ALD Pro

# СЛУЖБА КАТАЛОГА ДЛЯ LINUX

## Примечания к выпуску 3.1.0 (Release Notes)



**Оглавление**

Аннотация....3
Ключевые доработки и нововведения....6
Прочие доработки и исправления....9
Изменения в документации....12

**Аннотация**

В настоящих примечаниях к выпуску вы можете найти описание улучшений и дополнений, реализованных в ALD Pro версии 3.1.0, а также информацию об известных ограничениях, исправлении ошибок, новых технологиях, устаревших функциях и других важных деталях.

Релиз 3.1.0 является очередным минорным релизом в ветке, поэтому сохраняет полную обратную совместимость с версией 3.0.0, что позволит обновить систему, расширяя ее функциональные возможности. При работе над данным релизом решены задачи, которые сделали систему еще более отказоустойчиво и защищенной.

Важно отметить, что релиз 3.1.0 станет основой для предстоящей LTS-версии 3.2.0 (Long Term Support), для которой в соответствии с принятой политикой жизненного цикла продукта будут выпускаться патчи безопасности на срок не менее 12 месяцев, что позволит снизить накладные расходы на обновление инфраструктуры при промышленной эксплуатации продукта.

**Основная информация**

Контроллеры домена и подсистемы продукта необходимо устанавливать на операционную систему ALSE версий **1.7.7.UU2** и **1.7.8**.

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, 1.7.8, 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, 1.8.3.UU1, 4.7.6** (ARM-архитектура);
- **Альт Linux 10.2.1** и **10.4**;
- **РЕД ОС 7.3** и **8**.

Программные интерфейсы ALD Pro 3.1.0 имеют полную обратную совместимость с предыдущими версиями 3.0.0, что позволяет обновить систему без каких-либо затруднений.

В версии 3.0.0 в утилите установки и обновления контроллеров домена aldpro-server-install реализован расширенный набор проверок системных требований и входных параметров. Для сохранения обратной совместимости с инструментами автоматизации от сторонних разработчиков функция расширенной валидации по умолчанию отключена и активируется с помощью ключа --validate.

Начиная с версии 3.2.0 расширенная валидация будет включена по умолчанию. Чтобы обновление до 3.2.0 не повлияло на существующие скрипты, заранее вызывайте утилиту с флагами --validate --force.

Ранее мы писали, что в 3.2.0 для сохранения обратной совместимости с автоматизацией нужно указывать --validate=false. Однако, этот механизм, оказался избыточен, так как с предыдущей версии есть возможность (описанная выше) настроить автоматизацию для сохранения обратной совместимости.

Вместе с релизом 3.1.0 через личный кабинет дополнительно предоставляются следующие инструменты:

- графическая утилита aldpro-dcpromo для установки первого контроллера домена, предоставляющая дополнительные проверки входных параметров и возможность возврата системы к исходному состоянию при возникновении ошибки в ходе установки;
- 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 No17 и No239;
- инструмент по экспорту/импорту объектов групповых политик.

**Ключевые доработки и нововведения**

В рамках релиза ALD Pro 3.1.0 стали доступны следующие улучшения:

1. **Для возможности авторизованного взаимодействия компонентов ALD Pro между собой всем подсистемам и сервисам назначены уникальные учетные записи, что значительно повышает общую безопасность системы.**

   Теперь каждый контроллер домена, подсистема и сервис имеют свою уникальную учетную запись. При этом все пароли скрыты, что снижает риск компрометации данных. В результате работа системы становится еще более надежной и безопасной.

   В случае, если учетные данные окажутся скомпрометированы, системный администратор сможет сменить пароль или заблокировать учетную запись, чтобы обеспечить безопасную работу системы.

   Наличие уникальной учетной записи для каждой подсистемы и сервиса, упрощает анализ логов и существенно сокращается время реагирования на инциденты.

2. **Увеличено количество параметров и повышена надежность скриптов.**

   Скрипты параметров групповых политик требуется регулярно тестировать и дорабатывать, так как со временем синтаксис конфигурационных файлов может меняться при обновлении приложений. В рамках релиза 3.1.0 внесены улучшения по 35 параметрам групповых политик, исправлены ошибки работы параметров Санкции-PolicyKit1, улучшены и скорректированы 22 описания параметров ГП.

