа в Систему через веб-интерфейс;
- завершение текущей сессии в веб-интерфейсе Системы;
- управление цветовой схемой веб-интерфейса Системы.

9. Справочный центр:

- наличие встроенного в Систему справочного центра на русском языке;
- возможность доступа к справочному центру из любого компонента Системы.

Модуль инвентаризации на базе **ACM** не поддерживает следующие возможности полнофункциональной версии **ACM 1.3.0**:

- управление динамическими коллекциями;
- управление репозиториями и пакетами ПО;
- управление ПО: настраиваемая автоматическая установка, удаление пакетов ПО, выполнение команд и скриптов на управляемых компьютерах клиентах;
- установка ОС по сети, управление профилями и параметрами первичной установки

ОС;

- минорное обновление **ОС Astra Linux** компьютеров клиентов;
- мажорное обновление **ОС Astra Linux** компьютеров клиентов;
- возможность получения результатов выполнения профилей управления, профилей обновления ОС и файлов логов выполнения команд с управляемых компьютеров клиентов;
- сервис отчетов **ACM DWH**.

Порядок установки и обновления модуля инвентаризации представлен в рабочей документации по продукту **ACM**.

# Обновление подсистем

## 3.1. Обновление первого контроллера домена

При обновлении ПК ALD Pro необходимо придерживаться совместимых версий ОС Astra Linux согласно Матрице совместимости ПК ALD Pro в разделе *Матрицы совместимости и обновлений*.

Пример порядка обновления с версии 2.3.0 до 2.4.1

Исходные данные: ОС Astra Linux 1.7.4 ALD Pro 2.3.0

Согласно Матрице совместимости, **ALD Pro** 2.4.1 не поддерживает **ОС Astra Linux** 1.7.4, поэтому напрямую обновить **ALD Pro** до версии 2.4.1 невозможно. Необходимо вычислить версию ОС, совместимую одновременно с **ALD Pro** 2.3.0 и ALD Pro 2.4.1. В данном случае такая версия 1.7.5 UU1 (из наивысших).

Порядок обновления может быть следующим: 1. Обновление ОС до 1.7.5 UU1. 2. Обновление ALD Pro до 2.4.1.

Пример порядка обновления с версии 2.3.0 до 2.5.0

Исходные данные: ОС Astra Linux 1.7.4 ALD Pro 2.3.0

Согласно Матрице совместимости нет такой версии ОС, которая совместима и с **ALD Pro** 2.3.0, и с **ALD Pro** 2.5.0, поэтому напрямую обновить **ALD Pro** 2.3.0 до версии 2.5.0 невозможно. В таком случае необходимо провести обновление через промежуточную версию **ALD Pro**.

Порядок обновления может быть следующим: 1. Обновление ОС до 1.7.5 UU1. 2. Обновление ALD Pro до 2.4.1. 3. Обновление ОС до 1.7.6 UU2. 4. Обновление ALD Pro до 2.5.0.

---

**Важно:** Перед обновлением до ALD Pro 3.0.0 рекомендуется создать резервную копию настроек `Apache` (см. раздел **Устранение проблем с авторизацией после обновления до версии 3.0.0 Известные проблемы Руководство администратора. Часть 2**).

---

### 3.1.1. Подготовка к обновлению

Версия ОС должна совпадать на контроллерах домена, между которыми настроена репликация. Если требуется установка оперативного обновления ОС, она должна выполняться перед обновлением **ALD Pro**. На первом контроллере домена необходимо выполнить следующие действия:

1. убедиться, что в качестве источников пакетов для ОС зарегистрированы основной репозиторий (`main`) и репозиторий с обновлениями основного репозитория (`repository-update`), а в файле `/etc/apt/sources.list` указаны следующие строки, при необходимости — добавить, если имеются другие записи, то закомментировать их или удалить:

```
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/<номер_обновления_ОС>
 ↪/repository-main 1.7_x86-64 main non-free contrib
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/<номер_обновления_ОС>
 ↪/repository-update 1.7_x86-64 main non-free contrib
```

2. обновить пакеты ОС, выполнив в терминале команду:

```
sudo apt update && sudo apt install astra-update -y && sudo astra-update
 ↪-A -r -T
```

3. для корректной работы функций репликации на контроллере домена необходимо импортировать новые конфигурации службы каталога, выполнив в терминале команды:

```
sudo ipa-server-upgrade
sudo ipactl restart
```

#### 3.1.1.1. Проверки, которые необходимо выполнить до начала обновления

Начиная с версии 3.0.0, утилита `aldpro-server-install` была доработана и дополнена механизмом автоматической валидации системных параметров и вводимых значений.

Перед установкой и обновлением контроллера домена утилита выполняет набор предварительных проверок, чтобы убедиться, что система соответствует установленным требованиям. По умолчанию валидация отключена и должна быть активирована с помощью флага `--validate`.

---

**Важно:** В версии 3.0.0 был введен механизм валидации параметров для утилиты `aldpro-server-install`.

При обновлении первого КД с помощью утилиты `aldpro-server-install` с ключем `--validate`, пункты 2, 6, 9, 10 из списка проверок ниже, выполняются автоматически. Обновление резервных КД выполняется через портал управления, поэтому необходимо выполнить все проверки.

Подробное описание механизма валидации параметров см. в **Руководство администратора. Часть 2 → Инструкция по валидации параметров установки/обновления ALD Pro** .

---

Перед запуском обновления Системы на контроллерах домена необходимо выполнить следующие проверки:

1. Перезапуск служб **IPA**. Нужно убедиться, что не происходит задержек при перезапуске **FreeIPA** служб и что все службы стартуют успешно. Выполняется на первом КД и на резервных КД:

```
ipactl restart
```

2. Проверка работоспособности основных служб `krb5-kdc`, `dirsrv@DC-1-ALDPRO-LAN.service`, `bind9-pkcs11`, `aldpro-salt-minion`, `sssd`. Название службы dirsrv@DC-1-ALDPRO-LAN.service состоит из имени контроллера домена в первой части и имени домена во второй. Нельзя начинать обновление, если какие-то из служб не функционируют. Выполняется на первом КД и резервных КД:

```
systemctl status krb5-kdc dirsrv@DC-1-ALDPRO-LAN.service bind9-pkcs11 salt-
 ↪minion-standalone sssd
kinit admin
nslookup имя_хоста
```

3. Отключение служб, связанных с ролями: `celerybeat` и `aldpro-roles-sweeper`. Отключение производится на контроллере домена путем остановки таймеров для соответствующих служб:

```
systemctl disable --now celerybeat.service aldpro-roles-sweeper.timer
```

4. Проверка подключенных репозиториев, отключение лишних репозиториев. Необходимо убедиться, что при доступе к репозиториям не происходит ошибок и задержек. Выполняется на первом КД и резервных КД:

```
Редактирование *.list файлов в каталоге /etc/apt/ и его подкаталогах
apt update
```

5. Отключение плагина `389ds - compat`. Позволяет ускорить выполнение обновления. Выполняется на первом КД и резервных КД:

```
ipa-compat-manage status
ipa-compat-manage disable
```

6. Деактивация `winbind_krb5_locator`. Выполняется на резервных КД:

```
ln -s -f /dev/null /usr/lib/x86_64-linux-gnu/krb5/plugins/libkrb5/winbind_
↪krb5_locator.so
```

7. Отсутствие двух подсистем на одном хосте. Выполняется перед началом обновления первого КД.

