

Coletores do perfilador NAC e do SERVER NAC em um manual de configuração fora da banda da camada 3

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Vista geral do perfilador NAC](#)

[Vista geral NAC](#)

[Vista geral do guia de distribuição](#)

[Configuração](#)

[Configurar o perfilador NAC na topologia da camada 3 OOB](#)

[Configurar os módulos do coletor NAC no server NAC](#)

[Configurar o interruptor de Acesso remoto para enviar o SNMP traps ao coletor NAC](#)

[Configurar o interruptor de Acesso remoto no perfilador para o recolhimento da informação de SNMP](#)

[Configurar o roteador do Acesso remoto no perfilador para o recolhimento da informação de SNMP](#)

[Configurar os coletores NAC para receber o tráfego do PERÍODO em seus switch locais](#)

[Configurar o roteador do Acesso remoto para enviar dados de Netflow ao coletor no local principal](#)

[Verificar](#)

[Troubleshooting](#)

[Procedimento de Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento descreve como executar coletores do perfilador NAC e do SERVER NAC em um desenvolvimento fora da banda da camada 3. Se você distribui o server NAC no requisito de alta disponibilidade (HA), a seguir somente um coletor é ativo e o outro está no apoio. Se você não faz o HA, você pode adicionar cada coletor no perfilador separadamente e ter ambos os server NAC executados como coletores. Este guia reflete na distribuição de servidor HA.

[Pré-requisitos](#)

[Requisitos](#)

As exigências deste guia são que você configurou seu gerente NAC, server NAC, perfilador NAC, e infraestrutura de rede de acordo com os Guias de Instalação e Configuração para cada produto.

Componentes Utilizados

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

- Gerente NAC
- Server NAC
- Perfilador NAC
- Switch de distribuição 3750
- Switch de acesso de 3750 locais remotos
- Roteador de site remoto 2800
- Roteador de distribuição 3800

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Vista geral do perfilador NAC

O Cisco NAC Profiler permite administradores de rede de distribuir e controlar eficientemente o Network Admission Control (NAC) nas redes de empreendimento da escala de variação e da complexidade com a identificação, no lugar e na determinação das capacidades de todos os valores-limite de rede anexa, apesar do tipo de dispositivo, a fim assegurar e manter o acesso de rede apropriado. O Cisco NAC Profiler é um sistema agentless que descubre, catálogos, e perfila todos os valores-limite conectados a uma rede.

Vista geral NAC

O dispositivo do Cisco Network Admission Control (NAC), que é sabido igualmente como o acesso limpo de Cisco, é solução um controle de admissão e de uma aplicação poderosos, fáceis de usar da conformidade. Com recursos de segurança detalhados, em-faixa ou opções de distribuição fora da banda, ferramentas da autenticação de usuário, e controles da largura de banda e do filtragem de tráfego, a ferramenta NAC de Cisco é uma solução completa para controlar e fixar redes. Como o ponto central do gerenciamento de acesso para sua rede, a ferramenta NAC de Cisco deixa-o executar a Segurança, o acesso, e as políticas da conformidade em um lugar em vez da necessidade de propagar as políticas durante todo a rede em muitos dispositivos.

Vista geral do guia de distribuição

Em figura 1, há um desenvolvimento simples do local remoto com os server centrais HA NAC que atue como o ponto da aplicação para dispositivos fora da banda da camada 3. O perfilador NAC e

o gerente NAC sentam-se na mesma rede de gerenciamento e enviam-se e recebem-se a informação dos server e dos coletores. Há igualmente um coletor autônomo que agarre a informação DHCP essencial sobre os dispositivos através do PERÍODO no centro de dados ou na camada central. Há diversas maneiras de descobrir que os pontos finais remotos e este guia podem o ajudar em seu desenvolvimento. Não se pretende ser um guia imperativo mas mostra-se lhe como cada módulo nos coletores pode ser usado e como os dados do valor-limite são considerados pelo perfilador para fazer as decisões de perfilamento para você.

