Problemen oplossen met hoge CPU op Catalyst 9000 veroorzaakt door SISF-proces

Inhoud

Inleiding

In dit document wordt het hoge CPU-gebruik beschreven van switches uit de Cisco Catalyst 9000-reeks die worden veroorzaakt door het proces voor geïntegreerde beveiligingsfuncties van de Switch.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van LAN-switchtechnologie
- Kennis van Cisco Catalyst 9000 serie switches
- Bekendheid met Cisco IOS® XE command-line interface (CLI)
- Vertrouwdheid met Device Tracking-functie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Catalyst 9000 Series switches
- Softwareversie: Alle versies

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Switch Integrated Security Features (SISF) is een framework dat is ontwikkeld om de beveiliging in Layer 2-domeinen te optimaliseren. Het combineert de IP Device Tracking (IPDT) en *bepaalde* IPv6 first-hop security (FHS) functionaliteit, om de migratie van IPv4 naar IPv6 stack of een dual-stack te vereenvoudigen.

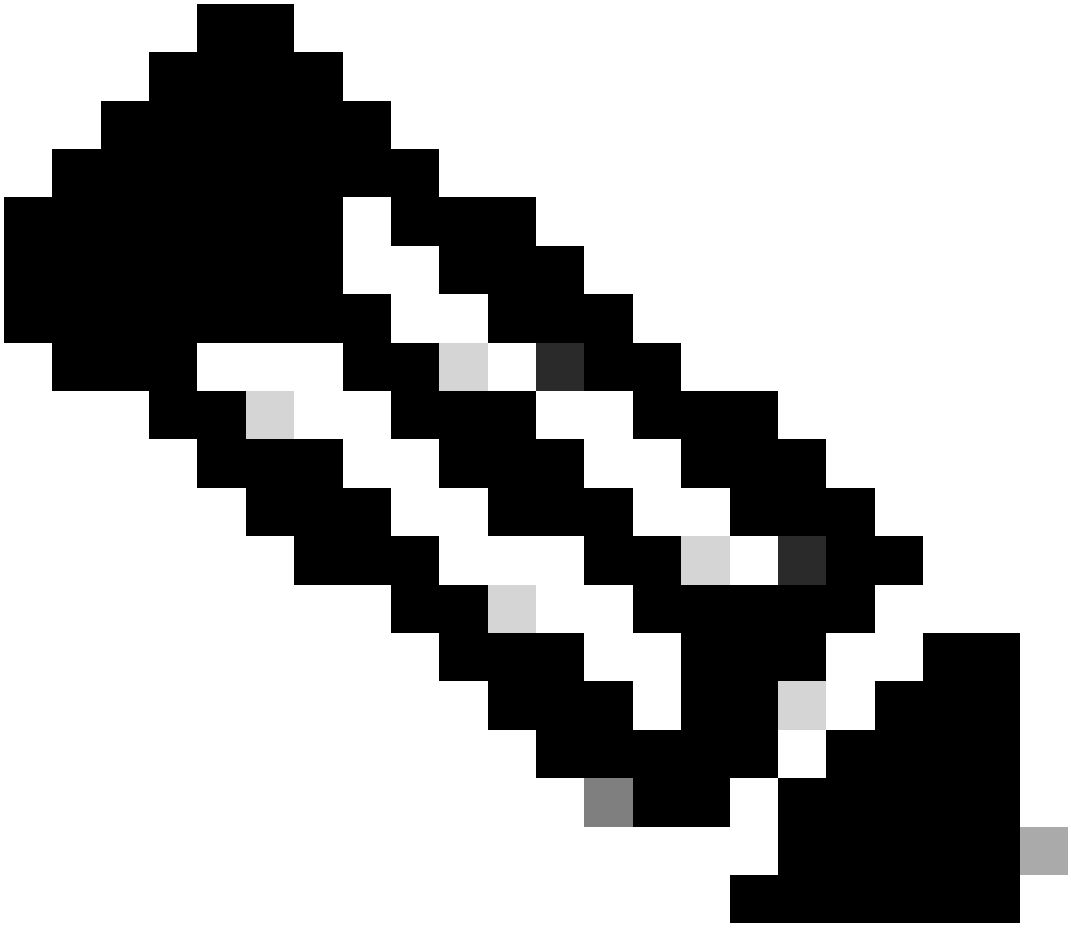
In dit gedeelte wordt een overzicht gegeven van het probleem met het hoge CPU-gebruik dat wordt waargenomen bij switches uit de Cisco Catalyst 9000-reeks die worden veroorzaakt door het SISF-proces. Het probleem wordt geïdentificeerd door middel van specifieke CLI-opdrachten en is gerelateerd aan apparaattracking op trunk-interfaces.

