Интеграция Гарант со службой каталога ALD Pro

06/10/2025

Содержание

Гарант – это информационно-правовая система для решения профессиональных задач юриста, бухгалтера, кадровика, специалиста по закупкам с актуальной информацией и широким функционалом для оперативного поиска и анализа материалов. Система устанавливается внутри предприятия и доступна пользователям из браузера по протоколу HTTP.

В настоящей инструкции описана процедура интеграции Гарант со службой каталога ALD Pro. Интеграция позволяет обеспечить прозрачную аутентификацию доменных пользователей по безопасному протоколу Kerberos V5. Для возможности централизованного управления лицензиями доступ к приложению получают только авторизованные пользователи, которые были включены в специальную доменную группу.

Авторизация Гарант в домене ALD Pro

ВНИМАНИЕ! В качестве примера будет использована тестовая конфигурация:

- пользователь ***garant-ldap*** для доступа к LDAP каталогу;

- группа ***garant-ldap-group;***

- имя домена: ***ald.company.lan;***

- полное имя сервера Гарант: **garant.ald.company.lan**.

Имена можно заменить на любые, соответствующие настройкам вашей сети. Данная инструкция описывает настройку доменной авторизации для Гарант, которая доступна по умолчанию на порту 8082.

Необходимые условия для реализации и условные обозначения

- Домен ALD Pro: **ALD.COMPANY.LAN**
- Сервер Гарант: 10.0.0.11 **server-name.ald.company.lan**
- Web-сайт Гарант**: http://garant.ald.company.lan:8082**
- Контроллер домена ALD Pro: 10.0.0.10 **dc-1.ald.company.lan**
- Рабочая станция пользователя: **client.ald.company.lan**
- Пользователь ALD Pro **admin**: Администратор домена **ALD.COMPANY.LAN**
- Пользователь ALD Pro **garant-ldap:** необходим для доступа сервиса Apache к LDAP каталогу
- Группа **garant-ldap-group**, разрешающая пользователям получать доступ к сайту **http:// garant. ald.company.lan:8082**
- Пользователи ALD Pro входящие в группу **garant-ldap-group**.

1 Предварительные настройки

Предварительные настройки выполняются только в случае, если сервер Гарант не был введен в домен. Если сервер в домене, можете переходить к пункту 2.

1.1 Настройки на контроллере домена **dc-1.ald.company.lan**

Создайте DNS-записи для сервера **server-name.ald.company.lan:**

```
$ sudo kinit admin
$ sudo ipa dnsrecord-add ald.company.lan garant --a-rec 10.0.0.11
```

, где

- kinit – получение Kerberos-билета для пользователя admin;
- ipa dnsrecord-add – создание в зоне ald.company.lan записи типа --a-rec для сервера server-name.

1.2 Настройки на сервере Гарант **garant.ald.company.lan**

1.2.1 Настройка DNS на сервере Гарант

Приложение Гарант использует домен только для аутентификации пользователей, поэтому оно не выполняет никаких запросов к другим хостам домена по DNS-именам. Однако при работе сервера в составе домена настоятельно рекомендуется в качестве DNS использовать один из контроллеров домена. Например, чтобы иметь возможность указывать FQDN-имена контроллеров для синхронизации времени.

Если на сервере не используются такие службы как resolvconf или network manager, достаточно напрямую отредактировать файл **resolv.conf**:

```
nameserver 10.0.0.10
search ald.company.lan
```

1.2.2 Настройка синхронизации времени

Для корректной работы Kerberos-аутентификации системное время на сервере Гарант и рабочих станциях может расходиться не более, чем на +/- 5 минут. Вы можете синхронизировать время вручную, но при работе сервера в составе домена настоятельно рекомендуется использовать автоматическую синхронизацию времени, например, с помощью службы chrony.

