Методическое пособие по выполнению домашнего задания по курсу «Администратор Linux. Professional»

Vagrant-стенд с LDAP на базе FreeIPA

Цель домашнего задания

Научиться настраивать LDAP-сервер и подключать к нему LDAP-клиентов

Описание домашнего задания

1) Установить FreeIPA
2) Написать Ansible-playbook для конфигурации клиента

Дополнительное задание
3)* Настроить аутентификацию по SSH-ключам
4)** Firewall должен быть включен на сервере и на клиенте

Введение

LDAP (**Lightweight Directory Access Protocol** — легковесный протокол доступа к каталогам) — это протокол для хранения и получения данных из каталога с иерархической структурой.

LDAP не является протоколом аутентификации или авторизации

С увеличением числа серверов затрудняется управление пользователями на этих сервере. LDAP решает задачу централизованного управления доступом.

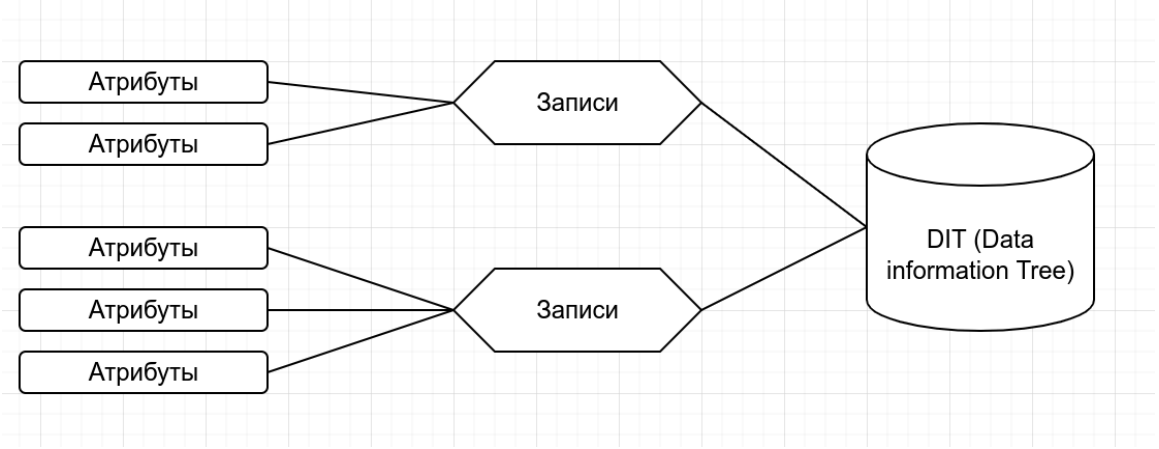
С помощью LDAP можно синхронизировать:

- UID пользователей
- Группы (GID)
- Домашние каталоги
- Общие настройки для хостов
- И т. д.

LDAP работает на следующих портах:

- 389/TCP — без TLS/SSL
- 636/TCP — с TLS/SSL

Основные компоненты LDAP



- Атрибуты — пара «ключ-значение». Пример атрибута: *mail: admin@example.com*
- Записи (entry) — набор атрибутов под именем, используемый для описания чего-либо

  Пример записи:
  dn: sn=Ivanov, ou=people, dc=digitalocean,dc=com
  objectclass: person
  sn: Ivanov
  cn: Ivan Ivanov

- Data Information Tree (DIT) — организационная структура, где каждая запись имеет ровно одну родительскую запись и под ней может находиться любое количество дочерних записей. Запись верхнего уровня — исключение

На основе LDAP построено много решений, например: Microsoft Active Directory, OpenLDAP, FreeIPA и т. д.

В данной лабораторной работе будет рассмотрена установка и настройка FreeIPA. FreeIPA — это готовое решение, включающее в себе:

- Сервер LDAP на базе Novell 389 DS с предустановленными схемами
- Сервер Kerberos
- Предустановленный BIND с хранилищем зон в LDAP
- Web-консоль управления

Функциональные и нефункциональные требования

- ПК на Unix с 8ГБ ОЗУ или виртуальная машина с включенной Nested Virtualization.
- Созданный аккаунт на GitHub - https://github.com/
- Если Вы находитесь в России, для корректной работы Вам может потребоваться VPN.

Предварительно установленное и настроенное следующее ПО:

- Hashicorp Vagrant (https://www.vagrantup.com/downloads)
- Oracle VirtualBox (https://www.virtualbox.org/wiki/Linux_Downloads).
- Любой редактор кода, например Visual Studio Code, Atom и т.д.

