# Быстрый ввод Astra Linux SE 1.5 в AD Windows

Описание процесса настройки Astra Linux 1.5 SE для ввода в домен Windows. Настройка SAMBA, Winbind, Apache и Postgresql.



---

## Графическая утилита для ввода Astra Linux SE/CE в домен AD

Существует графическая утилита для ввода Astra Linux SE 1.5 и Astra Linux CE 1.11 в домен AD. Для ее использования необходим пакет astra-winbind_1.7-1_all.deb

Пакет можно скачать по указанной выше ссылке, и установить командой:

```
sudo dpkg -i astra-winbind_1.7-1_all.deb
```

Автоматически установить необходимые зависимости:

```
sudo apt-get -f install
```

Скачать утилиту для ввода Astra Linux в домен AD:

fly-admin-ad_0.1.2_amd64.deb

и установить командой:

```
sudo dpkg -i fly-admin-ad_0.1.2_amd64.deb
```

После запуска утилиты, в Главном меню  Настройки  появится утилита "Настройка Active Directory"

> Напоминаем о том, что перед вводом клиента в AD или ALD необходимо корректно настроить сеть.

Копия

Внимание! Если в дальнейшем будет изменятся конфигурационный файл samba, будет выполнено повторное введение в AD или возникнет затруднение, то обязательно потребуется очистка /var/cache/samba/* и /var/lib/samba/*

---

## Ввод Astra Linux в домен Windows

**Исходные данные:**

Контроллер домена:Копия

```
 - dc
 – dev.local
 - Windows Server 2008 R2.
ip - 192.168.1.1
```

Веб-сервер:

```
 – ws3
 - Astra Linux 1.5 SE.   ALD    .       :  ,   Fly,    ,  , .
ip - 192.168.1.3
```

## Разблокирование суперпользователя (root)

Для более удобной работы разблокируем учётную запись root:

```
sudo passwd –u root
```

Назначим пароль для учётной записи root:

```
sudo passwd root
```

root разблокирован. Можно использовать su или перезайти root-ом. Можно не использовать учётную запись root, а команды выполнять с использованием sudo. По завершении настроек учётную запись root необходимо заблокировать!

## Настройка сети

В начало файла /etc/hosts добавить строки:

**/etc/hosts**

```
192.168.1.3        ws3.dev.local ws3
127.0.0.1        localhost
```

Строку с 127.0.1.1 ws3 удалить.

Убедиться, что в файле /etc/hostname правильно указано имя машины:

**/etc/hostname**

```
ws3
```

Назначим статический ip-адрес. В файл /etc/network/interfaces добавить строки:

**/etc/network/interfaces**

```
auto eth0
iface eth0 inet static
address 192.168.1.3
gateway 192.168.1.1
netmask 255.255.255.0
```

Создать файл /etc/resolv.conf и добавить строки:

**/etc/resolv.conf**

```
domain dev.local
search dev.local
nameserver 192.168.1.1
```

Перезапустим сетевую службу:

```
sudo service networking restart
```

Просмотреть доступные сетевые интерфейсы и назначенные адреса:

```
ip a
```

с ws3 можно проверить отклик контроллера домена по протоколу icmp по имени:

```
ping dc.dev.local
```

Синхронизируем время с контроллером домена:

```
sudo ntpdate dc.dev.local
```

## Установка требуемых пакетов

Проверить установлены ли samba, winbind, ntp, apache2 и postgresql:

```
sudo dpkg -l samba winbind ntp apache2 postgresql
```

Установить дополнительные пакеты (потребуется диск с дистрибутивом):

```
sudo apt-get install nscd nslcd libpam-winbind libpam-krb5 libapache2-mod-
auth-kerb php5 php5-pgsql php5-sybase php5-ldap libsasl2-modules-ldap
libsasl2-modules-gssapi-mit krb5-user
```

Выполнить команду:

```
sudo ldconfig
```

## Настройка конфигурационных файлов

Редактируем файл /etc/krb5.conf и добавляем недостающую информацию в соответствующие разделы:

```
[libdefaults]
    default_realm = DEV.LOCAL
    krb4_config = /etc/krb.conf
    krb4_realms = /etc/krb.realms
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true
    v4_instance_resolve = false
    v4_name_convert = {
        host = {
            rcmd = host
            ftp = ftp
        }
        plain = {
            something = something-else
        }
    }
    fcc-mit-ticketflags = true
    [realms]
    DEV.LOCAL = {
        kdc = dc.dev.local
        admin_server = dc.dev.local
        default_domain = dev.local
    }
    [domain_realm]
    .dev.local = DEV.LOCAL
    dev.local = DEV.LOCAL
    [login]
    krb4_convert = true
    krb4_get_tickets = false
```

Редактируем файл /etc/samba/smb.conf. Если каких-то параметров нет, то добавляем:

```
[global]
workgroup = DEV
realm = DEV.LOCAL
os level = 0
invalid users = root
load printers = no
show add printer wizard = no
printcap name = /dev/null
disable spoolss = yes
dns proxy = no
security = ads
kerberos method = secrets and keytab
dedicated keytab file = /etc/krb5.keytab
encrypt passwords = true
domain logons = no
socket options = TCP_NODELAY
local master = no
domain master = no
preferred master = no
idmap config * : range = 10000-20000
idmap config * : backend = tdb
template shell = /bin/bash
template homedir = /home/%D/%U
winbind enum groups = yes
winbind enum users = yes
winbind use default domain = yes
winbind offline logon = yes
winbind refresh tickets = yes
```

