内容服务交换机常见问题

目录

简介

本文讨论多数常见问题(FAQ) Cisco内容服务交换机(CSS)。

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

Q. 在哪里能找到CSS的MIB ？

A. MIB已经在CSS。您能认为CSS在简单网络管理协议(SNMP)网络方案的一个代理程序。您需要执行的所有是配置在CSS的SNMP参数。参考配置简单网络管理协议(SNMP)欲知更多信息的本文。

Q. 什么是CSS支持脚本Keepalive的最大？

A. CSS支持脚本Keepalive的最大是255。参考*在版本注释的软件版本5.00*部分的*新特性*Cisco 11000系列内容服务交换机的。

Q. 清除或如何能删除内核文件？

A. 发出**clear core命令**。命令是可用的在CSS软件版本5.00和以上，在调试模式。语法为：

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

Q. 在哪里能找到日志消息的解释？

A. 对于日志消息的解释，参考本文日志消息。

Q. 有没有命令控制对等体多频繁发送彼此负载报告？

A. 您能使用**dns-peer interval命令**。也有您能本地配置为了达到本地负载的一次更加快速的测量的其它命令：

- **超龄定时器**—设置时期(以秒钟)的过时的负载信息ageout。
- **拆卸定时器**—设置系统等待发送拆卸报告的最大时间段(以秒钟)。

Q. 与代码版本的许可证密钥关键变动？

A. 不，许可证密钥不随代码版本改变。

Q. 我丢失我的许可证密钥。我该如何操作？

A. 发送一电子邮件用您的CSS序列号对licensing@cisco.com。**version命令**显示功能包，但是不是许可证密钥。

Q. 何时是条目的挽留的默认时间在粘滞表里？

A. 除非使用sticky-inact-timeout命令，没有默认时间。粘滞表保持根据FIFO基本类型(32,000个或128,000个条目，根据设备类型和内存联机)，或者直到CSS的重新启动。

Q. 如何配置粘性屏蔽为了报道从大型代理的请求类似America Online (AOL) ？

A. 如果应用程序要求在会话的整个生活将滞留的用户，请考虑一第3层粘贴。粘贴的第3层停留一个用户到服务器根据用户IP地址。CSS有粘滞表32,000，因此意味着，当32,000个同步用户是在站点时，表包裹和第一个用户变得“失灵”。然而，音量您的站点可以是这样您每次有超过32,000个用户。或者大比例您的客户能走向您通过大型代理。在这些情况下，请考虑使用一个不同的粘性方法(例如Cookie、cookieurl或者URL)或您的粘性屏蔽增加。默认粘性屏蔽是255.255.255.255，因此意味

着每个条目在粘滞表里是一个单个IP地址。某些大型代理有一个情况在哪个用户在一会话期间生活在地址范围使用几个不同的IP地址。此情况造成某些TCP连接获得卡住对一个服务器，并且能造成其他连接获得卡住对同一处理的一个不同的服务器。结果可以是一些项目损耗从副食品购物车的。如果不能使用其中一个更加先进的方法停留，请使用255.255.240.0粘性屏蔽，当您的客户端基础通过这些大型代理之一时来。

Q. 为什么有粘贴的没有选项，当我使用高级平衡安全套接字层时(SSL) ？

A. 高级平衡SSL是相同的象粘贴SSL。

Q. 内容和应用对等协议(CAPP)或应用对等协议(APP)使用什么类型的加密？

A. 默认情况下， CAPP用途不加密。您能配置APP会话使用消息摘要5 (MD5)。加密类型必须是相同的在两对等体为了APP会话能出现。

Q. " gratuitous arp "消息是什么意思？

A. 当备用交换机不检测从主控交换机的一检测信号在3秒以内时，备用交换机过渡变为主控并且发送" gratuitous arp "消息。消息指示从新的主控交换机的地址解析服务(ARP)传送。消息包含当前主控交换机的MAC地址。免费ARP由**ip gratuitous-arps** in命令全局配置模式启用。它在单个接口在其他接口不能启用和阻塞它。

Q. 如何同步在CSS的配置在故障切换模式？

A. 为了同步在软件版本4.0的配置，请使用**commit config sync命令**。为了同步配置用软件版本3.10代码，您必须使用FTP为了移动从一交换机的配置到另一个。为了同步在软件版本6.x和7.x的配置请编码，请使用commit_redundancy命令活动/等待或全套设备冗余。或者您能使用commit_vip_redundancy命令Virtual IP (VIP) /interface冗余。您在脚本的报头能使用show script commit_redundancy命令为了查看**commit_redundancy**脚本的可用的命令行选项。同样适用于**commit_vip_redundancy命令**。

