Проблемы с авторизацией

⚠ Обновление: Архива v2.5 (или выше) обладает исправленной системой авторизации, которая вместо Kereberos использует NTLM v2 аутентификацию. Как часть процесса обновления предыдущих версий (таких как v2.3, v2.1, v2.0, OSE и других), настройки Active Directory прежних версий продукта должны быть переустановлены. Для более подробной информации смотрите Авторизацию.

Выберите ваш механизм авторизации:

- Авторизация Active Directory через NTLM - Используется последними версиями Архива для авторизации в MS Exchange.
- LDAP авторизация - авторизация через сервер LDAP, например, такой как OpenLDAP.
- Авторизация Active Directory через Kerberos - Используется ранними версиями Архива для авторизации в MS Exchange.

Авторизация Active Directory через NTLM (Архива v2.2 или выше)

⚠ NTLM SSO: со всеми проблемами, связанными с ошибкой NTLM аутентификации, обращайтесь к разделу Ошибка NTLM авторизации.

⚠ Подготовка: прежде чем начать, убедитесь, что вы точно следовали всем шагам настройки конфигурации AD в разделе Авторизация. В особенности, вы должны были запустить скрипт ADSetupWizard.vbs. Этот скрипт создает требуемый аккаунт компьютера в Active Directory. Более того, он устанавливает пароль, выбранный вами, для этого аккаунта.

Обычные настройки Active Directory

Типичные настройки вы найдете во вкладке Настройка -> Авторизация:

> DNS сервер: отмечено галочкой (если устанавливается интернет-соединение, то галочки не должно быть)
> Выполнять DNS запросы серверов: отмечено галочкой.
> DNS сервер IP адрес: 192.168.0.1 (Замечание: Это IP-адрес вашего DNS-сервера)
> DNS сайт: (оставьте незаполненным)
> Bind DN: DC=company,DC=local (Замечание: написание DC заглавными буквами)
> Логин на чтение LDAP: service$@company.local (Замечание: учетная запись компьютера (она же сервисная) должна быть создана в Active Directory).
> Active Directory Сервер Адреса: activedirectory.company.local (Замечание: здесь должно быть указано полное доменное имя. Если это не работает, попробуйте company.local) (НЕ вводите сюда IP-адрес!!!)
> Bind Attribute: SAMAccountName
> Email Attribute: proxyAddresses (если вы используете MS Exchange)
> Значение сообщения: SMTP:(.*) (если используете MS Exchange)
> UPN атрибут: userPrincipalName
> UPN Значение: (.*)
> NTLM SSO (единый пароль на вход) авторизация: Не отмечено галочкой(если отмечено, вы должны внимательно следовать шагам подготовки для NTLM-аутентификации)

Во вкладке Настройка -> Домены проверьте, что все домены введены правильно.

Следующие порты должны быть открыты на сервере Архива для Active Directory: 389 (LDAP), 445 (SMB) and 53 (DNS).

⚠ Замечание: при соединении с сервером AD через Интернет, обычно поле "DNS сервер" не должно быть отмечено галочкой. Когда это поле отмечено, DNS сервер будет возвращать внутренний IP-адрес по подсети, где находится AD-сервер. Это не желательно, если вы подключаетесь извне. Лучше просто указать IP-адрес AD сервера.

Роли не назначены

Ошибка: Пользователь прошёл авторизацию, но его роль не определена

Авторизация прошла успешно, хотя пользователю не присвоена определенная роль. Вам нужно назначить соответствующую роль в Active Directory.

Отсутствует LDAP атрибут при назначении роли

Ошибка: LDAP атрибут должен быть указан при назначении роли Active Directory

Вы назначили роль, в которой отсутствует атрибут LDAP. Необходимо заново назначить данную роль.

Неверный Bind атрибут

Ошибка: Авторизация пользователя невозможна: не найдена учетная запись

Отредактируйте файл server.conf, находящийся в C:\Program Files\MailArchiva\Server\webapps\ROOT\WEB-INF\conf\server.conf. Измените параметр "authentication.bind.attribute=UserPrincipalName" на "authentication.bind.attribute=sAMAccountName".

