ЛАБОРАТОРНАЯ РАБОТА №8. КОНФИГУРИРОВАНИЕ СЛУЖБЫ ASTRA LINUX DIRECTORY.

Цель работы: Получить практический опыт установки и настройки параметров службы *Astra Linux Directory* (*ALD*) в ОССН.

Время выполнения работы: 6 академических часов.

Краткие теоретические сведения

В компьютерных сетях, построенных на основе ОССН, имеется возможность организовать централизованное хранение учётных записей пользователей в домене *ALD* (далее – домене), а также развёртывать централизованный защищённый файловый сервер, содержащий сетевые домашние каталоги данных учётных записей пользователей. Таким образом, у учётных записей пользователей *ALD* появляется возможность регистрации и доступа к своим сетевым объектам с любого компьютера, входящего в домен. Это особенно актуально, в случае территориальной удалённости между контроллером *ALD* и компьютерами, входящими в состав домена.

Хотя в ОССН версии 1.6 также реализована более современная доменная инфраструктура *FreeIPA*, которая подробно рассмотрена в главах 1 и 3, её конфигурирование и настройка являются гораздо более сложными, чем *ALD*, и поэтому выходят за рамки лабораторной работы.

Администратор домена *ALD* выполняет следующие функции по управлению доменом:

- централизованное управление учётными записями пользователей домена с использованием команды *ald-admin* и графической утилиты «Политика безопасности» (для этого необходимо установить расширение *smolensk-security-ald*);
- настройка СЗИ, управляющих их доступом к файловым сущностям защищённого файлового сервера.

Централизованная база данных учётных записей пользователей домена (*DIB – Domain Information Base*) создаётся на основе службы *LDAP* (*Lightweight Directory Access Protocol*), обеспечивающей, как организацию хранилища учётных записей пользователей *ALD*, так и процедуру аутентификации пользователей на компьютере с использованием *ALD*. Безопасность процедуры аутентификации пользователей домена обеспечивается

применением протокола доверенной аутентификации *Kerberos*. Для синхронизации временных меток при взаимодействии контроллера и клиентов *Kerberos* используется протокол *NTP* (*Network Time Protocol*).

При доступе к сущностям файловой системы компьютера, с которого осуществлён вход в домен с некоторой учётной записью пользователя, для неё применяются настройки управления доступом, хранящиеся на контроллере *ALD*. Если же на контроллере *ALD* (или на специально выделенном компьютере) организуется защищённый файловый сервер, то настройки управления доступом для этой учётной записи пользователя применяются также к сущностям файловой системы этого контроллера. При этом доступ к ним от имени учётной записи пользователя *ALD* осуществляется по протоколу *CIFS* (*Common Internet File System*), являющемуся развитием протокола сетевого файлового обмена *SMB*.

Служба *ALD* обладает расширяемой архитектурой, состоящей из ядра, отвечающего за основной функционал системы, ряда интерфейсов (*LDAP*, *Kerberos*) и модулей расширения, команд и графических утилит настройки служб и подсистем *ALD*, что позволяет расширять функциональность *ALD*, устанавливая дополнительные пакеты. Основные пакеты, используемые при установке и настройке *ALD*, являются:

- *ald-client-common* – клиентская часть *ALD* (можно также использовать метапакет *ald-client*);
- *ald-admin* – команды администрирования *ALD*;
- *ald-server-common* – серверная часть *ALD* (можно также использовать метапакет *ald-server*);
- *smolensk-security-ald* – расширения графической утилиты «Политика безопасности», позволяющие осуществлять управление доменом (можно также использовать метапакеты *ald-admin-ald-se* или *ald-admin-ald-server*).

На компьютере, осуществляющем функции контроллера *ALD*, операции по администрированию *ALD* выполняются от имени учётных записей пользователей, обладающих соответствующими административными полномочиями. В зависимости от назначенных привилегий администраторов *ALD* можно разделить на следующие группы по полномочиям:

- корневой администратор (имя *admin*/*admin*, администратор *ALD*) – обладает всеми полномочиями по управлению доменом;
- администраторы (пользователи с привилегией *admin*) – обладают полномочиями по управлению конфигурацией домена и учётными записями пользователей;
- ограниченные администраторы (учётные записи пользователей с привилегиями *hosts-add* или *ald-hosts-add*) – обладают полномочиями по добавлению компьютеров в домен;

- пользователи утилит администрирования (пользователи с привилегией *adm-user*) – обладают полномочиями по запуску утилит администрирования;
- обычные пользователи.

Для администрирования домена используются команды *ald-admin* и графическая утилита «Политика безопасности», которая позволяет выполнять следующие действия с доменом:

- создание и администрирование учётных записей пользователей;
- создание и администрирование групп;
- добавление и удаление компьютеров;
- резервирование и восстановление учётной информации баз данных домена;
- конфигурирование привилегий и политик СЗИ для учётных записей пользователей и групп;
- конфигурирование политик паролей *Kerberos*;
- администрирование доступа к съёмным устройствам;
- администрирование учётных записей сетевых служб (сервисов);
- контроль целостности (аудит) конфигурации домена.

