

ИМПОРТОЗАМЕЩЕНИЕ СЛУЖБЫ КАТАЛОГОВ: МИГРАЦИЯ С MICROSOFT ACTIVE DIRECTORY НА ALD PRO

Елизаров Д.А., к.т.н., доцент

Дубляженко В.Д., студент

Филатова А.А., студент

Омский государственный университет путей сообщения, г. Омск, Россия

Аннотация. Миграции с Microsoft Active Directory на ALD Pro – это ключевой этап импортозамещения ИТ-инфраструктуры, позволяющий перейти на отечественное решение для управления доменами. Целью миграции является обеспечение технологической независимости и соответствие нормативным требованиям регуляторов.

Ключевые слова: миграция, домен, служба каталогов, ALD Pro, Active Directory.

В условиях постоянного развития информационных технологий и повышения требований к защите данных, перед организациями все острее встает задача эффективного управления учетными записями пользователей и обеспечения строгого контроля доступа. В современных реалиях особую важность приобретает переход на отечественное программное обеспечение, что позволяет не только соответствовать нормативным требованиям регуляторов, но и повысить уровень информационной безопасности, обеспечивая полный контроль над используемыми технологиями и данными. Импортозамещение службы каталогов является ключевым этапом перехода организации на суверенную ИТ-инфраструктуру. Ранее для этих целей широко использовалась система Microsoft Active Directory (MS AD) – мощный инструмент централизованного управления пользователями и сетевыми ресурсами. В настоящее время многие компании задумываются над миграцией в инфраструктуру Linux и вместо MS AD планируют использовать службу

каталога с открытым исходным кодом FreeIPA или более функциональные решения на ее основе [1].

Согласно рейтингу CnewsMarket на 2025 год, российская служба каталога корпоративного класса ALD Pro «Группы Астра» заняла лидирующую позицию [2]. Рейтинг включил отечественные решения для управления доступами, компьютерами и пользователями и учитывает функциональность, интеграции, кибербезопасность и поддержку продукта.

ALD Pro предоставляет расширенные возможности по управлению учетными записями, централизованному контролю прав доступа, а также поддерживает интеграцию как с Linux-, так и с Windows-средами [3]. Удобный интерфейс и функциональная гибкость делают ALD Pro оптимальным выбором для организаций, стремящихся к цифровой независимости.

В статье описаны этапы перехода от службы каталога MS AD на отечественное решение ALD Pro [4, 5]. При реализации миграции с MS AD на ALD Pro использовались следующие конфигурации:

- контроллер домена ALD Pro, выбрана операционная система Astra Linux SE 1.8 в релизе «Смоленск» (IP-адрес – 10.0.2.28);

- контроллер домена Microsoft Active Directory выбрана операционная системы Windows Server 2016 (IP-адрес – 10.0.2.27/24, имя компьютера - wsdhc).

Первоначально требуется развернуть новую инфраструктуру. Перед установкой ALD Pro на Astra Linux SE необходимо отключить службу NetworkManager (используется для управления сетевыми соединениями). Для отключения нужно выполнить следующие команды:

```
sudo systemctl stop NetworkManager.service
```

```
sudo systemctl disable NetworkManager.service
```

```
sudo systemctl mask NetworkManager.service
```

Далее требуется настроить статический IP-адрес и шлюз по умолчанию.

После обновления источников репозиториев можно приступить к установке ALD Pro. Далее следует настроить систему Astra Linux как контроллер домена ALD Pro с помощью следующей команды

```
sudo aldpro-server-install -d al.cfd.loc -n aldfc -p "password" -ip 10.0.2.28 -  
setup_syncer -setup_gc -no-reboot.
```

Для проверки правильности установки и первичной настройки ALD Pro можно использовать команду `sudo ipactl status`, которая подтверждает запуск необходимых служб.

После перезапуска система в форме входа появился выбор: войти в домен или войти в компьютер (рисунок 1).

