Процедура аутентификации с использованием RADIUS-сервера

Успешно сдайте бесплатный сертификационный экзамен в Академии "Инфинет" и получите статус сертифицированного инженера Инфинет.

Пройти сертификационный экзамен

Ниже приведен пример настройки аутентификации с использованием RADIUS для устройств **InfiNet Wireless R5000**. В качестве RADIUS сервера выбран Free RADIUS, установленный на CentOS 7.

Шаг 1

Добавьте IP-адреса и пароли устройств, которые будут обращаться к серверу FreeRADIUS, в файл */etc/raddb/clients.conf.*

```
client MASTER{
                                ipaddr=1.1.10.1
                                secret=pass
                        }
```

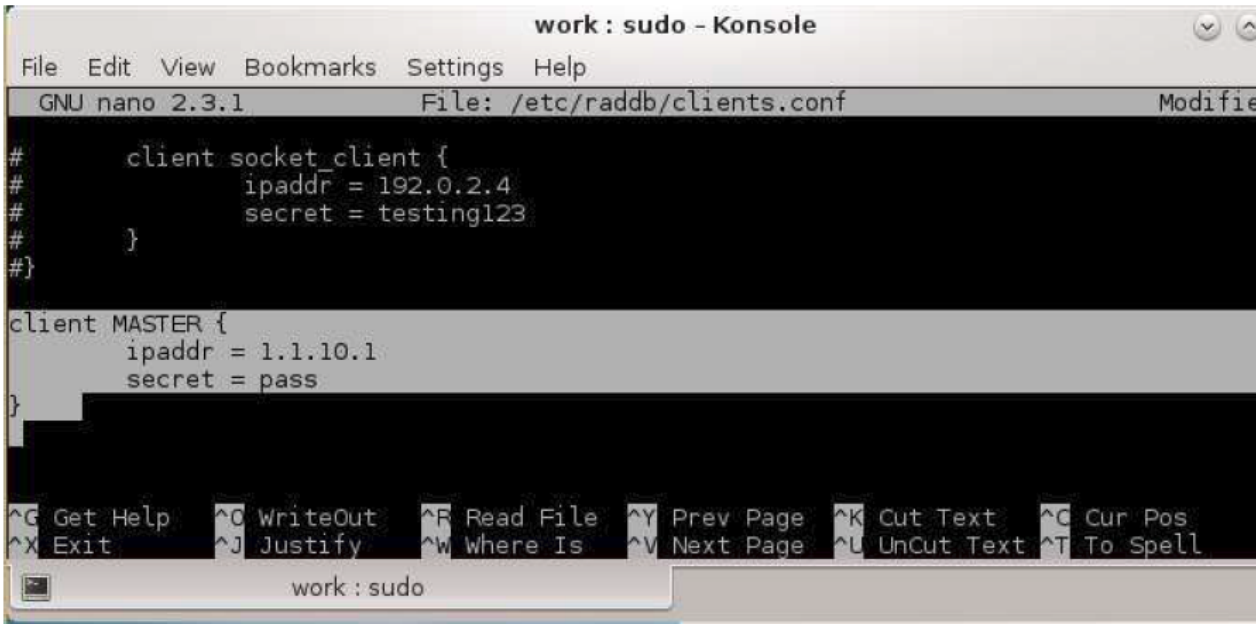

Рисунок - Добавление устройства

ВНИМАНИЕ

Файл */etc/raddb/clients.conf* содержит список всех устройств, которые могут выполнять AAA запрос на сервер FreeRADIUS.

Шаг 2

Добавьте пользователей в файл */etc/raddb/users.*

```
login Cleartext-Password:="password"
```

- "*login*" - имя пользователя.
- "*password*" - пароль.

