ALD Pro

РУКОВОДСТВО АДМИНИСТРАТОРА. ЧАСТЬ 2

РДЦП.10101-01 95 01-03
Версия 3.0.0

Содержание

1 Портал управления. Настройка и работа 12

1.1 О системе . . . 12

1.1.1 Общие сведения . . . 12

1.1.2 Функциональное назначение . . . 12

1.1.3 Используемые технические средства и дополнительное программное обеспечение . . . 13

1.1.4 Входные и выходные данные . . . 14

1.1.5 Вызов и загрузка . . . 15

1.2 Аутентификация пользователей . . . 15

1.2.1 Вход в Систему по логину или паролю . . . 15

1.2.2 Вход в Систему с Kerberos . . . 17

1.2.3 Выход из Системы или Смена пользователя . . . 18

1.3 Управление доменом . . . 18

1.3.1 Общая информация . . . 18

1.3.2 Сайты и службы . . . 21

1.3.3 Дополнительные параметры групповых политик . . . 29

1.3.4 Каталог заданий автоматизации . . . 41

1.3.5 Службы и параметры Kerberos . . . 46

1.3.6 Пользователи и группы . . . 49

1.3.7 Интеграция с доменами . . . 54

1.3.8 Роли и права доступа . . . 62

1.3.9 Мандатное управление доступом (МРД) . . . 65

1.4 Пользователи и компьютеры . . . 77

1.4.1 Организационная структура . . . 77

1.4.2 Пользователи . . . 88

1.4.3 Группы пользователей . . . 102

1.4.4 Компьютеры . . . 112

1.4.5 Группы компьютеров . . . 117

1.4.6 Корзина . . . 123

1.5 Автоматизация . . . 124

1.5.1 Задания автоматизации . . . 124

1.5.2 Установка ОС по сети . . . 127
1.6 Мониторинг . . . 144
1.6.1 Журнал событий мониторинга . . . 144
1.6.2 Витрины мониторинга домена . . . 146
1.6.3 Расширение функционала мониторинга . . . 149
1.7 Модуль синхронизации . . . 149
1.7.1 Настройки . . . 150
1.7.2 Источники . . . 154
1.7.3 Сопоставление атрибутов . . . 156
1.7.4 Особенности работы модуля синхронизации . . . 159
1.8 Журнал событий . . . 162
1.8.1 Серверы журнала событий . . . 162
1.8.2 Настройка сбора журналов событий . . . 164
1.9 Групповые политики . . . 167
1.9.1 Групповые политики . . . 167
1.9.2 Политики доступа к узлу . . . 176
1.9.3 Политики повышения привилегий . . . 185
1.9.4 Политики паролей . . . 197
1.10 Установка и обновление ПО . . . 198
1.10.1 Политики ПО . . . 198
1.10.2 Каталог ПО . . . 206
1.10.3 Репозитории ПО . . . 216
1.10.4 Политики обновления ALD Pro . . . 224
1.11 Роли и службы сайта . . . 229
1.11.1 Служба разрешения имен . . . 229
1.11.2 Служба динамической настройки узла . . . 244
1.11.3 Служба синхронизации времени . . . 251
1.11.4 Служба глобального каталога . . . 255
1.11.5 Служба печати . . . 257
1.11.6 Общий доступ к файлам . . . 261
1.12 Личный кабинет . . . 269
1.12.1 Основное . . . 269
1.12.2 Группы . . . 271
1.12.3 Дополнительные сведения . . . 273
1.12.4 Групповые политики . . . 273
1.12.5 Расширенные настройки . . . 273
1.12.6 Роли . . . 273
1.12.7 МРД . . . 274
1.13 Начало работы с ALD Pro . . . 275

1.14 Интерфейс Портала Управления . . . 276
1.15 Навигация по Порталу Управления . . . 277

2 Отладка подсистем ALD Pro 278

2.1 Архитектура SSSD . . . 278
2.1.1 Монитор (Monitor) . . . 281
2.1.2 Серверные части или Бэкенды (backends) . . . 282
2.1.3 Ответчики (responders) . . . 284
2.1.4 Клиентские библиотеки и приложения . . . 285
2.1.5 Механизм кэширования службы SSSD . . . 286
2.1.6 Инструменты администрирования . . . 292
2.2 Учетная запись компьютера в домене . . . 294
2.3 Способы аутентификации в домене . . . 298
2.3.1 Аутентификация по протоколу LDAP . . . 298
2.3.2 Аутентификация по протоколу Kerberos . . . 300
2.3.3 Аутентификация по протоколу NTLM . . . 308
2.4 Безопасный обмен данными с применением SSL/TLS . . . 309
2.4.1 Механизм защиты данных по протоколу SSL . . . 310
2.4.2 Доступ к каталогу по протоколам LDAP+StartTLS и LDAPS . . . 313
2.4.3 Доступ к веб-интерфейсам и REST API контроллера домена по протоколу HTTPS . . . 316
2.4.4 Доступ к удаленному рабочему столу по протоколу VNC через HTTPS 319
2.5 Работа механизмов автоматического обнаружения сервисов LDAP и KDC . . 321
2.5.1 Автоматическое обнаружение при вводе хоста в домен утилитой ipa-client-install . . . 321
2.5.2 Автоматическое обнаружение сервисов в SSSD . . . 323
2.5.3 Автоматическое обнаружение сервисов в библиотеке libkrb5 . . . 328
2.6 Работа компьютера в автономном режиме . . . 337
2.6.1 Автономный вход по кэшу пароля . . . 338
2.6.2 Автоматическая Kerberos аутентификация при переходе в онлайн режим 340
2.7 Динамическое обновление DNS-записей в домене . . . 343
2.8 Отладка работы службы SSSD . . . 344
2.8.1 Журналы отладки SSSD . . . 344
2.8.2 Общие рекомендации . . . 346
2.8.3 Отладка Бэкенда . . . 348
2.8.4 Устранение неисправностей аутентификации, изменения пароля и контроля доступа . . . 350
2.9 Расположение значимых файлов . . . 352

3 Справочные материалы **353**
3.1 Создание дополнительных параметров групповых политик 353
3.1.1 Функционал групповых политик 353
3.1.2 Как работают групповые политики 354
3.1.3 Как создать дополнительный параметр 354
3.1.4 Как настроить атрибуты дополнительного параметра 362
3.1.5 Скрипт дополнительного параметра 363
3.1.6 Требования к скриптам и наследование параметров 370
3.1.7 Отладка 371
3.2 Резервное копирование подсистем ALD Pro 373
3.2.1 Резервное копирование (далее - бэкапирование) 373
3.2.2 Раздел 2. Восстановление 379
3.3 Инструкция по обеспечению безопасной работы в домене ALD Pro: правила HBAC 390
3.3.1 Что такое HBAC-правила 391
3.3.2 Механизм работы HBAC-правил 391
3.3.3 Доступ для администраторов ко всем компьютерам в домене, ограничение правила allow_all 395
3.3.4 Доступ для сотрудников на рабочие станции, создание правила allow_computers 396
3.3.5 Гранулированный доступ к отдельным службам и отладка правил . . 400
3.3.6 Лучшие практики: ограничение доступа локальным пользователям . . 406
3.3.7 Лучшие практики: создание HBAC-правил для структурных подразделений 407
3.4 Автоматизация задач администрирования через LDAP-запросы 411
3.4.1 Введение 411
3.4.2 Технология LDAP 411
3.4.3 Взаимодействие с каталогом через LDAP-протокол 418
3.4.4 Примеры автоматизации 447
3.4.5 Расширение схемы пользовательскими классами и атрибутами 466
3.4.6 Заключение 482
3.5 Повышение привилегий доменных пользователей с помощью правил SUDO . 482
3.5.1 Что такое правила SUDO 483
3.5.2 Механизм работы правил SUDO 487
3.5.3 Механизм получения правил SUDO из LDAP 489
3.5.4 Настройка правил SUDO в домене 491
3.5.5 Отладка правил SUDO 502
3.5.6 Лучшие практики 505

3.6 Инструкция по обеспечению безопасной работы в домене ALD Pro: политики паролей 509
3.6.1 Пароли пользователей в домене 509
3.6.2 Что такое политики паролей 510
3.6.3 Механизм работы политик паролей 510
3.6.4 Создание политики паролей 519
3.6.5 Список запрещённых слов 524
3.7 Доверительные отношения 527
3.7.1 Модуль доверия между доменами ALD Pro 527
3.8 Инструкция по установке доверительных отношений между Microsoft Active Directory и ALD Pro 533
3.8.1 Постановка задачи 533
3.8.2 Подготовка контроллера домена ALD Pro 535
3.8.3 Подготовка контроллера домена MS 540
3.8.4 Контрольный список межлесного доверия 541
3.8.5 Контроллеры доверия и агенты доверия (Trust controllers and trust agents) 541
3.8.6 Проверка доступности портов 542
3.8.7 Взаимное перенаправление DNS-зон 545
3.8.8 Настройка DNS - доверительные сети (bind trusted_network) 547
3.8.9 Настройка времени 548
3.8.10 Создание двустороннего доверия (Forest Trust) 551
3.8.11 Создание доверия между двумя доменами (External Trust) 554
3.8.12 Проверка работоспособности доверия (id-идентификация) 564
3.8.13 Проверка работоспособности доверия (Kerberos) 567
3.8.14 Дополнительные проверки 569
3.8.15 Включение поддержки UPN на стороне клиента 572
3.8.16 Проверка поддержки UPN на стороне сервера 573
3.8.17 Проверка работоспособности UPN через графику 574
3.8.18 Проверка работоспособности UPN через SSH 574
3.8.19 Настройка сервера ALD Pro (FreeIPA) на определенный сайт MS AD (id, logon) 575
3.8.20 Настройка клиента на определенный сайт MS AD (id, logon) 575
3.8.21 Настройка журналов отладки для доменов SSSD 577
3.8.22 Описание уровней логирования SSSD 578
3.8.23 Описание SSSD журналов событий 579
3.8.24 Настройка журналов отладки 581
3.8.25 Проблемы с конфигурационном файлом SSSD.conf 585
3.8.26 Отсутствие групп при выполнении команды id 587
3.8.27 Долгое выполнение команды id 588

3.8.28 SSSD не удается подключиться к MS AD из-за ошибок с GSS-API . . . 588
3.8.29 Настройка игнорирования участников групп (ignore_group_members) . 591
3.8.30 Настройка таймаута конфигурации для плагина ipa-extdom на ALD Pro (FreeIPA)-серверах . . . 593
3.8.31 Настройка максимального размера буфера для плагина ipa-extdom на ALD Pro-серверах . . . 594
3.8.32 Настройка максимального количества экземпляров для плагина ipa-extdom на ALD Pro-серверах . . . 595
3.8.33 Настройка SSSD в ALD Pro-клиентах для крупных доверительных развертываний IdM-AD . . . 597
3.8.34 Монтирование кэша SSSD в tmpfs . . . 598
3.8.35 Создание сетевой папки в домене MS AD . . . 600
3.8.36 Подключение сетевой папки на рабочей станции под управлением Astra Linux . . . 604
3.8.37 Добавление пользователей и групп из ALD Pro домена в домен MS AD. 608
3.8.38 Инструкция по работе двусторонних доверительных отношений между MS AD и ALD Pro . . . 617
3.8.39 Инструкция по присоединению системы Windows к FreeIPA Realm без Active Directory . . . 627
3.9 Модуль Синхронизации . . . 650
3.9.1 Инструкция по дополнительной настройке модуля синхронизации . . 650
3.9.2 Отладка работы модуля синхронизации . . . 688
3.9.3 Инструкция по выдаче ограниченных прав на управление паролями пользователей в домене MS AD . . . 697
3.9.4 Инструкция по обновлению ALD Pro до версии 2.4.0 и более поздних с ранее установленным модулем синхронизации . . . 702
3.10 Суммирование политик ПО . . . 704
3.10.1 Термины и определения . . . 704
3.10.2 Назначение политик ПО на подразделение . . . 705
3.10.3 Описание принципов суммирования политики ПО . . . 706
3.10.4 Отладка политик ПО . . . 714
3.11 Настройка синхронизации пользователей из ALD Pro в Keycloak . . . 717
3.11.1 Термины и определения . . . 717
3.11.2 Предварительная настройка ALD Pro . . . 717
3.11.3 Краткая инструкция настройки Keycloak . . . 719
3.11.4 Подробная инструкция настройки Keycloak . . . 719
3.11.5 Синхронизация групп пользователей из ALD Pro в Keycloak . . . 725
3.11.6 Синхронизация подразделений . . . 729

3.12 Инструкция по развертыванию ALD Pro в виртуальной среде (знакомство с ALD Pro) . . . 731
3.12.1 Аннотация . . . 731
3.12.2 Предварительные требования . . . 731
3.12.3 Постановка задачи . . . 731
3.12.4 Создайте сеть в VirtualBox . . . 732
3.12.5 Создайте VM для контроллера (dc-1.ald.company.local) . . . 734
3.12.6 Установите пакеты ALD Pro на DC-1 . . . 735
3.12.7 Выполните продвижение DC-1 до контроллера домена . . . 742
3.12.8 Создайте VM для пользовательского компьютера (pc-1.ald.company.local) . . . 749
3.12.9 Установите клиентские пакеты ALD Pro на PC-1 . . . 750
3.12.10 Выполните ввод компьютера в домен . . . 753
3.12.11 Проверка работы синхронизации времени . . . 754
3.12.12 Как работает вход в доменный компьютер . . . 758
3.12.13 Как управлять билетами Kerberos из командной строки . . . 765
3.13 Настройка прочих подсистем . . . 766
3.13.1 Подготовительные действия . . . 766
3.13.2 Развертывание основных подсистем ПК «ALD Pro» . . . 766
3.13.3 Добавление компьютера ПК «ALD Pro» в домен . . . 768
3.14 Создание сервисной учетной записи для почтового сервиса RuPost . . . 778
3.14.1 Введение . . . 778
3.14.2 Создание сервисной УЗ . . . 778
3.15 Инструкция по настройке журналирования событий . . . 779
3.15.1 Область применения . . . 779
3.15.2 Термины и определения . . . 779
3.15.3 Описание . . . 787
3.15.4 Системные требования . . . 790
3.15.5 Настройка журналирования событий безопасности на КД и сбор данных журналов на сервере аудита . . . 791
3.15.6 Ротация журналов . . . 815
3.15.7 Отправка журналов в стороннюю SIEM . . . 838
3.15.8 Настройка журналирования на КД, сервере общего доступа к файлам и сервере аудита (только команды) . . . 843
3.16 Инструкция по управлению зонами ответственности при администрировании 854
3.16.1 Аннотация . . . 854
3.16.2 Введение . . . 854
3.16.3 Назначение типов администратора . . . 855
3.16.4 Управление типами администратора . . . 857

3.16.5 Политики повышения возможностей при администрировании (SUDO) 858
3.16.6 Политики доступа к узлу (HBAC) 863
3.17 Рекомендации по настройке hostname & fqdn 865
3.17.1 Введение 865
3.17.2 Рекомендации 865
3.18 Наследование и суммирование параметров групповых политик 867
3.18.1 Аннотация 867
3.18.2 Термины и определения 867
3.18.3 Предварительные настройки 872
3.18.4 Наследование 873
3.18.5 Суммирование 878
3.18.6 Просмотр смоделированного отчета о назначенных параметрах ГП . . 890
3.19 Синхронизация объектов, содержащих специальные символы 891
3.19.1 Введение 891
3.19.2 Описание базовых правил замены 893
3.20 Инструкция по настройке браузера для сквозной авторизации в Web-интерфейсе портала управления ALD Pro 904
3.20.1 Браузер Firefox 904
3.20.2 Браузер Chromium 904
3.21 Матрица и описание ролей 905
3.21.1 Описание ролей 905
3.21.2 Матрицы ролей 995
3.22 Матрица и описание привилегий 1005
3.22.1 Описание привилегий 1006
3.22.2 Матрица привилегий 1088
3.23 Миграция ролей 1098
3.23.1 Введение 1099
3.23.2 Миграция системных ролей 1099
3.23.3 Миграция предустановленных ролей 1099
3.23.4 Миграция пользовательских ролей 1110
3.24 Доступные точки входа для пользователей без дополнительных привилегий (ролей) 1112
3.24.1 Аннотация 1112
3.24.2 Описание точек входа 1112
3.25 Особенности работы системы при гранулярном управлении доступом 1116
3.25.1 Особенности работы привилегий 1116
3.25.2 Особенности работы методов PUT и PATCH 1117
3.25.3 Возможные ответы системы на запросы GET при отсутствии прав на выполнение операции 1118

3.26 Механизм репликации FreeIPA . . . 1118
3.26.1 Соглашения о репликации . . . 1119
3.26.2 Порядок решения конфликтов репликации . . . 1120
3.27 Удаление первого контроллера домена . . . 1121
3.27.1 Подготовка к удалению . . . 1121
3.27.2 Если контроллер домена недоступен . . . 1122
3.27.3 Удаление контроллера домена . . . 1126
3.28 Удаление резервного контроллера домена . . . 1127
3.28.1 Подготовка к удалению . . . 1127
3.28.2 Удаление контроллера домена . . . 1128
3.29 Обновление подсистем ALD Pro через портал управления . . . 1129
3.30 Проверка работы сервисов ALD Pro . . . 1135
3.30.1 Конфигурация . . . 1135
3.30.2 Перечень команд . . . 1137
3.30.3 Варианты отображения статуса сервиса . . . 1137
3.31 Проверка статуса репликации . . . 1137
3.31.1 Проверка статуса репликации утилитой dsconf . . . 1137
3.31.2 Проверка репликации с помощью скриптов checkipaconsistency . . . 1140
3.32 Управление сетевыми папками . . . 1143
3.32.1 Права доступа на новую папку . . . 1143
3.32.2 Уровень «Чтение» - viewer . . . 1143
3.32.3 Уровень «Полный доступ» - fullcontrol . . . 1144
3.32.4 Уровень «Изменение и назначение прав» - editor . . . 1144
3.32.5 Уровень «Доступ запрещен» - invalid . . . 1145
3.32.6 Дополнительные параметры . . . 1145
3.32.7 Управление папками . . . 1147
3.32.8 Аутентификация . . . 1148
3.33 Создание репозиториев из ISO образа . . . 1149
3.34 Утилиты для работы с групповыми политиками, подсистемами и заданиями автоматизации . . . 1154
3.34.1 Форсированная установка подсистем . . . 1154
3.34.2 Утилита для работы с групповыми политиками . . . 1155
3.34.3 Утилита для работы с заданиями автоматизации . . . 1156
3.35 Создание репозитория из загруженных пакетов deb . . . 1156
3.36 Установка браузера из deb репозитория . . . 1159
3.37 Необходимые привилегии для ввода компьютера в домен . . . 1161
3.37.1 Предварительная настройка . . . 1162
3.38 Присоединение к домену с помощью одноразового пароля . . . 1167
3.39 Повторное присоединение к домену, используя keytab-файл хоста . . . 1169

3.40 Служба синхронизации времени . . . 1170
3.40.1 Динамические DNS-записи . . . 1171
3.40.2 Алгоритм автоматической настройки подсистемы NTP . . . 1172
3.41 Проверка алгоритма хэширования пароля пользователя по умолчанию в ALD Pro . . . 1174
3.42 Удаление информации о серверах и пулах NTP при обновлении ALD Pro . . . 1175
3.42.1 Предусловие . . . 1175
3.42.2 Последовательность действий . . . 1175
3.43 Настройка мониторинга целостности каталога . . . 1176
3.43.1 Введение . . . 1176
3.43.2 Действия на контроллерах домена . . . 1176
3.43.3 Действия на подсистеме мониторинга . . . 1177
3.44 Инструкция по настройке автомонтирования с помощью групповых политик ALD Pro . . . 1189
3.44.1 Введение . . . 1189
3.44.2 Автомонтирование в Linux . . . 1189
3.44.3 Управление автомонтированием через FreeIPA UI . . . 1200

4 Известные проблемы 1212

4.1 Исправление односторонних отношений Left-Right . . . 1212
4.2 Вход в систему занимает слишком много времени . . . 1213
4.3 Решение проблемы с запросами на получение билетов kerberos . . . 1214
4.4 Команды getent passwd и getent group не отображают пользователей и групп . 1215
4.5 Изменений на сервере довольно долго не видно на клиенте . . . 1215
4.6 Как включить аутентификацию LDAP через незащищенное соединение . . . 1215
4.7 В журналах нет ни одного сообщения от pam_sss . . . 1215
4.8 Я могу переключиться на доменного пользователя командой su из-под root, но не под обычным пользователем, SSH тоже не работает . . . 1216
4.9 Я получаю сообщение Access denied for user $user: 6 (Permission denied) . . . 1216
4.10 Исправление ошибки глобального каталога . . . 1216
4.11 При обновлении контроллера домена возникает ошибка «Error updating rbtaSubsystemLog» . . . 1217
4.12 При настройке доверительных отношений появляется ошибка «saf_fetch: failed to find server for «WINAD» domain» . . . 1218
4.13 Медленное монтирование сетевых ресурсов пользователями доверенных доменов . . . 1220
4.14 Некорректное отображение ошибки «Значение максимального уровня должно быть не меньше значения минимального уровня» . . . 1220
4.15 Ограничение проверки на удаление уровней конфиденциальности . . . 1221

4.16 Устранение проблем с авторизацией после обновления до версии 3.0.0 1221
4.16.1 Ошибки и порядок их решения в процессе обновления Системы . . . 1222
4.17 Решение проблемы долгих запросов при работе с почтовой системой RuPost 1223

Портал управления. Настройка и работа

1.1. О системе

В данном разделе приведено описание функциональных характеристик программного обеспечения **ALD Pro** и информация, необходимая для его эксплуатации.

1.1.1. Общие сведения

Наименование программы — «Программный комплекс «ALD Pro».

Сокращенное наименование программы — **ALD Pro**.

Тексты программы **ALD Pro** написан на следующих языках:

- **Python**;
- **JavaScript**.

1.1.2. Функциональное назначение

ALD Pro предназначен для централизованного администрирования ресурсами домена под управлением ОС **Astra Linux** и использования в организациях различного масштаба.

Функциональные возможности программы:

- управление конфигурацией домена;
- удаленное подключение к рабочему столу пользователя;
- установка и обновление программного обеспечения;
- установка операционной системы по сети;
- управление службой разрешения имен;
- управление службой динамической настройки узла;
- управление службой синхронизации времени;
- управление службой печати;

- управление заданиями автоматизации;
- навигация и поиск объектов;
- справочный центр;
- интеграция с почтовым сервисом;
- аутентификация пользователей изделия;
- управление параметрами групповых политик;
- управление службами и политиками билетов Kerberos;
- управление параметрами пользователей и групп;
- управление доверительными отношениями с доменами;
- управление организационной структурой, пользователями и компьютерами;
- управление групповыми политиками;
- управление общим доступом к файлам;
- управление доступом к функциям изделия;
- управление мониторингом;
- управление журналированием событий;
- доступ к личному кабинету.

1.1.3. Используемые технические средства и дополнительное программное обеспечение

Компоненты **ALD Pro** функционируют на технических средствах, состав и характеристики которых представлены в данном подразделе.

Клиентская часть — это набор ПО, который устанавливается на компьютеры домена и состоит из подсистемы **Агент домена**. В качестве браузера рекомендуется использовать **Chromium** или **Mozilla FireFox**. При использовании любого другого браузера возможно предупреждение “Вероятная угроза безопасности”. Чтобы продолжить работу в выбранном браузере, необходимо нажать на кнопку “Принять риски и продолжить”.

Требования к оборудованию для функционирования клиентской части:

- **компьютер:**
  - операционная система семейства **Astra Linux**;
  - процессор (**CPU**) — не менее двух ядер;

    - оперативная память (**RAM**) — не менее 1 Гб;
    - свободное место на диске — не менее 4 Гб;
    - видеокарта;
- монитор;
- клавиатура;
- мышь.

Для установки пакетов клиентской части приложения на компьютере должен быть доступ к официальным репозиториям компании-производителя (https://dl.astralinux.ru) либо к репозиториям, развернутым во внутренней сети.

Серверная часть работает на специальном промышленном компьютере (сервере), который не предназначен для бытового использования.

1.1.4. Входные и выходные данные

Входными данными для обеспечения функционирования **ALD Pro** являются:

- обращение пользователей (процессов и команд) к подсистемам **ALD Pro** и их специальным модулям, а также средствам **IPC**.
- атрибуты, определяющие полномочия пользователя и правила разграничения доступа к функциям **ALD Pro**

Выходными данными является результат обработки обращений пользователя (процессов и команд) к функциям **ALD Pro**:

- авторизация пользователя;
- развертывания сетевых служб;
- запуск служб;
- запись, редактирование, удаление объектов;
- запуск, редактирование и исполнение команд управления;
- регистрация результатов выполнения команд управления.

1.1.5. Вызов и загрузка

Для клиентской части **ALD Pro** вызов осуществляется путем запуска браузера на компьютере, подключенном к домену, и ввода в адресной строке браузера **URL** системы.

Вызов и загрузка серверной части **ALD Pro** производится путем запуска приложения в соответствии с эксплуатационной документацией.

Примечание: Для корректной работы с порталом управления администратор домена должен использовать доменное имя контроллера домена (не IP-адрес).

1.2. Аутентификация пользователей

Раздел содержит следующие подразделы:

1.2.1. Вход в Систему по логину или паролю

Окно **Вход в Систему** открывается автоматически при входе на **ALD Pro**.

Для входа ввести логин и пароль в соответствующие поля. Для безопасности пароль скрыт. Чтобы просмотреть пароль, нужно нажать на значок глаза в поле **Пароль**.

Нажать кнопку **Войти**. Откроется страница **ALD Pro**, соответствующая зонам ответственности пользователя.

Примечание: Время непрерывной сессии составляет 23 часа. При этом будет создан действующий TGT-билет, и на время его действия авторизация комьютера будет проходить через билет.

При некорректно введенном логине/пароле появляется сообщение об ошибке. В Системе число попыток входа ограничено и регулируется администратором.

Вход на портал управления пользователя с пустым паролем невозможен, независимо от того, каким образом такой пользователь был создан.

Если есть проблемы с входом, то возможна одна из следующих причин:

- превышено число попыток ввода логина/пароля;
- срок действия пароля истек или пароль не активирован.

Ежедневно один раз в день после обновления сессии или входа в систему появляется уведомление о сроке действия пароля “Дней до окончания действия пароля N”, при условии, что дней до истечения пароля осталось не больше, чем указано в настройках.

1.2.1.1. Смена пароля с истекшим сроком действия

Информационное сообщение об истечении срока действия пароля появляется у пользователя согласно настройке Системы.

Если пользователь по каким-то причинам не обновил пароль своевременно, то Система поддерживает возможность смены пароля без авторизации.

При вводе пароля с истекшим сроком действия, на странице входа появляются дополнительные поля, позволяющие пользователю сменить пароль.

Для смены пароля необходимо ввести текущий пароль, новый пароль и подтверждение нового пароля в соответствующие поля и нажать кнопку сохранения изменений.

Пароль изменен. Теперь пользователь может войти в Систему, используя новый пароль.

Таким же образом пользователь может сменить пароль при первом входе в Систему или в случае, если ему был выдан временный пароль в замен анулированного администратором.

1.2.1.2. Первый вход

При первом входе Система требует смены пароля, полученного от администратора. Сделать это можно одним из следующих способов:

1. Через окно входа на портал управления.
2. Через доменный компьютер.

Смена пароля через доменный компьютер

Для первого входа использовать доменный компьютер пользователя. В открывшуюся форму аутентификации на компьютере ввести полученные от администратора логин и пароль. Откроется форма смены пароля, где нужно указать старый пароль, новый пароль и подтверждение нового пароля. Нажать кнопку сохранения изменений.

Пароль изменен. Теперь вход на портал с доменного компьютера осуществляется без дополнительного ввода логина и нового пароля.

Смена пароля через через окно входа на портал управления

Действия по смене пароля при первом входе аналогичны смене пароля с истекшим сроком действия и подробно описаны *здесь*.

1.2.2. Вход в Систему с Kerberos

Вход в Систему с Kerberos - один из способов аутентификации, поддерживаемый **ALD Pro**.

Доступен только для компьютеров в домене. Настройка браузера и выдача билета автоматическая и не требует участия пользователя.

Для входа нужно нажать **Вход с Kerberos**. Логин и пароль не используются. Откроется страница **ALD Pro**, соответствующая зонам ответственности пользователя.

Примечание: Вход с Kerberos возможен только для тех пользователей, у которых есть действующий билет.

1.2.3. Выход из Системы или Смена пользователя

Для выхода из Системы или смены пользователя в правом верхнем углу навести курсор мыши на значок пользователя. В выпадающем меню выбрать **Выход**. Откроется окно **Вход в Систему**.

Для входа под другим пользователем воспользуйтесь формой аутентификации.

По умолчанию в Системе зарегистрирован пользователь с типом **главный администратор (ALDPRO - Main Administrator)**. Он изначано регистрирует пользователей и выдает логины и пароли для работы в Системе. Доступ к Системе имеют зарегистрированные администратором пользователи.

Система поддерживает два типа входа в систему:

- вход в Систему по логину/паролю;
- вход в Систему с Kerberos.

1.3. Управление доменом

В данном разделе осуществляется настройка и управление структурой и конфигурацией ALD Pro.

1.3.1. Общая информация

1.3.1.1. Описание

Подраздел отображает состояние домена, состав системы, граф топологии и основные параметры домена.

Подраздел состоит из вкладок:

- **Работоспособность домена**;
- **Состав системы**;
- **Граф топологии**;
- **Параметры домена**.

1.3.1.2. Работоспособность домена

На вкладке располагаются четыре виджета с информацией о работоспособности системы:

- **Общее состояние системы** — состояние системы на данный момент;
- **Состояние домена** — общее количество контроллеров домена, которые заведены в систему, количество сайтов, которые есть в системе, и количество проблем с контроллерами домена и сайтами;
- **Количество типов объектов системы** — типы объектов и их количество;
- **Принадлежность сайтов к подсистемам** — количество объектов в каждой подсистеме и их состояние. Также можно узнать к каким именно подсистемам относится тот или иной сайт и его состояние в подсистеме на данный момент. Переключение между сайтами реализованно поисковой строкой с выпадающим списком созданных сайтов.

1.3.1.3. Состав системы

На вкладке приводится список подсистем с указанием наименования подсистемы (**Подсистема**), сервера (**Сервер**), сайта (**Сайт**), состояния (**Состояние**) и версии системы (**Версия ALD Pro**).

Каждая подсистема может прибывать в одном из следующий состояний:

- **Ошибка**: установка или обновление подсистемы не выполнено;
- **Устанавливается**: выполняется установка подсистемы;
- **Установлена**: подсистема успешно установлена;
- **Удаляется**: выполняется удаление подсистемы;
- **Удалена**: подсистема успешно удалена;
- **Обновляется**: выполняется обновление подсистемы;
- **Обновлена**: подсистема успешно обновлена.

Внимание: Для установки подсистемы на контроллер домена, на котором уже была установлена подсистема (устанавливаемая или любая другая), необходимо предварительно вывести компьютер из домена и переустановить операционную систему на нем.

Для поиска по имени сервера сверху, под меню вкладок доступна поисковая строка.

Для списка доступна фильтрация по значениям полей **Сайт** и **Состояние**. Для фильтрации необходимо кликнуть по значку фильтрации и выбрать значение из выпадающего списка. Для поиска необходимого значения доступен функционал поиска. Для этого в поле **Найти значение** вверху списка начать вводить значение. В результате будет обновлен список фильтрации, отвечающий требованиям поиска.

Для списка доступна сортировка по значениям поля **Сервер**.

В левом нижнем углу указано количество подсистем.

1.3.1.4. Граф топологии

Граф топологии представляет собой модель связи сайта и контроллера домена.

В верхней правой части вкладки указаны сущности, которые отображены на графе.

При наведении курсора на объект будет показано название объекта и его сущность. При наведении курсора на линию, соединяющую объекты, будет показано какие объекты эта линия соединяет и тип соединения (одностороннее/двустороннее).

Для перемещения по модели необходимо переместить курсор на вкладку, зажать левую кнопку мыши и переместить курсор. Для увеличения/уменьшения масштаба использовать колесо мыши.

В левой верхней части вкладки располагается фильтр отображения объектов топологии. Для его использования необходимо нажать на кнопку **[Фильтр]** и ввести опцию или выбрать из выпадающего списка. Чтобы сбросить опцию фильтра, необходимо нажать на кнопку закрытия **[X]** в опции. Чтобы сбросить все опции, необходимо нажать на кнопку закрытия **[X]** рядом с выпадающим списком. Для скрытия опций нажать на кнопку **[Скрыть]**.

Отображение топологии можно отфильтровать также по типу сущности, для этого в верхней правой части вкладки нажать на название сущности для ее скрытия/отображения.

1.3.1.5. Параметры домена

Во вкладке отображается информация о домене: версия системы **ALD Pro**, исполнение **ALD Pro**, имя области **Kerberos (REALM)** и уровень домена **FreeIPA**.

Поле **Исполнение ALD Pro** принимает значения:

- `РДЦП.10101-01` - при несертифицированном исполнении ALD Pro;
- `РДЦП.10101-02` - при сертифицированном исполнении ALD Pro.

1.3.2. Сайты и службы

В подразделе приведены функции управления сайтами и репликацией домена.

1.3.2.1. Сайты и службы

На вкладке **Сайты и службы** осуществляется управление сайтами домена. Сайты в ALD Pro — это способ сегментирования системы.

Список сайтов и сервисов

Подраздел **Сайты и службы** раздела **Упрвленеие доменом** при выборе открывает вкладку **Сайты**. На данной вкладке приводится список сайтов с указанием их имен (**Имя сайта**) и расположения (**Расположение IPA**), по которым доступна сортировка в алфавитном порядке.

Для поиска по названию сайта сверху, под меню вкладок доступна поисковая строка. Справа от нее расположена кнопка для создания нового сайта **[+ Новый сайт]**.

Для просмотра информации о сайте нажать на соответствующий сайт в списке. Будет открыта карточка сайта с информацией о нем.

В левом нижнем углу указано количество сайтов, а в правом нижнем углу располагаются кнопки переключения страниц.

Создание нового сайта

Для создания нового сайта нажать кнопку **[+ Новый сайт]** в подразделе **Сайты и службы** на вкладке **Сайты**. Будет выполнен переход на карточку создания сайта.

На вкладке **Основное** карточки сайта необходимо заполнить обязательные поля **Имя сайта** (например, *Сибирский офис*) и **Расположение IPA** (например, *siberia*). Опционально

можно заполнить поле **Описание сайта**.

Важно: В поле **Расположение IPA** допустимы для использования цифры и строчные латинские буквы.

Для сохранения сайта необходимо в правом верхнем углу нажать на кнопку сохранения **[Сохранить]** и подтвердить действие в диалоговом окне.

Для закрытия карточки без сохранения сайта нажать кнопку **[X Закрыть]**.

Вкладки **Контроллеры домена** и **Подсистемы сайта** станут доступны для заполнения после сохранения сайта (см. *Управление сайтом*).

Управление сайтом

Управление сайтом и редактирования информации о нем выполняется на его карточке. Для открытия карточки необходимо на вкладке **Сайты** подраздела **Сайты и службы** нажать на соответствующий сайт.

На карточке сайта информация о нем содержится на вкладках:

- **Основное**;
- **Контроллеры домена**;
- **Подсистемы сайта**.

Для закрытия карточки сайта и возврата к списку сайтов нажать на кнопку **[X Закрыть]**.

Основное

Данная вкладка отображает основную информацию о сайте.

Поля **Описание сайта** и **Расположение IPA** доступны для редактирования. Поле **Расположение IPA** является обязательным для заполнения.

Для сохранения изменений необходимо в правом верхнем углу нажать на кнопку **[Сохранить]**.

Контроллеры домена

Список контроллеров домена

На вкладке **Контроллеры домена** карточки сайта приводится список контроллеров домена, назначенных сайту, с указанием **Имени компьютера** и его **IP-адреса**.

В левом нижнем углу указано количество контроллеров, а в правом нижнем углу располагаются кнопки переключения страниц.

Для списка доступен поиск по названию. Для этого сверху над списком, под меню вкладок, в поле поиска ввести значение. Справа от поисковой строки находятся кнопки **[+ Новый контроллер домена]** и **[+ Назначить контроллер домена]**.

Для просмотра информации о контроллере домена необходимо открыть его карточку. Для открытия карточки нажать на контроллер домена в списке.

Добавление контроллера домена

Для создания контроллера домена нажать кнопку **[+ Новый контроллер домена]** на вкладке **Контроллеры домена** карточки сайта. Будет выполнен переход на карточку создания нового контроллера домена, где нужно заполнить обязательные поля **Имя компьютера** и **Имя сайта**.

Доступны функции назначения ролей Глобального Каталога и PKI Proxy выставлением флажков в соответствующих клетках: **Назначить роль глобального каталога** и **Назначить роль PKI Proxy**.

Важно: Для корректной работы PKI Proxy необходимо наличие ключа „ca.key“ в папке /etc/ssl/freeipa/ Иначе назначение роли завершится с ошибкой.

Для сохранения нового контроллера необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу и подтвердить сохранение. Будет выполнен переход к списку контроллеров, назначенных сайту.

Для закрытия карточки создания контроллера и возврата к списку контроллеров, назначенных сайту, нажать на кнопку закрытия. В случае, если были введены какие-либо данные, будет запрошено подтверждение закрытия картиочки создания домена без

сохранения изменений.

Назначение контроллера домена

Для назначения данному сайту контроллера домена необходимо на вкладке **Контроллеры домена** нажать кнопку **[+ Назначить контроллер домена]**, будет открыта карточка назначения контроллера домена. В поле **Имя компьютера** из выпадающего списка выбрать компьютер, который будет назначен контроллером домена. Поле **Имя сайта** заполняется автоматически и не доступно для изменения.

Для сохранения нового контроллера необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу и подтвердить сохранение. Будет выполнен переход к списку контроллеров, назначенных сайту.

Для закрытия карточки создания контроллера и возврата к списку контроллеров, назначенных сайту, нажать на кнопку закрытия. В случае, если были введены какие-либо данные, будет запрошено подтверждение закрытия картиочки создания домена без сохранения изменений.

Удаление контроллера домена

Удаление контроллера домена выполняется на его карточке. Для открытия карточки на вкладке **Контроллеры домена** карточки сайта нажать на контроллер домена в списке. Для удаления контроллера нажать кнопку **[Удалить]**.

После удаления контроллера будет выполнен переход на вкладку управления контроллерами ALD Pro (см. *Контроллеры домена*).

Подсистемы сайта

На вкладке **Подсистемы сайта** карточки сайта приводится список подсистем с указанием наименования подсистемы (**Подсистема**), сервера (**Сервер**), состояния (**Состояние**) и версии системы (**Версия ALD Pro**).

Для списка доступна фильтрация по значению **Состояние**. Для фильтрации необходимо кликнуть по значку фильтрации и выбрать значение из выпадающего списка. Для поиска необходимого значения доступен функционал поиска. Для этого в поле **Найти значение** вверху списка, под меню вкладок начать вводить значение. В результате будет обновлен

список фильтрации, отвечающий требованиям поиска.

Состояния соответствуют приведенным в разделе *Состав системы*.

Для списка доступна сортировка по значениям поля **Сервер**.

В левом нижнем углу указано количество подсистем.

Удаление сайта

Удаление сайта осуществляется на его карточке. Для открытия карточки необходимо на вкладке **Сайты и службы** нажать на соответствующий сайт, затем на карточке нажать кнопку **[Удалить сайт]** и в открывшемся окне подтвердить удаление. После удаления сайта будет выполнен переход к списку сайтов.

Важно: Нельзя удалить сайт, к которому привязана хотя бы одна подсистема. При попытке удаления такого сайта появляется сообщение “Удаление невозможно, так как в рамках данного сайта присутствуют подсистемы”.

1.3.2.2. Контроллеры домена

На вкладке осуществляется управление контроллерами домена.

Список контроллеров домена

На вкладке приведен список контроллеров домена с указанием имени компьютера и его IP-адреса, а также имени сайта, которому назначен контроллер домена.

В левом нижнем углу указано количество контроллеров, а в правом нижнем углу располагаются кнопки переключения страниц.

Для списка доступен поиск по названию. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Для просмотра информации о контроллере домена нажать на контроллер домена. Будет открыта карточка контроллера домена с информацией о нем: имя компьютера и сайта, роли компьютера, соглашение о репликации.

Роли компьютера

Роли компьютера показывают администратору функции, которые выполняет компьютер в домене. Роли компьютера отображаются в графическом интерфейсе портала и не связаны с ролевой моделью пользователей. Каждая роль определяется уникальным состоянием записей LDAP.

Описание ролей компьютера:

```
* ``AD Trust Controller`` отображается, если текущий контроллер является
 ↪членом группы sysaccounts;

* ``AD Trust Agent`` отображается, если у ipa-мастера есть запись в LDAP с
 ↪определенными параметрами в `cn=ADTRUST,cn=XXX,cn=masters,cn=ipa,cn=etc,
 ↪dc=XXX`, где `XXX` – имя домена;

* `IPA master`` отображается, если компьютер отвечает за запуск и работу
 ↪служб IPA для обеспечения основных функций: доступ к серверной части LDAP,
 ↪аутентификация Kerberos, HTTP-сервер;

* ``DNS server`` отображается, если контроллер выполняет функции DNS-сервера,
 ↪ DNSKeySync;

* ``Глобальный каталог`` отображается, если контроллер выполняет функции
 ↪глобального каталога;

* ``PKIProxy`` отображается, если котроллер назначается для транслирования
 ↪запроса сертификатов для контроллеров домена и подсистем ALD Pro на любой
 ↪сервис выпуска сертификатов (Удостоверяющий центр).
```

Для просмотра администратором ролей компьютера необходимо открыть **Управление доменом** → **Контроллеры**.

Добавление контроллера домена

Для добавления контроллера домена нажать кнопку **[Новый контроллер домена]**. Будет выполнен переход на карточку добавления нового контроллера домена. На карточке из выпадающего списка **Имя компьютера** выбрать компьютер для назначения роли контроллера домена, затем из выпадающего списка **Имя сайта** выбрать сайт, для которого будет назначен контроллер.

Если контроллеру домена будет назначена роль глобального каталога, необходимо установить флаг **Назначить роль глобального каталога**.

Если контроллеру домена будет назначена роль для транслирования запроса сертификатов для контроллеров домена и подсистем ALD Pro на любой сервис выпуска сертификатов(Удостоверяющий центр), необходимо установить флаг **Назначить роль PKI proxy**.

Для сохранения нового контроллера необходимо нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку контроллеров.

Для закрытия карточки и возврата к списку контроллеров домена нажать на кнопку закрытия.

Важно: Среднее время разворачивания контроллера домена может составлять от 10 до 70 минут, в зависимости от используемой конфигурации.

Удаление контроллера домена

На вкладке **Контроллеры домена** нажать на контроллер домена и в открывшейся карточке с информацией о нем нажать кнопку **[Удалить]**. После удаления будет выполнен переход к списку контроллеров домена.

1.3.2.3. Соглашения о репликации

На вкладке **Соглашения о репликации** осуществляется управление репликациями домена. Наличие соглашения о репликации между двумя доменами ALD Pro означает, что данные двух доменов будут синхронизироваться при изменении с обеих сторон.

Список соглашений о репликации

На вкладке приведен список соглашений о репликации. Каждая строка в списке отображает связь двух контроллеров домена, между которыми настроена репликация. В случае недоступности одного контроллера домена его функции переходят другому контроллеру, с которым было создано соглашение.

Для списка доступен поиск по названию контроллера домена. Для этого начать вводить в поле поиска название, результат поиска будет выводиться по мере ввода.

Для просмотра информации о соглашении нажать на соответствующее соглашение в списке. Будет открыта карточка соглашения с информацией о нем.

В левом нижнем углу указано количество соглашений, а в правом нижнем углу располагаются кнопки переключения страниц.

Создание соглашения о репликации

Для создания соглашения о репликации нажать кнопку **[Новое соглашение]**. Будет открыта карточка создания нового соглашения.

На карточке необходимо из выпадающих списков **Левый узел** и **Правый узел** выбрать контроллеры домена, между которыми необходимо установить соглашение о репликации.

В поле **Название соглашения** задать имя соглашения. Если имя не будет задано, то при сохранении соглашения оно присвоится автоматически.

Для сохранения нового соглашения нажать на кнопку сохранения в правом верхнем углу и подтвердить действие.

Для закрытия карточки нажать кнопку закрытия.

Управление соглашениями о репликации

Управление соглашением осуществляется на его карточке. Для открытия карточки необходимо на вкладке **Соглашения о репликации** нажать на соглашение. На карточке указано название соглашения и контроллеры, между которыми установлено соглашение.

Поля **Левый узел** и **Правый узел** можно переинициализировать, тем самым вернув работоспособность недоступному контроллеру.

Для активации или отмены соглашения, соответственно, установить флаг **Включено** или **Выключено**.

Для закрытия карточки и возврата к списку соглашений нажать кнопку закрытия.

Удаление соглашения о репликации

Удалить соглашения можно из его карточки. Для открытия карточки необходимо на вкладке **Соглашения о репликации** нажать на соглашение списке, затем на карточке нажать кнопку **[Удалить соглашение]**. После подтверждения удаления будет выполнен переход к списку соглашений.

1.3.3. Дополнительные параметры групповых политик

Подраздел содержит функции расширения параметров и атрибутов групповых политик.

1.3.3.1. Параметры компьютеров

На вкладке осуществляется настройка и управление дополнительными параметрами компьютеров.

Каталог дополнительных параметров

На вкладке **Параметры компьютеров** отображен каталог дополнительных параметров, содержащий корневую папку **Дополнительные параметры**.

Внутри корневой папки параметров возможно добавлять параметры компьютеров и дополнительные папки. Папки возможно использовать для группировки параметров по функциональному назначению. Папки и параметры компьютеров отображаются в иерархическом виде.

Корневая папка недоступна для удаления и редактирования. Нельзя создавать объекты на одном уровне с этой папкой.

На вкладке доступен поиск папки или параметра. Для этого в соответствующем поле поиска начать вводить название параметра/папки, результат поиска будет выводиться по мере ввода.

Параметры из каталога дополнительных параметров компьютеров будут отображаться в карточке групповой политики, настраиваемой в подразделе *Групповые политики* (раздел *Групповые политики*).

Управление папками

Создание новой папки

Для создания папки нажать кнопку **[Новая папка]**. Будет открыта карточка создания папки.

На карточке необходимо заполнить обязательные поля **Название папки** и **Родительская папка**. По умолчанию для поля **Родительская папка** указана корневая папка **Дополнительные параметры**, при необходимости ее можно сменить.

Поле **Тип каталога** заполняется автоматически.

Для сохранения новой папки нажать на кнопку сохранения. Будет выполнен переход к каталогу дополнительных параметров.

Для закрытия карточки создания папки и возврата к каталогу дополнительных параметров нажать на кнопку закрытия.

Редактирование папки

Для редактирования папки необходимо выделить папку и нажать на кнопку **[Редактировать]**. Откроется карточка папки, где можно изменить поля **Название папки**, **Тип каталога** и **Родительская папка**.

Для применения изменений нажать на кнопку сохранения.

Для закрытия карточки создания папки и возврата к каталогу дополнительных параметров нажать на кнопку закрытия.

Удаление папки

Для удаления папки необходимо открыть карточку соответствующей папки и нажать на кнопку **[Удалить папку]**. После удаления папки будет выполнен переход к каталогу дополнительных параметров.

Управление параметрами

Добавление параметра

Для добавления параметра необходимо нажать кнопку **[Новый параметр]**. Будет открыта карточка создания нового параметра.

В карточке создания на вкладке **Основное** необходимо заполнить обязательные поля **Название параметра** (например, *Создание файла*), **Уникальный идентификатор** (например, *rbta_ldap_filemanaged*), **Тип параметра**, **Папка параметра**.

В разделе **Требования к ОС** задается информация о том, с какими версиями ОС совместим данный параметр.

Для определения требований к ОС необходимо выбрать в выпадающем списке **Параметр ОС** один из атрибутов, задать значение параметра и выбрать один из следующих операторов сравнения:

- = - точное соответствие;
- ~ - указанная подстрока присутствует в значении;
- *;* - задать несколько требований в ОС, читается через ИЛИ.

Если фильтр не указан, то проверка не выполняется.

В качестве значения в поле **Уникальный идентификатор** задать уникальное имя параметра, которое не совпадает с идентификаторами других параметров.

В поле **Тип параметра** выбор значения **Составной параметр** дает возможность использовать данный параметр множество раз при настройке групповой политики в подразделе *Групповые политики* (раздел *Групповые политики*). Выбор значения **Простой параметр** такую возможность исключает.

В поле **Папка параметра** в качестве значения указывается папка, из которой была нажата кнопка создания нового параметра. При необходимости папку можно изменить.

Поле **Тип каталога** будет заполнено автоматически.

Также можно заполнить поле **Назначение параметра**, указав описание параметра.

Вкладки **Атрибуты параметра** и **Конфигурация скрипта** станут доступны после сохранения параметра (см. *Редактирование параметра*).

Для сохранения нового параметра необходимо нажать кнопку сохранения. Будет выполнен переход к каталогу дополнительных параметров.

Для закрытия карточки создания параметра и возврата к каталогу дополнительных параметров нажать на кнопку закрытия.

Редактирование параметра

Редактирование параметра выполняется на его карточке. Для открытия карточки параметра необходимо в каталоге параметров выделить параметр и нажать кнопку **[Редактировать]**.

На карточке параметра присутствуют вкладки:

- **Основное**;
- **Атрибуты параметра**;
- **Конфигурация скрипта**.

Для закрытия карточки и возврата к каталогу дополнительных параметров нажать на кнопку закрытия.

Основное

На вкладке **Основное** приведена основная информация о параметре (см. *Добавление параметра*). Для редактирования доступны поля **Название параметра**, **Папка параметра** и **Назначение параметра**.

Для сохранения изменений нажать на кнопку сохранения. Будет выполнен переход к каталогу дополнительных параметров.

Атрибуты параметра

Список атрибутов параметра

На вкладке **Атрибуты параметра** приведен список атрибутов данного параметра с указанием их имен, идентификаторов и описания.

Для атрибутов в списке доступен поиск по названию и по идентификатору. Для этого в

поле поиска начать вводить название/идентификатор атрибута, результат поиска будет выводиться по мере ввода.

Добавление атрибута параметра

Для добавления нового атрибута нажать кнопку **[Новый атрибут]**. Будет открыта карточка создания атрибута. В карточке указать обязательные поля **Имя атрибута** (например, *Наименование файла*) и **Идентификатор** (например, *rbta_ldap_filename*). Также можно указать **Описание**.

Для сохранения атрибута нажать на кнопку сохранения. Будет выполнен переход к списку атрибутов.

Для закрытия карточки атрибута и возврата к списку атрибутов нажать на кнопку закрытия.

Редактирование атрибута параметра

Редактирование атрибута выполняется на его карточке. Для открытия карточки необходимо на вкладке **Атрибуты параметра** в списке нажать на атрибут. На карточке возможно изменить название атрибута и его описание.

Атрибут можно сделать обязательным. Атрибуты, отмеченные как **Обязательный**, должны быть заполнены при применении параметра. По умолчанию флаг **Обязательный** снят для нового атрибута параметра.

Атрибут составного параметра можно сделать уникальным, т.е. установить запрет на использование данного имени в параметрах этой или других групповых политик. Для этого необхожимо нажать на кнопку **Сделать уникальным**. Уникальным можно сделать только обязательный атрибут. У параметра может быть только один уникальный атрибут, который используется для разрешения конфликтов при суммировании.

Для сохранения изменений нажать на кнопку сохранения. Будет выполнен переход к списку атрибутов.

Для закрытия карточки и возврата к списку атрибутов нажать на кнопку закрытия.

Удаление атрибута параметра

Удаление атрибута выполняется из его карточки. Для открытия карточки необходимо на вкладке **Атрибуты параметра** в списке нажать на атрибут. Для удаления атрибута нажать кнопку **[Удалить]**.

После подтверждения удаления будет выполнен переход к списку атрибутов.

Конфигурация скрипта

На вкладке **Конфигурация скрипта** в текстовом поле указывается скрипт, выполняемый при включении данного параметра.

Пример скрипта

Описание: скрипт создает файл в директории /opt, содержащий строку “Содержание файла”

```
{% set my_host = salt['grains.get']("nodename") %}
{% if salt['pillar.get']('aldpro-hosts:' + my_host) is defined %}
{% set filename = salt['pillar.get']('aldpro-hosts:' + my_host +
↪':gpid:attrid') %}

create_file:
  cmd.run:
    - name : |
        touch /opt/{{ filename }}.txt
        echo "Содержимое файла" >> /opt/{{ filename }}.txt

{% endif %}
```

Скрипт доступен для редактирования, для этого необходимо нажать кнопку **Редактировать файл**. Для сохранения изменений в скрипте нажать на кнопку сохранения в правом верхнем углу. Для отмены внесения изменений нажать кнопку **[Отменить]**.

Так как выполняется проверка конфигурации скрипта на предмет соблюдения общих правил, при сохранении может возникнуть предупреждение **Ошибка конфигурации скрипта. Игнорировать ошибку и сохранить изменения**. В случае, если автор скрипта уверен в его правильности, необходимо игнорировать данное предупреждение, нажав кнопку **Да**.

Для просмотра истории изменений скрипта нажать кнопку **История изменений**, будет открыта карточка с журналом изменений. Для закрытия карточки нажать на кнопку закрытия.

Удаление параметра

Удаление параметра выполняется из его карточки. Для открытия карточки параметра необходимо в каталоге параметров выделить параметр и нажать кнопку **[Редактировать]**. В карточке параметра нажать кнопку **[Удалить параметр]**.

После подтверждения удаления будет выполнен переход к каталогу дополнительных параметров.

1.3.3.2. Параметры пользователей

На вкладке осуществляется настройка и управление дополнительными параметрами пользователей.

Каталог дополнительных параметров

На вкладке **Параметры пользователей** отображен каталог дополнительных параметров, содержащий корневую папку **Дополнительные параметры**.

Внутри корневой папки параметров возможно добавлять параметры пользователей и дополнительные папки. Папки возможно использовать для группировки параметров по функциональному назначению. Папки и параметры пользователей отображаются в иерархическом виде.

Корневая папка недоступна для удаления и редактирования. Нельзя создавать объекты на одном уровне с этой папкой.

На вкладке доступен поиск папки или параметра. Для этого в соответствующем поле поиска начать вводить название параметра/папки, результат поиска будет выводиться по мере ввода.

Параметры из каталога дополнительных параметров пользователей будут отображаться в карточке групповой политики, настраиваемой в подразделе *Групповые политики* (раздел *Групповые политики*)

Управление папками

Создание новой папки

Для создания папки нажать кнопку **[Новая папка]**. Будет открыта карточка создания папки.

На карточке необходимо заполнить обязательные поля **Название папки** и **Родительская папка**. По умолчанию для поля **Родительская папка** указана корневая папка **Дополнительные параметры**, при необходимости ее можно сменить.

Поле **Тип каталога** заполняется автоматически.

Для сохранения новой папки нажать на кнопку сохранения. Будет выполнен переход к каталогу дополнительных параметров.

Для закрытия карточки создания папки и возврата к каталогу дополнительных параметров нажать на кнопку закрытия.

Редактирование папки

Для редактирования папки необходимо выделить папку и нажать на кнопку **[Редактировать]**. Откроется карточка папки, где можно изменить поля **Название папки**, **Тип каталога** и **Родительская папка**.

Для применения изменений нажать на кнопку сохранения.

Для закрытия карточки создания папки и возврата к каталогу дополнительных параметров нажать на кнопку закрытия.

Удаление папки

Для удаления папки необходимо открыть карточку соответствующей папки и нажать на кнопку **[Удалить папку]**. После удаления папки будет выполнен переход к каталогу дополнительных параметров.

Управление параметрами

Добавление параметра

Для добавления параметра необходимо нажать кнопку **[Новый параметр]**. Будет открыта карточка создания нового параметра.

В карточке создания на вкладке **Основное** необходимо заполнить обязательные поля **Название параметра** (например, *Создание файла*), **Уникальный идентификатор** (например, *rbta_ldap_filemanaged*), **Тип параметра** и **Папка параметра**.

В разделе **Требования к ОС** задается информация о том, с какими версиями ОС совместим данный параметр.

Для определения требований к ОС необходимо выбрать в выпадающем списке **Параметр ОС** один из атрибутов, задать значение параметра и выбрать один из следующих операторов сравнения:

- = - точное соответствие;
- ~ - указанная подстрока присутствует в значении;
- *;* - задать несколько требований в ОС, читается через ИЛИ.

В качестве значения в поле **Уникальный идентификатор** задать уникальное имя параметра, которое не совпадает с идентификаторами других параметров.

В поле **Тип параметра** выбор значения **Составной параметр** дает возможность использовать данный параметр множество раз при настройке групповой политики в подразделе *Групповые политики* (раздел *Групповые политики*). Выбор значения **Простой параметр** такую возможность исключает.

В поле **Папка параметра** в качестве значения указывается папка, из которой была нажата кнопка создания нового параметра. При необходимости папку можно изменить.

Поле **Тип каталога** будет заполнено автоматически.

Также можно заполнить поле **Назначение параметра**, указав описание параметра.

Вкладки **Атрибуты параметра** и **Конфигурация скрипта** станут доступны после сохранения параметра (см. *Редактирование параметра*).

Для сохранения нового параметра необходимо нажать кнопку сохранения. Будет выполнен переход к каталогу дополнительных параметров.

Для закрытия карточки создания параметра и возврата к каталогу дополнительных параметров нажать на кнопку закрытия.

Редактирование параметра

Редактирование параметра выполняется на его карточке. Для открытия карточки параметра необходимо в каталоге параметров выделить параметр и нажать кнопку **[Редактировать]**.

На карточке параметра присутствуют вкладки:

- **Основное**;
- **Атрибуты параметра**;
- **Конфигурация скрипта**.

Для закрытия карточки и возврата к каталогу дополнительных параметров нажать на кнопку закрытия.

Основное

На вкладке **Основное** приведена основная информация о параметре (см. *Добавление параметра*). Для редактирования доступны поля **Название параметра**, **Папка параметра** и **Назначение параметра**.

Для сохранения изменений нажать на кнопку сохранения. Будет выполнен переход к каталогу дополнительных параметров.

Атрибуты параметра

Список атрибутов параметра

На вкладке **Атрибуты параметра** приведен список атрибутов данного параметра с указанием их имен, идентификаторов и описания.

Для атрибутов в списке доступен поиск по названию и по идентификатору. Для этого в поле поиска начать вводить название/идентификатор атрибута, результат поиска будет выводиться по мере ввода.

Добавление атрибута параметра

Для добавления нового атрибута нажать кнопку **[Новый атрибут]**. Будет открыта карточка создания атрибута. В карточке указать обязательные поля **Имя атрибута** (например, *Наименование файла*) и **Идентификатор** (например, *rbta_ldap_filename*). Также можно указать **Описание**.

Для сохранения атрибута нажать на кнопку сохранения. Будет выполнен переход к списку атрибутов.

Для закрытия карточки атрибута и возврата к списку атрибутов нажать на кнопку закрытия.

Редактирование атрибута параметра

Редактирование атрибута выполняется на его карточке. Для открытия карточки необходимо на вкладке **Атрибуты параметра** в списке нажать на атрибут. На карточке возможно изменить название атрибута и его описание.

Атрибут можно сделать обязательным. Атрибуты, отмеченные как **Обязательные**, должны быть заполнены при применении параметра. По умолчанию флаг **Обязательный** снят для нового атрибута параметра.

Атрибут составного параметра можно сделать уникальным, т.е. установить запрет на использование данного имени в параметрах этой или других групповых политик. Для этого необхожимо нажать на кнопку **Сделать уникальным**. Уникальным можно сделать только обязательный атрибут. У параметра может быть только один уникальный атрибут, который используется для разрешения конфликтов при суммировании.

Для сохранения изменений нажать на кнопку сохранения. Будет выполнен переход к списку атрибутов.

Для закрытия карточки и возврата к списку атрибутов нажать на кнопку закрытия.

Удаление атрибута параметра

Удаление атрибута выполняется из его карточки. Для открытия карточки необходимо на вкладке **Атрибуты параметра** в списке нажать на атрибут. Для удаления атрибута нажать кнопку **[Удалить]**.

После подтверждения удаления будет выполнен переход к списку атрибутов.

Конфигурация скрипта

На вкладке **Конфигурация скрипта** в текстовом поле указывается скрипт, выполняемый при включении данного параметра.

Пример скрипта

```
{% if user is not defined %}
  {% set user = salt['pillar.get']("user") %}
{% endif %}
{% set homedir = salt['user.info'](user).home %}

{% set folder_name = salt['pillar.get']('aldpro-users:'+ user +':gpid:attrid
↪') %}

{% if folder_name %}
file_create:
  cmd.run:
    - name : "touch {{ homedir }}/'{{folder_name}}.txt'"

{% endif %}
```

где:

`gpid` - Уникальный идентификатор параметра - значение из поля “Уникальный идентификатор” карточки созданного параметра

`attrid` - Уникальный идентификатор атрибута параметра - значение из поля “Уникальный идентификатор” карточки атрибута созданного параметра.

Скрипт доступен для редактирования, для этого необходимо нажать кнопку **Редактировать файл**. Для сохранения изменений в скрипте нажать на кнопку сохранения в правом верхнем углу. Для отмены внесения изменений нажать кнопку **[Отменить]**.

Так как выполняется проверка конфигурации скрипта на предмет соблюдения общих правил, при сохранении может возникнуть предупреждение **Ошибка конфигурации скрипта. Игнорировать ошибку и сохранить изменения**. В случае, если автор скрипта уверен в его правильности, необходимо игнорировать данное предупреждение, нажав кнопку **Да**.

Для просмотра истории изменений скрипта нажать кнопку **История изменений**, будет открыта карточка с журналом изменений. Для закрытия карточки нажать на кнопку закрытия.

Удаление параметра

Удаление параметра выполняется из его карточки. Для открытия карточки параметра необходимо в каталоге параметров выделить параметр и нажать кнопку **[Редактировать]**. В карточке параметра нажать кнопку **[Удалить параметр]**.

После подтверждения удаления будет выполнен переход к каталогу дополнительных параметров.

> **Внимание:** Названия дополнительных параметров групповых политик должны быть уникальными, в т.ч. относительно списка заданий автоматизации.

1.3.4. Каталог заданий автоматизации

В подразделе представлены функции управления заданиями автоматизации для рабочих станций и серверов.

В подразделе на вкладке **Задания автоматизации** приведен каталог заданий автоматизации, содержащий корневую папку **Задания автоматизации**. Внутри корневой папки дополнительных настроек возможно добавлять задания автоматизации и дополнительные папки. Папки и задания автоматизации отображаются в иерархическом виде.

Корневая папка недоступна для удаления и редактирования. Нельзя создавать объекты на одном уровне с этой папкой.

На вкладке доступен поиск папки или задания. Для этого в соответствующем поле поиска начать вводить название задания/папки, результат поиска будет выводиться по мере ввода.

Данные задания автоматизации будут отображаться в подразделе *Задания автоматизации* (раздел *Автоматизация*).

1.3.4.1. Управление папками

Создание новой папки

Для создания папки необходимо в структуре папок выбрать любую папку и нажать кнопку **[Новая папка]**. Будет открыта карточка создания папки.

На карточке необходимо заполнить обязательные поля **Название папки** и **Родительская папка**. По умолчанию для поля **Родительская папка** указана папка, из которой была нажата кнопка создания папки, при необходимости ее можно сменить.

Для сохранения новой папки нажать на кнопку сохранения. Будет выполнен переход к каталогу дополнительных заданий автоматизации.

Для закрытия карточки создания папки и возврата к каталогу дополнительных заданий автоматизации нажать на кнопку закрытия.

Редактирование папки

Для редактирования папки необходимо выделить папку в структуре и нажать на кнопку **[Редактировать]**. Откроется карточка папки, для редактирования доступны все поля.

Для применения изменений нажать на кнопку сохранения.

Для закрытия карточки создания папки и возврата к каталогу дополнительных заданий автоматизации нажать на кнопку закрытия.

Удаление папки

Для удаления папки необходимо открыть ее карточку и на карточке нажать кнопку **[Удалить папку]**. После удаления папки будет выполнен переход к каталогу дополнительных заданий автоматизации.

1.3.4.2. Управление заданиями

Добавление задания

Для добавления задания необходимо в структуре выбрать папку и нажать кнопку **[Новое задание]**. Будет открыта карточка добавления нового задания.

В карточке добавления задания на вкладке **Основное** необходимо заполнить обязательные поля **Название задания**, **Уникальный идентификатор** и **Родительская папка**. По умолчанию для поля **Родительская папка** указана папка, из которой была нажата кнопка добавления задания, при необходимости ее можно сменить. Также можно заполнить атрибут **Описание**.

Важно: Названия заданий должны быть уникальными, в т.ч. относительно списка кастомных параметров групповых.

После сохранения задания станут доступны для редактирования остальные вкладки (см. *Редактирование задания*).

Для сохранения нового задания необходимо нажать на кнопку сохранения. Будет выполнен переход к каталогу дополнительных заданий автоматизации.

Для закрытия карточки и возврата к каталогу дополнительных заданий автоматизации нажать на кнопку закрытия.

Редактирование задания

Для редактирования задания необходимо в каталоге дополнительных заданий выделить задание и нажать на кнопку **[Редактировать]**. Будет открыта карточка задания.

На карточке задания присутствуют вкладки:

- **Основное**;
- **Атрибуты задания**;
- **Конфигурация скрипта**.

Для закрытия карточки задания и возврата к каталогу дополнительных заданий автоматизации нажать на кнопку закрытия.

Основное

На вкладке **Основное** приведена основная информация о задании. Для редактирования доступны поля **Название задания** (например, *Создать новый файл*), **Уникальный идентификатор** (например, *createafile*), **Родительская папка** и **Описание**.

Для сохранения изменений нажать на кнопку сохранения. Будет выполнен переход к каталогу дополнительных заданий автоматизации.

Атрибуты задания

Список атрибутов задания

На вкладке **Атрибуты задания** приведен список атрибутов данного задания с указанием их имен, идентификаторов и описания.

Данные атрибуты будут использоваться в качестве параметров задания. Значения этих параметров будут задаваться при запуске задания автоматизации на вкладке **Каталог заданий автоматизации** в подразделе *Задания автоматизации* (раздел *Автоматизация*).

Для атрибутов в списке доступен поиск по названию и по идентификатору. Для этого в поле поиска начать вводить название/идентификатор атрибута, результат поиска будет выводиться по мере ввода.

Добавление атрибута задания

Для добавления нового атрибута нажать кнопку **[Новый атрибут]**. Будет открыта карточка создания атрибута. В карточке заполнить обязательные поля **Название атрибута** (например, *Содержимое файла*) и **Уникальный идентификатор** (например, *content*). Также можно указать **Описание**.

Для сохранения атрибута нажать на кнопку сохранения. Будет выполнен переход к списку атрибутов.

Для закрытия карточки атрибута и возврата к списку атрибутов нажать на кнопку закрытия.

Редактирование атрибута задания

Редактирование атрибута выполняется на его карточке. Для открытия карточки необходимо на вкладке **Атрибуты задания** в списке нажать на атрибут. На карточке возможно изменить название атрибута и его описание.

Для сохранения изменений нажать на кнопку сохранения. Будет выполнен переход к списку атрибутов.

Для закрытия карточки и возврата к списку атрибутов нажать на кнопку закрытия.

Удаление атрибута задания

Удаление атрибута выполняется из его карточки. Для открытия карточки необходимо на вкладке **Атрибуты задания** в списке нажать на атрибут. Для удаления атрибута нажать кнопку **[Удалить атрибут]**.

После подтверждения удаления будет выполнен переход к списку атрибутов.

Конфигурация скрипта

На вкладке **Конфигурация скрипта** в текстовом поле указывается скрипт, выполняемый при выполнении данного задания.

Пример

```
{% set vars1 = salt['pillar.get']("content") %}
test:
  cmd.run:
    - name: |
        echo {{ vars1 }} > /opt/test.txt
    - failhard: True
```

Скрипт доступен для редактирования, для этого необходимо нажать кнопку **Редактировать файл**. Для сохранения изменений в скрипте нажать на кнопку сохранения в правом верхнем углу. Для отмены внесения изменений нажать кнопку **[Отменить]**.

Для просмотра истории изменений скрипта нажать кнопку **История изменений**, будет открыта карточка с журналом изменений. Для закрытия карточки нажать на кнопку

закрытия.

1.3.4.3. Удаление задания

Удаление задания выполняется из его карточки. Для открытия карточки задания необходимо в каталоге дополнительных заданий автоматизации выбрать задание и нажать кнопку **[Редактировать]**. В карточке задания нажать кнопку **[Удалить задание]**.

После подтверждения удаления будет выполнен переход к каталогу дополнительных заданий автоматизации.

1.3.5. Службы и параметры Kerberos

Подраздел отображает функции управления службами Kerberos (те службы ALD Pro, где необходима аутентификация пользователя через действующий TGT-билет) и политикой билетов Kerberos.

1.3.5.1. Политика билетов Kerberos

На вкладке приведены поля для установки значений следующих настроек политики билетов Kerberos:

- **Максимальный срок для обновления (в секундах)** — срок, до наступления которого можно продлевать срок действия билета. Значение по умолчанию 604 800 секунд;
- **Максимальный срок жизни (в секундах)** — срок действия билета. Значение по умолчанию 86 400 секунд.

Максимально возможное значение для установки 2 147 483 647 секунд.

Для сохранения изменений нажать на кнопку сохранения в правом верхнем углу.

Чтобы вернуть настройки по умолчанию необходимо нажать кнопку **[Сбросить по умолчанию]**.

1.3.5.2. Службы Kerberos

На вкладке осуществляется управление службами. Доступно добавление новых служб, настройка и управление службами, а также удаление служб.

Список служб

На вкладке приводится список служб с указанием имени учетной записи.

Для служб в списке доступен поиск по названию атрибутов. Для этого в поле поиска начать вводить название/идентификатор атрибута, результат поиска будет выводиться по мере ввода.

Для просмотра информации о службе нажать на соответствующую службу в списке. Будет открыта карточка службы с информацией о ней.

В левом нижнем углу указано количество служб, а в правом нижнем углу располагаются кнопки переключения страниц.

Добавление службы

Для добавления новой службы нажать кнопку **[+ Новая служба]**. Будет выполнен переход на карточку новой службы.

На карточке из выпадающего списка **Класс службы** выбрать службу, затем из выпадающего списка **Имя компьютера** выбрать компьютер, на котором она будет запущена.

Для сохранения новой службы необходимо нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к карточке настройки службы (см. *Управление службой*).

Для закрытия карточки службы и возврата к списку служб нажать на кнопку закрытия.

Управление службой

Управление службой осуществляется на ее карточке. Карточка открывается при нажатии на службу в списке служб.

Настройка службы

На карточке службы приведено присвоенное автоматически имя учетной записи службы, информация о классе службы и имени компьютера, на котором запущена служба. Данная информация недоступна для редактирования.

Для настройки доступны следующие пункты:

- **Доверено для делегирования**;
- **Доверие для аутентификации в качестве пользователя**;
- **Требуется предварительная аутентификация**.

Для включения/выключения соответствующей возможности установить/снять флаг в пункте.

Состояние службы определяется пунктом **Имеется ключ Kerberos, служба подготовлена к работе**. Если для службы создан контейнер ключа Kerberos, то отметка в пункте ставится автоматически, и служба готова к работе.

Добавление сертификата

Сертификат Kerberos возможно добавить двумя способами:

- загрузить сертификат в формате base64 или PEM из файла;
- ввести ключ сертификата вручную.

Для загрузки сертификата из файла нажать на кнопку **[Добавить из файла]**, в открывшемся окне навигации выбрать необходимый файл и затем в карточке нажать **[Сохранить]**. Система преобразует выбранный файл в необходимый формат. После успешной загрузки сертификата отобразятся даты начала и окончания действия сертификата, а также ключ сертификата.

Для ввода ключа сертификата вручную необходимо ввести его в поле **Введите ключ сертификата** и нажать **[Сохранить]**. После успешной загрузки сертификата отобразятся даты начала и окончания действия сертификата.

Одновременно можно установить только один сертификат. Для добавления нового сертификата с обновленным сроком действия необходимо удалить действующий сертификат и затем добавить новый.

Удаление сертификата

Удаления сертификата службы (например, при замене на сертификат с новым сроком действия) выполняется из карточки службы. Необходимо открыть карточку нажатием на службу в списке служб, затем на карточке нажать кнопку **[Удалить]**.

Для закрытия карточки службы и возврата к списку служб нажать на кнопку закрытия.

Удаление службы

Для удаления службы или одновременно несколько служб необходимо на вкладке **Службы** в списке отметить требуемые службы и нажать кнопку **[Удалить]**.

Чтоб отметить все имеющиеся службы — отметить пункт **Имя учетной записи**.

Также удалить службу можно из ее карточки: открыть карточку нажатием на службу в списке служб, затем на карточке нажать кнопку **[Удалить службу]**. После подтверждения удаления будет выполнен переход к списку служб.

1.3.6. Пользователи и группы

В подразделе выполняется управление параметрами пользователей и групп, а также расширение списка дополнительных атрибутов пользователей.

Подраздел состоит из вкладок:

- **Параметры пользователей**;
- **Параметры групп**;
- **POSIX идентификаторы**;
- **Атрибуты пользователей**.

1.3.6.1. Параметры пользователей

На вкладке приводятся значения параметров пользователей, которые будут использоваться по умолчанию при добавлении новых пользователей.

Параметры пользователей, обязательные для заполнения (заполняются автоматически

после развертывания контроллера домена, при необходимости могут быть изменены):

- **Группа пользователей по умолчанию** — указывается наименование группы пользователей, в которую добавляются все новые пользователи;
- **Основа домашних каталогов** — указывается директория, в которой будут создаваться домашние папки пользователей при первой авторизации на клиентском компьютере;
- **Оболочка по умолчанию** — указывается оболочка, которая будет отображена при работе в терминале;
- **Максимальная длина имени пользователя** — задается максимальная длина имени учетной записи пользователя;
- **Уведомление об окончании действия пароля (в днях)** — настраивается за сколько дней до истечения срока действия пароля уведомлять пользователя о необходимости сменить пароль.

Важно: Для корректной работы пользователя на портале управления **ALD Pro** при чтении информации о группах пользователей или работе пользователя с **API** по получению данных о группах пользователей рекомендуется оставить значение `ipausers` для поля **Группа пользователей по умолчанию**. Если такой возможности нет – необходимо, чтобы роль, назначенная пользователю, включала в себя привилегию `User groups - Read`.

Дополнительно можно указать следующие параметры:

- заполнить поля **Почтовый домен по умолчанию** и **Порядок разрешения доменов** - разделенный двоеточиями список доменов, которые используются для обработки кратких имен. По умолчанию поле не заполнено, т.к. используется контроллер домена;
- в блоке **Возможности подключаемого модуля пароля** отметить требуемые возможности:
  - **AllowNThash** (отключен по умолчанию. Параметр необходим в случае использования траста с MS AD. Хэш NT будет записан в атрибуты sambaNTPassword и/или ipaNTHash во время смены пароля);
  - **KDC:Disable Last Success** (отслеживание последней успешной аутентификации пользовательских аккаунтов отключено по умолчанию во FreeIPA для уменьшения нагрузки на серверы, отключено . Если параметр активировать, то вырастет нагрузка на контроллеры домена);

  - **KDC:Disable Lockout** (отключение блокировки учетной записи при неверном вводе пароля. По умолчанию опция отключена, т.е. учетные записи будут блокироваться);
- при необходимости отметить пункт **Включить режим миграции**.

В списке **Выбранные объектные классы** приведены объектные классы, которые будут отображаться в карточке пользователя.

Чтобы добавить объектные классы для отображения необходимо в списке **Все объектные классы** отметить требуемые классы и перенести их в список **Выбранные объектные классы** нажатием кнопки **[<-]**.

Чтобы исключить объектные классы необходимо в списке **Выбранные объектные классы** отметить требуемые классы и перенести их в список **Все объектные классы** нажатием кнопки **[→]**.

Для списков объектных классов доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списков указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

1.3.6.2. Параметры групп

На вкладке приводятся значения параметров групп пользователей, которые будут использоваться по умолчанию при добавлении новых групп.

В списке **Выбранные объектные классы** приведены объектные классы, которые будут отображаться в карточке группы.

Чтобы добавить объектные классы для отображения необходимо в списке **Все объектные классы** отметить требуемые классы и перенести их в список **Выбранные объектные классы** нажатием кнопки **[<-]**.

Чтобы исключить объектные классы необходимо в списке **Выбранные объектные классы** отметить требуемые классы и перенести их в список **Все объектные классы** нажатием кнопки **[→]**.

Для списков объектных классов доступен поиск по названию. Для этого в соответствующем

поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списков указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

1.3.6.3. POSIX идентификаторы

На вкладке осуществляется управление диапазонами идентификаторов.

Список диапазонов

На вкладке приведен список с указанием имени диапазона, первого идентификатора POSIX диапазона и общего количества идентификаторов в диапазоне.

Для списка доступен поиск по имени диапазона, первому идентификатору и количеству идентификаторов. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество записей в списке.

Добавление диапазона

Для добавления нового диапазона необходимо нажать на кнопку **[Новый диапазон]**, будет выполнен переход на карточку нового диапазона.

На карточке заполнить обязательные поля **Имя диапазона**, **Основной ID**, **Размер диапазона**, **Основа основного RID** и **Основа вторичного RID**.

Для сохранения нового диапазона необходимо нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку диапазонов.

Для закрытия карточки и возврата к списку диапазонов нажать на кнопку закрытия.

Удаление диапазона

Для удаления диапазона или одновременно несколько диапазонов необходимо в списке отметить требуемый диапазон и нажать кнопку **[Удалить диапазон]**.

1.3.6.4. Атрибуты пользователей

Список атрибутов

На вкладке приведен список атрибутов пользователей с указанием имени атрибута, типа данных атрибута и статуса атрибута.

Данные атрибуты будут определять поля для заполнения на вкладке **Дополнительные сведения** карточки пользователя в подразделе *Пользователи* (раздел *Пользователи и компьютеры*).

Для списка доступен поиск по имени и типу данных атрибута. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество записей в списке.

Добавление атрибута

Для добавления нового атрибута необходимо нажать на кнопку **[Новый атрибут]**, будет выполнен переход на карточку нового атрибута.

На карточке заполнить обязательные поля **Имя атрибута** (например, *Дата рождения*) и **Тип данных атрибута**. Пункт **Статус атрибута** отмечается автоматически и не может быть изменен.

Для сохранения нового атрибута необходимо нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку атрибутов.

Для закрытия карточки и возврата к списку атрибутов нажать на кнопку закрытия.

Удаление атрибута

Удаление атрибута выполняется на его карточке. Для открытия карточки необходимо в списке нажать на соответствующий атрибут, затем на карточке нажать кнопку **[Удалить атрибут]**. После подтверждения удаления будет выполнен переход к списку атрибутов.

1.3.7. Интеграция с доменами

1.3.7.1. Доверительные отношения

В подразделе представлены функции управления доверительными отношениями с доменами ALD Pro и Microsoft Active Directory (MS AD).

На вкладке подраздела приведен список доменов ALD Pro и MS AD, к которым выполнено подключение данным доменом.

Подключения к домену находятся в одном из трех состояний, указанные в столбце **Тип доверия**:

- входящие: доверительные отношения установлены для данного домена ALD Pro касательно пользователей другого домена ALD Pro или MS AD (ALD Pro имеет доступ к пользователям другого домена ALD Pro или MS AD). Входящее доверие нельзя создать на данном домене, оно создается автоматически, при создании исходящего доверия на другом домене с данным доменом;
- исходящие: доверительные отношения установлены для другого домена ALD Pro или MS AD касательно пользователей данного домена ALD Pro (другой домен ALD Pro или MS AD имеет доступ к пользователям ALD Pro);
- двусторонние: доверительные отношения установлены между другим доменом ALD Pro или MS AD и данным доменом ALD Pro.

После установки доверительных отношений между доменами пользователи Active Directory получают возможность авторизоваться на рабочих станциях в домене ALD Pro, используя свои идентификаторы в домене Active Directory.

Для списка доступен поиск по названию домена. Для этого в поле поиска начать вводить название, результат поиска будет выводиться по мере ввода. Список может быть отфильтрован по типу домена (**ALD Pro** или **MS AD**) и по типу доверия.

Справа от поисковой строки расположена кнопка **[+ Новое подключение]**.

В левом нижнем углу указано количество доменов, а в правом нижнем углу кнопки переключения страниц.

Создание нового подключения

Для установки доверительных отношений с новым доменом необходимо нажать на кнопку **[+ Новое подключение]**.

В карточке подключения в разделе **Настройка доверенного домена** указать:

- **Имя домена**: имя домена, с которым устанавливаются доверительные отношения, без указания контроллера домена;
- **Тип домена**: тип домена **ALD Pro** или **MS AD**, выбирается вручную в соответсвие с типом домена, с которым устанавливаются доверительные отношения. При выборе некорректного типа домена доверительные отношения установлены не будут;
- **Учетная запись**: учетная запись, под которой устанавливаются доверительные отношения, должна принадлежать домену, с которым устанавливаются доверительные отношения и обладать правами на установку доверительных отношений;
- **Пароль**: пароль учетной записи домена, с которым устанавливаются доверительные отношения;
- **Подтверждение пароля**.

В разделе **Настройки доверия** выбрать тип доверия: двусторонние или исходящие.

Для сохранения нового подключения необходимо нажать на кнопку **+ Добавить** в правом нижнем углу.

Для закрытия карточки и возврата к списку доменов нажать на кнопку закрытия.

Важно: Установление доверительных отношений (ДО) с доменами **MS AD** требует дополнительных действий.

Перед установкой ДО на всех контроллерах домена **ALD Pro** необходимо выполнить команды:

```
sudo net conf setparm global "restrict anonymous" "0"
```

```
sudo aldproctl restart -i
```

После необходимо создать на портале управления **ALD Pro** ДО с доменом **MS AD**.

Затем на каждом контроллере домена **ALD Pro** необходимо выполнить команду:

```
rm /var/lib/sss/db/* && systemctl restart sssd
```

Для сохранения нового подключения необходимо нажать на кнопку **[+ Добавить]** в правом верхнем углу.

Для закрытия карточки и возврата к списку подключений следует нажать на кнопку **[X]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Редактирование подключения

Созданное подключение нельзя редактировать. Для внесения изменений в подключение необходимо удалить и создать заново.

Удаление подключения

Для удаления подключения на вкладке **Доверительные отношения** необходимо выбрать домен, отношения с которым необходимо разорвать, и нажать на кнопку **[Удалить]**. После подтверждения удаления домен пропадет из списка.

Внимание: При удалении доверительных отношений с доменом **ALD Pro** требуется дополнительное подтверждение. Необходимо ввести данные учетной записи (логин и пароль) домена, с которым удаляются отношения. Учетная запись должна обладать правами на управление доверительными отношениями.

1.3.7.2. Миграции MS AD

Внимание: В следующей версии ALD Pro LTS данный функционал будет исключен из портала управления. Для синхронизации объектов из домена MS AD необходимо использовать модуль синхронизации.

В подразделе представлены функции управления миграцией LDAP-объектов службы каталогов Microsoft Active Directory – пользователей, группы пользователей и подразделения в домен ALD Pro. Также, можно настроить правила переноса атрибутов, поскольку структура LDAP-объектов в MS AD и ALD Pro отличается.

Внимание: Для управления миграцией объектов из MS AD, учетная запись пользователя должна обладать соответствующей привилегией и должна быть добавлена в группы пользователей `trust admins` и `ald trust admin`.

Важно: Необходимо использовать Модуль синхронизации вместо функционала Миграции MS AD, так как Модуль синхронизации имеет ряд преимуществ:

1. Непрерывная синхронизация изменений из MS AD в отличие от разовой миграции.
2. Возможность синхронизации любых атрибутов объектов MS AD (в миграции список атрибутов ограничен).
3. Возможность настроить двустороннюю синхронизацию паролей пользователей между доменами ALD Pro и MS AD.
4. Возможность проверки потенциальных ошибок синхронизации посредством функционала «Проверка конфликтов синхнронизации».
5. Отслеживание объектов синхронизации и их конфликтов через дерево синхронизации.

Миграция объектов Active Directory

При выборе пункта **Миграция объектов Active Directory** отобразятся обязательные для заполнения поля **Учетная запись для миграции**, **Пароль пользователя**, **Подтверждение пароля**, **Базовое уникальное имя (base DN)**, **Имя домена** и **Контроллер домена**.

Имя домена - это имя контроллера домена Active Directory.

Значеине в поле **Контроллер домена** необходимо указать в формате:

```
protocol://имя.контроллера.домена:порт
```

Учетная запись для миграции должна быть заведена в домене Active Directory и должна обладать правами администратора домена.

Поле **Базовое уникальное имя (base DN)** определяет откуда начинать поиск объекта в Active Directory.

В поле **Базовое уникальное имя (base DN)** указывается имя домена в формате:

```
dc=поддомен_1,dc=поддомен_2,dc=основное_имя_сайта,dc=доменная_зона
```

Например, для домена `win-ad.subdomain.ald.pro` указывается:

```
dc=win-ad,dc=subdomain,dc=ald,dc=pro
```

Для выполнения можно отметить пункт **Игнорировать ошибки SSL**.

Перенаправление зоны DNS

Перенаправление позволяет посылать запросы для домена на определенный DNS-сервер.

Для корректной работы миграции необходимо настроить зоны перенаправления (см. *Перенаправление запросов*).

Создание миграции MS AD

Создание миграции **MS AD** выполняется на вкладке **Миграции MS AD** раздела **Интеграция с доменами**. Для создания нового подключения необходимо нажать кнопку **[+**

Новая миграция].

Появится карточка создания новой миграции, которая содержит столбцы **Настройки домена MS AD** и **Настройки учетной записи MS AD**, все поля ввода в столбцах обязательны к заполнению.

- Имя домена - имя домена **MS AD**.
- Контроллер домена - имя контроллера домена **MS AD** в формате **FQDN**.
- Базовое уникальное имя (**base DN**) - **RDN** (относительное уникальное имя) домена **MS AD**.

Например, для домена **MS AD** `win12.domain.local.ru` **RDN** будет иметь значение `dc=win12`, `dc=domain`, `dc=local`, `dc=ru`.

- Учетная запись для миграции - учетная запись домена **MS AD**, обладающая правами администратора.
- Пароль и Подтверждение пароля - пароль от учетной записи **MS AD**.

Для сохранения новой миграции необходимо нажать на кнопку **[+ Добавить]** в правом верхнем углу.

Для закрытия карточки и возврата к списку подключений следует нажать на кнопку **[X]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Настройка миграции MS AD

Настройка миграции осуществляется на карточке **Миграция домена**. Для ее открытия необходимо выбрать миграцию и нажать кнопку **[Настроить и запустить миграцию]**.

Появится карточка миграции домена, которая содержит столбцы **Настройки миграции** и **Учетная запись администратора**, все поля ввода в столбцах обязательны к заполнению.

- Подразделение **Active Directory** - список подразделений **MS AD** из которых можно мигрировать объекты.
- Подразделение **ALD Pro** - список подразделений **ALD Pro** из которых можно мигрировать объекты.
- Объекты миграций - выбор типов объектов, которые будут мигрированы.

При выборе объекта миграции **Пользователи** появится дополнительное поле **Пароль**

пользователя, в котором необходимо указать временный пароль, который предоставляется всем мигрированным пользователям. При первой авторизации пользователю или администратору необходимо сбросить пароль.

- Учетная запись для миграции - учетная запись домена **MS AD**, обладающая правами администратора.
- Пароль - пароль от учетной записи **MS AD**.

После заполнения нажать **[Запустить миграцию]**.

Для закрытия карточки и возврата к списку подключений следует нажать на кнопку **[X]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Редактирование подключения к Active Directory

Редактирование подключения к Active Directory выполняется на его карточке. Для открытия карточки необходимо на вкладке **Миграция MS AD** нажать на соответствующий домен в списке.

Для закрытия карточки и возврата к списку нажать на кнопку закрытия.

На вкладке настраивается сопоставление полей домена Active Directory с полями домена ALD Pro при выполнении миграции.

Список миграций

На вкладке приведен список настроенных сопоставлений с указанием поля в домене Active Directory, соответствующего поля в домене ALD Pro и относящегося к ним объекта миграции.

Для списка доступен поиск по названиям полей доменов. Для этого в поле поиска начать вводить название, результат поиска будет выводиться по мере ввода.

В левом нижнем углу указано количество записей в списке, а в правом нижнем углу кнопки переключения страниц.

Новое сопоставление полей миграции

Для создания нового сопоставления полей миграции необходимо выбрать подключение к домену, нажать на кнопку **[Редактировать]**, будет выполнен переход на карточку нового сопоставления.

На карточке необходимо в поле **Атрибут AD** указать поле домена Active Directory, в поле **Атрибут ALD Pro** указать поле домена ALD Pro и в выпадающем списке **Объект миграции** выбрать тип объекта.

Для сохранения новой миграции необходимо нажать на кнопку **[+ Добавить]** в правом верхнем углу.

Для закрытия карточки и возврата к списку подключений следует нажать на кнопку **[X]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Удаление сопоставления полей миграции

Для удаления сопоставления полей миграции или несколько сопоставлений одновременно необходимо в списке отметить требуемые сопоставления и нажать кнопку **[Удалить]**.

Чтоб отметить все имеющиеся сопоставления — отметить пункт **Атрибут Active Directory**.

Запуск миграции

Для запуска миграции из данного домена Active Directory необходимо выбрать подключение к домену, нажать кнопку **[Настроить и запустить миграцию]**, будет выполнен переход на карточку запуска миграции.

На карточке в обязательных для заполнения выпадающих списках необходимо выбрать из какого подразделения Active Directory в какое подразделение ALD Pro будет выполнена миграция.

При необходимости отметить требуемые объекты миграции. При выборе пункта **Пользователи** необходимо ввести пароль. Пароль должен соответствовать политике паролей ALD Pro по умолчанию. Контроль соответствия пароля политике возлагается на администратора.

Затем необходимо заполнить поля **Логин администратора ALD Pro** и **Пароль администратора ALD Pro**. Учетная запись должна обладать правами администратора домена.

Для сохранения новой миграции необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу.

Для закрытия карточки и возврата к списку подключений следует нажать на кнопку **[X]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Удаление подключения к Active Directory

Удаление подключения к Active Directory выполняется на его карточке. Для открытия карточки подключения необходимо в списке подключений на вкладке **Миграция объектов Active Directory** нажать на подключение, затем нажать на кнопку **Удалить**. После подтверждения удаления будет выполнен переход к списку подключений.

Важно: При удалении подключения к Active Directory, связанная с ним зона DNS не будет удалена автоматически. Удаление такой зоны DNS осуществляется только в ручном режиме (при необходимости).

1.3.8. Роли и права доступа

В подразделе приведены функции управления зонами ответственности при администрировании к разделам и функциям системы.

1.3.8.1. Возможности учетной записи пользователя

По умолчанию любой пользователь с учетной записью и без назначенных ему ролей в портале управления **ALD Pro** имеет доступ к следующей информации:

- **Личный кабинет портала управления ALD Pro:**
  - просмотр информации о своей учетной записи (данные с вкладки **Основное** карточки пользователя);

  - изменение мобильного телефона, открытых ключей SSH и пароля;
- Чтение информации и ряд операций с использованием **API ALD Pro**.

1.3.8.2. Права на операции в портале управления

Привилегии

Чтобы разрешить пользователю дополнительные (помимо доступных по умолчанию любой учетной записи без ролей) действия в портале управления, необходимо выдать ему привилегии на требуемые операции. На каждую операцию или группу операций в портале управления есть соответствующая привилегия.

Привилегии выдаются на:

- Чтение (Read);
- Создание (Create или Add);
- Измение (Modify);
- Удаление (Drop или Delete);
- Полные права: создание, изменение, удаление (Manage).

Каждая привилегия в составе роли позволяет выполнять определенные действия в конкретном подразделе портала управления. Полный перечень привилегий доступен в *Матрица и описание привилегий*.

Для выполнения некоторых действий в портале управления одной выбранной привилегии может быть недостаточно. Поэтому для корректной работы необходимо добавление дополнительных (связанных) привилегий.

При добавлении каждой привилегии в роль выполняется автоматическая проверка на наличие связанных с ней привилегий. Если связанные привилегии есть, отображается их перечень. Необходимо ознакомиться со списком дополнительных привилегий и убедиться, что их наличие в роли допускается. Связанные привилегии будут добавлены в роль только после подтверждения. Если добавление связанных привилегий не будет подтверждено, активация роли завершится с ошибкой.

Добавление связанных привилегий можно выполнить в любой момент до активации роли. Все привилегии, требующие внимания, отмечены в списке привилегий роли информационным значком.

Роли

Привилегии выдаются в составе ролей. Роли назначаются (делегируются) пользователям напрямую или могут наследоваться пользователями от групп, в которых они состоят.

На одного пользователя (группу пользователей) можно назначить несколько ролей. Тогда привилегии пользователя на операции в протале управления будут суммироваться по всем назначенным ему ролям и ролям, унаследованных от групп.

Внимание: Использование циклических (замкнутых) наследований групп пользователей будет приводить к некорректной работе механизма управления доступом на основе ролей в связи с особенностями работы с такими зависимостями. Будут учитываться только вложенные группы первого уровня. Создание таких наследований в продуктивных средах не рекомендуется.

На пользователей (группы пользователей) с помощью портала управления **ALD Pro** можно назначать роли с типами:

- Предустановленная;
- Пользовательская.

Все варианты ролей, доступных по умолчанию в портале управления, описаны в документе «Матрица и описание ролей».

Внимание: Назначение предустановленных ролей, созданных НЕ с помощью интерфейса **ALD Pro** (cli или web-интерфейс **FreeIPA**), не будет подчиняться дополнительным ограничениям по подразделениям, которые актуальны для ролей, созданных в интерфейсе **ALD Pro**. Таким образом, пользователь, которому назначена роль с привилегией **Roles Membership - Manage** с ограничением на любое подразделение домена, сможет управлять членством любых пользователей в любых ролях, созданных вне интерфейса **ALD Pro**. Для корректной работы рекомендуется создание всех ролей с помощью портала управления **ALD Pro**.

1.3.8.3. Возможности для ограничения областей действия ролей и привилегий

В **ALD Pro** существует возможность ограничения областей действия ролей и привилегий.

Область действия роли - это совокупность привязки роли к подразделению и признака **Включая дочерние подразделения**. Если признак **Включая дочерние подразделения** не выбран, то область действия роли будет ограничена указанным подразделением. Если признак **Включая дочерние подразделения** выбран, то область действия роли будет ограничиваться всеми подразделениями ниже в иерархии, начиная с указанного подразделения.

Область действия привилегии наследуется от роли. Но есть исключения:

- Привилегии, которые не могут быть ограничены подразделением. Независимо от того, какая привязка указана для роли, в состав которой входит привилегия, такая привилегия всегда будет действовать на весь домен.
- Привилегии, которые могут быть ограничены и подразделением, и сайтом. Это привилегии на администрирование сервисов и подсистем. Для таких привилегий привязка к сайту указывается в свойствах самой привилегии в составе роли и от роли не наследуется. В роль можно включить несколько одинаковых привилегий с привязками к разным сайтам (одна привилегия - один сайт) или одну привилегию с привязкой ко всем сайтам домена. При этом привязку к подразделению такие привилегии будут наследовать от роли.

Если привилегия назначена пользователю в составе нескольких ролей с разными областями действия, то суммарная область действия привилегии для пользователя будет складываться из областей действия всех его ролей с этой привилегией.

1.3.9. Мандатное управление доступом (МРД)

Мандатное управление доступом представляет собой подход к управлению безопасностью в информационных системах, при котором система сама определяет и принимает решения о предоставлении или ограничении доступа к ресурсам в зависимости от заданных правил безопасности.

В подразделе выполняется поддержка МРД, настройка классификаторов уровней и категорий конфиденциальности и настройка их для пользователя.

Поддержка МРД включает в себя применение политик безопасности, ведение журналов

аудита и контроль за перемещением информации между уровнями доступа. Настройка уровней и категорий для пользователя дает возможность точно определить, к каким ресурсам системы пользователь имеет право получить доступ, что минимизирует риски несанкционированного доступа к защищаемой информации.

1.3.9.1. Модель мандатного управления доступом

Модель МРД основана на правилах WURD (write up, read down) — субъекты могут записывать только в объекты с уровнем конфиденциальности равным или выше своего, а читать только из объектов с уровнем равным или ниже своего. В Astra Linux используется МРОСЛ ДП-модель, которая объединяет мандатное управление доступом (МРД), мандатный контроль целостности (МКЦ) и дискреционное управление доступом.

1.3.9.2. Уровни конфиденциальности

Классификаторы уровней определяют иерархическую структуру допуска к информации по степени секретности. Уровни конфиденциальности представляют целые числа от 0 до 255 с текстовыми наименованиями. По умолчанию создается четыре уровня (0-3), где 0 означает отсутствие конфиденциальности. Администратор может добавлять новые уровни, при этом рекомендуется использовать значения 10, 20, 30 вместо 1, 2, 3 для возможности вставки промежуточных уровней. Для работы с уровнями выше 3 необходимо изменить параметр sysmaclev в /usr/sbin/pdp-init-fs и перезагрузить систему.

1.3.9.3. Категории конфиденциальности

Категории конфиденциальности — неиерархические метки от 0 до 63 с текстовыми наименованиями, позволяющие разделять доступ к информации по функциональным областям и рабочим группам. В метках безопасности набор категорий задается 64-битным числом в шестнадцатеричном формате, где каждый бит соответствует отдельной категории. Пользователь с несколькими категориями может читать файлы с любой из них, но записывать только в файлы со всеми своими категориями одновременно.

1.3.9.4. Делегирование прав обычному пользователю

Чтобы назначить пользователя администратором мандатного разграничения доступа (МРД), необходимо назначить ему следующие привилегии:

- `PARSEC_CAP_CHMAC` — дает право изменять метки безопасности;
- `PARSEC_CAP_IGNMACLVL` — для обхода контроля уровней конфиденциальности (рекомендуется);
- `PARSEC_CAP_IGNMACCAT` — для обхода контроля категорий конфиденциальности (рекомендуется).

1.3.9.5. Ограничения делегированных прав

Пользователь может потерять доступ к объекту, если назначит ему метку безопасности выше своей. Утилиты администрирования доступны по абсолютному пути `/sbin/pdpl-file`. Полное администрирование мандатного контроля целостности (МКЦ) доступно только пользователю root с максимальным уровнем целостности `max_ilev` (63).

1.3.9.6. Управление метками безопасности

Для назначения меток используется утилита pdpl-file с синтаксисом:

```
pdpl-file [Уровень_МРД]:[Уровень_МКЦ:[Категории_МРД:[Флаги]]] Имя_объекта
```

где:

- Уровень **МРД** — уровень конфиденциальности, который задается как именем (например, «Совершенно_секретно»), так и числом в обычной десятичной системе счисления (например, «2»). Если значение будет не задано, то по умолчанию назначается нулевой уровень МРД.
- Уровень **МКЦ** — уровень целостности, который задается как именем (например, «Высокий»), так и числом в обычной десятичной системе счисления (например, «63»). Если значение будет не задано, то по умолчанию назначается нулевой уровень МКЦ.
- Категории **МРД** — список категорий конфиденциальности, которые можно перечислить как по именам через запятую (например, «Мотострелковые_войска,Танковые_войска»), так и задать одним числом в шестнадцатеричной системе счисления (например, 0x3).

Если значение не задано, то по умолчанию метка безопасности будет без категорий конфиденциальности. Если нужно задать сразу все доступные категории (значение `sysmaxcat`), то можно использовать специальное значение «-1». Процессы наследуют метки от родительских процессов, изменить метку может только администратор через утилиту `pdp-exec`.

1.3.9.7. Контейнеры объектов

По умолчанию действует политика **CCR** — в каталоге могут находиться только объекты с меткой, полностью совпадающей с меткой каталога. Новые объекты наследуют метку родительского каталога. Политику можно инвертировать атрибутом `CCNR`.

1.3.9.8. Мандатные атрибуты

Основные атрибуты для изменения политики **МРД**:

- `CCNR` — позволяет хранить в каталогах объекты с различными метками конфиденциальности не выше метки каталога. Новые объекты получают нулевую метку. Каталоги с `CCNR` недоступны на запись обычным пользователям во избежание скрытых каналов связи.
- `EHOLE` — делает низкоцелостные файлы с нулевой меткой доступными на запись для процессов с любой меткой. Технически применим к любым файлам, но административно разрешен только для устройств и сокетов (например, `/dev/null`) во избежание рассекречивания информации.

`WHOLE` — делает файлы с максимальной меткой доступными на запись для процессов с любой меткой. Используется для файлов журналов, в которые пишут приложения разных уровней конфиденциальности.

Чтобы получить полный список файлов, на которые установлен атрибут `ehole` или `whole`, необходимо воспользоваться следующей командой:

```
find / -exec pdp-ls -MXda {} \; 2> /dev/null | grep ':ehole'
```

Уровни конфиденциальности

Модель мандатного управления доступом как механизм предотвращения утечки секретной информации использует уровни конфиденциальности.

Уровень конфиденциальности задается целым числом в диапазоне от 0 до 255 включительно, где 0 означает отсутствие конфиденциальности.

Максимально разрешенным уровнем конфиденциальности по умолчанию является 3. Созданные администратором уровни конфиденциальности имеют значение выше 3 и автоматически становятся максимально разрешенными. Администратор может добавлять новые уровни, при этом рекомендуется использовать значения 10, 20, 30 вместо 1, 2, 3 для возможности вставки промежуточных уровней.

Важно: При задании уровня конфиденциальности со значением выше 3 необходимо изменить значение параметра sysmaclev в конфигурационном файле /usr/sbin/pdp-init-fs и перезагрузить операционную систему.

Страница **Уровни конфиденциальности** содержит таблицу, в которой показаны все созданные уровни конфиденциальности.

1.3.9.9. Создание уровня

При нажатии кнопки **[+Создать]** откроется карточка создания нового уровня конфиденциальности.

Карточка содержит два обязательных поля.

Уровень - для выбора уникального числового значения уровня конфиденциальности, доступны только ранее не использованные, валидные значения в диапазоне от 0 до 255.

Название - для введения текста с названием уровня конфиденциальности. Количество символов в названии может быть от 1 до 255. Допустимо использование любых символов в названии. Исключение - первый и последний символ названия. Они должны содержать цифры 0-9 или буквы A-Z, a-z, А-Я, а-я.

Чтобы сохранить новый уровень, необходимо нажать **Сохранить**.

Для отмены создания нового уровня нажать **Отмена**. Появится предупреждающее окно с

текстом: «Были внесены изменения. Продолжить выход?». Выбрать нужный ответ.

Информацию о правилах валидации сложных полей уровней конфиденциальности можно найти в личном кабинете ALD Pro, в файле **Документация API 3.0.0**, в разделе 12 **Правила валидации сложных полей**.

1.3.9.10. Список уровней

Таблица содержит два столбца: **Уровень** и **Название**.. Первый столбец показывает порядковый номер уровня конфиденциальности, валидные значения от 0 до 255. Для невалидного уровня на месте числового значения отображается иконка красного восклицательного знака. При наведении курсора на иконку появляется всплывающая подсказка.

Второй — название уровня конфиденциальности. Оба столбца поддерживают функцию прямой и обратной сортировки.

Вертикальная прокрутка таблицы возможна в пределах 25 строк. В левом нижнем углу списка указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Для поиска уровня необходимо в строке поиска ввести от одного символа названия и нажать кнопку **Поиск**. Если уровня с введенным названием нет, отобразится надпись «Данные отсутствуют». При возникновении ошибки загрузки данных отобразится сообщение «Ошибка загрузки данных» красным цветом и кнопка **Попробовать снова** для повторной загрузки.

В строке поиска сохраняются данные о последнем запросе. Если последним действием был выполнен поиск по одному или нескольким символам, возможно стереть данные в строке поиска, нажать кнопку **Поиск** или **Enter**, и выполнится исходный запрос. Операция работает однократно.

1.3.9.11. Удаление уровня

Для удаления одного из уровней конфиденциальности требуется выбрать нужную строку и нажать **Удалить**. При удалении записи из таблицы появится предупреждающее окно с текстом.

Для подтверждения удаления данных из каталога и со страницы нажать **Удалить** в модальном окне.

Категории конфиденциальности

На вкладке приводятся настройки категорий конфиденциальности, позволяющие организовать защищенный доступ к секретным материалам разных уровней в общей информационной среде.

1.3.9.12. Создание категории конфиденциальности

Для создания новой категории конфиденциальности нажать кнопку **[+Создать]**. Будет выполнен переход на карточку добавления новой категории конфиденциальности. На карточке **Новая категория конфиденциальности** в поле **Разряд** из выпадающего списка выбрать значение и заполнить поле **Название**. Для сохранения изменений нажать кнопку **Сохранить**.

1.3.9.13. Список категорий конфиденциальности

На вкладке приведен список категорий конфиденциальности с указанием разряда и названия.

Для списка доступен поиск по названию. Для этого вверху вкладки в поле поиска ввести значение от 1 символа.

В столбце **Разряд** (порядковый номер) для невалидной категории на месте числового значения отображается иконка воклицательного знака в круге. В столбце **Разряд** доступна сортировка по возрастанию и убыванию числовых значений. В столбце **Название** доступна стандартная сортировка значений в прямом и обратном порядке.

1.3.9.14. Удаление категории конфиденциальности

На основной вкладке **Категории конфиденциальности** выбрать нужную категорию конфиденциальности, установив соответствующую радиокнопку, затем нажать кнопку **[Удалить]** над таблицей и подтвердить операцию.

Примечание: Модальное окно для подтверждения удаления содержит текст:

- для валидной категории конфиденциальности: «Категория будет удалена. Категорию будет невозможно использовать при входе в систему у доменных учетных записей.»;

- для невалидной категории конфиденциальности: «Категория будет удалена.»

Аудит Parsec

На странице **Аудит Parsec** представлена таблица с событиями мониторинга и контроля операций безопасности в операционной системе «Astra Linux».

Страница **Аудит Parsec** доступна только в режиме чтения. В таблице сначала отображаются все валидные события, потом — невалидные.

Разряд - столбец с числовым значением события аудита. Разряд события означает номер бита двоичного представления значения атрибута, нумерация начинается с нуля.

Для невалидного события на месте числового значения отображается иконка красного восклицательного знака. При наведении курсора на иконку появляется надпись «Ошибка».

Событие - столбец с названием события аудита.

Описание - столбец с описанием события аудита.

Вертикальная прокрутка таблицы возможна в пределах 25 строк. В левом нижнем углу списка указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Привилегии Parsec

На странице **Привилегии Parsec** представлена таблица с полным списком и описанием привилегий Parsec операционной системы «Astra Linux».

Страница **Привилегии Parsec** доступна только в режиме чтения. В таблице сначала отображаются все валидные привилегии, потом — невалидные.

Разряд - столбец с числовым значением привилегии Parsec. Разряд привилегии означает номер бита двоичного представления значения атрибута, нумерация начинается с нуля.

Для невалидной привилегии на месте числового значения отображается иконка красного восклицательного знака. При наведении курсора на иконку появляется всплывающая подсказка ошибки.

Название - столбец с названием привилегии Parsec.

Описание - столбец с описанием привилегии Parsec.

Вертикальная прокрутка таблицы возможна в пределах 25 строк. В левом нижнем углу списка указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Учтенные устройства

На вкладке приводится настройка учтенных устройств. Учтенное устройство - это устройство, для которого создано индивидуальное правило, определяющее параметры подключения в системе.

1.3.9.15. Создание учтенного устройства

Для создания нового устройства нажать кнопку **[+Создать]**. Будет выполнен переход в карточку добавления нового учтенного устройства.

На карточке **Новое устройство** заполнить поле **Название**, в поле **Владелец** и **Группа пользователей устройства** из выпадающего списка выбрать значение. В выпадающих списках доступен поиск: для владельца — по логину, фамилии, имени, отчеству; для группы пользователей устройства — по имени группы. При отсутствии результатов поиска отображается «Значений не найдено». Заполнить поле **Атрибуты**, нажав на кнопку **[+ Добавить атрибут]**. При необходимости заполнить поле **Описание**, переключатель **Включить**: устройство может быть включено, т.е. учитываться при работе, или выключено, т.е. не учитываться при работе. По умолчанию переключатель включен. Чтобы отключить необходимо снять флаг **Включен**. Нажать кнопку **Сохранить**. После сохранения в карточке учтенного устройства становятся доступными для редактирования вкладки **Параметры**, **МРД**, **Аудит Parsec** и **Правила для устройств** (см. подраздел edit_devices)

Атрибуты — это системные параметры и характеристики оборудования, которые используются операционной системой для идентификации учтенных устройств при их подключении. Допустимые символы для атрибута: буквы и цифры.

Примечание: В поле **Атрибут** должен быть заполнен хотя бы 1 атрибут.

Информацию о правилах валидации сложных полей учтенных устройств можно найти в личном кабинете ALD Pro, в файле **Документация API 3.0.0**, в разделе 12 **Правила валидации сложных полей**.

1.3.9.16. Редактирование учтенного устройства

Для редактирования выбрать устройство и перейти в его карточку. Данные об устройстве представлены на четырех вкладках: **Параметры**, **МРД**, **Аудит Parsec**, **Правила для устройства**.

Вкладка **Параметры** содержит нередактируемые поля **Название**, **Классификационная метка устройства** и **Метка аудита устройства**. Для редактирования доступны поля **Владелец**, **Группа пользователей устройства** и **Описание**. В полях **Владелец** и **Группа пользователей устройства** доступен выбор из выпадающего списка и поиск от 3-х символов: для владельца — по логину, фамилии, имени, отчеству; для группы пользователей устройства — по имени группы. При отсутствии результатов поиска отображается сообщение «Значений не найдено». Поле **Права доступа к устройству** не обязательно для заполнения, значение по умолчанию 640 (присутствует подсказка Формат UGO). Переключатель **Включить** активирует правило учета и по умолчанию включен. В обязательном поле **Атрибуты** должен быть указан минимум один атрибут. Для добавления нового атрибута необходимо нажать кнопку **[+Добавить атрибут]**. Для удаления атрибута нажать на кнопку **[–]** Для сохранения внесенных изменений нажать кнопку **[Сохранить]**. Появится модальное окно подтверждения действия.

Вкладка **МРД** содержит обязательно поле с выпадающим списком для выбора уровня конфиденциальности - **Уровень конфиденциальности**. Значение по умолчанию - «0: Низкий». На вкладке присутствует таблица, в которой доступно добавление или удаление категорий конфиденциальности. Для добавления категории в таблице нажать на кнопку **[+Добавить]**, появляется вкладка **Добавить записи** с полем для поиска необходимой категории и таблицей категорий. Выбрать один или несколько чекбоксов в первом столбце, нажать на кнопку **[Добавить]**. Для удаления категории конфиденциальности в таблице на вкладке МРД выбрать один или несколько чекбоксов в первом столбце и нажать кнопку **[Исключить]**. Появится модальное окно подтверждения действия. Изменения на этой вкладке сохраняются автоматически.

Вкладка **Аудит Parsec** содержит таблицу для настройки событий аудита со столбцами **Разряд**, **Событие** и чекбоксами в столбцах **Успех** и **Отказ**. Чекбоксы доступны для редактирования. Столбцы **Успех** и **Отказ** позволяют администратору указать, какие события следует записывать в журнал аудита: успешно выполненные операции с устройством, отказы в выполнении операций, или оба типа событий одновременно. Для сохранения изменений необходимо нажать на кнопку **[Сохранить]**.

На вкладке **Правила для устройства** содержит таблицу назначенных правил для устройств с возможностью добавления и исключения элементов из общего списка. Для

добавления правила нажать на кнопку **[+Добавить]**. Для удаления правила нажать на кнопку **[–Исключить]** и подтвердить операцию. Все изменения на этой вкладке сохраняются автоматически.

1.3.9.17. Список учтенных устройств

На вкладке приведен список учтенных устройств с указанием названия, владельца, описания и состояния.

Для списка доступен поиск по полям **Название**, **Владелец** и **Описание**. Для этого в поле поиска ввести значение от 1 символа.

В столбце **Владелец** указан логин пользователя. В столбце **Описание** приведено описание устройства.

В столбце **Название** доступна прямая и обратная сортировка. В столбце **Состояние** доступна фильтрация для отображения включенных или отключенных правил. Для этого необходимо выбрать состояние и нажать кнопку **ОК**.

1.3.9.18. Удаление учтенного устройства

На основной вкладке **Учтенные устройства** выбрать необходимое устройство и в открывшейся карточке с информацией о нем в разделе **Параметры** нажать кнопку **[Удалить]**, подтвердить удаление. После удаления будет выполнен переход к списку оставшихся устройств.

Правила для устройств

На вкладке отображаются правила для учтенных устройств. Учтенными устройствами считаются внешние носители, которые заранее зарегистрированы в системе. Каждое правило позволяет задать один атрибут, который затем можно назначить на любое количество устройств.

1.3.9.19. Создание правила

Для создания нового правила нажать кнопку **[+Создать]**. Будет выполнен переход на карточку добавления нового правила. На карточке **Новое правило** заполнить

обязательные поля **Название**, **Атрибут**, при необходимости поле **Описание**, переключатель **Включить**: правило может быть включено, т.е. учитываться при работе, или выключено, т.е. не учитываться при работе. По умолчанию чекбокс включен. Чтобы отключить необходимо снять флаг **Включен**. Нажать кнопку **Сохранить**.

Информацию о правилах валидации сложных полей правил учтенных устройств можно найти в личном кабинете ALD Pro, в файле **Документация API 3.0.0**, в разделе 12 **Правила валидации сложных полей**.

1.3.9.20. Список правил

На вкладке приведен список правил учтенных устройств с указанием названия правила, описания и состояния.

Для списка доступен поиск по названию и по описанию. Поиск работает от 1 символа.

В столбце **Правило** доступна сортировка по алфавиту. В столбце **Состояние** доступна фильтрация для отображения включенных или отключенных правил. Для этого необходимо выбрать состояние и нажать кнопку **ОК**

Для просмотра информации о правиле необходимо нажать на правило. Откроется карточка с информацией о нем: **Название**, **Атрибут**, переключатель **Включить**, **Описание**

1.3.9.21. Удаление правила

На вкладке **Правила для устройств** нажать на правило и в открывшейся карточке с информацией о нем нажать кнопку **[Удалить]**, подтвердить удаление. После удаления будет выполнен переход к списку оставшихся правил.

1.4. Пользователи и компьютеры

В разделе осуществляется управление организационными единицами, учетными записями пользователей и групп пользователей, а также учетными записями компьютеров и групп компьютеров.

1.4.1. Организационная структура

1.4.1.1. Общие сведения

В подразделе осуществляется создание и управление организационной структурой подразделений домена. Также в подразделе выполняется назначение прав и ролей структурным подразделениям и управление учетными записями, входящими в состав структурного подразделения.

В подразделе в качестве корневого подразделения отображается домен. Структурные подразделения добавляются в домен в иерархическом виде.

При переходе в подраздел отображается поле поиска подразделений и контроллер домена.

Для поиска подразделения следует начать вводить в поле поиска название, результат поиска будет выводиться по мере ввода.

Для раскрытия структуры подразделений необходимо нажать на подразделение.

При выделении подразделения вверху страницы отобразятся кнопки управления структурой подразделений (см. разделы **Добавление нового подразделения** и **Редактирование подразделения**), а также кнопки добавления нового пользователя (см. *Пользователи*), новой группы пользователей (см. *Группы пользователей*) и новой группы компьютеров (см. *Группы компьютеров*) в состав подразделения.

1.4.1.2. Добавление нового подразделения

Для добавления нового подразделения в структуру нажать кнопку **[+ Подразделение]**, будет открыта карточка нового подразделения.

На карточке на вкладке **Основное** необходимо заполнить обязательные поля

Наименование подразделения и **Родительское подразделение**. В поле **Расположение подразделения в организационной структуре** автоматически указывается полный путь выбранного структурного подразделения. В поле **Родительское подразделение** по умолчанию указывается подразделение, которое было выбрано при нажатии кнопки добавления нового подразделения. Данное значение можно изменить вручную. Также можно заполнить поля **Описание** и **Руководитель подразделения**.

Остальные вкладки для редактирования станут доступны после сохранения подразделения (см. editing_unit).

Для сохранения нового подразделения необходимо нажать на кнопку сохранения в правом верхнем углу. После сохранения подразделения будет выполнен переход к структуре подразделений.

1.4.1.3. Редактирование подразделения

Для редактирования подразделения необходимо выделить его в структуре и нажать кнопку **[Редактировать]** для открытия карточки подразделения.

На карточке подразделения информация приводится на вкладках:

- **Основное**;
- **Пользователи**;
- **Группы пользователей**;
- **Компьютеры**;
- **Дочерние подразделения**;
- **Групповые политики**;
- **Политики ПО**.

Для закрытия карточки подразделения и возврата к структуре подразделений следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Основное

На вкладке отображается основная информация о подразделении: наименование подразделения, родительское подразделение, руководитель подразделения, описание и

расположение.

Поля **Наименование подразделения** и **Расположение подразделения в организационной структуре** не могут быть изменены, остальные поля доступны для редактирования.

Для применения изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Для изменения родительского подразделения требуется наличие привилегии Organization units - Modify. Области действия активных ролей с этой привилегией должны включать:

- Подразделение, для которого выполняется изменение родительского подразделения;
- Старое родительское подразделение;
- Новое родительское подразделение.

К подразделению, над которым выполняется операция, не должны быть привязаны роли.

Если к подразделению привязаны роли, для него нельзя изменить родительское подразделение.

Для выполнения операции требуется отвязать от подразделения все роли, и выполнить назначение ролей после перемещения (требуется привилегия Roles - Modify)

Если требуется отвязать от подразделения роли и выполнить привязку после перемещения, то необходима привилегия Roles - Modify.

Области действия активных ролей с этой привилегией должны включать подразделение, для которого выполняется изменение родительского подразделения.

Пользователи

На вкладке осуществляется управление штатным составом подразделения.

В списке **Пользователи** в карточке подразделения отображается блок с данными о сотрудниках: ФИО, логин, должность и состояние.

Для списка пользователей доступен поиск по ФИО и логину. Поиск работает по одному из

ключей: имени, фамилии, отчеству или логину. Для поиска в соответствующем поле ввести значение от трех символов, результат поиска будет выводиться после нажатия кнопки **лупа**. Отображаются только те результаты поиска, у которых в столбце содержится значение, частично или полностью совпадающее со строкой поиска. Если значение некорректно, в результатах поиска появится надпись «Данные отсутствуют».

Столбцы с ФИО и логином поддерживают функцию прямой и обратной сортировки пользователей в алфавитном порядке.

В столбце с ФИО сортировка происходит по фамилии. Если столбец с ФИО заполнен полностью, то для прямого порядка сортировки сначала выводятся результаты на английском языке от A до Z, потом на русском от А до Я, для обратного порядка — наоборот: сначала на русском от Я до А, потом на английском от Z до A.

Столбец с названием должности поддерживает функцию фильтрации по уникальным значениям. При нажатии на кнопку фильтра появится список со значениями. Выбрать необходимое. Если значения отсутствуют (должности не назначены), появится окно с надписью «Без фильтров». Для сброса фильтра нажать **[Сбросить]**, затем **[ОК]**, чтобы применить изменения.

Вертикальная прокрутка таблицы возможна в пределах 25 строк.

В левом нижнем углу списка указано количество учетных записей. При достижении лимита в 2000 пользователей, отобразится надпись «Результатов: 2000, лимит достигнут».

В правом нижнем углу кнопки переключения страниц.

Для добавления пользователей в таблицу подразделения необходимо нажать **[+ Добавить]**. Появится таблица **Добавить записи** со списком пользователей. Выбрать нужные учетные записи и нажать **[Добавить]** в правом нижнем углу таблицы.

В таблице **Добавить записи** также доступен поиск по ФИО и логину от трех символов.

Для отмены добавления учетных записей пользователей в подразделение нажать **[Отмена]**.

Для добавления пользователя в подразделение требуется наличие привилегии Users - Set organization unit. Области действия активных ролей с этой привилегией должны включать:

- подразделение пользователя до выполнения операции;
- подразделение, в которое переводится пользователь.

Если на пользователя назначены роли, исполнителю операции потребуются привилегии:

Roles — Modify или Roles Membership — Manage.

При наличии ролей, назначенных на пользователя: области действия активных ролей пользователя должны включать новое подразделение, в которое переводится пользователь.

Пользователя нельзя добавить в подразделение, если область действия хотя бы одной из его активных ролей не включает новое подразделение.

При возникновении ошибки о несоответствии областей действия роли пользователя и нового подразделения требуется выполнить одно из действий в отношении роли, вызвавшей ошибку:

- изменить привязку роли к подразделению таким образом, чтобы она включала новое подразделение (исполнитель операции должен обладать привилегией Roles - Modify), и повторить операцию добавления пользователя в подразделение;
- исключить пользователя из участников роли (исполнитель операции должен обладать привилегией Roles Membership - Manage) и повторить операцию добавления пользователя в подразделение.

Система поддерживает исключение одного или нескольких пользователей одновременно. Для этого необходимо отметить требуемые записи в списке и нажать **[- Исключить]**.

При массовом исключении пользователей появится модальное окно с надписью: «Исключить записи? Будет исключено записей: (выбранное количество)». В окне нажать **[Исключить]** для подтверждения действия или **[Отмена]** для прерывания.

Для удаления пользователя из подразделения требуется наличие привилегии Users - Set organization unit. Области действия активных ролей с этой привилегией должны включать:

- подразделение пользователя до выполнения операции;
- корневое подразделение (пользователь при удалении из подразделения автоматически переносится в корень домена).

Если на пользователя назначены роли, исполнителю операции потребуются привилегии: Roles - Modify или Roles Membership - Manage.

При наличии ролей, назначенных на пользователя: области действия активных ролей пользователя должны распространяться на корень домена.

Пользователя нельзя удалить из подразделения, если область действия хотя бы одной из его активных ролей не распространяется на корень домена

При возникновении ошибки о несоответствии областей действия роли пользователя и нового подразделения требуется выполнить одно из действий в отношении роли, вызвавшей ошибку:

- изменить привязку роли к подразделению таким образом, чтобы она включала родительское подразделение (исполнитель операции должен обладать привилегией Roles - Modify), и повторить операцию удаления пользователя из подразделения;
- исключить пользователя из участников роли (исполнитель операции должен обладать привилегией Roles Membership - Manage) и повторить операцию удаления пользователя из подразделения.

Компьютеры

На вкладке осуществляется управление составом компьютеров подразделения: выбор компьютеров и групп компьютеров, которые будут входить в состав данного подразделения.

В списках **Выбранные компьютеры** и **Выбранные группы** указаны компьютеры и группы компьютеров, входящие в состав подразделения.

В списках **Все компьютеры** и **Все группы** указаны все компьютеры и группы компьютеров, зарегистрированные в домене.

Список компьютеров соответствует списку в подразделе *Компьютеры*.

Во всех списках доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить название компьютера/группы компьютеров, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для добавления компьютеров в подразделение необходимо в блоке **Компьютеры** в списке **Все компьютеры** отметить требуемые записи и перенести их в список **Выбранные компьютеры** нажатием кнопки **[<-]**.

Для добавления компьютера в подразделение требуется наличие привилегии Computers - Set organization unit. Области действия активных ролей с этой привилегией должны включать:

- Подразделение компьютера до выполнения операции;
- Подразделение, в которое переносится компьютер.

Для исключения компьютеров из подразделения необходимо в списке **Выбранные компьютеры** отметить требуемые записи и перенести их в список **Все компьютеры** нажатием кнопки **[→]**.

Для удаления компьютера из подразделения требуется наличие привилегии Computers - Set organization unit. Области действия активных ролей с этой привилегией должны включать:

- Подразделение компьютера до выполнения операции;
- Корневое подразделение (после удаления из подразделения компьютер автоматически переносится в корень домена).

Добавление/исключение группы компьютеров выполняется в блоке **Группы компьютеров** аналогично добавлению/исключению компьютеров.

Для добавления/удаления группы компьютеров требуется наличие привилегии Computer groups - Set organization unit. Для добавления группы компьютеров области действия активных ролей с этой привилегией должны включать:

- Подразделение группы компьютеров до выполнения операции;
- Подразделение, в которое переносится группа компьютеров.

Для удаления группы компьютеров области действия активных ролей с этой привилегией должны включать:

- Подразделение группы компьютеров до выполнения операции;
- Корневое подразделение (после удаления из подразделения группа компьютеров автоматически переносится в корень домена).

При нажатии на кнопку **[+ Новая группа]** будет выполнен переход на карточку создания новой группы компьютеров в подразделе *Группы компьютеров*.

Дочерние подразделения

На вкладке приведен список дочерних подразделений выбранного подразделения.

Для списка доступен поиск по названию. Для этого в поле поиска начать вводить название подразделения, результат поиска будет выводиться по мере ввода.

При нажатии на кнопку слева от поисковой строки **[+ Новое подразделение]** будет выполнен переход на карточку создания нового подразделения (см. раздел **Добавление**

нового подразделения).

При выборе дочернего подразделения из списка будет открыта карточка подразделения с возможностью редактирования (см. editing_unit).

Внизу списка указано количество дочерних подразделений данного подразделения.

Групповые политики

Список групповых политик

На вкладке приведен список групповых политик, которые были назначены на подразделение, с указанием их приоритета.

Флаг **Включить наследование** позволяет включить или отключить наследование параметров, определенных в объектах групповых политик, назначенных на родительские подразделения.

Для списка доступен поиск по названию. Для этого в поле поиска начать вводить название политики, результат поиска будет выводиться по мере ввода.

Справа от поисковой строки расположена кнопка **[+ Добавить групповую политику]**.

Внизу списка указано количество групповых политик, назначенных на подразделение.

Назначение групповой политики

Подразделению можно назначить групповые политики, созданные в подразделе *Групповые политики* (раздел *Групповые политики*)

Назначенные групповые политики будут применяться к учетным записям пользователей, к компьютерам данного подразделения и объектам его дочерних подразделений.

Для назначения подразделению групповой политики нажать кнопку **[Добавить групповую политику]**, будет выполнен переход на карточку назначения групповой политики. На карточке необходимо из выпадающего списка **Групповая политика** выбрать групповую политику. В поле **Приоритет** задать приоритет ее применения. В поле **Расположение подразделения в организационной структуре** будет автоматически отображаться dn подразделения.

Флаг **Наследовать принудительно** делает наследование параметров выбранное ГПО обязательным для подразделения и для всех дочерних подразделений, даже если где-то было отключено наследование. (см. инструкцию *Наследование и суммирование параметров групповых политик*)

> **Внимание:** Приоритет групповой политики должен быть уникальным. Одному подразделению не может быть назначено несколько групповых политик с одинаковым приоритетом.

Для применения изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Изменение приоритета и порядка наследования назначенной групповой политики

Для изменения приоритета и порядка наследования назначенной групповой политики необходимо перейти в карточку политики, нажав на нее в списке.

Изменение приоритета определяет порядок применения групповых политик, т.е. какие настройки будут применены к объекту.

Для изменения приоритета применения групповой политики в поле **Приоритет групповой политики** задать новое значение.

Флаг **Наследовать принудительно** позволяет сделать наследование параметров соответствующего объекта обязательным для всех дочерних подразделений, даже если где-то наследование отключено. Связанные ГПО, отмеченные флагом **Принудительно**, применяются после обычных ГПО, поэтому переопределяют их значения.

Для включения принудительного наследования параметров ГПО, необходимо установить флаг **Наследовать принудительно**.

Для применения изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X**

Закрыть]. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Отмена назначения групповой политики

Для отмены назначения на подразделение групповой политики или одновременно нескольких групповых политик необходимо на вкладке **Групповые политики** в списке отметить требуемые групповые политики и нажать кнопку **[Удалить]**.

Также отменить назначение на подразделение групповой политики можно из ее карточки: нажать на групповую политику в списке для открытия ее карточки, затем на карточке нажать кнопку **[Удалить]**. После подтверждения удаления будет выполнен переход к списку групповых политик.

Политики ПО

Список групповых политик

На вкладке приведен список политик ПО, которые были назначены на подразделение, с указанием их приоритета.

Для списка доступен поиск по названию. Для этого в поле поиска начать вводить название политики, результат поиска будет выводиться по мере ввода.

Справа от поисковой строки расположена кнопка **[+ Назначить политику ПО]**.

Внизу списка указано количество политик ПО, назначенных на подразделение.

Назначение политики ПО

Подразделению можно назначить политики ПО, созданные в подразделе *Политики ПО* (раздел *Установка и обновление ПО*)

Политики ПО определяют перечень программного обеспечения, устанавливаемого на компьютеры данного подразделения и его дочерних подразделений.

Для назначения подразделению политики ПО нажать кнопку **[+ Назначить политику ПО]**, будет выполнен переход на карточку назначения политики. На карточке необходимо из

выпадающего списка **Имя политики ПО** выбрать политику ПО и в поле **Приоритет политики ПО** задать приоритет ее применения.

Важно: Приоритет политики ПО должен быть уникальным. Одному подразделению не может быть назначено две (или более) политики ПО, которые имеют одинаковый приоритет.

Для применения изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Изменение приоритета назначенной политики ПО

Для изменения приоритета назначенной политики ПО необходимо нажать на политику ПО в списке, затем на открывшейся карточке отредактировать поле **Приоритет политики ПО**.

Для применения изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Отмена назначения политики ПО

Для отмены назначения на подразделение политики ПО или одновременно нескольких политик ПО необходимо на вкладке **Политики ПО** в списке отметить требуемые политики ПО и нажать кнопку **[Удалить]**.

Также отменить назначение на подразделение политики ПО можно из ее карточки: нажать на политику ПО в списке для открытия ее карточки, затем на карточке нажать кнопку **[Удалить]**. После подтверждения удаления будет выполнен переход к списку групповых политик.

1.4.1.4. Удаление подразделения

Для удаления подразделения необходимо выделить его в иерархической структуре и нажать кнопку **[Редактировать]**. В открывшейся карточке подразделения нажать кнопку **[Удалить]**. После подтверждения удаления будет выполнен переход к структуре подразделений домена.

Для удаления подразделения требуется привилегия Organization Units — Delete. Области действия активных ролей с этой привилегией должны включать удаляемое подразделение.

В удаляемом подразделении должны отсутствовать объекты (пользователи, компьютеры, группы компьютеров, группы пользователей).

К подразделению, над которым выполняется операция, не должны быть привязаны роли.

Если к подразделению привязаны роли, его нельзя удалить.

Для удаления подразделения требуется выполнить одно из действий:

- переназначить роли на другое подразделение (требуется привилегия Roles — Modify с привязкой к подразделению, на которое выполняется перепривязка ролей);
- удалить роли, назначенные на удаляемое подразделение (требуется привилегия Roles — Delete с привязкой к удаляемому подразделению).

1.4.2. Пользователи

1.4.2.1. Список пользователей

В подразделе осуществляется управление учетными записями пользователей.

В подразделе приведен список всех учетных записей пользователей с указанием имени пользователя, имени учетной записи (логина), подразделения, должности и состояния учетной записи.

Для списка пользователей доступен поиск по ФИО и логину. Поиск работает по одному из ключей: имени, фамилии, отчеству или логину. Для поиска в соответствующем поле ввести значение от трех символов, результат поиска будет выводиться после нажатия кнопки **лупа**. Отображаются только те результаты поиска, у которых в столбце содержится значение, частично или полностью совпадающее со строкой поиска. Если значение некорректно, в результатах поиска появится надпись «Данные отсутствуют».

Столбцы с ФИО и логином поддерживают функцию прямой и обратной сортировки пользователей в алфавитном порядке.

В столбце с ФИО сортировка происходит по фамилии. Если столбец с ФИО заполнен полностью, то для прямого порядка сортировки сначала выводятся результаты на английском языке от A до Z, потом на русском от А до Я, для обратного порядка — наоборот: сначала на русском от Я до А, потом на английском от Z до A.

Столбцы с названием подразделения и должности поддерживают функцию фильтрации по уникальным значениям.

При нажатии на кнопку фильтра появится список со значениями. Выбрать необходимое. Если значения отсутствуют (подразделение или должность не назначены), появится окно с надписью «Без фильтров». Для сброса фильтра нажать **[Сбросить]**, затем **[ОК]**, чтобы применить изменения.

Вертикальная прокрутка таблицы возможна в пределах 25 строк.

В левом нижнем углу списка указано количество учетных записей. При достижении лимита в 2000 пользователей, отобразится надпись «Результатов: 2000, лимит достигнут».

В правом нижнем углу кнопки переключения страниц.

1.4.2.2. Добавление пользователя

Для добавления нового пользователя необходимо нажать на кнопку **[+ Создать]**, будет выполнен переход на карточку нового пользователя.

На карточке на вкладке **Основное** ввести данные о пользователе и его учетной записи. Обязательные для заполнения поля отмечены соответствующим образом. Новый пароль должен соответствовать политике паролей по умолчанию.

Остальные вкладки карточки пользователя станут доступны после сохранения информации (см. раздел **Редактирование информации о пользователе**)

Для добавления пользователя нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку пользователей.

Для закрытия карточки и возврата к списку пользователей нажать на кнопку **[X Закрыть]**.

Важно: Учетная запись, которой не присвоен ни один системный тип администратора не

имеет допуска к функциям Системы. Управление системными типами администратора осуществляется:

- из карточки типа администратора подраздел **Типы администратора в системе** раздела *Роли и права доступа*;
- из карточки пользователя (вкладка “Назначенные роли”)

1.4.2.3. Редактирование информации о пользователе

Редактирование информации о пользователе осуществляется на его карточке. Для перехода на карточку необходимо в списке нажать на пользователя.

На карточке информация о пользователе размещается на вкладках:

- **Основное**;
- **Группы**;
- **Дополнительные сведения**;
- **Групповые политики**;
- **Расширенные настройки**;
- **Роли**;
- **МРД**.

Для закрытия карточки пользователя и возврата к списку пользователей нажать на кнопку **[X Закрыть]**.

Для изменения подразделения пользователя требуется наличие привилегии Users - Set organization unit.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение пользователя до выполнения операции;
- Подразделение, в которое переводится пользователь.

При наличии ролей, назначенных на пользователя: области действия активных ролей пользователя должны включать новое подразделение, в которое переводится пользователь.

Пользователю нельзя изменить подразделение, если область действия хотя бы одной из

его активных ролей не включает новое подразделение.

При возникновении ошибки о несоответствии областей действия роли пользователя и нового подразделения требуется выполнить одно из действий в отношении роли, вызвавшей ошибку:

- изменить привязку роли (исполнитель операции должен обладать привилегией Roles - Modify) и повторить операцию изменения подразделения пользователя;
- отменить назначение роли пользователю (исполнитель операции должен обладать привилегией Roles Membership - Manage) и повторить операцию изменения подразделения пользователя.

Области действия активных ролей с этими привилегиями также должны включать:

- Подразделение пользователя до выполнения операции;
- Подразделение, в которое переводится пользователь.

Основное

Информация о пользователе

На вкладке приведена информация о пользователе и о его учетной записи. Не доступно для редактирования имя учетной записи (логин) и дата окончания действия пароля, остальные поля доступны для изменения.

Информация о пользователе размещается в соответствующих блоках:

- **Персональные данные** — ФИО, отображаемое имя пользователя и его фотография;
- **Учетная запись** — идентификатор учетной записи и логин, смена пароля и управление состоянием учетной записи;
- **Организационные данные** — подразделение, расположение в организационной структуре и должность пользователя, а также его руководитель;
- **Контактная информация** — адрес электронной почты, номера рабочего и мобильного телефонов пользователя;
- **Расположение** — адрес пользователя;
- **Сертификаты пользователя** — управление сертификатами пользователя;
- **Открытые ключи SSH** — управление открытыми ключами пользователя.

При выборе подразделения пользователя открывается модальное окно с вложенной иерархической структурой и поиском.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Сброс пароля пользователя

На карточке пользователя на вкладке **Основное** задать новый пароль в полях **Пароль** и **Подтверждение пароля** и нажать кнопку **[Сбросить пароль]**. Новый пароль должен соответствовать его политике паролей. Исключение составляет параметр «Минимальный срок действия», который игнорируется при сбросе пароля.

Управление сертификатами пользователя

Для добавления сертификата необходимо ввести его в поле **Сертификат в формате base64 или PEM** и нажать на кнопку **[Добавить]**.

Для пользователя можно добавить несколько сертификатов. Для добавление второго и последующих сертификатов необходимо в пустом поле **Сертификат в формате base64 или PEM** ввести новый сертификат и нажать на кнопку **[Добавить еще]**.

Для удаления сертификата нажать кнопку **[Удалить]** рядом с соответствующим сертификатом.

Управление открытыми ключами пользователя

Для добавления открытого ключа SSH необходимо ввести его в поле **Ключ в формате SSH** и нажать на кнопку **[Добавить]**.

Для пользователя можно добавить несколько открытых ключей SSH. Для добавление второго и последующих открытых ключей необходимо в пустом поле **Ключ в формате SSH** ввести новый открытый ключ SSH и нажать на кнопку **[Добавить еще]**.

Для удаления открытого ключа SSH нажать кнопку **[Удалить]** рядом с соответствующим ключом.

Группы

На вкладке задаются группы пользователей, в которых будет состоять учетная запись пользователя.

В блоке **Состоит в группах** в списке **Выбранные группы** указаны группы пользователей, в которых состоит данная учетная запись. В списке **Все группы** указаны все группы пользователей домена.

Во всех списках доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить название группы, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для включения пользователя в состав группы необходимо в списке **Все группы** отметить группы, в состав которых требуется включить пользователя, и перенести их в список **Выбранные группы** нажатием кнопки **[<-]**.

Для добавление пользователя в группу требуется наличие привилегии User groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение пользователя;
- Подразделение группы, в которую добавляется пользователь.

Если на группу назначены роли, исполнителю операции потребуются привилегия Roles Membership - Manage.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение пользователя;
- Подразделения всех ролей, назначенных на группу.

При добавлении в группу пользователь наследует все роли, назначенные на группу.

Для исключения пользователя из состава групп необходимо в списке **Выбранные группы** отметить требуемые записи и перенести их в список **Все группы** нажатием кнопки **[→]**.

Для удаления пользователя из группы требуется наличие привилегии User groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение пользователя;
- Подразделение группы, из которой исключается пользователь.

Если на группу, из которой удаляется пользователь, назначены роли, исполнителю операции потребуется привилегия Roles Membership - Manage.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение пользователя;
- Подразделения всех ролей, назначенных на группу.

При исключении из группы пользователь лишается ролей, унаследованных от группы (требуется привилегия Roles Membership - Manage с привязкой к подразделению пользователя)

При нажатии на кнопку **[+ Новая группа]** будет выполнен переход на карточку создания новой группы в подразделе *Группы пользователей*.

В блоке **Состоит в группах непрямое наследование** приведен список всех групп, которые входят в состав групп, в которые включена просматриваемая группа.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Дополнительные сведения

На вкладке приводятся дополнительные сведения о пользователе. Поля дополнительных сведений настраиваются на вкладке **Атрибуты пользователей** в подразделе *Пользователи и группы* (раздел *Управление доменом*)

Все поля на вкладке доступны для редактирования.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в

правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Групповые политики

На левой вкладке приводится список назначенных параметров групповых политик, которые могут быть применены к данному пользователю. Групповые политики назначаются на подразделение в подразделе *Групповые политики* (раздел *Групповые политики*) или на вкладке **Групповые политики** карточки подразделения в подразделе *Организационная структура* (раздел *Пользователи и компьютеры*).

> **Внимание:** Данный список представляет собой моделирование результатов применения групповых политик. Это значит, что не все политики из данного списка могут быть применены к конкретному пользователю и не все параметры могут быть отображены в данном списке. Чтобы групповая политика применилась к пользователю, необходимо соблюдение требований к операционной системе и заполнение значений атрибутов.

Внизу списка указано количество параметров групповых политик, применяемых к данному пользователю.

Настройки параметра выводятся в правой панели **Настройка параметра <имя параметра>**. Здесь отображается общая информация о параметре: объект групповой политики, подразделение, расположение подразделения в организационной структуре, требования к ОС и настройки атрибутов.

Расширенные настройки

Заполнение информации на вкладке формирует псевдонимы почтового ящика пользователя: основной адрес почты и дополнительные адреса (proxyAddresses).

Данные атрибуты используются для взаимодействия с почтовым сервисом.

Для заполнения информации о дополнительных адресах (proxyAddresses) необходимо

заполнить поле **Основной адрес**. Данное поле заполняется в SMTP формате: `SMTP:<регистрационное имя>@<домен получателя>`

Пример

SMTP:a.ivanov@ald.pro

Для добавления дополнительных адресов необходимо перейти в блок **Дополнительные адреса (proxyAddresses)** и заполнить поле **Адрес**. Данное поле доступно для заполнения в одном из следующих форматов:

- для формата smtp: `smtp:<регистрационное имя>@<домен получателя>`

Пример

smtp:alex_ivanov@ald.pro

- для формата x500: `x500:/o=<имя организации>/ou=<имя сайта>/cn=Recipients/cn=<псевдоним>`

Пример

x500:/o=ALDPro/ou=Департамент разработки/cn=Recipients/cn=a.ivanov

- Для формата sip:

1) `sip:<имя пользователя>@<имя домена>`

Пример

sip:a.ivanov@ald.pro

2) `sip:<регистрационное имя>@<имя хоста>`

Пример

sip:a.ivanov@client01.aldpro

3) `sip:<регистрационное имя>@<IP-адрес хоста>`

Пример

sip:a.ivanov@10.11.1.8

4) `sip:<№ телефона пользователя>@<имя шлюза>`

Пример

sip:+74952232343@192.168.31.254

После заполнения поля необходимо нажать на кнопку **[Добавить]**. Для сохранения изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу и подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Роли

На вкладке задаются типы администратора, которыми будет наделена учетная запись пользователя, и отображаются наследуемые типы.

В блоке **Содержит роли** в списке **Выбранные роли** указаны типы администратора, которыми будет наделена учетная запись пользователя. В списке **Все роли** указаны все типы администратора в системе. В списке **Все роли** отображаются не только предустановленные роли, но и те, которые создали сами пользователи.

Во всех списках доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить название типа администратора, результат поиска будет выводиться по мере ввода.

Во всех списках доступна фильтрация по значению поля **Состояние**. Для этого необходимо кликнуть на значок фильтрации и выбрать значение,по которому список будет отфильтрован.

Внизу каждого списка указано количество записей в данном списке.

Для наделения пользователей возможностями соответствующего типа администратора необходимо в списке **Все роли** отметить типы, которыми требуется наделить пользователя, и перенести их в список **Выбранные роли** нажатием кнопки **[<-]**.

Для исключения пользователей из списка обладателей соответствующего типа администратора необходимо в списке **Выбранные роли** отметить требуемые записи и перенести их в список **Все роли** нажатием кнопки **[→]**.

Для применения изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем

углу. И подтвердить действие во всплывающем окне.

В блоке **Наследует роли** указаны типы администратора, которые наследуются учетной записью пользователя.

В списке доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить название типа администратора, результат поиска будет выводиться по мере ввода.

В списке доступна фильтрация по значению поля **Состояние**. Для этого необходимо кликнуть на значок фильтрации и выбрать значение,по которому список будет отфильтрован.

Внизу списка указано количество записей в данном списке.

Управление типами администратора также осуществляется в подразделе *Роли и права доступа* раздела *Управление доменом*

МРД

Данные об МРД в карточке пользователя расположены на отдельной вкладке и разделены внутри на 3 вкладки:

- **Параметры**;
- **Привилегии Parsec**;
- **Аудит Parsec**.

Параметры

Вкладка **Параметры** содержит группу нередактируемых полей **Возможные мандатные атрибуты пользователя**, в которую входят поля **Допустимые параметры конфиденциальности**, **Маска привилегий** и **Маска аудита**.

Вкладка **Параметры** содержит группу редактируемых полей **Уровни конфиденциальности**. Для редактирования нажать на кнопку **[Изменить]**. Открывается вкладка **Выбор уровня конфиденциальности**, на которой присутствует таблица со столбцами **Уровень**, **Название**, **Минимальный**, **Максимальный**. В столбцах **Минимальный** и **Максимальный** доступны радиокнопки для выбора или изменения значения. Для сохранения нажать на кнопку **[Сохранить]**.

При нарушении логики назначенного диапазона (когда максимальный уровень меньше минимального) система отображает сообщение об ошибке: «Неверные данные: максимальный уровень меньше минимального». Для сброса назначенного диапазона уровней конфиденциальности нажать на кнопку **[Сбросить]**.

Примечание: Минимальный и максимальный уровни конфиденциальности определяют границы диапазона доступа пользователя к информации. Минимальный уровень задает нижнюю границу информации, с которой пользователь может работать, а максимальный — верхнюю границу доступных данных в соответствии с иерархией секретности.

Для максимального/минимального уровня разрешены значения в диапазоне от 0 до 255.

Вкладка **Параметры** содержит группу полей **Уровни целостности**. Поле **Минимальный** нередактируемое. Значение по умолчанию : «0:Низкий». Поле **Максимальный** — необязательное поле с возможностью выбора из выпадающего списка предустановленных уровней целостности. Максимальный уровень целостности определяет верхнюю границу доверия к пользователю и возможности администрирования в домене:

- 255 — администрирование всех машин домена, включая контроллеры домена;
- 127 — администрирование всех машин, кроме контроллеров домена;
- 63 — администрирование только обычных компьютеров;
- 31 — администрирование компьютеров с пониженным доверием;
- 0 — минимальный уровень доверия.

Список уровней целостности предустановлен и не изменяется. Администратор может использовать как данную градацию, так и традиционный подход с высоким (63) и низким (0) уровнями.

Вкладка **Параметры** содержит таблицу **Категории конфиденциальности** со столбцами **Разряд**, **Наименование**, **Мин.**, **Макс.**. В столбцах **Мин.** и **Макс.** доступны чекбоксы.

Примечание: Минимальная (мин.) и максимальная (макс.) категории определяют диапазон неиерархических категорий конфиденциальности, в пределах которого пользователю разрешен доступ к информации.

Для сохранения изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем

углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Аудит Parsec

Вкладка **Аудит Parsec** содержит таблицу для настройки событий аудита со столбцами **Разряд**, **Событие** и чекбоксами в столбцах **Успех** и **Отказ**. Чекбоксы доступны для редактирования. Столбцы **Успех** и **Отказ** позволяют администратору указать, какие события следует записывать в журнал аудита: успешно выполненные операции пользователя, отказы в выполнении операций, или оба типа событий одновременно. Для сохранения изменений нажать на кнопку **[Сохранить]** и подтвердить.

Вкладка **Аудит Parsec** содержит нередактируемое поле **Маска аудита**.

Маска аудита - это битовая маска (числовое значение), которая определяет, какие типы событий будут регистрироваться в системе аудита безопасности Parsec.

Привилегии Parsec

Вкладка **Привилегии Parsec** содержит таблицу **Привилегии Parsec** со столбцами **Разряд**, **Название**, **Выбрать**. В столбце **Выбрать** доступны чекбоксы с возможностью множественного выбора для назначения пользователю. Для сохранения изменений нажать на кнопку **[Сохранить]** и подтвердить.

Вкладка **Привилегии Parsec** содержит нередактируемое поле **Маска привилегий**.

Маска привилегий — это битовая маска, определяющая набор специальных возможностей пользователя в операционной системе.

1.4.2.4. Блокировка и разблокировка пользователя

Система поддерживаем возможность блокировки и разблокировки одного или нескольких пользователей одновременно. Для этого необходимо в списке отметить пользователя, нажать кнопку **[Действия]**, выбрать соответственно **[Заблокировать]** или **[Разблокировать]**.

Для снятия отметки с пользователя можно нажать кнопку **[X Закрыть]** в правом верхнем углу.

При массовой блокировке пользователей появится модальное окно с надписью: «Заблокировать пользователей? Все выбранные пользователи будут переведены в статус «Заблокирован»». В окне нажать **[Заблокировать]** для подтверждения действия или **[Отменить]** для прерывания.

При массовой разблокировке пользователей появится модальное окно с надписью: «Разблокировать пользователей? Все выбранные пользователи будут переведены в статус «Активен»». В окне нажать **[Разблокировать]** для подтверждения действия или **[Отменить]** для прерывания.

Также заблокировать или разблокировать пользователя можно из его карточки: открыть карточку нажатием на пользователя в списке, затем на карточке на вкладке **Основное** нажать, соответственно, кнопку **[Заблокировать УЗ]** или **[Разблокировать УЗ]**.

Для блокировки/разблокировки учетной записи пользователя требуется наличие привилегий: Users Block - Manage или Users - Modify.

Области действия активных ролей с этой привилегией должны включать подразделение пользователя.

Если на заблокированного пользователя назначены роли, он полностью теряет делегированные ему права на время блокировки.

Разблокированный пользователь имеет доступ, полностью соответствующий привилегиям в составе его ролей.

Для закрытия карточки пользователя и возврата к списку нажать на кнопку **[X Закрыть]**.

1.4.2.5. Удаление пользователя

Система поддерживает удаление одного или нескольких пользователей одновременно. Для этого необходимо отметить пользователя в списке и нажать кнопку **[Удалить]**.

При массовом удалении пользователей появится модальное окно с надписью: «Удалить пользователей? Пользователи будут перемещены в корзину». В окне нажать **[Удалить]** для подтверждения действия или **[Отмена]** для прерывания.

Для снятия отметки с пользователя можно нажать кнопку **[X Закрыть]** в правом верхнем

углу.

Также удалить пользователя можно из его карточки: открыть карточку нажатием на пользователя в списке, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить учетную запись]**. После подтверждения удаления учетная запись будет перенесена в *Корзину* и будет выполнен переход к списку пользователей.

Для переноса пользователя в Корзину требуется привилегия Users - Move to trash.

Области действия активных ролей с этой привилегией должны включать подразделение пользователя.

Пользователь, перенесенный в Корзину, теряет доступ, соответствующий назначенным ему ролям.

1.4.3. Группы пользователей

В подразделе осуществляется управление группами пользователей.

1.4.3.1. Список групп пользователей

В подразделе приведен список групп пользователей домена с указанием названия группы, подразделения, в которое входит группа, и описания группы.

Если группа входит в состав другой группы и напрямую (прямое наследование), и как участник другой группы (непрямое наследование), то отражается только прямое участие группы (**Состоит в группах**), а участие в составе другой группы (**Состоит в группах непрямое наследование**) не отражается.

Группа пользователей может входить в состав только одного подразделения, при этом в состав одного подразделения может входить несколько групп пользователей.

Для списка доступен поиск. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Справа от поисковой строки расположена кнопка **[+ Новая группа]**.

Внизу списка указано количество групп в домене.

1.4.3.2. Добавление новой группы

Для добавления новой группы нажать кнопку **[+ Новая группа]**, будет выполнен переход на карточку новой группы пользователей.

На карточке на вкладке **Основное** заполнить обязательные поля **Название группы** и **Подразделение**. В поле **Расположение подразделения в организационной структуре** автоматически указывается полный путь выбранного структурного подразделения. Также можно заполнить поле **Описание**.

Остальные вкладки станут доступны после сохранения группы пользователей (см. подраздел **Пользователи и компьютеры → Группы пользователей → Редактирование информации о группе пользователей**).

Для сохранения группы пользователей необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Для добавление родительской группы пользователей (состоит в группах) требуется наличие привилегии User groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение группы, для которой выполняется добавление родительской;
- Подразделение группы, которая добавляется в качестве родительской.

Если на родительскую группу назначены роли, исполнителю операции потребуются привилегия Roles Membership - Manage.

При наличии активных ролей, назначенных на группу, которая добавляется в качестве родительской группы: подразделения всех без исключения пользователей дочерней группы должны попадать в области действия всех ролей, назначенных на родительскую группу.

После операции:

- дочерняя группа наследует роли, назначенные на родительскую группу;
- все пользователи в составе дочерней группы наследуют роли, назначенные на родительскую группу.

При добавление дочерней группы пользователей (содержит группы) требуется наличие привилегии User groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение группы, в которую выполняется добавление дочерней группы;
- Подразделение группы, которая добавляется в качестве дочерней.

Если на родительскую группу назначены роли, исполнителю операции потребуются привилегия Roles Membership - Manage.

При наличии активных ролей, назначенных на группу, в которую выполняется добавление дочерней группы: подразделения всех без исключения пользователей дочерней группы должны попадать в области действия всех ролей, назначенных на родительскую группу.

После операции:

- дочерняя группа наследует роли, назначенные на родительскую группу;
- все пользователи в составе дочерней группы наследуют роли, назначенные на родительскую группу.

1.4.3.3. Редактирование информации о группе пользователей

Редактирование информации о группе пользователей осуществляется на ее карточке. Для перехода на карточку необходимо нажать на группу пользователей в списке.

На карточке информация о группе пользователей размещается на вкладках:

- **Основное**;
- **Пользователи**;
- **Группы**;
- **Роли**.

Для закрытия карточки группы пользователей и возврата к списку групп следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Основное

На вкладке приведена информация о группе пользователей, а также указывается UID группы, присвоенный автоматически при создании группы.

На вкладке можно изменить подразделение, в которое будет входить группа пользователей, и описание группы.

Для изменения подразделения группы пользователей требуется наличие привилегии User groups - Set organization unit.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение группы до выполнения операции;
- Подразделение, в которое переводится группа.

Наличие ролей, назначенных на группу, не имеет значения.

Для применения внесенных изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Пользователи

В списке **Пользователи** в карточке группы пользователей отображается блок с данными о сотрудниках: ФИО, логин, подразделение, должность, состояние.

Для списка пользователей доступен поиск по ФИО и логину. Поиск работает по одному из ключей: имени, фамилии, отчеству или логину. Для поиска в соответствующем поле ввести значение от трех символов, результат поиска будет выводиться после нажатия кнопки **лупа**. Отображаются только те результаты поиска, у которых в столбце содержится значение, частично или полностью совпадающее со строкой поиска. Если значение некорректно, в результатах поиска появится надпись «Данные отсутствуют».

Столбцы с ФИО и логином поддерживают функцию прямой и обратной сортировки пользователей в алфавитном порядке.

В столбце с ФИО сортировка происходит по фамилии. Если столбец с ФИО заполнен

полностью, то для прямого порядка сортировки сначала выводятся результаты на английском языке от A до Z, потом на русском от А до Я, для обратного порядка — наоборот: сначала на русском от Я до А, потом на английском от Z до A.

Столбцы с названием подразделения и должности поддерживают функцию фильтрации по уникальным значениям. При нажатии на кнопку фильтра появится список со значениями. Выбрать необходимое. Если значения отсутствуют (подразделение или должность не назначены), появится окно с надписью «Без фильтров». Для сброса фильтра нажать **[Сбросить]**, затем **[ОК]**, чтобы применить изменения.

Сортировка, поиск и фильтрация доступны, если количество пользователей в группе не превышает 2000.

Вертикальная прокрутка таблицы возможна в пределах 25 строк.

В левом нижнем углу списка указано количество учетных записей. При достижении лимита в 2000 пользователей, отобразится надпись «Результатов: 2000, лимит достигнут».

В правом нижнем углу кнопки переключения страниц.

Для добавления пользователей в таблицу подразделения необходимо нажать **[+ Добавить]**. Появится таблица **Добавить записи** со списком пользователей. Выбрать нужные учетные записи и нажать **[Добавить]** в правом нижнем углу таблицы.

В таблице **Добавить записи** также доступен поиск по ФИО и логину от трех символов.

Для отмены добавления учетных записей пользователей в подразделение нажать **[Отмена]**.

Для добавления пользователя в группу требуется наличие привилегии User groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- подразделение пользователя;
- подразделение группы, в которую добавляется пользователь.

Если на группу назначены роли, исполнителю операции потребуются привилегия Roles Membership - Manage.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение пользователя;

- Подразделения всех ролей, назначенных на группу.

При добавлении в группу пользователь наследует все роли, назначенные на группу.

Система поддерживает исключение одного или нескольких пользователей одновременно. Для этого необходимо отметить требуемые записи в списке и нажать **[Исключить]**.

При массовом исключении пользователей появится модальное окно с надписью: «Исключить записи? Будет исключено записей: (выбранное количество)». В окне нажать **[Исключить]** для подтверждения действия или **[Отмена]** для прерывания.

После исключения из группы пользователь лишается ролей, унаследованных им от группы.

Для удаления пользователя из группы требуется наличие привилегии User groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- подразделение пользователя;
- подразделение группы, из которой исключается пользователь.

Если на группу назначены роли, исполнителю операции дополнительно требуется привилегия Roles Membership - Manage.

Области действия активных ролей с этой привилегией должны включать:

- подразделение пользователя;
- подразделения всех ролей, назначенных на группу.

При нажатии на кнопку **[+ Новый пользователь]** будет выполнен переход на карточку добавления нового пользователя в подразделе users_1.

Для применения изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу.

Группы

В разделе **Содержит группы** на вкладке в списке **Выбранные группы** приведен список групп, включенных в состав данной группы (прямое наследование). В списке **Все группы** приведен список всех групп пользователей домена.

Внимание: Использование циклических (замнутых) наследований групп пользователей может привести к нежелательному поведению системы в различных ее частях. Не рекомендуется использовать данную архитектуру групп.

Во всех списках доступен поиск по названию группы. Для этого в соответствующем поле поиска начать вводить название группы, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для включения групп пользователей в состав данной группы необходимо в списке **Все группы** отметить группы пользователей и перенести их в список **Выбранные группы** нажатием кнопки **[<-]**. При этом все пользователи из добавляемых групп будут добавлены в список **Выбранные пользователи** на вкладке users_1.

Для добавления группы пользователей в данную группу требуется наличие привилегии User groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение данной группы;
- Подразделение группы пользователей, которая добавляется в качестве дочерней.

При наличии активных ролей, назначенных на группу, в которую выполняется добавление дочерней группы, исполнителю операции требуется дополнительная привилегия Roles Membership — Manage. Области действия активных ролей с этой привилегией должны включать:

- Подразделения всех ролей, назначенных на родительскую группу
- Подразделения всех пользователей из дочерней группы

Также подразделения всех без исключения пользователей дочерней группы должны попадать в области действия всех ролей, назначенных на родительскую группу.

По результатам операции:

- Дочерняя группа наследует роли, назначенные на родительскую группу;
- Все пользователи в составе дочерней группы наследуют роли, назначенные на родительскую группу.

Для исключения групп пользователей из состава данной группы необходимо в списке

Выбранные группы отметить требуемые записи и перенести их в список **Все группы** нажатием кнопки **[→]**. При этом все пользователи из исключаемых групп будут исключены из списка **Выбранные пользователи** на вкладке users_1.

Для удаления дочерней группы пользователей из данной группы требуется наличие привилегии User groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение данной группы;
- Подразделение дочерней группы пользователей, которая удаляется из данной группы.

При наличии активных ролей, назначенных на группу, из которой выполняется удаление дочерней группы, исполнителю операции требуется дополнительная привилегия Roles Membership — Manage. Области действия активных ролей с этой привилегией должны включать:

- Подразделения всех ролей, назначенных на родительскую группу;
- Подразделения всех пользователей из дочерней группы.

По результатам операции все пользователи дочерней группы теряют роли, которые наследовали от родительской группы.

Для включения данной группы пользователей в состав других групп пользователей необходимо в блоке **Состоит в группах** в списке **Все группы** отметить группы пользователей и перенести их в список **Выбранные группы** нажатием кнопки **[<-]**.

Для включения данной группы в состав группы пользователей (состоит в группах) требуется наличие привилегии User groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение данной группы;
- Подразделение группы пользователей, добавляемой в качестве родительской группы.

При наличии активных ролей, назначенных на группу, которая добавляется в качестве родительской группы, исполнителю операции требуется дополнительная привилегия Roles Membership — Manage. Области действия активных ролей с этой привилегией должны включать:

- Подразделения всех ролей, назначенных на родительскую группу;

- Подразделения всех пользователей из дочерней группы.

Также подразделения всех без исключения пользователей дочерней группы должны попадать в области действия всех ролей, назначенных на родительскую группу.

По результатам операции:

- Дочерняя группа наследует роли, назначенные на родительскую группу;
- Все пользователи в составе дочерней группы наследуют роли, назначенные на родительскую группу.

Для исключения данной группы пользователей из состава группы пользователей необходимо в блоке **Состоит в группах** в списке **Выбранные группы** отметить группу пользователей и перенести ее в список **Все группы** нажатием кнопки **[→]**.

Для удаления родительской группы для данной группы пользователей (состоит в группах) требуется наличие привилегии User groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение данной группы;
- Подразделение родительской группы пользователей, из которой удаляется данная группа.

При наличии активных ролей, назначенных на удаляемую родительскую группу, исполнителю операции требуется дополнительная привилегия Roles Membership — Manage. Области действия активных ролей с этой привилегией должны включать:

- Подразделения всех ролей, назначенных на родительскую группу;
- Подразделения всех пользователей из дочерней группы.

По результатам операции все пользователи дочерней группы теряют роли, которые наследовали от родительской группы.

При нажатии на кнопку **[+ Новая группа]** будет выполнен переход на карточку добавления новой группы (см. раздел **Пользователи и компьютеры → Группы пользователей → Добавление новой группы**).

Для применения изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу.

В разделе **Содержит группы непрямое наследование** приведен список всех групп, которые входят в состав групп, которые включены в состав просматриваемой группы.

В разделе **Состоит в группах** приведен список групп, в которых состоит просматриваемая группа.

В разделе **Состоит в группах непрямое наследование** приведен список всех групп, которые входят в состав групп, в которые включена просматриваемая группа.

Роли

На вкладке задаются типы администратора, которыми будут наделены группы пользователей, и отображаются наследуемые типы.

В блоке **Содержит роли** в списке **Выбранные роли** указаны типы администратора, которыми будут наделены группы пользователей. В списке **Все роли** указаны все типы администратора в системе. В списке **Все роли** отображаются не только предустановленные роли, но и те, которые создали сами пользователи.

Во всех списках доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить название типа администратора, результат поиска будет выводиться по мере ввода.

Во всех списках доступна фильтрация по значению поля **Состояние**. Для этого необходимо кликнуть на значок фильтрации и выбрать значение,по которому список будет отфильтрован.

Внизу каждого списка указано количество записей в данном списке.

Для наделения групп пользователей возможностями при администрировании соответствующему типу администратора необходимо в списке **Все роли** отметить типы, которыми требуется наделить группу пользователей, и перенести их в список **Выбранные роли** нажатием кнопки **[<-]**.

Для исключения групп пользователей из списка обладателей соответствующего типа необходимо в списке **Выбранные роли** отметить требуемые записи и перенести их в список **Все роли** нажатием кнопки **[→]**.

Для применения изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу.

В блоке **Наследует роли** указаны типы администратора, которые наследуются группами пользователей.

В списке доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить название типа администратора, результат поиска будет выводиться по мере ввода.

В списке доступна фильтрация по значению поля **Состояние**. Для этого необходимо кликнуть на значок фильтрации и выбрать значение, по которому список будет отфильтрован.

Внизу списка указано количество записей в данном списке.

Управление типами администратора также осуществляется в подразделе *Роли и права доступа* раздела *Управление доменом*.

1.4.3.4. Удаление группы пользователей

Группу пользователей или одновременно несколько групп пользователей можно удалить. Для этого необходимо отметить группу пользователей в списке и нажать кнопку **[- Удалить]**.

Для снятия отметки с группы пользователей можно нажать кнопку закрытия в правом верхнем углу.

Также удалить группу пользователей можно из ее карточки: открыть карточку нажатием на группу в списке, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить группу]**. После подтверждения удаления будет выполнен переход к списку групп пользователей.

1.4.4. Компьютеры

1.4.4.1. Список компьютеров

В подразделе осуществляется управления компьютерами, введенными в домен.

В подразделе приведен список компьютеров, введенных в домен, с указанием имени компьютера и его IP-адреса.

Для списка доступен поиск по имени компьютера. Для этого в поле поиска начать вводить имя, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество записей в списке.

1.4.4.2. Редактирование информации о компьютере

Редактирование информации о компьютере осуществляется на его карточке. Для перехода на карточку необходимо нажать на компьютер в списке.

На карточке информация о компьютере размещается на вкладках:

- **Основное**;
- **Группы**;
- **Групповые политики**;
- **Назначение ПО**;
- **Политики обновления**;
- **Удаленный доступ**.

Для изменение подразделения компьютера требуется наличие привилегия Computers - Set organization unit.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение компьютера до выполнения операции;
- Подразделение, в которое переносится компьютер.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки компьютера и возврата к списку компьютеров следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Основное

На вкладке приведена информация о компьютере и о его местоположении.

Для редактирования не доступно имя компьютера и псевдоним учетной записи компьютера. Остальные поля возможно изменить.

Группы

На вкладке задаются группы компьютеров, в которые будет входить компьютер.

В блоке **Состоит в группах** в списке **Выбранные группы** указаны группы компьютеров, в которые входит данный компьютер. В списке **Все группы** указаны все группы компьютеров домена.

Во всех списках доступен поиск по названию группы. Для этого в соответствующем поле поиска начать вводить название группы, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для добавления компьютера в состав группы необходимо в списке **Все группы** отметить группы, в которые требуется добавить компьютер, и перенести их в список **Выбранные группы** нажатием кнопки **[<-]**.

Для добавления компьютера в группу требуется наличие привилегии Computer groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение компьютера;
- Подразделение группы, в которую добавляется компьютер.

Для исключения компьютера из состава групп необходимо в списке **Выбранные группы** отметить требуемые записи и перенести их в список **Все группы** нажатием кнопки **[→]**.

Для удаление компьютера из группы требуется наличие привилегии Computer groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение компьютера;
- Подразделение группы, из которой исключается компьютер.

Создание новой группы компьютеров осуществляется в подразделе *Группы компьютеров*.

В блоке **Состоит в группах непрямое наследование** приведен список всех групп, которые входят в состав групп, в которые включена просматриваемая группа.

Групповые политики

На вкладке приводится список назначенных параметров групповых политик, которые могут быть применены к данному компьютеру. Групповые политики назначаются на подразделение в подразделе *Групповые политики* (раздел *Групповые политики*) или на вкладке **Групповые политики** карточки подразделения в подразделе *Организационная структура* (раздел *Пользователи и компьютеры*).

> **Внимание:** Данный список представляет собой моделирование результатов применения групповых политик. Это значит, что не все политики из данного списка могут быть применены на конкретном компьютере и не все политики могут быть отображены в данном списке. Чтобы групповая политика применилась к компьютеру, необходимо соблюдение требований к операционной системе и заполнение значений атрибутов.

Внизу списка указано количество параметров групповых политик, применяемых к данному компьютеру.

Настройки параметра выводятся в правой панели **Настройка параметра <имя параметра>**. Здесь отображается общая информация о параметре: объект групповой политики, подразделение, расположение подразделения в организационной структуре, требования к ОС и настройки атрибутов.

Назначение ПО

На вкладке в табличном виде отображается информация о ПО, устанавливаемом на данный компьютер в соответствии с политиками ПО.

Для устанавливаемого ПО указывается статус установки, значения параметров устанавливаемого ПО, а также информация об изменении на данном компьютере параметров, заданных политикой.

Для списка доступен поиск по наименованию ПО. Для этого в поле поиска начать вводить наименование, результат поиска будет выводиться по мере ввода.

Для списка ПО доступна фильтрация по значению столбца **Переопределено на хосте**, для этого необходимо нажать на значок фильтра рядом с названием столбца и отметить требуемые значения для фильтрации.

Внизу списка указано количество записей в списке.

Назначение политики ПО осуществляется на карточке политики ПО в подразделе *Политики ПО* (раздел *Установка и обновление ПО*)

Политики обновления

На вкладке в табличном виде отображается информация о политиках обновления ALD Pro, назначенных на данный компьютер: имя политики обновления и статус.

Для списка доступен поиск по наименованию политики обновления. Для этого в поле поиска начать вводить наименование, результат поиска будет выводиться по мере ввода.

Для списка политик обновления доступна фильтрация по значению столбца **Статус**, для этого необходимо нажать на значок фильтра рядом с названием соответствующего столбца и отметить требуемые значения для фильтрации.

Внизу списка указано количество записей в списке.

Назначение политики обновления ALD Pro осуществляется на карточке политики обновления ALD Pro в подразделе *Политики обновления ALD Pro*.

Удаленный доступ

Вкладка предоставляет возможность удаленного подключения к выбранному компьютеру с помощью установленного на нем приложения **Удаленный рабочий стол**.

Для удаленного подключения к компьютеру необходимо из выпадающего списка **Активные сессии** выбрать сессию, запущенную на компьютере, в поле **Пароль** ввести код доступа, который сообщит пользователь активной сессии, и затем нажать кнопку **[Подключиться]**.

После успешного подключения на вкладке отобразится рабочий стол выбранного компьютера.

На открывающейся боковой панеле (слева) расположены кнопки **Развернуть** - открыть рабочий стол удаленного компьютера на весь экран администратора, и **Выключить** - завершить подключение к удаленному компьютеру.

По умолчанию, администратор, подключающийся к выбранному компьютеру, имеет право на управление этим компьютером: открывать файлы и папки, запускать приложения и т.д.

Если при открытии приложения **Удаленный рабочий стол** пользователь активной сессии установит чек-бокс **Только просмотр**, то администратор сможет только видеть изменения на экране удаленного компьютера, без права управления.

1.4.4.3. Добавление компьютера в домен

Добавление компьютера в домен ALD Pro возможно двумя способами:

- путем подготовки компьютера и установки на нем клиентской части (см. *Подготовка компьютера и установка на нем клиентской части*)
- путем установки на компьютер ОС по сети с использованием портала управления ПК «ALD Pro» в соответствии с описанием подраздела *Установка ОС по сети* (раздел *Автоматизация*).

1.4.4.4. Удаление компьютера

Компьютер или одновременно несколько компьютеров возможно удалить. Для этого необходимо отметить компьютер в списке и нажать кнопку **[- Удалить]**.

Также удалить компьютер можно из его карточки: открыть карточку нажатием на компьютер в списке, затем на карточке нажать кнопку **[Удалить компьютер]**. После подтверждения удаления будет выполнен переход к списку компьютеров.

1.4.5. Группы компьютеров

В подразделе осуществляется управления группами компьютеров.

1.4.5.1. Список групп компьютеров

В подразделе приведен список групп компьютеров домена с указанием названия группы, подразделения, в которое входит группа, и описания группы.

Если группа входит в состав другой группы и напрямую (прямое наследование), и как участник другой группы (непрямое наследование), то отражается только прямое участие группы (**Состоит в группах**), а участие в составе другой группы (**Состоит в группах непрямое наследование**) не отражается.

Группа компьютеров может входить в состав только одного подразделения, при этом в состав одного подраздления может входить несколько групп компьютеров.

Для списка доступен поиск. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Справа от поисковой строки расположена кнопка **[+ Новая группа]**.

Внизу списка указано количество групп в домене.

1.4.5.2. Добавление новой группы компьютеров

Для добавления новой группы компьютеров нажать кнопку **[+ Новая группа]**, будет выполнен переход на карточку новой группы компьютеров.

На карточке на вкладке **Основное** заполнить обязательные поля **Имя группы компьютеров** и **Название подразделения**. В поле **Расположение подразделения в организационной структуре** автоматически указывается полный путь выбранного структурного подразделения. Также можно заполнить поле **Описание**.

Остальные вкладки станут доступны после сохранения группы компьютеров (см. *Редактирование информации о группе компьютеров*).

Для сохранения группы компьютеров нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку групп компьютеров нажать на кнопку закрытия.

Для добавление родительской группы компьютеров (состоит в группах) требуется наличие привилегии Computer groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение дочерней группы компьютеров;
- Подразделение группы компьютеров, добавляемой в качестве родительской группы.

Для добавление дочерней группы компьютеров (состоит в группах) требуется наличие привилегии Computer groups - Set group membership. Области действия активных ролей с этой привилегией должны включать:

- Подразделение родительской группы компьютеров;
- Подразделение группы компьютеров, которая добавляется в качестве дочерней.

1.4.5.3. Редактирование информации о группе компьютеров

Редактирование информации о группе компьютеров осуществляется на ее карточке. Для перехода на карточку необходимо нажать на группу компьютеров в списке.

На карточке информация о группе компьютеров размещается на вкладках:

- **Основное**;
- **Компьютеры**;
- **Группы**;
- **Политики обновления**

Для изменения подразделения группы компьютеров требуется наличие привилегии Computer groups - Set organization unit.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение группы компьютеров до выполнения операции;
- Подразделение, в которое переносится группа компьютеров.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Основное

На вкладке приведена информация о группе компьютеров. Поле **Имя группы компьютеров** недоступно для редактирования, остальные поля можно изменить.

Компьютеры

На вкладке в списке **Выбранные компьютеры** приведен список компьютеров, включенных в состав данной группы. В списке **Все компьютеры** приведен список всех компьютеров домена.

Во всех списках доступен поиск по имени компьютера. Для этого в соответствующем поле

поиска начать вводить имя, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для добавления компьютера в группу необходимо в списке **Все компьютеры** отметить компьютеры и перенести их в список **Выбранные компьютеры** нажатием кнопки **[<-]**.

Для добавления компьютера в группу требуется наличие привилегии Computer groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение группы компьютеров;
- Подразделение компьютера, добавляемого в группу.

Для исключения компьютеров из состава группы необходимо в списке **Выбранные компьютеры** отметить требуемые компьютеры и перенести их в список **Все компьютеры** нажатием кнопки **[→]**.

Для удаления компьютера из группы требуется наличие привилегии Computer groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение группы компьютеров;
- Подразделение компьютера, удаляемого из группы.

Группы

В разделе **Содержит группы** в списке **Выбранные группы** приведены группы компьютеров, которые включены в данную группу.

> **Внимание:** Использование циклических (замнутых) наследований групп компьютеров может привести к нежелательному поведению системы в различных ее частях. Не рекомендуется использовать данную архитектуру групп.

В разделе **Состоит в группах** в списке **Выбранные группы** приведены группы компьютеров, в которые входит данная группа.

В каждом разделе приведен список **Все группы**, в котором указаны все группы компьютеров домена.

Во всех списках доступен поиск по названию группы. Для этого в соответствующем поле поиска ввести значение от трех символов, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для включения групп компьютеров в состав данной группы компьютеров необходимо в разделе **Содержит группы** в списке **Все группы** отметить группы компьютеров и перенести их в список **Выбранные группы** нажатием кнопки **[<-]**.

Для добавления группы компьютеров в данную группу требуется наличие привилегии Computer groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение данной группы;
- Подразделение группы компьютеров, которая добавляется в качестве дочерней.

Для исключения групп компьютеров из состава данной группы компьютеров необходимо в разделе **Содержит группы** в списке **Выбранные группы** отметить требуемые записи и перенести их в список **Все группы** нажатием кнопки **[→]**.

Для удаления группы компьютеров из данной группы требуется наличие привилегии Computer groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение данной группы;
- Подразделение дочерней группы компьютеров, которая удаляется из данной группы.

Для включения данной группы компьютеров в состав других групп компьютеров необходимо в разделе **Состоит в группах** в списке **Все группы** отметить группы компьютеров и перенести их в список **Выбранные группы** нажатием кнопки **[<-]**.

Для включения данной группы в состав группы компьютеров (состоит в группах) требуется наличие привилегии Computer groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение данной группы;

- Подразделение группы компьютеров, добавляемой в качестве родительской группы.

Для исключения данной группы компьютеров из состава группы компьютеров необходимо в разделе **Состоит в группах** в списке **Выбранные группы** отметить группу компьютеров и перенести ее в список **Все группы** нажатием кнопки **[→]**.

Для удаления данной группы из состава группы компьютеров (состоит в группах) требуется наличие привилегии Computer groups - Set group membership.

Области действия активных ролей с этой привилегией должны включать:

- Подразделение данной группы;
- Подразделение родительской группы компьютеров, из которой удаляется данная группа.

В разделе **Содержит группы непрямое наследование** приведен список всех групп, которые входят в состав групп, которые включены в состав просматриваемой группы.

В разделе **Состоит в группах** приведен список групп, в которых состоит просматриваемая группа.

В разделе **Состоит в группах непрямое наследование** приведен список всех групп, которые входят в состав групп, в которые включена просматриваемая группа.

Политики обновления

На вкладке в табличном виде отображается информация о политиках обновления ALD Pro, назначенных на группу компьютеров: имя политики обновления и статус.

Для списка доступен поиск по наименованию политики обновления. Для этого в поле поиска начать вводить наименование, результат поиска будет выводиться по мере ввода.

Для списка политик обновления доступна фильтрация по значению столбца **Статус**, для этого необходимо нажать на значок фильтра рядом с названием соответствующего столбца и отметить требуемые значения для фильтрации.

Внизу списка указано количество записей в списке.

Назначение политики обновления ALD Pro осуществляется на карточке политики обновления ALD Pro в подразделе *Политики обновления ALD Pro*.

1.4.5.4. Удаление группы компьютеров

Удаление группы компьютеров осуществляется из ее карточки. Для открытия карточки нажать на группу в списке, затем на карточке нажать кнопку **[Удалить группу]**. После подтверждения удаления будет выполнен переход к списку групп компьютеров.

1.4.6. Корзина

В разделе осуществляется управления учетными записями пользователей, которые были перемещены в корзину.

1.4.6.1. Список пользователей, перемещенных в корзину

В подразделе приведен список всех учетных записей пользователей с указанием имени пользователя, имени учетной записи, даты перемещения в корзину и даты окончательного удаления.

Для списка доступен поиск по имени пользователя. Для этого в поле поиска начать вводить имя, результат поиска будет выводиться по мере ввода. Доступна фильтрация списка по дате перемещения в корзину и дате окончательного удаления.

Внизу списка указано количество учетных записей.

Важно: Срок хранения удаленных учетных записей составляет 180 календарных дней. По истечению этого периода учетные записи будут удалены окончательно.

1.4.6.2. Восстановление пользователя из корзины

Восстановить пользователя можно из его карточки: открыть карточку нажатием на пользователя в списке, затем на карточке на вкладке **Основное** нажать кнопку **[Восстановить учетную запись]**. Далее необходимо задать новый пароль для восстанавливаемой учетной записи после чего будет выполнен переход к списку пользователей, перемещенных в корзину.

Для восстановления пользователя из Корзины требуется наличие привилегии Users -

Return from trash.

Области действия активных ролей с этой привилегией должны включать привязку к корневому подразделению.

Пользователь восстанавливается в корень домена.

Восстановленному из Корзины пользователю автоматически не возвращаются назначенные ему ранее роли.

1.4.6.3. Окончательное удаление пользователя

Пользователя или одновременно нескольких пользователей можно удалить. Для этого необходимо отметить пользователя в списке и нажать кнопку **[Удалить]**.

Для снятия отметки с пользователя можно нажать кнопку **[X Закрыть]** в правом верхнем углу.

Также удалить пользователя можно из его карточки: открыть карточку нажатием на пользователя в списке, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить учетную запись]**. После подтверждения удаления будет выполнен переход к списку пользователей, перемещенных в корзину.

1.5. Автоматизация

В разделе представлены функции автоматизации управления рабочими станциями и серверами. Включает в себя подразделы:

1.5.1. Задания автоматизации

Автоматизация — это любые действия с компьютером: от установки пакетов до запуска и управления процессами в операционной системе. Задачи автоматизации создаются через скрипт на **Salt-Stack**, который портал управления может принудительно запустить на одном из включенных в домен компьютеров или группе компьютеров.

Подраздел предоставляет функции запуска заданий автоматизации и сведения о запущенных заданиях.

1.5.1.1. Журнал заданий

Список заданий

На вкладке в табличном виде приведена информация о запущенных заданиях автоматизации с указанием даты запуска, названия задания, инициатора задания и статуса задания.

В столбце **Статус** отображается статус выполнения задания.

В списке доступен поиск по названию. Для этого в соответствующем поле поиска ввести значение. Также доступна фильтрация по дате запуска задания и статусу задания, для этого нажать на значок фильтра рядом с названием соответствующего столбца и выбрать значения для фильтрации.

При выборе задания будет отображена карточка с полной информацией о запуске задания.

В левом нижнем углу списка указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Для закрытия вкладки нажать на кнопку закрытия.

Карточка задания

Для открытия карточки задания нажать на соответствующую строку в списке заданий.

На карточке задания приводится вся информация о задании.

В системе используются задания двух типов:

- кастомные задания;
- миграции.

Для закрытия карточки и возврата к списку заданий нажать на кнопку закрытия.

Основное

На вкладке отображается следующая основная информация о задании:

- **Название**;

- **Статус**;
- **Дата запуска**;
- **Инициатор запуска**;
- **Участники**.

Параметры задания

На вкладке отображаются параметры задания и их значения, с которыми было запущено задание автоматизации.

В левом нижнем углу списка указано количество записей, а в правом нижнем углу кнопки переключения страниц.

1.5.1.2. Каталог заданий автоматизации

На вкладке в структурированном виде представлены задания автоматизации, созданные в подразделе *Каталог заданий автоматизации* (раздел *Управление доменом*).Для просмотра содержимого папки необходимо выбрать ее.

Выбор и просмотр задания

В каталоге доступен поиск по названию папки или задания. Для этого в соответствующем поле поиска ввести значение.

При выборе задания будет отображена форма **Задание автоматизации** в правой части вкладки, которой приведено описание задания автоматизации.

Запуск задания

Для запуска задания необходимо выбрать его в каталоге и нажать кнопку **[Запустить задание]**.

В открывшейся карточке запуска задания необходимо выбрать компьютеры, на которых требуется запустить задание.

Значения полей **Наименование задания автоматизации** и **Каталог заданий** заполняются

автоматически (параметры заданию задаются на карточке задания в подразделе *Каталог заданий автоматизации* (раздел *Управление доменом*))

Для выбора компьютеров, на которых необходимо запустить задание, в блоке **Запустить на компьютер** в списке **Все компьютеры** отметить требуемые записи и перенести их в список **Выбранные компьютеры** нажатием кнопки **[<-]**.

Для исключения компьютеров из списка выбранных необходимо в списке **Выбранные компьютеры** отметить требуемые записи и перенести их в список **Все компьютеры** нажатием кнопки **[→]**.

Выбор группы компьютеров выполняется в блоке **Запустить на группу компьютеров** аналогично выбору компьютеров.

Выбор компьютеров подразделений выполняется в блоке **Запустить на компьютеры подразделения** аналогично выбору компьютеров.

Во всех списках доступен поиск по названию. Для этого в соответствующем поле поиска ввести значение от трех символов, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для запуска задания необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки без запуска задания нажать на кнопку закрытия.

1.5.2. Установка ОС по сети

В подразделе выполняется управление серверами для установки ОС по сети, а также:

- определение перечня компьютеров для установки ОС по сети;
- выполнение установки ОС по сети и ввод компьютеров в домен;
- управление сценариями автоматической установки ОС и конфигурирования рабочей станции после установки ОС.

1.5.2.1. Список серверов установки ОС

В подразделе на вкладке **Серверы установки ОС** приведен список серверов установки ОС с указанием имени сервера, его IP-адреса и имени сайта.

В списке доступен поиск по названию и по IP-адресу сервера. Для этого в поле поиска ввести значение. Внизу списка указано количество записей в списке.

1.5.2.2. Создание сервера установки ОС

Для создания сервера установки ОС нажать кнопку **[Новый сервер]**, будет выполнен переход на карточку нового сервера.

На карточке на вкладке **Основное** заполнить обязательные поля:

- **Имя компьютера** — из перечня компьютеров, добавленных в ALD Pro выбрать компьютер, который будет выполнять функции сервера для установки ОС по сети;
- **Имя сайта** — из выпадающего списка выбрать сайт;
- **DHCP-сервер** — из списка развернутых в ALD Pro DHCP-серверов выбрать сервер для данного сервера установки ОС (поле для выбора доступно, если не отмечен пункт **Использовать внешний DHCP-сервер**).

Пункт **Использовать внешний DHCP-сервер** необходимо отметить, если планируется использовать внешний DHCP-сервер. При отмеченном пункте выбор DHCP-сервера не доступен.

Остальные вкладки станут доступны после сохранения сервера.

Для сохранения сервера необходимо нажать на кнопку сохранения. Будет выполнен переход к списку серверов.

Для закрытия карточки и возврата к списку серверов нажать на кнопку закрытия.

1.5.2.3. Редактирование сервера установки ОС

Редактирование сервера осуществляется на его карточке. Для перехода на карточку необходимо нажать на сервер в списке.

Для закрытия карточки сервера и возврата к списку нажать на кнопку закрытия.

Основное

На вкладке указана основная информация о сервере: имя компьютера, имя сайта и DHCP-сервер (если не установлен флаг **Использовать внешний DHCP-сервер**).

Для редактирования доступно имя сайта и DHCP-сервер см. *Создание сервера установки ОС*.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Перечень компьютеров

На вкладке осуществляется управление компьютерами, на которые будет выполняться установка ОС с данного сервера.

Список компьютеров

На вкладке приведен список компьютеров, которые подключены к данному серверу, с указанием имени компьютера, его MAC-адреса, операционной системы и профиля.

В списке доступен поиск по названию и MAC-адресу компьютера. Для этого в поле поиска ввести значение.

Добавление компьютера

Для добавления в перечень нового компьютера нажать кнопку **[+ Новый компьютер]**, будет выполнен переход на карточку нового компьютера.

На карточке заполнить обязательные поля:

- **Имя компьютера** — задать имя, которое будет использоваться для идентификации компьютера в ALD Pro;

Важно: В названии имени компьютера можно использовать только строчные латинские буквы[a-z], цифры [1-9] и дефис[-]

- **Профиль загрузки** — из выпадающего списка выбрать профиль, в соответствии с которым будет установлено и настроено программное обеспечение на добавляемом компьютере. Профили загрузок формируются на вкладке *Профили загрузок*
- **MAC-адрес** — указать MAC-адрес добавляемого компьютера.

Также можно заполнить поле **Модель**, указав в нем дополнительную информацию о добавляемом компьютере.

Поле **Домен** заполняется автоматически, в нем указан домен, в который будет введен добавляемый компьютер после установки на нем ОС.

Для добавления компьютера нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки без добавления компьютера нажать на кнопку закрытия.

Редактирование информации о компьютере

Редактирование информации о компьютере осуществляется на его карточке. Для перехода на карточку необходимо нажать на компьютер в списке.

На карточке приведена основная информация о компьютере. Для редактирования доступны поля **Профиль загрузки** и **Модель** (см. *Добавление компьютера*).

Для применения изменений нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку компьютеров нажать на кнопку закрытия.

Удаление компьютера

Компьютер или одновременно несколько компьютеров можно удалить из перечня подключенных к серверу. Для этого необходимо отметить компьютер в списке и нажать кнопку **[Удалить]**.

Также удалить компьютер из перечня можно из его карточки: открыть карточку нажатием на компьютер в списке, затем на карточке нажать кнопку **[Удалить компьютер]**. После подтверждения удаления будет выполнен переход к списку компьютеров.

Профили загрузок

На вкладке осуществляется управление профилями установки ОС и ПО на компьютеры, подключаемые к данному серверу.

Список профилей загрузки

На вкладке приведен список профилей для установки ОС и ПО на компьютеры с указанием названия профиля.

В списке доступен поиск по названиям профиля. Для этого в поле поиска ввести значение.

Внизу списка указано количество записей в списке.

Создание профиля загрузки

Для создания нового профиля загрузки нажать кнопку **[Новый профиль]**, будет выполнен переход на карточку нового профиля.

На карточке на вкладке **Основные свойства** заполнить обязательное поле:

- **Название профиля** — отображаемое имя профиля.

После сохранения профиля станут доступны для редактирования остальные вкладки (см. *Редактирование профиля загрузки*).

Для сохранения профиля нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки профиля без сохранения нажать на кнопку закрытия.

Редактирование профиля загрузки

Редактирование профиля осуществляется на его карточке. Для перехода на карточку необходимо нажать на профиль в списке.

Для закрытия карточки и возврата к списку профилей нажать на кнопку закрытия.

Основные свойства

На вкладке указана основная информация о профиле загрузки - название профиля, доступное для редактирования.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Preseed

На вкладке **Preseed** осуществляется управление файлом конфигурации для автоматической установки ОС на клиентах ALD Pro.

На вкладке отображается актуальный текст файла конфигурации.

Пример

```
# Подключение сетевого репозитория
d-i mirror/protocol string http
d-i mirror/http/hostname string download.astralinux.ru
d-i mirror/http/directory string /astra/frozen/1.7_x86-64/1.7.3/repository-
↪base
# Установка локали и языка
d-i mirror/country string manual
d-i debian-installer/locale string ru_RU
d-i debian-installer/locale select ru_RU.UTF-8
d-i debian-installer/language string ru
d-i debian-installer/country string RU
d-i debian-installer/keymap string ru
# Выбор клавиатуры
d-i console-tools/archs select at
d-i console-keymaps-at/keymap select ru
d-i console-setup/toggle string Alt+Shift
d-i console-setup/layoutcode string ru
d-i keyboard-configuration/toggle select Alt+Shift
d-i keyboard-configuration/layoutcode string ru
d-i keyboard-configuration/xkb-keymap select ru
d-i languagechooser/language-name-fb select Russian
d-i countrychooser/country-name select Russia
# Автоматический выбор сетевого интерфейса
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
d-i netcfg/choose_interface select auto
# Подключение non-free,contrib компонентов в репозитории
d-i apt-setup/non-free boolean true
d-i apt-setup/contrib boolean true
d-i apt-setup/services-select none
# Установка часового пояса UTC
d-i clock-setup/utc boolean true
# Временная зона
d-i time/zone string Europe/Moscow
# Не обновлять время
d-i clock-setup/ntp boolean false
# Автоматическая разметка дисков
d-i partman-base    partman/default_filesystem      string  ext4
d-i partman-auto/init_automatically_partition \
      select Авто - использовать весь диск
d-i partman-auto/method string regular
d-i partman-auto/purge_lvm_from_device boolean true
d-i partman-lvm/confirm boolean true
# Разметка для режима bios
#d-i partman-auto/choose_recipe select atomic
# для UEFI режима:
#d-i partman-auto/choose_recipe select /lib/partman/recipes-amd64-efi/
 ↪30atomic
# Не задавать вопросов при разметке
d-i partman/confirm_write_new_label boolean true
d-i partman/choose_partition select finish
d-i partman/confirm boolean true
d-i partman-auto-crypto/erase_disks     boolean true
d-i partman-basicfilesystems/no_swap boolean    false
d-i partman-target/mount_failed boolean true
d-i partman-partitioning/unknown_label boolean  true
d-i partman-auto/purge_lvm_from_device string   true
d-i partman-lvm/vgdelete_confirm boolean        true
d-i partman/confirm_write_new_label     string  true
d-i partman-lvm/confirm boolean true
d-i partman/confirm_nooverwrite boolean true
d-i anna/no_kernel_modules boolean true
d-i base-installer/kernel/image string linux-image-generic
# Создание пользователя при установке
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
d-i passwd/make-user boolean true
# Имя пользователя
d-i passwd/user-fullname string astra
d-i passwd/username string astra
# Пароль пользователя
d-i passwd/user-password password 12345678
d-i passwd/user-password-again password 12345678
d-i debian-installer/allow_unauthenticated string true
# Выбор рабочего стола Fly
tasksel tasksel/first multiselect Fly, Fly-ssh
tasksel tasksel/astra-feat-setup multiselect
# Дополнительные пакеты
# Специфические настройки Астры
d-i astra-additional-setup/os-check select Base security level Orel
d-i astra-additional-setup/additional-settings-orel multiselect
astra-additional-setup astra-additional-setup/automatic-network-disable
 ↪multiselect
d-i     astra-additional-setup/automatic-network-disable multiselect
d-i desktop-tablet-mode-switch/tablet-mode multiselect
popularity-contest popularity-contest/participate boolean false
#  В GRUB будет только 1 операционная система
d-i grub-installer/only_debian boolean true
# Установка в mbr
d-i grub-installer/with_other_os boolean true
# Установка пароля Grub
d-i grub-installer/password password 12345678
d-i grub-installer/password-again password 12345678
grub-installer grub-installer/password-mismatch error
# Не показывать диалог окончания установки
d-i finish-install/reboot_in_progress note
d-i finish-install/exit/poweroff boolean true
# Команды, выполняемые после установки ОС
d-i preseed/late_command string in-target systemctl enable ssh; \
    in-target bash -c "echo -e \"astra:astra\" | chpasswd"; \
    in-target bash -c "apt-get -y purge linux-image-*-hardened"; \
    in-target bash -c "apt-get -y autoremove --purge"; \
    in-target bash -c "sed -i 's/deb-src/#deb-src/g' /etc/apt/sources.list"; \
 ↪
    in-target bash -c "/usr/bin/wget -O /tmp/postinstall.sh http://192.168.17.
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
↪5/tftp/{PROFILE_UNIQ_NAME}/{POSTINSTALL_FILE_NAME}";\
    in-target bash -c "/bin/sh -x /tmp/postinstall.sh";\
    echo
```

Важно: Репозиторий `/astra/frozen/1.7_x86-64/1.7.3/repository-base` - это стандартный репозиторий Astra Linux, использованный в качестве примера. Для установки ОС по сети необходимо вместо базового репозитория указать репозиторий установочного диска.

Добавить или изменить файл конфигурации можно двумя способами:

- добавить текст из файла на компьютере;
- вручную ввести или изменить текст файла конфигурации на вкладке.

Для добавления текста конфигурации из файла необходимо нажать кнопку **[Загрузить из файла]**, в окне навигации выбрать на компьютере необходимый файл в формате *.cfg и нажать **[Открыть]**.

Содержимое файла отобразится в форме **Редактировать скрипт вручную**, при этом предыдущее содержимое файла конфигурации будет заменено. При необходимости добавленный текст можно отредактировать.

Для сохранения файла конфигурации необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку **[Отменить]**.

Для добавления или редактирования файла конфигурации вручную необходимо нажать на кнопку **[Редактировать файл]**, после чего форма **Редактировать скрипт вручную** станет доступна для редактирования.

Для сохранения файла конфигурации необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку **[Отменить]**.

Для просмотра истории изменений файла конфигурации необходимо нажать на кнопку **[История изменений]**. Откроется карточка с отображением списка изменений с указанием даты изменения, автора изменения и комментария. В списке доступен поиск, для этого в верхнем левом углу вкладки в поле поиска ввести значение. В левом нижнем углу указано

количество записей, а в правом нижнем углу кнопки переключения страниц.

Postinstall

На вкладке **Postinstall** осуществляется управление скриптом настройки ОС после ее установки на клиентах ALD Pro.

На вкладке отображается актуальный текст скрипта.

Пример

```
#!/bin/bash
set -x

sudo systemctl enable ssh
#Добавление репозиториев Astra Linux
cat <<EOL > /etc/apt/sources.list
deb http://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/repository-
 ↪base 1.7_x86-64 main non-free contrib
deb http://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/repository-
 ↪extended 1.7_x86-64 main contrib non-free
EOL
#Добавление репозиториев ALD Pro
cat <<EOL > /etc/apt/sources.list.d/aldpro.list
deb http://download.astralinux.ru/aldpro/stable/repository-main/ 1.4.0 main
deb http://download.astralinux.ru/aldpro/stable/repository-extended/ generic
 ↪main
EOL
#Установка приоритетов репозиториев
cat <<EOL > /etc/apt/preferences.d/aldpro
Package: *
Pin: release n=generic
Pin-Priority: 900
EOL
# Скачать скрипт первого запуска
# Необходимо заменить IP адрес на ваш сервер ОС
wget http://192.168.17.5/tftp/{PROFILE_UNIQ_NAME}/{FIRSTSTART_FILE_NAME} -O /
 ↪usr/bin/firststart.sh
# Подготовка сервиса первого запуска ОС
cat <<EOL > /etc/systemd/system/firststart.service
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
[Unit]
Wants=network-online.target
After=network-online.target

[Service]
Type=oneshot
RemainAfterExit=yes
ExecStart=/usr/bin/firststart.sh start

[Install]
WantedBy=multi-user.target
EOL
# Запуск сервиса
chmod 774 /usr/bin/firststart.sh
systemctl enable firststart || true
```

Добавить или изменить скрипт можно двумя способами:

- добавить текст скрипта из файла на компьютере;
- вручную ввести или изменить текст скрипта на вкладке.

Для добавления текста скрипта из файла необходимо нажать кнопку **[Загрузить из файла]**, в окне навигации выбрать на компьютере необходимый файл в формате *.sh и нажать **[Открыть]**.

Содержимое файла отобразится в форме **Редактировать скрипт вручную**, при этом предыдущее содержимое скрипта будет заменено. При необходимости добавленный текст скрипта можно отредактировать.

Для сохранения изменений в скрипте необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в скрипт нажать кнопку **[Отменить]**.

Для добавления или редактирования скрипта вручную необходимо нажать кнопку **[Редактировать файл]**, после чего форма **Редактировать скрипт вручную** станет доступна для редактирования.

Для сохранения изменений в скрипте необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в скрипт нажать кнопку **[Отменить]**.

Для просмотра истории изменений скрипта необходимо нажать кнопку **[История изменений]**. Откроется карточка с отображением списка изменений с указанием даты

изменения, автора изменения и комментария. В списке доступен поиск, для этого в верхнем левом углу вкладки в поле поиска ввести значение. В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Первый запуск

На вкладке **Первый запуск** осуществляется управление скриптом конфигурирования клиента ALD Pro при первом запуске ОС после ее установки и настройки.

На вкладке отображается актуальный текст скрипта.

Пример

```
#!/bin/bash
set -x
# Установка клиента ALD Pro и ввод компьютера в домен
case $1 in
    start)
        apt-get update
        export DEBIAN_FRONTEND=noninteractive
        apt-get install -yq aldpro-client wget
        mkdir -p /etc/ssl/freeipa
        wget -O /root/token http://192.168.17.5/tftp/tokens/$(hostname -f).
↪pwd # Указать IP адрес вашего сервера установки ОС
        ipa-client-install --hostname=$(hostname -f) --domain=$(hostname -d) -
↪-mkhomedir --password=$(cat /root/token) -U
        rm -f /etc/aldpro-salt/minion_id
        /usr/bin/python3 /opt/rbta/aldpro/client/bin/aldpro-service-discovery.
↪py single
        systemctl restart aldpro-salt-minion
        ln -s /usr/bin/astra-freeipa-domains-ctl /etc/domains.list.d/
        sed -e "s/^astra-admin.*/&,admin,admin@$(hostname -d)/" -i /etc/
↪group 2>/dev/null >/dev/null
        systemctl disable firststart
        reboot
        ;;
    stop)
        systemctl disable firststart
        ;;
    *)
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
        echo "$Usage: $0 {start|stop}"
        ;;
esac
```

Добавить или изменить скрипт можно двумя способами:

- добавить текст скрипта из файла на компьютере;
- вручную ввести или изменить текст скрипта на вкладке.

Для добавления текста скрипта из файла необходимо нажать кнопку **[Загрузить из файла]**, в окне навигации выбрать на компьютере необходимый файл в формате *.sh и нажать **[Открыть]**.

Содержимое файла отобразится в форме **Редактировать скрипт вручную**, при этом предыдущее содержимое скрипта будет заменено. При необходимости добавленный текст скрипта можно отредактировать.

Для сохранения изменений в скрипте необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в скрипт нажать кнопку **[Отменить]**.

Для добавления или редактирования скрипта вручную необходимо нажать кнопку **[Редактировать файл]**, после чего форма **Редактировать скрипт вручную** станет доступна для редактирования.

Для сохранения изменений в скрипте необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в скрипт нажать кнопку **[Отменить]**.

Для просмотра истории изменений скрипта необходимо нажать кнопку **[История изменений]**. Откроется карточка с отображением списка изменений с указанием даты изменения, автора изменения и комментария. В списке доступен поиск, для этого в верхнем левом углу вкладки в поле поиска ввести значение. В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Настройка boot-меню

На вкладке **Настройка boot-меню** осуществляется управление файлом настройки boot-меню на клиентах ALD Pro.

На вкладке отображается актуальный текст файла настройки.

Пример

```
UI vesamenu.c32

# 0 - отключение приглашения командной строки. Загрузка начнется сразу
PROMPT 0

# Автоматический выбор меню по таймеру. Секунды вычисляются делением на 10
 ↪введенного значения
TIMEOUT 100

DEFAULT bootlocal # Выбор по умолчанию загрузки с диска
#DEFAULT pxeinstall # Выбор по умолчанию загрузки по сети

menu background isolinux/aldpro_bios.png
menu title User Management Portal Boot Menu

# Локальная загрузка с диска
LABEL bootlocal
    menu label Boot from first HDD
    kernel chain.c32
    append hd0 0
TEXT HELP
Normal boot from HDD
ENDTEXT

# Загрузка из сети
LABEL pxeinstall
    menu label PXE operation system install
    kernel linux
    append initrd=initrd.gz vga=788 auto=true priority=critical debian-
 ↪installer/locale=ru_RU console-keymaps-at/keymap=ru hostname={HOSTNAME}
 ↪domain={DOMAIN_REALM} astra-license/license=true url=http://192.168.17.5/
 ↪tftp/{PROFILE_UNIQ_NAME}/{PRESEED_FILE_NAME} interface=auto netcfg/dhcp_
 ↪timeout=60 # Необходимо указать IP адрес Вашего сервера установи ОС по сети
TEXT HELP
Install AstraLinux Operating System
ENDTEXT
```

Добавить или изменить файл настройки можно двумя способами:

- добавить текст из файла на компьютере;
- вручную ввести или изменить текст файла на вкладке.

Для добавления текста из файла необходимо нажать кнопку **[Загрузить из файла]**, в окне навигации выбрать на компьютере необходимый файл в формате *.conf или *.txt и нажать **[Открыть]**.

Содержимое файла отобразится в форме **Редактировать скрипт вручную**, при этом предыдущее содержимое файла настройки будет заменено. При необходимости добавленный текст можно отредактировать.

Для сохранения файла настройки необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл настройки нажать кнопку **[Отменить]**.

Для добавления или редактирования файла настройки вручную необходимо нажать на кнопку **[Редактировать файл]**, после чего форма **Редактировать скрипт вручную** станет доступна для редактирования.

Для сохранения файла настройки необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку **[Отменить]**.

Для просмотра истории изменений файла конфигурации необходимо нажать на кнопку **[История изменений]**. Откроется карточка с отображением списка изменений с указанием даты изменения, автора изменения и комментария. В списке доступен поиск, для этого в верхнем левом углу вкладки в поле поиска ввести значение. В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

GRUB.

На вкладке **GRUB** осуществляется управление скриптом настройки GRUB для клиента ALD Pro.

На вкладке отображается актуальный текст скрипта.

Пример

```
if loadfont $prefix/font.pf2 ; then
  set gfxmode=800x600
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
  set gfxpayload=keep
  insmod efi_gop
  insmod efi_uga
  insmod video_bochs
  insmod video_cirrus
  insmod gfxterm
  insmod png
  terminal_output gfxterm
fi

if background_image /isolinux/aldpro.png; then
  set color_normal=light-gray/black
  set color_highlight=white/black
else
  set menu_color_normal=cyan/blue
  set menu_color_highlight=white/blue
fi

# Установка Astra Linux Special Edition
menuentry 'Install AstraLinux Operating System' {
    set background_color=black
    linux    (http,192.168.17.5)/tftp/linux modprobe.blacklist=evbug debian-
 ↪installer/allow_unauthenticated=true auto=true priority=critical debian-
 ↪installer/locale=en_US console-keymaps-at/keymap=ru hostname={HOSTNAME}
 ↪domain={DOMAIN_REALM} astra-license/license=true url=http://192.168.17.5/
 ↪tftp/{PROFILE_UNIQ_NAME}/{PRESEED_FILE_NAME} interface=auto netcfg/dhcp_
 ↪timeout=60
    initrd   (http,192.168.17.5)/tftp/initrd.gz
}
```

Добавить или изменить файл настройки можно двумя способами:

- добавить текст из файла на компьютере;
- вручную ввести или изменить текст файла на вкладке.

Для добавления текста конфигурации из файла необходимо нажать кнопку **[Загрузить из файла]**, в окне навигации выбрать на компьютере необходимый файл в формате *.cfg и нажать **[Открыть]**.

Содержимое файла отобразится в форме **Редактировать скрипт вручную**, при этом

предыдущее содержимое файла настройки будет заменено. При необходимости добавленный текст можно отредактировать.

Для сохранения файла настройки необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл настройки нажать кнопку **[Отменить]**.

Для добавления или редактирования файла настройки вручную необходимо нажать на кнопку **[Редактировать файл]**, после чего форма **Редактировать скрипт вручную** станет доступна для редактирования.

Для сохранения файла настройки необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку **[Отменить]**.

Для просмотра истории изменений файла конфигурации необходимо нажать на кнопку **[История изменений]**. Откроется карточка с отображением списка изменений с указанием даты изменения, автора изменения и комментария. В списке доступен поиск, для этого в верхнем левом углу вкладки в поле поиска ввести значение. В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Удаление профиля загрузки

Профиль загрузки или одновременно несколько профилей можно удалить. Для этого необходимо отметить профиль в списке и нажать кнопку **[Удалить]**.

Также удалить профиль можно из его карточки: открыть карточку нажатием на профиль в списке, затем на карточке нажать кнопку **[Удалить профиль]**. После подтверждения удаления будет выполнен переход к списку профилей.

1.5.2.4. Удаление сервера установки ОС

Для удаления сервера установки ОС открыть его карточку, нажав на сервер в списке, затем на карточке нажать кнопку **[Удалить]**. После подтверждения удаления будет выполнен переход к списку серверов.

1.6. Мониторинг

В разделе доступен просмотр журнала событий мониторинга и мониторинг подсистем ALD Pro.

1.6.1. Журнал событий мониторинга

В подразделе приводится информация о мониторинге событий.

Подраздел состоит из вкладок:

- **Журнал событий**;
- **Серверы мониторинга**.

1.6.1.1. Журнал событий

На вкладке в табличном виде приводится перечень событий мониторинга. Настройка сбора событий выполняется в подразделе *Настройка сбора журналов событий* (раздел *Журнал событий*)

Для событий указывается:

- дата и время появления;
- критичность события — предупреждение, ошибка и т.д.;
- сервер, на котором произошло событие;
- описание события;
- длительность события.

Для поиска или фильтрации событий необходимо в блоке **Фильтр** в соответствующих полях задать значения для поиска или фильтрации и нажать кнопку **[Применить]**.

Поиск или фильтрация доступны по одному или нескольким атрибутам:

- **Сервер**;
- **Описание события**;
- **Дата начала**;
- **Дата окончания**.

Дополнительно в списке событий доступна фильтрация по критичности события, для этого в столбце **Критичность** нажать на значок фильтра и указать значения для фильтрации.

В левом нижнем углу указано количество правил, а в правом нижнем углу кнопки переключения страниц.

Внизу списка событий в левом углу указано количество записей в журнале, в правом углу размещены кнопки смены страниц журнала.

Если не установлен глобальный каталог, то в портале управления будут на постоянной основе отображаться ошибки, не влияющие на работу Системы, при этом в журнале событий мониторинга будут зафиксированы события чрезвычайной критичности на контроллере домена:

- о неактивности глобального каталога (globalcatalog)
- о неактивности службы синхронизации объектов с глобальным каталогом (ipa-gcsyncd)

1.6.1.2. Серверы мониторинга

На вкладке осуществляется управление серверами мониторинга.

Список серверов мониторинга

На вкладке в табличном виде приведен список серверов мониторинга с указанием имени сервера, IP-адреса сервера, функций сервера и имени сайта.

В списке доступен поиск по всем значениям. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

В левом нижнем углу указано количество записей в списке, а в правом нижнем углу кнопки переключения страниц.

Развертывание сервера мониторинга

Для развертывания нового сервера мониторинга необходимо нажать на кнопку **[Развернуть сервер мониторинга]**, будет выполнен переход на карточку нового сервера мониторинга.

На карточке заполнить обязательные поля **Имя компьютера** и **Имя сайта**.

Для сохранения нового сервера мониторинга необходимо нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку серверов мониторинга.

Для закрытия карточки и возврата к списку серверов мониторинга нажать на кнопку закрытия.

Редактирование сервера мониторинга

Редактирование сервера мониторинга выполняется на его карточке. Для открытия карточки необходимо в списке нажать на соответствующий сервер мониторинга.

Для редактирования доступны функции сервера и имя сайта.

Для применения изменений нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку серверов мониторинга.

Для закрытия карточки и возврата к списку серверов мониторинга нажать на кнопку закрытия.

Удаление сервера мониторинга

Удаление сервера мониторинга выполняется из его карточки: открыть карточку нажатием в списке на соответствующий сервер мониторинга, затем на карточке нажать кнопку **[Удалить]**. После подтверждения удаления будет выполнен переход к списку серверов мониторинга.

1.6.2. Витрины мониторинга домена

Витрина мониторинга – это UI-виджет (дашборд) который отображает некоторую информацию о состоянии ALD Pro, её подсистем или подмодулей. Серве(а) мониторинга занимается сбором информации о состоянии ALD Pro и выводит их пользователю в графическом интерфейсе браузера в виде набора витрин мониторинга, что позволяет пользователю оценить состояние системы.

В подразделе осуществляется:

- просмотр виджетов событий мониторинга и графиков производительности;

- просмотр шаблонов мониторинга;
- контроль доступности, работоспособности и утилизации ресурсов компонентов системы.

Список серверов формируется автоматически из серверов, развернутый в домене. Требуется порядка 30 минут с момента развертывания, чтобы сервер попал в данный список.

Витрина из выпадающего списка **Каталог витрин** выводит данные в виде виджетов на панели ниже. С помощью витрины отслеживаются системные показатели каждой подсистемы:

- **Динамическая настройка узла**
- **Мониторинг**
- **Общий доступ к файлам**
- **Печать**
- **Портал управления**
- **Разрешение имен**
- **Репозитории программного обеспечения**
- **Синхронизация времени**
- **Служба каталогов**
- **Установка ОС по сети**

1.6.2.1. Просмотр витрины

Для просмотра информации необходимо выбрать значения из выпадающих списков **Сервер** и **Каталог витрин**, после чего будет отображена соответствующая информация о сервере. Для для поиска сервера или витрины необходимо начать вводить название по соответствующем поле.

По умолчанию выводится информация за последние 6 часов. Для вывода информации за более или менее продолжительный период необходимо выбрать период в выпадающем меню в правом верхнем углу панели виджетов.

Информация на виджетах может быть обновлена вручную или может быть настроено обновление через заданный период. По умолчанию обновление через заданный период отключено. Для обновления данных или задания периода обновления необходимо

кликнуть кнопку **Refresh dashboard** в правом верхнем углу панели виджетов.

Каждый из отображаемых на панели статусов может быть раскрыт. Для этого необходимо выбрать пункт “View” из выпадающего меню названия виджета. Для возврата к панели используется стрелка рядом с название панели.

Для каждой витрины подсистемы отображаются виджеты со статусом используемых на выбранном сервере служб. Доступные статусы:

- **Доступно**: служба установлена на сервере, работает в штатном режиме;
- **Авария**: служба недоступна, но установлена на сервере;
- **Нет данных**: служба не установлена на сервере.

Витрина **Мониторинг подсистемы “Портал управления”** также отображает данные по использованию памяти и ЦП процессами служб.

Витрина **Мониторинг подсистемы “Служба каталогов”** также отображает срок действия используемых сертификатов.

Витрина **Мониторинг системных показателей** отображает системные показатели каждого сервера.

Витрина **Мониторинг посистемы «Глобальный каталог»** отображает состояние целостности глобального каталога и служб контроля целостности и синхронизации глобального каталога. Целостность глобального каталога - соответствие объектов контроллера домена объектам глобального каталога. На панели **Целостность глобального каталога** отображается количество ошибок.

Примечание: Если не установлен глобальный каталог, на витринах мониторинга подсистемы «Глобальный каталог» контроллера домена будет зафиксирован статус ГК «Авария».

1.6.3. Расширение функционала мониторинга

Мониторинг событий ALD Pro реализован с использованием решения Zabbix. ALD Pro позволяет подключиться к web-интерфейсу Zabbix. Использование web-интерфейса Zabbix позволяет:

- расширить перечень событий, подлежащих мониторингу;
- использовать полный перечень функций Zabbix.

Для доступа к web-интерфейсу Zabbix необходимо ввести в браузере адрес сервера мониторинга ALD Pro в формате: `https://<адрес сервера мониторинга>/zabbix`

Пример `https://mon.aldpro.astralinux.ru/zabbix`

Далее в открывшемся окне авторизации необходимо ввести логин и пароль системной учетной записи администрирования Zabbix.

1.7. Модуль синхронизации

В разделе осуществляется управление модулем синхронизации объектов MS AD и ALD Pro.

Модуль синхронизации является отдельным от портала управления модулем. Основная задача модуля синхронизации – миграция в реальном времени изменений отлеживаемых LDAP-объектов в подключенном сервере Active Directory в контроллер домена ALD Pro, за которым закреплен модуль синхронизации.

Синхронизация может быть односторонней (MS AD → ALD Pro) и двусторонней (MS AD <→ ALD Pro).

Односторонняя синхронизация доступна объектам:

- User (Пользователи);
- OU (Подразделения);
- User Groups (Группы пользователей).

Двусторонняя синхронизация реализована только для паролей пользователей.

Важно: Для работы модуля синхронизации на контроллере домена Windows **Active**

Directory необходимо установить утилиту `passwdhk` на контроллере домена, используя установочный файл `PasswdhkSetup.msi`. Утилита автоматически регистрируется как фильтр паролей и не требует ручного конфигурирования групповых политик (GPO).

Модуль синхронизации имеет ряд ограничений в части синхронизации объектов, имеющих в своем составе специальные символы. Для удобства работы предоставлен инструмент обработки запрещенных символов (см. раздел **Справочные материалы → Синхронизация объектов, содержащих специальные символы**).

1.7.1. Настройки

В подразделе представлены функции управления синхронизацией паролей и контроллерами домена, участвующими в синхронизации.

1.7.1.1. Контроллеры домена AD

Создание нового контроллера AD

Для создания нового контроллера AD на вкладке **Контроллеры домена AD** необходимо нажать на кнопку **Создать**. В новом окне откроется карточка создания контроллера AD.

Все поля в карточке являются обязательными для заполнения.

В поле **Имя сервера** необходимо ввести наименование контроллера домена AD. В названии допустимо использовать строчные буквы латинского алфавита **a-z** и символы **.** и **-**.

В поле **Имя пользователя** необходимо ввести логин пользователя в формате `логин@домен_AD`. В названии допустимо использовать строчные буквы латинского алфавита **a-z** и символы @, **.** и **-**. Учетная запись пользователя должна обладать правами администратора домена в домене AD или ограниченными правами на контейнер **Delete Object** (Корзина) в домене AD и организационное подразделение (OU), задействованное для процесса синхронизации (см. раздел **Справочные материалы → Модуль синхронизации → Инструкция по дополнительной настройке модуля синхронизации**).

В поле **Пароль** ввести пароль от учетной записи.

Для заполнения поля **Сертификат** необходимо нажать на кнопку **Загрузить из файла** и загрузить сертификат в формате **.pem**. Данный сертификат должен быть сформирован и выгружен с помощью Центра сертификации AD.

Для сохранения нового контроллера AD нажать на кнопку **Сохранить**. Будет выполнен переход к вкладке контроллеров домена AD.

Для закрытия карточки создания нового контроллера AD и возврата к вкладке контроллеров домена AD нажать на кнопку закрытия «X».

Редактирование контроллера AD

Для редактирования контроллера AD необходимо нажать на запись контроллера AD в списке **Имя сервера**. Откроется карточка контроллера AD, для редактирования доступны все поля.

Для применения изменений нажать на кнопку **Сохранить**.

Для закрытия карточки редактирования контроллера AD и возврата к вкладке контроллеров домена AD нажать на кнопку закрытия «X».

Удаление контроллера AD

Контроллер домена AD можно удалить:

- на вкладке контроллеров домена AD, выделив нужный домен и нажав кнопку **Удалить**;
- на карточке контроллера домена AD, нажав кнопку **Удалить**.

После удаления контроллера AD будет выполнен переход на вкладку **Контроллеры домена AD**.

1.7.1.2. Контроллеры домена ALD

Создание нового контроллера ALD

Модуль синхронизации всегда устанавливается на первый контроллер домена. При установке модуля синхронизации контроллер домена **ALD** добавляется на вкладку

Контроллеры домена ALD автоматически.

При установке модуля синхронизации создается учетная запись имеющая вид `syncer/<имя сервера>@<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.

> **Внимание:** При обновлении на версию 2.4.0 и выше учетная запись текущего подключения изменится на сервисную.

Для создания нового контроллера ALD на вкладке **Контроллеры домена ALD** необходимо нажать на кнопку **Создать**. В новом окне откроется карточка создания контроллера ALD.

Все поля в карточке являются обязательными для заполнения.

В поле **Имя сервера** необходимо ввести имя компьютера в формате FQDN («имя_сервера.полное_имя_домена»), который выполняет роль первого контроллера домена ALD Pro. В названии допустимо использовать строчные буквы латинского алфавита **«a-z»** и символы **.** и **-**.

В поле **Имя пользователя** необходимо ввести служебную учетную запись, которая создается на контроллере домена и имеет вид `syncer/<имя сервера>@<имя домена>`.

Использование служебной учетной записи избавляет от необходимости смены пароля по истечению срока его действия.

Для заполнения поля **Сертификат** необходимо нажать на кнопку **Загрузить из файла** и загрузить сертификат в формате **.pem**. Данный сертификат можно получить на web-сайте ALD Pro средствами стандартного браузера.

Для сохранения нового контроллера ALD нажать на кнопку **Сохранить**. Будет выполнен переход к вкладке контроллеров домена ALD.

Для закрытия карточки создания нового контроллера ALD и возврата к вкладке контроллеров домена ALD нажать на кнопку закрытия «X».

Редактирование контроллера ALD

Для редактирования контроллера ALD необходимо нажать на запись контроллера ALD в списке **Имя сервера**.. Откроется карточка контроллера ALD, для редактирования доступны все поля.

Для применения изменений нажать на кнопку **Сохранить**.

Для закрытия карточки редактирования контроллера ALD папки и возврата к вкладке контроллеров домена ALD нажать на кнопку закрытия «X».

Удаление контроллера ALD

Контроллер домена ALD можно удалить:

- на вкладке контроллеров домена ALD, выделив нужный домен и нажав кнопку **Удалить**;
- на карточке контроллера домена ALD, нажав кнопку **Удалить**.

После удаления контроллера ALD будет выполнен переход на вкладку **Контроллеры домена ALD**.

1.7.1.3. Синхронизация паролей

Вкладка синхронизации паролей содержит поле получения пароля для сервиса отправки паролей.

Для получения открытого ключа необходимо нажать на кнопку **Получить ключ**.

Откроется окно подтверждения запроса на генерацию нового ключа. Для подтверждения необходимо нажать на кнопку **Перевыпустить**. Для отмены операции следует нажать на кнопку **Отменить**.

Результатом генерации нового ключа будет файл открытого ключа **public.gpg**, скачанный на устройство. В поле **Номер ключа** после нажатия кнопки обновиться порядковый номер сгенерированного открытого ключа.

После генерации необходимо добавить новый файл **public.gpg** на каждую реплику ALD Pro в расположение */opt/rbta/aldpro/syncer*. При каждом выпуске нового файла **public.gpg**, его необходимо тиражировать по всем репликам.

1.7.2. Источники

В подразделе представлены функции управления структурой синхронизации.

1.7.2.1. Сопоставление подразделений

Создание нового сопоставления

Важно: Синхронизация из ALD Pro в MS AD выполняется только для паролей пользователей. Все остальные атрибуты синхронизируются только из MS AD в ALD Pro.

Для создания нового сопоставления подразделений необходимо нажать на кнопку **Создать**. В новом окне будет открыта карточка создания сопоставления.

На карточке необходимо заполнить обязательные поля из выпадающих списков **Источник** и **Получатель**. Для каждого поля из структуры подразделений необходимо выбрать одно, для которых будет выполнена синхронизация.

Список поля **Источник** содержит перечень подразделений AD.

Список поля **Получатель** содержит перечень подразделений ALD, свернутый до родительского.

После выбора значений для полей **Источник** и **Получатель** для проверки возможных конфликтов синхронизации необходимо нажать кнопку **Проверить наличие конфликтов**.

На данном этапе проверяется наличие конфликтов синхронизации между **Источником** и **Получателем** до создания сопоставления подразделений.

Если конфликты не будут обнаружены, появится всплывающее уведомление об отсутствии конфликтов.

Если конфликты будут обнаружены, сообщение об их наличии будет отображено во всплывающем окне. Так же появится возможность скачать файл на вкладке **Структура дерева синхронизации**, содержащий список конфликтов. Решение о разрешении конфликтов вручную или их игнорировании принимает администратор.

Важно: Если проигнорировать возникшие конфликты и сохранить сопоставление

подразделений, объекты ALD Pro, конфликтующие с объектами AD, не будут изменены.

Для сохранения нового сопоставления нажать на кнопку **Сохранить**. Будет выполнен переход к вкладке сопоставления подразделений.

Для закрытия карточки создания сопоставления и возврата к вкладке сопоставления подразделений нажать на кнопку закрытия «X».

Важно: Подразделения, выбранные в качестве **Источника** и **Получателя**, должны сохранять своё положение и наименование в структуре. Изменение этих параметров приведёт к сбоям в синхронизации.

Удаление сопоставления

Для удаления сопоставления подразделений необходимо выделить запись в списке и нажать кнопку **Удалить**.

1.7.2.2. Структура дерева синхронизации

Вкладка содержит информацию об объектах, конфликтах синхронизации и о структуре подразделений виртуального дерева, через которое проходит синхронизация изменений.

Конфликты синхронизации

Для просмотра списка конфликтов необходимо нажать на кнопку **Проверить наличие конфликтов**. По нажатию кнопки запускается проверка наличия конфликтов синхронизации для всех сопоставлений подразделений AD и ALD Pro.

На данном этапе проверяется наличие конфликтов синхронизации оставшихся в процессе синхронизации сопоставлений подразделений.

Результатом будет всплывающее уведомление об отсутствии конфликтов или их наличии. При наличии конфликтов можно будет скачать файл, содержащий список конфликтов. Решение о разрешении конфликтов вручную или их игнорировании принимает администратор.

При выборе подразделения для просмотра объектов синхронизации становится доступен функционал ручного разрешения конфликтов:

- кнопка **Решить конфликт подразделения** разрешает конфликты синхронизации подразделения и появляется опционально при наличии конфликта синхронизации выбранного подразделения.
- кнопка **Решить**, имеющаяся у каждого объекта синхронизации, разрешает конфликты синхронизации конкретного объекта и делает его доступным для всех последующих синхронизаций.

Важно: Если кнопка **Решить конфликт подразделения** отображается в интерфейсе. Необходимо в первую очередь разрешить конфликты синхронизации подразделения, во вторую - конфликты синхронизации конкретных объектов.

1.7.3. Сопоставление атрибутов

В подразделе Сопоставление атрибутов представлен функционал управления атрибутами LDAP-объектов синхронизации.

1.7.3.1. Карта сопоставлений

Сопоставления по умолчанию

В модуле синхронизации имеется список сопоставлений атрибутов, синхронизирующихся по умолчанию.

Сопоставления отражаются на вкладке **Карта сопоставлений** и не доступны для удаления.

Кроме отображаемых сопоставлений по умолчанию, для объектов синхронизируются атрибуты, которые отвечают за наименование. Добавление сопоставлений атрибутов, отвечающих за имя объекта, может привести к ошибке. Например, сопоставление атрибутов OU-OU для подразделений.

Создание нового сопоставления

Важно: Синхронизация из ALD Pro в MS AD выполняется только для паролей пользователей. Все остальные атрибуты синхронизируются только из MS AD в ALD Pro.

Для создания нового сопоставления атрибутов необходимо нажать на кнопку **Создать**. Будет открыта карточка создания сопоставления.

В карточке необходимо заполнить обязательные поля из выпадающих списков:

- **Тип объекта синхронизации**:
  - **Подразделение**,
  - **Пользователь**,
  - **Группа**,
- **Атрибут AD**
- **Атрибут ALD**.

Для сохранения нового сопоставления нажать на кнопку **Сохранить**. Будет выполнен переход к вкладке карты сопоставления.

Для закрытия карточки создания сопоставления и возврата к вкладке карты сопоставления нажать на кнопку закрытия «X».

Удаление сопоставления

Для удаления сопоставления необходимо выделить запись в списке и нажать кнопку **Удалить**.

1.7.3.2. Атрибуты AD

Атрибуты AD по умолчанию

В модуле синхронизации имеется список атрибутов синхронизирующихся по умолчанию.

Атрибуты отражаются на вкладке Атрибуты AD и не доступны для удаления.

Создание нового атрибута AD

Для создания нового атрибута AD необходимо нажать на кнопку **Создать**. Будет открыта карточка создания атрибута AD.

В карточке необходимо заполнить обязательные поля **Имя атрибута** и **Атрибут LDAP**.

В значении поля **Имя атрибута** допустимо использовать строчные и прописные буквы латинского алфавита **a-z**, **A-Z** и цифры **0-9**.

В значении поля **Атрибут LDAP** допустимо использовать строчные и прописные буквы латинского алфавита **a-z**, **A-Z**, цифры **0-9** и символ **-**.

Для сохранения нового атрибута нажать на кнопку **Сохранить**. Будет выполнен переход к вкладке атрибуты AD.

Для закрытия карточки создания атрибута и возврата к вкладке атрибуты AD нажать на кнопку закрытия «X».

Удаление атрибута AD

Для удаления атрибута AD необходимо выделить запись в списке и нажать кнопку **Удалить**.

1.7.3.3. Атрибуты ALD

Атрибуты ALD по умолчанию

В модуле синхронизации имеется список атрибутов синхронизирующихся по умолчанию.

Атрибуты отражаются на вкладке Атрибуты ALD и не доступны для удаления.

Создание нового атрибута ALD

Для создания нового атрибута ALD необходимо нажать на кнопку **Создать**. Будет открыта карточка создания атрибута ALD.

В карточке необходимо заполнить обязательные поля **Имя атрибута** и **Атрибут LDAP**.

В значении поля **Имя атрибута** допустимо использовать строчные и прописные буквы латиницы и кириллицы **a-z**, **A-Z**, **а-я**, **А-Я** и цифры **0-9**.

В значении поля **Атрибут LDAP** допустимо использовать строчные и прописные буквы латинского алфавита **a-z**, **A-Z**, цифры **0-9** и символ **-**.

Для сохранения нового атрибута нажать на кнопку **Сохранить**. Будет выполнен переход к вкладке атрибуты ALD.

Для закрытия карточки создания атрибута и возврата к вкладке атрибуты ALD нажать на кнопку закрытия «X».

Удаление атрибута ALD

Для удаления атрибута ALD необходимо выделить запись в списке и нажать кнопку **Удалить**.

1.7.4. Особенности работы модуля синхронизации

1. При настройке модуля синхронизации рекомендуется поддерживать соотношение доменов один к одному, то есть выполнять синхронизацию объектов из одного домена MS AD в один домен ALD Pro. Настройка синхронизации из нескольких доменов MS AD в один домен ALD Pro увеличивает риски возникновения конфликтов синхронизации (так как конфликты могут возникать и между объектами доменов MS AD).

2. Нельзя производить переименование подразделений, добавленных в **Сопоставление подразделений**. Если возникла такая необходимость, корректно будет удалить сопоставление, произвести переименование и создать новое сопоставление подразделений. Область работы модуля синхронизации ограничена типами объектов `User`, `Group`, `OrganizationalUnit`, а так же контейнером `CN=Users`. Объекты других типов не отображаются для выбора в источниках синхронизации.

3. Нельзя создавать сопоставления подразделений для дочерних подразделений подразделения, уже участвующего в синхронизации.

4. В домене ALD Pro в разделе **Управление доменом → Пользователи и группы** содержится настройка **Максимальная длина имени пользователя**. Для успешной синхронизации длина имени пользователя AD должна быть меньше установленного

значения, в противном случае возникнет ошибка синхронизации.

5. Необходимо учесть, что в момент синхронизации учетная запись синхронизируемого пользователя временно блокируется. Блокировка не превышает 30 секунд.

6. Атрибуты по умолчанию и соответствующие им сопоставления ограничены перечнем обязательных атрибутов для объектов ALD Pro:

   - Пользователи: **Логин, Пароль, Подразделение, Фамилия** либо **Имя**
   - Группы пользователей: **Название группы, Подразделение**
   - Подразделения: **Наименование подразделения, Родительское подразделение**.

   Однако не все эти атрибуты явно указаны на карточке **Атрибуты AD, Атрибуты ALD**, так как их синхронизация происходит внутренними процессами модуля синхронизации. Добавляя эти атрибуты в явном виде в **Карте сопоставления**, есть риск нарушить логику работы модуля синхронизации.

7. Наименование подразделений, наименования групп, логины пользователей не должны содержать специальных символов, за исключением “.”, “-”, “_“.

8. Модуль синхронизации может быть установлен при первичной установке или в процессе обновления контроллера домена. Ограничением настоящей версии является установка модуля синхронизации только на первый контроллер домена. В случае отключении первого контроллера домена, синхронизация новых данных, добавленных после отключения первого контроллера домена, выполняться не будет. Ранее синхронизированные данные сохранятся и будут реплицироваться между контроллерами домена, для которых созданы соглашения о репликации.

9. Для успешной синхронизации учетную запись администратора, которая используется для подключения к контроллеру домена, необходимо добавить в группу **admins**.

10. При изменении пароля синхронизированного пользователя через интерфейс FreeIpa, синхронизация пароля **ALD Pro → AD** не произойдет. Для изменения пароля с последующей успешной синхронизацией необходимо использовать интерфейс ALD Pro.

11. Процесс изменения пароля пользователя через личный кабинет с последующей синхронизацией **ALD Pro → AD** проходит успешно, только при использовании личного кабинета, на котором был развернут модуль синхронизации.

12. При сбросе пароля пользователя через интерфейс ALD Pro временный пароль не

синхронизируется. После сброса пароля пользователя необходимо залогиниться в домене, изменить пароль с временного на постоянный и только тогда произойдет синхронизация пароля **ALD Pro → AD**.

13. Пароли пользователей MS AD, установленные до настройки модуля синхронизации, синхронизированы не будут.

    Синхронизация паролей пользователей после настройки модуля синхронизации и сопоставлений подразделений происходит по логике:

    - синхронизирован пользователь в домен ALD Pro → изменен пароль пользователя в домене MS AD → синхронизирован пароль пользователя в домен ALD Pro;
    - создан пользователь в домене MS AD → синхронизирован пользователь в домен ALD Pro.

14. При настройке синхронизации паролей между ALD Pro и MS AD рекомендуется вручную задать согласованные значения параметров политики паролей в обеих системах, так как их автоматическая синхронизация не предусмотрена.

15. При изменении расположения синхронизированного подразделения через MS AD, групповые политики привязанные к подразделению в домене ALD Pro, не сохранятся.

    Варианты решения:

    - Планировать иерархию подразделений таким образом, чтобы перенос подразделений не сказывался на работе групповых политик: добавление еще одного уровня вложенности, на который будут применяться ГП;
    - Повторно привязывать групповые политики после переноса подразделения.

1.8. Журнал событий

В разделе осуществляется настройка журнала событий (система аудита). Сервера журнала событий занимаются сбором ограниченного (но настраиваемого) набора событий с определённого набора компьютеров домена ALD Pro с помощью инструмента syslog-ng.

1.8.1. Серверы журнала событий

В подразделе выполняется развертывание серверов журнала событий.

1.8.1.1. Список серверов журнала событий

В подразделе на вкладке **Серверы журнала событий** приводится список серверов с указанием имени сервера, IP-адреса и имени сайта.

В списке доступен поиск по имени сервера, IP-адресу сервера и имени сайта. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

В левом нижнем углу указано количество серверов, а в правом нижнем углу кнопки переключения страниц.

1.8.1.2. Развертывание сервера журнала событий

Для создания нового сервера необходимо нажать на кнопку **[+ Развернуть сервер журнала событий]**, будет выполнен переход на карточку нового сервера.

На карточке выбрать из выпадающего списка значения полей **Имя компьютера** и **Имя сайта**. Оба поля являются обязательными для заполнения. Управление сервером осуществляется после его сохранения (см. *Управление сервером журнала событий*).

Важно: В выпадающем списке предлагаются только те компьютеры, которые не заняты под серверы в других подсистемах и в системе журнала событий.

Для сохранения сервера нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку серверов.

Важно: Развертывание сервера занимает некоторое время. Отслеживать процесс развертывания можно одним из следующих вариантов:

- через всплывающие сообщения, которые появляются по мере наступления очередного события;
- на вкладке **Журнал заданий** (**Автоматизация**→**Задания автоматизации**) по названию **audit_install**.

Система не имеет ограничений на количество серверов журнала событий и на количество серверов на одном сайте.

Для закрытия карточки и возврата к списку серверов нажать на кнопку закрытия.

1.8.1.3. Управление сервером журнала событий

Управление сервером журнала событий выполняется на его карточке. Для открытия карточки необходимо в списке серверов нажать на соответствующий сервер.

На карточке сервера доступно для редактирования поле **Имя сайта**.

Для сохранения изменений нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к списку серверов.

Для закрытия карточки и возврата к списку серверов нажать на кнопку закрытия.

1.8.1.4. Удаление сервера журнала событий

Удаление сервера журнала событий осуществляется из его карточки: открыть карточку, нажав в списке серверов на соответствующий сервер, затем на карточке нажать кнопку **[Удалить]**. После подтверждения удаления будет выполнен переход к списку серверов журнала событий.

1.8.2. Настройка сбора журналов событий

В подразделе выполняется настройка правил сбора информации о событиях.

1.8.2.1. Список правил

В подразделе на вкладке **Правила сбора событий** приводится список правил сбора информации о событиях с указанием имени правила и его состояния (включено или выключено). Журнал собранных событий отображается в подразделе *Журнал событий мониторинга* (раздел *Мониторинг*)

Важно: При обновлении Системы до версии 2.0.0 все добавленные правила, у которых не настроен параметр состояния и/или сервер сбора логов, отобразятся в таблице, но будут недоступны для работы в этой версии Системы. Для корректной работы правил, их нужно удалить, развернуть и настроить.

В списке доступен поиск по имени правила. Для этого в верхнем левом углу вкладки в поле поиска начните вводить значение.

В списке доступна фильтрация по значению **Состояние**, для этого необходимо нажать на значок фильтра рядом с названием столбца и отметить требуемые значения для фильтрации.

В левом нижнем углу указано количество правил, а в правом нижнем углу кнопки переключения страниц.

1.8.2.2. Добавление нового правила сбора информации о событиях

Для добавления нового правила необходимо нажать на кнопку **[+ Новое правило]**, будет выполнен переход на карточку нового правила.

В карточке на вкладке **Основное** заполнить обязательные поля **Имя правила**, **Тип логов**, **Сервер сбора логов**.

В поле **Тип логов** задается тип событий, информация о которых будет собираться. Доступны следующие значения:

- **Логи авторизации Fly** — сбор информации о входе пользователей в графический интерфейс клиентов домена;
- **Логи удаленного подключения** — сбор информации обо всех удаленных подключениях к клиентам домена по протоколу ssh;
- **Логи состояния подключения к сети** — сбор информации о состоянии подключения к сети всех клиентов домена.

Важно: Версия 2.0.0 Системы поддерживает использование уникального типа логов для одного сервера логов. Т.е. создание двух правил с типом логов, например, **Логи авторизации Fly** на одном сервере сбора логов запрещено.

Также можно заполнить поле **Описание**.

Для включения или выключения правила, соответственно, установить флаг **Включено** или **Выключено**.

Для сохранения правила нажать на кнопку сохранения в правом верхнем углу.

Важно: Создание правила занимает некоторое время. Отслеживать процесс создания можно одним из следующих вариантов:

- через всплывающие сообщения, которые появляются по мере наступления очередного события;
- на вкладке Журнал заданий (Автоматизация→Задания автоматизации) по названию add_rule.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку правил нажать на кнопку закрытия.

1.8.2.3. Просмотр информации о правиле

Просмотр информации о правиле доступен на его карточке. Для открытия карточки правила необходимо в списке правил нажать на соответствующее правило.

На вкладке **Основное** можно изменить описание правила. Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку правил нажать на кнопку закрытия.

1.8.2.4. Редактирование правила сбора информации о событии

Для редактирования доступно поле **Описание** на вкладке **Основное** карточки правила. Правило можно включать и выключать - изменять его состояние.

Важно: Начиная с версии 2.0.0 не предусмотрена возможность настройки правил сбора логов.

Важно: При внесении изменений в правило сбора информации о событии, его версия меняется автоматически.

Управление состоянием правила

Управление состоянием правила осуществляется из его карточки на вкладке **Основное**.

Для включения или выключения правила отметить, соответственно, пункт **Включено** или **Выключено**.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку правил нажать на кнопку закрытия.

1.8.2.5. Удаление правила

Для удаления правила или одновременно несколько правил необходимо в списке правил отметить требуемое правило и нажать кнопку **[Удалить]**.

Чтоб отметить все записи — отметить пункт **Имя правила**. Для снятия отметок со всех правил — нажать кнопку закрытия в правом верхнем углу.

Также удалить правило можно из его карточки: открыть карточку, нажав в списке правил на соответствующее правило, затем на карточке на вкладке **Основное** нажать кнопку **[- Удалить правило]**. После подтверждения удаления будет выполнен переход к списку правил.

1.9. Групповые политики

В разделе осуществляется настройка и управление групповыми политиками. Групповая политика – это набор правил, в соответствии с которыми отдельный компьютер домена ALD Pro выполняет настройку рабочей среды. Настройка рабочей среды производится с помощью запуска скриптов групповой политики. Групповые политики используются для массовой настройки однотипной рабочей среды на компьютерах, подключенных в домен. Группу компьютеров можно выбрать разными способами.

1.9.1. Групповые политики

В подразделе осуществляется управление групповыми политиками: создание, настройка и удаление групповых политик, назначение политик на подразделение и др.

1.9.1.1. Список групповых политик

В подразделе приведен список групповых политик с указанием имени, версии, даты изменения и имени пользователя, внесшего изменения.

В списке доступен поиск по имени политики, версии и автору изменений. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Для просмотра информации о политике нажать на соответствующую политику в списке. Будет открыта карточка политики с информацией о ней.

В левом нижнем углу указано количество групповых политик, а в правом нижнем углу кнопки переключения страниц.

1.9.1.2. Создание групповой политики

Для создания новой групповой политики нажать кнопку **[Новая групповая политика]**, будет открыта карточка создания новой групповой политики.

На карточке на вкладке **Основное** заполнить обязательно поле **Имя групповой политики**, а также при необходимости добавить ее описание в поле **Описание групповой политики**.

Остальные вкладки станут доступны для редактирования после сохранения групповой политики (см. раздел **Групповые политики → Групповые политики → Настройка групповой политики → Конфигурация политики**).

Для сохранения новой групповой политики необходимо нажать на кнопку сохранения в правом верхнем углу. После сохранения групповой политики на вкладке **Основное** отобразится информация о датах создания и изменения политики, версии политики и авторе изменений.

Для закрытия карточки и возврата к списку групповых политик нажать на кнопку закрытия.

1.9.1.3. Настройка групповой политики

Настройка групповой политики выполняется на ее карточке. Для открытия карточки необходимо в списке групповых политик нажать на соответствующую политику.

Важно: При внесении изменений в настройку групповой политики, ее версия меняется автоматически.

В карточке управление групповой политикой осуществляется на вкладках:

- **Основное**;
- **Конфигурация политики**;
- **Параметры компьютеров**;
- **Параметры пользователей**;
- **Подразделения**.

Для закрытия карточки и возврата к списку групповых политик необходимо нажать на кнопку закрытия.

Основное

На вкладке отображается информация о групповой политике: ее название, описание, дата создания, дата изменения, версия изменения и имя пользователя, внесшего последние изменения.

Для редактирования доступны имя групповой политики и ее описание.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Конфигурация политики

На вкладке приведен в табличном виде список параметров пользователей и параметров компьютеров, применяемых в данной групповой политике. Параметры могут быть как «коробочные» (предустановленные), так и созданные пользователем. Для каждого параметра указывается его название, тип (параметр пользователя или компьютера), папка хранения параметра (в каталоге параметров пользователей или в каталоге параметров компьютеров), и состояние параметра.

В списке доступен поиск по названию параметра и каталогу параметра. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

В списке доступна фильтрация по значениям столбцов **Тип** и **Состояние**, для этого необходимо нажать на значок фильтра рядом с названием соответствующего столбца и отметить требуемые значения для фильтрации.

При нажатии на параметр будет выполнен переход на вкладку **Параметры пользователя** или **Параметры компьютера** (в зависимости от типа параметра), к форме настройки данного параметра.

Для удаления из групповой политики параметра или одновременно нескольких параметров необходимо в списке отметить требуемые параметры и нажать кнопку **[Удалить]**.

Чтоб отметить все имеющиеся параметры — установить флаг выбора всех записей в заголовке таблицы.

В левом нижнем углу указано количество параметров, а в правом нижнем углу кнопки переключения страниц.

Параметры компьютеров/пользователей (далее «Параметры»)

На вкладке осуществляется настройка параметров и их включение в состав данной групповой политики.

В левой части страницы приведен каталог с параметрами в иерархическом виде.

Доступен поиск папки или параметра. Для этого в соответствующем поле поиска начать вводить название параметра или папки, результат поиска будет выводиться по мере ввода.

В папке **Дополнительные параметры** отображаются параметры, созданные пользователем на вкладке *Параметры компьютеров* и *Параметры пользователей*.

При выборе параметра справа будет отображена форма настройки параметра, состоящая из трех логических блоков. Каждый блок содержит атрибуты, значения которых задаются с помощью одного или нескольких полей.

Блоки 1 и 2 аналогичны для любого параметра. Атрибуты блока 3 уникальны для каждого параметра. Детальная информация по настройке атрибутов и общее назначение параметра описаны в справке (**?** в правом верхнем углу).

Блок 1 **Основное**

Блок предназначен для управления состоянием параметра, значение по умолчанию **Выключено**. Когда состояние параметра установлено как **Включено**, он применяется к объектам назначенного подразделения.

Изменения вступают в силу по расписанию (по умолчанию в течение 80 минут). В противном случае, когда состояние **Выключено**, применение параметра к объектам не происходит, тогда настройки параметра могут быть изменены локально средствами графического интерфейса операционной системы.

Также присутствует специальное поле, чтобы можно было оставить комментарий к настраиваемому параметру.

Блок 2 **Требования к ОС**

Блок предназначен для применения параметра только на компьютеры в домене, операционная система (ОС) которых соответствует требованиям, указанным в этом блоке.

Для заполнения поля **Параметр ОС** необходимо выбрать атрибут из выпадающего списка. Выпадающий список сформирован из данных словаря `grains`, где хранится информация о целевом хосте. Возможные варианты для выбора:

- `os` - операционная система;
- `os_family` - семейство операционных систем;
- `osarch` - разрядность операционной системы;
- `oscodename` - кодовое имя операционной системы;
- `osfinger` - информация о версии операционной системы и других ее особенностях;
- `osfullname` - полное название операционной системы. Обычно содержит название операционной системы, версию и сопутствующую информацию о версии;
- `osmajorrelease` - основной номер версии операционной системы;
- `osrelease` - полный номер версии операционной системы.

Поле **Оператор** содержит выпадающий список из операторов сравнения:

- = - полное соответствие;
- ~ - частичное соответствие.

Поле **Значение** содержит конкретное значение, по которому требуется фильтровать ОС. Перед настройкой рекомендуется проверить значения параметров ОС на конкретном компьютере в домене, указав в терминале команду `sudo aldpro-salt-call grains.items`.

Примеры фильтров:

- применение параметра на компьютерах с ОС Astra Linux - фильтр `OS~astra`;
- применение параметра на компьютерах с ОС РЕД ОС версии 7.X - фильтр `osfinger~RED OS-7`;
- применение параметра на компьютерах с ОС ALT Linux версии 10.4 - фильтр `oscodename~ALT Workstation 10.4`.

Фильтр по умолчанию `OS~astra` ограничивает параметр компьютерами с ОС Astra Linux.

Для добавления фильтра необходимо нажать рядом с заголовком блока, для удаления — значок корзины. Если задано несколько фильтров, то для отбора данных используется логическая операция **ИЛИ**.

Для сохранения настроек параметра необходимо в форме нажать кнопку **[Применить]**, при этом параметр будет добавлен в конфигурацию групповой политики.

Подразделения

На вкладке настраивается список подразделений, к пользователям и компьютерам которых будет применяться данная групповая политика. При этом групповая политика также будет применяться к пользователям и компьютерам дочерних подразделений.

Список подразделений с назначенными групповыми политиками

На вкладке приведен список подразделений, на которые назначена данная групповая политика, с указанием названия подразделения, приоритетом политики и принудительного наследования ее параметров.

В списке доступен поиск по названию подразделения. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Для доступа к функционалу нужно настроить привилегии. Список необходимых привилегий приведен в таблице ниже.

Привилегия	Описание	На что распространяется
Group Policies - Read	Привилегия позволяет: Видеть список групповых политик (Групповые политики/Групповые политики); Видеть карточки групповых политик (Групповые политики/Групповые политики/<Групповая политика>)	На весь домен

продолжение на следующей странице

Таблица 1.1 – продолжение с предыдущей страницы

Привилегия	Описание	На что распространяется
Group Policies User Parameters - Manage	Привилегия позволяет: Видеть список групповых политик в карточке подразделения (Пользователи и компьютеры/Организационная структура/<Подразделение>/вкладка Групповые политики); Видеть карточки групповых политик в карточке подразделения (Пользователи и компьютеры/Организационная структура/<Подразделение>/вкладка Групповые политики/<Групповая политика>)	На весь домен
Group Policy Membership - Manage	Привилегия позволяет: Добавлять и удалять политики для подразделений (Групповые политики/Групповые политики/<Групповая политика>/вкладка Подразделения); Добавлять, удалять и изменять приоритет политик для подразделений (Пользователи и компьютеры/Организационная структура/<Подразделение>/вкладка Групповые политики)	Выбранное подразделение

В левом нижнем углу указано количество подразделений, которым назначена данная групповая политика.

Назначение групповой политики на подразделение

Для назначения на подразделение групповой политики с заданными параметрами нажать кнопку **[Добавить подразделение]**. На карточке необходимо выбрать подразделение, на которое будет назначена данная групповая политика. При нажатии на кнопку **[Выбрать]** рядом с полем **Подразделение** открывается модальное окно с вложенной иерархической структурой подразделений и поиском.

После выбора подразделения появляется кнопка **[Изменить]**. При нажатии на кнопку открывается модальное окно с вложенной иерархической структурой подразделений и поиском. Эта же кнопка присутствует, когда необходимо изменить уже имеющееся подразделение. Поле **Расположение подразделения в организационной структуре** заполняется автоматически при выборе подразделения.

Также на карточке необходимо назначить приоритет применения групповой политики.

Если необходимо, чтобы дочерние подразделения наследовали параметры данной групповой политики, даже если где-то наследование отключено, необходимо установить флаг **Наследовать принудительно**.

На одно подразделение может быть назначено несколько групповых политик, но с разным приоритетом — приоритет должен быть уникальным числовым значением. Значение приоритета не может быть больше количества групповых политик, назначенных на это подразделение. Если на выбранное подразделение уже назначены другие групповые политики, то они и их приоритет будут отображены в блоке **Групповые политики, ранее назначенные на подразделения**.

Если каждая из групповых политик, назначенных одному подразделению, задает непересекающийся набор параметров, то к подразделению применяются все параметры назначенных политик.

Если несколько политик, назначенных одному подразделению, то применяется алгоритм разрешения конфликтов (см. *Наследование и суммирование параметров групповых политик*).

Для применения изменений нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку подразделений нажать на кнопку закрытия.

Изменение приоритета и порядка наследования назначенной групповой политики

Изменение приоритета и порядка наследования назначенной на подразделение групповой политики осуществляется на карточке подразделения. Для открытия карточки необходимо на вкладке **Подразделения** нажать на соответствующее подразделение.

Изменение приоритета определяет порядок применения групповых политик, т.е. какие настройки будут применены к объекту.

Для изменения приоритета применения групповой политики в поле **Приоритет групповой политики** задать новое значение.

Флаг **Наследовать принудительно** позволяет сделать наследование параметров соответствующего объекта обязательным для всех дочерних подразделений, даже если где-то наследование отключено. Связанные ГПО, отмеченные флагом **Принудительно**, применяются после обычных ГПО, поэтому переопределяют их значения.

Для включения принудительного наследования параметров ГПО, необходимо установить флаг **Наследовать принудительно**.

Для применения изменений нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку подразделений нажать на кнопку закрытия.

Удаление назначения групповой политики на подразделение

Удаление назначения групповой политики на подразделение выполняется путем удаления подразделения из списка.

Удалить подразделение или одновременно несколько подразделений из списка можно, отметив требуемые подразделения и нажав кнопку **[Удалить]**.

Чтобы отметить все имеющиеся подразделения — отметить пункт **Подразделение**.

Также удалить назначенние групповой политики можно на карточке подразделения. Для открытия карточки на вкладке **Подразделения** нажать на соответствующее подразделение, затем на карточке нажать кнопку **[Удалить подразделение]**. После подтверждения удаления будет выполнен переход к списку подразделений.

1.9.1.4. Удаление групповой политики

Удаления групповой политики осуществляется из ее карточки на вкладке **Основное**. Для открытия карточки необходимо в списке групповых политик нажать на политику. Затем на карточке нажать кнопку **[Удалить групповую политику]**. После подтверждения удаления будет выполнен переход к списку групповых политик.

1.9.2. Политики доступа к узлу

В подразделе, на соответствующих вкладках, выполняется настройка правил доступа пользователей к компьютерам с использованием определенных служб HBAC (Host-based access control) FreeIPA.

1.9.2.1. Правила HBAC

На вкладке Правила HBAC выполняется создание, настройка и удаление правил HBAC, а также определяется порядок их применения.

Список правил HBAC

На вкладке приведен список правил HBAC с указанием имени правила, его состояния и описания.

В списке доступен поиск по имени или описанию правила. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Для просмотра информации о правиле HBAC нажать на соответствующее правило в списке. Будет открыта карточка правила HBAC.

В левом нижнем углу указано количество правил HBAC, а в правом нижнем углу кнопки переключения страниц.

Создание нового правила HBAC

Для создания нового правила необходимо нажать на кнопку **[Новое правило]**, будет выполнен переход на карточку нового правила.

На карточке на вкладке **Основное** заполнить обязательное поле **Имя правила**. Остальные вкладки станут доступны для заполнения после сохранения правила (см. *Управление правилом HBAC*).

Важно: В имени правила можно использовать `a-z`, `A-Z`, `0-9`, `-_`

Для сохранения нового правила необходимо нажать на кнопку сохранения в правом верхнем углу. Будет выполнен переход к карточке управления правилом.

Для закрытия карточки и возврата к списку правил нажать на кнопку закрытия.

Управление правилом HBAC

Управление правилом HBAC выполняется на его карточке. Для открытия карточки необходимо на вкладке **Правила HBAC** нажать на соответствующее правило в списке.

На карточке управление правилом HBAC осуществляется на вкладках:

- **Основное**;
- **Пользователи**;
- **Компьютеры**;
- **Службы HBAC**.

Для закрытия карточки и возврата к списку правил нажать на кнопку закрытия.

Основное

На вкладке отображается информация о правиле HBAC: его название, описание, а также состояние (включено/выключено).

Описание правила доступно для редактирования.

Для включения или выключения правила HBAC отметить, соответственно, **Включено** или **Выключено**.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Пользователи

На вкладке настраивается каким категориям пользователей разрешено запускать службы HBAC из данного правила.

В списках **Все пользователи** и **Выбранные пользователи** отображается блок с данными о сотрудниках: ФИО, логин, подразделение и должность.

Список служб HBAC, которые будет разрешено запускать, настраивается на вкладке *Службы HBAC*.

Список компьютеров, на которых будет разрешено запускать службы, настраивается на вкладке *Компьютеры*.

Для разрешения всем пользователям запускать службы HBAC из данного правила необходимо в поле **Категория пользователей, к которой применяется правило** выбрать значение **Любой пользователь**.

Для разрешения отдельным пользователям и группам пользователей запускать службы HBAC из данного правила необходимо в поле **Категория пользователей, к которой применяется правило** выбрать значение **Указанные пользователи и группы** (при создании правила значение по умолчанию).

Для выбора пользователей, которым будет разрешено запускать службы HBAC из данного правила, необходимо в блоке **Пользователи** в списке **Все пользователи** отметить требуемые записи и перенести их в список **Выбранные пользователи** нажатием кнопки **[<-]**.

Для исключения пользователей необходимо в списке **Выбранные пользователи** отметить требуемые записи и перенести их в список **Все пользователи** нажатием кнопки **[→]**.

Выбор и исключение групп пользователей выполняется в блоке **Группы пользователей** аналогично выбору/исключению пользователей.

Для таблицы **Все пользователи** доступен поиск по ФИО и логину. Поиск работает по одному из ключей: имени, фамилии, отчеству или логину.

Для таблицы **Выбранные пользователи** поиск доступен только по одному ключу: фамилии.

Для поиска в соответствующем поле ввести значение от трех символов, результат поиска будет выводиться по мере ввода. В обоих полях отображаются только те результаты

поиска, у которых в столбце содержится значение, частично или полностью совпадающее со строкой поиска. Если значение некорректно, в результатах поиска появится надпись «Данные отсутствуют».

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Компьютеры

На вкладке настраивается на каких компьютерах разрешено запускать службы HBAC.

Список служб HBAC, которые будет разрешено запускать, настраивается на вкладке *Службы HBAC*.

Список пользователей, которым будет разрешено запускать службы HBAC, настраивается на вкладке *Пользователи*.

Для разрешения запускать службы HBAC из данного правила на всех компьютерах необходимо в поле **Категория пользователей, к которой применяется правило** выбрать значение **Любой компьютер**.

Для разрешения запускать службы HBAC из данного правила на отдельных компьютерах и группах компьютеров необходимо в поле **Категория компьютеров, к которой применяется правило** выбрать значение **Указанные компьютеры и группы** (при создании правила значение по умолчанию).

Для выбора компьютеров, на которых будет разрешено запускать службы HBAC из данного правила, необходимо в блоке **Компьютеры** в списке **Все компьютеры** отметить требуемые записи и перенести их в список **Выбранные компьютеры** нажатием кнопки **[<-]**.

Для исключения компьютеров необходимо в списке **Выбранные компьютеры** отметить требуемые записи и перенести их в список **Все компьютеры** нажатием кнопки **[→]**.

Выбор и исключение групп компьютеров выполняется в блоке **Группы компьютеров** аналогично выбору/исключению компьютеров.

Во всех списках доступен поиск по имени(названию). Для этого в соответствующем поле поиска ввести значение от трех символов, результат поиска будет выводиться по мере

ввода.

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Службы HBAC

На вкладке настраивается какие службы HBAC разрешает запускать данное правило.

Список пользователей, которым будет разрешено запускать службы HBAC, настраивается на вкладке *Пользователи*.

Список компьютеров, на которых будет разрешено запускать службы, настраивается на вкладке *Компьютеры*.

Для разрешения запускать все службы HBAC необходимо в поле **Категория служб, к которой применяется правило** выбрать значение **Любая служба**.

Для разрешения запускать отдельные службы HBAC и группы служб необходимо в поле **Категория служб, к которой применяется правило** выбрать значение **Указанные службы и группы** (при создании правила значение по умолчанию).

Для выбора служб HBAC, которые будет разрешено запускать, необходимо в блоке **Службы** в списке **Все службы** отметить требуемые записи и перенести их в список **Выбранные службы** нажатием кнопки **[<-]**.

Для исключения служб HBAC необходимо в списке **Выбранные службы** отметить требуемые записи и перенести их в список **Все службы** нажатием кнопки **[→]**.

Выбор и исключение групп служб выполняется в блоке **Группы служб** аналогично выбору/исключению служб HBAC.

Список служб HBAC настраивается на вкладке *Службы HBAC* (подраздел *Политики доступа к узлу*).

Список групп служб настраивается на вкладке *Группы служб HBAC* (подраздел *Политики доступа к узлу*).

Во всех списках доступен поиск по имени(названию). Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Удаление правила HBAC

Для удаления правила HBAC или одновременно несколько правил HBAC необходимо на вкладке **Правила HBAC** в списке отметить требуемые правила и нажать кнопку **[Удалить]**.

Чтоб отметить все имеющиеся правила — отметить пункт **Имя правила**.

Также удалить правило HBAC можно из его карточки: открыть карточку нажатием на правило в списке, затем на карточке нажать кнопку **[Удалить правило]**. После подтверждения удаления будет выполнен переход к списку правил.

1.9.2.2. Службы HBAC

На вкладке Службы HBAC осуществляется управление службами HBAC: создание, настройка и удаление служб HBAC.

Список служб HBAC

На вкладке приведен список служб с указанием имени службы и описания.

В списке доступен поиск по имени и описанию службы. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Для просмотра информации о службе нажать на соответствующую службу в списке. Будет открыта карточка службы с информацией о ней.

В левом нижнем углу указано количество служб.

Создание службы HBAC

Для создания новой службы необходимо нажать на кнопку **[Новая служба]**, будет выполнен переход на карточку новой службы.

На карточке заполнить обязательное поле **Имя службы**. Также можно добавить описание службы в соответствующем поле.

Важно: В имени службы можно использовать `a-z`, `A-Z`, `0-9`, `!-_`

Вкладка **Группы** станет доступна для заполнения после сохранения службы (см. *Управление службой HBAC*).

Для сохранения новой службы необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку служб нажать на кнопку закрытия.

Управление службой HBAC

Управление службой выполняется на ее карточке. Для открытия карточки необходимо на вкладке **Службы HBAC** нажать на соответствующую службу в списке.

На карточке управление службой осуществляется на вкладках:

- **Основное**;
- **Группы**.

На вкладке **Основное** отображается информация о службе: ее название и описание.

Для редактирования доступно описание службы.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

На вкладке **Группы** осуществляется добавление данной службы HBAC в состав групп служб.

Для выбора групп служб, в которые будет входить данная служба HBAC, необходимо в списке **Все группы** отметить требуемые записи и перенести их в список **Выбранные группы** нажатием кнопки **[<-]**.

Для исключения данной службы HBAC из групп служб необходимо в списке **Выбранные группы** отметить требуемые записи и перенести их в список **Все группы** нажатием кнопки **[→]**.

Список групп служб задается на вкладке *Группы служб HBAC* (подраздел *Политики доступа к узлу*).

Во всех списках доступен поиск по названию. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку служб нажать на кнопку закрытия.

Удаление службы HBAC

Для удаления службы или одновременно несколько служб необходимо на вкладке **Службы HBAC** в списке отметить требуемые службы и нажать кнопку **[Удалить]**.

Чтоб отметить все имеющиеся службы — отметить пункт **Имя службы**.

Также удалить службу HBAC можно из ее карточки: открыть карточку нажатием на службу в списке служб, затем на карточке нажать кнопку **[Удалить службу]**. После подтверждения удаления будет выполнен переход к списку служб.

1.9.2.3. Группы служб HBAC

На вкладке осуществляется управление группами служб HBAC: создание, настройка и удаление групп служб HBAC.

Список групп служб HBAC

На вкладке приведен список групп служб с указанием имени группы и описания.

В списке доступен поиск по имени и описанию группы. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Для просмотра информации о группе служб нажать на соответствующую группу в списке. Будет открыта карточка группы служб с информацией о ней.

В левом нижнем углу указано количество групп служб.

Создание группы служб HBAC

Для создания новой группы служб необходимо нажать на кнопку **[Новая группа]**, будет выполнен переход на карточку новой группы.

На карточке заполнить обязательное поле **Имя группы**. Также можно добавить описание группы в соответствующем поле.

Важно: В имени группы можно использовать `a-z`, `A-Z`, `0-9`, `-_`

Вкладка **Службы** станет доступна для заполнения после сохранения группы (см. *Управление группой служб HBAC*).

Для сохранения новой группы служб необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку групп нажать на кнопку закрытия.

Управление группой служб HBAC

Управление группой служб выполняется на ее карточке. Для открытия карточки необходимо на вкладке **Группы служб HBAC** нажать на соответствующую группу в списке.

На карточке управление группой служб осуществляется на вкладках:

- **Основное**;
- **Службы**.

На вкладке **Основное** отображается информация о группе служб: ее название и описание.

Для редактирования доступно описание группы.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

На вкладке **Службы** осуществляется добавление служб HBAC в состав данной группы служб.

Для добавления служб HBAC в состав данной группы необходимо в списке **Все службы** отметить требуемые записи и перенести их в список **Выбранные службы** нажатием

кнопки **[<-]**.

Для исключения служб HBAC из состава данной группы необходимо в списке **Выбранные службы** отметить требуемые записи и перенести их в список **Все службы** нажатием кнопки **[→]**.

Список служб HBAC задается на вкладке *Службы HBAC* (подраздел *Политики доступа к узлу*).

Во всех списках доступен поиск по названию. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку групп служб нажать на кнопку закрытия.

Удаление группы служб HBAC

Для удаления группы служб или одновременно несколько групп необходимо на вкладке **Группы служб HBAC** в списке отметить требуемые группы и нажать кнопку **[Удалить]**.

Чтоб отметить все имеющиеся группы — отметить пункт **Имя группы**.

Также удалить группу служб можно из ее карточки: открыть карточку нажатием на группу служб в списке групп, затем на карточке нажать кнопку **[Удалить группу]**. После подтверждения удаления будет выполнен переход к списку групп.

1.9.3. Политики повышения привилегий

С помощью политик повышения привилегий (возможностей при администрировании) доступна возможность предоставления возможности обычным пользователям выполнять конкретные команды на целевом компьютере с привилегиями root-пользователя (или конкретного пользователя).

Повышение возможностей при администрировании работает через sssd-службу, которая в момент выполнения команды sudo запрашивает правила из LDAP-каталога.

1.9.3.1. Правила Sudo

На вкладке выполняется создание, настройка и удаление правил выполнения команд sudo, а также определяется порядок их применения.

Список правил sudo

Вкладка содержит правила для выполнения команд sudo.

В списке доступен поиск по имени и описанию правила. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

В списке доступна фильтрация по значению **Состояние**, для этого необходимо нажать на значок фильтра рядом с названием столбца и отметить требуемые значения для фильтрации.

Создание правила sudo

Для создания правила sudo нажать кнопку **[Новое правило]**, будет выполнен переход на карточку нового правила.

На карточке на вкладке **Основное** заполнить обязательное поле **Имя правила**.

Важно: В имени правила можно использовать `a-z`, `A-Z`, `0-9`, `-_`

Остальные вкладки станут доступны после сохранения правила (см. *Редактирование правила sudo*).

Для сохранения правила sudo нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку правил sudo нажать на кнопку закрытия.

Редактирование правила sudo

Редактирование правила sudo осуществляется на его карточке. Для перехода на карточку необходимо нажать на правило sudo в списке.

На карточке информация о правиле sudo размещается на вкладках:

- **Основное**;
- **Параметры**;
- **Пользователи**;
- **Компьютеры**;
- **Команды Sudo**;
- **Запуск от имени**.

Для закрытия карточки правила sudo и возврата к списку нажать на кнопку закрытия.

Основное. Управление состоянием правила

На вкладке указана основная информация о правиле sudo: имя правила, описание и состояние.

Для редактирования доступно описание правила и порядок его выполнения.

Для включения или выключения правила, соответственно, установить флаг **Включено** или **Выключено**.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Параметры

На вкладке приведен список параметров правила sudo.

В списке доступен поиск, для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Для добавления нового параметра нажать кнопку **[Новый параметр]**, будет открыта карточка нового параметра. В карточке необходимо указать добавляемый параметр.

Для сохранения параметра нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку параметров нажать на кнопку закрытия.

Для удаления параметра правила или одновременно несколько параметров необходимо

отметить параметр в списке и нажать кнопку **[Удалить]**.

Пользователи

На вкладке настраивается каким категориям пользователей разрешено/запрещено выполнение команд sudo из данного правила.

В списках **Все пользователи** и **Выбранные пользователи** отображается блок с данными о сотрудниках: ФИО, логин, подразделение и должность.

Список разрешенных/запрещенных команд sudo настраивается на вкладке *Команды Sudo*.

Список компьютеров, на которых разрешено/запрещено выполнять команды sudo, настраивается на вкладке *Компьютеры*.

Для разрешения всем пользователям выполнять команды sudo из данного правила необходимо в поле **Категория пользователей, к которой применяется правило** выбрать значение **Любой пользователь**.

Для разрешения отдельным пользователям и группам пользователей выполнять команды sudo из данного правила необходимо в поле **Категория пользователей, к которой применяется правило** выбрать значение **Указанные пользователи и группы** (при создании правила значение по умолчанию).

Для выбора пользователей, которым будет разрешено выполнять команды sudo из данного правила, необходимо в блоке **Пользователи** в списке **Все пользователи** отметить требуемые записи и перенести их в список **Выбранные пользователи** нажатием кнопки **[<-]**.

Для исключения пользователей необходимо в списке **Выбранные пользователи** отметить требуемые записи и перенести их в список **Все пользователи** нажатием кнопки **[→]**.

Выбор и исключение групп пользователей выполняется в блоке **Группы пользователей** аналогично выбору/исключению пользователей.

Для таблицы **Все пользователи** доступен поиск по ФИО и логину. Поиск работает по одному из ключей: имени, фамилии, отчеству или логину.

Для таблицы **Выбранные пользователи** поиск доступен только по одному ключу: фамилии.

Для поиска в соответствующем поле ввести значение от трех символов, результат поиска

будет выводиться по мере ввода. В обоих полях отображаются только те результаты поиска, у которых в столбце содержится значение, частично или полностью совпадающее со строкой поиска. Если значение некорректно, в результатах поиска появится надпись «Данные отсутствуют».

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Компьютеры

На вкладке настраивается на каких компьютерах разрешено/запрещено выполнение команд sudo.

Список разрешенных/запрещенных команд sudo настраивается на вкладке *Команды Sudo* .

Список пользователей, которым разрешено/запрещено выполнять команды sudo, настраивается на вкладке *Пользователи*.

Для разрешения выполнять команды sudo из данного правила на всех компьютерах необходимо в поле **Категория компьютеров, к которой применяется правило** выбрать значение **Любой компьютер**.

Для разрешения выполнять команды sudo из данного правила на отдельных компьютерах и группах компьютеров необходимо в поле **Категория компьютеров, к которой применяется правило** выбрать значение **Указанные компьютеры и группы** (при создании правила значение по умолчанию).

Для выбора компьютеров, на которых будет разрешено выполнять команды sudo из данного правила, необходимо в блоке **Компьютеры** в списке **Все компьютеры** отметить требуемые записи и перенести их в список **Выбранные компьютеры** нажатием кнопки **[<-]**.

Для исключения компьютеров необходимо в списке **Выбранные компьютеры** отметить требуемые записи и перенести их в список **Все компьютеры** нажатием кнопки **[→]**.

Выбор и исключение групп компьютеров выполняется в блоке **Группы компьютеров** аналогично выбору/исключению компьютеров.

Во всех списках доступен поиск по имени(названию). Для этого в соответствующем поле

поиска ввести значение от трех символов, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Команды Sudo

На вкладке настраивается какие команды sudo разрешено/запрещено выполнять.

Список пользователей, которым разрешено/запрещено выполнять команды sudo, настраивается на вкладке *Пользователи*.

Список компьютеров, на которых разрешено/запрещено выполнять команды sudo, настраивается на вкладке *Компьютеры*.

Для разрешения выполнять все команды sudo необходимо в поле **Категория команд, к которой применяется правило** выбрать значение **Любая команда**.

Для разрешения выполнять отдельные команды sudo и группы команд необходимо в поле **Категория команд, к которой применяется правило** выбрать значение **Указанные команды и группы** (при создании правила значение по умолчанию).

Для выбора команд sudo, которые будет разрешено выполнять, необходимо в блоке **Разрешенные команды** в списке **Все команды** отметить требуемые записи и перенести их в список **Выбранные команды** нажатием кнопки **[<-]**.

Для исключения команд из списка разрешенных необходимо в списке **Выбранные команды** отметить требуемые записи и перенести их в список **Все команды** нажатием кнопки **[→]**.

Выбор и исключение разрешенных групп команд sudo выполняется аналогично выбору и исключению команд sudo.

Для выбора команд sudo, которые будет запрещено выполнять, необходимо в блоке **Запрещенные команды** в списке **Все команды** отметить требуемые записи и перенести их в список **Выбранные команды** нажатием кнопки **[<-]**.

Для исключения команд из списка запрещенных необходимо в списке **Выбранные команды** отметить требуемые записи и перенести их в список **Все команды** нажатием

кнопки **[→]**.

Выбор и исключение запрещенных групп команд sudo выполняется аналогично выбору и исключению команд sudo.

Команды, выполняемые с sudo, добавляются на вкладке *Команды Sudo* (подраздел *Политики повышения привилегий*).

Группы команд, выполняемых с sudo, настраиваются на вкладке *Группы команд Sudo* (подраздел *Политики повышения привилегий*).

Во всех списках доступен поиск по имени. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Запуск от имени

На вкладке дополнительно настраиваются права выполнения команд sudo из данного правила от имени другого пользователя.

В списках **Все пользователи** и **Выбранные пользователи** отображается блок с данными о сотрудниках: ФИО и подразделение.

Для разрешения выполнять команды sudo из данного правила от имени любого пользователя необходимо в поле **Категория запуска от имени пользователей, к которой применяется правило** выбрать значение **Любой пользователь**.

Для разрешения выполнять команды sudo из данного правила от имени определенных пользователей и групп пользователей необходимо в поле **Категория запуска от имени пользователей, к которой применяется правило** выбрать значение **Указанные пользователи и группы** (при создании правила значение по умолчанию).

Если на вкладке выбран пункт **Указанные пользователи и группы**, но пользователи и группы не выбраны, то команды sudo из данного правила возможно будет выполнять только от имени суперпользователя root.

Для выбора пользователей, от имени которых будет разрешено выполнять команды sudo из данного правила, необходимо в блоке **От имени пользователей** в списке **Все**

пользователи отметить требуемые записи и перенести их в список **Выбранные пользователи** нажатием кнопки **[<-]**.

Для исключения пользователей необходимо в списке **Выбранные пользователи** отметить требуемые записи и перенести их в список **Все пользователи** нажатием кнопки **[→]**.

Для добавления локального пользователя, от имени которого будет разрешено выполнять команды sudo из данного правила, необходимо в поле **Имя локального пользователя** ввести имя локальной учетной записи пользователя и нажать кнопку **[Добавить]**.

Для исключения локального пользователя необходимо нажать кнопку **[Удалить]** рядом с соответствующей учетной записью.

Выбор и исключение групп пользователей выполняется в блоке **От имени группы пользователей** аналогично выбору и исключению пользователей.

Для таблицы **Все пользователи** доступен поиск по ФИО и логину. Поиск работает по одному из ключей: имени, фамилии, отчеству или логину.

Для таблицы **Выбранные пользователи** поиск доступен только по одному ключу: фамилии.

Для поиска в соответствующем поле ввести значение от трех символов, результат поиска будет выводиться по мере ввода. В обоих полях отображаются только те результаты поиска, у которых в столбце содержится значение, частично или полностью совпадающее со строкой поиска. Если значение некорректно, в результатах поиска появится надпись «Данные отсутствуют».

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Удаление правила sudo

Для удаления правила sudo или одновременно нескольких правил sudo необходимо на вкладке **Правила Sudo** отметить правило в списке и нажать кнопку **[Удалить]**.

Чтоб отметить все имеющиеся правила — отметить пункт **Имя правила**.

Также удалить правило sudo можно из его карточки: открыть карточку нажатием на правило sudo в списке, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить**

правило]. После подтверждения удаления будет выполнен переход к списку правил sudo.

1.9.3.2. Команды Sudo

На вкладке осуществляется управление командами, выполняемыми с sudo.

Список команд sudo

На вкладке приведен список команд, выполняемых с sudo.

В списке доступен поиск по имени или описанию команды. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество записей в списке.

Добавление команды

Для добавления команды нажать кнопку **[Новая команда]**, будет выполнен переход на карточку новой команды.

На карточке на вкладке **Основное** заполнить обязательное поле **Команда Sudo**.

Важно: В имени команды можно использовать `a-z`, `A-Z`, `0-9`, `-_./~` и пробелы (кроме первого и последнего)

Вкладка **Группы** станет доступна после сохранения команды (см. *Редактирование команды*).

Для сохранения команды sudo нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку команд sudo нажать на кнопку закрытия.

Редактирование команды

Редактирование команды sudo осуществляется на ее карточке. Для перехода на карточку необходимо нажать левой кнопкой мыши на команду sudo в списке.

На карточке информация о команде sudo размещается на вкладках:

- **Основное**;
- **Группы**.

Для закрытия карточки команды sudo и возврата к списку нажать на кнопку закрытия.

Основное

На вкладке указана команда и ее описание. Описание команды можно изменить.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Группы

На вкладке задаются группы команд, в состав которых будет входить данная команда.

Для выбора групп команд, в которые будет включена данная команда sudo, необходимо в списке **Все группы** отметить требуемые записи и перенести их в список **Выбранные группы** нажатием кнопки **[<-]**.

Для исключения данной команды sudo из групп команд необходимо в списке **Выбранные группы** отметить требуемые записи и перенести их в список **Все группы** нажатием кнопки **[→]**.

Список групп команд sudo задается на вкладке *Группы команд Sudo* (подраздел *Политики повышения привилегий*).

Во всех списках доступен поиск по имени. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку команд нажать на кнопку закрытия.

Удаление команды sudo

Команду sudo или одновременно несколько команд sudo можно удалить. Для этого необходимо выделить команду sudo в списке и нажать кнопку **[Удалить]**.

Также удалить команду sudo можно из ее карточки: открыть карточку нажатием на команду в списке, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить команду]**. После подтверждения удаления будет выполнен переход к списку команд sudo.

Если команда входит в состав правила sudo, то появится соответствующее сообщение об ошибке и команда не будет удалена.

1.9.3.3. Группы команд Sudo

На вкладке осуществляется управление группами команд, выполняемых с sudo.

Список групп команд

На вкладке приведен список групп команд, выполняемых с sudo.

В списке доступен поиск по имени или описанию группы. Для этого в поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество записей в списке.

Добавление группы команд

Для добавления группы команд sudo нажать кнопку **[Новая группа]**, будет выполнен переход на карточку новой группы.

На карточке на вкладке **Основное** заполнить обязательное поле **Имя группы**.

Важно: В имени группы можно использовать `a-z`, `A-Z`, `0-9`, `-_`

Вкладка **Команды** станет доступна после сохранения группы команды (см. *Редактирование группы команд*).

Для сохранения группы команд sudo нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку групп команд sudo нажать на кнопку закрытия.

Редактирование группы команд

Редактирование группы команд sudo осуществляется на ее карточке. Для перехода на карточку необходимо нажать на группу команд sudo в списке.

На карточке информация о группе команд sudo размещается на вкладках:

- **Основное**;
- **Команды**.

Для закрытия карточки группы команд sudo и возврата к списку нажать на кнопку закрытия.

Основное

На вкладке указано имя группы команд и ее описание. Описание группы команд можно изменить.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

Команды

На вкладке задаются команды, которые будут входить в состав данной группы.

Для добавления команд sudo в состав данной группы необходимо в списке **Все команды** отметить требуемые записи и перенести их в список **Выбранные команды** нажатием кнопки **[<-]**.

Для исключения команд из состава данной группы необходимо в списке **Выбранные команды** отметить требуемые записи и перенести их в список **Все команды** нажатием кнопки **[→]**.

Список команд sudo задается на вкладке *Команды Sudo* (подраздел *Политики повышения привилегий*).

Во всех списках доступен поиск по имени. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку групп команд sudo нажать на кнопку закрытия.

Удаление группы команд

Группу команд sudo или одновременно несколько групп команд sudo можно удалить. Для этого необходимо выделить группу команд sudo в списке и нажать кнопку **[Удалить]**.

Также удалить группу команд sudo можно из ее карточки: открыть карточку нажатием на группу команд sudo в списке, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить группу]**. После подтверждения удаления будет выполнен переход к списку групп команд sudo.

1.9.4. Политики паролей

В подразделе осуществляется управление политиками паролей: создание, настройка и удаление политик, а также управление списком запрещённых слов (См. **Список запрещённых слов**).

1.10. Установка и обновление ПО

В разделе осуществляется управление группами и репозиториями программного обеспечения (ПО), а также журналом заданий.

1.10.1. Политики ПО

В подразделе выполняется настройка политик установки и обновления программного обеспечения (ПО).

1.10.1.1. Список политик ПО

В подразделе приведен список политик ПО с указанием имени политики, версии, даты изменения и автора изменения.

По дате изменения возможна фильтрация. Для настройки фильтрации следует нажать на шапку столбца **Дата изменения**, выбрать принцип До, После или В диапазоне и интересующие даты.

В списке доступен поиск, для этого в поле поиска следует начать вводить имя политики, результат поиска будет выводиться по мере ввода.

Справа от поисковой строки расположена кнопка **[+ Новая политика ПО]** для *Создание политики ПО*.

В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

1.10.1.2. Создание политики ПО

Для создания новой политики ПО необходимо нажать на кнопку **[+ Новая политика ПО]** в списке политик ПО. Будет выполнен переход на карточку новой политики.

На карточке на вкладке **Основное** задать имя политики ПО. Также можно указать описание политики.

Остальные вкладки станут доступны после сохранения политики (см. *Настройка политики ПО*).

Для сохранения новой политики ПО необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к списку политик ПО нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

1.10.1.3. Настройка политики ПО

Настройка политики ПО выполняется на ее карточке. Для открытия карточки необходимо в списке политик ПО нажать на соответствующую политику ПО.

Важно: При внесении изменений в настройку политики ПО, ее версия меняется автоматически.

На карточке политики ПО представлены следующие вкладки:

- **Основное**;
- **Конфигурация политики**;
- **Каталог ПО**;
- **Подразделения**.

Для закрытия карточки и возврата к списку политик ПО нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Основное

На вкладке **Основное** приведена основная информация о политике ПО: имя политики (например, *Установка Chromium*) и ее описание. В раскрывающимся списке указаны ее свойства: даты создания и изменения, версия политики и автор последнего изменения. Поле **Описание** доступно для редактирования.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Конфигурация политики

На вкладке **Конфигурация политики** приведен список ПО с указанием каталога, которое входит состав данной политики ПО. Доступно упорядочивание в алфавитном порядке в обоих столбцах.

В списке доступен поиск, для этого в поле поиска следует начать вводить значение, результат поиска будет выводиться по мере ввода.

При нажатии на ПО в списке будет выполнен переход на вкладку *Каталог ПО* к форме настройки данного ПО.

Для удаления ПО из состава данной политики необходимо в списке отметить требуемое наименование ПО и нажать кнопку **[Удалить]**.

Важно: При удалении ПО из состава политики стандартным поведением ПО на устройстве будет удаление, независимо от того, каким образом было установлено ПО - через политики ПО или вручную. У ОС нет возможности определять способ установки ПО и удалять через состав политики ПО только то ПО, что было установлено через политику.

Чтобы отметить все записи — отметить пункт **Наименование ПО**.

В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Каталог ПО

На вкладке **Каталог ПО** настраивается ПО, которое будет входить в состав данной политики ПО.

ПО сгруппировано по разделам. Формирование разделов ПО и добавление ПО в разделы осуществляется в подразделе *Каталог ПО* (раздел *Установка и обновление ПО*).

Для поиска раздела ПО или ПО следует начать вводить в поле поиска название, результат поиска будет выводиться по мере ввода.

Для раскрытия раздела ПО нажать на соответствующий раздел.

При выборе ПО будет отображена форма **Настройка параметра**, в которой указываются

значения параметров данного ПО. Параметры ПО задаются на карточке ПО в подразделе *Каталог ПО* (раздел *Установка и обновление ПО*). Например, для ПО Chromium указан параметр **Стартовая страница** со значением по умолчанию https://yandex.ru. Значения параметров, заданные по умолчанию, могут быть изменены для данной политики ПО.

Для добавления ПО в состав данной политики ПО необходимо нажать кнопку **[Применить]** в правом нижнем углу формы.

Если параметр составной, то для него доступна возможность продублировать все поля параметров. Для этого необходимо нажать кнопку **[+]** справа от названия формы **Настройка параметра**.

Для сохранения изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу.

Подразделения

На вкладке настраивается список подразделений, к которым будет применена данная политика ПО.

Список подразделений

На вкладке приведен список подразделений, к которым применяется данная политика ПО, с указанием приоритета политики ПО. Доступно упорядочивание в алфавитном порядке в обоих столбцах.

В списке доступен поиск по названию подразделения. Для этого в поле поиска следует ввести значение поиска от трех символов, результат поиска будет выводиться по мере ввода.

Справа от поисковой строки расположена кнопка **[+ Добавить подразделение]**.

В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Назначение политики ПО на подразделение

Для назначения на подразделение политики ПО с заданными параметрами нажать кнопку **[+ Добавить подразделение]**, будет выполнен переход на карточку выбора нового подразделения.

На карточке необходимо выбрать подразделение, на которое будет назначена данная политика ПО, а также приоритет применения политики. Поле **Расположение подразделения в организационной структуре** заполняется автоматически при выборе подразделения.

На одно подразделение может быть назначено несколько политик ПО, но с разным приоритетом — приоритет должен быть уникальным числовым значением.

Блоки **Установить на компьютеры** и **Установить на группы компютеров** разделены на два столбца каждый. Левый столбец в каждом блоке содержит назначенные компьютеры и группы компьютеров соответственно, а правый - все компьютеры. Для всех списков доступен поиск, перенос объектов между списками осуществляется нажатием на соответсвующие стрелки влево и вправо (**[<-]** и **[→]**), если они отмечаны маркерами. В нижней части каждого столбца указано количество его объектов.

Если на выбранное подразделение уже назначены другие политики ПО, то они и их приоритет будут отображены в блоке **Назначенные ПО на подразделение**.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к списку политик ПО нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Назначение политики ПО на компьютеры и группы компьютеров

Для назначения политики ПО с заданными параметрами на компьютер, либо на группу компьютеров нажать кнопку **[+ Добавить подразделение]**,после чего будет выполнен переход на карточку выбора нового подразделения.

На карточке в выпадающем списке **Название подразделения** необходимо выбрать корневой каталог подразделения домена, после чего ниже отобразится форма выбора компьютеров и групп компьютеров, на которые необходимо установить ПО. Поле

Расположение подразделения в организационной структуре заполняется автоматически при выборе подразделения.

Для выбора компьютеров, на которые необходимо установить ПО, в блоке **Установить на компьютеры** в списке **Все компьютеры** отметить требуемые записи и перенести их в список **Выбранные компьютеры** нажатием кнопки **[<-]**.

Для исключения компьютеров из списка выбранных необходимо в списке **Выбранные компьютеры** отметить требуемые записи и перенести их в список **Все компьютеры** нажатием кнопки **[→]**.

Выбор группы компьютеров выполняется в блоке **Установить на группу компьютеров** аналогично выбору отдельных компьютеров.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к списку политик ПО нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Важно: При установке ПО на компьютеры/группу компьютеров возможно возникновение ошибки, связанной с распространением source-листов на целевых рабочих станциях. Для устранения данной проблемы необходимо через выполнение задания автоматизации передать на рабочие станции необходимые конфигурации, а именно:

- На портале управления перейти на карточку **Задания автоматизации** (раздел *Управление доменом* — подраздел *Каталог заданий автоматизации*). На карточке, в таблице **Каталог дополнительных заданий** выбрать корневой каталог **Дополнительные настройки** и нажать появившуюся кнопку **[+ Новое задание]**;
- В открывшемся окне, на вкладке **Основное**, в поле **Название задания** ввести наименование задания, например *repo*, в поле **Уникальный идентификатор** ввести значение идентификатора, например *repo*, после чего нажать кнопку сохранения;
- После успешного создания задания вкладка **Конфигурация скрипта** станет активной, нужно перейти на эту вкладку и нажать кнопку **[Редактировать файл]**;
- В поле **Редактировать скрипт вручную** добавить следующие данные:

```
repo:
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
    cmd.run:
        - name: |
            echo -e "deb http://repo.aldpro.ru/repos/astra/1 1.7_x86-64 main
↪contrib non-free" | sudo tee /etc/apt/sources.list.d/repo_aldpro.list
            apt update
        - failhard: True
```

где `http://repo.aldpro.ru/repos/astra/1 1.7_x86-64 main contrib non-free` - путь до репозитория.