При создании нового домена используется следующая последовательность действий:

- настройка сетевого соединения на контроллере *ALD* и компьютерах, которые будут включены в *ALD*;
- настройка именования контроллера и клиентов *ALD* для поддержки функционирования службы *LDAP*;
- конфигурирование и запуск контроллера *ALD*;
- запуск клиентов *ALD* на компьютерах, входящих в *ALD*.

Данная последовательность действий рассматривается при выполнении лабораторной работы.

При развёртывании средств обеспечения единого пространства пользователей с применением *ALD* используются следующие команды (примеры применения которых также рассмотрены в главе 3):

- *hostname* — команда вывода в терминал текущего имени компьютера;
- *apt-get* — команда управления пакетами;
- *ping* — команда отправки и получения пакетов *ICMP* (*Echo Request*/ *Echo Reply*);
- *ald-init* — команда инициализации базы данных *ALD*;
- *ald-client* — команда управления клиентом *ALD*;
- *ald-admin* — команда управления доменом *ALD*.

Используемое методическое и лабораторное обеспечение

1. Три компьютера с ОССН версии 1.6, объединённые в сеть. Первый предназначен для использования в качестве контроллера *ALD* — далее обозначается *gw.exampleX.com*; остальные — компьютеры, подключаемые в домен (*server.exampleX.com*, u*ser.exampleX.com*). В ОССН настроена синхронизация времени с использованием протокола *NTP*, либо, при использовании виртуальных машин временные метки считываются автоматически из единого системного времени.
2. В каждой ОССН создана учётная запись пользователя *student*, с параметрами: максимальный и минимальный уровни доступа — 0, неиерархические категории — нет, уровень целостности – «Высокий», входит в группу администраторов — *astra-admin* (вторичная группа), разрешено выполнение привилегированных команд (*sudo*).
3. Дистрибутив ОССН.
4. Документация: «Операционная система специального назначения «*Astra Linux Special Edition*». Руководство администратора. Часть 1», «Операционная система специального назначения «*Astra Linux Special Edition*». Руководство по КСЗ. Часть 1».
5. Для выполнения работы в течение двух занятий необходимо обеспечить возможность сохранения состояния ОССН за счёт применения технологий виртуализации (создания виртуальных машин с ОССН).

Порядок выполнения работы

1. Для настройки сетевого соединения на контроллере и клиентах *ALD* начать работу со входа в ОССН *server*, u*ser* и *gw* в графическом режиме с учётной записью пользователя *student* (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»).
2. В ОССН *server*, *user* и *gw* выполнить настройку статических сетевых адресов в соответствии с предыдущим модулем.
3. Выполнить перезагрузку и повторный вход в каждую ОССН с учётной записью пользователя *student* (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»), затем запустить терминал *Fly*.
4. Выполнить проверку корректности настроек командой *ping*. При этом проверить доступность *server*, *user* с *gw* по сети командами: *ping* 192.168.X.2 и *ping* 192.168.X.Y.
5. Выполнить настройку имени контроллера и клиентов *ALD* для поддержки функционирования службы *LDAP*. Для этого необходимо, чтобы разрешение сетевых имён было настроено таким образом, чтобы сетевое имя компьютеров разрешалось, в первую очередь, как полное имя (например, g*w.exampleX.com*). При этом команда

hostname должна возвращать короткое сетевое имя (например, g*w*). Для этого выполнить следующую последовательность действий:

- в ОССН *server*, *user* и *gw* в «привилегированном» режиме терминала *Fly* выполнить проверить настройки файла */etc/hostname в соответствии с предыдущей лабораторной работой*;
- в ОССН *server*, *user* и *gw* в «привилегированном» режиме *проверить настройки файла /etc/hosts в соответствии с предыдущей лабораторной работой* и закомментировать строку, содержащую запись «127.0.1.1» (для этого поставить в начале данной строки «#»);
- выполнить перезагрузку ОССН *server*, *user* и *gw* и войти в ОССН в графическом режиме с учётной записью пользователя s*tudent* (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»);
- в каждой ОССН запустить терминал *Fly*, выполнить команду *hostname* и проверить, что она возвращает короткие имена *server*, *user* и *gw* .

```
root@gw:~# hostname
gw
root@gw:~#
```

6. Выполнить установку, конфигурирование и запуск контроллера. Для этого реализовать следующую последовательность действий в ОССН *gw*:

- войти в графическом режиме с учётной записью пользователя *student* (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»);
- запустить терминал *Fly* в «привилегированном» режиме командой *sudo fly-term*;
- выполнить установку пакетов для работы с контроллером (если ALD сервер н был установлен при инсталляции ОС) командой:

 # apt -y install ald-server-common ald-admin-common ald-admin smolensk-security-ald fly-admin-ald-server

- при наличии ошибок запустите команду:

 # apt --fix-broken install

- перезагружаем ОС;
- выполнить команду *vim /etc/ald/ald.conf* и проверить наличие параметров «*SERVER*=gw*.exampleX.com*» и «*DOMAIN*=*.exampleX.com*»;

```
VERSION=1.7
# Version of ald


DOMAIN=.example2.com
# The name of your domain (also used as Kerberos realm in upper-case).
# Should be in the form:
# .example.com
# !NOTE! (for ald-server). If this value is changed - the server should be
# reinitialized by:
# $ ald-init init
# Or you should use the commands 'ald-init backup-ldif' and
# 'ald-init restore-backup-ldif'.


SERVER=gw.example2.com
# Fully qualified name of Astra Linux Directory server.
# Should be in the form:
# my-ald-server.example.com


SERVER_ID=1
```

- также проверьте в файле наличие параметра SERVER_ON=1 и CLIENT_ON=1, при необходимости сделайте изменения;
- для того, чтобы служба *ALD* заново считала изменения в файле */etc/ald/ald.conf* (если они реально делались, иначе пропустить указанную далее команду) выполнить инициализацию командой *ald-init commit-config* (результатом будет информация об успешном конфигурировании службы *ALD*);

```
root@gw:~# vi /etc/ald/ald.conf
root@gw:~# ald-init commit-config
ВНИМАНИЕ! Некоторые необходимые сервисы (OpenLDAP, Kerberos, nslcd, nscd) могут быть перез
апущены!
Выполнение smbstatus -d 0 -p
Продолжить? (yes/no) [no]: yes
Обработка шаблона конфигурационного файла '/etc/ald/config-templates/ldap.conf' в '/etc/ld
ap/ldap.conf'...
Переименование '/etc/ldap/ldap.conf' в '/etc/ldap/ldap.conf.before_ald'...
Переименование '/etc/ldap/ldap.conf.tmp' в '/etc/ldap/ldap.conf'...
Обработка шаблона конфигурационного файла '/etc/ald/config-templates/krb5.conf' в '/etc/kr
b5.conf'...
```

- выполнить команду инициализации *ald-init init* и по требованию этой команды подтвердить повторную инициализацию баз данных *LDAP* и *Kerberos*, ввести и подтвердить новый *Kerberos*-пароль «*kerberosroot*», ввести и подтвердить новый пароль администратора *ALD* «*aldroot*».

```
root@gw:~# ald-init init
ВНИМАНИЕ! Команда 'init' УНИЧТОЖИТ ВСЮ БАЗУ ДАННЫХ LDAP и Kerberos!
Также во время выполнения этой команды могут быть остановлены и перезапущены LDAP, Kerbero
s, NFS/Samba и некоторые другие службы.
Разыменованное имя компьютера: gw.example2.com

Контроллер домена '.example2.com' будет создан со следующими параметрами:
Сервер: gw.example2.com
Роль сервера: Первичный контроллер домена
ID сервера: 1
Первичный контроллер домена: gw.example2.com

Вы УВЕРЕНЫ, что хотите ВЫПОЛНИТЬ эту операцию? (yes/no) [no]: yes
Введите новый главный пароль к базе данных Kerberos (НЕ ЗАБУДЬТЕ ЕГО!): ********
Повторите пароль: ********
Введите новый пароль администратора Astra Linux Directory (НЕ ЗАБУДЬТЕ ЕГО!): ********
Повторите пароль: ********
Сохранение конфигурации...
Обработка конфигурационного файла '/etc/ald/ald.conf'...
```

.....

```
Обработка конфигурационного файла '/etc/exports'...
Переименование '/etc/exports.tmp' в '/etc/exports'...
Запуск сервиса nmbd...
Запуск сервиса smbd...
Перезапуск сервиса nscd...
Перезапуск сервиса nslcd...
Перезапуск сервиса aldd...

Astra Linux Directory сконфигурирована.
Сервер ALD активен.
Клиент ALD включен.

Astra Linux Directory сервер успешно инициализирован.
```

- Правильно ли установился сервер можно проверить с помощью следующих команд **ald-client status** и **ald-admin test-integrity**

```
student@gw:~$ sudo su -
root@gw:~# ald-client status
Текущие установки, основанные на конфигурацонном файле '/etc/ald/ald.conf':
ALDD_USER=aldd
ALD_CC_PREFIX=admin_tickets
ALD_CFG=/etc/ald/ald.conf
ALD_CFG_DIR=/etc/ald/config-templates
ALD_CFG_MODULES_DIR=/usr/lib/x86_64-linux-gnu/ald/config-modules
ALD_CFG_ROOT_DIR=/etc/ald
ALD_CFG_TEMPL_DIR=/usr/share/ald/config-templates
```

.....

