Despliegue el Profiler del NAC en un NAC fuera de banda existente

Contenido

Introducción

Este Guía de despliegue describe cómo implementar el servidor del Cisco NAC Profiler y los colectores del Cisco NAC Profiler (situados en el servidor de acceso limpio del dispositivo NAC de Cisco) en (OOB) un despliegue fuera de banda del campus. Este documento describe cómo el mejor despliega el Cisco NAC Profiler en una existencia despliegue OOB de gran disponibilidad del NAC. Se piensa para ayudarle a entender las funciones básicas y la topología de una solución del Cisco NAC Profiler integrada con el dispositivo NAC de Cisco. También le ayuda a entender cómo la información del punto final sobre todos los dispositivos del NAC-menos se envía de los colectores al servidor del Profiler. La meta de la solución es perfilar los puntos finales y agregarlos a la lista de filtros del dispositivo del Access Manager limpio del dispositivo NAC de Cisco (CAM) para aplicar la directiva apropiada.

prerrequisitos

Requisitos

Usted debe primero configurar servidor del NAC de su de Cisco del NAC administrador, de Cisco, y Cisco NAC Profiler de acuerdo con las guías de instalación y configuración para cada producto.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Administrador del NAC (IP del servicio de 192.168.96.10 HA)
- Servidor del NAC (IP del servicio de 192.168.97.10 HA)
- Profiler del NAC (192.168.96.21)
- Switch de acceso 3560 (192.168.100.35)
- Switch de distribución 3750 (192.168.97.1)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Descripción del Profiler del NAC

Administradores de la red de los permisos del Cisco NAC Profiler para desplegar y para manejar eficientemente el Network Admission Control (NAC) en las redes para empresas de la diversa escala y de la complejidad por la identificación, la localización, y la determinación de las capacidades de todos los puntos finales de red conectada, sin importar el tipo de dispositivo, para asegurar y mantener el acceso a la red apropiado. El Cisco NAC Profiler es un sistema que descubre, catálogos, y perfila todos los puntos finales conectados con una red con la tarea específica de perfilar los puntos finales del agente-menos.

Descripción del NAC

El dispositivo del Cisco Network Admission Control (NAC) (también conocido como acceso limpio de Cisco) es solución un control de admisión y de una aplicación potentes, fáciles de usar de la conformidad. Con las funciones de seguridad completas, la en-banda o las Opciones de instrumentación fuera de banda, las herramientas de la autenticación de usuario, y los controles del ancho de banda y del filtrado de tráfico, el dispositivo NAC de Cisco es una solución completa para controlar y para asegurar las redes. Como la punta central de la Administración de acceso para su red, el dispositivo NAC de Cisco le deja implementar la Seguridad, el acceso, y las directivas de la conformidad en un lugar en vez de tener que propagar las directivas en la red en muchos dispositivos.

Configurar

Descripción de la guía de configuración

En esta sección encontrará la información para configurar las funciones descritas en este documento.

El diagrama en el cuadro 1 muestra un despliegue del campus de la capa básica 2 con los servidores de gran disponibilidad del NAC (HA) a través de los switches de distribución. El servidor del Profiler y el administrador del NAC pueden sentarse en la misma red de administración y enviar y recibir la información de los servidores y de los colectores del NAC. Hay varias maneras que el Cisco NAC Profiler puede descubrir los puntos finales remotos del NON-NAC, y esta guía describe el más común y métodos recomendados. Esta guía de configuración describe cómo lograr éstos:

- Agregue la comunicación SNMP a y desde el switch de acceso a los colectores del NAC.
- Configure un puerto SPAN en los switches de distribución para capturar todo el tráfico de los dispositivos de la capa de acceso, específicamente tráfico del DHCP de los puntos finales, puesto que estamos los más interesados del atributo de la información de la clase del vendedor del DHCP sobre los puntos finales.
- Configure la comunicación del servidor y del colector del Cisco NAC Profiler por consiguiente para recibir toda la información recopilada por los colectores.

