Fehlerbehebung: Hohe CPU-Auslastung auf Catalyst 9000 durch SISF-Prozess

Inhalt

Einleitung

Dieses Dokument beschreibt die hohe CPU-Auslastung auf Cisco Catalyst Switches der Serie 9000, die durch den Prozess der Switch-integrierten Sicherheitsfunktionen verursacht wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegendes Verständnis der LAN-Switching-Technologie
- Kenntnis der Cisco Catalyst Switches der Serie 9000
- Vertrautheit mit Cisco IOS® XE Command Line Interface (CLI)
- Vertrautheit mit der Geräteverfolgungsfunktion

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Catalyst Switches der Serie 9000
- Software-Version: Alle Versionen

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Switch Integrated Security Features (SISF) ist ein Framework zur Optimierung der Sicherheit in Layer-2-Domänen. Es führt die IP Device Tracking (IPDT) und *bestimmte* IPv6 First-Hop Security (FHS)-Funktionen zusammen, um die Migration von einem IPv4- zu einem IPv6-Stack oder einem Dual-Stack zu vereinfachen.

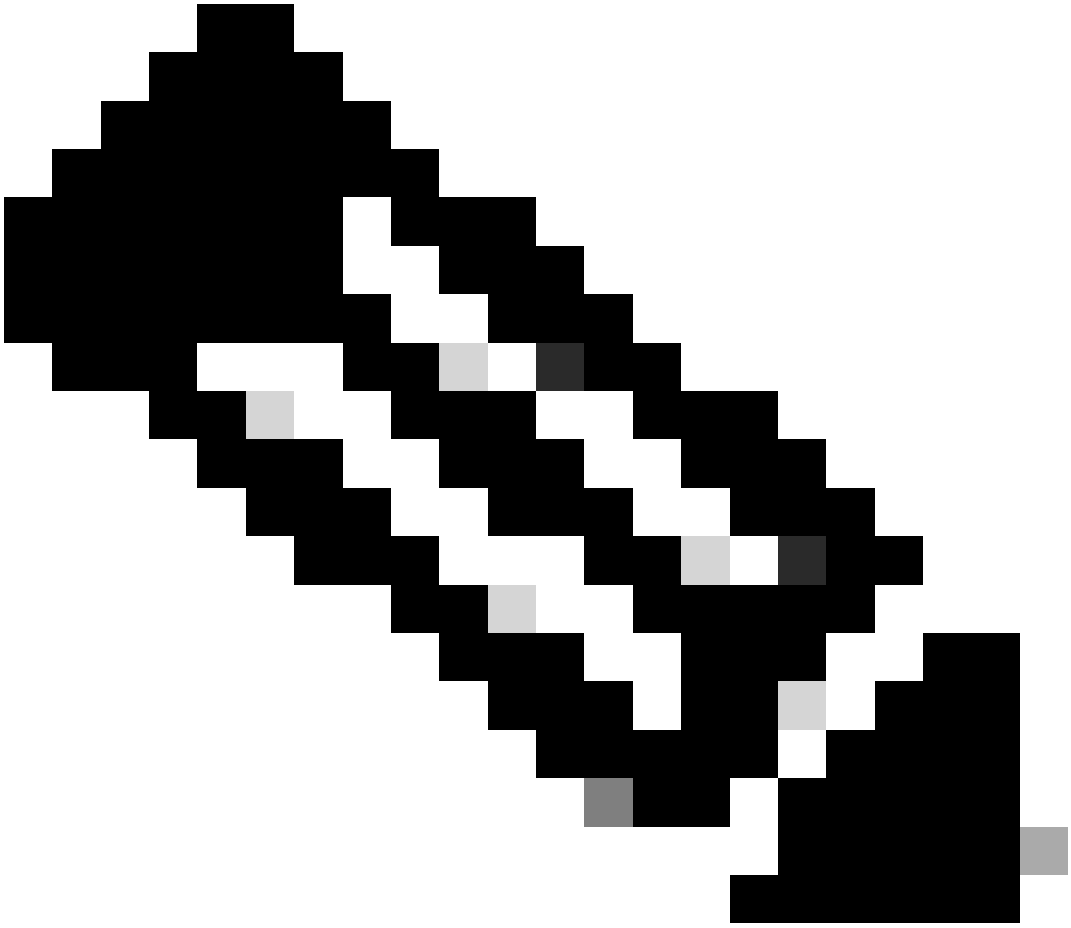
Dieser Abschnitt bietet einen Überblick über das Problem der hohen CPU-Auslastung, das auf Cisco Catalyst Switches der Serie 9000 durch den SISF-Prozess verursacht wurde. Das Problem wird durch spezifische CLI-Befehle identifiziert und bezieht sich auf die Geräteverfolgung an Trunk-Schnittstellen.

