配置实用工具用户指南

CA Application Delivery Analysis

10.1

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA Application Delivery Analysis
- CA GigaStor
- CA GigaStor 连接器
- CA Multi-Port Monitor
- CA Performance Center
- CA NetQoS Performance Center
- CA Standard Monitor
- CA Virtual Systems Monitor

联系技术支持

要获取在线技术帮助以及办公地址、主要服务时间和电话号码的完整列表，请联系技术支持：http://www.ca.com/worldwide。

目录

第 1 章： 概述

配置实用工具识别镜像到监控设备的 TCP 会话。通常，当您不确定流经您的网络的通信量时，此信息便非常有用。例如，按以下类型查找感兴趣的通信量：

- 服务器子网
- 服务器 VLAN
- 客户端网络

当您查找所需的通信量时，请将服务器和网络定义导出到 CA ADA 控制台并开始监控该通信量。配置实用工具不创建用户定义的应用程序。

运行该配置实用工具的位置

CA ADA 安装程序将配置实用工具 ConfigurationUtility.exe 安装在 <ADA 主目录>\bin 文件夹中。根据监控通信量的位置，您运行该配置实用工具的位置会有所不同。从以下位置监控时：

管理控制台

在管理控制台上运行该配置实用工具。

Standard Monitor

在标准监视器上运行该配置实用工具。

Multi-Port Monitor

在管理控制台上运行该配置实用工具。

大量通信量可能由 Multi-Port Monitor 发送到配置实用工具，因此两台计算机的位置应该保持最近距离。

Cisco NAM

在管理控制台上从 Cisco NAM 打开数据包捕获文件。

GigaStor

在管理控制台上从 GigaStor 打开数据包捕获文件。

交换机端口镜像要求

为了检测服务器和客户端之间的应用程序端口通信量，配置实用工具必须能够查看 SYN-ACK 数据包。用于确认客户端请求的 SYN-ACK 数据包从 TCP 会话的服务器端发出。配置实用工具必须查看 SYN-ACK 数据包，才能在其应用程序、服务器和网络列表中显示相应的 TCP 会话数据。

如果配置实用工具仅显示服务器端通信量（例如，“传出服务器的字节数”而非“传入服务器的字节数”），则您的路由可能不对称。TCP 会话的一个方向未流经您镜像的端口，便发生了*不对称路由*。为了正确监视应用程序的 TCP 响应时间，您可能需要将更多源端口镜像到监视设备，可能从观测 TCP 会话的客户端的冗余交换机镜像。

数据包捕获文件要求

要在 Cisco NAM 或 GigaStor 上配置数据收集，配置实用工具需要您从在监控设备上获取的数据包捕获文件加载网络、服务器和应用程序数据。在与数据包捕获文件一起使用时：

- 配置实用工具要求数据包捕获文件采用 NA (DOS) 格式。不支持 BNF 格式。使用能够转换捕获文件格式的任何实用工具可以采用 NA Sniffer (DOS) 格式保存文件。
- 为了防止与 CA ADA 数据包驱动程序发生冲突，请不要在 CA ADA 管理控制台或标准监视器上安装数据包捕获实用工具（如 *WireShark*）。

要准备数据包捕获文件 **遵循这些步骤:**：

1. 在 Cisco NAM 或 CA GigaStor 上，进行数据包捕获，将结果保存到文件中，然后将该文件下载到您的本地计算机。

   如果您在 CA GigaStor 上进行数据包捕获，则可以使用 CA Observer Expert 为 SYN 和 SYN-ACK 数据包创建筛选规则，以仅捕获基于服务器的通信。有关使用 CA Observer Expert 的更多信息，请参阅 CA Observer Expert 帮助。
2. 使用能够转换捕获文件格式的任何实用工具可以打开数据包捕获文件，然后采用 NA Sniffer (DOS) 格式保存文件。
3. 要确认捕获文件为 NA Sniffer (DOS) 格式，请检查该文件的第一行以 TRSNIFF 数据开头。在命令提示符下，键入以下命令，然后按 Enter 键：
   `type <文件名>.cap | more`
4. 将 NA Sniffer (DOS) 格式的数据包捕获文件复制到计划安装该配置实用工具的计算机。

