Интеграция 1С:Предприятие со службой каталога ALD Pro

06/10/2025

Содержание

Одной из самых популярных платформ для построения систем учета в России является 1С. На базе этого решения созданы такие продукты (конфигурации), как 1С:Бухгалтерия (автоматизации бухгалтерского и управленческого учета), 1С:ЗУП (автоматизация расчета заработной платы), 1С:Предприятие (автоматизация организационной деятельности предприятия).

В настоящей инструкции описана процедура интеграции сервера 1С со службой каталога ALD Pro. Данная интеграция обеспечит возможность сопоставления доменных учетных записей с пользователями 1С для аутентификации по безопасному протоколу Kerberos V5.

1 Описание стенда

Для примера будем использовать стенд, верхнеуровневый дизайн которого представлен на рисунке 1. Стенд содержит следующие компоненты:

- **1csrv** — сервер 1С, установленный на Linux не в домене;
- **alddc1.ald.lan** — контроллер домена ALD Pro;
- **srvsssd.ald.lan** — доменная рабочая станция.

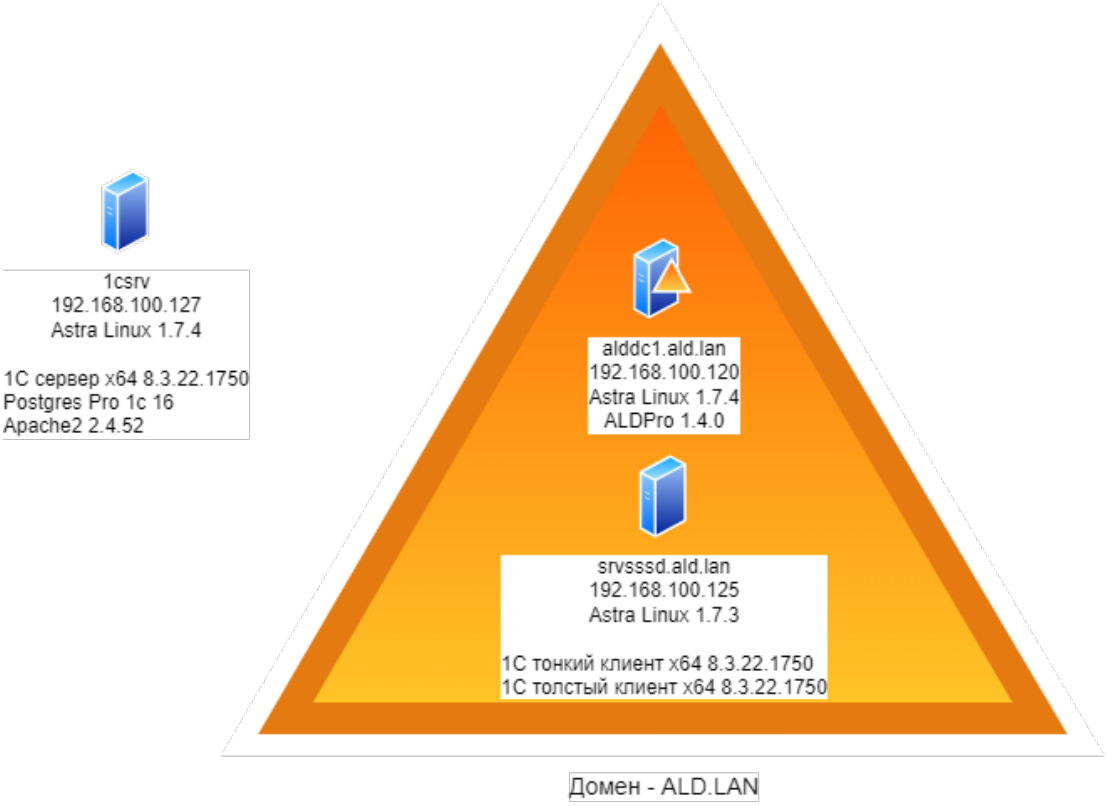

Рисунок 1 - Верхнеуровневый дизайн лабораторного стенда

2 Сценарии подключения к 1С

Сценарий 1 – подключение через тонкий/толстый клиент

Сценарий 2 – подключение через веб-браузер

3 Настройка пользователей в 1С

Вне зависимости от выбранного сценария, настройка пользовательских учетных записей в 1С сводится к тому, чтобы сопоставить внутреннего пользователя 1С с доменной учетной записью. Для этого необходимо зайти в 1С, открыть форму «Администрирование > Настройки пользователей и прав > Пользователи» (рис.2).

