

思科 ISE 分析设计指南

安全访问操作指南系列

作者：Craig Hysp

日期：2012 年 8 月

目录

解决方案概述.....	5
策略架构和组件.....	5
方案概览.....	6
分析服务要求.....	9
许可.....	9
设备要求.....	9
网络要求.....	10
分析服务全局配置.....	11
ISE 分析全局配置.....	11
配置全球分析设置.....	11
启用 ISE 分析服务.....	11
配置探测功能.....	14
探测功能概述.....	14
探测功能配置.....	15
配置 RADIUS 探测功能.....	16
配置 SNMP 陷阱探测功能.....	21
系统查询.....	27
接口查询.....	27
配置 SNMP 查询探测功能.....	29
DHCP SPAN 探测功能.....	34
DHCP 属性.....	34
配置 DHCP 和 DHCP SPAN 探测功能.....	35
使用 URL 重定向的 HTTP 探测功能.....	44
使用 SPAN 的 HTTP 探测功能.....	44
HTTP 探测功能和 IP 到 MAC 地址绑定要求.....	45
用于客户端调配的 URL 重定向.....	45
用于集中 Web 身份验证的 URL 重定向.....	45
配置 HTTP 探测功能.....	46

配置 DNS 探测功能	58
NetFlow 属性	62
NetFlow 探测功能和 IP 到 MAC 地址绑定要求	63
配置 NetFlow 探测功能	63
NMAP 探测功能扫描操作	71
NMAP 探测功能网络扫描	73
NMAP 探测功能终端扫描	74
NMAP 探测功能和 IP 到 MAC 地址绑定要求	74
配置 NMAP 探测功能	75
设备传感器	83
设备传感器概述	83
设备传感器详细信息	83
为 ISE 分析配置设备传感器	85
配置分析策略	98
分析策略配置概述	98
分析条件	98
配置分析条件	100
分析策略和规则	102
可信度 (CF)	103
例外和 NMAP 操作	106
终端身份组	108
分析和授权策略	112
配置文件转变和授权更改	114
例外操作	115
如果授权策略更改，自动在配置文件转变时发送 CoA	115
分析设计和最佳实践	120
分析设计注意事项	120
探测功能选择最佳实践	123
发现阶段 - 探测功能最佳实践	127
有线网络 - 探测功能最佳实践	128
无线网络 - 探测功能最佳实践	129
分析计划	130

附录 A: 参考	133
Cisco TrustSec 系统:	133
设备配置指南:	133

解决方案概述

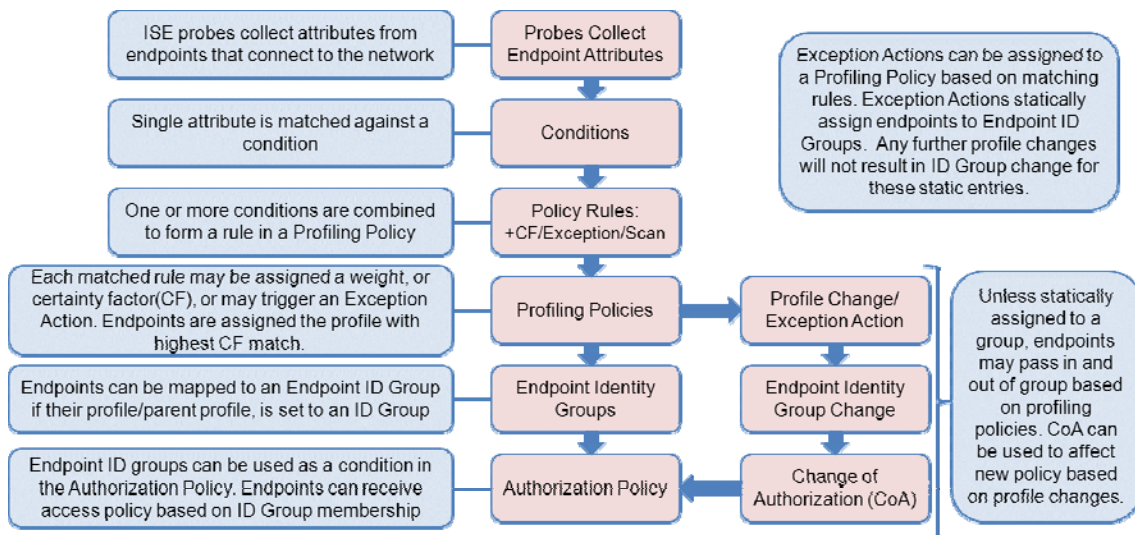
思科 ISE 分析服务对与网络连接的终端提供动态检测和分类。ISE 使用 MAC 地址作为唯一标识符，收集每个网络终端的各种属性，以建立内部终端数据库。分类流程将收集的属性与预置或用户定义的条件进行匹配，然后将这些属性与丰富的配置文件库进行关联。这些配置文件包括各种设备类型，例如移动客户端（iPad、Android 平板电脑、Blackberry 手机等）、桌面操作系统（例如 Windows 7、Mac OS X、Linux 等）和众多非用户系统（例如打印机、电话、摄像头和游戏控制台）。

终端经过分类之后，可获得授权访问网络并根据其配置文件获得访问权限。例如，可以将与 IP 电话配置文件匹配的终端放入使用 MAC 身份验证绕行作为身份验证方法的语音 VLAN。另一个示例是根据所使用的设备向用户提供不同的网络访问权限。例如，当员工从其公司工作站访问网络时，可以获得完全访问权限。但是，当员工从个人 iPhone 访问网络时，就只能获得有限网络访问权限。

