بسمه تعالی

امن‌سازی پایه زیرساخت شبکه

بخش پنجم: نظارت بر عملکرد شبکه از راه دور

به منظور حصول اطمینان از در دسترس بودن شبکه، بسیار مهم است که نسبت به آنچه که در هر لحظه و مکان از شبکه رخ می‌دهد آگاهی داشت. نظارت بر عملکرد شبکه از راه دور، قابلیت‌های تشخیصی گسترده و مفیدی با صرف هزینه اندک در اختیار قرار می‌دهد. در این گزارش فرم‌های پایه پیشنهادی برای نظارت بر عملکرد شبکه از راه دور معرفی می‌گردد:

- همگام‌سازی زمان‌ها
- آمارهای ترافیک دستگاه محلی
- اطلاعات وضعیت سیستم
- بهترین روش متداول CDP
- SNMP
- Syslog
- ACL
- حسابداری
- تغییر تنظیمات بایگانی
- ضبط بسته

نظارت بر عملکرد شبکه از راه دور از دید متدولوژی CSF

نتایج حاصل از اعمال متدولوژی CSF در حوزه نظارت بر عملکرد شبکه از راه دور در جدول زیر خلاصه شده است:

مانیتور	شناسایی
• NTP • آمارهای دستگاه محلی • اطلاعات وضعیت سیستم– حافظه/CPU/پردازش‌ها • CDP بهترین روش متداول • ورود به سیستم– SNMP –Syslog– حسابداری • ضبط بسته - SPAN/RSPAN –Copy/capture VACLs	• CDP • SNMP • Syslog

هم‌گام‌سازی

زمانی که نظارت بر عملکرد شبکه از راه دور پیاده‌سازی می‌شود، مهم است که تاریخ و زمان، هر دو در تمام دستگاه‌های زیرساخت شبکه دقیق و هم‌گام باشند. بدون هم‌گامی زمان، ارتباط منابع مختلف برای نظارت بر عملکرد شبکه از راه دور بسیار دشوار است. فعال کردن پروتکل زمان شبکه (NTP) رایج‌ترین روش هم‌گام‌سازی زمان می‌باشد.

عمومی‌ترین شیوه رایج برای پیاده‌سازی NTP عبارت است از:

- یک منطقه زمانی مشترک در کل شبکه زیرساخت به منظور فعال کردن و هم‌گام‌سازی زمان در تمام دستگاه‌های شبکه توصیه می‌شود.
- منبع هم باید از مجموعه‌ای محدود از سرورهای NTP مجاز تصدیق گردد.

در IOS سیسکو، مراحل فعال کردن برچسب زمانی و NTP عبارتند از:

۱. فعال کردن اطلاعات زمان برای پیام‌های اشکال‌زدایی
۲. فعال کردن اطلاعات برچسب زمان برای پیام نگار
۳. تعریف منطقه زمانی شبکه گسترده
۴. فعال کردن تنظیمات فصل تابستان
۵. محدود کردن اینکه کدام دستگاه‌ها می‌توانند با این دستگاه به عنوان یک سرور NTP ارتباط برقرار کنند.
۶. محدود کردن اینکه کدام دستگاه‌ها می‌توانند با این دستگاه به عنوان یک همتای NTP ارتباط برقرار کند.
۷. تعریف آدرس IP مبدا که برای بسته NTP استفاده می‌شود.
۸. فعال کردن احراز هویت NTP
۹. تعریف سرورهای NTP
۱۰. تعریف همتایان NTP

۱۱. فعال کردن NTP برای به روزرسانی ساعت سخت افزار دستگاه

دستورات IOS سیسکو برای رسیدن به مراحل بالا در بخش زیر ارائه شده است:

درج اطلاعات زمانی برای پیام‌های اشکال‌زدایی با دستور پیکربندی زیر فعال می‌شود:

```
service timestamps debug datetime localtime show-timezone msec
```

درج اطلاعات زمانی برای پیام نگار با دستور پیکربندی زیر فعال می‌شود:

```
service timestamps log datetime localtime show-timezone msec
```

منطقه زمان شبکه گسترده که در این مثال به عنوان PST نشان داده شده، می‌تواند با دستور پیکربندی زیر فعال شود:

```
clock timezone EST -5
```

تنظیمات فصل تابستان، که در این مثال برای PDT نشان داده شده است، می‌تواند با دستور پیکربندی زیر فعال شود:

```
clock  summer-time EDT recurring
```