启动配置实用工具

在您启动配置实用工具之前，请注意：

- 您启动配置实用工具时，监控设备上的数据收集暂时停止。例如，当您在 Standard Monitor 上运行一小时配置工具时，在该监视设备收集的数据中就会有一个小时的缺口。
- 要加载数据包捕获文件，配置实用工具要求 NA (DOS) 格式的数据包捕获文件。
- 不使用时请关闭该配置实用工具，以减少资源消耗。

遵循这些步骤:

1. 在管理控制台或 CA Standard Monitor 计算机上，浏览到 <ADA 主目录>\bin 文件夹并双击 ConfigurationUtility.exe。

   配置实用工具登录屏幕会自动检测管理控制台的 IP 地址。

2. 如果您正在配置 CA Standard Monitor 上的数据收集：
   a. 管理控制台和 CA Standard Monitor 的 IP 地址会自动填充。
   b. 如果为监控配置了多个 NIC，例如要监视不对称通信量，请选中“All Adapters”复选框，以便监测所有 NIC 上的通信量。此选项不适用于 CA Multi-Port Monitor。
   c. 单击“Start Detection”。
3. 如果您正在为 CA Multi-Port Monitor 配置数据收集：
   a. 在“Console”字段中，验证管理控制台的 IP 地址。
   b. 在“Collector IP”字段中，指定 CA Multi-Port Monitor 的 IP 地址。
   c. 单击“Start Detection”。
   d. 选择您要配置的逻辑端口，然后单击“OK”。
4. 如果您正在为 Cisco NAM 或 CA GigaStor 配置数据收集，请验证管理控制台的 IP 地址，并加载从设备获取的数据包捕获文件：
   a. 单击“Load Capture File”。
   b. 在“Browse”对话框中，指定 NA Sniffer (DOS) 格式的数据包捕获文件的位置，然后单击“OK”。
   c. 在配置实用工具登录屏幕中，单击“Process File”。
5. 在配置实用工具临时禁用监控设备上的数据收集时会向您发出报警。
6. 单击“确定”。
7. 在配置实用工具中，单击“Refresh”菜单显示检测到的网络、服务器和应用程序。配置实用工具不自动刷新列表。

8. 现在您已做好查找感兴趣通信量的准备工作。

状态信息

配置实用工具底部的状态栏提供了有用的信息。状态：

已连接

指示实用工具是否已连接以及连接到了哪个管理控制台。

正在侦听

指示正在监视的本地适配器的 IP。

检测到的组合和数据包

（仅 SPAN 数据）表示当前观测到的客户端/服务器/端口组合的数目。在您想确定监控是否正在观测 SPAN 数据时，此信息很有用。在读取数据包捕获文件时，组合计数不会变化。