策略架构和组件

图 3 重点介绍思科 ISE 分析服务的一般策略架构和关键组件。配置过程从在运行策略服务角色的 ISE 设备上启用特定探测功能开始。ISE 设备具有各种探测功能，负责收集不同类型的终端属性。这些属性将与各种条件进行匹配，随后相关条件将与设备类型库或配置文件库中的各种规则进行匹配。每个匹配条件都会根据通用权重比例分配得到不同的权重或可信度 (CF)，其中可信度是表示相应条件对按照具体配置文件进行设备分类的影响的相对值。虽然这些条件可能会与多个配置文件匹配，但系统只会将累计 CF 最高的终端所对应的配置文件分配给相应终端。

图 1. ISE 分析策略架构和组件



要使配置文件支持 ISE 授权策略，管理员必须通过简单选择复选框来配置配置文件，以创建匹配身份组。通过这个过程，可以终端身份组的形式将配置文件选为授权策略中的条件。

由于还会收集到新属性或之前收集的属性被覆盖，配置文件也会相应变化。分析策略变化也会导致其变化。在有些情况下，可能会自动发生转变 - 例如从通用 HP 设备转变为 HP-Color-LaserJet-4500 等更加具体的配置文件。在其他情况下，管理员可能需要执行专门的操作，以例外操作的形式绕过默认策略。通过例外操作可以将终端静态分配给具体分析策略，从而使进一步的属性收集或关联不会影响配置文件和所分配的可选身份组。

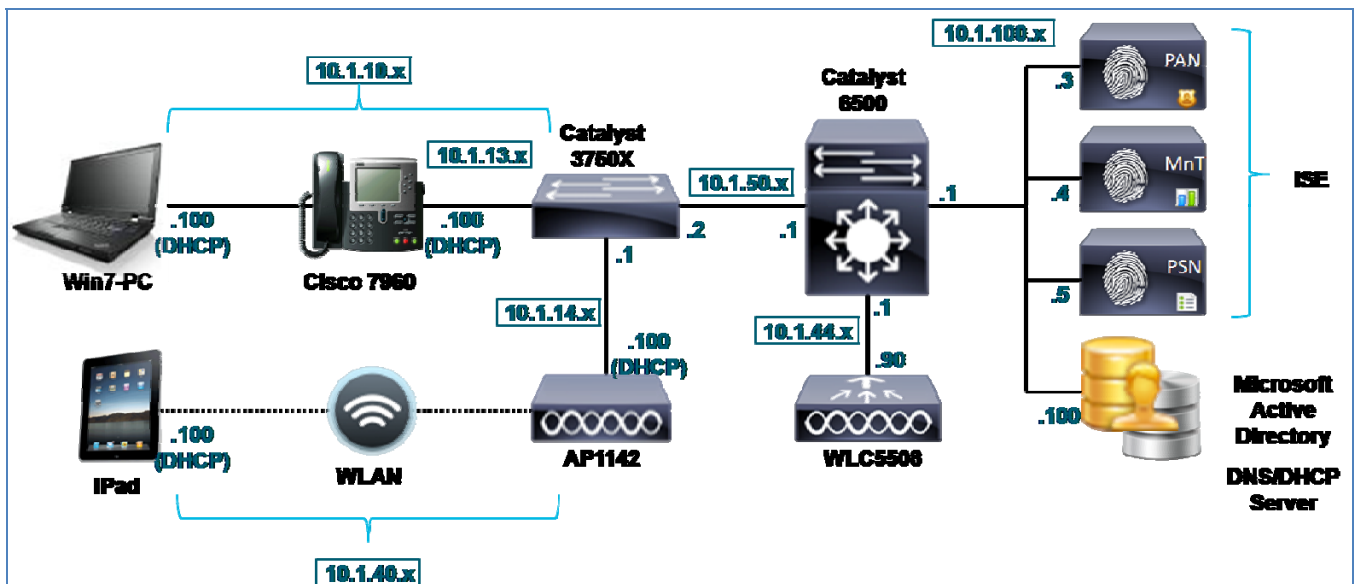
在上述各种情况（配置文件转变和例外操作）下，可能都需要允许 ISE 根据新的配置文件分配对终端执行新的访问策略。通过 RADIUS 授权更改 (CoA) 可在 ISE 中完成此任务。通过向终端所连接的接入设备发送 CoA 请求，ISE 可以要求按照身份验证和授权策略重新评估主机。

方案概览

网络拓扑

图 4 显示本指南中使用的网络拓扑的概况。虽然图 1 中描述的所有方案都是 TrustSec 整体架构的组成部分，但是本文档将只重点介绍适用于分析服务的有线和无线用户方案。由于缺乏必需的 VPN 网关的 MAC 地址信息，无法关联分析数据与唯一终端，远程访问 VPN 使用案例目前不支持 ISE 分析服务。

图 2. ISE 分析拓扑



组件

表 1 列出本指南编写过程中使用的硬件和软件。

表 1. 经过测试的 Cisco TrustSec 2.0 系统组件

组件	硬件	经过测试的特性	软件版本
思科身份服务引擎 (ISE)	运行 VMware ESXi4.1 的思科 UCS C200 M2 服务器	集成 AAA、策略服务器和分析服务	思科 ISE 软件版本 1.1.1 (基本和高级功能许可证)
Cisco Catalyst 3000 系列交换机	Cisco Catalyst 3560 系列	基本身份功能，包括 MAC 身份验证绕行 (MAB)、本地 Web 身份验证 (LWA)、集中 Web 身份验证 (CWA)、802.1X 身份验证和授权更改 (CoA)。 分析支持服务，包括简单网络管理协议 (SNMP)、RADIUS、动态主机配置协议 (DHCP) 中继和 URL 重定向。	思科 IOS [®] 软件版本 12.2(55)SE3 (IP Base)
	Cisco Catalyst 3750-X 系列	基本身份功能，包括 MAB、LWA、CWA、802.1X 身份验证和 CoA。 分析支持服务，包括 SNMP、RADIUS、DHCP 中继、URL 重定向和设备传感器。	思科 IOS 软件版本 15.0(1)SE2 (IP Base)
Cisco Catalyst 6000 系列交换机	Cisco Catalyst 6500 系列管理引擎 720 策略功能卡 3A (PFC3A)	分析支持服务，包括 Cisco NetFlow 版本 5 和版本 9 导出、DHCP 中继，以及交换端口分析器/远程交换端口分析器 (SPAN/RSPAN)。	思科 IOS 软件版本 12.2(33)SXJ2 (高级 IP 服务)

