

Готовые полезные инструкции ▪ Инструкция по работе двусторонних доверительных отношений

ALD Pro

Exported on 08/14/2023

Table of Contents

1	Введение	3
2	Как работали доверительные отношения MS AD и ALD Pro ранее	4
2.1	Проблема доверия MS AD с ALD Pro.....	4
3	Как работают теперь	5
3.1	Технические требования	5
3.2	Глобальный каталог.....	5
4	Настройка двусторонних доверительных отношений	6
4.1	Настройка и проверка перенаправления DNS ALD Pro.....	6
4.1.1	Настройка ALD Pro.....	6
4.1.2	Настройка MS AD	6
4.2	Установление двусторонних доверительных отношений между доменами.....	6
4.3	Отключение FAST аутентификации	7
4.4	Проверка двусторонних доверительных отношений	7
4.4.1	Авторизация на компьютере домена MS AD.....	7
4.4.2	Авторизация на компьютере домена ALD Pro	7
4.4.3	Создание общей папки	7
5	Заключение.....	9

1 Введение

Для удобства администрирования в организации может быть несколько доменов.

Например, домен MS AD и домен ALD Pro. В домене MS AD будут находиться 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.local). Для непрерывной 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.

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.

2.1 Проблема доверия MS AD с 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 Как работают теперь

3.1 Технические требования

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.

3.2 Глобальный каталог

Глобальный каталог устанавливается на сервер домена при обновлении и при разворачивании нового контролера домена.

4 Настройка двусторонних доверительных отношений

4.1 Настройка и проверка перенаправления DNS ALD Pro

Для работы доверительных отношений с компьютеров из домена ALD.company.local должны разрешаться имена компьютеров из домена WIN.company.local и наоборот, нужно сделать взаимное перенаправление DNS-зон.

4.1.1 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

Аналогично можно настроить из Управление доменом -> Интеграция с MS AD.

4.1.2 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:"

4.2 Установление двусторонних доверительных отношений между доменами

Создать двусторонние отношения доверия можно на вкладке портала управления ALD Pro **Управление доменом** → **Доверительные отношения**.

Необходимо настроить двусторонние доверительные отношения с сервером MS AD.

Чекбокс **Доверительные отношения** активен и доступен для изменения.

Заполнить поля формы для установки двусторонних доверительных отношений корректными данными:

- "Учетная запись для доверительных отношений" - учетная запись MS AD.
- "Пароль пользователя" и "Подтверждение пароля" - пароль учетной записи MS AD.

Нажать на кнопку сохранения и подтвердить операцию.

С указанным MS AD успешно настроены двусторонние доверительные отношения. Отображено соответствующее уведомление. Администратор остается в карточке добавленного подключения. Чекбокс **Двусторонние доверительные отношения** активен, но недоступен для изменения - после установки доверительных отношений изменить тип отношений нельзя.

В разделе **Пользователи и компьютеры** -> **Группы пользователей** необходимо убедиться, что отображены две добавленные группы администраторов для **MS AD**, которые были автоматически добавлены при установлении доверительных отношений.

В разделе **Роли и службы сайта** -> **Служба разрешения имен** -> **Вкладка "Перенаправление запросов"** необходимо убедиться, что таблица содержит зону перенаправления для **MS AD**, которая была добавлена автоматически при установлении доверительных отношений.

В разделе **Управление доменом** -> **Интеграция с MS AD** убедиться, что таблица содержит подключение MS AD. В столбце **Доверительные отношения** отображено значение **Двусторонние**.

4.3 Отключение FAST аутентификации

Для доступа к ресурсам windows с аутентификацией по kerberos (IIS, 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** → **FAST аутентификация**. Выставить параметр never.

ВАЖНО! Установка этого параметра понижает безопасность.

При первом применении может понадобиться перезагрузка сервиса sssd.

4.4 Проверка двусторонних доверительных отношений

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.

4.4.1 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.

4.4.2 Авторизация на компьютере домена ALD Pro

Необходимо 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.

4.4.3 Создание общей папки

а) 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 Properties\Sharing\Advanced Settings\Permissions** 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 Properties\Security**. Можно предоставить доступ к общей папке всем аутентифицированным пользователям.

В результате пользователи ALD Pro могут редактировать файлы, находящиеся в папке **Common**.

б) 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 компьютера в домене MS AD, который не является контроллером домена>/Common
```

В результате пользователи MS AD могут редактировать файлы, находящиеся в папке **Common**.

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.