لیست سرورهای مجاز NTP و همتایان می‌توانند با یک ACL اجرا شوند:

```
access-list 10 remark ACL for NTP Servers and peers
access-list 10 permit <NTPserver1>
access-list 10 permit <NTPserver2>
access-list 10 permit <NTPpeer1>
access-list 10 deny any log
!
ntp access-group peer 10
```

مشتریان NTP نیز می‌توانند با ACL محدود شوند:

```
access-list 15 remark ACL for NTP clients
access-list 15 permit <Client1>
access-list 15 permit <Client2>
access-list 15 deny any log
!
ntp access-group serve-only 15
```

آدرس IP مبدا که برای بسته‌های NTP می‌تواند استفاده شود، با دستور پیکربندی زیر تعریف می‌شود:

```
ntp source <Loopback or OOB interface>
```

اولین گام در احراز هویت NTP آن است که یک کلید MD5 تعریف شود و برای انجام تعاملات NTP استفاده شود:

```
ntp authentication-key <key#> md5 <strong8charkey>
```

کلیدهای پذیرفته‌شده برای احراز هویت NTP با دستور زیر تعریف می‌شوند:

```
ntp trusted-key <key#>
```

احراز هویت NTP با دستور پیکربندی زیر اجرا می‌گردد:

```
ntp authenticate
```

NTP برای به روزرسانی ساعت سخت‌افزار دستگاه از دستور پیکربندی زیر استفاده می‌کند:

```
ntp update-calendar
```

سرورهای NTP با دستور پیکربندی زیر تعریف می‌شوند:

```
ntp server <NTPserver1>
ntp server <NTPserver2>
```

هر همتای NTP نیز با دستور پیکربندی زیر تعریف می‌شود:

```
ntp peer <NTPpeer1>
ntp peer <NTPpeer2>
```

آمارهای ترافیک دستگاه محلی

آمارهای دستگاه محلی اساسی‌ترین فرم برای نظارت بر عملکرد شبکه از راه دور می‌باشند. در IOS سیسکو، این اطلاعات از رابط خط فرمان (CLI) قابل دسترسی می‌باشد. فرمت خروجی دستور وابسته به نوع پلتفرم است و بر اساس نوع آن تغییر می‌کند.

آمارهای per-interface

در IOS سیسکو، آمارهای per-interface در دسترس می‌باشند که شامل اطلاعات توان عملیاتی (PPS) و پهنای باند (BPS) می‌باشد. آمارهای per-interface می‌تواند با استفاده از دستور show interface در دسترس قرار گیرد:

```
Router#show interface gigabitEthernet 4/48
GigabitEthernet4/48 is up, line protocol is up (connected)
Hardware is C6k 1000Mb 802.3, address is 0013.5f21.6c80 (bia 0013.5f21.6c80)
Description: cr17-3845-1 fe0
Internet address is 10.139.5.8/31
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 1000Mb/s
input flow-control is off, output flow-control is off
Clock mode is auto
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:03, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/15005/235 (size/max/drops/flushes); Total output drops: 1
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 4751000 bits/sec, 3006 packets/sec
5 minute output rate 4499000 bits/sec, 2755 packets/sec
L2 Switched: ucast: 19841909032 pkt, 3347755205145 bytes - mcast: 96885779 pkt, 5131184435 bytes
L3 in Switched: ucast: 27282638229 pkt, 5095662463006 bytes - mcast: 94 pkt, 5191 bytes mcast
L3 out Switched: ucast: 43107617667 pkt, 7275264441541 bytes
47118207406 packets input, 9306459456266 bytes, 0 no buffer
Received 83653389 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 649 overrun, 0 ignored
0 input packets with dribble condition detected
43210876182 packets output, 8089398934796 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
```

0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

دستور pipe سیسکو IOS و گزینه‌های تجزیه آن نیز ممکن است با هدف قرار دادن اطلاعات خاص در خروجی رابط استفاده شود. به عنوان مثال، برای مشاهده سریع یک دقیقه نرخ ورودی و خروجی در یک رابط داریم:

Router#show interface <interface-type numer> | include 1 minute
1 minute input rate 54307000 bits/sec, 17637 packets/sec
1 minute output rate 119223000 bits/sec, 23936 packets/sec

توجه: نرخ ورودی یا خروجی بالا در طی یک دوره یک دقیقه‌ای، می‌تواند به منظورتشخیص رفتار غیرعادی بسیار مفید باشد.