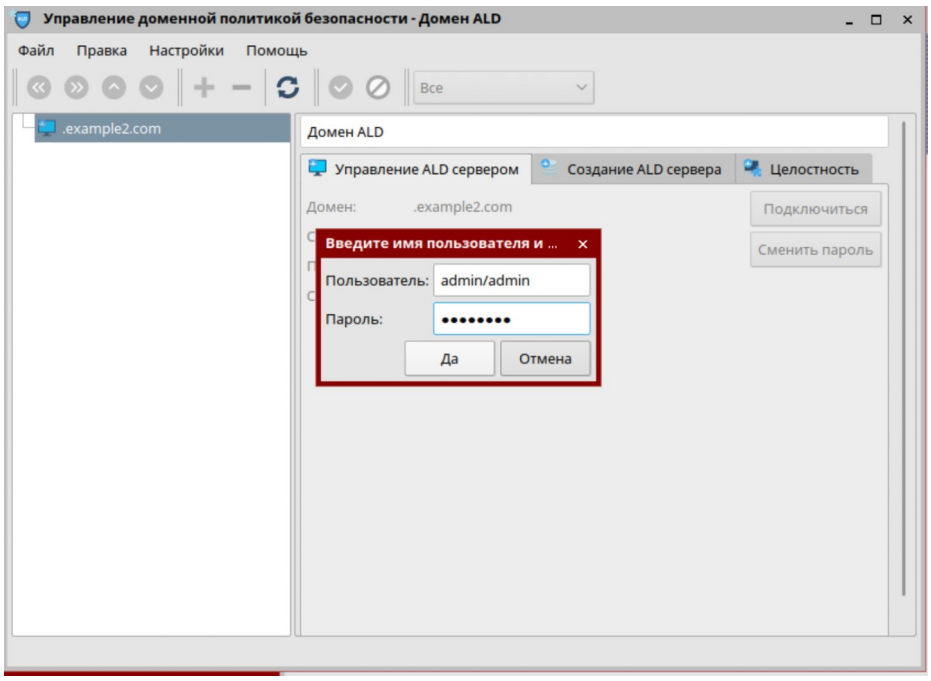
```
USE_DNS=0
USE_DOCUMENTS=1
USE_RPC=1
UTF8_GECOS=1
VALID_GROUP_NAMES=^[A-Za-z][A-Za-z0-9\.\_\-\ ]*$
VALID_USER_NAMES=^[a-z][a-z0-9\.\_\-]*$
VERSION=1.7

Astra Linux Directory сконфигурирована.
Сервер ALD активен.
Клиент ALD включен.
```

```
root@gw:~# ald-admin test-integrity
Введите пароль администратора ALD: ********
Проверка конфигурации домена.....................................ok
Проверка модулей LDAP............................................ok
Проверка индексов LDAP...........................................ok
Проверка ограничений уникальности LDAP...........................ok
Проверка системных принципалов...................................ok
Проверка компьютеров.............................................ok
Проверка имени сервера...........................................ok
Проверка групп компьютеров.......................................ok
Проверка серверов ALD............................................ok
Проверка политик паролей.........................................ok
Проверка пользователей...........................................ok
Проверка групп...................................................ok
Проверка администраторов.........................................ok
Проверка сервисов................................................ok
Проверка групп сервисов..........................................ok
Проверка доменных документов.....................................ok
Проверка доверенных доменов......................................ok
Проверка серверных заданий.......................................ok
Проверка политики регистрации событий по умолчанию.............ok
Проверка политик регистрации событий пользователей.............ok
Проверка групповых политик регистрации событий..................ok
Проверка правил доступа к устройствам............................ok
Проверка устройств...............................................ok
Проверка мандатных уровней.......................................ok
Проверка мандатных категорий.....................................ok
Проверка мандатных прав пользователей............................ok
root@gw:~#
```

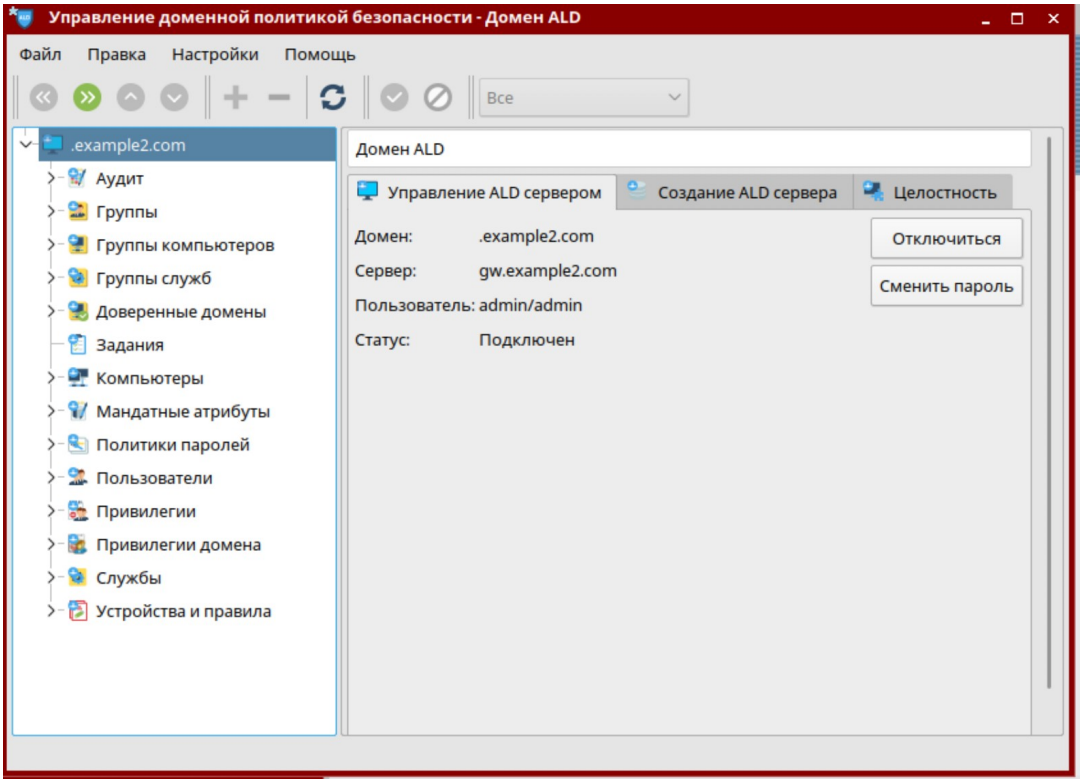
- Если возникают ошибки, следует перезагрузить ОС

