Интеграция Bitrix со службой каталога ALD Pro

06/10/2025

Содержание

Битрикс24 является платформой для построения корпоративных порталов и создания веб-сайтов организаций.

В настоящей инструкции описана процедура интеграции Битрикс24 со службой каталога ALD Pro. Данная интеграция даст возможность импортировать пользователей, привязать их к учетным записям из домена, обеспечить аутентификацию через единую точку входа по протоколам LDAP или Kerberos V5, использовать информацию об участии доменных пользователей в группах для назначения прав доступа.

1 Описание стенда

Наш стенд представляет из себя систему из трех виртуальных машин:

- **bitrix** — сервер 1С-Битрикс: Виртуальная машина VMBitrix (не в домене). Редакция продукта: 1С-Битрикс24: Энтерпрайз 1000, так как только в ней есть модуль для интеграции с Active Directory/LDAP;
- **dc-1.ald.lan** - контроллер домена ALD Pro;
- **pc-1.ald.lan** - доменная рабочая станция.

В настройках указывайте имя своего домена вместо используемого в примере ***ald.lan***.

2 Первоначальная установка и настройка решения Bitrix

Начальная установка и настройка решения, запущенного на виртуальной машине BitrixVM, проводится по общей инструкции.

При этом в мастере установки сайта **не** следует сразу указывать подключение к AD, так как требуемые параметры не могут быть предоставлены на начальном этапе настройки (рис.1).

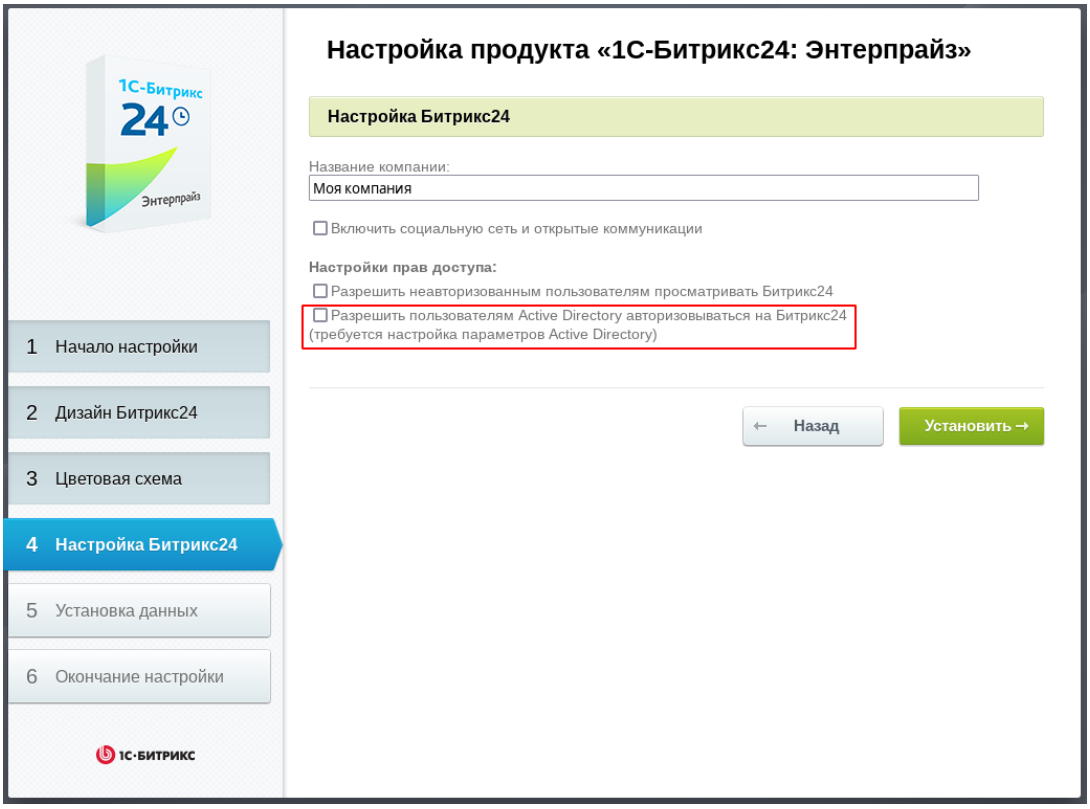

Рисунок 1 — Настройка Битрикс24

При последующей настройке решения Bitrix через консольное меню, которое запускается из-под учетной записи root, минимально необходимо настроить:

- имя сервера (hostname) как FQDN в домене ALD pro. Например *bitrix.ald.lan*(Инструкция);
- в настройке сетевого интерфейса в качестве DNS-сервера - IP адрес контроллера домена (Инструкция).

Затем мы рекомендуем присоединить сервер к домену ALD Pro, чтобы сократить количество действий по настройке сервера, получить возможность входить в операционную систему с помощью доменных учетных записей, управлять сервером через механизм групповых политик.

