Déployer NAC Profiler dans un NAC hors bande existant

Contenu

Introduction

Ce guide de déploiement décrit comment implémenter le serveur de Cisco NAC Profiler et les collecteurs de Cisco NAC Profiler (situés sur l'appliance Clean Access Server de Cisco NAC) dans un déploiement hors bande du campus (OOB). Ce document décrit comment le meilleur déploient le Cisco NAC Profiler dans un déploiement facilement disponible existant OOB NAC. On le destine pour vous aider à comprendre les fonctionnalités de base et la topologie d'une solution de Cisco NAC Profiler intégrée avec l'appliance de Cisco NAC. Il vous aide également à comprendre comment des informations de point final sur tous les périphériques sans NAC sont envoyées des collecteurs au serveur de profileur. Le but de la solution est de profiler les points finaux et de les ajouter à la liste de filtre de périphérique de l'appliance Clean Access Manager (CAM) de Cisco NAC afin d'appliquer la stratégie appropriée.

Conditions préalables

Conditions requises

Vous devez d'abord configurer votre gestionnaire de Cisco NAC, serveur de Cisco NAC, et Cisco NAC Profiler selon les guides d'installation et de configuration pour chaque produit.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Gestionnaire NAC (IP de service de 192.168.96.10 ha)
- Serveur NAC (IP de service de 192.168.97.10 ha)
- Profileur NAC (192.168.96.21)
- Commutateur d'accès de 3560 (192.168.100.35)
- Commutateur de distribution 3750 (192.168.97.1)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Aperçu de profileur NAC

Administrateurs réseau d'enables de Cisco NAC Profiler efficacement pour déployer et parvenir le Contrôle d'admission au réseau (NAC) dans les réseaux d'entreprise de la diverse échelle et de la complexité par l'identification, la localisation, et la détermination des capacités de tous les points finaux de réseau reliés, indépendamment du type de périphérique, afin d'assurer et mettre à jour l'accès au réseau approprié. Le Cisco NAC Profiler est un système qui le découvre, des catalogues, et profile tous les points finaux connectés à un réseau à la tâche spécifique de profiler des points finaux sans agent.

Aperçu NAC

L'appliance du Cisco Network Admission Control (NAC) (également connue sous le nom de Cisco Clean Access) est un contrôle d'admission et solution d'une mise en application puissants et faciles à utiliser de conformité. Avec les fonctionnalités de sécurité complètes, l'intrabande ou les options hors bande de déploiement, les outils d'authentification de l'utilisateur, et les contrôles de bande passante et de filtrage de trafic, l'appliance de Cisco NAC est une solution complète à contrôler et des réseaux sécurisés. Comme point central de Gestion d'accès pour votre réseau, l'appliance de Cisco NAC vous permet d'implémenter la Sécurité, l'accès, et les stratégies de conformité dans un endroit au lieu de devoir propager les stratégies dans tout le réseau sur beaucoup de périphériques.

Configurez

Aperçu de guide de configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Le diagramme dans la figure 1 affiche un déploiement de base de campus de la couche 2 avec (ha) les serveurs facilement disponibles NAC à travers des commutateurs de distribution. Le serveur de profileur et le gestionnaire NAC peuvent s'asseoir sur le même réseau de gestion et envoyer et recevoir les informations des serveurs et des collecteurs NAC. Il y a plusieurs manières que le Cisco NAC Profiler peut découvrir les points finaux non-NAC distants, et ce guide décrit le plus commun et les méthodes recommandées. Ce guide de configuration décrit comment accomplir ces derniers :

- Ajoutez la transmission SNMP à et du commutateur d'accès aux collecteurs NAC.
- Configurez un port SPAN sur les commutateurs de distribution pour capturer tout le trafic des périphériques de couche d'accès, spécifiquement le trafic DHCP des points finaux, puisque nous sommes les plus intéressés par l'attribut de l'information de classe du constructeur DHCP au sujet des points finaux.
- Configurez la transmission de serveur et de collecteur de Cisco NAC Profiler en conséquence pour recevoir toutes les informations recueillies par les collecteurs.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Figure 1 : Déploiement d'appareils de Cisco NAC OOB avec le Cisco NAC Profiler

Configurations

Ce document emploie ces configurations pour configurer le profileur et des collecteurs NAC dans une solution hors bande :

- Configurez le profileur NAC pour la topologie OOB
- Configurez le collecteur NAC
- Configurez le commutateur d'accès Pour envoyer des déroutements SNMP au collecteur NAC
- Configurez le commutateur d'accès Sur le profileur pour recueillir des informations SNMP
- Configurez le switchport ETH3 du collecteur NAC sur les commutateurs de distribution pour l'ENVERGURE

Configurez le profileur et les collecteurs NAC dans une solution hors bande

- Des serveurs NAC doivent être configurés par l'installation normale NAC ha.
- Le collecteur utilise l'adresse IP virtuelle du serveur NAC pour communiquer avec le profileur.
- La paire ha de collecteur NAC est ajoutée comme seule entrée dans le profileur et communiquée à l'adresse IP virtuelle du serveur NAC.

