Distribua o perfilador NAC em um NAC fora da banda existente

Índice

Introdução

Este guia de distribuição descreve como executar o server do Cisco NAC Profiler e os coletores do Cisco NAC Profiler (situados no servidor de acesso limpo da ferramenta NAC de Cisco) em um desenvolvimento fora da banda do terreno (OOB). Este documento descreve como o melhor distribui o Cisco NAC Profiler em uma Alta disponibilidade existente do desenvolvimento OOB NAC. Pretende-se ajudá-lo a compreender os recursos básicos e a topologia de uma solução do Cisco NAC Profiler integrada com a ferramenta NAC de Cisco. Igualmente ajuda-o a compreender como a informação do valor-limite sobre todos os dispositivos NAC-menos é enviada dos coletores ao server do perfilador. O objetivo da solução é perfilar os valores-limite e adicionar-los à lista de filtro do dispositivo do Access Manager limpo da ferramenta NAC de Cisco (CAM) a fim aplicar a política apropriada.

Pré-requisitos

Requisitos

Você deve primeiramente configurar seus gerente de Cisco NAC, server de Cisco NAC, e Cisco NAC Profiler 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 (IP do serviço de 192.168.96.10 HA)
- Server NAC (IP do serviço de 192.168.97.10 HA)
- Perfilador NAC (192.168.96.21)
- Switch de acesso 3560 (192.168.100.35)
- Switch de distribuição 3750 (192.168.97.1)

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.

Informações de Apoio

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 vária escala e da complexidade pela identificação, pelo lugar, e pela 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 que descubra, catálogos, e perfila todos os valores-limite conectados a uma rede com a tarefa específica de perfilar valores-limite do agente-menos.

Vista geral NAC

O dispositivo do Cisco Network Admission Control (NAC) (igualmente conhecido 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, a em-faixa ou as opções de distribuição fora da banda, as ferramentas da autenticação de usuário, e os controles da largura de banda e do filtragem de tráfego, a ferramenta NAC de Cisco são uma solução completa para controlar e fixar redes. Como o ponto central do gerenciamento de acesso para sua rede, a ferramenta NAC de Cisco deixam-no executar a Segurança, o acesso, e as políticas da conformidade em um lugar em vez de ter que propagar as políticas durante todo a rede em muitos dispositivos.

Configurar

Vista geral do manual de configuração

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

O diagrama em figura 1 mostra um desenvolvimento do terreno da camada básica 2 com (HA) Alta disponibilidade dos server NAC através dos switch de distribuição. O server do perfilador e o gerente NAC podem sentar-se na mesma rede de gerenciamento e enviar e receber a informação dos server e dos coletores NAC. Há diversas maneiras que o Cisco NAC Profiler pode descobrir os pontos finais remotos NON-NAC, e este guia descreve o mais comum e métodos recomendada. Este manual de configuração descreve como realizar estes:

- Adicionar uma comunicação SNMP a e do switch de acesso aos coletores NAC.
- Configurar uma porta span nos switch de distribuição para capturar todo o tráfego dos dispositivos da camada de acesso, especificamente tráfego DHCP dos valores-limite, desde que nós estamos os mais interessados no atributo da informação da classe de fornecedor DHCP sobre valores-limite.
- Configurar a comunicação do server e do coletor do Cisco NAC Profiler em conformidade para receber toda a informação recolhida pelos coletores.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Figura 1: Desenvolvimento da ferramenta NAC OOB Cisco com Cisco NAC Profiler

Configurações

Este documento usa estas configurações para configurar o perfilador e coletores NAC em uma solução fora da banda:

- Configurar o perfilador NAC para a topologia OOB
- Configurar o coletor NAC
- Configurar o switch de acesso para enviar o SNMP traps ao coletor NAC
- Configurar o switch de acesso no perfilador para recolher a informação de SNMP
- Configurar o Switchport ETH3 do coletor NAC nos switch de distribuição para o PERÍODO

Configurar o perfilador e os coletores NAC em uma solução fora da banda

- Os server NAC precisam de ser configurados com a instalação normal NAC HA.
- O coletor 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 comunicado ao endereço IP de Um ou Mais Servidores Cisco ICM NT virtual do server NAC.

1. Adicionar um coletor novo ao perfilador.Vá ao **coletor do > Add dos módulos da configuração > do Profiler NAC**.
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 a configuração do coletor.Nome do coletor: **CAS-OOB-Pair1**Endereço IP de Um ou Mais Servidores Cisco ICM NT: **192.168.97.10** (endereço virtual do server NAC)Conexão: Deixe-a como **NENHUNS** por agora
3. Configurar seus módulos de serviço do coletor. Deixe **NetMap** e **NetTrap** sozinhos (a configuração não é à revelia necessária).
4. Adicionar uma **relação de NetWatch** (ETH3) que seja conectada a uma porta span no switch de distribuição.
5. Adicionar um **bloco da sub-rede** para o módulo de NetInquiry para escutar o tráfego interessante que vem das redes de acesso. Seja específico nas redes e não taxe o server NAC desnecessariamente. Nesta instalação de laboratório, pode ser o espaço privado inteiro de 192.168.0.0.Deixe o **ping sweep** e a **coleção DNS** desabilitados.
6. Configurar o remetente como escutam 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 específica.
7. Deixe o **Netflow** desabilitado (desde que uma sessão de Netwatch /SPAN é usada) na configuração de NetRelay. Certifique-se de você clique o botão do **coletor da salvaguarda** salvar a configuração.
8. Vá ao **guia de configuração > aplicam mudanças > módulos da atualização**.

