Risoluzione dei problemi relativi all'utilizzo elevato della CPU su Catalyst 9000 causati dal processo SISF

Sommario

Introduzione

Questo documento descrive l'elevato utilizzo della CPU sugli switch Cisco Catalyst serie 9000 causato dal processo Switch Integrated Security Features.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base della tecnologia di switching LAN
- Conoscenza degli switch Cisco Catalyst serie 9000
- Familiarità con l'interfaccia della riga di comando (CLI) Cisco IOS® XE
- Familiarità con la funzione Device Tracking

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Switch Cisco Catalyst serie 9000
- Versione del software: Tutte le versioni

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il framework SISF (Switch Integrated Security Features) è stato sviluppato per ottimizzare la sicurezza nei domini di layer 2. Unisce le funzionalità IP Device Tracking (IPDT) e *alcune* funzionalità IPv6 first-hop security (FHS), per semplificare la migrazione da uno stack IPv4 a uno stack IPv6 o doppio.

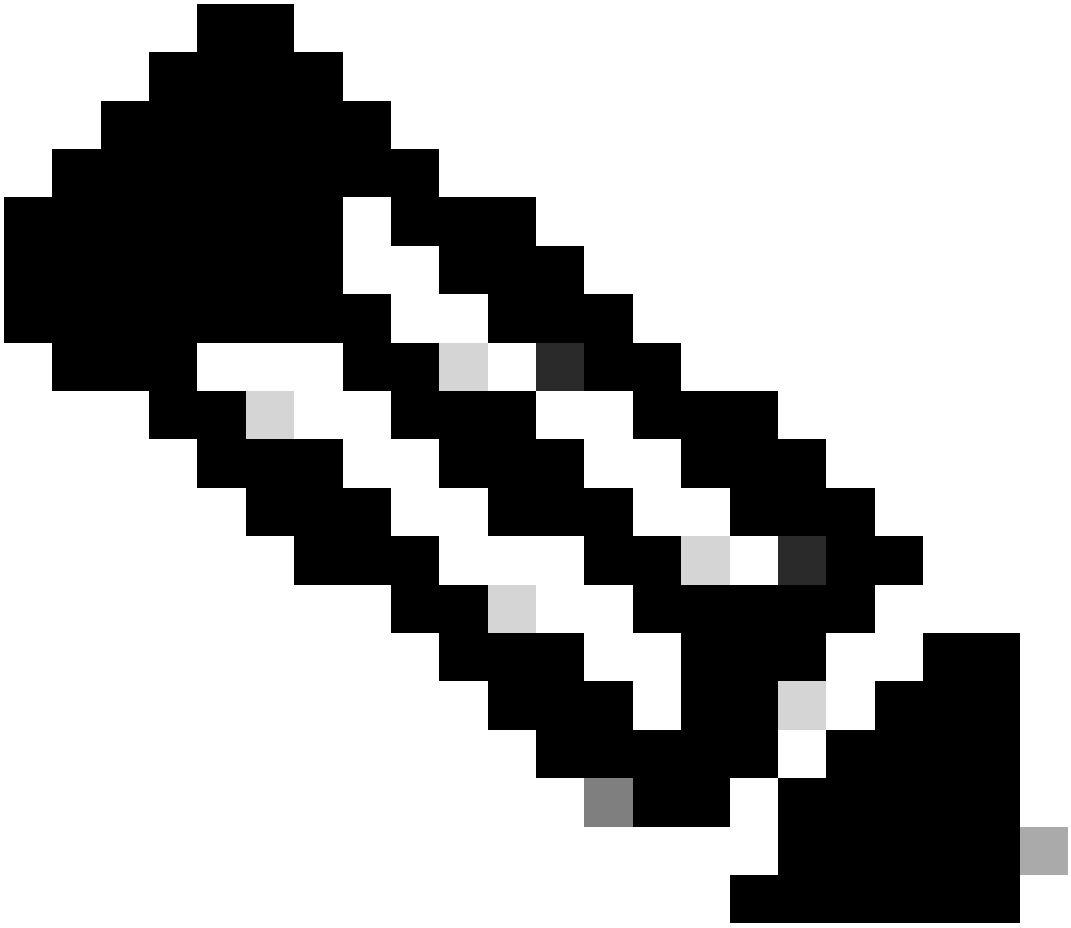
In questa sezione viene fornita una panoramica del problema di utilizzo elevato della CPU osservato sugli switch Cisco Catalyst serie 9000 causato dal processo SISF. Il problema è identificato tramite comandi CLI specifici ed è relativo al monitoraggio dei dispositivi sulle interfacce trunk.

Problema

La sonda keepalive inviata dallo switch viene trasmessa da tutte le porte quando il modulo SISF è abilitato a livello di programmazione. Gli switch collegati nello stesso dominio L2 inviano queste trasmissioni ai loro host. Di conseguenza, lo switch di origine aggiunge host remoti al proprio database di rilevamento dispositivi. Le voci host aggiuntive aumentano l'utilizzo della memoria sul dispositivo e il processo di aggiunta degli host remoti aumenta l'utilizzo della CPU del dispositivo.