Uma lista das ferramentas imperativas e opcionais que os coletores do server NAC usam é fornecida.

Módulos imperativos do coletor

NetTrap — Este módulo escuta o SNMP traps enviado pelo Switches para a notificação novo-MAC ou notificações Up/Down do link. Este módulo envia todos os endereços novos MAC ao perfilador para perfilar. Esta característica é definida pelo interruptor na linha de comando configuration do servidor snmp no ^{® do} Cisco IOS.

NetMap — Este módulo senta-se no coletor e é-se responsável para fazer o polling snmp dos dispositivos no filial remota em intervalos programados. No diagrama de figura 1, o coletor SNMP CAS1a vota o switch remoto e o roteador para a informação de MIB específica com acesso de leitura ao interruptor. Esta votação fornece coisas como o endereço MAC à informação de porta, relações, estado do link, informação do dot1x, informação de sistema e assim por diante.

NetWatch (PERÍODO) — O módulo de NetWatch pode escutar em uma porta span de um interruptor e enviar a informação de tráfego ingerida de volta ao perfilador. Um server NAC exige uma interface adicional em cada SERVER NAC recolher dados. Isto é essencial porque o perfilador é baseado primeiramente na informação DHCP passada dispositivos e por alguma outra harmonização do tráfego de aplicativo.

Módulos opcionais do coletor

Você pode usar o PERÍODO ou o Netflow. É até o desenvolvimento e os requisitos de cliente mas um é recomendado somente em um servidor devido NAC à quantidade de tráfego que é enviada aos módulos do coletor e às outras funcionalidades NAC que o server NAC tem que executar. Você igualmente perde umas partes informativas mais vitais sobre dispositivos com o Netflow como a informação do vendedor DHCP, destinos URL, informação do cliente web, informação do servidor de Web e assim por diante.

NetRelay — (Netflow) é configurado em cada roteador na pela base da relação e o destino é o endereço IP de gerenciamento do SERVER NAC. Um agente do Netflow senta-se no SERVER NAC e analisa-se gramaticalmente a informação de Netflow baseada em suas regras e redes de tráfego configuradas no perfilador.

NetInquiry — Este é um mecanismo passivo e ativo baseado em suas coisas como portas aberta TCP. Por exemplo o SERVER NAC faz um SYN/ACK e deixa cair então a conexão a fim votar uma escala ou umas escalas da sub-rede particular para portas TCP abertas. Se há uma resposta, envia a informação ao perfilador com o endereço IP de Um ou Mais Servidores Cisco ICM NT e a porta TCP votados.

Nota: Para NetInquiry, adicionar somente as sub-redes ou os anfitriões específicos que não podem ser alcançados ou considerado com Netflow ou NetWatch. NetInquiry pode sobrecarregar

seu server NAC com o processamento extra e os recursos do hardware como a memória e utilização CPU se não configurada corretamente. Use esta característica como um último recurso.

Nota: Se você tem um coletor autônomo você pode permitir o Netflow e o PERÍODO no mesmo dispositivo mas certificar-se não ao oversubscribe do coletor.

Figura 1

Configuração

Configurar o perfilador NAC na topologia da camada 3 OOB

- Os server NAC precisam de ser configurados com a instalação normal NAC HA.
- O coletor NAC utiliza o endereço IP de Um ou Mais Servidores Cisco ICM NT virtual do server NAC para comunicar-se com o perfilador.
- O par do coletor HA NAC é adicionado como uma única entrada no perfilador e comunica-se ao endereço IP de Um ou Mais Servidores Cisco ICM NT virtual de CAS.

