Настройка маршрутизатора Cisco с TACACS+ Authentication

Содержание

Введение

В данном документе описана настройка маршрутизатора Cisco для аутентификации с TACACS+, выполняющемся на UNIX. TACACS+ предоставляет меньше возможностей, чем доступные для приобретения Cisco Secure ACS для Windows или Cisco Secure ACS UNIX.

ПО TACACS+ ранее предлагаемое Cisco Systems больше не распространяется и не поддерживается компанией Cisco Systems.

В настоящее время можно найти много версий бесплатного ПО TACACS+, для этого достаточно ввести "TACACS+ freeware" в строке поиска любой поисковой системы в Интернете. Компания Cisco не дает специальных рекомендаций по использованию какой-либо конкретной версии бесплатного ПО TACACS+.

Cisco Secure Access Control Server (ACS) можно приобрести по обычным международным каналам распределения и продаж Cisco. Cisco Secure ACS для Windows содержит все обязательные компоненты, необходимые для независимой установки на рабочую станцию Microsoft Windows. Cisco Secure ACS Solution Engine поставляется с предустановленной лицензией на ПО Cisco Secure ACS. Разместить заказ можно на главной странице размещения заказов Cisco Ordering Home Page (только для зарегистрированных пользователей).

Примечание. Для получения пробной 90-дневной версии Cisco Secure ACS для Windows необходима учетная запись CCO и связанный с ней контракт на обслуживание.

Конфигурация маршрутизатора в данном документе создана на маршрутизаторе работающем под управлением ПО Cisco IOS® версии 11.3.3. ПО Cisco IOS версии 12.0.5.T и более поздние использует **group tacacs+** вместо **tacacs+**, поэтому инструкции, например **aaa authentication login default tacacs+ enable** будут иметь вид **aaa authentication login default group tacacs+ enable**.

Дополнительные сведения о командах маршрутизатора см. в документации на ПО Cisco IOS
.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в данном документе получены при использовании ПО Cisco IOS версии 11.3.3 и ПО Cisco IOS версии 12.0.5.T и более поздних.

Сведения, представленные в данном документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе в действующей сети необходимо понимать последствия выполнения любой команды.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Аутентификация

Выполните следующие действия.

Обязательно скомпилируйте код TACACS+ (TAC+) на сервере UNIX.

Приведенные здесь конфигурации сервера подразумевают использование серверной программы Cisco TAC+. Конфигурации маршрутизатора должны функционировать независимо от разработчика серверной программы (Cisco или др.). TAC+ должен функционировать в качестве корневого.

Скопируйте тестовый файл, приведенный в конце настоящего документа, разместите его на сервере TAC+ и присвойте имя **test_file**.

Убедитесь, что демон **tac_plus_executable** запущен с **test_file**. В этой команде параметр **-P** задает проверку наличия ошибок компиляции, но не запускает демон:

Чтобы увидеть содержимое файла test_file воспользуйтесь прокруткой, не должно быть сообщений подобных `cannot find file`, `cleartext expected--found cleartext` или `unexpected}` (не удалось найти, ожидается незашифрованный текст—найден незашифрованный текст или непредвиденный). В случае ошибок проверьте путь к файлу test_file, перепроверьте ввод и повторно проведите тестирование прежде чем продолжать.

Начало настройки TAC+ на маршрутизаторе.

Войдите в режим **enable** и введите **configure terminal** перед набором команд. Этот синтаксис команды предотвращает блокировку доступа к маршрутизатору на начальном этапе, если не выполняется **tac_plus_executable**:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

Прежде чем продолжать убедитесь в наличии доступа к маршрутизатору через порт консоли и по протоколу Telnet. Поскольку **tac_plus_executable** не выполняется пароль **enable** password должен приниматься.

Примечание. Не разрывайте соединение с маршрутизатором через порт консоли и оставайтесь в режиме enable. Этот сеанс связи не должен прерываться по тайм-ауту. На этом этапе доступ к маршрутизатору ограничен, необходимо иметь возможность внести изменения в конфигурацию без блокировки самого пользователя.

Выполните эти команды, чтобы на маршрутизаторе увидеть взаимодействие между маршрутизатором и сервером.

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

В качестве корневого запустите TAC+ на сервере:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

Убедитесь, что TAC+ запущен:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

или

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

Если TAC+ не запускается, вероятно ошибка в синтаксисе файла test_file. Вернитесь к шагу 1, чтобы исправить это.

Введите **tail -f /var/tmp/tac_plus.log**, чтобы на сервере увидеть взаимодействие между маршрутизатором и сервером.

Примечание. Параметр `-d 16` на шаге 5 разрешает отправку вывода всех транзакций в журнал /var/tmp/tac_plus.log.