Инструкция по выполнению домашнего задания

Все дальнейшие действия были проверены при использовании Vagrant 2.2.19, VirtualBox v6.1.32. В лабораторной работе используются Vagrant boxes с CentOS 8 Stream (версия 20210210.0). Серьёзные отступления от этой конфигурации могут потребовать адаптации с вашей стороны.

Создадим Vagrantfile, в котором будут указаны параметры наших ВМ:

```
Vagrant.configure("2") do |config|
    # Указываем ОС, версию, количество ядер и ОЗУ
    config.vm.box = "centos/stream8"
    config.vm.box_version = "20210210.0"

    config.vm.provider :virtualbox do |v|
      v.memory = 2048
```

```
    v.cpus = 1
  end

  # Указываем имена хостов и их IP-адреса
  boxes = [
    { :name => "ipa.otus.lan",
      :ip => "192.168.57.10",
    },
    { :name => "client1.otus.lan",
      :ip => "192.168.57.11",
    },
    { :name => "client2.otus.lan",
      :ip => "192.168.57.12",
    }
  ]
  # Цикл запуска виртуальных машин
  boxes.each do |opts|
    config.vm.define opts[:name] do |config|
      config.vm.hostname = opts[:name]
      config.vm.network "private_network", ip: opts[:ip]
    end
  end
end
```

После создания Vagrantfile, запустим виртуальные машины командой *vagrant up*. Будут созданы 3 виртуальных машины с ОС CentOS 8 Stream. Каждая ВМ будет иметь по 2ГБ ОЗУ и по одному ядру CPU.

1) Установка FreeIPA сервера

Для начала нам необходимо настроить FreeIPA-сервер. Подключимся к нему по SSH с помощью команды: *vagrant ssh ipa.otus.lan* и перейдём в root-пользователя: *sudo -i*

Начнем настройку FreeIPA-сервера:

- Установим часовой пояс: timedatectl set-timezone Europe/Moscow
- Установим утилиту chrony: yum install -y chrony
- Запустим chrony и добавим его в автозагрузку: systemctl enable chronyd —now
- Если требуется, поменяем имя нашего сервера: hostnamectl set-hostname <имя сервера>
  В нашей лабораторной работе данного действия не требуется, так как уже указаны корректные имена в Vagrantfile
- *Выключим Firewall: systemctl stop firewalld*
- *Отключаем автозапуск Firewalld: systemctl disable firewalld*
- *Остановим Selinux: setenforce 0*
- *Поменяем в файле **/etc/selinux/config**, параметр Selinux на **disabled***
  vi /etc/selinux/config

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
```

```
# SELINUXTYPE= can take one of these three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes
are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

- Для дальнейшей настройки FreeIPA нам потребуется, чтобы DNS-сервер хранил запись о нашем LDAP-сервере. В *рамках данной лабораторной работы мы не будем настраивать отдельный DNS-сервер и просто добавим запись в файл /etc/hosts*
  vi /etc/hosts

```
127.0.0.1   localhost localhost.localdomain
127.0.1.1 ipa.otus.lan ipa
192.168.57.10 ipa.otus.lan ipa
```

- Установим модуль DL1: yum install -y @idm:DL1
- Установим FreeIPA-сервер: yum install -y ipa-server

- Запустим скрипт установки: *ipa-server-install*

  Далее, нам потребуется указать параметры нашего LDAP-сервера, после ввода каждого параметра нажимаем Enter, если нас устраивает параметр, указанный в квадратных скобках, то можно сразу нажимать Enter:

  Do you want to configure integrated DNS (BIND)? [no]: **no**
  Server host name [ipa.otus.lan]: **<Нажимаем Enter>**
  Please confirm the domain name [otus.lan]: **<Нажимем Enter>**
  Please provide a realm name [OTUS.LAN]: **<Нажимаем Enter>**
  Directory Manager password: **<Указываем пароль минимум 8 символов>**
  Password (confirm): **<Дублируем указанный пароль>**

IPA admin password: **<Указываем пароль минимум 8 символов>**
Password (confirm): **<Дублируем указанный пароль>**
NetBIOS domain name [OTUS]: **<Нажимаем Enter>**
Do you want to configure chrony with NTP server or pool address? [no]: **no**
The IPA Master Server will be configured with:
Hostname: ipa.otus.lan
IP address(es): 192.168.57.10
Domain name: otus.lan
Realm name: OTUS.LAN