Далее описаны дополнительные настройки на сервере, если сервер не введён в домен.

- Для корректной работы Kerberos-аутентификации системное время на сервере 1С и рабочих станциях может расходиться не более, чем на +/- 5 минут. Можно синхронизировать время вручную, но при работе сервера с аутентификацией в домене настоятельно рекомендуется использовать автоматическую синхронизацию времени. В Bitrix используется демон ntpd, поэтому в настройках NTP-сервиса в файле /etc/ntp.conf в качестве сервера времени необходимо указать имя или IP контроллера домена, убрав остальные настройки «server»:

```
# vi /etc/ntp.conf
```

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

- При использовании протокола SSL приложения почти всегда проверяют цепочку подписи сертификата сервиса, к которому идёт обращение. Корневые сертификаты таких цепочек находятся в операционной системе локально, и с их помощью окончательно (по цепочке доверия) подтверждается корректность конечного сертификата. Все доменные сервисы используют в своей работе сертификаты, которые подписаны корневым сертификатом доменного центра сертификации. Для корректной работы с такими сервисами необходимо добавить на сервер Bitrix корневой сертификат доменного центра сертификации в список доверенных.
  Получить сертификат через контроллер домена и сохранить его на диске можно следующей командой:

```
echo "" | openssl s_client -connect dc-1:443 -showcerts 2>/dev/null | sed '0,/END
CERTIFICATE/d' | openssl x509 > /etc/pki/ca-trust/source/anchors/rootCA.pem
```

Для того, чтобы обновить список корневых сертификатов, выполните следующую команду:

```
update-ca-trust
```

3 Интеграция Bitrix с LDAP-сервером ALD Pro

- Аутентификация и авторизация выполняется методом LDAP Bind, поэтому необходимо создать сервисную учетную запись в ALD Pro, с помощью которой будет осуществляться подключение Bitrix к LDAP.

Для этого нужно подключиться по SSH к контроллеру домена и выполнить следующие шаги:

1. Создать файл с именем srv-bitrix.update и содержимым:

```
dn: uid=srv-bitrix,cn=sysaccounts,cn=etc,dc=ald,dc=lan
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: srv-bitrix
add:userPassword: securePassword
add:passwordExpirationTime: 20380119031407Z
add:nsIdleTimeout: 0
```

, где необходимо заменить «securePassword» на желаемый пароль учетной записи.

2. Выполнить добавление пользователя следующей командой:

```
kinit admin && ipa-ldap-updater srv-bitrix.update
```

Такой пользователь не является POSIX-пользователем, не имеет прав на вход в компьютеры домена и не отображается в портале управления ALD PRO, а имеет права только на чтение LDAP.

- В домене ALD Pro необходимо создать одну или несколько групп пользователей (например, bitrix-users) для предоставления и разграничения доступа к порталу Bitrix.
- В разделе AD/LDAP настроек bitrix добавить новую интеграцию с ALD Pro со следующими параметрами (рис. 2):
    - Тип подключения может быть SSL (ldaps) вместо TLS;
    - В качестве логина необходимо указать полный DN системного пользователя;
    - Корень дерева (base DN) должен быть именно таким, чтобы поиск пользователей выдавал корректные однозначные результаты.