اغلب برای دیدن آنچه که در یک شرایط خاص اتفاق می‌افتد، پاک کردن شمارنده لازم است. برای پاک کردن شمارنده رابط داریم:

Router#clear counters <interface-type number>

اطلاعات ویژه Per-Interface IP

در IOS سیسکو، اطلاعات ویژه per-interface، در مورد ویژگی‌های IP پیکربندی شده بر روی یک رابط اطلاعات ارائه می‌کند. به طور خاص، این دستور برای شناسایی شماره یا نام ACL در حال اجرا مفید می‌باشد. اطلاعات ویژه per-interface با دستور show ip interface در دسترس می‌باشد:

Router#show ip interface <interface-type number>
!
Router#show ip interface FastEthernet 2/0
FastEthernet2/0 is up, line protocol is up
Internet address is 198.133.219.6/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is 110
Proxy ARP is disabled

```
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are never sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Feature Fast switching turbo vector
IP Feature CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
Router#
```

همچنین دستور show ip interface آمار بسته‌های drop شده per-interface uRPF را ارائه می‌کند. دستور pipe در IOS سیسکو می‌تواند به منظور دسترسی به این اطلاعات استفاده شود:

```
Router#show ip interface <interface-type number> | include 1 verification
!
Router#show ip interface FastEthernet 2/0| include veri
IP verify source reachable-via ANY
794407 verification drops
1874428129 suppressed verification drops
```

آمارهای ترافیک IP

در IOS سیسکو، آمارگان ترافیک IP ، اطلاعات بسیار مفیدی فراهم می‌نماید از جمله ترافیک مربوط به پروتکل ICMP، TCP، UDP و همچنین ترافیک چندپخشی. آمار ترافیک IP می‌تواند با دستور show ip traffic در دسترس قرار گیرد:

```
Router#show ip traffic
IP statistics:
Rcvd: 4744853 total, 4650886 local destination
0 format errors, 0 checksum errors, 0 bad hop count
0 unknown protocol, 0 not a gateway
0 security failures, 0 bad options, 0 with options
Opts: 0 end, 0 nop, 0 basic security, 0 loose source route
0 timestamp, 0 extended security, 0 record route
0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
0 other
Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
0 fragmented, 0 fragments, 0 couldn't fragment
Bcast: 1432237 received, 9 sent
Mcast: 3156376 received, 3147383 sent
Sent: 3213086 generated, 284 forwarded
Drop: 42692 encapsulation failed, 0 unresolved, 0 no adjacency
0 no route, 0 unicast RPF, 0 forced drop
0 options denied
Drop: 0 packets with source IP address zero
Drop: 0 packets with internal loop back IP address
…
ARP statistics:
Rcvd: 1419832 requests, 4643 replies, 300822 reverse, 0 other
Sent: 1057 requests, 4897 replies (0 proxy), 0 reverse
```

این دستور برای عیب‌یابی کلی بسیار مفید است. همچنین می‌تواند برای تشخیص ناهنجاری‌ها نیز به کار می‌رود.

همچنین دستور show ip traffic آمار بسته‌های drop شده uRPF را ارائه می‌کند:

```
Router#show ip traffic | include RPF
0 no route, 124780722 unicast RPF, 0 forced drop
```

اطلاعات وضعیت سیستم

میزان مصرف حافظه، پردازشگر و پروسس‌ها

یکی از نشانه‌های اولیه بروز یک مسئله بالقوه بر روی یک دستگاه زیرساخت شبکه، بالا بودن میزان مصرف پردازشگر آن می‌باشد. در IOS سیسکو، اطلاعات در مورد میزان استفاده از پردازنده در بازه‌های ۵ ثانیه، ۱ دقیقه و ۵ دقیقه با دستور زیر در دسترس می‌باشد:

```
Router#show processes cpu
```