组件	硬件	经过测试的特性	软件版本
思科无线局域网控制器 (WLC)	思科 5508 无线局域网控制器	基本身份功能，包括 MAB、LWA、CWA、802.1X 身份验证和 CoA。 分析支持服务，包括 SNMP、RADIUS、DHCP 中继和 URL 重定向。	思科统一无线网络软件版本 7.2.103.0
思科无线接入点	Cisco Aironet® 轻型接入点 1142N	根据配置文件属性，使用 MAB 和授权策略对终端进行身份验证。	思科轻型接入点软件版本 12.4(25e)JA
思科 IP 电话	思科统一 IP 电话 7960	根据配置文件属性，使用 MAB 和授权策略对终端进行身份验证。	思科 IP 电话 7940 和 7960 固件版本 8.1(1.0)
工作站	VMware Guest	根据配置文件属性，使用 MAB、LWA、CWA 和 802.1X 以及授权策略对终端进行身份验证。	Windows 7
平板电脑	Apple iPad (G1)	根据配置文件属性，使用 MAB、LWA、CWA 和 802.1X 以及授权策略对终端进行身份验证。	iOS 5.0.1
智能手机	Motorola DROIDX	根据配置文件属性，使用 MAB、LWA、CWA 和 802.1X 以及授权策略对终端进行身份验证。	Android 2.3.4

注：思科 ISE 分析服务是本指南中验证的主要功能。部署其他 Cisco TrustSec 功能的主要目的是为了支持分析服务的配置和测试。

表中所示设备和版本是本指南测试和文档编制过程中具体使用的设备和版本，并不反映支持 TrustSec 和 ISE 分析服务的所有设备。有关更完整的支持 TrustSec 的设备及推荐版本的列表，请访问：

<http://www.cisco.com/go/trustsec>。

分析服务要求

许可

ISE 分析要求在策略管理节点 (PAN) 上安装以下一种许可证：

高级终端许可证（适用于有线或无线部署）

仅无线许可证（仅适用于无线部署）

主动对网络执行身份验证并且使用分析数据做出授权策略决策的各个终端都需要安装一个高级终端许可证。不考虑安全状态评估等要求安装高级终端许可证的其他服务，静态分配给配置文件的终端无需使用高级许可证。如果不使用配置文件信息向终端授权，则无需为每个终端安装高级终端许可证，即可分析多个终端并了解所连接的设备及其分类信息。高级终端许可证或仅无线许可证的最小数量为 100 个。

设备要求

ISE 分析服务只能在为策略服务角色配置的 ISE 设备上运行。表 2 显示关于策略服务专用设备可以分析的活动终端的数量的一般指导信息。基于 VMware 的设备的规模应根据等同于或高于基于硬件的设备的同等规格的原则加以确定。

表 2. ISE 设备规模

ISE 设备	最大终端数	EPS - 分析（分析现有终端）	EPS - 保存（分析新的终端）
ACS1121/NAC3315/ISE3315	3000	43	33
NAC3355/ISE3355	6000	不可用	不可用
NAC3395/ISE3395	10,000	100	5
VMware	3000/6000/10,000	取决于 VMware 配置	取决于 VMware 配置

此外，每个设备在每秒能处理的新事件 (EPS) 的速率方面都有限制。此值取决于所接收的分析数据是用于新发现的终端，还是用于现有终端。现有终端的分析速率如表 2 中“EPS - 分析”栏所示。“EPS - 保存”栏显示的是向数据库添加新发现的终端并进行分析的速率。

可以通过向多个 ISE 设备分配服务，扩展 ISE 分析服务。运行分析服务的 ISE 策略服务节点也可能是用于在负载均衡器后面群集策略服务的节点组中的一个成员。

网络要求

ISE 分析服务使用各种收集器或探测功能来收集关于所连接终端的属性。其中有些探测功能要求网络基础设施、接入设备甚至终端提供特定的支持。这些要求将在介绍具体探测功能的章节中加以详述，但是在此之前，您必须知悉如果无法从网络或终端获得相应数据，则有些探测功能可能无法使用。

分析服务全局配置

ISE 分析全局配置

本节介绍在策略服务节点全局启用 ISE 分析服务和配置全局分析参数的流程。

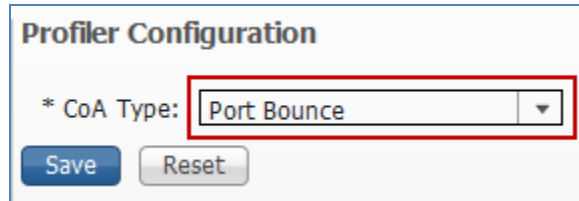
配置全球分析设置

从策略管理节点配置全局分析设置

- 步骤 1** 使用支持的 Web 浏览器和您的管理员凭证，访问主要策略管理节点 (PAN) 的 ISE 管理界面：
https://<ISE_PAN_FQDN_or_IP>
- 步骤 2** 导航至 Administration → System → Settings，从左侧窗格选择 Profiling。
- 步骤 3** 从右侧窗格选择用于分析转换和例外操作的默认 CoA 类型（图 5）。

如果只是为了获得可视性，请保留默认值 No CoA。否则，请选择 Port Bounce。这有助于确保包括无客户端终端在内的所有终端都将经过完整的重新授权流程（如有必要，还包括 IP 地址刷新）。如果在交换端口上检测到多个终端，ISE 将恢复使用 Reauth 选项，以免其他所连接设备的服务中断。