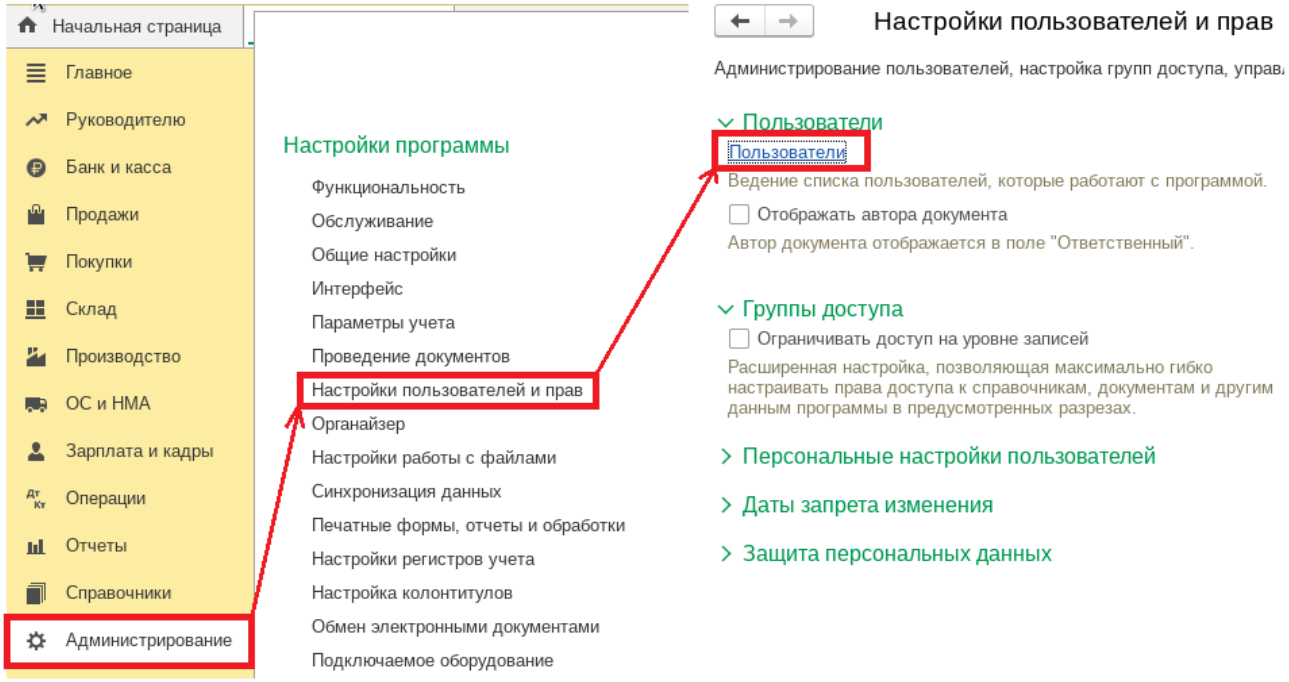

Рисунок 2 — Переход к редактированию локальных пользователей 1С

Далее выбираем пользователя, ставим флажок «Аутентификация операционной системы» и в поле «Пользователь» прописываем «**\\ald.lan\admin**», где ald.lan – реалм домена, admin – имя доменного пользователя. На примере ниже вы можете заметить, что имя пользователя 1С совпадает с доменным именем, но это не является обязательным требованием, поэтому имена могут и различаться (рис.3).