立即

指示当前时间。

上次刷新时间

指示上次刷新以便使用累积的数据更新显示的时间。

启动时间

指示实用工具上次启动或重新启动的时间。

第 2 章： 查找感兴趣的通信量

通过筛选应用程序、服务器和网络的列表来查找相关条目，以查找感兴趣的通信量。例如，按以下条件筛选：

应用程序

显示相关服务器和网络。

服务器

显示相关应用程序和客户端网络。

网络

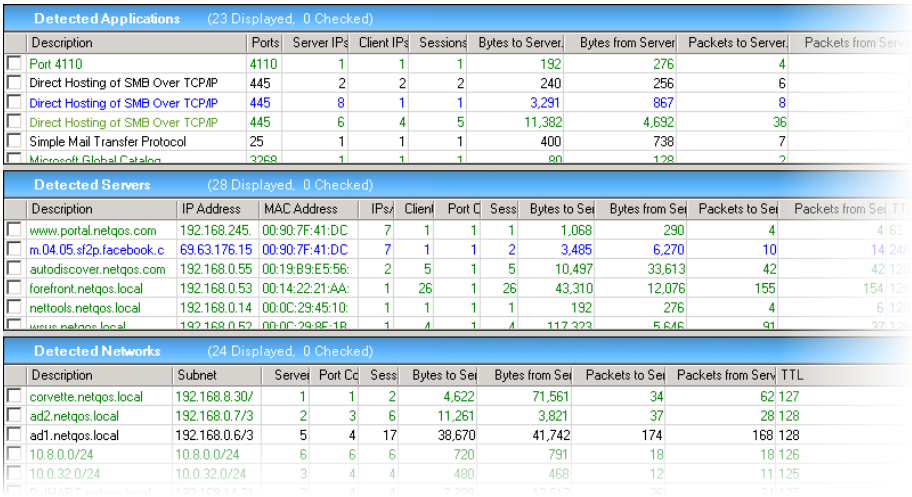
显示相关服务器和应用程序。

了解列表

单击“Refresh”显示当前检测到的网络、服务器和应用程序。配置实用工具不自动刷新列表。

彩色编码的条目列表指示应用程序、服务器和网络条目的状态。在以下示例中，CA ADA 不监控通信量。

重要说明！如果“Bytes From”或“Bytes To”列为 0，这可能表示 TCP 从交换机端口镜像的方式有问题。



Detected Applications (23 Displayed, 0 Checked)

Description	Ports	Server IPs	Client IPs	Sessions	Bytes to Server	Bytes from Server	Packets to Server	Packets from Serv
Port 4110	4110	1	1	1	192	276	4	
Direct Hosting of SMB Over TCP/IP	445	2	2	2	240	256	6	
Direct Hosting of SMB Over TCP/IP	445	8	1	1	3,291	867	8	
Direct Hosting of SMB Over TCP/IP	445	6	4	5	11,382	4,692	36	
Simple Mail Transfer Protocol	25	1	1	1	400	738	7	
Microsoft Global Catalog	3268	1	1	1	80	128	2	

Detected Servers (28 Displayed, 0 Checked)

Description	IP Address	MAC Address	IPs/	Client	Port C	Sess	Bytes to Ser	Bytes from Ser	Packets to Ser	Packets from Ser	TT
www.portal.netqos.com	192.168.245.	00:90:7F:41:DC	7	1	1	1	1,068	290	4	4	63
m.04.05.sf2p.facebook.c	69.63.176.15	00:90:7F:41:DC	7	1	1	2	3,485	6,270	10	14	246
autodiscover.netqos.com	192.168.0.55	00:19:B9:E5:56:	2	5	1	5	10,497	33,613	42	42	128
forefront.netqos.local	192.168.0.53	00:14:22:21:AA:	1	26	1	26	43,310	12,076	155	154	128
nettools.netqos.local	192.168.0.14	00:0C:29:45:10:	1	1	1	1	192	276	4	6	128
wsus.netqos.local	192.168.0.52	00:0C:29:8F:1B	1	4	1	4	117,323	5,646	91	37	128

Detected Networks (24 Displayed, 0 Checked)

Description	Subnet	Server	Port Cc	Sess	Bytes to Ser	Bytes from Ser	Packets to Ser	Packets from Serv	TTL
corvette.netqos.local	192.168.8.30/	1	1	2	4,622	71,561	34	62	127
ad2.netqos.local	192.168.0.7/3	2	3	6	11,261	3,821	37	28	128
ad1.netqos.local	192.168.0.6/3	5	4	17	38,670	41,742	174	168	128
10.8.0.0/24	10.8.0.0/24	6	6	6	720	791	18	18	126
10.0.32.0/24	10.0.32.0/24	3	4	4	480	468	12	11	125

状态：

未配置（黑色）

指示配置实用工具在监视设备或数据包捕获文件中检测到了条目，但是配置实用工具或管理控制台中不存在该条目的定义。请使用配置实用工具为条目配置定义。

已在管理控制台中配置（绿色）

表明 CA ADA 中存在该条目的定义。要编辑服务器或网络定义，请使用 CA ADA 控制台。

已在配置实用工具中配置（蓝色）

表明配置实用工具（而非管理控制台）中存在该条目的定义。请使用配置实用工具编辑条目定义。

请注意，如果未配置的服务器与已配置的（绿色）应用程序使用同一端口进行，该应用程序端口将出现两次：一次是作为已配置（绿色）条目，另一次是作为未配置（黑色）条目。对“Detected Applications by Port”列表进行排序，查找任何重复的端口条目。

刷新列表

然而，配置实用工具报告来自交换机端口的镜像通信量，您必须手动刷新列表才能显示当前状态。

如果应用程序、服务器或网络消失或其数据量减少，这可能是由于一个或多个服务器超出了“Maximum IPs/MAC”阈值引起的。来自那些服务器的统计不针对其关联的应用程序和网络同行而计算，如果降低到零，可能引起总计减少或完全消失。可以将“Maximum IPs/MAC”筛选调高或调为“All”，以便再次显示这些条目。

