Развертывание профилировщика NAC на существующем NAC вне диапазона

Содержание

Введение

Это руководство по развертыванию описывает, как внедрить Сервер Cisco NAC Profiler и Коллекторы Cisco NAC Profiler (расположенный на устройстве Cisco NAC Чистый Сервер доступа) во Внеполосных (OOB) развертываниях Кампуса. Этот документ описывает, как лучше всего развернуть Cisco NAC Profiler в существующих развертываниях NAC Высокой доступности OOB. Это предназначено, чтобы помочь вам понимать стандартные средства и топологию решения для Cisco NAC Profiler, интегрированного с устройством Cisco NAC. Это также помогает вам понимать, как информация об оконечной точке обо всех устройствах NAC меньше передается с Коллекторов на Сервер Профилировщика. Цель решения состоит в том, чтобы представить оконечные точки и добавить их к списку Фильтра устройств Clean Access Manager (CAM) устройства Cisco NAC для применения соответствующей политики.

Предварительные условия

Требования

Необходимо сначала настроить диспетчера Cisco NAC Manager, сервер Cisco NAC и Cisco NAC Profiler в соответствии с установкой и руководствами по конфигурации для каждого продукта.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Менеджер NAC (сервисный IP на 192.168.96.10 га)
- Сервер NAC (сервисный IP на 192.168.97.10 га)
- Профилировщик NAC (192.168.96.21)
- 3560 коммутаторов доступа (192.168.100.35)
- 3750 коммутаторов распределения (192.168.97.1)

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

Обзор профилировщика NAC

Cisco NAC Profiler позволяет администраторам сети эффективно развернуть и управлять Network Admission Control (NAC) в корпоративных сетях различного масштаба и сложности идентификацией, местоположением и определением возможностей всех оконечных точек подключенной сети, независимо от типа устройства, чтобы гарантировать и поддержать соответствующий доступ к сети. Cisco NAC Profiler является системой, которая обнаруживает, каталоги, и представляет все оконечные точки, связанные с сетью с определенной задачей профилирования бессубъектных оконечных точек.

Обзор NAC

Система контроля доступа к сети Cisco NAC (NAC) Устройство (также известный как Cisco Clean Access) является мощным, простым в использовании контролем доступа и решением для осуществления соответствия. С функциями универсальной безопасности, внутриполосными или внеполосными параметрами развертывания, программными средствами проверки подлинности пользователя, и пропускной способностью и средствами управления за фильтрацией трафика, устройство Cisco NAC является полным решением контроля и защищенных сетей. Как центральная точка управления доступом для вашей сети, устройство Cisco NAC позволяет вам внедрить безопасность, доступ и политику соответствия в одном месте вместо того, чтобы иметь необходимость распространиться

политику всюду по сети на многих устройствах.

Настройка

Обзор руководства по конфигурации

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Схема на рисунке 1 показывает базовому уровню 2 развертывания Кампуса с Серверами NAC Высокой доступности (HA) через коммутаторы распределения. Сервер Профилировщика и Менеджер NAC могут находиться на той же сети управления и передать и получить информацию от Серверов NAC и Коллекторов. Существует несколько способов, которыми Cisco NAC Profiler может обнаружить не-NAC удаленные оконечные точки, и это руководство описывает наиболее распространенное и рекомендуемые методы. Это руководство по конфигурации описывает, как выполнить их:

- Добавьте связь SNMP к и с коммутатора доступа на Коллекторы NAC.
- Настройте Порт SPAN на коммутаторах распределения для получения всего трафика от устройств уровня доступа, в частности трафика DHCP от оконечных точек, так как мы больше всего интересуемся атрибутом информации о классе поставщика DHCP об оконечных точках.
- Настройте связь Сервера и Коллектора Cisco NAC Profiler соответственно для получения всей информации, собранной Коллекторами.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:

Рисунок 1: Развертывания устройства Cisco NAC OOB с Cisco NAC Profiler

Конфигурации

Этот документ использует эти конфигурации для настройки Профилировщика NAC и Коллекторов во Внеполосном решении:

- Настройте профилировщика NAC для топологии OOB
- Настройте коллектор NAC
- Настройте коммутатор доступа для передачи trap-сообщений SNMP к коллектору NAC
- Настройте коммутатор доступа на профилировщике для сбора сведений SNMP
- Настройте порт коммутатора ETH3 коллектора NAC на коммутаторах распределения для SPAN

Настройте профилировщика NAC и коллекторы во внеполосном решении

- Серверы NAC должны быть настроены через обычный NAC, HA устанавливают.
- Коллектор использует виртуальный IP - адрес Сервера NAC для передачи с

Профилировщиком.
- Коллектор NAC HA пара добавлен как одиночная запись в Профилировщике и передан к виртуальному IP - адресу Сервера NAC.