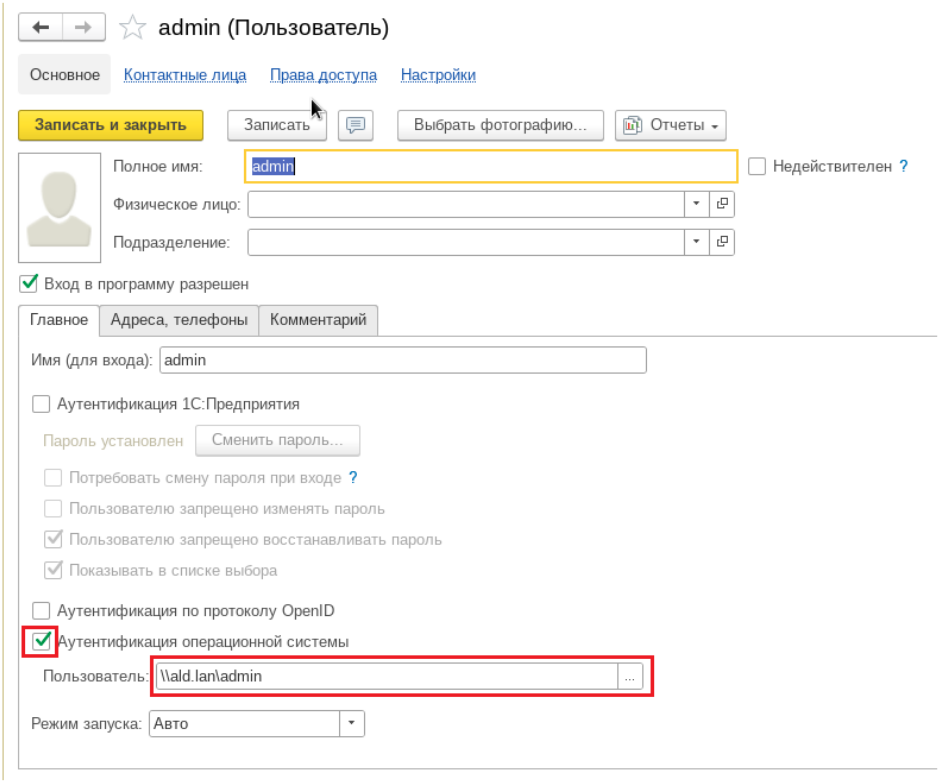

Рисунок 3 - Сопоставление внутреннего пользователя 1С с доменной учетной записью

4 Настройка для толстого/тонкого клиента

В данном разделе рассматриваются вопросы настройки сервера 1С для прозрачной Kerberos аутентификации пользователей из домена ALD Pro (FreeIPA) при подключении толстым/тонким клиентом.

Мы предполагаем, что у вас уже установлен сервер 1С, но, если вам нужны будут рекомендации по установке и настройке продукта, вы можете воспользоваться справочной информацией с официального сайта разработчика, например:

- Установка системы «1С:Предприятие»

  https://its.1c.ru/db/v8324doc#bookmark:adm:TI000000024

- Установка PostgresSQL

  https://its.1c.ru/db/v8321doc#bookmark:cs:TI000000112

- Служба сервера администрирования RAS

  https://its.1c.ru/db/v839doc#bookmark:cs:TI000000193

4.1 Настройки в домене

4.1.1 Создание DNS-записи

Когда доменный пользователь входит в операционную систему Linux, в связке ключей появляется TGT-билет, с помощью которого выполняется прозрачная аутентификация при обращении к керберизированным сервисам.

Взаимодействие между службами по протоколу Kerberos происходит по FQDN-именам, поэтому у каждого хоста в домене обязательно должна быть как минимум A-запись. Учитывая, что сервер, на котором установлена служба 1С, еще не в домене, то DNS-запись для этого хоста следует создать вручную. Сделать это можно как из командной строки, так и через веб-интерфейс.

Чтобы создать DNS-запись из командной строки, воспользуйтесь командой dnsrecord-add:

```
$ ipa dnsrecord-add ald.lan 1csrv --a-rec 192.168.100.127
```

, где

- ald.lan — имя DNS-зоны,
- 1csrv — имя сервера,
- a-rec — тип записи.

