Content Services Switch FAQ

Índice

Introdução

Este documento endereça mais frequentemente as perguntas feitas (FAQ) sobre o interruptor do Cisco Content Services (CSS).

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Q. Onde posso eu encontrar o MIBs para o CSS?

A. O MIBs está já no CSS. Você pode considerar o CSS um agente no esquema de rede do Simple Network Management Protocol (SNMP). Tudo que você precisa de fazer é configurar os parâmetros de SNMP no CSS. Refira o documento que configura o Simple Network Management Protocol (SNMP) para mais informação.

Q. Que é o número máximo de keepalive de script que o CSS apoia?

A. O número máximo de keepalive de script que o CSS apoia é 255. Refira os *novos recursos na* seção da *versão de software 5.00 do* Release Note para o Content Services Switch do Cisco 11000 Series.

Q. Como posso limpar ou remover arquivos principais?

A. Emita o **comando clear core**. O comando está disponível na versão 5.00 e mais recente do software CSS, debuga dentro o modo. A sintaxe é:

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

Q. Onde encontro interpretações das mensagens do registro?

A. Para interpretações dos mensagens de registro, refira os mensagens de registro do documento.

Q. Existe um comando que controla a freqüência com que os correspondentes enviam relatórios de carga uns aos outros?

A. É possível usar o comando dns-peer interval. Há igualmente os comandos adicionais que você pode configurar localmente a fim conseguir uma medida mais rápida da carga local:

- **ageout-temporizador** — Ajusta a época (nos segundos) do ageout da informação de carga vencida.
- **teardown-temporizador** — Ajusta o período máximo (nos segundos) que o sistema espera para enviar a uns relatórios de destruição.

Q. As chaves de licença mudam com as versões do código?

A. Não, as chaves de licença não mudam com as versões de código.

Q. Perdi minha chave de licença. Que eu faço?

A. Envie um email com o número de série de seu CSS a licensing@cisco.com. **O comando version** indica o pacote de recurso, mas não a chave de licença.

Q. Que é o tempo padrão para a retenção de uma entrada em uma tabela difícil?

A. A menos que você usar o comando sticky-inact-timeout, não há nenhum tempo padrão. A tabela difícil é mantida em uma base FIFO (32,000 ou 128,000 entradas, de acordo com o tipo de dispositivo e a memória disponíveis), ou até a repartição do CSS.

Q. Como eu configuro a máscara aderente a fim cobrir pedidos de um mega proxy como America Online (AOL)?

A. Se um aplicativo exige um usuário ser colado para a vida inteira da sessão, considere um Sticky da camada 3. Uma camada 3 pegajosa cola um usuário a um server com base no endereço IP de Um ou Mais Servidores Cisco ICM NT do usuário. O CSS tem uma tabela difícil de 32,000, assim que significa que quando 32,000 usuários simultâneos estão no local, os envoltórios da tabela e os primeiros usuários tornam-se “soltos”. Contudo, o volume de seu local pode ser tal que você tem mais de 32,000 usuários de cada vez. Ou um percentual alto de seus clientes pode vir-lhe com um mega proxy. Nesses casos, considere o uso de um método difícil diferente (tal como o Cookie, o cookieurl, ou a URL) ou um aumento de sua máscara aderente. A máscara permanente padrão é 255.255.255.255, o que significa que cada entrada na tabela permanente é um endereço IP individual. Alguns dos megas proxys têm uma situação em qual o usuário sobre a vida de uma sessão usa diversos endereços IP de Um ou Mais Servidores Cisco ICM NT diferentes em um intervalo de endereço. Esta situação faz com algumas das conexões de TCP obtenham coladas a um server, e pode fazer com que outras conexões obtenham coladas a um server diferente para a mesma transação. Um resultado pode ser a perda de alguns artigos do carrinho de supermercado. Se você não pode usar um dos métodos mais avançados da colagem, use a máscara aderente de 255.255.240.0 quando sua base do cliente vem com um destes megas proxys.

