Настраивая TACACS +, RADIUS, и Kerberos на Коммутаторах Cisco Catalyst

Содержание

Введение

Семейство Catalyst коммутаторов Cisco (Catalyst 4000, Catalyst 5000 и Catalyst 6000, в которых выполняется ПО CatOS), начиная с версии 2.2 поддерживают определенную форму аутентификации. Усовершенствования были внедрены в более поздние версии. Настройка пользователя сервера Kerberos, RADIUS или TACACS+ (TCP порт 49, не XTACACS протокол передачи дейтаграмм пользователя UDP порт 49) для аутентификации, авторизации и учета (AAA) такая же как и для пользователей маршрутизатора. В данном документе приведены самые необходимые команды для включения этих функций. Дополнительные варианты приведены в документации на коммутатор для рассматриваемой версии.

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.

Общие сведения

Поскольку поздние версии программного обеспечения поддерживают дополнительные варианты, необходимо выполнить команду **show version**, чтобы определить версию программного обеспечения коммутатора. После определения версии ПО, используемого коммутатором, воспользуйтесь этой таблицей для определения вариантов, доступных на конкретном устройстве, и вариантов, которые нужно настроить.

Всегда оставайтесь в коммутаторе при добавлении аутентификации и авторизации. Проверяйте конфигурацию в другом окне, чтобы избежать случайного блокирования.

Метод (минимум)	**Cat версия 2.2-5.1**	**Cat версия 5.1-5.4.1**	**Cat версия 5.4.1-7.5.1**	**Cat версии 7.5.1 и более поздней**
Аутентификация TACACS+ ИЛИ	Шаг A	Шаг A	Шаг A	Шаг A
Аутентификация RADIUS ИЛИ	Н/Д	Шаг B	Шаг B	Шаг B
Аутентификация Kerberos ИЛИ	Н/Д	Н/Д	Шаг K	Шаг K
Аутентификация и авторизация имени локального пользователя	Н/Д	Н/Д	Н/Д	Шаг C
Дополнительно (варианты)				
Авторизация TACACS+ Command	Н/Д	Н/Д	Шаг D	Шаг D
Авторизация TACACS+ Exec	Н/Д	Н/Д	Шаг E	Шаг E
Авторизация RADIUS Exec	Н/Д	Н/Д	Шаг F	Шаг F
Учет – TACACS+ или RADIUS	Н/Д	Н/Д	Шаг G	Шаг G
Авторизация TACACS+ Enable	Шаг H	Шаг H	Шаг H	Шаг H
Авторизация RADIUS Enable	Н/Д	Шаг I	Шаг I	Шаг I

Авторизация TACACS+ Enable	Н/Д	Н/Д	Шаг J	Шаг J

Порядок действий для настройки

Шаг A - аутентификация TACACS+

Для более ранних версий ПО команды не такие сложные как для поздних версий. На коммутаторе могут быть доступны дополнительные варианты в более поздних версиях.

Выполните команду **set authentication login local enable**, чтобы оставить запасной вариант входа в коммутатор в случае отказа сервера.

Выполните команду **set authentication login tacacs enable**, чтобы включить аутентификацию TACACS+.

Выполните команду **set tacacs server #.#.#.#**, чтобы определить сервер.

Выполните команду **set tacacs key** *ваш_ключ*, чтобы определить ключ сервера, который является дополнительной возможностью метода TACACS+, поскольку вводит шифрование данных, передаваемых между коммутатором и сервером. В случае использования, он должен быть согласован с сервером.

Примечание. ПО Cisco Catalyst OS **не** воспринимает вопросительный знак (**?**) как часть какого-либо ключа или пароля. Вопросительный знак в явной форме используется для получения помощи в синтаксисе команды.

Шаг B – аутентификация RADIUS

Для более ранних версий ПО команды не такие сложные как для поздних версий. На коммутаторе могут быть доступны дополнительные варианты в более поздних версиях.

Выполните команду **set authentication login local enable**, чтобы оставить запасной вариант входа в коммутатор в случае отказа сервера.

Выполните команду **set authentication login radius enable**, чтобы включить аутентификацию RADIUS.

Определите сервер. На остальном оборудовании Cisco портами RADIUS по умолчанию являются 1645/1646 (аутентификация/учет).

