ALD Pro

СЛУЖБА КАТАЛОГА ДЛЯ LINUX

Примечания к выпуску 3.0.0 (Release Notes)



Оглавление

Аннотация 3
Основная информация 4
Особенности бесплатной редакции Free 5
Модуль ACM 1.3.0 Инвентаризация 6
Ключевые доработки и нововведения 8
Прочие доработки и исправления 17

Аннотация

В настоящих примечаниях к выпуску вы можете найти описание улучшений и дополнений, реализованных в ALD Pro версии 3.0.0, а также информацию об известных ограничениях, исправлении ошибок, новых технологиях, устаревших функциях и других важных деталях.

Релиз 3.0.0 является прямым преемником версии 2.5.0 и сохранил с ней обратную совместимость, что позволит обновить систему без каких-либо затруднений. Выход этого релиза планировался ранее под номером 2.6.0, но учитывая общий объем улучшений, накопленный в рамках развития второй ветки продукта, мы пришли к выводу, что пора уже переходить на следующую мажорную версию.

Выбирая ALD Pro, вы выбираете лучшее. Безопасность и высокая надежность, простая миграция и удобство эксплуатации, мультивендорность и высокая совместимость с продуктами сторонних разработчиков — все это те качества, которые выгодно отличают продукт ALD Pro версии 3.0.0 от альтернативных решений на рынке.

Основная информация

Контроллеры домена и подсистемы продукта необходимо устанавливать на операционную систему ALSE версий **1.7.6.UU2** или **1.7.7.UU2.**

Рабочие станции могут работать под управлением ALSE в широком диапазоне версий: **1.7.6, 1.7.6.UU1, 1.7.6.UU2, 1.7.7, 1.7.7.UU1, 1.7.7.UU2, 1.8.1, 1.8.1.UU1, 1.8.1.UU2, 1.8.2, 1.8.2.UU1, 1.8.2.UU2, 1.8.3**. В релизе ALD Pro 3.0.0 мы не только расширили поддержку новых версий ALSE из очередных обновлений 1.7 и 1.8, но и добавили возможность присоединения к домену новых видов операционных систем. Теперь вы можете управлять в домене планшетами на архитектуре ARM с операционной системой **ALSE 4.7.6** и компьютеров на операционных системах **Альт Рабочая станция 10.4**, **Альт СП Рабочая станция 10**, **РЕД ОС 7.3.5**, **РЕД ОС 8**.

Программные интерфейсы ALD Pro 3.0.0 имеют обратную совместимость с предыдущими версиями 2.4.1 и 2.5.0, что позволит обновить систему без каких-либо затруднений (обращаем внимание на измененное количество параметров, необходимых для авторизации пользователя по API - более подробная информация представлена в документации API).

Вместе с релизом 3.0.0 через личный кабинет дополнительно предоставляются следующие инструменты:

- графическая утилита aldpro-join для присоединения компьютеров ALSE к домену с возможностью обновления пароля компьютера и рядом других востребованных функций;
- графическая утилита aldpro-setfacl для добавления доменных пользователей и групп в списки доступа на файловом сервере;
- решение по управлению паролями локальных администраторов (LAPS), позволяющее организовать регулярное обновление паролей администраторов с хранением информации в службе каталога в защищенных атрибутах компьютера;
- набор дополнительных параметров групповых политик, разработанных по требованиям ФСТЭК России №17 и №239;
- инструмент по экспорту/импорту объектов групповых политик.

Особенности бесплатной редакции Free

Мы рады сообщить, что, начиная с релиза ALD Pro 3.0.0, нашим пользователям стала доступна бесплатная редакция Free, которой можно воспользоваться для ознакомления с базовыми возможностями продукта или создания домена в небольших некоммерческих организациях, относящихся к категории SOHO (Small office/home office).

В редакции Free будут доступны следующие функции:

- установка одного контроллера домена;
- централизованная аутентификация для 25 пользователей домена;
- управление настройками через механизм групповых политик для 25 компьютеров;
- подключение к удаленному рабочему столу пользователей для оказания технической поддержки;
- доверительные отношения с одним доменом MS Active Directory;
- гарантированная возможность установки обновлений.

Для снятия ограничений бесплатной версии и получения доступа ко всем возможностям продукта вам нужно будет приобрести лицензию на коммерческое использование. Более подробную информацию вы можете получить на официальном сайте продукта aldpro.ru.