Затем в поле **Комментарий** указать любой комментарий и нажать кнопку сохранения;

- После успешного добавления задания перейти на вкладку **Каталог заданий автоматизации** (раздел *Автоматизация* — подраздел *Задания автоматизации*). На вкладке выбрать корневой каталог **Дополнительные настройки**. В открывшемся дереве найти созданное задание, например *repo* и нажать появившуюся кнопку **[Запустить задание]**;
- В открывшемся окне выбрать компьютер, группу компьютеров или подразделение, которому необходимо добавить задание и нажать кнопку сохранения;
- После успешного окончания работы задания на вкладке **Журнал заданий** (раздел *Автоматизация* — подраздел *Задания автоматизации* в таблице, в строке с этим заданием, в столбце статус будет значение **Успешно**;
- Выполнить операцию по установке ПО на компьютеры, либо группы компьютеров.

Изменение приоритета назначенной политики ПО

Изменение приоритета назначенной на подразделение политики ПО осуществляется на карточке подразделения. Для открытия карточки необходимо на вкладке **Подразделения** нажать на соответствующее подразделение.

Для изменения приоритета применения политики ПО в поле **Приоритет политики ПО** задать новое значение.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к списку политик ПО нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без

внесенных изменений, если таковые есть.

Отмена назначения политики ПО на подразделение

Отмена назначения на подразделение политики ПО выполняется путем удаления подразделения из списка.

Для удаления подразделения или одновременно нескольких подразделений из списка необходимо отметить требуемые подразделения, нажать возникшую на месте поисковой строки кнопку **[- Удалить]** и подтвердить удаление во всплывающем окне.

Чтобы отметить все записи — отметить пункт **Наименование подразделения**.

Также удалить подразделение можно из карточки подразделения: в списке подразделений нажать на соответствующее подразделение, затем на карточке нажать кнопку **[Удалить подразделение]**. После подтверждения удаления будет выполнен переход к списку подразделений.

1.10.1.4. Применение политики ПО

Установка ПО

Установка ПО согласно политики осуществляется по PULL-модели, т.е. после сохранения параметров политики ПО запускается один из следующих сценариев:

- если компьютер, к которому применяется политика, выключен (находится не в сети), то он получит список ПО, которое должно быть установлено/обновлено, сразу после включения (появления в сети);
- если компьютер, к которому применяется политика, в сети, он получает список ПО, которое должно быть установлено/обновлено, каждые 30 минут.

На компьютере ПО будет установлено автоматически после успешного применения данной политики ПО.

Для корректного применения назначенных политик ПО на доменном компьютере, информация о репозитории должна содержаться в Source list компьютера.

1.10.1.5. Дополнительные настройки установки ПО

Обновление ПО

Обновление версии ПО, участвующего в политиках, осуществляется на вкладке **Пакеты** подраздела *Каталог ПО* (раздел *Установка и обновление ПО*).

Обновление ПО осуществляется путем замены пакета ПО на более актуальную версию пакета ПО, доступную в репозитории ПО. При этом обновление соответствующей политики ПО не требуется.

1.10.1.6. Удаление политики ПО

Удаления политики ПО выполняется из ее карточки: открыть карточку, нажав в списке политик ПО на соответствующую политику, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить политику]**. После подтверждения удаления будет выполнен переход к списку политик ПО.

1.10.2. Каталог ПО

В подразделе выполняются функции управления программным обеспечением (ПО): добавление и удаление пакетов ПО, настройка шаблонов конфигурации и параметров ПО, создание структуры хранения пакетов ПО (добавление разделов хранения ПО).

1.10.2.1. Каталог программного обеспечения

На странице подраздела отображается **Каталог программного обеспечения**. В каталоге представлено ПО, добавленное в ALD Pro. ПО может быть сгруппировано по разделам. Для раскрытия раздела ПО необходимо нажать на соответствующий раздел в структуре каталога.

В каталоге доступен поиск ПО или раздела ПО, для этого следует начать вводить в поле поиска название, результат поиска будет выводиться по мере ввода.

Справа от поисковой строки расположены кнопки **[+ Раздел ПО]** и **[+ Программное обсепечение]**.

При выборе в каталоге раздела ПО будет отображена форма **Объекты**, в которой приводится список входящих в состав выбранного раздела объектов (ПО и других разделов). В списке доступен поиск по названию и типу объекта, для этого вверху формы в поле поиска ввести значение. Внизу формы отображено количество объектов, входящих в выбранный раздел.

При выборе в каталоге программного обеспечения будет отображена форма **Пакеты**, в которой приводится список входящих в выбранное ПО пакетов. В списке доступен поиск по названию и версии пакета, для этого вверху формы в поле поиска ввести значение. Внизу формы отображено количество пакетов, входящих в выбранное программное обеспечение.

Для закрытия карточки и возврата в Главное Меню **Портала Управления** следует нажать на кнопку **[X Закрыть]**.

1.10.2.2. Создание раздела ПО

Для создания раздела ПО необходимо нажать кнопку **[+ Раздел ПО]**. Будет открыта карточка создания нового раздела.

Раздел ПО можно создать внутри другого раздела. Внутри ПО невозможно создать раздел ПО.

На карточке раздела ПО на вкладке **Основное** необходимо заполнить обязательные поля **Наименование раздела** (например, *Браузеры*) и **Родительский раздел каталога ПО**. По умолчанию в качестве родительского раздела указан раздел, из которого была открыта карточка создания нового раздела. Также на карточке можно заполнить поле **Описание**.

Вкладка **Программное обеспечение** станет доступна для редактирования после сохранения раздела ПО (см. *Редактирование раздела ПО*).

Для сохранения раздела ПО необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к Каталогу ПО следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

1.10.2.3. Редактирование раздела ПО

Редактирование раздела ПО осуществляется на его карточке. Для перехода на карточку необходимо в каталоге выбрать требуемый раздел ПО и нажать кнопку **[Редактировать]**. Будет открыта карточка редактирования раздела ПО.

Карточка раздела ПО состоит из вкладок:

- **Основное**;
- **Программное обеспечение**.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки раздела ПО и возврата к каталогу программного обеспечения следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Основное

На вкладке приведена основная информация о разделе ПО: наименование, имя родительского раздела и описание. Для редактирования доступны все поля.

Программное обеспечение

На вкладке выполняется добавление и исключение ПО из данного раздела.

Для добавления ПО в данный раздел необходимо в списке **Все программное обеспечение** отметить ПО (например, *Chromium*) и перенести его в список **Выбранное программное обеспечение** нажатием кнопки **[<-]**. В списке **Все программное обеспечение** приведено ПО, которое не было добавлено ни в один раздел ПО.

Для исключения ПО из раздела необходимо в списке **Выбранное программное обеспечение** отметить требуемое ПО и перенести его в список **Все программное обеспечение** нажатием кнопки **[→]**.

Во всех списках доступен поиск по наименованию. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

1.10.2.4. Добавление ПО в каталог программного обеспечения

Новое ПО может быть добавлено в корень каталога ПО или в раздел ПО. Внутри ПО невозможно создать дочернее ПО.

Для добавления ПО необходимо нажать кнопку **[+ Программное обеспечение]**. Будет открыта карточка нового ПО.

На карточке на вкладке **Основное** необходимо заполнить обязательные поля **Наименование ПО** и **Родительский раздел каталога ПО**. По умолчанию в качестве родительского раздела будет указан раздел ПО, из которого была открыта карточка добавления нового ПО. Также можно заполнить поле **Описание**.

Остальные вкладки станут доступны после добавления ПО (см. *Редактирование ПО*).

Для добавления нового ПО необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к Каталогу ПО следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

1.10.2.5. Редактирование ПО

Редактирование ПО осуществляется на его карточке. Для перехода на карточку необходимо в каталоге ПО выбрать требуемое ПО и нажать кнопку **[Редактировать]**.

Карточка ПО состоит из вкладок:

- **Основное**;
- **Пакеты**;
- **Шаблоны конфигурации**;
- **Параметры**.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки ПО и возврата к каталогу программного обеспечения следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Основное

На вкладке приведена основная информация о ПО: наименование ПО, родительский раздел каталога ПО и описание. Для редактирования доступны родительский раздел ПО и описание ПО.

Пакеты

На вкладке осуществляется управление пакетами данного ПО.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Список пакетов

На вкладке приведен список пакетов, входящих в состав ПО, с указанием имени и версии пакета.

В списке доступен поиск по имени и версии. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списка указано количество записей в списке.

Добавление пакета в состав ПО

Для добавления пакета в состав ПО необходимо на вкладке **Пакеты** нажать кнопку **[+ Пакет]**. Будет открыта карточка добавления пакета ПО.

На карточке добавления пакета ввести наименование пакета (например, *chromium*) и сохранить его, нажав кнопку сохранения в правом верхнем углу. Для добавления доступны пакеты из состава репозиториев, настроенных в подразделе *Репозитории ПО* (раздел *Установка и обновление ПО*).

Удаление пакета из состава ПО

Пакет или одновременно несколько пакетов можно удалить из состава данного ПО. Для этого необходимо отметить пакет в списке и нажать кнопку **[Удалить]**.

Шаблоны конфигурации

На вкладке осуществляется настройка шаблонов конфигурации ПО.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Список шаблонов конфигурации

На вкладке приведен список шаблонов конфигурации для данного ПО.

В списке доступен поиск по названию и пути размещения. Для этого в поле поиска ввести значение.

Внизу списка указано количество записей в списке.

Добавление шаблона конфигурации

Для добавления шаблона конфигурации необходимо на вкладке **Шаблоны конфигурации** нажать кнопку **[+ Шаблон]**. Будет открыта карточка добавления шаблона.

На карточке на вкладке **Основное** указать наименование шаблона (например, *chromiumtemplate*) и путь размещения (например, */etc/chromium/policies/managed/chrome.json*).

Вкладка **Редактирование шаблона** будет доступна после сохранения нового шаблона (см. *Редактирование шаблона конфигурации*).

Редактирование шаблона конфигурации

Редактирование шаблона конфигурации осуществляется на его карточке. Для перехода на карточку необходимо в списке шаблонов выбрать требуемый шаблон.

Карточка шаблона состоит из вкладок:

- **Основное**;
- **Редактирование шаблона**.

Основное

На вкладке приведено наименование шаблона и путь его размещения. Для редактирования доступен путь размещения.

Редактирование шаблона

На вкладке указывается текст скрипта шаблона конфигурации с возможностью его редактирования.

Пример 1

```
{%- set StartPage = parameters.get('firefox_StartPage', none) -%}
{%- set Homepage = parameters.get('firefox_Homepage', none) -%}
{
   "policies":{
      "ImportEnterpriseRoots": true,
      "Certificates": {
         "Install": ["/etc/ipa/ca.crt"]
      },
{% if Authentication %}
    {%- set Authentication = Authentication.replace(" ","") -%}
    {%- set TempAuthentication = Authentication.split(",") -%}
    {%- set TempAuthenticationLen = TempAuthentication |length -%}
      "Authentication":{
         "SPNEGO": [
          {% for i in range(TempAuthenticationLen) %}
          "{{ TempAuthentication[i] }}"{% if TempAuthenticationLen - 1 != i %}
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
↪,{% endif %}
          {% endfor %}
         ],
         "Delegated": [
          {% for i in range(TempAuthenticationLen) %}
          "{{ TempAuthentication[i] }}"{% if TempAuthenticationLen - 1 != i %}
↪,{% endif %}
          {% endfor %}
          ]
      }{% endif %}{% if Authentication and (Homepage or StartPage) %},{%
↪endif %}
      {%- if Homepage or StartPage -%}
      "Homepage":{
          {%- if StartPage -%}"URL": "{{ StartPage }}",{% endif %}
         "Locked":true,
         "StartPage": {%- if Homepage == 'true' -%}"previous-session"{% else
↪%}"homepage"{% endif %}
      }{% endif %}
   }
}
```

Пример 2

```
{%- set HomepageLocation = parameters.get('chromium_HomepageLocation', none) -
↪%}
{%- set RestoreOnStartupURLs = parameters.get('chromium_HomepageLocation',
↪none) -%}
{%- set RestoreOnStartup = parameters.get('chromium_RestoreOnStartup', none) -
↪%}
{
   {%- if HomepageLocation -%}{{'\n'}}"HomepageLocation": "{{
↪HomepageLocation }}",{{'\n'}}{%- endif -%}
   "RestoreOnStartup": {%- if RestoreOnStartup == 'true' -%}1{%- if
↪HomepageLocation -%},{%- endif -%}{{'\n'}}{% else %}4{%- if
↪HomepageLocation -%},{%- endif -%}{{'\n'}}{%- endif -%}
   {%- if HomepageLocation -%}
   "RestoreOnStartupURLs":[
      "{{ RestoreOnStartupURLs }}"
   ]
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
   {%- endif -%}
}
```

Для редактирования скрипта необходимо внести изменения в текст скрипта и нажать на кнопку **[Сохранить]** в правом верхнем углу.

Для отмены внесенных, но еще не сохраненных изменений, нажать на кнопку **[Отменить]**.

Удаление шаблона конфигурации

Шаблон конфигурации или одновременно несколько шаблонов можно удалить. Для этого необходимо отметить шаблон конфигурации в списке и нажать кнопку **[Удалить]**.

Также удалить шаблон конфигурации можно из карточки: в списке шаблонов нажать на соответствующий шаблон для открытия карточки, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить шаблон]**. После подтверждения удаления будет выполнен переход к списку шаблонов.

Параметры

На вкладке осуществляется управление параметрами данного ПО.

Параметры ПО используются при создании шаблонов конфигурации (см. *Редактирование шаблона*). Значения параметров ПО могут быть заданы при настройке политики ПО на вкладке **Каталог ПО** в подразделе *Политики ПО* (раздел *Установка и обновление ПО*).

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Список параметров

На вкладке приведен список параметров с указанием имени параметра, значения параметра по умолчанию и его описания.

В списке доступен поиск, для этого в поле поиска ввести значение.

Внизу списка указано количество записей в списке, а в правом нижнем углу кнопки переключения страниц.

Добавление параметра

Для добавления параметра необходимо на вкладке **Параметры** нажать кнопку **[+ Параметр]**. Будет открыта карточка добавления параметра.

На карточке указать заполнить поля:

- **Имя параметра** — имя для использования в тексте шаблона конфигурации (например, *chromium_HomepageLocation*);

Важно: В имени параметра можно использовать `a-z`, `0-9`, `-_`

- **Отображаемое имя параметра** — имя для отображения в списке параметров и в формах настройки параметра (например, *Стартовая страница*);

Важно: В отображаемом имени параметра можно использовать `a-z`, `A-Z`, `а-я`, `А-Я`, ёЁ, `0-9`, `-_.` и пробел между словами

- **Значение параметра** — значение параметра, применяемое по умолчанию (например, https://yandex.ru).

Также можно указать описание параметра.

Редактирование параметра

Редактирование параметра осуществляется на его карточке. Для перехода на карточку необходимо в списке параметров нажать на требуемый параметр.

Для редактирования доступны поля **Отображаемое имя параметра**, **Значение параметра** и **Описание**.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в

правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Удаление параметра

Параметр или одновременно несколько параметров можно удалить. Для этого необходимо отметить параметр в списке и нажать кнопку **[Удалить]**.

Также удалить параметр можно из карточки: в списке параметров нажать на соответствующий параметр для открытия карточки, затем на карточке нажать кнопку **[Удалить параметр]**. После подтверждения удаления будет выполнен переход к списку параметров.

1.10.2.6. Удаление программного обеспечения или раздела

Для удаления программного обеспечения или раздела ПО необходимо в каталоге программного обеспечения выбрать требуемый объект и нажать кнопку **[Редактировать]**. Затем в открывшейся карточке нажать кнопку **[Удалить ПО]** или **[Удалить раздел]**, соответственно. После подтверждения удаления будет выполнен переход к каталогу программного обеспечения.

1.10.3. Репозитории ПО

В подразделе выполняются функции управления репозиториями ПО и серверами репозиториев.

1.10.3.1. Репозитории ПО

На вкладке осуществляется управление репозиториями ПО: создание, редактирование и удаление репозиториев.

Список репозиториев ПО

Вкладка содержит список репозиториев ПО с указанием имени репозитория, типа репозитория и его описания.

В списке доступен поиск по имени репозитория. Для этого в поле поиска ввести значение. Внизу списка указано количество записей в списке.

Справа от поисковой строки расположена кнопка **[+ Новый репозиторий]**.

Создание репозитория ПО

Для создания репозитория ПО следует нажать кнопку **[+ Новый репозиторий]**, будет выполнен переход на карточку нового репозитория.

На карточке на вкладке **Основное** заполнить обязательные поля **Имя репозитория** и **Относительный путь публикации репозитория**. В поле **Относительный путь публикации репозитория** указывается каталог на компьютере, куда будет сохранен репозиторий (например, */astra17/bin*).

Также можно указать описание репозитория. Поле **Тип репозитория** будет заполнено автоматически без возможности изменения.

Вкладка **Версии** станет доступна для редактирования после сохранения репозитория (см. edit_repository).

Для сохранения репозитория необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Редактирование репозитория ПО

Редактирование репозитория осуществляется на его карточке. Для перехода на карточку необходимо нажать на репозиторий в списке.

На карточке информация о репозитории размещается на вкладках:

- **Основное**;
- **Версии**.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Основное

На вкладке указана основная информация о репозитории: его имя, тип, описание, относительный и абсолютный путь публикации репозитория. Поля **Тип репозитория** и **Абсолютный путь до репозитория** недоступны для редактирования. Остальные поля возможно изменить.

Версия

Список версий репозитория

На вкладке в табличном виде приведен список версий репозитория с указанием номера версии, состояния версии, даты создания и типа источника.

В списке доступен поиск. Для этого в поле поиска ввести значение. Также в списке доступна фильтрация по значениям столбцов **Состояние**, **Дата создания** и **Тип источника**, для этого необходимо нажать на значок фильтра рядом с названием столбца и отметить требуемые значения для фильтрации.

В левом нижнем углу указано количество записей в списке, а в правом нижнем углу кнопки переключения страниц.

Пользователям с допуском к абсолютному пути публикации репозитория доступна для просмотра опубликованная версия репозитория.

Создание версии репозитория

Для создания новой версии репозитория нажать кнопку **[Новая версия]**, будет выполнен переход на карточку создания новой версии.

На карточке на вкладке **Основное** необходимо выбрать тип источника версии репозитория: **Пакеты** или **ISO-образ**.

Тип источника “ISO-образ”

При выборе типа источника **ISO-образ** необходимо загрузить версию репозитория в виде файла с расширением *.iso. Для этого нажать кнопку **[Выбрать ISO-образ]** и в окне навигации выбрать нужный файл.

При необходимости можно изменить выбранный файл, нажав кнопку **[Изменить ISO-образ]** и выбрав другой iso-файл.

Для загрузки образа нажать на кнопку сохранения в правом верхнем углу.

После загрузки ISO-образа версия репозитория опубликуется автоматически, а на вкладке **Основное** отобразятся автоматически заполненные поля:

- **Описание** (например, *Apt repository for project ALDPro*);
- **Источник** (например, *ALDPro*);
- **Метка** (например, *ALDPro*);
- **Номер версии** (например, *1*);
- **Ветка дистрибутива** (например, *stable*);
- **Кодовое имя дистрибутива** (например, *aldpro*);
- **Архитектура дистрибутива** (например, *amd64*);
- **Компоненты дистрибутива** (например, *salt*).

Также автоматически заполнятся остальные вкладки (см. current_content и change_history).

Для закрытия карточки версии репозитория и перехода к списку версий нажать на кнопку закрытия.

Тип источника “Пакеты”

При выборе типа источника **Пакеты** необходимо заполнить следующие обязательные поля:

- **Источник** (например, *ALDPro*);
- **Метка** (например, *ALDPro*);
- **Номер версии** (например, *1*);
- **Кодовое имя дистрибутива** (например, *aldpro*);
- **Архитектура дистрибутива** (например, *amd64*).

Также можно заполнить поля **Описание** и **Ветка дистрибутива**.

Поле **Компоненты дистрибутива** заполняется автоматически и недоступно для редактирования.

После сохранения версии станут доступны для редактирования остальные вкладки (см. edit_version).

Для сохранения версии репозитория нажать на кнопку сохранения в правом верхнем углу.

После формирования текущего содержимого репозитория (см. current_content) для настройки пользователей, которые смогут подключаться к версии репозитория, ее необходимо опубликовать (см. publish_version).

Для закрытия карточки и возврата к списку версий нажать на кнопку закрытия.

Редактирование версии репозитория

Для редактирования доступна только версия репозитория с состоянием **Редактирование**.

Редактирование версии репозитория осуществляется на ее карточке. Для перехода на карточку необходимо в списке версий нажать на версию репозитория.

На карточке информация о версии репозитории размещается на вкладках:

- **Основное**;
- **Текущее содержимое**;
- **История изменений**.

Для закрытия карточки версии репозитория и возврата к списку нажать на кнопку закрытия.

Основное

На вкладке указана основная информация о версии репозитории:

- **Тип источника**;
- **Описание**;
- **Источник**;
- **Метка**;
- **Номер версии**;
- **Ветка дистрибутива**;
- **Кодовое имя дистрибутива**;
- **Архитектура дистрибутива**;
- **Компоненты дистрибутива**.

Поля **Тип источника** и **Компоненты дистрибутива** недоступны для редактирования. Остальные поля возможно изменить.

Для применения внесенных изменений нажать на кнопку сохранения в правом верхнем углу.

История изменений

На вкладке отображаются изменения, внесенные в данную версию репозитория, с указанием наименования пакета и действия над ним (добавлен или удален).

В списке доступен поиск. Для этого в поле поиска ввести значение.

Внизу списка слева указано количество записей в списке, а справа располагаются кнопки переключения страниц.

Текущее содержимое

На вкладке отображаются пакеты, входящие в состав данной версии репозитория, с указанием наименования пакета, версии пакета и контрольных сумм md5.

В списке доступен поиск. Для этого в поле поиска ввести значение.

Внизу списка слева указано количество записей в списке, а справа располагаются кнопки переключения страниц.

Если версия репозитория имеет состояние **Редактирование**, то текущее содержимое может быть изменено:

- для добавления в версию репозитория пакета нажать кнопку **[Загрузить пакет]**. В открывшемся окне навигации выбрать файл на и нажать **[Открыть]**;
- для удаления из версии репозитория пакета или одновременно нескольких пакетов необходимо отметить пакет в списке и нажать кнопку **[Удалить]**.

Публикация версии репозитория

Для публикации версии репозитория с выбранными пакетами для открытого допуска необходимо открыть карточку версии и на вкладке **Текущее содержимое** нажать кнопку **[Опубликовать]**.

После публикации версия репозитория изменит состояние на **Опубликована** и станет недоступна для редактирования.

Удаление версии репозитория

Для удаления версии репозитория открыть ее карточку, нажав на версию в списке, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить версию]**. После подтверждения удаления будет выполнен переход к списку версий.

Удаление репозитория

Для удаления репозитория открыть его карточку, нажав на репозиторий в списке, затем на карточке нажать кнопку **[Удалить репозиторий]**. После подтверждения удаления будет выполнен переход к списку репозиториев.

1.10.3.2. Серверы репозиториев ПО

На вкладке осуществляется управление серверами репозиториев ПО: развертывание, редактирование и удаление серверов репозиториев ПО. Сервер репозиториев ПО это отдельная подсистема ALD Pro, устанавливается на выбранный компьютер домена и далее принимает команды портала управления.

Список серверов репозиториев ПО

Вкладка содержит в табличном виде список развернутых серверов репозиториев ПО с указанием имени сервера, его IP-адреса, функций сервера и имени сайта.

В списке доступен поиск. Для этого в поле поиска ввести значение. Также доступна фильтрация по функциям сервера, для этого нажать на значок фильтра рядом с названием столбца **Роль** и выбрать требуемое значение для фильтрации.

Справа от поисковой строки расположена кнопка **[+ Развернуть сервер репозиториев ПО]**.

Внизу списка указано количество записей в списке.

Развертывание сервера репозиториев ПО

Для развертывания сервера необходимо на вкладке нажать кнопку **[+ Развернуть сервер репозиториев ПО]**. Будет открыта вкладка нового сервера репозиториев ПО.

На карточке из выпадающего списка **Имя компьютера** выбрать компьютер из состава домена, который будет выполнять функцию сервера репозиториев. В поле **Имя сайта** выбрать сайт для сервера репозиториев.

Для сохранения сервера необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Управление сервером репозиториев ПО

Управление сервером осуществляется на его карточке. Для перехода на карточку необходимо нажать левой кнопкой мыши на сервер в списке.

На карточке отображена основная информация о сервере репозиториев ПО.

Доступны смена сервера и сайта, обновление ALD Pro и просмотр журнала событий.

Для применения внесенных изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Удаление сервера репозиториев ПО

Для удаления сервера открыть его карточку, нажав на сервер в списке, затем на карточке нажать кнопку **[Удалить]**. После подтверждения удаления будет выполнен переход к списку серверов.

1.10.4. Политики обновления ALD Pro

В подразделе выполняется настройка политик обновления ALD Pro на компьютеры и группы компьютеров.

1.10.4.1. Список политик обновления ALD Pro

В подразделе приведен список политик обновления ALD Pro с указанием имени политики, версии и статуса. Доступно упорядочивание в алфавитном порядке и фильтрация политик по статусу.

В списке доступен поиск, для этого в поле поиска следует начать вводить значение, результат поиска будет выводиться по мере ввода.

Справа от поисковой строки расположена кнопка **[+ Новая политика обновления]**.

Для закрытия списка и возврата в Главное Меню **Портала Управления** следует нажать на кнопку **[X Закрыть]**.

В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Версионность

Каждая политика обновления ALD Pro имеет версию, которая автоматически изменяется, если наступило одно из следующих событий:

1. Внесены любые изменения в политику обновления ALD Pro. В этом случае дата изменений - это дата, когда пользователь внес изменения. А автор - это ФИО пользователя, внесшего изменения.
2. Произошло обновление системы. В этом случае дата изменений - это дата обновления системы. А автор изменений - **Системное обновление**.

1.10.4.2. Создание политики обновления ALD Pro

Для создания новой политики обновления ALD Pro необходимо нажать на кнопку **[+ Новая политика обновления]**. Будет выполнен переход на карточку новой политики.

На карточке на вкладке **Основное** задать имя политики обновления ALD Pro. Также можно указать описание политики. Указать статус политики: включена или выключена.

Остальные вкладки станут доступны после сохранения политики (см. *Настройка политики обновления ALD Pro*).

Для сохранения новой политики обновления необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

1.10.4.3. Настройка политики обновления ALD Pro

Настройка политики обновления ALD Pro выполняется на ее карточке. Для открытия карточки необходимо в списке политик обновления нажать на соответствующую политику обновления.

На карточке политики обновления представлены следующие вкладки:

- **Основное**;
- **Source list**;
- **Компьютеры**.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Основное

На вкладке Основное приведена основная информация о политике обновления: имя политики, ее описание и статус.

Ниже отображаются свойства политики обновления: дата создания, дата изменения, версия и автор изменений.

Поле Описание доступно для редактирования. Также можно изменить статус политики обновления, включив или выключив ее.

Source list

На вкладке **Source list** осуществляется формирование source list.

На вкладке указывается список репозиториев пакетов для APT.

Добавить или изменить source list можно двумя способами:

- добавить текст из файла на компьютере;

- вручную ввести или изменить текст source list на вкладке.

Для добавления текста source list из файла необходимо нажать кнопку **[Загрузить из файла]**, в окне навигации выбрать на компьютере необходимый файл в формате .list или .txt и нажать [Открыть].

Содержимое файла отобразится в форме **Конфигурация Source list**, при этом предыдущее содержимое source list будет заменено. При необходимости добавленный текст можно отредактировать.

Для добавления или редактирования source list вручную необходимо нажать кнопку **[Редактировать]**, после чего форма **Конфигурация Source list** станет доступна для редактирования.

Для сохранения source list необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку **[Отменить]**.

Компьютеры

На вкладке **Установить на компьютеры** в списке **Выбранные компьютеры** приведен список компьютеров, на которые будет установлена данная политика. В списке **Все компьютеры** приведен список всех компьютеров домена.

Во всех списках доступен поиск по имени компьютера. Для этого в соответствующем поле поиска ввести значение от трех символов, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для назначения политики на компьютер необходимо в списке **Все компьютеры** отметить компьютеры и перенести их в список **Выбранные компьютеры** нажатием кнопки [<-].

Для отмены политики на компьютер необходимо в списке **Выбранные компьютеры** отметить требуемые компьютеры и перенести их в список **Все компьютеры** нажатием кнопки [→].

На вкладке **Установить на группы компьютеров** в списке **Выбранные группы** приведен список групп, на компьютеры которых будет установлена данная политика. В списке **Все группы** приведен список всех групп домена.

Во всех списках доступен поиск по имени группы. Для этого в соответствующем поле

поиска ввести значение от трех символов, результат поиска будет выводиться по мере ввода.

Внизу каждого списка указано количество записей в данном списке.

Для назначения политики на группу компьютеров необходимо в списке **Все группы** отметить группы и перенести их в список **Выбранные группы** нажатием кнопки [<-].

Для отмены политики на группу компьютеров необходимо в списке **Выбранные группы** отметить требуемые группы и перенести их в список **Все группы** нажатием кнопки [→].

1.10.4.4. Просмотр назначенных политик на компьютерах и группах компьютеров

Для просмотра политик, назначенных на компьютер, необходимо выбрать компьютер в разделе “Пользователи и компьютеры - Компьютеры”.

Для просмотра политик, назначенных на группу компьютеров, необходимо выбрать группу компьютеров в разделе “Пользователи и компьютеры - Группы компьютеров” и перейти в раздел “Политики обновления”.

1.10.4.5. Удаление политики обновления ALD Pro

Удаления политики обновления выполняется из ее карточки: открыть карточку, нажав в списке политик обновления на соответствующую политику, затем на карточке на вкладке Основное нажать кнопку **[Удалить]**. После подтверждения удаления будет выполнен переход к списку политик обновления ALD Pro.

Важно: Удаление политики обновления ALD Pro может занимать до часа после включения компьютера и применения политики.

1.11. Роли и службы сайта

В разделе осуществляется управление доменными службами.

1.11.1. Служба разрешения имен

В подраздел осуществляется управление прямыми и обратными зонами DNS, а также перенаправлением DNS-запросов.

1.11.1.1. Зоны DNS

Список зон DNS

На вкладке приведен в табличном виде список зон DNS с указанием имени зоны и ее состояния.

В списке доступен поиск по названию зоны. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Справа от поисковой строки расположена кнопка **[+ Новая зона]**.

Также возможна фильтрация зон по состоянию, для этого нажать на значок фильтра рядом с названием столбца **Состояние** и выбрать требуемое значение для фильтрации.

Для просмотра информации о зоне DNS нажать на соответствующую зону в списке. Будет открыта карточка зоны DNS.

В левом нижнем углу указано количество зон DNS, а в правом нижнем углу кнопки переключения страниц.

Включение и выключение зоны DNS

Управлять состоянием зоны DNS можно непосредственно на вкладке. Для этого необходимо в списке отметить зону DNS или одновременно несколько зон DNS и нажать кнопку **[Включить]** или **[Выключить]** для включения или выключения зоны соответственно.

Также управлять состоянием зоны можно из ее карточки. Для открытия карточки нажать на

зону в списке. В открывшейся карточке на вкладке **Параметры зоны** в пункте **Состояние зоны DNS** отметить **Включено** или **Выключено** для включения или выключения зоны, соответственно.

Создание зоны DNS

Для создания новой зоны DNS необходимо нажать на кнопку **[+ Новая зона]**, будет выполнен переход на карточку новой зоны.

На карточке заполнить обязательное поле **Имя зоны** и выбрать значение для пункта **Тип зоны**. При создании зоны DNS обратного типа, поле **Имя зоны** заполняется в формате:

Пример 1

`2001:db8::/64`

Пример 2

`192.0.2.0/24`

Дальнейшая настройка зоны осуществляется после ее сохранения (см. *Управление зоной DNS*).

Для сохранения новой зоны необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне. Будет выполнен переход к списку зон DNS.

Для закрытия карточки и возврата к списку зон DNS следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Создание обратной DNS-зоны

По умолчанию обратная зона создается с `/24` маской, игнорируя настройки сетевого адаптера.

Если подсеть отличается от размерности `/24` - необходимо вручную создать обратную зону нужной размерности, а созданную по умолчанию - выключить.

Для создания обратной зоны для подсети - в поле **Имя зоны** указывается подсеть в формате `10.201.192.0/22`, см. *Добавление обратной DNS-зоны*. Подробнее см. в

разделе **Роли и службы сайта → Служба разрешения имен → Перенаправление запросов → Карточка Перенаправления запросов**.

В созданной обратной зоне нужно будет вручную добавить PTR-запись для первого Контроллера Домена (автоматически она не создается).

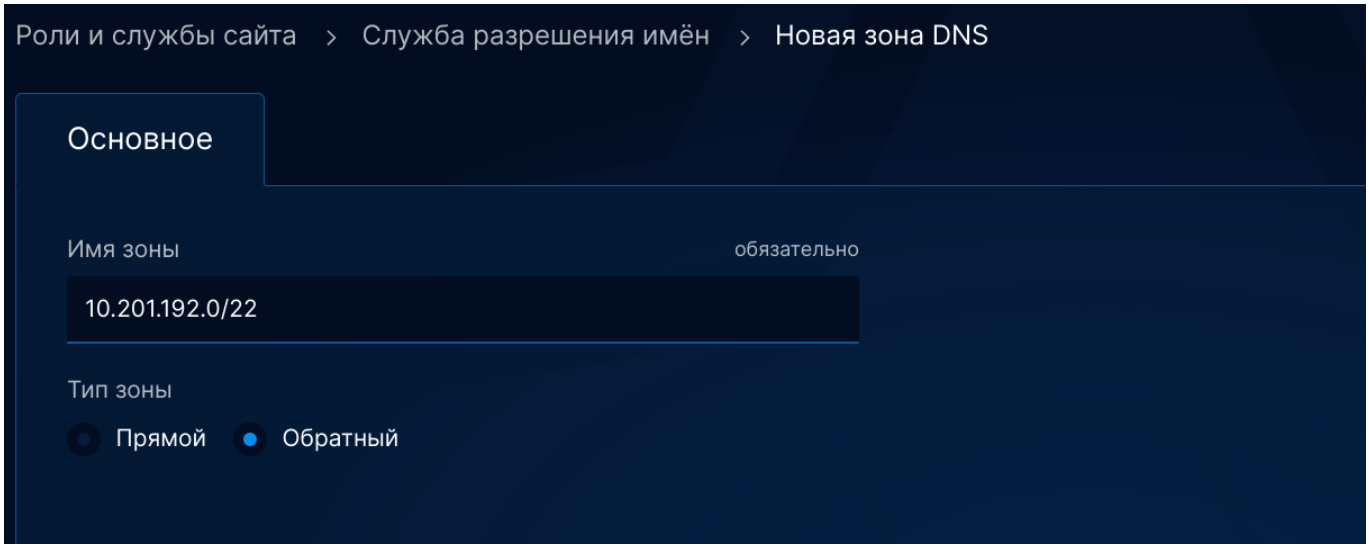


Рисунок 1.1 – Добавление обратной DNS-зоны

Если подсетей в инфраструктуре несколько и в какой-либо из них планируется создать реплику - необходимо вручную создать обратную зону для каждой подсети, в которой нужно будет разворачивать реплику Контроллера Домена (до разворачивания реплики в этих подсетях). Если этого не сделать - при разворачивании реплики из другой подсети произойдет сбой установки компонентов.

Рекомендуется разрешить динамическое обновление PTR-записей на вкладке **Глобальная конфигурация** (иначе при введении компьютера в домен прямая запись создастся, а обратная - нет).

Управление зоной DNS

Управление зоной DNS выполняется на ее карточке. Для открытия карточки необходимо в списке нажать на соответствующую зону DNS.

На карточке управление зоной DNS осуществляется на вкладках:

- **Записи ресурсов DNS**;
- **Параметры зоны**.

Записи ресурсов DNS

Список записей ресурсов DNS

На вкладке приведен список записей ресурсов, содержащихся в зоне, с указанием имени записи, типа записи и данных записи.

В списке доступен поиск по имени записи и по ее данным. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Справа от поисковой строки расположена кнопка **[+ Новая DNS-запись]**.

Также доступна фильтрация по типу записи, для этого нажать на значок фильтра рядом с названием столбца **Тип записи** и выбрать требуемое значение для фильтрации.

Для просмотра информации о записи ресурса нажать на соответствующую запись в списке. Будет открыта карточка записи ресурса DNS.

В левом нижнем углу указано количество записей ресурсов DNS, а в правом нижнем углу кнопки переключения страниц.

Добавление записи ресурса DNS

Для добавления новой записи ресурса DNS необходимо на вкладке **Записи ресурсов DNS** нажать на кнопку **[+ Новая DNS запись]**, будет выполнен переход на карточку новой записи.

На карточке заполнить обязательные поля:

- **Имя записи** — отображаемое имя записии, выбирается исходя из типа записи;
- **Тип записи** — определяет тип ресурсной записи. В зависимости от выбранного типа потребуется заполнить дополнительные поля.

В зависимости от выбранного типа записи отображаются следующие поля:

- тип **A** (в качестве имени записи должно быть указано имя компьютера):
  - поле **IP-адрес** — IP-адрес компьютера в формате IPv4;
- тип **AAAA** (в качестве имени записи должно быть указано имя компьютера):
  - поле **IP-адрес** — IP-адрес компьютера в формате IPv6;

- тип **A6**:
  - поле **Данные записи**;
- тип **AFSDB**:
  - поле **Подтип** (является необязательным);
  - поле **Имя узла** — имя компьютера, на котором размещена база данных AFS;
- тип **CERT**:
  - **Тип сертификата** — тип сертификата;
  - **Тег ключа** — числовое значение для выбора записи сертификата;
  - **Алгоритм** — алгоритм создания подписи;
  - **Сертификат** — сертификат или список отзыва сертификатов (CRL)**;
- тип **CNAME**:
  - **Имя узла**;
- тип **DNAME**:
  - **Цель**;
- тип **DS**:
  - **Тег ключа**;
  - **Алгоритм**;
  - **Тип дайджеста**;
  - **Дайджест**;
- тип **DLV**:
  - **Тег ключа**;
  - **Алгоритм**;
  - **Тип дайджеста**;
  - **Дайджест**;
- тип **KX**:
  - **Приоритет**;
  - **Обменник**;
- тип **LOC**:

  - **Градусы широты**;
  - **Минуты широты** (является необязательным);
  - **Секунды широты** (является необязательным);
  - переключатель **Направление широты**;
  - **Градусы долготы**;
  - **Минуты долготы** (является необязательным);
  - **Секунды долготы** (является необязательным);
  - переключатель **Направление долготы**;
  - **Высота над уровнем моря**;
  - **Размер** (является необязательным);
  - **Горизонтальная точность** (является необязательным);
  - **Вертикальная точность** (является необязательным);
- тип **MX**:
  - **Приоритет**;
  - **Обменник**;
- тип **NAPTR**:
  - **Порядок**;
  - **Приоритет**;
  - **Флаги**;
  - **Служба**;
  - **Регулярное выражение**;
  - **Замена**;
- тип **NS**:
  - **Имя узла**;
- тип **PTR**:
  - **Имя узла**;
- тип **SRV**:
  - **Приоритет (порядок)**;
  - **Вес**;

  - **Порт**;
  - **Цель**;
- тип **SSHFP**:
  - **Алгоритм**;
  - **Тип отпечатка**;
  - **Отпечаток**;
- тип **TLSA**:
  - **Использование сертификата**;
  - **Селектор**;
  - **Тип соответствия**;
  - **Данные сопоставления сертификата**;
- тип **TXT**:
  - **Текстовые данные**;
- тип **URI**:
  - **Приоритет (порядок)**;
  - **Вес**;
  - **Универсальный код ресурса (URI)**.

При выборе типа записи необходимо учитывать существующие ограничения (см. *Ограничения на типы записей*).

Для сохранения записи ресурса DNS необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне. Будет выполнен переход к списку записей ресурсов.

Для закрытия карточки и возврата к списку записей ресурсов следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Редактирование записи ресурса DNS

Для редактирования записи ресурса DNS нажать на соответствующую запись в списке. Будет открыта карточка записи ресурса DNS.

На карточке записи не доступны для редактирования имя и тип записи. Изменить возможно поля, соответствующие выбранному типу записи (см. add_entry).

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Удаление записи ресурса DNS

Для удаления записи ресурса DNS или одновременно нескольких записей ресурсов DNS необходимо в списке записей отметить запись и нажать кнопку **[Удалить]**.

Чтоб отметить все записи — отметить пункт **Имя записи**. Для снятия отметки нажать на кнопку закрытия в правом верхнем углу.

Также удалить запись ресурса DNS можно из ее карточки: открыть карточку нажатием на запись ресурса в списке, затем на карточке нажать кнопку **[Удалить данные записи]**. После подтверждения удаления будет выполнен переход к списку записей ресурсов DNS.

Параметры зоны

На вкладке приведены параметры выбранной зоны.

Значения параметров заполняются автоматически при создании зоны, при необходимости значения можно изменить:

- **Полномочный сервер имен**;
- **Адрес электронной почты администратора**;
- **Номер SOA**;
- **Обновление SOA**;
- **Повторный запрос SOA**;
- **Окончание действия SOA**;
- **Минимальный срок жизни SOA**;
- **Срок жизни по умолчанию**;

- **Срок жизни**;
- **Динамическое обновление**;
- **Разрешить запрос**;
- **Разрешить перенос**;
- **Глобальные перенаправители**;
- **Политика перенаправления**;
- **Состояние зоны DNS**.

Для параметров **Разрешить запрос**, **Разрешить перенос** и **Глобальные перенаправители** возможно добавить несколько значений. Для добавления значения необходимо в соответствующем параметре нажать кнопку **[Добавить]** и в появившемся поле ввести значение. Для удаления значения — нажать кнопку **[Удалить]** рядом с соответствующим полем.

Для применения изменений ннеобходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к списку зон DNS следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Удаление зоны DNS

Удаление зоны DNS осуществляется из ее карточки: открыть карточку, нажав в списке зон DNS на зону, затем на карточке на вкладке **Параметры зоны** нажать кнопку **[Удалить зону]**. После подтверждения удаления будет выполнен переход к списку зон DNS.

Ограничения на типы записей

Тип записи	Правила создания нового типа записи
A6	Запись NS нельзя использовать вместе с записью A6, если только они не расположены в корневой записи зоны

продолжение на следующей странице

Таблица 1.2 – продолжение с предыдущей страницы

Тип записи	Правила создания нового типа записи
AFSDB	Запись NS нельзя использовать вместе с записью AFSDB, если только они не расположены в корневой записи зоны
DNAME	Запись NS нельзя использовать вместе с записью DNAME, если только они не расположены в корневой записи зоны. Для одного имени можно использовать только одну запись DNAME
DS	Запись DS должна использоваться вместе с записью NS. Запись DS не должна находиться в начале зоны
DLV	Запись NS нельзя использовать вместе с записью DLV, если только они не расположены в корневой записи зоны
KX	Запись NS нельзя использовать вместе с записью KX, если только они не расположены в корневой записи зоны
LOC	Запись NS нельзя использовать вместе с записью LOC, если только они не расположены в корневой записи зоны
NAPTR	Запись NS нельзя использовать вместе с записью NAPTR, если только они не расположены в корневой записи зоны
PTR	Запись NS нельзя использовать вместе с записью PTR, если только они не расположены в корневой записи зоны
SRV	Запись NS нельзя использовать вместе с записью SRV, если только они не расположены в корневой записи зоны

продолжение на следующей странице

Таблица 1.2 – продолжение с предыдущей страницы

Тип записи	Правила создания нового типа записи
SSHFP	Запись NS нельзя использовать вместе с записью SSHFP, если только они не расположены в корневой записи зоны
TLSA	Запись NS нельзя использовать вместе с записью TLSA, если только они не расположены в корневой записи зоны
TXT	Запись NS нельзя использовать вместе с записью TXT, если только они не расположены в корневой записи зоны
URI	Запись NS нельзя использовать вместе с записью URI, если только они не расположены в корневой записи зоны

Проверка DNS-службы

Проверить настройки DNS-службы можно из терминала с помощью команды `dnsconfig-show` утилиты `ipa`:

```
kinit admin # получение билета Kerberos для учетной записи admin
ipa dnsconfig-show
```

Результат выполнения проверки настроек DNS:

```
Глобальные перенаправители: 77.88.8.8
Политика перенаправления: first
Разрешить PTR-синхронизацию: FALSE
DNS-серверы IPA: dc-1.ald.company.lan
```

В некоторых инструкциях для проверки DNS предлагают использовать утилиту `dig` с ключом `+trace`, но в этом случае утилита `dig` вместо того, чтобы обратиться к внешнему DNS-серверу, станет выполнять рекурсивные запросы, начиная с зоны верхнего уровня.

Поэтому, если вы все же хотите увидеть подтверждение, что при разрешении имен запросы

пошли к внешнему DNS-серверу, воспользуйтесь приложением `wireshark` или запустите в отдельном окне `tcpdump` для прослушивания пакетов, отправляемых на 53 порт:

```
sudo apt install tcpdump
sudo tcpdump port 53
```

В этом случае в окне терминала вы увидите следующее:

```
sudo tcpdump port 53
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
 ↪listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:23:35.806919 IP dc-1.ald.company.lan.41973 > dns.yandex.ru.domain: 23782+
 ↪[1au] NS? . (40)
11:23:35.807228 IP dc-1.ald.company.lan.58425 > dns.yandex.ru.domain: 28077+
 ↪% [1au] A? detectportal.firefox.com. (65)
11:23:35.808076 IP dc-1.ald.company.lan.55022 > dns.yandex.ru.domain: 48334+
 ↪% [1au] PT R? 8.8.88.77.in-addr.arpa. (63)
11:23:35.809802 IP dc-1.ald.company.lan.58539 > dns.yandex.ru.domain: 30468+
 ↪% [1au] AA AA? detectportal.firefox.com. (65)
11:23:35.828463 IP dns.yandex.ru.domain > dc-1.ald.company.lan.41973: 23782|
 ↪$ 0/0/1 (28)
...
```

На вкладке осуществляется управление зонами DNS.

1.11.1.2. Перенаправление запросов

На вкладке Перенаправление запросов осуществляется управление перенаправлением запросов.

Список перенаправлений

На вкладке приведен в табличном виде список зон, для которых настроено перенаправление, с указанием состояния зоны DNS, глобальных перенаправителей и политики перенаправления.

В списке доступен поиск по зоне и перенаправителю. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Справа от поисковой строки расположена кнопка **[+ Новая зона]**.

Также доступна фильтрация по состоянию зоны и политике перенаправления, для этого нажать на значок фильтра рядом с названием соответствующего столбца и выбрать значение для фильтрации.

Для просмотра информации о перенаправлении нажать на соответствующую зону в списке, будет открыта ее карточка.

В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Включение и выключение зоны

Управлять состоянием зоны можно непосредственно на вкладке **Перенаправление запросов**. Для этого необходимо в списке отметить зону или одновременно несколько зон и нажать кнопку **[Включить]** или **[Выключить]** для включения или выключения зоны, соответственно.

Также управление состоянием зоны возможно из карточки зоны: открыть карточку нажатием на зону в списке, затем на карточке установить переключатель **[Состояние зоны DNS]** в соответствующее положение. Для применения изменений нажать на кнопку сохранения в правом верхнем углу, после подтверждения сохранения будет выполнен переход к списку зон.

Добавление зоны

Для создания новой зоны необходимо нажать на кнопку **[+ Новая зона]**, будет выполнен переход на карточку новой зоны. На карточке необходимо:

- заполнить обязательное поля **Имя зоны**;
- добавить глобальный перенаправитель — нажать кнопку **[Добавить]** и ввести IP-адрес глобального перенаправителя (например, *127.1.1.3*). При необходимости можно добавить несколько глобальных перенаправителей, для удаления глобального перенаправителя нажать кнопку **[Удалить]** рядом с соответствующим IP-адресом;
- в пункте **Тип зоны** выбрать тип зоны DNS;
- в пункте **Политика перенаправления** выбрать политику перенаправления;
- пункт **Пропустить проверку пересечения** настраивается опционально. В случае

активации опции **Пропустить проверку пересечения** DNS-зона будет создана принудительно, даже если она будет пересекаться с существующей зоной.

При создании зоны перенаправления обратного типа, значение, введенное в поле **Имя зоны**, автоматически изменяется системой - в название добавляется суффикс:

IPv4:

При создании обратной зоны для адресов IPv4, название зоны будет автоматически изменяться на формат с суффиксом `.in-addr.arpa.`.

Пример

для диапазона адресов `192.0.2.0/24` зона будет отображаться как `0.0.0.192.in-addr.arpa.`

IPv6:

При создании обратной зоны для адресов IPv6, название зоны будет автоматически изменяться на формат с суффиксом `.ip6.arpa.`.

Пример

для диапазона адресов `2001:db8::/64` зона будет отображаться как `8.b.d.0.1.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa.`

Для сохранения новой зоны необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Редактирование зоны

Редактирование зоны осуществляется на ее карточке. Для открытия карточки необходимо в списке зон нажать на соответствующую зону.

На карточке доступны для редактирования поля **Глобальные перенаправители** и **Политика перенаправления** (см. *Добавление зоны*).

Также на карточке осуществляется управление состоянием зоны (см. *Включение и выключение зоны*).

Для применения изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Удаление зоны

Удаление зоны осуществляется из ее карточки: открыть карточку, нажав на зону в списке, затем на карточке нажать кнопку **[Удалить зону]**. После подтверждения удаления будет выполнен переход к списку зон.

1.11.1.3. Глобальная конфигурация DNS

На вкладке осуществляется управление глобальными перенаправителями запросов.

После настройки в ALD Pro первого контроллера домена он является единственным DNS-севером, в связи с этим необходимо добавить глобальный перенаправитель запросов на внешний DNS-сервер (публичный или сторонний внутренний).

Также на вкладке отображается информация о том, какие DNS-серверы IPA равернуты в ALD Pro.

Для добавления глобального перенаправителя необходимо указать его IP-адрес в поле **Глобальные перенаправители**. При необходимости можно добавить несколько глобальных перенаправителей: для добавления каждого последующего перенаправителя нажать кнопку **[Добавить]** и в отобразившемся поле ввести IP-адрес.

Для удаления глобального перенаправителя нажать кнопку **[Удалить]** рядом с соответствующим IP-адресом.

Для настройки политики перенаправления требуется выбрать необходимое значение для пункта **Политика перенаправления**.

Также можно отметить пункт **Разрешить PTR-синхронизацию**.

Для применения изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу.

1.11.2. Служба динамической настройки узла

В подразделе выполняется управление серверами службы динамической настройки узла (DHCP). DHCP-сервера развертываются с помощью команд с портала управления на выбранных компьютерах в домене ALD Pro.

1.11.2.1. Список серверов

В подразделе на вкладке **Перечень серверов** приводится список DHCP-серверов с указанием имени сервера, имени сайта и IP-адреса.

В списке доступен поиск по имени сервера, имени сайта или IP-адресу сервера. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Справа от поисковой строки расположена кнопка **[+ Новый сервер]**.

В левом нижнем углу указано количество серверов, а в правом нижнем углу кнопки переключения страниц.

1.11.2.2. Добавление DHCP-сервера

Для добавления нового DHCP-сервера необходимо нажать на кнопку **[+ Новый сервер]**, будет выполнен переход на карточку нового сервера.

На карточке на вкладке **Основное** заполнить обязательные поля:

- **Имя компьютера** — имя компьютера, добавленного в ALD Pro, который будет выполнять функции DHCP-сервера;
- **Имя сайта** — выбрать из списка сайт, добавленный на вкладке *Сайты и службы* подраздела *Сайты и службы* (раздел *Управление доменом*).

Вкладки **Конфигурация скрипта** и **Настройка сетевых интерфейсов** будут доступны после сохранения сервера (см. *Настройка конфигурации DHCP-сервера*).

Для сохранения сервера необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения

закрытия без внесенных изменений, если таковые есть.

1.11.2.3. Настройка конфигурации DHCP-сервера

Настройка конфигурации DHCP-сервера выполняется на его карточке. Для открытия карточки необходимо в списке серверов нажать на соответствующий сервер.

На карточке настройка сервера осуществляется на вкладках:

- **Основное**;
- **Конфигурация скрипта**;
- **Настройка сетевых интерфейсов**.

Для сохранения изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Основное

На вкладке **Основное** приведена основная информация о сервере. Для редактирования доступно поле **Имя сайта**.

Конфигурация скрипта

На вкладке **Конфигурация скрипта** осуществляется настройка файла конфигурации DHCP-сервера.

Пример 1: Конфигурация сервера DHCP с DDNS

```
ddns-updates on;
update-conflict-detection false;
allow booting;
do-forward-updates on;
update-optimization on;
allow declines;
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
ddns-update-style interim;
include "/etc/dhcp/rndc.key";
ddns-domainname "";
update-static-leases off;

option domain-name "aldpro.ru";
option domain-search "aldpro.ru";

option domain-name-servers 192.168.10.10;
option dhcp-server-identifier 192.168.10.15;

#Следующая строка нужна только если используется Samba с WINS

#option netbios-name-servers 10.0.2.102;

default-lease-time 129600;
max-lease-time 1296000;
authoritative;

#server-name "dc3.aldpro.ru";

#server-identifier 192.168.10.13;

#Эта подсеть должна соответствовать подсети вашей локальной сети, обращенной
↪к устройству Ethernet.
Subnet 192.168.10.0 netmask 255.255.255.0 {
    option broadcast-address 192.168.10.255;
    option subnet-mask 255.255.255.0;
    option routers 192.168.10.1;
    pool {
      range 192.168.10.220 192.168.10.230;
      allow known-clients;
      allow unknown-clients;
      max-lease-time 86400;
      default-lease-time 43200;
    }
    zone aldpro.ru. {
        primary 192.168.10.10;
        key "rndc-key";
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
    }
}
```

Пример 2: Конфигурация сервера DHCP для установки ОС по сети

```
#Все параметры расписаны тут https://github.com/42wim/isc-dhcp/blob/master/
 ↪server/dhcpd.conf.example
#Все опции DHCP тут https://www.iana.org/assignments/bootp-dhcp-parameters/
 ↪bootp-dhcp-parameters.xhtml

#Сетевой интерфейс
INTERFACES="eth1";
allow booting;
allow bootp;
option classless-routes-lin code 121 = array of unsigned integer 8;
#Подсеть и маска подсети
#Адрес сервера установки ОС
next-server 192.168.17.5;
#Путь до загрузчика
if substring (option vendor-class-identifier, 15, 5) = "00000" {
        filename "lpxelinux.0";
} elsif substring (option vendor-class-identifier, 15, 5) = "00007" {
        filename "bootx64.efi";
} else {
        filename "pxelinux.0";
}
subnet 192.168.17.0 netmask 255.255.255.0 {
#Пул адресов, из которого будут выдаваться адреса, где 192.168.17.10 -
 ↪первый адрес, 192.168.17.100 - последний адрес
range 192.168.17.10 192.168.17.100;
#DNS сервер. В результате 10.10.0.1 запишется в /etc/resolv.conf на клиенте
option domain-name-servers 10.10.0.1;
#DNS сервер. В результате domain ald.pro запишется в /etc/resolv.conf на
 ↪клиенте
option domain-name "ald.pro";
#Шлюз по-умолчанию
option routers 192.168.17.1;
#Статический маршрут (Опционально)
option classless-routes-lin  24, 192,168,17, 0, 192,168,17,1;
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
#Широковещательный адрес
option broadcast-address 192.168.17.255;
#Время аренды по-умолчанию
default-lease-time 6000;
#Максимальное время аренды
max-lease-time 72000;

}

#Статические адреса

#Задаем адрес tftp сервера + настраиваем его статику
host os {
  hardware ethernet 1E:0F:E6:05:7C:01;
  fixed-address 192.168.17.5;
}
```

На вкладке указывается актуальный текст файла конфигурации.

Добавить или изменить файл конфигурации можно двумя способами:

- добавить текст из файла на компьютере;
- вручную ввести или изменить текст файла конфигурации на вкладке.

Для добавления текста конфигурации из файла необходимо нажать кнопку **[Загрузить из файла]**, в окне навигации выбрать на компьютере необходимый файл в формате *.conf или* .txt и нажать **[Открыть]**.

Содержимое файла отобразится в форме **Редактировать скрипт вручную**, при этом предыдущее содержимое файла конфигурации будет заменено. При необходимости добавленный текст можно отредактировать.

Для сохранения файла конфигурации необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку **[Отменить]**.

Для добавления или редактирования файла конфигурации вручную необходимо нажать кнопку **[Редактировать файл]**, после чего форма **Редактировать скрипт вручную** станет доступна для редактирования.

Для сохранения файла конфигурации необходимо ввести комментарий и нажать кнопку

сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку **[Отменить]**.

Для просмотра истории изменений файла конфигурации необходимо нажать на кнопку **[История изменений]**. Откроется карточка с отображением списка изменений с указанием даты изменения, автора изменения и комментария. В списке доступен поиск, для этого в верхнем левом углу вкладки в поле поиска ввести значение. В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

Настройка сетевых интерфейсов

На вкладке **Настройка сетевых интерфейсов** осуществляется настройка перечня протоколов и сетевых интерфейсов, с которыми будет работать сервис DHCP.

При необходимости указать несколько сетевых интерфейсов, их можно перечислить через пробел.

Пример настроек (для протокола IPv4 используется интерфейс eth0, работа по протоколу IPv6 запрещена):

Пример

```
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="eth1" # Наименование сетевого интерфейса v4, с которого будут
 ↪раздаваться IP адреса
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
INTERFACESv6=""  # Наименование сетевого интерфейса v6, с которого будут
↪раздаваться IP адреса
```

На вкладке указывается актуальный текст файла конфигурации.

Добавить или изменить файл конфигурации можно двумя способами:

- добавить текст из файла на компьютере;
- вручную ввести или изменить текст файла конфигурации на вкладке.

Для добавления текста конфигурации из файла необходимо нажать кнопку **[Загрузить из файла]**, в окне навигации выбрать на компьютере необходимый файл в формате *.txt и нажать **[Открыть]**.

Содержимое файла отобразится в форме **Редактировать скрипт вручную**, при этом предыдущее содержимое файла конфигурации будет заменено. При необходимости добавленный текст можно отредактировать.

Для сохранения файла конфигурации необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку **[Отменить]**.

Для добавления или редактирования файла конфигурации вручную необходимо нажать кнопку **[Редактировать файл]**, после чего форма **Редактировать скрипт вручную** станет доступна для редактирования.

Для сохранения файла конфигурации необходимо ввести комментарий и нажать кнопку сохранения. Для отмены внесения изменений в файл конфигурации нажать кнопку **[Отменить]**.

Для просмотра истории изменений файла конфигурации необходимо нажать на кнопку **[История изменений]**. Откроется карточка с отображением списка изменений с указанием даты изменения, автора изменения и комментария. В списке доступен поиск, для этого в верхнем левом углу вкладки в поле поиска ввести значение. В левом нижнем углу указано количество записей, а в правом нижнем углу кнопки переключения страниц.

1.11.2.4. Удаление DHCP-сервера

Удаление сервера осуществляется из его карточки: открыть карточку, нажав в списке серверов на соответствующий сервер, затем на вкладке **Основное** нажать кнопку **[Удалить]**. После подтверждения удаления будет выполнен переход к списку серверов.

1.11.3. Служба синхронизации времени

В подразделе осуществляется добавление и удаление серверов синхронизации времени (NTP-серверов)

1.11.3.1. Внешний пул NTP-серверов

На вкладке настраиваются внешние сервера синхронизации времени. Внешний NTP-сервер не относятся к компьютерам данного домена и доступны из внешней сети (в т.ч. интернет).

Список NTP-серверов

На вкладке приведен список внешних NTP-серверов с указанием доменного имени и типа.

В списке доступен поиск, для этого в поле поиска следует начать вводить значение, результат поиска будет выводиться по мере ввода.

Справа от поисковой строки расположена кнопка **[+ Новый NTP-сервер]**.

В левом нижнем углу указано количество NTP-серверов, а в правом нижнем углу кнопки переключения страниц.

Добавление NTP-сервера

Для добавления нового NTP-сервера необходимо нажать на кнопку **[+ Новый NTP-сервер]**, будет выполнен переход на карточку добавления NTP-сервера.

На карточке заполнить обязательные поля:

- **NTP-сервер** — доменное имя внешнего NTP-сервера;

- **Тип** — отметить тип добавляемого ресурса (сервер или пул серверов).

Для сохранения нового NTP-сервера необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне. Будет выполнен переход к списку NTP-серверов.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Удаление NTP-сервера

Для удаления NTP-сервера или одновременно нескольких NTP-серверов необходимо в списке NTP-серверов отметить запись и нажать кнопку **[Удалить]**.

Чтоб отметить все записи — отметить пункт **Доменное имя**. Чтобы снять выделение — нажать кнопку закрытия в правом верхнем углу.

1.11.3.2. Корневые NTP-серверы домена

На вкладке настраиваются внутренние сервера синхронизации времени. Внутренний NTP-сервер это развернутый на компьютерах данного домена ALD Pro.

Список корневых NTP-серверов

На вкладке приведен список корневых NTP-серверов домена с указанием имени сервера, IP-адреса и имени сайта.

В списке доступен поиск по имени сервера, IP-адресу сервера и имени сайта. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Справа от поисковой строки расположена кнопка **[+ Новый NTP-сервер]**.

В левом нижнем углу указано количество NTP-серверов, а в правом нижнем углу кнопки переключения страниц.

Добавление корневого NTP-сервера

Для добавления нового корневого NTP-сервера необходимо нажать на кнопку **[+ Новый NTP-сервер]**, будет выполнен переход на карточку добавления NTP-сервера.

На карточке необходимо в поле **Имя компьютера** выбрать контроллер домена, на котором будет развернут NTP-сервер.

Для добавления нового NTP-сервера необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне. Будет выполнен переход к списку корневых NTP-серверов.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Удаление корневого NTP-сервера

Для удаления корневого NTP-сервера или одновременно нескольких корневых NTP-серверов необходимо в списке корневых NTP-серверов домена отметить требуемый NTP-сервер и нажать кнопку **[Удалить]**.

Чтоб отметить все записи — отметить пункт **Имя компьютера**. Для снятия выделения со всех серверов — нажать кнопку закрытия в правом верхнем углу.

Выбор источника точного времени в домене для каждого компьютера осуществляется на основании иерархической системы:

```
# КД - контроллер домена

Внешний источник (или другой эталон)

    Корневой КД сайта

        Обычный КД сайта

            Корневой КД домена (не из сайта)

                Обычный КД домена (не из сайта)
```

Внешний источник задается и настраивается на вкладке **Внешний пул NTP-серверов**. Корневые **NTP**-серверы домена задаются на вкладке **Корневые NTP-серверы домена**.

Корректная работа синхронизации времени осуществляется с помощью службы `chrony`, котора настраивается групповой политикой времени. Данная политика является коробочной и начинает свою работу после установки **ALD Pro** на контроллере или на клиенте домена.

Если необходимо добавить приоритетный источник, с которым должны синхронизироваться компьютеры в подразделении/подразделениях, то создаются пользовательские групповые политики, в которых настраиватся необходимые администратору параметры синхронизации времени: **Параметры компьютеров - Система - Дата и время**, параметры **Настройки сервиса сетевого времени Chrony** или **Параметры сервера или пула сетевого времени** (см. раздел **Групповые политики → Групповые политики → Настройка групповой политики**). Обязательно должно быть выбрано подразделение или подразделения на вкладке **Подразделения** этих групповых политик для применения заданных администратором параметров синхронизации времени к компьютерам, находящимся в выбранных подразделениях.

Созданная групповая политика распространяется на все компьютеры, которые входят в состав подразделений, выбранных на вкладке групповой политики **Подразделения**.

Подробная информация по атрибутам групповой политики представлена в справке (значок **(?)**). Ниже описаны особенности функционирования и настройки параметров времени групповых политик.

1.11.3.3. Настройки сервиса сетевого времени Chrony

«Коробочная» (предустановленная) групповая политика времени запускается каждый раз при старте операционной системы на каждом компьютере домена. Если какие-то из атрибутов данного параметра не заданы администратором, то для этих атрибутов используется значение по умолчанию:

- **Путь к файлу смещения**: `driftfile /var/lib/chrony/chrony.drift`;
- **Путь к файлу ключей**: `keyfile /etc/chrony/chrony.keys`;
- **Путь к директории журнала**: `logdir /var/log/chrony`;
- **Максимальное искажение для обновления**: `maxupdateskew 100.0`;
- **Настройка коррекции «шагом»**: `makestep 1 3`;

- **Использовать rtcsync**: строка `rtcsync` в файле отсутствует.

Значение атрибута `makestep` службы `chrony` складывается из значений трех полей:

- **Настройка коррекции «шагом» - Включить**: если атрибут включен, то учитываются значения двух следующих полей;
- **Настройка коррекции «шагом» - Порог**: минимальная величина отклонения (в секундах), при которой разрешается выполнение «шагового» изменения времени;
- **Настройка коррекции «шагом» - Предел**: максимальное количество раз, которое «шаговое» изменение времени может быть выполнено при первичной синхронизации с сервером.

1.11.3.4. Параметры сервера или пула сетевого времени

В поле **Адрес сервера или пула** указывается имя сервера (пула), который добавляется в конфигурацию службы `chrony` для компьютеров, на которую распространяется действие данной групповой политики.

Поле **Минимальный стратум** содержит значение минимального стратума для источника времени, чем оно меньше, тем источник более приоритетен при выборе в службе `chrony`. Допустимые значения: от 1 до 10 - при задании значений из этого диапазона сервер (пул) будет иметь приоритет над заданными с помощью «коробочной» групповой политики времени источниками.

1.11.4. Служба глобального каталога

В подразделе выполняется управление серверами службы динамической настройки узла (DHCP).

1.11.4.1. Список серверов

В подразделе на вкладке **Серверы глобального каталога** приводится список серверов с указанием названия сервера и имени сайта.

В списке доступен поиск по названию сервера и имени сайта. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Справа от поисковой строки расположена кнопка **[+ Развернуть сервер глобального каталога]**.

В левом нижнем углу указано количество серверов, а в правом нижнем углу кнопки переключения страниц.

1.11.4.2. Добавление сервера глобального каталога

Для добавления нового сервера необходимо нажать на кнопку **[+ Развернуть сервер глобального каталога]**, будет выполнен переход на карточку нового сервера.

На карточке необходимо заполнить обязательное поле:

- **Имя компьютера** — имя контроллера домена ALD Pro, который будет выполнять функции сервера глобального каталога, выбирается из выпадающего списка.

Поле **Имя сайта** заполняется автоматически после выбора имени компьютера.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

1.11.4.3. Удаление сервера глобального каталога

Удаление сервера осуществляется с таблицы серверов на странице **Служба глобального каталога**.

Для удаления сервера необходимо выделить его в талбице серверов и нажать кнопку **[Удалить]**. После подтверждения удаления сервер будет удалет из списка серверов.

1.11.5. Служба печати

В подразделе осуществляется добавление серверов печати, управление сетевыми принтерами и заданиями на печать. Сервер печати это отдельный компьютер, включенный в домен, на который установлен **CUPS**-сервер печати. CUPS-сервер получает команды от службы печати и запускает необходимые утилиты на компьютере.

1.11.5.1. Серверы печати

На вкладке подраздела приведен список серверов печати с указанием названия сервера, IP-адреса и имени сайта.

В списке доступен поиск по названию и IP-адресу сервера, а также по имени сайта. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Справа от поисковой строки расположена кнопка **[+ Развернуть сервер печати]**.

В левом нижнем углу указано количество серверов печати, а в правом нижнем углу кнопки переключения страниц.

1.11.5.2. Добавление сервера печати

Для добавления нового сервера печати необходимо нажать на кнопку **[+ Развернуть сервер печати]**, будет выполнен переход на карточку нового сервера печати.

На карточке на вкладке **Основное** заполнить обязательные поля:

- **Имя компьютера** — имя компьютера, добавленного в ALD Pro, который будет выполнять функции сервера печати;
- **Имя сайта** — выбрать из списка сайт, добавленный на вкладке *Сайты и службы* подраздела *Сайты и службы* (раздел *Управление доменом*).

Вкладка **Список принтеров** станет доступна после добавления сервера печати (см. раздел **Роли и службы сайта → Служба печати**→ ****Настройка сервера печати**).

Для добавления нового сервера печати необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X**

Закрыть]. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

1.11.5.3. Настройка сервера печати

Настройка сервера печати выполняется на его карточке. Для открытия карточки необходимо в списке серверов печати нажать на соответствующий сервер печати.

На карточке настройка сервера печати осуществляется на вкладках:

- **Основное**;
- **Список принтеров**.

Для закрытия карточки и возврата к списку серверов печати следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Основное

На вкладке приведено имя компьютера и имя сайта. Имя сайта доступно для редактирования.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Список принтеров

На вкладке осуществляется управление сетевыми принтерами.

На вкладке приведен список принтеров, добавленных к данному серверу печати, с указанием наименования принтера, его расположения, драйвера и описания.

В списке доступен поиск. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Справа от поисковой строки расположена кнопка **[+ Новый принтер]**.

В левом нижнем углу указано количество принтеров, а в правом нижнем углу кнопки переключения страниц.

Добавление принтера

Для добавления нового принтера необходимо на вкладке **Список принтеров** нажать на кнопку **[+ Новый принтер]**, будет выполнен переход на карточку нового принтера.

На карточке заполнить обязательные поля:

- **Подключение** — адрес подключения принтера в сети, с указанием протокола (ipp, socket, http(s)) (например, ipp://192.168.31.154);
- **Наименование принтера** — отображаемое имя принтера. Указывается на латинице, без пробелов.

Дополнительно можно заполнить поля:

- **Расположение** — местоположение принтера;
- **Драйвер** — загрузить драйвер принтера из файла (файлы с расширением *.ppd). Для загрузки драйвера необходимо в поле **Драйвер** нажать кнопку в виде папки и в открывшемся окне навигации выбрать требуемый файл;
- **Описание** — описание принтера.

Вкладка **Список заданий** станет доступна после добавления принтера (см. раздел **Роли и службы сайта → Служба печати**→ **Настройка сервера печати → Список принтеров → Настройка принтера**).

Для добавления принтера необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Настройка принтера

Настройка принтера выполняется на его карточке. Для открытия карточки необходимо в списке принтеров нажать на соответствующий принтер.

На карточке настройка принтера осуществляется на вкладках:

- **Основное**;
- **Список заданий**.

Для закрытия карточки и возврата к списку принтеров следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Основное

На вкладке приведена основная информация о принтере. Для редактирования доступны поля **Расположение** и **Описание** (см. раздел **Роли и службы сайта → Служба печати** → **Настройка сервера печати → Список принтеров → Добавление принтера**)..

Возможно заменить драйвер принтера, для этого в поле **Драйвер** нажать кнопку в виде папки и в открывшемся окне навигации выбрать требуемый файл.

Для сохранения изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Список заданий

На вкладке приведен список заданий, которые были отправлены для печати на данном принтере, с указанием наименования документа, имени пользователя, отправившего задание, размера файла, количества страниц и состояния задания на печать.

В списке доступен поиск. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Справа от поисковой строки расположена кнопка **[+ Новый принтер]**.

В левом нижнем углу указано количество заданий на печать, а в правом нижнем углу кнопки переключения страниц.

Для отмены задания на печать или одновременно нескольких заданий необходимо в списке заданий отметить требуемое и нажать кнопку **[Снять задание]**.

Чтобы отметить все задания — отметить пункт **Наименование задания**.

Удаление принтера

Для удаления принтера или одновременно нескольких принтеров необходимо в списке принтеров отметить требуемый и нажать кнопку **[Удалить]**.

Чтобы отметить все записи — отметить пункт **Наименование принтера**.

Также удалить принтер можно из его карточки: открыть карточку, нажав в списке принтеров на принтер, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить принтер]**. После подтверждения удаления будет выполнен переход к списку принтеров.

1.11.5.4. Удаление сервера печати

Удаление сервера печати осуществляется из его карточки: открыть карточку, нажав в списке серверов печати на сервер, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить]**. После подтверждения удаления будет выполнен переход к списку серверов печати.

1.11.6. Общий доступ к файлам

В подразделе осуществляется добавление серверов общего допуска (Samba-сервер), управление общими папками и допуском к ним. Samba-сервер развертывается на компьютере в домене ALD Pro и позволяет создать набор директорий, которые будут доступны для других компьютеров домена.

1.11.6.1. Серверы общих папок

В подразделе на вкладке **Перечень серверов** приведен список серверов с указанием названия сервера, его IP-адреса и имени сайта.

В списке доступен поиск по названию и IP-адресу сервера и по имени сайта. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Справа от поисковой строки расположена кнопка **[+ Новый сервер]**.

В левом нижнем углу указано количество серверов, а в правом нижнем углу кнопки переключения страниц.

1.11.6.2. Добавление сервера общих папок

Для добавления нового сервера необходимо нажать кнопку **[+ Новый сервер]**, будет выполнен переход на карточку нового сервера.

На карточке на вкладке **Основное** заполнить обязательные поля:

- **Имя компьютера** — имя компьютера, добавленного в ALD Pro, на котором будут размещаться папки общего допуска;
- **Имя сайта** — выбрать из списка сайт, добавленный на вкладке *Сайты и службы* подраздела *Сайты и службы* (раздел *Управление доменом*).

Вкладка **Общие папки** станет доступна после добавления сервера (см. *Настройка сервера общих папок*).

Для добавления нового сервера необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

1.11.6.3. Настройка сервера общих папок

Настройка сервера выполняется на его карточке. Для открытия карточки необходимо в списке серверов нажать на соответствующий сервер.

На карточке настройка сервера осуществляется на вкладках:

- **Основное**;
- **Общие папки**.

Для закрытия карточки и возврата к списку серверов следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Основное

На вкладке слева показана информация о подсистеме:

- название подсистемы,
- имя компьютера, на котором эта подсистема расположена,
- состояние подсистемы (см. *Состав системы*),
- дата создания подсистемы,
- дата последнего обновления подсистемы,
- версия установленного на компьютер подсистемы ALD Pro.

Есть возможность выполнить обновление ALD Pro на данном компьютере. Для этого необходимо нажать кнопку **Обновить ALD Pro**.

Есть возможность запустить удаление подсистемы с данного компьютера. Для этого необходимо нажать кнопку **Удалить**.

> **Внимание:** После удаления подсистемы, компьютер останется в домене. Установка новой подсистемы (удаленной или любой другой) возможна только после вывода компьютера из домена и переустановки операционной системы на нем.

Для просмотра всех изменений, произошедших с данным компьютером, необходимо нажать кнопку **Открыть журнал событий**. Откроется окно **Журнал истории изменений**, где отображены имя события и дата его наступления. Кнопка **Обновить** повзволяет получить актуальную информацию о событиях на компьютере.

На вкладке справа приведено имя компьютера, его IP-адрес и имя сайта. Имя сайта доступно для редактирования (см. *Добавление сервера общих папок*).

Для применения изменений необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X**

Закрыть]. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Общие папки

На вкладке осуществляется управление общими папками на данном сервере и допуском к ним.

Список общих папок

На вкладке приведен список общих папок данного сервера.

В списке доступен поиск по названию папки. Для этого в верхнем левом углу вкладки в поле поиска ввести значение.

Справа от поисковой строки расположена кнопка **[+ Новая папка]**.

Для просмотра информации об общей папке необходимо открыть ее карточку, нажав на папку в списке (см. *Информация об общей папке*).

В левом нижнем углу указано количество папок, а в правом нижнем углу кнопки переключения страниц.

Создание общей папки

Для создания новой общей папки необходимо нажать на кнопку **[+ Новая папка]**, будет выполнен переход на карточку новой папки.

На карточке на вкладке **Основное** указать следующие обязательные параметры:

- **Название папки**: задать отображаемое имя папки;
- **Относительный путь к локальной папке**: указать путь до папки, по умолчанию абсолютный путь `/opt/samba_shares + <относительный путь>`. Если локальной папки нет, она будет создана.

Так же можно указать:

- **Тип виртуальной файловой системы**: выбирается из выпадающего списка;
- **Browsable**: устанавливает, будет ли общая папка отображаться в списке доступных

общих ресурсов в сетевом окружении и в списке просмотра;

- **Access based share enum**: скрывает от пользователя файлы и папки, к которым у него нет доступа;
- **Права доступа для новых файлов**: набор разрешений Unix в восьмеричном коде, устанавливаемых на файл (см. подробнее документацию по Samba);
- **Права доступа для новых файлов**: набор разрешений Unix в восьмеричном коде, устанавливаемых на папку (см. подробнее документацию по Samba);
- **Наследование прав доступа**: управление правами доступа к новым файлам и папкам, созданным в общей папке. При установке флажка **Да** значения полей **Права доступа для новых файлов** и **Права доступа для новых папок** игнорируются.

Вкладки **Доступ пользователей** и **Доступ групп** станет доступна для редактирования после создания папки (см. *Управление допуском к общей папке*).

Для создания новой общей папки необходимо нажать на кнопку сохранения в правом верхнем углу.

Для закрытия карточки и возврата к списку папок нажать на кнопку закрытия.

Информация об общей папке

Информация об общей папке доступна на ее карточке. Для открытия карточки необходимо в списке общих папок нажать на соответствующую папку.

На вкладке **Основное** приведено название папки. Название можно изменить.

Для просмотра размера папки нажать кнопку **[Получить размер папки]**.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Управление допуском к общей папке

Управление допуском к папке выполняется на ее карточке. Для открытия карточки необходимо в списке общих папок нажать на соответствующую папку.

На карточке выбранной папки доступны вкладки:

- **Основное**;
- **Доступ пользователей**;
- **Доступ групп**.

Основное

На вкладке **Основное** для изменения доступны все поля:

- **Название папки**;
- **Относительный путь к локальной папке**;
- **Тип виртуальной файловой системы**;
- **Browsable**;
- **Access based share enum**;
- **Права доступа для новых файлов**;
- **Права доступа для новых папок**;
- **Наследование прав доступа**.

Для сохранения изменений в карточке необходимо нажать на кнопку **[Сохранить]** в правом верхнем углу. И подтвердить действие во всплывающем окне.

Для закрытия карточки и возврата к предыдущему списку следует нажать на кнопку **[X Закрыть]**. В случае закрытия карточки возникнет всплывающее окно для подтверждения закрытия без внесенных изменений, если таковые есть.

Доступ пользователей

На вкладке **Доступ пользователей** представлен список пользователей, которым предоставлен допуск к папке, с указанием типа предоставляемого права допуска (чтение/полный допуск).

Для изменения настроек допуска к папке необходимо нажать кнопку **[Редактировать доступ]**, после чего откроется карточка управления допуском к папке.

Открывшаяся карточка представляет из себя области со списками пользователей **Выбранные пользователи** и **Все пользователи**, а так же поле с выпадающим списком

Доступ для выбора типа предоставляемого допуска:

- **Чтение** — допуск на просмотр;
- **Полный доступ** — допуск на просмотр, добавление, изменение и удаление;
- **Изменение и назначение прав** - доступ на просмотр, запись, изменение прав доступа к объекам;
- **Доступ запрещен** - доступа к папке нет.

Для управления допуском к выбранной общей папке из выпадающего списка **Доступ** необходимо выбрать тип предоставляемого допуска к файлам данной общей папки, затем в списке **Все пользователи** отметить нужных пользователей и перенести их в список **Выбранные пользователи** нажатием кнопки **[<-]**.

Для отмены предоставления данного типа допуска пользователям необходимо в списке **Выбранные пользователи** отметить требуемые записи и перенести их в список **Все пользователи** нажатием кнопки **[→]**.

Для быстрого поиска пользователя в верхней части каждого из списков доступно поле поиска пользователей по фамилии или логину, в котором достаточно начать вводить нужные данные о пользователе.

После внесения изменений необходимо нажать кнопку **[Сохранить]** в правом верхнем углу.

Внизу каждого списка указано количество пользователей в данном списке.

Доступ групп

На вкладке **Доступ групп** представлен список групп, которым предоставлен допуск к папке, с указанием типа предоставляемого права допуска (чтение/полный допуска).

Для изменения настроек допуска к папке необходимо нажать кнопку **[Редактировать доступ]**, после чего откроется карточка управления допуском к папке.

Открывшаяся карточка представляет из себя области со списками групп **Выбранные группы** и **Все группы**, а так же поле с выпадающим списком **Доступ** для выбора типа предоставляемого допуска:

- **Чтение** — допуск на просмотр;
- **Полный доступ** — допуск на просмотр, добавление, изменение и удаление;
- **Изменение и назначение прав** - доступ на просмотр, запись, изменение прав

доступа к объекам;

- **Доступ запрещен** - доступа к папке нет.

Для управления допуском к выбранной общей папке из выпадающего списка **Доступ** необходимо выбрать тип предоставляемого допуска к файлам данной общей папки, затем в списке **Все группы** отметить нужных пользователей и перенести их в список **Выбранные группы** нажатием кнопки **[<-]**.

Для отмены предоставления данного типа допуска для групп необходимо в списке **Выбранные группы**отметить требуемые записи и перенести их в список **Все группы** нажатием кнопки**[→]**.

После внесения изменений необходимо нажать кнопку **[Сохранить]** в правом верхнем углу.

Для быстрого поиска группы в верхней части каждого из списков доступно поле поиска групп по названию, в котором достаточно начать название группы.

Внизу каждого списка указано количество групп в данном списке.

Удаление общей папки

Удаление общей папки выполняется на ее карточке. Для открытия карточки необходимо в списке общих папок нажать на соответствующую папку, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить папку]**. После подтверждения удаления будет выполнен переход к списку общих папок.

1.11.6.4. Удаление сервера общих папок

Удаление сервера общих папок осуществляется из его карточки: открыть карточку, нажав на сервер в списке серверов общих папок, затем на карточке на вкладке **Основное** нажать кнопку **[Удалить]**. После подтверждения удаления будет выполнен переход к списку серверов общих папок.

1.12. Личный кабинет

В этом разделе осуществляется управление данными личного кабинета авторизованного пользователя.

Раздел состоит из следующих вкладок:

1.12.1. Основное

На вкладке **Основное** приведены группы полей ввода данных:

- **Персональные данные**;
- **Учетная запись**;
- **Организационные данные**;
- **Контактная информация**;
- **Расположение**;
- **Сертификаты пользователей**;
- **Открытые ключи SSH**.

Для удобства работы группы полей ввода можно разворачивать/сворачивать нажимая на их название.

1.12.1.1. Персональные данные

В этой группе представлены следующие поля ввода:

- **Фамилия**;
- **Имя**;
- **Отчество**;
- **Отображаемое имя**.

Так же имеется поле для отображения загруженной фотографии пользователя, по умолчанию фото отсутствует, о чем свидетельствует надпись в поле (**Фото не загружено**). Для загрузки фотографии пользователя имеется кнопка **[Загрузить фото]**. При нажатии на эту кнопку, появляется окно для указания пути на компьютере, откуда фото будет загружено.

1.12.1.2. Учетная запись

В этой группе представлены следующие поля ввода:

- **Идентификатор пользователя (UID)**;
- **Логин**;
- **Текущий пароль**;
- **Новый пароль**;
- **Подтверждение пароля**;
- **Окончание действия пароля**.

Так же имеются кнопка **Заблокировать УЗ**, которая доступна в режиме администратора.

Важно: При смене паролей необходимо учитывать, что минимальный срок действия паролей составляет один час, максимальное количество попыток смены пароля — шесть, а длительность блокировки после израсходования попыток составляет 600 секунд. Эти значения могут быть изменены в политиках паролей (раздел *Групповые политики* — подраздел *Политики паролей*). Новый пароль должен соответствовать политике паролей, распространяющей своё действие на пользователя.

1.12.1.3. Организационные данные

В этой группе представлены следующие поля ввода:

- **Подразделение**;
- **Должность**;
- **Руководитель сотрудника**.

1.12.1.4. Контактная информация

В этой группе представлены следующие поля ввода:

- **Электронный адрес сотрудника**;
- **Номер рабочего телефона** и **Добавочный**;

- **Номер мобильного телефона**.

Так же имеется кнопка **Дополнительно…** для перехода на вкладку **Расширенные настройки** и ввода дополнительных данных о пользователе.

1.12.1.5. Расположение

В этой группе представлены следующие поля ввода:

- **Улица**;
- **Город**;
- **Область, край**;
- **Почтовый индекс**;
- **Страна или регион**.

1.12.1.6. Сертификаты пользователей

В этой группе отображено поле ввода сертификата в формате **base64** или **PEM**. Для добавления сертификана необходимо в поле **Сертификат в формате base64 или PEM** ввести имеющийся сертификат и нажать кнопку **[Добавить]**.

1.12.1.7. Открытые ключи SSH

В этой группе отображено поле ввода ключа в формате **SSH**. Для добавления ключа необходимо в поле **Ключ в формате SSH** ввести имеющийся ключ и нажать кнопку **[Добавить]**.

1.12.2. Группы

На вкладке **Группы** приведены две группы полей с данными:

- **Состоит в группах**;
- **Состоит в группах непрямое наследование**

1.12.2.1. Состоит в группах

В этом поле отображены два списка с группами:

- **Выбранные группы** — список с групп, в которых состоит пользователь;
- **Все группы** — список групп, доступных вступления.

Для того чтобы добавиться в одну или несколько групп, необходимо в списке **Все группы** отметить требуемые группы и перенести их в **Выбранные группы** нажав кнопку **[<-]**, расположенную между этими списками. Чтобы выйти из одной или нескольких групп, необходимо в списке **Выбранные группы** отметить требуемые группы и перенести их в **Все группы** нажав кнопку **[→]**, расположенную между этими списками.

Для списка **Все группы** так же доступна возможность добавления в список новых групп с помощью кнопки **[+ Новая группа]**.

Для списков групп доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списков указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

1.12.2.2. Состоит в группах непрямое наследование

В этом поле отображены группы имеющие непрямое наследование, в которых состоит владелец личного кабинета.

Для списка групп доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списков указано количество записей в данном списке.

1.12.3. Дополнительные сведения

На вкладке **Дополнительные сведения** приведены поля ввода данных:

- **Дополнительный номер телефона**;
- **Дата приема на работу**;
- **Дополнительные сведения**;
- поле с указанием пола пользователя (**[М]** или **[Ж]**);
- **Табельный номер**.

1.12.4. Групповые политики

На этой вкладке приведен список групповых политик, которые распространяются на владельца личного кабинета.

1.12.5. Расширенные настройки

На этой вкладке приведены поля ввода для дополнительных адресов пользователя.

1.12.6. Роли

На вкладке **Роли** приведены и отображены два списка с типами администратора:

- **Выбранные роли** — список типов администратора, присвоенных пользователю;
- **Все роли** — список типов администратора, доступных для присвоения пользователю.

Для того чтобы присвоить одну или несколько ролей, необходимо в списке **Все роли** отметить требуемые типы администратора и перенести их в **Выбранные роли**, нажав кнопку **[<-]**, расположенную между этими списками. Чтобы исключить пользователя из обладателя одного или нескольких типов администратора, необходимо в списке **Выбранные роли** отметить требуемые типы администратора и перенести их в **Все роли**, нажав кнопку **[→]**, расположенную между этими списками.

Для списков ролей доступен поиск по названию. Для этого в соответствующем поле поиска начать вводить значение, результат поиска будет выводиться по мере ввода.

Внизу списков указано количество записей в данном списке.

Для применения изменений необходимо нажать на кнопку сохранения в правом верхнем углу.

Пользователям без роли или без привилегии на чтение пользователей (**Users - Read**) доступен только ЛК с возможностью сброса пароля и изменения полей:

- **Номер мобильного телефона**;
- **Открытые ключи SSH**.

Пользователям с привилегией на чтение пользователей (Users - Read) доступен ЛК в разделе **Пользователи и компьютеры** → **Пользователи** → карточка текущего пользователя; просмотр всех вкладок, кроме **Дополнительные сведения**; изменение полей:

- **пароль**;
- **Номер мобильного телефона**;
- **Открытые ключи SSH**;

Остальные поля и таблицы - только для чтения.

Пользователям с привилегией на редактирование пользователей (**Users - Modify**) доступны все поля для изменения на вкладках **Основное** и **Расширенные настройки**.

Для изменения других вкладок требуются соответствующие привилегии **Modify**.

1.12.7. МРД

Данные об МРД в карточке пользователя расположены на отдельной вкладке и разделены внутри на 3 вкладки:

- **Параметры**;
- **Привилегии Parsec**;
- **Аудит Parsec**.

В данном разделе приведена информация о настройке и работе программного обеспечения «Программный комплекс «ALD Pro» (далее — **ALD Pro**). **ALD Pro** является системой централизованного администрирования доменной инфраструктуры.

Основная информация о программном обеспечении приведена в разделе *О системе*.

Аутентификация пользователя, вход, выход, смена пользователя описаны в разделе *Аутентификация пользователей*.

1.13. Начало работы с ALD Pro

При запуске **ALD Pro** отображается главная страница, на которой расположены разделы настройки и управления **ALD Pro**:

- *Управление доменом* — управление структурой и конфигурацией системы;
- *Пользователи и компьютеры* — управление организационной структурой, пользователями и компьютерами;
- *Групповые политики* — управление и назначение групповых политик;
- *Установка и обновление ПО* — управление журналом заданий, группами и репозиториями программного обеспечения;
- *Автоматизация* — настройка и запуск заданий автоматизации, а также инструменты для установки операционной системы по сети;
- *Роли и службы сайта* — службы разрешения имен, динамической настройки узла, синхронизации времени, печати и общий доступ к файлам;
- *Мониторинг* — настройка параметров мониторинга, а также журнал событий мониторинга и витрины мониторинга домена;
- *Журнал событий* — настройка и просмотр журналов событий;
- *Модуль синхронизации* — синхронизации объектов и их изменений, находящихся в домене **Microsoft Active Directory** (далее **MS AD**), в домен **ALD Pro**.

1.14. Интерфейс Портала Управления

Интерфейс ПК «ALD Pro» состоит из разделов и подразделов, которые содержат необходимые инструменты для выполнения различных задач и действий над задачами.

В правой верхней части слева направо отображены всегда доступные из любого раздела значки:

- значок **выбора доступных контроллеров домена** — при наведении на значок отображается имя выбранного домена, а при нажатии на треугольный значок появляется выпадающий список выбора доступных контроллеров домена. При плохом сетевом соединении, либо при его отсутствии с выбранным контроллером домена, можно произвести переключение на другой (резервный) контроллер домена;
- значок перехода в *Личный кабинет* — служит для перехода в *Личный кабинет* текущего авторизованного пользователя. В личном кабинете доступна смена пароля, редактирование личных данных и других настроек, связанных с текущей авторизованной учетной записью (см. *Личный кабинет*);
- значок **темы** (символ солнца или месяца) используется для переключения между темным и светлым оформлением интерфейса;
- значок перехода в на страницу **Справочного центра** (знак вопроса в круге).

В интерфейсе **ALD Pro** при создании или просмотре объекта открывается его карточка.

В карточке отмечены обязательные поля, без заполнения которых сохранить изменения невозможно.

Сохранение изменений в карточке осуществляется нажатием на кнопку **[Сохранить]** или нажатием на кнопку в виде дискеты в правом верхнем углу окна.

Если в поле карточки введены некорректные данные (информация о существующих ограничениях присутствует под соответствующим полем), то при сохранении изменений будет отображено сообщение об ошибке.

Закрыть карточку можно при помощи кнопки **[X]** в правом верхнем углу окна. После этого будет осуществлен переход к предыдущей открытой карточке.

1.15. Навигация по Порталу Управления

При запуске **Портала Управления «ALD Pro»** отображается главная страница. Во время работы с **ALD Pro**, для возврата на главную страницу из любого места, необходимо нажать значок **ALD Pro**, расположенный в левом верхнем углу окна программы.

При нахождении на главной странице программы, для перехода в требуемый раздел, необходимо нажатием выбрать этот раздел, и в выпадающем списке выбрать нужный подраздел.

При нахождении в любом из подразделов программы, для быстрого перехода в любой другой раздел, в левой части окна программы расположена панель навигации по разделам. Для того, чтобы показать/скрыть названия разделов и подразделов панели навигации в левой части окна, необходимо нажать на кнопку в виде стрелки вправо/влево, расположенную в нижнем левом углу окна.

Текущее местонахождение в системе **ALD Pro** отображается в левой верхней части окна интерфейса.

Отладка подсистем ALD Pro

Для эффективного управления доменом на предприятии системный администратор должен четко понимать, какие службы обеспечивают работу компьютера в домене и как выполнять отладку их работы, если возникнут какие бы то ни было внештатные ситуации. Настоящая инструкция ставит целью ответить на все указанные вопросы с максимальной степенью детализации.

2.1. Архитектура SSSD

За работу компьютера в домене отвечает служба **SSSD** (System Security Services Daemon), установка которой происходит вместе с пакетом **aldpro-client**, а настройка выполняется при вводе компьютера в домен с помощью утилиты **aldpro-client-installer**. Для управления службой используется приложение **systemctl**, которое позволяет запускать и останавливать службу, а также просматривать ее текущее состояние:

```
sudo systemctl stop sssd
sudo systemctl start sssd
sudo systemctl restart sssd
sudo systemctl status sssd
```

Результат выполнения команды:

```
sssd.service - System Security Services Daemon
  Loaded: loaded (/lib/systemd/system/sssd.service; enabled; vendor preset:
↪enabled)
  Active: active (running) since Mon 2023-07-31 22:38:35 MSK; 5s ago
Main PID: 3740 (sssd)
   Tasks: 4 (limit: 4597)
  Memory: 10.1M
  CGroup: /system.slice/sssd.service
          ├─3740 /usr/sbin/sssd -i --logger=files
          ├─3741 /usr/lib/x86_64-linux-gnu/sssd/sssd_be --domain ald.company.
↪lan --uid 0 --gid 0 --logger=files
          ├─3742 /usr/lib/x86_64-linux-gnu/sssd/sssd_ifp --uid 0 --gid 0 --
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
↪logger=files
         └─3743 /usr/lib/x86_64-linux-gnu/sssd/sssd_pac --uid 0 --gid 0 --
↪logger=files
```

Основная задача службы **SSSD** заключается в предоставлении доступа к информации удаленной службы каталога и механизмам централизованной аутентификации. В качестве поставщика данных для **SSSD** может выступать **FreeIPA**, **Active Directory**, **Kerberos** домен и даже простой LDAP каталог. Продукт ALD Pro построен на базе службы каталога **FreeIPA**, поэтому в конфигурационных файлах */etc/sssd/sssd.conf* на доменных компьютерах будет указан поставщик `ipa`, например, `id_provider = ipa`.

При входе доменного пользователя в систему у него появляется домашняя директория, но служба **SSSD** не создает его как локального пользователя. Для ускорения работы системы и возможности обслуживания пользователя в автономном режиме служба **SSSD** помещает информацию, полученную от поставщика данных, в локальный кэш.

Идентификационные данные пользователей всегда кэшируются, так же как и информация о доменных службах. Это означает, что **SSSD** всегда проверяет запросы на аутентификацию. Поддержание кэша в актуальном состоянии является сложной задачей, поэтому **SSSD** состоит из множества компонентов, которые взаимодействуют друг с другом с помощью различных методов межпроцессного взаимодействия, архитектура службы представлена см. *Архитектура службы SSSD*.

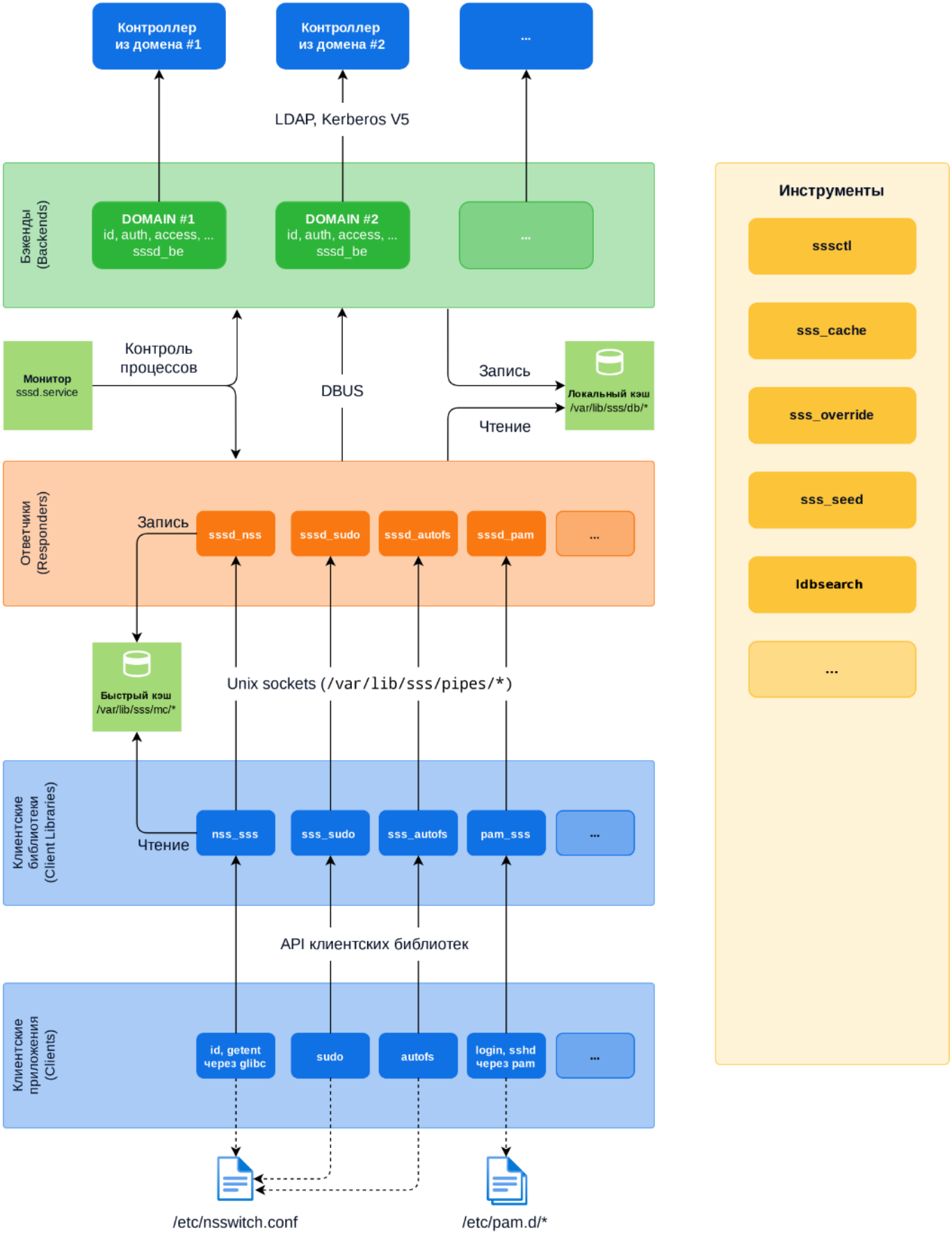


Рисунок 2.1 – Архитектура службы SSSD

2.1.1. Монитор (Monitor)

Службу **sssd.service** называют **Монитором** или **Наставником**, так как она порождает процессы всех других компонентов и управляет ими через систему межпроцессного взаимодействия **SBus** (**SSSD D-Bus**). Чтобы понять диаграмму процесса загрузки службы см. *Диаграмма загрузки службы SSSD*.

- В момент запуска службы **Монитор** анализирует файл конфигурации **sssd.conf** (1) и загружает его в кэш */var/lib/sss/db/config.ldb* (2). Далее **Монитор**, используя системные вызовы, порождает процесс **Бэкенда** (3), который загружает информацию из **config** (4, 5) и регистрирует себя в **Мониторе** (6).
- На следующем шаге **Монитор** порождает **Ответчиков NSS** и **PAM** (7), которые считывают информацию из **config** (8, 9) и регистрируются в **Мониторе** (10) и **Бэкенде** (11).

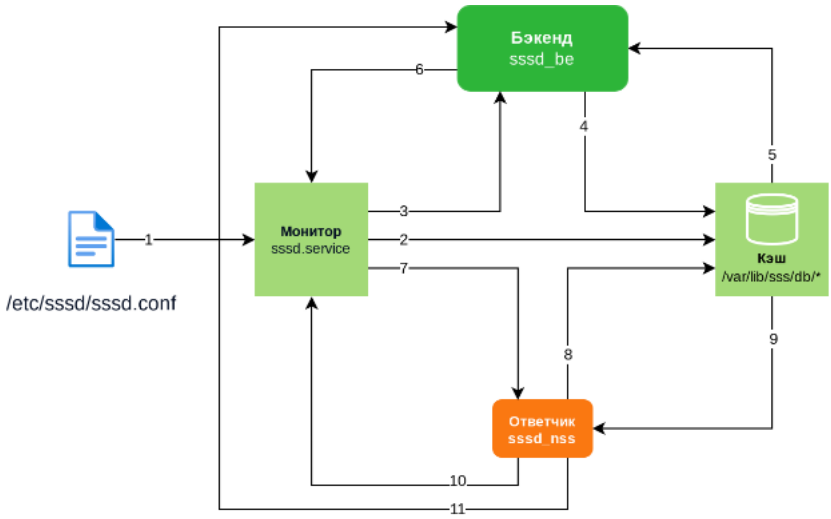


Рисунок 2.2 – Диаграмма загрузки службы SSSD

Помимо внутреннего взаимодействия через **SBus**, служба **SSSD** использует UNIX-сигналы, например, в тех случаях, когда процесс завис и не отвечает через **SBus**. Обработчики сигналов обычно интегрированы с главным циклом событий **tevent** с использованием вызова `tevent_add_signal`:

- ``SIGTERM — сигнал на завершение работы процесса.
- `SIGKILL` — сигнал для принудительного завершения работы процесса, который направляется монитором, если процесс не завершается после получения **SIGTERM**.
- `SIGUSR1` — сигнал на переключение **Бэкенда** в автономный режим. Если сигнал будет направлен Монитору, то он перешлет его всем дочерним процессам **sssd_be**.
- `SIGUSR2` — сигнал на переключение **Бэкенда** в режим онлайн. Если сигнал будет

направлен Монитору, то он перешлет его всем дочерним процессам **sssd_be**.

- `SIGHUP` — может быть передан **Монитору**, после чего тот начнет новый лог-файл и вызовет метод сброса журналов управляемым процессам. Управляемые процессы также начинают новые лог-файлы. Кроме того, процессы **sssd_be** перечитывают *resolv.conf*, а процесс **sssd_nss** выполнит очистку быстрого кэша.

2.1.2. Серверные части или Бэкенды (backends)

Бэкенд (Backend, BE) включает в себя **Поставщики данных** (Data Provider, DP) – это процесс приложения */usr/lib/x86_64-linux-gnu/sssd/sssd_be*, который запускается **Монитором** для взаимодействия с доменом в соответствии с настройками секции [domain/<имя_домена>] конфигурационного файла *sssd.conf*.

```
sudo ps -aux | grep sssd_be
```

Результат выполнения:

```
root    5885 0.0 0.6 118804 26532 ?  S 21:43 0:00 /usr/lib/x86_64-linux-gnu/
↪sssd/sssd_be --domain ald.company.lan --uid 0 --gid 0 --logger=files
```

Описание **бэкендов** в конфигурационном файле можно просмотреть командой:

```
sudo cat /etc/sssd/sssd.conf
```

Результат выполнения:

```
...
[domain/ald.company.lan]
id_provider = ipa
ipa_server = _srv_, dc-1.ald.company.lan
ipa_domain = ald.company.lan
ipa_hostname = pc-1.ald.company.lan
auth_provider = ipa
chpass_provider = ipa
access_provider = ipa
cache_credentials = True
ldap_tls_cacert = /etc/ipa/ca.crt
krb5_store_password_if_offline = True
...
```

Бэкенд не является монолитом и в зависимости от настроек подключает один и более **Поставщиков** данных, каждый из которых представляет из себя совместно используемую библиотеку (Shared Object, SO). Библиотеки **SSSD** находятся в каталоге */usr/lib/x86_64-linux-gnu/sssd/*, и за работу компьютера в домене ALD Pro (FreeIPA), например, отвечает **Поставщик ipa**, которому соответствует библиотека *libsss_ipa.so*. Если же ввести Linux компьютер напрямую в домен Active Directory, то будет использоваться *libsss_ad.so*.

Каждый **Поставщик** данных может оказывать **Бэкенду SSSD** следующие услуги:

- идентификация (`id_provider`) — предоставление информации о пользователях, служебных учетных записях, группах и т.д.;
- аутентификация (`auth_provider`) — проверка аутентичности пользователей и служб;
- авторизация (`access_provider`) — проверка прав доступа на запуск служб на уровне HBAC;
- поставщик sudo (`sudo_provider`) — предоставление информации о правилах SUDO на повышение привилегий;
- и другие.

Разные модули могут использовать разные настройки, например, для **Поставщика ipa** требуется задать параметр **ipa_server**, который используется для определения контроллера домена **FreeIPA**, с которым требуется поддерживать соединение. По умолчанию в конфигурационном файле *sssd.conf* для домена явно задается только несколько провайдеров (`id`, `auth`, `chpass`, `access`), а для других провайдеров подразумевается, что их имя совпадает с именем поставщика идентификационных данных (`id_provider`).

Для удобства, из соображений сокращения размера конфигурационного файла, служба **SSSD** руководствуется следующими правилами:

- Если параметр `ipa_domain` не указан, то используется FQDN имя домена из секции [`domain/<fqdn домена>`].
- Если параметр `ipa_server` не указан, то сервер определяется автоматически через DNS, как будто параметр `ipa_server` равен `_srv_`.
- Если провайдер не указан, то используется значение `id_provider` (например, **ipa**). Исключением является `access_provider`, если его значение не указано, то по умолчанию параметр принимает значение `permit`, что означает «всем пользователям разрешен доступ». Для управления доступом параметр

`access_provider` должен быть задан явно.

Таким образом, стандартный файл конфигурации */etc/sssd/sssd.conf* может быть упрощен до следующего вида:

```
...
[domain/ald.company.lan]
id_provider = ipa
access_provider = ipa
cache_credentials = True
ldap_tls_cacert = /etc/ipa/ca.crt
krb5_store_password_if_offline = True
...
```

2.1.3. Ответчики (responders)

Ответчик служит посредником между пользовательским приложением, таким как **id** или **getent**, и кэшем **SSSD**. Когда приложение запрашивает данные, например, ищет пользователя по имени, **Ответчик** выполняет поиск в локальном кэше и, если данные не найдены или устарели, обращается к **Бэкенду**, чтобы тот совершил запрос к северу службы каталога. Клиентские библиотеки взаимодействуют с **Ответчиком** через **Unix socket** (например, */var/lib/sss/pipes/nss*), а внутри ядра **SSSD** между **Ответчиками**, **Бэкендами** и **Монитором** взаимодействие осуществляется через **DBus**.

Каждый **Ответчик** работает в отдельном процессе и выполняет строго определенные задачи, например:

- Ответчик **NSS** (`sssd_nss`) обеспечивает данными диспетчер службы имен (Name Service Switch, NSS).
- Ответчик **PAM** (`sssd_pam`) предоставляет данные для работы подключаемых модулей аутентификации (Pluggable Authentication Modules, PAM).
- Ответчик **SUDO** (`sssd_sudo`) обеспечивает правилами утилиту `sudo`.
- И так далее.

2.1.4. Клиентские библиотеки и приложения

Для взаимодействия с **Ответчиком** приложению нужно обращаться к соответствующему **unix сокету** по специфичному сетевому протоколу, поэтому для упрощения разработки клиентских приложений были созданы вспомогательные совместно используемые библиотеки, такие как *libnss_sss.so.2*, *pam_sss.so* и др., которые можно найти в каталоге */usr/lib/x86_64-linux-gnu*.

Например, если в конфигурационном файле *nsswitch.conf* для базы **sudoers** источником данных будет указан **sss**, то утилита **sudo** для взаимодействия с **Ответчиком sssd_sudo** воспользуется функциями из библиотеки *libsss_sudo.so*. Аналогичным образом работает **autofs**.

Однако, есть и такие приложения, которые могут даже не знать о существовании **SSSD**, если используют более универсальные функции из библиотек **pam** и **glibc**, которые взаимодействуют с клиентскими библиотеками **SSSD** от имени приложения. Например, утилиты **id**, **getent**, **ls** вызывают стандартные функции **NSS**, которые извлекают информацию из нескольких баз данных имен (например, `passwd`, `group`, `service`, `netgroup` и т.д.). Рассмотрим поток данных, создаваемый клиентским приложением **id**, выполняющим **NSS** запрос через службу **SSSD**, см. *Диаграмма потока данных при вызове команды id*:

- Клиентское приложение */usr/bin/id* вызывает функцию `getpwnam` из библиотеки **glibc** для получения информации о пользователе (1).
- Библиотека `glibc` загружает конфигурационный файл *nsswitch.conf* (2, 3) и в соответствии с его настройками загружает совместно используемую библиотеку *libnss_sss.so.2* и вызывает ее функцию `_nss_sss_getpwnam_r` (4)
- Для получения данных от **Ответчика** */usr/lib/x86_64-linux-gnu/sssd/sssd_nss* библиотека *libnss_sss.so.2* отправляет запрос через **unix сокет** */var/lib/sss/pipes/nss* по специализированному протоколу обмена данными (5).
- Ответчик **NSS** проверяет наличие данных в кэше (6, 7), и в случае отсутствия данных или истекшего срока их действия отправляет запрос `getAccountInfo` к **Бэкенду**, запрашивая необходимые данные (8).
- **Бэкенд** из-под учетной записи хоста */etc/krb5.ketyab* направляет LDAP-запрос для получения данных от службы каталога (9). Если запрашиваемый пользователь принадлежит тому же домену, то это будет прямой запрос на поиск информации, в противном случае **SSSD** выполнит расширенную LDAP операцию.

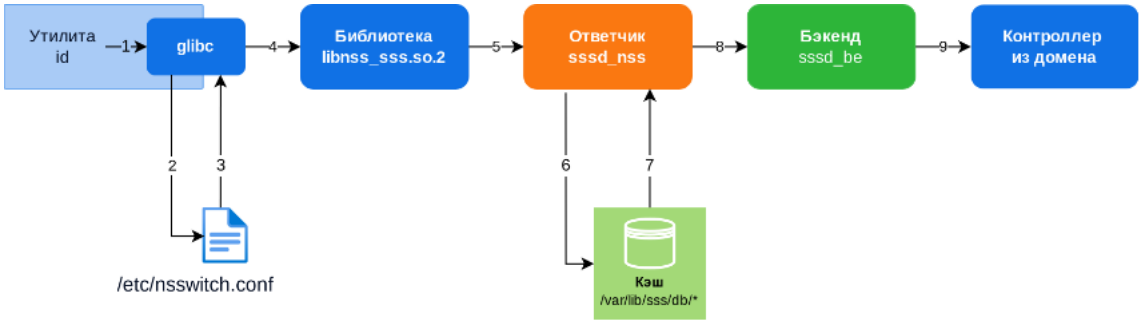


Рисунок 2.3 – Диаграмма потока данных при вызове команды id

Библиотека **PAM** работает аналогичным образом с небольшими отличиями. Например, если служба **SSSD** находится онлайн, то при входе пользователя в систему она обязательно предпримет попытку повторной аутентификации и получения информации об участии пользователя в группах, даже если срок действия кэша еще не истек, а все команды выполняются в контексте одной транзакции **PAM**. В качестве примеров клиентских приложений, использующих **PAM**, можно привести **login**, **su** и **sshd**.

Несмотря на то, что клиентские приложения и библиотеки не являются синонимами, в рабочей документации и программном коде службы **SSSD** под словосочетанием **SSSD Client** (суффикс **sss_cli**) часто подразумеваются именно клиентские библиотеки, а не сами приложения. Например, идентификатором **sss_cli** обозначается сетевой протокол, с помощью которого клиентские библиотеки общаются с **Ответчиками** службы **SSSD**.

2.1.5. Механизм кэширования службы SSSD

Служба **SSSD** в своей работе активно использует кэш, что позволяет исключить повторные обращения к серверу за получением одних и тех же данных, когда в этом нет необходимости, и обеспечивает возможность работы в автономном режиме без подключения к серверу. Система кэширования довольно сложна и включает в себя несколько взаимодополняющих механизмов.

2.1.5.1. Локальный кэш (local cache, cache)

Локальный кэш – это база данных, в которую **Бэкенды** записывают результаты, получаемые из службы каталога, чтобы **Ответчики** могли считывать их напрямую. При помещении объектов в кэш им назначается срок жизни, и до тех пор, пока он не истечет, все последующие запросы к этим данным обрабатываются без обращения к серверу.

Устаревшие данные могут извлекаться из кэша только в том случае, если служба находится в автономном режиме.

Файлы локального кэша находятся на диске в каталоге */var/lib/sss/db/*, для работы с этим кэшем служба **sssd** использует встроенную библиотеку баз данных облегченного доступа (light weight embedded database library, **ldb**) — ту же библиотеку, с помощью которой реализована база данных службы каталога **Samba AD**. Если установить пакет **ldb-tools**, то станет доступна утилита **ldbsearch**, с помощью которой можно заглянуть внутрь **ldb**-файлов. Структура этой базы данных подобна LDAP-каталогу, а параметры `ldbsearch` во многом повторяют параметры утилиты **ldapseach**:

```
sudo rm -rf /var/lib/sss/db/*; systemctl restart sssd ldbsearch -H /var/lib/
↪sss/db/cache_ald.company.lan.ldb /
-b name=admin@ald.company.lan,cn=users,cn=ald.company.lan,cn=sysdb uidNumber
asq: Unable to register control with rootdse!
# returned 0 records
# 0 entries
# 0 referrals
```

Для проверки кэша запрашивается информация командой `id`:

```
sudo id admin
```

Результат выполнения:

```
uid=959800000(admin) gid=959800000(admins) группы=959800000(admins),
↪1001(astra-admin),113(lpadmin)
```

Отображается, что сохранилось в локальном кэше командой:

```
sudo ldbsearch -H /var/lib/sss/db/cache_ald.company.lan.ldb /
-b name=admin@ald.company.lan,cn=users,cn=ald.company.lan,cn=sysdb uidNumber
```

Результат выполнения:

```
asq: Unable to register control with rootdse!
# record 1
dn: name=admin@ald.company.lan,cn=users,cn=ald.company.lan,cn=sysdb
uidNumber: 959800000
# returned 1 records
# 1 entries
```

(продолжение на следующей странице)

```
# 0 referrals
```

Но на низком уровне **ldb** использует библиотеку **Trivial DataBase**, поэтому сырые данные в формате ключ-значение можно извлекать с помощью утилит из пакета **tdb-tools**:

```
root@dc-1:~# tdbtool /var/lib/sss/db/config.ldb keys
```

Результат выполнения:

```
key 18 bytes: DN=@INDEX:CN:SSSD
key 21 bytes: DN=CN=SSSD,CN=CONFIG
key 18 bytes: DN=@INDEX:CN:SUDO
key 17 bytes: DN=@INDEX:CN:PAC
key 13 bytes: DN=CN=CONFIG
...
```

В папке */var/lib/sss/db/* находятся следующие **ldb**-файлы локального кэша:

- *config.ldb* – кэш для хранения настроек службы, загружаемых из конфигурационного файла /etc/sssd/sssd.conf
- *sssd.ldb* – база данных локального домена (**local provider**), который позволял использовать возможности вложенных групп без централизованной службы каталога. Для администрирования использовались команды `sss_useradd`, `sss_groupadd` и др., поддержка функции прекращена с версии **SSSD** 2.0.0.
- *cache_ald.company.lan.ldb* – кэш для хранения критически важной информации, получаемой из домена. Сохранение таких данных на диск требуется выполнять сразу при получении новых данных.
- *timestamps_ald.company.lan.ldb* – кэш для хранения некритичной и часто обновляемой информации. Сохранение данных на диск выполняется в фоновом режиме по усмотрению операционной системы. Кроме файлов локального кэша в этой же папке находятся файлы кэша учетных данных Kerberos, которые можно просматривать с помощью утилиты **klist** с ключом `-c`.
- *ccache_ALD.COMPANY.LAN* – кэш для хранения Kerberos-билетов службы **SSSD**, с помощью которых она выполняет LDAP-запросы к службе каталога.
- *fast_ccache_ALD.COMPANY.LAN* – кэш для хранения TGT-билета, с помощью сессионного ключа которого которого обеспечивается дополнительное шифрование запросов по технологии **FAST Armoring**.

Удаление всех файлов из директории **db** является самым простым, но в тоже время и самым полным способом очистки локального кэша службы **sssd**:

```
sudo systemctl stop sssd
sudo rm -rf /var/lib/sss/db/*
sudo systemctl start sssd
```

То же самое можно сделать с помощью команды `cache-remove` утилиты **sssctl** из состава пакета **sssd-tools**:

```
sudo sssctl cache-remove
```

Результат выполнения:

```
SSSD must not be running. Stop SSSD now? (yes/no) [yes] yes
Creating backup of local data...
Removing cache files...
SSSD needs to be running. Start SSSD now? (yes/no) [yes] yes
```

Однако, для отладки **SSSD** на нагруженном сервере рекомендуют использовать специализированную утилиту **sss_cache** из того же пакета **sssd-tools**, с помощью которой можно удалять не весь кэш, а отметить недействительными только отдельные записи, например, по конкретному пользователю, чтобы они были повторно извлечены из каталога при следующем обращении:

```
sudo sss_cache –u admin
```

2.1.5.2. Быстрый кэш (in-memory cache, memcache)

Все процессы **SSSD** (**Монитор**, **Бэкенд**, **Ответчик**), являются однопоточными приложениями и обрабатывают запросы со скоростью одного ядра, поэтому **Ответчик** мог бы стать узким местом и ограничить возможности вертикального масштабирования. В тоже время, из соображений безопасности клиентским библиотекам нельзя давать прямой доступ к локальному кэшу, т.к. в нем содержатся в том числе конфиденциальные данные, например, хэши паролей. Для устранения противоречия был создан дополнительный быстрый кэш, который доступен клиентским библиотекам напрямую, но содержит при этом только общую информацию о пользователях и группах.

Быстрый кэш представляет из себя хэш-таблицы, которые находятся в каталоге

/var/lib/sss/mc/ и отображаются на память (Memory-mapped). Ответчик **NSS** записывает информацию в быстрый кэш и до тех пор, пока эти данные остаются актуальными, клиентской библиотеке не требуется связываться с **SSSD** для их извлечения. Если же запись будет отсутствовать в кэше или ее срок жизни истечет, запрос будет перенаправлен **Ответчику NSS**, который извлечет данные из локального кэша или обратится к контроллеру домена через **Бэкенд**.

По умолчанию время хранения записей в быстром кэше составляет 300 секунд и может быть изменено с помощью параметра `memcache_timeout` в файле *sssd.conf*. Для отключения быстрого кэша нужно установить `memcache_timeout=0`, а для очистки, как и в случае локального кэша, просто удалить файлы и перезапустить службу:

```
sudo systemctl stop sssd
sudo rm -rf /var/lib/sss/mc/*
sudo systemctl start sssd
```

Команда `cache-remove` утилиты **sssctl** не удаляет файлы быстрого кэша, но `sss_cache`, как и в случае локального кэша, позволяет отметить недействительными отдельные записи, например, по конкретному пользователю, чтобы они были повторно извлечены из каталога при следующем обращении.

```
sudo sss_cache –u admin
```

2.1.5.3. Негативный или безрезультатный кэш (negative cache, ncache)

Для уменьшения нагрузки на сервер при обращении к несуществующим объектам каталога, внутри **Ответчика NSS** и ряда других компонентов реализован так называемый негативный или безрезультатный кэш. Этот кэш находится в оперативной памяти и обновляется каждые 15 секунд, изменить эту настройку можно с помощью параметра `entry_negative_timeout` в конфигурационном файле *sssd.conf* Для полной очистки негативного кэша достаточно просто перезапустить службу командой:

```
sudo systemctl restart sssd
```

2.1.5.4. Алгоритм использования кеша (cache lookup)

Служба **SSSD** кэширует пользователей, группы, правила HBAC/SUDO, SSH-ключи, карты монтирования дисков и другую информацию, но вне зависимости от типов объектов поиск

в кэше выполняется очень похожим образом, см. *Упрощенный алгоритм поиска*.

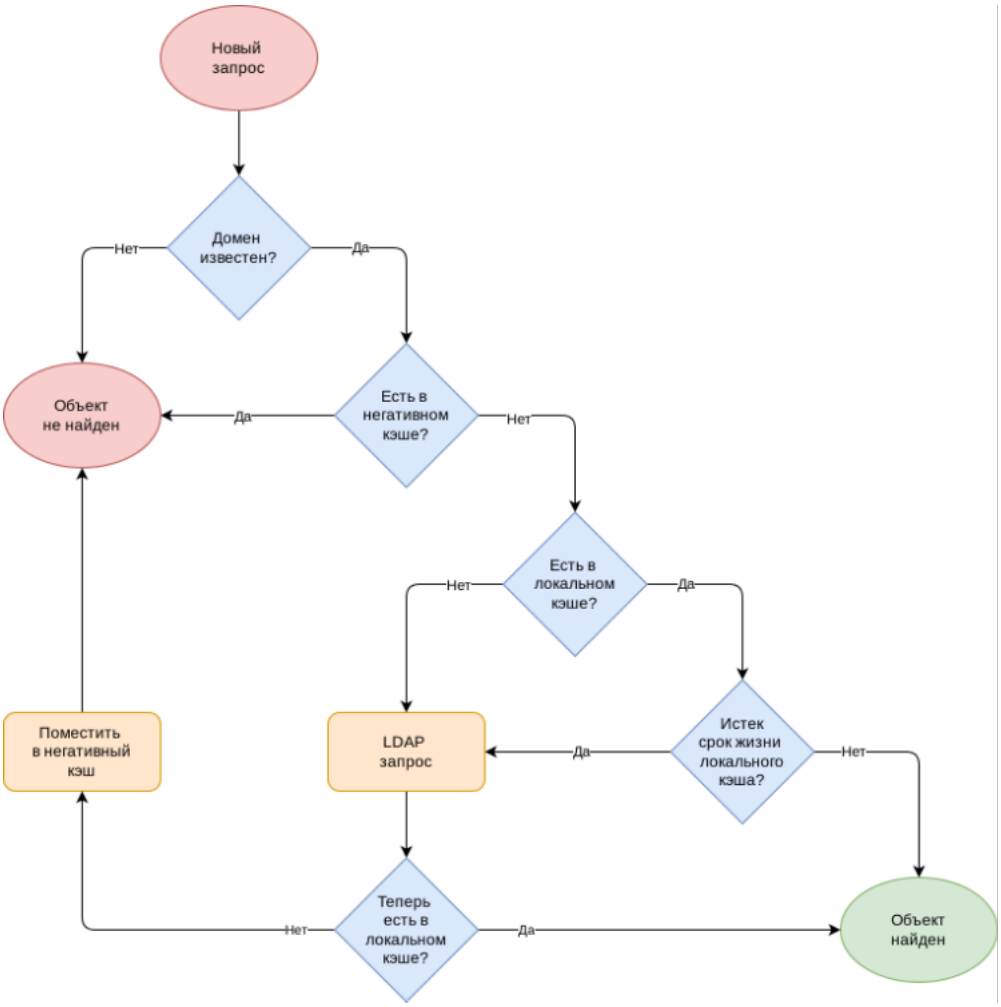


Рисунок 2.4 – Упрощенный алгоритм поиска

В действительности алгоритм немного сложнее и выполняется чуть больше проверок и действий, но приведенной схемы достаточно для получения общих представлений.

Рассмотрим поток данных при поиске информации с использованием кэша, см. *Поток данных при поиске информации о пользователе с использованием информации из кэша*:

- Клиентское приложение вызывает функцию **getpwnam** из библиотеки **glibc**, которая в соответствии настройками из *sswitch.conf* загружает Клиентскую библиотеку *libnss_sss.so.2* и вызывает ее функции, подробнее см. в разделе «Клиентские библиотеки и приложения».
- Клиентская библиотека проверяет, есть ли информация о запрашиваемом объекте в быстром кэше (**memcache**), и только после этого обращается к **Ответчику sssd_nss**.
- **Ответчик** проверяет, есть ли информация о запрашиваемом объекте в локальном кэше, и только после этого обращается к **Бэкенду sssd_be**.

- **Бэкенд** выполняет запрос к LDAP-каталогу, сохраняет информацию в локальный кэш и сообщает **Ответчику** о готовности.
- **Ответчик** повторно обращается к локальному кэшу, извлекает оттуда необходимую информацию, записывает ее в быстрый кеш и передает Клиентской библиотеке в качестве ответа.
- Клиентская библиотека возвращает ответ в функцию **glibc**, на чем поиск завершается.

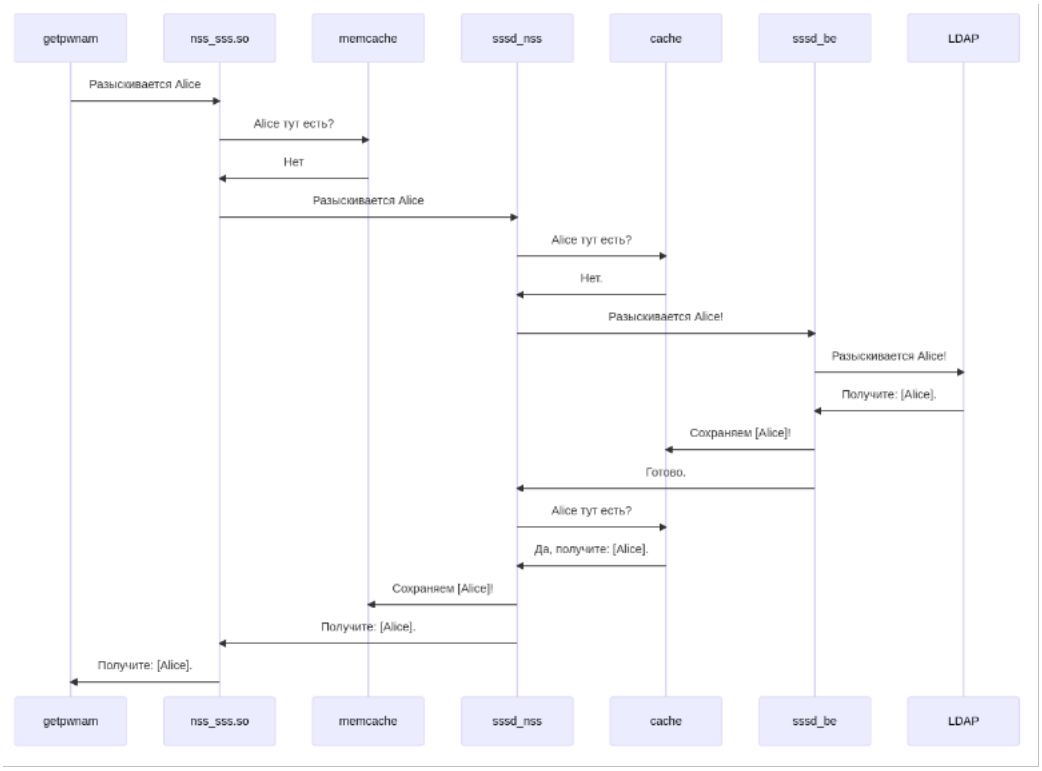


Рисунок 2.5 – Поток данных при поиске информации о пользователе с использованием информации из кэша

2.1.6. Инструменты администрирования

Одним из наиболее полезных приложений для диагностики работы службы **SSSD** является утилита **sssctl** из пакета **sssd-tools**, которая взаимодействует с компонентами **SSSD** напрямую через **SBus**. С ее помощью можно узнать, например, какой контроллер в данный момент обслуживает запросы компьютера:

```
sudo sssctl domain-list
```

Результат команды:

```
ald.company.lan
```

Узнать статус домена можно командой `domain-status` утилиты **sssctl**:

```
sudo sssctl domain-status ald.company.lan
```

Результат выполнения:

```
Online status: Online


Active servers:
IPA: dc-1.ald.company.lan

Discovered IPA servers:
- dc-1.ald.company.lan
- dc-2.ald.company.lan
- dc-3.ald.company.lan
```

С помощью команды `access-report` можно посмотреть HBAC правила, определенные в домене:

```
sudo sssctl access-report ald.company.lan
```

Результат выполнения:

```
2 rules cached

Rule name: allow_all
    User category: all
    Service category: all

Rule name: allow_systemd-user
    User category: all
    Member services: systemd-user
```

С помощью команды `debug-level` можно быстро изменить степень детализации журналирования, которая будет оставаться в силе до перезапуска службы, потому что файл */var/lib/sss/db/config.ldb* пересоздается при запуске службы.

Проверить текущий уровень отладки можно командой:

```
sudo ldbsearch -H /var/lib/sss/db/config.ldb | grep debug | head -n 1
```

Результат выполнения:

```
debug_level: 0x1f7f0
```

Применить новый уровень отладки можно командой:

```
sudo sssctl debug-level 6
```

Проверить новое значение в конфигурации можно командой:

```
sudo ldbsearch -H /var/lib/sss/db/config.ldb | grep debug | head -n 1
```

Результат выполнения:

```
debug_level: 0x07f0
```

2.2. Учетная запись компьютера в домене

У каждого компьютера в домене есть своя собственная учетная запись, с помощью которой он выполняет авторизованные LDAP-запросы к каталогу и проверяет аутентичность пользователей по протоколу **Kerberos V5**. Учетные записи компьютеров хранятся в контейнере `cn=computers,cn=accounts,dc=ald,dc=company,dc=lan`, имя LDAP-записи включает значение атрибута **fqdn**, например, `fqdn=pc-1.ald.company.lan`, а для аутентификации по протоколу Kerberos используется имя принципала в формате `host/pc-1.ald.company.lan@ALD.COMPANY.LAN`.

Билеты службы **SSSD** кэшируются в файле */var/lib/sss/db/ccache_ALD.COMPANY.LAN*, прочитать который можно с помощью утилиты **klist**, используя параметр `-c`:

```
sudo klist -c /var/lib/sss/db/ccache_ALD.COMPANY.LAN
```

Результат выполнения:

```
Ticket cache: FILE:/var/lib/sss/db/ccache_ALD.COMPANY.LAN
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
Default principal: host/dc-1.ald.company.lan@ALD.COMPANY.LAN

Valid starting    Expires    Service principal
10.10.2023 14:40:23 11.10.2023 14:40:23     krbtgt/ALD.COMPANY.LAN@ALD.
↪COMPANY.LAN
10.10.2023 14:40:23 11.10.2023 14:40:23     ldap/dc-1.ald.company.lan@ALD.
↪COMPANY.LAN
```

Пароль учетной записи хоста хранится в файле */etc/krb5.keytab*, поэтому можно быстро проходить аутентификацию и выполнять запросы от имени хоста. Проверка валидности keytab-файла является одной из рекомендаций по устранению неисправностей, если в журналах **SSSD** появится информация о том, что служба не смогла пройти аутентификацию в домене. Такие ситуации могут возникать, например, если компьютер был удален из домена.

Содержимое keytab-файла можно посмотреть с помощью утилиты **klist**, используя параметр `-k`. Если добавить параметр `-e`, то можно будет увидеть, что для одной версии пароля в файле содержится сразу два ключа, полученные с помощью разных алгоритмов хэширования:

```
sudo klist -ke /etc/krb5.keytab
```

Результат выполнения:

```
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
---- --------------------------------------------------------------------
↪-
   1 host/pc-1.ald.company.lan@ALD.COMPANY.LAN (aes256-cts-hmac-sha1-96)
   1 host/pc-1.ald.company.lan@ALD.COMPANY.LAN (aes128-cts-hmac-sha1-96)
```

Для того, чтобы пройти аутентификацию от имени хоста, достаточно использовать команду **kinit** с параметром `-k`, но если нужно задать путь к keytab-файлу в явном виде, то можно это сделать, используя дополнительный параметр `-t`. Если выполнить команду `ldapsearch`, то можно будет увидеть наличие сервисного билета для аутентификации в службе **LDAP**:

```
sudo kinit -kt /etc/krb5.keytab
ldapsearch > /dev/null
```

(продолжение на следующей странице)

```
klist
```

Результат выполнения:

```
Ticket cache: KEYRING:persistent:1421600000:krb_ccache_zgnOUA8
Default principal: host/dc-1.ald.company.lan@ALD.COMPANY.LAN
Valid starting Expires Service principal
10.10.2023 14:43:06 11.10.2023 14:43:06     ldap/dc-1.ald.company.lan@ALD.
 ↪COMPANY.LAN
10.10.2023 14:43:06 11.10.2023 14:43:06     krbtgt/ALD.COMPANY.LAN@ALD.
 ↪COMPANY.LAN
```

Для хэширования паролей используются устойчивые к взлому алгоритмы, и перед этим к паролю добавляется основное имя пользователя в качестве соли для того, чтобы исключить возможность перебора по таблицам хэшей, но даже такие меры не защищают от всех видов атак, поэтому пароли хостов рекомендуется время от времени менять, например, компания Microsoft предлагает делать это не реже одного раза в 30 дней.

Чтобы установить хосту новый пароль и выгрузить его в keytab-файл, можно воспользоваться утилитой **ipa-getkeytab**. Важно обратить внимание, что после смены пароля команда **klist** в колонке **KVNO** показывает новую версию ключей.

```
sudo rm -rf /etc/krb5.keytab
sudo ipa-getkeytab -p host/pc-1.ald.company.lan -k /etc/krb5.keytab -s dc-1.
 ↪ald.company.lan -D uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan -
 ↪W -P
```

Результат выполнения:

```
Введите пароль LDAP: **********
Новый пароль учётной записи: **********
Проверка пароля учётной записи: **********
Таблица ключей успешно получена и сохранена в: /etc/krb5.keytab
```

Проверить новый keytab-файл можно командой:

```
sudo klist -ke /etc/krb5.keytab
```

Результат выполнения:

```
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
---- --------------------------------------------------------------------
↪-
   2 host/pc-1.ald.company.lan@ALD.COMPANY.LAN (aes256-cts-hmac-sha1-96)
   2 host/pc-1.ald.company.lan@ALD.COMPANY.LAN (aes128-cts-hmac-sha1-96)
```

Поясним параметры вызова утилиты **ipa-getkeytab**:

- `-p` — имя учетной записи, для которой меняется пароль
- `-k` — имя keytab-файла, в который добавляются ключи
- `-s` — адрес контроллера домена, через который следует выполнить запрос
- `-D` — имя привилегированной учетной записи, от которой вносятся изменения в каталог.
- `-W` — ключ, указывающий на то, что пароль привилегированной учетной записи будет предоставлен в интерактивном режиме. Для того, чтобы задать пароль прямо в командной строке, используйте ключ `-w`, но делать это крайне не рекомендуется, т.к. значение этого параметра будет видно в выводе команды `ps` и попадет в историю команд.
- `-P` — ключ, указывающий на то, что пароль хоста будет введен вручную. Если этот параметр не указывать, пароль будет сгенерирован автоматически.

Если параметр `-D` не будет указан, то утилита **ipa-getkeytab** воспользуется учетными данными текущего Kerberos-пользователя из связки ключей. Это позволяет сменить пароль для компьютера, используя учетные данные самого хоста из keytab-файла:

```
sudo kinit -kt /etc/krb5.keytab
sudo ipa-getkeytab -p host/pc-1.ald.company.lan -k /etc/krb5.keytab
sudo klist -ke /etc/krb5.keytab
```

Результат выполнения:

```
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
---- --------------------------------------------------------------------
↪-
   2 host/pc-1.ald.company.lan@ALD.COMPANY.LAN (aes256-cts-hmac-sha1-96)
   2 host/pc-1.ald.company.lan@ALD.COMPANY.LAN (aes128-cts-hmac-sha1-96)
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
  3 host/pc-1.ald.company.lan@ALD.COMPANY.LAN (aes256-cts-hmac-sha1-96)
  3 host/pc-1.ald.company.lan@ALD.COMPANY.LAN (aes128-cts-hmac-sha1-96)
```

2.3. Способы аутентификации в домене

Служба каталога ALD Pro построена на базе **FreeIPA** и поддерживает три вида аутентификации: **LDAP Bind**, **Kerberos** и частично **NTLM**.

2.3.1. Аутентификация по протоколу LDAP

Простая аутентификация или привязка (**bind**) является самым распространенным, но при этом не самым безопасным способом аутентификации, т.к. пароль передается на сервер открытым текстом.

Поэтому во избежание разглашения учетных данных при выполнении авторизованных LDAP-запросов с использованием простой аутентификации рекомендуется всегда использовать шифрованный протокол **LDAPS** или включать **StartTLS**:

```
ldapsearch -H ldaps://dc-1.ald.company.lan -D 'uid=admin,cn=users,cn=accounts,
↪dc=ald,dc=company,dc=lan' -W
```

А также командой с ключом `-ZZ`:

```
ldapsearch -ZZ -H ldap://dc-1.ald.company.lan -D 'uid=admin,cn=users,
↪cn=accounts,dc=ald,dc=company,dc=lan' -W
```

Для лучшего понимания угрозы приведен пример, как делать категорически запрещается:

```
ldapsearch -H ldap://dc-1.ald.company.lan -D 'uid=admin,cn=users,cn=accounts,
↪dc=ald,dc=company,dc=lan' -W
```

Из программы **Wireshark** можно увидеть, см. *Пароль пользователя открытым текстом в запросе bindRequest*, что злоумышленник, у которого будет доступ к просмотру сетевых пакетов, может легко извлечь пароль «**AstraLinux_172**» из запроса, если канал связи не будет зашифрован:

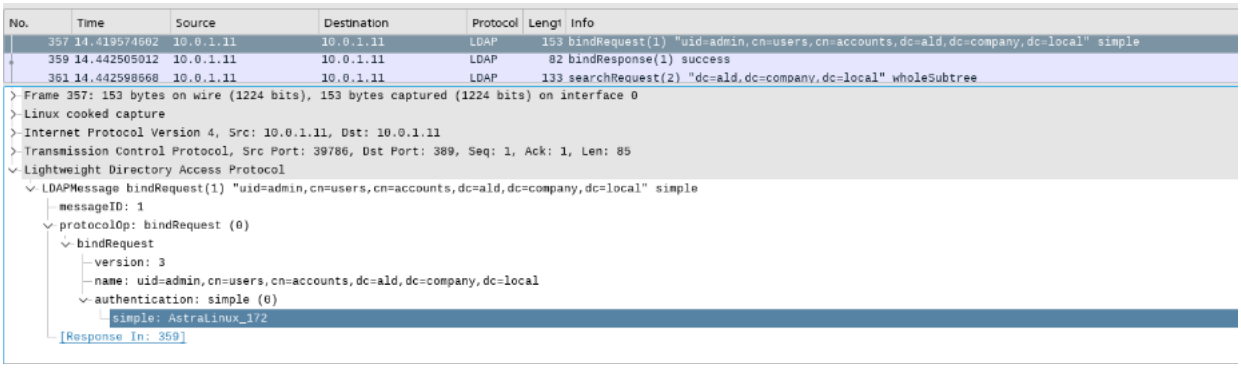


Рисунок 2.6 – Пароль пользователя открытым текстом в запросе bindRequest

Для проведения простой аутентификации LDAP-каталог хранит хэш пароля в атрибуте `userPassword`. Алгоритм проверки аутентичности работает следующим образом:

- Пользователь передает на сервер свое имя и пароль в открытом виде.
- Сервер извлекает из каталога хэш пароля для указанного пользователя.
- Пароль, полученный в запросе на аутентификацию, хэшируется тем же алгоритмом и сравнивается со значением, полученным из каталога. Если значения совпали, аутентификация считается успешной.

Хэширование паролей выполняется автоматически при изменении пароля, по умолчанию используется устойчивый к взлому алгоритм PBKDF2-SHA256:

```
ldapsearch -H ldaps://dc-1.ald.company.lan -o ldif-wrap=no -D 'cn=Directory
↪Manager' -W -b 'uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan' |
↪grep 'userPassword::' | cut -d" " -f2 | base64 -d
```

Где:

- опция `-o ldif-wrap=no` - выводит текст без переноса в одну строку, если она не помещается в 80 символов, что полезно использовать в **bash** командах и скриптах;
- командой `grep` мы делаем поиск строки с полем `userPassword::` и два символа «**:**» означают что строка закодирована в кодировке **base64**;
- командой `cut` отрезаем по символу пробел значение пароля во второй колонке;
- командой `base64 -d` значение из **base64** декодируем в текст.

Результат выполнения, декодированный из **base64** пароль пользователя admin:

```
{PBKDF2-SHA256}AAAIAPiA62CPFChuE0ZU908GI9DjhCb3fXPR4mWPH9/0molxZd7/
↪nWEGglROvy6WCXqri61+Wi76wyVSop6igG2JQR2RyHSI7Fxarm7Ur/2Fri70hw4kBl09Ih...
```

Если включить режим миграции пользователей, то при создании новых учетных записей в атрибут `userPassword` можно будет записать хэш пароля, при этом поддерживается целый ряд алгоритмов: CRYPT, CRYPT-MD5, CRYPT-SHA256, CRYPT-SHA512, MD5, SHA, SHA256, SHA384, SHA512, SMD5, SSHA, SSHA256, SSHA384, SSHA512.

```
sudo ipa config-mod --enable-migration=true
sudo ipa user-add userName --setattr userPassword='{TYPE}HASH'
```

Для завершения миграции пользователю потребуется один раз выполнить простую LDAP-аутентификацию, чтобы сервер смог сгенерировать недостающие ключи. Для этого на сервере существует даже специальная страница миграции, доступная по адресу https://dc-1.ald.company.lan/ipa/migration/, см. *Страница LDAP-аутентификации для завершения миграции пользователей*.

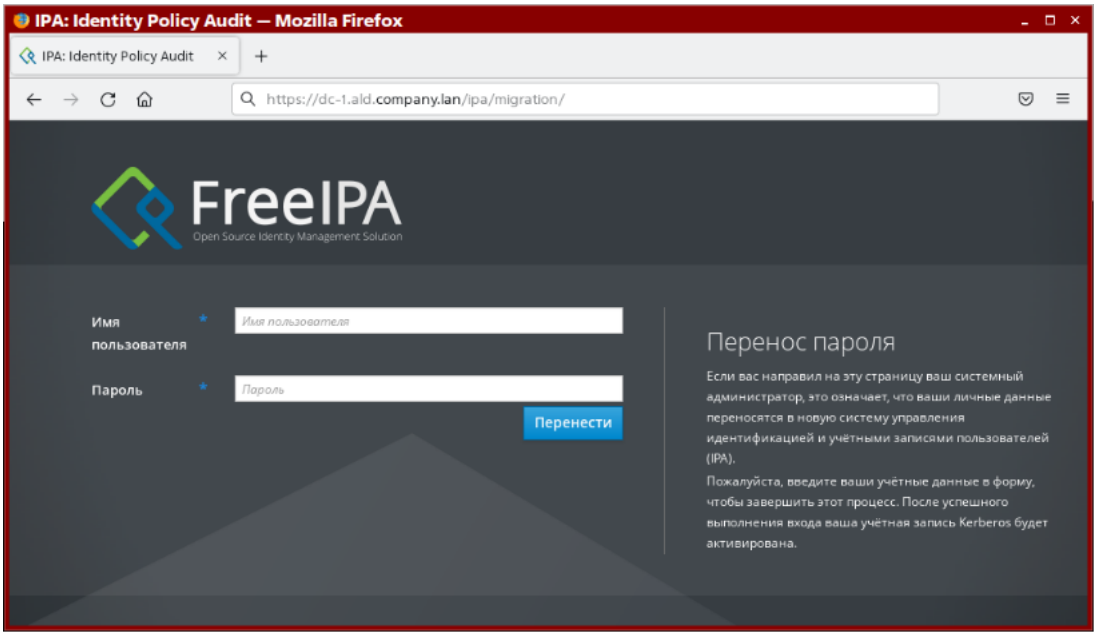


Рисунок 2.7 – Страница LDAP-аутентификации для завершения миграции пользователей

2.3.2. Аутентификация по протоколу Kerberos

Основным протоколом аутентификации в домене является Kerberos V5. Три участника процедуры аутентификации:

- **Клиент** (**Client**) — субъект, желающий получить доступ к ресурсу.
- **Сервер приложения** (Application Server, **AP**) — служба, к ресурсу которой **клиент** хочет получить доступ.

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

Протокол аутентификации был разработан для эксплуатации в незащищенных компьютерных сетях, когда сетевые пакеты могут быть подслушаны и изменены злоумышленником. Рассмотрим процесс аутентификации в упрощенном виде, см. *Начало аутентификации пользователя Алисы*, опуская несущественные детали, такие как фаза предварительной аутентификации, использование nonce и др.

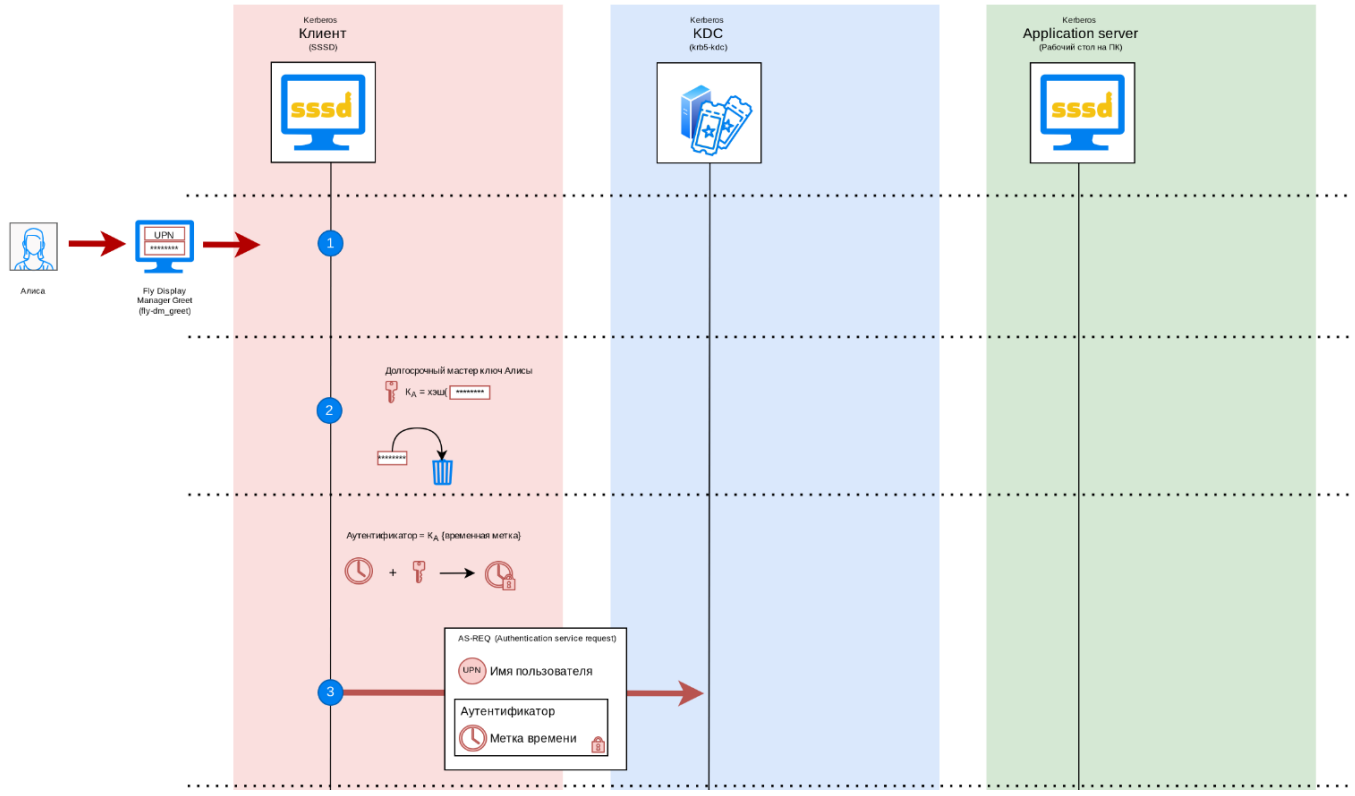


Рисунок 2.8 – Начало аутентификации пользователя Алисы

Шаг (1) Пользователь Алиса через приложение графического входа (Fly Display Manager Greet) передает стеку модулей аутентификации (Pluggable Authentication Modules, **PAM**) логин и пароль в открытом виде. За аутентификацию в домене отвечает модуль */usr/lib/x86_64-linux-gnu/security/pam_sss.so*, см. файл */etc/pam.d/common-auth*:

```
cat /etc/pam.d/common-auth
```

Результат выполнения:

```
...
auth [success=1 default=ignore] pam_sss.so use_first_pass
...
```

Шаг (2) Библиотека **libpam** загружает Клиентскую библиотеку *pam_sss.so*, через функции которой обращается к **Ответчику** */usr/lib/x86_64-linux-gnu/sssd/sssd_pam*. **Ответчик** обращается к **Бэкенду**, который порождает процесс **krb5_child** для аутентификации в домене по протоколу **Kerberos V5**.

Керберос клиент рассчитывает долгосрочный мастер-ключ Алисы (UPN long-term key или Master key) и может удалить из памяти компьютера пароль в открытом виде для повышения устойчивости системы к взлому. Хэш является соленым, к паролю добавляется основное имя принципала, включающее логин пользователя и реалм домена. В соответствии с политикой Kerberos для хэширования может использоваться алгоритм **AES128_CTS_HMAC_SHA1_96** или **AES256_CTS_HMAC_SHA1_96**.

Шаг (3) Клиент отправляет запрос службе аутентификации Центра распределения ключей (Key Distribution Center, **KDC**). В четвертой версии протокола на этом шаге никакие учетные данные не требовались, т.к. ответ будет зашифрован долгосрочным ключом пользователя, и способность расшифровать ответ является подтверждением того, что пользователь является тем, за кого себя выдает. Но с пятой версии протокола сервер отклонит запрос и потребует предварительную аутентификацию. В качестве аутентификатора выступает метка времени, зашифрованная симметричным алгоритмом с помощью долгосрочного ключа клиента. Такая проверка существенно затрудняет кибератаки, так как лишает злоумышленника возможности запросить **TGT**-билет на любого пользователя в системе.

Шаг (4) KDC расшифровывает аутентификатор, используя хэш пароля Алисы из LDAP-каталога, см. *Обработка запроса на стороне KDC, создание и отправка TGT-билета*. Ключи для аутентификации по протоколу Kerberos хранятся в атрибуте **krbPrincipalKey**, который представляет из себя бинарный объект, зашифрованный мастер-ключом **KDC** (**krbMKey**). Если процедура расшифровки завершилась успешно и полученная временная метка расходится со временем сервера не более, чем на 5 минут, то считается, что предварительная аутентификация пройдена успешно. По этой причине для корректной работы протокола важна синхронизация времени между всеми участниками.

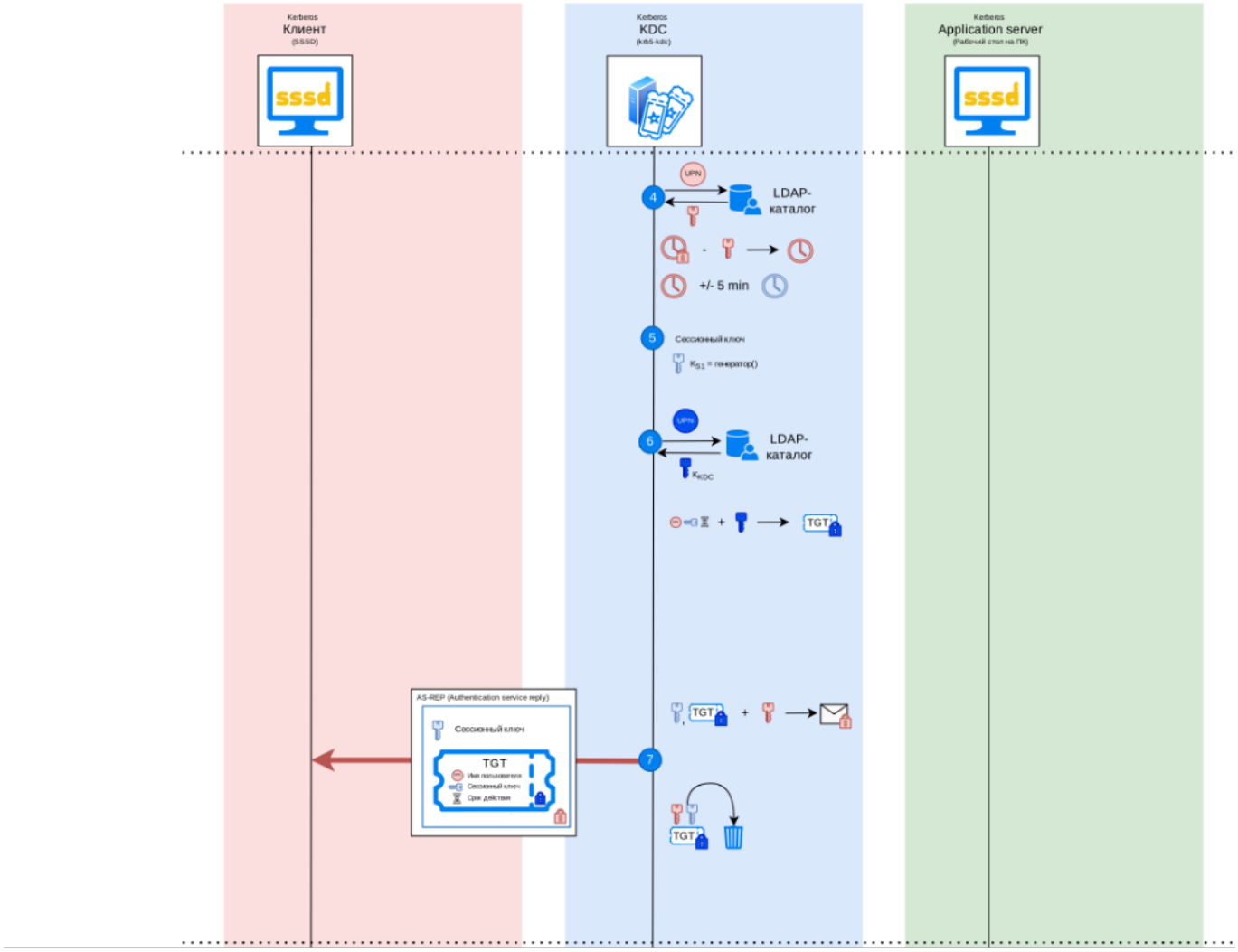


Рисунок 2.9 – Обработка запроса на стороне KDC, создание и отправка TGT-билета

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

Шаг (6) Несмотря на то, что сессионный ключ был сгенерирован сервером, в домене может быть несколько контроллеров, и **Клиент** вправе обратиться с последующим запросом к любому из них. Учитывая случайный характер сессионного ключа, другой контроллер домена не сможет рассчитать его математически, поэтому сессионный ключ следует передать ему в явном виде. По протоколу Kerberos ответственность за передачу сессионного ключа возлагается на **клиента**, для чего ему выдается зашифрованный билет на выдачу билетов (Ticket-granting ticket, **TGT**), который он должен предъявлять в **KDC** при последующих обращениях.

Внутри **TGT**-билета содержится имя пользователя, сессионный ключ и информация по сроку действия билета. Билет зашифрован симметричным алгоритмом с помощью

долгосрочного ключа **KDC** (хэш пароля служебной учетной записи **KRBTGT**, Key Distribution Center Service Account), поэтому расшифровать его можно только на контроллере, и подделать билет на стороне **Клиента** невозможно.

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

Долгосрочный ключ клиента, сессионный ключ и билет могут быть удалены из памяти сервера за ненадобностью для повышения безопасности системы.

Шаг (8) Клиент расшифровывает сессионный ключ и **TGT** билет своим долгосрочным ключом, см. *Запрос от клиента на получение сервисного билета с помощью TGT-билета*. Возможность использования этих данных в последующих запросах означает, что **Клиент** является тем, за кого себя выдает. Если результат расшифровки окажется недействительным, значит ответ получен от подставного Центра распределения ключей. Долгосрочный ключ может быть удален из памяти компьютера за ненадобностью для повышения безопасности системы.

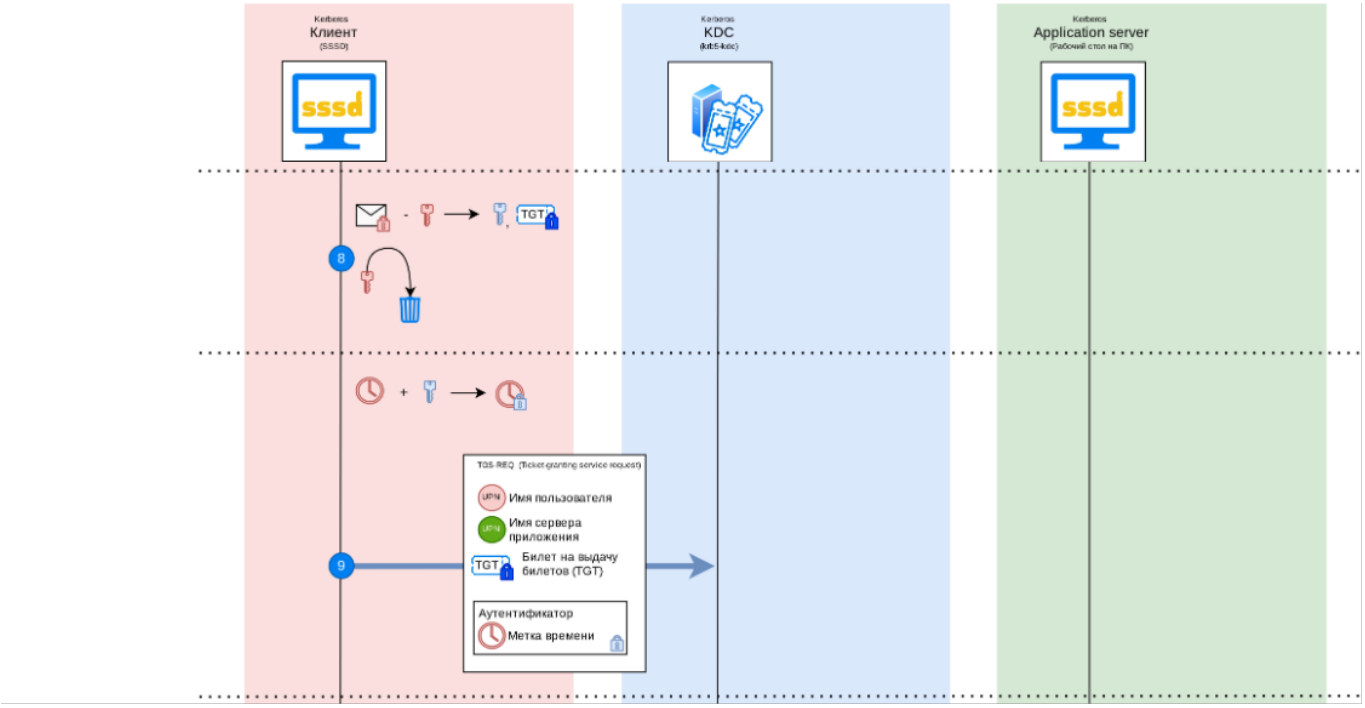


Рисунок 2.10 – Запрос от клиента на получение сервисного билета с помощью TGT-билета

Шаг (9) Процесс **krb5_child** сохраняет **TGT** билет в связке ключей Linux и передает результаты по цепочке **Бэкенд** — **Ответчик** — **Клиентская библиотека**, после чего **Клиентская библиотека** отправляет запрос на получение сервисного билета на доступ к

серверу приложения, в котором содержится имя пользователя (**user principal name**), имя сервера приложения (**service principal name**), билет на выдачу билетов (**TGT**) и аутентификатор. В качестве аутентификатора выступает метка времени, зашифрованная симметричным алгоритмом с помощью сессионного ключа **S1**. В качестве имени сервиса при входе в компьютер выступает **host/pc-fqdn**.

На этом шаге **TGT** билет закодирован только долгосрочным ключом **KDC**, но этого достаточно, чтобы злоумышленник, перехвативший сообщение, не смог подделать запросы, т.к. он не располагает сессионным ключом **S1**.

Шаг (10) KDC расшифровывает информацию из **TGT** билета, используя долгосрочный ключ **KDC** из LDAP-каталога, после чего ему становится доступна следующая информация: имя пользователя, сессионный ключ **S1** и срок действия билета, см. *Обработка запроса на сессионный ключ и выдача сессионного ключа по запросу клиента*.

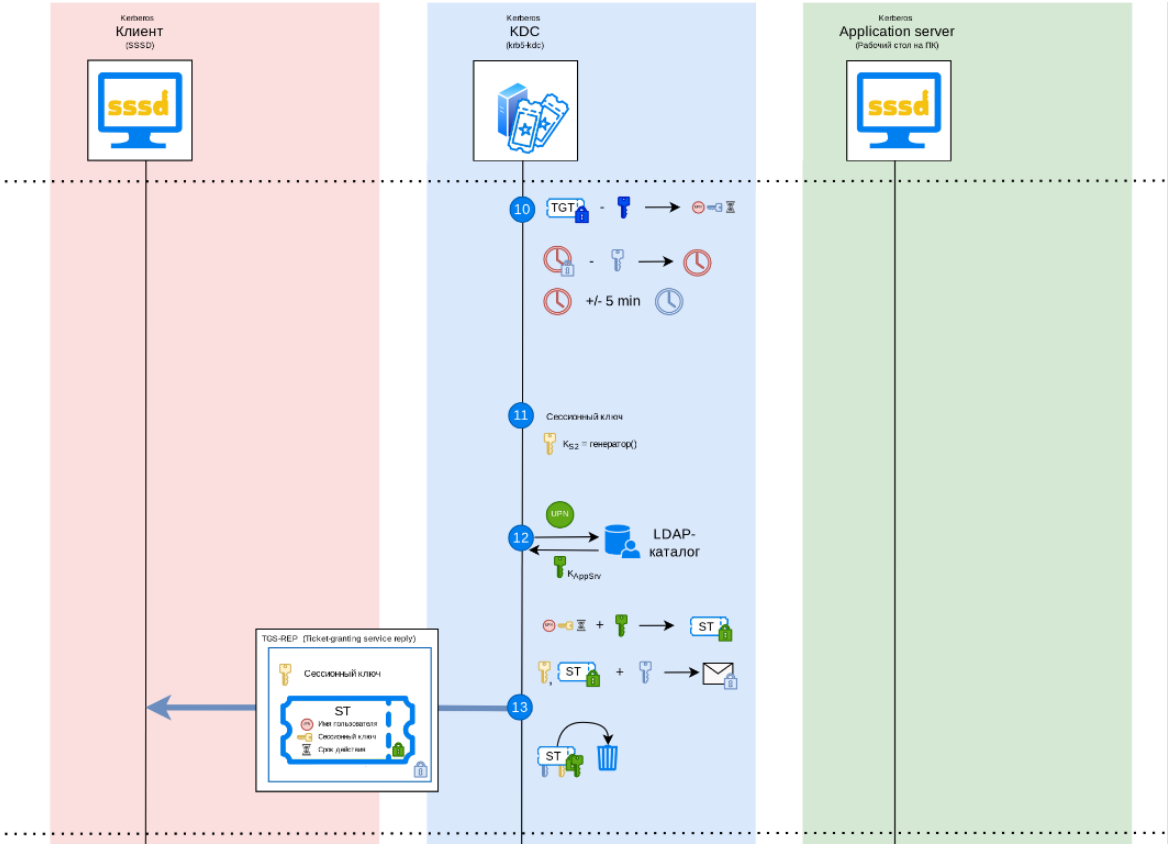


Рисунок 2.11 – Обработка запроса на сессионный ключ и выдача сессионного ключа по запросу клиента

Сервер расшифровывает аутентификатор, используя сессионный ключ из **TGT** билета, и, если полученное значение расходится со временем сервера не более, чем на 5 минут, то считается, что аутентификация пройдена успешно.

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

Шаг (12) Ключ **S2** был сгенерирован сервером **KDC** и его следует передать Серверу приложения. По протоколу Kerberos ответственность за передачу ключа возлагается на клиента, для чего ему выдается зашифрованный сервисный билет (Service ticket, **ST**), который он должен предъявлять серверу приложения.

Внутри **ST**-билета содержится имя пользователя, сессионный ключ и информация по сроку действия билета. Билет зашифрован симметричным алгоритмом с помощью долгосрочного ключа Сервера приложения, поэтому расшифровать его сможет только сервер приложения, и подделать билет на стороне **Клиента** невозможно.

У приложения может быть отдельная учетная запись, но может использоваться и учетная запись компьютера, на котором это приложение работает. В нашем случае это пароль компьютера, в который мы хотим войти.

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

Шаг (14) Клиент расшифровывает сессионный ключ **S2** и сервисный билет **ST** известным ему сессионным ключом **S1**. Возможность использования этих данных в последующих запросах означает, что **Клиент** является тем, за кого себя выдает. Если результат расшифровки окажется недействительным, значит ответ получен от подставного Центра распределения ключей.

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

На этом шаге **ST** билет закодирован только долгосрочным ключом сервера приложения, но этого достаточно, чтобы злоумышленник, перехвативший сообщение, не смог подделать запросы.

Шаг (16) Сервер приложения, в роли которого выступает служба **SSSD** на пользовательском компьютере, извлекает хэш пароля из файла */etc/krb5.keytab* для расшифровки запроса. Используя этот долгосрочный ключ, служба **SSSD** может расшифровать информацию из сервисного билета (**ST**), после чего ей становится доступна следующая информация: имя пользователя, сессионный ключ **S2** и срок

действия билета. **SSSD** расшифровывает аутентификатор, используя сессионный ключ **S2** из сервисного билета, и, если полученное значение расходится со временем компьютера не более, чем на 5 минут, то считается, что аутентификация пройдена успешно (см. *Запроса клиента к службе с помощью сервисного ключа*).

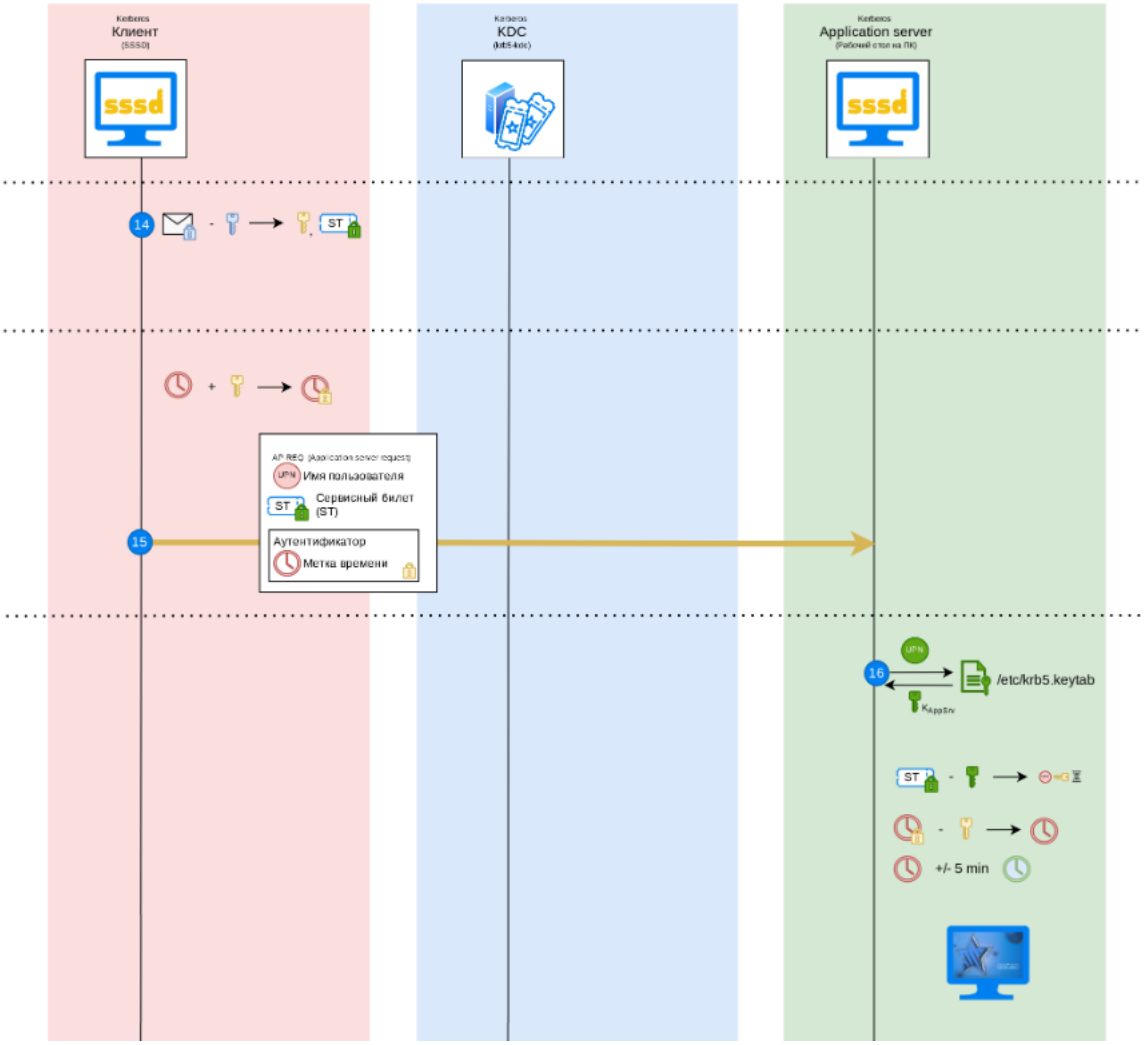


Рисунок 2.12 – Запроса клиента к службе с помощью сервисного ключа

Получив подтверждение, что вход в компьютер хочет выполнить действительно Алиса, приложение **Display Manager** запускает рабочий стол (Fly Windows Manager, **fly-wm**) от имени этого пользователя.

Сервисный билет на доступ к хосту более не требуется, поэтому он не сохраняется в связке ключей, и вы не увидите его в выводе команды **klist**, но на контроллере в журнале */var/log/auth.log* вы можете найти подтверждение, что такой билет запрашивался и был предоставлен рабочей станции.

2.3.3. Аутентификация по протоколу NTLM

Служба каталога **FreeIPA** тесно интегрирована с файловым сервером **Samba**, в котором реализована поддержка **NTLM**-протокола для возможности аутентификации пользователей по логину/паролю, например, если подключение выполняется не по доменному имени сервера, а по его IP адресу. Для этого у пользователей в каталоге есть атрибут `ipaNTHash`, который обновляется плагином **ipa_pwd_extop** каждый раз при смене пароля.

Рассмотрим поток данных при аутентификации по протоколу **NTLM** в упрощенном виде, см. *Поток данных при NTLM-аутентификации*:

- **Клиент** обращается к **Сервису** с запросом на аутентификацию (1) и получает в ответ случайное число длиной 8 байт, которое ему нужно подписать, используя свой пароль, для подтверждения аутентичности (2).
- **Клиент** подписывает сообщение и передает его **Сервису** (3), который пересылает подпись вместе с исходным сообщением на **Контроллер Домена** (4).
- **Контроллер** проверяет подпись и возвращает **PAC** сертификат, если проверка аутентичности пройдена успешно (5).

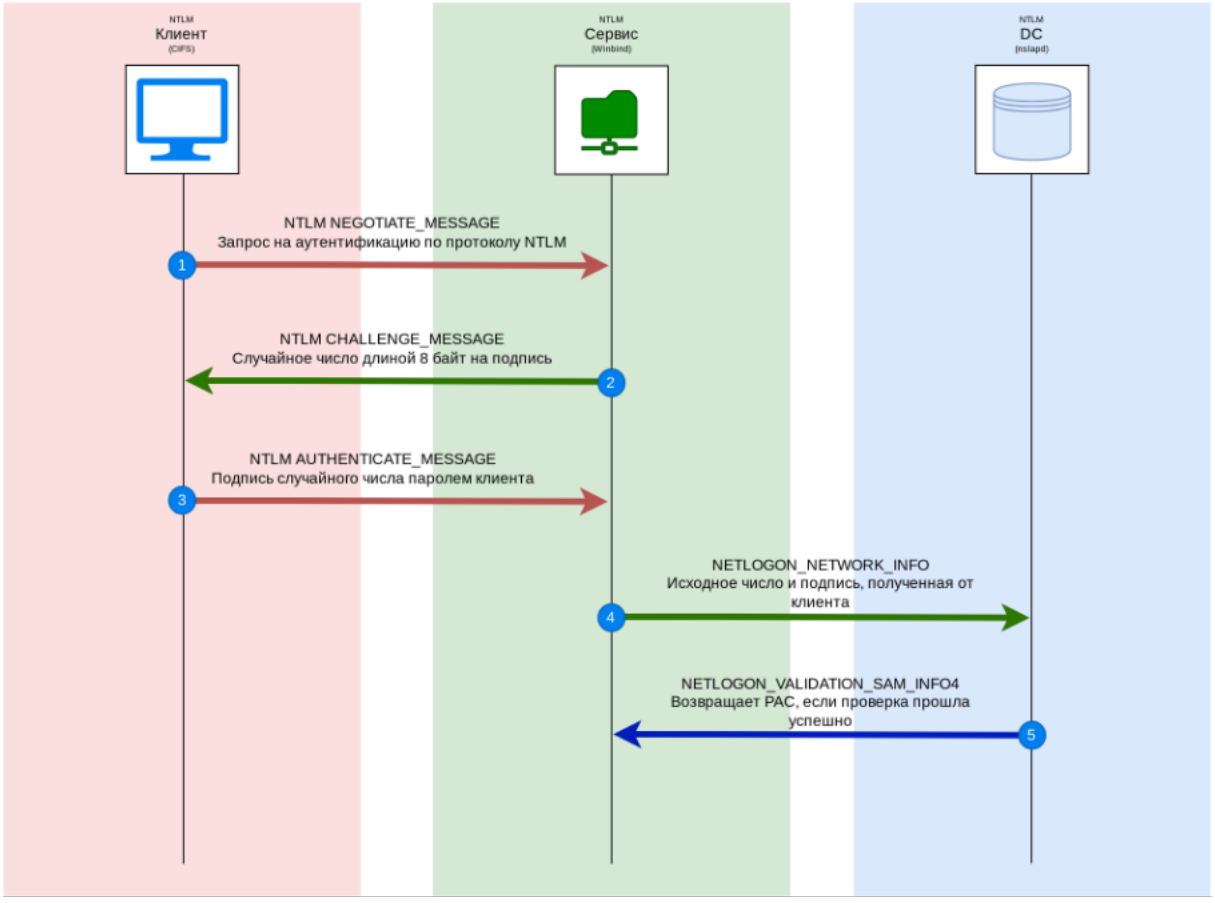


Рисунок 2.13 – Поток данных при NTLM-аутентификации

Интеграция **Samba** реализует представленную схему не полностью: служба **Winbind**, которая отвечает за **NTLM** аутентификацию на стороне **Samba**, не передает контроллеру домена информацию для проверки аутентичности пользователя, а выполняет ее самостоятельно, получая значение атрибута `ipaNTHash` из каталога напрямую через модуль **ipasam**. Доступ к этому атрибуту предоставляется учетной записи файлового сервера через назначение роли **CIFS server**. Роль по умолчанию не используется. Необходимо назначить ее вручную через интерфейс **FreeIPA**.

Указанный способ интеграции допустим, если **Samba** устанавливается на контроллер домена, но создает дополнительную точку уязвимости, если **Samba** используется отдельно, как сервер общего доступа к файлам. Учитывая вышеизложенное, ИТ-директорам нужно либо отключать возможность **NTLM**-аутентификации в домене, либо делегировать управление файловыми серверами тем же администраторам, кто управляет контроллерами домена.

2.4. Безопасный обмен данными с применением SSL/TLS

Доменный компьютер взаимодействует с подсистемами ALD Pro по разным протоколам, некоторые из которых используют шифрование:

- Доступ к каталогу по протоколам **LDAP+StartTLS** (**TCP/389**) и **LDAPS** (**TCP/636**) со стороны службы **SSSD** и с помощью инструментов пакета **ldap-utils**.
- Доступ к веб-интерфейсам контроллера домена по протоколу **HTTPS** (**TCP/443**) с помощью браузера и к **REST API** с помощью утилиты автоматизации **ipa**.
- Доступ к удаленному рабочему столу доменного компьютера с портала управления ALD Pro по протоколу **VNC** через **HTTPS** (**TCP/6080** - **TCP/608x**).
- Аутентификация с использованием расширения **PKINIT** по протоколу **Kerberos** (**TCP/88**) использует **X.509** сертификаты для взаимной аутентификации центра распределения ключей и клиента, но не является примером **SSL**-протокола.

Сертификаты применяются также для доступа к **PostgreSQL** (**TCP/5432**), взаимодействия со службой печати по протоколу **IPP** (**TCP/631**), а до версии 2.0.0 использовалось **REST API** системы конфигурирования **SaltStack** (**TCP/8000**), но все эти примеры не представляют интереса в виду локального характера сетевого взаимодействия.

2.4.1. Механизм защиты данных по протоколу SSL

Протокол **SSL** (Secure Sockets Layer, уровень защищенных сокетов) в его текущей реализации **TLS** (Transport Layer Security, безопасность транспортного уровня) обеспечивает быстрый и безопасный обмен данными между клиентом и сервером за счет сочетания симметричных и асимметричных алгоритмов шифрования: медленные асимметричные алгоритмы используются только на фазе рукопожатия для того, чтобы договориться о параметрах шифрования и безопасно обменяться сессионным ключом, а непосредственно обмен данными происходит уже с применением быстрых симметричных алгоритмов.

Разница между этими алгоритмами заключается в том, что симметричные алгоритмы позволяют расшифровать данные тем же ключом, с помощью которого они были зашифрованы, просто выполняя те же действия в обратном порядке, а в асимметричных алгоритмах используется пара взаимосвязанных ключей, поэтому данные, зашифрованные одним из ключей, могут быть расшифрованы только вторым ключом из той же пары.

Суть работы асимметричных алгоритмов можно продемонстрировать на примере из жизни, см. *Иллюстрация идеи асимметричного шифрования на примере использования сейфа с самозакрывающимся механизмом*.

Представьте, что для установления безопасного канала связи нужно обменяться с второй стороной общим кодовым словом. Для этого через службу доставки ей пересылается открытый сейф с самозакрывающимся механизмом, оставляя ключ у себя. Вторая сторона должна будет поместить в этот сейф записку с кодовым словом, защелкнуть замок и переслать сейф обратно. Не взламывая замок, открыть этот сейф можно будет только на вашей стороне, т.к. ключ есть только у вас.

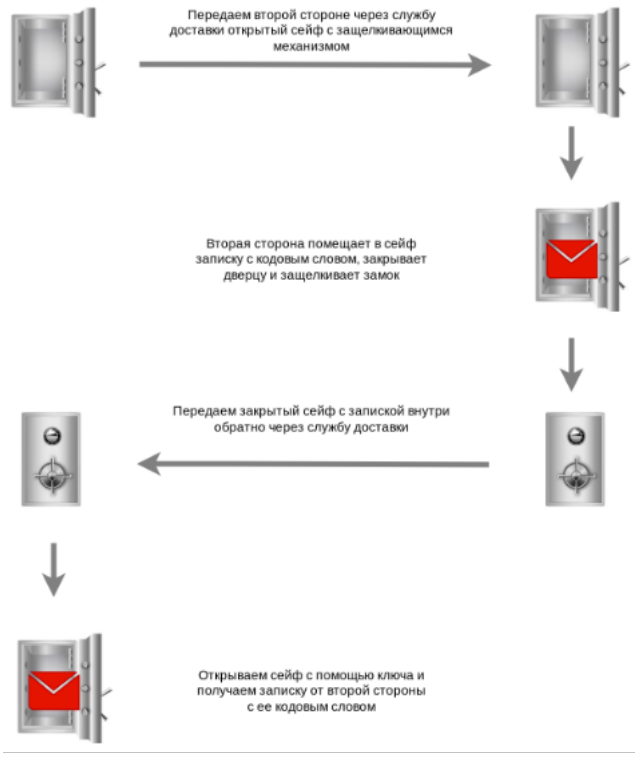


Рисунок 2.14 – Иллюстрация идеи асимметричного шифрования на примере использования сейфа с самозакрывающимся механизмом

Изначально протокол **SSL** разрабатывался для **HTTP**, но его универсальный **TCP**-подобный интерфейс позволил создать расширения и других транспортных протоколов прикладного уровня, например, **LDAPS**, **FTPS**, **SMTPS**, **IMAPS** и др. В качестве примера рассматривается открытие веб-страницы по **HTTPS**, см. *Установление безопасного HTTPS-соединения*.

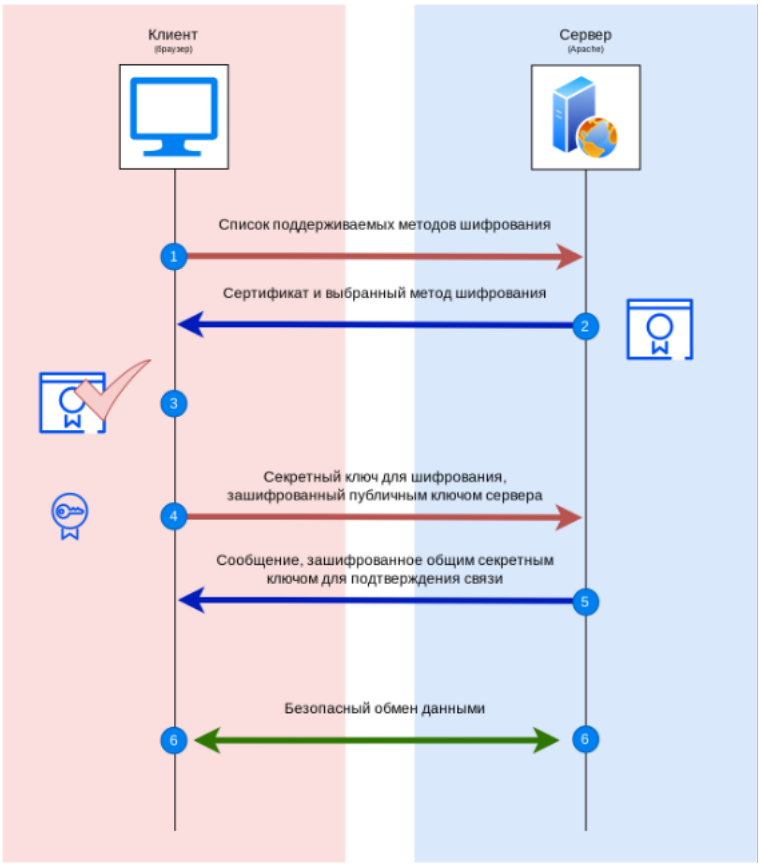


Рисунок 2.15 – Установление безопасного HTTPS-соединения

Шаг (1) Когда пользователь переходит по **https**-ссылке, браузер выполняет подключение к **веб-серверу** на **TCP/443** порт и передает список поддерживаемых методов шифрования для установления безопасного соединения.

Шаг (2) Веб-сервер выбирает метод шифрования и передает **клиенту** свой **SSL**-сертификат, который содержит публичный ключ и цифровую подпись для этого ключа. Вернее, он передает не один сертификат, а всю цепочку до корневого сертификата включительно.

Шаг (3) Клиент проверяет валидность цифровой подписи по своей базе доверенных корневых сертификатов, используя алгоритмы асимметричного шифрования. Также **клиент** проверяет подлинность **сервера**, сопоставляя имя, по которому обращается с именем, указанным внутри сертификата. Если подпись не пройдет проверку, то пользователь получит сообщение о небезопасности соединения ввиду возможности атак посредника (Man in the middle, **MITM**).

Шаг (4) Клиент генерирует случайный ключ и шифрует его асимметричным алгоритмом - публичным ключом **сервера** для безопасной передачи данных по сети.

Шаг (5) Сервер передает **клиенту** сообщение, зашифрованное общим ключом,

подтверждающее возможность начала безопасного обмена данными.

Шаг (6) Клиент и **сервер** выполняют обмен данными по защищенному каналу связи.

2.4.2. Доступ к каталогу по протоколам LDAP+StartTLS и LDAPS

Служба **SSSD** получает данные из каталога по протоколу **LDAP** (**TCP/389**) с использованием расширения **StartTLS**, которое позволяет инициировать шифрованный обмен данными внутри уже установленного **TCP**-соединения вместо открытия нового соединения на отдельном порту.

Администратор может проверить, что порт **TCP/389** действительно защищен шифрованием, и получить цепочку сертификатов с помощью утилиты **openssl**. Первый сертификат выписан на конкретный FQDN контроллера домена, а второй соответствует корневому сертификату домена.

```
echo Q | openssl s_client -starttls ldap -showcerts dc-1.ald.company.lan:389
```

Результат выполнения:

```
CONNECTED(00000003)
depth=1 CN = CA Signing Certificate
verify return:1
depth=0 CN = dc-1.ald.company.lan
verify return:1
---
Certificate chain
0 s:CN = dc-1.ald.company.lan
i:CN = CA Signing Certificate
1 s:CN = CA Signing Certificate
i:CN = CA Signing Certificate
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDxjCCAq6gAwIBAgIUZ4JathCvRrV6v+Aoi4kUNScViBswDQYJKoZIhvcN
AQEL
BQAwITEfMB0GA1UEAwwWQ0EgU2lnbmluZyBDZXJ0aWZpY2F0ZTAeFw0y
MjExMTYx
NzM4MjVaFw0zMjExMTMxNzM4MjVaMCExHzAdBgNVBAMMFmRjLTEuY
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
WxkLmNvbXBh
...
-----BEGIN CERTIFICATE-----
MIIDIzCCAgugAwIBAgIUULQd6OzgJ/ik7wJvV0gd6kUIFKAwDQYJKoZIhvcN
AQEL
BQAwITEfMB0GA1UEAwwWQ0EgU2lnbmluZyBDZXJ0aWZpY2F0ZTAeFw0y
MjExMTYx
NzM4MjVaFw00MjExMTExNzM4MjVaMCExHzAdBgNVBAMMFkNBIFNpZ
25pbmcgQ2Vy
...
```

Доверие к этой цепочке проверяется с помощью корневого сертификата из файла */etc/ipa/ca.crt*, на который указывает параметр `ldap_tls_cacert` из секции **domain** конфигурационного файла */etc/sssd/sssd.conf*. Данный сертификат загружается на компьютер автоматически при вводе компьютера в домен. Содержимое этого файла соответствует последнему сертификату из цепочки, полученной от сервера.

Открыть конфигурацию *sssd.conf* для проверки сертификата:

```
sudo cat /etc/sssd/sssd.conf | grep ldap_tls_cacert
```

Результат отображает файл */etc/ipa/ca.crt*:

```
ldap_tls_cacert = /etc/ipa/ca.crt
```

Открыть файл сертификата командой:

```
sudo cat /etc/ipa/ca.crt
```

В результате отображается сертификат **X509** формате **Base64String**:

```
-----BEGIN CERTIFICATE-----
MIIDIzCCAgugAwIBAgIUULQd6OzgJ/ik7wJvV0gd6kUIFKAwDQYJKoZIhvcN
AQEL
BQAwITEfMB0GA1UEAwwWQ0EgU2lnbmluZyBDZXJ0aWZpY2F0ZTAeFw0y
MjExMTYx
NzM4MjVaFw00MjExMTExNzM4MjVaMCExHzAdBgNVBAMMFkNBIFNpZ
25pbmcgQ2Vy
```

Проверить содержимое сертификата можно с помощью все той же утилиты **openssl**. Как

можно заметить, по умолчанию корневой сертификат выписан на 10 лет, после чего его нужно будет продлевать.

```
sudo openssl x509 -in /etc/ipa/ca.crt -text -noout
```

Результат выполнения:

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
50:b4:1d:e8:ec:e0:27:f8:a4:ef:02:6f:57:48:1d:ea:45:08:14:a0
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN = CA Signing Certificate
Validity
Not Before: Nov 16 17:38:25 2023 GMT
Not After : Nov 11 17:38:25 2043 GMT
...
```

Для упрощения отладки работы компьютеров в домене на них автоматически устанавливается и настраивается пакет **ldap-utils**, в состав которого входят такие утилиты как **ldapsearch**, **ldapadd** и др. Безопасность соединения проверяется с использованием корневого сертификата из файла */etc/ssl/certs/ca-certificates.crt*, на который указывает параметр `TLS_CACERT` из конфигурационного файла */etc/ldap/ldap.conf*.

```
sudo cat /etc/ldap/ldap.conf
```

Результат выполнения:

```
...
TLS_CACERT
/etc/ssl/certs/ca-certificates.crt
URI ldaps://dc-1.ald.company.lan
BASE dc=ald,dc=company,dc=lan
SASL_MECH GSSAPI
...
```

Файл *ca-certificates.crt* является связкой сертификатов, в которой содержится более 100 корневых сертификатов удостоверяющих центров, которым доверяет операционная система Astra Linux. Корневой сертификат домена, который ранее отображался в файле */etc/ipa/ca.crt*, обычно находится в самом конце этого файла. Чтобы просмотреть

информацию по всем сертификатам из файла, можно использовать следующую команду:

```
openssl crl2pkcs7 -nocrl -certfile /etc/ssl/certs/ca-certificates.crt |
↪openssl pkcs7 -print_certs -text -noout | less
```

2.4.3. Доступ к веб-интерфейсам и REST API контроллера домена по протоколу HTTPS

Портал управления ALD Pro и веб-интерфейс **FreeIPA** работают только по безопасному протоколу **HTTPS**, и, если обратиться к контроллеру с помощью утилиты **openssl**, то можно заметить, что веб-сервер **Apache** использует тот же самый сертификат, что и **LDAP-каталог**.

```
echo Q | openssl s_client -showcerts dc-1.ald.company.lan:443
```

Результат выполнения для сайта **dc-1.ald.company.lan**:

```
-----BEGIN CERTIFICATE-----
MIIDxjCCAq6gAwIBAgIUZ4JathCvRrV6v+Aoi4kUNScViBswDQYJKoZIhvcN
AQEL
BQAwITEfMB0GA1UEAwwWQ0EgU2lnbmluZyBDZXJ0aWZpY2F0ZTAeFw0y
MjExMTYx
NzM4MjVaFw0zMjExMTMxNzM4MjVaMCExHzAdBgNVBAMMFmRjLTEuY
WxkLmNvbXBh
...
```

Проверить сертификат для службы **389 directory server**:

```
echo Q | openssl s_client -showcerts dc-1.ald.company.lan:636
```

Результат для службы **LDAP-каталога** на **636** порту:

```
...
-----BEGIN CERTIFICATE-----
MIIDxjCCAq6gAwIBAgIUZ4JathCvRrV6v+Aoi4kUNScViBswDQYJKoZIhvcN
AQEL
BQAwITEfMB0GA1UEAwwWQ0EgU2lnbmluZyBDZXJ0aWZpY2F0ZTAeFw0y
MjExMTYx
NzM4MjVaFw0zMjExMTMxNzM4MjVaMCExHzAdBgNVBAMMFmRjLTEuY
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
WxkLmNvbXBh
...
```

Для того, чтобы браузер доменного компьютера открывал эти ресурсы без предупреждений, корневой сертификат ALD Pro должен быть добавлен в хранилище доверенных корневых сертификатов. На контроллерах домена для браузера Firefox это настроено через корпоративную политику, описанную в файле */usr/lib/firefox/distribution/policies.json*. С помощью этой же политики можно разрешить прозрачную Kerberos-аутентификацию для ресурсов из корпоративного домена, для этого нужно в секции **Authentication** задать параметр **SPNEGO** (Simple and Protected GSS-API Negotiation Mechanism, простой и защищенный механизм согласования **GSS-API**).

Проверить файл командой:

```
cat /usr/lib/firefox/distribution/policies.json
```

```
{
    "policies": {
        "BlockAboutAddons": true,
        "BlockAboutConfig": true,
        "Authentication": {
            "SPNEGO": ["ald.company.lan"]
        },
        "Certificates": {
            "ImportEnterpriseRoots": true,
            "Install": ["/etc/ipa/ca.crt"]
        },
        "Homepage": {
            "URL": "https://dc-1.ald.company.lan/",
            "Locked": true,
            "StartPage": "homepage-locked"
        }
    }
}
```

Для автоматической настройки рабочих станций можно задействовать механизм групповых политик ALD Pro:

1. Создать простой дополнительный параметр компьютера «**Политика браузера**

Firefox» с уникальным идентификатором **firefox_policy**.

2. Создать внутри этого параметра следующие атрибуты:

   - «Блокировать доступ к странице addons», идентификатор **block_about_addons**;
   - «Блокировать доступ к странице config», идентификатор **block_about_config**;
   - «Список доменов для Kerberos аутентификации», идентификатор **authentication_spnego**;
   - «Список доверенных сертификатов», идентификатор **trusted_certificates**;
   - «Адрес домашней страницы», идентификатор **homepage_url**.

3. Задать текст скрипта:

```
{% set node = salt['grains.get']('nodename') %}
{% set gpo = salt['pillar.get']('aldpro-hosts:' + node + ':firefox_policy' )
↪%}
{% if gpo %}
firefox_policy:
file.managed:
    - name: /usr/lib/firefox/distribution/policies.json
    - user: root
    - group: root
    - mode: 644
    - contents:
    - '{'
    - '        "policies": {'
{% if gpo['block_about_addons'] %}
    - '                "BlockAboutAddons": {{ gpo['block_about_addons'] }},'
{% endif %}{% if gpo['block_about_config'] %}
    - '                "BlockAboutConfig": {{ gpo['block_about_config'] }},'
{% endif %}{% if gpo['authentication_spnego'] %}
    - '                "Authentication": {'
    - '                        "SPNEGO": [{{ gpo['authentication_spnego'] }}
↪]'
    - '                },'
{% endif %}{% if gpo['trusted_certificates'] %}
    - '                "Certificates": {'
    - '                        "ImportEnterpriseRoots": true,'
    - '                        "Install": [{{ gpo['trusted_certificates'] }}]
↪'
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
    - '                },'
{% endif %}{% if gpo['homepage_url'] %}
    - '                "Homepage": {'
    - '                        "URL": "{{ gpo['homepage_url'] }}",'
    - '                        "Locked": true,'
    - '                        "StartPage": "homepage-locked"'
    - '                }'
{% endif %}
    - '        }'
    - '}'
{% endif %}
```

2.4.4. Доступ к удаленному рабочему столу по протоколу VNC через HTTPS

Для оказания пользователям услуги технической поддержки администратор может подключиться к удаленному рабочему столу компьютера, для этого пользователю нужно запустить приложение «Удаленный рабочий стол» и сообщить администратору случайный пароль из окна приложения. Подключение к сессии выполняется со страницы компьютера на портале управления, функция реализована на базе программного кода из проекта noVNC.

Открывая приложение удаленного рабочего стола, пользователь фактически запускает на своем компьютере упрощенный веб-сервер **websockify**, который перенаправляет запросы на порт **TCP/5900**, где их обрабатывает **x11vnc**-сервер. Веб-серверу порт назначается динамически, начиная с **TCP/6080** в зависимости от того, сколько сессий удаленного подключения было инициировано на рабочей станции. Для безопасного обмена данными **websockify** использует закрытый ключ и **SSL**-сертификат из файла */opt/rbta/aldpro/rd-gui/noVNC/novnc.pem*. Можно проверить, что это именно тот сертификат с помощью утилиты **openssl**.

Вывести сертификат для сравнения на экран:

```
cat /opt/rbta/aldpro/rd-gui/noVNC/novnc.pem
```

Результат выполнения:

```
-----BEGIN CERTIFICATE-----
MIIDazCCAlOgAwIBAgIUbKtAWP6659L+jsNqaemnAQVksoswDQYJKoZIhvc
NAQEL
BQAwRTELMAkGA1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3RhdGUxI
TAfBgNVBAoM
GEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDAeFw0yMjA2MTQxNzAxMDF
aFw0yMzA2
...
```

Сверить **SSL**-сертификат на порту **6080** утилитой **openssl**:

```
echo Q | openssl s_client -connect pc-1.ald.company.lan:6080
```

В результате выполнения команды отображается тот же сертификат:

```
-----BEGIN CERTIFICATE-----
MIIDazCCAlOgAwIBAgIUbKtAWP6659L+jsNqaemnAQVksoswDQYJKoZIhvc
NAQEL
BQAwRTELMAkGA1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3RhdGUxI
TAfBgNVBAoM
GEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDAeFw0yMjA2MTQxNzAxMDF
aFw0yMzA2
...
```

Подробности об этом сертификате можно посмотреть с помощью той же утилиты:

```
openssl x509 -in /opt/rbta/aldpro/rd-gui/noVNC/novnc.pem -text -noout
```

Результат выполнения команды это описание сертификата в удобочитаемом формате:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            6c:ab:40:58:fe:ba:e7:d2:fe:8e:c3:6a:69:e9:a7:01:05:64:b2:8b
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
...
```

Когда администратор подключается к **клиенту** с **веб-портала**, он обращается к URL вида

wss://dc-1.ald.company.lan/aldpro/rdproxy/pc-1.ald.company.lna/6080/websockify, поэтому **веб-сервер контроллера домена** проксирует запросы на указанный порт доменного компьютера. В конфигурационном файле */etc/apache2/conf-aldpro/aldpro-mp-rdproxy.conf* для параметра **SSLProxyVerify** определено значение none, поэтому принимаются любые самоподписанные сертификаты.

2.5. Работа механизмов автоматического обнаружения сервисов LDAP и KDC

2.5.1. Автоматическое обнаружение при вводе хоста в домен утилитой ipa-client-install

Ввод машины в домен осуществляется с помощью утилиты **aldpro-client-installer**, которая по цепочке вызывает **astra-freeipa-client** и **ipa-client-install**, см. табл. 6.

aldpro-client-installer >	astra-freeipa-client >	ipa-client-install

получает:
`--domain ald.company.lan`
`--account admin`
`--password 'AstraLinux_176'`
`--host pc-1 --gui`
`--force`
	получает:
	`-d ald.company.lan`
	`-u admin -p AstraLinux_172 -y`
	`--par "--hostname=pc-1.ald.company.lan"`
	`--force-join`
		получает:
		`'domain_name': None`,
		`'principal': 'admin'`,
		пароль не логируется,
		`'host_name': 'pc-1.ald.company.lan'`,
		`'force': False`,
		`'force_join': True`,
		`'mkhomedir': True`, и др.

продолжение на следующей странице

Таблица 2.1 – продолжение с предыдущей страницы

aldpro-client-installer >	astra-freeipa-client >	ipa-client-install

вызывает:
`/usr/bin/ astra-freeipa-client -d "{domain_name}" -u "{login}" -y --par "--hostname=pc-1. ald.company.lan --force-join"`
	устанавливает:
	`hostnamectl set-hostname $compname. ${domain}`
	и далее вызывает:
	`ipa-client-install -U -p $username -w $userpass $par`	

Таблица 6 — Передача параметров при вводе машины в домен

Механизм автоматического обнаружения сервисов предусмотрен только в скрипте **ipa-client-install** и работает для определения следующих параметров:

- **Realm/DNS Domain**: `ALD.COMPANY.LAN/ald.company.lan` - область Керберос и FQDN домена, отличаются обычно только регистром символов. Можно сделать так, чтобы эти значения были разными, но такие настройки сложны и не имеют значительных преимуществ, поэтому не рекомендуются.
- **IPA Server**: `dc-1.ald.company.lan` - FQDN имя контроллера, через который должен быть выполнен ввод машины в домен. Обычно не указывается явно и определяется автоматически.
- **Client hostname**: `pc-1.ald.company.lan` - FQDN имя, которое должно быть у компьютера после ввода в домен, DNS-зона должна совпадать с FQDN домена. Если значения не будут совпадать, то работа хоста будет нарушена, но разработчики целенаправленно не сделали такую проверку, т.к. это дает гибкость в редких сценариях развертывания.

Если домен не указан явно через параметр `--domain`, то скрипт будет пытаться получить это значение из следующих источников:

- из параметра `--host`;
- из текущего имени компьютера `hostname` (используется имя, а не FQDN, т.е. это то значение, которое возвращает команда `hostname`, а не `hostname -f`);
- из файла *resolv.conf*, параметры `search` и `domain`.

Проверка имени домена выполняется путем извлечения **SRV**-записей для протокола **LDAP**

по **TCP**. Для каждого FQDN скрипт проверяет все компоненты домена вверх по иерархии, поэтому, например, если в переменной `hostname` было значение «**pc-1.ald.company.lan**», то скрипт установки проверит следующие **SRV**-записи:

1. `_ldap._tcp.ald.company.lan`
2. `_ldap._tcp.company.lan`
3. `_ldap._tcp.lan`

Важно обратить внимание, что утилита **astra-freeipa-client** нарушает логику передачи параметров, т.к. вызывает утилиту **ipa-client-install** со значением `{'domain_name': None}`, но перед этим она устанавливает в системе имя хоста `pc-1.ald.company.lan`, поэтому ввод машины в домен отрабатывает корректно.

Сервер **IPA** можно указать явно через параметр `server`, но в том случае параметр `domain` также должен быть задан в явном виде. Если параметр `server` не будет указан, то сервер будет найден через поиск **SRV**-записей `_ldap._tcp.DOMAIN`.

При использовании опции `server` в файлы *sssd.conf* и *krb5.conf* будет внесен фиксированный список серверов. Параметр можно указывать несколько раз подряд, чтобы задать для переменной `ipa_server` список значений.

2.5.2. Автоматическое обнаружение сервисов в SSSD

Для обеспечения надежной работы компьютера в домене в службе **SSSD** реализован механизм автоматического обнаружения контроллеров домена. В момент загрузки служба **SSSD** берет параметр `domains` и обращается к соответствующей секции файла */etc/sssd/sssd.conf* для настройки **бэкенда**:

```
[sssd]
domains = ald.company.lan

[domain/ald.company.lan]
id_provider = ipa
ipa_server = _srv_, dc-1.ald.company.lan
ipa_domain = ald.company.lan
ipa_hostname = pc-1.ald.company.lan
auth_provider = ipa
chpass_provider = ipa
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
access_provider = ipa
cache_credentials = True
ldap_tls_cacert = /etc/ipa/ca.crt
krb5_store_password_if_offline = True
```

Ключевые параметры **бэкенда**:

- `id_provider` — указывает, что в качестве поставщика идентификационных данных будет выступать сервер **FreeIPA** **ipa_server** — список FQDN имен и IP адресов контроллеров домена в порядке, в каком нужно к ним подключаться. Может использоваться также служебное имя «_**srv**_», соответствующее механизму автоматического обнаружения (**service discovery**) через поиск **SRV**-записей `_ldap._tcp.DOMAIN`, как указано в стандарте (**RFC2782**).
- `ipa_backup_server` — с помощью этого параметра можно указать список резервных серверов, которые будут выбираться только в случае недоступности основных. Этот параметр не предполагает возможности использования механизма автообнаружения.
- `ipa_domain` — указывает имя домена **IPA**. Это необязательный параметр, если он не указан, то используется доменное имя из названия конфигурации.
- `ipa_hostname` — требуется устанавливать на машинах, где имя хоста не соответствует полному имени компьютера, которое используется в домене **IPA** для идентификации этого хоста.

Записи **SRV**, создаваемые **FreeIPA** для своих сервисов, существенно отличаются от тех, которые можно создать вручную из интерфейса. Этим записям в каталоге назначен класс `idnsTemplateObject` и задано дополнительное свойство `idnsTemplateAttribute;cnamerecord`, которое определяет шаблон подстановки для поддержки технологии сайтов (**локаций**), см. *Шаблон записи для SRV-записей в DNS*.

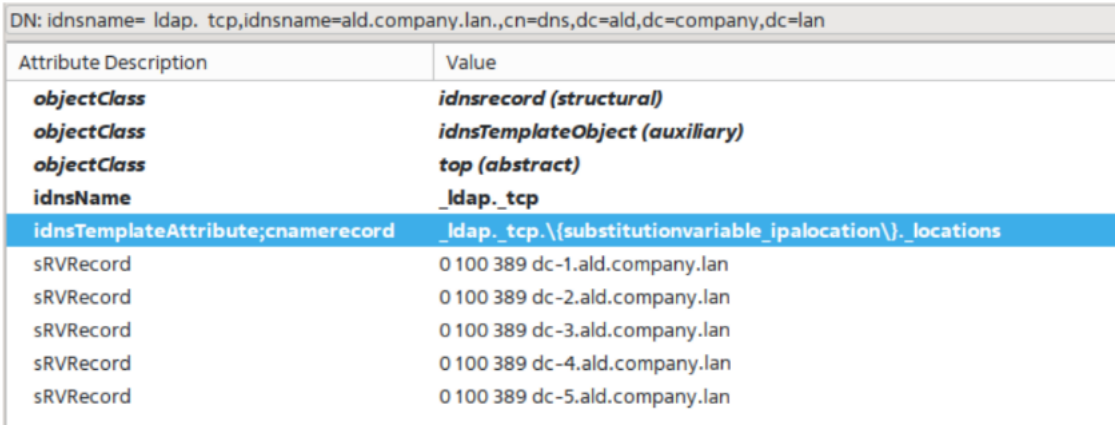


Рисунок 2.16 – Шаблон записи для SRV-записей в DNS

Для привязки серверов к локациям у дочерних записей **DN** `cn=servers,cn=dns,dc=ald,dc=company,dc=lan` задано значение атрибута `idnsSubstitutionVariable;ipalocation`, соответствующее имени сайта, в котором этот сервер находится.

Например, в домене из 5 контроллеров при обращении к DNS серверу 10.0.1.11 (**dc-1.ald.company.lan**) **Bind** выполняет подстановку и возвращает результат для `_ldap._tcp.hq_locations.ald.company.lan`, что соответствует сайту **hq** (head quarters, головной офис), см. *Атрибут idnsSubstitutionVariable для контроллера домена dc-1*. В список будут включены все контроллеры домена, но для серверов из сайта **hq** приоритет будет равен 0, а у всех остальных 50, поэтому служба **SSSD** в первую очередь будет обращаться к контроллерам из «своего» сайта, к которому компьютер косвенно привязан через DNS-сервер, который обслуживает его запросы командой:

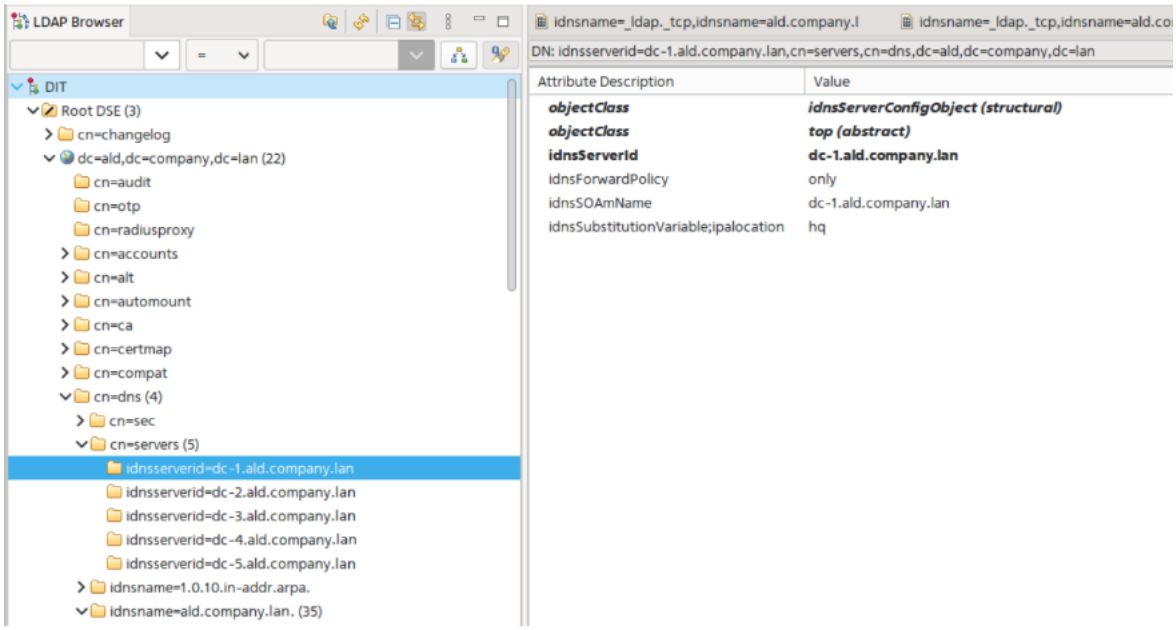


Рисунок 2.17 – Атрибут idnsSubstitutionVariable для контроллера домена dc-1

```
nslookup -q=SRV _ldap._tcp.ald.company.lan
```

Результат выполнения:

```
Server:     127.0.0.1
Address:    127.0.0.1#53

_ldap._tcp.ald.company.lan canonical name =
_ldap._tcp.hq._locations.ald.company.lan.
_ldap._tcp.hq._locations.ald.company.lan service = 50 100 389 dc-4.ald.
 ↪company.lan.
_ldap._tcp.hq._locations.ald.company.lan service = 0 100 389 dc-1.ald.company.
 ↪lan.
_ldap._tcp.hq._locations.ald.company.lan service = 0 100 389 dc-2.ald.company.
 ↪lan.
_ldap._tcp.hq._locations.ald.company.lan service = 50 100 389 dc-3.ald.
 ↪company.lan.
_ldap._tcp.hq._locations.ald.company.lan service = 50 100 389 dc-5.ald.
 ↪company.lan.
```

После того, как список серверов определен, **SSSD** начинает искать доступный контроллер. Сначала **SSSD** выполняет поиск по серверам с приоритетом 0 из того же сайта, и только в случае неудачи переключается на остальные. Если компьютер работает в домене ALD Pro (**FreeIPA**), то проверка выполняется по одному серверу, а если провайдером выступает AD, то сервера проверяются группами по 5 штук, но доступность контроллера в любом случае определяется возможностью совершения анонимных LDAP-запросов, например, выдержка из журнала */var/log/dirsrv/access.log*:

```
SRCH base="" scope=0 filter="(objectClass=*)" attrs="* altServer
 ↪namingContexts supportedControl supportedExtension supportedFeature"
```

Если служба **SSSD** сможет получить **TGT/TGS** билеты для доступа к **LDAP**, используя */etc/krb5.keytab* файл хоста, то она выполнит еще несколько авторизованных запросов для получения дополнительной информации о диапазонах идентификаторов, участии хоста в группах и др. настройках. Это можно увидеть также из файла журнала */var/log/dirsrv/access.log*:

```
...
SRCH base="fqdn=pc-1.ald.company.lan,cn=computers,cn=accounts,dc=ald,
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
↪dc=company,dc=lan" scope=0 filter="(objectClass=*)" attrs="objectClass cn
↪memberOf ipaUniqueID"
...
```

Адрес сервера, с которым происходил обмен, будет сохранен как активный сервер, а FQDN остальных контроллеров, полученных через **SRV**-запрос, служба запишет, как обнаруженные сервера (Discovered IPA servers).

Информацию о результатах автоматического обнаружения, можно узнать с помощью утилиты **sssctl** из состава пакета **sssd-tools**. Данный инструмент администрирования взаимодействует со службой **SSSD** напрямую через **SBus**.

```
sudo sssctl domain-list
```

Результат выполнения список доменов:

```
ald.company.lan
```

Вывести статус по имени домена:

```
sudo sssctl domain-status ald.company.lan
```

Результат выполнения команды это список найденных контроллеров в домене:

```
Online status: Online

Active servers:
IPA: dc-1.ald.company.lan

Discovered IPA servers:
- dc-1.ald.company.lan
- dc-3.ald.company.lan
- dc-2.ald.company.lan
- dc-4.ald.company.lan
- dc-5.ald.company.lan
- dc-1.ald.company.lan
```

2.5.3. Автоматическое обнаружение сервисов в библиотеке libkrb5

2.5.3.1. На обычном компьютере в домене

Для администрирования компьютеров в домене системные администраторы часто используют утилиты из пакета **krb5-user**, такие как **kinit**, **klist** и др., которые обращаются к функциям библиотеки *libkrb5*.

```
sudo ldd $(which kinit) | grep libkrb5
```

Результат выполнения:

```
libkrb5.so.3 => /lib/x86_64-linux-gnu/libkrb5.so.3 (0x00007fa558914000)
libkrb5support.so.0 => /lib/x86_64-linux-gnu/libkrb5support.so.0
↪(0x00007fa5588cb000)
```

Настройки этой библиотеки задаются в файле */etc/krb5.conf*, но при установке **sssd** в папку плагинов **libkrb5** копируется файл *sssd_krb5_locator_plugin.so*, поэтому, если служба **sssd** включена, то при выполнении **kinit** учитываются настройки из */etc/sssd/sssd.conf*.

```
sudo dpkg -S /usr/lib/x86_64-linux-gnu/krb5/plugins/libkrb5/sssd_krb5_locator_
↪plugin.so
```

Результат выполнения:

```
sssd-common: /usr/lib/x86_64-linux-gnu/krb5/plugins/libkrb5/sssd_krb5_locator_
↪plugin.so
```

На доменном компьютере в файле *sssd.conf* в секции `[domain/ald.company.lan]` в параметре `ipa_server` первым значением по умолчанию идет «_**srv**_», поэтому служба **sssd** выполняет поиск сервера **kdc** через обращение к **SRV**-записям `_kerberos._tcp.ald.company.lan`.

```
cat /etc/sssd/sssd.conf
```

Параметр `ipa_server` в конфигурационном *файле sssd.conf*:

```
[domain/ald.company.lan]
...
ipa_server = _srv_, dc-1.ald.company.lan
```

(продолжение на следующей странице)

```
...
```

После автоматического обнаружения сервера провайдер аутентификации (auth-provider) службы **sssd** записывает IP адрес контроллера и FQDN-имена еще двух запасных серверов в файл *kdcinfo* и функции Kerberos будут использовать эти данные для подключения.

```
sudo sssctl domain-status ald.company.lan
```

Результат выполнения:

```
Online status: Online

Active servers:
IPA: dc-1.ald.company.lan

Discovered IPA servers:
- dc-5.ald.company.lan
- dc-1.ald.company.lan
- dc-4.ald.company.lan
- dc-3.ald.company.lan
- dc-2.ald.company.lan
- dc-1.ald.company.lan
```

Проверить какой сервер используется в файле *kdcinfo* можно командой:

```
sudo cat /var/lib/sss/pubconf/kdcinfo.ALD.COMPANY.LAN
```

где `ALD.COMPANY.LAN` - домен предприятия.

Результат выполнения:

```
10.0.1.12
dc-1.ald.company.lan
dc-3.ald.company.lan
```

Например, при выполнении **kinit** запрос сначала будет направляться к серверу с IP адресом 10.0.1.11, в случае его недоступности к серверу **dc-2.ald.company.lan**, далее к **dc-3.ald.company.lan** и только в случае недоступности всех трех серверов запрос завершится ошибкой.

Если в параметре `ipa_server` убрать значение «_**srv**_» и оставить только FQDN контроллера, через который этот хост был введен в домен, то после перезапуска **sssd** все Kerberos запросы пойдут только через указанный сервер.

Если службу **sssd** выключить, то контроллер будет определяться штатными механизмами библиотеки *libkrb5*. По умолчанию в файле */etc/krb5.conf*, в секции `[libdefaults]` установлен параметр `dns_lookup_kdc = true`, поэтому поиск сервера будет выполняться похожим образом через обращение к **SRV**-записям, но отличие будет состоять в том, что *libkrb5* не поддерживает кэширование, поэтому автоматическое обнаружение будет срабатывать каждый раз при обращении к функциям библиотеки.

```
sudo cat /etc/krb5.conf | grep dns_lookup_kdc
```

Результат выполнения команды:

```
dns_lookup_kdc = true
```

Файл конфигурации *krb5.conf* позволяет отключать автоматическое обнаружение, тогда с помощью параметра `kdc` можно будет указать конкретный сервер:

```
sudo cat /etc/krb5.conf
```

Настройка параметра `kdc` на конкретный сервер **dc-1**:

```
[libdefaults]
...
dns_lookup_kdc = false
...
[realms]
 ALD.COMPANY.LAN = {
  kdc = dc-1.ald.company.lan
  ...
 }
```

2.5.3.2. На контроллере домена

На контроллерах домена **kinit** ведет себя иначе, чем на доменных компьютерах, т.к. кроме службы **sssd** устанавливается еще и служба **winbind**, у которой есть собственный плагин **winbind_krb5_locator.so**.

```
ls -l /usr/lib/x86_64-linux-gnu/krb5/plugins/libkrb5/
```

Результат выполнения на **dc-1**:

```
-rw-r--r-- 1 root root 19248 ноя 22 2021 sssd_krb5_locator_plugin.so
-rw-r--r-- 1 root root 14840 июн 6 2022 winbind_krb5_locator.so
```

Посмотреть какому пакету принадлежит файл библиотеки можно командой:

```
sudo dpkg -S /usr/lib/x86_64-linux-gnu/krb5/plugins/libkrb5/winbind_krb5_
↪locator.so
```

Результат выполнения:

```
winbind: /usr/lib/x86_64-linux-gnu/krb5/plugins/libkrb5/winbind_krb5_locator.
↪so
```

Активный контроллер домена, предлагаемый службой **winbind** можно узнать через команду `dsgetdcname` утилиты **wbinfo**:

```
wbinfo --dsgetdcname ALD.COMPANY.LAN
```

Результат выполнения команды:

```
dc-1.ald.company.lan
\\10.0.1.11
1
f35731b8-81fe-46c3-ac8f-feb6deb55889
ald.company.lan
ald.company.lan
0xe00003fd
Default-First-Site-Name
Default-First-Site-Name
```

Включить отладку **Kerberos** для проверки работы можно включив переменную `KRB5_TRACE`:

```
sudo i
set +o history
env KRB5_TRACE=/dev/stdout kinit admin <<< AstraLinux_176
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
set -o history
exit
```

Результат выполнения трассировки:

```
[3126] 1696423198.013624: Getting initial credentials for admin@ALD.COMPANY.
↪LAN
[3126] 1696423198.013626: Sending unauthenticated request
[3126] 1696423198.013627: Sending request (191 bytes) to ALD.COMPANY.LAN
[3126] 1696423198.013628: Initiating TCP connection to stream 10.0.1.11:88
[3126] 1696423198.013629: Sending TCP request to stream 10.0.1.11:88
[3126] 1696423198.013630: Received answer (513 bytes) from stream 10.0.1.
↪11:88
[3126] 1696423198.013631: Terminating TCP connection to stream 10.0.1.11:88
[3126] 1696423198.013632: Response was from master KDC
[3126] 1696423198.013633: Received error from KDC: -1765328359/Additional pre-
↪authentication required
[3126] 1696423198.013636: Preauthenticating using KDC method data
[3126] 1696423198.013637: Processing preauth types: PA-PK-AS-REQ (16), PA-FX-
↪FAST (136), PA-ETYPE-INFO2 (19), PA-PKINIT-KX (147), PA-SPAKE (151), PA-ENC-
↪TIMESTAMP (2), PA_AS_FRESHNESS (150), PA-FX-COOKIE (133)
[3126] 1696423198.013638: Selected etype info: etype aes256-cts, salt "T1!
↪dGW5C](`}^?2R", params ""
[3126] 1696423198.013639: Received cookie: MIT1\x00\x00\x00\x01uw\x951\xbb\
↪x06ew\x88]G\xa7\x87J\xf3\x02\xcb\xaf\x97<:\x0d\xa1\xb0\x96\xb4,\xbc\xd2\xb6\
↪x0c\xce\xa4"?\xa6\xe8\xf1\xa5\xf4\xe6K\x01\x00\xe2\x02Z6\x18#M\xf8\xd4w\x17\
↪xcd\xc5S\xe8\x13;\xa6\x01t2\xc6M\xdf\xddHIs{#\xc9\x15\xe2\x9d\x1f\x9c\xd20.\
↪x00 gG\x9d\xfb\x0c\x80\x04'\x9f\x8bZJt-S'\x06\x97\xd8\x92;\xa5^~Ep*\x81T\
↪xff\x7f\xd0\xb7\x9b\xf6Y\xf4\xdb\xd9,\xbb\x1a\x93\xd8\xca
[3126] 1696423198.013640: PKINIT client has no configured identity; giving up
[3126] 1696423198.013641: Preauth module pkinit (147) (info) returned: 0/
↪Success
[3126] 1696423198.013642: PKINIT client received freshness token from KDC
[3126] 1696423198.013643: Preauth module pkinit (150) (info) returned: 0/
↪Success
[3126] 1696423198.013644: PKINIT client has no configured identity; giving up
[3126] 1696423198.013645: Preauth module pkinit (16) (real) returned: 22/
↪Недопустимый аргумент
[3126] 1696423198.013646: SPAKE challenge received with group 1, pubkey
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
 ↪2F4F0F1B95AF467E3A718CB0B881B2C73FA1D9D132FC15DCD0CE504BC58ED756
Password for admin@ALD.COMPANY.LAN:
[3126] 1696423198.013647: SPAKE key generated with pubkey
 ↪EFFC0DE0B82CEEBD2B715C87EED0EA086C5F8E9E79570593A4C302125DE253D8
[3126] 1696423198.013648: SPAKE algorithm result:
 ↪5C447C5BB317672F202E15DC5B54C2DB2288D87D7AE12F75A9FFB6F825A0D930
[3126] 1696423198.013649: SPAKE final transcript hash:
 ↪F2250C79047924FEAD1416E2B75948CCF3BABD80E9B821CA03C47A74D1D69985
[3126] 1696423198.013650: Sending SPAKE response
[3126] 1696423198.013651: Preauth module spake (151) (real) returned: 0/
 ↪Success
[3126] 1696423198.013652: Produced preauth for next request: PA-FX-COOKIE
 ↪(133), PA-SPAKE (151)
[3126] 1696423198.013653: Sending request (450 bytes) to ALD.COMPANY.LAN
[3126] 1696423198.013654: Initiating TCP connection to stream 10.0.1.11:88
[3126] 1696423198.013655: Sending TCP request to stream 10.0.1.11:88
[3126] 1696423198.013656: Received answer (1575 bytes) from stream 10.0.1.
 ↪11:88
[3126] 1696423198.013657: Terminating TCP connection to stream 10.0.1.11:88
[3126] 1696423198.013658: Response was from master KDC
[3126] 1696423198.013659: AS key determined by preauth: aes256-cts/297C
[3126] 1696423198.013660: Decrypted AS reply; session key is: aes256-cts/D405
[3126] 1696423198.013661: FAST negotiation: available
[3126] 1696423198.013662: Initializing KEYRING:persistent:1421600000:krb_
 ↪ccache_zlQRxEn with default princ admin@ALD.COMPANY.LAN
[3126] 1696423198.013663: Storing admin@ALD.COMPANY.LAN → krbtgt/ALD.COMPANY.
 ↪LAN@ALD.COMPANY.LAN in KEYRING:persistent:1421600000:krb_ccache_zlQRxEn
[3126] 1696423198.013664: Storing config in KEYRING:persistent:1421600000:krb_
 ↪ccache_zlQRxEn for krbtgt/ALD.COMPANY.LAN@ALD.COMPANY.LAN: fast_avail: yes
[3126] 1696423198.013665: Storing admin@ALD.COMPANY.LAN → krb5_ccache_conf_
 ↪data/fast_avail/krbtgt\/ALD.COMPANY.LAN\@ALD.COMPANY.LAN@X-CACHECONF: in
 ↪KEYRING:persistent:1421600000:krb_ccache_zlQRxEn
[3126] 1696423198.013666: Storing config in KEYRING:persistent:1421600000:krb_
 ↪ccache_zlQRxEn for krbtgt/ALD.COMPANY.LAN@ALD.COMPANY.LAN: pa_type: 151
[3126] 1696423198.013667: Storing admin@ALD.COMPANY.LAN → krb5_ccache_conf_
 ↪data/pa_type/krbtgt\/ALD.COMPANY.LAN\@ALD.COMPANY.LAN@X-CACHECONF: in
 ↪KEYRING:persistent:1421600000:krb_ccache_zlQRxEn
```

В поставке **Samba** идет также утилита **net**, которая тоже выдает информацию о **KDC**, но ее результаты расходятся с тем, какой сервер фактически используют утилиты **kinit**:

```
sudo net ads info
```

Результат выполнения:

```
Failed to get server's current time!
LDAP server: 10.0.1.11
LDAP server name: dc-1.ald.company.lan
Realm: ALD.COMPANY.LAN
Bind Path: dc=ALD,dc=COMPANY,dc=LAN
LDAP port: 389
Server time: Чт, 01 янв 1970 03:00:00 MSK
KDC server: 10.0.1.11
Server time offset: 0
Last machine account password change: Чт, 01 янв 1970 03:00:00 MSK
```

2.5.3.3. Автоматическое обнаружение сервисов в клиенте IPA

Для автоматизации управления доменом системные администраторы используют утилиту **ipa**, которая обращается к одному из контроллеров домена через **REST API**, используя прозрачную Kerberos аутентификацию. После ее использования в связке ключей можно увидеть появление сервисного билета на доступ к HTTP конкретного контроллера.

```
klist
```

В результате в списке только **krbtgt** билет:

```
Ticket cache: KEYRING:persistent:1421600000:krb_ccache_zlQRxEn
Default principal: admin@ALD.COMPANY.LAN

Valid starting       Expires              Service principal
04.10.2023 15:52:52  05.10.2023 15:52:47  krbtgt/ALD.COMPANY.LAN@ALD.COMPANY.
 ↪LAN
```

Получить информацию о пользователе можно через команду `ipa`:

```
ipa user-show admin
```

Результат выполнения просмотра пользователя:

```
Имя учётной записи пользователя: admin
Фамилия: Administrator
Домашний каталог: /home/admin
Оболочка входа: /bin/bash
Псевдоним учётной записи: admin@ALD.COMPANY.LAN, root@ALD.COMPANY.LAN
UID: 1421600000
ID группы: 1421600000
Учётная запись отключена: False
Link to department: ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,
 ↪dc=company,dc=lan
Link to head department: ald.company.lan
Пароль: True
Участник групп: admins, lpadmin, trust admins, ald trust admin
Роли: ALDPRO - Main Administrator
Доступные ключи Kerberos: True
```

Повторно проверить список билетов можно командой `klist`:

```
Ticket cache: KEYRING:persistent:1421600000:krb_ccache_zlQRxEn
Default principal: admin@ALD.COMPANY.LAN

Valid starting       Expires              Service principal
04.10.2023 15:54:55  05.10.2023 15:52:47  HTTP/dc-1.ald.company.lan@ALD.
 ↪COMPANY.LAN
04.10.2023 15:52:52  05.10.2023 15:52:47  krbtgt/ALD.COMPANY.LAN@ALD.COMPANY.
 ↪LAN
```

Утилита **ipa** определяет сервер для подключения в следующем порядке:

- сначала используется значение директивы **xmlrpc_uri** из файла */etc/ipa/default.conf*;
- если сервер, указанный в *default.conf* окажется недоступен, утилита **ipa** через запрос **SRV**-записей `_ldap._tcp.DOMAIN` получит список всех доступных серверов и будет перебирать их случайным образом.

На контроллерах домена в файле */etc/ipa/default.conf* указан также параметр `ldap_uri`, который определяет адрес для подключения **бэкенда REST API** к LDAP-каталогу. По умолчанию предполагается, что **бэкенд** подключается только к той службе каталога, которая работает на том же сервере, поэтому подключение выполняется через UNIX сокет по **ldapi** (LDAP Over Interprocess Communication facilities, IPC).

```
cat /etc/ipa/default.conf | grep ldap_uri
```

Результат выполнения:

```
ldap_uri = ldapi://%2Frun%2Fslapd-ALD-COMPANY-LAN.socket
```

2.5.3.4. Автоматическое обнаружение сервисов клиентом LDAP

Для работы компьютера в домене утилиты **OpenLDAP** (`ldapsearch`, `ldapmodify` и др.) не требуются, но пакет **ldap-utils** устанавливается и настраивается автоматически для упрощения отладки возникающих проблем. За настройку LDAP-клиента отвечает скрипт *ipaclient/install/client.py*, который устанавливает в файле */etc/ldap/ldap.conf* следующие параметры по умолчанию:

- `TLS_CACERT` — определяет путь к файлу с цепочкой **SSL** сертификатов для проверки безопасности подключения по LDAPS и при использовании команды `StartTLS`.
- `URI` — определяет протокол подключения **LDAPS** и путь к LDAP-серверу по умолчанию. Значение в файле соответствует адресу контроллера домена, через который был выполнен ввод машины в домен. Это значение не обновляется динамически, поэтому при недоступности данного сервера утилиты перестанут работать без указания другого сервера явно через параметр `-H`.
- `BASE` — определяет DN-записи, которые будут использоваться в качестве базы поиска по умолчанию.
- `SASL_MECH` — определяет механизм аутентификации, по умолчанию используется **GSSAPI**, т.е. Kerberos аутентификация через связку ключей Linux.

Для обеспечения отказоустойчивости скриптов автоматизации можно использовать, например, результат автоматического обнаружения сервисов из файла *kdcinfo*:

```
ldapsearch -H ldaps://$(tail -n 1 /var/lib/sss/pubconf/kdcinfo.ALD.COMPANY.
↪LAN) -W -D
```

2.5.3.5. Автоматическое обнаружение сервисов ALD Pro

Автоматическое определение сервисов для подключения агентов **ALDPro-Salt-Minion** и **Zabbix** выполняет скрипт */opt/rbta/aldpro/client/bin/aldpro-service-discovery.py*.

Для определения списка серверов скрипт *aldpro-service-discovery.py* запрашивает **SRV**-записи `_ldap._tcp.DOMAIN`, в качестве FQDN домена используя значение параметра `domain` секции `global` из файла */etc/ipa/default.conf*. В предыдущих реализациях в список вносились только контроллеры из того же сайта, с версии 1.4.0 скрипт вносит в начало списка контроллеры из того же сайта, а в конец добавляет все остальные.

Агент **Zabbix** отвечает за передачу данных на сервер мониторинга. Он может работать как в активном, так и в пассивном режимах. Настройки подключения к серверу находятся в файле */etc/zabbix/zabbix_agentd.conf.d/00-servers.conf*. Для определения сервера мониторинга скрипт *aldpro-service-discovery.py* выполняет запрос к **REST API** */discover/api/ds/monitoring/servers*.

Агент **Syslog-NG** отвечает за передачу событий в подсистему журналирования. Он не предусматривает поддержки автоматического обнаружения сервисов и конфигурируется через **SaltStack**, за что отвечает скрипт *syslogng_install.sls* из папки */etc/salt/states/aldpro/automations/subsystems/projects/*.

2.6. Работа компьютера в автономном режиме

Для обеспечения комфортной работы пользователей в условиях нестабильного подключения к локальной сети по Wi-Fi или через VPN служба **SSSD** может предоставлять часть сервисов автономно, без подключения к серверу. Переход в автономный режим происходит автоматически в следующих случаях:

- пропало подключение к сети;
- нет возможности преобразовать FQDN сервера в IP адрес;
- не удается подключиться к серверу.

Работая автономно, Монитор службы **SSSD** предпринимает попытки возврата в режим онлайн по следующим триггерам:

- получено уведомление об изменении настроек сети, например, о подключении кабеля или изменении таблицы маршрутизации (см. `man netlink`);
- получено уведомление об изменении конфигурационного файла */etc/resolv.conf* (см. `man inotify`);
- по расписанию каждые 30 секунд;

В ходе отладки администратор может переключать режимы вручную, отправляя процессу **SSSD** сигналы SIGUSR1 (перейти в **offline**) и SIGUSR2 (перейти в **online**), но в большинстве случаев достаточно включить/выключить всю службу целиком.

Включение **Offline** режима можно командой:

```
sudo kill -SIGUSR1 $(pidof sssd) && sudo sssctl domain-status ald.company.
↪lan | grep status
```

Результат выполнения:

```
Online status: Offline
```

Включение **Online** режима можно командой:

```
sudo kill -SIGUSR2 $(pidof sssd) && sudo sssctl domain-status ald.company.
↪lan | grep status
```

Результат выполнения:

```
Online status: Online
```

2.6.1. Автономный вход по кэшу пароля

Когда пользователь в первый раз входит в компьютер, его аутентификация возможна только через контроллер домена, но при получении успешного статуса **PAM_SUCCESS** служба **SSSD** сохранит **SHA512** хэш в локальной базе, что гарантирует возможность автономной аутентификации этого пользователя даже в условиях отсутствия связи с сервером. Извлечь хэш пользовательского пароля из ldb-файла и проверить его валидность можно с помощью утилит **ldbsearch** из пакета **ldb-tools** и **openssl**.

Получить кэшированный пароль пользователя **admin**:

```
sudo ldbsearch -H /var/lib/sss/db/cache_ald.company.lan.ldb -b name=admin@ald.
↪company.lan,cn=users,cn=ald.company.lan,cn=sysdb cachedPassword
```

В результате отображается атрибут `cachedPassword`. Важно обратить внимание, что значение перенесло на другую строку, о чем говорит строка начинающаяся с символа пробел.

```
asq: Unable to register control with rootdse!
record 1
dn: name=admin@ald.company.lan,cn=users,cn=ald.company.lan,cn=sysdb
cachedPassword:
$6$o.zJdi5M.yDDUi5j$5YHQgKLFhRzt78sSx5R8AXqLYTo9fgkgzGflHI1SYG
rshTqIGPwEv7G1WUvgd8vW3LoCSYPt88KV7SeN2N6A.0
...
```

Проверить генерацию хэша пароля можно с помощью утилиты **openssl**, где:
`o.zJdi5M.yDDUi5j` — соль, которая получается из кэша пароля между символами `$`:

```
sudo i
set +o history
openssl passwd -6 -salt 'o.zJdi5M.yDDUi5j' 'AstraLinux_176'
set -o history
exit
```

Результат выполнения совпадает с кэшированными данными:

```
$6$o.zJdi5M.yDDUi5j
 ↪$5YHQgKLFhRzt78sSx5R8AXqLYTo9fgkgzGflHI1SYGrshTqIGPwEv7G1WUvgd8vW3LoCSYPt88KV7SeN2N
 ↪0
```

Функция хранения кэшей включена по умолчанию, за это отвечает параметр `cache_credentials` из файла *sssd.conf*. Срок хранения паролей не ограничен, так как параметр `offline_credentials_expiration` не задан.

Для первого входа в систему компьютер должен иметь доступ к контроллеру домена, что легко обеспечить из офиса, подключив устройство кабелем к локальной сети, но трудно выполнимо, если устройство нужно передать сотруднику для удаленной работы через службу доставки. В этом случае может оказаться, что офисная сеть будет ему недоступна до тех пор, пока он не войдет в систему и не подключится через VPN. Для решения этой проблемы в составе **sssd-tools** есть утилита **sss_seed**, которая позволяет имитировать первый вход, принудительно устанавливая ldb-кэш пароля.

Установить кэш пароля для тестовой учетной записи **olegovo**:

```
sudo i
set +o history
echo 'AstraLinux_176' > /tmp/ssd-pwd.txt
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
sss_seed --domain ALD.COMPANY.LAN --username olegovo --password-file /tmp/ssd-
 ↪pwd.txt
rm /tmp/ssd-pwd.txt
set -o history
exit
```

Результат выполнения команды:

```
Temporary password added to cache entry for olegovo@ald.company.lan
```

Проверить результат кэша командой:

```
sudo ldbsearch -H /var/lib/sss/db/cache_ald.company.lan.ldb -b
 ↪name=olegovo@ald.company.lan,cn=users,cn=ald.company.lan,cn=sysdb
 ↪cachedPassword
```

Результат выполнения команды:

```
...
dn: name=olegovo@ald.company.lan,cn=users,cn=ald.company.lan,cn=sysdb
 ↪cachedPassword:
$6$0Xa5CIrB1WRICTmM$eJ0bVItqEQeSfx6/B3.bodGHdn//uMuAYk.9fCnvcL.7iGdka/
 ↪Uhrn5TrV4HxKznikXeXc82LQcT/d1CYvWig.
...
```

Имя пользователя должно быть известно в домене, иначе команда не сможет получить его идентификатор и другие сведения. Если на момент выполнения команды пользователь уже входил в это устройство, то утилита переопределит кэш его пароля.

2.6.2. Автоматическая Kerberos аутентификация при переходе в онлайн режим

Хэш **SHA512** отлично подходит для долгосрочного хранения секретов на диске, но с его помощью не получится пройти Kerberos-аутентификацию, поэтому при входе в компьютер в автономном режиме служба **SSSD** помещает пароль в связку ключей ядра Linux, чтобы иметь возможность выписать **TGT**-билет, когда связь с сервером будет восстановлена. За возможность автоматической Kerberos-аутентификации пользователя при переключении в онлайн режим отвечает параметр **krb5_store_password_if_offline**, который по умолчанию

равен **True**.

Если потребуется, извлечь пароль из **Keyring**, можно с помощью утилиты **keyctl**, но из-за настроек прав доступа выполнять эти команды нужно будет в контексте процесса службы **SSSD**. Подключиться к действующему процессу можно с помощью отладчика **gdb** (GNU Debugger), для работы которого нужно будет отключить блокировку функции **ptrace**. Продемонстрируем данную технику, для этого сначала установим отладчик и отключим блокировку **ptrace**.

```
sudo apt install gdb
sudo astra-ptrace-lock disable
sudo reboot
```

После перезагрузки выполняется вход в систему тем же пользователем и смотрится `pid` службы **sssd** для подключения к процессу **Монитора** и номер текущего окна терминала для перенаправления стандартного вывода. Сетевая связанность компьютера **pc-1** с **контроллером домена** в этот момент должна быть заблокирована, т.к. после получения **TGT**-билета пароль больше не требуется и будет удален из связки ключей.

Найти идентификатор процесса можно командой:

```
pidof sssd
```

Результат выполнения потребуется для подключения к процессу **sssd**:

```
487
```

Вычисляется устройство текущего терминала для вывода:

```
tty
```

Результат вывода:

```
/dev/pts/0
```

Теперь осталось только подключиться к процессу, чтобы извлечь содержимое ключа.

```
sudo gdb -p 487
```

В результате подключиться к процессу через отладчик **gdb**:

```
GNU gdb (AstraLinuxSE 8.2.1-2) 8.2.1
...
(gdb) _
```

Для выхода из отладчика ввести команду q.

Выполнить команду gdb для получения связки ключей:

```
call system("keyctl show > /dev/pts/0")
```

Результат выполнения, где важен идентификатор ключа 835659210:

```
Session Keyring
 84684334 --alswrv      0     0  keyring: _ses
835659210 --alswrv      0     0   \_ user: admin@ald.company.lan
...
```

Выполнить запрос данных по идентификатору 835659210 на терминал */dev/pts/0*:

```
call system("keyctl print 835659210 > /dev/pts/0")
```

Результат выполнения:

```
[Detaching after fork from child process 7834]
AstraLinux_172
$2 = 0
```

Технология автоматической Kerberos аутентификации при переходе в онлайн режим является безопасной, потому что:

- пароль хранится в оперативной памяти и не сохраняется в системе при выключении компьютера;
- пароль хранится в системе ограниченное время и автоматически удаляется при появлении связи с контроллером домена;
- извлечь пароль может только пользователь, обладающий привилегиями суперпользователя.

2.7. Динамическое обновление DNS-записей в домене

Компьютеры в домене взаимодействуют между собой по DNS-именам, поэтому в каталоге важно иметь актуальную информацию по используемым IP адресам. С серверами обычно не возникает проблем, т.к. им назначаются статические адреса, а вот интерфейсы рабочих станций настраиваются динамически, поэтому администраторам нужно обеспечить такое же динамическое обновление этой информации в каталоге.

Обновление DNS-записей возможно как по инициативе DHCP-сервера (Remote Name Daemon Control, **RNDC**), так и по инициативе рабочей станции (**GSS-TSIG**). У каждого из подходов есть свои сильные и слабые стороны, но продуктовой команде ALD Pro второй способ видится наиболее простым и безопасным, так как в этом случае запросы на обновление DNS-записей авторизуются с помощью Kerberos-аутентификации.

Для настройки динамического обновления DNS-записей в конфигурационном файле */etc/sssd/sssd.conf* на стороне рабочей станции нужно добавить следующие параметры:

```
[domain/ald.company.lan]
...
dyndns_update = true
dyndns_refresh_interval = 43200
dyndns_update_ptr = true
dyndns_ttl = 3600
...
```

После внесения указанных изменений можно перезапустить службу **sssd** и проверить обновление записей в каталоге при изменении IP-адреса на хосте.

2.8. Отладка работы службы SSSD

Служба **SSSD** предоставляет две основные функции: получение информации о пользователях и их аутентификацию. Каждая из этих функций использует свои программные интерфейсы, поэтому должна рассматриваться отдельно. Однако успешная аутентификация возможна, только если информация о пользователе получена успешно, поэтому, если что-то не работает, то в первую очередь нужно убедиться, что возможно получить хотя бы информацию о пользователе с помощью команд `getent` и `id`:

```
getent passwd $USER
```

Результат выполнения:

```
admin:*:1421600000:1421600000:Administrator:/home/admin:/bin/bash
```

Выполнить команду `id`:

```
id $USER
```

Результат выполнения:

```
uid=959800000(admin) gid=959800000(admins) группы=959800000(admins),
↪1001(astra-admin),113(lpadmin)
```

2.8.1. Журналы отладки SSSD

Служба **SSSD** состоит из множества компонентов и для настройки каждого из них в конфигурационном файле предназначена отдельная секция (например, за настройки монитора отвечает секция `[sssd]`, а **Бэкенд** настраивается в секции `[domain/...]`), поэтому для включения отладки конкретного компонента в его секции следует задать параметр `debug_level=N`, где **N** - это число от 1 до 10.

Уровни отладки 1-3 регистрируют сбои, а уровни 8-10 обеспечивают излишнюю детализацию, которая затрудняет быстрый анализ журналов, поэтому для решения большинства проблем начать лучше с шестого уровня. Открыть конфигурацию командой:

```
sudo cat /etc/sssd/sssd.conf
```

Результат выполнения:

```
[domain/ald.company.lan]
debug_level = 10
id_provider = ipa
...
[sssd]
debug_level = 10
services = ifp
domains = ald.company.lan
[nss]
debug_level = 10
homedir_substring = /home
...
```

Уровень отладки можно менять не только через конфигурационный файл, но и «на лету» без перезагрузки службы **SSSD**, отправляя ей команды через **SBus** с помощью утилиты **sssctl** из пакета **sssd-tools**. Очистить логи, чтобы удобно было смотреть отладочную информацию:

```
sudo sssctl logs-remove
```

Изменить уровень отладки командой и просмотреть в лог файле изменение `grep` „Debug level changed“:

```
sudo sssctl debug-level 6
sudo cat /var/log/sssd/sssd.log | grep 'Debug level changed'
```

Результат выполнения отображает начало нужного события:

```
(2023-08-20 22:17:00): [sssd] [server_common_rotate_logs] (0x0010): Debug
↪level changed to 0x07f0
```

Повысить уровень логирования до 8:

```
sssctl debug-level 8
cat /var/log/sssd/sssd.log | grep 'Debug level changed'
```

В результате можно увидеть два события начало и конец. Это нужно для удобного просмотра лога, чтобы знать где искать интервал отладочной информации от и до:

```
...[sssd] [server_common_rotate_logs] (0x0010): Debug level changed to 0x07f0
...[sssd] [server_common_rotate_logs] (0x0010): Debug level changed to 0x37f0
```

Выбрать все строки между кодами смены уровня отладки **0x07f0** и **0x37f0** можно с помощью `regex` запроса:

```
cat /var/log/sssd/sssd.log | grep -zoP '(?<=0x07f0)(?s).*(?=0x37f0)'
```

В операционной системе Astra Linux журналы отладки хранятся в папке */var/log/sssd*, по одному файлу журнала на каждый компонент. **Ответчики** пишут в файлы с именами *SSSD_$service*, например, собеседник **NSS** пишет в файл */var/log/sssd/sssd_nss.log*. Сообщения от **Бэкенда** пишутся в файл с именем *sssd_$domainname.log*. Есть еще журналы вспомогательных процессов, таких как *ldap_child.log u krb5_child.log*.

Прежде чем погружаться в изучение журналов и файлов конфигурации, желательно внимательно ознакомиться с описанием архитектуры службы **SSSD**.

Во многих случаях полезно воспроизвести ошибку после очистки кэша, чтобы исключить его влияние, но важно помнить, что в локальной базе кэшируются также и учетные данные, поэтому не стоит удалять кэш, если работа идет в автономном режиме. А также важно обратить внимание, что приведенные примеры сообщений отладки могут меняться для последующих релизов.

2.8.2. Общие рекомендации

Если команды `getent` или `id` не выводят вообще никакой информации о пользователе или группе, то нужно проверить:

- Работу службы разрешения имен командой `ping dc-1` и, указаны ли в */etc/resolv.conf* правильные DNS-сервера.
- Работает ли служба с помощью команды `systemctl status sssd`.
- Конфигурацию */etc/nsswitch.conf*, что модуль **sss** указан для следующих баз данных: **passwd**, **group**, **shadow**, **services**, **netgroup**, **sudoers**, **automount**.
- Поведение команды `id` на контроллере домена ALD Pro.
- Доходит ли запрос до **Ответчика**. Для этого в разделе `[nss]` установите `debug_level = 6` и перезапустите службу **sssd**.

Приведем пример успешного запроса информации по пользователю.

```
[sssd[nss]] [get_client_cred] (0x4000): Client creds: euid[10327]
↪egid[10327] pid[18144].
[sssd[nss]] [setup_client_idle_timer] (0x4000): Idle timer re-set for client
↪[0x13c9960][22]
[sssd[nss]] [accept_fd_handler] (0x0400): Client connected!
[sssd[nss]] [sss_cmd_get_version] (0x0200): Received client version [1].
[sssd[nss]] [sss_cmd_get_version] (0x0200): Offered version [1].
[sssd[nss]] [nss_getby_name] (0x0400): Input name: admin
```

Если команда достигает **Ответчика NSS**, передается ли она **Поставщику** данных (Data Provider). Неудачный запрос может выглядеть так:

```
[sssd[nss]] [cache_req_search_dp] (0x0400): CR #3: Looking up [admin@ipa.
↪test] in data provider
[sssd[nss]] [sss_dp_issue_request] (0x0400): Issuing request for
↪[0x41e51c:1:admin@ipa.test@ipa.test]
[sssd[nss]] [sss_dp_get_account_msg] (0x0400): Creating request for [ipa.
↪test][0x1][BE_REQ_USER][name=admin@ipa.test:-]
[sssd[nss]] [sss_dp_internal_get_send] (0x0400): Entering request
↪[0x41e51c:1:admin@ipa.test@ipa.test]
[sssd[nss]] [sss_dp_req_destructor] (0x0400): Deleting request:
↪[0x41e51c:1:admin@win.trust.test@win.trust.test]
[sssd[nss]] [sss_dp_get_reply] (0x0010): The Data Provider returned an error
↪[org.freedesktop.sssd.Error.DataProvider.Offline]
[sssd[nss]] [cache_req_common_dp_recv] (0x0040): CR #3: Data Provider Error:
↪3, 5, Failed to get reply from Data Provider
[sssd[nss]] [cache_req_common_dp_recv] (0x0400): CR #3: Due to an error we
↪will return cached data
```

Успешно обработанный запрос напротив будет выглядеть так:

```
[sssd[nss]] [cache_req_search_dp] (0x0400): CR #3: Looking up [admin@ipa.
↪test] in data provider
[sssd[nss]] [sss_dp_issue_request] (0x0400): Issuing request for
↪[0x41e51c:1:admin@ipa.test@ipa.test]
[sssd[nss]] [sss_dp_get_account_msg] (0x0400): Creating request for [ipa.
↪test][0x1][BE_REQ_USER][name=admin@ipa.test:-]
[sssd[nss]] [sss_dp_get_reply] (0x1000): Got reply from Data Provider - DP
↪error code: 0 errno: 0 error message: Success
[sssd[nss]] [cache_req_search_cache] (0x0400): CR #3: Looking up [admin@ipa.
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
↪test] in cache
```

Если запрос к **Поставщику** данных успешно завершен, но по-прежнему не отображаются результаты, следует переходить к журналам **Бэкенда**.

2.8.3. Отладка Бэкенда

Бэкенд выполняет несколько различных операций, поэтому бывает трудно сразу понять, в чем заключается проблема. На самом высоком уровне **Бэкенд** выполняет следующие шаги в указанном порядке:

1. **Бэкенд** получает запрос от клиентской библиотеки и решает, к какому серверу следует подключиться для его обработки. Этот шаг может включать в себя поиск по **SRV**-записям.

2. **Бэкенд** устанавливает соединение с сервером и проходит аутентификацию, используя учетные данные из keytab-файла хоста, если это требуется.

3. Как только соединение установлено, **Бэкенд** отправляет запрос на поиск информации, поэтому вы должны увидеть в запросе критерии фильтрации, базовую запись и запрашиваемые атрибуты.

4. После того, как поиск завершится, соответствующие записи будут сохранены в кэше. Код состояния возвращается **собеседнику**. Установите `debug_level=6` в разделе `[domain/]`, перезапустите службу и выполните еще раз неудачный поиск информации о пользователе. При отладке работы **Бэкенда** в первую очередь убедитесь, что **Бэкенд** находится в режиме **онлайн**, сделать это можно с помощью утилиты **sssctl**.

```
sudo sssctl domain-status ald.company.lan
```

Результат выполнения:

```
Online status: Online

Active servers:
IPA: dc-1.ald.company.lan

```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
Discovered IPA servers:
- dc-1.ald.company.lan
```

Проверить, можно ли установить соединение с теми же параметрами безопасности, которые использует **SSSD**:

```
kinit -k && klist
```

Результат выполнения:

```
Ticket cache: KEYRING:persistent:959800000:krb_ccache_pMxi5Bu
Default principal: host/dc-1.ald.company.lan@ALD.COMPANY.LAN

Valid starting       Expires              Service principal
20.08.2023 23:15:25  21.08.2023 23:15:25  krbtgt/ALD.COMPANY.LAN@ALD.COMPANY.
 ↪LAN
```

Проверить запрос в **LDAP**, где Ключи `-H` и `-ZZ` делают запрос ближе к тому, как служба **SSSD** взаимодействует с каталогом:

```
ldapsearch -ZZ -H ldap://dc-1.ald.company.lan -b uid=admin,cn=users,
 ↪cn=accounts,dc=ald,dc=company,dc=lan cn
```

Результат выполнения:

```
# admin, users, accounts, ald.company.lan
dn: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
cn: Administrator
```

Для отладки **GSSAPI** аутентификации команду `kinit` можно использовать в сочетании с переменной окружения `KRB5_TRACE`. Если установлен для **Бэкенда** десятый уровень, то информация о трассировке Kerberos аутентификации будет отражаться также в журнале *ldap_child.log*.