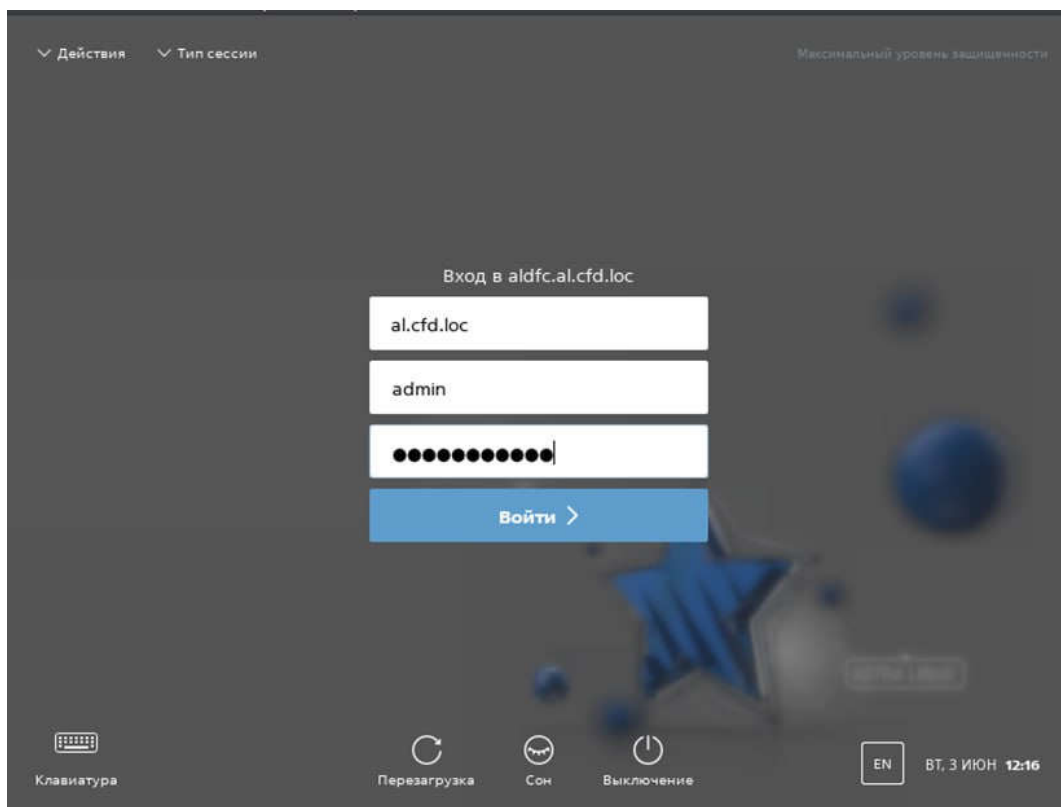


Рисунок 1 – Вход в систему

Следующий шаг – настройка ALD Pro. Панель администратора ALD Pro – это основной интерфейс для управления доменной инфраструктурой. Через нее настраиваются пользователи, группы, политики безопасности и другие параметры домена. После установки ALD Pro администратор входит в систему под учетной записью `admin`, с паролем, введенным при развертывании. Без доступа к панели администратора дальнейшая настройка домена невозможна.

Далее нужно выполнить настройку сервиса DNS. Для этого в панели администратора следует выбрать раздел «Глобальная конфигурация DNS» и указать IP-адрес DNS-сервера Яндекса (77.88.8.8).

Синхронизация времени является важным аспектом миграции на ALD Pro. В доменной инфраструктуре важно, чтобы все серверы и клиенты имели одинаковое время, иначе может нарушиться работа протокола аутентификации Kerberos, могут возникнуть ошибки при входе в систему и синхронизация данных между серверами будет некорректной. Для синхронизации времени в ALD Pro используется служба chrony.

Также необходимо подготовить контроллер домена Microsoft. Для добавления условного переадресатора на DNS-сервер ALD Pro в командном интерпретаторе PowerShell следует ввести команду `Add-DnsServerConditionalForwarderZone -Name "al.dfc.loc" -ReplicationScope "Forest" -MasterServers 10.0.2.28` и задать новое делегирование `al.dfc.cf.d.loc.dfc.loc`.

После требуется выдать права администратора домена учетной записи пользователя, выполняющего обязанности администратора в организации, и выдать права делегирования на ту же учетную запись. Необходимо создать организационное подразделение (в нашем примере TrustedUsers) и перенести в него пользователей, которые будут мигрированы в ALD Pro. После нужно создать новую зону DNS.