Для настройки chrony требуется внести следующие изменения в файл chrony.conf:

```
$ sudo mc /etc/chrony/chrony.conf
```

Далее добавьте следующую строку:

```
server dc-1.ald.company.lan iburst
```

2 Настройки на контроллере домена **dc-1.ald.company.lan**

Сначала необходимо инициализировать пользователя **admin**, ввести его пароль:

```
$ sudo kinit admin
```

Далее создаем службу и выгружаем ее ключ в файл.

При обращении клиентов к серверу Гарант в домене ALD.COMPANY.LAN на хосте garant.ald.company.lan с аутентификацией по Kerberos им нужно предъявить свой билет на имя Kerberos принципала HTTP/garant.ald.company.lan@ALD.COMPANY.LAN.

Для того, чтобы KDC смог выдать такой билет, в домене должна существовать такая служебная учетная запись, а для того, чтобы сервер Гарант смог проверять такие билеты, ему должен быть доступен keytab-файл с паролем от этой учетной записи.

Создавать служебную учетную запись можно как из командной строки, так и через веб-интерфейс.

Чтобы создать учетную запись из командной строки, воспользуйтесь командой service-add:

```
$ sudo ipa service-add HTTP/garant.ald.company.lan@ALD.COMPANY.LAN
```

Результат выполнения команды выглядит следующим образом:

```
#-----------------------------------
Добавлена служба "HTTP/garant.ald.company.lan@ALD.COMPANY.LAN"
----------------------------------------------------------------
Имя учётной записи: HTTP/garant.ald.company.lan@ALD.COMPANY.LAN
Псевдоним учётной записи: HTTP/garant.ald.company.lan@ALD.COMPANY.LAN
#-----------------------------------
```

Создать служебную учетную запись через веб-интерфейс ALD Pro можно на странице «Управление доменом > Службы и параметры Kerberos».

Чтобы сервер Гарант мог выполнять аутентификацию пользователей, т.е. расшифровать их сервисные билеты (TGS), ему необходимо предоставить keytab-файл с паролем от учетной записи службы. Сделать это можно только из командной строки с помощью утилиты ipa-getkeytab:

```
$ sudo ipa-getkeytab -p HTTP/garant.ald.company.lan@ALD.COMPANY.LAN -k /tmp/
http.keytab
```

Результат выполнения команды выглядит следующим образом:

```
#-----------------------------------

Таблица ключей успешно получена и сохранена в: /tmp/http.keytab

#-----------------------------------
```

3 Настройка на web-сервере Гарант **garant.ald.company.lan**.

Сначала добавьте пакеты для отладки из дистрибутива Astra Linux:

```
$ sudo apt-get -y install ldap-utils krb5-user libapache2-mod-auth-gssapi
```

Далее активируйте необходимые модули apache2:

```
$ sudo a2enmod auth_basic
$ sudo a2enmod authn_core
$ sudo a2enmod authn_file
$ sudo a2enmod authnz_ldap
$ sudo a2enmod authz_core
$ sudo a2enmod authz_host
$ sudo a2enmod authz_user
$ sudo a2enmod access_compat
$ sudo a2enmod auth_gssapi
$ sudo a2enmod headers
$ sudo a2enmod rewrite
$ sudo a2enmod proxy_balancer
$ sudo a2enmod proxy
$ sudo a2enmod proxy_http
$ sudo a2enmod slotmem_shm
```

Примечание

Модули находятся здесь в файле /etc/apache2/mods-available

Скопируйте ключ, сформированный ранее на контроллере домена **dc-1.ald.company.lan /tmp/http.keytab**, на сервер Гарант garant в директорию **/etc/apache2/.**

Измените права доступа на файл с ключом:

```
$ sudo chown www-data /etc/apache2/http.keytab
$ sudo chmod 644 /etc/apache2/http.keytab
```

Добавьте настройки для работы apache с ALD Pro в конфигурационный файл сайта: **/etc/apache2/sites-enabled/online.conf**.

