既存のアウトオブバンド NAC への NAC Profiler の導入

目次

概要

この導入ガイドでは、アウトオブバンド（OOB）のキャンパス導入内に Cisco NAC Profiler Server と Cisco NAC Profiler Collector（Cisco NAC アプライアンス Clean Access Server にある）を実装する方法について説明します。 このドキュメントでは、Cisco NAC Profiler を既存の OOB 高可用性 NAC 環境に導入する最適な方法について説明します。 また Cisco NAC アプライアンスと統合された Cisco NAC Profiler ソリューションの基本機能とトポロジの理解も目的としています。 また、すべての NAC レス デバイスのエンドポイント情報が Collector から Profiler Server にどのように送信されるかについて理解することも目的としています。 ソリューションの目的は、適切なポリシーを適用するため、エンドポイントをプロファイルし、それらを Cisco NAC アプライアンスの Clean Access Manager（CAM）のデバイス フィルタ リストに追加することです。

前提条件

要件

まず始めに、各製品の『インストールと設定のガイド』に従って、Cisco NAC Manager、Cisco NAC Server、および Cisco NAC Profiler を設定する必要があります。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- NAC Manager（192.168.96.10 HA サービス IP）
- NAC Server（192.168.97.10 HA サービス IP）
- NAC Profiler（192.168.96.21）
- 3560 アクセス スイッチ（192.168.100.35）
- 3750 ディストリビューション スイッチ（192.168.97.1）

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

NAC Profiler の概要

Cisco NAC Profiler を利用すれば、ネットワーク管理者は、適切なネットワーク アクセスを確保し維持するために、デバイス タイプに関わりなく、接続されたすべてのネットワーク エンドポイントの機能を、特定、検索、および決定することによって、さまざまなスケールおよび複雑度のエンタープライズ ネットワーク内の Network Admission Control（NAC）を効率的に配置および管理できます。 Cisco NAC Profiler は、エージェントレスのエンドポイントをプロファイリングする特定のタスクをもつネットワークに接続されている、すべてのエンドポイントを発見、カタログ化、およびプロファイリングするシステムです。

NAC の概要

Cisco Network Admission Control（NAC）アプライアンス（Cisco Clean Access と呼ぶこともあります）は、使いやすく強力なアドミッション コントロールおよび準拠性強制ソリューションです。 包括的なセキュリティ機能、インバンドまたはアウトオブバンドの配置オプション、ユーザ認証ツール、帯域およびトラフィックのフィルタリング制御機能を備えた Cisco NAC アプライアンスは、ネットワークを制御して保護するための完全なソリューションです。 Cisco NAC アプライアンスは、ネットワークの集中アクセス管理ポイントとして、セキュリティ、アクセス、コンプライアンス ポリシーを一箇所で導入できるため、ネットワークを通じて多くのデバイスにポリシーを伝播する必要はありません。

設定

構成ガイドの概要

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

図 1 のダイアグラムは、すべてのディストリビューション スイッチに高可用性（HA）NAC Server を使用した、基本的なレイヤ 2 キャンパス環境を示しています。 Profiler Server と NAC Manager は同じ管理ネットワーク上に配置でき、NAC Server および Collector からの情報を送受信できます。 Cisco NAC Profiler が 非 NAC リモート エンドポイントを検出する方法はいくつかあり、このガイドでは最も一般的で推奨される方法を説明します。 この構成ガイドでは、以下を実現する方法を説明します。

- アクセス スイッチと NAC Collector 間の SNMP 通信を追加する。
- アクセス レイヤ デバイスからのすべてのトラフィックをキャプチャする、中でも DHCP ベンダー クラス情報のエンドポイントに関する属性に最も関心があるため、具体的にはエンドポイントからの DHCP トラフィックについてキャプチャするため、ディストリビューション スイッチの SPAN ポートを設定する。
- Collector により収集されるすべての情報を受信するため、Cisco NAC Profiler Server と Collector の通信を適切に設定する。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