دستور pipe در IOS سیسکو به منظور حذف اطلاعات مصرفی توسط CPU می‌تواند مورد استفاده قرار گیرد:

```
Router#show processes cpu | exclude 0.00%__0.00%__0.00%
CPU utilization for five seconds: 38%/26%; one minute: 40%; five minutes: 43%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
5 192962596 13452649 14343 0.00% 0.52% 0.44% 0 Check heaps
15 4227662201540855414 274 0.65% 0.50% 0.49% 0 ARP Input
26 2629012683680473726 71 0.24% 0.29% 0.36% 0 Net Background
50 9564564 11374799 840 0.08% 0.07% 0.08% 0 Compute load avg
51 15291660 947844 16133 0.00% 0.03% 0.00% 0 Per-minute Jobs
58 15336356 92241638 166 0.08% 0.02% 0.00% 0 esw_vlan_stat_pr
67 10760516 506893631 21 0.00% 0.01% 0.00% 0 Spanning Tree
68 31804659682556402094 1244 7.02% 7.04% 7.75% 0 IP Input
69 25488912 65260648 390 0.00% 0.03% 0.00% 0 CDP Protocol
73 16425564 11367610 1444 0.08% 0.02% 0.00% 0 QOS Stats Export
81 12460616 1020497 12210 0.00% 0.02% 0.00% 0 Adj Manager
82 442430400 87286325 5068 0.65% 0.73% 0.74% 0 CEF process
83 68812944 11509863 5978 0.00% 0.09% 0.11% 0 IPC LC Message H
95 54354632 98373054 552 0.16% 0.12% 0.13% 0 DHCPD Receive
96 61891604 58317134 1061 1.47% 0.00% 4.43% 0 Feature Manager
```

مقدار بالای استفاده از پردازنده، شاخص خوبی برای ورود و خروج ترافیکی محسوب می‌گردد که موجب درگیری پردازشگر می‌شود. شناخت دستگاه‌های مستقر در شبکه و شناخت وضعیت عادی، یکی از اولین گام‌ها درتشخیص چنین ناهنجاری می‌باشد.

هشدار آستانه حافظه‌های Syslog

سیسکو IOS توانایی ارسال هشدار عبور از آستانه مصرف حافظه را دارد. پیام syslog زمانی فرستاده می‌شود که استفاده از حافظه پایین‌تر یا بالاتر از میزان مورد نظر باشد. این مکانیزم با استفاده از دستورهای زیر فعال می‌گردد:

```
Router(config)#memory free low-watermark processor <kilobytes threshold>
Router(config)#memory free low-watermark io <kilobytes threshold>
```

هنگامی که آستانه‌ها پیکربندی شود، روتر هر بار که حافظه آزاد موجود کمتر از حد آستانه خاص شود و هر بار که حافظه آزاد موجود ۵ درصد بالاتر از آستانه مشخص شده شود، اطلاع رسانی می‌کند. به عنوان مثال، هرگاه حافظه آزاد کمتر از حد آستانه مشخص شده باشد، خروجی زیر تولید می‌گردد:

```
000029: *Aug 12 22:31:19.559: %SYS-4-FREEMEMLOW: Free Memory has dropped below 2000k
Pool: Processor Free: 66814056 freemem_lwm: 204800000
Example output when available free processor memory recovered to more than the specified threshold
000032: *Aug 12 22:33:29.411: %SYS-5-FREEMEMRECOVER: Free Memory has recovered 2000k
Pool: Processor Free: 66813960 freemem_lwm: 0
```

رزرو حافظه برای هشدارهای بحرانی

IOS سیسکو توانایی محافظت از ورود به سیستم هنگامی که منابع یک دستگاه کم است را فراهم می‌کند. با استفاده از این ویژگی یک ناحیه از حافظه بر روی دستگاه فقط برای ثبت وقایع رزرو می‌شود و در دسترس خواهد بود. رزرو حافظه برای ثبت وقایع با دستور زیر فعال می‌گردد:

```
Router(config)# memory reserve critical <kilobytes>
```

هشدار عبور از سطح آستانه مصرف CPU از طریق SNMP

IOS سیسکو توانایی ارسال هشدار عبور از سطح آستانه مصرف CPU از طریق SNMP را دارد. SNMP زمانی ارسال می‌گردد که استفاده از پردازنده بالاتر یا پائین‌تر از سطح آستانه باشد.

افزایش ناگهانی بار CPU در روترها و سوئیچ‌ها اغلب نشان می‌دهد که رویدادی ناخوشایند در حال وقوع است، با این حال مصرف بالای CPU همواره نشانه انجام فعالیت‌های مخرب نیست. بنابراین تجزیه و تحلیل سایر اطلاعات در هنگام وقوع این امر بسیار توصیه می‌شود.