The CA will be configured with:
Subject DN: CN=Certificate Authority,O=OTUS.LAN
Subject base: O=OTUS.LAN
Chaining: self-signed
Проверяем параметры, если всё устраивает, то нажимаем yes
Continue to configure the system with these values? [no]: **yes**

Далее начнется процесс установки. Процесс установки занимает примерно 10-15 минут (иногда время может быть другим). Если мастер успешно выполнит настройку FreeIPA то в конце мы получим сообщение:
The ipa-server-install command was successful

При вводе параметров установки мы вводили 2 пароля:

- Directory Manager password — это пароль администратора сервера каталогов, У этого пользователя есть полный доступ к каталогу.
- IPA admin password — пароль от пользователя FreeIPA admin

После успешной установки FreeIPA, проверим, что сервер Kerberos может выдать нам билет:

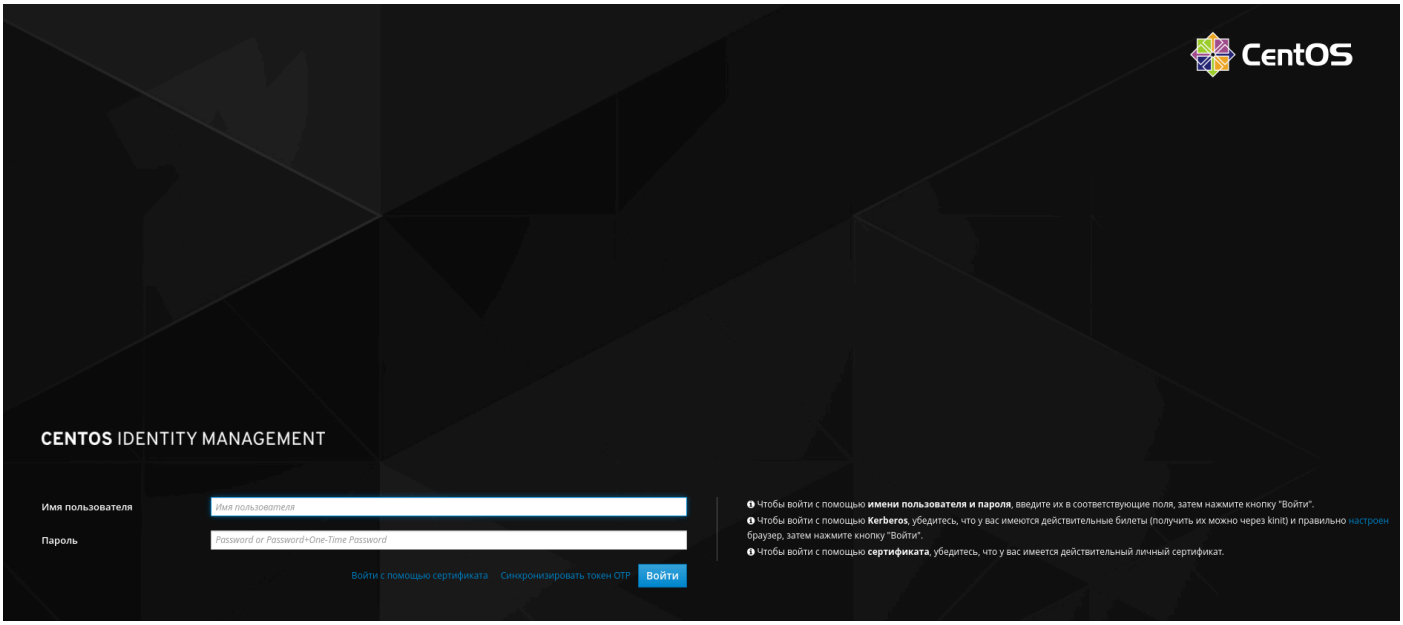
```
[root@ipa ~]# kinit admin
Password for admin@OTUS.LAN:  #Указываем Directory Manager password
[root@ipa ~]# klist           #Запросим список билетов Kerberos
Ticket cache: KCM:0
Default principal: admin@OTUS.LAN

Valid starting     Expires            Service principal
08/02/22 18:18:25  08/03/22 17:32:39  krbtgt/OTUS.LAN@OTUS.LAN
[root@ipa ~]#
```