Чтобы создать DNS-запись через веб-интерфейс ALD Pro, перейдите в раздел «Роли и службы сайта > Служба разрешения имен», выберите нужную зону и нажмите кнопку «Новая DNS-запись». Имя записи «1csrv», тип «A», IP адрес 192.168.100.127 (рис.4).

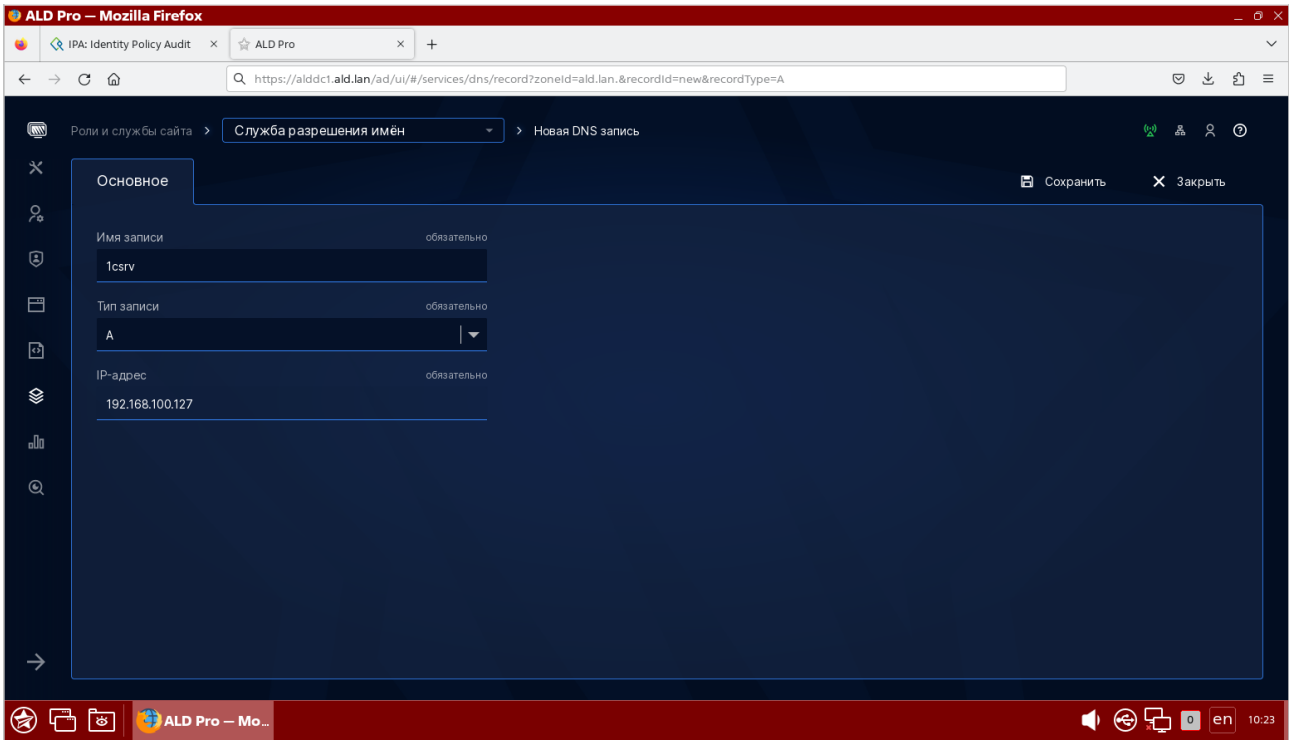

Рисунок 4 — Создание DNS-записи через веб-интерфейс ALD Pro

4.1.2 Создание учетной записи сервиса

При обращении клиентов к серверу 1С в домене **ALD.LAN** на хосте **1csrv.ald.lan** с аутентификацией по Kerberos им нужно предъявить билет на имя **usr1cv8/1csrv.ald.lan@ALD.LAN**, где usr1cv8 — это имя службы, которая «зашита» в логику работы приложения 1С.

Для того, чтобы KDC смог выдать такой билет, в домене должна существовать такая служебная учетная запись, а для того, чтобы сервер 1С смог проверять такие билеты, ему должен быть доступен keytab-файл с паролем от этой учетной записи.