На устройстве семейства Catalyst по умолчанию порт 1812/1813. При использовании Cisco Secure или сервера, взаимодействующего с другим оборудованием Cisco, используйте порт 1645/1646. Выполните команду **set radius server #.#.#.# auth-port 1645 acct-port 1646 primary**, чтобы определить сервер, а для Cisco IOS аналогичная команда **radius-server source-ports 1645-1646**.

Определите ключ сервера.

Это обязательно, поскольку применяет шифрование пароля между коммутатором и сервером, согласно документам Аутентификация/авторизация RADIUS (RFC 2865) и Учет RADIUS (RFC 2866) . В случае использования, он должен быть согласован с сервером. Выполните команду **set radius key** *ваш_ключ*.

Шаг C - аутентификация и авторизация имени локального пользователя

Начиная с CatOS версии 7.5.1 возможна аутентификация локального пользователя. Например, аутентификацию и авторизацию можно реализовать, используя пароль и имя пользователя, хранящиеся в Catalyst вместо аутентификации по локальному паролю.

Для аутентификации локального пользователя имеются только два уровня разрешений: 0 и 15. Уровень 0 — это непривилегированный уровень exec. Уровень 15 — это привилегированный уровень enable.

Если добавить эти команды в данном примере, пользователь `poweruser` перейдет в режим enable при подключении через Telnet или консоль к коммутатору, а пользователь `nonenable` перейдет в режим exec при подключении через Telnet или консоль к коммутатору.

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

Примечание. Если пользователь `nonenable` знает пароль **set enable**, то этот пользователь может продолжать работать в режиме enable.

После настройки пароли хранятся в зашифрованном виде.

Аутентификацию имени локального пользователя можно использовать в сочетании с удаленным TACACS+ exec, учетом command или удаленным учетом RADIUS exec. Ее также можно использовать в сочетании с удаленной авторизацией TACACS+ exec или command, но это не имеет смысла, поскольку имя пользователя должно храниться как на сервере TACACS+, так и локально в коммутаторе.

Шаг D - авторизация TACACS+ Command

В этом примере коммутатор получает указание требовать авторизацию только для команд конфигурации с TACACS+. В случае отказа сервера TACACS+, аутентификация отсутствует. Это относится как к порту консоли, так и к сеансу Telnet. Выполните следующую команду:

set authorization commands enable config tacacs none both

В этом примере сервер TACACS+ настраивается для разрешения при настройке следующих параметров:

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

Команда **set port enable 2/12** отправляется серверу TACACS+ для проверки.

Примечание. При включенной авторизации команд, в отличие от маршрутизатора, где

enable не считается командой, коммутатор отправляет команду **enable** серверу при попытке доступа. Убедитесь, что настройки сервера также разрешают команду **enable**.

Шаг E — авторизация TACACS+ Exec

В этом примере коммутатор получает указание требовать авторизацию только для сеанса exec с TACACS+. В случае отказа сервера TACACS+, авторизация отсутствует. Это относится как к порту консоли, так и к сеансу Telnet. Выполните команду **set authorization exec enable tacacs+ none both**

Помимо запроса аутентификации коммутатор отправляет отдельный запрос авторизации серверу TACACS+. Если профиль пользователя настроен для режима shell/exec на сервере TACACS+, то он может получить доступ к коммутатору.

Это предотвращает вход в коммутатор пользователей, для которых не настроена служба shell/exec на сервере, например PPP пользователей. Появится следующее сообщение: `Exec mode authorization failed` (Не удалось выполнить авторизацию режима Exec). Помимо разрешения или запрещения режима exec для пользователей, возможен принудительный перевод в режим enable, когда вход выполняется с уровнем разрешений 15, назначенным на сервере. На нем должно выполняться ПО с исправленной ошибкой с идентификатором Cisco CSCdr51314 (только длязарегистрированных пользователей).

Шаг F — авторизация RADIUS Exec

Отсутствует команда включения авторизации RADIUS exec. Другой способ состоит в том, чтобы задать для Service-Type (атрибут 6 RADIUS) значение Administrative (значение 6) на сервере RADIUS для включения пользователя в режиме enable на этом сервере. Если атрибуту Service-Type задано любое другое значение, отличное от 6-Administrative, например 1-login, 7-shell или 2-framed, пользователю предлагается начать работу в командной строке коммутатора с приглашением exec, а не enable.

