Часто задаваемые вопросы по коммутатору служб контента

Содержание

Введение

В данном документе рассмотрены часто задаваемые вопросы, связанные с Cisco Content Services Switch (CSS).

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

Вопрос. . Где я могу найти MIB для CSS?

О. MIB уже находятся на CSS. CSS можно рассматривать как агент в схеме сети SNMP. Вам остается только настроить параметры SNMP на CSS. Дополнительную информацию см. в документе Настройка протокола SNMP.

Вопрос. . Каково максимальное число сценариев поддержки активности, поддерживаемых CSS?

О. Максимальное число заданных сценарием средств поддержки активности, которые поддерживает CSS, 255. См. *Новые характеристики в* разделе *Версии программного обеспечения 5.00* Комментариев к выпуску для Cisco Коммутатор контент-сервисов серии 11000.

Вопрос. . Как очистить или удалить файлы ядра?

О. Выполните **команду clear core**. Команда доступна в ПО CSS 5.00 и более поздних версий в режиме отладки. Синтаксис:

```
css150(debug)#clear core filename CR
```

Вопрос. . Где можно найти интерпретированные сообщения журнала?

О. Для интерпретаций сообщений журнала обратитесь к документу Сообщения журнала.

Вопрос. . Есть ли команда, управляющая частотой отправки узлами друг другу отчетов о загрузке?

О. Можно использовать команду dns-peer interval. Кроме того, есть и другие команды – они настраиваются локально и дают более быструю оценку локальной загрузки:

- **ageout-timer** — Устанавливает время (в секундах) ageout устаревшей информации о загрузке.
- **teardown-timer** — Устанавливает максимальный временной интервал (в секундах), что система ждет для передачи отчета об освобождении.

Вопрос. . Изменяются ли ключи лицензии с переменой версии кода?

О. Нет, ключи лицензии не изменяются с переменой версии кода.

Вопрос. . Я потерял свой лицензионный ключ. Какие действия следует

предпринять?

О. Пошлите электронное письмо с серийным номером вашего CSS к licensing@cisco.com. **Выходные данные команды version содержат набор функций, а не лицензионный ключ.**

Вопрос. . Сколько времени по умолчанию хранится запись в таблице Sticky-объектов?

О. Пока вы не используете **команду sticky-inact-timeout**, нет никакого времени по умолчанию. Таблица Sticky-объектов используется по принципу FIFO (32 000 или 128 000 записей – в зависимости от типа устройства и доступного объема памяти), и хранится до перезагрузки CSS.

Вопрос. . Как настроить маску закрепления в памяти, чтобы закрыть запросы от мега-прокси, вроде Америка онлайн (AOL)?

О. Если приложение требует, чтобы пользователь застрял для всей жизни сеанса, рассмотрите sticky Уровня 3. В этом случае пользователь закрепляется за сервером на основании IP-адреса пользователя. Объем таблицы Sticky-объектов в CSS – 32 000, то есть когда на узле одновременно присутствует более 32 000 пользователей, таблица сворачивается и закрепление с первого пользователя снимается. Однако узел может быть весьма масштабным – на нем может быть более 32 000 пользователей одновременно –. Или большая часть клиентов может приходить через мега-прокси. В таких случаях стоит использовать другой метод закрепления (например cookie, cookieurl или url) или расширять маску закрепления. Маска закрепления в памяти по умолчанию - 255.255.255.255, то есть каждая запись в таблице закрепления в памяти представляет собой отдельный IP-адрес. На некоторых мега-прокси случается, что пользователь в течение одного сеанса использует несколько IP-адресов из некоего диапазона. Это приводит к тому, что часть TCP-соединений закрепляются на одном сервере, из-за чего другие соединения, связанные с той же транзацией, закрепляются на другом. В результате чать элементов из корзины может пропасть. Когда нет возможности использовать более сложные методы закрепления, используйте маску 255.255.240.0, если большая часть ваших клиентов приходит через один из этих мега-прокси.

Вопрос. . Почему при использовании Secure Socket Layer (SSL) с улучшенным балансом не предоставляется возможность закрепления?

О. SSL расширенной балансировки совпадает с sticky SSL.

Вопрос. . Какой тип шифрования используют протоколы CAPP и APP?

