第3层带外NAC 性能分析器和NAC 服务器收集器配置指南

目录

简介

本文描述如何实现美洲台在第3层带外部署的仿形铣床和美洲台服务器收集器。如果部署在高可用性(HA)的美洲台服务器，则仅一个收集器是活跃的，并且其他在待机。如果不执行HA，您能分开添加在仿形铣床的每个收集器和有作为收集器运行的两个美洲台服务器。此指南在HA服务器部署反射。

先决条件

要求

此指南的需求是您根据每种产品的安装和配置指南配置您的美洲台管理器、美洲台服务器、美洲台仿形铣床和网络基础设施。

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
- 美洲台服务器
- 美洲台仿形铣床
- 3750分布式交换机
- 3750个远程站点接入交换机
- 2800远程站点路由器
- 3800分布式路由器

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。

美洲台仿形铣床概述

Cisco NAC Profiler高效地部署和设法在变化的缩放和复杂性企业网络的网络准入控制(NAC)的enable (event)网络管理员所有连接的网络终端的功能的识别、位置和决断力，不管设备类型，为了保证和维护适当的网络访问。Cisco NAC Profiler是发现的一个agentless系统，目录和配置文件所有终端连接对网络。

美洲台概述

思科网络准入控制(美洲台)设备，亦称是思科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需要传播策略在网络中在许多设备。

部署指南概述

在图1，有作为第3层带外设备的实施点的一简单远程站点部署用中央HA美洲台服务器。美洲台仿形铣床和美洲台管理器坐同一个管理网络并且发送并且获得从服务器和收集器的信息。也有通过在数据中心或核心层的SPAN获取关于设备的重要DHCP信息的一个独立收集器。有几个方式发现远程终点，并且此指南在您的部署可帮助您。没有打算是一个必须指南，然而显示您如何可以使用在收集器的每个模块，并且终端数据如何由仿形铣床看到做出您的描出的决策。

美洲台服务器收集器使用提供必须和可选工具的列表。

必须收集器模块

NetTrap —此模块细听新MAC通知或林克Up/Down通知的交换机发送的SNMP陷阱。此模块发送所有对仿形铣床的新建的MAC地址描出的。此功能每在Snmp-server配置line命令的交换机定义在Cisco IOS。

NetMap —此模块坐收集器并且对执行设备SNMP轮询负责在远程分支机构的在计时的间隔。在图1中图表， CAS1a收集器SNMP轮询远程交换机和路由器对于特定MIB信息与读访问对交换机。此?提供事类似MAC地址给端口信息，接口，链接状态， dot1x信息，系统信息等等。

NetWatch (SPAN) — NetWatch模块在交换机的SPAN端口能侦听和送回被咽下的数据流信息到仿形铣床。美洲台服务器要求在每个美洲台服务器的一额外接口收集数据。因为仿形铣床主要根据设备和若干其他应用流量匹配，通过的DHCP信息这是重要的。

可选收集器模块

您能使用SPAN或Netflow。它是至部署和用户要求，但是一个在美洲台服务器只推荐由于发送对收集器模块和其他美洲台功能美洲台服务器必须执行的流量总量。您也丢失关于设备的更加重要的信息性片段有Netflow的类似DHCP供应商信息， URL目的地，网络客户端信息， Web服务器信息等等。

NetRelay — (Netflow)在a的每个路由器配置每接口上，并且目的地是美洲台服务器的管理IP地址。Netflow代理程序坐美洲台服务器并且解析根据您的交通规则和网络的NetFlow信息配置在仿形铣床。

NetInquiry —这是根据您的事的被动和激活机制类似TCP开放端口。例如美洲台服务器执行SYN/ACK然后切连接为了轮询一个特定子网范围或范围开放TCP端口的。如果有答复，发送信息到仿形铣床用轮询的IP地址和TCP端口。

注意： 对于NetInquiry，只请添加不能在Netflow或NetWatch到达或看到的特定子网或主机。NetInquiry能超载您的美洲台服务器与额外处理和硬件资源类似内存和CPU利用率，如果没适当地配置。请使用此功能作为最后一招。

注意： 如果有一个独立收集器您能启用Netflow和SPAN在同一个设备，但是确保不过度预定收集器。

图 1

配置

在第3层OOB拓扑里配置美洲台仿形铣床

- 美洲台服务器需要通过正常美洲台HA设置配置。
- 美洲台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通信对CAS的虚拟IP地址。