Probleem

De keepalive-sonde die door de switch wordt verzonden, wordt vanuit alle poorten uitgezonden wanneer SISF het programmatisch is ingeschakeld. Bijgevoegde switches in hetzelfde L2-domein sturen deze uitzendingen naar hun hosts, waardoor de oorspronkelijke switch externe hosts toevoegt aan de apparaatvolgdatabase. De extra hostvermeldingen verhogen het geheugengebruik op het apparaat en het proces van het toevoegen van de externe hosts verhoogt het CPU-gebruik van het apparaat.

Het verdient aanbeveling het programmatische beleid te omschrijven door een beleid voor uplink te configureren voor gekoppelde switches om de poort te definiëren als vertrouwd en gekoppeld aan een switch.

Het probleem dat in dit document wordt behandeld, is het hoge CPU-gebruik op switches uit de Cisco Catalyst 9000-reeks, veroorzaakt door het SISF-proces.



Opmerking: houd er rekening mee dat SISF-afhankelijke functies zoals DHCP-snooping SISF mogelijk maken, wat dit probleem kan veroorzaken.

Stap 1: Controle CPU-gebruik

Om het hoge CPU-gebruik te identificeren, gebruikt u de volgende opdracht:

<#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>
```

Stap 2: Apparaatvolgdatabase controleren

Gebruik deze opdracht om de database voor apparaattracking te controleren:

```
<#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>
```

Het is duidelijk dat er meerdere MAC-adressen worden bijgehouden in de Po1-interface. Dit wordt niet verwacht als dit toestel als een toegangsinterface fungeert en er een eindapparaat op de switch is aangesloten.

U kunt de leden van het poortkanaal controleren met deze opdracht:

Stap 3: Controleer Etherchannels

```
<#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)
```

Stap 3: Controleer de CDP-buur

Gebruik deze opdracht om de CDP-buur te controleren:

```
<#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
```

Een Catalyst 9500-switch is zichtbaar aan de andere kant verbonden. Dit kan een ander toegangsapparaat zijn in een seriële ketenconfiguratie of een distributie-/core-switch. In elk geval kunnen deze apparaten geen MAC-adressen bijhouden op een trunk-interfaces.

Oplossing

Het probleem met het hoge CPU-gebruik wordt veroorzaakt door apparaattracking. Schakel apparaattracking uit op de trunk-interfaces.

Maak hiervoor een apparaattraceringsbeleid en koppel dit aan de trunkinterfaces:

Stap 1: Apparaattraceringsbeleid configureren

Maak een apparaattraceringsbeleid om trunkinterfaces als vertrouwde poorten te behandelen:

<#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
```