О. По умолчанию CAPP не использует шифрования. Сеанс APP можно настроить так, чтобы использовался алгоритм Message Digest 5 (MD5). Тип шифрования на обоих одноранговых узлах должен совпадать, иначе сеанс APP не будет установлен.

Вопрос. . Что означает сообщение "gratuitous arp"?

О. Когда резервный коммутатор не обнаруживает биение от основного коммутатора в течение 3 секунд, переходы резервного коммутатора для становления ведущим устройством и передает "бесплатного arp" сообщение. Оно подтверждает передачу ARP с

нового основного коммутатора. В сообщении содержится MAC-адрес коммутатора, являющегося основным в данный момент времени. Бесплатный arp включен **командой ip gratuitous-arps** в режиме глобальной конфигурации. Это не может быть включено на одном интерфейсе и заблокировать его на других интерфейсах.

Вопрос. . Как синхронизировать конфигурации с помощью CSS в режиме обхода отказа?

O. Для синхронизации конфигураций в версии программного обеспечения 4.0 используйте **команду commit config sync**. В ПО версии 3.10 для переноса конфигурации с одного коммутатора на другой необходимо использовать FTP. **В ПО версий 6.x и 7.x синхронизация выполняется при помощи команды commit_redundancy для активного/аварийного резервирования или резервирования между устройствами. Для резервирования виртуальных IP (VIP) и интерфейсов можно использовать команду commit_vip_redundancy. Команду show script commit_redundancy можно использовать для просмотра доступных параметров командной строки для сценария commit_redundancy – они указаны в заголовке сценария. То же самое относится к команде commit_vip_redundancy.**

Вопрос. . Какие настройки следует использовать в терминальной программе?

O. Используйте эти параметры настройки:

- 9600 бод
- 8 битов
- Без контроля четности
- 1 стоповый бит
- No flow control

Вопрос. . Есть ли способ перепрограммировать MAC-адрес на CSS?

O. Да, существует путь.

Примечание: MAC-адрес и серийный номер указаны на задней стороне устройства.

Для перепрограммирования серийного номера и MAC-адреса выполните следующие действия. Это пример для MAC-адреса в шасси CS800:

1. **Откройте автономный диагностический монитор (ODM).**
2. **В основном меню ODM нажмите Shift-T, чтобы перейти в меню инженера.**
3. **Выберите пункт 1 (Настройка).**
4. **Выберите пункт 5 (Установить информацию производителя).**
5. **Выберите пункт 2 (Установить информацию производителя объединительной карты).**
6. Следуя подсказкам, введите соответствующие данные: серийный номер, MAC-адрес. Данные эти можно найти на крышке шасси CS800.
7. Перезапустите сервер.

Вопрос. . Как изменить приглашение на CSS так, чтобы оно сохранялось постоянно?

O. Войдите к коробке CSS как пользователь Fred и используйте свои учетные данные входа в систему. Чтобы изменить приглашение, выполните следующую команду:

```
Css100#prompt Redsox
<cr>
Redsox#
```

Чтобы сохранить изменения, выполните следующую команду:

```
Redsox#save_profile
```

Эта команда сохраняет профиль пользователя. Теперь при каждом входе пользователя в систему CSS будет использовать одно и то же приглашение. **При этом – как при использовании файлов ресурсов ?.? в UNIX – создается уникальный профиль для каждого пользователя.**

Когда вы возвращаетесь в CSS и входите в систему под учетной записью администратора, изменений приглашения вы не видите. **Изменения действуют только для одного пользователя, то есть команды prompt и save_profile нужно выполнить для каждого пользователя, желающего использовать другое приглашение.**

Вопрос. . В чем заключается отличие между работающей и заблокированной флэш-памятью?

O. Данный пример показывает различные типы Флэша, что отображается **команда Show version**:

```
CSS150-2#show version
Version:               ap0401049s (4.01 Build 49)
Flash (Locked):        3.10 Build 33
!--- This image is the original image that was installed on the CSS. !--- The image serves as a
backup in the event that the CSS is not able !--- to boot from the operational Flash because of
an image corruption. Flash (Operational):   5.00 Build 10-
!--- This is the image that currently runs on the CSS. Type: PRIMARY Licensed Cmd Set(s):
Standard Feature Set Enhanced Feature Set SSH Server
```

Вопрос. . Почему существуют различные версии флэш-памяти?