Figura 2

Instalação da configuração

Conclua estes passos:

1. O perfilador precisa uma *conexão de cliente* para os coletores novos NAC.
2. O perfilador precisa uma *conexão de servidor* para o dispositivo autônomo que se senta perto da distribuição|centro de dados|camada dos serviços no diagrama da rede.
3. Escolha os **módulos da configuração > do perfilador NAC – Aliste os módulos do perfilador NAC** e clique então a aba do **server**. O rolo à parte inferior da página e o clique **adicionam a conexão**. **Figura 3**
4. Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do serviço e a informação de chave secreta do coletor e do clique **HA adiciona a conexão**. **Figura 4**
5. O clique **adiciona a conexão** outra vez. **Figura 5** **Figura 6**
6. Incorpore o **endereço IP de Um ou Mais Servidores Cisco ICM NT** a fim configurar uma *conexão de servidor a* que o coletor autônomo conecta.
7. O clique **edita a conexão** quando você é feito a fim receber de volta à página da configuração do servidor.
8. **Server da atualização do** clique na página da configuração do servidor. **Figura 7**

Adicionar dois coletores novos ao perfilador. Conclua estes passos:

1. Escolha o **coletor do > Add dos módulos da configuração > do Profiler NAC**. **Figura 8**
2. Adicionar um nome novo do coletor para os pares do server HA NAC. Este pode ser qualquer coisa que você quer mas deve combinar na configuração do coletor. Nome do coletor — CAS-OOB-Pair1 Endereço IP 192.168.97.10 (endereço virtual do server NAC) Conexão — Deixe-a como **NENHUNS** por agora. Você pode mudar este mais tarde a uma conexão de servidor que seja escute dentro modo.
3. O clique **adiciona o botão do coletor**. **Figura 9**
4. Configurar seus módulos de serviço do coletor. Deixe NetMap e NetTrap sozinhos. **Figura 10**
5. Adicionar uma relação de NetWatch (eth3), que seja conectada a uma porta span no switch

de distribuição.**Figura 11**

6. Adicionar um bloco da sub-rede para o módulo de NetInquiry a fim escutar o tráfego interessante que vem das redes de acesso. Seja específico nas redes a respeito não do imposto o server NAC desnecessariamente. Nesta instalação de laboratório, pode ser o espaço privado inteiro de 192.168.0.0.**Figura 12** **Nota:** Deixe o ping sweep e a coleção DNS desabilitados. Use isto como um último recurso. O ping sweep e a coleção DNS provocam sibilos e nslookups na escala do sub-redes IP que você põe na seção dos blocos da rede. Isto não é recomendado e é usado raramente.
7. Configurar o remetente para escutar no endereço IP 192.168.97.10 (VIP) e na porta TCP 31416. Isto permite que o coletor atue como um server e escute uma conexão do perfilador à porta TCP específica. Isto reflete em etapas primeiras para a configuração do servidor.
8. Permita o Netflow para os pares do coletor. (Opcional)Você pode fazer este aqui desde que o Netflow é passado do roteador remoto devido a nenhum coletor remoto.
9. Incorpore os blocos do endereço IP de Um ou Mais Servidores Cisco ICM NT para o local remoto como descritos. Neste exemplo, o espaço privado inteiro de 192.168.0.0 é usado.**Figura 13**
10. O clique **salvar o coletor** a fim salvar sua configuração.

Adicionar o coletor autônomo adicional ao perfilador

Conclua estes passos:

1. O clique **adiciona o coletor**.**Figura 14**
2. O nome do coletor pode ser qualquer coisa que você quer. Neste exemplo, é CAS2.
3. O endereço IP de Um ou Mais Servidores Cisco ICM NT é próprio do remetente. O endereço IP de Um ou Mais Servidores Cisco ICM NT do eth0 é para o Gerenciamento.Neste exemplo, é 192.168.97.12.A conexão deve ser o endereço IP de Um ou Mais Servidores Cisco ICM NT do perfilador. Neste caso, é 192.168.96.21.
4. O clique **adiciona o coletor**.**Figura 15**
5. Após isto, você é trazido à página de configuração do coletor. Termine as etapas 5 – 9 na seção anterior. Isto permite que você altere e adicione os endereços IP exclusivos e os ajustes de configuração do coletor autônomo.
6. Um ajuste original para o coletor autônomo é a capacidade para adicionar interfaces múltiplas à configuração de NetWatch. Aqui você pode adicionar diversas relações assim que você pode ver o tráfego para o DHCP, o DNS, e a Telefonia IP dos pontos finais remotos.
7. Configurar as relações de NetWatch para sua instalação. Neste exemplo, três relações foram adicionadas PARA MEDIR o tráfego no coletor autônomo.**Figura 16**
8. **Nota:** Escolha a **configuração > aplicam mudanças > módulos da atualização** a fim salvar seus ajustes.