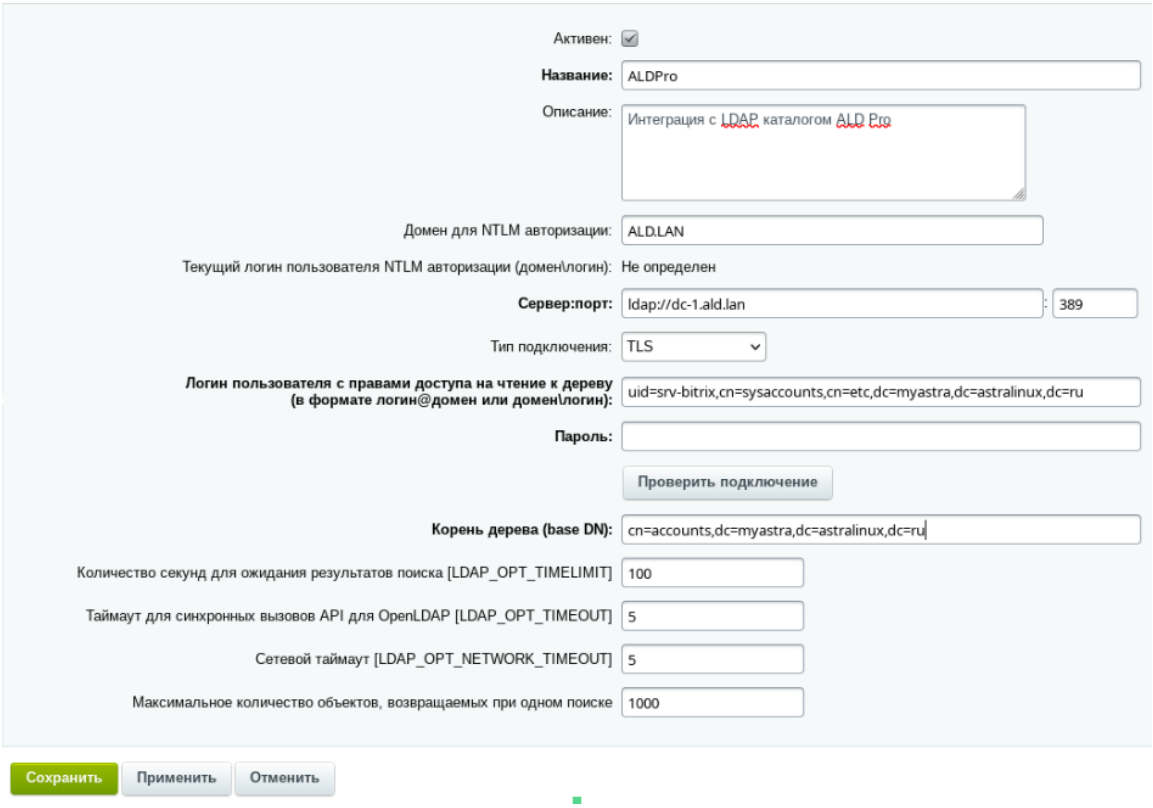

Рисунок 2 – Настройка параметров интеграции с доменом

На вкладке «Настройка полей» выбрать «Параметры схемы сервера LDAP». Это заполнит большинство полей правильными значениями. Затем отредактировать отдельные поля как показано на скриншоте ниже. Также в разделе «Соответствие полей пользователя и атрибутов LDAP» удалить поле «Активность» (рис. 3).

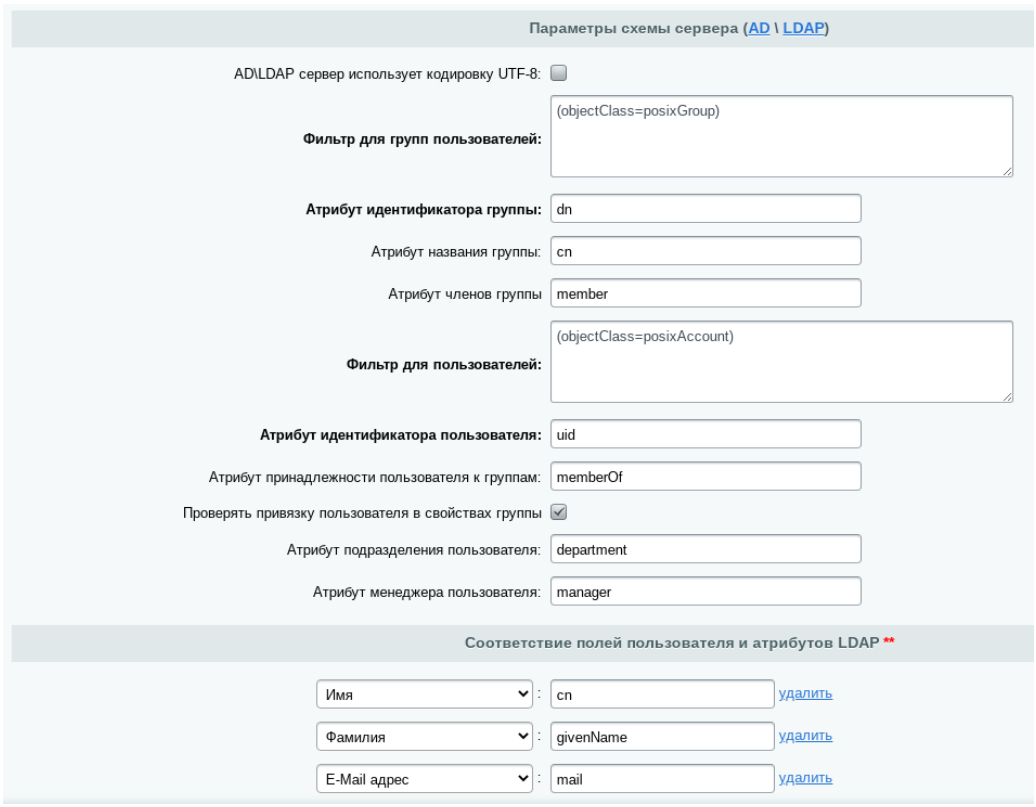

Рисунок 3 – Настройка схемы и соответствия полей

В поле «Атрибут идентификатора группы» используйте значение «dn», которое не является атрибутом для объекта типа «группа», а представляет собой уникальное имя объекта. Хотя этого атрибута в LDAP-ответе не существует, тем не менее Bitrix добавляет его в свой внутренний список атрибутов объекта.