Создавать служебную учетную запись можно командой service-add:

```
$ ipa service-add usr1cv8/1csrv.ald.lan --skip-host-check
--------------------------------------------------------------------
Добавлена служба "usr1cv8/1csrv.ald.lan@ALD.LAN"
--------------------------------------------------------------------
Имя учётной записи: usr1cv8/1csrv.ald.lan@ALD.LAN
Псевдоним учётной записи: usr1cv8/1csrv.ald.lan@ALD.LAN
```

, где

- usr1cv8/1csrv.ald.lan — имя учетной записи;
- skip-host-check — флаг, который позволяет отключить проверку на существование хоста в домене, т.к. сервер не находится в домене.

Чтобы сервер 1С 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 из командной строки с помощью утилиты ipa-getkeytab.

```
$ ipa-getkeytab -p usr1cv8/1csrv.ald.lan@ALD.LAN -k usr1cv8.keytab
Таблица ключей успешно получена и сохранена в: usr1cv8.keytab
```

Утилита ipa-getkeytab генерирует случайный пароль, добавляет к нему соль, полученную из имени Kerberos-принципала, и хеширует полученную строку указанными алгоритмами (по умолчанию aes256-cts-hmac-sha1-96 и aes128-cts-hmac-sha1-96). Посмотреть содержимое keytab-файла можно с помощью команды klist с ключами ket.

```
$ ls -l
итого 8
drwxr-xr-x 2 root root 4096 мая 16 2023 Desktop
-rw------- 1 root root 194 ноя 25 10:56 usr1cv8.keytab

$ klist -ket usr1cv8.keytab
Keytab name: FILE:usr1cv8.keytab
KVNO Timestamp         Principal
---- ------------------ ------------------------------------------------------
1 25.11.2023 10:56:17 usr1cv8/1csrv.ald.lan@ALD.LAN (aes256-cts-hmac-sha1-96)
1 25.11.2023 10:56:17 usr1cv8/1csrv.ald.lan@ALD.LAN (aes128-cts-hmac-sha1-96)
```

4.2 Настройки на сервере 1С

Если сервер 1С будет установлен в операционной системе Linux, которая присоединена к домену ALD Pro штатным порядком, то многие из следующих настроек будут выполнены автоматически. Если это не представляется возможным, то следует учесть предложенные рекомендации.

4.2.1 Настройка имени хоста

Имя хоста следует задать как полное FQDN имя сервера, иначе клиенты при обращении к KDC за сервисными билетами (TGS) будут запрашивать их на короткое имя **usr1cv8/1csrv@ALD.LAN** и получать ошибку, что такого принципала в базе данных не существует. Установить имя можно с помощью утилиты hostnamectl:

```
$ sudo hostnamectl set-hostname 1csrv.ald.lan
$ hostname
1csrv.ald.lan
```

Если вы не можете изменить имя хоста по какой-либо причине, то проблему короткого имени можно решить добавлением алиаса к служебной учетной записи, но такой способ видится менее предпочтительным.

4.2.2 Настройка DNS

Приложение 1С 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 192.168.100.120

search ald.lan
```

, где

- nameserver — задает IP-адрес DNS сервера;
- search — устанавливает DNS-суффикс, который добавляется к коротким именам.

4.2.3 Настройка синхронизации времени

Для корректной работы Kerberos-аутентификации системное время на сервере 1С 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 vi /etc/chrony/chrony.conf
server alddc1.ald.lan iburst
```

4.2.4 Настройка Kerberos (необязательно)

Служба 1С не обращается к LDAP-каталогу, она только проверяет Kerberos-билеты, поэтому настройка Kerberos-библиотек не требуется.

4.2.5 Настройка имени кластера

Рекомендуется также настроить имя кластера, хотя для работы в одном домене это необязательно.