[Configurar os módulos do coletor NAC no server NAC](#)

Nota: Esta configuração precisa de ser executada em todos os coletores.

Esta configuração permite que o perfilador e os coletores comuniquem e estabeleçam conexões seguras para obter informações sobre dos dispositivos para começar fluir. Conclua estes passos:

1. SSH ou console ao coletor e início de uma sessão como a **raiz do console** ou da **baliza da sessão SSH**.
2. Inscreva o **comando config do coletor do serviço**.
3. Seja executado através do script de configuração a fim setup a parcela do coletor

NAC.Exemplo do coletor HAO coletor setup como um tipo de *conexão de servidor*.

```
[root@cas1 ~]#service collector config Enable the NAC Collector (y/n) [y]: Configure NAC Collector (y/n) [y]: Enter the name for this remote collector. Please note that if this collector exists on a HA pair that this name must match its pair's name for proper operation. (24 char max) [cas1]: CAS-OOB-Pair1 Network configuration to connect to a NAC Profiler Server Connection type (server/client) [server]: Listen on IP [192.168.97.10]: Você é pedido para incorporar o endereço IP de Um ou Mais Servidores Cisco ICM NT dos NP. Isto é necessário para configurar o Access Control List usado por este coletor. Se os NP são parte de uns pares HA, a seguir você deve incluir o endereço IP real do cada NP independentes e o IP virtual para assegurar a conectividade apropriada no caso do Failover. Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do perfilador NAC.(Finish by typing 'done') [127.0.0.1]: 192.168.96.20 (Real IP address of NAC Server1) Enter the IP address(es) of the NAC Profiler. (Finish by typing 'done') [192.168.96.20]: 192.168.96.21 (Virtual IP of NAC Server) Enter the IP address(es) of the NAC Profiler. (Finish by typing 'done') [done]: 192.168.96.22 (Real IP of NAC Server2) Enter the IP address(es) of the NAC Profiler. (Finish by typing 'done') [done]: done Port number [31416]: Encryption type (AES, blowfish, none) [none]: AES Shared secret []: cisco123 •Configured CAS-OOB-Pair1-fw •Configured CAS-OOB-Pair1-nm •Configured CAS-OOB-Pair1-nt •Configured CAS-OOB-Pair1-nw •Configured CAS-OOB-Pair1-ni •Configured CAS-OOB-Pair1-nr
```

NAC Collector has been configured.

4. Enfie os serviços do coletor.[root@cas1 ~]#service collector start **Esteja o exemplo sozinho do coletor**
- ```
[root@cas2 ~]#service collector config Enable the NAC Collector (y/n) [y]: Configure NAC Collector (y/n) [y]: Enter the name for this remote collector. Please note that if this collector exists on a HA pair that this name must match its pair's name for proper operation. (24 char max) [cas2]: Network configuration to connect to a NAC Profiler Server Connection type (server/client) [client]: Connect to IP [192.168.96.21]: Port number [31416]: Encryption type (AES, blowfish, none) [none]: Shared secret []: -- Configured cas2-fw -- Configured cas2-nm -- Configured cas2-nt -- Configured cas2-nw -- Configured cas2-ni -- Configured cas2-nr NAC Collector has been configured. [root@cas2 ~]#service collector start
```

## [Configurar o interruptor de Acesso remoto para enviar o SNMP traps ao coletor NAC](#)

Esta configuração permite que o perfilador receba dinamicamente todos os dispositivos novos que conectam a um switchport através das armadilhas da MAC-notificação. Isto é especialmente importante desde que na topologia há um telefone IP e um PC conectados à mesma porta.