Далее необходимо подготовить ALD Pro для установления доверительных отношений и миграции с MS AD. Для этого следует внести изменения в блоки `realms` и `domain_realm` файла `/etc/krb5.conf`, указав домен MS AD:

```
[realms]
AL.CFD.LOC = {
    kdc = al.dfc.al.cfd.loc:88
    master_kdc = al.dfc.al.cfd.loc:88
    admin_server = al.dfc.al.cfd.loc:749
    default_domain = al.cfd.loc
    pkinit_anchors = FILE:/var/lib/ipa-client/pki/kdc-ca-bundle.pem
    pkinit_pool = FILE:/var/lib/ipa-client/pki/ca-bundle.pem
}
```

```
DFC.LOC = {  
    kdc = wsdfc.dfc.loc  
    admin_server = wsdfc.dfc.loc  
}  
[domain_realm]  
.al.cfd.loc = AL.CFD.LOC  
al.cfd.loc = AL.CFD.LOC  
aldfc.al.cfd.loc = AL.CFD.LOC  
.dfc.loc = DFC.LOC  
dfc.loc = DFC.LOC  
wsdfc.dfc.loc = DFC.LOC
```

После предыдущих настроек требуется выдать Kerberos тикет пользователю в домене MS AD с правами администратора домена и правами делегирования (в нашем примере – petrovpp) с помощью команды `kinit petrovpp@dfc.loc`.

Далее следует подключиться к LDAP-серверу `wsdfc.dfc.loc` по порту 389 и выполнить поиск всех объектов класса `user` в пределах дерева `dc=dfc,dc=loc`, используя простую аутентификацию от имени пользователя Peter Petrov с помощью команды

```
sudo ldapsearch -x -H ldap://wsdfc.dfc.loc:389 -D "CN=Peter Petrov",OU=TrustedUsers,DC=dfc,DC=loc -W -b "dc=dfc, dc=loc" "(objectClass=user)".
```

На заключительном этапе нужно настроить доверительные отношения и миграцию. В административной панели ALD Pro по пути «Управление доменом» -> «Интеграция с MS AD» -> «Новое подключение» требуется ввести домен `dfc.loc` (домен MS AD), установив флажки доверительные отношения и двусторонние доверительные отношения и указав данные учетной записи для доверительных отношений (в нашем примере – petrovpp). Запуск миграции производится на вкладке «Управление доменом» -> «Интеграция с MS AD» -> «Подключение: `dfc.loc`» -> «Новый запуск миграции».

После миграции на вкладке «Пользователи» в административной панели кроме пользователей, созданных в домене ALD Pro, после миграции отображаются также перенесенные пользователи из MS AD (рисунок 2).

