

Настройка RADIUS для сервера Livingston

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Authentication](#)

[Добавление автоматического учета](#)

[Файлы тестирования](#)

[Дополнительные сведения](#)

Введение

Этот документ предназначен для помощи начинающему пользователю RADIUS в создании и доводке конфигурации RADIUS. Это не является полным описанием возможностей Cisco IOS® RADIUS. Документация по серверу Livingston, имеющаяся от вебсайта Lucent Technologies.

Конфигурация маршрутизатора одинаковая, независимо от того, какой сервер использован. Cisco предлагает имеющийся на рынке код сервера RADIUS в Ciscos NA, Ciscos Unix, или Cisco Access Registrar.

Эта конфигурация маршрутизатора была разработана на маршрутизаторе, который выполняет Cisco IOS Software Release 11.3.3; Выпуск 12.0.5. Т и более поздний **групповой RADIUS** использования вместо **радиуса**, таким образом, операторы, такие как **включение RADIUS aaa authentication login default** появляются как **групповой RADIUS aaa authentication login default**, включают.

См. [Данные RADIUS](#) в документации по Cisco IOS для подробных данных о командах маршрутизатора RADIUS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

Authentication

Выполните следующие действия:

1. Удостоверьтесь, что вы скомпилировали КОД СЕРВЕРА RADIUS на сервере UNIX. Конфигурации сервера предполагают использование кода Сервера Livingston RADIUS. Конфигурации маршрутизатора должны работать с другим серверным кодом, но отличаются конфигурации сервера. Код, radiusd, должен быть выполнен как root.
2. Код Livingston RADIUS идет с тремя файлами примера, которые должны быть настроены для вашей системы: clients.example, users.example, и словарь. Они все обычно находятся в raddb каталоге. Можно или модифицировать эти файлы или пользователей и файлы клиентов в конце этого документа. Все три файла должны быть размещены в рабочий каталог. Тест, чтобы быть уверенным сервер RADIUS запускается с этих трех файлов:radiusd -x -d (directory_containing_3_files) Ошибки в запуске должны быть распечатаны на экран или directory_containing_3_files_logfile. Проверьте, чтобы быть уверенными, что RADIUS запустился от другого окна сервера:

```
ps -aux | grep radiusd
```

(or ps -ef | grep radiusd) Вы видите два процесса radiusd.

3. Уничтожьте процесс радиуса:

```
kill -9 highest_radiusd_pid
```
4. На порте консоли маршрутизатора начните настраивать RADIUS. **Войдите в режим enable и введите configure terminal перед набором команд.** Этот синтаксис гарантирует, что вас не блокируют из маршрутизатора первоначально, дают, тот RADIUS не работает на сервере:

```
!--- Turn on RADIUS aaa new-model enable password whatever !--- These are lists of authentication methods, !--- that is, "linmethod", "vtymethod", "conmethod" are !--- names of lists, and the methods listed on the same !--- lines are the methods in the order to be tried. As !--- used here, if authentication fails due to the radiusd !--- not being started, the enable password will be !--- accepted because it is in each list. aaa authentication login default radius enable aaa authentication login linmethod radius enable aaa authentication login vtymethod radius enable aaa authentication login conmethod radius enable !--- Point the router to the server, that is, !--- #.#.#.# is the server IP address. radius-server host #.#.#.# !--- Enter a key for handshaking !--- with the RADIUS server: radius-server key cisco line con 0 password whatever !--- No time-out to prevent being !--- locked out during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 password whatever flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being !--- locked out during debugging. exec-timeout 0 0 login authentication vtymethod
```

5. Оставайтесь подключенным к маршрутизатору через порт консоли пока вы проверяете порядок, чтобы быть уверенным, что вы все еще имеете доступ к маршрутизатору через Telnet прежде чем вы продолжите. Поскольку radiusd не работает, enable password должен быть принят с любым идентификатором пользователя. **Внимание.**

: Поддержите сеанс порта консоли активным и останьтесь в режиме включения.