Console ou telnet no interruptor (nac-3750-access#).

```
snmp-server community cleanaccess RW snmp-server community profiler RO snmp-server enable traps mac-notification snmp-server host 192.168.96.10 version 2c cleanaccess snmp-server host 192.168.97.10 version 1 profiler
```

## [Configurar o interruptor de Acesso remoto no perfilador para o recolhimento da informação de SNMP](#)

Conclua estes passos:

1. Escolha o **Profiler GUI > dispositivo do > Add da configuração > dos dispositivos de rede.Figura 18**
2. Adicionar o nome de host e o endereço IP de gerenciamento do interruptor.
3. Igualmente entre nas cordas de leitura apenas SNMP configuradas no interruptor. Certifique-se escolher o módulo do mapeamento do coletor NAC assim que o coletor é escolhido à votação SNMP o switch de acesso cada hora e dianteiro a informação ao perfilador.
4. O clique **adiciona o dispositivo** e **aplica mudanças** a fim atualizar os módulos do painel esquerdo do GUI.Figura 19

## [Configurar o roteador do Acesso remoto no perfilador para o recolhimento da informação de SNMP](#)

Isto permite o endereço IP de Um ou Mais Servidores Cisco ICM NT da camada 3 ao MAC que liga no base de dados do perfilador.

1. Escolha o **Profiler GUI > dispositivo do > Add da configuração > dos dispositivos de rede.Figura 20** Veja figura 21.
2. Adicionar o nome de host e o endereço IP de gerenciamento do roteador.
3. Igualmente entre nas cordas de leitura apenas SNMP configuradas no roteador. Certifique-se escolher o módulo do mapeamento do coletor NAC assim que o coletor é escolhido à votação SNMP o switch de acesso cada hora e dianteiro a informação ao perfilador.
4. O clique **adiciona o dispositivo** e **aplica mudanças** a fim atualizar os módulos do painel esquerdo do GUI.Figura 21

## [Configurar os coletores NAC para receber o tráfego do PERÍODO em seus switch locais](#)

**Nota:** Isto permite que o módulo de NetWatch comece escutar o tráfego na rede e a informação dianteira ao perfilador. Certifique-se que você não faz oversubscribe a relação do coletor NAC. Tem uma limitação de 1 GB/sec. Você pode fonte as relações ou os vlans do interruptor, e aquele depende de seus modelo de switch e versão de código.

**Nota:** Minimamente você quer ver as requisições DHCP e as ofertas dos valores-limite em seus switch de acesso. Se isto não é possível, tente adicionar um coletor NAC ou perto dos servidores DHCP em sua rede. Isto é feito neste manual de configuração.

Conclua estes passos:

1. Configurar uma sessão de monitor no switch de distribuição #1 para o local remoto entrante e o tráfego de saída:

```
monitor session 1 source interface F0/0
monitor session 1 destination interface Gi1/0/44
```
2. Configurar uma sessão de monitor duplicada no switch de distribuição #2 para o local remoto entrante e o tráfego de saída:

```
monitor session 1 source interface F0/0
monitor session 1 destination interface Gi1/0/44
```

3. Configurar uma outra sessão de monitor para o coletor autônomo. Este exemplo monitora diversas relações conectadas a um switch central que são da importância. Estes são o DHCP, o DNS, e os servidores do CallManager da Cisco para esta instalação de laboratório.

```
monitor session 1 source interface G1/0/7-9
monitor session 1 destination interface G1/0/48
```

## [Configurar o roteador do Acesso remoto para enviar dados de Netflow ao coletor no local principal](#)

Conclua estes passos:

1. Telnet ao roteador remoto.

2. Permita o Netflow globalmente.

```
ip flow-export version 5
```

```
ip flow-export destination 192.168.97.12 2055
```

**Nota:** Os coletores escutam na porta 2055 UDP o Netflow. O endereço IP de Um ou Mais Servidores Cisco ICM NT para enviar o Netflow é sempre os coletores endereço IP de gerenciamento.