8. Обновление модуля синхронизации не запущено одновременно с обновлением Системы. Обновление модуля синхронизации и миграцию его баз данных рекомендуется проводить после обновления всех резервных КД.

9. Проверка репликации и отсутствия односторонних соглашений о репликации:

```
dsconf ldap://<имя_КД> -D 'cn=Directory Manager' repl-conflict list dc=ald,
↪dc=company,dc=lan
dsconf ldap://<имя_КД> -D 'cn=Directory Manager' repl-agmt list --suffix
↪dc=ald,dc=company,dc=lan
ds-replcheck online -D "cn=Directory Manager" -W -m ldap://<имя_КД_1> -r
↪ldap://<имя_КД_2> -b "<dc=доменный,dc=суффикс>" # <имя_КД_1> и <имя_КД_2> -
↪ это контроллеры домена, между которыми установлены соглашения о репликации
```

10. Проверка наличия атрибутов `envvar` и `ipaLocation`. Выполняется на первом КД и резервных КД:

```
ldapsearch -b "cn=masters,cn=ipa,cn=etc,dc=aldpro,dc=company,dc=lan" -s one
↪ipaLocation envvar
```

11. Перезагрузка КД с последующей экспресс-проверкой работы служб (повторить пункты 1 и 2 данного раздела). Выполняется непосредственно перед началом обновления первого КД или резервных КД.

### 3.1.2. Обновление

Для установки обновления **ALD Pro** на первом контроллере домена необходимо подключить репозиторий **aldpro**, выполнив в терминале команды:

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

Полностью заменить содержимое файла `aldpro.list`:

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

Обновить индекс пакетов, выполнив в терминале команду:

```
sudo apt update
```

Обновить пакеты продукта **ALD Pro** командой:

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

В процессе выполнения обновления, при появлении сообщения с подтверждением изменения файла настройки пакета, необходимо выбрать **Установить версию, предлагаемую сопровождающим пакета**, введя в командной строке **Y**.

Перезагрузить контроллер, выполнив в терминале команду:

```
sudo reboot
```

После перезагрузки первого контроллера домена и проверки статуса прохождения аутентификации, для завершения обновления первого контроллера домена в терминале выполнить команды:

```
sudo aldpro-server-install -d ald.company.lan -n dc-1 --ip 10.0.1.11 --
↪update --setup_syncer --setup_gc
```

где:

- `-d` (domain) — имя домена;
- `-n` (name) — имя сервера;
- `-p` (password) — получить пароль администратора домена из командной строки (небезопасно);
- `--ip` — ip адрес контроллера домена. Адрес требуется указывать явно, если на контроллере домена активно несколько сетевых интерфейсов;
- `--update` — ключ запуска процесса обновления;
- `--setup_gc` — ключ указывает, что нужно настроить установленный ранее модуль глобального каталога;
- `--setup_syncer` — ключ указывает, что нужно настроить установленный ранее модуль синхронизации.

Описание параметров скрипта можно получить с помощью ключа `-h`.

После ввода команды система запросит ввести пароль администратора домена. При обновлении контроллера домена ALD Pro до версии 3.0.0, с ранее установленным модулем синхронизации, процесс миграции базы данных (БД) может занять продолжительное время. Если БД содержит 30000 пользователей и более, то рекомендуется сначала обновить ALD Pro, затем, выбрав отдельный интервал профилактики, обновить модуль синхронизации, согласно *Обновление с установкой Модуля Синхронизации*.

Если требуется произвести обновление ALD Pro с одновременной инициализацией ранее неустановленного модуля глобального каталога и/или модуля синхронизации, то следует обратиться к соответствующим разделам *Обновление с установкой Глобального Каталога* и *Обновление с установкой Модуля Синхронизации*.

Ошибки, которые могут возникнуть при обновлении системы, описаны в разделе **Известные проблемы Руководство администратора. Часть 2**.

#### 3.1.2.1. Проверки, которые необходимо выполнить после обновления

После завершения обновления системы необходимо выполнить следующие проверки, чтобы убедиться, что обновление выполнено корректно и **ALD Pro** готов к работе.

1. Проверить информацию на карточке КД (**Управление доменом** → **Сайты и службы** → **Контроллеры домена** или **Управление доменом**→ ****Общая информация** → **Состав системы**). Если КД находится в состоянии **Установлено**, **Ошибка**, не указана версия, то изучить логи (**первый КД - /var/log/ipaupgrade.log, резервные контроллеры домена - /var/log/aldpro-salt/subsystem.log**).

2. Проверить функционирование основных служб `dirsrv@DC-1-ALDPRO-LAN.service, krb5-kdc, bind9-pkcs11, sssd, aldpro-salt-minion`. Название службы `dirsrv@DC-1-ALDPRO-LAN.servie` состоит из имени контроллера домена в первой части и имени домена во второй.

```
systemctl status dirsrv@DC-1-ALDPRO-LAN.service krb5-kdc bind9-pkcs11 sssd
↪aldpro-salt-minion
ipactl status
aldproctl status
```

3. Остановить и замаскировать службу `salt-minion`, если она не используется для других задач:

```
systemctl stop salt-minion
systemctl disable salt-minion
systemctl mask salt-minion
```

4. Проверить наличие конфликтов репликации **LDAP**:

```
dsconf ldap://<имя_КД> -D 'cn=Directory Manager' repl-conflict list
↪<доменный суффикс>
```

5. Проверить работоспособность ролевой модели. Проверка осуществляется в портале управления путем просмотра списка ролей и их статуса, назначения роли или ролей пользователю с последующей проверкой доступа к разделам портала. Наличие конфликтов у записей в **LDAP**, имеющих отношение к ролям, привилегиям или разрешениям, также сигнализирует о возможных ошибках в функционировании ролевой модели. Если на первом КД ролевая модель работает, то на резервных контроллерах домена проверку можно осуществлять сравнением данных этого

резервного контроллера домена с первым КД (`ds-replcheck`).

6. Обновить модуль синхронизации и проверить миграцию данных (идентификаторы участников групп (должны быть `ObjectGUID` из **MS AD**), список ошибок до обновления и миграции и после) – выполняется только на первом КД, т.к. модуль синхронизации может быть установлен только на него:

```
sudo -u postgres psql -d syncer -c "SELECT schema_tracer.tracer_objects.name,
↪schema_provider.ipa_code_error.error_message, schema_provider.ipa_code_
↪error.error_name, schema_provider.virtual_tree.error_id, COUNT(*) FROM
↪schema_provider.virtual_tree JOIN schema_provider.ipa_code_error ON schema_
↪provider.virtual_tree.error_id =  schema_provider.ipa_code_error.id JOIN
↪schema_tracer.tracer_objects ON schema_provider.virtual_tree.object_class_
↪id = schema_tracer.tracer_objects.id WHERE error_id <> 90  GROUP BY schema_
↪tracer.tracer_objects.id,schema_provider.ipa_code_error.error_message,
↪schema_provider.ipa_code_error.error_name, schema_provider.virtual_tree.
↪error_id ORDER BY schema_tracer.tracer_objects.name;"
```

### 3.1.3. Обновление с установкой Глобального Каталога

При необходимости инициализации модуля глобального каталога одновременно с обновлением **ALD Pro** на первом контроллере домена, необходимо предварительно установить пакет глобального каталога из репозитория **ALD Pro** и добавить ключ `--setup_gc` в команду обновления `aldpro-server-install`.