هشدار عبور از سطح آستانه CPU می‌تواند برای موارد زیر تعریف شود:

- مجموع میزان استفاده از پردازنده
- مجموع میزان استفاده یک پروسه از پردازنده
- وقوع وقفه CPU

هشدار عبور از آستانه CPU می‌تواند با دستور process cpu threshold پیکربندی گردد:

Router(config)# process cpu threshold type {total | process | interrupt} rising <percentage> interval <seconds> [falling <percentage> interval <seconds>]

به عنوان مثال، برای ارسال یک بسته SNMP در هنگام استفاده بیش از ۸۰٪ از پردازنده برای بیش از ۵ ثانیه و مصرف کمتر از ۲۰٪ برای بیش از ۵ ثانیه داریم:

```
Router(config)# snmp-server enable traps cpu threshold
Router(config)# snmp-server host 172.26.150.206 traps public cpu
Router(config)# process cpu threshold type total rising 80 interval 5 falling 20 interval 5
```

البته بهتر است که بر روی نرخ ورود اطلاعات و سایز جدول آمار مصرف cpu توسط دستور process cpu محدودیت ایجاد کرد:

Router(config)# process cpu statistics limit entry-percentage number [size seconds]

مثال زیر نشان می‌دهد که چگونه می‌توان نرخ ورود اطلاعات را برابر ۴۰ درصد و بازه زمانی را ۳۰۰ ثانیه تنظیم کرد:

Router(config)# process cpu statistics limit entry-percentage 40 size 300

جدول وضعیت آدرس MAC

اطلاعاتی که در این جدول است، مشخص می‌کند کدام آدرس‌های MAC در حال حاضر به کدام پورت متصل هستند که می‌تواند برای ردیابی و شناسایی رفتارهای غیر عادی مفید باشد. IOS سیسکو توانایی مشاهده وضعیت جدول آدرس‌های MAC بر روی سوئیچ‌ها را با استفاده از دستور زیر ارائه می‌دهد:

```
Router#show mac-address-table
```

خروجی شامل اطلاعاتی در مورد آدرس‌های MAC ذخیره شده می‌باشد، از جمله اینکه به صورت استاتیک یا به صورت پویا فراگیری شده‌اند، مدت زمان حاضر بودن در جدول چقدر است و نیز VLAN و interface مربوطه.

این فرمان می‌تواند برای ردیابی یک MAC آدرس خاص به کار گرفته شود. به عنوان مثال برای آدرس MAC 0100.5e00.0128 در Catalyst6500 داریم:

```
Router# show mac-address-table address 0100.5e00.0128
Legend: * - primary entry
      age - seconds since last seen
      n/a - not available

vlan mac address       type    learn   age      ports
------+----------------+--------+-----+----------+--------------------------
Supervisor:
*   44 0100.5e00.0128   static Yes       - Fa6/44,Router
*   1 0100.5e00.0128    static Yes       - Router
Module 9:
*   44 0100.5e00.0128   static Yes       - Fa6/44,Router
*   1 0100.5e00.0128    static Yes       - Router
```

تعداد آدرس MAC ذخیره شده در جدول MAC Address و مقدار فضای باقی مانده می‌تواند با دستور mac-address-table count نشان داده شود. یک نمونه خروجی برای یک اسلات خاص در یک catalyst 6500 در زیر نشان داده شده است:

```
Router# show mac-address-table count slot 1
MAC Entries on slot 1 :
Dynamic Address Count: 4
Static Address (User-defined) Count: 25
Total MAC Addresses In Use: 29
Total MAC Addresses Available: 131072
```

ورودی‌های جدول MAC Address با توجه به زمان پیکربندی مرتب خواهد شد. آدرس‌های MAC یاد گرفته شده به صورت پویا را می‌توان با دستور زیر پاک کرد:

```
clear mac-address-table dynamic
```

سوکت‌ها و پورت‌های باز

سوکت‌ها و پورت‌های باز در یک دستگاه باید به منظور حصول اطمینان از اینکه پورت‌ها و سوکت‌های استفاده نشده یا غیرضروری غیر فعال هستند، بررسی شوند. در IOS سیسکو، سوکت‌ها وپورت‌های باز را می‌توان با دستور show control-plane host open-ports مشاهده کرد:

```
Router#show control-plane host open-ports
Active internet connections (servers and established)

Prot      Local Address          Foreign Address        Service         State
tcp       *:22                   *:0                    SSH-Server      LISTEN
tcp       *:23                   *:0                    Telnet          LISTEN
tcp       *:63771                172.26.150.206:49      IOS host service  ESTABLIS
udp       *:49                   172.26.150.206:0       TACACS service    LISTEN
udp       *:67                   *:0                    DHCPD Receive     LISTEN
Router#
```