Дополнительно нужно настроить как минимум одно соответствие групп пользователей домена с локальными группами пользователей Bitrix, чтобы отрабатывала авторизация и предоставлялся доступ на портал (рис. 4):

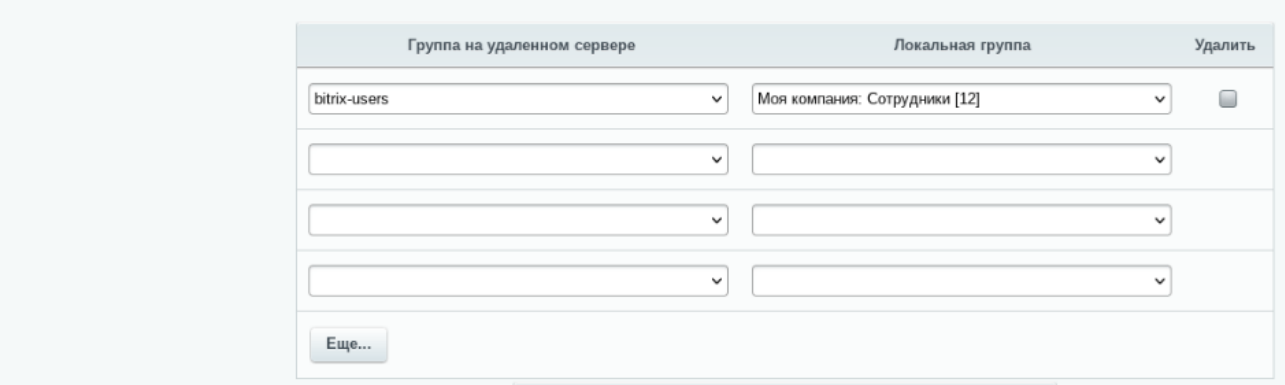

Рисунок 4 — Настройка соответствия групп пользователей

При создании реальных пользователей в домене необходимо заполнять поле mail, так как оно является обязательным при извлечении информации о пользователе из LDAP-каталога. После создания пользователей и добавления их в ранее созданную группу bitrix-users можно сделать импорт пользователей в Bitrix (рис. 5):

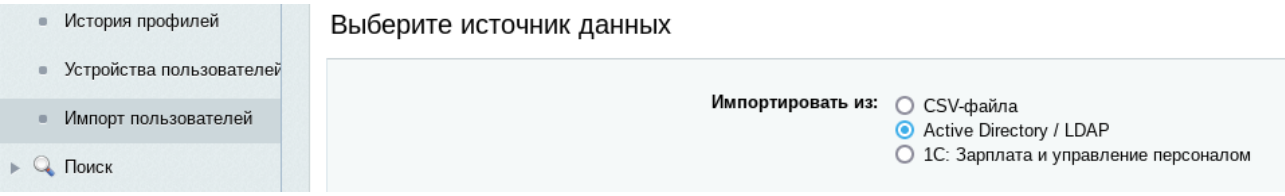

Рисунок 5 — Импорт пользователей в Bitrix

Хотя этот шаг и не обязателен, так как при включении соответствующей настройки пользователи будут создаваться автоматически, он позволит проверить, что связка с ALD Pro настроена корректно.

- Также необходимо проверить настройки модуля AD/LDAP (рис.6):