В файле /home/usr1cv8/.1cv8/1C/1cv8/1cv8wsrv.lst

```
{
{1,
{48cef145-4826-4a8f-90e9-4ad0c45e8f89,"Локальный кластер",1541,"1csrv.ald.lan",0,0,0,6
0,0,0,0,
{1,
{"1csrv.ald.lan",1541}
},0,0,1,0}
},
{0},0,1}
```

В файле /home/usr1cv8/.1cv8/1C/1cv8/reg_1541/1CV8Clst.lst

```
{0,
{48cef145-4826-4a8f-90e9-4ad0c45e8f89,"Локальный кластер",1541,"1csrv.ald.lan",0,0,0,6
0,0,0,0,
{1,
{"1csrv.ald.lan",1541}
},0,0,1,0},
{1,
```

```
{82f76315-f124-46d5-8d2e-ce52fe01258c,"test1","","PostgreSQL","127.0.0.1","test1","po
stgres","fPTES5DV+wGxEd6M+Y0ckMXWV25SwORqXbl3MSMMm/0=","CrSQLDB=Y;DB=test1;DBMS=Postg
reSQL;DBSrvr=127.0.0.1;DBUID=postgres;LIC=3746147098055347968;LicDstr=Y;Locale=ru_RU;
Ref=test1;SLev=0;Srvr=192.168.100.127",0,
{0,00010101000000,00010101000000,"","","",0},0,1,"",0,"","",20,0}
},
{1,
{112e3a3b-acd4-4f79-af63-f66344117b8e,"1csrv.ald.lan",1,0,1000,4c8ab57a-bce0-4d2f-
b056-71c78c738c66,0}
},
{0},
{1,
{4c8ab57a-bce0-4d2f-b056-71c78c738c66,"Центральный сервер",1540,"1csrv.ald.lan",1,
{1,
{1560,1591}
},"","UvOa5Ox95HBnpwzCH6HyZA==",0,0,8,256,1000,1,0,1,0,1,1541,0,0,300,""}
},
{1,
{c0196aef-4358-46e8-b07d-f3c2f63374cd,"Главный менеджер кластера","1csrv.ald.lan",1,1,
4c8ab57a-bce0-4d2f-b056-71c78c738c66}
},
{0},
{0},
{0},
{0},
{0},
{0,0},0,
{0},
{0},
{0},
{0},
{0},
{0},
{0},
{0},
{0},24,
{0},
{0},
{""},
{""},
{0},"d9RzLHbwiL8eEcQhVTx31P4XkRwI+DWvDZR+BgRkGMo="}
```

4.2.6 Настройка Keytab

Как уже было сказано ранее, keytab-файл используется сервером 1С для расшифровки сервисных билетов. Файл **usr1cv8.keytab** нужно скопировать в каталог **/opt/1cv8/x86_64/8.3.22.1750/** и разрешить чтение/запись для пользователя 1С и соответствующей группы:

```
chown usr1cv8:grp1cv8 /opt/1cv8/x86_64/8.3.22.1750/usr1cv8.keytab
chmod 600 /opt/1cv8/x86_64/8.3.22.1750/usr1cv8.keytab
```

Файл можно разместить в другом месте, путь задается параметром среды окружения SRV1CV8_KEYTAB, который можно изменить в конфигурационном файле srv1cv8-8.3.22.1750@.service:

```
vi /opt/1cv8/x86_64/8.3.22.1750/srv1cv8-8.3.22.1750@.service
```

```
Environment=SRV1CV8_KEYTAB=/opt/1cv8/x86_64/8.3.22.1750/usr1cv8.keytab
```

В случае, если вы изменили стандартный путь к keytab-файлу, необходимо перезагрузить службу:

```
systemctl restart srv1cv8-8.3.22.1750@[instance_name].service
```

5 Настройка сервера 1С для веб-клиента

В данном разделе рассматриваются вопросы настройки сервера 1С для прозрачной Kerberos-аутентификации пользователей из домена ALD Pro (FreeIPA) при подключении веб-клиентом.

Раздел написан из предположения, что на сервере 1С уже установлен и настроен веб-сервер Apache, а также выполнена публикация приложения 1С на этом веб-сервере, поэтому, если вам нужны будут рекомендации по установке и настройке сервера 1С, вы можете воспользоваться справочной информацией с официального сайта разработчика, например:

- Настройка веб-серверов для работы с «1С:Предприятием» https://its.1c.ru/db/v8322doc#bookmark:adm:TI000000668

Учитывая, что порядок настройки сервера 1С для веб-клиента во многом повторяет порядок настройки для толстого/тонкого клиента, мы не станем дублировать эту информацию во избежание путаницы и подчеркнем только специфические моменты.