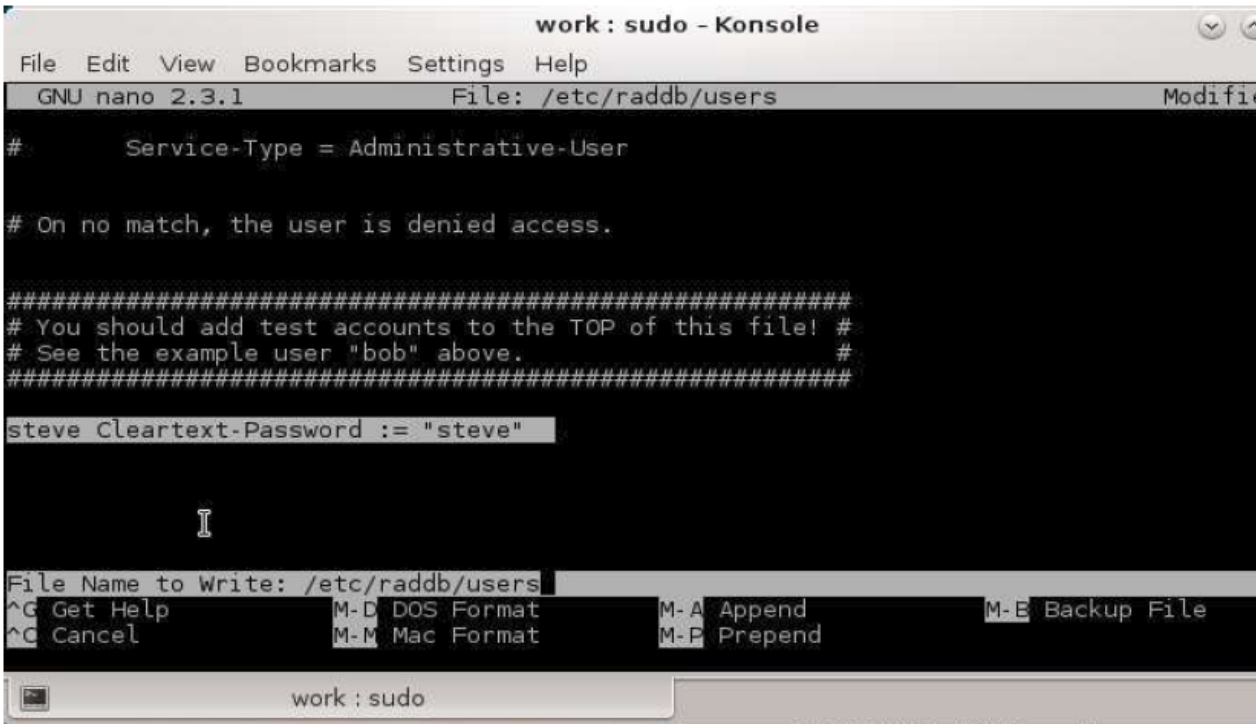

Рисунок - Добавление пользователя

Шаг 3

Выполните следующие настройки устройств:

- Настройте локальное имя и пароль.

```
sys user login
sys password pass
```

- Включите AAA аутентификацию.

```
sys useAAA
```

- Укажите адрес сервера, который будет использоваться для аутентификации. Вместо "*10.10.10.128*" используйте фактический адрес RADIUS-сервера.
- Вместо "*pass*" используйте пароль, указанный в шаге 1.

```
 aaa -auth=10.10.10.128,pass start
```

- Сохраните настройки.

```
co sa
```

Шаг 4

Убедитесь, что ваше устройство и RADIUS-сервер имеют полную IP-связность (устройство может пинговать адрес RADIUS-сервера и наоборот), и что между ними нет запущенных межсетевых экранов.

Межсетевой экран на сервере рекомендуется отключить.

```
sudo systemctl stop firewalld
```

Шаг 5

Запустите FreeRADIUS-сервер в режиме отладки.

```
sudo radiusd –X
```

Шаг 6

Попробуйте зайти на устройство через веб-интерфейс, либо по Telnet, используя имя и пароль, указанный в шаге 2. В случае, если все настройки выполнены правильно, вы сможете получить доступ к устройству. В логе FreeRADIUS сервера появятся сообщения об успешной аутентификации:

```
(1) # Executing group from file /etc/raddb/sites-enabled/default
(1)  Auth-Type PAP {
(1)  pap : Login attempt with password
(1)  pap : User authenticated successfully
(1)   [pap] = ok
(1)  } # Auth-Type PAP = ok
(1) # Executing section post-auth from file /etc/raddb/sites-enabled/defaul
(1)   post-auth {
(1)   [exec] = noop
(1)   remove_reply_message_if_eap remove_reply_message_if_eap {
(1)     if (&reply:EAP-Message && &reply:Reply-Message)
(1)     if (&reply:EAP-Message && &reply:Reply-Message)  -> FALSE
(1)    else else {
(1)     [noop] = noop
(1)    } # else else = noop
(1)   } # remove_reply_message_if_eap remove_reply_message_if_eap = noop
(1)  } #  post-auth = noop
(1) Sending Access-Accept packet to host 1.1.10.1 port 10317, id=202, lengt
Sending Access-Accept Id 202 from 1.1.10.128:1812 to 1.1.10.1:10317
(1) Finished request
Waking up in 0.3 seconds.
Waking up in 4.6 seconds.
(1) Cleaning up request packet ID 202 with timestamp +16
Ready to process requests
```

Рисунок - Пример записей в журнале FreeRADIUS-сервера