在现有的带外NAC中配置NAC性能分析器

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[背景信息](#)
[美洲台仿形铣床概述](#)
[美洲台概述](#)
[配置](#)
[配置指南概述](#)
[网络图](#)
[配置](#)
[配置美洲台仿形铣床和收集器在一带外解决方案](#)
[配置美洲台收集器](#)
[配置接入交换机发送SNMP陷阱到美洲台收集器](#)
[配置在仿形铣床的接入交换机收集SNMP信息](#)
[配置美洲台收集器的ETH3 Switchport在分布式交换机的SPAN的](#)
[验证](#)
[NTP的配置的支持](#)
[相关信息](#)

简介

此部署指南描述如何实现Cisco NAC Profiler服务器和Cisco NAC Profiler收集器(查找在Cisco NAC设备Clean Access服务器)在带外(OOB)校园部署。本文描述如何最佳部署在一现有OOB高性能的美洲台部署的Cisco NAC Profiler。打算帮助您了解Cisco NAC Profiler解决方案的基本功能和拓扑集成与Cisco NAC设备。它也帮助您知道关于所有美洲台少的设备的终端信息如何从收集器发送到仿形铣床服务器。解决方案的目标是描出终端和添加他们到Cisco NAC设备Clean Access管理器(CAM)的设备过滤器列表为了应用相应的策略。

先决条件

要求

您必须首先配置您的思科美洲台管理器、思科美洲台服务器和Cisco NAC Profiler符合每种产品的安装和配置指南。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 美洲台管理器(192.168.96.10 HA服务IP)
- 美洲台服务器(192.168.97.10 HA服务IP)
- 美洲台仿形铣床(192.168.96.21)
- 3560接入交换机(192.168.100.35)
- 3750分布式交换机(192.168.97.1)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

美洲台仿形铣床概述

Cisco NAC Profiler高效地部署和设法在多种缩放和复杂性企业网络的网络准入控制(NAC)的enable (event)网络管理员由识别、所有连接的网络终端的功能的位置和确定，不管设备类型，为了保证和维护适当的网络访问。Cisco NAC Profiler是发现的系统，目录和配置文件所有终端连接对与描出代理程序少的终端特定任务的网络。

美洲台概述

思科网络准入控制(美洲台)设备(亦称思科Clean Access)是一次强大，易用准入控制和标准实施解决方案。使用全面的安全功能，带内或带外部署选项、用户认证工具和带宽和流量过滤控制， Cisco NAC设备是控制和获取网络的完整的解决方案。作为您的网络的中央访问管理点， Cisco NAC设备在一个地方让您实现安全，访问和标准策略而不是必须传播在网络中的策略在许多设备。

配置

配置指南概述

本部分提供有关如何配置本文档所述功能的信息。

在图1的图表显示一基本层2校园部署用在分布式交换机间的高性能的(HA)美洲台服务器。仿形铣床服务器和美洲台管理器能坐同一个管理网络和发送和获得从美洲台服务器和收集器的信息。有几个方式Cisco NAC Profiler能发现非美洲台远程终点，并且此指南描述最普通和推荐的方法。此配置指南描述如何完成这些：

- 到/从接入交换机添加SNMP通信到美洲台收集器。
- 因为我们是对关于终端的DHCP供应商类信息属性感兴趣配置分布式交换机的SPAN端口捕获从接入层设备的所有流量，特别地从终端的DHCP流量。
- 相应地配置Cisco NAC Profiler服务器和收集器通信获得收集器收集的所有信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

图 1：OOB Cisco NAC设备部署用Cisco NAC Profiler

配置

本文使用这些配置配置美洲台仿形铣床和收集器在一带外解决方案：

- 配置OOB拓扑的美洲台仿形铣床
- 配置美洲台收集器
- 配置接入交换机发送SNMP陷阱到美洲台收集器
- 配置在仿形铣床的接入交换机收集SNMP信息
- 配置美洲台收集器的ETH3 Switchport在分布式交换机的SPAN的

配置美洲台仿形铣床和收集器在带外解决方案

- 美洲台服务器需要通过正常美洲台HA设置配置。
- 收集器使用美洲台服务器的虚拟IP地址与仿形铣床联络。
- 美洲台收集器HA对被添加作为在仿形铣床的单个条目并且被传达对美洲台服务器的虚拟IP地址。

1. 添加一个新的收集器到仿形铣床。去**Configuration>美洲台仿形铣床模块>Add收集器**。
2. 添加一新的收集器名称对于美洲台服务器HA对。这可以是您想要，但是必须匹配收集器配置的任何。收集器名称：**CAS-OOB-Pair1**IP 地址：**192.168.97.10** (美洲台服务器的虚拟地址)连接：暂时留下它作为**无**
3. 配置您的收集器服务模块。不理会的**NetMap**和的**NetTrap** (配置默认情况下不是必要的)。
4. 添加连接到分布式交换机的SPAN端口的一个**NetWatch接口**(ETH3)。
5. 添加NetInquiry模块的一**子网块**细听来自访问网络的关注数据流。是特定在网络，并且请勿不必要地纳税美洲台服务器。在此实验室设置，它可以是整个192.168.0.0私有空间。事假**查验清扫**和禁用的**DNS收藏**。
6. 配置转发器和侦听在IP地址192.168.97.10 (VIP)和TCP端口31416。这允许收集器作为服务器和细听从仿形铣床的一连接到特定端口。
7. 留给**Netflow**禁用(因为使用Netwatch /SPAN会话)在NetRelay配置里。确保您点击**保存收集器**按钮保存配置。
8. 去**Configuration选项>应用更改>更新模块**。

