Служба Astra Linux Directory

Astra Linux Directory в Astra Linux Special Edition версии 1.2

Служба Astra Linux Directory (ALD) представляет собой систему управления ЕПП. Таким образом, ALD является надстройкой над технологиями LDAP, Kerberos 5, CIFS и обеспечивает автоматическую настройку всех необходимых файлов конфигурации служб, реализующих перечисленные технологии, а так же предоставляет интерфейс управления и администрирования. Все необходимые компоненты службы ALD входят в состав следующих пакетов:

– `ald-client` — клиентская часть ALD. Содержит утилиту конфигурирования клиентского компьютера ald-client и утилиту автоматического обновления пользовательских билетов -renew-tickets. Пакет должен устанавливаться на все клиентские компьютеры, входящие в домен;

– `ald-admin` — содержит утилиту ald-admin и утилиту администрирования БД ALD. Пакет должен устанавливаться на компьютеры, с которых будет осуществляться администрирование БД ALD. При установке данного пакета также устанавливается клиентская часть;

– `ald-server` — серверная часть ALD. Содержит утилиту конфигурации сервера ald-init. Пакет должен устанавливаться на сервер домена. При установке данного пакета также устанавливается ald-admin и, соответственно, клиентская часть. В руководстве man подробно описаны все возможности указанных утилит.

Для поддержки централизации хранения атрибутов СЗИ в распределенной сетевой среде предназначены дополнительные пакеты ALD, первая часть наименования которых соответствует одному из основных пакетов:

– `ald-client-parsec` — расширение, необходимое клиентской части ALD; – ald-admin-parsec — расширение утилиты администрирования БД ALD;

– `ald-server-parsec` — расширение, необходимое для организации хранения атрибутов СЗИ на сервере ALD;

Без установки пакетов расширения совместно с соответствующими основными пакетами невозможна централизация хранения атрибутов СЗИ в распределенной сетевой среде, что может привести к невозможности входа пользователей в систему. В состав ОС входит графическая утилита fly-admin-ald, которая позволяет администратору произвести управление ЕПП в графическом режиме (см. электронную справку).

Настройка

Настройка всех компонентов ALD осуществляется автоматически утилитами конфигурирования. Настройки сервера и клиентов ALD содержатся в файле /etc /ald/ald.conf. После изменения данного файла необходимо выполнить команду commit-config для того, чтобы изменения вступили в силу:
ald-init commit-config (на сервере)
ald-client commit-config (на клиентах)
Формат файла: ИМЯ_ПАРАМЕТРА=значение # Комментарий
В файле для системы ALD задаются следующие параметры:

– VERSION — для текущей версии должно быть установлено значение 1.3; – DOMAIN — имя домена. Должно быть задано в формате: .example.ru

для сервера ALD. Если данный параметр меняется, то необходимо заново инициализировать сервер командой:

```
ald-init init
```

Можно также воспользоваться командами:

```
ald-init backup-ldif ald-init restore-backup-ldif
```

для переименования домена;

– SERVER — полное имя серверного компьютера ALD.

Пример

```
my-server.example.ru MINIMUM_UID
```

Минимальный номер глобального пользователя. Пользователи с номером меньше данного считаются локальными и аутентифицируются через локальные файлы /etc/passwd и /etc/shadow.

> **Примечание**
>
> Для нормальной работы домена не рекомендуется пересечение по номерам локальных и глобальных пользователей и групп. Не рекомендуется задавать MINIMUM_UID меньше 1000;

– TICKET_MAX_LIFE=10h — максимальное время жизни билета Kerberos (если его не обновлять). Формат параметра: NNd (дни), или NNh (часы), или NNm (минуты).
При входе в домен пользователь получает билет. При выходе из домена билет уничтожается. Если билет не обновлять, то после истечения срока действия билета пользователь потеряет доступ к своему домашнему каталогу. Чтобы восстановить доступ, ему придется выполнить команду kinit или зайти в систему заново. Чтобы доступ не был потерян, билет следует периодически обновлять (до истечения срока действия). Настроить автоматическое обновление можно с помощью утилиты ald-renew-ticket.
Для удобства можно настроить данный параметр на большое количество времени, например 30d. Но это менее безопасно;
– TICKET_MAX_RENEWABLE_LIFE=7d — максимальное обновляемое время жизни билета Kerberos. Формат параметра: NNd (дни), или NNh (часы), или NNm (минуты).
По истечении данного срока билет не может быть обновлен. Данный параметр должен быть больше, чем параметр TICKET_MAX_LIFE.

> **Примечание**
>
> Для клиентских компьютеров параметры TICKET_MAX_LIFE и TICKET_MAX_RENEWABLE_LIFE определяются как наименьшие значения этих параметров, заданных в файлах ald.conf на сервере и на клиентском компьютере;

– NETWORK_FS_TYPE — определяет, какая сетевая ФС будет использоваться для глобальных пользовательских домашних каталогов. Возможные значения:

– none — сетевая ФС не используется. Работает только аутентификация глобальных пользователей. Используются локальные домашние каталоги пользователей. (Следующие параметры, относящиеся к сетевой ФС, игнорируются);

– cifs — используется Samba/CIFS;

– SERVER_EXPORT_DIR — (только для сервера). Задает абсолютный путь к каталогу на сервере, где будет располагаться хранилище домашних каталогов. Данный каталог будет экспортирован по Samba/CIFS;
– CLIENT_MOUNT_DIR — задает абсолютный путь к точке монтирования хранилища домашних каталогов на клиентских компьютерах;
– SERVER_FS_KRB_MODES — (только для сервера). Задает режимы экспорта сервера Samba/CIFS (перечисленные через запятую). Возможные режимы:

– krb5 — только Kerberos-аутентификация;

– krb5i — (integrity) аутентификация и проверка целостности (подпись) пакетов.

Должен быть указан хотя бы один режим;
– CLIENT_FS_KRB_MODE — задает Kerberos-режим монтирования на клиентском компьютере. Должен быть указан один из режимов: krb5 или krb5i;
– SERVER_ON — включает/выключает сервер. Присвоенное значение может быть 0 или 1.
Если на клиентском компьютере SERVER_ON=0, это аналогично CLIENT_ON=0. Если на сервере SERVER_ON=0, то:

– домашние каталоги не экспортируются; – разрешение имен по LDAP выключается в nsswitch.conf; – все принципалы Kerberos деактивируются (allow_tickets=0); – службы LDAP, Samba, Kerberos, nss-ldapd останавливаются; – служба nscd перезапускается;

– CLIENT_ON — включает/выключает клиентскую часть ALD. Присвоенное значение может быть 0 или 1. Если CLIENT_ON=0, то:

– домашние каталоги не монтируются; – разрешение имен по LDAP выключается в nsswitch.conf; – служба nscd перезапускается.

Пример файла /etc/ald/ald.conf:

```
VERSION=1.3
DOMAIN=.example.ru
SERVER=my-server.example.ru
MINIMUM_UID=2500
TICKET_MAX_LIFE=10h
TICKET_MAX_RENEWABLE_LIFE=7d
NETWORK_FS_TYPE=cifs
SERVER_EXPORT_DIR=/ald_export_home
CLIENT_MOUNT_DIR=/ald_home
SERVER_FS_KRB_MODES=krb5,krb5i
CLIENT_FS_KRB_MODE=krb5i
SERVER_ON=1
CLIENT_ON=1
```