O. Блокировка flash - память показывает версию ПО, которая была первоначально установлена на том CSS. Эта версия не изменяется, она используется только в качестве резервной. Версия, хранящаяся в работающей флэш-памяти – это версия, которая в данный момент запущена на CSS.

Вопрос. . Почему я не могу попасть на порт управления CSS с удаленного порта?

O. Во всех версиях Cisco WebNS, которые являются ранее, чем 5.03, порт управления не является маршрутизируемым интерфейсом. В версии 5.03 он может быть маршрутизируемым: для этого нужно добавить к порту управления шлюз по умолчанию.

Вопрос. . Поддерживает ли техническая поддержка Cisco сценарии обеспечения активности, написанные пользователем?

O. Нет, [техническая поддержка Cisco] не поддерживает сценарии поддержки активности, которые пишет клиент.

Вопрос. . Как удалить файлы ядра с диска CSS?

О. После запуска **команды show core** при обнаружении списка ключевых файлов можно удалить файлы одним из двух способов:

Примечание: Метод, который вы используете, зависит от версии кода.

- `CSS50-1(config)#llama`
  `!--- This command places the CSS in debug mode.` `CSS50-1(debug)#clear core corefilename`

или

- `CSS50-1(config)#llama`
  `!--- This command places the CSS in debug mode.` `CSS50-1(debug)#dir c:/Core/?`
  `!--- This command lists the names of all the core !--- files in the c:/Core directory.`
  `CSS50-1(debug)#ap_file delete c:/Core/ corefilename`
  `!--- This command deletes the specified core file.`

Вопрос. . Когда я аутентифицируюсь на сервере RADIUS со своим CSS, я получаю сообщение об ошибке «RADIUS-4: RADIUS Authentication failed with reason code 2». Что означает это сообщение?

О. Это сообщение об ошибках указывает, что ответ достиг CSS и существует проблема. Причина может состоять в том, что на сервере RADIUS не удалось установить значение administrative для атрибута типа службы. Проверьте сервер RADIUS и атрибуты типа службы.

Вопрос. . Насколько велика таблица Sticky-объектов и что вызывает удаление записей в ней?

О. CSS имеет 32,000 или 128,000 (который зависит от типа модели и доступной памяти), таблица закрепления в памяти, которая содержит записи для **IP постоянного источника** и sticky Протокола SSL. Таблица Sticky-объектов не поддерживает закрепленные cookie на CSS. Записи из таблицы удаляются в следующих случаях:

- По умолчанию работает принцип FIFO. Записи хранятся в таблице, пока не заполнится буфер размером 32 000 или 128 000. В это время любые новые записи заставляют CSS удалять запись на основе FIFO.
- **sticky-inact-timeout minutes**. В правиле контента можно указать предельный период неактивности, по прошествии которого CSS будет удалять запись из таблицы Sticky-объектов. Пример приведен ниже:`CSS50-1(config)#llama`
  `!--- This command places the CSS in debug mode.` `CSS50-1(debug)#dir c:/Core/?`
  `!--- This command lists the names of all the core !--- files in the c:/Core directory.`
  `CSS50-1(debug)#ap_file delete c:/Core/ corefilename`
  `!--- This command deletes the specified core file.` **Примечание:** Когда все эти элементы истинны, CSS отклоняет следующий запрос сообщений на экране в случае:**Используется параметр sticky-inact-timeout.**Буфер в 32 000 или 128 000 на CSS заполнен.Нет записей, у которых истекает период хранения.
- Правило контента. При продлении или повторной активации правила контента производится удаление записей таблицы Sticky-объектов, к которым применимо данное правило.

Дополнительные сведения см. в документе Настройка Sticky-параметров для правил

контента.

Вопрос. . Как вывести службу из обращения?

О. С конфигурацией правила содержимого (Уровень 3, Уровень 4 или Уровень 5) как основание, CSS ведет себя по-другому с созданием WinSock сервиса, который берет сервер вне обслуживания. Очень часто разработчикам веб-приложений приходится временно приостанавливать службы, чтобы вносить в веб-страницы изменения, связанные с администрированием. Поскольку такие изменения могут вноситься в рабочее время, существующие соединения со службой или службами во время ручной приостановки могут быть прерваны, что нежелательно. Обновление служб следует выполнять, когда работа службы приостановлена.