Запись производится после указания корневой директории онлайн-версии, то есть после секции </Directory> :

```
<Location / >
AuthType GSSAPI
AuthName "Gssapi authenticated intranet ALD Pro"
```

```
GssapiAllowedMech krb5
GssapiCredStore keytab:/etc/apache2/http.keytab
GssapiLocalName On
GssapiBasicAuth On
AuthLDAPURL "ldap://dc-1.ald.company.lan/
cn=users,cn=accounts,dc=ald,dc=company,dc=lan?uid?sub?(objectClass=person)"
AuthLDAPBindDN "uid=garant-ldap,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"

AuthLDAPBindPassword "********"

# Require valid-user
<LIMIT GET POST PUT>
    Require ldap-group cn=garant-ldap,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
  </LIMIT>
  RewriteEngine On
  RewriteRule .* - [E=PROXY_USER:%{LA-U:REMOTE_USER}] # note mod_rewrite's lookahead
option
  RequestHeader set X-Logon-User "%{PROXY_USER}e"
</Location>

ProxyPass "/" "http://localhost:8082/"
ProxyPassReverse "/"  "http://localhost:8082/"
```

, где

GssapiAllowedMech krb5 – указывает, что в качестве механизма аутентификации GSSAPI должен использоваться Kerberos версии 5. Если этот параметр убрать, то система сама будет выбирать протокол в зависимости от того, что поддерживает удаленная система, например, NTLM, который считается менее безопасным;

GssapiBasicAuth On – включает механизм Basic-аутентификации, который позволяет пользователям вводить свои учетные данные (имя пользователя и пароль) в качестве альтернативного способа аутентификации;

GssapiCredStore – указывает путь к keytab-файлу, который содержит ключ для аутентификации Kerberos;

GssapiLocalName On – этот параметр говорит, что подключаемому пользователю необходимо удалить доменный суффикс. Например, если подключается пользователь admin@ALD.COMPANY.LAN, то GSSAPI отсечет @ALD.COMPANY.LAN и получит на выходе только admin. Делается это для того, чтобы ниже в строке **AuthLDAPURL** система смогла найти пользователя по атрибуту uid, так как там хранится учетная запись в коротком виде. Вы можете выключить параметр **GssapiLocalName**, в этом случае доменный суффикс сохраняется и вам потребуется искать по атрибуту krbPrincipalName;

AuthLDAPURL – параметр записывается в одну строку и задает адрес LDAP-каталога ldap://dc-1.ald.company.lan и протокол ldap или ldaps, далее указываем базу, где будет поиск пользователя, cn=users,cn=accounts,dc=ald,dc=company,dc=lan, uid - атрибут, значение которого будет сравниваться с пользователем, sub означает, что поиск будет происходить во всех вложенных подразделениях (OU), objectClass=person означает, что только объекты такого класса будут отфильтровываться;

AuthLDAPBindDN – пользователь, который имеет доступ к чтению LDAP-каталога;

AuthLDAPBindPassword – пароль пользователя AuthLDAPBindDN;

Require ldap-group – указывает, что пользователям, прошедшим аутентификацию, будет предоставлен доступ, если они включены в доменную группу garant-ldap-group по спецификации каталога X.500, которая определяет узлы в каталоге LDAP:

CN = Common Name,

OU = Organizational Unit,

DC = Domain Component;

RewriteEngine – параметр включает модуль, который позволяет переписывать URL-адреса;

RewriteRule – правило, согласно которому будет изменяться URL, в нашем случае:

(`.*`) - оно сопоставляет любой шаблон URL;

(`-`) - не выполняет никаких действий с ним;

(`[E=PROXY_USER:%{LA-U:REMOTE_USER}]`:) - это флаг, который устанавливает переменную окружения;

(`E=PROXY_USER`:) - устанавливает имя переменной как `PROXY_USER`;