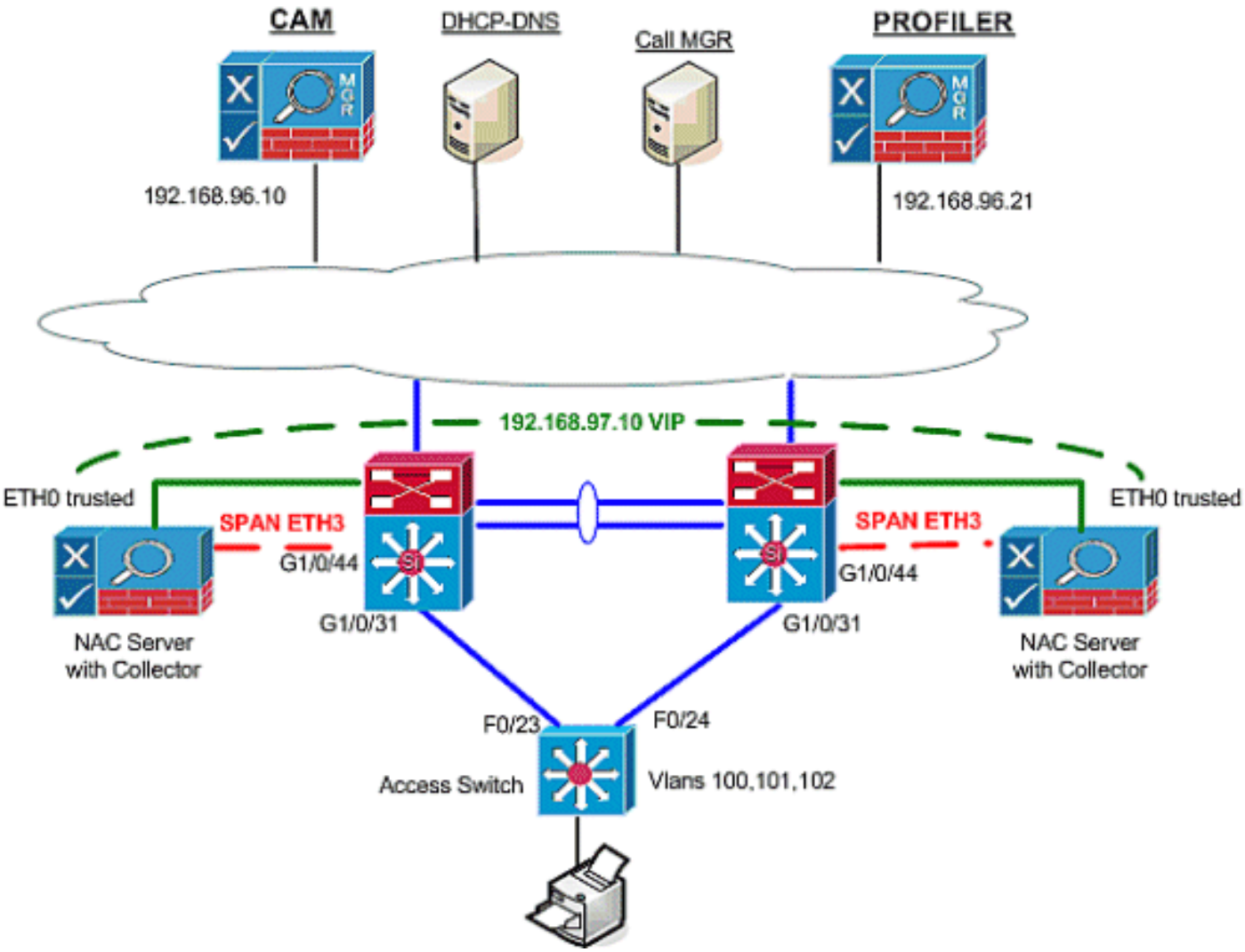
Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Figura 1: OOB despliegue del dispositivo NAC de Cisco con el Cisco NAC Profiler

OOB NAC Deployment with Profiler



Configuraciones

Este documento utiliza estas configuraciones para configurar el Profiler y los colectores del NAC en una solución fuera de banda:

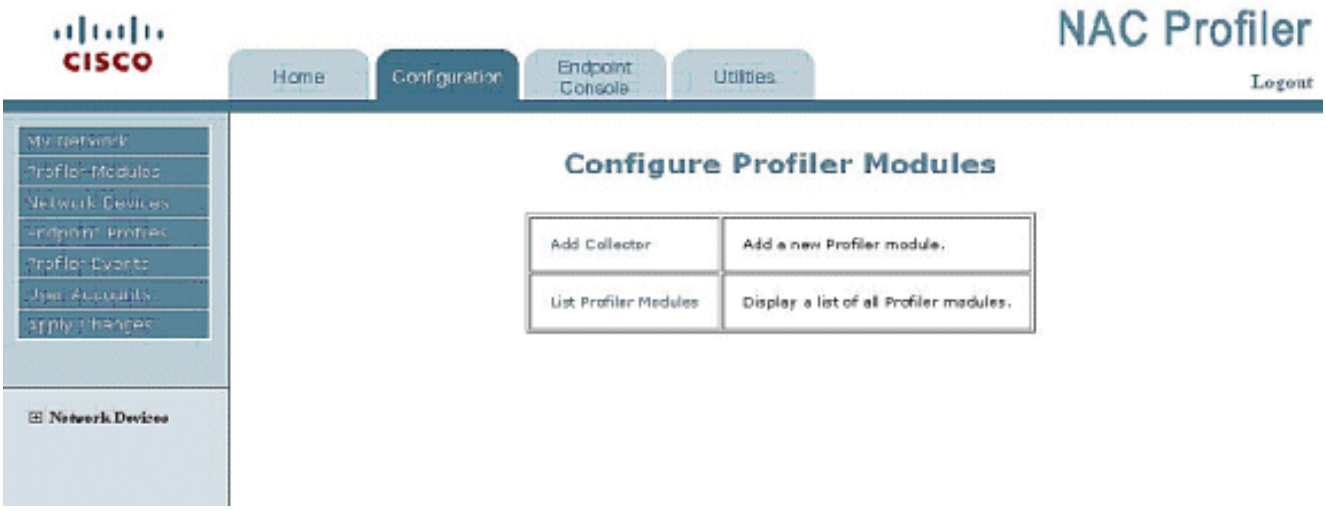
- Configure el Profiler del NAC para OOB la topología
- Configure el colector del NAC
- Configure el switch de acceso para enviar el SNMP traps al colector del NAC
- Configure el switch de acceso en el Profiler para recopilar la información de SNMP
- Configure el Switchport ETH3 del colector del NAC en los switches de distribución para el SPAN