В данном примере показаны правила контента уровня 5, 4 и 3:

```
CSS50-1(config)#llama
!--- This command places the CSS in debug mode. CSS50-1(debug)#dir c:/Core/?
!--- This command lists the names of all the core !--- files in the c:/Core directory. CSS50-
1(debug)#ap_file delete c:/Core/ corefilename
!--- This command deletes the specified core file.
```

CSS переадресует существующие соединения при использовании правил уровня 3 и 4. Если происходит приостановка службы при использовании правил уровня 3 или 4, CSS переадресует каждое установленное соединение и перенаправит все последующие TCP-запросы на активную службу согласно соответствующему правилу контента.

При ручной приостановке службы по правилу уровня 5 CSS восстановит соединения, связанные с данной службой.

Вопрос. . Является ли network proximity частью расширенного набора функций?

О. Функции сетевой близости не являются частью расширенного набора функций и требуют дополнительной лицензии. **Если попытаться выполнить команду proximity на CSS без соответствующей лицензии, вы получите сообщение об ошибке:**

```
CSS50-1(config)#proximity db 0 tier1
                              ^
%% Invalid License to execute command.
This command belongs to the Proximity Database.  Refer
to the user manual or contact Cisco Systems, Inc for
further information concerning license keys.
```

Приобрести лицензию вы можете у официального дилера Cisco в вашем регионе. Если вы приобрели лицензию и вам требуется замена, отправьте письмо по адресу licensing@cisco.com.

Вопрос. . Какие данные выдает команда show dos?

О. CSS Cisco может отобразить подробные данные о новых событиях атаки, которые включают:

- IP-адреса источника и получателя
- Тип события
- Общие вхождения

Если множественные атаки происходят с тем же типом Отказа в обслуживании (DoS) и адресом источника и назначения, существует попытка объединить их как одно событие. Это сокращает объем отображаемой информации о событиях.

Выполните команду show dos, чтобы получить следующие сведения:

- Общее число атак начиная с начальной загрузки CSS
- Типы атак и максимальное число этих атак в секунду
- Первое и последнее возникновение атаки

Данный пример показывает выходные данные от **команды show dos**:

```
CSS50-1#show dos
Denial of Service Attack Summary:
Total Attacks: 0
SYN Attacks:                          0 Maximum per second:                 0
LAND Attacks:                         0 Maximum per second:                 0
Zero Port Attacks:                    0 Maximum per second:                 0
Illegal Src Attacks:                  0 Maximum per second:                 0
Illegal Dst Attacks:                  0 Maximum per second:                 0
Smurf Attacks:                        0 Maximum per second:                 0


No attacks detected
```

В следующем списке приведены краткие описания полей выходных данных команды:

- Total Attacks – DoS- . Описания типов атак, указываемых в списке, и их число приводятся ниже.
- SYN Attacks – TCP- , (TCP-).
- LAND Attacks – , . CSS не позволяет использовать внутренние IP-адреса в качестве источника потока. Кроме того, CSS не допускает совпадения адреса источника фрейма и адреса назначения.
- Zero Port Attacks – , TCP- UDP- , .**Примечание:** Более старое программное обеспечение SmartBits может передать кадры, которые содержат источник или порты назначения, равные нулю. CSS регистрирует их как DoS-атаки и сбрасывает.
- Illegal Src Attacks – .
- Illegal Dst Attacks – .
- Smurf Attacks – -, . CSS по умолчанию не поддерживает направленные широковещательные рассылки. Smurf Attack ICMP- . CSS может блокировать доступ к эхо-портам UDP при помощи списков ACL.
- Maximum per second – . Используйте эту информацию для настройки пороговых значений ловушки SNMP.**Примечание:** Максимальное число событий в секунду является максимумом на Миниатюрный форм-фактор, Сменный (SFP). На CSS 11800, к примеру, может быть до четырех SFP, а значит максимальное число событий в секунду фактически может в четыре раза превышать значение, указанное в выходных данных.**Примечание:** Другие часто задаваемые вопросы спрашивают, можно ли запретить защиту от атак DoS на CSS. Нет, нельзя. DoS-защита является частью процесса допуска потока. Ее задача – защищать ресурсы CSS и сервера, стоящего за CSS. DoS настраивать нельзя. DoS-защита должна быть прозрачной при правильной работе протоколов. Процесс создания потока тесно связан с функциями DoS. Они помогают CSS сохранять быстрые маршруты и позволяют защитить устройства, с которыми взаимодействует CSS. Функции DoS есть во всех версиях ПО начиная с версии 3.0.