Добавьте эти команды в коммутатор для аутентификации и авторизации:

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

Шаг G — Учет – TACACS+ или RADIUS

Чтобы включить учет TACACS+ для пользователей в случае:

- Если доступна командная строка коммутатора, выполните команду **set accounting exec enable start-stop tacacs+**.
- В случае завершения сеанса Telnet с коммутатором выполните команду **set accounting exec enable start-stop tacacs+**.
- В случае перезагрузки коммутатора выполните команду **set accounting exec enable start-stop tacacs+**.
- В случае выполнения команд выполните команду **set accounting commands enable all**

start-stop tacacs+.

Для напоминания серверу, например, об обновлении записей раз в минуту, чтобы отображать состояние входа пользователя, выполните команду **set accounting update periodic 1**.

Чтобы включить учет RADIUS для пользователей в случае:

Если доступна командная строка коммутатора, выполните команду **set accounting exec enable start-stop radius**.

В случае завершения сеанса Telnet с коммутатором выполните команду **set accounting connect enable start-stop radius**.

В случае перезагрузки коммутатора выполните команду **set accounting system enable start-stop radius**.

Для напоминания серверу, например, об обновлении записей раз в минуту, чтобы отображать состояние входа пользователя, выполните команду **set accounting update periodic 1**.

Записи TACACS+ Freeware

Ниже приведен пример вывода, иллюстрирующий отображение записей на сервере:

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

Вывод записей RADIUS на UNIX

Ниже приведен пример вывода, иллюстрирующий отображение записей на сервере:

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

Шаг H — аутентификация TACACS+ Enable

Выполните следующие действия.

Выполните команду **set authentication enable local enable**, чтобы оставить запасной вариант входа в коммутатор в случае отказа сервера.

Выполните команду **set authentication enable tacacs enable**, чтобы указать коммутатору отправить запросы режима enable серверу.

Шаг I – аутентификация RADIUS Enable

Добавьте эти команды, чтобы коммутатор отправил имя пользователя `$enab15$` серверу RADIUS. Не все серверы RADIUS поддерживают этот тип имени пользователя. Другой способ см. в описании шага E, например, если задать атрибут service-type [атрибуту 6 RADIUS значение Administrative] произойдет включение отдельных пользователей в режиме enable.

Выполните команду **set authentication enable local enable**, чтобы оставить запасной вариант входа в коммутатор в случае отказа сервера.

Выполните команду **set authentication enable radius enable**, чтобы указать коммутатору отправить запросы режима enable серверу, если сервер RADIUS поддерживает имя пользователя $enab15$.

Шаг J — авторизация TACACS+ Enable

В результате добавления этой команды коммутатор отправляет запрос режима enable серверу при попытке пользователя войти в этот режим. Необходимо, чтобы на сервере была разрешена команда **enable**. В этом примере в случае отказа сервера обработка этой ситуации завершается ничем:

set author enable enable tacacs+ none both

Шаг K – аутентификация Kerberos

Дополнительные сведения о настройке Kerberos для коммутатора см. в Контроль и управление доступом к коммутатору с помощью аутентификации, авторизации и учета.

Восстановление пароля

Сведения о процедурах восстановления паролей см. в Процедуры восстановления пароля.

На этой странице приводится указатель процедур восстановления пароля для продуктов Cisco.

Команды ip permit для дополнительной безопасности

Чтобы повысить безопасность, Catalyst можно настроить для контроля доступа по протоколу Telnet посредством команд **ip permit**.

set ip permit enable telnet

set ip permit *маска диапазона*|*узел*

В результате только указанные узлы или диапазон узлов получают доступ по протоколу Telnet к коммутатору.

Отладка на Catalyst

Просмотрите журналы на сервере, чтобы определить причину ошибки прежде чем включать отладку Catalyst. Это облегчает отладку и уменьшает риски для коммутатора. В коммутаторах более ранних версий **debug** выполнялась в инженерном режиме. При использовании ПО более поздних версий необязательно переходить в инженерный режим для выполнения команд **debug**:

set trace tacacs|radius|kerberos 4

Примечание. Команда **set trace tacacs|radius|kerberos 0** возвращает Catalyst в режим без трассировки.

Дополнительные сведения о многоуровневых коммутаторах локальной сети см. на странице поддержки коммутаторов.

Дополнительные сведения

- Сравнение TACACS+ и RADIUS
- RADIUS, TACACS+ и Kerberos в документации Cisco IOS
- Страница поддержки RADIUS
- Страница поддержки TACACS/TACACS+
- Страница поддержки Kerberos
- Документы RFC
- Cisco Systems – техническая поддержка и документация