**Настройка сервера ALD**

1. Установим службу ALD и дополнительные пакеты к нему:

sudo apt install fly-admin-ald-server ald-server-common smolensk-security-ald ald-client-common fly-admin-ald-client

Пакет smolensk-security-ald необходим для ALD для управления мандатными привилегиями в Astra Linux Special Edition.

Если без мандатных привилегий, то достаточно пакета ald-server-common.   
Пакеты fly-admin-ald-server и fly-admin-ald-client — это графические пакеты управления сервером и клиентом соответственно.

1. Сконфигурируем сервер ald:

укажем в файле конфигурации /etc/ald/ald.conf следующие параметры:

DOMAIN=.test.ru

SERVER=srv1.test.ru

TICKET\_MAX\_LIFE=7d

TICKET\_MAX\_RENEWABLE\_LIFE=14d

SERVER\_ON=1

CLIENT\_ON=1

инициализировать домен командой ald-init init

1. Согласимся с перенастройкой параметров домена,   
   дважды введем главный пароль к БД Kerberos и пароль администратора домена ALD.   
     
   Данную операцию желательно проводить не удалённо, а непосредственно на сервере домена, так как для генерации ключей домена может потребоваться переместить манипулятор типа «мышь», чтобы обеспечить датчик случайных чисел нужными входными данными. Удалённый запуск данной процедуры может завершиться по таймауту (5 мин.).
2. Домен создан, далее необходимо зайти в настройку домена используя команду:

fly-admin-ald-server

1. Соединиться с доменом, нажав на пиктограмму подключения, и ввести пароль администратора домена ALD.
2. Ввести необходимые машины в домен, создать учетные записи пользователей, мандатный контекст.
3. Убедиться, что у всех принципалов (учётных записей) домена время жизни билета kerberos установлено в пять дней, для этого выполним команду

for i in `kadmin -p admin/admin -w пароль\_домена -q "listprincs"`; do kadmin -p admin/admin -w пароль\_домена -q "getprinc $i" |egrep &apos;Principal| life&apos;;done

1. Если в результате выполнения данной команды на экран выводится хотя бы одно значение параметра «Maximum ticket life:», отличное от значения «5 days», то необходимо выполнить команду по смене максимального времени жизни билета Kerberos

for i in `kadmin -p admin/admin -w пароль\_домена -q "listprincs"`; do kadmin -p admin/admin -w пароль\_домена -q "modprinc -maxlife 5days $i";done

1. На всех серверах рекомендуется увеличить ограничение по количеству открытых файлов. Для этого в файле /etc/security/limits.conf изменим параметры

soft nofile 2048 hard nofile 4096