Q. Por que há nenhuma opção para o Sticky quando eu uso o advanced-balance secure socket layer (SSL)?

A. O balanceamento avançado SSL é o mesmo que o Sticky SSL.

Q. Que tipo de criptografia o Content and Application Peering Protocol (CAPP) ou o protocolo application peering (APP) usam?

A. À revelia, o CAPP usa o no encryption. Você pode configurar a sessão de app para usar o message digest 5 (MD5). O tipo de criptografia deve ser o mesmo em ambos os pares para que a sessão de app venha acima.

Q. O que a mensagem "ARP gratuito" significa?

A. Quando o switch de backup não detecta uma pulsação do coração do switch mestre dentro de 3 segundos, as transições do switch de backup a transformar-se o mestre e enviam “uma mensagem arp gratuito”. A mensagem indica um transmissor do Address Resolution Protocol (ARP) do switch mestre novo. A mensagem contém o MAC address do switch mestre atual. O arp gratuito é permitido pelo comando **IP gratuito-ARP no** modo de configuração global. Não pode ser permitido em uma interface única e obstrui-la em outras relações.

Q. Como sincronizo configurações sobre o CSS no modo de failover?

A. A fim sincronizar configurações na versão de software 4.0, use o **comando commit config sync**. A fim sincronizar configurações no código da versão de software 3.10, você deve usar o FTP a fim mover a configuração de um interruptor para outro. A fim sincronizar configurações nas versões de software 6.x e 7.x codifique, use o comando commit_redundancy para o active/apoio ou a redundância de caixa a caixa. Ou você pode usar o comando commit_vip_redundancy para a Redundância do IP virtual (VIP) /interface. Você pode usar o comando show script commit_redundancy a fim ver no encabeçamento do script as opções de linha de comando disponíveis para o script do **commit_redundancy**. O mesmo aplica-se ao **comando commit_vip_redundancy**.

Q. Quais configurações devo utilizar em um programa terminal?

A. Use estes ajustes:

- 9600 bauds
- 8 bits
- Sem paridade
- 1 bit de parada
- Nenhum controle de fluxo

Q. Há uma maneira de reprogram o MAC address em um CSS?

A. Sim, há uma maneira.

Nota: É possível encontrar o endereço MAC e o número de série na parte de trás da unidade.

Termine estas etapas a fim reprogram o número de série e o MAC address. Este exemplo é para um endereço MAC no chassi CS800.

1. Abra o **Offline Diagnostic Monitor (ODM)**.
2. No menu principal ODM, pressione a **SHIFT-T** a fim alcançar o menu de técnico.
3. Escolha **1** (configurar).
4. Escolha **5** (ajuste a informação da fabricação).
5. Escolha **2** (ajuste a informação da fabricação do backplane).
6. Siga a alerta e incorpore os dados que correspondem, como o número de série e o MAC address. Você pode encontrar estes dados na parte superior do chassi CS800.
7. Reinicialize a caixa.

Q. Como eu faço uma mudança alerta permanente no CSS?

A. Entre à caixa CSS como o usuário fred, e use suas credenciais do início de uma sessão. A fim fazer uma mudança alerta permanente, emita este comando:

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

Emita este comando salvar a mudança:

```
Redsox#save_profile
```
Este comando salvar o perfil de usuário de modo que cada vez que o usuário entra, o CSS use a mesma alerta. Esta ação, similar para usar-se do**?.?** os arquivos de recurso em UNIX, criam um perfil original para cada usuário.

Quando você vai para trás ao CSS e ao início de uma sessão como o admin, a alerta não reflete estas mudanças. As mudanças são específicas de usuário, assim que você precisa de emitir os **comandos prompt e save_profile** para cada usuário que quer mandar a alerta refletir a mudança nova.

Q. Que é a diferença entre o flash operacional e bloqueado?

A. Este exemplo mostra os tipos diferentes de flash que o **comando show version** indica:

```
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
```

Q. Por que há versões diferentes do flash?

A. O flash bloqueada mostra a versão de software que foi instalada originalmente nesse CSS. A versão permanece a mesma e serve somente como um backup. A versão no flash operacional é a versão que é executado atualmente nesse CSS.