7. Если предыдущие команды были выполнены успешно, находясь в графическом режиме на компьютере gw проверьте работу ALD следующим образом:

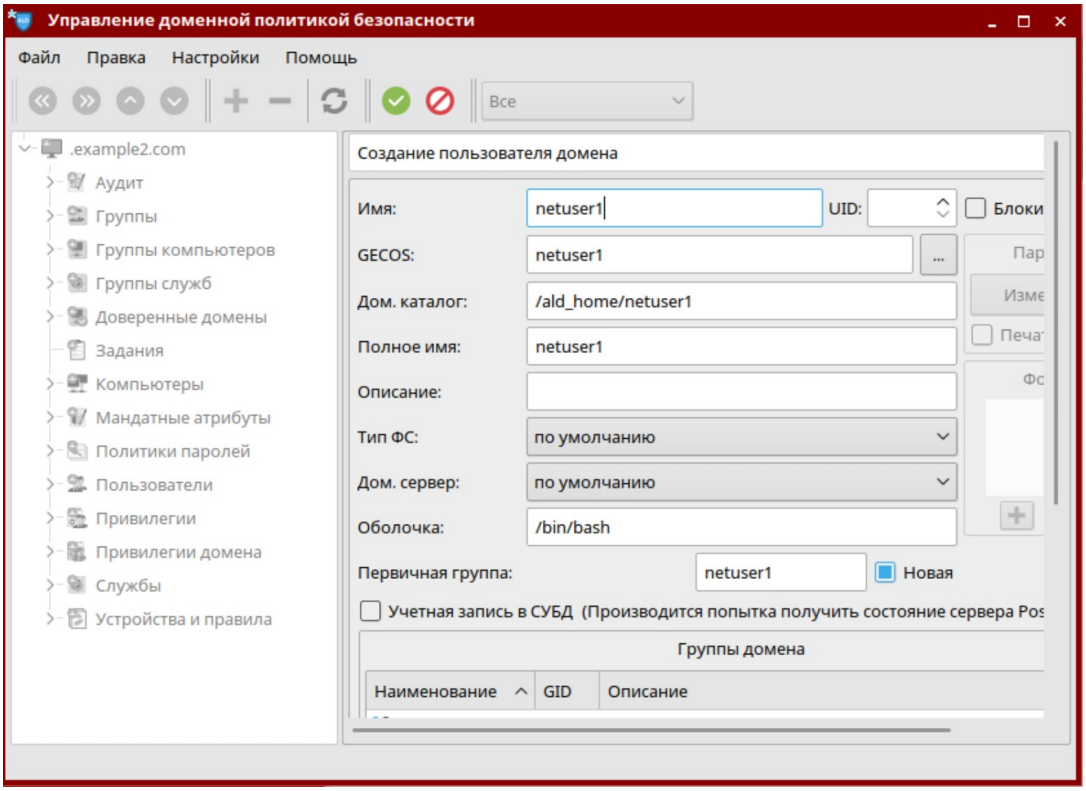
- Открываем на сервере приложение Управление доменной политикой безопасности: Пуск -> Панель управления -> Сеть -> Доменная политика безопасности



- Вводим логин и пароль, который задавали ранее



- Создайте доменного пользователя netuser1 и задайте ему пароль. А Во вкладке Привилегии домена разрешите вход на нужные ПК



- После этого можно выйти из под пользователя student и попробовать зайти в систему под доменным пользователем

8. Следующим шагом необходимо выполнить установку, конфигурирование, запуск клиентов *ALD*. Для этого реализовать следующую последовательность действий:

- в ОССН server запустить терминал *Fly* в «привилегированном» режиме командой *sudo fly-term*;
- выполнить установку пакета *ald-client-common* командой *apt-get install ald-client-common*;
- выполнить команду *nano /etc/ald/ald.conf* и отредактировать следующие параметры: «*SERVER=astra-server.example.ru*» и «*DOMAIN=.example.ru*»;
- выполнить инициализацию настроек и подключение к контроллеру командой *ald-client commit-config*;
- в качестве имени учётной записи пользователя администратора ввести пробел или *admin*/*admin*, далее ввести пароль администратора *ALD aldroot*;
- выполнить запуск клиента *ALD* командами *ald-client start* (для включения компьютера в домен может отдельно использоваться команда *ald-client join*).