図 1： Cisco NAC Profiler と OOB Cisco NAC アプライアンスの導入

設定

このドキュメントでは、アウトオブバンド ソリューションの NAC Profiler および Collector を設定するため、次の設定を使用します。

- OOB トポロジの NAC Profiler の設定
- NAC Collector の設定
- NAC Collector に SNMP トラップを送信するためのアクセス スイッチの設定
- SNMP 情報を収集するための Profiler のアクセス スイッチの設定
- SPAN 用ディストリビューション スイッチ上 NAC Collector の ETH3 スイッチポートの設定

アウトオブバンド ソリューションの NAC Profiler および Collector の設定

- NAC Server は標準の NAC HA セットアップを通して設定する必要があります。
- Collector は Profiler との通信に NAC Server の仮想 IP アドレスを使用します。
- NAC Collector HA ペアは Profiler に 1 つのエントリとして追加され、NAC Server の仮想 IP アドレスと通信します。

1. 新しい Collector を Profiler に追加します。[Configuration] > [NAC Profiler Modules] > [Add Collector] に移動します。
2. NAC Server HA ペアの新しい Collector 名を追加します。 この名前は自由に設定できますが、Collector の設定と一致させる必要があります。Collector 名： **CAS-OOB-Pair1**IPアドレス **192.168.97.10**（NAC Server の仮想アドレス）Connection: 当面の間、これは [NONE] のま

まにしておきます
3. Collector サービス モジュールを設定します。 [NetMap] と [NetTrap] のみのままにします（デフォルトの設定は必要ありません）。
4. ディストリビューション スイッチ上の SPAN ポートに接続する [NetWatch interface]（ETH3）を追加します。
5. アクセス ネットワークからの対象トラフィックをリッスンするため、NetInquiry モジュールの [subnet Block] を追加します。 ネットワークで固有にし、NAC server に不必要に負荷をかけないようにします。 このラボ設定では、完全な 192.168.0.0 のプライベート スペースです。[Ping Sweep] と [DNS Collection] は無効のままにします。
6. フォワーダを IP アドレス 192.168.97.10（VIP）および TCP ポート 31416 でリッスンするように設定します。 これにより、Collector がサーバのように動作し、Profiler から特定のポートへの接続をリッスンすることができます。
7. NetRelay 設定で、[NetFlow] を無効のままにします（Netwatch /SPAN セッションが使われるため）。 設定を保存するため、[Save Collector] ボタンをクリックします。
8. [Configuration tab] > [Apply Changes] > [Update Modules] に移動します。

NAC Collector の設定

この設定は、両方のデバイスでこのとおりに実行する必要があります。

1. Collector に SSH し、**root** としてログインします。
2. **service collector config** と入力し、設定スクリプトを実行して NAC Collector 部分を設定します。

```
[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
```

NAC Collector が設定されました。

3. Collector サービスを起動します。

```
[root@NAC Server1 ~]# service collector start
```

NAC Collector に SNMP トラップを送信するためのアクセス スイッチの設定

この設定により、ネットワーク全体でスイッチポートに接続するすべての新しいデバイスを Profiler が動的に受信できます。

注: また、すでに 標準 NAC 設定で入力された設定もあります。 その場合、するべきことは、新しいデバイスがスイッチポートに接続されると SNMP トラップを受信するよう、CAS Collector をホストとして SNMP 設定に追加するだけです。

スイッチ (nac-3560-access#) へのコンソール/Telnet。

```
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
```

SNMP 情報を収集するための Profiler のアクセス スイッチの設定

SNMP 情報を収集するよう、Profiler のアクセス スイッチを設定するには、次の手順に従います。

1. Profiler GUI： [Configuration] > [Network Devices] > [Add Device] に移動します。
2. スイッチのホスト名と管理 IP アドレスを追加します。
3. スイッチに設定されている読み取り専用の SNMP 文字列を入力します。 NAC Collector マッピング モジュールを必ず選択してください。これにより、SNMP がアクセス スイッチを毎時ポーリングし、その情報を Profiler に転送するよう、Collector が選択されます。
4. [Add Device] と [Apply Changes] をクリックします。 GUI の左側のペインからモジュールを更新します。**注:** NAC Manager が既にデバイスを制御しているため、NAC 環境で NAC Profiler に読み取り/書き込みアクセスは必要ありません。 これが不要な場合、これによりスイッチに競合や余分なオーバーヘッドが生じる場合があります。