Теперь для пользователей Telnet (VTY) должна действовать аутентификация через TAC+.

При выполнении отладки на маршрутизаторе и сервере (шаги 4 и 7) подключитесь по протоколу Telnet к маршрутизатору из другой части сети.

На маршрутизаторе появится приглашение ввести имя пользователя и пароль, на которое необходимо ответить:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

Пользователь `authenuser` входит в группу `admin` с паролем `admin`.

Наблюдайте за сервером и маршрутизатором, где можно видеть взаимодействие TAC+ — какие данные куда отправляются, ответы, запросы и т.д. Прежде чем продолжать устраните все неполадки.

Если необходимо, чтобы пользователи проходили аутентификацию через TAC+ для входа в режим enable, убедитесь в активности сеанса связи через порт консоли и добавьте следующую команду в маршрутизатор:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

Теперь пользователи должны входить в режим enable через TAC+.

При выполнении отладки на маршрутизаторе и сервере (шаги 4 и 7) подключитесь по протоколу Telnet к маршрутизатору из другой части сети. На маршрутизаторе появится приглашение ввести имя пользователя и пароль, на которое необходимо ответить:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
```

```
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

При входе в режим enable, маршрутизатор запрашивает пароль, на что нужно ответить:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

Наблюдайте за сервером и маршрутизатором, где можно видеть взаимодействие TAC+ — какие данные куда отправляются, ответы, запросы и т.д. Прежде чем продолжать устраните все неполадки.

Остановите процесс TAC+ на сервере, оставаясь подключенным через порт консоли, с целью убедиться, что пользователям по-прежнему доступен маршрутизатор даже при отказе TAC+:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
```

```
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

или

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

Повторите действия предыдущего шага для установления сеанса Telnet и режима enable. Затем маршрутизатор определяет, что процесс TAC+ не отвечает, и разрешает пользователям выполнить вход и войти в режим enable, используя пароли по умолчанию.

Проверьте аутентификацию пользователей, подключающихся через порт консоли, через TAC+. Для этого возобновите работу сервера TAC+ (шаги 5 и 6) и установите сеанс Telnet с маршрутизатором (который должен пройти аутентификацию через TAC+).

Оставайтесь подключенным к маршрутизатору по протоколу Telnet в режиме enable пока не убедитесь, что вы можете войти в маршрутизатор через порт консоли.

Разорвите исходное соединение с маршрутизатором через порт консоли, затем вновь подключитесь к порту консоли. Теперь, при подключении через порт консоли, аутентификация пользователей при входе в систему и режим enable, используя пароли и идентификаторы (см. шаг 10), должна осуществляться через TAC+.

При выполнении отладки на маршрутизаторе и сервере (шаги 4 и 7), оставаясь

подключенным по протоколу Telnet или через порт консоли, подключитесь через модем к каналу 1.

Теперь пользователи канала должны входить в систему и режим enable через TAC+.

На маршрутизаторе появляется приглашение ввести имя пользователя и пароль, на которое необходимо ответить:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

При входе в режим enable, маршрутизатор запрашивает пароль.

Ответ:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

Наблюдайте за сервером и маршрутизатором, где можно видеть взаимодействие TAC+ — какие данные куда отправляются, ответы, запросы и т.д. Прежде чем продолжать устраните все неполадки.

Теперь пользователи должны входить в режим enable через TAC+.

Добавление авторизации

Добавление авторизации необязательно.

По умолчанию на маршрутизаторе имеются три уровня команд:

уровень привилегий 0 содержит: disable, enable, exit, help и logout

уровень привилегий 1 — обычный уровень сеанса Telnet — приглашение: `router>`

уровень привилегий 15 — уровень enable — приглашение: `router#`

Поскольку набор доступных команд зависит от набора функций IOS, версии Cisco IOS, модели маршрутизатора и др., отсутствует полный список всех команд для уровней 1 и 15. Например, **show ipx route** отсутствует в наборе функций только IP, **show ip nat trans** отсутствует в ПО Cisco IOS версии 10.2.x, поскольку NAT не было внедрено на тот момент и **show environment** отсутствует в моделях маршрутизаторов без блока питания и контроля температуры. Чтобы определить команды, доступные в конкретном маршрутизаторе на определенном уровне, введите **?** в командной строке маршрутизатора на этом уровне привилегий.