```
sudo i
set +o history
env KRB5_TRACE=/dev/stdout kinit <<< AstraLinux_176
set -o history
exit
```

Результат выполнения:

```
[23001] 1696515238.426608: Getting initial credentials for admin@ALD.COMPANY.
↪LAN
[23001] 1696515238.426610: Sending unauthenticated request
[23001] 1696515238.426611: Sending request (191 bytes) to ALD.COMPANY.LAN
[23001] 1696515238.426612: Initiating TCP connection to stream 10.0.1.11:88
[23001] 1696515238.426613: Sending TCP request to stream 10.0.1.11:88
[23001] 1696515238.426614: Received answer (514 bytes) from stream 10.0.1.
↪11:88
[23001] 1696515238.426615: Terminating TCP connection to stream 10.0.1.11:88
[23001] 1696515238.426616: Response was from master KDC
...
[23001] 1696515238.426651: Storing admin@ALD.COMPANY.LAN → krb5_ccache_conf_
↪data/pa_type/krbtgt\/ALD.COMPANY.LAN\@ALD.COMPANY.LAN@X-CACHECONF: in
↪KEYRING:persistent:1421600000:krb_ccache_kFlzpn6
```

Необходимо проверить, присутствуют ли на сервере все атрибуты, необходимые для службы **SSSD**, правильно ли указана база поиска, особенно для доверенных поддоменов. По возможности, выполнить такой же поиск вручную утилитой **ldapsearch**.

2.8.4. Устранение неисправностей аутентификации, изменения пароля и контроля доступа

Если информация о пользователе может быть успешно получена, но аутентификация не проходит, то в первую очередь нужно смотреть журнал */var/log/auth.log* на предмет сообщений от **pam_sss**. Аутентификация начинается в **PAM**-стеке на фазе **auth** и выполняется с помощью провайдера аутентификации (auth_provider) службы **SSSD**. Однако, не все запросы на аутентификацию проходят через **SSSD**, например, аутентификация по **SSH** происходит непосредственно в **SSHD**, а **SSSD** взаимодействует с **PAM** стеком только на фазе **account**. Контроль доступа начинается в **PAM** стеке на фазе **account** и выполняется с помощью провайдера доступа (access_provider) службы **SSSD**.

Смена пароля начинается на стороне **PAM** стека на фазе **password** и выполняется с помощью провайдера смены пароля (chpass_provider) службы **SSSD**.

Аутентификация через **PAM** стек происходит по следующему шаблону:

1. Приложение с поддержкой **PAM** аутентификации начинает диалог. В зависимости от

настроек **PAM**-стека в диалог может быть вовлечен модуль **pam_sss**. Для отладки процесса аутентификации, сначала нужно проверить журнал */var/log/auth.log* на предмет того, есть ли вообще обращения к **pam_sss**. Если нет упоминания **pam_sss**, скорее всего, **PAM** стек настроен неправильно. Если обращения к **pam_sss есть**, нужно включить отладку для **Ответчика PAM**.

2. **Ответчик PAM** службы **SSSD** получает запрос на аутентификацию и в большинстве случаев пересылает его **Бэкенду**. Важно обратить внимание, что в отличие от запросов на идентификацию, запросы на аутентификацию и контроль доступа обычно не кэшируется и всегда завершаются обращением к **серверу**. В некоторых случаях это может приводить к задержкам, но это достаточно важно, потому что дополнительные группы в GNU/Linux устанавливаются только в момент входа в систему.

Журналы **собеседника PAM** должны показывать запросы, которые пришли от **PAM**-стека и были перенаправлены на **Бэкенд**. Если отображается запрос на аутентификацию к **собеседнику PAM**, но получается ошибка от **Бэкенда**, важно проверить журналы **Бэкенда**.

Пример ошибки может выглядеть как:

```
[sssd[pam]] [sss_dp_issue_request] (0x0400): Issuing request for
 ↪[0x411d44:3:admin@ipa.example.com]
[sssd[pam]] [sss_dp_get_account_msg] (0x0400): Creating request for [ipa.
 ↪example.com][3][1][name=admin]
[sssd[pam]] [sss_dp_internal_get_send] (0x0400): Entering request
 ↪[0x411d44:3:admin@ipa.example.com]
[sssd[pam]] [sss_dp_get_reply] (0x1000): Got reply from Data Provider - DP
 ↪error code: 1 errno: 11 error message: Offline
[sssd[pam]] [pam_check_user_dp_callback] (0x0040): Unable to get information
 ↪from Data Provider Error: 1, 11, Offline
```

3. **Бэкенд** обрабатывает запрос. Это может включать эквивалент выполнения команды `kinit` в процессе **krb5_child**, аутентификацию по **LDAP** или проверку по списку контроля доступа. После того, как запрос к **Бэкенду** завершится, результат отправляется обратно **собеседнику PAM**. Важно посмотреть также файл *krb5_child.log*, если установить уровень отладки `debug_level = 10`, то в этот файл будет включаться также низкоуровневая информация для трассировки работы протокола Kerberos. Также можно имитировать аутентификацию вручную с помощью утилиты **kinit**.

4. **Ответчик PAM** получает результат и пересылает его обратно в модуль **pam_sss**. Сообщения об ошибке или статусе отображается в */var/log/auth.log*.

2.9. Расположение значимых файлов

В качестве сводной информации по значимым компонентам продукта ALD Pro в табл. 7 представлен список файлов для отладки системы, в которых хранятся конфигурации компонентов и журналы работы этих компонентов.

Компонент системы	Конфигурация	Файл журнала
SSSD	/etc/sssd/sssd.conf	/var/log/sssd/
PAM	/etc/pam.d/system-auth	/var/log/sssd/sssd_pam.log
NSS	/etc/nsswitch.conf	/var/log/sssd/sssd_nss.log
krb5_child	/etc/sssd/sssd.conf	/var/log/sssd/krb5_child.log
ldap_child	/etc/sssd/sssd.conf	/var/log/sssd/ldap_child.log
Data Provider (Backend)	/etc/sssd/sssd.conf	/var/log/sssd/sssd_<domainFQDN>.log
DNS	/etc/resolv.conf	journalctl -u bind9-pkcs11.service
Samba	/etc/samba/smb.conf	/var/log/samba/*.log
Winbind	/etc/security/pam_winbind.conf	/var/log/samba/log.*
Kerberos	/etc/krb5.conf	/var/log/sssd/krb5_child.log
salt-master	/etc/salt/	/var/log/salt/master
aldpro-salt-minion	/etc/aldpro-salt/	/var/log/aldpro-salt/minion

Таблица 7 — Расположение значимых файлов

Справочные материалы

3.1. Создание дополнительных параметров групповых политик

3.1.1. Функционал групповых политик

Групповые политики позволяют снизить стоимость управления ИТ-инфраструктурой за счет автоматического применения одинаковых настроек на больших группах компьютеров, имеющих общее целевое назначение.

Каждая политика (в терминах MS объект групповой политики) представляет из себя именованный набор параметров, в соответствии с которыми производится автоматическая настройка операционной системы и прикладного программного обеспечения. Для настройки групповой политики нужно выполнить следующие действия:

- создать новую групповую политику
- добавить конфигурационный параметр в политику (включить его)
- установить желаемые значения атрибутов для параметра
- назначить политику на подразделение, внутри которого есть целевые компьютеры или пользователи
- подождать от 30 минут до 80 минут или изменить таймер для получения и применения политики

Администраторам доступны сотни параметров «из коробки», которые соответствуют настройкам панели управления ОС Astra Linux. Но для решения частных задач конкретного бизнеса может потребоваться разработка дополнительных параметров силами команды внедрения, и в ALD Pro для этого есть все необходимые инструменты.

3.1.2. Как работают групповые политики

Для получения данных групповых политик и их применения используется pull-модель. Инициатором работы является миньон SaltStack (standalone minion), установленный на каждом компьютере домена, который по протоколу LDAP к серверу службы каталогов получает актуальные данные о групповой политике.

- Миньон Standalone — это рабочие станции или серверы, на которых работает демон-миньон Salt, обладающий широкой функциональностью, работающий автономно от мастера. Используется для запуска заданий в системе без подключения к мастеру.

Важно: Получение данных групповых политик и применение политик с помощью standalone миньона реализовано с версии ALD Pro 2.2.0, ранее для этих задач использовался стандартный миньон SaltStack, который получал данные от мастера.

3.1.3. Как создать дополнительный параметр

Привилегия	Описание	На что распространяется
Computer Group Policy Additional Parameters Catalog - Read	Привилегия позволяет: • Видеть список параметров компьютеров (Управление доменом/Доп. параметры групповых политик/вкладка Параметры компьютеров); • Видеть список папок компьютеров (Управление доменом/Доп. параметры групповых политик/вкладка Параметры компьютеров); • Видеть карточки параметров компьютеров (Управление доменом/Доп. параметры групповых политик/вкладка Параметры компьютеров/<Параметр компьютеров>); • Видеть карточки папок параметров компьютеров (Управление доменом/Доп. параметры групповых политик/вкладка Параметры компьютеров/<Папка параметров компьютеров>)	На весь домен

продолжение на следующей странице

Таблица 3.1 – продолжение с предыдущей страницы

Привилегия	Описание	На что распространяется
User Group Policy Additional Parameters Catalog - Read	Привилегия позволяет: • Видеть список параметров пользователей (Управление доменом/Доп. параметры групповых политик/вкладка Параметры пользователей); • Видеть карточки параметров пользователей (Управление доменом/Доп. параметры групповых политик/вкладка Параметры пользователей/<Параметр пользователей>)	На весь домен

продолжение на следующей странице

Таблица 3.1 – продолжение с предыдущей страницы

Привилегия	Описание	На что распространяется
Computer Group Policy Additional Parameters - Manage	Привилегия позволяет: • Создавать новые папки параметров компьютеров (Управление доменом/Доп. параметры групповых политик/вкладка Параметры компьютеров); • Изменять папки параметров компьютеров (Управление доменом/Доп. параметры групповых политик/вкладка Параметры компьютеров/<Папка параметров компьютеров>); • Удалять папки параметров компьютеров (Управление доменом/Доп. параметры групповых политик/вкладка Параметры компьютеров/<Папка параметров компьютеров>); • Создавать новые параметры компьютеров (Управление доменом/Доп. параметры групповых политик/вкладка Параметры компьютеров); • Изменять параметры компьютеров (Управление доменом/Доп. параметры групповых политик/вкладка Параметры компьютеров/<Параметр компьютеров>);	На весь домен

Таблица 3.1 – продолжение с предыдущей страницы

Привилегия	Описание	На что распространяется
User Group Policy Additional Parameters - Manage	Привилегия позволяет: • Создавать новые папки параметров пользователей (Управление доменом/Доп. параметры групповых политик/вкладка Параметры пользователей); • Изменять папки параметров пользователей (Управление доменом/Доп. параметры групповых политик/вкладка Параметры пользователей/<Папка параметров пользователей>); • Удалять папки параметров пользователей (Управление доменом/Доп. параметры групповых политик/вкладка Параметры пользователей/<Папка параметров пользователей>); • Создавать новые параметры пользователей (Управление доменом/Доп. параметры групповых политик/вкладка Параметры пользователей); • Изменять параметры пользователей (Управление доменом/Доп. параметры групповых политик/вкладка Параметры компьютеров/<Параметр пользователей>);	На весь домен

Таблица 3.1 – продолжение с предыдущей страницы

Привилегия	Описание	На что распространяется

Привилегии для работы с дополнительными параметрами ГП

Параметр групповой политики (в терминах MS шаблон групповой политики) подобен классу из теории объектно-ориентированного программирования. Он определяет модель для создания объектов конфигурирования, описывая их свойства (атрибуты) и методы для работы с этими данными (скрипт). Продолжая аналогию из ООП, «объектом» в данном случае будет являться экземпляр параметра, добавленный в конкретную групповую политику.

Параметр может быть «простым» или «составным»:

- В случае **простого** параметра свойства представляют из себя плоский список атрибутов. Например, для настройки межсетевого экрана может потребоваться задать уровень детализации журнала, и эта настройка подразумевает одно конкретное значение, поэтому она может быть реализована атрибутом «простого» параметра.
- **Составные** параметры позволяют задавать массив списка атрибутов, где в каждом списке представлен однотипный набор данных. Если продолжать пример с межсетевым экраном, то для настройки фильтрации может потребоваться разрешить входящие ssh-соединения, запретить исходящие smtp и т.п., поэтому такие настройки нужно реализовывать атрибутами «составного» параметра.

Параметр может быть «параметром компьютера» или «параметром пользователя». «Параметры компьютеров» отвечают за настройку оборудования и служб вне зависимости от того, какой пользователь работает с системой. «Параметры пользователей» отвечают за настройку рабочей среды пользователя вне зависимости от того, на каком компьютере он работает. В обоих случаях скрипты выполняются с возможностями по администрированию root-пользователя.

Чтобы создать новый параметр групповой политики нужно перейти на страницу **Управление доменом - Доп. параметры групповых политик** и выбрать одну из вкладок:

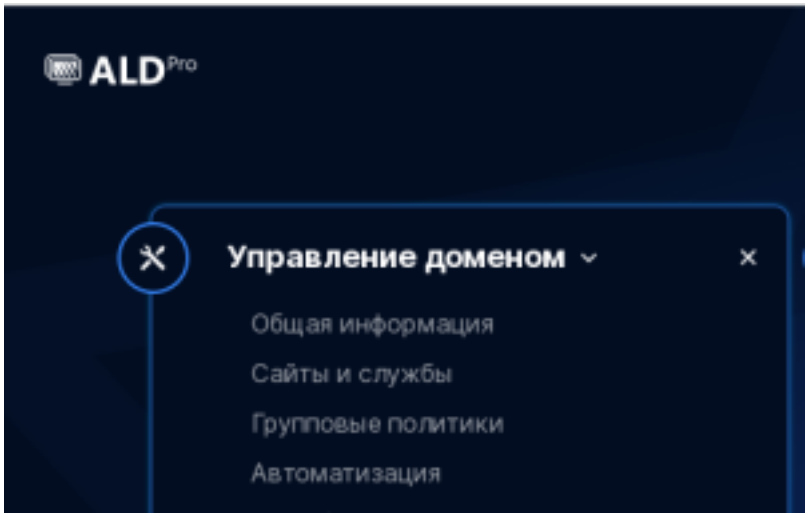


Рисунок 3.1 – Как создать дополнительный параметр 1

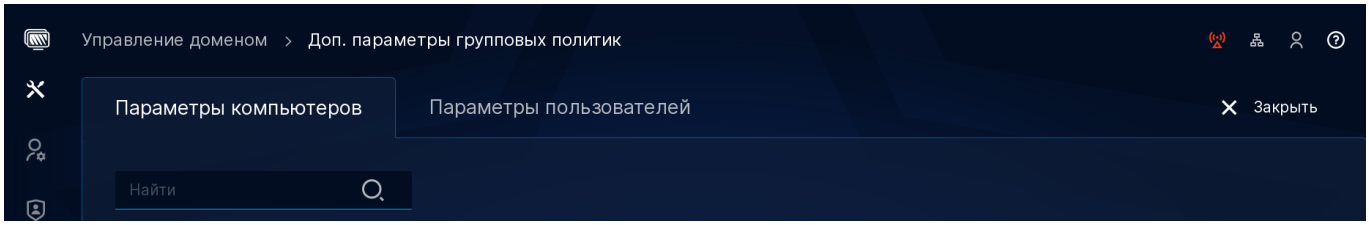


Рисунок 3.2 – Как создать дополнительный параметр 2

На каждой вкладке по умолчанию будет представлен корневой каталог «Каталог дополнительных параметров», внутри которого вы можете создавать свои пользовательские параметры. Если параметров станет слишком много, вы сможете группировать их по подразделам.

Выберите раздел «Каталог дополнительных параметров», нажмите кнопку «+ Новый параметр» и заполните карточку следующими значениями:

Раздел «Основные»

- Название параметра: «Диспетчер задач htop». Это название, которое будет отображаться в каталоге при редактировании групповых политик на портале управления.
- Уникальный идентификатор: «software_htop». Это название, которое будет использоваться в качестве имени `\*.sls` файла на диске и в скриптах SaltStack. Формируется по следующей формуле: `rbta_ldap_custom_gp_host_` + введенные пользователем данные «software_htop». Для пользователей `rbta_ldap_custom_gp_user_`.

- Тип каталога: «Параметр компьютерной групповой политики». Определяет, относится ли данный параметр к настройкам компьютера или пользователя. Параметр не доступен для редактирования, его значение определяется автоматически в зависимости от того, с какой страницы вы перешли к созданию дополнительного параметра.
- Тип параметра: «простой». Определяет вид параметра. **Простой** - простой список атрибутов, **Составной** - массив списка атрибутов.
- Папка параметра: «Дополнительные параметры». Указывает раздел каталога, в котором будет доступен данный параметр.
- Назначение параметра: «Управление установкой и настройкой диспетчера задач htop». Текстовое описание, позволяющее указать наиболее важную информацию о работе параметра для удобства последующего использования. Данный текст отображается при редактировании групповой политики по нажатию кнопки вопроса. Здесь же можно внести данные о требованиях к ОС (см. resource_planning).
- Разделы **Атрибуты параметра** и **Конфигурация скрипта** станут доступны при редактировании сохраненного параметра.

3.1.3.1. Особенности редактирования дополнительных параметров ГП

Для редактирования дополнительного параметра групповых политик нужно перейти на страницу **Управление доменом Доп. параметры групповых политик Параметры компьютеров или Параметры пользователей “Имя параметра”** и внести нужные изменения. После сохранить.

Чтобы эти параметры синхронизировались с групповыми политиками и применились на компьютерах и пользователях нужно перейти на карточку этих политик **Групповые политики Групповые политики “Имя политики”**, внести изменения и сохранить. Изменения в групповой политике приведут к повышению ее версии. Только после этого изменения дополнительных параметров ГП будут применены на компьютерах и для пользователей. Или принудительно применить политику (подробнее читайте в *Отладка*).

Аналогичные действия необходимо применить если дополнительный параметр групповой политики был удален.

3.1.4. Как настроить атрибуты дополнительного параметра

Атрибуты — это свойства, которые можно задавать при добавлении параметра к групповой политике. Например, если мы создадим параметр для управления диспетчером задач `htop` на рабочих станциях, то нам понадобится атрибут «Должен быть установлен», чтобы в зависимости от его значения устанавливать или удалять указанное программное обеспечение.

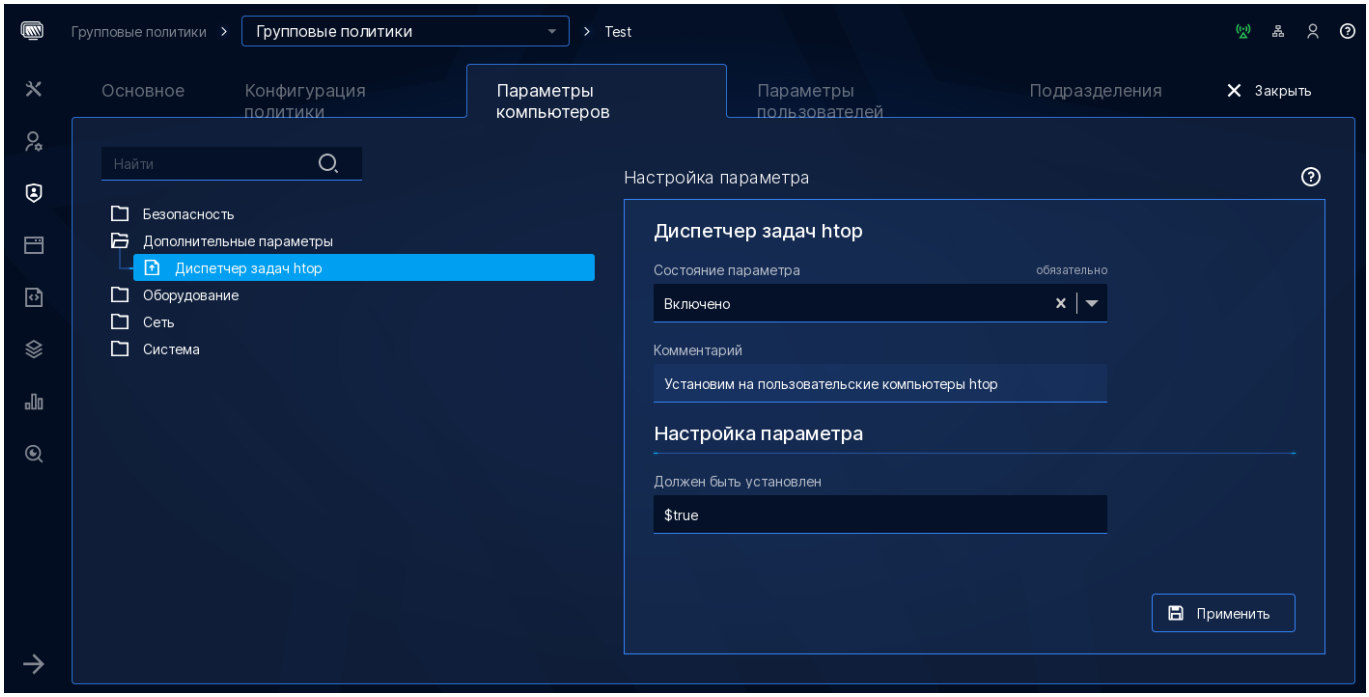


Рисунок 3.3 – Как настроить атрибуты дополнительного параметра

Атрибуты представляют из себя обычные текстовые строки, значение которых может быть интерпретировано в скриптах в том числе как числа, логические значения ($true и $false), списки и т.п. Добавьте атрибут:

- Название атрибута: «Должен быть установлен»

Название, под которым будут видеть этот атрибут на карточке параметра.

- Уникальный идентификатор: «must_be_installed»

Идентификатор атрибута, который будет использоваться как имя переменной в SaltStack скриптах.

- Описание: «атрибут используется как логическая переменная true / false для ветвления шаблона»

Краткие комментарии для инженера, которые помогут упростить поддержку этого атрибута в будущем, когда потребуется внести какие-либо изменения. Данная информация недоступна при настройке групповой политики, поэтому, если вы хотите дать подсказку администратору о возможных значениях этого атрибута, внесите эту информацию в описание параметра.

- Обязательный: `true`

Пользователь должен указать значение атрибута

- Уникальный: `true`

Применяется для составных параметров, у которых возможны конфликты. Для разрешения конфликтов для каждого параметра нужно определить уникальный атрибут. В рамках одного ГПО нельзя будет создать массив списка атрибутов с одинаковыми значениями уникального параметра.

3.1.5. Скрипт дополнительного параметра

Скрипты SaltStack похожи на PHP, в них текст перемежается императивными инструкциями языка программирования, по результату выполнения которых получается итоговый документ. За императивную часть отвечают инструкции шаблонизатора Jinja2, а декларативная часть задается по правилам SaltStack в YAML-подобном синтаксисе.

3.1.5.1. Императивные инструкции шаблонизатора Jinja

Инструкции языка Jinja внедряются с помощью фигурных скобок:

- `{% … %}` - синтаксис для вставки инструкции языка шаблонизатора Jinja. Аналог PHP: `<? … ?>`
- `{% print(…) %}` - пример инструкции для вывода в документ по месту вызова значения выражения. Аналог PHP: `<? echo (…) ?>`
- `{{ … }}` - краткий синтаксис для вывода в документ по месту вызова значения выражения. Аналог PHP: `<?= … ?>`
- `{### … #}` - синтаксис для вставки комментариев средствами языка Jinja2. Аналог PHP: `<?/* … */?>`

Для повышения читабельности кода управляющие структуры обычно оформляют

отступами, но yaml-документы крайне чувствительны к пробелам, поэтому данный инструмент форматирования оказывается недоступен без применения специальных операторов подавления отступов. Чтобы убрать лишние пробелы и пустые строки вам нужно всего лишь поставить знак дефиса слева, справа или с обоих концов управляющего блока:

- `{%-` - удаляет пробелы и пустые строки слева;
- `-%}` - удаляет перенос текущей строки и переносит ее на предыдущую;
- `{%-` и `-%}` - удаляет пробелы и пустые строки слева, в т.ч. перенос текущей строки, поэтому текст окажется в конце предыдущей строки.

> **Внимание:** При сохранении скрипта может появится предупреждение: «Ошибка конфигурации скрипта. Игнорировать ошибку и сохранить изменения?». Встроенный механизм проверяет соответствие указного скрипта формальным правилам, поэтому если есть уверенность, что скрипт корректный необходимо выбирать «Да» для сохранения.

Выполнение команд

Создайте файл `hello.sls` с простейшим Jinja-скриптом, чтобы проверить, как это работает, и выполните его с помощью команды `aldpro-salt-call` с указанными параметрами:

```
echo '{% do salt.log.info("Hello world!") %}' > hello.sls
aldpro-salt-call --local --file-root=. state.sls hello
```

Несколько комментариев:

- Оператор «do» вызывает метод `salt.log.info` с параметром „Hello world!“
- Команда `aldpro-salt-call` отвечает за локальное исполнение скриптов на миньонах.
- Параметр `local` исключает обращение к мастеру для получения настроек.
- Параметр `file-root` со значением «.» устанавливает в качестве рабочего каталога текущую директорию.
- Параметр `state.sls` указывает на то, что следует использовать метод sls модуля `salt.modules.state`, который применяет состояния, описанные в одном и более

файлов на диске из рабочей директории.

- Параметр `hello` задает имя файла `hello.sls`, которое должно быть указано без расширения файла.

Еще один пример. С помощью метода run модуля cmd можно выполнить на удаленном хосте любую команду `bash`:

```
echo '{% do salt.cmd.run("apt-get install htop") %}' > installhtop.sls
aldpro-salt-call --local --file-root=. state.sls installhtop
```

Полный перечень всех модулей SaltStack можно найти на странице документации: https://docs.saltproject.io/en/latest/ref/modules/all/index.html

Работа с переменными

Переменные на языке Jinja задаются оператором `set`. Вам доступен широкий перечень типов данных: булевые, числовые, текстовые, списки, кортежи, словари:

```
{% set boolean_val = True %}
{% set int_val = 777 %}
{% set string_val = 'hello' %}
{% set list_val = ['h', 'e', 'l', 'l', 'o'] %}
{% set tuple_val = ('h', 'e', 'l', 'l', 'o') %}
{% set dict_val = { b: True, i: 777, s: 'hello') %}
```

При работе с числовыми переменными доступны обычные математические операторы:

```
{% set a = 5 %}
{% set b = 10 %}
{% set a = a + b %}
{% set b = a - b %}
{% set a = a - b %}
```

Конкатенация строк возможна как специальным оператором «~», который предварительно конвертирует все значения в строки, так и обычным оператором сложения «+»:

```
{% set a = 5 %}
{% set b = 10 %}
{% set c = a ~ b %}
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
{% set d = 'World' %}
{% set e = 'Hello, ' + d %}
```

Для выполнения более сложных преобразований над переменными доступно множество функций, которые можно применять как методы через точку или в стиле конвейеров bash через символ вертикальной черты, за что их так же называют фильтрами:

```
{% set a = 'Hello'.upper() %}
{% set b = 'world' | upper %}
```

Полный перечень встроенных фильтров Jinja можно найти в документации: https://jinja.palletsprojects.com/en/2.11.x/templates/#list-of-builtin-filters

Ветвления и циклы

Если выполнение набора команд должно зависеть от некоторого условия, то ветвление можно задать с помощью операторов if/elseif/else/endif:

```
{% if ram >= 2048 %}
...
{% elseif ram <= 4096 %}
...
{% else %}
...
{% endif %}
```

Циклы for являются аналогом конструкций типа foreach других языков программирования и предназначены для выполнения заданного набора инструкций применительно к каждому элементу из списка:

```
{% set users = ['ivanov', 'petrov', 'kuznetsov'] %}
{% for user in users %}
{% do salt.log.info(user.upper()) %}
{% endfor %}
```

Если нужно обработать данные словаря, используется метод items(), чтобы получить список его элементов:

```
{% set users = {'u1':'ivanov', 'u2':'petrov', 'u3':'kuznetsov'} %}
{% for id, user in users.items() %}
{% do salt.log.info(user.upper()) %}
{% endfor %}
```

Так как циклы Jinja работают только со списками, то для эмуляции обычных циклов со счетчиком вам нужно воспользоваться функцией range([min], max). Если передать этой функции один параметр, то будет сгенерирован список с указанным количеством элементов, нумерация которых будет начинаться с нуля. Если передать два числа, то нумерация элементов будет в указанном диапазоне:

```
{% do salt.log.info('Обратный отсчет') %}
{% for i in range(0, 10) %}
{% do salt.log.info(10 - i) %}
{% endfor %}
```

Информация о целевой системе (grains)

При написании скриптов Jinja можно опираться на информацию о целевом хосте, на котором этот скрипт будет применен. Данная информация доступна в словаре grains, тут находится информация об операционной системе, памяти, дисках, настройках сетевых интерфейсов и многом другом. Например, используя ключ nodename можно получить имя хоста:

```
{% set node = salt['grains.get']('nodename') %}
```

Актуальное содержание словаря `grains` для конкретного хоста можно посмотреть с миньона утилитой `aldpro-salt-call`:

```
aldpro-salt-call grains.items
local:
     ----------
     astra_version:
     ----------
    distr:
        orel
    version:
        1.7.2
```

(продолжение на следующей странице)

```
    ...
```

Более подробную информацию о модулях grains можно найти в документации по проекту: https://docs.saltproject.io/en/latest/ref/modules/all/salt.modules.grains.html

Передача информации с мастера (pillar)

При настройке групповых политик администраторы задают значения атрибутов, которые доменным компьютерам передаются через механизм пилларов (`salt pillar`, соляной столб). Актуальное содержание словаря `pillar` можно посмотреть с миньона утилитой `aldpro-salt-call`.

Для компьютеров:

```
aldpro-salt-call pillar.get aldpro-hosts:pc-1.ald.company.lan
```

Для пользователей:

```
aldpro-salt-call pillar.get aldpro-users:<логин пользователя>
```

Содержание словаря определяется тем, какие политики назначены конкретному компьютеру (условный аналог GPResult в MS AD). Данные пиллара доступны только тем миньонам, для кого они предназначены, поэтому через атрибуты можно передавать в том числе конфиденциальную информацию, например пароли служебных учетных записей, сертификаты.

Если же нужно проверить, была ли уже применена конкретная политика на хосте, можно применить состояние с параметром test=True. Если по результатам выполнения команды появится сообщение “No changes needed to be made”, значит система уже получила pillar с заданной групповой политикой:

```
aldpro-salt-call state.apply rbta_ldap_env_vars_h test=True
...
         ID: /etc/bash.bashrc
    Function: file.blockreplace
      Result: True
     Comment: No changes needed to be made
...
```

Более подробную информацию о модулях pillar можно найти в документации по проекту: https://docs.saltproject.io/en/latest/topics/tutorials/pillar.html

Создание файлов на стороне миньона

Есть методы для создания файлов `touch`, переименования rename, удаления `clean`. Подробное описание возможностей доступно на странице:

- https://docs.saltproject.io/en/latest/ref/states/all/salt.states.file.html
- https://www.8host.com/blog/osnovy-saltstack-bazovye-terminy-i-ponyatiya/
- https://serverspace.ru/support/help/ispolzovanie-platformy-salt/

3.1.5.2. Декларативные описания SaltStack

Декларативная часть скрипта описывает в YAML-формате желаемую конфигурацию компьютера. В структуре документа указано, какие методы нужно вызывать для конфигурирования системы, и с какими параметрами. В качестве примера создадим файл `software.sls` со скриптом, который описывает состояние, после применения которого в системе должен стать доступен диспетчер задач `htop`:

```
cat software.sls
software_htop: ### Имя состояния
··pkg.installed: ### Вызов метода installed модуля pkg
·····-·pkgs: ### Аргументы метода installed
·······-·htop ### Значение аргумента pkgs
```

Можно выполнить скрипт с помощью команды aldpro-salt-call:

```
aldpro-salt-call --local --file-root=. state.sls software
```

Подробное рассмотрение параметров команды:

- `local` — означает локальную обработку без обращения к мастеру;
- `file-root=.` — устанавливает рабочую директорию, в которой будет выполняться поиск *.sls файлов;
- `state.sls` — указывает, что следует использовать модуль sls, который отвечает за применение состояний из файлов на диске;

- `software` — указывает имя *.sls файла без расширения.

Язык `YAML`, также как и `JSON`, является языком разметки текста для сериализации данных. Каждая строка задает пару ключ-значение, между которыми стоит знак двоеточия. Ключи могут состоять из одного и более слов, причем, заключать их в кавычки необязательно. В качестве значений поддерживаются как скалярные типы данных (`int, float, boolean, string`), так и вложенные словари, что позволяет создавать древовидные структуры данных. Второй и последующий уровни дерева должны обозначаться отступами с помощью двух и более пробелов, использовать символы табуляции вместо пробелов недопустимо. Если требуется прокомментировать какой-то фрагмент документа, то слева от комментария нужно поставить символ решетки.

На верхнем уровне структуры данных должен быть указан ключ с именем состояния, например, `software_htop`. Имя выбирается произвольно, в одном документе может быть описано несколько состояний, но их имена не должны повторяться.

На второй строке указано, что требуется вызвать метод `installed` модуля `salt.states.pkg`. Данный модуль является модулем состояния, т. е. его методы приводят систему к требуемому состоянию, описывая желаемый конечный результат, а не то, как к нему прийти. Есть также модули исполнения, которые выполняют в системе конкретные действия, ранее был приведен пример с использованием метода run модуля cmd для выполнения `bash` команды.

На третьей и четвертой строке методу передается аргумент `pkgs` со значением `htop`. Важно обратить внимание, что аргумент и его значение являются элементами списков, поэтому в начале этих строк стоит символ дефиса.

3.1.6. Требования к скриптам и наследование параметров

С 2.2.0 архитектура ALD Pro в части работы групповых политик изменилась, скрипты групповых политик получают только те компьютеры и пользователи, которым назначена политика. В связи с этим в скрипте может не быть проверки на назначение параметра конкретному компьютеру или пользователю.

Если на один компьютер или пользователя назначено несколько политик, использующих один и тот же параметр, то значения простых параметров будут переопределяться, а значения составных параметров суммироваться (см. «Наследования и суммирование групповых политик»).

Миньон получает политики, назначенные на компьютер или авторизованного на

компьютере пользователя. ALD Pro анализирует назначенные параметры, снизу вверх по дереву подразделений, оставляя только те которые соответствуют требованиям к операционной системе. Из оставшихся в результате операций суммирования и наследования формирует единый словарь `pillar`. Скрипты групповых политик отрабатываются миньоном только один раз с итоговым содержанием словаря `pillar`, вне зависимости от того, сколько раз соответствующий параметр был использован в объектах групповых политик, назначенных на этот компьютер или пользователя.

3.1.7. Отладка

Скрипт дополнительного параметра сохраняется в сервере службы каталогов (`{корень} → cn=etc → cn=aldpro → cn=vcsStorage → cn=grouppolicy → cn={Идентификатор ГП}`) и при получении по протоколу LDAP кешируется на миньоне в папках вместе с остальными групповыми политиками:

- Параметры компьютеров: `/srv/aldpro-salt/roots/states/policies/host-policies/`
- Параметры пользователей: `/srv/aldpro-salt/roots/states/policies/user-policies/`

В соответствии с расписанием из файла `/srv/aldpro-salt/roots/_modules/utils.py` скрипты выполняются при запуске службы `aldpro-salt-minion` и по расписанию каждые 30 минут + от 5 до 50 минут случайного времени. Другими словами политики гарантировано применятся в течение 80 минут. Посмотреть текущее значение таймера можно командой:

```
aldpro-salt-call schedule.show_next_fire_time build_gp_pillars
```

При необходимости можно локально изменить время стационарного таймера (по умолчанию 30 минут):

1. В файле на клиентском компьютере: `/srv/aldpro-salt/config/minion.d/standalone_scheduler.con` изменить значение атрибута `seconds/minutes` в блоке интересующего задания. Для групповых политик это `build_gp_pillars`.
2. В файле `/srv/aldpro-salt/_modules/utils.py` заменить `_25_MINUTES = dt.timedelta(minutes=25)`. Выставлять значения таймера менее 10 минут нежелательно, это может привести к повышению нагрузки и на контроллер домена и

на доменный компьютер.

3. Перезапускаем миньон командой:

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

Другой способ применения групповых политик: можно на миньоне вручную ввести команду (аналог `gpupdate /force`):

```
aldpro-salt-call state.apply gpupdate.gp
```

Можно в конце команды добавить `pillar='{“force”: True}'` - принудительное удаление связанного с политикой кэша. `pillar='{“verbose”: True}'` нужен для получения логов выполнения заданий применения. Использовать рекомендуется осторожно, поскольку вызывает повышенную нагрузку на контроллер домена.

Применить отдельно политики пользователя можно командой:

```
aldpro-salt-call state.apply policies.user-policies  pillar="{'user':
↪'username'}"
```

Для работы с политиками пользователей нужно явно передавать имя пользователя, чьи настройки вы хотите применить `pillar=“{'user': 'username'}”`.

3.1.7.1. Версионность

Каждая политика ГП имеет версию, которая автоматически изменяется, если наступило одно из следующих событий:

1. Внесены любые изменения в политики ГП или связанный с ней дополнительный параметр ГП. В этом случае дата изменений - это дата, когда пользователь внес изменения. А автор - это ФИО пользователя, внесшего изменения.

2. Произошло обновление версии ALD Pro. В этом случае дата изменений - это дата обновления системы. В этом случае «автором» изменений будет указано Системное обновление.

3.2. Резервное копирование подсистем ALD Pro

3.2.1. Резервное копирование (далее - бэкапирование)

- Раздел состоит из перечня скриптов резервного копирования каждой подсистемы (сервера).
- Требования к последовательности запуска скриптов - отсутствуют.
- Допустимо выборочное резервное копирование подсистем (серверов).

3.2.1.1. Резервное копирование Контроллера домена

Для выполнения резервного копирования Контроллера Домена необходимо перейти на рабочую станцию, которая выполняет роль Контроллера Домена и выполнить скрипт:

```
#!/usr/bin/env bash
# Название директории для резервной копии формируется
# из текущей даты и находится в папке /tmp/backup
now=$(date +"%d-%m-%Y")
BACKUP_PATH=/tmp/backup/$now
# Создание временной директории для резервных копий
mkdir -p $BACKUP_PATH
# Ограничение прав доступа к каталогу с резервными копиями
chown root:root $BACKUP_PATH && chmod 700 $BACKUP_PATH
# Создание резервной копии FreeIPA
ipa-backup
# Архивирование PK FreeIPA
tar -zcvf $BACKUP_PATH/ipa.tar.gz /var/lib/ipa/backup
# Очистка промежуточного бэкапа FreeIPA
rm -rf /var/lib/ipa/backup/*
# Остановка затрагиваемых бэкапом сервисов
systemctl stop apache2 celery celerybeat rabbitmq-server postgresql aldpro-
↪salt-minion
# Архивирование БД PostgreSQL
tar -zcvf $BACKUP_PATH/postgresql.tar.gz /var/lib/postgresql/
# Архивирование RabbitMQ
tar -zcvf $BACKUP_PATH/rabbitmq.tar.gz /var/lib/rabbitmq/mnesia/
# Архивирование директории ipa-client
tar -zcvf $BACKUP_PATH/ipa-client.tar.gz /var/lib/ipa-client/
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
# Архивирование логов
tar -zcvf $BACKUP_PATH/log.tar.gz --exclude=faillog --exclude=lastlog /var/
↪log/
# Архивирование директории etc
tar -zcvf $BACKUP_PATH/etc.tar.gz /etc/
# Архивирование директории rbta
tar -zcvf $BACKUP_PATH/rbta.tar.gz /opt/rbta/
# Запуск затрагиваемых бэкапом сервисов
systemctl start apache2 celery celerybeat rabbitmq-server postgresql aldpro-
↪salt-minion
```

Реплики - это равноправные серверы, не требующие отдельных условий для резервного копирования. Для их копирования используются команды, аналогичные командам для резервного копирования Контроллера домена.

3.2.1.2. Резервное копирование подсистемы журналирования событий

Для выполнения резервного копирования подсистемы журналирования событий необходимо перейти на рабочую станцию, которая выполняет функцию сервера журналирования событий и выполнить скрипт:

```
#!/usr/bin/env bash
# Название директории для резервной копии формируется
# из текущей даты и находится в папке /tmp/backup
now=$(date +"%d-%m-%Y")
BACKUP_PATH=/tmp/backup/$now
# Создание временной директории для резервных копий
mkdir -p $BACKUP_PATH
# Ограничение прав доступа к каталогу с резервными копиями
chown root:root $BACKUP_PATH && chmod 700 $BACKUP_PATH
# Архивирование логов
tar -zcvf $BACKUP_PATH/log.tar.gz --exclude=faillog --exclude=lastlog /var/
↪log/
# Архивирование директории etc
tar -zcvf $BACKUP_PATH/etc.tar.gz /etc/
# Архивирование директории ipa-client
tar -zcvf $BACKUP_PATH/ipa-client.tar.gz /var/lib/ipa-client/
```

3.2.1.3. Резервное копирование подсистемы печати

Для выполнения резервного копирования подсистемы печати необходимо перейти на рабочую станцию, которая выполняет функцию сервера печати и выполнить скрипт:

```
#!/usr/bin/env bash
# Название директории для резервной копии формируется
# из текущей даты и находится в папке /tmp/backup
now=$(date +"%d-%m-%Y")
BACKUP_PATH=/tmp/backup/$now
# Создание временной директории для резервных копий
mkdir -p $BACKUP_PATH
# Ограничение прав доступа к каталогу с резервными копиями
chown root:root $BACKUP_PATH && chmod 700 $BACKUP_PATH
# Остановка затрагиваемых бэкапом сервисов
systemctl stop cups aldpro-salt-minion
# архивирование директории ipa-client
tar -zcvf $BACKUP_PATH/ipa-client.tar.gz /var/lib/ipa-client/
# архивирование логов
tar -zcvf $BACKUP_PATH/log.tar.gz --exclude=faillog --exclude=lastlog /var/
↪log/
# архивирование директории etc
tar -zcvf $BACKUP_PATH/etc.tar.gz /etc/
# Запуск затрагиваемых бэкапом сервисов
systemctl start cups aldpro-salt-minion
```

3.2.1.4. Резервное копирование подсистемы DHCP

Для выполнения резервного копирования подсистемы DHCP необходимо перейти на рабочую станцию, которая выполняет функцию сервера DHCP и выполнить скрипт:

```
#!/usr/bin/env bash
# Название директории для резервной копии формируется
# из текущей даты и находится в папке /tmp/backup
now=$(date +"%d-%m-%Y")
BACKUP_PATH=/tmp/backup/$now
# Создание временной директории для резервных копий
mkdir -p $BACKUP_PATH
# Ограничение прав доступа к каталогу с резервными копиями
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
chown root:root $BACKUP_PATH && chmod 700 $BACKUP_PATH
# Архивирование директории ipa-client
tar -zcvf $BACKUP_PATH/ipa-client.tar.gz /var/lib/ipa-client/
# Архивирование логов
tar -zcvf $BACKUP_PATH/log.tar.gz --exclude=faillog --exclude=lastlog /var/
↪log/
# Архивирование директории etc
tar -zcvf $BACKUP_PATH/etc.tar.gz /etc/
```

3.2.1.5. Резервное копирование подсистемы мониторинга

Для выполнения резервного копирования подсистемы мониторинга необходимо перейти на рабочую станцию, которая выполняет функцию сервера мониторинга и выполнить скрипт:

```
#!/usr/bin/env bash
# Название директории для резервной копии формируется
# из текущей даты и находится в папке /tmp/backup
now=$(date +"%d-%m-%Y")
BACKUP_PATH=/tmp/backup/$now
# Создание временной директории для резервных копий
mkdir -p $BACKUP_PATH
# Ограничение прав доступа к каталогу с резервными копиями
chown root:root $BACKUP_PATH && chmod 700 $BACKUP_PATH
# Остановка затрагиваемых бэкапом сервисов
systemctl stop apache2 zabbix-agent zabbix-server postgresql aldpro-salt-
↪minion
# Архивирование директории ipa-client
tar -zcvf $BACKUP_PATH/ipa-client.tar.gz /var/lib/ipa-client/
# Архивирование логов
tar -zcvf $BACKUP_PATH/log.tar.gz --exclude=faillog --exclude=lastlog /var/
↪log/
# Архивирование директории etc
tar -zcvf $BACKUP_PATH/etc.tar.gz /etc/
# Архивирование zabbix
tar -zcvf $BACKUP_PATH/zabbix.tar.gz /usr/share/zabbix/
# Архивирование БД PostgreSQL
tar -zcvf $BACKUP_PATH/postgresql.tar.gz /var/lib/postgresql/
# Запуск затрагиваемых бэкапом сервисов
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
systemctl start apache2 zabbix-agent zabbix-server postgresql aldpro-salt-
↪minion
```

3.2.1.6. Резервное копирование подсистемы установки ОС по сети

Для выполнения резервного копирования подсистемы установки ОС по сети необходимо перейти на рабочую станцию, которая выполняет функцию сервера установки ОС по сети и выполнить скрипт:

```
#!/usr/bin/env bash
# Название директории для резервной копии формируется
# из текущей даты и находится в папке /tmp/backup
now=$(date +"%d-%m-%Y")
BACKUP_PATH=/tmp/backup/$now
# Создание временной директории для резервных копий
mkdir -p $BACKUP_PATH
# Ограничение прав доступа к каталогу с резервными копиями
chown root:root $BACKUP_PATH && chmod 700 $BACKUP_PATH
# Остановка затрагиваемых бэкапом сервисов
systemctl stop apache2 postgresql aldpro-salt-minion
# Архивирование PostgreSQL
tar -zcvf $BACKUP_PATH/postgresql.tar.gz /var/lib/postgresql/
# Архивирование логов
tar -zcvf $BACKUP_PATH/log.tar.gz --exclude=faillog --exclude=lastlog /var/
↪log/
# Архивирование директории etc
tar -zcvf $BACKUP_PATH/etc.tar.gz /etc/
# Архивирование директории ipa-client
tar -zcvf $BACKUP_PATH/ipa-client.tar.gz /var/lib/ipa-client/
# Архивирование директории tftp
tar -zcvf $BACKUP_PATH/tftp.tar.gz /var/www/tftp/
# Запуск затрагиваемых бэкапом сервисов
systemctl start apache2 postgresql aldpro-salt-minion
```

3.2.1.7. Резервное копирование подсистемы репозиториев ПО

Для выполнения резервного копирования подсистемы репозиториев ПО необходимо перейти на рабочую станцию, которая выполняет функцию сервера репозиториев ПО по сети и выполнить скрипт:

```
#!/usr/bin/env bash
# Название директории для резервной копии формируется
# из текущей даты и находится в папке /tmp/backup
now=$(date +"%d-%m-%Y")
BACKUP_PATH=/tmp/backup/$now
# Создание временной директории для резервных копий
mkdir -p $BACKUP_PATH
# Ограничение прав доступа к каталогу с резервными копиями
chown root:root $BACKUP_PATH && chmod 700 $BACKUP_PATH
# Остановка затрагиваемых бэкапом сервисов
systemctl stop apache2 postgresql rabbitmq-server aldpro-salt-minion
# Архивирование БД PostgreSQL
tar -zcvf $BACKUP_PATH/postgresql.tar.gz /var/lib/postgresql/
# Архивирование данных брокера очередей RabbitMQ
tar -zcvf $BACKUP_PATH/rabbitmq.tar.gz /var/lib/rabbitmq/mnesia/
# Архивирование логов
tar -zcvf $BACKUP_PATH/log.tar.gz --exclude=faillog --exclude=lastlog /var/
 ↪log/
# Архивирование директории etc
tar -zcvf $BACKUP_PATH/etc.tar.gz /etc/
# Архивирование директории ipa-client
tar -zcvf $BACKUP_PATH/ipa-client.tar.gz /var/lib/ipa-client/
# Архивирование директории repo/storage
tar -zcvf $BACKUP_PATH/storage.tar.gz /opt/rbta/aldpro/repo/storage/
tar -zcvf $BACKUP_PATH/ipa-client.tar.gz /var/lib/ipa-client/
# Архивирование домашнего каталога учетной записи repo
tar -zcvf $BACKUP_PATH/repo.tar.gz  /var/lib/repo/
# Запуск бэкапируемых сервисов
systemctl start apache2 postgresql rabbitmq-server aldpro-salt-minion
```

3.2.1.8. Резервное копирование подсистемы общего доступа

Для выполнения резервного копирования подсистемы общего доступа необходимо перейти на рабочую станцию, которая выполняет функцию сервера общего доступа по сети и выполнить скрипт:

```
#!/usr/bin/env bash
# Название директории для резервной копии формируется
# из текущей даты и находится в папке /tmp/backup
now=$(date +"%d-%m-%Y")
BACKUP_PATH=/tmp/backup/$now
# Создание временной директории для резервных копий
mkdir -p $BACKUP_PATH
# Ограничение прав доступа к каталогу с резервными копиями
chown root:root $BACKUP_PATH && chmod 700 $BACKUP_PATH
# Остановка затрагиваемых бэкапом сервисов
systemctl stop aldpro-salt-minion
# Архивирование логов
tar -zcvf $BACKUP_PATH/log.tar.gz --exclude=faillog --exclude=lastlog /var/
↪log/
# Архивирование директории etc
tar -zcvf $BACKUP_PATH/etc.tar.gz /etc/
# Архивирование директории ipa-client
tar -zcvf $BACKUP_PATH/ipa-client.tar.gz /var/lib/ipa-client/
# Архивирование директории /opt/samba_shares/
tar -zcvf $BACKUP_PATH/samba.tar.gz /opt/samba_shares/
# Запуск затрагиваемых бэкапом сервисов
systemctl start aldpro-salt-minion
```

3.2.2. Раздел 2. Восстановление

- Раздел состоит из перечня скриптов восстановления каждой подсистемы (сервера).
- Требования к последовательности запуска скриптов восстановления - отсутствуют.
- Допустимо выборочное восстановление подсистем (серверов).

Внимание: Все подсистемы устанавливаются только на машины-клиенты. Запрещено устанавливать две подсистемы на одну машину. Версия ОС и установленных пакетов

должна быть идентична версии ОС, на которой работала подсистема.

При восстановлении данных через **RuBackup** на одном из контроллеров домена выполняется авторитативное восстановление. В этом случае восстанавливаемый контроллер домена получает новое значение генератора **CSN** и прекращает участие в репликации. Чтобы завершить восстановление домена, необходимо выполнить реинициализацию остальных контроллеров. Используйте команду:

```
ipa-replica-manage re-initialize --from <имя_восстановленного_контроллера>
```

После реинициализации все контроллеры скопируют базу данных с восстановленного контроллера, включая новое значение генератора **CSN**, поэтому репликация в домене восстановится.

Внимание: Все изменения, внесённые в домен после создания резервной копии, будут утеряны.

3.2.2.1. Восстановление Контроллера Домена

Для восстановления Контроллера Домена (КД) с использованием резервной копии небходимо соблюдение следующих условий:

- Имя и адрес машины, на которой будет производиться восстановление КД, должно совпадать с именем и адресом машины, с которой была сделана резервная копия.
- Версия ОС и версия обновления ОС на машине, на которой будет восстановлен КД, должны быть идентичны тем, что были установленны на машине, с которой сделана резервная копия.

В зависимости от количества КД в системе, восстановление резервной копии может отличаться:

- В домене только один рабочий КД, на котором необходимо откатить данные на момент создания резервной копии. Необходимо воспользоваться скриптом для восстановления ниже.
- В домене один КД, который вышел из строя, и восстановить его работостособность

невозможно или нецелесообразно. Необходимо развернуть новый КД, идентичный вышедшему из строя, и воспользоваться скриптом для восстановления ниже. После перезагрузки восстановленного КД, необходимо проверить синхронизацию времени на КД и на других машинах, введенных в домен, для корректной работы билетов **Kerberos**.

- В домене несколько КД, машина, накотором был установлен один из них, вышла из строя. Необходимо настроить машину и завести ее в домен с именем и адресом, идентичными тем, что были у машины, вышедшей из строя. С помощью команды `aldpro-roles --uid --action install` установить подсистему на новую машину. Воспользоваться скриптом для восстановления ниже. Повторить инициализацию КД для получения им актуальных данных с работающих КД.
- В домене несколько КД, на одном из них произошел сбой и часть актуальной информации утрачена. Необходимо воспользоваться скриптом восстановления ниже. Произвести инициализацию работающих КД с восстановленным.

Скрипт для восстановления КД:

```
#!/bin/bash
# Перейти в директорию с резервными копиями
cd /tmp/backup/{дата создания бэкапа}
# Разархивирование РК IPA
tar -C "/" -xvf ipa.tar.gz
# Восстановление IPA из РК
ipa-restore /var/lib/ipa/backup/ipa-full-YOUR_BACKUP_DATE
# Остановка затрагиваемых восстановлением сервисов
systemctl stop apache2 celery celerybeat rabbitmq-server postgresql aldpro-
↪salt-minion
# Чистим кеш у sssd service
rm -f /var/lib/sss/db/*
# Восстановление БД Postgresql
tar -C "/" -xvf postgresql.tar.gz
# Восстановление RabbitMQ
tar -C "/" -xvf rabbitmq.tar.gz
# Восстановление логов
tar -C "/" -xvf log.tar.gz
# Восстановление директории etc
tar -C "/" -xvf etc.tar.gz
# Восстановление директории rbta
tar -C "/" -xvf rbta.tar.gz
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
# Восстановление ipa-client
tar -C "/" -xvf ipa-client.tar.gz
# Перезагрузка
reboot
```

При выполнении скрипта `backup_dc.sh` архивируется бэкап, имя которого необходимо впоследствии подставить в скрипт восстановления. Имя бэкапа хранится в архиве. Если имя не указать, возникнет ошибка, но при этом бэкап разархивируется в `/var/lib/ipa/backup/`, по этому пути также можно будет найти имя бэкапа и подставить в скрипт для повторного выполнения.

Команда для просмотра содержимого архива:

```
tar -ztvf /tmp/backup/{дата создания бэкапа}/ipa.tar.gz
```

Команда для переинициализации репликации:

```
ipa-replica-manage re-initialize --from dc-1.ald.company.lan
```

3.2.2.2. Восстановление подсистемы журналирования событий

Восстановить подсистему необходимо, потому что:

- Производились работы в конфигурационных файлах, после чего подсистема перестала работать. Для восстановления подсистемы необходимо воспользоваться скриптом ниже.
- Машина, на которой располагалась подсистема, вышла из строя и нет возможности восстановить ее работу. Для восстановления подсистемы необходимо завести в домен машину с именем и адресом, идентичными тем, что были у машины, вышедшей из строя. С помощью команды `aldpro-roles --uid --action install` установить подсистему на новую машину. Запустить команду для получения переменных конфигурации для подсистемы `aldpro-salt-call aldpro_subsystems.build_audit_role_pillar`. Запустить команду для генерации конфигурационных файлов из полученных переменных `aldpro-salt-call state.apply roles.audit`. Воспользоваться скриптом для восстановления ниже.

Скрипт для восстановления подсистемы:

```
#!/bin/bash
# Переход в директорию с резервными копиями
cd /tmp/backup/
# Остановка затрагиваемых восстановлением сервисов
systemctl stop syslog-ng aldpro-salt-minion
# Восстановление логов
tar -C "/" -xvf log.tar.gz
# Перезагрузка
reboot
```

3.2.2.3. Восстановление подсистемы печати

Восстановить подсистему необходимо, потому что:

- Производились работы в конфигурационных файлах, после чего подсистема перестала работать. Для восстановления подсистемы необходимо воспользоваться скриптом ниже.
- Машина, на которой располагалась подсистема, вышла из строя и нет возможности восстановить ее работу. Для восстановления подсистемы необходимо завести в домен машину с именем и адресом, идентичными тем, что были у машины, вышедшей из строя. С помощью команды `aldpro-roles --uid --action install` установить подсистему на новую машину. Запустить команду для получения переменных конфигурации для подсистемы `aldpro-salt-call aldpro_subsystems.build_cups_role_pillar`. Запустить команду для генерации конфигурационных файлов из полученных переменных `aldpro-salt-call state.apply roles.cups`. Воспользоваться скриптом для восстановления ниже.

Скрипт для восстановления подсистемы:

```
#!/bin/bash
# Переход в директорию с резервными копиями
cd /tmp/backup/
# Остановка затрагиваемых бэкапом сервисов
systemctl stop cups aldpro-salt-minion
# Восстановление логов
tar -C "/" -xvf log.tar.gz
# Восстановление директории etc
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
tar -C "/" -xvf etc.tar.gz
# Восстановление ipa-client
tar -C "/" -xvf ipa-client.tar.gz
# Перезагрузка
reboot
```

Внимание: При восстановлении указанным способом информация в LDAP и на сервере может отличаться. Чтобы избежать этого, после восстановления системы необходимо выполнить команду: `aldpro-roles --subsystem_settings cups`

3.2.2.4. Восстановление подсистемы DHCP

Восстановить подсистему необходимо, потому что:

- Производились работы в конфигурационных файлах, после чего подсистема перестала работать. Для восстановления подсистемы необходимо воспользоваться скриптом ниже.
- Машина, на которой располагалась подсистема, вышла из строя и нет возможности восстановить ее работу. Для восстановления подсистемы необходимо завести в домен машину с именем и адресом, идентичными тем, что были у машины, вышедшей из строя. С помощью команды `aldpro-roles --uid --action install` установить подсистему на новую машину. Запустить команду для получения переменных конфигурации для подсистемы `aldpro-salt-call aldpro_subsystems.build_dhcp_role_pillar`. Запустить команду для генерации конфигурационных файлов из полученных переменных `aldpro-salt-call state.apply roles.dhcp`. Воспользоваться скриптом для восстановления ниже.

Скрипт для восстановления подсистемы:

```
#!/bin/bash
# Перейти в директорию с резервными копиями
cd /tmp/backup/
# Остановка затрагиваемых восстановлением сервисов
systemctl stop isc-dhcp-server aldpro-salt-minion
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
# Восстановление логов
tar -C "/" -xvf log.tar.gz
# Восстановление директории  etc
tar -C "/" -xvf etc.tar.gz
# Восстановление  ipa-client
tar -C "/" -xvf ipa-client.tar.gz
# Перезагрузка
reboot
```

Внимание: При восстановлении указанным способом информация в LDAP и на сервере может отличаться. Чтобы избежать этого, после восстановления системы необходимо выполнить команду: `aldpro-roles --subsystem_settings dhcp`

3.2.2.5. Восстановление подсистемы мониторинга

Восстановить подсистему необходимо, потому что:

- Производились какие-то работы, после чего подсистема перестала работать. Для восстановления подсистемы необходимо воспользоваться скриптом ниже.
- Машина, на которой располагалась подсистема, вышла из строя и нет возможности восстановить ее работу. Для восстановления подсистемы необходимо завести в домен машину с именем и адресом, идентичными тем, что были у машины, вышедшей из строя. С помощью команды `aldpro-roles --uid --action install` установить подсистему на новую машину. Воспользоваться скриптом для восстановления ниже.

Скрипт для восстановления подсистемы:

Пароль для восстановления базы данных - `postgres`

```
#!/bin/bash
# Перейти в директорию с резервными копиями
cd /tmp/backup/
# Остановка затрагиваемых бэкапом сервисов
systemctl stop apache2 zabbix-agent zabbix-server postgresql aldpro-salt-
↪minion
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
# Восстановление БД PostgreSQL
tar -C "/" -xvf postgresql.tar.gz
# Восстановление логов
tar -C "/" -xvf log.tar.gz
# Восстановление директории zabbix
tar -C "/" -xvf zabbix.tar.gz
# Перезагрузка
reboot
```

3.2.2.6. Восстановление подсистемы установки ОС по сети

Восстановить подсистему необходимо, потому что:

- Производились работы в конфигурационных файлах, после чего подсистема перестала работать. Для восстановления подсистемы необходимо воспользоваться скриптом:
- Машина, на которой располагалась подсистема, вышла из строя и нет возможности восстановить ее работу. Для восстановления подсистемы необходимо завести в домен машину с именем и адресом, идентичными тем, что были у машины, вышедшей из строя. С помощью команды `aldpro-roles --uid --action install` установить подсистему на новую машину. Воспользоваться скриптом для восстановления:

```
#!/bin/bash
# Переход в директорию с резервными копиями
cd /tmp/backup
# Остановка затрагиваемых восстановлением сервисов
systemctl stop apache2 tftpd-hpa postgresql aldpro-salt-minion
# Восстановление БД PostgreSQL
tar -C "/" -xvf postgresql.tar.gz
# Восстановление логов
tar -C "/" -xvf log.tar.gz
# Восстановление директории tftp
tar -C "/" -xvf tftp.tar.gz
# Перезагрузка
reboot
```

Внимание: При восстановлении указанным способом информация в LDAP и на сервере может отличаться. Чтобы избежать этого, после восстановления системы необходимо выполнить команду: `aldpro-roles --subsystem_settings os`

3.2.2.7. Восстановление подсистемы репозиториев ПО

Восстановить подсистему необходимо, потому что:

- Производились работы с конфигурационным файлом, после чего подсистема перестала работать. Для восстановления подсистемы необходимо воспользоваться скриптом:

```
#!/bin/bash
# Переход в директорию с резервными копиями
cd /tmp/backup
# Остановка затрагиваемых восстановлением сервисов
systemctl stop apache2 postgresql rabbitmq-server aldpro-salt-minion
# Восстановление БД PostgreSQL
tar -C "/" -xvf postgresql.tar.gz
# Восстановление RabbitMQ
tar -C "/" -xvf rabbitmq.tar.gz
# Восстановление логов
tar -C "/" -xvf log.tar.gz
# Восстановление директории etc
tar -C "/" -xvf etc.tar.gz
# Восстановление ipa-client
tar -C "/" -xvf ipa-client.tar.gz
# Восстановление директории с репозиториями
t ar -C "/" -xvf storage.tar.gz
# Перезагрузка
reboot
```

- Машина, на которой располагалась подсистема, вышла из строя и нет возможности восстановить ее работу. Для восстановления подсистемы необходимо завести в домен машину с именем и адресом, идентичными тем, что были у машины, вышедшей из строя. С помощью команды `aldpro-roles --uid --action install` установить подсистему на новую машину. Запустить команду для получения переменных конфигурации для подсистемы `aldpro-salt-call`

`aldpro_subsystems.build_repo_role_pillar`. Запустить команду для генерации конфигурационных файлов из полученных переменных `aldpro-salt-call state.apply roles.repo`. Воспользоваться скриптом для восстановления ниже.

Скрипт для восстановления подсистемы:

```
#!/bin/bash
# Переход в директорию с резервными копиями
cd /tmp/backup
# Остановка затрагиваемых восстановлением сервисов
systemctl stop apache2 postgresql rabbitmq-server aldpro-salt-minion
# Восстановление БД PostgreSQL
tar -C "/" -xvf postgresql.tar.gz
# Восстановление RabbitMQ
tar -C "/" -xvf rabbitmq.tar.gz
# Восстановление директории с репозиториями
tar -C "/" -xvf storage.tar.gz
# Восстановление логов
tar -C "/" -xvf log.tar.gz
# Перезагрузка
reboot
```

3.2.2.8. Восстановление подсистемы общего доступа к файлам

Восстановить подсистему необходимо, потому что:

- Производились работы в конфигурационных файлах, после чего подсистема перестала работать. Для восстановления подсистемы необходимо воспользоваться скриптом:

```
#!/bin/bash
# Переход в директорию с резервными копиями
cd /tmp/backup
# Остановка затрагиваемых восстановлением сервисов
systemctl stop smbd nmbd aldpro-salt-minion
# Восстановление логов
tar -C "/" -xvf log.tar.gz
# Восстановление директории etc
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
tar -C "/" -xvf etc.tar.gz
# Восстановление ipa-client
tar -C "/" -xvf ipa-client.tar.gz
# Восстановление общих директорий samba
tar -C "/" -xvf samba.tar.gz
# Перезагрузка
reboot
```

- Машина, на которой располагалась подсистема, вышла из строя и нет возможности восстановить ее работу. Для восстановления подсистемы необходимо завести в домен машину с именем и адресом, идентичными тем, что были у машины, вышедшей из строя. С помощью команды `aldpro-roles --uid --action install` установить подсистему на новую машину. Запустить команду для получения переменных конфигурации для подсистемы `aldpro-salt-call aldpro_subsystems.build_smb_role_pillar`. Запустить команду для генерации конфигурационных файлов из полученных переменных `aldpro-salt-call state.apply roles.smb`. Воспользоваться скриптом для восстановления ниже.

Скрипт для восстановления подсистемы:

```
#!/bin/bash
# Переход в директорию с резервными копиями
cd /tmp/backup
# Остановка затрагиваемых восстановлением сервисов
systemctl stop smbd nmbd aldpro-salt-minion
# Восстановление общих директорий samba
tar -C "/" -xvf samba.tar.gz
# Восстановление логов
tar -C "/" -xvf log.tar.gz
# Перезагрузка
reboot
```

Внимание: При восстановлении указанным способом информация в LDAP и на сервере может отличаться. Чтобы избежать этого, после восстановления системы необходимо выполнить команду:

```
aldpro-roles --subsystem_settings smb
```

3.2.2.9. Особенности интеграции с RuBackup

При копировании и восстановлении данных с помощью `rubackup-client` или непосредственно утилитами `ipa-backup/ipa-restore` из-за перезапуска служб каталога на контроллерах перестает работать WEB-сервис `apache2`, обеспечивающий доступ к консоли управления **ALD Pro**.

Для восстановления доступа к консоли управления **ALD Pro** нужно запустить сервис `apache2`.

При восстановлении данных из `rubackup manager` необходимо установить ползунок **Восстановить на целевом ресурсе**. Без этой опции восстановление данных каталога выполнено не будет.



3.3. Инструкция по обеспечению безопасной работы в домене ALD Pro: правила HBAC

Когда сотруднику выдают доменную учетную запись, у него появляется возможность зайти с ее помощью на любой хост в домене, включая сервера, что при неправильной настройке зон ответственности при администрировании к объектам файловой системы создает угрозу несанкционированного доступа к информации, хранящейся на этих компьютерах.

Для повышения безопасности работы в домене администраторам следует ограничить доступ к компьютерам, что можно сделать с помощью правил управления доступом к хостам (host-based access control, HBAC).

3.3.1. Что такое HBAC-правила

Правила HBAC создают дополнительный слой авторизации, позволяя разрешить определенным пользователям использовать указанные службы на конкретных хостах.

Правила являются разрешающими, для каждого из трех субъектов безопасности следует определить область одним из двух способов:

- Любой субъект — правило будет распространяться на все субъекты и группы субъектов данного вида.
- Указанные субъекты — правило будет распространяться только на указанный перечень субъектов и групп субъектов данного вида.

Что такое «пользователи» и «хосты» обычно вопросов не вызывает, но вот понятие «служб» требует отдельного пояснения.

3.3.2. Механизм работы HBAC-правил

Службами в контексте HBAC являются любые приложения, которые используют PAM-стек для авторизации пользователей, при этом не важно, являются ли эти приложения обычными исполняемыми файлами или работают в фоне.

Стек подключаемых модулей аутентификации (Pluggable Authentication Modules, PAM) - это система библиотек, обеспечивающая унифицированный программный интерфейс (Application Programming Interface, API) для абстрагирования приложений (таких как login и sudo) от выполнения стандартных задач аутентификации, причем, настройки аутентификации администраторы могут задавать для каждого приложения индивидуально с помощью файлов из директории `/etc/pam.d/\*`

Библиотека PAM делит задачи аутентификации на четыре независимые группы управления, которые отвечают за различные аспекты пользовательских запросов:

- **account** – группа модулей, которые отвечают за проверку аккаунта, не истек ли пароль, разрешен ли пользователю доступ к запрашиваемому сервису.
- **authentication** – группа модулей, которые отвечают за получение учетных данных пользователя и выполнение аутентификации. Чаще всего они реализуют какой-то диалог с пользователем для получения данных, но также возможны и способы аутентификации с использованием аппаратных ключей, биометрических устройств и пользовательских сертификатов.

- **password** – группа модулей, которые отвечают за проверку пароля на соответствие требованиям безопасности по длине, стойкость к перебору, наличию часто запрещенных слов.
- **session** – группа модулей, которые отвечают за выполнение задач до и после предоставления услуги, например, запись событий в журналы, монтирование домашнего каталога.

За работу HBAC-правил отвечает модуль `pam_sss.so`:

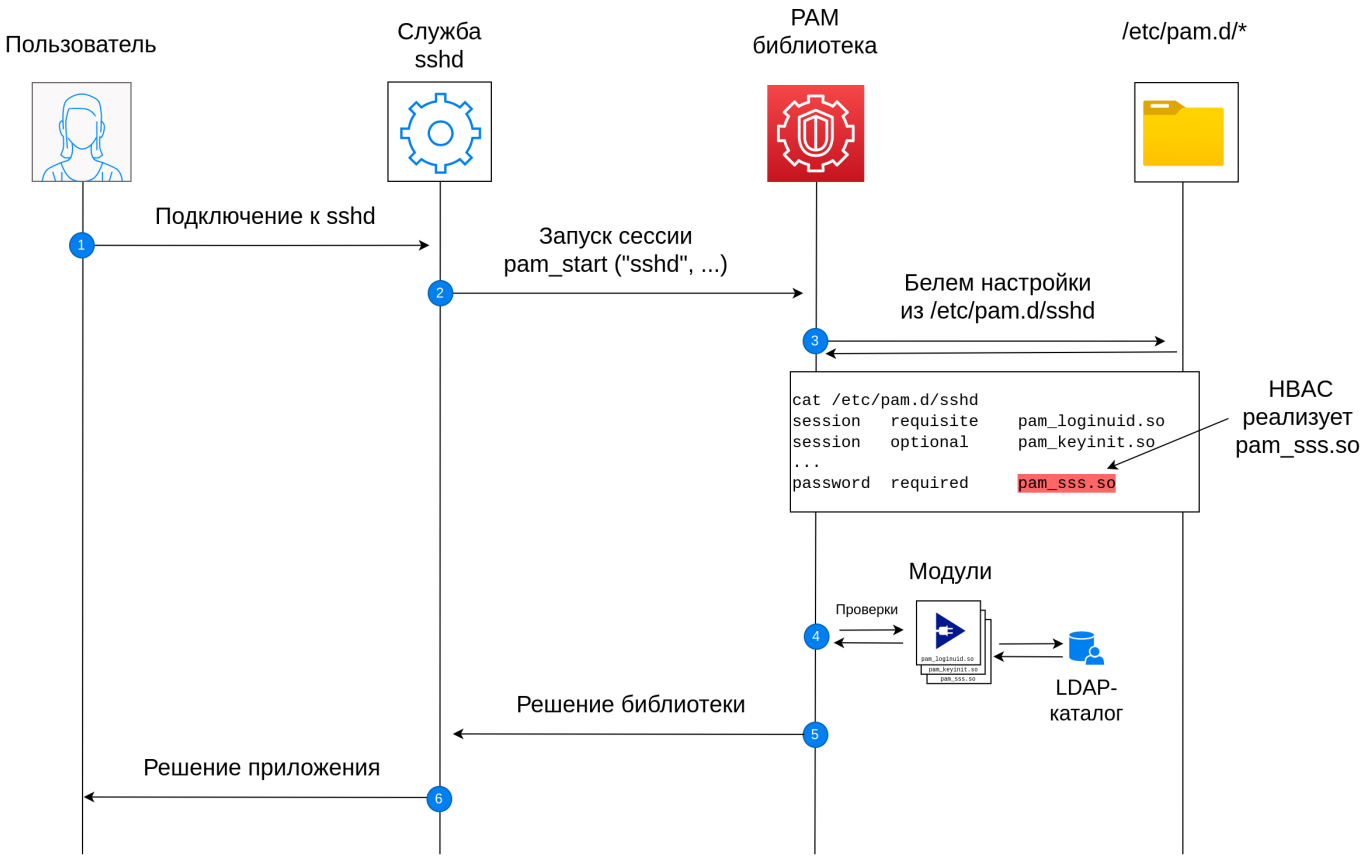


Рисунок 3.4 – Механизм работы HBAC-правил 1

При подключении пользователя по SSH (1) служба обращается к PAM библиотеке, чтобы создать контекст безопасности для выполнения команд от его имени (2). При вызове функции pam_start служба передает библиотеке свой идентификатор (PAM service name), который представляет из себя обычную строку, например `sshd`. Идентификатор службы обычно совпадает с именем исполняемого файла, но это не обязательно. Некоторые приложения могут использовать несколько идентификаторов, например, утилита sudo использует дополнительный идентификатор «sudo-i», а модуль mod_authnz_pam веб-сервера Apache2 так вообще позволяет проверять доступ к каждому разделу сайта с помощью отдельного идентификатора. Обратите также внимание, что в разных

дистрибутивах Linux одни и те же службы могут использовать разные идентификаторы, например, ssh и sshd.

Значение идентификатора службы определяет имя файла, откуда библиотека PAM будет брать настройки стека модулей (3), для службы sshd настройки будут браться из файла `/etc/pam.d/sshd`. В конфигурационных файлах PAM-стека перечисляются необходимые модули и параметры их вызова. Для того, чтобы упросить управление PAM-стеком, конфигурационные файлы допускают использование инструкций @include, которые позволяют включить содержимое других файлов.

Получив необходимые настройки, библиотека PAM выполняет проверки, используя указанные модули (4), причем, за работу HBAC-правил отвечает модуль pam_sss.so. Итоговый ответ библиотека передает приложению (5), которое, в свою очередь, использует эту информацию для организации взаимодействия с пользователем (6).

Модуль pam_sss.so является клиентской библиотекой службы sssd, основная задача которой заключается в получении информации от службы каталога и локальном кешировании данных для ускорения обработки запросов. Учитывая необходимость кеширования, архитектура службы предусматривает наличие серверной части (backend), собеседника (responder) и локального кеша между ними, см. рисунок 2.

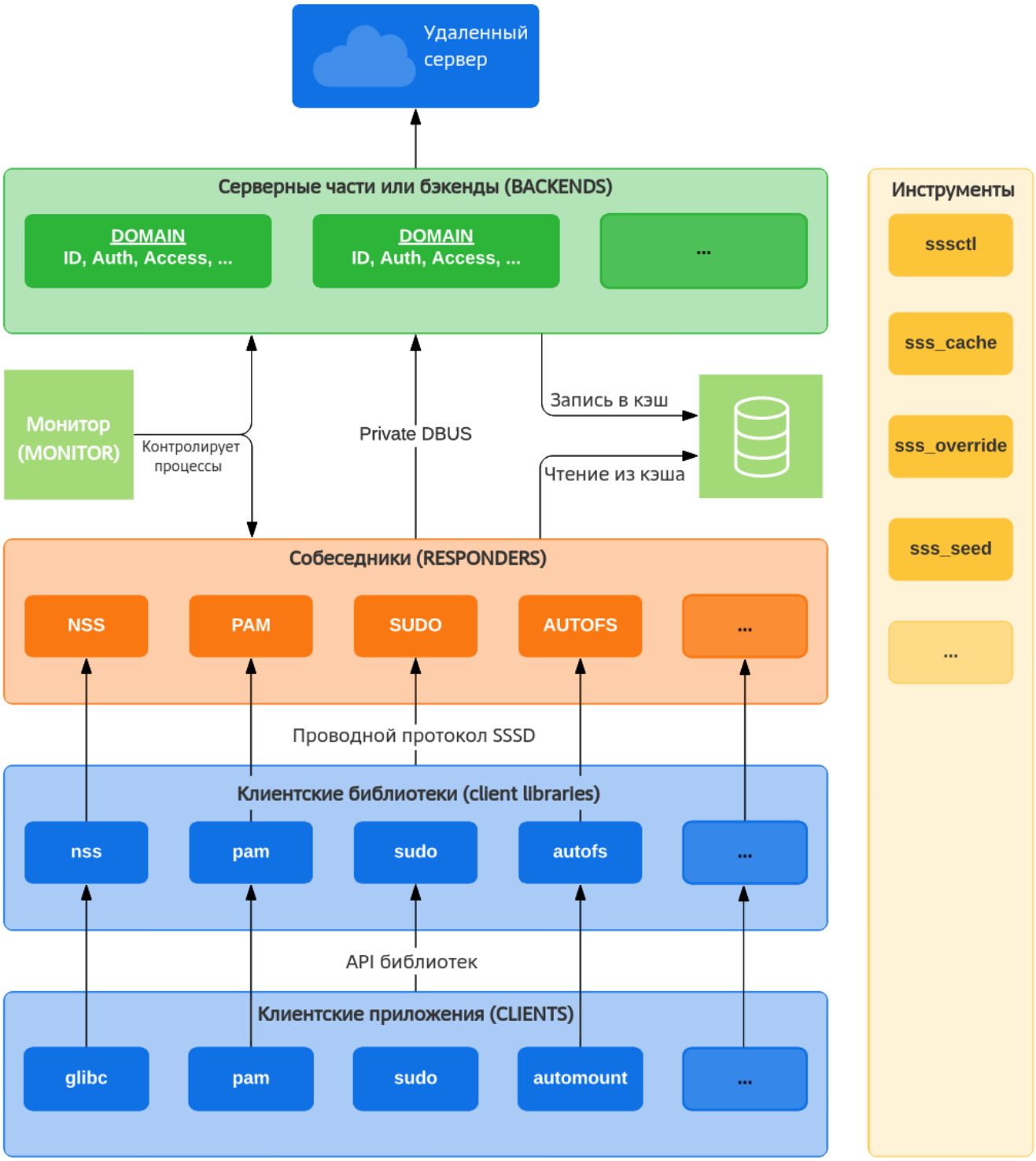


Рисунок 3.5 – Архитектура службы SSSD

Для вступления в силу изменений в настройках HBAC-правил вы можете воспользоваться на целевой машине командами `sss_cache -E` или `sssctl cache-remove`, чтобы очистить локальный кеш службы `sssd`. Утилиты входят в состав пакета sssd-tools, который нужно устанавливать дополнительно.

3.3.3. Доступ для администраторов ко всем компьютерам в домене, ограничение правила allow_all

Правила HBAC являются «разрешающими», т. е. «по умолчанию» доступ к службам на доменных компьютерах запрещен, и его нужно открывать с помощью правил. Однако, при развертывании домена автоматически создается правило allow_all, которое разрешает доступ «всех ко всему», поэтому для управления авторизацией на уровне HBAC вам нужно сначала ограничить область применения этого правила, например, только группой администраторов.

Внести указанные настройки можно через веб-портал на странице «Групповые политики > Политики доступа к узлу > allow_all > Пользователи»

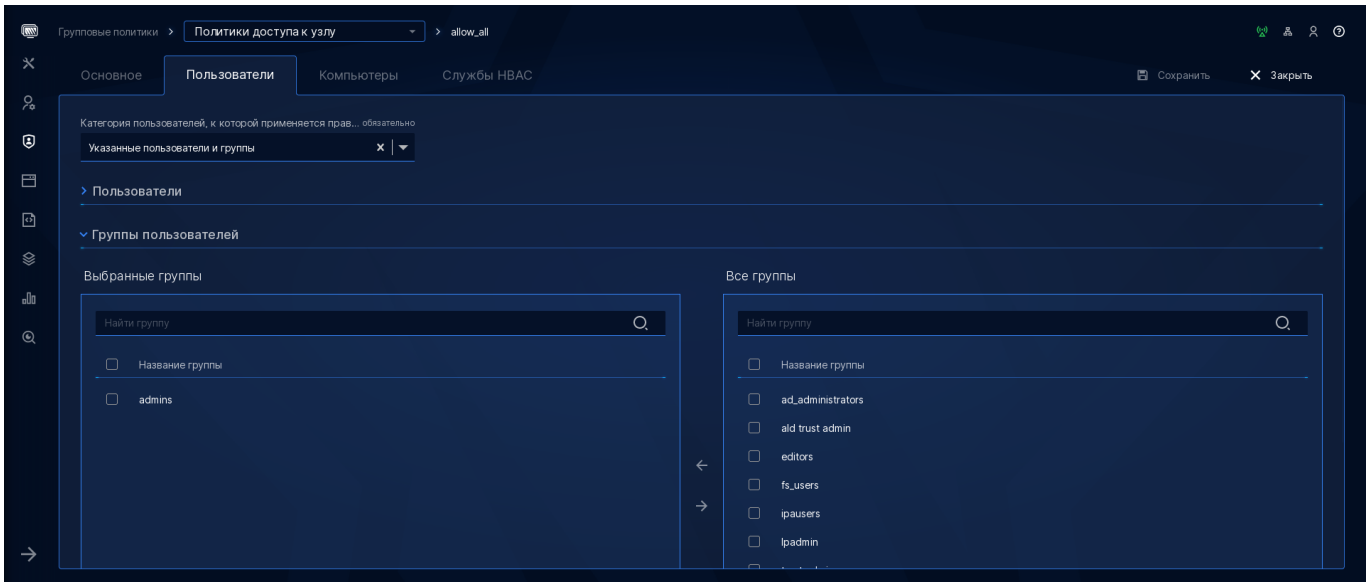


Рисунок 3.6 – Группа компьютера

или из командной строки:

```
ipa hbacrule-mod allow_all --usercat=''
ipa hbacrule-mod allow_all --desc='Разрешает администраторам доступ к любому
↪хосту в домене'
ipa hbacrule-add-user allow_all --group admins
ipa hbacrule-show allow_all
```

где:

- hbacrule-mod — команда, с помощью которой можно модифицировать настройки существующей группы;

- allow_all — имя правила, которые мы хотим модифицировать;
- usercat — ключ, который позволяет изменить категорию для области применения в части пользователей. Может принимать два возможных значения — ‘all’ и пустая строка ’’;
- hbacrule-add-user — команда, с помощью которой можно расширить область применения правила в части пользователей;
- allow_all — имя правила, которое мы хотим модифицировать;
- group — ключ, который позволяет добавить группу пользователей в область применения HBAC-правила;
- admins — имя группы, которая будет добавлена в область применения правила;
- hbacrule-show — команда, с помощью которой можно получить информацию о существующем HBAC-правиле;
- allow_all — имя правила, по которому мы хотим получить информацию.

Примечание: Если из-за неправильной настройки HBAC-правил доступ к хостам будет все же заблокирован, вы сможете подключиться к порталу управления с любого другого компьютера, который не находится в домене, чтобы исправить ошибку. Доступ к порталу управления не регулируется через механизм HBAC.

3.3.4. Доступ для сотрудников на рабочие станции, создание правила allow_computers

Если ограничить область действия правила allow_all группой администраторов, то для остальных сотрудников компании нужно будет создать правило allow_computers, которое предоставит им право входа на обычные компьютеры в домене.

Создадим это правило с использованием веб-интерфейса:

1. Создайте группу хостов **computers**. Откройте страницу «Пользователи и компьютеры > Группы компьютеров» и нажмите кнопку «+ Новая группа». Введите имя группы, ее описание и нажмите кнопку «Сохранить».

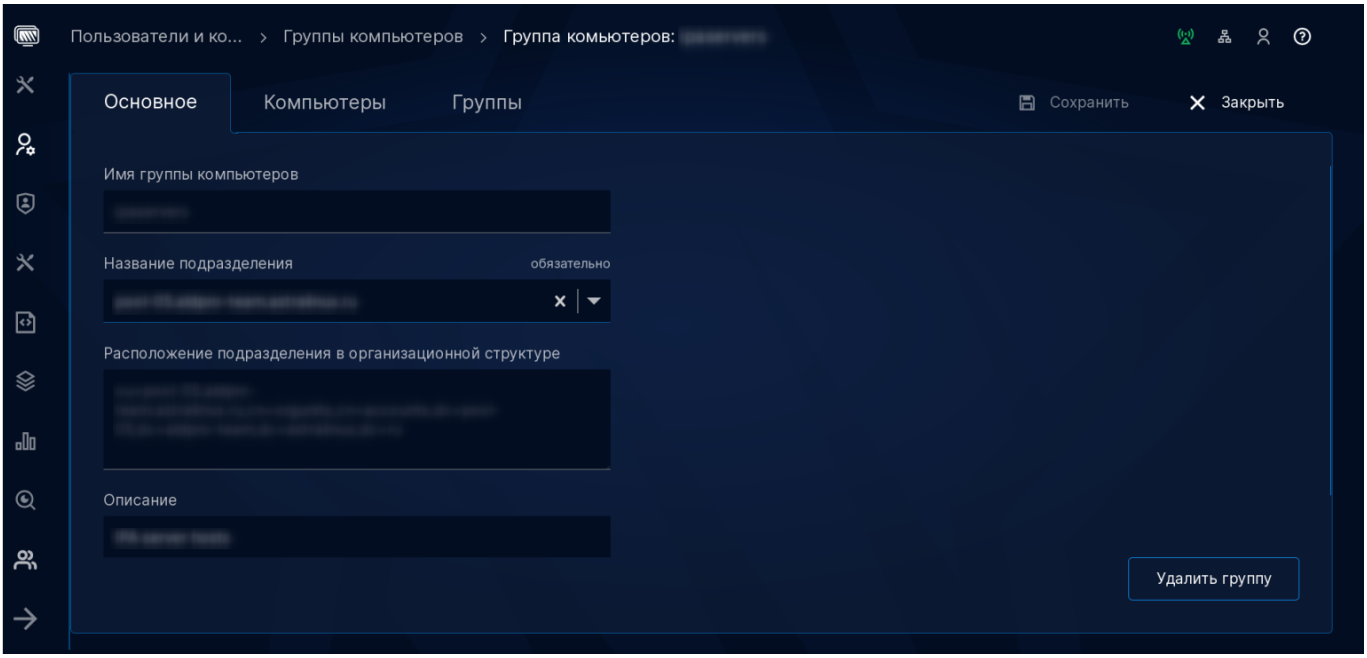


Рисунок 3.7 – Компьютеры

2. На вкладке «Компьютеры» внесите рабочие станции в список участников группы.

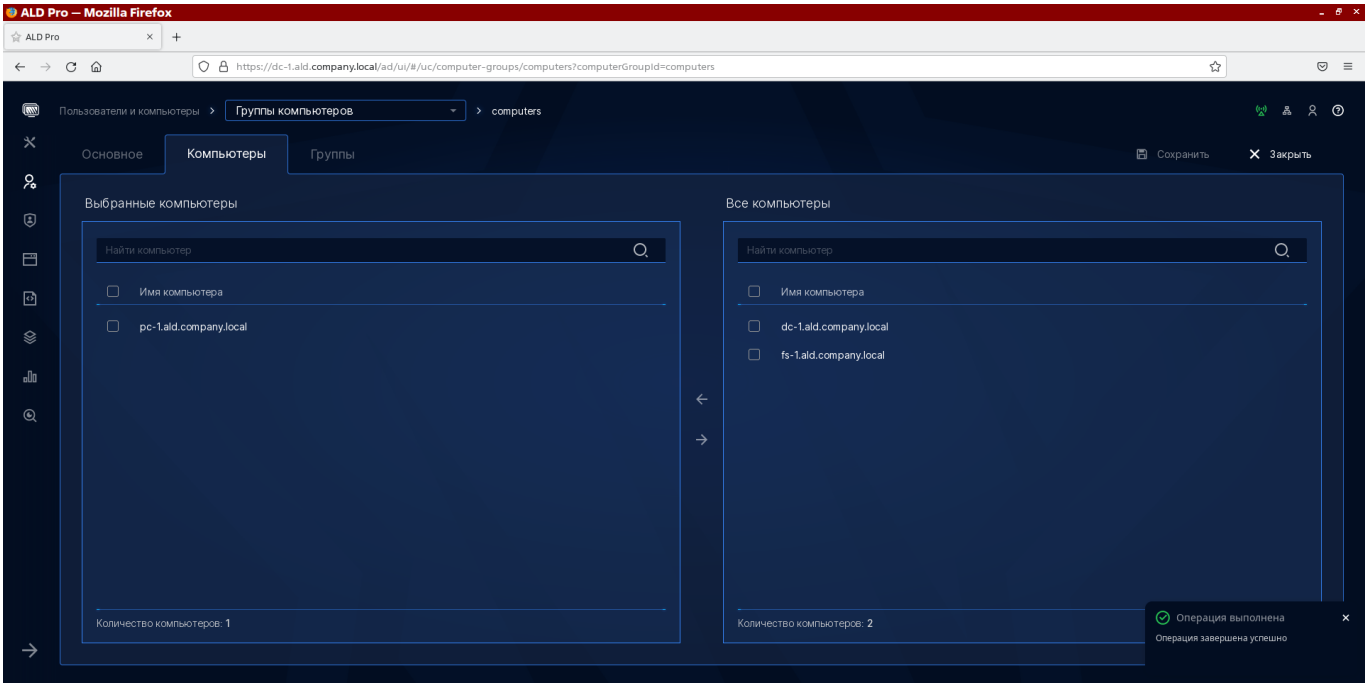


Рисунок 3.8 – Политика доступа к узлу 1

3. Создайте HBAC-правило. Откройте страницу «Групповые политики > Политики доступа к узлу > Правила HBAC» и нажмите кнопку «+ Новое правило». Введите имя правила allow_computers и сохраните его. Для созданного правила определите следующую область действия:

- пользователи — любой пользователь;
- хосты — указанные компьютеры и группы, группа computers;
- службы — любая служба.

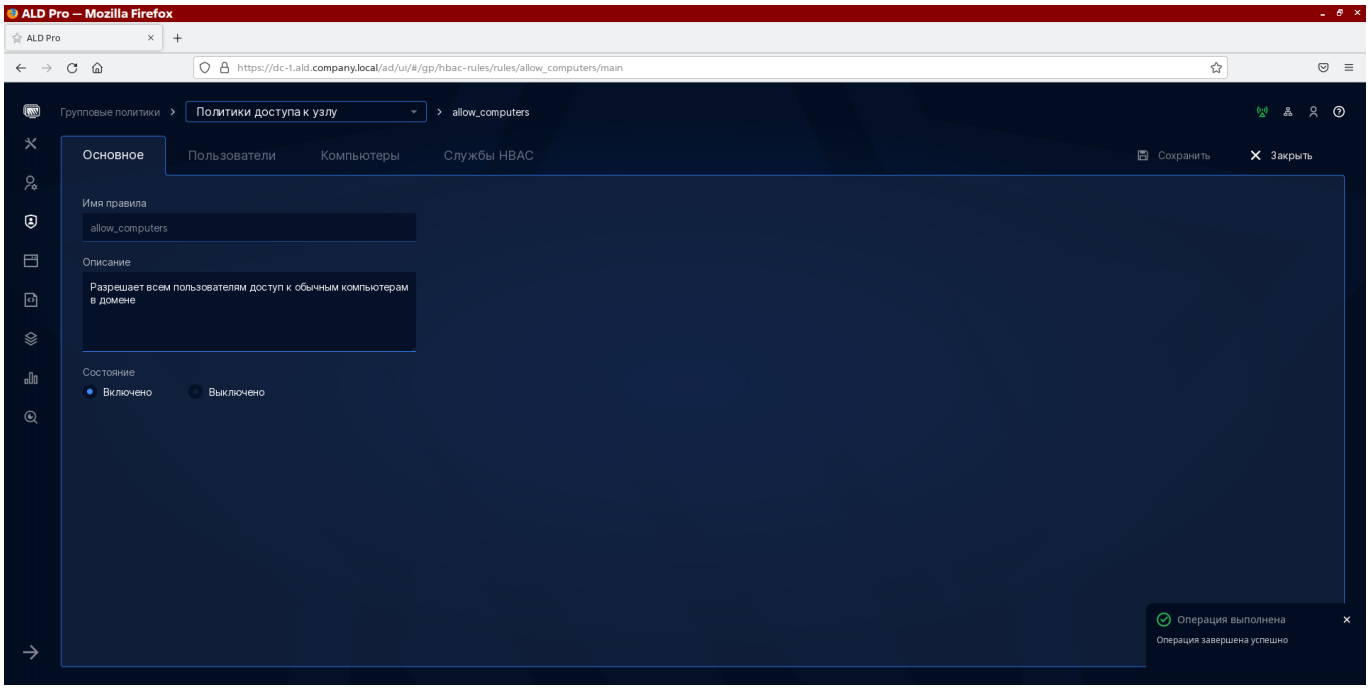


Рисунок 3.9 – Политика доступа к узлу 2

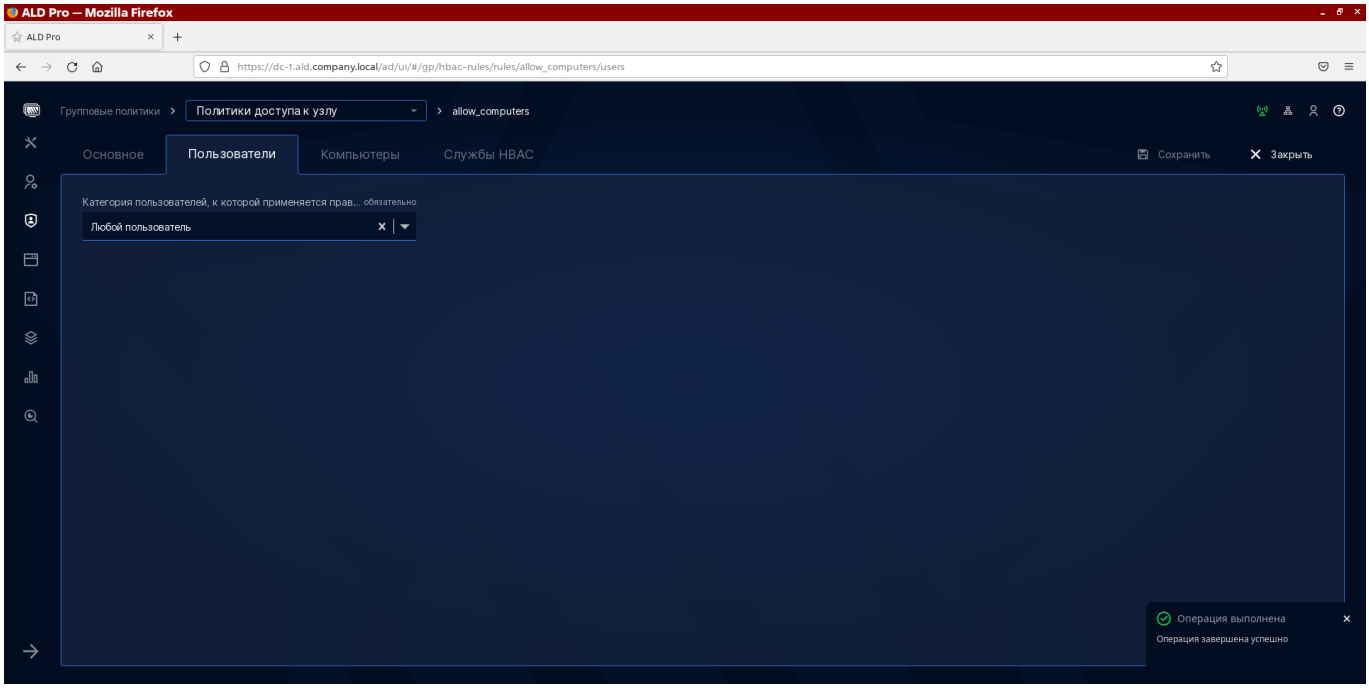


Рисунок 3.10 – Политика доступа к узлу 3

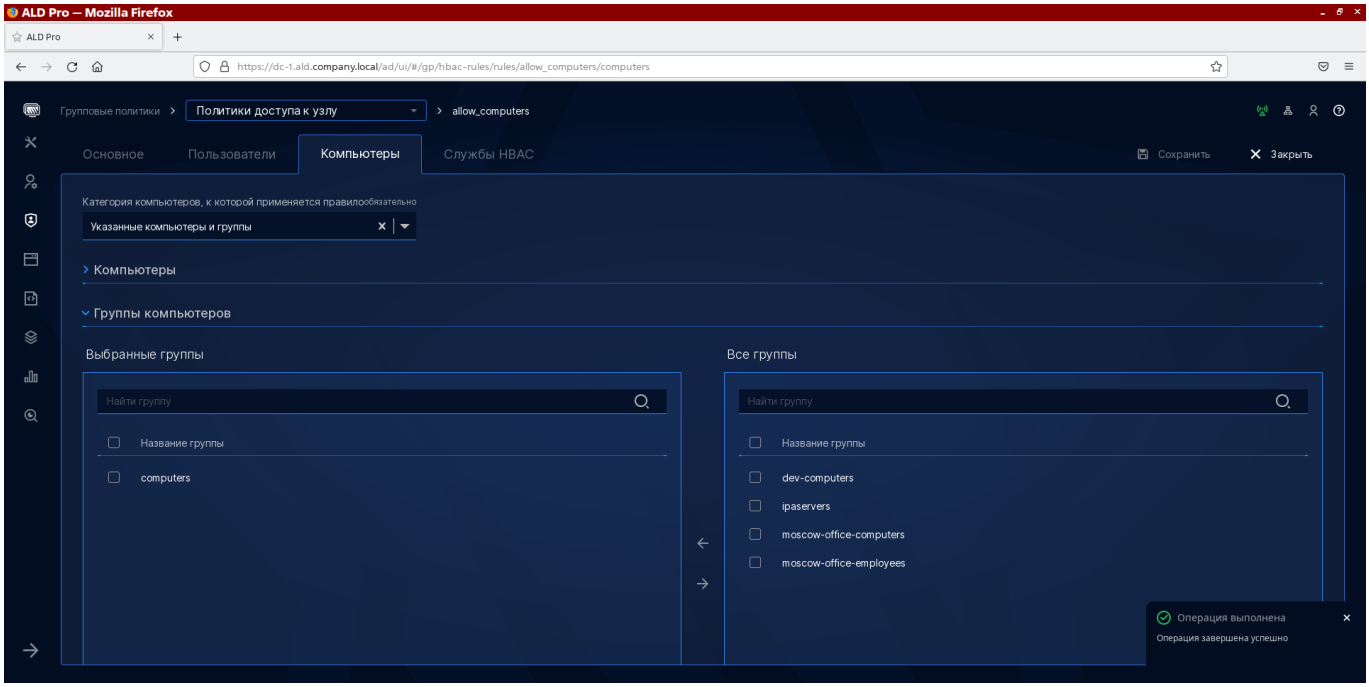


Рисунок 3.11 – Политика доступа к узлу 4

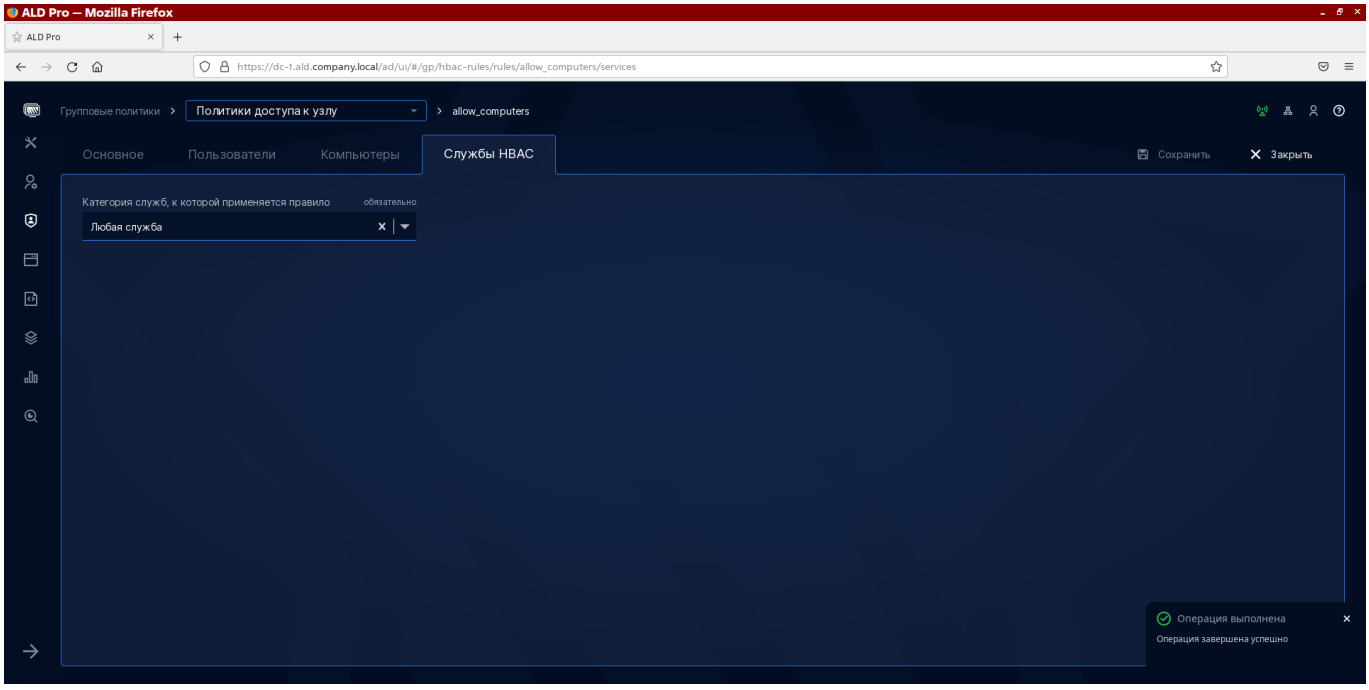


Рисунок 3.12 – Политика доступа к узлу 5

Сделаем то же самое из командной строки:

```
ipa hostgroup-add computers
ipa hostgroup-mod computers --desc='Группа, в которой будут все обычные
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
↪компьютеры домена'
ipa hostgroup-add-member computers --hosts pc-1

ipa hbacrule-add allow_computers
ipa hbacrule-mod allow_computers --desc='Разрешает всем пользователям доступ
↪к обычным компьютерам в домене'
ipa hbacrule-mod allow_computers --usercat=all
ipa hbacrule-mod allow_computers --servicecat=all
ipa hbacrule-add-host allow_computers --hostgroup computers
```

3.3.5. Гранулированный доступ к отдельным службам и отладка правил

Для тонкой настройки HBAC вам потребуется тщательно анализировать типовые сценарии работы пользователей в части используемых служб. Например, для подключения по RDP потребуются fly-wm и xrdp-sesman, см. табл. 9.

Сценарий работы пользователя	К каким идентификаторам служб следует предоставить доступ	Комментарий
Локальный вход в операционную систему	fly-dm, fly-wm	fly-dm - разрешает вход, fly-wm - нужен, чтобы можно было разблокировать экран
Удаленный доступ к менеджеру окон по протоколу RPD	xrdp-sesman, fly-wm	xrdp-sesman - разрешает вход по rdp, fly-wm - нужен, чтобы можно было разблокировать экран
Удаленное администрирование по SSH	sshd, sudo	sshd - разрешает подключение по ssh, sudo - разрешает повышать привилегии в соответствии с правилами SUDO

Службы, необходимые для типовых сценариев работы

Внимание: При переходе с ранних версий ALD Pro до 2.5.0 в системе будет создана группа служб HBAC fly куда будут входить: fly-dm, fly-dm-greeter, fly-dm-np, fly-wm. Если группа fly уже существовала, в нее будут добавлены перечисленные службы.

После установки системы в домене уже есть список наиболее распространенных служб, но какие-то службы все равно потребуется добавить вручную. Сделать это можно будет через веб-интерфейс на странице «Групповые политики > Политики доступа к узлу > Службы HBAC». Пример создания «xrdp-sessman».

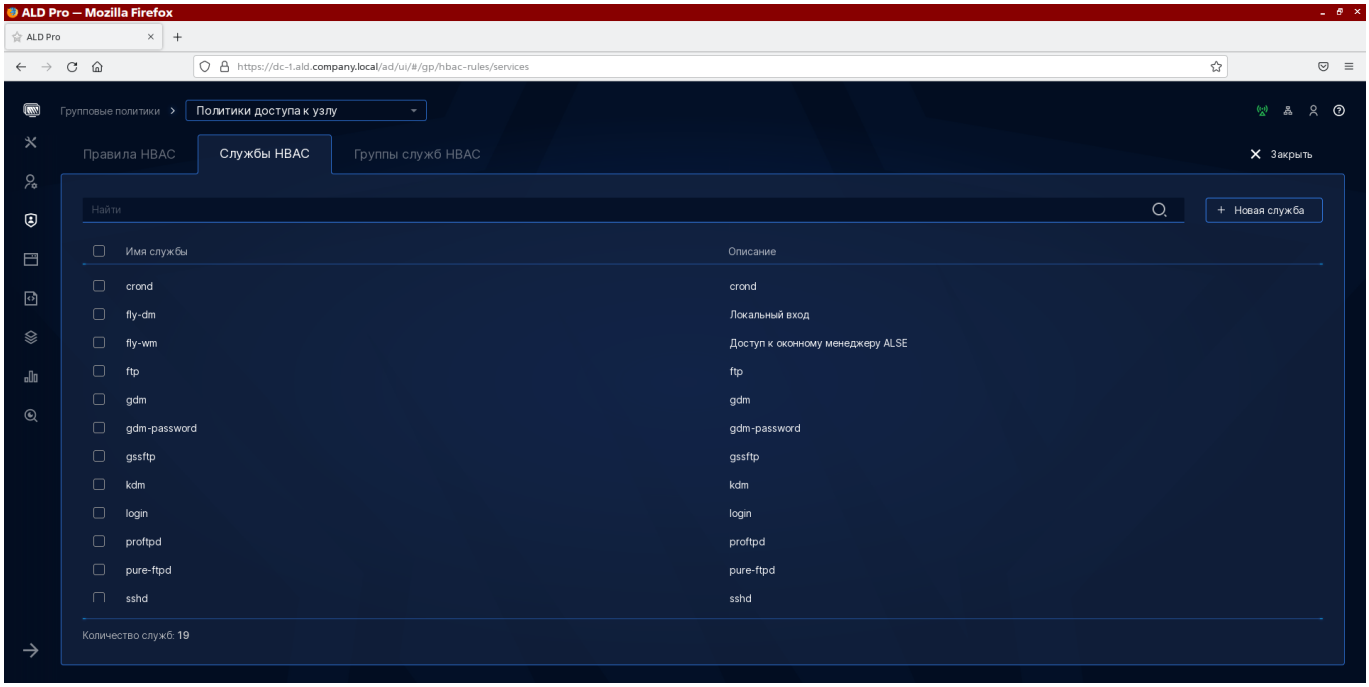


Рисунок 3.13 – Политика доступа к узлу 6

То же самое можно сделать из командной строки:

```
ipa hbacsvc-add 'xrdp-sesman'
ipa hbacsvc-mod 'xrdp-sesman' --desc='Доступ по RDP'
```

Чтобы понять, к какой службе требуется предоставить доступ, выполните необходимое действие на целевой системе и посмотрите, какие сообщения об ошибках появятся в журнале авторизации auth.log:

```
# tail -f varlog/auth.log
...
Mar 15 15:25:22 client 4 sshd[30424]: pam_sss(sshd:account): Access denied
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
↪for user ivanov: 6 (Permission denied)
...
```

Допустим, нам нужно предоставить возможность разработчикам из группы dev-users на своих компьютерах из группы dev-computers только входить в операционную систему, а далее уже расширять возможности при администрировании до root с помощью утилиты su. Создать соответствующее HBAC-правило можно как через портал управления ALD Pro, так и из командной строки.

С использованием веб-интерфейса делается это следующим образом:

1. Создайте HBAC-правило. Для этого откройте страницу «Групповые политики > Политики доступа к узлу > Правила HBAC» и нажмите кнопку «+ Новое правило».

Введите имя правила **«allow_developers»** и нажмите кнопку «Сохранить». Пока вы не сохраните правило, остальные вкладки с настройками будут недоступны.

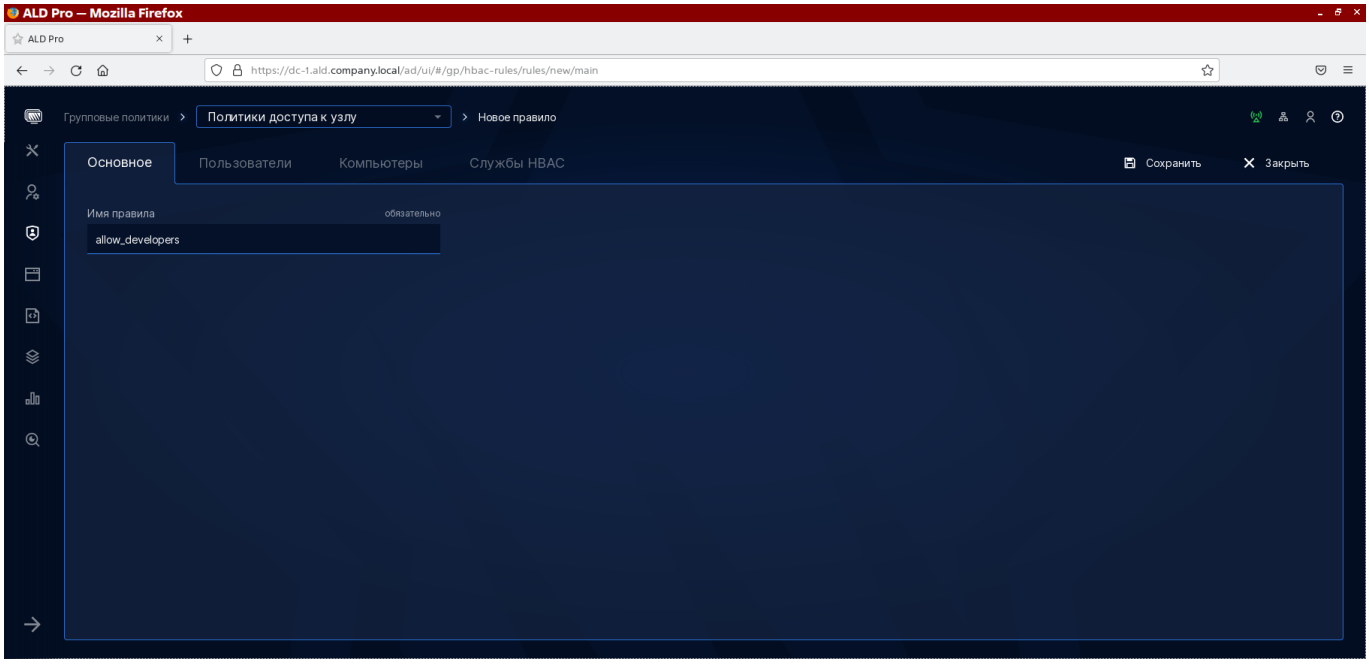


Рисунок 3.14 – Политика доступа к узлу 7

2. Настройте область применения правила в части пользователей, выберите категорию «Указанные пользователи и группы» и добавьте группу «dev-users». В части компьютеров добавьте группу «dev-computers». Не забудьте нажать кнопку «Сохранить» в правом верхнем углу прежде чем переходить к следующей вкладке.

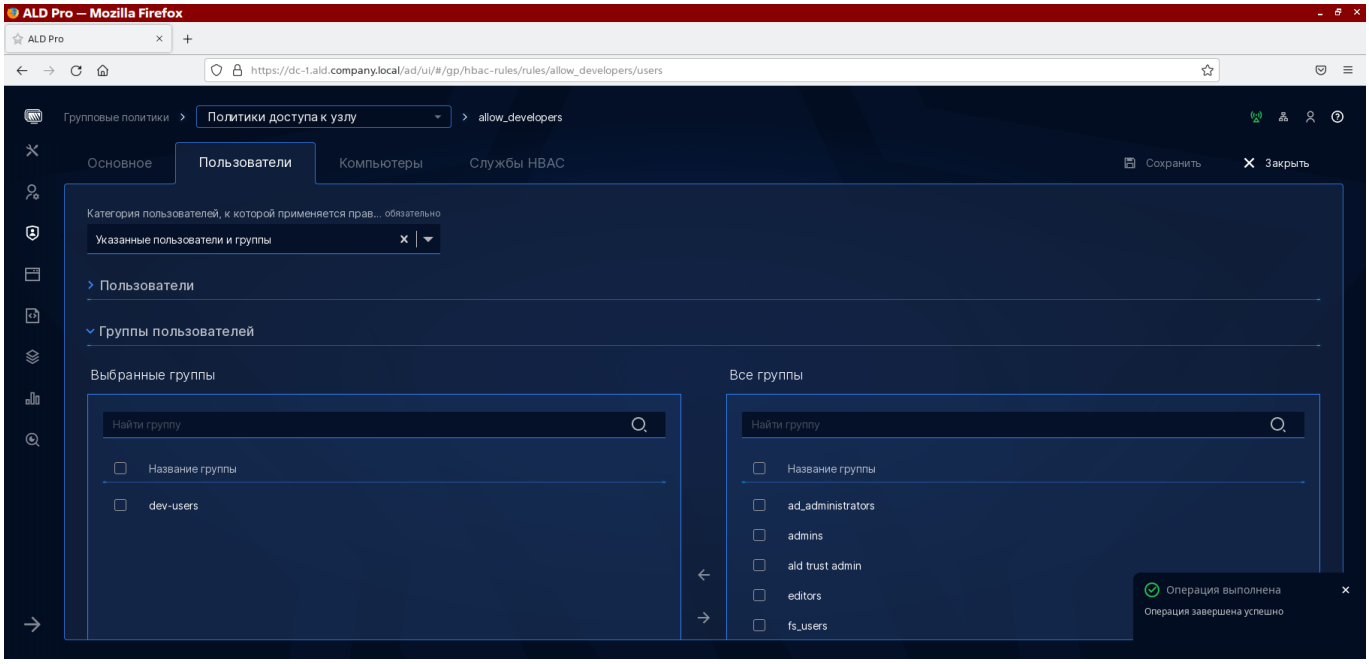


Рисунок 3.15 – Политика доступа к узлу 8

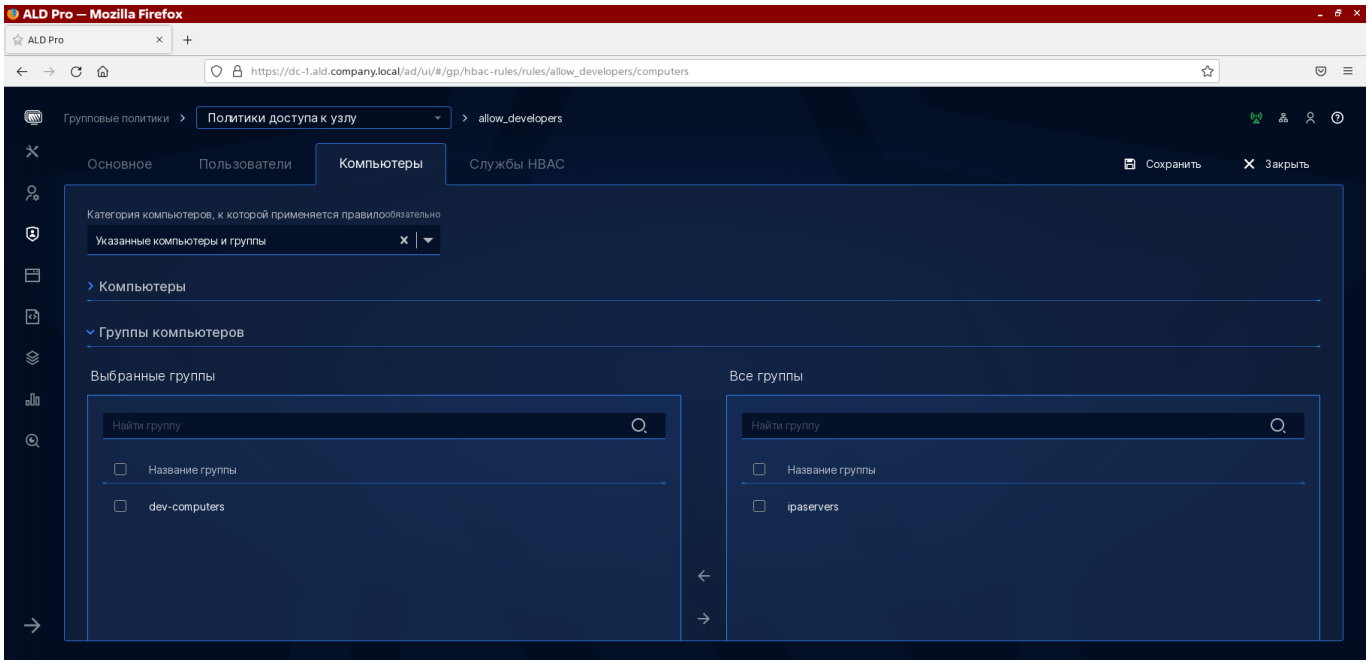


Рисунок 3.16 – Политика доступа к узлу 9

3. Настройте область применения правила в части служб, добавьте «fly-dm», «su» и «su-l» (используется утилитой su при вызове с параметром «-», «-l» или «–login»).

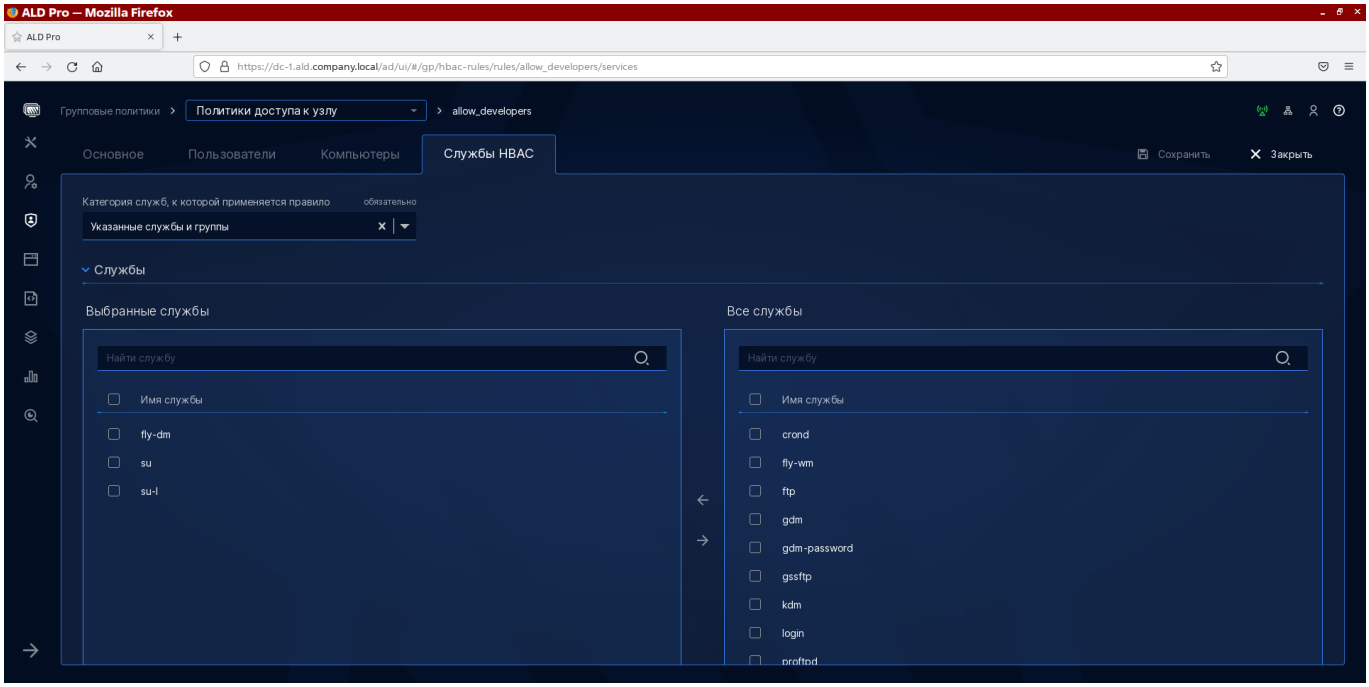


Рисунок 3.17 – Политика доступа к узлу 10

Из командной строки такое правило можно создать следующим образом:

```
kinit admin
ipa hbacrule-add allow_developers
ipa hbacrule-mod allow_developers --desc='Доступ для разработчиков'
ipa hbacrule-add-user allow_developers --groups dev-users
ipa hbacrule-add-host allow_developers --hostgroups dev-computers
ipa hbacrule-add-service allow_developers --hbacsvcs fly-dm
ipa hbacrule-add-service allow_developers --hbacsvcs su
ipa hbacrule-add-service allow_developers --hbacsvcs su-l
```

где:

- `kinit admin` — аутентификация в системе под учетной записью admin;
- `hbacrule-add` — команда для создания HBAC-правила;
- `hbacrule-mod` — команда для модификация правила, ключ desc позволяет задать описание;
- команды `hbacrule-add-user`, `hbacrule-add-host` и `hbacrule-add-service` позволяют определить область применения правила;
- ключ groups — позволяет указать группу пользователей;
- ключ hostgroups — позволяет указать группу хостов;

- ключ hbacsvcs — позволяет указать идентификатор PAM службы.

Следует напомнить, что сразу после создания правила оно может заработать на целевой машине не сразу из-за кеширования sssd.

Теперь, чтобы пользователь смог воспользоваться утилитой `su` на личном компьютере, вам нужно передать ему пароль от учетной записи root.

Скорее всего, у пользователя `root` нет пароля и в файле `/etc/shadow-` в том месте, где должен быть указан хэш пароля вы увидите восклицательный знак. Откройте терминал на целевой системе и установите пользователю root пароль следующим образом:

```
admin@pc-1:~$ sudo -i
root@pc-1:~# passwd root
Новый пароль : *****
Повторите ввод нового пароля : *****
passwd: пароль успешно обновлён
```

Теперь пользователь может проверить, что у него есть доступ к компьютеру через графику и он может с помощью команды `su` запустить `bash` от имени root.

Когда у вас в домене два-три правила, их довольно легко проверить напрямую подключаясь к целевым хостам под тестовыми учетными записями, но в реальной инфраструктуре потребуется управлять десятками правил, и упростить их отладку поможет команда ipa hbactest. Команду можно выполнить на контроллере домена и для любого сочетания пользователь-хост-сервис получить ответ, есть ли в домене правило, которое соответствует этим критериям.

Выполним проверку, сможет ли пользователь ivanov воспользоваться службой sshd при подключении к хосту client4 по протоколу ssh:

```
ipa hbactest --user=ivanov --host=client4 --service=sshd
--------------------------
Доступ предоставлен: False
--------------------------
Несоответствующие правила: 1
Несоответствующие правила: allow_systemd-user
```

Решение False означает, что пользователю будет отказано в доступе.

Выполним проверку конкретного правила allow_developers с помощью ключа –rules, сможет ли пользователь ivanov выполнить вход на компьютер client4, для чего ему нужна

служба fly-dm:

```
ipa hbactest --user=ivanov --host=client4 --service=fly-dm --rules allow_
 ↪developers
-------------------------
Доступ предоставлен: True
-------------------------
Соответствующие правила: allow_developers
```

Решение True означает, что пользователю будет предоставлен доступ в соответствии с правилом allow_developers, значит пользователь ivanov входит в группу пользователей dev-users, а хост client4 в группу хостов dev-computers.

3.3.6. Лучшие практики: ограничение доступа локальным пользователям

Вопрос управления локальными учетными записями на компьютерах домена является одним из важнейших аспектов безопасности, который требует повышенного внимания со стороны системных администраторов.

Есть разные подходы к организации управления учетными записями локальных администраторов в домене, например, вы можете их полностью отключить, организовать управление через скрипты групповых политик или даже разработать стороннее решение, реализующее функции, аналогичные программному продукту LAPS от Microsoft (Local admin password solution).

В рамках данной статьи рассмотрим самый простой из них — это полное блокирование локальных учетных записей. Для того, чтобы заблокировать локальную учетную запись localadmin после ввода компьютера в домен вам достаточно будет выполнить команду:

```
passwd -l localadmin
```

Теперь вы можете убедиться, что вход и доступ к системе с помощью этой учетной записи будет запрещен.

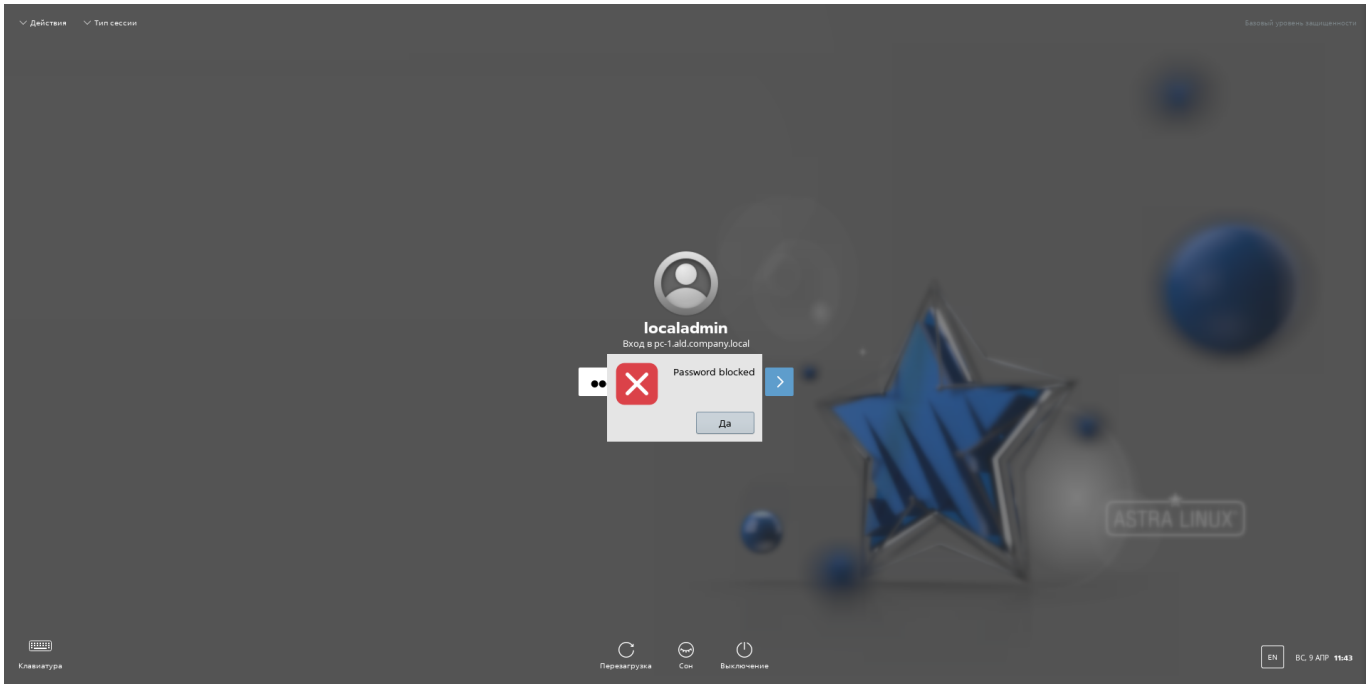


Рисунок 3.18 – Группа пользователей

3.3.7. Лучшие практики: создание HBAC-правил для структурных подразделений

Область применения HBAC-правил можно задать с помощью групп пользователей и групп хостов, но в некоторых случаях может быть удобнее использовать для этого структурные подразделения. В этом случае вы можете воспользоваться вспомогательными группами и правилами автоучастия (automember).

Привязка объектов к структурным подразделениям в ALD Pro осуществляется с помощью атрибута rbtadp, в котором хранится ссылка на целевое подразделение в формате полного уникального имени записи (Distinguished name, DN). Например, если у вас в корне домена есть структурное подразделение «Московский офис», то значение атрибута rbtadp всех его дочерних объектов будет содержать `ou=Московский офис,ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan`. Если вам потребуется ограничить выборку только прямыми наследниками, вы можете поставить символ подстановки «^» в начало строки, что позволит вам исключить объекты из подразделений, расположенных ниже по иерархии организационной структуры.

Создадим группу пользователей и правило автоучастия из веб-интерфейса:

1. Создайте группу пользователей, для этого на странице «Пользователи и компьютеры

> Группы пользователей» нажмите кнопку «+ Новая группа», введите название группы «moscow-office-employees», выберите подразделение «Московский офис» и нажмите кнопку «Сохранить».

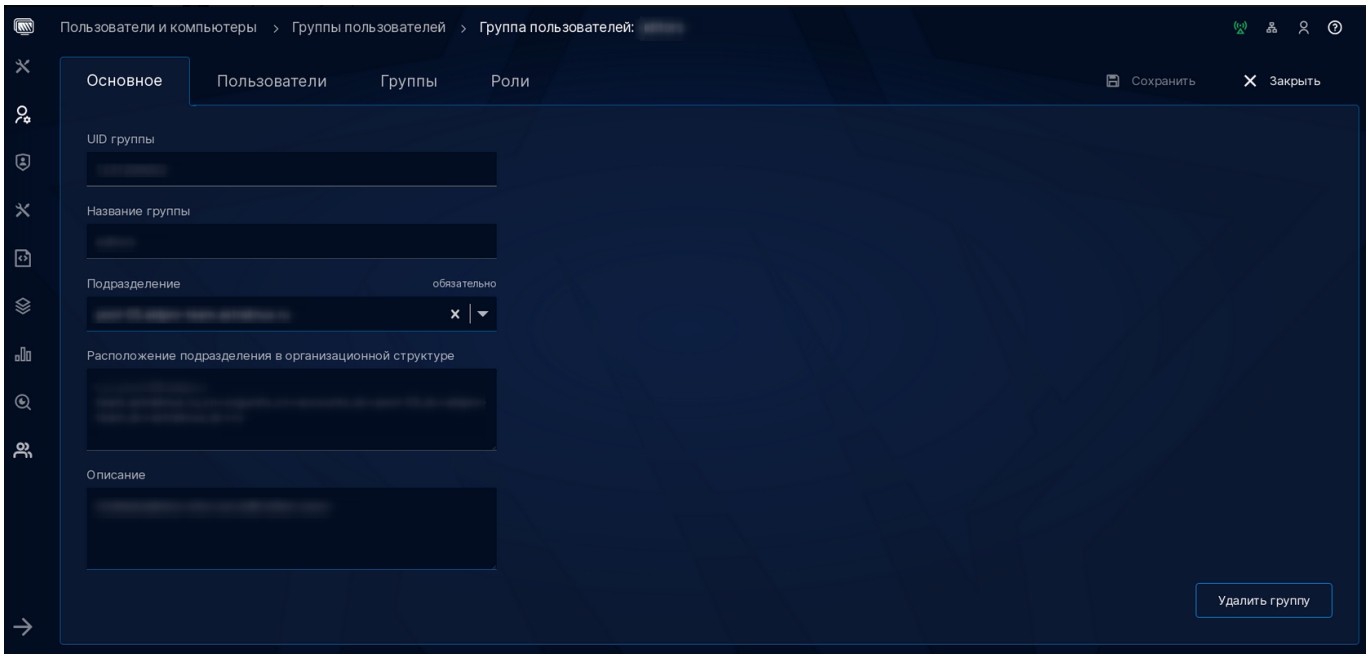


Рисунок 3.19 – Добавление правила

2. Создайте правило автоучастия, для этого потребуется воспользоваться интерфейсом FreeIPA. Откройте страницу «Идентификация > Автоучастник > Правила группы пользователей», нажмите кнопку «Добавить». В диалоговом окне добавления правила выберите группу «moscow-office-employees» из списка и нажмите кнопку «Добавить и изменить».

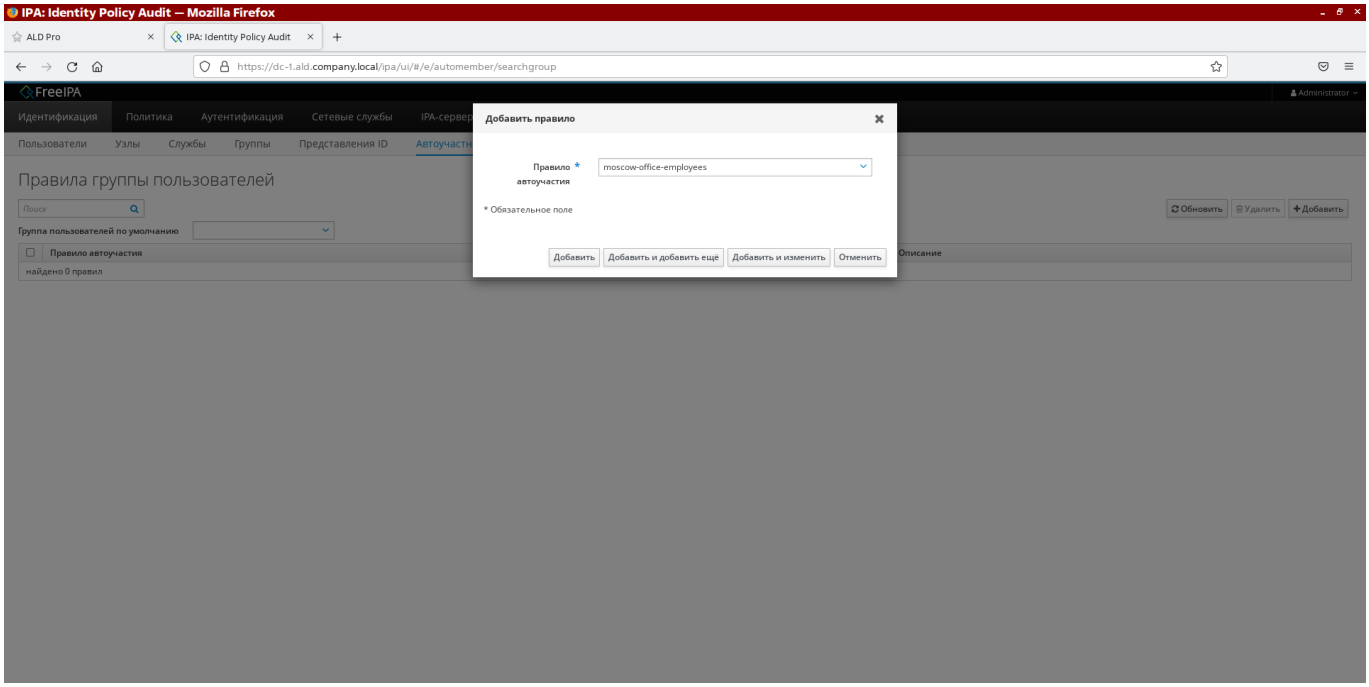


Рисунок 3.20 – Правило группы пользователей

3. На странице редактирования правила добавьте включающий критерий отбора записей по атрибуту rbtadp и значению ou=Московский офис,ou=ald.company.lan, cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan.

Пересчет правил автоучастия происходит не мгновенно, но вы можете ускорить применение этих правил с помощью команды automember-rebuild:

```
ipa automember-rebuild --type=group
```

Если пользователи так и не появятся в списке участников группы, проверьте корректность фильтра. Обзор записей выполняется по полному вхождению, поэтому никаких лишних пробелов в середине строки быть не должно.

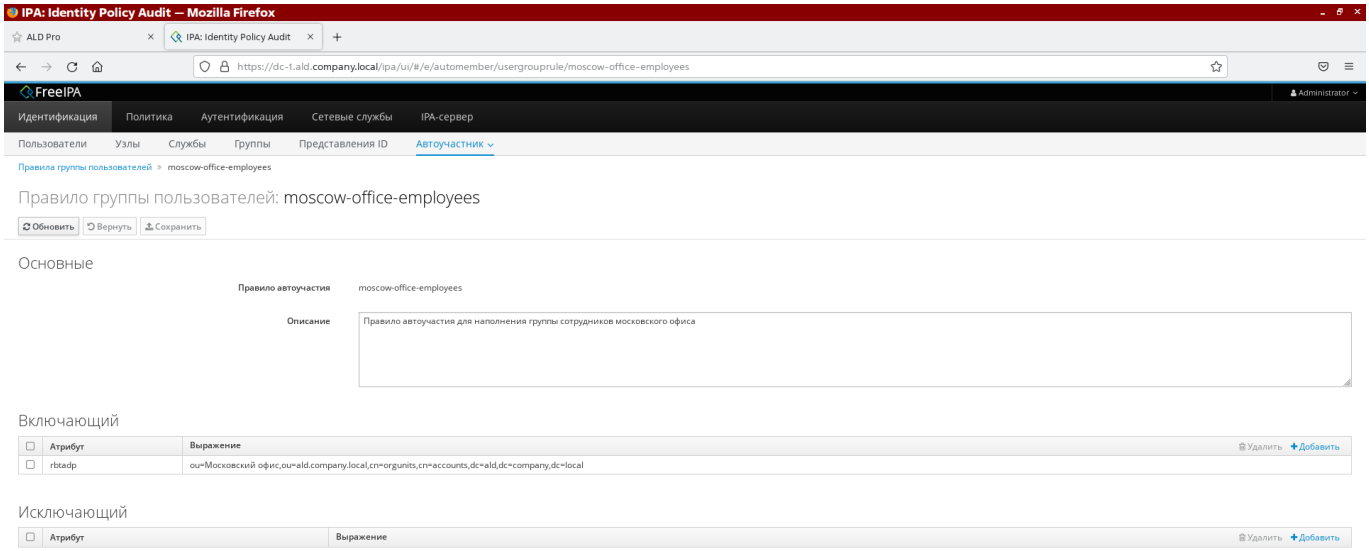


Рисунок 3.21 – Правило группы пользователей

То же самое вы можете сделать из командной строки:

1. Создайте группу пользователей moscow-office-employees в подразделении «Московский офис»:

```
ipa group-add moscow-office-employees
ipa group-mod moscow-office-employees setattr="rbtadp=ou=Московский офис,
↪ou=ald.company.lan, cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan"
ipa group-mod moscow-office-employees --desc='Группа, в которой будут все
↪сотрудники московского офиса'
```

2. Создайте правило автоучастия и определите критерий автоучастие:

```
ipa automember-add moscow-office-employees --type=group
ipa automember-mod moscow-office-employees --type=group --desc='Правило
↪автоучастия для наполнения группы сотрудников московского офиса'
ipa automember-add-condition moscow-office-employees --type=group --
↪key=rbtadp --inclusive-regex='ou=Московский офис,ou=ald.company.lan,
↪cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan'
```

3. Принудительно обновите состав автоучастников (запускать команду нужно только 1 раз, в дальнейшем правила будут срабатывать автоматически при изменении подразделения объекта):

```
ipa automember-rebuild --type=group
```

3.4. Автоматизация задач администрирования через LDAP-запросы

3.4.1. Введение

Автоматизация позволяет ускорить выполнение массовых операций администрирования, например, если требуется завести тысячу пользователей, следует написать скрипт для импорта учетных записей из **CSV-файла**, автоматически распределяющий пользователей по подразделениям и в соответствующие группы. Этот способ позволяет экономить время и исключает ошибки, связанные с человеческим фактором.

В данной инструкции описано устройство **LDAP-каталога**, алгоритм управления доменом с помощью прямых запросов к каталогу, а также несколько полезных запросов для решения реальных задач администрирования.

3.4.2. Технология LDAP

Служба каталога **ALD Pro** построена на базе 389 Directory Server, который реализует функции каталога и поддерживает протокол **LDAPv3**. Облегченный протокол доступа к данным каталога (Lightweight Directory Access Protocol, **LDAP**) является упрощенной модификацией более строгих стандартов для построения службы распределенного каталога сети X.500.

Каталог **LDAP** является специализированной нереляционной базой данных, файлы которой расположены в папке `/var/lib/dirsrv/slapd-ald-company-lan/db`. Информация каталога представлена в виде древовидной структуры, которую также называют **Directory Information Tree** или сокращенно **DIT**. См. *Рисунок 6.4.1 Структура каталога Directory Information Tree*

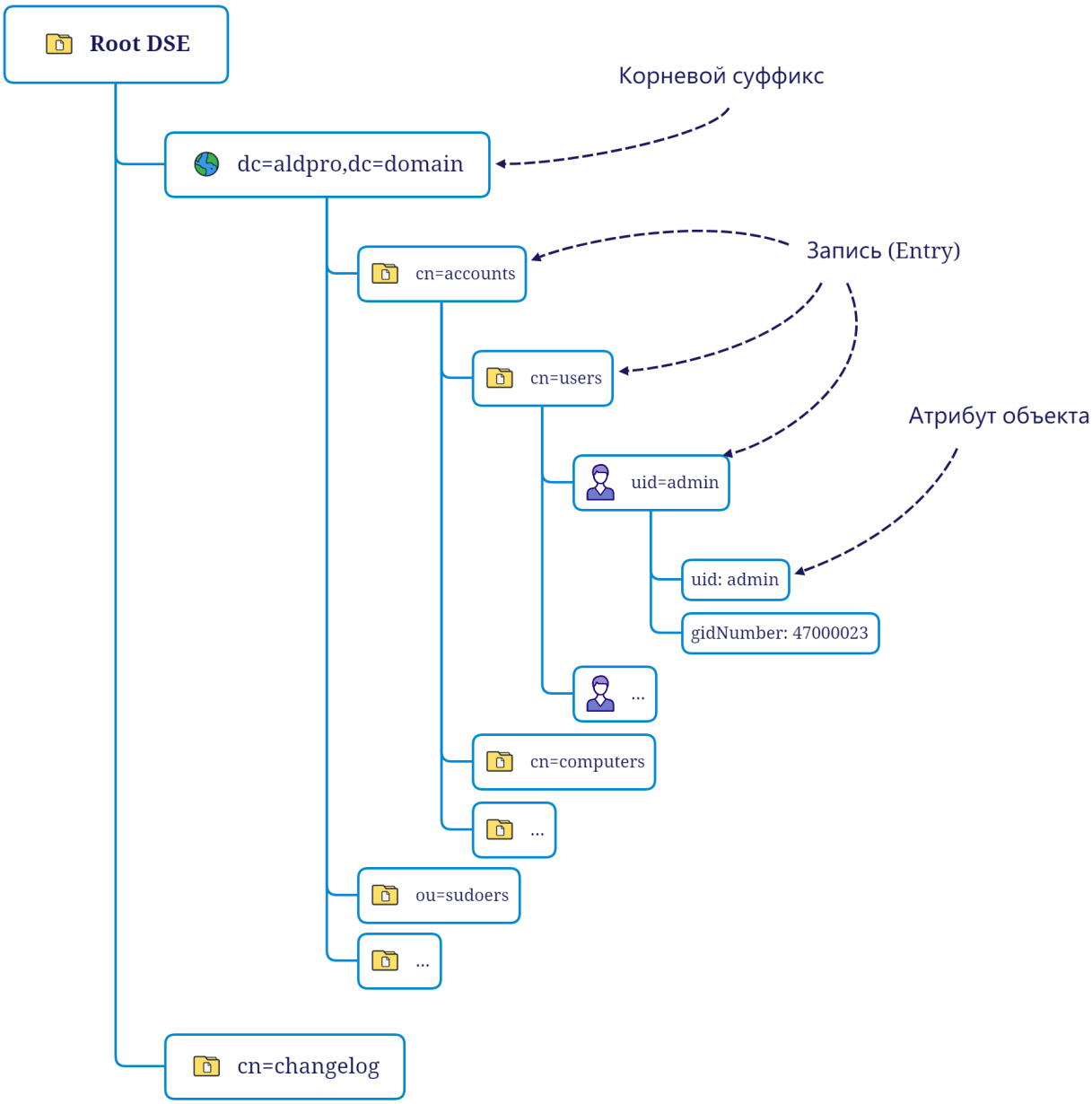


Рисунок 3.22 – Рисунок 6.4.1 Структура каталога Directory Information Tree

Корень каталога называется **Root DSE**, где **DSE** означает **Directory system agent Specific Entry**, то есть специализированная запись агента системы директорий. Эта запись не имеет родителя, и она описана в файле `/etc/dirsrv/slapd-ALD-COMPANY-LAN/dse.ldif`, где `slapd-ALD-COMPANY-LAN` - директория сервиса `slapd` с именем домена.

Корень **Root DSE** является родителем для записей `dc=ald,dc=company,dc=lan` и `cn=changelog`, которые так же называют базовыми записями, корневыми суффиксами

или контекстами именования (base entry, root suffix, naming context). В контексте `dc=ald,dc=company,dc=lan` хранятся все объекты каталога, а в `cn=changelog` – журнал изменений для работы плагина `Retro Changelog Plugin`. Все контексты, определенные в каталоге, указаны в операционном атрибуте `namingContexts` записи **Root DSE**, однако спецификация **LDAP** позволяет также использовать служебные контексты, например, в записи `cn=config` представлены настройки каталога, а через запись `cn=monitor` можно получить доступ к информации о состоянии сервера в режиме реального времени.

Существуют разные подходы в задании наименований корневых суффиксов, в **ALD Pro** (FreeIPA) используются правила спецификации RFC-2247, поэтому для домена `ald.company.lan` имя корневого суффикса будет `dc=ald,dc=company,dc=lan`, где `dc` – компонент имени домена, сокращение от **Domain Component**. Правила наименования необходимы для возможности преобразования DNS-имени в имя **LDAP-записи** и наоборот.

От корневого суффикса `dc=ald,dc=company,dc=lan` ответвляются дочерние записи (Entry), которые, в свою очередь, могут быть контейнерами для других записей, за счет чего и образуется древовидная структура. Таким образом, записи каталога можно сравнить с директориями файловой системы.

У каждой записи каталога есть имя, которое должно быть уникальным в пределах родительского контейнера, поэтому оно называется относительно уникальным именем **Relative Distinguished Name** или кратко **RDN**. Учетные записи пользователей, например, имеют имена `uid=admin`, `uid=ivan.kuznetsov` и т.д. Особенность имен объектов в **LDAP** заключается в том, что они хранят не конкретные значения, а только ссылки на хранимые атрибуты записей, которые используются для идентификации объектов. Например, для идентификации учетных записей пользователей используют атрибут `uid`, для учетных записей компьютеров `FQDN` (fully qualified domain name, полное доменное имя хоста), а в именах контейнеров обычно присутствует `cn` (common name, общее имя).

В приведенном примере **RDN** учетной записи доменного администратора `uid=admin` состоит из названия атрибута `uid`, после которого идет символ присвоения `=` и далее значение атрибута `admin`. Вся эта запись вместе называется «Определением Значения Атрибута» - **Attribute Value Assertion (AVA)**. Обычно имена записей задаются значением одного атрибута, но могут использоваться и несколько, тогда в имени **RDN** эти определения AVA будут объединяться знаком `+`, например: `cn=Ivan+l=Moscow`. Каталог 389 Directory Server поддерживает такой способ именования записей, но в **ALD Pro** (FreeIPA) он не используется.

Для идентификации объекта в пределах всего каталога используют уникальное имя

Distinguished Name или сокращенно **DN**. Уникальное имя представляет из себя цепочку **RDN**, которые записывают через запятую слева направо, начиная с целевой записи и до корневого суффикса вверх по иерархии, см. *Рисунок 6.4.2 Пример формирования уникального имени записи DN*. Если привести аналогию с объектами файловой системы, то **RDN** будет соответствовать имени объекта директории или файла, а **DN** – полному имени объекта файловой системы, которое включает путь к родительскому объекту и имени объекта. И также как на одном диске не может быть двух директорий с одинаковыми полными именами, в каталоге **LDAP** не может быть двух записей с одинаковыми **DN**. Описание формата **DN** можно найти RFC 4514.

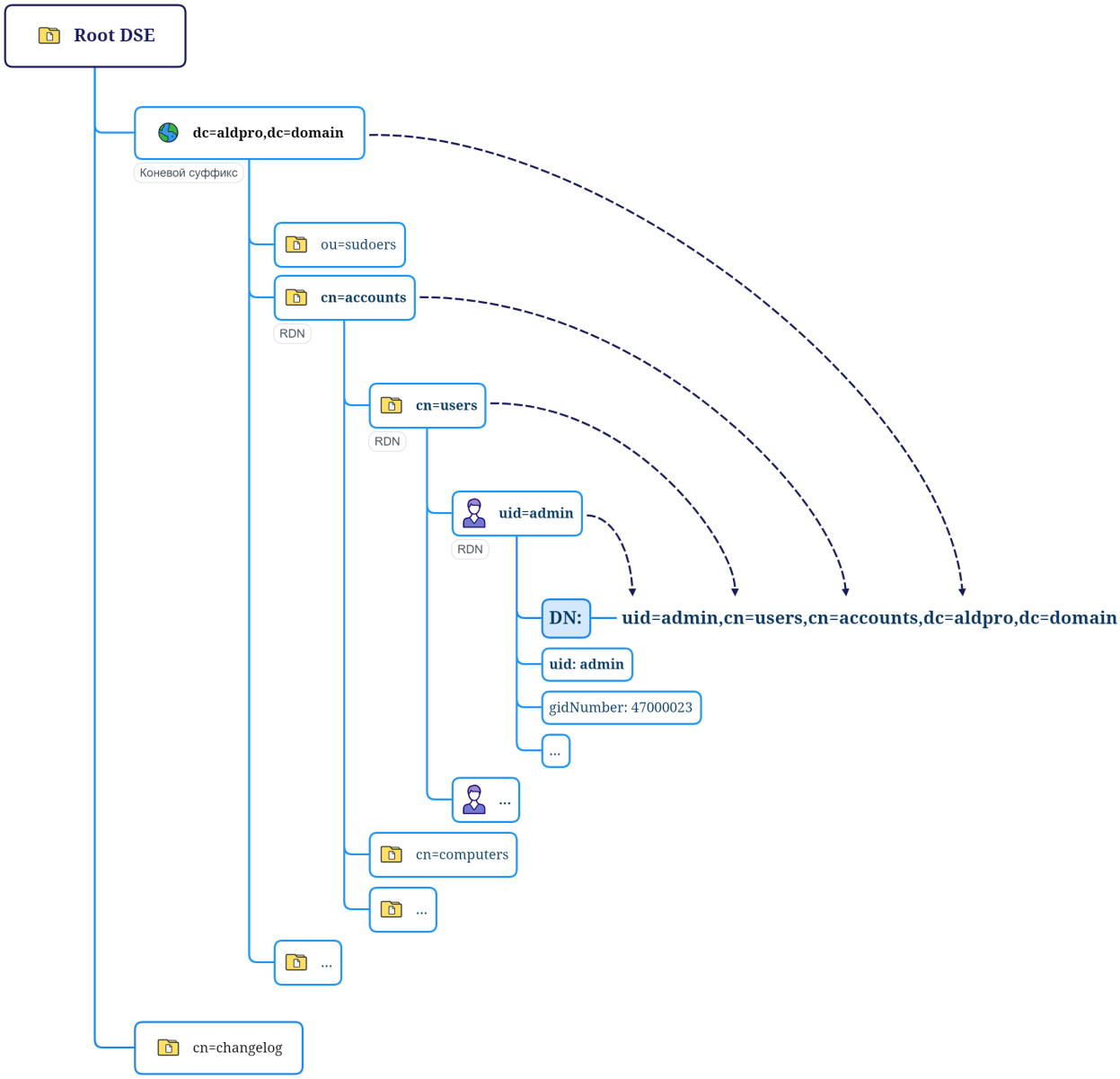


Рисунок 3.23 – Рисунок 6.4.2 Пример формирования уникального имени записи DN

Запись каталога может хранить не только дочерние записи, но и набор атрибутов, описывающих ее свойства. Например, для учетной записи пользователя это могут быть ФИО, должность, номер телефона и т.д.

Данные в **LDAP-каталоге** строго структурированы и все атрибуты должны быть определены в схеме данных заранее. Перечень доступных для конкретного объекта атрибутов задается списком назначенных ему классов, см. атрибут `objectClass`. Например, учетные записи пользователей могут содержать атрибут `gidNumber` по той причине, что им назначен класс объектов `posixAccount`, см. *Рисунок 6.4.3 Возможность указать gidNumber определяется наличием класса объектов posixAccount*.

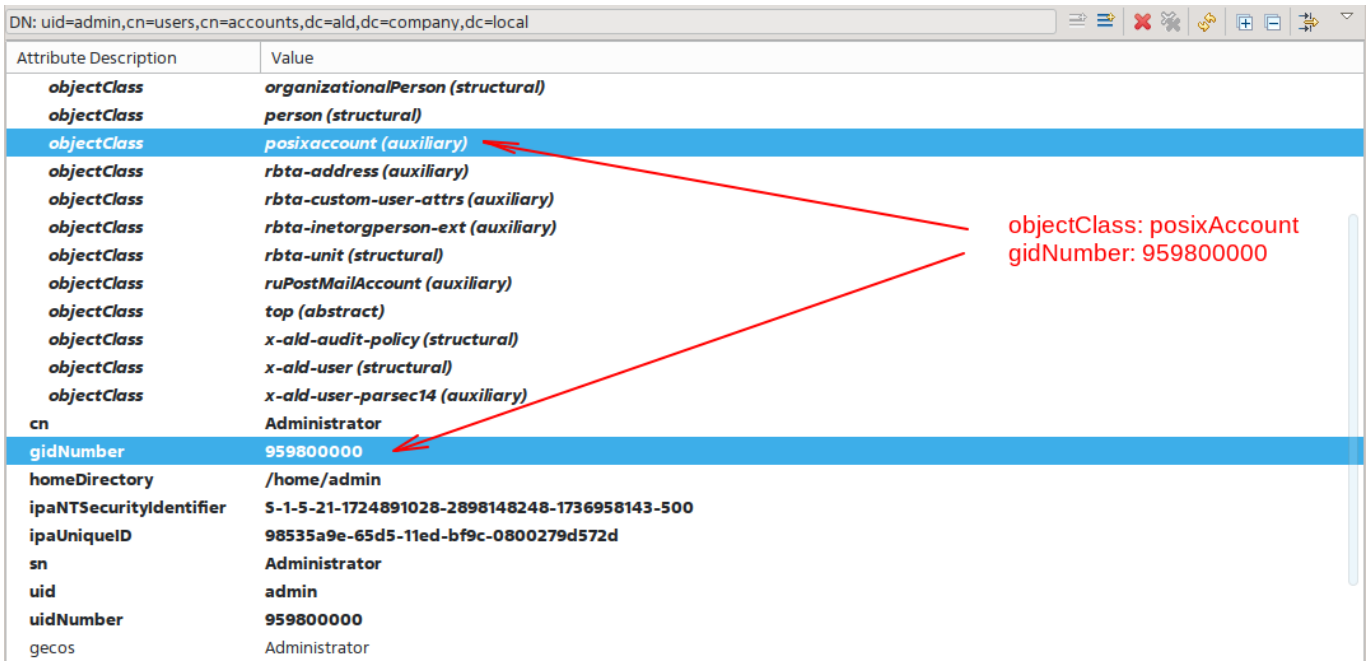


Рисунок 3.24 – Рисунок 6.4.3 Возможность указать gidNumber определяется наличием класса объектов posixAccount

Всем объектам каталога назначен, как минимум, один класс `top`, т.к. в нем описан атрибут `objectClass`, с помощью которого работает механизм назначения классов. Объекты с одним классом практически не используются, поэтому в каталоге у объектов два и более класса.

Для демонстрации ниже указан класс объектов `posixGroup`, который определен в схеме следующим образом:

```
( 1.3.6.1.1.1.2.2 NAME 'posixGroup' DESC 'Standard LDAP objectclass' SUP top
 ↪STRUCTURAL MUST ( cn $ gidNumber ) MAY ( userPassword $ memberUid $
 ↪description ) X-ORIGIN 'RFC 2307' )
```

где:

- `1.3.6.1.1.1.2.2` – это идентификатор объекта (object id, `OID`). Глобальные идентификаторы присваиваются международными организациями (IANA, ISO, ITU-T, ANSI, BSI), а для расширения схемы в прикладных системах используется пространство номеров с префиксом `1.3.6.1.4.1.X`, где `X` – это внутренний номер организации. Например, объекты компании X имеют префикс `1.3.6.1.4.1.47836.`;
- `NAME ' '` – инструкция NAME задает имя класса;
- `DESC ' '` – инструкция DESC задает описание класса;
- `SUP ' '` – инструкция SUP указывает родительский класс. В приведенном примере наследование идет от класса `top`, поэтому объектам будет доступен его атрибут `objectClass`;
- `STRUCTURAL` – инструкция указывает, что класс относится к виду структурных. Существуют также абстрактные (ABSTRACT) и вспомогательные (AUXILIARY) классы, но в контексте автоматизации различия между видами классов не принципиальны;
- `MUST` и `MAY` – инструкции, которые позволяют задать списки обязательных и дополнительных атрибутов. Полный перечень атрибутов, доступных объекту, расширяется атрибутами, которые наследуются от всех родительских классов;
- `X-ORIGIN ' '` – инструкция, которая позволяет задать комментарий с ссылкой на документацию, из которой можно почерпнуть дополнительную информацию об этом классе. В приведенном примере информацию следует искать в документе RFC 2307.

Один и тот же атрибут может быть использован в нескольких классах, поэтому пользователям можно задать значение `gidNumber`, т.к. им назначен класс `posixAccount`, и, в то же время, он может быть задан у групп, т.к. им назначен класс `posixGroup`, см. *Рисунок 6.4.4 Использование атрибута gidNumber классами posixAccount и posixGroup*.

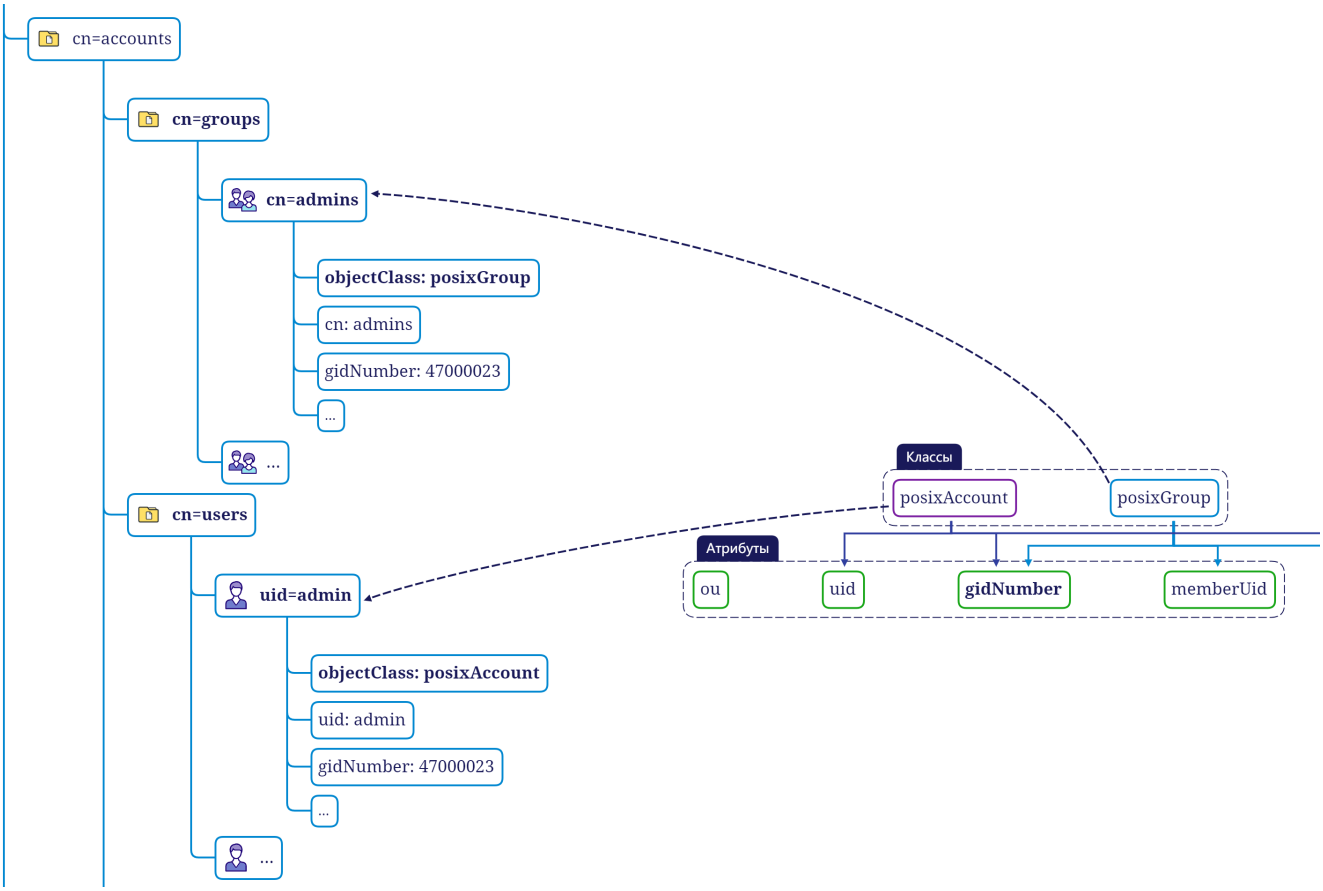


Рисунок 3.25 – Рисунок 6.4.4 Использование атрибута gidNumber классами posixAccount и posixGroup

Подробное описание атрибута `gidNumber`:

```
( 1.3.6.1.1.1.1.1 NAME 'gidNumber' DESC 'Standard LDAP attribute type'
↪SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE X-ORIGIN 'RFC 2307' )
```

где:

- `1.3.6.1.1.1.1.1` – это уникальный идентификатор атрибута;
- `NAME ' '` – инструкция NAME задает атрибута;
- `DESC ' '` – инструкция DESC задает описание атрибута;
- `SYNTAX ' '` – инструкция задает тип хранимого в атрибуте значения. В приведенном примере `1.3.6.1.4.1.1466.115.121.1.27` соответствует целым числам. Описание всех типов данных можно найти в RFC4517;
- `SINGLE-VALUE` – инструкция указывает, что атрибут может хранит только одно значение. Если этой инструкции не будет, то объектам можно будет присваивать несколько значений этого атрибута;

- `X-ORIGIN ' '` – инструкция, которая позволяет задать комментарий с ссылкой на документацию.

Описание схемы данных хранится в файлах на диске в директориях:

- `/usr/share/dirsrv/schema/`
- `/etc/dirsrv/schema/`
- `/usr/share/dirsrv/updates/`
- `/etc/dirsrv/slapd-ALD-COMPANY-LAN/`

При обращении к каталогу по **LDAP** информацию можно получить из операционного **DIT** `cn=schema`.

3.4.3. Взаимодействие с каталогом через LDAP-протокол

3.4.3.1. Графическое приложение для работы с LDAP-каталогом (Apache Directory Studio)

Для работы с **LDAP-каталогом** из графического интерфейса: просмотра структуры каталога, редактирования записей, импорта и экспорта данных – можно воспользоваться таким бесплатным инструментом, как Apache Directory Studio, см. *Рисунок 6.4.5 Apache Directory Studio*. Загрузить приложение можно с официального сайта, для работы потребуется `java runtime`.

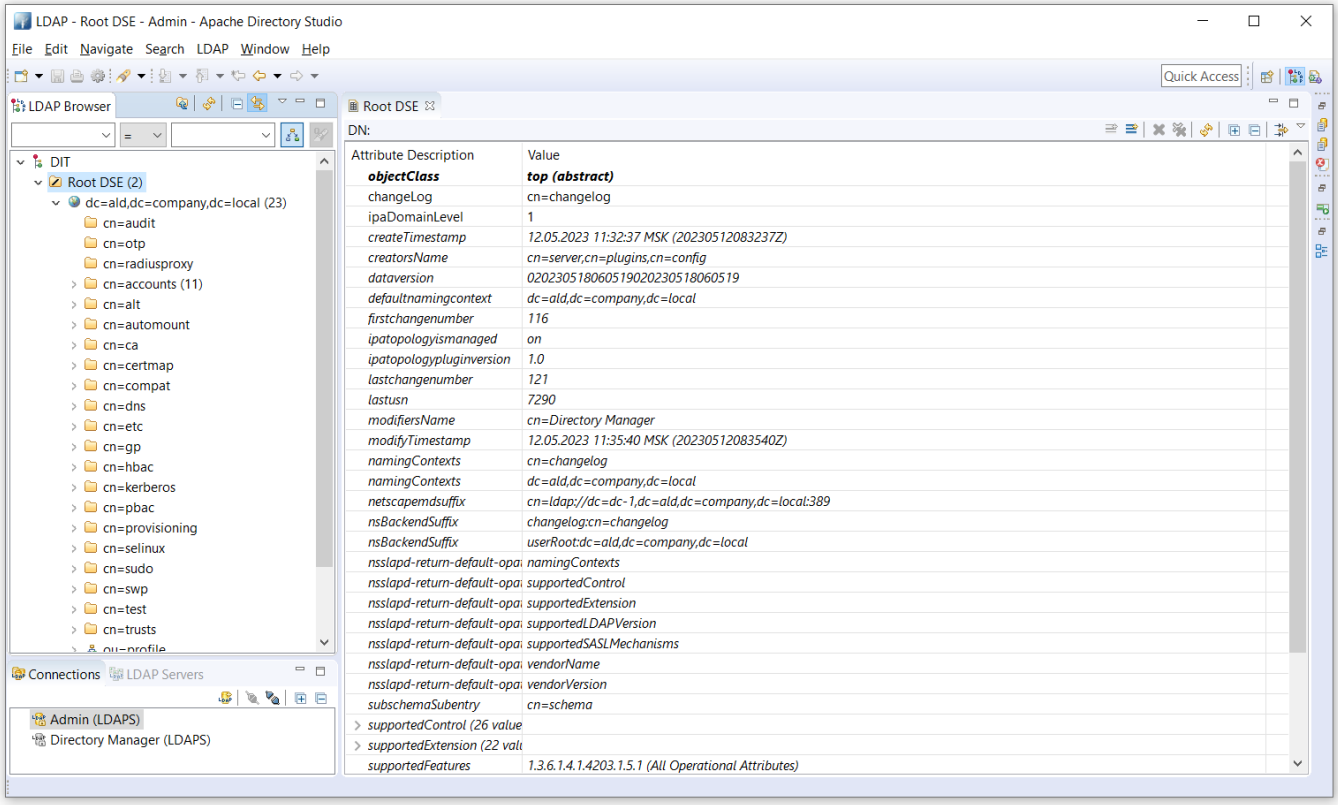


Рисунок 3.26 – Рисунок 6.4.5 Apache Directory Studio

Настройка соединения

Чтобы подключиться к **LDAP-каталогу** нужно создать новое соединение через меню **LDAP** > **New connection**. Откроется окно для создания нового подключения см. *Рисунок 6.4.6 Настройка сети для нового LDAP-подключения*.

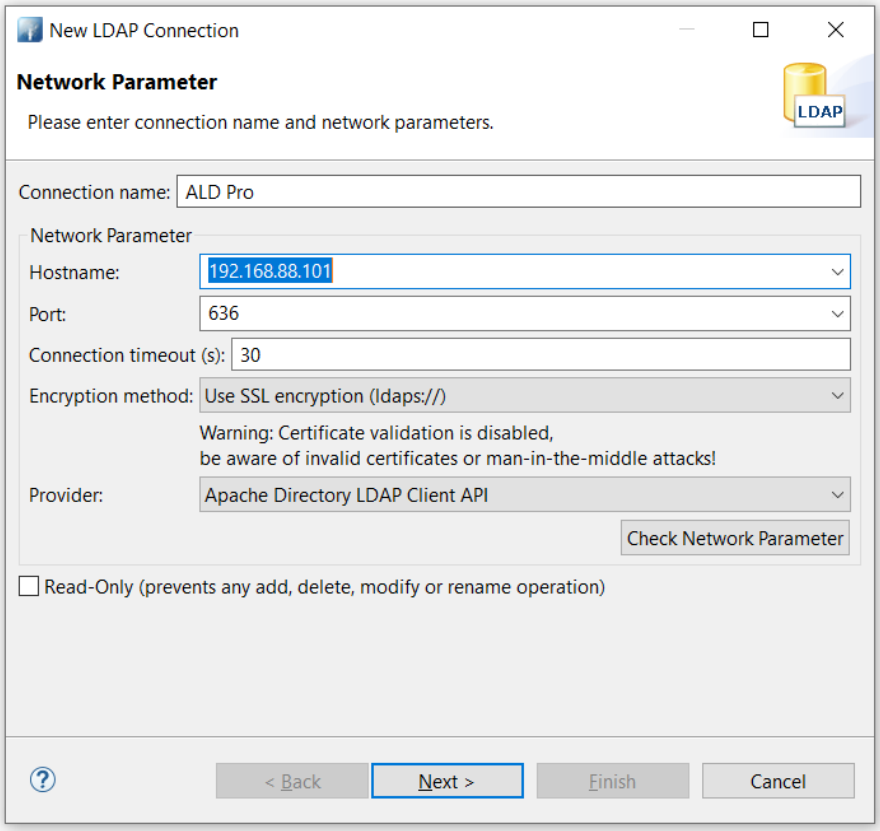


Рисунок 3.27 – Рисунок 6.4.6 Настройка сети для нового LDAP-подключения

Примечание: По умолчанию Apache Directory Studio предлагает создать незащищенное подключение на порт 389, что допустимо только при обращении к каталогу по `localhost`, т.е. приложение должно быть установлено непосредственно на контроллер домена, т.к. при подключении пароль будет передаваться в открытом виде. В случае подключения к каталогу с клиента, обязательно использование порта 636 и метода шифрования SSL, чтобы перехват пароля был невозможен.

Аутентификация по паролю называется связыванием (Bind). Подключение к каталогу доступно с правами супер-пользователя `cn=Directory Manager` или доменного администратора **ALD Pro** `uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan`, см. *Рисунок 6.4.7 Настройка аутентификации для нового LDAP-подключения*. В зависимости от учетной записи права на доступ к записям и атрибутам разнятся.

Примечание: Сразу после установки системы пароли этих учетных записей совпадают.

Чтобы сбросить пароль Directory Manager потребуется вручную менять хэш, записанный в файле *dse.ldif*, в строке, начинающейся с `nsslapd-rootpw`.

Перед закрытием окна следует проверить корректность подключения нажатием кнопки **Check Authentication**.

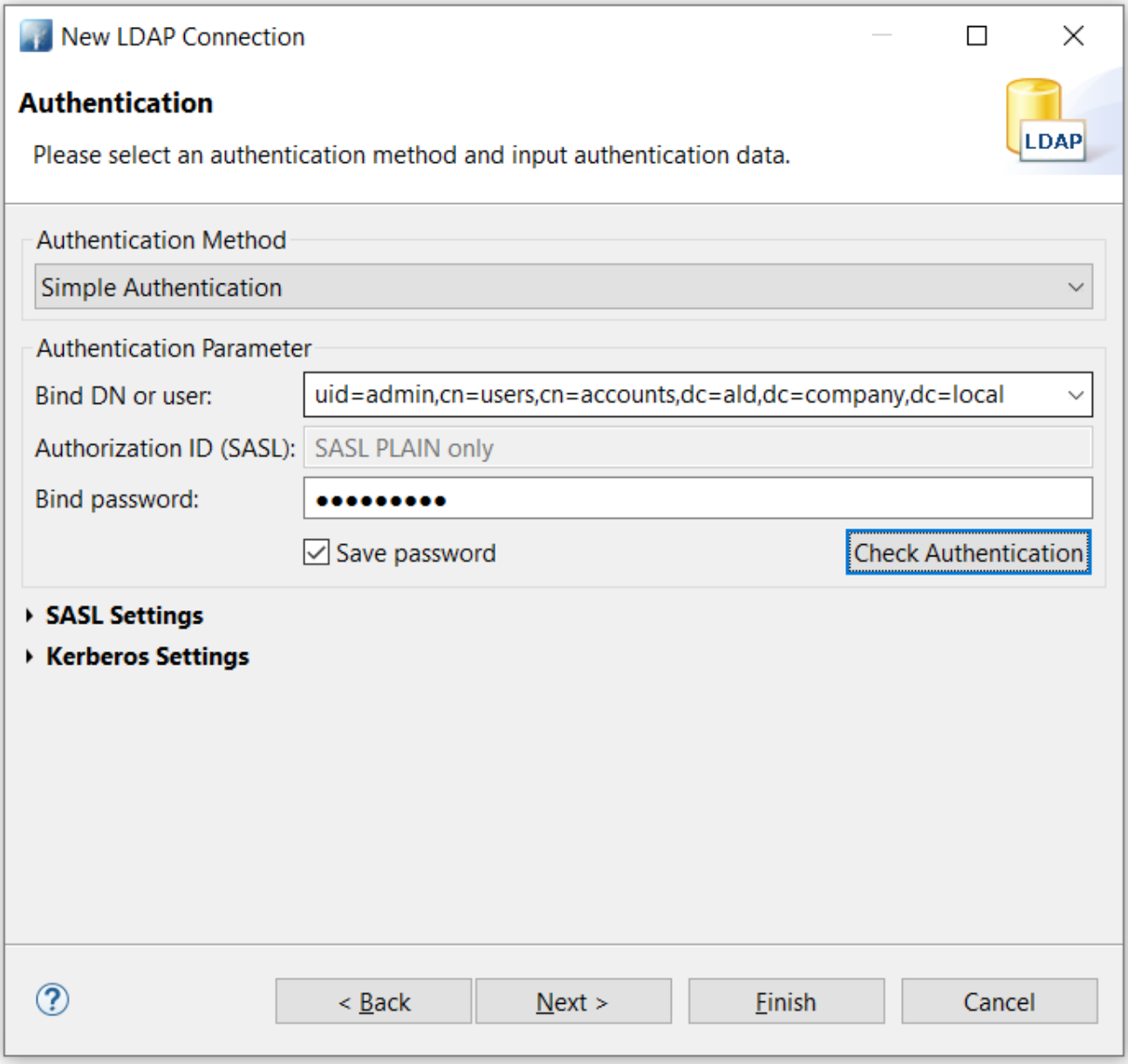


Рисунок 3.28 – Рисунок 6.4.7 Настройка аутентификации для нового LDAP-подключения

После добавления подключения новый сервер появится в списке **Connections**. Для подключения к серверу нужно дважды кликнуть по новой записи.

Просмотр и экспорт объектов каталога

Для просмотра записи в древе каталога следует выбрать нужный **RDN** из окна **LDAP browse**. Например, при нажатии на пункт `cn=accounts` из списка слева, основные атрибуты отобразятся в центральном окне с именем `cn=accounts,dc=ald,dc=company,dc=lan`. См. *Рисунок 6.4.8 Окно LDAP browse*.

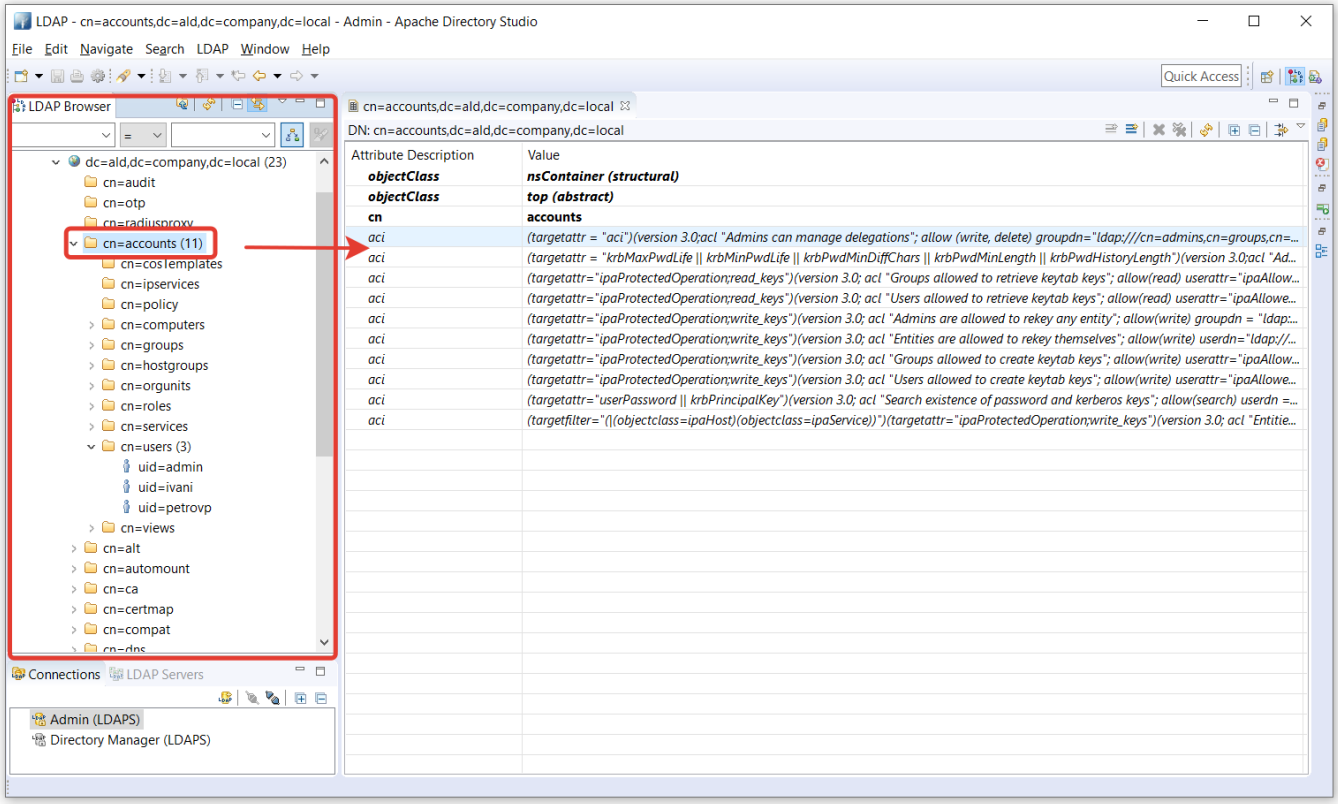


Рисунок 3.29 – Рисунок 6.4.8 Окно LDAP browse

Также можно открыть любой **DN** из меню **Navigate** > **Go to DN**, например `cn=config`, но для его просмотра нужна учетная запись `cn=Directory Manager`, см. Полезные DN.

Запись DN	Описание
cn=accounts,dc=ald,dc=company,dc=lan	Контейнер который содержит дочерние записи контейнеров учетных записей, компьютеров, групп и д.р.
cn=computers,cn=accounts,…	Содержит список компьютеров в домене

продолжение на следующей странице

Таблица 3.3 – продолжение с предыдущей страницы

Запись DN	Описание
cn=dns,…	Содержит информацию о записях DNS
cn=groups,cn=accounts,…	Содержит список групп пользователей
cn=hostgroups, cn=accounts,…	Содержит группы компьютеров домена, например ipaservers
cn=orgunits,cn=accounts,…	Содержит список подразделений, которые отображаются у других записей в атрибуте rbtadp, например у пользователя или компьютера
cn=users,cn=accounts,…	Содержит список пользователей домена

Экспорт объектов производится через контекстное меню, кликом по требуемой записи, например, `cn=users` в дереве см. *Рисунок 6.4.9 Окно LDAP browse*, а затем по **Export** с дальнейшим выбором формата.

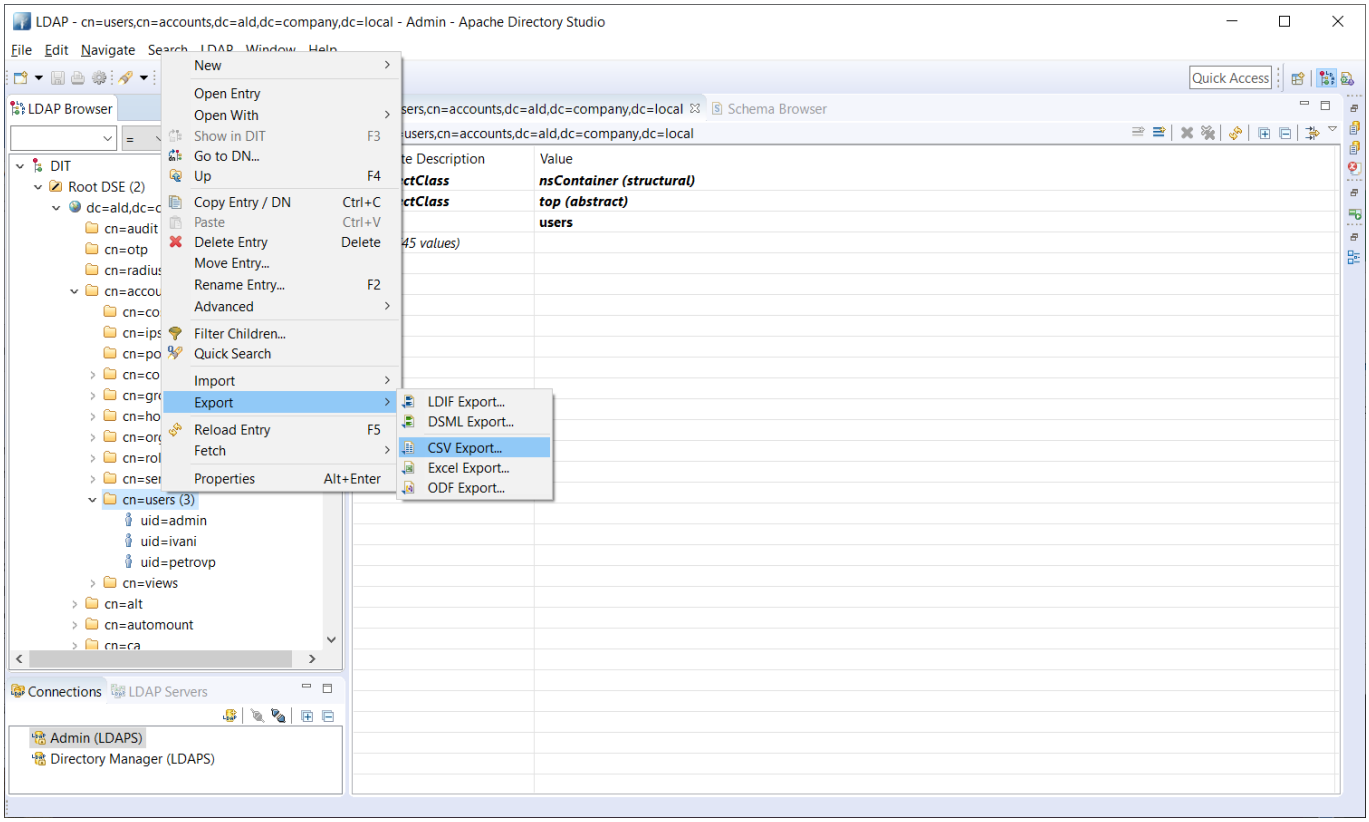


Рисунок 3.30 – Рисунок 6.4.9 Окно LDAP browse

После выбора формата **CSV** откроется диалог настроек параметров экспорта данных, см. *Рисунок 6.4.10 Окно параметров CSV Export*. В окне параметров настройте нужные фильтры и список требуемых атрибутов для вывода.

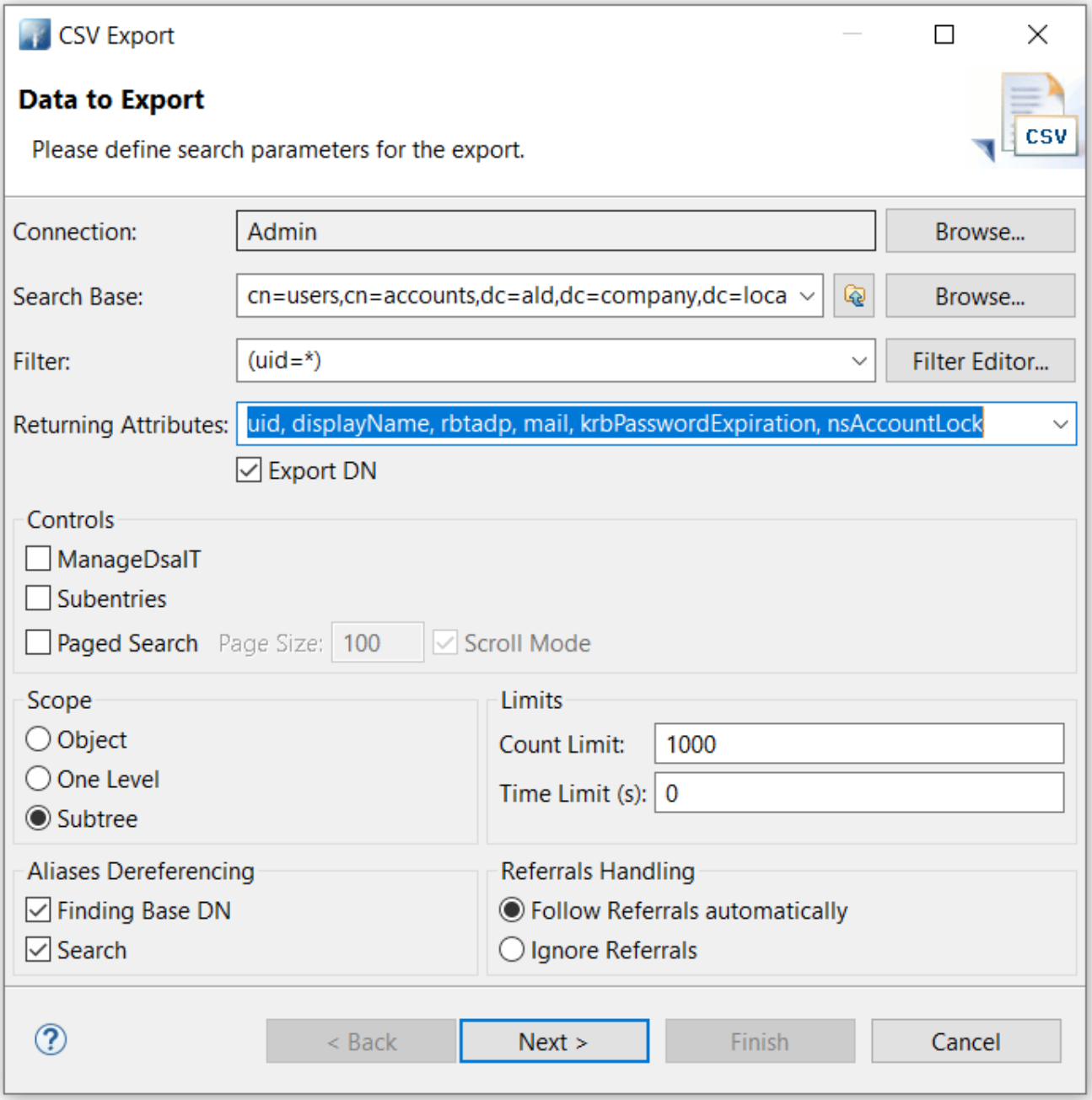


Рисунок 3.31 – Рисунок 6.4.10 Окно параметров CSV Export

Следующим шагом укажите имя файла, в который вы хотите записать **CSV**, см. *Рисунок 6.4.11 Окно CSV Export выбор имени файла*, а затем нажмите **Finish**.

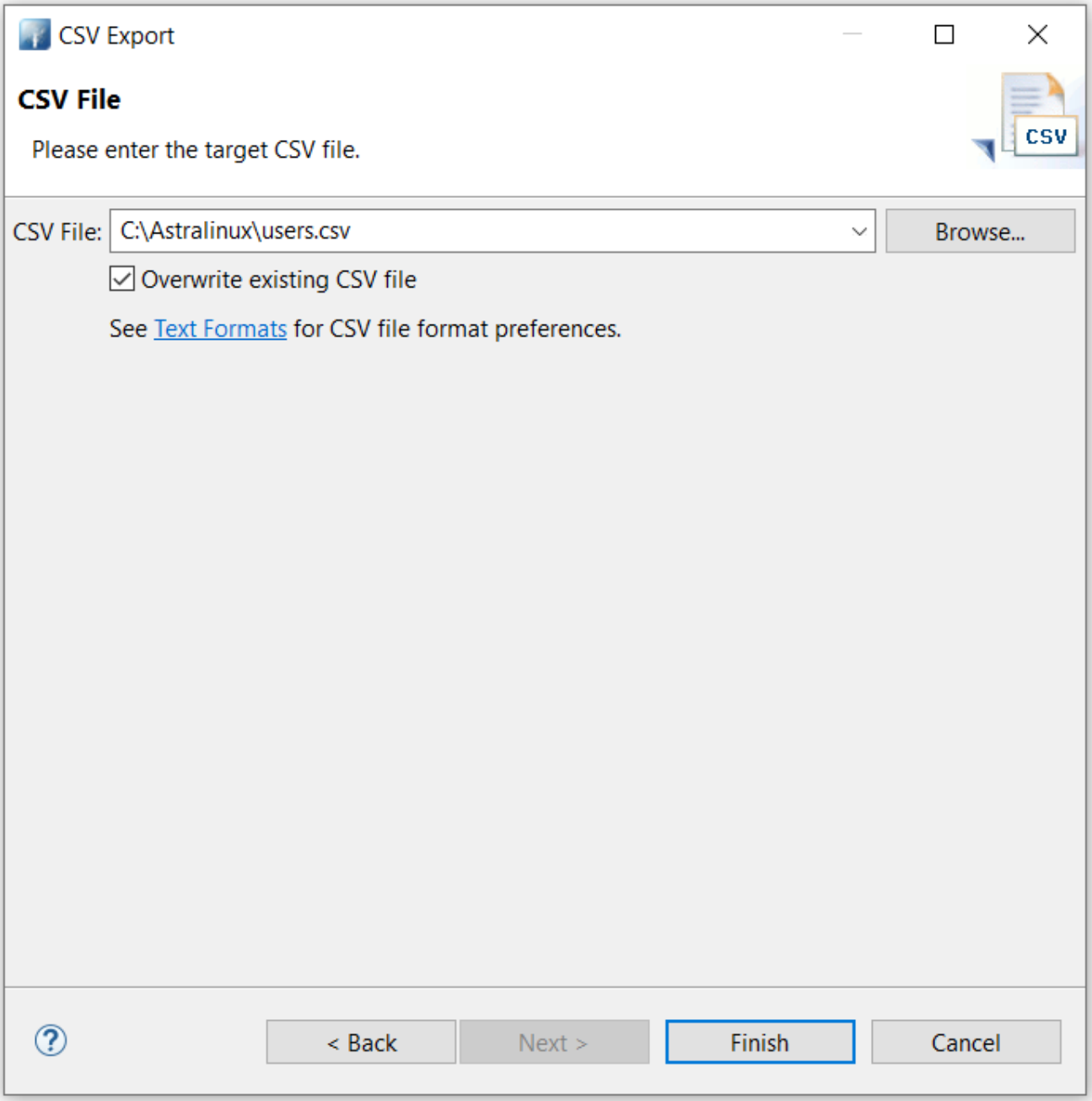


Рисунок 3.32 – Рисунок 6.4.11 Окно CSV Export выбор имени файла

Если нажать на ссылку **Text Formats** см. *Рисунок 6.4.12 Настройки вывода текстового форматирования*, откроются настройки генерации текстовых данных, таких как обрамление данных кавычками, разделитель строк и др.

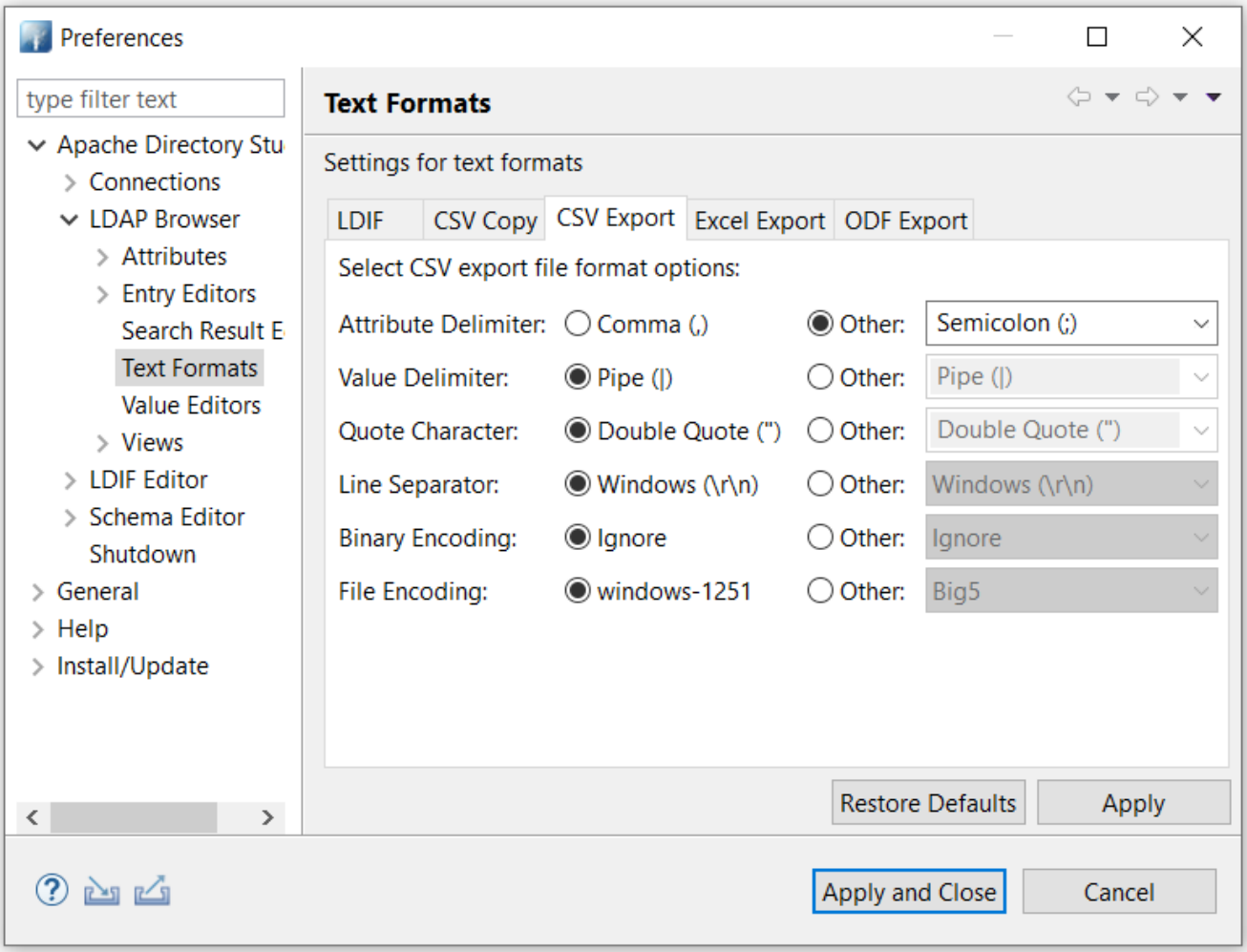


Рисунок 3.33 – Рисунок 6.4.12 Настройки вывода текстового форматирования

Результат выполнения экспорта данных в программе **LibreOffice Calc** - см. *Рисунок 6.4.13 Результат выполнения экспорта данных*.

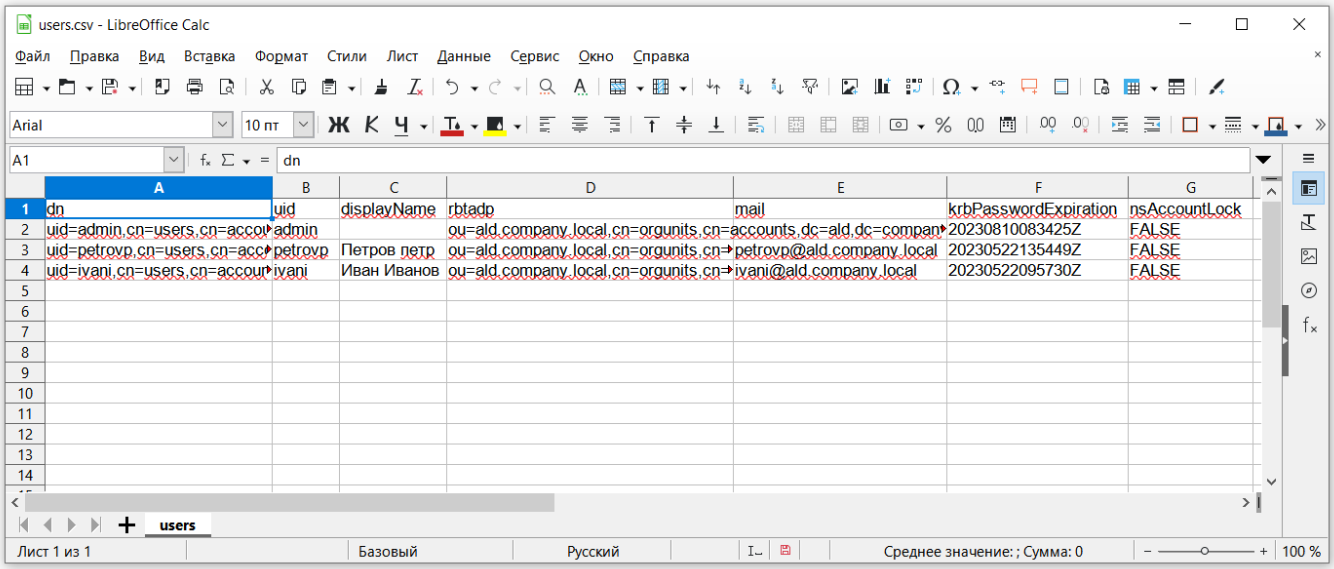


Рисунок 3.34 – Рисунок 6.4.13 Результат выполнения экспорта данных

Этот файл можно использовать для автоматизации в качестве входной информации или для подготовки отчета по объектам из каталога **LDAP**.

Просмотр схемы каталога

Для просмотра схемы каталога следует выбрать **Root DSE** в дереве **LDAP Browser** и выполнить команду **LDAP** > **Open Schema Browser** см. *Рисунок 6.4.14 Меню Open Schema Browser*.

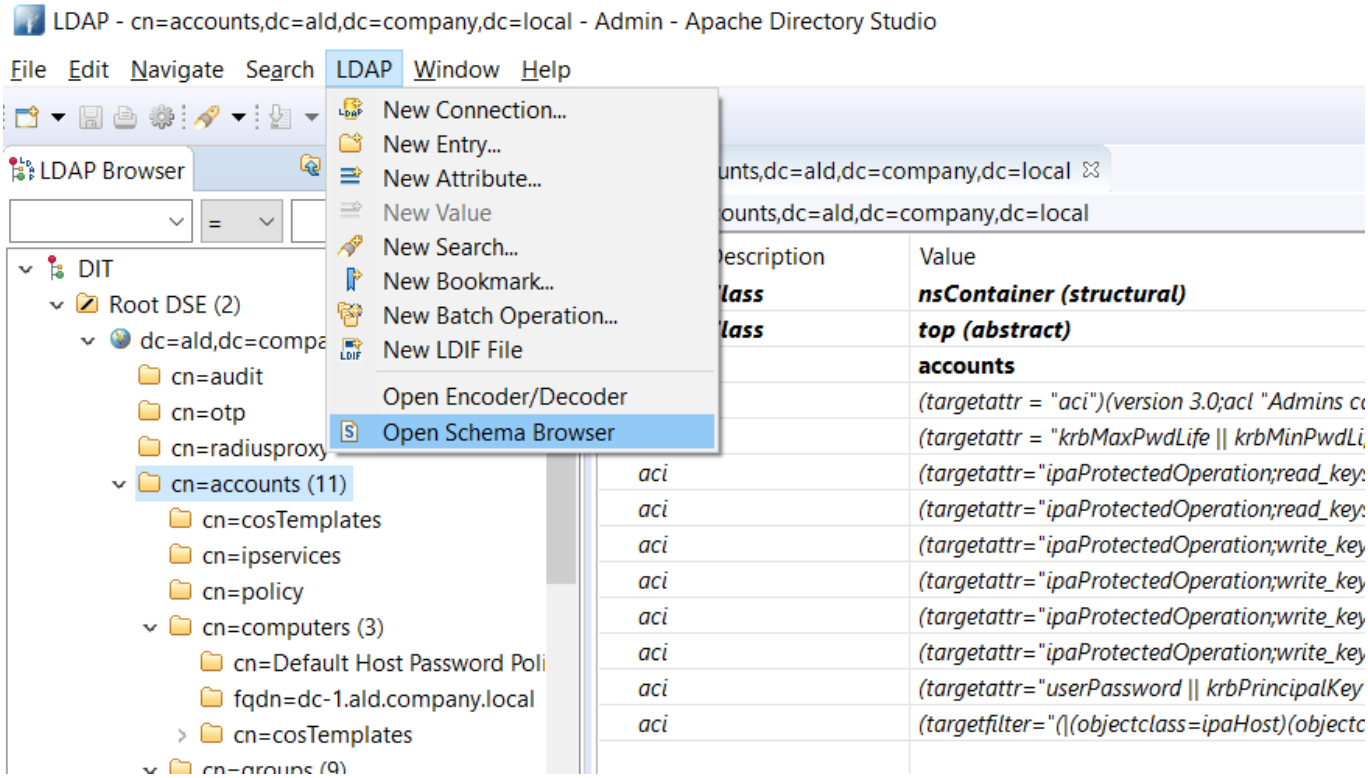


Рисунок 3.35 – Рисунок 6.4.14 Меню Open Schema Browser

По умолчанию в **Schema Browser** открывается страница для просмотра классов объектов `(Object Classes)`, подробной информации `(Details)` и поиска. Например, по фильтру `posix` выводятся упоминаемые ранее классы `posixAcccount` и `posixGroup`, см. *Рисунок 6.4.15 Schema Browser и вкладка Object Classes*.

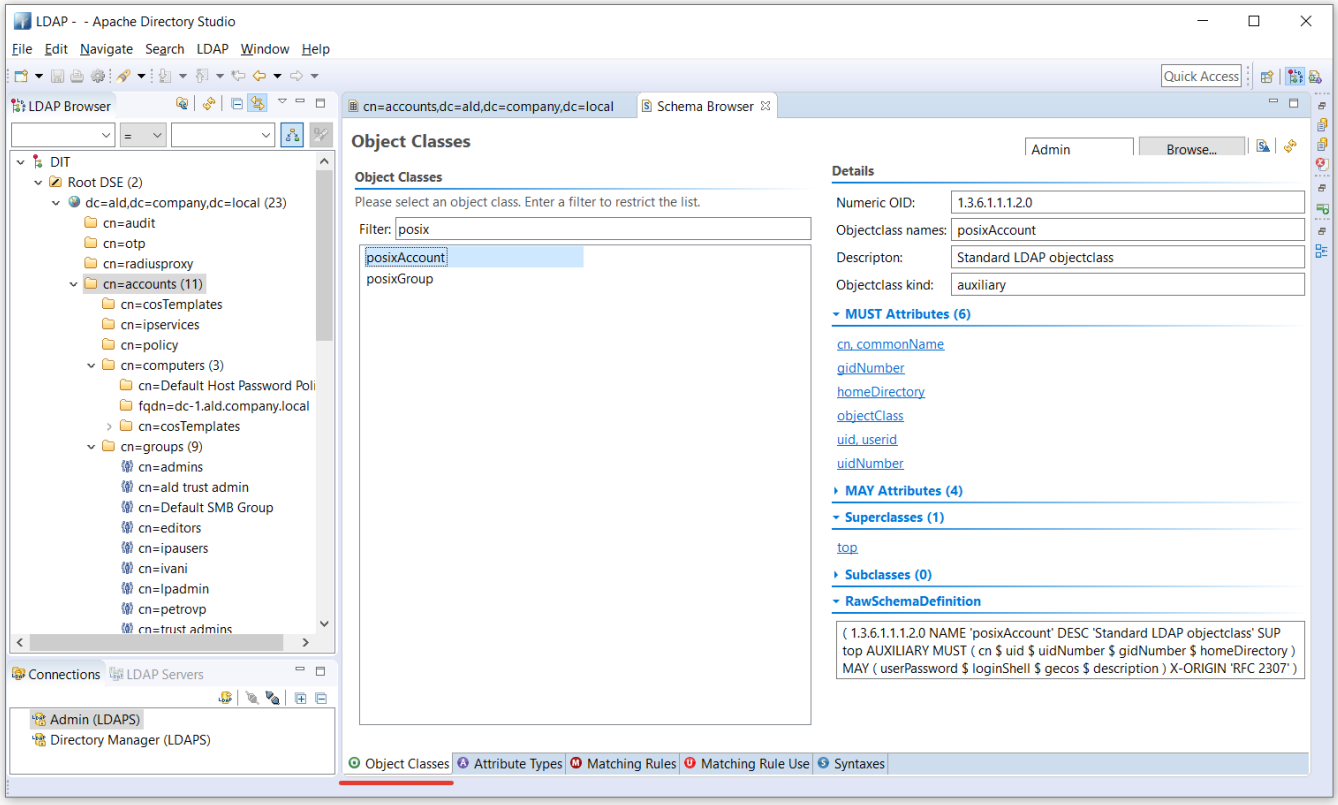


Рисунок 3.36 – Рисунок 6.4.15 Schema Browser и вкладка Object Classes

Для перехода к другим группам объектов предназначены ярлычки в нижней части вкладки. Страница **Attribute Types** предназначена для просмотра атрибутов, поиска по списку всех атрибутов и просмотра деталей выбранного атрибута. Например, поиск по фильтру `gid` выводит несколько атрибутов, в именах которых содержится эта подстрока, см. *Рисунок 6.4.16 Schema Browser и вкладка Attribute Types*.

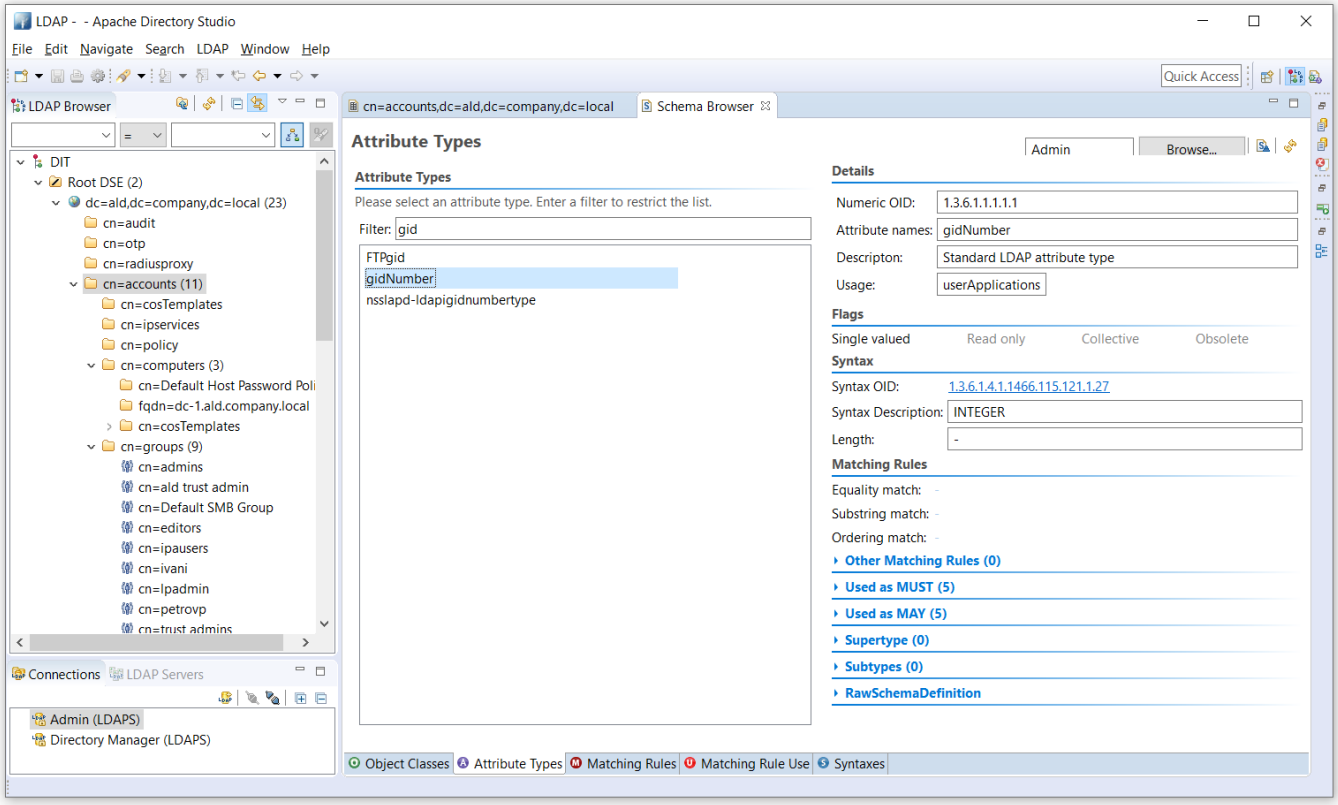


Рисунок 3.37 – Рисунок 6.4.16 Schema Browser и вкладка Attribute Types

3.4.3.2. Утилиты для работы с LDAP-каталогом

Для работы с **LDAP-каталогом** из командной строки используются утилиты пакета `ldap-utils`:

- `ldapwhoami` - выполняет подключение к каталогу и возвращает имя текущего пользователя;
- `ldapsearch` - выполняет поиск по каталогу с указанными параметрами;
- `ldapadd` - позволяет создать новый объект в каталоге;
- `ldapdelete` - позволяет удалить объект из каталога;
- `ldapmodify` - позволяет изменить атрибуты существующего объекта в каталоге;
- `ldapcompare` - позволяет сравнить текущее значение атрибута конкретной записи с желаемым значением и получить результат в формате TRUE/FALSE;
- `ldapexop` - позволяет выполнять расширенные операции, добавленные разработчиками конкретного **LDAP-сервера**. Расширенные операции подобны хранимым процедурам SQL, и позволяют расширять возможности взаимодействия с

сервером без внесения изменений в **LDAP-протокол**;

- `ldappasswd` - позволяет сбросить пароль для учетной записи;
- `ldapmodrdn` - позволяет переименовывать существующие объекты каталога.

Подключение к LDAP

Подключение к **LDAP-каталогу** происходит в рамках вызова каждой утилиты. Допустимо задавать параметры подключения в явном виде или полагаться на настройки по умолчанию, которые описаны в файле */etc/ldap/ldap.conf*. При вводе компьютера в домен указанный файл настраивается автоматически, подключение будет выполняться к одному из контроллеров домена по протоколу **LDAPS** с использованием **Kerberos-билета** из связки ключей.

Проверка доступа в каталог осуществляется командой **ldapwhoami**:

```
ldapwhoami
```

Результат выполнения:

```
SASL/GSSAPI authentication started
ldap_sasl_interactive_bind_s: Local error (-2)
        additional info: SASL(-1): generic failure: GSSAPI Error:
↪Unspecified GSS failure.  Minor code may provide more information (No
↪Kerberos credentials available (default cache: KEYRING:persistent:1000))
```

Данный результат сообщает об отсутствии учетных записей в кэше Kerberos. Поэтому следует выполнить вход `kinit admin` и проверить доступ повторно **ldapwhoami**:

```
kinit admin
ldapwhoami
```

Результат выполнения:

```
Password for admin@ALDPRO.DOMAIN:
SASL/GSSAPI authentication started
SASL username: admin@ALDPRO.DOMAIN
SASL SSF: 256
SASL data security layer installed.
dn: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
```

Наличие TGT-Kerberos билета позволяет получить сервисный билет на доступ к **LDAP-серверу**. Проверить текущие билеты в кэше можно командой `klist`:

```
klist
```

Результат выполнения:

```
Ticket cache: KEYRING:persistent:1000:1000
Default principal: admin@ALD.COMPANY.LAN

Valid starting       Expires              Service principal
22.05.2023 09:58:25  23.05.2023 09:58:01  ldap/dc-1.ald.company.lan@ALD.
 ↪COMPANY.LAN
22.05.2023 09:58:08  23.05.2023 09:58:01  krbtgt/ALD.COMPANY.LAN@ALD.COMPANY.
 ↪LAN
```

В кеше присутствует билет **LDAP**: `ldap/dc-1.ald.company.lan@ALD.COMPANY.LAN`, благодаря этому возможно использование утилиты из пакета `ldap-utils`.

При подключении к серверу можно переопределять любой из параметров по умолчанию, задавая их в явном виде:

```
ldapsearch -H dc-1.ald.company.lan -ZZ -x -W -D "uid=admin,cn=users,
 ↪cn=accounts,dc=ald,dc=company,dc=lan" -b "cn=users,cn=accounts,dc=ald,
 ↪dc=company,dc=lan" '(uid=*)' uid givenName sn
```

где:

- **Параметр** `-H` - для указания адреса **LDAP-сервера**, например `dc-1.ald.company.lan`. Параметр позволяет указать нешифрованный протокол **ldap** или шифрованный **ldaps**, например, `ldap://dc-1.ald.company.lan`. Подключение к **LDAP-каталогу** возможно также через unix-сокет, если приложение выполняется на том же сервере. В этом случае следует указать `ldapi://%2fvar%2frun%2fslapd-ALD-COMPANY-LAN.socket`.
- **Параметр** `-ZZ` - это параметр включения шифрованного соединения, где первая **Z** означает отправку серверу запроса `STARTTLS`. Если сервер не поддерживает TLS, соединение продолжится, и оно не будет шифроваться. Вторая **Z** устанавливает требование использовать только шифрованное соединение, если сервер не поддерживает TLS, соединение прервется. Рекомендуется использовать двойной ключ `-ZZ` для установления шифрованного соединения, если по каким-либо

причинам 636-порт недоступен, а также требование использовать безопасный протокол TLS на 636-порту можно задать с помощью ключа `-H`, указав порт явно `ldaps://dc-1.ald.company.lan`;

- **Параметр** `-x` - указывает на необходимость выполнить простую аутентификацию по логину/паролю;
- **Параметр** `-D` - задает **Bind DN** пользователя для аутентификации, например, `uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan` или супер-пользователя, `cn=Directory Manager`;
- **Параметр** `-W` - указывает, что пароль должен быть предоставлен в интерактивном режиме (а если нужно передать пароль в параметре, то это можно сделать с помощью ключа `-w`);

Используя параметры `-D` и `-W`, доступно подключение к нужному серверу по IP или имени сервера и файл конфигурации задействован не будет.

Поиск по каталогу ldapsearch

Для поиска информации можно использовать утилиту **ldapsearch**, которая извлекает из каталога набор записей с указанными атрибутами в соответствии с заданными критериями фильтрации и заданного списка атрибутов. Синтаксис команды в общем виде выглядит следующим образом:

```
ldapsearch [options] [filter [attributes…]]
```

где:

- `options` - параметры вызова, в т.ч. параметры подключения. Для простоты использованы параметры подключения по умолчанию;
- `filter` - служит для точного указания критериев поиска;
- `attributes` - указывает, какие атрибуты необходимо запросить.

Далее приведен пример запроса, который должен выдавать список всех пользователей домена из `cn=users`, которая в свою очередь является потомком записи `cn=accounts`, и все они находятся в пространстве корневого суффикса `dc=ald,dc=company,dc=lan`. Таким образом полным уникальным именем записи (Distinguished Name, **DN**), в которой хранятся пользователи, является `cn=users,cn=accounts,dc=ald,dc=company,dc=lan`.

Поиск по каталогу с помощью команды **ldapsearch**:

```
ldapsearch -Q -s sub -b "cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
 ↪'(uid=*)' uid givenName sn
```

где:

- Параметр `-Q` – это тихий режим SASL, не выводится информация о SASL-подключении, который полезен при автоматизации для очистки данных от технической информации.
- **Параметр `-s` – это область поиска (scope). Может принимать следующие значения:**
  - `one` - поиск идет по дочерним записям на один уровень ниже в иерархии;
  - `sub` - поиск идет по всем дочерним записям на всю глубину иерархии, параметр по умолчанию;
  - `children` - то же, что и `sub`, но ограничивает поиск только дочерними записями;
  - `base` - ограничивает поиск по текущей записи, заданной параметром `-b`. Если задан `one`, поиск идет по дочерним записям на один уровень ниже в иерархии. Если задан `sub`, то поиск идет по всем дочерним записям на всю глубину иерархии, начиная с записи, заданной параметром `-b`, при этом включая саму базовую запись. `children` - то же, что и `sub`, но ограничивает поиск только дочерними записями, не включая базовую запись.
- Параметр `-b` – это базовая запись (base), которая будет использоваться в качестве начальной точки для поиска по древу.
- Параметр `'(uid=\*)'` – это фильтр, в котором осуществлен поиск всех записей, имеющих атрибут `uid`. Фильтры и составные фильтры рассматриваются далее.
- Параметры `uid givenName sn` – это атрибуты, которые нужно вывести в результат. Если их не указывать, то будут отображены все атрибуты найденных записей.

Результат поиска по каталогу:

```
### extended LDIF
#
### LDAPv3
### base <cn=users,cn=accounts,dc=ald,dc=company,dc=lan> with scope subtree
### filter: (uid=*)
### requesting: uid givenName sn
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
#

### admin, users, accounts, ald.company.lan
dn: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
uid: admin
sn: Administrator

### petrovp, users, accounts, ald.company.lan
dn: uid=petrovp,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
uid: petrovp
givenName:: 0J/RkdGC0YA=
sn:: 0J/QtdGC0YDQvtCy

### ivani, users, accounts, ald.company.lan
dn: uid=ivani,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
uid: ivani
givenName:: 0JjQstCw0L0=
sn:: 0JjQstCw0L3QvtCy

### search result
search: 4
result: 0 Success

### numResponses: 4
### numEntries: 3
```

Результат выводится в поток `stdout` в текстовом формате **LDIF** и его можно использовать по конвейеру `pipeline` или перенаправить в файл для дальнейшей обработки. Подробнее о формате **LDIF** см. в разделе 2.2.3.

Существуют операционные атрибуты (operational attributes), которые встроены в **LDAP-сервер** и управляются им самим, например, `entrydn`, `entryid`, `parentid` или `nsAccountLock`. Большинство операционных атрибутов для пользователей доступны только для чтения. Чтобы их увидеть, необходимо указать “+” в конце команды, однако не все операционные атрибуты доступны для просмотра таким образом:

```
ldapsearch -Q -LLL -s base -b "cn=users,cn=accounts,dc=ald,dc=company,dc=lan
↪" "+"
```

Результат выполнения:

```
dn: cn=users,cn=accounts,dc=ald,dc=company,dc=lan
creatorsName: cn=Directory Manager
modifiersName: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
createTimestamp: 20230324160645Z
modifyTimestamp: 20230324161206Z
nsUniqueId: df91d884-ca5d11ed-b5f0ee72-e6acffe1
parentid: 2
entryid: 3
entryusn: 6055
numSubordinates: 6
```

Например, из результата видно, что запись `cn=users` имеет операционный атрибут `numSubordinates`, который показывает число дочерних записей.

Фильтры запроса

Поиск **ldapsearch** можно сделать более гибким с помощью фильтров, задав условие для отбора нужной информации. Синтаксис фильтра выглядит следующим образом:

```
(attribute operator value)
```

В таблице ниже приведены операторы `(operator)`, используемые в фильтрах:

Оператор	Комментарий
>=	Больше или равно. Возвращает результат, если атрибут больше или равен ка
<=	Меньше или равно. Возвращает результат, если атрибут меньше или равен ка
=*	Наличие. Возвращает результат, если атрибут содержит одно или более значе
=	Равенство. Возвращает результат, если атрибут равен некоторому значению,
~=	Примерное равенство. Возвращает результат, если атрибут содержит приблиз
=string*string	Включает в себя. Возвращает значение, если атрибут содержит определенну

Например, чтобы вывести список пользователей с фамилией `petrov`, потребуется указать фильтр по атрибуту `sn` (surname):

```
ldapsearch -Q -LLL -s one -b "cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
↪"(sn=Петров)" cn
```

Результат выполнения:

```
dn: uid=ppetrov,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
cn: Petr Petrov
```

В результате запрос отфильтрован по атрибуту `sn`. Таким образом можно подготовить любые данные для обработки.

Составные фильтры запроса

Для большей гибкости можно использовать несколько фильтров, объединяя их с помощью логических операторов. Синтаксис составного фильтра выглядит следующим образом:

```
(Boolean-operator(filter)(filter)(filter)...)
```

Ниже приведены логические операторы `(Boolean-operator)`, используемые в составных фильтрах:

- & - Логическое И. Фильтр возвращает те записи, которые удовлетворяют всем указанным условиям, например: `(&(uid=user)(uidNumber=180003))`
- | - Логическое ИЛИ. Фильтр возвращает те записи, которые удовлетворяют одному из указанных условий, например:
- ! - Логическое НЕ. Фильтр возвращает те записи, которые не удовлетворяют указанному условию, например: `(!(uid=admin))`

Например, поиск пользователей из группы `admins`, которые два и более месяца не меняли пароль, выглядит так:

```
ldapsearch -Q -LLL -s one -b "cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
↪"(&(memberof=cn=admins*)(krbLastPwdChange>=$(date +"%Y%m%d000000Z" -d "-60
↪days")))" cn krbLastPwdChange
```

Результат выполнения:

```
dn: uid=admin,cn=users,cn=accounts,
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
cn: Administrator
krbLastPwdChange: 20230324160900Z
```

В результате запроса, выведен список администраторов, у которых пароль изменялся за последние 60 дней. Через конструкцию можно добавлять подкоманды: `$(date +"%Y%m%d000000Z" -d "-60 days")` между двойными кавычками фильтра. Так, например, можно вычислить дату и подставить ее в фильтр в нужном формате.

Получение схемы объектных классов

Объектные классы описаны в операционном атрибуте `objectClasses` из специальной записи схемы `cn=schema`. Посмотреть список всех классов можно командой:

```
ldapsearch -Q -LLL -o ldif-wrap=no -s base -b "cn=schema" objectClasses
```

Результат выполнения:

```
dn: cn=schema
objectClasses: ( 2.5.6.0 NAME 'top' ABSTRACT MUST objectClass X-ORIGIN 'RFC
 ↪45
 12' )
objectClasses: ( 2.5.6.1 NAME 'alias' SUP top STRUCTURAL MUST
 ↪aliasedObjectNam
 e X-ORIGIN 'RFC 4512' )
objectClasses: ( 2.5.20.1 NAME 'subschema' AUXILIARY MAY ( dITStructureRules
 ↪$
  nameForms $ dITContentRules $ objectClasses $ attributeTypes $
 ↪matchingRules
  $ matchingRuleUse ) X-ORIGIN 'RFC 4512' )
objectClasses: ( 1.3.6.1.4.1.1466.101.120.111 NAME 'extensibleObject' SUP top
 AUXILIARY X-ORIGIN 'RFC 4512' )
objectClasses: ( 2.5.6.11 NAME 'applicationProcess' SUP top STRUCTURAL MUST
 ↪cn
  MAY ( seeAlso $ ou $ l $ description ) X-ORIGIN 'RFC 4519' )
...
```

В результате выведется список всех классов, в котором можно искать через команду `grep`:

```
ldapsearch -Q -LLL -o ldif-wrap=no -s base -b "cn=schema" objectClasses |
 ↪grep --color posix
```

Результат выполнения:

```
objectClasses: ( 1.3.6.1.1.1.2.0 NAME 'posixAccount' DESC 'Standard LDAP
 ↪objectclass' SUP top AUXILIARY MUST ( cn $ uid $ uidNumber $ gidNumber $
 ↪homeDirectory ) MAY ( userPassword $ loginShell $ gecos $ description ) X-
 ↪ORIGIN 'RFC 2307' )
objectClasses: ( 1.3.6.1.1.1.2.2 NAME 'posixGroup' DESC 'Standard LDAP
 ↪objectclass' SUP top STRUCTURAL MUST ( cn $ gidNumber ) MAY ( userPassword
 ↪$ memberUid $ description ) X-ORIGIN 'RFC 2307' )
objectClasses: ( 2.16.840.1.113730.3.2.326 NAME 'dynamicGroup' DESC 'Group
 ↪containing internal dynamically-generated members' SUP posixGroup
 ↪AUXILIARY MAY dsOnlyMemberUid X-ORIGIN 'Red Hat Directory Server' )
```

Получение схемы атрибутов

Также, как и объектные классы, атрибуты описаны через операционный атрибут `attributeTypes` корневой записи схемы `cn=schema`. Посмотреть список всех атрибутов можно командой:

```
ldapsearch -Q -LLL -o ldif-wrap=no -s base -b "cn=schema" attributeTypes
```

Результат выполнения:

```
dn: cn=schema
attributeTypes: ( 2.16.840.1.113730.3.1.582 NAME 'nsDS5ReplicaCredentials'
 ↪DES
 C 'Netscape defined attribute type' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
 ↪SINGL
 E-VALUE X-ORIGIN 'Netscape Directory Server' )
attributeTypes: ( 2.16.840.1.113730.3.8.22.1.2 NAME 'ipaCertMapMapRule' DESC
 ↪'
 Certificate Mapping Rule' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE
 ↪X
 -ORIGIN 'IPA v4.5' )
attributeTypes: ( 1.3.6.1.4.1.15953.9.1.1 NAME 'sudoUser' DESC 'User(s) who
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
↪ma
 y  run sudo' EQUALITY caseExactIA5Match SUBSTR caseExactIA5SubstringsMatch
↪SY
 NTAX 1.3.6.1.4.1.1466.115.121.1.26 X-ORIGIN 'SUDO' )
...
```

Результат команды также можно перенаправить в файл командой перенаправления >:

```
ldapsearch -Q -LLL -o ldif-wrap=no -s base -b "cn=schema" attributeTypes >
↪attrs
```

Формат данных LDIF

Как упоминалось ранее, утилита **ldapsearch** возвращает результаты в формате **LDIF**, **LDAP Data Interchange Format** – это формат представления записей службы каталогов или их изменений в текстовой форме. Записи каталога или их изменения представляются набором **LDIF-записей**, по одной на каждую запись каталога или изменение. **LDIF** был разработан в начале 90-х годов и был доработан для использования с **LDAPv3**. Описание формата опубликовано в RFC 4525. Пример структуры **LDIF**:

dn: уникальное имя

имя атрибута: значение атрибута

имя атрибута:: base64 значение атрибута

dn: уникальное имя

имя атрибута: значение атрибута

имя атрибута:< значение атрибута url

Записи каталога представляются группами строк, разделенных пустой строкой, при этом каждая строка в группе представляет отдельное значение атрибута записи. Первая строка в группе должна представлять уникальное имя записи **DN**. Значение атрибута записывается в кодировке ASCII и отделяется от его имени символом :. Значения, не

подходящие под эту кодировку, записываются в кодировке base64 и отделяются от имени атрибута символами `::`. Данный формат можно использовать для хранения данных, добавления и модификации записей в каталоге. Пример **LDIF-файла** добавления записи в каталог нового подразделения `add_dp.ldif`:

```
dn: ou=marketing,ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,dc=company,
 ↪dc=lan
objectClass: rbta-org-unit
objectClass: top
ou: marketing
displayName: Маркетинг
```

Примечание: В конце **LDIF** стоит пустая строка, которая определяет разделение между записями. Даже если запись одна, нужно ставить разделитель из пустой строки.

При модификации используется директива `changetype`, которая может принимать значения: `add`, `modify`, `replace`, `delete` и `moddn`, более подробно рассмотренные далее в примере **ldapmodify**.

Добавление записи в каталог через ldapadd

Добавление в каталог информации возможно утилитами `ldapadd` и `ldapmodify`, где `ldapadd` это символическая ссылка на команду `ldapmodify`, поэтому можно использовать `ldapmodify -a`. Добавьте новое подразделение через описанный выше **LDIF-файл** `add_dp.ldif` командой перенаправления <:

```
Ldapadd -Q < add_dp.ldif
```

Результат выполнения:

```
adding new entry "ou=marketing,cn=orgunits,cn=accounts,dc=ald,dc=company,
 ↪dc=lan"
```

В результате выводится сообщение `adding new entry` и **DN** новой записи.

Второй способ добавления – это работа с утилитой в интерактивном режиме для этого используется команда `ldapadd`:

```
ldapadd -Q
```

Введите текст записи в формате **LDIF**, в конце которого должна быть пустая строка:

```
dn: ou=develop,ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,dc=company,
 ↪dc=lan
objectClass: rbta-org-unit
objectClass: top
ou: develop
displayName: Разработка ПО
```

Мигающий курсор означает ожидание ввода символов или сигналов. Отправьте терминалу сигнал EOF командой `Ctrl+`.

```
Ctrl + <d>
```

Результат выполнения:

```
objectClass: rbta-org-unit
objectClass: top
ou: Develop
displayName: Разработка ПО
adding new entry "ou=Develop,cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan
 ↪"
```

Программа сообщит об успешном добавлении `adding new entry`. Для выхода без изменений отправьте другой сигнал `SIGINT Ctrl +`. Использовать интерактивный режим для скриптов не рекомендуется, потому что может произойти событие ожидания ввода и скрипт зависнет, ожидая ввода пользователя. Поэтому в написании скриптов для команд используют параметр `-y` для подтверждения всех запросов. В примерах далее использован первый подход с перенаправлением.

Модификация записей в каталоге через ldapmodify

Как говорилось ранее, директива `changetype` должна следовать сразу после dn. Это нужно для того, чтобы утилита понимала, какая запись изменяется. Если в **LDIF** отсутствует директива `changetype`, то по умолчанию подразумевается `changetype: add` - добавление записи в каталог.

Директивы changetype: modify и add

Данная директива **LDIF** позволяет добавить атрибут к записи, но есть атрибуты, которые могут быть только в единичном числе, например, атрибут `displayName`. В этом случае при добавлении второго атрибута возникнет ошибка `ldap_add: Already exists (68)`. В примере ниже пользователю `admin` добавляется новая локация - атрибут `L` в файл *add_loc.ldif*:

```
dn: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
changetype: modify
add: l
l: Казань
\n
```

Пустая строка (n) - это разделитель между записями. Ее необходимо добавлять даже при операциях с одной записью. Запуск команды модификации **ldapmodify**:

```
ldapmodify -Q < add_loc.ldif
```

Также ее можно передать по конвейеру:

```
cat add_loc.ldif  | ldapmodify -Q
```

Результат выполнения:

```
modifying entry "uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
```

Директивы changetype: modify и replace

Для перемещения пользователя в другой департамент ему нужно изменить атрибут `rbtadb`. Сначала создается файл, например *changedp.ldif*:

```
dn: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
changetype: modify
replace: rbtadp
rbtadp: ou=marketing,ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,
 ↪dc=company,dc=lan
```

А затем производится запуск команды модификации **ldapmodify**:

```
ldapmodify -Q < changedp.ldif
```

Результат выполнения:

```
modifying entry "uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
```

Успешное изменение записи можно проверить в Apache Directory Studio.

Директивы changetype: modify и delete

Если необходимо изменить несколько атрибутов у записи, то можно несколько операций разделить с новой строки символом `-`. Пример изменений нескольких атрибутов удаляет атрибут `l: Казань` и добавляет `l: Москва`. Сначала создается файл, например *change_two_attrs.ldif*:

```
dn: uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
changetype: modify
delete: l
l: Казань
-
add: l
l: Москва
```

А затем производится запуск команды модификации **ldapmodify**, указав файл:

```
change_two_attrs.ldif через параметр -f:
ldapmodify -Q -f change_two_attrs.ldif
```

Результат выполнения:

```
modifying entry "uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
```

Директивы changetype: modrdn и newrdn

Директива `modrdn` изменяет **RDN** записи, другими словами переименовывает запись. Например, переименуйте подразделение Разработки ПО `ou=develop` на `ou=arch` архитекторов через файл `rename_rdn.ldif`, в котором директива `deleteoldrdn: 1` удалит старый **DN**:

```
dn: ou=develop,ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,dc=company,
 ↪dc=lan
changetype: modrdn
newrdn: ou=arch
deleteoldrdn: 1

dn: ou=arch,ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,dc=company,
 ↪dc=lan
changetype: modify
replace: displayName
displayName: Архитекторы
```

Перенапрвление файла с помощью команды **ldapmodify**:

```
rename_rdn.ldif:
ldapmodify -Q < rename_rdn.ldif
```

Результат выполнения:

```
modifying rdn of entry "ou=develop,ou=ald.company.lan,cn=orgunits,cn=accounts,
 ↪dc=ald,dc=company,dc=lan"

modifying entry "ou=arch,ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,
 ↪dc=company,dc=lan"
```

Важно: При использовании директивы `modrdn` есть угроза возникновения ошибки в виде некорректного количества записей (`total`).

Директива changetype: delete

Если необходимо удалить запись из каталога, используется директива `changetype: delete`, однако, у записи не должно быть ни одной дочерней записи. Например, удаление группы `ou=arch` через файл `del_ou.ldif`:

```
dn: ou=arch,ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,dc=company,
 ↪dc=lan
changetype: delete
```

Проверка результата:

```
ldapmodify -Q < del_ou.ldif
```

Результат выполнения:

```
deleting entry "ou=arch,ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,
 ↪dc=company,dc=lan"
```

Если запись будет не найдена, то выведется сообщение об ошибке:

```
ldap_delete: No such object (32)
        matched DN: ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,
 ↪dc=company,dc=lan
```

Работа с кириллицей и Unicode

Если атрибуты содержат значения не в ASCII-кодировке, то утилита **ldapsearch** при выводе значений представляет их в base64 кодировке. В примере, при создании пользователя `ppetrov` атрибуту `displayName` было присвоено значение `Петров П.П.`:

```
ldapsearch -Q -LLL -s base -b "uid=ppetrov,cn=users,cn=accounts,dc=ald,
 ↪dc=company,dc=lan" displayname
```

Результат выполнения:

```
dn: uid=petrov.pp,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
displayname:: 0J/QtdGC0YDQvtCyINCfLtCfLg==
```

Поскольку **ldapsearch** понимает только ASCII-символы, она представила значение `displayName` в неудобной для чтения base64 строке. Увидеть исходное значение можно только сделав обратное преобразование:

```
echo '0J/QtdGC0YDQvtCyINCfLtCfLg==' | base64 -d
```

Результат выполнения:

```
Петров П.П.
```

Для того, чтобы получить результат сразу в удобном для автоматизации виде, можно

использовать команду:

```
ldapsearch -Q -LLL -s base -b "uid=ppetrov,cn=users,cn=accounts,dc=ald,
 ↪dc=company,dc=lan" displayname  | perl -MMIME::Base64 -Mutf8 -pe 's/^([-a-
 ↪zA-Z0-9;]+):(:\s+)(\S+)$/$1.$2.&decode_ba    se64($3)/e'
```

Результат выполнения:

```
dn: uid=petrov.pp,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
displayName: Петров П.П.
```

Производить какие-то дополнительные действия в фильтрах при поиске по строкам, не содержащим ASCII-символы, не требуется:

```
ldapsearch -Q -LLL -b "cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
 ↪"(displayName=Петров П.П.)" cn
```

Результат выполнения:

```
dn: uid=petrov.pp,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
cn: Petr Petrov
```

3.4.4. Примеры автоматизации

В предыдущих разделах объясняется, как можно управлять каталогом через **LDAP-протокол**, это своего рода «кирпичики», из которых можно «строить дома», т.е. решать сложные задачи автоматизации. Ниже представлены примеры на языках bash и python, а также работа с форматами **CSV**, **LDIF**, **JSON**.

3.4.4.1. Работа с объектами из командной строки bash

В операционных системах Microsoft Windows для решения задач автоматизации раньше использовали командную оболочку и интерпретатор командной строки CMD. На замену ему пришел более мощный объектно-ориентированный PowerShell, который предоставляет удобные инструменты для работы с датами, хэш-таблицами, словарями, **CSV** и **JSON** объектами, а также имеет множество дополнительных модулей, например, для взаимодействия с каталогом **Active Directory**, объектной моделью офисных приложений и пр.

В мире Linux есть множество оболочек и интерпретаторов, например, sh, bash, zsh и др., каждый из которых предлагает свой вариант синтаксиса и может вызывать утилиты, доступные в операционной системе, например, ls, ping, sed, cat, cut и др. Но все они в какой-то степени являются эквивалентом CMD, т.к. работают только с текстовыми переменными и не поддерживают объекты.

Обрабатывать текстовый поток, получаемый от других приложений, средствами командной строки довольно сложно, поэтому bash целесообразно дополнить возможностями языка программирования Python, который в мире Linux можно считать эквивалентом PowerShell, по крайней мере, в части удобства работы с объектами. Далее приведены примеры скриптов Python для конвертации **LDIF** в **JSON** / **CSV**, и способы работы с этими данными с помощью утилит `jq` / `cut`.

Конвертер ldif2csv и генерация отчетов

Обрабатывать **LDIF** довольно сложно, т.к. данные представлены в блоках строк, а нужные атрибуты могут отсутствовать. Вот пример Python скрипта, который позволяет конвертировать поток **LDIF** в **CSV**, для его использования нужно создать файл, например *ldif2csv.py*, и скопировать туда следующее:

```
#!/usr/bin/python3
import sys
import base64
import re

if sys.version_info[0] < 3:
  raise Exception("Use Python 3: python3 ldif2csv.py")

### read from sdtin
data = sys.stdin.readlines()
header_string = ""
atrcheck = ""
entry = ""
dic_entries = {}
dic_entry = {}
current_dn = ""
val_base64 = False
max_size_cell = 32000  ### limit chars in excel cell
### main loop for parse headers and collect dict
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
for line in data:
  ln = line.replace("\n", "").replace("\r", "")
  if len(ln) == 0:
    if not current_dn == "":
      dic_entries[current_dn] = dic_entry
      dic_entry = {}
      entry = ""
  else:
    if ln.startswith("version"):
      #dic_entries["version"] = ln.split(": ")[1]
      continue
    elif ln.lstrip()[0] == "#":
      continue
    elif ln[0] == " ":
      ### if line wrapped line starts with " " then add line to last attr
      dic_entry[atrcheck] += ln.lstrip()
      if val_base64:
        val_to_decode = dic_entry[atrcheck]
        try:
          dic_entry[atrcheck] = base64.b64decode(val_to_decode).decode(
            'utf-8').strip()
        except:
          dic_entry[atrcheck] = val_to_decode
      continue
    entry += ln
    attribute = []
    attribute_name = ""
    attribute_value = ""
    if ln.find(":: ") > 0:
      val_base64 = True
      attribute = ln.split(":: ")
      try:
        attribute_value = base64.b64decode(
          attribute[1]).decode('utf-8').strip()
      except:
        attribute_value = attribute[1]
    elif ln.find(":< ") > 0:
      val_base64 = False
      attribute = ln.split(":< ")
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
      attribute_value = attribute[1]
    else:
      val_base64 = False
      attribute = ln.split(": ")
      try:
        attribute_value = re.sub(r"^.*?: ", "", ln)
      except:
        attribute_value = ""

    atrcheck = attribute[0].replace(":", "")
    ### get attribute and check if attribute exist

    if dic_entry.get(atrcheck):
      new_len = len(dic_entry[atrcheck]) + len("|" + str(attribute_value))
      if new_len < max_size_cell:
        dic_entry[atrcheck] = str(
          dic_entry[atrcheck]) + "|" + str(attribute_value)
    else:
      dic_entry[atrcheck] = attribute_value
    if atrcheck == "dn":
      current_dn = attribute[1]
  if header_string.find(atrcheck) < 0:
    if header_string == "":
      header_string += atrcheck
    else:
      header_string += ";" + atrcheck
### add row if row not empty
if entry != "":
  dic_entries[current_dn] = dic_entry
  dic_entry = {}
  entry = ""

### print utf-8-BOM and headers
print('\ufeff' + "\"" + header_string.replace(";", "\";\"") + "\"")
### print data
for d in dic_entries:
  od = dic_entries[d]
  csv_row = ""  ### row csv value
  split_char = ""  ### spliter for values
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
  for column in header_string.split(";"):
    if len(csv_row) > 0:
      split_char = ";"  ### need split because csv row have chars
    find_column = od.get(column)
    if find_column and find_column.strip():
      csv_row += split_char + "\"" + od[column].replace("\"", "\"\"") + "\""
    else:
      csv_row += split_char + "\"\""
  print(csv_row)
```

Пример конвертации данных из **ldapsearch** через конвейер:

```
ldapsearch -Q -LLL -s one -b "cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
 ↪"(uid=*)" uid displayName sn mail rbtadb | python3 ldif2csv.py
```

Результат выполнения:

```
"dn";"uid";"sn";"displayName";"mail"
"uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan";"admin";
 ↪"Administrator";"";""
"uid=petrovp,cn=users,cn=accounts,dc=ald,dc=company,dc=lan";"petrovp";"Петров
 ↪";"Петров петр";"petrovp@ald.company.lan"
"uid=ivani,cn=users,cn=accounts,dc=ald,dc=company,dc=lan";"ivani";"Иванов";
 ↪"Иван Иванов";"ivani@ald.company.lan"
"uid=petrovss,cn=users,cn=accounts,dc=ald,dc=company,dc=lan";"petrovss";
 ↪"Сидоров";"Петр С.";"petrov.ss@ald.company.lan"
```

Сохранить этот вывод в файл *users.csv* можно простым перенаправлением:

```
ldapsearch -Q -LLL -s one -b "cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
 ↪"(uid=*)" uid displayName sn mail rbtadb | python3 ldif2csv.py > users.csv
```

На *Рисунок 6.4.17 Файл, экспортированный с помощью ldif2csv.py, открытый в LibreOffice Calc* можно увидеть, как будет выглядеть содержимое файла, если его открыть в **LibreOffice Calc**.

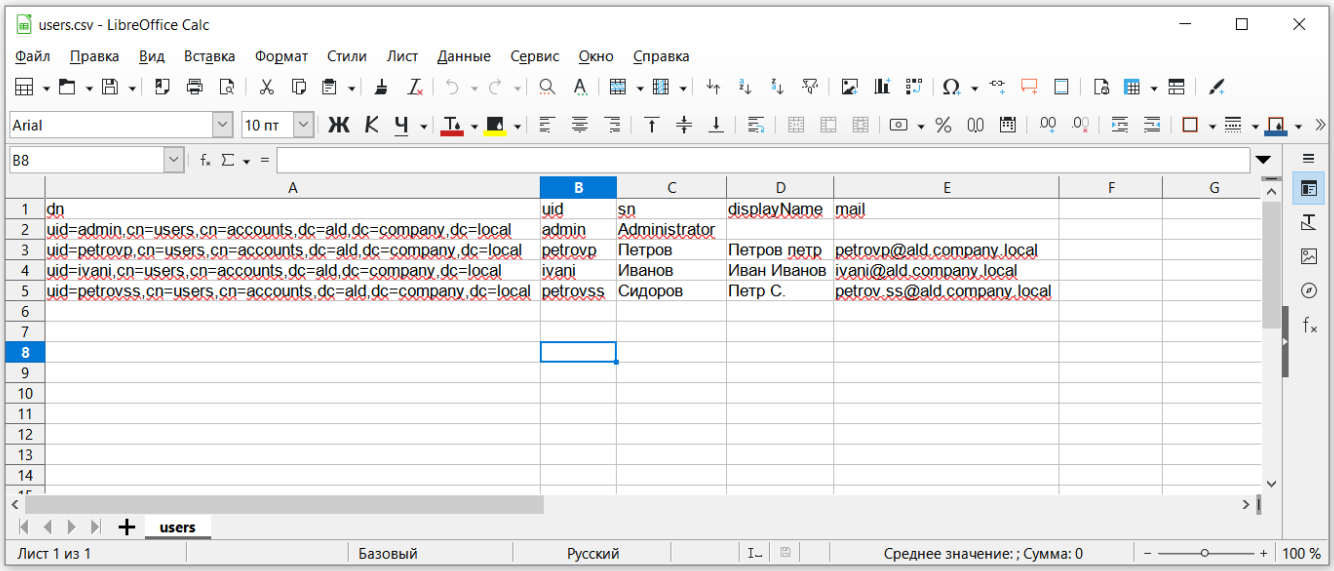


Рисунок 3.38 – Рисунок 6.4.17 Файл, экспортированный с помощью ldif2csv.py, открытый в LibreOffice Calc

Далее можно использовать полученный **CSV-файл** следующим образом:

```
#!/bin/bash
csv_file=$1
cat $csv_file | while read line
do
  if [ ! -z "${line}" ]; then
    if [[ "${line:0:1}" == "\"" ]]; then
     column1=$(echo ${line} | cut -d ";" -f 1 | sed "s/^\"//g" | sed "s/\"$//
↪g")
     column2=$(echo ${line} | cut -d ";" -f 2 | sed "s/^\"//g" | sed "s/\"$//
↪g")
     column3=$(echo ${line} | cut -d ";" -f 3 | sed "s/^\"//g" | sed "s/\"$//
↪g")
     echo -e "$column1\t$column2\t$column3"
     ### можете добавить свои действия по обработке данных из файла
    fi
  fi
done
```

Если сохранить приведенный скрипт в файл `parse_csv.sh`, то ему можно передать имя **CSV-файла** для обработки, как параметр. А также, необходимо назначить скрипту права на выполнение:

```
chmod +x ./parse_csv.sh
./parse_csv.sh users.csv
```

Результат выполнения:

```
uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan       admin  
 ↪Administrator
uid=petrovp,cn=users,cn=accounts,dc=ald,dc=company,dc=lan     petrovp Петров
uid=ivani,cn=users,cn=accounts,dc=ald,dc=company,dc=lan       ivani   Иванов
uid=petrovss,cn=users,cn=accounts,dc=ald,dc=company,dc=lan    petrovss      
 ↪ Сидоров
```

Как мы видно на примере выше, выводится несколько колонок с разделителем табуляции `\t`.

Конвертер ldif2json и работа с JSONPath

Для работы со структурированными данными можно также использовать формат **JSON**, и в Linux есть очень удобный процессор **JSON**, который называется **jq**. Вот пример Python-скрипта, который позволяет конвертировать поток **LDIF** в **JSON**, для его использования нужно создать файл, например *ldif2json.py*, и скопировать туда следующее содержимое:

```
#!/usr/bin/python3
import sys
import base64
import json
import re
### parse bool and int to json
def parce_value(value):
  try:
    return int(value)
  except:
    if value == "FALSE" or value == "FALSE": return bool(value)
    else: return value

if sys.version_info[0] < 3:
  raise Exception("Use Python 3: python3 ldif2json.py")
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
data = sys.stdin.readlines()
header_string = ""
atrcheck = ""
entry = ""
dic_entries = {}
dic_entry = {}
current_dn = ""
val_base64 = False
### main loop for parse headers and collect dict
for line in data:
  ln = line.replace("\n", "").replace("\r", "")
  if len(ln) == 0:
    if not current_dn == "":
      dic_entries[current_dn] = dic_entry
      dic_entry = {}
      entry = ""
  else:
    if ln.startswith("version"):
      dic_entries["version"] = ln.split(": ")[1]
      continue
    elif ln.lstrip()[0] == "#":
      continue

    ### if line wrapped line starts with " " then add line to last attr
    elif ln[0] == " ":
      dic_entry[atrcheck] += ln.lstrip()
      if val_base64:
        val_to_decode = dic_entry[atrcheck]
        try:
          dic_entry[atrcheck] = base64.b64decode(val_to_decode).decode(
            'utf-8').strip()
        except:
          dic_entry[atrcheck] = val_to_decode
      continue
    entry += ln
    attribute = []
    attribute_name = ""
    attribute_value = ""
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
    if ln.find(":: ") > 0:
      val_base64 = True
      attribute = ln.split(":: ")
      try:
        attribute_value = base64.b64decode(
          attribute[1]).decode('utf-8').strip()
      except:
        attribute_value = attribute[1]
    elif ln.find(":< ") > 0:
      val_base64 = False
      attribute = ln.split(":< ")
      attribute_value = attribute[1]
    else:
      val_base64 = False
      attribute = ln.split(": ")
      try:
        attribute_value = re.sub(r"^.*?: ", "", ln)
      except:
        attribute_value = ""
    atrcheck = attribute[0].replace(":", "")
    ### get attribute and check if attribute exist

    if dic_entry.get(atrcheck):
      dic_entry[atrcheck] = str(
        dic_entry[atrcheck]) + "|" + str(attribute_value)
    else:
      dic_entry[atrcheck] = parce_value(attribute_value)
    if atrcheck == "dn":
      current_dn = attribute[1]
  if header_string.find(atrcheck) < 0:
    if header_string == "":
      header_string += atrcheck
    else:
      header_string += ";" + atrcheck
### add row if row not empty
if entry != "":
  dic_entries[current_dn] = dic_entry
  dic_entry = {}
  entry = ""
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
### print stdout json from dict
print(json.dumps(dic_entries, ensure_ascii=False))
```

Пример конвертации данных из **ldapsearch** через конвейер:

```
ldapsearch -Q -LLL -s one -b "cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
↪"(uid=*)" uid displayName sn mail rbtadb | python3 ldif2json.py
```

Результат выполнения:

```
{
  "uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan": {
    "dn": "uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan",
    "uid": "admin",
    "sn": "Administrator"
  },
  "uid=petrovss,cn=users,cn=accounts,dc=ald,dc=company,dc=lan": {
    "dn": "uid=petrovss,cn=users,cn=accounts,dc=ald,dc=company,dc=lan",
    "uid": "petrovss",
    "displayName": "Петр С.",
    "sn": "Сидоров",
    "mail": "petrov.ss@ald.company.lan"
  },
}
```

Сохранить этот вывод в файл *users.json* можно простым перенаправлением и далее с помощью утилиты `jq` из одноименного пакета извлекать любые данные с помощью запросов **JSONPath**. Например, чтобы узнать значение атрибута `mail` для пользователя `petrovss` нужно ввести следующее:

```
ldapsearch -Q -LLL -s one -b "cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
↪"(uid=*)" uid displayName sn mail rbtadb | python3 ldif2json.py > users.
↪json && jq -r '."uid=petrovss,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
↪".mail' users.json
```

где:

- параметр `-r` – означает, что выводить нужно сырые данные без кавычек;
- `".”uid=petrovss,cn=users,cn=accounts,dc=ald,dc=company,dc=lan.`

`mail"` - это текст запроса **JSONPath**.

Результат выполнения:

```
petrov.ss@ald.company.lan
```

Для обработки полученных **JSON** данных в цикле, следует создать файл, например *json_cycle.sh*, со следующим содержимым:

```
#!/bin/bash
echo -e "uid\tdisplayName\tsn\tmail"
ldapsearch -Q -LLL -s one -b "cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
 ↪"(uid=*)" uid displayName sn mail rbtadb | python3 ldif2json.py > users.
 ↪json
cat users.json | jq -r 'delpaths([paths | select(length > 1)])' | jq -r
 ↪'[paths | join(".")]'| jq -r 'join("\n")' | while read key
do
 uid=$(jq -r ".\"$key\".uid" users.json)
 mail=$(jq -r ".\"$key\".mail" users.json)
 displayName=$(jq -r ".\"$key\".displayName" users.json)
 sn=$(jq -r ".\"$key\".sn" users.json)
 echo -e "$uid\t$displayName\t$sn\t$mail"
 ### можете добавить свои действия по обработке данных из файла
done
```

Результат выполнения:

```
uid     displayName     sn      mail
admin   null    Administrator   null
petrovp Петров петр     Петров  petrovp@ald.company.lan
ivani   Иван Иванов     Иванов  ivani@ald.company.lan
petrovss        Петр С. Сидоров petrov.ss@ald.company.lan
```

3.4.4.2. Добавление пользователей

В этом примере при добавлении пользователя `objectClass` класс с именем `ipantuserattrs` не добавляется, чтобы атрибут `ipaNTSecurityIdentifier` сгенерировался автоматически. Содержимое файла *add_user.ldif*:

```
dn: uid=petrovss,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
objectClass: top
objectClass: person
objectClass: organizationalperson
objectClass: inetorgperson
objectClass: inetuser
objectClass: posixaccount
objectClass: krbprincipalaux
objectClass: krbticketpolicyaux
objectClass: ipaobject
objectClass: ipasshuser
objectClass: x-ald-user
objectClass: x-ald-user-parsec14
objectClass: x-ald-audit-policy
objectClass: ruPostMailAccount
objectClass: rbtaCustomUserAttrs
objectClass: rbtaUserMeta
objectClass: rbta-unit
objectClass: rbta-address
objectClass: rbta-inetorgperson-ext
objectClass: ipaSshGroupOfPubKeys
objectClass: mepOriginEntry
givenName: Петр
sn: Сидоров
uid: petrovss
cn: petrov.ss
uidNumber: -1
gidNumber: -1
displayName: Петр С.
initials: P.C.
gecos: Тел. +71234567890
rbtamiddlename: Сидоров
rbtadp: ou=ald.company.lan,cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan
loginShell: /bin/bash
homeDirectory: /home/petrov.ss
mail: petrov.ss@ald.company.lan
x-ald-user-mac: 0:0x0:0:0x0
krbCanonicalName: petrov.ss@ALD.COMPANY.LAN
krbPrincipalName: petrov.ss@ALD.COMPANY.LAN
userPassword: somepassword
```

Примечание: Атрибуты `uidNumber` и `gidNumber` нужно устанавливать равными `-1`, в этом случае DNA-плагин автоматически сгенерирует значения идентификаторов при добавлении пользователя. Пароль следует передавать открытым текстом. Он будет хэширован алгоритмом PBKDF2-SHA256 автоматически. Записать пользователю, сгенерированный где-то в другом месте hash-пароля возможно только при создании пользователя, если сервер переведен в режим миграции.

Далее выполняется команда по добавлению нового пользователя:

```
ldapadd -Q < add_user.ldif
```

Результат выполнения:

```
adding new entry "uid=petrovss,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
```

После входа пользователю нужно будет задать новый пароль, так как пароль назначенный таким способом является временным.

Теперь нужно добавить пользователей в цикле, используя данные из **CSV-файла** - создать файл, например *cycleadd.csv*, с разделителем `;` в любом тектовом редакторе:

```
givenName;sn;uid
Александр;Петров;alexp
Михаил;Иванов;mikhaili
Артём;Сидоров;artems
```

Затем создается скрипт `add_from_csv.sh` по добавлению пользователей из **CSV-файла**:

```
#!/bin/bash
csv_file=$1
delim=$2
function template()
{
   psw=$(cat /dev/urandom| tr -dc '0-9a-zA-Z!@#$%^&*_+-' | head -c 14;echo;)
   uid=$1 #установить uid из первого параметра
   givenName=$2 #установить Имя из второго
   sn=$3 #установить Фамилию из третьего
   suffix=$(ldapsearch -Q -LLL -s base|grep 'dn:'|cut -d ' ' -f2) #получить
↪suffix домена
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
    realm=$(hostname -d|tr '[a-zA-Z]' '[A-Za-z]')
    domain=$(hostname -d)
    cat <<EOF
dn: uid=$uid,cn=users,cn=accounts,$suffix
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalperson
objectClass: inetorgperson
objectClass: inetuser
objectClass: posixaccount
objectClass: krbprincipalaux
objectClass: krbticketpolicyaux
objectClass: ipaobject
objectClass: ipasshuser
objectClass: x-ald-user
objectClass: x-ald-user-parsec14
objectClass: x-ald-audit-policy
objectClass: ruPostMailAccount
objectClass: rbtaCustomUserAttrs
objectClass: rbtaUserMeta
objectClass: rbta-unit
objectClass: rbta-address
objectClass: rbta-inetorgperson-ext
objectClass: ipaSshGroupOfPubKeys
objectClass: mepOriginEntry
givenName: $givenName
sn: $sn
uid: $uid
cn: $uid
uidNumber: -1
gidNumber: -1
displayName: $givenName ${sn:0:1}.
initials: ${givenName:0:1}. ${sn:0:1}.
rbtadp: ou=ald.company.lan,cn=orgunits,cn=accounts,$suffix
loginShell: /bin/bash
homeDirectory: /home/$uid
mail: $uid@$domain
x-ald-user-mac: 0:0x0:0:0x0
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
krbCanonicalName: $uid@$realm
krbPrincipalName: $uid@$realm
userPassword: $psw



EOF
}
echo Добавление пользователей из $csv_file
truncate -s 0 cycleadd.ldif
chmod 500 ./cycleadd.ldif
while read line; do let c++;
   if [ $c -gt 1 ]; then
      p_givenName=$(echo ${line} | cut -d $delim -f 1 | sed "s/^\"//g" | sed
 ↪"s/\"$//g" | sed "s/^\'//g" | sed "s/\'$//g")
      p_sn=$(echo ${line} | cut -d $delim -f 2 | sed "s/^\"//g" | sed "s/\"$//
 ↪g"| sed "s/^\'//g" | sed "s/\'$//g")
      p_uid=$(echo ${line} | cut -d $delim -f 3 | sed "s/^\"//g" | sed "s/\"$/
 ↪/g" | sed "s/^\'//g" | sed "s/\'$//g")
      template $p_uid $p_givenName $p_sn >> cycleadd.ldif
   fi
done < $csv_file
### добавим пользователей одним пакетом
ldapadd -c -f cycleadd.ldif
```

Функцией `template` описан шаблон одной записи. Этот шаблон можно настроить по своему усмотрению, прописав свои корневые суффиксы и реалмы.

Далее следует назначить права запуска скрипту `add_from_csv.sh` и запустить его:

```
chmod +x ./add_from_csv.sh && ./add_from_csv.sh cycleadd.csv ';'
```

Результат выполнения:

```
Добавление пользователей из cycleadd.csv
adding new entry "uid=alexp,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
adding new entry "uid=mikhaili,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
adding new entry "uid=artems,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
```

Скрипт `add_from_csv.sh` создал временный **LDIF-файл** *cycleadd.ldif* и передал команде **ldapadd**. После чего можно создать новый файл *new_users.csv* уже после добавления

пользователей, потому что там уже сохранены новые пароли пользователей:

```
cat cycleadd.ldif | python3 ldif2csv.py > new_users.csv
```

Файл *new_users.csv* можно скачать, для последующей рассылки пользователям паролей и учетных данных для входа, см *Рисунок 6.4.18 Файл с новыми паролями для добавленных в цикле пользователей*.

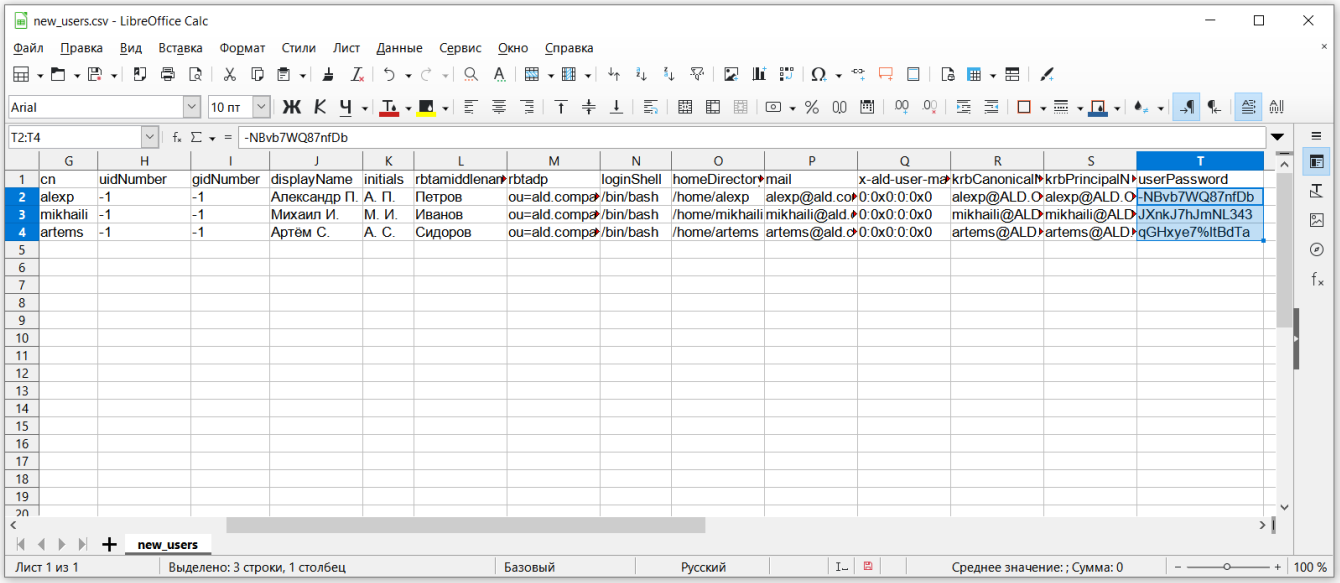


Рисунок 3.39 – Рисунок 6.4.18 Файл с новыми паролями для добавленных в цикле пользователей

3.4.4.3. Смена пароля пользователей

В случае взлома системы необходимо изменить пароли всех пользователей. Для этого создается скрипт на языке bash `change_all_pass.sh`:

```
#!/bin/sh
read -p "Вы хотите создать новые пароли всем пользователям (Yes|no)? " yn
if [[ $yn =~ "Yes" ]]; then
  echo '"dn";"password"' > new_passwords.csv
  echo "" > tmp_new_pass
  ldapsearch -Q -LLL -s one -b "cn=users,cn=accounts,dc=ald,dc=company,dc=lan
↪" "(!(uid=admin))" dn | while read line
  do
  if [ ! -z "${line}" ]; then
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
    psw=$(cat /dev/urandom| tr -dc '0-9a-zA-Z!@#$%^&*_+-' | head -c 14;echo;)
    echo "\"$line\";\"$psw\"" >> new_passwords.csv
    echo -e "${line}\nchangetype: modify\nreplace: userPassword\
↪nuserPassword: $psw\n" >> tmp_new_pass
  fi
  done
  ldapmodify -Q < tmp_new_pass
fi
```

Запуск скрипта:

```
chmod +x change_all_pass.sh && ./change_all_pass.sh
```

Результат выполнения:

```
Вы хотите создать новые пароли всем пользователям (Yes|no)? Yes
modifying entry "uid=petrovp,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
modifying entry "uid=ivani,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
modifying entry "uid=petrovss,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
```

Далее следует подготовить **CSV-файл** *newpass.csv* с паролями из временного *tmp_new_pass* **LDIF** через конвертер `ldif2CSV.py`:

```
cat tmp_new_pass  | python3 ldif2csv.py > newpass.csv
```

Результат выполнения:

```
"dn";"changetype";"replace";"userPassword"
"uid=petrovp,cn=users,cn=accounts,dc=ald,dc=company,dc=lan";"modify";
↪"userPassword";"l@q%yTU1hf_EP7"
"uid=ivani,cn=users,cn=accounts,dc=ald,dc=company,dc=lan";"modify";
↪"userPassword";"nM^ZER_z_sULpE"
"uid=petrovss,cn=users,cn=accounts,dc=ald,dc=company,dc=lan";"modify";
↪"userPassword";"oxK*HzeFmGJw5w"
```

А также можно открыть файл *newpass.csv* в редакторе электронных таблиц, см. *Рисунок 6.4.19 Пакетное изменение паролей пользователей*.

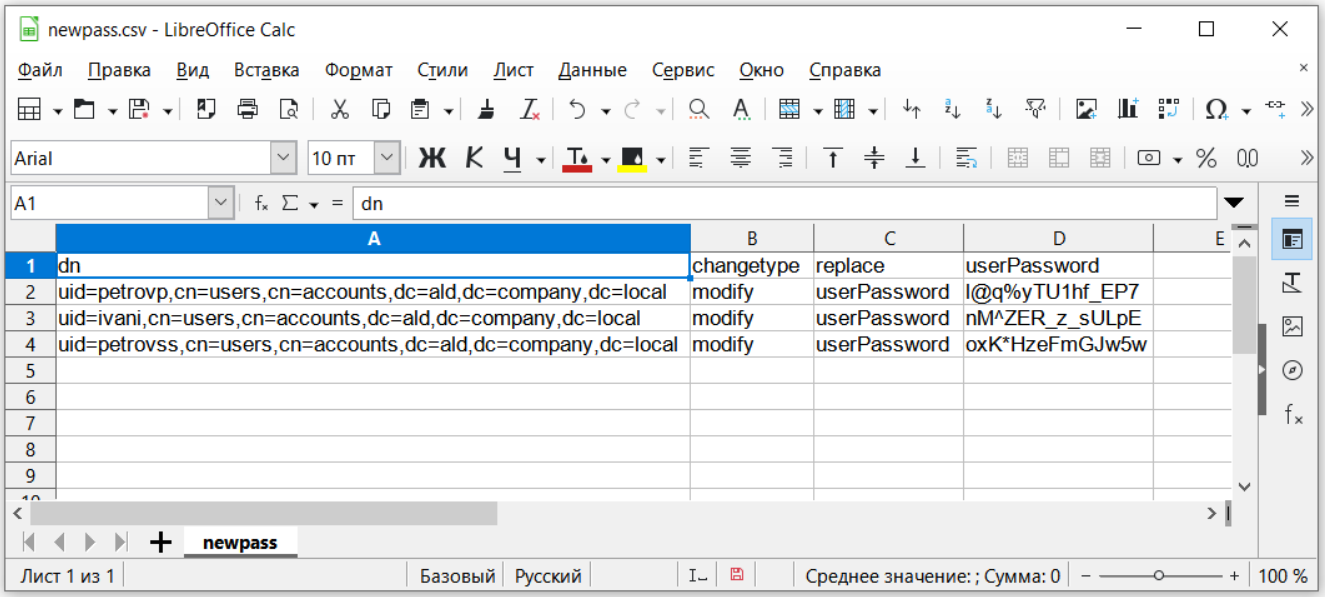


Рисунок 3.40 – Рисунок 6.4.19 Пакетное изменение паролей пользователей

3.4.4.4. Проверка просроченных паролей

Проверка просроченных паролей пользователей с помощью скрипта `check_expired.sh`:

```
#!/bin/bash
### 1. Получить список пользователей из DN cn=users,cn=accounts,dc=ald,
 ↪dc=company,dc=lan
### 2. Отфильтровать список с полями uid, displayname, mail,
 ↪krbPasswordExpiration
### 3. Оставить пользователей, у которых дата просрочки пароля
 ↪(krbPasswordExpiration) от даты сегодня до даты сегодня + 7 дней
ldapsearch -Q -LLL -o ldif-wrap=no -b "cn=users,cn=accounts,dc=ald,dc=company,
 ↪dc=lan" "(&(krbPasswordExpiration>=$(date +"%Y%m%d000000Z
 ↪"))(krbPasswordExpiration<=$(date +"%Y%m%d000000Z" -d "+7 days")))" uid
 ↪displayname mail krbPasswordExpiration > expired_ldif
while read line
do ### 4. Цикл пользователь из пользователей
if [ -z "${line}" ]; then
 if [ ! -z $user_mail ]; then
  ###   4.1 Если почта у пользователя есть
  timeExp=$(date -d "${date_expire:0:4}-${date_expire:4:2}-${date_expire:6:2}
 ↪ ${date_expire:8:2}:${date_expire:10:2}:${date_expire:12:2}Z" +"%s")
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
  timeNow=$(date +"%s")
  seconds=$(( timeExp - timeNow ))
  min=$(( seconds / 60 ))
  hours=$(( min / 60 ))
  days=$(( hours / 24 ))
  ago=$(echo "через $daysдн.")
  if [ $timeNow -gt $timeExp ]; then
   ago="просрочен!!"
  fi
  dateprint=$(date -d "@$timeExp")
  echo "$user_name ($user_mail), пароль просрочится ${dateprint} $ago"
  ### Тут вы можете добавить свою обработку пользователя.
else
  ###   4.3 Иначе добавить пользователя в лог
  echo "$(date) [expire.sh] uid $user_uid mail is epmty" >> "expired.log"
 fi
 ### очистим переменные для следующей записи
 user_uid=""
 user_name=""
 user_mail=""
 date_expire=""
else
  attr=$(echo $line | cut -d ":" -f 1)
  attvalue=$(echo $line | cut -d ":" -f 2)
  if [ -z "$attvalue" ]; then
    attvalue=$(echo $line | cut -d " " -f 2 | base64 -d)
  fi
  ### проверка атрибута и присвоение переменной значения
  case $attr in
    uid) user_uid=$(echo $attvalue | xargs echo -n);;
    displayname) user_name=$(echo $attvalue | xargs echo -n) ;;
    mail) user_mail=$(echo $attvalue | xargs echo -n);;
    krbPasswordExpiration) date_expire=$(echo $attvalue | xargs echo -n);;
  esac
fi
done < expired_ldif
```

Следует указать атрибут выполнения и запустить скрипт:

```
chmod +x ./check_expired.sh && ./check_expired.sh
```

Результат выполнения:

```
Петров петр (petrovp@ald.company.lan), пароль просрочится Вт мая 30 12:18:21
 ↪MSK 2023 через 2дн.
Александр П. (alexp@ald.company.lan), пароль просрочится Сб мая 27 12:46:42
 ↪MSK 2023 просрочен!!
Михаил И. (mikhaili@ald.company.lan), пароль просрочится Сб мая 27 12:46:42
 ↪MSK 2023 просрочен!!
Артём С. (artems@ald.company.lan), пароль просрочится Сб мая 27 12:46:42 MSK
 ↪2023 просрочен!!
```

Скрипт обработал даты просрочки пароля, указав просроченные пароли и дни до их завершения. В данном примере использованы только bash и вывод **ldapsearch**. Также можно добавить в скрипт обработку просроченных учетных записей. Например, отправку сообщения в корпоративный мессенджер или на электронную почту.

3.4.5. Расширение схемы пользовательскими классами и атрибутами

При работе в домене **ALD Pro** появляется потребность в создании пользовательских атрибутов и классов для расширения схемы данных каталога, когда стандартные классы и атрибуты не позволяют описать в полной мере существующие объекты. Далее показано несколько способов реализации этой задачи. Для примеров использованы два контроллера домена: `dc-1.ald.company.lan` и `dc-2.ald.company.lan`.

3.4.5.1. Выбор OID

В каталоге классы и атрибуты имеют свой уникальный номер `OID`. Чтобы получить `OID`, необходимо обратиться к региональным или международным организациям, например, IANA, которые занимаются их регистрацией. На сайте https://oidref.com/org/marina-ignatyeva указаны контакты организации, которая ответственна за регистрацию `OID`, начинающихся с `1.2.643`. Базовый `OID` `1.2.643` специально выделен для России, а `1.2.643.6` для различных организаций внутри страны (https://oidref.com/1.2.643). Если ваша организация уже имеет свой собственный `OID`, то лучше выбрать номера в соответствии с вашими внутренними правилами. Зарегистрированные номера предприятий можно посмотреть:

https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers. При использовании OID, которые еще не зарегистрированы, не рекомендуется публикация новой схемы данных вне своей организации. При назначении OID атрибутам и классам, следует быть внимательным, использование одного и того же номера может привести к проблемам в работе **LDAP-каталога**. Префиксы OID 1.3.6.1.4.1.32702 и 1.3.6.1.4.1.52616 являются зарезервированными и используется для служебных классов и атрибутов **ALD Pro** и **Astra Linux**. Префикс OID 2.16.840.1.113730.3.8 используется для служебных классов и атрибутов **FreeIPA**. Их использование для расширения схемы может привести к сбоям в работе системы и невозможности ее корректного обновления.

В примерах выбран свободный незарегистрированный OID, то есть в данный момент не принадлежащий какой-либо организации. OID состоит чисел, разделенных точками, число цифр не должно превышать 128. Числа в OID могут иметь значения до 2^64-1. Следует сгенерировать три больших числа, для того чтобы уменьшить вероятность их совпадения при выборе OID:

```
dc-1:~$ shuf  -n 3 -i 1000000000-3000000000
2685147094
2741111200
2726881669
```

Первое число соответствует номеру организации, поэтому базовый OID - 1.2.643.6.2685147094. В примере, внутри организации есть несколько подразделений и сервисов, за которые отвечают эти подразделения. Одному из подразделений присвоен номер 2741111200 и номер 2726881669 сервису или приложению, за которое ответственно это подразделение. В итоге OID для подразделения внутри организации будет 1.2.643.6.2685147094.2741111200.2726881669. Атрибутам сервиса соответствует число 1, а классам число 2. Поэтому OID для атрибутов начинается с 1.2.643.6.2732288946.2741111200.2726881669.1, а для классов с 1.2.643.6.2732288946.2741111200.2726881669.2.

В итоге OID - 1.2.643.6.2685147094.2741111200.2726881669.x.y:

- 1.2.643.6 – номер, выделенный для различных организаций в России;
- 2732288946 – номер организации;
- 2741111200 – номер подразделения внутри организации;
- 2726881669 – номер сервиса или приложения;
- x – тип объекта: атрибут или класс;
- y – номер атрибута или класса, каждый атрибут и класс должен иметь свой

уникальный номер.

Возможны другие варианты выбора OID, его составных частей, это зависит от принятой иерархии и правил внутри организации.

3.4.5.2. Создание классов и объектов

В примере требуется создать новый класс и новые атрибуты для хранения информации о рабочем месте пользователя. Рабочее место включает в себя номер кабинета, номер рабочего стола. Новый класс будет называться `workplace` и содержать два атрибута: название кабинета `idCabinet` и номер стола `idTable`. Есть возможность не создавать новый класс, а атрибуты добавить в существующий класс, например, `person`, но так делать не рекомендутся, желательно не менять базовую схему каталога.

Примеры команд были запущены на стенде, состоящем из двух контроллеров домена `dc-1.ald.company.lan` и `dc-2.ald.company.lan`. Команды в примерах могут быть запущены на любом компьютере домена, кроме утилиты **dsconf**, она доступна **только на контроллерах домена** и должна быть запущена под пользователем **root**.

Подготовка **LDIF-файла** для использования с утилитой `ldapmodify` и добавление в него определения класса и атрибутов:

```
dc-1:~$ cat workplace.ldif

dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: ( 1.2.643.6.2732288946.2741111200.2726881669.1.100 NAME
 ↪'idCabinet' DESC 'Cabinet number for employee' SYNTAX 1.3.6.1.4.1.1466.115.
 ↪121.1.15 SINGLE-VALUE X-ORIGIN 'user defined' )
-
add: attributeTypes
attributeTypes: ( 1.2.643.6.2732288946.2741111200.2726881669.1.101 NAME
 ↪'idTable' DESC 'Table number for employee' SYNTAX 1.3.6.1.4.1.1466.115.121.
 ↪1.27 SINGLE-VALUE X-ORIGIN 'user defined' )
-
add: objectClasses
objectClasses: ( 1.2.643.6.2732288946.2741111200.2726881669.2.50 NAME
 ↪'workplace' DESC 'Workplace for employee' SUP top AUXILIARY MAY (
 ↪idCabinet $ idTable ) X-ORIGIN 'user defined' )
```

В файле:

- OID атрибута idCabinet равен 1.2.643.6.2732288946.2741111200.2726881669.1.100, в нем будет содержаться строковый тип данных, которому соответствует OID 1.3.6.1.4.1.1466.115.121.1.15. Например, “Приемная” или “Отдел статистики”.
- OID атрибута idTable равен 1.2.643.6.2732288946.2741111200.2726881669.1.101, он будет содержать числовой тип данных, которому соответствует OID 1.3.6.1.4.1.1466.115.121.1.27.
- OID класса workplace равен 1.2.643.6.2732288946.2741111200.2726881669.2.50, он имеет родительский класс top. Класс содержит необязательные атрибуты idCabinet, idTable, если они должны быть обязательными, необходимо поменять MAY на MUST.

Теперь следует добавить новые данные схемы в каталог:

```
dc-1:~$ ldapmodify -D "cn=Directory Manager" -W -f workplace.ldif
Enter LDAP Password:

modifying entry "cn=schema"
```

В cn=schema должны появиться новые данные:

```
dc-1:~# dsconf -D "cn=Directory Manager" - W ldap://localhost schema
 ↪objectclasses query workplace
Enter password for cn=Directory Manager on ldap://localhost:

( 1.2.643.6.2732288946.2741111200.2726881669.2.50 NAME 'workplace' DESC
 ↪'Workplace for employee' SUP top AUXILIARY MUST ( idCabinet $ idTable ) X-
 ↪ORIGIN 'user defined' )
dc-1:~#
dc-1:~# dsconf -D "cn=Directory Manager" - W ldap://localhost schema
 ↪attributetypes query idCabinet
Enter password for cn=Directory Manager on ldap://localhost:

( 1.2.643.6.2732288946.2741111200.2726881669.1.100 NAME 'idCabinet' DESC
 ↪'Cabinet number for employee' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-
 ↪VALUE X-ORIGIN 'user defined' )
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
MUST

MAY
( 1.2.643.6.2732288946.2741111200.2726881669.2.50 NAME 'workplace' DESC
 ↪'Workplace for employee' SUP top AUXILIARY MUST ( idCabinet $ idTable ) X-
 ↪ORIGIN 'user defined' )
dc-1:~#
dc-1:~# dsconf -D "cn=Directory Manager" - W ldap://localhost schema
 ↪attributetypes query idTable
Enter password for cn=Directory Manager on ldap://localhost:

( 1.2.643.6.2732288946.2741111200.2726881669.1.101 NAME 'idTable' DESC
 ↪'Table number for employee' SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-
 ↪VALUE X-ORIGIN 'user defined' )

MUST

MAY
( 1.2.643.6.2732288946.2741111200.2726881669.2.50 NAME 'workplace' DESC
 ↪'Workplace for employee' SUP top AUXILIARY MUST ( idCabinet $ idTable ) X-
 ↪ORIGIN 'user defined' )
```

Текущая схема данных пока не обновлена, если была допущена какая-то неточность, надо удалить созданные классы и атрибуты, а затем снова создать их. Удаление будет рассмотрено в следующем разделе. Если все нормально и нет ошибок, для обновления схемы необходимо выполнить следующую команду и проверить результат:

```
dc-1:~# dsconf -D "cn=Directory Manager" -W ldap://localhost schema reload
Enter password for cn=Directory Manager on ldap://localhost:

Attempting to add task entry... This will fail if Schema Reload plug-in is
 ↪not enabled.
Successfully added task entry cn=schema_reload_2023-11-21T16:53:52.560422,
 ↪cn=schema reload task,cn=tasks,cn=config
To verify that the schema reload operation was successful, please check the
 ↪error logs.
```

Если добавление прошло успешно, в лог файле */var/log/dirsrv/slapd-ALD-COMPANY-LAN/errors* должны быть следующие строки:

```
dc-1:~$ vi /var/log/dirsrv/slapd-ALD-COMPANY-LAN/errors
...
[23/Nov/2023:07:21:37.108569846 +0300] - INFO - schemareload - schemareload_
 ↪thread - Schema reload task starts (schema dir: default) ...
[23/Nov/2023:07:21:37.249203959 +0300] - INFO - schemareload - schemareload_
 ↪thread - Schema validation passed.
[23/Nov/2023:07:21:37.370369733 +0300] - INFO - schemareload - schemareload_
 ↪thread - Schema reload task finished.
...
```

Обновленная схема данных реплицируется на другие контроллеры домена не сразу, а только в том случае, если в каталоге произойдут какие-либо изменения, например, изменения какого-либо объекта каталога.

Создание нового класса к записи пользователя в каталоге для проверки, что схема данных реплицировалась на другой контроллер домена:

```
dc-1:~$ ldapmodify -D "cn=Directory Manager" -W
Enter LDAP Password:

dn: uid=user0,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
changetype: modify
add: objectClass
objectClass: workplace

modifying entry "uid=user0,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
```

Если теперь проверить на втором контроллере домена, то новый класс и новые атрибуты отобразятся в его каталоге:

```
dc-2:~# dsconf -D "cn=Directory Manager" - W ldap://localhost schema
 ↪objectclasses query workplace
Enter password for cn=Directory Manager on ldap://localhost:

( 1.2.643.6.2732288946.2741111200.2726881669.2.50 NAME 'workplace' DESC
 ↪'Workplace for employee' SUP top AUXILIARY MUST ( idCabinet $ idTable ) X-
 ↪ORIGIN 'user defined' )
dc-2:~#
dc-2:~# dsconf -D "cn=Directory Manager" - W ldap://localhost schema
 ↪attributetypes query idCabinet
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
Enter password for cn=Directory Manager on ldap://localhost:

( 1.2.643.6.2732288946.2741111200.2726881669.1.100 NAME 'idCabinet' DESC
 ↪'Cabinet number for employee' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-
 ↪VALUE X-ORIGIN 'user defined' )

MUST

MAY
( 1.2.643.6.2732288946.2741111200.2726881669.2.50 NAME 'workplace' DESC
 ↪'Workplace for employee' SUP top AUXILIARY MUST ( idCabinet $ idTable ) X-
 ↪ORIGIN 'user defined' )
dc-2:~#
dc-2:~# dsconf -D "cn=Directory Manager" - W ldap://localhost schema
 ↪attributetypes query idTable
Enter password for cn=Directory Manager on ldap://localhost:

( 1.2.643.6.2732288946.2741111200.2726881669.1.101 NAME 'idTable' DESC
 ↪'Table number for employee' SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-
 ↪VALUE X-ORIGIN 'user defined' )

MUST

MAY
( 1.2.643.6.2732288946.2741111200.2726881669.2.50 NAME 'workplace' DESC
 ↪'Workplace for employee' SUP top AUXILIARY MUST ( idCabinet $ idTable ) X-
 ↪ORIGIN 'user defined' )
```

Если после добавления классов и атрибутов изменения не были применены, то есть не была выполнена команда `reload`, для удаления достаточно запустить команды `dcsonf` или `ldapmodify`. Если же была применена команда `reload` и произошла репликация схемы на другие контроллеры, то перед удалением на каждом контроллере домена необходимо отключить репликацию схемы. Иначе новая схема снова появится на контроллере, на котором она была удалена, из-за репликации с другими контроллерами, так как они будут включать в себя более полный набор атрибутов и классов, включая новые данные. Когда один контроллер содержит схему с большим набором, чем второй, он реплицирует свой набор на первый. Сначала надо отключить репликацию схемы на каждом контроллере. В данном примере на двух.

На первом контроллере:

```
dc-1:~# dsconf -D "cn=Directory Manager" -W ALD-COMPANY-LAN config replace
 ↪nsslapd-schemareplace=off
Enter password for cn=Directory Manager on ALD-COMPANY-LAN:
Successfully replaced "nsslapd-schemareplace"
```

На втором контроллере:

```
dc-2:~# dsconf -D "cn=Directory Manager" -W ALD-COMPANY-LAN config replace
 ↪nsslapd-schemareplace=off
Enter password for cn=Directory Manager on ALD-COMPANY-LAN:
Successfully replaced "nsslapd-schemareplace"
```

После этого можно удалить новую схему с помощью утилиты `dsconf` или `ldapmodify`, не опасаясь снова ее появления из-за репликации. Для удаления созданных атрибутов и классов команды запускаются на каждом контроллере:

```
dc-n:~# dsconf -D "cn=Directory Manager" -W ldap://localhost schema
 ↪objectclasses remove workplace
Enter password for cn=Directory Manager on ldap://localhost:

Successfully removed the objectClass
dc-n:~#
dc-n:~# dsconf -D "cn=Directory Manager" -W ldap://localhost schema
 ↪attributetypes remove idCabinet
Enter password for cn=Directory Manager on ldap://localhost:

Successfully removed the attributetype
dc-n:~$
dc-n:~$ dsconf -D "cn=Directory Manager" -W ldap://localhost schema
 ↪attributetypes remove idTable
Enter password for cn=Directory Manager on ldap://localhost:

Successfully removed the attributetype
```

Или удаление с помощью **ldapmodify**:

```
dc-n:~# cat workplace_delete.ldif

dn: cn=schema
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
changetype: modify
delete: objectClasses
objectClasses: ( 1.2.643.6.2732288946.2741111200.2726881669.2.50 NAME
 ↪'workplace' DESC 'Workplace for employee' SUP top AUXILIARY MAY (
 ↪idCabinet $ idTable ) X-ORIGIN 'user defined' )
-
delete: attributeTypes
attributeTypes: ( 1.2.643.6.2732288946.2741111200.2726881669.1.100 NAME
 ↪'idCabinet' DESC 'Cabinet number for employee' SYNTAX 1.3.6.1.4.1.1466.115.
 ↪121.1.15 SINGLE-VALUE X-ORIGIN 'user defined' )
-
delete: attributeTypes
attributeTypes: ( 1.2.643.6.2732288946.2741111200.2726881669.1.101 NAME
 ↪'idTable' DESC 'Table number for employee' SYNTAX 1.3.6.1.4.1.1466.115.121.
 ↪1.27 SINGLE-VALUE X-ORIGIN 'user defined' )
dc-n:~#
dc-n:~# ldapmodify -v -D "cn=Directory Manager" -W -f workplace_delete.ldif
ldap_initialize( <DEFAULT> )
delete objectClasses:
     ( 1.2.643.6.2732288946.2741111200.2726881669.2.50 NAME 'workplace' DESC
 ↪'Workplace for employee' SUP top AUXILIARY MAY ( idCabinet $ idTable ) X-
 ↪ORIGIN 'user defined' )
delete attributeTypes:
     ( 1.2.643.6.2732288946.2741111200.2726881669.1.100 NAME 'idCabinet'
 ↪DESC 'Cabinet number for employee' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 ↪SINGLE-VALUE X-ORIGIN 'user defined' )
delete attributeTypes:
     ( 1.2.643.6.2732288946.2741111200.2726881669.1.101 NAME 'idTable' DESC
 ↪'Table number for employee' SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-
 ↪VALUE X-ORIGIN 'user defined' )
modifying entry "cn=schema"
modify complete
```

После удаления обязательно выполнить `reload` на каждом контроллере:

```
dc-n:~# dsconf -D "cn=Directory Manager" -W ldap://localhost schema reload
Enter password for cn=Directory Manager on ldap://localhost:

Attempting to add task entry... This will fail if Schema Reload plug-in is
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
 ↪not enabled.
Successfully added task entry cn=schema_reload_2023-11-21T16:53:52.560422,
 ↪cn=schema reload task,cn=tasks,cn=config
To verify that the schema reload operation was successful, please check the
 ↪error logs.
dc-n:~#
dc-n:~# dsconf -D "cn=Directory Manager" -W ldap://localhost schema
 ↪objectclasses query workplace
Enter password for cn=Directory Manager on ldap://localhost:
None
```

Необходимо убедиться, что в лог-файле *error* нет ошибок:

```
dc-1:~# tail /var/log/dirsrv/slapd-ALD-COMPANY-LAN/errors
...
[27/Nov/2023:07:04:59.065768985 +0300] - INFO - schemareload - schemareload_
 ↪thread - Schema reload task starts (schema dir: default) ...
[27/Nov/2023:07:04:59.192963349 +0300] - INFO - schemareload - schemareload_
 ↪thread - Schema validation passed.
[27/Nov/2023:07:04:59.314138040 +0300] - INFO - schemareload - schemareload_
 ↪thread - Schema reload task finished.
```

После этого включить репликацию обратно на каждом контроллере:

```
dc-n:~# dsconf -D "cn=Directory Manager" -W ALD-COMPANY-LAN config replace
 ↪nsslapd-schemareplace=replication-only
Enter password for cn=Directory Manager on ALD-COMPANY-LAN:

Successfully replaced "nsslapd-schemareplace"
```

Создание пользовательского класса и атрибутов в отдельном файле схемы и интеграция в директорию */etc/dirsrv/slapd-instance_name/schema/*. В данном примере это */etc/dirsrv/slapd-ALD-COMPANY-LAN/schema/*. Имя файла и его содержимое должно удовлетворять нескольким критериям:

- в самом начале файла должна быть строка dn: `cn=schema`;
- название файла должно быть в формате `[1-9][0-9]text.ldif` и всегда начинаться с двух цифр;
- важно, чтобы число в имени файла было меньше или равно числу в имени

99user.ldif;

- в случае, если число в имени равно 99, то в отсортированном алфавитном порядке `text` должен быть ниже, чем имя `user` в имени файла `99user.ldif`. Например, имя `99z.ldif` будет неверным, а `99a.ldif` верным, так как буква “a” расположена в алфавите раньше буквы “u”;
- в файле атрибуты и классы могут быть определены одновременно или по отдельности, причем сначала должны идти описания атрибутов, а затем классов;
- в файле могут быть использованы уже существующие атрибуты, описанные в других классах.

LDAP-сервер будет читать файлы в директории */etc/dirsrv/slapd-ALD-COMPANY-LAN/schema/* по порядку, начиная с файлов с именами, содержащими меньшие числа и заканчивая файлом с именем `99user.ldif`. Если числа одинаковы, то в алфавитном порядке. Сервер ожидает, что самым последним прочитанным файлом будет *99user.ldif*. Когда добавляются новые элементы схемы, сервер записывает добавленные пользователем атрибуты и классы в файл, имя которого в директории */etc/dirsrv/slapd-ALD-COMPANY-LAN/schema/* стоит последним после сортировки. Если имя последнего файла не совпадает с `99user.ldif`, в работе каталога могут быть проблемы. Файл *99user.ldif** является служебным и всегда должен читаться сервером последним, напрямую в него не рекомендуется добавлять новую схему. Если в файлах встречаются определения одинаковых атрибутов и классов, определения загруженные позже перезаписывают предыдущие.

Нужно создать файл *99a.ldif* и добавить в него определения класса `workplace` и атрибутов `idCabinet`, `idTable`.

```
dc-1:~# cat /etc/dirsrv/slapd-ALD-COMPANY-LAN/schema/99a.ldif

dn: cn=schema
attributeTypes: ( 1.2.643.6.2732288946.2741111200.2726881669.1.100 NAME
 ↪'idCabinet' DESC 'Cabinet number for employee' SYNTAX 1.3.6.1.4.1.1466.115.
 ↪121.1.15 SINGLE-VALUE X-ORIGIN 'user defined' )
attributeTypes: ( 1.2.643.6.2732288946.2741111200.2726881669.1.101 NAME
 ↪'idTable' DESC 'Table number for employee' SYNTAX 1.3.6.1.4.1.1466.115.121.
 ↪1.27 SINGLE-VALUE X-ORIGIN 'user defined' )
objectClasses: ( 1.2.643.6.2732288946.2741111200.2726881669.2.50 NAME
 ↪'workplace' DESC 'Workplace for employee' SUP top AUXILIARY MAY (
 ↪idCabinet $ idTable ) X-ORIGIN 'user defined' )
```

Применение новой схемы:

```
dc-1:~# dsconf -D "cn=Directory Manager" -W ldap://localhost schema reload
Enter password for cn=Directory Manager on ldap://localhost:

Attempting to add task entry... This will fail if Schema Reload plug-in is
 ↪not enabled.
Successfully added task entry cn=schema_reload_2023-11-27T07:43:36.534129,
 ↪cn=schema reload task,cn=tasks,cn=config
To verify that the schema reload operation was successful, please check the
 ↪error logs.
```

После репликации файл *99a.ldif* не будет скопирован на второй контроллер, а новый класс и новые атрибуты появятся на нем в файле */etc/dirsrv/slapd-ALD-COMPANY-LAN/schema/99user.ldif*.

```
dc-2:~# grep -A 2 "workpl\|idCab\|idTab" /etc/dirsrv/slapd-ALD-COMPANY-LAN/
 ↪schema/99user.ldif

objectClasses: ( 1.2.643.6.2732288946.2741111200.2726881669.2.50 NAME
 ↪'workpla
 ce' DESC 'Workplace for employee' SUP top AUXILIARY MAY ( idCabinet $
 ↪idTable
  ) X-ORIGIN 'user defined' )
attributeTypes: ( 2.16.840.1.113730.3.1.2384 NAME 'passwordTPRDelayValidFrom'
--
attributeTypes: ( 1.2.643.6.2732288946.2741111200.2726881669.1.100 NAME
 ↪'idCab
 inet' DESC 'Cabinet number for employee' SYNTAX 1.3.6.1.4.1.1466.115.121.1.
 ↪15
  SINGLE-VALUE X-ORIGIN 'user defined' )
--
attributeTypes: ( 1.2.643.6.2732288946.2741111200.2726881669.1.101 NAME
 ↪'idTab
 le' DESC 'Table number for employee' SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
 ↪SIN
 GLE-VALUE X-ORIGIN 'user defined' )
```

В данный момент, при создании пользователей на Портале Управления **ALD Pro** записям пользователей в каталоге, находящимся в `cn=users,cn=accounts,dc=ald,dc=company,dc=lan`, новый созданный класс не будет добавлен автоматически. Если создать пользователя `user1` и посмотреть список

классов, он будет выглядеть так:

```
dc-1:~# ldapsearch -Q -LLL -D "cn=Directory Manager" -W -b "uid=user1,
↪cn=users,cn=accounts,dc=ald,dc=company,dc=lan" objectclass
Enter LDAP Password:
dn: uid=user0,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
objectclass: top
objectclass: person
objectclass: x-ald-user
objectclass: x-ald-user-parsec14
objectclass: x-ald-audit-policy
objectclass: rbta-unit
objectclass: rbta-address
objectclass: rbtaCustomUserAttrs
objectclass: rbta-inetorgperson-ext
objectclass: ruPostMailAccount
objectclass: rbtaUserMeta
objectclass: ipaSshGroupOfPubKeys
objectclass: mepOriginEntry
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: inetUser
objectclass: posixAccount
objectclass: krbPrincipalAux
objectclass: krbTicketPolicyAux
objectclass: ipaObject
objectclass: ipaSshUser
objectclass: ipaNTUserAttrs
```

Команда `ipa config-show` покажет, какие классы по умолчанию добавляются к записи пользователя и к записи группы при их создании. Команда `ipa` должна быть запущена под администратором домена. Для этого надо войти под ним в систему или пройти **kerberos-аутентификацию** с помощью `kinit`. Атрибут `ipaUserObjectClasses` в записи `cn=ipaConfig,cn=etc,dc=ald,dc=company,dc=lan` содержит все классы пользователя, а `ipaGroupObjectClasses` все классы для группы.

```
dc-1:~# ipa config-show --all --raw
  dn: cn=ipaConfig,cn=etc,dc=ald,dc=company,dc=lan
...
  cn: ipaConfig
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
  ipaGroupObjectClasses: top
  ipaGroupObjectClasses: groupofnames
  ipaGroupObjectClasses: nestedgroup
  ipaGroupObjectClasses: ipausergroup
  ipaGroupObjectClasses: ipaobject
  ipaGroupObjectClasses: x-ald-audit-policy
  ipaGroupObjectClasses: rbta-unit
  ipaUserObjectClasses: top
  ipaUserObjectClasses: person
  ipaUserObjectClasses: organizationalperson
  ipaUserObjectClasses: inetorgperson
  ipaUserObjectClasses: inetuser
  ipaUserObjectClasses: posixaccount
  ipaUserObjectClasses: krbprincipalaux
  ipaUserObjectClasses: krbticketpolicyaux
  ipaUserObjectClasses: ipaobject
  ipaUserObjectClasses: ipasshuser
  ipaUserObjectClasses: x-ald-user
  ipaUserObjectClasses: x-ald-user-parsec14
  ipaUserObjectClasses: x-ald-audit-policy
  ipaUserObjectClasses: rbta-unit
  ipaUserObjectClasses: rbta-address
  ipaUserObjectClasses: rbtaCustomUserAttrs
  ipaUserObjectClasses: rbta-inetorgperson-ext
  ipaUserObjectClasses: ruPostMailAccount
  ipaUserObjectClasses: rbtaUserMeta
```

С помощью `ipa config-mod` можно добавить новый класс `workplace` и тогда он будет добавляться автоматически к новым записям пользователей при их создании. В команде необходимо перечислить все классы через запятую, добавив в конце новый класс:

```
dc-1:~# ipa config-mod --userobjectclasses={top,person,organizationalperson,
 ↪inetorgperson,inetuser,posixaccount,krbprincipalaux,krbticketpolicyaux,
 ↪ipaobject,ipasshuser,x-ald-user,x-ald-user-parsec14,x-ald-audit-policy,rbta-
 ↪unit,rbta-address,rbtaCustomUserAttrs,rbta-inetorgperson-ext,
 ↪ruPostMailAccount,rbtaUserMeta,workplace}


...
  Классы объектов для пользователей по умолчанию: top, person,
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
↪organizationalperson, inetorgperson, inetuser,
                                                    posixaccount,
↪krbprincipalaux, krbticketpolicyaux,
                                                    ipaobject, ipasshuser, x-
↪ald-user, x-ald-user-parsec14,
                                                    x-ald-audit-policy, rbta-
↪unit, rbta-address,
                                                    rbtaCustomUserAttrs, rbta-
↪inetorgperson-ext,
                                                    ruPostMailAccount,
↪rbtaUserMeta, workplace
...
```

Аналогично для групп, если надо создать новый класс для групп, в команде вместо ключа `--userobjectclasses` используется ключ `--groupobjectclasses`.

Удобнее добавлять новые классы через Портал Управления **ALD Pro** через пункты меню **Управление доменом** – **Пользователи и группы**. Справа будет список существующих классов, слева список классов по умолчанию. См. *Рисунок 6.4.20 Параметры пользователей. Классы*.

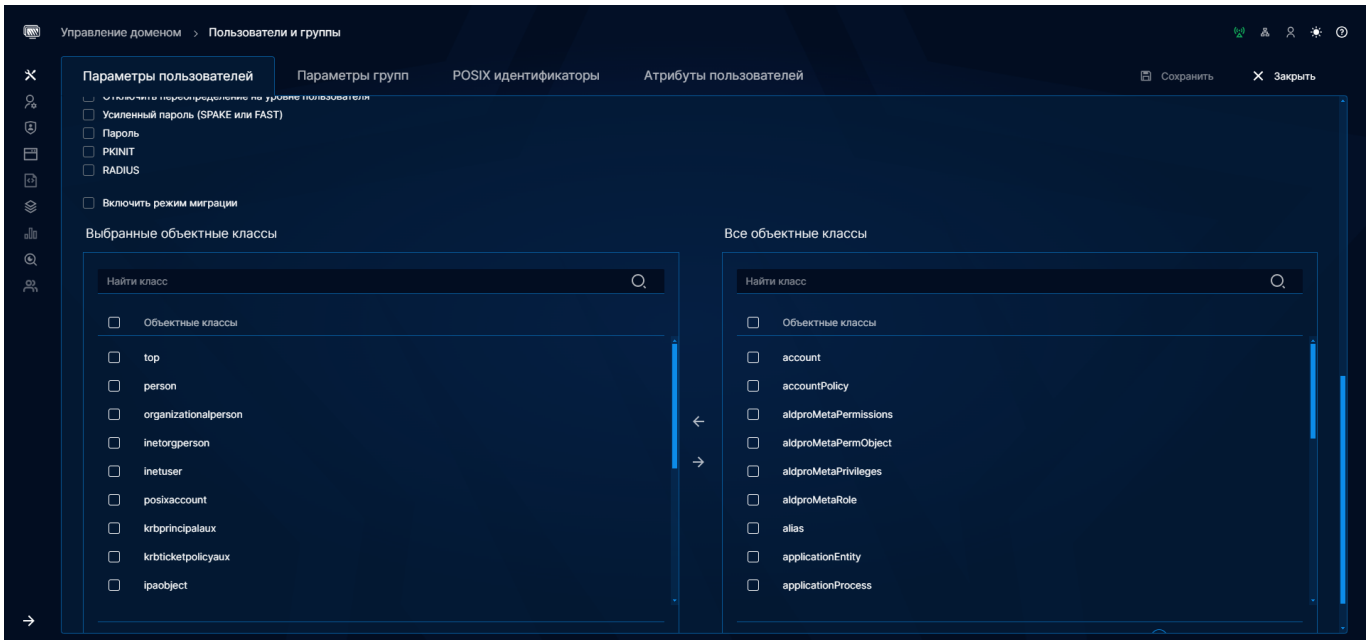


Рисунок 3.41 – Рисунок 6.4.20 Параметры пользователей. Классы

На следующей вкладе доступны аналогичные настройки для групп. См. *Рисунок 6.4.21 Параметры групп. Классы*.

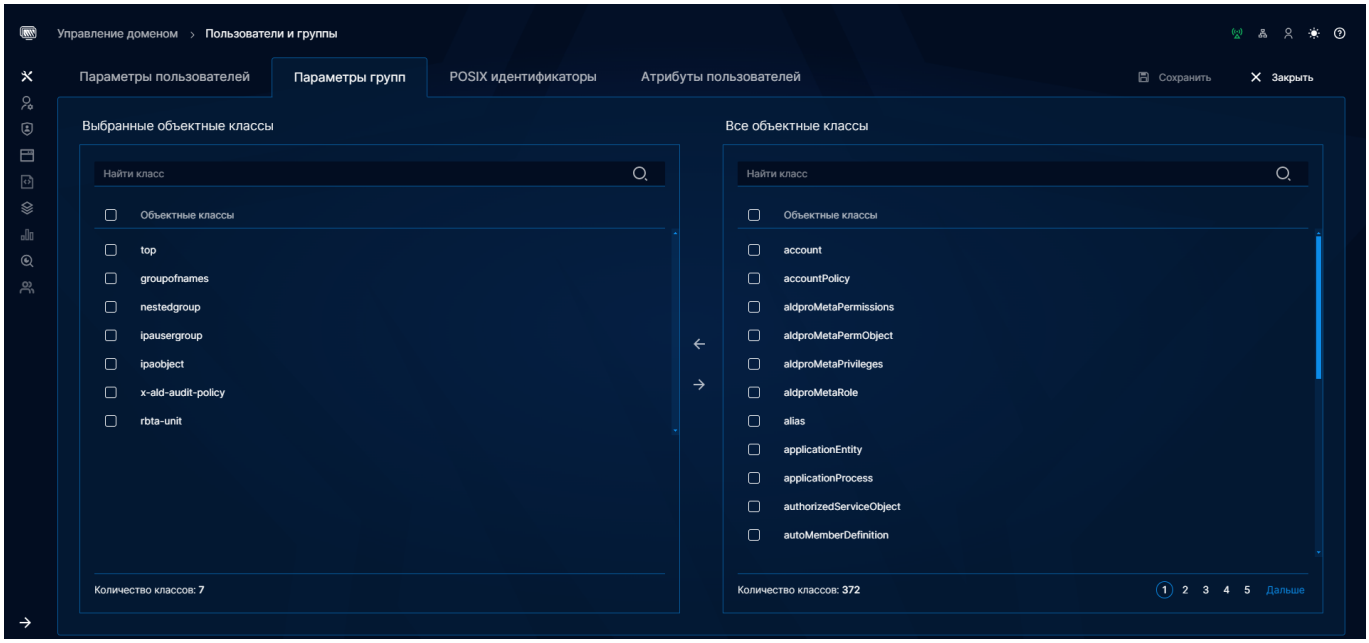


Рисунок 3.42 – Рисунок 6.4.21 Параметры групп. Классы

После того, как класс добавлен для записей пользователей, атрибуты `idCabinet`, `idTable` доступны для добавления и редактирования. Пользователь `user2` был создан через Портал Управления **ALD Pro**. Присвойте значения атрибутам `idCabinet`, `idTable` для `user2`:

```
dc-1:~# ldapmodify -D "cn=Directory Manager" -W
Enter LDAP Password:

dn: uid=user2,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
changetype: modify
add: idCabinet
idCabinet: Отдел статистики
-
add: idTable
idTable: 10
modifying entry "uid=user1,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"
```

Команда завершена успешно, для проверки можно обратить внимание на атрибуты пользователя `user2`:

```
dc-1:~# ldapsearch -Q -LLL -D "cn=Directory Manager" -W -b "uid=user2,
↪cn=users,cn=accounts,dc=ald,dc=company,dc=lan" idCabinet idTable
Enter LDAP Password:
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
dn: uid=user1,cn=users,cn=accounts,dc=ald,dc=company,dc=lan
idCabinet:: 0J7RgtC00LXQuyDRgdGC0LDRgtC40YHRgtC40LrQuA==
idTable: 10
```

Так как `IdCabinet` содержит кириллицу, в выводе команды он отображается в base64-кодировке.

3.4.6. Заключение

LDAP разрабатывался с целью хранения любой информации об объектах на предприятии, таких как пользователи, компьютеры, серверы, подразделения и др. Информация удобно расположена в виде иерархического древа, которое строго типизировано объектными классами. База данных ориентирована на чтение, где быстро и легко можно получить любую информацию по объектам.

На сегодняшний день **LDAP-каталог** – это стандарт. Множество продуктов имеют встроенные интеграции с службой каталога, а также существует большое количество библиотек для разных языков для доступа к **LDAP-серверу**, например: python-ldap для python, ldaptive для java. В некоторые языки программирования уже встроена работа **LDAP**, например, в языки PHP и C#. А также у продукта **ALD Pro** есть REST API, через него можно управлять каталогом, используя простые Web-запросы.

3.5. Повышение привилегий доменных пользователей с помощью правил SUDO

Для установки программного обеспечения и выполнения других задач администрирования пользователю нужны привилегии суперпользователя. Сотрудники могут использовать учетную запись root, но из соображений безопасности более корректным считается работать из-под обычной учетной записи и повышать привилегии только при выполнении отдельных команд. Еще более востребован указанный подход, когда часть административных прав нужно делегировать обычным пользователям, например, чтобы разрешить им перезапуск служб или установку приложений.

В ОС Windows повышение привилегий реализуется с помощью команды «Запуск от имени

администратора», которая вызывает утилиту runas.exe с требуемыми параметрами. На компьютерах под управлением Linux аналогичного результата можно добиться с помощью утилиты sudo (Substitute User and do, подменить пользователя и выполнить), которая имеет богатые настройки и позволяет журналировать неудачные аутентификации.

Например, вызовом следующей команды обычный пользователь Иван Кузнецов может установить приложение `htop`, если ему разрешено запускать утилиту `apt` через `sudo`:

```
ivan.kuznetsov@dc-1:~$ sudo apt install htop
```

Примечание: Кроме sudo повышать привилегии возможно также с помощью команд `su/runuser` и битов SUID/GUID, но эти способы не являются предметом рассмотрения данной инструкции.

3.5.1. Что такое правила SUDO

Правила SUDO позволяют определенным пользователям на конкретных хостах выполнять отдельные команды с повышенными привилегиями, создавая, таким образом, дополнительный слой авторизации, также как и в случае правил HBAC. Отличие между этими видами правил заключается в том, что правила HBAC проверяются на уровне PAM-стека, а правила SUDO непосредственно утилитой sudo.

Для возможности использования утилиты sudo пользователю в первую очередь нужны права на обращение к этому приложению на уровне HBAC-правил, так как при вызове утилиты sudo сначала создается PAM-контекст, а уже потом утилита приступает к проверке правил. Если таковых прав у него не будет, то до проверки правил SUDO дело не дойдет.

Локальные настройки утилиты sudo находятся в файле `/etc/sudoers`, который назван так потому, что пользователей, кому разрешено повышать привилегии с помощью утилиты `sudo`, называют sudo enabled users или кратко sudoers. В файле могут быть строки трех типов: параметры по умолчанию, псевдонимы (алиасы, именованные списки или проще переменные) и сами правила. Синтаксис правил представлен на рисунке 1.

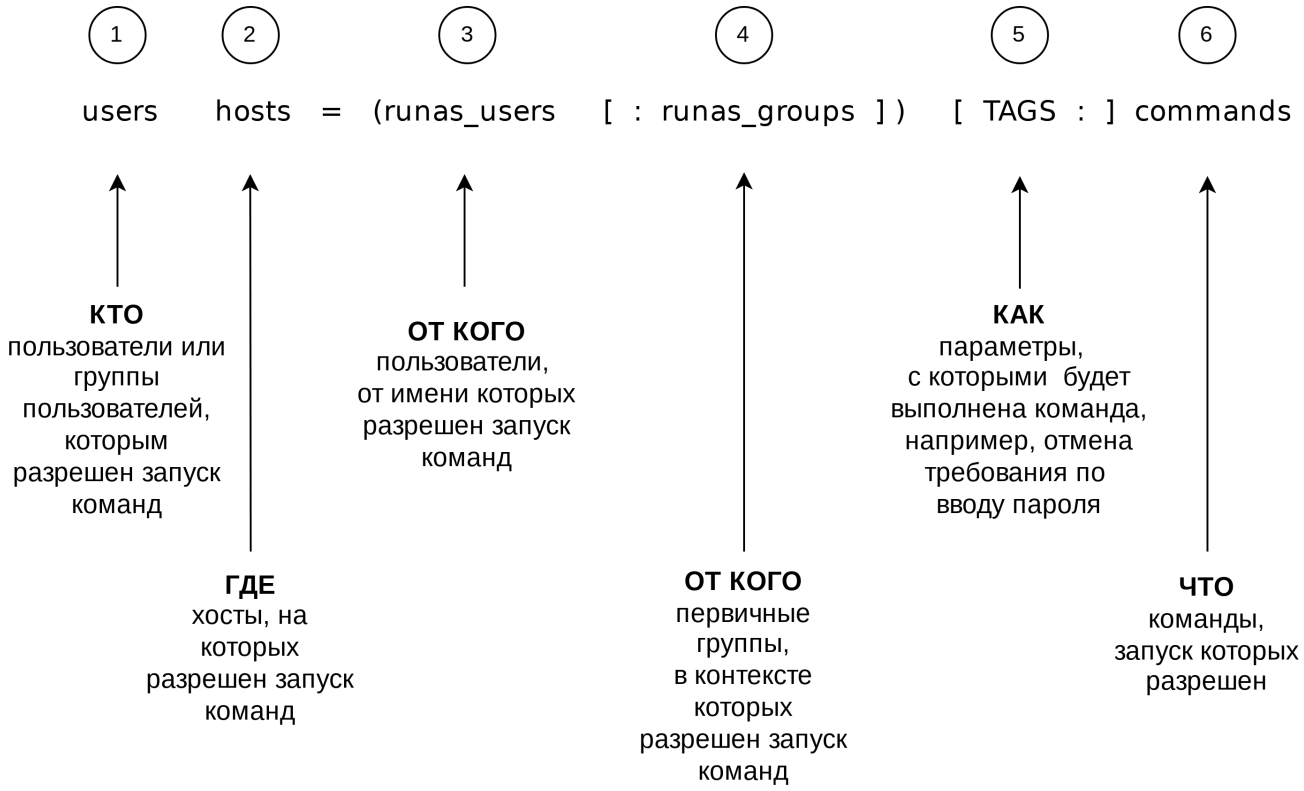


Рисунок 3.43 – Синтаксис правил SUDO

Правила могут быть как разрешающими, так и запрещающими, но по умолчанию считается, что прав на выполнение команд через sudo ни у кого нет. Для первых четырех компонентов правил следует определить область действия одним из двух способов:

- Любой субъект (ALL) — правило будет распространяться на все субъекты данного вида.
- Указанные субъекты — правило будет распространяться только на указанный перечень субъектов данного вида. Если требуется задать несколько значений, элементы списка должны быть разделены символом запятой. Для упрощения работы с большими списками синтаксис файла позволяет задавать именованные списки, или так называемые алиасы. Для удобства настройки синтаксис именованных списков позволяет исключать из них отдельные значения.

Компоненты правила:

1. **Пользователи и группы пользователей**, которым разрешен запуск команд в рамках данного правила. Перед именем группы следует указывать символ процента.

```
localuser       ALL=(ALL:ALL)                   NOPASSWD:       /usr/bin/netstat
%localgroup     pc1=(root:root)                 PASSWD:         /usr/bin/systemctl restart sssd
%localgroup     192.168.45.12=(root:root)       PASSWD:         /usr/bin/systemctl restart sssd
```

2. **Хосты**, на которых разрешен запуск команд. Это может быть имя компьютера или его IP адрес. Параметр полезен, если один и тот же файл копируется на несколько хостов.

```
localuser      ALL=(ALL:ALL)                NOPASSWD:      /usr/bin/netstat
%localgroup    pc1=(root:root)              PASSWD:        /usr/bin/systemctl restart sssd
%localgroup    192.168.45.12=(root:root)    PASSWD:        /usr/bin/systemctl restart sssd
```

3. **Пользователи, от имени которых разрешен запуск команд**. При выполнении команды через `sudo` по умолчанию предполагается, что команда запускается от имени root, но можно указать имя пользователя в явном виде с помощью ключа -u, и данный компонент правила позволяет ограничить перечень допустимых значений.

```
localuser      ALL=(ALL:ALL)                NOPASSWD:      /usr/bin/netstat
%localgroup    pc1=(root:root)              PASSWD:        /usr/bin/systemctl restart sssd
%localgroup    192.168.45.12=(root:root)    PASSWD:        /usr/bin/systemctl restart sssd
```

4. **Первичные группы, в контексте которых разрешен запуск команд**. По умолчанию используется первичная группа пользователя, от имени которого выполняется команда, но группу можно указать явно с помощью ключа -g. Данное значение проявляет себя, когда выполняются команды, которые создают новые файлы и папки, например, `touch` или `mkdir`. Этот параметр не является обязательным.

```
localuser      ALL=(ALL:ALL)                NOPASSWD:      /usr/bin/netstat
%localgroup    pc1=(root:root)              PASSWD:        /usr/bin/systemctl restart sssd
%localgroup    192.168.45.12=(root:root)    PASSWD:        /usr/bin/systemctl restart sssd
```

5. **Параметры, с которыми будет выполнена команда**, позволяют изменить поведение утилиты `sudo`, например, можно отключить запрос пароля с помощью параметра NOPASSWD. Этот параметр не является обязательным. Полный перечень доступных значений: EXEC, NOEXEC, FOLLOW, NOFOLLOW, LOG_INPUT, NOLOG_INPUT, LOG_OUTPUT, NOLOG_OUTPUT, MAIL, NOMAIL, PASSWD, NOPASSWD, SETENV и NOSETENV. О значении параметров можно посмотреть в справке `man sudoers`.

```
localuser      ALL=(ALL:ALL)                NOPASSWD:      /usr/bin/netstat
%localgroup    pc1=(root:root)              PASSWD:        /usr/bin/systemctl restart sssd
%localgroup    192.168.45.12=(root:root)    PASSWD:        /usr/bin/systemctl restart sssd
```

6. **Команды**, которые разрешено запускать в рамках этого правила. Это должен быть полный путь к исполняемому файлу, в конце строки можно указать допустимые параметры вызова.

```
localuser      ALL=(ALL:ALL)                NOPASSWD:      /usr/bin/netstat
%localgroup    pc1=(root:root)              NOPASSWD:      /usr/bin/systemctl restart sssd
%localgroup    192.168.45.12=(root:root)    NOPASSWD:      /usr/bin/systemctl restart sssd
```

Полный путь к исполняемым файлам можно узнать с помощью команды which, которую лучше запускать на целевых хостах, где предполагается запускать эти команды:

```
#which systemctl
/usr/bin/systemctl
```

В правилах SUDO можно использовать не только конкретные значения, но и шаблоны. В Astra Linux до версии 1.7.4 включительно используется проверенная версия sudo 1.8.x, в которой доступны только шаблоны в стиле shell, обработка которых выполняется через функции glob и fnmatch. С версии sudo 1.9.10 появится возможность использовать полноценные регулярные выражения.

В шаблонах можно использовать следующие символы подстановки (wildcards), или как их еще называют метасимволы:

- **«?»** – соответствует одному любому символу;
- **«*»** – соответствует любому количеству любых символов, в т.ч. пустой строке. С использованием символа * следует быть крайне осторожным, подробнее смотри в разделе «5 Лучших практик»;
- **«\»** – позволяет экранировать спецсимволы, т.е. отключить их управляющую функцию. Используется, когда нужен знак вопроса, звездочки, двоеточия и др.;
- **«“”»** – соответствует пустой строке, если пустая строка указана в качестве единственного параметра команды, то эта команда может быть выполнена только без параметров;
- **[…]** – соответствует одному символу из указанного диапазона, например:
  - **[abc]** соответствует символу a, b или c;
  - **[a-z]** соответствует строчному символу латинского алфавита;
  - **[[:lower:]]** соответствует строчному символу латинского алфавита, но диапазон задан с помощью именованного класса символов (named character classes), полный перечень которых включает alnum, alpha, blank, cntrl, digit, graph, lower, print, punct, space, upper, xdigit.
- **[!…]** – восклицательный знак в начале диапазона позволяет инвертировать набор символов, т.е. шаблон соответствует любому символу, который не входит в указанный диапазон.

3.5.2. Механизм работы правил SUDO

Настройки утилиты sudo определяются содержимым файла `/etc/sudoer``s`. В этом файле находится также инструкция `#includedir /etc/sudoers.d`, которая включает содержимое дополнительных файлов из указанной директории. Инструкция начинается с символа решетки #, как обычный комментарий, но комментарием не является, что может ввести в заблуждение. Сделано это так из соображений обратной совместимости, т.к. инструкции include и includedir были добавлены значительно позже, в 2004 и 2017 годах соответственно. С версии 1.9.1 появится возможность использовать символ @ собачки вместо решетки, что уменьшит путаницу.

В начале файла есть предупреждение о том, что редактировать правила sudo напрямую не рекомендуется, и нужно воспользоваться утилитой `visudo`. Указанная утилита откроет файл в nano и обеспечит проверку синтаксиса перед сохранением изменений. Заменить редактор по умолчанию можно командой `sudo update-alternatives -config editor`.