1. Осуществить проверку функционирования и настройку контроллера и клиентов *ALD*. Для этого выполнить следующую последовательность действий:

- в ОССН *AstraServer* выполнить установку расширения графической утилиты «Управление политикой безопасности», используемого для конфигурирования контроллера *ALD* командой *apt-get install smolensk-security-ald*;
- запустить графическую утилиту «Политика безопасности» через меню «Панель управления» главного пользовательского меню и открыть вкладку «Домен *ALD*», соответствующую настройкам созданного домена;
- для администрирования домена необходимо выполнить подключение, проверить имя пользователя «*admin*/*admin*», ввести пароль администратора *ALD* «*aldroot*», а затем проверить, что контроллер *ALD* активирован (при этом должна отображаться надпись «Сервер домена: *astra-server.example.ru*»);
- в дереве элементов вкладки политик безопасности контроллера *astra-server.example.ru* выбрать узел «Компьютеры» и проверить, что в состав домена с именем «.*example.ru*» входят контроллер *ALD* «*astra-server.example.ru*» и клиент «*astra-client*1.*example.ru*»;

1. Создать новую учётную запись пользователя *ALD* и осуществить вход с ней в ОССН *AstraClient*1. Для этого осуществить следующие действия:

- в ОССН *AstraServer* запустить графическую утилиту «Политика безопасности» через меню «Панель управления» главного пользовательского меню и открыть вкладку «Домен *ALD*» в разделе «Элементы»;
- осуществить подключение с учётной записью пользователя «*admin*/*admin*»;
- в дереве элементов вкладки политик безопасности контроллера *astra-server.example.ru* выбрать узел «Пользователи» и создать новую учётную запись пользователя *userald*, при этом, задав её пароль (обратить внимание на требование политики по сложности пароля);
- в учётной записи пользователя *userald* в вкладке «Привилегии домена» выбрать «Компьютеры» добавить только *astra-server.example.ru* и применить изменения;
- в ОССН *AstraClient*1, *AstraClient*2 выйти из ОССН;
- осуществить попытку входа в ОССН *AstraClient*1 с новой учётной записью пользователя *userald* и проанализировать выводимые ошибки;
- теперь в учётной записи пользователя *userald* в вкладке «Привилегии домена» выбрать «Компьютеры» и добавить *astra-client*1*.example.ru*;
- войти в ОССН *AstraClient*1 с учётной записью пользователя *userald*;
- осуществить попытку входа в ОССН *AstraClient*2 с учётной записью пользователя *userald* и проанализировать выводимую ошибку.

1. Осуществить установку, конфигурирование, запуск клиента *ALD* на *AstraClient*2. Для этого выполнить следующую последовательность действий:

- войти в ОССН *AstraClient*2 в графическом режиме с учётной записью пользователя *user* (уровень доступа — 0, неиерархические категории — нет, уровень целостности — «Высокий»);
- запустить терминал *Fly* в «привилегированном» режиме командой *sudo fly-term*;
- выполнить установку пакета *ald-client-common* командой *apt-get install ald-client-common*;
- выполнить подключение к домену командой *ald-client join astra-server.example.ru*;
- проверить корректность модификации файла настройки клиента *ALD*, выполнив команду *head* -25 /*etc*/*ald*/*ald.conf*, при этом должны быть установлены следующие параметры: «*SERVER*=*astra-server.example.ru*» и «*DOMAIN*=.*example.ru*».

1. Проверить корректность включения компьютера *astra-client*2.*example.ru* в домен «.*example.ru*». Для этого выполнить следующую последовательность действий:

- в ОССН *AstraServer* перезапустить графическую утилиту «Политика безопасности», затем открыть вкладку «Домен *ALD*» и выполнить подключение к домену;
- выбрать узел «Компьютеры» и проверить, что в состав домена с именем «.*example.ru*» входит клиент *ALD astra-client2*.*example.ru*;

- открыть узел «Привилегии домена» – «*userald*», в поле «Компьютеры» добавить «*astra-client*2.*example.ru*» к списку разрешённых компьютеров;
- выйти из ОССН.

1. Проверить функционирование сетевой файловой системы при доступе к домашним каталогам учётных записей пользователей *ALD*. Для этого выполнить следующую последовательность действий:

- войти в ОССН *AstraClient*2 в графическом режиме с учётной записью пользователя *userald*;
- в ОССН *AstraClient*2 в графической утилите «Менеджер файлов» открыть каталог «Документы», создать в нем текстовый файл с именем *file-from-al*3.*txt*, затем открыть данный файл в редакторе *Juffed* и добавить строку «Создан на ЦК 3»;
- в ОССН *AstraClient*1 в сессии, функционирующей от имени учётной записи пользователя *userald*, в графической утилите «Менеджер файлов» открыть каталог «Документы» и проверить наличие файла с именем *file-from-al*3.*txt*;
- в ОССН *AstraServer* запустить терминал *Fly* и перейти в каталог */ald_export_home* командой *cd* */ald_export_home*;
- вывести содержимое текущего каталога командой *ls*, проанализировать результат;
- определить дискреционные и мандатные атрибуты каталога *userald* командой *pdp-ls -M*;
- выполнить попытку перехода в каталог *userald* и проанализировать выводимые ошибки;
- запустить терминал *Fly* в «привилегированном» режиме командой *sudo fly-term*, запустить *Midnight Commander* командой *mc* и перейти в каталог */ald_export_home/userald/l*0*i*0*c*0*x*0*t*0*x*0/Документы;
- вывести в терминал содержимое файла *file-from-al*3.*txt* командой *cat file-from-al*3.*txt*.