Stap 2: Bevestig het beleid aan de Trunk-interface

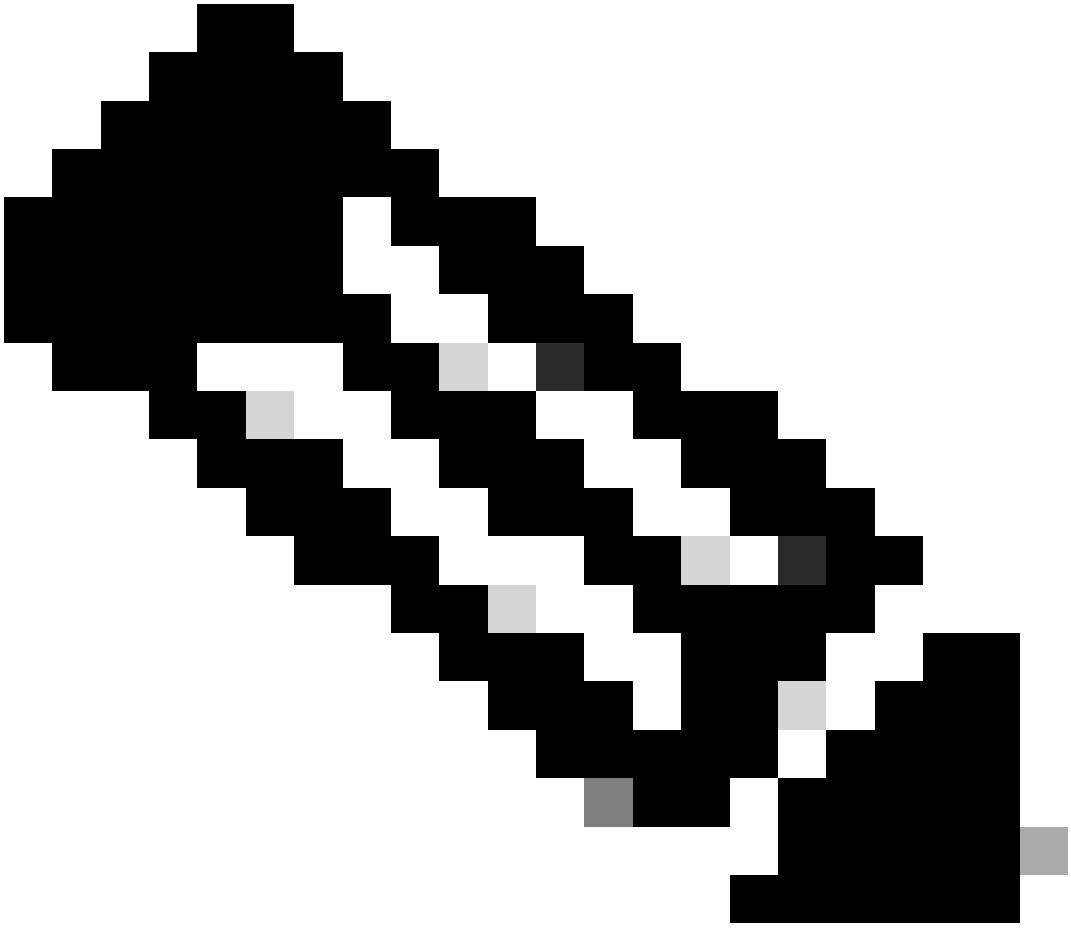
<#root>

```
device#
cconfigure terminal

device(config)#
interface Po1

device(config-if)#
```

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

- **De apparaatrolschakelaar en de** opties voor **vertrouwde** poorten helpen u een efficiënte en schaalbare beveiligde zone te ontwerpen. Wanneer deze twee parameters samen worden gebruikt, kunt u een efficiënte verdeling van de creatie van items in de bindingstabel bereiken. Hierdoor blijft de grootte van de bindingstabellen onder controle.
- **De optie met de vertrouwde** portoptie: schakelt de bewakingsfunctie uit op geconfigureerde doelen. Bindingen die via een vertrouwde poort zijn geleerd, hebben de voorkeur boven bindingen die via een andere poort zijn geleerd. Een vertrouwde poort heeft ook de voorkeur in het geval van een botsing tijdens het maken van een vermelding in de tabel.
- **De apparaatroloptie**: geeft het type apparaat aan dat naar de poort is gericht en dit kan een knooppunt of een switch zijn. Als u wilt toestaan dat er bindende vermeldingen voor een poort worden gemaakt, configureert u het apparaat als een node. Als u het maken van bindingvermeldingen wilt stoppen, configureert u het apparaat als switch.

Het configureren van het toestel als switch is geschikt voor meerdere switch set-ups, waarbij de mogelijkheid van grote apparaatvolgtafels erg groot is. Hier kan een poort die naar een apparaat kijkt (een uplink trunk-poort) worden geconfigureerd om te stoppen met het maken van bindende vermeldingen, en het verkeer dat op een dergelijke poort aankomt, kan worden vertrouwd, omdat de switch aan de andere kant van de trunk-poort apparaattracking heeft ingeschakeld en de validiteit van de bindende vermelding heeft gecontroleerd.



Opmerking: hoewel er scenario's zijn waarin het configureren van slechts één van deze opties geschikt kan zijn, is de gebruikscase vaker dat zowel de opties voor de switch van de vertrouwde poort als de apparaatrol op de poort worden geconfigureerd.

Gerelateerde informatie

- Cisco Technical Support en downloads
- Problemen oplossen met SISF op Catalyst 9000-serie Switches
- Beveiligingsconfiguratiehandleiding, Cisco IOS XE Dublin 17.12.x (Catalyst 9300 Switches)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.