Q. Por que não posso eu alcançar a porta de gerenciamento do CSS de uma porta remota?

A. Em todas as versões de Cisco WebNS que estão mais adiantadas de 5.03, a porta de gerenciamento não é uma interface roteável. Na versão 5.03, você pode adicionar um gateway padrão à porta de gerenciamento a fim fazer à porta uma interface roteável.

Q. O Suporte técnico de Cisco apoia o Keepalives do script personalizado que o cliente escreve?

A. Não, Suporte técnico de Cisco não apoia os scripts do keepalive que um cliente escreve.

Q. Como eu removo os arquivos principais do disco CSS?

A. Se, depois que você emite o **comando show core**, você encontra uma lista de arquivos principais, você pode remover os arquivos em uma de duas maneiras:

Nota: O método que você se usa depende da versão de código.

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

ou

- ```
  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.
```

Q. Quando eu autentico a um servidor Radius com meu CSS, eu obtenho o "RADIUS-4: Autenticação RADIUS falhada com Mensagem de Erro do código de motivo 2". O que significa a mensagem?

A. Este Mensagem de Erro indica que a resposta alcançou o CSS e há um problema. Uma falha ajustar o atributo de tipo de serviço a administrativo no servidor Radius pode ser a causa do problema. Verifique o servidor Radius e verifique os atributos de tipo de serviço.

Q. Como grande é a tabela difícil, e o que causa a remoção de entradas?

A. O CSS tem (que depende do tipo modelo e da memória disponíveis) uma tabela difícil 32,000 ou 128,000 que contenha entradas para o fonte-**IP do Sticky** e o Secure Socket Layer (SSL) pegajoso. A tabela difícil não mantém cookies difíceis no CSS. A remoção de entradas na tabela difícil no CSS ocorre nestas situações:

- Àrevelia, com um método FIFO. As entradas permanecem na tabela até os 32,000 ou os 128,000 que o buffer está completo. Neste tempo, todas as entradas novas fazem com que o CSS remova uma entrada com base no FIFO.
- minutos do **Sticky-inact-timeout**. Em uma regra de conteúdo, você pode especificar o timeout por inatividade por que o CSS remove uma entrada difícil, porque este exemplo mostra:`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.
  ```
  Nota: O CSS rejeita a solicitação difícil seguinte em um caso quando todos estes artigos são verdadeiros:O parâmetro do **Sticky-inact-timeout** é usado.O CSS encheu o buffer 32,000 ou 128,000.Nenhuma entrada está aproximadamente ao intervalo.
- Regra de conteúdo. Com a suspensão e o reactivation de uma regra de conteúdo, a remoção das entradas de tabela difíciis que se aplicam a essa regra ocorre.

Para mais informação, refira o documento que configura parâmetros difíciis para regras de conteúdo.

Q. Como posso eu tomar um serviço fora da rotação?

A. Com a configuração da regra de conteúdo (camada 3, camada 4, ou camada 5) como base, o CSS comporta-se diferentemente com a suspensão manual de um serviço, que tome um server fora de serviço. Muitas vezes, os desenvolvedores de Web precisam de suspender um serviço e de fazer temporariamente mudanças da administração aos página da web. Porque estas mudanças da Web podem ocorrer durante horários de produção, você não quer matar as conexões que existem ao serviço ou aos serviços quando a suspensão manual do serviço ocorre. Execute as atualizações a um serviço durante a suspensão manual do serviço.

Este exemplo mostra a camada 5 da amostra, a camada 4, e mergulha 3 regras de conteúdo:

```
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.
```

O CSS desvia as conexões que existem quando as regras de conteúdo são a camada 3 ou a camada 4. Se a suspensão de um serviço sob uma regra de conteúdo da camada 3 ou da camada 4 ocorre, o CSS desvia toda a conexão que existir e para a frente todo o TCP subsequente pede ao serviço ativo sob essa regra de conteúdo respectiva.

Com a suspensão manual de um serviço que resida sob uma regra de conteúdo da camada 5, o CSS restaura alguns ou todas as conexões que associarem com esse serviço.

Q. É a proximidade de rede parte do conjunto de recursos aprimorados?

A. As características da proximidade de rede não são parte do conjunto de recursos aprimorados e exigem uma licença adicional. Se você tenta emitir **comandos proximity no** CSS sem a licença apropriada, você recebe este Mensagem de Erro:

```
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.
```

A fim comprar uma licença, veja seu revendedor local de Cisco. Se você comprou uma licença e precisa uma substituição, envie um email a licensing@cisco.com.

Q. Que detalhes o comando show dos fornece?

A. Cisco CSS pode indicar detalhes sobre os eventos os mais recentes do ataque, que incluem:

- Endereços IP de origem e de destino
- O tipo de evento
- Ocorrências totais

Se múltiplo os ataques ocorrem com a mesma recusa do tipo e do endereço de rementente e destinatário do serviço (DoS), há uma tentativa de fundi-los como um evento. Esta fusão reduz o indicador dos eventos.

Emita o **comando show dos** a fim indicar:

- O número total de ataques desde que a bota do CSS
- Os tipos de ataques e do número máximo destes atacam por segundo
- Primeiro e último a ocorrência de um ataque

Este exemplo mostra a saída do **comando 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
```

Esta lista fornece uma breve descrição de cada um dos campos que o comando indica:

- `Ataques total` — O número total de ataques DoS que foram detectados desde que a bota da caixa. Você pode encontrar uma descrição do tipo de ataques que aparecem na lista, junto com o número de ocorrências, abaixo.
- `Ataques SYN` — As conexões de TCP que uma fonte inicia mas que não são seguidas com um quadro do reconhecimento a fim terminar o cumprimento de TCP tripartido.
- `Ataques da TERRA` — Alguns pacotes que tiverem endereços de rementente e destinatário idênticos. O CSS não permite que os endereços IP internos sejam o endereço de origem de um fluxo. Também, o CSS não permite que os endereços de rementente e destinatário dos quadros sejam iguais.
- `Ataques zero da porta` — Quadros que contêm a fonte ou o TCP destino ou as portas do User Datagram Protocol (UDP) que são iguais a zero.**Nota:** Um software mais velho dos SmartBits pode enviar os quadros que contêm as portas de origem ou destino iguais a zero. O CSS registra-os como ataques DoS e o deixa cair estes quadros.
- `Ataques ilegais de Src` — Endereços de origem ilegais.
- `Ataques ilegais de Dst` — Endereços de destino ilegais.
- `Ataques de smurf` — Sibilos com um endereço de destino da transmissão. O CSS não permite transmissões direcionada à revelia. `Um ataque de smurf` usa um eco do Internet Control Message Protocol (ICMP) a um endereço de broadcast. O CSS pode obstruir o acesso às portas UDP echo através do Access Control Lists (ACLs).
- `Máximo por segundo` — O número máximo de eventos por segundo. Use a máximo-evento-por-segunda informação para ajustar valores de limiar da armadilha de Protocolo de Gerenciamento de Rede Simples (SNMP).**Nota:** O número máximo de eventos é por segundo o máximo pelo form fatora pequeno Pluggable (SFP). Para um CSS11800, por exemplo, que possa ter até quatro SFP, a taxa máxima por segundo pode ser tão alta quanto quatro vezes o número que aparece no indicador.**Nota:** Um outro FAQ pergunta se você pode desabilitar a proteção de DOS no CSS. A resposta é não. A proteção de DOS é parte do processo da admissão do fluxo. A intenção de proteção de DOS é proteger os recursos no CSS assim como os server atrás do CSS. O DoS não é um item configurável. A intenção é para que o DoS seja transparente quando os protocolos trabalham corretamente. O processo de instalação do fluxo envolve profundamente as características DoS. A ajuda das características o CSS conserva recursos do caminho rápido e protege os dispositivos que o CSS alcança. As características estão sempre atuais no 3.0 da versão de software e mais tarde.