Модуль «ACM 1.3.0 Инвентаризация»

Редакция ACM 1.3.0 Инвентаризация разработана на основе полнофункциональной версии ACM 1.3.0 для включения в состав программного комплекса «ALD Pro Инвентаризация»

Редакция ACM 1.3.0 Инвентаризация имеет ограничения по предоставляемому функционалу, относительно полнофункциональной версии ACM 1.3.0, и предоставляет следующие функции:

1. Управление инфраструктурой Системы:
    - создание, редактирование и удаление сегментов управления;
    - создание, редактирование и удаление серверов агентов.
2. Управление пользователями и их возможностями:
    - ведение списка пользователей;
    - разграничение возможностей пользователей;
    - управление наборами возможностей пользователей.
3. Управление организационной структурой (директориями) компьютеров:
    - создание, редактирование и удаление подразделений (директорий) компьютеров;
    - ведение списка подразделений (директорий) компьютеров;
    - возможность настройки организационной структуры подразделений (директорий) компьютеров в иерархическом виде;
    - возможность управления составом компьютеров в директории.
4. Управление компьютерами:
    - установка агента и подключение управляемого компьютера к системе;
    - создание, редактирование и удаление записей компьютеров;
    - ведение списка компьютеров;
    - возможность экспорта отчета по списку компьютеров в файл;
    - возможность экспорта отчета по инвентарным данным компьютера в файл.
5. Аппаратная инвентаризация:
    - возможность сбора инвентарных данных об аппаратной части управляемых компьютеров;
    - возможность просмотра собранных сведений об аппаратной части управляемых компьютеров.

6. Инвентаризация установленного ПО:
    - возможность сбора инвентарных данных по программной части управляемых компьютеров;
    - управление (создание, изменение, удаление) правилами обнаружения ПО на управляемых компьютерах;
    - предоставление предустановленных правил обнаружения ПО;
    - возможность просмотра собранных сведений о программной части управляемых компьютеров;
    - возможность просмотра собранных сведений о пакетах ПО на управляемых компьютерах.
7. Учет лицензий:
    - выполнение учета лицензий ОС Astra Linux на основе собранных инвентарных данных с управляемых компьютеров;
    - возможность экспорта отчета по списку лицензий ОС Astra Linux в файл;
    - возможность экспорта отчета по данным отдельной выбранной лицензии ОС Astra Linux в файл.
8. Управление пользовательской сессией в веб-браузере:
    - возможность входа в Систему через веб-интерфейс;
    - завершение текущей сессии в веб-интерфейсе Системы;
    - управление цветовой схемой веб-интерфейса Системы.
9. Справочный центр:
    - наличие встроенного в Систему справочного центра на русском языке;
    - возможность доступа к справочному центру из любого компонента Системы.

Ключевые доработки и нововведения

В рамках релиза ALD Pro 3.0.0 стали доступны следующие улучшения:

1. **Реализована возможность централизованного управления функциями мандатного контроля для операционных систем Astra Linux.**

   Одним из ключевых преимуществ операционной системы специального назначения Astra Linux является встроенный комплекс средств защиты информации «PARSEC», реализующий функции мандатного (обязательного) контроля, позволяющие обеспечить возможность безопасной работы инфраструктур любого масштаба и с данными любой степени конфиденциальности, что подтверждается сертификатами ФСТЭК России, ФСБ России и Минобороны России.

   Модуль ядра «PARSEC» позволяет динамически контролировать целостность системных файлов и предотвращать утечку конфиденциальной информации даже в том случае, если все предыдущие уровни защиты окажутся неспособны сдержать кибератаку злоумышленников. Обязательность модели мандатного контроля выражается в том, что мандатными метками может управлять только администратор системы, в то время как классические дискреционные права доступа могут раздавать и обычные пользователи, являющиеся просто владельцами файлов (от лат. discretio — решение должностным лицом какого-либо вопроса по собственному усмотрению).

   В версии ALD Pro 3.0.0 реализована возможность централизованного управления функциями мандатного контроля через портал управления: появились соответствующие интерфейсы для управления уровнями и категориями конфиденциальности, а в карточке пользователя теперь есть возможность назначить допустимые значения этих параметров для конкретного сотрудника. Централизованная настройка уровней и категорий МКЦ/МРД на рабочих станциях выполняется с помощью групповых политик ALD Pro, а допустимые значения для пользователя, выполняющего вход в систему, предоставляет служба SSSD.

2. **Реализована возможность централизованного управления учтенными USB-накопителями для операционных систем Astra Linux.**

   Для предотвращения угрозы проникновения вредоносных программ в ИТ-инфраструктуру предприятия через использование сотрудниками случайных USB-накопителей в операционной системе Astra Linux есть возможность запрета монтирования неучтенных носителей, для которых не созданы специальные udev-правила, определяющие параметры их подключения в системе. При регистрации накопителя администратор может указать дискреционные и мандатные права доступа, с которыми это устройство должно монтироваться в

системе, что позволяет безопасно использовать внешние накопители даже в тех случаях, когда на предприятии введен режим секретности.