Configure el Profiler y los colectores del NAC en una solución fuera de banda

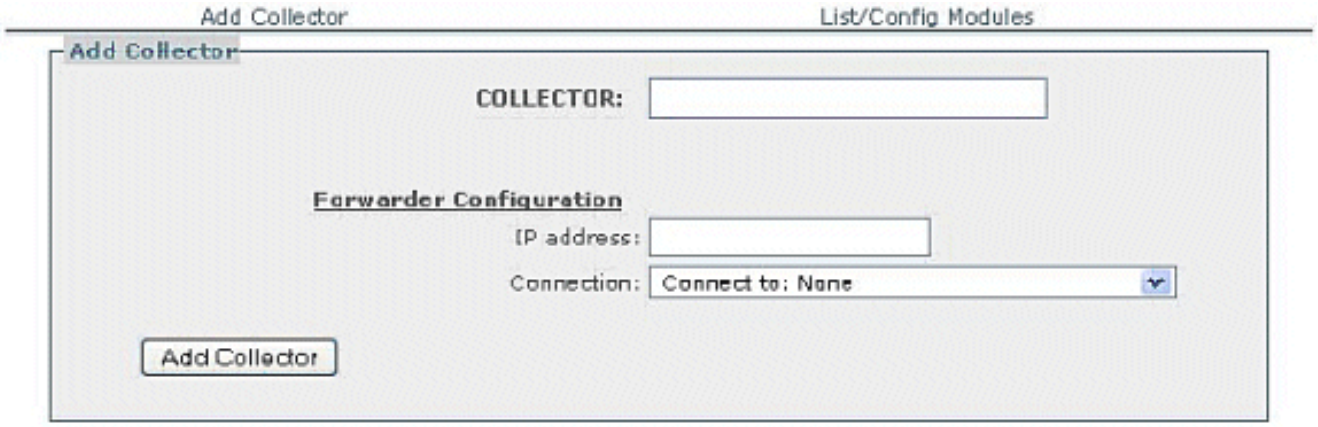
- Los servidores del NAC necesitan ser configurados con la configuración normal del NAC HA.
- El colector utiliza a la dirección IP virtual del servidor del NAC para comunicar con el Profiler.
- El par del colector HA del NAC se agrega como sola entrada en el Profiler y se comunica a la

dirección IP virtual del servidor del NAC.

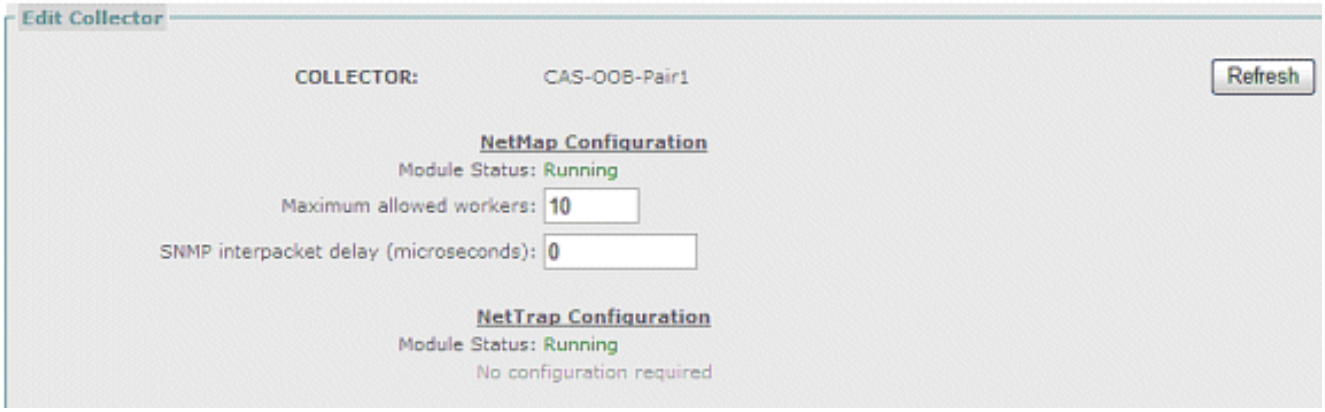
1. Agregue un nuevo colector al Profiler.Vaya al **colector de los módulos de la configuración > del Profiler del NAC > Add**.