3. Permita o Netflow nas relações.

```
interface FastEthernet0/1
```

```
ip address 192.168.121.1 255.255.255.0
ip flow ingress
ip route-cache flow
```

## [Verificar](#)

Veja a seção do [procedimento de Troubleshooting](#) a fim confirmar que sua configuração trabalha corretamente.

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

## [Troubleshooting](#)

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

**Nota:** Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

## [Procedimento de Troubleshooting](#)

Termine estas etapas a fim pesquisar defeitos sua configuração.

1. Certifique-se que o perfilador e o coletor se estão comunicando e se estão sendo executado. Se não são, a seguir você não vê nenhuma informação sobre dispositivos em sua rede. Se há umas edições, não continue até que todos os módulos do coletor e o server *sejam* executado. No perfilador, escolha os **módulos da configuração > do perfilador NAC > os módulos do perfilador da lista NAC**.
2. Verifique que o switch de acesso envia armadilhas da notificação novo-MAC ao coletor. Seja cuidadoso quando você permite debug e você deve conhecer seus perigos.

```
nac-3750-
access#debug snmp packet nac-3750-access#debug snmp header
```



3. Verifique que o coletor tem o SNMP votado o interruptor: Olhe a última coluna da varredura.
4. Debugar o SNMP outra vez no interruptor.
5. Do perfilador, escolha a **configuração > os dispositivos de rede**. Escolha **alistar dispositivos de rede** e escolher então o **dispositivo**.

6. Clique a **pergunta**.

7. Olhe o resultado do debug no interruptor para o coletor ao SNMP votar o interruptor:
 

```
*Mar 30 23:09:24: SNMP: Packet received via UDP from 192.168.97.11 on Vlan100 *Mar 30 23:09:24:
SNMP: Get-next request, reqid 1347517983, errstat 0, erridx 0 ifType = NULL TYPE/VALUE *Mar
30 23:09:24: SNMP: Response, reqid 1347517983, errstat 0, erridx 0 ifType.1 = 53 *Mar 30
23:09:24: SNMP: Packet sent via UDP to 192.168.97.11
```

8. Obstrua dentro seu telefone IP no interruptor ou emita o comando no shut então fechado na

```
relação:15w4d: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/4, changed state to down
15w4d: %ILPOWER-5-POWER_GRANTED: Interface Gil/0/4: Power granted
15w4d: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/4, changed state to up
15w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed state
to up
15w4d: SNMP: Queuing packet to 192.168.97.12
15w4d: Outgoing SNMP packet
15w4d: v2c packet
15w4d: community string: profiler
15w4d: SNMP: V2 Trap, reqid 14430, errstat 0, erridx 0
 sysUpTime.0 = 949829672
 snmpTrapOID.0 = cmnMacChangedNotification
 cmnHistMacChangedMsg.0 =
01 00 79 00 07 50 C6 82 27 00 04 00
```