5.1 Настройки в домене

5.1.1 Создание DNS записи

Рекомендации те же самые, что и для настройки толстого/тонкого клиента.

5.1.2 Создание учетной записи сервиса

Если для толстого/тонкого клиента требуется учетная запись **usr1cv8/1csrv.ald.lan@ALD.LAN**, то веб-клиент будет обращаться к службе с именем **HTTP/1csrv.ald.lan@ALD.LAN**. В остальном рекомендации будут те же самые. После создания службы нужно с помощью утилиты ipa-getkeytab сгенерировать для нее пароль и выгрузить его в файл **apache2.keytab**.

```
$ ipa-getkeytab -p HTTP/1csrv.ald.lan@ALD.LAN -k apache2.keytab
Таблица ключей успешно получена и сохранена в: apache2.keytab
```

5.2 Настройки на сервере 1С

5.2.1 Настройка имени хоста

Рекомендации те же самые, что и для настройки толстого/тонкого клиента.

5.2.2 Настройка DNS

Рекомендации те же самые, что и для настройки толстого/тонкого клиента.

5.2.3 Настройка синхронизации времени

Рекомендации те же самые, что и для настройки толстого/тонкого клиента.

5.2.4 Настройка Kerberos

Для работы Kerberos-аутентификации на веб-сервере нужно настроить библиотеку Kerberos в файле /etc/krb5.conf следующим образом:

```
[libdefaults]
default_realm = ALD.LAN
dns_lookup_realm = true
dns_lookup_kdc = true
rdns = false
dns_canonicalize_hostname = false
ticket_lifetime = 24h
forwardable = true
udp_preference_limit = 0
default_ccache_name = KEYRING:persistent:%{uid}
```

5.2.5 Настройка имени кластера

Рекомендации те же самые, что и для настройки толстого/тонкого клиента.

5.2.6 Настройка Keytab

Как уже было сказано ранее, keytab-файл используется сервером Apache для расшифровки сервисных билетов. Файл **apache2.keytab** нужно скопировать в каталог **/etc/apache2/** и разрешить чтение/запись для пользователя www-data и соответствующей группы:

```
chown www-data:www-data /etc/apache2/apache2.keytab
chmod 600 /etc/apache2/apache2.keytab
```

На веб-сервере Apache обеспечить Kerberos-аутентификацию пользователей можно с помощью модулей kerb и gssapi. Модуль gssapi считается более современным и должен заместить модуль kerb, поэтому рекомендуем использовать модуль GSSAPI.

Установим модуль gssapi для веб-сервера Apache2:

```
apt install libapache2-mod-auth-gssapi
```

Следующим шагом настроим каталог для хранения кэша учетных данных для дальнейшего их делегирования 1С серверу. Скопируйте юнит сервиса Apache в /etc/systemd/system/system/ :

```
cp /lib/systemd/system/apache2.service /etc/systemd/system/
```

Далее внесите дополнительную опцию в секцию **[Service]** /etc/systemd/system/apache2.service:

```
Environment=KRB5CCNAME=/tmp
```

Выглядеть должно так:

```
[Unit]
Description=The Apache HTTP Server
After=network.target remote-fs.target nss-lookup.target
Documentation=https://httpd.apache.org/docs/2.4/

[Service]
Type=forking
Environment=APACHE_STARTED_BY_SYSTEMD=true
Environment=KRB5CCNAME=/tmp
ExecStart=/usr/sbin/apachectl start
ExecStop=/usr/sbin/apachectl graceful-stop
ExecReload=/usr/sbin/apachectl graceful
KillMode=mixed
PrivateTmp=true
Restart=on-abort

[Install]
WantedBy=multi-user.target
```

Перезагрузите конфигурацию всех юнитов:

```
systemctl daemon-reload
```

Теперь перезагрузите Apache для применения новых настроек:

```
systemctl restart apache2
```

После применения настроек выше временные файлы с кешем пользователей будут находится в /tmp/systemd-private-*-apache2.service-*/tmp/.