1. Ajoutez un nouveau collecteur au profileur.Allez aux **modules de configuration > de profileur NAC > ajoutent le collecteur**.
2. Ajoutez un nouveau nom de collecteur pour les paires ha de serveur NAC. Ceci peut être quelque chose que vous voulez mais devez apparier la configuration de collecteur.Nom de collecteur : **CAS-OOB-Pair1**Adresse IP : **192.168.97.10** (adresse virtuelle du serveur NAC)Connexion : Laissez-le en tant qu'**AUCUN** pour l'instant
3. Configurez vos modules de service de collecteur. Congé seul **NetMap** et **NetTrap** (la configuration par défaut n'est pas nécessaire).
4. Ajoutez une **interface de NetWatch** (ETH3) qui est connectée à un port SPAN sur le commutateur de distribution.
5. Ajoutez un **bloc de sous-réseau** pour le module de NetInquiry pour écouter le trafic intéressant qui provient les réseaux d'accès. Soyez spécifique sur les réseaux et n'imposez pas le serveur NAC inutilement. Dans cette installation de laboratoire, ce peut être l'espace privé entier de 192.168.0.0.**Balayage ping de** congé et **collection de DN** désactivée.
6. Configurez l'expéditeur comme écoutent sur l'adresse IP 192.168.97.10 (VIP) et le port TCP 31416. Ceci permet au collecteur pour agir en tant que serveur et pour écouter une connexion du profileur au port spécifique.
7. Laissez le **NetFlow** désactivé (puisqu'une session de Netwatch /SPAN est utilisée) dans la configuration de NetRelay. Veillez-vous clic le bouton de **collecteur de sauvegarde** pour sauvegarder la configuration.
8. Allez à l'**onglet de configuration > appliquent des modifications > des modules de mise à jour**.

Configurez le collecteur NAC

Cette configuration doit être exécutée exactement comme est sur les deux périphériques.

1. SSH au collecteur et procédure de connexion comme **racine**.
2. Tapez le **config** et le passage de **collecteur de service** par le script de configuration pour installer la partie de collecteur 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` Le collecteur NAC est configuré.
3. Commencez les services de collecteur.`[root@NAC Server1 ~]#` **`service collector start`**

Configurez le commutateur d'accès Pour envoyer des déroutements SNMP au collecteur NAC

Cette configuration permet au profileur pour recevoir dynamiquement tous les nouveaux périphériques qui se connectent à un switchport dans tout le réseau.

Remarque: Vous pouvez également avoir une configuration déjà remplie pour votre configuration du NAC normale. Si oui, tout que vous devez faire est d'ajouter le collecteur de CAS car un hôte dans votre configuration SNMP pour recevoir les déroutements SNMP quand les nouveaux périphériques se connectent aux switchports.

Console/telnet dans le commutateur (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
```

Configurez le commutateur d'accès Sur le profileur pour recueillir des informations SNMP

Suivez ces instructions de configurer le commutateur d'accès sur le profileur pour recueillir des informations SNMP.

1. Allez au GUI de profileur : **Les périphériques de configuration > de réseau > ajoutent le périphérique**.
2. Ajoutez l'adresse IP de nom d'hôte et de Gestion du commutateur.
3. Écrivez les chaînes en lecture seule SNMP configurées sur le commutateur. Veillez à choisir le module de mappage de collecteur NAC, ainsi le collecteur est choisi au balayage SNMP le commutateur d'accès chaque heure et en avant les informations au profileur.
4. Cliquez sur Add le **périphérique** et **appliquez les modifications**. Mettez à jour les modules du volet gauche du GUI.**Remarque:** L'accès en lecture-écriture n'est pas nécessaire pour le profileur NAC dans un déploiement NAC puisque le gestionnaire NAC contrôle le périphérique déjà. Il peut y avoir des conflits et de temps système supplémentaire aux Commutateurs quand il n'est pas nécessaire.

Configurez le switchport ETH3 du collecteur NAC sur les commutateurs de distribution pour l'ENVERGURE

Remarque: Ceci permet au module de NetWatch pour écouter le trafic sur le réseau et les informations en avant au profileur. Assurez-vous que vous ne faites pas oversubscribe l'interface du collecteur NAC. Il a une limite de 1GB/sec. Source les interfaces ou les VLAN du commutateur selon votre modèle de commutateur et version de code.

Remarque: D'une façon minimum, vous voulez voir les requêtes DHCP et les offres des points finaux sur vos commutateurs d'accès. Si ce n'est pas possible, ajoutez un collecteur NAC sur ou près des serveurs DHCP sur votre réseau.

Configurez une session de surveillance sur le commutateur de distribution.

