SISFプロセスが原因で発生するCatalyst 9000のCPU高使用率のトラブルシューティング

内容

はじめに

このドキュメントでは、スイッチ統合セキュリティ機能(ISR)プロセスによって発生するCisco Catalyst 9000シリーズスイッチでの高いCPU使用率について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- LANスイッチングテクノロジーに関する基礎知識
- Cisco Catalyst 9000シリーズスイッチに関する知識
- Cisco IOS® XEコマンドラインインターフェイス(CLI)に精通していること
- デバイストラッキング機能に精通していること

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Catalyst 9000 シリーズ スイッチ
- ソフトウェアバージョン：すべてのバージョン

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

スイッチ統合型セキュリティ機能(SISF)は、レイヤ2ドメインのセキュリティを最適化するために開発されたフレームワークです。IPデバイストラッキング(IPDT)と特定のIPv6 First-Hop Security(FHS)機能を統合し、IPv4からIPv6スタックまたはデュアルスタックへの移行を簡素化します。

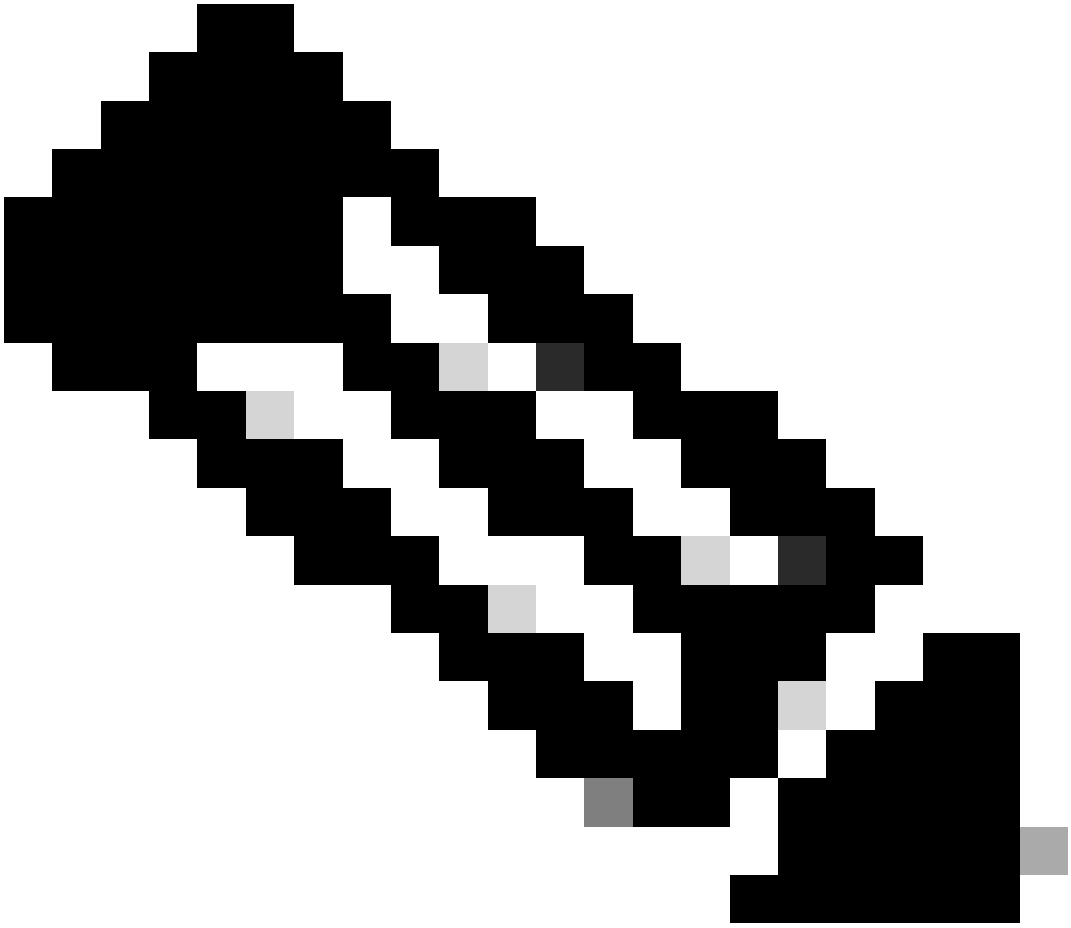
このセクションでは、Cisco Catalyst 9000シリーズスイッチで発生する、SISFプロセスによる高CPU使用率の問題の概要を説明します。この問題は、特定のCLIコマンドを通じて特定され、トランクインターフェイスでのデバイストラッキングに関連しています。

