

如何读或解释WCCP注册Cisco Web安全工具？

Contents

[问题](#)

[环境](#)

问题

如何读或解释WCCP注册Cisco Web安全工具？

环境

Cisco Web安全工具(WSA) , AsyncOS的所有版本

在AsyncOS版本7.1和以下 : WCCP消息登陆代理日志。

在AsyncOS版本7.5和以上 : WCCP消息在WCCP日志被看到与代理日志一起。

检查您的“日志订阅”(在GUI >**System Administration** >日志订阅下)确定代理并且/或者WCCP日志是启用的。

在AsyncOS版本7.1和以下 : WCCP操作日志级别可以被输入以下CLI命令更改 :

```
wsa01> advancedproxyconfig
```

```
[> WCCP
```

输入多种“WCCP”选项的值 :

输入调试的WCCP日志级别 :

```
[0]> 3
```

在AsyncOS版本7.5和以上 : WCCP日志和代理日志的操作日志级别在“系统管理>日志订阅 > <Corresponding-WCCP-Log-Name>下的” GUI可以更改

操作日志级别将显示以下data:

7.1级的日志(CLI) 7.5级的日志(GUI) 在日志看到的信息在被配置的日志级别

0	关键	错误
1	警告	错误, 设置,
2	信息	错误, 设置, INFO
3	调试	错误, 设置, INFO, 状态
4	跟踪	错误, 设置, INFO, 状态, 更改(状态变换)

日志可以分成一些个不同的区域(分离由空间凹进), 在设置被打印后:

###时间戳###

SVC : 服务ID数据

连结 : 连结数据-对于每项服务, 每个路由器的, 有一个连结(能认为作为数据保持)的一个虚拟篮子

Rtr : 路由器数据

WC : Web缓存数据

以下下面是解释可能重视您能找到在WCCP跟踪记录水平。下面确切的示例是从一个实际方案。

```
wccp: CONFIG:SG:0: type 0
wccp: CONFIG:SG:0: 80
wccp: CONFIG:0:[raptor]
wccp: CONFIG:0: GRE & L2
wccp: CONFIG:0:ret GRE & L2
wccp: CONFIG:0:TCP
wccp: CONFIG:0: 172.28.15.33
wccp: CONFIG:SG:0: Security enable <- 1
wccp: CONFIG:SG:0: Hash enable <- 1
wccp: CONFIG:SG:0: Mask enable <- 1
wccp: CONFIG:SG:0: Service direction <- 0
wccp: CONFIG:SG:0: Hash/mask on client <- 0
wccp: INFO:WCCPv2: local IP is 10.251.0.73
wccp: INFO:Accepting WCCP messages on port 2048, FD 3 at 10.251.0.73.
wccp: INFO:Opening a socket set
```

WCCP配置信息

```
wccp: INFO:### Timestamp 100 ###
```

总是时间戳开始于100。此值以秒钟增加。

服务(SVC)数据

```
wccp: STATE:SVC@0x0x85bd000: index=0 type=0 ID=0
```

SVC : 服务@<<memory指示器-发展debugging>>的

索引 : 此服务的位置在所有被配置的服务列表在WSA -开始于0并且增加+1

类型 : 0 =预定义的ID (例如web-cache)。1 =标准的ID

目前web-cache (服务ID 0)是唯一的现有的预定义的ID

ID : 服务ID编号(0 - 255)

```
wccp: STATE:SVC@0x0x85bd000: index=0 type=0 ID=0
```

[MH_UNDECIDED]负载均衡方法此时(散列是未确定的与屏蔽)

[HASH_OK]切细允许

[MASK_OK]屏蔽允许

[HASHING]切细是选择的方法

[MASKING]屏蔽是选择的方法

[MH_DONE]屏蔽/散列协商完成

向前重定向的**[L2FWD_OK]** L2允许

向前重定向的**[GREFWD_OK]** GRE允许

[LGR_UNDECIDED]返回重定向方法此时(L2是未确定的与GRE)

回归重定向方法的[L2RET_OK] L2允许
回归重定向方法的[GRERET_OK] GRE允许
回归方法的[RET_GRE] GRE更喜欢
[LGR_DONE] GRE/L2回归方法negotiation完成