在您加载数据包捕获文件并刷新视图之后，配置实用工具将显示数据包捕获文件的内容。您不需要再次刷新视图。

遵循这些步骤:

- 单击“Refresh”菜单。

详细信息：

状态信息 (p. 10)

隐藏已定义的条目

隐藏已定义的条目，可以更轻松地浏览应用程序、服务器和网络的列表。

重要说明！隐藏条目后，您无法创建服务器或网络定义。如果您隐藏了所有条目，确保将它们显示出来。

要筛选：

所有应用程序、服务器和网络条目

- 依次单击“View”、“All”、“Display All”，以删除筛选并显示所有条目。要创建定义，必须将视图配置为显示所有应用程序、服务器和网络条目。
- 依次单击“View”、“All”>“Ignore Configured”，以显示所有未配置（黑色）的条目。不会显示任何已在“配置实用工具”中配置的（蓝色）条目或已在管理控制台中配置的（绿色）的条目。
- 依次单击“View”、“All”>“Configured Only”，以显示在配置实用工具中配置（蓝色）或在管理控制台中配置（绿色）的所有条目。不显示未配置条目（黑色）。

按应用程序、服务器或网络条目

- 依次单击“View”、“Applications|Servers|Networks”、“Display All”，以显示所有应用程序、服务器或网络条目。
- 依次单击“View”、“Applications|Servers|Networks”、“Ignore Configured”，以显示所有未配置（黑色）的应用程序、服务器或网络条目。不会显示任何已在“配置实用工具”中配置的（蓝色）条目或已在管理控制台中配置的（绿色）的条目。
- 依次单击“View”、“Applications|Servers|Networks”、“Configured Only”，以显示在配置实用工具中配置（蓝色）或在管理控制台中配置（绿色）的所有应用程序、服务器或网络条目。不显示未配置条目（黑色）。

筛选条件

“Detection Criteria”组显示应用于当前视图的筛选条件。

应用程序筛选

筛选依据:

- 单个端口 (80)。要筛选特定应用程序端口，您还可以在“Detected Applications”列表中右键单击，然后单击“Apply description (port) as Application Filter”。
- 端口范围 (1024-2000)。

服务器筛选

筛选依据:

- 单个 IP 地址 (192.168.0.10)。要筛选特定服务器，您还可以在“Detected Servers”或“Detected Networks”列表中右键单击，然后单击“Apply description (IP) as Server Filter”。
- IP 地址范围 (192.168.0.0-192.168.0.255)。
- 子网 (192.168.0.0/24)。

  在筛选标记的 VLAN 通信量时，将“Group By Mask for the Server Filter”设置为对应某特定 VLAN 的服务器子网。或者，将“Group By Mask to Server (/32)”设置为显示所有标记的 VLAN 通信量。

“Maximum IPs/MAC”筛选出来自共享相同 MAC 地址的服务器的数据。高比率表明服务器可能位于路由器的另一端，并且不应当由 CA ADA 监视。此比率显示在“Detected Servers”面板上的“IP/MAC”列中。在列表顶端提供了一个“All”值，此值可用于关闭该筛选。

如果以前可见的检测到的应用程序、服务器或网络在后来刷新时消失了，则很可能是与该数据关联的服务器超过了“Maximum IPs/MAC”筛选。

网络筛选

筛选依据:

- 单个 IP 地址 (192.168.0.10)。要筛选特定网络，您还可以在网络或服务器列表中右键单击，然后单击“Apply description (IP) as Network Filter”。
- IP 地址范围 (192.168.0.0-192.168.0.255)。
- 子网 (192.168.0.0/24)。

“Group By Mask”定义了如何将检测到(但非已配置)的客户端 IP 组织到子网中。例如，假定检测到 3 个客户端 IP（192.168.0.2、192.168.1.3 和 192.168.1.23），且“Group By Mask”设置为 24。这些 IP 将被组织到 2 个网络 192.168.0.0/24 (192.168.0.2) 和 192.168.1.0/24（192.168.1.3 和 192.168.1.23）中。

筛选应用程序

应用程序是某个 TCP 端口或端口范围上的请求和响应的集合。配置实用工具会自动检测服务器上的端口通信量，并在“Detected Applications”窗格中显示应用程序端口。