2. Agregue un nuevo nombre del colector para los pares del servidor HA del NAC. Éste puede ser cualquier cosa que usted quiere pero que debe hacer juego la configuración del colector.Nombre del colector: **CAS-OOB-Pair1**Dirección IP: **192.168.97.10** (dirección virtual del servidor del NAC)Conexión: Déjela como **NINGUNOS** por ahora

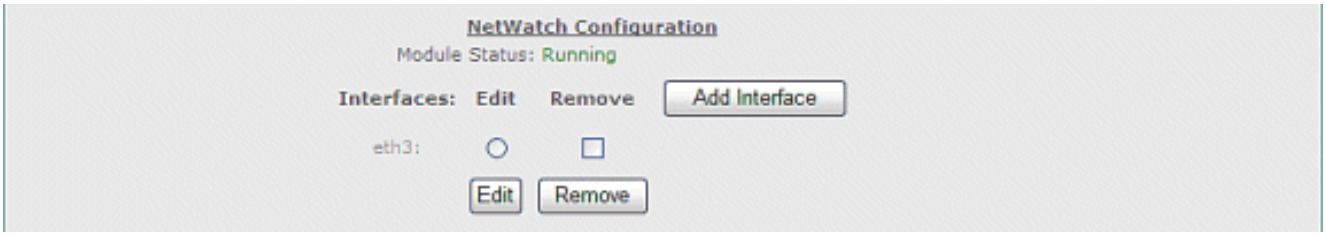


3. Configure sus módulos de servicio del colector. Deje **NetMap** y **NetTrap** solos (la configuración por abandono no es necesaria).

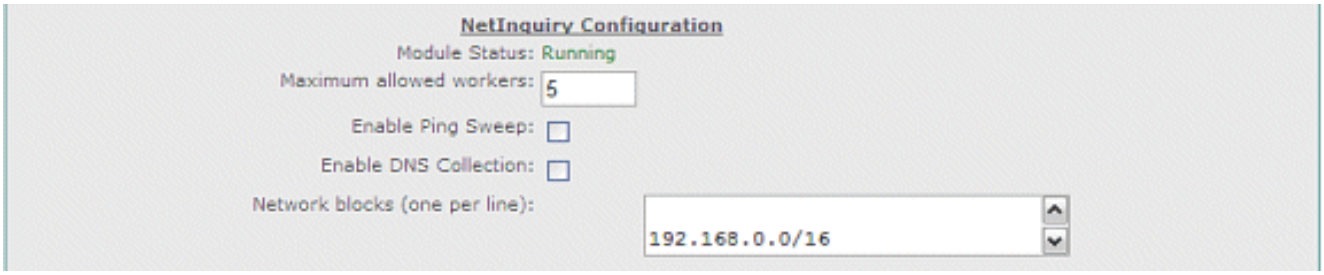


4. Agregue una **interfaz de NetWatch** (ETH3) que esté conectada con un puerto SPAN en el

switch de
distribución.

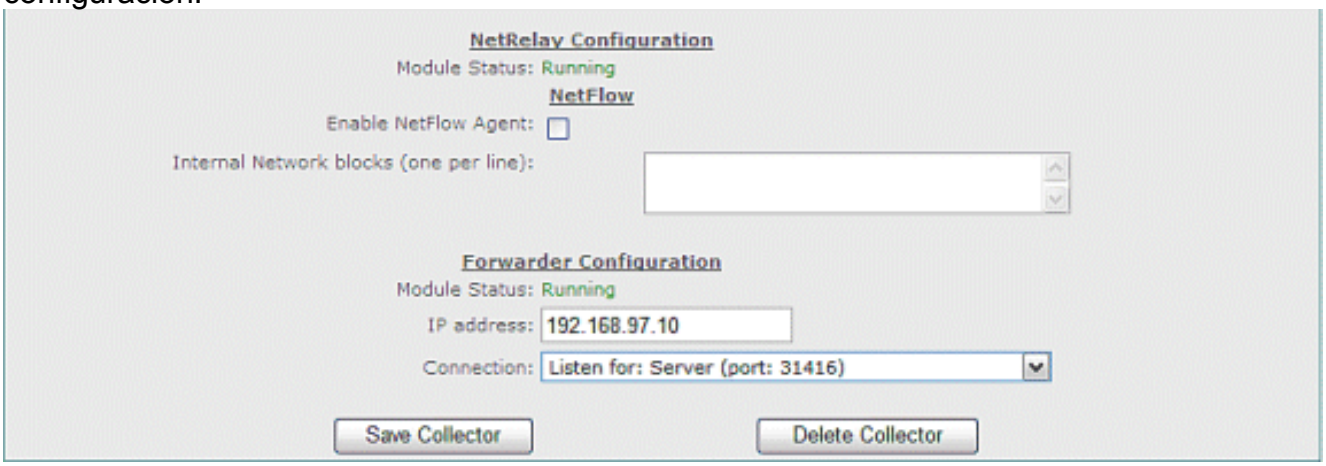


5. Agregue un **bloque de la subred** para el módulo de NetInquiry para estar atento el tráfico interesante que viene de las redes de acceso. Sea específico en las redes y no grave el servidor del NAC innecesariamente. En esta configuración de laboratorio, puede ser el espacio entero del soldado de
192.168.0.0.



Deje el **ping sweep** y la **colección DNS** inhabilitados.