选定Web缓存的[DWC_UNKNOWN] (DWC)此时是未知
[FWD]重定向根据目的地端口
[SERVER]切细/屏蔽根据服务器地址
[CLIENT]切细/屏蔽根据客户端地址

服务视图更改了的[VIEW_CHANGED]

```
wccp: STATE: needRA(=0)@0, ISY@0, viewchg=0, viewused=0, keychg=0
```

NeedRA : 需要重定向分配(RA)。如果1=某事在此服务视图更改了。如果我们是DWC, 我们需要发送RA

- 仅DWC发送Ras -我们这时不知道我们是否是DWC)
- @0 : 被安排的时间戳在将来发送RA。(如果此值是115, RA在15秒将被发送)

ISY@ : 接收的时间戳前“我为此服务看到您(ISY)”。

Viewchg : 次数此服务有所有更改(路由器加入/事假, 被添加/被去除的wc, 那么)

Viewused : 最后更改编号我们通知了路由器。

Keychg : 次数我们生成一张不同的哈希/掩码表派出

```
wccp: STATE: this period:(HIAs=0, ISYs=0) proto=6
```

此周期: 在前10秒(标准的瞬间)内, 多少:

HIA : “这里我在(HIA)”我们发送了的信息包

ISY : “我看到您(ISY)”我们收到了的信息包

原始: 此服务要求重定向的协议。6是TCP

```
wccp: STATE: ports = 0, 0, 0, 0, 0, 0, 0, 0
```

端口: 将重定向的端口到Web缓存(WC)。当曾经web-cache端口时空出空白, 但是端口80将重定向。

连结数据

```
wccp: STATE: nexus@0x0x85bf000: rcvd_key(0.0.0.0,0) sent_key(0.0.0.0,0)
```

连结: 对于每项服务, 每个路由器的, 有一个连结(能认为作为数据保持)的一个虚拟篮子

Recvd_key : 发送RA DWC的地址, keychg编号被发送的DWC (递增)

Sent_key : 我们的地址+ key_chg编号, 当我们是DWC

```
wccp: STATE: rtr_mention@0, ISY@0 rtr_change#= 0 refs=0
```

Rtr_mention : 路由器最后提到的本身@ <timestamp>

ISY : 前看到了从此路由器的ISY在此服务组@<timestamp> (连结路由器)

Rtr_changer# : 路由器相信的次数视图更改了

```
wccp: STATE: rtr_mention@0, ISY@0 rtr_change#= 0 refs=0
```

这些是此连结的标志位

[FIXED] : 配置路由器使用

[DEAD] : 不响应的路由器/未使用它

[ALIVE] : 路由器回应ISY

[FWD_xxx] : 同意转发重定向方法(L2/ GRE)

[NEG_PEND] : WCCP协商是待定的

[ACTIVE] : WCCP协商完成, 并且WCCP是‘活跃’

[VIEW_VALID] : WCCP协商完成, 并且WSA +路由器对capabilities达成协议

```
wccp: STATE:      rstate=0, outst_HIA=0, receiveID=0
```

Rstate : ? ?

Outst_HIA : 我们发送了HIAs的编号, 但是没接受ISY。在有ISY以后, 这重置0。

ReceiveID : 接受在每个成功的ISY的ID增量。

路由器数据

```
wccp: STATE:      rtr@0x0x85be000: fd(3) gre-1, bind=10.251.0.73, sentto=172.28.15.33
```

Rtr : 为在同一路由器的nexii -复制的此连结的路由器信息

Fd : 发送信息包的插槽的文件描述符到此路由器

Gre : GRE接口的编号我们应该从此路由器(gre0, gre1接受数据, ...)

捆绑 : 寻址我们捆绑我们的插槽对, 发送信息包到此路由器(我们从/源地址)

Sentto : 寻址路由器报告得到了信息包对那从我们被发送了(仅有用, 当曾经组播)时

```
wccp: STATE:      configaddr=172.28.15.33, ID_addr=0.0.0.0, from_addr=172.28.15.33
```

Configaddr : 配置的路由器的IP地址

ID_addr : 做通告的路由器标识地址

From_addr : 地址信息包确实来自的地方(来源IP)

Web缓存数据

```
wccp: STATE:      WC@0x0x85b9020: (10.251.0.73) mentioned:111 weight:1 status:0
```