图 3. 全局分析设置：CoA 配置

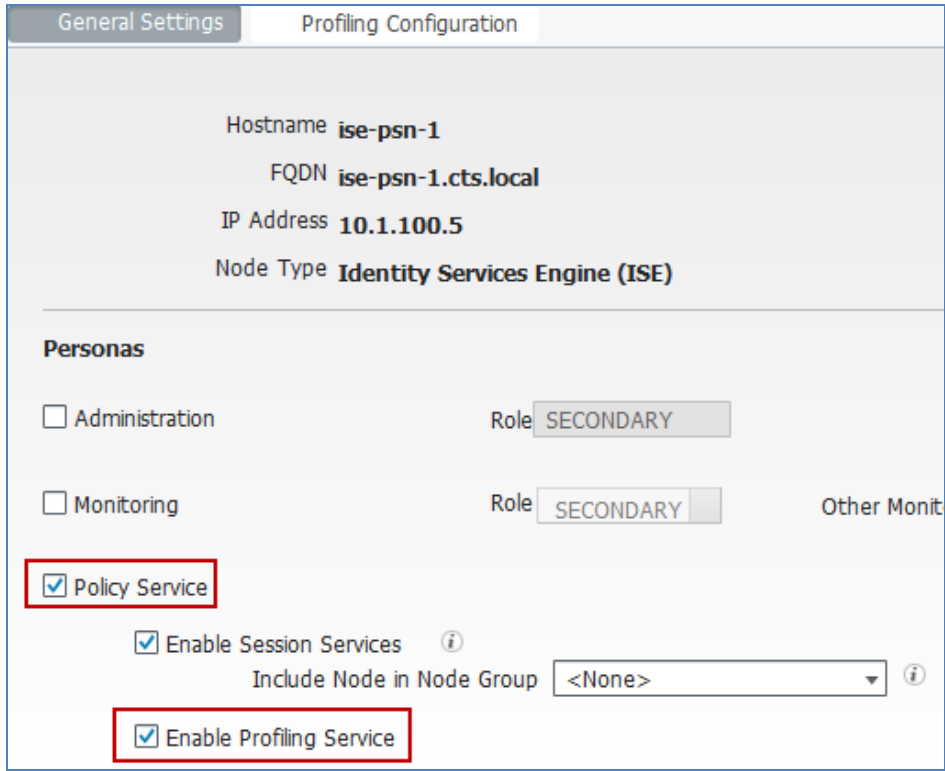


启用 ISE 分析服务

在策略服务节点上启用分析服务

- 步骤 1** 转至 Administration → System → Deployment，并从右侧窗格已部署节点的列表中选择要执行分析的策略服务节点。
- 步骤 2** 在 General Settings 选项卡下，确认选择节点角色 Policy Service 和 Enable Profiling Service（图 6）。

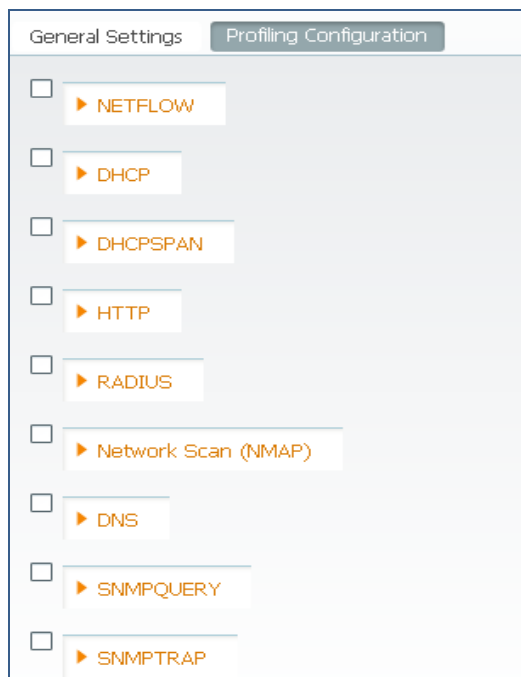
图 4. 在策略服务节点上启用分析器服务



访问并查看分析配置页面

步骤 3 点击 Profiling Configuration 选项卡，查看只需通过选中相应复选框并选择可选探测参数即可启用和配置的各个探测功能（图 7）。

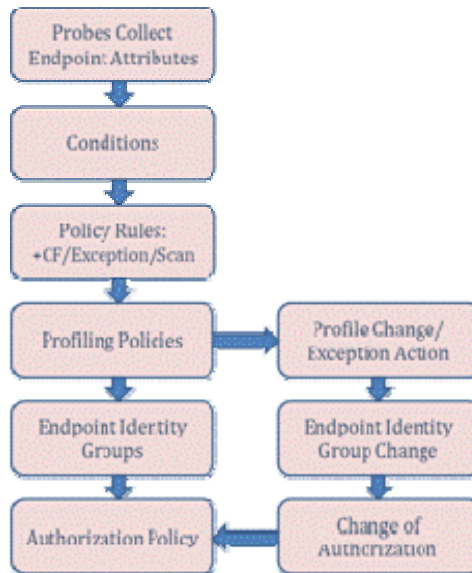
图 5. 探测功能配置



步骤 4 每当您更改分析配置时，请确保点击页面底部的 Save，以提交更改。

配置探测功能

图 6. 配置流程：探测功能和属性收集



探测功能概述

ISE 探测功能是收集终端属性的 ISE 分析服务组件。每个探测功能都使用不同的收集方法并且可以收集关于终端的独特信息。因此，某些探测功能会比其他探测功能更适用于对特定设备类型进行分类，或者根据特定环境优先使用某些探测功能。

ISE 支持以下探测功能：

- RADIUS
- SNMP 陷阱
- SNMP 查询
- DHCP
- DHCP SPAN
- DNS
- HTTP
- NetFlow
- 网络扫描 (NMAP)