È consigliabile definire l'ambito della policy a livello di programmazione configurando una policy sull'uplink sugli switch collegati in modo da definire la porta come attendibile e collegata a uno switch.

Il problema trattato in questo documento è l'elevato utilizzo della CPU sugli switch Cisco Catalyst serie 9000 causato dal processo SISF.



Nota: Tenere presente che le funzionalità dipendenti da SISF, ad esempio lo snooping DHCP, consentono di attivare il protocollo SISF.

Passaggio 1: Verifica utilizzo CPU

Per identificare l'utilizzo elevato della CPU, utilizzare questo comando:

<#root>

```
device#

show processes cpu sorted

CPU utilization for five seconds: 93%/6%; one minute: 91%; five minutes: 87%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process

 439     3560284      554004       6426 54.81% 52.37% 47.39%   0 SISF Main Thread


 438     2325444      675817       3440 22.67% 25.17% 26.15%   0
```

```
SISF Switcher Th

 104      548861       84846       6468 10.76%  8.17%  7.51%   0 Crimson flush tr
 119      104155      671081        155  1.21%  1.27%  1.26%   0 IOSXE-RP Punt Se
<SNIP>
```

Passaggio 2: Controlla database di Device Tracking

Utilizzare questo comando per controllare il database di rilevamento dispositivi:

<#root>

```
device#

show device-tracking database


Binding Table has 2188 entries, 2188 dynamic (limit 200000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DH
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    Network Layer Address                  Link Layer Address     Interface  vlan       prlvl      ag

ARP 192.168.187.204                        c815.4ef1.d457         Po1        602        0005       546
ARP 192.168.186.161                        4c49.6c7b.6722         Po1        602        0005       171
ARP 192.168.186.117                        4c5f.702b.61eb         Po1        602        0005       459
ARP 192.168.185.254                        20c1.9bac.5765         Po1        602        0005       546
ARP 192.168.184.157                        c815.4eeb.3d04         Po1        602        0005       3mn


ARP 192.168.1.2                            0004.76e0.cff8         Gi1/0/19   901        0005       23

ARP 192.168.152.97                         001c.7f3c.fd08         Po1        620        0005       54s
ARP 169.254.242.184                        1893.4125.9c57         Po1        602        0005       209
ARP 169.254.239.56                         4c5f.702b.61ff         Po1        602        0005       142
ARP 169.254.239.4                          8c17.59c8.fff0         Po1        602        0005       223
ARP 169.254.230.139                        70d8.235f.2a08         Po1        600        0005       6mn
ARP 169.254.229.77                         4c5f.7028.4231         Po1        602        0005       107


<SNIP>
```

È evidente che nell'interfaccia Po1 sono registrati più indirizzi MAC. Ciò non è previsto se il dispositivo funge da switch di accesso e all'interfaccia è collegato un dispositivo terminale.

È possibile controllare i membri del canale della porta utilizzando questo comando:

Passaggio 3: Controlla Etherchannel

<#root>

device#

show etherchannel summary

```
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
```

1 Po1(SU) LACP Te1/1/1(P) Te2/1/1(P)

Passaggio 3: Controlla router adiacente CDP

Utilizzare questo comando per controllare il CDP adiacente:

<#root>

device#

show cdp neighbor

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
```

C9500 Ten 2/1/1 132 R S C9500-48Y Twe 2/0/16
C9500 Ten 1/1/1 165 R S C9500-48Y Twe 1/0/16

Uno switch Catalyst 9500 è collegato in modo visibile dall'altro lato. Potrebbe trattarsi di un altro dispositivo di accesso in una configurazione a catena o di uno switch di distribuzione/core. In ogni caso, questi dispositivi non possono tenere traccia degli indirizzi MAC su interfacce trunk.

Soluzione

Il problema di utilizzo elevato della CPU è causato dal rilevamento dei dispositivi. Disabilitare il rilevamento dei dispositivi sulle interfacce trunk.

A tale scopo, creare un criterio di rilevamento dispositivi e collegarlo alle interfacce trunk:

Passaggio 1: Configura criterio di rilevamento dispositivi

Creare un criterio di rilevamento dispositivi per considerare le interfacce trunk come porte attendibili:

<#root>