(`%{LA-U:REMOTE_USER}`:) - параметр использует утверждение предпросмотра (`LA-U` - lookahead assertion) для захвата переменной `REMOTE_USER` (которая содержит имя пользователя удаленного пользователя), не переписывая сам URL-адрес;

RequestHeader – параметр устанавливает новый заголовок запроса с именем `X-Logon-User` со значением полученного имени пользователя из переменной окружения `PROXY_USER`;

ProxyPass - параметр означает, что при обращении на корневую страницу Apache "/", произойдет переадресация на страницу гарант http://localhost:8082/;

ProxyPassReverse - параметр означает, что ответ от Гарант http://localhost:8082/ будет переадресован на страницу Apache "/".

Для включения доступа всем доменным пользователям к ресурсу Гарант без группы, вместо блока <LIMIT GET POST PUT> используется директива <Require valid-user>.

Для включения защищенного режима передачи данных с LDAP-каталогом можно настроить SSL-соединения.

В случае, если сервер Гарант введен в домен, то достаточно в параметре AuthLDAPURL "ldap://dc-1.ald.company.lan..... заменить ldap на ldaps:

```
AuthLDAPURL "ldaps://dc-1.ald.company.lan/
cn=users,cn=accounts,dc=ald,dc=company,dc=lan?uid?sub?(objectClass=person)"
```

В этом случае будет устанавливаться SSL-соединение по порту 636, вместо 389.

Если вы хотите использовать порт 389, но при этом защитить соединение, то можно воспользоваться протоколом STARTTLS. Для его активации в конце строчки **AuthLDAPURL** нужно добавить TLS:

```
AuthLDAPURL "ldap://dc-1.ald.company.lan/
cn=users,cn=accounts,dc=ald,dc=company,dc=lan?uid?sub?(objectClass=person)" TLS
```

В случае, если сервер не в домене, то вам понадобится сертификат скопировать на сервер Гарант и добавить глобальный параметр в настройку Apache. Чтобы получить корневой сертификат средствами браузера Firefox, следует выполнить несложные шаги:

1. Перейти на страницу портала управления контроллером домена ALD Pro https://dc-1.ald.company.lan.
2. Нажать сочетание клавиш **<CTRL+I>**.
3. В открывшемся окне **Информация о странице** перейти во вкладку **Защита**.
4. Нажать кнопку **Просмотреть сертификат**. Откроется новая вкладка браузера со сведениями о сертификатах.
5. В открывшейся вкладке выбрать **CA Signing Certificate**.
6. В разделе **Разное** в строке **Загрузить** нажать на ссылку **PEM (сертификат)**.

Копируем полученный сертификат на сервер Гарант в каталог /etc/apache2.

Добавляем в настройки /etc/apache2/sites-enabled/online.conf следующий параметр:

```
LDAPTrustedGlobalCert CA_BASE64 /etc/apache2/dc-1-ald-company-lan.pem
```

Файл /etc/apache2/sites-enabled/online.conf будет выглядеть следующим образом:

```
LDAPTrustedGlobalCert CA_BASE64 /etc/apache2/dc-1-ald-company-lan_client.pem

<Location / >
AuthType GSSAPI
AuthName "Gssapi authenticated intranet ALD Pro"
GssapiAllowedMech krb5
GssapiCredStore keytab:/etc/apache2/http.keytab
GssapiLocalName On
GssapiBasicAuth On
AuthLDAPURL "ldap://dc-1.ald.company.lan/
cn=users,cn=accounts,dc=ald,dc=company,dc=lan?uid?sub?(objectClass=person)"
AuthLDAPBindDN "uid=garant-ldap,cn=users,cn=accounts,dc=ald,dc=company,dc=lan"

AuthLDAPBindPassword "********"

# Require valid-user
<LIMIT GET POST PUT>
    Require ldap-group cn=garant-ldap,cn=groups,cn=accounts,dc=ald,dc=company,dc=lan
  </LIMIT>
  RewriteEngine On
  RewriteRule .* - [E=PROXY_USER:%{LA-U:REMOTE_USER}] # note mod_rewrite's lookahead
option
  RequestHeader set X-Logon-User "%{PROXY_USER}e"
</Location>

ProxyPass "/" "http://localhost:8082/"
ProxyPassReverse "/"  "http://localhost:8082/"
```