顾名思义，有些探测功能（例如 DHCP 和 DHCP SPAN）具有收集特定属性的独特功能。在本例中，DHCP 探测功能和 DHCP SPAN 探测功能可以收集 DHCP 数据包中的 DHCP 属性和相关选项字段。选择 DHCP 还是 DHCP SPAN 取决于特定网络环境是否支持 DHCP 流量到 ISE 策略服务节点的中继，或使用某个交换端口分析器 (SPAN) 方法是否更适合网络拓扑和基础设施的功能。本指南包括关于探测功能选择的详细指导，各个探测功能将在各个章节逐一介绍。

每个探测功能类型的启用难易程度各不相同。根据所使用的协议及其部署方式，每个探测类型对于网络或终端的影响程度也不一样。最后，每个探测功能在其所产生数据的价值方面以及对网络中相关的具体终端进行分类的适用性方面也各不相同。本指南介绍各个探测功能的配置和部署方式，并且全面介绍其部署的难易程度、网络影响以及基于部署类型的相对分析价值。

探测功能配置

在为分析服务配置的 ISE 策略服务节点上启用 ISE 探测功能。本节介绍启用各个 ISE 探测功能以收集不同终端属性的步骤。此外，还将提供支持网络基础设施的有效配置示例，以及基础设施和 ISE 管理界面的预期输出。

使用 RADIUS 探测功能进行分析

RADIUS 探测功能收集 RADIUS 客户端向 RADIUS 服务器（运行会话服务的 ISE 策略服务节点）发送的 RADIUS 属性（包括有线接入交换机和无线控制器）。标准 RADIUS 端口包括用于身份验证和授权的 UDP/1645 或 UDP/1812，以及用于 RADIUS 记帐的端口 UDP/1646 和 UDP/1813。

注：RADIUS 探测功能不直接侦听 RADIUS 流量，而是侦听和解析系统日志中向默认 UDP 端口 20514 上的监控节点发送的 RADIUS 属性。然后，所捕获的 RADIUS 配置文件属性将转发给默认 UDP 端口 30514 上的内部记录器。

RADIUS 探测功能还可以收集在 RADIUS 记帐数据包中使用设备传感器功能发送的思科发现协议 (CDP)、链路层发现协议 (LLDP) 和 DHCP 属性。下文将详细介绍此功能（请参阅[设备传感器](#)一章）。图 9 显示思科 RADIUS 探测功能示例的拓扑。

图 7. RADIUS 探测功能示例

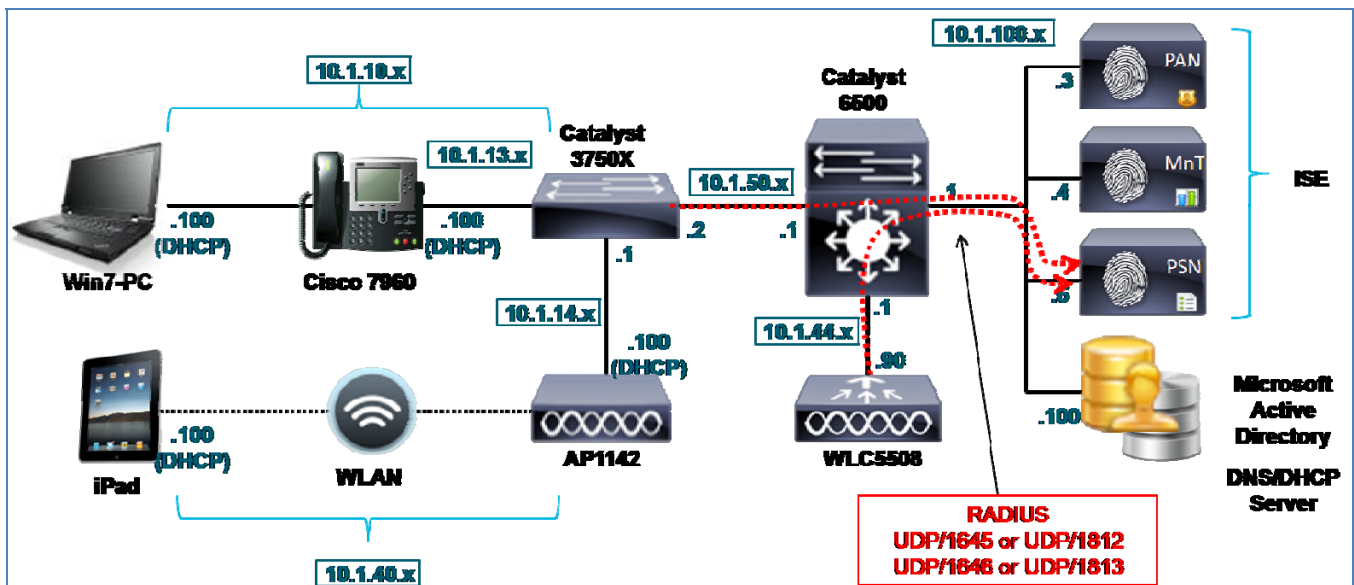


表 3 显示使用 RADIUS 探测功能收集的常见属性。

表 3. 示例 RADIUS 属性

User-Name	NAS-IP-Address	NAS-Port	Framed-IP-Address
Calling-Station-Id	Acct-Session-Id	Acct-Session-Time	Acct-Terminate-Cause

虽然 Calling-Station-ID 取决于接入设备配置，但是其通常是所连接终端的 MAC 地址。此属性一个立竿见影的好处是可以根据 MAC 地址在终端连接至网络并进行身份验证时快速识别唯一终端。它还根据从 MAC 地址前三个字节提取的组织唯一标识符 (OUI)，提供关于供应商网络适配器的信息。

RADIUS 记帐数据包中的 Framed-IP-Address 提供所连接终端的 IP 地址。此属性与 Calling-Station-ID 相结合，可向 ISE 提供支持依赖于 IP 地址的其他探测功能（例如 DNS、HTTP、Cisco NetFlow 和 NMAP）所需的关键 IP 到 MAC 绑定。