3. **Разработаны рекомендации по шифрованию системного диска с необходимостью ввода пароля при загрузке сервера.**

   Для быстрой аутентификации пользователей в удаленных офисах с плохими каналами связи в этих локациях рекомендуется размещать как минимум один контроллер домена. При этом такие офисы обычно отличаются не только плохими каналами связи, но и более низкой физической безопасностью ИТ-инфраструктуры, а так как контроллеры содержат полную копию каталога, то кража любого из этих серверов приведет к компрометации всего домена.

   Мы обеспечили безопасность учетных данных, разработав рекомендации по настройке шифрования системного диска. Такой подход решает задачу защиты данных в условиях пониженной физической безопасности инфраструктуры:

   - при выключенном сервере содержимое диска полностью недоступно для чтения;
   - даже при физической краже оборудования доступ к учётным данным и копии каталога невозможен без обладания ключом шифрования;
   - уровень безопасности сопоставим с концепцией, которую Microsoft реализует через RODC (Read-only Domain Controller), где исключается хранение паролей.

Шифрование системного диска в рамках ALD Pro реализуется средствами LUKS (Linux Unified Key Setup), встроенными в операционную систему Astra Linux, на базе которой функционирует контроллер домена. Технология LUKS обеспечивает полное шифрование корневого диска сервера, включая каталоги с данными контроллера домена. Доступ к системе возможен только после ввода пароля расшифровки при загрузке. В удалённых офисах это может выполняться через интерфейс удалённого управления сервером.

4. **Улучшение интерфейса и пользовательского опыта.**

   Выполнено несколько улучшений по запросам заказчиков:

   - При редактировании параметра ГП теперь можно обратиться к справочной информации и продолжить работу с параметром без потери введенных ранее значений.
   - При создании прямой DNS-зоны реализована опция "Пропустить проверку пересечения", при активации которой зона будет создана принудительно, даже если такая зона уже существует в распределенной базе доменных имен. Например, если в компании ранее использовалась зона msk.company.ru, но ее обслуживание решено было передать в домен ALD Pro, то администратор сможет создать эту зону, не дожидаясь когда она будет удалена в настройках родительской зоны company.ru.
   - Оптимизировали поиск в поле «Имя компьютера». При большом количестве хостов в домене нужную запись можно быстро найти по фрагменту имени, поиск работает со строками от 3 символов.
   - Тексты этих сообщений были локализованы и приведены к единому формату для лучшего восприятия сообщений об ошибках.

Выполнен ряд доработок в часть информационной безопасности.

6. **Разработаны методические рекомендации по безопасной настройке ALD Pro.** Подготовлены методические рекомендации по безопасной настройке программного комплекса «ALD Pro», которые включают:
   - Перечень параметров, влияющих на безопасность (hardening, аудит, права, службы и т. д.).
   - Рекомендуемые значения этих параметров.
   - Обоснование предлагаемых значений в аспекте защищённости системы.
7. **При установке подсистемы общего доступа к файлам взаимодействие с LDAP-сервером осуществляется теперь по шифрованному каналу связи с использованием StartTLS, что снижает риск компрометации учетных данных**.
8. **Реализовано предупреждение о переполнении диска, выделенного для хранения локальных журналов регистрации событий ИБ, и возможность настройки порогового значения для получения указанного предупреждения.**

В рамках расширения возможностей ALD Pro реализовано отслеживание каталога /var/log, в котором хранятся системные и прикладные файлы журналов регистрации событий, включая данные об информационной безопасности. Этот каталог является ключевым для сбора и анализа логов, необходимых для аудита и оперативного реагирования на инциденты.

При достижении заданного процента заполнения объема памяти, выделенного для каталога /var/log, система автоматически формирует соответствующие оповещения, которые администратор получает в журнале событий мониторинга. Это позволяет предотвращать потерю важных событий из-за переполнения дискового пространства. Внедрение данного механизма повышает надежность и управляемость системы, обеспечивая контроль за ресурсами хранения.

9. **Реализован поиск входа и выхода пользователей и других событий на портале управления ALD Pro.**

   Дополнена документация, описывающая поиск событий авторизации и настройку их логирования на портале. В документации теперь явно указан файл логов, в который сохраняются события авторизации пользователей на портале (ранее предоставлялись общие рекомендации). Это позволяет более гибко настраивать логирование и реакцию на события безопасности, чтобы приоритизировать угрозы и значительно повысить эффективность управления рисками и реагирования на инцидент.