جهت چک کردن پورت‌های UDP از دستور show ip sockets استفاده می‌شود:

```
Router#show ip sockets
```

یک نمونه خروجی در زیر نشان داده شده است:

```
Router#show ip sockets
Proto      Remote  Port     Local       Port   In    Out   Stat   TTY OutputIF
17 0.0.0.0          0          198.133.219.6  67     0     0     2211   0
88       --listen--  --any-- 100 0 0 0 0
17    172.26.150.206    49    172.26.159.165 49     0     0     21     0
17    --listen--       --any--  161 0 0 1 0
17    --listen--       --any--  162 0 0 11 0
17    --listen--       --any--             56443  0     0     1      0
17    172.26.150.206  514 172.26.159.165     55759  0     0     210    0
Router#
```

در نسخه‌های جدید سیسکو IOS، پورت‌های باز می‌توانند در دو مرحله با دستورات زیر نشان داده شوند:

```
Router#show tcp brief all
Router#show tcp tcb
```

استفاده از دستور show tcp brief all جهت دیدن آدرس IP مبدا و مقصد و وضعیت نشست TCP استفاده می‌شود. این دستور همچنین بلوک کنترل انتقال (TCB) که یک شناسه داخلی استفاده شده توسط روتر / سوئیچ برای شناسایی اتصال است را فراهم می‌کند. مقادیر TCB برای شناسایی پورت مرتبط با اتصالات استفاده می‌شود.

```
Router#show tcp brief all
TCB          Local Address          Foreign Address        (state)
661BB46C     172.26.159.165.49128       172.26.150.206.49          ESTAB
6612A398     198.133.219.6.179          198.133.219.10.11003       ESTAB
20465FC8     172.26.159.165.22          172.26.159.164.15774       ESTAB
50711308     198.133.219.6.16422        198.133.219.5.179          ESTAB
661B9248     172.26.159.165.19110       172.26.150.206.49          CLOSEWAIT
6612ACC4     *.179                      198.133.219.5.*       LISTEN
661294C0     *.179                      198.133.219.10.*      LISTEN
Router#
```

از دستور show TCB TCP برای مشاهده سوکت‌های مبدا و مقصد برای یک نشست TCP استفاده می‌شود:

```
Router#show tcp tcb 20465FC8
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 255
Local host: 172.26.159.165, Local port: 22
Foreign host: 172.26.159.164, Foreign port: 15774
Connection tableid (VRF): 0
```

توصیه‌هایی درخصوص پروتکل CDP

پروتکل شناسایی سیسکو (CDP) یک پروتکل کشف دستگاه‌های سیسکو می‌باشد که با اجرا در لایه ۲ اجازه می‌دهد تا دستگاه‌های سیسکو به تبادل اطلاعات با یکدیگر بپردازند.

اطلاعات CDP به صورت متن فاش و ارتباطات نا امن فرستاده می‌شود. در نتیجه، CDP نسبت به سوءاستفاده آسیب‌پذیر می‌باشد، از جمله افشای اطلاعات حساس در مورد یک دستگاه زیرساخت شبکه مانند آدرس IP، نسخه نرم افزار، مدل روتر و توپولوژی شبکه.

بهترین روش امن‌سازی CDP عبارت است از:

- فعال کردن CDP در زیرساخت نقطه-به-نقطه
- غیر فعال کردن CDP در دستگاه‌های مرزی و یا رابط‌هایی که مورد نیاز نیست از جمله:
  - لبه دسترسی LAN
  - لبه انتقال اینترنت
  - لبه extranret
  - تمامی رابط‌های عمومی

لازم به ذکر است که CDP برای مدیریت شبکه در برخی از برنامه‌های کاربردی سیسکو، برخی محصولات و برخی ویژگی‌ها از قبیل سیسکو IP Telephony مورد نیاز است. در موارد نادری که CDP به‌خاطر عیب‌یابی و یا مسائل امنیتی استفاده نمی‌شود، این سرویس می‌تواند با استفاده از دستور no cdp run غیرفعال گردد:

```
Router(config)#no cdp run
```

خدمات CDP می‌تواند به‌صورت per-interface با استفاده از no cdp run غیرفعال گردد:

```
Router(config)# interface <interface-type number>
Router(config-if)# no cdp enable
```