在应用程序端口上应用“Application”筛选可确定具有访问这些端口的网络的服务器。例如，通过筛选端口可显示关联的服务器和网络的列表。

可以单击列标题来对此列表进行排序。

说明

显示应用程序端口的名称。如果您看到同一应用程序名称同时列为已配置的应用程序（绿色）和未配置的应用程序（黑色），则服务器在该应用程序端口上有通信量，但它未由 CA ADA 监视。

“Bytes To”和“Bytes From”，以及“Packets To”和“Packets From”

显示通信量最多的应用程序。作为最佳实践，我们建议监控最繁忙的应用程序。

遵循这些步骤:

1. 在“Detected Applications”窗格中，右键单击某个端口，然后单击“Apply description (port) as Application Filter”。

   如果您要按端口范围筛选应用程序，则在“Application Filter detection criteria”字段中键入端口范围（如 60-80），并按 Enter 键。

2. （可选）将网络或服务器定义添加到 CA ADA 中。

详细信息：

定义服务器 (p. 20)
定义网络 (p. 21)

筛选网络

网络是指代表特定位置或用户逻辑组的 IP 地址范围或一个 IP 地址。配置实用工具会自动检测客户端 IP，并根据当前的“Group By Mask”设置，在“Detected Networks”窗格中进行显示。例如，如果将“Group By Mask”设置为 24，则配置实用工具将未配置的客户端 IP 分组到 /24 网络。

在筛选网络时，我们建议对 /24 网络进行筛选。定义 /24 客户端网络（有 1 个地区）可以启用“Users”上的 QoS 报告，以列出网络中的实际客户端 IP。要查看针对某个特定 /24 网络检测到的客户端 IP，请对需要的 /24 网络应用网络筛选，然后将“Group By Mask”设置为 32。

单击列标题可对网络列表进行排序。

“Bytes To”和“Bytes From”，以及“Packets To”和“Packets From”

显示通信量最多的网络。作为最佳实践，我们建议监控最繁忙的网络。

TTL

显示从网络中的所有客户端到所有查看的服务器的存在时间 (TTL) 值。与服务器 TTL 值不同，被监视的网络可以具有（而且通常具有）不同的非默认值。

使用筛选来保证感兴趣的网络：

网络筛选

列出客户端网络访问的服务器和端口。例如，对某个客户端网络应用网络筛选，可将该网络添加到“Network Filter”条件中，并显示关联的服务器和应用程序端口的列表。

服务器筛选

列出服务器子网上的所有应用程序。例如，应用服务器筛选 192.168.0.0/16，可显示该服务器子网上的服务器和应用程序。

遵循这些步骤:

1. 在“Detected Networks”窗格中，右键单击某个网络，然后单击“Apply network (network) as Network Filter ”或“Apply network (network) as Server Filter ”。

   如果要按 IP 范围或子网筛选服务器，请在“Server Filter detection criteria”字段中键入 IP 范围或子网并按 Enter 键。

2. （可选）将网络或服务器定义添加到 CA ADA 中。

筛选服务器

服务器是网络中响应客户端 TCP 请求的计算机。配置实用工具检测 SYN-ACK 数据包，并在“Detected Servers”窗格中自动显示相应的服务器。

我们建议定义服务器子网以监控服务器通信量。

可以单击列标题来对此列表进行排序：

“Bytes To”和“Bytes From”，以及“Packets To”和“Packets From”

将服务器和最大通信量等同。作为最佳实践，我们建议监控最繁忙服务器上的应用程序。如果“Bytes From”或“Bytes To”列为 0，这可能表示 TCP 数据包被镜像到监控设备的方式有问题。

VLAN

识别标记的服务器 VLAN 通信量。

在筛选标记的 VLAN 通信量时，将“Group By Mask for the Server Filter”设置为对应某特定 VLAN 的服务器子网。或者，将“Group By Mask to Server (/32)”设置为显示所有标记的 VLAN 通信量。

TTL

表示从服务器到客户端的观察到的生存时间 (TTL) 值。在理想配置中，被监视的服务器直接跨接到监控，并且此值应当为未减小的默认 TTL 值。128 和 64 分别是 Windows 和 UNIX 服务器上常见的 TTL 值。