10. **Реализован контроль целостности компонентов ALD Pro с использованием утилиты astra-int-check.**

    Для обеспечения контроля целостности файлов ALD Pro в состав дистрибутива включен файл gostsums.txt со списком контрольных сумм для всех файлов, входящих в пакеты программ дистрибутива. Используя утилиту astra-int-check, можно вычислить контрольные суммы файлов ALD Pro и проверить соответствие полученных значений по эталону.

**Прочие доработки и исправления**

| # | Компонент | Описание улучшения |
|---|---|---|
| 1 | Подсистема “Мониторинг” | Исправлена ошибка назначения шаблона мониторинга GC, при которой на КД, на котором не развернута подсистема GC, назначался шаблон мониторинга GC, что приводило к сообщению об ошибке в журнале событий мониторинга (не активность globalcatalog и ipa-gcsyncd). |
| 2 | Подсистема «Мониторинг» | Ограничен доступ к конфигурационным файлам Zabbix с цель усиления защищенности от возможных атак на инфраструктуру компании. |
| 3 | Глобальный каталог, Подсистема "Мониторинг" | Триггеры на мониторинг глобального каталога были настроены неверно. Из-за этого выдавалось предупреждение, когда ошибок целостности ГК - 0 и когда ошибок целостости ГК > 1. Исправлено, теперь предупреждение выдается при количестве ошибок целостности ГК > 0. |
| 4 | Подсистема "Портал управления" | Путём добавления ограничения времени выполнения запроса, решена проблема неработоспособности портала управления при удаленном подключении к компьютеру |
| 5 | Подсистема "Портал управления" | OTP теперь доступен как второй фактор аутентификации: пользователи могут входить в систему, вводя основной пароль вместе с одноразовым кодом, что повышает безопасность учётных записей и снижает риск несанкционированного доступа |
| 6 | Установка, обновление и настройки подсистем | Исправлена ошибка в описании утилиты aldpro-server-install: указан обязательный ключ --ip и подкорректировано его описание. |
| 7 | Установка, обновление и настройки подсистем | Исправлены ошибки установки КД при IP-адресе с различными масками подсети, доработаны проверки наличия корректной обратной DNS-зоны. |
| 8 | Установка, обновление и настройки подсистем | Оптимизирован процесс обновления первого контроллера домена в части миграции данных при большом количестве пользователе |

| | | |
|---|---|---|
| 9 | Компонент 389DS | Устранена необходимость в ручной индексации атрибута ipaExternalMember в LDAP при развертывании КД |
| 10 | Компонент 389DS | Добавлена автоматическая индексация атрибута ipaExternalMember в LDAP при развертывании контроллеров домена (основного и резервных). Теперь пользователям не придётся вручную выполнять процедуру на каждом КД. |
| 11 | Компонент 389DS | Устранено дублирование изменений в LDAP-каталоге плагином watch_rbtadp при репликации. В результате повысилась скорость работы системы в кейсах, связанных с изменением атрибута rbtadp, и увеличилась отказоустойчивость 389ds при работе с каталогами, содержащими большое количество объектов, связанных с подразделениями. |
| 12 | Гранулярное управление доступом | Исправлена ошибка, возникающая при удалении вложенной группы из родительской, на которую назначена роль главного администратора домена. Ошибка возникала в ситуации, когда в результате удаления дочерней группы роль главного администратора оказывалась не назначена ни на одну активную учетную запись пользователя в домене. |
| 13 | Гранулярное управление доступом | Исправлена ошибка в работе роли ALDPRO - Software Update Policies Administrators, при которой привилегия Update Policies Computers - Manage не могла быть ограничена подразделением. |
| 14 | Гранулярное управление доступом, Политики паролей | Исправлена проблема, когда у пользователя есть права на чтение данных политик паролей, но в портале управления и в API выдавалась ошибка об отсутствии прав. |
| 15 | Механизмы групповых политик | Обновлена справка для параметра компьютера “Система -> Вход в систему -> Дополнительно”. |
| 16 | Механизмы групповых политик, Подсистема "Портал управления" | Исправлено поведение при открытии справки: введённые атрибуты параметров больше не сбрасываются. Теперь работа с параметрами на портале управления стала значительно удобнее и |