1. Добавьте новый Коллектор к Профилировщику.Перейдите **к Конфигурации>, Модули Профилировщика NAC> Добавляют Коллектор**.
2. Добавьте новое название Коллектора для Сервера NAC HA Пара. Это может быть чем-либо, что вы хотите, но должны совпасть с конфигурацией Коллектора.Название коллектора: **CAS-OOB-Pair1**IP-адрес: **192.168.97.10** (виртуальный адрес Сервера NAC)Соединение: Оставьте его как **NONE** на данный момент
3. Настройте свои Сервисные модули Коллектора. Оставьте **NetMap в покое**, и **NetTrap** (конфигурация по умолчанию не необходима).
4. Добавьте **интерфейс NetWatch** (ETH3), который связан с Портом SPAN на коммутаторе распределения.
5. Добавьте **Блок подсети** для модуля NetInquiry для прислушиваний к представляющему интерес трафику, который прибывает из доступов к сети. Будьте определенными в сетях и не облагайте налогом сервер NAC излишне. В этой лабораторной установке это может быть все 192.168.0.0 личного пространства.**Развернутая проверка доступности адресата (ping sweep)** выхода и **Набор DNS** отключены.
6. Настройте Средство передачи, как слушают на IP-адресе 192.168.97.10 (VIP) и порт TCP 31416. Это позволяет Коллектору действовать как сервер и прислушиваться к соединению от Профилировщика к определенному порту.
7. **NetFlow** выхода отключил (так как Netwatch / СЕССИЯ SPAN используется) в Конфигурации NetRelay. Удостоверьтесь, что вы нажимаете кнопку **Save Collector** для сохранения конфигурации.
8. Перейдите **к Вкладке конфигурация>, Применяют Изменения> Модули Обновления**.

Настройте коллектор NAC

Эта конфигурация должна быть выполнена точно, как находится на обоих устройствах.

1. SSH к Коллектору и входу в систему как **root**.
2. Введите **сервисный config коллектора** и пробегите сценарий конфигурации для устанавливания части Коллектора 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` Коллектор NAC настроен.

3. Запустите сервисы коллектора.`[root@NAC Server1 ~]# service collector start`

Настройте коммутатор доступа для передачи trap-сообщений SNMP к коллектору NAC

Эта конфигурация позволяет Профилировщику динамично получать все новые устройства, которые соединяются с портом коммутатора всюду по сети.

Примечание: Можно было также заполнить конфигурацию уже для обычной конфигурации NAC. Если так, все, что необходимо сделать, добавляет Коллектор CAS как хост в конфигурации SNMP для получения trap-сообщений SNMP, когда новые устройства соединяются с switchports.

Консоль/Telnet в коммутатор (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
```

Настройте коммутатор доступа на профилировщике для сбора сведений SNMP

Следуйте этим инструкциям для настройки коммутатора доступа на Профилировщике для сбора сведений SNMP.

1. Перейдите к GUI Профилировщика: **Конфигурация> Сетевые устройства> Добавляет Устройство**.
2. Добавьте имя хоста и управление IP-адресами коммутатора.
3. Введите строки SNMP только для чтения, настроенные в коммутатор. Удостоверьтесь, что выбрали модуль сопоставления Коллектора NAC, таким образом, Коллектор выбран к SNMP, опрашивают коммутатор доступа каждый час и передают информацию Профилировщику.
4. **Нажмите Add Устройство** и **Примените Изменения**. Обновите модули от левой области GUI.**Примечание:** Доступ для чтения-записи не необходим для Профилировщика NAC в развертываниях NAC, так как Менеджер NAC уже управляет устройством. Могут быть конфликты и дополнительные издержки к коммутаторам когда необязательно.

Настройте порт коммутатора ETH3 коллектора NAC на коммутаторах распределения для SPAN

Примечание: Это позволяет Модулю NetWatch прислушиваться к трафику в сети и передавать информацию Профилировщику. Удостоверьтесь, что вы не превышаете намеченную сумму интерфейса Коллектора NAC. Это имеет ограничение 1GB/sec. Получите интерфейсы или VLAN коммутатора в зависимости от вашей модели коммутатора и версии кода.

Примечание: Минимально, вы хотите видеть запросы DHCP и предложения от оконечных точек на ваших коммутаторах доступа. Если это не возможно, включите Коллектор NAC или около серверов DHCP в вашей сети.

Настройте сеанс монитора на коммутаторе распределения.