1. Осуществить настройку политики паролей учётных записей пользователей *ALD*. Для этого выполнить следующую последовательность действий:

- в ОССН *AstraServer* в графической утилите «Политика безопасности» выбрать «Домен *ALD*» (при необходимости выполнить подключение к домену), далее «Политики паролей» – «*default*»;
- во вкладке «Общие» в поле «Минимальная длина» ввести значение 5;
- перейти к узлу «Пользователи» – «*userald*» и сменить пароль на «1234», затем на «*Asdf*1».

1. Создать учётную запись пользователя *ALD* с использованием утилиты *ald-admin*. Для этого выполнить следующую последовательность действий:

- в ОССН *AstraServer* запустить терминал *Fly*;

- создать новую учётную запись пользователя *ALD* командой *ald-admin user-add userald*2, задать новый пароль в соответствии с требованиями политики безопасности (не менее 5 символов): «*Qwer*1»;
- далее все параметры учётной записи пользователя *ALD*, установленные по умолчанию, за исключением последнего (там значение «*yes*»);
- вывести список учётных записей пользователей и компьютеров *ALD* командами *ald-admin user-list* и *ald-admin host-list*, соответственно;
- создать группу компьютеров *ald_host_group*1 со следующим составом: *astra-client*1.*example.ru*, *astra-client*2.*example.ru*, командой *ald-admin hgroup-add ald_host_group*1 *--host=astra-client*1.*example.ru --host=astra-client*2.*example.ru* (также второй узел можно включить в группу командой *ald-admin hgroup-mod ald_host_group*1 *--add-hosts --host=astra-client*2.*example*.*ru*);
- в графической утилите «Политика безопасности» проверить наличие узла «Группы компьютеров/*ald_host_group*1»;
- модифицировать группу компьютеров *ald_host_group*1, добавив в неё компьютер *astra-server.example.ru* командой *ald-admin hgroup-mod ald_host_group*1 *--add-hosts --hosts=astra-server.example.ru*;
- добавить учётной записи пользователя *userald*2 привилегию доступа к группе компьютеров *ald_host_group*1 командой *ald-admin user-ald-cap userald*2 *--host-group=ald_host_group*1 *--add-hosts*;
- в графической утилите «Политика безопасности» проверить наличие компьютера *astra-server.example.ru* в узле «Группы компьютеров» – «*ald_host_group1*» и наличие привилегии доступа к группе компьютеров *ald_host_group*1 у учётной записи пользователя *userald*2;
- проверить возможность входа в ОССН *AstraClient*1 и *AstraClient*2 с учётной записью пользователя *userald*2, после успешной проверки выйти из ОССН *AstraClient*1 и *AstraClient*2.

1. Осуществить проверку целостности и настроек *ALD*, для чего выполнить команду *ald-admin test-integrity* и обратить внимание на выдаваемые предупреждения.
2. Перейти к администрированию учётной записи пользователей домена:

- в ОССН *AstraServer* в графической утилите «Политика безопасности» выбрать «Домен *ALD*»;
- настроить параметры мандатного управления доступом учётной записи пользователя *userald*2: установить в вкладке «МРД» максимальный уровень доступа 3, минимальный — 0;

- настроить параметры мандатного управления доступом учётной записи пользователя *userald*: установить в вкладке «МРД» максимальный уровень доступа 2, минимальный — 0;
- для проверки войти в ОССН *AstraClient*1 в графическом режиме с учётной записью пользователя *userald* (уровень доступа — 2, неиерархические категории — нет, уровень целостности — «Низкий»);
- выполнить команду *ald-admin test-integrity* и проверить отсутствие предупреждений.