Q. 应该使用什么设置在终端程序？

A. 请使用这些设置：

- 9600 波特
- 8 位
- 无奇偶校验
- 1 个停止位
- 无流控制

Q. 有没有方式重编程序在CSS的MAC地址？

A. 是，有方式。

注意： 您能找到MAC地址和序列号在单元背面。

完成这些步骤为了重编程序序列号和MAC地址。此示例是为在CS800机箱的MAC地址：

1. 打开**脱机诊断监视程序(ODM)**。
2. 在ODM主菜单，请按**班次T**为了到达Technician菜单。
3. 选择**1** (请配置)。
4. 选择**5** (集制造信息)。
5. 选择**2** (集背板制造信息)。
6. 按照提示符并且输入对应的数据，例如序列号和MAC地址。您能找到在CS800机箱的上面的此数据。
7. 重新启动方框。

Q. 如何做永久性提示符更改在CSS ？

A. 登陆到CSS方框作为用户弗雷德，并且请使用您的登录凭证。为了做一永久性提示符更改，请发出此命令：

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

发出此命令保存更改：

```
Redsox#save_profile
```

每次用户登录， CSS使用同一提示符，此命令保存用户配置文件，以便。此操作，类似使用**？。？**在UNIX的资源文件，创建每个用户的一唯一配置文件。

当您回到CSS并且登陆作为admin时，提示符不反映这些更改。更改使用物精确，因此您需要发出要安排提示符反映新的更改的每个用户的**及时**和**save_profile**命令。

Q. 运行和锁定闪存有何区别？

A. 此示例显示**show version命令**显示的不同种类的闪存：

```
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. 为什么有闪存不同的版本？

A. 锁定闪存显示在该CSS最初安装的软件版本。版本依然是同样并且仅担当备份。在运行的闪存的版本是在该CSS当前运行的版本。

Q. 为什么不能访问CSS的管理端口从远程端口的？

A. 在早于5.03 Cisco WebNS中的所有版本，管理端口不是路由可达接口。在版本5.03，您能添加默认网关到管理端口为了做端口路由可达接口。

Q. 技术支持是否支持客户写道的自定义脚本Keepalive ？

A. 不，技术支持不支持客户写的Keepalive脚本。

Q. 如何从CSS磁盘删除内核文件？

A. 如果，在您发出**show core命令后**，查找内核文件列表，您在两种方式之一中能删除文件：

注意： 您使用的方法取决于编码版本。

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

或

- 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. 当我验证到有我的CSS的时RADIUS服务器，我获得"RADIUS-4 ：RADIUS验证失败与原因代码2"错误消息。此消息是什么意思？

A. 此错误消息表明回复到达了CSS，并且有问题。疏忽设置类型属性到管理在RADIUS服务器可以是问题的原因。检查RADIUS服务器并且验证类型属性。

Q. 多么大是粘滞表，并且什么原因条目删除？

A. CSS有包含**粘贴来源IP**和粘贴安全套接字层SSL的条目的一(依靠型号类型和内存联机)的32,000或128,000粘滞表。粘滞表不维护在CSS的粘性Cookie。条目在这些情况下删除在CSS的粘滞表里发生：

- 默认情况下，与FIFO方法。条目在直到缓冲区全双工的32,000或128,000的表里依然是。此时，其中任一新建的条目造成CSS根据FIFO删除条目。
- **sticky-inact-timeout**分钟。在内容规则，您能指定CSS删除粘性条目的休眠超时，因为此示例显示：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. **注意：** 当所有这些项目是真的时，CSS拒绝在案件的下个粘性请求：使用**sticky-inact-timeout**参数。CSS充满32,000或128,000缓冲区。条目不对超时。
- 内容规则。使用内容规则的保持和重新激活，适用于该规则粘性表条目的删除发生。

欲知更多信息，参考配置内容规则的本文粘性参数。

Q. 如何能采取服务出于循环？

A. 使用内容规则的配置(第3层， Layer4或者请分层堆积5)为据， CSS不同运行与服务的手工的保持，采取服务器服务中断。许多次， Web开发人员需要临时地暂停服务和做对网页的管理变动。在制作小时，由于这些Web更改能发生，您不要杀害存在对服务或服务的连接，当手工的服务保持发生时。在手工的服务保持期间，执行更新对服务。

此示例显示示例第五层、Layer4和第3层内容规则：

```
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牵制存在的连接，当内容规则是第3层或Layer4。如果一服务的保持根据第3层或Layer4内容规则发生， CSS牵制存在并且寄所有随后的TCP请求给活动服务根据该各自内容规则的所有连接。

使用根据第五层内容规则驻留服务的手工的保持， CSS重置与该服务产生关联的任一或所有的连接。

Q. 网络接近度零件高级功能集？

A. 网络接近度功能不作为高级功能集的部分并且要求一个另外的许可证。如果设法发出**接近度**on命令CSS，不用适当的许可证，您收到此错误消息：

```
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.
```

为了采购许可证，请参阅您的活动进程分销商。如果采购许可证并且需要更换，请发送电子邮件对 licensing@cisco.com。

Q. 什么详细信息show dos命令提供？

A. Cisco CSS能显示关于最最近的攻击事件的详细信息，包括：

- 源和目的 IP 地址
- 事件类型
- 全面出现

如果多个攻击发生在同一拒绝服务类型和源地址和目的地址，有尝试合并他们作为一个事件。此合并减少事件显示。

发出**show dos命令**为了显示：

- 攻击总数，自从CSS的引导程序
- 攻击种类和这些攻击最大每秒
- 攻击的第一和最后出现

此示例显示从**show dos命令的**输出：

```
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
```