```
#
## This file MUST be edited with the 'visudo' command as root.
#
## Please consider adding local content in /etc/sudoers.d/ instead of
## directly modifying this file.
#
## See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/
 ↪bin:/sbin:/bin"

## Host alias specification
## User alias specification
## Cmnd alias specification

## User privilege specification
root    ALL=(ALL:ALL) ALL

## Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
### See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d

%astra-admin    ALL=(ALL:ALL) ALL
```

После предупреждения задано несколько параметров по умолчанию:

- Параметр env_reset позволяет ограничить набор переменных из среды окружения пользователя, которые будут доступны запускаемой утилите. Это важно из соображений безопасности, поскольку эти переменные могут влиять на поведение утилит, запускаемых с привилегиями супрепользователя.
- Параметр mail_badpass предписывает системе отправлять уведомления о неудачных попытках ввода пароля при выполнении команды sudo. Предполагается доставка в локальный почтовый ящик `/var/mail/root` через exim. На ALSE 1.7 с уровнем доступа Смоленск exim не заработает без дополнительных настроек системы мандатного контроля.
- Параметр secure_path позволяет задать список каталогов, в которых будет выполняться поиск запускаемых через sudo утилит, когда не указан полный путь к файлу. Это исключает запуск вредоносных приложений с повышенными привилегиями.

Правила, представленные в файле `/etc/sudoers` сразу после установки операционной системы:

- Правило «root ALL=(ALL:ALL) ALL» означает, что пользователь root может на любом хосте от имени любого пользователя и в контексте любой первичной группы выполнить любую команду.
- Правило «%sudo ALL=(ALL:ALL) ALL» означает тоже самое для группы sudo.
- Правило «%astra-admin ALL=(ALL:ALL) ALL» означает тоже самое для группы astra-admin. Обратите внимание на тот факт, что после продвижения сервера доменный пользователь admin автоматически вносится в список участников локальной группы astra-admin, за счет чего получает право на выполнение команд от имени суперпользователя.

3.5.3. Механизм получения правил SUDO из LDAP

Правила SUDO можно хранить не только в локальных файлах, но и централизованно. Любой сервер каталогов можно сделать поставщиком правил SUDO, если расширить схему должным образом и назначить его источником правил. Список источников утилита sudo получает через библиотеку службы имен (Name Service Switch, NSS), настройки которой находятся в файле `/etc/nsswitch.conf`. В операционных системах Linux через этот механизм настраиваются источники для получения информации о пользователях, группах, DNS-записях и многом другом. Основные вызовы NSS реализованы в библиотеке libc, а та уже, в свою очередь, выполняет обращение к необходимым бэкендам

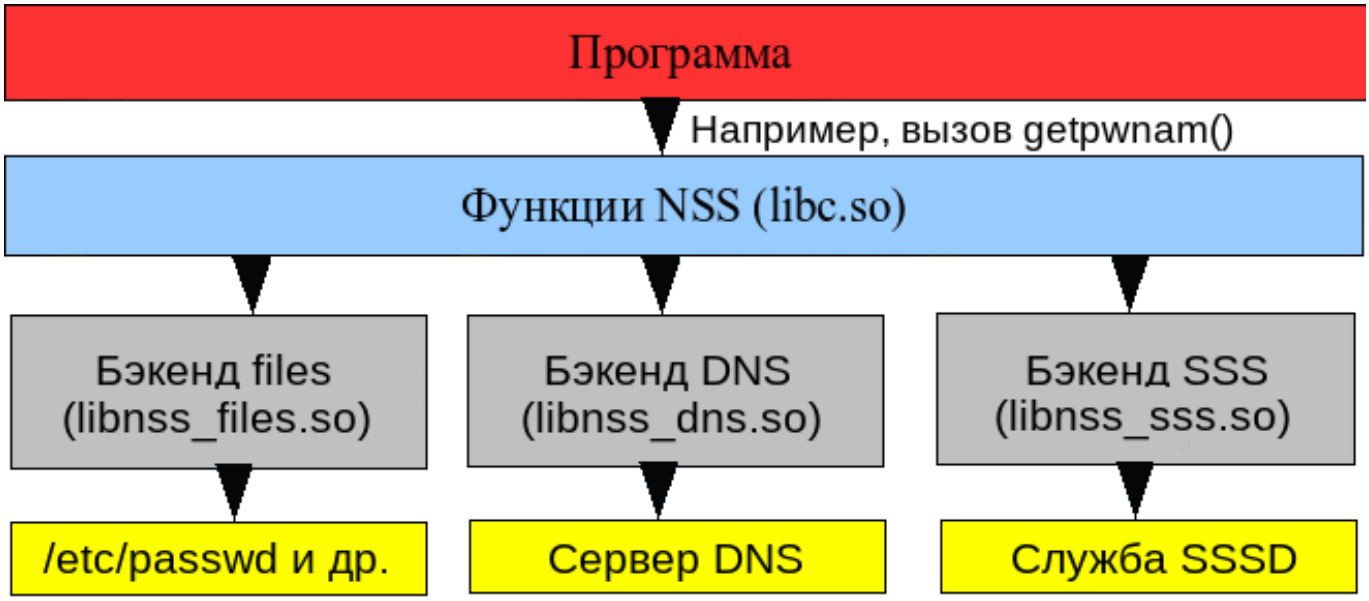


Рисунок 3.44 – Архитектура диспетчера службы имен (Name Service Switch, NSS)

После установки freeipa-client в файле `/etc/nsswitch` можно найти строку с настройкой базы данных sudoers. По умолчанию правила сначала берутся из локального файла, а затем через модуль sss, который отвечает за взаимодействие с LDAP-каталогом через службу SSSD.

```
$ cat /etc/nsswitch.conf

sudoers: files sss
```

Поддержка каталогов появилась в sudo с выходом модуля ldap для nss в 2004 году. Источником правил для модуля служили записи из DN `ou=sudoers,{basedn}=имя,{basedn}=домена,{basedn}=организации`. Модуль использовал примитивную схему хранения данных, которая повторяла синтаксис

локального файла sudoers, игнорируя доступную в каталоге нормализацию данных, например, в части пользователей, групп и хостов. Поэтому при реализации поддержки правил SUDO разработчики FreeIPA создали новую схему, лишенную указанных недостатков. Информация о правилах во FreeIPA хранится в DN `cn=sudorules,cn=sudo,{basedn}=имя,{basedn}=домена,{basedn}=организации`, и модуль sss через службу SSSD берет данные напрямую из этой ветки каталога.

Для обеспечения совместимости со старым модулем ldap, служба каталога FreeIPA с помощью плагина Compat автоматически конвертирует настройки правил в старый формат, см. рисунок 3. Например, если для правила в `cn=sudorules` установить ipaEnabledFlag=FALSE, то соответствующая запись в `ou=sudoers` будет автоматически удалена, но стоит вернуть атрибуту значение TRUE и запись будет автоматически воссоздана.

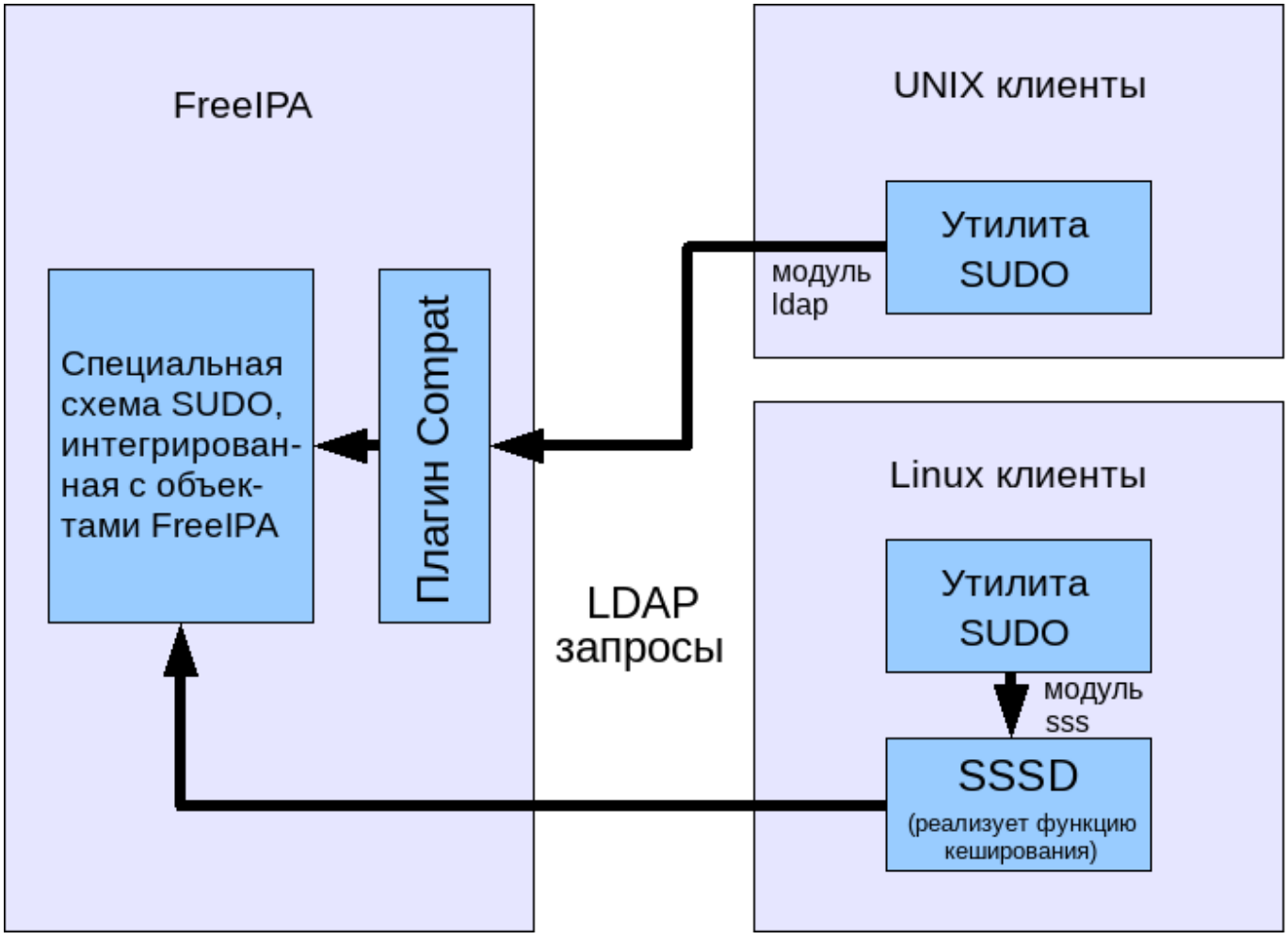


Рисунок 3.45 – Источник правил SUDO в зависимости от реализации клиентской части

Служба SSSD реализует дополнительно функцию кеширования, что дает пользователям возможность повышать свои привилегии, даже если они находятся вне домена. По

умолчанию время кеширования составляет 5400 секунд, и для немедленного применения правил на клиентской машине необходимо выполнить очистку кеша следующими командами:

```
sudo systemctl stop sssd
sudo rm /var/lib/sss/db/*
sudo systemctl start sssd
```

Или воспользоваться инструментом `sssctl`, входящим в пакет sssd-tools:

```
sudo sssctl cache-remove
```

Еще один важный момент. В силу особенностей FreeIPA в правилах sudo не получится использовать следующие группы:

- группу пользователей ipausers, т.к. у нее нет POSIX идентификатора и поэтому на целевых хостах служба SSSD не отображает участие пользователей в этой группе;
- группу хостов ipaservers, т.к. у нее нет класса mepmanagedentry и соответствующих зависимостей.

Самый простой способ обойти указанные проблемы – это создать вспомогательные группы sudo-ipausers/sudo-ipaservers и сделать группы ipausers/ipaservers их участниками. В этом случае можно использовать вспомогательные группы в правилах SUDO без ограничений.

3.5.4. Настройка правил SUDO в домене

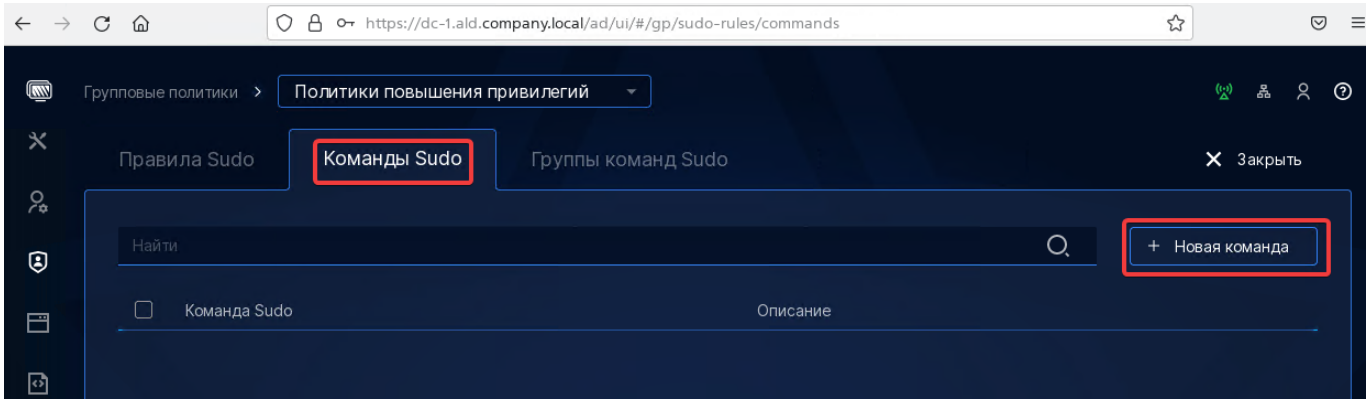
3.5.4.1. Через портал управления ALD Pro

Создание команды

Учитывая, что пользователи и хосты уже есть в домене, настройку правил следует начать с создания команды. Сделать это можно через портал управления ALD Pro, веб-интерфейс FreeIPA или из командной строки. Единственное, интерфейс ALD Pro до версии 2.0.0 не позволяет использовать пробелы в названии команд, поэтому для создания команд с параметрами потребуется воспользоваться интерфейсом FreeIPA или командной строкой.

1. Открыть страницу «Групповые политики > Политики повышения привилегий > Команды Sudo».

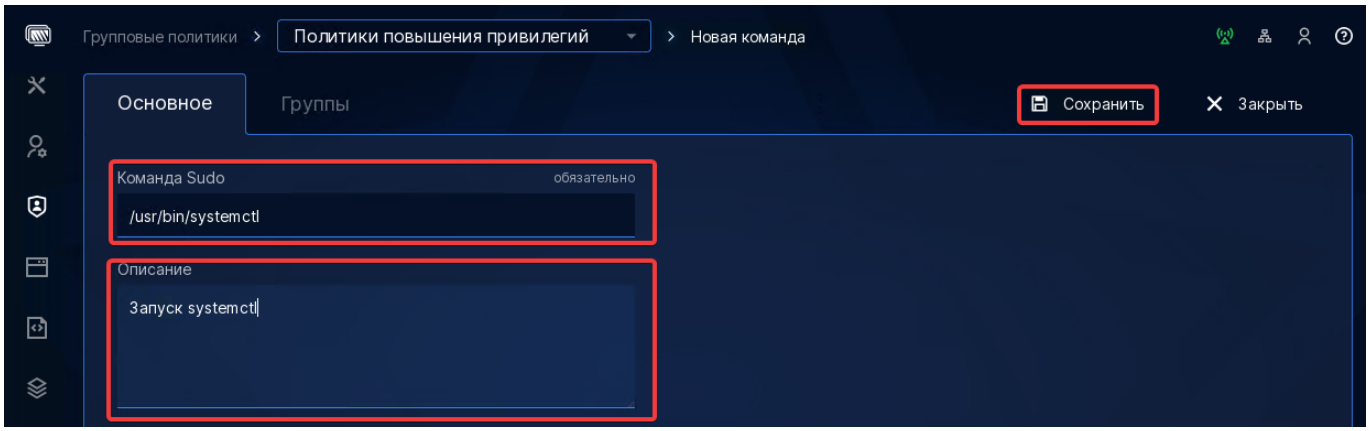
2. Нажать кнопку «+ Новая команда».



Примечание: В имени команды можно использовать `a-z`, `A-Z`, `0-9`, `-_./~`и пробелы (кроме первого и последнего).

---

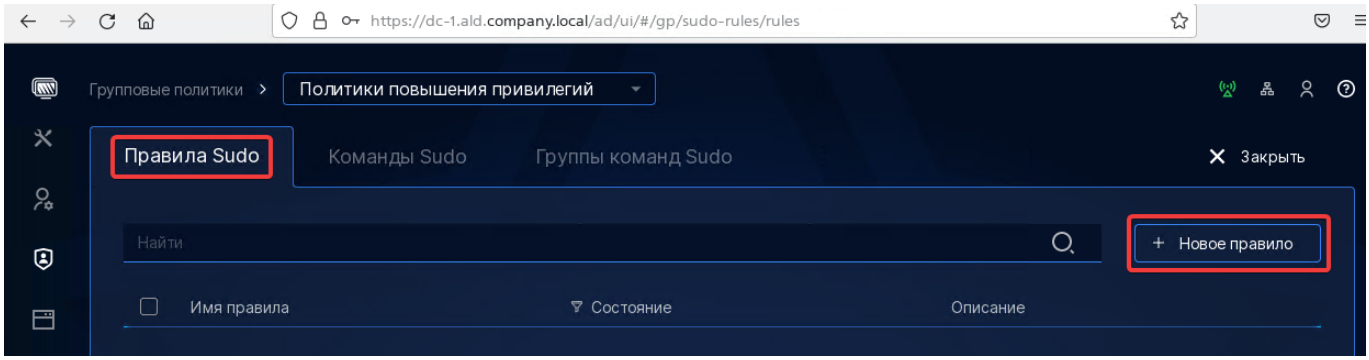
3. Ввести команду /usr/bin/systemctl, описание (опционально) и нажать «Сохранить».



Создание правила

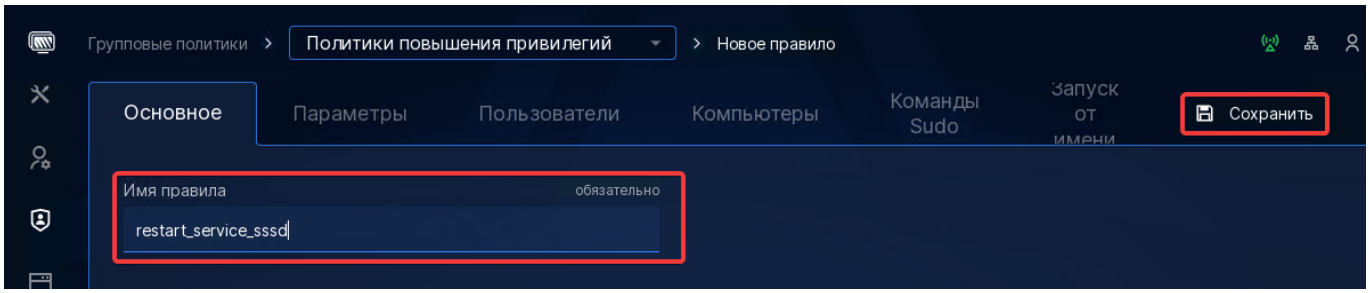
1. Открыть страницу «Групповые политики > Политики повышения привилегий > Правила Sudo».

2. Нажать кнопку «+ Новое правило».



3. На странице «Новое правило» ввести имя правила и нажать кнопку «Сохранить».

Примечание: В имени правила можно использовать `a-z`, `A-Z`, `0-9`, `-_`

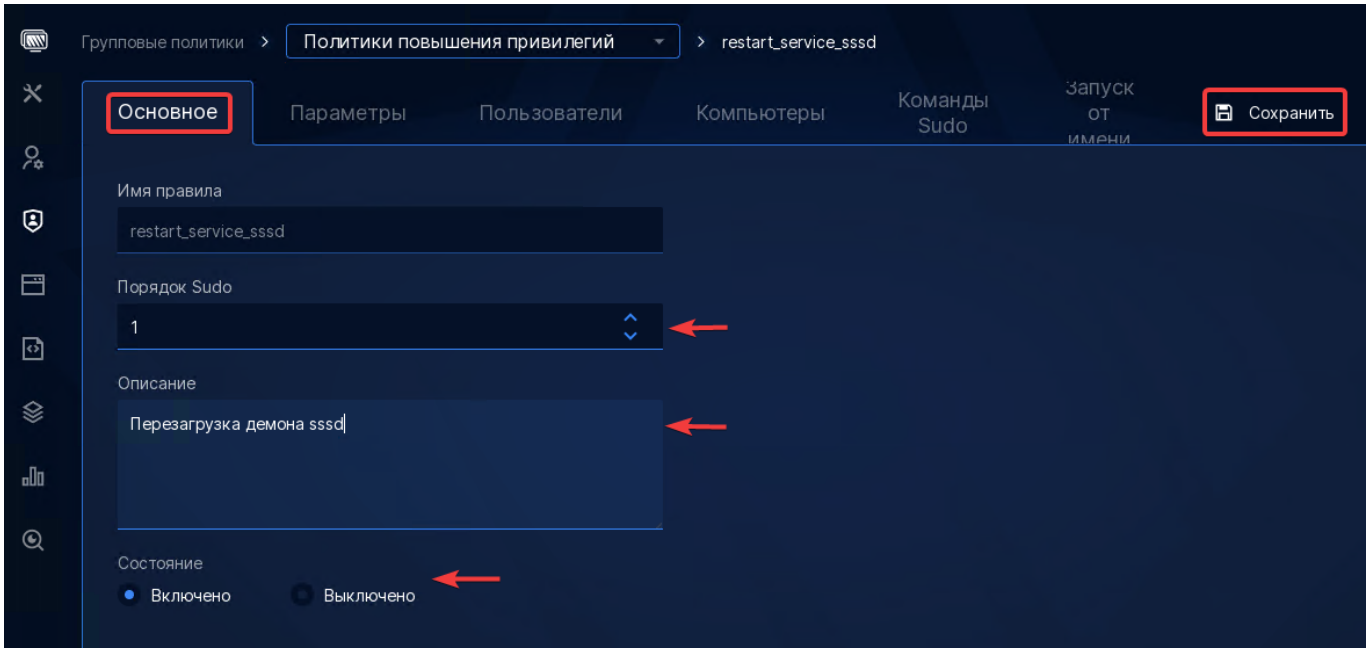


4. На странице правила задать следующие параметры:

    1. Раздел «Основные»

        - **Порядок sudo** (необязательный параметр) – целое число, которое определяет очередность выполнения правил. Чем больше значение, тем позже обрабатывается правило, а значит оно может переопределить те правила, которые стоят перед ним.
        - Если список команд содержит несколько значений, они обрабатываются в указанном порядке. Если у правила одновременно заданы и разрешающие, и запрещающие команды, то сначала обрабатываются разрешающие.
        - **Описание** - необязательный комментарий к правилу.
        - **Состояние** - переключатель определяет, включено правило или нет.

Обязательно сохранить изменения до перехода к следующей вкладке, иначе изменения будут утеряны.



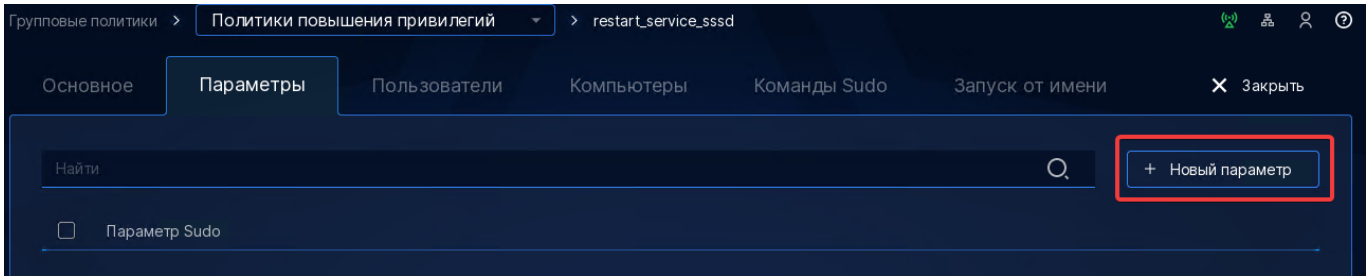
2. Раздел «Параметры». С помощью параметров можно изменить поведение утилиты для ее тонкой настройки. Ниже приведено несколько наиболее востребованных параметров:

    - authenticate – с помощью этого флага можно обязать пользователей вводить пароль при выполнении команды через sudo. Параметр включен по умолчанию, и для отмены требования по вводу пароля его следует отключить, для чего нужно поставить восклицательный знак перед названием параметра «!authenticate»;
    - passwd_tries – задает количество попыток ввода пароля, прежде чем sudo завершит работу и зарегистрирует ошибку. Задается в виде переменной, по умолчанию passwd_tries=3;
    - timestamp_timeout – задает количество минут, которое должно пройти перед тем, как sudo повторно запросит пароль. Если установить таймаут равным 0, то утилита будет запрашивать пароль всегда, если установить отрицательное значение, таймаут будет отключен и введенный ранее пароль будет храниться бессрочно. По умолчанию таймаут составляет 15 минут.

Информацию по остальным параметрам можно найти в `man sudoers`. Значения по умолчанию, с которыми утилита `sudo` была скомпилирована, можно узнать, вызвав команду sudo с ключом -V под суперпользователем, например `sudo sudo -V`.

Для создания параметра:

1. Нажать кнопку «+ Новый параметр»:



2. Ввести параметр, например «timestamp_timeout=5», и нажать кнопку «Сохранить»:

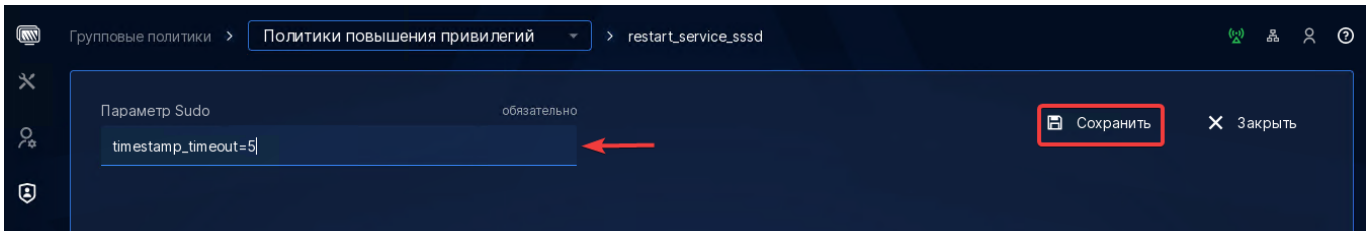


Рисунок 3.46 – Сохранить 1

3. Раздел «Пользователи». На этой вкладке можно задать список пользователей и их групп, которым в соответствии с этим правилом будет разрешено вызывать команды через sudo. Указать пользователя и нажать кнопку «Сохранить».

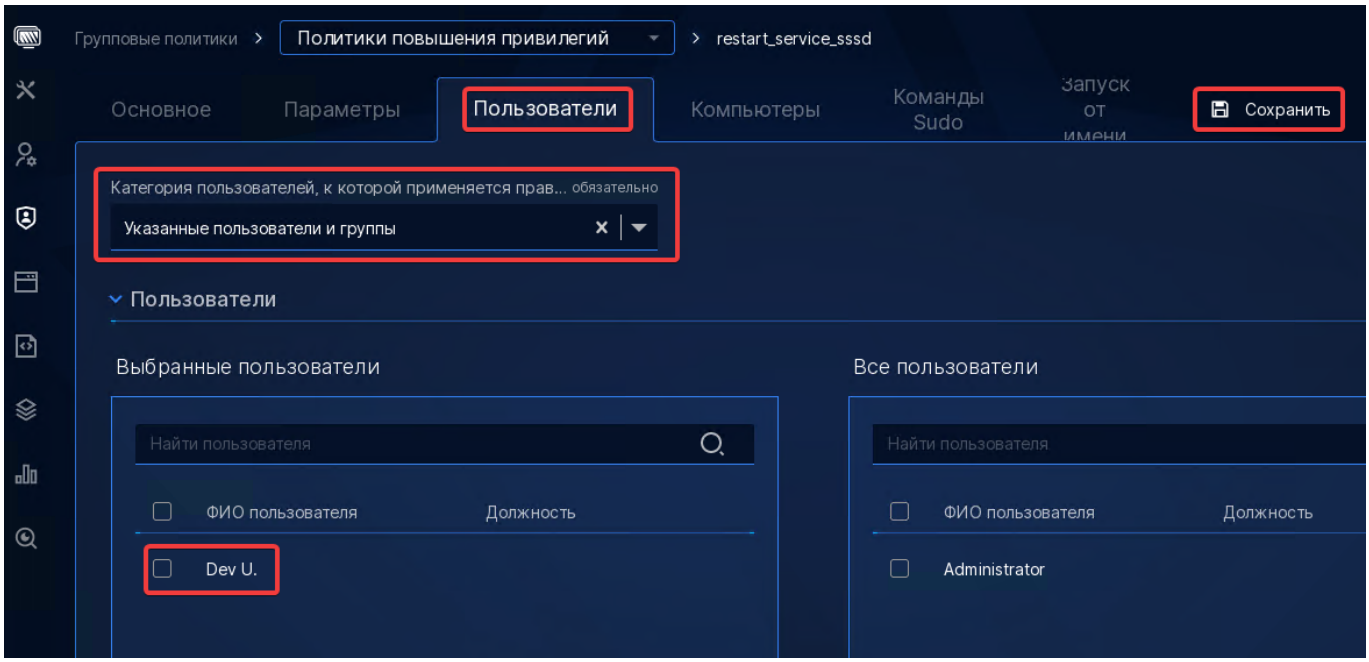


Рисунок 3.47 – Сохранить 2

4. Раздел «Компьютеры». На этой вкладке можно задать список компьютеров или их групп, на которых в соответствии с этим правилом будет разрешено вызывать команды через sudo. Указать компьютер и нажать кнопку «Сохранить».

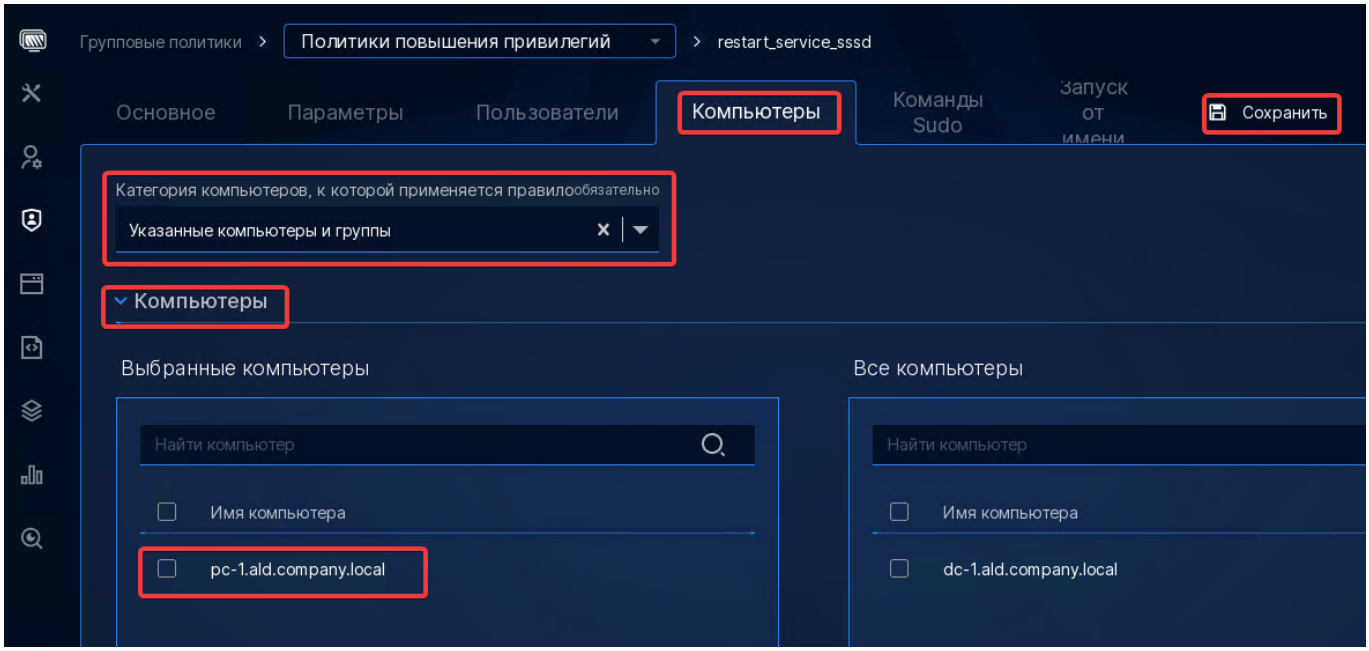


Рисунок 3.48 – Сохранить 3

5. Раздел «Команды Sudo». На этой вкладке можно задать список команд, которые разрешено/запрещено будет выполнять. Выбрать команды и нажать кнопку «Сохранить». Сначала применяются разрешающие команды, затем запрещающие, поэтому у запрещающих будет выше приоритет.

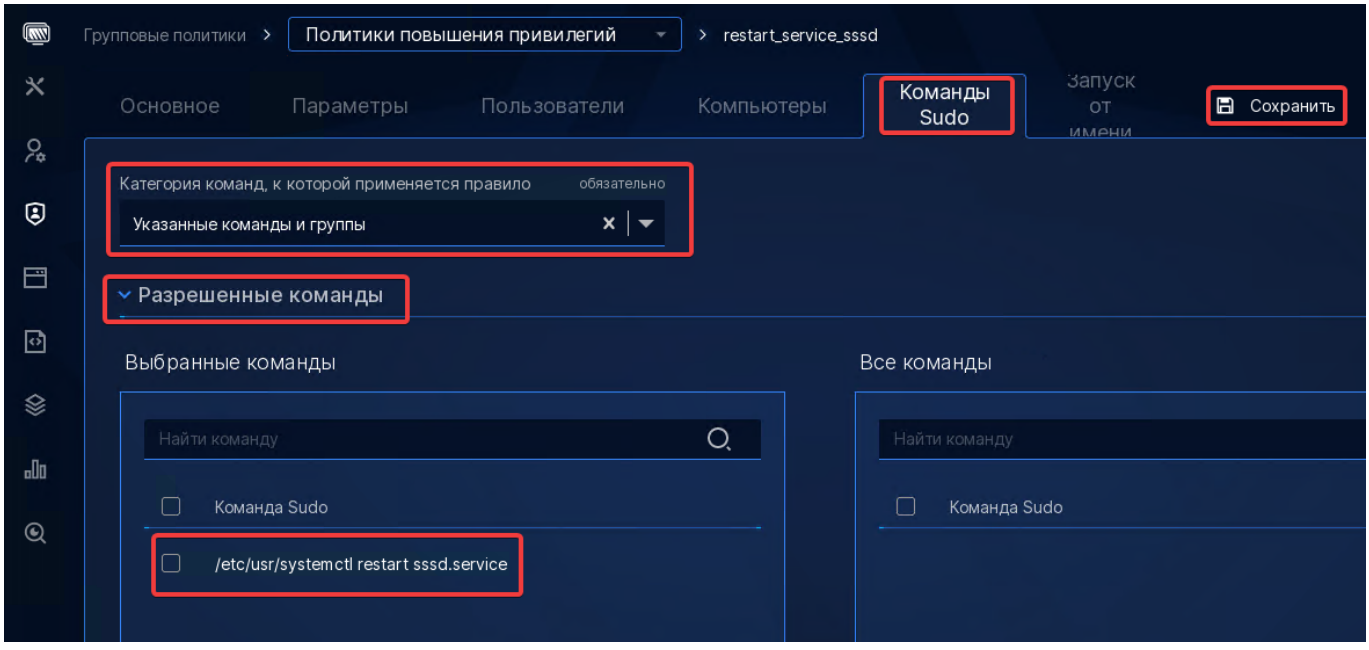
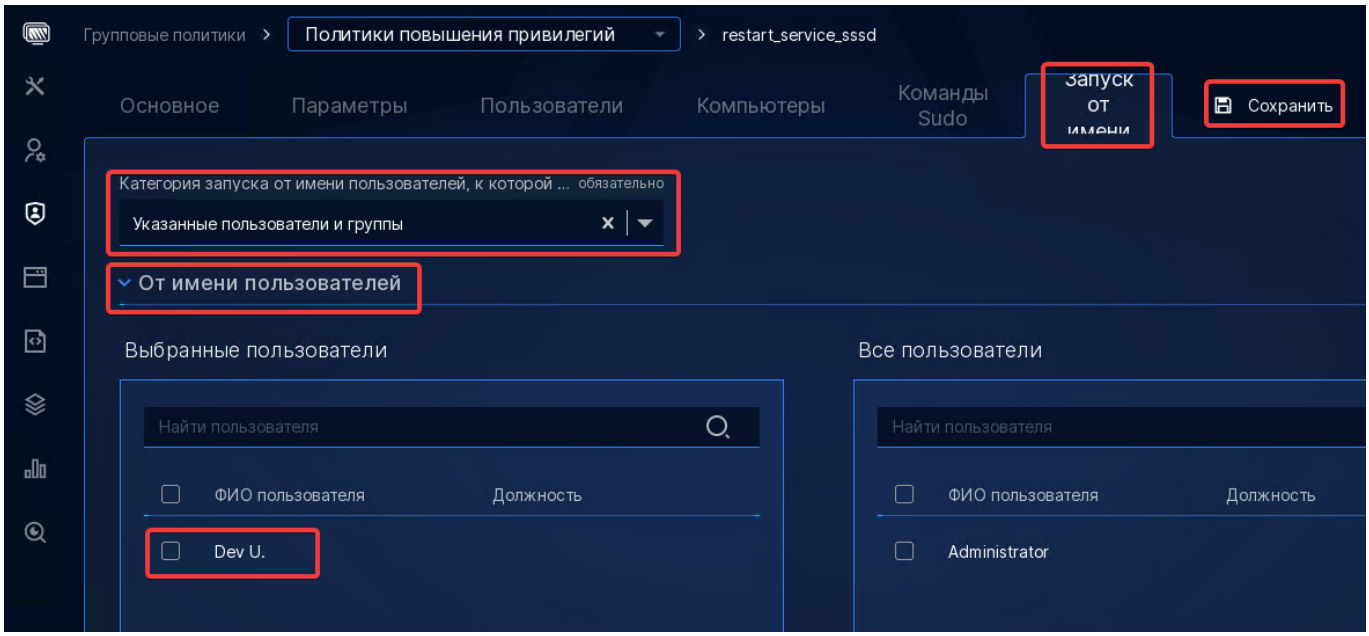


Рисунок 3.49 – Команды sudo

6. Раздел «Запуск от имени» По умолчанию команды sudo запускаются от имени суперпользователя root в контексте его первичной группы, но это поведение можно изменить с помощью ключей -u и -g. На этой вкладке можно определить список

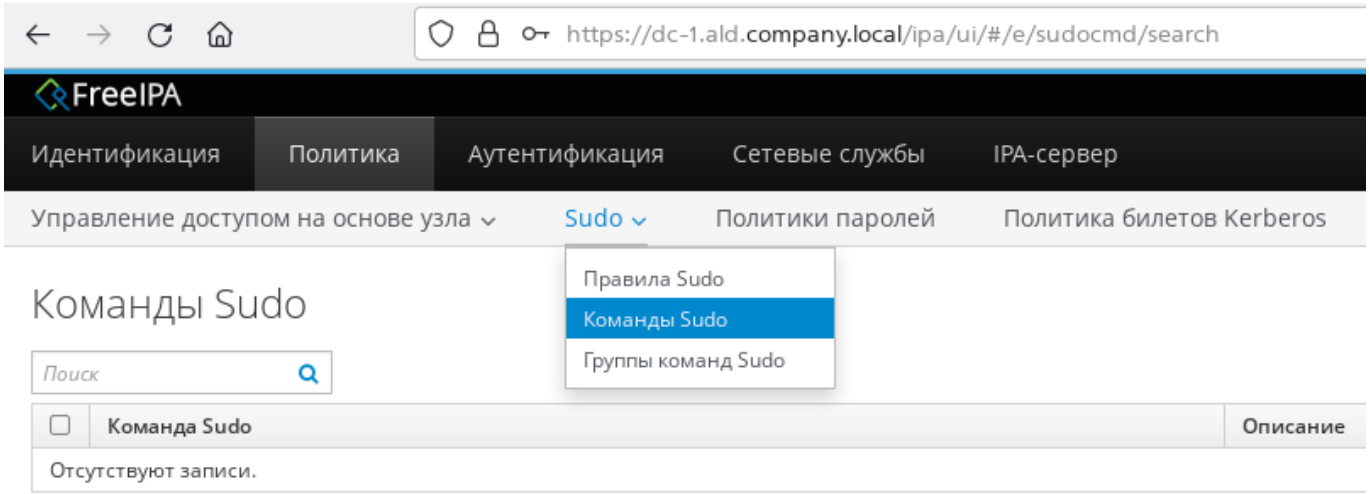
пользователей и групп, от имени которых пользователь сможет действовать. Для того, чтобы разрешить действовать от суперпользователя следует оставить эту вкладку незаполненной.



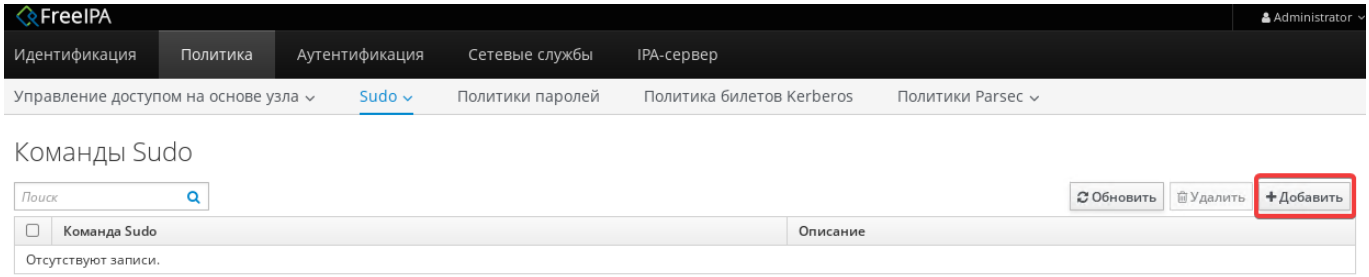
3.5.4.2. Через web-интерфейс FreeIPA

Создание команды

1. Открыть страницу «Политика > Sudo > Команды Sudo».

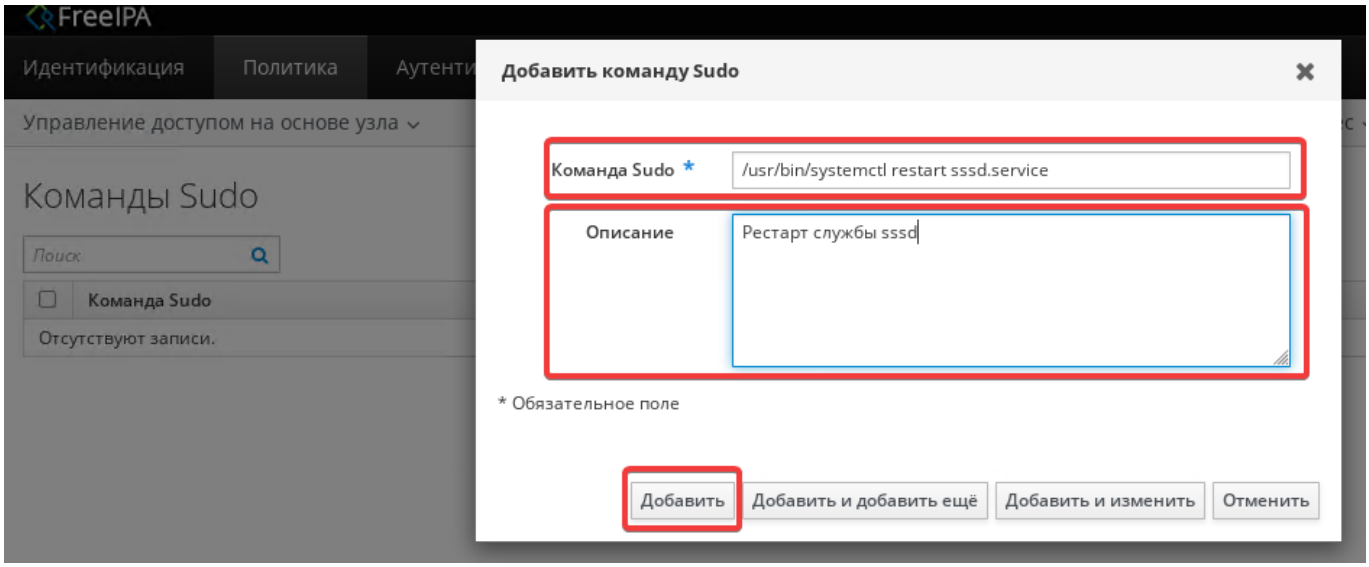


2. Нажать кнопку «+ Добавить».



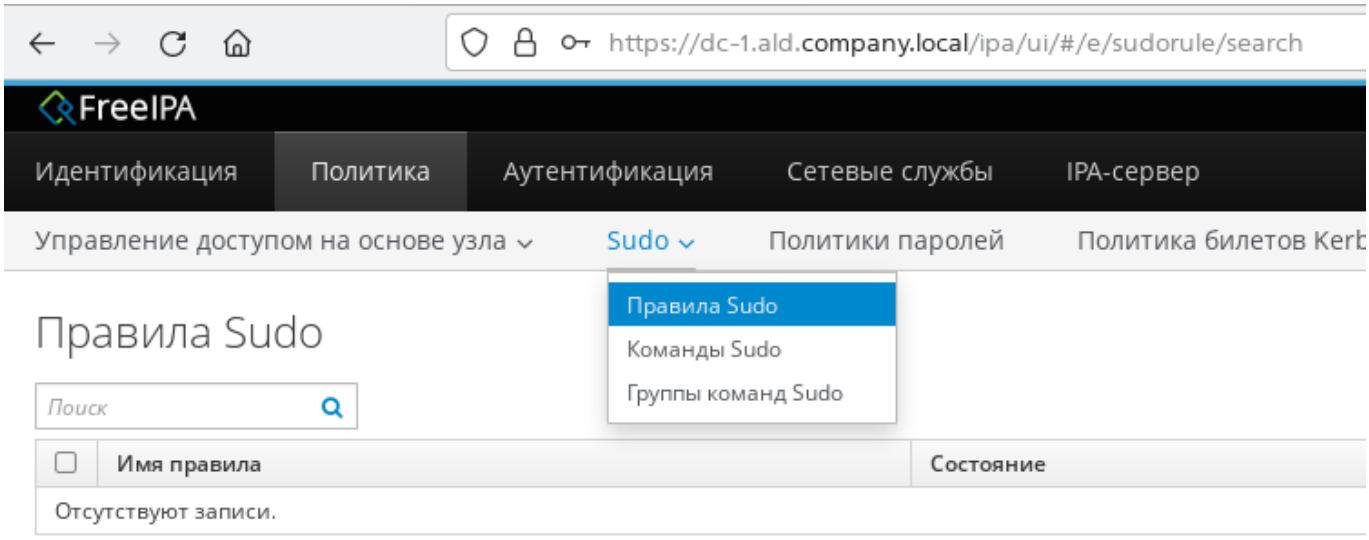
3. В открывшемся окне ввести команду `/usr/bin/systemctl restart sssd.service` и её описание, нажать кнопку «Добавить».

Примечание: В имени команды можно использовать `a-z`, `A-Z`, `0-9`, `-_./~`и пробелы (кроме первого и последнего).



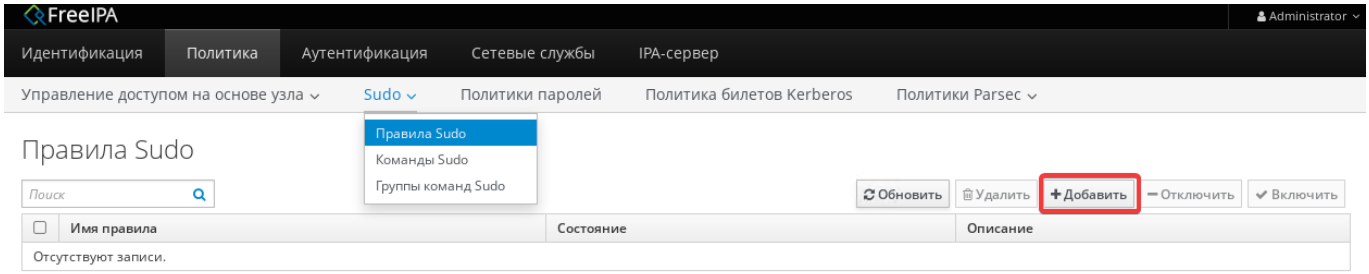
Создание правила

1. Открыть страницу «Веб-портал FreeIPA> Политика > Sudo > Правила Sudo».

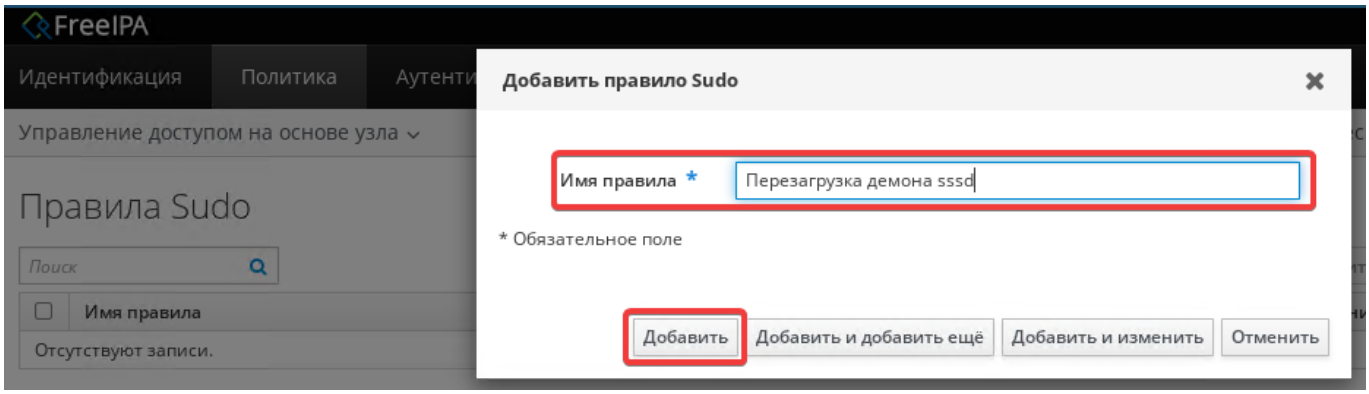


2. Нажать кнопку «+ Добавить».

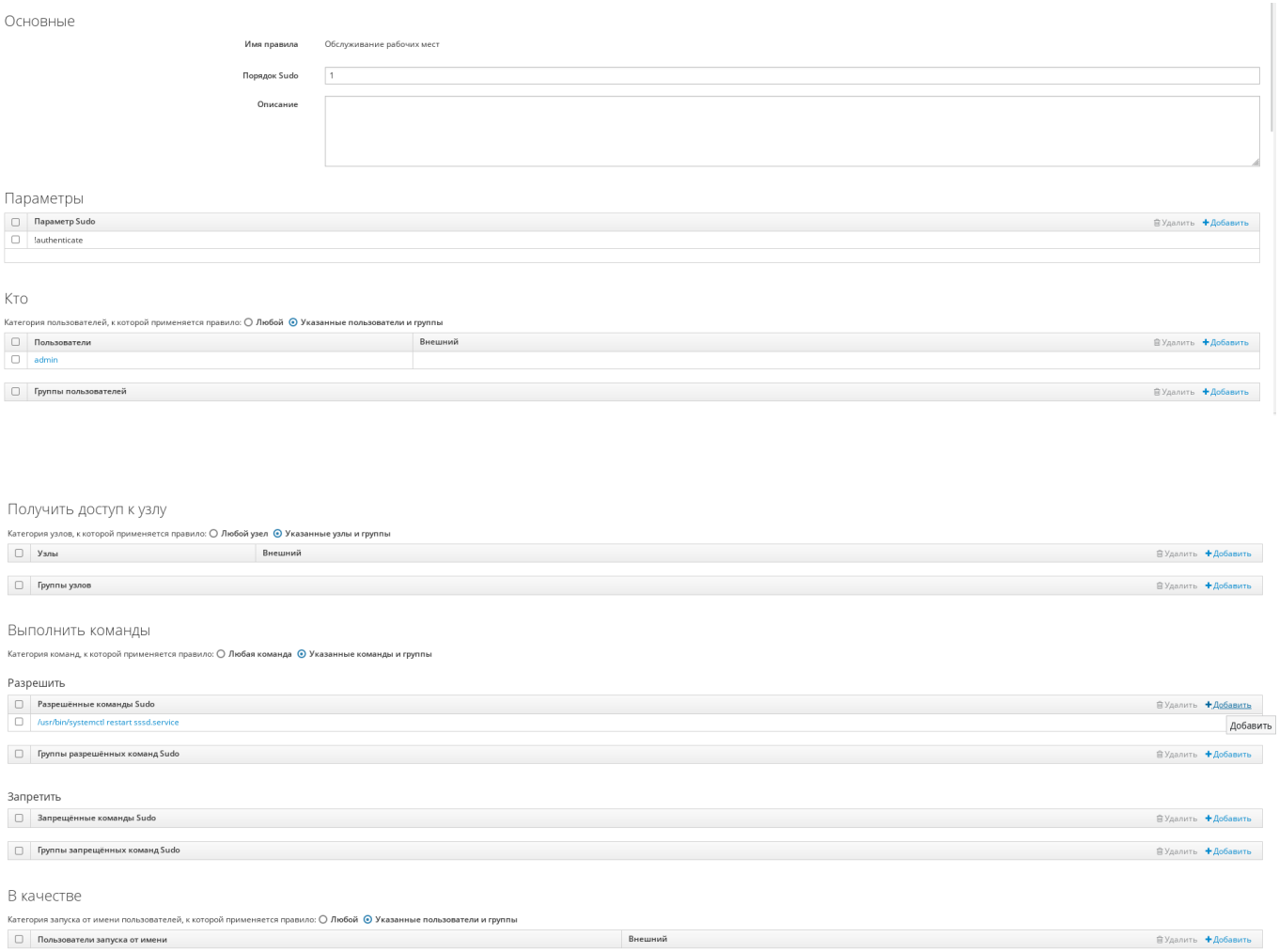
Важно: В имени правила можно использовать `a-z`, `A-Z`, `0-9`, `-_./~`.



3. В открывшемся окне ввести имя правила Sudo (обязательно) и нажать кнопку «Добавить».



4. Указать необходимые параметры.



3.5.4.3. Через терминал

Создание команды

Создать команду SUDO через терминал с помощью команды sudocmd-add:

```
ipa sudocmd-add '/etc/usr/systemctl restart sssd.service' --desc='sssd_daemon_
↪restart'
```

где:

- `sudocmd-add` - название команды, с помощью которой можно создать в системе новую команду sudo;

Примечание: В имени команды можно использовать `a-z`, `A-Z`, `0-9`, `-_./~`и пробелы

(кроме первого и последнего).

- `/etc/usr/systemctl restart sssd.service` - полный путь к утилите и разрешенные параметры вызова;
- desc – ключ, который позволяет задать описание команды “Рестарт службы sssd”;

Создание правила

1. Создать правило SUDO через терминал с помощью команды `sudorule-add`:

```
ipa sudorule-add 'sssd_daemon_restart'
```

где:

- sudorule-add – команда, с помощью которой можно создать новое правило sudo;
- `sssd_daemon_restart` – имя нового правила.

Примечание: В имени правила можно использовать `a-z`, `A-Z`, `0-9`, `-_`.

---

2. Добавить пользователя в правило:

```
ipa sudorule-add-user 'sssd_daemon_restart' --users crashtest
```

3. Добавить в правило целевые хосты:

```
ipa sudorule-add-host 'sssd_daemon_restart' --hosts client2
```

4. Добавить команду в правило:

```
ipa sudorule-add-allow-command 'sssd_daemon_restart' --sudocmds="/usr/bin/
↪systemctl restart sssd.service"
```

5. Проверить результат:

```
ipa sudorule-show 'sssd_daemon_restart'
```

3.5.5. Отладка правил SUDO

3.5.5.1. Список правил пользователя

Результирующий набор правил SUDO для конкретного пользователя можно узнать вызовом на целевой машине команды `sudo` с ключами -l и -U:

```
root@dc-1:~### sudo -l -U admin
Matching Defaults entries for admin on dc-1:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/
↪usr/sbin\:/usr/bin\:/sbin\:/bin,
    secure_path=/usr/lib/parsec/bin\:/usr/local/sbin\:/usr/local/bin\:/usr/
↪sbin\:/usr/bin\:/sbin\:/bin

User admin may run the following commands on dc-1:
    (ALL : ALL) ALL
    (root) ALL
```

3.5.5.2. Журнал отладки sudo

Для включения журналирования требуется создать файл `/etc/sudo.conf` со следующим содержимым:

```
Debug sudo /var/log/sudo_debug.log all@debug
Debug sudoers.so /var/log/sudo_debug.log all@debug
```

На контроллере домена редактирование этого файла заблокировано подсистемой мандатного контроля, см. `sudo astra-mic-control status`.

В файле `sudo_debug.log` будет представлена информация о пользователе и среде окружения в момент запуска команды *sudo*:

```
sudo[22259] settings: debug_flags=all@debug
sudo[22259] settings: run_shell=true
sudo[22259] settings: progname=sudo
sudo[22259] settings: network_addrs=192.0.2.1/255.255.255.0
↪fe80::250:56ff:feb9:7d6/ffff:ffff:ffff:ffff::
sudo[22259] user_info: user=user_name
sudo[22259] user_info: pid=22259
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
sudo[22259] user_info: ppid=22172
sudo[22259] user_info: pgid=22259
sudo[22259] user_info: tcpgid=22259
sudo[22259] user_info: sid=22172
sudo[22259] user_info: uid=10000
sudo[22259] user_info: euid=0
sudo[22259] user_info: gid=554801393
sudo[22259] user_info: egid=554801393
sudo[22259] user_info: groups=498,6004,6005,7001,106501,554800513,554801107,
↪554801108,554801393,554801503,554802131,554802244,554807670
sudo[22259] user_info: cwd=/
sudo[22259] user_info: tty=/dev/pts/1
sudo[22259] user_info: host=client
sudo[22259] user_info: lines=31
sudo[22259] user_info: cols=237
```

С помощью этой информации можно получить ответы на ряд вопросов.

Какой источник информации использовался для извлечения правил SUDO.

```
sudo[22259] <- sudo_parseln @ ./fileops.c:178 := sudoers: files sss
```

Со следующей строки включается в работу плагин SSSD.

```
udo[22259] <- sudo_sss_open @ ./sssd.c:305 := 0
```

Как много правил было получено от службы SSSD.

```
sudo[22259] Received 3 rule(s)
```

Подошли эти правила или нет.

```
sudo[22259] sssd/ldap sudoHost 'ALL' ... MATCH!
sudo[22259] <- user_in_group @ ./pwutil.c:1010 := false
```

3.5.5.3. Журнал отладки SSSD

Чтобы включить отладку SSSD в файле `/etc/sssd/sssd.conf` в секциях domain и sudo нужно установить параметр уровня отладки debug_level на значение 0x3ff0, что

соответствует восьмому уровню, который содержит достаточно информации для решения большинства проблем и включает флаги SSSDBG_FATAL_FAILURE, SSSDBG_CRIT_FAILURE, SSSDBG_OP_FAILURE, SSSDBG_MINOR_FAILURE, SSSDBG_CONF_SETTINGS, SSSDBG_FUNC_DATA, SSSDBG_TRACE_FUNC, SSSDBG_TRACE_LIBS, SSSDBG_TRACE_INTERNAL.

```
[domain/domain_name]
debug_level = 0x3ff0
...
[sudo]
debug_level = 0x3ff0
```

После внесения изменений для того, чтобы настройки вступили в силу, нужно выполнить перезапуск службы.

```
### systemctl restart sssd
```

При использовании утилиты `sudo` будет создан файл журнала `/var/log/sssd/sssd_domain_name.log` с помощью которого можно будет получить информацию по ряду вопросов.

Как много правил было получено от службы SSSD.

```
[sdap_sudo_refresh_load_done] (0x0400): Received 4-rules rules
```

Какие правила служба SSSD загрузила с сервера.

```
[sssd[be[LDAP.PB]]] [sysdb_save_sudorule] (0x0400): Adding sudo rule demo-
↪name
```

Находились ли подошедшие правила в кеше.

```
[sdap_sudo_refresh_load_done] (0x0400): Sudoers is successfully stored in
↪cache
```

Какой фильтр был использован для загрузки правил с сервера.

```
[sdap_get_generic_ext_step] (0x0400): calling ldap_search_ext with [(&
↪(objectClass=sudoRole)(|(!(sudoHost=*))(sudoHost=ALL)(sudoHost=client.
↪example.com)(sudoHost=client)(sudoHost=192.0.2.1)(sudoHost=192.0.2.0/
↪24)(sudoHost=2620:52:0:224e:21a:4aff:fe23:1394)(sudoHost=2620:52:0:224e::/
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
↪64)(sudoHost=fe80::21a:4aff:fe23:1394)(sudoHost=fe80::/
↪64)(sudoHost=+*)(|(sudoHost=*\\*)(sudoHost=*?*)(sudoHost=*\
↪2A*)(sudoHost=*[*]*))))][dc=example,dc=com]
```

Используйте этот фильтр, чтобы выполнить поиск в базе LDAP каталога напрямую:

```
### ldapsearch -x -D "cn=Directory Manager" -W -H ldap://server.example.com -
↪b dc=example,dc=com '(&(objectClass=sudoRole)...)'
```

Собеседник (Responder) службы SSSD регистрирует свои события в файле журнала `/var/log/sssd/sssd_sudo.log`, с помощью которого можно ответить на следующие вопросы.

Как много правил было получено от службы SSSD.

```
[sssd[sudo]] [sudosrv_get_sudorules_from_cache] (0x0400): Returning 4-rules
↪rules for [user@idm.example.com]
```

Какой фильтр был применен при поиске кеша SSSD.

```
[sudosrv_get_sudorules_query_cache] (0x0200): Searching sysdb with [(&
↪(objectClass=sudoRule)(|(sudoUser=ALL)(sudoUser=user)(sudoUser=
↪#10001)(sudoUser=%group-1)(sudoUser=%user)(sudoUser=+*)))]
```

Для поиска извлечения правил из кеша используйте команду ldbsearch из состава пакета ldb-tools:

```
### ldbsearch -H /var/lib/sss/db/cache_domain_name.ldb -b cn=sysdb '(&
↪(objectClass=sudoRule)...)'
```

3.5.6. Лучшие практики

3.5.6.1. Работа с локальными настройками sudo

Предполагается, что в файле sudoers должны быть заданы правила для локальных пользователей, а в LDAP-каталоге, соответственно, для управления привилегиями доменных пользователей, но использование двух источников одновременно может привести к очень неприятной коллизии.

Администратор с ограниченными правами, которому были делегированы полномочия только на управление объектами отдельного структурного подразделения, может создать в этом подразделении группу с именем sudo или astra-admin, включить себя в состав одной из этих групп и получить привилегии суперпользователя на всех компьютерах в домене, включая сервера, так как в файле `/etc/sudoers` на этих машинах по умолчанию содержатся соответствующие правила.

Чтобы избежать указанной проблемы можно воспользоваться одним из следующих способов:

1. Заранее создать на портале управления ALD Pro группы с именами astra-admin и sudo, чтобы администраторы с ограниченными правами не смогли создать такие группы в вверенных им подразделениях. Список зарезервированных имен можно расширить с учетом того, какие операционные системы используются в домене и какие на них настройки в файле `sudoers`.

2. Удалить источник files для базы `sudoers` из файла `/etc/nsswitch` . В этом случае при вызове утилиты sudo настройки из локального файла учитываться не будут, и пользователи групп `sudo` и astra-admin потеряют возможность повышать свои привилегии.

Для повышения безопасности по умолчанию с версии 2.0.0 слова sudo и astra-admin будут включены в список системных имен.

3.5.6.2. Особенности использования символов подстановки

Символ «звездочки» в правилах SUDO следует использовать крайне осторожно, так как ошибки в его использовании могут привести к предоставлению несанкционированного доступа.

Допустим, администратору нужно было предоставить сотруднику доступ на чтение журналов messages и он создал следующее правило:

```
localuser      ALL=(ALL:ALL) NOPASSWD :        /usr/bin/cat /var/log/
↪messages*
```

На первый взгляд все правильно, и пользователь сможет получить доступ к журналам:

```
localuser@astra:~$ cat /var/log/messages
localuser@astra:~$ cat /var/log/messages.1
```

Но утилита `cat` называется так от слова concatenate (сцеплять), и на самом деле она позволяет объединять в один поток содержимое сразу нескольких файлов, поэтому никто не помешает пользователю добавить к журналу messages содержимое файла shadow, чтобы увидеть пароли:

```
localuser@astra:~$ cat /var/log/messages /etc/shadow
...
localadmin:$gost12512hash$JQmInL3jM2ni7vs/$qVDReAiNXXpPDgQW1/
↪e26C7bAvRaMrwizV924KN4YYXDgPnYDlWqvpETfk29S9q7LKlxZeO7qA/.OcCO2XG3U/
↪:19296:0:99999:7:::
localuser:$gost12512hash$OEbYsS/bODT9ux.t
↪$0CY2yXvZTdZ3LO3cCfD7KI61DQiuOZ6bHEvzn3YXWZLjO.vcNU6pQQEz/hhWXHmuVCQbMHFWtl.
↪YmTdoctUZq.:19518:0:99999:7:::
...
```

Конкретно в этом случае для предотвращения нежелательного поведения утилиты sudo в шаблон следует добавить еще одну команду, которая будет запрещать вызов команды `cat` с пробелами в параметре:

```
localuser      ALL=(ALL:ALL) NOPASSWD :        /usr/bin/cat /var/log/
↪messages*, !/usr/bin/cat /var/log/messages* *
```

3.5.6.3. Запрет на использование редактора vi

Работая в приложении vi, пользователь может не только редактировать текст, но и запускать команды оболочки, что дает значительные преимущества. Например, если в процессе редактирования файла конфигурации потребуется ввести точный путь к какому-то сертификату, пользователь сможет выполнить команду :shell, чтобы провалиться в оболочку и стандартными командами cd и ls уточнить необходимую информацию, а затем командой exit вернуться к редактированию файла.

Вместе с тем, такая реализация утилиты делает крайне опасным использование этого редактора вместе с правилами SUDO. Допустим, администратору нужно было предоставить сотруднику право на редактирование файла `ldap.conf` и он создал следующее правило:

```
localuser      ALL=(ALL:ALL) NOPASSWD :        /usr/bin/vi /etc/ldap/ldap.
↪conf
```

На первый взгляд все правильно, и пользователь сможет получить право редактировать файл от имени суперпользователя. Но при этом ему ничто не помешает запустить из редактора оболочку и прочитать содержимое файла shadow.

```
localuser@dc-1:~$ sudo vi /etc/ldap/ldap.conf
...
### File modified by ipa-client-install
### We do not want to break your existing configuration, hence:
###   URI, BASE, TLS_CACERT and SASL_MECH
:shell
...
root@dc-1:/home/localuser### cat /etc/shadow
...
localadmin:$gost12512hash$JQmInL3jM2ni7vs/$qVDReAiNXXpPDgQW1/
 ↪e26C7bAvRaMrwizV924KN4YYXDgPnYDlWqvpETfk29S9q7LKlxZeO7qA/.OcCO2XG3U/
 ↪:19296:0:99999:7:::
localuser:$gost12512hash$OEbYsS/bODT9ux.t
 ↪$0CY2yXvZTdZ3LO3cCfD7KI61DQiuOZ6bHEvzn3YXWZLjO.vcNU6pQQEz/hhWXHmuVCQbMHFWtl.
 ↪YmTdoctUZq.:19518:0:99999:7:::
```

3.5.6.4. Использование группы пользователей, комментирование

Довольно простой рекомендацией является отказ от назначения прав на конкретных пользователей – используйте вместо этого группы. В этом случае и список правил будет короче, и за списками участников групп обычно удается лучше следить.

3.5.6.5. Принцип предоставления минимальных прав

При настройке правил SUDO следует предоставлять доступ только к тем командам, которые необходимы сотрудникам для выполнения должностных обязанностей. Чтобы избежать наличие излишних привилегий у пользователей крайне важно регулярно проводить аудит и отзывать те разрешения, которые более не требуются.

3.6. Инструкция по обеспечению безопасной работы в домене ALD Pro: политики паролей

Пароли являются самым простым, но при этом не самым безопасным способом аутентификации, поэтому в работе с паролями пользователи должны придерживаться определенных правил и политики паролей помогают гарантировать, что эти правила соблюдаются.

3.6.1. Пароли пользователей в домене

Пароль представляет из себя набор символов, который известен только самому пользователю и проверяющей стороне, поэтому, если пользователь может предъявить доказательство того, что пароль ему известен, это является подтверждением аутентичности пользователя, что он именно тот, за кого себя выдает.

В открытом виде пароли не хранят, в базу данных записывают хэши, и так как в домене ALD Pro (FreeIPA) используется сразу несколько разных механизмов аутентификации, у пользователей есть несколько хэшей:

- userPassword хранит PBKDF2-SHA256 хэш, который используется для обычной LDAP аутентификации, так называемой привязки (Bind). Во избежание перехвата пароля этот способ аутентификации рекомендуют использовать только с шифрованием траффика (LDAPS или LDAP+StartTLS).
- krbPrincipalKey хранит AES хэши, которые используются для аутентификации по протоколу Kerberos V5. Это наиболее рекомендуемый способ аутентификации с использованием паролей, т.к. он обеспечивает наибольший уровень безопасности.
- ipaNTHash хранит MD4 хэш, который используется для NTLM аутентификации. Этот механизм аутентификации необходим для интеграции с MS AD, простой аутентификации на файловом сервере при обращении к нему по IP адресу и интеграции с некоторыми другими внешними системами.

Для изменения пароля новое значение следует записать открытым текстом в атрибут userPassword, сервер автоматически сгенерирует все необходимые ключи и запишет в базу уже хэшированные значения. В силу такой особенности работы сервера записывать в каталог уже хэшированные значения запрещено. Обойти это ограничение можно только при создании новых пользователей, если сервер будет переведен в режим миграции.

3.6.2. Что такое политики паролей

Пароли, к сожалению, являются не самым безопасным механизмом аутентификации, так как их можно подобрать или перехватить, поэтому в работе с паролями необходимо следовать определенным правилам, или так называемым политикам, которые повышают уровень безопасности учетных записей в домене: пароли нужно периодически обновлять, использовать следует достаточно длинные комбинации, состоящие из разных категорий символов, и т.п.

Чем более строгие требования задает политика паролей, тем сложнее злоумышленнику подобрать пароль и воспользоваться результатами успешной атаки. Но, вместе с тем, и пользователям сложнее работать в таком домене, поэтому для разных групп пользователей следует устанавливать разные требования, обеспечивающий компромисс между удобством и безопасностью.

3.6.3. Механизм работы политик паролей

Механизм политик паролей в домене ALD Pro (FreeIPA) очень гибкий: для каждой группы пользователей можно создать свою собственную политику паролей. Список политик с их приоритетами хранится в контейнере с DN `cn=cosTemplates,cn=accounts,{base_dn}=ald,{base_dn}=company,{base_dn}=lan`, параметры политик вынесены отдельно в `cn=kerberos,{base_dn}=ald,{base_dn}=company,{base_dn}=lan`. Связь между записями осуществляется через значение атрибута krbPwdPolicyReference. При удалении группы пользователей все связанные с ней записи политики паролей удаляются автоматически.

Учитывая, что пользователь может входить сразу в несколько групп, алгоритм проверки выглядит следующим образом:

- Из «cn=cosTemplates, …» отбираются политики, под действие которых попадает текущий пользователь в соответствии с его участием в группах. Параметры политики берутся из «cn=kerberos, …» по ссылке из атрибута krbPwdPolicyReference.
- Если на пользователя не распространяется действие ни одной политики, ему будет назначена глобальная политика по умолчанию (global_policy).
- Если некоторый пользователь попадает под действие сразу нескольких политик, то выбирается одна из них, у которой будет наименьшее значение по приоритету, параметры политик не суммируются, см. Выбор политики в зависимости от приоритета.

Параметр	Политика для группы A (приоритет 0)	Политика для группы B (приоритет 1)	Результат (используются параметры для группы A)
Максимальный срок действия	60 дней	90 дней	60 дней
Минимальная длина	10 символов	0 (без ограничений)	10 символов

Выбор политики в зависимости от приоритета

Проверки паролей включают возможности MIT Kerberos, а также поддерживают набор некоторых дополнительных параметров, см. табл. 11 и табл. 12.

Параметр политики	Значение глобальной политики по умолчанию
Максимальный срок действия задает период в количестве дней, в течение которого система не будет требовать смены пароля	krbMaxPwdLife = 90 Пароль активен 90 дней, после чего пользователю будет предложено сменить его
Минимальный срок действия задает период в часах, в течение которого система будет запрещать повторную смену пароля	krbMinPwdLife = 1 После смены пароля, пользователь должен подождать 1 час перед повторной сменой
Размер журнала определяет количество предыдущих паролей, которые нельзя использовать повторно	krbPwdHistoryLength = 0 Запрет на повторное использование паролей не налагается

продолжение на следующей странице

Таблица 3.6 – продолжение с предыдущей страницы

Параметр политики	Значение глобальной политики по умолчанию
Классы символов – этот параметр указывает, сколько разных классов символов должно быть использовано в пароле. Все возможные символы подразделяются на следующие пять классов: цифры (ASCII), буквы нижнего регистра (ASCII), буквы верхнего регистра (ASCII), прочие символы ASCII, все остальные символы, не вошедшие ни в одну из предыдущих групп, например, €, ‰, Ğ, ¼, ¤ и т.д. Использование одного и того же символа более двух раз подряд уменьшает количество классов на один, например, у пароля «Secret11pwd» будет три класса (большие буквы + маленькие буквы + цифры), а у пароля «Secret111pwd» их станет два (минус штраф за повторы символа «1»). Если повторяющиеся символы окажутся в конце пароля, то последний из них не будет учитываться, поэтому на пароль «Secret111pwd» штраф налагаться не будет	krbPwdMinDiffChars = 0 Значение по умолчанию – 0. Это говорит об отсутствии каких либо требований к сложности пароля
Минимальная длина задает минимально допустимое количество символов в пароле	krbPwdMinLength = 8 Пользователь не может использовать пароль короче 8 символов
Максимальное количество ошибок определяет, сколько раз пользователь может неправильно ввести пароль, прежде чем его аккаунт будет временно заблокирован. Блокировка выполняется только на текущем контроллере, на другие сервера эта информация не передается	krbPwdMaxFailure = 6 Пользователь будет заблокирован после 7 неверно введенных паролей подряд

продолжение на следующей странице

Таблица 3.6 – продолжение с предыдущей страницы

Параметр политики	Значение глобальной политики по умолчанию
Интервал сброса ошибок задает период в секундах, по истечении которого счетчик неудачных попыток входа будет сброшен	krbPwdFailureCountInterval = 60 Если после 6 неудачных попыток введения пароля подряд пользователь подождет 1 минуту, у него будет еще 6 попыток до временной блокировки учетной записи
Длительность блокировки задает период в секундах, в течение которого пользователь не сможет выполнить аутентификацию в домене. Блокировка накладывается после превышения количества разрешенных неудачных попыток входа. Блокировка выполняется только на текущем контроллере, на другие сервера эта информация не передается	krbPwdLockoutDuration = 600 Заблокированный пользователь не сможет выполнить вход в систему в течение 10 минут

Таблица 11 — Параметры политик паролей. Проверки Kerberos

Параметр политики	Значение глобальной политики по умолчанию
Использовать список запрещённых слов - определяет необходимость проверки пароля по списку запрещённых слов: создание или изменение пароля будет завершаться ошибкой, если в составе любой подстроки нового пароля будет использовано любое слово из списка запрещённых. Актуальный список может быть найден в разделе Групповые политики - Политики паролей - Список запрещённых слов. Проверка не чувствительна к регистру	aldproBadWordsCheck = FALSE Проверка по списку запрещённых слов отключена (Подробнее об использовании списка запрещённых слов описано в разделе 6.6.5 Руководства администратора)

продолжение на следующей странице

Таблица 3.7 – продолжение с предыдущей страницы

Параметр политики	Значение глобальной политики по умолчанию
Минимум заглавных - задаёт минимальное количество заглавных символов в пароле	aldproUpCredit = 0 Значение по умолчанию – 0. Это говорит об отсутствии требования к наличию заглавных символов в пароле
Минимум строчных - задаёт минимальное количество строчных символов в пароле	aldproLowCredit = 0 Значение по умолчанию – 0. Это говорит об отсутствии требования к наличию строчных символов в пароле
Минимум цифр - задаёт минимальное количество цифр в пароле	aldproDigCredit = 0 Значение по умолчанию – 0. Это говорит об отсутствии требования к наличию цифр в пароле
Проверять совпадение с логином - создание или изменение пароля будет завершаться ошибкой, если в составе любой подстроки нового пароля будет использован логин пользователя. Проверка не чувствительна к регистру	ipaPwdUserCheck = FALSE Проверка на совпадение с логином отключена
Максимум повторений подряд - максимальное количество повторений подряд одинаковых символов которое может быть использовано в пароле. При подсчёте повторений подряд учитываются все символы кроме первого, т.е. в последовательности «ааа» всего два повторения	ipaPwdMaxRepeat = 0 Значение по умолчанию – 0. Это говорит об отсутствии требования к максимальному количеству повторений символов в пароле

продолжение на следующей странице

Таблица 3.7 – продолжение с предыдущей страницы

Параметр политики	Значение глобальной политики по умолчанию
Максимум монотонной последовательности - максимальное количество символов монотонной последовательности которое может быть использовано в пароле. Монотонной считается последовательность букв или цифр которые убывают либо возрастают по порядку, например: «ABCDEF» или «98765432». При определении максимума монотонной последовательности учитываются все символы кроме первого, т.е. в последовательности «АБВ» максимум равняется двум	ipaPwdMaxSequence = 0 Значение по умолчанию – 0. Это говорит об отсутствии требования к максимальной длине монотонной последовательности символов в пароле
Максимум одного класса подряд - задаёт максимальное количество повторений подряд символов одного класса которое может быть использовано в пароле. Проверка относит к разным классам заглавные и строчные символы не только из набора ASCII, а символы классов «прочие символы ASCII» и «остальные символы» относятся к одному классу. При подсчёте повторений подряд учитываются все символы кроме первого, т.е. в последовательности «ааа» всего два повторения	aldproMaxClassRepeat = 0 Значение по умолчанию – 0. Это говорит об отсутствии требования к максимальному количеству повторений символов одного класса в пароле

Таблица 12 — Параметры политик паролей. Дополнительные проверки

Также создание или изменение пароля всегда будет завершаться ошибкой несоответствия политике паролей, в случаях если:

- пароль является палиндромом;
- пароль содержит менее 6 символов.

При использовании различных сценариев установки/смены/сброса пароля текст ошибки

может отличаться.

Внимание: До версии ALD Pro 3.0.0 первый пароль, назначаемый администратором при создании учётной записи пользователя, считался временным, поэтому мог быть установлен в обход политики паролей, распространяющей своё действие на пользователя. По такой же логике происходил сброс пароля пользователя администратором. Начиная с версии 3.0.0 пароли, устанавливаемые администраторами, проходят обязательную проверку на соответствие политике паролей. Исключения составляют:

1. Смена пароля пользователя от имени суперпользователя LDAP-каталога *cn=Directory Manager*;
2. Смена пароля пользователя от имени root-пользователя командой ipa-getkeytab с ключом -p;
3. Создание/сброс пароля пользователя от имени пользователя, который является членом группы «passSyncManagersDNs» (соответствующий атрибут имеет конфигурационный файл плагина 389ds - ipa_pwd_extop);
4. Настройка «Минимальный срок действия» политики не учитывается при сбросе пароля пользователем, имеющим необходимые привилегии.

Сценарий	Текст ошибки
Установка/смена/сброс пароля на портале управления ALD Pro	Пароль не соответствует требованиям политики
Сброс пароля пользователю от имени привилегированной УЗ или смена пользователем своего пароля с помощью ipa passwd	В зависимости от типа проверки, которая была провалена возможны варианты: • ipa: ERROR Constraint violation: Failed to update password • ipa: ERROR Constraint violation: <текст сообщения>

продолжение на следующей странице

Таблица 3.8 – продолжение с предыдущей страницы

Сценарий	Текст ошибки
Сброс пароля пользователю от имени привилегированной УЗ с помощью ipa user-mod с ключом –password	В зависимости от типа проверки, которая была провалена возможны варианты: • ipa: ERROR Constraint violation: Failed to update password • ipa: ERROR Constraint violation: <текст сообщения>
Смена пользователем пароля с использованием kpasswd	В зависимости от типа проверки, которая была провалена возможны варианты: • Server error: Password not changed. Kerberos database constraints violated while trying to change password; • Password change rejected: <текст сообщения>
Смена пользователем пароля (если срок действия текущего пароля истёк) с использованием kinit	В зависимости от типа проверки, которая была провалена возможны варианты: • kinit: Password change failed while getting initial credentials • Password change rejected: <текст сообщения> Password not changed.. Please try again
Сброс пароля пользователю от имени привилегированной УЗ с помощью ldapmodify (с явным указанием атрибута userPassword)	ldap_modify: Constraint violation (19) additional info: <текст сообщения>
Сброс пароля пользователю от имени привилегированной УЗ с помощью ldappasswd	Result: Constraint violation (19) Additional info: Failed to update password

продолжение на следующей странице

Таблица 3.8 – продолжение с предыдущей страницы

Сценарий	Текст ошибки
Смена пользователем пароля (если срок действия текущего пароля истёк) с использованием fly-dm_greet	В зависимости от типа проверки, которая была провалена возможны варианты: • Не удалось сменить пароль. Сообщение сервера: Kerberos database constraints violated while trying to change password • Не удалось сменить пароль. Сообщение сервера:<текст сообщения> Password not changed
Сброс пароля пользователю от имени привилегированной УЗ с помощью расширенной ldap-операции (Password Modify)	Error while executing extended operation - [LDAP result code 19 - constraintViolation] Failed to update password
Смена пользователем пароля с использованием fly-passwd	В зависимости от типа проверки, которая была провалена возможны варианты: • Ваш пароль не изменён. Password change failed. Server message: <текст сообщения> • Ваш пароль не изменён. Password change failed. Server message: Password not changed. Kerberos database constraints violated while trying to change password
Смена пользователем пароля (если срок действия текущего пароля истёк) при попытке установки ssh-подключения	В зависимости от типа проверки, которая была провалена возможны варианты: • Password change failed. Server message: Password not changed. Kerberos database constraints violated while trying to change password • Server message: <текст сообщения>

Таблица 13 — Возможные варианты ошибок при попытке установить пароль, не

соответствующий политике

3.6.4. Создание политики паролей

3.6.4.1. Через портал управления

Откройте страницу «Групповые политики → Политики паролей» и нажмите кнопку «+ Создать». Заполните обязательные поля «Группа пользователей», «Приоритет» и нажмите кнопку «Сохранить».

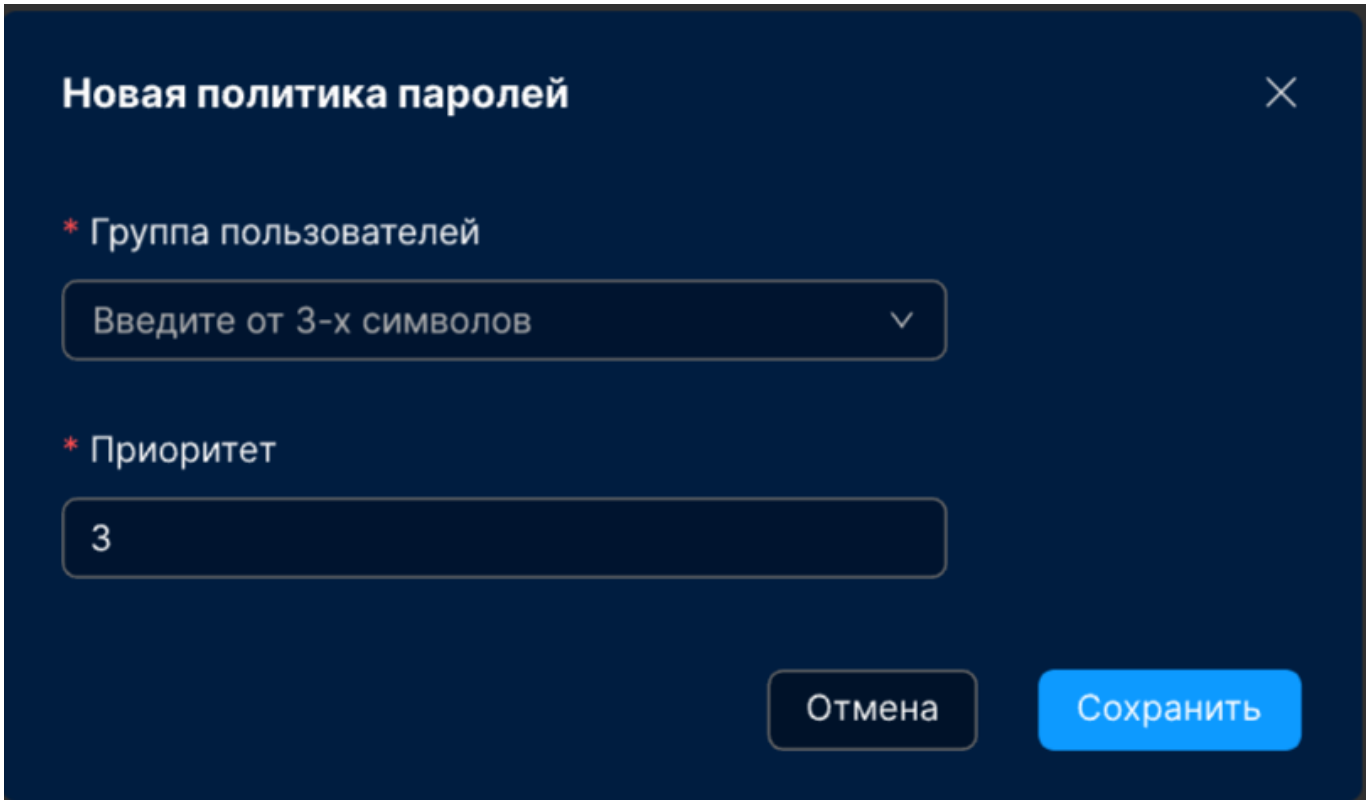


Рисунок 3.50 – Создание политики паролей

Далее вам станет доступна страница управления политикой, где вы можете задать необходимые настройки.

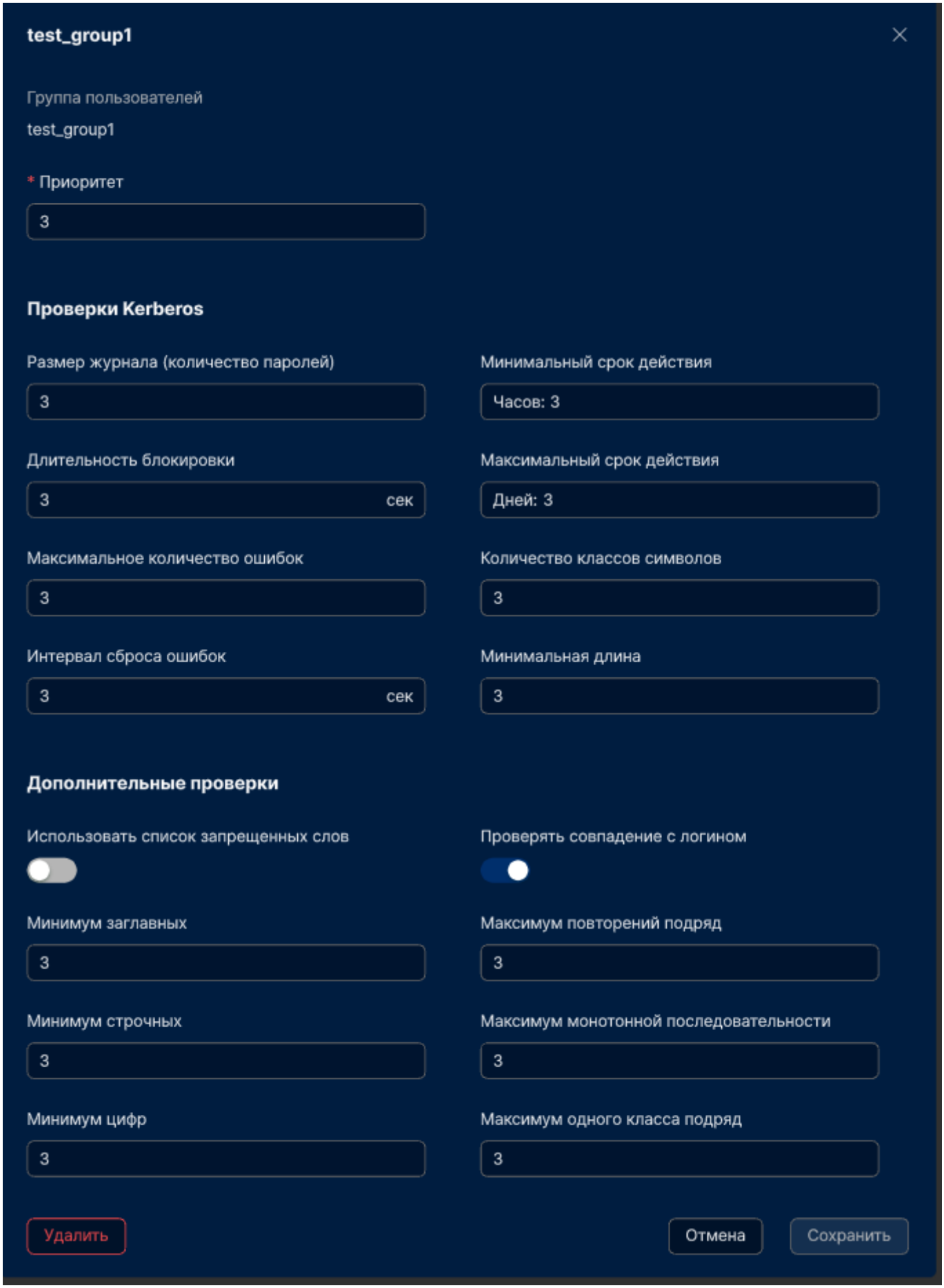


Рисунок 3.51 – Настройка политики паролей

3.6.4.2. Из командной строки

Внимание: При переходе с ранних версий ALD Pro на версию 3.0.0 схема данных расширена двумя новыми классами aldpro-pwd-policy и ipaPwdPolicy, позволяющими настраивать дополнительные параметры политик. Если политика уже существовала, необходимые атрибуты будут добавлены автоматически, однако для избежания ошибок при создании новой политики с помощью командной строки необходимо сперва добавить новые классы.

Для этого воспользуйтесь ключом –addattr команды pwpolicy-add, который также используется при добавлении атрибутов, соответствующих дополнительным проверкам. При использовании ключа –addattr его аргумент передаётся в формате «атрибут=значение».

```
$ ipa pwpolicy-add admins --priority=0 --addattr="objectClass=aldpro-pwd-
↪policy" --addattr="objectClass=ipaPwdPolicy" --addattr="ipaPwdMaxRepeat=3" -
↪-addattr="ipaPwdMaxSequence=3" --addattr="aldproBadWordsCheck=TRUE" --
↪addattr="ipaPwdUserCheck=TRUE" --addattr="aldproDigCredit=2" --addattr=
↪"aldproUpCredit=2" --addattr="aldproLowCredit=2" --addattr=
↪"aldproMaxClassRepeat=5" --maxlife=45 --minlife=0 --history=12 --
↪minclasses=5 --minlength=12 --maxfail=3 --failinterval=120 --
↪lockouttime=1200
  Группа: admins
  Максимальный срок действия (в днях): 45
  Минимальный срок действия (в часах): 0
  Размер журнала : 12
  Классы символов: 5
  Минимальная длина: 12
  Приоритет: 0
  Максимальное количество ошибок: 3
  Интервал сброса ошибок: 120
  Длительность блокировки: 1200
```

где:

–maxlife= - Максимальный срок действия в днях;

–minlife= - Минимальный срок действия в часах;

–history= - Размер журнала;

–minclasses= - Классы символов;

–minlength= - Минимальная длина;

–priority= - Приоритет политики;

–maxfail= - Максимальное количество ошибок;

–failinterval= - Интервал сброса ошибок в секундах;

–lockouttime= - Длительность блокировки в секундах.

Чтобы изменить параметры kerberos уже существующей политики, воспользуйтесь командой ipa pwpolicy-mod:

```
$ ipa pwpolicy-mod admins --maxlife=30
  Группа: admins
  Максимальный срок действия (в днях): 30
  Минимальный срок действия (в часах): 0
  Размер журнала : 12
  Классы символов: 5
  Минимальная длина: 12
  Приоритет: 0
  Максимальное количество ошибок: 3
  Интервал сброса ошибок: 120
  Длительность блокировки: 1200
```

Для изменения дополнительных параметров воспользуйтесь ключом –setattr команды pwpolicy-mod. При использовании ключа –setattr его аргумент передаётся в формате «атрибут=значение».

```
$ ipa pwpolicy-mod admins --setattr="aldproMaxClassRepeat=2"
```

Следует учитывать, что срок действия пароля проверяется не по значению maxlife в политике, а по значению атрибута krbPasswordExpiration, которое устанавливается пользователю при изменении пароля, поэтому изменение параметра в политике сразу ни на что не повлияет. Чтобы принудительно изменить пользователю значение атрибута krbPasswordExpiration вы можете воспользоваться командой `user-mod`:

```
$ ipa user-mod admin --password-expiration 20230528010101Z
----------------------------
Изменён пользователь "admin"
----------------------------
  Имя учётной записи пользователя: admin
  Фамилия: Administrator
  Домашний каталог: /home/admin
  Оболочка входа: /bin/bash
  Псевдоним учётной записи: admin@ALD.COMPANY.LAN, root@ALD.COMPANY.LAN
  Окончание действия пароля пользователя: 20230528010101Z
  UID: 959800000
  ID группы: 959800000
  Учётная запись отключена: False
  Link to department: ou=ald.company.lan,cn=orgunits,cn=accounts,{base_dn}
↪=ald,{base_dn}=company,{base_dn}=lan
  Пароль: True
  Участник групп: trust admins, lpadmin, admins
  Роли: ALDPRO - Main Administrator
  Доступные ключи Kerberos: True
```

Срок действия пароля задается в формате временной метки, где:

- 2023 – год;
- 05 – месяц;
- 28 – день месяца;
- 010101 – часы, минуты, секунды;
- Z – часовой пояс. Точность до секунд не имеет большого значения, поэтому обычно используют время по нулевому (Zero) меридиану.

Проверить текущее значение можно командой user-show

```
$ ipa user-show admin --raw --all | grep krbPasswordExpiration
  krbPasswordExpiration: 20230528010101Z
```

3.6.5. Список запрещённых слов

Список запрещённых слов является одной из функций политик паролей (подробно описана в Руководство Администратора. Часть 2 → Портал управления. Настройка и работа → Групповые политики → Политики паролей → Список запрещённых слов).

При создании или изменении пароля пользователя функция выполняет проверку вхождения слов списка в состав любой подстроки текста пароля. «Подстрокой» считается непустая связанная часть строки.

Если вхождение запрещённого слова в состав пароля обнаружено - такой пароль не пройдёт проверку на соответствие политике. Проверка вхождения игнорирует регистр символов и запрещённые слова короче четырёх символов.

Список запрещённых слов одинаков для всей системы, при этом включение и отключение функции проверки паролей по списку индивидуально настраивается в карточке политики паролей с помощью переключателя «Использовать список запрещённых слов».

При нахождении в списке 1000 слов длиной 8 символов производительность функции проверки пароля по списку запрещённых слов составляет около 100 операций в секунду (проверка выполнялась на 20 тысячах одновременных операций смены пароля). Производительность зависит от количества одновременных операций и может уменьшаться при росте их числа.

Просмотр и управление списком осуществляются на странице «Групповые политики > Политики паролей > Список запрещённых слов».

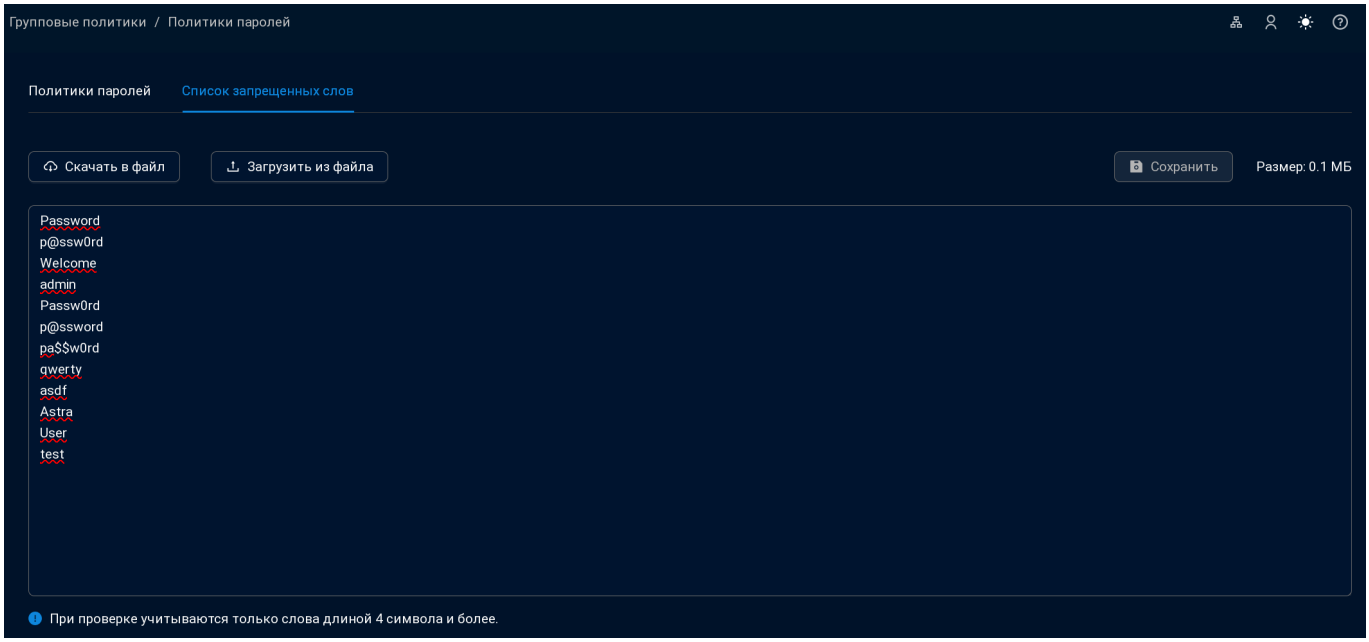


Рисунок 3.52 – Список запрещённых слов

Список хранится в виде строки в реплицируемом атрибуте aldproBadWords, который хранится в контейнере с DN cn=<область Керберос>,cn=kerberos,<доменный_суффикс> и по умолчанию содержит несколько распространённых паролей, но может быть просмотрен и изменён при наличии необходимых привилегий.

Привилегия	Описание	На что распростра-няется
Password Policies - Read	Предоставляемые права на: • просмотр списка политик паролей; • просмотр карточек политик паролей; • просмотр списка запрещенных слов	На весь домен
Password Policies - Modify	Предоставляемые права на: • изменение настроек политик паролей системы; • редактирование списка запрещенных слов	На весь домен

Таблица 14 — Привилегии для работы со списком запрещённых слов.

Также доступен функционал скачивания списка в локальный файл и загрузки списка из

текстового файла, подготовленного заранее локально. Файл должен содержать слова, разделённые как минимум одним пробельным символом, а его размер не должен превышать 2 Мб. Рекомендуется использовать файлы в кодировке UTF-8, форматов .odt, .txt, .rtf, .doc, .docx.

Из командной строки возможна полная замена списка с помощью утилиты ldapmodify из пакета ldap-utils (См. Руководство администратора. Часть 2 → Справочные материалы → Автоматизация задач администрирования через LDAP-запросы → Взаимодействие с каталогом через LDAP-протокол → Утилиты для работы с LDAP-каталогом → Модификация записей в каталоге через ldapmodify).

Для этого выполните следующие действия:

1. Ввести команду на подключение к каталогу и нажать клавишу Enter:

```
ldapmodify -Y GSSAPI -H ldap://dc-1.ald.company.lan:389
```

2. В интерактивном режиме ввести DN целевого контейнера, в котором хранится атрибут aldproBadWords:

```
dn: cn=ALD.COMPANY.LAN,cn=kerberos,dc=ald,dc=company,dc=lan
```

3. В интерактивном режиме ввести и нажать Enter:

```
changetype: modify
```

4. В интерактивном режиме ввести и нажать Enter:

```
replace: aldproBadWords
```

5. В интерактивном режиме ввести и нажать Enter (после знака «:» слова для добавления в список запрещённых вводятся через пробел):

```
aldproBadWords: Welcome admin Passw0rd
```

6. Нажать Enter ещё раз.

7. Завершить подключение:

```
Ctrl+C
```

3.7. Доверительные отношения

3.7.1. Модуль доверия между доменами ALD Pro

3.7.1.1. Особенности установки при использовании Astra Linux версии 1.7.6 и выше

При использовании **Astra Linux** версией 1.7.6 и выше установка дополнительных пакетов не требуется, так как реализация доверительных отношений **ALD Pro** встроена в пакеты системы.

Чтобы настроить модуль **Доверие между доменами ALD Pro**, необходимо:

1. На контроллере домена нужно установить пакет `libipa-aldpro` командами:

```
sudo apt update
sudo apt install libipa-aldpro
```

2. В файл `/usr/share/aldpro/updates/92-aldpro-extdom-extop-plugin.update` нужно добавить следующие строки для расширения схемы каталога:

```
dn: cn=ipa_extdom_extop,cn=plugins,cn=config
only:changetype: add
only:objectclass: top
only:objectclass: nsSlapdPlugin
only:objectclass: extensibleObject
only:cn: ipa_extdom_extop
only:nsslapd-pluginpath: libaldpro_extdom_extop
only:nsslapd-plugininitfunc: ipa_extdom_init
only:nsslapd-plugintype: extendedop
only:nsslapd-pluginenabled: on
only:nsslapd-pluginid: ipa_extdom_extop
only:nsslapd-pluginversion: 1.0
only:nsslapd-pluginvendor: AstraLinux
only:nsslapd-plugindescription: Support resolving IDs in trusted domains to
 ↪names and back
only:nsslapd-plugin-depends-on-type: database
only:nsslapd-basedn: $SUFFIX
```

3. Выполнить обновление схемы каталога и перезапустить службы следующими

командами:

```
sudo ipa-ldap-updater /usr/share/aldpro/updates/92-aldpro-extdom-extop-plugin.
 ↪update
sudo net conf setparm global "passdb backend" "aldprosam:ldapi://%2fvar%2frun
 ↪%2fslapd-$(hostname -d | sed 's/\./-/g; s/.*/\U&/').socket"
sudo aldproctl restart
```

Полный перечень обновляемых пакетов:

- libipa-hbac-dev
- libipa-hbac0
- libnss-sss
- libpam-sss
- libsss-certmap-dev
- libsss-certmap0
- libsss-idmap-dev
- libsss-idmap0
- libsss-nss-idmap-dev
- libsss-nss-idmap0
- libsss-simpleifp-dev
- libsss-simpleifp0
- libsss-sudo
- libwbclient-sssd
- libwbclient-sssd-dev
- python3-libipa-hbac
- python3-libsss-nss-idmap
- python3-sss
- sssd
- sssd-ad
- sssd-ad-common
- sssd-common
- sssd-dbus
- sssd-ipa

- sssd-kcm
- sssd-krb5
- sssd-krb5-common
- sssd-ldap
- sssd-proxy
- sssd-tools

3.7.1.2. Установка при использовании Astra Linux версии ниже 1.7.6

Если планируется устанавливать доверительные отношения между доменами ALD Pro, необходимо установить модуль доверия между доменами ALD Pro.

Для установки доверительных отношений между доменами ALD Pro предъявляются следующие технические требования:

1. Установку пакетов и выполнение инструкций по настройке модуля доверия необходимо выполнять на обоих контроллерах домена, между которыми настраивается доверие.
2. Установку необходимо выполнять от имени учетной записи администратора системы с высоким уровнем целостности.
3. На обоих контроллерах домена должно быть установлено обновление ALD Pro 2.5.0.

> **Внимание:** При установке модуля доверия между доменами ALD Pro для компонентов SSSD будет выполнено понижение версий (даунгрейд) до 2.5.0-1astra.se8-aldpro1 из состава срочного оперативного обновления операционной системы Astra Linux Special Edition 1.7.3.UU.2.

Порядок установки модуля на контроллерах домена ALD Pro:

1. Подключить репозиторий, содержащий необходимые для функционирования модуля обновления:
    - Примонтировать iso-образ *ALDPro-2.5.0-trust.iso*, выполнив команду:

```
sudo mkdir /mnt/aldpro_2.5.0_trust
sudo mount -o loop /distr/ALDPro-2.5.0-trust.iso /mnt/aldpro_2.5.0_trust

Где:

   - ``mount`` -- утилита обеспечивает монтирование файловой системы;

   - ``-o loop`` -- ключ позволяет связать свободное петлевое устройство (/
↪dev/loopN) с указанным iso-образом;

   - ``/distr/ALDPro-2.5.0-trust.iso`` -- параметр определяет абсолютный
↪путь к iso-образу;

   - ``/mnt/aldpro_2.5.0_trust`` -- параметр определяет точку монтирования.

* Создать файл ``/etc/apt/sources.list.d/trust.list`` со следующим
↪содержимым:

.. code-block:: console

   deb file:///media/cdrom 2.5.0 aldpro
```

1. Добавить в файл */etc/apt/preferences.d/aldpro* следующее содержимое:

```
Package: *
Pin: release n=2.5.0
Pin-Priority: 1000
```

3. Выполнить команды:

```
sudo apt update
sudo apt dist-upgrade
sudo apt install libipa-aldpro
```

4. Добавить в файл */usr/share/aldpro/updates/92-aldpro-extdom-extop-plugin.update*:

```
dn: cn=ipa_extdom_extop,cn=plugins,cn=config
only:changetype: add
only:objectclass: top
only:objectclass: nsSlapdPlugin
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
only:objectclass: extensibleObject
only:cn: ipa_extdom_extop
only:nsslapd-pluginpath: libaldpro_extdom_extop
only:nsslapd-plugininitfunc: ipa_extdom_init
only:nsslapd-plugintype: extendedop
only:nsslapd-pluginenabled: on
only:nsslapd-pluginid: ipa_extdom_extop
only:nsslapd-pluginversion: 1.0
only:nsslapd-pluginvendor: AstraLinux
only:nsslapd-plugindescription: Support resolving IDs in trusted domains to
 ↪names and back
only:nsslapd-plugin-depends-on-type: database
only:nsslapd-basedn: $SUFFIX
```

5. **Последовательно** выполнить команды, каждую **после завершения** предыдущей:

```
sudo ipa-ldap-updater /usr/share/aldpro/updates/92-aldpro-extdom-extop-plugin.
 ↪update

sudo net conf setparm global "passdb backend" "aldprosam:ldapi://%2fvar%2frun
 ↪%2fslapd-$(hostname -d | sed 's/\./-/g; s/.*/\U&/').socket"

sudo ipactl restart
```

Для автоматизации процесса установки модуля «Доверие между доменами ALD Pro» на **клиентах** домена ALD Pro рекомендуется создать репозиторий из ISO-образа *ALDPro-2.5.0-trust.iso* и с помощью задания автоматизации произвести установку модуля.

Описание процесса создания репозитория из ISO-образа приведено в *Создание репозиториев из ISO образа*. Описание порядка создания и запуска заданий автоматизации приведено в Справочном центре ALD Pro.

Порядок установки модуля на **Клиентах** ALD Pro:

> **Внимание:** Следующие действия актуальны при использовании ОС Astra Linux версией ниже 1.7.6. Если на клиентах установлена ОС Astra Linux версии 1.7.6, см. os_1_7_6.

1. Подключить репозиторий, содержащий необходимые для функционирования модуля обновления:

   - Примонтировать ISO-образ *ALDPro-2.5.0-trust.iso*, выполнив команду:

```
sudo mkdir /mnt/ald_pro_2.5.0_trust
sudo mount -o loop /distr/ALDPro-2.5.0-trust.iso /mnt/ald_pro_2.5.0_trust
```

   Где:

   - `mount` – утилита обеспечивает монтирование файловой системы;
   - `-o loop` – ключ позволяет связать свободное петлевое устройство (/dev/loopN) с указанным iso-образом;
   - `/distr/ALDPro-2.5.0-trust.iso` – параметр определяет абсолютный путь к iso-образу;
   - `/mnt/ald_pro_2.5.0_trust` – параметр определяет точку монтирования.

   - Создать файл `/etc/apt/sources.list.d/aldpro_trust.list` со следующим содержимым:

```
deb file:///mnt/ald_pro_2.5.0_trust 2.5.0 aldpro
```

2. Добавить в файл `/etc/apt/preferences.d/aldpro` следующее содержимое для настройки приоритетов:

```
Package: *
Pin: release n=2.5.0
Pin-Priority: 1000
```

3. Выполнить команды:

```
sudo apt update
sudo apt dist-upgrade
```

3.8. Инструкция по установке доверительных отношений между Microsoft Active Directory и ALD Pro

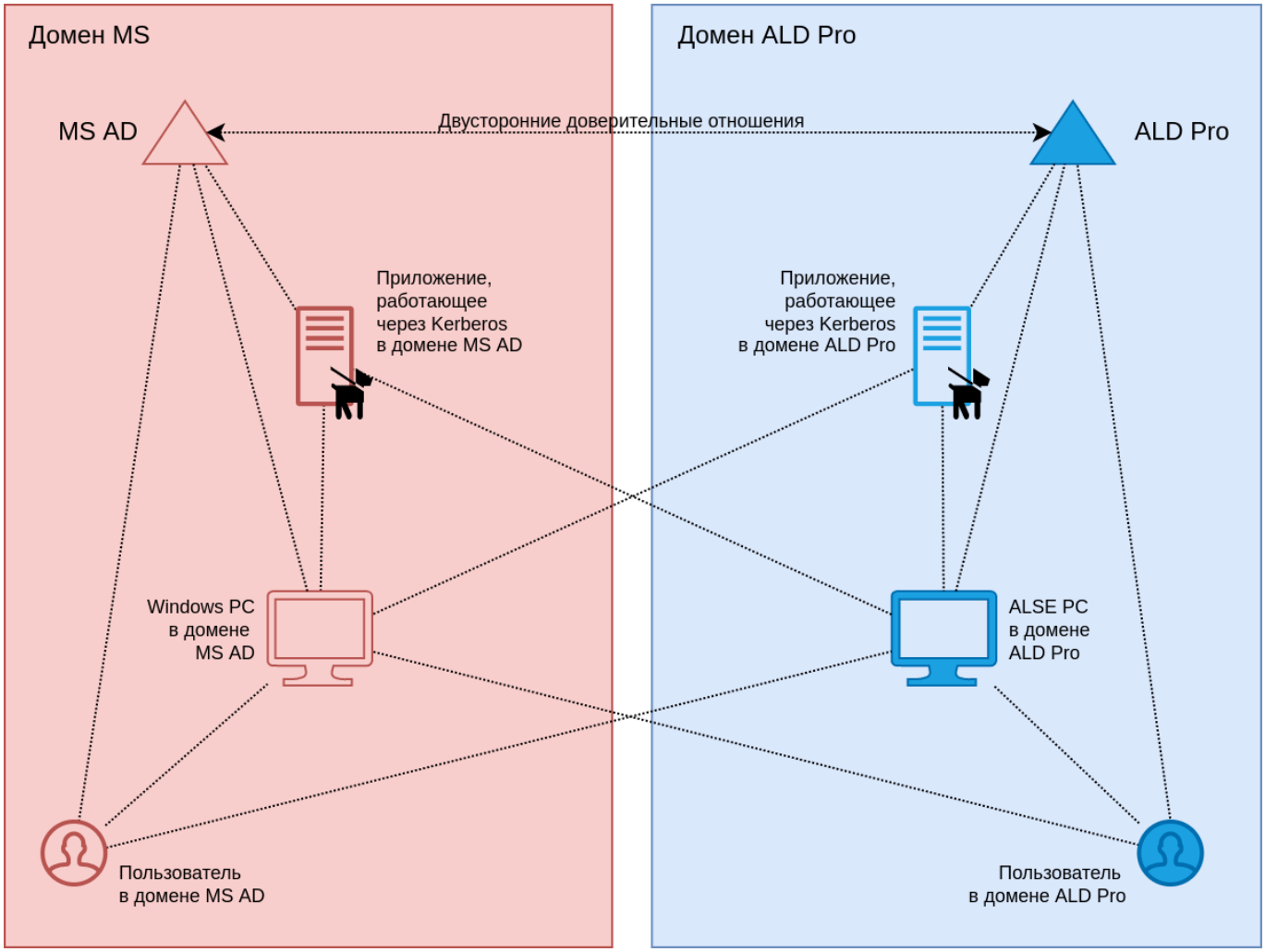
В настоящей инструкции представлены рекомендации по настройке доверительных отношений между доменами ALD Pro и Microsoft Active Directory (далее по тексту MS AD), которые позволяют пользователям одного домена проходить прозрачную аутентификацию на контроллерах другого домена. Эти возможности актуальны в переходный период, когда часть пользователей и сервисов работают уже в новом домене, а часть остаются в старом.

Подготовленная VM windc01 –для домена windomain.lan (Win2019)

Подготовленная VM alddc01 –для домена alddomain.lan (ALD Pro 2.1.0)

3.8.1. Постановка задачи

Ранее организация работала в домене MS AD (**windomain.lan**) и в рамках миграции был развернут домен ALD Pro (**alddomain.lan**). В соответствии с составленным планом предполагается постепенный перевод сервисов и пользователей на работу в новом домене, поэтому необходимо в течение некоторого времени обеспечить гибридную работу пользователей сразу в двух доменах с помощью механизма доверительных отношений.



Данные отношения называются «доверительными» (Domain Trust), т. к. контроллеры доверяющего домена напрямую не аутентифицируют пользователей доверенного домена, а только принимают доказательство об успешной аутентификации этих пользователей от контроллеров из доверенного домена. Невозможность выполнить аутентификацию напрямую объясняется тем, что у доверяющего домена просто нет учетных данных пользователей из доверенного домена.

Порядок работы аутентификации с использованием доверительных отношений (Domain Trust):

1. Пользователю доверенного домена ALD Pro нужно пройти аутентификацию в службе из доверяющего домена MS AD.

2. Пользователь ALD Pro успешно проходит аутентификацию на контроллере ALD Pro и получает от него TGT билет.

3. Пользователь ALD Pro обращается к своему контроллеру за сервисным билетом к службе из доверяющего домена MS AD. Контроллер ALD Pro видит, что служба

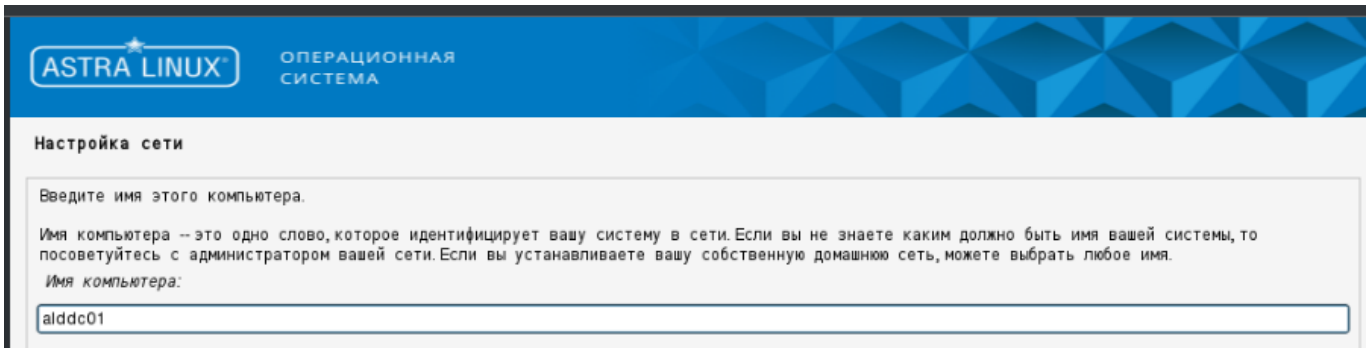
находится в доверяющем домене MS AD, поэтому выписывает билет на выполнение рекурсивного Kerberos запроса к контроллеру из доверяющего домена MS AD. Билет зашифрован паролем служебной учетной записи, соответствующей доверительному отношению. Таким образом, пользователь получает своего рода сервисный билет на доступ к службе распространения ключей доверяющего домена (Key Distribution Center, KDC).

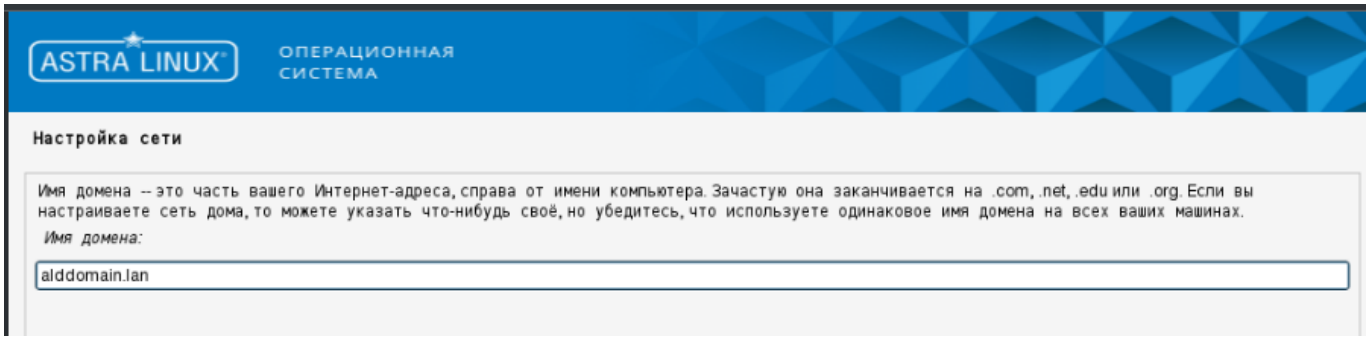
4. Пользователь ALD Pro обращается с полученным билетом к контроллеру доверяющего MS AD, совершая рекурсивный Керберос запрос. Контроллер MS AD расшифровывает билет, используя пароль учетной записи, соответствующей доверительному отношению, и, доверяя контроллеру ALD Pro, что тот выполнил проверку аутентичности пользователя должным образом, выписывает пользователю сервисный билет на доступ к своей службе.

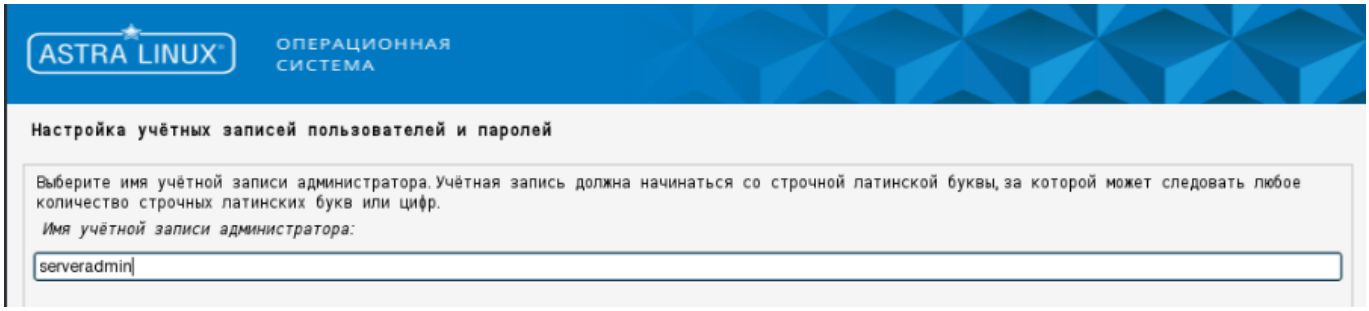
5. Клиент идет к службе из домена MS AD, используя сервисный билет, полученный от контроллера из этого же домена.

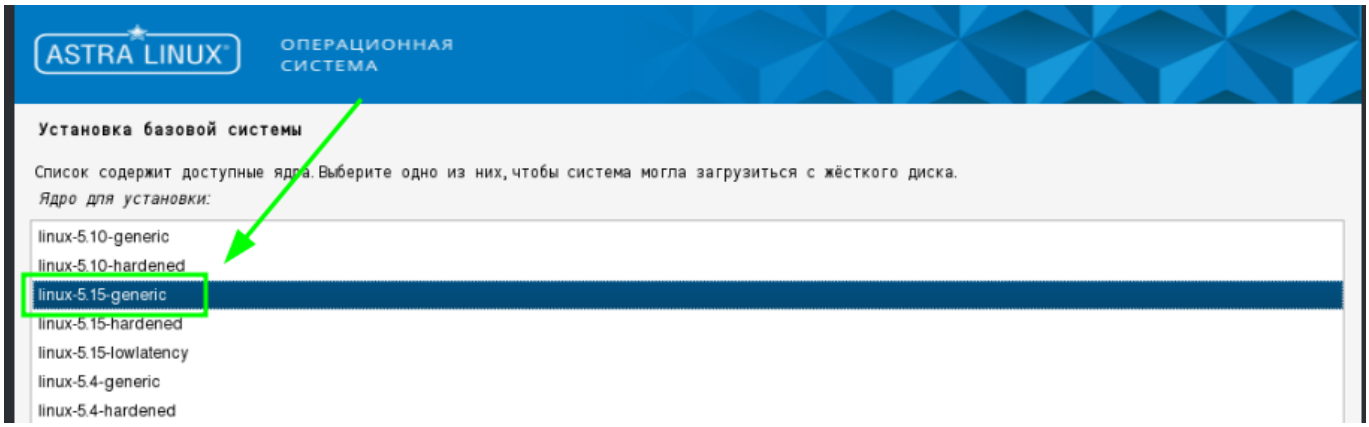
3.8.2. Подготовка контроллера домена ALD Pro

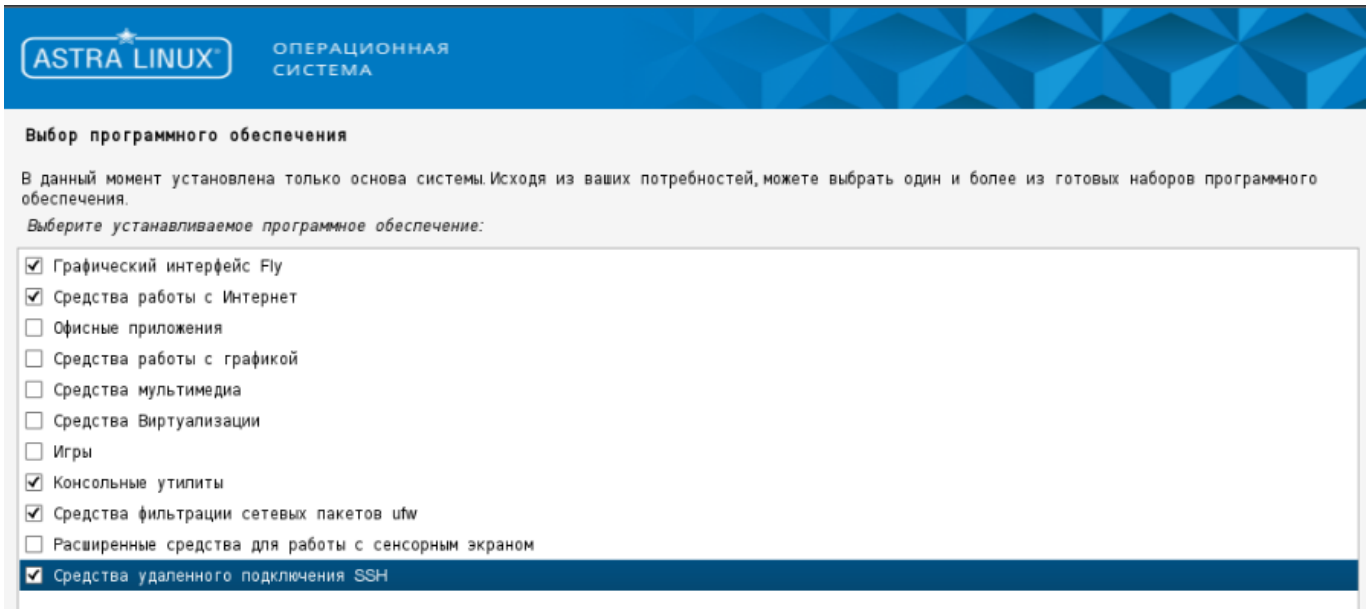
Для взаимодействия между компьютерами будет использована сеть 192.168.88.0/24.

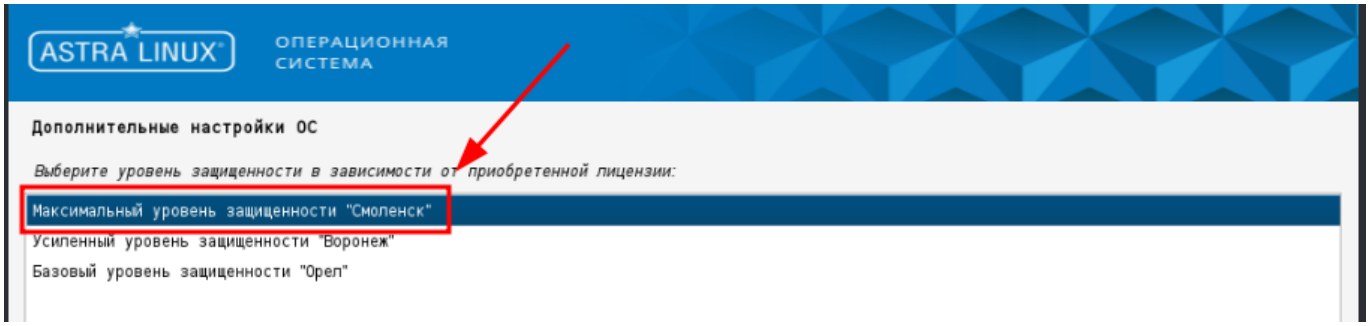





ASTRA LINUX
ОПЕРАЦИОННАЯ СИСТЕМА
Настройка учётных записей пользователей и паролей
Выберите имя учётной записи администратора. Учётная запись должна начинаться со строчной латинской буквы, за которой может следовать любое количество строчных латинских букв или цифр.
Имя учётной записи администратора:
serveradmin


ASTRA LINUX
ОПЕРАЦИОННАЯ СИСТЕМА
Установка базовой системы
Список содержит доступные ядра. Выберите одно из них, чтобы система могла загрузиться с жёсткого диска.
Ядро для установки:
linux-5.10-generic
linux-5.10-hardened
linux-5.15-generic
linux-5.15-hardened
linux-5.15-lowlatency
linux-5.4-generic
linux-5.4-hardened


ASTRA LINUX
ОПЕРАЦИОННАЯ СИСТЕМА
Выбор программного обеспечения
В данный момент установлена только основа системы. Исходя из ваших потребностей, можете выбрать один и более из готовых наборов программного обеспечения.
Выберите устанавливаемое программное обеспечение:
Графический интерфейс Fly
Средства работы с Интернет
Офисные приложения
Средства работы с графикой
Средства мультимедиа
Средства Виртуализации
Игры
Консольные утилиты
Средства фильтрации сетевых пакетов ufw
Расширенные средства для работы с сенсорным экраном
Средства удаленного подключения SSH


ASTRA LINUX
ОПЕРАЦИОННАЯ СИСТЕМА
Дополнительные настройки ОС
Выберите уровень защищенности в зависимости от приобретенной лицензии:
Максимальный уровень защищенности "Смоленск"
Усиленный уровень защищенности "Воронеж"
Базовый уровень защищенности "Орел"

Для первоначальной настройки сети необходимо выполнить **поочередно** нижеперечисленные команды под пользователем root (sudo -i).

```
#Смена имени
hostnamectl set-hostname alddc01

#Закомментировать все строки в основном файле sources.list
sed -i '/^deb.*/s/^/#/' /etc/apt/sources.list

#Создание отдельного frozen.list
cat <<EOF > /etc/apt/sources.list.d/frozen.list
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.4/repository-base/ 1.
↪7_x86-64 main contrib non-free
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.4/repository-
↪extended/ 1.7_x86-64 main contrib non-free
EOF

#Создание отдельного aldpro.list
cat <<EOF > /etc/apt/sources.list.d/aldpro.list
deb https://dl.astralinux.ru/aldpro/stable/repository-main/ 2.1.0 main
deb https://dl.astralinux.ru/aldpro/stable/repository-extended/ generic main
EOF

#Настройка приоритетов пакета aldpro
cat <<EOF > /etc/apt/preferences.d/aldpro
Package: *
Pin: release n=generic
Pin-Priority: 900
EOF

#Остановка NetworkManager сервиса, в дальнейшем будет использоваться
↪Networking + resolvconf
systemctl stop NetworkManager.service && systemctl disable NetworkManager.
↪service

#Обновление файла /etc/hosts, указание ip адреса и FQDN,hostname
cat <<EOF > /etc/hosts
127.0.0.1 localhost
192.168.88.80 alddc01.alddomain.lan alddc01
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
EOF

#Обновление файла /etc/network/interfaces установка статичного адреса,маски,
 ↪шлюза,dns сервера и поискового домена
cat <<EOF > /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 192.168.88.80
        netmask 255.255.255.0
        gateway 192.168.88.1
        dns-nameservers 77.88.8.8
        dns-search alddomain.lan
EOF

#Установка пакета resolvconf
apt update && apt install resolvconf
#Перезагрузка сервера, после перезагрузки сервер будет доступен по
 ↪указанному статичному IP адресу
reboot now
```

Теперь система готова к установке ALD Pro. Для этого необходимо выполнить **поочередно** команды под пользователем root (sudo -i)

```
#Установка обновлений
apt update && astra-update -A -r -T

#Установка пакетов ALD Pro
DEBIAN_FRONTEND=noninteractive apt-get install -y -q aldpro-mp aldpro-gc
 ↪aldpro-syncer
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
#Обновление файла для продвижения /etc/network/interfaces установка
 ↪статичного адреса,маски,шлюза,dns сервера и поискового домена
cat <<EOF > /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 192.168.88.80
        netmask 255.255.255.0
        gateway 192.168.88.1
        dns-nameservers 192.168.88.80
        dns-search alddomain.lan
EOF

#Перезагрузка networking.service для обновления измененного dns-nameservers
systemctl restart networking.service

#Перезагрузка сервера
reboot now

#Отключение dnssec-validation в файле /etc/bind/named.conf.options
sed -i "s/dnssec-validation.*\$/dnssec-validation no;/g" /etc/bind/named.conf.
 ↪options

#Перезапуск службы bind9.service
systemctl restart bind9.service

#Продвижение контроллера домена
set +o history
/opt/rbta/aldpro/mp/bin/aldpro-server-install.sh --setup_gc --setup_syncer -
 ↪d 'alddomain.lan' -n 'alddc01' -p 'Astra123'  --no-reboot >/var/log/
 ↪promotion_aldpro_domain-controler.log
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
set -o history
#Отключение dnssec-validation в файле /etc/bind/ipa-options-ext.conf
sed -i "s/dnssec-validation.*\$/dnssec-validation no;/g" /etc/bind/ipa-
↪options-ext.conf

#Перезагрузка контроллера домена
reboot now
```

3.8.3. Подготовка контроллера домена MS

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

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

Необходимо выполнить следующие команды в **powershell** на контроллере домена

```
#Переименовать контроллер домена
Rename-Computer -NewName windc01
Restart-Computer

#Установить IP адрес,маску подсети и основной шлюз (настройки tcp/ipv4)
New-NetIPAddress -IPAddress 192.168.88.85 -PrefixLength 24 -DefaultGateway
↪192.168.88.1 -InterfaceIndex (Get-NetAdapter).InterfaceIndex

#Установить DNS сервер  (настройки tcp/ipv4)
Set-DnsClientServerAddress –InterfaceIndex (Get-NetAdapter).InterfaceIndex -
↪ServerAddresses "192.168.88.85"

#Установка необходимых компонентов
Install-WindowsFeature -name AD-Domain-Services -IncludeManagementTools

#Установка первого контроллера домена Active Directory в новом лесу
Install-ADDSForest -DomainName windomain.lan -DomainNetBIOSName WINDOMAIN -
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
 ↪InstallDNS

#Установка forwarder на a DNS сервер
Set-DnsServerForwarder -IPAddress "77.88.8.8" -PassThru
```

3.8.4. Контрольный список межлесного доверия

1. Проверка доступности портов
2. Взаимное перенаправление DNS-зон
3. Настройка времени

3.8.5. Контроллеры доверия и агенты доверия (Trust controllers and trust agents)

3.8.5.1. Контроллеры доверия

Это ALD Pro контроллеры, которые могут выполнять поиск идентификационных данных на контроллерах домена AD. Они также запускают Samba suite, чтобы установить доверительные отношения с MS AD. Контроллеры домена MS AD связываются с контроллерами доверия при установлении и проверке доверия к MS AD. Компьютеры, зарегистрированные в MS AD, взаимодействуют с контроллерами доверия ALD Pro для запросов аутентификации Kerberos.

Первый контроллер доверия создается при настройке доверия. Если есть несколько контроллеров домена в разных географических местоположениях, необходимо использовать команду `ipa-adtrust-install` , чтобы назначить серверы ALD Pro доверенными контроллерами по этим местоположениям.

Контроллеры доверия управляют большим количеством сетевых служб, чем агенты доверия и таким образом, представляют большую площадь для атак потенциальных злоумышленников.

Контроллер доверия - это мастер FreeIPA, который запускает следующие службы:

- Сервер LDAP с плагинами sigden, extdom и ldap

- KDC с драйвером IPA
- Samba сконфигурирован с помощью модуля ipasam PASSDB
- SSSD с ipa_server_mode=True
- Экземпляр глобального каталога (отдельный экземпляр LDAP с AD-совместимой схемой)

3.8.5.2. Агенты доверия

Это серверы ALD Pro, которые могут разрешать запросы идентификационных данных от клиентов Astra Linux к контроллерам домена MS AD, используя SSSD. В отличие от контроллеров доверия, агенты доверия не могут обрабатывать запросы на аутентификацию Kerberos.

Доверительный агент - это мастер FreeIPA, который запускает следующие сервисы:

- Сервер LDAP с подключаемыми модулями siding и ext dom
- KDC с драйвером IPA
- SSSD с ipa_server_mode=True

Важно: Нельзя понизить статус существующего контроллера доверия до агента доверия.

3.8.6. Проверка доступности портов

Для проверки доступности портов контроллера домена **alddc01**.alddomain.lan необходимо:

- Получить список всех контроллеров ALD Pro (FreeIPA) **ipa trustconfig-show | grep -i Контроллеры**
- Запустить PowerShell скрипт на контроллере домена **windc01**.windomain.lan (MS AD)

```
$Servers = "localhost"#,"addc02" #Контроллеры домена Active Directory
$Ports   =  "80",
            "443",
#UDP        "123",
            "135",
#UDP        "137",
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
#UDP        "138",
            "139",
            "464",
            "389",
            "636",
            "3268",
            "3269",
            "53",
            "445",
            "88"

$Destination = "192.168.88.80" #Контроллер домена ALD Pro
$Results = @()
$Results = Invoke-Command $Servers {param($Destination,$Ports)
                $Object = New-Object PSCustomObject
                $Object | Add-Member -MemberType NoteProperty -Name
↪"ServerName" -Value $env:COMPUTERNAME
                $Object | Add-Member -MemberType NoteProperty -Name
↪"Destination" -Value $Destination
                    Foreach ($P in $Ports){
                        $PortCheck = (Test-NetConnection -Port $p -
↪ComputerName $Destination ).TcpTestSucceeded
                        If($PortCheck -notmatch "True|False"){$PortCheck =
↪"ERROR"}
                        $Object | Add-Member Noteproperty "$("Port " + "$p")
↪" -Value "$($PortCheck)"
                    }
                $Object
        } -ArgumentList $Destination,$Ports | select * -ExcludeProperty
↪runspaceid, pscomputername

$Results | Out-GridView -Title "Testing Ports"

$Results | Format-Table -AutoSize
```

([см. подробнее](https://learn.microsoft.com/ru-ru/troubleshoot/windows-server/identity/config-firewall-for-ad-domains-and-trusts))

```
Server             Port Service
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
123/UDP          W32Time
135/TCP          RPC Endpoint Mapper
137/UDP          netbios-ns
138/UDP          NetBIOS Datagram Service
464/TCP/UDP          Kerberos password change
49152-65535/TCP    RPC for LSA, SAM, NetLogon
389/TCP/UDP          LDAP
636/TCP          LDAP SSL
3268/TCP             LDAP GC
3269/TCP             LDAP GC SSL
53/TCP/UDP           DNS
445/TCP          SMB
49152-65535/TCP    FRS RPC, DFSR RPC
88/TCP/UDP         Kerberos
```

Для проверки доступности портов контроллера домена **windc01**.windomain.lan необходимо:

- Получить список всех MS AD контроллеров домена – запустить в PowerShell

```
Get-ADDomainController -Filter * | ft Hostname,IPv4Address,OperatingSystem,
↪Enabled
```

- Установить nmap и запустить команду на контроллере домена **alddc01**.alddomain.lan (ALD Pro)

```
apt update && apt install nmap -y
nmap -sT -sU -p 123,135,137,138,464,389,636,3268,3269,53,445,88 192.168.88.
↪85 #Указать IP всех контроллеров домена Active Directory
```

Список портов контроллера домена **ALD Pro**

```
Server             Port Service
80/TCP             Http
443/TCP            Https
123/UDP          W32Time
135/TCP          RPC Endpoint Mapper
137/UDP          netbios-ns
138/UDP          NETBIOS Datagram Service
139/TCP/UDP        NETBIOS Session Service
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
464/TCP/UDP          Kerberos password change
49152-65535/TCP    RPC for LSA, SAM, NetLogon
389/TCP/UDP          LDAP
636/TCP          LDAP SSL
3268/TCP             LDAP GC
3269/TCP             LDAP GC SSL
53/TCP/UDP           DNS
445/TCP/UDP          SMB
49152-65535/TCP    FRS RPC, DFSR RPC
88/TCP/UDP         Kerberos
1024-1300/TCP      Epmap listener range
```

3.8.7. Взаимное перенаправление DNS-зон

Важно: Все контроллеры домена MS AD должны разрешать DNS-запросы к контроллерам домена ALD Pro (прямая и обратная зоны).

Варианты реализации:

- Хранение в Active Directory;
- Ручное добавление.

Для работы доверительных отношений с компьютеров в домене alddomain.lan должны разрешаться имена компьютеров домена windomain.lan и наоборот. Для этого необходимо выполнить взаимное перенаправление DNS-зон.

Для создания перенаправителя (ConditionalForwarder) из домена windomain.lan в alddomain.lan необходимо:

- Запустить PowerShell на контроллере домена **windc01**.windomain.lan (MS AD)

```
Add-DnsServerConditionalForwarderZone -Name "alddomain.lan" -
↪ReplicationScope "Forest" -MasterServers 192.168.88.80

#Вывести список всех созданных ConditionalForwarder
$DNSServer = "windc01"
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
$Zones = Get-WMIObject -Computer $DNSServer -Namespace "root\MicrosoftDNS" -
↪Class "MicrosoftDNS_Zone"
$Zones | Select-Object Name,MasterServers,DsIntegrated,ZoneType | where {$_.
↪ZoneType -eq "4"} | ft -AutoSize
```

Для проверки доступности домена alddomain.lan необходимо выполнить следующие команды:

```
ping alddc01.alddomain.lan
Resolve-DnsName _ldap._tcp.alddomain.lan -Type SRV
Resolve-DnsName _kerberos._tcp.alddomain.lan -Type SRV
```

Для создания перенаправителя (ConditionalForwarder) из домена alddomain.lan в windomain.lan необходимо:

- Запустить команду на контроллере домена **alddc01**.alddomain.lan (ALD Pro)

```
kinit admin
ipa dnsforwardzone-add windomain.lan --forwarder=192.168.88.85 --forward-
↪policy=only

#Показать параметры зоны windomain.lan
ipa dnsforwardzone-show windomain.lan
```

Для проверки доступности домена windomain.lan необходимо выполнить следующие команды:

```
ping windc01.windomain.lan
dig SRV _ldap._tcp.windomain.lan
dig SRV _kerberos._tcp.windomain.lan
```

3.8.8. Настройка DNS - доверительные сети (bind trusted_network)

В случаях необходимости ограничения DNS-запросов из определенных сетей на каждом ALD Pro (FreeIPA) контроллере, необходимо внести изменения в файл /etc/bind/ipa-ext.conf:

```
p/* User customization for BIND named
*
* This file is included in /etc/bind/named.conf and is not modified during
 ↪IPA
* upgrades.
*
* "options" settings must be configured in /etc/bind/ipa-options-ext.conf.
*
* Example: ACL for recursion access:
*
* acl "trusted_network" {
*   localnets;
*   localhost;
*   234.234.234.0/24;
*   2001::co:ffee:babe:1/48;
* };
*/

acl "trusted_network" {
localnets;
localhost;
192.168.88.0/24;
172.19.3.0/24;
172.19.4.0/24;
};
```

Для активации дополнительных опций DNS Bind, на каждом ALD Pro (FreeIPA) контроллере необходимо внести изменения в файл **/etc/bind/ipa-options-ext.conf:**

```
/* User customization for BIND named
*
* This file is included in /etc/bind/named.conf and is not modified during
 ↪IPA
* upgrades.
*
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
* It must only contain "options" settings. Any other setting must be
* configured in /etc/bind/ipa-ext.conf.
*
* Examples:
* allow-recursion { trusted_network; };
* allow-query-cache { trusted_network; };
*/

allow-recursion { trusted_network; };
allow-query-cache { trusted_network; };

/* turns on IPv6 for port 53, IPv4 is on by default for all ifaces */
listen-on-v6 { any; };

/* dnssec-enable is obsolete and 'yes' by default */
dnssec-validation no;
```

3.8.9. Настройка времени

Перед установлением межлесного доверия необходимо выполнить дополнительную настройку даты/времени и убедиться, что настройки часового пояса и даты/времени на обоих серверах совпадают.

3.8.9.1. На стороне ALD Pro

1. Статус сервиса времени

```
systemctl status chrony.service
```

2. Проверка источника времени

```
chronyc sources -v
210 Number of sources = 4

.-- Source mode  '^' = server, '=' = peer, '#' = local clock.
/ .- Source state '*' = current synced, '+' = combined , '-' = not combined,
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
| /   '?' = unreachable, 'x' = time may be in error, '~' = time too variable.
||                                                .- xxxx [ yyyy ] +/- zzzz
||      Reachability register (octal) -.          |  xxxx = adjusted offset,
||      Log2(Polling interval) --.      |         |  yyyy = measured offset,
||                                \     |         |  zzzz = estimated error.
||                                 |    |          \
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^- 82.142.168.18                 3  10   377   760   +597us[ +579us] +/-  
 ↪64ms
^* ntp.ix.ru                     1  10   377   106   -135us[ -153us] +/-
 ↪5999us
^- ground.corbina.net            2  10   377   148  -6714us[-6731us] +/-  
 ↪44ms
^- cello.corbina.net             2  10   377  1007  -6747us[-6765us] +/-  
 ↪38ms
```

3. Подробная статистика по источникам времени

```
chronyc sourcestats -v
210 Number of sources = 4
                             .- Number of sample points in measurement set.
                             /    .- Number of residual runs with same sign.
                           |    /    .- Length of measurement set (time).
                           |    |    /      .- Est. clock freq error (ppm).
                           |    |   |      /           .- Est. error in freq.
                           |    |   |     |           /         .- Est. offset.
                           |    |   |     |          |          |   On the -.
                           |    |   |     |          |          |   samples. \
                           |    |   |     |          |          |             |
Name/IP Address            NP  NR  Span  Frequency  Freq Skew  Offset  Std
 ↪Dev
===============================================================================
82.142.168.18              14   8  224m     +0.020      0.065   -215us  
 ↪229us
ntp.ix.ru                  18  13  361m     +0.000      0.030    +29ns  
 ↪186us
ground.corbina.net         16   9  258m     +0.012      0.053  -8380us  
 ↪228us
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
cello.corbina.net           25   15   430m     +0.055       0.035   -7950us  
↪334us
```

4. Проверка расхождение времени

```
chronyc tracking
```

Пример результата

```
admin@aldpro01:~$ chronyc tracking
Reference ID    : BC5D6802 (188.93.104.2)
Stratum         : 3
Ref time (UTC)  : Thu Apr 13 10:21:39 2023
System time     : 0.000400797 seconds slow of NTP time
Last offset     : +0.000018209 seconds
RMS offset      : 0.000149458 seconds
Frequency       : 17.812 ppm slow
Residual freq   : +0.000 ppm
Skew            : 0.136 ppm
Root delay      : 0.014107514 seconds
Root dispersion : 0.019041860 seconds
Update interval : 515.2 seconds
Leap status     : Normal
```

Текущий конфиг можно посмотреть в файле:

```
less /etc/chrony/chrony.conf
```

3.8.9.2. На стороне MS AD

Для настройки синхронизации времени с внешним NTP-сервером (настраивается только на PDC в корневом домене) необходимо выполнить следующие команды:

```
w32tm /config /reliable:yes /syncfromflags:manual /manualpeerlist:"ntp.msk-ix.
↪ru" /update
net stop w32time
net start w32time
w32tm /resync
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
w32tm /monitor /computers:"ntp.msk-ix.ru"
w32tm /stripchart /computer:ntp.msk-ix.ru
```

Пример результата

```
PS C:\Users\Administrator> w32tm /stripchart /computer:ntp.msk-ix.ru
Tracking ntp.msk-ix.ru [194.190.168.1:123].
The current time is 4/13/2023 1:40:55 PM.
13:40:55, d:+00.0091883s o:-00.0110417s  [                       *       ]
 ↪                     ]
13:40:57, d:+00.0093593s o:-00.0111335s  [                       *       ]
 ↪                     ]
13:40:59, d:+00.0099441s o:-00.0112867s  [                       *       ]
 ↪                     ]
13:41:01, d:+00.0100102s o:-00.0113176s  [                       *       ]
 ↪                     ]
13:41:03, d:+00.0101050s o:-00.0112696s  [                       *       ]
 ↪                     ]
```

Создание доверительных отношений

3.8.10. Создание двустороннего доверия (Forest Trust)

Во всех инструкциях создание доверия начинают с выполнения команды `ipa-adtrust-install` , которая подготавливает домен FreeIPA к работе с доверительными отношениями, в частности, добавляет атрибут для хранения windows security identifier (SID). В случае с ALD Pro это не требуется. Команда `trustconfig-show` показывает, что домен уже готов к работе с доверительными отношениями:

```
# ipa trustconfig-show
Домен: alddomain.lan
Идентификатор безопасности: S-1-5-21-1307086432-2724870100-1147875473
Имя NetBIOS: ALDDOMAIN
GUID домена: 7a522ccc-a0d7-4eac-a46a-46b12c93fa0e
Резервная основная группа: Default SMB Group
Агенты отношений доверия AD IPA: alddc01.alddomain.lan
Контроллеры отношений доверия AD IPA: alddc01.alddomain.lan
```

Доверие может быть добавлено на стороне ALD Pro из командной строки. При появлении проблем рекомендуется использовать ключи -d и -v для получения дополнительной информации об ошибках.

Перед созданием доверительных отношений нужно запросить Kerberos-билет для учетной записи **admin:**

```
root@alddc01:~# kinit admin
Password for admin@ALDDOMAIN.LAN:
root@alddc01:~#
root@alddc01:~# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: admin@ALDDOMAIN.LAN

Valid starting       Expires              Service principal
22.10.2023 14:55:39  23.10.2023 14:55:36  krbtgt/ALDDOMAIN.LAN@ALDDOMAIN.LAN


#ipa -d -v trust-add --type=ad <DomainName> --admin administrator --password -
 ↪-two-way=true

ipa -d -v trust-add --type=ad windomain.lan --admin administrator --password -
 ↪-two-way=true

------------------------------------------------------------------------------
 ↪--
Добавлено отношение доверия Active Directory для области (realm) "windomain.
 ↪lan"
------------------------------------------------------------------------------
 ↪--
Имя области (realm): windomain.lan
Имя домена NetBIOS: WINDOMAIN
Идентификатор безопасности домена: S-1-5-21-292663598-2229028806-4201728183
Направление отношения доверия: Двустороннее отношение доверия
Тип отношения доверия: Домен Active Directory
Состояние отношения доверия: Установлено и проверено
```

Если в этот момент отслеживать сетевой трафик, то можно будет увидеть, что аутентификация в Windows-домене выполняется по Kerberos, а установление доверия выполняется по транспортному протоколу SMB2 путем вызова удаленных команд RPC. В то же время билет на доступ к службе `krbtgt` в Windows домене не сохраняется в кеше

sssd службы, поэтому команда `klist` после установления доверия не покажет дополнительных билетов.

После создания доверия можно посмотреть информацию о созданном доверии командами `trust-find` и `trust-show` :

```
root@alddc01:~# ipa trust-find
---------------------------
найдено 1 отношение доверия
---------------------------
Имя области (realm): windomain.lan
Имя домена NetBIOS: WINDOMAIN
Идентификатор безопасности домена: S-1-5-21-292663598-2229028806-4201728183
Тип отношения доверия: Домен Active Directory
---------------------------------
Количество возвращённых записей 1
---------------------------------
root@alddc01:~#
root@alddc01:~# ipa trust-show  windomain.lan
Имя области (realm): windomain.lan
Имя домена NetBIOS: WINDOMAIN
Идентификатор безопасности домена: S-1-5-21-292663598-2229028806-4201728183
Направление отношения доверия: Двустороннее отношение доверия
Тип отношения доверия: Домен Active Directory
```

Так же можно просмотреть, какие контроллеры ALD Pro обрабатывают запросы при работе с доверительными отношениями:

```
root@alddc01:~# ipa trustconfig-show
Домен: alddomain.lan
Идентификатор безопасности: S-1-5-21-1307086432-2724870100-1147875473
Имя NetBIOS: ALDDOMAIN
GUID домена: 7a522ccc-a0d7-4eac-a46a-46b12c93fa0e
Резервная основная группа: Default SMB Group
Агенты отношений доверия AD IPA: alddc01.alddomain.lan
Контроллеры отношений доверия AD IPA: alddc01.alddomain.lan
```

С помощью команд `trust-fetch-domains` и `trustdomain-find` можно подгрузить информацию о дочерних доменах леса и доменах, с которыми у доверенного домена, в свою очередь, построены доверительные отношения. Они потребуются, если позднее в лесе MS AD появятся новые дочерние домены или будут созданы транзитивные

доверительные отношения с другими MS AD доменами. При добавлении информации о домене MS AD в каталог ALD Pro каждому домену назначается диапазон POSIX идентификаторов.

3.8.11. Создание доверия между двумя доменами (External Trust)

3.8.11.1. Поддержка внешнего доверия к домену из леса MS AD

Внешнее доверие - это доверительные отношения между доменами MS AD, которые находятся в разных лесах MS AD. В то время как для обеспечения доверия к лесу всегда требуется установить доверие **между корневыми доменами** лесов MS AD, внешнее доверие может быть установлено к любому домену в лесу.

3.8.11.2. Варианты использования

Администратор домена MS AD хочет установить доверие между ALD Pro и своим доменом. Доверие между ALD Pro и внешним доменом MS AD будет непереходным, поскольку никакие пользователи или группы из других доменов MS AD не будут иметь доступа к ресурсам ALD Pro.

3.8.11.3. Дизайн

Внешнее доверие между доменами MS AD по определению является нетранзитивным и обеспечивает фильтрацию SID между границами домена. Это означает, что только пользователи и группы с SID из доверенного домена могут использовать ресурсы и быть видимыми в системах ALD Pro. Никому из других пользователей и групп из доменов, которым доверенный домен доверяет в своем собственном лесу MS AD, или других доменов, которым доверяют извне, не будет разрешен доступ к ресурсам ALD Pro.

3.8.11.4. Реализация

Функция внешнего доверия повторно использует существующую инфраструктуру лесного доверия. Существуют изменения, позволяющие поддерживать внешнее доверие:

- Нетранзитивность: поскольку внешнее доверие является нетранзитивным по

определению, любая попытка установить функцию транзитивности доверительной ссылки с помощью команды **LSA SetInformationTrustedDomain()** завершится неудачей. Таким образом, нет необходимости устанавливать транзитивность для внешнего доверия.

- Атрибуты доверия: внешнее доверие может быть обнаружено путем проверки отсутствия атрибута `ipaNTTrustAttributes` LDAP-объекта доверенного домена.

Траст можно добавить на стороне ALD Pro из командной строки. При появлении проблем рекомендуется использовать ключи -d и -v для получения дополнительной информации об ошибках.

Перед созданием доверительных отношений запрашивается Kerberos-билет для учетной записи **admin**:

```
root@alddc01:~# kinit admin
Password for admin@ALDDOMAIN.LAN:
root@alddc01:~#
root@alddc01:~# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: admin@ALDDOMAIN.LAN

Valid starting       Expires              Service principal
22.10.2023 15:10:49  23.10.2023 15:10:46  krbtgt/ALDDOMAIN.LAN@ALDDOMAIN.LAN



ipa -d -v trust-add --type=ad <DomainName> --external=true --admin
 ↪administrator --password --two-way=true

ipa -d -v trust-add --type=ad windomain.lan --external=true --admin
 ↪administrator --password --two-way=true
```

Пример результата:

```
--------------------------------------------------------------------------------
 ↪--
Добавлено отношение доверия Active Directory для области (realm) "windomain.
 ↪lan"
--------------------------------------------------------------------------------
 ↪--
```

(продолжение на следующей странице)

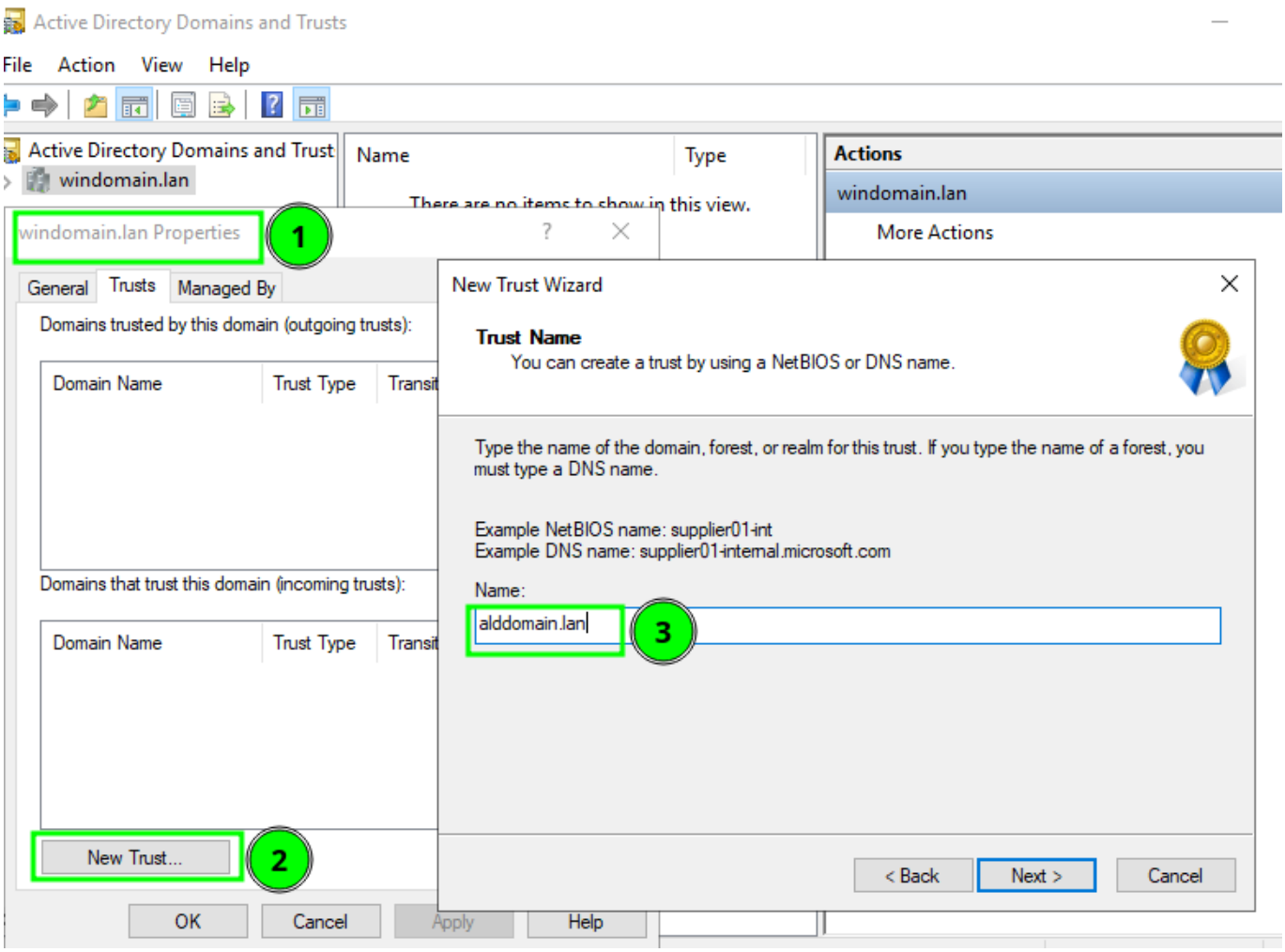
(продолжение с предыдущей страницы)

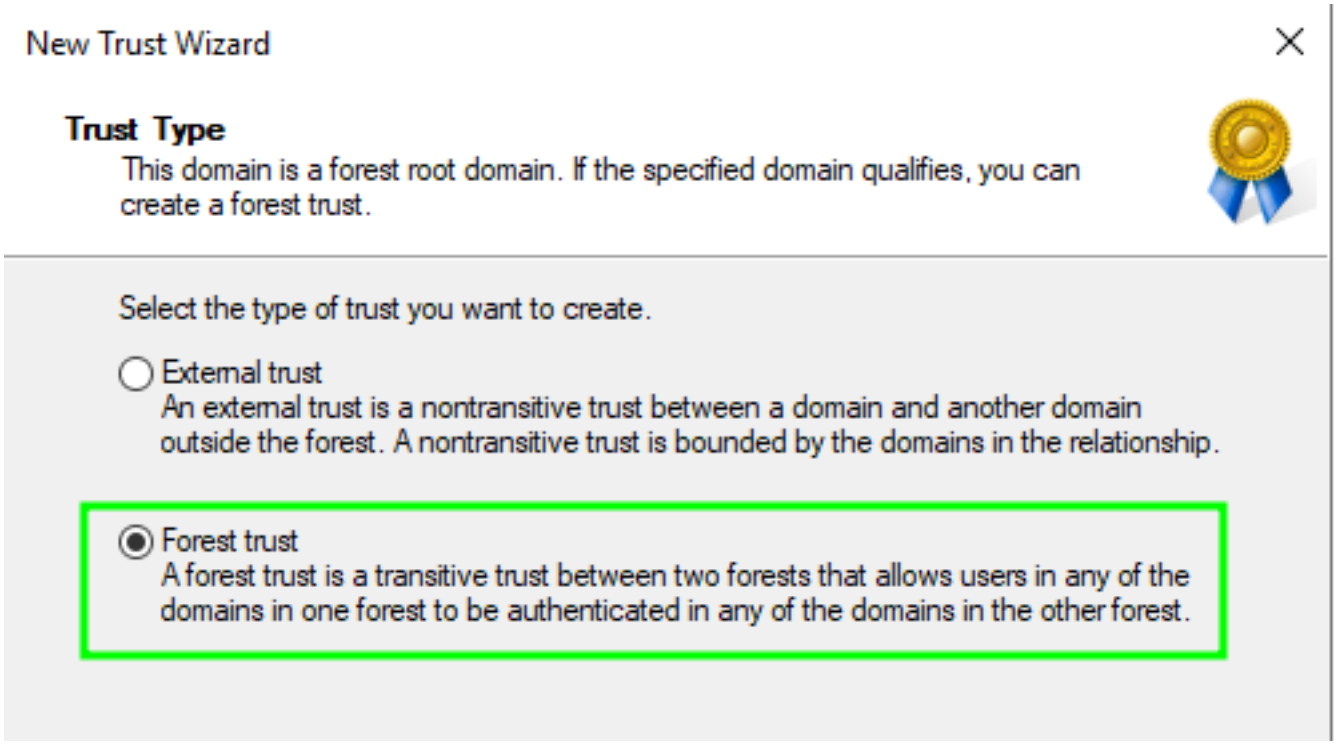
```
Имя области (realm): windomain.lan
Имя домена NetBIOS: WINDOMAIN
Идентификатор безопасности домена: S-1-5-21-292663598-2229028806-4201728183
Направление отношения доверия: Двустороннее отношение доверия
Тип отношения доверия: Нетранзитивное внешнее отношение доверия с доменом в
 ↪другом лесу Active Directory
Состояние отношения доверия: Установлено и проверено
```

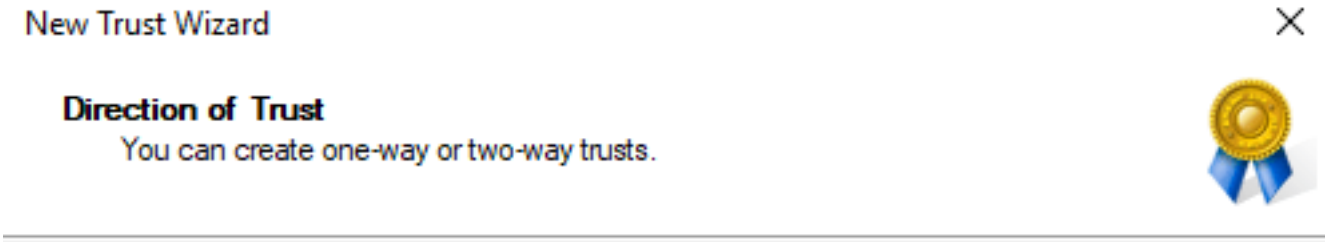
3.8.11.5. Создание траста (one-way trust using a trust-secret)

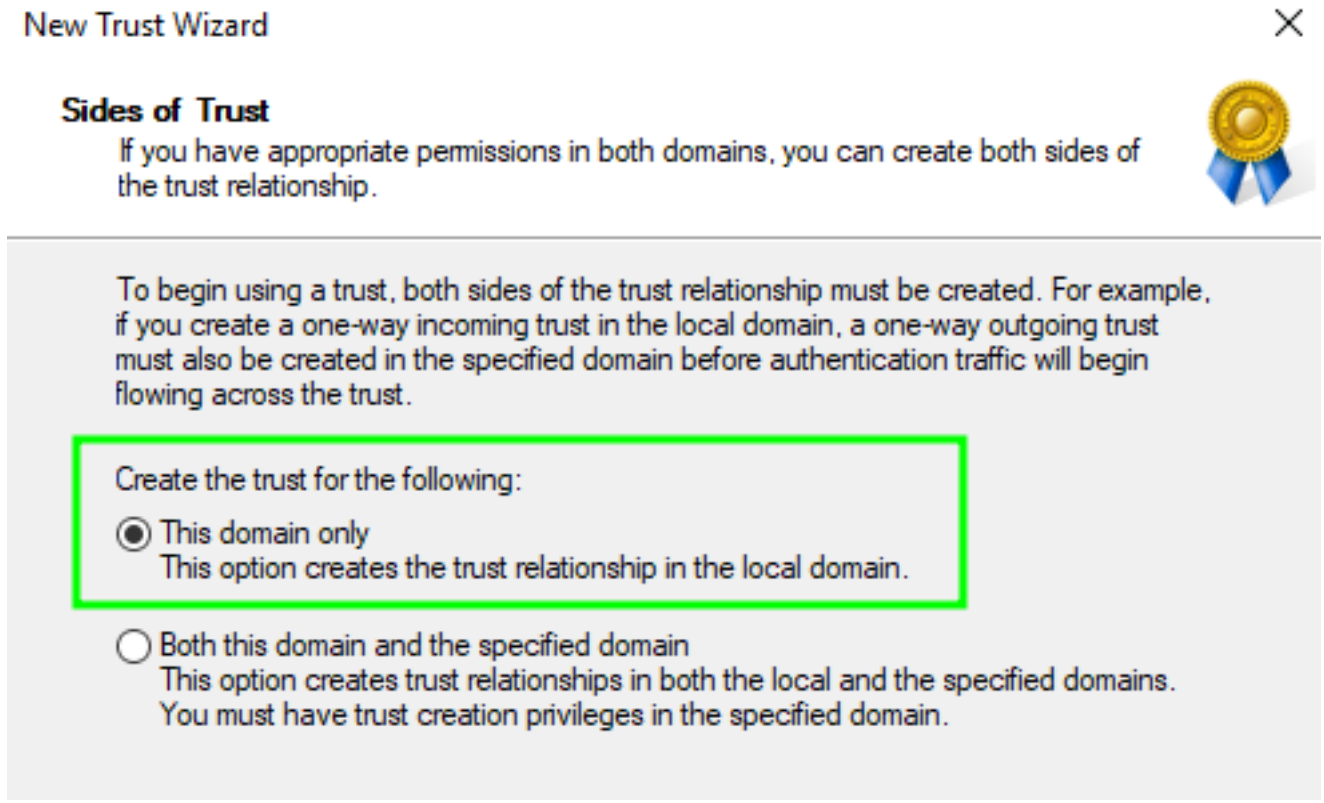
Для создания доверительных отношений, используя секрет доверия, требуется предварительно создать доверие на стороне MS AD (win.company.local).

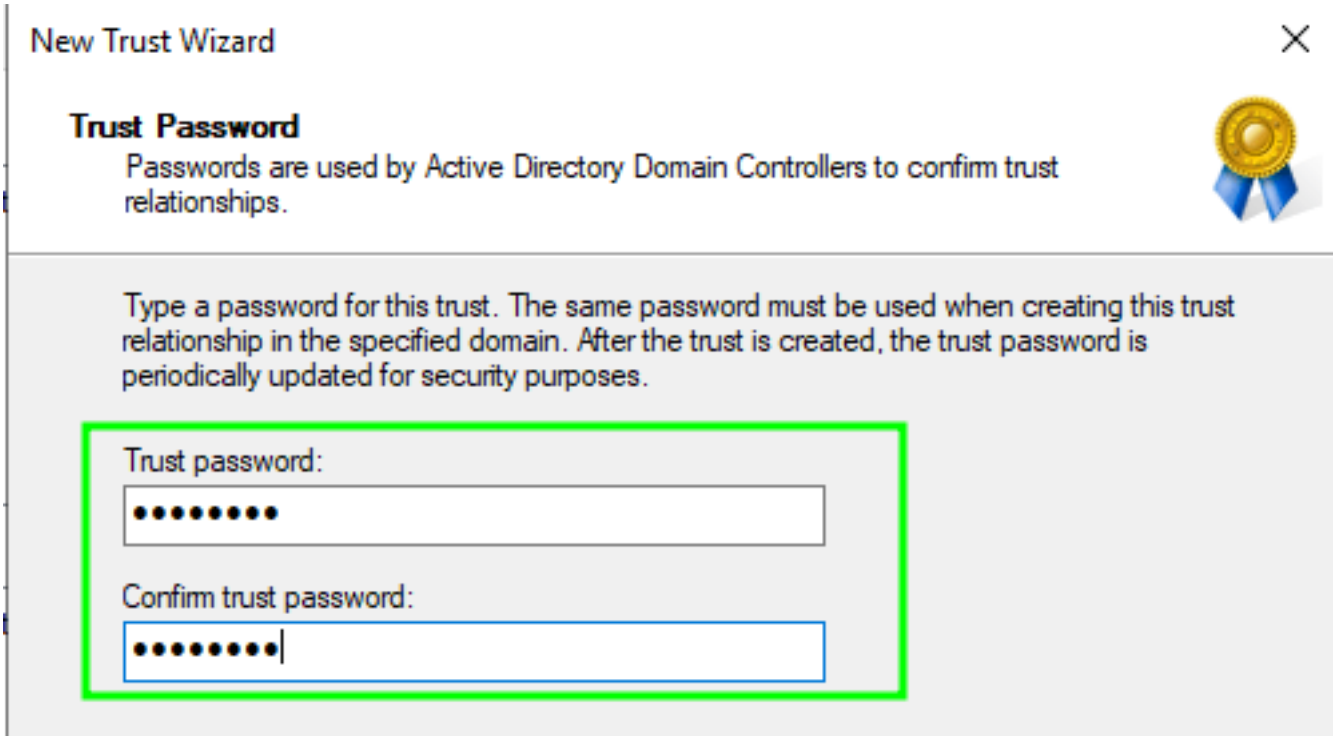
1. На стороне Windows открыть MS AD Domain and Trusts tool
2. Открыть свойства для леса Windows
3. Выбрать вкладку «Трасты» и нажать «Создать траст»
4. Перейти к мастеру создания доверия, введя: - Название ALD Pro-леса, затем «следующий»
5. Выбрать «Лесное доверие» на странице «Тип доверия»
6. Выбрать «Односторонний: входящий» на странице «Направление доверия»
7. Выбрать «Только для этого домена» по бокам страницы доверия
8. Ввести тот же общий секрет, который использовался на шаге (1), с помощью «ipa trust-add»

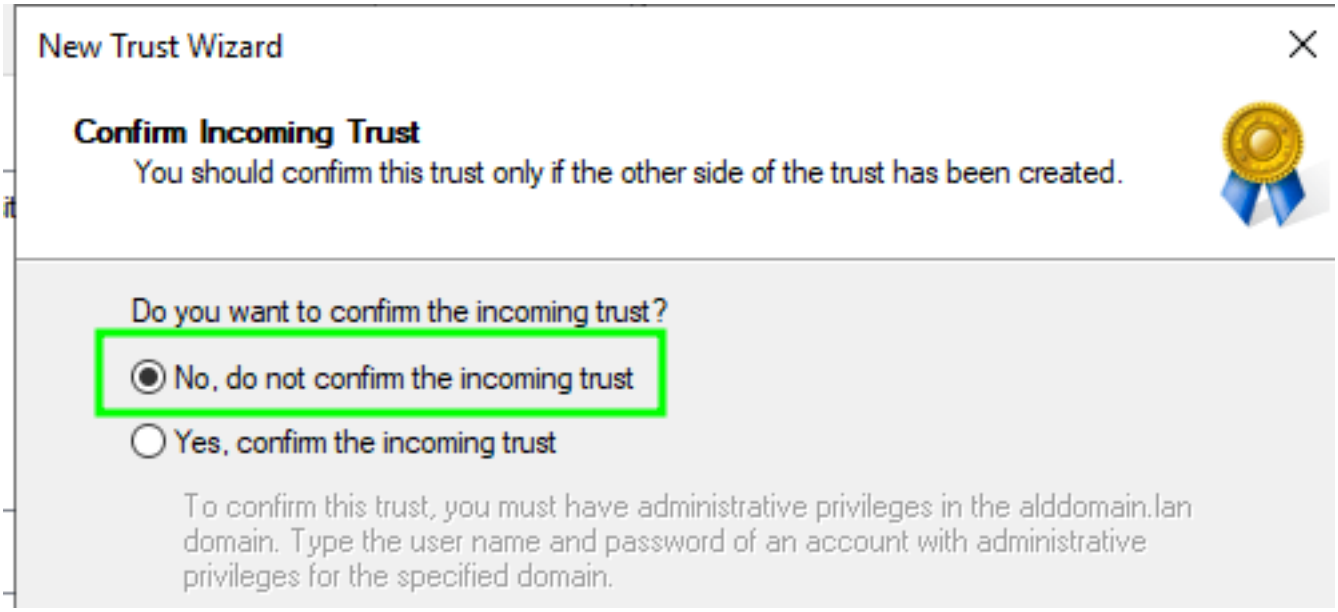

Active Directory Domains and Trusts
File Action View Help
Active Directory Domains and Trust
windomain.lan
Name
Type
There are no items to show in this view.
Actions
windomain.lan
More Actions
windomain.lan Properties
1
General Trusts Managed By
Domains trusted by this domain (outgoing trusts):
Domain Name
Trust Type
Transit
Domains that trust this domain (incoming trusts):
Domain Name
Trust Type
Transit
New Trust...
2
OK
Cancel
Apply
Help
New Trust Wizard
Trust Name
You can create a trust by using a NetBIOS or DNS name.
Type the name of the domain, forest, or realm for this trust. If you type the name of a forest, you must type a DNS name.
Example NetBIOS name: supplier01-int
Example DNS name: supplier01-internal.microsoft.com
Name:
alddomain.lan
3
< Back
Next >
Cancel


New Trust Wizard
Trust Type
This domain is a forest root domain. If the specified domain qualifies, you can create a forest trust.
Select the type of trust you want to create.
External trust
An external trust is a nontransitive trust between a domain and another domain outside the forest. A nontransitive trust is bounded by the domains in the relationship.
Forest trust
A forest trust is a transitive trust between two forests that allows users in any of the domains in one forest to be authenticated in any of the domains in the other forest.


New Trust Wizard
Direction of Trust
You can create one-way or two-way trusts.
Select the direction for this trust.
Two-way
Users in this domain can be authenticated in the specified domain, realm, or forest, and users in the specified domain, realm, or forest can be authenticated in this domain.
One-way: incoming
Users in this domain can be authenticated in the specified domain, realm, or forest.
One-way: outgoing
Users in the specified domain, realm, or forest can be authenticated in this domain.


New Trust Wizard
Sides of Trust
If you have appropriate permissions in both domains, you can create both sides of the trust relationship.
To begin using a trust, both sides of the trust relationship must be created. For example, if you create a one-way incoming trust in the local domain, a one-way outgoing trust must also be created in the specified domain before authentication traffic will begin flowing across the trust.
Create the trust for the following:
This domain only
This option creates the trust relationship in the local domain.
Both this domain and the specified domain
This option creates trust relationships in both the local and the specified domains.
You must have trust creation privileges in the specified domain.





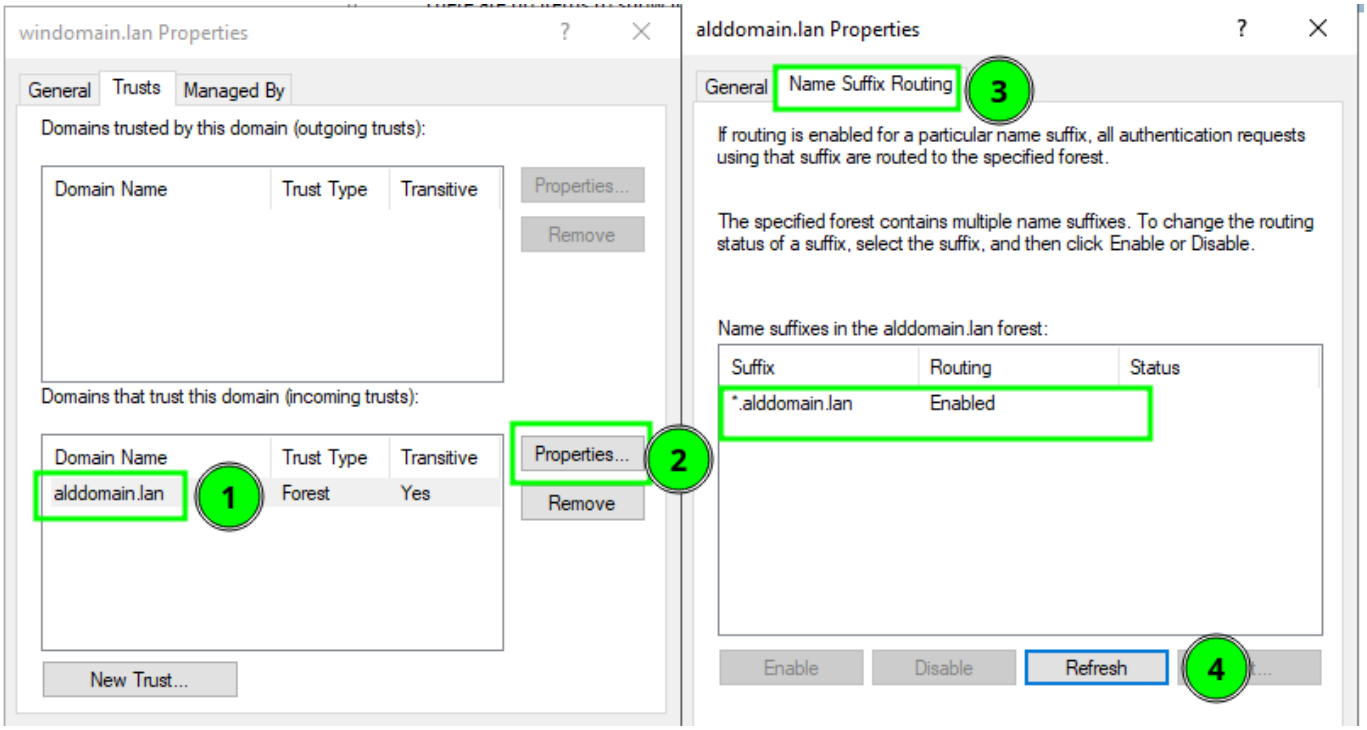

```
# ipa trust-add --type=ad  <DomainName> --trust-secret
root@alddc01:~# ipa trust-add --type=ad  windomain.lan --trust-secret
Общий секрет для отношения доверия:
-------------------------------------------------------------------------------
 ↪--
Добавлено отношение доверия MS AD для области (realm) "windomain.lan"
-------------------------------------------------------------------------------
 ↪--
Имя области (realm): windomain.lan
```

(продолжение на следующей странице)

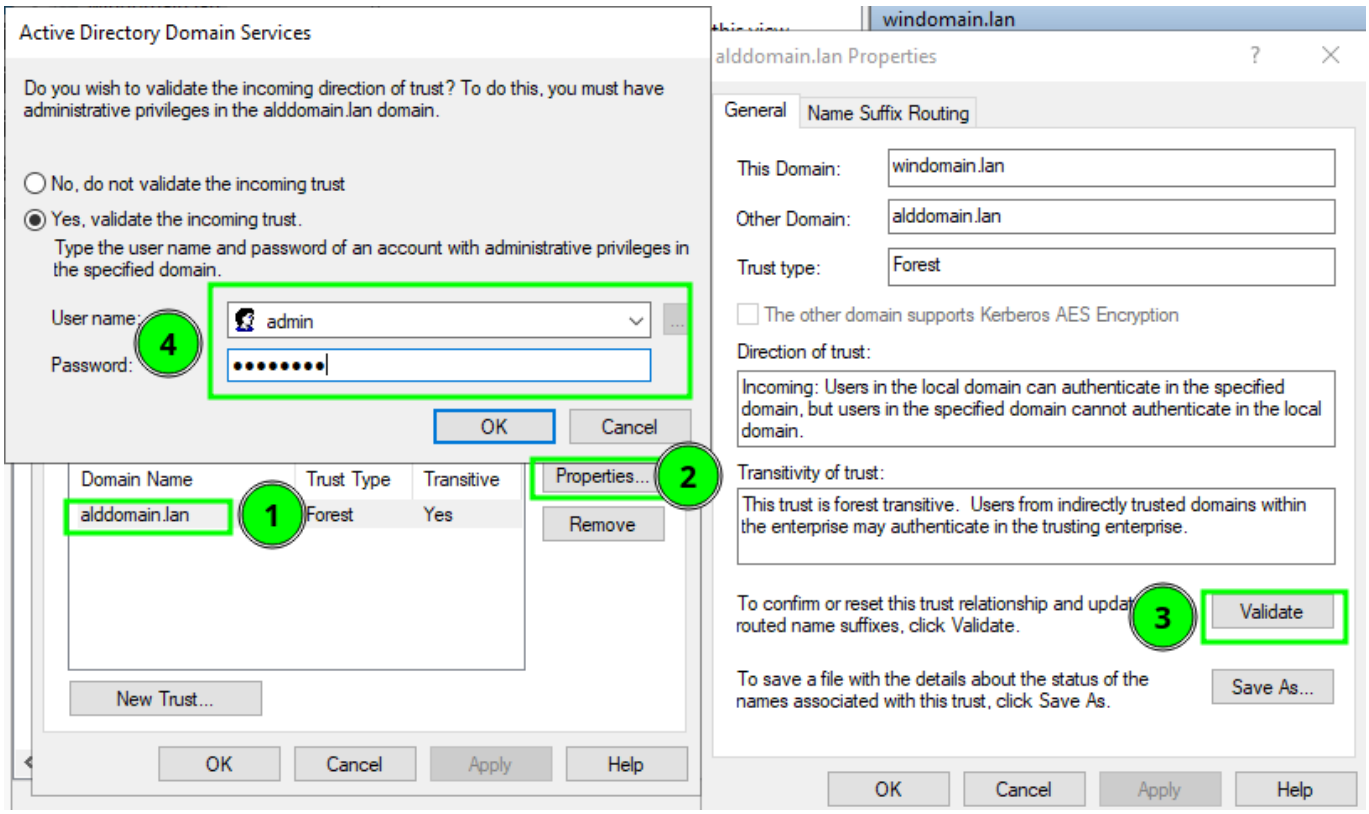
(продолжение с предыдущей страницы)

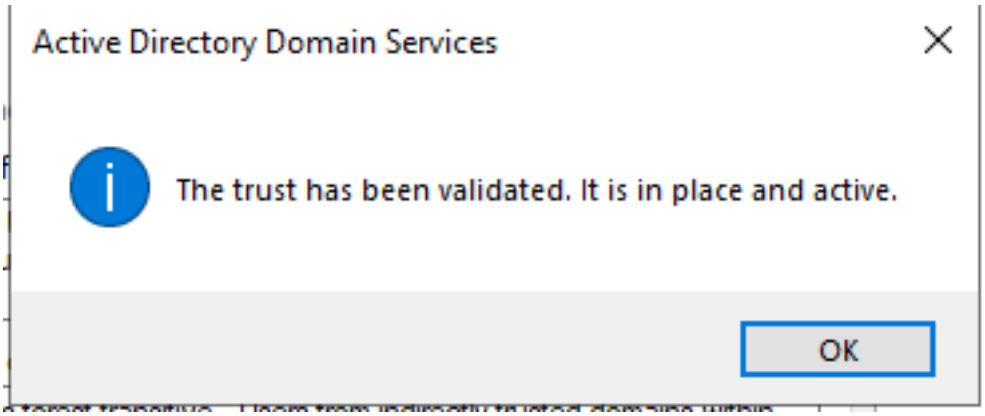
```
Имя домена NetBIOS: WINDOMAIN
Идентификатор безопасности домена: S-1-5-21-292663598-2229028806-4201728183
Направление отношения доверия: Доверяющий лес
Тип отношения доверия: Домен MS AD
Состояние отношения доверия: Ожидание подтверждения удалённой стороной
```

На стороне MS AD необходимо убедиться, что появился суффикс роутинг



Провести валидацию доверия





Если требуется установить двусторонее доверие, то команды будет выглядеть следующим образом:

```
# ipa trust-add --type=ad <DomainName>--trust-secret  --two-way=true

ipa trust-add --type=ad windomain.lan --trust-secret  --two-way=true


#root@aldpro01:~# ipa trust-add --type=ad windomain.lan --trust-secret  --two-
↪way=true
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
Общий секрет для отношения доверия:
--------------------------------------------------------------------------------
 ↪------
Добавлено отношение доверия Active Directory для области (realm) "win.company.
 ↪local"
--------------------------------------------------------------------------------
 ↪------
Имя области (realm): windomain.lan
Имя домена NetBIOS: WINDOMAIN
Идентификатор безопасности домена: S-1-5-21-292663598-2229028806-4201728183
Направление отношения доверия: Двустороннее отношение доверия
Тип отношения доверия: Домен Active Directory
Состояние отношения доверия: Ожидание подтверждения удалённой стороной
```

Для удаление траста необходимо выполнить команду:

```
ipa trust-del windomain.lan
```

3.8.11.6. MS AD доверие с множеством поддоменов

В больших организация, где поддоменов MS AD более одного, требуется производить дополнительные действия.

Чтобы выполнить прямую (неиерархическую) аутентификацию между областями, необходима база данных для построения путей аутентификации между областями. В этом разделе определяется нужная база данных.

Клиент использует этот раздел, чтобы найти путь аутентификации между своей областью и областью сервера. Сервер использует этот раздел для проверки пути аутентификации, используемого клиентом, путем проверки поля «Пройдено» в полученном билете. ([см. подробнее](https://web.mit.edu/kerberos/krb5-1.5/krb5-1.5.4/doc/krb5-admin/capaths.html)).

Далее приведен упрощенный визуализированный пример.

Пример многодоменной инфраструктуры, в данном примере для того, чтобы пользователи из поддоменов **msk.child.win2019.dom** и **stupino.msk.child.win2019.dom** смогли войти на PC-1.ALDPRO.DOM. Необходимо добавить в файл **/etc/krb5.conf** следующую информацию:

```
[capaths]

MSK.CHILD.WIN2019.DOM = {

ALDPRO.DOM = CHILD.WIN2019.DOM

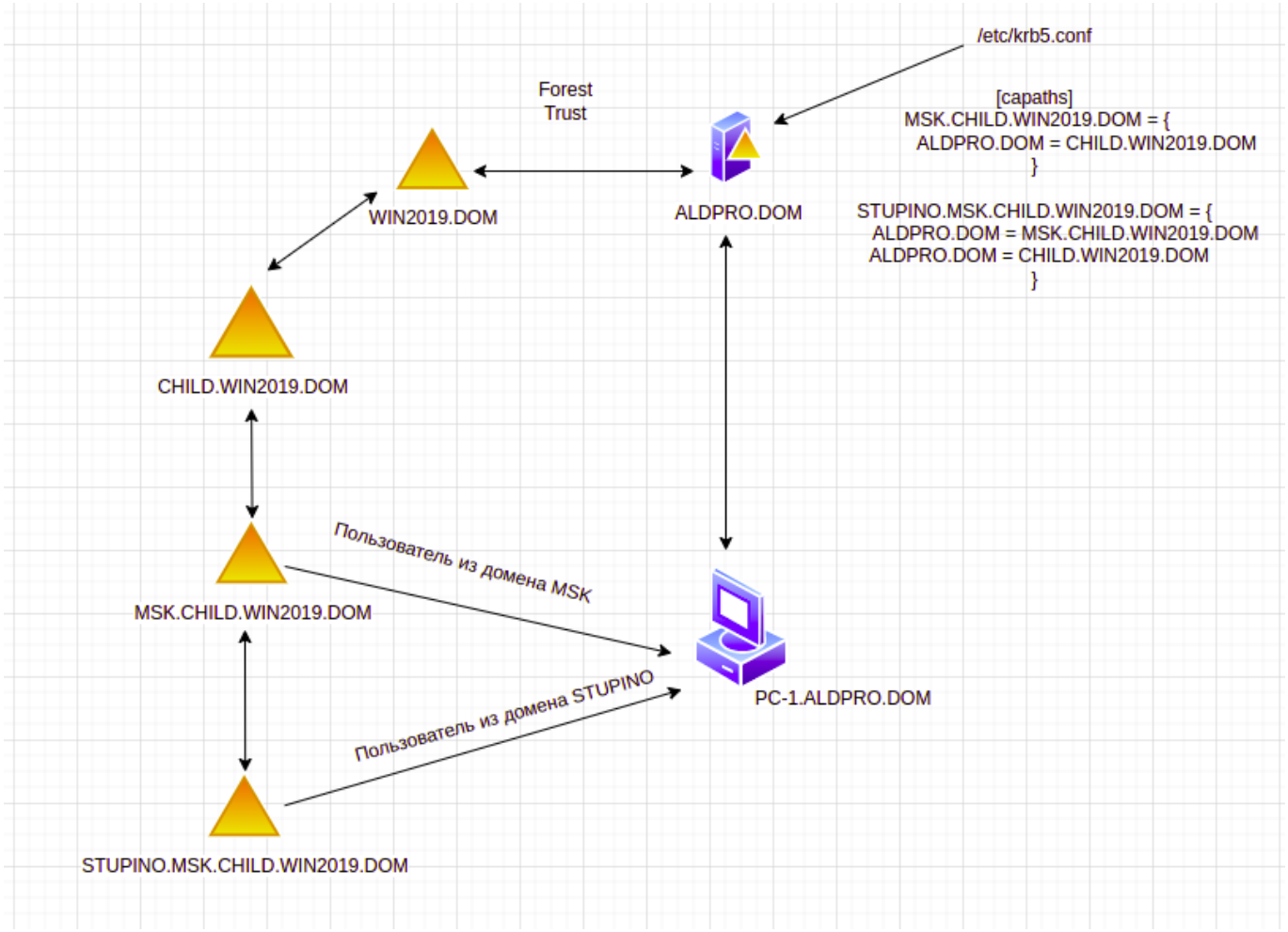
}

STUPINO.MSK.CHILD.WIN2019.DOM = {

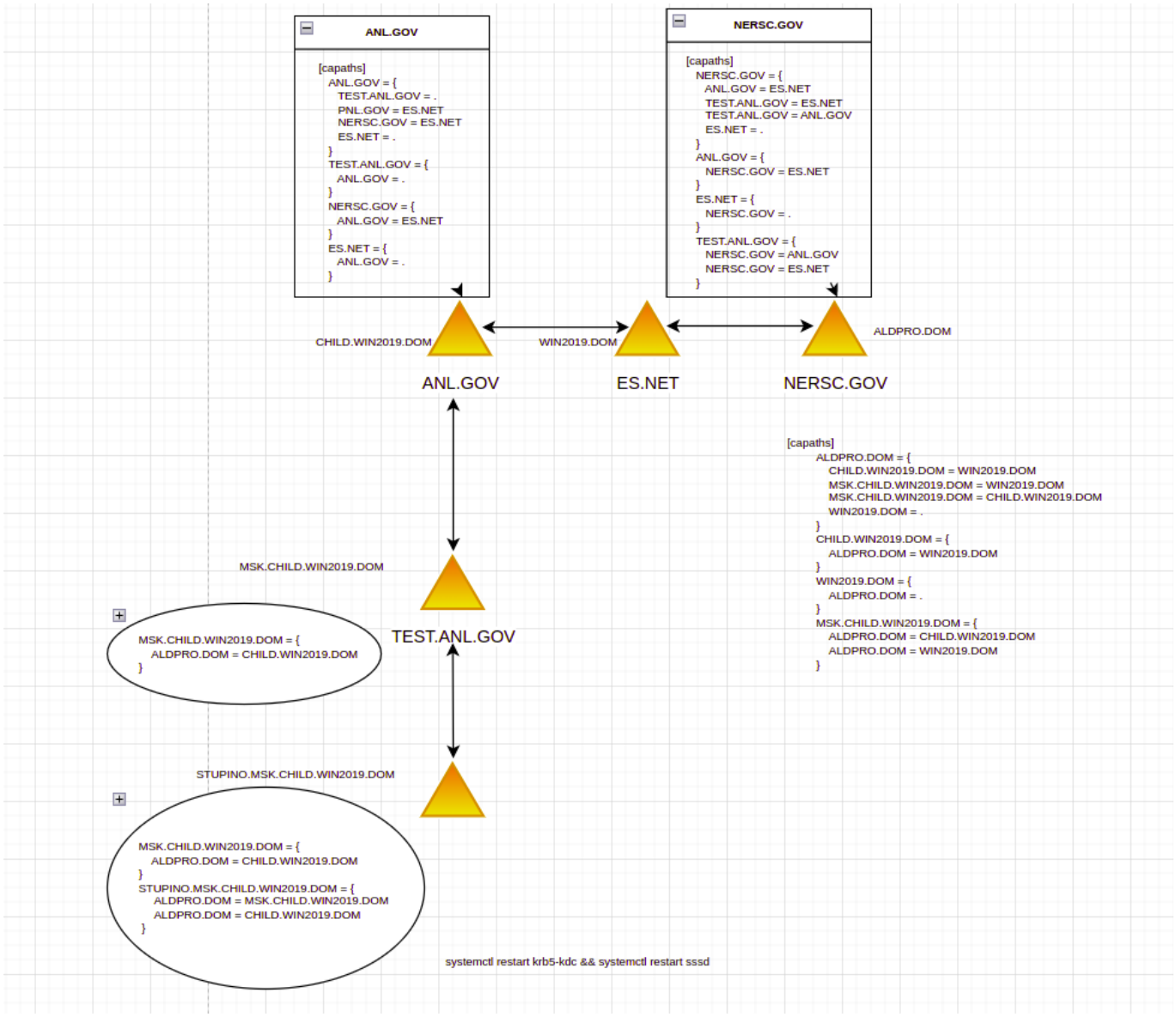
ALDPRO.DOM = MSK.CHILD.WIN2019.DOM

ALDPRO.DOM = CHILD.WIN2019.DOM

}
```



Пример визуализации официальной статьи (https://web.mit.edu/kerberos/krb5-1.5/krb5-1.5.4/doc/krb5-admin/capaths.html)



Проверки работоспособности доверительных отношений

3.8.12. Проверка работоспособности доверия (id-идентификация)

Два основных типа запросов, которые может выполнять клиент - это поиск идентификационных данных (id) и аутентификация (login). Для пользователей IPA поиск идентификационных данных представляет собой обычный поиск по протоколу LDAP **на IPA-сервере**, а аутентификация выполняется с помощью внутреннего инструмента, подобного kinit, также подключающегося к IPA-серверу.

Доверенные пользователи MS AD (Trusted AD users) работают по-другому. Поиск идентификационных данных (id) с клиентских компьютеров подключается к IPA-серверу с помощью расширенной операции LDAP. Плагин extdom сервера IPA запрашивает у

экземпляра SSSD, запущенного на сервере, информацию о пользователе AD, экземпляр SSSD выполняет поиск на сервере MS AD с использованием протокола LDAP и передает данные обратно клиенту IPA. Для запросов аутентификации на основе пароля (**login**) клиенты IPA подключаются **непосредственно к серверам AD** с помощью Kerberos.

Важно помнить, что во время проверки подлинности должен быть задан правильный набор групп. Поскольку это требование существует, запрос на проверку подлинности также должен выполнить поиск идентификатора (обычно операцию initgroups) перед проверкой подлинности:

1. Убедиться, что все ALD Pro контроллеры отображаются при выполнении команды **ipa trustconfig-show**

```
#Выполнить аутентификацию
kinit admin
#Показать какие контроллеры домена могут обрабатывать Trust с Active
 ↪Directory
ipa trustconfig-show
root@alddc01:~# ipa trustconfig-show
Домен: alddomain.lan
Идентификатор безопасности: S-1-5-21-1307086432-2724870100-1147875473
Имя NetBIOS: ALDDOMAIN
GUID домена: 7a522ccc-a0d7-4eac-a46a-46b12c93fa0e
Резервная основная группа: Default SMB Group
Агенты отношений доверия AD IPA: alddc01.alddomain.lan alddcXX.alddomain.lan
Контроллеры отношений доверия AD IPA: alddc01.alddomain.lan alddcXX.alddomain.
 ↪lan
#Показать созданный траст
ipa trust-find windomain.lan
#Показать Направление отношения доверия
ipa trust-show windomain.lan
```

Если контроллер ALD Pro не указан в списке, то требуется проверить наличие ошибок в логах на проблемном контроллере

```
root@alddc02:~# grep -insRH --color=auto "ipa-ad" /var/log
/var/log/ipaserver-install.log:162:2023-05-11T14:56:28Z DEBUG The ipa-adtrust-
 ↪install command failed, exc
eption: ScriptError: Unrecognized error during check of admin rights: 'member_
 ↪user'
```

В данном случае нужно вручную повторно запустить команду **ipa-adtrust-install** на alddc02 контроллере.

2. Проверка топологии репликации суффикса

```
root@alddc01:~# ipa topologysuffix-verify --help
Usage: ipa [global-options] topologysuffix-verify NAME [options]

Проверка топологии репликации для суффикса.

Проверки, которые выполняются:
1. проверка того, не отключена ли топология (иначе говоря, имеются ли пути
 ↪репликации между всеми серверами).
2. проверка того, не превышено ли рекомендованное количество соглашений о
 ↪репликации между серверами.
Options:
-h, --help  show this help message and exit
#
root@alddc01:~# ipa topologysuffix-verify domain
----------------------------------------------------------------------
Топология репликации суффикса "domain" соответствует требованиям.
----------------------------------------------------------------------
```

3. Проверка работоспособности траста с помощью команды **id** (**Требуется выполнить на каждом ALD Pro (FreeIPA) контроллере** домена)

SSSD предоставляет две основные функции: получение информации о пользователях и аутентификацию пользователей. Каждый из них подключается к разным системным API и должен рассматриваться отдельно. Однако успешная аутентификация (**login**) может быть выполнена **только тогда, когда может быть получена информация о пользователе (id).** Поэтому, если аутентификация не работает, важно убедиться, что можно, по крайней мере, получить информацию о пользователе с помощью id.

```
#Очистка всего доступного кеша и перезапуск службы sssd
rm -f /var/lib/sss/db/* /var/lib/sss/mc/* && systemctl restart sssd
#Получение информации о пользователе в домене windomain.lan
id 'windomain\administrator'
#Или
id administrator@windomain.lan

#Пример результата
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
root@alddc01:~# id administrator@windomain.lan
uid=1131400500(administrator@windomain.lan)
 ↪gid=1131400500(administrator@windomain.lan)
 ↪группы=1131400500(administrator@windomain.lan),1131400520(group policy
 ↪creator
owners@windomain.lan),1131400513(domain users@windomain.lan),
 ↪1131400519(enterprise admins@windomain.lan),1131400518(schema
 ↪admins@windomain.lan),1131400512(domain admi
ns@windomain.lan)
```

3.8.13. Проверка работоспособности доверия (Kerberos)

Ниже представлены примеры запросов Kerberos-билетов

https://web.mit.edu/kerberos/krb5-1.12/doc/user/user_commands/kinit.html

Запрос Kerberos-билета для примера из домена windomain.lan

Запрос KINIT (kinit получает и кэширует первоначальный билет, предоставляющий право на получение билета для принципала).

```
root@alddc01:~# KRB5_TRACE=/dev/stderr kinit administrator@windomain.lan
[30804] 1698829046.855690: Resolving unique ccache of type KEYRING
[30804] 1698829046.855691: Getting initial credentials for
 ↪administrator@windomain.lan
[30804] 1698829046.855693: Sending unauthenticated request
[30804] 1698829046.855694: Sending request (195 bytes) to windomain.lan
[30804] 1698829046.855695: Initiating TCP connection to stream 192.168.88.
 ↪85:88
[30804] 1698829046.855696: Sending TCP request to stream 192.168.88.85:88
[30804] 1698829046.855697: Received answer (198 bytes) from stream 192.168.88.
 ↪85:88
[30804] 1698829046.855698: Terminating TCP connection to stream 192.168.88.
 ↪85:88
[30804] 1698829046.855699: Response was from master KDC
[30804] 1698829046.855700: Received error from KDC: -1765328359/Additional
 ↪pre-authentication required
[30804] 1698829046.855703: Preauthenticating using KDC method data
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
[30804] 1698829046.855704: Processing preauth types: PA-PK-AS-REQ (16), PA-PK-
↪AS-REP_OLD (15), PA-ETYPE-INFO2 (19), PA-ENC-TIMESTAMP (2)
[30804] 1698829046.855705: Selected etype info: etype aes256-cts, salt "WIN-
↪F8I3I8FPJ70Administrator", params ""
[30804] 1698829046.855706: PKINIT client has no configured identity; giving
↪up
[30804] 1698829046.855707: PKINIT client has no configured identity; giving
↪up
[30804] 1698829046.855708: Preauth module pkinit (16) (real) returned: 22/
↪Недопустимый аргумент
Password for administrator@windomain.lan:
```

KLIST перечисляет участника Kerberos и билеты Kerberos, хранящиеся в кэше учетных данных или ключи, хранящиеся в файле keytab.

https://web.mit.edu/kerberos/krb5-1.12/doc/user/user_commands/klist.html

```
root@alddc01:~# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_6c40ahD
Default principal: Administrator@WINDOMAIN.LAN

Valid starting       Expires              Service principal
24.10.2023 13:48:50  24.10.2023 23:48:50  krbtgt/WINDOMAIN.LAN@WINDOMAIN.LAN
        renew until 25.10.2023 13:48:44
```

Запрос KVNO (kvno получает служебный билет для указанных участников Kerberos)

https://web.mit.edu/kerberos/krb5-devel/doc/user/user_commands/kvno.html

```
root@alddc01:~# kvno -S CIFS windc01.windomain.lan
CIFS/windc01.windomain.lan@WINDOMAIN.LAN: kvno = 3
root@alddc01:~#
root@alddc01:~# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_6c40ahD
Default principal: Administrator@WINDOMAIN.LAN

Valid starting       Expires              Service principal
24.10.2023 14:17:17  24.10.2023 23:48:50  CIFS/windc01.windomain.
↪lan@WINDOMAIN.LAN
24.10.2023 13:48:50  24.10.2023 23:48:50  krbtgt/WINDOMAIN.LAN@WINDOMAIN.LAN
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
        renew until 25.10.2023 13:48:44
```

3.8.14. Дополнительные проверки

```
#Выполняем аутентификацию пользователя из домена AD DS, получаем TGT-билет
 ↪от контроллера AD DS
kinit administrator@windomain.lan
#Получаем для пользователя Cross realm TGT билет у контроллера AD DS для
 ↪сквозной аутентификации на контроллерах ALD Pro
kvno krbtgt/ALDDOMAIN.LAN@WINDOMAIN.LAN
#Используя Cross realm TGT билет получаем у контроллера ALD Pro сервисный
 ↪билет для аутентификации на хосте из домена ALD Pro с fqdn именем alddc01.
 ↪alddomain.lan
kvno host/alddc01.alddomain.lan@ALDDOMAIN.LAN

#Получаем для пользователя Cross realm TGT билет у контроллера ALD Pro для
 ↪сквозной аутентификации на контроллерах Active Directory
kvno krbtgt/WINDOMAIN.LAN@ALDDOMAIN.LAN
#Используя Cross realm TGT билет получаем у контроллера Active Directory
 ↪сервисный билет для аутентификации на хосте из домена Active Directory
kvno host/windc01.windomain.lan@WINDOMAIN.LAN

#Конечный результат
root@alddc01:~# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_B4jH9CO
Default principal: Administrator@WINDOMAIN.LAN

Valid starting       Expires              Service principal
24.10.2023 14:41:04  25.10.2023 00:22:09  host/windc01.windomain.
 ↪lan@WINDOMAIN.LAN
24.10.2023 14:39:55  25.10.2023 00:22:09  krbtgt/WINDOMAIN.LAN@ALDDOMAIN.LAN
24.10.2023 14:28:13  25.10.2023 00:22:09  host/alddc01.alddomain.
 ↪lan@ALDDOMAIN.LAN
24.10.2023 14:25:15  25.10.2023 00:22:09  krbtgt/ALDDOMAIN.LAN@WINDOMAIN.LAN
24.10.2023 14:22:09  25.10.2023 00:22:09  krbtgt/WINDOMAIN.LAN@WINDOMAIN.LAN
        renew until 25.10.2023 14:22:04
```

3.8.14.1. Как работает кросс-доверительная аутентификация Kerberos (Kerberos cross-trust authentication)

Чтобы пройти аутентификацию в службе через доверительное управление с использованием Kerberos, необходим реферал (также известный как билет на получение реферального билета [TGT]). Это билет, запрошенный у локального контроллера домена (DC) для стороннего домена. Чтобы продемонстрировать, как выполняются запросы тикетов в разных доверительных системах, в этом разделе основное внимание уделяется semperis (лабораторный лес).

TGT (Ticket Granting Ticket) = это билет, выдаваемый контроллером домена (DC) после успешной аутентификации пользователя. Он позволяет запрашивать билеты на обслуживание (Service Tickets, ST) для доступа к конкретным сервисам в домене.

TGS(Ticket Granting Service) - это компонент KDC, который выдает запрос на обслуживание, когда участник запрашивает подключение к службе Kerberos. Изначально должен быть билет на предоставление доступа (TGT) для домена (MS AD), прежде чем будет выдан билет на обслуживание в этом домене MS AD.

PAC(Privilege Attribute Certificate) = Сертификат атрибута привилегий. Содержится в TGT, скопирован в служебный билет. Сообщает службе, каким пользователем вы являетесь и в каких группах состоите, на основе идентификаторов безопасности (SID).

Пример SID: S-1-5-21-3286968501-24975625-1618430583-512



1. Пользовательский NTLM hash для запроса TGT
2. TGT зашифрованный krbtgt hash
3. Запрос TGS для server.ad.local
4. TGT зашифрованный Inter Realm trust key krbtgt/MSK.CHILD.ALD.DOM@MSK.CHILD.ALD.DOM
5. Клиент запрашивает TGT krbtgt/CHILD.ALD.DOM@MSK.CHILD.ALD.DOM
6. Cross-realm ticket granting ticket krbtgt/CHILD.ALD.DOM@MSK.CHILD.ALD.DOM
7. С помощью билета krbtgt/CHILD.ALD.DOM@MSK.CHILD.ALD.DOM клиент запрашивает билет krbtgt/ALD.DOM@CHILD.ALD.DOM для пересечения границ (cross-realm ticket)
8. Cross-realm ticket granting ticket krbtgt/ALD.DOM@CHILD.ALD.DOM
9. С помощью билета krbtgt/ALD.DOM@CHILD.ALD.DOM клиент запрашивает билет krbtgt/AD.LOCAL@ALD.DOM для пересечения границ (cross-realm ticket)
10. Cross-realm ticket granting ticket krbtgt/AD.LOCAL@ALD.DOM
11. С помощью билета krbtgt/AD.LOCAL@ALD.DOM, выданного KDC области ALD.DOM, клиент запрашивает у KDC области AD.LOCAL (TGS) билет для участника обслуживания (service principal) в области AD.LOCAL.
12. TGS ticket granting service билет service/server@AD.LOCAL, требовалось получить три промежуточных (cross-realm tickets) билета для разных областей.

После этого кэш учетных данных содержит заявки для:

- krbtgt/MSK.CHILD.ALD.DOM@MSK.CHILD.ALD.DOM,
- krbtgt/CHILD.ALD.DOM@MSK.CHILD.ALD.DOM,
- krbtgt/ALD.DOM@CHILD.ALD.DOM,
- krbtgt/AD.LOCAL@ALD.DOM и service/hostname@AD.LOCAL.

13. TGS ticket granting service билет service/server@AD.LOCAL (AP REQ включающий TGS для доступа)
14. AP REP (SERVER считывает учетные данные безопасности пользователя и соответствующим образом создает токен доступа)

Поддержка UPN (User Principal Names) для доверенных доменов (trusted_domains)

Основное имя пользователя (UPN) в MS AD является основной формой обращения к пользователям. UPN имеет структуру «**имя пользователя@суффикс**», где как имя пользователя, так и части суффикса могут различаться. По умолчанию суффикс совпадает с доменным именем MS AD, но администраторы MS AD могут создавать дополнительные суффиксы имен и связывать их с конкретными пользователями. Эти дополнительные UPN для пользователей затем могут использоваться для проверки подлинности Kerbers в доменах MS AD.

Альтернативные UPN часто используются, когда несколько компаний с развертываниями MS AD объединяются и хотят предоставить единое пространство имен для входа в систему.

Цель - разрешить использование альтернативных UPN, связанных с пользователями MS AD, при доступе к ресурсам в домене ALD Pro.

Пример:

Пользователь MS AD хочет войти в систему, используя свое **имя пользователя@EXAMPLE** (user pricipal), даже если его домен Active Directry назван REGION.EXAMPLE.COM.

3.8.15. Включение поддержки UPN на стороне клиента

SSSD уже поддерживает вход в систему с помощью UPN, запрашивая у KDC принятие корпоративных имен для входа. По умолчанию использование корпоративных участников **отключено**, поэтому в sssd.conf необходимо добавить **krb5_use_enterprise_principal = True** чтобы включить его.

```
root@pc-1:~# nano /etc/sssd/sssd.conf

[domain/windomain.lan]

id_provider = ipa
ipa_server = _srv_, alddc01.windomain.lan
ipa_domain = ald.dom
ipa_hostname = pc-1.windomain.lan
auth_provider = ipa
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
chpass_provider = ipa
access_provider = ipa
cache_credentials = True
ldap_tls_cacert = /etc/ipa/ca.crt
krb5_store_password_if_offline = True
krb5_use_enterprise_principal = True
```

3.8.16. Проверка поддержки UPN на стороне сервера

IPA KDC действительно понимает несколько доменов, связанных с доверенным лесом AD. Однако, поскольку информация о суффиксах имен, связанных с лесом, недоступна, он не может учитывать их при обработке имен входа enteprise для выдачи ссылок в правильную область. Необходимо добавить поддержку, позволяющую ALD Pro (FreeIPA) KDC искать суффиксы имен, связанные с доверенным лесом.

Первым делом необходимо убедиться, что ALD Pro контроллер видит необходимый суффикс

```
#Выполняем аутентификацию
kinit admin

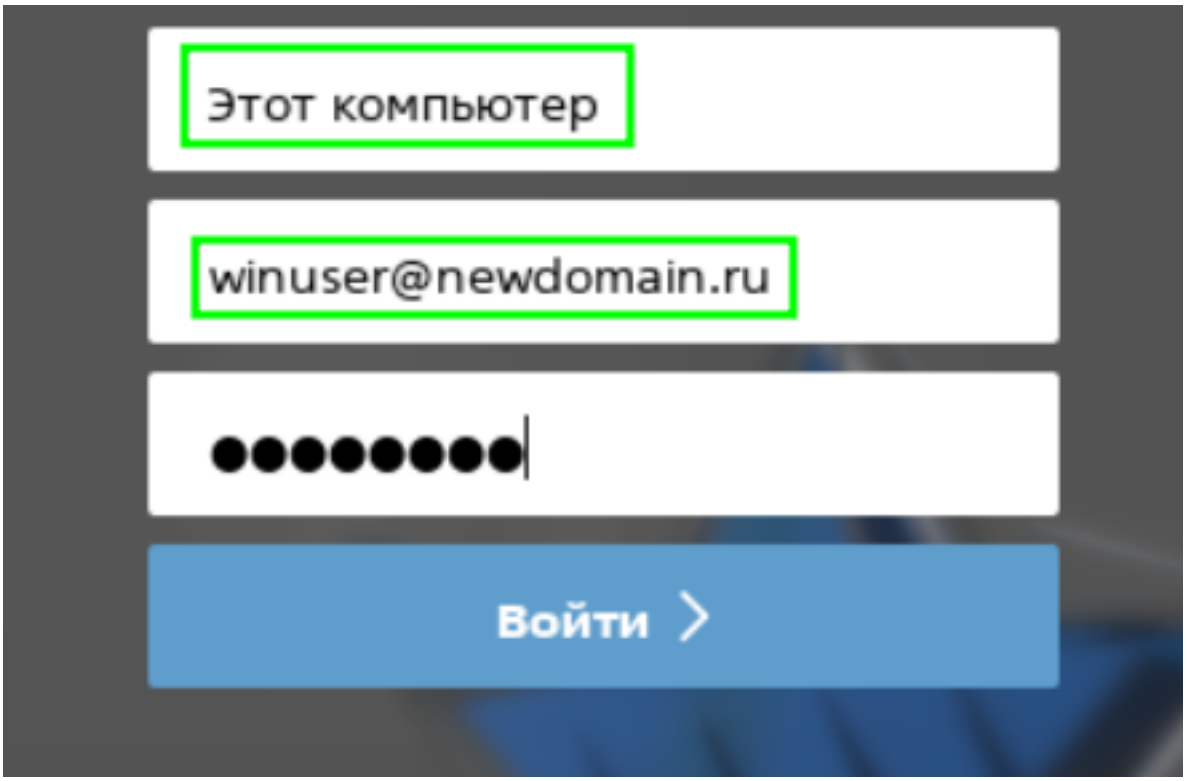
#Обновляем список надежных доменов
ipa trust-fetch-domains windomain.lan

#Получить информацию по домену
ipa trustdomain-find

#Обновляем информацию по Trust windomain.lan
ipa trust-show windomain.lan

#Пример результата
root@alddc01:~# ipa trust-show windomain.lan
Имя области (realm): windomain.lan
Имя домена NetBIOS: WINDOMAIN
Идентификатор безопасности домена: S-1-5-21-292663598-2229028806-4201728183
Направление отношения доверия: Двустороннее отношение доверия
Тип отношения доверия: Домен Active Directory
Суффиксы UPN: newdomain.ru
```

3.8.17. Проверка работоспособности UPN через графику



3.8.18. Проверка работоспособности UPN через SSH

```
ssh winuser@newdomain.lan@pc-1
winuser@windomain.lan@pc-1:~$ whoami
winuser@windomain.lan
winuser@windomain.lan@pc-1:~$ id winuser@newdomain.lan
uid=1524001110(winuser@windomain.lan) gid=1524001110(winuser@windomain.lan)
 ↪группы=1524001110(winuser@windomain.lan),1524000513(domain users@windomain.
 ↪lan)
```

Администратор может отключить автоматическое обнаружение серверов и сайтов MS AD в доверенном домене MS AD и вместо этого вручную перечислить серверы, сайты или и то, и другое, чтобы ограничить список серверов MS AD, с которыми взаимодействует SSSD. Например, это позволит избежать обращения к сайтам, которые недоступны.

Эта процедура описывает ручную настройку серверов MS AD, к которым подключается SSSD, путем редактирования файла **/etc/sssd/sssd.conf**.

Если SSSD-клиенты напрямую подключены к домену MS AD, процедура выполняется на всех клиентах.

В настройке ограничение доступа к контроллерам домена MS AD(DCs) или сайтам также настраивает SSSD-клиенты для подключения к определенному серверу или сайту для проверки подлинности.

Если SSSD-клиенты находятся в домене ALD Pro (FreeIPA), который находится в доверительном управлении с MS AD, процедура выполняется только на сервере управления идентификацией ALD Pro (FreeIPA).

Важно убедиться, что у ALD Pro (FreeIPA) домена есть **отдельный раздел [domain]** в **/etc/sssd/sssd.conf**. Заголовки разделов доверенного домена соответствуют этому шаблону:

```
[domain/ald.example.com/ad.example.com]
```

3.8.19. Настройка сервера ALD Pro (FreeIPA) на определенный сайт MS AD (id, logon)

```
[domain/alddomain.lan/windomain.lan]
ad_site = Default-First-Site-Name
```

В этой настройке ограничение (Restricting) сайтов MS AD выполняется **только для** идентификации (команда **id**), для аутентификации (**logon**) в указанном сайте MS AD требуется выполнить вышеуказанную настройку на **каждом клиенте**.

3.8.20. Настройка клиента на определенный сайт MS AD (id, logon)

```
[[domain/alddomain.lan]
id_provider = ipa
ipa_server = _srv_, alddc01.alddomain.lan
ipa_domain = alddomain.lan
ipa_hostname = alddc01.alddomain.lan
auth_provider = ipa
chpass_provider = ipa
access_provider = ipa
cache_credentials = True
ldap_tls_cacert = /etc/ipa/ca.crt
krb5_store_password_if_offline = True
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
debug_level = 9
[sssd]
services = ifp
domains = alddomain.lan
[nss]
homedir_substring = /home
[pam]
[sudo]
[autofs]
[ssh]
[pac]
[ifp]
allowed_uids = 0, 33, 114, fly-dm, ipaapi
[secrets]
[session_recording]
[domain/alddomain.lan/windomain.lan]
ad_site = Default-First-Site-Name
```

Расположение конфигурационных файлов

```
SSSD
/etc/sssd/sssd.conf
PAM
/etc/pam.d/system-auth or
/etc/pam.d/system-auth-ac (with authconfig)
NSS
/etc/nsswitch.conf
DNS
/etc/resolv.conf
Samba
/etc/samba/smb.conf
Winbind
/etc/security/pam_winbind.conf
Kerberos
/etc/krb5.conf
```

3.8.21. Настройка журналов отладки для доменов SSSD

Каждый домен устанавливает свой собственный уровень журнала отладки. Увеличение уровня журнала может предоставить больше информации о проблемах с SSSD или с конфигурацией домена.

Чтобы изменить уровень ведения журнала, существует 2 способа:

A) Установить параметр **debug_level** для каждого раздела в файле /etc/sssd/sssd.conf, для которого будут создаваться дополнительные журналы, перезапустите сервис SSSD.

```
systemctl restart sssd.service
```

Данный способ **будет работать даже после перезапуска сервиса SSSD**.

Пример:

```
[domain/alddomain.lan]
debug_level = 9
[sssd]
debug_level = 9
[nss]
debug_level = 9
[pam]
debug_level = 9
```

B) Установить дополнительный пакет и включить необходимый уровень логирования. **Все изменения применяются «на лету» ко всем разделам**, вносить вручную в sssd.conf файл не требуется.

Данный способ работает **до перезапуска службы SSSD**.

```
apt update && apt install sssd-tools

sss_debuglevel 6
```

3.8.22. Описание уровней логирования SSSD

Описание уровней сообщений в журналах SSSD:

0 Фатальные сбои: Любые сбои, которые могли бы помешать запуску SSSD или привести к его остановке.

1 Критические сбои: Ошибка, которая не останавливает SSSD, но указывает на то, что как минимум одна основная функция не будет работать должным образом.

2 Серьезные сбои: Ошибка, объявляющая, что определенный запрос или операция завершился неудачей.

3 Мелкие сбои: Это ошибки, которые могли бы привести к сбою операции с уровнем 2.

4 Настройки конфигурации: Сообщения, связанные с настройками конфигурации.

5 Данные о функции: Информация о функциях и данных, связанных с ними.

6 Сообщения трассировки для функций операций: Сообщения, предназначенные для отслеживания выполнения определенных операций.

7 Сообщения трассировки для внутренних управляющих функций: Сообщения, связанные с внутренними функциями управления SSSD.

8 Содержимое внутренних переменных функций, которое может быть интересным: Отладочная информация, связанная с переменными внутри функций.

9 Информация с очень низким уровнем трассировки: Экстремально низкоуровневая отладочная информация.

3.8.23. Описание SSSD журналов событий

SSDD использует ряд файлов журнала для представления информации о своей работе, расположенных в каталоге **/var/log/sssd/**.

SSSD создает файл журнала для каждого домена, а также файл sssd_pam.log и sssd_nss.log.

krb5_child.log: (short-lived helper process) содержит информацию, связанную с аутентификацией Kerberos, которая используется для безопасной аутентификации в сетевой среде.

ldap_child.log: (short-lived helper process) Этот журнальный файл связан с службами LDAP (Lightweight Directory Access Protocol), участвующего в обмене данными с сервером LDAP (MS AD).

selinux_child.log: (short-lived helper process) SELinux (Security-Enhanced Linux) - это функция безопасности в Linux. Этот журнальный файл содержит информацию, связанную с событиями и активностью, связанной с SELinux.

sssd_<ALD Domain Name>.log: Эти журнальные файлы специфичны для службы SSSD (System Security Services Daemon) и обычно именуются именем домена MS AD, с которым взаимодействует SSSD.

sssd_ifp.log: Этот журнальный файл относится к службе InfoPipe (IFP) в SSSD, обеспечивает интерфейс общей шины, доступный по системной шине.

sssd.log: Файл журнала для SSSD, взаимодействующего со своими процессами-ответчиками.

sssd_nss.log: Этот журнальный файл фокусируется на компоненте Name Service Switch (NSS) SSSD, которая обрабатывает разрешение имен пользователей и групп (выполнение команды id).

sssd_pac.log: Этот журнальный файл содержит информацию, связанную с Privilege Attribute Certificate (PAC) в контексте SSSD и аутентификации. Определяет, как SSSD работает с Kerberos для управления пользователями и группами MS AD.

sssd_pam.log: Этот журнальный файл связан с службой Pluggable Authentication Module (PAM) в SSSD, отвечающей за аутентификацию и авторизацию.

sssd_ssh.log: Этот журнальный файл специфичен для действий, связанных с SSH в

рамках SSSD, особенно в отношении аутентификации SSH.

Кроме того, в файле /var/log/secure регистрируются сбои аутентификации и причина сбоя.

```
### Все тесты необходимо выполнять на контроллере домена ALD Pro(FreeIPA)
#Установка sssd-tools на контроллер домена
apt update && apt install sssd-tools

#Проверка сервисов контроллера домена ALD Pro (FreeIPA)
ipactl status
#Проверка конфигурационного файла /etc/sssd/sssd.conf на ошибки
sssctl config-check

#Проверка доступности Winbind
wbinfo --ping
#Проверка  NETLOGON соединения с контроллером ALD Pro (FreeIPA)
wbinfo --ping-dc
#Показать к какому контроллеру Active Directory подключен Winbind
wbinfo --dsgetdcname=windomain.lan
#Проверка активных подключений через Winbind
wbinfo --online-status

#Проверка работоспособности службы SSSD
sssd -d4 -i
#Вывести список доменов которые видет SSSD
sssctl domain-list
#Проверка активных подключений через SSSD(предварительно выполните id
 ↪Administrator@windomain.lan)
sssctl domain-status windomain.lan

# Включение уровня логирования
sss_debuglevel 6
# Обнуление журналов по необходимости
truncate -s 0 /var/log/sssd/*
#Удаление всего кеша с контроллера домена и перезапуск службы sssd
rm -f /var/lib/sss/db/* /var/lib/sss/mc/* && systemctl restart sssd

#identity lookups(id) проверка способ 1
id winuser@windomain.lan
#identity lookups(id) проверка способ 2
id 'windomain\winuser'
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
#Все ошибки id будут фиксироваться в 2 журнала sssd_nss.log и sssd_<ALD
 ↪Domain Name>.log
#Команда отображает пользовательские данные, доступные через NSS и ответчик
 ↪Infopipe для интерфейса D-Bus. Отображаемые данные показывают, авторизован
 ↪ли пользователь для входа в систему с помощью служб system-auth PAM.
sssctl user-checks winuser@windomain.lan
```

3.8.24. Настройка журналов отладки

Вся конфигурация Samba располагается в двух местах, стандартный файл конфигурации располагается по пути ./etc/samba/smb.conf, этот файл не рекомендуется изменять, при проблемах с доверием в некоторых случаях потребуется повторно выполнить команду **ipa-adtrust-install** которая **перетрет** все внесенные изменения в указанный файл, а также обнулит и запишет из шаблона по умолчанию параметры реестра в файл /var/lib/samba/registry.tdb, так же команду **ipa-adtrust-install** потребуется сделать, если база данных, содержащая реестр параметров для Samba (/var/lib/samba/registry.tdb), была удалена.

```
#root@dc1:/var/lib/samba# ls -lh
итого 2,2M
-rw-------  1 root root          412K ноя 14 16:20 account_policy.tdb
-rw-r--r--  1 root root           225 ноя 17 10:41 browse.dat
drwxr-xr-x  4 root root          4,0K ноя 13 15:52 DriverStore
-rw-------  1 root root          416K ноя 14 17:33 group_mapping.tdb
-rw-------  1 root root           12K ноя 17 09:15 netsamlogon_cache.tdb
drwxr-xr-x 11 root root          4,0K ноя 13 15:52 printers
drwxr-xr-x  2 root root          4,0K ноя 14 10:33 printing
drwxr-xr-x  3 root root          4,0K ноя 13 16:04 private
-rw-------  1 root root          516K ноя 14 17:32 registry.tdb
-rw-------  1 root root          412K ноя 14 16:20 share_info.tdb
drwxrwx--T  2 root sambashare    4,0K ноя 13 15:52 usershares
-rw-------  1 root root           32K ноя 17 08:47 winbindd_cache.tdb
-rw-r--r--  1 root root          412K ноя 14 17:45 winbindd_idmap.tdb
drwxr-x---  2 root winbindd_priv 4,0K ноя 17 08:47 winbindd_privileged
```

account_policy.tdb Основное предназначение заключается в хранении настроек политики учетных записей для пользователей на сервере Samba. Эти настройки включают параметры, связанные с политикой паролей, блокировкой учетных записей и другие

параметры безопасности.

browse.dat Файл в директории /var/lib/samba в Samba используется для хранения информации о браузере (Browser Information). Этот файл содержит данные о доступных ресурсах и службах в сети, которые могут быть предоставлены сервером Samba.

group_mapping.tdb Файл в директории /var/lib/samba в Samba используется для хранения отображений между группами в системе Samba и соответствующими группами в сетевой службе, например, в Microsoft Active Directory.

netsamlogon_cache.tdb Файл в директории /var/lib/samba в Samba представляет собой базу данных TDB, которая используется для кэширования информации, связанной с обработкой запросов NetLogon в рамках протокола аутентификации в сетевых службах, таких как Microsoft Active Directory.

registry.tdb - это файл TD (Trivial Database), используемый Samba, который представляет собой реализацию протокола Server Message Block (SMB) с открытым исходным кодом. Файл registry.tdb специально хранит данные конфигурации в формате ключ-значение, аналогичном кусту реестра Windows.

В контексте Samba файл registry.tdb **используется для хранения параметров конфигурации, относящихся к реестру Windows. Сюда входит информация о системе, сетевых настройках и других параметрах конфигурации, необходимых для функционирования сервера Samba.**

share_info.tdb Файл в директории /var/lib/samba в Samba представляет собой базу данных TDB, используемую для хранения информации о совместно используемых ресурсах (шарах) в Samba.

winbindd_cache.tdb Файл в директории /var/lib/samba в Samba представляет собой базу данных TDB, используемую для кэширования данных и запросов, выполняемых службой Winbind в рамках протокола аутентификации и авторизации в среде Samba.

winbindd_idmap.tdb Файл в директории /var/lib/samba в Samba представляет собой базу данных TDB, используемую для хранения информации о сопоставлении (маппинге) идентификаторов безопасности (SID) и POSIX UID/GID в процессе аутентификации и авторизации через Winbind.

Для просмотра содержимого файлов XXXX.tdb в Samba используется утилита tdbtool. Пример команды для просмотра содержимого registry.tdb:

tdbtool registry.tdb dump

Эта команда выводит содержимое registry.tdb в формате ключ-значение. Важно убедиться, что каманда выполняется с правами пользователя, достаточными для чтения файла registry.tdb.

Для более удобного просмотра всех настроек Samba, **включая реестр**, можно использовать команду **net conf list**

Команда net conf list в Samba используется для отображения текущей конфигурации Samba. Она выводит различные параметры и настройки, связанные с работой Samba, включая параметры глобальной секции smb.conf, информацию о доменах, настройки Kerberos и другие параметры.

Более подробную информацию о реестре можно найти по адресу

https://www.samba.org/~obnox/presentations/linux-kongress-2008/lk2008-obnox.pdf

Каждая служба устанавливает свой собственный уровень журнала отладки. Увеличение уровня журнала может предоставить больше информации о проблемах с Winbind,Samba(smbd) или nmbd

Чтобы изменить уровень ведения журнала, существует 2 способа:

1. Увеличение уровня ведения журнала winbind или samba без перезапуска служб

```
#Проверяем текущие настройки для сервисов smdb и winbind
smbcontrol smbd debuglevel
smbcontrol winbind debuglevel
#smbcontrol nmbd debuglevel

#Устанавливаем уровень логирования(на лету) 100 для сервисов smdb и winbind
smbcontrol smbd debug 100
smbcontrol winbind debug 100
#smbcontrol nmbd debug 100
```

Настройка журналов без перезапуска демона также полезно в тех случаях, когда перезапуск службы временно устраняет проблему на неопределенный период времени. Недостатком является то, что увеличение количества журналов после возникновения проблемы может привести к отсутствию информации, но это не требуется в тех случаях, когда известно, как воспроизвести проблему.

2. Увеличение уровня ведения журнала winbind или samba с перезапуском служб

```
#Остановите службы smb и winbind.
systemctl stop smbd.service winbind.service

#Установите уровень логирования для служб smb и winbind
net conf setparm global 'log level' 100

#Удалите предыдущие журналы samba
rm /var/log/samba/log.*
#Запустите службы smb и winbind
systemctl start smbd.service winbind.service
#Проведите необходимые тесты и создайте архив с журналами
tar -cvf debugging-smb_winbind.tar  /var/log/samba/log.*
```

Выключение режима повышенного журналирования (Disable debugging)

```
#Остановите службы smb и winbind.
systemctl stop smbd.service winbind.service
#Установите уровень логирования для служб smb и winbind
net conf setparm global 'log level' 0
#Запустите службы smb и winbind
systemctl start smbd.service winbind.service
```

3. Так же можно интерективно смотреть, что происходит с winbind в момент старта службы для этого выполните поочередно команды ниже:

```
systemctl stop  winbind.service
winbindd -i -d 100
```

4. Если требуется повысить логирование только для определенного сервиса, в данном примере логирование включено «1» для всех сервисов, кроме winbind - для него включен уровень «100» . **/etc/samba/smb.conf**

```
### Added by IPA Installer ###
#         DO NOT EDIT         #
[global]
debug pid = yes
state directory = /var/lib/samba
cache directory = /var/lib/samba
include = registry
log level = 1 winbind:100

[gluster-aldpro-volume01]
comment = For samba share of volume aldpro-volume01
vfs objects = glusterfs
glusterfs:volume = aldpro-volume01
glusterfs:logfile = /var/log/samba/glusterfs-aldpro-volume01.%M.log
glusterfs:loglevel = 7
path = /
read only = no
guest ok = yes
~
~
~
```

```
smbcontrol winbind debuglevel
PID 26871: all:1 tdb:1 printdrivers:1 lanman:1 smb:1 rpc_parse:1 rpc_srv:1
 ↪rpc_cli:1 passdb:1 sam:1 auth:1 winbind:100 vfs:1 idmap:1 quota:1 acls:1
 ↪locking:1 msdfs:1 dmapi:1 registry:1 scavenger:1 dns:1 ldb:1 tevent:1 auth_
 ↪audit:1 auth_
json_audit:1 kerberos:1 drs_repl:1 smb2:1 smb2_credits:1 dsdb_audit:1 dsdb_
 ↪json_audit:1 dsdb_password_audit:1 dsdb_password_json_audit:1 dsdb_
 ↪transaction_audit:1 dsdb_transaction_json_audit:1 dsdb_group_audit:1 dsdb_
 ↪group_json_audit:1
```

3.8.25. Проблемы с конфигурационном файлом SSSD.conf

Проблема: не удается запустить SSSD.

Решение. SSSD требует, чтобы файл конфигурации был правильно настроен со всеми необходимыми записями, прежде чем демон запустится. Для запуска службы SSSD требуется по крайней мере один правильно настроенный домен. Без домена попытка запустить SSSD возвращает ошибку о том, что домены не настроены:

```
# sssd -d4 -i
```

(продолжение на следующей странице)

```
[sssd] [ldb] (3): server_sort:Unable to register control with rootdse!
[sssd] [confdb_get_domains] (0): No domains configured, fatal error!
[sssd] [get_monitor_config] (0): No domains configured.
Необходимо отредактировать файл /etc/sssd/sssd.conf и создать хотя бы один
↪домен.
```

SSSD также требует наличия по крайней мере одного доступного поставщика услуг, прежде чем он запустится. Если проблема связана с конфигурацией поставщика услуг, сообщение об ошибке указывает на то, что службы не настроены:

```
[sssd] [get_monitor_config] (0): No services configured!
```

Необходимо отредактировать файл /etc/sssd/sssd.conf и настроить по крайней мере одного поставщика услуг.

Важно: SSSD требует, чтобы поставщики услуг были настроены в виде списка, разделенного запятыми, в одной записи служб в файле /etc/sssd/sssd.conf. Если службы перечислены в нескольких записях, SSSD распознает только последнюю запись.

SSSD также требует, чтобы для /etc/sssd/sssd.conf были правильно установлены права собственности и разрешения. Если владелец или разрешения установлены неправильно, попытка запустить SSSD возвращает эти сообщения об ошибках:

```
[sssd] [confdb_ldif_from_ini_file] (0x0020): Permission check on config file
↪failed.
[sssd] [confdb_init_db] (0x0020): Cannot convert INI to LDIF [1]: [Operation
↪not permitted]
[sssd] [confdb_setup] (0x0010): ConfDB initialization has failed [1]:
↪Operation not permitted
[sssd] [load_configuration] (0x0010): Unable to setup ConfDB [1]: Operation
↪not permitted
[sssd] [main] (0x0020): Cannot read config file /etc/sssd/sssd.conf. Please
↪check that the file is accessible only by the owner and owned by root.root.
```

Необходимо установить правильное имя владельца и разрешения для файла /etc/sssd/sssd.conf:

```
chmod 600 /etc/sssd/sssd.conf
chown root:root /etc/sssd/sssd.conf
```

3.8.26. Отсутствие групп при выполнении команды id

Проблема: нет групп при выполнении команды id username@FQDN_WindowsDomain или членов группы с getent group.

Решение. Проверить количество объектов в домене MS AD

```
# В Домене Active directory запустить Powershell и выполнить команду ниже
(Get-ADObject -Filter *).count
```

Проверить диапазоны идентификаторов пользователей домена MS AD:

```
# Для вывода списка доменных пользователей и их SID в домене Active
 ↪Directory запустить Powershell и выполнить команду ниже
Get-ADUser -Filter * -Property SID | Select-Object Name, SID
```

Если количество объектов или последняя часть SID некоторых доменных пользователей MS AD превышает 200 000 – выполнить расширение диапазона:

```
#Показать текущие диапазоны (idrange) для всех доменов
# Произвести аутентификацию
kinit admin
#Вывести список доступных диапозонов
ipa idrange-find
#Изменить id_range для домена windomain.lan к примеру до 500 000
ipa idrange-mod WINDOMAIN.LAN_id_range --range-size=500000
#Удаление всего кеша с контроллера домена и перезапуск службы sssd
rm -f /var/lib/sss/db/* /var/lib/sss/mc/* && systemctl restart sssd
```

3.8.27. Долгое выполнение команды id

Проблема: Выполнение команды id занимает много времини или прерывается по таймауту.

Решение. Одной из причин может быть большая вложенность групп

```
#Выполните команду id с параметром -G(вывести все ID групп)- эта каманда
 ↪игнорирует вложенность групп
id -G  winuser@windomain.lan

#Если команда отрабатывает быстро то требуется добавить в существующую
 ↪секцию в /etc/sssd/sssd.conf на каждом контроллере домена -игнорирование
 ↪вложенных групп
[domain/alddomain.lan]
...
ignore_group_members = true
subdomain_inherit = ignore_group_members

#Выполнить очистку кеша и произвести перезапуск службы sssd
rm -f /var/lib/sss/db/* /var/lib/sss/mc/* && systemctl restart sssd
```

3.8.28. SSSD не удается подключиться к MS AD из-за ошибок с GSS-API

Проблема: поставщик удостоверений MS AD правильно настроен в файле sssd.conf, но SSSD не удается подключиться к нему с ошибками GSS-API.

Решение. SSSD может подключаться только к поставщику MS AD, используя его имя хоста. Если имя хоста не указано, SSSD-клиент не может разрешить IP-адрес хоста, и аутентификация завершается неудачей.

Например, при такой конфигурации:

```
[domain/ADEXAMPLE]
debug_level = 0xFFF0
id_provider = ad
ad_server = 172.16.0.1
ad_domain = example.com
krb5_canonicalize = False
```

SSSD-клиент возвращает этот сбой GSSAPI, и запрос аутентификации завершается

неудачей:

```
(Fri Jul 27 18:27:44 2012) [sssd[be[ADTEST]]] [sasl_bind_send] (0x0020): ldap_
↪sasl_bind failed (-2)[Local error]
(Fri Jul 27 18:27:44 2012) [sssd[be[ADTEST]]] [sasl_bind_send] (0x0080):
↪Extended failure message: [SASL(-1): generic failure: GSSAPI Error:
↪Unspecified GSS failure.  Minor code may provide more information (Cannot
↪determine realm for numeric host address)]
```

Чтобы избежать этой ошибки, необходимо установить для ad_server значение имени узла MS AD или использовать ключевое слово _srv_ для использования обнаружения службы DNS.

ALD Pro(FreeIPA) использует BIND в качестве интегрированного DNS-сервера. Если есть подозрения, что с DNS что-то не так, необходимо проверить журналы, сгенерированные BIND.

```
journalctl -u bind9-pkcs11.service
```

Если требуется создать tcp dump, необходимо воспользоваться командой:

```
tcpdump -i eth0 -w /home/${USER}/$(date +%Y-%m-%d_%H-%M)_$(hostname).pcap
```

№	Проблема	Решение

1	Не работает DNS resolving имен из новой подсети	Необходимо добавить новую подсеть в **trusted_network** на каждом контроллере домена ALD Pro (FreeIPA)
		/etc/bind/**ipa-ext.conf**
		Пример:
		`.....`
		`acl "trusted_network" {`
		`  localnets;`
		`  localhost;`
		`  192.168.88.0/24;`
		`  172.19.3.0/24;`
		`  172.19.4.0/24;`
		`  <НОВАЯ Подсеть>;`
		`};`

2	Не работают рекурсивные запросы	Необходимо включить дополнительные опции на каждом контроллере домена ALD Pro (FreeIPA)
		/etc/bind/**ipa-options-ext.conf**
		Пример:
		`allow-recursion { trusted_network; };`
		`allow-query-cache { trusted_network; };`

№	Проблема	Решение
	Ошибка 3221225485 при создании доверительных отношений: **ipa: ERROR: Ошибка обмена данными с сервером CIFS: код «3221225485», сообщение «An invalid parameter was passed to a service or function.» (оба значения могут быть «None»)**	Проверить, что параметры реестра /var/lib/samba/registry.tdb – существуют и не были удалены. Для проверки выполнить команду **net conf list**. Если вывод пустой или есть уверенность, что файл был поврежден, требуется повторно выполнить команду ipa-adtrust-instal, предварительно сделав копию файла конфигурацуии smb.conf **cp smb.conf{,_bkp}**, так как он будет перезаписан из шаблона.

3.8.29. Настройка игнорирования участников групп (ignore_group_members)

Извлечение информации о пользователях (id <username@<ADdomain>) и группах является трудоемкой операцией для демона служб системной безопасности (SSSD), особенно при развертывании ALD Pro с доверием к большому домену MS AD. Улучшить производительность можно, настроив, какую информацию и как долго SSSD извлекает из поставщиков удостоверений (identity providers).

3.8.29.1. Предварительное требование

Необходимы права root для редактирования конфигурационного файла **/etc/sssd/sssd.conf**.

3.8.29.2. Процедура

1. Открыть конфигурационный файл /etc/sssd/sssd.conf в текстовом редакторе.
2. Добавить следующие параметры в раздел [домен] для домена MS AD. Если доменного раздела для домена MS AD еще нет, необходимо создать его.

```
[domain/ald.example.com]
ignore_group_members = true
subdomain_inherit = ignore_group_members
...
```

3. Сохранить и закрыт файл /etc/sssd/sssd.conf на сервере.
4. Перезапустить службу SSSD, чтобы загрузить изменения конфигурации.

```
systemctl restart sssd
```

ignore_group_members

Наиболее трудоемкой операцией является загрузка групп, включая их участников. Обычно на начальном этапе важно, членом каких групп является пользователь (id aduser@ad_domain), а не какие участники входят в конкретные группы (getent group adgroup@ad_domain). При установке для параметра ignore_group_members значения **True**, все группы отображаются как пустые, таким образом загружается только информация о самих объектах группы, а не об их членах, что обеспечивает значительное повышение производительности. Важно обратить внимание, что идентификатор aduser@ad_domain все равно вернет все правильные группы.

subdomain_inherit_inherit

Вышеуказанные параметры могут быть переданы в конфигурацию доверенных доменов MS AD. На данный момент единственным поддерживаемым методом является использование опции subdomain_inherit в разделе домена sssd.conf. Имена любого из двух приведенных выше параметров могут быть указаны в качестве значения subdomain_inherit, и они будут применяться как к основному домену (IPA), так и к поддомену MS AD.

3.8.30. Настройка таймаута конфигурации для плагина ipa-extdom на ALD Pro (FreeIPA)-серверах

Клиенты ALD Pro не могут напрямую получать информацию о пользователях и группах из MS AD, поэтому серверы ALD Pro используют плагин **ipa-extdom** для получения информации о пользователях и группах MS AD, и эта информация пересылается запрашивающему клиенту.

Плагин **ipa-extdom** отправляет запрос в SSSD на получение данных о пользователях MS AD. Если информации нет в кэше SSSD, SSSD запрашивает данные у контроллера домена MS AD (DC). Можно настроить значение таймаута конфигурации, которое определяет, как долго подключаемый модуль **ipa-extdom** ожидает ответа от **SSSD**, прежде чем подключаемый модуль отменит соединение и вернет вызывающей стороне сообщение об ошибке таймаута. Значение по умолчанию равно 10000 миллисекунд (10 секунд).

В следующем примере время ожидания настройки устанавливается равным 20 секундам (20000 миллисекунд).

3.8.30.1. Предупреждение

Необходимо соблюдать осторожность при настройке таймаута конфигурации:

Если задается слишком малое значение, например 500 миллисекунд, у **SSSD может не хватить времени для ответа**, и запросы всегда будут возвращать таймаут.

Если задается слишком большое значение, например 30000 миллисекунд (30 секунд), **один запрос может заблокировать подключение к SSSD на этот промежуток времени**. Поскольку **только один поток может подключаться к SSSD одновременно**, все остальные запросы от подключаемого модуля должны ждать.

Если ALD Pro-клиенты отправляют много запросов, они могут заблокировать все доступные рабочие процессы, настроенные для сервера каталогов на ALD Pro-сервере. Как следствие, сервер может быть не в состоянии ответить на какой-либо запрос в течение некоторого времени.

Изменять время ожидания конфигурации рекомендуется только в следующих ситуациях:

- Если клиенты ALD Pro при запросе информации о пользователях и группах Ms AD часто получают ошибки таймаута до истечения их собственного таймаута поиска.

Значение таймаута конфигурации слишком мало.

- Если сервер каталогов на ALD Pro-сервере часто блокируется, а утилита **pstack** сообщает, что многие или все рабочие потоки в это время обрабатывают запросы **ipa-extdom**. Значение слишком велико.

3.8.30.2. Предварительное требование.

Пароль менеджера каталогов LDAP (LDAP Directory Manager password)

3.8.30.3. Процедура

Используется следующая команда, чтобы настроить время ожидания настройки на 20000 миллисекунд:

```
# ldapmodify -D "cn=directory manager" -W dn: cn=ipa_extdom_extop,cn=plugins,
↪cn=config changetype: modify replace: ipaExtdomMaxNssTimeout
↪ipaExtdomMaxNssTimeout: 20000
```

3.8.31. Настройка максимального размера буфера для плагина ipa-extdom на ALD Pro-серверах

Клиенты ALD Pro не могут напрямую получать информацию о пользователях и группах из MS AD, поэтому серверы IdM используют плагин ipa-extdom для получения информации о пользователях и группах MS AD, и эта информация пересылается запрашивающему клиенту.

Можно настроить максимальный размер буфера для плагина ipa-extdom, который регулирует размер буфера, в котором SSSD может хранить полученные данные. Если буфер слишком мал, SSSD возвращает ошибку ERANGE, и подключаемый модуль повторяет запрос с буфером большего размера. Размер буфера по умолчанию составляет 134217728 байт (128 МБ).

В следующем примере максимальный размер буфера устанавливается равным 256 МБ (268435456 байт).

3.8.31.1. Предварительное требование.

Пароль менеджера каталогов LDAP (LDAP Directory Manager password)

3.8.31.2. Процедура

Используется следующая команда, чтобы установить максимальный размер буфера равным 268435456 байтам:

```
# ldapmodify -D "cn=directory manager" -W dn: cn=ipa_extdom_extop,cn=plugins,
 ↪cn=config changetype: modify replace: ipaExtdomMaxNssBufSize
 ↪ipaExtdomMaxNssBufSize: 268435456
```

3.8.32. Настройка максимального количества экземпляров для плагина ipa-extdom на ALD Pro-серверах

Поскольку клиенты ALD Pro не могут напрямую получать информацию о пользователях и группах из MS AD, серверы ALD Pro используют плагин **ipa-extdom** для получения информации о пользователях и группах MS AD, а затем пересылают эту информацию запрашивающему клиенту.

По умолчанию плагин **ipa-extdom** настроен на использование до **80%** рабочих потоков LDAP для обработки запросов от ALD Pro-клиентов. Если служба SSSD на ALD Pro-клиенте запросила большой объем информации о пользователях и группах **AD trust**, эта операция **может остановить службу LDAP**, если она использует большинство потоков LDAP. Если данная проблема возникла, можно увидеть аналогичные ошибки в файле журнала SSSD для домена MS AD, **/var/log/sssd/sssd__your-ad-domain-name.com_.log**:

```
(2022-05-22  5:00:13): [be[ad.example.com]] [ipa_s2n_get_user_done]
 ↪(0x0040): s2n exop request failed.
(2022-05-22  5:00:13): [be[ad.example.com]] [ipa_s2n_get_user_done]
 ↪(0x0040): s2n exop request failed.
(2022-05-22  5:00:13): [be[ad.example.com]] [ipa_s2n_exop_done] (0x0040):
 ↪ldap_extended_operation result: Server is busy(51), Too many extdom
 ↪instances running.
```

Можно настроить максимальное количество экземпляров ipa-extdom, установив значение

для параметра ipaExtdomMaxInstances, которое должно быть целым числом больше 0 и меньше общего числа рабочих потоков.

3.8.32.1. Предварительное требование.

Пароль менеджера каталогов LDAP (LDAP Directory Manager password)

3.8.32.2. Процедура

1. Извлечь общее количество рабочих потоков.

```
# ldapsearch -xLLLD cn=directory\ manager -W -b cn=config -s base nsslapd-
 ↪threadnumber
Enter LDAP Password:
dn: cn=config
nsslapd-threadnumber: 16
```

Это означает, что текущее значение для ipaExtdomMaxInstances равно 13.

2. Отрегулировать максимальное количество экземпляров. В этом примере значение изменяется на 14:

```
# ldapmodify -D "cn=directory manager" -W
dn: cn=ipa_extdom_extop,cn=plugins,cn=config
changetype: modify
replace: ipaExtdomMaxInstances
ipaExtdomMaxInstances: 14
```

3. Следить за производительностью сервера каталогов ALD Pro и, если она не улучшится, повторить эту процедуру и отрегулировать значение переменной ipaExtdomMaxInstances.

3.8.33. Настройка SSSD в ALD Pro-клиентах для крупных доверительных развертываний IdM-AD

Эта процедура применяет параметры настройки к конфигурации службы SSSD в ALD Pro-клиенте, чтобы увеличить время отклика при получении информации из большой среды MS AD.

3.8.33.1. Предварительное требование.

Нужны права **root** для редактирования конфигурационного файла **/etc/sssd/sssd.conf**.

3.8.33.2. Процедура

1. Определить, сколько секунд занимает один незакешированный вход в систему.

a) Очистить кэш SSD на ALD Pro-клиенте client.example.com

Требуется предварительная установка **apt install sssd-tools**

```
[root@client ~]# sss_cache -E
```

b) Измерить сколько времени требуется для входа в систему в качестве пользователя MS AD с помощью команды time. В этом примере из клиента ALD Pro client.example.com войnb на тот же хост, что и пользователь ad-user из **ad**.example.com AD Domain

```
[root@client ~]# time ssh ad-user@ad.example.com@client.example.com
```

Ввести пароль как можно скорее.

```
Password:
Last login: Sat Jan 23 06:29:54 2021 from 10.0.2.15
[ad-user@ad.example.com@client ~]$
```

c) Выйти из системы как можно скорее, чтобы отобразить прошедшее время. В этом примере один некэшированный вход в систему занимает около 9 секунд.

```
[ad-user@ad.example.com@client /]$ exit
logout
Connection to client.example.com closed.

real 0m8.755s
user    0m0.017s
sys     0m0.013s
```

2. Открыть конфигурационный файл /etc/sssd/sssd.conf в текстовом редакторе.

3. Добавить следующие параметры в раздел [домен] для домена MS AD. Установить параметры pam_id_timeout и krb5_auth_timeout на количество секунд, которое занимает некэшированная логика. Если доменного раздела для домена MS AD еще нет, создать его.

```
[domain/example.com/ad.example.com]
krb5_auth_timeout = 9
ldap_deref_threshold = 0
...
```

4. Добавить следующую опцию в раздел [pam]:

```
[pam]
pam_id_timeout = 9
```

5. Сохранить и закрыть файл **/etc/sssd/sssd.conf** на сервере.

6. Перезапустить службу SSSD, чтобы загрузить изменения конфигурации.

```
systemctl restart sssd
```

3.8.34. Монтирование кэша SSSD в tmpfs

Демон служб системной безопасности (SSSD) постоянно записывает объекты LDAP в свой кэш. Эти внутренние транзакции SSSD записывают данные на диск, что намного медленнее, чем чтение и запись из оперативной памяти (RAM).

Чтобы повысить производительность, необходимо смонтировать кэш SSSD в оперативной памяти.

Кэшированная информация не сохраняется после перезагрузки, если кэш SSSD находится в оперативной памяти.

Это изменение безопасно выполнять на серверах ALD Pro, поскольку экземпляр SSSD на сервере ALD Pro не может потерять соединение с сервером каталогов на том же хосте.

Если выполнить эту настройку на ALD Pro-клиенте, и он потеряет подключение к серверам ALD Pro, пользователи не смогут пройти проверку подлинности после перезагрузки, пока не будет восстановлено подключение.

3.8.34.1. Предварительное требование.

Нужны права root для редактирования файла конфигурации **/etc/fstab**.

3.8.34.2. Процедура

Довольно много времени, затрачиваемого на обработку запроса, уходит на запись объектов LDAP в кэш. Поскольку кэш поддерживает полные свойства ACID, он выполняет синхронизацию диска с каждой внутренней транзакцией SSSD, что приводит к записи данных на диск. С положительной стороны, это гарантирует, что кэш всегда доступен в случае сбоя сети и будет доступен для использования после сбоя компьютера, но, с другой стороны, запись данных требует времени. Можно смонтировать кэш на **ramdisk**, сократив затраты на ввод-вывод с диска, добавив в **/etc/fstab** в виде одной строки следующее:

```
tmpfs /var/lib/sss/db/ tmpfs size=300M,mode=0700,rootcontext=system_u:object_
↪r:sssd_var_lib_t:s0 0 0
```

Затем необходимо подключить каталог и перезапустить sssd после этого:

```
mount /var/lib/sss/db/

systemctl restart sssd
```

Важно настроить параметр размера в соответствии с требуемым IPA и размером каталога объявлений. Как правило, можно использовать **100 Мб на 10000 записей LDAP**.

Выполнение этого изменения на ALD-сервере немного безопаснее, чем на ALD-клиентах, поскольку экземпляр SSSD на сервере никогда не потеряет подключение к ALD-серверу, поэтому кэш всегда можно перестроить. Но в случае, если кэш был потерян после

перезагрузки, и MS AD был недоступен из-за сетевой ошибки или аналогичного состояния, узел не смог бы вернуться к кэшированным данным о MS AD пользователях.

Плюсы: Операции ввода-вывода в кэше выполняются намного быстрее.

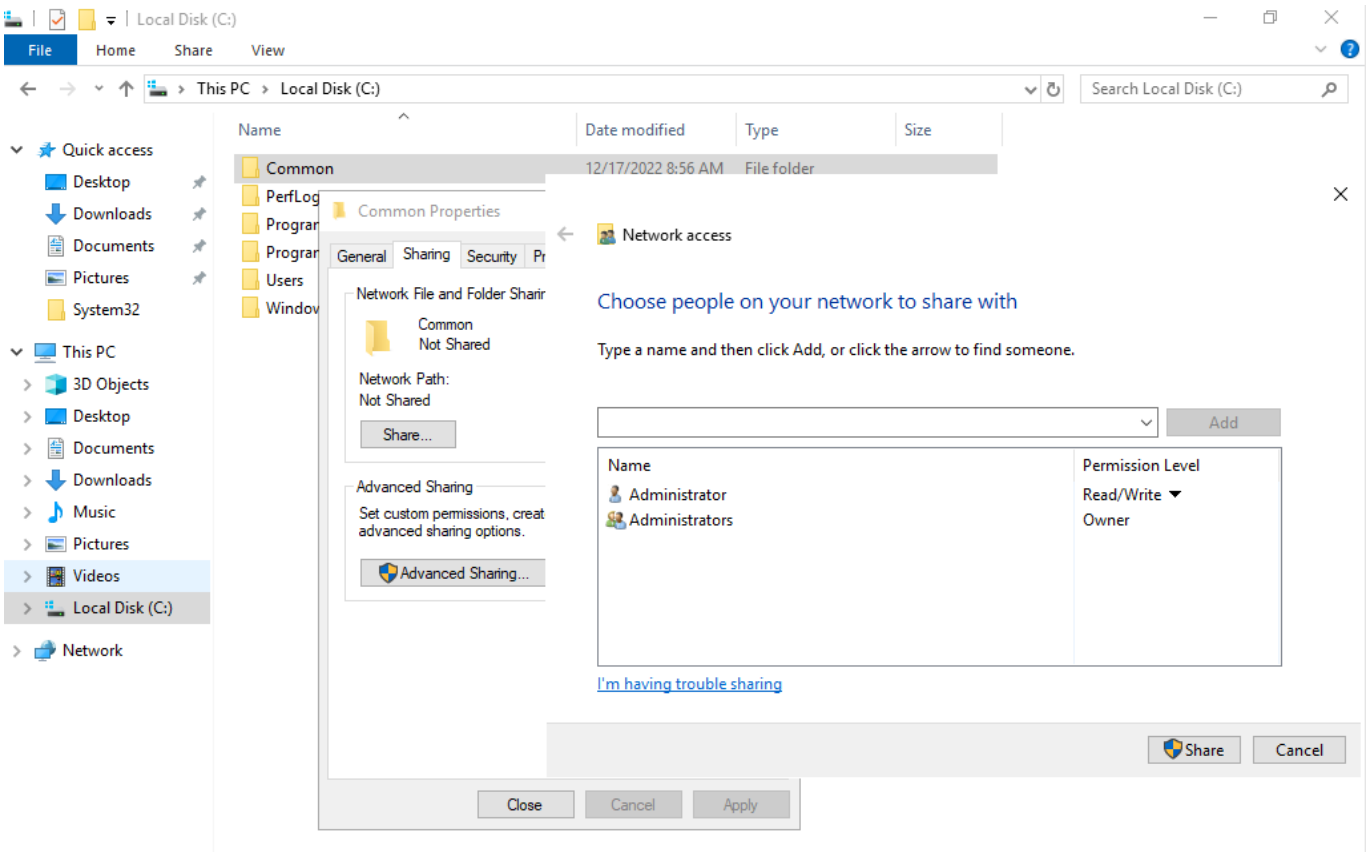
Минусы: Кэш не сохраняется при перезагрузках. Это означает, что кэш должен быть восстановлен после перезагрузки компьютера, но также и то, что cachedpassword теряются после перезагрузки.

Доступ пользователей ALD Pro к ресурсам MS AD

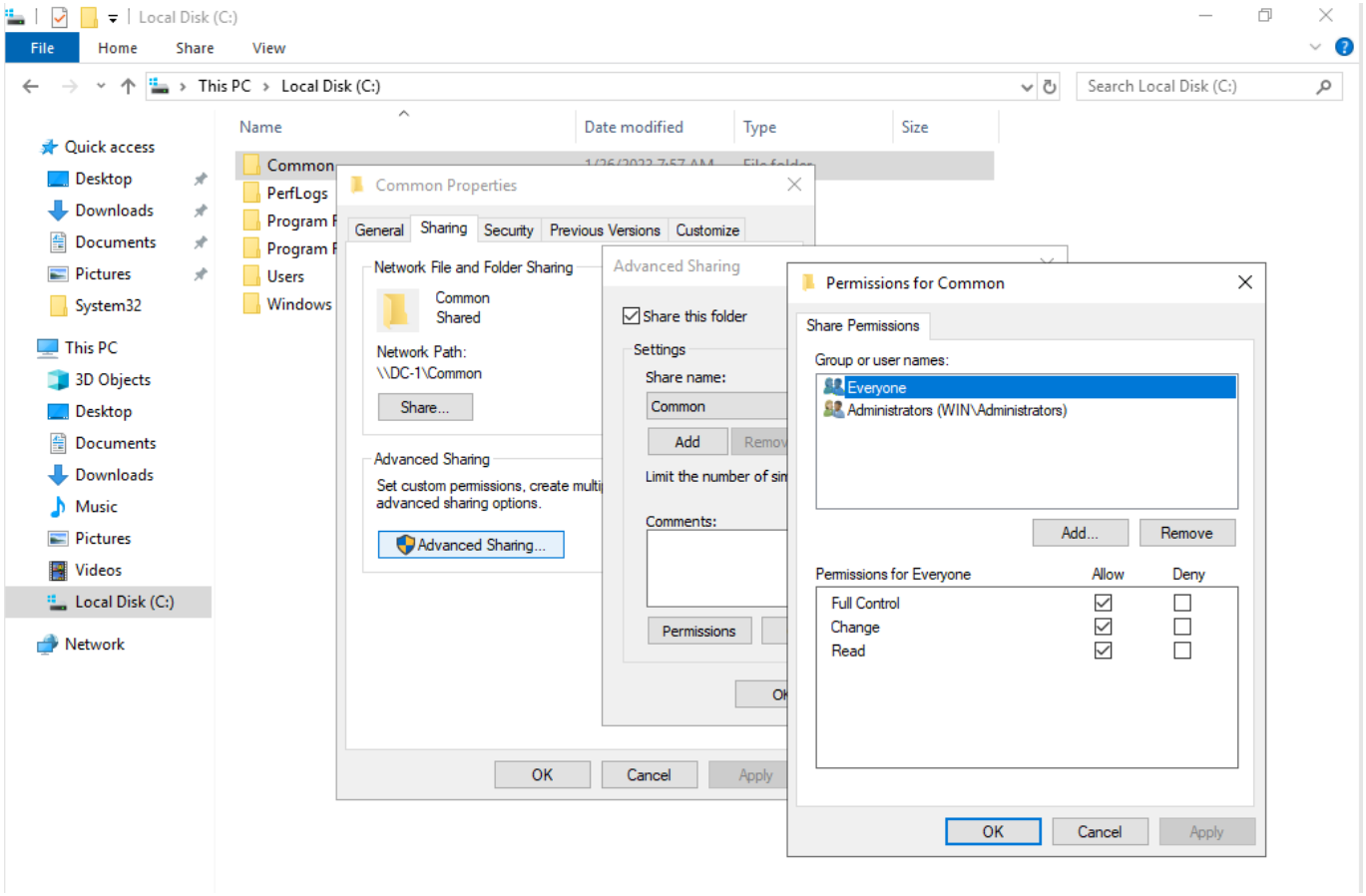
3.8.35. Создание сетевой папки в домене MS AD

Контроллер домена не рекомендуется использовать для создания общих сетевых ресурсов. Он используется в примере для упрощения процесса.

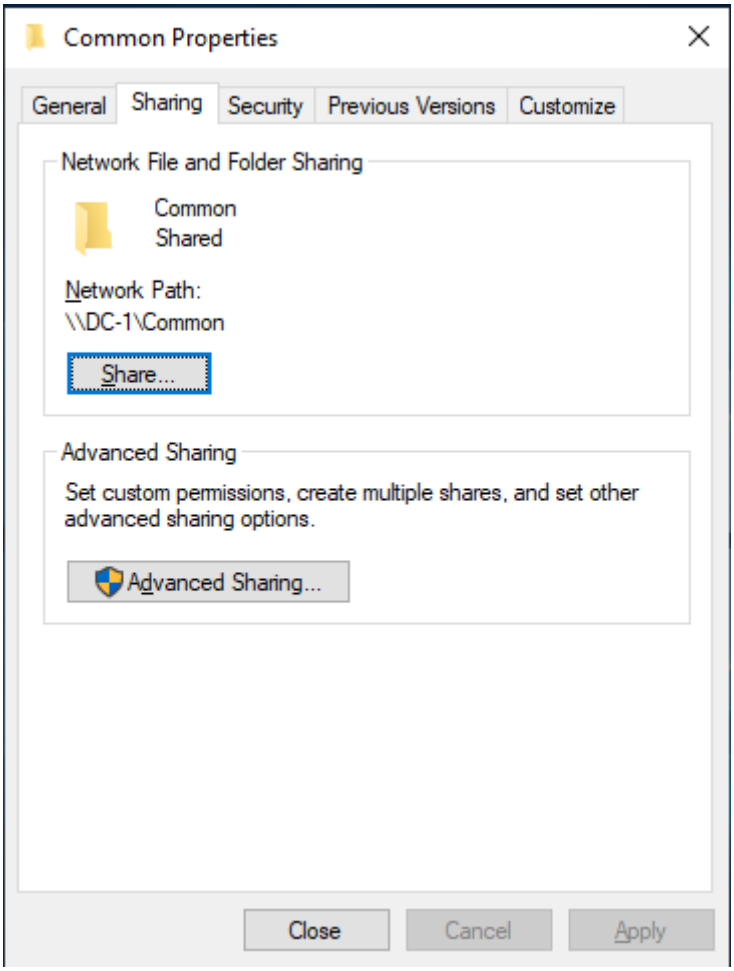
Создать папку C:Common, в свойствах на закладке «Sharing» выбрать «Share» и в окне «Network access» выбрать «Share», оставив все по умолчанию.

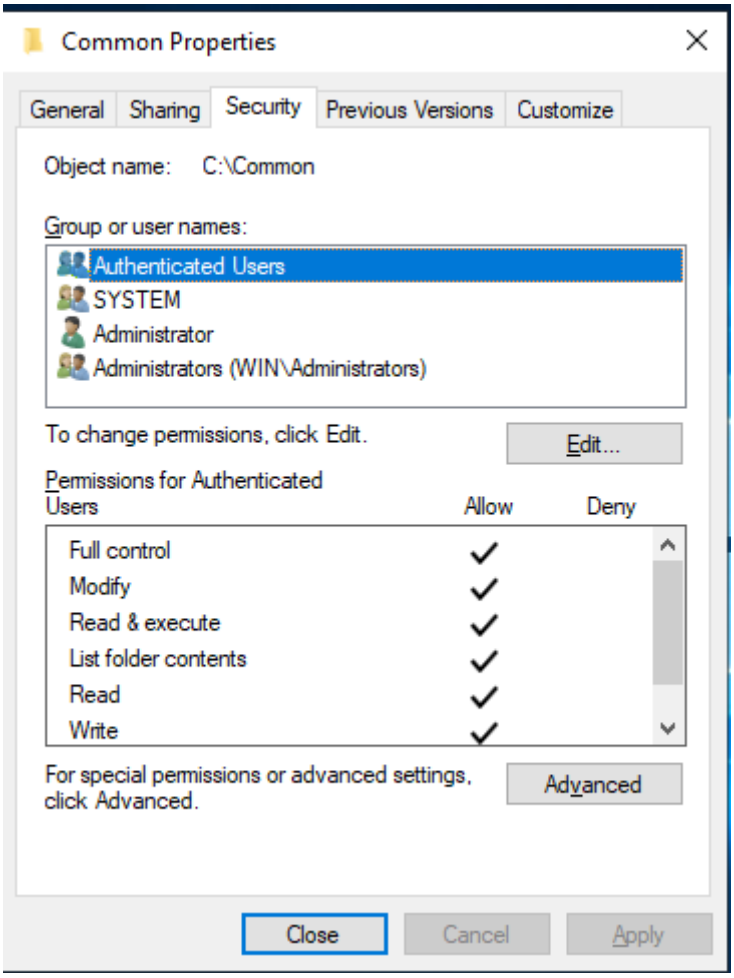


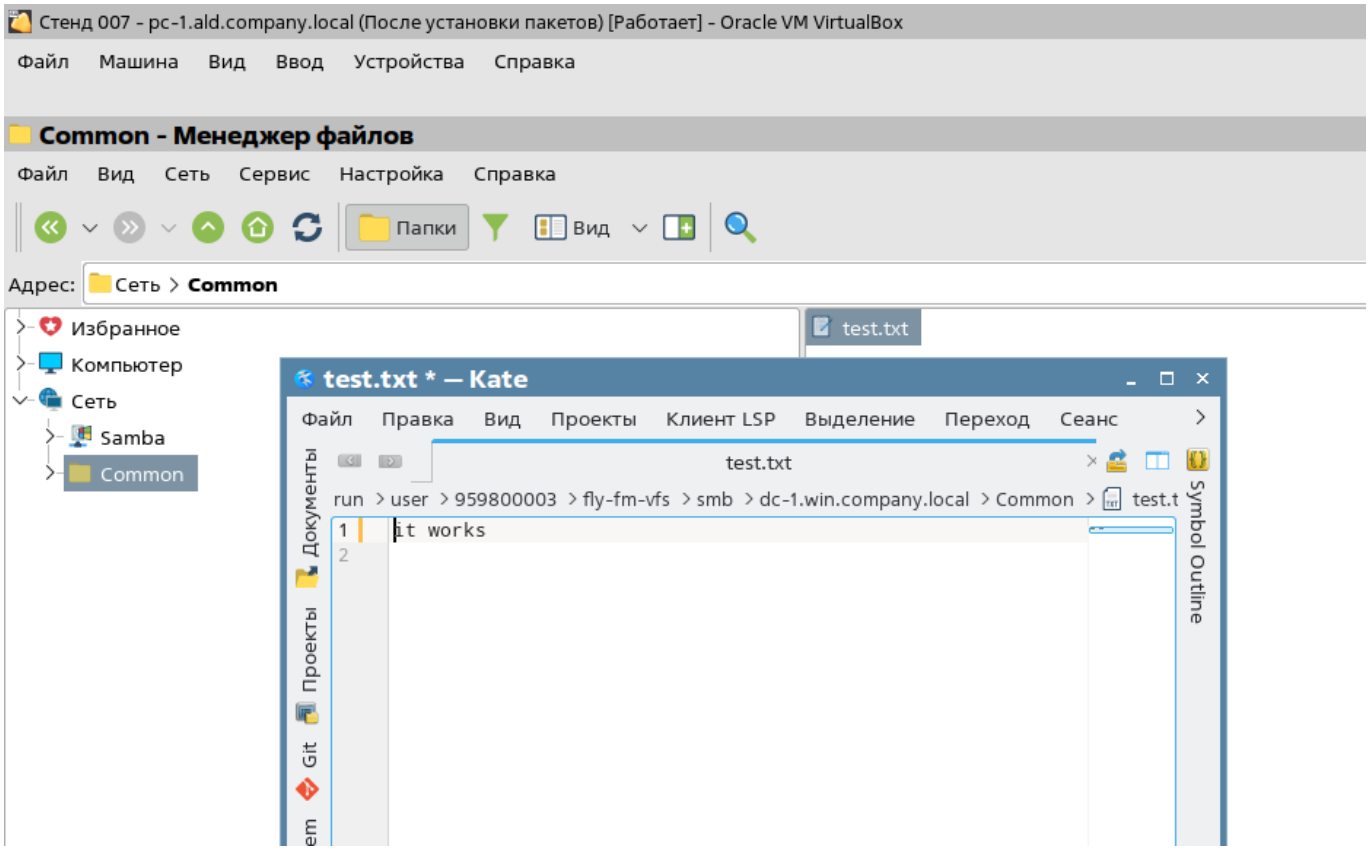
Если открыть окно «Common PropertiesSharingAdvanced SettingsPermissions», то будет видно, что по умолчанию на уровне SMB все пользователи имеют полные права.



Но доступ к файлам регулируется также на уровне NTFS разрешений, которые настраиваются на вкладке «Common PropertiesSecurity». Можно предоставить доступ к общей папке всем аутентифицированным пользователям, и это позволит пользователям ALD Pro редактировать файлы в папке, доказывая работу доверительных отношений в направлении MS → ALD.


Common Properties
General
Sharing
Security
Previous Versions
Customize
Network File and Folder Sharing
Common
Shared
Network Path:
\\DC-1\Common
Share...
Advanced Sharing
Set custom permissions, create multiple shares, and set other advanced sharing options.
Advanced Sharing...
Close
Cancel
Apply


Common Properties
General
Sharing
Security
Previous Versions
Customize
Object name: C:\Common
Group or user names:
Authenticated Users
SYSTEM
Administrator
Administrators (WIN\Administrators)
To change permissions, click Edit.
Edit...
Permissions for Authenticated Users
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
Write
For special permissions or advanced settings, click Advanced.
Advanced
Close
Cancel
Apply


Стенд 007 - pc-1.ald.company.local (После установки пакетов) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Common - Менеджер файлов
Файл Вид Сеть Сервис Настройка Справка
Папки
Вид
Адрес: Сеть > Common
Избранное
Компьютер
Сеть
Samba
Common
test.txt
test.txt * — Kate
Файл Правка Вид Проекты Клиент LSP Выделение Переход Сеанс
test.txt
run > user > 959800003 > fly-fm-vfs > smb > dc-1.win.company.local > Common > test.t
1 it works
2
Документы
Проекты
Git
Symbol Outline

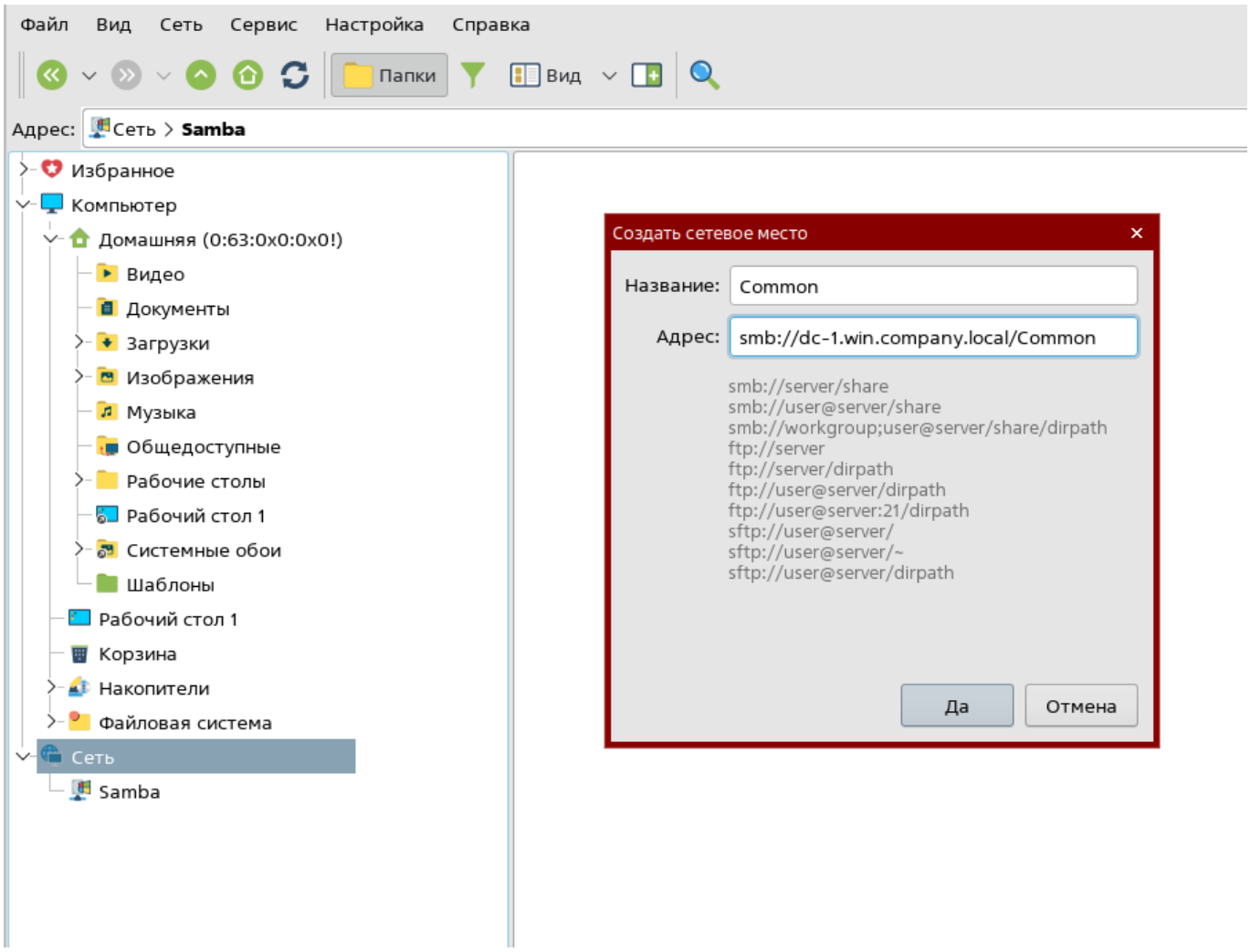
3.8.36. Подключение сетевой папки на рабочей станции под управлением Astra Linux

Для подключения сетевой папки из домена MS AD в Astra Linux необходимо открыть проводник, кликнуть правой кнопкой мыши по узлу «Сеть» и выбрать команду «Новое место». Задать следующие параметры подключения:

В примере Windows Domain Controller именуется как **dc-1**.win.company.local

- Название: Common (любое)
- Адрес: smb://dc-1.win.company.local/Common

формат протокол://имя_сервера/название_общей_папки



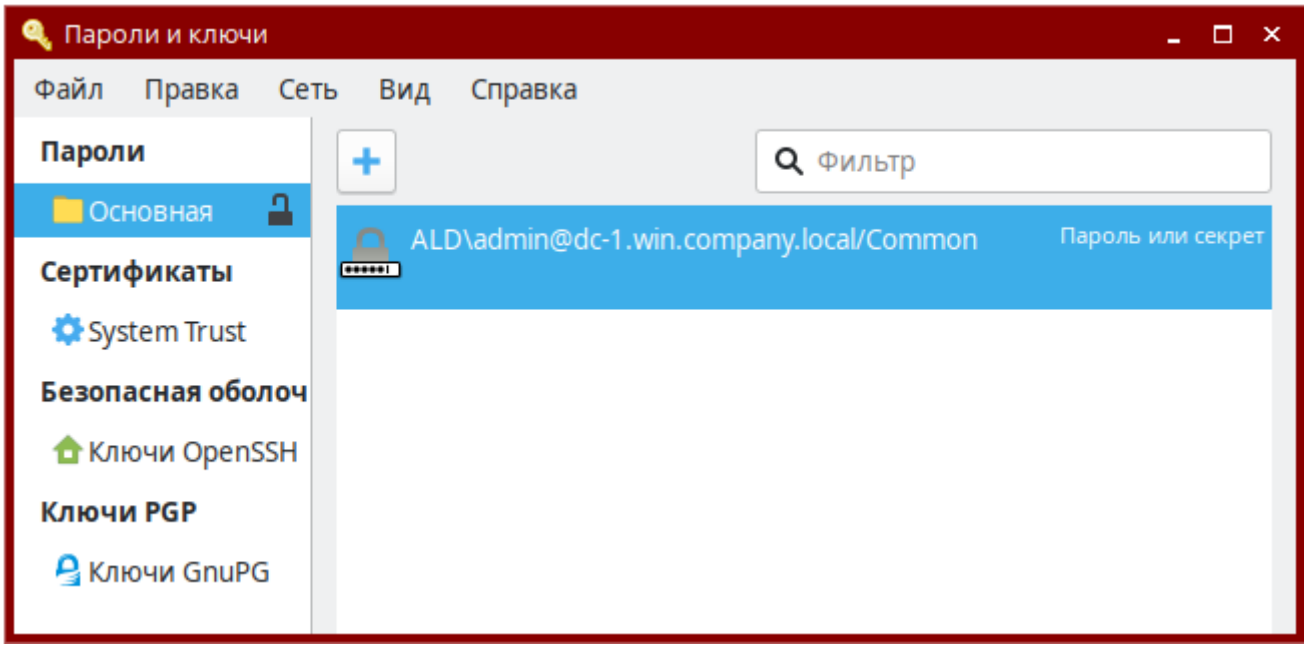
Необходимо обязательно проверить, что время на контроллерах MS AD и ALD Pro синхронизировано, т. к. для работы протокола Kerberos нужно, чтобы время всех участниках расходилось не более, чем на 5 минут.

Если нет необходимости настраивать прозрачную аутентификацию, то можно указать имя пользователя в формате:

```
#имя пользователя
ALD\admin
#в формате
ДОМЕН\имя_пользователя
```

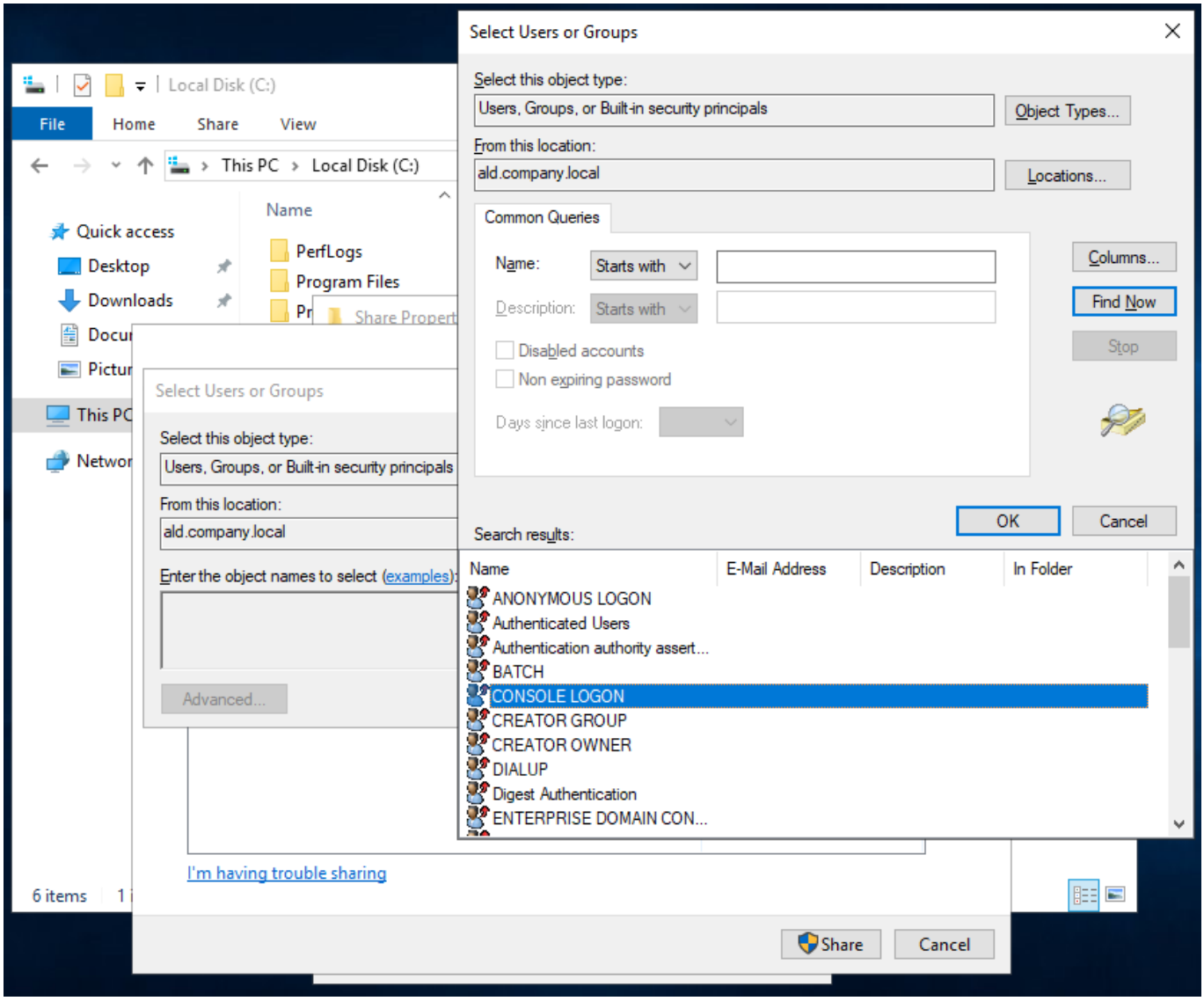
Система предложит сохранить учетные данные в связке ключей, для работы с которой можно воспользоваться приложением seahorse «Пароли и ключи»

```
# apt-get install seahorse
# seahorse
```



3.8.36.1. Ограничение доступа по SID

Сценарий, когда доступ к сетевому ресурсу предоставляется всем пользователям домена, является крайне редким. На практике обычно требуется предоставить доступ только строго ограниченной группе пользователей. Если воспользоваться окном «Select Users or Groups», можно обнаружить, что объекты доверенного домена ALD Pro найти не удается.



Стандартный механизм поиска объектов из доверенного домена работает через глобальный каталог, которого в обычной FreeIPA нет. Глобальный каталог — это еще один LDAP-каталог, который должен быть доступен на порту 3268 и предоставлять данные обо всех объектах леса в определенной схеме данных. Не имея этой службы на стороне FreeIPA, доступ конкретным пользователям можно предоставить только по SID через PowerShell.

Посмотреть SID пользователя ALD Pro можно с помощью утилиты wbinfo на ALD Pro контроллере домена:

Используя wbinfo

```
root@aldpro01:~# wbinfo -n 'ald\admin'
S-1-5-21-896088827-1417987318-1335504985-500 SID_USER (1)
```

Используя ipa command

```
root@ald01:~# ipa user-show admin --all | grep ipantsecurityidentifier
ipantsecurityidentifier: S-1-5-21-896088827-1417987318-1335504985-500
```

Назначить права доступа можно командой ICACLS (Integrity Control Access Control List)

Наиболее популярные разрешения:

r = чтение

rx = Чтение, Выполнение, Список содержимого папки

rxm = Чтение, Выполнение, Список содержимого папки, Запись, Изменение

f = Полный доступ

(OI) = Для этой папки и её файлов

(CI) = Для этой папки и её подпапок

Таким образом, чтобы дать обычные права на чтение и запись на папку, используются разрешения (OI)(CI)rxm. Тогда команда будет выглядеть так:

```
PS C:\Users\Administrator> ICACLS "C:\Temp" /grant "*S-1-5-21-896088827-
↪1417987318-1335504985-500:(OI)(CI)rxm"
```

После добавления объектов в ACL, в стандартном окне безопасности они будут отображаться даже не по своим SID, а по привычным именам, т. к. для разрешения имен глобальный каталог не требуется.

Для упрощения администрирования в MS AD можно создать вспомогательные группы. Например, для администраторов ALD Pro в MS AD создается группа «WINALD_Pro_Administrators», в эту группу добавляются SID группы «ALDAdmins» из доверенного домена ALD Pro. Далее при назначении прав доступа на общий сетевой ресурс можно будет использовать группу «WINALD_Pro_Administrators».

3.8.37. Добавление пользователей и групп из ALD Pro домена в домен MS AD.

Процесс добавления пользователей из одного домена в другой осуществляется через доверительные отношения между доменами. По умолчанию в доверенных доменах MS AD используется Global Catalog для поиска пользователя или группы, однако ALD Pro версии ниже 2.0.0 по умолчанию не имеет глобальный каталог, по этой причине для добавления пользователя или группы из домена без глобального каталога в домен MS AD с глобальным каталогом, используется PowerShell скрипт.

При добавлении пользователя или группы в домене MS AD будет создан специальный объект Foreign Security Principal.

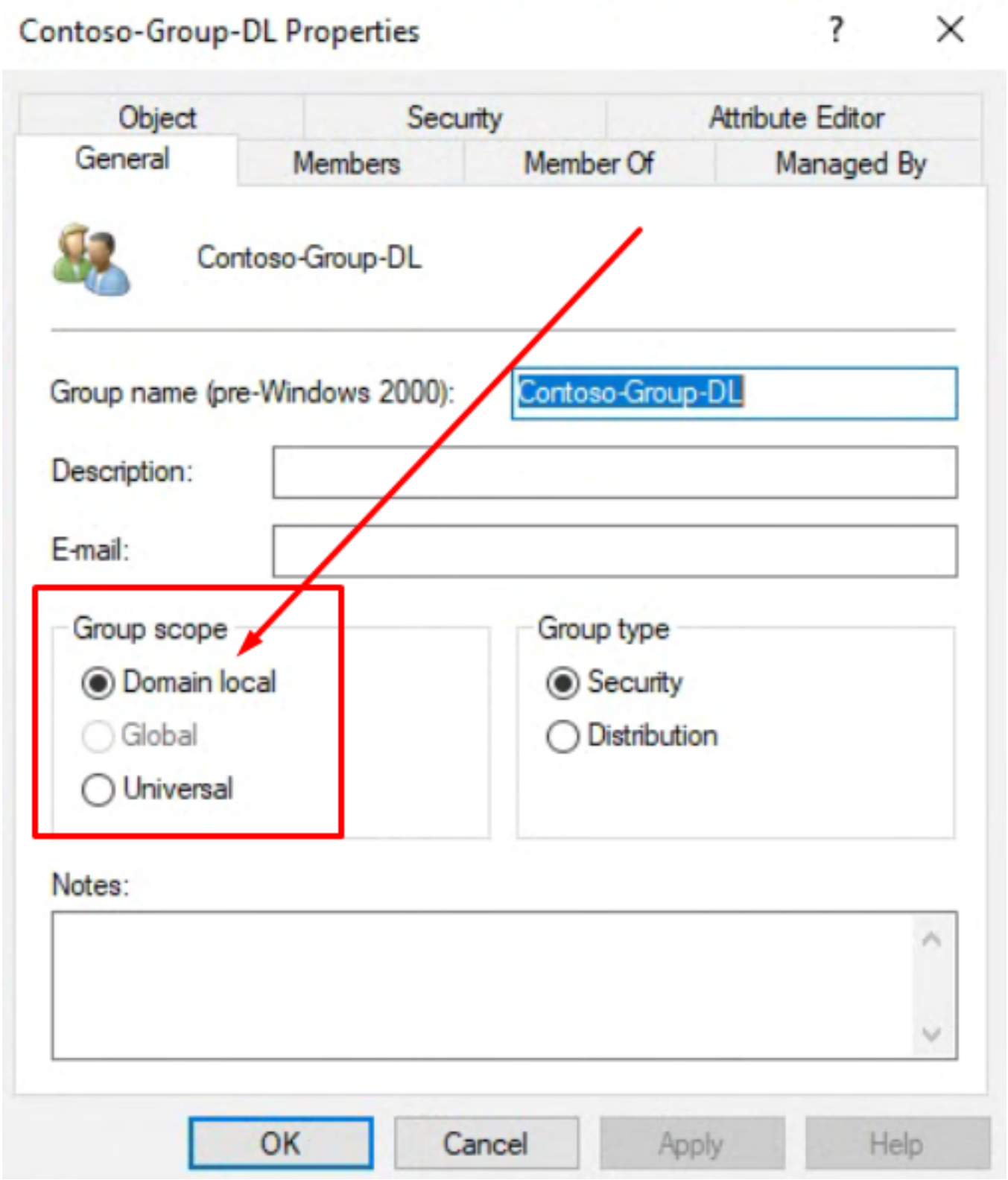
https://social.technet.microsoft.com/wiki/contents/articles/51367.active-directory-foreign-security-principals-and-special-identities.aspx#:~:text=A%20Foreign%20Security%20Principal%20(FSP,security%20groups%20and%20granted%20permissions.

3.8.37.1. Порядок добавления пользователя или группы

1. Посмотреть SID пользователя ALD Pro можно с помощью утилиты ldapsearch:

```
root@aldpro01:~# wbinfo -n 'ald\elena.kuznetsova'
S-1-5-21-1784717832-1844364183-3442789864-1013 SID_USER (1)
```

2. На стороне MS AD необходимо создать Domain Local группу, куда можно добавит SID из домена ALD Pro



3. На стороне MS AD на контроллере домена необходимо запустить скрипт

<S-1-5-21-1784717832-1844364183-3442789864-1013>– SID пользователя или группы

<CN=Contoso-Group-DL,CN=Users,DC=contoso,DC=dom >- Distinguished Name группы

```
#SID Из леса ALD_Pro(Пользователь или группа)
$AldSid = 'S-1-5-21-1784717832-1844364183-3442789864-1013'

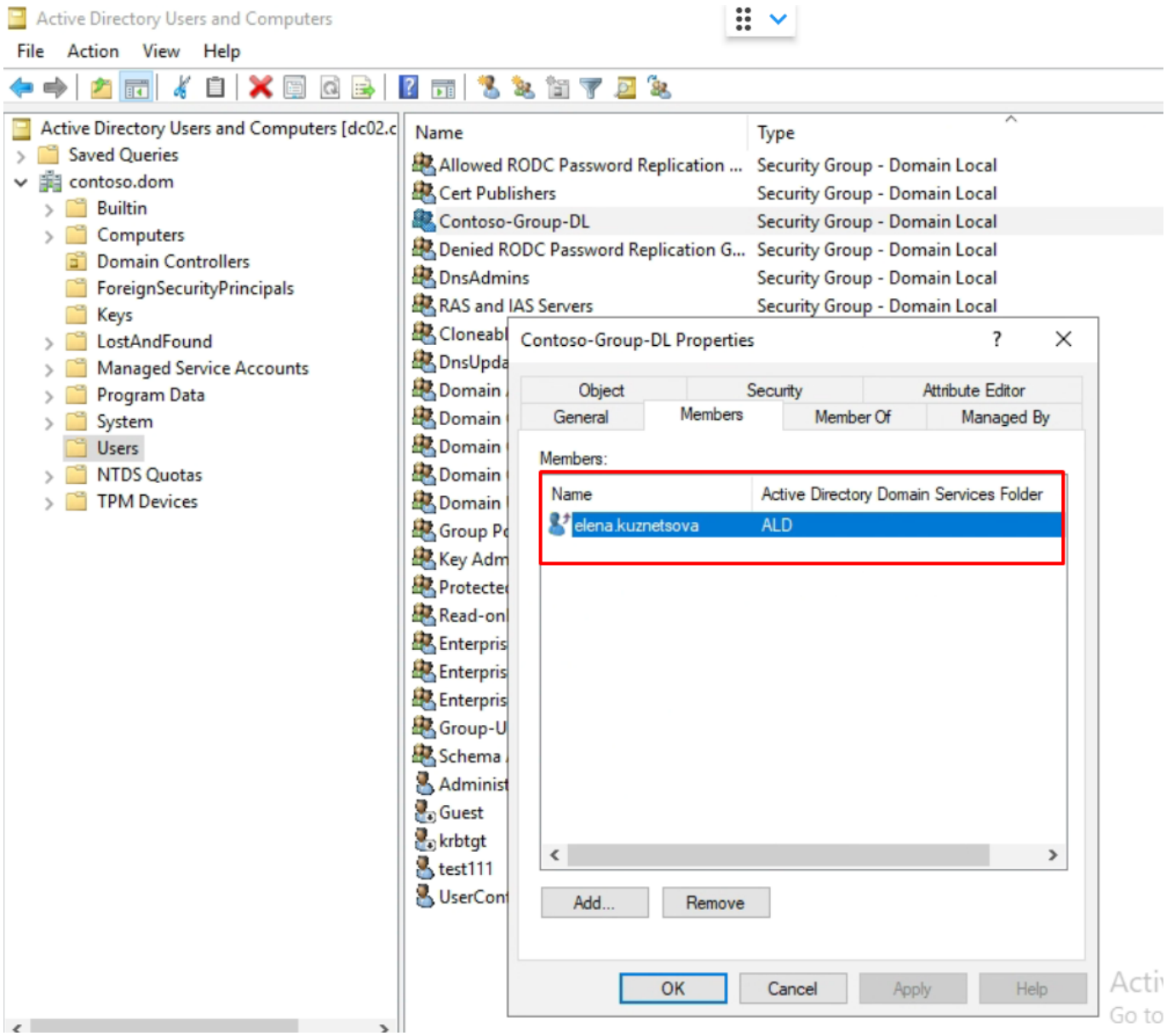
#Domain Local Group из леса Active Directory
$DomainLocalGroupDN = 'CN=Contoso-Group-DL,CN=Users,DC=contoso,DC=dom'

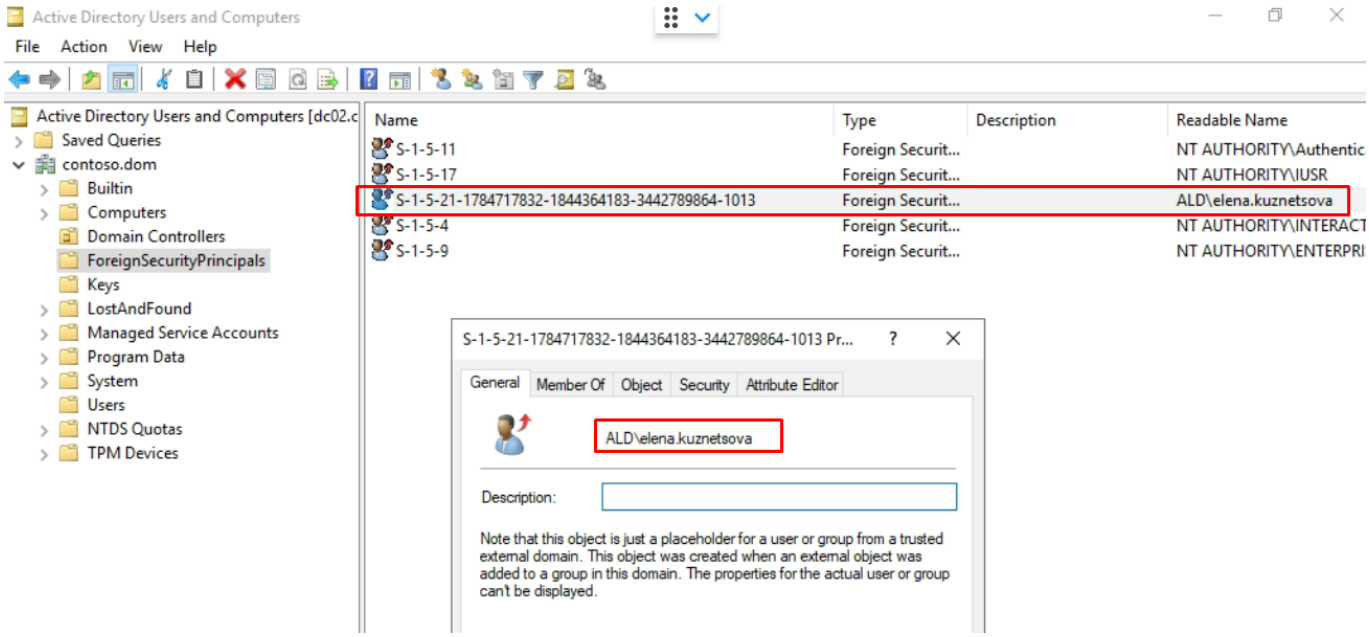
#Создание нового Directory Entry
$group = New-Object DirectoryServices.DirectoryEntry("LDAP://$(
 ↪$DomainLocalGroupDN)")

#Добавление AldSid в DomainLocal группу
[void]$group.member.Add("<SID=$AldSid>")
$group.CommitChanges()
$group.Close()
```

После выполнения скрипта пользователь будет добавлен в группу и соответствующий объект Foreign Security Principal будет создан автоматически.

Теперь можно назначить Domain Local группу, к примеру, на файловые ресурсы, и все пользователи или группы внутри нее будут иметь доступ к ресурсу в домене MS AD.


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [dc02.c
Saved Queries
contoso.dom
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Keys
LostAndFound
Managed Service Accounts
Program Data
System
Users
NTDS Quotas
TPM Devices
Name
Type
Allowed RODC Password Replication ...
Security Group - Domain Local
Cert Publishers
Security Group - Domain Local
Contoso-Group-DL
Security Group - Domain Local
Denied RODC Password Replication G...
Security Group - Domain Local
DnsAdmins
Security Group - Domain Local
RAS and IAS Servers
Security Group - Domain Local
Contoso-Group-DL Properties
Object
Security
Attribute Editor
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
elena.kuznetsova
ALD
Add...
Remove
OK
Cancel
Apply
Help


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [dc02.c
Saved Queries
contoso.dom
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Keys
LostAndFound
Managed Service Accounts
Program Data
System
Users
NTDS Quotas
TPM Devices
Name
Type
Description
Readable Name
S-1-5-11
Foreign Securit...
NT AUTHORITY\Authentic
S-1-5-17
Foreign Securit...
NT AUTHORITY\IUSR
S-1-5-21-1784717832-1844364183-3442789864-1013
Foreign Securit...
ALD\elena.kuznetsova
S-1-5-4
Foreign Securit...
NT AUTHORITY\INTERACT
S-1-5-9
Foreign Securit...
NT AUTHORITY\ENTERPRI
S-1-5-21-1784717832-1844364183-3442789864-1013 Pr...
General
Member Of
Object
Security
Attribute Editor
ALD\elena.kuznetsova
Description:
Note that this object is just a placeholder for a user or group from a trusted external domain. This object was created when an external object was added to a group in this domain. The properties for the actual user or group can't be displayed.

Доступ пользователей MS Windows к ресурсам ALD Pro

Доступ к ресурсам ALD Pro пользователям из доверенного домена MS AD предоставляется через внешние группы.

На стороне ALD Pro пользователям из доверенного домена MS AD предоставляется доступ к ресурсам через внешние группы.