問題

スイッチから送信されたキープアライブプローブは、SISFがプログラム的に有効にされると、すべてのポートからブロードキャストされます。同じL2ドメイン内に接続されたスイッチは、これらのブロードキャストをホストに送信します。その結果、発信元スイッチはデバイストラッキングデータベースにリモートホストを追加します。ホストエントリを追加すると、デバイスのメモリ使用量が増加し、リモートホストを追加するプロセスによってデバイスのCPU使用率が増加します。

接続されたスイッチへのアップリンクにポリシーを設定して、ポートを信頼できるポートとして定義し、スイッチに接続することで、プログラム的なポリシーの範囲を設定することを推奨します。

このドキュメントで説明されている問題は、SISFプロセスによって引き起こされるCisco Catalyst 9000シリーズスイッチでの高いCPU使用率です。



注:DHCPスヌーピングなどのSISFに依存する機能によってSISFが有効になり、この問題が引き起こされる可能性があることに注意してください。

ステップ1:CPU使用率の確認

高いCPU使用率を識別するには、次のコマンドを使用します。

<#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>
```

ステップ2：デバイストラッキングデータベースの確認

デバイストラッキングデータベースを確認するには、次のコマンドを使用します。

```
<#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       234

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>
```

Po1インターフェイスで複数のMACアドレスがトラッキングされていることは明らかです。このデバイスがアクセススイッチとして機能していて、インターフェイスに接続されたエンドデバイスがある場合、これは予想されません。

ポートチャネルのメンバを確認するには、次のコマンドを使用します。

ステップ3:Etherchannelの確認

<#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)

ステップ3:CDPネイバーの確認

次のコマンドを使用して、CDPネイバーを確認します。

<#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

Catalyst 9500スイッチは、反対側に目に見える形で接続されています。これは、デイジーチェーン設定の別のアクセスデバイスや、ディストリビューション/コアスイッチである可能性があります。いずれの場合も、このデバイスはトランクインターフェイスのMACアドレスを追跡できません。

解決方法

CPU高使用率の問題は、デバイストラッキングが原因で発生します。トランクインターフェイスでデバイストラッキングを無効にします。