被提及的<IP> : 被参考的WC和时间戳的IP它介绍到服务ID

重量 : 在WCs被共享的权值共享负荷数据。

状态 : ? ?

```
wccp: STATE:      WC@0x0x85b9020: (10.251.0.73) mentioned:111 weight:1 status:0
```

[ME] : 此WC是WSA运行此守护程序

[ACTIVE] : WC由此服务的所有路由器汇报

下面一完全输出示例:并且划分WCCP第3级日志。在此日志, WSA加入有2其他WSAs已经在它的服务ID。(因为有最低的IP在服务), WSA将成为DWC :

```
wccp: INFO:### Timestamp 100 ###
```

```
wccp: STATE:SVC@0x0x85bd000: index=0 type=0 ID=0
```

```
wccp: STATE:      [MD5][MH_UNDECIDED][HASH_OK][MASK_OK][HASHING]
```

```
      [L2FWD_OK][GREFWD_OK][LGR_UNDECIDED][L2RET_OK]
```

```
      [GRERET_OK][RET_GRE][DWC_UNKNOWN][FWD][SERVER]
```

```
wccp: STATE:      needRA(=0)@0, ISY@0, viewchg=0, viewused=0, keychg=0
```

```
wccp: STATE:      this period:(HIAs=0, ISYs=0) proto=6
```

```
wccp: STATE:      ports = 0, 0, 0, 0, 0, 0, 0, 0
```

```
wccp: STATE:      nexus@0x0x85bf000: rcvd_key(0.0.0.0,0) sent_key(0.0.0.0,0)
```

```
wccp: STATE:      rtr_mention@0, ISY@0 rtr_change#= 0 refs=0
```

```
wccp: STATE:      [FIXED][DEAD][FWD_???
```

```
wccp: STATE:      rstate=0, outst_HIA=0, receiveID=0
```

```
wccp: STATE:      rtr@0x0x85be000: fd(3) gre-1, bind=10.251.0.73, sentto=172.28.15.33
```

```
wccp: STATE: configaddr=172.28.15.33, ID_addr=0.0.0.0, from_addr=172.28.15.33
```

什么都未被派出，-所有初始化数据。

```
wccp: INFO:### Timestamp 101 ###
wccp: STATE:SVC@0x0x85bd000: index=0 type=0 ID=0
wccp: STATE: [MD5][MH_UNDECIDED][HASH_OK][MASK_OK][HASHING]
[L2FWD_OK][GREFWD_OK][LGR_UNDECIDED][L2RET_OK]
[GRERET_OK][RET_GRE][DWC_UNKNOWN][FWD][SERVER]
wccp: STATE: needRA(=0)@0, ISY@0, viewchg=0, viewused=0, keychg=0
wccp: STATE: this period:(HIAs=0, ISYs=0) proto=6
wccp: STATE: ports = 0, 0, 0, 0, 0, 0, 0, 0
wccp: STATE: nexus@0x0x85bf000: rcvd_key(0.0.0.0,0) sent_key(0.0.0.0,0)
wccp: STATE: rtr_mention@0, ISY@0 rtr_change#= 0 refs=0
wccp: STATE: [FIXED][DEAD][FWD_???]
wccp: STATE: rstate=0, outst_HIA=0, receiveID=0
wccp: STATE: rtr@0x0x85be000: fd(3) gre-1, bind=10.251.0.73, sentto=172.28.15.33
wccp: STATE: configaddr=172.28.15.33, ID_addr=0.0.0.0, from_addr=172.28.15.33
wccp: INFO:send_HIA called
wccp: INFO:### Timestamp 101 ###
wccp: INFO:HIA sent to 172.28.15.33 -- 1 ISY(s) outstanding
wccp: INFO:### Timestamp 101 ###
wccp: INFO:ISY received from 172.28.3.46.(708 bytes)
wccp: INFO:ISY: accepted
```