В версии ALD Pro 3.0.0 реализована возможность централизованного управления учтенными носителями через портал управления. Теперь администратор может регистрировать устройства не только локально в операционной системе конкретного компьютера, но и централизованно в службе каталога, чтобы эта информация была доступна на всех компьютерах в ИТ-инфраструктуре предприятия. За извлечение этой информации из домена отвечает служба SSSD, которая в операционной системе ALSE тесно интегрирована с модулем «PARSEC».

3. **Реализована проверка паролей по списку запрещенных слов.**

В службе каталога ALD Pro уже были политики, которые позволяли установить ограничения по длине и сложности паролей, но с их помощью невозможно было запретить использование в паролях широко распространенных слов, таких как названия городов, брендов или имен известных людей. Пароли с такими словами намного легче подобрать, поэтому для повышения безопасности ИТ-инфраструктуры была реализована дополнительная проверка по списку запрещенных слов.

Проверка новых паролей на отсутствие запрещенных слов выполняется плагином LDAP-сервера на стороне контроллеров домена. Редактировать список запрещенных слов можно непосредственно на портале управления, а распространение этой информации между контроллерами домена осуществляется через стандартную LDAP-репликацию.

В дальнейшем планируется дополнительно реализовать возможность проверки новых учетных данных по базам утекших паролей, что дополнительно снизит вероятность успешных атак методом перебора. Особенность такой проверки заключается в том, что базы утекших паролей могут содержать сотни миллионов строк, поэтому потребуется более простой и быстрый алгоритм проверки, учитывающий только полное совпадение слов, и принципиально иной способ распространения баз утекших паролей между контроллерами домена.

4. **Реализована поддержка операционных систем Альт и РЕД ОС.**

Хорошо известно, что моновендорный подход, при котором построение ИТ-инфраструктуры выполняется с использованием оборудования и программного обеспечения ограниченного числа поставщиков, позволяет добиться наилучшей совместимости и существенно сократить накладные расходы на поддержку и обучение сотрудников. Вместе с тем мы понимаем, что в текущих условиях организации не всегда могут себе позволить придерживаться лучших практик,

поэтому в рамках принятого мультивендорного подхода была реализована поддержка операционных систем альтернативных вендоров.

К домену ALD Pro всегда можно было присоединить любую операционную систему Linux, у которой есть служба SSSD, но в этом случае становились доступны только базовые функции аутентификации/авторизации и минимальный набор политик, таких как правила HBAC, SUDO и Automount. Начиная с версии ALD Pro 3.0.0 для операционных систем Альт Рабочая станция 10.4, Альт СП Рабочая станция 10, РЕД ОС 7.3 и РЕД ОС 8 официально предоставляется клиентская часть ALD Pro, которая реализует возможность управления этими операционными системами через механизм групповых политик на базе Salt-скриптов.

На данный момент выполнена адаптация и подтверждена кроссплатформенность Salt-скриптов для следующих параметров групповых политик:

- Параметры компьютера:
  - Оборудование > Установить принтеры;
  - Дата и время > Настройки сервиса сетевого времени Chrony;
  - Дата и время > Параметры сервера или пула сетевого времени;
  - Загрузчик GRUB2 > Автоматическая загрузка;
- Параметры пользователя:
  - Приложения для типов файлов > Приложение для типов файлов;
  - Приложения для типов файлов > Сетевые приложения.

Работа по расширению количества кроссплатформенных параметров групповых политик, которые могут быть использованы для централизованного управления операционными системами альтернативных вендоров, будет продолжена в следующих релизах.

5. **Увеличена надежность и производительность модуля синхронизации.**

Создавая модуль синхронизации, мы оказались правы, что этот механизм будет крайне востребован на проектах импортозамещения, так как мигрировать всю ИТ-инфраструктуру разом зачастую просто невозможно, а этот модуль позволяет обеспечить доступ пользователей по логину/паролю к любой системе вне зависимости от того, к какому домену она подключена.

За последний год мы получили много конструктивной обратной связи и нашли более эффективные алгоритмы для обеспечения быстрой и надежной синхронизации данных, которые воплотили в нашей новой версии модуля синхронизации. Можно отметить следующие основные улучшения:

- сопоставление объектов выполняется теперь по уникальным идентификаторам objectGUID и nsUniqueId, что исключает любые коллизии;
- улучшен алгоритм синхронизации пользователей, что полностью исключает нежелательные задержки при извлечении и применении этих изменений;
- синхронизация паролей вынесена в отдельный поток, что повышает скорость применения этих изменений;
- журнал событий разделен на три потока:
  - сервисный поток — события о запуске и остановке сервисов;
  - операционный поток — события о выполнении операций с объектами внутри сервисов: сохранение, удаление, обновление закэшированных данных в базе Postgres;
  - поток синхронизации — все события, связанные с применением изменений в каталоге ALD Pro.