```
# ipa group-add 'ad_administrators_external' --desc='Внешняя группа
 ↪администраторов из MS AD' --external
# ipa -n group-add-member 'ad_administrators_external' --external 'WIN.
 ↪COMPANY.LOCAL\Domain Admins'
```

Внешние группы не имеют gid (являются не POSIX-группами), поэтому их нельзя использовать напрямую для предоставления доступа к сетевым файлам. Следует создать еще одну обычную POSIX-группу и включить в нее группу ad_administrators.

Важно отметить, что добавление двустороннего доверия возможно в обычной инсталляции FreeIPA, даже не имея поддержки глобального каталога.

Установка глобального каталога(в ALD Pro 2.0.0)

Склонировать репозиторий:

```
# git clone --branch AD-39377-mvp1 https://git.astralinux.ru/scm/ad/aldpro-
 ↪backend-global-catalog.git /opt/gc/
```

где

- git clone — команда для клонирования репозитория
- AD-39377-mvp1 — имя ветки, в которой содержатся необходимые исходные коды
- https://git.astralinux.ru/… - адрес репозитория с кодом глобального каталога
- /opt/gc/ - имя папки, в которую нужно клонировать репозиторий

Запустить скрипт, который выполнит настройку глобального каталога в системе:

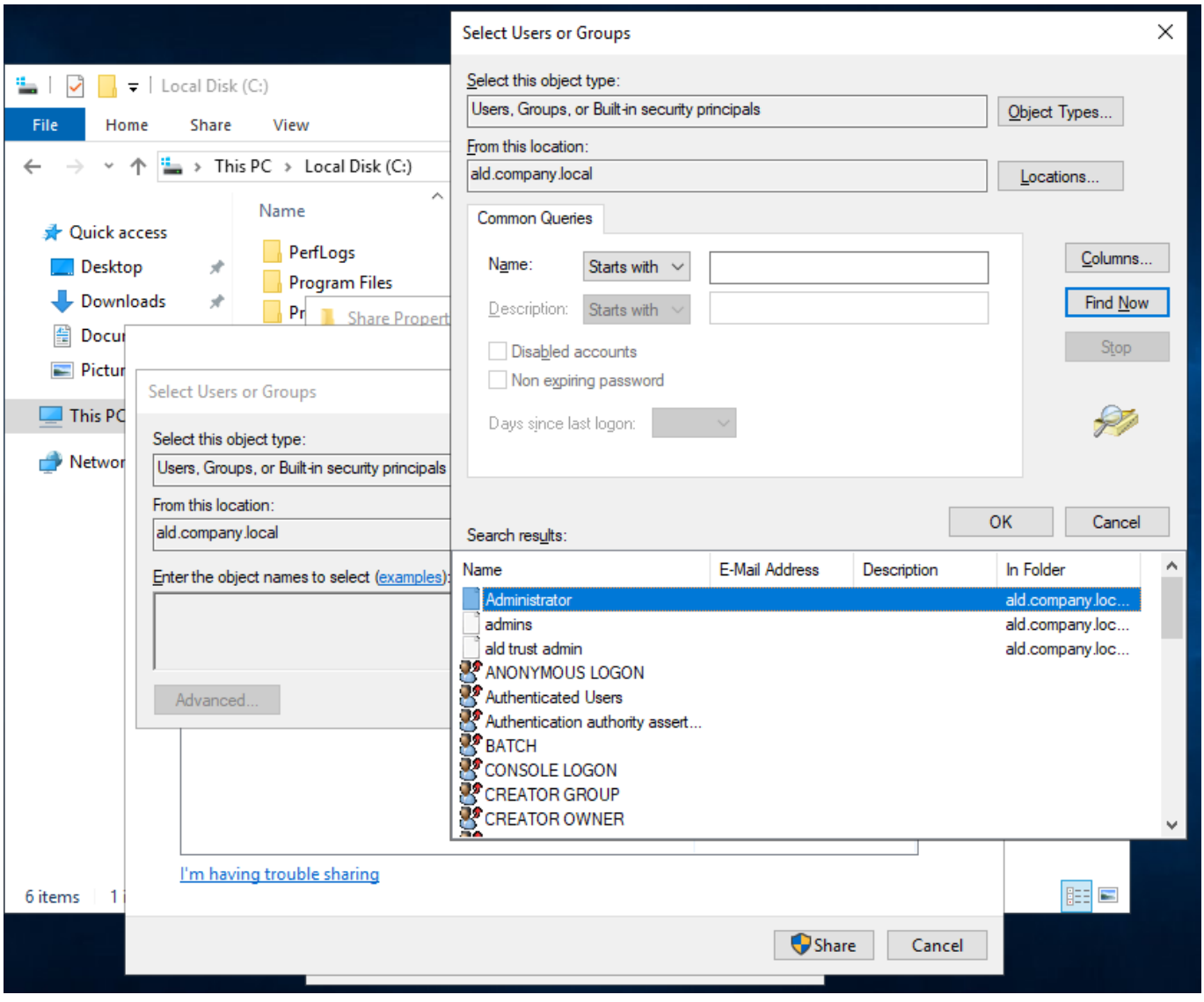
```
# /opt/gc/ipa-gc-install.py --gc-cert-file /etc/ssl/freeipa/server.p12 --gc-
 ↪pin 'AstraLinux_172' --disable-fast-preauth
```

где

- ipa-gc-install.py — имя файла со скриптом для настройки GC
- server.p12 — контейнер с сертификатом удостоверяющего центра и сервера
- gc-pin — пароль к контейнеру p12, совпадает с паролем доменного админа на момент установки IPA

Для настройки глобального каталога требуется контейнер p12 с сертификатом сервера и удостоверяющего центра. Используется уже существующий контейнер p12, который был создан FreeIPA при установке. Паролем к этому контейнеру является пароль доменного администратора, который использовался в момент продвижения сервера до контроллера домена.

После выполнения указанных действий на контроллере домена WINDC-1 при назначении прав доступа на сетевые ресурсы, стандартная оснастка «Select Users or Groups» начнет находить пользователей и группы из доверенного домена ald.company.local. Если уже придпринималась попытка обращения к глобальному каталогу, которая закончилась неудачно, необходимо очистить кеш и перезагрузить Windows сервер.



Настройка Samba для корректной работы RPC-сервера

Для обеспечения стабильной работы доверительных отношений с **MS AD** рекомендуется выполнить следующие действия:

1. Отключить **NetBIOS** на контроллере домена **MS AD**;
2. Изменить конфигурацию **Samba** с помощью утилиты `samba-regedit`;
3. Запустить **RPC**-сервер `samba-dcerpcd` с нужными опциями.

В начале следует настроить контроллер домена **MS AD** следующим способом:

Навести курсор на иконку **Сеть «Доступ к Интернету»** в нижнем правом углу экрана и жмем по нему правой кнопкой мыши и выбрать **Открыть «Параметры сети и Интернет»**.

Выбрать пункт **Ethernet**, раздел **Центр управления сетями и общим доступом**.

Нажать в графе **Подключения** на **Ethernet** → **Свойства** → раздел **IP версии 4 (TCP/IPv4)** → **Дополнительно** → вкладка **WINS**.

Нажать **Отключить NetBIOS через TCP/IP** и подтвердить все изменения, последовательно выбрав **Ок** в открытых окнах, в окне **Состояние: Ethernet** нажать клавишу **Закрыть**.

Важно: В результате установки доверительных отношений может возникнуть ошибка связанная с одним из обновлений **KB Windows**, клиент **Windows** разрывает соединение с сервером, если в пакете **RPC** ответа `bind_ack` не заполнено поле **ScndryAddr** (**Secondary Address**) (резервный адрес RPC службы).

Для корректной работы доверительных отношений на контроллере домена **MS AD** должны отсутствовать следующие обновления **KB**:

Для **Windows Server 2012 R2**: `KB5020447` (входит в обновления `KB5022352` и `KB5021294`).

Рекомендуется также установить на КД **MS AD** последние обновления безопасности.

Настройка в `samba-regedit` осуществляется вводом соответствующей команды с правами администратора:

```
sudo samba-regedit
```

Сначала необходимо открыть настройки `smbconf`, переходя в левом меню по следующим директориям: `/HKEY_LOCAL_MACHINE/SOFTWARE/Samba/smbconf`.

Перейти в правое меню нажатием клавиши `Tab` на клавиатуре, найти параметр `disable netbios`.

Если он существует, то необходимо присвоить ему значение `yes` либо `true`: клавишами стрелок выбрать его в линию курсора и нажать клавишу `Enter` на клавиатуре. В появившемся диалоговом окне поменять его значение на `yes` либо `true`.

Если параметр отсутствует, то нужно создать новый параметр нажатием клавиши `N` на клавиатуре, в появившемся окне под названием **New Value** нажатием клавиши `Tab` найти тип **REG_SZ** и нажать клавишу `Enter`. В появившемся окне **Edit Value**, в поле **Name** присвоить название `disable netbios`, а в поле **Data** значение `yes` либо `true`. Подтвердить создание параметра нажатием клавиши `Enter` (диалоговое окно создания параметра закроется).

Отключение **NetBIOS** необходимо, поскольку эта устаревшая технология не поддерживает межсетевые соединения, в отличие от **DNS-запросов**, которые решают эту проблему.

Если контроллер домена **MS AD** и контроллер домена **ALDPro** находятся в разных подсетях, **RPC-запросы** от **MS AD** к **ALDPro** будут завершаться с ошибкой таймаута.

Начиная с версии **Windows Server 2025** поддержка **NetBIOS** будет полностью отключена.

Затем нужно создать необходимые для корректной работы **RPC**-сервисов параметры:

Name = `rpc start on demand helpers`

Data = `false`

по аналогии с созданием параметра `disable netbios`.

После создания всех необходимых параметров нажать на клавиатуре клавишу `Q` для выхода из `samba-regedit` и перезапустить некоторые службы **Samba**:

```
sudo net cache flush
sudo systemctl restart smbd winbind
```

Параметр `rpc start on demand helpers` отвечает за запуск обработчиков

RPC-запросов. Значение по умолчанию `true` настраивает **Samba** на работу с внутренними именованными каналами, в то время как `false` переключает на работу с внешними **RPC**-сервисами, что нам и требуется.

Параметр `rpc server port:netlogon` отвечает за список портов, с которыми работает внешний **RPC**-сервер. На эти порты назначаются службы `winreg`, `lsad`, `netlogon` и др.

После перезапуска **Samba** нужно запустить **RPC**-сервер `samba-dcerpcd` с дополнительными опциями:

```
sudo /usr/libexec/samba/samba-dcerpcd --debuglevel 10 --no-process-group --
↪interactive --libexec-rpcds --debug-stdout
```

С такими опциями **RPC**-сервер работает следующим образом:

- в режиме демона (по умолчанию);
- `--libexec-rpcds`: использует все **RPC**-сервисы в директории `libexec`;
- `--debuglevel 10`: уровень логирования максимальный. Такая опция необязательна;
- `--no-process-group` : не создавать новые группы процесса для `samba-dcerpcd`;
- `--interactive` : если этот параметр указан, это заставляет сервер работать в «интерактивном» режиме, а не в режиме демона, даже если сервер запущен из командной строки оболочки. Установка этого параметра отменяет неявный режим демона при запуске из командной строки. samba-dcerpcd примет только одно соединение и завершит работу;
- `--debug-stdout` : вывести отладочную информацию в консоль/

Подробная информация о работе утилиты `samba-dcerpcd` предоставляется через запрос командой `man`:

```
man samba-dcerpcd
```

Для получения краткой справки необходимо вызвать утилиту с опцией `--help` или `-?`:

```
/usr/libexec/samba/samba-dcerpcd --help
/usr/libexec/samba/samba-dcerpcd -?
```

Samba перенастроена и внешний **RPC**-сервер запущен.

Для удобной работы на КД **ALD Pro** рекомендуется создать службу. Для этого необходимо

создать файл `/lib/systemd/system/samba-dcerpcd.service` со следующим содержимым:

```
[Unit]
Description=Samba DCERPC Daemon
Documentation=man:samba-dcerpcd(8)
After=network.target smbd.service
[Service]
Type=notify
PIDFile=/run/samba/samba-dcerpcd.pid
ExecStart=/usr/libexec/samba/samba-dcerpcd --libexec-rpcds
Restart=on-failure
[Install]
WantedBy=multi-user.target
```

3.8.38. Инструкция по работе двусторонних доверительных отношений между MS AD и ALD Pro

3.8.38.1. Введение

Для удобства администрирования в организации может быть несколько доменов.

Например, домен MS AD и домен ALD Pro. В домене MS AD будут находится компьютеры с операционной системой Windows. Домен ALD Pro будут содержать компьютеры с AstraLinux.

Для корректной работы необходима возможность гибридной работы пользователей сразу в двух доменах с помощью механизма доверительных отношений.

Ранее в ALD Pro уже были реализованы доверительные отношения MS AD –> ALD Pro. Но для полноценной работы, необходимы двусторонние доверительные отношения.

Популярный кейс:

Ранее организация работала в домене MS AD, и в рамках миграции инфраструктур был развернут домен ALD Pro (ald.company.lan). Для беспрерывной работы предполагается постепенный перевод сервисов и пользователей на работу в новом домене. В течение некоторого времени необходимо обеспечивать гибридную работу пользователей сразу в двух доменах с помощью механизма доверительных отношений.

3.8.38.2. Как работали доверительные отношения MS AD и ALD Pro ранее

До внедрения функционала глобального каталога и двусторонних доверительных отношений, было реализовано в полном объеме только одностороннее доверие. Домен ALD Pro полностью доверял домену под управлением MS AD, следовательно пользователи MS AD имели возможность доступа на клиентские компьютеры и сетевые ресурсы в домене ALD Pro.

Доступ на клиентские машины в домене MS AD осуществляется только с машинами под ОС Windows. Доступ через SSSD-client осуществляется только путем ввода машины в два домена, что возможно и без доверия.

При разграничении доступа к ресурсам не было возможности сопоставить пользователя ALD Pro с атрибутом, и осуществлять поиск пользователей.

3.8.38.3. Как работают теперь

1. Версии Windows Server работающие с глобальным каталогом ALD Pro
    - Windows Server 2008 R2
    - Windows Server 2012
    - Windows Server 2012 R2
    - Windows Server 2016
    - Windows Server 2019
2. ALD Pro должен быть версии 2.1.0 и выше, с установленным глобальным каталогом.
3. Версия Astra Linux не ниже 1.7.4.

Для работы с глобальным каталогом, его необходимо установить согласно разделу gc_syncer.

Механизм работы глобального каталога

В лесу Active Directory может быть много поддоменов, и, чтобы ускорить поиск нужной информации, разработчики Microsoft придумали такую роль, как **глобальный каталог** (англ. Global Catalog, GC).

Контроллер домена MS AD, которому назначена роль глобального каталога, с помощью штатной процедуры репликации извлекает из всех поддоменов краткую информацию об

объектах (англ. Partial Attribute Set, PAT) и предоставляет ее приложениям по запросу.

В FreeIPA нет глобального каталога, что становится проблемой при работе в доверительных отношениях с доменом MS AD, т.к. из-за этого Windows-администраторы не могу назначить права доступа пользователям доверенного домена FreeIPA с помощью стандартных оснасток (просто не работает поиск объектов из доверенного домена). Для решения этой проблемы в ALD Pro была реализована функция глобального каталога в виде дополнительного модуля.

Глобальный каталог ALD Pro – это отдельный экземпляр LDAP-сервера, в котором содержится копия всех объектов домена в схеме данных Active Directory. Глобальный каталог обеспечивает возможность поиска объектов (пользователей и групп) из стандартных оснасток Windows, что нужно для добавления субъектов доверенного домена в списки доступа на стороне Windows.

ГК состоит из следующих компонентов:

- Экземпляр LDAP-каталога (`dirsrv@GLOBAL-CATALOG`), работающий на стандартном для глобального каталога MS AD порту *3268/TCP*.
- Модуль синхронизации (`ipa-gcsyncd`) – служба, обеспечивающая синхронизацию объектов домена из обычного каталога в базу глобального каталога на том же контроллере домена.
- Модуль проверки целостности глобального каталога (`aldpro-gc-inspector`) – служба для выявления конфликтов синхронизации.

Для того чтобы клиенты MS AD могли обнаружить контроллеры домена ALD Pro, выполняющие функцию глобального каталога, в домене создаются SRV-записи вида:

- _gc._tcp.fqdn_имя_домена
- _gc._tcp.Default-First-Site-Name._sites.fqdn_имя_домена
- _ldap._tcp.Default-First-Site-Name._sites.gc._msdcs.fqdn_имя_домена
- _ldap._tcp.gc._msdcs.fqdn_имя_домена

Синхронизация работает на основе механизма репликации syncrepl. Служба ipa-gcsyncd извлекает информацию о пользователях и группах из основного LDAP-каталога, модифицирует ее с учетом схемы AD DS, которую ожидают увидеть клиенты Windows, и сохраняет в базу глобального каталога. Модификация учетных записей пользователей при синхронизации глобального каталога выполняется по шаблону `/opt/gc/templates/gcsync/gc_user_template.tmpl`:

```
{% macro first_val(attr) -%}
   {{ entry[attr][0] }}
{%- endmacro %}
dn: cn={{ first_val('uid') }},cn=users,{{ suffix }}
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: ad-top
objectClass: ad-organizationalPerson
objectClass: user
objectClass: securityPrincipal
objectClass: posixAccount
objectClass: inetUser
objectClass: gcobject
cn: {{ first_val('uid') }}
sn: {{ first_val('sn') }}
{%- if entry['givenname'] %}
givenName: {{ first_val('givenname') }}
{%- endif %}
instanceType: 4
{%- if entry['displayname'] %}
displayName: {{ entry.single_value['displayname'] }}
{%- endif %}
name: {{ first_val('cn') }}
objectGUID:: {{ guid }}
userAccountControl: 66048
primaryGroupID: 513
objectSid:: {{ sid }}
sAMAccountName: {{ pkey }}
sAMAccountType: 805306368
{%- if entry['krbcanonicalname'] %}
userPrincipalName: {{ entry.single_value['krbcanonicalname'] }}
{%- else %}
userPrincipalName: {{ first_val('krbprincipalname') }}
{%- endif %}
objectCategory: CN=Person,CN=Schema,CN=Configuration,{{ suffix }}
{%- if entry['mail'] %}
mail: {{ first_val('mail') }}
{%- endif %}
uidnumber: {{ first_val('uidnumber') }}
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
gidnumber: {{ first_val('gidnumber') }}
{%- for uid in entry['uid'] %}
uid: {{ uid }}
{%- endfor %}
homeDirectory: {{ first_val('homedirectory') }}
{%- for group in entry['memberof'] %}
memberof: {{ group }}
{%- endfor %}
nTSecurityDescriptor: D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;
 ↪RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY)(A;;RPLCLORC;;;AU)(OA;;WP;736e4812-af31-
 ↪11d2-b7df-00805f48caeb;bf967ab8-0de6-11d0-a285-00aa003049e2;CO)(A;;SD;;;CO)
gcuuid: {{ entryuuid }}
```

Модификация групп пользователей выполняется по шаблону `/opt/gc/templates/gcsync/gc_group_template.tmpl`:

```
{% macro first_val(attr) -%}
   {{ entry[attr][0] }}
{%- endmacro %}
dn: cn={{ pkey }},cn=users,{{ suffix }}
objectClass: top
objectClass: ad-top
objectClass: group
objectClass: securityprincipal
objectClass: nsmemberof
objectClass: gcobject
objectClass: posixGroup
cn: {{ pkey }}
instanceType: 4
name: {{ pkey }}
objectGUID:: {{ guid }}
objectSid:: {{ sid }}
sAMAccountName:  {{ pkey }}
sAMAccountType: 268435456
objectCategory: CN=Group,CN=Schema,CN=Configuration,{{ suffix }}
ntsecuritydescriptor: D:(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;
 ↪RPWPCRCCDCLCLORCWOWDSDDTSW;;;SY)(A;;RPLCLORC;;;AU)(A;;
 ↪RPWPCRCCDCLCLORCWOWDSDDTSW;;;AO)(A;;RPLCLORC;;;PS)(OA;;CR;ab721a55-1e2f-
 ↪11d0-9819-00aa0040529b;;AU)
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
{%- for member in entry['member'] %}
member: {{ member }}
{%- endfor %}
{%- for group in entry['memberof'] %}
memberof: {{ group }}
{%- endfor %}
gidnumber: {{ gidnumber }}
groupType: {{ groupType }}
gcuuid: {{ entryuuid }}
```

Одним из наиболее важных атрибутов для синхронизации объектов глобального каталога является **ipaNTSecurityIdentifier**, который определяет уникальный идентификатор субъектов безопасности Windows. Этот атрибут генерируется плагином **sidgen** и есть у всех пользователей и групп ALD Pro. При синхронизации глобального каталога значение текстового атрибута **ipaNTSecurityIdentifier** записывается в бинарный атрибут **ObjectSid**, который, собственно, и используется при добавлении субъектов безопасности в списки доступа на стороне Windows.

Механизм поиска и добавления субъектов ALD Pro в списки ACL на стороне Windows работает следующим образом:

1. Windows-администратор при добавлении пользователя/группы в ACL с помощью стандартной оснастки выполняет поиск объектов в доверенном домене ALD Pro. Запрос направляется к глобальному каталогу на порт 3268/TCP (LDAP) с аутентификацией по Kerberos. Если Kerberos-аутентификация по какой-либо причине не сработает (например, время в доменах отличается более, чем на 5 минут), то оснастка Windows попытается выполнить NTLM-аутентификацию, поэтому пользователь увидит окно для ввода учетных данных.

2. После успешного поиска появится список объектов ALD Pro с отображением их `uid` (в случае пользователя) или `cn` (в случае группы).

3. При добавлении субъекта в список доступа, система безопасности Windows выполнит еще один запрос к контроллеру домена ALD Pro по протоколу SMB для дополнительной проверки, существует ли субъект с таким SID в домене.

4. Для успешного выполнения указанного запроса на контроллере ALD Pro должны работать службы smbd и winbind. Обработка запроса выполняется с использованием библиотеки **ipasam** (или **aldprosam** в случае доверительных отношений между доменами ALD Pro).

5. После получения поодтверждения, что субъект с указанным SID существует в домене ALD Pro, система Windows добавит его в редактируемый список доступа.

3.8.38.4. Настройка двусторонних доверительных отношений

Для работы доверительных отношений с компьютеров из домена ALD.company.lan должны разрешаться имена компьютеров из домена WIN.company.lan и наоборот, нужно сделать взаимное перенаправление DNS-зон.

Настройка ALD Pro

Добавление зоны перенаправления можно сделать из графического интерфейса «Роли и службы сайта Служба разрешения имен Перенаправление запросов».

1. Имя зоны = имя домена MS AD.
2. Глобальные перенаправители = IP-адрес контроллера домена MS AD, с которым устанавливаются доверительные отношения.
3. Остальные поля и параметры оставить без изменений.

Настройка MS AD

Настройка контроллера домена MS AD осуществляется согласно официальным инструкциям к MS AD. (Пуск → Оснастка “DNS”):

1. Контекстное меню к “Серверы условной пересылки” → Создать сервер условной пересылки.
2. В поле “DNS-домен” ввести имя домена ALD Pro.
3. Добавить IP-адрес контроллера домена ALD Pro в блоке “IP-адреса основных серверов:”.

Создание двусторонних доверительных отношений осуществляется на портале управления ALD Pro на вкладке **Управление доменом** → **Интеграция с доменом** → **Доверительные отношения** (см. Справочный центр на портале или Руководство пользователя).

Выполнение данных команд предоставляет УЗ Администратора доступ к атрибуту krbPrincipalKey у сервисного принципала cifs, что необходимо для успешного создания двусторонних доверительных отношений.

При создании доверительных отношений с доменом MS AD необходимо указать диапазон идентификаторов для доверенного домена MS AD.

На всех контроллерах домена ALD Pro и файловых серверах в конфигурационный файл `samba` необходимо добавить следующие параметры:

```
idmap config <netbios домена MS AD> : range = 261600000 - 261800000
idmap config <netbios домена MS AD> : backend = sss
```

Диапазон идентификаторов выводится с помощью команды:

```
ipa idrange-find
```

Пример:

```
astr@dc01:~$ ipa idrange-find
-------------------
найдено 4 диапазона
-------------------
Имя диапазона: MSAD.DOMEN.RU_id_range
Первый идентификатор POSIX диапазона: 618600000
Количество идентификаторов в диапазоне: 200000
Первый RID соответствующего диапазона RID: 0
SID доверенного домена: S-1-5-21-3537296142-1636428635-2476405179
Тип диапазона: Active Directory domain range
Имя диапазона: MVPWIN16.DOMEN.RU_id_range
Первый идентификатор POSIX диапазона: 261600000
Количество идентификаторов в диапазоне: 200000
Первый RID соответствующего диапазона RID: 0
SID доверенного домена: S-1-5-21-3894048104-315847931-183599100
Тип диапазона: Active Directory domain range
```

Из этого:

```
idmap config <netbios домена MS AD> : range = <Первый идентификатор POSIX
 ↪диапазона> - <Первый идентификатор POSIX диапазона> + <Количество
 ↪идентификаторов в диапазоне>
```

После указания диапазонов идентификаторов необходимо перезапустить `samba`:

```
sudo systemctl restart smbd winbind
```

Необходимо обратить внимание на созданный диапазон идентификаторов, чрезвычайно важно чтобы в созданный диапазон доверенного домена входили RID пользователей этого домена. В противном случае диапазон необходимо расширить или пересоздать двусторонние доверительные отношения с параметром `--range-size=<количество идентификаторов в диапазоне>`.

Важно: После создания двусторонних доверительных отношений через некоторое время (в зависимости от того сколько реплик MS AD) может возникнуть ошибка с добавлением объектов через групповые политики. В этом случае необходимо удалить, а затем заново создать доверительные отношения. При этом записи с диапазона идентификаторов для доверенного домена и конфигурационный файл с `samba` оставить как есть (не удалять).

Для доступа к ресурсам windows с аутентификацией по kerberos (IIIS, cifs, принтеры с общим доступом по smb) необходимо отключить у клиентских компьютеров FAST аутентификацию, так как windows её не поддерживает. Для этого на всех клиентах ALD Pro, где предполагается доступ, необходимо настроить глобальную политику **Групповые политики → Параметры компьютеров → Безопасность → FAST аутентификация**. Выставить параметр never.

Важно: Установка этого параметра понижает безопасность.

При первом применении может понадобиться перезагрузка сервиса sssd.

Проверить двусторонние доверительные отношения можно следующими способами:

1. авторизация на компьютере домена MS AD;
2. авторизация на компьютере домена ALD Pro;
3. создание общей папки.

Авторизация на компьютере домена MS AD

Необходимо авторизоваться на компьютере домена MS AD, используя учетную запись пользователя ALD Pro. Логин должен быть указан полностью, включая имя домена:

```
<имя_пользователя ALD Pro>@<имя_домена>
```

В результате пользователь под учетной записью ALD Pro авторизуется на компьютере домена MS AD.

Авторизация на компьютере домена ALD Pro

Необходимо выбрать нужный домен MS AD и авторизоваться на компьютере домена ALD Pro, используя учетную запись пользователя MS AD. В поле **Имя пользователя** необходимо указать имя пользователя, без имени домена.

В результате пользователь под учетной записью MS AD авторизуется на компьютере домена ALD Pro.

Создание общей папки

1. Создание общей папки на компьютере домена MS AD.

Необходимо создать папку **C:Common** и добавить в нее хотя бы один файл. Открыть доступ к созданной папке из контекстного меню **Sharing → Share → Network access**. Настройки оставить по умолчанию.

В окне **Common PropertiesSharingAdvanced SettingsPermissions** будет отображена информация, что по умолчанию на уровне SMB все пользователи, включая пользователей ALD Pro, имеют полные права.

Но доступ к файлам регулируется также на уровне NTFS разрешений, которые настраиваются на вкладке **Common PropertiesSecurity**. Можно предоставить доступ к общей папке всем аутентифицированным пользователям.

В результате пользователи ALD Pro могут редактировать файлы, находящиеся в папке **Common**.

2. Создание общей папки на компьютере домена ALD Pro.

Необходимо создать новое сетевое место, которое соответствует папке **Common** в файловом менеджере. Для этого выбрать **Сеть → Создать сетевое место**. Указать **Название** и **Адрес** в формате:

```
smb://<полное наименование контроллера домена MS AD, на котором создана папка>
↪/<Наименование папки из MS AD>
```

В результате пользователи MS AD могут редактировать файлы, находящиеся в папке **Common**.

3.8.38.5. Заключение

Благодаря внедрению ряда решений, включая глобальный каталог ALD Pro, есть возможность настраивать двусторонние доверительные отношения. В отличие от MS AD, в ALD Pro направления доверия MS AD → ALD Pro и ALD Pro → MS AD реализованы разными механизмами.

Двусторонние доверительные отношения, предоставляют возможность общаться доменам ALD Pro и MS AD, решая ряд важных задач:

- Авторизация пользователей доверенных доменах на рабочих станциях;
- Доступ к сетевым ресурсам пользователей доверенного домена (веб сервер, файловый сервер, базы данных и т.д.);
- Разграничение доступа к ресурсам доверенных доменов.

3.8.39. Инструкция по присоединению системы Windows к FreeIPA Realm без Active Directory

Большинство системных администраторов имеют опыт использования компьютеров под управлением ОС Windows в домене Active Directory, но в качестве источника идентификационной информации компьютеры Windows могут использовать и область Kerberos от ALD Pro (FreeIPA). Способ, которым можно ввести Windows в домен FreeIPA был известен давно, но не получил широкого распространения, т. к. содержал существенный недостаток — внутри операционной системы пользователь действовал от имени локальной учетной записи, которую нужно было создавать заранее. В настоящей инструкции описан способ, который позволяет обеспечить вход в операционную систему именно доменной учетной записью, сохраняя ее SID, участие в группах и Kerberos билеты, что открывает новые возможности по решению задач гибридного развертывания и миграции.

3.8.39.1. Что такое Active Directory

Active Directory - это база данных специального назначения со службами, которые позволяют пользователям подключаться к привязанным к ней сетевым ресурсам. В этой базе данных хранится важная информация о вашей среде, такая как пользователь и компьютеры, которым разрешено устанавливать подключения. Поскольку Active Directory является продуктом Microsoft, он часто используется в среде Windows.Он обеспечивает эти функциональные возможности путем хранения пользовательских, групповых, хостовых и любых других данных, необходимых для управления безопасностью сетевых компьютеров. Что делает этот инструмент более совершенным, так это его простой и понятный в использовании веб-интерфейс, а также командная строка для администрирования.

3.8.39.2. Что такое FreeIPA

FreeIPA - это бесплатное интегрированное решение для управления информацией о безопасности с открытым исходным кодом, спонсируемое RedHat. Он сочетает в себе MIT Kerberos, Dogtag (систему сертификатов), NTP, DNS и сервер каталогов 389. Основная цель состоит в том, чтобы обеспечить функциональность, аналогичную Active Directory. Его можно использовать для обеспечения централизованной аутентификации, авторизации и получения информации об учетной записи.

FreeIPA не является повторной реализацией Microsoft Active Directory и может работать независимо. Основное различие между ними заключается в том, что FreeIPA ориентирована на Linux и другие системы, соответствующие стандартам POSIX, в то время как Active Directory является инструментом Windows.

ALD Pro(FreeIPA) может быть интегрирован для работы с Active Directory путем установления доверия между двумя службами. Но в этом руководстве настраивается система Windows на использование области FreeIPA для аутентификации пользователей без Active Directory.

Чтобы достичь этого, необходимо выполнить приведенные ниже шаги.

3.8.39.3. Требования к настройке

В этом руководстве будут настроены две системы со статическими IP-адресами и именами хостов:

TASK	HOSTNAME	IP_ADDRESS
FreeIPA server(ALD Pro)	ald01.ald.dom	192.168.88.210
Windows client	Win10test.ald.dom	192.168.88.76

3.8.39.4. Порядок присоединения

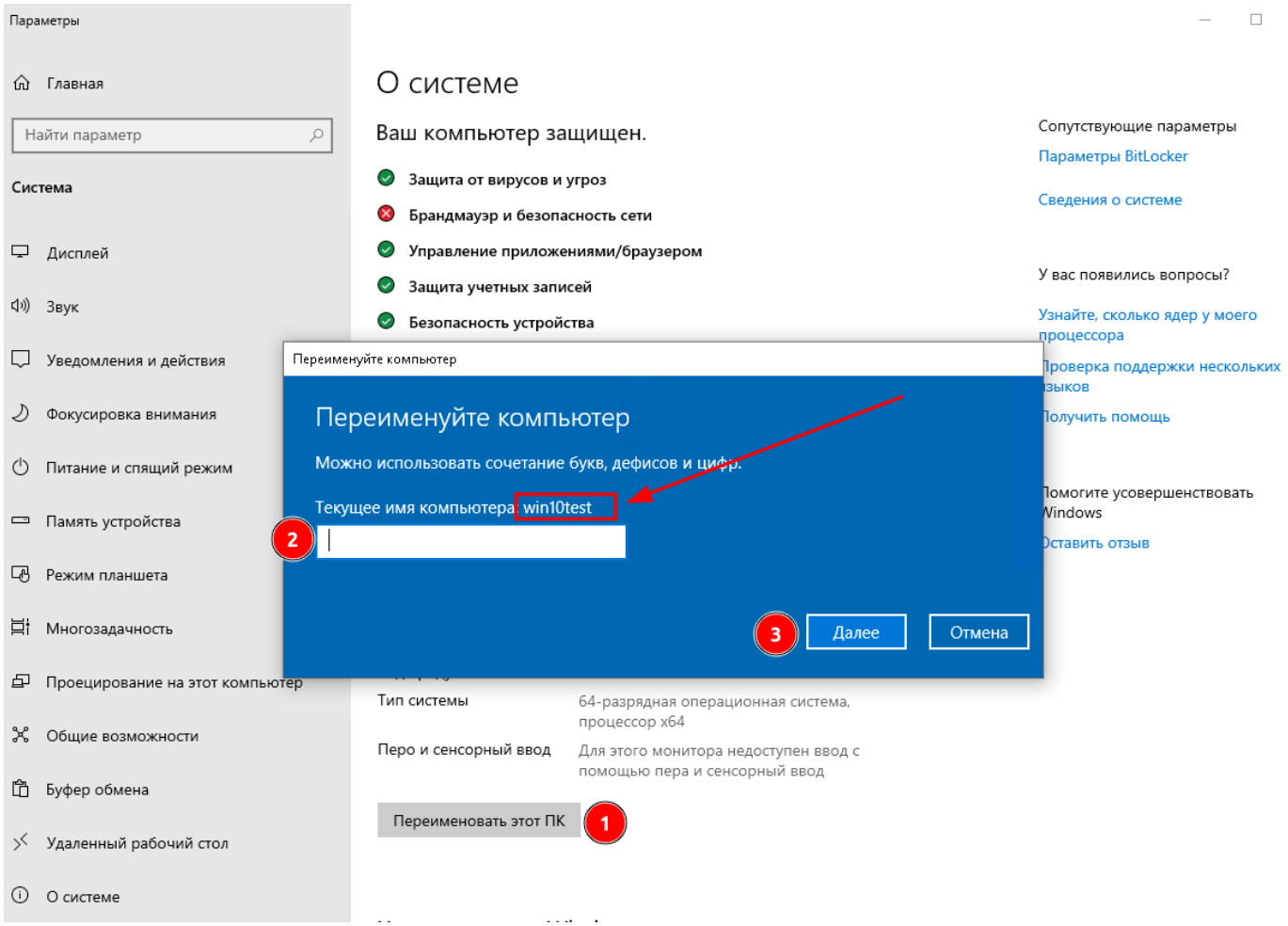


Рисунок 3.53 – Установка имени хоста

Нажать Win+R и запустить ncpa.cpl для настройки сети. Сначала настраивается DNS таким образом, чтобы он мог разрешать имя ALD Pro(IPA)-сервера.

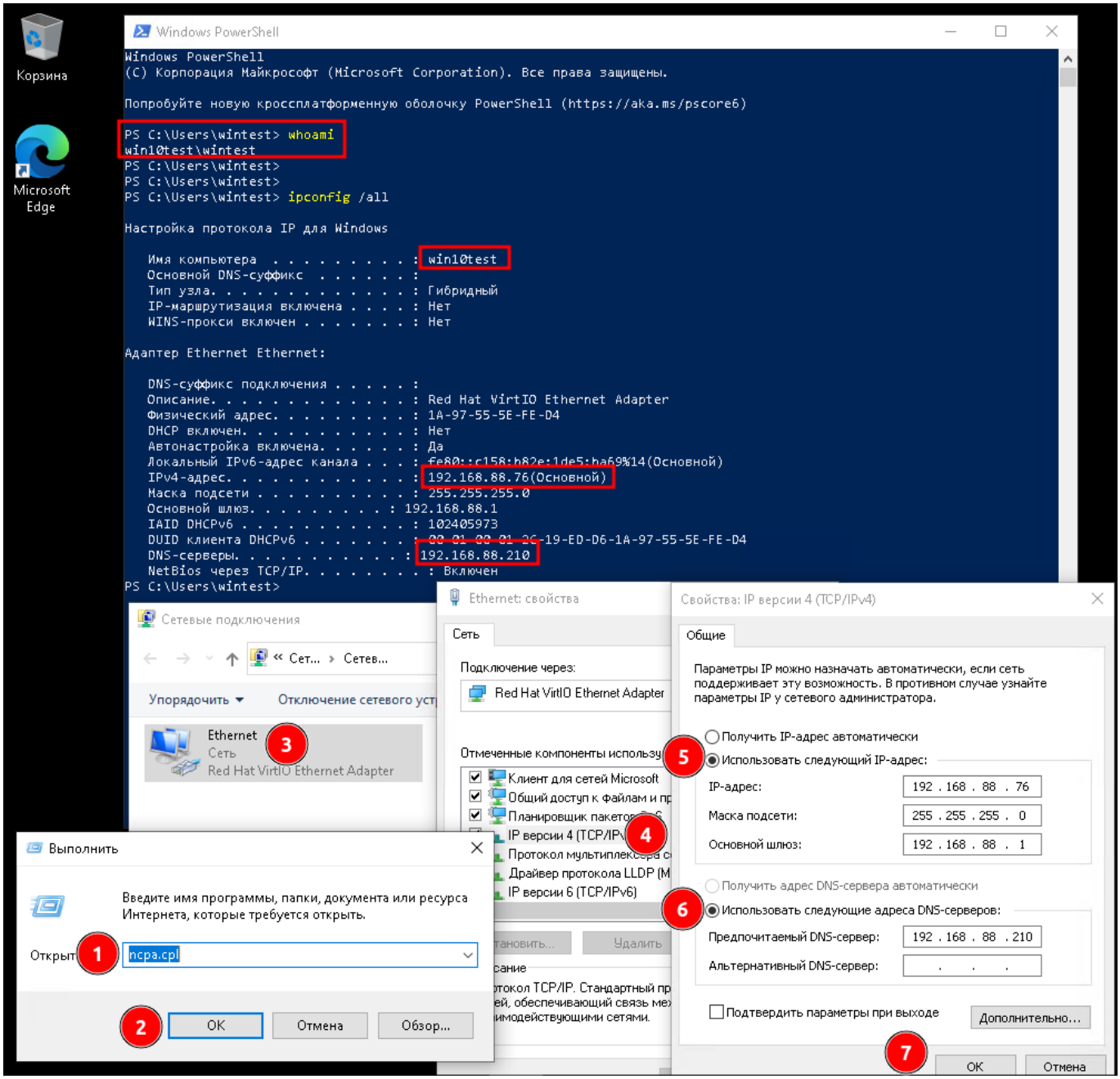


Рисунок 3.54 – Настройка сети на Windows машине 1

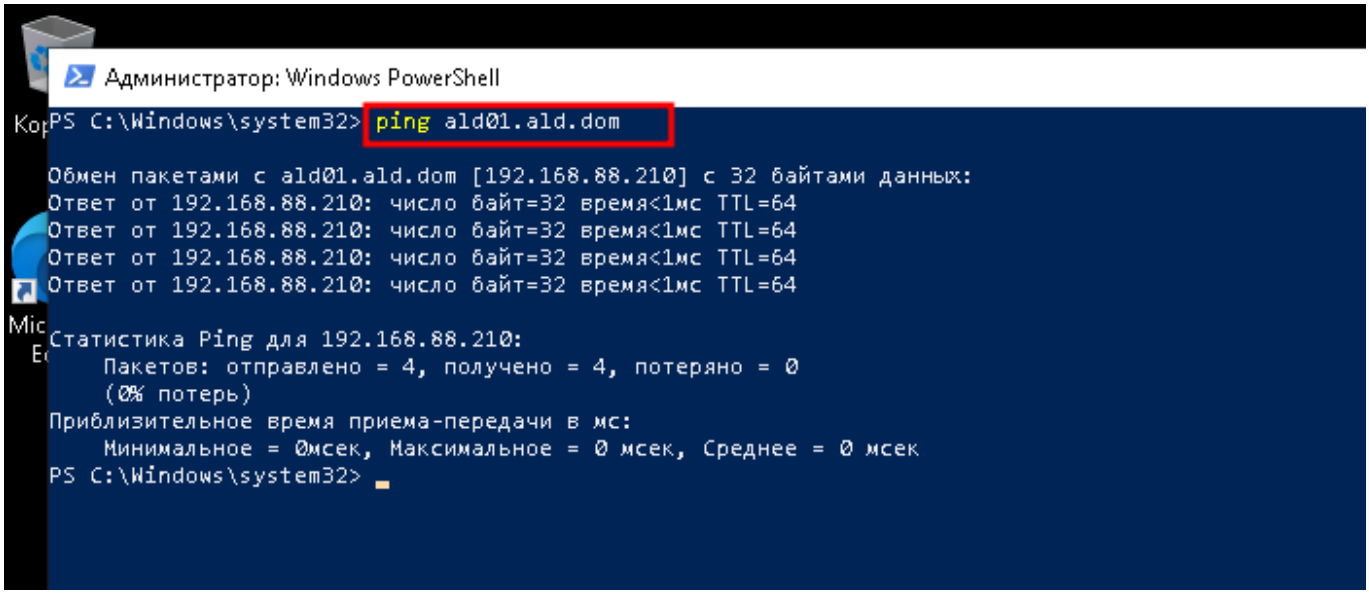


Рисунок 3.55 – Настройка сети на Windows машине 2

На стороне ALD Pro(FreeIPA) необходимо убедиться, что время не расходится с внешним NTP сервером

```
# chronyc tracking
root@ald01:~# chronyc tracking
Reference ID    : BCE109A7 (188.225.9.167)
Stratum         : 3
Ref time (UTC)  : Tue Jun 13 10:08:13 2023
System time     : 0.000034270 seconds slow of NTP time
Last offset     : -0.000079430 seconds
RMS offset      : 0.000206107 seconds
Frequency       : 9.831 ppm slow
Residual freq   : -0.001 ppm
Skew            : 0.061 ppm
Root delay      : 0.017628554 seconds
Root dispersion : 0.003091000 seconds
Update interval : 1040.0 seconds
Leap status     : Normal
root@ald01:~#
root@ald01:~#
root@ald01:~# timedatectl
               Local time: Tue 2023-06-13 13:14:55 MSK
           Universal time: Tue 2023-06-13 10:14:55 UTC
                 RTC time: Tue 2023-06-13 10:14:55
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
               Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
              NTP service: inactive
          RTC in local TZ: no
```

На стороне Windows настраивается синхронизация времени с контроллером домена в роли NTP сервера. Можно указать несколько значений (FQDN или IP адрес) через запятую, что не обеспечивает возможность автообнаружения контроллеров

```
w32tm /config /reliable:yes /syncfromflags:manual /manualpeerlist:"<NTPServer>
 ↪" /update
```

```
net start w32time

w32tm /config /reliable:yes /syncfromflags:manual /manualpeerlist:"ald01.ald.
 ↪dom" /update
net stop w32time
net start w32time
w32tm /resync
w32tm /monitor /computers:"ald01.ald.dom"
w32tm /stripchart /computer:ald01.ald.dom
```

Результат проверки времени

```
PS C:\Users\Administrator> w32tm /stripchart /computer:ald01.ald.dom
Tracking ald01.ald.dom [192.168.88.210:123].
The current time is 4/13/2023 1:40:55 PM.
13:40:55, d:+00.0091883s o:-00.0110417s  [                              *      □
 ↪                     ]
13:40:57, d:+00.0093593s o:-00.0111335s  [                              *      □
 ↪                     ]
13:40:59, d:+00.0099441s o:-00.0112867s  [                              *      □
 ↪                     ]
13:41:01, d:+00.0100102s o:-00.0113176s  [                              *      □
 ↪                     ]
```

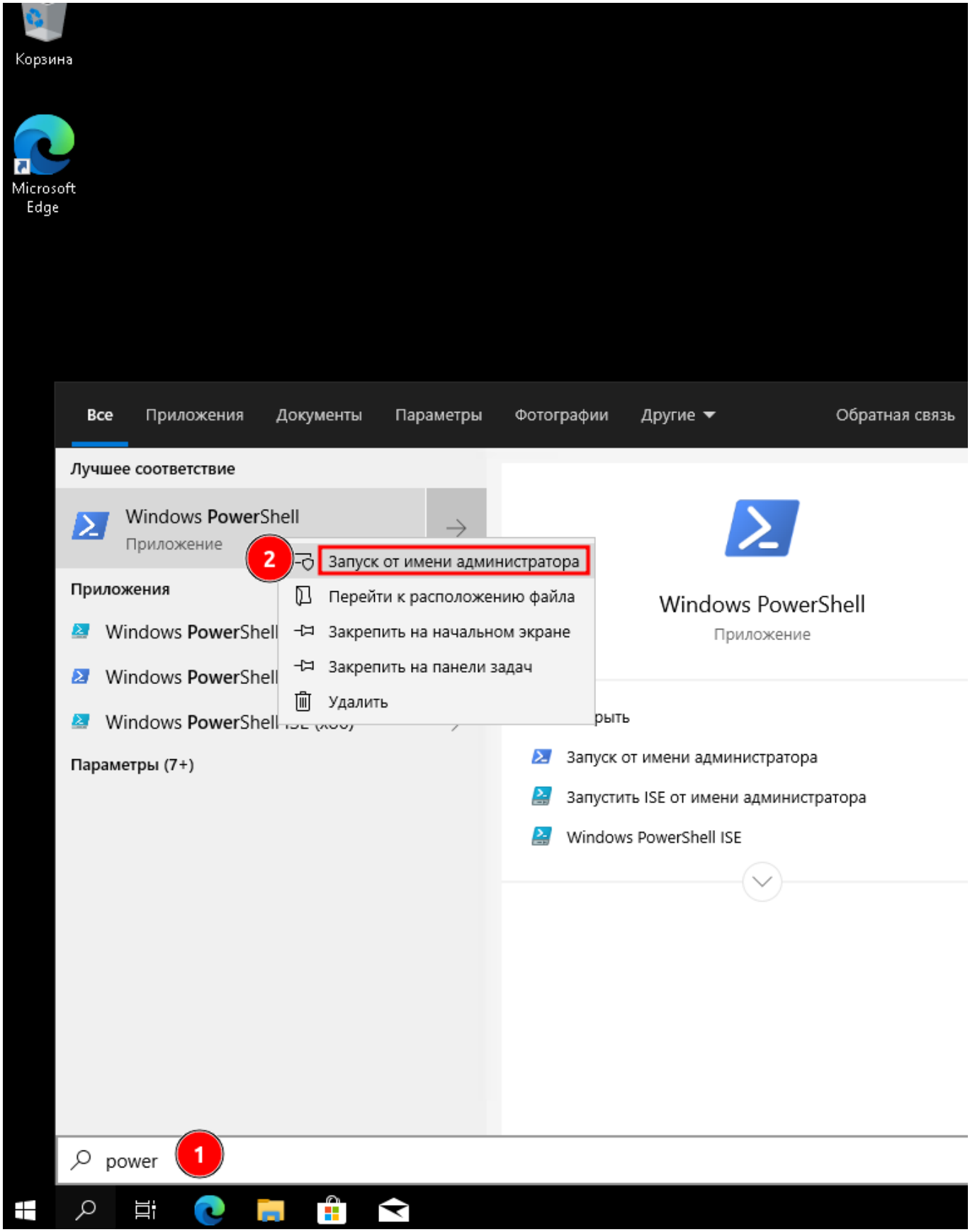


Рисунок 3.56 – Настройки даты/времени 1

В данном примере указан IP адрес

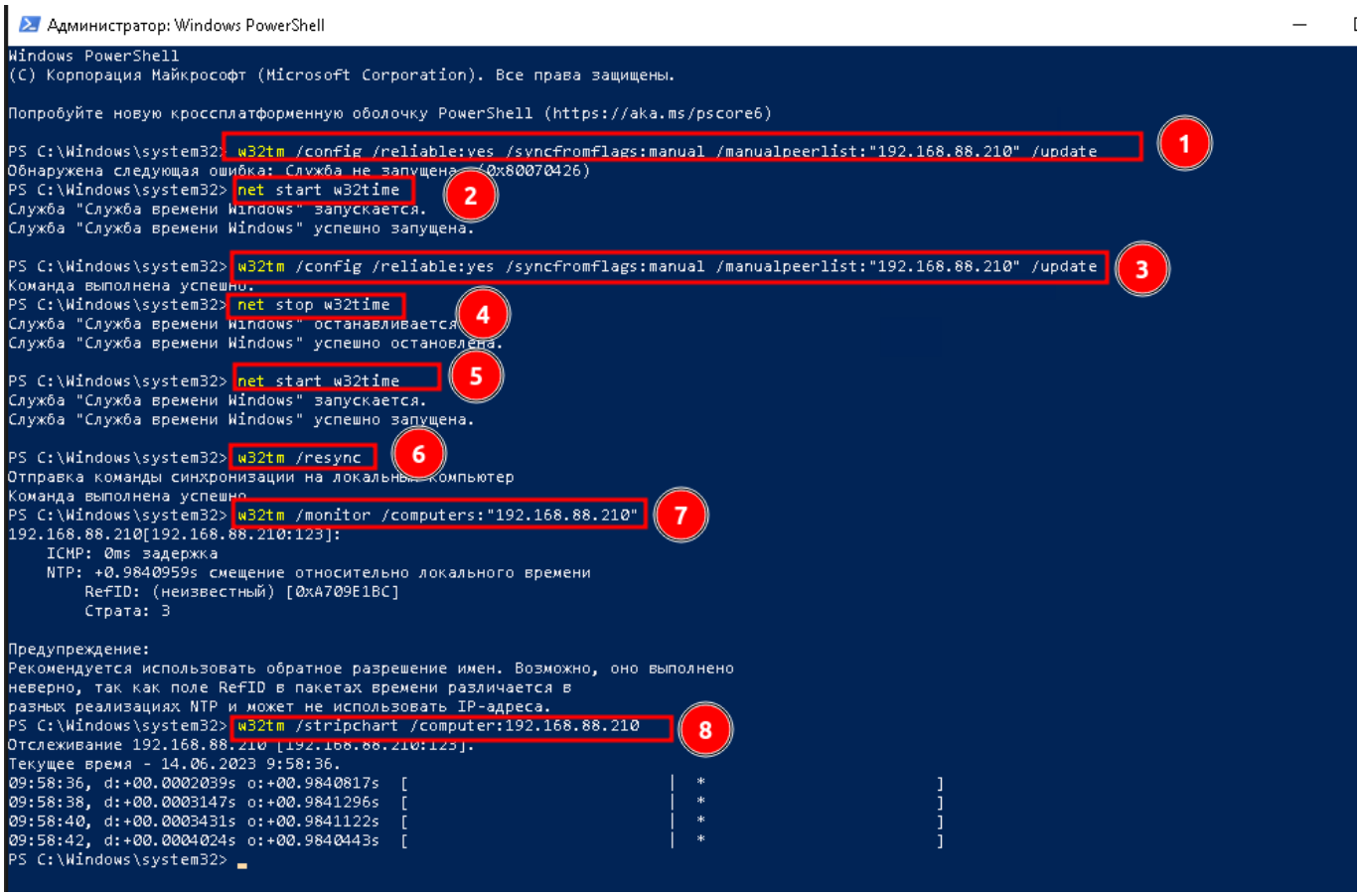


Рисунок 3.57 – Настройки даты/времени 2

В веб-консоли перейти на вкладку хосты и нажать кнопку Добавить.

Указать имя хоста и IP-адрес клиента Windows, как показано на рисунке.

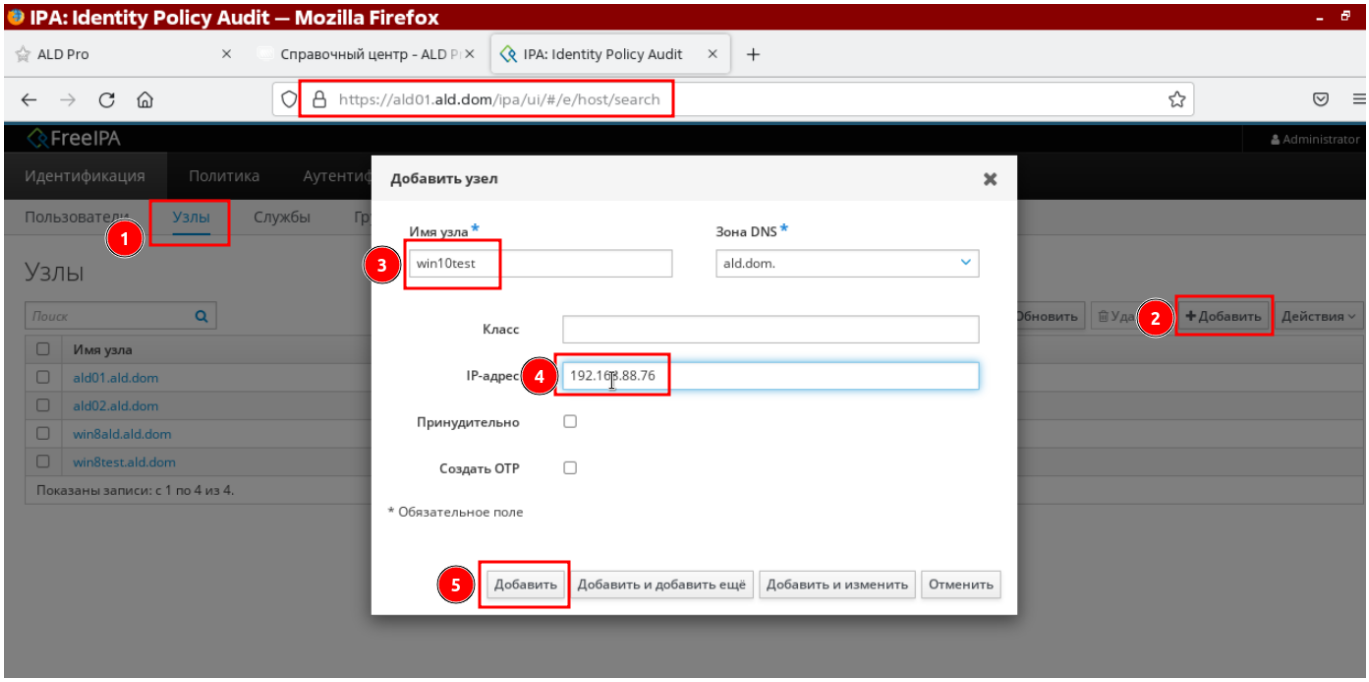


Рисунок 3.58 – Создание нового узла в консоли FreeIPA 1

Клиент был добавлен, но еще не зарегистрирован.

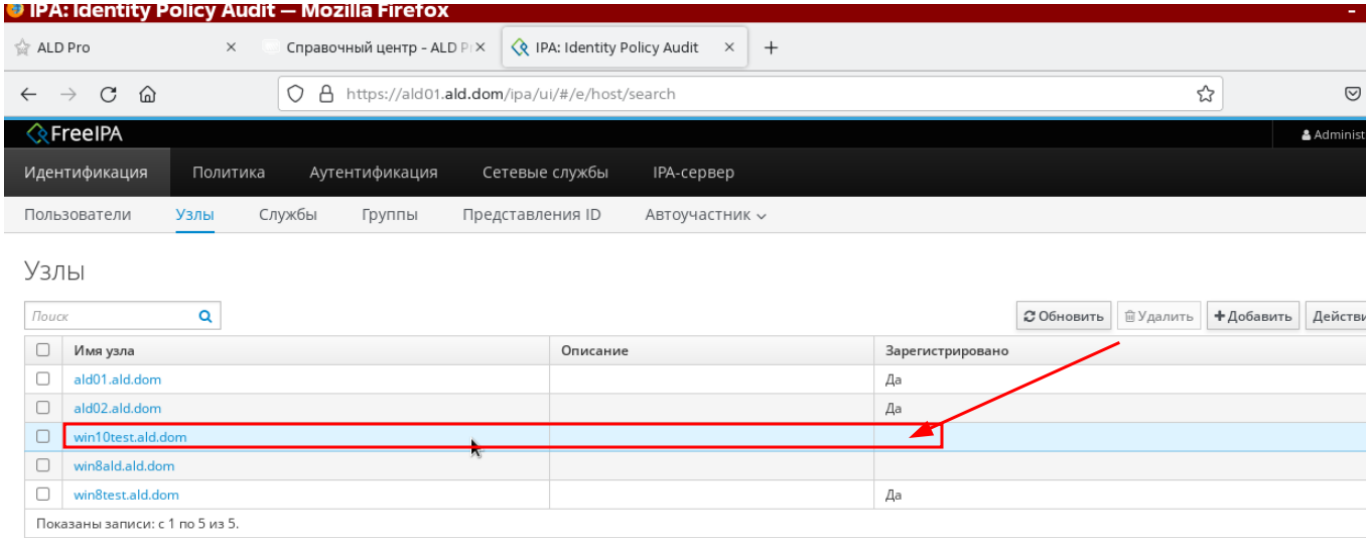


Рисунок 3.59 – Создание нового узла в консоли FreeIPA 2

Таблица ключей(keytab) - это файл, содержащий пары участников Kerberos и зашифрованные ключи (которые являются производными от пароля Kerberos).

Аутентификация(Authentication) - это процесс проверки личности зарегистрированного пользователя или процесса перед предоставлением доступа к защищенным сетям и системам.

В командной строке FreeIPA добавить клиента.

Сначала генерируется билет (Выполните аутентификацию) с помощью команды:

```
root@ald01:~#kinit admin
root@ald01:~#kinit admin
Password for admin@ALD.DOM:
root@ald01:~#
root@ald01:~#
root@ald01:~# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_sN0WuVv
Default principal: admin@ALD.DOM

Valid starting     Expires            Service principal
06/13/23 13:36:28  06/14/23 13:36:24  krbtgt/ALD.DOM@ALD.DOM
```

Для получения поддерживаемых типов шифрования выполнить команду:

```
root@ald01:~# ipa-getkeytab --permitted-enctypes
Failed to load translations
Supported encryption types:
AES-256 CTS mode with 96-bit SHA-1 HMAC
AES-128 CTS mode with 96-bit SHA-1 HMAC
AES-256 CTS mode with 192-bit SHA-384 HMAC
AES-128 CTS mode with 128-bit SHA-256 HMAC
Triple DES cbc mode with HMAC/sha1
ArcFour with HMAC/md5
Camellia-128 CTS mode with CMAC
Camellia-256 CTS mode with CMAC
```

Добавить участника, используя команду с приведенным ниже синтаксисом. Необходимо включить типы шифрования:

```
root@ald01:~#ipa-getkeytab -s ald01.ald.dom -p host/win10test.ald.dom@ALD.
 ↪DOM -e aes256-cts,aes128-cts,aes256-sha2,aes128-sha2,camellia256-cts-cmac,
 ↪camellia128-cts-cmac -k /etc/krb5.keytab.windows -P
```

В приведенной выше команде:

-s указывает сервер FreeIPA;

-e определяет шифрование;

-k путь до существующего или нового keytab файла;

-p указывает нового участника, который будет добавлен;

-P устанавливает пароль (**не забудьте, так как он будет использоваться при настройке клиента позже**).

```
root@ald01:~# kinit admin
Password for admin@ALD.DOM:
root@ald01:~#
root@ald01:~# ipa-getkeytab -s ald01.ald.dom -p host/win10test.ald.dom@ALD.
 ↪DOM -e aes256-cts,aes128-cts,aes256-sha2,aes128-sha2,camellia256-cts-cmac,
 ↪camellia128-cts-cmac -k /etc/krb5.keytab.windows -P
Failed to load translations
New Principal Password:
Verify Principal Password:
Keytab successfully retrieved and stored in: /etc/krb5.keytab.windows
```

Проверка, был ли добавлен ключ:

```
root@ald01:~# klist -k /etc/krb5.keytab.windows
Keytab name: FILE:/etc/krb5.keytab.windows
KVNO Principal
---- --------------------------------------------------------------------------
 ↪-
   1 host/win8test.ald.dom@ALD.DOM
   1 host/win8test.ald.dom@ALD.DOM
   1 host/win8test.ald.dom@ALD.DOM
   1 host/win8test.ald.dom@ALD.DOM
   1 host/win8test.ald.dom@ALD.DOM
   1 host/win8test.ald.dom@ALD.DOM
   1 host/win10test.ald.dom@ALD.DOM
   1 host/win10test.ald.dom@ALD.DOM
   1 host/win10test.ald.dom@ALD.DOM
   1 host/win10test.ald.dom@ALD.DOM
   1 host/win10test.ald.dom@ALD.DOM
   1 host/win10test.ald.dom@ALD.DOM
```

Вернуться к веб-интерфейсу FreeIPA, клиент должен быть зарегистрирован.

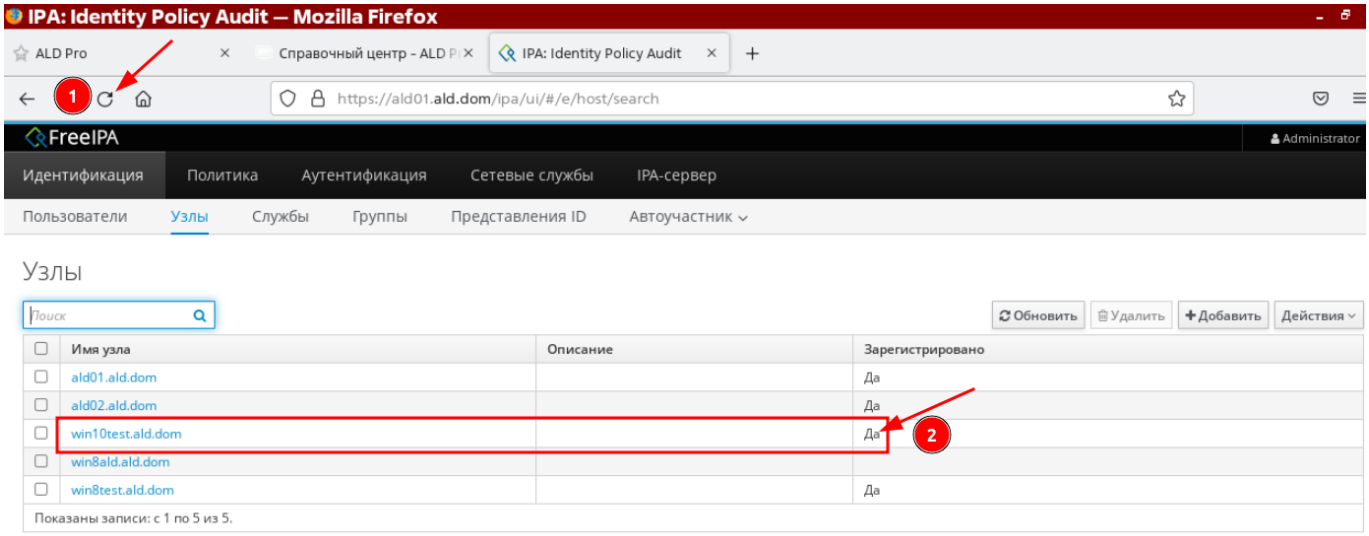


Рисунок 3.60 – Создание keytab 1

Чтобы иметь возможность использовать FreeIPA для аутентификации в Windows, необходимо создать пользователя в FreeIPA. На FreeIPA странице перейти на вкладку Пользователи и добавить пользователя, как показано на рисунке:

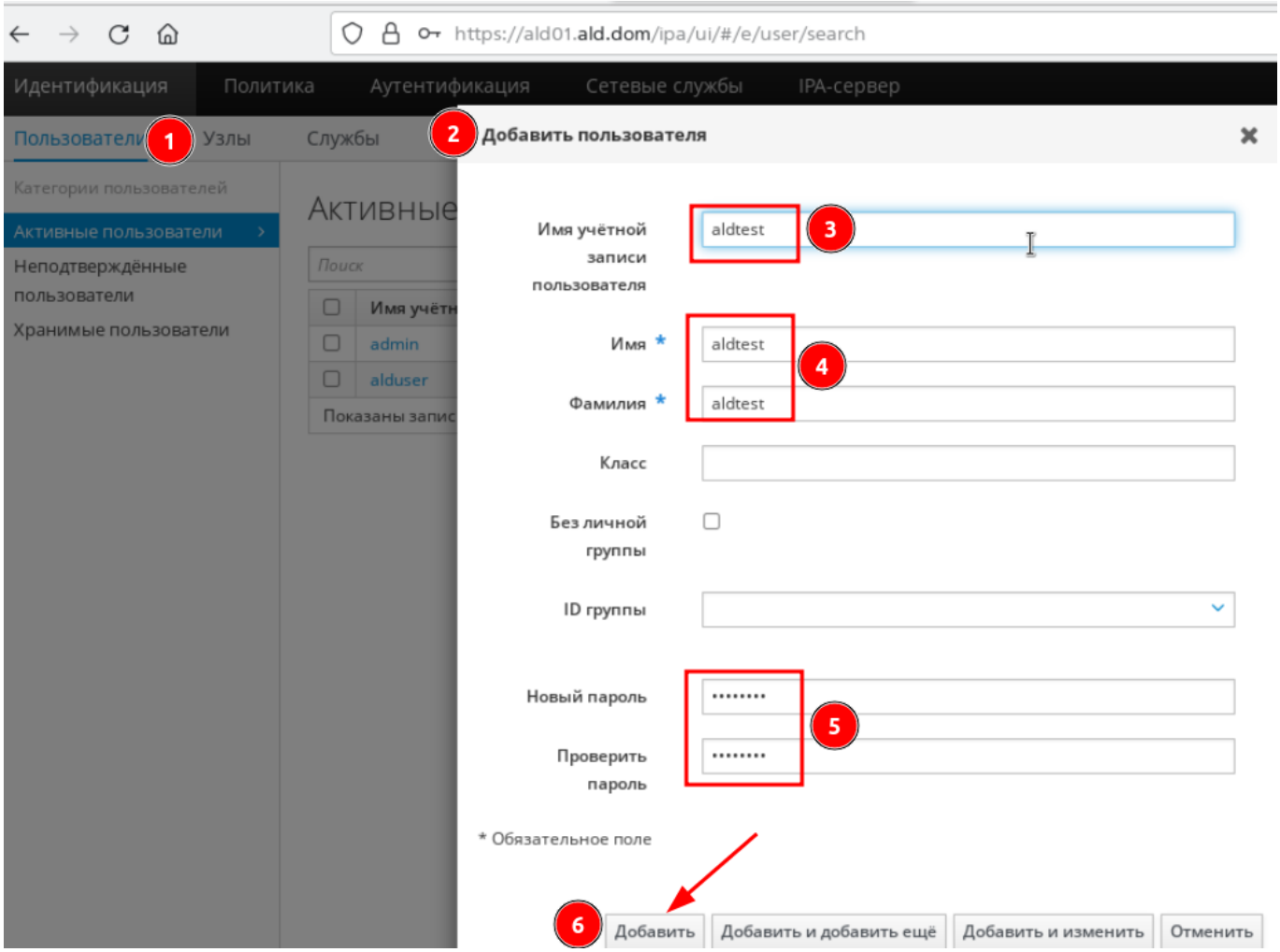


Рисунок 3.61 – Создание пользователя в FreeIPA

Указанный пароль при создании пользователя необходимо сменить при первом входе в систему.

Добавленный пользователь появится, как показано на рисунке.

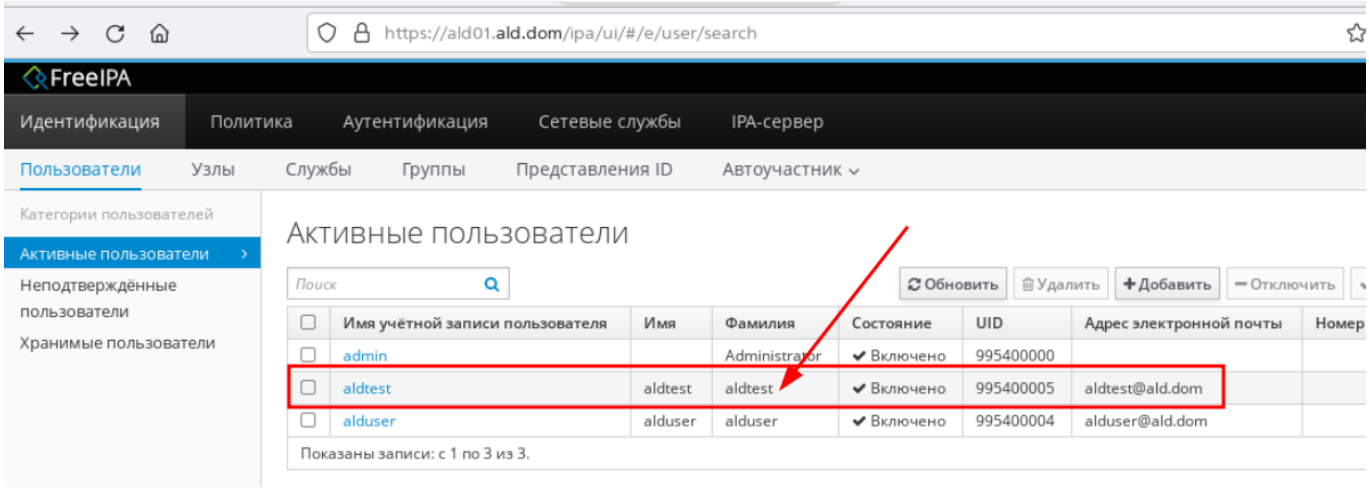


Рисунок 3.62 – Добавленный пользователь

```
ksetup /setdomain [REALM NAME]
ksetup /addkdc [REALM NAME] [kdc DNS name]
ksetup /addkpasswd [REALM NAME] [kdc DNS name]
ksetup /setcomputerpassword [MACHINE_PASSWORD] #(пароль из шага 5 при
 ↪генерировании keytab)
# ksetup /mapuser * *
```

`ksetup /setdomain` - Задает доменное имя для всех операций Kerberos.

https://learn.microsoft.com/ru-ru/windows-server/administration/windows-commands/ksetup-domain

`ksetup /addkdc` - Добавляет адрес центра распространения ключей (KDC) для заданной области Kerberos.

https://learn.microsoft.com/ru-ru/windows-server/administration/windows-commands/ksetup-addkdc

`ksetup addkpasswd` - Добавляет адрес сервера kerberos password (kpasswd) для области.

https://learn.microsoft.com/ru-ru/windows-server/administration/windows-commands/ksetup-addkpasswd

`ksetup /setcomputerpassword` - Задает пароль для локального компьютера. Эта команда влияет только на учетную запись компьютера и требует перезагрузки, чтобы изменение пароля вступило в силу.

Примечание: Пароль учетной записи компьютера не отображается в реестре или в качестве выходных данных команды ksetup.

https://learn.microsoft.com/ru-ru/windows-server/administration/windows-commands/ksetup-setcomputerpassword

В инструкциях встречается указание, что необходимо выполнить команду ksetup /mapuser, чтобы сопоставить все учетные записи в области ALD.DOM Kerberos с любой существующей учетной записью с тем же именем на этом компьютере.

Благодаря использованию доменных учётных записей пользователей, нет необходимости сопоставлять им локальные “учётки”.

https://learn.microsoft.com/ru-ru/windows-server/administration/windows-commands/ksetup-mapuser

Выполнить поочередно следующие команды (Не перезагружать компьютер):

```
ksetup /setdomain ALD.DOM
ksetup /addkdc ALD.DOM ald01.ald.dom
ksetup /addkpasswd ALD.DOM ald01.ald.dom
ksetup /setcomputerpassword !QAZ1qaz (укажите свой пароль)
```

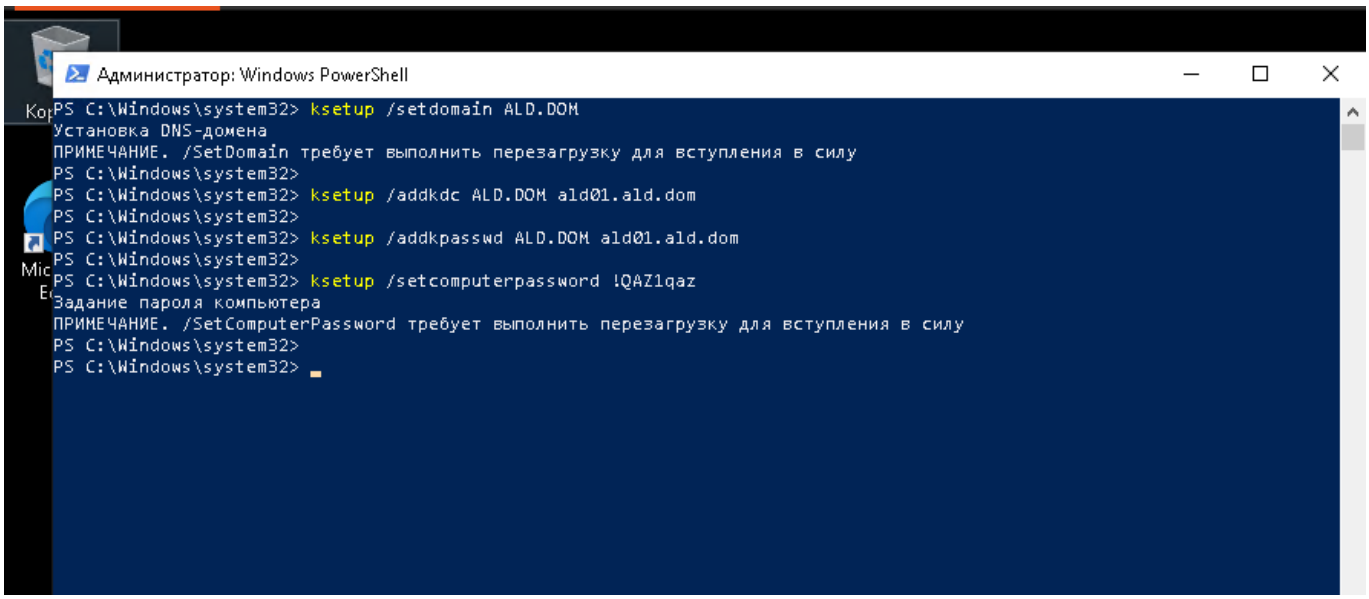


Рисунок 3.63 – Результат выполнения команд

Теперь запустить **gpedit.msc**, нажав клавишу Windows + R.

Конфигурация Windows > Параметры безопасности, Локальные политики, Параметры Безопасности > Сетевая безопасность: настройка типов шифрования, разрешенных Kerberos

Windows Settings > Security Settings > Local Policies > Security Options > Network Security: Configure encryption types allowed for Kerberos

Указать следующие типы шифрования:

RC4_HMAC_MD5,AES128_HMAC_SHA1,AES256_HMAC_SHA1,Будущие типы шифрования

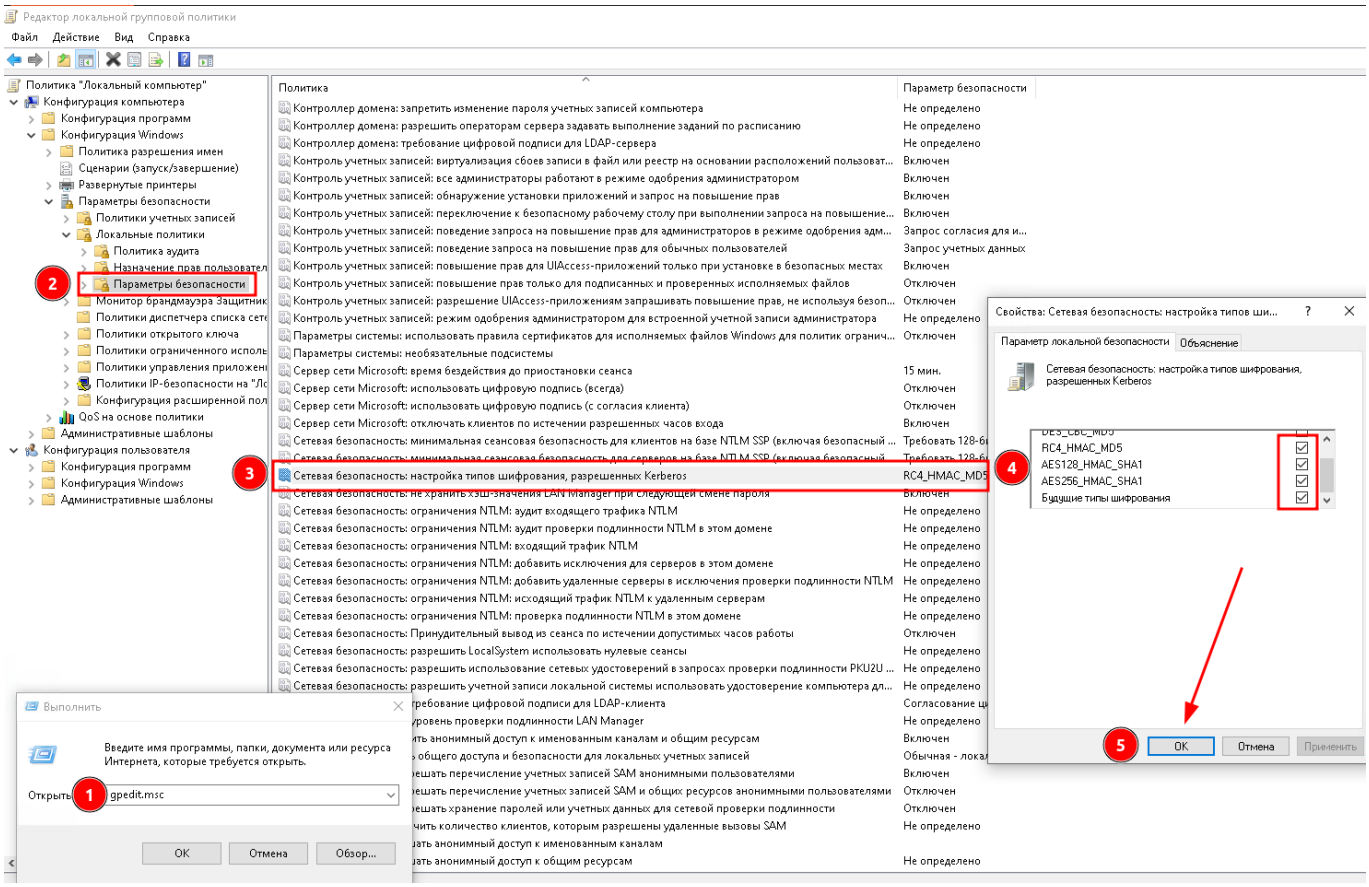


Рисунок 3.64 – Типы шифрования

Применить, нажав кнопку OK, и перезагрузить систему.

Имя Пользователя@REALM aldtest@ALD.DOM

Когда система перезагрузится, войти в систему с помощью пользователя FreeIPA, как показано на рисунке:

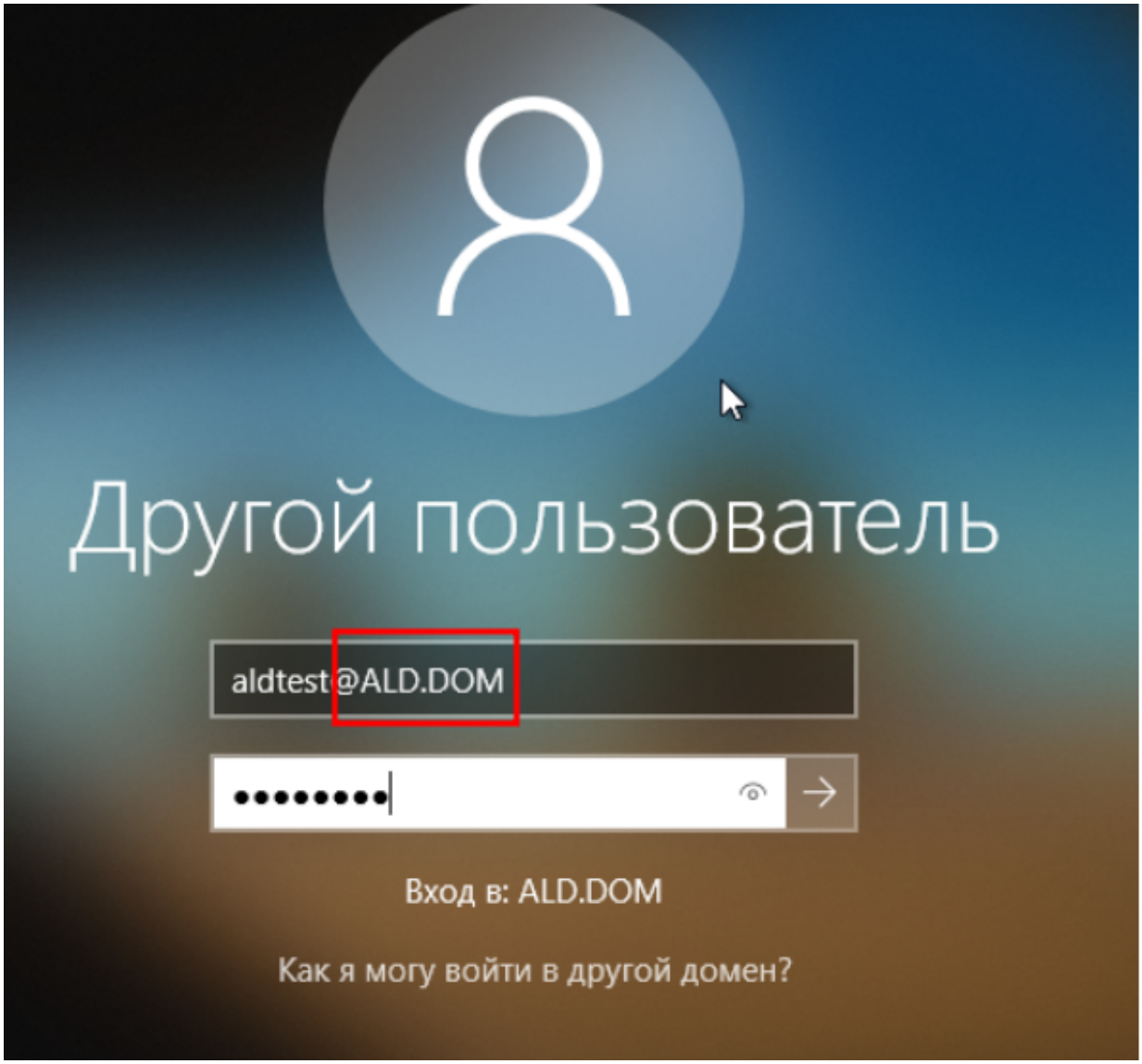


Рисунок 3.65 – Вход в систему

Будет предложено изменить пароль для пользователя IPA.

Выполнить следующие команды в PowerShell или CMD:

```
whoami
klist
```

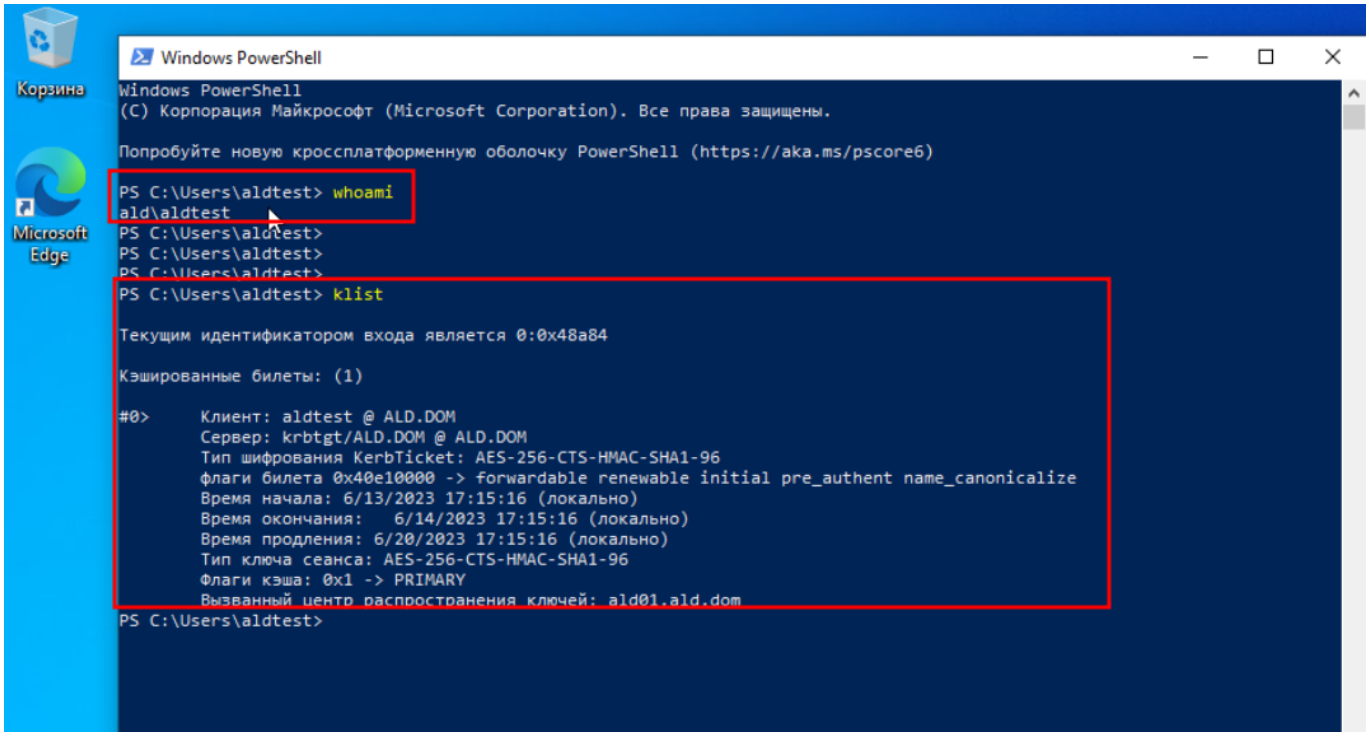


Рисунок 3.66 – Проверки 1

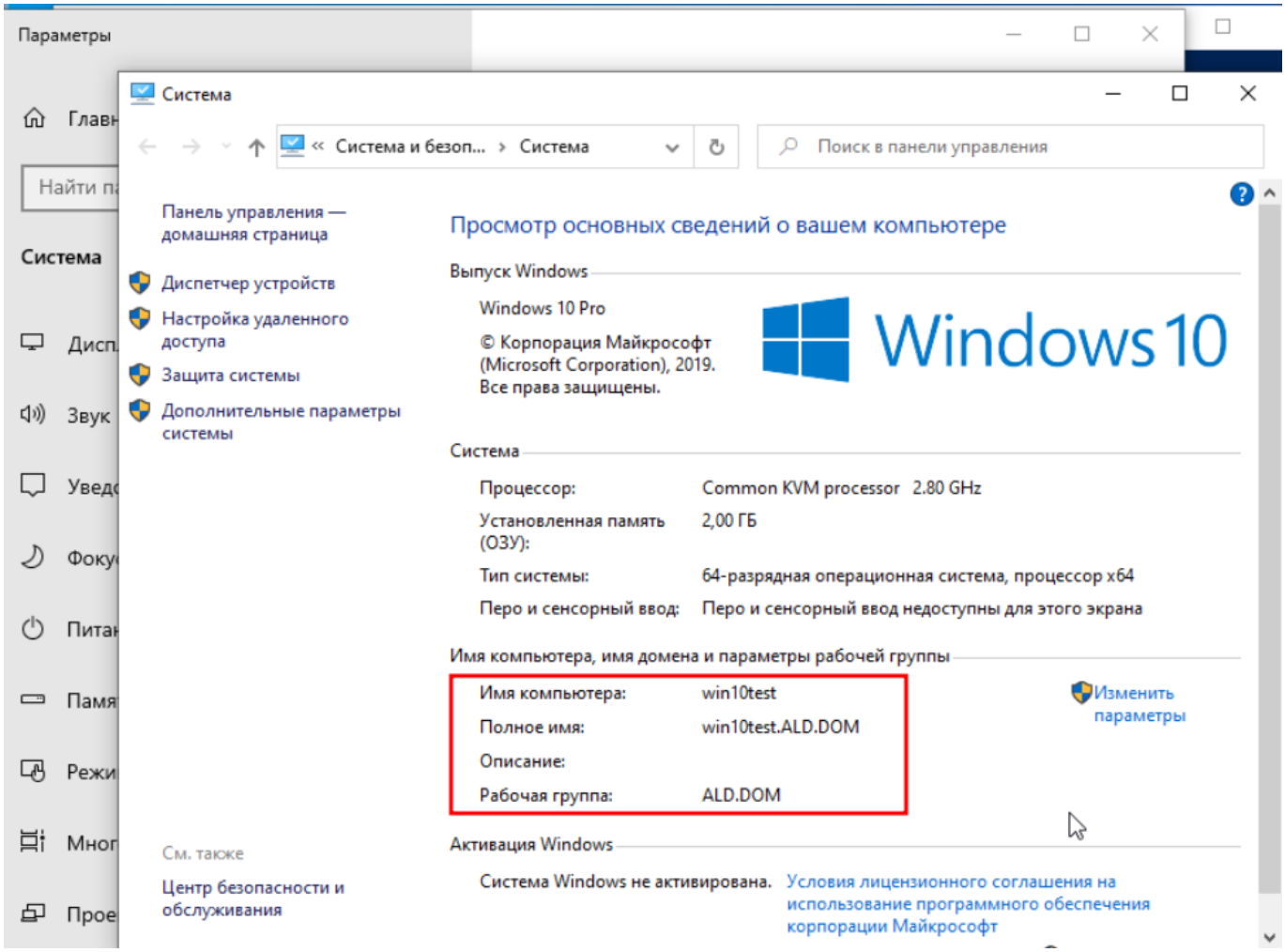


Рисунок 3.67 – Проверки 2

На Ald Pro сервере создать общую тестовую папку и попробовать зайти:

```
root@ald01:~# nano /etc/samba/smb.conf
[testshare]
path = /srv/testshare
browseable = yes
valid users = aldtest
admin users = aldtest
writable = yes
```

```
root@ald01:~# systemctl reload smbd.service
```

После успешного входа klist будет содержать дополнительный билет:

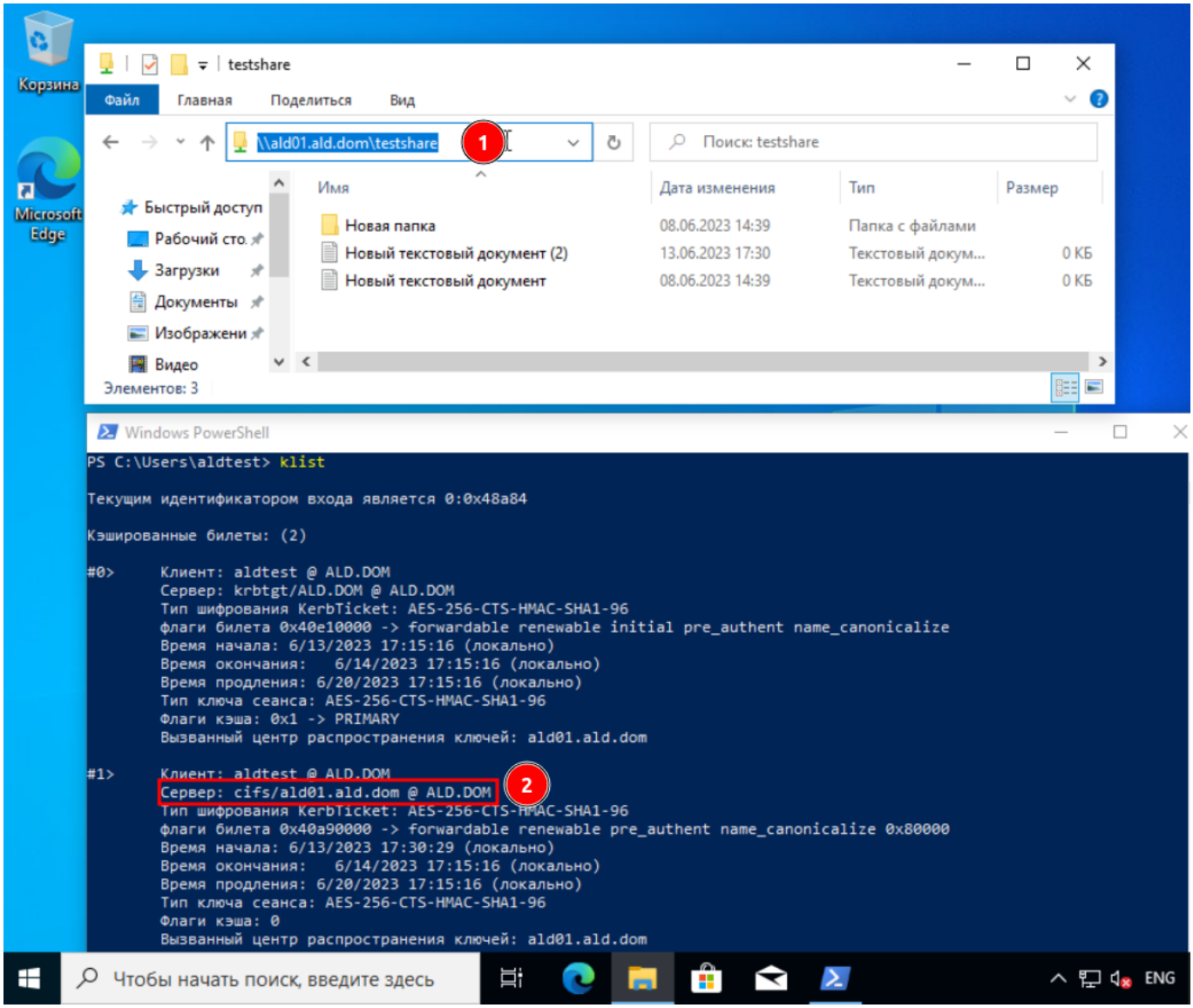


Рисунок 3.68 – Билет Kerberos

3.8.39.5. Добавление доменных(ALD Pro) пользователей или групп в локальные группы Windows

Скачать пакет WMF 5.1 для той операционной системы и архитектуры, в которой будет производиться установка.

Операционная система	Предварительные требования	Ссылка на пакеты
Windows Server 2012 R2		Win8.1AndW2K12R2-KB3191564-x64.msu
Windows Server 2012		W2K12-KB3191565-x64.msu
Windows Server 2008 R2	.NET Framework 4.5.2	Win7AndW2K8R2-KB3191566-x64.ZIP
Windows 8.1	x64:Win8.1AndW2K12R2-KB3191564-x64.msu, x86:Win8.1-KB3191564-x86.msu	
Windows 7 с пакетом обновления 1 (SP1)	.NET Framework 4.5.2	x64:Win7AndW2K8R2-KB3191566-x64.ZIP, x86:Win7-KB3191566-x86.ZIP

https://learn.microsoft.com/ru-ru/powershell/scripting/windows-powershell/wmf/setup/install-configure?view=powershell-7.3#download-and-install-the-wmf-51-package

Используя wbinfo

```
root@ald01:~# wbinfo -n "ald\admin"
S-1-5-21-109148531-2531787706-4107538291-500 SID_USER (1)
```

Используя ipa command

```
root@ald01:~# ipa user-show admin --all | grep ipantsecurityidentifier
  ipantsecurityidentifier: S-1-5-21-109148531-2531787706-4107538291-500
```

Используя ipa command

```
root@ald01:~# ipa group-show group_high --all | grep ipantsecurityidentifier
  ipantsecurityidentifier: S-1-5-21-109148531-2531787706-4107538291-1007
root@ald01:~#
root@ald01:~# ipa group-show group_high --all
  dn: cn=group_high,cn=groups,cn=accounts,dc=ald,dc=dom
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
  Имя группы: group_high
  ID группы: 995400007
  Группы-участники: group_low
  Пользователи с непрямым участием: alduser, aldtest
  ipantsecurityidentifier: S-1-5-21-109148531-2531787706-4107538291-1007
  ipauniqueid: d1410fd4-0a8c-11ee-9d12-422c2492509f
  objectclass: top, groupofnames, nestedgroup, ipausergroup, ipaobject, x-ald-
↪audit-policy, rbta-unit, posixgroup, ipantgroupattrs
```

```
Windows PowerShell (C) Корпорация Майкрософт (Microsoft Corporation). Все
↪права защищены.

Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/
↪pscore6)

PS C:\Windows\system32> Add-LocalGroupMember -Group 'Пользователи удаленного
↪рабочего стола' -Member 'S-1-5-21-109148531-2531787706-4107538291-500'
```

Наиболее популярные разрешения:

r = чтение

rx = Чтение, Выполнение, Список содержимого папки

rxm = Чтение, Выполнение, Список содержимого папки, Запись, Изменение

f = Полный доступ

(OI) = Для этой папки и её файлов

(CI) = Для этой папки и её подпапок

Таким образом, чтобы дать обычные права на чтение и запись на папку, используются разрешения (OI)(CI)rxm. То есть результирующая команда будет выглядеть так:

PowerShell или CMD

```
ICACLS "C:\Temp" /grant "*S-1-5-21-109148531-2531787706-4107538291-
↪500:(OI)(CI)rxm"
```

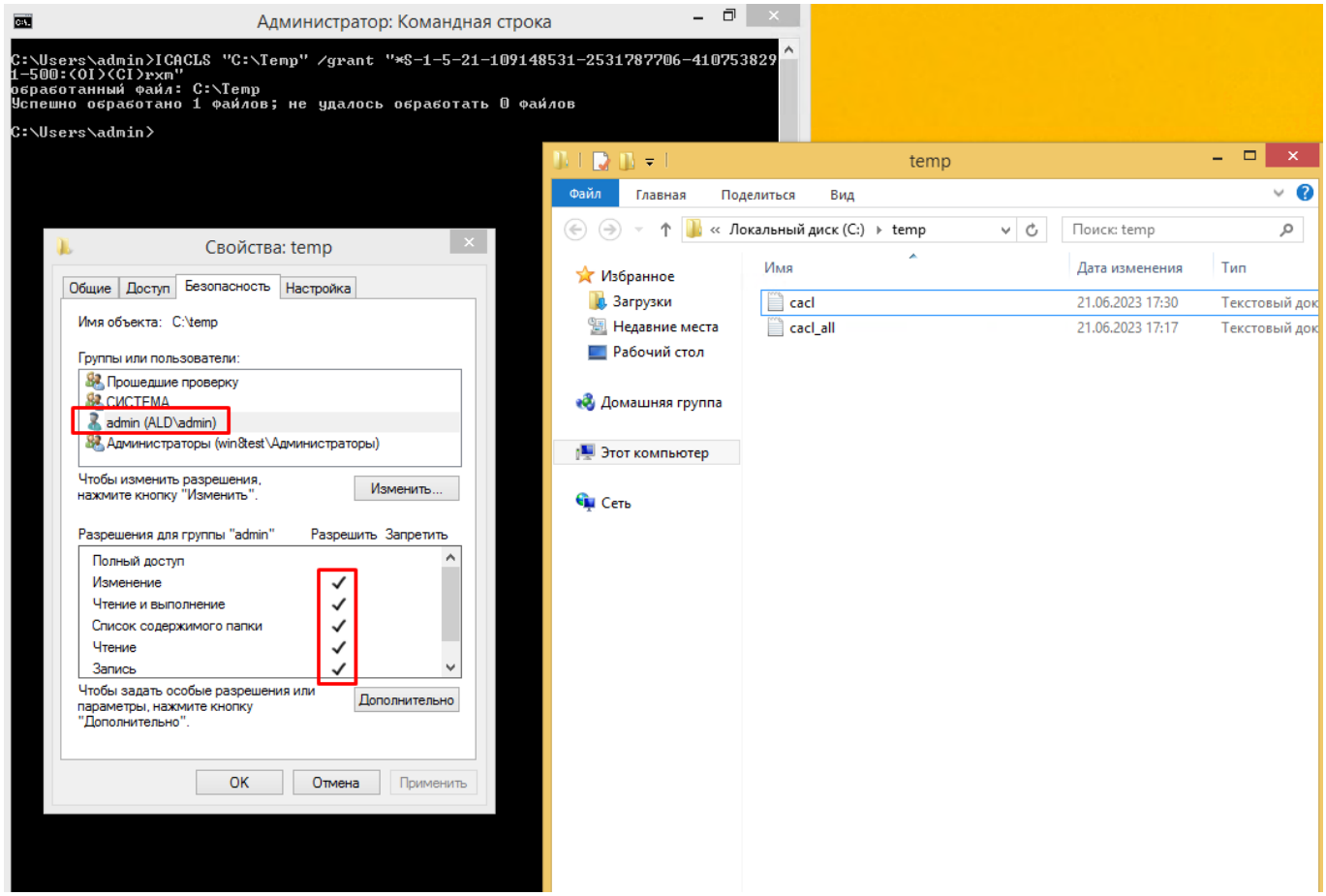


Рисунок 3.69 – Результат работы команд

Более детальная информация может быть найдена на сайте Microsoft:

https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/icacls

К сожалению в текущей реализации не поддерживается прямое добавление доменных групп в дискретные списки доступа (DACL).

Для того, чтобы обойти это ограничение:

1. Создать соответствующую доменной локальную группу.
2. В локальную группу добавить SID доменной группы (см. Добавление доменных(ALD Pro) пользователей или групп в локальные группы Windows).
3. Добавить в безопасность папки или файла локальную группу, которую создали в п. 1.

```
Alddom_fs_c_temp_r

Alddom_fs_c_temp_rw
```

3.9. Модуль Синхронизации

3.9.1. Инструкция по дополнительной настройке модуля синхронизации

Для предотвращения конфликтов при миграции и синхронизации данных из Microsoft Active Directory (MS AD) используется синхронная модель поведения. В качестве ведущего сервера обработки информации выбран главный сервер в кластере серверов ALD Pro.

Модуль синхронизации работает по следующим принципам:

- **Источник данных LDAP:** используется только MS AD DS (*Microsoft Active Directory Domain Services*). Все изменения объектов выполняются исключительно в MS AD;
- **Направление:** односторонняя синхронизация (MS AD → ALD Pro);
- **Контроль изменений:** - объекты, управляемые модулем синхронизации, не редактируются напрямую в ALD Pro; - все изменения (создание, модификация, удаление) производятся только в MS AD.

3.9.1.1. Исходные настройки

Предполагается, что на момент настройки модуля синхронизации у нас имеются:

- Настроенный контроллер домена MS AD;
- Настроенный контроллер домена ALD Pro;
- В обоих доменах MS AD и ALD Pro настроены корзины с одинаковыми интервалами ротации(очистки);
- Для сетей, в которых находятся контроллеры домена Microsoft AD и ALD Pro, настроено перенаправление DNS-зон;
- В домене MS AD поднят центр сертификации и выдан сертификат для доступа по LDAPs (см. cert_ms_ad);
- Для учетной записи MS AD, под которой идет подключение модуля синхронизации к контроллерам домена MS AD, необходимо через powershell выдать права на контейнер “Deleted Objects” и организационное подразделение (OU), задействованное для процесса синхронизации.

Примечание: В примере ниже при помощи команд powershell выдаются права на контейнер **Deleted Objects** и организационное подразделение (OU) **Подразделение А** для пользователя **aldagent** в домене **winad.lan**

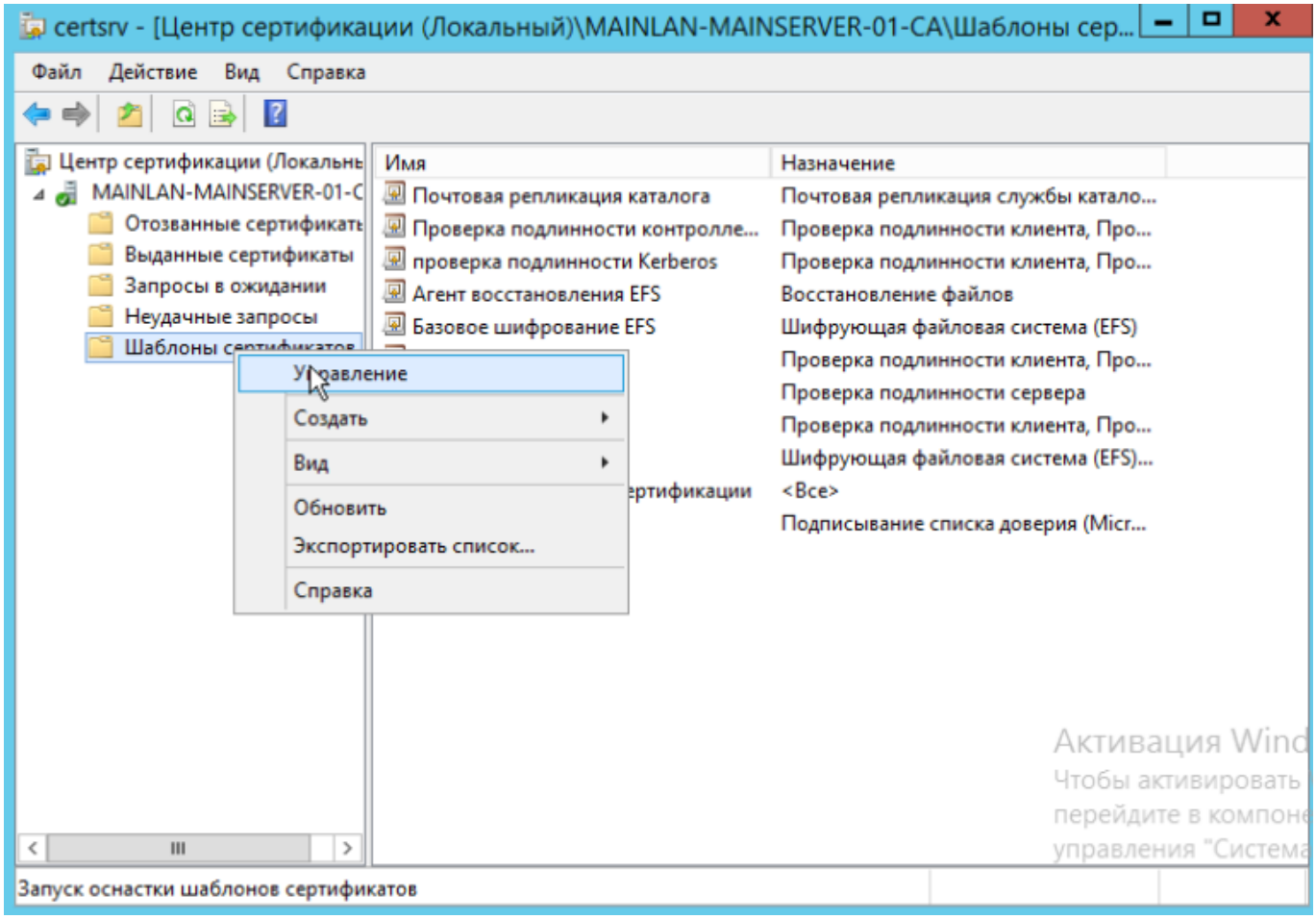
```
// для выдачи прав на контейнер запускаем ``powershell`` от имени
 ↪администратора
dsacls "CN=Deleted Objects,DC=winad,DC=lan" /takeownership
dsacls "CN=Deleted Objects,DC=winad,DC=lan" /g winad\aldagent:LCRP
dsacls "OU=Подразделение А,DC=winad,DC=lan" /g "winad\aldagent:CA;Reset
 ↪Password;user" /I:S
```

Выгрузка сертификатов для контроллера домена MS AD

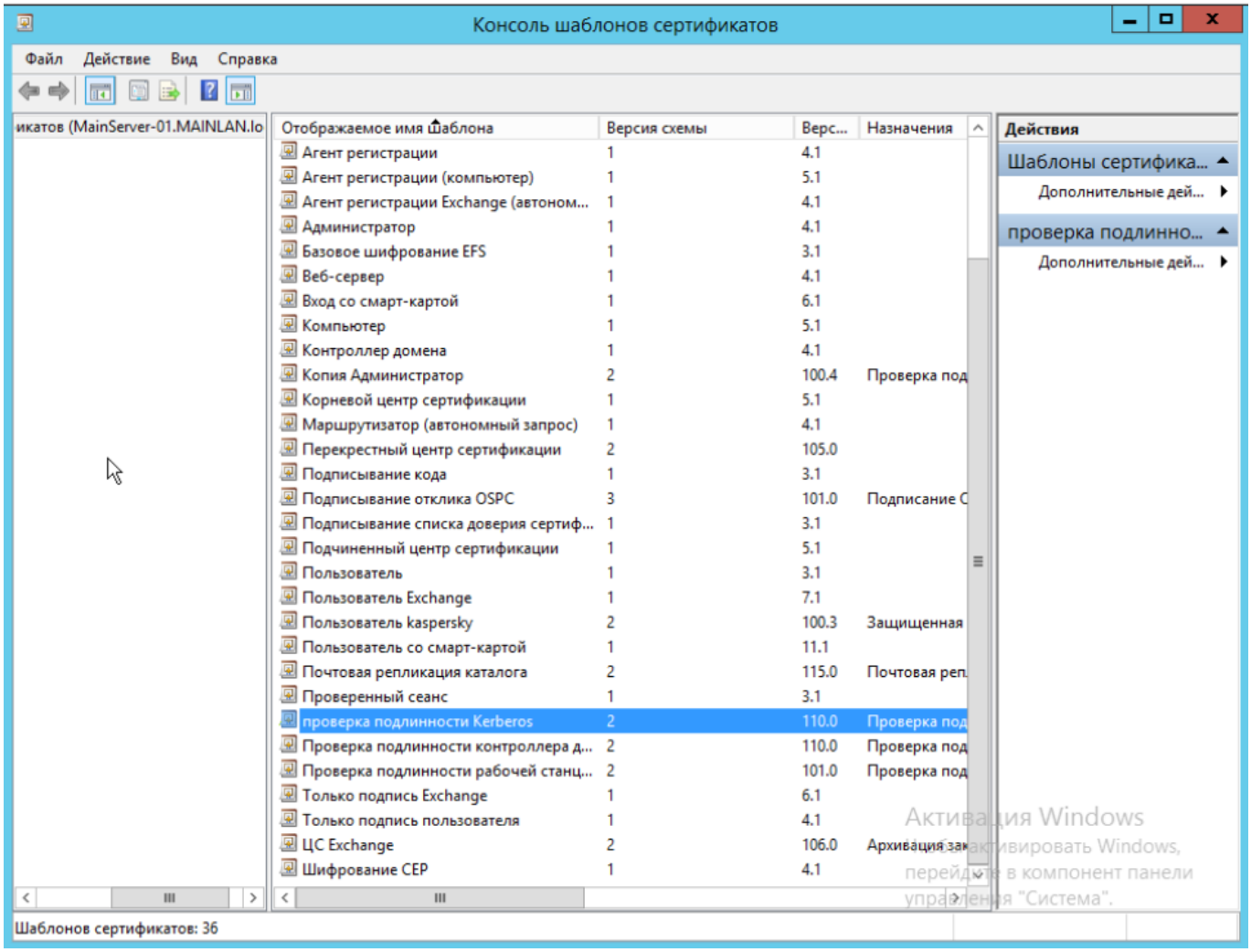
Для выгрузки сертификатов необходимо, чтобы в домене был настроен **Центр Сертификации**.

Примечание: Для корректного отображения окна конфигуратора используйте разрешение экрана не ниже 1280×1024, иначе элементы интерфейса могут выходить за пределы экрана.

Запустить **Центр Сертификации** → **Шаблоны Сертификатов** → **Управление** на сервере с ролью **Центр Сертификации**:

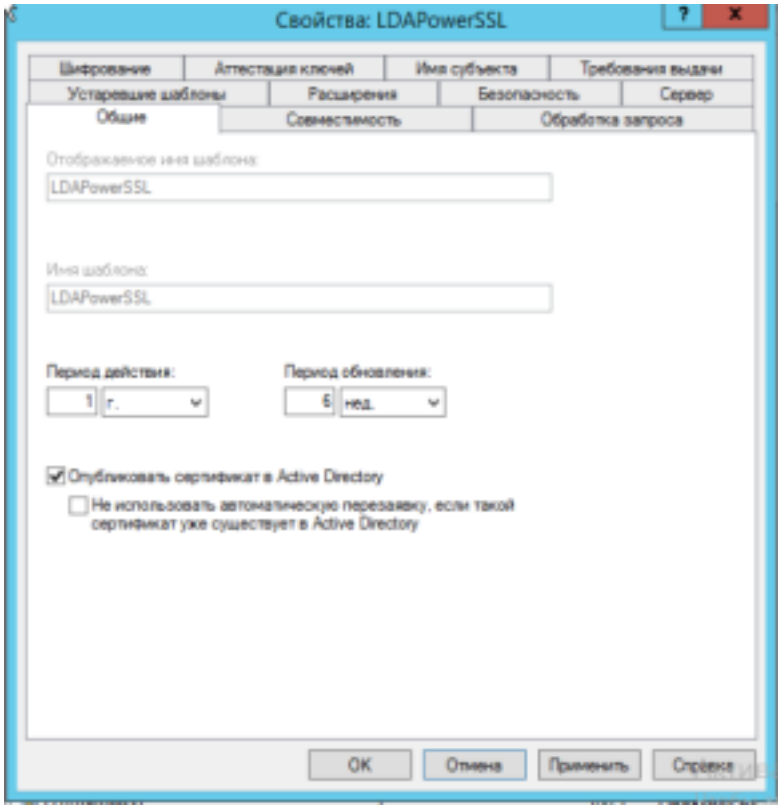


Создать копию шаблона **Проверка подлинности Kerberos**, выбрав пункт **Скопировать шаблон** контекстного меню:



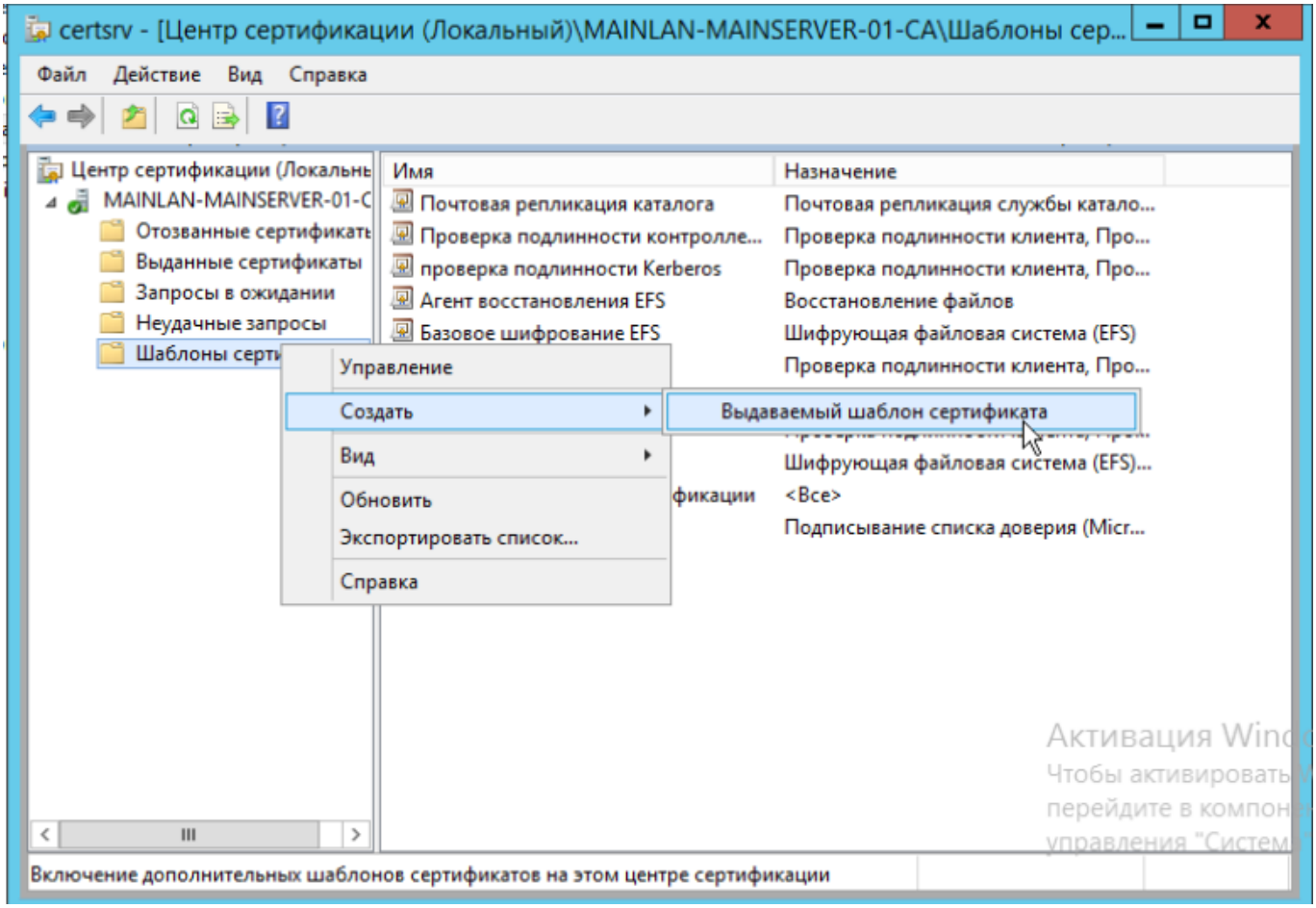
Настроить шаблон сертификата на вкладке **Общие**:

- имя сертификата **LDAPowerSSL**;
- период действия сертификата.

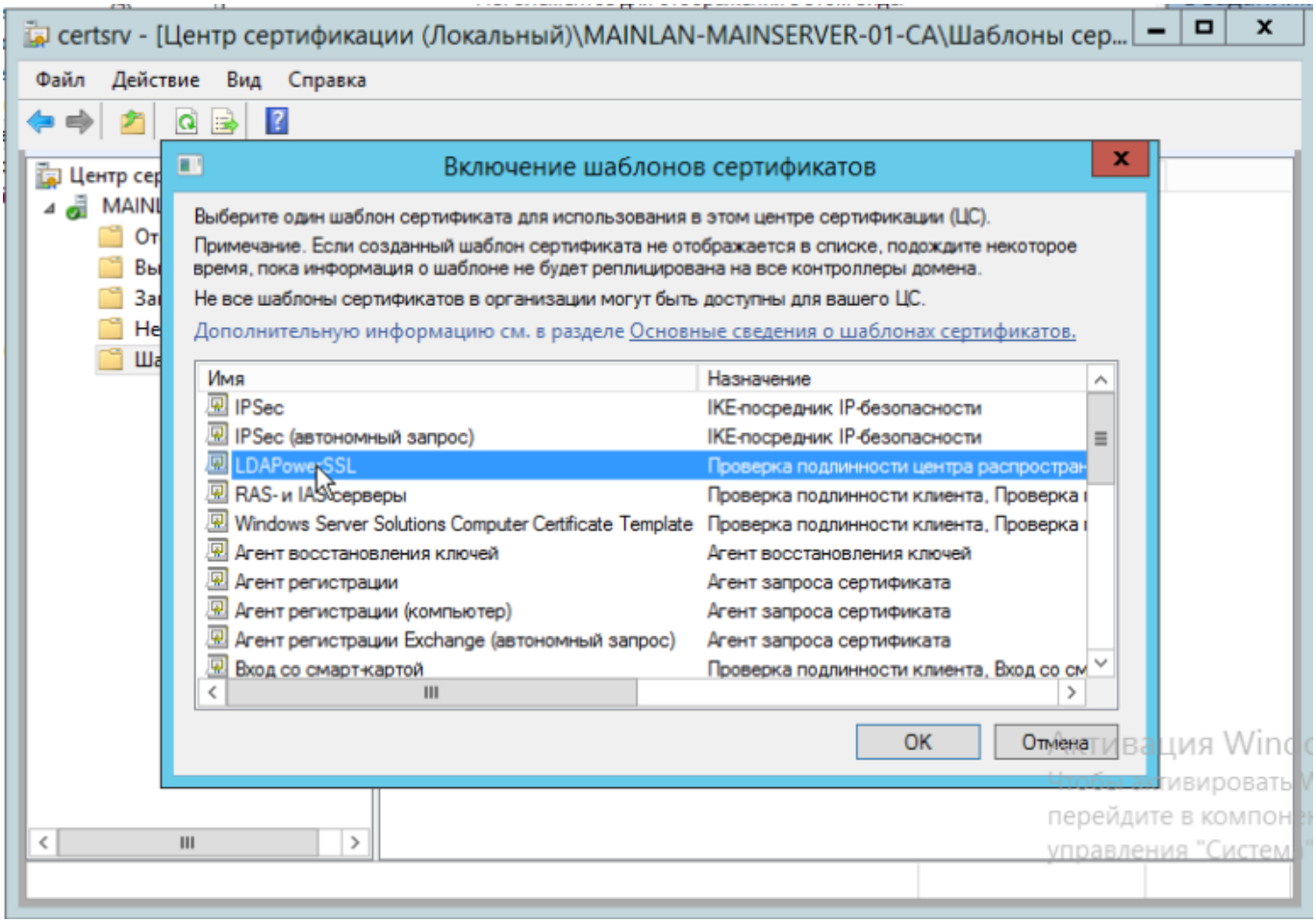


Отметить галочкой пункт меню **Опубликовать сертификат в MS AD**.

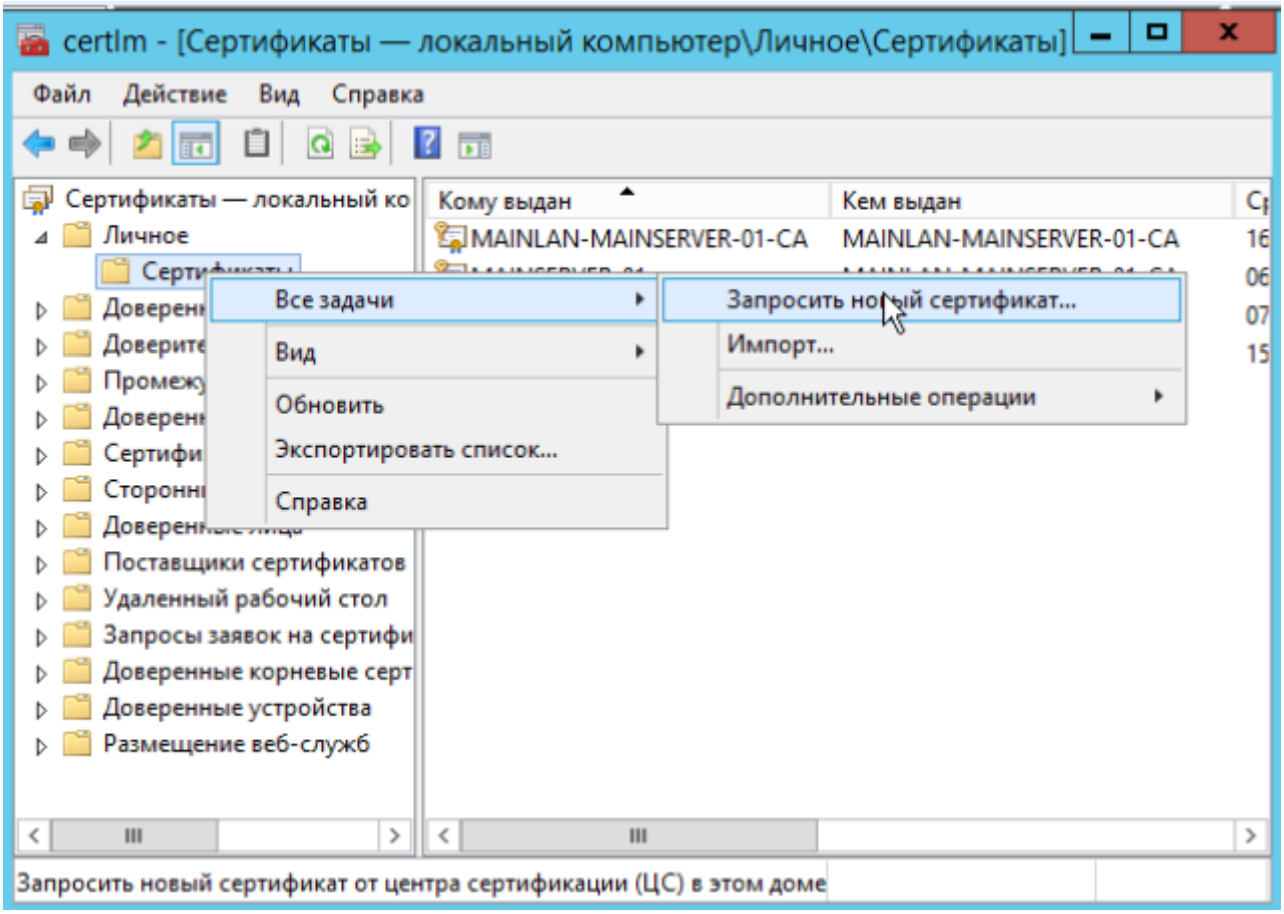
Опубликовать новый тип сертификата. Для этого в в контекстном меню раздела **Шаблоны сертификатов** выбрать **Создать → Выдаваемый шаблон сертификата**.



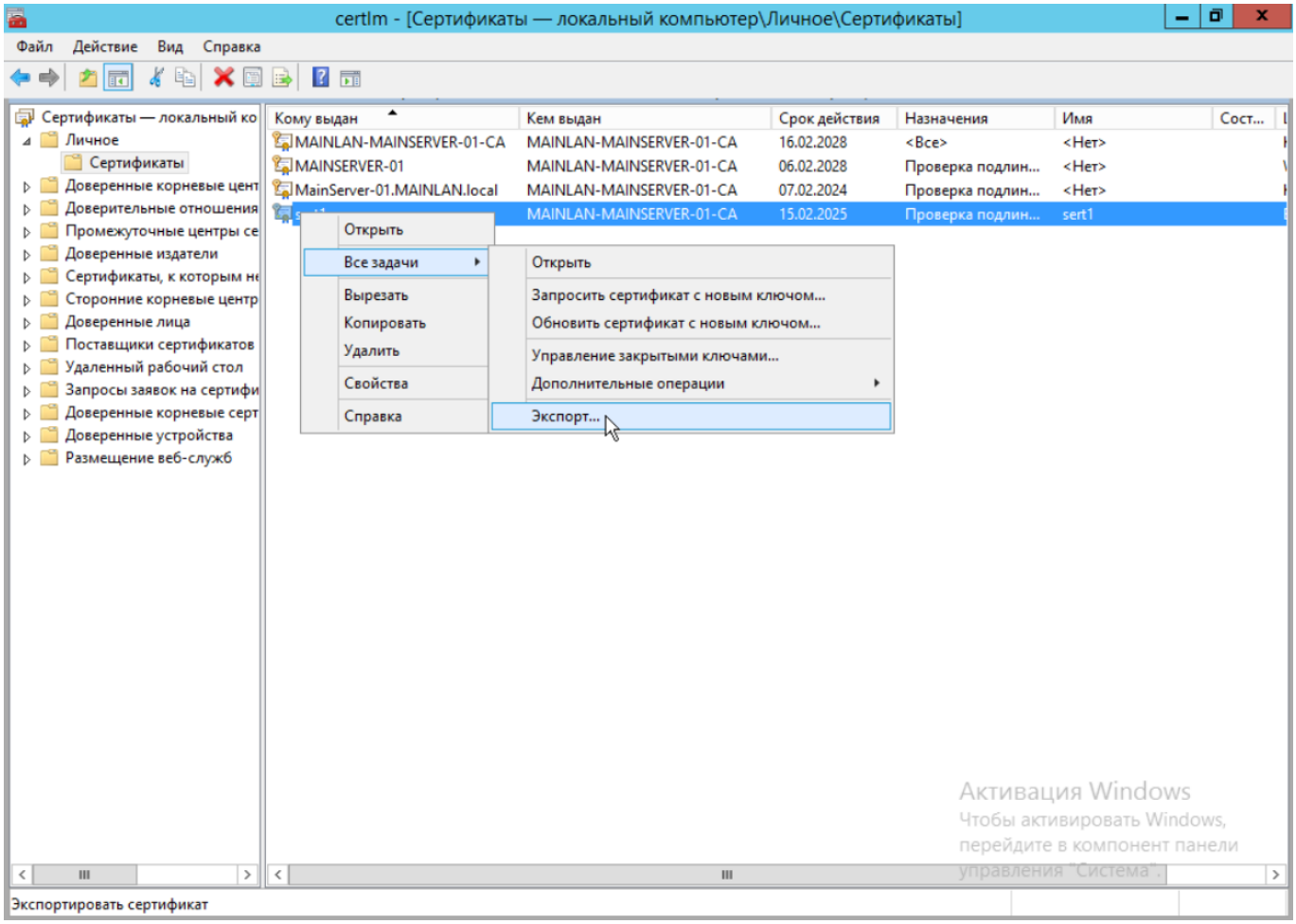
В списке доступных шаблонов выбрать созданный ранее:



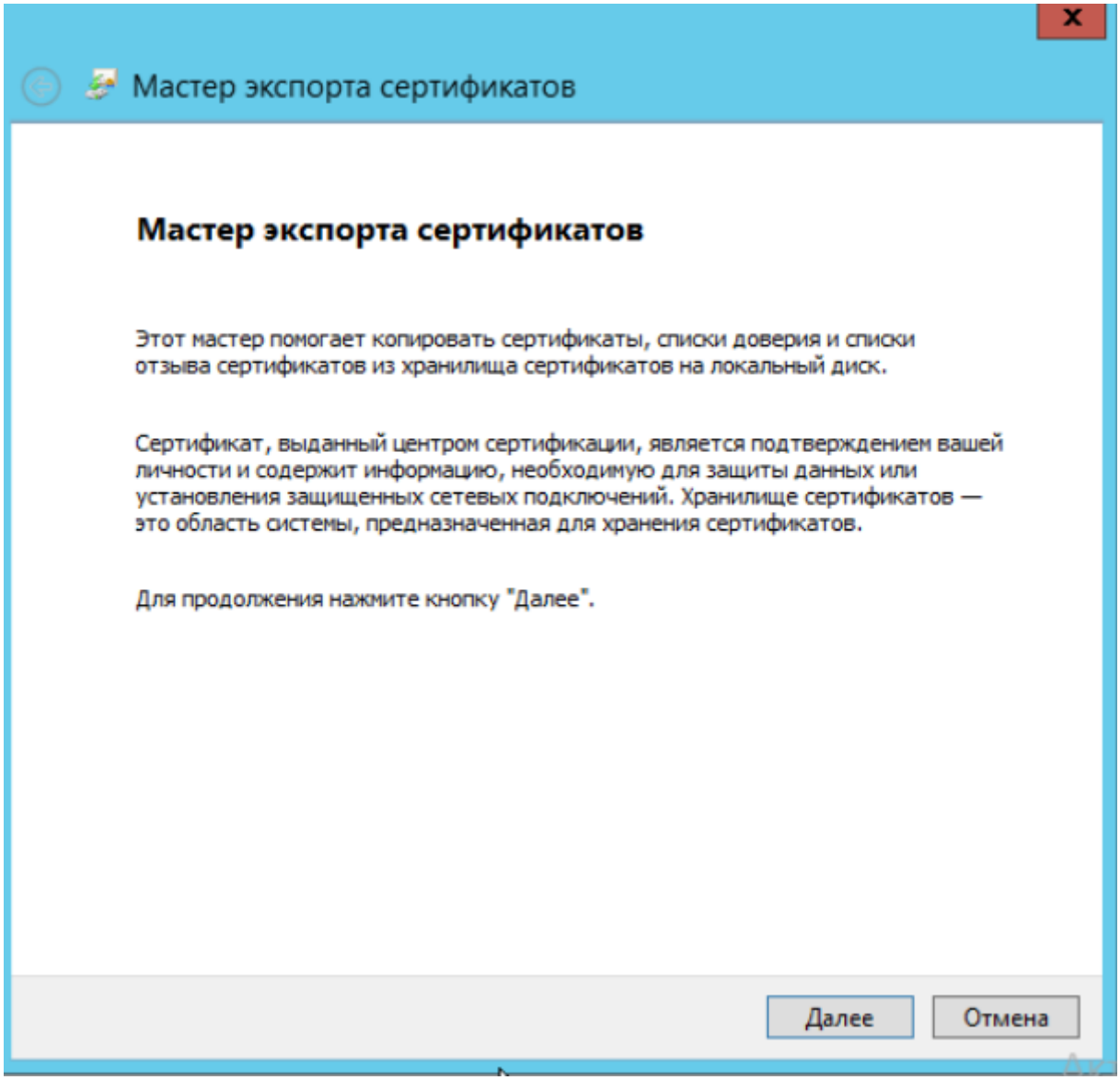
На контроллере домена, который будет задействован в процессе синхронизации данных со стороны MS AD, открыть оснастку **Управление сертификатами** компьютера. В дереве сертификатов перейти в папку **Личное** и в контекстном меню выбрать **Все задачи** → **Запросить новый сертификат**:

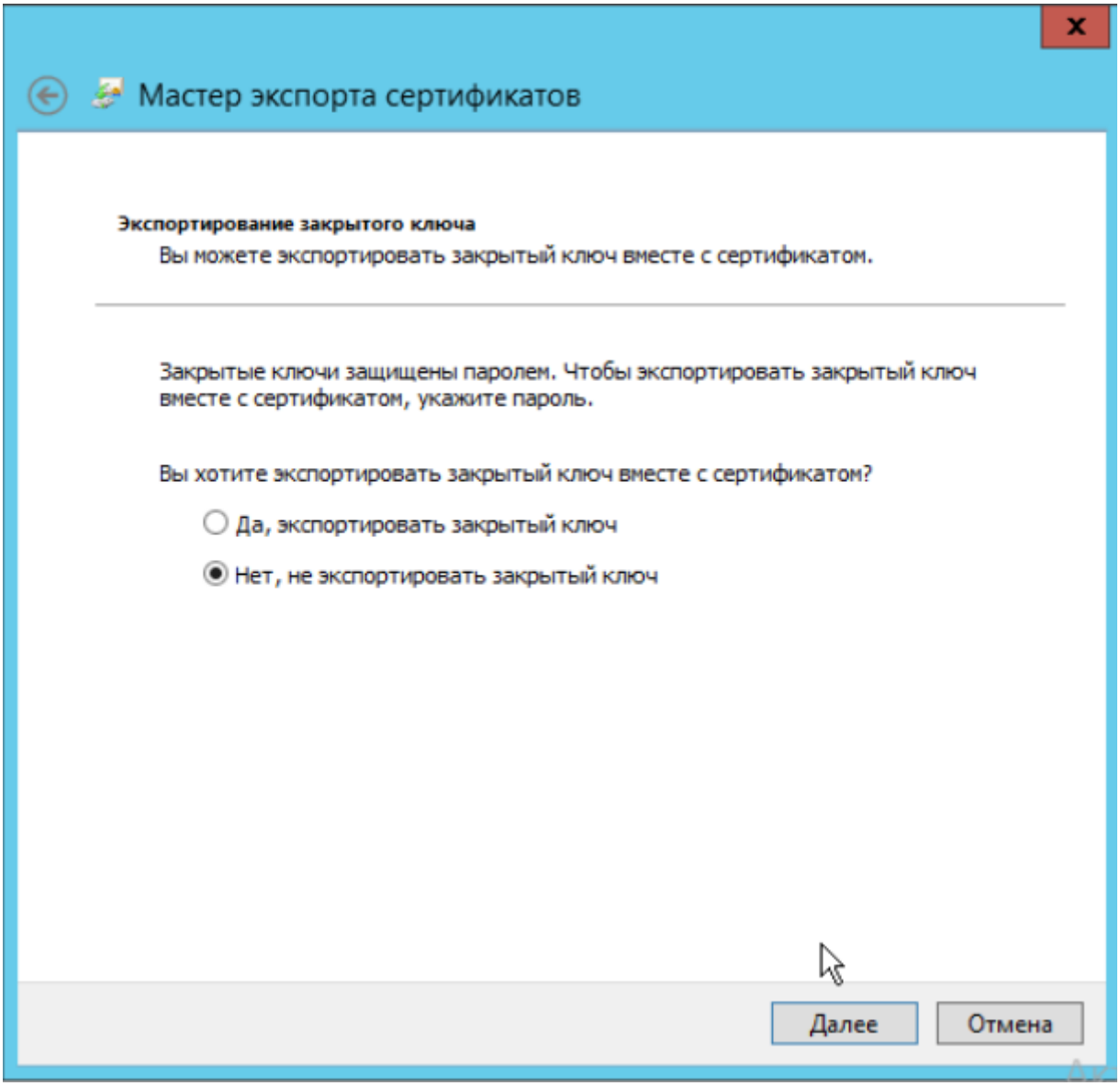


В списке доступных сертификатов выбрать созданный ранее, выпустить сертификат (кнопка **Выпустить сертификат**) и экспортировать (контекстное меню **Все задачи** → **Экспорт**).

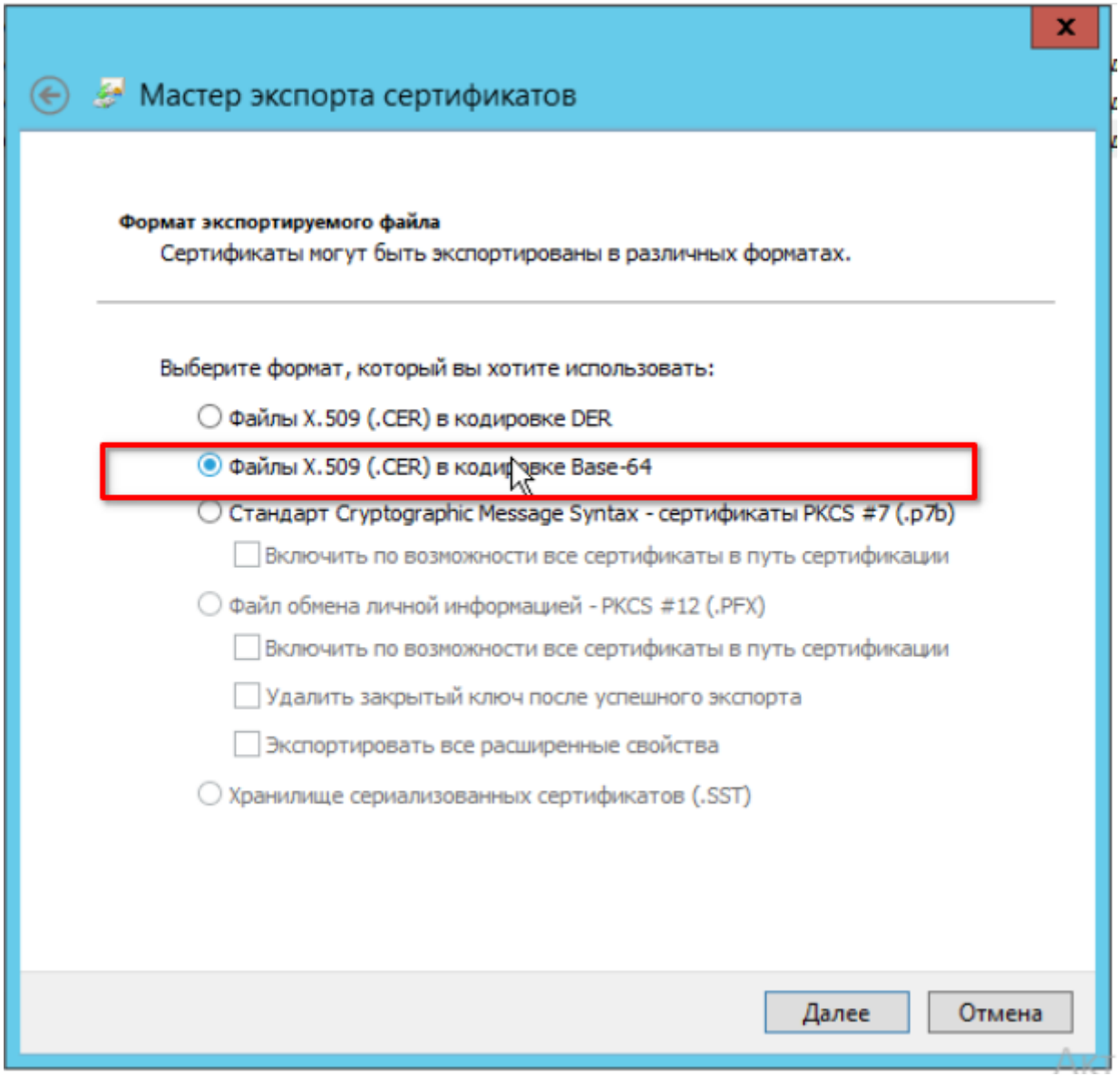


Откроется мастер экспорта сертификатов:

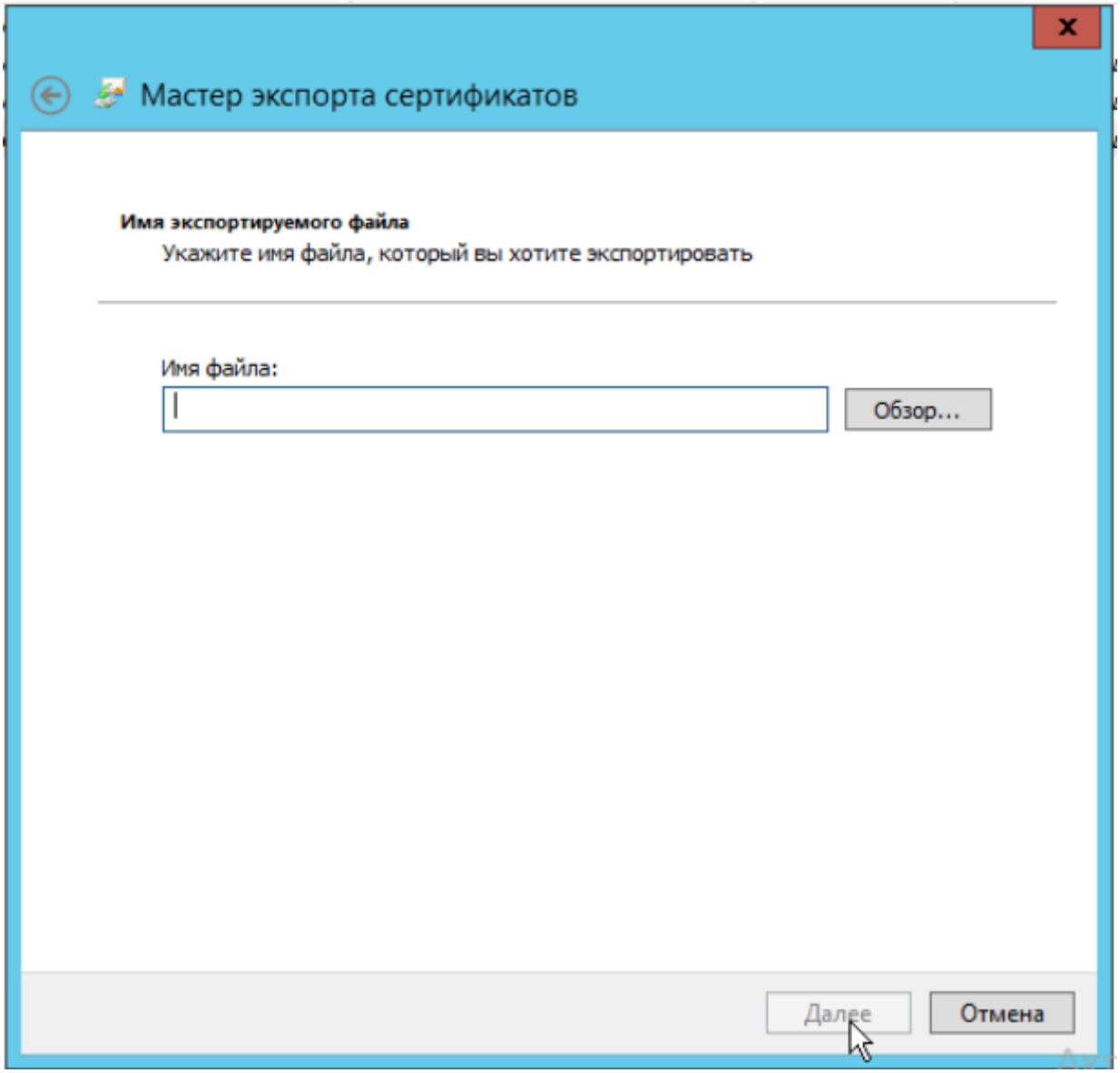

Мастер экспорта сертификатов
Мастер экспорта сертификатов
Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов из хранилища сертификатов на локальный диск.
Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов.
Для продолжения нажмите кнопку "Далее".
Далее
Отмена



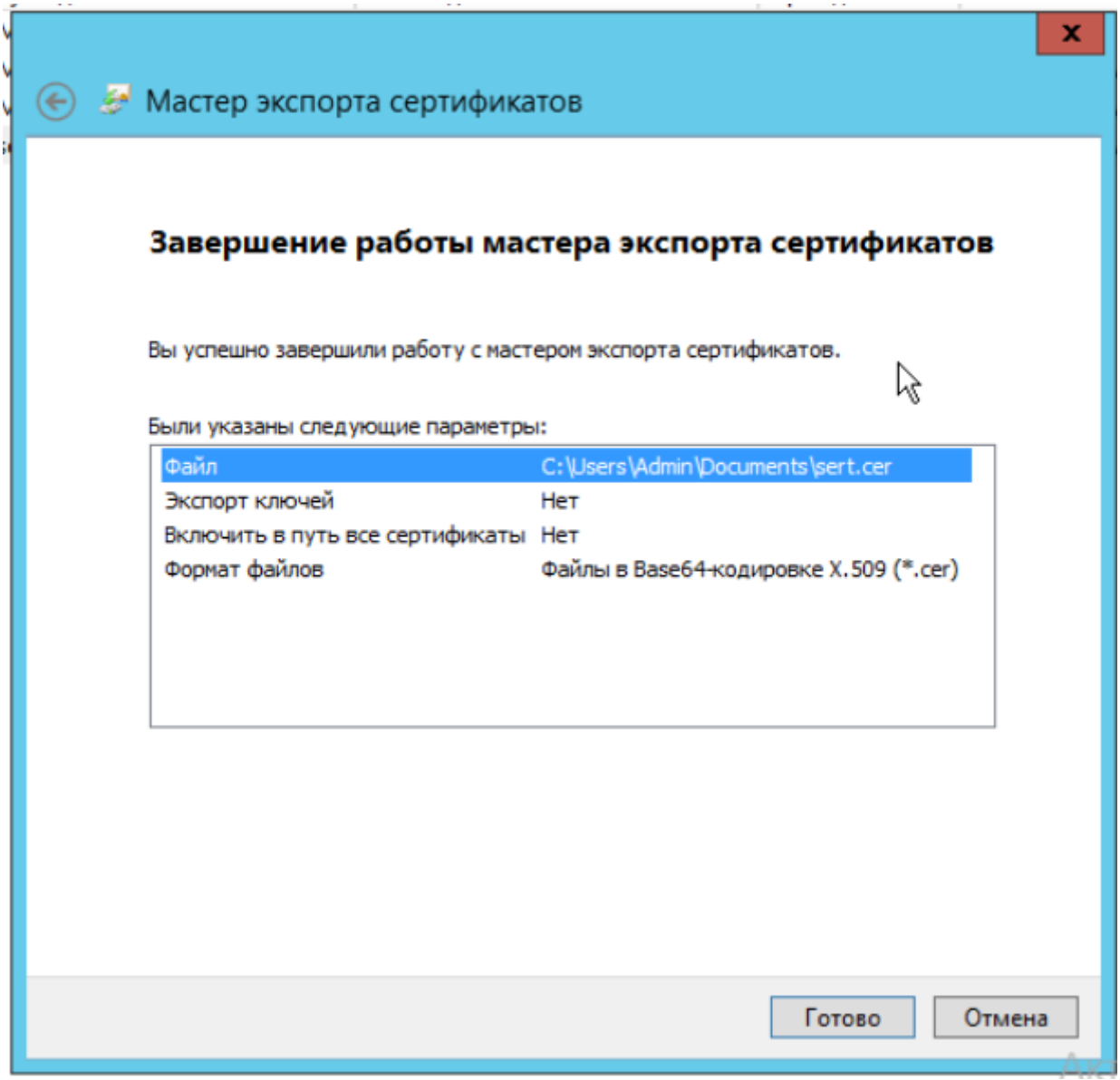
Выбрать кодировку base64 для файла сертификата:



Задать имя файла:



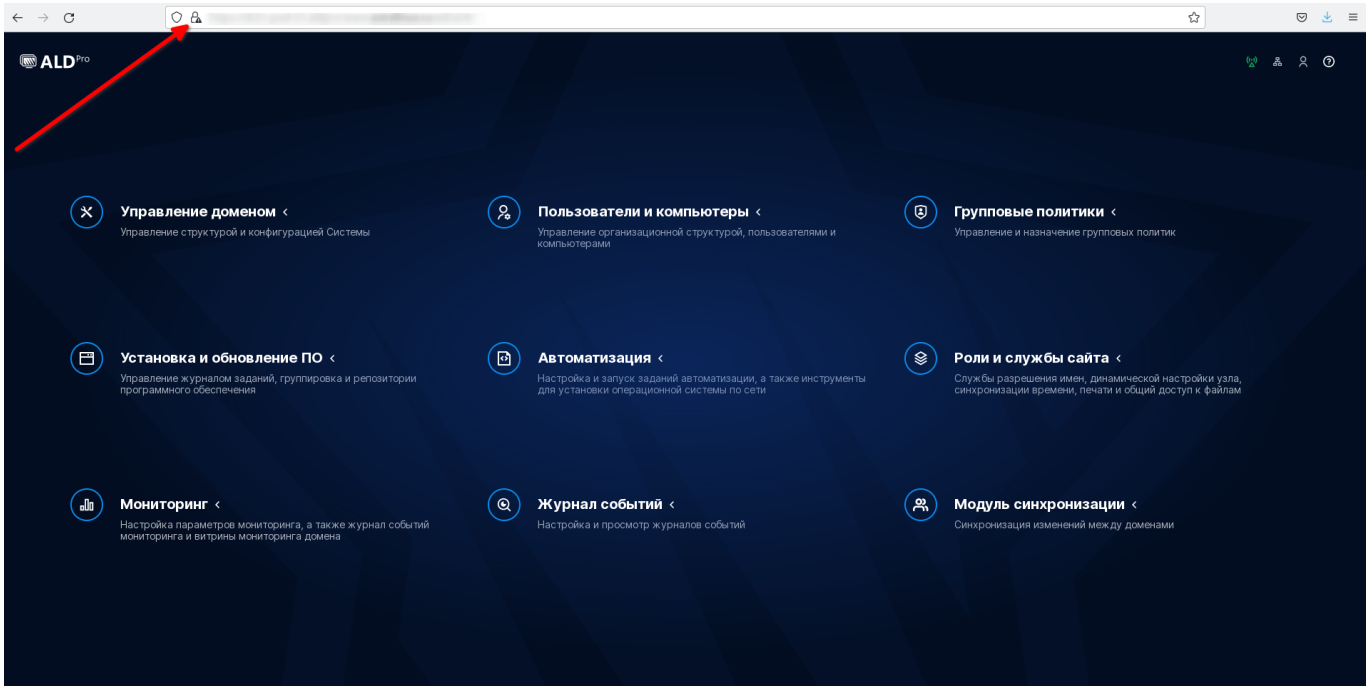
После нажатия кнопки **Готово** будет выгружен файл сертификата <имя_сертификата.cer>.



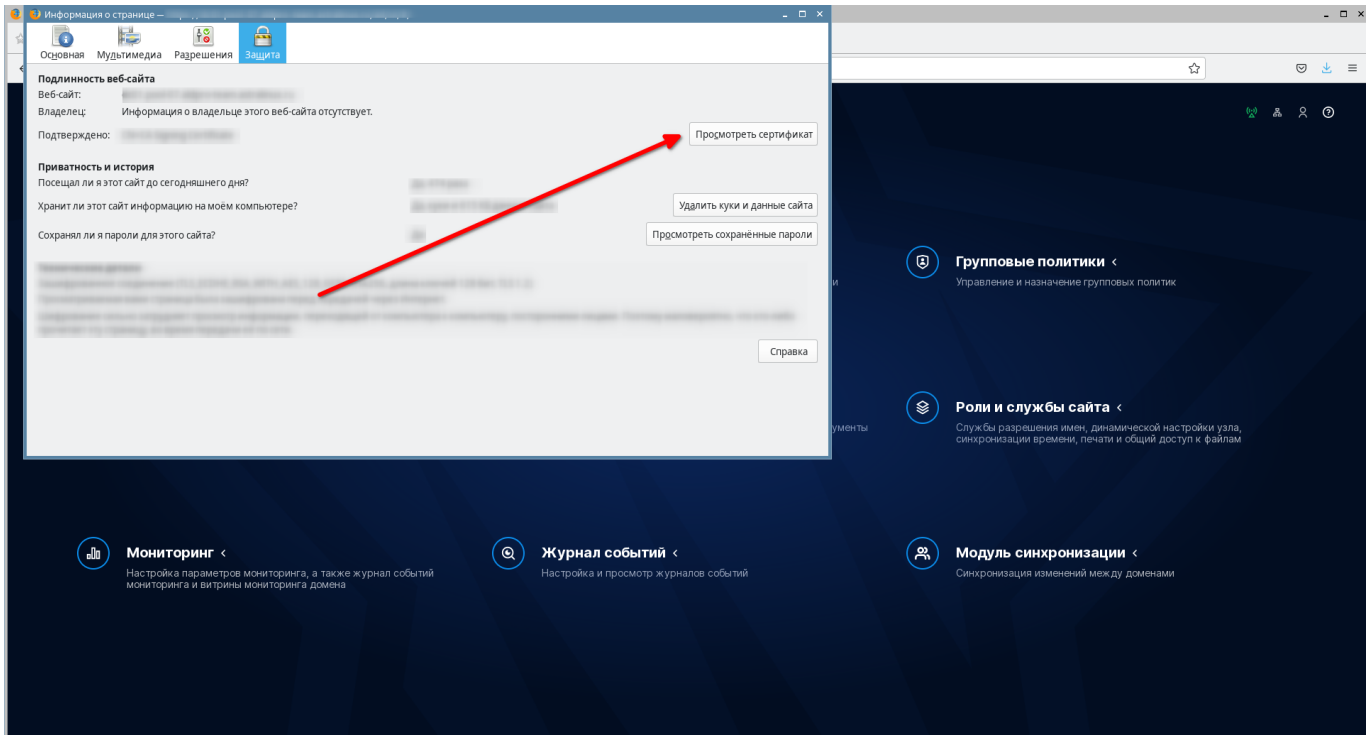
Необходимо изменить формат файла сертификата на *.pem, переименовав файл в <имя_сертификата.pem>. (например sert.pem - как публичный ключ для подключения по LDAPS к контроллеру MS AD)

Выгрузка сертификатов для контроллера домена ALD Pro

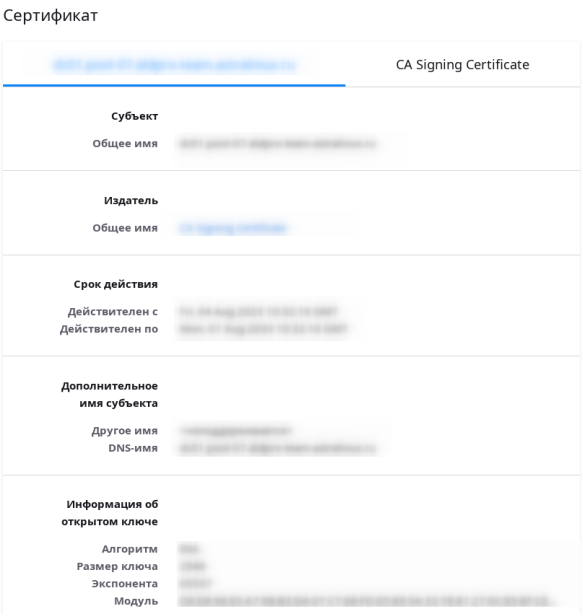
Для выгрузки сертификата необходимо зайти на портал управления ALD Pro, нажать на кнопку просмотра информации о сайте и выбрать **Незащищенное соединение** → **Подробнее**:



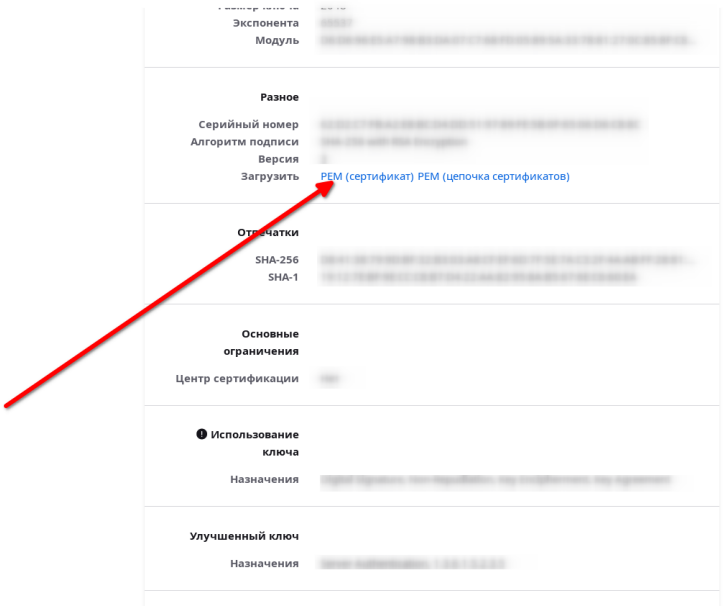
Выбрать **Просмотреть сертификат**:



Откроется файл сертификата:



Открыть ссылку **PEM (сертификат)**:



Сертификат сайта сохранен.

3.9.1.2. Настройка синхронизации паролей MS AD → ALD

Установка passwdhk на контроллер домена (если ранее не устанавливался)

Для настройки потребуется файл PasswdhkSetup.msi, который можно скачать в личном кабинете пользователя Astra Linux https://lk-new.astralinux.ru.

Синхронизация пароля пользователя будет успешна только для тех учетных записей **MS AD**, для которых пароль задавался после создания групповой политики `passwdhk`. Пароли, изменяемые до установки passwdhk, не смогут быть синхронизированы в целевой LDAP (ALD Pro). Для синхронизации паролей у существующих пользователей необходимо сменить/обновить пароль в LDAP-источнике (MS AD DS).

Перед началом установки необходимо установить компонент `Visual C++ Redistributable 2022`.

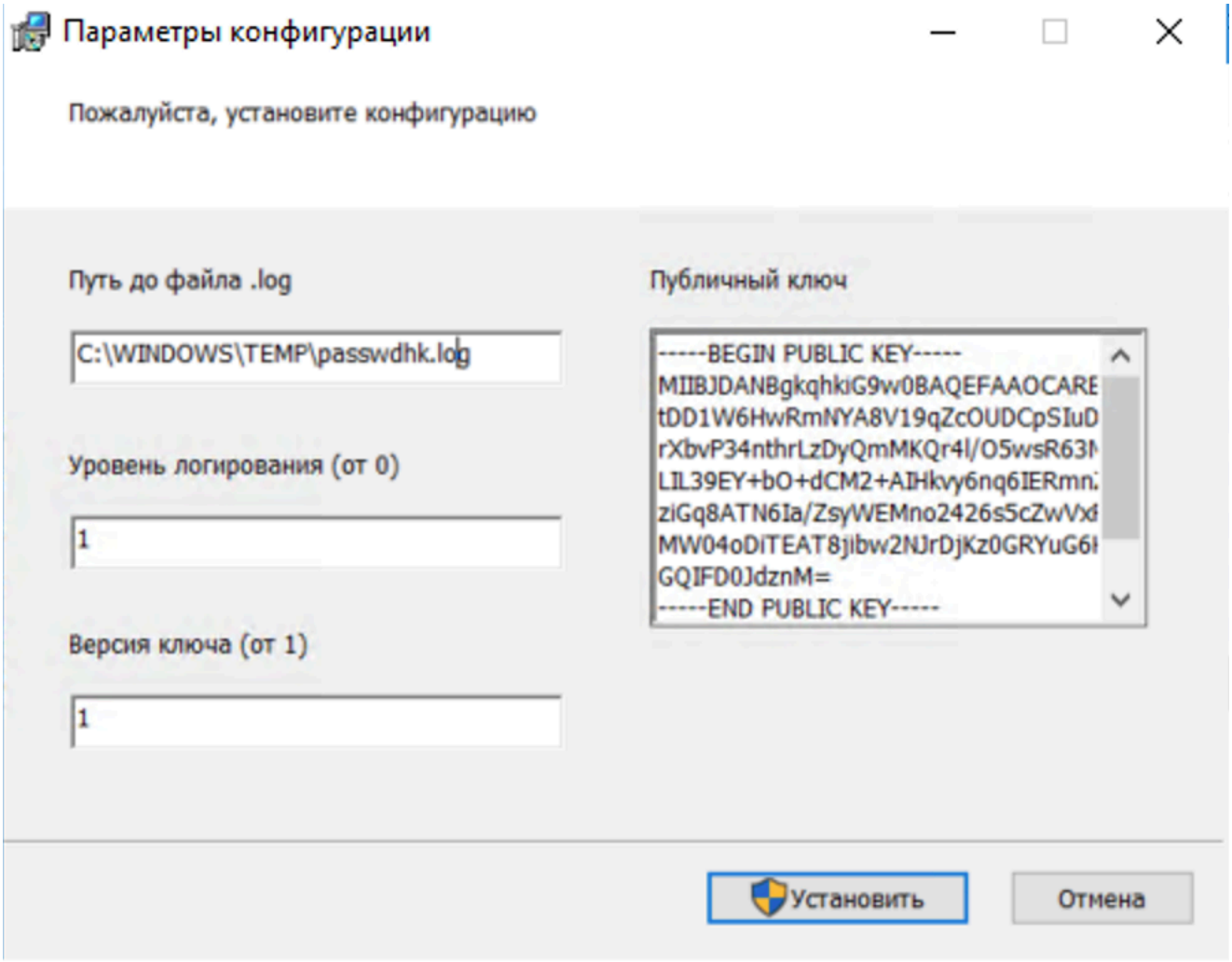
1. Выполнить запуск установочного файла passwdhk_install/util/VC_redist.x64.exe

Установку необходимо выполнить на каждом контроллере домена, где планируется установка утилиты `passwdhk`.

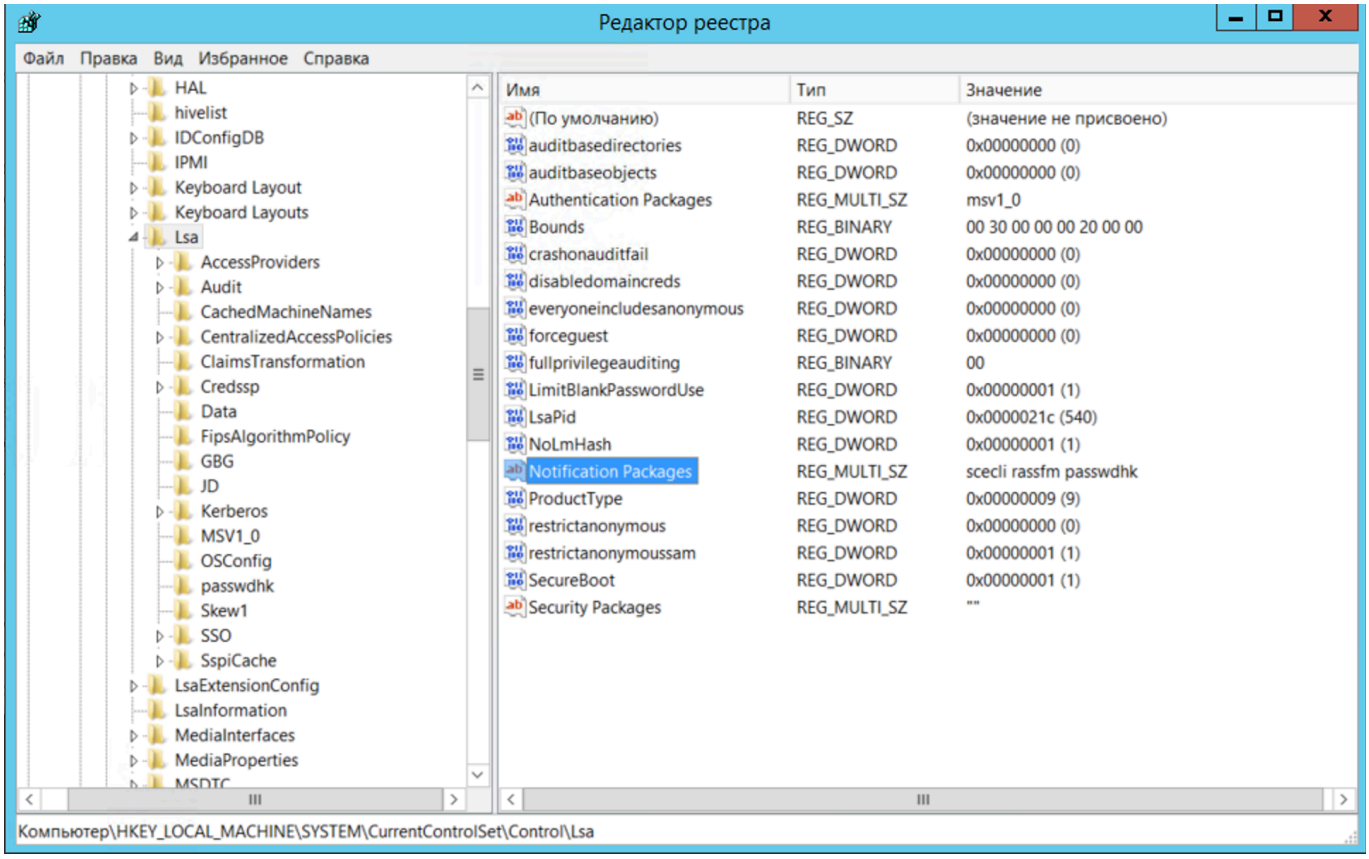
2. Запустить файл `PasswdhkSetup.msi` от имени администратора.
3. На экране параметров установки указать следующие значения:

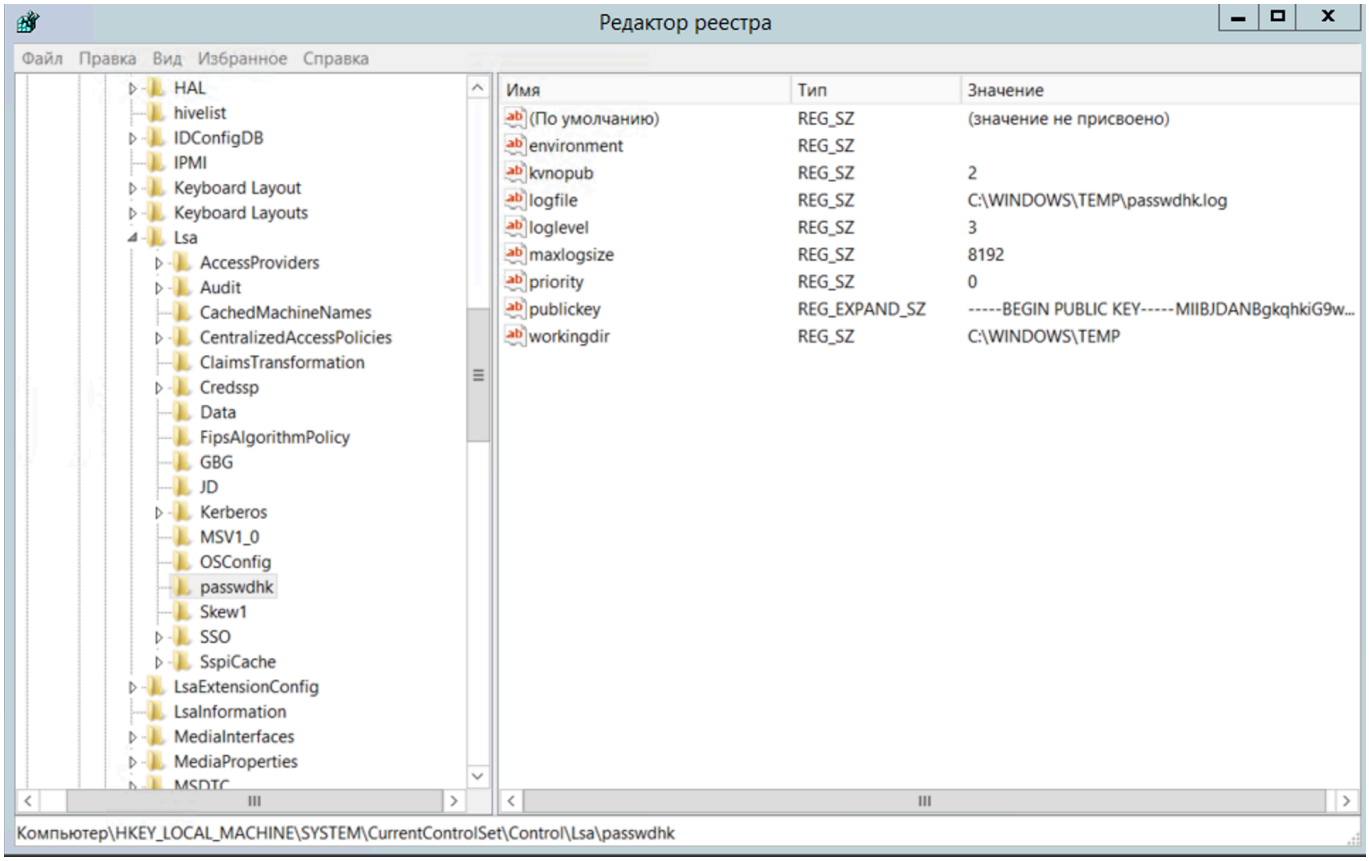
- **Уровень логирования** - указать один из четырех уровней логирования;
- **Номер ключа регистрации** - ввести значение, полученное на портале управления **ALD Pro**;
- **Публичный ключ регистрации** - вставить файл открытого ключа, скачанный при развертывании модуля синхронизации в ALD Pro **Модуль синхронизации -> Настройки -> Синхронизация паролей -> Кнопка “Получить ключ”** (подробнее в разделе **Синхронизация паролей ALD Pro → MS AD**).

Примечание: Если ключ подгрузился автоматически, это означает, что на контроллере домена имеются артефакты. В этом случае необходимо выполнить шаги из раздела Настройка **синхронизации паролей MS AD → ALD** для удаления артефактов старой версии. Это позволит избежать некорректной работы утилиты и ошибок установки или нарушения работы компонентов.



1. После заполнения всех параметров нажать на кнопку **Установить**, затем — **Готово**.
2. Дождаться завершения перезагрузки контроллера домена.
3. Проверить, что в реестре создались необходимые записи.


Редактор реестра
Файл Правка Вид Избранное Справка
HAL
hivelist
IDConfigDB
IPMI
Keyboard Layout
Keyboard Layouts
Lsa
AccessProviders
Audit
CachedMachineNames
CentralizedAccessPolicies
ClaimsTransformation
Credssp
Data
FipsAlgorithmPolicy
GBG
JD
Kerberos
MSV1_0
OSConfig
passwdhk
Skew1
SSO
SspiCache
LsaExtensionConfig
LsaInformation
MediaInterfaces
MediaProperties
Имя Тип Значение
(По умолчанию) REG_SZ (значение не присвоено)
auditbasedirectories REG_DWORD 0x00000000 (0)
auditbaseobjects REG_DWORD 0x00000000 (0)
Authentication Packages REG_MULTI_SZ msv1_0
Bounds REG_BINARY 00 30 00 00 00 20 00 00
crashonauditfail REG_DWORD 0x00000000 (0)
disabledomaincreds REG_DWORD 0x00000000 (0)
everyoneincludesanonymous REG_DWORD 0x00000000 (0)
forceguest REG_DWORD 0x00000000 (0)
fullprivilegeauditing REG_BINARY 00
LimitBlankPasswordUse REG_DWORD 0x00000001 (1)
LsaPid REG_DWORD 0x0000021c (540)
NoLmHash REG_DWORD 0x00000001 (1)
Notification Packages REG_MULTI_SZ scecli rassfm passwdhk
ProductType REG_DWORD 0x00000009 (9)
restrictanonymous REG_DWORD 0x00000000 (0)
restrictanonymoussam REG_DWORD 0x00000001 (1)
SecureBoot REG_DWORD 0x00000001 (1)
Security Packages REG_MULTI_SZ ""
Компьютер\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

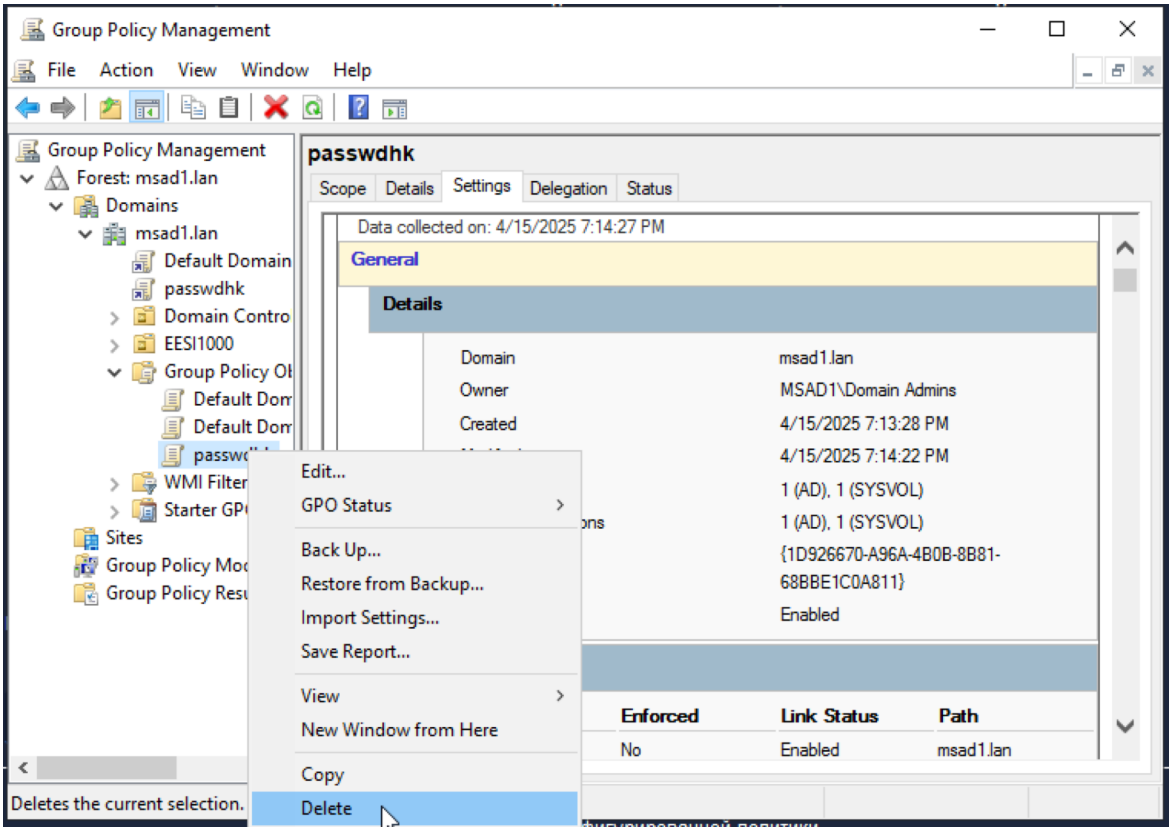

Редактор реестра
Файл Правка Вид Избранное Справка
HAL
hivelist
IDConfigDB
IPMI
Keyboard Layout
Keyboard Layouts
Lsa
AccessProviders
Audit
CachedMachineNames
CentralizedAccessPolicies
ClaimsTransformation
Credssp
Data
FipsAlgorithmPolicy
GBG
JD
Kerberos
MSV1_0
OSConfig
passwdhk
Skew1
SSO
SspiCache
LsaExtensionConfig
LsaInformation
MediaInterfaces
MediaProperties
Имя Тип Значение
(По умолчанию) REG_SZ (значение не присвоено)
environment REG_SZ
kvnopub REG_SZ 2
logfile REG_SZ C:\WINDOWS\TEMP\passwdhk.log
loglevel REG_SZ 3
maxlogsize REG_SZ 8192
priority REG_SZ 0
publickey REG_EXPAND_SZ -----BEGIN PUBLIC KEY-----MIIBJDANBgkqhkiG9w...
workingdir REG_SZ C:\WINDOWS\TEMP
Компьютер\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\passwdhk

3.9.1.3. Обновление passwdhk, установленного через групповую политику (GPO), на версию MSI

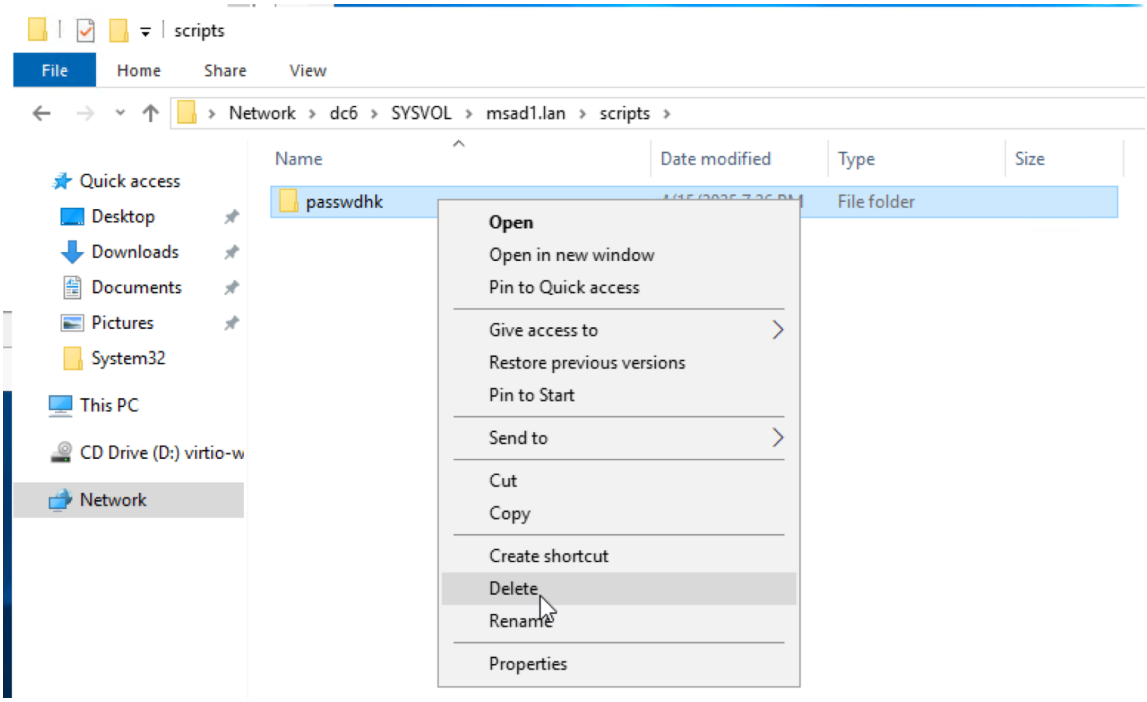
Важно: Утилита может сработать некорректно, если в системе присутствуют артефакты предыдущих установок. В редких случаях это может привести к ошибкам установки или нарушению работы компонентов.

Если на контроллере домена ранее был установлен `passwdhk` через групповую политику (GPO), необходимо выполнить удаление старой версии перед установкой новой версии через MSI:

1. Удалить объект групповой политики `passwdhk` в редакторе групповых политик (gpmc.msc).

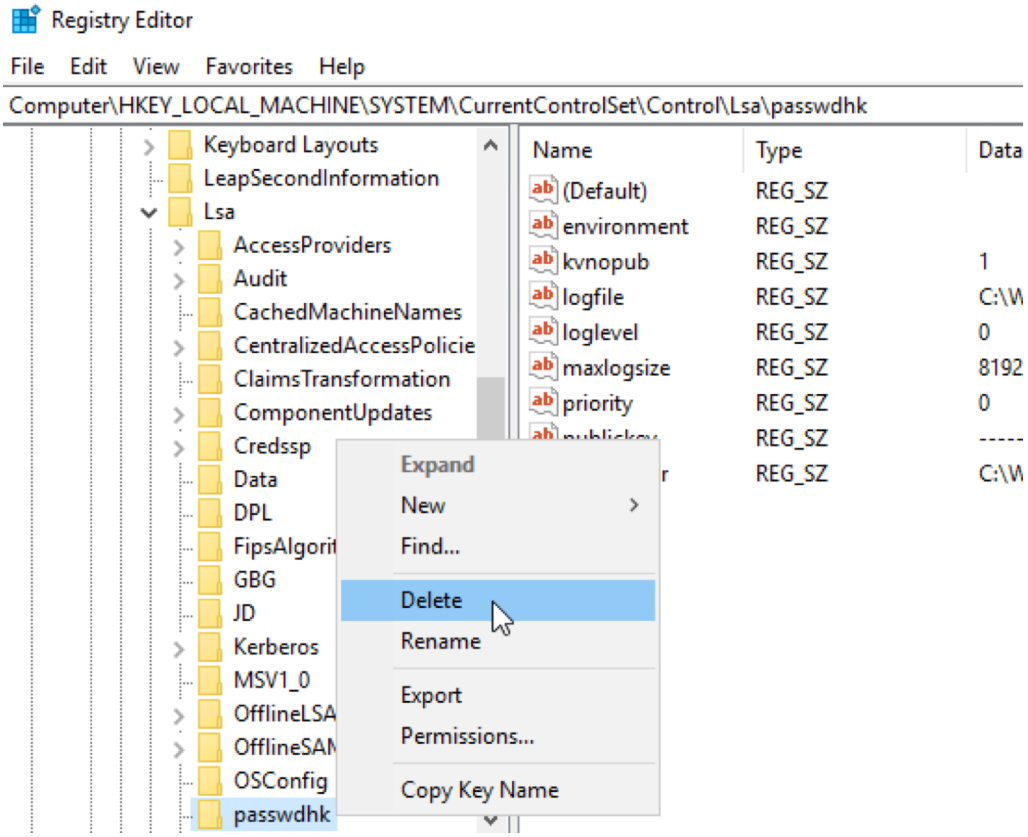


2. Удалить папку `passwdhk` из сетевого каталога `\\<Имя-контроллера-домена>\SYSVOL\<Имя-домена>\scripts`.



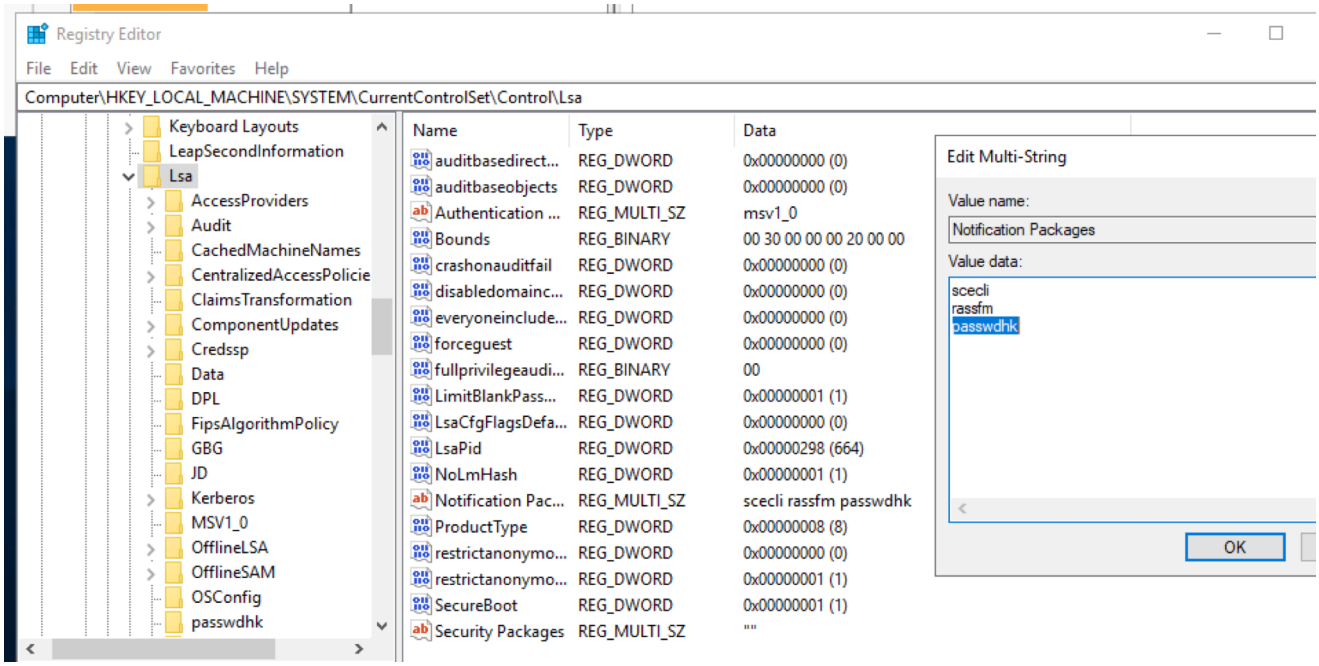
3. Очистить параметры в реестре:

- Удалить ключ `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\passwdhk`.



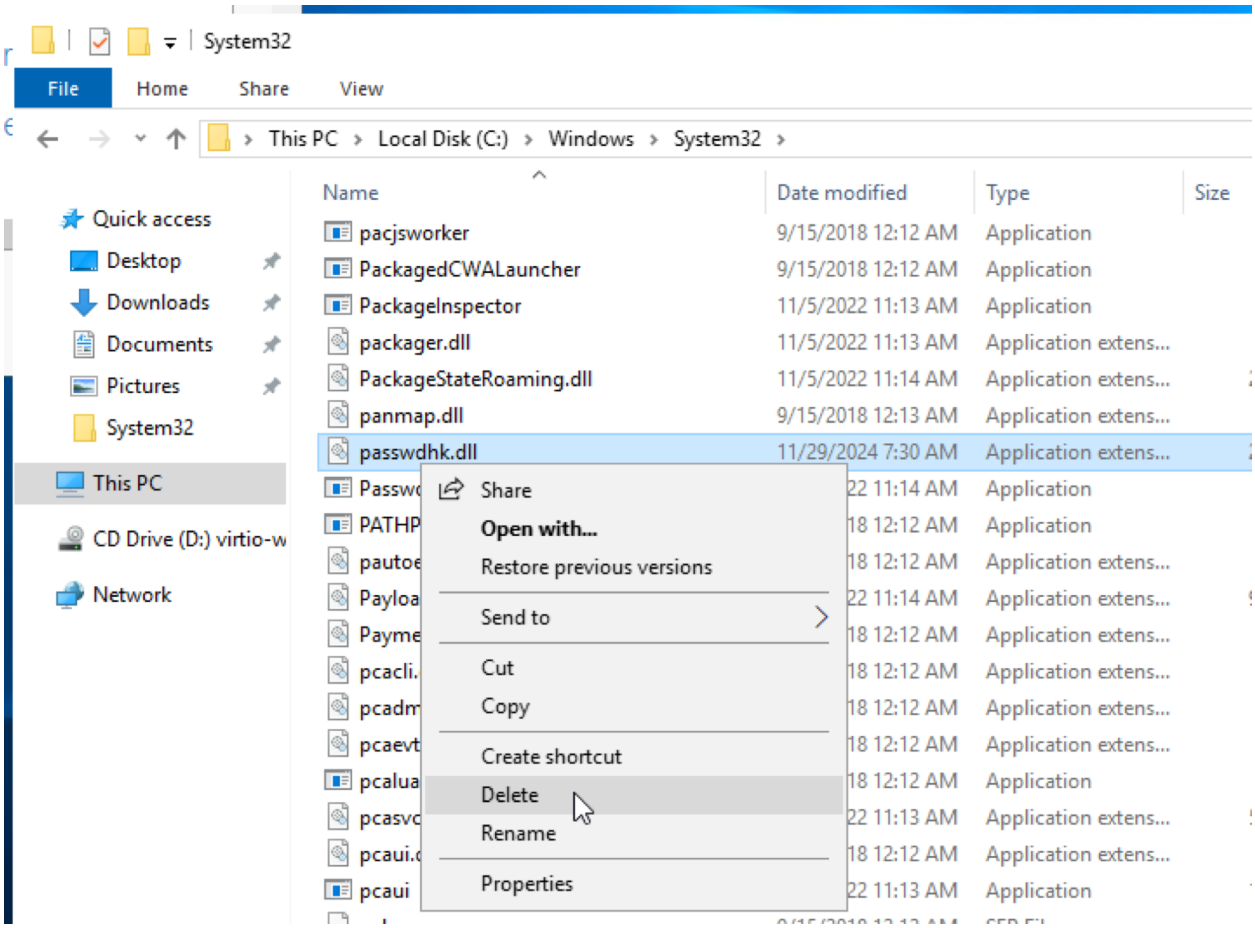
- В параметре Notification Packages по пути `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`

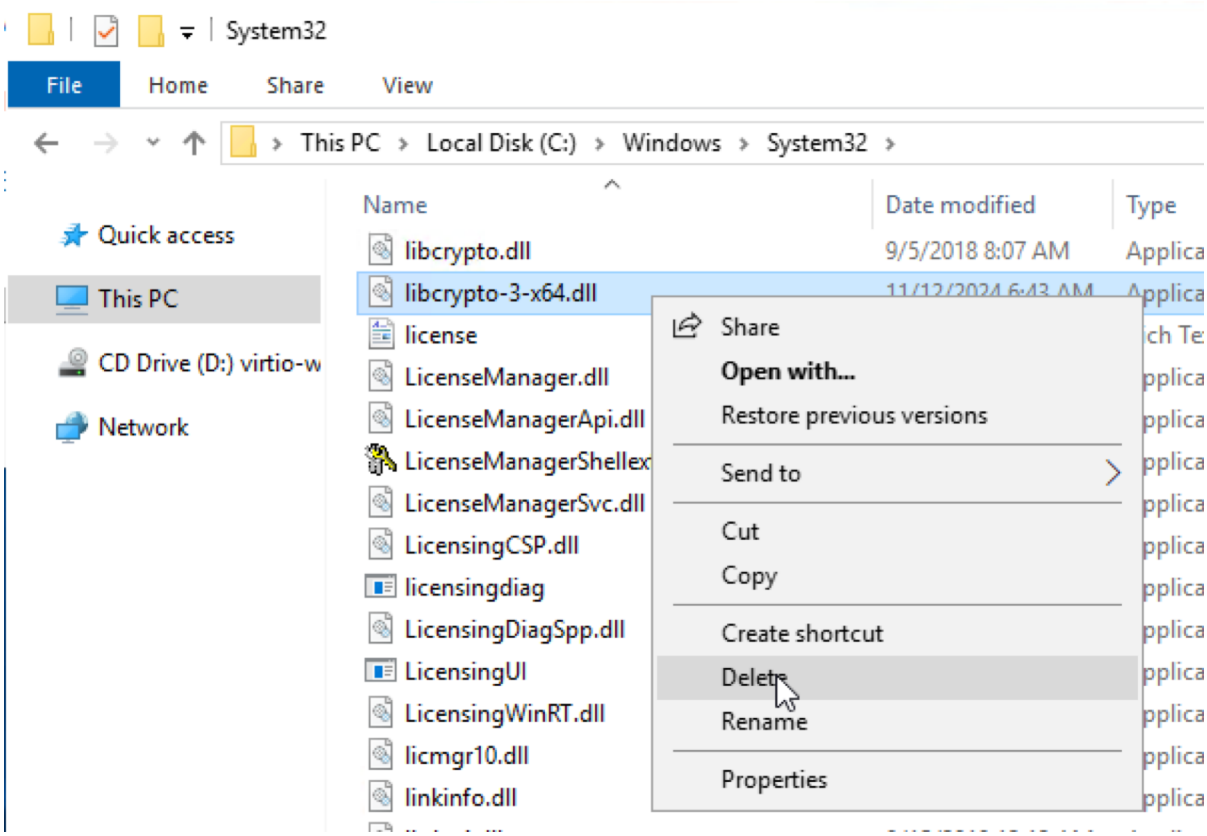
удалите значение `passwdhk`.



1. Перезагрузить контроллер домена для применения изменений.

2. После перезагрузки вручную удалить из каталога `C:\Windows\System32` файлы `passwdhk.dll` и `libcrypto-3-x64.dll`.





6. Выполнить установку новой версии `passwdhk` через `PasswdhkSetup.msi`, следуя инструкции из пункта инструкции **Исходные настройки** для модуля синхронизации.

3.9.1.4. Автоматизированная установка passwdhk через MST-файл

Для массовой установки утилиты `passwdhk` на контроллеры домена можно использовать файл трансформации (MST), содержащий заранее заданные параметры конфигурации, который можно развернуть с помощью групповой политики (GPO).

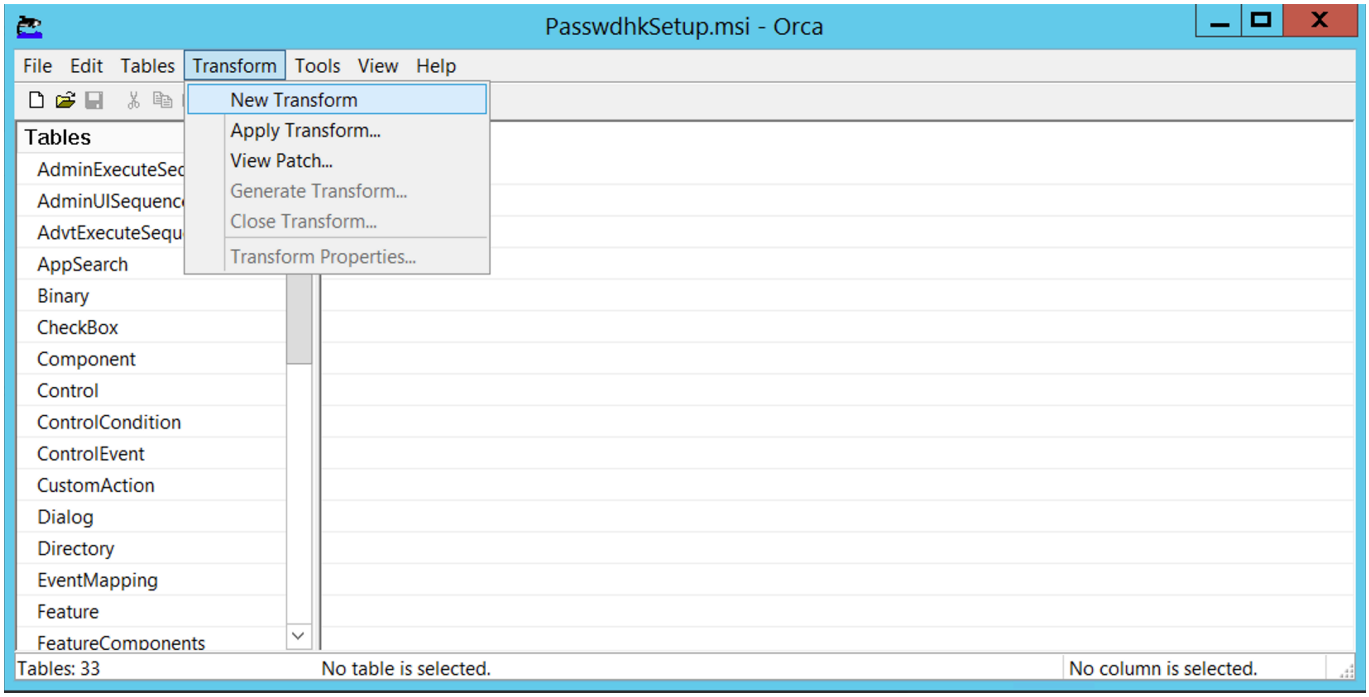
Примечание: Для редактирования установочного файла `.msi` и создания `.mst` трансформации можно использовать любую утилиту, поддерживающую редактирование таблиц MSI-файлов (например, **Orca** или аналогичные средства). В данной инструкции приведены примеры с использованием Orca.

Создание MST-файла

1. Открыть `PasswdhkSetup.msi` в утилите редактирования MSI-файлов и создать новый трансформационный файл (MST).

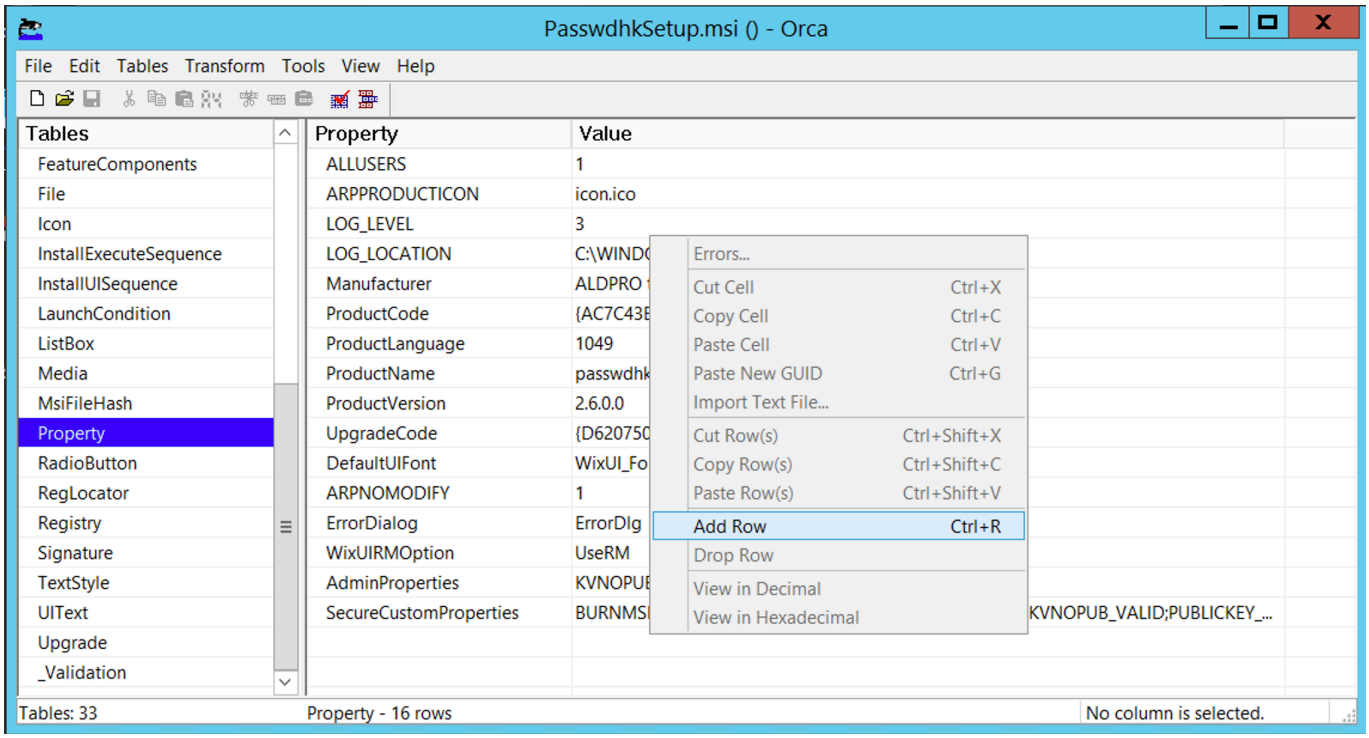
2. В меню File → Open выбрать установочный файл `PasswdhkSetup.msi`.

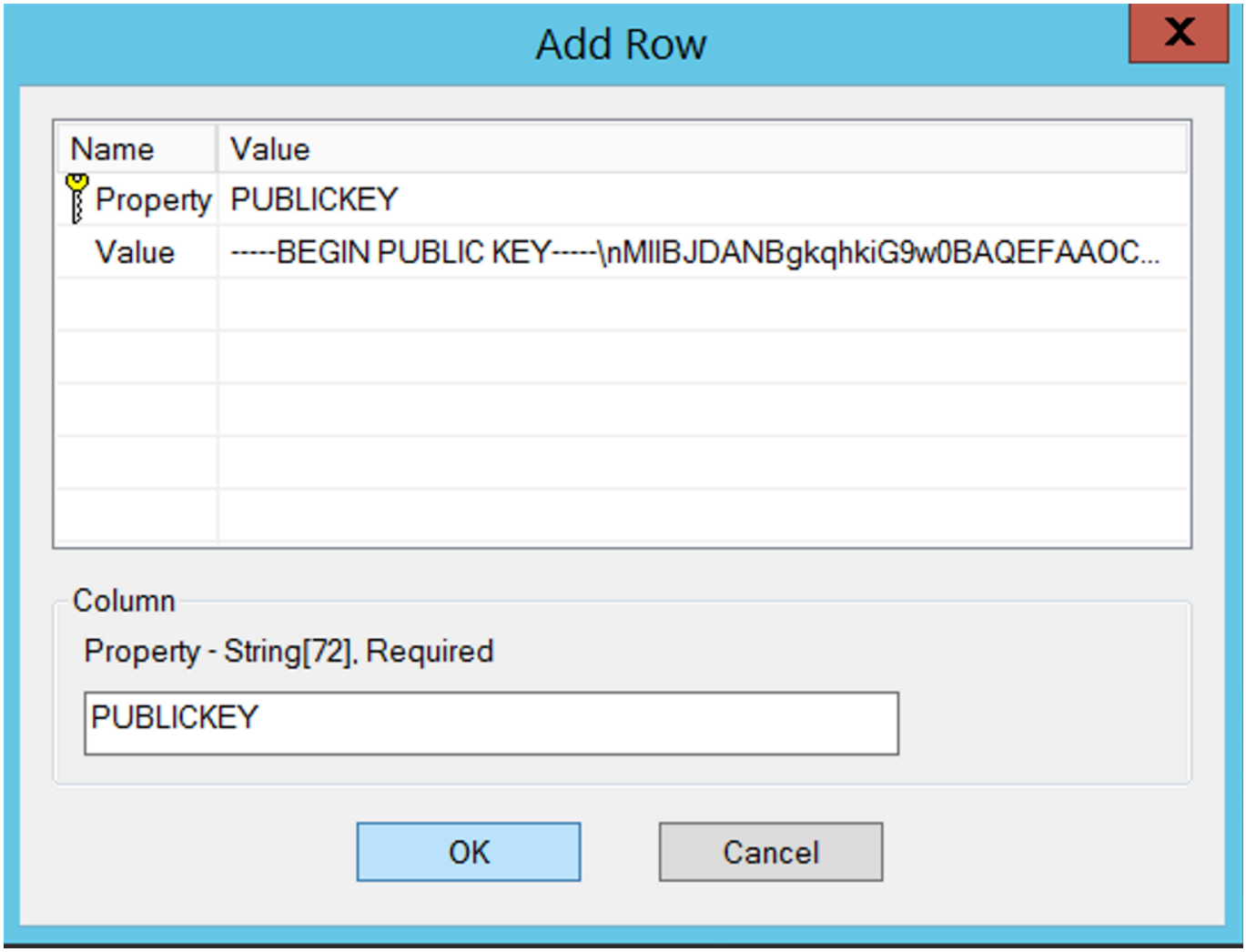
3. В меню **Transform** выбрать **New Transform**.

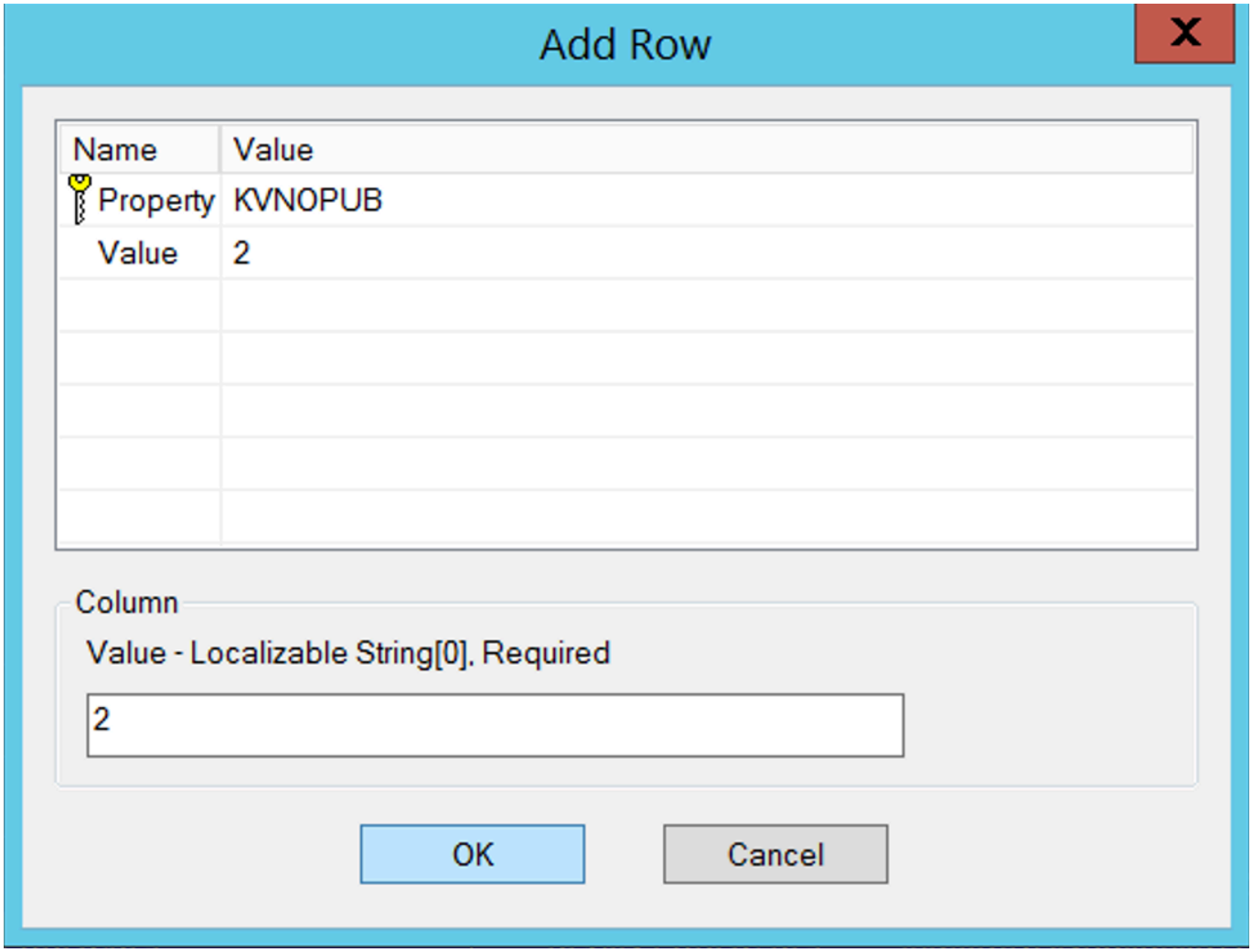


4. Перейти на вкладку **Property** и добавить следующие свойства:

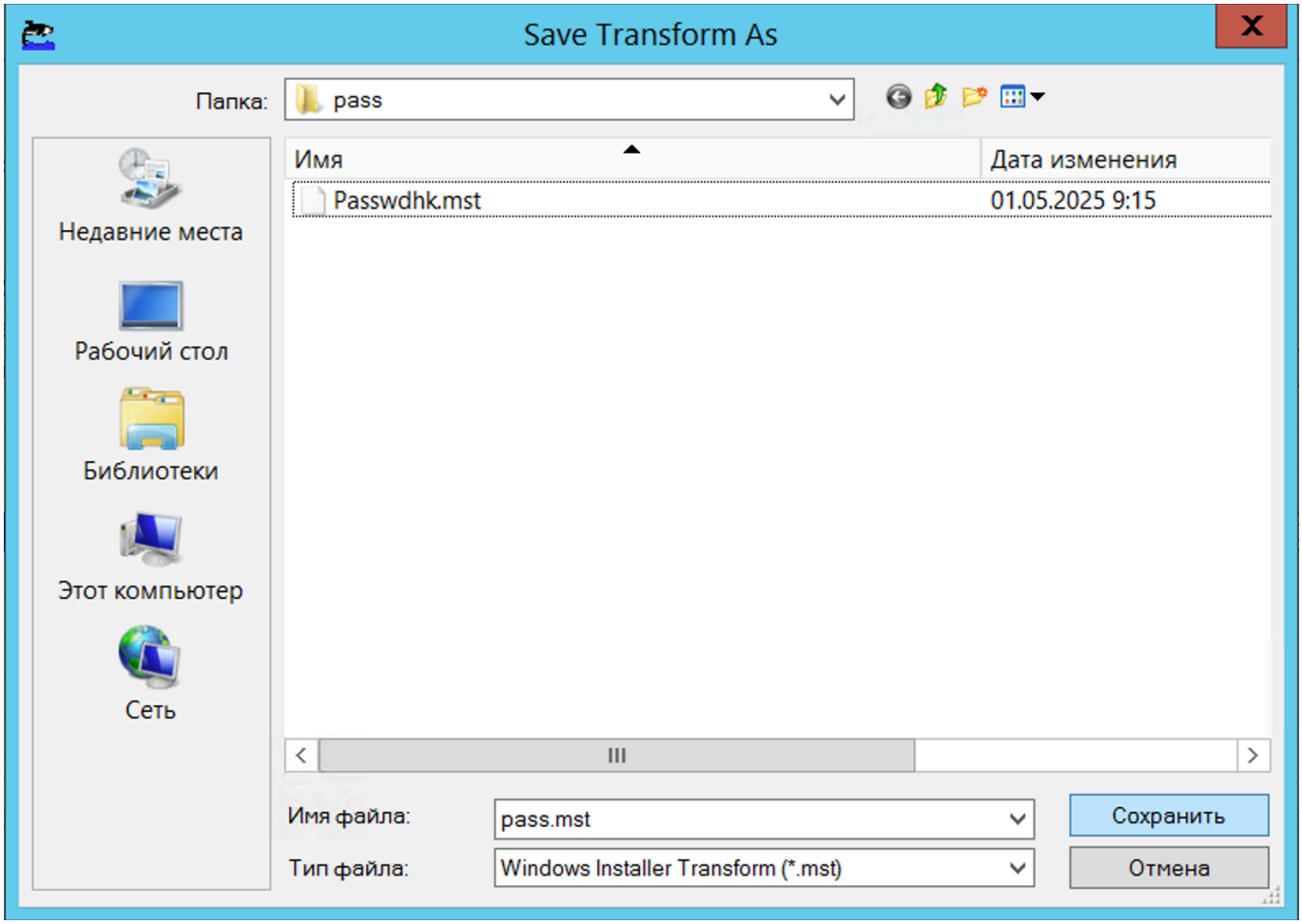
- `REGKEY` — вставьте публичный ключ регистрации, полученный на портале управления **ALD Pro**. Каждую строку ключа необходимо экранировать символом n (перевод строки).
- `KVNOPUB` — номер ключа, также полученный на портале.




Add Row
Name
Value
Property
PUBLICKEY
Value
-----BEGIN PUBLIC KEY-----\nMIIBJDANBgkqhkiG9w0BAQEFAAOC...
Column
Property - String[72]. Required
PUBLICKEY
OK
Cancel



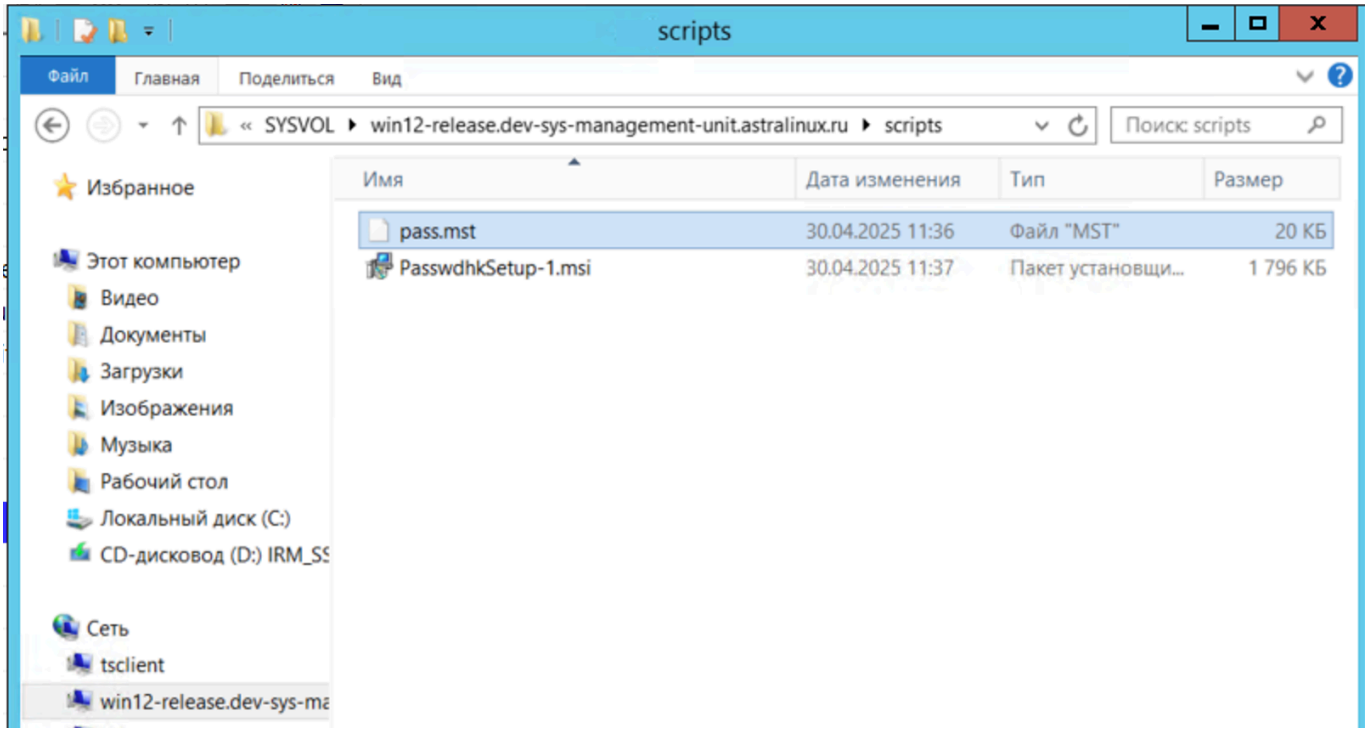
5. После добавления параметров выбрать **Transform** → **Generate Transform** и сохранить полученный файл под именем, например, `pass.mst`.



Подготовка файлов для установки

1. Перейти в сетевую папку:
   `\\<Имя-контроллера-домена>\SYSVOL\<Имя-домена>\scripts`
2. Скопировать в нее следующие файлы:

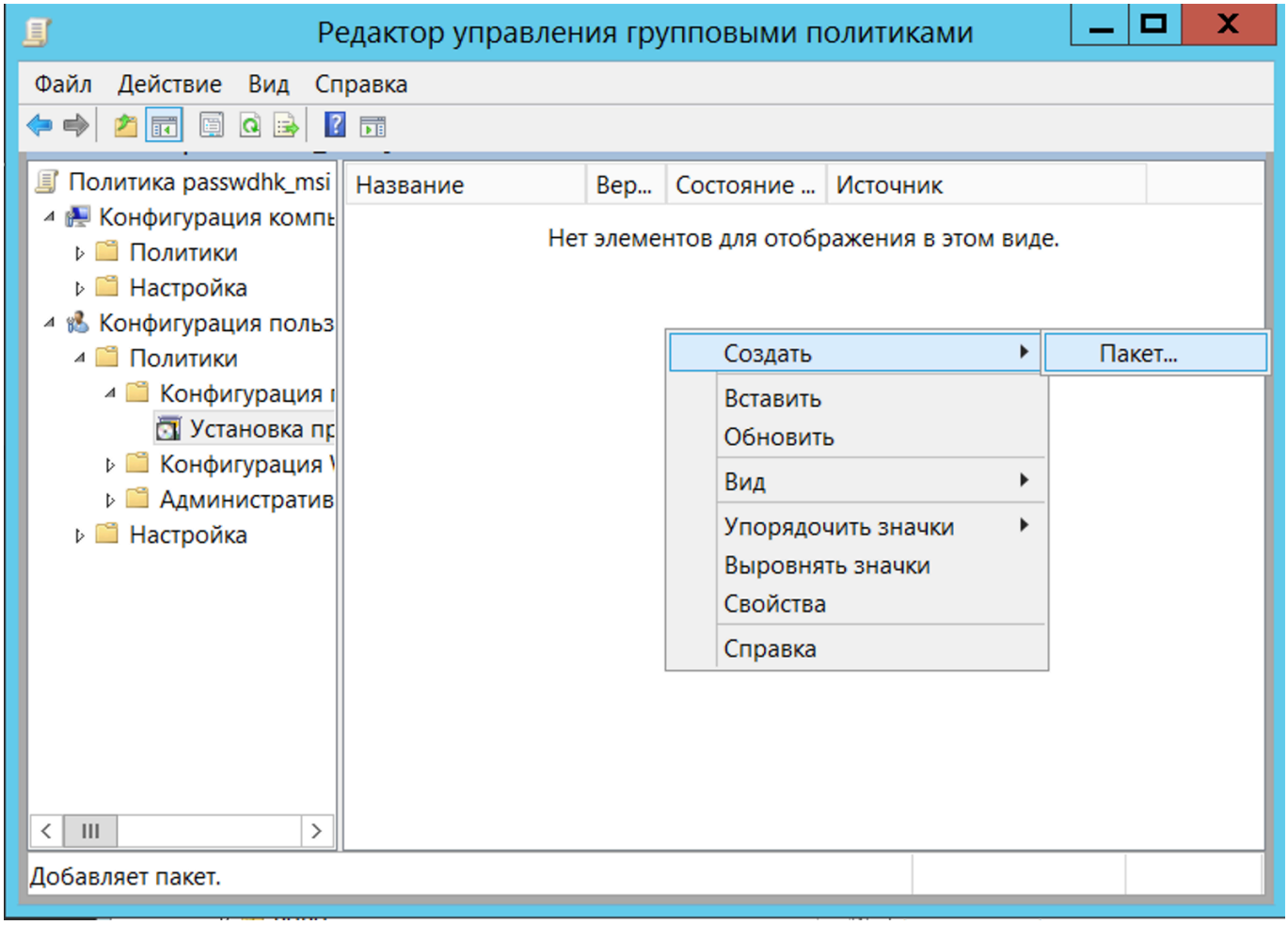
- `PasswdhkSetup.msi`;
- `pass.mst`.



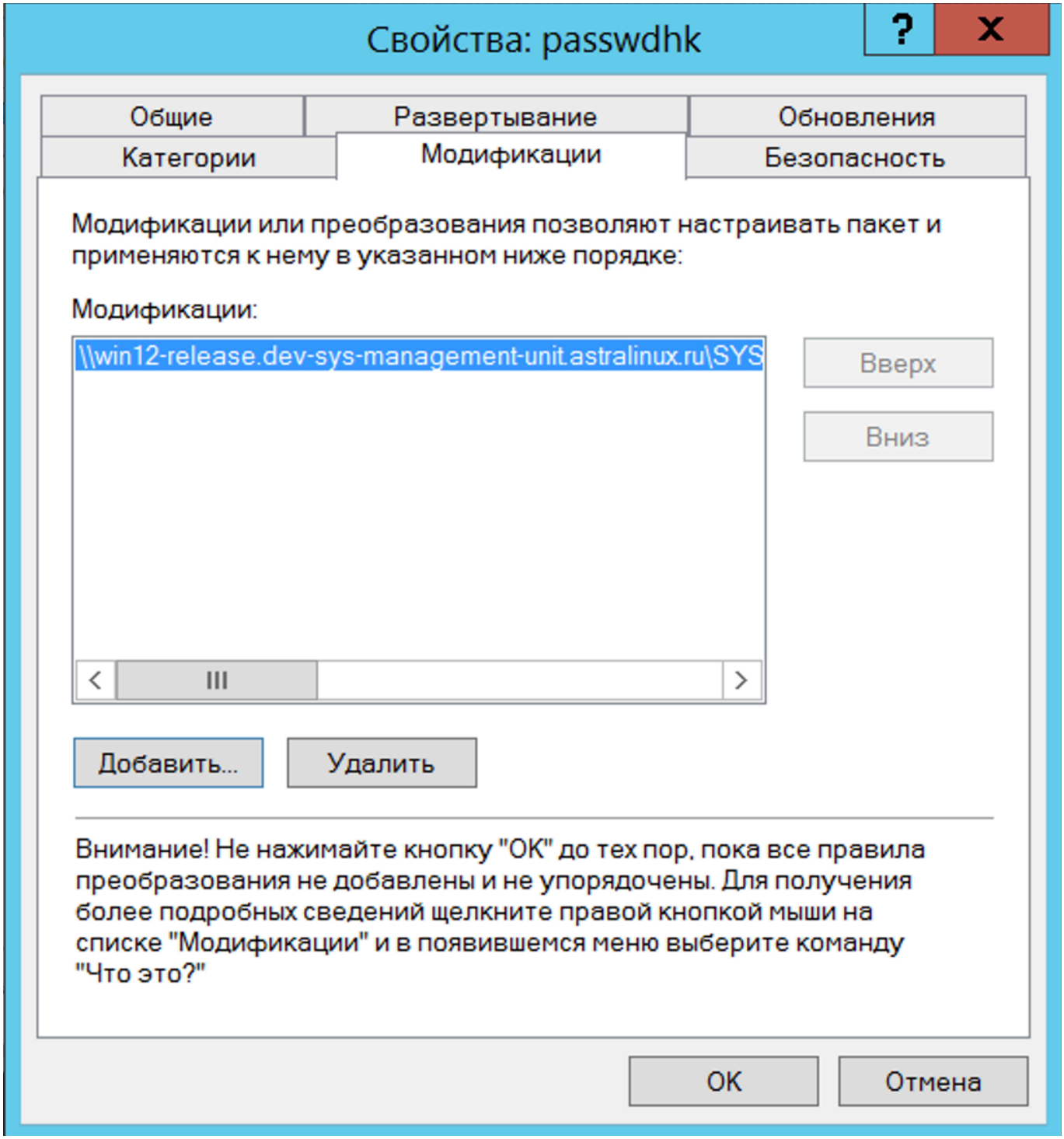
Настройка групповой политики

1. Открыть редактор групповой политики (gpmc.msc).
2. В узле **Domain Controllers** создать новую групповую политику или использовать существующую.
3. Перейти в раздел: **Конфигурация пользователя** → **Политики** → **Конфигурация программ** → **Установка программ**.
4. Создать новый пакет:

- Указать путь к `PasswdhkSetup.msi` из сетевой папки;
- в способе развертывания выбрать Особый.



5. Добавить MST-файл `pass.mst` по тому же сетевому пути.



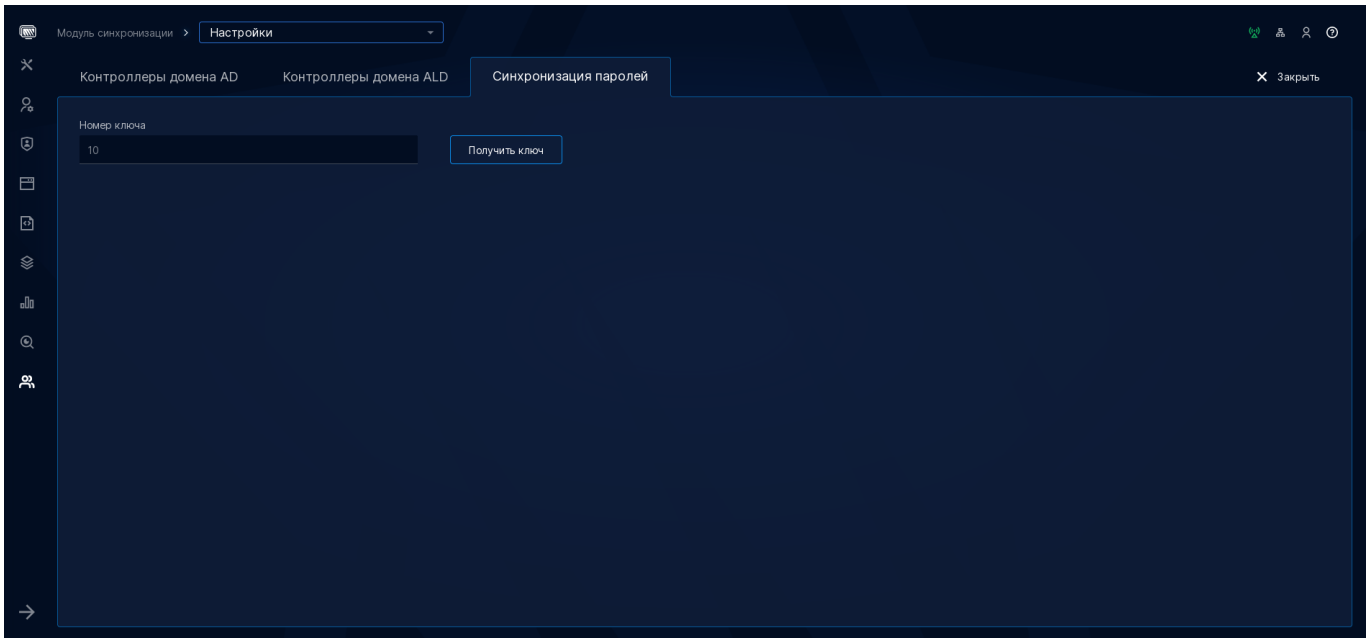
Применение политики

1. Применить политику командой: `gpupdate /force`
2. Перезагрузить контроллер домена.

3.9.1.5. Синхронизация паролей ALD Pro → MS AD

Получение открытого ключа

В интерфейсе ALD Pro открыть **Модуль синхронизации** → **Конфигурации** → **Синхронизация паролей**



По нажатию кнопки **Получить ключ** скачивается файл открытого ключа и актуализируется порядковый номер ключа.

Синхронизация паролей

Скачанный файл открытого ключа необходимо сохранить в любую директорию, например, `/tmp/`. Следующим шагом файл открытого ключа необходимо скопировать в расположение `/opt/rbta/aldpro/syncer/`:

```
sudo cp /tmp/public.gpg  /opt/rbta/aldpro/syncer/public.gpg
```

Перезагружаем контроллер домена:

```
sudo aldproctl restart
```

Примечание:

- При изменении пароля синхронизированного пользователя через интерфейс FreeIpa, синхронизация пароля от ALD Pro к MS AD не произойдет. Для изменения пароля с последующей успешной синхронизацией необходимо использовать интерфейс ПК «ALD Pro»;
- Процесс изменения пароля пользователя через личный кабинет с последующей синхронизацией от ALD Pro к MS AD проходит успешно только при использовании личного кабинета контроллера домена, на котором был развернут модуль синхронизации;
- При сбросе пароля пользователя через интерфейс ПК «ALD Pro» временный пароль не синхронизируется. После сброса пароля пользователя необходимо залогиниться в домене, изменить пароль с временного на постоянный. При данных условиях произойдет синхронизация пароля от ALD Pro к MS AD.

Пароли пользователей MS AD, установленные до настройки модуля синхронизации, синхронизированы не будут.

Синхронизация паролей пользователей после настройки модуля синхронизации и сопоставлений подразделений происходит по логике:

- синхронизирован пользователь в домен ALD Pro → изменен пароль пользователя в домене MS AD → синхронизирован пароль пользователя в домен ALD Pro;
- создан пользователь в домене MS AD → синхронизирован пользователь в домен ALD Pro.

Внимание: При настройке синхронизации паролей между ALD Pro и MS AD рекомендуется вручную задать согласованные значения параметров политики паролей в обеих системах, так как их автоматическая синхронизация не предусмотрена.

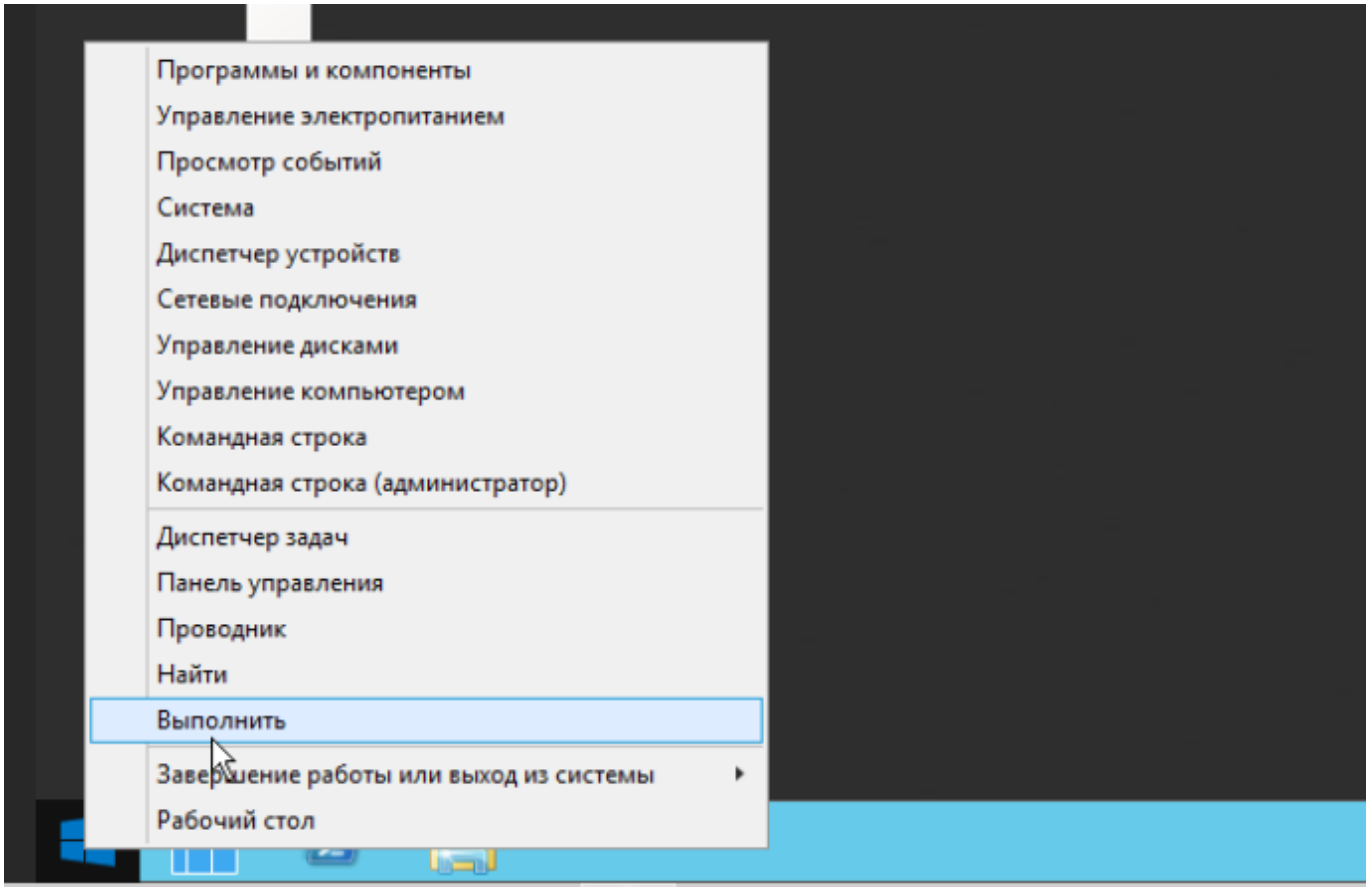
3.9.1.6. Включение TLS на Windows Server 2008R2

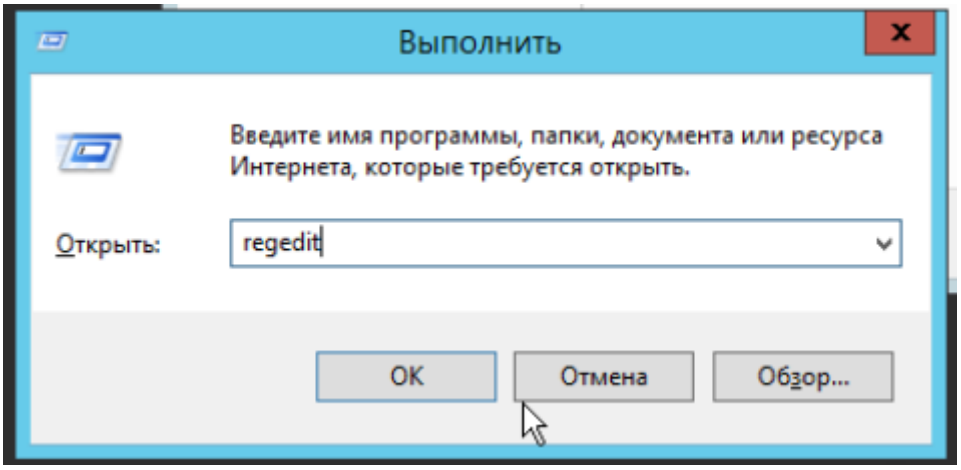
Важно: Настройка выполняется, если на контроллере домена отключено TLS. Данная инструкция применима к контроллерам домена с ОС WS 2008R2. Если версия ОС отличается, необходимо обратиться к официальной документации Microsoft для выбора

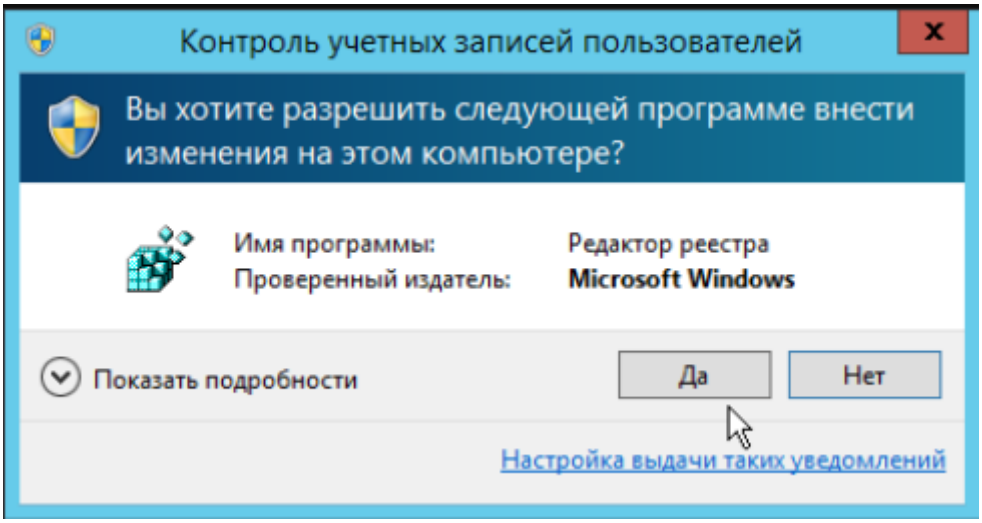
подходящей инструкции.

Алгоритм включения TLS

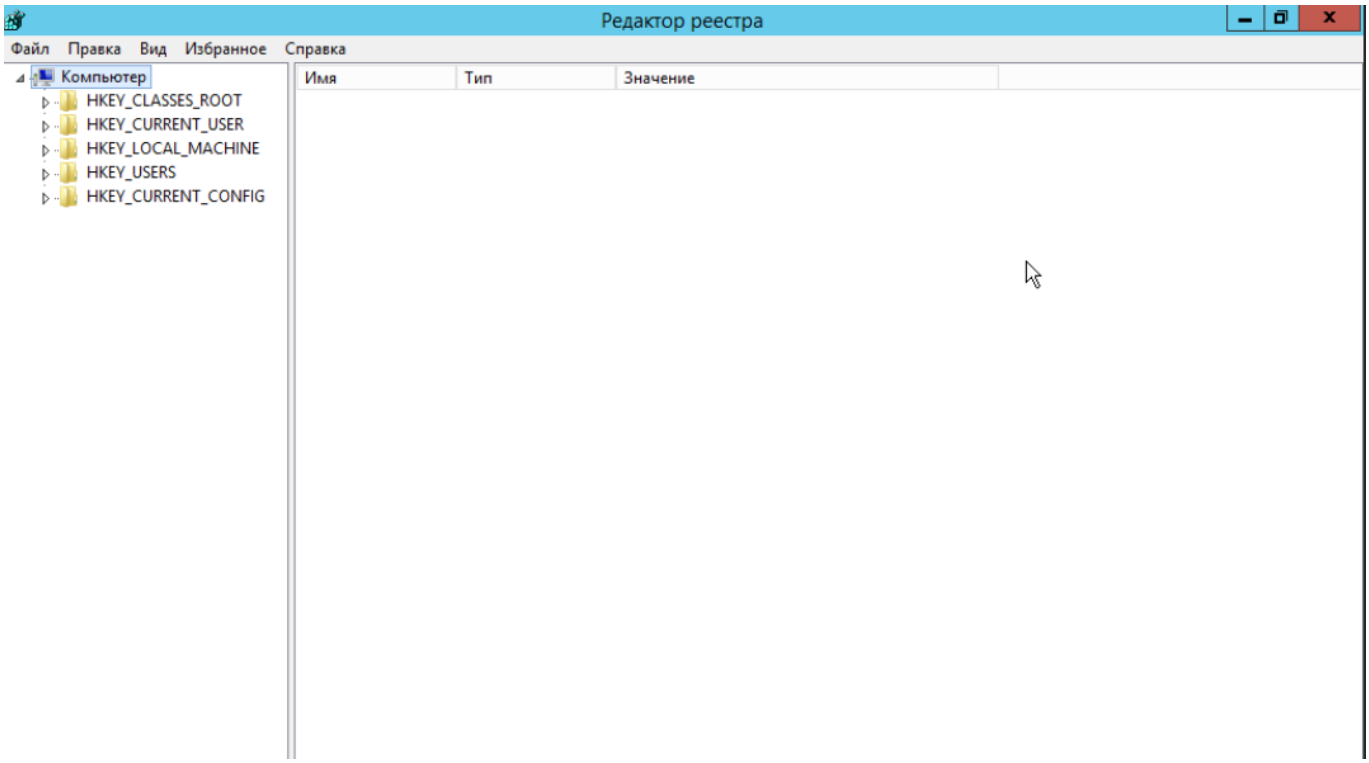
1. Для включения TLS необходимо обновить реестр на сервере контроллера домена.
    - Необходимо открыть реестр: выполнить “regedit” в окне запуска.





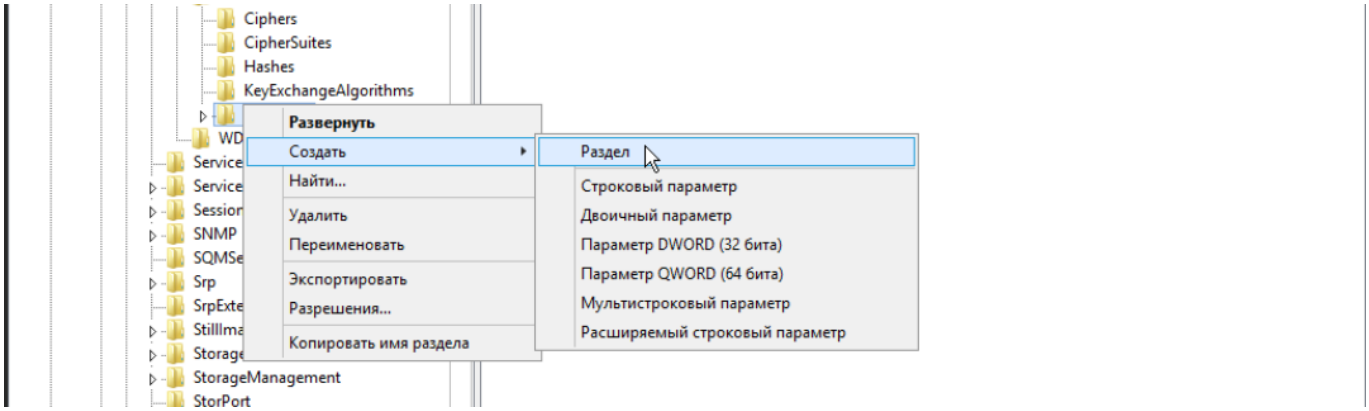


Откроется окно редактора реестра:



- Необходимо перейти к расположению и добавить разделы TLS 1.1 и TLS.
- В разделе Protocol:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\
SCHANNEL\Protocol
```



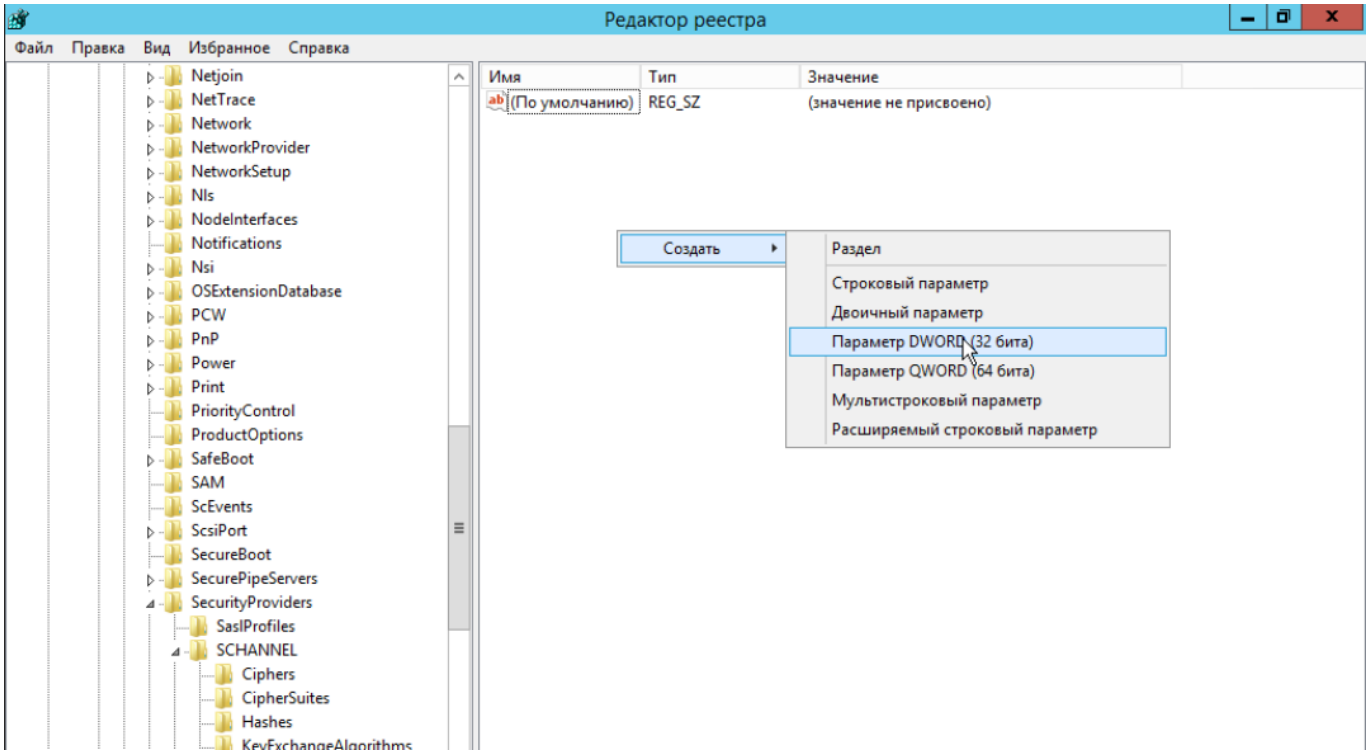


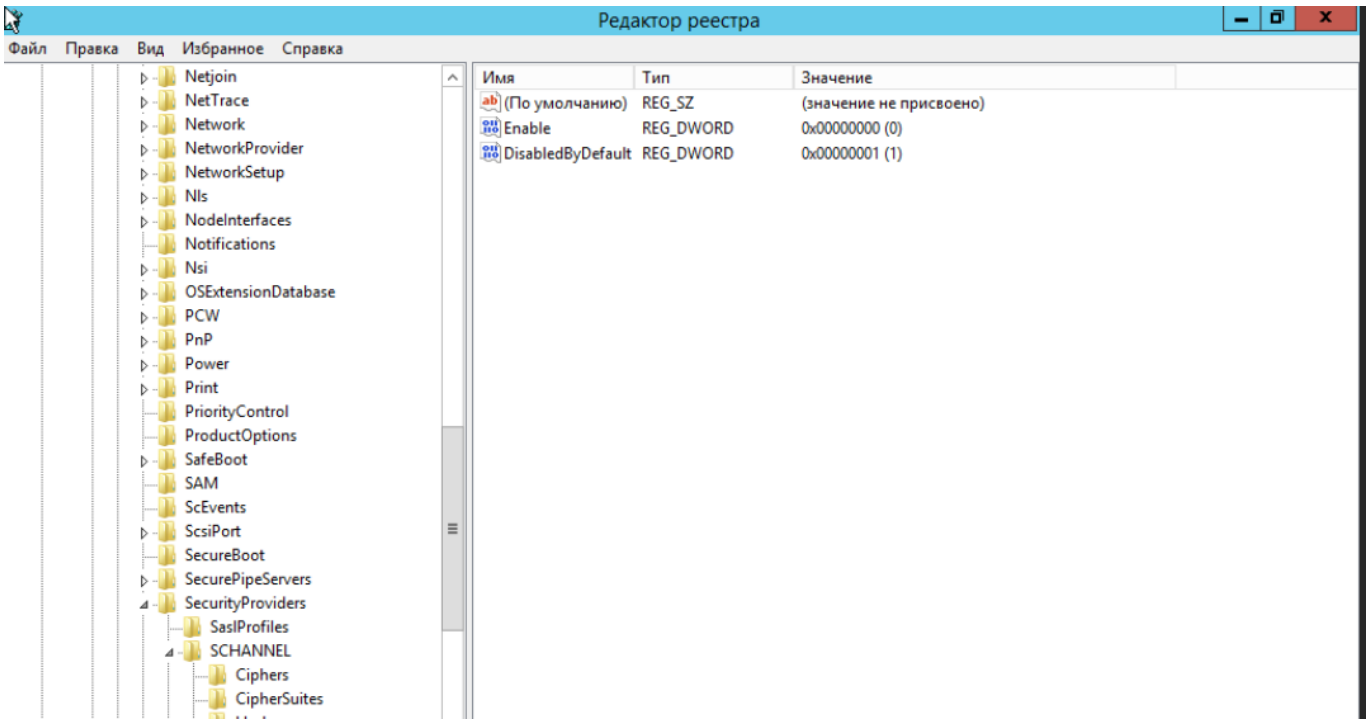
Создаются еще два раздела Client и Server под обоими ключами TLS.



- Теперь необходимо создать значения DWORD в разделе Server и Client со следующими значениями:

```
DisabledByDefault [Значение = 0]
Enabled [Значение = 1]
```





2. Необходимо отключить старые версии TLS и SSL. Для этого:

    1. Открыть реестр на сервере контроллера домена: выполнить “regedit” в окне запуска (аналогично шагу 1).

    2. Перейти к расположению:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`

3. Изменить значения DWORD в разделе Server и Client в разделе ключи TLS 1.0, SSL 3.0 и более старых версий SSL.

```
DisabledByDefault [Значение = 0]
Enabled [Значение = 0]
```

3. После выполнения всех вышеперечисленных настроек необходимо перезагрузить сервер контроллера домена. Данная настройка выполняется на всех контроллерах домена.

3.9.1.7. Особенности настройки при миграции большого количества объектов

По умолчанию 389ds выполняет обновления ссылочной целостности сразу после операции удаления или переименования. В зависимости от количества операций это может повлиять на производительность. Чтобы уменьшить влияние на производительность, есть возможность увеличить время между обновлениями, для этого необходимо задать интервал обновления в секундах. По умолчанию интервал обновления равен 0.

Чтобы показать имя 389ds-сервера:

```
sudo dsctl -l
```

Скопируйте в буфер имя вашего сервера (рядом с ним вы увидите `slapd-GLOBAL-CATALOG`). Чтобы отобразить текущий интервал обновления, запустите (заменив <имя LDAP-сервера> на имя нужного вам LDAP-сервера):

```
sudo dsconf <имя LDAP-сервера> plugin referential-integrity show | grep
 ↪referint-update-delay
```

Задать новое значение интервала обновления:

```
sudo dsconf <имя LDAP-сервера> plugin referential-integrity set --update-
 ↪delay <новое_значение>
```

Перезапустите инстанс:

```
sudo dsctl <имя LDAP-сервера> restart
```

3.9.1.8. Логирование событий и отладка (работы модуля синхронизации) с MS AD

Логирование событий и отладка

Данный раздел посвящён диагностике и устранению ошибок, возникающих при синхронизации между ALD Pro и Microsoft Active Directory (MS AD). Приведены типовые сценарии возникновения проблем, способы их диагностики, а также рекомендации по их устранению.

События, возникающие в процессе синхронизации, фиксируются в соответствующих журналах событий. Выполнение диагностики **целесообразно начинать с анализа этих журналов**.

Общие категории ошибок:

- Ошибки при установке и первоначальной настройке;
- Ошибки, возникающие при отсутствии связности между ALD Pro и MS AD;
- Ошибки при сопоставлении структур (например, дочерних подразделений) между ALD Pro и MS AD.

Ошибки могут проявляться при взаимодействии компонентов, выполняющих синхронизацию данных:

- компонент `passwdhk`;
- служба `syncer-watcher`;
- служба `syncer-loadrunner`;
- служба `pwdSync`.

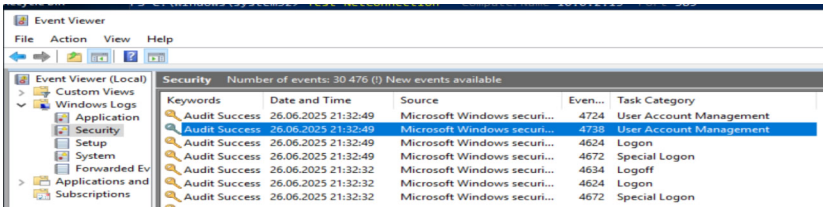
Под данными службами подразумевается следующее: - Служба syncer-watcher выполняет синхронизацию данных из LDAP контроллера MS AD в базу PostgreSQL на контроллера ALD Pro; - Служба syncer-loadrunner выполняет синхронизацию из базы PostgreSQL в LDAP на контроллере ALD Pro; - Служба pwdSync выполняет синхронизацию паролей пользователей в MS AD и ALD Pro.

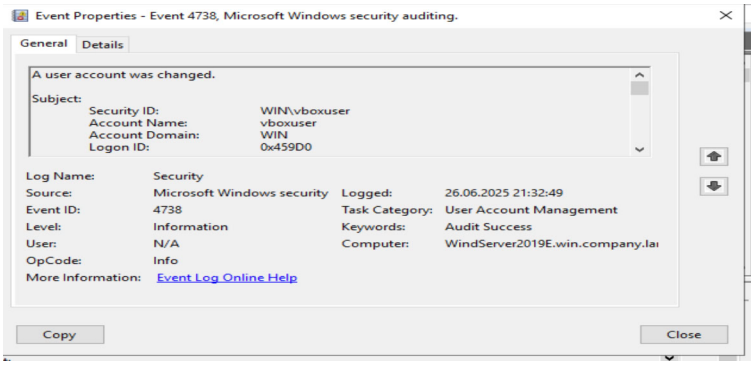
3.9.2. Отладка работы модуля синхронизации

3.9.2.1. Диагностика интеграции с MS AD

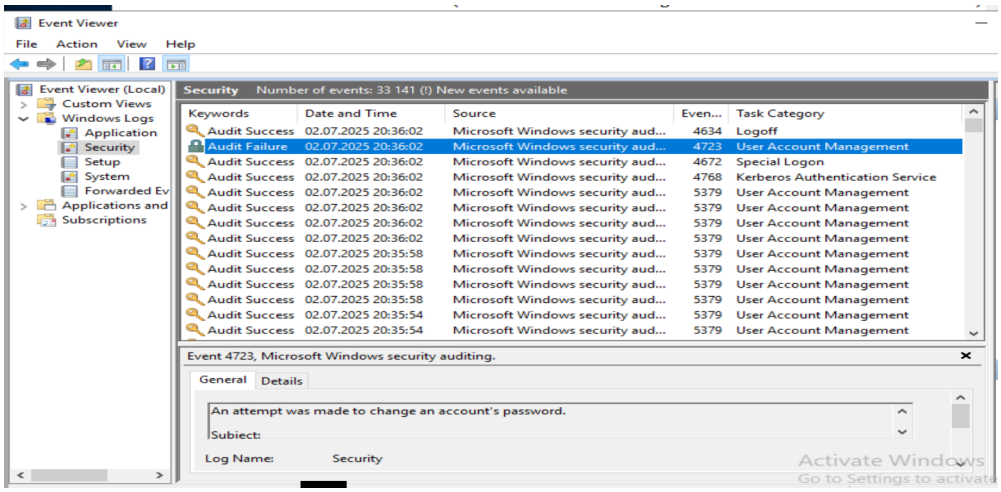
Диагностическая информация модуля интеграции с MS AD фиксируется в журналах событий LSA (Login Security Authority). В этих журналах отражаются:

- Успешная смена пароля





- Неуспешная смена пароля





Внимание: **Типичная ошибка**: После вставки публичного ключа LDAP может возникнуть ошибка вида ``**id2 not found**``. **Решение**: Проверить директорию, в которую скопирован ключ. Убедиться, что путь указан верно, и повторно задать ключ в web-интерфейсе ALD Pro, если он не найден.

Примечание:

- При сопоставлении подразделений необходимо убедиться, что логин указывается в виде `user@domain`, иначе возможны ошибки авторизации;
- В случае потери ключа авторизации (например, ``**id2 not found**``), необходимо проверить директорию хранения ключей и выполнить переустановку через интерфейс управления.

3.9.2.2. Отладка работы модуля syncer

Для отладки работы модуля синхронизации необходимо включить режим отладки (debug):

```
root@syncer-dc1:~# nano /opt/rbta/aldpro/syncer/.env
DEBUG=True
```

Логи:

- *syncer_loadrunner.log* — отвечает за синхронизацию из PostgreSQL в ALD Pro:

  ```
  /var/log/aldpro/syncer/syncer_loadrunner.log
  ```

- *syncer_watcher.log* — отвечает за чтение данных из MS AD и запись в PostgreSQL:

```
/var/log/aldpro/syncer/syncer_watcher.log
```

3.9.2.3. Отладка работы модуля pwdSync

Модуль синхронизации паролей между MS AD и ALD Pro поддерживает включение режима отладки через файл:

```
root@syncer-dc1:~# nano /opt/rbta/aldpro/syncer/pwd_sync/standalone/__init__.
↪py
DEBUG = True
```

Журналы:

- Журнал отладки:

```
/var/log/aldpro/syncer/pwd_sync/standalone_debug.log
```

- Журнал ошибок:

```
/var/log/aldpro/syncer/pwd_sync/standalone_error.log
```

Важно: Текущая реализация не требует ручного перезапуска служб — запуск синхронизации осуществляется по расписанию **systemd** (таймеры, относящиеся к службам syncer-watcher, syncer-loadrunner, pwdSync).

3.9.2.4. Сценарии отладки

Ниже представлены типовые сценарии поиска и устранения ошибок.

3.9.2.5. Проверка состояния служб

Следует проверить, что таймеры служб активны, а службы запущены:

```
systemctl status syncer-watcher.timer
systemctl status syncer-loadrunner.timer
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
systemctl status syncer-pwdsync.timer

systemctl status syncer-watcher.service
systemctl status syncer-loadrunner.service
systemctl status syncer-pwdsync.service
```

При наличии ошибок рекомендуется проверить журнал службы:

```
journalctl -u syncer-watcher.service
journalctl -u syncer-loadrunner.service
journalctl -u syncer-pwdsync.service
```

3.9.2.6. Ошибка дублирования имени при создании объекта

Если имя пользователя или группы совпадает в ALD Pro и MS AD, процесс *syncer-loadrunner* завершится с ошибкой:

```
CRITICAL     ipa_load_runner   Объект objectGUID=2f880038-bba4-4f05-b115-
↪8b3a8da217b5 не может быть создан в ALD Pro из-за дублирования имени.
ERROR        ipa_load_runner   Объект не может быть создан в ALD Pro из-за
↪дублирования имени.
```

Решение:

- Переименовать объект в одном из источников;
- Удалить объект из ALD Pro.

Важно: Перед началом синхронизации важно убедиться, что в настроенной точке синхронизации (подразделении) в MS AD и ALD Pro отсутствуют записи пользователей, групп, полностью идентичных друг другу (с одинаковыми именами). Если такие записи существуют, то в процессе синхронизации это приведет к ошибке и невозможности синхронизации.

3.9.2.7. Повторное появление удалённого объекта

Если пользователь/группа была удалена из ALD Pro и корзины, но осталась в MS AD, она может быть вновь синхронизирована.

Примеры логов:

```
ERROR     ipa_load_runner   Объект objectGUID=... не найден в ALD Pro
INFO      ipa_load_runner   Сохранение объекта objectGUID=..., sync_status=3
CRITICAL  ipa_load_runner   Ошибка при обработке объекта. Требуется
↪устранить ошибку вручную
```

Решение:

- Удалить объект в MS AD или исключить его из области синхронизации;
- Дождаться появления в корзине ALD Pro и удалить повторно.

3.9.2.8. Отладка проблемы: объект не создаётся в ALD Pro

Пошаговая диагностика:

1. Определить значение атрибута `objectGUID` объекта в LDAP MS AD;
2. Найти строки с ключевыми словами `Error` и нужным `objectGUID` в `syncer_watcher.log`.

```
grep '2f880038-bba4-4f05-b115-8b3a8da217b5' /var/log/aldpro/syncer/syncer_
↪watcher.log
```

3. Найти строки с ключевыми словами *Error* и нужным *objectGUID* в *syncer_loadrunner.log*.

```
grep '2f880038-bba4-4f05-b115-8b3a8da217b5' /var/log/aldpro/syncer/syncer_
↪loadrunner.log
```

Примечание: Если при создании точки синхронизации MS AD → ALD Pro задано одно сопоставление, второе сопоставление в той же точке будет невозможно. Такое поведение также фиксируется в логах и требует пересмотра структуры.

3.9.2.9. Неизвестный класс объекта в логах syncer-watcher

В процессе поиска объектов для синхронизации в журнале **`syncer-watcher.log`** могут встречаться ошибки следующего вида:

```
2025-06-25 07:12:03 syncer INFO     runners   Число объектов для обработки в
↪watcher: 3
2025-06-25 07:12:03 syncer INFO     runners   Обработка объектов
2025-06-25 07:12:03 syncer ERROR    runners   Неизвестный класс объекта
2025-06-25 07:12:03 syncer ERROR    runners   Неизвестный класс объекта
2025-06-25 07:12:03 syncer ERROR    runners   Неизвестный класс объекта
```

Примечание: Данная ошибка **не является критичной** и не влияет на дальнейшую работу службы **`syncer-watcher`**.

В процессе выполнения запроса к каталогу LDAP MS AD в результат поиска могут попасть **служебные объекты**, которые не подлежат синхронизации. Например:

```
# search reference
ref: ldap://ForestDnsZones.corp.test/DC=ForestDnsZones,DC=corp,DC=test

# search reference
ref: ldap://DomainDnsZones.corp.test/DC=DomainDnsZones,DC=corp,DC=test

# search reference
ref: ldap://corp.test/CN=Configuration,DC=corp,DC=test
```

Подобные объекты игнорируются при синхронизации и не влияют на корректность основного процесса.

3.9.2.10. Ошибка удаления объекта, отсутствующего в ALD Pro

Если объект был удалён из точки синхронизации (подразделения в MS AD) или перемещён в другое подразделение, **но при этом его уже нет в ALD Pro**, возможно появление ошибки при попытке удаления:

```
2025-06-25 11:26:41 syncer DEBUG     ipa_load_runner   Обработка объекта
↪objectGUID=6cc876e1-40ae-44b3-b4a8-a9044f7dd69a, nsuniqueID=None, тип
↪объекта=user, sync_status=3
2025-06-25 11:26:41 syncer DEBUG     ipa_load_runner   Удаление объекта
↪nsuniqueID=None
2025-06-25 11:26:41 syncer DEBUG     provider   Запрос для объекта в целевой
↪LDAP используя метод user_del
2025-06-25 11:26:41 syncer ERROR     ipa_load_runner   Ошибка во время
↪удаления {'code': 4001, 'message': 'user1: user not found', 'data': {
↪'reason': 'user1: user not found'}, 'name': 'NotFound'}
2025-06-25 11:26:41 syncer INFO      ipa_load_runner   Сохранение объекта
↪objectGUID=6cc876e1-40ae-44b3-b4a8-a9044f7dd69a, nsuniqueID=None с sync_
↪status=0
2025-06-25 11:26:41 syncer INFO      ipa_load_runner   Удаление записи 1 в
↪точки синхронизации
```

Ошибка **`user not found`** означает, что в ALD Pro уже нет объекта, который предполагается удалить. Это может произойти, если:

- объект был удалён вручную или автоматически на предыдущих этапах;
- объект изначально не был синхронизирован, но был добавлен в список на удаление из-за изменений в MS AD.

Решение: данная ошибка не требует вмешательства. При следующем запуске службы **`syncer-loadrunner.service`** состояние синхронизации будет скорректировано, и сообщение об ошибке исчезнет.

3.9.2.11. Ошибка отсутствия TLS-сертификата для подключения к MS AD

Если в процессе подключения к целевому контроллеру MS AD отсутствует необходимый файл TLS-сертификата, в журнале *syncer_loadrunner.log* появится следующая ошибка:

```
2025-06-27 03:19:06 syncer DEBUG     strategy   Подключение к хосту dc1.ald.
↪company.lan успешно. Протокол API
2025-06-27 03:19:06 syncer DEBUG     provider   Подключение к целевой LDAP
2025-06-27 03:19:06 syncer DEBUG     strategy   Попытка подключения к dc1.ald.
↪company.lan
2025-06-27 03:19:06 syncer ERROR     ipa_load_runner   Нет файла сертификата
↪для подключения id=1
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
Traceback (most recent call last):
  ...
AttributeError: Нет файла сертификата для подключения id=1
2025-06-27 03:19:06 syncer DEBUG     provider   Отключение соединения от
↪целевой LDAP
2025-06-27 03:19:06 syncer INFO      ipa_load_runner   loadrunner завершился
```

Причина: отсутствует файл публичного ключа для LDAPS-подключения к контроллеру MS AD.

Решение: Скопировать сертификат *sert.pem* в требуемое расположение:

```
cp sert.pem /run/syncer/provider/key1.pem
```

Где *sert.pem* — это публичный ключ для LDAPS-подключения.

Либо проверить директорию, в которую скопирован ключ. Убедиться, что путь указан верно, и повторно задать ключ в web-интерфейсе ALD Pro, если он не найден.

Подробнее о подготовке и настройке сертификатов (см. cert_ms_ad).

3.9.2.12. Отсутствие связи с контроллером MS AD

Если со стороны ALD Pro отсутствует сетевое соединение с контроллером MS AD, в журнале *syncer_watcher.log* зафиксируется ошибка следующего вида:

```
2025-06-30 14:43:52 syncer DEBUG     provider   Подключение к LDAP источник
2025-06-30 14:43:52 syncer DEBUG     strategy   Попытка подключения к windc1.
↪corp.test
2025-06-30 14:43:55 syncer ERROR     strategy   {'desc': "Can't contact LDAP
↪server", 'errno': 107, 'info': 'Transport endpoint is not connected'}
2025-06-30 14:43:58 syncer ERROR     strategy   {'desc': "Can't contact LDAP
↪server", 'errno': 107, 'info': 'Transport endpoint is not connected'}
syncer ERROR     run   Не удалось подключиться к хосту=windc1.corp.test.
↪Протокол LDAP
```

Решение: Проверить доступность порта **389** на контроллере MS AD

```
nc -vz windc1.corp.test 389
```

Если порт недоступен — устранить ограничения, связанные с настройками сетевых экранов, маршрутизацией и другими компонентами инфраструктуры.

3.9.2.13. Неверный пароль при доступе из web-интерфейса ALD Pro

В случае, когда web-интерфейсе ALD Pro неверно указано пароль пользователя, под которым происходит подключение к LDAP MS AD, в файле `syncer_watcher.log` будет ошибка:

```
2025-07-02 12:17:40 syncer DEBUG     provider   Подключение к LDAP источник
2025-07-02 12:17:40 syncer DEBUG     strategy   Попытка подключения к windc1.
↪corp.test
2025-07-02 12:17:40 syncer ERROR     strategy   {'desc': 'Invalid credentials
↪', 'info': '80090308: LdapErr: DSID-0C09042A, comment:
↪AcceptSecurityContext error, data 52e, v3839'}
2025-07-02 12:17:40 syncer ERROR     strategy   {'desc': 'Invalid credentials
↪', 'info': '80090308: LdapErr: DSID-0C09042A, comment:
↪AcceptSecurityContext error, data 52e, v3839'}
syncer ERROR     run   Не удалось подключиться к хосту=windc1.corp.test.
↪Протокол LDAP
```

Решение: Проверить правильность ввода пароля.

3.9.2.14. Проблемы с синхронизацией пароля новых пользователей MS AD

При первой попытке синхронизации пароля пользователя из Microsoft Active Directory в ALD Pro может возникать при условиях:

- данный пользователь только что создан в MS AD;
- пароль пользователя ни разу не изменялся в MSAD;
- синхронизация завершилась с ошибкой.

При попытке синхронизации данных пользователя из MS AD в ALD Pro журнал работы модуля синхронизации `syncer` (файл `syncer_standalone_error.log`) содержит записи следующего вида:

```
2025-08-24 13:06:49 pwd-sync ERROR  utils  Возникло исключение во время
 ↪выполнения <function ADldap.delete_attr ...>
2025-08-24 13:06:55 pwd-sync ERROR  processors  Ошибка NO_SUCH_ATTRIBUTE,
 ↪текст ошибки {'desc': 'No such attribute', 'info': '00002076: AtrErr: DSID-
 ↪030F194C, ... (userParameters)'}
Traceback (most recent call last):
  ...
ldap.NO_SUCH_ATTRIBUTE: {'desc': 'No such attribute', 'info': '00002076:
 ↪AtrErr: DSID-030F194C, ... Att 9008a (userParameters)'}
```

Причина:

У новых пользователей MS AD, для которых пароль ещё ни разу не был изменён, отсутствует ряд служебных атрибутов (например, `userParameters` и `whenChanged`). При первой синхронизации из ALD PRO модуль `syncer` пытается работать с этими атрибутами, и каталог возвращает ошибку `NO_SUCH_ATTRIBUTE`. В результате синхронизация пароля не выполняется.

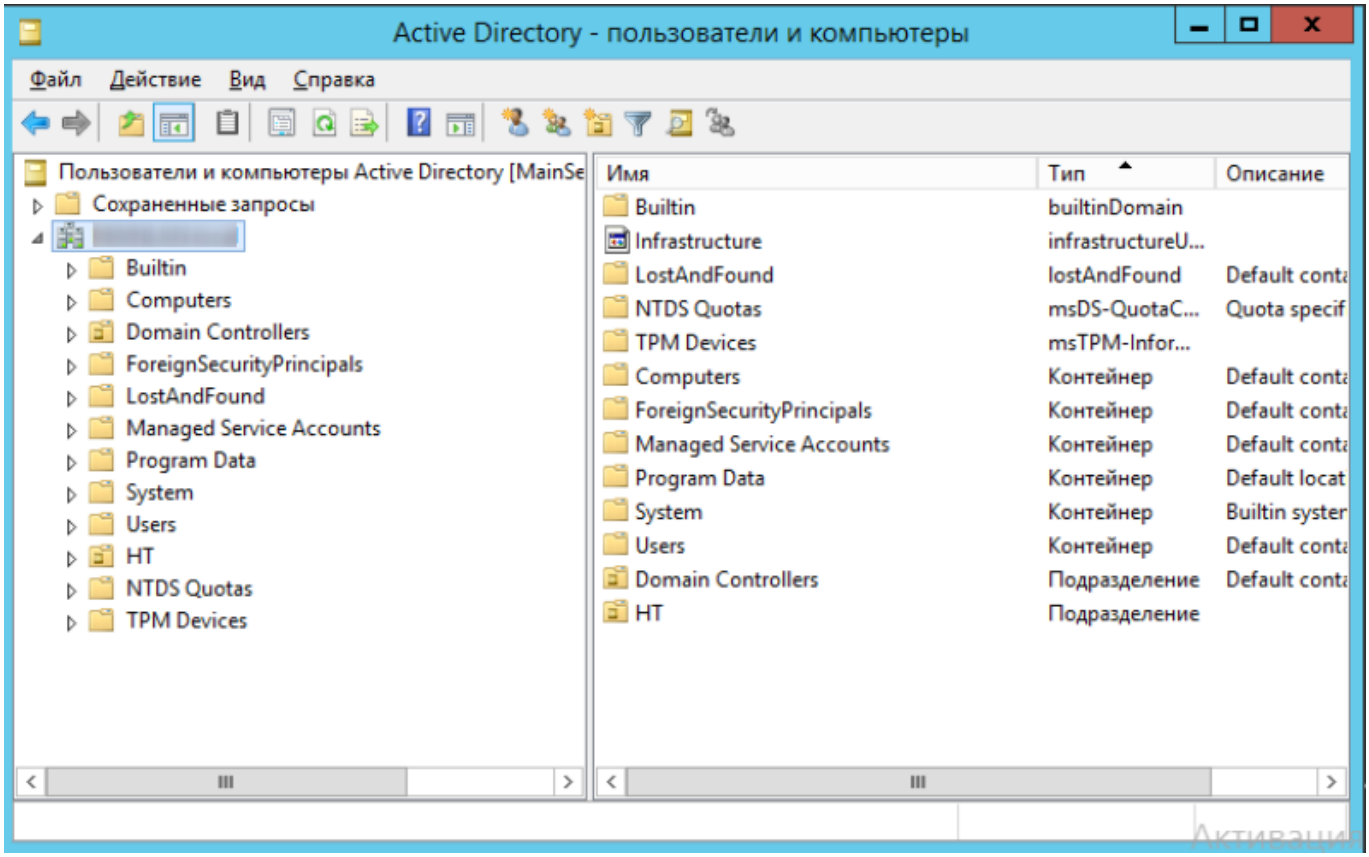
Решение:

Для всех новых пользователей, созданных в MS AD, необходимо **однократно сменить пароль** (достаточно через стандартные средства Windows или административные утилиты). После этого в каталоге будут установлены значения атрибутов (в том числе `whenChanged`), и последующая синхронизация паролей из ALD PRO в MS AD будет выполняться без ошибок.

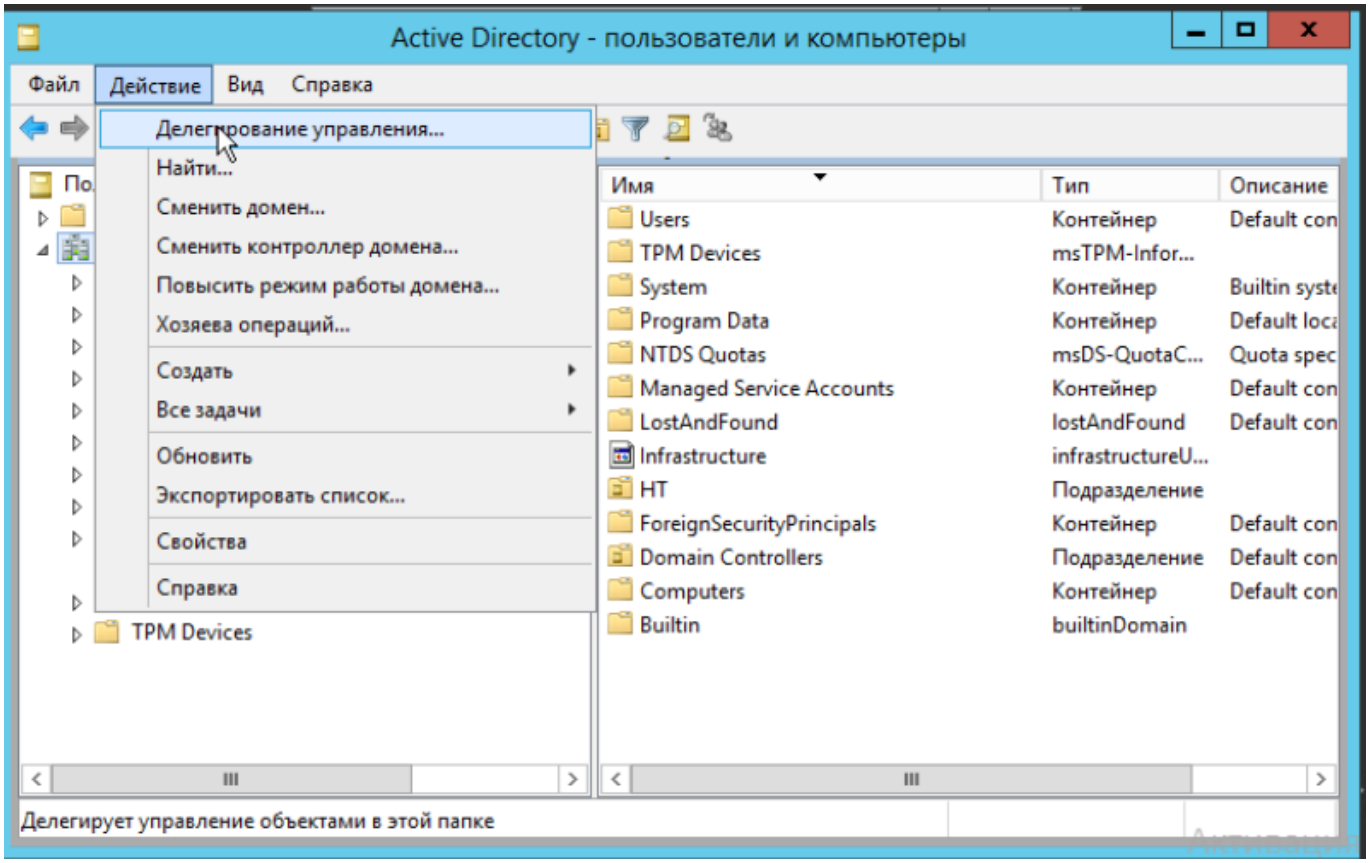
3.9.3. Инструкция по выдаче ограниченных прав на управление паролями пользователей в домене MS AD

Для работы модуля синхронизации учетная запись домена MS AD, под которой устанавливаются отношения синхронизации, должна обладать правами на управление паролями пользователей, которые, по умолчанию, имеются у администраторов домена. В случае невозможности или нежелательности работы модуля синхронизации под учетной записью администратора домена допускается выдача ограниченных прав на учетную запись. Для этого:

1. На контроллере домена MS AD необходимо запустить оснастку “Active Directory - пользователи и компьютеры”.