我们派出了第一个HIA @ 101并且接受了ISY @101。下面视图的更新，即然我们接受了ISY。

```
wccp: INFO:### Timestamp 101 ###
wccp: STATE:SVC@0x0x85bd000: index=0 type=0 ID=0
wccp: STATE: [MD5][MH_DONE][HASH_OK][MASK_OK][MASKING][L2FWD_OK]
[GREFWD_OK][LGR_DONE][L2RET_OK][GRERET_OK][RET_GRE]
[DWC_UNKNOWN][VIEW_CHANGED][FWD][SERVER]
wccp: STATE: needRA(=0)@0, ISY@101, viewchg=1, viewused=0, keychg=0
wccp: STATE: this period:(HIAs=1, ISYs=1) proto=6
wccp: STATE: ports = 0, 0, 0, 0, 0, 0, 0, 0
wccp: STATE: WC@0x0x85b9160: (172.17.0.10) mentioned:101 weight:1 status:0
wccp: STATE: [ACTIVE]
wccp: STATE: WC@0x0x85b9140: (172.28.6.34) mentioned:101 weight:1 status:0
wccp: STATE: [ACTIVE]
wccp: STATE: nexus@0x0x85bf000: rcvd_key(172.17.0.10,5) sent_key(0.0.0.0,0)
wccp: STATE: rtr_mention@101, ISY@101 rtr_change#= 23 refs=0
wccp: STATE: [FIXED][ALIVE][ACTIVE][NEG_PEND][FWD_???][FWD_GRE]
[VIEW_VALID]
wccp: STATE: rstate=0, outst_HIA=0, receiveID=158
wccp: STATE: rtr@0x0x85be000: fd(3) gre-1, bind=10.251.0.73, sentto=172.28.15.33
wccp: STATE: configaddr=172.28.15.33, ID_addr=172.28.15.33, from_addr=172.28.15.33
```

我们认可其他2个Web缓存，并且他们是被标记的活跃。当前DWC是172.17.0.10每在连结的rcvd_key。连结状态是NEG_PEND，ReceiveID=158。

```
wccp: INFO:### Timestamp 111 ###
wccp: STATE:SVC@0x0x85bd000: index=0 type=0 ID=0
wccp: STATE: [MD5][MH_DONE][HASH_OK][MASK_OK][MASKING][L2FWD_OK]
[GREFWD_OK][LGR_DONE][L2RET_OK][GRERET_OK][RET_GRE]
[DWC_UNKNOWN][FWD][SERVER]
wccp: STATE: needRA(=1)@117, ISY@101, viewchg=1, viewused=0, keychg=0
```

```

wccp: STATE:      this period:(HIAs=1, ISYs=1) proto=6
wccp: STATE:      ports = 0, 0, 0, 0, 0, 0, 0, 0
wccp: STATE:      WC@0x0x85b9160: (172.17.0.10) mentioned:101 weight:1 status:0
wccp: STATE:      [ACTIVE]
wccp: STATE:      WC@0x0x85b9140: (172.28.6.34) mentioned:101 weight:1 status:0
wccp: STATE:      [ACTIVE]
wccp: STATE:      nexus@0x0x85bf000: rcvd_key(172.17.0.10,5) sent_key(0.0.0.0,0)
wccp: STATE:      rtr_mention@101, ISY@101 rtr_change#= 23 refs=0
wccp: STATE:      [FIXED][ALIVE][ACTIVE][NEG_PEND][FWD_??][FWD_GRE]
wccp: STATE:      [VIEW_VALID]
wccp: STATE:      rstate=0, outst_HIA=0, receiveID=158
wccp: STATE:      rtr@0x0x85be000: fd(3) gre-1, bind=10.251.0.73, sentto=172.28.15.33
wccp: STATE:      configaddr=172.28.15.33, ID_addr=172.28.15.33, from_addr=172.28.15.33
wccp: INFO:send_HIA called
wccp: INFO:### Timestamp 111 ###
wccp: INFO:HIA sent to 172.28.15.33 -- 1 ISY(s) outstanding
wccp: INFO:### Timestamp 111 ###
wccp: INFO:ISY received from 172.28.3.46.(1252 bytes)
wccp: INFO:ISY: accepted