6. **Обеспечена поддержка централизованного управления пространством имен распределенной файловой системы (аналог DFS Namespaces).**

   На файловых серверах Windows была очень востребованная технология Distributed File System Namespaces (DFS-N), которая позволяла группировать общие папки, расположенные на разных серверах, в одно логическое пространство имен. Используя эту функцию, системные администраторы могли скрыть от пользователей детали физического размещения ресурсов.

   В мире Linux альтернативой DFS-Namespaces является технология автоматического монтирования дисков, которая работает на связке из нескольких компонентов: ловушек файловой системы autofs, утилиты automount, службы autofs, а также стандартных компонентов для работы с SMB-ресурсами. Карты автомонтирования, по сути, решают сразу две задачи – это и построение дерева ресурсов, и монтирование этих ресурсов на рабочих станциях.

   В службе каталога FreeIPA и клиентской части SSSD уже были все функции, необходимые для централизованной работы с картами монтирования, поэтому в рамках ALD Pro 3.0.0 нам осталось только реализовать параметр групповой политики (Параметры компьютера > Служба автомонтирования), с помощью которого можно централизованно активировать этот механизм на рабочих станциях.

В дальнейшем мы планируем реализовать на портале управления удобный интерфейс для управления пространством имен, чтобы упростить администраторам поддержку и развитие инфраструктуры файловых серверов.

7. **Повышена производительность портала управления.**

   В качестве LDAP-сервера служба каталога ALD Pro использует 389 Directory Server, программный код которого изначально создавался для операторов связи, поэтому способен выдержать колоссальные нагрузки по количеству операций чтения. Продуктовая команда ALD Pro провела тщательное исследование возможностей горизонтального и вертикального масштабирования и подтверждает возможность работы больших доменов, в которых более 400 контроллеров и 30 млн. объектов. Вместе с тем для возможности работы с такими предельными значениями требовалась тонкая настройка параметров системы и оптимизация программного кода портала управления.

   Для обеспечения комфортной работы администраторов в доменах на 300+ тысяч пользователей в версии ALD Pro 3.0.0 мы уделили внимание следующим разделам портала управления:

   - Пользователи и компьютеры > Пользователи;
   - Пользователи и компьютеры > Организационная структура > Карточка подразделения > Вкладка «Пользователи»;
   - Пользователи и компьютеры > Группы пользователей > Карточка группы пользователей > Вкладка «Пользователи».

   В рамка этих работ были реализованы следующие улучшения:

   - устранена медленная загрузка списка пользователей при количестве пользователей в системе более 300 000;
   - устранено медленное добавление пользователей в подразделения с количеством участников более 300 000;
   - оптимизировано добавление пользователей в группы пользователей;
   - устранены ошибки в работе с подразделениями, в названиях которых используются символы на кириллице;
   - взамен медленной сортировки по атрибутам «Должность» и «Подразделение» реализована фильтрация по уникальным значениям в пределах 2000 результатов для страниц:
     - Пользователи и компьютеры > Пользователи;

- Пользователи и компьютеры > Организационная структура > Карточка Подразделения > Вкладка «Пользователи».

На странице «Пользователи и компьютеры > Группы пользователей > Карточка группы пользователей > Вкладка "Пользователи"» фильтрация доступна только если в группе не более 2000 пользователей;

- исправлена некорректная работа сортировки по атрибутам «ФИО» и «Логин».

8. **Решение по управлению паролями локальных учетных записей (LAPS) встроено в состав продукта.**

Для обеспечения безопасности ИТ-инфраструктуры в домене ALD Pro рекомендуется настраивать групповую политику для регулярного обновления паролей локальных администраторов, чтобы уволенные сотрудники не могли располагать этой информацией.

В пилотном варианте исполнения политика LAPS стала доступна вместе с релизом ALD Pro 2.5.0 и получила положительные отзывы со стороны заказчиков. В версии 3.0.0 были выполнены следующие работы по встраиванию решения LAPS в состав продукта:

- параметр групповой политики LAPS включен в общий каталог (см. «Параметры компьютеров > Безопасность > Пароли локальных администраторов»), поэтому для использования решения LAPS импортировать параметр групповой политики вручную больше не требуется;
- в схему каталога внесены необходимые атрибуты и объектные классы, поэтому для использования решения LAPS расширять схему каталога вручную больше не требуется.

В дальнейшем планируем отказаться от дополнительного приложения и встроить функциональные возможности этого приложения в портал управления.

9. **Улучшена графическая утилита для ввода машины в домен.**

В рамках релиза ALD Pro 2.5.0 вышла новая графическая утилита aldpro-join для присоединения компьютеров Astra Linux к домену ALD Pro с привычным для Windows-администраторов интерфейсом, что существенно упростило выполнение данной процедуры. Мы получили много положительной обратной связи от заказчиков и смогли учесть предложения по улучшениям в нашей новой версии, которая доступна также через личный кабинет пользователя в виде архива с deb-пакетом и инструкцией по применению.