Igualmente considere a instalação de determinado SNMP traps para a detecção de ataques possíveis DoS. As armadilhas disponíveis são:

- **empresa do tipo de armadilha SNMP** — A fim permitir armadilhas corporativas SNMP e configurar tipos de armadilha, emita o **comando snmp trap-type enterprise**. Emita o **comando no snmp trap-type enterprise** a fim desabilitar todas as armadilhas. Você deve permitir armadilhas corporativas antes que você configure uma opção da armadilha corporativa. Você pode permitir o CSS de gerar armadilhas corporativas quando os eventos do ataque DoS ocorrem, um início de uma sessão falha, ou um estado de transições do serviço CSS.
- ***dos_attack_type*** — Gerencie armadilhas corporativas SNMP quando um evento do ataque DoS ocorre. Uma geração de armadilha ocorre cada segundo em que o número de ataques

durante aquele excede em segundo o ponto inicial para o ataque-tipo configuração DoS. As opções são:**dos-ilegal-ataque** — Gerencie armadilhas para endereços ilegais, fonte ou destino. Os endereços ilegais são:Endereços de origem do laço de retornoEndereços de origem da transmissãoEndereços de destino do laço de retornoEndereços de origem de transmissão múltiplaOs endereços de origem esses você possuiO limiar trap do padrão para este tipo de ataque é um por segundo.**dos-terra-ataque** — Geras armadilha para pacotes que têm endereços de rementente e destinatário idênticos. O limiar trap do padrão para este tipo de ataque é um por segundo.**dos-sibilo-ataque** — Gerencie armadilhas quando o número de sibilos excede o valor de limiar. O limiar trap do padrão para este tipo de ataque é 30 por segundo.**Nota:** Esta opção não segue ataques DoS dos ping de desativação.**dos-smurf-ataque** — Gerencie armadilhas quando o número de sibilos com um endereço de destino da transmissão excede o valor de limiar. O limiar trap do padrão para este tipo de ataque é um por segundo.**dos-SYN-ataque** — Gerencie armadilhas quando o número de conexões de TCP que uma fonte inicia mas que não está seguido com um quadro do reconhecimento para terminar o cumprimento de TCP tripartido excede o valor de limiar. O limiar trap do padrão para este tipo de ataque é 10 por segundo.

Q. Posso eu desligar a recusa de recursos de proteção do serviço (DoS) na linha CSS de Switches?

A. Na linha atual de software para o CSS (Cisco WebNS), não há nenhuma opção para desabilitar a característica de proteção de DOS.

Q. Posso eu desligar a recusa de contadores da proteção do serviço (DoS)?

A. Não há nenhuma opção para desabilitar os contadores que registram ataques DoS/SYN.

Nota: Para obter mais informações sobre do DoS e dos ataques SYN, veja que a resposta ao FAQ que detalhes fazem o comando show dos forneça?.

Q. Como eu uso intervalos de porta nas Listas de acesso?

A. O uso dos intervalos de porta no ajudas do Access Control List (ACL) simplifica o número de ACL que você configura, dado uma situação em que você quer obstruir o acesso de usuário para portas do User Datagram Protocol (UDP) algum TCP/. Por exemplo, supõe que você quer obstruir as portas 20 a 23 para todos os usuários que entram a caixa fora de sua rede. Primeiramente, supõe que a rede externa ou o lado público do CSS estão no VLAN2. Igualmente supõe que o interno ou o lado de servidor da rede estão no VLAN1. A configuração ACL é:

```
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
```

Informações Relacionadas

- Fim do anúncio da venda para a Cisco CSS 11000 Series
- Boletins do Switches de serviços de conteúdo Cisco CSS série 11000
- Suporte técnico dos CSS 11000 Series Content Services Switch
- Centro de software (transferências) - Rede de conteúdo (clientes registrados somente)
- Suporte Técnico e Documentação - Cisco Systems