これを行うには、デバイストラッキングポリシーを作成し、トランクインターフェイスに適用します。

ステップ1：デバイストラッキングポリシーの設定

トランクインターフェイスを信頼できるポートとして扱うデバイストラッキングポリシーを作成します。

<#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

ステップ2：トランクインターフェイスへのポリシーの適用

<#root>

device#

cconfigure terminal

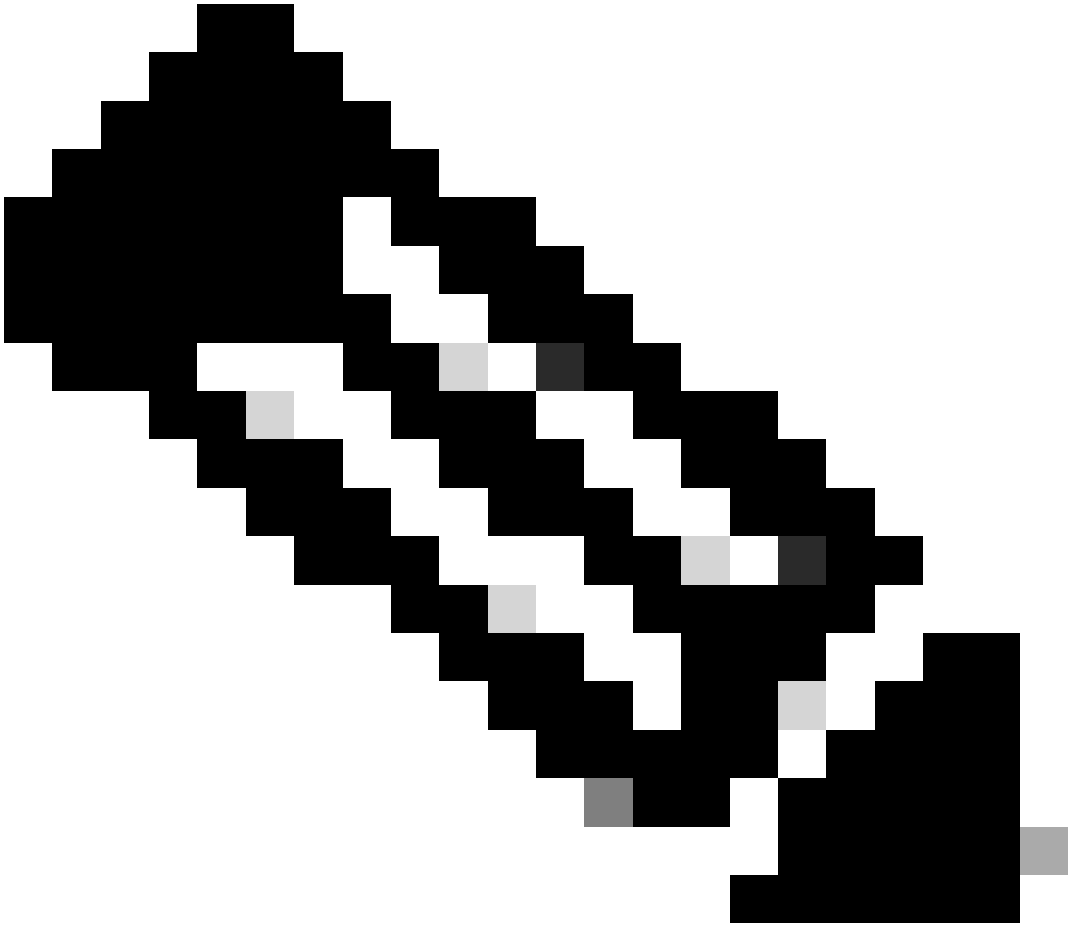
device(config)#

interface Po1

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

- デバイスロールのスイッチと信頼できるポートオプションを使用すると、効率的でスケーラブルなセキュアゾーンを設計できます。これら2つのパラメータを一緒に使用すると、バインディングテーブル内のエントリ作成を効率的に分散するのに役立ちます。これにより、バインディングテーブルのサイズが制御されます。
- **trusted-**portoption：設定されたターゲットのガード機能を無効にします。信頼できるポートを通じて学習されたバインディングは、他のポートを通じて学習されたバインディングよりも優先されます。テーブルにエントリを作成する際に衝突が発生した場合には、信頼できるポートが優先されます。
- **device-**roleoption：ポートに面しているデバイスのタイプを示します。ノードまたはスイッチを指定できます。ポートのバインディングエントリの作成を許可するには、デバイスをノードとして設定します。バインディングエントリの作成を停止するには、デバイスをスイッチとして設定します。

デバイスをスイッチとして設定することは、複数のスイッチを設定する場合に適しています。複数のスイッチを設定すると、デバイストラッキングテーブルが大きくなる可能性が非常に高くなります。ここで、デバイスに面したポート（アップリンクトランクポート）は、バインディングエントリの作成を停止するように設定できます。トランクポートの反対側のスイッチではデバイストラッキングが有効になっており、バインディングエントリの有効性がチェックされているため、このようなポートに到達するトラフィックは信頼できます。



注：これらのオプションのどちらか一方だけを設定するのが適切なシナリオもありますが、より一般的な使用例は、ポートで設定されるtrusted-portとdevice-roleの両方のスイッチオプションです。

関連情報

- シスコのテクニカルサポートとダウンロード
- Catalyst 9000シリーズスイッチのSISFのトラブルシューティング
- セキュリティ設定ガイド、Cisco IOS XE Dublin 17.12.x（Catalyst 9300スイッチ）

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。