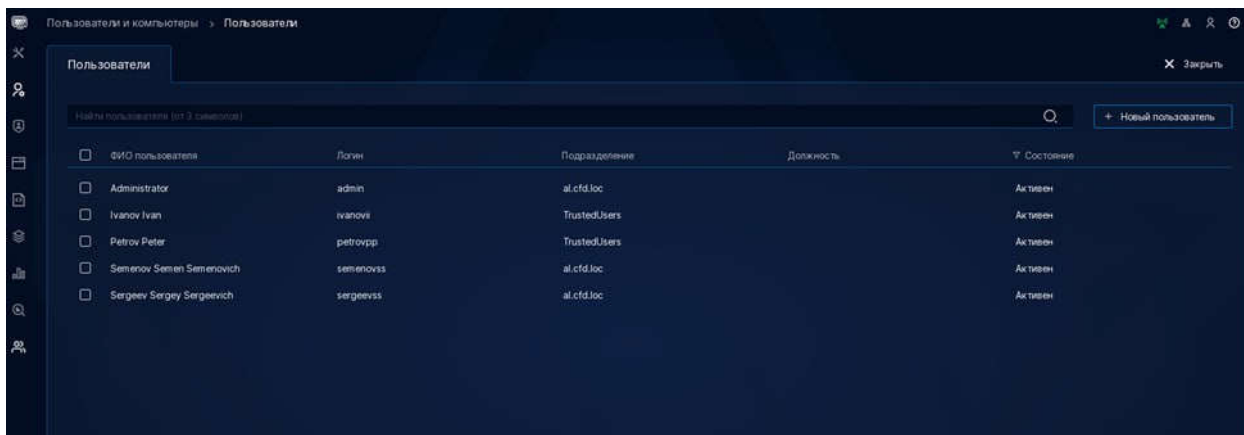


Рисунок 2 – Пользователи в ALD Pro после миграции

Для проверки проведенных настроек можно также выполнить вход в учетную запись пользователя MS AD через рабочую станцию Astra Linux (рисунок 3). Успешный вход подтверждает завершение процедуры миграции.

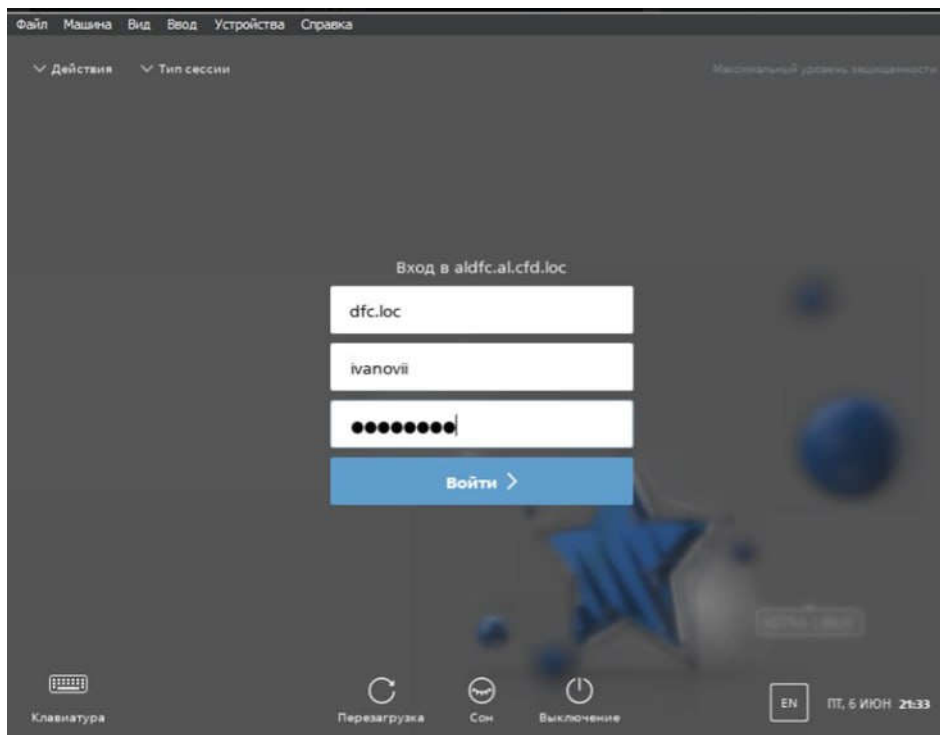


Рисунок 3 – Вход в учетную запись пользователя MS AD через рабочую станцию Astra Linux

Литература

1. Обзор рынка российских служб каталогов. – URL: anti-malware.ru/analytics/Market_Analysis/Russian-Directory-Service (дата обращения: 12.05.2026).
2. Российские службы каталогов 2025. – URL: cnews.ru/projects/2025/catalogs2025 (дата обращения: 12.05.2026).
3. ALD Pro – программный комплекс для централизованного управления объектами, доменом организации, службой каталогов. – URL: astra.ru/software-services/application-software-astra-group/ald-pro/ (дата обращения: 12.05.2026).
4. Модуль 3. Базовые функции и настройка ALD Pro — документация Курс по службе каталога ALD Pro 3.1.0. – URL: aldpro.ru/professional/ALD_Pro_Module_03/ALD_Pro_basic_functionality_and_setup.html (дата обращения: 12.05.2026).
5. Администрирование ald домена на Astra Linux / Хабр [Электронный ресурс] . – URL: habr.com/ru/articles/688842/ (дата обращения: 12.05.2026).