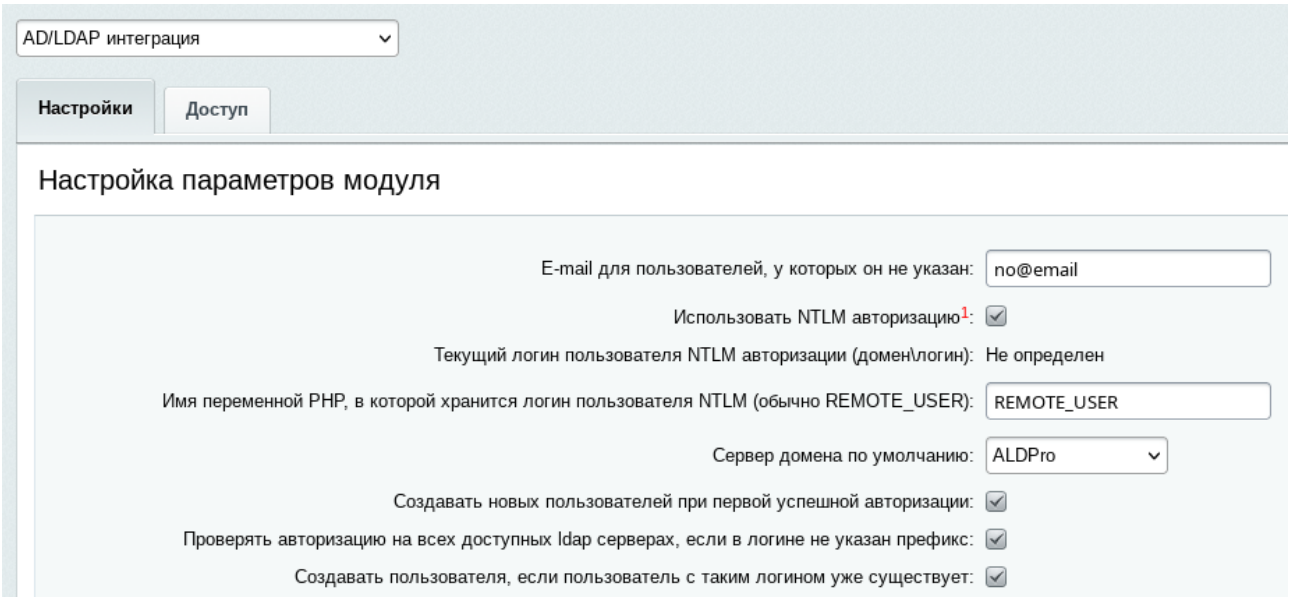

Рисунок 6 - Настройка модуля AD/LDAP

С этого момента проверка аутентичности пользователей на портале Bitrix будет осуществляться через контроллер домена ALD Pro по протоколу LDAP.

Но данный метод аутентификации содержит риски компрометации пароля на стороне сервера Bitrix, поскольку пароль передаётся в открытом виде внутри модулей Bitrix для возможности проверки корректности пароля на стороне LDAP-сервера (контроллера домена). В этом случае, роль администраторов сервера Bitrix может быть возложена только на очень привилегированных администраторов домена.

4 Аутентификация пользователей Bitrix по протоколу NTLM

При интеграции решения Bitrix с Active Directory от Microsoft возможна настройка более безопасного чем LDAP метода аутентификации по протоколу NTML. Однако этот метод является устаревшим и уязвимым в силу своей реализации перед атаками:

- подбор пароля (хеш не содержит переменной части - «соли»);
- восстановление пароля из хеша (слабый хеш);
- man-in-the-middle, так как нет взаимной аутентификации сторон.

Поэтому мы не рекомендуем настраивать данный тип аутентификации.

5 Настройка Kerberos для аутентификации пользователей Bitrix

5.1 Настройки на стороне домена ALD Pro

5.1.1 Создание DNS-записи

Следующая настройка необходима, если сервер не введён в домен. При вводе в домен DNS-запись создаётся автоматически.

При выполнении Kerberos-аутентификации доменный компьютер получает у контроллера от имени пользователя сервисный билет, с помощью которого в дальнейшем при обращении к сервису подтверждает аутентичность пользователя. Взаимодействие между службами по протоколу Kerberos выполняется по FQDN-именам, поэтому у каждого хоста в домене обязательно должна быть как минимум A-запись. Учитывая, что сервер, на котором установлена служба Bitrix не в домене, то DNS-запись для этого хоста следует создать вручную. Создать DNS-запись можно как из командной строки, так и через веб-интерфейс.

Чтобы создать DNS-запись из командной строки, воспользуйтесь командой dnsrecord-add на доменной машине с необходимыми правами пользователя:

```
$ ipa dnsrecord-add ald.lan bitrix --a-rec {IP_ADDR}
```

, где

- ald.lan – имя DNS зоны,
- bitrix — имя сервера,
- --a-rec — тип записи,
- {IP_ADDR} - настроенный на сервере IP-адрес.

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 «bitrix», тип «A», в поле IP-адрес укажите настроенный на сервере IP (рис. 7).