Убедитесь, что во вкладке Настройка -> Авторизация указан Bind атрибут "sAMAccountName".

Неверный DN

Ошибка: учетная запись [имя_пользователя] не была найдена в ldap репозитории.

DN, указанный во вкладке Настройка -> Авторизация, неверен. К примеру, он НЕ ДОЛЖЕН БЫТЬ следующим:

> DN=demo.local (.local неверная запись, вместо этого должно быть DN=demo, DN=local)

Ошибка: ошибка соединения с LDAP {javax.naming.NamingException: [LDAP: error code 1 - 000020D6: SvcErr: DSID-031007DB, problem 5012 (DIR_ERROR), data 0

Вы используете строчные буквы: dn вместо DN. Как это выглядит у вас:

dc=demo,dc=local (Неверно: DC должно быть написано заглавными буквами: DC=demo, DC=local)

Неверное имя учетной записи сервиса

Учетная запись сервиса должна быть записана в правильном формате. Предположим, что учетная запись сервиса - service, он НЕ МОЖЕТ БЫТЬ следующим:

> service
> service@company.local

Правильное значение: service$@company.local.

Обратите внимание, после имени учетной записи идёт знак доллара. Это обозначение учетной записи компьютера в AD. Если вы не знаете, что такое учетная запись компьютера или зачем она нужен, обратитесь в раздел Авторизация.

Сообщения не видны во время поиска

Убедитесь, что почтовый атрибут (Email Attribute) в Active Directory установлен верно. Если вы используете MS Exchange, в поле атрибута во вкладке Настройки -> Авторизация должно быть задано значение "proxyAddresses". Если вы используете другой почтовый сервер, может быть указано что-то другое, например, mail. В дополнение в качестве фильтра роли пользователя там может быть указано значение %email%.

Нет соединения с Active Directory

Следующие порты должны быть открыты на сервере Архива для Active Directory: 389 (LDAP), 445 (SMB) and 53 (DNS).

Если вы не уверены в этом, обратитесь с помощью Telnet к каждому порту от сервера Архива, чтобы подтвердить, что соединение может быть установлено.

NTLM SSO авторизация включена без предварительной подготовки

Ошибка: Если вы заходите в веб-интерфейс через бразуер, и браузер при этом начинает быстро переключаться между "определить разрешение экрана" и другой страницей.

В поле NTLM SSO (единый пароль на вход) авторизация во во вкладке Настройка -> Авторизация стоит галочка, без прохождения предварительно подготовкли для NTLM-авторизации. Или NTLM-авторизация должна быть отключена илил ваш браузен должен быть правильно настроен. Для получения дальнейших сведений, как решить эту проблему, обратитесь в раздел Ошибка NTLM авторизации. Или же отключите NTLM-авторизацию, как описано ниже:

Зайдите напряму на https://localhost:8090/signonform.do. Зайдите во вкладке Настройка -> Авторизация, и уберите галочку из поля "NTLM SSO авторизация" и нажмите "Сохранить".

Неверное имя сервера Active Directory

Во вкладке Настройка -> Авторизация необходимо указать полное доменное имя сервера Active Directory (например, activedirectory.company.name). Замечание: имя сервера должно быть действительным именем сервера AD, а не просто DNS-именем (если оно другое). Не вводите туда IP-адрес сервера!

Для проверки, пожалуйста, пропингуйте полное доменное имя сервера Active Directory, чтобы убедиться, что он доступен. Если нет, то имеет место проблема DNS.

Ошибка "Свойство не задано или не создано"

Ошибка "Свойство не задано или не создано" (англ. Property not set or constructed) может возникнуть, когда Архива не может установить соединение с DC во время авторизации AD.

Чтобы избавиться от этой ошибки, проверьте следующее:

- Убедитесь, что нужные нужные соединительные порты открыты между Архива и AD сервером.
- Записи прямого и обратного вызова для сервера Архива указаны в DNS настройщике на AD сервере.
- Сервер, на котором находится Архива имеет имя хоста, ip-адрес и полное доменное имя.