В последующих релизах планируется встроить программный код утилиты в состав штатного приложения aldpro-client-installer, что даст возможность использовать этот инструмент в том числе для присоединения к домену альтернативных операционных систем сторонних разработчиков.

10. **Улучшена утилита установки и обновления контроллеров домена.**

    В утилите aldpro-server-install версии 3.0.0 был реализован расширенный набор проверок системных требований и входных параметров, что позволяет системному администратору получить подробную информацию о возможности установки или обновления продукта еще до начала выполнения соответствующей операции.

    Для сохранения обратной совместимости с инструментами автоматизации от сторонних разработчиков функция расширенной валидации в утилите aldpro-server-install по умолчанию отключена и должна быть активирована с помощью ключа --validate, что указано в руководстве администратора. Со следующей LTS-версии продукта поведение утилиты будет изменено, поэтому для отключения проверок нужно будет явно указывать ключ --validate=false.

11. **Оптимизирована работа механизма аутентификации на портале управления.**
    Для аутентификации на портале управления теперь используется связка модулей mod_auth_gssapi и mod_session с сессионной cookie, что позволило избежать повторных GSSAPI-аутентификаций при выполнении каждого авторизованного запроса и снизить общую нагрузку на сеть.

12. **Автоматизирована очистка хранилища сервера репозиториев.**

    Улучшена работа скрипта aldpro-repo-garbage-collector при обрыве связи в процессе загрузки больших ISO-образов. Теперь ненужные файлы удаляются автоматически, чтобы не занимать лишнее место на диске.

13. **Улучшена валидация входных значений.**
    Мы продолжили работу над улучшением валидации входных значений, что необходимо для повышения информационной безопасности продукта и предотвращения нарушений в его работе. Важность правильной валидации данных обусловлена следующими ключевыми факторами:

    - информационная безопасность – валидация предотвращает различные виды атак, такие как XSS, SQL-инъекции, DoS и другие;
    - защита логики приложения – отсутствие валидации может привести к нарушению бизнес-логики и некорректной работе системы.

    В рамках версии 3.0.0 были реализованы следующие улучшения:

    - добавлена проверка идентификаторов заданий автоматизации на наличие запрещенных символов. В идентификаторах допускается использовать

только латинские символы в любом регистре (A-Za-z), цифры (0-9) и символ подчеркивания (_);

- добавлена возможность указывать порт в поле «Подключение» при создании нового принтера на вкладке «Роли и службы сайта > Служба печати > Сервер > Новый принтер»;
- исправлена валидация полей «Разрешить запрос» и «Разрешить перенос» для зон DNS на вкладке «Роли и службы сайта > Служба разрешения имён > Зоны DNS > Зона > Вкладка "Параметры зоны"»;
- исправлена валидация поля «Базовое уникальное имя (base DN)» на вкладке «Управление доменом > Доверительные отношения > Новое подключение к Active Directory». В значении Base DN теперь допускается использовать пробелы;
- исправлена валидация поля «Домен» на вкладке «Управление доменом > Доверительные отношения > Новое подключение к Active Directory». В имени домена теперь допускается использовать символ дефиса. Имя домена может содержать латинские символы в любом регистре (A-Z a-z), цифры (0-9) и специальные символы (.-).

14. **Повышена безопасность системы.**

    В версии ALD Pro 3.0.0 реализовано порядка 40 различных запросов, направленных на повышение безопасности систем, в том числе устраняющих такие уязвимости, как CVE-2020-27783, CVE-2021-28957 и др.

15. **Улучшена документация.**

    Мы непрерывно улучшаем качество нашей документации, ее структурированность, полноту и достоверность, в том числе с учетом обратной связи от наших заказчиков и коллег с проектов внедрения. Начиная с версии ALD Pro 3.0.0, стали доступны следующие улучшения:

    - Для упрощения знакомства администраторов с возможностями продукта в комплект документации было включено краткое руководство по началу работы «Быстрый старт», которое представляет собой пошаговую инструкцию по установке первого контроллера домена и присоединению к нему типовой рабочей станции под управлением Astra Linux.

      Этот документ содержит краткое описание требуемых действий с небольшими пояснениями и подсказками, в каких разделах основной документации можно получить исчерпывающие подробности. Если вам потребуется провести краткий инструктаж для нового администратора, мы настоятельно рекомендуем начинать с краткого руководства «Быстрый старт».