Problem

Die vom Switch gesendete Keepalive-Anfrage wird über alle Ports gesendet, wenn SISF programmgesteuert aktiviert ist. Verbundene Switches in derselben L2-Domäne senden diese Broadcasts an ihre Hosts, sodass der ursprüngliche Switch Remote-Hosts seiner Geräteverfolgungsdatenbank hinzufügt. Die zusätzlichen Hosteinträge erhöhen die Speichernutzung auf dem Gerät, und der Vorgang des Hinzufügens der Remote-Hosts erhöht die CPU-Nutzung des Geräts.

Es wird empfohlen, die programmatische Richtlinie durch Konfigurieren einer Richtlinie für den Uplink zu angeschlossenen Switches zu erweitern, um den Port als vertrauenswürdig und an einen Switch angeschlossen zu definieren.

Das in diesem Dokument behandelte Problem ist die hohe CPU-Auslastung auf Cisco Catalyst Switches der Serie 9000, die durch den SISF-Prozess verursacht wird.



Anmerkung: Beachten Sie, dass SISF-abhängige Funktionen wie DHCP-Snooping SISF aktivieren, was dieses Problem auslösen kann.

Schritt 1: CPU-Auslastung überprüfen

Um die hohe CPU-Auslastung zu ermitteln, verwenden Sie den folgenden Befehl:

<#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>
```

Phase 2: Geräteverfolgungsdatenbank überprüfen

Verwenden Sie diesen Befehl, um die Geräteverfolgungsdatenbank zu überprüfen:

<#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>
```

Es ist ersichtlich, dass die Po1-Schnittstelle mehrere MAC-Adressen verfolgt. Dies ist nicht zu erwarten, wenn dieses Gerät als Access Switch fungiert und ein Endgerät mit der Schnittstelle verbunden ist.

Sie können die Member des Port-Channels mit dem folgenden Befehl überprüfen:

Schritt 3: Etherchannels überprüfen

<#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)
```

Schritt 3: CDP-Nachbarn überprüfen

Verwenden Sie diesen Befehl, um den CDP-Nachbarn zu überprüfen:

<#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
```

Ein Catalyst Switch der Serie 9500 ist auf der anderen Seite sichtbar verbunden. Dies können weitere Zugriffsgeräte in einer Reihenschaltung oder ein Distribution/Core-Switch sein. In jedem Fall können diese Geräte keine MAC-Adressen auf Trunk-Schnittstellen verfolgen.

Lösung

Das Problem der hohen CPU-Auslastung wird durch die Geräteverfolgung verursacht. Deaktivieren Sie die Geräteverfolgung auf den Trunk-Schnittstellen.

Erstellen Sie dazu eine Richtlinie zur Geräteverfolgung, und fügen Sie diese an die Trunk-Schnittstellen an:

Schritt 1: Konfigurieren der Richtlinie für die Gerätenachverfolgung

Erstellen Sie eine Richtlinie zur Geräteverfolgung, um Trunk-Schnittstellen als vertrauenswürdige Ports zu behandeln:

```
<#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
```

