Как назначать уровни привилегий при использовании TACACS+ и RADIUS

Содержание

Введение

В данном документе описывается порядок изменения уровня привилегий для различных команд, а также приведены примеры конфигурации для маршрутизатора и сервера TACACS+ и RADIUS.

Предварительные условия

Требования

Читатели данной документации должны ознакомиться с уровнями привилегий на маршрутизаторе.

По умолчанию на маршрутизаторе существует три уровня привилегий.

- уровень привилегий 1 = непривилегированный (приглашением является `router>`), уровень по умолчанию для регистрации
- `privilege level 15 = privileged (prompt is router#), enable`
- уровень привилегий 0 = редко используемый, но включает 5 команд: **отключите**, **включите**, **выйдите**, **помогите**, и **выход из системы**

Уровни 2-14 не используются в стандартной конфигурации, но команды уровня 15 можно опустить до одного из предшествующих уровней, а команды уровня 1 - поднять. Очевидно, данная модель безопасности предусматривает применение определенных функций управления маршрутизатором.

Чтобы определить уровень привилегий, являясь зарегистрированным пользователем, введите команду show privilege. Чтобы определить, какие команды доступны на конкретном уровне привилегий для используемой версии программного обеспечения Cisco IOS®,

введите в командной строке команду ? на этом уровне привилегий.

Примечание: Если сервер проверки подлинности поддерживает TACACS +, вместо того, чтобы назначить уровни привилегий, можно сделать авторизацию для выполнения команд. Протокол RADIUS не поддерживают командную авторизацию.

Используемые компоненты

Сведения в этом документе основываются на программном обеспечении Cisco IOS версии 11.2 и позже.

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Пример

В данном примере команды snmp-server переносятся с уровня привилегий 15 (по умолчанию) на уровень привилегий 7. Команда ping переносится с уровня привилегий 1 на уровень привилегий 7. После проверки пользователя seven сервер назначает ему уровень привилегий 7, а команда show privilege показывает "Current privilege level is 7". В режиме настройки пользователь может выдавать команды ping и snmp-server configuration. Другие команды настройки недоступны.

Конфигурации: маршрутизатор

Маршрутизатор - 11.2

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Маршрутизатор выпуска 11.3.3.T и более поздних (до 12.0.5.T)

```
aaa new-model
aaa authentication login default tacacs+|radius local
```

```
aaa authorization exec default tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Маршрутизатор выпуска 12.0.5.T и более поздних

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Конфигурации - сервер

TACACS Cisco Secure NT +

Чтобы настроить сервер, выполните данные шаги.

1. Введите имя пользователя и пароль.
2. Убедитесь в том, что в разделе Group Settings установлен флажок shell/exec и в текстовом поле уровня привилегий введено число 7.

TACACS+ - Stanza в свободно распространяемом сервере

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Cisco Secure UNIX TACACS+

```
aaa new-model
```

```
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

RADIUS Cisco Secure NT

Чтобы настроить сервер, выполните данные шаги.

1. Введите имя пользователя и пароль.
2. **В групповых настройках для IETF, тип сервиса (атрибут 6) = Nas-Prompt**
3. **В области CiscoRADIUS проверьте AV-Pair и введите в прямоугольное поле ниже: shell:priv-lvl=7.**

Cisco Secure UNIX RADIUS

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Это пользовательский файл для имени пользователя "seven."."

Примечание: Сервер должен поддерживать Cisco av-pairs.

- **седьмой пароль = passwdxyz**
- **Service-Type = Shell-User**
- cisco-avpair **=shell:priv-lvl=7**

Дополнительные сведения

- Страница поддержки RADIUS
- Запросы комментариев (RFC)
- TACACS+ в документации по IOS
- Страница поддержки TACACS+
- Страница поддержки Cisco Secure UNIX
- Страница поддержки Cisco Secure ACS для Windows

- Техническая поддержка - Cisco Systems