Команда обновления контроллера домена с инициализацией модуля глобального каталога:

```
sudo apt update && sudo apt install aldpro-gc
sudo aldpro-server-install -d ald.company.lan -n dc-1 --ip 10.0.1.11 --
↪update --setup_gc
```

После ввода команды система запросит ввести пароль администратора домена.

### 3.1.4. Обновление с установкой Модуля Синхронизации

При необходимости инициализации модуля синхронизации одновременно с обновлением **ALD Pro** на первом контроллере домена, необходимо предварительно установить пакет модуля синхронизации из репозитория **ALD Pro** и добавить ключ `--setup_syncer` в команду обновления `aldpro-server-install`.

Модуль синхронизации всегда устанавливается на первый контроллер домена. При установке модуля синхронизации контроллер домена **ALD Pro** добавляется в карточку **Контроллеры домена ALD** автоматически.

При установке модуля синхронизации создается учетная запись имеющая вид `syncer/dc01.<имя домена>@<ИМЯ ДОМЕНА>`. Данная учетная запись является сервисной и используется для работы модуля синхронизации. Пароль данной учетной записи является бессрочным, что делает работу модуля синхронизации более стабильной и устойчивой.

Команда обновления контроллера домена с инициализацией модуля синхронизации:

```
.. code-block:: bash
```

sudo apt update && sudo apt install aldpro-syncer sudo aldpro-server-install -d ald.company.lan -n dc-1 –ip 10.0.1.11 –update –setup_syncer

После ввода команды система запросит ввести пароль администратора домена.

## 3.2. Обновление клиентов домена

В системе с версии 2.2.0 внедрен функционал централизованного обновления **aldpro-client** на компьютерах домена через **Портал Управления**. Подробную инструкцию см. в **Руководство администратора. Часть 2 → Полезные инструкции → Обновление подсистем ALD Pro через портал управления**.

### 3.2.1. Подготовка к обновлению

Убедиться, что в качестве источников пакетов для ОС зарегистрированы основной репозиторий (`main`) и репозиторий с обновлениями основного репозитория (`repository-update`), а в файле `/etc/apt/sources.list` указаны следующие строки, при необходимости — добавить, если имеются другие записи, то закомментировать их или удалить:

```
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/<номер_
↪обновления_ОС>/repository-main 1.7_x86-64 main non-free contrib
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/<номер_
↪обновления_ОС>/repository-update 1.7_x86-64 main non-free contrib
```

Обновить пакеты ОС, выполнив в терминале команду:

```
sudo apt update && sudo apt install astra-update -y && sudo astra-
↪update -A -r -T
```

### 3.2.2. Обновление

Подключить репозиторий **aldpro**, выполнив в терминале команды:

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

Полностью заменить содержимое файла `aldpro.list`:

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

Обновить индекс пакетов, выполнив команду:

```
sudo apt update
```

Обновить пакеты **ALD Pro**, выполнив в терминале команду:

```
sudo apt dist-upgrade -y -o Dpkg::Options::="--force-confnew"
```

Запустить обновление клиентской части **ALD Pro**, выполнив в терминале команду:

```
sudo aldpro-gpupdate --pm
```

## 3.3. Обновление репликаций контроллера домена

### 3.3.1. Подготовка к обновлению

#### 3.3.1.1. Проверки, которые необходимо выполнить до начала обновления

Убедиться, что в качестве источников пакетов для ОС зарегистрированы основной репозиторий (`main`) и репозиторий с обновлениями основного репозитория (`repository-update`), а в файле `/etc/apt/sources.list` указаны следующие строки, при необходимости — добавить, если имеются другие записи, то закомментировать их или удалить:

```
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/<номер_
↪обновления_ОС_СН>/repository-main 1.7_x86-64 main non-free contrib
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/<номер_
↪обновления_ОС_СН>/repository-update 1.7_x86-64 main non-free
↪contrib
```

**Внимание:** Перед обновлением ОС на серверах подсистемы сетевого репозитория необходимо убедиться, что пакет `dpkg-dev` установлен из репозиториев **ALD Pro**:

```
apt-cache policy dpkg-dev
```

Пример результата выполнения команды:

```
dpkg-dev:
    Установлен: 1.19.8
    Кандидат: 1.19.8
    Таблица версий:
        1.19.8 900
            900 https://dl.astralinux.ru/aldpro/frozen/01/2.5.0 1.7_x86-
↪64/base amd64 Packages
            100 /var/lib/dpkg/status
```

Если установлена другая версия, то необходимо выполнить команду:

```
apt install dpkg-dev=<версия в составе ALD Pro>
```

Пример:

```
apt install dpkg-dev=1.19.8
```

dpkg-dev является обязательной зависимостью aldpro-sr. При этом dpkg-dev присутствует только в **base** репозитории **ALSE**. Если установка или обновление производились на этот репозиторий, то dpkg-dev будет установлен из состава **base**. Если для очередного обновления будет заменен **base** репозиторий на **main + update**, в таком случае обновятся пакеты dpkg, а dpkg-dev будет удален (что повлечёт за собой удаление aldpro-sr), так как у него в зависимостях указана конкретная версия библиотеки libdpkg-perl.

Обновить пакеты ОС, выполнив в терминале команду:

```
sudo apt update && sudo apt install astra-update -y && sudo astra-
↪update -A -r -T
```

**Внимание:** После завершения команды по обновлению пакетов ОС на сервере подсистемы **Мониторинг** необходимо осуществить перезагрузку службы zabbix-server, выполнив в терминале команду:

```
systemctl restart zabbix-server
```

Если выполняется обновление резервного контроллера домена, для корректной работы функций репликации необходимо импортировать новые конфигурации службы каталога, выполнив команды:

```
sudo ipa-server-upgrade
sudo ipactl restart
```

и выполнить проверки из *Проверки, которые необходимо выполнить до начала обновления*.

### 3.3.2. Обновление

В системе с версии 2.2.0 внедрен функционал централизованного обновления **aldpro-client** на компьютерах домена через **Портал Управления**. Подробную инструкцию см. в **Руководство администратора. Часть 2 → Полезные инструкции → Обновление подсистем ALD Pro через портал управления**.