- Для упрощения знакомства сотрудников, не являющихся специалистами ИТ-отдела, с особенностями работы персональных компьютеров в составе домена было переработано руководство пользователя, в котором оставлены только наиболее важные разделы по использованию рабочей станции в домене, а все разделы, имеющие отношение к настройке домена через портал управления, перенесены в руководство администратора.
  Если вам потребуется провести краткий инструктаж нового сотрудника при выдаче корпоративного ноутбука, мы настоятельно рекомендуем начинать с руководства пользователя.
- Так как установка, обновление подсистем и их настройка, использование и поддержка - это две разные задачи, то мы разделили руководство администратора на две части. В Руководство администратора, часть 1 попали инструкции по развертыванию и обновлению подсистем (ранее главы 1, 2 и 3 из руководства администратора)
- В Руководство администратора, часть 2 попали:
  - информация о работе в портале управления, которая раньше была в руководстве пользователя;
  - полезные инструкции (ранее глава 6 руководства пользователя);
  - известные проблемы (ранее глава 4 руководства пользователя);
  - отладка подсистем (ранее глава 5 руководства пользователя);
  - другие актуализированные инструкции.
- Добавлена инструкция по настройке регулярного резервного копирования информации службы каталога с помощью системы RuBackup, в которой подробно раскрыты нюансы процедуры авторитативного восстановления.
- Добавлена инструкция по настройке подсистемы мониторинга для сбора и отображения информации о целостности каталога, что позволит оперативно получать информацию о проблемах с репликацией, которые могут возникать, например, по причине отсутствия связи между контроллерами домена.
- Для удобства доступа к информации и оперативного поиска представлена документация на сайте ALD Pro. Информацию для версии ALD Pro 3.0.0 можно найти на странице https://www.aldpro.ru/materials/3.0.0/.

Прочие доработки и исправления

#	Компонент	Описание улучшения
1.	Глобальный каталог	Исправлена ошибка некорректного формирования атрибута «name» в глобальном каталоге.
2.	Глобальный каталог	Исправлена проблема некорректного удаления SRV-записей при удалении роли глобального каталога.
3.	Гранулярное управление доступом	Изменен ответ при обращении к API методом POST по адресу /api/syncer/options/key. Если у пользователя недостаточно прав, теперь он будет получать ошибку «ForbiddenError» вместо «DeniedIPAError».
4.	Гранулярное управление доступом	Изменен ответ при обращении к API методом POST по адресу /api/ds/dns/globalconfig. В поле «error» теперь передается текст «Отсутствуют права на выполнение данной операции».
5.	Гранулярное управление доступом	Изменен ответ при обращении к API методом PATCH по адресу /api/ds/dns/zones/{zoneName}, возвращаемый при попытке изменения DNS-зоны из-под учетной записи пользователя, который не имеет достаточных прав доступа. Текст ошибки «Cannot update entry» изменен на «Операция завершена с ошибкой. Отсутствуют права на выполнение данной операции».
6.	Доверительные отношения	Исправлена проблема создания доверительных отношений при наличии цифр в имени домена первого уровня.
7.	Компонент 389DS	Из состава дистрибутива исключен неиспользуемый плагин ldap-plugin-postop-sender.
8.	Модуль миграции и синхронизации	Устранена проблема с зависанием заданий автоматизации на контроллере, где выполнялась миграция пользователей.
9.	Параметры групповых	Устранена проблема автоматического упорядочивания ярлыков рабочего стола при

#	Компонент	Описание улучшения
	политик	применении групповых политик. Теперь пользователь может разместить ярлыки любым удобным для него способом.
10.	Параметры групповых политик	В состав дополнительных параметров групповых политик, поставляемых через личный кабинет, включено два параметра, с помощью которых можно управлять настройками конфигурационного файла sssd.conf. В дальнейшем эти параметры будут включены в состав основного продукта.
11.	Параметры групповых политик	Расширены возможности групповых политик по настройке горячих клавиш. Дополнительные функции реализованы в новом параметре, а прежние параметры, размещенные в каталоге "Горячие клавиши", с версии 3.0.0 считаются устаревшими, но оставлены в каталоге для обеспечения обратной совместимости. Новый параметр решает также проблему невозможности использования горячего сочетания <Ctrl> + <Shift> для изменения раскладки.
12.	Параметры групповых политик	Параметры групповых политик теперь применяются даже в том случае, если не задан ни один из атрибутов, что больше соответствует ожиданиям пользователей.
13.	Параметры групповых политик	Переработан скрипт параметра групповой политики «Планировщик задач» для повышения надежности его работы в различных сценариях использования.
14.	Параметры групповых политик, Подсистема «Печать»	Параметр групповой политики по добавлению принтеров будет использовать драйвер everywhere вместо raw, так как raw считается устаревшим и не будет поддерживаться в будущих версиях. Это решает также проблему некорректной работы функций дуплексной и цветной печати в некоторых приложениях.