6. Configure el promotor como escuchan en la dirección IP 192.168.97.10 (VIP) y el puerto TCP 31416. Esto permite que el colector actúe como servidor y esté atenta una conexión del Profiler al puerto específico.
7. Deje el **Netflow** inhabilitado (puesto que se utiliza una sesión de Netwatch /SPAN) en la configuración de NetRelay. Aseegurese le hacer clic el botón del **colector de la salvaguardia** para salvar la
configuración.



8. Vaya a la **ficha de configuración > aplican los cambios > los módulos de la actualización**.

[Configure el colector del NAC]

Esta configuración necesita ser funcionada con exactamente como está en ambos dispositivos.

1. SSH al colector y login como **raíz**.
2. Teclee los **config del colector del servicio** y ejecútese a través de la secuencia de comandos de configuración para configurar la porción del colector del NAC.`[root@NAC Server1 ~]# **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) [NAC Server1]: CAS-OOB-Pair1 Network configuration to connect to a NAC Profiler Server Connection type (server/client) [server]: Listen on IP [192.168.97.10]: You will be asked to enter the IP address(es) of the NPS. This is necessary to configure the access control list used by this collector. If the NPS is part of an HA pair then you must include the real IP address of each independent NPS and the virtual IP to ensure proper connectivity in the NAC Server of failover. Enter the IP address(es) of the NAC Profiler. (Finish by typing 'done') [127.0.0.1]: 192.168.96.20 (Real IP address of NAC Profiler1) 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 Profiler) Enter the IP address(es) of the NAC Profiler. (Finish by typing 'done') [done]: 192.168.96.22 (Real IP of NAC Profiler2) 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 NAC SERVER-OOB-Pair1-fw -- Configured NAC SERVER-OOB-Pair1-nm -- Configured NAC SERVER-OOB-Pair1-nt -- Configured NAC SERVER-OOB-Pair1-nw -- Configured NAC SERVER-OOB-Pair1-ni -- Configured NAC SERVER-OOB-Pair1-nr` Se configura el colector del NAC.
3. Comience los servicios del colector.`[root@NAC Server1 ~]# **service collector start**`

Configure el switch de acceso para enviar el SNMP traps al colector del NAC

Esta configuración permite que el Profiler reciba dinámicamente todos los nuevos dispositivos que conecten con un switchport en la red.

Nota: Usted puede también tener una configuración poblada ya para su configuración de NAC normal. Si es así todo lo que usted necesita hacer es agregar el colector de CAS como host en su configuración SNMP para recibir el SNMP traps cuando los nuevos dispositivos conectan con los switchports.

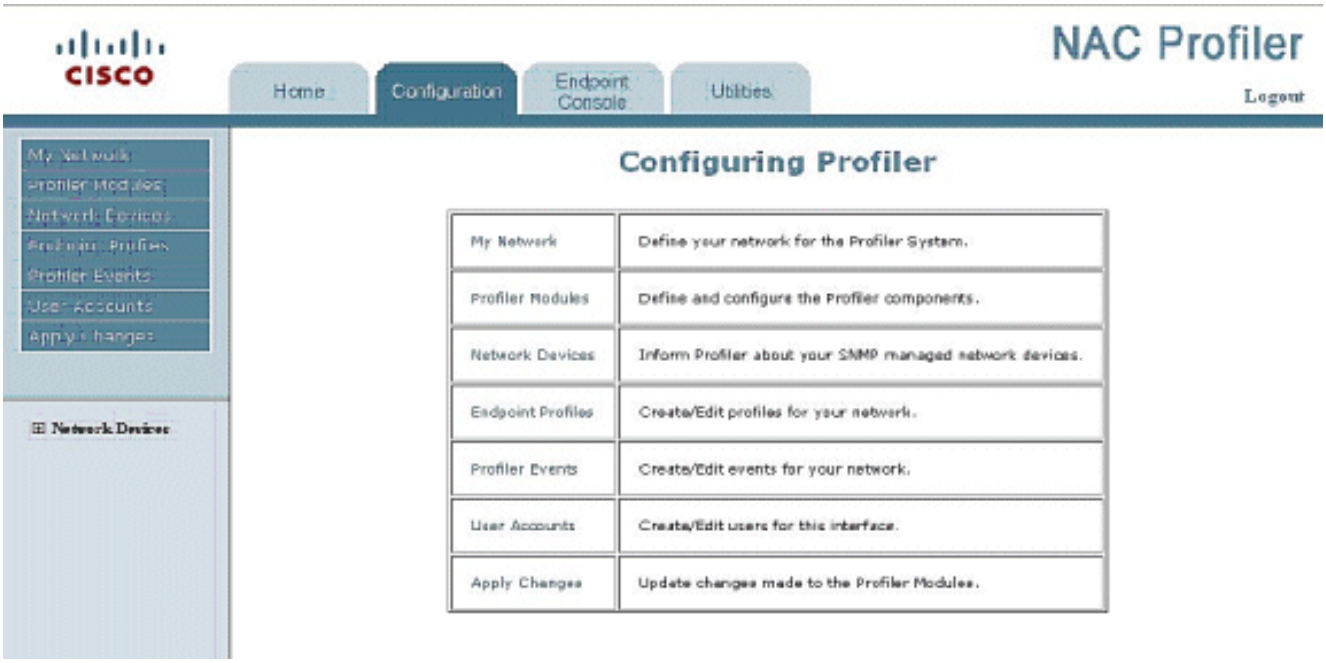
Consola/Telnet en el Switch (nac-3560-access#).

```
snmp-server community cleanaccess RW ## Allows read-write access from the NAC Manager snmp-server community profiler RO ## Allows read only access from Collectors snmp-server enable traps mac-notification ## Enables new-mac notification traps snmp-server host 192.168.97.10 version 1 profiler mac-notification snmp ## Allow traps to the NAC Collectors Managment IP addresss
```