如果 TTL 不是默认值，则默认值与该值之差就是服务器与所跨接交换机之间的网络跃点数。作为最佳实践，我们建议监控最靠近所跨接交换机的服务器。使用生存时间 (TTL) 列来查找要监控的感兴趣的候选人。

“Maximum IPs/Mac”和“Group By Mask”

细化筛选结果。通过设置为“All”可查看 SPAN 中的所有服务器，并查找每个 MAC 地址的 IP 地址比率低的服务器。

使用筛选来查找感兴趣的网络：

服务器筛选

列出访问服务器的客户端网络以及访问的应用程序端口。例如，通过对服务器应用服务器筛选，可将该服务器添加到“Server Filter”条件中，并显示关联的应用程序端口和客户端网络的列表。

对于基于 VLAN 的 SPAN (VSPAN)，请使用 VLAN 列查找 SPAN 中的服务器，或使用与具有所需服务器通信量的 VLAN 对应的服务器子网掩码筛选。例如，添加服务器筛选 192.168.0.0/16，可以看到该子网上的所有服务器和应用程序。

网络筛选

指明服务器是否充当另一服务器的客户端以及使用的端口。请记住，为了监视多层应用程序，CA ADA 会自动为每个服务器定义创建 /32 网络。例如，通过对服务器应用网络筛选，可将该服务器添加到“Network Filter”条件中，并显示关联的服务器和应用程序端口的列表。此筛选对于发现多层应用程序很有用。

通过从“Group By Mask”列表中选择所需掩码，可以分组匹配网络。

遵循这些步骤:

1. 在“Detected Servers”窗格中，右键单击某个服务器，然后单击“Apply description (port) as Server Filter”或“Apply description (port) as Network Filter”。

   如果要按 IP 范围或子网筛选服务器，请在“Server Filter detection criteria”字段中键入 IP 范围或子网并按 Enter 键。

2. （可选）将服务器或网络定义添加到 CA ADA 中。

定义服务器

我们建议首先定义最繁忙的服务器。对于基于 VLAN 的 SPAN (VSPAN)，请使用 VLAN 列查找 SPAN 中的服务器，或使用与具有所需服务器通信量的 VLAN 对应的服务器子网掩码筛选，然后排序列表以查找最忙碌的服务器。找到最繁忙的服务器之后，您可以应用服务器筛选，以便找到服务器上与最繁忙的应用程序相对应的应用程序端口。

定义服务器时，我们建议遵循以下命名约定。

服务器类型	推荐的命名约定	示例
单一功能服务器	*DNS 名称* 请注意，CA ADA、CA PC 和 CA NPC 中的许多报告视图附加 IP 地址。	Goliath-196.128.34.1
一个应用程序、场中的多个服务器	*应用程序名称-DNS 名称* 为了帮助您标识应用程序名称，可以应用“Server”筛选来查找相应的应用程序端口。	Citrix-Zeus Citrix-Athena Citrix-Mercury

一个应用程序、多个服务器、多个位置	*应用程序名称-DNS 名称-位置* 为了帮助您标识应用程序名称，可以应用“Server”筛选来查找相应的应用程序端口。	Citrix-Hamlet-NewYork Citrix-Romeo-Milan Citrix-Othello-London

遵循这些步骤:

1. 右键单击“Detected Servers”窗格中的服务器，然后单击“Define Server *description*”。

   要定义一组服务器，请选中需要的每个服务器对应的复选框，然后右键单击服务器并单击“Quick Define Checked Servers”。

2. 单击“Export”、“To Management Console”以将您的更改保存到 CA ADA。

   重要说明！要开始监视新定义，请在 CA ADA 中同步监视器设备。

详细信息：

筛选服务器 (p. 19)

定义网络

定义与环境中的实际客户端子网对应的客户端网络。设置“Group By Mask”以筛选客户端通信量。

定义网络时，我们建议遵循以下命名约定：

网络类型	推荐的命名约定	示例
网络	*位置-说明*	Singapore-backbone
子网	*位置-区域-带宽*	Austin-Subnet10-128k

遵循这些步骤:

1. 在“Detected Networks”窗格中右键单击某个网络，然后单击“Define Network *description*”。

   要定义一组网络，请选择需要的每个网络，然后右键单击某个网络并单击“Quick Define Checked Networks”。

2. 单击“Export”、“To Management Console”以将您的更改保存到 CA ADA。

   重要说明！要开始监视新定义，请在 CA ADA 中同步监视器设备。

详细信息：

筛选网络 (p. 17)