图 2

配置设置

完成这些步骤：

1. 仿形铣床需要新的美洲台收集器的*客户端连接*。
2. 仿形铣床需要坐接近分配的独立设备的*服务器连接*|数据中心|服务层在网络图中。
3. 选择**Configuration>美洲台仿形铣床模块–列出美洲台仿形铣床模块**然后单击**Server选项**。移动到下面页并且单击**添加连接。图 3**
4. 输入HA收集器的服务IP地址和密钥关键信息并且单击**添加连接。图 4**
5. 单击再**添加连接。图 5图 6**
6. 输入**IP地址**为了配置独立收集器连接的*服务器连接*。
7. 当您执行为了有上一步Server Configuration页时，请单击**编辑连接**。
8. 点击在Server Configuration页的**更新服务器。图 7**

添加两个新的收集器到仿形铣床。完成这些步骤：

1. 选择**Configuration>美洲台仿形铣床模块>Add收集器。图 8**
2. 添加一新的收集器名称对于美洲台服务器HA对。这可以是您在收集器配置希望，但是必须匹配的任何。收集器名称— CAS-OOB-Pair1IP地址192.168.97.10 (NAC服务器的虚拟地址)连接—暂时留下它作为**无**。您能以后更改此到是侦听模式的服务器连接。
3. 单击**添加收集器按钮。图 9**
4. 配置您的收集器服务模块。不理会的NetMap和的NetTrap。**图 10**
5. 添加一个NetWatch接口(eth3)，连接到分布式交换机的SPAN端口。**图 11**
6. 添加NetInquiry模块的一子网块为了细听来自访问网络的关注数据流。不必要地是特定在网络至于不是税款美洲台服务器。在此实验室设置，它可以是全部的192.168.0.0私有空间。**图 12注意：** 事假查验清扫和禁用的DNS收藏。请使用此作为最后一招。查验清扫和DNS集触发ping和nslookups在范围您在网络块部分放置的IP子网。没有推荐这和很少使用。
7. 配置转发器侦听在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TCP端口。这在服务器配置的最初的少数步骤反射。
8. 收集器对的以启用NetFlow。（可选）因为Netflow从远程路由器通过由于没有远程收集器，您能执行此此处。
9. 输入远程站点的IP地址块如表示。在本例中，使用全部的192.168.0.0私有空间。**图 13**
10. 点击**保存收集器**为了保存您的配置。

添加另外的独立收集器到仿形铣床

完成这些步骤：

1. 单击**添加收集器。图 14**
2. 收集器名称可以是您希望的任何。在本例中，它是CAS2。
3. 转发器IP地址是本身。eth0的IP地址是为管理。在本例中，它是192.168.97.12。连接应该是仿形铣床的IP地址。在这种情况下，它是192.168.96.21。
4. 单击**添加收集器。图 15**
5. 在此以后，您给收集器配置页带来。在前面部分的完整步骤5 – 9。这允许您修改和添加独立收集器的唯一IP地址和配置设置。
6. 独立收集器的一唯一设置是能力添加多个接口对NetWatch配置。您能添加几个接口，因此您能为DHCP、DNS和IP电话看到流量从远程终点。
7. 配置您的设置的NetWatch接口。在本例中，三个接口被添加了到在独立收集器的SPAN流量。**图 16**
8. **注意：** 选择**Configuration>应用更改>更新模块**为了保存您的设置。

配置在美洲台服务器的美洲台收集器模块

注意： 此配置在所有需要运行收集器。

此配置允许仿形铣床和收集器传达和建立安全连接关于设备的信息开始流。完成这些步骤：

1. SSH或控制台收集器的和登录作为**根**从控制台或**信标**从SSH会话。
2. 输入**config命令服务的收集器**。
3. 通过配置脚本运行为了设置美洲台收集器部分。**HA收集器示例**收集器设置作为*服务器连接*连接类型：`[root@cas1 ~]#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) [cas1]: CAS-OOB-Pair1 Network configuration to connect to a
NAC Profiler Server Connection type (server/client) [server]: Listen on IP [192.168.97.10]:
```
您询问输入NP的IP地址。这是必要配置此收集器访问控制表使用的。如果NP是一个HA对的一部分，则您必须包括每独立NP和虚拟IP实际IP地址保证适当的连接一旦故障切换。输入美洲台仿形铣床的IP地址。
```
(Finish by typing ‘done’) [127.0.0.1]: 192.168.96.20  (Real IP address of  NAC Server1)
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 Server)
Enter the IP address(es) of the NAC Profiler.
(Finish by typing ‘done’) [done]: 192.168.96.22 (Real IP of NAC Server2)
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 CAS-OOB-Pair1-fw
•Configured CAS-OOB-Pair1-nm
•Configured CAS-OOB-Pair1-nt
•Configured CAS-OOB-Pair1-nw
•Configured CAS-OOB-Pair1-ni
•Configured CAS-OOB-Pair1-nr