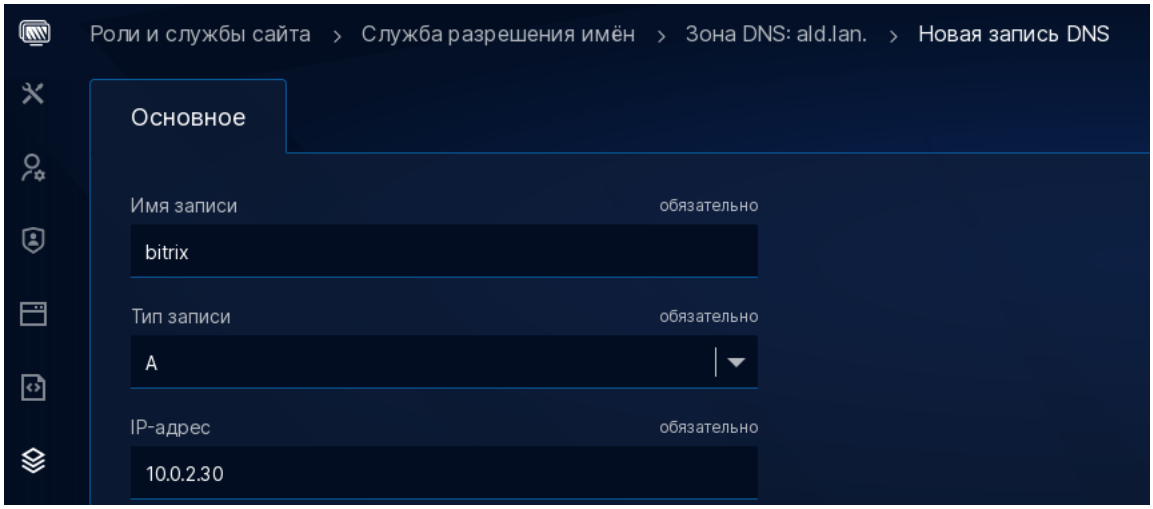

Рисунок 7 — Создание DNS-записи

5.1.2 Создание учетной записи сервиса

При обращении клиентов к серверу Bitrix в домене ALD.LAN на хосте bitrix.ald.lan с аутентификацией по Kerberos им нужно предъявить свой билет на имя Kerberos принципала «HTTP/bitrix.ald.lan@ALD.LAN».

Для того, чтобы KDC смог выдать такой билет, в домене должна существовать такая служебная учетная запись, а для того, чтобы сервер Bitrix 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 ipa service-add:

```
# ipa service-add HTTP/bitrix.ald.lan --skip-host-check
-----------------------------------------------------------
Добавлена служба "HTTP/bitrix.ald.lan@ALD.LAN"
-----------------------------------------------------------
Имя учётной записи: HTTP/bitrix.ald.lan@ALD.LAN
Псевдоним учётной записи: HTTP/bitrix.ald.lan@ALD.LAN
```

, где

  - HTTP/bitrix.ald.lan — имя учетной записи сервиса,
  - skip-host-check — флаг для отключения проверки на существование хоста, если сервер не находится в домене.
- Создать служебную учетную запись через веб-интерфейс ALD Pro можно на странице «Управление доменом > Службы и параметры Kerberos».

Если сервер не введён в домен, то для того, чтобы иметь возможность выбрать хост из списка, нужно создать учетную запись хоста из следующей командной строки:

```
$ ipa host-add bitrix.ald.lan --ip-address={IP_ADDR}
--------------------------------------
Добавлен узел "bitrix.ald.lan"
--------------------------------------
Имя узла: bitrix.ald.lan
Имя учётной записи: host/bitrix.ald.lan@ALD.LAN
Псевдоним учётной записи: host/bitrix.ald.lan@ALD.LAN
Link to department: ou=ald.lan,cn=orgunits,cn=accounts,dc=ald,dc=lan
Link to head department: ald.lan
Пароль: False
Таблица ключей: False
Managed by: bitrix.ald.lan
```

На странице «Управление доменом > Службы и параметры Kerberos» заполните поля, нажав кнопку “Новая служба”, и нажмите кнопку «Сохранить» (рис. 8).

Рисунок 8 – Создание учетной записи для портала Bitrix

- Вы также можете воспользоваться веб-интерфейсом IPA на странице «Идентификация > Службы». Нажмите кнопку «Добавить», укажите службу HTTP, имя узла bitrix и включите опцию "Пропустить проверку узла" (рис. 9).