Внимание! Если в дальнейшем будет изменятся конфигурационный файл samba, обязательно требуется очистка /var/cache/samba/* и /var/lib/samba/*

Проверим нет ли ошибок в конфигурации samba, выполнив команду:

```
testparm
```

Редактируем файл /etc/security/limits.conf. Добавляем в конец:

**/etc/security/limits.conf**

```
* - nofile 65536
root - nofile 65536
```

Выполнить команду:

```
ulimit -n 65536
```

Радактируем файл /etc/nsswitch.conf:

```
passwd: compat winbind
group: compat winbind
shadow: compat
hosts: files dns
networks: files
protocols: db files
services: db files
ethers: db files
rpc: db files
netgroup: nis
```

Редактируем файл /etc/pam.d/common-session. Добавляем в конец:

```
session optional pam_mkhomedir.so skel=/etc/skel/ umask=0077
```

Перезапустим службы:

```
sudo service samba restart
sudo service winbind restart
sudo service ntp restart
sudo service nscd restart
sudo service nslcd restart
```

Вводим Astra Linux в домен windows (требуется учётная запись администратора домена):

```
sudo net ads join -U Administrator
```

В результате успешного выполнения предыдущей команды должен появиться файл /etc/krb5.keytab. Просмотреть список принципалов в этом файле можно командой:

```
sudo net ads keytab list
```

Позволим остальным читать файл /etc/krb5.keytab:

```
sudo chmod 0644 /etc/krb5.keytab
```

Добавим в автозапуск:

```
sudo insserv -v /etc/init.d/apache2
sudo insserv -v /etc/init.d/samba
```

Проверить установлен ли Postgresql в автозагрузку:

```
chkconfig --list postgresql
```

Перезагрузим ОС:

```
sudo reboot
```

Проверим загрузились ли требуемые службы:

```
sudo service samba status
sudo service winbind status
sudo service nscd status
sudo service nslcd status
sudo service apache2 status
sudo service postgresql status
```

Проверим связь с доменом и работу служб, последовательно выполнив команды:

```
sudo net ads testjoin
sudo wbinfo –p
sudo wbinfo –t
sudo wbinfo –u
sudo getent passwd | grep DEV
```

Проверим Kerberos. Попробуем получить tgt для доменного пользователя:

```
kinit Administrator
klist
kdestroy
```

## Настройка Apache и Postgresql на работу с Kerberos

Редактируем файл /etc/apache2/sites-available/default. Настраиваем директорию на использование Kerberos:

```
<Directory /var/www/>
    AuthType Kerberos
    KrbServiceName host/ws3.dev.local@DEV.LOCAL
    Krb5Keytab /etc/krb5.keytab
    KrbMethodK5Passwd off
    KrbLocalUserMapping on
    KrbSaveCredentials on
    Require valid-user
</Directory>
```

Принципал, задаваемый параметром KrbServiceName, должен быть в файле таблицы ключей /etc/krb5.keytab. Проверить можно командой:

```
net ads keytab list
```

Назначим права для пользователя www-data, от имени которого работает Apache, для доступа к macdb и к файлу таблицы ключей:

```
usermod -a -G shadow www-data
setfacl -d -m u:www-data:r /etc/parsec/macdb
setfacl -R -m u:www-data:r /etc/parsec/macdb
setfacl -m u:www-data:rx /etc/parsec/macdb
setfacl -m u:www-data:r /etc/krb5.keytab
```

Всем доменным пользователям, которым требуется доступ к веб-серверу, необходимо назначить метки безопасности:

```
sudo pdpl-user -z domain_user
```

Перезапустим Apache:

```
sudo service apache2 restart
```

Редактируем файл /etc/postgresql/9.4/main/postgresql.conf.:

```
listen_addresses = '*'
krb_server_keyfile = '/etc/krb5.keytab'
krb_caseins_users = off
```

Редактируем файл /etc/postgresql/9.4/main/pg_hba.conf:

```
local all all peer
host all all 192.168.1.0/24 gss
```

Назначим права для пользователя postgres, от имени которого работает Postgresql, для доступа к macdb и к файлу таблицы ключей:

```
sudo usermod -a -G shadow postgres
sudo setfacl -d -m u:postgres:r /etc/parsec/macdb
sudo setfacl -R -m u:postgres:r /etc/parsec/macdb
sudo setfacl -m u:postgres:rx /etc/parsec/macdb
sudo setfacl -m u:postgres:r /etc/krb5.keytab
```

Перезапустим Postgresql:

```
sudo service postgresql restart
```

На контроллере домена dc нужно добавить принципала к учётной записи машины ws3, для чего выполнить команду от имени администратора:

```
sudo setspn -A postgres/ws3.dev.local ws3
```

Если пользователь root был разблокирован, то его необходимо заблокировать выполнив команду:

```
sudo usermod –e 1 root
```