```
device#
configure terminal

device(config)#
device-tracking policy DT_trunk_policy

device(config-device-tracking)#
trusted-port

device(config-device-tracking)#
device-role switch

device(config-device-tracking)#
end
```

Passaggio 2: Collegare il criterio all'interfaccia trunk

<#root>

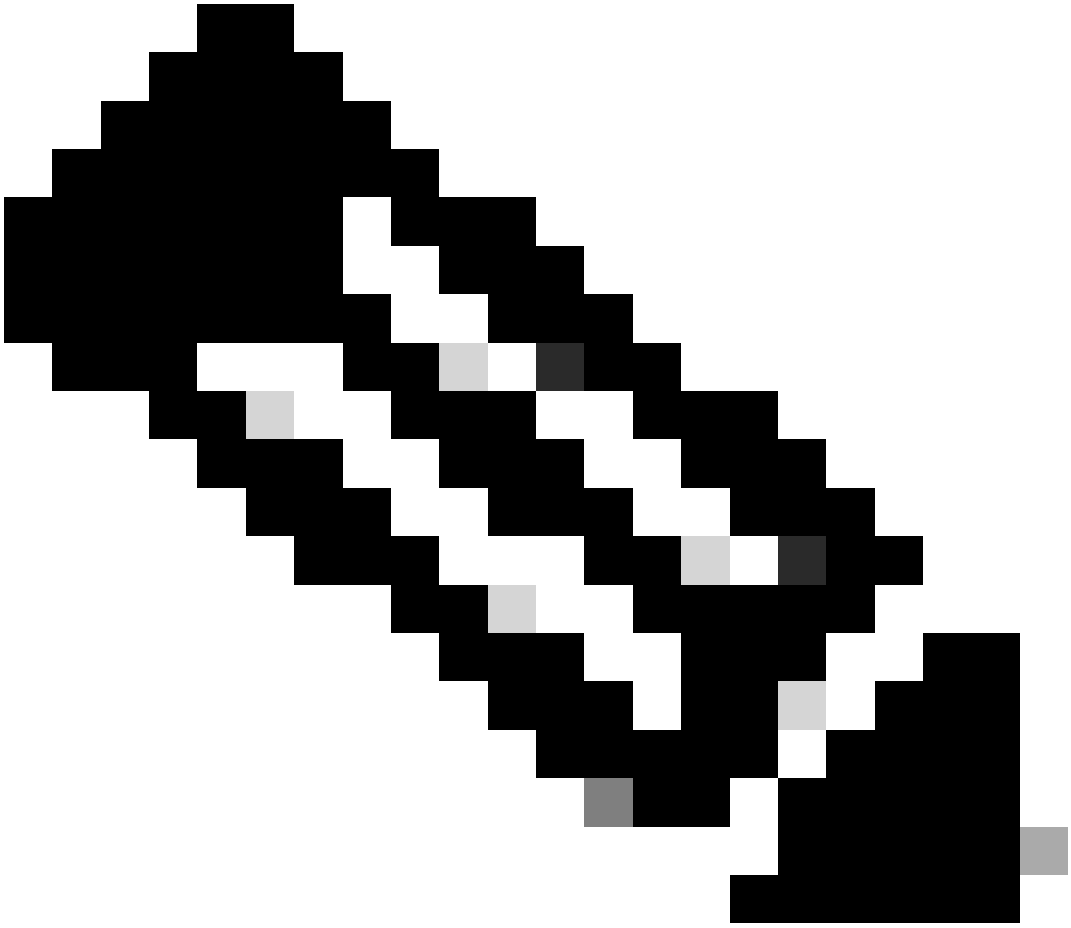
```
device#
cconfigure terminal

device(config)#
interface Po1

device(config-if)#
device-tracking attach-policy DT_trunk_policy
```

```
device(config-if)#
```

end

- **Le opzioni switchandtrusted-**portoptions per il **ruolo dispositivo** consentono di progettare un'area sicura efficiente e scalabile. Se utilizzati insieme, questi due parametri consentono di ottenere una distribuzione efficiente della creazione di voci nella tabella di associazione. In questo modo le dimensioni delle tabelle di associazione rimangono sotto controllo.
- **L'opzione della** porta **attendibile**: Disabilita la funzione guard sulle destinazioni configurate. Le associazioni apprese tramite una porta trusted hanno la preferenza sulle associazioni apprese tramite qualsiasi altra porta. In caso di collisione, una porta attendibile viene inoltre preferita quando si crea una voce nella tabella.
- **L'**opzione **device-**role: Indica il tipo di dispositivo rivolto verso la porta e può essere un nodo o uno switch. Per consentire la creazione di voci di binding per una porta, configurare il dispositivo come nodo. Per interrompere la creazione delle voci di binding, configurare il dispositivo come switch.

La configurazione del dispositivo come switch è ideale per la configurazione di più switch, in cui è molto probabile che esistano tabelle di monitoraggio dei dispositivi di grandi dimensioni. In questo caso, è possibile configurare una porta rivolta verso un dispositivo (una porta trunk uplink) in modo che interrompa la creazione delle voci di binding e considerare attendibile il traffico in arrivo su tale porta, in quanto sullo switch sull'altro lato della porta trunk è abilitata la traccia dei dispositivi e la voce di binding è stata verificata.



Nota: Sebbene in alcuni scenari sia possibile configurare solo una di queste opzioni, il caso di utilizzo più comune riguarda la configurazione sulla porta sia della porta trusted sia dello switch del ruolo del dispositivo.

Informazioni correlate

- Supporto tecnico Cisco e download
- Risoluzione dei problemi relativi a SISF sugli switch Catalyst serie 9000
- Guida alla configurazione della sicurezza, Cisco IOS XE Dublin 17.12.x (switch Catalyst 9300)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).