NAC Collector has been configured.
```
4. 开始收集器服务。
```
[root@cas1 ~]#service collector start
```
突出单独收集器示例
```
[root@cas2 ~]#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) [cas2]: Network configuration to connect to a NAC Profiler Server Connection type (server/client) [client]: Connect to IP [192.168.96.21]: Port number [31416]: Encryption type (AES, blowfish, none) [none]: Shared secret []: -- Configured cas2-fw -- Configured cas2-nm -- Configured cas2-nt -- Configured cas2-nw -- Configured cas2-ni -- Configured cas2-nr NAC Collector has been configured. [root@cas2 ~]#service collector start
```

配置远程访问交换机发送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switchport的新建的设备通过MAC通知陷阱。因为在拓扑里有IP电话和PC连接对相同端口，这是特别重要。

控制或远程登录到交换机(nac-3750-access#)。

```
snmp-server community cleanaccess RW snmp-server community profiler RO snmp-server enable traps mac-notification snmp-server host 192.168.96.10 version 2c cleanaccess snmp-server host 192.168.97.10 version 1 profiler
```

配置在仿形铣床的远程访问交换机SNMP信息收集的

完成这些步骤：

1. 选择**仿形铣床GUI > Configuration>网络设备>Add设备。图 18**
2. 添加交换机的主机名和管理IP地址。
3. 并且请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和转发对仿形铣床的信息。
4. 单击**添加设备**并且**应用更改**为了更新从GUI的左边窗格的模块。**图 19**

配置仿形铣床的远程访问路由器SNMP信息收集的

这允许第3层IP地址对在仿形铣床数据库绑定的MAC。

1. 选择**仿形铣床GUI > Configuration>网络设备>Add设备**。**图 20**参见图21。
2. 添加路由器的主机名和管理IP地址。
3. 并且请输入在路由器配置的只读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和转发对仿形铣床的信息。
4. 单击**添加设备**并且**应用更改**为了更新从GUI的左边窗格的模块。**图 21**

配置美洲台收集器收到在他们的本地交换机的SPAN流量

注意： 这允许NetWatch模块开始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1个GB/sec。您能来源交换机的接口或VLAN，并且那取决于您的交换机型号和编码版本。

注意： 您最低限度地要发现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，尝试添加一个美洲台收集器在或在您的网络的DHCP服务器附近。这在此配置指南执行。

完成这些步骤：

1. 配置分布式交换机的#1一个监控会话流入的远程站点和流出流量的：`monitor session 1 source interface F0/0`
   `monitor session 1 destination interface Gi1/0/44`
2. 配置分布式交换机的#2一个重复的监控会话流入的远程站点和流出流量的：`monitor session 1 source interface F0/0`
   `monitor session 1 destination interface Gi1/0/44`
3. 配置独立收集器的另一个监控会话。此示例监控是重要的几个接口连接对核心交换机。这些是DHCP、DNS和Cisco CallManager服务器此实验室设置的。`monitor session 1 source interface G1/0/7-9`
   `monitor session 1 destination interface G1/0/48`

在主要站点配置远程访问路由器发送NetFlow数据到收集器

完成这些步骤：

1. 对远程路由器的Telnet。
2. 全局以启用NetFlow。`ip flow-export version 5`
   `ip flow-export destination 192.168.97.12 2055`**注意：** 收集器在Netflow的UDP端口2055侦听。发送Netflow的IP地址总是收集器管理IP地址。
3. 在接口的以启用NetFlow。`interface FastEthernet0/1`
   `ip address 192.168.121.1 255.255.255.0`
   `ip flow ingress`
   `ip route-cache flow`

验证

请参阅故障排除程序部分为了确认您的配置适当地工作。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

故障排除

本部分提供的信息可用于对配置进行故障排除。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

故障排除步骤

完成以下步骤，对配置进行故障排除。

1. 确保仿形铣床，并且收集器通信并且运行。如果他们不是，则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。在仿形铣床上，请选择**Configuration>美洲台仿形铣床模块>列表美洲台仿形铣床模块**。
2. 验证接入交换机发送新MAC通知陷阱到收集器。小心，当您启用调试时，并且您应该认识其危险。`nac-3750-access#debug snmp packet nac-3750-access#debug snmp header`
3. 验证收集器有轮询交换机的SNMP ：查看最后扫描列。
4. 再调试SNMP在交换机。
5. 从仿形铣床，请选择**Configuration>网络设备**。选择列出**网络设备**然后选择**设备**。
6. 点击**查询**。
7. 观看在交换机的debug输出收集器的对SNMP轮询交换机：`*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***`
8. 接通您的在交换机的IP电话或发出**然后关闭的no shut命令**在接口：
```
15w4d: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/4, changed state to down
15w4d: %ILPOWER-5-POWER_GRANTED: Interface Gi1/0/4: Power granted
15w4d: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/4, changed state to up
15w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed state to up
15w4d: SNMP: Queuing packet to 192.168.97.12
15w4d: Outgoing SNMP packet
15w4d: v2c packet
15w4d: community string: profiler
15w4d: SNMP: V2 Trap, reqid 14430, errstat 0, erridx 0
 sysUpTime.0 = 949829672
 snmpTrapOID.0 = cmnMacChangedNotification
 cmnHistMacChangedMsg.0 =
01 00 79 00 07 50 C6 82 27 00 04 00
```
9. 验证收集器发送一个新的陷阱要求接收的MAC地址：
```
15w4d: SNMP: Packet received via UDP from 192.168.97.11 on Vlan120
15w4d: SNMP: Get request, reqid 1576567642, errstat 0, erridx 0
 system.1.0 = NULL TYPE/VALUE
 ifIndex.10104 = NULL TYPE/VALUE
 ifDescr.10104 = NULL TYPE/VALUE
 ifType.10104 = NULL TYPE/VALUE
 ifSpeed.10104 = NULL TYPE/VALUE
 ifPhysAddress.10104 = NULL TYPE/VALUE
 ifAdminStatus.10104 = NULL TYPE/VALUE
 ifOperStatus.10104 = NULL TYPE/VALUE
 ifName.10104 = NULL TYPE/VALUE
 dot1xAuthAuthControlledPortStatus.10104 = NULL TYPE/VALUE
 dot1xAuthAuthControlledPortControl.10104 = NULL TYPE/VALUE
paeMIBObjects.2.4.1.9.10104 = NULL TYPE/VALUE

