Уровни привилегии IOS не могут видеть полную работающую конфигурацию

Содержание

Введение

В этом документе поясняется влияние уровней полномочий на возможность выполнения определенных команд пользователем на маршрутизаторе.

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 Технические рекомендации Cisco. Условные обозначения.

Просмотрите конфигурацию маршрутизатора

Когда доступ к маршрутизатору настроен уровнями привилегий, общая проблема - то, что **выполнение показа** или **команды write terminal** настроены в или ниже уровня привилегий пользователя. Когда пользователь выполняет команду, конфигурация, кажется, пробел. Это фактически дизайном по этим причинам:

- **Write terminal** / **команда show running-config** показывает пустую конфигурацию. Эта команда отображает все команды, которые текущий пользователь в состоянии модифицировать (другими словами, все команды в или ниже текущего уровня привилегий пользователя). Команды отображения команды should not выше текущего уровня привилегий пользователя из-за учитываемых факторов безопасности. Если так, команды, такие как **snmp-server community** могли использоваться, чтобы модифицировать текущую конфигурацию маршрутизатора и получить полный доступ к маршрутизатору.
- **Show config** / **команда show start-up config** отображает полную конфигурацию, но действительно не показывает фактическую конфигурацию. Вместо этого команда просто распечатывает содержание NVRAM, который, оказывается, конфигурация маршрутизатора в то время, когда пользователь делает **write memory**.

Уровни привилегий

Чтобы позволить привилегированному пользователю просмотреть полную конфигурацию в памяти, пользователь должен модифицировать привилегии для всех команд, которые настроены на маршрутизаторе. Пример:

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local

username john privilege 9 password 0 doe
username six privilege 6 password 0 six
username poweruser privilege 15 password poweruser
username inout password inout
username inout privilege 15 autocommand show running

privilege configure level 8 snmp-server community
privilege exec level 6 show running
privilege exec level 8 configure terminal
```

Для понимания данного примера необходимо понять уровни привилегий. По умолчанию на маршрутизаторе имеются три уровня команд:

- уровень привилегий 0 — Включает **запрещение**, **включите**, **выйдите**, **помогите**, и команды **выхода из системы**.
- уровень привилегий 1 — Обычный уровень на Telnet; включает все команды пользовательского уровня в приглашение `router>`.
- уровень привилегий 15 — Включает все команды разрешать-уровня в приглашение `router#`.

Команды, доступные на определенном уровне в конкретном маршрутизаторе, могут быть найдены путем ввода а**?** в командной строке маршрутизатора. Команды могут быть перемещены между уровнями привилегий при помощи команды **привилегии**, как проиллюстрировано в примере. В то время как данный пример показывает локальную проверку подлинности и авторизацию, команды работают так же для TACACS + или Проверка подлинности RADIUS, и проверка авторизации в режиме EXEC (больше глубины детализации в контроле маршрутизатора может быть достигнуто с реализацией TACACS + авторизация для выполнения команд с сервером.)

Дополнительные сведения на пользователях и уровнях привилегий представили в примере:

- Пользователь *шесть* в состоянии к Telnet в, и выполните **команду show run**, но итоговая конфигурация фактически пуста, потому что этот пользователь ничего не может настроить (**configure terminal** на уровне 8, не на уровне 6). Пользователю не разрешают видеть имена пользователя и пароли других пользователей или видеть информацию о Протоколе SNMP.
- *Пользователь с именем Джон* в состоянии к Telnet в, и выполните **команду show run**, но только видит команды, которые он может настроить (часть **snmp-server community** конфигурации маршрутизатора, так как этот пользователь является нашим администратором управления сетью). Он может настроить **snmp-server community**, потому что **configure terminal** на уровне 8 (в или ниже уровня 9), и **snmp-server community** является командой уровня 8. Пользователю не разрешают видеть имена пользователя и пароли других пользователей, но ему доверяют конфигурацию SNMP.
- *Вход/выход пользователя* в состоянии к Telnet в, и, на основании того, чтобы быть настроенным для **покажите выполнение autocommand**, видит отображенную конфигурацию, но разъединен после того.
- *Пользователь poweruser* в состоянии к Telnet в и выполнить **команду show run**. Этот пользователь на уровне 15 и в состоянии видеть все команды. Все команды в или ниже уровня 15; пользователи на этом уровне могут также просмотреть и управлять именами пользователя и паролями.

Дополнительные сведения

- Средство поиска команд Command Lookup Tool (зарегистрированный только клиенты)
- Документация IOS для TACACS + и RADIUS
- Страница поддержки TACACS/TACACS+
- Страница поддержки RADIUS
- Запросы комментариев (RFC)
- Техническая поддержка - Cisco Systems