Phase 2: Richtlinie an Trunk-Schnittstelle anhängen

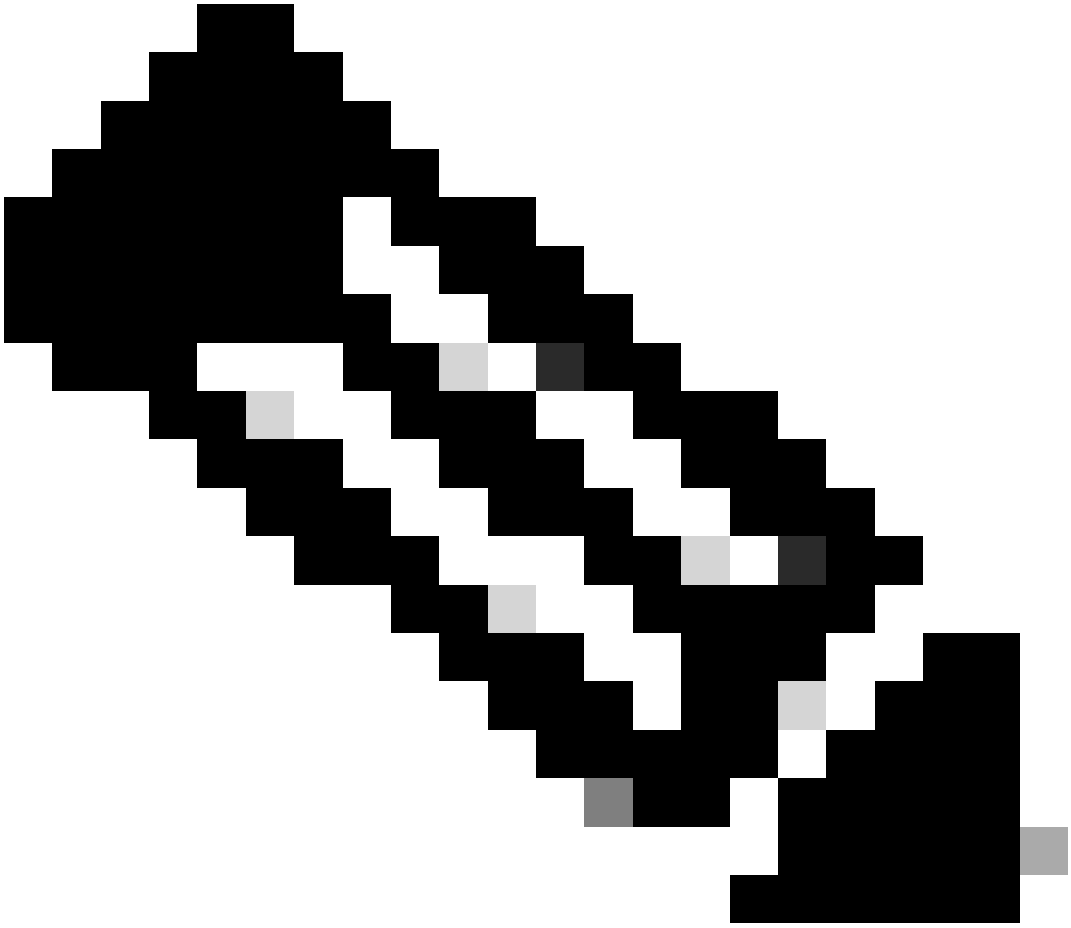
```
<#root>
device#
cconfigure terminal

device(config)#
interface Po1
```

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

- **Die** Optionen für **Geräterollen-Switchund** vertrauenswürdige Ports helfen Ihnen, eine effiziente und skalierbare sichere Zone zu erstellen. Wenn diese beiden Parameter zusammen verwendet werden, können Sie eine effiziente Verteilung der Erstellung von Einträgen in der Bindungstabelle erreichen. Dadurch bleibt die Größe der Bindungstabellen unter Kontrolle.
- **Vertrauenswürdige** Portoption: Deaktiviert die Schutzfunktion für konfigurierte Ziele. Bindungen, die über einen Trusted-Port abgerufen werden, haben Vorrang vor Bindungen, die über einen anderen Port abgerufen werden. Bei einer Kollision mit einem Eintrag in der Tabelle wird einem vertrauenswürdigen Port ebenfalls der Vorzug gegeben.
- **Die** Option **für** die Geräterolle: Zeigt den Gerätetyp an, der zum Port zeigt, und dies kann ein Knoten oder ein Switch sein. Um die Erstellung von Bindungseinträgen für einen Port zu ermöglichen, konfigurieren Sie das Gerät als Knoten. Um die Erstellung von Bindungseinträgen zu stoppen, konfigurieren Sie das Gerät als Switch.

Die Konfiguration des Geräts als Switch eignet sich für mehrere Switch-Konfigurationen, bei denen die Möglichkeit großer Geräte-Tracking-Tabellen sehr groß ist. Hier kann ein zu einem Gerät weisender Port (ein Uplink-Trunk-Port) so konfiguriert werden, dass keine Bindungseinträge mehr erstellt werden. Der an einem solchen Port ankommende Datenverkehr kann als vertrauenswürdig eingestuft werden, da die Geräteverfolgung auf dem Switch auf der anderen Seite des Trunk-Ports aktiviert ist und die Gültigkeit des Bindungseintrags überprüft wurde.



Anmerkung: Es gibt zwar Szenarien, in denen sich die Konfiguration nur einer dieser Optionen eignet, am häufigsten werden jedoch sowohl die Optionen für vertrauenswürdige Ports als auch die Optionen für Geräterollen auf dem Port konfiguriert.

Zugehörige Informationen

- Technischer Support und Downloads von Cisco
- Fehlerbehebung bei SISF auf Catalyst Switches der Serie 9000
- Leitfaden zur Sicherheitskonfiguration, Cisco IOS XE Dublin 17.12.x (Catalyst 9300 Switches)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.