LDAP авторизация

Обычные настройки LDAP

Типичные настройки вы найдете во вкладке Настройка -> Авторизация:

> DNS сервер: отмечено галочкой (если устанавливается интернет-соединение, то галочки не должно быть)
> Выполнять DNS запросы серверов: отмечено галочкой.
> DNS сервер IP адрес: 192.168.0.1 (Замечание: Это IP-адрес вашего DNS-сервера)
> DNS сайт: (оставьте незаполненным)
> Адрес LDAP сервера: ldap.company.local(Замечание: здесь должно быть указано полное доменное имя. Если это не работает, попробуйте company.local)
> Bind DN: DC=company,DC=local (Замечание: написание DC заглавными буквами)
> Service DN: CN=Administrator,CN=Users,DC=company,DC=local.
> Bind Attribute: uid
> Email Attribute: mail
> Значение сообщения: (.*)
> UPN атрибут: userPrincipalName
> UPN Значение: (.*)
> NTLM SSO (единый пароль на вход) авторизация: Не отмечено галочкой(если отмечено, вы должны внимательно следовать шагам подготовки для NTLM-аутентификации)

Пользователь не найден из-за несовпадения UID

Архива не может найти логин пользователя, так как ваш uid не включает домен (к примеру, "@company.com"), а вы ошибочно указали по умолчанию логин с указанием домена. По умолчанию домен логина должен оставаться незаполненным (пустое поле), если ваш uid не включает в себя имя домена.

Авторизация Active Directory через Kerberos (v2.1 и более ранние версии, включая OSE)

⚠ Замечание: Следующие варианты решения проблем не подходят для Архива v2.5 и более новых версий.

Существует несколько причин, почему архивный сервер Архива не может авторизоваться с использованием Active Directory. Все они перечислены ниже:

Неверный домен в логине: krb Error 68

KDC_ERR_WRONG_REALM 68 Reserved for future use (зарезервировано для использования в будущем).

Неверный домен указан в учетной записи администратора или в учетной записи пользователя.
Решение: проверьте домен, указанный в учетной записи администратора (например, admin@business.local) или домен в учетной записи

пользователя (например, user@smallbusiness.local).

Отсутствует строка в файле hosts

Или ваш DNS неверно настроен, или же вы запустили Архива в тестовой среде. В этих случаях необходимо добавить в файл hosts, чтобы помочь Архива разрешить Active Directory использовать полные доменные имена (FQDN). Для Архива 2.0 и более поздних версий, вам понадобится кликнуть по кнопке Добавить хост (Add To Hosts), для того чтобы автоматически добавить ip-адрес в файл hosts. Для OSE и более ранних версий EE, файл hosts обновляется автоматически, но иногда что-то может пойти не так и в файл добвится больше строк, чем требуется, что приведет к ошибке авторизации. В этом случае:

1. Удалите все строчки, созданные Архива, в файле hosts.
2. Добавьте IP-адрес, полное доменное имя (FQDN) и имя сервера, на котором запущена Active Directory в файлах c:\windows\system32 \drivers\etc\hosts file (Windows) или \etc\hosts (Linux) .

Вам необходимо добавить следующую строку (включая написанное ЗАГЛАВНЫМИ БУКВАМИ) в файл hosts на компьюетере, где запущен сервер Архива.

192.168.0.100 ACTIVEDIRECTORY.COMPANY.LOCAL ACTIVEDIRECTORY

(Замечание: Пожалуйста, замените ACTIVEDIRECTORY.COMPANY.LOCAL действительным полным доменных именем вашего сервера Active Directory!!! Если вы этого не сделаете, то вы продожите получать ошибку Сервер не найдет (Server Not Found In Kerberos Database) в базе данных Kereberos. Эта ошибка появится только в файле debug.log).