Для обнаружения возможных DoS-атак можно также использовать различные SNMP-ловушки. Ловушки доступны следующие:

- **snmp trap-type enterprise — чтобы включить SNMP-ловушки enterprise и настроить их типы, используйте команду snmp trap-type enterprise. Команда no snmp trap-type enterprise отключает все ловушки.** Ловушки enterprise должны включаться до настройки параметра ловушек. Можно позволить CSS генерировать корпоративные ловушки, когда события DoS-атаки происходят, вход в систему отказывает, или состояние переходов сервиса CSS.
- ***dos_attack_type*** — Когда событие DoS-атаки происходит, генерирует корпоративные ловушки SNMP. Ловушка создается каждую секунду, если число атак в секунду превышает пороговое значение, установленное для DoS-атак. Имеются следующие варианты:**недопустимая атака dos** — Генерирует trap-сообщения для недопустимых адресов, или источник или назначение. К недопустимым адресам относятся:Петлевые адреса источникаШироковещательные адреса источникаПетлевые адреса назначения (DA)Адреса источника для групповой адресацииАдреса источника, которыми вы владеетеПорог прерывания по умолчанию для этого типа атаки является тем в секунду.**атака земли dos** — Генерируеты ловушку для пакетов, которые имеют идентичные адреса источника и назначения. Порог прерывания по умолчанию для этого типа атаки является тем в секунду.когда количество эхо-запросов превышает пороговое значение, **атака эхо-запроса dos** — Генерирует trap-сообщения. Стандартное пороговое значение для этого типа атак – 30 в секунду.**Примечание:** Эта опция не отслеживает атаки DoS деструктивных эхо-запросов.когда количество эхо-запросов с широковещательным адресом назначения превышает пороговое значение, **smurf-атака dos** — Генерирует trap-сообщения. Порог прерывания по умолчанию для этого типа атаки является тем в секунду.**dos-syn-attack** — Генерирует trap-сообщения, когда количество TCP - подключений, которые инициирует источник, но которые не придерживаются с кадром подтверждений для завершения квитирования TCP - подключения с тремя путями, превышает пороговое значение. Стандартное пороговое значение для этого типа атак – 10 в секунду.

Вопрос. . Можно ли отключить функцию DoS-защиты на линейке коммутаторов CSS?

О. В текущей линии программного обеспечения для CSS (Cisco WebNS) нет никакой опции для отключения опции защиты от атак DoS.

Вопрос. . Можно ли отключить счетчики DoS-защиты?

О. Нет никакой опции для отключения счетчиков та регистрационная DOS/АТАКИ SYN.

Примечание: Для получения дополнительной информации о DoS и Атаках SYN, посмотрите ответ на часто задаваемые вопросы, Какую подробную информацию **команда show dos** предоставляет?.

Вопрос. . Как использовать диапазоны портов в списках доступа?

О. Использование диапазонов портов в Списке контроля доступа (ACL) помогает упрощать

количество ACL, которые вы настраиваете учитывая ситуацию, в которой вы хотите блокировать пользовательский доступ для некоторого TCP/портов протокола пользовательских датаграмм (UDP). Допустим, нужно блокировать порты 20 – 23 для всех пользователей из внешней сети. Пусть внешняя сеть или общедоступная сторона CSS находится в сети VLAN 2, а внутренняя или серверная сторона сети находится в сети VLAN 1. ACL настраивается следующим образом:

```
CSS50-1#show dos
Denial of Service Attack Summary:
Total Attacks: 0
SYN Attacks:                        0 Maximum per second:                  0
LAND Attacks:                       0 Maximum per second:                  0
Zero Port Attacks:                  0 Maximum per second:                  0
Illegal Src Attacks:                0 Maximum per second:                  0
Illegal Dst Attacks:                0 Maximum per second:                  0
Smurf Attacks:                      0 Maximum per second:                  0


No attacks detected
```

Дополнительные сведения

- Конец объявления продажи для серии Cisco css 11000
- Бюллетени коммутаторов сервисов контента Cisco серии CSS 11000
- Техническая поддержка коммутаторов контент-сервисов CSS 11000
- Центр программного обеспечения (загрузки) - Сети передачи контента только для зарегистрированных пользователей)
- Cisco Systems – техническая поддержка и документация