配置美洲台收集器

此配置需要正确地运行和在两个设备。

1. 对收集器和登录的SSH作为**根**。
2. 类型**服务收集器设置**和运行通过设置美洲台收集器部分的配置脚本。

```
[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
```

美洲台收集器配置。

3. 开始收集器服务。

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

配置接入交换机发送SNMP陷阱到美洲台收集器

此配置允许仿形铣床动态地接收所有连接对在网络中的一switchport的新建的设备。

注意： 您能也有为您的正常美洲台配置已经填充的配置。如果那样，您需要执行的所有是添加CAS收集器作为一台主机在您的SNMP配置方面收到SNMP陷阱，当新的设备连接到连接孔时。

控制台/Telnet到交换机(nac-3560-access#)里。

```
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
```

配置在仿形铣床的接入交换机收集SNMP信息

遵从这些说明配置在仿形铣床的接入交换机收集SNMP信息。

1. 去仿形铣床GUI ：**Configuration>网络设备>Add设备**。
2. 添加交换机的主机名和管理IP地址。

3. 输入在交换机配置的只读SNMP字符串。确保选择美洲台收集器映射模块，因此收集器选择对SNMP投票接入交换机每个小时并且寄信息给仿形铣床。
4. 单击**添加设备**并且**应用更改**。更新从GUI的左边窗格的模块。**注意：** 因为美洲台管理器已经，控制设备读写访问为在美洲台部署的美洲台仿形铣床不是需要的。当不是必要的时，可以有冲突和额外的开销到交换机。

配置美洲台收集器的ETH3 Switchport在分布式交换机的SPAN的

注意： 这允许NetWatch模块细听在网络的流量和转发信息到仿形铣床。确保您不过度预定美洲台收集器的接口。它有限制关于1GB/sec。根据您的交换机型号和编码版本来源交换机的接口或VLAN。

注意： 最低限度地，您要发现DHCP请求和提供从终端在您的接入交换机。如果这不是可能的，请添加一个美洲台收集器在或在您的网络的DHCP服务器附近。

配置分布式交换机的一个监控会话。

```
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
```

验证

使用本部分可确认配置能否正常运行。

- 确保仿形铣床和收集器通信和运行。如果他们不是，您看不到关于设备的所有信息在您的网络。如果有问题，请勿继续，直到所有收集器模块和服务器运行。在仿形铣床上，去**Configuration>美洲台仿形铣床模块>列表美洲台仿形铣床模块**。
- 验证接入交换机能发送新MAC通知陷阱到收集器。**注意：** 小心，当您启用调试时，并且认识其危险。

```
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
```

- 验证仿形铣床接收从收集器的新的MAC地址。去**终端Console>视图/由设备端口>设备的未分组的>表管理终端>显示终端> (请选择交换机)**。
- 验证收集器SNMP轮询了交换机。

1. 查看**最后扫描**列。这验证默认情况下收集器扫描了交换机每60分钟。
2. 再**调试SNMP**在交换机CLI。
3. 从仿形铣床GUI，请去**Configuration>网络设备>列表网络设备> (请选择设备)**。
4. **当前**单击**查询**。
5. 观看在交换机的debug输出收集器SNMP投票的交换机。

```
*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. 验证在交换机和收集器的SPAN工作能收到流量。对美洲台仿形铣床的SSH。类型**tcpdump – i eth3**。

```
*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. 观看在屏幕的输出。如果关注相当数量输出，您能管道传送输出到在美洲台收集器的一个文件。参考Linux的主页。
8. 证实您是否能看到关于终端的DHCP流量在您的交换机。去**仿形铣床GUI >终端Console>视图/管理终端**。点击配置文件;点击设备，并且点击终端数据。您看到DHCP从在收集器的NetWatch/SPAN流量捕获的设备的供应商类信息：

NTP的配置的支持

NAC仿形铣床支持NTP仅配置与版本3.1和以上。它准许通过一个项目单取使的Web接口配置时间服务器的不同的选项。参考在Cisco NAC Profiler服务器部分的配置NTP关于完整详细信息。

如果NAC仿形铣床版本是在3.1前，则您不能配置NTP，因为NAC仿形铣床版本2.1.8没有功能通过Web接口执行它。参考在NAC仿形铣床版本2.1.8版本注释提及的打开警告。欲知更多信息，参考Cisco Bug ID CSCsu46273 (仅限注册用户)。

您能通过CLI手工配置同样。完成这些步骤：

1. 从仿形铣床的一SSH会话，对/etc的cd，和编辑ntp.conf文件。
2. 添加在此文件的适当时间时间服务器。
3. 配置时钟时间区域。

```
*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
```

相关信息

- Cisco NAC Appliance (Clean Access)
- 技术支持和文档 - Cisco Systems