#	Компонент	Описание улучшения
15.	Подсистема «Динамическая настройка узла» DHCP	Исправлено некорректное заполнение конфигурационного файла dhcpd.conf в тех случаях, когда полное FQDN-имя одного DHCP-сервера являлось подстрокой другого DHCP-сервера. Теперь каждый DHCP-сервер получает свои настройки независимо.
16.	Подсистема «Контроллер домена»	Снято ограничение на использование доменов, которые в компонентах имени содержат следующие слова: localhost, PRN, AUX, CLOCK, NUL, COM1 … COM9, LPT1 … LPT9, Total, Maximum, arpa, admin, root, ftp, web, www, mail, mailer.
17.	Подсистема «Контроллер домена»	После удалении контроллера домена теперь не вызывается стейт send_log_to_ldap, который записывает результаты операции в LDAP-каталог, т. к. по завершении процедуры удаления в домене уже нет учетной записи сервера и такая попытка будет приводить к появлению лишних ошибок в журнале службы Salt Minion.
18.	Подсистема «Контроллер домена»	Из состава дистрибутива исключен более неактуальный скрипт 95-2.3.0-sys-account.update.
19.	Подсистема «Контроллер домена»	Алгоритм хеширования паролей изменен с PBKDF2-SHA512 на PBKDF2-SHA256 (реализация Rust), что дает значительный прирост производительности при выполнении LDAP-аутентификации по паролю.
20.	Подсистема «Контроллер домена»	Исправлены опечатки во встроенной справке к утилите aldpro-server-install для установки контроллера домена.
21.	Подсистема «Контроллер домена»	Изменен ответ при обращении к API методом PATCH по адресу /api/ds/users/{userName}, возвращаемый при попытке изменения несуществующего пользователя. Текст ошибки изменен на «Пользователь с идентификатором

#	Компонент	Описание улучшения
		<uid пользователя> не найден».
22.	Подсистема «Контроллер домена»	Изменен ответ при обращении к API методом POST по адресу /ad/api/ds/users и методом PATCH по адресу /api/ds/users/{userName}, возвращаемый в том случае, если при создании или изменении пользователя в поле user_organizational_unit_dn будет указано несуществующее подразделение. Код ответа 404 NotFound изменен на 409 IntegrityError. Текст ошибки изменен на «Подразделение с dn <DN подразделения> не существует».
23.	Подсистема «Контроллер домена», Подсистема «Портал управления»	В модуле миграции устранена ошибка, возникающая при выполнении поиска подразделений MS AD по подстроке, состоящей только из цифр.
24.	Подсистема «Мониторинг»	Из состава пакета aldpro-ms исключен неиспользуемый скрипт aldpro-update-ms.
25.	Подсистема «Портал управления»	Исправлена проблема назначения дополнительных классов (objectClass) на новые группы при их создании через веб-интерфейс портала управления. Дополнительные классы настраиваются в интерфейсе «Параметры групп».
26.	Подсистема «Портал управления»	Для упрощения работы с однофамильцами в веб-интерфейсах, где использовались списки пользователей, в дополнение к полям «ФИО» и «Должность» добавлены поля «Логин» и «Подразделение». Изменения затронули следующие страницы: ● Управление доменом > Роли и права доступа > Карточка роли > Вкладка «Пользователи»; ● Пользователи и компьютеры > Организационная структура > Карточка подразделения > Вкладка «Пользователи»;

#	Компонент	Описание улучшения
		• Пользователи и компьютеры > Группы пользователей > Карточка Группы > Вкладка «Пользователи»; • Групповые политики > Политики доступа к узлу >Вкладка «Правила HBAC» > Карточка правила HBAC > вкладка «Пользователи» > Категория «Указанные пользователи и группы»; • Групповые политики > Политики повышения привилегий > Вкладка «Правила Sudo» > Карточка правила > Вкладка «Пользователи» > Категория «Указанные пользователи и группы».
27.	Подсистема «Портал управления»	Устранена проблема, которая периодически приводила к появлению ошибки аутентификации на портале управления с описанием «Can't contact LDAP server».
28.	Подсистема «Портал управления»	По нажатию кнопки «Получить ключ» на вкладке «Модуль синхронизации > Настройки > Синхронизация паролей > Получить ключ» теперь открывается окно с требованием подтвердить желаемое действие.
29.	Подсистема «Портал управления»	Изменен ответ при обращении к API методом POST по адресу /api/ds/dhcp/servers, возвращаемый при попытке назначения роли DHCP-сервера на несуществующий хост. Код ответа 500 InternalServerError заменен на 409 IntegrityError.
30.	Подсистема «Портал управления»	Изменен ответ при обращении к API методом POST по адресу /api/ds/users, возвращаемый при попытке создания пользователя, длина имени которого превышает максимально допустимую длину, указанную на странице Управление доменом > Пользователи и группы > Вкладка «Параметры пользователей» > Поле «Максимальная длина имени пользователя». Код ошибки «ValidationError» заменен на