```
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
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

- Удостоверьтесь, что Профилировщик и Коллектор связываются и работают. Если они не, вы не видите информации об устройствах в вашей сети. Если существуют проблемы, не продолжайтесь, пока все Модули Коллектора и Сервер не работают.На Профилировщике перейдите **к Конфигурации> Модули Профилировщика NAC> Модули Профилировщика NAC Списка**.
- Проверьте, что коммутатор доступа может передать trap-сообщения уведомления нового MAC к Коллектору.**Примечание:** Будьте осторожны, когда вы будете включать отладку и будете знать ее опасности.`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`
- Проверьте, что Профилировщик получил новый MAC-адрес от Коллектора.Перейдите **к Консоли Оконечной точки>, Просматривают/Управляют Оконечные точки> Оконечные точки Показа Портами устройства> Разгруппированный> Таблица Устройств> (Выберите коммутатор)**.
- Проверьте, что Коллектор опросил SNMP коммутатор.

1. Посмотрите на столбец **Last Scan**. Это проверяет, что Коллектор просмотрел коммутатор каждые 60 минут по умолчанию.
2. **Debug SNMP** снова на CLI коммутатора.
3. От GUI Профилировщика перейдите **к Конфигурации> Сетевые устройства> Сетевые устройства Списка> (Выберите устройство)**.
4. Нажмите **Query Now**.
5. Наблюдайте выходные данные отладки на коммутаторе для Коллектора к опросу SNMP коммутатор.`*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. Проверьте, что SPAN работает на коммутатор, и Коллектор может получить трафик.SSH профилировщику NAC.Введите **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. Наблюдайте выходные данные на экране. Если вы обеспокоены суммой выходных данных, можно передать выходные данные по каналу к файлу на Коллекторе NAC. См. главные страницы в Linux.
8. Проверьте, видите ли вы трафик DHCP об оконечных точках на вашем коммутаторе.Перейдите **к GUI Профилировщика>, Консоль Оконечной точки> Просматривает/Управляет Оконечные точки**. Нажмите профиль; нажмите устройство и нажмите данные оконечной точки.Вы видите информацию о Классе поставщика DHCP устройства, перехваченного от трафика NetWatch/SPAN на Коллекторе:

Поддержка конфигурации NTP

Профилировщик NAC поддерживает конфигурацию NTP только с версией 3.1 и позже. Это позволяет настраивать различные варианты для временных серверов через управляемый с помощью меню веб-интерфейс. См. Настраивать NTP на Cisco NAC Profiler Сервер разделяют для завершенных подробных данных.

Если версия Профилировщика NAC прежде 3.1, то вы не можете настроить NTP, потому что версия 2.1.8 Профилировщика NAC не имеет возможности сделать это через веб-интерфейс. См. Открытые Предупреждения, упомянутые в Комментариях к выпуску версии 2.1.8 Профилировщика NAC. Для получения дополнительной информации обратитесь к идентификатору ошибки Cisco CSCsu46273 (только зарегистрированные клиенты).

Можно настроить то же вручную через CLI. Выполните следующие действия:

1. От Сеанса SSH до Профилировщика, CD к / и т.д., и редактируют ntp.conf файл.
2. Добавьте серверы подходящего времени в этом файле.
3. Настройте зону времени синхронизации.`mv /etc/localtime /etc/localtime-old`
   `ln -sf /usr/share/zoneinfo/<your_time_zone> /etc/localtime`

Дополнительные сведения

- Cisco NAC Appliance (Clean Access)
- Cisco Systems – техническая поддержка и документация