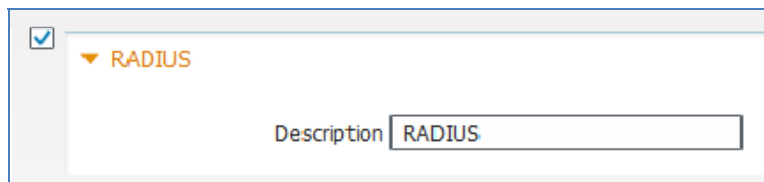
配置 RADIUS 探测功能

RADIUS 探测功能是最容易启用和部署的探测功能之一，因为网络接入设备已经配置为向运行会话服务的 ISE 策略服务节点发送 RADIUS 数据包，以进行用于网络身份验证和授权。

在 ISE 中启用 RADIUS 探测功能

- 步骤 1** 转至 Administration → System → Deployment，在右侧窗格中从已部署节点的列表中，选择要执行分析的策略服务节点。
- 步骤 2** 选择 Profiling Configuration 选项卡，然后选中相应复选框以启用 RADIUS 探测功能。此探测功能将在为 RADIUS 服务配置的接口上自动启用（图 10）。

图 8. RADIUS 探测功能配置



- 步骤 3** 点击 Save 以提交更改。
- 步骤 4** 对已配置分析服务的所有其他策略服务节点重复本程序中的步骤。

验证是否已在 ISE 中配置接入设备

本指南假定已在 Administration → Network Resources → Network Devices 下配置了网络接入设备，可进行标准 RADIUS 通信。

验证是否已将接入设备配置为向 ISE PSN 发送 RADIUS

本指南假定已配置网络接入设备，可对 ISE 策略服务节点 (PSN) 进行 RADIUS 身份验证、授权和记帐。以下是适用于有线交换机的一个示例 RADIUS 配置：

```

aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
ip radius source-interface <Interface>
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server host <ISE_PSN_Address> auth-port 1812 acct-port 1813 key xxx
radius-server vsa send accounting
radius-server vsa send authentication

```

图 11 显示的是一个无线控制器的示例 RADIUS 服务器配置。要访问此配置页面，请转至 WLC Web 管理界面上的 Security → AAA → RADIUS → Authentication。

图 9. 无线控制器的全局 RADIUS 服务器配置示例



The screenshot shows the 'RADIUS Authentication Servers' configuration page. The 'Call Station ID Type' is set to 'System MAC Address'. Below this, there are checkboxes for 'Use AES Key Wrap' and a 'MAC Delimiter' set to 'Hyphen'. A table lists the configured RADIUS servers:

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2	10.1.100.5	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3	10.1.100.6	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4	10.1.100.7	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5	10.1.101.3	1812	Disabled	Enabled

思科最佳实践：如图 11 所示，请务必将 Call Station ID Type 设置为 System MAC Address 以允许分析非 802.1X 客户端。这样可以确保 ISE 能够将终端添加到数据库中并根据已知 MAC 地址将所接收的其他配置文件数据与同一终端关联。

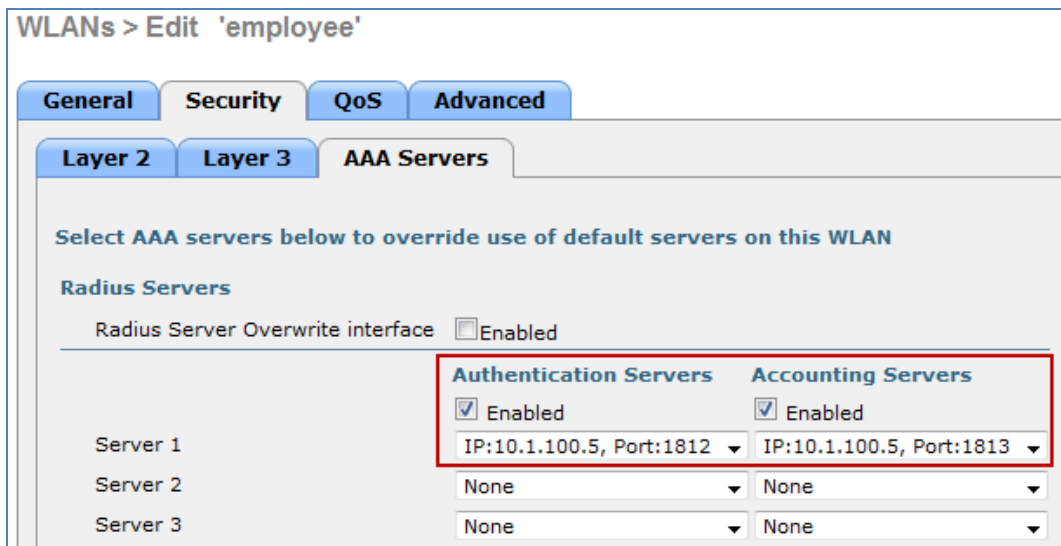
对于无线控制器，在 RADIUS 记帐配置下应该显示类似的条目（图 12）。

图 10. 无线控制器的全局 RADIUS 记帐配置示例



为指定适当的 ISE 策略服务节点。应对每个 WLAN 进行配置（图 13）。

图 11. 无线控制器的 WLAN RADIUS 配置示例



验证 RADIUS 探测功能数据

- 步骤 1** 对连接至网络的新终端进行身份验证。
- 步骤 2** 转至 ISE Policy Administration 节点并导航至 Administration → Identity Management → Identities。
- 步骤 3** 从左侧窗格选择 Endpoints。
- 步骤 4** 查找并选择新连接的终端的 MAC 地址，以显示 RADIUS 探测功能捕获的属性。
- 步骤 5** 可以捕获大量属性。图 14 中的示例输出只突出显示四个属性：**Calling-Station-ID**、**EndPointSource**、**Framed-IP-Address** 和 **OUI**。