#	Компонент	Описание улучшения
		«StorageConflictError».
31.	Подсистема «Печать»	Из состава пакета aldpro-ps исключен неиспользуемый сервис aldpro-allow-discovery.
32.	Подсистема «Печать»	Теперь в описании принтеров допустимо использовать значения, состоящие только из цифр. Ранее при наличии таких принтеров в системе применение настроек сервера печати завершалось ошибкой.
33.	Подсистема «Печать»	Устранена проблема, из-за которой с портала управления невозможно было отменить задание на печать.
34.	Подсистема «Печать»	Новые принтеры теперь добавляются с параметром printer-is-shared=True, что позволяет их сразу использовать без выполнения дополнительных настроек на стороне сервера печати.
35.	Подсистема «Печать»	В списке принтеров подсистемы печати исправлено некорректное отображение названия драйвера.
36.	Подсистема «Установка ОС по сети»	Изменен ответ при обращении к API методом POST по адресу /api/os/installer-servers/{installer Server Common Name}/computers, возвращаемый при попытке создания привязки профиля установки ОС по сети к компьютеру, имя которого уже существует в домене. Код ответа 500 InternalServerError и код ошибки «ProjectError» заменены на код ответа 409 IntegrityError и код ошибки «Duplicate Entry» соответственно.
37.	Документация. Инструкция по резервному копированию подсистем ALD Pro	Исправлен путь к директории с резервными копиями, а также уточнена информация по работе со скриптом backup_dc.sh. Добавлены команды для просмотра содержимого архива и для реинициализации репликации.

#	Компонент	Описание улучшения
38.	Документация. Руководство администратора, часть 1	В раздел «Подготовка к обновлению ALD Pro» добавлена рекомендация о временном отключении расширенного аудита 389-ds перед выполнением обновления.
39.	Документация. Руководство администратора, часть 1	В раздел «Обновление подсистем ALD Pro до новой версии» добавлена информация о порядке обновления ALD Pro и ОС.
40.	Документация. Руководство администратора, часть 1	В раздел «Развертывание контроллеров домена и подсистем» добавлена информация о том, что установка подсистем возможна только на «чистую» операционную систему, поэтому после удаления подсистемы соответствующий хост нужно вывести из домена, т. к. повторная установка подсистем на него будет невозможна.
41.	Документация. Руководство администратора, часть 2	В раздел «Известные проблемы» добавлена инструкция по решению проблемы медленного монтирования сетевых ресурсов пользователями доверенных доменов.
42.	Документация. Руководство администратора, часть 2	В разделе «Групповые политики > Групповые политики > Настройка групповой политики > Параметры компьютеров/пользователей» расширено описание атрибутов для настройки требований к операционной системе.
43.	Документация. Справочный центр	Актуализирована информация в разделе справочного центра «Мониторинг > Витрины мониторинга домена > Просмотр витрины». Убрано предупреждение об ошибке «ERROR - cn=test1,cn=users - ошибка в атрибуте name», ошибку можно игнорировать.
44.	Документация. Справочный центр	Актуализирована информация в разделе справочного центра «Установка ОС по сети > Редактирование сервера установки ОС». Удалена информация о вкладке «Операционные системы», которая была упразднена в предыдущих релизах продукта.

#	Компонент	Описание улучшения
45.	Документация. Справочный центр	В справочном центре внесены уточнения по установке и удалению подсистемы «Общий доступ к сетевым дискам». Кнопка для удаления подсистемы с хоста называется «Удалить», а не «Удалить сервер», после удаления подсистемы учетная запись хоста остается в домене, а ее запись продолжает отображаться в списке подсистем с соответствующим статусом.
46.	Документация. Справочный центр, Руководство администратора, часть 2	В справочный центр и в Руководство администратора, часть 2 добавлено предупреждение о том, что модуль миграции устарел и вместо него следует использовать модуль синхронизации с доменом MS AD.
47.	Документация. Справочный центр, Руководство администратора, часть 2	В справочном центре в раздел «Модуль синхронизации > Источники > Сопоставление подразделений > Создание нового сопоставления» и в соответствующие разделы Руководства администратора, часть 2 добавлено предупреждение о том, что синхронизация из ALD Pro в MS AD выполняется только в части паролей пользователей. Все остальные атрибуты синхронизируются только в направлении из MS AD в ALD Pro.
48.	Документация. Справочный центр, Руководство администратора, часть 2	В раздел «Управление доменом > Интеграции с доменами > Миграции MS AD» расширено описание полей для настройки миграции.