Identificar e Solucionar Problemas de Alta Utilização de CPU no Catalyst 9000 Causados por Processo SISF

Contents

Introdução

Este documento descreve a alta utilização da CPU nos switches Cisco Catalyst 9000 Series causada pelo processo de Recursos de Segurança Integrados do Switch.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Entendimento básico da tecnologia de LAN switching
- Conhecimento dos switches Cisco Catalyst 9000 Series
- Familiaridade com a interface de linha de comando (CLI) do Cisco IOS® XE
- Familiaridade com o recurso de rastreamento de dispositivo

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Switches Cisco Catalyst 9000 Series

- Versão de software: Todas as versões

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Switch Integrated Security Features (SISF) é uma estrutura desenvolvida para otimizar a segurança em domínios de Camada 2. Ele mescla a funcionalidade IP Device Tracking (IPDT) e *determinada* segurança de primeiro salto (FHS) IPv6 para simplificar a migração da pilha de IPv4 para IPv6 ou de uma pilha dupla.

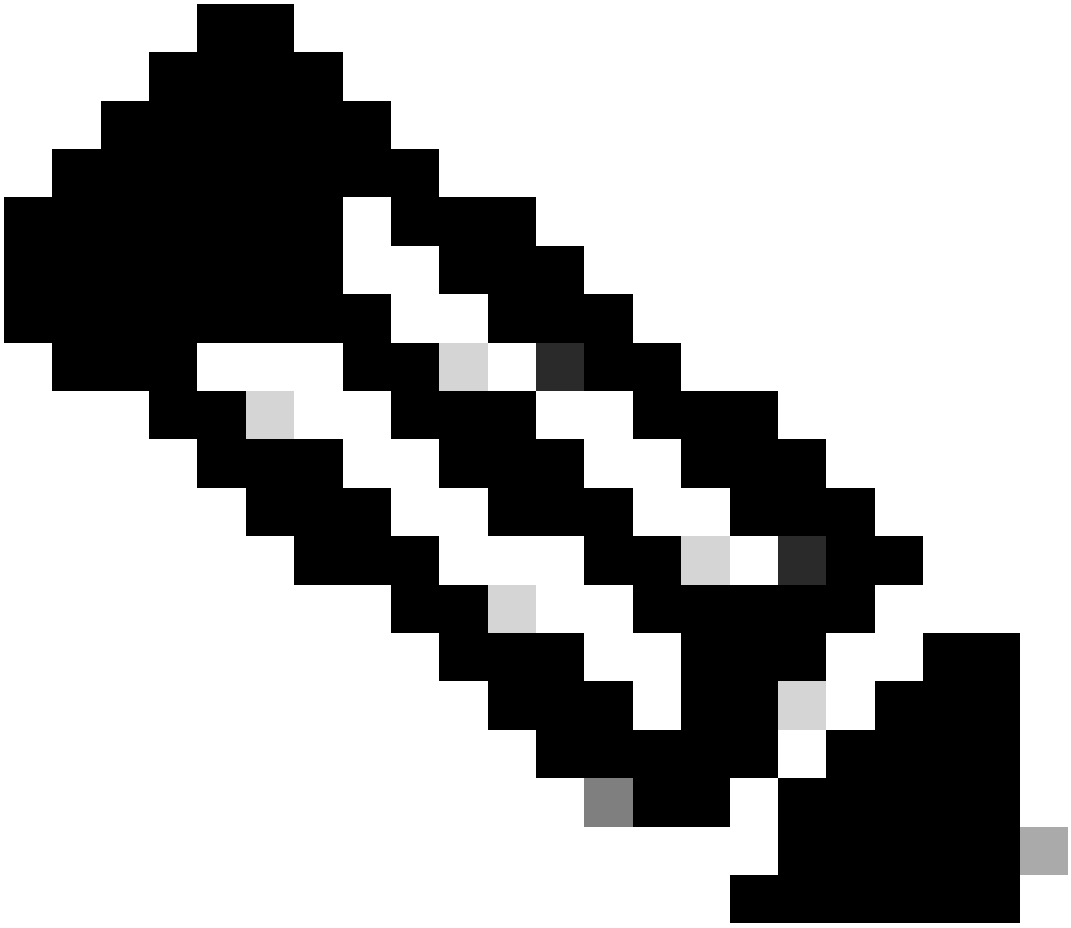
Esta seção fornece uma visão geral do problema de alta utilização da CPU observado nos Cisco Catalyst 9000 Series Switches causado pelo processo SISF. O problema é identificado através de comandos CLI específicos e está relacionado ao rastreamento de dispositivos em interfaces de tronco.