```

因为服务视图更改了，needRA被标记。期待RA @117。并且请注意路由器更改#是23。您看到我们派出了另一个HIA在111并且接受了另一个ISY在111。

```

wccp: INFO:### Timestamp 111 ###
wccp: STATE:SVC@0x0x85bd000: index=0 type=0 ID=0
wccp: STATE:      [MD5][MH_DONE][HASH_OK][MASK_OK][MASKING][L2FWD_OK]
wccp: STATE:      [GREFWD_OK][LGR_DONE][L2RET_OK][GRERET_OK][RET_GRE]
wccp: STATE:      [DWC_UNKNOWN][VIEW_CHANGED][FWD][SERVER]
wccp: STATE:      needRA(=1)@117, ISY@111, viewchg=2, viewused=0, keychg=0
wccp: STATE:      this period:(HIAs=1, ISYs=1) proto=6
wccp: STATE:      ports = 0, 0, 0, 0, 0, 0, 0, 0
wccp: STATE:      WC@0x0x85b9020: (10.251.0.73) mentioned:111 weight:1 status:0
wccp: STATE:      [ME][ACTIVE]
wccp: STATE:      WC@0x0x85b9160: (172.17.0.10) mentioned:111 weight:1 status:0
wccp: STATE:      [ACTIVE]
wccp: STATE:      WC@0x0x85b9140: (172.28.6.34) mentioned:111 weight:1 status:0
wccp: STATE:      [ACTIVE]
wccp: STATE:      nexus@0x0x85bf000: rcvd_key(172.17.0.10,5) sent_key(0.0.0.0,0)
wccp: STATE:      rtr_mention@111, ISY@111 rtr_change#= 24 refs=0
wccp: STATE:      [FIXED][ALIVE][ACTIVE][FWD_GRE]
wccp: STATE:      rstate=0, outst_HIA=0, receiveID=161
wccp: STATE:      rtr@0x0x85be000: fd(3) gre-1, bind=10.251.0.73, sentto=172.28.15.33
wccp: STATE:      configaddr=172.28.15.33, ID_addr=172.28.15.33, from_addr=172.28.3.46

```

视图再更改了，并且viewchg相应地被增加。路由器也注意了更改并且增加了其更改#。您看到此WSA当前报道和被标记的激活。这意味着此服务的所有路由器提及了WC。

```

wccp: INFO:### Timestamp 117 ###
wccp: STATE:SVC@0x0x85bd000: index=0 type=0 ID=0
wccp: STATE:      [MD5][MH_DONE][HASH_OK][MASK_OK][MASKING][L2FWD_OK]
wccp: STATE:      [GREFWD_OK][LGR_DONE][L2RET_OK][GRERET_OK][RET_GRE]
wccp: STATE:      [DWC][FWD][SERVER]
wccp: STATE:      needRA(=1)@117, ISY@111, viewchg=2, viewused=0, keychg=0
wccp: STATE:      this period:(HIAs=1, ISYs=1) proto=6
wccp: STATE:      ports = 0, 0, 0, 0, 0, 0, 0, 0
wccp: STATE:      WC@0x0x85b9020: (10.251.0.73) mentioned:111 weight:1 status:0
wccp: STATE:      [ME][ACTIVE]
wccp: STATE:      WC@0x0x85b9160: (172.17.0.10) mentioned:111 weight:1 status:0
wccp: STATE:      [ACTIVE]