第 3 章： 维护您的配置

我们建议定期使用配置实用工具来识别您网络中的通信量。

第 4 章： 故障排除

本节讨论常见问题。

- 我无法找到 VLAN 标记的通信量。为什么？

  在筛选标记的 VLAN 通信量时，将“Group By Mask for the Server Filter”设置为对应某特定 VLAN 的服务器子网。或者，将“Group By Mask to Server (/32)”设置为显示所有标记的 VLAN 通信量。

- 底部指示器显示检测到了大量数据包，但是配置实用工具未显示任何捕获的数据。为什么？

  这可能由一个或多个服务器超出了“Maximum IPs/MAC”阈值引起。来自这些服务器的统计不针对其关联的应用程序和对应的网络进行计算，这可能会导致总计完全消失。上调“Maximum IPs/MAC”筛选，或者将其调整为“All”，即可显示这些条目。

- 单击“Refresh”后，应用程序、服务器或网络消失，或者数据量减少。这是一个缺陷吗？

  这可能由一个或多个服务器超出了“Maximum IPs/MAC”阈值引起。来自那些服务器的统计不针对其关联的应用程序和网络同行而计算，如果降低到零，可能引起总计减少或完全消失。可以将“Maximum IPs/MAC”筛选调高或调为“All”，以便再次显示这些条目。

- 连接到 CA Multi-Port Monitor 时，为何发生异常？

  尝试将配置实用工具连接到 CA Multi-Port Monitor 时，如果显示以下消息，请关闭配置实用工具、同步监视器设备，然后重新连接配置实用工具：

  ```
  System.Exception: There is already one SuperAgent Configuration Utility request in process.
  ```

  为了避免此问题，当您在 CA Multi-Port Monitor 的逻辑端口上完成对应用程序、服务器和网络的定义后，请确保断开配置实用工具连接，并同步监视设备上的配置，然后再尝试配置另一个逻辑端口。

- 启动配置实用工具时，为何发生异常？

  运行配置实用工具的计算机必须同时承载管理控制台或 CA Standard Monitor，否则将显示以下消息：

  ```
  System.NullReferenceException: Object reference not set to an instance of an object.
  ```

- 如何知道 SPAN 到监控的过程是否存在问题？

  如果“Bytes From”或“Bytes To”列为 0，这可能表示 TCP 数据包被镜像到监控设备的方式有问题。

- 在检测到的网络中如何组织重叠子网？

  假设存在两个网络定义，其子网络分别为 192.168.0.0/16 和 192.168.10.0/24。如果 /24 包含在 /16 内，那么数据是存储在 /24、/16 还是两者中？对于 CA ADA 控制台和配置实用工具，答案都一样：更具体（更高的 /x）的网络定义将获得数据。

  在上一个示例中，192.168.10.0/24 将从范围为 192.168.10.0 到 192.168.10.255 的 IP 获取数据，而 192.168.0.0/16 将从范围为 192.168.0.0 到 192.168.9.255 和 192.168.11.0 到 192.168.255.255 的 IP 获取数据。

  正因为这种“更具体”的子网络数据组织，所以配置实用工具中的首选工作流是定义更具体的密集子网，并逐渐过渡到范围更大（较低的 /x）的子网。如果您首先创建了一个广泛的用户定义子网（如 0.0.0.0/0），那么所有项都将聚合到该条目中，这样，创建更具体的子网就变得很困难。

- 为何无法添加定义或将定义导出到管理控制台？
  - 在实用工具中，无法修改现有的控制台配置条目（绿色）。必须在控制台的用户界面中执行此操作。
  - 仅可以添加检测到但未配置的条目（黑色）。
  - 只能编辑或删除在实用工具中已配置（蓝色）的条目。
  - 应用视图菜单中“All”以外的其他选项时，修改定义和导出到管理控制台功能被禁用。这么做是为了避免配置实用工具与管理控制台发生定义冲突。

  通常，您应当更新客户端网络和服务器子网的列表，以指定您要监视的应用程序通信量。如果 CA ADA 控制台未显示您预期的应用程序通信量，请使用配置实用工具来确认监视设备正在观测应用程序通信量。

详细信息：

交换机端口镜像要求 (p. 8)
运行该配置实用工具的位置 (p. 7)