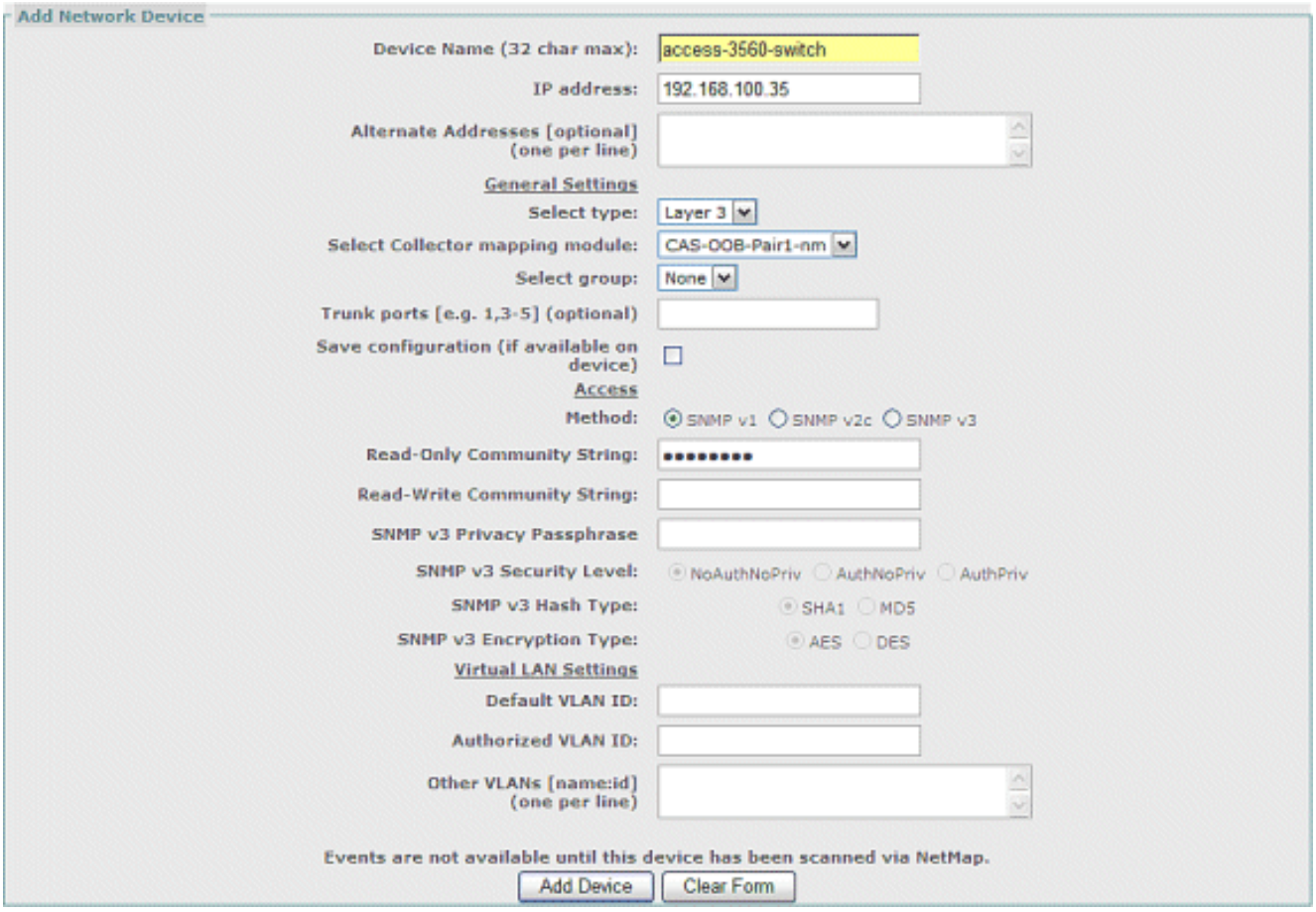
Configure el switch de acceso en el Profiler para recopilar la información de SNMP

Siga estas instrucciones de configurar el switch de acceso en el Profiler para recopilar la información de SNMP.