Для удаление полученного билета воспользуемся командой: kdestroy

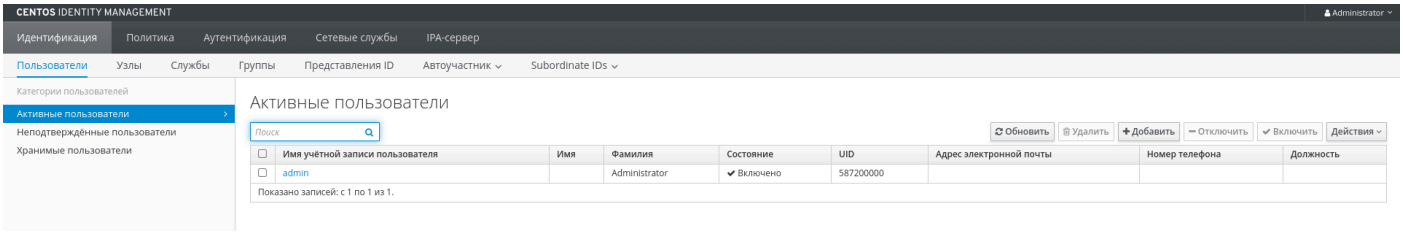
Мы можем зайти в Web-интерфейс нашего FreeIPA-сервера, для этого на нашей хостой машине нужно прописать следующую строку в файле Hosts:
192.168.57.10 ipa.otus.lan

*В Unix-based системах файл хост находится по адресу **/etc/hosts**, в Windows — **c:\Windows\System32\Drivers\etc\hosts**. Для добавления строки потребуются права администратора.*

После добавления DNS-записи откроем с нашей хост-машины веб-страницу vagranvagra



Откроется окно управления FreeIPA-сервером. В имени пользователя укажем admin, в пароле укажем наш IPA admin password и нажмём войти.



Откроется веб-консоль управления FreeIPA. Данные во FreeIPA можно вносить как через веб-консоль, так и средствами командной строки.

На этом установка и настройка FreeIPA-сервера завершена.

2. Ansible playbook для конфигурации клиента

Настройка клиента похожа на настройку сервера. На хосте также нужно:

- Настроить синхронизацию времени и часовой пояс
- Настроить (или отключить) firewall
- Настроить (или отключить) SElinux
- В файле hosts должна быть указана запись с FreeIPA-сервером и хостом

Хостов, которые требуется добавить к серверу может быть много, для упрощения нашей работы выполним настройки с помощью Ansible:

В каталоге с нашей лабораторной работой создадим каталог Ansible: *mkdir ansible*
В каталоге ansible создадим файл **hosts** со следующими параметрами:

```
[clients]
client1.otus.lan ansible_host=192.168.57.11 ansible_user=vagrant
ansible_ssh_private_key_file=./.vagrant/machines/client1.otus.lan/virtual
box/private_key
client2.otus.lan ansible_host=192.168.57.12 ansible_user=vagrant
ansible_ssh_private_key_file=./.vagrant/machines/client2.otus.lan/virtual
box/private_key
```

Файл содержит группу clients в которой прописаны 2 хоста:

- client1.otus.lan
- client2.otus.lan

Также указаны и ip-адреса, имя пользователя от которого будет логин и ssh-ключ.

Далее создадим файл **provision.yml** в котором непосредственно будет выполняться настройка клиентов:

```
- name: Base set up
  hosts: all
  #Выполнять действия от root-пользователя
  become: yes
  tasks:
  #Установка текстового редактора Vim и chrony
  - name: install softs on CentOS
    yum:
      name:
        - vim
        - chrony
      state: present
```

```
    update_cache: true


#Отключение firewalld и удаление его из автозагрузки
- name: disable firewalld
  service:
    name: firewalld
    state: stopped
    enabled: false


#Отключение SElinux из автозагрузки
#Будет применено после перезагрузки
- name: disable SElinux
  selinux:
    state: disabled


#Отключение SElinux до перезагрузки
- name: disable SElinux now
  shell: setenforce 0


#Установка временной зоны Европа/Москва
- name: Set up timezone
  timezone:
    name: "Europe/Moscow"


#Запуск службы Chrony, добавление её в автозагрузку
- name: enable chrony
  service:
    name: chronyd
    state: restarted
    enabled: true


#Копирование файла /etc/hosts с правами root:root 0644
- name: change /etc/hosts
  template:
    src: hosts.j2
    dest: /etc/hosts
    owner: root
    group: root
    mode: 0644


#Установка клиента Freeipa
- name: install module ipa-client
  yum:
    name:
      - freeipa-client
    state: present
    update_cache: true


#Запуск скрипта добавления хоста к серверу
- name: add host to ipa-server
```

```
    shell: echo -e "yes\nyes" | ipa-client-install --mkhomedir
--domain=OTUS.LAN --server=ipa.otus.lan --no-ntp -p admin -w otus2022
```