CDP و اطلاعات تجهیزات همسایه

برای مشاهده اطلاعات دقیق کشف شده توسط CDP در مورد دستگاه‌های همسایه، از دستور زیر استفاده می‌شود:

```
Router#show cdp neighbors
```

یک نمونه خروجی اجرای دستور فوق در زیر نشان داده شده است:

```
cr18-7301-1#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge ,                S -
Switch, H - Host, I - IGMP, r - Repeater
Device ID        Local Intrfce     Holdtme Capability       Platform Port ID
```

```
cr17-2821-1       Gig 0/2  154          R S I          2821          Gig 0/0
cr18-6500-2.cisco.com
                  Gig 0/1  150          R S I          WS-C6506      Gig 2/1
cr18-6500-1.cisco.com
                  Gig 0/0  123          R S I          WS-C6506-E    Gig 2/1
cr18-7301-1#
```

Syslog

syslog یک استاندارد ارسال log مبتنی بر UDP می‌باشد. بسته‌های Syslog بر اساس وقوع حوادث خاص در یک دستگاه تولید شده و حاوی اطلاعات عملیاتی ارزشمندی از جمله وضعیت سیستم، آمار ترافیک و دسترسی به اطلاعات دستگاه است.

توصیه‌هایی درخصوص syslog

یکی از چالش‌های syslog، حجم داده syslog است که می‌تواند بار قابل توجهی در هر دو دستگاه فرستنده داده‌ها و سرور syslog ایجاد کند. از این‌رو مهم است که برای اطمینان، ملاحظات زیر در نظر گرفته شوند:

- ارسال لاگ‌های syslog به یک سرور مرکزی
- حصول اطمینان از وجود فضای ذخیره‌سازی و ظرفیت پردازش کافی در سرور syslog
- توصیه می‌شود که نرخ ارسال لاگ محدود گردد.
- بهتر است تجهیزات مهم لاگ بیشتری تولید و ذخیره کنند و بالعکس.
- عدم نمایش لاگ‌ها در کنسول روتر و سوئیچ
- حصول اطمینان از صحت زمان (توسط NTP)
- حصول اطمینان از ذخیره لاگ‌ها در یک دیتابیس جستجوپذیر
- حصول اطمینان از امنیت سرور Syslog و همچنین رمز شدن محتویات دیتابیس

سرور مرکزی syslog

در IOS سیسکو، پیام‌های syslog می‌تواند به یک سرور مرکزی با تعریف آدرس IP مبداء استفاده شود:

```
Router(config)#logging source-interface <interface>
```

```
Router(config)#logging host <syslogserver>
Router(config)#logging trap <level>
```

امکانات syslog

می‌توان لاگ‌ها را به‌صورت منطقی جداسازی نمود و آن‌ها را در شاخه‌های مجزایی ذخیره نمود. در IOS سیسکو می‌توان از facility بدین منظور استفاده نمود:

```
Router(config)#logging facility <facility>
```

محدودسازی نرخ ارسال پیام syslog

درصورتی‌که قابلیت محدودسازی نرخ ارسال پیام در Syslog وجود داشته باشد، توصیه می‌شود که این قابلیت برای حصول اطمینان از آن‌که ارسال پیام syslog، CPU را در هر دو دستگاه فرستنده یا سرور syslog تحت تاثیر قرار نمی‌دهد، فعال شود. همان‌طور که از نام این قابلیت مشخص است، محدودسازی نرخ ارسال پیام‌های syslog، نرخ ارسال پیام‌ها در هر ثانیه را محدود می‌کند.

در نسخه‌های IOS سیسکو که دارای قابلیت محدودسازی نرخ ارسال پیام Syslog هستند، مقدار ۱۰ پیام در ثانیه به طور پیش فرض تنظیم شده است. مقدار پیش فرض می‌تواند با دستور logging rate-limit تغییر کند. دستور logging rate-limit اجازه می‌دهد تا یک محدوده برای نرخ‌های مختلف برای تمام سطوح تنظیم گردد.