SPAN 用ディストリビューション スイッチ上 NAC Collector の ETH3 スイッチポートの設定

注: これにより、NetWatch モジュールが Profiler へのネットワーク トラフィックおよび転送情報をリッスンできるようになります。 NAC Collector のインターフェイスをオーバーサブスクライブしないようにします。 これには 1GB/秒の制限があります。 スイッチのモデルとコードのバージョンに応じて、スイッチのインターフェイスまたは VLAN をソースします。

注: 少なくとも、アクセス スイッチのエンドポイントからの DHCP 要求とオファーも見たいはずです。 これが不可能な場合、ネットワークの DHCP サーバ上またはその近くに NAC Collector を追加します。

ディストリビューション スイッチのモニタ セッションを設定します。

```
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
```

確認

ここでは、設定が正常に動作していることを確認します。

- Profiler と Collector が通信し、動作していることを確認します。 これが確認できない場合、ネットワーク上のデバイスに関する情報を一切見ることができません。 問題がある場合、すべての Collector モジュールとサーバが動作するまで次に進まないでください。Profiler で、[Configuration] > [NAC Profiler Modules] > [List NAC Profiler Modules] に移動します。
- アクセス スイッチが Collector に新しい MAC 通知トラップを送信できることを確認します。 **注:** デバッグを有効にする場合、注意し、その危険を理解しておいてください。

```
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
```

- Profiler は Collector から新しい MAC アドレスを受け取ったことを確認します。[Endpoint Console] > [View/Manage Endpoints] > [Display Endpoints by Device Ports] > [Ungrouped] > [Table of Devices] > (スイッチを選択) に移動します。
- Collector がこのスイッチに SNMP ポーリングしたことを確認します。

1. [Last Scan] 列を確認します。 ここから、Collector がデフォルトで 60 分ごとにスイッチをスキャンしたことを確認できます。
2. スイッチ CLI で再度、[Debug SNMP] を実行します。
3. Profiler GUI から、[Configuration] > [Network Devices] > [List Network Devices] > (デバイスを選択) に移動します。

4. [Query Now] をクリックします。
5. スイッチのデバッグの出力で、Collector がそのスイッチを SNMP ポーリングしていることを確認します。

```
*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. スイッチで SPAN が機能し、Collector がトラフィックを受信できることを確認します。NAC Profiler に SSH します。**tcpdump – i eth3** と入力します。

```
*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
```

7. 画面の出力を確認します。 出力量が心配な場合、出力を NAC Collector のファイルに保存できます。 Linux のメイン ページを参照してください。
8. スイッチのエンドポイントに関する DHCP トラフィックを表示できるかどうかを確認します。[Profiler GUI] > [Endpoint Consol]e > [View/Manage Endpoints] に移動します。 プロファイルをクリックし、 デバイスをクリックし、エンドポイント データをクリックします。Collector の NetWatch/SPAN トラフィックからキャプチャしたデバイスの DHCP ベンダー クラス情報が表示されます。

NTP の設定サポート

NAC Profiler は、バージョン 3.1 以降でのみ NTP 設定をサポートします。 また、メニュー ベースの Web インターフェイスを使用して、タイム サーバのさまざまなオプションを設定することができます。 詳細については、「Cisco NAC Profiler Server の NTP 設定」セクションを参照してください。

NAC Profiler バージョンが 3.1 以前の場合、NTP を設定できません。NAC Profiler バージョン 2.1.8 には Web インターフェイス経由でこれを実行する機能がないためです。 NAC Profiler バージョン 2.1.8 のリリース ノートに記載されている「Open Caveats」を参照してください。 詳細については、Cisco Bug ID CSCsu46273（登録ユーザ専用）を参照してください。

CLI から手動で同じ設定ができます。 次の手順を実行します。

1. Profiler への SSH セッションから、cd to /etc を実行し、ntp.conf ファイルを編集します。
2. このファイルに適切なタイミング サーバを追加します。
3. クロック タイム ゾーンを設定します。

```
*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
```

関連情報

- シスコ NAC アプライアンス (Clean Access)
- テクニカル サポートとドキュメント – Cisco Systems