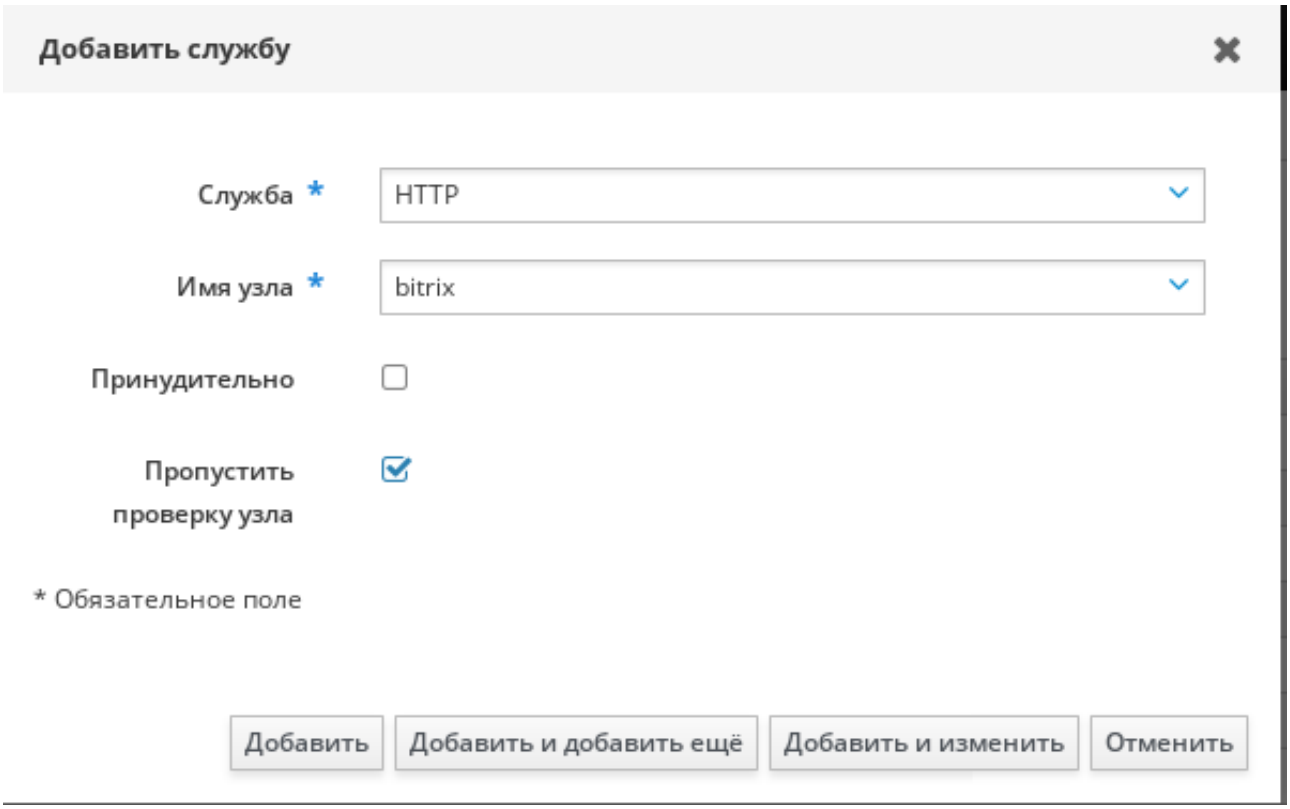

Рисунок 9 — Создание учетной записи для портала Bitrix через интерфейс FreeIPA

5.1.3 Получение keytab-файла

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

```
$ ipa-getkeytab -p HTTP/bitrix.ald.lan@ALD.LAN -k bitrix.keytab
Таблица ключей успешно получена и сохранена в: bitrix.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 bitrix.keytab
-rw------- 1 root root 224 апр 8 11:57 bitrix.keytab

# file bitrix.keytab
bitrix.keytab: Kerberos Keytab file, realm=ALD.LAN, principal=HTTP/bitrix.ald.lan@ALD.
LAN, type=1, date=Mon Apr 8 08:57:37 2024, kvno=1

$ klist -ket bitrix.keytab
Keytab name: FILE:bitrix.keytab
```

```
KVNO Timestamp Principal
---- ------------------ ---------------------------------------------------------
   1 08.04.2024 11:57:37 HTTP/bitrix.ald.lan@ALD.LAN (aes256-cts-hmac-sha1-96)
   1 08.04.2024 11:57:37 HTTP/bitrix.ald.lan@ALD.LAN (aes128-cts-hmac-sha1-96)
```

5.2 Настройки на стороне сервера Bitrix

5.2.1 Установка модуля

Для использования Kerberos-аутентификации веб-сервером Apache установите пакет модуля из стандартного репозитория:

```
yum install -y mod_auth_kerb
```

5.2.2 Настройка Kerberos на сервере для локальных утилит (необязательно)

Следующие настройки необходимо проводить, только если сервер не введён в домен.

Веб-сервер Apache только проверяет Kerberos-билеты, поэтому настройка работы локальных утилит не требуется, но если нужна возможность использовать на этом хосте kinit и другие утилиты в целях отладки, то отредактируйте файл /etc/krb5.conf следующим образом:

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

[realms]
 ALD.LAN = {
   kdc = dc-1.ald.lan
   admin_server = dc-1.ald.lan

 }

[domain_realm]
 .ald.lan = ALD.LAN
 ald.lan = ALD.LAN
```

5.2.3 Настройка веб-сервера Apache на использование аутентификации Kerberos.

Скопируйте bitrix.keytab-файл в каталог /etc/httpd/ и дайте права на чтение:

```
chmod 644 /etc/httpd/bitrix.keytab
```

Создайте файл /etc/httpd/bx/conf/kerberos.conf следующего содержания:

```
Listen 8890

<VirtualHost *:8890>

    ServerAdmin webmaster@localhost
    ServerName bitrix.ald.lan
    ServerAlias *.bitrix.ald.lan
        DocumentRoot /home/bitrix/www
        KeepAlive On

        # Possible values include: debug, info, notice, warn, error, crit, alert,
emerg.
        LogLevel warn
        ErrorLog logs/default_error_log
       #CustomLog logs/default_access_log combined
       #

    <Directory />
        Options FollowSymLinks
        AllowOverride None
    </Directory>