Configurar o coletor NAC

Esta configuração precisa de ser executada exatamente como está em ambos os dispositivos.

1. SSH ao coletor e início de uma sessão como a **raiz**.
2. Datilografe a **configuração do coletor do serviço** e seja-a executado através do script de configuração para estabelecer a parcela do coletor 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` O coletor NAC é configurado.
3. Enfie os serviços do coletor.`[root@NAC Server1 ~]#` **`service collector start`**

Configurar o switch de acesso 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 durante todo a rede.

Nota: Você pode igualmente ter uma configuração já povoada para sua configuração NAC normal. Em caso afirmativo, tudo que você precisa de fazer é adicionar o coletor de CAS como um host em sua configuração de SNMP para receber o SNMP traps quando os dispositivos novos conectam aos switchports.

Console/telnet no interruptor (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
```

Configurar o switch de acesso no perfilador para recolher a informação de SNMP

Siga estas instruções para configurar o switch de acesso no perfilador para recolher a informação de SNMP.

1. Vá ao perfilador GUI: **Dispositivo do > Add da configuração > dos dispositivos de rede**.
2. Adicionar o nome de host e o endereço IP de gerenciamento do interruptor.
3. 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**. Atualize os módulos do painel esquerdo do GUI.**Nota:** O acesso de leitura/gravação não é precisado para o perfilador NAC em um desenvolvimento NAC desde que o gerente NAC controla o dispositivo já. Pode haver uns conflitos e umas despesas gerais extra ao Switches quando não é necessário.

Configurar o Switchport ETH3 do coletor NAC nos switch de distribuição para o PERÍODO

Nota: Isto permite que o módulo de NetWatch escute 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 1GB/sec. Fonte as relações ou os VLAN do interruptor segundo 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, adicionar um coletor NAC ou perto dos servidores DHCP em sua rede.

Configurar uma sessão de monitor no switch de distribuição.

```
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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

- Certifique-se de que o perfilador e o coletor se comunicam e estão sendo executado. Se não são, você não vê nenhuma informação sobre os dispositivos em sua rede. Se há umas edições, não continue até que todos os módulos do coletor e o server sejam executado.No perfilador, vá aos **módulos da configuração > do perfilador NAC > aos módulos do perfilador da lista NAC**.
- Verifique que o switch de acesso pode enviar armadilhas da notificação novo-MAC ao coletor.**Nota:** Seja cuidadoso quando você permite debuga, e conhece seus perigos.`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 o perfilador recebeu o MAC address novo do coletor.Vá ao **console > à opinião do valor-limite/controle valores-limite > valores-limite do indicador por portas do dispositivo > por Ungrouped > por tabela dos dispositivos > (escolha o interruptor)**.
- Verifique que o coletor SNMP-votou o interruptor.

1. Olhe a **última** coluna da **varredura**. Isto verifica que o coletor fez a varredura do interruptor cada 60 minutos à revelia.
2. **Debugar o SNMP** outra vez no interruptor CLI.
3. Do perfilador GUI, vá à **configuração > aos dispositivos de rede > aos dispositivos de rede da lista > (escolha o dispositivo)**.
4. Clique a **pergunta agora**.
5. Olhe o resultado do debug no interruptor para a SNMP-votação do coletor 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`**
6. Verifique que os trabalhos do PERÍODO no interruptor e no coletor podem receber o tráfego.SSH ao perfilador NAC.Tipo **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) 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. 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. Refira as páginas principal em Linux.
8. Verifique se você possa ver o tráfego DHCP sobre os valores-limite em seu interruptor.Vão ao **perfilador o GUI > o console > a opinião do valor-limite/controlam valores-limite**. Clique um perfil; clique um dispositivo, e clique os dados do valor-limite.Você vê a informação da classe de fornecedor DHCP do dispositivo capturado do tráfego NetWatch/SPAN no coletor:

Apoio para a configuração do NTP

O perfilador NAC apoia a configuração de NTP somente com versão 3.1 e mais recente. Reserva configurar as opções diferentes para Times Server através de uma interface da WEB menu-conduzida. Refira configurar NTP na seção do server do Cisco NAC Profiler para detalhes completos.

Se a versão do perfilador NAC é antes de 3.1, a seguir você não pode configurar o NTP porque a versão 2.1.8 do perfilador NAC não tem a capacidade da fazer através da interface da WEB. Refira as interrupções de processo aberto mencionadas nos Release Note da versão 2.1.8 do perfilador NAC. Para mais informação, refira a identificação de bug Cisco CSCsu46273 (clientes registrados somente).

Você pode configurar o mesmos manualmente com o CLI. Conclua estes passos:

1. De uma sessão SSH ao perfilador, o CD a /etc, e edita o arquivo ntp.conf.
2. Adicionar os server de período apropriado neste arquivo.
3. Configurar a zona de tempo.`mv /etc/localtime /etc/localtime-old`
   `ln -sf /usr/share/zoneinfo/<your_time_zone> /etc/localtime`

Informações Relacionadas

- Cisco NAC Appliance (Clean Access)
- Suporte Técnico e Documentação - Cisco Systems