| | | |
|---|---|---|
| | | быстрее. |
| 17 | Служба синхронизации времени | Добавлена поддержка указания внешних NTP-серверов по IP-адресу и по любым доменным именам (включая имена с произвольными латинскими словами, например .test). Это расширяет сценарии использования и делает настройку времени более гибкой и удобной. |
| 18 | Модуль синхронизации | Доработана синхронизация атрибута telephoneNumber (номера телефонов пользователей). Выполнен ряд доработок для повышения удобства работы администраторов с файлами логов модуля синхронизации. |
| 19 | Компонент BIND9 | Разработана инструкция по настройке ограничений внешнего трафика от пакета BIND9 с целью исключения неконтролируемых сетевых взаимодействий и соблюдения современных стандартов информационной безопасности и повышенных требований к надежности и предсказуемости работы программного продукта |

**Изменения в документации**

| # | Компонент | Тема |
|---|---|---|
| 1 | Подсистема установки, настройки и обновления подсистем | Руководство администратора часть 1. Добавлены общие требования к обновлению ALD Pro и типовые сценарии обновления |
| 2 | Подсистема установки, настройки и обновления подсистем | Из раздела 4 «Известные проблемы» руководства администратора, часть 2, удален подраздел «Решение проблемы медленного монтирования» в виду решения данной проблемы |
| 3 | Подсистема установки, настройки и обновления подсистем | В матрицу совместимости руководства администратора,<br>часть 1, добавлено предупреждение о невозможности обновления |
| 4 | Подсистема установки, настройки и обновления подсистем | В матрице совместимости руководства администратора,<br>часть 1, отмечены все LTS-версии (Long-Term Support) |
| 5 | Подсистема установки, настройки и обновления подсистем | В руководстве администратора, часть2, в разделе «Настройка подсистем» добавлена информация об аутентификации с использованием OTP. |
| 6 | Подсистема установки, настройки и обновления подсистем | В руководство администратора, часть 1, добавлена информация о средстве контроля соответствия дистрибутиву |
| 7 | Механизмы групповых политик | В руководстве администратора, часть2, в подразделе «Групповые политика» раздела «Портал управления. Настройка и работа» добавлена информация об особенностях работы с дополнительными параметрами групповых политики — параметрами, созданными пользователями |
| 8 | Доверительные отношения | Переработана полезная инструкция «Доверительные отношения» в части настройки RPC-сервера. Также добавлена информация о том, что установка глобального каталога необходима при установке любых доверительных отношений |
| 9 | Словарь паролей | В справочных материалах руководства администратора, часть 2, обновлена информация о создании политики паролей с помощью утилиты ipa pwpolicy-add |
| 10 | Подсистема «Журналирование | В справочных материалах руководства |

| | | |
|---|---|---|
| | событий» | администратора, часть 2, инструкция о настройке журналирования событий дополнена информацией о входе/выходе web aldpro |
| 11 | Служба разрешенных имен | В руководстве администратора, часть 2, в разделе «Портал управления. Настройка и работа» в подразделе «Роли и службы сайта / Служба разрешения имен / Новая зона DNS» при создании зоны DNS добавлено описание параметра «Пропустить проверку пересечения» с чексбоксом и подсказкой «DNS-зона будет создана принудительно, даже если она будет пересекаться с существующей зоной» |
| 12 | Подсистема «Портал управления» | В руководстве администратора, часть 2, в разделе «Портал управления. Настройка и работа» при развертывании нового сервера добавлена информация о выборе хоста |
| 13 | Дополнительная документация | Добавлена новая инструкция по настройке мониторинга заполнения каталога /var/log/ |
| 14 | Дополнительная документация | Разработан новый документ Redbook, включающий в себя методические рекомендации по безопасной настройке программного комплекса ALD Pro, безопасный обмен данными с применением SSL/TLS, инструкцию по обеспечению безопасной работы в домене ALD Pro: правила HBAC, инструкцию по повышению привилегий доменных пользователей с помощью правил SUDO, инструкцию по обеспечению безопасной работы в домене ALD Pro: политики паролей |
| 15 | Дополнительная документация | Добавлена новая инструкция по замене и блокировке учетных записей |