Подключить обновленный репозиторий **ALD Pro**:

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

Полностью заменить содержимое файла `aldpro.list`:

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

Обновить индекс пакетов, выполнив в терминале команду:

```
sudo apt update
```

Обновить пакеты продукта **ALD Pro** командой:

```
sudo apt dist-upgrade -y -o Dpkg::Options::=--force-confnew
sudo aldpro-gpupdate --pm
```

В процессе выполнения обновления, при появлении сообщения с подтверждением изменения файла настройки пакета, необходимо выбрать **Установить версию, предлагаемую сопровождающим пакета**, введя в командной строке **Y**.

Перезагрузить контроллер, выполнив в терминале команду:

```
sudo reboot
```

На портале управления **ALD Pro** первого контроллера домена, в карточке обновляемого сервера нажать **Обновить ALD Pro**. Выбор карточки резервного контроллера домена осуществляется в разделе **Управление доменом → Сайты и службы → Контроллеры домена**.

---

**Примечание:** Запуск команд по обновлению резервного контроллера домена осуществляется по таймеру. Для лучшего контроля за процессом обновления резервного контроллера домена рекомендуется использовать форсированное

обновление на сервере резервного контроллера домена:

```
sudo aldpro-roles --iud
```

---

После обновления системы на портале управления первого контроллера домена необходимо перейти в карточку обновляемого сервера и убедиться, что состояние подсистемы имеет статус **Обновлена**, без ошибок. Поле **Версия системы ALD Pro** должно содержать версию системы, до которой было выполнено обновление.

После завершения обновления резервных контроллеров домена необходимо выполнить проверки из *Проверки, которые необходимо выполнить после обновления*.

## 3.4. Обновление подсистем

### 3.4.1. Обновление подсистемы сетевого репозитория

В системе с версии 2.2.0 внедрен функционал централизованного обновления **aldpro-client** на компьютерах домена через **Портал Управления**. Подробную инструкцию см. в **Руководство администратора. Часть 2 → Полезные инструкции → Обновление подсистем ALD Pro через портал управления**.

Подключить обновленный репозиторий **ALD Pro**:

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

Полностью заменить содержимое файла `aldpro.list`:

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

Обновить индекс пакетов, выполнив в терминале команду:

```
sudo apt update
```

Обновить пакеты продукта **ALD Pro** командой:

```
sudo apt dist-upgrade -y -o Dpkg::Options::=--force-confnew
sudo aldpro-gpupdate --pm
```

В процессе выполнения обновления, при появлении сообщения с подтверждением изменения файла настройки пакета, необходимо выбрать **Установить версию, предлагаемую сопровождающим пакета**, введя в командной строке **Y**.

Перезагрузить контроллер, выполнив в терминале команду:

```
sudo reboot
```

Выбор карточки сервера подсистем осуществляется в соответствующем разделе: подсистема **Репозиторий ПО**: **Установка и обновление ПО** → **Репозитории ПО** → **Серверы репозиториев ПО**.

---

**Примечание:** Запуск команд по обновлению подсистемы сетевого репозитория осуществляется по таймеру. Для лучшего контроля за процессом обновления рекомендуется использовать форсированное обновление на сервере подсистемы сетевого репозитория:

```
sudo aldpro-roles --iud
```

---

После обновления системы на портале управления первого контроллера домена необходимо перейти в карточку обновляемого сервера и убедиться, что состояние подсистемы имеет статус **Обновлена**, без ошибок. Поле **Версия системы ALD Pro** должно содержать версию системы, до которой было выполнено обновление.

После завершение обновления резервных контроллеров домена необходимо выполнить проверки из *Проверки, которые необходимо выполнить после обновления*.

### 3.4.2. Обновление подсистемы общего доступа к файлам

В системе с версии 2.2.0 внедрен функционал централизованного обновления **aldpro-client** на компьютерах домена через **Портал Управления**. Подробную инструкцию см. в **Руководство администратора. Часть 2** → **Полезные инструкции** → **Обновление подсистем ALD Pro через портал управления**.

Подключить обновленный репозиторий **ALD Pro**:

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

Полностью заменить содержимое файла `aldpro.list`:

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

Обновить индекс пакетов, выполнив в терминале команду:

```
sudo apt update
```

Обновить пакеты продукта **ALD Pro** командой:

```
sudo apt dist-upgrade -y -o Dpkg::Options::=--force-confnew
sudo aldpro-gpupdate --pm
```

В процессе выполнения обновления, при появлении сообщения с подтверждением изменения файла настройки пакета, необходимо выбрать **Установить версию, предлагаемую сопровождающим пакета**, введя в командной строке **Y**.

Перезагрузить контроллер, выполнив в терминале команду:

```
sudo reboot
```

Выбор карточки сервера подсистем осуществляется в соответствующем разделе: подсистема **Общий доступ к сетевым дискам**: **Роли и службы сайта → Общий доступ к файлам → Перечень серверов**.

---

**Примечание:** Запуск команд по обновлению подсистемы общего доступа к файлам осуществляется по таймеру. Для лучшего контроля за процессом обновления рекомендуется использовать форсированное обновление на сервере подсистемы общего доступа к файлам:

```
sudo aldpro-roles --iud
```

---

После обновления системы на портале управления первого контроллера домена необходимо перейти в карточку обновляемого сервера и убедиться, что состояние подсистемы имеет статус **Обновлена**, без ошибок. Поле **Версия системы ALD Pro** должно содержать версию системы, до которой было выполнено обновление.

После завершение обновления резервных контроллеров домена необходимо выполнить проверки из *Проверки, которые необходимо выполнить после обновления*.

### 3.4.3. Обновление подсистемы сервера печати

В системе с версии 2.2.0 внедрен функционал централизованного обновления **aldpro-client** на компьютерах домена через **Портал Управления**. Подробную инструкцию см. в **Руководство администратора. Часть 2 → Полезные инструкции → Обновление подсистем ALD Pro через портал управления**.

Подключить обновленный репозиторий **ALD Pro**:

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

Полностью заменить содержимое файла `aldpro.list`:

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

Обновить индекс пакетов, выполнив в терминале команду:

```
sudo apt update
```

Обновить пакеты продукта **ALD Pro** командой:

```
sudo apt dist-upgrade -y -o Dpkg::Options::=--force-confnew
sudo aldpro-gpupdate --pm
```

В процессе выполнения обновления, при появлении сообщения с подтверждением изменения файла настройки пакета, необходимо выбрать **Установить версию, предлагаемую сопровождающим пакета**, введя в командной строке **Y**.

Перезагрузить контроллер, выполнив в терминале команду:

```
sudo reboot
```

Выбор карточки сервера подсистем осуществляется в соответствующем разделе: подсистема **Печать**: **Роли и службы сайта → Служба печати → Серверы печати**.

---

**Примечание:** Запуск команд по обновлению подсистемы сервера печати осуществляется по таймеру. Для лучшего контроля за процессом обновления рекомендуется использовать форсированное обновление на сервере подсистемы сервера печати:

```
sudo aldpro-roles --iud
```

---

После обновления системы на портале управления первого контроллера домена необходимо перейти в карточку обновляемого сервера и убедиться, что состояние подсистемы имеет статус **Обновлена**, без ошибок. Поле **Версия системы ALD Pro** должно содержать версию системы, до которой было выполнено обновление.

После завершение обновления резервных контроллеров домена необходимо выполнить проверки из *Проверки, которые необходимо выполнить после обновления*.