1. Vaya al Profiler GUI: **Dispositivo de la configuración > de los dispositivos de red > Add**.



2. Agregue el nombre del host y el IP Address de administración del Switch.
3. Ingrese las cadenas solo lecturas SNMP configuradas en el Switch. Aseegurese elegir el módulo de la asignación del colector del NAC, así que el colector se elige a la encuesta SNMP el switch de acceso cada hora y delantero la información al Profiler.
4. Haga clic **agregan el dispositivo** y **aplican los cambios**. Ponga al día los módulos del panel de la izquierda del
GUI.



Nota: El acceso de lectura/escritura no es necesario para el Profiler del NAC en un despliegue del NAC puesto que el administrador del NAC controla el dispositivo ya. Puede haber conflictos y gastos indirectos adicionales al Switches cuando no es necesario.

Configure el Switchport ETH3 del colector del NAC en los switches de distribución para el SPAN

Nota: Esto permite que el módulo de NetWatch esté atenta el tráfico en la red y la información delantera al Profiler. Aseegurese le no hacen oversubscribe la interfaz del colector del NAC. Tiene una limitación de 1GB/sec. Fuente las interfaces o los VLA N del Switch dependiendo de su modelo de switches y versión del código.

Nota: Como mínimo, usted quiere ver los pedidos de DHCP y las ofertas de los puntos finales en sus switches de acceso. Si esto no es posible, agregue un colector del NAC en o cerca de los servidores DHCP en su red.

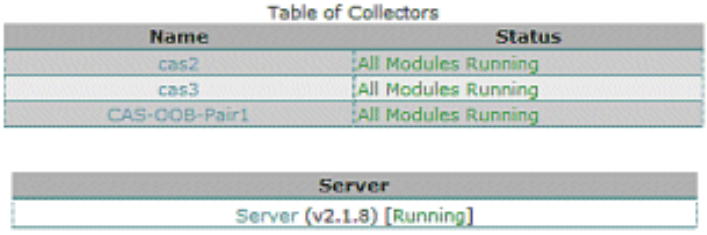
Configure a una sesión de monitoreo en el switch de distribución.

```
monitor session 1 source interface Gi1/0/1 - 43 , Gi1/0/46 - 48
monitor session 1 source interface Po10
monitor session 1 destination interface Gi1/0/44
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

- Aseegurese que el Profiler y el colector comunican y se están ejecutando. Si no son, usted no ve ninguna información sobre los dispositivos en su red. Si hay problemas, no proceda hasta que todos los módulos del colector y el servidor se estén ejecutando.En el Profiler, vaya de la **lista de la configuración > del Profiler del NAC a los módulos del Profiler del NAC de los módulos >**.



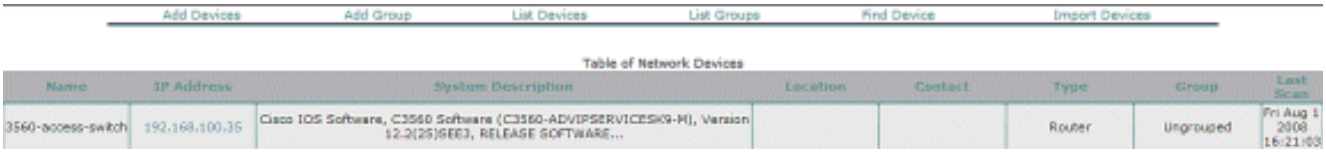
- Verifique que el switch de acceso pueda enviar los desvíos de la notificación nuevo-MAC al colector.**Nota:** Tenga cuidado cuando usted habilita el debug, y conozca sus peligros.`nac-3560-access# debug snmp packet nac-3560-access# debug snmp header SNMP packet debugging is on SNMP packet debugging is on *Mar 30 22:45:12: SNMP: Queuing packet to 192.168.97.10 *Mar 30 22:45:12: Outgoing SNMP packet *Mar 30 22:45:12: v1 packet *Mar 30 22:45:12: community string: profiler *Mar 30 22:45:12: SNMP: V1 Trap, ent cmnMIBNotificationPrefix, addr 192.168.100.35, gentrap 6, spectrap 1 cmnHistMacChangedMsg.0 = 01 00 65 00 04 23 B3 82 60 00 04 00 cmnHistTimestamp.0 = 258751290`
- Verifique que el Profiler recibiera la nueva dirección MAC del colector.Vaya a la **consola > a la opinión del punto final/maneje los puntos finales > los puntos finales de la visualización por los puertos del dispositivo > Ungrouped > la tabla de dispositivos > (elija el Switch)**.

Table of 3560-access-switch

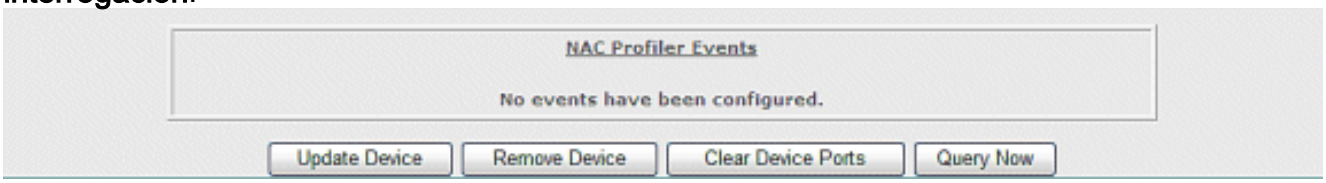
Port	Profile	MAC	IP Address	Link State	802.1X	VLAN
Fa0/1 (10001)				Down		100
Fa0/2 (10002)	Windows Users	00:04:23:b3:82:60 (Intel Corporation)	192.168.100.23	Up		101
Fa0/3 (10003)				Down		101
Fa0/4 (10004)				Down		101

- Verifique que el colector SNMP-haya sondeado el Switch.

1. Mire la columna **más reciente de la exploración**. Esto verifica que el colector analizara el Switch cada 60 minutos por abandono.



2. **Debug SNMP** otra vez en el Switch CLI.
3. Del Profiler GUI, vaya a la **configuración > a los dispositivos de red > a los dispositivos de red de la lista > (elija el dispositivo)**.
4. **Ahora** haga clic la **interrogación**.



5. Mire la salida de los debugs en el Switch para la SNMP-encuesta del colector el Switch.`*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`**
6. Verifique que los trabajos del SPAN sobre el Switch y el colector puedan recibir el tráfico.SSH al Profiler del NAC.**Tcpdump del** tipo **– 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)
16:54:36.432223 IP cas2.nacelab2.cisco.com.9308 >
   elab2-dns-dhcp.nacelab2.cisco.com.domain:
   48871+ PTR? 68.39.168.192.in-addr.arpa. (44)
16:54:36.432468 IP cas2.nacelab2.cisco.com.9308 >
   elab2-dns-dhcp.nacelab2.cisco.com.domain:
   58368+ PTR? 69.39.168.192.in-addr.arpa. (44)
16:54:36.432472 IP cas2.nacelab2.cisco.com.9308 >
   elab2-dns-dhcp.nacelab2.cisco.com.domain:
   58368+ PTR? 69.39.168.192.in-addr.arpa. (44)
16:54:36.432842 IP cas2.nacelab2.cisco.com.9308 >
   elab2-dns-dhcp.nacelab2.cisco.com.domain:
   1650+ PTR? 70.39.168.192.in-addr.arpa. (44)
16:54:36.432846 IP cas2.nacelab2.cisco.com.9308 >
   elab2-dns-dhcp.nacelab2.cisco.com.domain:
   1650+ PTR? 70.39.168.192.in-addr.arpa. (44)
```
7. Mire la salida en la pantalla. Si usted se refiere sobre la cantidad de salida, usted puede transmitir la salida a un archivo en el colector del NAC. Refiera a las páginas principales en Linux.
8. Marque si usted puede ver el tráfico del DHCP sobre los puntos finales en su Switch.Van al **Profiler el GUI > la consola > la opinión del punto final/manejan los puntos finales**. Haga clic