Теперь нам нужно изменить настройки Apache, для этого отредактируем файл настроек /etc/apache2/apache2.conf, где поменяем секцию «1c publication».

Старое значение:

```
# 1c publication
Alias "/demo" "/var/www/demo/"
<Directory "/var/www/demo/">
AllowOverride All
Options None
Require all granted
SetHandler 1c-application
ManagedApplicationDescriptor "/var/www/demo/default.vrd"
</Directory>
```

Новое значение:

```
# 1c publication
Alias "/demo" "/var/www/demo/"
```

```
<Directory "/var/www/demo/">

AuthType GSSAPI
AuthName "GSSAPI SSO 1C Login"
GssapiCredStore keytab:/etc/apache2/apache2.keytab
GssapiAllowedMech krb5
GssapiDelegCcacheDir /tmp
GssapiDelegCcacheUnique On

Require valid-user
AllowOverride All
Options None
#Require all granted
SetHandler 1c-application
ManagedApplicationDescriptor "/var/www/demo/default.vrd"
</Directory>
```

Здесь вы можете увидеть следующие параметры:

- GssapiDelegCcacheDir– опция сохранения билета Kerberos в кэше /tmp/systemd-private-*-apache2.service-*/tmp/. Если не настроить, то браузер проходит Kerberos аутентификацию, но не передает данные о пользователе дальше в 1С, поэтому 1С просит ввести локальную учетную запись;
- GssapiDelegCcacheUnique – опция, которая, при сохранении кэша билета Kerberos, добавляет 6 символов к имени. Так же этот параметр удаляет кэш после установления сессии с приложением. Если не настроить этот параметр и при этом параметр GssapiDelegCcacheDir будет включен, то при обращении из доверенного домена к сервису 1С, apache2 может выдать чужой кэшированный билет Kerberos, тем самым предоставить несанкционированный доступ;
- GssapiAllowedMech - опция, которая принудительно ограничивает выбор механизма аутентификации. В нашем случае это Kerberos. Если опции не настроена, то GSSAPI может переключиться на NTLM при неудаче с Kerberos;
- #Require all granted – предоставление доступа всем. Комментируем эту строчку, чтобы не прошедший аутентификацию пользователь не смог получить доступ;
- Require valid-user – предоставление доступа аутентифицированным пользователям. Включаем доступ только аутентифицированным пользователям.

5.3 Настройки на рабочей станции

Для того, чтобы браузер доменного компьютера отправлял веб-серверу Kerberos-билеты, это должно быть явно разрешено в настройках браузера для этого домена.

В браузере Firefox это можно настроить через корпоративную политику в файле /usr/lib/firefox/distribution/policies.json. Для этого нужно в секции Authentication задать параметр SPNEGO (Simple and Protected GSS-API Negotiation Mechanism, простой и защищенный механизм согласования GSS-API), как показано ниже:

```
# vi /usr/lib/firefox/distribution/policies.json
{
     "policies": {
          "BlockAboutAddons": true,
          "BlockAboutConfig": true,
          "Authentication": {
              "SPNEGO": ["ald.lan"]
          },
```

```
        "Certificates": {
            "ImportEnterpriseRoots": true,
            "Install": ["/etc/ipa/ca.crt"]
        },
        "Homepage": {
           "URL": "https://dc-1.ald.lan/",
           "Locked": true,
           "StartPage": "homepage-locked"
        }
    }
}
```

Для браузеров на базе Chromium возможность Kerberos аутентификации можно настроить с помощью файла "policies.json" в каталоге приложения /policies/managed. Для этого в нем нужно определить значение параметра AuthServerAllowlist. Вот пример для Яндекс браузера:

```
$ cat /etc/opt/yandex/policies/managed/policies.json
{"AuthServerAllowlist": "*.ald.lan",}
```

На компьютерах Astra Linux в домене ALD Pro указанные настройки можно внести автоматически путем создания дополнительного параметра групповой политики (см. Руководство администратора, раздел «5.4.3 Доступ к веб-интерфейсам и REST API контроллера домена по протоколу HTTPS»).