### 3.4.4. Обновление подсистемы «Динамическая настройка узла» DHCP

В системе с версии 2.2.0 внедрен функционал централизованного обновления **aldpro-client** на компьютерах домена через **Портал Управления**. Подробную инструкцию см. в **Руководство администратора. Часть 2 → Полезные инструкции → Обновление подсистем ALD Pro через портал управления**.

Подключить обновленный репозиторий **ALD Pro**:

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

Полностью заменить содержимое файла `aldpro.list`:

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

Обновить индекс пакетов, выполнив в терминале команду:

```
sudo apt update
```

Обновить пакеты продукта **ALD Pro** командой:

```
sudo apt dist-upgrade -y -o Dpkg::Options::=--force-confnew
sudo aldpro-gpupdate --pm
```

В процессе выполнения обновления, при появлении сообщения с подтверждением изменения файла настройки пакета, необходимо выбрать **Установить версию, предлагаемую сопровождающим пакета**, введя в командной строке **Y**.

Перезагрузить контроллер, выполнив в терминале команду:

```
sudo reboot
```

Выбор карточки сервера подсистем осуществляется в соответствующем разделе: подсистема **Динамическая настройка узла**: **Роли и службы сайта → Служба динамической настройки узла → Перечень серверов** .

---

**Примечание:** Запуск команд по обновлению подсистемы «Динамическая настройка узла» DHCP осуществляется по таймеру. Для лучшего контроля за процессом обновления рекомендуется использовать форсированное обновление на сервере подсистемы «Динамическая настройка узла» DHCP:

```
sudo aldpro-roles --iud
```

---

После обновления системы на портале управления первого контроллера домена необходимо перейти в карточку обновляемого сервера и убедиться, что состояние подсистемы имеет статус **Обновлена**, без ошибок. Поле **Версия системы ALD Pro** должно содержать версию системы, до которой было выполнено обновление.

После завершение обновления резервных контроллеров домена необходимо выполнить проверки из *Проверки, которые необходимо выполнить после обновления*.

### 3.4.5. Обновление подсистемы «Установка ОС по сети» TFTP + PXE

В системе с версии 2.2.0 внедрен функционал централизованного обновления **aldpro-client** на компьютерах домена через **Портал Управления**. Подробную инструкцию см. в **Руководство администратора. Часть 2 → Полезные инструкции → Обновление подсистем ALD Pro через портал управления**.

Подключить обновленный репозиторий **ALD Pro**:

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

Полностью заменить содержимое файла `aldpro.list`:

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

Обновить индекс пакетов, выполнив в терминале команду:

```
sudo apt update
```

Обновить пакеты продукта **ALD Pro** командой:

```
sudo apt dist-upgrade -y -o Dpkg::Options::=--force-confnew
sudo aldpro-gpupdate --pm
```

В процессе выполнения обновления, при появлении сообщения с подтверждением изменения файла настройки пакета, необходимо выбрать **Установить версию, предлагаемую сопровождающим пакета**, введя в командной строке **Y**.

Перезагрузить контроллер, выполнив в терминале команду:

```
sudo reboot
```

Выбор карточки сервера подсистем осуществляется в соответствующем разделе: подсистема **Установка ОС по сети**: **Автоматизация → Установка ОС по сети → Серверы установки ОС**.

---

**Примечание:** Запуск команд по обновлению подсистемы «Установка ОС по сети» TFTP + PXE осуществляется по таймеру. Для лучшего контроля за процессом обновления рекомендуется использовать форсированное обновление на сервере подсистемы «Установка ОС по сети» TFTP + PXE:

```
sudo aldpro-roles --iud
```

---

После обновления системы на портале управления первого контроллера домена необходимо перейти в карточку обновляемого сервера и убедиться, что состояние подсистемы имеет статус **Обновлена**, без ошибок. Поле **Версия системы ALD Pro** должно содержать версию системы, до которой было выполнено обновление.

После завершение обновления резервных контроллеров домена необходимо выполнить проверки из *Проверки, которые необходимо выполнить после обновления*.

## 3.4.6. Обновление подсистемы мониторинга

### 3.4.6.1. Обновление службы мониторинга Zabbix

---

**Примечание:** Обновление **Zabbix** необходимо выполнить только на серверах с развернутой подсистемой **Мониторинг**.

---

Для обновления **Zabbix** с 5.0.7 до 6.0.7 следует создать резервные копии конфигурационных файлов **Zabbix**, последовательно выполнив команды:

```
mkdir /opt/zabbix-backup/
cp /etc/zabbix/zabbix_server.conf /opt/zabbix-backup/
cp /etc/apache2/conf-enabled/zabbix-frontend-php.conf /opt/zabbix-backup/
cp -R /usr/share/zabbix/ /opt/zabbix-backup/
cp -R /usr/share/zabbix-* /opt/zabbix-backup/
```

Установить обновленные пакеты **Zabbix**:

```
sudo apt install --only-upgrade zabbix-server-pgsql zabbix-frontend-php
 ↪zabbix-agent
```

Для обновления базы данных **Zabbix** следует остановить службу севера командой:

```
sudo systemctl stop zabbix-server
```

В конфигурационный файл `/etc/zabbix/zabbix_server.conf` добавить параметр

```
AllowUnsupportedDBVersions=1;
```

Если требуется сохранить текущие таблицы с историей, то переименовать их, выполнив команду:

```
zcat /usr/share/zabbix-server-pgsql/history_pk_prepare.sql.gz | psql -h
 ↪localhost zabbix
```

Проверить в `/etc/zabbix/zabbix_server.conf` логин и пароль для подключения к базе данных **Zabbix** (параметры **DBUser** и **DBPassword**);

Запустить службу сервера **Zabbix** командой:

```
sudo systemctl start zabbix-server
```

Будет выполнено обновление базы данных **Zabbix**. Проверить статус обновления возможно командой:

```
sudo cat /var/log/zabbix-server/zabbix_server.log | grep database
```

Пример вывода команды:

```
82263:20230627:235018.484 current database version
(mandatory/optional):
05000000/05000002
82263:20230627:235018.484 starting automatic database upgrade
82263:20230627:235018.487 completed 0% of database upgrade
...
82263:20230627:235023.532 completed 97% of database upgrade
82263:20230627:235023.535 completed 98% of database upgrade
82263:20230627:235023.537 completed 99% of database upgrade
82263:20230627:235023.542 completed 100% of database upgrade
82263:20230627:235023.542 database upgrade fully completed
```

Для восстановления таблиц с историей мониторинга сначала следует остановить службу севера **Zabbix**:

```
sudo systemctl stop zabbix-server
```

Подключиться к серверу **PostgreSQL**:

```
psql -U zabbix -h localhost
```

Перезаписать историю из сохраненных таблиц в новые таблицы, выполнив запросы:

```
INSERT INTO history SELECT * FROM history_old ON CONFLICT
(itemid,clock,ns) DO NOTHING;
INSERT INTO history_uint SELECT * FROM history_uint_old ON CONFLICT
(itemid,clock,ns) DO NOTHING;
INSERT INTO history_str SELECT * FROM history_str_old ON CONFLICT
(itemid,clock,ns) DO NOTHING;
INSERT INTO history_log SELECT * FROM history_log_old ON CONFLICT
(itemid,clock,ns) DO NOTHING;
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
INSERT INTO history_text SELECT * FROM history_text_old ON CONFLICT
(itemid,clock,ns) DO NOTHING;
```