此列表提供的其中每一的简要描述个命令显示字段：

- —检测，因为方框的引导程序DOS攻击的总数。您能找到攻击的种类的说明在列表出现，与出现一起数量，下面。
- SYN—来源首次没有带有确认帧为了完成三向交握的TCP连接，但是。
- —有相同的源地址和目的地址的任何数据包。CSS不允许内部IP地址是流的源地址。并且，CSS不允许帧源地址和目的地址是相等的。
- —包含来源或目的地TCP或者用户数据报协议(UDP)端口是相等的到零的帧。**注意：** 更旧的Smartbits软件能发送包含源或目的地端口等于到零的帧。CSS记录他们作为DOS攻击并且丢弃这些帧。
- Src—非法源地址。
- Dst—非法目的地址。
- Smurf—与广播目的地址的Ping。默认情况下CSS不允许定向广播。Smurf使用一互联网控制消息协议(ICMP)响应对广播地址。CSS能通过访问控制列表(ACL)阻止对UDP响应端口的访问。
- 事件最大每秒。请使用最大数量事件每第二信息设置简单网络管理协议(SNMP)陷阱阈值。**注意：** 事件最大每秒是最大数量每可插入的小的尺寸(SFP)。对于CSS 11800，例如，能有四SFP，最大速率每秒可以是一样高象四倍在显示出现的编号。**注意：** 如果能禁用在CSS的DoS保护另一个FAQ要求。答案是不。DoS保护是流接纳进程的一部分。DoS保护的目的将保护在CSS的资源以及在CSS后的服务器。DoS不是一个可配置项目。目的是为了的DoS能透明，当协议正确地时运作。流安装过程深深地介入DoS功能。功能帮助CSS保存快速路径资源并且保护CSS到达的设备。功能总是存在软件版本3.0及以上版本。

并且请考虑某些SNMP陷阱设置可能的DOS攻击的检测的。联机陷阱是：

- **snmp陷阱类型企业**—为了启用SNMP企业陷阱和配置陷阱类型，请发出**snmp trap-type enterprise命令**。发出**no snmp trap-type enterprise命令**为了禁用所有陷阱。在您配置企业陷阱选项前，您必须启用企业陷阱。您能使CSS形成企业陷阱，当DOS攻击事件发生时，登录出故障或者CSS服务转换状态。
- ***dos_attack_type*** —，当DOS攻击事件发生时，形成SNMP企业陷阱。当攻击数量在那期间的第二超出DoS攻击类型配置的时，阈值一个陷阱生成发生每秒钟。选项有：**DOS非法攻击**—形成非法地址的陷阱，来源或目的地。非法地址是：环回源地址广播源地址环回目的地址组播源地址该的源地址您拥有此种攻击的默认陷井门限值是一个每秒。**DOS地产攻击**—形成有相同的源地址和目的地址的数据包的陷阱。此种攻击的默认陷井门限值是一个每秒。**DOS PING攻击**—，当ping数量超过阈值时，形成陷阱。此种攻击的默认陷井门限值是30每秒。**注意：** 此选项不跟踪致死ping DOS攻击。**DOS smurf攻击**—，当ping数量与广播目的地址的超过阈值时，形成陷阱。此种攻击的默认陷井门限值是一个每秒。**DOS SYN攻击**—形成陷阱，当的TCP连接数量来源首次时，但是没有带有确认帧完成三向交握超过阈值。此种攻击的默认陷井门限值是10每秒。

Q. 能否关闭在交换机CSS线路的拒绝服务保护特点？

A. 在软件中当前线路CSS的(Cisco WebNS)，没有选项禁用DoS保护特点。

Q. 能否关闭拒绝服务保护计数器？

A. 没有选项禁用记录DoS/SYN攻击的计数器。

注意： 关于DoS和SYN攻击的更多信息，请参阅对FAQ的答复什么详细信息执行show dos命令请提供？。

Q. 如何使用端口范围在访问列表？

A. 使用在访问控制表(ACL)的端口范围帮助简化您配置ACL的数量，给您要阻止一些TCP用户数据报协议(UDP)端口的用户访问的情况。例如，请假设您要阻塞进入方框从您的网络之外的所有用户的端口20至23。首先，假设， CSS的外部网络或公共侧在VLAN 2。并且假设，网络的内部或服务器端在VLAN1。ACL配置是：

```
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
```

相关信息

- Cisco CSS 11000系列的销售终止通告
- Cisco CSS 11000系列内容服务交换机公告版
- CSS 11000系列内容服务交换机技术支持
- 软件中心(下载) -内容联网(仅限注册用户)
- 技术支持和文档 - Cisco Systems