图 12. RADIUS 探测功能属性示例

Endpoint

* MAC Address **00:1A:70:38:B6:66**

* Policy Assignment Cisco-Device

Static Assignment

* Identity Group Assignment Profiled

Static Group Assignment

Attribute List

ADDomain	cts.local		
AcsSessionID	ise-psn-1/123830140/32632		
Airespace-Wlan-Id	1		
AuthState	Authenticated		
AuthenticationIdentityStore	AD1		
AuthenticationMethod	MSCHAPV2		
AuthorizationPolicyMatchedRule	Employee_NoPosture		
CPMSessionID	0a012c5a00005954f98e8cc		
Called-Station-ID	cc-ef-48-0c-99-a0		
Calling-Station-ID	00-1a-70-38-b6-66	Calling-Station-ID	00-1a-70-38-b6-66
DestinationIPAddress	10.1.100.5		
DestinationPort	1812		
Device IP Address	10.1.44.90		
Device Type	Device Type#All Device Types#Wireless		
EapAuthentication	EAP-MSCHAPv2		
Eap Tunnel	PEAP		
EndPointMACAddress	00-1A-70-38-B6-66		
EndPointMatchedProfile	Cisco-Device		
EndPointPolicy	Cisco-Device		
EndPointProfilerServer	ise-psn-1	EndPointSource	RADIUS Probe
ExternalGroups	cts.local/users/employees\,cts.local/users/domain users\,cts.local/builtin/users		
Framed-IP-Address	10.1.40.100	Framed-IP-Address	10.1.40.100
IdentityAccessRestricted	false		
IdentityGroup	Profiled		
IdentityPolicyMatchedRule	Default		
Location	Location#All Locations#North_America#RTP		
MACAddress	00:1A:70:38:B6:66		
MatchedPolicy	Cisco-Device		
MessageCode	3000		
NAS-IP-Address	10.1.44.90		
NAS-Identifier	Cisco_0c99:a4		
NAS-Port	1		
NAS-Port-Type	Wireless - IEEE 802.11		
NetworkDeviceGroups	Device Type#All Device Types#Wireless, Location#All Locations#North_America#RTP		
NetworkDeviceName	wlc5508		
OUI	Cisco-Linksys, LLC	OUI	Cisco-Linksys, LLC
PolicyVersion	22		
PostureAssessmentStatus	NotApplicable		
RequestLatency	1		
Response	{User-Name=CTS\employee1; State=ReauthSession:0a012c5a00005954f98e8cc; Class=CACS:0a012c5a00005954f98e8cc;ise-psn-1/123830140/32632; Termination-Action=RADIUS-Request; cisco-av-pair=ACS:CiscoSecure-Defined-ACL=#ACSACL#-JP-PERMIT_ALL_TRAFFIC-4f57e406; MS-MPPE-Send-Key=7d:90:04:93:07:bc:92:1e:e5:4d:97:6f:39:51:02:6e:eb:39:46:35:4f:e4:76:06:27:58:96:98:b4:bf:51:cb; MS-MPPE-Recv-Key=ac:0e:b6:a9:6f:c7:72:5d:cf:fe:9d:8b:9d:95:7a:8c:c6:2c:a7:54:1f:ee:3e:40:ed:53:48:d8:68:76:38:e8; Airespace-ACL-Name=PERMIT_ALL_TRAFFIC; }		
SelectedAccessService	Default Network Access		
SelectedAuthenticationIdentityStores	AD1, Internal Users		
SelectedAuthorizationProfiles	Employee		
Service-Type	Framed		
StaticAssignment	false		
StaticGroupAssignment	false		
TimeToProfile	20		
Total Certainty Factor	20		
User-Name	CTS\employee1		
attribute-S2	00:00:00:00		
attribute-S3	00:00:00:00		
cisco-av-pair	audit-session-id=0a012c5a00005954f98e8cc		
ip	10.1.40.100		

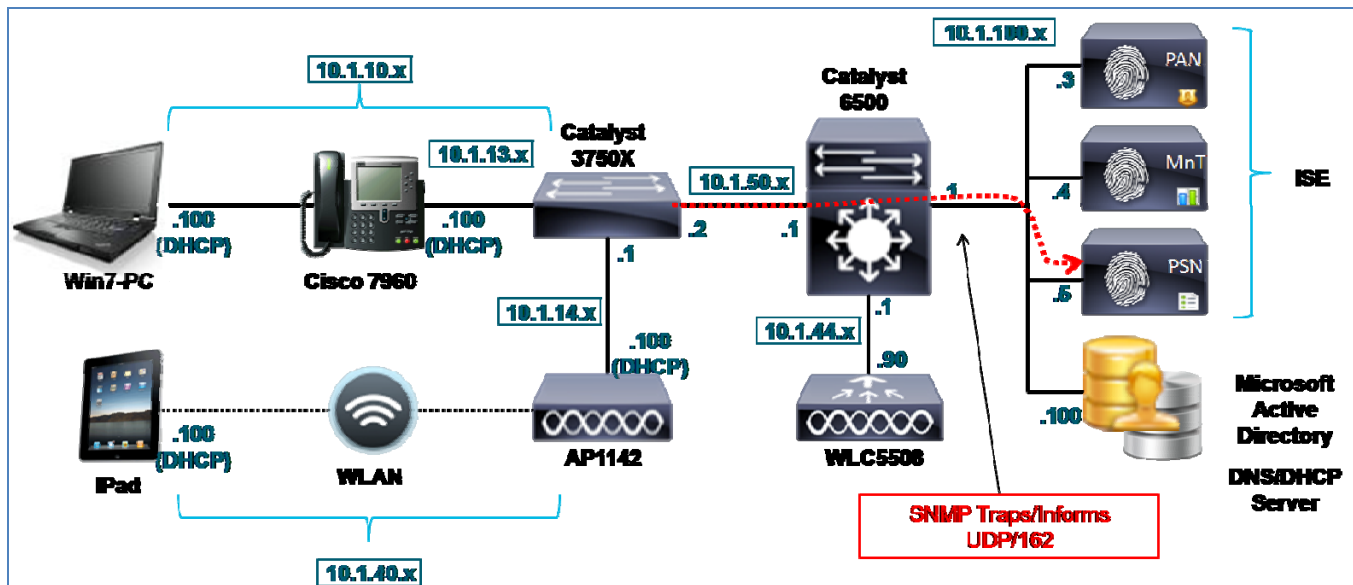
- 步骤 6** Calling-Station-ID 填充于 **MACaddress** 属性中。此外，网络适配器的供应商 OUI 确定为 **Cisco-Linksys**。在本例中，网络适配器是 Linksys 无线 USB 适配器。与 OUI 匹配的条件是在分析策略规则中的常见条目。在有些情况（例如 Nintendo 或 Sony 游戏控制台）下，匹配条件可能是终端分类所需的全部条目。
- 步骤 7** Framed-IP-Address 值填充于 **ip** 属性中。对于此终端，我们现在有 IP 到 MAC 地址绑定。
- 步骤 8** **EndPointSource** 属性指定配置文件属性最后一次更新的来源。在这种情况下，RADIUS 探测功能是该终端记录最后一次更新的来源。
- 步骤 9** 其他 RADIUS 属性也可用于分析，但是由于其中大多数属性都可以直接提供给授权策略以创建策略条件和规则，所以重点介绍上述属性。