Удалить переименованные таблицы, выполнив запросы:

```
DROP TABLE history_old;
DROP TABLE history_uint_old;
DROP TABLE history_str_old;
DROP TABLE history_log_old;
DROP TABLE history_text_old;
```

Запустить службу сервера **Zabbix**:

```
sudo systemctl start zabbix-server
```

### 3.4.7. Обновление подсистемы журналирования

В системе с версии 2.2.0 внедрен функционал централизованного обновления **aldpro-client** на компьютерах домена через **Портал Управления**. Подробную инструкцию см. в **Руководство администратора. Часть 2 → Полезные инструкции → Обновление подсистем ALD Pro через портал управления**.

Подключить обновленный репозиторий **ALD Pro**:

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

Полностью заменить содержимое файла `aldpro.list`:

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

Обновить индекс пакетов, выполнив в терминале команду:

```
sudo apt update
```

Обновить пакеты продукта **ALD Pro** командой:

```
sudo apt dist-upgrade -y -o Dpkg::Options::=--force-confnew
sudo aldpro-gpupdate --pm
```

В процессе выполнения обновления, при появлении сообщения с подтверждением изменения файла настройки пакета, необходимо выбрать **Установить версию, предлагаемую сопровождающим пакета**, введя в командной строке **Y**.

Перезагрузить контроллер, выполнив в терминале команду:

```
sudo reboot
```

Выбор карточки сервера подсистем осуществляется в соответствующем разделе: подсистема **Журналирование событий**: **Журнал событий → Серверы журнала событий**.

---

**Примечание:** Запуск команд по обновлению подсистемы журналирования осуществляется по таймеру. Для лучшего контроля за процессом обновления рекомендуется использовать форсированное обновление на сервере подсистемы журналирования:

```
sudo aldpro-roles --iud
```

---

После обновления системы на портале управления первого контроллера домена необходимо перейти в карточку обновляемого сервера и убедиться, что состояние подсистемы имеет статус **Обновлена**, без ошибок. Поле **Версия системы ALD Pro** должно содержать версию системы, до которой было выполнено обновление.

После завершение обновления резервных контроллеров домена необходимо выполнить проверки из *Проверки, которые необходимо выполнить после обновления*.

## 3.5. Централизованное обновление менеджера политик программного обеспечения

Начиная с версии **ALD Pro** 2.4.0 внедрена возможность централизованного автообновления менеджера политик (**Policy Manager**) на клиентских компьютерах без участия администратора. Таким образом, процесс управления обновлениями и поддержание актуальности **ALD Pro** стали гораздо проще.

Менеджер политик отвечает за работу и применение групповых политик, политик программного обеспечения, правил сбора событий, развертывание подсистем, установку резервных контроллеров домена, заданий автоматизации.

Для корректной работы рекомендуется обновить все клиентские компьютеры до 2.5.0. При обновлении **ALD Pro** до 2.5.0 на компьютерах появится задание, которое централизованно обновляет менеджер политик.

В дальнейшем при обновлении **ALD Pro** на контроллере домена до последней версии, менеджер политик будет самостоятельно централизовано обновляться на клиентах, если в новой версии **ALD Pro** в него были внесены изменения.

Данные изменения гарантируют использование последней актуальной версии **ALD Pro** на доменных компьютерах без участия администраторов.

Актуальная версия менеджера политик обновляется на первом контроллере домена вместе с обновлением **ALD Pro**.

На остальных контроллерах домена информация об актуальной версии и содержание **Policy Manager** обновляется при репликации.

На всех клиентских компьютерах домена выполняется задание, которое гарантировано проверяет наличие обновления каждые 80 минут. Пакет менеджера политик обновляется при наличии изменений.

Если на отдельной клиентской машине нужно обновить **Policy Manager** вне расписания, необходимо использовать команду:

```
sudo aldpro-gpupdate --pm
```

или

```
sudo aldpro-gpupdate --policy-manager
```

# Матрицы совместимости и обновлений

## 4.1. Матрица совместимости ПК ALD Pro

В данной статье представлена матрица совместимости ПК ALD Pro с ОС Astra Linux и другим ПО.

Информация в таблице сформирована командой разработки ALD Pro. Тестирование с другими продуктами (не отмеченными в таблице, в том числе - с другими версиями ALSE) может быть осуществлено и подтверждено другими продуктовыми командами.

* - Совместимость с ACM. Установка ACM на серверную группировку ALD Pro не поддерживается и не допускается. Совместимость ALD Pro и ACM предполагает возможность использования двух продуктов в одной инфраструктуре заказчика. Дополнительные проверки отсутствия аффекта решений друг на друга связаны с тем, что ряд механизмов для пользовательских ПК в обоих решениях используют SaltStack.

---

**Важно:** Версия ОС Astra Linux должна совпадать на контроллере домена и подсистемах. Использования разных версий ОС может привести к возникновению проблемы или частичной неработоспособности системы.

Версия ОС Astra Linux на клиентах может не совпадать с версией на контроллере домена и подсистемах (дополнительная детализация - в таблице ниже).