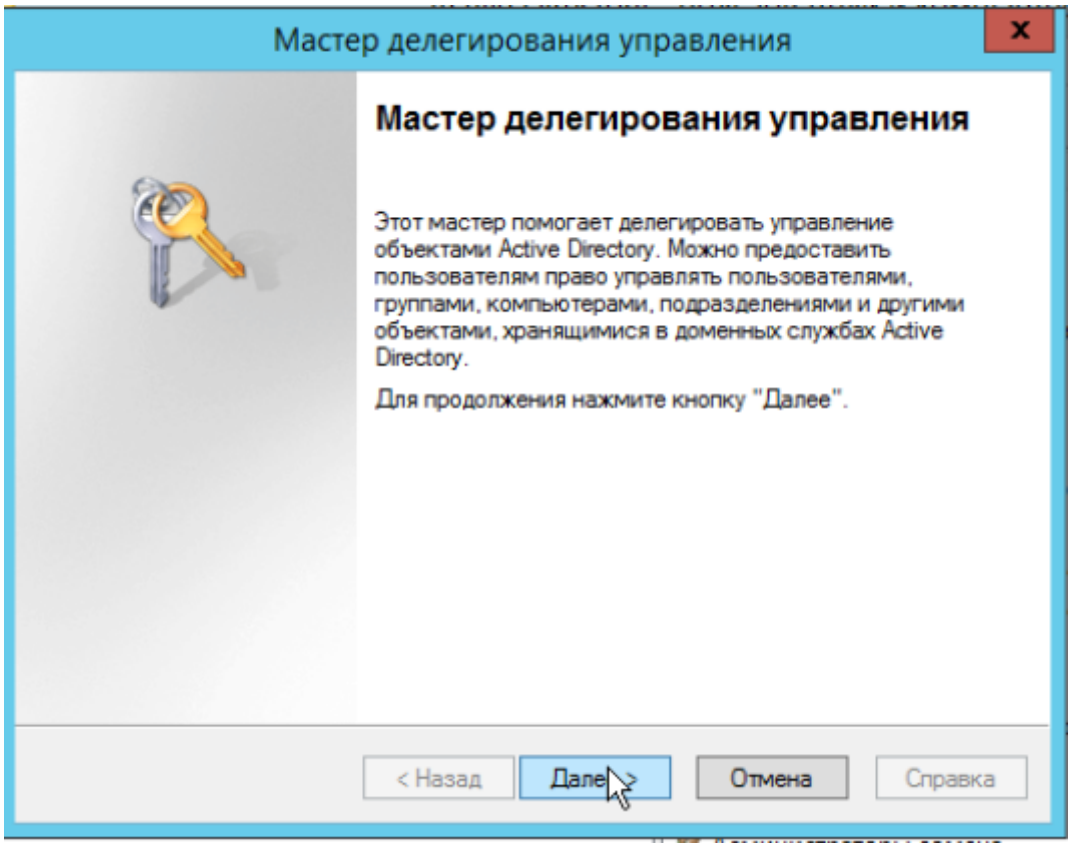


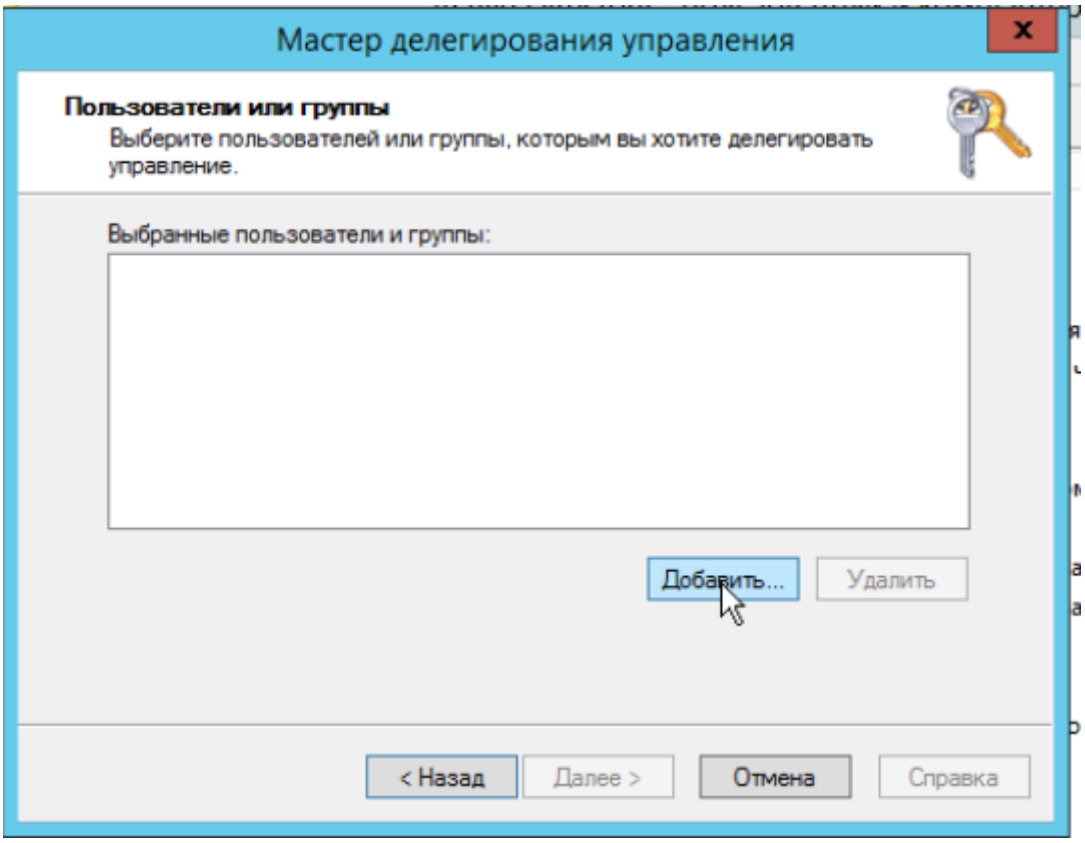
2. Выбрать OU корень домена и открыть “Делегирование управления”.

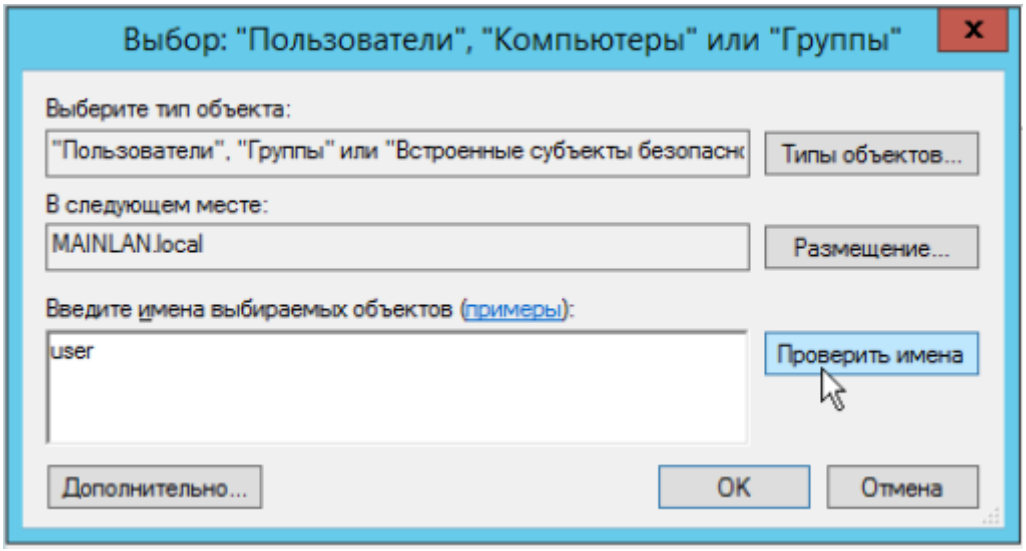


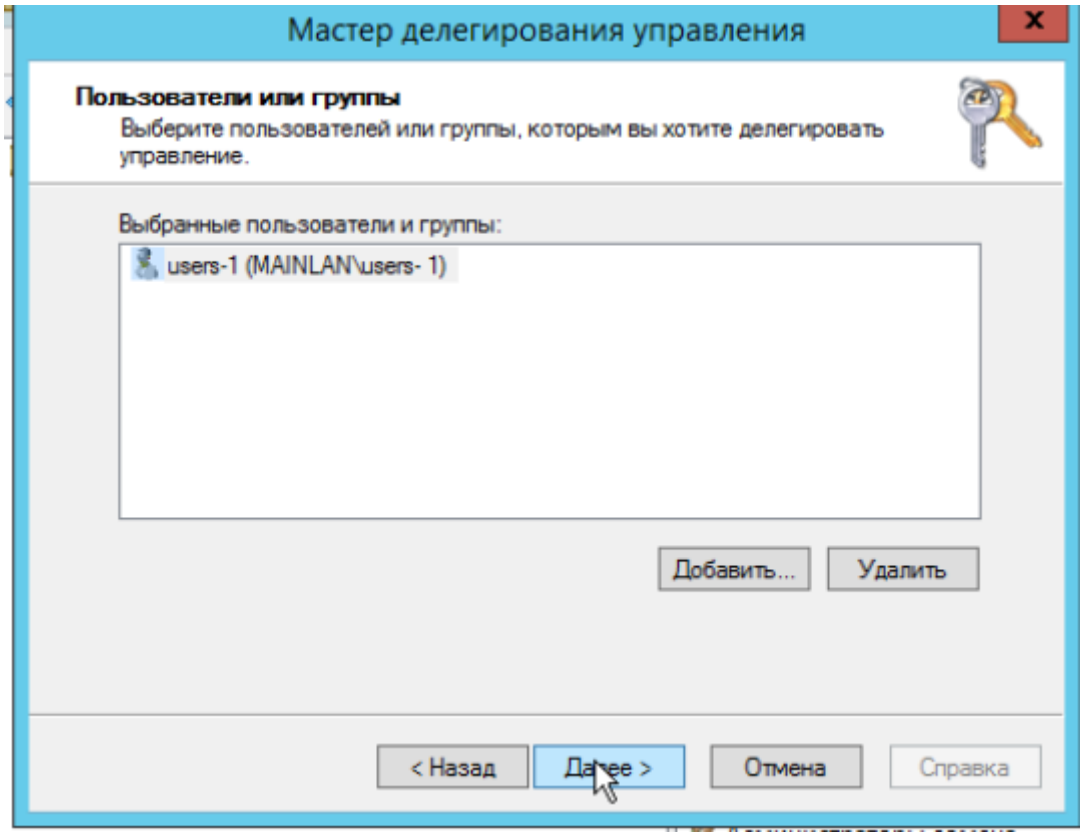
3. В открывшемся окне “Мастер делегирования управления”, после нажатия кнопки

[Далее] необходимо указать учетную запись пользователя, которой выдаются права.

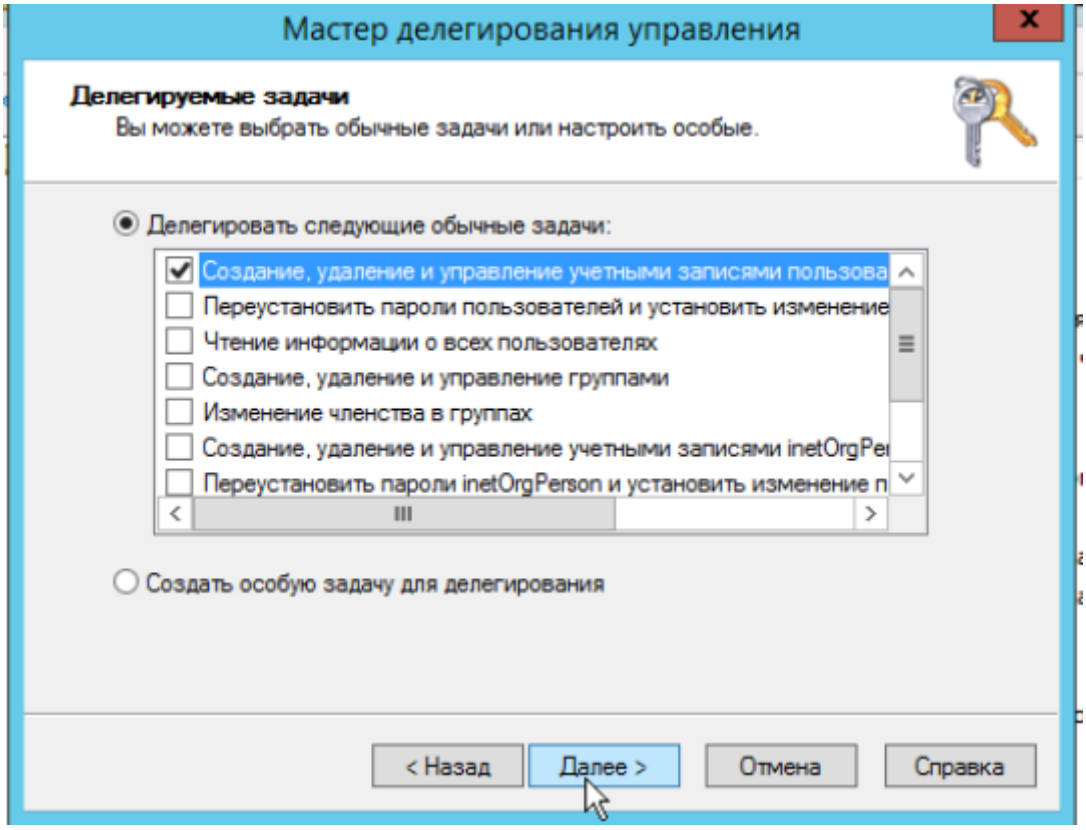




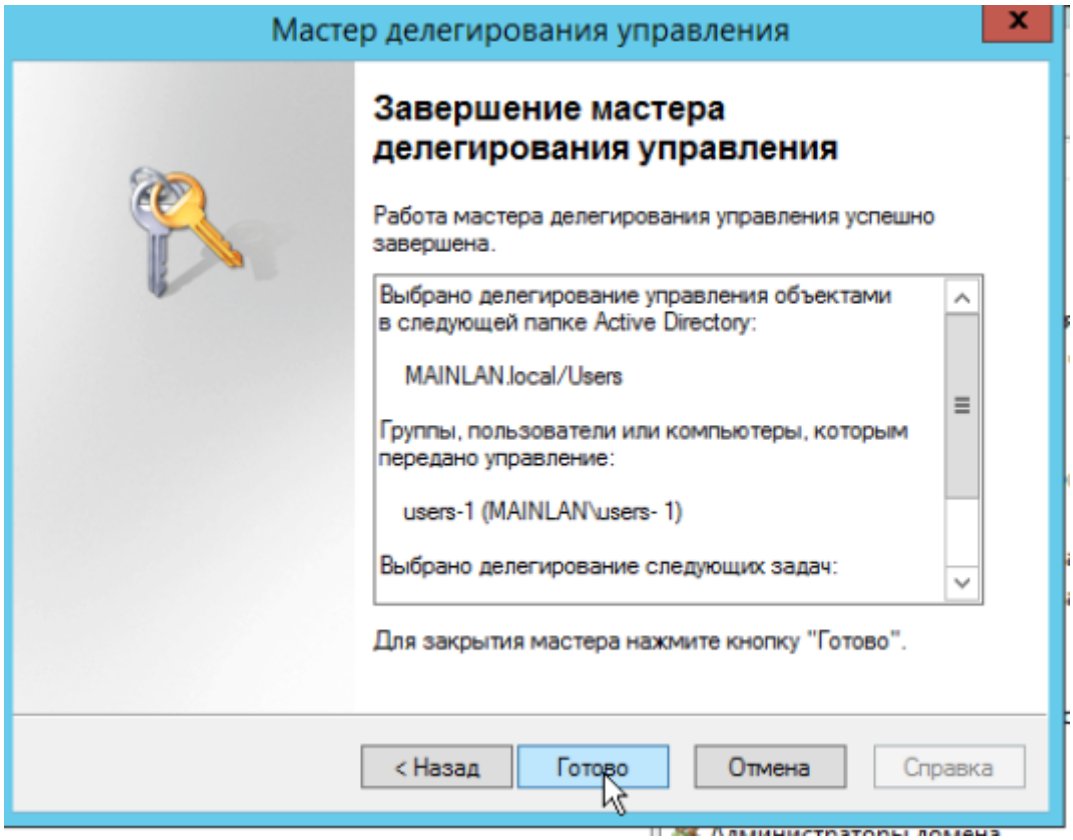




4. Выбрать права для делегирования: Создание, удаление и управление учетными записями пользователей.



5. Нажать кнопку [Готово].



Права выданы.

Примечание: В зависимости от версии домена MS AD набор делегируемых задач может отличаться.

3.9.4. Инструкция по обновлению ALD Pro до версии 2.4.0 и более поздних с ранее установленным модулем синхронизации

3.9.4.1. Общая информация

При обновлении контроллера домена **ALD Pro** до версии 2.4.0 и более поздних, с ранее установленным модулем синхронизации, процесс миграции базы данных может занять продолжительное время. Если база данных содержит 30000 пользователей и более, то рекомендуется сначала обновить **ALD Pro**, затем выбрав отдельный интервал профилактики обновить модуль синхронизации, согласно этой инструкции.

3.9.4.2. Проверка и подготовка состояния синхронизации

Перед началом обновления необходимо убедиться в отсутствии ошибок в работе модуля синхронизации. Если ошибки синхронизации присутствуют, их необходимо устранить до начала обновления, чтобы избежать проблем миграции и работы системы после обновления.

Проверить состояние служб синхронизации:

```
systemctl status syncer-loadrunner.timer
systemctl status syncer-watcher.timer
```

Проверить логи на наличие ошибок:

```
tail -n 100 /var/log/aldpro/syncer/syncer_loadrunner.log
tail -n 100 /var/log/aldpro/syncer/syncer_watcher.log
```

Также проверить журналы ошибок синхронизации паролей:

```
tail -n 100 /var/log/aldpro/syncer/pwd_sync/standalone_error.log
```

Если в логах обнаружены ошибки (например, *CRITICAL* или *ERROR* связанные с

синхронизацией пользователей и групп), необходимо их устранить до начала обновления. В случае, если устранить ошибки самостоятельно невозможно — рекомендуется обратиться в техническую поддержку.

3.9.4.3. Предварительный этап

Делается резервная копия базы данных модуля синхронизации в отдельную директорию (выбрать в соответствии с инфраструктурой):

```
mkdir /srv/pg_backup && chown postgres:postgres /srv/pg_backup/
sudo -i -u postgres
$ pg_dump -d  syncer -F d -f /srv/pg_backup/syncer_$(date +%Y%m%d-%H%M)
$ du -sh /srv/pg_backup/syncer_20240913-0938/
520K        /srv/pg_backup/syncer_20240913-0938/
```

Проверить, что модуль синхронизации установлен, и запретить обновлять его пакеты (на примере ранее установленной версии ALD Pro 2.3.0):

```
apt list --installed | grep -E 'aldpro(.*)sync'
aldpro-mp-ui-syncer/1.7_x86-64,now 2.3.0-22 amd64 [установлен, автоматически]
aldpro-syncer/1.7_x86-64,now 2.3.0-31 amd64 [установлен]
apt-mark hold aldpro-syncer aldpro-mp-ui-syncer
```

3.9.4.4. Обновление ALD Pro до новой версии

Обновить source.list и пакеты на контроллере домена с установленным модулем обновления.

```
sudo apt dist-upgrade -y -o Dpkg::Options::=--force-confnew
sudo aldpro-server-install --update --domain <domain> --host <hostname> --ip
 ↪<ip> --setup_syncer [--setup_gc]
```

Внимание: Параметр `--setup_gc` необходим только в случае ранее установленного модуля глобального каталога на данном контроллере домена.

3.9.4.5. Обновление модуля синхронизации

После основного этапа обновления **ALD Pro** и проверки работоспособности можно переходить к обновлению модуля синхронизации.

Снять удержание с пакетов:

```
sudo apt-mark unhold aldpro-syncer aldpro-mp-ui-syncer
```

Обновить пакеты и завершить обновление **ALD Pro**:

```
sudo apt dist-upgrade -y -o Dpkg::Options::=--force-confnew
sudo aldpro-server-install --update --domain <domain> --host <hostname> --ip
↪<ip> --setup_syncer [--setup_gc]
```

После завершения обновления, необходимо перезагрузить контроллер домена.

```
sudo reboot
```

Обновление завершено.

3.10. Суммирование политик ПО

3.10.1. Термины и определения

Термин	Определение
SaltStack	Система управления конфигурацией машин и инструмент дистанцион
Salt-master	Центральный демон Salt, которой может отдавать команды слушающи
Salt-minion	Сервер, на котором запущен демон Salt-minion, который может прослу
Standalone minion	Автономно от мастера запущенный клиент на компьютере домена. Вы
Pillar	Хранилище ключ-значение для пользовательских данных, которые буд
Приоритет политики	Позволяет управлять очередностью применения политик.

Таблица 3.12 – пр

Термин	Определение
Сервер службы каталогов	Сервер, хранящий и передающий важную конфиденциальную информ
LDAP-протокол	Протокол прикладного уровня для доступа к службе каталогов.
Фильтр политики ПО	Выборка определенных компьютеров и/или групп компьютеров.
Портал управления	Графический web-интерфейс, предоставляющий привилегированному
Политика ПО	Набор правил, позволяющих устанавливать, настраивать и обновлять

3.10.2. Назначение политик ПО на подразделение

Для работы с политиками ПО у пользователя должны быть соответствующие права. Для 2.2.0 это ALDPRO - Main Administrator и ALDPRO - IT Specialist. Начиная с версии 2.4.0 это может быть набор привилегий (подробнее см. Роли и права доступа). Перед назначением политики ПО на подразделения, подготовьте программное обеспечение (см. Каталог ПО) и создайте политику ПО (см. Создание политики ПО).

Важно: Политики ПО доступны для работы только клиентам с **ОС ALSE**.

Для назначения политик ПО (подробнее см. Подразделения) перейти: **Установка и обновление ПО** → **Политики ПО** → **{Имя политики}** → **Вкладка “Подразделения”**. На вкладке выбрать **+ Добавить подразделение**, на которое будет назначена политика ПО. Или сделать аналогичные действия в карточке подразделения: **Пользователи и компьютеры** → **Организационная структура** → **{Имя подразделения}** → **Вкладка Политики ПО**. На вкладке выбрать **+ Назначить политику ПО**.

Есть 2 способа назначить политику ПО:

- На подразделение. Для этого выберите любое подразделение. В этом случае политика ПО применяется ко всем компьютерам подразделения.
- На корневое подразделение с указанием компьютера или группы компьютеров. Для этого в выпадающем списке выберите корневое подразделение. Вам станут доступны блоки выбора компьютеров и групп компьютеров. В блоке “Все компьютеры” и/или “Все группы” укажите соответствующие компьютеры и/или группы

компьютеров для применения политики ПО. Данная функция предусмотрена исключительно для корневого подразделения.

На вкладке **Установка и обновление ПО → Политики ПО → {Имя политики} → Вкладка “Подразделения”** приведен список подразделений, к которым применяется данная политика ПО, с указанием приоритета политики ПО (см. Политики ПО).

3.10.2.1. Версионность

Каждая политика ПО имеет версию, которая автоматически изменяется, если наступило одно из следующих событий:

1. Внесены любые изменения в политику ПО. В этом случае дата изменений - это дата, когда пользователь внес изменения. А автор - это ФИО пользователя, внесшего изменения.

2. Произошло обновление системы. В этом случае дата изменений - это дата обновления системы. А автора изменений - **Системное обновление**.

3. Внесены изменения в ПО, которое есть в составе политики. В этом случае дата изменений - дата внесения изменений в конкретном ПО (изменения в каталоге ПО). А автор - это ФИО пользователя, внесшего изменения в ПО.

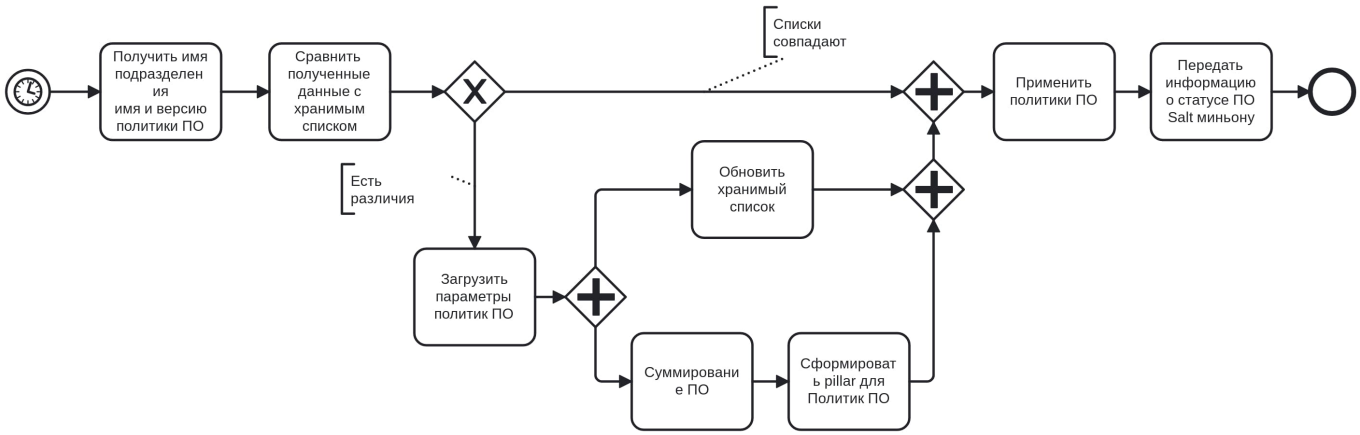
3.10.3. Описание принципов суммирования политики ПО

3.10.3.1. Область действия политики ПО

Область действия политики ПО определяется этапом назначения на подразделение. Это могут быть:

- Все компьютеры в рамках выбранного подразделения, но группы компьютеров, входящие в подразделение, не учитываются. Стоит учесть, что корневое подразделение - главное подразделение домена, в которое входят все компьютеры, поэтому политики ПО, назначенные на корневое подразделение, назначаются всем компьютерам домена.
- Определенные компьютеры и/или группы компьютеров. При назначении на группу компьютеров, политика ПО так же применяется и ко вложенным группам (см. Как назначаются политики ПО).

3.10.3.2. Порядок формирования pillar политик ПО



Для получения данных политик ПО и их применения на компьютере используется pull-модель. Инициатором работы является ALD Pro Salt миньон (standalone minion), установленный на каждом компьютере домена, который по протоколу LDAP к серверу службы каталогов получает актуальные данные о конкретной политике.

- ALD Pro Salt миньон (Standalone миньон) — это рабочие станции или серверы, на котором работает демон-миньон Salt, обладающий широкой функциональностью, работающий автономно от мастера. Используется для запуска заданий в системе без подключения к мастеру.

Формирование конфигураций политик ПО происходит по расписанию или принудительному вызову. По расписанию, применение политик ПО гарантированно происходит каждые 80 минут, но не чаще каждых 30 минут.

При первом запуске задания на формирование pillar Standalone миньон обращается к серверу службы каталогов и получает:

1. имена подразделения компьютера и его родительских подразделений;
2. все настройки и данные назначенных на них политики ПО.

Имена подразделений, идентификаторы политик ПО и их версии сохраняются в файлах `sw-assigments.json, sw-versions.json, sw-settings.json` в директории `/opt/rpta/aldpro-salt/minion`. Настройки всех назначенных политик суммируются и сохраняются в `sw-pillar.json` той же директории. Далее политики ПО применяются.

При последующих запусках, Standalone миньон обращается к серверу службы каталогов с коротким запросом на получение:

1. имен подразделений связанных с компьютером или пользователем;
2. идентификаторов назначенных на них политик ПО;
3. версий этих политик.

Полученные данные миньон сравнивает со списками, сформированными ранее `sw-assigments.json, sw-versions.json`. Если изменений нет, pillar остается без изменений, политики применяются. Если данные отличаются, перед применением, Standalone миньон предварительно запрашивает у сервера службы каталогов настройки отличающихся политик ПО, которые используются для формирования нового pillar.

3.10.3.3. Порядок суммирования политик ПО

Суммирование политик происходит согласно иерархической структуре домена, последовательно, начиная с корневого подразделения, заканчивая подразделением в котором состоит компьютер. Условно, каждое подразделение можно обозначить уровнем:

- 1 уровень - корневое подразделение
-
- N уровень - родительское подразделение компьютера.

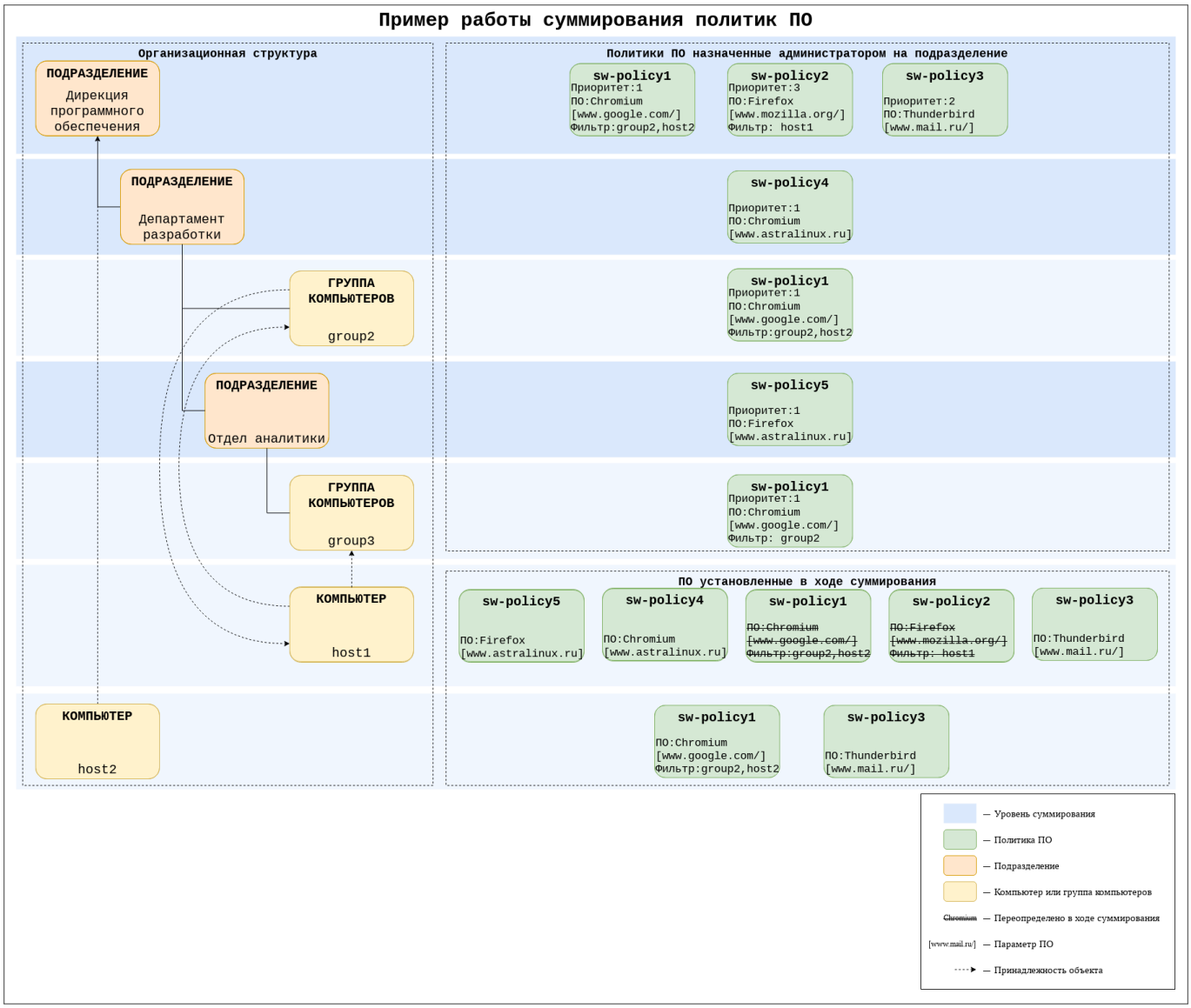
Политики ПО 1 уровня, которые применяются к компьютеру, суммируются с политиками ПО последующего уровня. Если в политиках присутствует одинаковое ПО с разными параметрами, то применяются параметры политики с приоритетом выше (наивысший приоритет 1). Если же приоритеты одинаковые, такое возможно если политики наследованы с разных подразделений, то для компьютера применяются параметры той политики, что является для данного компьютера ближайшей по структуре, поэтому одинаковые приоритеты для компьютера переопределяются, согласно иерархической структуре домена.

При возникновении конфликтов среди одинакового программного обеспечения после назначения политики ПО, то программное обеспечение, что по итогу не применилось в ходе суммирования, в карточке компьютера отображается со статусом “Переопределено”. Подробнее о статусах в разделе **Просмотр результатов применения политики**.

После суммирования, на компьютере формируется конечный pillar (см. Порядок формирования pillar политик ПО), который и задаёт основную конфигурацию устанавливаемого программного обеспечения (см. Просмотр результирующего pillar).

3.10.3.4. Схема применения ПО

Пример работы нового функционала суммирования ПО выглядит следующим образом:

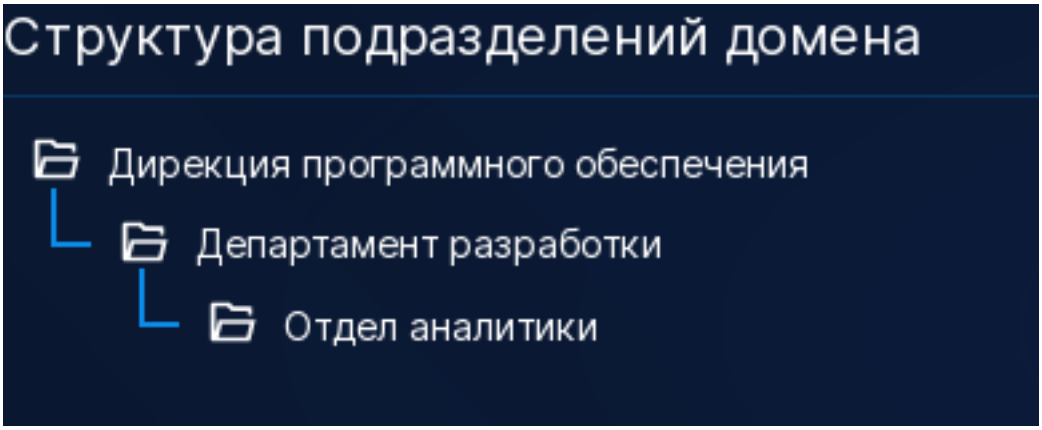


Реализация данной схемы так же представлена в портале ALD Pro (см. Пример суммирования политик ПО через портал управления).

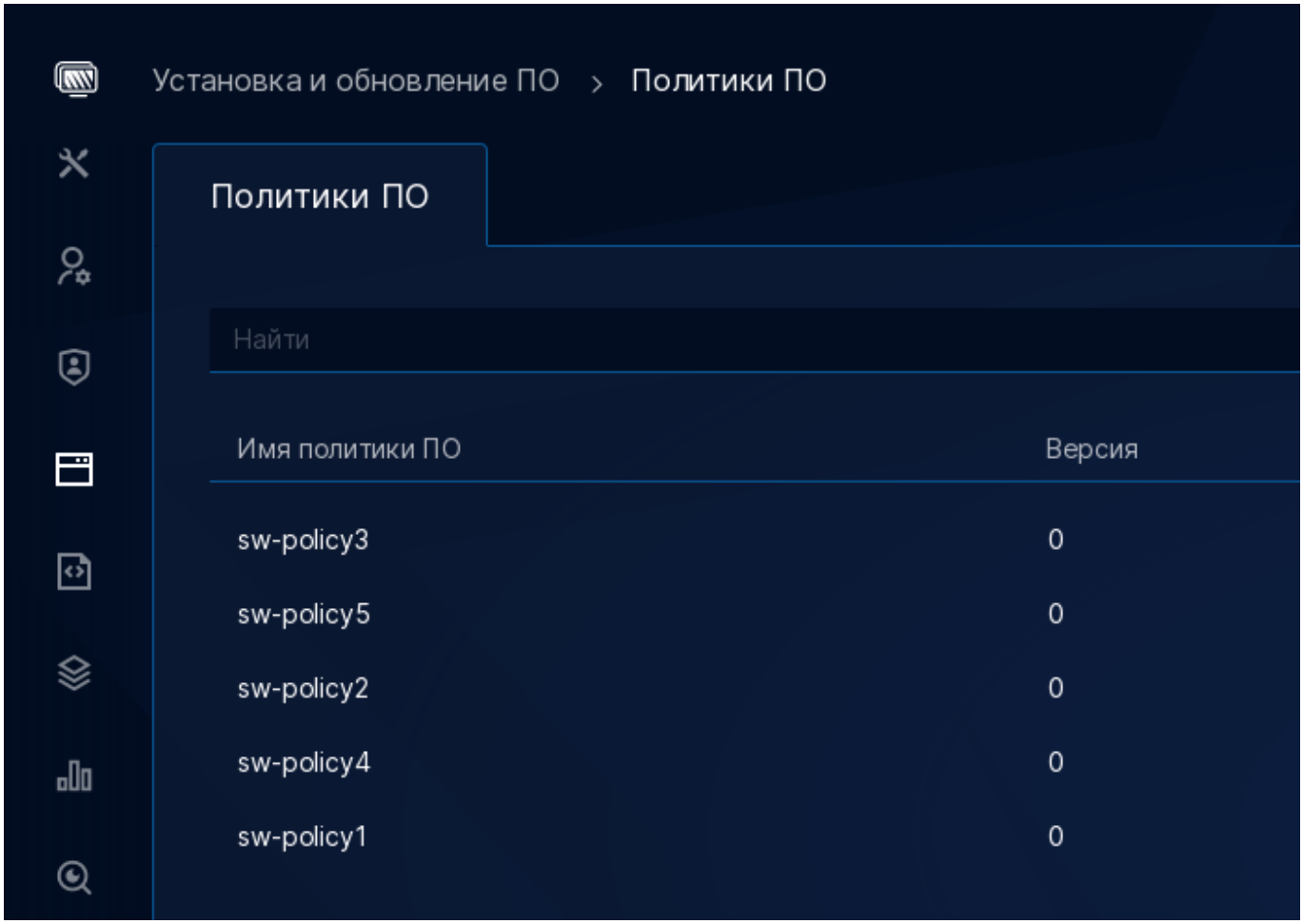
Пример суммирования политик ПО через портал управления

Для того, чтобы показать работу политик ПО в портале управления, приведем пример из схемы (см. Схема применения ПО).

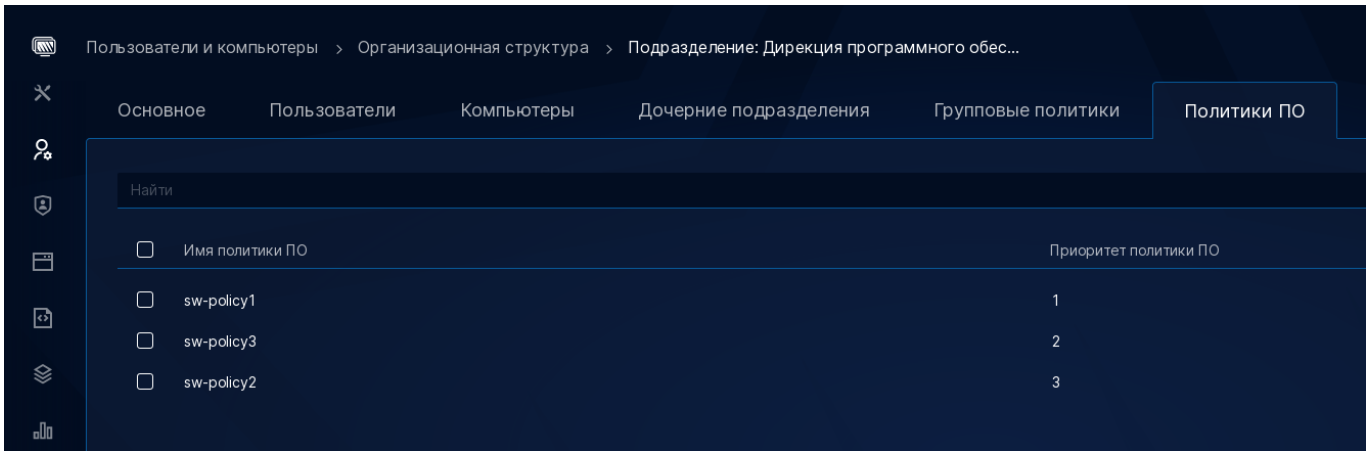
1. Создана следующая структура домена:



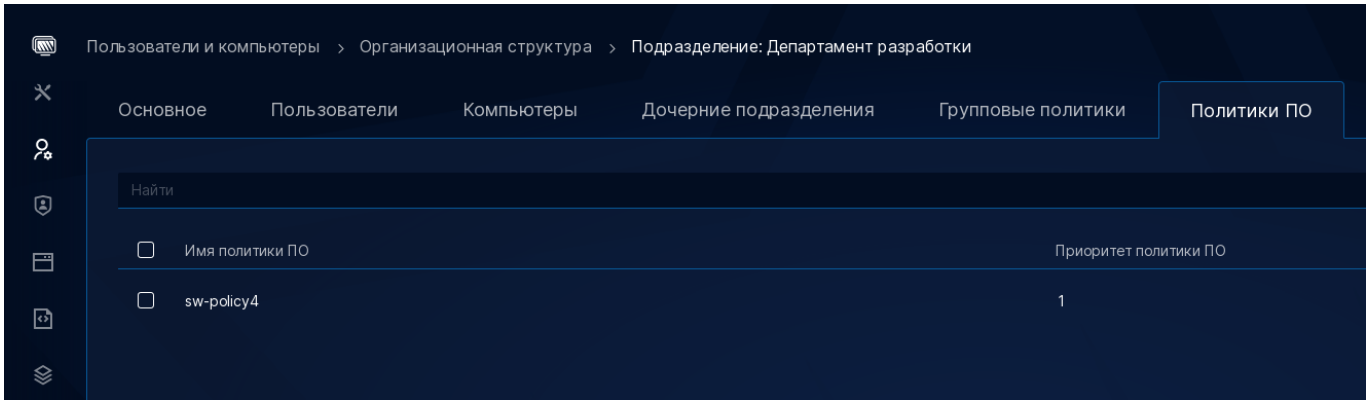
2. В системе присутствуют компьютеры “host1” и “host2”.
3. Созданы группы компьютеров: “group3”, содержащая компьютер “host1”, и “group 2”. Группы взаимно вложены. “group2” добавлена в “Департамент разработки”, “group3” в “Отдел аналитики”.
4. В подразделение “Отдел аналитики” добавлен компьютер “host1”, а в “Дирекцию программного обеспечения” компьютер “host2”.
5. Созданы политики ПО, содержащие идентичное схеме программное обеспечение и параметры:



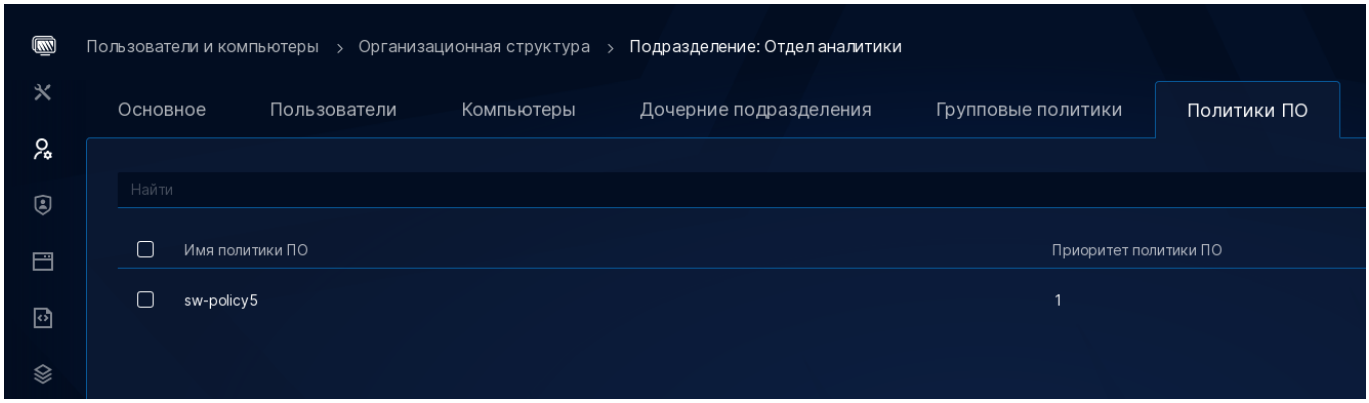
6. Политики ПО назначены на подразделения согласно схеме. Перейти: Пользователи и компьютеры → Организационная структура → Дирекция программного обеспечения. Назначенные политики ПО:



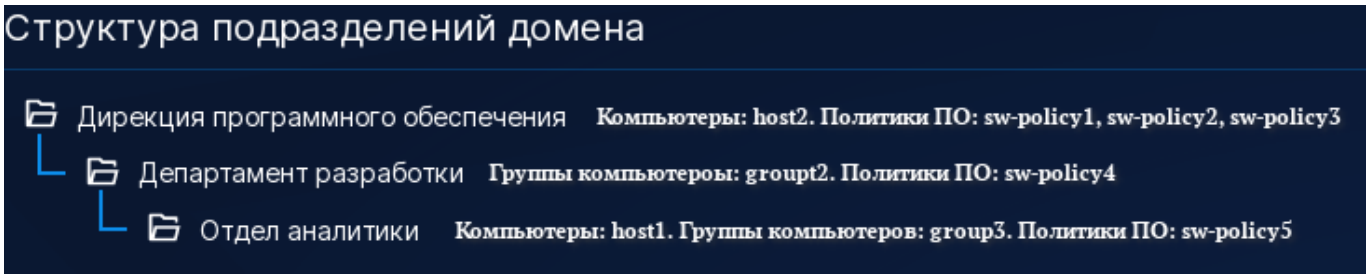
Перейти: Пользователи и компьютеры → Организационная структура → Департамент разработки. Назначенные политики ПО:



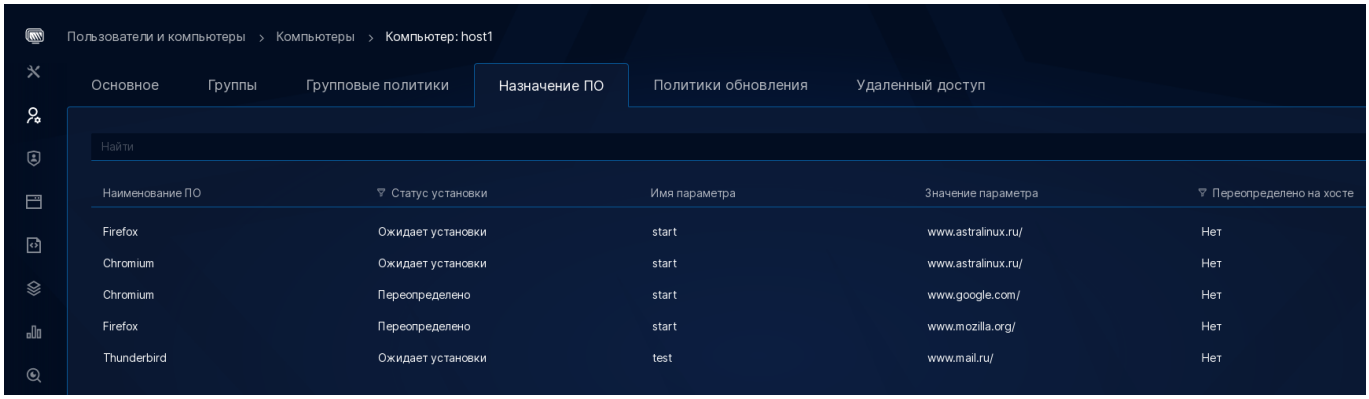
Перейти: Пользователи и компьютеры → Организационная структура → Отдел аналитики. Назначенные политики ПО:



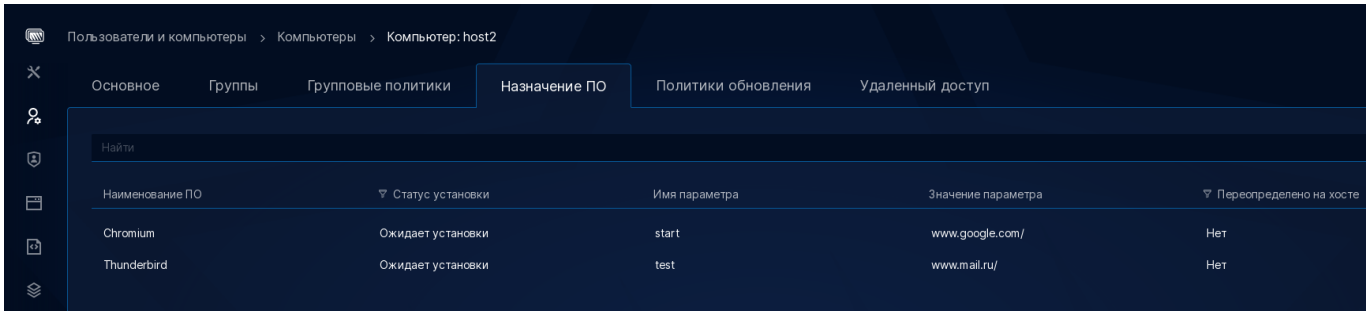
7. Не учитывая вложенность групп и точечно назначенные политики ПО, структура будет выглядеть следующим образом:



8. Перейти: **Пользователи и компьютеры → Компьютеры → host1 → Вкладка “Назначение ПО”**. Как можно увидеть, присутствует одинаковое ПО. Из него в статусе **Ожидает установки**, то программное обеспечение, что было назначено соответствующей политикой ПО на родительское подразделение компьютера, остальное отмечается как **Переопределено**:



9. Перейти: **Пользователи и компьютеры → Компьютеры → host2 → Вкладка “Назначение ПО**. Назначенное ПО определено следующим образом:



3.10.3.5. Просмотр результирующего pillar

Для просмотра назначенного программного обеспечения и его параметров на компьютере домена проверьте сформированный pillar командой:

```
aldpro-salt-call pillar.get aldpro-software
```

Вывод команды должен соответствует назначенным ПО с итоговыми параметрами (см. Просмотр результатов применения политики).

Пользователь также может посмотреть pillar с результатами суммирования в файле `/srv/aldpro-salt/roots/pillar/aldpro_po.sls`:

```
sudo cat /srv/aldpro-salt/roots/pillar/aldpro_po.sls
```

3.10.4. Отладка политик ПО

Для корректного применения назначенных политик ПО на доменном компьютере, необходимо добавить информацию о репозитории в Source list компьютера.

3.10.4.1. Применение политик по умолчанию

Применение политик ПО запускается при старте standalone minion. Пользователю доступна проверка текущего статуса работы standalone миньона:

```
Заменить на systemctl status aldpro-salt-minion.service
```

После старта standalone minion, начинается таймер применения Политики ПО. Просмотр таймера:

```
aldpro-salt-call schedule.show_next_fire_time build_and_run_swp
```

Система показывает примерное время, равное постоянному таймеру. Программное обеспечение установится в течение ещё 5-50 минут от указанного.

3.10.4.2. Форсированное применение ПО

Пользователь может выполнить принудительное обновление pillar и применение политик командой:

```
aldpro-salt-call state.apply gpupdate.swp pillar='{"verbose": True, "force":
↪True}'
```

Флаг pillar=“{“verbose”: True}“ нужен для получения логов выполнения заданий применения. Флаг pillar=“{“force”: True}“ используется для принудительного удаления сохранённых ранее pillar. Использовать флаг force: True рекомендуется не чаще одного раза в 10 минут, поскольку это приводит к повышенной нагрузке на контроллер домена.

Команда обновления pillar в обычном порядке и последующее выполнение политики:

```
aldpro-salt-call state.apply gpupdate.build
```

Ранее из интерфейса была возможность принудительно установить ПО на доменном

компьютере. Теперь этот функционал из портала управления недоступен. Для принудительной установки воспользуйтесь командой на доменном компьютере:

```
aldpro-salt-call state.apply policies.sw-policies
```

3.10.4.3. Редактирование времени выполнения заданий

Таймер заданий для групповых политик, политик ПО и правил аудита состоит из двух частей:

- Постоянная часть таймера в 25 минут. Минимальное время между заданиями 30 минут.
- Случайный разброс от 5 до 50 минут. Добавляется к постоянному таймеру, для снижения пиковой нагрузки на контроллер домена.

Таким образом, гарантированное время выполнение каждого задания 80 минут.

На доменном компьютере пользователь может установить собственные значения таймера в расписании, для внесения изменений нужно обладать sudo правами. В файле `/srv/aldpro-salt/config/minion.d/standalone_scheduler.conf` измените значения атрибутов `build_and_run_swp`:

- minutes - постоянный таймер;
- splay: * start - минимальное значение случайного таймера; * end - максимальное значение случайного таймера.

Выставлять значения таймера менее 10 минут нежелательно, это может привести к повышенной нагрузке и на контроллер домена, и на компьютер.

Далее в файле `/srv/aldpro-salt/roots/_modules/utils.py` на доменном компьютере внесите изменения в строчке _25_MINUTES = dt.timedelta(minutes=25), поменяв значение 25. После внесения изменений перезапустите standalone minion:

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

3.10.4.4. Просмотр результатов применения политики

Кроме моделирования результатов применения политики ПО непосредственно на компьютере, результат применения возможно увидеть в портале ALD Pro. Для просмотра назначенных политик ПО на компьютер или подразделение следует:

1. Перейти: **Пользователи и компьютеры → Компьютеры → {Имя компьютера} → Вкладка “Назначение ПО”**

Во вкладке отображается ПО, которое назначено на компьютер политиками ПО (см. Как назначаются политики ПО). Вкладка содержит следующие разделы:

Наименование ПО	Статус установки	Имя параметра	Значение параметра	Переопределено на хосте
Наименование ПО, которое содержится в назначенной на компьютер политике ПО. Задаётся в каталоге ПО, для просмотра перейти: Установка и обновление ПО → Каталог ПО.	Статус установки данного ПО на компьютере. Предусмотрено 4 значения: Успешно - Если ПО установилось успешно; Ошибка установки - Если при установке ПО возникли ошибки; Переопределено - Если есть аналогичное ПО из другой политики ниже приоритетом; Ожидает установки - ПО назначено, но не установлено.	ПО задаётся с определенными параметрами. Например, для браузеров параметр это часто «Стартовая страница», который задаёт первую страницу по умолчанию при открытии браузера.	Так как ПО задаётся с определенными параметрами, то для них определяются свои значения. В случае, например, параметра «Стартовая страница», его значение может быть «www.aldpro.ru».	Применяется для случаев изменения значения параметра. Если для данного ПО по итогу изменился параметр, «Переопределено на хосте» будет отображаться как «Да».

2. Перейти: **Пользователи и компьютеры → Подразделения → {Имя**

подразделения} → **Политики ПО**. Во вкладке отображаются политики ПО, назначенные на подразделение. Вкладка содержит следующие разделы:

Имя политики	Приоритет политики
Имя политики ПО. Задаётся при создании (см. Создание политики ПО).	Приоритет назначенной

3.11. Настройка синхронизации пользователей из ALD Pro в Keycloak

Основная настройка Keycloak подробно описана на официальном сайте Keycloak. В данной инструкции описано создание Федерации пользователей (User federation) с пользователями ALD Pro.

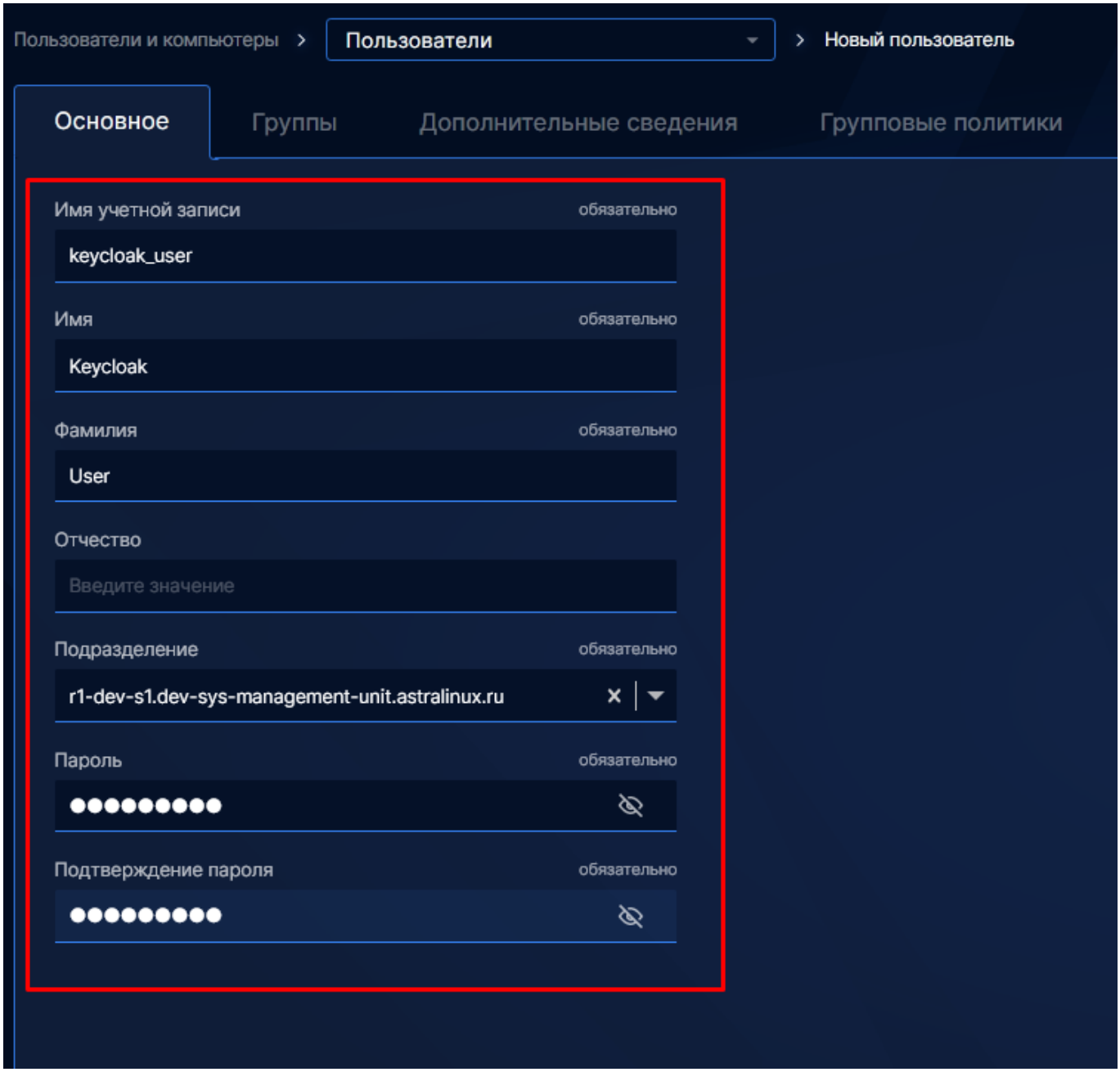
3.11.1. Термины и определения

- Федерация пользователей - синхронизация пользователей с сервером ALD Pro;
- Single Sign-On - SSO - метод аутентификации, который позволяет пользователям безопасно аутентифицироваться сразу в нескольких приложениях и сайтах, используя один набор учетных данных.

3.11.2. Предварительная настройка ALD Pro

3.11.2.1. Создание пользователя

В ALD Pro необходимо создать пользователя (рисунок 1), через которого будет осуществляться синхронизация пользователей, групп, подразделений. В целях безопасности пользователь не должен обладать правами администратора. Для синхронизации пользователей достаточно прав обычного пользователя.



3.11.2.2. Активация пользователя

Перед дальнейшей работы, следует авторизоваться под созданным пользователем и сменить ему пароль.

3.11.3. Краткая инструкция настройки Keycloak

Наименование	Значение
Hostname	astralinux.ru
URI/Port	ldap://astralinux.ru.ru:389 (_STARTTLS_) **Note**: Plaint
	ldaps://astralinux.ru:636
BaseDN	uid=_ALD_user_,cn=users,cn=_accounts_,dc=astralin
UserDN	cn=users,cn=_accounts_,dc=astralinux,dc=ru
GroupDN	ou=users,o=_YOUR_ORG_ID_,dc=jumpcloud,dc=com
Username LDAP attribute, RDN LDAP attribute	uid
UID LDAP attribute	ipaUniqueId
Search scope	One level

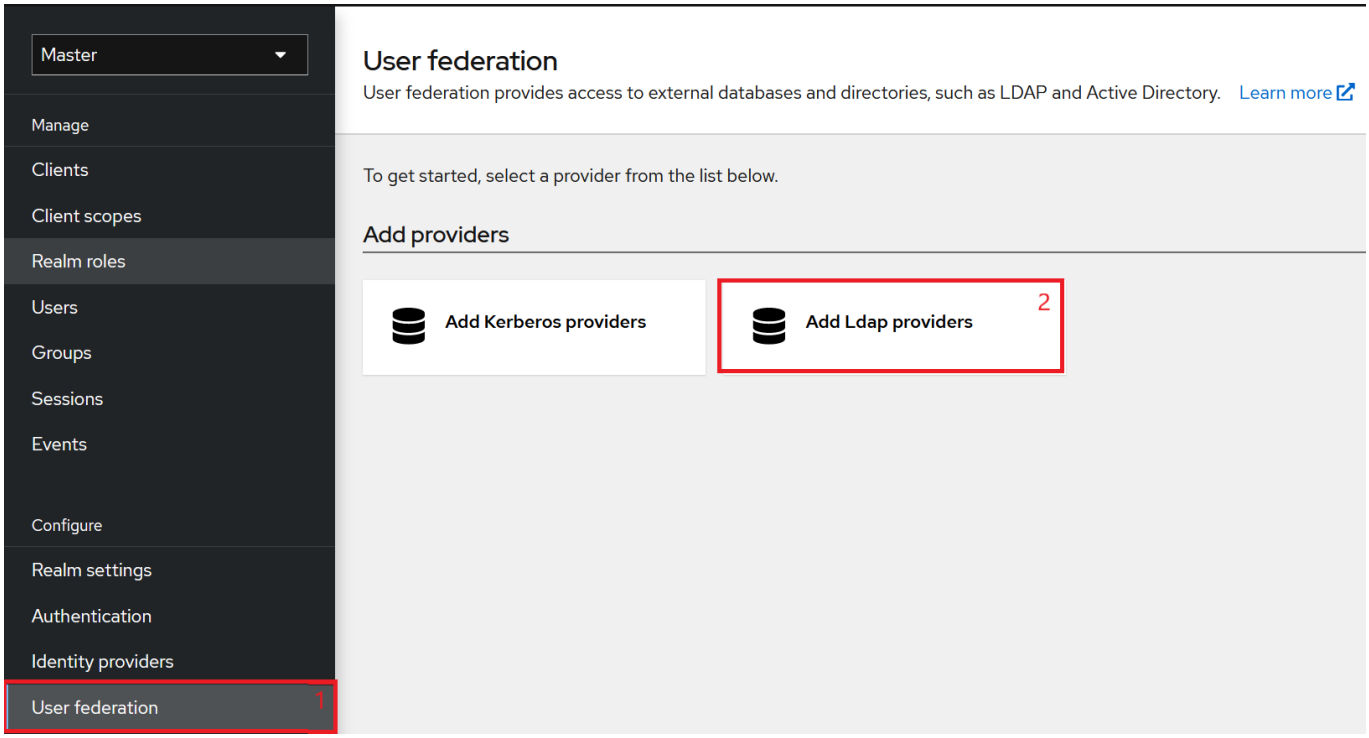
3.11.4. Подробная инструкция настройки Keycloak

Приведенная ниже инструкция актуальна для Keycloak Version 23.0.3

3.11.4.1. Создание User Federation с ALD Pro

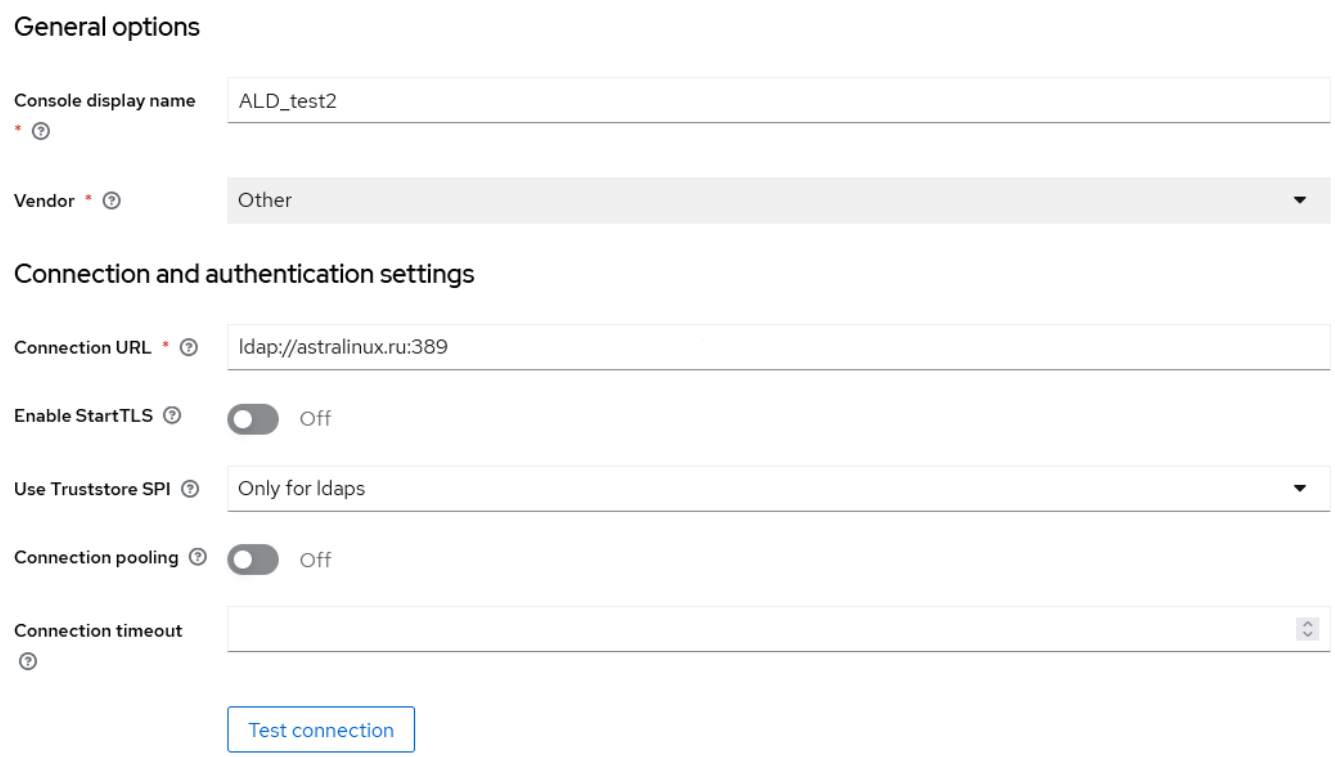
Создание User Federation

1. Выполнен вход в Keycloak с правами администратора и создан рабочий Realm.
2. На вкладке “User federation” выбран “Add Ldap providers”, во всплывающем окне выбран “LDAP” (рисунок 2).



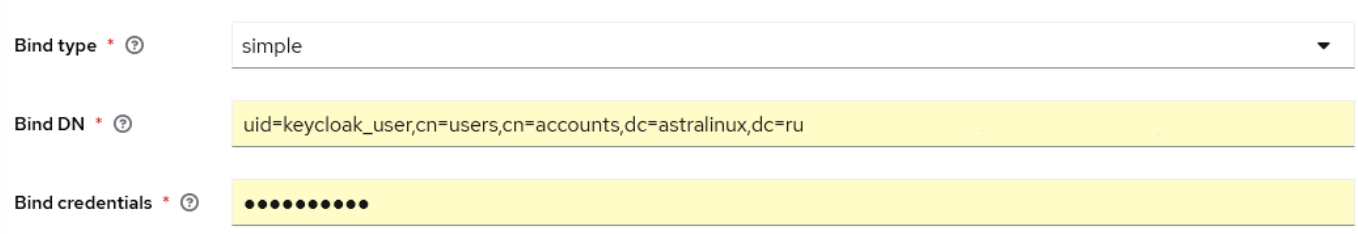
Заполнение блока General options

3. В открывшемся окне заполнены обязательные поля (рисунок 3).
4. В качестве вендора выбран “Other” или “Red Hat Directory Server”. В дальнейшем вендора для созданной федерации пользователя изменить нельзя.
5. Connection URL: URL-адрес подключения ALD Pro в формате: ldap://astralinux.ru:389
6. Остальные настройки остаются на усмотрение.



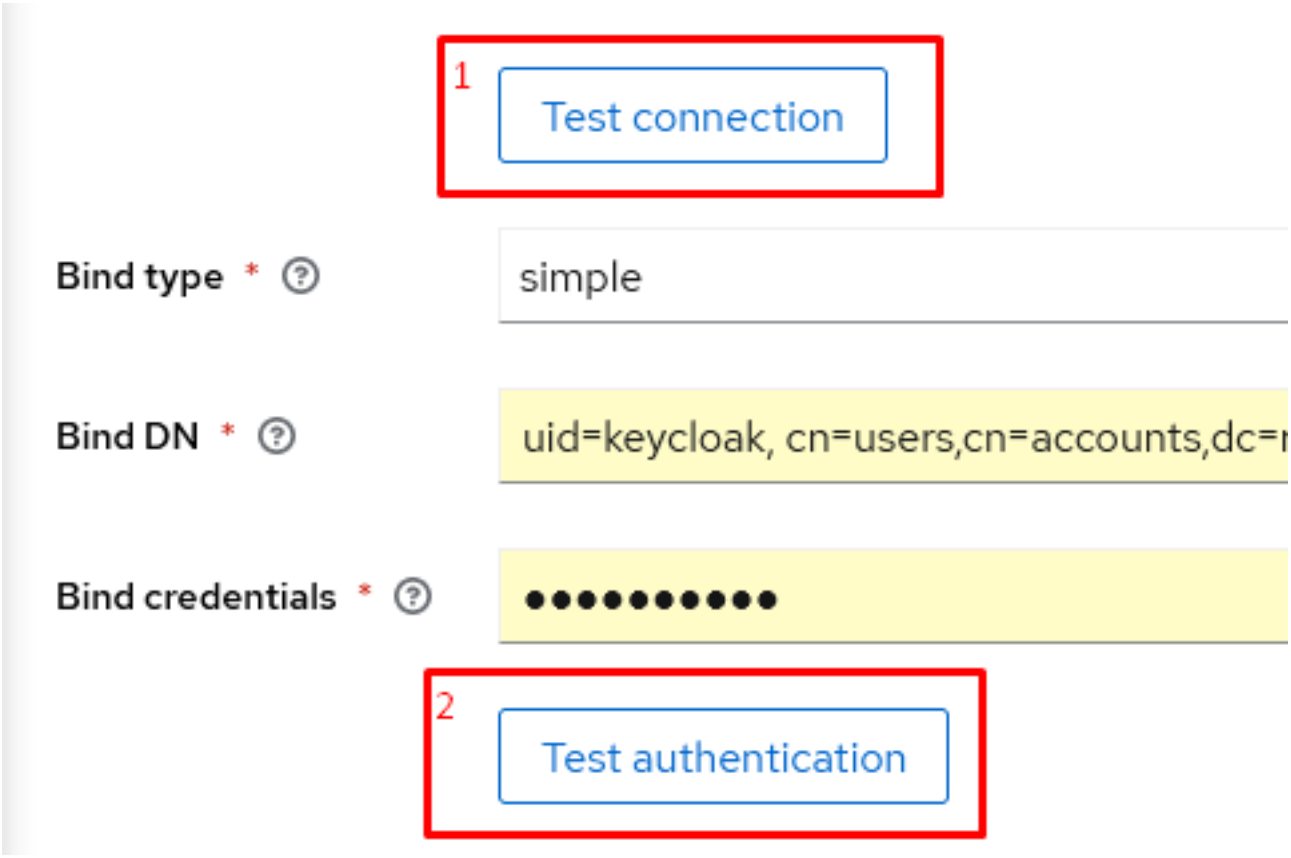
Заполнение блока Connection and authentication settings

7. Тип связи (Bind type) выбран простой (simple).
8. В “Bind DN” указан путь навигации к созданному ранее пользователю ALD Pro. DN записывается слева направо.
9. В “Bind credentials” указан пароль от привязанного пользователя ALD Pro.

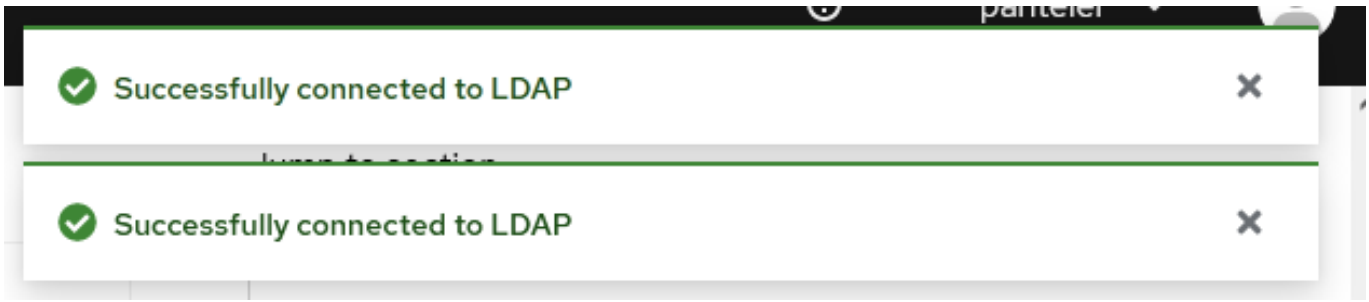


Тест соединения и аутентификации

На этом этапе можно проверить успешность заполнения форм, нажав последовательно на “Test connection” и “Test authentication” (рисунок 5).



При успешном соединении и аутентификации пользователей появятся сообщения об успешном завершении операции (рисунок 6).



Заполнение блока LDAP searching and updating

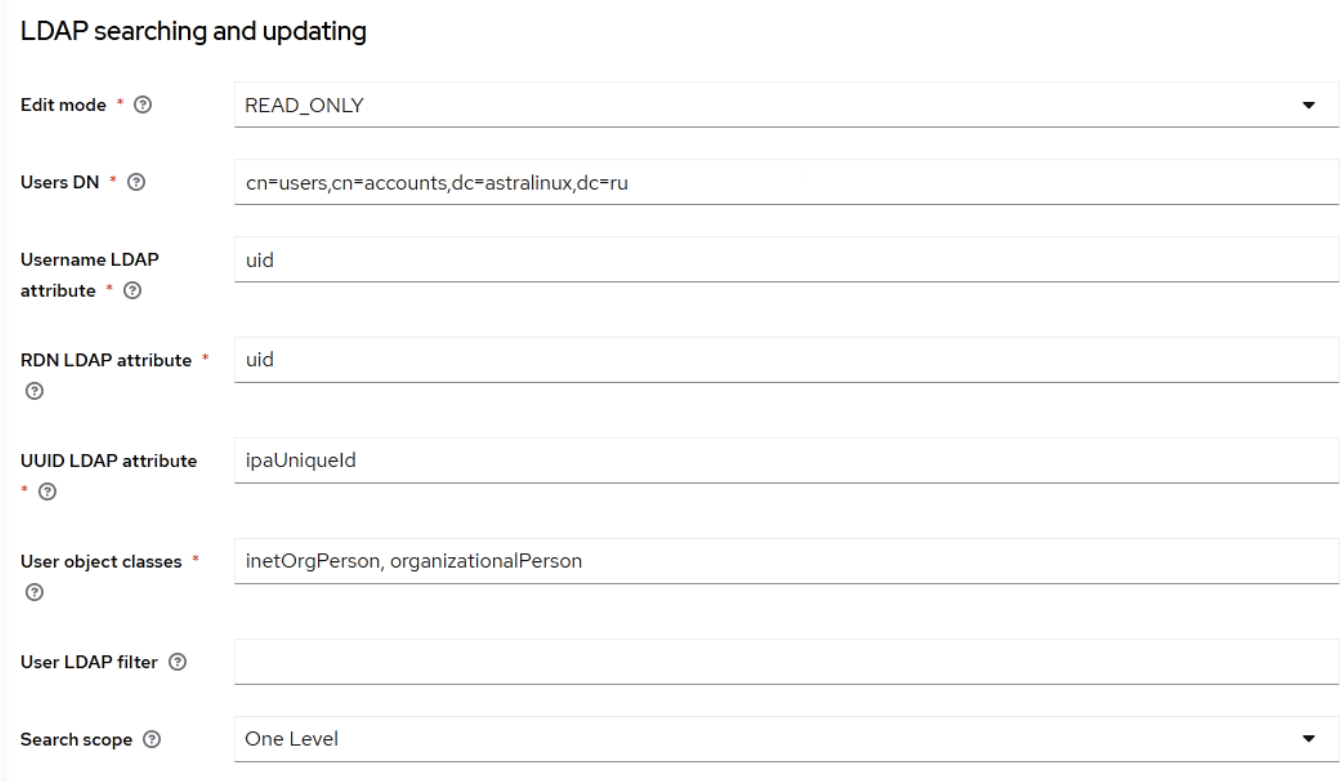
10. Режим редактирования (Edit mode) выбран “READ_ONLY”.
11. Указан путь навигации к пользователям (User DN) сервера ALD Pro.
12. Атрибуты “Username LDAP” и “RDN LDAP” - “uid”.
13. “UUID LDAP” - “ipaUniqueId”.
14. Поле “User object classes” можно оставить по умолчанию.

15. В целях безопасности каталога ALD Pro, по желанию, можно указать фильтры синхронизации для пользователей.

16. Область поиска (Search scope) для ALD Pro - “One Level”.

17. Параметры тайм-аут чтения (Read timeout) и пагинация (Pagination) - на усмотрение.

Пример заполнения на рисунке 7.

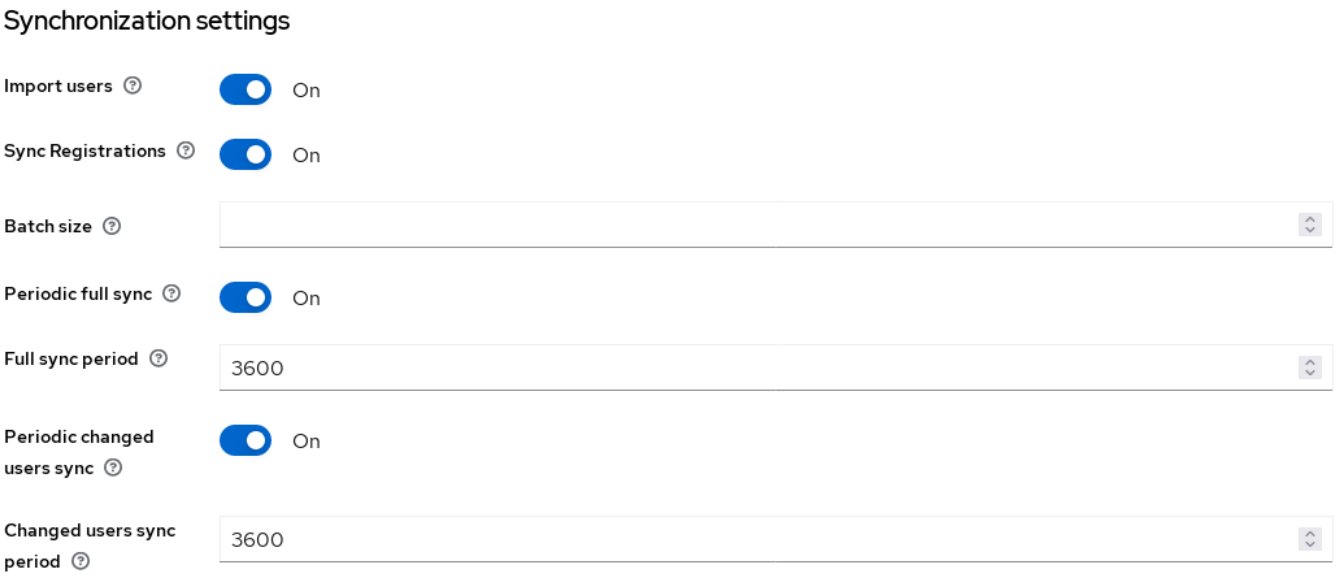


Заполнение блока Synchronization settings

18. Для настройки импорта пользователей слайдер Import users находится в положении ON.

19. Если пользователей много, рекомендуется при их импорте разбивать их на партии с помощью настройки размера партии (Batch size).

20. Для полной и периодической синхронизации пользователей рекомендуется настроить время синхронизации с помощью параметров (Periodic full sync, Periodic changed users syn). Значения указываются в секундах.

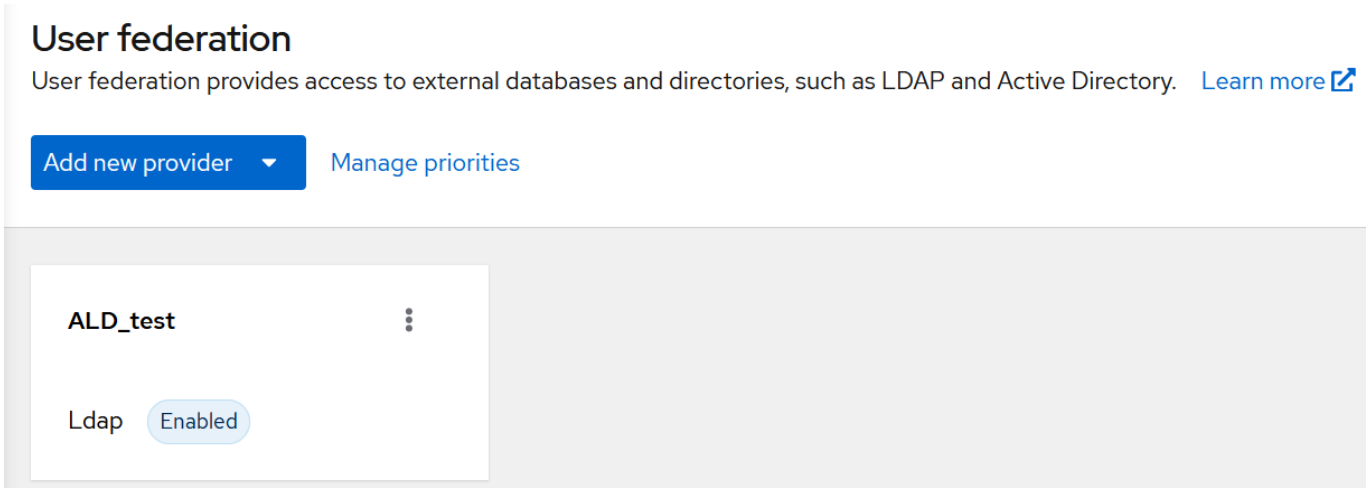


Заполнение блоков Kerberos integration, Cache settings, Advanced settings

Остальные параметры настраиваются индивидуально и позволяют гибко управлять синхронизацией и безопасностью единого входа с помощью федерации пользователей.

Проверка синхронизации пользователей

21. При завершении настроек сохранить федерацию пользователей. После сохранения федерация появится на вкладке “User federation” (рисунок 9).



22. Выполнить переход на вкладку пользователи, здесь находятся все пользователи Realm, включая пользователей федерации. Иногда в настройках Keycloak для

оптимизации работы на вкладке пользователи не отображаются пользователи федерации. Для того чтобы увидеть всех пользователей нужно в поиске ввести * и выполнить поиск.

3.11.4.2. Настройка соответствия атрибутов

Атрибуты пользователей keycloak не полностью соответствуют атрибутам ALD Pro. В таблице приведены основные соответствия атрибутов ALD Pro к Keycloak.

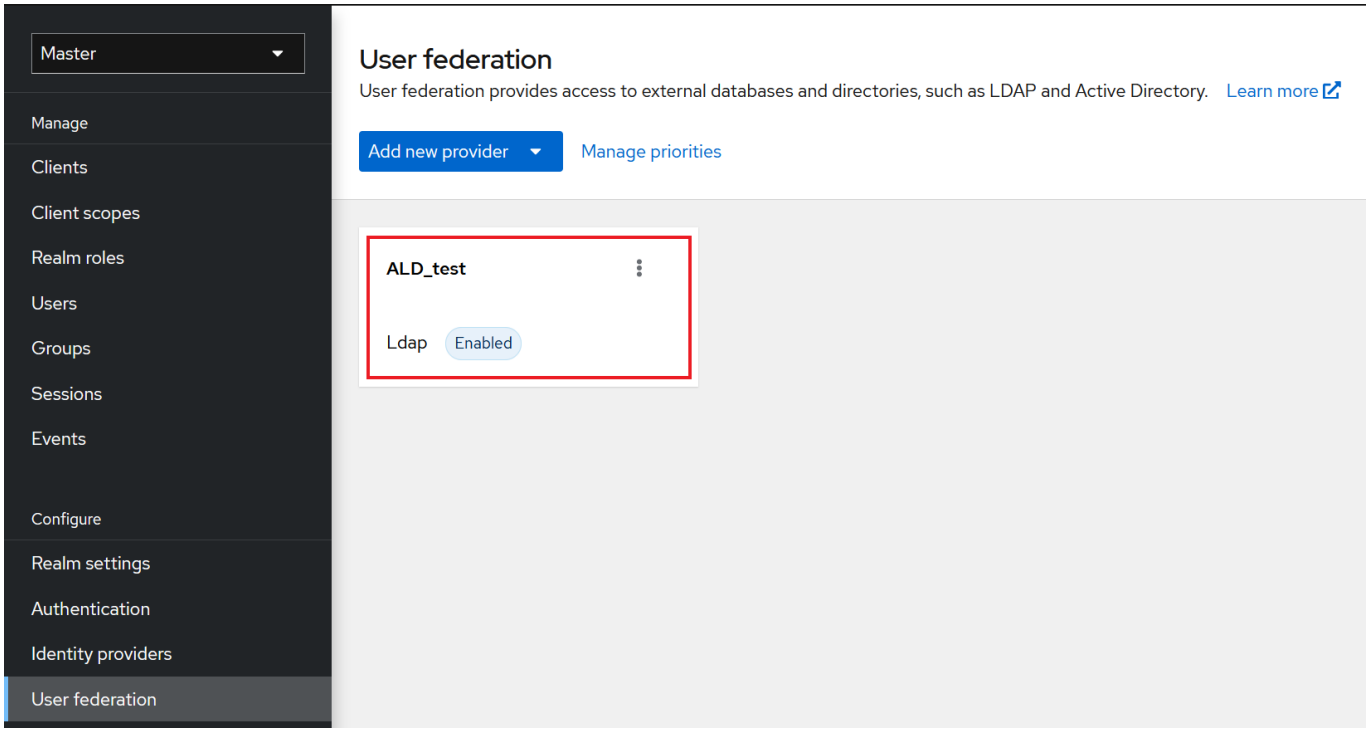
Keycloak	ALD Pro	Mapper type
email	mail	user-attribute-ldap-mapper
firstName	givenName	user-attribute-ldap-mapper

3.11.5. Синхронизация групп пользователей из ALD Pro в Keycloak

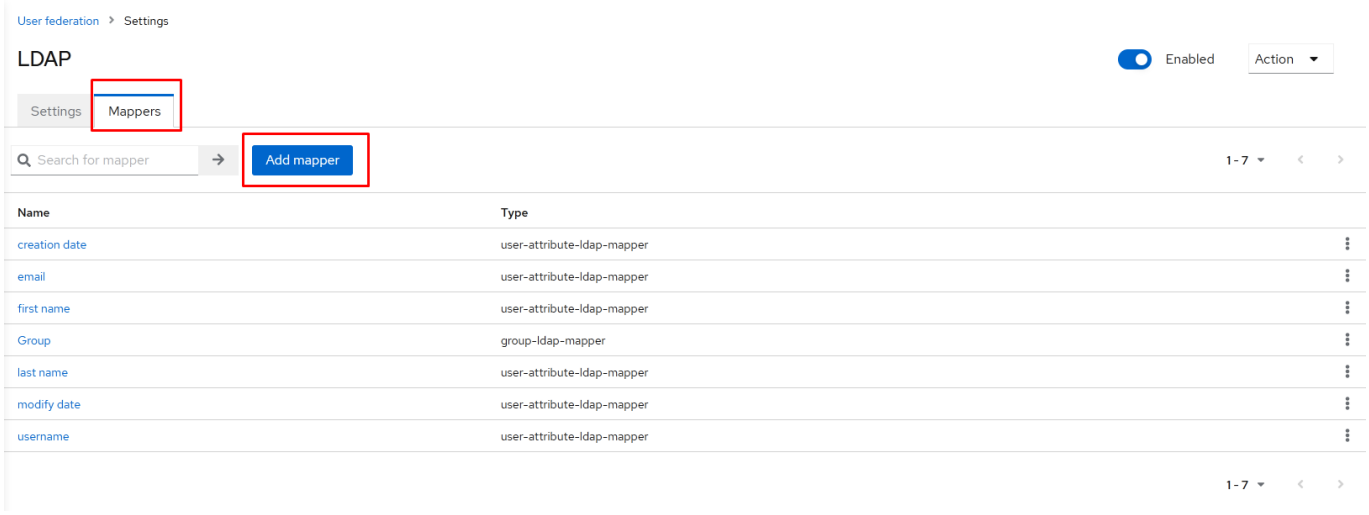
3.11.5.1. Настройка mapper в User federation

Для синхронизации пользователь должен обладать правами на чтение групп пользователей.

1. Выбрать ldap для которой нужно синхронизировать группы (рисунок 10).



2. На странице “Mappers” необходимо создать новое соответствие (рисунок 11).



3. Для создания правильного mapper необходимо заполнить следующие поля:

Поле	Значение
Name	<название mapper>
Mapper type	group-ldap-mapper

продолжение на следующей странице

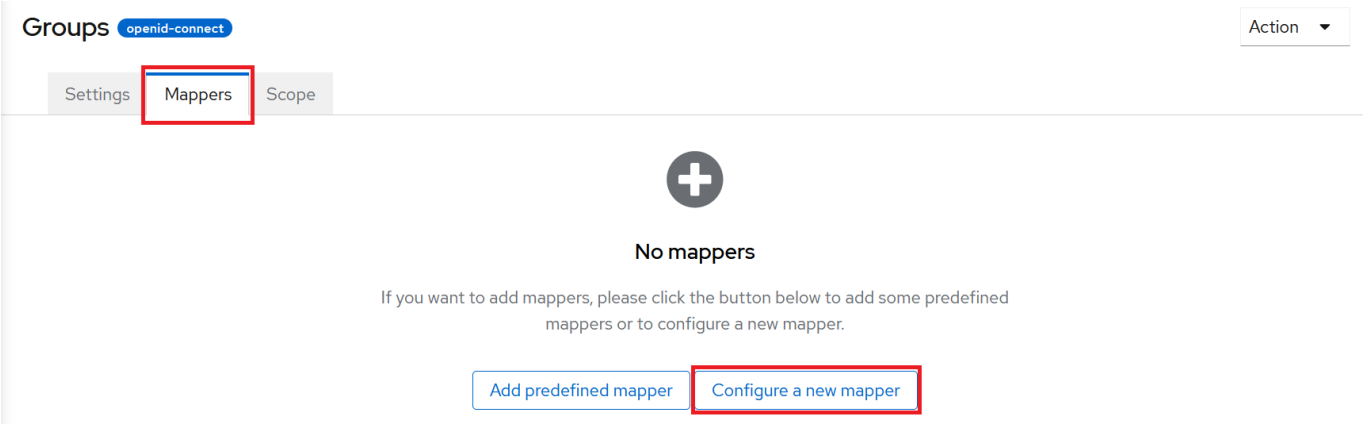
Таблица 3.17 – продолжение с предыдущей страницы

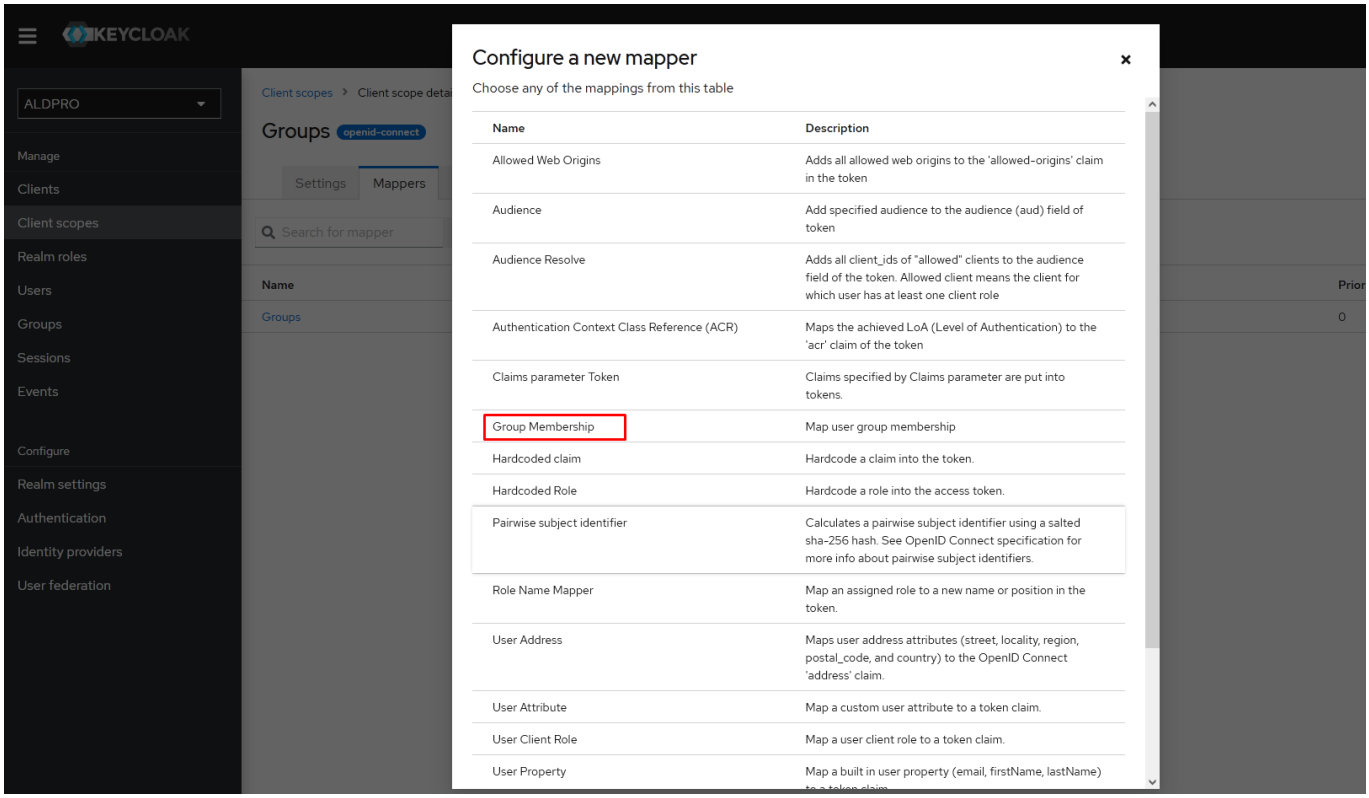
Поле	Значение
LDAP Groups DN (в соответствии с примером по созданию федерации пользователя)	cn=groups,cn=accounts,dc=astralinux,dc=ru
User Groups Retrieve Strategy	GET_GROUPS_FROM_USER_MEMBEROF_ATTRIBUTE

Остальные поля возможно оставить в значении по умолчанию.

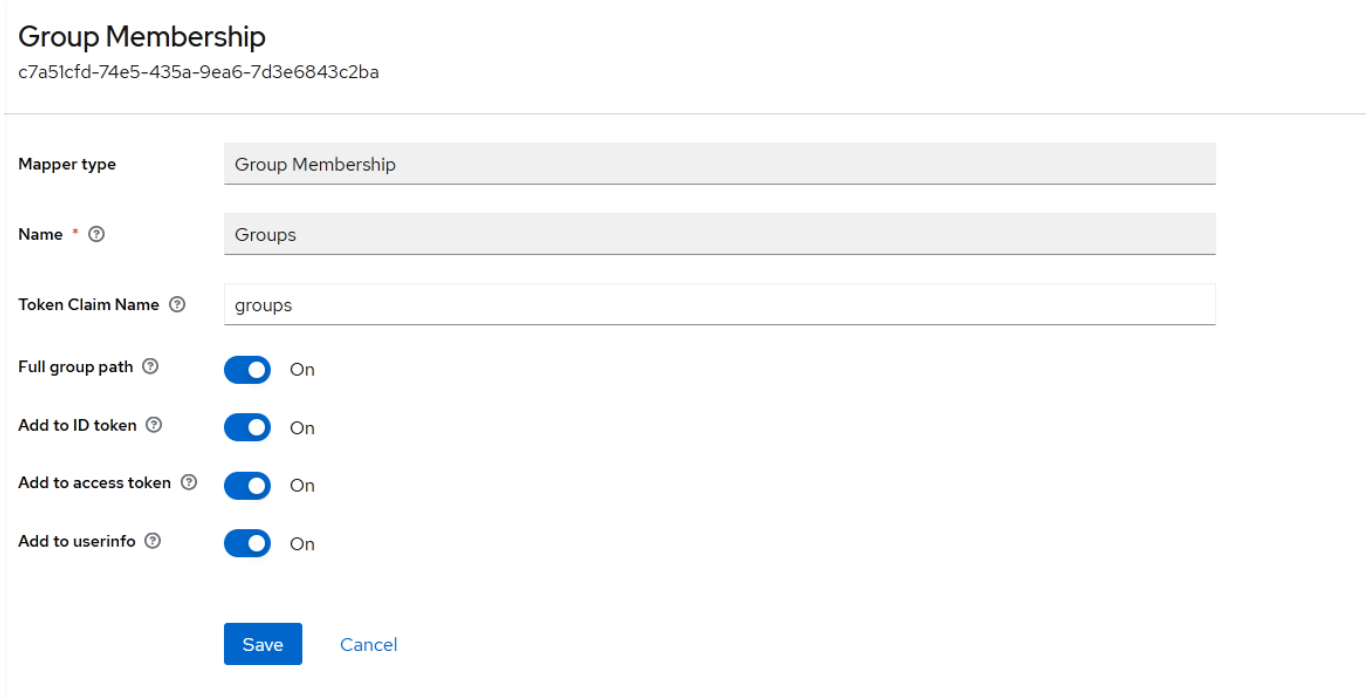
3.11.5.2. Настройка Client scope

1. На вкладке “Client Scopes” выбран “Create client scope”.
2. Параметр имя - “Groups”. Остальные по умолчанию. Сохранить.
3. Настройка mapper для этого “Client Scopes” (рисунок 12, 13).





7. mapper заполнен в соответствии с рисунком 14.



На данном шаге настройка синхронизации пользователей и групп из ALD Pro завершена.

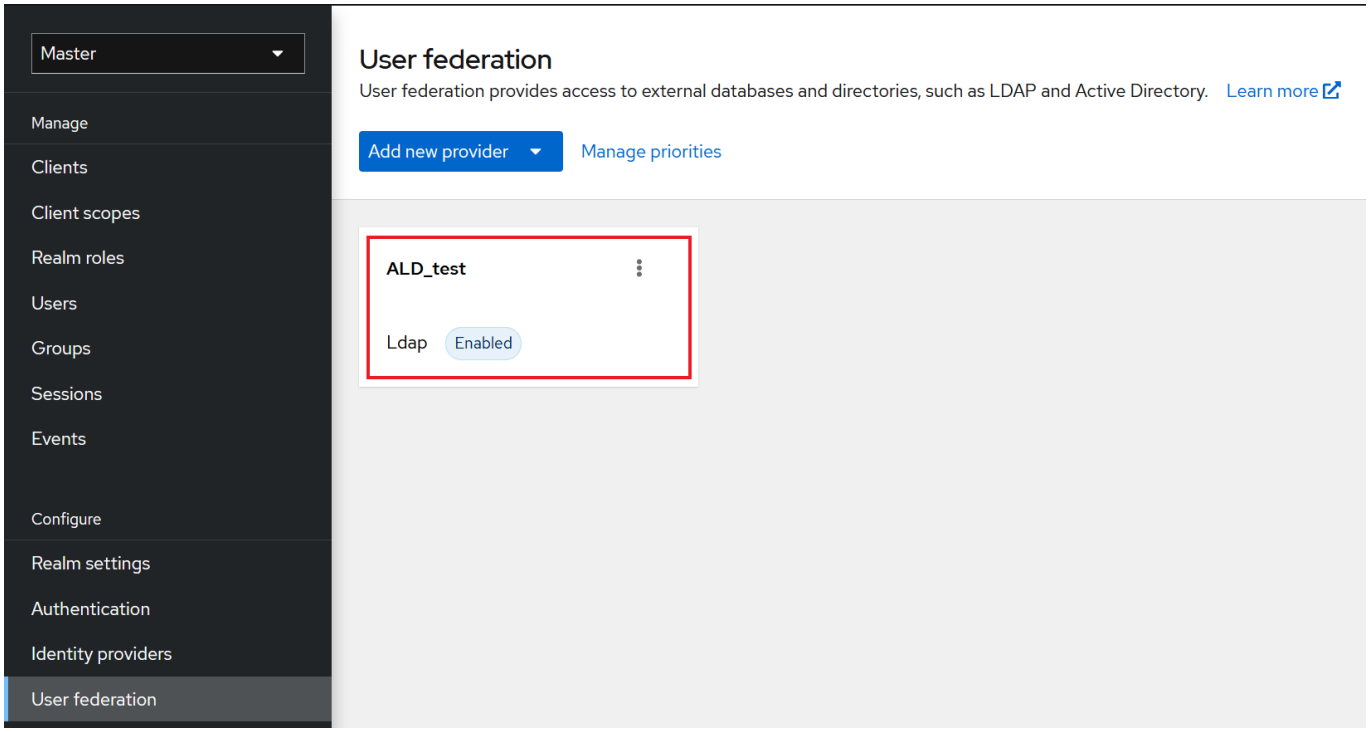
3.11.6. Синхронизация подразделений

3.11.6.1. Создание mapper

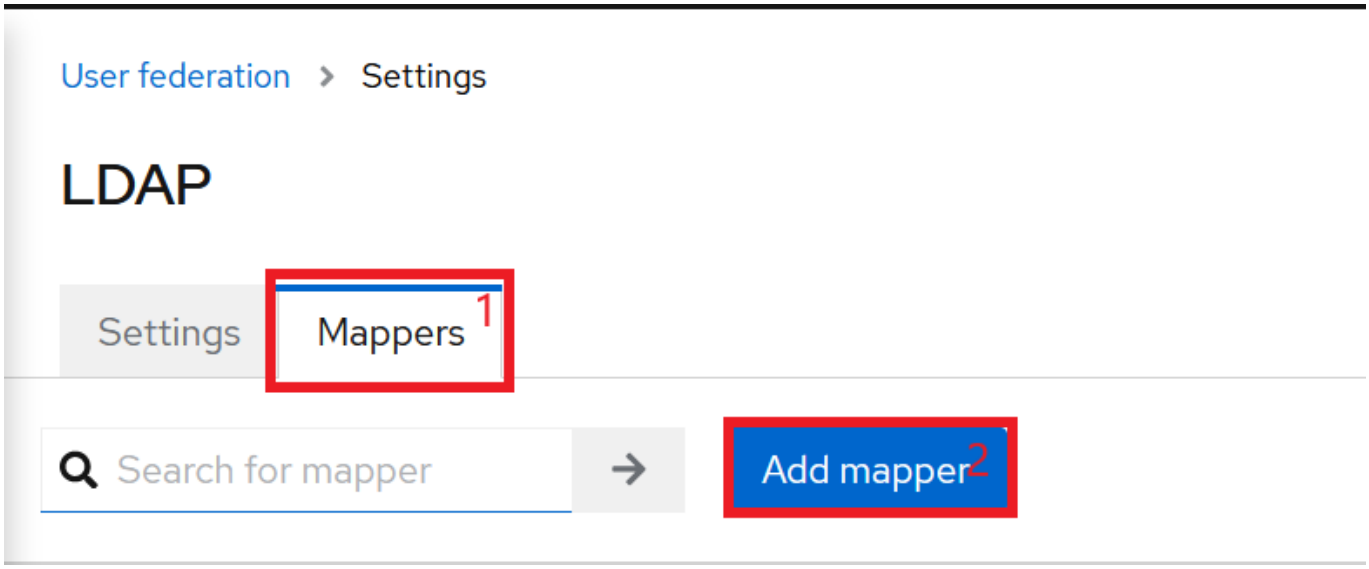
Для синхронизации подразделений сервисный пользователь должен обладать правами на просмотр подразделений.

В Keycloak из коробки нет такой сущности как подразделение, но возможна синхронизация через сущность “группы”.

1. Выполнен переход в карточку “User Federation”.



2. Во вкладке “Mappers” добавлен mapper (рисунок 16).



3. Для создания правильного mapper необходимо заполнить следующие поля:

Поле	Значение
Name	<название
Mapper type	group-ldap-
LDAP Groups DN (в соответствии с примером по созданию федерации пользователя)	ou=astralin
Group Name LDAP Attribute	ou
Group Object Classes	rbta-org-uni
Member-Of LDAP Attribute	rbtadp
User Groups Retrieve Strategy	GET_GROUP

Остальные поля остаются в значении по умолчанию.

Для корректной работы протоколов может понадобиться настройка Keycloak.

3.12. Инструкция по развертыванию ALD Pro в виртуальной среде (знакомство с ALD Pro)

3.12.1. Аннотация

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

3.12.2. Предварительные требования

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

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

3.12.3. Постановка задачи

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

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

отвечает еще одна служба контроллера домена — центр распределения ключей (Key Distribution Center, KDC).

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

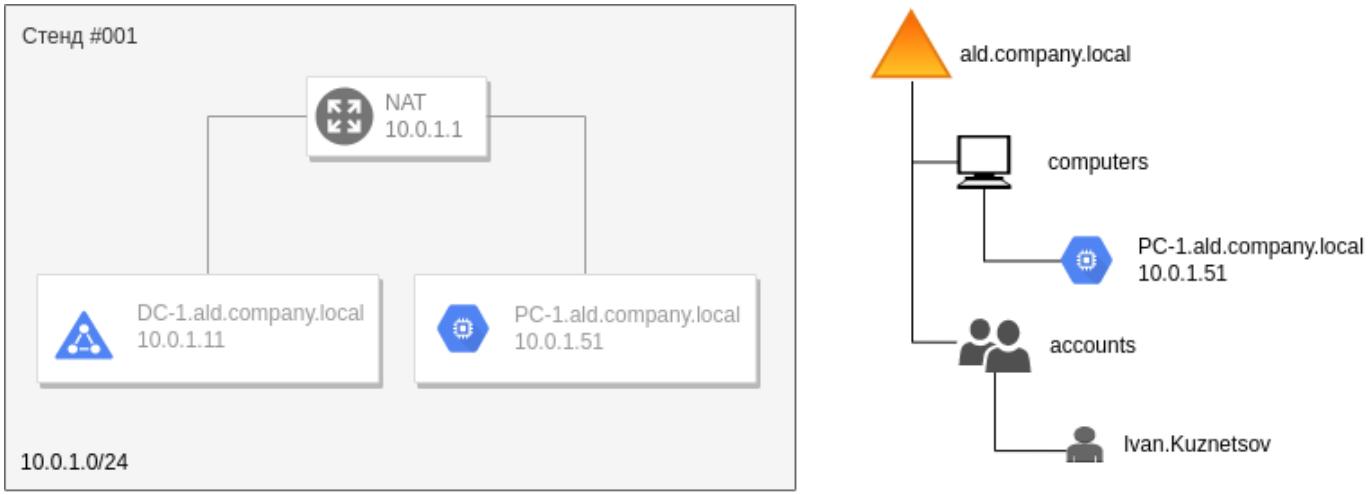


Рисунок 3.70 – Пример топологии домена

3.12.4. Создайте сеть в VirtualBox

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

Чтобы создать сеть в VirtualBox, вам нужно:

- Открыть «Настройки» из меню «Файл»
- В разделе «Сеть» выполнить команду «Добавить»
- Открыть настройки сети и указать следующее: * Имя сети: «Стенд 001» * CIDR сети (диапазон адресов): «10.0.1.0/24» * Поддержка DHCP: Откл (будем использовать собственную службу динамической настройки узлов ALD Pro)

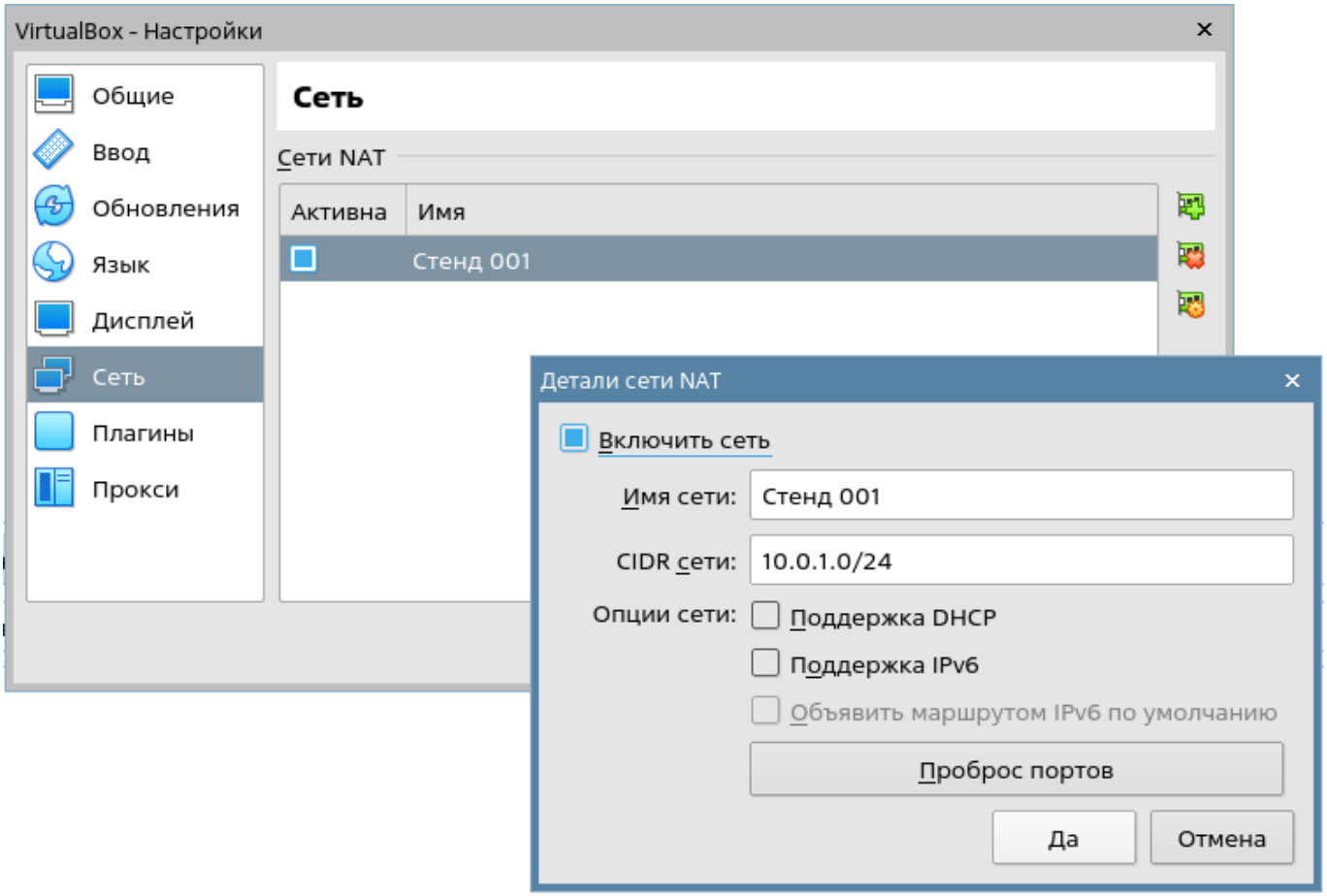


Рисунок 3.71 – Настройки сети virtualbox

В данной сети средствами VirtualBox будет создан NAT-шлюз, через который виртуальные машины смогут выходить в Интернет. IP-адресом шлюза будет является первый адрес в указанной сети 10.0.1.1

В настройках виртуальной машины, на вкладке «Сеть»

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

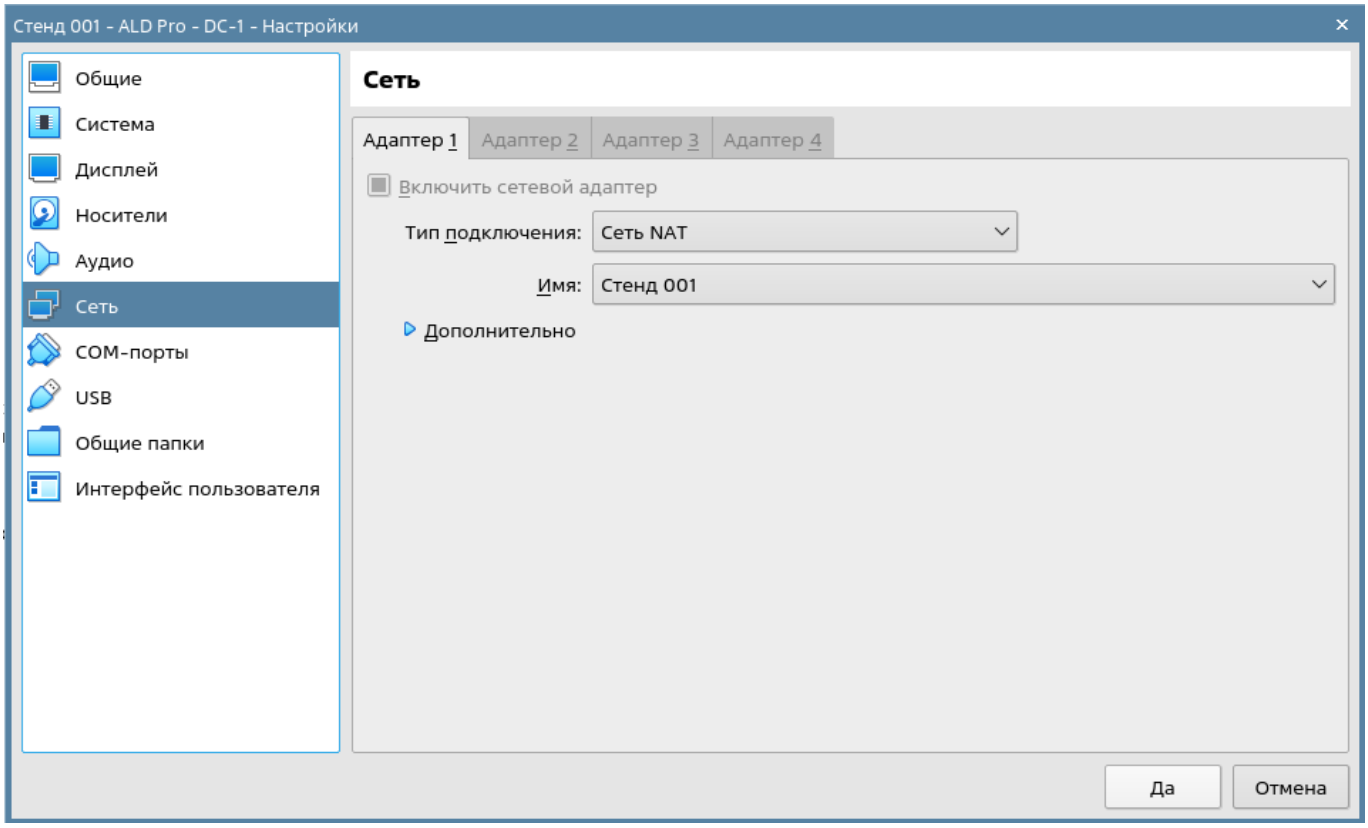


Рисунок 3.72 – Настройки сети виртуальной машины

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

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

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

- **Укажите имя и тип:**
  - Имя: «Стенд 001 — dc-1.ald.company.local»
  - Папка машины: по умолчанию
  - Тип: Linux
  - Версия: Other Linux (64-bit)
- Объем памяти: 4096 МБ
- Жесткий диск: создать новый виртуальный жесткий диск
- Тип файла: VDI (VirtualBox Disk Image)

- Формат хранения: Динамический виртуальный жесткий диск

•Укажите имя и размер файла:

  - Путь: по умолчанию
  - Размер: 32 ГБ

После создания виртуальной машины в ее настройках:

•на вкладке «Система Процессор» укажите:

  - Процессоры: 4 ЦП

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

  - тип подключения: Сеть NAT
  - имя: Стенда 001

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

3.12.6. Установите пакеты ALD Pro на DC-1

3.12.6.1. Настройте сеть для доступа к репозиториям

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

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

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

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

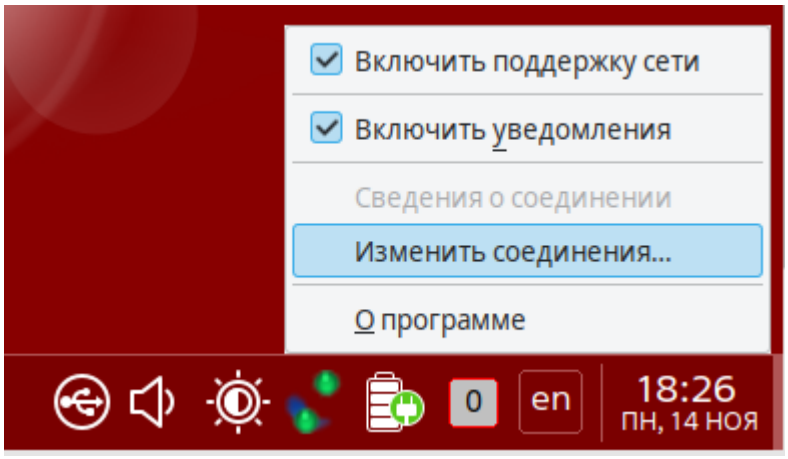


Рисунок 3.73 – Настройка сети для доступа к репозиториям 1

- Сделайте двойной клик по заголовку «Проводное соединение 1»

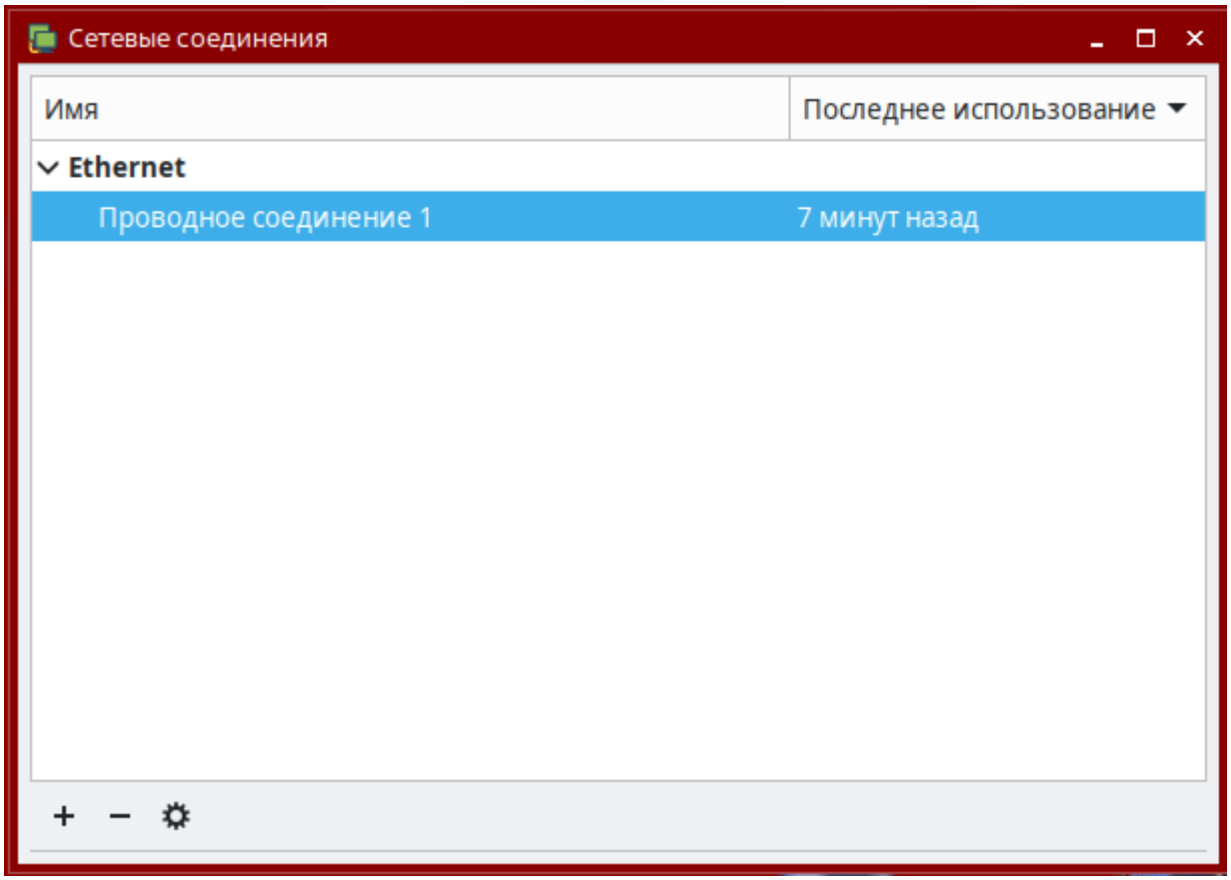


Рисунок 3.74 – Настройка сети для доступа к репозиториям 2

•На закладке Параметры IPv4 укажите следующее:

– Метод: Вручную

– Адрес: 10.0.1.11
– Маска: 255.255.255.0
– Шлюз: 10.0.1.1
– Серверы DNS: 77.88.8.8 (бесплатная служба разрешения имен от Яндекс).

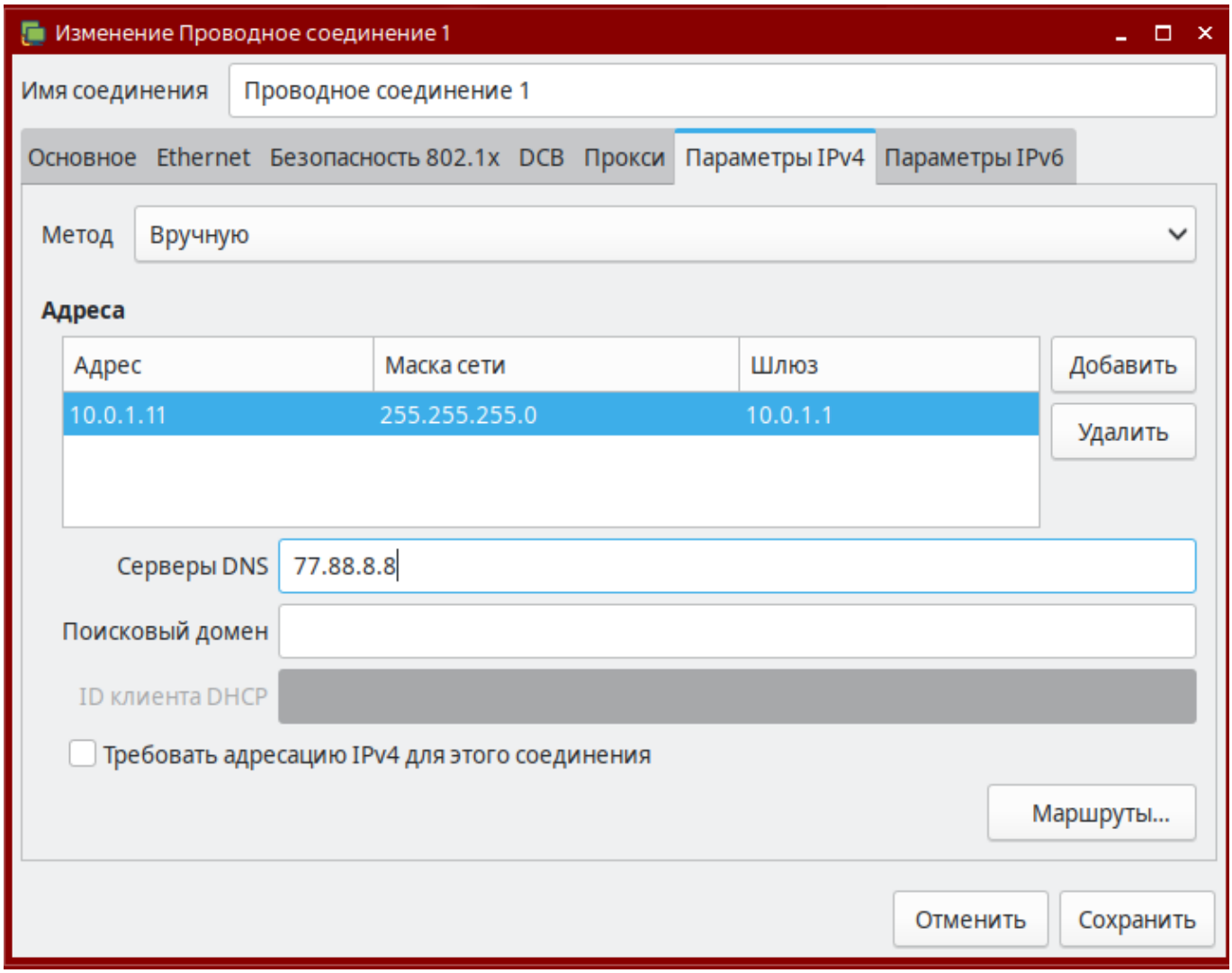


Рисунок 3.75 – Настройка сети для доступа к репозиториям 3

- Проверьте, что у вас есть доступ к репозиториям:

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

3.12.6.2. Настройте доступные репозитории

Файлы программ Linux объединяются в пакеты и распространяются через специальные хранилища, называемые репозиториями. Основным файлом для хранения списка

доступных репозиториев является `/etc/apt/sources.list`, дополнительные списки могут храниться в файлах `\*.list` в директории `/etc/apt/sources.list.d/`

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

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

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

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

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

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

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

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

используйте команды «:wq». Если нужно закрыть документ без сохранения «:q!».

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

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

Комментарии по использованным инструкциям:

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

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

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

компонент — это группа пакетов, объединенная по условиям использования:

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

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

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

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

```
apt update
```

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



Рисунок 3.76 – Формирование ссылки репозитория

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

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

3.12.6.3. Настройте приоритеты пакетов

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

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

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

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

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

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

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

Следует учитывать, что приоритет 900 не позволит понизить версию уже установленного в системе пакета, т. к. для выполнения даунгрейда приоритет кандидата должен быть P > 1000. Поэтому рекомендуется не выполнять обновление операционной системы из интернет-репозиториев, отличных от frozen, во избежание установки конфликтующих версий пакетов.

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

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

3.12.6.4. Установите пакеты

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

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

Комментарии по использованным инструкциям и параметрам:

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

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

-q — параметр позволяет скрыть сообщения о прогрессе установки, делая журнал более читаемым

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

Ознакомьтесь с журналом установки и выполните перезагрузку системы

```
reboot
```

Во время перезагрузки в сообщениях ядра появятся ошибки запуска некоторых только что установленных служб. Это нормальное поведение продукта, которое происходит по причине того, что эти службы еще не настроены должным образом.

3.12.7. Выполните продвижение DC-1 до контроллера домена

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

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

3.12.7.1. Настройте сеть для работы контроллера домена

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

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

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

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

`interfaces` следующее:

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


auto lo
iface lo inet loopback

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

Комментарии по использованным инструкциям:

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

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

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

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

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

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

Файл `/etc/resolv.conf` определяет настройки для процедур разрешения имен из библиотеки `glibc`, которая используется в сетевых утилитах ping, dig и т.д. В этом файле следует следует указать:

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

Комментарии по использованным инструкциям:

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

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

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

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

```
named-checkconf -p
```

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

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

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

3.12.7.2. Задайте имя сервера

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

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

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

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

Проверить можно командой ping:

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

3.12.7.3. Выполните скрипт продвижения

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

```
set +o history
/opt/rbta/aldpro/mp/bin/aldpro-server-install.sh -d ald.company.local -n dc-
↪1 -p 'AstraLinux_172' --no-reboot
set -o history
```

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

Комментарии по использованным ключам:

d — имя домена

n — имя сервера

p — пароль администратора домена

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

Описание параметров скрипта можно получить с помощью ключа -h

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

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

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

Для применения всех настроек выполните перезагрузку сервера:

```
reboot
```

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

```
login: admin

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

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

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

Для доступа на портал управления откройте на контроллере домена браузер Mozilla Firefox, адрес портала будет установлен страницей по умолчанию, авторизация должна пройти прозрачно без запроса пароля.

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

Для проверки работы портала добавьте настройку глобального перенаправления, чтобы BIND9 использовал внешний резолвер, а не обходил все DNS сервера, начиная с корневых каждый раз. На вкладке «Роли и службы сайта — Служба разрешения имен — Глобальная конфигурация DNS» рекомендуется установить адрес публичного DNS, например от Яндекс 77.88.8.8, с политикой перенаправления «Сначала перенаправлять». И не забудьте нажать кнопку «Сохранить» в правом верхнем углу.

3.12.7.4. Отключите DNSSEC, настройте глобальное перенаправление

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

Для завершения настройки портала добавьте настройку глобального перенаправления, чтобы BIND9 использовал внешний DNS сервер, а не обходил все DNS сервера, начиная с корневых, каждый раз. На вкладке «Роли и службы сайта — Служба разрешения имен — Глобальная конфигурация DNS» рекомендуется установить адрес публичного DNS, например от Яндекс 77.88.8.8, с политикой перенаправления «Сначала перенаправлять». И не забудьте нажать кнопку «Сохранить» в правом верхнем углу.

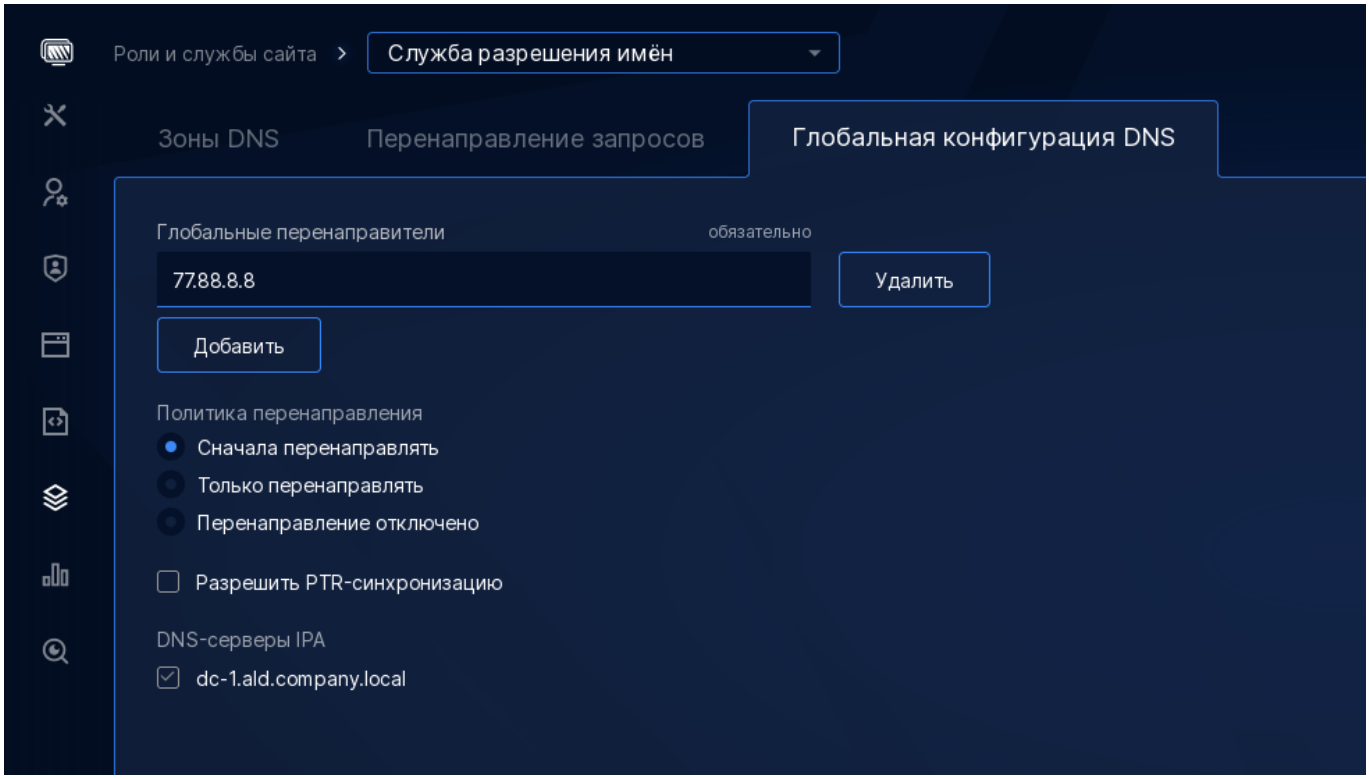


Рисунок 3.77 – Настройка глобального перенаправления

Проверить настройки DNS службы можно из командной строки:

```
ipa dnsconfig-show
```

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

отправляемых на 53 порт:

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

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

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

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

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

После создания виртуальной машины в ее настройках

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

de1e72c271497a2b27909ea148f93f1f

•**на вкладке «Сеть» выберите:**

– тип подключения: Сеть NAT

– имя: Стенда 001

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

3.12.9. Установите клиентские пакеты ALD Pro на PC-1

3.12.9.1. Настройте сеть для доступа к репозиториям

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

На пользовательских компьютерах настройка сети выполняется через стандартную службу NetworkManager. В реальной инфраструктуре для настройки пользовательских компьютеров используется DHCP, но в рамках данной инструкции с целью упрощения компьютеру будет назначен статический адрес.

На вкладке «Параметры IPv4» установите следующие значения:

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

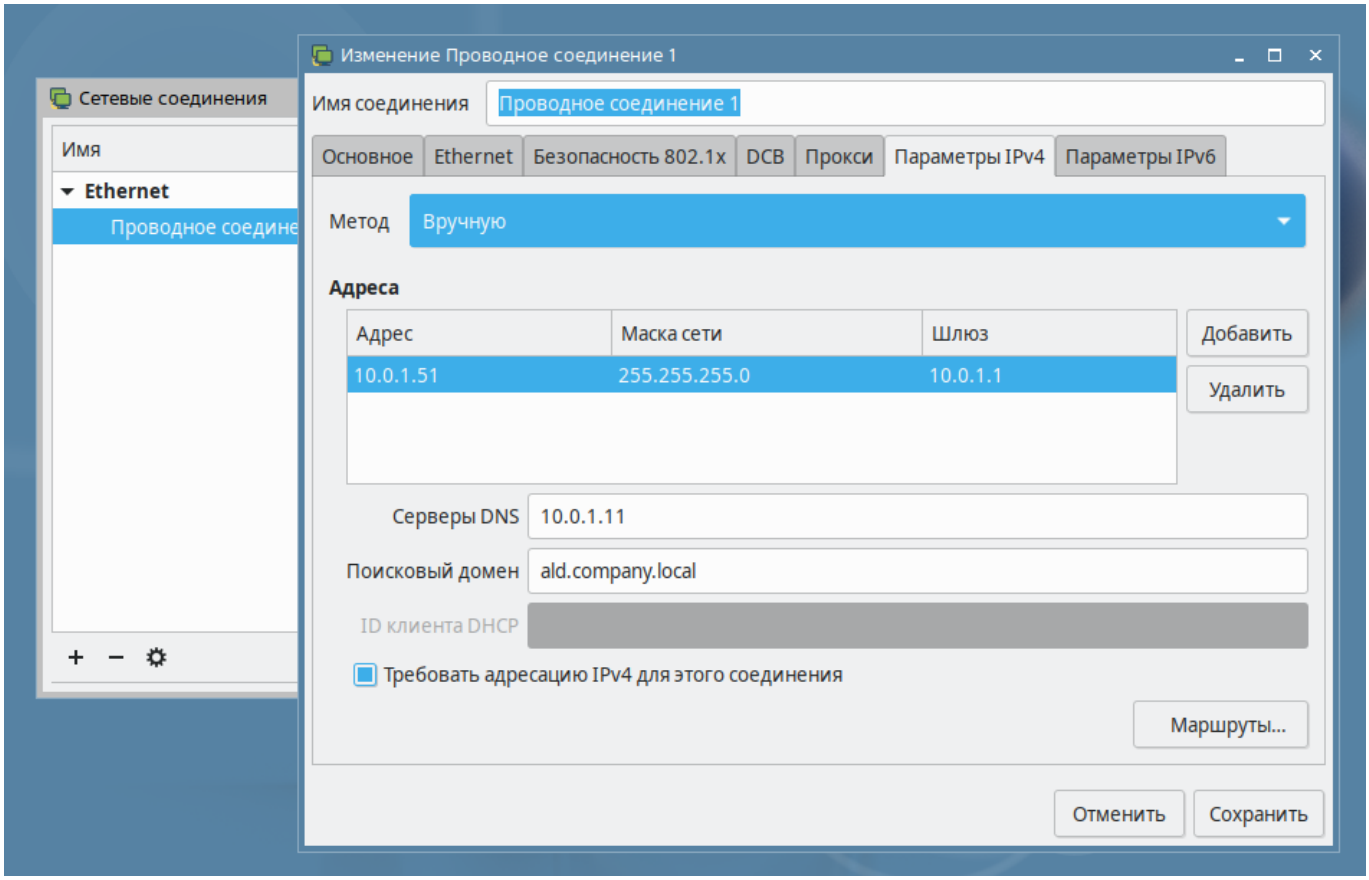


Рисунок 3.78 – Настройка параметров IPv4

Можете проверить результат ваших действий командами:

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

3.12.9.2. Настройте доступные репозитории

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

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

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

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

Настройте приоритеты, так же как делали на сервере

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

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

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

3.12.9.3. Установите пакеты

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

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

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

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

3.12.10. Выполните ввод компьютера в домен

Для ввода компьютера в домена требуется несколько условий:

у компьютера должно быть задано уникальное имя, которое еще не используется в домене;

в качестве DNS-сервера должен быть указан IP адрес контроллера домена.

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

```
nslookup pc-1
```

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

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

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

Вы также можете сгенерировать случайное имя хосту следующей командой:

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

Все готово для ввода компьютера в домен:

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

Комментарии по использованным ключам:

c — имя домена

u — логин администратора домена

p — пароль администратора домена

d — имя компьютера

i — использовать интерактивный режим

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

Для применения всех настроек выполните перезагрузку компьютера:

```
reboot
```

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

```
login: admin

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

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

3.12.11. Проверка работы синхронизации времени

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

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

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

компьютеры синхронизируют время с контроллером, а контроллер берет его у публичных серверов.

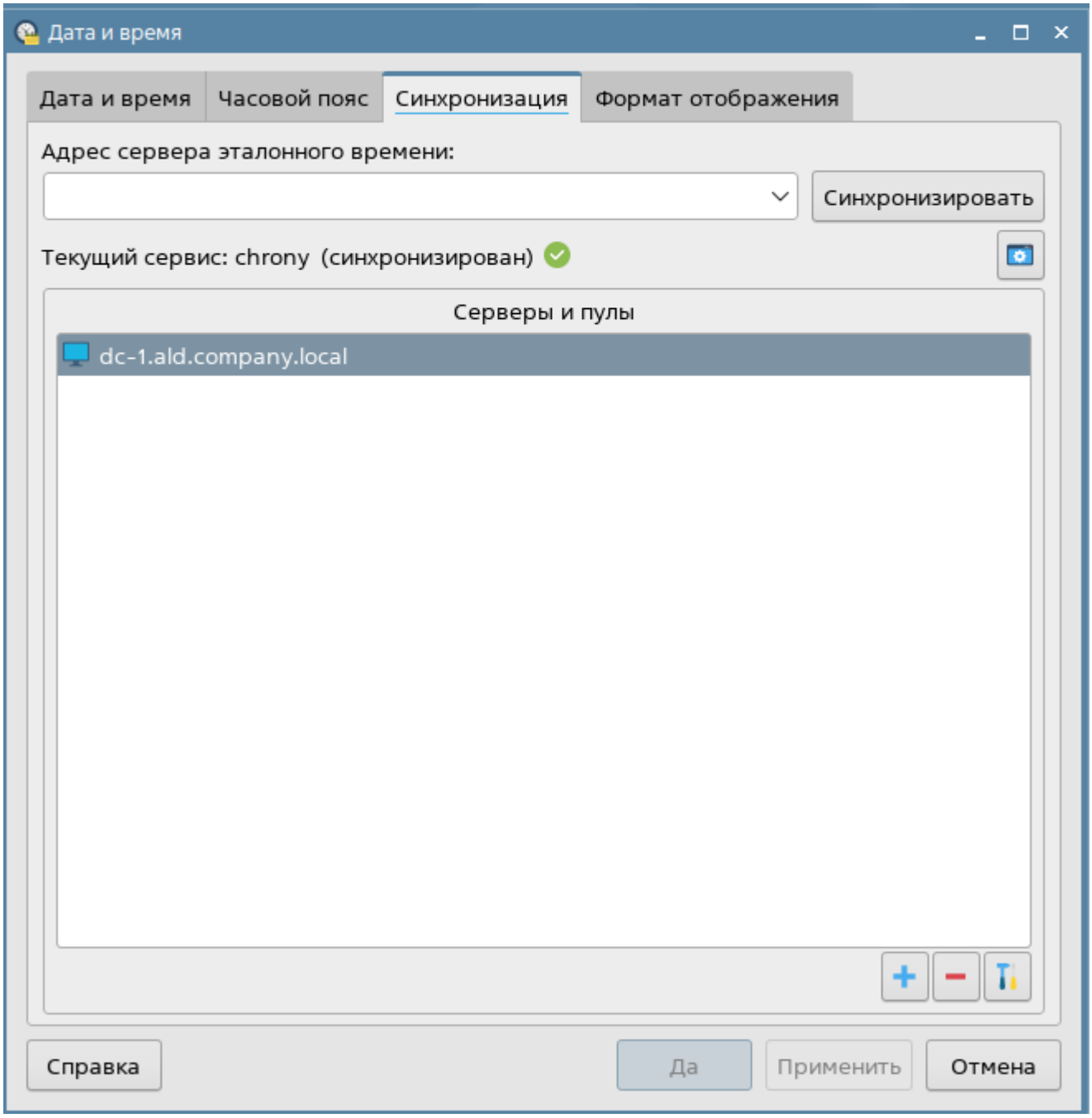


Рисунок 3.79 – Синхронизация даты и времени 1

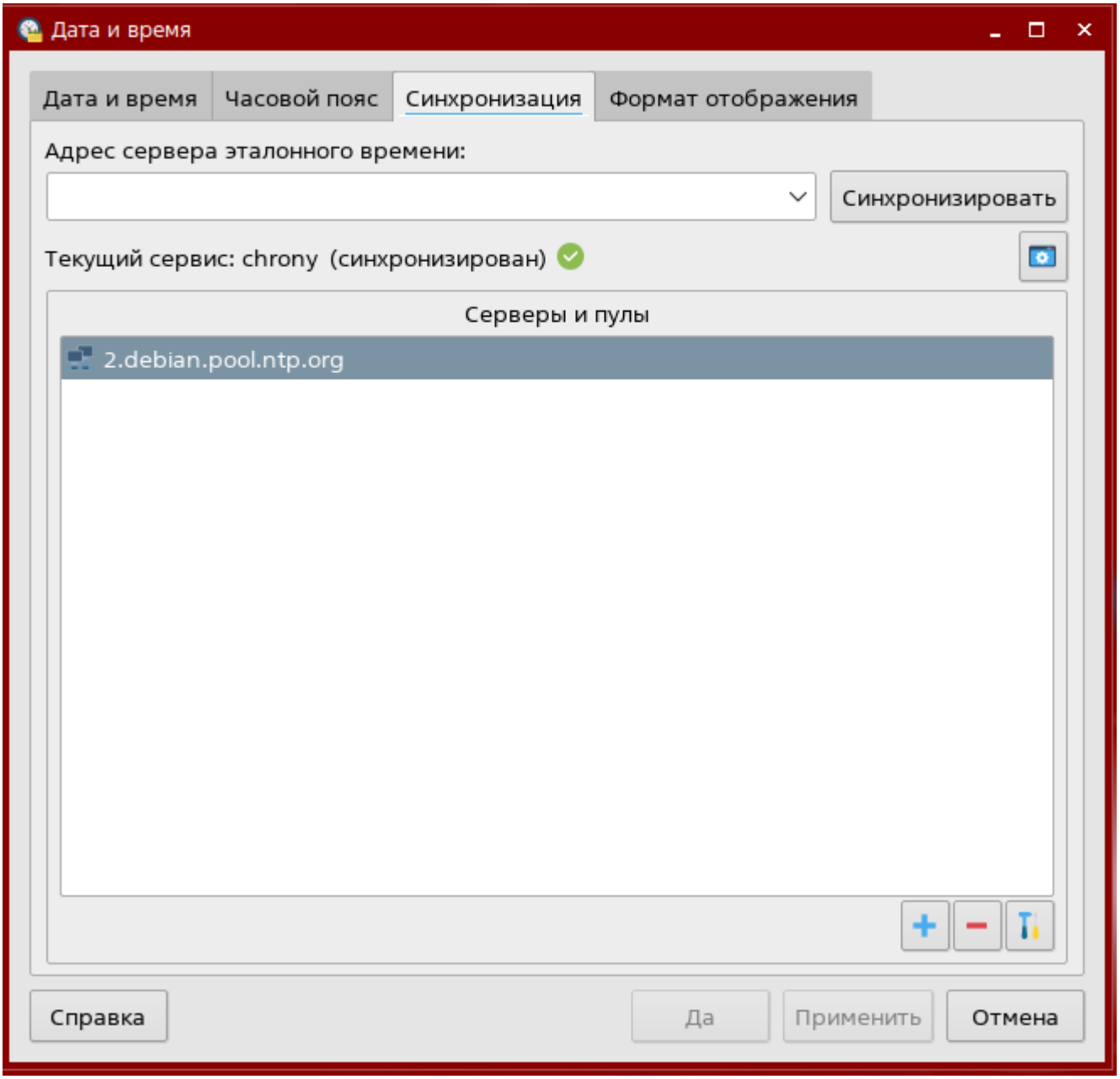


Рисунок 3.80 – Синхронизация даты и времени 2

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

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

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

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

Принудительно запустить синхронизацию времени можно перезапуском службы

```
systectl restart chrony
```

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

```
timedatectl
```

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

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

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

```
chronyc makestep
```

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

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

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

После синхронизации времени указанная выше команда `timedatectl` может показать расхождение между системным временем ALSE (Universal time) и значением времени в BIOS (RTC time, real time clock), так как запись в BIOS происходит только при выключении компьютера. Записать текущее время системы в BIOS можно утилитой hwclock с параметром systohc:

```
hwclock --systohc
```

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

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

Информацию о выданных билетах можно увидеть командой `klist`:

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

3.12.12. Как работает вход в доменный компьютер

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

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

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

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

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

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

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

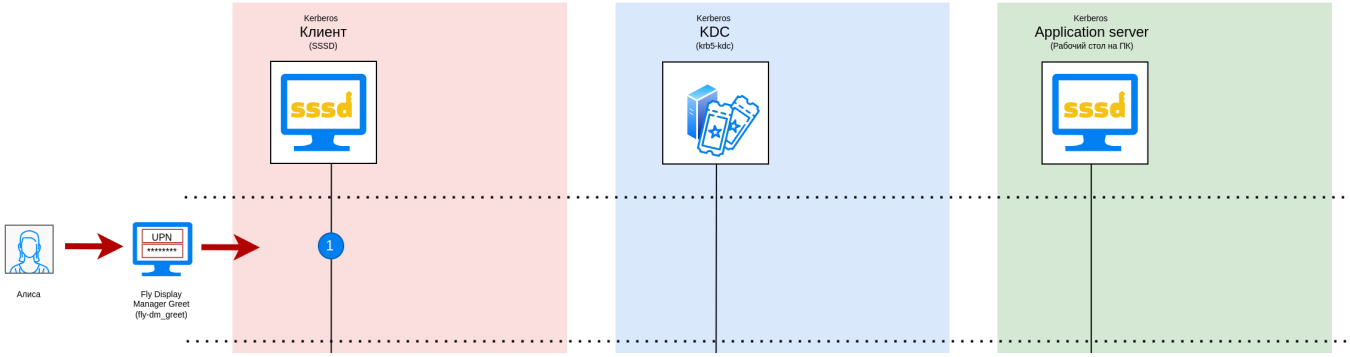


Рисунок 3.81 – Как работает вход в доменный компьютер 1

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



Рисунок 3.82 – Как работает вход в доменный компьютер 2

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

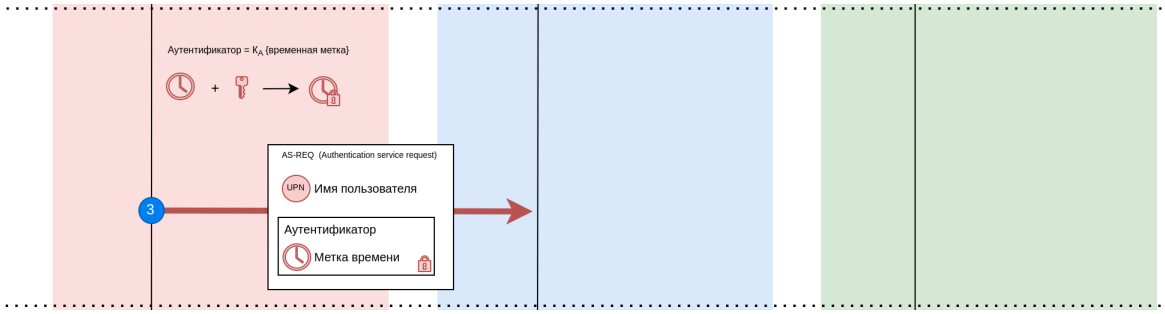


Рисунок 3.83 – Как работает вход в доменный компьютер 3

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

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

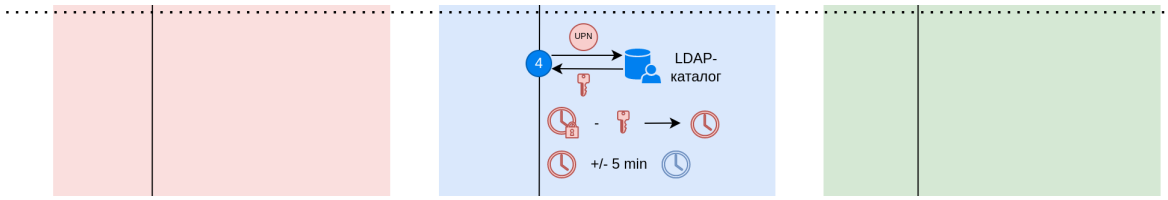


Рисунок 3.84 – Как работает вход в доменный компьютер 4

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

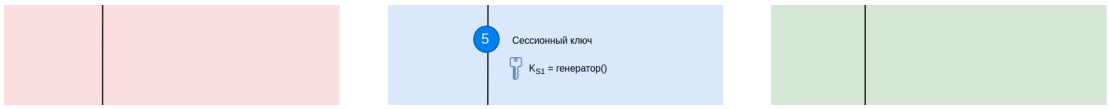


Рисунок 3.85 – Как работает вход в доменный компьютер 5

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

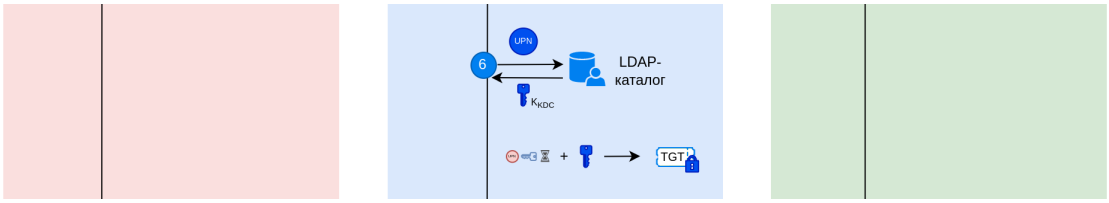


Рисунок 3.86 – Как работает вход в доменный компьютер 6

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

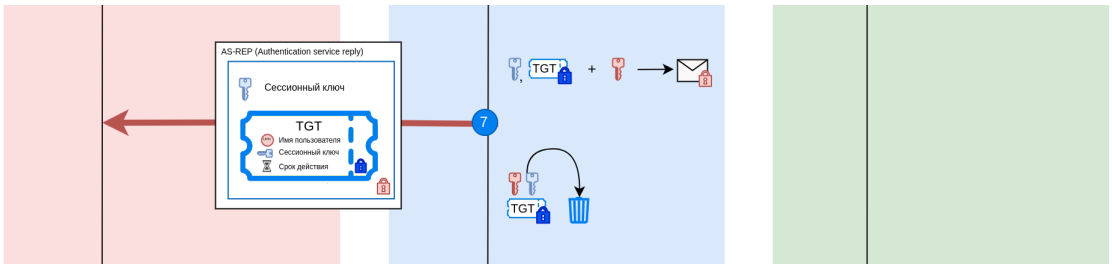


Рисунок 3.87 – Как работает вход в доменный компьютер 7

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



Рисунок 3.88 – Как работает вход в доменный компьютер 8

9. Клиент отправляет контроллеру запрос на доступ к серверу приложению, в котором содержится имя пользователя, имя сервера приложения, билет на выдачу билетов (TGT) и аутентификатор. В качестве аутентификатора выступает метка времени, зашифрованная симметричным алгоритмом с помощью сессионного ключа S1.



Рисунок 3.89 – Как работает вход в доменный компьютер 9

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

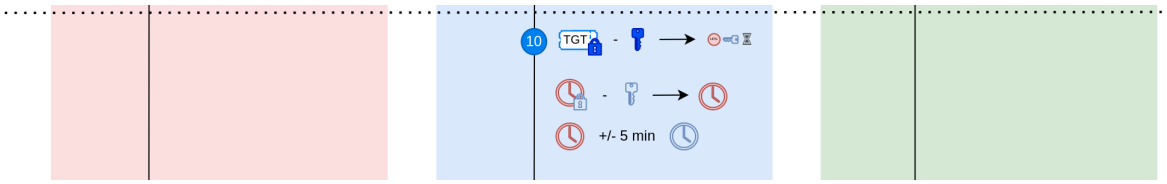


Рисунок 3.90 – Как работает вход в доменный компьютер 10

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

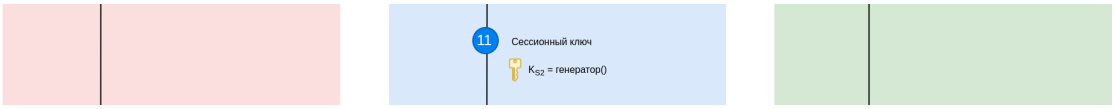


Рисунок 3.91 – Как работает вход в доменный компьютер 11

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

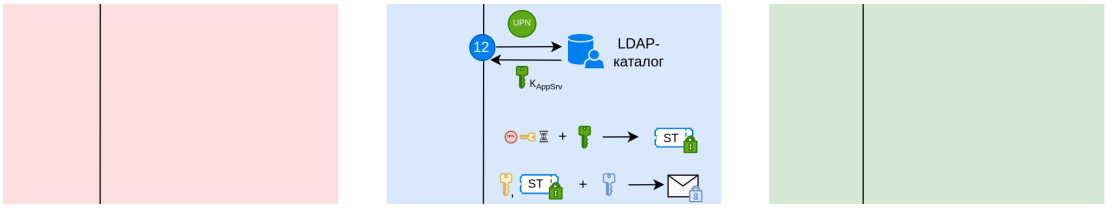


Рисунок 3.92 – Как работает вход в доменный компьютер 12

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

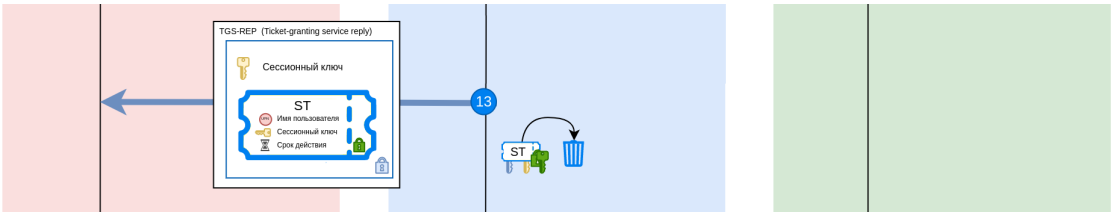


Рисунок 3.93 – Как работает вход в доменный компьютер 13

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

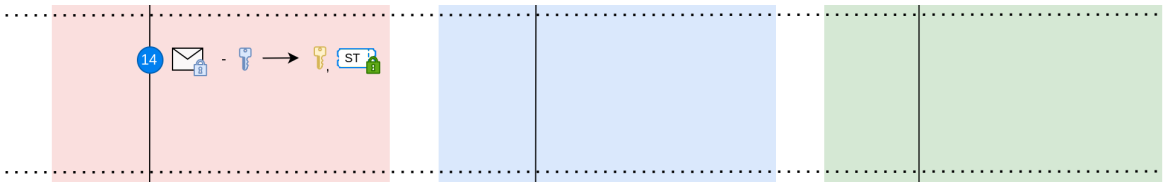


Рисунок 3.94 – Как работает вход в доменный компьютер 14

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

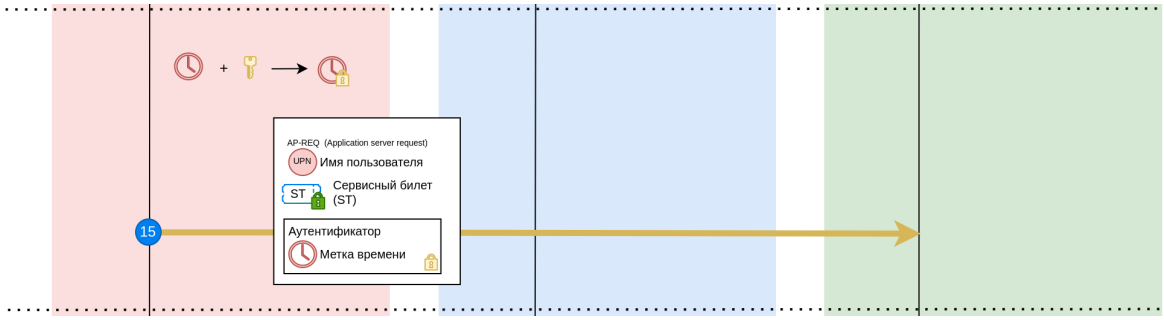


Рисунок 3.95 – Как работает вход в доменный компьютер 15

16. Сервер приложения, в роли которого выступает служба SSSD на пользовательском компьютере расшифровывает ответ. Используя этот долгосрочный ключ, служба SSSD может расшифровать информацию из сервисного билета (ST), после чего ей становится доступна следующая информация: имя пользователя, сессионный ключ S2 и срок действия билета. SSSD расшифровывает аутентификатор, используя сессионный ключ S2 из сервисного билета, и, если полученное значение расходится со временем компьютера не более, чем на 5 минут, то считается, что аутентификация пройдена успешно.

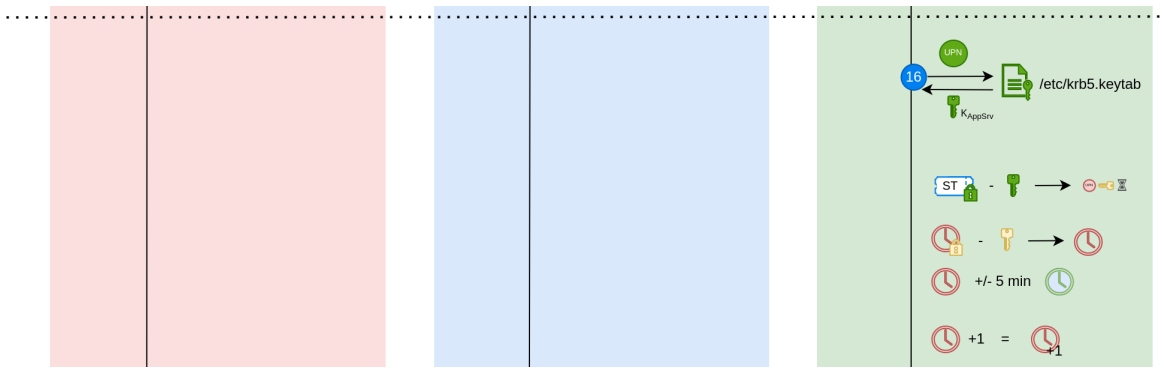


Рисунок 3.96 – Как работает вход в доменный компьютер 16

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

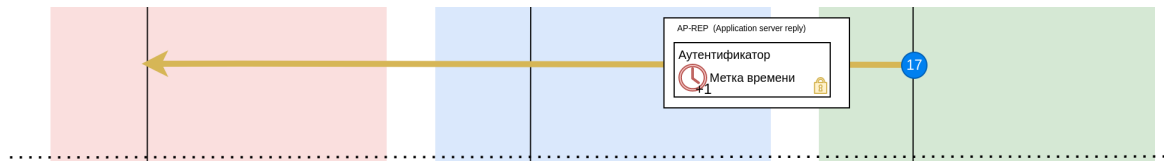


Рисунок 3.97 – Как работает вход в доменный компьютер 17

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



Рисунок 3.98 – Как работает вход в доменный компьютер 18

3.12.13. Как управлять билетами Kerberos из командной строки

Информацию о выданных билетах можно увидеть командой `klist`:

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

Очистить кэш можно командой `kdestroy`:

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

Пройти аутентификацию в домене можно командой kinit:

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

Сменить пароль текущего пользователя можно командой kpasswd:

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

3.13. Настройка прочих подсистем

3.13.1. Подготовительные действия

После развертывания контроллера домена и первого запуска подсистемы «Портал управления» необходимо ввести в домен три клиента, которые будут выполнять следующие основные роли:

- сервер подсистемы «Репозитории программного обеспечения»;
- сервер подсистемы «Динамическая настройка узла» (сервер DHCP);
- сервер подсистемы «Установка ОС по сети».

Данная минимальная серверная группа обеспечит работу ПК «ALD Pro».

Описание характеристик серверного оборудования и инструкция по подготовке клиентов для вышеперечисленных серверов приводятся в документе РДЦП.10101-01 95 01 «Программный комплекс «ALD Pro». Руководство администратора. Инструкция по развертыванию».

Дальнейшее масштабирование инфраструктуры осуществляется средствами портала управления.

3.13.2. Развертывание основных подсистем ПК «ALD Pro»

Для каждой роли должен быть выделен отдельный клиент, отвечающий следующим условиям:

- на клиенте установлена операционная система Astra Linux 1.7;
- клиент введен в домен и отображается в списке компьютеров в портале управления (раздел **Пользователи и компьютеры** — подраздел **Компьютеры**) (см. *Компьютеры*);
- на клиенте не развернута ни одна из подсистем ПК «ALD Pro».

Основные подсистемы ПК «ALD Pro» разворачиваются в следующем порядке:

- сервер подсистемы «Репозитории программного обеспечения»;
- сервер подсистемы «Динамическая настройка узла» (сервер DHCP);
- сервер подсистемы «Установка ОС по сети».

3.13.2.1. Сервер подсистемы «Репозитории программного обеспечения»

Развертывание сервера репозиториев программного обеспечения выполняется в портале управления (раздел **Установка и обновление ПО** — подраздел **Репозитории ПО** — вкладка **Серверы репозиториев ПО**) в соответствии с описанием вкладки *Серверы репозиториев ПО*.

Готовность сервера репозиториев можно отследить в панели управления (раздел **Автоматизация** — подраздел **Задания автоматизации** — вкладка **Журнал заданий**): при успешном завершении задания по развертыванию сервера репозиториев ПО в столбце **Статус** отобразится **Успешно** (см. *Задания автоматизации*).

3.13.2.2. Сервер подсистемы «Динамическая настройка узла» (сервер DHCP)

Развертывание сервера динамической настройки узла выполняется в портале управления (раздел **Роли и службы сайта** — подраздел **Служба динамической настройки узла**) в соответствии с описанием подраздела *Служба динамической настройки узла*.

В результате успешного развертывания сервера динамической настройки узла:

- в панели управления (раздел **Автоматизация** — подраздел **Задания автоматизации** — вкладка **Журнал заданий**) соответствующее задание автоматизации будет иметь статус **Успешно** (см. *Задания автоматизации*);
- в панели управления (раздел **Роли и службы сайта** — подраздел **Служба динамической настройки узла** — вкладка **Перечень серверов**) отобразится добавленный сервер динамической настройки узла (см. *Служба динамической настройки узла*).

Файл конфигурации сервера динамической настройки узла для инфраструктуры системы подготавливается в формате `*.txt` и загружается на сервер средствами портала управления согласно порядку, описанному в главе *Настройка конфигурации DHCP-сервера* (раздел *Роли и службы сайта*, подраздел *Служба динамической настройки узла*).

3.13.2.3. Сервер подсистемы «Установка ОС по сети»

Развертывание сервера установки ОС по сети выполняется в портале управления (раздел **Автоматизация** — подраздел **Установка ОС по сети** — вкладка **Серверы установки ОС**)

в соответствии с описанием вкладки *Установка ОС по сети*.

В результате успешной установки сервера:

- в панели управления (раздел **Автоматизация** — подраздел **Задания автоматизации** — вкладка **Журнал заданий**) соответствующее задание автоматизации будет иметь статус **Успешно** (см. *Задания автоматизации*);
- в панели управления (раздел **Автоматизация** — подраздел **Установка ОС по сети** — вкладке **Серверы установки ОС**) отобразится установленный сервер (см. *Установка ОС по сети*).

Для установки ОС по сети на компьютеры домена на сервере должны быть созданы соответствующие профили загрузки. Порядок создания профилей описан в подразделе *Установка ОС по сети*.

3.13.3. Добавление компьютера ПК «ALD Pro» в домен

Добавление клиента ПК «ALD Pro» в домен осуществляется после развертывания контроллера домена и развертывания серверной группы (сервера подсистемы «Репозитории программного обеспечения», сервера подсистемы «Динамическая настройка узла» (сервер DHCP), сервера подсистемы «Установка ОС по сети»).

Добавление компьютера в домен ALD Pro возможно двумя способами:

- путем подготовки компьютера и установки на нем клиентской части (см. *Подготовка компьютера и установка на нем клиентской части*);
- путем установки на компьютер ОС по сети с использованием портала управления ПК «ALD Pro» в соответствии с описанием подраздела *Установка ОС по сети* (раздел :ref:`install_ALD_client).

3.13.3.1. Подготовка компьютера и установка на нем клиентской части

На компьютере, предназначенном для развертывания клиентской части ПК «ALD Pro», должна быть установлена ОС Astra Linux очередное обновление 1.7 с графической оболочкой Fly с установленным оперативным обновлением 1.7.2 (бюллетень № 2022-0819SE17), 1.7.3 (бюллетень № 2022-1110SE17) либо 1.7.4 (бюллетень №2023-0426SE17).

Внимание: Программное обеспечение ОС Astra Linux должно совпадать на контроллере домена, подсистемах и клиенте, например везде должно быть установлено либо ОС Astra Linux совместно с оперативным обновлением 1.7.2 (бюллетень 2022-0819SE17), либо ОС Astra Linux совместно с оперативным обновлением 1.7.3 (бюллетень № 2022-1110SE17), либо ОС Astra Linux совместно с оперативным обновлением 1.7.4 (бюллетень №2023-0426SE17).

При этом для контроллера домена и подсистем ОС Astra Linux должна функционировать на максимальном уровне защищенности («Смоленск»). Если ОС Astra Linux функционирует на уровне защищенности «Базовый» («Орел») или уровне защищенности «Усиленный» («Воронеж»), то для перевода на уровень защищенности «Максимальный» необходимо от имени привилегированного пользователя выполнить в терминале команду:

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

На компьютере необходимо выполнить следующие действия:

1. в файле `/etc/hostname` указать имя сервера контроллера домена в формате FQDN: <имя_компьютера>.<домен>

Пример

```
dc.domain.test
```

2. в файле `/etc/hosts` внести следующие изменения:

```
127.0.0.1   localhost.localdomain   localhost
IP-адрес_сервера>   <имя_сервера>.<домен>   <имя_сервера>
127.0.1.1   <имя_сервера>
```

Пример

```
127.0.0.1   localhost.localdomain   localhost
192.168.30.15 dc.domain.test dc
127.0.1.1   dc
```

3. убедиться, что файл `/etc/apt/sources.list` содержит следующие строки (при необходимости — добавить, если имеются другие записи, то закомментировать их или удалить):

- для ОС Astra Linux очередного обновления 1.7 с установленным оперативным обновлением 1.7.2 (бюллетень № 2022-0819SE17):

```
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.2/
repository-base 1.7_x86-64 main non-free contrib
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.2/
repository-extended 1.7_x86-64 main contrib non-free
```

- для ОС Astra Linux очередного обновления 1.7 с установленным оперативным обновлением 1.7.3 (бюллетень № 2022-1110SE17):

```
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/
repository-base 1.7_x86-64 main non-free contrib
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/
repository-extended 1.7_x86-64 main contrib non-free
```

- для ОС Astra Linux очередного обновления 1.7 с установленным оперативным обновлением 1.7.4 (бюллетень №2023-0426SE17)

```
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.4/
repository-base 1.7_x86-64 main non-free contrib
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.4/
repository-extended 1.7_x86-64 main contrib non-free
```

4. подключить репозиторий `aldpro`, выполнив в терминале команды:

```
echo -e "deb https://dl.astralinux.ru/aldpro/stable/repository-main/
1.4.0 main" | sudo tee /etc/apt/sources.list.d/aldpro.list echo -e "deb
 ↪https://dl.astralinux.ru/aldpro/stable/repository-
extended/ generic main" | sudo tee -a /etc/apt/sources.list.d/ aldpro.list
```

5. добавить конфигурационный файл `/etc/apt/preferences.d/aldpro` настроек приоритета `apt` со следующим содержимым:

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

6. обновить пакеты, выполнив в терминале команду:

```
sudo apt update && sudo apt dist-upgrade -y
```

7. настроить статический сетевой интерфейс.

> **Предупреждение:** При настройке файла `/etc/network/interfaces` необходимо убедиться, что Network-manager отключен, для этого ввести в терминале команду:

```
sudo systemctl status network-manager
```

Если Network-manager работает, то выполнить его отключение, введя в терминале команды:

```
sudo systemctl stop network-manager
sudo systemctl disable network-manager
```

Для настройки файла `/etc/network/interfaces` внести следующие изменения:

```
auto eth0
iface eth0 inet static
address <IP-адрес_контроллера_домена>
netmask <маска_подсети>
gateway <шлюз>
dns-nameservers <IP-адрес_dns_сервера>
dns-search <домен>
```

Пример

```
auto eth0
iface eth0 inet static
address 192.168.30.15
netmask 255.255.255.0
gateway 192.168.30.1
dns-nameservers 77.88.8.8
dns-search domain.test
```

8. применить настройки сети, выполнив команду в терминале:

```
sudo systemctl restart networking
```

3.13.3.2. Проверка корректной установки окружения

Перед установкой клиентской части ПК «ALD Pro» следует проверить корректность настроек, а именно:

1. на компьютере клиентской части ПК «ALD Pro» объем оперативной памяти не менее 4 ГБ;
2. на компьютере клиентской части ПК «ALD Pro» ОС Astra Linux функционирует на максимальном уровне защищенности. Для проверки необходимо от имени пользователя, имеющего нужные возможности по администрированию, выполнить в терминале команду:

```
sudo astra-modeswitch get
```

Результат выполнения команды должен быть: 2

3. в файле `/etc/hostname` указано корректное имя сервера контроллера домена в формате FQDN;
4. в файле `/etc/hosts` указаны корректные данные первого контроллера домена;
5. в файле `/etc/apt/sources.list` указаны репозитории ОС Astra Linux;
6. в файле `/etc/apt/sources.list.d/aldpro.list` указаны репозитории ПК «ALD Pro»;
7. для ПК «ALD Pro» присутствует файл `/etc/apt/preferences.d/aldpro`, определяющий его приоритет;
8. сетевой интерфейс первого контроллера домена настроен на статический IP-адрес;
9. проверить доступность dl.astralinux.ru с сервера первого контроллера домена, выполнив в терминале команду:

```
ping -c 3 dl.astralinux.ru
```

3.13.3.3. Подготовка окружения к установке с установочного диска

На компьютере, предназначенном для развертывания клиентской части ПК «ALD Pro», должна быть установлена ОС Astra Linux очередное обновление 1.7 с графической оболочкой Fly с установленным оперативным обновлением 1.7.2 (бюллетень № 2022-0819SE17), 1.7.3 (бюллетень № 2022-1110SE17) либо 1.7.4 (бюллетень №2023-0426SE17).

> **Внимание:** Программное обеспечение ОС Astra Linux должно совпадать на контроллере домена, подсистемах и клиенте, например везде должно быть установлено либо ОС Astra Linux совместно с оперативным обновлением 1.7.2 (бюллетень 2022-0819SE17), либо ОС Astra Linux совместно с оперативным обновлением 1.7.3 (бюллетень № 2022-1110SE17), либо ОС Astra Linux совместно с оперативным обновлением 1.7.4 (бюллетень №2023-0426SE17).

При этом для контроллера домена и подсистем ОС Astra Linux должна функционировать на максимальном уровне защищенности («Смоленск»). Если ОС Astra Linux функционирует на уровне защищенности «Базовый» («Орел») или уровне защищенности «Усиленный» («Воронеж»), то для перевода на уровень защищенности «Максимальный» необходимо от имени привилегированного пользователя выполнить в терминале команду:

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

На компьютере необходимо выполнить следующие действия:

1. в файле `/etc/hostname` указать имя компьютера в формате FQDN:

```
<имя_компьютера>.<домен>
```

Пример

```
dc.domain.test
```

2. в файле `/etc/hosts` внести следующие изменения:

```
127.0.0.1   localhost.localdomain   localhost
IP-адрес_сервера>   <имя_сервера>.<домен>   <имя_сервера>
127.0.1.1   <имя_сервера>
```

Пример

```
127.0.0.1   localhost.localdomain   localhost
192.168.30.15 dc.domain.test dc
127.0.1.1   dc
```

3. убедиться, что файл `/etc/apt/sources.list` содержит следующие строки, при необходимости — добавить, если имеются другие записи, то закомментировать их или удалить:

- для ОС Astra Linux очередного обновления 1.7 с установленным оперативным обновлением 1.7.2 (бюллетень № 2022-0819SE17):

```
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.2/
repository-base 1.7_x86-64 main non-free contrib
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.2/
repository-extended 1.7_x86-64 main contrib non-free
```

- для ОС Astra Linux очередного обновления 1.7 с установленным оперативным обновлением 1.7.3 (бюллетень № 2022-1110SE17):

```
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/
repository-base 1.7_x86-64 main non-free contrib
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/
repository-extended 1.7_x86-64 main contrib non-free
```

- для ОС Astra Linux очередного обновления 1.7 с установленным оперативным обновлением 1.7.4 (бюллетень №2023-0426SE17)

```
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.4/
repository-base 1.7_x86-64 main non-free contrib
deb http://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.4/
repository-extended 1.7_x86-64 main contrib non-free
```

4. примонтировать диск и подключить репозиторий aldpro, выполнив в терминале команды:

```
sudo mount /dev/sr0 /media/cdrom
sudo apt-cdrom -m add
```

5. ввести имя диска:

```
ALDPro_N.N.N
```

где N.N.N. - номер версии ALD Pro.

6. добавить расширенный репозиторий aldpro, выполнив в терминале команду:

```
echo -e "deb
https://dl.astralinux.ru/aldpro/stable/repository-extended/
generic main" | sudo tee /etc/apt/sources.list.d/aldpro.list
```

7. добавить конфигурационный файл `/etc/apt/preferences.d/aldpro` настроек приоритета apt со следующим содержимым:

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

8. обновить пакеты, выполнив в терминале команду:

```
sudo apt update && sudo apt dist-upgrade -y
```

9. настроить статический сетевой интерфейс.

Внимание: При настройке файла `/etc/network/interfaces` необходимо убедиться, что Network-manager отключен, для этого ввести в терминале команду:

```
sudo systemctl status network-manager
```

Если `Network-manager` работает, то выполнить его отключение, введя в терминале команды:

```
sudo systemctl stop network-manager
sudo systemctl disable network-manager
```

Для настройки файла `/etc/network/interfaces` внести следующие изменения:

```
auto eth0
iface eth0 inet static
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
address <IP-адрес_контроллера_домена>
netmask <маска_подсети>
gateway <шлюз>
dns-nameservers <IP-адрес_dns_сервера>
dns-search <домен>```
```

Пример

```
auto eth0 iface eth0 inet static address 192.168.30.15 netmask 255.255.255.0
 ↪gateway 192.168.30.1 dns-nameservers 77.88.8.8 dns-search domain.test
```

1. применить настройки сети, выполнив команду в терминале:

```
sudo systemctl restart networking
```

3.13.3.4. Проверка корректной установки окружения с установочного диска

Перед установкой клиентской части ПК «ALD Pro» следует проверить корректность настроек, а именно:

1. на компьютере объем оперативной памяти не менее 4 ГБ;
2. на сервере первого контроллера домена ОС Astra Linux функционирует на максимальном уровне защищенности. Для проверки необходимо от имени пользователя, имеющего нужные возможности по администрированию, выполнить в терминале команду:

```
sudo astra-modeswitch get
```

Результат выполнения команды должен быть: *2*

3. в файле `/etc/hostname` указано корректное имя сервера контроллера домена в формате FQDN;
4. в файле `/etc/hosts` указаны корректные данные первого контроллера домена;
5. в файле `/etc/apt/sources.list` указаны репозитории ОС Astra Linux и ПК «ALD Pro»;
6. для ПК «ALD Pro» присутствует файл `/etc/apt/preferences.d/aldpro`,

определяющий его приоритет;

7. сетевой интерфейс первого контроллера домена настроен на статический IP-адрес.
8. проверить доступность dl.astralinux.ru с сервера первого контроллера домена, выполнив в терминале команду:

```
ping -c 3 dl.astralinux.ru
```

3.13.3.5. Установка клиентской части ПК «ALD Pro» на компьютер

На компьютер, подготовленном для развертывания клиентской части ПК «ALD Pro», необходимо выполнить в терминале команду:

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

3.13.3.6. Настройка клиентской части ПК «ALD Pro»

Для настройки клиентской части ПК «ALD Pro» необходимо:

1) выполнить в терминале команду:

```
sudo /opt/rbta/aldpro/mp/bin/aldpro-server-install.sh -d -n -p –ip –no-reboot
```

где в качестве значения *<пароль_администратора_домена>* указывается пароль, установленный при настройке первого контроллера домена, в соответствии с описанием РДЦП.10101-01 95 01 «Программный комплекс «ALD Pro». Руководство администратора. Инструкция по развертыванию».

Внимание: При вводе имени контроллера домена не допускается использование заглавных букв. Кроме того, в случае планирования настройки доверительных отношений с MS AD версий 2016 и 2019, не допускается использование символов дефис (-) или тире (—).

При вводе значения пароля недопустимо использование символа «$», а минимальное количество символов должно быть не менее девяти.

Пример

```
sudo /opt/rbta/aldpro/mp/bin/aldpro-server-install.sh -d domain.test -n dc -
↪p GTtfjtg27 –ip 192.168.30.15 –no-reboot \``\`
```

При запуске данной команды выполняется ввод клиента ПК «ALD Pro» в домен и настройка подсистем;

1) для гарантированного применения всех выполненных изменений требуется перезагрузить компьютер.

3.13.3.7. Установка на компьютер ОС по сети с использованием портала управления ПК «ALD Pro»

При добавлении и настройке клиентов ПК «ALD Pro» для автоматизации процесса рекомендуется использовать скрипты, примеры которых приведены во вкладке *Редактирование профиля загрузки* (раздел *Автоматизация*, подраздел *Установка ОС по сети*).

3.14. Создание сервисной учетной записи для почтового сервиса RuPost

3.14.1. Введение

Добавление сервисной учетной записи для почтового сервиса RuPost необходимо для обеспечения интеграции ALD Pro и RuPost.

3.14.2. Создание сервисной УЗ

Для создания сервисной учетной записи для RuPost необходимо:

1. Под учетной записью с ролью главный администратор (ALDPRO - Main Administrator) или с любой ролью (без ограничений по подразделениям — с привязкой к корню домена), содержащей привилегию на создание пользователей, выполнить вход на рабочую станцию, которая выполняет роль мастер контроллер домена. При этом у

данного администратора должны быть права sudo на первом контроллере домена. Управление ролями системы описано в разделе *Роли и права доступа* подразделе types_of_administrator

2. В командной строке выполнить команду по созданию сервисной учетной записи RuPost, указав любые корректные значения имени и пароля

```
sudo -i
kinit <логин администратора из п.1>
sudo /opt/rbta/venvs/aldpro-common/bin/python3 /opt/rbta/ad/mgmtportal/api/
↪core/manage.py rupostadmin add -u user -p password
```

Пример

```
sudo /opt/rbta/venvs/aldpro-common/bin/python3 /opt/rbta/ad/mgmtportal/api/
↪core/manage.py rupostadmin add -u rupostservice -p @qazWSX1
```

3.15. Инструкция по настройке журналирования событий

3.15.1. Область применения

Данная инструкция в полном объеме актуальна для домена, в котором на контроллерах домена установлена операционная система (ОС) Astra Linux 1.7.4 или выше, а также установлен ALD Pro версией выше 2.0.0.

3.15.2. Термины и определения

Термин	Эквивалент	Определение
Контроллер домена	КД	Сервер, который контролирует определенную область компьютерной сети, а также управляет доступом к различным ресурсам внутри этой области
Логи	Журналы событий	Записи о различных событиях, происходящих в системе и пр.
Хронологический порядок		Упорядоченное по дате и времени расположение (хранение) событий
Журналирование событий		Автоматическая запись информации о событиях, происходящих с некоторым объектом. Ведется в хронологическом порядке. Записывается в локальные файлы, базу данных и т.д. Используется для последующей обработки
Сервер аудита		Компьютер из состава домена ALD Pro, на котором развернута подсистема аудита
Security Information and Event Management	SIEM	Инструменты для сбора, анализа, интерпретации и управления информацией об активности в информационной системе, чтобы обнаруживать и предотвращать угрозы безопасности

продолжение на следующей странице

Таблица 3.19 – продолжение с предыдущей страницы

Термин	Эквивалент	Определение
Служба каталога		Средство иерархического представления ресурсов и информации об этих ресурсах
Uniform Resource Locator	URL	Уникальный адрес ресурса, в котором должны быть специфицированы как минимум протокол и доменное имя ресурса. Также опционально могут быть заполнены и другие части адреса: путь и параметры
Lightweight Directory Access Protocol	LDAP	Протокол прикладного уровня для доступа к службе каталогов, разработанный как облегчённый вариант протокола DAP. LDAP — относительно простой протокол, использующий TCP/IP и позволяющий производить операции аутентификации (*bind*), поиска (*search*) и сравнения (*compare*), а также операции добавления, изменения или удаления записей
SSH	Secure SHell	Сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений

продолжение на следующей странице

Таблица 3.19 – продолжение с предыдущей страницы

Термин	Эквивалент	Определение
Samba		Пакет программ, которые позволяют обращаться к сетевым дискам и принтерам на различных операционных системах по протоколу SMB/CIFS
DNS	Domain Name System	Система доменных имён — это иерархическая децентрализованная система именования для ресурсов, подключённых к глобальной сети, которая ведёт список доменных имён вместе с их числовыми IP-адресами или местонахождениями

продолжение на следующей странице

Таблица 3.19 – продолжение с предыдущей страницы

Термин	Эквивалент	Определение
Kerberos		Сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними. Kerberos выполняет аутентификацию в качестве службы аутентификации доверенной третьей стороны, используя криптографический ключ. Kerberos построен на криптографии симметричных ключей и требует наличия центра распределения ключей. Расширения Kerberos могут обеспечить использование криптографии с открытым ключом на определённых этапах аутентификации
Тэг	TAG (tag)	Произвольная строка, используемая для фильтрации информации в журналах

продолжение на следующей странице

Таблица 3.19 – продолжение с предыдущей страницы

Термин	Эквивалент	Определение
Пути журналов	(Log paths)	Сочетание источников, мест назначения и других объектов, таких как фильтры, синтаксические анализаторы и правила перезаписи. Приложение syslog-ng отправляет сообщения, поступающие из источников путей журнала, в определенные пункты назначения, а также выполняет фильтрацию, анализ и перезапись сообщений. Пути журналов также называются операторами журнала. Операторы могут включать другие (встроенные) операторы журнала и соединения для создания сложных путей журнала
Источник	source	Именованная коллекция сконфигурированных исходных драйверов
Internet Protocol	IP	Маршрутизируемый протокол сетевого уровня стека TCP/IP. Именно IP стал тем протоколом, который объединил отдельные компьютерные сети во всемирную сеть Интернет. Неотъемлемой частью протокола является адресация сети

продолжение на следующей странице

Таблица 3.19 – продолжение с предыдущей страницы

Термин	Эквивалент	Определение
IP-адрес		Уникальный числовой идентификатор устройства в компьютерной сети, работающей по протоколу IP
DoS-атака	denial-of-service attack	Атака типа «отказ в обслуживании» — хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён. Отказ системы может быть только первым шагом к овладению системой (если в нештатной ситуации ПО выдаёт какую-либо критическую информацию — например, версию, часть программного кода и т. д.)

продолжение на следующей странице

Таблица 3.19 – продолжение с предыдущей страницы

Термин	Эквивалент	Определение
ACL	access control list	Список управления доступом, который определяет, кто или что может получать доступ к объекту (программе, процессу или файлу), и какие именно операции разрешено или запрещено выполнять субъекту (пользователю, группе пользователей). Списки контроля доступа являются основой систем с избирательным управлением доступа (DAC)
DAC	discretionary access control	Управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа. Также используются названия: • дискреционное управление доступом; • контролируемое управление доступом; • разграничительное управление доступом.

3.15.3. Описание

Подсистема аудита ALD Pro реализует централизованный сбор событий служб контроллеров домена в коллекторе, которым выступает сервер аудита, и собранные данные могут в дальнейшем передаваться в систему управления информационной безопасностью и событиями безопасности (SIEM) для дальнейшего анализа.

Журнал событий в ALD Pro для версии 2.0.0 и выше основан на open source решении Syslog-ng и позволяет собирать информацию на сервере журнала событий о следующих событиях безопасности:

1. логи авторизации Fly;
2. логи удаленного подключения;
3. логи состояния подключения к сети.

Подробности о работе с журналом событий из портала управления ALD Pro версией 2.0.0 и выше можно найти в разделе «Журнал событий» Справочного центра.

В ALD Pro не предусмотрено расширение списка регистрируемых событий средствами графического интерфейса портала управления. Данная инструкция содержит необходимую информацию о действиях администратора и настройках, которые которые необходимо сделать на каждом контроллере домена и сервере аудита под управлением ALD Pro. После выполнения этой настройки будет включено журналирование событий и осуществлен сбор журналов на сервере аудита, что позволяет значительно увеличить количество регистрируемых и собираемых на сервере аудита событий безопасности. Кроме того, собираемую на сервере аудите информацию о событиях безопасности можно отправить в стороннюю SIEM (см. скрипт для отправки в разделе 7.1).

Перечень событий безопасности, которые собираются в журналах событий на контроллерах домена и информация о которых перенаправляется на сервер аудита с помощью данной инструкции, приведен в таблице ниже. Для корректного отображения в таблице эквивален собития в Active Directory указан без знака нижнего подчеркивания между словами.

	Наименование события	Эквивалент события в Active Directory (при наличии)	Примечание
1	Подключение к рабочему столу Fly	4624 An account was successfully logged_on	См. раздел 5.1
2	Ввод некорректных данных аутентификации при подключении к рабочему столуFly	4625 An account failed to log on	См. раздел 5.1
3	Отключение сессии рабочего стола Fly		См. раздел 5.1
4	Вход (подключение) по SSH	4624 An account was successfully logged on	См. раздел 5.1
5	Ввод некорректных данных аутентификации при подключении поSSH	4625 An account failed to log on	См. раздел 5.1
6	Завершение сессии SSH		См. раздел 5.1
7	Чтение информации из службы каталога	1644_ldap_query	См. раздел 5.2
8	Создание нового пользователя (группы) в LDAP	4720 A user account was created	См. раздел 5.2
9	Изменение пользователя (группы)	4738 A user account was changed	См. раздел 5.2
10	Удаление пользователя (группы)		См. раздел 5.2
11	Ввод в домен нового компьютера	4741 A computer account was created	См. раздел 5.2
12	Изменение параметров компьютера в домене	4742 A computer account was changed	См. раздел 5.2

продолжение на следующей странице

Таблица 3.20 – продолжение с предыдущей страницы

	Наименование события	Эквивалент события в Active Directory (при наличии)	Примечание
13	Удаление компьютера из домена		См. раздел 5.2
14	Запрос объекта службы каталога (для CRUD операций)	4661 The handle to an object was requested	См. раздел 5.2
15	Создание новой реплики путем продвижения сервера до контроллера домена	4928 Active Directory replica source naming context established	См. раздел 5.2
16	Удаление контроллера домена, в процессе чего удаляется реплика	4929 Active Directory replica source naming context removed	См. раздел 5.2
17	Добавление и удаление ролей	5136 A directory service object was modified	См. раздел 5.2
18	Доступ к файлам в службе Samba	5145 A network share object was_checked	См. раздел 5.3
19	Ошибка при попытке переноса зоны DNS	6001 dns server successfully completed transfer of zone version	См. раздел 5.4
20	Успешный перенос зоны DNS	6001 dns server successfully completed transfer of zone version	См. раздел 5.4
21	Запрос билета подлинности службы Kerberos	4768 A Kerberos authentication ticket was requested	См. раздел 5.5
22	Запрос билета TGS службы Kerberos	4769 Kerberos service ticket requested	См. раздел 5.5

продолжение на следующей странице

Таблица 3.20 – продолжение с предыдущей страницы

	Наименование события	Эквивалент события в Active Directory (при наличии)	Примечание
23	Сбой при предварительной проверке подлинности Kerberos	4771 Kerberos pre authentication failed	См. раздел 5.5
24	Создание и запуск нового процесса пользователем	4688 A new process has been created	См. раздел 5.6
25	Подключение к каталогу LDAP	5156 WFP has permitted connection	См. раздел 5.7

3.15.4. Системные требования

1. Для корректной работы всех описанных ниже сценариев необходимо, чтобы на всех контроллерах домена и серверах аудита была установлена операционная система Astra Linux 1.7.4 или выше. В операционной системе Astra Linux версий **до** версии 1.7.4 используются другие версии пакета службы каталога и включение расширенных атрибутов с помощью команды «`dsconf`» с опцией `config replace nsslapd-auditlog-display-attrs=*` невозможно (выполнение завершается ошибкой). Остальные пункты инструкции выполняются без изменений. Расширенные атрибуты журнала аудита службы каталога - это атрибуты, начинающиеся с символа «#».

2. Для применения настоящей инструкции предварительно необходимо:

- выполнить установку ALD Pro версии 2.0.0 (или выше);
- настроить домен под управлением данного продукта (настроить согласно «Руководству администратора ALD Pro»);
- развернуть подсистему аудита в домене.

3.15.5. Настройка журналирования событий безопасности на КД и сбор данных журналов на сервере аудита

3.15.5.1. Настройка журналирования событий из интерфейса портала управления

На портале управления ALD Pro версии 2.0.0 и выше есть возможность включить правила для настройки сборов журналов событий на сервере аудита из состава домена с помощью syslog-ng. Для этого в разделе портала управления «Журнал событий → Настройка сбора журналов событий → Новое правило» необходимо заполнить обязательные поля «Имя правила» (произвольная строка для администратора), «Сервер сбора логов» (выбрать из списка компьютер с развернутой подсистемой аудита) и «Тип логов» (выбрать из списка тип события, информация о котором будет собираться).

Для поля «Тип логов» доступны следующие значения:

- «Логи авторизации Fly» — сбор информации о входе пользователей в графический интерфейс клиентов домена (в том числе ввод некорректных данные при авторизации пользователей домена);
- «Логи удаленного подключения» — сбор информации обо всех удаленных подключениях к клиентам домена по протоколу ssh (в том числе ввод некорректных данные при авторизации пользователей домена);
- «Логи состояния подключения к сети» — сбор информации о состоянии подключения к сети всех клиентов домена.

Более подробно настройка журналирования и сборов событий на сервере аудита из интерфейса портала управления изложена в Справочном центре портала управления ALD Pro в разделе «Журнал событий».

3.15.5.2. Настройка журналирования событий службы каталога

Настройка журналирования событий службы каталога на контроллере домена

Все описания настройки журналов в разделах 5.2.1, 5.3.1, 5.4.1, 5.5.1, 5.6.1, 5.7.1 (для каждого КД или сервера общего доступа к файлам из состава домена) и 5.2.2, 5.3.2, 5.4.2, 5.5.2, 5.6.2, 5.7.2 (для сервера аудита) написаны как полностью независимые блоки (то есть каждый раздел 5.2.x, где x - [1,2], можно настраивать полностью самостоятельно), поэтому внутри каждого из разделов идет пункт о перезапуске сервиса `syslog-ng`.

Однако если инструкция применяется целиком, то можно последовательно выполнить все пункты 5.x.1 (где x - [2-7]) для КД и затем перезапустить сервис `syslog-ng` на данном КД или сервере общего доступа к файлам один раз. Затем повторить для следующего КД и т.д.

Затем можно последовательно выполнить все пункты 5.x.2 (где x - [2-7] или какой-то другой набор настроек, которые должны совпадать с настройками соответствующих пунктов на КД) для сервера аудита и перезапустить сервис `syslog-ng` один раз на сервере аудита.

Можно обратиться к разделу 8, где указаны последовательно все команды для полной настройки КД и сервера общего доступа к файлам, а также сервера аудита для сбора всех журналов по данной инструкции.

Во всех командах и примерах далее в документе:

- `ldap://alddc1.ald.lan` - URL в LDAP контроллера домена ALD Pro, на котором требуется включить расширенный аудит;
- `ALDPRO-LAN` - наименование домена ALD Pro, на котором происходит настройка правил;
- `ПАРОЛЬ_АДМИНИСТРАТОРА` - вместо данной строки должен использоваться реальный пароль администратора (пользователя с правами на конфигурацию служб) конкретного КД;
- `100.100.100.100` - IP-адрес компьютера (возможно использование и доменного имени компьютера, но предпочтительно использовать IP-адрес), с развернутой подсистемой аудита.

Перед выполнением команд по конфигурации службы каталога можно выключить запись истории команд в командной строке, чтобы пароль администратора или другого привилегированного пользователя не сохранялся в истории, или же использовать другие способы (например, не использовать ключ «-w», тогда после ввода каждой команды потребуется ввод пароля администратора, помимо этого, можно использовать переменные среды в командах ниже, куда предварительно необходимо внести нужную информацию).

Ниже приведен минимальный алгоритм включения и настройки файлов журналов службы каталога для выполнения настоящей инструкции. Более подробная информация про назначение журналов службы каталога `389 DS`, настройку отображения файлов журналов, а также настройку ротации файлов журналов приведена в разделе 6.1 настоящей инструкции.

Расширенный аудит на сервере службы каталога включается вручную, после чего станет доступен файл журнала аудита `/var/log/dirsrv/slapd-ALDPRO-LAN/audit`.

Команда для включения расширенного аудита на контроллере домена:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
 ↪lan config replace nsslapd-auditlog-logging-enabled=on
```

Расширенный аудит ошибок включается вручную, записи добавляются в общий файл расширенного аудита, который должен быть включён предыдущей командой.

Команда для включения расширенного аудита ошибок на контроллере домена:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
 ↪lan config replace nsslapd-auditfaillog-logging-enabled=on
```

Для включения записи в журнал аудита **основных** расширенных атрибутов операций необходимо добавить в конфигурационный файл службы каталога специальную запись с помощью команды ниже (работает для версии Astr Linux SE 1.7.4 или выше, см. раздел 4 настоящей инструкции). Данная команда должна быть введена без пробелов и переносов строк.

Команда для включения записи в журнал аудита службы каталогов расширенных атрибутов операции:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
 ↪lan config replace nsslapd-auditlog-display-attrs=loginShell,krbExtraData,
 ↪krbLastPwdChange,krbPasswordExpiration,
x-ald-user-mac,uid,displayName,initials,gecos,sn,homeDirectory,mail,
 ↪krbPrincipalName,krbCanonicalName,givenName,rbtamiddlename,street,l,st,
 ↪postalCode,c,employeeNumber,telephoneNumber,title,rbtadp,rbtaou,
entyusn,modifyTimestamp,modifiersName,objectClass,ipaNTSecutityIdentifier,cn,
 ↪creatorsName,createTimestamp,modifyTimestamp,nsUniqueId,ipaUniqueId,
 ↪parentid,entryid,uidNumber,gidNumber,entryUUID,dsEntryDN,entrydn
```

Расширенный аудит безопасности включается вручную, после чего станет доступен файл журнала аудита событий безопасности `/var/log/dirsrv/slapd-ALDPRO-LAN/security`.

Команда для включения аудита безопасности на контроллере домена:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
 ↪lan config replace nsslapd-securitylog-logging-enabled=on
```

Примечание: Администратору необходимо настроить ротацию журналов на контроллерах домена и сервере аудита (смотри раздел 6 настоящей инструкции), поскольку размеры журналов будут достаточно большими и возможно полное заполнение ими дискового пространства!

После выполнения необходимых настроек службы каталога для журналирования событий с необходимым в каждом конкретном случае уровнем детальности, требуется провести настройку службы `syslog-ng` для перенаправления с её помощью информации на сервер аудита из логов службы каталога.

Для предварительной настройки службы `syslog-ng` на контроллере домена необходимо:

1. Создать дополнительный каталог `/etc/syslog-ng/siem`;
2. В файле конфигурации `/etc/syslog-ng/syslog-ng.conf` добавить строку для подключения конфигураций службы:

```
@include "/etc/syslog-ng/siem/*.conf"
```

Для выполнения настройки службы `syslog-ng` для пересылки журналов службы каталога на контроллере домена необходимо выполнить следующую последовательность действий (создать набор путей журналов):

1. Настроить единую точку пересылки журналов на сервер аудита в службе `syslog-ng` .
2. Настроить перенаправление журнала доступа службы каталога в точку пересылки журналов в службе `syslog-ng` .
3. Настроить перенаправление журнала аудита службы каталога в точку пересылки журналов в службе `syslog-ng` .
4. Настроить перенаправление журнала ошибок службы каталога в точку пересылки журналов в службе `syslog-ng` .
5. Настроить перенаправление журнала событий безопасности службы каталога в точку пересылки журналов в службе `syslog-ng` .

Для настройки точки пересылки журналов в службе `syslog-ng` необходимо создать файл конфигурации `/etc/syslog-ng/siem/destination.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию (ip-адрес сервера аудита из состава домена):

```
destination d_audit {
    network("100.100.100.100" transport("tcp") port(514) flags(syslog-
↪protocol) template("${ISODATE} ${HOST} ${MESSAGE} ${TAGS}\n"));
};
```

Где `100.100.100.100` - IP-адрес компьютера с развернутой *подсистемой аудита*.

Примечание: При настройке пересылки различных журналов в один и тот же пункт назначения (destination) в службе `syslog-ng` возникает ошибка дубликатов. Для устранения данной ошибки можно воспользоваться директивой `@define allow-config-dups 1`, которую необходимо добавить в начало конфигурационного файла `/etc/syslog-ng/syslog-ng.conf`. Однако данную директиву необходимо применять с осторожностью, поскольку, если дубликаты пунктов назначения содержат различные настройки, то во всех случаях будет использоваться последний встреченный `syslog-ng` вариант. Что может привести к нежелательному поведению для тех источников, которые были настроены с помощью первого из дубликатов. Администратору рекомендуется разобраться с настройкой пунктов назначения и не использовать директиву `@define allow-config-dups 1` без детального понимания ее необходимости.

Для настройки фильтрации записей в журнале доступа к службе каталога на КД и последующего перенаправления отфильтрованных записей в точку пересылки журналов в службе `syslog-ng` необходимо создать файл конфигурации `/etc/syslog-ng/siem/output-dirsrv-access.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
source s_access_dirsrv {
    file("/var/log/dirsrv/slapd-ALDPRO-LAN/access" follow-freq(1) flags(no-
↪parse));
};

filter f_access_dirsrv {
    match("MOD" value("MESSAGE")) or match("DEL" value("MESSAGE")) or match(
↪"ADD" value("MESSAGE")) or match("SRCH" value("MESSAGE")) or match(
↪"connection from" value("MESSAGE")) or match("RESULT" value("MESSAGE"));
};

log {
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
    source(s_access_dirsrv);
    filter(f_access_dirsrv);
    rewrite
    {
            set-tag("tag-dirsrv-access");
    };
    destination(d_audit);
};
```

Для настройки перенаправления журнала аудита к службе каталога в точку пересылки журналов в службе `syslog-ng` необходимо создать файл конфигурации `/etc/syslog-ng/siem/output-dirsrv-audit.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
source s_audit_dirsrv {
    file("/var/log/dirsrv/slapd-ALDPRO-LAN/audit" follow-freq(1) flags(no-
↪parse) );
};

log {
    source(s_audit_dirsrv);
    rewrite
    {
            set-tag("tag-dirsrv-audit");
    };
    destination(d_audit);
};
```

Поскольку информация в журнал аудита (и в журнал ошибок аудита) службы каталога попадает в формате `ключ: значение\n` и к одному событию может быть достаточно большое количество таких пар, то для объединения всех таких записей от одного события в одну строку (flags(no-multi-line)) можно использовать следующий файл конфигурации (`/etc/syslog-ng/siem/output-dirsrv-audit.conf`):

```
source s_audit_dirsrv {
    file("/var/log/dirsrv/slapd-ALDPRO-LAN/audit"  multi-line-mode(prefix-
↪suffix) multi-line-prefix("time: [0-9]+") multi-line-suffix("\n$") flags(no-
↪multi-line) follow-freq(1));
};
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
log {
    source(s_audit_dirsrv);
    rewrite
    {
        subst("^", "time: ", value("MESSAGE"));
        set-tag("tag-dirsrv-audit");
    };
    destination(d_audit);
};
```

Для настройки перенаправления журнала ошибок службы каталога в точку пересылки журналов в службе `syslog-ng` необходимо создать файл конфигурации `/etc/syslog-ng/siem/output-dirsrv-error.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
source s_errors_dirsrv {
    file("/var/log/dirsrv/slapd-ALDPRO-LAN/errors" follow-freq(1) flags(no-
↪parse));
};

log {
    source(s_errors_dirsrv);
    rewrite
    {
            set-tag("tag-dirsrv-error");
    };
    destination(d_audit);
};
```

Для настройки перенаправления журнала событий безопасности службы каталога в точку пересылки журналов в службе `syslog-ng` необходимо создать файл конфигурации `/etc/syslog-ng/siem/output-dirsrv-security.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
source s_security_dirsrv {
    file("/var/log/dirsrv/slapd-ALDPRO-LAN/security" follow-freq(1) flags(no-
↪parse));
};
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
log {
    source(s_security_dirsrv);
    rewrite
    {
            set-tag("tag-dirsrv-security");
    };
    destination(d_audit);
};
```

Функция `subst` в данной инструкции используется в файлах конфигурации двумя способами:

- заменяет первый указанный параметр (в нашем случае это строка с наименованием тэга и источника) вторым параметром (в нашем случае это пустая строка) внутри значения, указанного третьим параметром (в нашем случае это текст сообщения соответствующего журнала событий службы каталога);
- заменяет первый указанный параметр (в нашем случае это регулярное выражение, следовательно заменяется строка, которая соответствует этому регулярному выражению) вторым параметром (в нашем случае это пустая строка), затем идет указание типа регулярного выражения (в нашем случае это `type``("``pcre»), где `pcre - perl compartible regular expression`), внутри значения, указанного четвертым параметром (в нашем случае это текст сообщения соответствующего журнала событий службы каталога).

Более подробную информацию по конфигурации службы `syslog-ng` можно посмотреть в справке операционной системы Astra Linux с помощью команды «`man syslog-ng.conf`».

Во всех примерах в данном разделе и ниже в настоящем документе наименования папок и файлов могут задаваться администратором самостоятельно и находиться в других каталогах операционной системы в соответствии с настройками службы `syslog-ng` . Значение параметра `set-tag` для каждого типа лога может быть любым, но именно это значение необходимо использовать при настройки перенаправления событий в соответствующий журнал на сервере аудита из состава домена (смотри раздел 5.2.2).

После выполнения действий необходимо перезапустить службу `syslog-ng` на контроллере домена с помощью следующей команды:

```
systemctl restart syslog-ng
```

Настройка журналирования событий службы каталога на сервере аудита

После выполнения необходимых настроек на контроллере домена, требуется провести настройку службы `syslog-ng` на сервере аудита из состава домена для сбора с помощью нее информации с контроллера домена.

Для предварительной настройки службы `syslog-ng` на сервере аудита необходимо:

1. Создать дополнительный каталог `/etc/syslog-ng/siem`;
2. В файле конфигурации `/etc/syslog-ng/syslog-ng.conf` добавить строку для подключения конфигураций службы:

```
@include "/etc/syslog-ng/siem/*.conf"
```

Для настройки службы `syslog-ng` на сервере аудита необходимо выполнить следующую последовательность действий (каждый пункт из списка ниже сопоставляется с соответствующим пунктом раздела 5.1.1):

1. Настроить точку сбора журналов в службе `syslog-ng` .
2. Настроить перенаправление по тегу журнала доступа службы каталога в журнал службы `syslog-ng` .
3. Настроить перенаправление по тегу журнала аудита службы каталога в журнал службы `syslog-ng` .
4. Настроить перенаправление по тегу журнала ошибок службы каталога в журнал службы `syslog-ng` .
5. Настроить перенаправление по тегу журнала событий безопасности службы каталога в журнал службы `syslog-ng` .

Перед выполнением следующего пункта необходимо убедиться, что источник «`source s_net`» не был создан предварительно (например при настройке сбора журналов на сервере аудита из портала управления). Для этого необходимо осуществить поиск подстроки «`source s_net`» по всем каталогам в файлах «*.conf», в которых служба `syslog-ng` читает файлы конфигурации (пути к каталогам начинаются с символа «@» и

чаще всего находятся в файле `/etc/syslog-ng/syslog-ng.conf`). Если такой источник был найден и совпадает с приведенным ниже, то следующий пункт по созданию файла `/etc/syslog-ng/siem/source.conf` не выполняется. Если же источник «`s_net`» не был найден, то тогда для настройки точки сбора журналов службы каталогов в службе `syslog-ng` на сервер аудита необходимо создать файл конфигурации `/etc/syslog-ng/siem/source.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
source s_net {
    network(
        transport("tcp")
        port(514)
        flags(syslog-protocol)
        log_iw_size(65536)
        max_connections(1000)
    );
};
```

Для настройки перенаправления по тэгу журнала доступа к службе каталога в журнал службы `syslog-ng` необходимо создать файл конфигурации этого журнала `/etc/syslog-ng/siem/input-dirsrv-access.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
destination d_access_dirsrv_file {
    file("/var/log/aldpro/access_dirsrv.log" template("${MESSAGE}\n"));
};

filter f_dirsrv_access {
    message("tag-dirsrv-access");
};

log {
    source(s_net);
    filter(f_dirsrv_access);
    rewrite {
        subst(" tag-dirsrv-access,.source.s_access_dirsrv", "", value(
↪"MESSAGE"));
    };
    destination(d_access_dirsrv_file);
};
```

Для настройки перенаправления по тэгу журнала аудита службы каталога в журнал службы `syslog-ng` необходимо создать файл конфигурации этого журнала `/etc/syslog-ng/siem/input-dirsrv-audit.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
destination d_audit_dirsrv_file {
    file("/var/log/aldpro/audit_dirsrv.log" template("${MESSAGE}\n"));
};

filter f_dirsrv_audit {
    message("tag-dirsrv-audit");
};

log {
    source(s_net);
    filter(f_dirsrv_audit);
    rewrite {
        subst(" tag-dirsrv-audit,.source.s_audit_dirsrv", "", value("MESSAGE
↪"));
    };
    destination(d_audit_dirsrv_file);
};
```

Для настройки перенаправления по тэгу журнала ошибок в службе каталога в журнал службы `syslog-ng` необходимо создать файл конфигурации этого журнала `/etc/syslog-ng/siem/input-dirsrv-error.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
destination d_error_dirsrv_file {
    file("/var/log/aldpro/error_dirsrv.log" template("${MESSAGE}\n"));
};

filter f_dirsrv_error {
    message("tag-dirsrv-error");
};

log {
    source(s_net);
    filter(f_dirsrv_error);
    rewrite {
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
        subst(" tag-dirsrv-error,.source.s_errors_dirsrv", "", value("MESSAGE
↪"));
    };
    destination(d_error_dirsrv_file);
};
```

Для настройки перенаправления по тэгу журнала событий безопасности в службе каталога в журнал службы `syslog-ng` необходимо создать файл конфигурации этого журнала `/etc/syslog-ng/siem/input-dirsrv-security.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
destination d_security_dirsrv_file {
    file("/var/log/aldpro/security_dirsrv.log" template("${MESSAGE}\n"));
};

filter f_dirsrv_security {
    message("tag-dirsrv-security");
};

log {
    source(s_net);
    filter(f_dirsrv_security);
    rewrite {
        subst(" tag-dirsrv-security,.source.s_security_dirsrv", "", value(
↪"MESSAGE"));
    };
    destination(d_security_dirsrv_file);
};
```

Во всех примерах в данном разделе и ниже в документе наименования папок и файлов задаются администратором самостоятельно и находиться в других каталогах операционной системы в соответствии с необходимыми администратору настройками. Также значение параметра `message` внутри фильтра (filter) должно совпадать с соответствующим параметром `set-tag` для каждого типа лога (смотри раздел 5.2.1).

После выполнения действий необходимо перезапустить службу `syslog-ng` на сервере аудита с помощью следующей команды:

```
systemctl restart syslog-ng
```

3.15.5.3. Настройка журналирования событий доступа к файлам в службе Samba

Настройка журналирования событий доступа к файлам в службе Samba на сервере общего доступа к файлам

Для включения записи событий доступа к файлам в службе Samba в файле конфигурации `/etc/samba/smb.conf` в секцию «global» добавить следующие строки:

```
vfs objects = full_audit
full_audit:prefix = %u|%I|%S
full_audit:success = connect, create_file, linkat, mkdirat, open, read,
↪renameat, unlinkat, write
full_audit:failure = connect, create_file, linkat, mkdirat, open, read,
↪renameat, unlinkat, write
full_audit:facility = local5
full_audit:priority = notice
```

Если в файле конфигурации `/etc/samba/smb.conf` в секции «global» присутствует следующая строка: `log level = N`, где N - это уровень журналирования событий в службе, то к данной строке дописываем через пробел строку « vfs:1». Если такой строки нет, то записываем:

```
log level = 1 vfs:1
```

После этого необходимо перезапустить службу `samba` и службу `winbind` с помощью следующей команды:

```
systemctl restart smbd winbind
```

Для предварительной настройки службы `syslog-ng` на сервере общего доступа к файлам необходимо:

1. Создать дополнительный каталог `/etc/syslog-ng/siem`;
2. В файле конфигурации `/etc/syslog-ng/syslog-ng.conf` добавить строку для подключения конфигураций службы:

```
@include "/etc/syslog-ng/siem/*.conf"
```

Для настройки службы `syslog-ng` на сервере общего доступа к файлам необходимо выполнить следующую последовательность действий:

1. Настроить единую точку пересылки журналов на сервер аудита в службе `syslog-ng` .
2. Настроить перенаправление журнала службы Samba в точку пересылки журналов в службе `syslog-ng` .

Для настройки точки пересылки журналов в службе `syslog-ng` необходимо создать файл конфигурации `/etc/syslog-ng/siem/destination.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
destination d_audit {
    network("100.100.100.100" transport("tcp") port(514) flags(syslog-
↪protocol) template("${ISODATE} ${HOST} ${PROGRAM} ${MESSAGE} ${TAGS}\n"));
};
```

Где 100.100.100.100 - IP-адрес компьютера, с развернутой подсистемой аудита.

Для настройки перенаправления записей о доступе к файловым ресурсам службы Samba из системного журнала в точку пересылки журналов в службе `syslog-ng` необходимо создать файл конфигурации `/etc/syslog-ng/siem/output-samba.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
filter f_smbd {
    program('smbd_audit');
};

log {
    source(s_src);
    filter(f_smbd);
    destination(d_audit);
};
```

Примечание: Источник source(s_src) описан в файле /etc/syslog-ng/syslog-ng.conf.

После выполнения настроек необходимо перезапустить службу `syslog-ng` на сервере

общего доступа к файлам с помощью следующей команды:

```
systemctl restart syslog-ng
```

Настройка журналирования событий доступа к файлам в службе Samba на сервере аудита

Далее приведена настройка файлов конфигурации службы `syslog-ng` на сервере аудита. Если предварительная настройка службы `syslog-ng`, а также если настройка точки сбора журналов в службе `syslog-ng` (создание файла конфигурации `/etc/syslog-ng/siem/source.conf`) не выполнялись, то необходимо произвести настройки в соответствии с описанием в разделе 5.2.2 настоящей инструкции. Затем необходимо создать набор файлов конфигурации для фильтрации событий службы samba.

Для настройки журнала службы samba в службе `syslog-ng` на сервере аудита необходимо создать файл `/etc/syslog-ng/siem/input-samba.conf` с правами на чтение всем пользователям и внести в этот файл следующую информацию:

```
destination d_samba {
    file("/var/log/aldpro/samba.log" template("${MESSAGE}\n"));
};

filter f_samba {
    message("smbd_audit");
};

log {
    source(s_net);
    filter(f_samba);
    rewrite {
        subst(" .source.s_src", "", value("MESSAGE"));
    };
    destination(d_samba);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на сервере аудита с помощью следующей команды:

```
systemctl restart syslog-ng
```

3.15.5.4. Настройка журналирования событий переноса зоны DNS

Настройка журналирования событий переноса зоны DNS на контроллере домена

Настройка журналирования событий переноса зоны DNS на контроллере домена выполняется после предварительной настройки службы `syslog-ng`, а также настройки точки пересылки журналов в службе `syslog-ng` (создание файла конфигурации `/etc/syslog-ng/siem/destination.conf`) в соответствии с описанием в разделе 5.2.1 настоящей инструкции (если такая настройка не проводилась ранее). Затем необходимо создать файл конфигурации для фильтрации событий переноса зоны DNS.

Для настройки журналирования событий переноса зоны на контроллере домена необходимо создать файл конфигурации `/etc/syslog-ng/siem/output-dns-zone.conf` с правами на чтение для всех пользователей и внести в него следующую информацию:

```
filter f_dnszone {
    message('AXFR') or message('IXFR');
};

log {
    source(s_src);
    filter(f_dnszone);
    destination(d_audit);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на контроллере домена с помощью следующей команды:

```
systemctl restart syslog-ng
```

Настройка журналирования событий переноса зоны DNS на сервере аудита

Настройка журналирования событий переноса зоны DNS на сервере аудита выполняется после предварительной настройки службы `syslog-ng`, а также настройки точки сбора

журналов в службе `syslog-ng` (создание файла конфигурации /etc/syslog-ng/siem/source.conf) в соответствии с описанием в разделе 5.2.2 настоящей инструкции (если такая настройка не проводилась ранее). Затем необходимо создать файл конфигурации для фильтрации событий переноса зоны DNS.

Для настройки журналирования событий переноса зоны на сервере аудита необходимо создать файл конфигурации `/etc/syslog-ng/siem/input-dns-zone.conf` с правами на чтение для всех пользователей и внести в него следующую информацию:

```
destination d_dnszone {
    file("/var/log/aldpro/dnszone.log" template("${MESSAGE}\n"));
};

filter f_dnszone {
    message('AXFR') or message('IXFR');
};

log {
    source(s_net);
    filter(f_dnszone);
    rewrite {
        subst(" .source.s_src", "", value("MESSAGE"));
    };
    destination(d_dnszone);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на сервере аудита с помощью следующей команды:

```
systemctl restart syslog-ng
```

3.15.5.5. Настройка журналирования событий Kerberos

Настройка журналирования событий Kerberos на контроллере домена

На первом этапе необходимо настроить службу `Kerberos`. Для этого необходимо:

1. В файле `/lib/systemd/system/krb5-kdc.service` в параметр `ReadWriteDirectories` добавить `/var/log`;

2. Перечитать файл: `systemctl daemon-reload`;

3. Перезапустить службу: `systemctl restart krb5-kdc.service`.

Настройка журналирования событий `Kerberos` на контроллере домена выполняется после предварительной настройки службы `syslog-ng`, а также настройки точки пересылки журналов в службе `syslog-ng` (создание файла конфигурации `/etc/syslog-ng/siem/destination.conf`) в соответствии с описанием в разделе 5.2.1 настоящей инструкции (если такая настройка не проводилась ранее). Затем необходимо создать файл конфигурации для фильтрации событий `Kerberos`.

Для настройки журналирования событий Kerberos на контроллере домена необходимо создать файл конфигурации `/etc/syslog-ng/siem/output-krb-audit.conf` с правами на чтение для всех пользователей и внести в него следующую информацию:

```
source s_krb_audit {
    file("/var/log/krb5kdc.log" follow-freq(1) flags(no-parse) );
};

filter f_krb_audit {
    match("AS_REQ" value("MESSAGE")) or match("TGS_REQ" value("MESSAGE"));
};

log {
    source(s_krb_audit);
    filter(f_krb_audit);
    rewrite
    {
        set-tag("tag-krb-audit");
    };
    destination(d_audit);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на контроллере домена с помощью следующей команды:

```
systemctl restart syslog-ng
```

Настройка журналирования событий Kerberos на сервере аудита

Настройка журналирования событий Kerberos на сервере аудита выполняется после предварительной настройки службы `syslog-ng`, а также настройки точки сбора журналов в службе `syslog-ng` (создание файла конфигурации `/etc/syslog-ng/siem/source.conf`) в соответствии с описанием в разделе 5.2.2 настоящей инструкции (если такая настройка не проводилась ранее). Затем необходимо создать файл конфигурации для фильтрации событий Kerberos.

Для настройки журналирования событий `Kerberos` на контроллере домена необходимо создать файл конфигурации `/etc/syslog-ng/siem/input-krb-audit.conf` с правами на чтение для всех пользователей и внести в него следующую информацию:

```
destination d_krb_audit_file {
    file("/var/log/aldpro/krb_audit.log" template("${MESSAGE}\n"));
};

filter f_krb_audit {
    message("tag-krb-audit");
};

log {
    source(s_net);
    filter(f_krb_audit);
    rewrite {
        subst(" tag-krb-audit,.source.s_krb_audit", "", value("MESSAGE"));
    };
    destination(d_krb_audit_file);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на сервере аудита с помощью следующей команды:

```
systemctl restart syslog-ng
```

3.15.5.6. Настройка журналирования событий создания и запуска нового процесса пользователем

Настройка журналирования событий создания и запуска нового процесса пользователем на контроллере домена

Для настройки журналирования событий создания и запуска нового процесса пользователем на контроллере домена необходимо создать файл `/etc/audit/rules.d/siem.rules` со следующим содержимым (или добавить в этот файл следующие строки, если он уже создан):

```
-a always,exit -F arch=b32 -S execve -F auid>=1000
-a always,exit -F arch=b64 -S execve -F auid>=1000
```

Внести в файл /etc/audit/audit.conf следующее изменение (для установки максимального размера файла `/var/log/audit/audit.log` в мегабайтах):

```
max_log_file = 500
```

И перезапустить службу `auditd` следующей командой:

```
systemctl restart auditd
```

Настройка журналирования событий создания и запуска нового процесса пользователем на контроллере домена выполняется после предварительной настройки службы `syslog-ng`, а также настройки точки пересылки журналов в службе `syslog-ng` (создание файла конфигурации `/etc/syslog-ng/siem/destination.conf`) в соответствии с описанием в разделе 5.2.1 настоящей инструкции (если такая настройка не проводилась ранее). Затем необходимо создать файл конфигурации для фильтрации событий создания и запуска нового процесса пользователем.

Для настройки журналирования событий создания и запуска нового процесса пользователем на контроллере домена необходимо создать файл конфигурации `/etc/syslog-ng/siem/output-user-proc.conf` с правами на чтение для всех пользователей и внести в него следующую информацию:

```
source s_user_proc {
    file("/var/log/audit/audit.log" flags(no-parse) persist-name("user_proc
↪") follow-freq(1));
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
};

filter f_user_proc {
        match("syscall=59" value("MESSAGE"));
};

log {
    source(s_user_proc);
    filter(f_user_proc);
    destination(d_audit);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на контроллере домена с помощью следующей команды:

```
systemctl restart syslog-ng
```

Настройка журналирования событий создания и запуска нового процесса пользователем на сервере аудита

Настройка журналирования событий создания и запуска нового процесса пользователем на сервере аудита выполняется после предварительной настройки службы `syslog-ng`, а также настройки точки сбора журналов в службе `syslog-ng` (создание файла конфигурации `/etc/syslog-ng/siem/source.conf`) в соответствии с описанием в разделе 5.2.2 настоящей инструкции (если такая настройка не проводилась ранее). Затем необходимо создать файл конфигурации для фильтрации событий создания и запуска нового процесса пользователем.

Для настройки журналирования событий создания и запуска нового процесса пользователем на сервере аудита необходимо создать файл конфигурации `/etc/syslog-ng/siem/input-user-proc.conf` с правами на чтение для всех пользователей и внести в него следующую информацию:

```
destination d_user_proc {
    file("/var/log/aldpro/userproc.log" template("${MESSAGE}\n"));
};
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
filter f_user_proc {
        match("syscall=59" value("MESSAGE"));
};

log {
    source(s_net);
    filter(f_user_proc);
    rewrite {
        subst(" .source.s_user_proc", "", value("MESSAGE"));
    };
    destination(d_user_proc);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на сервере аудита с помощью следующей команды:

```
systemctl restart syslog-ng
```

3.15.5.7. Настройка журналирования события подключения к каталогу LDAP

Настройка журналирования события подключения к каталогу LDAP на контроллере домена

Для настройки журналирования событий подключения к каталогу LDAP на контроллере домена необходимо создать файл `/etc/audit/rules.d/siem.rules` со следующим содержимым (или добавить в этот файл следующие строки, если он уже создан):

```
-a always,exit -S accept -S accept4 -F exe=/usr/sbin/ns-slapd -k ldapconnect
-a exit,always -F exit=-EACCES -F exe=/usr/sbin/ns-slapd -k ldapconnect
```

Где `ldapconnect` - строка, которая является ключом для фильтрации сообщений и может задаваться администратором произвольно (но затем эта строка используется в файлах конфигурации).

После внесения изменений необходимо перезапустить службу `auditd` следующей командой:

```
systemctl restart auditd
```

Настройка журналирования событий подключения к каталогу LDAP на контроллере домена выполняется после предварительной настройки службы `syslog-ng`, а также настройки точки пересылки журналов в службе `syslog-ng` (создание файла конфигурации `/etc/syslog-ng/siem/destination.conf`) в соответствии с описанием в разделе 5.2.1 настоящей инструкции (если такая настройка не проводилась ранее). Затем необходимо создать файл конфигурации для фильтрации событий подключения к каталогу LDAP.

Для настройки журналирования событий подключения к каталогу LDAP на контроллере домена необходимо создать файл конфигурации `/etc/syslog-ng/siem/output-ldapconnect.conf` с правами на чтение для всех пользователей и внести в него следующую информацию:

```
source s_ldap {
    file("/var/log/audit/audit.log" flags(no-parse) persist-name("ldap_conn
↪") follow-freq(1));
};

filter f_ldapconnect {
    message('ldapconnect');
};

log {
    source(s_ldap);
    filter(f_ldapconnect);
    destination(d_audit);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на контроллере домена с помощью следующей команды:

```
systemctl restart syslog-ng
```

Настройка журналирования события подключения к каталогу LDAP на сервере аудита

Настройка журналирования событий подключения к каталогу LDAP на сервере аудита выполняется после предварительной настройки службы `syslog-ng`, а

также настройки точки сбора журналов в службе `syslog-ng` (создание файла конфигурации `/etc/syslog-ng/siem/source.conf`) в соответствии с описанием в разделе 5.2.2 настоящей инструкции (если такая настройка не проводилась ранее). Затем необходимо создать файл конфигурации для фильтрации событий подключения к каталогу LDAP.

Для настройки журналирования событий подключения к каталогу LDAP на сервере аудита необходимо создать файл конфигурации `/etc/syslog-ng/siem/input-ldapconnect.conf` с правами на чтение для всех пользователей и внести в него следующую информацию:

```
destination d_ldapconnect {
    file("/var/log/aldpro/ldapconnect.log" template("${MESSAGE}\n"));
};

filter f_ldapconnect {
    message("ldapconnect");
};

log {
    source(s_net);
    filter(f_ldapconnect);
    rewrite {
        subst(" .source.s_ldap", "", value("MESSAGE"));
        subst(' key="ldapconnect"', "", value("MESSAGE"));
    };
    destination(d_ldapconnect);
};
```

После выполнения действий необходимо перезапустить службу `syslog-ng` на сервере аудита с помощью следующей команды:

```
systemctl restart syslog-ng
```

3.15.6. Ротация журналов

3.15.6.1. Настройка режимов ведения и ротации журналов событий службы каталога на контроллерах домена

Вся конфигурационная информация службы каталога находится в файле `dse.ldif`, в главной ветке хранения информации о конфигурации `cn=config`, как это показано на следующем рисунке:

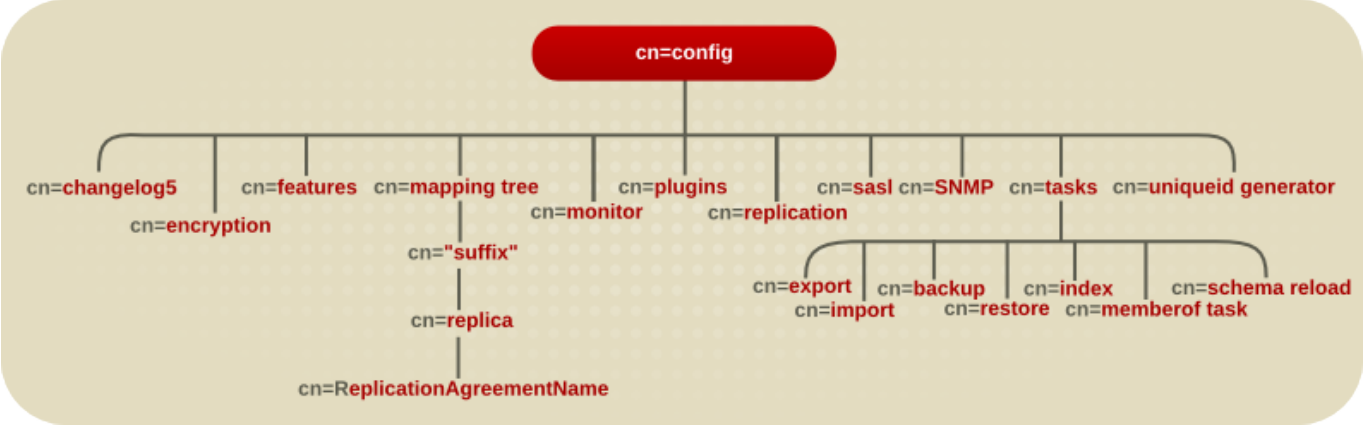


Рисунок 3.99 – Ветка службы каталога, показывающая записи для хранения различных данных о конфигурации.

Важно: Перед внесением любых изменений в конфигурацию подсистемы журналирования службы каталога администратору **настоятельно рекомендуется** ознакомиться с данным разделом в полном объёме!

Служба каталога 389 Directory Server может осуществлять запись о событиях журналы следующих типов:

- `access log` - журнал доступа, который содержит информацию о клиентских подключениях и попытках подключения к экземпляру сервера каталогов; данный тип журнала включен по умолчанию;
- `error log` - журнал ошибок, который содержит подробные сообщения об ошибках и неудачных операциях, а также о событиях, с которыми служба каталога сталкивается во время работы; при установке определенных уровней журналирования для данного типа журнала в него записываются сообщения о транзакциях и операциях сервера каталогов или общая информацию о процессах сервера каталогов и задачах LDAP,

например сообщения о запуске сервера, входах в систему и поиске в каталоге, а также информация о соединении; данный тип журнала включен по умолчанию;

- `audit log` - журнал аудита, который записывает **успешные** изменения, внесенные в каждую базу данных службы каталога, а также в конфигурацию сервера; данный тип журнала **не включен по умолчанию**;
- `audit fail log` - журнал ошибок аудита, который записывает только события о **неудачных** попытках изменений в базе данных или конфигурации сервера, этот тип журнала имеет идентичный формат с типом журнала аудита; данный тип журнала **не включен по умолчанию**;
- `security log` - журнал событий безопасности, который записывает ряд событий об ошибках авторизации/аутентификации, блокировки учетных записей, событий DoS и TCP атак и прочее; данный тип журнала **не включен по умолчанию**.

Каждый из типов журналов имеет свой формат (кроме журналов аудита и ошибок аудита, которые имеют идентичный формат).

Примечание: Если серверу службы каталога не удается выполнить запись в журнал ошибок, сервер отправляет сообщение об ошибке в службу системного журнала (чаще всего это служба `syslog`) и завершает работу.

Чтобы посмотреть пути для сохранения файлов журналов данного экземпляра службы каталога на конкретном КД можно выполнить команду:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config get nsslapd-accesslog nsslapd-errorlog nsslapd-auditlog nsslapd-
↪auditfaillog nsslapd-securitylog
```

Пример результата (для всех файлов использованы значения по умолчанию):

```
nsslapd-accesslog: /var/log/dirsrv/slapd-ALDPRO-LAN/access
nsslapd-errorlog: /var/log/dirsrv/slapd-ALDPRO-LAN/errors
nsslapd-auditlog: /var/log/dirsrv/slapd-ALDPRO-LAN/audit
nsslapd-auditfaillog: /var/log/dirsrv/slapd-ALDPRO-LAN/audit
nsslapd-securitylog: /var/log/dirsrv/slapd-ALDPRO-LAN/security
```

Для изменения конфигурация включения файлов журналов на каждом контроллере домена необходимо выполнить команды для каждого файла журнала, при этом необходимо использовать опцию replace. Для изменения режима ведения различных типов

журналов (включения записи в журнал или прекращения записи) необходимо использовать параметры, приведенные в таблице 6.1. Для включения ведения журналов определенного типа необходимо использовать опцию on.

Таблица 6.1. Параметры изменения режима ведения всех типов журналов службы каталога.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможны
access log	*nsslapd-accesslog-logging-enabled*	on	on/off
error log	*nsslapd-errorlog-logging-enabled*	on	on/off
audit log	*nsslapd-auditlog-logging-enabled*	off	on/off
audit fail log	*nsslapd-auditfaillog-logging-enabled*	off	on/off
security log	*nsslapd-securitylog-logging-enabled*	off	on/off

Пример включения ведения файла `security` на конкретном экземпляре сервера каталога:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-securitylog-logging-enabled=on
```

Если ведение журнала определенного типа включено, то для изменения пути для сохранения файла используется команда dsconf с опцией `config replace` и параметрами `nsslapd-accesslog`, `nsslapd-errorlog`, `nsslapd-auditlog`, `nsslapd-auditfaillog`, `nsslapd-securitylog`.

Пример изменения пути и наименования для сохранения журнала безопасности службы каталога на конкретном экземпляре сервера каталога:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-securitylog=/var/log/dirsrv_security.log
```

Журнал доступа, и журнал ошибок могут записывать разные объемы информации в зависимости от установленного уровня журналирования. Администратор службы каталога может установить следующие параметры конфигурации для управления уровнями журналирования:

1. ля журнала доступа: `nsslapd-accesslog-level` (необходимо установить значение

on, по умолчанию `off`)

2. для журнала ошибок: `nsslapd-errorlog-level` (необходимо установить значение on, по умолчанию `off`)

Изменение уровня журналирования для журнала доступа, установленного по умолчанию, может привести к очень быстрому росту файла журнала. В документации, описывающей службу каталога, не рекомендуется изменять значения по умолчанию без предварительного контакта со службой технической поддержки.

Значения параметров для установки уровня журналирования в журнала доступа к службе каталога:

- 0 — журналирование доступа к каталогу не ведется
- 4 — журналирование только внутренних операций доступа к каталогу
- 256 — журналирование всех подключений, операций и результатов доступа к конкретной записи каталога (это значение по умолчанию)
- 512 — журналирование доступа не только к самой записи каталога, но и к связанным с ней записям.

Эти значения можно складывать, чтобы получить необходимые администратору типы записей при ведении журнала доступа, например 516 (4 + 512) для получения журналирования внутренних операций доступа к каталогу, а также журналирование доступа к записи и связанных с ней записям.

Для установки уровня журналирования используется команда `dsconf` с опцией `config replace`.

Пример установки максимального уровня журналирования для журнала доступа (крайне не рекомендуется к применению).

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-accesslog-level=772
```

После установки уровня журналирования значением 256 или выше для журнала доступа можно также добавить запись статистики по каждой операции поиска. Во время некоторых операций поиска, особенно с такими фильтрами, как (`cn=user*`), время, затрачиваемое сервером на получение данных, обработку результата и выдачу ответа (`etime`), может быть очень продолжительным. Поэтому расширение журнала доступа информацией, связанной с индексами, используемыми во время операции поиска, помогает диагностировать проблемы с операциями чтения в службе каталога.

Чтобы включить сбор статистики и запись ее в журнал доступа (информация о количестве поисков в индексе - операций чтения базы данных и общая продолжительность поиска в индексе для каждой операции поиска, с минимальным воздействием на сервер) необходимо использовать атрибут `nsslapd-statlog-level`.

Пример включения записи информации о статистике использования индексов при операциях чтения службы каталога.

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-statlog-level=1
```

Пример включения записи информации о статистике использования индексов при операциях чтения службы каталога.

```
ldapsearch -D "cn=Directory Manager" -H ldap://alddc1.ald.lan -b "dc=ald,
↪dc=lan" -s sub -x "cn=user*"
```

Фрагмент журнала доступа после включения опции записи статистики и выполнения операции поиска с фильтром «cn=user*»:

```
[30/Nov/2023:11:34:11.834135997 +0300] conn=1 op=73 SRCH base="dc=ald,dc=lan
↪" scope=2 filter="(cn=user)"* attrs=ALL
[30/Nov/2023:11:34:11.835750508 +0300] conn=1 op=73 STAT read index:
↪attribute=objectclass key(eq)=referral → count 0
[30/Nov/2023:11:34:11.836648697 +0300] conn=1 op=73 STAT read index:
↪attribute=cn key(sub)=er_ → count 25
[30/Nov/2023:11:34:11.837538489 +0300] conn=1 op=73 STAT read index:
↪attribute=cn key(sub)=ser → count 25
[30/Nov/2023:11:34:11.838814948 +0300] conn=1 op=73 STAT read index:
↪attribute=cn key(sub)=use → count 25
[30/Nov/2023:11:34:11.841241531 +0300] conn=1 op=73 STAT read index:
↪attribute=cn key(sub)=^us → count 25
[30/Nov/2023:11:34:11.842230318 +0300] conn=1 op=73 STAT read index:
↪duration 0.000010276
[30/Nov/2023:11:34:11.843185322 +0300] conn=1 op=73 RESULT err=0 tag=101
↪nentries=24 wtime=0.000078414 optime=0.001614101 etime=0.001690742
```

Изменение уровня журналирования для журнала ошибок, установленного по умолчанию, может привести к очень быстрому росту файла журнала, а также серьезно снизить производительность сервера службы каталога. В документации на службу каталога не рекомендуется изменять значения по умолчанию без предварительного контакта со

службой технической поддержки.

Принимаемые значения параметров для установки уровня журналирования в журнале ошибок:

- 1 —записывает событие о том, когда сервер службы каталога выполняет функции (входит и выходит из каждой функции);
- 2 —записывает отладочную информацию для пакетов, обрабатываемых сервером службы каталога;
- 4 —записывает событие о том, когда сервер службы каталога выполняет функции (входит и выходит из каждой функции) с дополнительными сообщениями для отладки;
- 8 —записывает текущий статус подключения, включая методы подключения, используемые для привязки SASL;
- 16 —записывает информацию о количестве пакетов, отправленных и полученных сервером;
- 32 —записывает событие о всех функциях, вызываемые операцией поиска в каталоге;
- 64 —записывает ошибок построчно информацию из всех файлов конфигурации (`*.conf`), которые использовал сервер при запуске, по умолчанию сервер службы каталога обрабатывает только файл `slapd-collations.conf`;
- 128 —записывает подробную информацию об обработке списка управления доступом (ACL);
- 2048 —записывает отладочную информацию о разборе схемы базы данных (при внутренних операциях сервера службы каталога);
- 4096 —записывает отладочную информацию для служебных потоков сервера службы каталога;
- 8192 —записывает подробную информацию о каждой операции, связанной с репликацией, включая обновления и ошибки, данная информация может быть полезна для отладки проблем репликации;
- 16384 —записывает критические ошибки и другие сообщения, которые сервер каталогов всегда записывает в журнал ошибок, например сообщения о запуске сервера, нужно учитывать, что журнал **ошибок содержит эти сообщения независимо от настройки уровня журнала**;
- 32768 —записывает отладочную информацию для кэша записей базы данных;
- 65536 —записывает событие о том, когда подключаемый модуль сервера вызывает

функцию `slapi-log-error()`, этот уровень журнала можно использовать для отладки подключаемого модуля сервера службы каталога.

Эти значения можно складывать, чтобы получить необходимые администратору типы записей при ведении журнала ошибок.

Важно: Включение высокого уровня ведения журнала ошибок может значительно снизить производительность сервера. Поэтому следует включать высокие уровни ведения журнала отладки, такие как репликация (8192), только для устранения неполадок!

Для установки уровня журналирования для журнала ошибок службы каталога необходимо использовать команду dsconf с опцией config replace.

Пример установки уровня журналирования для журнала ошибок.

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-errorlog-level=96
```

Примечание: Для корректного функционирования службы каталога (устранения проблем с занимаемым журналами местом на диске) требуется настроить ротацию журналов. Для этого необходимо настроить политики **создания** и **удаления** для всех типов файлов журналов. Политика создания журнала задается при запуске нового файла журнала, а политика удаления журнала задается при удалении старого файла журнала.

Для определения политики создания журналов службы каталога необходимо задать (изменить при необходимости) следующие параметры:

1. Режим доступа к вновь создаваемым файлам журналов.
2. Максимальное количество журналов.
3. Максимальный размер файла для каждого журнала.
4. Максимальное время записи в файл для каждого журнала.

Для задания режима доступа к вновь создаваемым файлам журналов администратор может использовать нумерованные права доступа к файлам UNIX. Это трехзначные числа, где первый разряд определяет разрешения владельца файла, второй разряд определяет разрешения группы, а в третьем разряде определены разрешения всех остальных

пользователей данного компьютера. При этом в каждом разряде которых стоит число от нуля до семи, причем каждое из чисел означает следующее:

- 0 — Всё запрещено
- 1 — Разрешено только выполнять
- 2 — Разрешено только писать
- 3 — Разрешено писать и выполнять
- 4 — Разрешено только читать
- 5 — Разрешено читать и выполнять
- 6 — Разрешено читать и писать
- 7 — Разрешено читать, писать и выполнять

При этом, вновь заданный с помощью соответствующей команды режим доступа к конкретному типу журнала влияет только на вновь создаваемые файлы во время ротации. Параметры службы каталога, которые определяют режим доступа к файлам журналов, приведены в таблице 6.2.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможны
access log	`nsslapd-accesslog-mode`	600	000/777
error log	`nsslapd-errorlog-mode`	600	000/777
audit log	`nsslapd-auditlog-mode`	600	000/777
audit fail log	`nsslapd-auditfaillog-mode`	600	000/777
security log	`nsslapd-securitylog-mode`	600	000/777

Для задания максимального количества журналов службы каталога определенного типа необходимо использовать параметры службы каталога, которые приведены в таблице 6.3.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможны
access log	`nsslapd-accesslog-maxlogsperdir`	10	Натуралы
error log	`nsslapd-errorlog-maxlogsperdir`	1	Натуралы

Таблица 3.23 – продолжение с предыдущей страницы

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможны
audit log	`nsslapd-auditlog-maxlogsperdir`	1	Натуралы
audit fail log	`nsslapd-auditfaillog-maxlogsperdir`	1	Натуралы
security log	`nsslapd-securitylog-maxlogsperdir`	10	Натуралы

Однако, задание **только** атрибута `*-maxlogsperdir` **не** позволит реализовать полноценную ротацию журналов, необходимо также задать параметры максимального времени записи в журналы.

Для задания максимального времени записи в файл журнала службы каталога определенного типа необходимо использовать **совместно** параметры службы каталога, указанные в таблицах 6.4 и 6.5. Значение в таблице 6.4 задает количество диапазонов времени, через которые будет осуществляться ротация журнала определенного типа, а значение в таблице 6.5 задает сам диапазона времени ротации (`minute` - минута, `hour` - час, `day` - день, `week` - неделя, `month` - месяц).

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможны
access log	`nsslapd-accesslog-logrotationtime`	1	«-1» или
error log	`nsslapd-errorlog-logrotationtime`	1	«-1» или
audit log	`nsslapd-auditlog-logrotationtime`	1	«-1» или
audit fail log	`nsslapd-auditfaillog-logrotationtime`	1	«-1» или
security log	`nsslapd-securitylog-logrotationtime`	1	«-1» или

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
access log	`nsslapd-accesslog-logrotationtimeunit`	day	Диапазон времени: minute/hour/day/week/month

продолжение на следующей странице

Таблица 3.25 – продолжение с предыдущей страницы

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
error log	nsslapd-errorlog-logrotationtimeunit	week	Диапазон времени: minute/hour/day/week/month
audit log	nsslapd-auditlog-logrotationtimeunit	week	Диапазон времени: minute/hour/day/week/month
audit fail log	nsslapd-auditfaillog-logrotationtimeunit	week	Диапазон времени: minute/hour/day/week/month
security log	nsslapd-securitylog-logrotationtimeunit	week	Диапазон времени: minute/hour/day/week/month

Помимо этого, необходимо учитывать тот факт, что при достаточно высокой нагрузке на сервер каталога, размер журнала доступа (access) будет расти достаточно быстро, поэтому значения по умолчанию для параметров nsslapd-accesslog-logrotationtime и nsslapd-accesslog-logrotationtimeunit необходимо изменить в соответствии с потребностями администратора с учетом свободного места на дисковой подсистеме каждого контроллера домена. Также необходимо проанализировать скорость роста остальных файлов журнала службы каталога и, при необходимости, поменять значения по умолчанию для параметров максимального времени записи в соответствующие файлы журналов.

Помимо задания ротации журналов по времени существует параметр задания ротации журналов по занимаемому им месту на диске. Для задания максимального размера каждого журнала службы каталога определенного типа в мегабайтах необходимо использовать параметры самого службы каталога, указанные в таблице 6.6. Если значение параметра равно «-1», то это означает, что размер файла не задан и журнал будет расти в объеме до тех пор, пока не заполнит все пространство на жестком диске.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможны
access log	nsslapd-accesslog-maxlogsize	100	«-1» или н
error log	nsslapd-errorlog-maxlogsize	100	«-1» или н

Таблица 3.26 – продолжение с предыдущей стран

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможны
audit log	`nsslapd-auditlog-maxlogsize`	100	«-1» или н
audit fail log	`nsslapd-auditfaillog-maxlogsize`	100	«-1» или н
security log	`nsslapd-securitylog-maxlogsize`	100	«-1» или н

Важно:

1. Для реализации ротации журналов администратор должен изменить параметр `*-maxlogsperdir` для тех типов файлов журналов службы каталога, у которых значение этого параметра равно единице (поскольку в этом случае, параметры службы каталога `*-logrotationtime`, `*-logrotationtimeunit` и `*-maxlogsize` игнорируются и сервер службы каталога **не осуществляет ротацию** тех типов журналов, у которых значение параметра `*-maxlogsperdir` равно единице).

2. При этом, если значение атрибута `*-logrotationtime` равно «-1» для какого-то типа файла журнала, то сервер службы каталога также **не будет осуществлять ротацию** журналов этого типа по времени и атрибут `*-maxlogsperdir` для этого типа журнала будет проигнорирован. Фактически, установка значения «`*-logrotationtime=-1`» для определенного типа журнала означает, что время для проведения ротации этого типа журнала не задано. Однако ротация этого журнала по объему занимаемого им места на диске будет происходить (если параметр `*-maxlogsize` для этого типа журнала **не равен «-1»**).

Например, для изменения конфигурации ротации журнала ошибок службы каталога можно использовать следующую команду:

Пример включения ведения файла `security` на конкретном экземпляре сервера каталога:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-errorlog-mode=644 nsslapd-errorlog-
↪maxlogsperdir=5 nsslapd-errorlog-maxlogsize=500 nsslapd-errorlog-
↪logrotationtime=7 nsslapd-errorlog-logrotationtimeunit=day
```

Эта команда для файла журнала ошибок (в примере выше это файл error) службы

каталога на данном экземпляре 389 Directory Server выполнит следующие действия:

- установит режим доступа для файла журнала ошибок равный «644» (означающий, что владелец файла имеет права на чтение и запись, а группа и остальные пользователи — только на чтение);
- установит максимальное количество файлов журнала ошибок в каталоге хранения журналов равное 5;
- установит режим ротации журнала таким образом, что файл будет ротироваться (текущий журнал становится архивным) либо по достижению размера в 500 Мб, либо один раз в 7 дней.

Также для задания времени ротации файлов журналов службы каталога определенного типа необходимо использовать **совместно** параметры службы каталога, указанные в таблицах 6.7, 6.8 и 6.9. Значение в таблице 6.8 задает конкретное значение часа, когда будет осуществляться ротация журнала определенного типа, а значение в таблице 6.9 задает значение минуты в этом часе, когда будет осуществляться ротация журнала определенного типа. Для использования параметров ротации журналов из таблиц 6.8 и 6.9, необходимо предварительно включить параметр (задать значение on для параметра журнала определенного типа) из таблицы 6.7, который определяет, будут ли читаться параметры таблиц 6.8 и 6.9, после чего задать значения часов и минут для журнала необходимого типа. Задание механизма ротации всех типов журналов службы каталога таким способом значительно облегчит последующий анализ журналов или инцидентов (поскольку все журналы могут ротироваться в одно и то же время, затем можно их архивировать и отправлять в какое-то хранилище, где затем в случае необходимости проведения поиска конкретных записей журналов можно будет достаточно быстро найти всю записанную информацию по дате и времени журналов).

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию
access log	`nsslapd-accesslog-logrotationsync-enabled`	off
error log	`nsslapd-errorlog-logrotationsync-enabled`	off
audit log	`nsslapd-auditlog-logrotationsync-enabled`	off
audit fail log	`nsslapd-auditfaillog-logrotationsync-enabled`	off
security log	`nsslapd-securitylog-logrotationsync-enabled`	off

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возм
access log	`nsslapd-accesslog-logrotationsynchour`	0	Цели
error log	`nsslapd-errorlog-logrotationsynchour`	none	Цели
audit log	`nsslapd-auditlog-logrotationsynchour`	none	Цели
audit fail log	`nsslapd-auditfaillog-logrotationsynchour`	none	Цели
security log	`nsslapd-securitylog-logrotationsynchour`	none	Цели

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возмо
access log	`nsslapd-accesslog-logrotationsyncmin`	0	Целы
error log	`nsslapd-errorlog-logrotationsyncmin`	none	Целы
audit log	`nsslapd-auditlog-logrotationsyncmin`	none	Целы
audit fail log	`nsslapd-auditfaillog-logrotationsyncmin`	none	Целы
security log	`nsslapd-securitylog-logrotationsyncmin`	none	Целы

Пример включения ротации журнала `access` в 11 часов 11 минут на конкретном экземпляре сервера каталога:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-auditlog-logrotationsync-enabled=on nsslapd-
↪accesslog-logrotationsynchour=11 nsslapd-accesslog-logrotationsyncmin=11
```

Аналогично вышеприведенным примерам и используя данные таблиц 6.1-6.9 можно настроить политики создания новых файлов при ротации всех журналов для текущего экземпляра службы каталога.

Для определение политики **удаления** журналов службы каталога при ротации журналов необходимо задать (изменить при необходимости) параметры для каждого типа журналов, приведенные в таблицах 6.10 и 6.11:

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возм
access log	`nsslapd-accesslog-logminfreediskspace`	100	«-1»
error log	`nsslapd-errorlog-logminfreediskspace`	100	«-1»
audit log	`nsslapd-auditlog-logminfreediskspace`	100	«-1»
audit fail log	`nsslapd-auditfaillog-logminfreediskspace`	100	«-1»
security log	`nsslapd-securitylog-logminfreediskspace`	100	«-1»

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможны
access log	`nsslapd-accesslog-logmaxdiskspace`	100	«-1» или
error log	`nsslapd-errorlog-logmaxdiskspace`	100	«-1» или
audit log	`nsslapd-auditlog-logmaxdiskspace`	100	«-1» или
audit fail log	`nsslapd-auditfaillog-logmaxdiskspace`	100	«-1» или
security log	`nsslapd-securitylog-logmaxdiskspace`	100	«-1» или

При задании одной из вышеуказанных опций будет происходить удаление соответствующих файлов службы каталога во время ротации журналов.

При задании опции `logminfreediskspace` произойдет следующее: при достижении указанного в параметре значения свободного места на диске, где хранится соответствующий файл журнала, самый старый архивный файл этого журнала автоматически удаляется.

При задании опции `logmaxdiskspace` произойдет следующее: при достижении указанного в параметре значения суммарного места на диске для определенного типа журналов (например, всех журналов `audit`, включая архивные), самый старый архивный файл этого журнала автоматически удаляется.

Примечание: Важно обратить внимание, что в зависимости от значений, установленных в `nsslapd-accesslog-logminfreediskspace` и `nsslapd-accesslog-maxlogsize`, фактическое количество журналов может быть меньше того, которое настроил администратор в параметре `nsslapd-accesslog-maxlogsperdir`. Например, если для

параметра `nsslapd-accesslog-maxlogsperdir` используется значение по умолчанию (10 файлов), а администратор установил `nsslapd-accesslog-logminfreediskspace=500` и `nsslapd-accesslog-maxlogsize=100`, сервер каталогов сохранит только 5 файлов доступа.

Также можно определить **временную** политику **удаления** журналов службы каталога. Для этого необходимо **совместно** задать параметры для каждого типа журналов, приведенные в таблицах 6.12 и 6.13:

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможны
access log	`nsslapd-accesslog-logmaxdiskspace`	100	«-1» или
error log	`nsslapd-errorlog-logmaxdiskspace`	100	«-1» или
audit log	`nsslapd-auditlog-logmaxdiskspace`	100	«-1» или
audit fail log	`nsslapd-auditfaillog-logmaxdiskspace`	100	«-1» или
security log	`nsslapd-securitylog-logmaxdiskspace`	100	«-1» или

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
access log	`nsslapd-accesslog-logexpirationtimeunit`	`month`	Диапазон времени: day/week/month
error log	`nsslapd-errorlog-logexpirationtimeunit`	`month`	Диапазон времени: day/week/month
audit log	`nsslapd-auditlog-logexpirationtimeunit`	`week`	Диапазон времени: day/week/month
audit fail log	`nsslapd-auditfaillog-logexpirationtimeunit`	`week`	Диапазон времени: day/week/month

продолжение на следующей странице

Таблица 3.33 – продолжение с предыдущей страницы

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможные значения
security log	`nsslapd-securitylog-logexpirationtime`	-1	Диапазон времени: day/week/month

Если у параметров `*-logexpirationtime` или `*-logexpirationtimeunit` установлены значения минус единица или ноль (или любое другое значение, которое не входит в диапазон возможных значений для этого параметра, в том числе и строковое), то это означает, что соответствующий тип журнала службы каталога никогда не удаляется.

Пример настройки для автоматического удаления самого старого журнала `access`, если суммарный размер всех журналов этого типа превышает 500 Мб на жестком диске на конкретном экземпляре сервера каталога:

```
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
↪lan config replace nsslapd-accesslog-logmaxdiskspace=500
```

Также существуют параметры для задания сжатия журналов службы каталога после проведения ротации, что позволяет существенно (в десять и более раз) уменьшить занимаемое архивными журналами место на жестком диске. Для задания режима сжатия файлов журнала службы каталога определенного типа необходимо использовать параметры службы каталога, указанные в таблице 6.14.

Тип журнала	Параметр службы каталога для типа журнала	Значение по умолчанию	Возможны
access log	`nsslapd-accesslog-compress`	off	on/off
error log	`nsslapd-errorlog-compress`	off	on/off
audit log	`nsslapd-auditlog-compress`	off	on/off
audit fail log	`nsslapd-auditfaillog-compress`	off	on/off
security log	`nsslapd-securitylog-compress`	on	on/off

Несмотря на то, что ряд параметров применяется без перезагрузки сервера службы каталога, тем не менее, после выполнения всех необходимых настроек журналов службы

следует перезапустить службу каталога с помощью следующей команды:

```
dsctl INSTANCE_NAME restart
```

Где INSTANCE_NAME - имя экземпляра службы каталога.

3.15.6.2. Настройка ротации журналов событий службы аудита и службы kerberos на контроллере домена

События службы `kerberos` можно как перенаправить в системный журнал (по умолчанию в ОС Astra Linux SE 1.7.4 - `/var/log/syslog`), так и записать их в свой собственный файл. Каким образом будет проводиться запись в журнал указано в файле конфигурации службы - `/etc/krb5.conf` в секции `logging`. Настройка корректной записи в свой журнал по указанному в секции `logging` пути по умолчанию приведена в пункте 5.5.1 настоящей инструкции. Однако в этом случае необходимо настраивать ротацию этого журнала с помощью утилиты `logrotate`.

Утилита `logrotate` — это утилита, выполняющая ротацию и сжатие файлов журналов. При правильной настройке этой утилиты для работы с файлом конкретного журнала, его размеры никогда не увеличатся до такой степени, что будут угрожать стабильности системы.

По умолчанию утилита `logrotate` предустановлена в ОС Astra Linux 1.7 и выше. Она уже настроена для своевременной обработки журналов некоторых имеющихся в системе и используемых пользователями приложений, в том числе `syslog`.

Конфигурация самой утилиты `logrotate` находится в следующем каталоге:

- `/etc/logrotate.conf` — основной файл конфигурации, который, как правило, содержит некоторые параметры, предустановленные автоматически, настройки для ряда базовых журналов, не принадлежащих системным пакетам и инструкцию include для подключения конфигурации, хранящейся по адресу `/etc/logrotate.d`;
- `/etc/logrotate.d` — содержит файлы с конфигурацией; в этом каталоге утилита logrotate считывает файлы конфигурации для различных журналов и системных пакетов, при этом каждый из таких файлов — конфигурация ротации соответствующего журнала; администратор при необходимости может добавить свои файлы конфигурации в этот каталог, и они также будут обработаны утилитой `logrotate`.

Также необходимо после настройки утилиты настроить режим запуска этой утилиты в планировщике задач операционной системы (cron). Подробную инструкцию по настройке планировщика, по диагностике возможных проблем и прочим возможностям можно посмотреть в справке операционной системе по утилите cron.

Для службы kerberos необходимо провести настройку утилиты logrotate самостоятельно. Для настройки ротации журнала службы kerberos (должен сохраняться по пути /var/log/krb5kdc.log после проведения настройки из пункта 5.5.1 настоящей инструкции) с помощью утилиты logrotate необходимо выполнить следующие действия:

1. Создать файл /etc/logrotate.d/kerberos с правами «644», в который внести и сохранить следующую информацию:

```
/var/log/krb5kdc.log {
    daily
    rotate 5
    minsize 1G
    compress
    missingok
    notifempty}
```

2. Для применения изменений и запуска утилиты в текущий момент времени необходимо выполнить команду:

```
logrotate /etc/logrotate.conf
```

3. Для запуска утилиты logrotate по расписанию необходимо настроить планировщик операционной системы таким образом, чтобы он запускал утилиту не реже самого минимального интервала времени для ротации всех журналов, которые есть в конфигурационных файлов утилиты logrotate: в данном случае (рассматривается только один журнал службы kerberos) это будет один раз в день, тогда необходимо выполнить следующую команду с правами пользователя root или другого привилегированного пользователя, который может запускать утилиту logrotate:

```
crontab -e
```

Для запуска утилиты logrotate ежедневно в 0 часов 5 минут в появившемся в результате выполнения предыдущей команды файле необходимо ввести в пустой строке следующие данные, после чего сохранить файл (требуются соответствующие привилегии):

```
5 0 * * * /usr/sbin/logrotate /etc/logrotate.conf
```

После выполнения настройки (внесения изменений в файл `crontab`) можно перезапустить сервис `cron` с помощью следующей команды (хотя это и не обязательно, `cron` должен читать изменения по дате их сохранения):

```
systemctl restart cron
```

В первой строке файла конфигурации утилиты `logrotate` указан путь к файлу, к которому будут применять различные директивы, которые перечислены ниже в этом конфигурационном файле. Указанные в примере директивы описывают следующее поведение утилиты:

- `daily` — ротацию выполнять один раз в сутки (для сервисов, которые записывают в свои журналы достаточно мало информации, можно использовать опцию monthly — один раз в месяц или `weekly` — один раз в неделю, а для сервисов, которые записывают в журналы **очень** много информации можно использовать опцию `hourly`, которая говорит о том, что ротация будет выполняться один раз в час);
- `rotate 5` — позволяет в автоматическом режиме хранить последние 5 журналов;
- `minsize` — журнал будет ротироваться, когда его размер больше указанного, но не ранее, чем наступает соответствующий временной интервал ротации (`hourly`, `daily`, `weekly`, `monthly`, `yearly`), для указания размеров файла журнала можно использовать большие буквы «G» — гигабайт, «M» — мегабайт;
- `compress` — используется для сжатия архивных журналов (стандартно используется утилита `gzip`);
- `missingok` — не оставляет сообщение об ошибке в работе в системном журнале, если ротируемый журнал пуст;
- `notifempty` — запрещает ротировать файл, если он пустой.

Дополнительную информацию о работе утилит `logrotate` и `cron`, а также обо всех допустимых параметрах настройки ротации журналов и способах запуска команд по расписанию можно посмотреть в справке операционной системы по данным утилитам.

После настройки ротации журнала службы `kerberos` необходимо провести настройку журнала службы аудита. Настройка журнала службы аудита производится путем редактирования файла конфигурации `/etc/audit/auditd.conf`. Этот файл, в числе, прочих содержит следующие параметры:

- `log_file` — файл, в котором будут храниться журналы подсистемы аудита;
- `log_format`— формат, в котором будет сохранены журналы;
- `freq` — максимальное число записей протокола аудита, которые могут храниться в буфере;
- `flush` — режим синхронизации буфера с диском: - `none` — ничего не делать, - `incremental` — переносить данные из буфера на диск с частотой, указанной в значении параметра `freq`, - `data` — синхронизировать немедленно, - `sync` — синхронизировать как данные, так и метаданные файла при записи на диск;
- `max_log_file` — максимальный размер файла лога в мегабайтах;
- `max_log_file_action` — действие при превышении максимального размера файла лога;
- `space_left` — минимум свободного пространства в мегабайтах, по достижении которого должно быть осуществлено действие, указанное в следующем параметре;
- **`space_left_admin` — указывает, что делать, когда на диске недостаточно свободного места:**
  - `ignore` — ничего не делать,
  - `syslog` — отправлять в журнал `syslog`,
  - `email` — отправлять уведомление по почте,
  - `suspend` — прекратить запись логов на диск,
  - `single` — перейти в однопользовательский режим,
  - `halt` — выключить машину;
- `disk_full_action` — действие, которое нужно осуществить при переполнении диска (этот параметр может принимать те же значения, что и `space_left_admin`).

В разделе 5.6.1 приведена настройка журнала аудита, при которой все параметры, кроме `max_log_file`, остаются неизменными. По аналогии с данным примером можно провести требуемые администратору изменения конфигурации журналирования событий аудита. После всех изменений файла конфигурации необходимо перезапустить сервис `auditd` с помощью команды:

```
systemctl restart auditd
```

3.15.6.3. Настройка ротации журналов событий на сервере аудита

Настройку ротации журналов, которые перенаправляются с контроллеров домена на сервер аудита из состава домена ALD Pro согласно настоящей инструкции, необходимо проводить с помощью утилиты `logrotate`. Основные сведения о работе данной утилиты приведены в разделе 6.2 настоящей инструкции.

Ниже приведены файлы конфигурации для утилиты `logrotate`, обеспечивающие ротацию всех журналов, которые создаются в папке `/var/log/aldpro/` на сервера аудита, согласно настоящей инструкции.``

1. Файл конфигурации `/etc/logrotate.d/access_dirsrv` для ротации журнала доступа к службе каталога, который необходимо создать с правами «644», внести в него следующую информацию и сохранить:

```
/var/log/aldpro/access_dirsrv.log {
    hourly
    rotate 10
    minsize 1G
    compress
    missingok
    notifempty
}
```

2. Файл конфигурации `/etc/logrotate.d/audit_dirsrv` для ротации журнала аудита службы каталога, который необходимо создать с правами «644», внести в него следующую информацию и сохранить:

```
/var/log/aldpro/audit_dirsrv.log {
    hourly
    rotate 10
    minsize 100M
    compress
    missingok
    notifempty
}
```

3. Файл конфигурации `/etc/logrotate.d/error_dirsrv` для ротации журнала ошибок службы каталога, который необходимо создать с правами «644», внести в него следующую информацию и сохранить:

```
/var/log/aldpro/error_dirsrv.log {
    hourly
    rotate 5
    minsize 100M
    compress
    missingok
    notifempty
}
```

4. Файл конфигурации `/etc/logrotate.d/security_dirsrv` для ротации журнала событий безопасности службы каталога, который необходимо создать с правами «644», внести в него следующую информацию и сохранить:

```
/var/log/aldpro/security_dirsrv.log {
    hourly
    rotate 5
    minsize 100M
    compress
    missingok
    notifempty
}
```

5. Файл конфигурации `/etc/logrotate.d/samba` для ротации журнала событий службы `samba`, который необходимо создать с правами «644», внести в него следующую информацию и сохранить:

```
/var/log/aldpro/samba.log {
    hourly
    rotate 5
    minsize 10M
    compress
    missingok
    notifempty
}
```

6. Файл конфигурации `/etc/logrotate.d/dns_audit` для ротации журнала событий трансфера зоны `dns`, который необходимо создать с правами «644», внести в него следующую информацию и сохранить:

```
/var/log/aldpro/dnszone.log {
    hourly
    rotate 5
    minsize 1M
    compress
    missingok
    notifempty
}
```

7. Файл конфигурации `/etc/logrotate.d/kerberos_audit` для ротации журнала событий получения билетов службы `kerberos`, который необходимо создать с правами «644», внести в него следующую информацию и сохранить:

```
/var/log/aldpro/krb_audit.log {
    hourly
    rotate 10
    minsize 1G
    compress
    missingok
    notifempty
}
```

8. Файл конфигурации `/etc/logrotate.d/user_proc` для ротации журнала событий запуска новых процессов пользователями домена, который необходимо создать с правами «644», внести в него следующую информацию и сохранить:

```
/var/log/aldpro/userproc.log {
    hourly
    rotate 10
    minsize 1G
    compress
    missingok
    notifempty
}
```

9. Файл конфигурации `/etc/logrotate.d/ldap_audit` для ротации журнала событий подключения к каталогу `ldap`, который необходимо создать с правами «644», внести в него следующую информацию и сохранить:

```
/var/log/aldpro/ldapconnect.log {
    hourly
    rotate 10
    minsize 1G
    compress
    missingok
    notifempty
}
```

После создания описанных выше файлов конфигурации необходимо добавить ежечасный запуск утилиты `logrotate` в конфигурационный файл утилиты `cron`. Для этого необходимо скопировать файл `/etc/cron.daily/logrotate` в каталог `/etc/cron.hourly` и выполнить команду под пользователем root или другим привилегированным пользователем, который может запускать утилиту logrotate:

```
crontab -e
```

Затем в открывшемся файле конфигурации утилиты cron добавить новую строку (запуск утилиты `/usr/sbin/logrotate` от имени пользователя каждый час каждого дня в 0 минут) и сохранить сделанные изменения:

```
0 * * * * /usr/sbin/logrotate /etc/logrotate.conf
```

3.15.7. Отправка журналов в стороннюю SIEM

3.15.7.1. Настройка отправки журналов событий с сервера аудита в стороннюю SIEM

Собираемые журналы можно перенаправлять с помощью инструментов `syslog-ng` как с клиентов домена или контроллеров домена, так и с сервера аудита в сторонние SIEM. В настоящей инструкции не рассматривается настройка отправки журналов событий с клиентов или контроллеров домена, поскольку приведенный ниже файл конфигурации позволяет администратору самостоятельно модифицировать его и реализовать необходимую настройку отправки журналов событий по той схеме, которая отвечает требованиям безопасности в конкретной реализации системы.

Ниже приведен пример файла конфигурации отправки всех файлов, создаваемых в разделах 5.x.2 (где x - [2-7]) настоящей инструкции, в стороннюю SIEM, которая установлена на компьютере с IP-адресом «8.8.8.8» и настроена на «прослушивание»

следующих портов по заданным протоколам :

1. протокол tcp, порт 5154;
2. протокол tcp, порт 5155;
3. протокол tcp, порт 5156;
4. протокол tcp, порт 5157;
5. протокол udp, порт 5173.

Для настройки `syslog-ng` по отправке файлов журналов с сервера аудита в стороннюю SIEM необходимо на сервере аудита (при условии модификации файла конфигурации `/etc/syslog-ng/syslog-ng.conf` в соответствии с разделом 5.2.2) создать файл `/etc/syslog-ng/siem/siem_rules.conf` с правами на чтение всем пользователям (644), куда вставить приведенный ниже текст файла конфигурации (параметр `follow-freq(10)` определяет интервала опроса (в секундах) для каждого конкретного файла службой `syslog-ng`, в данном случае 1 раз в 10 секунд, этот параметр можно корректировать по необходимости, минимальное значение единица, если задано нулевое значение, то служба `syslog-ng` будет использовать значение по умолчанию):

```
#destinations
destination siem_dirsrv {
    network("8.8.8.8" transport("tcp") port(5154) flags(syslog-protocol)
 ↪template("${MESSAGE}\n"));
};

destination siem_krb5kdc {
    network("8.8.8.8" transport("tcp") port(5155) flags(syslog-protocol)
 ↪template("${MESSAGE}\n"));
};

destination siem_samba {
    network("8.8.8.8" transport("tcp") port(5156) flags(syslog-protocol)
 ↪template("${MESSAGE}\n"));
};

destination siem_bind {
    network("8.8.8.8" transport("tcp") port(5157) flags(syslog-protocol)
 ↪template("${MESSAGE}\n"));
};
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
destination siem_audit {
    network("8.8.8.8" transport("udp") port(5154) flags(syslog-protocol)
 ↪template("${MESSAGE}\n"));
};

#sources
source aldpro_access {
    file(
        "/var/log/aldpro/access_dirsrv.log"
        follow-freq(10)
        flags(no-parse)
    );
};

source aldpro_audit {
    file(
        "/var/log/aldpro/audit_dirsrv.log"
        follow-freq(10)
        flags(no-parse)
    );
};

source aldpro_security {
    file(
        "/var/log/aldpro/security_dirsrv.log"
        follow-freq(10)
        flags(no-parse)
    );
};

source aldpro_errors {
    file(
        "/var/log/aldpro/errors_dirsrv.log"
        follow-freq(10)
        flags(no-parse)
    );
};
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
source aldpro_krb5kdc {
    file(
        "/var/log/aldpro/krb_audit.log"
        follow-freq(10)
        flags(no-parse)
    );
};

source aldpro_samba {
    file(
        "/var/log/aldpro/samba.log"
        follow-freq(10)
        flags(no-parse)
    );
};

source aldpro_bind {
    file(
        "/var/log/aldpro/dnszone.log"
        follow-freq(10)
        flags(no-parse)
    );
};

source aldpro_ldap {
    file(
        "/var/log/aldpro/ldapconnect.log"
        follow-freq(10)
        flags(no-parse)
    );
};

source aldpro_userproc {
    file(
        "/var/log/aldpro/userproc.log"
        follow-freq(10)
        flags(no-parse)
    );
};
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
#logs
log {
    source(aldpro_access);
    destination(siem_dirsrv);
};

log {
    source(aldpro_audit);
    destination(siem_dirsrv);
};

log {
    source(aldpro_security);
    destination(siem_dirsrv);
};

log {
    source(aldpro_errors);
    destination(siem_dirsrv);
};

log {
    source(aldpro_krb5kdc);
    destination(siem_krb5kdc);
};

log {
    source(aldpro_samba);
    destination(siem_samba);
};

log {
    source(aldpro_bind);
    destination(siem_bind);
};

log {
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
    source(aldpro_ldap);
    destination(siem_audit);
};

log {
    source(aldpro_userproc);
    destination(siem_audit);
};
```

Затем необходимо заменить настройки пунктов назначения для файлов журналов (раздел `#destinations`) на актуальные в системе, и в случае коррекции наименований и отправки данных на меньшее или большее количество точек отправки, необходимо изменить в разделе `#logs` соответствующие записи.

После выполнения действий необходимо перезапустить службу `syslog-ng` на сервере аудита с помощью следующей команды:

```
systemctl restart syslog-ng
```

3.15.8. Настройка журналирования на КД, сервере общего доступа к файлам и сервере аудита (только команды)

Информация в данном разделе приведена максимально коротко и ёмко, для более глубокого понимания и индивидуальной настройки системы журналирования за помощью необходимо обращаться к соответствующему разделу инструкции, где приведена детальная информация.

После настройки, описанной в данном разделе:

1. будет осуществляться полное журналирование всех событий безопасности и перенаправление ряда журналов с КД и сервера общего доступа к файлам на сервер аудита из состава изделия;
2. НЕ будет настроена ротация журналов служб на КД, на сервере общего доступа к файлам и на сервере аудита;
3. НЕ будет осуществлено перенаправление информации с сервера аудита в стороннюю SIEM.

Для настройки ротации журналов на КД необходимо обратиться к разделам 6.1 и 6.2 настоящей инструкции. Для настройки ротации журналов на сервере аудита необходимо обратиться к разделу 6.3 настоящей инструкции. Для настройки перенаправления информации журналов с сервера аудита (или сразу с КД) в стороннюю SIEM необходимо обратиться к разделу 7.1.

1. Настройка всех КД в домене (изменение конфигурации 389 DS, настройка syslog-ng, перезапуск служб). **Дальнейшие действия нужно выполнить на каждом контроллере в домене!**

а) настроить 389 DS, службы Kerberos и auditd

```
# настройка 389 DS
# ldap://alddc1.ald.lan - необходимо по очереди заменить на адрес каждого
 ↪конкретного КД в домене, "ПАРОЛЬ_АДМИНИСТРАТОРА" - необходимо вписать
 ↪реальный пароль администратора
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
 ↪lan config replace nsslapd-auditlog-logging-enabled=on
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
 ↪lan config replace nsslapd-auditfaillog-logging-enabled=on
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
 ↪lan config replace nsslapd-securitylog-logging-enabled=on

# следующая команда без пробелов в одну строку
dsconf -D "cn=Directory Manager" -w "ПАРОЛЬ_АДМИНИСТРАТОРА" ldap://alddc1.ald.
 ↪lan config replace nsslapd-auditlog-display-attrs=loginShell,
krbExtraData,krbLastPwdChange,krbPasswordExpiration,x-ald-user-mac,uid,
 ↪displayName,initials,gecos,sn,homeDirectory,mail,krbPrincipalName,
krbCanonicalName,givenName,rbtamiddlename,street,l,st,postalCode,c,
 ↪employeeNumber,telephoneNumber,title,rbtadp,rbtaou,entyusn,modifiersName,
objectClass,ipaNTSecutityIdentifier,cn,creatorsName,createTimestamp,
 ↪modifyTimestamp,nsUniqueId,ipaUniqueId,parentid,entryid,uidNumber,gidNumber,
 ↪
entryUUID,dsEntryDN,entrydn

# настройка службы Kerberos
# в файле /lib/systemd/system/krb5-kdc.service в параметр
 ↪ReadWriteDirectories добавить /var/log и прочитать новую конфигурацию
 ↪службы
systemctl daemon-reload
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
# настройка службы auditd
# создаем файл /etc/audit/rules.d/siem.rules
touch /etc/audit/rules.d/siem.rules

# вставить в файл /etc/audit/rules.d/siem.rules следующее содержимое
-a always,exit -F arch=b32 -S execve -F auid>=1000
-a always,exit -F arch=b64 -S execve -F auid>=1000
-a always,exit -S accept -S accept4 -F exe=/usr/sbin/ns-slapd -k ldapconnect
-a exit,always -F exit=-EACCES -F exe=/usr/sbin/ns-slapd -k ldapconnect

# перезапустить службы
systemctl restart krb5-kdc.service auditd
```

б) настроить syslog-ng на КД

```
# создать каталог /etc/syslog-ng/siem для дальнейшего включения его в
 ↪конфигурацию службы syslog-ng и записи в него необходимых файлов
 ↪конфигурации этой службы
mkdir /etc/syslog-ng/siem

# вставить в файл /etc/syslog-ng/syslog-ng.conf следующую строку
@include "/etc/syslog-ng/siem/*.conf"

# создать набор файлов конфигурации syslog-ng и задать им права
touch /etc/syslog-ng/siem/destination.conf
touch /etc/syslog-ng/siem/output-dirsrv-access.conf
touch /etc/syslog-ng/siem/output-dirsrv-audit.conf
touch /etc/syslog-ng/siem/output-dirsrv-error.conf
touch /etc/syslog-ng/siem/output-dirsrv-security.conf
touch /etc/syslog-ng/siem/output-dns-zone.conf
touch /etc/syslog-ng/siem/output-krb-audit.conf
touch /etc/syslog-ng/siem/output-user-proc.conf
touch /etc/syslog-ng/siem/output-ldapconnect.conf
chmod 744 /etc/syslog-ng/siem/*

# вставить в файл /etc/syslog-ng/siem/destination.conf следующее содержимое
 ↪(IP-адрес заменить на реальный адрес сервера аудита из состава домена)
destination d_audit {network("100.100.100.100" transport("tcp") port(514)
 ↪flags(syslog-protocol) template("${ISODATE} ${HOST} ${MESSAGE} ${TAGS} \n
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
 ↪"));};

# вставить в файл /etc/syslog-ng/siem/output-dirsrv-access.conf следующее
 ↪содержимое
source s_access_dirsrv {file("/var/log/dirsrv/slapd-ALDPRO-LAN/access" follow-
 ↪freq(1) flags(no-parse));};
filter f_access_dirsrv {match("MOD" value("MESSAGE")) or match("DEL" value(
 ↪"MESSAGE")) or match("ADD" value("MESSAGE")) or match("SRCH" value("MESSAGE
 ↪")) or match("connection from" value("MESSAGE")) or match("RESULT" value(
 ↪"MESSAGE"));};
log {
    source(s_access_dirsrv);
    filter(f_access_dirsrv);
    rewrite {set-tag("tag-dirsrv-access");};
    destination(d_audit);
};

# вставить в файл /etc/syslog-ng/siem/output-dirsrv-audit.conf следующее
 ↪содержимое (если НЕТ необходимости в передаче данных о событии в одну
 ↪строку)
source s_audit_dirsrv {file("/var/log/dirsrv/slapd-ALDPRO-LAN/audit" follow-
 ↪freq(1) flags(no-parse) );};
log {
    source(s_audit_dirsrv);
    rewrite { set-tag("tag-dirsrv-audit"); };
    destination(d_audit);
};

# вставить в файл /etc/syslog-ng/siem/output-dirsrv-audit.conf следующее
 ↪содержимое (если ЕСТЬ необходимость в передаче данных о событии в одну
 ↪строку)
source s_audit_dirsrv {file("/var/log/dirsrv/slapd-ALDPRO-LAN/audit" multi-
 ↪line-mode(prefix-suffix) multi-line-prefix("time: [0-9]+") multi-line-
 ↪suffix("\n$") flags(no-multi-line) follow-freq(1));};
log {
    source(s_audit_dirsrv);
    rewrite { subst("^", "time: ", value("MESSAGE")); set-tag("tag-dirsrv-
 ↪audit"); };
    destination(d_audit);
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
};

# вставить в файл /etc/syslog-ng/siem/output-dirsrv-error.conf следующее
 ↪содержимое
source s_errors_dirsrv {file("/var/log/dirsrv/slapd-ALDPRO-LAN/errors" follow-
 ↪freq(1) flags(no-parse));};
log {
    source(s_errors_dirsrv);
    rewrite {set-tag("tag-dirsrv-error");};
    destination(d_audit);
};

# вставить в файл /etc/syslog-ng/siem/output-dirsrv-error.conf следующее
 ↪содержимое
source s_security_dirsrv {file("/var/log/dirsrv/slapd-ALDPRO-LAN/security"
 ↪follow-freq(1) flags(no-parse));};
log {
    source(s_security_dirsrv);
    rewrite {set-tag("tag-dirsrv-security"); };
    destination(d_audit);
};

# вставить в файл /etc/syslog-ng/siem/output-dns-zone.conf следующее
 ↪содержимое
filter f_dnszone{message('AXFR') or message('IXFR');};
log {
    source(s_src);
    filter(f_dnszone);
    destination(d_audit);
};

# вставить в файл /etc/syslog-ng/siem/output-krb-audit.conf следующее
 ↪содержимое
source s_krb_audit {file("/var/log/krb5kdc.log" follow-freq(1) flags(no-
 ↪parse) );};
filter f_krb_audit {match("AS_REQ" value("MESSAGE")) or match("TGS_REQ"
 ↪value("MESSAGE"));};
log {
    source(s_krb_audit);
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
    filter(f_krb_audit);
    rewrite {set-tag("tag-krb-audit");};
    destination(d_audit);
};

# вставить в файл /etc/syslog-ng/siem/output-user-proc.conf следующее
 ↪содержимое
source s_user_proc {file("/var/log/audit/audit.log" flags(no-parse) persist-
 ↪name("user_proc") follow-freq(1));};
filter f_user_proc {match("syscall=59" value("MESSAGE"));};
log {
    source(s_user_proc);
    filter(f_user_proc);
    destination(d_audit);
};

# вставить в файл /etc/syslog-ng/siem/output-ldapconnect.conf следующее
 ↪содержимое
source s_ldap {file("/var/log/audit/audit.log" flags(no-parse) persist-name(
 ↪"ldap_conn") follow-freq(1));};
filter f_ldapconnect {message('ldapconnect');};
log {
    source(s_ldap);
    filter(f_ldapconnect);
    destination(d_audit);
};

# перезапустить сервис syslog-ng
systemctl restart syslog-ng
```

2. Настройка сервера общего доступа к файлам для журналирования операций с общими файловыми ресурсами с помощью пакета программ Samba.

```
# в файле конфигурации /etc/samba/smb.conf  в секцию "global" добавить
 ↪следующие строки
vfs objects = full_audit
full_audit:prefix = %u|%I|%S
full_audit:success = connect, create_file, linkat, mkdirat, open, read,
 ↪renameat, unlinkat, write
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
full_audit:failure = connect, create_file, linkat, mkdirat, open, read,
 ↪renameat, unlinkat, write
full_audit:facility = local5
full_audit:priority = notice

# Если в файле конфигурации /etc/samba/smb.conf в секции "global"
 ↪присутствует следующая строка "log level = N" где N - это уровень
 ↪журналирования событий в службе, то к данной строке дописываем через
 ↪пробел строку " vfs:1". Если такой строки нет, то записываем
log level = 1 vfs:1

# создать каталог /etc/syslog-ng/siem для дальнейшего включения его в
 ↪конфигурацию службы syslog-ng и записи в него необходимых файлов
 ↪конфигурации этой службы
mkdir /etc/syslog-ng/siem

# вставить в файл /etc/syslog-ng/syslog-ng.conf следующую строку
@include "/etc/syslog-ng/siem/*.conf"

# создать набор файлов конфигурации syslog-ng и задать им права
touch /etc/syslog-ng/siem/destination.conf
touch /etc/syslog-ng/siem/output-samba.conf
chmod 744 /etc/syslog-ng/siem/*

# вставить в файл /etc/syslog-ng/siem/destination.conf следующее содержимое
 ↪(IP-адрес заменить на реальный адрес сервера аудита из состава домена)
destination d_audit {network("100.100.100.100" transport("tcp") port(514)
 ↪flags(syslog-protocol) template("${ISODATE} ${HOST} ${PROGRAM} ${MESSAGE} $
 ↪{TAGS} \n"));};

# вставить в файл /etc/syslog-ng/siem/output-samba.conf следующее содержимое
filter f_samba{program('smbd_audit');};
log {
    source(s_src);
    filter(f_samba);
    destination(d_audit);
};

# перезапустить службы
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
systemctl restart smbd winbind syslog-ng
```

3. Настройка сервера аудита из состава домена для журналирования событий с КД и с сервера общего доступа к файлам.