در مثال زیر، پیام‌های هر سطح به ۵ ثانیه محدود شده‌اند:

```
Router(config)#logging rate-limit 5
```

در این مثال، پیام در سطح ۳ و بالاتر به یک پیام در ثانیه محدود شده است، در حالی که پیام‌های در سطوح ۰ تا ۲ محدود نیستند:

```
Router(config)#logging rate-limit 1 except 2
```

سرورهای مشترک Syslog

برخی از سرویس‌دهنده‌های مشترک syslog عبارتند از:

- همبسته‌ساز ساده وقایع (Simple Event Correlator)(SEC) : یک ابزارقدرتمند منبع باز که قادر به محاسبه همبستگی میان پیام‌های syslog است.
- سیسکو CS-MARS: قادر به دریافت ورودی syslog از روترها، سوئیچ‌ها، فایروال‌ها، IDS، VPN با انواع دیگری از تله متری با هدف همبسته‌سازی و تشخیص ناهنجاری است.
- Sawmill : یک ابزار مبتنی بر وب تجاری می‌باشد که جهت تجزیه و تحلیل بسیاری از انواع مختلف خروجی Syslog و تولید گزارش‌های HTML استفاده می‌شود.

توجه: پایگاه‌های داده منبع باز مانند MySQL و Postgres اغلب برای ذخیره خروجی syslog و سپس پردازش و جستجو استفاده می‌شوند.

SNMP

پروتکل مدیریت شبکه (SNMP) یک پروتکل شبکه محبوب می‌باشد که طیف وسیعی از اطلاعات را برای نظارت بر عملکرد شبکه از راه دور فراهم می‌کند.

سرورهای رایج SNMP

برخی از ابزارها و سیستم عامل‌های مدیریت در تله متری SNMP عبارتند از:

- ابزارهای منبع باز از جمله NET-SNMP، MRTG، کریکت، RRDTool، Nagios
- سیسکو MARS و Arbor PeakFlow Dos
- پلتفرم‌های NMS مانند HP OpenView و Nagios

ثبت ACL

ثبت ACL برای موارد زیر می‌تواند مفید باشد:

- تلاش‌های دسترسی موفق در یک ارتباط مجاز
- تلاش‌های دسترسی ناموفق در یک ارتباط غیر مجاز

اعلام تغییر پیکربندی و ثبت آن

در IOS سیسکو، قابلیت اعلام تغییر پیکربندی و ثبت آن وجود دارد که دستورات وارد شده از طریق خط دستور CLI و HTTP را ثبت و ذخیره می‌کند.

ضبط بسته

معمولاً ضبط بسته‌ها پس از مشاهده ناهنجاری از طریق SNMP یا syslog انجام می‌گیرد. توصیه‌های موجود در این زمینه عبارتند از:

- بایستی ضبط بسته‌ها در نقاط کلیدی توپولوژی مانند دروازه توزیع و ... انجام گیرد.
- مهم است که تنها بسته‌های خاص ضبط شوند (برای جلوگیری از مصرف بی‌حد منابع).
- بسیار مهم است که اطمینان حاصل شود که ترافیک در هر دو جهت ضبط شود.
- مهم است که در توپولوژی‌های پیچیده، ترافیک تکراری ضبط نشود.

SPAN / RSPAN

Switchport و Remote Switchport (SPAN / RSPAN) از جمله ویژگی‌های سیسکو IOS است که بسته‌ها را به سوی سیستم‌های تحلیل ترافیک منتقل می‌کند.

نشست‌های SPAN اجازه نظارت ترافیک بر روی یک یا چند درگاه یا یک یا چند VLAN را مهیا می‌نمایند. SPAN یک کپی از بسته‌های دریافت شده یا منتقل شده توسط پورت مبدا و VLANها را به پورت مقصد ارسال می‌کند.

کپی / ضبط VLAN ACLها

قابلیت VLAN ACL ها باعث می‌شود که بسته‌ها به سوی سیستم تجزیه و تحلیل ترافیک هدایت شوند. با استفاده از forward capture می‌توان در حین عبور عادی ترافیک، یک نسخه از بسته‌ها را به سوی پورت پیکربندی شده هدایت نمود. به عنوان مثالی از چگونگی تعریف و استفاده از VACL جهت ضبط تمام ترافیک منطبق با net_10، کافی است دستورات زیر وارد شوند:

```
Router(config)# vlan access-map capture1 10
Router(config-access-map)# match ip address net_10
```

```
Router(config-access-map)# action forward capture
Router(config-access-map)# exit
Router(config)# vlan filter capture1 vlan-list 2, 4-6
```

با استفاده از دستورات زیر، یک رابط می‌تواند به عنوان یک پورت به منظور ضبط ترافیک پیکربندی شود:

```
Router(config)# interface interface
Router(config-if)# switchport capture
```