```
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
```

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

- Assurez-vous que le profileur et le collecteur communiquent et s'exécutent. S'ils ne sont pas, vous ne voyez aucune information sur les périphériques dans votre réseau. S'il y a des questions, ne poursuivez pas jusqu'à ce que tous les modules de collecteur et serveur s'exécutent.Sur le profileur, allez aux **modules de configuration > de profileur NAC > aux modules de profileur de la liste NAC**.
- Vérifiez que le commutateur d'accès peut envoyer des déroutements de notification de nouveau-MAC au collecteur.**Remarque:** Faites attention quand vous activez mettez au point, et connaissez ses dangers.`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`
- Vérifiez que le profileur a reçu la nouvelle adresse MAC du collecteur.Allez à la **console > à la vue de point final/gérez les points finaux > les points finaux d'affichage par le périphérique met en communication > Ungrouped > Tableau des périphériques > (choisissez le commutateur)**.
- Vérifiez que le collecteur SNMP-a voté le commutateur.

1. Regardez la **dernière** colonne de **balayage**. Ceci vérifie que le collecteur a balayé le commutateur toutes les 60 minutes par défaut.
2. **Debug snmp** de nouveau sur le commutateur CLI.
3. Du GUI de profileur, allez aux **périphériques de configuration > de réseau > aux périphériques de réseau de liste > (choisissez le périphérique)**.
4. **Requête de** clic **maintenant**.
5. Observez la sortie de débogage sur le commutateur pour le SNMP-balayage de collecteur le commutateur.`*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. Vérifiez que les travaux d'ENVERGURE sur le commutateur et le collecteur peuvent recevoir le trafic.SSH au profileur NAC.**Tcpdump de** type **– l 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. Observez la sortie sur l'écran. Si vous êtes préoccupé par la quantité de sortie, vous pouvez siffler la sortie à un fichier sur le collecteur NAC. Référez-vous aux pages principales dans le Linux.

8. Vérifiez si vous pouvez voir le trafic DHCP au sujet des points finaux sur votre commutateur.Allez au **profileur GUI > console > vue de point final/gérez les points finaux**. Cliquez sur un profil ; cliquez sur un périphérique, et cliquez sur les données de point final.Vous voyez les informations de classe du constructeur DHCP du périphérique capturé du trafic NetWatch/SPAN sur le collecteur :

Soutien de configuration de NTP

Le profileur NAC prend en charge la configuration de NTP seulement avec la version 3.1 et ultérieures. Il laisse configurer les différentes options pour des Serveurs de synchronisation par une interface web pilotée par menus. Référez-vous au NTP de configurer sur la section Serveur de Cisco NAC Profiler pour les détails complets.

Si la version de profileur NAC est avant 3.1, alors vous ne pouvez pas configurer le NTP parce que la version 2.1.8 de profileur NAC n'a pas la capacité pour le faire par l'interface de Web. Référez-vous aux notifications ouvertes mentionnées dans les notes en version de la version 2.1.8 de profileur NAC. Le pour en savoir plus, se rapportent à l'ID de bogue Cisco CSCsu46273 (clients enregistrés seulement).

Vous pouvez configurer la même chose manuellement par le CLI. Procédez comme suit :

1. D'une session de SSH au profileur, le cd à /etc, et éditent le fichier ntp.conf.
2. Ajoutez les Serveurs de synchronisation compétents dans ce fichier.
3. Configurez le fuseau horaire d'horloge.`mv /etc/localtime /etc/localtime-old`
   `ln -sf /usr/share/zoneinfo/<your_time_zone> /etc/localtime`

Informations connexes

- Dispositif Cisco NAC (Clean Access)
- Support et documentation techniques - Cisco Systems