Problema

O teste keepalive enviado pelo switch é transmitido para todas as portas quando o SISF está programaticamente habilitado. Os switches conectados no mesmo domínio L2 enviam esses broadcasts para seus hosts, resultando no switch de origem adicionando hosts remotos ao seu banco de dados de rastreamento de dispositivo. As entradas adicionais do host aumentam o uso de memória no dispositivo e o processo de adição dos hosts remotos aumenta a utilização da CPU do dispositivo.

Recomenda-se definir o escopo da política programática configurando uma política no uplink para switches conectados para definir a porta como confiável e conectada a um switch.

O problema abordado neste documento é a alta utilização da CPU nos Cisco Catalyst 9000 Series Switches causada pelo processo SISF.



Note: Lembre-se de que os recursos dependentes de SISF, como o rastreamento de DHCP, habilitam o SISF, que pode disparar esse problema.

Passo 1: Verificar Utilização da CPU

Para identificar a alta utilização da CPU, use este 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>
```

Passo 2: Verificar Banco de Dados de Acompanhamento de Dispositivos

Use este comando para verificar o banco de dados de rastreamento do dispositivo:

<#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>
```

É evidente que há vários endereços MAC rastreados na interface Po1. Isso não é esperado se esse dispositivo estiver atuando como um switch de acesso e se houver um dispositivo final conectado à interface.

Você pode verificar os membros do port channel usando este comando:

Passo 3: Verificar 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)
```

Passo 3: Verificar CDP Neighbor

Use o comando this para verificar o vizinho CDP:

<#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
```

Um switch Catalyst 9500 está visivelmente conectado no outro lado. Podem ser outros dispositivos de acesso na configuração de daisy chain ou um switch de distribuição/núcleo. De qualquer forma, esses dispositivos não podem rastrear endereços MAC em interfaces de tronco.

Solução

O problema de alta utilização da CPU é causado pelo rastreamento do dispositivo. Desative o rastreamento de dispositivo nas interfaces de tronco.

Para fazer isso, crie uma política de rastreamento de dispositivo e anexe-a às interfaces de tronco:

Passo 1: Configurar Política de Rastreamento de Dispositivo

Crie uma política de rastreamento de dispositivo para tratar interfaces de tronco como portas confiáveis:

<#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
```

Passo 2: Anexar a política à interface do tronco

<#root>

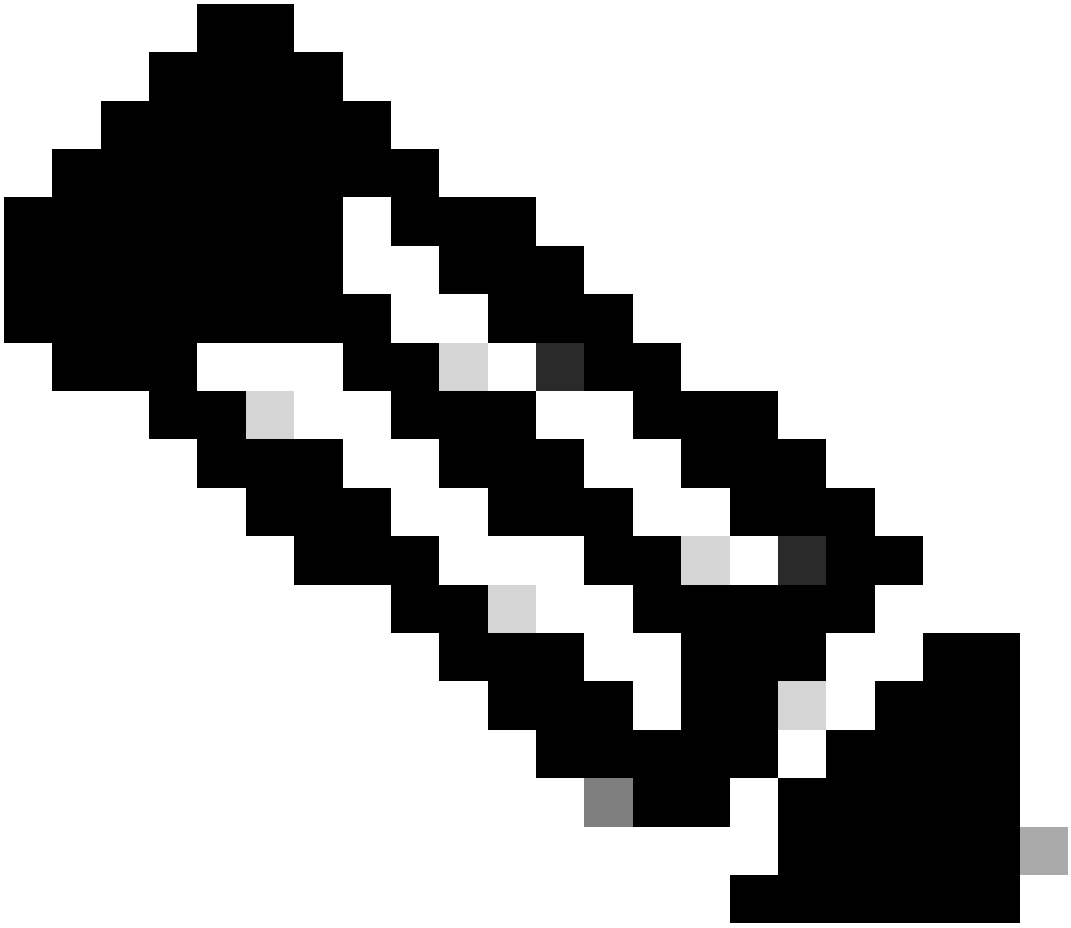
```
device#
cconfigure terminal

device(config)#
interface Po1
```

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

- **O switch de função de dispositivo e as** portas **confiáveis** ajudam a projetar uma zona segura eficiente e escalável. Quando usados juntos, esses dois parâmetros ajudam a obter uma distribuição eficiente da criação de entradas na tabela de vinculação. Isso mantém o tamanho das tabelas de vinculação sob controle.
- **A** porta **confiável**: Desabilita a função de proteção em destinos configurados. As vinculações aprendidas através de uma porta confiável têm preferência sobre as vinculações aprendidas através de qualquer outra porta. Também é dada preferência a uma porta confiável em caso de colisão ao fazer uma entrada na tabela.
- **Aopção de** função de **dispositivo**: Indica o tipo de dispositivo voltado para a porta e pode ser um nó ou um switch. Para permitir a criação de entradas de vinculação para uma porta, configure o dispositivo como um nó. Para interromper a criação de entradas de vinculação, configure o dispositivo como switch.

Configurar o dispositivo como um switch é adequado para várias configurações de switch, onde a possibilidade de grandes tabelas de rastreamento de dispositivo é muito alta. Aqui, uma porta voltada para um dispositivo (uma porta de tronco de uplink) pode ser configurada para parar de criar entradas de vinculação, e o tráfego que chega a essa porta pode ser confiável, porque o switch no outro lado da porta de tronco tem o rastreamento de dispositivo habilitado e verificou a validade da entrada de vinculação.



Note: Embora haja cenários em que a configuração de apenas uma dessas opções pode ser adequada, o caso de uso mais comum é que as opções de switch de porta confiável e de função de dispositivo sejam configuradas na porta.

Informações Relacionadas

- Suporte técnico e downloads da Cisco
- Identificar e Solucionar Problemas do SISF nos Catalyst 9000 Series Switches
- Guia de configuração de segurança, Cisco IOS XE Dublin 17.12.x (switches Catalyst 9300)

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.