---

| ALD Pro | ОС Astra Linux | Ядро ОС | Уровень защищенности ОС | Поддержка MS AD | Браузеры | Proxmox | VMware Workstation Pro | VirtualBox | RuPost | ACM* |
|---|---|---|---|---|---|---|---|---|---|---|
| **1.1.3** | **Серверная группа ALD Pro:** 1.7.1 **Клиенты ALD Pro:** 1.7.1 | **Серверная группа ALD Pro:** 5.15-generic **Клиенты ALD Pro:** 5.4-generic; 5.10-generic; 5.15-generic | **Серверная группа ALD Pro:** Смоленск **Клиенты ALD Pro:** Орел; Воронеж; Смоленск | Windows Server (2008 R2; 2012; 2012 R2; 2016; 2019) | Firefox 102.0 и выше Тестирование на других браузерах до 2.3.0 не осуществлялось | 7.2-7 | 16.2.3 | от 6.1 и выше | 1.0 | - |
| **1.2.0** | **Серверная группа ALD Pro:** 1.7.1; 1.7.2 **Клиенты ALD Pro:** 1.7.1; 1.7.2 | **Серверная группа ALD Pro:** 5.15-generic **Клиенты ALD Pro:** 5.4-generic; 5.10-generic; 5.15-generic | **Серверная группа ALD Pro:** Смоленск **Клиенты ALD Pro:** Орел; Воронеж; Смоленск; | Windows Server (2008 R2; 2012; 2012 R2; 2016; 2019) | Firefox 102.0 и выше Тестирование на других браузерах до 2.3.0 не осуществлялось | 7.2-7 | 16.2.3 | от 6.1 и выше | 1.0 | - |
| **1.2.1** | **Серверная группа ALD Pro:** 1.7.1; 1.7.2 **Клиенты ALD Pro:** 1.7.1; 1.7.2 | **Серверная группа ALD Pro:** 5.15-generic **Клиенты ALD Pro:** 5.4-generic; 5.10-generic; 5.15-generic | **Серверная группа ALD Pro:** Смоленск **Клиенты ALD Pro:** Орел; Воронеж; Смоленск | Windows Server (2008 R2; 2012; 2012 R2; 2016; 2019) | Firefox 102.0 и выше Тестирование на других браузерах до 2.3.0 не осуществлялось | 7.2-7 | 16.2.3 | от 6.1 и выше | 1.0 | - |
| **1.3.0** | **Серверная группа ALD Pro:** 1.7.1; 1.7.2; 1.7.3 **Клиенты ALD Pro:** 1.7.1; 1.7.2; 1.7.3 | **Серверная группа ALD Pro:** 5.15-generic **Клиенты ALD Pro:** 5.4-generic; 5.10-generic; 5.15-generic | **Серверная группа ALD Pro:** Смоленск **Клиенты ALD Pro:** Орел; Воронеж; Смоленск | Windows Server (2008 R2; 2012; 2012 R2; 2016; 2019) | Firefox 102.0 и выше Тестирование на других браузерах до 2.3.0 не осуществлялось | 7.2-7 | 16.2.3 | от 6.1 и выше | 1.0 | - |
| **1.4.0** | **Серверная группа ALD Pro:** 1.7.1 (только обновление с ALD Pro ранних версий); 1.7.2; 1.7.3 **Клиенты ALD Pro:** 1.7.1; 1.7.2; 1.7.3 | **Серверная группа ALD Pro:** 5.15-generic **Клиенты ALD Pro:** 5.4-generic; 5.10-generic; 5.15-generic | **Серверная группа ALD Pro:** Смоленск **Клиенты ALD Pro:** Орел; Воронеж; Смоленск | Windows Server (2008 R2; 2012; 2012 R2; 2016; 2019) | Firefox 102.0 и выше Тестирование на других браузерах до 2.3.0 не осуществлялось | 7.2-7 | 16.2.3 | от 6.1 и выше | 1.0 | - |
| **1.4.1** | **Серверная группа ALD Pro:** 1.7.1 (только обновление с ALD Pro ранних версий); 1.7.2; 1.7.3 **Клиенты ALD Pro:** 1.7.1; 1.7.2; 1.7.3 | **Серверная группа ALD Pro:** 5.15-generic **Клиенты ALD Pro:** 5.4-generic; 5.10-generic; 5.15-generic | **Серверная группа ALD Pro:** Смоленск **Клиенты ALD Pro:** Орел; Воронеж; Смоленск | Windows Server (2008 R2; 2012; 2012 R2; 2016; 2019) | Firefox 102.0 и выше Тестирование на других браузерах до 2.3.0 не осуществлялось | 7.2-7 | 16.2.3 | от 6.1 и выше | 1.0 | - |
| **2.0.0** | **Серверная группа ALD Pro:** 1.7.1 (только обновление с ALD Pro ранних версий); 1.7.2; 1.7.3; 1.7.4 **Клиенты ALD Pro:** 1.7.1; 1.7.2; 1.7.3; 1.7.4 | **Серверная группа ALD Pro:** 5.15-generic **Клиенты ALD Pro:** 5.4-generic; 5.10-generic; 5.15-generic | **Серверная группа ALD Pro:** Смоленск **Клиенты ALD Pro:** Орел; Воронеж; Смоленск | Windows Server (2008 R2; 2012; 2012 R2; 2016; 2019) | Firefox 102.0 и выше Тестирование на других браузерах до 2.3.0 не осуществлялось | 7.2-7 | 16.2.3 | от 6.1 и выше | 1.0 | - |
| **2.1.0** | **Серверная группа ALD Pro:** 1.7.1 (только обновление с ALD Pro ранних версий); 1.7.2; 1.7.3; 1.7.4 **Клиенты ALD Pro:** 1.7.1; 1.7.2; 1.7.3; 1.7.4 | **Серверная группа ALD Pro:** 5.15-generic **Клиенты ALD Pro:** 5.4-generic; 5.10-generic; 5.15-generic | **Серверная группа ALD Pro:** Смоленск **Клиенты ALD Pro:** Орел; Воронеж; Смоленск | Windows Server (2008 R2; 2012; 2012 R2; 2016; 2019) | Firefox 102.0 и выше Тестирование на других браузерах до 2.3.0 не осуществлялось | 7.2-7 | 16.2.3 | от 6.1 и выше | 1.0 | - |
| **2.2.0** | **Серверная группа ALD Pro:** 1.7.4 **Клиенты ALD Pro:** 1.7.1; 1.7.2; 1.7.3; 1.7.4 | **Серверная группа ALD Pro:** 5.15-generic **Клиенты ALD Pro:** 5.4-generic; 5.10-generic; 5.15-generic | **Серверная группа ALD Pro:** Смоленск **Клиенты ALD Pro:** Орел; Воронеж; Смоленск | Windows Server (2008 R2; 2012; 2012 R2; 2016; 2019) | Firefox 102.0 и выше Тестирование на других браузерах до 2.3.0 не осуществлялось | 7.2-7 | 16.2.3 | от 6.1 и выше | 1.0 | - |