    <DirectoryMatch .*\.(svn|git|hg)/.*>
    Require all denied
        </DirectoryMatch>

    <DirectoryMatch /home/bitrix/www/bitrix/(cache|managed_cache|local_cache|
stack_cache)>
        AllowOverride none
        AddType text/plainsyste
php,php3,php4,php5,php6,phtml,pl,asp,aspx,cgi,dll,exe,ico,shtm,shtml,fcg,fcgi,fpl,asm
x,pht
        php_value engine off
    </DirectoryMatch>

    <DirectoryMatch /home/bitrix/www/(upload|bitrix/images|bitrix/tmp)>
        AllowOverride none
        AddType text/plain
php,php3,php4,php5,php6,phtml,pl,asp,aspx,cgi,dll,exe,ico,shtm,shtml,fcg,fcgi,fpl,asm
x,pht
        php_value engine off
    </DirectoryMatch>

        <Directory /home/bitrix/www/>
                Options FollowSymLinks MultiViews
                AllowOverride All
                DirectoryIndex index.php index.html index.htm

                AuthType Kerberos
                AuthName "Kerberos Login"
                KrbMethodNegotiate On
                #для недоменных - basic
                KrbDelegateBasic On
```

```
                KrbSaveCredentials On
                KrbVerifyKDC Off
                KrbMethodK5Passwd On
                KrbAuthRealms ALD.LAN
                KrbServiceName HTTP/bitrix.ald.lan@ALD.LAN
                Krb5KeyTab /etc/httpd/bitrix.keytab
                Require valid-user

                php_admin_value session.save_path /tmp/php_sessions/www
                php_admin_value upload_tmp_dir /tmp/php_upload/www
        </Directory>

    <Directory /home/bitrix/www/upload/support/not_image>
        AllowOverride none
        Require all denied
            </Directory>

</VirtualHost>
```

Перезапустите веб-сервер командой systemctl reload httpd.

Проверьте работоспособность настроенной аутентификации. Для этого на доменной рабочей станции pc-1.ald.lan войдите под доменным пользователем, который добавлен в группу bitrix-users, и в браузере firefox используйте ссылку http://bitrix.ald.lan:8890/.

В случае настройки SSL-соединения для аутентификации Kerberos по алгоритмам работы Bitrix должен быть настроен ещё один виртуальный хост, работающий на порту 8891 и содержащий корректные настройки SSL. В этом случае ссылка для проверки будет https://bitrix.ald.lan:8891/.

5.2.4 Автоматизация сквозной аутентификации

В системе Bitrix предусмотрен функционал автоматической пересылки запросов на настроенный механизм аутентификации (порт 8890/8891). Для этого в настройках модуля «AD/LDAP интеграция» необходимо «включить переадресацию NTLM-авторизации». При необходимости можно ограничить такую пересылку только для отдельных подсетей.

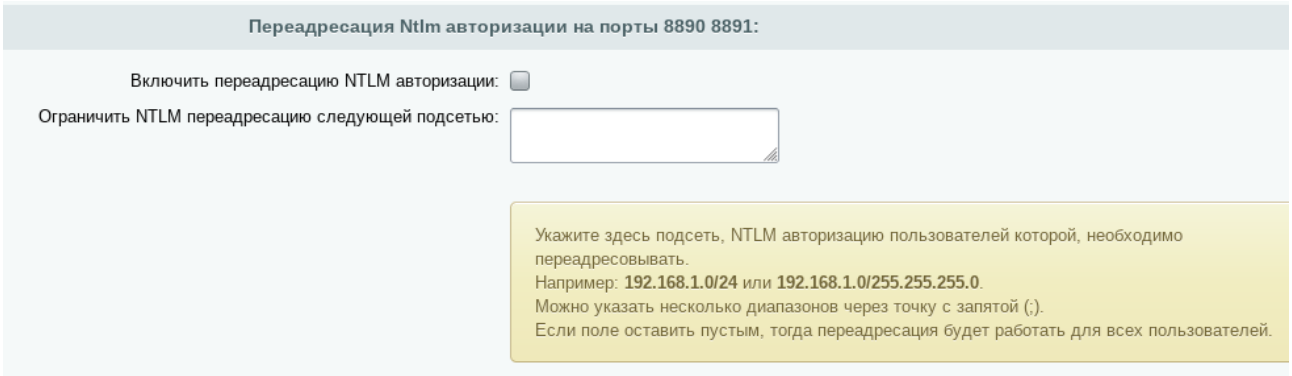

Рисунок 10 — Настройка переадресации на порты 8890 и 8891

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).

```
# 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. Данный пример приводится в инструкции по отладке работы компьютера под управлением Astra Linux в домене ALD Pro (см. раздел «5.3. Доступ к веб-интерфейсам и REST API контроллера домена по протоколу HTTPS» https://life.astralinux.ru/pages/viewpage.action?pageId=176032069).