```

```

wccp: STATE: WC@0x0x85b9140: (172.28.6.34) mentioned:111 weight:1 status:0
wccp: STATE: [ACTIVE]
wccp: STATE: nexus@0x0x85bf000: rcvd_key(172.17.0.10,5) sent_key(0.0.0.0,0)
wccp: STATE: rtr_mention@111, ISY@111 rtr_change#= 24 refs=0
wccp: STATE: [FIXED][ALIVE][ACTIVE][FWD_GRE]
wccp: STATE: rstate=0, outst_HIA=0, receiveID=161
wccp: STATE: rtr@0x0x85be000: fd(3) gre-1, bind=10.251.0.73, sentto=172.28.15.33
wccp: STATE: configaddr=172.28.15.33, ID_addr=172.28.15.33, from_addr=172.28.3.46
wccp: INFO:send_RA: called.
wccp: INFO:initial mask is 0x00000000
wccp: INFO:slots = 32 WCs = 3, mask = 0x00000526, inc = 0x2
wccp: INFO:slot 0,val 0x00000000, index - 0
wccp: INFO:slot 1,val 0x00000002, index - 1
wccp: INFO:slot 2,val 0x00000004, index - 2
wccp: INFO:slot 3,val 0x00000006, index - 0
wccp: INFO:slot 4,val 0x00000020, index - 1
wccp: INFO:slot 5,val 0x00000022, index - 2
wccp: INFO:slot 6,val 0x00000024, index - 0
wccp: INFO:slot 7,val 0x00000026, index - 1
wccp: INFO:slot 8,val 0x00000100, index - 2
wccp: INFO:slot 9,val 0x00000102, index - 0
wccp: INFO:slot 10,val 0x00000104, index - 1
wccp: INFO:slot 11,val 0x00000106, index - 2
wccp: INFO:slot 12,val 0x00000120, index - 0
wccp: INFO:slot 13,val 0x00000122, index - 1
wccp: INFO:slot 14,val 0x00000124, index - 2
wccp: INFO:slot 15,val 0x00000126, index - 0
wccp: INFO:slot 16,val 0x00000400, index - 1
wccp: INFO:slot 17,val 0x00000402, index - 2
wccp: INFO:slot 18,val 0x00000404, index - 0
wccp: INFO:slot 19,val 0x00000406, index - 1
wccp: INFO:slot 20,val 0x00000420, index - 2
wccp: INFO:slot 21,val 0x00000422, index - 0
wccp: INFO:slot 22,val 0x00000424, index - 1
wccp: INFO:slot 23,val 0x00000426, index - 2
wccp: INFO:slot 24,val 0x00000500, index - 0
wccp: INFO:slot 25,val 0x00000502, index - 1
wccp: INFO:slot 26,val 0x00000504, index - 2
wccp: INFO:slot 27,val 0x00000506, index - 0
wccp: INFO:slot 28,val 0x00000520, index - 1
wccp: INFO:slot 29,val 0x00000522, index - 2
wccp: INFO:slot 30,val 0x00000524, index - 0
wccp: INFO:slot 31,val 0x00000526, index - 1
wccp: INFO:### Timestamp 117 ###
wccp: INFO:RA (mask) sent to 172.28.15.33.(624 bytes)

```

它当前是117，为了需要的指定时间能发送RA。即然此WSA是活跃的，我们决定我们是DWC，因为我们是WCS中的最低的IP。INFO阐明，我们需要发送RA。我们协商的负载均衡方法屏蔽。屏蔽的表使用一个循环法索引和显示。在底部的INFO表示，我们发送了RA @ 117。

```

wccp: INFO:### Timestamp 121 ###
wccp: STATE:SVC@0x0x85bd000: index=0 type=0 ID=0
wccp: STATE: [MD5][MH_DONE][HASH_OK][MASK_OK][MASKING][L2FWD_OK]
           [GREFWD_OK][LGR_DONE][L2RET_OK][GRERET_OK][RET_GRE]
           [DWC][FWD][SERVER]
wccp: STATE: needRA(=2)@127, ISY@111, viewchg=2, viewed=2, keychg=1
wccp: STATE: this period:(HIAs=1, ISYs=1) proto=6
wccp: STATE: ports = 0, 0, 0, 0, 0, 0, 0, 0
wccp: STATE: WC@0x0x85b9020: (10.251.0.73) mentioned:111 weight:1 status:0
wccp: STATE: [ME][ACTIVE]

```

```
wccp: STATE: WC@0x0x85b9160: (172.17.0.10) mentioned:111 weight:1 status:0
wccp: STATE: [ACTIVE]
wccp: STATE: WC@0x0x85b9140: (172.28.6.34) mentioned:111 weight:1 status:0
wccp: STATE: [ACTIVE]
wccp: STATE: nexus@0x0x85bf000: rcvd_key(172.17.0.10,5) sent_key(10.251.0.73,1)
wccp: STATE: rtr_mention@111, ISY@111 rtr_change#= 24 refs=0
wccp: STATE: [FIXED][ALIVE][ACTIVE][FWD_GRE][VIEW_VALID]
wccp: STATE: rstate=0, outst_HIA=0, receiveID=161
wccp: STATE: rtr@0x0x85be000: fd(3) gre-1, bind=10.251.0.73, sentto=172.28.15.33
wccp: STATE: configaddr=172.28.15.33, ID_addr=172.28.15.33, from_addr=172.28.3.46
wccp: INFO:send_HIA called
```

视图当前是有效的，并且我们发送了1重定向分配，如notified由**sent_key**。这时一切应该是正在运行和好。