-------snip ----------
```

```
ifIndex.10104 = 10104
 ifDescr.10104 = GigabitEthernet1/0/4
 ifType.10104 = 6
 ifSpeed.10104 = 100000000
 ifPhysAddress.10104 = 00 14 A8 2E A5 04
 ifAdminStatus.10104 = 1
 ifOperStatus.10104 = 1
 ifName.10104 = Gi1/0/4
 dot1xAuthAuthControlledPortStatus.10104 = 1
 dot1xAuthAuthControlledPortControl.10104 = 3
15w4d: SNMP: Packet sent via UDP to 192.168.97.11
```

10. 验证仿形铣床接收IP电话的新的MAC地址从收集器的：选择**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**然后选择您的交换机。
11. 验证在交换机的SPAN工作，并且收集器接收流量。`SSH to the NAC Profiler : Type : 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)` 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。请参阅在Linux的联机资料关于怎样执行此。
12. 确认关于IP电话终端的DHCP流量是否通过SPAN端口被看到了并且发送至仿形铣床。选择**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**然后选择您的交换机。然后请选择您的设备**MAC地址**。点击**视图配置文件数据**。您应该看到DHCP从从在收集器的NetWatch/SPAN流量捕获的设备的供应商类信息。此信息能来自DHCP服务器或DHCP提供在SPAN端口回到客户端，取决于您的路由和环境。
13. 验证Netflow从收集器的管理接口的远程路由器通过。`NAC-2800-Remote#`**`show ip flow export`** `Flow export v5 is enabled for main cache Exporting flows to 192.168.97.12 (2055) Exporting using source IP address 10.0.0.2 Version 5 flow records 2602429 flows exported in 554968 udp datagrams 0 flows failed due to lack of export packet NAC-2800-Remote#`**`show ip flow top 10 aggregate source-address`** 有四位高级健谈的人：

    ```
    IPV4 SRC-ADDR         bytes        pkts        flows
    ===============  ==========  ==========  ==========
    192.168.122.60           44           1           1
    192.168.122.59           88           2           2
    192.168.121.90          367           3           3
    10.0.0.1              19320         322           1
    ```
14. 验证从收集器的仿形铣床接收Netflow。选择您的远程MAC或终端IP并且查看被描出的数据：选择**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**然后选择您的交换机。然后请选择您的设备MAC地址。点击**视图配置文件数据**。在输出中，您看到目的地流量对IP 192.168.70.50和目的地端口2000年。这是Cisco CallManager的IP地址，并且目的地端口2000年使用SCCP控制流量。

相关信息

- 技术支持和文档 - Cisco Systems