Гарантируйте, что этот сеанс не испытывает таймаут. Не блокируйте себя, в то время как вы изменяете конфигурацию. Выполните эти команды для наблюдения сервера к взаимодействию маршрутизаторов в маршрутизаторе:

```
terminal monitor
```

```
debug aaa authentication
```

6. Как root, запустите RADIUS на сервере:

```
radiusd -x -d
```

(directory_containing_3_files) Ошибки в запуске распечатаны на экран или `directory_containing_3_files_logfile`. Проверьте, чтобы быть уверенными, что RADIUS запустился с другого окна сервера:

```
Ps -aux | grep radiusd
```

(or `Ps -ef | grep radiusd`) Необходимо видеть два процесса `radiusd`.
7. Telnet (VTY) пользователи теперь должны аутентифицироваться через RADIUS. С отладкой на маршрутизаторе и сервере, шагах 5 и 6, Telnet в маршрутизатор от другой части сети. На маршрутизаторе появляется приглашение ввести имя пользователя и пароль, на которое необходимо ответить:

```
ciscoursr (username from users file)
```

```
ciscopas (password from users file)
```

Наблюдайте сервер и маршрутизатор, где необходимо видеть Взаимодействие с сервером RADIUS, например, что передается где, ответы и запросы, и т.д. Прежде чем продолжать устраните все неполадки.
8. Если вы также хотите, чтобы ваши пользователи аутентифицировались через RADIUS для вхождения в режим включения, удостоверьтесь, что сеанс порта консоли все еще активен, и добавьте эту команду к маршрутизатору.
!--- For enable mode, list "default" looks to RADIUS !--- then enable password if RADIUS not running.

```
aaa authentication enable default radius enable
```
9. Пользователям придется теперь **включить** через RADIUS. С отладкой, идущей на маршрутизатор и сервер, шаги 5 и 6, Telnet в маршрутизатор от другой части сети. Маршрутизатор должен произвести приглашение имени пользователя и пароля, на которое вы отвечаете:

```
ciscoursr (username from users file)
```

```
ciscopas (password from users file)
```

Когда вы вводите режим включения, маршрутизатор посылает имя пользователя `$enable15$` и спрашивает пароль, на что вы отвечаете:

```
shared
```

Наблюдайте сервер и маршрутизатор, где необходимо видеть Взаимодействие с сервером RADIUS, например, что передается где, ответы и запросы, и т.д. Прежде чем продолжать устраните все неполадки.
10. Проверьте для аутентификации ваших пользователей консольного порта через RADIUS установлением сеанса Telnet к маршрутизатору, который должен аутентифицироваться через RADIUS. Оставайтесь Telnetted в маршрутизатор и в режиме включения, пока вы не уверены, что можно войти к маршрутизатору через консольный порт, выйти исходного соединения к маршрутизатору через консольный порт, и затем воссоединиться с консольным портом. Проверка подлинности порта консоли, чтобы войти и включить с помощью имен и паролей пользователя в шаге 9 должна теперь быть через RADIUS.
11. В то время как вы остаетесь связанными или через сеанс Telnet или через консольный порт и с отладкой, идущей на маршрутизатор и сервер, шаги 5 и 6, устанавливаете подключение с помощью модема для выравнивания 1. Пользователям линии придется теперь войти и включить через RADIUS. Маршрутизатор должен произвести приглашение имени пользователя и пароля, на которое вы отвечаете:

```
ciscoursr (username from users file)
```

```
ciscopas (password from users file)
```

Когда вы вводите режим включения, маршрутизатор посылает имя пользователя `$enable15$` и спрашивает пароль, на что вы отвечаете:

```
shared
```

Наблюдайте сервер и маршрутизатор, где необходимо видеть Взаимодействие с сервером RADIUS, например, что передается где, ответы и запросы, и т.д. Прежде чем продолжать устраните все неполадки.

[Добавление автоматического учета](#)

Добавление учета необязательно.

1. Учет не имеет место, пока не настроено в маршрутизаторе. Позвольте считать в маршрутизаторе как в данном примере:

```
aaa accounting exec default start-stop radius
aaa accounting connection default start-stop radius
aaa accounting network default start-stop radius
aaa accounting system default start-stop radius
```
2. Запустите RADIUS на сервере с бухгалтерской опцией: Start RADIUS on the server with the accounting option:
3. Для наблюдения сервера к взаимодействию маршрутизаторов в маршрутизаторе:

```
terminal monitor
debug aaa accounting
```
4. Обратитесь к маршрутизатору, в то время как вы наблюдаете сервер и взаимодействие маршрутизаторов посредством отладки, и затем проверяете бухгалтерский каталог для файлов журнала.

Файлы тестирования

Это - пользовательский тестовый файл:

```
ciscour      Password = "ciscopas"
             User-Service-Type = Login-User,
             Login-Host = 1.2.3.4,
             Login-Service = Telnet

$enable15$   Password = "shared"
             User-Service-Type = Shell-User
```

Это - тестовый файл клиентов:

```
# 1.2.3.4 is the ip address of the client router and cisco is the key
1.2.3.4      cisco
```

Дополнительные сведения

- [Служба удаленной аутентификации пользователей коммутируемого доступа \(RADIUS\)](#)
- [Запросы комментариев \(RFC\)](#)
- [Cisco Systems – техническая поддержка и документация](#)