Server Not Found In Kerberos Database

В вашем файле hosts вы должны заменить ACTIVEDIRECTORY.COMPANY.LOCAL действительным полным доменных именем вашего сервера Active Directory. К примеру, если ваш сервер называется AD01, а ваша компания HITECHINC, то ввести в файл hosts вам нужно такую строку:

192.168.0.100 HITECHINC.LOCAL AD01

В архивном сервере Архива, на экране Настройка укажите следующие настройки Active Directory:

Kerberos Server: ad01.hitechinc.local:88 LDAP Server Address: ad01.hitechinc.local:389

Важно, чтобы полное доменное имя контроллера AD соответствовало имени сервера, зарегистированного в Active Directory.

KDC и LDAP адреса должеы быть полными доменными именами.
Проверьте, что ваши KDC и LDAP адреса - это полные доменные имена (к примеру, activedirectory.company.com)
Не используйте сокращения или ip-дрес сервера.
При авторизации используйте полное доменное имя.
При авторизации используйте полную учетную запись пользователя, например, john@company.com, а не просто john.

Разное время установлено на AD контроллере и сервере Архива

На обеих машинах должно быть установлено одинаковое время.

Неверный пароль

Вы ввели неверный пароль при тестировании учётной записи.

Сервер не может установить связь с AD-контроллером

Переключитесь в режим командной строки DOS и попробуйте "попинговать" AD-сервер используя полное доменное имя, т.е. напечатайте следующее:
ping ACTIVEDIRECTORY.COMPANY.LOCAL

Брандмауэр или антивирус блокируют порты 88 и 389

Разрешите порты 88 и 389 в вашем брандмауэре (антивирусе). Так же хорошо отключить антивирус/брандмауэр во время тестирования (если у вас серьёзные проблемы).

Неверная база DN

Убедитесь, что вы используете правильную Базу DN (Base DN, отличительное имя расположения в AD, где Архива должны начать поиск). Кавычки не требуются. Используйте: DC=company, DC=com. Это не должно выглядеть сложнее.

Роли не назначены

Не забудьте назначить роль для тестовой учетной записи пользователя. Если ни одна роль не назначена, вы не сможете пройти пробную авторизацию для этого пользователя.

Данный тип шифрования не поддерживается

При поптыке авторизации на сервере Windows 2008 вы можете получить сообщение "данный тип шифрования не поддерживается" (англ. no support for encryption type) или что-то похожее. Для того чтобы соблюсти обратную совместимость с более ранними версиями AD-контроллеров, для kerberos-авторизации Архива использует по умолчанию DES-шифрование. Оно не совместимо с Windows 2008 сервером, который по

умолчанию использует алгоритм шифрования AES.

Самый простой способ настроить Архива для авторизации - разрешить DES-аутентификацию в персональных учетных записях AD. В AD консоли выберите Свойства пользователя, выберите вкладку Учетная запись и там выберите "Use kerberos DES encryption types for this account" (рус. Использовать тип шифрования kerberos DES для данной учетной записи).

Другой способ - включить AES-шифрование в Архива, создав файл kr5.conf со следующим содержанием:

```
[libdefaults]

default_tkt_enctypes = aes256-cts

default_tgs_enctypes = aes256-cts

permitted_enctypes = aes256-cts
```

Сохраните файл krb5.conf в /usr/local/mailarchiva/server/webapps/mailarchiva/WEB-INF/conf (на Linux) или в c:\Program Files\MailArchiva\Server\webapps\mailarchiva\server\WEB-INF\conf (на Windows).

Решение сложных проблем Active Directory

1. Прежде всего перезагрузите сервер и попробуйте все приведенные выше инструкции ещё раз. Иногда для решения проблем с Kerberos требуется перезагрузка.
2. Остановите сервер.
3. Включите опцию Отладка (DEBUG) в Логах в ServerLog.
4. Запустите сервер из DOS-консоли (в Windows запустите следующий exe-файл: C:\Program Files\MailArchiva\Server\bin\MailArchivaServer.exe)
5. На экране Настроек (англ. Configuration Screen) в Email Discovery и Консоли администратора (англ. Administration Console) кликните по кнопке Test Login в настройках AD.
6. Просмотрите вывод консоли и логи отладки (информация о kerberos protocol handshake должна быть показана в выводе консоли).
7. Проверьте Jaas Kereberos Troubleshooting для решения ваших проблем.