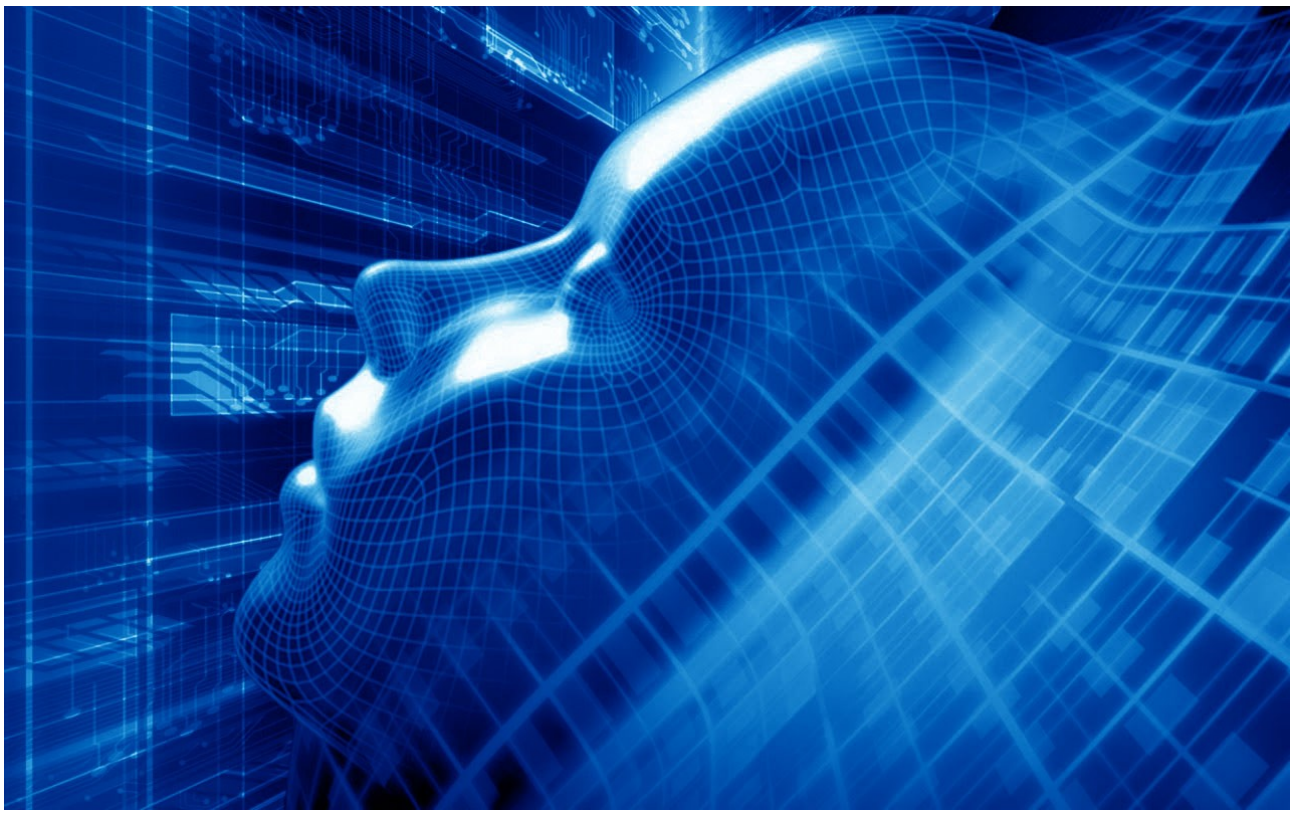
1. Выполнить проверку функционирования единого задания устройств в *ALD*:

- в ОССН *AstraServer* в графической утилите «Политика безопасности» выбрать «Домен *ALD*»;
- открыть «Устройства и правила», «Правила», создать новое правило: выбрать импорт свойств, затем выполнить подключение *USB*-носителя, в появившемся дереве выбрать устройство, ввести имя правила «*Rule*1», отметить «Включено» и применить изменения;
- открыть «Устройства и правила», «Устройства», выполнить добавление *USB*-носителя через импорт свойств, затем установить для него разрешения на чтение и запись для учётной записи пользователя *userald*, группы «*Domain Users*» и всех остальных, установить уровень конфиденциальности — 1, выбрать правило «*Rule*1» и активировать данное устройство, установив флаг «Включено»;
- войти в ОССН *AstraClient*1, в сессии, функционирующей от имени учётной записи пользователя *userald* на уровнях доступа 0, 1 и 2, выполнить подключение *USB*-носителя, при этом проверить возможность монтирования (в соответствии с «Руководством администратора. Часть 1» монтирование учтённого носителя с файловой системой *VFAT* возможно только при входе в ОССН на том же уровне, с которым данный носитель учтён) и корректность (соответствие МРОСЛ ДП-модели) выполнения операций записи и чтения файлов на *USB*-носитель для каждого уровня доступа.

Содержание отчёта по выполненной работе

В отчёте о выполненной работе необходимо указать:

1. Полный перечень использованных команд с кратким описанием их назначения.
2. Примеры выполнения команд, которые были использованы в ходе работы с описанием результатов их выполнения.
3. Описание порядка работы с командами *ALD* (*ald-admin*, *ald-init*, *ald-client*) и графической утилитой «Политика безопасности» (*fly-admin-smc*) при осуществлении следующих действий со службой *ALD*:



- настройка адресации сетевого интерфейса;
- настройка контроллера *ALD*;
- настройка клиента *ALD*;
- управление параметрами контроллера *ALD*.

Контрольные вопросы

1. Каково назначение служб контроллера *ALD*?
2. Какие службы устанавливаются на контроллере *ALD*?
3. Какие особенности настройки имён компьютеров, входящих в домен *ALD*?
4. Каковы особенности настройки контроллера *ALD*?
5. Каковы особенности настройки клиента *ALD*?
6. Чем отличаются настройки *ALD* в режиме контроллера и в режиме клиента?
7. Какие основные настройки домена можно выполнять с использованием команды *ald-admin*?