Добавьте или скорректируйте параметры в основной конфигурационный файл apache2: **/etc/apache2/apache2.conf**:

```
KeepAlive On
LDAPSharedCacheSize 500
LDAPCacheEntries 1024
LDAPCacheTTL 60
LDAPOpCacheEntries 1024
LDAPOpCacheTTL 60
```

, где

KeepAlive – позволяет обслуживать несколько запросов по одному соединению, сокращая время, затрачиваемое на установление новых соединений TCP;

LDAPSharedCacheSize – устанавливает максимальный размер (в байтах) кэша для всех виртуальных хостов, использующих LDAP;

LDAPCacheEntries – определяет максимальное количество записей (например, пользователи, группы), которые могут быть сохранены в кэше для каждого виртуального хоста;

LDAPCacheTTL – устанавливает время жизни для кэшированных данных в секундах;

LDAPOpCacheEntries - устанавливает максимальное количество записей, которые могут быть сохранены в кэше для каждого виртуального хоста, содержащих результаты операций LDAP (поиск, добавление, изменение, удаление);

LDAPOpCacheTTL - устанавливает время жизни для кэшированных результатов операций LDAP в секундах.

Перезапустите Apache:

```
$ sudo systemctl restart apache2
```

3.1 Настройка Гарант

Добавьте следующие строчки в конец файла /usr/local/garant/intranet/web/config.py:

```
allow_login_by_header = True
is_proxima_disabled = True
```

, где

allow_login_by_header – разрешает аутентификацию пользователей по заголовкам HTTP-запроса, в нашем случае будет использоваться переменная X-Logon-User;

is_proxima_disabled – (необязательный параметр) принудительное использование локальной базы. Если параметр выключен (False), то Гарант будет автоматически, при наличии доступа в Интернет, переадресовывать на Интернет-версию, где база данных всегда актуализирована.

Перезагрузите сервисы Гарант:

```
$ /usr/local/garant/intranet/bin/restart.sh
```

Далее необходимо открыть веб-адрес страницы администрирования Гарант http://garant.ald.company.lan:8082/admin, перейти во вкладку **Настройки** и выбрать **Разрешена под именем учетной записи Windows или Linux**, затем нажать кнопку Сохранить.

Примечание: В случае, если вы почистите «куки» в браузере и попытаетесь зайти снова под тем же пользователем, то система вас не пустит, необходимо выждать 5 минут. Связано это с тем, что Гарант не закрывает сессию при закрытии вкладки браузера, а запускает таймер, по истечении которого закроет ее. Если пользователь снова решит подключиться в течение работы таймера, то вернется в свою старую сессию.

4 Настройка клиента **client.ald.company.lan**

Дополнительных настроек на клиенте не требуется при условии, что компьютер введен в домен.

Для проверки работы Гарант необходимо зайти в систему под доменным пользователем, открыть в браузере Firefox сайт http://garant.ald.company.lan. Apache автоматически вас аутентифицирует по протоколу Kerberos и авторизует согласно членству в группе garant-ldap-group и перенаправит на страницу Гарант. Обратите внимание, что веб-адрес изменился, теперь мы не используем порт 8082, а порт 80 непосредственно сервиса Apache.

Произойдет это по причине того, что браузер уже настроен на передачу веб-серверу Kerberos-билетов.

Убедиться в этом можно, зайдя в настройки Firefox:

- открыть в браузере страницу настройки конфигурации **about:config**;
- найти параметры **network.negotiate-auth.trusted-uris** и **network.negotiate-auth.delegation-uris**;
- Убедиться в наличии значения **.ald.company.lan.**