продолжение на следующей странице

Таблица 4.1 – продолжение с предыдущей страницы

| ALD Pro | ОС Astra Linux | Ядро ОС | Уровень защищенности ОС | Поддержка MS AD | Браузеры | Proxmox | VMware Workstation Pro | VirtualBox | RuPost | ACM* |
|---|---|---|---|---|---|---|---|---|---|---|
| **2.2.1** | **Серверная группа ALD Pro:** 1.7.4 **Клиенты ALD Pro:** 1.7.1; 1.7.2; 1.7.3; 1.7.4 | **Серверная группа ALD Pro:** 5.15-generic **Клиенты ALD Pro:** 5.4-generic; 5.10-generic; 5.15-generic | **Серверная группа ALD Pro:** Смоленск **Клиенты ALD Pro:** Орел; Воронеж; Смоленск | Windows Server (2008 R2; 2012; 2012 R2; 2016; 2019) | Firefox 102.0 и выше Тестирование на других браузерах до 2.3.0 не осуществлялось | 7.2-7 | 16.2.3 | от 6.1 и выше | 1.0 | - |
| **2.3.0** | **Серверная группа ALD Pro:** 1.7.4; 1.7.5; 1.7.5 UU 1 **Клиенты ALD Pro:** 1.7.1; 1.7.2; 1.7.3; 1.7.4; 1.7.5; 1.7.5 UU 1; 1.8.1* | **Серверная группа ALD Pro:** 5.15.0-70-generic; 6.1.50-1-generic **Клиенты ALD Pro:** 5.4-generic; 5.10-generic; 5.15-generic | **Серверная группа ALD Pro:** Смоленск **Клиенты ALD Pro:** Орел; Воронеж; Смоленск | Windows Server (2008 R2; 2012; 2012 R2; 2016; 2019) | Firefox 102.0 и выше Google Chrome 121 и выше Chromium 111 и выше Chromium-gost 121 и выше Яндекс Браузер 23 и выше | 7.2-7 | 16.2.3 | от 6.1 и выше | 1.0 | 1.0.0 |
| **2.4.0** | **Серверная группа ALD Pro:** 1.7.5; 1.7.5 UU 1; 1.7.6; 1.7.6 UU 1; 1.7.6 UU 2 **Клиенты ALD Pro:** 1.7.1; 1.7.2; 1.7.3; 1.7.4; 1.7.5; 1.7.5 UU 1; 1.7.6; 1.7.6 UU 1; 1.7.6 UU 2; 1.8.1 | **Серверная группа ALD Pro:** 5.15-generic; 6.1-generic **Клиенты ALD Pro:** 5.4-generic; 5.10-generic; 5.15-generic; 6.1-generic | **Серверная группа ALD Pro:** Смоленск **Клиенты ALD Pro:** Орел; Воронеж; Смоленск | Windows Server (2008 R2; 2012; 2012 R2; 2016; 2019) | Firefox 102.0 и выше Google Chrome 121 и выше Chromium 111 и выше Chromium-gost 121 и выше Яндекс Браузер 23 и выше | 7.2-7 | 16.2.3 | от 6.1 и выше | 1.0 | 1.1.0 |
| **2.4.1** | **Серверная группа ALD Pro:** 1.7.5; 1.7.5 UU 1; 1.7.6; 1.7.6 UU 1; 1.7.6 UU 2 **Клиенты ALD Pro:** 1.7.1; 1.7.2; 1.7.3; 1.7.4; 1.7.5; 1.7.5 UU 1; 1.7.6; 1.7.6 UU 1; 1.7.6 UU 2; 1.8.1; 1.8.1 UU 1; | **Серверная группа ALD Pro:** 5.15-generic; 6.1-generic **Клиенты ALD Pro:** 5.4-generic; 5.10-generic; 5.15-generic; 6.1-generic | **Серверная группа ALD Pro:** Смоленск **Клиенты ALD Pro:** Орел; Воронеж; Смоленск | Windows Server (2008 R2; 2012; 2012 R2; 2016; 2019) | Firefox 102.0 и выше Google Chrome 121 и выше Chromium 111 и выше Chromium-gost 121 и выше Яндекс Браузер 23 и выше | 7.2-7 | 16.2.3 | от 6.1 и выше | 1.0 | 1.1.0 |
| **2.5.0** | **Серверная группа ALD Pro:** 1.7.6 UU 2 **Клиенты ALD Pro:** 1.7.3; 1.7.4; 1.7.5; 1.7.5 UU 1; 1.7.6; 1.7.6 UU 1; 1.7.6 UU 2; 1.7.7; 1.8.1; 1.8.1 UU 1; 1.8.1 UU 2 | **Серверная группа ALD Pro:** 5.15-generic; 6.1-generic **Клиенты ALD Pro:** 5.4-generic; 5.10-generic; 5.15-generic; 6.1-generic | **Серверная группа ALD Pro:** Смоленск **Клиенты ALD Pro:** Орел; Воронеж; Смоленск | Windows Server (2008 R2; 2012; 2012 R2; 2016; 2019) | Firefox 102.0 и выше Google Chrome 121 и выше Chromium 111 и выше Chromium-gost 121 и выше Яндекс Браузер 23 и выше | 7.2-7 | 16.2.3 | от 6.1 и выше | 1.0 | 1.1.0 1.2.0 |
| **3.0.0** | **Серверная группа ALD Pro:** 1.7.6 UU 2; 1.7.7.UU 2 **Клиенты ALD Pro:** 1.7.6; 1.7.6 UU 1; 1.7.6 UU 2; 1.7.7; 1.7.7.UU 1; 1.7.7.UU 2; 1.8.1; 1.8.1.UU 1; 1.8.1.UU 2; 1.8.2; 1.8.2.UU 1; 1.8.2.UU 2; 1.8.3 | **Серверная группа ALD Pro:** 5.15-generic; 6.1-generic **Клиенты ALD Pro:** 5.4-generic; 5.10-generic; 5.15-generic; 6.1-generic | **Серверная группа ALD Pro:** Смоленск **Клиенты ALD Pro:** Орел; Воронеж; Смоленск | Windows Server (2008 R2; 2012; 2012 R2; 2016; 2019) | Firefox 102.0 и выше Google Chrome 121 и выше Chromium 111 и выше Chromium-gost 121 и выше Яндекс Браузер 23 и выше | 7.2-7 | 16.2.3 | от 6.1 и выше | 1.0+ | 1.2.0 1.3.0 |

Таблица 12 — Несертифицированное исполнение ALD Pro (РДЦП.10101-01)

## 4.2. Матрица обновлений ПК ALD Pro

В матрице показана поддержка обновления с версии на версию **ALDPro**. В строках - исходные версии, с которых происходит обновление, в столбцах - целевые версии, на которые происходит обновление.

**+** – точно можно обновлять;

**-** – точно нельзя обновлять напрямую, только с обновлением через другую версию;

**+/-** – потенциально можно обновить, но тестирование не было выполнено и в документации нет информации.

| | 1.0.0 | 1.1.0 | 1.1.1 | 1.1.2 | 1.1.3 | 1.2.0 | 1.2.1 | 1.3.0 | 1.4.0 | 1.4.1 | 2.0.0 | 2.1.0 | 2.2.0 | 2.2.1 | 2.3.0 | 2.4.0 | 2.4.1 | 2.5.0 | 3.0.0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1.0.0 | X | + | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| 1.1.0 | X | X | + | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| 1.1.1 | X | X | X | + | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| 1.1.2 | X | X | X | X | + | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| 1.1.3 | X | X | X | X | X | + | + | + | + | + | - | - | - | - | - | - | - | - | - |
| 1.2.0 | X | X | X | X | X | X | + | + | + | + | - | - | - | - | - | - | - | - | - |
| 1.2.1 | X | X | X | X | X | X | X | + | + | + | - | - | - | - | - | - | - | - | - |
| 1.3.0 | X | X | X | X | X | X | X | X | + | + | - | - | - | - | - | - | - | - | - |
| 1.4.0 | X | X | X | X | X | X | X | X | X | + | - | - | - | - | - | - | - | - | - |
| 1.4.1 | X | X | X | X | X | X | X | X | X | X | + | - | - | - | - | - | - | - | - |
| 2.0.0 | X | X | X | X | X | X | X | X | X | X | X | + | + | + | + | +- | +- | - | - |
| 2.1.0 | X | X | X | X | X | X | X | X | X | X | X | X | + | + | + | +- | +- | - | - |
| 2.2.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | + | + | + | + | - | - |
| 2.2.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X | + | + | + | - | - |
| 2.3.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | + | + | - | - |
| 2.4.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | + | + | +- |
| 2.4.1 | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | + | + |
| 2.5.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | + |
| 3.0.0 | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |

Таблица 13 — Матрица обновлений ПК ALD Pro