```
# создать каталог /etc/syslog-ng/siem для дальнейшего включения его в
 ↪конфигурацию службы syslog-ng и записи в него необходимых файлов
 ↪конфигурации этой службы
mkdir /etc/syslog-ng/siem

# вставить в файл /etc/syslog-ng/syslog-ng.conf следующую строку
@include "/etc/syslog-ng/siem/*.conf"

# создать набор файлов конфигурации syslog-ng и задать им права
touch /etc/syslog-ng/siem/destination.conf
touch /etc/syslog-ng/siem/input-dirsrv-access.conf
touch /etc/syslog-ng/siem/input-dirsrv-audit.conf
touch /etc/syslog-ng/siem/input-dirsrv-error.conf
touch /etc/syslog-ng/siem/input-dirsrv-security.conf
touch /etc/syslog-ng/siem/input-samba.conf
touch /etc/syslog-ng/siem/input-dns-zone.conf
touch /etc/syslog-ng/siem/input-krb-audit.conf
touch /etc/syslog-ng/siem/input-user-proc.conf
touch /etc/syslog-ng/siem/input-ldapconnect.conf
chmod 744 /etc/syslog-ng/siem/*

# если такого источника на сервере аудита нет (осуществить поиск подстроки "s_
 ↪net" во всех файлах конфигурации syslog-ng), то создать файл /etc/syslog-ng/
 ↪siem/source.conf и вставить в него следующее содержимое
source s_net {
    network(
        transport("tcp")
        port(514)
        flags(syslog-protocol)
        log_iw_size(65536)
        max_connections(1000)
    );
};
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
# все файлы журналов сохраняются в каталог /var/log/aldpro
# вставить в файл /etc/syslog-ng/siem/input-dirsrv-access.conf следующее
 ↪содержимое
destination d_access_dirsrv_file {file("/var/log/aldpro/access_dirsrv.log"
 ↪template("${MESSAGE}\n"));};
filter f_dirsrv_access {message("tag-dirsrv-access");};
log {
    source(s_net);
    filter(f_dirsrv_access);
    rewrite { subst(" tag-dirsrv-access,.source.s_access_dirsrv", "", value(
 ↪"MESSAGE")); };
    destination(d_access_dirsrv_file);
};

# вставить в файл /etc/syslog-ng/siem/input-dirsrv-audit.conf следующее
 ↪содержимое
destination d_audit_dirsrv_file {file("/var/log/aldpro/audit_dirsrv.log"
 ↪template("${MESSAGE}\n"));};
filter f_dirsrv_audit { message("tag-dirsrv-audit");};
log {
    source(s_net);
    filter(f_dirsrv_audit);
    rewrite { subst(" tag-dirsrv-audit,.source.s_audit_dirsrv", "", value(
 ↪"MESSAGE")); };
    destination(d_audit_dirsrv_file);
};

# вставить в файл /etc/syslog-ng/siem/input-dirsrv-error.conf следующее
 ↪содержимое
destination d_error_dirsrv_file {file("/var/log/aldpro/error_dirsrv.log"
 ↪template("${MESSAGE}\n"));};
filter f_dirsrv_error {message("tag-dirsrv-error");};
log {
    source(s_net);
    filter(f_dirsrv_error);
    rewrite { subst(" tag-dirsrv-error,.source.s_errors_dirsrv", "", value(
 ↪"MESSAGE")); };
    destination(d_error_dirsrv_file);
};
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
# вставить в файл /etc/syslog-ng/siem/input-dirsrv-security.conf следующее
 ↪содержимое
destination d_security_dirsrv_file {file("/var/log/aldpro/security_dirsrv.log
 ↪" template("${MESSAGE}\n"));};
filter f_dirsrv_security {message("tag-dirsrv-security");};
log {
    source(s_net);
    filter(f_dirsrv_security);
    rewrite { subst(" tag-dirsrv-security,.source.s_security_dirsrv", "",
 ↪value("MESSAGE")); };
    destination(d_security_dirsrv_file);
};  destination d_samba {
    file("/var/log/aldpro/samba.log" template("${MESSAGE}\n"));
};

# вставить в файл /etc/syslog-ng/siem/input-samba.conf следующее содержимое
destination d_samba {file("/var/log/aldpro/samba.log" template("${MESSAGE}\n
 ↪"));};
filter f_samba {message("smbd_audit");};
log {
    source(s_net);
    filter(f_samba);
    rewrite { subst(" .source.s_src", "", value("MESSAGE")); };
    destination(d_samba);
};

# вставить в файл /etc/syslog-ng/siem/input-dns-zone.conf следующее
 ↪содержимое
destination d_dnszone {file("/var/log/aldpro/dnszone.log" template("${MESSAGE}
 ↪\n"));};
filter f_dnszone {message('AXFR') or message('IXFR');};
log {
    source(s_net);
    filter(f_dnszone);
    rewrite {subst(" .source.s_src", "", value("MESSAGE"));};
    destination(d_dnszone);
};
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
# вставить в файл /etc/syslog-ng/siem/input-krb-audit.conf следующее
 ↪содержимое
destination d_krb_audit_file {file("/var/log/aldpro/krb_audit.log" template("
 ↪${MESSAGE}\n"));};
filter f_krb_audit {message("tag-krb-audit");};
log {
    source(s_net);
    filter(f_krb_audit);
    rewrite { subst(" tag-krb-audit,.source.s_krb_audit", "", value("MESSAGE
 ↪")); };
    destination(d_krb_audit_file);
};

# вставить в файл /etc/syslog-ng/siem/input-user-proc.conf следующее
 ↪содержимое
destination d_user_proc {file("/var/log/aldpro/userproc.log" template("$
 ↪{MESSAGE}\n"));};
filter f_user_proc {match("syscall=59" value("MESSAGE"));};
log {
    source(s_net);
    filter(f_user_proc);
    rewrite { subst(" .source.s_user_proc", "", value("MESSAGE")); };
    destination(d_user_proc);
};

# вставить в файл /etc/syslog-ng/siem/input-ldapconnect.conf следующее
 ↪содержимое
destination d_ldapconnect {file("/var/log/aldpro/ldapconnect.log" template("$
 ↪{MESSAGE}\n"));};
filter f_ldapconnect {message("ldapconnect");};
log {
    source(s_net);
    filter(f_ldapconnect);
    rewrite {
        subst(" .source.s_ldap", "", value("MESSAGE"));
        subst(' key="ldapconnect"', "", value("MESSAGE"));
    };
    destination(d_ldapconnect);
};
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
# перезапустить сервис syslog-ng
systemctl restart syslog-ng
```

3.16. Инструкция по управлению зонами ответственности при администрировании

3.16.1. Аннотация

Назначение документа: Особенности распределения зон ответственности при администрировании в крупных организациях, делегирование полномочий по подразделениям, распределение зон ответственности при администрировании через группы безопасности, понятие типов администраторов и возможностей по администрированию, настройка пользовательских типов администраторов.

3.16.2. Введение

Разграничение зон ответственности администраторов позволяет определять полномочия и/или зоны ответственности пользователей (администраторов ALD Pro), что обеспечивает удобство и информационную безопасность.

В ALD Pro реализованы следующие инструменты разграничения зон ответственности администраторов:

Пользовательские роли - создание пользовательских типов администратора, назначение их на пользователей и группы пользователей.

Назначение типа администратора - определение полномочий администраторов в соответствии с назначенным типом

Политики повышения возможностей по администрированию (SUDO) - возможность запрещать и разрешать определённым пользователям или группам выполнение конкретного набора программ, а также разрешить выполнение определённых программ без необходимости ввода своего пароля

Политики доступа к узлу (HBAC) - определение правил для настройки доступа пользователей или групп пользователей к определенным хостам с использованием определенных сервисов

3.16.3. Назначение типов администратора

3.16.3.1. Модель ALD Pro для типа администратора

Модель ALD Pro для типа администратора включает следующие сущности:

- **Разрешение** - право на выполнение операции/действия.
- **Возможности по администрированию** - “тематический” набор разрешений. Например, для управления группами пользователей необходимы разрешения на создание, удаление, редактирование группы пользователей. Эти три действия можно объединить в возможности по администрированию на управление группами пользователей. Аналогично можно создать возможности по администрированию на управление группами компьютеров.
- **Тип администратора** - набор возможностей по администрированию. Например, для выделенного типа, участники которой будут управлять только группами пользователей и группами компьютеров, можно назначить два вида возможностей (одна на управление группами пользователей, вторая - на управление группами компьютеров) вместо назначения множества разрешений на операции с группами, которые надо выбрать из большого общего списка разрешений.

Примечание: Любые возможности при администрировании запрещают создание и работу с следующими пользователями и группами пользователей.

Пользователи:

```
'root', 'daemon', 'bin', 'sys', 'sync', 'games', 'man', 'lp', 'mail', 'news',
↪ 'uucp', 'proxy', 'www-data', 'backup', 'list', 'irc', 'gnats', 'nobody',
↪'systemd-timesync', 'systemd-network', 'systemd-resolve', '_apt',
↪'messagebus', 'sshd', 'systemd-coredump', '_chrony', 'postgres',
↪'opendnssec', 'zabbix', '_rpc', 'statd', 'redis', 'sssd', 'custodia',
↪'dirsrv', 'bind', 'gluster', 'pkiuser', 'kdcproxy', 'ipaapi'
```

Группы пользователей:

```
'root', 'daemon', 'bin', 'sys', 'adm', 'tty', 'disk', 'lp', 'mail', 'news',
↪'uucp', 'man', 'proxy', 'kmem', 'dialout', 'fax', 'voice', 'cdrom', 'floppy
↪', 'tape', 'sudo', 'audio', 'dip', 'www-data', 'backup', 'operator', 'list',
↪ 'irc', 'src', 'gnats', 'shadow', 'utmp', 'video', 'sasl', 'plugdev',
↪'staff', 'games', 'users', 'nogroup', 'systemd-journal', 'systemd-timesync',
↪ 'systemd-network', 'systemd-resolve', 'crontab', 'input', 'kvm', 'render',
↪ 'netdev', 'messagebus', 'ssh', 'astra-admin', 'astra-console', 'systemd-
↪coredump', 'softhsm', '_chrony', 'ssl-cert', 'postgres', 'opendnssec',
↪'zabbix', 'redis', 'rdma', 'sssd', 'custodia', 'dirsrv', 'bind', 'gluster',
↪ 'sambashare', 'winbindd_priv', 'pkiuser', 'kdcproxy', 'ipaapi'
```

Функция назначения типа администратора предназначена для предоставления списка разрешений, т.е. действий, доступных обладателю конкретного типа администратора. Набор разрешений логически объединен в возможности. Конкретный вид возможности позволяет управлять только заданной группой параметров.

По умолчанию наборы возможностей разграничены между следующими типами:

- предустановленная роль главного администратора;
- роли для администрирования подразделов портала управления;
- роль на чтение всего портала;
- роль регионального администратора.

У пользователей есть возможность создать свои типы администраторов с требуемыми наборами возможностей.

Список доступных опций для каждого типа содержится в разделе **Управление доменом — Роли и права доступа — Типы администратора в системе — Таблица соответствий «Возможность (Доступный раздел/подраздел) - Роль администратора»**

В ALD Pro реализован механизм суммирования типов, т.е. при назначении пользователю нескольких типов все доступные возможности и разрешения суммируются.

Учетная запись, которой не присвоен ни один системный тип, имеет доступ только к Личному кабинету и не может использовать другие функции Системы.

Тип главного администратора по умолчанию назначен учетной записи admin.

Кроме типов администратора в разделе представлены базовые типы FreeIPA:

- ALDPRO - CIFS server

- ALDPRO - Organization units
- ALDPRO - Organizational Units Service Account
- ALDPRO - RuPost Service Integrations
- ALDPRO - SaltStack Administrators
- ALDPRO - Service Role
- ALDPRO - Trusts Service Account
- Enrollment Administrator
- helpdesk
- Security Architect
- User Administrator

Примечание: При назначении пользователю типа администратора для работы с порталом ALD Pro рекомендуется использовать типы, созданные пользователем, и типы с префиксом ALDPRO: предустановленный и пользовательские. Использование базовых типов FreeIPA без префекса ALDPRO не рекомендуется.

Для просмотра списка функций (возможностей при администрировании) доступных для конкретного типа администратора необходимо выбрать наименование необходимого типа, после чего, справа в связанной таблице отобразится перечень возможностей администратора (список разделов, подразделов ALD Pro, доступных для данного типа).

3.16.4. Управление типами администратора

Управление типами администратора доступно:

- из карточки **роли администратора**;
- из **карточки пользователя**.

Управление типами администратора из карточки роли осуществляется в разделе **Управление доменом — Роли и права доступа — вкладка Роли в системе - карточка Роли**. На вкладке в списке **Выбранные пользователи** приведен список пользователей, наделенных данным типом администратора. Доступна опция настройки данного списка.

Управление типами администратора из карточки пользователя осуществляется в разделе **Пользователи и компьютеры — Пользователи — карточка Пользователя — вкладка**

Роли. На вкладке задаются типы, которыми будет наделена учетная запись пользователя.

3.16.5. Политики повышения возможностей при администрировании (SUDO)

Команда sudo (Substitute User and do, дословно «подменить пользователя и выполнить») предоставляет возможность пользователям выполнять команды от имени суперпользователя root, либо других пользователей. Правила, используемые sudo для принятия решения о предоставлении доступа, находятся в файле `/etc/sudoers` (для редактирования файла можно использовать специальный редактор `visudo`, запускаемый из командной строки без параметров, в том числе без указания пути к файлу); язык их написания и примеры использования подробно изложены в `man sudoers`.

В большинстве случаев грамотная настройка sudo делает небезопасную работу от имени суперпользователя ненужной. Все действия оказываются выполнимы из-под аккаунта пользователя, которому разрешено использовать sudo без ограничений. Имеется возможность запрещать и разрешать определённым пользователям или группам выполнение конкретного набора программ, а также разрешить выполнение определённых программ без необходимости ввода своего пароля.

ALD Pro позволяет настраивать правила разрешения и запрета на использование sudo для пользователей и групп пользователей. В правилах могут задаваться:

- Пользователи (группы пользователей), к которым применяются правила;
- Команды (группы команд), которые можно (нельзя) выполнять этим пользователям с применением sudo;
- Компьютеры (группы компьютеров), на которых применяется правило;
- Опции команды sudo, использующиеся при применении правила.

При инициализации контроллера (реплики) FreeIPA или при вводе клиента в домен FreeIPA система автоматически конфигурируется так, чтобы команда sudo использовала доменную службу sssd как источник данных о разрешениях использования sudo. Эта конфигурация задается в файле `/etc/nsswitch.conf`:

```
sudoers: files sss
```

где:

files — использовать данные из локального файла `/etc/sudoers`; sss — использовать

данные, предоставленные службой sssd.

Служба sssd, в свою очередь, настроена таким образом, чтобы получать данные по правилам sudo от доменной службы каталогов (LDAP). Подробная информация по работе команды sudo приведена в справочной системе man sudo, man sudoers.

Примечание: Правила sudo не могут применяться к встроенной доменной группе хостов ipaserver, т.к. эта группа не имеет свойства mepmanagedentry, следовательно, не имеет в objectclass запись mepOriginEntry, что необходимо для идентификации группы. Это является особенностью схемы в FreeIPA.

Служба sssd выполняет кеширование данных с периодом обновления по умолчанию 5400 секунд. Для немедленного применения правил sudo необходимо очистить кеш, выполнив на клиентской машине следующие команды:

```
sudo systemctl stop sssd
sudo rm /var/lib/sss/db/*
sudo systemctl start sssd
```

Или воспользоваться инструментом sssctl, входящим в пакет sssd-tools:

```
sudo sssctl cache-remove
```

3.16.5.1. Команды sudo

В разделе Групповые политики — Политики повышения привилегий — вкладка Команды Sudo перечислены зарегистрированные команды Sudo, которые могут быть затронуты при создании правил Sudo. Регистрация команд Sudo осуществляется вручную.

Регистрация команды для использования в правилах sudo

Команды, которые будут далее использоваться в правилах sudo (т.е. которые далее могут выполняться от имени sudo указанными в правилах пользователями) должны быть зарегистрированы. Зарегистрировать можно любую команду, имеющуюся в системе, на которой будет применяться правило. Для регистрации:

1. Перейти в раздел Групповые политики — Политики повышения привилегий —

вкладка Команды Sudo;

2. Кликнуть кнопку “+ Новая команда”;
3. В появившемся окне карточки команды Sudo:
    - Указать полный путь расположения команды, которая должна выполняться от имени sudo (например, текстовый редактор `nano`, имеющий полный путь `/usr/bin/nano`);
    - Узнать полный путь расположения команды можно командой `which`, например `which nano`

Примечание: Пути расположения команд стандартны и обычно зависят от системы, однако в случае нестандартных системе может понадобиться получить пути на той машине, на которой будет применяться правило.

- Опционально указать описание команды в произвольной форме.

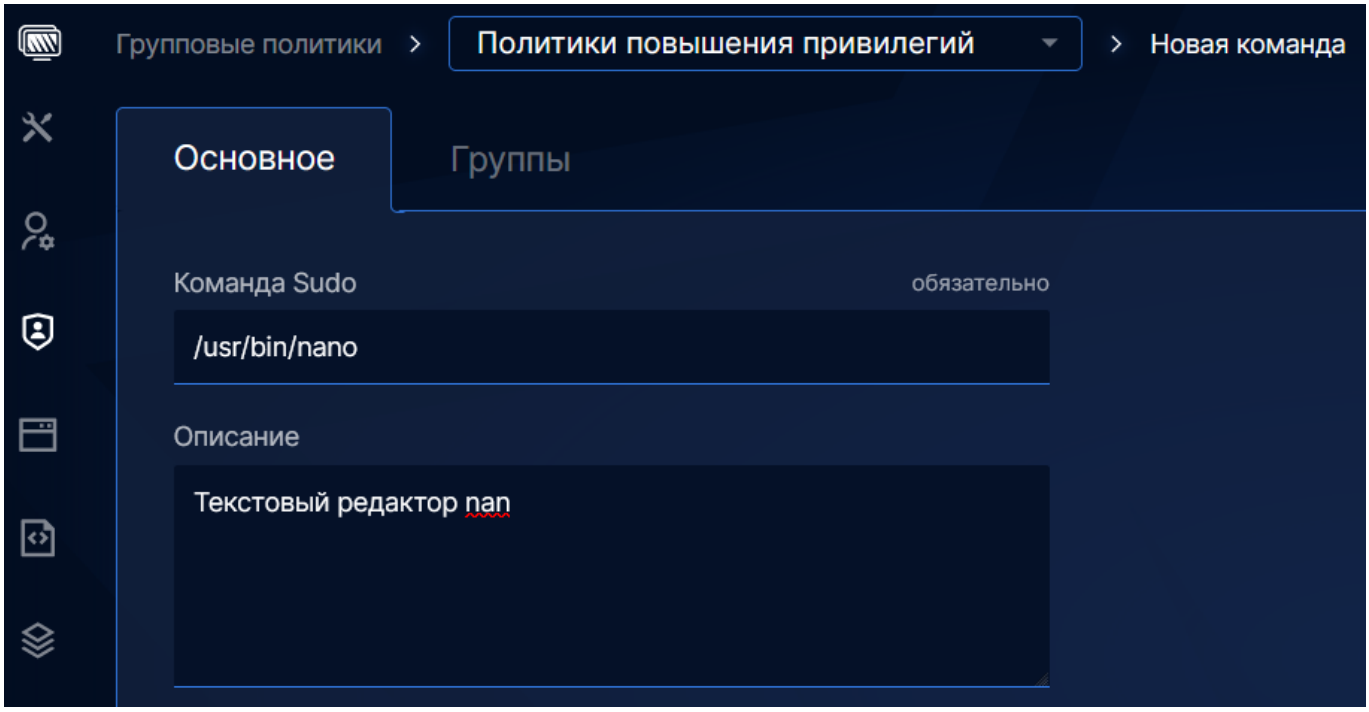


Рисунок 3.100 – Новая команда sudo

- Для сохранения и редактирования вкладки Группы нажать “Сохранить”. В результате указанная команда будет добавлена в список зарегистрированных команд. Далее эту команду можно будет использовать в правилах `sudo`.
- Во вкладке **Группы** опционально настроить список групп команд sudo, в которые

должны быть включена вновь добавленная команда.

3.16.5.2. Группы команд Sudo

В разделе **Групповые политики — Политики повышения привилегий — вкладка Группы команд Sudo** для удобства администратора возможно объединять несколько команд Sudo в группу.

Для создания новой группы команд Sudo необходимо нажать на кнопку **+ Новая группа**, будет выполнен переход в карточку новой группы. В карточке заполнить обязательное поле **Имя группы** и нажать кнопку **Сохранить**. Новая группа служб успешно создана, после чего доступен просмотр и настройка данной группы из ее карточки. Карточка группы содержит вкладки:

- **Основное** - отображается информация о группе команд Sudo: ее название и описание. Для редактирования доступно описание группы.
- **Команды** - осуществляется добавление команд Sudo в состав данной группы команд Sudo.

Для добавления команд Sudo в состав данной группы необходимо в списке **Все команды** отметить требуемые записи и перенести их в список **Выбранные команды**.

3.16.5.3. Создание правила sudo

Для создания нового правила sudo:

1. Перейти в раздел **Групповые политики — Политики повышения привилегий — вкладка Правила Sudo**.
2. Кликнуть кнопку **+ Новое правило**, будет выполнен переход в карточку нового правила.
3. В карточке на вкладке **Основное** заполнить обязательное поле **Имя правила**. Остальные вкладки станут доступны после сохранения правила.

Настройка параметров правила sudo

Настройка правила sudo осуществляется во вкладках:

- **Параметры** — параметры для команды sudo. Например, наиболее распространенная опция - не запрашивать пароль у пользователя при использовании команды sudo (опция “!authenticate”). Если в правиле указать эту опцию, то указанные в правиле команды можно будет выполнять через sudo без ввода пароля, если опция не используется - то потребуется ввести пароль пользователя, выполняющего команду. Полный список поддерживаемых параметров см. в справочной системе: man sudoers
- **Пользователи** — список пользователей и групп пользователей, которым разрешено применять sudo в соответствии с правилом. Можно разрешить применять правило всем пользователям (группам пользователей);
- **Компьютеры** — список узлов в домене, на которых применяется правило. Можно разрешить применять правило на всех узлах;
- **Команды Sudo** — команды, к которым применяется данное правило. Возможно “Разрешить” или “Запретить” выполнение команды или группы команд (порядок объединения команд в группы см. далее), также возможно разрешить выполнять все команды;
- **Запуск от имени** — от имени какого пользователя или группы пользователей (не root-пользователя) может быть выполнена команда. При добавлении группы пользователей в “Группы пользователей запуска от имени” для выполнения команды могут использоваться идентификаторы пользователей (UID) членов этой группы. При добавлении в “Группы запуска от имени” для выполнения команды могут использоваться GID этой группы.

После внесения изменений в правило следует убедиться, что все изменения сохранены (кнопка **Сохранить** в начале формы) и нажать эту кнопку для сохранения изменений если она доступна.

3.16.5.4. Удаление или отключение правила

Для удаления или отключения правила:

1. Выбрать из списка правило, которое необходимо отключить или удалить;
2. Для отключения правила нажать кнопку **Отключить**, для удаления — **Удалить**.

3.16.6. Политики доступа к узлу (HBAC)

HBAC (Host-based access control) — набор правил для настройки доступа пользователей или групп пользователей к определенным хостам с использованием определенных сервисов. Например:

- ограничение доступа по ssh к контроллеру домена определенной локации только для группы администраторов этой локации;
- разрешение использовать только определенную службу для доступа определенным пользователям на определенных хостах.

Примечание:

- Правила предоставляют только разрешения доступа. Правила запрета доступа настроить невозможно.
- В домене ALD Pro по умолчанию установлено правило `allow_all`, которое после настройки и проверки своих правил следует отключить.
- FreeIPA хранит основную группу пользователя в виде числового значения атрибута gidNumber. В связи с этим, правила HBAC могут ссылаться только на дополнительные группы пользователя, но не на его основную группу.

3.16.6.1. Службы HBAC

В разделе **Групповые политики — Политики доступа к узлу — вкладка Службы HBAC** перечислены службы и программы, которые могут быть затронуты при создании правил HBAC. Например, `ftp, sshd, su, login`.

Администратор имеет возможность добавить любые необходимые службы.

3.16.6.2. Группы служб HBAC

В разделе **Групповые политики — Политики доступа к узлу — вкладка Группы служб HBAC** для удобства администратора возможно объединять несколько служб HBAC в группу.

Для создания новой группы служб необходимо нажать на кнопку **+ Новая группа**, будет

выполнен переход в карточку новой группы. В карточке заполнить обязательное поле **Имя группы** и нажать кнопку **Сохранить**. Новая группа служб успешно создана, после чего доступен просмотр и настройка данной группы из ее карточки. Карточка группы содержит вкладки:

Основное - отображается информация о группе служб: ее название и описание. Для редактирования доступно описание группы.

Службы - осуществляется добавление служб HBAC в состав данной группы служб.

Для добавления служб HBAC в состав данной группы необходимо в списке **Все службы** отметить требуемые записи и перенести их в список **Выбранные службы**.

3.16.6.3. Добавление правила HBAC

В разделе **Групповые политики — Политики доступа к узлу — вкладка Правила HBAC** нажать кнопку **+ Новое правило**, откроется окно, в котором необходимо указать имя правила и нажать кнопку **Сохранить**. Новое правило успешно создано, после чего доступен просмотр и настройка данного правила из его карточки. Карточка правила содержит вкладки:

Основное - содержит информацию о правиле (название и описание) и опцию включения/отключения правила.

Пользователи - осуществляется настройка списка пользователей и/или групп пользователей, на которых будет применяться данное правило.

Компьютеры - осуществляется настройка списка рабочих станций и/или групп рабочих станций, на которые будет применяться данное правило.

Службы HBAC - осуществляется настройка списка служб и/или групп служб, использование которых будет регулироваться данным правилом.

Допускается указывать совместно пользователей и группы пользователей, компьютеры и группы компьютеров, службы и группы служб. При этом, если в группе находится только один элемент, и эта группа уже добавлена, то добавить этот элемент отдельно невозможно.

3.16.6.4. Отключение и удаление правила

Для отключения правила HBAC необходимо перейти в карточку правила и выбрать **Выключено**.

Удаление правила HBAC доступно как из карточки правила так и из общего списка правил.

Для удаления правила HBAC из карточки необходимо перейти в карточку правила, кликнуть кнопку **Удалить правило** и подтвердить удаление.

Для удаления правила из списка необходимо перейти к списку правил, отметить чек-боксом правило (несколько правил) на удаление и кликнуть кнопку **Удалить**.

3.17. Рекомендации по настройке hostname & fqdn

3.17.1. Введение

Компьютеры в домене используют fqdn имена, поэтому администраторам крайне важно понимать механизм их формирования. В операционных системах Linux для получения ответа на этот вопрос используется информация сразу из нескольких источников.

3.17.2. Рекомендации

Утилита **hostname** без параметров возвращает локальное имя машины из файла виртуальной системы ядра `/proc/sys/kernel/hostname`. Есть так же файл `/etc/hostname`, который позволяет менять имя, но изменения вступают в силу только после перезагрузки. Можно поменять имя хоста без перезагрузки, используя утилиту `hostnamectl set-hostname`

При использовании дистрибутивов Debian рекомендуют в качестве имени хоста устанавливать короткое имя, например, «pc-1», а не полное доменное имя fqdn, например, «pc-1.ald.company.local». В этом случае при вызове утилиты hostname без параметров будет отображаться значение «pc-1». Но можно в качестве имени хоста установить и полное имя fqdn, т. е. «pc-1.ald.company.local», тогда очевидно, что вызов hostname без параметров будет уже выдавать «pc-1.ald.company.local», а не «pc-1». Разница проявит себя в тех ситуациях, где используется имя хоста, например:

1) Утилита hostname с ключом -f в соответствии с настройками `/etc/nsswitch.conf` сначала ищет fqdn хоста по файлу `/etc/hosts`, который содержит строки вида:

```
IP-адрес каноническое_имя_узла [псевдонимы…]
```

Алгоритм берет локальное имя хоста и ищет в файле `/etc/hosts` строку с этим именем, если оно было найдено, возвращает каноническое имя из строки, как fqdn хоста.

Если в качестве hostname будет выступать fqdn, то поиск сработает, но не по псевдониму из строки, а по каноническому имени узла.

2) Если в файле `hosts` искомая запись не найдена, то в соответствии с настройками `/etc/nsswitch.conf` выполняется поиск хоста по DNS. Так как имя hostname, например, «pc-1», не содержит точек (см. параметр ndots), то к нему добавляется суффикс search из файла `/etc/resolv.conf`, например, «ald.company.local» и получает полное имя fqdn «pc-1.ald.company.local», и запрашивает A- и AAAA-записи для этого fqdn у DNS сервера. Если DNS сервер вернет какую-нибудь запись, пусть даже с IP адресом, который не назначен ни одному из интерфейсов этого компьютера, то этот fqdn будет считаться валидным.

При вводе машины в домен инструментами ALD Pro именем хоста устанавливается fqdn. При вводе в домен ванильного Debian с помощью ванильного freeipa клиента поведение продукта в части hostname аналогичное — именем хоста устанавливается fqdn машины. Такой подход принят в Red Hat, и он наследуется при использовании FreeIPA, т. к. она сейчас разрабатывается как upstream Red Hat IdM.

При данном подходе вызов команды hostname без параметров будет выдавать fqdn хоста. Для серверов будет правильно указать в файле `/etc/hosts` строку, которая будет соответствовать этому fqdn, чтобы hostname -f работал без обращения к DNS, это и быстрее и надежнее.

На серверах предпочитаемая форма `hosts` выглядит следующим образом:

```
127.0.0.1 localhost
10.0.1.2 dc-1.ald.domain.local dc-1
# 127.0.1.1 dc-1 - данную строку нужно закомментировать или удалить, т.к.
 ↪адрес локальной петли будет иметь приоритет по отношению к любому другому
 ↪локальному адресу
```

На клиентских машинах и серверах, где нет служб, настроенных на конкретный адрес локальной сети, можно разрешать доменное имя в IP адрес локальной петли.

```
127.0.0.1 localhost
127.0.1.1 pc-1.ald.domain.local pc-1
```

Если у вас в hosts есть две записи для имени сервера, то при разрешении имени сервера предпочтение отдается адресу 127.0.1.1, так как он имеет больший приоритет. Настройки приоритетов указаны в файле `/etc/gai.conf`.

```
127.0.0.1 localhost
127.0.1.1 pc-1.ald.domain.local pc-1
10.0.1.2  pc-1.ald.domain.local pc-1
```

3.18. Наследование и суммирование параметров групповых политик

3.18.1. Аннотация

Настоящий документ объясняет порядок наследования и суммирования параметров групповых политик в ALD Pro в сравнении с Microsoft Active Directory (MS AD).

3.18.2. Термины и определения

Термин	Альтернатива	Определение
Групповая политика	ГП	Разделы параметров, с помощью которых можно выполнить централизованную настройку ОС и окружения пользователя. Например, «безопасность», «оборудование», «сеть», «система»

продолжение на следующей странице

Таблица 3.35 – продолжение с предыдущей страницы

Термин	Альтернатива	Определение
Объект групповой политики	ГПО, group policy object, gpo, Объект ГПО	Именованный набор параметров с конкретными значениями, которые могут быть назначены на структурные подразделения. В ALD Pro соответствуют записям в DN `cn=gpolicy,cn=gp,cn=domain_suffix`
Параметр групповой политики		Именованный набор атрибутов, которые позволяют сконфигурировать определенную функцию операционной системы или окружения пользователя. Например, параметр «Переменная окружения» объединяет такие атрибуты как «Имя переменной» и «Значение переменной»
Атрибут параметра групповой политики		Именованное значение, которое позволяет управлять конкретной настройкой операционной системы или окружения пользователя. Например, атрибуту «Имя переменной» можно присвоить значение «var1»

продолжение на следующей странице

Таблица 3.35 – продолжение с предыдущей страницы

Термин	Альтернатива	Определение
Связанный объект ГП	Связанный ГПО, Назначенный ГПО, gpo link	Объект групповой политики, назначенный на конкретное подразделение. В ALD Pro соответствуют записям в DN `cn=gprules,cn=gp,dc=domain_suffix`
Наследуемые ГПО		Объекты групповых политик, назначенные на родительские подразделения, параметры которых по умолчанию наследуются дочерними подразделениями. В ALD Pro соответствуют записям в DN `cn=gprules,cn=gp,dc=domain_suffix`
Простой параметр		Параметр групповой политики, имеющий один список атрибутов
Составной параметр	Списочный параметр	Параметр групповой политики, атрибуты которого представлены массивом списков
Подразделение	Organizational unit, ou	Структурные подразделения организации, предназначенные для группировки объектов, чтобы на них можно было назначать ГПО. В ALD Pro соответствуют записям в DN `cn=orgunits,cn=accounts,dc=domain_suffix`

продолжение на следующей странице

Таблица 3.35 – продолжение с предыдущей страницы

Термин	Альтернатива	Определение
Приоритет		Целое число, определяющее порядок применения параметров ГПО, если на одно подразделение назначено несколько объектов. Если у объекта приоритет равен единице, то его параметры будут применяться в самую последнюю очередь и смогут переопределить все ранее установленные значения в соответствии с правилами суммирования. В ALD Pro соответствует атрибуту `rbtaprioritypolicy` в `gprules`
Флаг «Отключить наследование»	block inheritance	Устанавливается для подразделения и позволяет отключить наследование параметров, определенных в объектах групповых политик, назначенных на родительские (вышестоящие) подразделения

продолжение на следующей странице

Таблица 3.35 – продолжение с предыдущей страницы

Термин	Альтернатива	Определение
Флаг «Наследовать принудительно»	enforced	Устанавливается для связанного объекта ГП (gpo link) и позволяет сделать наследование параметров соответствующего объекта обязательным на все дочерние подразделения, даже если где-то наследование отключено. В ALD Pro еще нет этого параметра, должен стать атрибутом записей в DN `cn=gprules,cn=gp,dc=domain_suffix`
Флаг «Связь включена»	Link Enabled	Устанавливается для связанного объекта ГП (gpo link) и позволяет отключить применение параметров соответствующего объекта, не удаляя назначение ГПО на структурное подразделение

продолжение на следующей странице

Таблица 3.35 – продолжение с предыдущей страницы

Термин	Альтернатива	Определение
Флаг «Состояние объекта групповой политики»	GPO Status	Устанавливается для ГПО и позволяет отключить применение параметров этого объекта, не удаляя настроек. Переключатель имеет следующие состояния: • Все параметры (enabled) - применяются все параметры ГПО при его назначении на структурное подразделение, • Параметры пользователей, • Параметры компьютеров

3.18.3. Предварительные настройки

3.18.3.1. Создание дополнительных параметров групповых политик

Если для работы с функционалом групповых политик будут созданы дополнительные параметры групповых политик, необходимо воспользоваться разделом **Портал управления. Настройка и работа → Групповые политики → Групповые политики → Создание групповой политики**.

3.18.3.2. Создание объекта групповой политики

Для создания объектов групповой политики необходимо перейти в раздел **Портал управления. Настройка и работа → Групповые политики → Групповые политики**

3.18.4. Наследование

В домене **ALD Pro** назначить объект групповой политики (далее - ГПО) возможно только на подразделения. ГПО, назначенный на подразделение, называется связанным объектом групповой политики. Назначение ГПО на подразделение возможно 2 способами:

- Групповые политики → Групповые политики → {Имя ГПО} → Подразделения;
- Более удобный способ: Пользователи и компьютеры → Организационная структура → {Имя подразделения} → Групповые политики.

При назначении ГПО на структурное подразделение, его параметры по умолчанию наследуются пользователями/компьютерами всех нижестоящих подразделений. На рис. 1 показано, что на Целевой компьютер распространяется действие как объектов групповой политики ГПО-7 и ГПО-8, назначенных на OU3 напрямую, так и объектов ГПО-1 … ГПО-6, назначенных на вышестоящие подразделения. Приоритет ГПО - это выставленный пользователем приоритет ГПО в рамках выбранного подразделения. Порядок применения - порядок в котором параметры ГПО будут суммироваться.

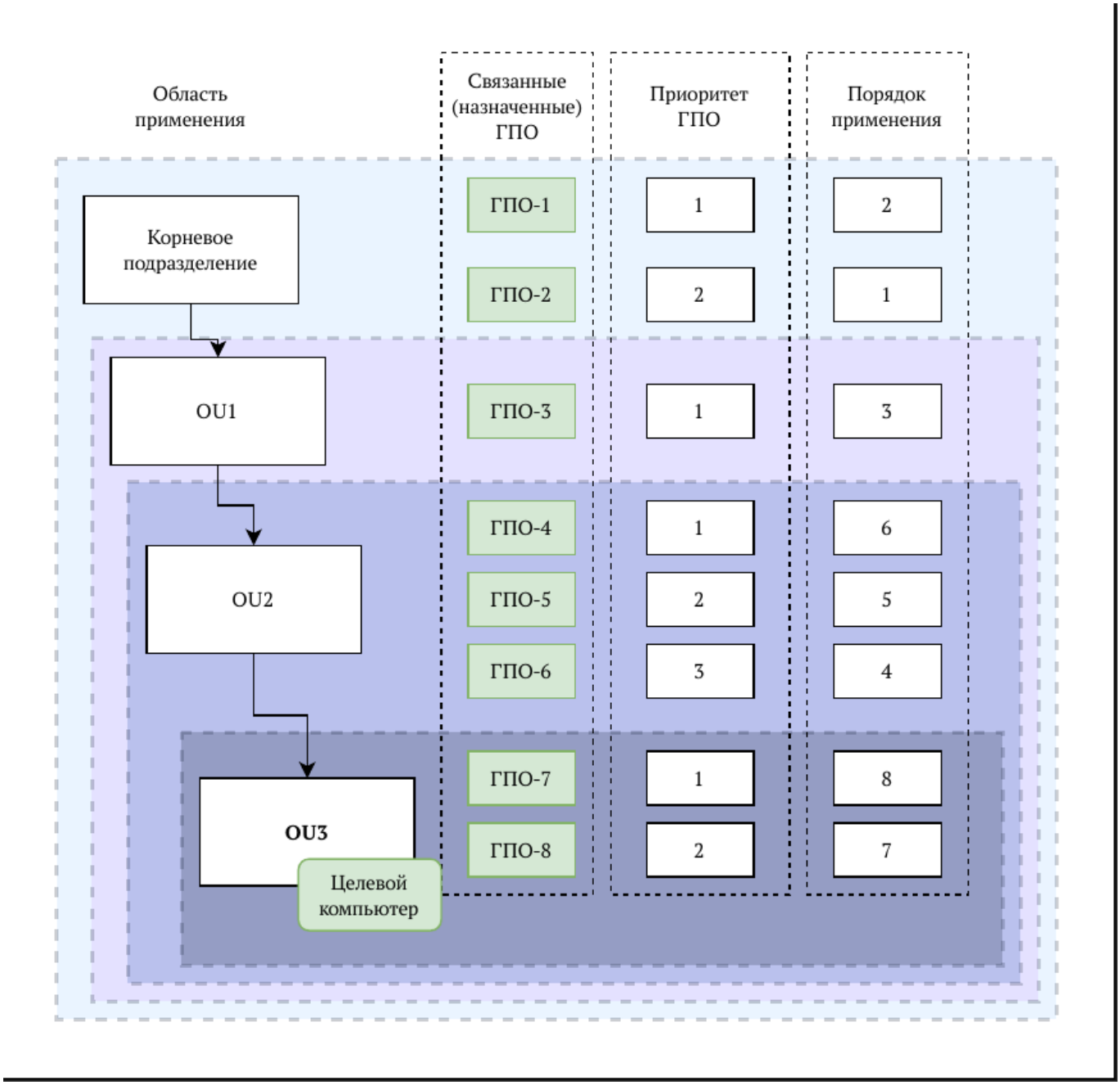


Рис. 1. Порядок наследования суммирования групповых политик

3.18.4.1. Флаг «Отключить наследование»

С 2.4.0 в домене **ALD Pro** для структурного подразделения можно установить флаг **Включить наследование** (аналог `Block Inheritance` (отключить наследование) в MS AD), что позволит включать и отключить наследование параметров, определенных в объектах групповых политик, назначенных на родительские (вышестоящие) подразделения, см. рисунок 2.

По умолчанию наследование включено для всех подразделений. Функция удобна для отладки или если в рамках организационной структуры есть объекты, на которые нужно назначить принципиально иные настройки. Например, в рамках московского офиса может быть open space или компьютерный класс, для которых проще задать настройки заново, чем переопределять общие настройки, заданные для офиса в целом.

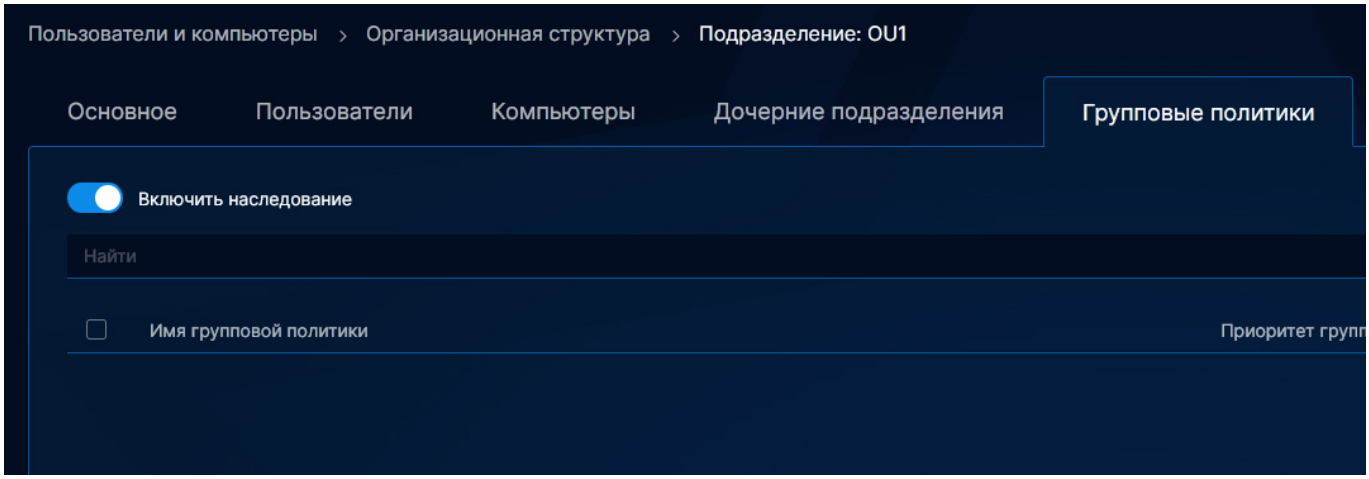


Рис. 2. Включение наследования ГПО для структурного подразделения в интерфейсе ALD Pro

Если отключить наследование для OU1, то объекты групповой политики ГПО-1 и ГПО-2, назначенные на Корневое подразделение, перестанут распространять свое действие на Целевой компьютер. Применяться будут только объекты ГПО-3 … ГПО-8, см. рисунок 3.

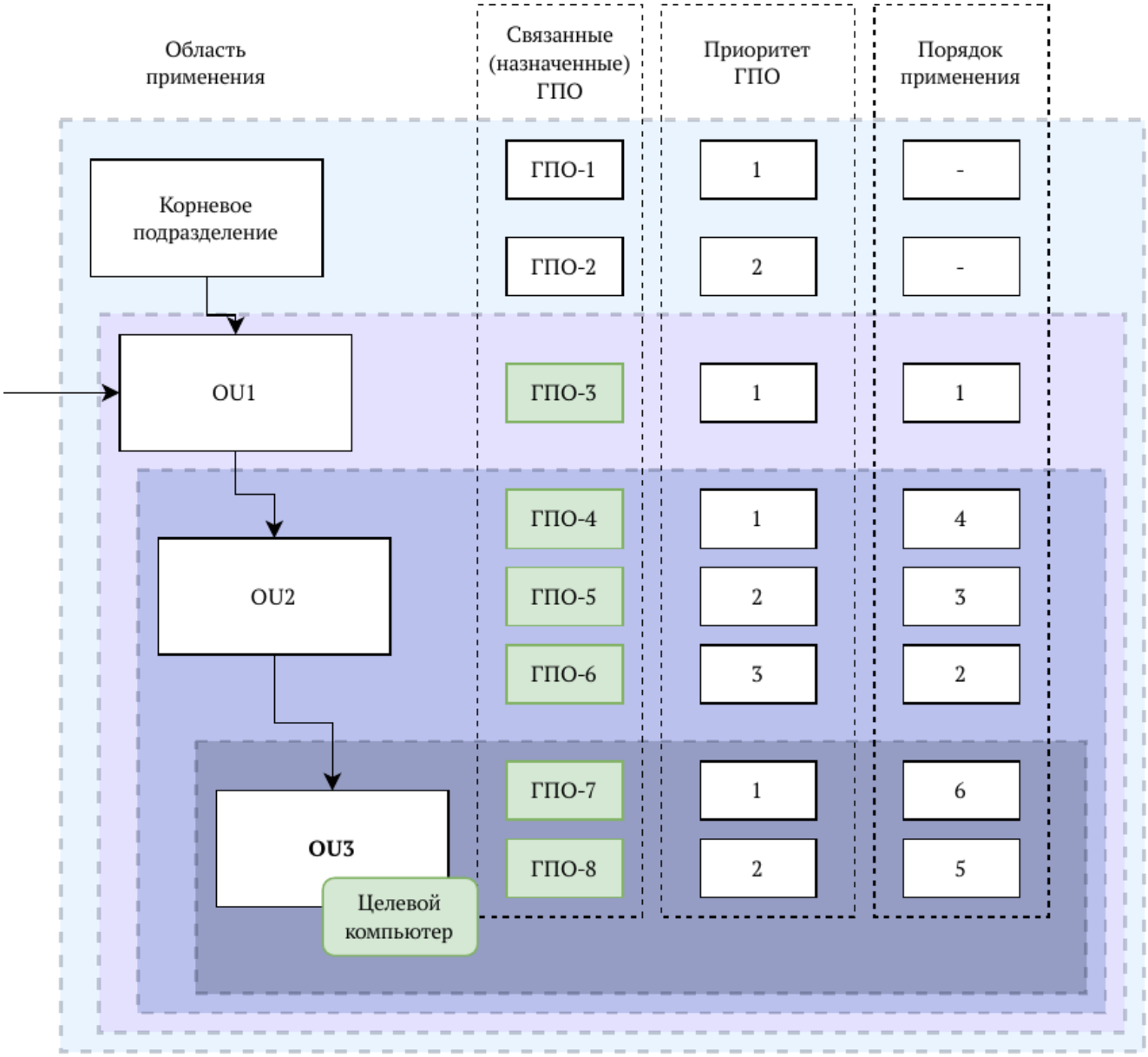


Рис. 3. Иллюстрация работы блокировки наследования ГПО для структурного подразделения

3.18.4.2. Флаг «Наследование принудительно»

С **ALD Pro** версии 2.4.0 для связанного ГПО, можно установить флаг **Наследовать принудительно** (аналог флага `Enforced` (Наследовать принудительно) в MS AD), что позволит сделать наследование параметров соответствующего объекта групповой политики обязательным для всех дочерних подразделений, даже если где-то наследование отключено, см. рисунок 4.

По умолчанию флаг выключен для всех ГПО. Более того, связанные ГПО, отмеченные флагом **Наследовать принудительно**, применяются после обычных ГПО, поэтому переопределяют их значения. То есть алгоритм суммирования имеет два вложенных цикла, сначала суммирует параметры обычных ГПО, потом сверху накладывает суммирование `Enforced` ГПО. Функция удобна, например, для настройки параметров безопасности, действие которых должно распространяться на все структурные подразделения, вне зависимости от того, используется ли отключение наследования или нет.

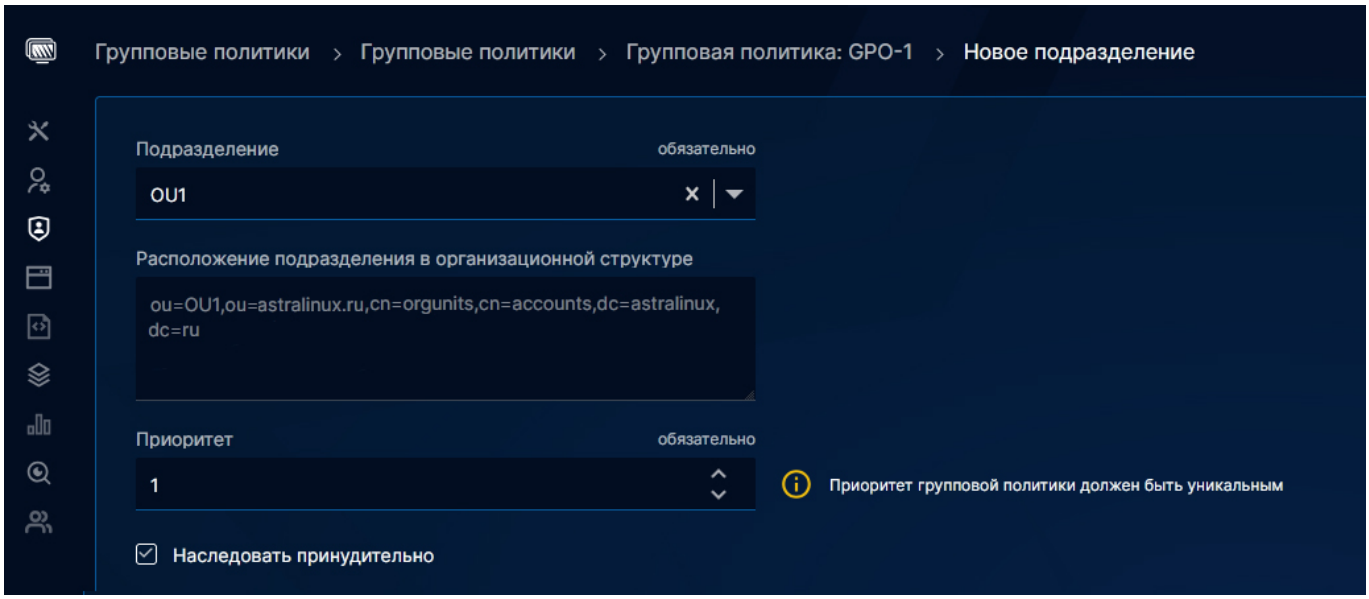


Рис. 4. Включение принудительного наследования параметров для связанного ГПО в интерфейсе ALD Pro

Если для ГПО-1 включить флаг принудительного наследования, то параметры этого объекта будут применяться к Целевому компьютеру, несмотря на то, что для OU1 установлен флаг на запрет наследования. В итоге будут применяться объекты ГПО-1, ГПО-3 … ГПО-8, см. рисунок 5.

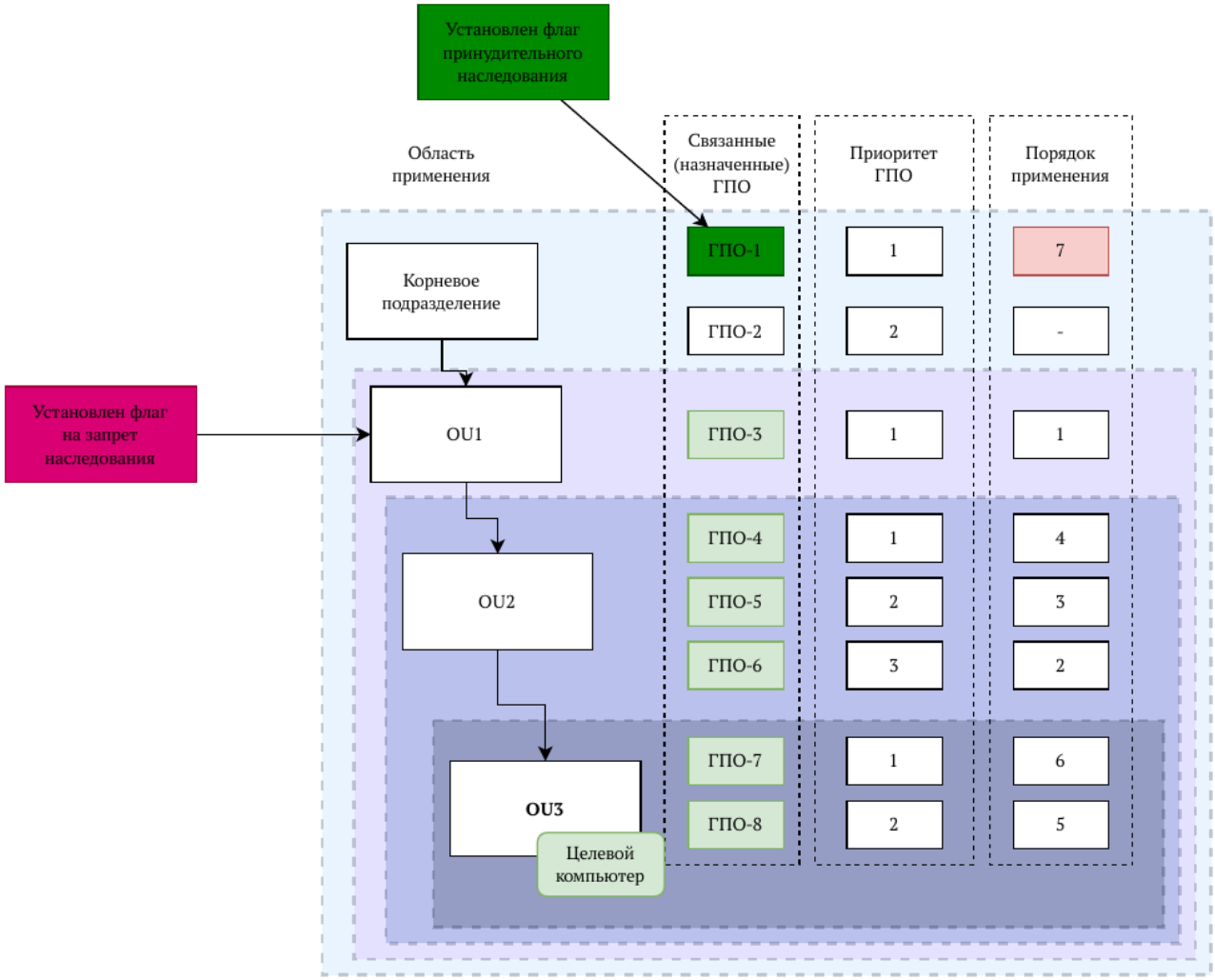


Рис. 5. Иллюстрация работы флага принудительного наследования для ГПО

3.18.5. Суммирование

3.18.5.1. Порядок суммирования

Если пользователь или компьютер попадает в область действия нескольких объектов групповых политик, их параметры суммируются следующим образом:

1. Если на одно и тоже структурное подразделение назначено несколько объектов групповых политик, то порядок применения параметров устанавливается с помощью приоритета. Приоритет представляет из себя целое число, если приоритет равен единице, то параметры этого ГПО будут применяться в самую последнюю очередь и смогут переопределить ранее установленные значения в случае конфликтов. На

рисунке 6 показано, что на подразделение OU3 назначено два объекта GPO-7 и GPO-8 и первым из них применяется GPO-8, т.к. у него приоритет 2, а вторым GPO-7, поэтому параметры GPO-7 будут перетирать параметры GPO-8 в случае конфликтов.

2. Если ГПО назначены на разные подразделения, то порядок их применения определяется иерархией подразделений. Чем ближе ГПО по иерархии к целевому пользователю/компьютеру, тем позже будут применяться параметры этого объекта, поэтому параметры этого ГПО смогут переопределить ранее установленные значения в случае конфликтов. На рисунке 6 показано, что GPO-1 и GPO-2, назначенные на корневое подразделение, применяются в самом начале, а GPO-7 и GPO-8, которые назначены на OU3, в котором компьютер находится непосредственно, выполняются в последнюю очередь.

Конфликтом считается если на целевого пользователя/компьютер назначено несколько одинаковых параметров групповых политик, которые наследуются от разных ГПО.

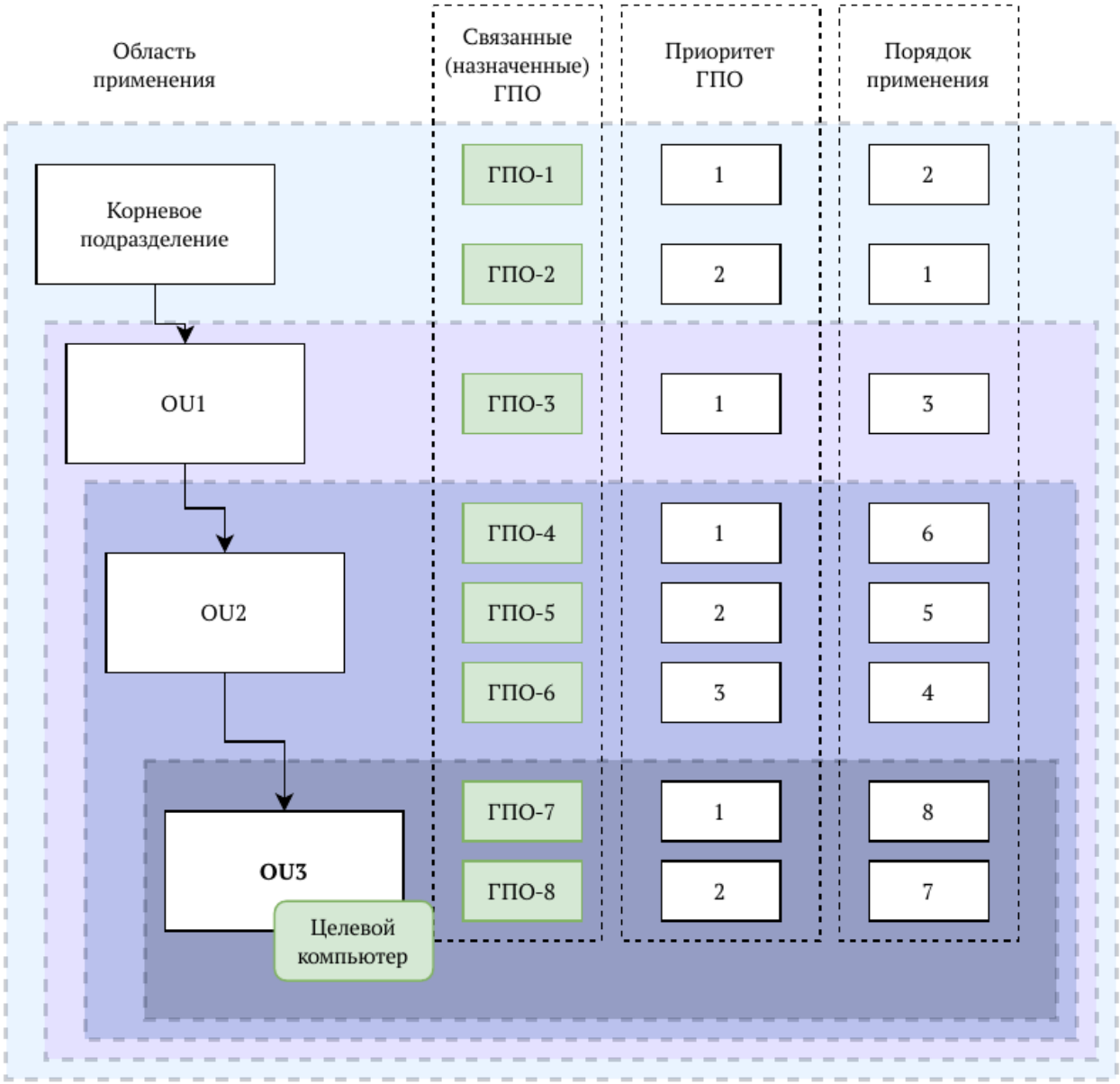


Рис. 6. Порядок суммирования ГПО

3.18.5.2. Механика разрешения конфликтов для простых параметров

Простой параметр имеет один список атрибутов, и если такой параметр определен в нескольких ГПО, остается один список значений атрибутов согласно правилам суммирования и наследования. В этом случае берется список атрибутов целиком, и, если какие-то из атрибутов не определены, то будет взято его «пустое» значение.

3.18.5.3. Механика разрешения конфликтов для составных (списочных) параметров

В домене ALD Pro есть составные (списочные) параметры для которых можно задавать таблицу однотипных таблицу атрибутов, например, ярлыки, принтеры и т.п. Если такой параметр определен в нескольких объектах ГПО, то после суммирования получатся результирующий массив строк в том же порядке, в котором параметры должны применяться на целевом хосте. Бизнес-логика разрешения конфликтов для составных параметров может различаться. Есть 3 типа разрешения конфликтов для составных параметров:

Тип разрешения конфликта	Описание работы
С уникальными атрибутами	Составные параметры, у которых возможны конфликты. Для разрешения конфликтов для каждого параметра определен уникальный атрибут. В рамках одного ГПО нельзя создать массив списка атрибутов с одинаковыми значениями уникального параметра. Результат суммирования будет состоять из массива списка атрибутов с неповторяющимися значениями уникальных атрибутов в случайном порядке
Без уникальных атрибутов	Составные параметры, массивы списка атрибутов, которых суммируются без конфликтов
Комбинация уникальных атрибутов	Составные параметры, у которых массивы списка атрибутов считаются уникальными при комбинации атрибутов. С точки зрения работы механизма Групповых политик, эти составные атрибуты суммируются аналогично типу «Без уникальных атрибутов».Конфликты в этом случае разрешаются на стороне операционной системы

Поведение составных параметров компьютеров

В таблице ниже приведено описание работы каждого составного параметра компьютеров, в зависимости от его типа. Для корректного отображения в таблице название в БД указано без знака нижнего подчеркивания между элементами параметра.

	Параметр	Уникальный атрибут	Поведение при конфликте в случае суммирования и наследования
	С уникальными атрибутами		Нельзя создать в рамках одного ГПО массивы списка атрибутов одинаковыми значениями уникальных атрибутов
1	Безопасность → Глобальные настройки киоска → Автозапуск приложения в киоске	Путь до исполняемого файла. *Название в БД:* rbta ldap kiosk global parametrs app path	
2	Безопасность → Конфигурация параметра ядра	Имя конфигурационного файла. *Название в БД:* rbta ldap kernel parametrs params name	
3	Безопасность → Мандатные атрибуты → Категории	Наименование. *Название в БД:* rbta ldap mandate attrs categories name	
4	Безопасность → Мандатные атрибуты → Уровни конфиденциальности	Наименование. *Название в БД:* rbta ldap mandate attrs levels name``	

продолжение на следующей странице

Таблица 3.37 – продолжение с предыдущей страницы

	Параметр	Уникальный атрибут	Поведение при конфликте в случае суммирования и наследования
5	Безопасность → Мандатный целостности (**МКЦ**) → Исключения конфигурации защиты файловой системы	Путь к объекту. *Название в БД:* rbta ldap integrity control fs protection exceptions exception``	
6	Безопасность → Мандатный целостности (**МКЦ**) → Конфигурация защиты файловой системы	Путь к объекту. *Название в БД:* rbta ldap integrity control fs protection config path``	
7	Безопасность → **Политика** очистки памяти → Настройка гарантированного удаления файлов на устройстве	Адрес устройства или точка монтирования. *Название в БД:* rbta ldap memory clearing drives path``	
8	Безопасность → Управление квотами → Квота устройства	Адрес устройства или точка монтирования. *Название в БД:* rbta ldap quotas drives path	
9	Система → Вход в систему → Изображение пользователя	Логин пользователя. *Название в БД:* rbta ldap login user pics login``	
10	Система → Дата и время → Параметры сервера или пула сетевого времени	Адрес сервера или пула. *Название в БД:* rbta ldap date time h servers name``	
11	Система → Приложение для типа файлов	Перечень mime-типов. *Название в БД:* rbta ldap mimeapps h local mimes``	

продолжение на следующей странице

Таблица 3.37 – продолжение с предыдущей страницы

	Параметр	Уникальный атрибут	Поведение при конфликте в случае суммирования и наследования
12	Система → Системная альтернатива	Символическая ссылка. *Название в БД:* rbta ldap system alternatives alternatives name``	
13	Безопасность → Санкции PolicyKit-1 → Привилегированное действие	Название привилегированного действия. *Название в БД:* rbta ldap policykit actions explicit name``	
	Без уникального атрибута		Все массивы атрибутов суммируются и появляются в интерфейсе
14	Безопасность → Управление квотами → Расписание проверки квот	Нет уникального атрибута	
15	Оборудование → Редактор маркеров → Входная переменная	Нет уникального атрибута	
16	Оборудование → Редактор маркеров → Маркер	Нет уникального атрибута	
17	Система → Переменная окружения	Нет уникального атрибута	
18	Система → Планировщик задач → Планировщик задач пользователя cron	Нет уникального атрибута	
	Третья категория		

продолжение на следующей странице

Таблица 3.37 – продолжение с предыдущей страницы

	Параметр	Уникальный атрибут	Поведение при конфликте в случае суммирования и наследования
19	Безопасность → Управление квотами → Индивидуальная квота	Комбинация «Адрес устройства или точка монтирования» + «Имя группы пользователей или логин пользователя»	При полном совпадении атрибутов «Адрес устройства или точка монтирования» + «Имя группы пользователей или логин пользователя» квота создастся только одна, первая которая была применена
20	Оборудование → Установить принтер(ы)	Комбинация «Имя принтера» + «Имя сервера печати»	При полном совпадении атрибутов «Имя принтера» + «Имя сервера печати» принтер появится только один
21	Сеть → Настройка межсетевого экрана → Обычное правило	Комбинация «**Политика**» + «Направление» + «Протокол» + «Порт»	При полном совпадении атрибутов «**Политика**» + «Направление» + «Протокол» + «Порт» новые правила с такими же атрибутами не создаются
22	Сеть → Настройка межсетевого экрана → Предустановленное правило	Уникальна комбинация «**Политика**» + «Направление» + «Протокол» + «Порт», **ОС** сама решает конфликт в случае дублей принтеров.	При полном совпадении атрибутов «Наименование предустановленного приложения» + «**Политика**» + «Направление» новые правила с такими же атрибутами не создаются

продолжение на следующей странице

Таблица 3.37 – продолжение с предыдущей страницы

	Параметр	Уникальный атрибут	Поведение при конфликте в случае суммирования и наследования
23	Сеть → Настройка межсетевого экрана → Расширенное правило	Комбинация «**Политика**» + «Направление» + «Протокол» + «Порт»	При полном совпадении атрибутов «**Политика**» + «Направление» + «Протокол» + «Порт» новые правила с такими же атрибутами не создаются
24	Система → Планировщик задач → Переменная пользователя cron	Нет уникального атрибута, графика дает создавать одинаковые переменные пользователя cron	Все массивы атрибутов суммируются и появляются в интерфейсе. Дальнейшее применение зависит от операционной системы, в основном случае будет использована последняя добавленная переменная

Поведение составных параметров пользователей

В таблице ниже приведено описание работы каждого составного параметра компьютеров, в зависимости от его типа. Для корректного отображения в таблице название в БД указано без знака нижнего подчеркивания между элементами параметра.

	Параметр	Уникальный атрибут	Поведение при конфликте в случае суммирования и наследования
	1 категория		Нельзя создать в рамках одного ГПО массивы списка атрибутов одинаковыми значениями уникальных атрибутов
1	Оборудование → Значение для предпросмотра редактора маркеров	Название переменной. *Название в БД:* rbta ldap marker editor u preview values name	
2	Оборудование → Обработка «горячего» подключения	*Имя. Название в БД:* rbta ldap fly reflex actions name	
3	Рабочий стол → Параметры окон → Настройки программы или класса окон	Название программы или класса окон. *Название в БД:* rbta ldap windows settings presets name	
4	Система → Приложения для типов файлов → Приложение для типа файлов	Перечень mime-типов. *Название в БД:* rbta ldap mimeapps u local mimes	

продолжение на следующей странице

Таблица 3.38 – продолжение с предыдущей страницы

	Параметр	Уникальный атрибут	Поведение при конфликте в случае суммирования и наследования
5	Оборудование → Электропитание → Настройки уведомлений о событиях	Наименование уведомления. *Название в БД:* rbta ldap power management notifications execute	Нельзя создать в рамках одного ГПО массивы списка атрибутов одинаковыми значениями уникальных атрибутов. Итоговое количество настроенных уведомлений не более 6, потому что поле «Наименование уведомления» может содержать только одно из 6 значений: • pluggedin, • unplugged, • fullbattery, • lowbattery, • criticalbattery, • lowperipheral battery
	2 категория		Все массивы атрибутов суммируются и появляются в интерфейсе
6	Рабочий стол → Меню «Пуск» → Каталог	Нет уникального атрибута	

продолжение на следующей странице

Таблица 3.38 – продолжение с предыдущей страницы

	Параметр	Уникальный атрибут	Поведение при конфликте в случае суммирования и наследования
7	Рабочий стол → Меню «Пуск» → Приложение	Нет уникального атрибута	
8	Рабочий стол → Меню «Пуск» → Ссылка	Нет уникального атрибута	
9	Рабочий стол → Панель быстрого запуска → Каталог	Нет уникального атрибута	
10	Рабочий стол → Панель быстрого запуска → Приложение	Нет уникального атрибута	
11	Рабочий стол → Панель быстрого запуска → Приложение	Нет уникального атрибута	
12	Система → Автозапуск → Приложение	Нет уникального атрибута	
13	Система → Автозапуск → Ссылка	Нет уникального атрибута	
14	Система → Переменные окружения → Переменная окружения	Нет уникального атрибута	

Суммирование дополнительных параметров ГП

Суммирование дополнительных параметров ГП не отличается от коробочных. Для составных дополнительных параметров ГП можно настроить уникальный атрибут.

3.18.6. Просмотр смоделированного отчета о назначенных параметрах ГП

Для каждого компьютера и пользователя можно посмотреть моделирование результатов применения групповых политик (рисунок 7). (см. Пользователи и Компьютеры).

Для компьютера: **Пользователи и компьютеры → Компьютеры → {Имя компьютера} → Групповые политики**. Для пользователя: **Пользователи и компьютеры → Пользователи → {Логин пользователя} → Групповые политики**. Данный список представляет собой моделирование результатов применения групповых политик. Это значит, что не все параметры из данного списка могут быть применены к конкретному пользователю и не все политики могут быть отображены в данном списке. Чтобы групповая политика применилась к пользователю, необходимо соблюдать требования к операционной системе и заполнять значения атрибутов.

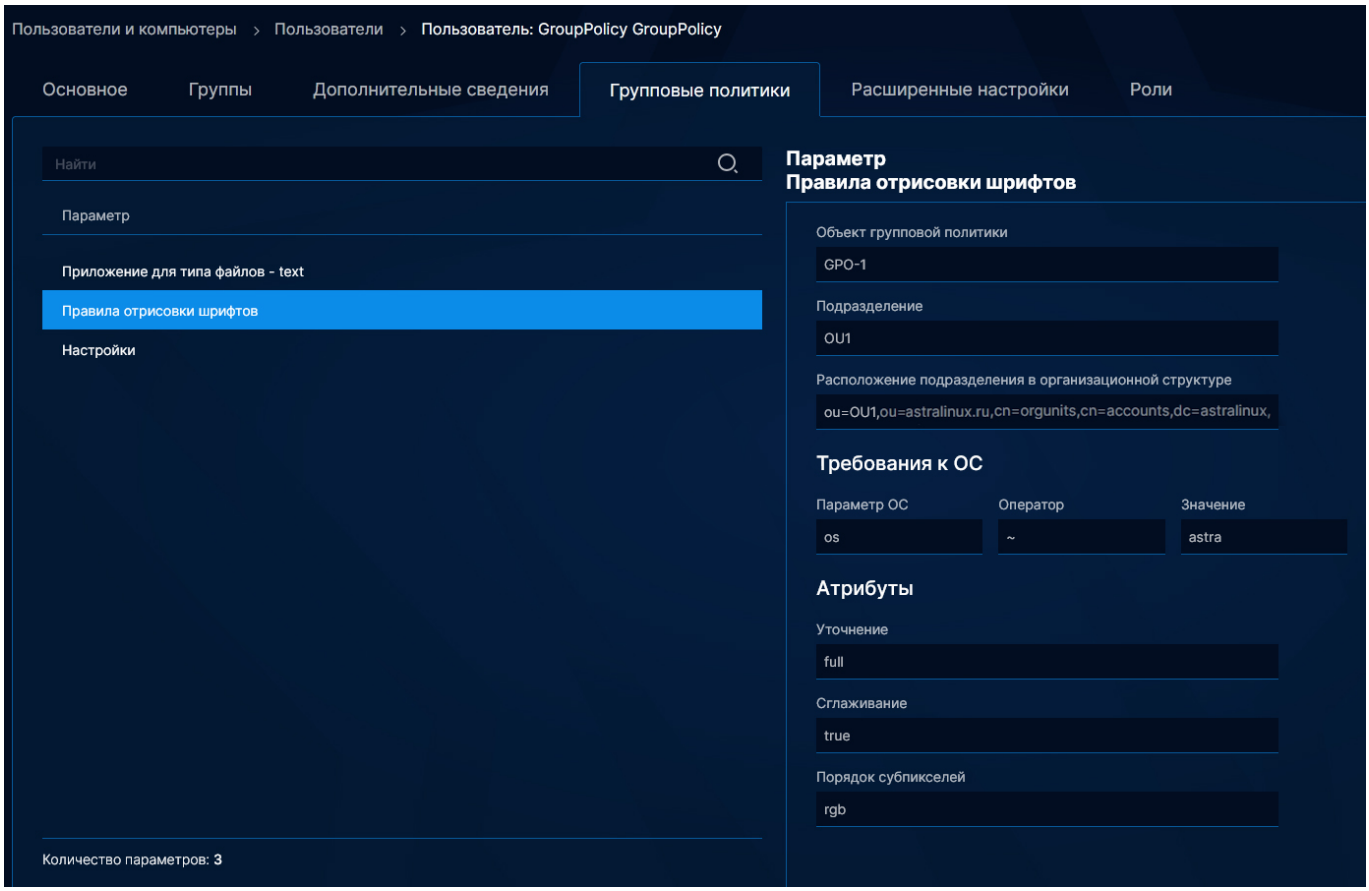


Рис. 7. Моделирование результата применения параметров ГП на пользователя

3.19. Синхронизация объектов, содержащих специальные символы

3.19.1. Введение

При синхронизации объектов из доменов Microsoft Active Directory в домен ALD Pro возникает ряд проблем: домены MS AD позволяют создавать объекты с любым типом символов (буквенные, цифровые, специальные и т.д.). Домен ALD Pro имеет ряд ограничений в валидации объектов и их атрибутов. Для устранения данной проблемы администратор домена имеет возможность заменить запрещенные символы с помощью редактирования файла конфигурации.

Замена символов производится в несколько этапов: пользовательские правила замены → базовые правила замены → транслитерация.

Базовые правила замены представляют собой файл конфигурации, поставляемый вместе с модулем синхронизации. Файл содержит базовый набор несинхронизируемых символов согласно требованиям домена.

Файл должен иметь имя `base_rule.yaml` и располагаться в директории `/opt/rbta/aldpro/syncer/services/utils/`

Важно: Файл с базовыми правилами нельзя редактировать. Здесь содержаться корректные правила замены. Внесение изменений в файл оказывает влияние на работу модуля синхронизации.

Пользовательские правила замены представляют собой файл конфигурации, позволяющий настраивать правила замены и расширять список символов. Не входит в конфигурацию модуля синхронизации.

Файл должен иметь имя `custom_rule.yaml` и располагаться в директории `/opt/rbta/aldpro/syncer/services/utils/`

Структура файла

```
version: 2.4.0

customrule:
type-user:
   uid:
   - rule:
            source:
            - "^"
            dest: "_"
type-group:
   cn:
   - rule:
            source:
            - "^"
            dest: "_"
type-ou:
   ou:
   - rule:
            source:
            - ",,"
            dest: "aa."
```

где

`version` - версия ALD Pro;

`customrule` - заголовок;

`type-user (type-group, type-ou)` - тип объекта синхронизации;

`uid (cn, ou)` - атрибуты объектов домена ALD Pro.

При создании пользовательских правил сопоставления следует учитывать:

Примечание:

1. Настройка пользовательских правил замены должна производиться перед добавлением сопоставлений подразделений. Замена, добавленная после создания сопоставления подразделения, будет обрабатываться только для новых, изменённых объектов или при пересоздании сопоставления подразделений.

2. Правила в файле конфигурации выполняются сверху вниз, слева направо (в случае, если несколько специальных символов заменяются одной комбинацией).

3. Правила замены запрещенных символов применяются едино ко всем символам, вне зависимости от порядкового номера символам в атрибуте.

4. Если для некоторых атрибутов требуется, чтобы первый символ был буквенно-цифровым, то правило замены обязательно должно это учитывать.

3.19.2. Описание базовых правил замены

3.19.2.1. Базовые правила замены для объекта «Пользователь»

Атрибуты, для которых реализованы правила замены:

Атрибут	Наименование
uid	Логин
sn	Фамилия
givenname	Имя
displayname	Отображаемое имя
title	Должность
street	Улица
l	Город
st	Область, край
c	Страна или регион

Атрибуты *Электронный адрес*, *Мобильный телефон* и *Почтовый индекс* исключены из правил замены.

uid

Локализация: Латиница, нижний регистр

Использование цифр: Разрешено, но не могут быть только цифры

Использование специальных символов: Разрешено, кроме первого символа. Можно использовать: `_` , `.` и `-`.

Использование пробелов, символа переноса строки, символа табуляции: Запрещено

Первый символ: буквенно-цифровой символ (буква или цифра)

Последний символ: Все разрешенные символы

Символ	Замена	Удвоенный символ
,	a.	aa.
;	b	bb.
:	c.	cc.
!	d.	dd.
?	e.	ee.
'	f.	ff.
“	h.	hh.
»	g.	gg.
«	h.	hh.
(	x.	xx.
)	i.	ii.
{	j.	jj.
}	k.	kk.
[	q.	qq.

продолжение на следующей странице

Таблица 3.40 – продолжение с предыдущей страницы

Символ	Замена	Удвоенный символ
]	l.	ll.
$	p.	pp.
#	n.	nn.
№	o.	oo.
%	r.	rr.
@	s.	ss.
&	t.	tt.
l	u.	uu.
\	v.	vv.
/	y.	yy.
“ ”	z.	zz.
t	a_	aa_
n	b_	bb_
^	c_	cc_
=	d_	dd_
+	e_	ee_
*	f_	ff_
<	h_	hh_
>	g_	gg_

SN, GIVENNAME

Локализация: Кириллица и латиница

Использование цифр: Разрешено

Использование специальных символов: _, -, . , $

Использование пробелов: Разрешено

Использование символа переноса строки, символа табуляции: Запрещено

Первый символ: Все разрешенные символы кроме пробела

Последний символ: Все разрешенные символы кроме пробела

Символ	Замена	Удвоенный символ
,	a.	aa.
;	b	bb.
:	c.	cc.
!	d.	dd.
?	e.	ee.
'	f.	ff.
“	h.	hh.
»	g.	gg.
«	h.	hh.
(	x.	xx.
)	i.	ii.
{	j.	jj.
}	k.	kk.
[	q.	qq.
]	l.	ll.
$	p.	pp.
#	n.	nn.

продолжение на следующей странице

Таблица 3.41 – продолжение с предыдущей страницы

Символ	Замена	Удвоенный символ
№	o.	oo.
%	r.	rr.
@	s.	ss.
&	t.	tt.
l	u.	uu.
\	v.	vv.
/	y.	yy.
“ ”	z.	zz.
t	a_	aa_
n	b_	bb_
^	c_	cc_
=	d_	dd_
+	e_	ee_
*	f_	ff_
<	h_	hh_
>	g_	gg_

DISPLAYNAME

Локализация: Кириллица и латиница

Использование цифр: Разрешено

Использование специальных символов: ASCII (коды от 32 до 126 включительно)

Использование пробелов: Разрешено

Использование символа переноса строки, символа табуляции: Запрещено

Первый символ: Все разрешенные символы кроме пробела

Последний символ: Все разрешенные символы кроме пробела

Символ	№	»	«	t	n	{	}	l
Замена	o.	g.	h.	a_	b_	j.	k.	u.
Удвоенный символ	oo.	gg.	hh.	aa_	bb_	jj.	kk.	uu.

TITLE, STREET, ST, L, C

Локализация: Кириллица и латиница

Использование цифр: Разрешено

Использование специальных символов: ASCII-символы (коды от 32 до 126 включительно)

Использование пробелов: Разрешено

Использование символа переноса строки, символа табуляции: Запрещено

Первый символ: Буквы и цифры

Последний символ: Все, кроме пробела

Символ	№	»	«	t	n	{	}	l
Замена	o.	g.	h.	a_	b_	j.	k.	u.
Удвоенный символ	oo.	gg.	hh.	aa_	bb_	jj.	kk.	uu.

3.19.2.2. Базовые правила замены для объекта «Группа пользователей»

Атрибуты, для которых реализованы правила замены:

Атрибут	Наименование
cn	Название
description	Описание

CN

Локализация: Латиница, нижний регистр.

Использование цифр: Разрешено, но не могут быть только цифры

Использование специальных символов: Разрешено, кроме первого символа. Можно использовать: `_` , `.` и `-`.

Использование пробелов, символа переноса строки, символа табуляции: Запрещено

Первый символ: буквенно-цифровой символ (буква или цифра)

Последний символ: Все разрешенные символы и „$“

Символ	Замена	Удвоенный символ
,	a.	aa.
;	b	bb.
:	c.	cc.
!	d.	dd.
?	e.	ee.
'	f.	ff.
“	h.	hh.
»	g.	gg.
«	h.	hh.
(	x.	xx.

продолжение на следующей странице

Таблица 3.45 – продолжение с предыдущей страницы

Символ	Замена	Удвоенный символ
)	i.	ii.
{	j.	jj.
}	k.	kk.
[	q.	qq.
]	l.	ll.
$	p.	pp.
#	n.	nn.
№	o.	oo.
%	r.	rr.
@	s.	ss.
&	t.	tt.
I	u.	uu.
\	v.	vv.
/	y.	yy.
“ ”	z.	zz.
t	a_	aa_
n	b_	bb_
^	c_	cc_
=	d_	dd_
+	e_	ee_
*	f_	ff_
<	h_	hh_

продолжение на следующей странице

Таблица 3.45 – продолжение с предыдущей страницы

Символ	Замена	Удвоенный символ
>	g_	gg_

DESCRIPTION

Локализация: Кириллица и латиница

Использование цифр: Разрешено

Использование специальных символов: ASCII-символы (коды от 32 до 126)

Использование пробелов, символа переноса строк: Разрешено, но не может быть первым и последним символом

Использование символа табуляции: Запрещено

Первый символ: Все разрешенные значения, кроме пробелов

Последний символ: Все разрешенные значения, кроме пробелов

Символ	№	»	«	t	n	{	}	l
Замена	o.	g.	h.	a_	b_	j.	k.	u.
Удвоенный символ	oo.	gg.	hh.	aa_	bb_	jj.	kk.	uu.

3.19.2.3. Базовые правила замены для объекта «Подразделение»

Атрибуты, для которых реализованы правила замены:

Атрибут	Наименование
ou	Название

ou

Локализация: Кириллица и латиница

Использование цифр: Разрешено

Использование специальных символов: -, _, ", « » .

Использование пробелов, символа переноса строки: Разрешено, но не может быть первым и последним символом.

Использование символа табуляции: Запрещено

Первый символ: Все разрешенные значения, кроме пробелов.

Последний символ: Все разрешенные значения, кроме пробелов.

Символ	Замена	Удвоенный символ
,	a.	aa.
;	b	bb.
:	c.	cc.
!	d.	dd.
?	e.	ee.
'	f.	ff.
“	h.	hh.
»	g.	gg.
«	h.	hh.
(	x.	xx.
)	i.	ii.

продолжение на следующей странице

Таблица 3.48 – продолжение с предыдущей страницы

Символ	Замена	Удвоенный символ
{	j.	jj.
}	k.	kk.
[	q.	qq.
]	l.	ll.
$	p.	pp.
#	n.	nn.
№	o.	oo.
%	r.	rr.
@	s.	ss.
&	t.	tt.
I	u.	uu.
\	v.	vv.
/	y.	yy.
“ ”	z.	zz.
t	a_	aa_
n	b_	bb_
^	c_	cc_
=	d_	dd_
+	e_	ee_
*	f_	ff_
<	h_	hh_
>	g_	gg_

3.20. Инструкция по настройке браузера для сквозной авторизации в Web-интерфейсе портала управления ALD Pro

3.20.1. Браузер Firefox

Если Firefox уже установлен на доменном компьютере или для его установки на доменном компьютере используется команда:

```
apt install
```

то сертификат ALD Pro подгружается автоматически.

Если для установки Firefox используется политика ПО, то в шаблоне политики ПО (**Установка и обновление ПО - Каталог ПО - карточка ПО - Шаблоны конфигурации**) необходимо явно прописать путь до сертификата ALD Pro `/etc/ipa/ca.crt`:

```
{
"policies":{
       "ImportEnterpriseRoots": true,
      "Certificates": {
         "Install": ["/etc/ipa/ca.crt"]
      }
```

Войти в веб-интерфейс портала управления ALDPro.

3.20.2. Браузер Chromium

Загрузить сертификат, находящийся по адресу `/ipa/config/ca.crt` или на клиенте домена ALDPro `/etc/ipa/ca.crt`

Войти в настройки браузера через меню или по адресу chrome://settings.

В разделе “Конфиденциальность и безопасность” развернуть подраздел “Безопасность” и выбрать “Настроить сертификаты”. Во вкладке “Центры сертификации” нажать кнопку “Импорт” и выбрать загруженный сертификат”. Убедиться в том, что выбраны все три чекбокса с вариантами применения сертификата.

Закрыть браузер.

Создать файл `/etc/chromium/policies/managed/mydomain.json` с содержимым:

```
{ "AuthServerWhitelist": "*.<Имя домена ALDPro>" }
```

Пример

```
{ "AuthServerWhitelist": "*.ald.pro" }
```

Примечание: В зависимости от версии браузера может быть использована опция с наименованием “AuthServerAllowlist”:

```
{ "AuthServerAllowlist": "*.<Имя домена ALDPro>" }
```

Пример

```
{ "AuthServerAllowlist": "*.ald.pro" }
```

3.21. Матрица и описание ролей

3.21.1. Описание ролей

3.21.1.1. ALDPRO - Domain Info Readers

Подробное описание возможностей роли

- Видеть общую информацию о домене
- Просматривать сервера
- Видеть список сайтов
- Видеть карточки сайтов
- Видеть список компьютеров
- Видеть карточки компьютера
- Видеть дерево подразделений

- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS

Привилегии в составе роли

- Domain Info - Read
- IPA Servers - Read
- Sites - Read
- Computers - Read
- Organization units - Read
- DNS Zones - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Общая информация
  - Сайты и службы
- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
- Роли и службы сайта:
  - Служба разрешения имён

Возможность ограничения области действия

В составе роли нет привилегий, область действия которых может быть ограничена.

3.21.1.2. ALDPRO - Domain Controllers and Sites Service Administrators

Подробное описание возможностей роли

- Видеть список контроллеров доменов
- Видеть карточки контроллеров доменов
- Видеть журнал изменений
- Удалять контроллеры домена на указанном сайте.
- Создавать новые контроллеры домена на указанном сайте.
- Видеть список сайтов домена
- Видеть карточки сайтов домена
- Создавать новые сайты
- Изменять сайты
- Назначать для сайтов контроллеры домена
- Удалять сайты
- Видеть список соглашений о репликациях
- Видеть карточки соглашений о репликациях
- Создавать новые соглашения о репликации
- Изменять соглашения о репликации
- Удалять соглашения о репликации
- Обновлять сервер контроллера домена на указанном сайте
- Видеть список компьютеров
- Видеть карточки компьютера
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS
- Управлять зонами DNS: добавлять, удалять, редактировать
- Просматривать сервера

Привилегии в составе роли

- Domain Controllers - Read
- Domain Controllers - Drop
- Domain Controllers - Create

- Site Parameters - Read
- Site Parameters - Add
- Site Parameters - Modify
- Site Domain Controllers - Add
- Site Parameters - Delete
- Replication Agreements - Read
- Replication Agreements - Add
- Replication Agreements - Modify
- Replication Agreements - Delete
- Domain Controllers - Modify
- Sites - Read
- Computers - Read
- Organization units - Read
- DNS Zones - Read
- IPA Servers - Read
- DNS Zones - Manage

Доступ к подразделам портала управления

- Управление доменом:
  - Общая информация
  - Сайты и службы
- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
- Роли и службы сайта:
  - Служба разрешения имён

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Удалять контроллеры домена на указанном сайте (Domain Controllers - Drop)
- Создавать новые контроллеры домена на указанном сайте (Domain Controllers - Create)
- Обновлять сервер контроллера домена на указанном сайте (Domain Controllers - Modify)

3.21.1.3. ALDPRO - Group Policies Additional Parameters Administrators

Подробное описание возможностей роли

- Видеть список параметров компьютеров
- Видеть список папок компьютеров
- Видеть карточки параметров компьютеров
- Видеть карточки папок параметров компьютеров
- Видеть список параметров пользователей
- Видеть карточки параметров пользователей
- Управлять папками параметров компьютеров: создавать, редактировать, удалять
- Управлять параметрами компьютеров: создавать, редактировать, удалять
- Управлять папками параметров пользователей: создавать, редактировать, удалять;
- Управлять параметрами пользователей: создавать, редактировать, удалять.

Привилегии в составе роли

- Computer Group Policy Additional Parameters - Read
- User Group Policy Additional Parameters - Read
- Computer Group Policy Additional Parameters - Manage
- User Group Policy Additional Parameters - Manage

Доступ к подразделам портала управления

- Управление доменом:
  - Доп. параметры групповых политик

Возможность ограничения области действия

В составе роли нет привилегий, область действия которых может быть ограничена.

3.21.1.4. ALDPRO - Automation Tasks Catalog Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список папок заданий автоматизации
- Видеть список заданий автоматизации
- Видеть карточки папок заданий автоматизации
- Видеть карточки заданий автоматизации
- Управлять атрибутами задания автоматизации: создавать, редактировать, удалять.
- Управлять конфигурацией скрипта задания автоматизации: редактировать.
- Управлять папками заданий автоматизации: создавать, редактировать, удалять.
- Управлять заданиями автоматизации: создавать, редактировать, удалять.

Привилегии в составе роли

- Automation Tasks - Read
- Automation Task Attributes - Manage
- Automation Task Script - Manage
- Automation Tasks Folders - Manage
- Automation Tasks - Manage

Доступ к подразделам портала управления

- Управление доменом:
  - Каталог заданий автоматизации

Возможность ограничения области действия

В составе роли нет привилегий, область действия которых может быть ограничена

3.21.1.5. ALDPRO - Kerberos Service Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список служб Kerberos
- Видеть карточки служб Kerberos
- Создавать новые службы Kerberos
- Изменять службы Kerberos
- Удалять службы Kerberos
- Управлять политикой билетов Kerberos: редактировать.
- Просматривать сервера
- Видеть список сайтов
- Видеть карточки сайтов
- Видеть список компьютеров
- Видеть карточки компьютера
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS

Привилегии в составе роли

- Kerberos Services - Read
- Kerberos Services - Add
- Kerberos Services - Modify
- Kerberos Services - Delete
- Kerberos Configurations - Manage
- IPA Servers - Read
- Sites - Read
- Computers - Read
- Organization units - Read
- DNS Zones - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Сайты и службы
  - Службы и параметры Kerberos
- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
- Роли и службы сайта:
  - Служба разрешения имён

Возможность ограничения области действия

В составе роли нет привилегий, область действия которых может быть ограничена.

3.21.1.6. ALDPRO - Users and Groups Settings Administrators

Подробное описание возможностей роли

Роль позволяет:

- Управлять параметрами пользователей: редактировать
- Управлять параметрами групп: добавлять, удалять
- Управлять диапазонами POSIX идентификаторов: создавать, удалять
- Управлять атрибутами пользователей: создавать, удалять
- Видеть список параметров пользователей
- Видеть список параметров групп
- Видеть список POSIX идентификаторов
- Видеть список атрибутов пользователей
- Видеть карточки атрибутов пользователей
- Видеть список дополнительных параметров пользователей
- Изменять дополнительные параметры пользователя
- Изменять пользователей (кроме выбора подразделения)
- Видеть список пользователей
- Видеть карточки пользователей
- Видеть дерево подразделений
- Видеть карточки подразделений

Привилегии в составе роли

- Users and Groups Settings - Manage
- Users and Groups Settings - Read
- Users - Modify
- Users - Read
- Organization units - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Пользователи и группы
- Пользователи и компьютеры:

- Организационная структура
- Пользователи

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Изменять пользователей (кроме выбора подразделения) (Users - Modify)

3.21.1.7. ALDPRO - Domain Integrations Administrators

Подробное описание возможностей роли

Участники роли получают набор привилегий для администрирования интеграции с доменами (при обязательном участии в группах trust admin и ald trust admins). Для выполнения корректной миграции необходимо дополнительно добавить привилегии Organization Units - Add, Organization Units - Delete, Organization Units - Modify, Organization Units - Read, User groups - Add, User groups - Delete, User groups - Modify, User groups - Read, Users - Modify, Users - Add, Users - Move to trash, Users - Delete from trash, Users - Read. Подразделение роли должно соответствовать подразделению, в рамках которого выполняется миграция.

Роль позволяет:

- Видеть список доверительных отношений
- Видеть список миграций с MS AD
- Управлять записями в LDAP связанными с доверительными отношениями и миграциями: создавать, редактировать, удалять
- Управлять миграциями с MS AD и доверительными отношениями: создавать, удалять
- Изменять перенаправления запросов
- Удалять перенаправления запросов
- Создавать новые перенаправления запросов
- Видеть список перенаправлений запросов
- Видеть карточки перенаправлений запросов

Привилегии в составе роли

- Domain Integrations - Manage
- DNS Forward Zones - Modify
- DNS Forward Zones - Delete
- DNS Forward Zones - Add
- DNS Forward Zones - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Интеграция с доменами
- Роли и службы сайта:
  - Служба разрешения имён

Возможность ограничения области действия

В составе роли нет привилегий, область действия которых может быть ограничена.

3.21.1.8. ALDPRO - Roles Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список ролей
- Видеть карточки ролей
- Видеть роли пользователя в карточке пользователя
- Видеть роли группы пользователей в карточке группы пользователей
- Создавать и копировать роли
- Изменять описание роли и ее состояние
- Управлять назначением ролей на пользователей и группы пользователей: добавлять, удалять

- Управлять назначением ролей на пользователей: добавлять, удалять
- Управлять назначением ролей на группы пользователей: добавлять, удалять.
- Удалять роли
- Добавлять привилегии в состав роли
- Изменять сайт для привилегий у которых есть ограничение по сайту
- Удалять привилегии из состава роли
- Видеть список групп пользователей
- Видеть карточки групп пользователей
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список пользователей
- Видеть карточки пользователей
- Видеть список сайтов
- Видеть карточки сайтов

Привилегии в составе роли

- Roles - Read
- Roles - Add
- Roles - Modify
- Roles Membership - Manage
- Roles - Delete
- Role Privileges - Add
- Role Privileges - Modify
- Role Privileges - Delete
- User groups - Read
- Organization units - Read
- Users - Read
- Sites - Read

Внимание: Важно использовать привилегию **Roles Membership - Manage** с осторожностью. Пользователь, на которого назначена роль, привязанная к корневому подразделению домена с установленным признаком **Включая дочерние подразделения**, в составе которой есть данная привилегия, получает возможность как назначать любые роли на любого пользователя, получая таким образом возможность назначить набор ролей, аналогичный роли **ALDPRO - Main Administrator**, так и снимать назначение уже назначенных ролей с любых пользователей домена, что приведет к лишению этих пользователей имеющихся у них привилегий.

Доступ к подразделам портала управления

- Управление доменом:
  - Сайты и службы
  - Роли и права доступа
- Пользователи и компьютеры:
  - Организационная структура
  - Пользователи
  - Группы пользователей

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Создавать и копировать роли (Roles - Add)
- Изменять описание роли и ее состояние (Roles - Modify)
- Управлять назначением ролей на пользователей и группы пользователей: добавлять, удалять (Roles Membership - Manage)
- Управлять назначением ролей на пользователей: добавлять, удалять (Roles Membership - Manage)
- Управлять назначением ролей на группы пользователей: добавлять, удалять (Roles Membership - Manage)
- Удалять роли (Roles - Delete)

- Добавлять привилегии в состав роли (Role Privileges - Add)
- Изменять сайт для привилегий у которых есть ограничение по сайту (Role Privileges - Modify)
- Удалять привилегии из состава роли (Role Privileges - Delete)

3.21.1.9. ALDPRO - Organizational Units Administrators

Подробное описание возможностей роли

Роль позволяет:

- Создавать новые подразделения
- Удалять подразделения
- Изменять параметры подразделений
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список групповых политик
- Видеть карточки групповых политик
- Видеть список групповых политик в карточке подразделения
- Видеть карточки групповых политик в карточке подразделения
- Видеть список групповых политик в карточке пользователя
- Видеть список групповых политик в карточке компьютера
- Управлять политиками для подразделений: добавлять, удалять
- Управлять политиками для подразделений: добавлять, удалять, изменять приоритет
- Видеть список политик ПО
- Видеть карточки политик ПО
- Видеть параметры ПО в подразделениях
- Видеть параметры ПО в карточке компьютера
- Управлять подразделениями в политиках ПО: добавлять, удалять
- Управлять параметрами ПО в подразделениях: добавлять, удалять, изменять приоритет параметра
- Управлять параметрами ПО в карточке компьютера: редактировать
- Видеть список пользователей

- Видеть карточки пользователей
- Видеть список параметров компьютеров
- Видеть список папок компьютеров
- Видеть карточки параметров компьютеров
- Видеть карточки папок параметров компьютеров
- Видеть список параметров пользователей
- Видеть карточки параметров пользователей
- Видеть список групп компьютеров
- Видеть карточки групп компьютеров
- Видеть список компьютеров
- Видеть карточки компьютера
- Видеть список зон DNS
- Видеть карточки зон DNS
- Видеть список программного обеспечения, пакетов и разделов (групп) ПО
- Видеть карточки разделов (групп) ПО
- Видеть карточки записей ПО

Привилегии в составе роли

- Organization units - Add
- Organization units - Delete
- Organization units - Modify
- Organization units - Read
- Group Policies - Read
- Group Policies Membership - Manage
- Software Policies - Read
- Software Policies Membership - Manage
- Users - Read
- Computer Group Policy Additional Parameters - Read
- User Group Policy Additional Parameters - Read
- Computer groups - Read

- Computers - Read
- DNS Zones - Read
- Software Catalog - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Доп. параметры групповых политик
- Пользователи и компьютеры:
  - Организационная структура
  - Пользователи
  - Компьютеры
  - Группы компьютеров
- Установка и обновление ПО:
  - Политики ПО
  - Каталог ПО
- Роли и службы сайта:
  - Служба разрешения имён

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Создавать новые подразделения (Organization units - Add)
- Удалять подразделения (Organization units - Delete)
- Изменять параметры подразделений (Organization units - Modify)

3.21.1.10. ALDPRO - Users Administrators

Подробное описание возможностей роли

Роль позволяет:

- Сбрасывать пароль для пользователя
- Блокировать и разблокировать пользователя
- Изменять пользователей (кроме выбора подразделения)
- Перемещать пользователей в корзину
- Видеть список пользователей в корзине
- Видеть карточки пользователей в корзине
- Управлять составом пользователей в подразделениях
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список пользователей
- Видеть карточки пользователей
- Создавать новых пользователей

Привилегии в составе роли

- Users Password - Modify
- Users Block - Modify
- Users - Modify
- Users - Move to trash
- Users - Read trash
- Users - Set organization unit
- Organization units - Read
- Users - Read
- Users - Add

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Организационная структура
  - Пользователи
  - Корзина

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Сбрасывать пароль для пользователя (Users Password - Modify)
- Блокировать и разблокировать пользователя (Users Block - Modify)
- Изменять пользователей (кроме выбора подразделения) (Users - Modify)
- Перемещать пользователей в корзину (Users - Move to trash)
- Управлять составом пользователей в подразделениях (Users - Set organization unit)
- Создавать новых пользователей (Users - Add)

3.21.1.11. ALDPRO - User Groups Administrators

Подробное описание возможностей роли

Роль позволяет:

- Создавать новые группы пользователей
- Удалять группы пользователей
- Изменять параметры групп пользователей (кроме выбора подразделения)
- Видеть список групп пользователей
- Видеть карточки групп пользователей
- Управлять составом пользователей в группе пользователей
- Управлять составом групп пользователей в группе пользователей
- Управлять составом групп пользователей в подразделениях
- Управлять составом групп пользователей в подразделениях
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список пользователей
- Видеть карточки пользователей

Привилегии в составе роли

- User groups - Add

- User groups - Delete
- User groups - Modify
- User groups - Read
- User groups - Set group membership
- User groups - Set organization unit
- Organization units - Read
- Users - Read

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Организационная структура
  - Пользователи
  - Группы пользователей

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Создавать новые группы пользователей (User groups - Add)
- Удалять группы пользователей (User groups - Delete)
- Изменять параметры групп пользователей (кроме выбора подразделения) (User groups - Modify)
- Управлять составом пользователей в группе пользователей (User groups - Set group membership)
- Управлять составом групп пользователей в группе пользователей (User groups - Set group membership)
- Управлять составом пользователей в подразделениях (User groups - Set organization unit)
- Управлять составом групп пользователей в подразделениях (User groups - Set organization unit)

3.21.1.12. ALDPRO - Computers Administrators

Подробное описание возможностей роли

Роль позволяет:

- Удалять компьютеры
- Изменять параметры компьютеров
- Видеть список компьютеров
- Видеть карточки компьютера
- Осуществлять удаленный доступ к компьютеру
- Управлять составом компьютеров в подразделениях
- Видеть список зон DNS
- Видеть карточки зон DNS
- Видеть дерево подразделений
- Видеть карточки подразделений

Привилегии в составе роли

- Computers - Delete
- Computers - Modify
- Computers - Read
- Computers - Remote access
- Computers - Set organization unit
- DNS Zones - Read
- Organization units - Read

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
- Роли и службы сайта:

– Служба разрешения имён

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Удалять компьютеры (Computers - Delete)
- Изменять параметры компьютеров (Computers - Modify)
- Осуществлять удаленный доступ к компьютеру (Computers - Remote access)
- Управлять составом компьютеров в подразделениях (Computers - Set organization unit)

3.21.1.13. ALDPRO - Computer Groups Administrators

Подробное описание возможностей роли

Роль позволяет:

- Создавать новые группы компьютеров
- Удалять группы компьютеров
- Изменять параметры группы компьютеров (кроме выбора подразделения)
- Видеть список групп компьютеров
- Видеть карточки групп компьютеров
- Управлять составом компьютеров в группе компьютеров
- Управлять составом групп компьютеров в группе компьютеров
- Управлять составом групп компьютеров в подразделениях
- Видеть список компьютеров
- Видеть карточки компьютера
- Видеть список зон DNS
- Видеть карточки зон DNS
- Видеть дерево подразделений
- Видеть карточки подразделений

Привилегии в составе роли

- Computer groups - Add
- Computer groups - Delete
- Computer groups - Modify
- Computer groups - Read
- Computer groups - Set group membership
- Computer groups - Set organization unit
- Computers - Read
- DNS Zones - Read
- Organization units - Read

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
  - Группы компьютеров
- Роли и службы сайта:
  - Служба разрешения имён

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Создавать новые группы компьютеров (Computer groups - Add)
- Удалять группы компьютеров (Computer groups - Delete)
- Изменять параметры группы компьютеров (кроме выбора подразделения) (Computer groups - Modify)
- Управлять составом компьютеров в группе компьютеров (Computer groups - Set group membership)
- Управлять составом групп компьютеров в группе компьютеров (Computer groups - Set

group membership)

- Управлять составом групп компьютеров в подразделениях (Computer groups - Set organization unit)

3.21.1.14. ALDPRO - Deleted User Accounts Administrators

Подробное описание возможностей роли

Роль позволяет:

- Восстанавливать пользователей из корзины
- Окончательно удалять пользователей из корзины
- Видеть список пользователей в корзине
- Видеть карточки пользователей в корзине
- Создавать новых пользователей
- Изменять параметры групп пользователей (кроме выбора подразделения)
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список групп пользователей
- Видеть карточки групп пользователей
- Видеть список пользователей
- Видеть карточки пользователей

Привилегии в составе роли

- Users - Return from trash
- Users - Delete from trash
- Users - Read trash
- Users - Add
- User groups - Modify
- Organization units - Read
- User groups - Read
- Users - Read

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Организационная структура
  - Пользователи
  - Группы пользователей
  - Корзина

Возможность ограничения области действия

Для корректной работы роль должна распространяться на корневое подразделение, т.к. пользователей из корзины можно восстановить только в корневое подразделение (Users - Return from trash)

3.21.1.15. ALDPRO - Group Policies Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список групповых политик
- Видеть карточки групповых политик
- Видеть список групповых политик в карточке подразделения
- Видеть карточки групповых политик в карточке подразделения
- Создавать новые групповые политики
- Изменять групповые политики
- Удалять групповые политики
- Управлять значениями параметров компьютеров: редактировать, удалять
- Управлять конфигурациями с типом «Компьютеры»
- Управлять значениями параметров пользователей: редактировать, удалять
- Управлять конфигурациями с типом «Пользователи»
- Управлять политиками для подразделений: добавлять, удалять, изменять приоритет
- Видеть список параметров дополнительных параметров компьютеров

- Видеть список папок каталога дополнительных параметров компьютеров
- Видеть карточки дополнительных параметров компьютеров
- Видеть карточки папок каталога дополнительных параметров компьютеров
- Видеть список дополнительных параметров пользователей
- Видеть карточки дополнительных параметров пользователей
- Видеть дерево подразделений
- Видеть карточки подразделений

Привилегии в составе роли

- Group Policies - Read
- Group Policies - Add
- Group Policies - Modify
- Group Policies - Delete
- Group Policies Computer Parameters - Manage
- Group Policies User Parameters - Manage
- Group Policies Membership - Manage
- Computer Group Policy Additional Parameters - Read
- User Group Policy Additional Parameters - Read
- Organization units - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Доп. параметры групповых политик
- Пользователи и компьютеры:
  - Организационная структура
- Групповые политики:
  - Групповые политики

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Управлять политиками для подразделений: добавлять, удалять, изменять приоритет (Group Policies Membership - Manage)

3.21.1.16. ALDPRO - HBAC Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список правил HBAC
- Видеть список служб HBAC
- Видеть список групп служб HBAC
- Видеть карточки правил HBAC
- Видеть карточки служб HBAC
- Видеть карточки групп служб HBAC
- Создавать новые правила HBAC
- Изменять правила HBAC
- Удалять правила HBAC
- Создавать новые службы HBAC
- Изменять службы HBAC
- Удалять службы HBAC
- Создавать новые группы служб HBAC
- Изменять группы служб HBAC
- Удалять группы служб HBAC
- Видеть список пользователей
- Видеть карточки пользователей
- Видеть список групп компьютеров
- Видеть карточки групп компьютеров
- Видеть список групп пользователей
- Видеть карточки групп пользователей

- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть список зон DNS
- Видеть карточки зон DNS

Привилегии в составе роли

- HBAC - Read
- HBAC Rules - Add
- HBAC Rules - Modify
- HBAC Rules - Delete
- HBAC Services - Add
- HBAC Services - Modify
- HBAC Services - Delete
- HBAC Service Groups - Add
- HBAC Service Groups - Modify
- HBAC Service Groups - Delete
- Users - Read
- Computer Groups - Read
- User groups - Read
- Organization units - Read
- Computers - Read
- DNS Zones - Read

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Организационная структура
  - Пользователи

  - Группы пользователей
  - Компьютеры
  - Группы компьютеров
- Групповые политики:
  - Политики доступа к узлу
- Роли и службы сайта:
  - Служба разрешения имён

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Изменять правила HBAC (HBAC Rules - Modify)

3.21.1.17. ALDPRO - SUDO Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список правил SUDO
- Видеть список команд SUDO
- Видеть список групп команд SUDO
- Видеть карточки правил SUDO
- Видеть карточки команд SUDO
- Видеть карточки групп команд SUDO
- Создавать новые правила SUDO
- Изменять правила SUDO, кроме вкладки Параметры
- Управлять параметрами SUDO для правил SUDO: создавать, удалять.
- Удалять правила SUDO
- Создавать новые команды SUDO
- Изменять команды SUDO
- Удалять команды SUDO

- Создавать новые группы команд SUDO
- Изменять группы команд SUDO
- Удалять группы команд SUDO
- Видеть список пользователей
- Видеть карточки пользователей
- Видеть список групп компьютеров
- Видеть карточки групп компьютеров
- Видеть список групп пользователей
- Видеть карточки групп пользователей
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть список зон DNS
- Видеть карточки зон DNS

Привилегии в составе роли

- SUDO - Read
- SUDO Rules - Add
- SUDO Rules - Modify
- SUDO Parameters - Manage
- SUDO Rules - Delete
- SUDO Commands - Add
- SUDO Commands - Modify
- SUDO Commands - Delete
- SUDO Command Groups - Add
- SUDO Command Groups - Modify
- SUDO Command Groups - Delete
- Users - Read
- Computer groups - Read

- User groups - Read
- Organization units - Read
- Computers - Read
- DNS Zones - Read

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Организационная структура
  - Пользователи
  - Группы пользователей
  - Компьютеры
  - Группы компьютеров
- Групповые политики:
  - Политики повышения привилегий
- Роли и службы сайта:
  - Служба разрешения имён

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Изменять правила SUDO, кроме вкладки Параметры (SUDO Rules - Modify)

3.21.1.18. ALDPRO - Password Policies Administrators

Подробное описание возможностей роли

Роль позволяет:

- Создавать новые политики паролей
- Изменять политики паролей
- Удалять политики паролей

- Видеть список групп пользователей
- Видеть карточки групп пользователей
- Видеть список политик паролей
- Видеть карточки политик паролей
- Видеть дерево подразделений
- Видеть карточки подразделений

Привилегии в составе роли

- Password Policies - Add
- Password Policies - Modify
- Password Policies - Delete
- User groups - Read
- Password Policies - Read
- Organization units - Read

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Организационная структура
  - Группы пользователей
- Групповые политики:
  - Политики паролей

Возможность ограничения области действия

В составе роли нет привилегий, область действия которых может быть ограничена

3.21.1.19. ALDPRO - Software Policies Administrators

Подробное описание возможностей роли

Роль позволяет:

- Создавать новые политики ПО
- Изменять политики ПО
- Удалять политики ПО
- Удалять ПО из политики ПО
- Удалять подразделения из политики ПО
- Добавлять ПО в политику ПО
- Удалять ПО из политики ПО
- Управлять подразделениями из политиках ПО: добавлять, удалять;
- Управлять параметрами ПО в подразделениях: добавлять, удалять, изменять приоритет параметра;
- Управлять параметрами ПО в карточке компьютера: редактировать.
- Видеть список программного обеспечения, пакетов и разделов (групп) ПО
- Видеть карточки разделов (групп) ПО
- Видеть карточки записей ПО
- Видеть список групп компьютеров
- Видеть карточки групп компьютеров
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS

Привилегии в составе роли

- Software Policies - Add
- Software Policies - Modify
- Software Policies - Delete
- Software Policies Configurations - Manage
- Software Policies Membership - Manage
- Software Catalog - Read
- Computer groups - Read

- Software Policies - Read
- Computers - Read
- Organization units - Read
- DNS Zones - Read

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
  - Группы компьютеров
- Установка и обновление ПО:
  - Политики ПО
  - Каталог ПО
- Роли и службы сайта:
  - Служба разрешения имён

Возможность ограничения области действия

В составе роли нет привилегий, область действия которых может быть ограничена

3.21.1.20. ALDPRO - Software Catalog Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список программного обеспечения, пакетов и разделов (групп) ПО
- Видеть карточки разделов (групп) ПО
- Видеть карточки записей ПО
- Управлять пакетами ПО: просматривать, создавать, удалять
- Управлять шаблонами конфигурации ПО: просматривать, создавать, редактировать,

удалять

- Управлять параметрами ПО: просматривать, создавать, редактировать, удалять
- Управлять разделами (группами) ПО: создавать, редактировать, удалять.
- Управлять ПО: создавать, редактировать, удалять
- Просматривать сервера
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS
- Видеть список репозиториев ПО
- Видеть карточки репозиториев ПО
- Видеть список серверов репозиториев ПО
- Видеть карточки серверов репозиториев ПО
- Видеть журнал изменений
- Видеть список сайтов
- Видеть карточки сайтов

Привилегии в составе роли

- Software Catalog - Read
- Software Packages - Manage
- Software Templates - Manage
- Software Parameters - Manage
- Software Groups - Manage
- Software - Manage
- IPA Servers - Read
- Computers - Read
- Organization units - Read
- DNS Zones - Read

- Repositories - Read
- Repository Servers - Read
- Sites - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Сайты и службы
- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
- Установка и обновление ПО:
  - Каталог ПО
  - Репозитории ПО
- Роли и службы сайта:
  - Служба разрешения имён

Возможность ограничения области действия

В составе роли нет привилегий, область действия которых может быть ограничена

3.21.1.21. ALDPRO - Software Repositories Administrators

Подробное описание возможностей роли

Роль позволяет:

- Создавать новые репозитории ПО
- Видеть список репозиториев ПО
- Видеть карточки репозиториев ПО
- Изменять параметры репозитория ПО
- Управлять версиями репозитория: просматривать, добавлять, удалять,

редактировать

- Удалять репозитории ПО
- Создавать новые серверы репозиториев ПО на указанном сайте
- Видеть список серверов репозиториев ПО
- Видеть карточки серверов репозиториев ПО
- Видеть журнал изменений
- Изменять сайт основного сервера репозиториев ПО. Привилегия должна быть назначена на оба сайта (из которого переносим и в который переносим)
- Обновлять серверы репозиториев ПО на указанном сайте
- Удалять серверы репозиториев ПО на указанном сайте
- Просматривать сервера
- Видеть список сайтов
- Видеть карточки сайтов
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS

Привилегии в составе роли

- Repositories - Add
- Repositories - Read
- Repositories - Modify
- Repository Versions - Manage
- Repositories - Delete
- Repository Servers - Create
- Repository Servers - Read
- Repository Servers - Modify
- Repository Servers - Drop

- IPA Servers - Read
- Sites - Read
- Computers - Read
- Organization units - Read
- DNS Zones - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Сайты и службы
- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
- Установка и обновление ПО:
  - Каталог ПО
  - Репозитории ПО
- Роли и службы сайта:
  - Служба разрешения имён

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Создавать новые серверы репозитория ПО на указанном сайте (Repository Servers - Create)
- Изменять сайт основного сервера репозитория ПО. Привилегия должна быть назначена на оба сайта (из которого переносим и в который переносим) (Repository Servers - Modify)
- Обновлять серверы репозитория ПО на указанном сайте (Repository Servers - Modify)
- Удалять серверы репозитория ПО на указанном сайте (Repository Servers - Drop)

3.21.1.22. ALDPRO - Software Update Policies Administrators

Подробное описание возможностей роли

Роль позволяет:

- Создавать новые политики обновления ALD Pro
- Редактировать политики обновления ALD Pro
- Удалять политики обновления ALD Pro
- Управлять конфигурацией Sources list в политике обновления ALD Pro: редактировать
- Управлять составом компьютеров и групп компьютеров в политиках обновления ALD Pro: добавлять, удалять
- Видеть список групп компьютеров
- Видеть карточки групп компьютеров
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS
- Видеть список политик обновления ALD Pro
- Видеть карточки политик обновления ALD Pro
- Видеть список политик обновления ALD Pro в карточке группы компьютеров
- Видеть список политик обновления ALD Pro в карточке компьютера

Привилегии в составе роли

- Update Policies - Add
- Update Policies - Modify
- Update Policies - Delete
- Update Policies Sources list - Manage
- Update Policies Computers - Manage
- Computer groups - Read

- Computers - Read
- Organization units - Read
- DNS Zones - Read
- Update Policies - Read

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
  - Группы компьютеров
- Установка и обновление ПО:
  - Политики обновления ALD Pro
- Роли и службы сайта:
  - Служба разрешения имён

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Управлять составом компьютеров и групп компьютеров в политиках обновления ALD Pro: добавлять, удалять (Update Policies Computers - Manage)

3.21.1.23. ALDPRO - Automation Tasks Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список заданий автоматизации в журнале заданий
- Видеть карточки заданий автоматизации в журнале заданий
- Запускать задания автоматизации
- Видеть список пользователей

- Видеть карточки пользователей
- Управлять атрибутами задания автоматизации: создавать, редактировать, удалять
- Видеть список групп компьютеров
- Видеть карточки групп компьютеров
- Управлять конфигурацией скрипта задания автоматизации: редактировать
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список папок заданий автоматизации
- Видеть список заданий автоматизации
- Видеть карточки папок заданий автоматизации
- Видеть карточки заданий автоматизации
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть список зон DNS
- Видеть карточки зон DNS

Привилегии в составе роли

- Automation Tasks Journal - Read
- Automation Tasks Membership - Manage
- Users - Read
- Automation Task Attributes - Manage
- Computer groups - Read
- Automation Task Script - Manage
- Organization units - Read
- Automation Tasks - Read
- Computers - Read
- DNS Zones - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Каталог заданий автоматизации
- Пользователи и компьютеры:
  - Организационная структура
  - Пользователи
  - Компьютеры
  - Группы компьютеров
- Автоматизация:
  - Задания автоматизации
- Роли и службы сайта:
  - Служба разрешения имён

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Запускать задания автоматизации (Automation Tasks Membership - Manage)

3.21.1.24. ALDPRO - Install OS Service Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список серверов установки ОС по сети
- Видеть карточки серверов установки ОС по сети
- Видеть перечень компьютеров
- Видеть карточки компьютеров
- Видеть список профилей загрузки
- Видеть карточки профилей загрузки

- Создавать новые серверы установки ОС по сетина указанном сайте
- Изменять параметры серверов установки ОС по сети на указанном сайте
- Обновлять сервер установки ОС по сети на указанном сайте
- Удалять серверы установки ОС по сети на указанном сайте
- Управлять компьютерами для сервера установки ОС по сети: добавлять, удалять
- Управлять профилями загрузки для сервера установки ОС по сети: добавлять, редактировать, удалять
- Просматривать сервера
- Видеть список сайтов
- Видеть карточки сайтов
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS
- Видеть список серверов динамической настройки узла
- Видеть карточки серверов динамической настройки узла
- Видеть журнал изменений
- Видеть общую информацию о домене
- Удалять компьютеры

Привилегии в составе роли

- Installation Servers - Read
- Installation Servers - Create
- Installation Servers - Modify
- Installation Servers - Drop
- Installation Server Computers - Manage
- Installation Server Profiles - Manage
- IPA Servers - Read

- Sites - Read
- Computers - Read
- Organization units - Read
- DNS Zones - Read
- DHCP - Read
- Domain Info - Read
- Computers - Delete

Доступ к подразделам портала управления

- Управление доменом:
  - Общая информация
  - Сайты и службы
- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
- Автоматизация:
  - Установка ОС по сети
- Роли и службы сайта:
  - Служба разрешения имён
  - Служба динамической настройки узла

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Создавать новые серверы установки ОС по сети на указанном сайте (Installation Servers - Create)
- Изменять параметры серверов установки ОС по сети на указанном сайте (Installation Servers - Modify)
- Обновлять сервер установки ОС по сети на указанном сайте (Installation Servers -

Modify)

- Удалять серверы установки ОС по сети на указанном сайте (Installation Servers - Drop)
- Управлять компьютерами для сервера установки ОС по сети: добавлять, удалять (Installation Server Computers - Manage)
- Управлять профилями загрузки для сервера установки ОС по сети: добавлять, редактировать, удалять (Installation Server Profiles - Manage)
- Удалять компьютеры (Computers - Delete)

3.21.1.25. ALDPRO - DNS Service Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список зон DNS
- Видеть карточки зон DNS
- Видеть список перенаправлений запросов
- Видеть карточки перенаправлений запросов
- Изменять перенаправления запросов
- Удалять перенаправления запросов
- Создавать новые перенаправления запросов
- Управлять глобальными конфигурациями DNS: просматривать, добавлять, удалять, редактировать

Привилегии в составе роли

- DNS Zones - Read
- DNS Zones - Manage
- DNS Forward Zones - Read
- DNS Forward Zones - Modify
- DNS Forward Zones - Delete
- DNS Forward Zones - Add
- DNS Global Configurations - Manage

Доступ к подразделам портала управления

- Роли и службы сайта:
  - Служба разрешения имён

Возможность ограничения области действия

В составе роли нет привилегий, область действия которых может быть ограничена.

3.21.1.26. ALDPRO - DHCP Service Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список серверов динамической настройки узла
- Видеть карточки серверов динамической настройки узла
- Видеть журнал изменений
- Создавать новые серверы динамической настройки узла на указанном сайте
- Изменять параметры серверов динамической настройки узла на указанном сайте
- Обновлять серверы динамической настройки узла на указанном сайте
- Удалять серверы динамической настройки узла на указанном сайте
- Видеть список сайтов
- Видеть карточки сайтов
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS
- Просматривать сервера

Привилегии в составе роли

- DHCP - Read
- DHCP Servers - Create
- DHCP Servers - Modify
- DHCP Configuration - Modify
- DHCP Servers - Drop
- Sites - Read
- Computers - Read
- Organization units - Read
- DNS Zones - Read
- IPA Servers - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Сайты и службы
- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
- Роли и службы сайта:
  - Служба разрешения имён
  - Служба динамической настройки узла

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Создавать новые серверы динамической настройки узла на указанном сайте (DHCP Servers - Create)
- Изменять параметры серверов динамической настройки узла на указанном сайте (DHCP Servers - Modify)

- Обновлять серверы динамической настройки узла на указанном сайте (DHCP Servers - Modify)
- Удалять серверы динамической настройки узла на указанном сайте (DHCP Servers - Drop)

3.21.1.27. ALDPRO - NTP Service Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список внешних NTP серверов
- Видеть список корневых NTP-серверов домена
- Добавлять новые внешние NTP-серверы
- Создавать новые корневые NTP-серверы
- Удалять внешние NTP-серверы
- Удалять корневые NTP-серверы
- Видеть список контроллеров доменов
- Видеть карточки контроллеров доменов
- Видеть журнал изменений
- Просматривать сервера
- Видеть карточки сайтов
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS

Привилегии в составе роли

- NTP Servers - Read
- External NTP Servers - Create

- Root NTP Servers - Create
- External NTP Servers - Drop
- Root NTP Servers - Drop
- Domain Controllers - Read
- IPA Servers - Read
- Sites - Read
- Computers - Read
- Organization units - Read
- DNS Zones - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Сайты и службы
- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
- Роли и службы сайта:
  - Служба разрешения имён
  - Служба синхронизации времени

Возможность ограничения области действия

В составе роли нет привилегий, область действия которых может быть ограничена.

3.21.1.28. ALDPRO - Print Service Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список серверов печати

- Видеть карточки серверов печати
- Видеть журнал изменений
- Создавать новые серверы печати
- Изменять параметры серверов печати на указанном сайте
- Обновлять серверы печати на указанном сайте
- Удалять серверы печати
- Управлять принтерами серверов печати: добавлять, удалять, редактировать, снимать задания печати на указанном сайте
- Просматривать сервера
- Видеть карточки сайтов
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS

Привилегии в составе роли

- Print Servers - Read
- Print Servers - Create
- Print Servers - Modify
- Print Servers - Drop
- Printers - Manage
- IPA Servers - Read
- Sites - Read
- Computers - Read
- Organization units - Read
- DNS Zones - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Сайты и службы
- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
- Роли и службы сайта:
  - Служба разрешения имён
  - Служба печати

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Создавать новые серверы печати (Print Servers - Create)
- Изменять параметры серверов печати на указанном сайте (Print Servers - Modify)
- Обновлять серверы печати на указанном сайте (Print Servers - Modify)
- Удалять серверы печати (Print Servers - Drop)
- Управлять принтерами серверов печати: добавлять, удалять, редактировать, снимать задания печати на указанном сайте (Printers - Manage)

3.21.1.29. ALDPRO - File Servers Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список серверов общего доступа к файлам
- Видеть карточки серверов общего доступа к файлам
- Видеть список папок с общим доступом
- Видеть карточки папок с общим доступом
- Видеть журнал изменений

- Создавать новые серверы общего доступа к файлам на указанном сайте
- Изменять параметры серверов общего доступа к файлам на указанном сайте
- Обновлять серверы общего доступа к файлам на указанном сайте
- Управлять папками с общим доступом: просматривать, добавлять, удалять, редактировать, настраивать доступ пользователям/компьютерам на указанном сайте
- Удалять серверы общего доступа к файлам на указанном сайте
- Просматривать сервера
- Видеть карточки сайтов
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS
- Видеть список пользователей
- Видеть карточки пользователей
- Видеть список групп пользователей
- Видеть карточки групп пользователей

Привилегии в составе роли

- File Servers - Read
- File Servers - Create
- File Servers - Modify
- File Server Folders - Manage
- File Servers - Drop
- IPA Servers - Read
- Sites - Read
- Computers - Read
- Organization units - Read
- DNS Zones - Read

- Users - Read
- User groups - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Сайты и службы
- Пользователи и компьютеры:
  - Организационная структура
  - Пользователи
  - Группы пользователей
  - Компьютеры
- Роли и службы сайта:
  - Служба разрешения имён
  - Общий доступ к файлам

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Создавать новые серверы общего доступа к файлам на указанном сайте (File Servers - Create)
- Изменять параметры серверов общего доступа к файлам на указанном сайте (File Servers - Modify)
- Обновлять серверы общего доступа к файлам на указанном сайте (File Servers - Modify)
- Управлять папками с общим доступом: просматривать, добавлять, удалять, редактировать, настраивать доступ пользователям/компьютерам на указанном сайте (File Server Folders - Manage)
- Удалять серверы общего доступа к файлам на указанном сайте (File Servers - Drop)

3.21.1.30. ALDPRO - Global Catalog Service Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список контроллеров домена с ролью глобального каталога
- Создавать новые серверы с ролью глобального каталога на указанном сайте
- Добавить роль глобального каталога при создании контроллера домена при помощи признака «Назначить роль глобального каталога» на указанном сайте
- Удалять новые серверы с ролью глобального каталога на указанном сайте
- Видеть список контроллеров доменов
- Видеть карточки контроллеров доменов
- Видеть журнал изменений
- Просматривать сервера
- Видеть карточки сайтов
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS

Привилегии в составе роли

- Global Catalog - Read
- Global Catalog - Add
- Global Catalog - Delete
- Domain Controllers - Read
- IPA Servers - Read
- Sites - Read
- Computers - Read
- Organization units - Read

- DNS Zones - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Сайты и службы
- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
- Роли и службы сайта:
  - Служба разрешения имён
  - Служба глобального каталога

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Создавать новые серверы с ролью глобального каталога на указанном сайте (Global Catalog - Add)
- Добавить роль глобального каталога при создании контроллера домена при помощи признака «Назначить роль глобального каталога» на указанном сайте (Global Catalog - Add)
- Удалять новые серверы с ролью глобального каталога на указанном сайте (Global Catalog - Delete)

3.21.1.31. ALDPRO - Monitoring Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список событий журнала мониторинга событий
- Видеть список серверов мониторинга

- Видеть карточки серверов мониторинга
- Видеть журнал изменений
- Создавать новые серверы мониторинга на указанном сайте
- Изменять параметры серверов мониторинга на указанном сайте
- Обновлять сервер мониторинга на указанном сайте
- Удалять серверы мониторинга на указанном сайте
- Просматривать сервера
- Видеть карточки сайтов
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS
- Видеть витрины мониторинга

Привилегии в составе роли

- Monitoring Event Logs - Read
- Monitoring Servers - Read
- Monitoring Servers - Create
- Monitoring Servers - Modify
- Monitoring Servers - Drop
- IPA Servers - Read
- Sites - Read
- Computers - Read
- Organization units - Read
- DNS Zones - Read
- Dashboards - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Сайты и службы
- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
- Роли и службы сайта:
  - Служба разрешения имён
- Мониторинг:
  - Журнал событий мониторинга
  - Витрины мониторинга домена

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Создавать новые серверы мониторинга на указанном сайте (Monitoring Servers - Create)
- Изменять параметры серверов мониторинга на указанном сайте (Monitoring Servers - Modify)
- Обновлять сервер мониторинга на указанном сайте (Monitoring Servers - Modify)
- Удалять серверы мониторинга на указанном сайте (Monitoring Servers - Drop)

3.21.1.32. ALDPRO - Monitoring Dashboards Readers

Подробное описание возможностей роли

Роль позволяет:

- Видеть витрины мониторинга
- Видеть список серверов мониторинга
- Видеть карточки серверов мониторинга

- Видеть журнал изменений
- Просматривать сервера
- Видеть карточки сайтов
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS

Привилегии в составе роли

- Dashboards - Read
- Monitoring Servers - Read
- IPA Servers - Read
- Sites - Read
- Computers - Read
- Organization units - Read
- DNS Zones - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Сайты и службы
- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
- Роли и службы сайта:
  - Служба разрешения имён
- Мониторинг:

- Журнал событий мониторинга
- Витрины мониторинга домена

Возможность ограничения области действия

В составе роли нет привилегий, область действия которых может быть ограничена

3.21.1.33. ALDPRO - Event Log Servers Administrators

Подробное описание возможностей роли

Роль позволяет:

- Создавать новые серверы журнала событий на указанном сайте
- Удалять серверы журнала событий на указанном сайте
- Изменять параметры серверов журнала событий на указанном сайте
- Обновлять серверы журнала событий на указанном сайте
- Видеть список серверов журнала событий
- Видеть карточки серверов журнала событий
- Видеть журнал изменений
- Просматривать сервера
- Видеть карточки сайтов
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS

Привилегии в составе роли

- Event Log Servers - Create
- Event Log Servers - Drop

- Event Log Servers - Modify
- Event Log Servers - Read
- IPA Servers - Read
- Sites - Read
- Computers - Read
- Organization units - Read
- DNS Zones - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Сайты и службы
- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
- Роли и службы сайта:
  - Служба разрешения имён
- Журнал событий:
  - Сервера журнала событий

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Создавать новые серверы журнала событий на указанном сайте (Event Log Servers - Create)
- Удалять серверы журнала событий на указанном сайте (Event Log Servers - Drop)
- Изменять параметры серверов журнала событий на указанном сайте (Event Log Servers - Modify)
- Обновлять серверы журнала событий на указанном сайте (Event Log Servers - Modify)

3.21.1.34. ALDPRO - Event Log Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список правил сбора событий
- Видеть карточки правил сбора событий
- Создавать новые правила сбора событий на сервере, расположенном на указанном сайте
- Изменять параметры правил сбора событий на сервере, на указанном сайте
- Удалять правила сбора событий на сервере, расположенном на указанном сайте
- Просматривать сервера
- Видеть карточки сайтов
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS
- Видеть список серверов журнала событий
- Видеть карточки серверов журнала событий
- Видеть журнал изменений

Привилегии в составе роли

- Event Registration Rules - Read
- Event Registration Rules - Add
- Event Registration Rules - Modify
- Event Registration Rules - Delete
- IPA Servers - Read
- Sites - Read
- Computers - Read

- Organization units - Read
- DNS Zones - Read
- Event Log Servers - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Сайты и службы
- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
- Роли и службы сайта:
  - Служба разрешения имён
- Журнал событий:
  - Сервера журнала событий
  - Настройка сбора журналов событий

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Создавать новые правила сбора событий на сервере, расположенном на указанном сайте (Event Registration Rules - Add)
- Изменять параметры правил сбора событий на сервере, на указанном сайте (Event Registration Rules - Modify)
- Удалять правила сбора событий на сервере, расположенном на указанном сайте (Event Registration Rules - Delete)

3.21.1.35. ALDPRO - Syncer Settings Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список контроллеров доменов AD
- Видеть карточки контроллеров доменов AD
- Видеть список контроллеров доменов ALD
- Видеть карточки контроллеров доменов ALD
- Видеть содержимое вкладки Синхронизация паролей
- Добавлять новые контроллеры домена AD
- Добавлять новые контроллеры домена ALD
- Получать файл ключа для синхронизации паролей AD ↔ ALD
- Изменять контроллеры домена AD
- Изменять контроллеры домена ALD
- Удалять контроллеры домена AD
- Удалять контроллеры домена ALD
- Видеть список контроллеров доменов
- Видеть карточки контроллеров доменов
- Видеть журнал изменений
- Просматривать сервера
- Видеть карточки сайтов
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS

Привилегии в составе роли

- MS AD and ALD Pro Controllers - Read
- MS AD and ALD Pro Controllers - Create
- MS AD and ALD Pro Controllers - Modify
- MS AD and ALD Pro Controllers - Drop

- Domain Controllers - Read
- IPA Servers - Read
- Sites - Read
- Computers - Read
- Organization units - Read
- DNS Zones - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Сайты и службы
- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
- Роли и службы сайта:
  - Служба разрешения имён
- Модуль синхронизации:
  - Настройки

Возможность ограничения области действия

В составе роли нет привилегий, область действия которых может быть ограничена.

3.21.1.36. ALDPRO - Syncer Sources Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список сопоставлений подразделений
- Видеть карточки сопоставлений подразделений
- Управлять карточками сопоставлений подразделений: создавать, редактировать,

удалять

- Видеть структуру дерева синхронизации
- Проверять на наличие конфликтов синхронизации и решать их
- Видеть список контроллеров доменов
- Видеть карточки контроллеров доменов
- Видеть журнал изменений
- Просматривать сервера
- Видеть карточки сайтов
- Видеть список компьютеров
- Видеть карточки компьютеров
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список зон DNS
- Видеть карточки зон DNS
- Видеть список контроллеров доменов AD
- Видеть карточки контроллеров доменов AD
- Видеть список контроллеров доменов ALD
- Видеть карточки контроллеров доменов ALD
- Видеть содержимое вкладки Синхронизация паролей

Привилегии в составе роли

- Organizational Units Mapping - Read
- Organizational Units Mapping - Manage
- Synchronization Tree - Read
- Synchronization Tree - Manage
- Domain Controllers - Read
- IPA Servers - Read
- Sites - Read
- Computers - Read
- Organization units - Read

- DNS Zones - Read
- MS AD and ALD Pro Controllers - Read

Доступ к подразделам портала управления

- Управление доменом:
  - Сайты и службы
- Пользователи и компьютеры:
  - Организационная структура
  - Компьютеры
- Роли и службы сайта:
  - Служба разрешения имён
- Модуль синхронизации:
  - Настройки
  - Источники

Возможность ограничения области действия

В составе роли нет привилегий, область действия которых может быть ограничена.

3.21.1.37. ALDPRO - Syncer Attributes Mapping Administrators

Подробное описание возможностей роли

Роль позволяет:

- Видеть список атрибутов AD
- Видеть список атрибутов ALD
- Видеть список сопоставлений атрибутов
- Управлять атрибутами AD: создавать, удалять;
- Управлять атрибутами ALD: создавать, удалять;
- Управлять сопоставлениями атрибутов: создавать, удалять

Привилегии в составе роли

- Attributes Mapping - Read
- Attributes Mapping - Manage

Доступ к подразделам портала управления

- Модуль синхронизации:
  - Сопоставление атрибутов

Возможность ограничения области действия

В составе роли нет привилегий, область действия которых может быть ограничена.

3.21.1.38. ALDPRO - Domain Viewer

Подробное описание возможностей роли

Роль позволяет:

- Видеть список атрибутов AD
- Видеть список атрибутов ALD
- Видеть список сопоставлений атрибутов
- Видеть список папок заданий автоматизации
- Видеть список заданий автоматизации
- Видеть карточки папок заданий автоматизации
- Видеть карточки заданий автоматизации
- Видеть список заданий автоматизации в журнале заданий
- Видеть карточки заданий автоматизации в журнале заданий
- Видеть список параметров компьютеров
- Видеть список папок компьютеров
- Видеть карточки параметров компьютеров
- Видеть карточки папок параметров компьютеров

- Видеть список групп компьютеров
- Видеть карточки групп компьютеров
- Видеть список компьютеров
- Видеть карточки компьютера
- Видеть витрины мониторинга
- Видеть список серверов динамической настройки узла
- Видеть карточки серверов динамической настройки узла
- Видеть журнал изменений
- Видеть список перенаправлений запросов
- Видеть карточки перенаправлений запросов
- Видеть список зон DNS
- Видеть карточки зон DNS
- Видеть список контроллеров доменов
- Видеть карточки контроллеров доменов
- Видеть общую информацию о домене
- Видеть список серверов журнала событий
- Видеть карточки серверов журнала событий
- Видеть список правил сбора событий
- Видеть карточки правил сбора событий
- Видеть список серверов общего доступа к файлам
- Видеть карточки серверов общего доступа к файлам
- Видеть список папок с общим доступом
- Видеть карточки папок с общим доступом
- Видеть список контроллеров домена с ролью глобального каталога
- Видеть список групповых политик
- Видеть карточки групповых политик
- Видеть список групповых политик в карточке подразделения
- Видеть карточки групповых политик в карточке подразделения
- Видеть список групповых политик в карточке пользователя
- Видеть список групповых политик в карточке компьютера
- Видеть список правил HBAC

- Видеть список служб HBAC
- Видеть список групп служб HBAC
- Видеть карточки правил HBAC
- Видеть карточки служб HBAC
- Видеть карточки групп служб HBAC
- Видеть список серверов установки ОС по сети
- Видеть карточки серверов установки ОС по сети
- Видеть перечень компьютеров
- Видеть карточки компьютеров
- Видеть список профилей загрузки
- Видеть карточки профилей загрузки
- Просматривать сервера
- Видеть список служб Kerberos
- Видеть карточки служб Kerberos
- Видеть список событий журнала мониторинга событий
- Видеть список серверов мониторинга
- Видеть карточки серверов мониторинга
- Видеть список контроллеров доменов AD
- Видеть карточки контроллеров доменов AD
- Видеть список контроллеров доменов ALD
- Видеть карточки контроллеров доменов ALD
- Видеть содержимое вкладки Синхронизация паролей
- Видеть список внешних NTP серверов
- Видеть список корневых NTP-серверов домена
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список сопоставлений подразделений
- Видеть карточки сопоставлений подразделений
- Видеть список политик паролей
- Видеть карточки политик паролей
- Видеть список серверов печати

- Видеть карточки серверов печати
- Видеть список соглашений о репликациях
- Видеть карточки соглашений о репликациях
- Видеть список репозиториев ПО
- Видеть карточки репозиториев ПО
- Видеть список серверов репозиториев ПО
- Видеть карточки серверов репозиториев ПО
- Видеть список ролей
- Видеть карточки ролей
- Видеть роли группы пользователей в карточке группы пользователей
- Видеть список сайтов домена
- Видеть карточки сайтов домена
- Видеть список программного обеспечения, пакетов и разделов (групп) ПО
- Видеть карточки разделов (групп) ПО
- Видеть карточки записей ПО
- Видеть список политик ПО
- Видеть карточки политик ПО
- Видеть параметры ПО в подразделениях
- Видеть параметры ПО в карточке компьютера
- Просматривать подсистемы
- Видеть список правил SUDO
- Видеть список команд SUDO
- Видеть список групп команд SUDO
- Видеть карточки правил SUDO
- Видеть карточки команд SUDO
- Видеть карточки групп команд SUDO
- Видеть структуру дерева синхронизации
- Видеть список политик обновления ALD Pro
- Видеть карточки политик обновления ALD Pro
- Видеть список политик обновления ALD Pro в карточке группы компьютеров
- Видеть список политик обновления ALD Pro в карточке компьютера

- Видеть список параметров пользователей
- Видеть карточки параметров пользователей
- Видеть список групп пользователей
- Видеть карточки групп пользователей
- Видеть список пользователей
- Видеть карточки пользователей
- Видеть список пользователей в корзине
- Видеть карточки пользователей в корзине
- Видеть список параметров пользователей
- Видеть список параметров групп
- Видеть список POSIX идентификаторов
- Видеть список атрибутов пользователей
- Видеть карточки атрибутов пользователей
- Видеть список дополнительных параметров пользователей

Привилегии в составе роли

- Attributes Mapping - Read
- Automation Tasks - Read
- Automation Tasks Journal - Read
- Computer Group Policy Additional Parameters - Read
- Computer groups - Read
- Computers - Read
- Dashboards - Read
- DHCP - Read
- DNS Forward Zones - Read
- DNS Zones - Read
- Domain Controllers - Read
- Domain Info - Read
- Event Log Servers - Read
- Event Registration Rules - Read

- File Servers - Read
- Global Catalog - Read
- Group Policies - Read
- HBAC - Read
- Installation Servers - Read
- IPA Servers - Read
- Kerberos Services - Read
- Monitoring Event Logs - Read
- Monitoring Servers - Read
- MS AD and ALD Pro Controllers - Read
- NTP Servers - Read
- Organization units - Read
- Organizational Units Mapping - Read
- Password Policies - Read
- Print Servers - Read
- Replication Agreements - Read
- Repositories - Read
- Repository Servers - Read
- Roles - Read
- Site Parameters - Read
- Sites - Read
- Software Catalog - Read
- Software Policies - Read
- Subsystems - Read
- SUDO - Read
- Synchronization Tree - Read
- Update Policies - Read
- User Group Policy Additional Parameters - Read
- User groups - Read
- Users - Read
- Users - Read trash

- Users and Groups Settings - Read

Доступ к подразделам портала управления

Весь портал, кроме раздела «Управление доменом: Интеграция с доменами»

Возможность ограничения области действия

В составе роли нет привилегий, область действия которых может быть ограничена.

3.21.1.39. ALDPRO - Regional Administrator

Подробное описание возможностей роли

Роль позволяет:

- Видеть список серверов печати
- Видеть карточки серверов печати
- Видеть журнал изменений
- Создавать новые серверы печати
- Изменять параметры серверов печати на указанном сайте
- Обновлять серверы печати на указанном сайте
- Удалять серверы печати на указанном сайте
- Управлять принтерами серверов печати: добавлять, удалять, редактировать, снимать задания печати на указанном сайте
- Создавать новые серверы журнала событий на указанном сайте
- Удалять серверы журнала событий на указанном сайте
- Изменять параметры серверов журнала событий на указанном сайте
- Обновлять серверы журнала событий на указанном сайте
- Видеть список серверов журнала событий
- Видеть карточки серверов журнала событий
- Видеть список правил сбора событий
- Видеть карточки правил сбора событий

- Создавать новые правила сбора событий на сервере, расположенном на указанном сайте
- Изменять параметры правил сбора событий на сервере, на указанном сайте
- Удалять правила сбора событий на сервере, расположенном на указанном сайте
- Видеть список событий журнала мониторинга событий
- Видеть список серверов мониторинга
- Видеть карточки серверов мониторинга
- Создавать новые серверы мониторинга на указанном сайте
- Изменять параметры серверов мониторинга на указанном сайте
- Обновлять сервер мониторинга на указанном сайте
- Удалять серверы мониторинга на указанном сайте
- Видеть витрины мониторинга
- Видеть список серверов динамической настройки узла
- Видеть карточки серверов динамической настройки узла
- Создавать новые серверы динамической настройки узла на указанном сайте
- Изменять параметры серверов динамической настройки узла на указанном сайте
- Обновлять серверы динамической настройки узла на указанном сайте
- Управлять конфигурациями скрипта и настройками сетевых интерфейсов: просматривать, добавлять, удалять, редактировать
- Удалять серверы динамической настройки узла на указанном сайте
- Видеть список серверов общего доступа к файлам
- Видеть карточки серверов общего доступа к файлам
- Видеть список папок с общим доступом
- Видеть карточки папок с общим доступом
- Создавать новые серверы общего доступа к файлам на указанном сайте
- Изменять параметры серверов общего доступа к файлам на указанном сайте
- Обновлять серверы общего доступа к файлам на указанном сайте
- Управлять папками с общим доступом: просматривать, добавлять, удалять, редактировать, настраивать доступ пользователям/компьютерам на указанном сайте
- Удалять серверы общего доступа к файлам на указанном сайте
- Видеть общую информацию о домене

- Видеть список контроллеров доменов
- Видеть карточки контроллеров доменов
- Удалять контроллеры домена на указанном сайте
- Создавать новые контроллеры домена на указанном сайте
- Видеть список сайтов домена
- Видеть карточки сайтов домена
- Создавать новые сайты
- Изменять сайты
- Назначать для сайтов контроллеры домена
- Удалять сайты
- Видеть список соглашений о репликациях
- Видеть карточки соглашений о репликациях
- Создавать новые соглашения о репликации
- Изменять соглашения о репликации
- Удалять соглашения о репликации
- Обновлять сервер контроллера домена на указанном сайте
- Видеть список групповых политик
- Видеть карточки групповых политик
- Видеть список групповых политик в карточке подразделения
- Видеть карточки групповых политик в карточке подразделения
- Видеть список групповых политик в карточке пользователя
- Видеть список групповых политик в карточке компьютера
- Создавать новые групповые политики
- Изменять групповые политики
- Удалять групповые политики
- Управлять значениями параметров компьютеров: редактировать, удалять
- Управлять конфигурациями с типом «Компьютеры»: редактировать, удалять
- Управлять значениями параметров пользователей: редактировать
- Управлять конфигурациями с типом «Пользователи»
- Управлять политиками для подразделений: добавлять, удалять, изменять приоритет
- Видеть список параметров пользователей

- Видеть карточки параметров пользователей
- Видеть список параметров компьютеров
- Видеть список папок компьютеров
- Видеть карточки параметров компьютеров
- Видеть карточки папок параметров компьютеров
- Видеть список правил HBAC
- Видеть список служб HBAC
- Видеть список групп служб HBAC
- Видеть карточки правил HBAC
- Видеть карточки служб HBAC
- Видеть карточки групп служб HBAC
- Создавать новые правила HBAC
- Изменять правила HBAC
- Удалять правила HBAC
- Создавать новые службы HBAC
- Изменять службы HBAC
- Удалять службы HBAC
- Создавать новые группы служб HBAC
- Изменять группы служб HBAC
- Удалять группы служб HBAC
- Видеть список правил SUDO
- Видеть список команд SUDO
- Видеть список групп команд SUDO
- Видеть карточки правил SUDO
- Видеть карточки команд SUDO
- Создавать новые правила SUDO
- Изменять правила SUDO, кроме вкладки Параметры
- Управлять параметрами SUDO для правил SUDO
- Удалять правила SUDO
- Создавать новые команды SUDO
- Изменять команды SUDO

- Удалять команды SUDO
- Создавать новые группы команд SUDO
- Изменять группы команд SUDO
- Удалять группы команд SUDO
- Видеть список заданий автоматизации в журнале заданий
- Видеть карточки заданий автоматизации в журнале заданий
- Запускать задания автоматизации
- Управлять атрибутами задания автоматизации: создавать, редактировать, удалять
- Видеть список папок заданий автоматизации
- Видеть список заданий автоматизации
- Видеть карточки папок заданий автоматизации
- Видеть карточки заданий автоматизации
- Управлять конфигурацией скрипта задания автоматизации: редактировать
- Управлять компьютерами для сервера установки ОС по сети: добавлять, удалять
- Управлять профилями загрузки для сервера установки ОС по сети: добавлять, редактировать, удалять
- Видеть список серверов установки ОС по сети
- Видеть карточки серверов установки ОС по сети
- Видеть список политик обновления ALD Pro
- Видеть карточки политик обновления ALD Pro
- Видеть список политик обновления ALD Pro в карточке группы компьютеров
- Видеть список политик обновления ALD Pro в карточке компьютера
- Создавать новые политики обновления ALD Pro
- Редактировать политики обновления ALD Pro
- Удалять политики обновления ALD Pro
- Управлять конфигурацией Sources list в политике обновления ALD Pro: редактировать
- Управлять составом компьютеров и групп компьютеров в политиках обновления ALD Pro: добавлять, удалять
- Видеть список ролей
- Видеть карточки ролей
- Видеть роли пользователя в карточке пользователя

- Видеть роли группы пользователей в карточке группы пользователей
- Создавать и копировать роли
- Управлять назначением ролей на пользователей и группы пользователей: добавлять, удалять
- Управлять назначением ролей на пользователей: добавлять, удалять
- Управлять назначением ролей на группы пользователей
- Удалять роли
- Добавлять привилегии в состав роли
- Изменять сайт для привилегий, у которых есть ограничение по сайту
- Удалять привилегии из состава роли
- Создавать новые группы компьютеров
- Удалять группы компьютеров
- Изменять параметры группы компьютеров (кроме выбора подразделения)
- Видеть список групп компьютеров
- Видеть карточки групп компьютеров
- Управлять составом компьютеров в группе компьютеров
- Управлять составом групп компьютеров в группе компьютеров
- Управлять составом групп компьютеров в подразделениях
- Видеть список зон DNS
- Видеть карточки зон DNS
- Создавать новые подразделения
- Удалять подразделения
- Изменять параметры подразделений
- Видеть дерево подразделений
- Видеть карточки подразделений
- Видеть список сайтов
- Видеть карточки сайтов
- Просматривать подсистемы
- Создавать новые группы пользователей
- Удалять группы пользователей
- Изменять группы пользователей

- Видеть список групп пользователей
- Видеть карточки групп пользователей
- Управлять составом пользователей в группе пользователей
- Управлять составом групп пользователей в группе пользователей
- Управлять составом групп пользователей в подразделениях
- Создавать новых пользователей
- Изменять пользователей (кроме выбора подразделения)
- Перемещать пользователей в корзину
- Видеть список пользователей
- Видеть карточки пользователей
- Управлять составом пользователей в подразделениях
- Видеть список пользователей в корзине
- Видеть карточки пользователей в корзине
- Сбрасывать пароль для пользователя
- Блокировать и разблокировать пользователя
- Print Servers - Read
- Print Servers - Create
- Print Servers - Modify
- Print Servers - Drop
- Printers - Manage
- Event Log Servers - Create
- Event Log Servers - Drop
- Event Log Servers - Modify
- Event Log Servers - Read
- Event Registration Rules - Read
- Event Registration Rules - Add
- Event Registration Rules - Modify
- Event Registration Rules - Delete
- Monitoring Event Logs - Read
- Monitoring Servers - Read
- Monitoring Servers - Create

- Monitoring Servers - Modify
- Monitoring Servers - Drop
- Dashboards - Read
- DHCP - Read
- DHCP Servers - Create
- DHCP Servers - Modify
- DHCP Configuration - Modify
- DHCP Servers - Drop
- File Servers - Read
- File Servers - Create
- File Servers - Modify
- File Server Folders - Manage
- File Servers - Drop
- Domain Info - Read
- Domain Controllers - Read
- Domain Controllers - Drop
- Domain Controllers - Create
- Site Parameters - Read
- Site Parameters - Add
- Site Parameters - Modify
- Site Domain Controllers - Add
- Site Parameters - Delete
- Replication Agreements - Read
- Replication Agreements - Add
- Replication Agreements - Modify
- Replication Agreements - Delete
- Domain Controllers - Modify
- Group Policies - Read
- Group Policies - Add
- Group Policies - Modify
- Group Policies - Delete

- Group Policies Computer Parameters - Manage
- Group Policies User Parameters - Manage
- Group Policies Membership - Manage
- User Group Policy Additional Parameters - Read
- Computer Group Policy Additional Parameters - Read
- HBAC - Read
- HBAC Rules - Add
- HBAC Rules - Modify
- HBAC Rules - Delete
- HBAC Services - Add
- HBAC Services - Modify
- HBAC Services - Delete
- HBAC Service Groups - Add
- HBAC Service Groups - Modify
- HBAC Service Groups - Delete
- SUDO - Read
- SUDO Rules - Add
- SUDO Rules - Modify
- SUDO Parameters - Manage
- SUDO Rules - Delete
- SUDO Commands - Add
- SUDO Command - Modify
- SUDO Command - Delete
- SUDO Command Groups - Add
- SUDO Command Groups - Modify
- SUDO Command Groups - Delete
- Automation Tasks Journal - Read
- Automation Tasks Membership - Manage
- Automation Task Attributes - Manage
- Automation Tasks - Read
- Automation Task Script - Manage

- Installation Server Computers - Manage
- Installation Server Profiles - Manage
- Installation Servers - Read
- Update Policies - Read
- Update Policies - Add
- Update Policies - Modify
- Update Policies - Delete
- Update Policies Sources list - Manage
- Update Policies Computers - Manage
- Roles - Read
- Roles - Add
- Roles - Modify
- Roles Membership - Manage
- Roles - Delete
- Role Privileges - Add
- Role Privileges - Modify
- Role Privileges - Delete
- Computer groups - Add
- Computer groups - Delete
- Computer groups - Modify
- Computer groups - Read
- Computer groups - Set group membership
- Computer groups - Set organization unit
- Computers - Delete
- Computers - Modify
- Computers - Read
- Computers - Remote access
- Computers - Set organization unit
- DNS Zones - Read
- IPA Servers - Read
- Organization Units - Add

- Organization units - Delete
- Organization units - Modify
- Organization units - Read
- Sites - Read
- Subsystems - Read
- User groups - Add
- User groups - Delete
- User groups - Modify
- User groups - Read
- User groups - Set group membership
- User groups - Set organization unit
- Users - Add
- Users - Modify
- Users - Move to trash
- Users - Read
- Users - Set organization unit
- Users - Read trash
- Users Password - Modify
- Users Block - Modify

Привилегии в составе роли

- Print Servers - Read
- Print Servers - Create
- Print Servers - Modify
- Print Servers - Drop
- Printers - Manage
- Event Log Servers - Create
- Event Log Servers - Drop
- Event Log Servers - Modify
- Event Log Servers - Read

- Event Registration Rules - Read
- Event Registration Rules - Add
- Event Registration Rules - Modify
- Event Registration Rules - Delete
- Monitoring Event Logs - Read
- Monitoring Servers - Read
- Monitoring Servers - Create
- Monitoring Servers - Modify
- Monitoring Servers - Drop
- Dashboards - Read
- DHCP - Read
- DHCP Servers - Create
- DHCP Servers - Modify
- DHCP Configuration - Modify
- DHCP Servers - Drop
- File Servers - Read
- File Servers - Create
- File Servers - Modify
- File Server Folders - Manage
- File Servers - Drop
- Domain Info - Read
- Domain Controllers - Read
- Domain Controllers - Drop
- Domain Controllers - Create
- Site Parameters - Read
- Site Parameters - Add
- Site Parameters - Modify
- Site Domain Controllers - Add
- Site Parameters - Delete
- Replication Agreements - Read
- Replication Agreements - Add

- Replication Agreements - Modify
- Replication Agreements - Delete
- Domain Controllers - Modify
- Group Policies - Read
- Group Policies - Add
- Group Policies - Modify
- Group Policies - Delete
- Group Policies Computer Parameters - Manage
- Group Policies User Parameters - Manage
- Group Policies Membership - Manage
- User Group Policy Additional Parameters - Read
- Computer Group Policy Additional Parameters - Read
- HBAC - Read
- HBAC Rules - Add
- HBAC Rules - Modify
- HBAC Rules - Delete
- HBAC Services - Add
- HBAC Services - Modify
- HBAC Services - Delete
- HBAC Service Groups - Add
- HBAC Service Groups - Modify
- HBAC Service Groups - Delete
- SUDO - Read
- SUDO Rules - Add
- SUDO Rules - Modify
- SUDO Parameters - Manage
- SUDO Rules - Delete
- SUDO Commands - Add
- SUDO Command - Modify
- SUDO Command - Delete
- SUDO Command Groups - Add

- SUDO Command Groups - Modify
- SUDO Command Groups - Delete
- Automation Tasks Journal - Read
- Automation Tasks Membership - Manage
- Automation Task Attributes - Manage
- Automation Tasks - Read
- Automation Task Script - Manage
- Installation Server Computers - Manage
- Installation Server Profiles - Manage
- Installation Servers - Read
- Update Policies - Read
- Update Policies - Add
- Update Policies - Modify
- Update Policies - Delete
- Update Policies Sources list - Manage
- Update Policies Computers - Manage
- Roles - Read
- Roles - Add
- Roles - Modify
- Roles Membership - Manage
- Roles - Delete
- Role Privileges - Add
- Role Privileges - Modify
- Role Privileges - Delete
- Computer groups - Add
- Computer groups - Delete
- Computer groups - Modify
- Computer groups - Read
- Computer groups - Set group membership
- Computer groups - Set organization unit
- Computers - Delete

- Computers - Modify
- Computers - Read
- Computers - Remote access
- Computers - Set organization unit
- DNS Zones - Read
- IPA Servers - Read
- Organization Units - Add
- Organization units - Delete
- Organization units - Modify
- Organization units - Read
- Sites - Read
- Subsystems - Read
- User groups - Add
- User groups - Delete
- User groups - Modify
- User groups - Read
- User groups - Set group membership
- User groups - Set organization unit
- Users - Add
- Users - Modify
- Users - Move to trash
- Users - Read
- Users - Set organization unit
- Users - Read trash
- Users Password - Modify
- Users Block - Modify

Внимание: Важно использовать привилегию **Roles Membership - Manage** с осторожностью. Пользователь, на которого назначена роль, привязанная к корневому подразделению домена с установленным признаком **Включая дочерние подразделения**, в составе которой есть данная привилегия, получает возможность

как назначать любые роли на любого пользователя, получая таким образом возможность назначить набор ролей, аналогичный роли **ALDPRO - Main Administrator**, так и снимать назначение уже назначенных ролей с любых пользователей домена, что приведет к лишению этих пользователей имеющихся у них привилегий.

Доступ к подразделам портала управления

- Управление доменом:
  - Общая информация
  - Сайты и службы
  - Доп. Параметры групповых политик
  - Каталог заданий автоматизации
  - Роли и права доступа
- Пользователи и компьютеры:
  - Организационная структура
  - Пользователи
  - Группы пользователей
  - Компьютеры
  - Группы компьютеров
  - Корзина
- Групповые политики:
  - Групповые политики
  - Политики доступа к узлу
  - Политики повышения привилегий
- Установка и обновление ПО:
  - Политики обновления ALD Pro
- Автоматизация:
  - Задания автоматизации
  - Установка ОС по сети

- Роли и службы сайта:
  - Служба разрешения имен
  - Служба динамической настройки узла
  - Служба печати
  - Общий доступ к файлам
- Мониторинг:
  - Журнал событий мониторинга
  - Витрины мониторинга домена
- Журнал событий:
  - Серверы журнала событий
  - Настройка сбора журналов событий

Возможность ограничения области действия

Роль может ограничивать область действия для возможностей:

- Создавать новые серверы печати (Print Servers - Create)
- Изменять параметры серверов печати на указанном сайте (Print Servers - Modify)
- Обновлять серверы печати на указанном сайте (Print Servers - Modify)
- Удалять серверы печати на указанном сайте (Print Servers - Drop)
- Управлять принтерами серверов печати: добавлять, удалять, редактировать, снимать задания печати на указанном сайте (Printers - Manage)
- Создавать новые серверы журнала событий на указанном сайте (Event Log Servers - Create)
- Удалять серверы журнала событий на указанном сайте (Event Log Servers - Drop)
- Изменять параметры серверов журнала событий на указанном сайте (Event Log Servers - Modify)
- Обновлять серверы журнала событий на указанном сайте (Event Log Servers - Modify)
- Создавать новые правила сбора событий на сервере, расположенном на указанном сайте (Event Registration Rules - Add)
- Изменять параметры правил сбора событий на сервере, на указанном сайте (Event Registration Rules - Modify)

- Удалять правила сбора событий на сервере, расположенном на указанном сайте (Event Registration Rules - Delete)
- Создавать новые серверы мониторинга на указанном сайте (Monitoring Servers - Create)
- Изменять параметры серверов мониторинга на указанном сайте (Monitoring Servers - Modify)
- Обновлять сервер мониторинга на указанном сайте (Monitoring Servers - Modify)
- Удалять серверы мониторинга на указанном сайте (Monitoring Servers - Drop)
- Создавать новые серверы динамической настройки узла на указанном сайте (DHCP Servers - Create)
- Изменять параметры серверов динамической настройки узла на указанном сайте (DHCP Servers - Modify)
- Обновлять серверы динамической настройки узла на указанном сайте (DHCP Servers - Modify)
- Управлять конфигурациями скрипта и настройками сетевых интерфейсов: просматривать, добавлять, удалять, редактировать (DHCP Configuration - Modify)
- Удалять серверы динамической настройки узла на указанном сайте (DHCP Servers - Drop)
- Создавать новые серверы общего доступа к файлам на указанном сайте (File Servers - Create)
- Изменять параметры серверов общего доступа к файлам на указанном сайте (File Servers - Modify)
- Обновлять серверы общего доступа к файлам на указанном сайте (File Servers - Modify)
- Управлять папками с общим доступом: просматривать, добавлять, удалять, редактировать, настраивать доступ пользователям/компьютерам на указанном сайте (File Server Folders - Manage)
- Удалять серверы общего доступа к файлам на указанном сайте (File Servers - Drop)
- Удалять контроллеры домена на указанном сайте (Domain Controllers - Drop)
- Создавать новые контроллеры домена на указанном сайте (Domain Controllers - Create)
- Обновлять сервер контроллера домена на указанном сайте (Domain Controllers - Modify)
- Управлять политиками для подразделений: добавлять, удалять, изменять приоритет

(Group Policies Membership - Manage)

- Изменять правила HBAC (HBAC Rules - Modify)
- Изменять правила SUDO, кроме вкладки Параметры (SUDO Rules - Modify)
- Запускать задания автоматизации (Automation Tasks Membership - Manage)
- Управлять компьютерами для сервера установки ОС по сети: добавлять, удалять (Installation Server Computers - Manage)
- Управлять профилями загрузки для сервера установки ОС по сети: добавлять, редактировать, удалять (Installation Server Profiles - Manage)
- Управлять составом компьютеров и групп компьютеров в политиках обновления ALD Pro: добавлять, удалять (Update Policies Computers - Manage)
- Создавать и копировать роли (Roles - Modify)
- Управлять назначением ролей на пользователей и группы пользователей: добавлять, удалять (Roles Membership - Manage)
- Управлять назначением ролей на пользователей: добавлять, удалять (Roles Membership - Manage)
- Управлять назначением ролей на группы пользователей (Roles Membership - Manage)
- Удалять роли (Roles - Delete)
- Добавлять привилегии в состав роли (Role Privileges - Add)
- Изменять сайт для привилегий, у которых есть ограничение по сайту (Role Privileges - Modify)
- Удалять привилегии из состава роли (Role Privileges - Delete)
- Создавать новые группы компьютеров (Computer groups - Add)
- Удалять группы компьютеров (Computer groups - Delete)
- Изменять параметры группы компьютеров (кроме выбора подразделения) (Computer groups - Modify)
- Управлять составом компьютеров в группе компьютеров (Computer groups - Set group membership)
- Управлять составом групп компьютеров в группе компьютеров (Computer groups - Set group membership)
- Управлять составом групп компьютеров в подразделениях (Computer groups - Set organization unit)
- Создавать новые подразделения (Organization Units - Add)
- Удалять подразделения (Organization Units - Delete)

- Изменять параметры подразделений (Organization Units - Modify)
- Создавать новые группы пользователей (User groups - Add)
- Удалять группы пользователей (User groups - Delete)
- Изменять группы пользователей (User groups - Modify)
- Управлять составом пользователей в группе пользователей (User groups - Set group membership)
- Управлять составом групп пользователей в группе пользователей (User groups - Set group membership)
- Управлять составом групп пользователей в подразделениях (User groups - Set organization unit)
- Создавать новых пользователей (Users - Add)
- Изменять пользователей (кроме выбора подразделения) (Users - Modify)
- Перемещать пользователей в корзину (Users - Move to trash)
- Управлять составом пользователей в подразделениях (Users - Set organization unit)
- Сбрасывать пароль для пользователя (Users Password - Modify)
- Блокировать и разблокировать пользователя (Users Block - Modify)

3.21.1.40. ALDPRO - Main Administrator

Подробное описание возможностей роли

Роль позволяет выполнять все операции в портале управления. Доступны все привилегии. Обеспечен полный доступ ко всем разделам портала управления. Роль не может быть ограничена.

3.21.2. Матрицы ролей

3.21.2.1. Обозначения

- o - Возможность Ограничения области действия роли
- но - Область действия Не может быть Ограничена

3.21.2.2. Управление доменом

Роли	Общая информация	Сайты и службы	Доп. параметры групповых политик	Каталог заданий автоматизации	Службы и параметры Kerberos	Пользователи и группы	Интеграция с доменами	Роли и права доступа
ALDPRO - Domain Info Reader	но	но						
ALDPRO - Domain Controllers and Sites Service Administrators		о						
ALDPRO - Group Policies Additional Parameters Administrators			но					
ALDPRO - Automation Tasks Catalog Administrators				но				
ALDPRO - Kerberos Service Administrators		но			но			
ALDPRO - Users and Groups Settings Administrators						но		
ALDPRO - Domain Integrations Administrators							но	
ALDPRO - Roles Administrators		о						о
ALDPRO - Organizational Units Administrators			но					
ALDPRO - Group Policies Administrators			но					
ALDPRO - Software Catalog Administrators		но						
ALDPRO - Software Repositories Administrators		о						
ALDPRO - Automation Tasks Administrators				но				
ALDPRO - Install OS Service Administrators	но	о						
ALDPRO - DHCP Service Administrators		о						
ALDPRO - NTP Service Administrators		но						
ALDPRO - Print Service Administrators		о						
ALDPRO - File Servers Administrators		о						
ALDPRO - Global Catalog Service Administrators		о						
ALDPRO - Monitoring Administrators		о						
ALDPRO - Monitoring Dashboards Readers		но						
ALDPRO - Event Log Servers Administrators		о						
ALDPRO - Event Log Administrators		о						
ALDPRO - Syncer Settings Administrators		но						
ALDPRO - Syncer Sources Administrators		но						
ALDPRO - Syncer Attributes Mapping Administrators		но						
ALDPRO - Domain Viewer	но	но	но	но	но	но		но

продолжение на следующей странице

Таблица 3.49 – продолжение с предыдущей страницы

Роли	Общая информация	Сайты и службы	Доп. параметры групповых политик	Каталог заданий автоматизации	Службы и параметры Kerberos	Пользователи и группы	Интеграция с доменами	Роли и права доступа
ALDPRO - Regional Administrator	но	о	но	но				о
ALDPRO - Main Administrator	но	но	но	но	но	но	но	но

3.21.2.3. Пользователи и группы

Роли	Организационная структура	Пользователи	Группы пользователей	Компьютеры	Группы компьютеров	Корзина
ALDPRO - Domain Info Reader	но			но		
ALDPRO - Domain Controllers and Sites Service Administrators	о			о		
ALDPRO - Kerberos Service Administrators	но			но		
ALDPRO - Users and Groups Settings Administrators	о	о				
ALDPRO - Roles Administrators	о	о	о			
ALDPRO - Organizational Units Administrators	о	о		о	о	
ALDPRO - Users Administrators	о	о				о
ALDPRO - User Groups Administrators	о	о	о			
ALDPRO - Computers Administrators	о			о		
ALDPRO - Computer Groups Administrators	о			о	о	
ALDPRO - Deleted User Accounts Administrators	но	но	но			но
ALDPRO - Group Policies Administrators	о					
ALDPRO - HBAC Administrators	о	о	о	о	о	
ALDPRO - SUDO Administrators	о	о	о	о	о	
ALDPRO - Password Policies Administrators	но		но			
ALDPRO - Software Policies Administrators	но			но	но	
ALDPRO - Software Catalog Administrators	но			но		
ALDPRO - Software Repositories Administrators	о			о		
ALDPRO - Software Update Policies Administrators	о			о	о	
ALDPRO - Automation Tasks Administrators	о	о		о	о	
ALDPRO - Install OS Service Administrators	о			о		
ALDPRO - DHCP Service Administrators	о			о		
ALDPRO - NTP Service Administrators	но			но		
ALDPRO - Print Service Administrators	о			о		
ALDPRO - File Servers Administrators	о	о	о	о		
ALDPRO - Global Catalog Service Administrators	о			о		
ALDPRO - Monitoring Administrators	о			о		
ALDPRO - Monitoring Dashboards Readers	но			но		
ALDPRO - Event Log Servers Administrators	о			о		
ALDPRO - Event Log Administrators	о			о		
ALDPRO - Syncer Settings Administrators	но			но		
ALDPRO - Syncer Sources Administrators	но			но		
ALDPRO - Syncer Attributes Mapping Administrators	но			но		
ALDPRO - Domain Viewer	но	но	но	но	но	но

продолжение на следующей странице

Таблица 3.50 – продолжение с предыдущей страницы

Роли	Организационная структура	Пользователи	Группы пользователей	Компьютеры	Группы компьютеров	Корзина
ALDPRO - Regional Administrator	o	o	o	o	o	o
ALDPRO - Main Administrator	но	но	но	но	но	но

3.21.2.4. Групповые политики

Роли	Групповые политики	Политики доступа к узлу	Политики повышения привилегий	Политики паролей
ALDPRO - Group Policies Administrators	o			
ALDPRO - HBAC Administrators		o		
ALDPRO - SUDO Administrators			o	
ALDPRO - Password Policies Administrators				но
ALDPRO - Domain Viewer	но	но	но	но
ALDPRO - Regional Administrator	o	o	o	
ALDPRO - Main Administrator	но	но	но	но

3.21.2.5. Установка и обновление ПО

Роли	Политики ПО	Каталог ПО	Репозитории ПО	Политики обновления ALD Pro
ALDPRO - Organizational Units Administrators	но			
ALDPRO - Software Policies Administrators	но	но		
ALDPRO - Software Catalog Administrators		но	но	
ALDPRO - Software Repositories Administrators		но	o	
ALDPRO - Software Update Policies Administrators				o
ALDPRO - Domain Viewer	но	но	но	но
ALDPRO - Regional Administrator				o
ALDPRO - Main Administrator	но	но	но	но

3.21.2.6. Автоматизация

Роли	Задания автоматизации	Установка ОС по сети
ALDPRO - Automation Tasks Administrators	о	
ALDPRO - Install OS Service Administrators		о
ALDPRO - Domain Viewer	но	но
ALDPRO - Regional Administrator	о	о
ALDPRO - Main Administrator	но	но

3.21.2.7. Роли и службы сайта

Роли	Служба разрешения имен	Служба динамической настрой-ки узла	Служба синхронизации времени	Служба печати	Общий доступ к файлам	Служба глобального каталога
ALDPRO - Domain Info Reader	но					
ALDPRO - Domain Controllers and Sites Service Administrators	но					
ALDPRO - Kerberos Service Administrators	но					
ALDPRO - Domain Integrations Administrators	но					
ALDPRO - Organizational Units Administrators	но					
ALDPRO - Computers Administrators	но					
ALDPRO - Computer Groups Administrators	но					
ALDPRO - HBAC Administrators	но					
ALDPRO - SUDO Administrators	но					
ALDPRO - Software Policies Administrators	но					
ALDPRO - Software Catalog Administrators	но					
ALDPRO - Software Repositories Administrators	но					
ALDPRO - Software Update Policies Administrators	но					
ALDPRO - Automation Tasks Administrators	но					
ALDPRO - Install OS Service Administrator	но	о				
ALDPRO - DNS Service Administrators	но					
ALDPRO - DHCP Service Administrators	но	о				
ALDPRO - NTP Service Administrators	но		но			
ALDPRO - Print Service Administrators	но			о		
ALDPRO - File Servers Administrators	но				о	
ALDPRO - Global Catalog Service Administrators	но					о
ALDPRO - Monitoring Administrators	но					
ALDPRO - Monitoring Dashboards Readers	но					
ALDPRO - Event Log Servers Administrators	но					
ALDPRO - Event Log Administrators	но					
ALDPRO - Syncer Settings Administrators	но					
ALDPRO - Syncer Sources Administrators	но					
ALDPRO - Syncer Attributes Mapping Administrators	но					
ALDPRO - Domain Viewer	но	но	но	но	но	но
ALDPRO - Regional Administrator	но	о		о	о	
ALDPRO - Main Administrator	но	но	но	но	но	но

3.21.2.8. Мониторинг

Роли	Журнал событий мониторинга	Витрины мониторинга домена
ALDPRO - Monitoring Administrators	о	но
ALDPRO - Monitoring Dashboards Readers	но	но
ALDPRO - Domain Viewer	но	но
ALDPRO - Regional Administrator	о	но
ALDPRO - Main Administrator	но	но

3.21.2.9. Журнал событий

Роли	Серверы журнала событий	Настройка сбора журналов событий
ALDPRO - Event Log Servers Administrators	о	
ALDPRO - Event Log Administrators	о	о
ALDPRO - Domain Viewer	но	но
ALDPRO - Regional Administrator	о	о
ALDPRO - Main Administrator	но	но

3.21.2.10. Модуль синхронизации

Роли	Настройки	Источники	Сопоставление атрибутов
ALDPRO - Syncer Settings Administrators	но		
ALDPRO - Syncer Sources Administrators	но	но	
ALDPRO - Syncer Attributes Mapping Administrators	но		но
ALDPRO - Domain Viewer	но	но	но
ALDPRO - Main Administrator	но	но	но

3.22. Матрица и описание привилегий

3.22.1. Описание привилегий

3.22.1.1. Domain Info - Read

Подробное описание

Привилегия позволяет:

- Видеть общую информацию о домене (Управление доменом/Общая информация вкладки: Работоспособность домена, Состав системы, Граф топологии, Параметры домена).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Общая информация

3.22.1.2. Domain Controllers - Read

Подробное описание

Привилегия позволяет:

- Видеть список контроллеров доменов (Управление доменом/Сайты и службы/вкладка Контроллеры домена);
- Видеть карточки контроллеров доменов (Управление доменом/Сайты и службы/вкладка Контроллеры домена/<Контроллер домена>);
- Видеть журнал изменений (Управление доменом/Сайты и службы/вкладка Контроллеры домена/<Контроллер домена>/Журнал истории изменений).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Сайты и службы

3.22.1.3. Domain Controllers - Drop

Подробное описание

Привилегия позволяет:

- Удалять контроллеры домена (Управление доменом/Сайты и службы/вкладка Контроллеры домена/<Контроллер домена>) на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Сайты и службы

3.22.1.4. Domain Controllers - Create

Подробное описание

Привилегия позволяет:

- Создавать новые контроллеры домена (Управление доменом/Сайты и службы/вкладка Контроллеры домена) на указанном сайте.

Вместе с Global Catalog - Add позволяет:

- Добавить роль глобального каталога при создании контроллера домена (Управление доменом/Сайты и службы/вкладка Контроллеры домена) при помощи признака «Назначить роль глобального каталога» на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Сайты и службы

3.22.1.5. Site Parameters - Read

Подробное описание

Привилегия позволяет:

- Видеть список сайтов домена (Управление доменом/Сайты и службы/вкладка Сайты);
- Видеть карточки сайтов домена (Управление доменом/Сайты и службы/вкладка

Сайты/<Сайт>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Сайты и службы

3.22.1.6. Site Parameters - Add

Подробное описание

Привилегия позволяет:

- Создавать новые сайты (Управление доменом/Сайты и службы/вкладка Сайты).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Сайты и службы

3.22.1.7. Site Parameters - Modify

Подробное описание

Привилегия позволяет:

- Изменять сайты (Управление доменом/Сайты и службы/вкладка Сайты/<Сайт>/вкладка Основное).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Сайты и службы

3.22.1.8. Site Domain Controllers - Add

Подробное описание

Привилегия позволяет:

- Назначать для сайтов контроллеры домена (Управление доменом/Сайты и службы/вкладка Сайты/<Сайт>/вкладка Контроллеры домена).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Сайты и службы

3.22.1.9. Site Parameters - Delete

Подробное описание

Привилегия позволяет:

- Удалять сайты (Управление доменом/Сайты и службы/вкладка Сайты/<Сайт>/вкладка Основное).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Сайты и службы

3.22.1.10. Replication Agreements - Read

Подробное описание

Привилегия позволяет:

- Видеть список соглашений о репликациях (Управление доменом/Сайты и службы/вкладка Соглашения о репликации);
- Видеть карточки соглашений о репликациях (Управление доменом/Сайты и службы/вкладка Соглашения о репликации/<Соглашение о репликации>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Сайты и службы

3.22.1.11. Replication Agreements - Add

Подробное описание

Привилегия позволяет:

- Создавать новые соглашения о репликации (Управление доменом/Сайты и службы/вкладка Соглашения о репликации).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Сайты и службы

3.22.1.12. Replication Agreements - Modify

Подробное описание

Привилегия позволяет:

- Изменять соглашения о репликации (Управление доменом/Сайты и службы/вкладка Соглашения о репликации/<Соглашение о репликации>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Сайты и службы

3.22.1.13. Replication Agreements - Delete

Подробное описание

Привилегия позволяет:

- Удалять соглашения о репликации (Управление доменом/Сайты и службы/вкладка Соглашения о репликации/<Соглашение о репликации>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Сайты и службы

3.22.1.14. Domain Controllers - Modify

Подробное описание

Привилегия позволяет:

- Обновлять сервер контроллера домена на указанном сайте (Управление доменом/Сайты и службы/вкладка Контроллеры домена/<Контроллер домена>/кнопка «Обновить ALD Pro»).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Сайты и службы

3.22.1.15. Sites - Read

Подробное описание

Привилегия позволяет:

- Видеть список сайтов (Управление доменом/Сайты и службы/вкладка Сайты);
- Видеть карточки сайтов (Управление доменом/Сайты и службы/вкладка Сайты/<Сайт>).

Для отображения содержимого вкладки «Подсистемы сайта» на роль должна быть назначена добавочная привилегия Computers - Read.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Сайты и службы

3.22.1.16. Computer Group Policy Additional Parameters - Read

Подробное описание

Привилегия позволяет:

- Видеть список параметров компьютеров (Управление доменом/Доп. параметры групповых политик/вкладка Параметры компьютеров);
- Видеть список папок компьютеров (Управление доменом/Доп. параметры групповых политик/вкладка Параметры компьютеров);
- Видеть карточки параметров компьютеров (Управление доменом/Доп. параметры групповых политик/вкладка Параметры компьютеров/<Параметр компьютеров>);
- Видеть карточки папок параметров компьютеров (Управление доменом/Доп. параметры групповых политик/вкладка Параметры компьютеров/<Папка параметров компьютеров>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Доп. параметры групповых политик

3.22.1.17. Computer Group Policy Additional Parameters - Manage

Подробное описание

Привилегия позволяет:

- Управлять папками параметров компьютеров (Управление доменом/Доп. параметры групповых политик/вкладка Параметры компьютеров): создавать, редактировать, удалять;
- Управлять параметрами компьютеров (Управление доменом/Доп. параметры групповых политик/вкладка Параметры компьютеров): создавать, редактировать, удалять.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Доп. параметры групповых политик

3.22.1.18. User Group Policy Additional Parameters - Read

Подробное описание

Привилегия позволяет:

- Видеть список параметров пользователей (Управление доменом/Доп. параметры групповых политик/вкладка Параметры пользователей);
- Видеть карточки параметров пользователей (Управление доменом/Доп. параметры групповых политик/вкладка Параметры пользователей/<Параметр пользователей>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Доп. параметры групповых политик

3.22.1.19. User Group Policy Additional Parameters - Manage

Подробное описание

Привилегия позволяет:

- Управлять папками параметров пользователей (Управление доменом/Доп. параметры групповых политик/вкладка Параметры пользователей): создавать, редактировать, удалять;
- Управлять параметрами пользователей (Управление доменом/Доп. параметры групповых политик/вкладка Параметры пользователей): создавать, редактировать, удалять.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Доп. параметры групповых политик

3.22.1.20. Automation Tasks - Read

Подробное описание

Привилегия позволяет:

- Видеть список папок заданий автоматизации (Управление доменом/Каталог заданий автоматизации);
- Видеть список заданий автоматизации (Управление доменом/Каталог заданий автоматизации);
- Видеть карточки папок заданий автоматизации (Управление доменом/Каталог заданий автоматизации/<Папка заданий автоматизации>);

- Видеть карточки заданий автоматизации (Управление доменом/Каталог заданий автоматизации/<Задание автоматизации>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Каталог заданий автоматизации

3.22.1.21. Automation Task Attributes - Manage

Подробное описание

Привилегия позволяет:

- Управлять атрибутами задания автоматизации (Управление доменом/Каталог заданий автоматизации/<Задание автоматизации>/вкладка Атрибуты задания): создавать, редактировать, удалять.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Каталог заданий автоматизации

3.22.1.22. Automation Task Script - Manage

Подробное описание

Привилегия позволяет:

- Управлять конфигурацией скрипта задания автоматизации(Управление доменом/Каталог заданий автоматизации/<Задание автоматизации>/вкладка Конфигурация скрипта): редактировать.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Каталог заданий автоматизации

3.22.1.23. Automation Tasks Folders - Manage

Подробное описание

Привилегия позволяет:

- Управлять папками заданий автоматизации (Управление доменом/Каталог заданий автоматизации): создавать, редактировать, удалять.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Каталог заданий автоматизации

3.22.1.24. Automation Tasks - Manage

Подробное описание

Привилегия позволяет:

- Управлять заданиями автоматизации (Управление доменом/Каталог заданий автоматизации): создавать, редактировать, удалять.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Каталог заданий автоматизации

3.22.1.25. Kerberos Services - Read

Подробное описание

Привилегия позволяет:

- Видеть список служб Kerberos (Управление доменом/Службы и параметры Kerberos/вкладка Службы);
- Видеть карточки служб Kerberos (Управление доменом/Службы и параметры Kerberos/вкладка Службы/<Служба>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Службы и параметры Kerberos

3.22.1.26. Kerberos Services - Add

Подробное описание

Привилегия позволяет:

- Создавать новые службы Kerberos (Управление доменом/Службы и параметры Kerberos/вкладка Службы).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Службы и параметры Kerberos

3.22.1.27. Kerberos Services - Modify

Подробное описание

Привилегия позволяет:

- Изменять службы Kerberos (Управление доменом/Службы и параметры Kerberos/вкладка Службы/<Служба>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Службы и параметры Kerberos

3.22.1.28. Kerberos Services - Delete

Подробное описание

Привилегия позволяет:

- Удалять службы Kerberos (Управление доменом/Службы и параметры Kerberos/вкладка Службы/<Служба>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Службы и параметры Kerberos

3.22.1.29. Kerberos Configurations - Manage

Подробное описание

Привилегия позволяет:

- Управлять политикой билетов Kerberos (Управление доменом/Службы и параметры Kerberos/вкладка Политика билетов Kerberos): редактировать.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Службы и параметры Kerberos

3.22.1.30. Users and Groups Settings - Read

Подробное описание

Привилегия позволяет:

- Видеть список параметров пользователей (Управление доменом/Пользователи и группы/вкладка Параметры пользователей);
- Видеть список параметров групп (Управление доменом/Пользователи и группы/вкладка Параметры групп);
- Видеть список POSIX идентификаторов (Управление доменом/Пользователи и группы/вкладка POSIX идентификаторы);
- Видеть список атрибутов пользователей (Управление доменом/Пользователи и группы/вкладка Атрибуты пользователей);
- Видеть карточки атрибутов пользователей (Управление доменом/Пользователи и группы/вкладка Атрибуты пользователей/<Атрибут пользователей>).

Вместе с Users - Read позволяет:

- Видеть список дополнительных параметров пользователей (Пользователи компьютеры/Пользователи/<Пользователь>/вкладка Дополнительные сведения).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Пользователи и группы

3.22.1.31. Users and Groups Settings - Manage

Подробное описание

Привилегия позволяет:

- Управлять параметрами пользователей (Управление доменом/Пользователи и группы/вкладка Параметры пользователей): редактировать;
- Управлять параметрами групп (Управление доменом/Пользователи и группы/вкладка Параметры групп): добавлять, удалять;
- Управлять диапазонами POSIX идентификаторов (Управление доменом/Пользователи и группы/вкладка POSIX идентификаторы): создавать, удалять;
- Управлять атрибутами пользователей (Управление доменом/Пользователи и группы/вкладка Атрибуты пользователей): создавать, удалять.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Пользователи и группы

3.22.1.32. Domain Integrations - Manage

Подробное описание

Совместно с членством в группах trust admins и ald trust admin привилегия позволяет:

- Видеть список доверительных отношений (Управление доменами/Интеграция с доменами/вкладка Доверительные отношения);
- Видеть список миграций с MS AD (Управление доменами/Интеграция с доменами/вкладка Миграции с MS AD);
- Управлять записями в LDAP связанными с доверительными отношениями и миграциями: создавать, редактировать, удалять;
- Управлять миграциями с MS AD и доверительными отношениями (Управление доменами/Интеграция с доменами/вкладка Доверительные отношения): создавать, удалять.

Для выполнения корректной миграции требуются привилегии Organization Units - Add, Organization Units - Delete, Organization Units - Modify, Organization Units - Read, User groups

- Add, User groups - Delete, User groups - Modify, User groups - Read, Users - Modify, Users - Add, Users - Move to trash, Users - Delete from trash, Users - Read.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Интеграция с доменами

3.22.1.33. Roles - Read

Подробное описание

Привилегия позволяет:

- Видеть список ролей (Управление доменом/Роли и права доступа);
- Видеть карточки ролей (Управление доменом/Роли и права доступа/<Роль>);
- Видеть роли пользователя в карточке пользователя (Пользователи и компьютеры/Пользователи/<Пользователь>/вкладка Роли);
- Видеть роли группы пользователей в карточке группы пользователей (Пользователи и компьютеры/Группы пользователей/<Группа пользователей>/вкладка Роли).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Роли и права доступа

3.22.1.34. Roles - Add

Подробное описание

Привилегия позволяет:

- Создавать и копировать роли (Управление доменом/Роли и права доступа).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Роли и права доступа

3.22.1.35. Roles - Modify

Подробное описание

Привилегия позволяет:

- Изменять описание роли и ее состояние (Управление доменом/Роли и права доступа/<Роль>/вкладка Основное).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Роли и права доступа

3.22.1.36. Roles Membership - Manage

Подробное описание

Привилегия позволяет:

- Управлять назначением ролей на пользователей и группы пользователей (Управление доменом/Роли и права доступа/<Роль>/вкладка Пользователи): добавлять, удалять;
- Управлять назначением ролей на пользователей (Пользователи и компьютеры/Пользователи/<Пользователь>/вкладка Роли): добавлять, удалять;
- Управлять назначением ролей на группы пользователей (Пользователи и компьютеры/Группы пользователей/<Группа пользователей>/вкладка Роли): добавлять, удалять.

Внимание: Важно использовать привилегию **Roles Membership - Manage** с осторожностью. Пользователь, на которого назначена роль, привязанная к корневому подразделению домена с установленным признаком **Включая дочерние подразделения**, в составе которой есть данная привилегия, получает возможность как назначать любые роли на любого пользователя, получая таким образом возможность назначить набор ролей, аналогичный роли **ALDPRO - Main Administrator**, так и снимать назначение уже назначенных ролей с любых пользователей домена, что приведет к лишению этих пользователей имеющихся у них привилегий.

Вместе с User groups - Set group membership позволяет:

- Управлять составом пользователей в группе пользователей (Пользователи и компьютеры/Группы пользователей/<Группа пользователей>/вкладка Пользователи): добавлять, удалять;
- Управлять составом групп пользователей в группе пользователей (Пользователи и компьютеры/Группы пользователей/<Группа пользователей>/вкладка Группы): добавлять, удалять.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Роли и права доступа

3.22.1.37. Roles - Delete

Подробное описание

Привилегия позволяет:

- Удалять роли (Управление доменом/Роли и права доступа/<Роль>/вкладка Основное).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Роли и права доступа

3.22.1.38. Role Privileges - Add

Подробное описание

Привилегия позволяет:

- Добавлять привилегии в состав роли (Управление доменом/Роли и права доступа/<Роль>/вкладка Привилегии).

Для корректной работы роль, включающая в себя данную привилегию, должна

распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Роли и права доступа

3.22.1.39. Role Privileges - Modify

Подробное описание

Привилегия позволяет:

- Изменять сайт для привилегий, у которых есть ограничение по сайту (Управление доменом/Роли и права доступа/<Роль>/вкладка Привилегии/<Привилегия>).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Роли и права доступа

3.22.1.40. Role Privileges - Delete

Подробное описание

Привилегия позволяет:

- Удалять привилегии из состава роли (Управление доменом/Роли и права доступа/<Роль>/вкладка Привилегии/<Привилегия>).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Управление доменом:

- Роли и права доступа

3.22.1.41. Organization Units - Add

Подробное описание

Привилегия позволяет:

- Создавать новые подразделения (Пользователи и компьютеры/Организационная структура/<Подразделение>).

Для корректной работы роль, в которой состоит данная привилегия, должна распространяться на подразделение, которое указывается родительским.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Организационная структура

3.22.1.42. Organization Units - Delete

Подробное описание

Привилегия позволяет:

- Удалять подразделения (Пользователи и компьютеры/Организационная структура/<Подразделение>/вкладка Основное).

Для корректной работы роль, в которой состоит данная привилегия, должна распространяться на удаляемое подразделение.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Организационная структура

3.22.1.43. Organization Units - Modify

Подробное описание

Привилегия позволяет:

- Изменять параметры подразделений (Пользователи и компьютеры/Организационная структура/<Подразделение>/вкладка Основное).

Для корректной работы роль, в которой состоит данная привилегия, должна распространяться на изменяемое подразделение.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Организационная структура

3.22.1.44. Organization Units - Read

Подробное описание

Привилегия позволяет:

- Видеть дерево подразделений (Пользователи и компьютеры/Организационная структура);
- Видеть карточки подразделений (Пользователи и компьютеры/Организационная структура/<Подразделение>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Организационная структура

3.22.1.45. Users Password - Modify

Подробное описание

Привилегия позволяет:

- Сбрасывать пароль для пользователя (Пользователи и компьютеры/Пользователи/<Пользователь>/вкладка Основное).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Пользователи

3.22.1.46. Users Block - Modify

Подробное описание

Привилегия позволяет:

- Блокировать и разблокировать пользователя (Пользователи и компьютеры/Пользователи).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Пользователи

3.22.1.47. Users - Add

Подробное описание

Привилегия позволяет:

- Создавать новых пользователей (Пользователи и компьютеры/Пользователи).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Пользователи

3.22.1.48. Users - Modify

Подробное описание

Привилегия позволяет:

- Изменять пользователей (кроме выбора подразделения) (Пользователи и компьютеры/Пользователи/<Пользователь>).

Вместе с Users and Groups Settings - Read позволяет:

- Изменять дополнительные параметры пользователя (Пользователи компьютеры/Пользователи/<Пользователь>/вкладка Дополнительные сведения).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Пользователи

3.22.1.49. Users - Read

Подробное описание

Привилегия позволяет:

- Видеть список пользователей (Пользователи и компьютеры/Пользователи);
- Видеть карточки пользователей (Пользователи и компьютеры/Пользователи/<Пользователь>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Пользователи

3.22.1.50. Users - Set organization unit

Подробное описание

Привилегия позволяет:

- Управлять составом пользователей в подразделениях (Пользователи и компьютеры/Пользователи/<Пользователь>/вкладка Основное);
- Управлять составом пользователей в подразделениях (Пользователи и компьютеры/Организационная структура/<Подразделение>/вкладка Пользователи).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Пользователи
- Пользователи и компьютеры:
  - Организационная структура

3.22.1.51. Users - Move to trash

Подробное описание

Привилегия позволяет:

- Перемещать пользователей в корзину (Пользователи и компьютеры/Пользователи/<Пользователь>).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Пользователи
- Пользователи и компьютеры:
  - Корзина

3.22.1.52. Users - Return from trash

Подробное описание

Привилегия позволяет:

- Восстанавливать пользователей из корзины (Пользователи и компьютеры/Корзина).

Для корректной работы роль, в которой состоит данная привилегия, должна распространяться на корневое подразделение.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Корзина
- Пользователи и компьютеры:
  - Пользователи

3.22.1.53. Users - Delete from trash

Подробное описание

Привилегия позволяет:

- Окончательно удалять пользователей из корзины.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Корзина

3.22.1.54. Users - Read trash

Подробное описание

Привилегия позволяет:

- Видеть список пользователей в корзине (Пользователи и компьютеры/Корзина);
- Видеть карточки пользователей в корзине (Пользователи и компьютеры/Корзина/<Пользователь>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Корзина

3.22.1.55. User groups - Add

Подробное описание

Привилегия позволяет:

- Создавать новые группы пользователей (Пользователи и компьютеры/Группы пользователей).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Группы пользователей

3.22.1.56. User groups - Delete

Подробное описание

Привилегия позволяет:

- Удалять группы пользователей (Пользователи и компьютеры/Группы пользователей/<Группа пользователей>).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Группы пользователей

3.22.1.57. User groups - Modify

Подробное описание

Привилегия позволяет:

- Изменять параметры групп пользователей (кроме выбора подразделения) (Пользователи и компьютеры/Группы пользователей/<Группа пользователей>/вкладка Основное).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Группы пользователей

3.22.1.58. User groups - Read

Подробное описание

Привилегия позволяет:

- Видеть список групп пользователей (Пользователи и компьютеры/Группы пользователей);
- Видеть карточки групп пользователей (Пользователи и компьютеры/Группы пользователей/<Группа пользователей>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Группы пользователей

3.22.1.59. User groups - Set group membership

Подробное описание

Привилегия позволяет:

- Управлять составом пользователей в группе пользователей (Пользователи и компьютеры/Группы пользователей/<Группа пользователей>/вкладка Пользователи и Пользователи и компьютеры/Пользователи/<Пользователь>/Группы);
- Управлять составом групп пользователей в группе пользователей (Пользователи и компьютеры/Группы пользователей/<Группа пользователей>/вкладка Группы).

Для управления составом групп, на которые назначены роли требуется дополнительная привилегия Roles Membership - Manage.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Группы пользователей
- Пользователи и компьютеры:
  - Пользователи

3.22.1.60. User groups - Set organization unit

Подробное описание

Привилегия позволяет:

- Управлять составом групп пользователей в подразделениях (Пользователи и компьютеры/Группы пользователей/<Группа пользователей>/вкладка Основное);
- Управлять составом групп пользователей в подразделениях (Пользователи и компьютеры/Организационная структура/<Подразделение>/вкладка Пользователи).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Группы пользователей
- Пользователи и компьютеры:
  - Организационная структура

3.22.1.61. Computers - Delete

Подробное описание

Привилегия позволяет:

- Удалять компьютеры (Пользователи и компьютеры/Компьютеры и Пользователи и компьютеры/Компьютеры/<Компьютер>/вкладка Основное).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Компьютеры

3.22.1.62. Computers - Modify

Подробное описание

Привилегия позволяет:

- Изменять параметры компьютеров (Пользователи и компьютеры/Компьютеры/<Компьютер> вкладки Основное (кроме выбора подразделения), Группы).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Компьютеры

3.22.1.63. Computers - Read

Подробное описание

Привилегия позволяет:

- Видеть список компьютеров (Пользователи и компьютеры/Компьютеры);
- Видеть карточки компьютера (Пользователи и компьютеры/Компьютеры/<Компьютер>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Компьютеры

3.22.1.64. Computers - Remote access

Подробное описание

Привилегия позволяет:

- Осуществлять удаленный доступ к компьютеру (Пользователи и компьютеры/Компьютеры/<Компьютер>/Удаленный доступ).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Компьютеры

3.22.1.65. Computers - Set organization unit

Подробное описание

Привилегия позволяет:

- Управлять составом компьютеров в подразделениях (Пользователи и компьютеры/Компьютеры/<Компьютер>/вкладка Основное или Пользователи и компьютеры/Организационная структура/<Подразделение>/вкладка Компьютеры).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Компьютеры
- Пользователи и компьютеры:

– Организационная структура

3.22.1.66. Computer groups - Add

Подробное описание

Привилегия позволяет:

- Создавать новые группы компьютеров (Пользователи и компьютеры/Группы компьютеров).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

ривилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Группы компьютеров

3.22.1.67. Computer groups - Delete

Подробное описание

Привилегия позволяет:

- Удалять группы компьютеров (Пользователи и компьютеры/Группы компьютеров/<Группа компьютеров>/вкладка Основное).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Группы компьютеров

3.22.1.68. Computer groups - Modify

Подробное описание

Привилегия позволяет:

- Изменять параметры группы компьютеров (кроме выбора подразделения) (Пользователи и компьютеры/Группы компьютеров/<Группа компьютеров>/вкладка Основное).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Группы компьютеров

3.22.1.69. Computer groups - Read

Подробное описание

Привилегия позволяет:

- Видеть список групп компьютеров (Пользователи и компьютеры/Группы компьютеров);
- Видеть карточки групп компьютеров (Пользователи и компьютеры/Группы компьютеров/<Группа компьютеров>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Пользователи и компьютеры:

- Группы компьютеров

3.22.1.70. Computer groups - Set group membership

Подробное описание

Привилегия позволяет:

- Управлять составом компьютеров в группе компьютеров (Пользователи и компьютеры/Группы компьютеров/<Группа компьютеров>/вкладка Компьютеры);
- Управлять составом групп компьютеров в группе компьютеров (Пользователи и компьютеры/Группы компьютеров/<Группа компьютеров>/вкладка Группы).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к

которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Группы компьютеров
- Пользователи и компьютеры:
  - Компьютеры

3.22.1.71. Computer groups - Set organization unit

Подробное описание

Привилегия позволяет:

- Управлять составом групп компьютеров в подразделениях (Пользователи и компьютеры/Группы компьютеров/<Группа компьютеров>/вкладка Основное или Пользователи и компьютеры/Организационная структура/<Подразделение>/вкладка Компьютеры).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

- Пользователи и компьютеры:
  - Группы компьютеров
- Пользователи и компьютеры:
  - Организационная структура

3.22.1.72. Group Policies - Read

Подробное описание

Привилегия позволяет:

- Видеть список групповых политик (Групповые политики/Групповые политики);
- Видеть карточки групповых политик (Групповые политики/Групповые политики/<Групповая политика>).

Вместе с привилегией Organizational Units - Read позволяет:

- Видеть список групповых политик в карточке подразделения (Пользователи и компьютеры/Организационная структура/<Подразделение>/вкладка Групповые политики);
- Видеть карточки групповых политик в карточке подразделения (Пользователи и компьютеры/Организационная структура/<Подразделение>/вкладка Групповые политики/<Групповая политика>).

Вместе с привилегией Users - Read позволяет:

- Видеть список групповых политик в карточке пользователя (Пользователи и компьютеры/Пользователи/<Пользователь>/вкладка Групповые политики).

Вместе с привилегией Computers - Read позволяет:

- Видеть список групповых политик в карточке компьютера (Пользователи и компьютеры/Компьютеры/<Компьютер>/вкладка Групповые политики).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Групповые политики

3.22.1.73. Group Policies - Add

Подробное описание

Привилегия позволяет:

- Создавать новые групповые политики (Групповые политики/Групповые политики).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Групповые политики

3.22.1.74. Group Policies - Modify

Подробное описание

Привилегия позволяет:

- Изменять групповые политики (Групповые политики/Групповые политики/<Групповая

политика>/вкладка Основное).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Групповые политики

3.22.1.75. Group Policies - Delete

Подробное описание

Привилегия позволяет:

- Удалять групповые политики (Групповые политики/Групповые политики/<Групповая политика>/вкладка Основное).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Групповые политики

3.22.1.76. Group Policies Computer Parameters - Manage

Подробное описание

Привилегия позволяет:

- Управлять значениями параметров компьютеров (Групповые политики/Групповые политики/<Групповая политика>/вкладка Параметры компьютеров): редактировать, удалять;
- Управлять конфигурациями с типом «Компьютеры» (Групповые политики/Групповые политики/<Групповая политика>/вкладка Конфигурация политики): редактировать, удалять.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Групповые политики

3.22.1.77. Group Policies User Parameters - Manage

Подробное описание

Привилегия позволяет:

- Управлять значениями параметров пользователей (Групповые политики/Групповые политики/<Групповая политика>/вкладка Параметры пользователей): редактировать;
- Управлять конфигурациями с типом «Пользователи» (Групповые политики/Групповые политики/<Групповая политика>/вкладка Конфигурация политики): редактировать, удалять.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Групповые политики

3.22.1.78. Group Policies Membership - Manage

Подробное описание

Привилегия позволяет:

- Управлять политиками для подразделений (Групповые политики/Групповые политики/<Групповая политика>/вкладка Подразделения): добавлять, удалять;

Управлять политиками для подразделений (Пользователи и компьютеры/Организационная структура/<Подразделение>/вкладка Групповые политики): добавлять, удалять, изменять приоритет.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделения, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Групповые политики

3.22.1.79. HBAC - Read

Подробное описание

Привилегия позволяет:

- Видеть список правил HBAC (Групповые политики/Политики доступа к узлу/вкладка Правила HBAC);
- Видеть список служб HBAC (Групповые политики/Политики доступа к узлу/вкладка Службы HBAC);
- Видеть список групп служб HBAC (Групповые политики/Политики доступа к узлу/вкладка Группы служб HBAC);
- Видеть карточки правил HBAC (Групповые политики/Политики доступа к узлу/вкладка Правила HBAC/<Правило HBAC>);
- Видеть карточки служб HBAC (Групповые политики/Политики доступа к узлу/вкладка Службы HBAC/<Служба HBAC>);
- Видеть карточки групп служб HBAC (Групповые политики/Политики доступа к узлу/вкладка Группы служб HBAC/<Группа служб HBAC>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики доступа к узлу

3.22.1.80. HBAC Rules - Add

Подробное описание

Привилегия позволяет:

- Создавать новые правила HBAC (Групповые политики/Политики доступа к узлу/вкладка Правила HBAC).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики доступа к узлу

3.22.1.81. HBAC Rules - Modify

Подробное описание

Привилегия позволяет:

- Изменять правила HBAC (Групповые политики/Политики доступа к узлу/вкладка Правила HBAC/<Правило HBAC>).

Для корректной работы роль, включающая в себя данную привилегию, должна

распространяться на подразделение, в состав которого входят пользователи и компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики доступа к узлу

3.22.1.82. HBAC Rules - Delete

Подробное описание

Привилегия позволяет:

- Удалять правила HBAC (Групповые политики/Политики доступа к узлу/вкладка Правила HBAC/<Правило HBAC>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики доступа к узлу

3.22.1.83. HBAC Services - Add

Подробное описание

Привилегия позволяет:

- Создавать новые службы HBAC (Групповые политики/Политики доступа к узлу/вкладка Службы HBAC).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики доступа к узлу

3.22.1.84. HBAC Services - Modify

Подробное описание

Привилегия позволяет:

- Изменять службы HBAC (Групповые политики/Политики доступа к узлу/вкладка Правила HBAC/<Служба HBAC>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики доступа к узлу

3.22.1.85. HBAC Services - Delete

Подробное описание

Привилегия позволяет:

- Удалять службы HBAC (Групповые политики/Политики доступа к узлу/вкладка Правила HBAC/<Служба HBAC>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики доступа к узлу

3.22.1.86. HBAC Service Groups - Add

Подробное описание

Привилегия позволяет:

- Создавать новые группы служб HBAC (Групповые политики/Политики доступа к узлу/вкладка Группы служб HBAC).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики доступа к узлу

3.22.1.87. HBAC Service Groups - Modify

Подробное описание

Привилегия позволяет:

- Изменять группы служб HBAC (Групповые политики/Политики доступа к узлу/вкладка Группы служб HBAC/<Группа служб HBAC>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики доступа к узлу

3.22.1.88. HBAC Service Groups - Delete

Подробное описание

Привилегия позволяет:

- Удалять группы служб HBAC (Групповые политики/Политики доступа к узлу/вкладка Группы служб HBAC/<Группа служб HBAC>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики доступа к узлу

3.22.1.89. SUDO - Read

Подробное описание

Привилегия позволяет:

- Видеть список правил SUDO (Групповые политики/Политики повышения привилегий/вкладка Правила SUDO);
- Видеть список команд SUDO (Групповые политики/Политики повышения привилегий/вкладка Команды SUDO);

- Видеть список групп команд SUDO (Групповые политики/Политики повышения привилегий/вкладка Группы команд SUDO);
- Видеть карточки правил SUDO (Групповые политики/Политики повышения привилегий/вкладка Правила SUDO/<Правило SUDO>);
- Видеть карточки команд SUDO (Групповые политики/Политики повышения привилегий/вкладка Команды SUDO/<Команда SUDO>);
- Видеть карточки групп команд SUDO (Групповые политики/Политики повышения привилегий/вкладка Группы команд SUDO/<Группа команд SUDO>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики повышения привилегий

3.22.1.90. SUDO Rules - Add

Подробное описание

Привилегия позволяет:

- Создавать новые правила SUDO (Групповые политики/Политики повышения привилегий/вкладка Правила SUDO).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики повышения привилегий

3.22.1.91. SUDO Rules - Modify

Подробное описание

Привилегия позволяет:

- Изменять правила SUDO, кроме вкладки Параметры (Групповые политики/Политики повышения привилегий/вкладка Правила SUDO/<Правило SUDO>).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят пользователи и компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики повышения привилегий

3.22.1.92. SUDO Parameters - Manage

Подробное описание

Привилегия позволяет:

- Управлять параметрами SUDO для правил SUDO (Групповые политики/Политики повышения привилегий/вкладка Правила SUDO/<Правило SUDO>/вкладка Параметры): создавать, удалять.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики повышения привилегий

3.22.1.93. SUDO Rules - Delete

Подробное описание

Привилегия позволяет:

- Удалять правила SUDO (Групповые политики/Политики повышения привилегий/вкладка Правила SUDO/<Правило SUDO>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики повышения привилегий

3.22.1.94. SUDO Commands - Add

Подробное описание

Привилегия позволяет:

- Создавать новые команды SUDO (Групповые политики/Политики повышения привилегий/вкладка Команды SUDO).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики повышения привилегий

3.22.1.95. SUDO Commands - Modify

Подробное описание

Привилегия позволяет:

- Изменять команды SUDO (Групповые политики/Политики повышения привилегий/вкладка Команды SUDO/<Команда SUDO>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики повышения привилегий

3.22.1.96. SUDO Commands - Delete

Подробное описание

Привилегия позволяет:

- Удалять команды SUDO (Групповые политики/Политики повышения привилегий/вкладка Команды SUDO/<Команда SUDO>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики повышения привилегий

3.22.1.97. SUDO Command Groups - Add

Подробное описание

Привилегия позволяет:

- Создавать новые группы команд SUDO (Групповые политики/Политики повышения привилегий/вкладка Группы команд SUDO).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики повышения привилегий

3.22.1.98. SUDO Command Groups - Modify

Подробное описание

Привилегия позволяет:

- Изменять группы команд SUDO (Групповые политики/Политики повышения привилегий/вкладка Группы команд SUDO/<Группа команд SUDO>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики повышения привилегий

3.22.1.99. SUDO Command Groups - Delete

Подробное описание

Привилегия позволяет:

- Удалять группы команд SUDO (Групповые политики/Политики повышения привилегий/вкладка Группы команд SUDO/<Группа команд SUDO>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики повышения привилегий

3.22.1.100. Password Policies - Read

Подробное описание

Привилегия позволяет:

- Видеть список политик паролей (Групповые политики/Политики паролей);
- Видеть карточки политик паролей (Групповые политики/Политики паролей/<Политика паролей>);
- Видеть список запрещенных слов (Групповые политики/Политики паролей/Список запрещенных слов);
- Скачать содержимое текстового поля списка запрещенных слов в локальный текстовый файл;
- Видеть список запрещенных слов (Групповые политики/Политики паролей/Список запрещенных слов);
- Скачать содержимое текстового поля списка запрещенных слов в локальный текстовый файл.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики паролей

3.22.1.101. Password Policies - Add

Подробное описание

Привилегия позволяет:

- Создавать новые политики паролей (Групповые политики/Политики паролей).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики паролей

3.22.1.102. Password Policies - Modify

Подробное описание

Привилегия позволяет:

- Изменять политики паролей (Групповые политики/Политики паролей/<Политика паролей>);
- Изменять содержимое источника списка запрещенных слов (Групповые политики/Политики паролей/Список запрещенных слов).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики паролей

3.22.1.103. Password Policies - Delete

Подробное описание

Привилегия позволяет:

- Удалять политики паролей (Групповые политики/Политики паролей/<Политика паролей>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Групповые политики:

- Политики паролей

3.22.1.104. Software Policies - Read

Подробное описание

Привилегия позволяет:

- Видеть список политик ПО (Установка и обновление ПО/Политики ПО);
- Видеть карточки политик ПО (Установка и обновление ПО/Политики ПО/<Политика ПО>).

Вместе с привилегией Organizational Units - Read позволяет:

- Видеть параметры ПО в подразделениях (Пользователи и

компьютеры/Организационная структура/<Подразделение>/вкладка Политики ПО).

Вместе с привилегией Computers - Read позволяет:

- Видеть параметры ПО в карточке компьютера (Пользователи и компьютеры/Компьютеры/<Компьютер>/вкладка Назначение ПО).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Политики ПО

3.22.1.105. Software Policies - Add

Подробное описание

Привилегия позволяет:

- Создавать новые политики ПО (Установка и обновление ПО/Политики ПО).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Политики ПО

3.22.1.106. Software Policies - Modify

Подробное описание

Привилегия позволяет:

- Изменять политики ПО (Установка и обновление ПО/Политики ПО/<Политика ПО>/вкладка Основное).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Политики ПО

3.22.1.107. Software Policies - Delete

Подробное описание

Привилегия позволяет:

- Удалять политики ПО (Установка и обновление ПО/Политики ПО/<Политика ПО>/вкладка Основное);
- Удалять ПО из политики ПО (Установка и обновление ПО/Политики ПО/<Политика ПО>/вкладка Конфигурация политики);
- Удалять подразделения из политики ПО (Установка и обновление ПО/Политики ПО/<Политика ПО>/Вкладка Подразделения).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Политики ПО

3.22.1.108. Software Policies Configurations - Manage

Подробное описание

Привилегия позволяет:

- Добавлять ПО в политику ПО (Установка и обновление ПО/Политики ПО/<Политика ПО>/вкладка Каталог ПО);
- Удалять ПО из политики ПО (Установка и обновление ПО/Политики ПО/<Политика ПО>/вкладка Конфигурация политики).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Политики ПО

3.22.1.109. Software Policies Membership - Manage

Подробное описание

Привилегия позволяет:

- Управлять подразделениями из политиках ПО (Установка и обновление ПО/Политики ПО/<Политика ПО>/Вкладка Подразделения): добавлять, удалять;

- Управлять параметрами ПО в подразделениях (Пользователи и компьютеры/Организационная структура/<Подразделение>/вкладка Политики ПО): добавлять, удалять, изменять приоритет параметра;
- Управлять параметрами ПО в карточке компьютера (Пользователи и компьютеры/Компьютеры/<Компьютер>/вкладка Назначение ПО): редактировать.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Политики ПО

3.22.1.110. Software Catalog - Read

Подробное описание

Привилегия позволяет:

- Видеть список программного обеспечения, пакетов и разделов (групп) ПО (Установка и обновление ПО/ Каталог ПО/вкладка Каталог ПО);
- Видеть карточки разделов (групп) ПО (Установка и обновление ПО/ Каталог ПО/вкладка Каталог ПО/<Группа ПО>);
- Видеть карточки записей ПО (Установка и обновление ПО/ Каталог ПО/вкладка Каталог ПО/<ПО>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Каталог ПО

3.22.1.111. Software Packages - Manage

Подробное описание

Привилегия позволяет:

- Управлять пакетами ПО (Установка и обновление ПО/ Каталог ПО/вкладка Каталог ПО/<ПО>/вкладка Пакеты): просматривать, создавать, удалять.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Каталог ПО

3.22.1.112. Software Templates - Manage

Подробное описание

Привилегия позволяет:

- Управлять шаблонами конфигурации ПО (Установка и обновление ПО/ Каталог ПО/вкладка Каталог ПО/<ПО>/вкладка Шаблоны конфигурации): просматривать, создавать, редактировать, удалять.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Каталог ПО

3.22.1.113. Software Parameters - Manage

Подробное описание

Привилегия позволяет:

- Управлять параметрами ПО (Установка и обновление ПО/ Каталог ПО/вкладка Каталог ПО/<ПО>/вкладка Параметры): просматривать, создавать, редактировать, удалять.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Каталог ПО

3.22.1.114. Software Groups - Manage

Подробное описание

Привилегия позволяет:

- Управлять разделами (группами) ПО (Установка и обновление ПО/ Каталог ПО/вкладка Каталог ПО): создавать, редактировать, удалять.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Каталог ПО

3.22.1.115. Software - Manage

Подробное описание

Привилегия позволяет:

- Управлять ПО (Установка и обновление ПО/ Каталог ПО/вкладка Каталог ПО): создавать, редактировать, удалять.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Каталог ПО

3.22.1.116. Repositories - Add

Подробное описание

Привилегия позволяет:

- Создавать новые репозитории ПО (Установка и обновление ПО/ Репозитории ПО/ вкладка Репозитории ПО).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Репозитории ПО

3.22.1.117. Repositories - Read

Подробное описание

Привилегия позволяет:

- Видеть список репозиториев ПО (Установка и обновление ПО/ Репозитории ПО/ вкладка Репозитории ПО);
- Видеть карточки репозиториев ПО (Установка и обновление ПО/ Репозитории ПО/ вкладка Репозитории ПО/ <Репозиторий> вкладка Основное).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Репозитории ПО

3.22.1.118. Repositories - Modify

Подробное описание

Привилегия позволяет:

- Изменять параметры репозитория ПО (Установка и обновление ПО/ Репозитории ПО/ вкладка Репозитории ПО/ <Репозиторий> вкладка Основное).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Репозитории ПО

3.22.1.119. Repositories - Delete

Подробное описание

Привилегия позволяет:

- Удалять репозитории ПО (Установка и обновление ПО/ Репозитории ПО/ вкладка Репозитории ПО/ <Репозиторий> вкладка Основное).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Репозитории ПО

3.22.1.120. Repository Servers - Create

Подробное описание

Привилегия позволяет:

- Создавать новые серверы репозиториев ПО (Установка и обновление ПО/ Репозитории ПО/ вкладка Серверы репозиториев ПО) на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Репозитории ПО

3.22.1.121. Repository Servers - Read

Подробное описание

Привилегия позволяет:

- Видеть список серверов репозиториев ПО (Установка и обновление ПО/ Репозитории ПО/ вкладка Серверы репозиториев ПО);
- Видеть карточки серверов репозиториев ПО (Установка и обновление ПО/ Репозитории ПО/ вкладка Серверы репозиториев ПО/<Сервер репозиториев ПО>);
- Видеть журнал изменений (Установка и обновление ПО/ Репозитории ПО/ вкладка Серверы репозиториев ПО/<Сервер репозиториев ПО>/Журнал истории изменений).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Репозитории ПО

3.22.1.122. Repository Servers - Modify

Подробное описание

Привилегия позволяет:

- Изменять любой сайт основного сервера репозиториев ПО(Установка и обновление

ПО/ Репозитории ПО/ вкладка Серверы репозиториев ПО/<Сервер репозиториев ПО> вкладка Основное) на указанный в привилегии;

- Обновлять серверы репозиториев ПО на указанном сайте (Установка и обновление ПО/ Репозитории ПО/ вкладка Серверы репозиториев ПО/<Сервер репозиториев ПО> вкладка Основное/кнопка «Обновить ALD Pro»).

Смена сайта для резервного сервера репозиториев ПО недоступна.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Репозитории ПО

3.22.1.123. Repository Servers - Drop

Подробное описание

Привилегия позволяет:

- Удалять серверы репозиториев ПО (Установка и обновление ПО/ Репозитории ПО/ вкладка Серверы репозиториев ПО/<Сервер репозиториев ПО> вкладка Основное) на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Репозитории ПО

3.22.1.124. Update Policies - Read

Подробное описание

Привилегия позволяет:

- Видеть список политик обновления ALD Pro (Установка и обновление ПО/Политики обновления ALD Pro);
- Видеть карточки политик обновления ALD Pro (Установка и обновление ПО/Политики обновления ALD Pro/<Политика обновления ALD Pro>).

Вместе с привилегией Computer groups - Read позволяет:

- Видеть список политик обновления ALD Pro в карточке группы компьютеров (Пользователи и компьютеры/Группы компьютеров /<Группа компьютеров>/вкладка Политики обновления).

Вместе с привилегией Computers - Read позволяет:

- Видеть список политик обновления ALD Pro в карточке компьютера (Пользователи и компьютеры/Компьютеры/<Компьютер>/вкладка Политики обновления).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Политики обновления ALD Pro

3.22.1.125. Update Policies - Add

Подробное описание

Привилегия позволяет:

- Создавать новые политики обновления ALD Pro (Установка и обновление ПО/Политики обновления ALD Pro).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Политики обновления ALD Pro

3.22.1.126. Update Policies - Modify

Подробное описание

Привилегия позволяет:

- Редактировать политики обновления ALD Pro (Установка и обновление ПО/Политики обновления ALD Pro/<Политика обновления ALD Pro>/вкладка Основное).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Политики обновления ALD Pro

3.22.1.127. Update Policies - Delete

Подробное описание

Привилегия позволяет:

- Удалять политики обновления ALD Pro (Установка и обновление ПО/Политики обновления ALD Pro/<Политика обновления ALD Pro>/вкладка Основное).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Политики обновления ALD Pro

3.22.1.128. Update Policies Sources list - Manage

Подробное описание

Привилегия позволяет:

- Управлять конфигурацией Sources list в политике обновления ALD Pro (Установка и обновление ПО/Политики обновления ALD Pro/<Политика обновления ALD Pro>/вкладка Sources list): редактировать.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Политики обновления ALD Pro

3.22.1.129. Update Policies Computers - Manage

Подробное описание

Привилегия позволяет:

- Управлять составом компьютеров и групп компьютеров в политиках обновления ALD Pro (Установка и обновление ПО/Политики обновления ALD Pro/<Политика обновления ALD Pro>/вкладка Компьютеры): добавлять, удалять.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Политики обновления ALD Pro

3.22.1.130. Automation Tasks Journal - Read

Подробное описание

Привилегия позволяет:

- Видеть список заданий автоматизации в журнале заданий (Автоматизация/Задания автоматизации/вкладка Журнал заданий);
- Видеть карточки заданий автоматизации в журнале заданий (Автоматизация/Задания автоматизации/вкладка Журнал заданий<Отчет о задании>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Автоматизация:

- Задания автоматизации

3.22.1.131. Automation Tasks Membership - Manage

Подробное описание

Привилегия позволяет:

- Запускать задания автоматизации (Автоматизация/Задания автоматизации/вкладка Каталог заданий автоматизации).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Автоматизация:

- Задания автоматизации

3.22.1.132. Installation Servers - Create

Подробное описание

Привилегия позволяет:

- Создавать новые серверы установки ОС по сети (Автоматизация/Установка ОС по сети) на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Автоматизация:

- Установка ОС по сети

3.22.1.133. Installation Servers - Modify

Подробное описание

Привилегия позволяет:

- Изменять используемый DHCP-сервер и любой сайт сервера установки ОС по сети (Автоматизация/Установка ОС по сети/<Сервер установки ОС по сети> вкладка Основное) на указанный в привилегии;
- Обновлять сервер установки ОС по сети на указанном сайте (Автоматизация/Установка ОС по сети/<Сервер установки ОС по сети> вкладка Основное/кнопка «Обновить ALD Pro»).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Автоматизация:

- Установка ОС по сети

3.22.1.134. Installation Servers - Drop

Подробное описание

Привилегия позволяет :

- Удалять серверы установки ОС по сети (Автоматизация/Установка ОС по сети) на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Автоматизация:

- Установка ОС по сети

3.22.1.135. Installation Servers - Read

Подробное описание

Привилегия позволяет:

- Видеть список серверов установки ОС по сети (Автоматизация/Установка ОС по сети/вкладка Серверы установки ОС по сети);
- Видеть карточки серверов установки ОС по сети (Автоматизация/Установка ОС по сети/вкладка Серверы установки ОС по сети/<Сервер установки ОС по сети> вкладка Основное);
- Видеть перечень компьютеров (Автоматизация/Установка ОС по сети/вкладка Серверы установки ОС по сети/<Сервер установки ОС по сети> вкладка Перечень компьютеров);
- Видеть карточки компьютеров (Автоматизация/Установка ОС по сети/вкладка Серверы установки ОС по сети/<Сервер установки ОС по сети> вкладка Перечень компьютеров/ <компьютер>);
- Видеть список профилей загрузки (Автоматизация/Установка ОС по сети/вкладка Серверы установки ОС по сети/<Сервер установки ОС по сети> вкладка Профили загрузки);
- Видеть карточки профилей загрузки (Автоматизация/Установка ОС по сети/вкладка Серверы установки ОС по сети/<Сервер установки ОС по сети> вкладка Профили загрузки/ <Профиль загрузки>);
- Видеть журнал изменений (Автоматизация/Установка ОС по сети/вкладка Серверы установки ОС по сети/<Сервер установки ОС по сети> вкладка Основное/Журнал истории изменений).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Автоматизация:

- Установка ОС по сети

3.22.1.136. Installation Server Computers - Manage

Подробное описание

Привилегия позволяет:

- Управлять компьютерами для сервера установки ОС по сети (Автоматизация/Установка ОС по сети/<Сервер установки ОС по сети>/вкладка Перечень компьютеров): добавлять, удалять.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Автоматизация:

- Установка ОС по сети

3.22.1.137. Installation Server Profiles - Manage

Подробное описание

Привилегия позволяет:

- Управлять профилями загрузки для сервера установки ОС по сети (Автоматизация/Установка ОС по сети/<Сервер установки ОС по сети>/вкладка Профили загрузки): добавлять, редактировать, удалять.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Автоматизация:

- Установка ОС по сети

3.22.1.138. DNS Zones - Read

Подробное описание

Привилегия позволяет:

- Видеть список зон DNS (Роли и службы сайта/ Служба разрешения имен/ вкладка Зоны DNS);
- Видеть карточки зон DNS (Роли и службы сайта/ Служба разрешения имен/<Зона DNS>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба разрешения имён

3.22.1.139. DNS Zones - Manage

Подробное описание

Привилегия позволяет:

- Управлять зонами DNS (Роли и службы сайта/ Служба разрешения имен/<Зона DNS>): создавать, редактировать, удалять;
- Управлять записями ресурсов DNS (Роли и службы сайта/ Служба разрешения имен/<Зона DNS> вкладка Записи ресурсов DNS/ <Запись>): просматривать, добавлять, удалять, редактировать.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба разрешения имён

3.22.1.140. DNS Forward Zones - Read

Подробное описание

Привилегия позволяет:

- Видеть список перенаправлений запросов (Роли и службы сайта/ Служба разрешения имен/ вкладка Перенаправление запросов);
- Видеть карточки перенаправлений запросов (Роли и службы сайта/ Служба

разрешения имен/ вкладка Перенаправление запросов/ <Перенаправление запросов>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба разрешения имён

3.22.1.141. DNS Forward Zones - Modify

Подробное описание

Привилегия позволяет:

- Изменять перенаправления запросов (Роли и службы сайта/ Служба разрешения имен/ вкладка Перенаправление запросов/ <Перенаправление запросов>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба разрешения имён

3.22.1.142. DNS Forward Zones - Delete

Подробное описание

Привилегия позволяет:

- Удалять перенаправления запросов (Роли и службы сайта/ Служба разрешения имен/ вкладка Перенаправление запросов/ <Перенаправление запросов>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба разрешения имён

3.22.1.143. DNS Forward Zones - Add

Подробное описание

Привилегия позволяет:

- Создавать новые перенаправления запросов (Роли и службы сайта/ Служба разрешения имен/ вкладка Перенаправление запросов/ <Перенаправление запросов>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба разрешения имён

3.22.1.144. DNS Global Configurations - Manage

Подробное описание

Привилегия позволяет:

- Управлять глобальными конфигурациями DNS (Роли и службы сайта/ Служба разрешения имен/<Зона DNS> вкладка Глобальные конфигурации DNS): просматривать, добавлять, удалять, редактировать.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба разрешения имён

3.22.1.145. DHCP - Read

Подробное описание

Привилегия позволяет:

- Видеть список серверов динамической настройки узла (Роли и службы сайта/ Служба динамической настройки узла/вкладка Перечень серверов);
- Видеть карточки серверов динамической настройки узла (Роли и службы сайта/ Служба динамической настройки узла/вкладка Перечень серверов/<Сервер динамической настройки узла>);
- Видеть журнал изменений (Роли и службы сайта/ Служба динамической настройки узла/вкладка Перечень серверов/<Сервер динамической настройки узла>/Журнал

истории изменений).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба динамической настройки узла

3.22.1.146. DHCP Servers - Create

Подробное описание

Привилегия позволяет:

- Создавать новые серверы динамической настройки узла (Роли и службы сайта/ Служба динамической настройки узла/<Сервер динамической настройки узла> вкладка Основное) на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба динамической настройки узла

3.22.1.147. DHCP Servers - Modify

Подробное описание

Привилегия позволяет:

- Изменять любой сайт сервера динамической настройки узла (Роли и службы сайта/ Служба динамической настройки узла/<Сервер динамической настройки узла> вкладка Основное) на указанный в привилегии;
- Обновлять серверы динамической настройки узла на указанном сайте (Роли и службы сайта/ Служба динамической настройки узла/<Сервер динамической настройки узла> вкладка Основное/кнопка «Обновить ALD Pro»).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба динамической настройки узла

3.22.1.148. DHCP Configuration - Modify

Подробное описание

- Привилегия позволяет на сервере динамической настройки узла, расположенном на указанном сайте:
- Управлять конфигурациями скрипта и настройками сетевых интерфейсов (Роли и службы сайта/ Служба динамической настройки узла/<Сервер динамической настройки узла> вкладка Конфигурация скрипты и вкладка настройка сетевых интерфейсов): просматривать, добавлять, удалять, редактировать.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба динамической настройки узла

3.22.1.149. DHCP Servers - Drop

Подробное описание

Привилегия позволяет:

- Удалять серверы динамической настройки узла (Роли и службы сайта/ Служба динамической настройки узла/<Сервер динамической настройки узла> вкладка Основное) на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба динамической настройки узла

3.22.1.150. NTP Servers - Read

Подробное описание

Привилегия позволяет:

- Видеть список внешних NTP серверов (Роли и службы сайта/Служба синхронизации времени/вкладка Внешний пул NTP-серверов);
- Видеть список корневых NTP-серверов домена (Роли и службы сайта/Служба синхронизации времени/вкладка Корневые NTP-серверы домена).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба синхронизации времени

3.22.1.151. External NTP Servers - Create

Подробное описание

Привилегия позволяет:

- Добавлять новые внешние NTP-серверы (Роли и службы сайта/Служба синхронизации времени/вкладка Внешний пул NTP-серверов).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба синхронизации времени

3.22.1.152. Root NTP Servers - Create

Подробное описание

Привилегия позволяет:

- Создавать новые корневые NTP-серверы (Роли и службы сайта/Служба синхронизации времени/вкладка Корневые NTP-серверы домена).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба синхронизации времени

3.22.1.153. External NTP Servers - Drop

Подробное описание

Привилегия позволяет:

- Удалять внешние NTP-серверы (Роли и службы сайта/Служба синхронизации времени/вкладка Внешний пул NTP-серверов).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба синхронизации времени

3.22.1.154. Root NTP Servers - Drop

Подробное описание

Привилегия позволяет:

- Удалять корневые NTP-серверы (Роли и службы сайта/Служба синхронизации времени/вкладка Корневые NTP-серверы домена).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба синхронизации времени

3.22.1.155. Print Servers - Read

Подробное описание

Привилегия позволяет:

- Видеть список серверов печати (Роли и службы сайта/Служба печати);
- Видеть карточки серверов печати (Роли и службы сайта/Служба печати/<Сервер печати>/вкладка Основное);
- Видеть журнал изменений (Роли и службы сайта/Служба печати/<Сервер печати>/вкладка Основное/Журнал истории изменений).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба печати

3.22.1.156. Print Servers - Create

Подробное описание

Привилегия позволяет:

- Создавать новые серверы печати (Роли и службы сайта/Служба печати) на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба печати

3.22.1.157. Print Servers - Modify

Подробное описание

Привилегия позволяет:

- Изменять любой сайт сервера печати (Роли и службы сайта/Служба печати/<Сервер печати> вкладка Основное) на указанный в привилегии;
- Обновлять серверы печати на указанном сайте (Роли и службы сайта/Служба печати/<Сервер печати> вкладка Основное/кнопка «Обновить ALD Pro»).

Для корректной работы роль, включающая в себя данную привилегию, должна

распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба печати

3.22.1.158. Print Servers - Drop

Подробное описание

Привилегия позволяет:

- Удалять серверы печати (Роли и службы сайта/Служба печати) на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба печати

3.22.1.159. Printers - Manage

Подробное описание

Привилегия позволяет:

- Управлять принтерами серверов печати (Роли и службы сайта/Служба печати/<Сервер печати> вкладка Список принтеров): добавлять, удалять, редактировать, снимать задания печати на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Внимание: Для корректной работы привилегии, пользователь должен входить в предустановленную группу пользователей print_admins.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба печати

3.22.1.160. File Servers - Read

Подробное описание

Привилегия позволяет:

- Видеть список серверов общего доступа к файлам (Роли и службы сайта/Общий доступ к файлам/вкладка Перечень серверов);
- Видеть карточки серверов общего доступа к файлам (Роли и службы сайта/Общий доступ к файлам/вкладка Перечень серверов/<Сервер общего доступа к файлам>/вкладка Основное);
- Видеть список папок с общим доступом (Роли и службы сайта/Общий доступ к файлам/вкладка Перечень серверов/<Сервер общего доступа к файлам>/вкладка Общие папки);
- Видеть карточки папок с общим доступом (Роли и службы сайта/Общий доступ к файлам/вкладка Перечень серверов/<Сервер общего доступа к файлам>/вкладка Общие папки/<Общая папка>/вкладка Основное);
- Видеть журнал изменений (Роли и службы сайта/Общий доступ к файлам/вкладка Перечень серверов/<Сервер общего доступа к файлам>/вкладка Основное/Журнал истории изменений).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Общий доступ к файлам

3.22.1.161. File Servers - Create

Подробное описание

Привилегия позволяет:

- Создавать новые серверы общего доступа к файлам (Роли и службы сайта/Общий доступ к файлам) на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к

которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Общий доступ к файлам

3.22.1.162. File Servers - Modify

Подробное описание

Привилегия позволяет: - Изменять любой сайт сервера общего доступа к файлам (Роли и службы сайта/Служба общего доступа к файлам/<Сервер общего доступа к файлам> вкладка Основное) на указанный в привилегии; - Обновлять серверы общего доступа к файлам на указанном сайте (Роли и службы сайта/Служба общего доступа к файлам/<Сервер общего доступа к файлам> вкладка Основное/кнопка «Обновить ALD Pro»).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Общий доступ к файлам

3.22.1.163. File Server Folders - Manage

Подробное описание

Привилегия позволяет:

- Управлять папками с общим доступом (Роли и службы сайта/Служба общего доступа к файлам/<Сервер общего доступа к файлам> вкладка Общие папки): просматривать, добавлять, удалять, редактировать, настраивать доступ пользователям/компьютерам на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Общий доступ к файлам

3.22.1.164. File Servers - Drop

Подробное описание

Привилегия позволяет:

- Удалять серверы общего доступа к файлам (Роли и службы сайта/Служба общего доступа к файлам) на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Общий доступ к файлам

3.22.1.165. Global Catalog - Read

Подробное описание

Привилегия позволяет:

- Видеть список контроллеров домена с ролью глобального каталога (Роли и службы сайта/Служба глобального каталога).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба глобального каталога

3.22.1.166. Global Catalog - Add

Подробное описание

Привилегия позволяет:

- Создавать новые серверы с ролью глобального каталога (Роли и службы сайта/Служба глобального каталога) на указанном сайте;
- Добавить роль глобального каталога при создании контроллера домена (Управление доменом/Сайты и службы/вкладка Контроллеры домена) при помощи признака «Назначить роль глобального каталога» на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба глобального каталога

3.22.1.167. Global Catalog - Delete

Подробное описание

Привилегия позволяет:

- Удалять новые серверы с ролью глобального каталога (Роли и службы сайта/Служба глобального каталога) на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Роли и службы сайта:

- Служба глобального каталога

3.22.1.168. Monitoring Event Logs - Read

Подробное описание

Привилегия позволяет:

- Видеть список событий журнала мониторинга событий (Мониторинг/Журнал событий мониторинга).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Мониторинг:

- Журнал событий мониторинга

3.22.1.169. Monitoring Servers - Read

Подробное описание

Привилегия позволяет:

- Видеть список серверов мониторинга (Мониторинг/Журнал событий мониторинга/вкладка Серверы мониторинга);
- Видеть карточки серверов мониторинга (Мониторинг/Журнал событий мониторинга/вкладка Серверы мониторинга/<Сервер мониторинга>/вкладка Основное);
- Видеть журнал изменений (Мониторинг/Журнал событий мониторинга/вкладка Серверы мониторинга/<Сервер мониторинга>/вкладка Основное/Журнал истории изменений).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Мониторинг:

- Журнал событий мониторинга

3.22.1.170. Monitoring Servers - Create

Подробное описание

Привилегия позволяет:

- Создавать новые серверы мониторинга (Мониторинг/Журнал событий мониторинга/Серверы мониторинга) на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Мониторинг:

- Журнал событий мониторинга

3.22.1.171. Monitoring Servers - Modify

Подробное описание

Привилегия позволяет:

- Изменять любой сайт сервера мониторинга (Мониторинг/Журнал событий мониторинга/Серверы мониторинга/<Сервер мониторинга>) на указанный в привилегии;
- Обновлять сервер мониторинга на указанном сайте(Мониторинг/Журнал событий мониторинга/Серверы мониторинга/<Сервер мониторинга>/кнопка «Обновить ALD Pro»).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Мониторинг:

- Журнал событий мониторинга

3.22.1.172. Monitoring Servers - Drop

Подробное описание

Привилегия позволяет:

- Удалять серверы мониторинга (Мониторинг/Журнал событий мониторинга/Серверы мониторинга/<Сервер мониторинга>) на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Мониторинг:

- Журнал событий мониторинга

3.22.1.173. Dashboards - Read

Подробное описание

Привилегия позволяет:

- Видеть витрины мониторинга (Мониторинг/Витрины мониторинга).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Мониторинг:

- Витрины мониторинга домена

3.22.1.174. Event Log Servers - Create

Подробное описание

Привилегия позволяет на указанном сайте и подразделении:

- Создавать новые серверы журнала событий (Журнал событий/Серверы журнала событий) на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Журнал событий:

- Серверы журнала событий

3.22.1.175. Event Log Servers - Drop

Подробное описание

Привилегия позволяет:

- Удалять серверы журнала событий (Журнал событий/Серверы журнала событий) на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Журнал событий:

- Серверы журнала событий

3.22.1.176. Event Log Servers - Modify

Подробное описание

Привилегия позволяет:

- Изменять любой сайт сервера журнала событий (Журнал событий/Серверы журнала событий/<Сервер журнала событий>) на указанный в привилегии;
- Обновлять серверы журнала событий на указанном сайте (Журнал событий/Серверы журнала событий/<Сервер журнала событий>/кнопка «Обновить ALD Pro»).

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Журнал событий:

- Серверы журнала событий

3.22.1.177. Event Log Servers - Read

Подробное описание

Привилегия позволяет:

- Видеть список серверов журнала событий (Журнал событий/Серверы журнала событий);
- Видеть карточки серверов журнала событий (Журнал событий/Серверы журнала

событий/<Сервер журнала событий>);
- Видеть журнал изменений (Журнал событий/Серверы журнала событий/<Сервер журнала событий>/вкладка Основное/Журнал истории изменений).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Журнал событий:

- Серверы журнала событий

3.22.1.178. Event Registration Rules - Read

Подробное описание

Привилегия позволяет:

- Видеть список правил сбора событий (Журнал событий/Настройка сбора журнала событий);
- Видеть карточки правил сбора событий (Журнал событий/Настройка сбора журнала событий/<Правило сбора событий>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Журнал событий:

- Настройка сбора журналов событий

3.22.1.179. Event Registration Rules - Add

Подробное описание

Привилегия позволяет:

- Создавать новые правила сбора событий (Журнал событий/Настройка сбора журнала событий) на сервере, расположенном на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Журнал событий:

- Настройка сбора журналов событий

3.22.1.180. Event Registration Rules - Modify

Подробное описание

Привилегия позволяет:

- Изменять параметры правил сбора событий (Журнал событий/Настройка сбора журнала событий/<Правило сбора событий>) на сервере, на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Журнал событий:

- Настройка сбора журналов событий

3.22.1.181. Event Registration Rules - Delete

Подробное описание

Привилегия позволяет:

- Удалять правила сбора событий (Журнал событий/Настройка сбора журнала событий/<Правило сбора событий>) на сервере, расположенном на указанном сайте.

Для корректной работы роль, включающая в себя данную привилегию, должна распространяться на подразделение, в состав которого входят серверы или компьютеры, к которым применяются действия данной привилегии.

Привилегия может быть ограничена подразделением.

Привилегия может быть ограничена сайтом.

Доступ к подразделам портала управления

Журнал событий:

- Настройка сбора журналов событий

3.22.1.182. MS AD and ALD Pro Controllers - Read

Подробное описание

Привилегия позволяет:

- Видеть список контроллеров доменов AD (Модуль синхронизации/Настройки/вкладка Контроллеры домена AD);
- Видеть карточки контроллеров доменов AD (Модуль синхронизации/Настройки/вкладка Контроллеры домена AD/<Контроллер AD>);
- Видеть список контроллеров доменов ALD (Модуль синхронизации/Настройки/вкладка Контроллеры домена ALD);
- Видеть карточки контроллеров доменов ALD (Модуль синхронизации/Настройки/вкладка Контроллеры домена ALD/<Контроллер ALD>);
- Видеть содержимое вкладки Синхронизация паролей (Модуль синхронизации/Настройки/вкладка Синхронизация паролей).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Модуль синхронизации:

- Настройки

3.22.1.183. MS AD and ALD Pro Controllers - Create

Подробное описание

Привилегия позволяет:

- Добавлять новые контроллеры домена AD (Модуль синхронизации/Настройки/вкладка Контроллеры домена AD);
- Добавлять новые контроллеры домена ALD (Модуль синхронизации/Настройки/вкладка Контроллеры домена ALD);
- Получать файл ключа для синхронизации паролей AD ↔ ALD(Модуль синхронизации/Настройки/вкладка Синхронизация паролей).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Модуль синхронизации:

- Настройки

3.22.1.184. MS AD and ALD Pro Controllers - Modify

Подробное описание

Привилегия позволяет:

- Изменять контроллеры домена AD (Модуль синхронизации/Настройки/вкладка Контроллеры домена AD/<Контроллер AD>);
- Изменять контроллеры домена ALD (Модуль синхронизации/Настройки/вкладка Контроллеры домена ALD/<Контроллер ALD>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Модуль синхронизации:

- Настройки

3.22.1.185. MS AD and ALD Pro Controllers - Drop

Подробное описание

Привилегия позволяет:

- Удалять контроллеры домена AD (Модуль синхронизации/Настройки/вкладка Контроллеры домена AD/<Контроллер AD>);
- Удалять контроллеры домена ALD (Модуль синхронизации/Настройки/вкладка Контроллеры домена ALD/<Контроллер ALD>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Модуль синхронизации:

- Настройки

3.22.1.186. Organizational Units Mapping - Read

Подробное описание

Привилегия позволяет:

- Видеть список сопоставлений подразделений (Модуль синхронизации/Источники/вкладка Сопоставление подразделений);
- Видеть карточки сопоставлений подразделений (Модуль синхронизации/Источники/вкладка Сопоставление подразделений/<Сопоставление

подразделений>).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Модуль синхронизации:

- Источники

3.22.1.187. Organizational Units Mapping - Manage

Подробное описание

Привилегия позволяет:

- Управлять карточками сопоставлений подразделений (Модуль синхронизации/Источники/вкладка Сопоставление подразделений/<Сопоставление подразделений>): создавать, редактировать, удалять.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Модуль синхронизации:

- Источники

3.22.1.188. Synchronization Tree - Read

Подробное описание

Привилегия позволяет:

- Видеть структуру дерева синхронизации (Модуль синхронизации/Источники/вкладка Структура дерева синхронизации).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Модуль синхронизации:

- Источники

3.22.1.189. Synchronization Tree - Manage

Подробное описание

Привилегия позволяет:

- Проверять на наличие конфликтов синхронизации и решать их (Модуль синхронизации/Источники/вкладка Структура дерева синхронизации).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Модуль синхронизации:

- Источники

3.22.1.190. Attributes Mapping - Read

Подробное описание

Привилегия позволяет:

- Видеть список атрибутов AD (Модуль синхронизации/Сопоставление атрибутов/вкладка Атрибуты AD);
- Видеть список атрибутов ALD (Модуль синхронизации/Сопоставление атрибутов/вкладка Атрибуты ALD);
- Видеть список сопоставлений атрибутов (Модуль синхронизации/Сопоставление атрибутов/вкладка Карта сопоставлений).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Модуль синхронизации:

- Сопоставление атрибутов

3.22.1.191. Attributes Mapping - Manage

Подробное описание

Привилегия позволяет:

- Управлять атрибутами AD (Модуль синхронизации/Сопоставление атрибутов/вкладка Атрибуты AD): создавать, удалять;
- Управлять атрибутами ALD (Модуль синхронизации/Сопоставление атрибутов/вкладка Атрибуты ALD): создавать, удалять;

- Управлять сопоставлениями атрибутов (Модуль синхронизации/Сопоставление атрибутов/вкладка Карта сопоставлений): создавать, удалять.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Модуль синхронизации:

- Сопоставление атрибутов

3.22.1.192. Repository Versions - Manage

Подробное описание

Привилегия позволяет в указанном репозитории:

- Управлять версиями репозитория (Установка и обновление ПО/ Репозитории ПО/ вкладка Репозитории ПО/ <Репозиторий> вкладка Версии): просматривать, добавлять, удалять, редактировать.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

Доступ к подразделам портала управления

Установка и обновление ПО:

- Репозитории ПО

3.22.1.193. IPA Servers - Read

Подробное описание

Привилегия позволяет:

- Просматривать сервера.

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

3.22.1.194. Subsystems - Read

Подробное описание

Привилегия позволяет:

- Просматривать подсистемы (Управление доменом/Сайты и службы/вкладка Сайты).

Привилегия не может быть ограничена подразделением.

Привилегия не может быть ограничена сайтом.

3.22.2. Матрица привилегий

3.22.2.1. Обозначения

- о - Возможность Ограничения области действия роли
- но - Область действия Не может быть Ограничена

3.22.2.2. Управление доменом

3.22.2.3. Пользователи и группы

Роли	Организационная структура	Пользователи	Группы пользователей	Компьютеры	Группы компьютеров	Корзина
ALDPRO - Domain Info Reader	но			но		
ALDPRO - Domain Controllers and Sites Service Administrators	о			о		
ALDPRO - Kerberos Service Administrators	но			но		
ALDPRO - Users and Groups Settings Administrators	о	о				
ALDPRO - Roles Administrators	о	о	о			
ALDPRO - Organizational Units Administrators	о	о		о	о	
ALDPRO - Users Administrators	о	о				о
ALDPRO - User Groups Administrators	о	о	о			
ALDPRO - Computers Administrators	о			о		
ALDPRO - Computer Groups Administrators	о			о	о	
ALDPRO - Deleted User Accounts Administrators	но	но	но			но
ALDPRO - Group Policies Administrators	о					
ALDPRO - HBAC Administrators	о	о	о	о	о	
ALDPRO - SUDO Administrators	о	о	о	о	о	
ALDPRO - Password Policies Administrators	но		но			
ALDPRO - Software Policies Administrators	но			но	но	
ALDPRO - Software Catalog Administrators	но			но		
ALDPRO - Software Repositories Administrators	о			о		
ALDPRO - Software Update Policies Administrators	о			о	о	
ALDPRO - Automation Tasks Administrators	о	о		о	о	
ALDPRO - Install OS Service Administrators	о			о		
ALDPRO - DHCP Service Administrators	о			о		
ALDPRO - NTP Service Administrators	но			но		
ALDPRO - Print Service Administrators	о			о		
ALDPRO - File Servers Administrators	о	о	о	о		
ALDPRO - Global Catalog Service Administrators	о			о		
ALDPRO - Monitoring Administrators	о			о		
ALDPRO - Monitoring Dashboards Readers	но			но		
ALDPRO - Event Log Servers Administrators	о			о		
ALDPRO - Event Log Administrators	о			о		
ALDPRO - Syncer Settings Administrators	но			но		
ALDPRO - Syncer Sources Administrators	но			но		
ALDPRO - Syncer Attributes Mapping Administrators	но			но		
ALDPRO - Domain Viewer	но	но	но	но	но	но

продолжение на следующей странице

Таблица 3.58 – продолжение с предыдущей страницы

Роли	Организационная структура	Пользователи	Группы пользователей	Компьютеры	Группы компьютеров	Корзина
ALDPRO - Regional Administrator	о	о	о	о	о	о
ALDPRO - Main Administrator	но	но	но	но	но	но

3.22.2.4. Групповые политики

Роли	Групповые политики	Политики доступа к узлу	Политики повышения привилегий	Политики паролей
ALDPRO - Group Policies Administrators	о			
ALDPRO - HBAC Administrators		о		
ALDPRO - SUDO Administrators			о	
ALDPRO - Password Policies Administrators				но
ALDPRO - Domain Viewer	но	но	но	но
ALDPRO - Regional Administrator	о	о	о	
ALDPRO - Main Administrator	но	но	но	но

3.22.2.5. Установка и обновление ПО

Роли	Политики ПО	Каталог ПО	Репозитории ПО	Политики обновления ALD Pro
ALDPRO - Organizational Units Administrators	но			
ALDPRO - Software Policies Administrators	но	но		
ALDPRO - Software Catalog Administrators		но	но	
ALDPRO - Software Repositories Administrators		но	о	
ALDPRO - Software Update Policies Administrators				о
ALDPRO - Domain Viewer	но	но	но	но
ALDPRO - Regional Administrator				о
ALDPRO - Main Administrator	но	но	но	но

3.22.2.6. Автоматизация

Роли	Задания автоматизации	Установка ОС по сети
ALDPRO - Automation Tasks Administrators	о	
ALDPRO - Install OS Service Administrators		о
ALDPRO - Domain Viewer	но	но
ALDPRO - Regional Administrator	о	о
ALDPRO - Main Administrator	но	но

3.22.2.7. Роли и службы сайта

Роли	Служба разрешения имен	Служба динамической настрой-ки узла	Служба синхронизации времени	Служба печати	Общий доступ к файлам	Служба глобального каталога
ALDPRO - Domain Info Reader	но					
ALDPRO - Domain Controllers and Sites Service Administrators	но					
ALDPRO - Kerberos Service Administrators	но					
ALDPRO - Domain Integrations Administrators	но					
ALDPRO - Organizational Units Administrators	но					
ALDPRO - Computers Administrators	но					
ALDPRO - Computer Groups Administrators	но					
ALDPRO - HBAC Administrators	но					
ALDPRO - SUDO Administrators	но					
ALDPRO - Software Policies Administrators	но					
ALDPRO - Software Catalog Administrators	но					
ALDPRO - Software Repositories Administrators	но					
ALDPRO - Software Update Policies Administrators	но					
ALDPRO - Automation Tasks Administrators	но					
ALDPRO - Install OS Service Administrator	но	о				
ALDPRO - DNS Service Administrators	но					
ALDPRO - DHCP Service Administrators	но	о				
ALDPRO - NTP Service Administrators	но		но			
ALDPRO - Print Service Administrators	но			о		
ALDPRO - File Servers Administrators	но				о	
ALDPRO - Global Catalog Service Administrators	но					о
ALDPRO - Monitoring Administrators	но					
ALDPRO - Monitoring Dashboards Readers	но					
ALDPRO - Event Log Servers Administrators	но					
ALDPRO - Event Log Administrators	но					
ALDPRO - Syncer Settings Administrators	но					
ALDPRO - Syncer Sources Administrators	но					
ALDPRO - Syncer Attributes Mapping Administrators	но					
ALDPRO - Domain Viewer	но	но	но	но	но	но
ALDPRO - Regional Administrator	но	о		о	о	
ALDPRO - Main Administrator	но	но	но	но	но	но

3.22.2.8. Мониторинг

Роли	Журнал событий мониторинга	Витрины мониторинга домена
ALDPRO - Monitoring Administrators	о	но
ALDPRO - Monitoring Dashboards Readers	но	но
ALDPRO - Domain Viewer	но	но
ALDPRO - Regional Administrator	о	но
ALDPRO - Main Administrator	но	но

3.22.2.9. Журнал событий

Роли	Серверы журнала событий	Настройка сбора журналов событий
ALDPRO - Event Log Servers Administrators	о	
ALDPRO - Event Log Administrators	о	о
ALDPRO - Domain Viewer	но	но
ALDPRO - Regional Administrator	о	о
ALDPRO - Main Administrator	но	но

3.22.2.10. Модуль синхронизации

Роли	Настройки	Источники	Сопоставление атрибутов
ALDPRO - Syncer Settings Administrators	но		
ALDPRO - Syncer Sources Administrators	но	но	
ALDPRO - Syncer Attributes Mapping Administrators	но		но
ALDPRO - Domain Viewer	но	но	но
ALDPRO - Main Administrator	но	но	но

3.23. Миграция ролей

3.23.1. Введение

При обновлении ALD Pro до версии 2.4.0 выполняется миграция ролей и привилегий обновляемой Системы.

Все события миграции регистрируются в журналах на контроллере домена по пути /opt/rbta/migration:

- в директории «migrate_user_roco_roles» хранятся журналы миграции ролей ALDPRO - IT Security Specialist, ALDPRO - IT Specialist и пользовательских ролей, созданных до обновления портала управления;
- в директории «migrate_roles_main_and_regional_administrator» хранятся журналы миграции роли ALD PRO - Main Administrator и создания роли ALD Pro - Regional Administrator
- в директории «create_preset_roles» хранятся журналы миграции, создающей пользовательские роли, поставляемые по умолчанию в версии 2.4.0.

Описанные выше директории появляются по пути /opt/rbta/migration только в том случае, если миграция запускалась хотя бы один раз.

3.23.2. Миграция системных ролей

Все системные роли мигрируются полностью и в том же составе. В результате миграции:

- замена привилегий во время миграции в системных ролях не выполняется;
- в БД сохраняются системные роли, назначенные на пользователей (в интерфейсе портала управления системные роли, назначенные на пользователей, не отображаются и не выполняются).

3.23.3. Миграция предустановленных ролей

3.23.3.1. Миграция Enrollment Administrator, helpdesk, Security Architect, User Administrator

Enrollment Administrator, helpdesk, Security Architect, User Administrator до версии 2.4.0 были предустановленными ролями. После обновления на версию 2.4.0:

- эти роли становятся системными (тип «Системная»), и меняется их поведение в портале управления (работать с ними теперь можно, как с системными ролями. См. раздел Системные роли)
- в БД сохраняются существующие до обновления назначения пользователей на роли Enrollment Administrator, helpdesk, Security Architect, User Administrator
- В БД сохраняются все существующие до обновления привязки привилегий и разрешений для данных ролей (см. Руководство Администратора раздел 2.2.6)

3.23.3.2. Миграция ALDPRO - Main Administrator

В результате миграции на версию 2.4.0 для роли ALD PRO - Main Administrator выполняется:

- тип роли остается «Предустановленная»;
- роль привязывается к корню домена с установленным признаком «Включая дочерние подразделения»;
- для всех привилегий, которые могут быть ограничены сайтом, устанавливается привязка ко всем сайтам;
- роль остается назначенной на всех пользователей и группы пользователей, на которых была назначена до обновления;
- по результатам миграции роль автоматически переводится Системой в состояние «Активна».

Важно: Для получения возможности после обновления до версии 2.4.0 делегировать роли средствами портала управления необходимо, чтобы до начала обновления на роль ALD PRO - Main Administrator был назначен хотя бы один пользователь.

3.23.3.3. Миграция ALDPRO - IT Security Specialist и ALDPRO - IT Specialist

В результате миграции на версию 2.4.0 для ролей ALDPRO - IT Security Specialist и ALDPRO - IT Specialist выполняется:

- тип ролей ALDPRO - IT Security Specialist и ALDPRO - IT Specialist становится «Пользовательская»;
- названия ролей не меняются
- роли привязываются к корню домена с установленным признаком «Включая дочерние подразделения»;
- для всех привилегий, которые могут быть ограничены сайтом, устанавливается привязка ко всем сайтам;
- роли остаются назначенными на всех пользователей и группы пользователей, на которых были назначены до обновления.

В связи с приобретением дополнительных привилегий для мигрированных ролей ALDPRO - IT Security Specialist и ALDPRO - IT Specialist добавляются следующие доступы к подразделам портала управления:

Раздел / Подраздел	ALDPRO - IT Specialist до 2.4.0	ALDPRO - IT Specialist в 2.4.0 после миграции	Привилегии в 2.4.0, которые предоставляют доступ к подразделам
Управление доменом / Доп. параметры групповых политик	-	+	Поскольку роли ALDPRO - IT Specialist было доступно чтение групповых политик назначенных на подразделения, пользователей и компьютеры, в 2.4.0 требуются новые привилегии: - Computer Group Policy Additional Parameters - Read - User Group Policy Additional Parameters - Read
Управление доменом / Пользователи и группы	-	+	• Users and Groups Settings - Read
Групповые политики / Групповые политики	-	+	Поскольку роли ALDPRO - IT Specialist было доступно чтение групповых политик назначенных на подразделения, пользователей и компьютеры, в 2.4.0 требуется новая привилегия: - Group Policies - Read

Раздел / Подраздел	ALDPRO - IT Security Specialist до 2.4.0	ALDPRO - IT Security Specialist в 2.4.0 после миграции	Привилегии в 2.4.0, которые предоставляют доступ к подразделам
Установка и обновление ПО / Политики ПО	-	+	Поскольку ранее администратору ALDPRO - IT Security Specialist было доступно изменение конфигураций политик программного обеспечения, то в текущей парадигме прав доступа требуются следующие привилегии для управления политиками ПО: - Software Policies - Read - Software Policies - Modify - Software Policies Configurations - Manage - Software Policies Membership - Manage

продолжение на следующей странице

Таблица 3.67 – продолжение с предыдущей страницы

Раздел / Подраздел	ALDPRO - IT Security Specialist до 2.4.0	ALDPRO - IT Security Specialist в 2.4.0 после миграции	Привилегии в 2.4.0, которые предоставляют доступ к подразделам
Установка и обновление ПО / Каталог ПО	-	+	Для корректной работы политик ПО, ALDPRO - IT Security Specialist необходимо чтение каталога ПО: - Software Catalog - Read
Роли и службы сайта / Служба разрешения имен	-	+	Для корректной работы с подсистемами, ALDPRO - IT Security Specialist необходим доступ к чтению DNS: - DNS Zones - Read - DNS Forward Zones - Read

Предоставляемые права для ALDPRO - IT Specialist

Права, предоставляемые роли «ALDPRO - IT Specialist» по умолчанию после миграции со старших версий. Доступы могут измениться после внесения изменений в состав привилегий.

Раздел / Подраздел	Предоставляемые права
Автоматизация / Установка ОС по сети	1. **Installation Server Computers - Manage** - Позволяет осуществлять полное управление компьютерами в рамках серверов установки 1. **Installation Server Profiles - Manage** - Дает возможность управлять профилями загрузки 2. **Installation Servers - Create** - Позволяет создавать серверы установки в системе 3. **Installation Servers - Drop** - Дает возможность удалять существующие серверы установки 4. **Installation Servers - Modify** - Позволяет изменять настройки и конфигурации существующих серверов установки 5. **Installation Servers - Read** - Предоставляет доступ для чтения к информации о серверах установки
Автоматизация / Задания автоматизации	1. **Automation Tasks Journal - Read** - Предоставляет возможность просматривать журнал заданий автоматизации 1. **Automation Tasks Membership - Manage** - Дает право управлять участниками заданий автоматизации
Управление доменом / Пользователи и группы	**Users and Groups Settings - Read** - Предоставляет доступ для чтения к настройкам пользователей и групп
Управление доменом / Доп. параметры групповых политик	1. **User Group Policy Additional Parameters - Read** - Предоставляет возможность только для чтения для просмотра дополнительных параметров групповых политик для пользователей 1. **Computer Group Policy Additional Parameters - Read** - Предоставляет доступ для чтения к дополнительным параметрам групповых политик, применяемых к компьютерам

продолжение на следующей странице

Таблица 3.68 – продолжение с предыдущей страницы

Раздел / Подраздел	Предоставляемые права
Управление доменом / Сайты и службы	1. **Replication Agreements - Add** - Позволяет добавлять новые соглашения о репликации 1. **Replication Agreements - Delete** - Дает возможность удалять существующие соглашения о репликации 2. **Replication Agreements - Modify** - Позволяет изменять параметры существующих соглашений о репликации 3. **Replication Agreements - Read** - Предоставляет доступ только для чтения к соглашениям о репликации 4. **Domain Controllers - Create** - Позволяет создавать новые контроллеры домена в системе 5. **Domain Controllers - Drop** - Дает возможность удалять существующие контроллеры домена 6. **Domain Controllers - Modify** - Позволяет изменять параметры и настройки существующих контроллеров домена 7. **Domain Controllers - Read** - Предоставляет доступ для чтения к информации о контроллерах домена 8. **Site Parameters - Add** - Позволяет добавлять новые параметры конфигурации сайтов 9. **Site Parameters - Delete** - Дает возможность удалять существующие параметры сайтов 10. **Site Parameters - Modify** - Позволяет изменять существующие параметры сайта 11. **Site Parameters - Read** - Предоставляет доступ только для чтения к параметрам сайтов 12. **Site Domain Controllers - Add** - Позволяет назначить контроллер домена на сайт 13. **Sites - Read** - Позволяет просматривать информацию о сайтах в системе
Управление доменом / Общая информация	**Domain Info - Read** - Предоставляет возможность просматривать информацию о домене
Управление доменом / Каталог заданий автоматизации	1. **Automation Task Attributes - Manage** - Позволяет управлять атрибутами заданий автоматизации 1. **Automation Task Script - Manage** - Дает возможность управлять скриптами заданий автоматизации 2. **Automation Tasks - Manage** - Предоставляет полный контроль заданий автоматизации 3. **Automation Tasks - Read** - Предоставляет доступ для чтения к заданиям автоматизации 4. **Automation Tasks Folders - Manage** - Позволяет управлять папками в рамках заданий автоматизации
Пользователи и компьютеры / Организационная структура	**Organization units - Read** - Предоставляет доступ для чтения к организационным единицам
Пользователи и компьютеры / Группы компьютеров	1. **Computer groups - Add** - Позволяет создавать новые группы компьютеров в системе 1. **Computer groups - Delete** - Дает возможность удалять существующие группы компьютеров 2. **Computer groups - Modify** - Позволяет изменять параметры и состав существующих групп компьютеров 3. **Computer groups - Read** - Предоставляет доступ только для чтения к информации о группах компьютеров 4. **Computer groups - Set group membership** - Позволяет управлять членством компьютеров в определенных группах 5. **Computer groups - Set organization unit** - Позволяет назначать или изменять подразделение (OU) для групп компьютеров
Пользователи и компьютеры / Группы пользователей	**User groups - Read** - Предоставляет доступ для чтения к пользовательским группам
Пользователи и компьютеры / Пользователи	**Users - Read** - Предоставляет доступ только для чтения к пользовательским учетным записям

продолжение на следующей странице

Таблица 3.68 – продолжение с предыдущей страницы

Раздел / Подраздел	Предоставляемые права
Пользователи и компьютеры / Компьютеры	1. **Computers - Delete** - Позволяет удалять учетные записи компьютеров из системы 1. **Computers - Modify** - Дает возможность изменять свойства и настройки существующих учетных записей компьютеров 2. **Computers - Read** - Предоставляет доступ для чтения к информации о компьютерах в системе 3. **Computers - Remote access** - Позволяет осуществлять удаленный доступ к компьютерам 4. **Computers - Set organization unit** - Позволяет назначать или изменять подразделения (OU) для учетных записей компьютеров
Групповые политики / Групповые политики	**Group Policies - Read** - Предоставляет доступ только для чтения к существующим групповым политикам
Роли и службы сайта / Служба печати	1. **Print Servers - Create** - Позволяет создавать новые серверы печати в системе 1. **Print Servers - Drop** - Дает возможность удалять существующие серверы печати из системы 2. **Print Servers - Modify** - Позволяет изменять настройки и конфигурации существующих серверов печати 3. **Print Servers - Read** - Предоставляет доступ для чтения к информации о серверах печати 4. **Printers - Manage** - Позволяет управлять принтерами, подключенными к серверам печати, включая добавление, удаление и изменение настроек
Роли и службы сайта / Служба динамической настройки узла	1. **DHCP - Read** - Предоставляет доступ для чтения к DHCP 1. **DHCP Configuration - Modify** - Позволяет изменять конфигурации DHCP-сервера 2. **DHCP Servers - Create** - Дает возможность создавать новые DHCP-серверы 3. **DHCP Servers - Drop** - Позволяет удалять существующие DHCP-серверы 4. **DHCP Servers - Modify** - Позволяет вносить изменения в существующие DHCP-серверы
Роли и службы сайта / Служба разрешения имён	1. **DNS Forward Zones - Add** - Позволяет добавлять новые перенаправления запросов **DNS** 1. **DNS Forward Zones - Delete** - Дает возможность удалять существующие перенаправления запросов **DNS** 2. **DNS Forward Zones - Delete** - Позволяет изменять конфигурацию существующих перенаправлений запросов **DNS** 3. **DNS Forward Zones - Read** - Предоставляет доступ для чтения к информации о перенаправлении запросов **DNS** 4. **DNS Global Configurations - Manage** - Позволяет управлять глобальными конфигурациями **DNS** 5. **DNS Zones - Manage** - Дает возможность управлять DNS-зонами, включая создание, изменение и удаление зон 6. **DNS Zones - Read** - Предоставляет доступ только для чтения к информации о DNS-зонах
Роли и службы сайта / Служба синхронизации времени	1. **Root NTP Servers - Create** - Позволяет создавать новые корневые NTP-серверы 1. **Root NTP Servers - Drop** - Дает возможность удалять существующие корневые NTP-серверы из конфигурации системы 2. **NTP Servers - Read** - Предоставляет доступ для чтения к информации о NTP-серверах 3. **External NTP Servers - Create** - Позволяет добавлять новые внешние NTP-серверы 4. **External NTP Servers - Drop** - Дает возможность удалять внешние NTP-серверы из конфигурации системы

продолжение на следующей странице

Таблица 3.68 – продолжение с предыдущей страницы

Раздел / Подраздел	Предоставляемые права
Установка и обновление ПО / Каталог ПО	1. **Software Templates - Manage** - Позволяет управлять шаблонами программного обеспечения в системе 1. **Software - Manage** - Дает возможность управлять всем программным обеспечением в системе 2. **Software Catalog - Read** - Предоставляет доступ только для чтения к каталогу программного обеспечения 3. **Software Groups - Manage** - Позволяет управлять группами программного обеспечения 4. **Software Packages - Manage** - Дает возможность управлять программными пакетами в системе 5. **Software Parameters - Manage** - Позволяет управлять параметрами, связанными с программным обеспечением
Установка и обновление ПО / Политики ПО	1. **Software Policies - Add** - Позволяет добавлять новые политики программного обеспечения в системе 1. **Software Policies - Delete** - Дает возможность удалять существующие политики программного обеспечения 2. **Software Policies - Modify** - Позволяет изменять существующие политики программного обеспечения 3. **Software Policies - Read** - Обеспечивает доступ только для чтения к текущим политиками программного обеспечения 4. **Software Policies Configurations - Manage** - Позволяет управлять конфигурациями, связанными с политиками программного обеспечения 5. **Software Policies Membership - Manage** - Позволяет управлять членством в политиках программного обеспечения
Установка и обновление ПО / Репозитории ПО	1. **Repositories - Add** - Позволяет создавать новые репозитории в системе 1. **Repositories - Delete** - Дает возможность удалять существующие репозитории из системы 2. **Repositories - Modify** - Позволяет изменять параметры и содержимое существующих репозиториев 3. **Repositories - Read** - Предоставляет доступ для чтения к информации о репозиториях 4. **Repository Servers - Create** - Позволяет создавать новые сервера-репозитории в системе 5. **Repository Servers - Drop** - Дает возможность удалять существующие сервера-репозитории 6. **Repository Servers - Modify** - Позволяет изменять конфигурацию и параметры существующих серверов-репозиториев 7. **Repository Servers - Read** - Предоставляет доступ только для чтения к серверам-репозиториям 8. **Repository Versions - Manage** - Позволяет управлять версиями программных пакетов и репозиториев
Установка и обновление ПО / Политики обновления ALD Pro	1. **Update Policies - Add** - Позволяет добавлять новые политики обновления в системе 1. **Update Policies - Delete** - Дает возможность удалять существующие политики обновления 2. **Update Policies - Modify** - Позволяет изменять параметры существующих политик обновления 3. **Update Policies - Read** - Предоставляет доступ только для чтения к существующим политикам обновления 4. **Update Policies Computers - Manage** - Позволяет управлять применением политик обновления к конкретным компьютерам или группам компьютеров 5. **Update Policies Sources list - Manage** - Дает возможность управлять списком источников обновлений
Доступ только через БД и API	**IPA Servers - Read** - Предоставляет доступ для чтения к информации об IPA серверах

Предоставляемые права для ALDPRO - IT Security Specialist

Права, предоставляемые роли «ALDPRO - IT Security Specialist» по умолчанию после миграции со старших версий. Доступы могут измениться после внесения изменений в состав привилегий.

Раздел / Подраздел	Предоставляемые права
Автоматизация / Задания автоматизации	1. **Automation Tasks Journal - Read** - Предоставляет возможность просматривать журнал заданий автоматизации 1. **Automation Tasks Membership - Manage** - Дает право управлять участниками заданий автоматизации
Управление доменом / Сайты и службы	1. **Site Parameters - Read** - Предоставляет возможность просматривать параметры конфигурации сайтов 1. **Sites - Read** - Даёт доступ для чтения к информации о сайтах в домене 2. **Domain Controllers - Read** - Позволяет просматривать информацию о контроллерах домена 3. **Replication Agreements - Read** - Обеспечивает доступ для чтения к соглашениям о репликации
Управление доменом / Пользователи и группы	1. **Users and Groups Settings - Manage** - Позволяет управлять настройками пользователей и групп в системе 1. **Users and Groups Settings - Read** - Предоставляет доступ для чтения к настройкам пользователей и групп
Управление доменом / Роли и права доступа	1. **Role Privileges - Add** - Позволяет добавлять новые привилегии к существующим ролям 1. **Role Privileges - Delete** - Дает возможность удалять привилегии из ролей 2. **Role Privileges - Modify** - Позволяет изменять существующие привилегии в ролях ролями 3. **Roles - Add** - Позволяет создавать новые роли в систем 4. **Roles - Delete** - Позволяет удалять существующие роли 5. **Roles - Modify** - Дает возможность изменять параметры существующих ролей 6. **Roles - Read** - Предоставляет доступ для чтения к существующим ролям 7. **Roles Membership - Manage** - Позволяет управлять членством в ролях, включая добавление или удаление пользователей или групп из определенных ролей
Управление доменом / Общая информация	**Domain Info - Read** - Предоставляет возможность просматривать информацию о домене
Управление доменом / Доп. параметры групповых политик	1. **Computer Group Policy Additional Parameters - Manage** - Позволяет управлять дополнительными параметрами групповых политик для компьютеров 1. **Computer Group Policy Additional Parameters - Read** - Предоставляет возможность просматривать дополнительные параметры групповых политик для компьютеров 2. **User Group Policy Additional Parameters - Manage** - Позволяет управлять дополнительными параметрами групповых политик для пользователей 3. **User Group Policy Additional Parameters - Read** - Предоставляет возможность только для чтения дополнительных параметров групповых политик для пользователей
Управление доменом / Службы и параметры Kerberos	1. **Kerberos Configurations - Manage** - Позволяет управлять конфигурациями Kerberos в системе 1. **Kerberos Services - Add** - Дает возможность добавлять новые Kerberos службы в систему 2. **Kerberos Services - Delete** - Позволяет удалять существующие Kerberos службы 3. **Kerberos Services - Modify** - Предоставляет возможность изменять параметры существующих Kerberos служб 4. **Kerberos Services - Read** - Предоставляет доступ только для чтения к информации о Kerberos службах

продолжение на следующей странице

Таблица 3.69 – продолжение с предыдущей страницы

Раздел / Подраздел	Предоставляемые права
Управление доменом / Каталог заданий автоматизации	1. **Automation Task Attributes - Manage** - Позволяет управлять атрибутами заданий автоматизации 1. **Automation Task Script - Manage** - Дает возможность управлять скриптами, связанными с заданиями автоматизации 2. **Automation Tasks - Manage** - Позволяет управлять заданиями автоматизации, включая их создание, изменение 3. **Automation Tasks - Read** - Предоставляет возможность только просматривать задания автоматизации 4. **Automation Tasks Folders - Manage** - Позволяет управлять папками, содержащими задания автоматизации
Журнал событий / Серверы журнала событий	1. **Event Log Servers - Create** - Позволяет создавать новые серверы журналов событий в системе 1. **Event Log Servers - Drop** - Дает возможность удалять существующие серверы журналов событий из системы 2. **Event Log Servers - Modify** - Позволяет изменять конфигурации и настройки существующих серверов журналов событий 3. **Event Log Servers - Read** - Предоставляет доступ для чтения к информации о серверах журналов событий
Журнал событий / Настройка сбора журналов событий	1. **Event Registration Rules - Add** - Позволяет добавлять новые правила регистрации событий в системе 1. **Event Registration Rules - Delete** - Дает возможность удалять существующие правила регистрации событий 2. **Event Registration Rules - Modify** - Позволяет изменять параметры и условия существующих правил регистрации событий 3. **Event Registration Rules - Read** - Предоставляет доступ только для чтения к правилам регистрации событий
Роли и службы сайта / Общий доступ к файлам	1. **File Server Folders - Manage** - Предоставляет возможность управлять папками на файловых серверах 1. **File Servers - Create** - Позволяет создавать новые файловые серверы в системе 2. **File Servers - Drop** - Дает возможность удалять существующие файловые серверы из системы 3. **File Servers - Modify** - Позволяет изменять конфигурации и параметры существующих файловых серверов 4. **File Servers - Read** - Предоставляет доступ только для чтения к информации о файловых серверах
Роли и службы сайта / Служба разрешения имён	1. **DNS Forward Zones - Read** - Предоставляет доступ для чтения к информации о перенаправлении запросов DNS 1. **DNS Zones - Read** - Предоставляет доступ только для чтения к информации о DNS-зонах
Групповые политики / Политики паролей	1. **Password Policies - Add** - Позволяет добавлять новые политики паролей в систему 1. **Password Policies - Delete** - Дает возможность удалять существующие политики паролей 2. **Password Policies - Modify** - Позволяет изменять настройки существующих политик паролей 3. **Password Policies - Read** - Предоставляет доступ только для чтения к существующим политикам паролей

продолжение на следующей странице

Таблица 3.69 – продолжение с предыдущей страницы

Раздел / Подраздел	Предоставляемые права
Групповые политики / Политики повышения привилегий	1. **SUDO - Read** - Предоставляет возможность просматривать текущие настройки и конфигурации SUDO 1. **SUDO Command Groups - Add** - Позволяет добавлять новые группы команд SUDO 2. **SUDO Command Groups - Delete** - Дает возможность удалять существующие группы команд SUDO 3. **SUDO Command Groups - Modify** - Позволяет изменять состав или параметры существующих групп команд SUDO 4. **SUDO Commands - Add** - Предоставляет возможность добавлять отдельные SUDO команды в группы или правила 5. **SUDO Commands - Delete** - Позволяет удалять отдельные SUDO команды из их групп или правил 6. **SUDO Commands - Modify** - Дает возможность изменять параметры существующих SUDO команд 7. **SUDO Parameters - Manage** - Позволяет управлять параметрами конфигурации SUDO 8. **SUDO Rules - Add** - Позволяет добавлять новые правила SUDO 9. **SUDO Rules - Delete** - Позволяет удалять существующие правила SUDO 10. **SUDO Rules - Modify** - Дает возможность изменять существующие правила SUDO
Групповые политики / Групповые политики	1. **Group Policies - Add** - Позволяет добавлять новые групповые политики в системе 1. **Group Policies - Delete** - Дает возможность удалять существующие групповые политики 2. **Group Policies - Modify** - Позволяет изменять настройки существующих групповых политик 3. **Group Policies - Read** - Предоставляет доступ только для чтения к существующим групповым политикам 4. **Group Policies Computer Parameters - Manage** - Позволяет управлять параметрами компьютеров в рамках групповых политик 5. **Group Policies User Parameters - Manage** - Предоставляет возможность управлять пользовательскими параметрами в рамках групповых политик 6. **Group Policies Membership - Manage** - Позволяет управлять членством в групповых политиках
Групповые политики / Политики доступа к узлу	1. **HBAC - Read** - Предоставляет возможность просматривать настройки и правила контроля доступа на основе хоста (HBAC) 1. **HBAC Rules - Add** - Позволяет добавлять новые правила HBAC 2. **HBAC Rules - Delete** - Дает возможность удалять существующие правила HBAC 3. **HBAC Rules - Modify** - Позволяет изменять существующие правила HBAC 4. **HBAC Service Groups - Add** - Позволяет создавать новые группы служб в рамках HBAC 5. **HBAC Service Groups - Delete** - Дает возможность удалять существующие группы служб в рамках HBAC 6. **HBAC Service Groups - Modify** - Позволяет изменять состав или параметры существующих групп служб 7. **HBAC Services - Add** - Предоставляет возможность добавлять новые службы для контроля доступа в HBAC 8. **HBAC Services - Delete** - Позволяет удалять существующие службы из списка контролируемых доступа 9. **HBAC Services - Modify** - Дает возможность изменять параметры существующих служб
Мониторинг / Витрины мониторинга домена	**Dashboards - Read** - Предоставляет доступ для чтения к дашбордам системы

продолжение на следующей странице

Таблица 3.69 – продолжение с предыдущей страницы

Раздел / Подраздел	Предоставляемые права
Мониторинг / Журнал событий мониторинга	1. **Monitoring Event Logs - Read** - Предоставляет доступ только для чтения к журналам событий мониторинга 1. **Monitoring Servers - Create** - Позволяет создавать новые сервера для мониторинга в системе 2. **Monitoring Servers - Drop** - Дает возможность удалять существующие сервера мониторинга из системы 3. **Monitoring Servers - Modify** - Позволяет изменять конфигурации и настройки существующих серверов мониторинга 4. **Monitoring Servers - Read** - Предоставляет доступ только для чтения к информации о серверах мониторинга
Установка и обновление ПО / Каталог ПО	**Software Catalog - Read** - Предоставляет доступ для чтения к каталогу программного обеспечения
Установка и обновление ПО / Политики ПО	1. **Software Policies - Modify** - Позволяет изменять существующие политики программного обеспечения 1. **Software Policies - Read** - Предоставляет доступ для чтения к текущим политикам программного обеспечения 2. **Software Policies Configurations - Manage** - Позволяет управлять конфигурациями, связанными с политиками программного обеспечения
Модуль синхронизации / Настройки	1. **MS AD andALD Pro Controllers - Create** - Позволяет создавать новые контроллеры Microsoft Active Directory (AD) и ALD Pro 1. **MS AD and ALD Pro Controllers - Drop** - Дает возможность удалять существующие контроллеры Microsoft AD и ALD Pro из системы 2. **MS AD and ALD Pro Controllers - Modify** - Позволяет изменять настройки и конфигурации существующих контроллеров Microsoft AD и ALD Pro 3. **MS AD and ALD Pro Controllers - Read** - Предоставляет доступ для чтения к информации о контроллерах Microsoft AD и ALD Pro
Модуль синхронизации / Сопоставление атрибутов	1. **Attributes Mapping - Manage** - Позволяет управлять отображением атрибутов в системе 1. **Attributes Mapping - Read** - Предоставляет доступ только для чтения к отображению атрибутов
Модуль синхронизации / Источники	1. **Organizational Units Mapping - Manage** - Позволяет управлять сопоставлением подразделений (OU) 1. **Organizational Units Mapping - Read** - Предоставляет доступ для чтения к сопоставлению подразделений 2. **Synchronization Tree - Manage** - Позволяет управлять деревом синхронизации в системе 3. **Synchronization Tree - Read** - Предоставляет доступ для чтения к дереву синхронизации
Пользователи и компьютеры / Группы компьютеров	1. **Computer groups - Add** - Позволяет создавать новые группы компьютеров в системе 1. **Computer groups - Delete** - Дает возможность удалять существующие группы компьютеров 2. **Computer groups - Modify** - Позволяет изменять настройки и состав существующих групп компьютеров 3. **Computer groups - Read** - Предоставляет доступ только для чтения к информации о группах компьютеров 4. **Computer groups - Set group membership** - Позволяет управлять членством компьютеров в определенных группах 5. **Computer groups - Set organization unit** - Позволяет назначать или изменять подразделение (OU)
Пользователи и компьютеры / Компьютеры	1. **Computers - Delete** - Позволяет удалять учетные записи компьютеров из системы 1. **Computers - Modify** - Дает возможность изменять свойства и настройки существующих учетных записей компьютеров 2. **Computers - Read** - Предоставляет доступ для чтения к информации о компьютерах в системе 3. **Computers - Remote access** - Позволяет осуществлять удаленный доступ к компьютерам 4. **Computers - Set organization unit** - Позволяет назначать или изменять подразделения (OU) для учетных записей компьютеров

продолжение на следующей странице

Таблица 3.69 – продолжение с предыдущей страницы

Раздел / Подраздел	Предоставляемые права
Пользователи и компьютеры / Организационная структура	1. **Organization Units - Add** - Позволяет создавать новые подразделения (OU) в системе 1. **Organization units - Delete** - Дает возможность удалять существующие подразделения 2. **Organization units - Modify** - Позволяет изменять параметры существующих подразделения 3. **Organization units - Read** - Предоставляет доступ для чтения к организационным единицам
Пользователи и компьютеры / Группы пользователей	1. **User groups - Add** - Позволяет создавать новые пользовательские группы в системе 1. **User groups - Delete** - Дает возможность удалять существующие пользовательские группы 2. **User groups - Modify** - Позволяет изменять параметры существующих пользовательских групп 3. **User groups - Read** - Предоставляет доступ для чтения к пользовательским группам 4. **User groups - Set group membership** - Позволяет управлять членством пользователей в группах 5. **User groups - Set organization unit** - Позволяет назначать или изменять подразделение (OU) для пользовательских групп
Пользователи и компьютеры / Пользователи	1. **Users - Add** - Позволяет добавлять новые пользовательские учетные записи в систему 1. **Users - Modify** - Позволяет изменять существующие пользовательские учетные записи 2. **Users - Read** - Предоставляет доступ только для чтения к пользовательским учетным записям 3. **Users - Set organization unit** - Позволяет назначать или изменять подразделение (OU) для учетных записей 4. **Users Password - Modify** - Дает возможность изменять пароли для учетных записей
Пользователи и компьютеры / Корзина	1. **Users - Read trash** - Позволяет просматривать учетные записи, которые были перемещены в корзину 1. **Users - Delete from trash** - Дает возможность окончательно удалять пользовательские учетные записи из корзины 2. **Users - Return from trash** - Дает возможность восстанавливать из корзины пользовательские учетные записи, которые были ранее перемещены туда 3. **Users - Move to trash** - Дает возможность перемещать пользовательские учетные записи в корзину
Доступ только через БД и API	**IPA Servers - Read** - Предоставляет доступ для чтения к информации об IPA серверах

3.23.4. Миграция пользовательских ролей

3.23.4.1. Миграция пользовательских ролей, поставляемых по умолчанию в версии 2.4.0

После обновления до версии 2.4.0 появляются новые пользовательские роли, установленные в Системе по умолчанию:

- роли на операции в каждом подразделе портала управления;
- роль на чтение всего портала управления;
- роль регионального администратора.

Для этих ролей выполняются следующие условия:

- тип ролей «Пользовательская»;

- роли привязываются к корню домена с установленным признаком «Включая дочерние подразделения»;
- для всех привилегий, которые могут быть ограничены сайтом, устанавливается привязка ко всем сайтам;
- на эти роли не делегированы пользователи и группы пользователей.

3.23.4.2. Миграция пользовательских ролей, созданных до обновления портала управления

В версию 2.4.0 переносятся все роли, созданные пользователями до обновления.

С версии 2.4.0 привязка к подразделению указывается для роли. Привилегии в составе роли, которым требуется привязка к подразделению, наследуют эту настройку от роли.

Привилегии одной роли, привязанные к разным подразделениям, в результате миграции будут распределены по нескольким ролям с учетом общей привязки к подразделению и признака «Включая дочерние подразделения».

Правила миграции пользовательских ролей:

- тип ролей сохраняется: «Пользовательская»;
- создается набор ролей по количеству привязок привилегий с учетом признака «Включая дочерние подразделения» в мигрируемой роли:
  - если в результате миграции из одной роли создается несколько ролей, для новых ролей в наборе к старому названию добавляется порядковый номер;
  - если в результате миграции из одной роли создается несколько ролей, каждая новая роль в наборе содержит все привилегии старой роли, которые не могут быть ограничены подразделением;
- если мигрируемая роль была в статусе «Активна», то все соответствующие ей новые роли будут активированы:
  - будет выполнена попытка делегировать все новые роли всем пользователям и группам пользователей, на которых была назначена старая роль:
    - если некоторые пользователи выпадут из области действия привязки новой роли (т.е. подразделение новой роли и подразделение пользователя или хотя бы одного из пользователей в группе не совпадают с учетом признака «Включая дочерние подразделения» у новой роли), такой пользователь или группа не получат новую роль, в журнал миграции будет внесена запись об ошибке делегирования;
- если статус мигрируемой роли отличен от «Активна», то статус наследуется, и все пользователи и все группы переносятся во все новые роли:
  - при процедуре активации всех новых ролей будет происходить проверка возможности наличия перенесенных пользователей в каждой роли (с привязкой к конкретному подразделению);
  - привязку роли к подразделению можно сменить таким образом, чтобы подразделения всех пользователей, назначенных на роль, подпадали в область действия роли (обязательное условие успеха активации роли).

Примечание: После обновления появляются дополнительные зависимости в правах доступа. Поэтому в привилегии могут быть добавлены связанные привилегии. Роли с

такими привилегиями сохраняют свой статус согласно указанному алгоритму. Активные роли продолжают работать, но для полной функциональности после обновления необходимо деактивировать роль и добавить все связанные привилегии.

3.24. Доступные точки входа для пользователей без дополнительных привилегий (ролей)

3.24.1. Аннотация

Ниже приведен список точек входа, доступных пользователю со стандартной учетной записью. Основная часть открытых точек входа — это запросы типа GET, предназначенные для чтения данных без изменения состояния системы. В некоторых случаях запросы могут возвращать код успеха (200), но не содержать данных, что является нормальным поведением системы. В таблице также присутствуют запросы типа POST и PATCH, которые предназначены для операций, связанных с аутентификацией и операциями в личном кабинете пользователя ALD Pro.

3.24.2. Описание точек входа

Метод	ТВ	Описание	Ответ
	Аутентификация пользователя		
POST	/api/ds/login	Аутентификация пользователя: вход	Аутентификация
POST	/api/ds/logout	Аутентификация пользователя: выход	Завершение сеанса
GET	/api/ds/whoami	Аутентификация пользователя: получить данные о текущей сессии пользователя	Возвращает данные
	Конфигурация службы каталогов		
GET	/api/ds/dsserver/schema/attributetypes	Конфигурация службы каталогов: Получить значения справочника типов данных атрибутов схемы	Возвращает данные
	Справочники		
GET	/api/ds/countries	Служба каталогов: получить значения справочника стран	Возвращает данные
	Пользователи		
GET	/api/ds/user-profile	Пользователи: Получить параметры текущего пользователя (Личный кабинет)	Возвращает данные

продолжение на следующей странице

Таблица 3.70 – продолжение с предыдущей страницы

Метод	ТВ	Описание	Ответ
PATCH	/api/ds/user-profile	Пользователи: Обновить параметры текущего пользователя (Личный кабинет)	Изменяет данные
PATCH	/api/ds/user-profile/reset-password	Пользователи: Изменить пароль текущего пользователя (Личный кабинет)	Изменяет пароль
GET	/api/ds/users/ {userName}/custom-attributes	Пользователи: Получить список дополнительных атрибутов пользователя	Возвращает данные
GET	/api/ds/users	Пользователи: Получить список пользователей	Возвращает данные
GET	/api/ds/users/ {userName}	Пользователи: Получить параметры пользователя	Возвращает данные
GET	/api/ds/users/ {userName}/user-groups	Пользователи: Получить список групп пользователей, в которые входит пользователь	Возвращает данные
GET	/api/ds/users/ {userName}/user-groups/indirect	Пользователи: Получить список групп пользователей, в которые косвенно входит пользователь	Возвращает данные
GET	/api/ds/users/ {userName}/roles	Пользователи: Получить список ролей пользователя	Возвращает данные
GET	/api/ds/users/ {userName}/roles/ indirect	Пользователи: Получить список ролей, в которые косвенно входит пользователь	Возвращает данные
GET	/api/ds/users/ {userName}/ proxy_addresses	Пользователи: Получить перечень значений прокси адресов пользователя	Возвращает данные
GET	/api/ds/preserved/ users/{userName}/ proxy_addresses	Пользователи: Получить перечень значений прокси адресов хранимого пользователя в корзине	Возвращает данные
	Группы пользователей		
GET	/api/ds/user-groups	Группы пользователей: Получить список групп пользователей	Возвращает данные
GET	/api/ds/user-groups/ {userGroupName}	Группы пользователей: Получить карточку группы пользователей	Возвращает данные
GET	/api/ds/user-groups/ {userGroupName}/ groups/child-group	Группы пользователей: Получить список групп в составе группы пользователей	Возвращает данные

продолжение на следующей странице

Таблица 3.70 – продолжение с предыдущей страницы

Метод	ТВ	Описание	Ответ
GET	/api/ds/user-groups/ {userGroupName}/ groups/child-group/indirect	Группы пользователей: Получить группы, которые косвенно содержит группа пользователей	Возвращает данные
GET	/api/ds/user-groups/ {userGroupName}/ groups/parent-group	Группы пользователей: Получить список групп, в состав которых входит группа пользователей	Возвращает данные
GET	/api/ds/user-groups/ {userGroupName}/ groups/parent-group/indirect	Группы пользователей: Получить список групп, в состав которых косвенно входит группа пользователей	Возвращает данные
GET	/api/ds/user-groups/ {userGroupName}/ users	Группы пользователей: Получить список пользователей в составе группы пользователей	Возвращает данные
GET	/api/ds/user-groups/ {userGroupName}/ roles	Группы пользователей: Получить список ролей в составе группы пользователей	Возвращает данные
GET	/api/ds/user-groups/ {userGroupName}/ roles/indirect	Группа пользователей: Получить список ролей, в которые косвенно входит группа пользователей	Возвращает данные
	Компьютеры		
GET	/api/ds/computers	Компьютеры: Получить список компьютеров	Возвращает данные
GET	/api/ds/computers/ {computerName}	Компьютеры: Получить параметры компьютера	Возвращает данные
GET	/api/ds/computers/ {computerName}/ groups	Компьютеры: Получить группы компьютеров, в которые входит компьютер	Возвращает данные
GET	/api/ds/computers/ {computerName}/ groups/indirect	Компьютеры: Получить группы компьютеров, в которые косвенно входит компьютер	Возвращает данные
	Группы компьютеров		
GET	/api/ds/computer-groups	Группы компьютеров: Получить список групп компьютеров	Возвращает данные
GET	/api/ds/computer-groups/ {computerGroupName}	Группы компьютеров: Получить параметры группы компьютеров	Возвращает данные

продолжение на следующей странице

Таблица 3.70 – продолжение с предыдущей страницы

Метод	ТВ	Описание	Ответ
GET	/api/ds/computer-groups/ {computerGroupName}/ computers	Группы компьютеров: Получить компьютеры в составе группы	Возвращает данные
GET	/api/ds/computer-groups/ {computerGroupName}/ groups/child-groups	Группы компьютеров: Получить группы, которые содержит группа компьютеров	Возвращает данные
GET	/api/ds/computer-groups/ {computerGroupName}/ groups/child-groups/indirect	Группы компьютеров: Получить группы, которые косвенно содержит группа компьютеров	Возвращает данные
GET	/api/ds/computer-groups/ {computerGroupName}/ groups/parent-groups	Группы компьютеров: Получить группы, в которых состоит группа компьютеров	Возвращает данные
	Организационные подразделения		
GET	/api/ds/organizational-units	Организационные подразделения: Получить список организационных подразделений	Возвращает данные
GET	/api/ds/organizational-units/ catalogue/children	Организационные подразделения: Получить корневые объекты дерева каталога. Переход между уровнями дерева каталога организационных подразделений	Возвращает данные
GET	/api/ds/organizational-units/ catalogue/parent-tree	Организационные подразделения: Возврат в выбранный объект каталога после его конфигурации	Возвращает данные
GET	/api/ds/organizational-units/ catalogue/search	Организационные подразделения: Поиск по дереву каталога организационных подразделений	Возвращает данные
GET	/api/ds/organizational-units/ {organizationalUnit DistinguishedName}	Организационные подразделения: Получить параметры организационного подразделения	Возвращает данные
GET	/api/ds/organizational-units/ {organizationalUnit DistinguishedName}/ organizational-units	Организационные подразделения: Получить список дочерних организаций подразделения	Возвращает данные
GET	/api/ds/organizational-units/ {organizationalUnit DistinguishedName}/ computers-groups	Организационные подразделения: Получить группы компьютеров организационного подразделения	Возвращает данные

продолжение на следующей странице

Таблица 3.70 – продолжение с предыдущей страницы

Метод	ТВ	Описание	Ответ
GET	/api/ds/organizational-units/ {organizationalUnit DistinguishedName}/ computers	Организационные подразделения: Получить список компьютеров организационного подразделения	Возвращает данные
GET	/api/ds/organizational-units/ {organizationalUnit DistinguishedName}/ group-policies	Организационные подразделения: Получить список объектов групповых политик подразделения	Возвращает данные
GET	/api/ds/organizational-units/ {organizationalUnit DistinguishedName}/ users-groups	Организационные подразделения: Получить список групп пользователей организационного подразделения	Возвращает данные
GET	/api/ds/organizational-units/ {organizationalUnit DistinguishedName}/ users	Организационные подразделения: Получить список пользователей организационного подразделения	Возвращает данные

3.25. Особенности работы системы при гранулярном управлении доступом

3.25.1. Особенности работы привилегий

Привилегии	Особенности работы привилегий
• Print Servers - Read • Event Log Servers - Read • Event Registration Rules - Add • Monitoring Servers - Read • Replication Servers - Read • DHCP - Read • Backup - Read • Group Policies - Read • Software Updates - Read • Automation Tasks - Manage	Привилегии позволяют видеть в базе данных автора изменений для ГП, политик ПО, заданий автоматизации, правил сбора событий и серверных подсистем (DHCP, серверы печати и т.д.)
• Computers - Read	Привилегия позволяет видеть в базе данных информацию об установленных на компьютер подсистемах
• Users - Return from trash	Для успешной активации роль с данной привилегией должна быть назначена на корень домена (при этом признак «Включая дочерние подразделения» может быть как установлен, так и не установлен)
• Users and Groups Settings - Manage	Роль с данной привилегией должна быть привязана к корню домена с установленным признаком »Включая дочерние подразделения»

продолжение на следующей странице

Таблица 3.71 – продолжение с предыдущей страницы

Привилегии	Особенности работы привилегий
• Users - Read	Привилегия дает права на чтение дополнительных атрибутов пользователей только через API и в базе данных. Для чтения дополнительных атрибутов пользователей через интерфейс ALD Pro (вкладка «Дополнительные сведения» карточки пользователя) необходимы две привилегии: • Users - Read • Users and Groups Settings - Read
• Computers - Remote access	До версии 2.4.0 привилегия распространялась на весь домен. С 2.4.0 привилегия имеет привязку к подразделению
• SUDO Rules - Modify	Для возможности назначения правила SUDO на всех пользователей домена при выборе пункта «Любой пользователь» на вкладке «Пользователи» необходимо, чтобы привилегия входила в роль, которая привязана к корню домена с активным признаком «Включая дочерние подразделения». Для возможности назначения правила SUDO на все компьютеры домена при выборе пункта «Любой компьютер» на вкладке «Компьютеры» необходимо, чтобы привилегия входила в роль, которая привязана к корню домена с активным признаком «Включая дочерние подразделения»
• HBAC Rules - Modify	Для возможности назначения правила HBAC на всех пользователей домена при выборе пункта «Любой пользователь» на вкладке «Пользователи» необходимо, чтобы привилегия входила в роль, которая привязана к корню домена с активным признаком «Включая дочерние подразделения». Для возможности назначения правила HBAC на все компьютеры домена при выборе пункта «Любой компьютер» на вкладке «Компьютеры» необходимо, чтобы привилегия входила в роль, которая привязана к корню домена с активным признаком «Включая дочерние подразделения».

3.25.2. Особенности работы методов PUT и PATCH

При работе этих методов могут не возвращаться ошибки об отсутствии прав на выполнение операций на изменение сущностей.

При методах PUT и PATCH работает следующим образом:

1. выполняется метод GET, который возвращает сущность в текущем состоянии;
2. выполняется метод PUT или PATCH, который меняет сущность;

3. выполняется метод GET, который возвращает измененную сущность.

Если отправлять PUT или PATCH запрос с телом запроса без изменения сущности, выполняется 1-й шаг - метод GET, который возвращает сущность в текущем состоянии, а метод PUT (2-й шаг) не будет выполняться, так как запись не меняется.

В этом случае пользователю без прав на изменение сущности (методами PUT или PATCH) системой не будет выдана ошибка об отсутствии прав на операцию, т.к. эта операция не выполнялась.

Если отправить PUT или PATCH запрос с изменением от пользователя, не имеющем на это права, тогда валидация прав корректно отработает.

3.25.3. Возможные ответы системы на запросы GET при отсутствии прав на выполнение операции

При отсутствии прав на запросы GET система может выдавать следующие варианты ответов:

- сообщение об ошибке на выполнение операции из-за отсутствия прав:

```
// {
    "error": "Отсутствуют права на выполнение данной операции",
    "success": false,
    "code": "ForbiddenError"
}
```

```
// {
    "error": "Отсутствуют права на выполнение данной операции",
    "success": false,
    "code": "DeniedIPAError"
}
```

- успех операции с пустыми списками, для которых указано ненулевое количество записей:

```
// {    "data": [],    "total": 45,    "success": true}
```

- успех операции с пустыми списками, для которых возвращается ноль записей:

```
// {    "data": [],    "total": 0,    "success": true}
```

3.26. Механизм репликации FreeIPA

Репликация — это процесс, в ходе которого содержимое каталога синхронизируется между серверами, за счет чего достигается целостность данных или так называемая конвергентность. В службе каталога **FreeIPA** используется протокол «DS 5.0 multi-supplier incremental replication protocol», в котором учитываются отдельные положения (**RFC3384**).

Каждая Реплика FreeIPA является Мастером, т.е. доступна на запись, и с ее помощью можно вносить изменения в каталог. Разрешение конфликтов основано на использовании меток времени, поэтому для корректной работы механизма крайне важно, чтобы время было синхронизировано между всеми серверами и ни в коем случае не уходило вперед/назад более, чем на сутки, иначе для устранения проблемы искажения времени (too much time skew) может потребоваться восстановления контроллеров из резервной копии.

3.26.1. Соглашения о репликации

На низком уровне репликация проходит по модели **Ведущий-Ведомый** (**Master-Slave**), в рамках которой Сервер, передающий изменения, называется **Поставщиком**, а Сервер, принимающий изменения, называется **Потребителем**. По итогам репликации на **Потребителе** формируется полная копия данных каталога, поэтому его также называют **Репликой**.

Для работы механизма репликации требуется заранее определить топологию домена через создание **Сегментов** и **Соглашений о репликации**. **Сегмент топологии** (**Topology segment**) определяет связь между двумя узлами и является информацией, которая реплицируется в домене между всеми контроллерами, а **Соглашения о репликации** хранятся только на **Поставщике** и содержат настройки для подключения к **Потребителю**. Таким образом, на каждый двусторонний **Сегмент** приходится по два **Соглашения**.

Для управления топологией на портале управления нужно перейти к странице **Управление доменом > Сайты и службы > Соглашения о репликации**, см. *Соглашения о репликации контроллера домена dc-1 с резервным контроллером dc-2*.

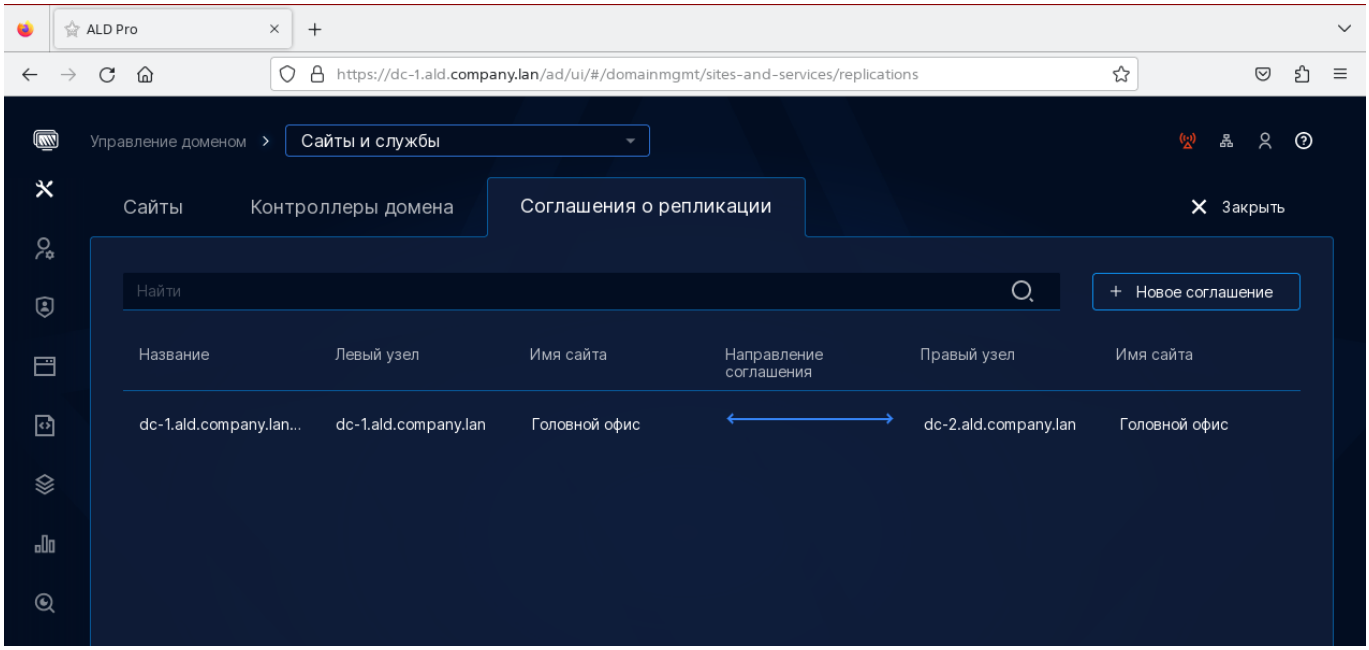


Рисунок 3.101 – Соглашения о репликации контроллера домена **dc-1** с резервным контроллером **dc-2**

В интерфейсе сущности названы **Соглашениями**, но, по сути, это **Сегменты топологии**. Соответствующие **Соглашения о репликации** будут созданы на каждом из контроллеров

домена автоматически, как только ими будет получена информация о соответствующем **Сегменте топологии**, за что отвечает плагин топологии (IPA Topology Configuration).

3.26.2. Порядок решения конфликтов репликации

Репликация всегда инициируется **Поставщиком**, а не **Потребителем** (т.е. работает по модели **Push**). Алгоритм основан на использовании журнала изменений, который хранится в отдельной базе данных, для ALSE до версии 1.7.4 см. файл «/var/lib/dirsrv/slapd-ALD-COMPANY-LOCAL/cldb/*.db», для ALSE 1.7.4 и выше см. файл */var/lib/dirsrv/slapd-ALD-COMPANY-LOCAL/db/userRoot/replication_changelog.db*.

Открыть файл можно командой **dbscan -f**:

```
dbscan -f
/var/lib/dirsrv/slapd-ALD-COMPANY-LOCAL/db/userRoot/replication_change
log.db
```

В сеансе репликации **Поставщик** связывается с **Потребителем**, запрашивает у того сводную информацию о состоянии его репликации (так называемую таблицу RUV, Replica Update Vector), чтобы определить, есть ли у него для **Потребителя** более свежие данные, которые можно было бы передать, и запускает передачу данных. В случае изменения одного и того же атрибута на двух разных контроллерах домена, при репликации приоритет будет выше у последнего изменения по времени.

В случае, когда на нескольких контроллерах одновременно создаются записи с одинаковыми DN, автоматический механизм разрешения конфликтов оставит только ту запись, которая была создана раньше других по метке времени. Остальные записи будут переименованы и скрыты. К имени записи добавляется атрибут `nsuniqueid`, например, дубликат учетной записи пользователя **ivan.kuznetsov** будет называться `nsuniqueid=7341f021-20b331ee-a3ef96ae-a91d3705+uid=ivan.kuznetsov, cn=accounts,dc=ald,dc=company,dc=lan`.

Дополнительно таким записям назначается атрибут `nsds5ReplConflict`, чтобы их было легко найти в каталоге:

```
ldapsearch -H ldap://localhost:389 -x -D "cn=Directory Manager" -W -b
↪"cn=users,cn=accounts,dc=ald,dc=company,dc=local" -s one -a always -z 1000
↪"(|(objectClass=subentry)(objectClass=ldapSubentry))" "hasSubordinates"
↪"objectClass"
```

Если создать пользователя на одном сервере, а на другом сервере удалить структурное подразделение, в котором этот пользователь был создан, то на уровне репликации LDAP конфликт не произойдёт, т.к. отношение пользователя к структурному подразделению в ALD Pro реализуется через атрибут `rbtadp`, а не через связь родительской и дочерней записи. Пользователь не будет отражаться в каком-либо структурном подразделении. Но будет присутствовать в списке всех пользователей.

3.27. Удаление первого контроллера домена

Удаление первого контроллера домена (КД) возможно и при наличии доступа к нему, и если первый контроллер домена недоступен.

3.27.1. Подготовка к удалению

Важно: Во время переноса (удаления) первого КД следует воздержаться от сторонних операций с контроллерами. Минимизировать запросы к LDAP. В процессе процедуры обновления реплики некоторые возможности будут недоступны.

Перед удалением первого КД необходимо проверить наличие `/etc/ssl/freeipa/ca.key` на всех КД с ролью `pkiproxy` и на КД, который предполагается сделать первым.

До начала процедуры удаления первого контроллера домена необходимо произвести следующие действия:

1. Выполнить резервное копирование всех контроллеров домена одним из следующих способов:
    1. создание **снапшотов**,
    2. согласно данной инструкции, при условии, что контроллеры не являются виртуальными машинами.
2. Проверить доступность выделения на `id_range` на новом контроллере. Если пользователи не создавались на контроллерах, отличных от первого, то новые `id_range` предоставлены не будут. Решением проблемы может стать добавление пользователя на любом КД, отличном от первого. Либо, обращение к **LDAP** и изменение `ldif`. Выделяемые на контроллере `id_range` находятся в **LDAP** по пути: `cn=Posix IDs,cn=Distributed Numeric Assignment Plugin,cn=plugins,cn=config`. На новый первый кд можно перенести данные со старого первого КД, используя 2 способа:
    1. `ldapsearch` и `ldapmodify`

```
admin@dc-1:~$ ldapsearch -Q -LLL -b "cn=posix ids,cn=distributed
↪numeric assignment plugin,cn=plugins,cn=config" -o ldif-
↪wrap=no > old.ldif
admin@dc-1:~$ scp old.dif dc-2:/tmp/new.ldif
admin@dc-1:~$ ssh dc-2
admin@dc-2:~$ nano /tmp/new.ldif
---
dn: cn=posix ids,cn=distributed numeric assignment plugin,
↪cn=plugins,cn=config
changetype: modify
replace: dnaMaxValue
dnaMaxValue: [значение]
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
changetype: modify
replace: dnaNextValue
dnaNextValue: [значение]
---
admin@dc-2:~$ ldapmodify /tmp/new.ldif
```

В выводе не должно быть ошибок - строк со словами `Invalid`, `wrong`, `error` и т.д.

Примечание: Показаны примерные данные, которые должны содержаться в файле:

```
admin@dc-2:~$ nano /tmp/new.ldif
---
dn: cn=posix ids,cn=distributed numeric assignment plugin,cn=plugins,
↪cn=config
changetype: modify
replace: dnaMaxValue
dnaMaxValue: [значение]
changetype: modify
replace: dnaNextValue
dnaNextValue: [значение]
```

---

2. `ldapsearch` и `ipa-replica-manage`

```
admin@dc-1:~$ dnamaxvalue=[желаемый максимальный id]
admin@dc-1:~$ let dnaminvalue=$dnamaxvalue-200000
admin@dc-1:~$ sudo ipa-replica-manage dnanextrange-set $HOSTNAME $
↪{dnaminvalue}-${dnamaxvalue}
```

3.27.2. Если контроллер домена недоступен

Если контроллер домена вышел из строя внезапно, и не осталось копии, необходимо:

1. Изменить сервер авторизации для всех серверов мониторинга:
    1. произвести авторизацию по адресу `https://<адрес сервера мониторинга>/zabbix`. Логин и пароль для входа можно узнать с любого контроллера домена при помощи команды:

```
sudo cat /opt/rbta/ad/mgmtportal/api/core/.env | grep ZABBIX
```

    2. слева нажать **Administration - Authentication**;
    3. выбрать вкладку **LDAP settings**;

4. в поле **LDAP host** ввести адрес любого контроллера, кроме первого (который будет удален);

5. нажать кнопку **Update**.

2. Если служба:

```
aldpro-roles-management
```

была запущена на вышедшем из строя контроллере домена, необходимо запустить ее на любом доступном контроллере, необязательно первом. Важно, чтобы она была запущена только на одном контроллере домена.

Чтобы включить службу:

```
systemctl start aldpro-roles-management
```

Чтобы отключить службу:

```
systemctl stop aldpro-roles-management
```

Начиная с версии 2.5.0 **ALD Pro** службы `aldpro-roles-sweeper, aldpro-process-pending-roles, aldpro-check-in-restore` объединены в одну службу `aldpro-roles-management`, сохранившую функционал трех предыдущих. Данная служба имеет созможность форсированной отладки путем изменения интервалов запуска тех или иных функций службы.

Атрибуты службы:

`-r` - период, в который будет запускаться рендер ролей ожидающих активацию (`default: 1m`). Значение `0` отключит данную функцию;

`-f` - период, в который будет запускаться проверка/исправление целостности ролей после репликации (`default: 1h`). Значение `0` отключит данную функцию;

`-u` - период, в который будет запускаться сборщик мусора (`default: 24h`). Значение `0` отключит данную функцию. Формат: целое положительное число [s-секунды | m-минуты | h-часы] либо 0;

`-ust` - примерное время, в которое должен будет запускаться сборщик мусора минимальное значение среди остальных флагов (`default: 00:00`). Формат: часы:минуты.

Период рендера ролей должен быть самым маленьким иначе демон не запустится

Пример передачи аргументов в демона и возврата дефолтных значений:

```
systemctl stop aldpro-roles-management
systemctl set-environment ROLES_DAEMON_ARGS="-r 10s -f 15s"
systemctl start aldpro-roles-management
```

Пример возврата работы демона на значениях по умолчанию:

```
systemctl stop aldpro-roles-management
systemctl unset-environment ROLES_DAEMON_ARGS
systemctl start aldpro-roles-management
```

3. Удалить первый контроллер домена из всех серверов мониторинга:
    1. произвести авторизацию на сервере мониторинга;
    2. слева нажать **Configuration - Hosts**;
    3. отметить галкой нужный сервер и нажать кнопку **Delete**.
4. Проверить, что на КД, который заменит первый имеется файл `/etc/ssl/freeipa/ca.key`.
5. Адреса контроллеров в файле `/etc/resolv.conf`
    1. На каждом компьютере в домене в файле `/etc/resolv.conf` необходимо изменить адрес удаляемого сервера на адрес любого другого. Пример: Если адрес первого контроллера домена `10.2.0.10`, а адрес второго контроллера домена `10.2.0.11`, то содержимое файла должно быть следующим:

```
domain <имя домена>
nameserver 10.2.0.11
```

    2. Данное действие можно выполнить при помощи задания автоматизации или групповой политикой. Пример кода:

```
replace_string:
  file.replace:
      - name: /etc/resolv.conf
      - pattern: 10.2.0.10
      - repl: 10.2.0.11
```

6. Адреса контроллеров в файле `/etc/sssd/sssd.conf`

На каждом компьютере в домене в файле `/etc/sssd/sssd.conf` необходимо изменить адрес удаляемого сервера на адрес любого другого. Пример:

```
[domain/ald.company.lan]
...
ipa_server = _srv_,<fqdn.НОВОГО.КД>
...
```

Важно помнить, что на контроллерах домена параметр будет содержать собственный адрес, его менять не следует.

7. На всех клиентах (в т.ч. части серверной группировки), которые вводились в домен через удаляемый контроллер внести изменения в файл `/etc/ldap/ldap.conf`:

```
...
URI ldaps://<fqdn.НОВОГО.КД>
...
```

8. На всех клиентах (в т.ч. части серверной группировки), которые вводились в домен через удаляемый контроллер внести изменения в файл `/etc/ipa/default.conf`:

```
[global]
...
server = <fqdn.НОВОГО.КД>
...
xmlrpc_uri = https://<fqdn.НОВОГО.КД>/ipa/xml
...
```

9. Перезапустить службы sssd после изменения параметров:

```
sudo systemctl restart sssd
```

10. Внести изменения в параметры **DNS** зон (**Роли и службы сайта > Служба разрешения имён**):

    1. выбрать прямую зону, открыть ее записи, перейти в **Параметры зоны**, изменить **Полномочный сервер имён** на fqdn нового «первого» контроллера;

    2. выбрать обратную зону, открыть ее записи, перейти в **Параметры зоны**, изменить **Полномочный сервер имён** на fqdn нового «первого» контроллера.

11. Если есть только 1 корневой `NTP-сервер` (**Роли и службы сайта > Служба синхронизации времени > Корневые NTP-серверы домена**) добавить новый, выбрав новый «первый» КД из доступных. Удалить тот, который ссылается на контроллер, который будет удален. После действий проверить изменения в **LDAP**:

```
suffix=$(ldapsearch -Q -LLL -s base|grep dn:|cut -d ' ' -f2)
ldapsearch -Q -LLL -b cn=ntp,cn=services,cn=aldpro,cn=etc,$suffix -o ldif-
↪wrap=no
```

Важно помнить, что если много внешних `ntp-серверов` в конец запроса можно добавить `isexternal=FALSE`, тогда не будут показаны внешние сервера.

12. Убедиться, что между удаляемым контроллером домена и другим контроллером домена установлены двусторонние соглашения о репликации. Сделать это можно двумя способами:

    1. На портале управления в разделе **Управление доменом - Сайты и службы - Соглашения о репликации** должны быть двусторонние стрелки между контроллерами домена.

    2. В консоли любого контроллера домена командой (вместо `dc=aldpro,dc=test` необходимо подставить имя своего домена):

    ```
    suffix=$(ldapsearch -Q -LLL -s base|grep dn:|cut -d ' ' -f2)
    ldapsearch -D -Q -LLL "cn=directory manager" -W -b "cn=topology,cn=ipa,
    ↪cn=etc,$suffix"
    unset suffix
    ```

    В выводе команды должно быть `ipaReplTopoSegmentDirection: both` для всех контроллеров домена.

    3. Если это не так, необходимо восстановить репликации. В противном случае, удаление контроллера домена будет невозможно.

13. Проверить репликацию между удаляемым КД и новым «первым» КД. Проверить не идет ли в данный момент синхронизация:

```
suffix=$(ldapsearch -Q -LLL -s base|grep dn:|cut -d ' ' -f2)
ds-replcheck online -D "cn=Directory Manager" -m ldap://<fqdn.старого.кд>
 ↪:389 -r ldap://<fqdn.новоого.кд>:389 -b $suffix
dsconf -j ALD-COMPANY-LAN replication status --suffix $domain_name|grep
 ↪update-in-progres -A1
unset suffix
```

В случае отсутствия команды `dsconf` следует установить ее следующей командой:

```
sudo apt-get install python3-lib389
```

Важно помнить, что не должны совпадать `krbloginfailedcount`. Если идет репликация - дождаться окончания.

14. На новом первом КД внести изменения: значения атрибута `rbtaSubsystemConfig` должны соответствовать `"is_master": true, "setup_pkiproxy": true`:

```
suffix=$(ldapsearch -Q -LLL -s base|grep dn:|cut -d ' ' -f2)
ldapsearch -Q -LLL -b cn=computers,cn=accounts,$suffix fqdn=*$HOSTNAME* dn
 ↪rbtaSubsystemConfig -o ldif-wrap=no > new-config.ldif
nano new-config.ldif
---
dn: fqdn=dc-2.ald.company.test,cn=computers,cn=accounts,dc=ald,dc=company,
 ↪dc=test
changetype: modify
replace: rbtaSubsystemConfig
rbtaSubsystemConfig: {"config_state": "applied", "is_master": true, "setup_gc
 ↪": true, "setup_pkiproxy": true, "setup_syncer": true, "config_state_local
 ↪": "applied"}
---
ldapmodify -f new-config.ldif
```

3.27.3. Удаление контроллера домена

1. От имени `root`'а на НОВОМ первом КД выполнить команду:

   ```
   ipa-replica-manage del <fqdn.старого.кд>
   ```

2. Авторизоваться на портале управления по адресу `https://<fqdn.НОВОГО.КД>`

3. Проверить успешность удаления можно на портале управления в разделе **Управление доменом - Сайты и службы - Контроллеры домена**. Удаленного контроллера домена не должно быть в списке.

4. Зайти в раздел **Роли и службы сайта - Служба разрешения имён**.
5. В списке **Имя зоны** кликнуть на имя вашего домена.
6. В строке поиска набрать имя удаленного контроллера домена.
7. Галочкой выделить все появившиеся записи и нажать кнопку **Удалить**.
8. Пункты 6-7 повторить до полного удаления всех записей, относящихся к удаленному контроллеру домена.
9. Запустить процедуру обновления первого КД. Важно помнить, что у модуля синхронизации локальная база данных, нужно выполнить перенос базы:

```
aldpro-server-install -d $(hostname -d) -n $(hostname -s) --ip $(hostname -
↪i) --setup_syncer --setup_gc --no-reboot --update
```

После ввода команды система запросит ввести пароль администратора домена.

Внимание: Если после удаления контроллера домена подсистемы невозможно развернуть, необходимо проверить содержимое файла `/etc/resolv.conf` на компьютере, на котором будет развернута подсистема - в файле не должно быть адреса удалённого КД

3.28. Удаление резервного контроллера домена

3.28.1. Подготовка к удалению

1. Удалить контроллер домена (КД) из всех серверов мониторинга.
2. Адреса контроллеров в файле `/etc/resolv.conf`
    1. На каждом компьютере в домене в файле `/etc/resolv.conf` необходимо изменить адрес удаляемого сервера на адрес любого другого.
    2. Данное действие можно выполнить при помощи задания автоматизации или групповой политикой. Пример кода:

```
replace_string:
  file.replace:
      - name: /etc/resolv.conf
      - pattern: 10.2.0.11
      - repl: 10.2.0.12
```

3. Адрес контроллера в файле `/etc/sssd/sssd.conf`. На каждом компьютере в домене, который вводился через удаляемый КД в файле `/etc/sssd/sssd.conf` необходимо изменить адрес удаляемого сервера на адрес любого другого. Пример:

```
[domain/ald.company.lan]
...
ipa_server = _srv_,<fqdn.НЕ.УДАЛЯЕМЫЙ.КД>
...
```

Важно помнить, что на контроллерах домена параметр будет содержать собственный адрес, его менять не следует.

4. На всех клиентах (в т.ч. части серверной группировки), которые вводились в домен через удаляемый контроллер внести изменения в файл `/etc/ldap/ldap.conf`:

```
URI ldaps://<fqdn.НЕ.УДАЛЯЕМЫЙ.КД>
```

5. На всех клиентах (в т.ч. части серверной группировки), которые вводились в домен через удаляемый контроллер внести изменения в файл `/etc/ipa/default.conf`:

```
[global]
...
server = <fqdn.НЕ.УДАЛЯЕМЫЙ.КД>
...
xmlrpc_uri = https://<fqdn.НЕ.УДАЛЯЕМЫЙ.КД>/ipa/xml
...
```

6. Перезапустить службы sssd после изменения параметров:

```
sudo systemctl restart sssd
```

7. Убедиться, что контроллер не является единственным связующим звеном сегментов топологии, то есть при удалении не должно возникнуть разрыва между любыми КД, это можно сделать через портал управления **Управление доменом > Общая информация > Граф топологии**.

3.28.2. Удаление контроллера домена

1. От имени `root`'а на любом КД, отличном от удаляемого, выполнить команду

```
ipa-replica-manage del <fqdn.удаляемого.кд>
```

2. Авторизоваться на портале управления по адресу `https://<fqdn.первый.КД>`

3. Проверить успешность удаления можно на портале управления в разделе **Управление доменом - Сайты и службы - Контроллеры домена.** Удаленного контроллера домена не должно быть в списке

4. Зайти в раздел **Роли и службы сайта - Служба разрешения имён**

5. В списке **Имя зоны** кликнуть на имя своего домена

6. В строке поиска набрать имя удаленного контроллера домена

7. Галочкой выделить все появившиеся записи и нажать кнопку **Удалить**

8. Пункты 6-7 повторить до полного удаления всех записей, относящихся к удаленному контроллеру домена

Внимание: Если после удаления контроллера домена подсистемы невозможно развернуть, необходимо проверить содержимое файла /etc/resolv.conf на компьютере, на котором будет развернута подсистема - в файле не должно быть адреса удалённого КД.

3.29. Обновление подсистем ALD Pro через портал управления

В системе с версии 2.2.0 внедрен функционал централизованного обновления **aldpro-client** на компьютерах домена через **Портал Управления**. Функционал реализован в виде Политик обновления ALD Pro и функционирует аналогично **Групповым Политикам** по pull-модели. **Standalone-миньон** - автономный клиент на компьютерах домена для запуска заданий и локальных задач без подключений к мастеру - отвечает за формирование *source.list* и обновление **aldpro-client** при появлении новых версий **ALD Pro** в репозиториях, повышая гибкость и автономность процесса обновления на компьютерах клиентов.

Управление политикой обновления осуществляется через интерфейс **Портала Управления** в разделе **Установка и обновление ПО** – **Политики обновления ALD Pro**:

Для создания новой политики обновления ALD Pro необходимо нажать на кнопку [**+ Новая политика обновления**]. Будет выполнен переход на карточку новой политики.

На карточке на вкладке **Основное** задать имя политики обновления ALD Pro. Также можно указать описание политики. Указать статус политики: [**Включена**] и нажать кнопку [**Сохранить**] (рис. 3.2).

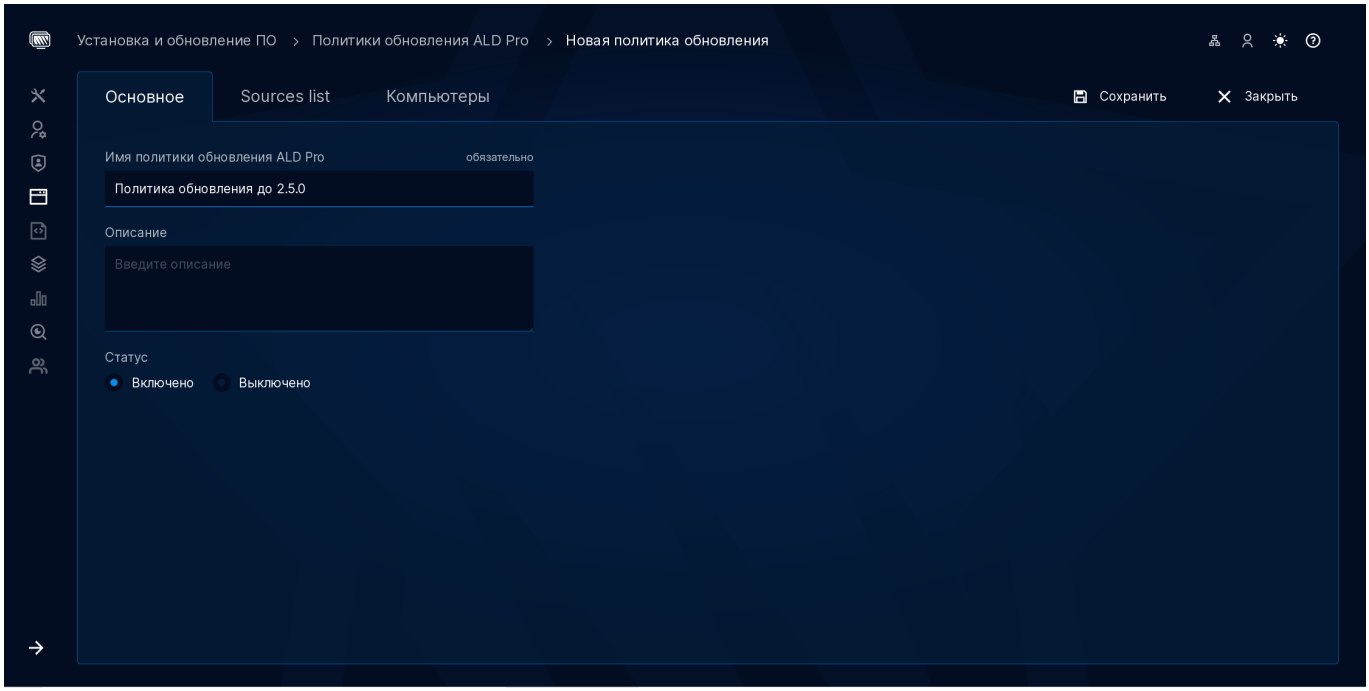


Рисунок 3.102 – Создание Групповой Политики обновления подсистем. Вкладка «Основное»

На вкладке **Source list** нажать кнопку [**Редактировать**] и ввести:

```
deb https://dl.astralinux.ru/aldpro/frozen/01/2.5.0/ 1.7_x86-64 main base
```

Затем оставить внизу комментарий (обязательно) и нажать кнопку [**Сохранить**].

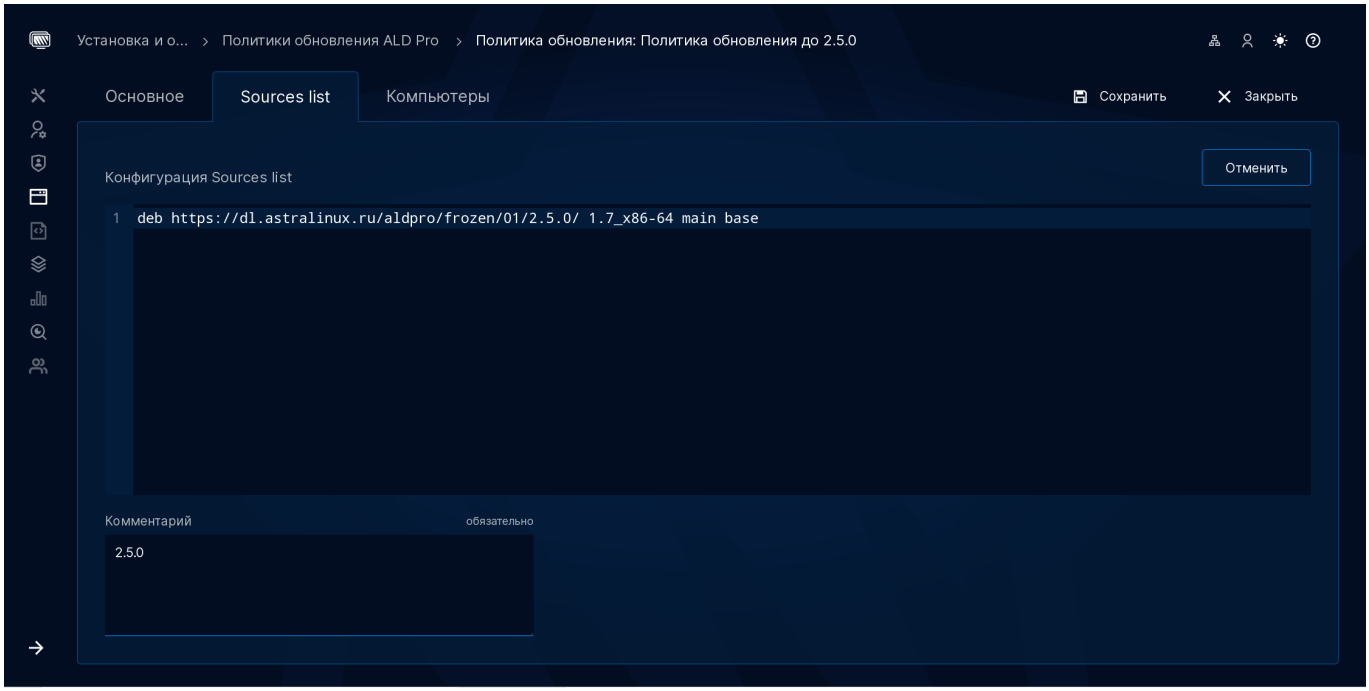


Рисунок 3.103 – Создание Групповой Политики обновления подсистем. Вкладка «Source list»

На вкладке **Компьютеры** указать все компьютеры или группы компьютеров, требующих обновления:

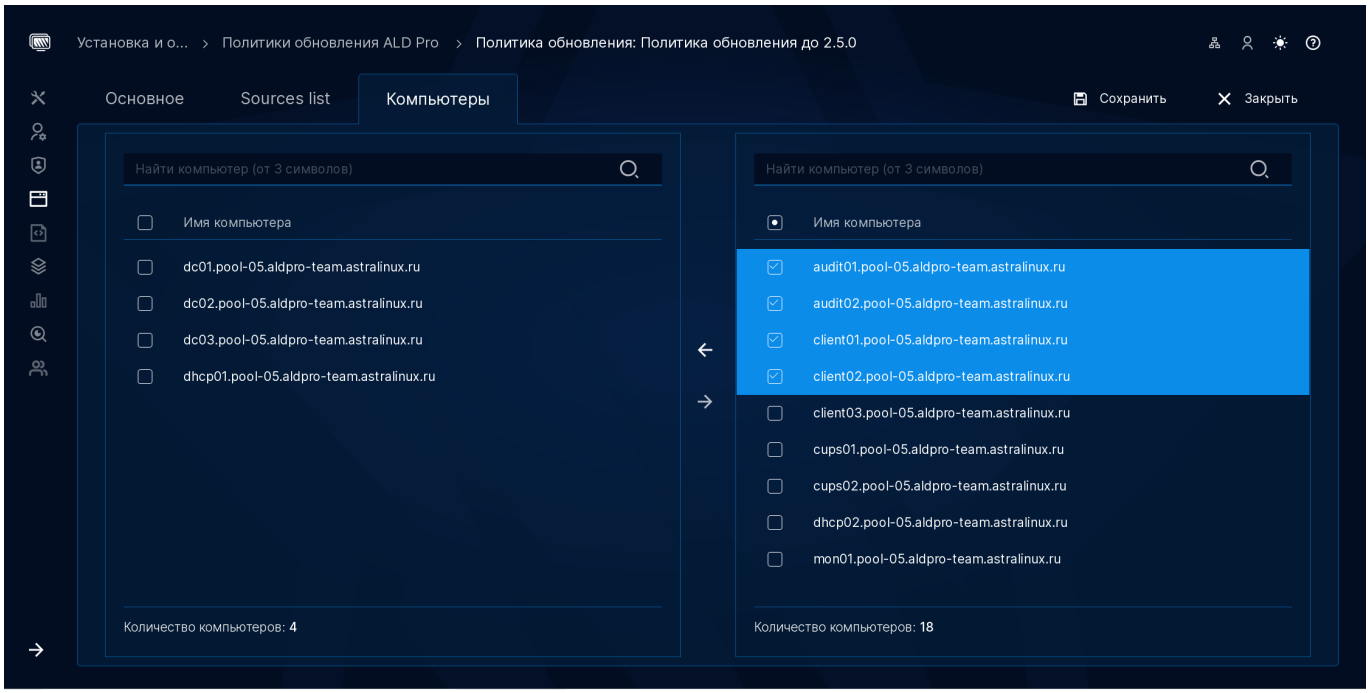


Рисунок 3.104 – Создание Групповой Политики обновления подсистем. Вкладка «Компьютеры»

Важно: При запуске политики обновления проверяется значение osfamily компьютера и, в зависимости от него, формируется разный путь к источнику обновлений на клиенте.

Для **ALSE 1.7**, **1.8** и всех оперативных обновлений `sources.list` расположен по пути `/etc/apt/sources.list.d/aldpro.list`.

Для клиентов с **Альт Рабочая станция 10.4** и **Альт СП 10** - `etc/apt/sources.list.d/aldpro.list`.

Для клиентов с **ОС РЕД ОС 7.3** и **РЕД ОС 8** - `/etc/yum.repos.d/aldpro.repo`.

Для более удобной и правильной работы политик обновления ALD Pro и указания `sources.list` рекомендуется создавать отдельные политики для каждой ОС.

Политика обновления выполняется раз в сутки по таймеру.

Начиная с версии 2.3.0 после создания ГП и перед обновлением клиента, необходимо **на компьютере подсистемы Общего Доступа к Файлам** выполнить следующую команду:

```
kdestroy -A
```

Для проверки успешного применения политик обновления необходимо выполнить следующие команды (при условии, что в */etc/apt/sources.list.d/aldpro.list* указан репозиторий с версией выше, чем установлена на компьютере):

```
# Проверка версии aldpro-client
apt-cache policy aldpro-client
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
# Проверка версий зависимостей
apt-cache policy astra-freeipa-client salt-minion zabbix-agent python3 aldpro-
↪client-rdm syslog-ng initramfs-tools aldpro-common python3-distro python3-
↪yaml aldpro-policy-manager
```

Форсированное применение политики:

```
aldpro-salt-call aldpro_update_policy.build_and_run_updatepolicy
```

`Verbose=True` указывает на необходимость вывода подробной информации, а `force=True` обозначает, что нужно очистить кэши перед началом работы команды. По умолчанию оба параметра имеют значение `False`.

```
aldpro-salt-call aldpro_update_policy.build_and_run_updatepolicy force
```

Если политика была успешно применена, в выводе будут строки, подобные следующим:

```
aldpro-client:
    new:
        2.5.0
    old:
        2.4.0-8
```

Для принудительного обновления пакетов ALD Pro в терминале клиентов:

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

Так же необходимо в версии ALD Pro 2.5.0 выполнить принудительно через терминалы клиентов скачивание и установку последней версии **Policy Manager**:

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

Для повышения производительности домена с помощью Групповой Политики можно отключить связь с **salt master-minion** в разделе **Групповые Политики** на вкладке **Параметры компьютеров** в папке **Система** (рис. 3.5):

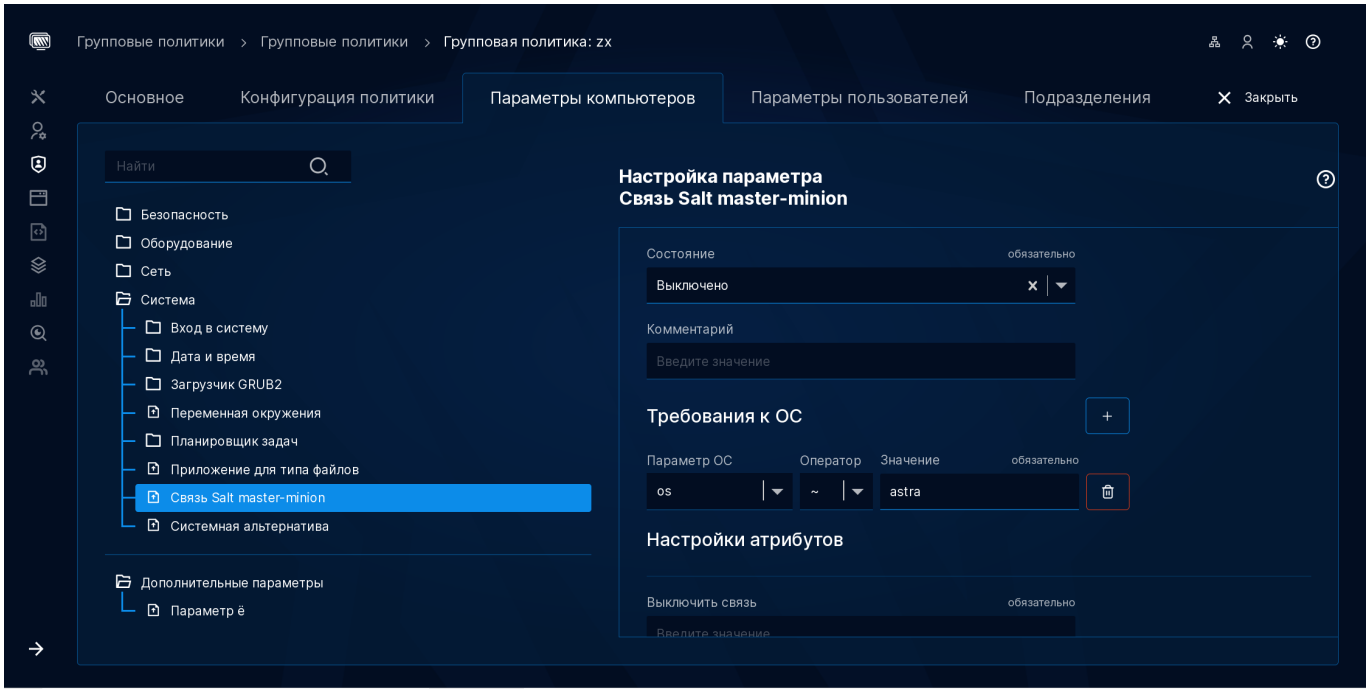


Рисунок 3.105 – Перевести состояние параметра в режим «Выключено»

Принудительное применение ГП:

```
sudo aldpro-gpupdate --gp
```

В связи с тем, что реализован функционал централизованного обновления **Policy Manager** на клиентских компьютерах, для применения ГП необходимо дождаться загрузки актуального **Policy Manager** на клиент, что занимает максимум 80 минут. Ожидание применения ГП на клиенте также составляет максимум 80 минут. Таким образом, максимальное время применения ГП - 160 минут.

Обновление подсистем запускается в карточке подсистемы из списка, находящегося в **Управление доменом** - **Общая информация** - **Состав системы** (рис. 3.5):

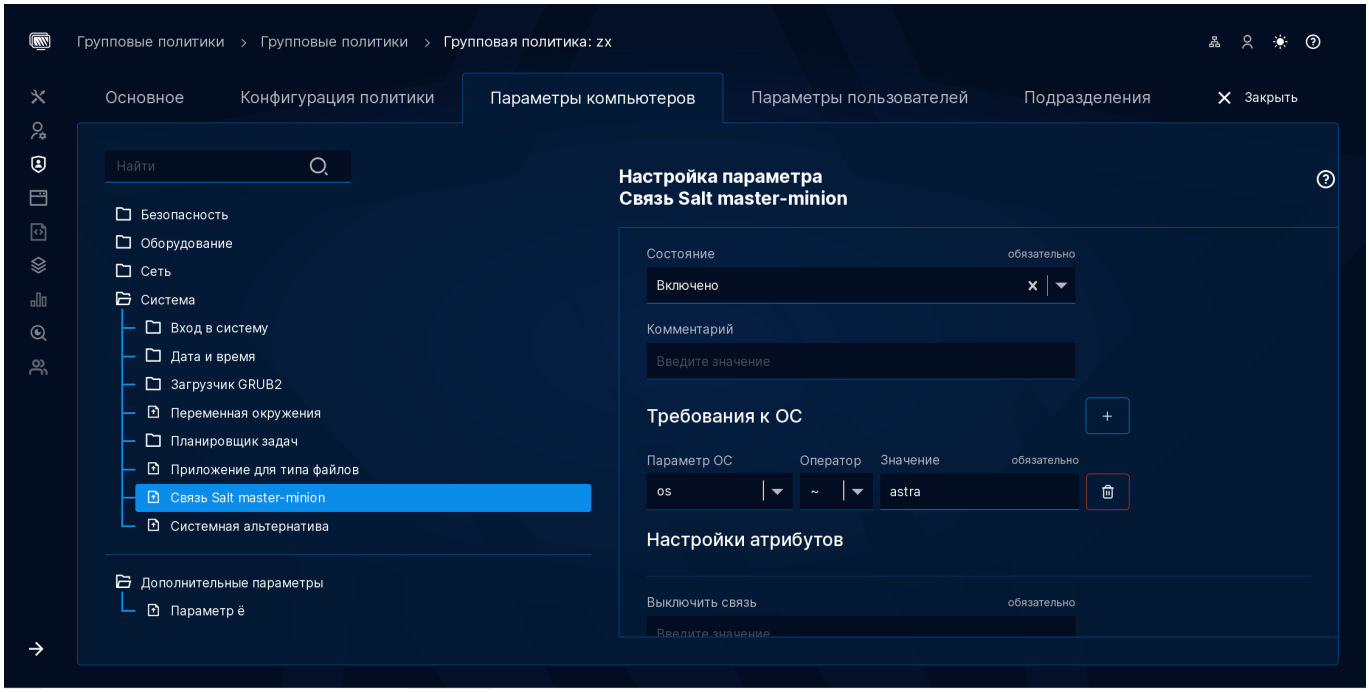


Рисунок 3.106 – Перевести состояние параметра в режим **Включено**

Обновление запускается кнопкой [**Обновить ALD Pro**] (рис. 3.6):

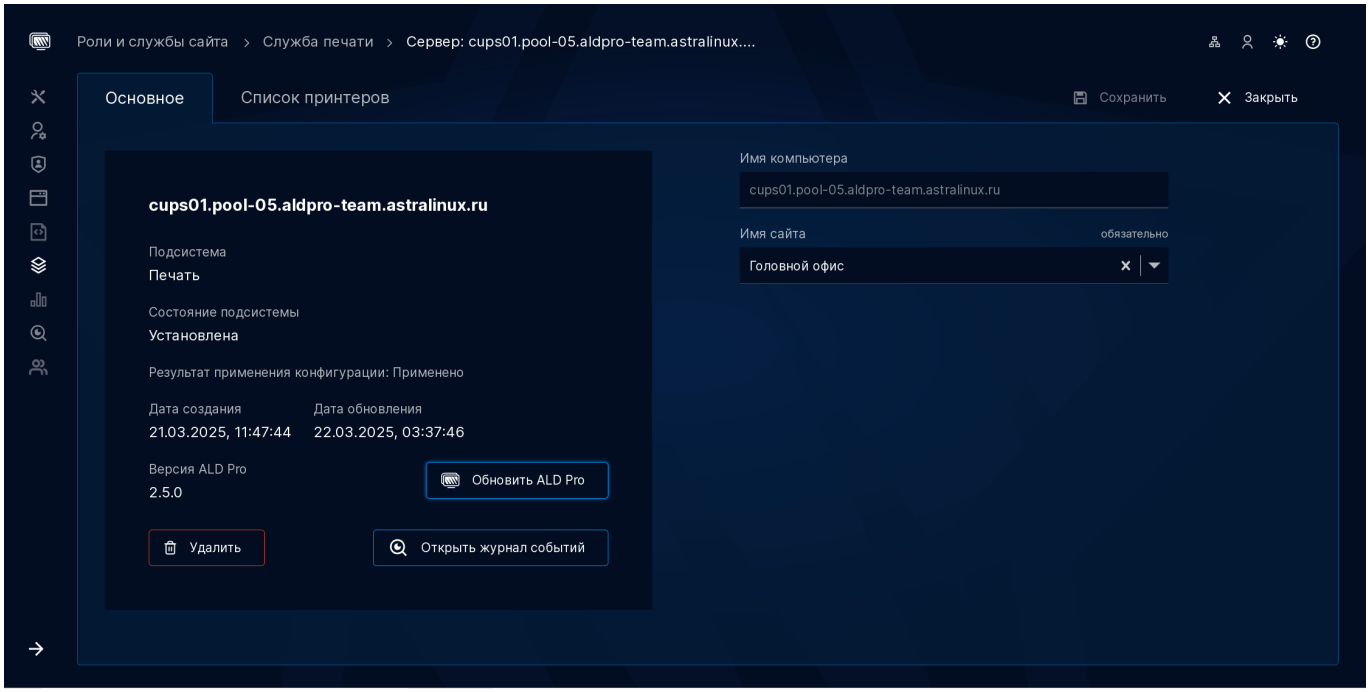


Рисунок 3.107 – Карточка подсистемы

На клиенте выполнить форсированное применение обновления:

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

Для лучшего контроля за процессом обновления реплик рекомендуется использовать форсированное обновление из командной строки на реплике:

```
aldpro-roles --iud --action update
```

В случае успешного обновления ALD Pro на компьютере подсистемы карточка подсистемы будет выглядеть так (рис. 3.7):

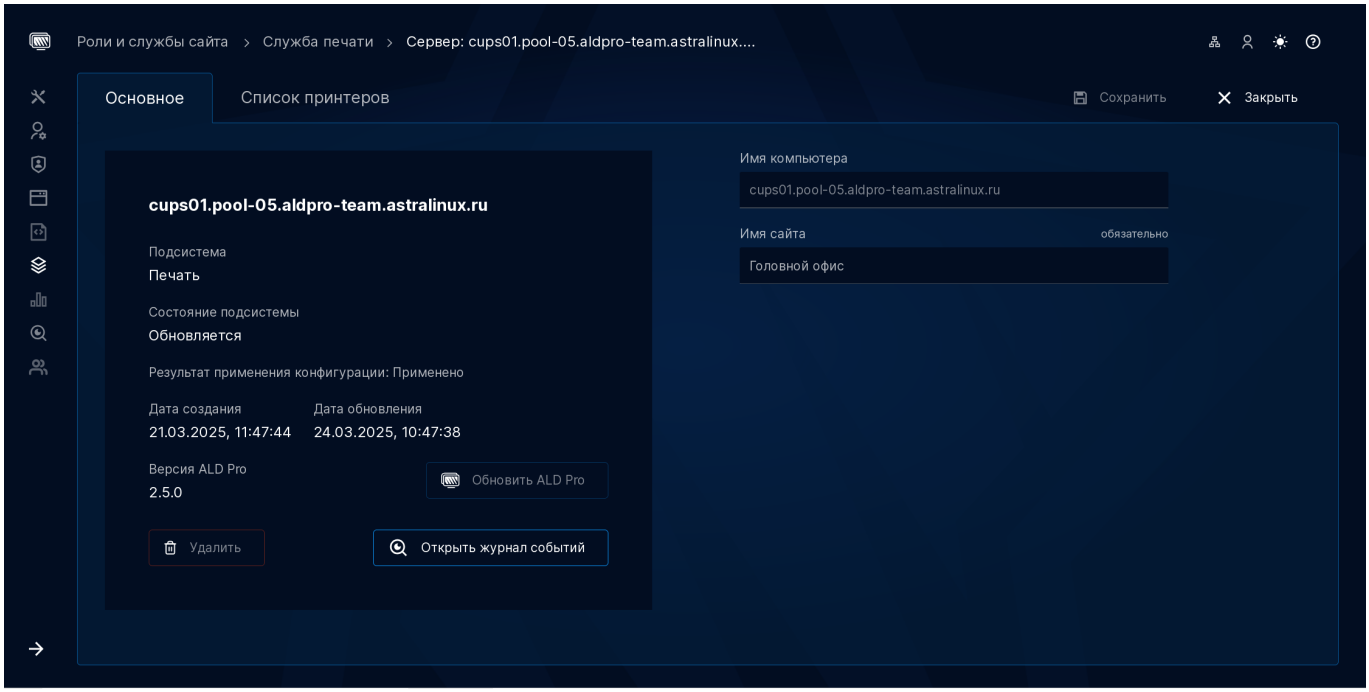


Рисунок 3.108 – Карточка подсистемы после успешного обновления

Если в процессе обновления что-то пошло не так, в карточке подсистемы будет отображаться ошибка.

3.30. Проверка работы сервисов ALD Pro

Для проверки работоспособности сервисов **ALD Pro** добавлена утилита **aldproctl**, которая расширяет функционал **ipactl**, проверяя также сервисы **ALD Pro**.

3.30.1. Конфигурация

Файл конфигурации имеет три обязательных блока: **FreeIPA**, **ALD Pro** и **Other**. Для начала работы необходимо скопировать файл *aldproctl.env* и внести перечень сервисов для проверки по примеру ниже:

```
[FreeIPA]
Directory Service
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
krb5kdc
kadmin
named
httpd
ipa-custodia
smb
winbind
ipa-otpd
ipa-dnskeysyncd
[ALD Pro]
GLOBAL-CATALOG
GCSync
aldpro-mp-services
aldpro-canclient
ad-salt-canrunner
syncer
syncer.timer
[Other]
celery
celerybeat
```

Примечание: Название сервисов в конфигурационном файле должны полностью соответствовать примеру. Ниже приведен список сервисов, доступных к проверке:

- Directory Service
- krb5kdc
- kadmin
- named
- httpd
- ipa-custodia
- smb
- winbind
- ipa-otpd
- ipa-dnskeysyncd
- dirsrv@GLOBAL-CATALOG
- ipa-gcsync
- celery
- celerybeat
- aldpro-mp-service
- aldpro-canclient
- ad-salt-canrunner
- syncer

- syncer.timer

3.30.2. Перечень команд

Для выполнения команд с сервисами используется `systemctl`.

Команда	Описание
`sudo aldproctl -h`	Отображает сп
`sudo man aldproctl`	Отображает ра
`sudo aldproctl --version`	Отображает ис
`sudo aldproctl start|stop|restart|status --timeout=TIMEOUT`	Устанавливает
`sudo aldproctl start`	Запускает серв
`sudo aldproctl status`	Отображает ст
`sudo aldproctl stop`	Останавливает
`sudo aldproctl restart`	Перезапускает
`sudo aldproctl start|stop|restart|status --service=service_name`	Флаг `service`
`sudo aldproctl start|stop|restart|status --ipa-check-only`	Флаг `-i`, `--ipa`
`sudo aldproctl start|stop|restart|status --aldpro-check-only`	Флаг `-a`, `--ald`
`sudo aldproctl start|stop|restart|status --other-check-only`	Флаг `-o`, `--oth`

Перечень команд

3.30.3. Варианты отображения статуса сервиса

- ЗАПУЩЕН - команда start сработала без ошибок и сервис запустился
- ОСТАНОВЛЕН - команда stop сработала без ошибок и сервис остановлен
- ПЕРЕЗАПУЩЕН - команда restart сработала без ошибок и сервис перезапущен
- НЕ НАЙДЕН - сервис с таким именем не найден
- НЕАКТИВЕН (МЕРТВ) - сервис неактивен
- ОШИБКА - ошибка при вызове команды или работе сервиса
- ПРЕВЫШЕНО ВРЕМЯ ОЖИДАНИЯ - превышено время выполнения операции

3.31. Проверка статуса репликации

3.31.1. Проверка статуса репликации утилитой dsconf

Чтобы получить детальную информацию по соглашениям о репликации текущего сервера, нужно выполнить следующую команду:

```
sudo dsconf -j ALD-COMPANY-LAN replication status --suffix dc=ald,dc=company,
↪dc=lan
```

Информация будет предоставлена в json-формате:

```
{
    "type": "list", "items": [{
        "agmt-name": ["meTodc-2.ald.company.lan"],
        "replica": ["dc-2.ald.company.lan:389"],
        "replica-enabled": ["on"],
        "update-in-progress": ["FALSE"],
        "last-update-start": ["20230824143651Z"],
        "last-update-end": ["20230824143651Z"],
        "number-changes-sent": ["4:25/723 5:1/0 "],
        "number-changes-skipped": ["unavailable"],
        "last-update-status": ["Error (0) Replica acquired successfully:
↪Incremental update succeeded"],
        "last-init-start": ["20230824120948Z"],
        "last-init-end": ["20230824120954Z"],
        "last-init-status": ["Error (0) Total update succeeded"],
        "reap-active": ["0"],
        "replication-status": ["Not in Synchronization: supplier
↪(64e76843000000040000) consumer (Unavailable) State (green) Reason (error
↪(0) replica acquired successfully: incremental update succeeded)"],
        "replication-lag-time": ["unavailable"]
    }]
}
```


Полученную информацию можно представить в формате таблицы, но потребуется установить пакет `jq` и использовать комплексную команду форматирования, которую можно сохранить в виде скрипта:

```
sudo apt install jq -y

(printf 'SUFFIX \tAGREEMENT \tSTATE \tTIME-SINCE \tLDAP-STATUS \tREPL-STATUS \
↪n'; sudo dsconf -j ALD-COMPANY-LAN replication list | jq '.items[]' -r |
↪xargs -P8 -i -- sudo dsconf -j ALD-COMPANY-LAN repl-agmt list --suffix={}
↪| jq '.items[].attrs | (.nsds5replicalastupdatestatusjson[0] | fromjson)
↪as $status | [.nsds5replicaroot[0], .cn[0], $status.state, $status.date,
↪$status.ldap_rc_text, $status.repl_rc_text] | @tsv' -r | sort ) | column -s
↪$'\t' -t
```

Результат выполнения команды смотри на рисунке *Состояние соглашений о репликации в табличном виде*.

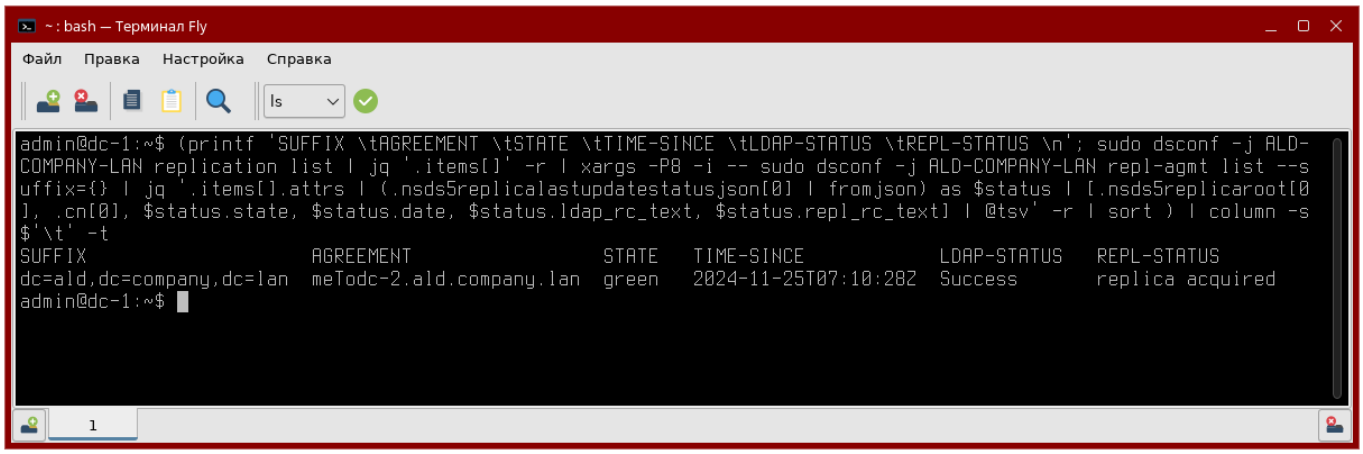


Рисунок 3.109 – Состояние соглашений о репликации в табличном виде

Есть также возможность с помощью команды `replication monitor` утилиты `dsconf` собрать информацию сразу со всех контроллеров домена, но в состоянии репликации не будет указан агрегированный статус, что затруднит анализ:

```
sudo dsconf ldap://localhost:389 replication monitor
```

Для каждого сервера в домене нужно будет ввести учетные данные пользователя `cn=Directory Manager`:

```
Enter Bind DN: cn=Directory Manager
Enter password for cn=Directory Manager on ldap://localhost:389: *****

Enter a bind DN for dc-2.ald.company.lan:389: cn=Directory Manager
Enter a password for cn=Directory Manager on dc-2.ald.company.lan:389: *****
```

Чтобы не вводить учетные данные каждый раз вручную, на рабочей станции администратора их можно определить в текстовом файле `~/.dsrc`:

```
[repl-monitor-connections]
connection1 = dc-1.ald.company.lan:389:cn=Directory Manager:*
connection2 = dc-2.ald.company.lan:389:cn=Directory Manager:[~/pwd.txt]
connection3 = dc-3.ald.company.lan:389:cn=Directory Manager:S3cret
```

Где:

- для dc-1 будет запрошен пароль;
- для dc-2 пароль будет взят из файла `pwd.txt`;
- для dc-3 в качестве пароля будет использована строка `S2cret`.

3.31.2. Проверка репликации с помощью скриптов checkipaconsistency

Внимание: В данном разделе представлена информация о том, как можно проверить целостность домена с использованием модуля **checkipaconsistency** из публичного pip-репозитория, установка которого в продуктивных средах без дополнительной проверки скриптов категорически запрещается.

Сначала проверьте текущую версию Python, в ALSE 1.7.xxx по умолчанию устанавливается 3.7.3:

```
sudo python3 -V
Python 3.7.3
```

Скачайте установочный файл системы управления пакетами `pip` соответствующей версии:

```
wget https://bootstrap.pypa.io/pip/3.7/get-pip.py

--2024-11-25 10:44:34--  https://bootstrap.pypa.io/pip/3.7/get-pip.py
Распознаётся bootstrap.pypa.io (bootstrap.pypa.io)… 151.101.84.175,
 ↪2a04:4e42:14::175
Подключение к bootstrap.pypa.io (bootstrap.pypa.io)|151.101.84.175|:443...
 ↪соединение установлено.
HTTP-запрос отправлен. Ожидание ответа… 200 OK
Длина: 2636033 (2,5M) [text/x-python]
Сохранение в: «get-pip.py»

get-pip.py                                          100
 ↪%[=================================================================================
 ↪]   2,51M  5,32MB/s    за 0,5s

2024-11-25 10:44:35 (5,32 MB/s) - «get-pip.py» сохранён [2636033/2636033]
```

Установите `pip`:

```
sudo python3 ./get-pip.py

Collecting pip<24.1
Downloading pip-24.0-py3-none-any.whl.metadata (3.6 kB)
Collecting wheel
Downloading wheel-0.42.0-py3-none-any.whl.metadata (2.2 kB)
Downloading pip-24.0-py3-none-any.whl (2.1 MB)
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 2.1/2.1 MB 4.4 MB/s eta 0:00:00
Downloading wheel-0.42.0-py3-none-any.whl (65 kB)
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 65.4/65.4 kB 1.3 MB/s eta 0:00:00
DEPRECATION: python-apt 1.8.4.3-ci202309111239-astra1-b1 has a non-standard
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
 ↪version number. pip 24.1 will enforce this behaviour change. A possible
 ↪replacement is to upgrade to a newer version of python-apt or contact the
 ↪author to suggest that they release a version with a conforming version
 ↪number. Discussion can be found at https://github.com/pypa/pip/issues/12063
Installing collected packages: wheel, pip
Successfully installed pip-24.0 wheel-0.42.0
WARNING: Running pip as the 'root' user can result in broken permissions and
 ↪conflicting behaviour with the system package manager. It is recommended
 ↪to use a virtual environment instead: https://pip.pypa.io/warnings/venv
```

Установите модуль `checkipaconsistency`:

```
sudo python3 -m pip install checkipaconsistency

Collecting checkipaconsistency
Downloading checkipaconsistency-2.7.10-py2.py3-none-any.whl.metadata (9.6 kB)
Collecting pplogger (from checkipaconsistency)
Downloading pplogger-4.2.0-py2.py3-none-any.whl.metadata (1.4 kB)
Requirement already satisfied: python-ldap in /usr/lib/python3/dist-packages
 ↪(from checkipaconsistency) (3.1.0)
Collecting prettytable (from checkipaconsistency)
Downloading prettytable-3.7.0-py3-none-any.whl.metadata (26 kB)
Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages
 ↪(from checkipaconsistency) (1.16.0)
Collecting importlib-metadata (from prettytable→checkipaconsistency)
Downloading importlib_metadata-6.7.0-py3-none-any.whl.metadata (4.9 kB)
Collecting wcwidth (from prettytable→checkipaconsistency)
Downloading wcwidth-0.2.13-py2.py3-none-any.whl.metadata (14 kB)
Collecting zipp>=0.5 (from importlib-
 ↪metadata→prettytable→checkipaconsistency)
Downloading zipp-3.15.0-py3-none-any.whl.metadata (3.7 kB)
Collecting typing-extensions>=3.6.4 (from importlib-
 ↪metadata→prettytable→checkipaconsistency)
Downloading typing_extensions-4.7.1-py3-none-any.whl.metadata (3.1 kB)
Downloading checkipaconsistency-2.7.10-py2.py3-none-any.whl (24 kB)
Downloading pplogger-4.2.0-py2.py3-none-any.whl (14 kB)
Downloading prettytable-3.7.0-py3-none-any.whl (27 kB)
Downloading importlib_metadata-6.7.0-py3-none-any.whl (22 kB)
Downloading wcwidth-0.2.13-py2.py3-none-any.whl (34 kB)
Downloading typing_extensions-4.7.1-py3-none-any.whl (33 kB)
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
Downloading zipp-3.15.0-py3-none-any.whl (6.8 kB)
DEPRECATION: python-apt 1.8.4.3-ci202309111239-astra1-b1 has a non-standard
 ↪version number. pip 24.1 will enforce this behaviour change. A possible
 ↪replacement is to upgrade to a newer version of python-apt or contact the
 ↪author to suggest that they release a version with a conforming version
 ↪number. Discussion can be found at https://github.com/pypa/pip/issues/12063
Installing collected packages: wcwidth, pplogger, zipp, typing-extensions,
 ↪importlib-metadata, prettytable, checkipaconsistency
Successfully installed checkipaconsistency-2.7.10 importlib-metadata-6.7.0
 ↪pplogger-4.2.0 prettytable-3.7.0 typing-extensions-4.7.1 wcwidth-0.2.13
 ↪zipp-3.15.0
WARNING: Running pip as the 'root' user can result in broken permissions and
 ↪conflicting behaviour with the system package manager. It is recommended
 ↪to use a virtual environment instead: https://pip.pypa.io/warnings/venv
```

При установке модуля в системе будет создан скрипт `/usr/local/bin/cipa`, который позволит запускать утилиту в одну строку. Учитывая, что пароль нужно передавать утилите открытым текстом, не забудьте поставить дополнительный пробел перед именем утилиты cipa или отключить ведение истории:

```
set +o history
cipa -d ald.company.lan -W 'AstraLinux_176'

+--------------------+---------+---------+-------+
| FreeIPA servers:   | dc-1    | dc-2    | STATE |
+--------------------+---------+---------+-------+
| Active Users       | 1       | 1       | OK    |
| Stage Users        | 0       | 0       | OK    |
| Preserved Users    | 0       | 0       | OK    |
| Hosts              | 2       | 2       | OK    |
| Services           | 10      | 10      | OK    |
| User Groups        | 6       | 6       | OK    |
| Host Groups        | 1       | 1       | OK    |
| Netgroups          | 0       | 0       | OK    |
| HBAC Rules         | 2       | 2       | OK    |
| SUDO Rules         | 0       | 0       | OK    |
| DNS Zones          | 2       | 2       | OK    |
| Certificates       | 0       | 0       | OK    |
| LDAP Conflicts     | 0       | 0       | OK    |
| Ghost Replicas     | 0       | 0       | OK    |
| Anonymous BIND     | ROOTDSE | ROOTDSE | OK    |
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
| Microsoft ADTrust  | True    | True    | OK    |
| Replication Status | dc-2 0  | dc-1 0  | OK    |
+--------------------+---------+---------+-------+
```

3.32. Управление сетевыми папками

3.32.1. Права доступа на новую папку

Для общих папок обязательны следующие параметры, настраиваемые на портале управления **ALD Pro** (Роли и службы сайта-Общий доступ к файлам-Сервер-Папка)- на примере папки `shared_folder`:

```
[shared_folder]
path = /opt/samba_shares/shared_folder
map archive = no
browseable = yes
writable = yes
valid users = @NOBODY
invalid users =
read list =
write list =
admin users =
```

Для того, чтобы при создании новых файлов владельцу не устанавливался флаг Execute, нужно отключить сопоставление DOS атрибута Archive с помощью параметра «map archive = no».

Значения NOBODY для списка `valid users` указывается, когда нет списка пользователей, которым открыт доступ к папке. Это необходимо в целях ограничения доступа пользователей к ресурсу.

```
[shared_folder]
path = /opt/samba_shares/shared_folder
browseable = yes
valid users = @admin
```

3.32.2. Уровень «Чтение» - viewer

Чтобы пользователям группы назначить доступ на чтение, их необходимо включить в списки `valid users` и `read list`. А группу NOBODY удалить. Пример для группы `viewers`:

```
[shared_folder]
path = /opt/samba_shares/shared_folder
browseable = yes
writable = yes
valid users = @viewers
invalid users =
read list = @viewers
write list =
admin users =
```

Пользователь видит папку, но доступа на создание, редактирование и удаление нет.

3.32.3. Уровень «Полный доступ» - fullcontrol

Чтобы пользователям/группам назначить полный административный доступ (Root доступ), их необходимо включить в списки `valid users`, `admin users` и `write list`. Это позволит действовать на файловом сервере от имени `root` в обход списков доступа файловой системы.

```
[shared_folder]
path = /opt/samba_shares/shared_folder
browseable = yes
writable = yes
valid users = @viewers @admins
invalid users =
read list = @viewers
write list = @admins
admin users = @admins
```

Пользователь видит папку, есть доступы на создание, редактирование и удаление.

3.32.4. Уровень «Изменение и назначение прав» - editor

Чтобы пользователям группы были назначены права на запись и на изменение прав доступа к объектам, их необходимо включить в списки `valid users` и `write list`. Пример для группы `editors`:

```
[shared_folder]
path = /opt/samba_shares/shared_folder
browseable = yes
writable = yes
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
valid users = @viewers @admins @editors
invalid users =
read list = @viewers
write list = @admins @editors
admin users = @admins
```

3.32.5. Уровень «Доступ запрещен» - invalid

Чтобы пользователям группы запретить доступ к ресурсу, их необходимо включить в список `invalid users`. Пример для группы `guests`:

```
[shared_folder]
path = /opt/samba_shares/shared_folder
browseable = yes
writable = yes
valid users = @viewers @admins @editors
invalid users = @guests
read list = @viewers
write list = @admins @editors
admin users = @admins
```

Пользователь не видит папку, соответственно доступов на создание, редактирование и удаление нет.

3.32.6. Дополнительные параметры

В свойствах сетевой папки присутствуют параметры **Тип виртуальной файловой системы**, **Права доступа для новых файлов**, **Права доступа для новых папок** и **Наследование прав доступа**.

3.32.6.1. Дополнительный параметр «Тип виртуальной файловой системы»

В настройки общей сетевой папки присутствует переключатель «Тип виртуальной файловой системы» со следующими значениями:

`POSIX ACL` — использование стандартных механизмов `POSIX ACL` без подключения дополнительных модулей виртуальной файловой системы, что обеспечивает полную поддержку Linux и базовую совместимость с Windows. При выборе этого типа виртуальной файловой системы параметр `vfs objects` не должен содержать модулей `ACL`:

```
[shared_folder]
...
vfs objects =
```

ACL XATTR — подключение модуля acl_xattr, который обеспечивает хранение Windows ACL, используя базовые механизмы POSIX ACL, что обеспечивает максимально возможную совместимость моделей безопасности Linux и Windows. При выборе этого типа виртуальной файловой системы параметр vfs objects должен содержать модуль acl_xattr:

```
[shared_folder]
...
vfs objects = acl_xattr
```

NFS4 ACLs — подключение модуля nfs4acl_xattr, который хранит списки доступа NFS4 в виде бинарных объектов в расширенных атрибутах файлов (EAs/xattrs), что обеспечивает полную поддержку Windows без поддержки Linux. При выборе этого типа виртуальной файловой системы параметр vfs objects должен содержать модуль nfs4acl_xattr:

```
[shared_folder]
...
vfs objects = nfs4acl_xattr
```

3.32.6.2. Дополнительный параметр «Права доступа для новых файлов и папок»

При создании новых файлов/папок через SMB подключение им назначаются права доступа «rw-r–r–» и «rwxr-xr-x» соответственно, что подходит для личных папок, но не подходит для общих папок, которые используются для совместной работы, поэтому в настройки сетевой папки необходимо добавить переключатель «Права доступа на файлы/папки» со следующими значениями:

- Права на файлы — устанавливает параметр force create mode, по умолчанию 0777
- Права на папки — устанавливает параметр force directory mode, по умолчанию 0777

3.32.6.3. Дополнительный флажок «Наследовать права доступа»

Если необходимо управлять правами доступа через механизм наследования, то в настройки сетевой папки добавляется флажок «Наследовать права доступа». Если этот флажок включен, то значения параметров force create mode и force directory mode игнорируются, поэтому соответствующие поля можно делать неактивными.

При установке флажка «Наследовать права доступа» в конфигурационном файле smb.conf должны быть заданы следующие параметры:

```
[hared_folder]
...
inherit permissions = yes
inherit acls = yes
```

3.32.7. Управление папками

При удалении общей папки, локальная папка остается.

- `path`: указывает на директорию на сервере Samba, которая будет доступна по сети. Если изменить этот параметр, сетевая папка будет указывать на другую локальную папку. Если по пути локальной папки нет, то она создастся

Пример:

```
path = /home/samba/shared
```

- `browseable`: определяет, будет ли эта папка доступна для просмотра в браузерах сетевых ресурсов (например, в проводнике Windows).

Значения: `yes`: папка будет доступна для просмотра. no: папка будет скрыта.

Пример:

```
browseable = yes
```

- `access based share enum` (ABE): позволяет создавать правила доступа к папке на основе пользователей и групп. Например, можно разрешить только чтение для определенной группы, а другим - запись.

Значения: `yes`: ABE включен. no: ABE отключен.

Пример:

```
access based share enum = yes
```

- `vfs objects`: список модулей, которые расширяют функциональность Samba. Например, модуль `streams_xattr` позволяет работать с расширенными атрибутами файлов.

Пример:

```
vfs objects = streams_xattr
```

- `force directory mode`: устанавливает режим доступа (права) для всех новых подкаталогов, создаваемых в данной папке.

Значения: Число, представляющее собой режим доступа в восьмеричной системе счисления.

Пример:

```
force directory mode = 0755 (чтение, запись для владельца, чтение для группы,
↪ чтение для других)
```

- `force create mode`: устанавливает режим доступа для всех новых файлов, создаваемых в данной папке.

Значения: Число, представляющее собой режим доступа в восьмеричной системе счисления.

Пример:

```
force create mode = 0644 (чтение, запись для владельца, чтение для группы,
↪чтение для других)
```

- `inherit permissions`: указывает, будут ли права доступа к файлам и папкам наследуемы от родительской папки.

Значения: `yes`: права наследуются. no: права не наследуются.

Пример:

```
inherit permissions = yes
```

- `inherit acls`: указывает, будут ли ACL (списки управления доступом) наследуемы от родительской папки.

Значения: `yes`: ACL наследуются. no: ACL не наследуются.

Пример:

```
inherit acls = yes
```

3.32.8. Аутентификация

Начиная с версии 2.4.0 `passdb backend` больше не используется. Теперь конфигурация **Samba** генерируется по шаблону:

```
[global]
workgroup = c-1.ald.company.lan
realm = c-1.ald.company.lan
dedicated keytab file = FILE:/etc/samba/samba.keytab
kerberos method = dedicated keytab
idmap config c-1 : 1457400000-1457599999
idmap config c-1 : backend = sss
idmap config * : range = 0 - 0
log file = /var/log/samba/log.%m
include = registry
include = /etc/samba/share.conf
```

```
[homes]
browsable = yes
writable = yes
create mask = 0600
directory mask = 0700
valid users = %S
read only = No
guest ok = no
```

где: - c-1 - это значение до первой точке в имени домена в верхнем регистре.

- 1457400000-1457599999 - это диапазон id. Он считается по формуле из атрибутов записи `cn=c-1.ald.company.lan_id_range,cn=ranges,cn=etc,dc=c-1,dc=ald,dc=company,dc=lan`:
- первое число - `ipaBaseID`
- второе число - `ipaBaseID + ipaIDRangeSize - 1`
- `include = registry` - активирует работу регистра. позволяет переопределять в нем конфигурации
- `include = /etc/samba/share.conf` - подключает конфигурационный файл, в который пишется конфигурация.

3.33. Создание репозиториев из ISO образа

Для установки программного обеспечения через групповые политики требуется репозиторий, созданный с использованием официального ISO-образа. Это позволит устанавливать и обновлять программное обеспечение без обращения к сети Интернет.

Необходимо скачать образ-ISO с базовым дистрибутивом на сайте в личном кабинете, перейдя по ссылке https://lk-new.astralinux.ru/, или вставить диск в привод, скопировав ISO-образ в текущую директорию командой dd:

```
dd if=/dev/sr0 of=al174main.iso bs=100M status=progress
```

Создать новый репозиторий для корпоративной сети, перейдя в раздел «Установка и обновление ПО — Репозитории ПО». На вкладке «Репозитории ПО» нажать на кнопку «Новый репозиторий».

В открывшемся окне «**Основное**» назвать новый репозиторий «astra-linux-base» и указать абсолютный путь */astralinux17base*, см. *Новый репозиторий с базового образа Astra Linux 1.7*. Необходимо обратить внимание, что путь начинается с символа «/». После заполнения нажать на кнопку «**Сохранить**».

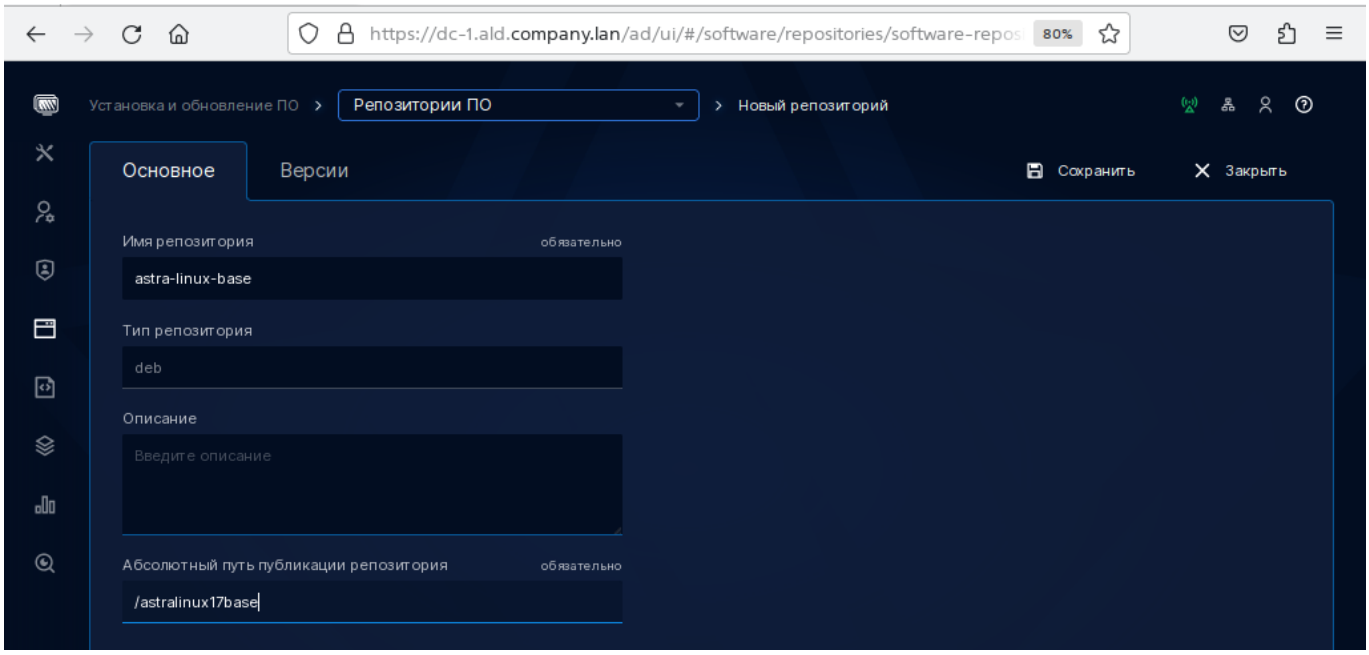


Рисунок 3.110 – Новый репозиторий с базового образа Astra Linux 1.7

После сохранения станут доступны дополнительные вкладки для настройки репозитория. Перейти на вкладку «**Версии**» и создать новую запись, см. *Вкладка Версии нового репозитория astra-linux-base*.

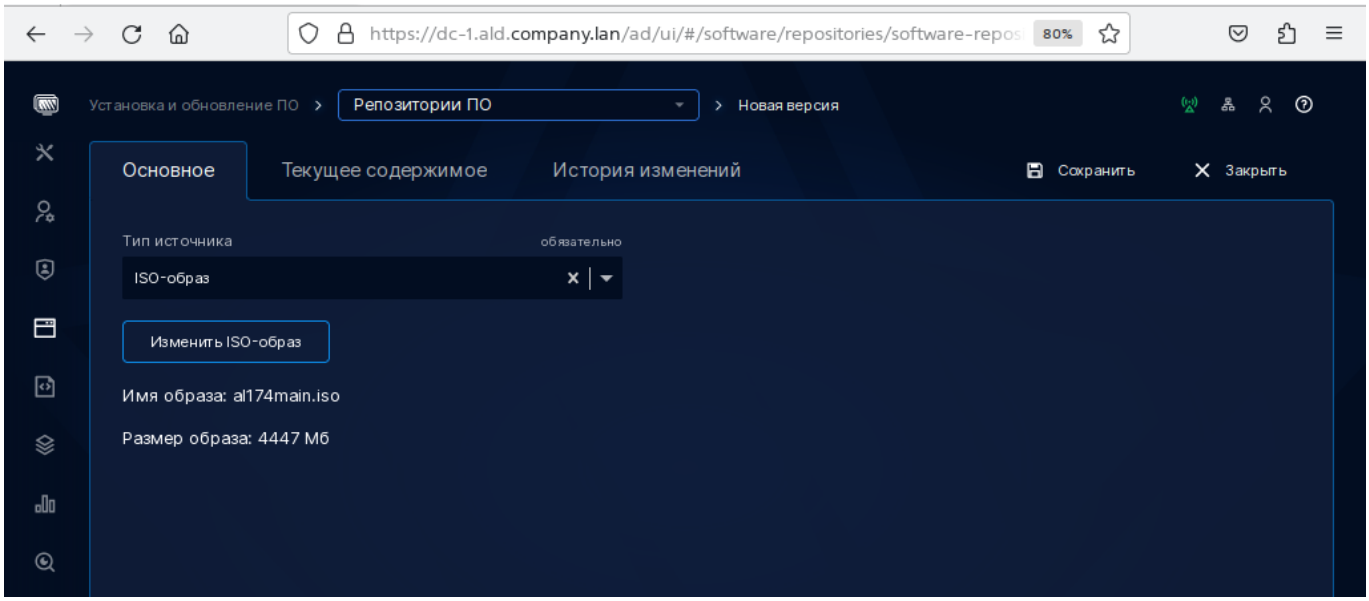


Рисунок 3.111 – Вкладка Версии нового репозитория astra-linux-base

Необходимо создать Версию из ISO-образа, для этого из списка выбрать загруженный образ. Чтобы начался процесс загрузки образа на сервер репозиториев, нажать на кнопку «**Сохранить**».

После загрузки файла на сервер, он будет обрабатываться некоторое время. Проверить статус обработки можно на странице с версией, см. рис. *Обработка ISO образа на вкладке «Версия»*.

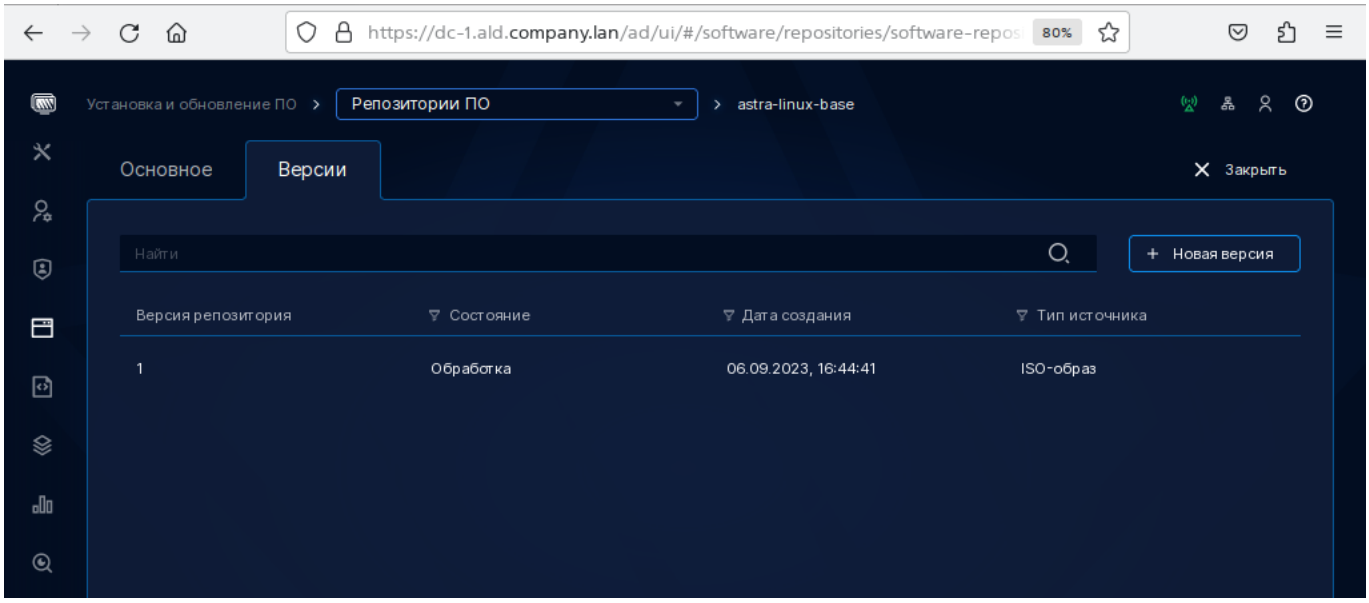


Рисунок 3.112 – Обработка ISO образа на вкладке «Версия»

После обработки статус поменяется на Опубликована, см. *Обработанный ISO образ Версии 1 со статусом «Опубликована»*, после чего его можно использовать в файле */etc/apt/sources.list*.

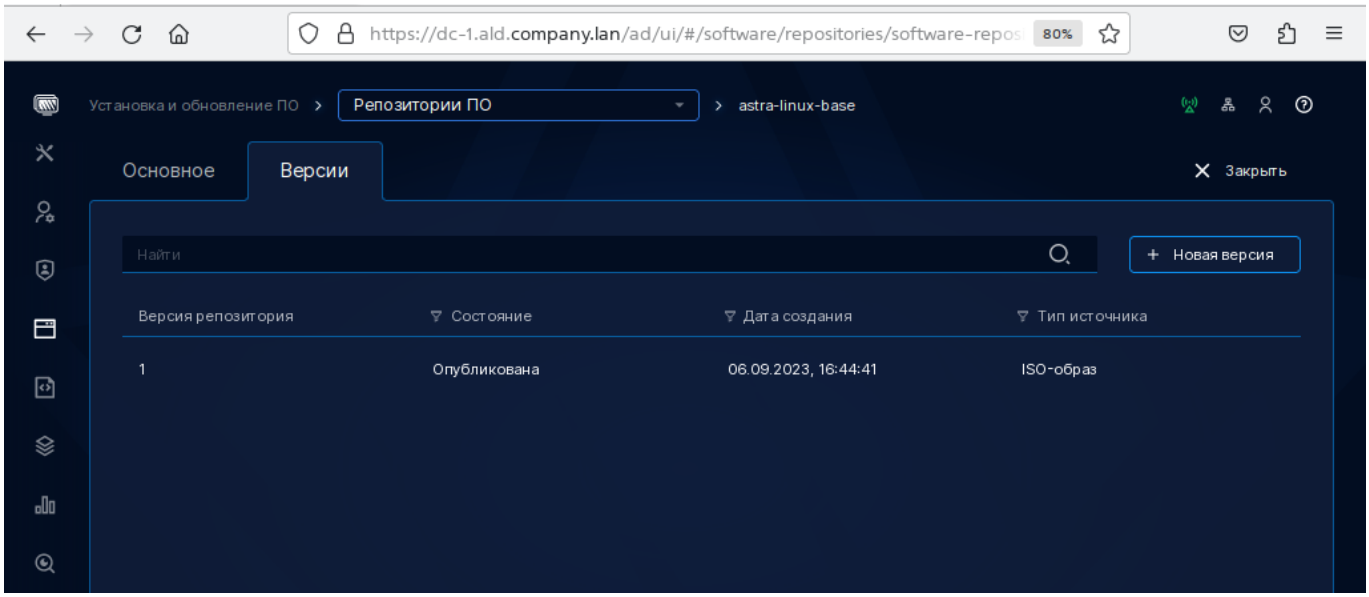


Рисунок 3.113 – Обработанный ISO образ Версии 1 со статусом «Опубликована»

Открыть файл *sources.list* на **pc-1** для настройки базовой версии Astra Linux:

```
ssh pc-1
sudo nano /etc/apt/sources.list
```

Вставить добавленный репозиторий в *source.list*, а адреса **dl.astralinux.ru** закомментировать через символ #:

```
#deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.xxx/repository-base/
 ↪ 1.7_x86-64 main contrib non-free
#deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.xxx/repository-
 ↪extended/ 1.7_x86-64 main contrib non-free
deb [trusted=yes] https://repo.ald.company.lan/repos/astralinux17base/ 1.7_
 ↪x86-64 main contrib non-free
```

Где:

- `[trusted=yes]` — обозначает, что есть доверие к этому репозиторию, т.е можно устанавливать пакеты без цифровых подписей.
- `https://repo.ald.company.lan/repos/astralinux17base/` — полный путь до репозитория, который можно посмотреть во вкладке «Основное» выбранного репозитория. Порт 443 можно не указывать, потому что он используется для протокола https.

В версии 2.1.0 была особенность, что подсистема репозитория получала сертификат на короткое имя по названию компьютера, например, **repo** вместо **repo.ald.company.lan**, поэтому для использования **https** в этом случае требовалось указывать адрес в формате `deb [trusted=yes] https://repo/repos/astralinux17base/ ...`.

- `1.7_x86-64` — кодовое имя дистрибутива, которое можно посмотреть в описании версии.
- `main`, `contrib` и `non-free` — компоненты дистрибутива, которое можно посмотреть в описании версии.

Сохранить и проверить, что установка пакетов будет с адреса нового репозитория в корпоративной сети:

```
sudo apt update
```

Результат выполнения обновления кэша:

```
Игн:1 https://repo.ald.company.lan/repos/astralinux17base 1.7_x86-64
 ↪InRelease
Пол:2 https://repo.ald.company.lan/repos/astralinux17base 1.7_x86-64 Release
 ↪[5 766 B]
Пол:3 https://repo.ald.company.lan/repos/astralinux17base 1.7_x86-64 Release.
 ↪gpg [833 B]
Пол:4 https://repo.ald.company.lan/repos/astralinux17base 1.7_x86-64/main
 ↪amd64 Packages [1 310 kB]
Пол:5 https://repo.ald.company.lan/repos/astralinux17base 1.7_x86-64/contrib
 ↪amd64 Packages [2 155 B]
Пол:6 https://repo.ald.company.lan/repos/astralinux17base 1.7_x86-64/non-
 ↪free amd64 Packages [55,8 kB]
Сущ:7 https://dl.astralinux.ru/aldpro/stable/repository-main 2.5.0 InRelease
Сущ:8 https://dl.astralinux.ru/aldpro/stable/repository-extended generic
 ↪InRelease
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
Получено 1 374 kB за 0с (3 214 kB/s)
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Все пакеты имеют последние версии.
```

Установить **htop** для проверки, что пакет установится из сервера репозитория **astralinux17base**:

```
sudo apt install htop -y
```

Результат выполнения установки **htop**:

```
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Предлагаемые пакеты:
strace
Следующие НОВЫЕ пакеты будут установлены:
htop
Обновлено 0 пакетов, установлено 1 новых пакетов, для удаления
отмечено 0 пакетов, и 0 пакетов не обновлено.
...
Необходимо скачать 89,9 kB архивов.
После данной операции объём занятого дискового пространства
возрастёт на 213 kB.
Пол:1 https://repo.ald.company.lan/repos/astralinux17base 1.7_x86-64/main
amd64 htop amd64 2.5.0-1 [89,9 kB]
Получено 89,9 kB за 0с (6 817 kB/s)
Выбор ранее не выбранного пакета htop.
(Чтение базы данных ... на данный момент установлено 176626 файлов и
↪каталогов.)
Подготовка к распаковке .../htop_2.5.0-1_amd64.deb ...
Распаковывается htop (2.5.0-1) ...
Настраивается пакет htop (2.5.0-1) ...
Обрабатываются триггеры для man-db (2.8.5-2) ...
Обрабатываются триггеры для desktop-file-utils (0.26-1astra1) ...
Обрабатываются триггеры для mime-support (3.62) ...
Обрабатываются триггеры для xserver-xorg-core (2:1.20.14-
1ubuntu1astra.se31) ...
update exec ids due to /usr/bin changed
```

В результате видно, что пакет установился с корпоративного репозитория **repo** с адреса:

https://repo.ald.company.lan/repos/astralinux17base

3.34. Утилиты для работы с групповыми политиками, подсистемами и заданиями автоматизации

3.34.1. Форсированная установка подсистем

При установке, обновлении или удалении подсистем с Портала Управления, команды установки, обновления и удаления подсистем осуществляются по таймеру. Форсировать процесс можно с помощью команды `aldpro-roles`, выполненной на машине, выбранной ранее на Портале Управления.

Форсирование доступно для подсистем:

- общего доступа к файлам (`smb`);
- печати (`cups`);
- динамической настройки узла (`dhcp`);
- установки ОС по сети (`os`);
- журналирования событий (`audit`);
- «Репозиторий ПО» (`repo`).

1. Собрать данные из ldap в файл `/etc/aldpro-salt/stack/deploy/subsystem.yml`:

```
aldpro_deploy_data:
  action:install
  location: hq
  service_name: smb # Подсистема общего доступа к файлам
  service_name: ups # Подсистема печати
  service_name: dhcp # Подсистема динамической настройки узла
  service_name: os # Подсистема установки ОС по сети
  service_name: audit # Подсистема журналирования событий
  service_name: repo # Подсистема "Репозиторий ПО"
  site: {имя сайта}
  state_created: {временная метка}
  state_updated: {временная метка}
  target_host: {имя машины}
```

Примечание: Ключ конфигурации service_name может быть только один, его необходимо выбрать в соответствии с форсируемой подсистемой.

2. Запустить установку/обновление/удаление, в соответствии с этими данными.

```
aldpro-roles --iud --action [install, update, remove]
```

1. Собрать данные из **ldap** в файл `/etc/aldpro-salt/stack/deploy/subsystem.yml)`, заменив action на указанный выше.

2. Запустить установку/обновление/удаление, согласно указанному action.

```
aldpro-roles --subsystem_settings [имя подсистемы: 'cups', 'dhcp',
'smb', 'os', 'repo', 'audit']
```

1. Собрать данные настройки/конфигурации из **ldap**.

2. Применить параметры для указанной подсистемы. Может использоваться только со следующими параметрами/подсистемами: `cups`, `dhcp`, `smb`, `os`, `repo`, `audit`.

Внимание: Запрещено одновременно использовать аргументы по установке подсистемы и применению параметров как указано ниже на примере подсистемы общего доступа к файлам:
`aldpro-iud --iud --action update --subsystem_settings smb`

3.34.2. Утилита для работы с групповыми политиками

Для принудительного обновления групповых политик компьютера и/или пользователя используется утилита **aldpro-gpupdate**.

Для вывода подсказки по использованию утилиты **aldpro-gpupdate** необходимо ввести в терминале следующую команду:

```
sudo aldpro-gpupdate -h
```

Ниже приведен список ключей для применения с утилитой **aldpro-gpupdate**:

- `--gp` Форсированное применение групповых политик с очисткой кэша и формированием нового pillar, может использоваться с ключами **verbose** и **noupdate**
- `--swp` Форсированное применение политик ПО с очисткой кэша и формированием нового pillar, может использоваться с ключами **verbose** и **noupdate**
- `--audit` Форсированное применение правил сбора событий
- `--verbose` Детальный вывод результата выполняемой команды
- `--noupdate` Применение команды без очистки кэша и формирования pillar
- `--gp_timer` Проверка таймера применения групповых политик
- `--swp_timer` Проверка таймера применения политик ПО
- `--audit_timer` Проверка таймера применения правил сбора событий
- `--user_session_timer` Проверка таймера очистки неактивных сессий
- `--client_update_timer` Проверка таймера применения политики обновлений клиента ALD Pro
- `--gp_host_pillar [GP_HOST_PILLAR]` Просмотр PILLAR
- `--pm`, `--policy_manager` Получить данные из ldap и обновить policy-manager

3.34.3. Утилита для работы с заданиями автоматизации

Для работы с задниями автоматизации используется утилита **aldpro-automation**

Для вывода подсказки по использованию утилиты **aldpro-automation** необходимо ввести в терминале следующую команду:

```
sudo aldpro-automation -h
```

3.35. Создание репозитория из загруженных пакетов deb

В качестве примера создается репозиторий с названием **yandex-browser-corp**, в который загрузится корпоративный браузер Яндекс. Для этого потребуется скачать deb пакет для Astra Linux. Его по умолчанию можно загрузить командой:

```
cd ~/Загрузки
wget https://download.yandex.ru/browser/astra-os/yandex-browser.deb
mv yandex-browser.deb "yandex-browser-$(dpkg -f yandex-browser.deb version).
↪deb"
```

В рабочей директории появится файл с последней версией, например, **yandex-browser-23.7.1.1219-1.deb**. Его нужно загрузить в репозиторий, также есть возможность настроить пакет в личном кабинете https://browser.yandex.ru/corp, см. *Подготовка сборки для Linux из личного кабинета*.

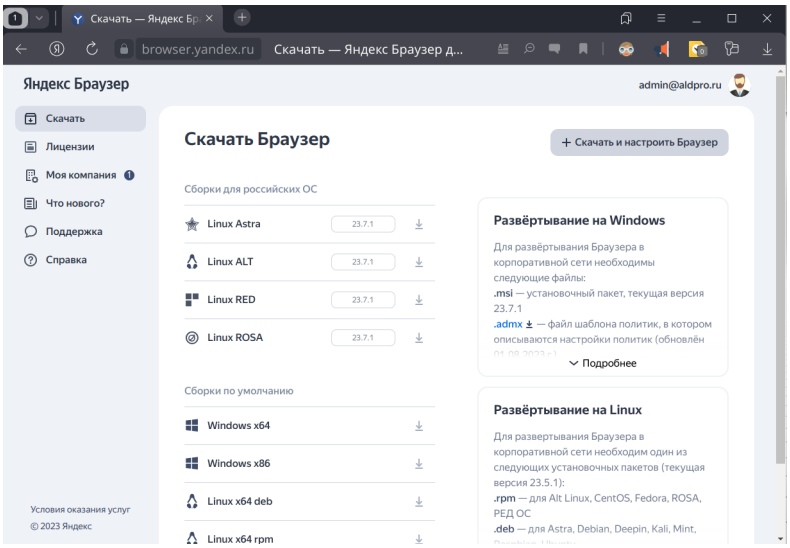


Рисунок 3.114 – Подготовка сборки для Linux из личного кабинета

На портале ALD Pro создать новый репозиторий с названием «**yandex-browser-corp**» и указать абсолютный путь */yandexbrowser*, см. рис. 2.8.. Примените изменения нажатием кнопки «**Сохранить**».

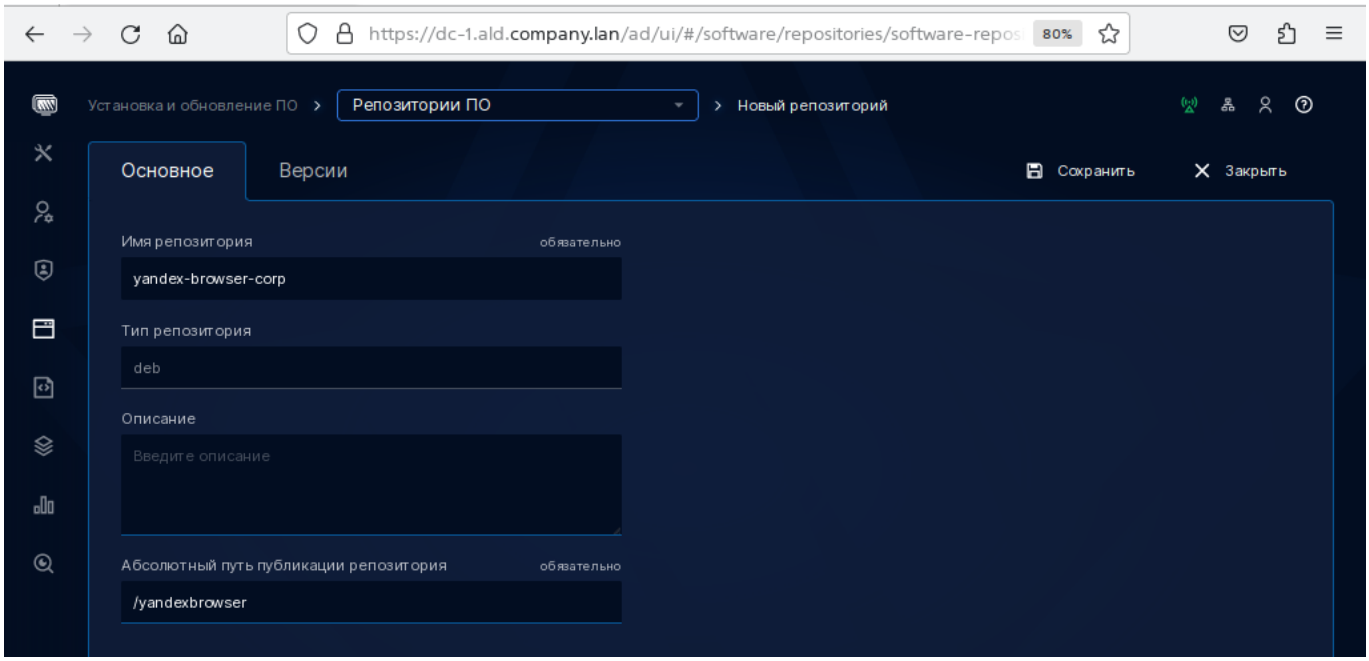


Рисунок 3.115 – Новый репозиторий для пакета deb на примере корпоративного браузера Яндекс

Создать новую версию deb репозитория в **yandex-browser-corp** во вкладке Версии, см. *Описание версии deb пакета для браузера Яндекс*.

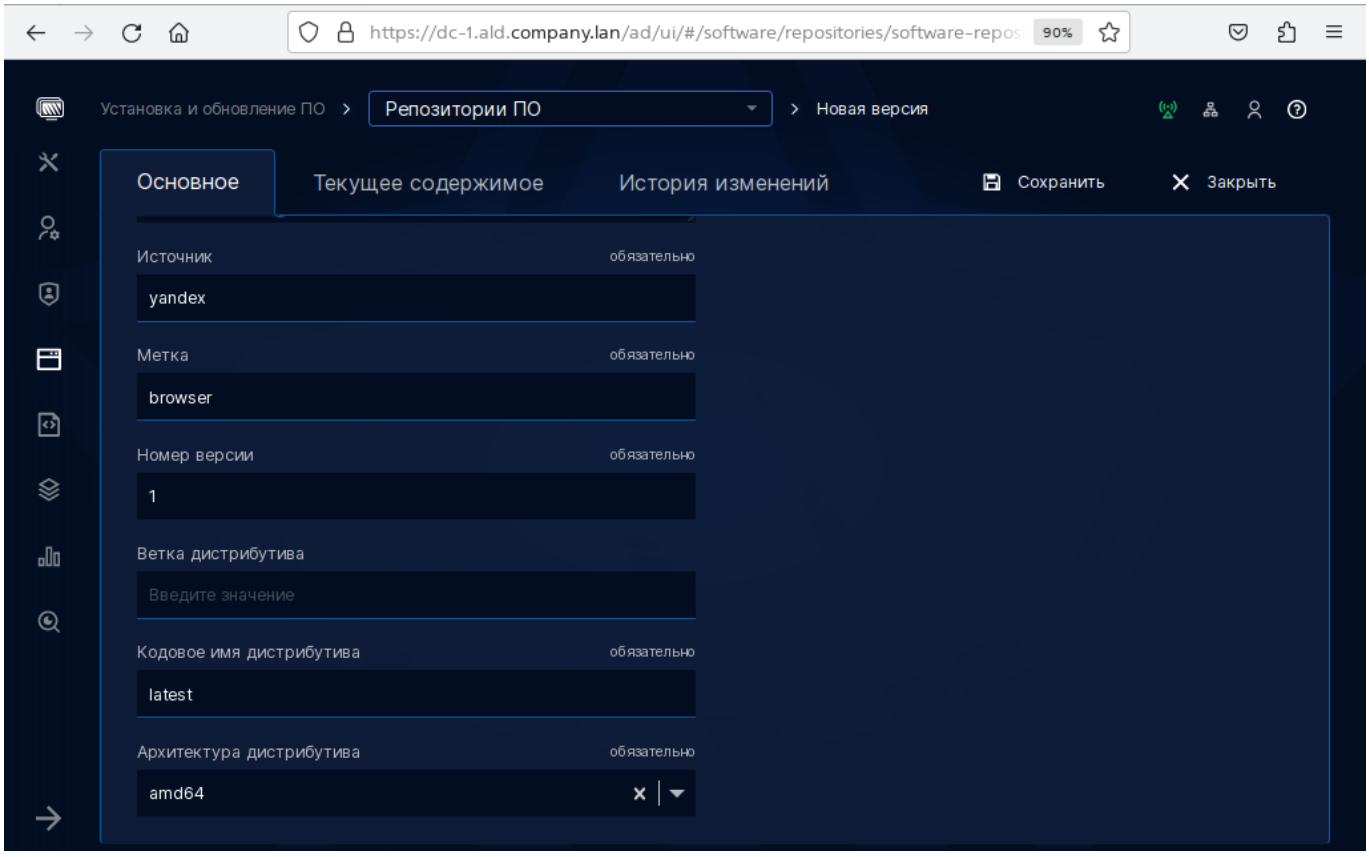


Рисунок 3.116 – Описание версии deb пакета для браузера Яндекс

Заполните поля значениями, см. табл. 4, и нажмите на кнопку «**Сохранить**», чтобы активировать вкладку «**Текущее содержимое**».

Поле	Значение	Описание
Источник	yandex	Справочное поле для описания источника пакета
Метка	browser	Справочное поле для описания вида программного пакета
Номер версии	1	Целое число для версионирования репозитория. При обн
Кодовое имя дистрибутива	latest	Используется для возможности размещения в одном репо
Архитектура дистрибутива	amd64	Используется для возможности размещения в одном репо
Компоненты дистрибутива	main	Используется для возможности распределения пакетов по

Назначение полей при создании репозитория из deb пакета

Добавить в версию №1 файл *yandex-browser-23.7.4.981-1.deb* на вкладке «**Текущее содержимое**», см. *Вкладка «Текущее содержимое» версии №1 deb репозитория yandex-browser-corp*.

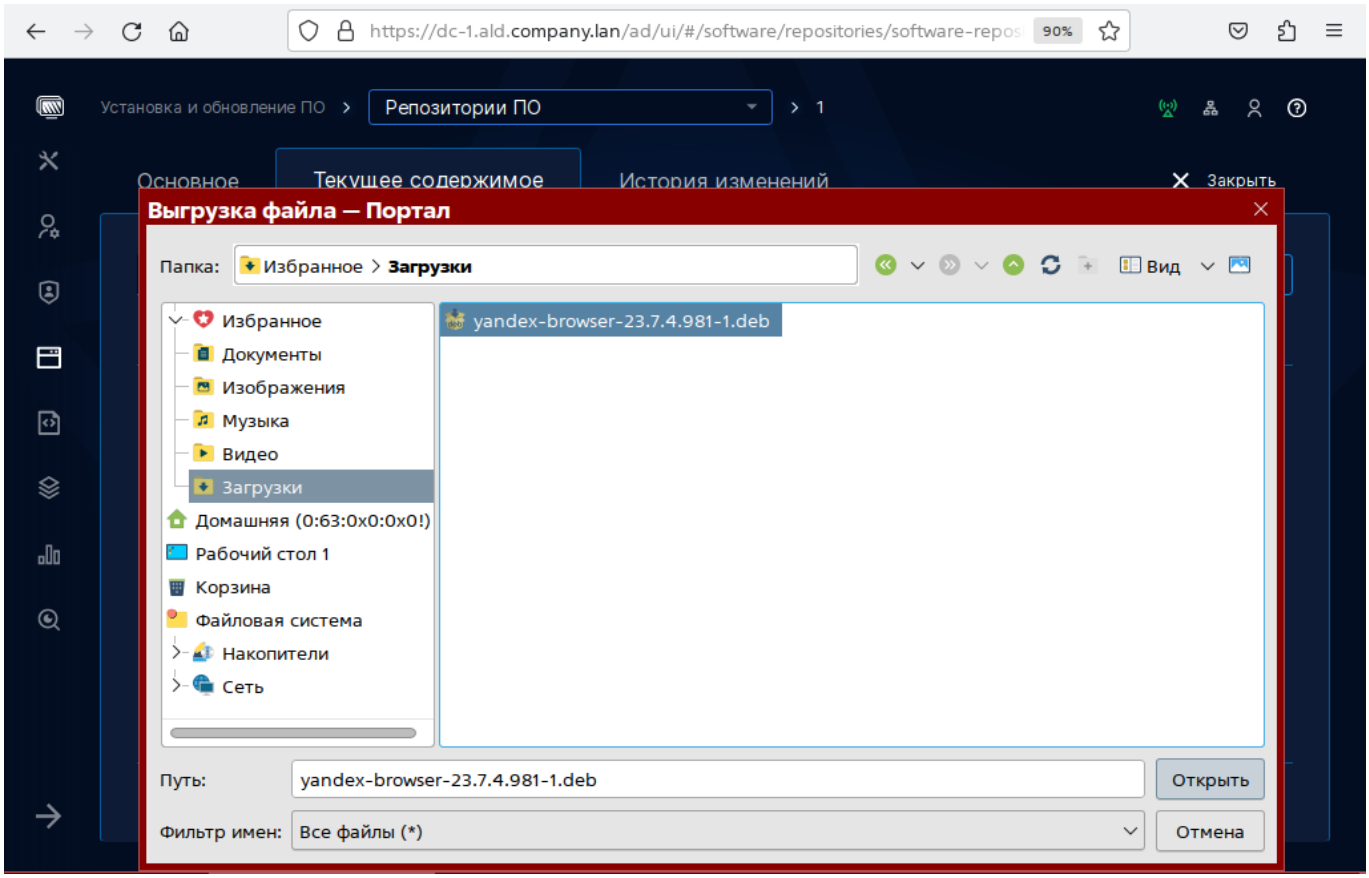


Рисунок 3.117 – Вкладка «Текущее содержимое» версии №1 deb репозитория yandex-browser-corp

Выбрать загруженный файл из директории и дождаться обработки его добавления в список пакетов. После обработки файлов требуется нажать на кнопку «**Опубликовать**», см. *Публикация версии №1 deb-репозитория yandex-browser-corp*.

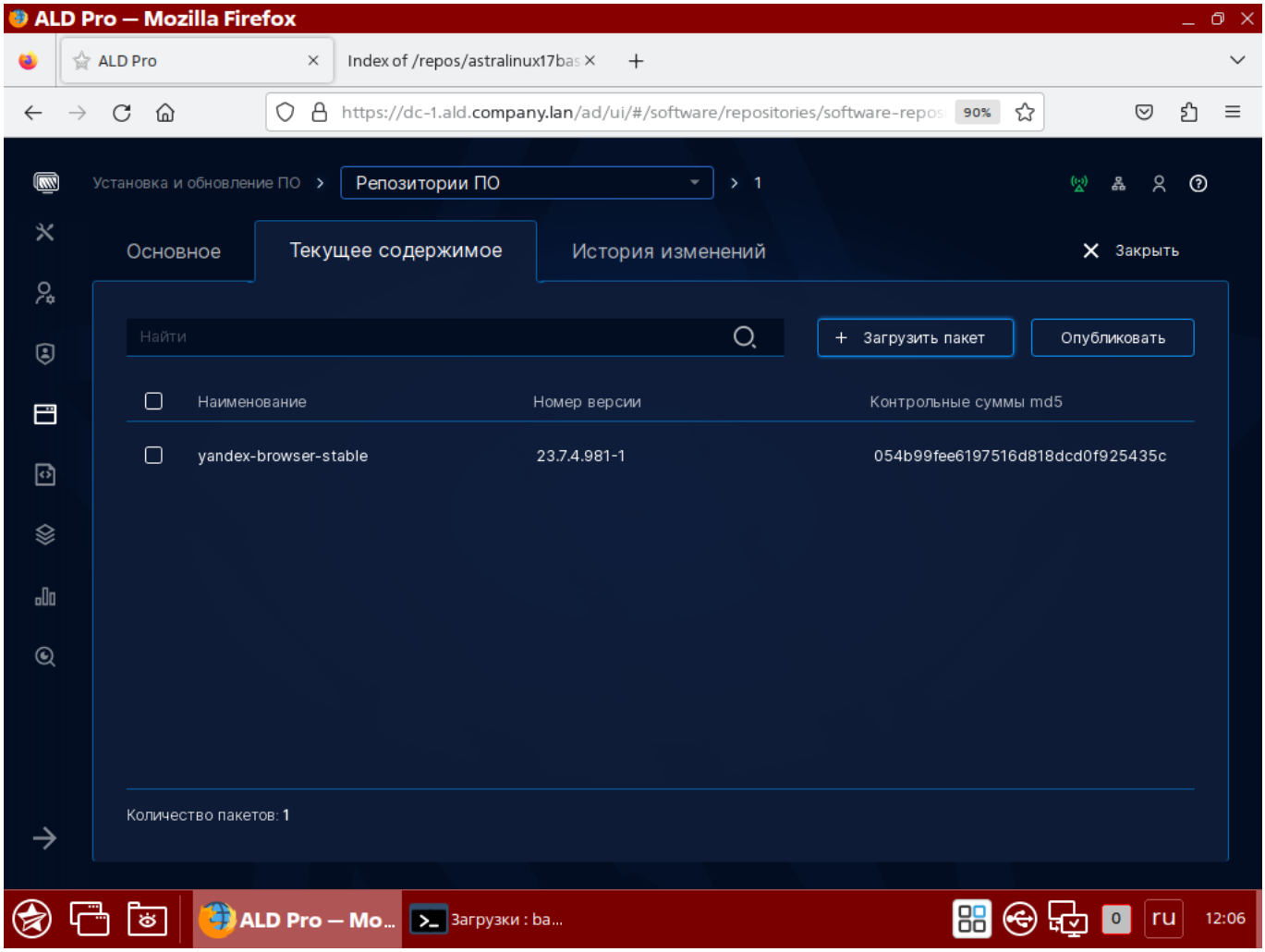


Рисунок 3.118 – Публикация версии №1 deb-репозитория yandex-browser-corp

Важно: В текущей реализации подсистемы репозиториев действие «Опубликовать» нельзя отменить, поэтому для обновления приложения нужно будет создать новую версию репозитория.

3.36. Установка браузера из deb репозитория

На клиентском компьютере настроить *sources.list*, добавив репозиторий с браузером Яндекс:

```
admin@pc-1:~$ sudo nano /etc/apt/sources.list
```

Добавить второй репозиторий в файл *sources.list*:

```
deb [trusted=yes] https://repo.ald.company.lan/repos/astralinux17base/ 1.7_
↪x86-64 main contrib non-free
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
deb [trusted=yes] https://repo.ald.company.lan/repos/yandexbrowser/ latest
 ↪main
```

Внимание: Базовый дистрибутив 1.7_x86-64 main тоже подключен, потому что могут потребоваться дополнительные пакеты и библиотеки.

Обновить новые списки в кэше **apt**:

```
sudo apt update
```

В результате добавлен репозиторий https://repo.ald.company.lan/repos/yandexbrowser latest:

```
Игн:1 https://repo.ald.company.lan/repos/astralinux17base 1.7_x86-64
 ↪InRelease
Игн:2 https://repo.ald.company.lan/repos/yandexbrowser latest InRelease
Сущ:3 https://repo.ald.company.lan/repos/astralinux17base 1.7_x86-64 Release
Пол:4 https://repo.ald.company.lan/repos/yandexbrowser latest Release [865 B]
Игн:5 https://repo.ald.company.lan/repos/yandexbrowser latest Release.gpg
Пол:6 https://repo.ald.company.lan/repos/yandexbrowser latest/main amd64
 ↪Packages [854 B]
Сущ:8 https://dl.astralinux.ru/aldpro/stable/repository-main 2.5.0 InRelease
Сущ:9 https://dl.astralinux.ru/aldpro/stable/repository-extended generic
 ↪InRelease
Получено 1 719 B за 0c (4 396 B/s)
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Все пакеты имеют последние версии.
```

Установить браузер из нового репозитория командой:

```
sudo apt install yandex-browser-stable -y
```

После установки, браузер появится в меню Пуск - Сеть, см. *Браузер был установлен из корпоративного репозитория*.

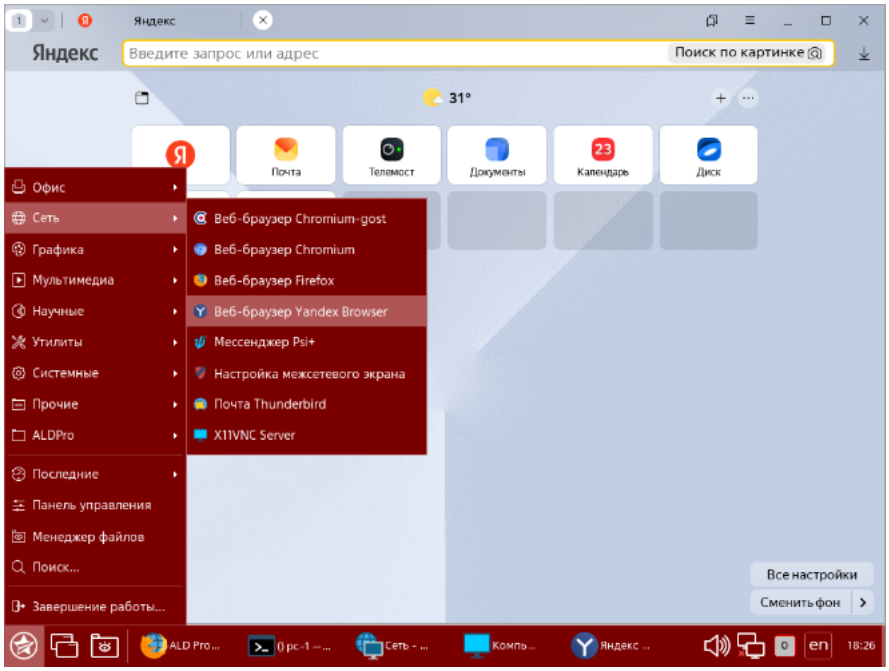


Рисунок 3.119 – Браузер был установлен из корпоративного репозитория

Настроим возможность Kerberos-аутентификации для браузера Яндекс:

```
#создать категорию так как по умолчанию её не существует
sudo mkdir -p /etc/opt/yandex/browser/policies/managed/
sudo nano /etc/opt/yandex/browser/policies/managed/managed_policies.json
```

Вставить в файл *managed_policies.json* следующее содержимое:

```
{
    "AuthServerAllowlist": "*.ald.company.lan",
    "AuthNegotiateDelegateAllowlist": "*.ald.company.lan",
    "HomepageLocation": "https://dc-1.ald.company.lan/"
}
```

Примечание: Также системный администратор может управлять браузером Яндекс через политики. Более подробно с политиками можете ознакомиться в справке браузера: https://yandex.ru/support/browser-corporate/policy/list.html. Посмотреть список примененных политик можно перейдя по адресу browser://policy/

3.37. Необходимые привилегии для ввода компьютера в домен

3.37.1. Предварительная настройка

Для выполнения предварительной настройки ввода компьютеров в домен с помощью Портала Управления ALD Pro необходимо:

- Создать и настроить сервер **DHCP** для установки ОС по сети (см. **Справочный Центр - Роли службы сайта - Служба динамической настройки узла**).
- Создать и настроить сервер репозиториев ПО, а также репозиторий ПО, откуда будет проходить установка ОС на компьютер (см. **Справочный центр - Установка и обновление ПО - Репозитории ПО**).
- Создать и настроить сервер установки ОС по сети, добавить шаблон компьютера и профиль загрузки (см. **Справочный центр - Автоматизация - Установка ОС по сети**).

Для выполнения настройки вышеуказанных разделов необходимо:

- создать роль;
- привязать ее к корню домена;
- установить признак **Включая дочерние подразделения**;
- сохранить эту роль;
- добавить необходимый набор привилегий для управления всеми разделами портала управления;
- назначить роль на администратора, который будет выполнять предварительную настройку. Данный администратор будет обладать всеми необходимыми привилегиями для выполнения настройки и ввода компьютера в домен.

3.37.1.1. Привилегии, необходимые для работы с подразделом портала Роли службы сайта - Служба динамической настройки узла

Для создания и настройки нового сервера службы динамической настройки узла (**DHCP**), который будет использоваться в процессе ввода компьютера в домен, необходимы следующие привилегии:

1. `DHCP Servers - Create` (привязка ко всем сайтам домена), для корректной работы данной привилегии в роль также необходимо добавить следующие связанные привилегии:

    1.1 `Computers - Read`

    1.2 `DHCP - Read`

    1.3 `DNS Zones - Read`

    1.4 `IPA Servers - Read`

    1.5 `Organization units - Read`

    1.6 `Sites - Read`

2. `DHCP Configuration - Modify` (привязка ко всем сайтам домена), для корректной работы данной привилегии в роль также необходимо добавить следующие связанные привилегии:

    2.1 `Computers - Read`

2.2 DHCP - Read

2.3 DNS Zones - Read

2.4 IPA Servers - Read

2.5 Organization units - Read

2.6 Sites - Read

3.37.1.2. Привилегии, необходимые для работы с подразделом портала Установка и обновление ПО - Репозитории ПО

Для создания и настройки нового сервера репозиториев ПО, а также нового репозитория на этом сервере, который будет использоваться в процессе ввода компьютера в домен, необходимы следующие привилегии:

1. Repository Servers - Create (привязка ко всем сайтам домена), для корректной работы данной привилегии в роль также необходимо добавить следующие связанные привилегии:

    1.1 Computers - Read

    1.2 DNS Zones - Read

    1.3 IPA Servers - Read

    1.4 Organization units - Read

    1.5 Repository Servers - Read

    1.6 Sites - Read

2. Repositories - Add, для корректной работы данной привилегии в роль также необходимо добавить следующие связанные привилегии:

    2.1 Computers - Read`

    2.2 DNS Zones - Read

    2.3 IPA Servers - Read

    2.4 Organization units - Read

    2.5 Repositories - Read

    2.6 Repository Servers - Read

    2.7 Sites - Read

3. Repository Versions - Manage (привязка ко всем сайтам домена), опционально при необходимости, для корректной работы данной привилегии в роль также необходимо добавить следующие связанные привилегии:

    3.1 Computers - Read

    3.2 DNS Zones - Read

3.3 IPA Servers - Read

3.4 Organization units - Read

3.5 Repositories - Read

3.6 Repository Servers - Read

3.7 Sites - Read

3.37.1.3. Привилегии, необходимые для работы с подразделом портала Автоматизация - Установка ОС по сети

Для создания и настройки нового сервера установки ОС по сети, который будет использоваться в процессе ввода компьютера в домен, а также для добавления компьютеров и создания новых профилей загрузки, необходимы следующие привилегии:

1. Installation Server Computers - Manage, для корректной работы данной привилегии в роль также необходимо добавить следующие связанные привилегии:

    1.1 Computers - Delete

    1.2 Computers - Read

    1.3 DNS Zones - Read

    1.4 DHCP - Read

    1.5 Domain Info - Read

    1.6 IPA Servers - Read

    1.7 Installation Server Profiles - Manage

    1.8 Installation Servers - Read

    1.9 Organization units - Read

    1.10 Sites - Read

2. Installation Servers - Create (привязка ко всем сайтам домена), для корректной работы данной привилегии в роль также необходимо добавить следующие связанные привилегии:

    2.1 Computers - Read

    2.2 DNS Zones - Read

    2.3 DHCP - Read

    2.4 Domain Info - Read

    2.5 IPA Servers - Read

    2.6 Installation Servers - Read

    2.7 Organization units - Read

2.8 Sites - Read

3. Installation Servers - Modify (при необходимости не только создавать, но и изменять имеющиеся сервера установки ОС), (привязка ко всем сайтам домена), для корректной работы данной привилегии в роль также необходимо добавить следующие связанные привилегии:

   3.1 Computers - Read

   3.2 DNS Zones - Read

   3.3 DHCP - Read

   3.4 Domain Info - Read

   3.5 IPA Servers - Read

   3.6 Installation Servers - Read

   3.7 Organization units - Read

   3.8 Sites - Read

3.37.1.4. Полный набор привилегий, необходимых для настройки возможности ввода компьютера в домен с помощью портала управления ALD Pro

Таким образом, для настройки возможности ввода компьютера в домен необходимо создать роль с приведенным ниже набором привилегий и назначить эту роль на того администратора, который будет выполнять настройку:

1. DHCP Servers - Create (привязка ко всем сайтам домена)
2. DHCP Configuration - Modify (привязка ко всем сайтам домена)
3. Repository Servers - Create (привязка ко всем сайтам домена)
4. Repositories - Add
5. Repository Versions - Manage (привязка ко всем сайтам домена)
6. Installation Server Computers - Manage
7. Installation Servers - Create (привязка ко всем сайтам домена)
8. Computers - Delete (связанная)
9. Computers - Read (связанная)
10. DHCP - Read (связанная)
11. DNS Zones - Read (связанная)
12. IPA Servers - Read (связанная)
13. Domain Info - Read (связанная)

14. Organization units - Read (связанная)
15. Sites - Read (связанная)
16. Installation Server Profiles - Manage (связанная)
17. Installation Servers - Read (связанная)
18. Repositories - Read (связанная)
19. Repository Servers - Read (связанная)

3.37.1.5. Настройка возможности ввода компьютеров в домен с помощью ролей для подразделов портала управления

Для обеспечения предварительной настройки возможности ввода компьютера в домен также можно воспользоваться поставляемыми при начальной установке ролями для подразделов Портала Управления ALD Pro.

Для этого администратору необходимо делегировать следующие роли:

1. ALDPRO - DHCP Service Administrators
2. ALDPRO - Software Repositories Administrators
3. ALDPRO - Install OS Service Administrators

Однако необходимо помнить, что при этом администратор будет обладать полными правами на эти подразделы (то есть добавляется возможность удалять и модифицировать все данные во всех подразделах портала, на которые предоставляется доступ, а не только возможностью создания новых данных).

3.37.1.6. Привилегии, необходимые для ввода компьютера в домен, при условии, что все настройки сделаны предварительно

В том случае, если все необходимые настройки для ввода компьютера в домен были предварительно проведены одним администратором, то набор привилегий, необходимых администратору исключительно для ввода компьютера в домен без возможности модификации данных в подразделах портала, не связанных с установкой ОС по сети, может быть сокращен до следующего набора привилегий:

1. Installation Server Computers - Manage, для корректной работы данной привилегии в роль также необходимо добавить следующие связанные привилегии:
    1.1 Computers - Delete
    1.2 Computers - Read
    1.3 DNS Zones - Read
    1.4 DHCP - Read
    1.5 Domain Info - Read

1.6 IPA Servers - Read

1.7 Installation Server Profiles - Manage

1.8 Installation Servers - Read

1.9 Organization units - Read

1.10 Sites - Read

3.38. Присоединение к домену с помощью одноразового пароля

Чтобы при вводе компьютеров в домен уменьшить риск разглашения привилегированных учетных данных, в **ALD Pro** предусмотрена возможность ввода компьютера по одноразовому паролю.

Использование одноразовых паролей обладает несколькими преимуществами:

- Учетная запись хоста может быть создана сразу в правильном организационном подразделении, чтобы на него распространялось действие необходимых групповых политик.
- Учетную запись хоста можно сразу включить во все группы, чтобы на него распространялись необходимые правила HBAC и SUDO.
- Для ввода машины в домен на стороне рабочей станции не нужно будет использовать пароль привилегированной учетной записи.

Для присоединения компьютера к домену с помощью одноразового пароля в **ALD Pro** используется графическая утилита `aldpro-client-install`.

1. Необходимо создать учетную запись компьютера с помощью команды `ipa host-add`, используя ключ `--random` для генерации одноразового пароля:

```
kinit admin
ipa host-add pc-2.ald.company.lan --random --ip-address=10.0.1.52 --force \--
↪department='ou=Московский офис,ou=ald.company.lan,cn=orgunits,cn=accounts,
↪dc=ald,dc=company,dc=lan'
```

В результате выполнения получен одноразовый пароль, который необходимо сохранить для дальнейшего ввода компьютера в домен:

```
 admin@dc-1:~$ kinit admin
admin@dc-1:~$ ipa host-add pc-2.ald.company.lan --random --ip-address=10.0.1.
↪52 --force \    --department='ou=Московский офис,ou=ald.company.lan,
↪cn=orgunits,cn=accounts,dc=ald,dc=company,dc=lan'
----------------------------------
Добавлен узел "pc-2.ald.company.lan"
----------------------------------
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
Имя узла: pc-2.ald.company.lan
Случайный пароль: 2LyXwGJItweZbvJP3LLqFCT
```

Где:

- `pc-2.ald.company.lan` – FQDN имя компьютера в нижнем регистре;
- `--random` – ключ, указывающий на требование сгенерировать случайный одноразовый пароль;
- `--ip-address` – адрес компьютера для создания DNS записи в домене;
- `--force` – ключ, позволяющий принудительно установить значение имени узла, даже если такое имя уже присутствует в DNS.

2. Настроить компьютер **pc-2**:

- Настроить IP-адрес: **10.0.1.52**.
- Установить репозитории **ALSE** и **ALD Pro**:

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

Вставить в файл ссылку на deb-репозиторий продукта:

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

- Проверить доступ к dc-1 `ping -c 2 dc-1` и интернет-репозиториям `ping -c 2 dl.astralinux.ru`
- Обновить кэш `apt` и установить обновления:

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

- Установить клиентские библиотеки **aldpro-client**

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

- Проверить отсутствие **pc-2** в домене **ald.company.lan**:

```
localadmin@astra:~$ ping pc-2
ping: pc-2: Неизвестное имя или служба
```

3. Запустить графическую утилиту ввода в домен `aldpro-client-installer`:

```
sudo /opt/rbta/aldpro/client/bin/aldpro-client-installer
```

4. Заполнить поля и выставить флаги:

- наименование домена: **ald.company.lan**;
- поле **Учетная запись** оставить пустым;
- в поле Хост: **pc-2**;
- в поле Пароль вставить одноразовый пароль из пункта 1;
- обязательно поставить флаг *Ввод в домен по паролю компьютера*.

5. Запустить процесс ввода кнопкой *Добавить в домен*. Нажать **Да** для подтверждения ввода.

Ввод компьютера в домен выполнен.

3.39. Повторное присоединение к домену, используя keytab-файл хоста

Если администратору нужно переустановить операционную систему на доменном компьютере, то утилита **ipa-client-install** позволяет для авторизации повторного ввода машины в домен с тем же именем воспользоваться предыдущим *krb5.keytab*-файлом.

При этом она не просто скопирует файл, а сбросит хосту пароль и запишет новые ключи, поэтому версия ключей изменится:

```
sudo klist -k /home/localadmin/krb5.keytab
```

Результат выполнения:

```
Keytab name: FILE:/home/localadmin/krb5.keytab
KVNO Principal
---------------------------------------------------------------------------
 ↪
   1 host/pc-1.ald.company.lan@ALD.COMPANY.LAN
   1 host/pc-1.ald.company.lan@ALD.COMPANY.LAN
```

Необходимо установить имя хоста и клиент с keytab-файлом:

```
sudo hostnamectl set-hostname pc-1.ald.company.lan
sudo ipa-client-install -U -k /home/localadmin/krb5.keytab
```

Результат выполнения:

```
...
The ipa-client-install command was successful
root@pc-1:~# klist -k /etc/krb5.keytab
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
---------------------------------------------------------------------------
 ↪
2 host/pc-1.ald.company.lan@ALD.COMPANY.LAN
2 host/pc-1.ald.company.lan@ALD.COMPANY.LAN
```

Для применения всех настроек необходимо выполнить перезагрузку компьютера:

```
sudo reboot
```

3.40. Служба синхронизации времени

Служба синхронизации времени в домене необходима для корректной работы следующих механизмов:

- аутентификации по протоколу **Kerberos**;
- двухфакторной аутентификации на основе синхронизированных по времени одноразовых паролей;
- разрешения конфликтов при репликации;
- возможности сопоставления журналов событий с разных серверов.

Служба `chrony` (демон `chronyd`) запускается после загрузки операционной системы и начинает отправлять запросы на **NTP**-серверы, перечисленные в файле конфигурации `/etc/chrony/chrony.conf`. После получения ответа от **NTP**-сервера, `chronyd` обновляет системное время. Процесс синхронизации времени с сервером продолжается на протяжении всего времени работы службы `chrony` на этих компьютерах. Служба синхронизации времени автоматически определяет оптимальную частоту запросов, обычно делая их каждые несколько минут. Это минимизирует ошибки времени и обеспечивает точность работы системных часов, приближенную к реальной.

Выбор источника точного времени (в реализации «коробочной» групповой политики) в домене для каждого компьютера осуществляется на основе иерархической системы:

```
# КД - контроллер домена

Внешний источник (или другой эталон)
# это сервер, который находится за пределами инфраструктуры компании

    Корневой КД сайта
    # это контроллеры домена, которые объявлены корневыми через портал
↪управления ALD Pro и которые непосредственно синхронизируются с внешним NTP-
↪сервером

        Обычный КД сайта
        # это контроллер домена, который синхронизирует время с корневым NTP-
↪сервером и дополнительно выступает в качестве источника времени для
↪клиентов из того же сайта

            Корневой КД домена (не из сайта)
            # это контроллер домена, который объявлен корневым через портал
↪управления ALD Pro, но находится в другом сайте относительно клиента NTP

                Обычный КД домена (не из сайта)
                # это контроллер домена, который синхронизирует время с
↪корневым NTP-сервером, но при этом находится в другом сайте
```

Уровень внешнего источника используется только для корневых контроллеров домена

(КД). Если КД на каком-то уровне нет, то берется следующий за ним уровень и осуществляется попытка синхронизации с КД этого уровня.

При установке первый КД автоматически становится корневым **NTP**-сервером домена. Дальнейшие изменения конфигурации администратор делает самостоятельно.

На всех корневых КД должна быть следующая конфигурация службы `chrony` (после применения групповой политики - timeGP):

```
{{allow 0/0       }}
{{stratumweight 1 }}
{{combinelimit 0  }}
{{local stratum 11 orphan     }}
server some_external_ntp_server iburst minstratum 11        # при наличии
 ↪записи (записей) в ПУ
```

На всех КД, которые не являются корневыми, должна быть следующая конфигурация службы `chrony` (после применения групповой политики - timeGP):

```
{{allow 0/0       }}
{{stratumweight 1 }}
{{combinelimit 0  }}
{{local stratum 11    }}
{{pool _ntp._udp._roots.{dc_component} iburst minstratum 12 }}
{{pool _ntp._udp._roots._default.{dc_component} iburst minstratum 14 }}
```

Форсировать обновление настроек `/etc/chrony/chrony.conf` можно командой:

```
aldpro-salt-call state.apply policies.host-policies.rbta_ldap_date_time_h
```

Функционирование подсистемы **NTP** осуществляется с помощью динамических **DNS**-записей и групповой политики для синхронизации времени. Дополнительные настройки конфигурационного файла `chrony` не требуются, т.к. они выполняются в ходе работы групповой политики времени.

3.40.1. Динамические DNS-записи

Начиная с 2.5.0, реализован функционал подсистемы **NTP**, который выполняет корректировку **DNS**-записей в базе данных:

- при добавлении и удалении контроллеров в домен;
- при изменении привязки контроллеров к сайтам;
- при изменении параметров корневых **NTP**-серверов (добавлении и удалении их через портал управления).

Поддерживает выполнение следующих действий:

- Добавление двух динамических записей типа **CNAME** для корневых и простых контроллеров в рамках сайтов (`locations`):

  - `_ntp._udp._roots.ald.company.lan` ведет на `_ntp._udp._roots.{this_location}._locations.ald.company.lan`, где:

    `{this_location}` - конкретный `location` того **DNS**-сервера, который обрабатывает запрос;
  - `_ntp._udp.ald.company.lan` ведет на `_ntp._udp.{this_location}._locations.ald.company.lan`.
- Создание двух множеств **DNS**-записей типа A в рамках сайта (`location`):
  - `_ntp._udp._roots.{some_location}._locations.ald.company.lan` - пул A-записей с корневыми **NTP**-серверами в текущей локации;
  - `_ntp._udp.{some_location}._locations.ald.company.lan` - пул обычных контроллеров домена в текущей локации (может включать все контроллеры домена, если все КД находятся в одном `location`).
- Создание двух множеств **DNS**-записей типа A в рамках домена:
  - `_ntp._udp._roots._default.ald.company.lan` - пул всех корневых **NTP**-серверов домена (**CNAME**), в том числе и тех, у которых признак `location` не заполнен;
  - `_ntp._udp._default.ald.company.lan` - пул контроллеров домена (не **CNAME**), в том числе и тех, у которых признак `location` не заполнен.

3.40.2. Алгоритм автоматической настройки подсистемы NTP

Начиная с версии 2.5.0, на КД устанавливается служба `aldpro-ntp-management`, которая раз в 2 минуты запускает проверку `healthcheck NTP`. Демон **NTP** получает данные из **LDAP**-каталога о записях сайтов, о внешних и корневых **NTP**-серверах домена, данные всех активных КД (по умолчанию в конфигурационном файле `chrony` прописана строка «allow 0/0», что позволяем им выступать в качестве **NTP**-сервера) и данные о **DNS**-записях. Демон проводит расчет того, как должны выглядеть dns-записи, исходя из всех полученных из LDAP-каталога данных, и сверяет это рассчитанное состояние с тем, которое хранится в каталоге. Если все совпадает, то никаких изменений демон не производит, после чего демон засыпает на 2 минуты, затем процедура повторяется.

Внимание: Демон **NTP** `aldpro-ntp-management` устанавливается на каждый КД из состава домена, при этом должен функционировать (находиться в статусе `active(running)`) только на одном КД домена. Для проверки необходимо на каждом КД выполнить команду:
`systemctl is-active aldpro-ntp-management`
На всех КД, кроме одного, этот демон должен иметь состояние `inactive`.

Все запросы к **LDAP**-каталогу этот демон делает под системной учетной записью `uid=saltstackservice,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan`.

Все действия демона записываются в журнал службы `journalctl`, который можно просмотреть командой:

```
journalctl -u aldpro-ntp-management # для просмотра полного лога службы
journalctl -fu aldpro-ntp-management # для потокового просмотра лога службы
```

При добавлении любого КД в домен, в сайт, в состав которого вошел этот КД, добавляются записи в ветку службы **dns** по следующим путям:

```
idnsname=_ntp._udp._default,idnsname={DOMAIN_NAME}.,cn=dns,dc=*  добавляется
↪атрибут aRecord=IP_ADDRESS_DC
idnsname=_ntp._udp.hq._locations,idnsname={DOMAIN_NAME}.,cn=dns,dc=* при
↪добавлении этого КД в сайт hq также добавляется атрибут aRecord=IP_ADDRESS_
↪DC
```

При добавлении внешнего **NTP**-сервера с наименованием `server1`, в ветку **LDAP**-каталога `cn=ntp,cn=services,cn=aldpro,cn=etc,dc*` добавляется запись `ntpserver=server1` с атрибутами:

```
externalntpservertype=server # для пула будет значение pool
isexternal=true
ntpserver=server1
```

В дальнейшем из этой ветки берутся данные при заполнении конфигурации службы `chronyd` на всех компьютерах домена с помощью групповой политики времени (см. ниже).

При добавлении нового корневого **NTP**-сервера домена, т.е. при смене статуса КД с «обычного» на «корневой», его запись (`aRecord` с IP-адресом этого КД) перемещается и располагается между записями в ветке службы **DNS**:

1. из записи сайта для «обычных» КД в запись сайта для «корневых» КД по пути `idnsname=_ntp._udp._roots.hq._locations,idnsname={DOMAIN_NAME}.,cn=dns,dc=*`;

2. добавляется `aRecord=IP-ADDR_DC` в запись `idnsname=_ntp._udp._roots._default,idnsname={DOMAIN_NAME}.,cn=dns,dc=*`.

Помимо этого, в **LDAP**-каталог в ветку `cn=ntp,cn=services,cn=aldpro,cn=etc,dc*` добавляется запись `ntpserver=FQDN_DC`, где `FQDN_DC` - `fqdn` добавленного корневого **NTP**-сервера домена. Эта запись содержит атрибут `isexternal=FALSE` и атрибут `server=FQDN_DC`.

При удалении корневого **NTP**-сервера домена происходит процесс, обратный сценарию добавления нового корневого **NTP**-сервера.

Групповая политика времени берет данные из службы каталога, и вносит в конфигурацию `chrony` необходимую информацию как о наборе параметров, так и о пулах по умолчанию:

```
pool _ntp._udp._roots.ald.company.lan iburst minstratum 12
pool _ntp._udp.ald.company.lan iburst minstratum 13
pool _ntp._udp._roots._default.ald.company.lan iburst minstratum 14
pool _ntp._udp._default.ald.company.lan iburst minstratum 15
```

Также политика дополнительно добавляет следующие строки только корневых КД:

```
pool external_ntp_pool iburst minstratum 11  // при наличии в LDAP записей
↪об одном или нескольких внешних NTP-пулах
server external_ntp_server iburst minstratum 11 // при наличии в LDAP
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
↪записей об одном или нескольких внешних NTP-серверах
```

заменяя значения `external_ntp_pool` на значения атрибутов `ntpserver` тех записей, у которых атрибут `externalntpservertype=pool`` (количество таких строк будет равно количеству записей) и значения `external_ntp_server` на значения атрибутов `ntpserver` тех записей, у которых атрибут `externalntpservertype=server` по такой же схеме.

При удалении КД из домена нигде не должно оставаться атрибутов `aRecord` с IP-адресом этого КД.

При удалении внешних **NTP**-серверов или пулов должно происходить удаление соответствующей записи `cn=ntpserver=DELETED_ITEM` в ветке `cn=ntp,cn=services,cn=aldpro,cn=etc,dc*`. И после срабатывания групповой политики времени (в том числе после перезагрузки корневого КД домена) на всех корневых КД домена эти записи с удаленным сервером/пулом должны пропасть из `/etc/chrony/chrony.conf`.

3.41. Проверка алгоритма хэширования пароля пользователя по умолчанию в ALD Pro

Для уменьшения времени аутентификации и авторизации в LDAP, начиная с версии ALD Pro 3.0.0, изменен алгоритм хэширования пароля, используемый по умолчанию, на PBKDF2-SHA256 (Rust реализация).

Это дает значительный прирост производительности на операции SIMPLE BIND.

Для проверки алгоритма хэширования пароля по умолчанию после чистой установки контроллера домена в терминале от пользователя root выполнить команду:

```
dsconf -D "cn=Directory Manager" ldap://$(hostname -f) config get
↪passwordStorageScheme nsslapd-rootpwstoragescheme
```

Ввести пароль Directory Manager, он же admin:

```
Enter password for cn=Directory Manager on ldap://dc01.aldpro.local:
passwordStorageScheme: PBKDF2-SHA256
nsslapd-rootpwstoragescheme: PBKDF2-SHA256
```

В полях passwordStorageScheme, nsslapd-rootpwstoragescheme должно быть: PBKDF2-SHA256.

Примечание: Хэш пароля, с использованием алгоритма хэширования пароля по умолчанию, применяется только при изменении пароля.

3.42. Удаление информации о серверах и пулах NTP при обновлении ALD Pro

3.42.1. Предусловие

Удаление информации о серверах и пулах **NTP** необходимо для предотвращения возможных конфликтов или ошибок в работе **Групповых политик**, а именно параметров по настройке `chrony`, обновлённой версии **ALD Pro**.

Эта инструкция актуальна при обновлении **ALD Pro** на контроллерах домена с версии 2.4.1 до более новых версий.

Внимание: Если резервной копии файла `chrony.conf` нет, ее можно сохранить на случай необходимости восстановления предыдущих настроек.

3.42.2. Последовательность действий

1. Необходимо открыть файл конфигурации `chrony.conf` для редактирования.

Файл расположен по адресу `/etc/chrony/chrony.conf`. Для редактирования можно использовать любой удобный текстовый редактор, например **nano** или **kate**.

Команда для запуска **nano**:

```
sudo nano /etc/chrony/chrony.conf
```

1. Удалить строки, содержащие информацию о серверах и пулах NTP, т.е. все строки, которые начинаются с ключевых слов `server` и `pool`.

Например:

```
server ntp.example.com iburst
pool 2.pool.ntp.org iburst
```

1. Сохранить изменения в файле и выйти из редактора: для **nano** нажать `Ctrl + O`, затем `Enter`, чтобы сохранить файл. Для выхода нажать `Ctrl + X`.

2. Проверить, что информация о серверах и пулах удалена.

Для этого необходимо выполнить следующую команду:

```
grep -i 'server' /etc/chrony/chrony.conf | wc -l; grep -i 'pool' /etc/chrony/
↪chrony.conf | wc -l
```

- Первая часть команды подсчитает строки с ключевым словом `server`.
- Вторая часть команды подсчитает строки с ключевым словом `pool`.

Если все строки удалены, обе команды выведут `0`.

1. После внесения изменений необходимо перезапустить службу `chronyd`, чтобы настройки вступили в силу:

```
sudo systemctl restart chronyd
```

1. Проверить статус службы `chronyd` и убедиться, что служба работает корректно:

```
sudo systemctl status chronyd
```

Если служба запущена, появится строка с текстом `Active: active (running)`.

3.43. Настройка мониторинга целостности каталога

3.43.1. Введение

Инструкция описывает настройку контроллеров домена и подсистемы мониторинга для отображения данных из LDAP.

К инструкции прилагается файл скрипта. Скрипт располагается в папке «Скрипт мониторинга целостности каталога». (Личный кабинет → Дистрибутивы → aldpro → Без сертификации/x86_64 → 3.0 → Документы → 3.0.0)

3.43.2. Действия на контроллерах домена

1. Создать директорию `/etc/zabbix/scripts/`:

```
mkdir /etc/zabbix/scripts/
```

1. Переместить скрипт `getobjects.py` в директорию `/etc/zabbix/scripts/`

2. Сделать скрипт исполняемым:

```
chmod +x /etc/zabbix/scripts/getobjects.py
```

4. В файл `/etc/zabbix/zabbix_agentd.conf.d/userparameters.conf` добавить строку:

```
echo "UserParameter=getobjects,python3 /etc/zabbix/scripts/getobjects.py --
↪ldap-server \"localhost\" --ldap-port 389 --bind-dn \"cn=Directory Manager\
↪" --bind-password \"password\" --base-dn \"DC=test,DC=lan\" --dump" >> /etc/
↪zabbix/zabbix_agentd.conf.d/userparameters.conf
```

где:

- `--ldap-server` – адрес сервера LDAP;
- `--ldap-port` – порт для подключения к каталогу;

- `--bind-dn` – учетная запись для подключения к каталогу (рекомендуется использовать УЗ Directory Manager);
- `--bind-password` – пароль учетной записи;
- `--base-dn` – стартовая точка поиска в каталоге.

5. Проверить, что строки добавлены:

```
grep "getobjects" /etc/zabbix/zabbix_agentd.conf.d/userparameters.conf
```

6. Разрешить сервису `zabbix` выполнять скрипт:

```
sed -i -e 's/EnableRemoteCommands=1/AllowKey=system.run[*]/g' /etc/zabbix/
↪zabbix_agentd.conf.d/zabbix_agent.conf
```

7. Перезапустить агент мониторинга:

```
systemctl restart zabbix-agent
```

8. Убедиться в работе скрипта:

```
zabbix_agentd -t getobjects
```

Пример вывода команды:

```
getobjects                                        [t|{
"users": 1,
"computers": 3,
"services": 10,
"usergroups": 6,
"hostgroups": 2,
"hbacrules": 2,
"sudorules": 0,
"dnszones": 2,
"certificates": 0,
"replication_conflicts": 0
}]
```

3.43.3. Действия на подсистеме мониторинга

3.43.3.1. Действия на web-портале Zabbix

Примечание: Для перехода на web-портал `zabbix` необходимо перейти по адресу https://mon.test.lan/zabbix,

где: - mon - идентификатор сервера мониторинга; - test.lan - имя домена; - /zabbix - подсистема на которую мы авторизуемся на сервере мониторинга.

В поле логина указать `aldpro_srv_zabbix`. В поле пароль указать данные из файла `/etc/systemd/system/aldpro-zabbix-discovering-systemd.conf`, расположенного на сервере мониторинга.

1. Перейти в Configuration → Templates → Подсистема «Служба каталогов» → Items и создать новый Item (Create Item)

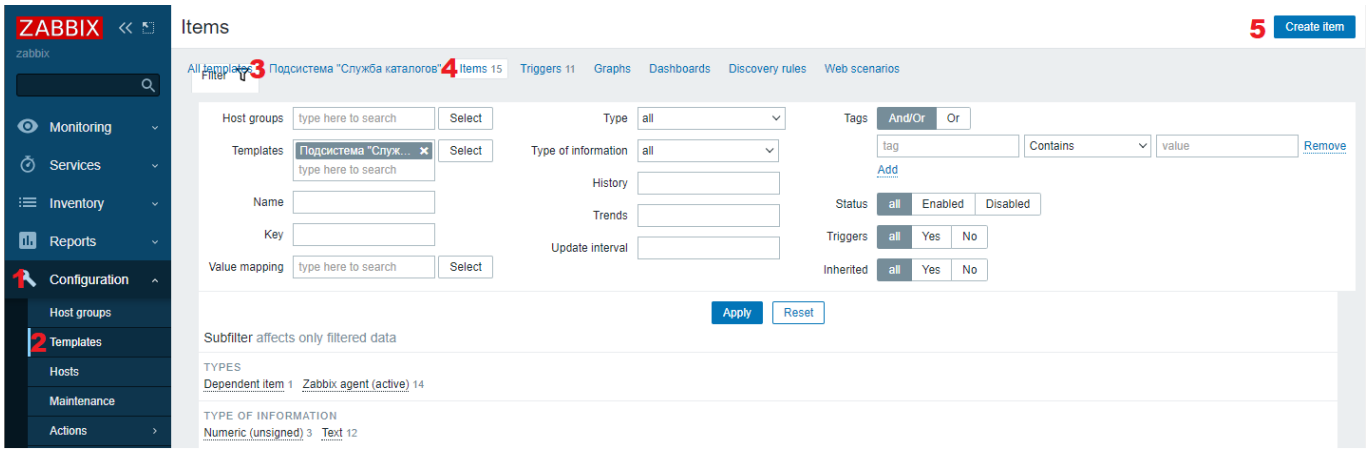


Рисунок 3.120 – Создание нового Item

Заполнить следующие данные:

Name	Type	Key	Type of information
getobjects	Zabbix agent (active)	getobjects	Text

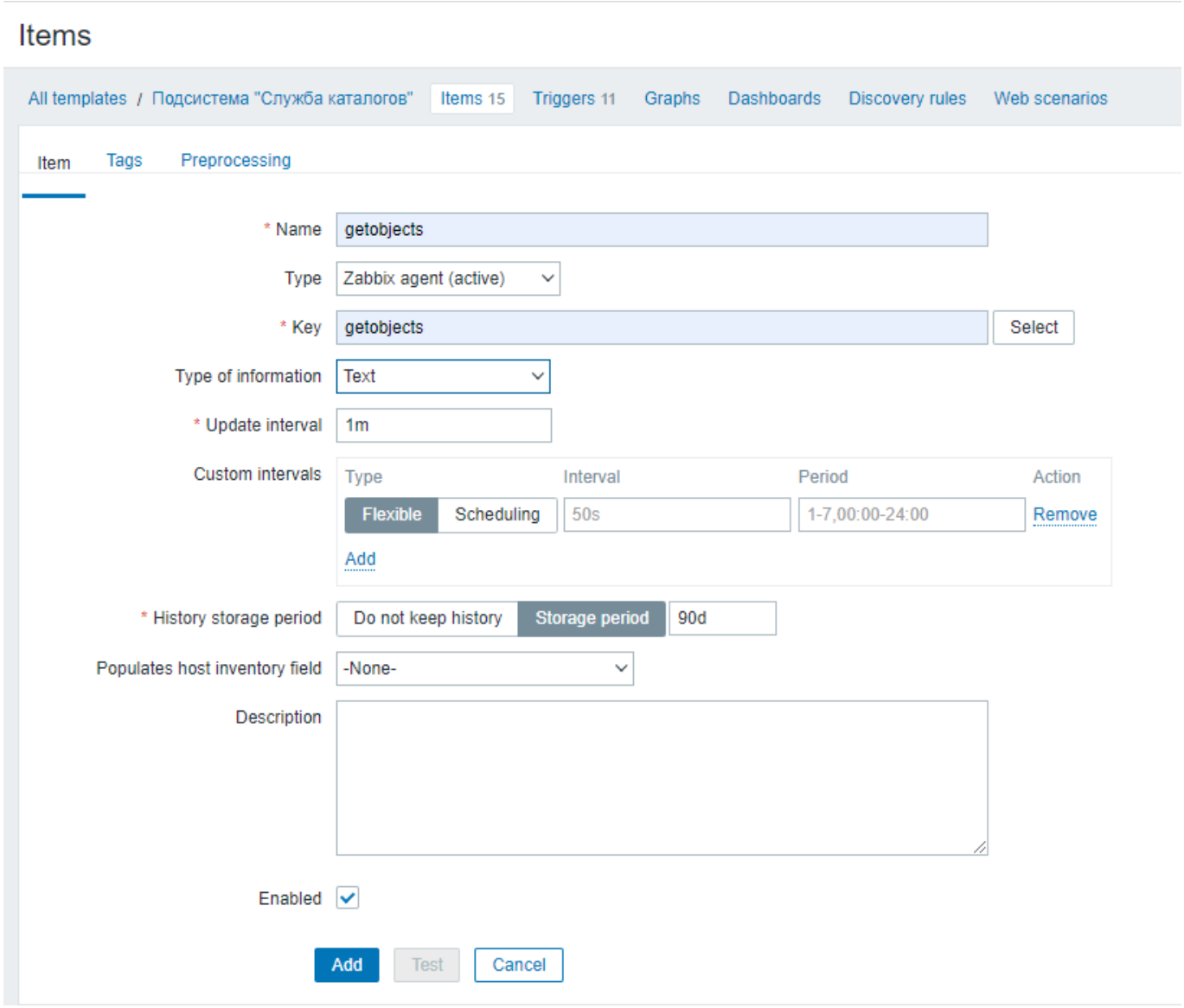


Рисунок 3.121 – Items

2. Создать связанные элементы данных. Для этого перейти в **Configuration → Templates → Подсистема «Служба каталогов» → Items → Create Item**

Заполнить следующие данные:

Вкладка Item	
Name	getobjects.users
Type	Dependent item
Key	getobjects.users
Master item	Подсистема «Служба каталогов»: getobjects
Вкладка Preprocessing	
Name	JSONPath
Parameters	$.users
Type of information	Numeric (unsigned)

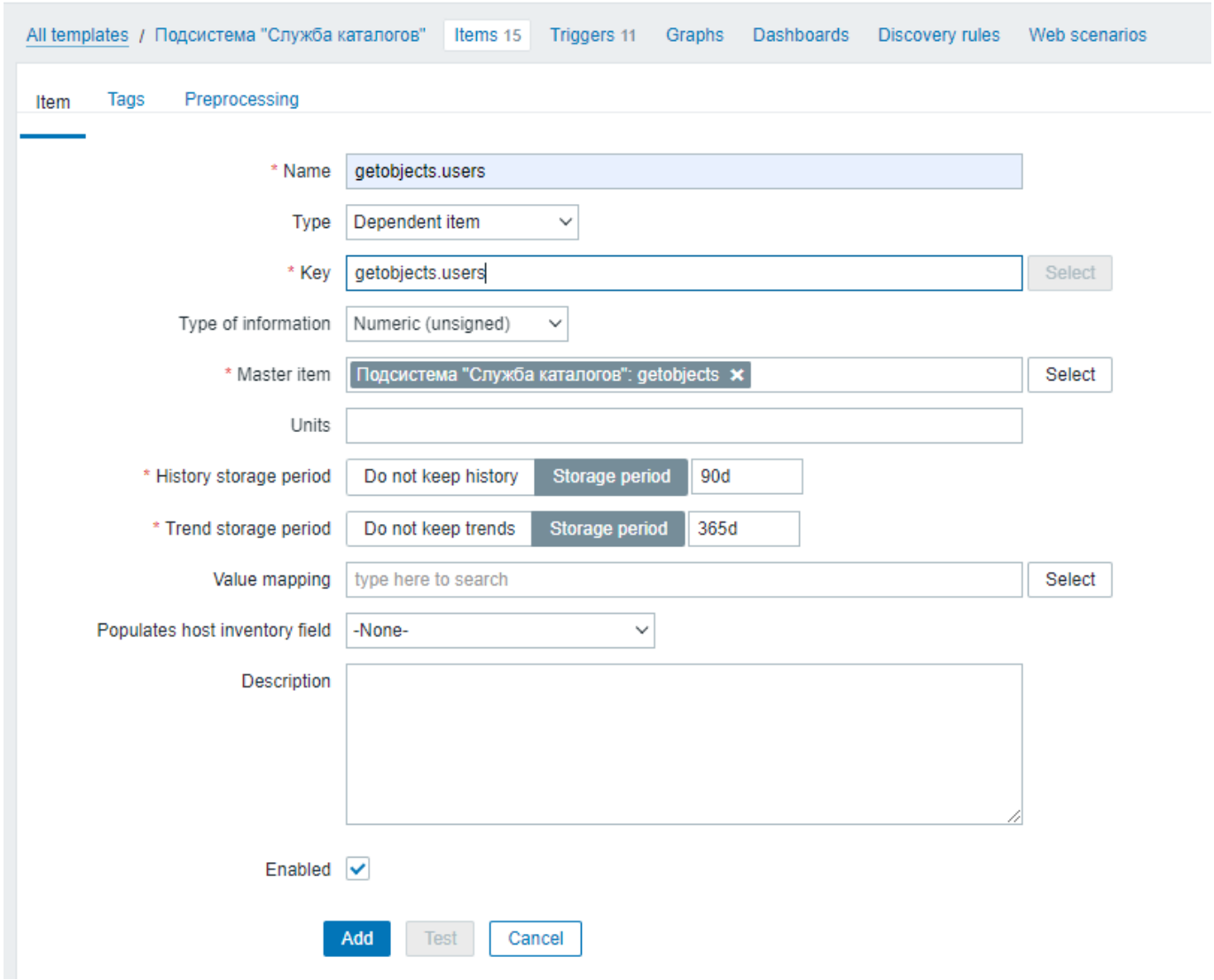


Рисунок 3.122 – Вкладка Item

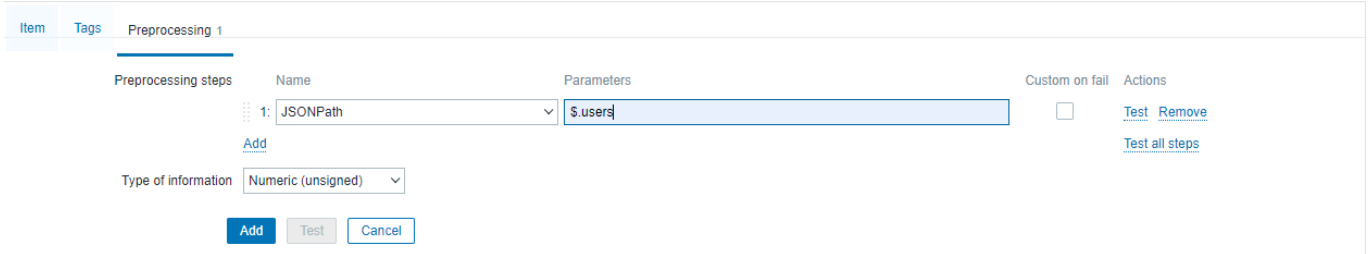


Рисунок 3.123 – Вкладка Preprocessing

Нажать кнопку [**Add**]

Данный пример показывает создание связанных элементов данных для типа объектов `users`. Для остальных типов элементы данных создаются аналогичным образом.

Перечень типов объектов:

- `total`;

- users;
- computers;
- services;
- usergroups;
- hostgroups;
- hbacrules;
- sudorules;
- dnszones;
- certificates;
- replication_conflicts.

3. Проверить корректность настроек:

Проверить получение и обработку данных можно на странице Latest data. Для этого установить фильтр `getobjects` по полю Name. Нажать кнопку [**Apply**] (применить).

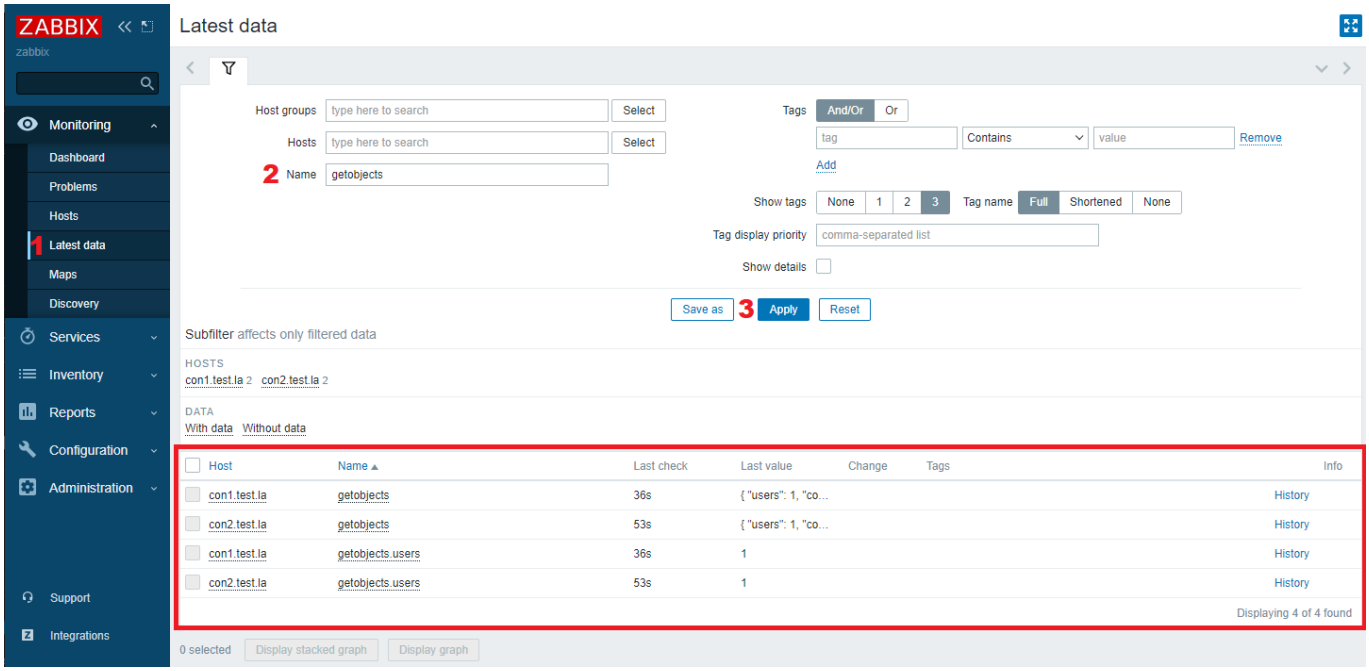


Рисунок 3.124 – Вкладка Latest data

3.43.3.2. Действия в терминале

Разрешаем серверу `zabbix` запуск скриптов на удаленной машине без ввода пароля sudo. Необходимо внести изменения в файл `/etc/sudoers.d/zabbix`. Привести файл к виду:

```
zabbix ALL = (ALL) NOPASSWD: /usr/bin/nmap -O *, /etc/zabbix/scripts/
↪getobjects.py
```

3.43.3.3. Действия выполняемые в web-портал Grafana

Примечание: Для перехода на web-портал `grafana` необходимо перейти по адресу https://mon.test.lan:3000/aldpro/dashboards,

где: - mon - идентификатор сервера мониторинга; - test.lan - имя домена; - :3000 - подсистема на которую мы авторизуемся на сервере мониторинга.

В поле логина указать `admin`. В поле пароль указать данные из файла `/etc/systemd/system/aldpro-zabbix-discovering-systemd.conf` расположенного на сервере мониторинга.

Вариант 1. Панели с последними значениями

1. Перейти на страницу Dashboards. **Home** → **Dashboards** → **New** → **New Dashboard**

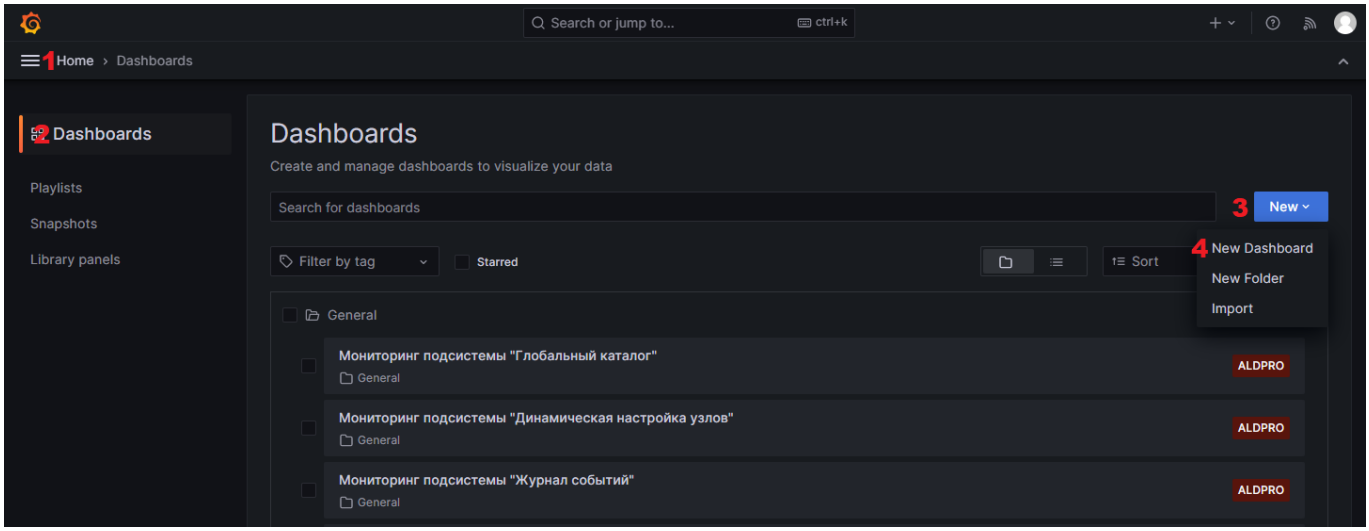


Рисунок 3.125 – Страница Dashboards

2. Создать визуализацию. Нажать на кнопку [**+ Add visualization**]

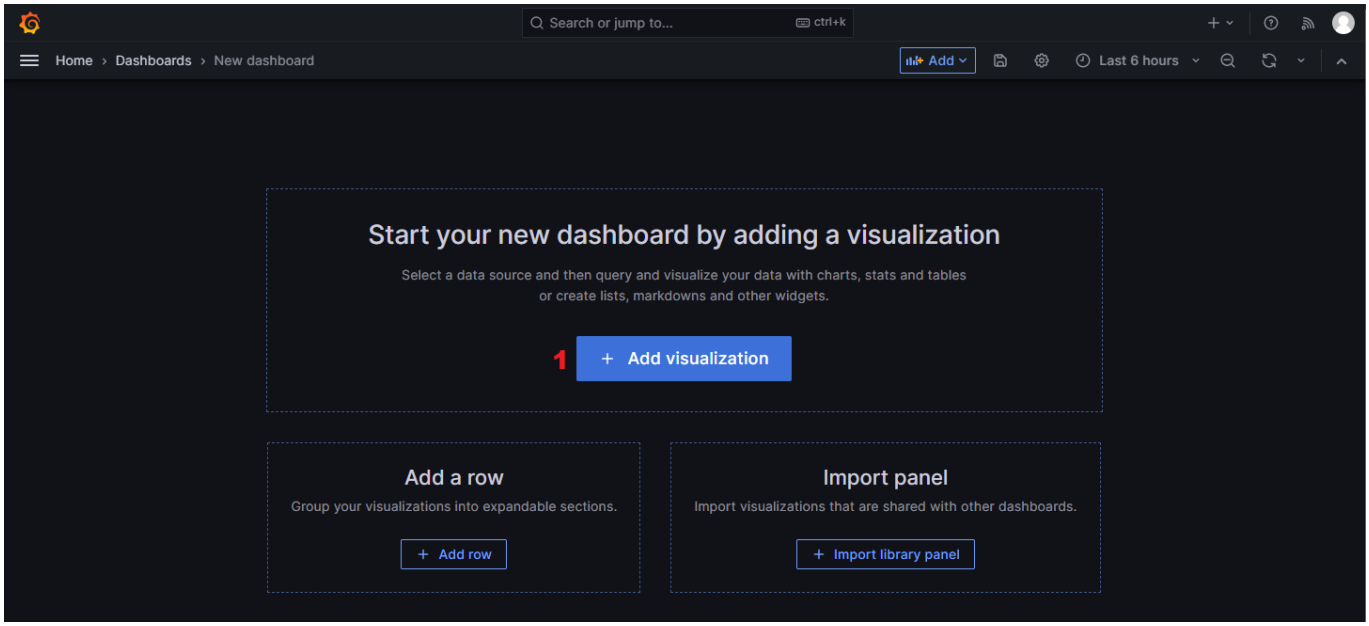


Рисунок 3.126 – Страница New dashboards

3. Выбрать как источник данных Zabbix

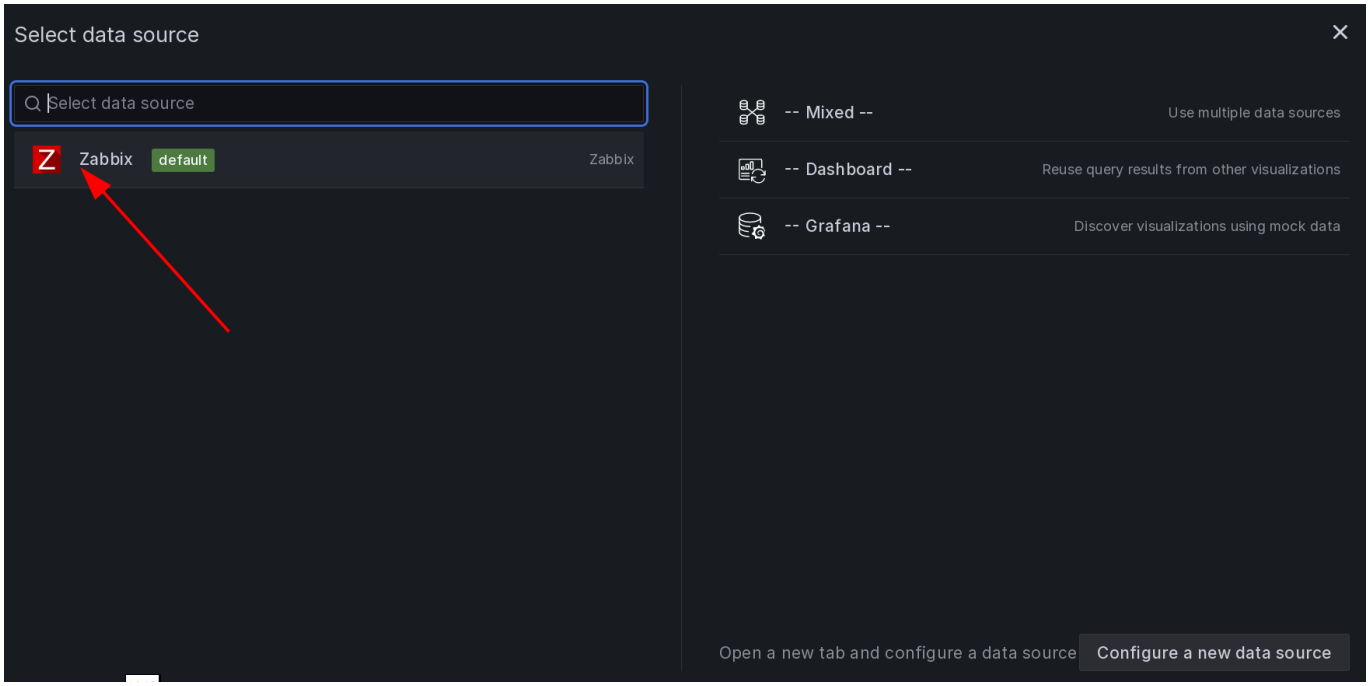


Рисунок 3.127 – Выбор источника данных Zabbix

4. Заполнить настройки панели визуализации

Group	ALD Pro discovery
Host	/.*/
Item	getobjects.users
Visualisations > Stat	
Suggestions > Stat colored background	
Panel options	
Title	Users
Value options	
Show	Calculate
Calculation	Last
Stat styles	
Text mode	Value или Value and Name
Color mode	Background Gradient
Apply	

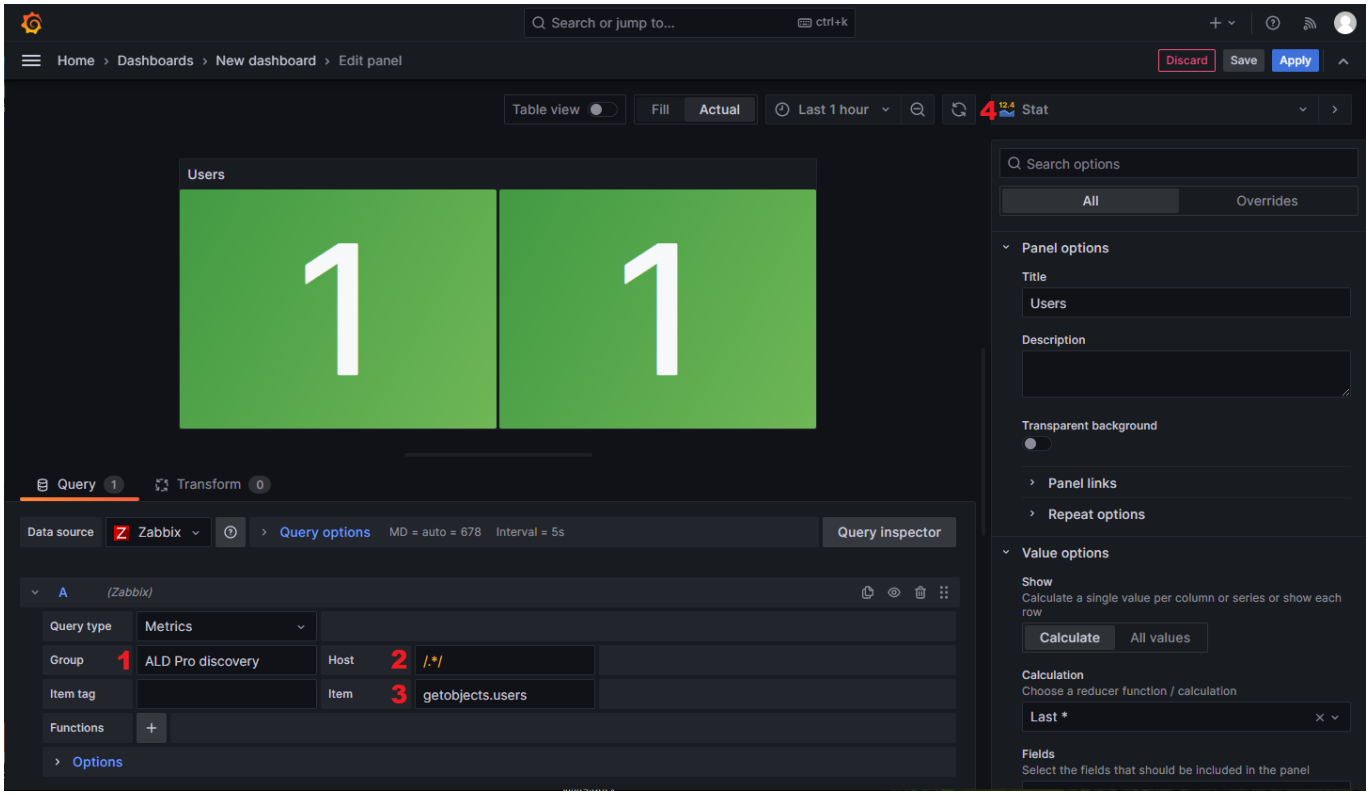


Рисунок 3.128 – Настройки панели визуализации



Рисунок 3.129 – Настройки панели визуализации

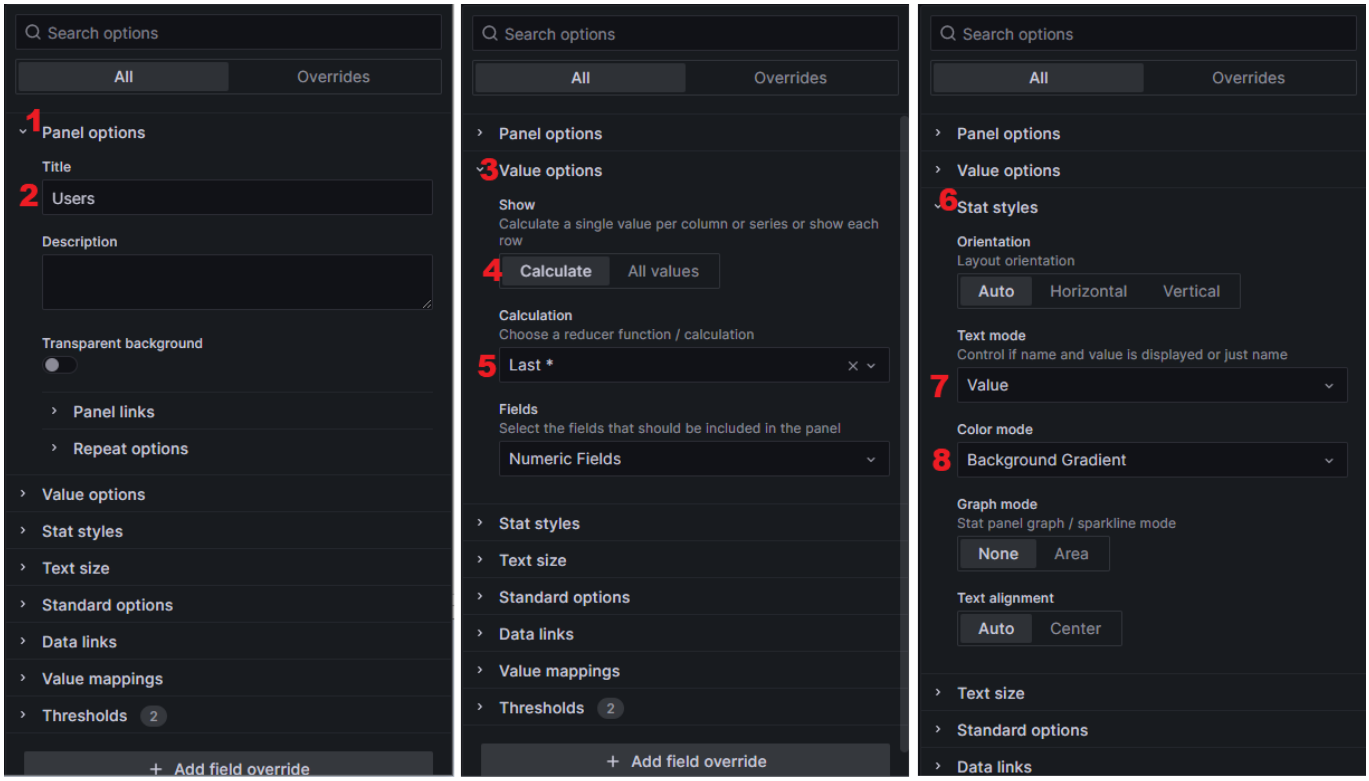


Рисунок 3.130 – Настройки панели визуализации

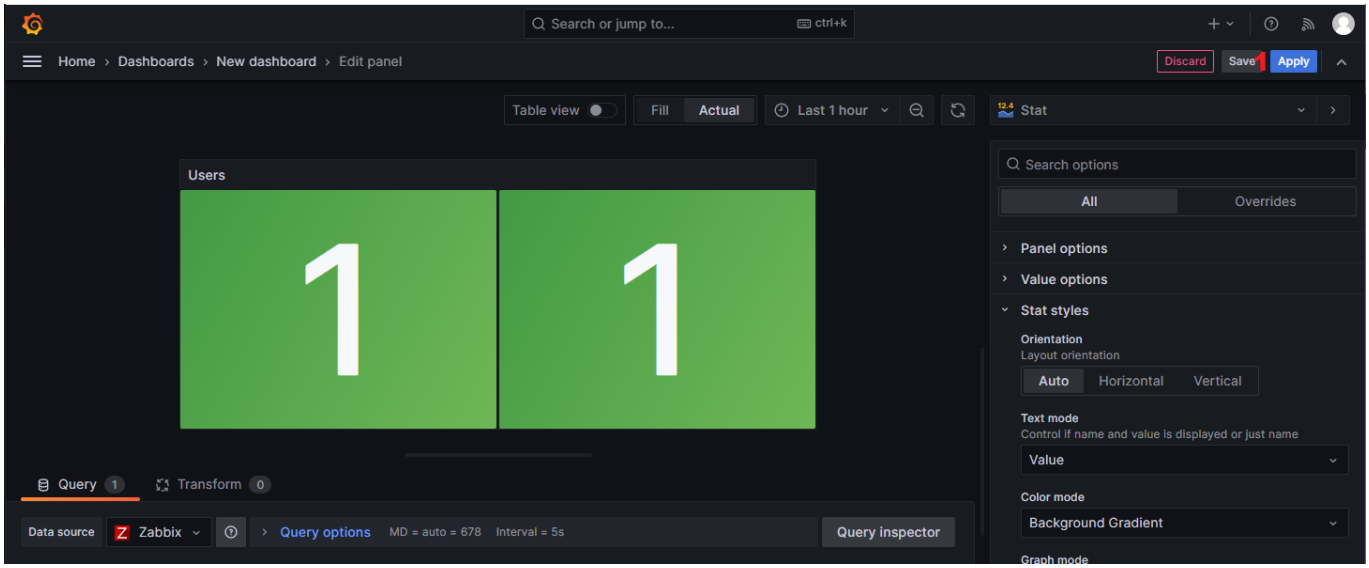


Рисунок 3.131 – Настройки панели визуализации

5. Повторить создание блоков визуализации для остальных типов элементов:

- `total`;
- `users`;
- `computers`;
- `services`;
- `usergroups`;
- `hostgroups`;

- `hbacrules`;
- `sudorules`;
- `dnszones`;
- `certificates`;
- `replication_conflicts`.

Вариант 2. Столбчатая диаграмма

1. Перейти на страницу Dashboards. **Home** → **Dashboards** → **New** → **New Dashboard**
2. Создать визуализацию. Нажать на кнопку [**+ Add visualization**]
3. Заполнить настройки панели визуализации

Group	ALD Pro discovery
Host	/.*/
Item	getobjects.users
Visualisations > Time series	
Panel options	
Title	Users
Apply	

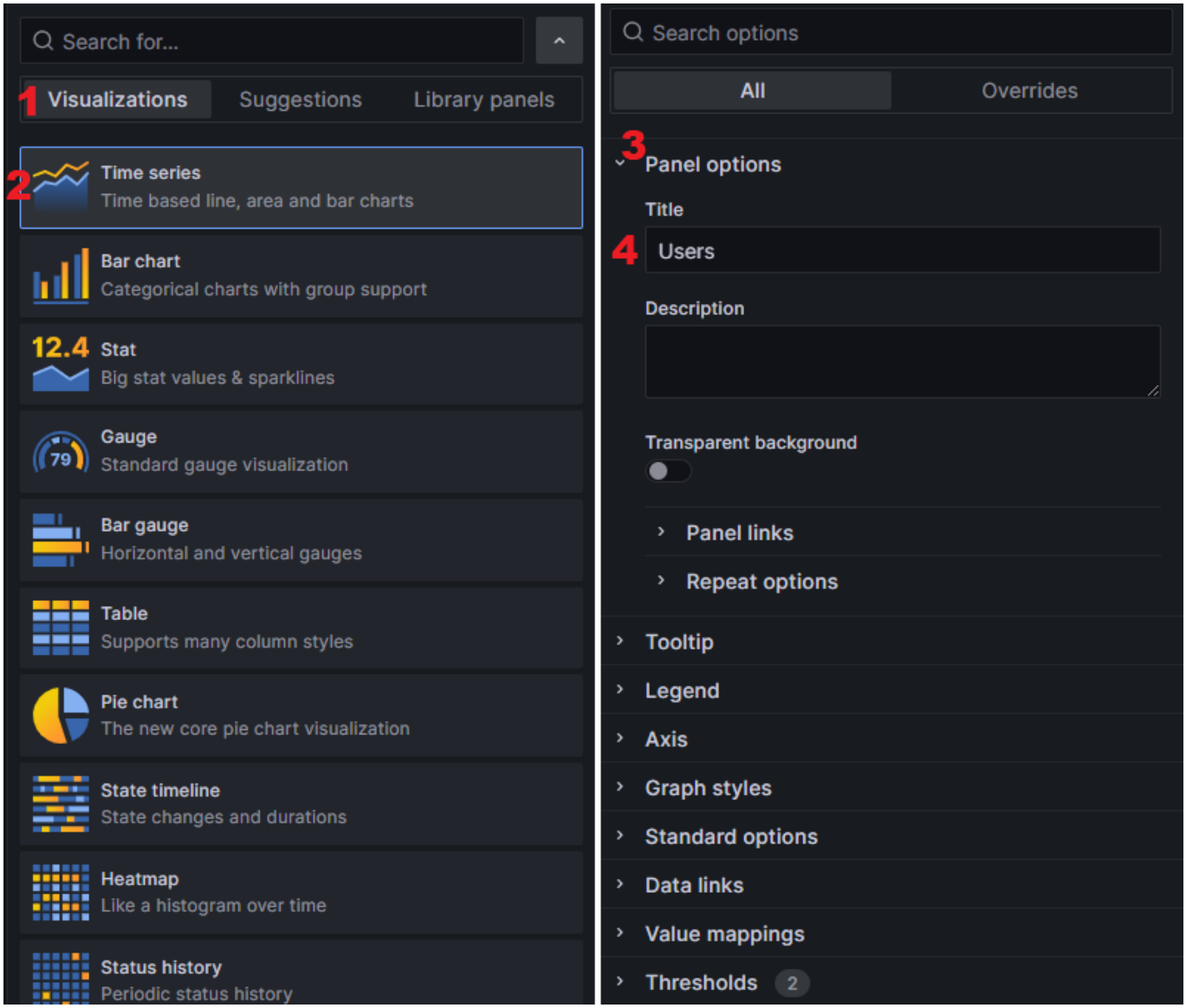


Рисунок 3.132 – Настройки панели визуализации



Рисунок 3.133 – Настройки панели визуализации

4. Повторить создание панелей визуализации для остальных типов элементов

Расположение и размер панелей настраиваются в соответствии с требованиями. После создания всех визуализаций дашборд сохраняется.

3.44. Инструкция по настройке автомонтирования с помощью групповых политик ALD Pro

3.44.1. Введение

В Linux существует механизм автоматического монтирования, который работает на связке из нескольких компонентов: * ловушек файловой системы autofs * утилиты automount и службы autofs, которая ее запускает * стандартных компонентов для работы с SMB-ресурсами – файловой системы cifs и утилит для их монтирования из пакета cifs-utils.

Механизм автоматического монтирования реализует в Linux функции, аналогичные DFS от Microsoft Windows. В рамках ALD Pro разработан параметр групповой политики для подключения сетевых дисков с использованием механизма автомонтирования. Linux-утилита automount позволяет использовать карты монтирования, которые управляются централизованно через службу каталога. Подключение (монтирование) удалённых ресурсов с Samba файлового сервера выполняется в момент обращения к ним со стороны пользователя на клиенте. Такая реализация позволяет утилите automount избежать задержек при загрузке компьютера и входе пользователя в систему.

3.44.2. Автомонтирование в Linux

3.44.2.1. Общий механизм работы

Работу механизма автоматического монтирования в Linux обеспечивают несколько компонентов:

1. Служба autofs — запускает утилиту automount от имени суперпользователя в момент загрузки операционной системы. Это systemd-служба, входит в состав deb-пакета autofs.

2. Утилита automount — обеспечивает расстановку ловушек монтирования и подключение целевых файловых систем общих ресурсов в соответствии с настройками из конфигурационных файлов, основными из которых являются /etc/autofs.conf и /etc/auto.master. Утилита входит в состав deb-пакета autofs.

3. Файловая система autofs — монтируется утилитой automount в первоначальный набор каталогов, чтобы превратить их в так называемые триггерные узлы (англ. trigger nodes) или ловушки монтирования (англ. mount traps). Файловая система реализована в виде модуля ядра операционной системы autofs4.ko. Когда модуль файловой системы autofs перехватывает запрос пользователя к каталогу, в который еще не смонтирована целевая файловая система общего ресурса, модуль обращается к запущенному экземпляру утилиты automount для выполнения этой операции. Взаимодействие между модулем autofs4 и утилитой automount осуществляется через именованные каналы (англ. FIFO, first input first output), файлы которых можно найти по маске /var/run/autofs.fifo-*.

4. Файловая система cifs — монтируется утилитой automount по запросу со стороны модуля ядра autofs4, когда пользователь обращается к файлам общего ресурса, для которого параметр «fstype» равен «cifs». Эта файловая система реализована в виде модуля cifs.ko.

5. Утилита mount.cifs — вызывается утилитой automount для монтирования общих ресурсов по протоколу CIFS (SMB). Утилита входит в состав deb-пакета cifs-utils.

Рассмотрим работу механизма автоматического монтирования на примере простой общей папки с документами. Допустим, что в файле /etc/auto.master у нас определена строка для подключения карты косвенного монтирования /etc/auto.docs, а в карте /etc/auto.docs определена строка для монтирования общей папки share с файлового сервера fs-1.ald.company.lan в каталог /docs/share:

```
cat /etc/auto.master
...
/docs                                    /etc/auto.docs
...


cat /etc/auto.docs
share  -fstype=cifs,user,sec=krb5,cruid=$UID,uid=$UID,gid=$UID     ://fs-1.
 ↪ald.company.lan/share
```

На данном этапе, файл /docs является ловушкой монтирования в виртуальной файловой системе autofs. При взаимодействии пользователя с ловушкой монтирования как с директорией, запускается процедура монтирования директории с файлового сервера общей папки share с файлового сервера fs-1.ald.company.lan в каталог /docs. Поэтому /docs до момента взаимодействия с пользователей не является директорией.

Таким образом, в момент запуска утилита automount выполняет следующие действия:

- Загружает пространство имен, начиная с главного файла */etc/auto.master*.
- Создает каталог */docs*, если его не было ранее.
- Монтирует в каталог */docs* файловую систему *autofs*, чтобы установить ловушку монтирования. Проверить это можно с помощью утилиты *findmnt*`:

```
sudo findmnt
TARGET                          SOURCE                          FSTYPE       
↪OPTIONS
...
└─/docs                         /etc/auto.docs                  autofs        rw,
↪relatime,fd=7,pgrp=10901...
```

Теперь при первом обращении пользователя к каталогу /docs/share, например, с помощью утилиты cd или ls, сработает ловушка монтирования, установленная на каталог /docs. Модуль файловой системы autofs обратится к утилите automount, которая создаст каталог share и смонтирует в него общую папку с файлового сервера с помощью утилиты mount. Проверить это можно с помощью утилиты findmnt:

```
root@pc-1:~# findmnt
TARGET                          SOURCE           FSTYPE        OPTIONS
/                               /dev/sda1        ext4          rw,relatime,
↪errors=remount-ro
...
└─/docs                         /etc/auto.docs autofs     rw,relatime,fd=7,
↪pgrp=10901,timeout=300,...
└─/docs/share                 //fs-1.ald.company.lan/share   cifs        rw,
↪nosuid,nodev,noexec,relatime, vers=3.1.1,sec=krb5,cruid=310400000,
↪cache=strict,username=root,uid=310400000,noforceuid,gid=310400
```

Учитывая, что обычные пользователи работают с общими файловыми ресурсами не по прямым ссылкам, а из файлового менеджера, в файле /etc/autofs.conf рекомендуется установить параметр «browse_mode = yes», чтобы имя общей папки share отображалось всегда, вне зависимости от того, примонтирована она или нет. По умолчанию установлено значение «no» для повышения производительности, но это актуально только в случае очень больших карт монтирования, в которых содержатся ссылки на десятки или даже сотни общих ресурсов. Не рекомендуется использование параметра –ghost в опциях монтирования карты auto.docs из главной карты, т.к. способ считается устаревшим.

3.44.2.2. Управление службой autofs

В операционной системе Astra Linux утилита automount автоматически запускается службой autofs. Управлять службой можно с помощью утилиты systemctl обычными командами start, stop, restart. Проверить текущее состояние можно с помощью команды status:

```
root@pc-1:~# systemctl status autofs
autofs.service - Automounts filesystems on demand
Loaded: loaded (/lib/systemd/system/autofs.service; enabled; vendor preset:
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
 ↪enabled)
Active: active (running) since Sun 2024-10-20 16:15:23 MSK; 966ms ago
Process: 23356 ExecStart=/usr/sbin/automount -d -v $OPTIONS --pid-file /var/
 ↪run/autofs.pid (code=exited, status=0/SUCCESS)
Main PID: 23357 (automount)
    Tasks: 5 (limit: 4593)
Memory: 1.0M
    CPU: 21ms
CGroup: /system.slice/autofs.service
        └─23357 /usr/sbin/automount -d -v --pid-file /var/run/autofs.pid
```

В целях отладки можно в файле /lib/systemd/system/autofs.service установить запуск утилиты с ключами -d (англ. debug) и -v (англ. verbose), как на представленном выше примере, и смотреть файлы журналов syslog. Но проще запускать утилиту с ключом -f (англ. foreground):

```
root@pc-1:~# automount -f -d -v
Starting automounter version 5.1.2, master map /etc/auto.master
using kernel protocol version 5.05
lookup_nss_read_master: reading master file /etc/auto.master
do_init: parse(sun): init gathered global options: (null)
...
```

Завершить работу утилиты в этом случае можно сочетанием клавиш <Ctrl> + <C>:

```
^Cdo_notify_state: signal 2
master_notify_state_change: sig 2 switching /docs from 1 to 5
st_prepare_shutdown: state 1 path /docs
....
autofs stopped
```

Если вы по ошибке запустите утилиту automount без параметров, то она начнет работать в фоновом режиме, что можно будет увидеть с помощью команды ps:

```
root@pc-1:~# automount
root@pc-1:~# ps aux | grep automount
root     27976  0.0  0.1 114340  4100 ?        Ssl  22:32   0:00 automount
root     27990  0.0  0.0   6228   868 pts/0    S+   22:32   0:00 grep
 ↪automount
```

Завершить работу такого процесса можно будет отправкой ему сигнала SIGTERM:

```
root@pc-1:~# kill -SIGTERM $(pidof automount)
root@pc-1:~# ps aux | grep automount
root     27995  0.0  0.0   6228   884 pts/0    S+   22:32   0:00 grep
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
↪automount
```

При завершении работы утилита `automount` удаляет каталоги, используемые в качестве точек монтирования, если эти каталоги не существовали на момент запуска, но в некоторых ситуациях, например, при внештатном выключении компьютера, эти каталоги могут оставаться на диске. Будьте крайне внимательны, если у вас появится желание удалить такой каталог вручную, т.к. при наличии монтирования такая команда приведет к удалению всех файлов на общем ресурсе.

3.44.2.3. Настройка основных параметров

Настройки утилиты automount находятся в конфигурационном файле /etc/autofs.conf, в котором по умолчанию определено две секции для карт монтирования в форматах autofs и amd (automounter от BSD) соответственно.

```
root@pc-1:~# cat /etc/autofs.conf | grep -v '#'
[ autofs ]
master_map_name = /etc/auto.master
timeout = 300
browse_mode = yes
[ amd ]
dismount_interval = 300
```

Дополнительные секции могут быть определены для точек монтирования в формате amd, но в рамках настоящего документа мы будем рассматривать только основной формат autofs. В секции autofs определены следующие три основных параметра:

- master_map_name — определяет, что главная карта будет загружаться из файла /etc/auto.master. Рекомендуется оставлять это значение по умолчанию.
- timeout — задает интервал времени в секундах, по истечению которого общий ресурс должен быть автоматически размонтирован, если к нему не поступает больше обращений со стороны пользователей. По умолчанию 300 секунд (5 минут).
- browse_mode — определяет, должна ли утилита automount сразу создавать каталоги для монтирования общих ресурсов. Учитывая, что пользователи будут работать с общими ресурсами из файлового менеджера, рекомендуется установить значение «yes». По умолчанию установлено значение «no» для повышения производительности.

Описание дополнительных параметров вы сможете получить с помощью команды man autofs.conf

3.44.2.4. Настройка карт монтирования

В приложении automount пространство имен распределенной файловой системы настраивается с помощью конфигурационных файлов, которые называются картами монтирования. Эти файлы находятся в папке /etc и начинаются с префикса «auto.*». По назначению и используемому синтаксису карты разделяются на несколько типов, описаны ниже.

Главная карта

Главная карта (англ. master map) это файл, на который указывает параметр master_map_name из конфигурационного файла /etc/autofs.conf. Главная карта является точкой входа для построения пространства имен, но из этого файла не получится подключить конкретные общие ресурсы, т.к. главная карта содержит ссылки только на другие карты монтирования — прямые, косвенные и специальные. Кроме ссылок на другие карты в главной карте могут быть инструкции для включения содержимого из дополнительных источников, например, из других файлов или через механизм NSS.

Карты прямого монтирования

Карты прямого монтирования (англ. direct maps) — это файлы, которые встраиваются в пространство имен из главной карты с помощью специальной точки монтирования «/-». Если в главной карте определено несколько карт прямого монтирования, то содержимое этих файлов будет суммироваться. Карты прямого монтирования называются «прямыми», потому что файловая система **autofs** монтируется напрямую в каталоги, определенные точками монтирования этих карт. Например, если в файле */etc/auto.direct`* задана ссылка с точкой монтирования */docs/share*, то файловая система **autofs** будет смонтирована напрямую в каталог */docs/share*, и он станет ловушкой монтирования, что можно будет проверить с помощью утилиты **findmnt**.

Карты косвенного монтирования

Карты косвенного монтирования (англ. indirect maps) — это файлы, которые встраиваются в пространство имен одним из следующих способов: * из главной карты, если в качестве точки монтирования указан абсолютный путь к каталогу; * из других карт, если задан параметр монтирования «-fstype=autofs».

Если несколько карт косвенного монтирования используют одну и туже точку монтирования, то будет подключена только первая из них. Остальные записи утилита **automount** проигнорирует.

Карты косвенного монтирования называются «косвенными», потому что файловая система **autofs** монтируется не напрямую в каталоги, определенные точками монтирования этих карт, а в родительские каталоги. Например, если в главной карте определена точка монтирования */docs* с ссылкой на карту */etc/auto.share*, а в карте *auto.share*, в свою очередь, определена точка монтирования share, ведущая уже на файловый сервер, то файловая система autofs будет смонтирована в родительский каталог */docs*, а не */docs/share*.

Карты косвенного монтирования позволяют формировать сведения динамически с помощью символов подстановки («*» и «&») и программных карт.

Программные карты

Программные карты (англ. program map) — это разновидность карт косвенного монтирования, когда на файл устанавливается атрибут исполнения +x. Исполняемый код получает имя точки монтирования в качестве параметра и должен передать необходимые параметры для монтирования в стандартный поток вывода.

Специальные карты

Специальные карты (англ. special maps) — это карты, содержимое которых предопределено в программном коде утилиты *automount*. Для того, чтобы указать

специальную карту, в сведениях для монтирования нужно использовать одно из следующих значений: * -hosts — подключает специальную карту NFS-ресурсов. Если в главной карте будет определена строка «/net -hosts», то при обращении к каталогу «/net/moscow» в эту точку будут автоматически смонтированы ресурсы сервера moscow по протоколу NFS. Аналогичную функциональность для CIFS-ресурсов предоставляет программная карта */etc/auto.smb*` * -passwd — подключает домашние директории пользователей с NFS-сервера. * -null — позволяет занулить точку монтирования, чтобы исключить ее последующее использование. Учитывая, что утилита automount использует только первое значение ключа, строка с значением «-null» должна быть в самом начале.

3.44.2.5. Синтаксис главной карты монтирования

Главная карта может содержать строки для подключения других карт. Синтаксис этих строк следующий:

Точка_монтирования Карта_монтирования [Параметры]

Где:

- **Точка_монтирования** (или ключ монтирования) — для карт косвенного монтирования указывается абсолютный путь, по которому следует монтировать карту, например /docs, а для подключения карт прямого монтирования нужно указать значение «/-». Если указано несколько карт прямого монтирования, их содержимое суммируется. Если указано несколько карт косвенного монтирования, использующих один и тот же ключ, утилита automount будет использовать только первое значение, а остальные проигнорирует.
- **Карта_монтирования** — если карта находится на диске, то указывается абсолютный путь к файлу в формате /etc/auto.direct или file:/etc/auto.direct. Если содержание карты извлекается через механизм NSS, то указывается просто имя карты, например, auto.direct.
- **Параметры** — необязательная часть. Например, можно переопределить значение timeout и указать «–timeout=600»

Кроме ссылок на карты прямого и косвенного монтирования главная карта может содержать инструкции для включения содержимого из других источников:

- **Инструкция «+file:file_path»** — позволяет включить в главную карту содержимое отдельного файла. Например, если вы захотите вынести описание карты косвенного монтирования /docs в отдельный файл /etc/auto.master.docs, то его можно будет включить следующим образом:

```
cat /etc/auto.master
...
+file:/etc/auto.master.docs
...
```

- Инструкции «+dir:dir_path» — позволяет включить в главную карту содержимое всех файлов из указанной директории. Имена включаемых файлов должны заканчиваться на «.autofs». Файлы будут проигнорированы, если в их имени нет указанного суффикса или имя начинается с точки, т.е. файлы являются скрытыми. Например, по умолчанию в главную карту включается содержимое файлов из каталога /etc/auto.master.d. Поэтому того же эффекта, как в предыдущем примере, можно достичь, если скопировать файл /etc/auto.master.docs в папку /etc/auto.master.d под именем docs.autofs:

```
cp /etc/auto.master.docs /etc/auto.master.d/docs.autofs
cat /etc/auto.master
...
+dir:/etc/auto.master.d
...
```

- Инструкция «+map_name» — позволяет включить в главную карту содержимое через механизм NSS по указанному имени. Например, по умолчанию в главную карту включается содержимое карты auto.master, и, учитывая, что в файле /etc/nsswitch.conf определена строка «automount: sss», карта с именем auto.master на компьютерах в домене FreeIPA загружается из LDAP-каталога через службу SSSD.

```
cat /etc/auto.master
...
+auto.master
...
```

3.44.2.6. Синтаксис карты прямого монтирования

Карта прямого монтирования может содержать строки для монтирования общих ресурсов и подключения карт косвенного монтирования. Синтаксис этих строк следующий:

Точка_монтирования [Параметры] Расположение

Где:

- Точка_монтирования — указывает абсолютный путь, по которому следует выполнить монтирование.
- Параметры — определяют параметры монтирования. Например, для подключения карты косвенного монтирования нужно использовать параметр -fstype=autofs.
- Расположение — указывает на общий ресурс или карту косвенного монтирования.

> **Примечание:** Примечание: В справочных материалах по automount можно встретить упоминания о том, что расположение может указывать на несколько файловых систем сразу для отказоустойчивости и географической балансировки, но это актуально только для NFS-ресурсов, а в случае CIFS-ресурсов такое эта функция недоступна.

3.44.2.7. Синтаксис карты косвенного монтирования

Карта косвенного монтирования может содержать строки для монтирования общих ресурсов и подключения вложенных карт косвенного монтирования. Синтаксис этих строк такой же, как в картах прямого монтирования, за исключением нескольких моментов:

- Точка монтирования определяет каталог относительно абсолютного пути, заданного родительскими картами монтирования.
- Расположение может указывать на исполняемый файл, который будет получать ключ в качестве параметра и должен вернуть остальные сведения для монтирования в

стандартный поток вывода.

- В строках подключения можно использовать символы подстановки. Более подробный пример будет приведен далее по тексту.

3.44.2.8. Записи множественного монтирования

Карты прямого и косвенного монтирования допускают создание записей множественного монтирования, которые позволяют определить несколько точек монтирования сразу. Допустим, если нужно смонтировать две общие папки `/docs/fs-1/share` и `/docs/fs-1/share2`, то стоит определить каждую из них по отдельности в файле auto.direct :

```
cat /etc/auto.docs

/docs/fs-1/share   -fstype=cifs,user,sec=krb5,cruid=$UID,uid=$UID,gid=$UID  :/
↪/fs-1.ald.company.lan/share

/docs/fs-1/share2  -fstype=cifs,user,sec=krb5,cruid=$UID,uid=$UID,gid=$UID  :/
↪/fs-1.ald.company.lan/share2
```

В этом случае после монтирования список точек монтирования будет выглядеть так:

```
admin@pc-1:~$ findmnt
...
├─/docs/fs-1/share          /etc/auto.direct autofs     rw,relatime,fd=7,...
│ └─/docs/fs-1/share        //fs-1.ald.company.lan/share   cifs       rw,
↪nosuid,nodev,...
└─/docs/fs-1/share2         /etc/auto.direct autofs     rw,relatime,fd=7,...
└─/docs/fs-1/share2       //fs-1.ald.company.lan/share2  cifs       rw,
↪nosuid,nodev,...
```

Можно воспользоваться записью множественного монтирования и описать это все одной строкой, используя символ косой черты для переноса строк:

```
/docs/fs-1 \
/share   -fstype=cifs,user,sec=krb5,cruid=$UID,uid=$UID,gid=$UID     ://fs-1.
↪ald.company.lan/share \
/share2  -fstype=cifs,user,sec=krb5,cruid=$UID,uid=$UID,gid=$UID     ://fs-1.
↪ald.company.lan/share2
```

Тогда после монтирования ситуация будет отображаться несколько иначе:

```
admin@pc-1:~$ findmnt
...
└─/docs/fs-1                /etc/auto.direct autofs     rw,relatime,fd=7,...
├─/docs/fs-1/share        /etc/auto.direct autofs     rw,relatime,fd=7,...
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
| └─/docs/fs-1/share       //fs-1.ald.company.lan/share   cifs       rw,
↪nosuid,nodev,...
└─/docs/fs-1/share2        /etc/auto.direct autofs     rw,relatime,fd=7,...
    └─/docs/fs-1/share2      //fs-1.ald.company.lan/share2   cifs       rw,
↪nosuid,nodev,...
```

В отличии от предыдущего способа ресурсы имеют общую точку монтирования `/docs/fs-1`, что позволяет сократить накладные расходы, если требуется подключить большое количество общих папок.

Не смотря на то, что записи множественного монтирования дают некоторые преимущества, составлять их сложнее. При этом интерфейс службы каталогов FreeIPA на это не рассчитан и позволяет задавать свойства подключения только в одну строку.

3.44.2.9. Настройка программной карты на примере карты хостов

Программная карта `/etc/auto.smb` дает возможность просматривать CIFS-ресурсы примерно так же, как это можно настроить с помощью специальной карты -hosts. Если в главной карте определить строку «/cifs /etc/auto.smb», то при просмотре содержимого каталога `/cifs/fs-1.ald.company.lan` вы увидите общие папки с этого файлового сервера. Список общих папок извлекается по протоколу CIFS непосредственно с указанного сервера с помощью утилиты **smbclient**.

```
admin@pc-1:~$ ls -l /cifs/fs-1.ald.company.lan/
итого 0
drwxr-xr-x 2 root root 0 окт 20 15:11 admin
drwxr-xr-x 2 root root 0 окт 20 15:11 homes
drwxr-xr-x 2 root root 0 окт 20 15:11 share
```

Данный скрипт (`/etc/auto.smb`) использует утилиту mount (и её опции) для монтирования SMB-ресурсов. Предполагается, что файлы с ключами находятся в файловой системе клиента в `/etc/creds`, или существует Kerberos-кэш, позволяющий совершить аутентификацию. В противном случае скрипт пробует смонтировать ресурсы анонимно (с помощью опции guest, утилиты mount). Подробнее – в комментариях в самом скрипте. Если клиент находится в Kerberos-среде и необходимо оставить только этот способ аутентификации (чтобы не было попыток монтирования анонимно), нужно закомментировать следующий блок кода, за исключением двух строк:

```
cat /etc/auto.smb
...
#creds=/etc/creds/$key
#
#if [ -f "$creds" ]; then
#    opts="$opts"',uid=$UID,gid=$GID,credentials='"$creds"
#    smbopts="-A $creds"
#else
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
#    get_krb5_cache
#    if [ -n "$cache" ]; then
        opts="$opts"',multiuser,cruid=$UID,sec=krb5i'
        smbopts="-k"
#       export KRB5CCNAME=$cache
#    else
#        opts="$opts"',guest'
#        smbopts="-N"
#    fi
#fi
...
```

3.44.2.10. Использование символов подстановки на примере карты хостов

В картах косвенного монтирования вместо имени ключа можно использовать «*», как символ подстановки, тогда в расположении можно будет использовать символ амперсанд «&» для подстановки имени текущего ключа. В дополнение к этому возможности подстановки можно расширить с помощью переменных, которые можно определять в формате «-Dvariable=value».

Задействуем указанные возможности, чтобы реализовать более простой способ монтирования CIFS-ресурсов сети без использования bash-скрипта. В главной карте нужно определить ключ `/cifs` для включения карты косвенного монтирования `/etc/auto.smb.hosts`:

```
cat /etc/auto.master
...
/cifs   /etc/auto.smb.hosts
...
```

В карте косвенного монтирования `/etc/auto.smb.hosts` нужно задать ключ с использованием символов подстановки на другую карту и определить переменную host в формате карт монтирования sun «-Dvariable=value»:

```
cat /etc/auto.smb.hosts
*        -fstype=autofs,-Dhost=&       file:/etc/auto.smb.shares
```

Во второй карте косвенного монтирования `/etc/auto.smb.shares`, которая будет включаться по цепочке, нужно определить следующий ключ подстановки с использованием ранее определенной переменной host:

```
cat /etc/auto.smb.shares
*          -fstype=cifs,user,sec=krb5,cruid=$UID     ://${host}/&
```

Обратите внимание, что при просмотре содержимого каталога `/cifs/fs-1.ald.company.lan/` в нем не будут отображаться общие папки до тех пор, пока пользователь не обратится к ним по полному имени.

3.44.3. Управление автомонтированием через FreeIPA UI

Управляя рабочими станциями в домене FreeIPA администраторы могут настраивать карты монтирования централизованно. Работает этот механизм следующим образом:

- Утилита automount поддерживает извлечение информации через механизм NSS
- В файле /etc/auto.master по умолчанию присутствует запись +auto.master, которая указывает на то, что в главную карту должно включаться содержимое карты с именем auto.master через механизм NSS.
- В файле /etc/nsswitch.conf в строке «automount: sss» в качестве источника для automount указан модуль sss, который извлекает ее путем обращения к соответствующему ответчику службы SSSD.
- Служба SSSD извлекает из домена карты автоматического монтирования для одной конкретной локации, имя которой указано параметром ipa_automount_location в конфигурационном файле /etc/sssd/sssd.conf секции domain.

В качестве инструмента применения и автоматизации настроек автомонтирования общих ресурсов на конечных клиентских машинах используется утилита ipa-client-automount.

Далее приведены примеры настройки для использования централизованных карт монтирования общих ресурсов через FreeIPA UI.

3.44.3.1. Создание расположения (локации) автомонтирования

Расположение автомонтирования (англ. automount location) – контейнер для хранения карт монтирования. С помощью расположений (локаций) можно создать изолированные пространства имен распределенной файловой системы для разных категорий рабочих станций. Локации автомонтирования используются для того, чтобы определить для групп компьютеров разные настройки автомонтирования, а значит и разные условия доступа к общим ресурсам.

В интерфейсе FreeIPA список существующих локаций размещён в **Сетевые службы** → **Автомонтирование** (Network Services → Automount). По умолчанию в домене средствами FreeIPA создаётся расположение default.

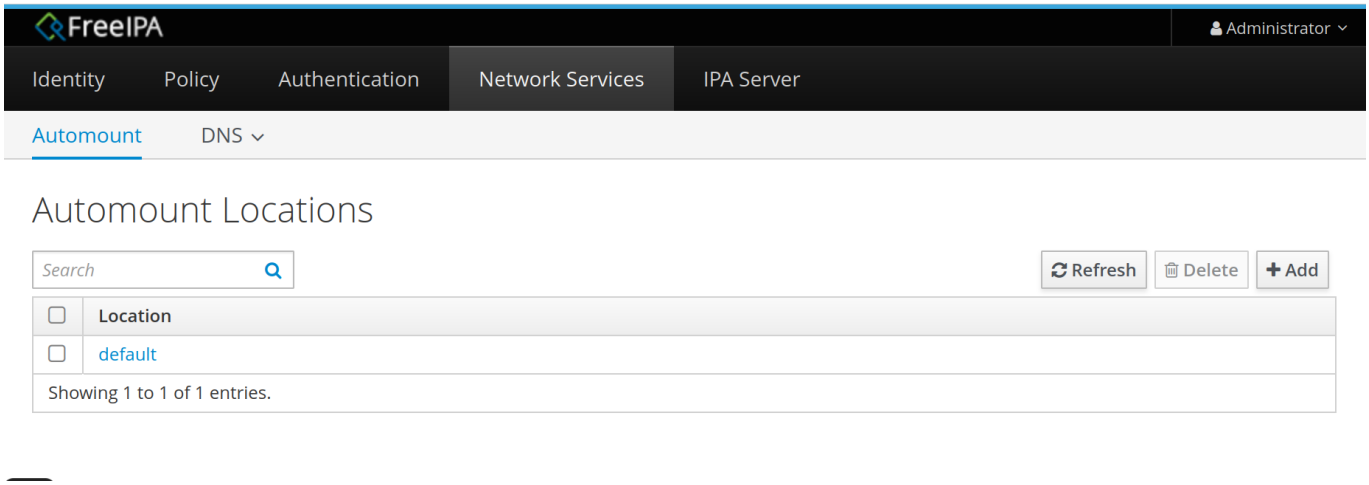


Рисунок 3.134 – Список локаций автомонтирования

Создание новой локации осуществляется по кнопке «Add». Для этого достаточно указать название новой локации.

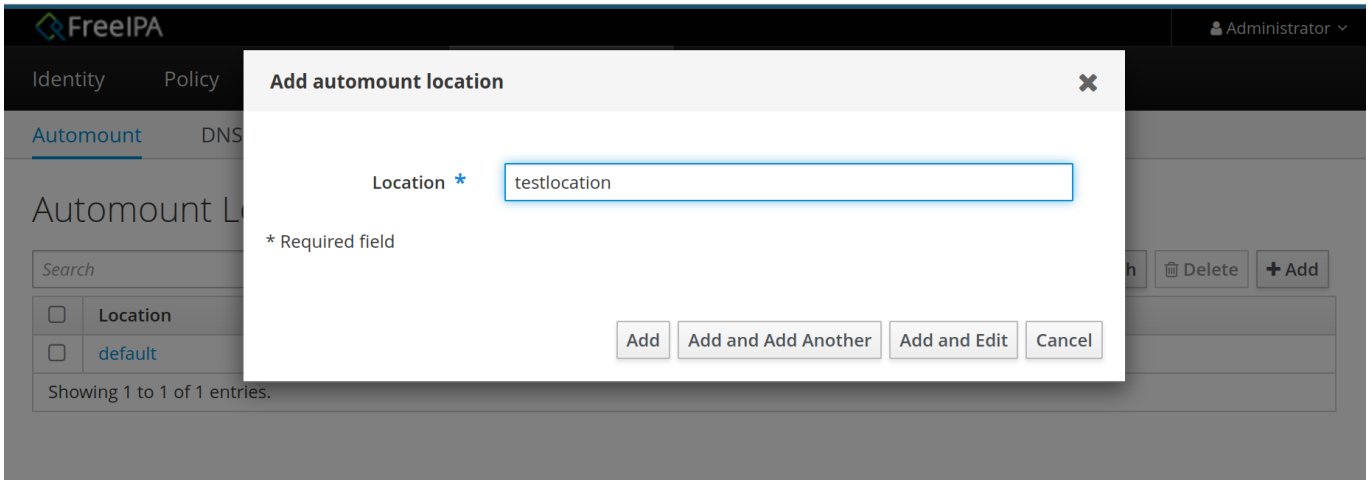


Рисунок 3.135 – Создание локации testlocation

Такой сущности как «расположение автомонтирования» в утилите automount нет, это доработка со стороны FreeIPA и SSSD. Информация о локациях автомонтирования находится в LDAP в разделе `cn=automount,dc=example,dc=com`.

```
admin@dc01:~$ ldapsearch -x -H ldap://localhost -b "cn=automount,
 -D "cn=Directory Manager" -W "(cn=*)"
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <cn=automount> with scope subtree
# filter: (cn=*)
# requesting: ALL
#

# automount,
dn: cn=automount,
objectClass: nsContainer
objectClass: top
cn: automount

# default, automount,
dn: cn=default,cn=automount,
objectClass: nsContainer
objectClass: top
cn: default

# testlocation, automount,
dn: cn=testlocation,cn=automount,
cn: testlocation
objectClass: nscontainer
objectClass: top
```

Рисунок 3.136 – LDAP-записи о локациях

3.44.3.2. Создание и настройка карт монтирования

Внутри расположения, по умолчанию, есть два списка соответствия автомонтирования. Списки соответствия также называют **картами монтирования**. Главным списком (картой) является `auto.master`, ключи этого списка будут включены в главную карту монтирования на рабочей станции пользователя. Имя `auto.master` является предопределенным, т.к. на рабочих станциях пользователей в главной карте `/etc/auto.master` по умолчанию присутствует строка «+auto.master». Если вы удалите эту карту по ошибке, то ее можно создать вручную, главное – сохранить тоже самое имя для этой карты. Подробнее о картах монтирования см. Раздел 3.44.2.4.

По нажатию на одну из локаций в списке **Сетевые службы → Автомонтирование** выводится список карт монтирования, этой локации. Пример, для вновь созданной локации testlocation:

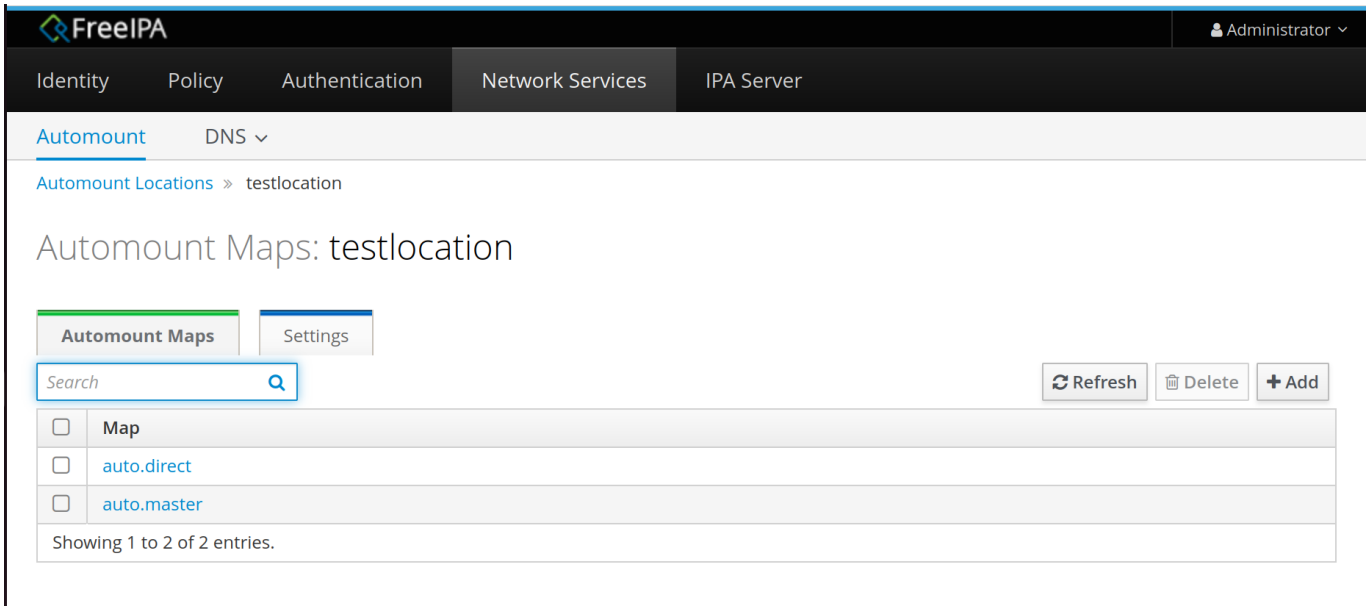


Рисунок 3.137 – Список карт монтирования в локации testlocation

Создание новой карты монтирования осуществляется по кнопке «Add». Карты в интерфейсе FreeIPA могут быть 2 типов – прямые и косвенные (см. Раздел 3.44.2.4). Обратите внимание, что такое деление карт монтирования в некоторой степени условное по следующим причинам: * При добавлении «прямой» карты интерфейс FreeIPA не создаст ключ прямого монтирования «/-» в главной карте auto.master, таким образом карта создаётся в «вакууме» и необходимо будет вручную делать на неё ссылку в той карте которой необходимо (в самом простом варианте – auto.master). То есть с помощью этого интерфейса можно добавить не «прямые карты», а карты, на который не указывают никакие ключи. * При добавлении «непрямой» карты допускается использовать ключ «/-» и указать в качестве родительской карты auto.master (если оставить соответствующее поле пустым), в этом случае будет добавлена карта прямого монтирования.

Поэтому предлагается относиться к этому переключателю `FreeIPA UI` иначе: он позволяет создать карту без ссылок (значение «прямой») или создать карту и сделать запись ключ-значение в родительской карте (иначе – ссылку) на создаваемую карту.

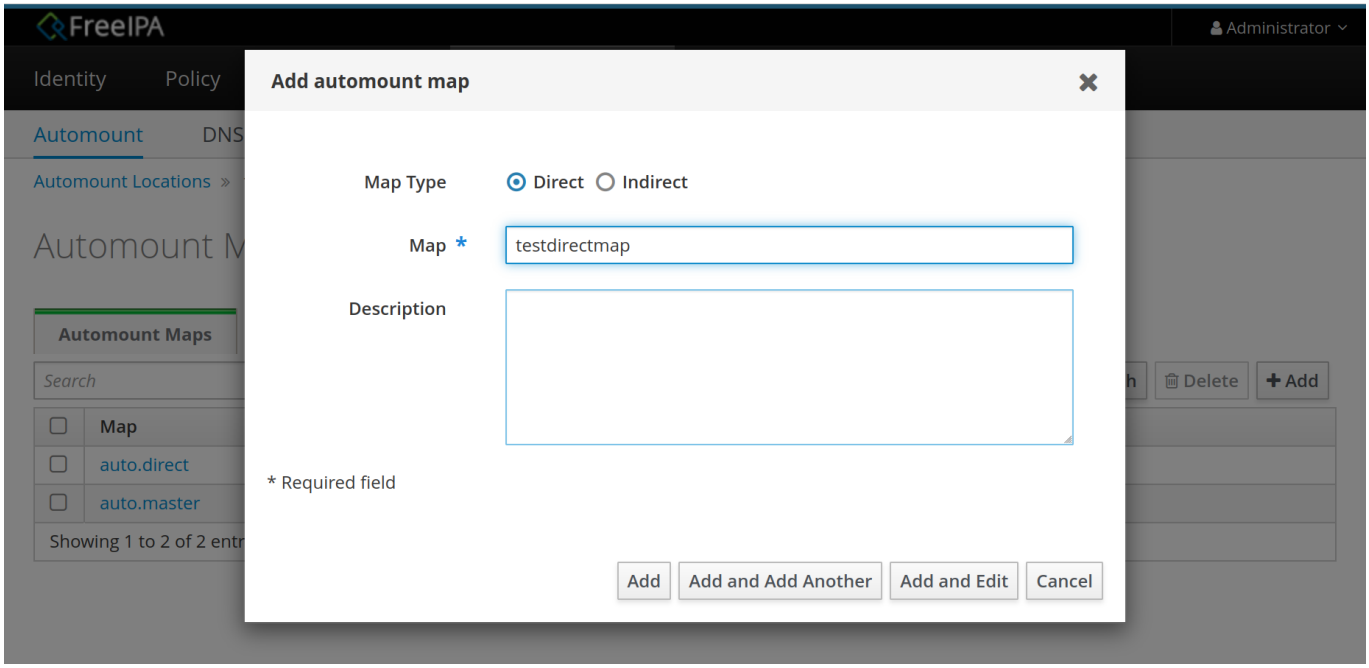


Рисунок 3.138 – Создание прямой карты монтирования testdirectmap

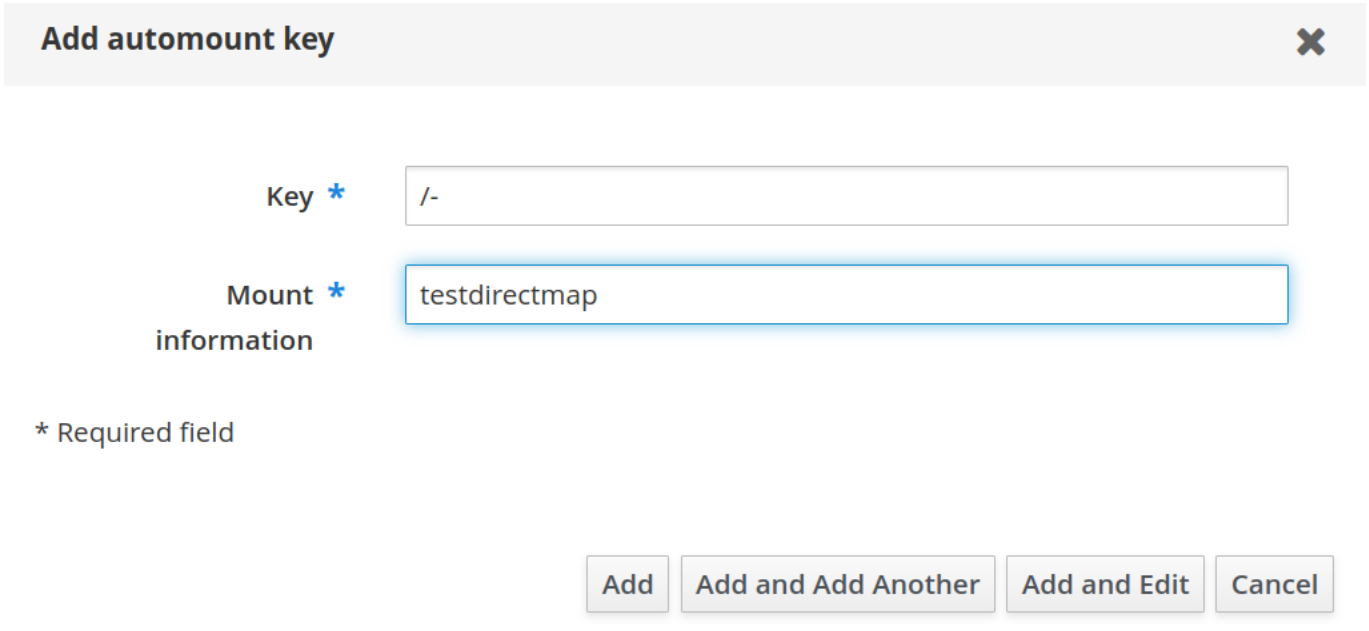


Рисунок 3.139 – Создание прямой карты монтирования testdirectmap, добавление ссылки

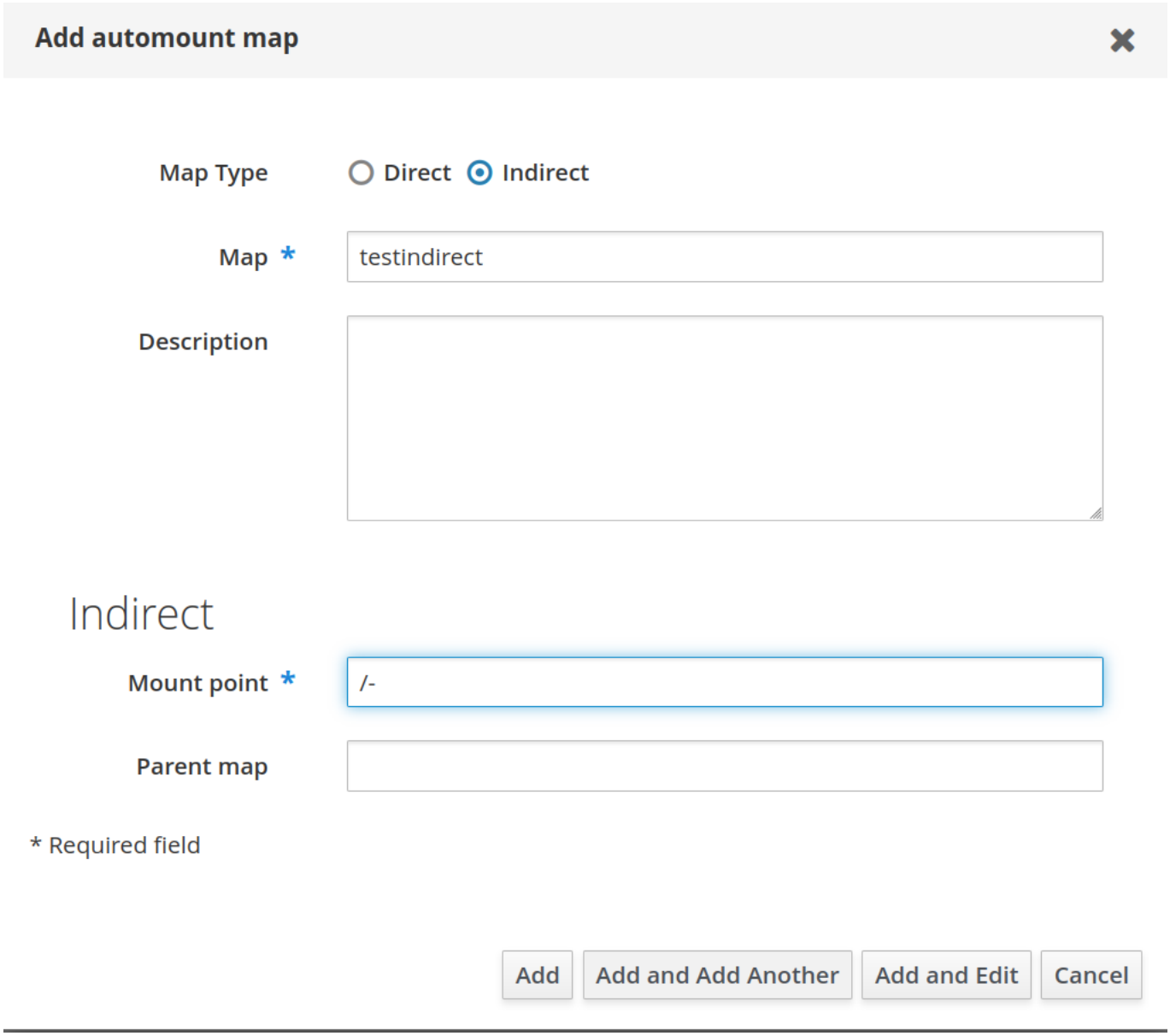


Рисунок 3.140 – Создание непрямой карты монтирования testindirectmap на auto.master

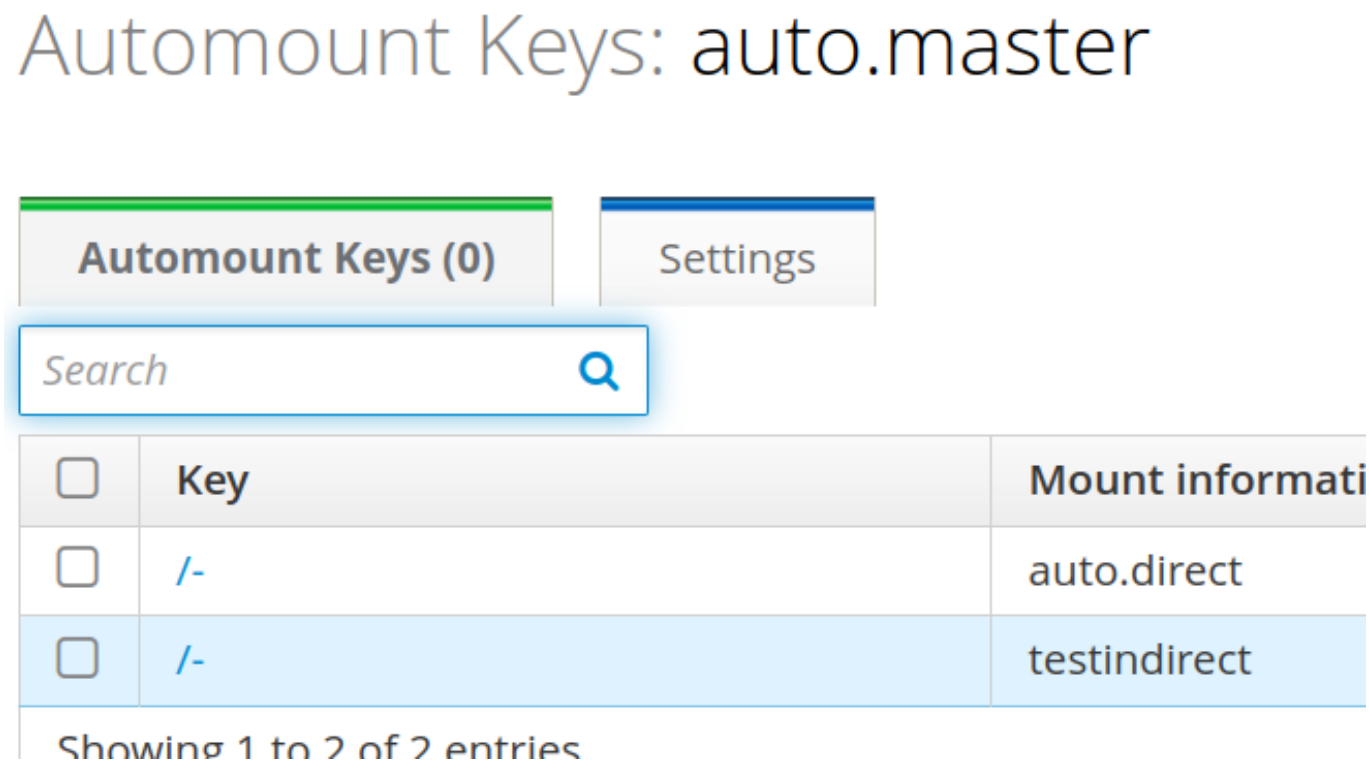


Рисунок 3.141 – Создание непрямой карты монтирования testindirectmap на auto.master

---

Примечание: Создание непрямых карт монтирования через FreeIPA UI множественной вложенности в текущей версии продукта может приводить к ошибкам на уровне службы autofs при попытке найти информацию в LDAP по ссылке `-fstype=autofs ldap:<mapname>`.

Таким образом, рекомендуется в текущей версии продукта пользоваться прямыми картами монтирования, который включаются в auto.master с помощью ссылки `/-`.

3.44.3.3. Создание и настройка точек монтирования

Подключение общих ресурсов с файловых серверов SMB настраивается на этапе создания точек монтирования. При добавлении общей папки, назначается ключ монтирования, как путь к директории на **клиентской** машине (через неё пользователь будет получать доступ к удалённой папке) и настройки (флаги) для запуска утилиты mount (поле mount information). После применения на клиенте утилиты `ipa-client-automount` локации, содержащей карту монтирования с этой точкой монтирования создается **ловушка монтирования**, и при попытке пользователя открыть директорию служба autofs вызывает утилиту mount с флагами, указанными в поле mount information. Подробнее о возможных настройках см. `man autofs`, `man automount`, `man mount`.

Для примера создадим точку монтирования в прямой карте testdirectmap:

- Ключ монтирования – `/test`. Таким образом, при применении автомонтирования удалённая папка будет доступна с клиента по пути `test`.
- Настройки монтирования – `-fstype=cifs,user,sec=krb5i,cruid=$UID,uid=$UID,gid=$UID`

`://smb01.testpool01/myfolder`. Разбор настроек: * Из `-fstype=cifs` будет собрано `mount -t cifs` * Опции `user,sec=krb5i,cruid=$UID,uid=$UID,gid=$UID` проброшено в флаг `mount -o user,sec=krb5i,cruid=$UID,uid=$UID,gid=$UID`. * `://smb01.testpool01/myfolder` – путь к физической директории на файловом сервере, где `smb01.testpool01` это имя файлового сервера в локальной сети, а `/myfolder` – путь к директории.

Предварительно, перед созданием точек монтирования на физические директории стоит настроить сами физические директории через интерфейс ALD Pro (см. Раздел 1.11.6.3).

Примечание: Обратите внимание что путь к директории не абсолютный относительно корня файлового сервера, а относительно настроек samba-сервера, которые прописывают префикс-директорию на файловом сервере, по умолчанию, указаны в `/etc/samba/smb.conf` и `/etc/samba/share.conf`. По умолчанию, общие папки создаются в `/opt/samba_shares`.

Создадим 2 точки монтирования на одну и ту же директорию.

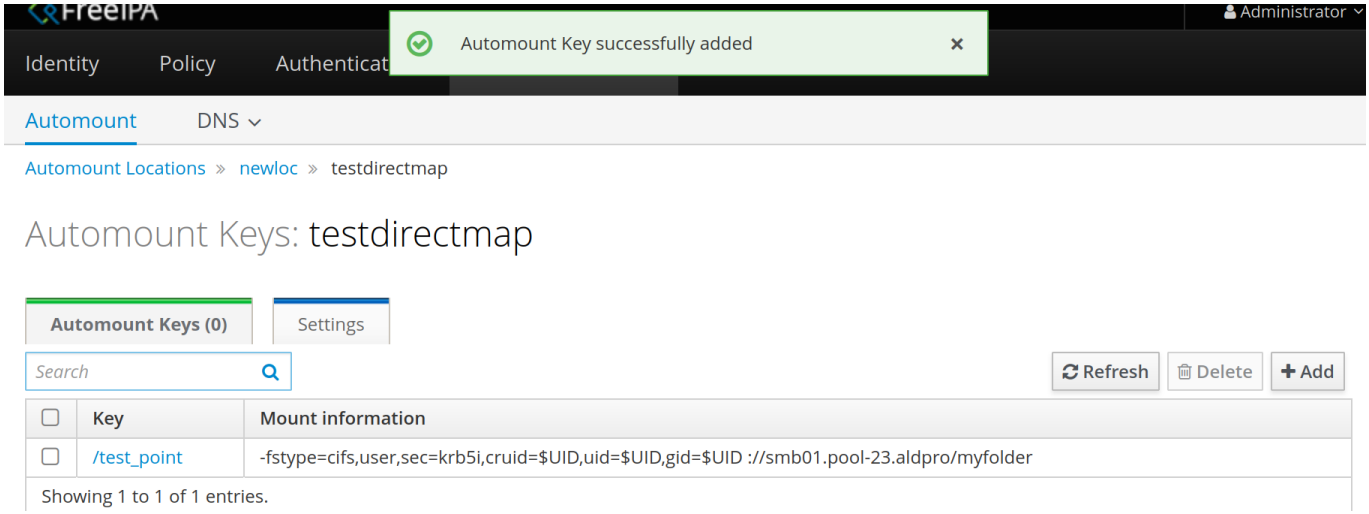


Рисунок 3.142 – Создание точки монтирования в карту testdirectmap в /test

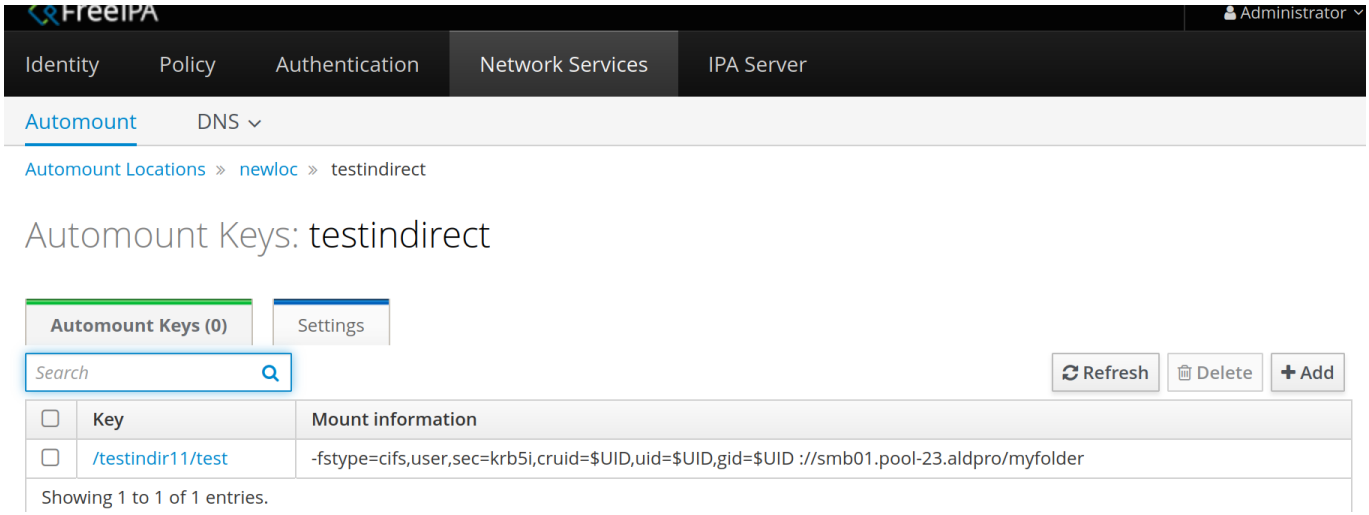


Рисунок 3.143 – Создание точки монтирования в карту testdirectmap в /testindir11/test

Таким образом на клиентской машине должно будет появится 2 новых ловушки монтирования по указанным путям. В директории на файловом сервере лежит файл `file` и папка `test`.

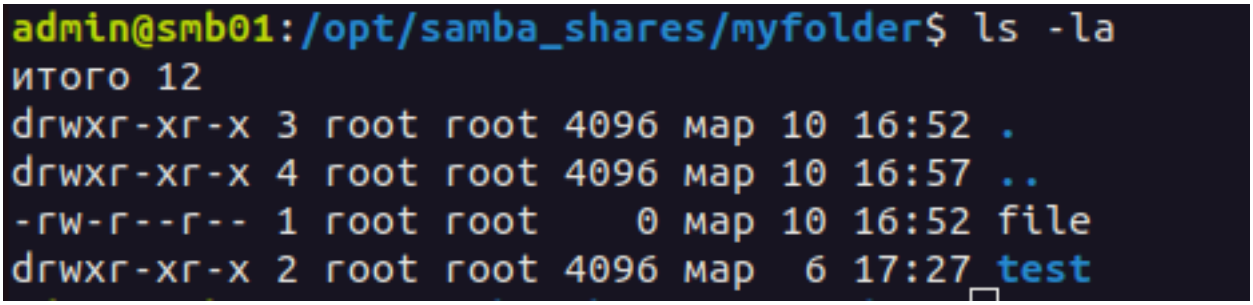


Рисунок 3.144 – Наполнение директории на файловом сервере

3.44.3.4. Применение настроек автомонтирования на клиентской машине

На данном этапе вся информация о картах монтирования, точках и т.п расположена в LDAP и необходимо данные настройки использовать на клиентской машине, для того, чтобы пользователь мог получить доступ к удалённым папкам через точки монтирования. Для этого используется утилита `ipa-client-automount`, которая принимает флаг `--location`. Необходимо использовать локацию, в которой были ранее настроены точки и карты монтирования (по умолчанию это default, в случае данного примера – newloc).

Примечание: Использование утилиты вручную вполне допускается администраторами ALD Pro для точечных решений, однако для масштабных инфраструктур на десятки, сотни и тп. клиентов рекомендуется использовать параметр ГП, о котором пойдёт речь в следующем разделе.

Если рабочая станция была ранее настроена на работу с другой локацией, сначала нужно выполнить удаление настроек, а затем выполнить присоединение к требуемой локации:

```
root@client01:/# ipa-client-automount --uninstall
Restoring configuration
root@client01:/# ipa-client-automount --location newloc
Searching for IPA server...
IPA server: DNS discovery
Location: newloc
Continue to configure the system with these values? [no]: yew
Configured /etc/default/nfs-common
Configured /etc/idmapd.conf
Restarting sssd, waiting for it to become available.
Started autofs
```

Служба autofs будет автоматически перезапущена, поэтому на каталоги будут установлены ловушки монтирования:

```
root@client01:/# findmnt
TARGET                          SOURCE         FSTYPE     OPTIONS
...
├─/testindir11/test             testindirect   autofs     rw,relatime,fd=6,
 ↪pgrp=5999,timeout=300,minproto=5,maxproto=5,direct,pipe_ino=73026
├─/test_point                   testdirectmap autofs     rw,relatime,fd=6,
 ↪pgrp=5999,timeout=300,minproto=5,maxproto=5,direct,pipe_ino=73026
```

Теперь при попытке получить доступ к содержимому директории `/test_point` произойдёт запуск утилиты `mount` (о чём будет запись в `/var/log/syslog`). В качестве credentials будут использованы UID и TGT-билет того пользователя, под которым залогинился пользователь. Например пользователь `root` с `$UID = 0` не получит доступ к содержимому директории, поскольку на него не выписан kerberos-билет, а также на smb файловом сервере его нет в списке допущенных к содержимому папки:

```
root@client01:/# cd test_point/
bash: cd: test_point/: Нет такого файла или каталога
```



Рисунок 3.145 – Настройки доступов папки на файловом сервере

В списке допущенных есть только пользователь admin, который действительно может получить доступ к папке согласно настройкам доступов папки, заданным ранее в ALD Pro.

```
admin@client01:/$ cd test_point/
admin@client01:/test_point$ ls -la
итого 4
drwxr-xr-x  2 admin admins    0 июл  1 09:24 .
drwxr-xr-x 27 root  root   4096 июл  1 09:23 ..
-rwxr-xr-x  1 admin admins    0 июл  1 09:23 file
drwxr-xr-x  2 admin admins    0 июл  1 09:24 test
```

3.44.3.5. Параметр групповой политики «Служба автомонтирования»

С версии 3.0 ALD Pro в официальной комплектации продукта появляется параметр компьютера «Служба автомонтирования» для групповых политик. Параметр позволяет настроить автомонтирование общих samba-папок на клиентской рабочей станции

AstraLinux. Базовая задача параметра – запустить `ipa-client-automount --location <LOC>`.

Основные сценарии использования параметра – применение и сброс локации автомонтирования для подразделений, содержащих компьютеры. При применении локации на каждый компьютер подразделения применяются применены ловушки монтирования, ведущие к директориям на файловых серверах. Доступ к содержимому папок осуществляется исходя из разрешений, выданных shared-директориям на пользователей или группы пользователей. Все пользователи видят ловушки монтирования на клиентской машине, но доступ пользователя к каждой папке, скрывающейся за ловушкой, проверяется отдельно.

Локация хранится в конфигурационном файле настроек sssd (`/etc/sssd/sssd.conf`) в ключе `ipa_automount_location`. Для проверки корректности настройки автомонтирования в терминале можно воспользовать командой `findmnt -t autofs`, которая отображает все точки монтирования в системе. В списке содержатся также находятся и ловушки монтирования, которые настроены в картах монтирования выбранной ранее локации.

Тип параметра – простой.

Поле «Локация» содержит название локации автомонтирования. Название локации задаётся при её создании одим из следующих способов:

- Портала управления FreeIPA (Сетевые службы → Автомонтирование → Расположение автомонтирования). Подробнее о том, как использовать FreeIPA для настройки автомонтирования см. Раздел 3.44.3.
- С помощью утилиты ipa. Подробнее об этом способе можно узнать, введя в терминале запущенного контроллера домена команду `ipa help automount`.

Поле «Разрешено использование» включает работу с указанной локацией. Допускается установка в поле одного из следующих значений:

- `true` - Включить автомонтирование и применить локацию (по умолчанию).
- `false` - Выключить автомотирование и отключить локацию.

Отключение параметра (перевод атрибута «Состояние» в состояние «Выключено») не приведет к отключению автомонтирования в системе. Для фактического выключения локации необходимо оставить параметр активным, при этом для локации установить атрибут «Разрешено использование» в значение «false» (systemd-процесс autofs отключен).

Важно обратить внимание, что при удалении локации, которая используется в объекте групповой политики, содержащем параметр «Служба автомонтирования», через портал управления ALD Pro или 389ds, локации, ловушки и все прочие настройки автомонтирования на компьютерах подразделения сброшены не будут.

Применение данного параметра групповой политики подчиняется стандартным механизмам групповых политик (см. руководство администратора). Для конфигурации созданной ранее (см. Раздел 3.44.3.4) создаётся групповая политика с параметром «Служба Автомонтирования» и соответствующими аргументами.

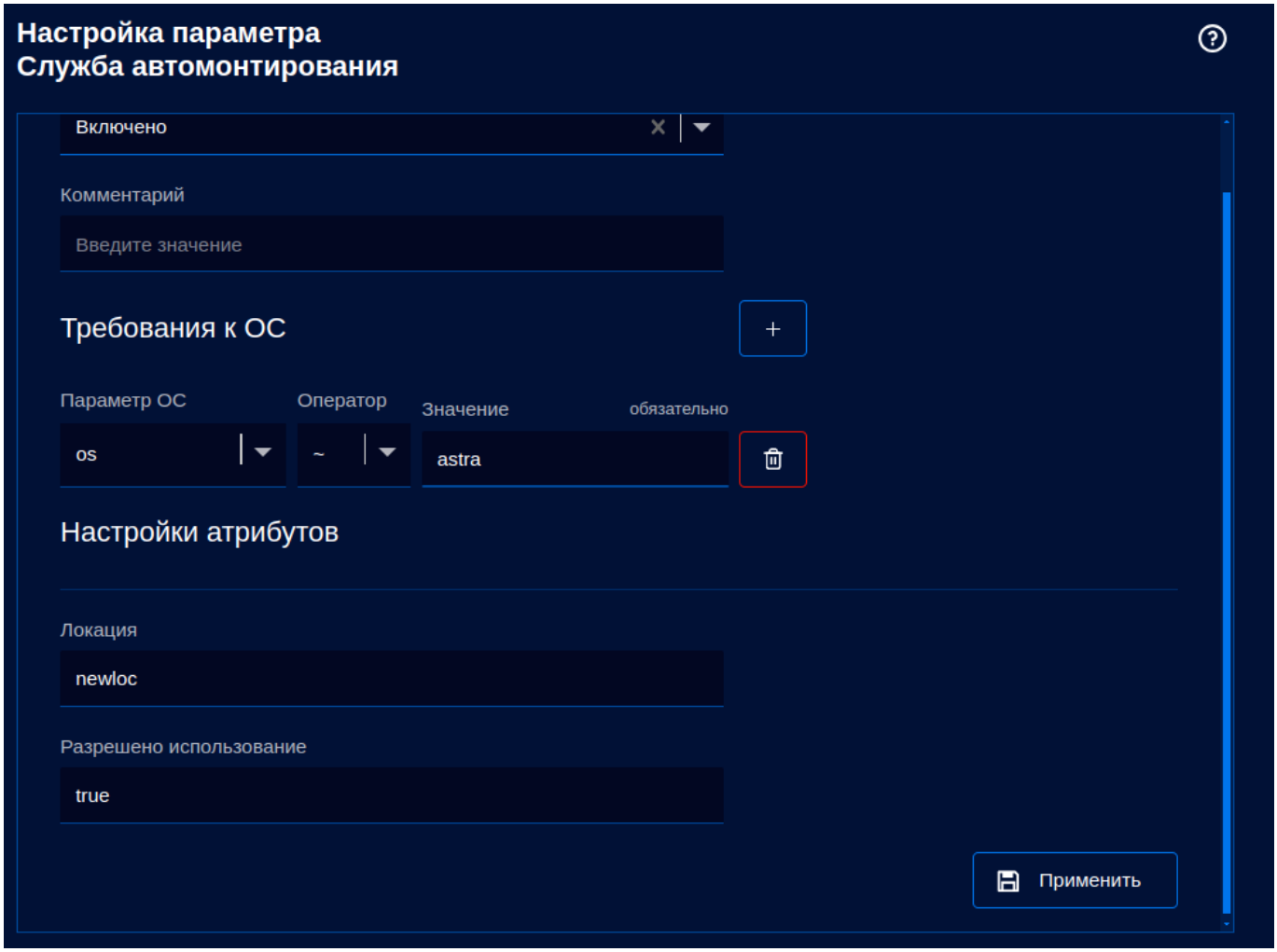


Рисунок 3.146 – Настройки параметра ГП

По нажатию на кнопку «Применить» групповая политика сохраняется и на связанных с подразделением клиентах она будет применена по таймеру. Можно воспользоваться форсированным применением групповых политик на конкретной машине с помощью команды `aldpro-gpupdate --gp`. В результате на клиенте будет применена та локация, которая была указана на портале управления в параметре «Локация»:

```
root@client01:/home/admin# findmnt -t autofs
TARGET                     SOURCE      FSTYPE OPTIONS
/proc/sys/fs/binfmt_misc systemd-1   autofs rw,relatime,fd=30,pgrp=1,
↪timeout=0,minproto=5,maxproto=5,direct,pipe_ino=1387
/myfolderkey               auto.direct autofs rw,relatime,fd=6,pgrp=213686,
↪timeout=300,minproto=5,maxproto=5,direct,pipe_ino=816641
/myffffff                  auto.direct autofs rw,relatime,fd=6,pgrp=213686,
↪timeout=300,minproto=5,maxproto=5,direct,pipe_ino=816641
root@client01:/home/admin# aldpro-gpupdate --gp
Форсированное применение групповых политик
...
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
root@client01:/home/admin# findmnt -t autofs
TARGET                   SOURCE        FSTYPE OPTIONS
/proc/sys/fs/binfmt_misc systemd-1     autofs rw,relatime,fd=30,pgrp=1,
 ↪timeout=0,minproto=5,maxproto=5,direct,pipe_ino=1387
/testindir11/test        testindirect  autofs rw,relatime,fd=6,pgrp=213936,
 ↪timeout=300,minproto=5,maxproto=5,direct,pipe_ino=819129
/test_point              testdirectmap autofs rw,relatime,fd=6,pgrp=213936,
 ↪timeout=300,minproto=5,maxproto=5,direct,pipe_ino=819129
```

Известные проблемы

4.1. Исправление односторонних отношений Left-Right

Перед созданием соглашения о репликации в LDAP-каталоге сначала создается такая сущность, как сегмент. Как только **Topology** плагин контроллера видит относящийся к нему сегмент, для которого не создано соглашение, он создает такое соглашение. Сначала создается соглашение в одном направлении, затем в обратном, и при наличии двух взаимонаправленных сегментов они удаляются и создается третий сегмент, у которого направление **Both**.

Если в домене наблюдается однонаправленное соглашение о репликации, т.е. стрелочка только в одну сторону, и не становится двунаправленной, это означает, что второй сегмент не был создан и для устранения проблемы его нужно создать вручную.

Найти однонаправленные **Left-Right** сегменты и записать их в файл.

```
sudo i
set +o history
ldapsearch -Q -xLLL -D "cn=directory manager" -w "AstraLinux_176" -b
 ↪"cn=domain,cn=topology,cn=ipa,cn=etc,dc=ald,dc=company,dc=lan"
 ↪"(ipaReplTopoSegmentDirection=left-right)" > direction.ldif
set -o history
exit
```

Создать **python** скрипт *parcing_topology.py* командой, а также этот файл можно скачать в личном кабинете:

```
nano parcing_topology.py
```

Сохранить файл с таким содержимым:

```
with open('direction.ldif') as f:
    lines = f.readlines()
ldif_change=""
text_block=""
for line in lines:
    text_block=f"{text_block}{line}"
    if "ipaReplTopoSegmentLeftNode" in line:
        left_node=line.split(":")[1].strip()
    if "ipaReplTopoSegmentRightNode" in line:
        right_node=line.split(":")[1].strip()
    if not line.strip():
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
        text_block=text_block.replace(f"{left_node}-to-{right_node}",f"{right_
↪node}-to-{left_node}")
        text_block=text_block.replace(f"ipaReplTopoSegmentLeftNode: {left_
↪node}",f"ipaReplTopoSegmentLeftNode: {right_node}")
        text_block=text_block.replace(f"ipaReplTopoSegmentRightNode: {right_
↪node}",f"ipaReplTopoSegmentRightNode: {left_node}")
        ldif_change+=f"{text_block}"
        text_block=""
with open('add_direction.ldif','w') as f:
    f.write(ldif_change)
```

Запустить следующий скрипт в той же папке и убедиться, что скрипт отработал корректно.

```
python3 parcing_topology.py
```

Теперь внести изменения из LDIF-файла в каталог от пользователя **admin**:

```
ldapadd -f add_direction.ldif
```

Проверить, что в системе не осталось **Left-Right** сегментов.

```
sudo i
set +o history
ldapsearch -xLLL -D "cn=Directory Manager" -w "AstraLinux_176" -b "cn=domain,
↪cn=topology,cn=ipa,cn=etc,dc=ald,dc=company,dc=lan"
↪"(ipaReplTopoSegmentDirection=left-right)"
set -o history
exit
```

Перезагрузить сервис **ipa** или последовательно все серверы, где были проблемы с односторонними соглашениями, для того, чтобы плагин **Topology** создал недостающие соглашения.

```
sudo ipactl restart
```

Соглашение создается, но не всегда запускается репликация после рестарта реплик. Как решение можно использовать команду:

```
ipa-replica-manage force-sync --from
```

4.2. Вход в систему занимает слишком много времени

Если время выполнения команды `id $USER` занимает слишком много времени, то в первую очередь необходимо выполнить команду `id -G $USER`. Если команда отработает мгновенно, то требуется добавить следующие значения в */etc/sssd/sssd.conf* в секцию

`[domain/ald.company.lan]`:

```
[domain/ald.company.lan]
...
ignore_group_members = true
subdomain_inherit = ignore_group_members
...
```

Для применения настроек нужно перезапустить службу **sssd**:

```
sudo systemctl restart sssd
```

Обычно наиболее трудоемкой операцией является загрузка групп, включая их участников. На начальном этапе важно знать, членом каких групп является пользователь (`id aduser@ad_domain`), а не какие участники входят в конкретные группы (`getent group adgroup@ad_domain`). При установке, для параметра `ignore_group_members`, значения **True** - все группы отображаются как пустые. Таким образом загружается только информация о самих объектах группы, а не об их членах, что обеспечивает значительное повышение производительности LDAP запросов. Важно обратить внимание, что идентификатор `aduser@ad_domain` все равно вернет все правильные группы.

Параметр `ignore_group_members` может быть указан в разделе домена в *sssd.conf* как явно, так и одним из значений параметра `subdomain_inherit`. В этом случае данный параметр применится и к родительскому домену ALD Pro, и к доверенным поддоменам MS AD.

4.3. Решение проблемы с запросами на получение билетов kerberos

При попытке получить билет **Kerberos** с реплик, все запросы уходят на первый контроллер домена вместо того КД, с которого делается запрос. Данное поведение может привести к невозможности работы портала при выходе из строя первого контроллера домена.

Для решения проблемы необходимо удалить или сделать неработающую ссылку для `winbind_krb5_locator.so`

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

Затем выполнить команду `ipactl restart`.

Внимание: Данное поведение не актуально для ОС **Astra Linux** версии **1.7.6 UU2** и выше.

4.4. Команды getent passwd и getent group не отображают пользователей и групп

Функция **Enumeration** отключена. Для получения дополнительной информации обратитесь в службу технической поддержки.

4.5. Изменений на сервере довольно долго не видно на клиенте

Служба **SSSD** кэширует идентификационную информацию в течение некоторого времени. Можно принудительно обновить кэш при следующем поиске с помощью команды `sss_cache -E`, предварительно установив пакет с нужной утилитой:

```
sudo apt install sssd-tools
```

Важно обратить внимание, что при входе в систему обновленная информация всегда перечитывается с сервера.

4.6. Как включить аутентификацию LDAP через незащищенное соединение

Это запрещено по соображениям безопасности, служба **SSSD** требует использовать **TLS** или **LDAPS** для аутентификации по **LDAP**.

4.7. В журналах нет ни одного сообщения от pam_sss

Скорее всего, стек **PAM** настроен неправильно. Нужно убедиться, что используется аутентификация, которая поддерживает **PAM**, поскольку некоторые методы аутентификации, такие как открытые ключи **SSH**, обрабатываются непосредственно в **SSHD** и вообще не используют стек **PAM**.

4.8. Я могу переключиться на доменного пользователя командой su из-под root, но не под обычным пользователем, SSH тоже не работает

Если есть сложность с переключением на другого пользователя командой `su` из-под **root**, это обычно означает, что полностью обходится аутентификация **SSSD**, используя модуль `pam_rootok.so`. Вероятно, неверно настроена служба **SSSD**. Необходимо войти в систему как локальный пользователь и продолжить отладку под этим профилем.

4.9. Я получаю сообщение Access denied for user $user: 6 (Permission denied)

Аутентификация прошла успешно, но пользователю было отказано в доступе к клиентской машине. Можно временно отключить управление доступом, задав `access_provider=permit`, но важно вернуть значение по умолчанию после выяснения основной причины.

Если отключение контроля доступа не помогает, возможно, учетная запись заблокирована на стороне сервера. Нужно проверить журналы домена **SSSD**, чтобы получить дополнительную информацию.

4.10. Исправление ошибки глобального каталога

При выполнении команды `ipactl start` и `ipactl restart` может возникать ошибка:

```
ipactl start
Existing service file detected!
Assuming stale, cleaning and proceeding
Starting Directory Service
Starting krb5kdc Service
Starting kadmin Service
Starting named Service
Starting httpd Service
Starting ipa-custodia Service
Starting smb Service
Starting winbind Service
Starting ipa-otpd Service
Starting ipa-dnskeysyncd Service
```

(продолжение на следующей странице)

(продолжение с предыдущей страницы)

```
Starting globalcatalog Service
Failed to start globalcatalog Service
Shutting down
```

Для исправления ошибки необходимо запустить сервисы **ipa** и обновить глобальный каталог на контроллерах домена, отвечая на все вопросы **yes**:

```
ipactl start --ignore-service-failure
aldpro-gc-install
```

Перезапустить сервисы **ipa** на контроллерах домена:

```
ipactl restart
```

4.11. При обновлении контроллера домена возникает ошибка «Error updating rbtaSubsystemLog»

Если при обновлении контроллера домена обнаружена ошибка вида:

```
[INFO ] EVENT: Error updating rbtaSubsystemLog: {'desc': 'Insufficient access
↪', 'info': "Insufficient 'write' privilege to the 'rbtasubsystemlog'
↪attribute of entry 'fqdn=dc02.corp.lan,cn=computers,cn=accounts,dc=corp,
↪dc=lan'.\n"}
```

необходимо проверить регистр атрибутов `rbtaSubsystem` на контроллере домена, у которого произошел сбой обновления, командой `ldapsearch`.

Пример:

```
ldapsearch -b cn=computers,cn=accounts,dc=corp,dc=lan 'fqdn=dc02.corp.lan' |
↪grep -i rbtasub
```

где `dc02.corp.lan` - **FQDN** необновленного контроллера домена.

В результате выполнения команды выводятся все атрибуты `rbtaSubsystem`, которые должны содержать буквы верхнего регистра, например:

```
rbtaSubsystemConfig: {"is_master": false, "setup_gc": false, "setup_pkiproxy
↪": true, "setup_syncer": false}
rbtaSubsystemRole: dc
rbtaSubsystemSite:: 0JPQvtC70L7QstC90L7QuSDQvtGE0LjRgQ==
```

Если в результате выполнения команды все атрибуты `rbtaSubsystem` содержат буквы только нижнего регистра, например:

```
rbtasubsystemConfig: {"is_master": false, "setup_gc": false, "setup_pkiproxy
↪": true, "setup_syncer": false}
rbtasubsystemRole: dc
rbtasubsystemSite:: 0JPQvtC70L7QstC90L7QuSDQvtGE0LjRgQ==
```

необходимо выполнить на необновленном контроллере домена переинициализацию:

```
sudo ipa-replica-manage re-initialize --from=dc01.corp.lan
```

где `dc01.corp.lan` - **FQDN** первого контроллера домена.

После переинициализации необходимо убедиться, что все атрибуты `rbtaSubsystem` содержат буквы верхнего регистра, повторив команду `ldapsearch`.

Пример:

```
ldapsearch -b cn=computers,cn=accounts,dc=corp,dc=lan 'fqdn=dc02.corp.lan' |
↪grep -i rbtasub
```

При необходимости выполнить переинициализацию повторно.

Корректный вывод после переинициализации выглядит, например, так:

```
rbtaSubsystemConfig: {"is_master": false, "setup_gc": false, "setup_pkiproxy
↪": true, "setup_syncer": false}
rbtaSubsystemRole: dc r
btaSubsystemSite:: 0JPQvtC70L7QstC90L7QuSDQvtGE0LjRgQ==
```

После корректного завершения переинициализации необходимо выполнить перезапуск служб IPA и повторный запуск обновления командами:

```
sudo ipactl restart
sudo aldpro-gpupdate --pm
sudo aldpro-gpupdate --gp
sudo aldpro-roles --iud --action update
```

4.12. При настройке доверительных отношений появляется ошибка «saf_fetch: failed to find server for «WINAD» domain»

В ситуациях, когда:

- контроллеры домена **MS AD** и **ALD Pro** находятся в разных подсетях;
- в сетевых настройках контроллера **MS AD** установлен параметр `Disable NetBIOS over TCP/IP`;

- на контроллере домена **MS AD** в реестре HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters имеется ключ AllowNBToInternet со значением 0:

```
Value Name: AllowNBToInternet
Type: Dword
Value: 0
Default value of the flag: 0
```

после настройки доверительных отношений между доменами **ALD Pro** и **MS AD** служба winbind может существенно замедлить или приостановить свою работу (зависнуть).

В результате на контроллере домена **ALD Pro** появятся циклические сообщения в лог-файле /var/log/samba/log.wb-WINAD вида:

```
[2024/11/13 16:16:54.570356,  5, pid=9866] ../../source3/libsmb/namequery.
↪c:275(saf_fetch)
saf_fetch: failed to find server for "WINAD" domain
[2024/11/13 16:16:54.822034,  5, pid=9866] ../../source3/libsmb/namequery.
↪c:275(saf_fetch)
saf_fetch: failed to find server for "winad.company.lan" domain
```

где:

- WINAD - NetBIOS контроллера домена **MS AD**;
- winad.company.lan - домен **MS AD**, с которым построены доверительные отношения.

Для исправления данной ошибки необходимо:

1. Убедиться, что ОС **Astra Linux** на контроллерах домена **ALD Pro** обновлена до версии 1.7.6.UU2 или выше.

2. Установить параметр disable netbios = yes для **Samba**, выполнив команду:

```
sudo samba-regedit
```

Используя стрелки (UP, DOWN, LEFT, RIGHT), необходимо перейти в /HKEY_LOCAL_MACHINE/SOFTWARE/Samba/smbconf/global и нажать клавишу Tab, переместившись в окно Value. Далее нажать клавишу n и создать параметр со следующими значениями:

```
Name: disable netbios
Type: REG_SZ
Data: yes
```

Для выхода нажать клавишу q и перезапустить службу IPA, используя команду:

```
sudo ipactl restart
```

Данные действия необходимо повторить на всех контроллерах домена **ALD Pro**.

4.13. Медленное монтирование сетевых ресурсов пользователями доверенных доменов

Если подключение к сетевому ресурсу в рамках подсистемы «Общий доступ к файлам» из состава **ALD Pro** с доменного компьютера **MS AD** под УЗ **MS AD** занимает слишком много времени, то необходимо обратить внимание на внешние группы (external groups) со стороны **ALD Pro**. При использовании внешних групп рекомендуется провести индексацию атрибута `ipaExternalMember` на всех контроллерах домена **ALD Pro**.

Для этого необходимо:

1. остановить экземпляр (instance) LDAP командой:

```
dsctl slapd-INSTANCE-NAME stop
```

2. выполнить блок команд для индексации атрибута `ipaExternalMember`:

```
sudo dsconf INSTANCE-NAME backend index add --index-type eq --attr
↪ipaExternalMember userRoot
sudo dsctl INSTANCE-NAME stop
sudo dsctl slapd-INSTANCE-NAME db2index userRoot
sudo dsctl INSTANCE-NAME start
```

где `INSTANCE-NAME` - имя контроллера домена **ALD Pro**, который можно посмотреть в `/etc/dirsrv/slapd-INSTANCE-NAME` или через команду:

```
sudo dsctl -l
```

На всех контроллерах домена, в т.ч. - на новых, необходимо выполнить индексацию один раз.

4.14. Некорректное отображение ошибки «Значение максимального уровня должно быть не меньше значения минимального уровня»

При установке пользователю максимального уровня конфиденциальности больше минимального может возникать ошибка «Значение максимального уровня должно быть не меньше значения минимального уровня», даже если максимальное значение действительно больше минимального.

Данная ошибка возникает из-за особенности валидации в FreeIPA — при сравнении уровней конфиденциальности производится сравнение чисел как строк, а не как целых чисел, что приводит к некорректному результату сравнения.

Проблема затрагивает определенные комбинации значений уровней.

ALD Pro корректно работает с созданными по умолчанию в системе мандатного контроля доступа ОС Astra Linux 4 уровнями конфиденциальности: Уровень_0, Уровень_1,

Уровень_2, Уровень_3, а при добавлении дополнительных уровней может возникать описанная выше ошибка.

4.15. Ограничение проверки на удаление уровней конфиденциальности

При удалении уровней конфиденциальности через API службы каталога FreeIPA или ALD Pro выполняется дополнительная проверка на то, что удаляемый уровень не используется в домене. Например, если в домене создано четыре уровня конфиденциальности от 0 до 3, то вы сможете удалить третий уровень только в том случае, если он не назначен ни одному из пользователей или учтенных устройств. Вместе с тем, вы не должны полагаться на указанную проверку, т.к. она учитывает параметры только первых двух тысяч пользователей домена или учтенных устройств. Если третий уровень конфиденциальности будет назначен 2001-му пользователю или учтенному устройству, то система не будет запрещать удаление этого уровня.

4.16. Устранение проблем с авторизацией после обновления до версии 3.0.0

После обновления **ALD Pro** до версии 3.0.0 у клиентов могут возникнуть проблемы с авторизацией: невозможность входа в систему, отсутствие отклика формы входа или ошибка 401 Unauthorized.

Важно: Перед обновлением необходимо создать резервную копию текущих настроек `Apache`:

```
cp /etc/apache2/conf-aldpro/aldpro-mp.conf /etc/apache2/conf-aldpro/aldpro-mp.
↪conf_default
```

В случае недоступности авторизации после обновления:

1. Временно отключить новый механизм авторизации:

   - Отредактировать файл `/etc/aldpro/core.env`, добавив параметр `IS_GSSAPI_AUTH_METHOD=0`

2. Восстановить предыдущую версию конфигурации `Apache`:

   - из резервной копии:

```
sudo cp /etc/apache2/conf-aldpro/aldpro-mp.conf_default /etc/apache2/conf-
↪aldpro/aldpro-mp.conf ;
```

   - или вручную, заменив содержимое файла `/etc/apache2/conf-aldpro/aldpro-mp.conf` на следующую конфигурацию:

```
# строки конфигурации Apache до блока <Location "/ad">

<Location "/ad">
WSGIProcessGroup rbta-ad
WSGIApplicationGroup rbta-ad
<If "%{REQUEST_URI} =~ m#^.*/login/kerberos.*$#">
    AuthType GSSAPI
    AuthName "Kerberos Login"
    GssapiSessionKey file:/etc/apache2/ipasession.key
    GssapiSessionKey key:{ключ динамический — используйте значение из
 ↪дефолтной конфигурации}
    GssapiImpersonate On
    GssapiUseSessions On
    GssapiDelegCcacheDir /run/ipa/ccaches
    GssapiDelegCcachePerms mode:0660 gid:ipaapi
    GssapiUseS4U2Proxy on
    GssapiAllowedMech krb5
    GssapiDelegCcacheUnique On
    Require valid-user
</If>
<Else>
    Satisfy Any
    Require all granted
</Else>
</Location>
```

3. Перезапустить службу Apache:

```
sudo systemctl restart apache2
```

4.16.1. Ошибки и порядок их решения в процессе обновления Системы

Ошибка 1. Во время обновления реплики при выполнении стейта `aldpro_subsystems.send_log_to_ldap` произошла ошибка.

Необходимо проверить:

1. В **LDAP**-записи компьютера (`fqdn=<имя_реплики>,cn=computers,cn=accounts,<доменный_суффикс>`), на котором проводится обновление, все атрибуты, начинающиеся на `rbtaSubsystem`, имеют правильные имена (с заглавными буквами, например, `rbtaSubsystemLog`, а не `rbtasubsystemlog`):

```
ldapsearch -Q -LLL -b fqdn=<имя_КД>,cn=computers,cn=accounts,<доменный_
↪суффикс> -o ldif-wrap=no | grep -i rbtasubsystem
```

2. в **LDAP**-записи компьютера (`fqdn=<имя_реплики>,cn=computers,cn=accounts,<доменный_суффикс>`), на котором проводится обновление, имеются четыре `aci`

```
ldapsearch -Q -LLL -b fqdn=<имя_КД>,cn=computers,cn=accounts,<доменный_
↪суффикс> -o ldif-wrap=no aci``
```

Решение: если на первом КД валидные данные, то можно переинициализировать обновляемую реплику, взяв в качестве источника первый КД. Альтернативно изменять имена атрибутов и добавлять `aci` непосредственно в **LDAP**.

Ошибка 2. Во время выполнения стейта `aldpro_subsystems.get_crt_to_fs` происходит повторяющаяся (через каждые 5 минут) попытка получить сертификат (`State result does not match retry until value, state will be re-run in 300 seconds`). Необходимо убедиться, что сертификат сгенерирован на первом КД (значение атрибута `rbta-crt` в записи обновляемой реплики):

```
ldapsearch -Q -LLL -h <имя_первого_КД> -b fqdn=<имя__обновляемого_КД>,
↪cn=computers,cn=accounts,<доменный_суффикс> -o ldif-wrap=no rbta-crt
```

и реплицирован на обновляемый КД:

```
ldapsearch -Q -LLL -h <имя_обновляемого_КД> -b fqdn=<имя__обновляемого_КД>,
↪cn=computers,cn=accounts,<доменный_суффикс> -o ldif-wrap=no rbta-crt
```

Решение: поверить работу и скорость репликации данных **LDAP**

4.17. Решение проблемы долгих запросов при работе с почтовой системой RuPost

На контроллеры **ALD Pro** со стороны **RuPost** массово поступают запросы на поиск (*ldapsearch*), которые выполняются по 3-6 секунд, что приводит к отказу в обслуживании **LDAP** и останавливает работу **DNS**:

```
SRCH base="cn=users,cn=accounts,dc=company,dc=ru" scope=2 filter="(&
↪(|(mail=aldpro@company.ru)(mail=aldpro@company.
↪ru)(proxyAddresses=aldpro@company.ru))(&(objectClass=person)(mail=*@*)
```

Если таких запросов одновременно больше, чем потоков в *389 DS*, то *389 DS* перестает отвечать на любые запросы. В лог-файле это выглядит как выделение файловых дескрипторов без дальнейших операций.

Запросом ниже можно произвести проверку:

```
time ldapsearch -b "cn=users,cn=accounts,$(ipa env basedn|cut -d ' ' -f4)"
 ↪"(&(|(mail=somebody@$(hostname -d))(mail=somebody@$(hostname -
 ↪d))(proxyAddresses=somebody@$(hostname -d)))(&
 ↪(objectClass=person)(mail=*@*)(proxyAddresses=SMTP:*)))" "* aci" -Q
```

Если зафиксировано время более 1000 мс, то рекомендуется провести индексацию атрибута *proxyAddresses* в **LDAP**. Данную процедуру необходимо произвести на каждом контроллере домена только один раз.

Для этого необходимо выполнить действия ниже.

Вывести название *INSTANCE LDAP* командой, индексы нужно добавить на основной каталог, не на глобальный каталог:

```
sudo dsctl -l
```

Произвести добавление индексов:

```
sudo dsconf INSTANCE-NAME backend index add --index-type eq --attr
 ↪proxyAddresses userRoot
sudo dsconf INSTANCE-NAME backend index set --add-type sub --attr
 ↪proxyAddresses userRoot
sudo dsconf INSTANCE-NAME backend index set --add-type pres --attr
 ↪proxyAddresses userRoot
```

Проверить командой, что все типы добавлены:

```
sudo dsconf INSTANCE-NAME backend index get --attr proxyAddresses userRoot
```

Произвести остановку *INSTANCE LDAP* командой:

```
sudo dsctl INSTANCE-NAME stop
```

Запустить переиндексацию (может занять до нескольких минут) командой:

```
sudo dsctl slapd-INSTANCE-NAME db2index userRoot
```

Произвести запуск *INSTANCE LDAP* командой:

```
sudo dsctl INSTANCE-NAME start
```