Авторизация для порта консоли не была добавлена как функция до исправления ошибки с идентификатором Cisco CSCdi82030 (только длязарегистрированных пользователей). Авторизация для порта консоли отключена по умолчанию, чтобы уменьшить вероятность случайной блокировки доступа к маршрутизатору. Если пользователь имеет физический доступ к маршрутизатору через консоль, то авторизация для порта консоли не очень эффективна. Однако, авторизацию для порта консоли можно включить на канале `con 0` в образе, в котором исправлена ошибка с идентификатором Cisco CSCdi82030 (только для зарегистрированных пользователей), командой:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of
authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on
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 !--
- tac_plus_executable not being started, the !--- enable password is accepted because
!--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP address.
```

```
! tacacs-server host #.#.#.# 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 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
```

Маршрутизатор можно настроить для авторизации команд через TAC+ на всех или только некоторых уровнях.

Эта конфигурация маршрутизатора позволяет всем пользователям иметь настроенную на сервере аутентификацию каждой команды. В данном примере выполняется авторизация всех команд через TAC+, но в случае отказа сервера, авторизация не требуется.

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

Во время работы сервера TAC+, установите сеанс Telnet с маршрутизатором, используя **authenuser** в качестве имени пользователя.

Поскольку пользователю authenuser установлен атрибут default service = permit в test_file, этот пользователь может выполнять все функции.

Выполнив вход в маршрутизатор, войдите в режим **enable** и включите отладку авторизации:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.
```

```
!
aaa authentication login linmethod tacacs+ enable
aaa authentication login vtymethod tacacs+ enable
aaa authentication login conmethod tacacs+ enable
!
!--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

Установите сеанс Telnet с маршрутизатором, используя имя пользователя **authoruser** и пароль **operator**.

Этот пользователь не может выполнять две команды show: **traceroute** и **logout** (см. тестовый файл).

Наблюдайте за сервером и маршрутизатором, где можно видеть взаимодействие TAC+ (какие данные куда отправляются, ответы, запросы и т.д.). Прежде чем продолжать устраните все неполадки.

Если нужно настроить пользователя для автоматического перенаправления (autocommand), удалите знаки комментария в строках для пользователя transient в тестовом файле и укажите действительный IP-адрес назначения вместо #.#.#.#.

Остановите и запустите вновь сервер TAC+.

На маршрутизаторе:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.

!
aaa authentication login linmethod tacacs+ enable
aaa authentication login vtymethod tacacs+ enable
aaa authentication login conmethod tacacs+ enable
!
!--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

Установите сеанс Telnet с маршрутизатором, используя имя пользователя **transient** и пароль **transient**. Выполняется команда **telnet #.#.#.#** и пользователь transient перенаправляется в другой пункт назначения.

Добавление учета

Добавление учета необязательно.

Ссылка на файл учета в тестовом файле: accounting file = /var/log/tac.log. Но учет не выполняется, если не настроен в маршрутизаторе (при условии, что на маршрутизаторе выполняется ПО Cisco IOS версии старше 11.0).

Включите учет в маршрутизаторе:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

Примечание. Учет AAA не осуществляет учет каждой команды в некоторых версиях. Выходом из этой ситуации является использование авторизации каждой команды и протоколирование событий в журнале учета. (См. ошибку с идентификатором Cisco CSCdi44140.) Если используется образ, в котором эта ошибка исправлена [ПО Cisco IOS версии 11.2(1.3)F, 11.2(1.2), 11.1(6.3), 11.1(6.3)AA01, 11.1(6.3)CA на 24 сентября 1997 г.], также можно включить учет для команд.

Во время выполнения TAC+ на сервере введите эту команду на сервере, чтобы увидеть записи, вносимые в файл учета:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
```

```
password is accepted because !--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

Затем выполните вход в маршрутизатор и выход, завершите сеанс Telnet с маршрутизатором и т.д. Если требуется, введите на маршрутизаторе:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
so on 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 !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# 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 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
```

Тестовый файл

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of
authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on
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 !--
- tac_plus_executable not being started, the !--- enable password is accepted because
!--- it is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
```

```
    aaa authentication login conmethod tacacs+ enable
    !
    !--- Point the router to the server, where #.#.#.# !--- is the server IP address.
! tacacs-server host #.#.#.# 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 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
```

Примечание. Это сообщение об ошибке формируется, если сервер TACACS недоступен: `%AAAA-3-DROPACCTSNDFAIL: accounting record dropped,send to server failed: system-start` (%AAAA-3-DROPACCTSNDFAIL: запись учета отброшена, не удалось отправить серверу:система-старт). Убедитесь в работоспособном состоянии сервера TACACS+.

Дополнительные сведения

- Безопасность сетевого однопользовательского доступа TACACS+
- Terminal Access Controller Access Control System (TACACS+)
- Cisco Secure Access Control Server для Windows
- Cisco Systems – техническая поддержка и документация