un perfil; haga clic un dispositivo, y haga clic los datos del punto final.Usted ve la información de la clase del vendedor del DHCP del dispositivo capturado del tráfico NetWatch/SPAN en el
colector:

Table of Other Data for 00:04:23:b3:82:60

Data Type	Data	Last Updated
DHCP Host Name	cca-xp2	Fri Aug 1 2008 16:54:40
DHCP Vendor Class	MSFT 5.0	Fri Aug 1 2008 16:54:40
DHCP Options List	53,61,12,81,60,55,255	Fri Aug 1 2008 16:54:40
DHCP Inform Requests		Fri Aug 1 2008 16:54:40
DHCP Requested Options	1,15,3,6,44,46,47,31,33,249,43,255	Fri Aug 1 2008 16:54:40
Network Stack Info	TTL: 128 Window: 65535(0) TCPOptionList: 2,1,1,4	2008-08-01 16:58:17.252152

Soporte para la configuración del NTP

El Profiler del NAC soporta la configuración del NTP solamente con la versión 3.1 y posterior. Permite configurar las diversas opciones para los Servidores de tiempo a través de una interfaz Web controlada por menú. Refiera a la configuración NTP en la sección del servidor del Cisco NAC Profiler para los detalles completos.

Si la versión del Profiler del NAC está antes de 3.1, después usted no puede configurar el NTP porque la versión 2.1.8 del Profiler del NAC no tiene la capacidad para hacerlo a través de la interfaz Web. Refiera a las Advertencias abiertas mencionadas en los Release Note de la versión 2.1.8 del Profiler del NAC. Para más información, refiera al Id. de bug Cisco CSCsu46273 (clientes registrados solamente).

Usted puede configurar lo mismo manualmente con el CLI. Complete estos pasos:

1. De una sesión SSH al Profiler, cd a /etc, y edite el archivo ntp.conf.
2. Agregue los servidores de momento apropiado en este archivo.
3. Configure la zona de Hora del reloj.`mv /etc/localtime /etc/localtime-old`
   `ln -sf /usr/share/zoneinfo/<your_time_zone> /etc/localtime`

Información Relacionada

- Cisco NAC Appliance (Clean Access)
- Soporte Técnico y Documentación - Cisco Systems