Template файла */etc*/hosts выглядит следующим образом:

```
127.0.0.1   localhost localhost.localdomain localhost4
localhost4.localdomain4
::1         localhost localhost.localdomain localhost6
localhost6.localdomain6
192.168.57.10 ipa.otus.lan ipa
```

Почти все модули нам уже знакомы, давайте подробнее остановимся на последней команде *echo -e "yes\nyes" | ipa-client-install --mkhomedir --domain=OTUS.LAN --server=ipa.otus.lan --no-ntp -p admin -w otus2022*

При добавлении хоста к домену мы можем просто ввести команду *ipa-client-install и следовать мастеру подключения к FreeIPA-серверу (как было в первом пункте).*

Однако команда позволяет нам сразу задать требуемые нам параметры:
--domain — имя домена
--server — имя FreeIPA-сервера
--no-ntp — не настраивать дополнительно ntp (мы уже настроили chrony)
-p — имя админа домена
-w — пароль администратора домена (IPA password)
--mkhomedir — создать директории пользователей при их первом логине

Если мы сразу укажем все параметры, то можем добавить эту команду в Ansible и автоматизировать процесс добавления хостов в домен.

Альтернативным вариантом мы можем найти на GitHub отдельные модули по подключениею хостов к FreeIPA-сервер.

После подключения хостов к FreeIPA-сервер нужно проверить, что мы можем получить билет от Kerberos сервера: *kinit admin*
Если подключение выполнено правильно, то мы сможем получить билет, после ввода пароля.

Давайте проверим работу LDAP, для этого на сервере FreeIPA создадим пользователя и попробуем залогиниться к клиенту:

- Авторизируемся на сервере: kinit admin
- Создадим пользователя otus-user

```
[root@ipa ~]# ipa user-add otus-user --first=Otus --last=User --password
Password:      #Вводим пароль пользователя otus-user
Enter Password again to verify: #повторно вводим пароль пользователя
otus-user
----------------------
Added user "otus-user"
----------------------
  User login: otus-user
  First name: Otus
  Last name: User
  Full name: Otus User
  Display name: Otus User
```

```
  Initials: OU
  Home directory: /home/otus-user
  GECOS: Otus User
  Login shell: /bin/sh
  Principal name: otus-user@OTUS.LAN
  Principal alias: otus-user@OTUS.LAN
  User password expiration: 20220802164239Z
  Email address: otus-user@otus.lan
  UID: 587200003
  GID: 587200003
  Password: True
  Member of groups: ipausers
  Kerberos keys available: True
[root@ipa ~]#
```

На хосте client1 или client2 выполним команду *kinit otus-user*

```
[root@client1 ~]# kinit otus-user
Password for otus-user@OTUS.LAN:
Password expired.  You must change it now.
Enter new password:
Enter it again:
[root@client1 ~]#
```

Система запросит у нас пароль и попросит ввести новый пароль.

На этом процесс добавления хостов к FreeIPA-серверу завершен.

Критерии оценивания

Статус «Принято» ставится при выполнении следующих условий:

1. Ссылка на репозиторий GitHub.
2. Vagrantfile, который будет разворачивать виртуальные машины
3. Документация по каждому заданию:

Создайте файл README.md и снабдите его следующей информацией:
- название выполняемого задания;
- текст задания;
- описание команд и их вывод;
- особенности проектирования и реализации решения,
- заметки, если считаете, что имеет смысл их зафиксировать в репозитории.

Рекомендуемые источники

- Статья о LDAP - https://ru.wikipedia.org/wiki/LDAP
- Статья о настройке FreeIPA - https://www.dmosk.ru/miniinstruktions.php?mini=freeipa-centos
- FreeIPA wiki - https://www.freeipa.org/page/Wiki_TODO
- Статья «Chapter 13. Preparing the system for IdM client installation» - https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/installing_identity_management/preparing-the-system-for-ipa-client-installation_installing-identity-management
- Статья «про LDAP по-русски» - https://pro-ldap.ru/