9. Verifique que o coletor envia um pedido novo da armadilha para o MAC address

```
recebido:15w4d: SNMP: Packet received via UDP from 192.168.97.11 on Vlan120
15w4d: SNMP: Get request, reqid 1576567642, errstat 0, erridx 0
 system.1.0 = NULL TYPE/VALUE
 ifIndex.10104 = NULL TYPE/VALUE
 ifDescr.10104 = NULL TYPE/VALUE
 ifType.10104 = NULL TYPE/VALUE
 ifSpeed.10104 = NULL TYPE/VALUE
 ifPhysAddress.10104 = NULL TYPE/VALUE
 ifAdminStatus.10104 = NULL TYPE/VALUE
 ifOperStatus.10104 = NULL TYPE/VALUE
 ifName.10104 = NULL TYPE/VALUE
 dot1xAuthAuthControlledPortStatus.10104 = NULL TYPE/VALUE
 dot1xAuthAuthControlledPortControl.10104 = NULL TYPE/VALUE
 paeMIBObjects.2.4.1.9.10104 = NULL TYPE/VALUE
```

```
-----snip -----
ifIndex.10104 = 10104
ifDescr.10104 = GigabitEthernet1/0/4
ifType.10104 = 6
ifSpeed.10104 = 100000000
ifPhysAddress.10104 = 00 14 A8 2E A5 04
ifAdminStatus.10104 = 1
ifOperStatus.10104 = 1
ifName.10104 = Gil/0/4
dot1xAuthAuthControlledPortStatus.10104 = 1
dot1xAuthAuthControlledPortControl.10104 = 3
15w4d: SNMP: Packet sent via UDP to 192.168.97.11
```

10. Verifique que o perfilador recebeu o MAC address novo do telefone IP do coletor: Escolha o **console > a opinião do valor-limite/controle valores-limite > valores-limite do indicador por portas do dispositivo > ungrouped > tabela dos dispositivos** e escolha então seu interruptor.
11. Verifique que trabalhos do PERÍODO no interruptor e no coletor está recebendo o

```
tráfego.SSH to the NAC Profiler :
Type : tcpdump -i eth3
```

```
16:54:36.432218 IP cas2.nacelab2.cisco.com.9308 > elab2-dns-
```

dhcp.nacelab2.cisco.com.domain: 48871+ PTR? 68.39.168.192.in-addr.arpa. (44) Olhe a saída na tela. Se você é referido sobre a quantidade de saída, você pode conduzir a saída a um arquivo no coletor NAC. Veja as páginas man em Linux em como executar isto.

12. Verifique para ver se o tráfego DHCP sobre o valor-limite do telefone IP foi considerado através da porta span e enviou até o perfilador. Escolha o **console > a opinião do valor-limite/controle valores-limite > valores-limite do indicador por portas do dispositivo > ungrouped > tabela dos dispositivos** e escolha então seu interruptor. Escolha então o **MAC address** de seus dispositivos. Clique **dados de perfil da vista**. Você deve ver a informação da classe de fornecedor DHCP dos dispositivos capturados do tráfego NetWatch/SPAN no coletor. Esta informação pode vir do servidor DHCP ou da oferta de DHCP na porta span de volta ao cliente, que depende de seus roteamento e ambiente.

13. Verifique que o Netflow está sendo passado do roteador remoto à interface de

```
gerenciamento do coletor.NAC-2800-Remote#show ip flow export Flow export v5 is enabled
for main cache Exporting flows to 192.168.97.12 (2055) Exporting using source IP address
10.0.0.2 Version 5 flow records 2602429 flows exported in 554968 udp datagrams 0 flows
failed due to lack of export packet NAC-2800-Remote#show ip flow top 10 aggregate source-
```

```
address Há quatro oradores superiores:IPV4 SRC-ADDR bytes pkts flows
=====
192.168.122.60 44 1 1
192.168.122.59 88 2 2
192.168.121.90 367 3 3
10.0.0.1 19320 322 1
```

14. Verifique que o perfilador dos coletores recebe o Netflow. Escolha seu IP do MAC remoto ou do valor-limite e olhe os dados perfilados: Escolha o **console > a opinião do valor-limite/controle valores-limite > valores-limite do indicador por portas do dispositivo > ungrouped > tabela dos dispositivos** e escolha então seu interruptor. Escolha então o **MAC address** de seus dispositivos. Clique **dados de perfil da vista**. Na saída, você vê o tráfego do destino a IP 192.168.70.50 e porta do destino 2000. Este é o endereço IP de Um ou Mais Servidores Cisco ICM NT do CallManager da Cisco e a porta do destino 2000 é usada para o tráfego de controle SCCP.

## [Informações Relacionadas](#)

- [Suporte Técnico e Documentação - Cisco Systems](#)