使用 SNMP 陷阱探测功能进行分析

SNMP 陷阱探测功能用于为网络终端的在线状态（连接或断开连接）功能提供 ISE 分析服务警报以及触发 SNMP 查询探测功能。

要使用 SNMP 陷阱探测功能，终端连接的接入设备必须配置为向为分析服务配置的 ISE 策略服务节点发送 SNMP 陷阱。图 15 显示我们的示例 SNMP 陷阱探测功能的拓扑。

图 13. SNMP 陷阱探测功能示例



如果 RADIUS 探测功能已经启用，可能会不再需要 SNMP 陷阱探测功能，因为 RADIUS 记帐开始消息也可以触发 SNMP 查询探测功能。此探测功能的主要使用案例是用于尚需为网络身份验证配置 RADIUS 的预部署发现阶段。另一个使用案例是集成不依赖于 RADIUS 的环境，例如思科网络准入控制设备 4.9 以及更高版本。

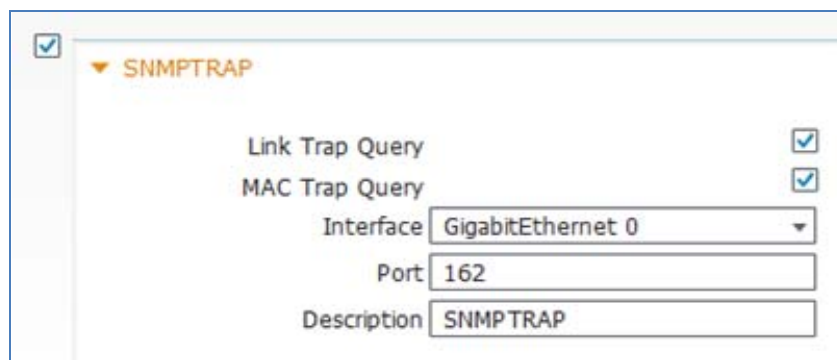
配置 SNMP 陷阱探测功能

要使用 SNMP 陷阱探测功能，必须首先在 ISE 中启用此探测功能。如前所述，终端连接的接入设备必须配置为向为分析服务配置的 ISE 策略服务节点发送 SNMP 陷阱。ISE 还必须配置为接受和处理来自这些网络接入设备的陷阱。

在 ISE 中启用 SNMP 陷阱探测功能

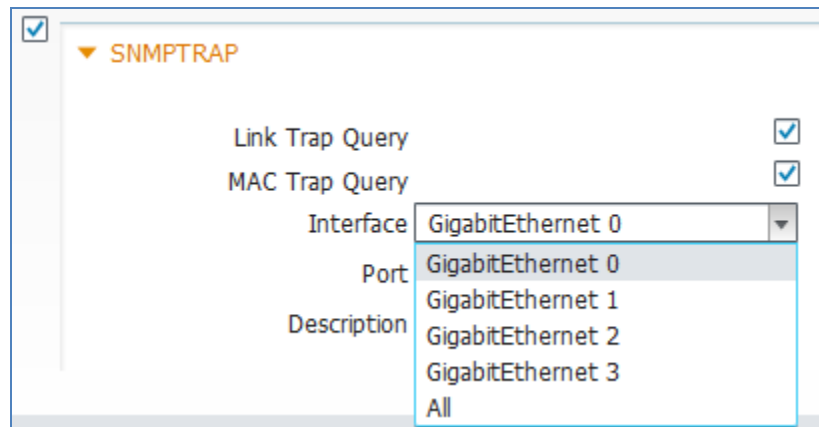
- 步骤 1** 转至 Administration → System → Deployment，并从右侧窗格已部署节点的列表中选择要执行分析的策略服务节点。
- 步骤 2** 选择 Profiling Configuration 选项卡，并且选中启用 SNMP 陷阱探测功能的复选框（图 14）。

图 14. SNMP 陷阱探测功能配置



- 步骤 3** 选中标记为 Link Trap Query 和 MAC Trap Query 的复选框，启用该探测功能以响应各个陷阱类型。
- 步骤 4** 验证用于接收陷阱的 ISE PSN 接口。在大多数情况下，接口会是默认的千兆以太网接口 0，但是可以在其他接口上处理所接收的陷阱或选择全部接口。

图 15. SNMP 陷阱探测功能 - 接口配置



- 步骤 5** 如果您决定在其他接口上处理陷阱，请确保这些接口已启用并分配了 IP 地址。这些地址必须在 SNMP 主机陷阱目标处的接入设备上配置。
- 步骤 6** 点击 Save 以提交更改。
- 步骤 7** 对已配置分析服务的所有其他策略服务节点重复本程序中的步骤。

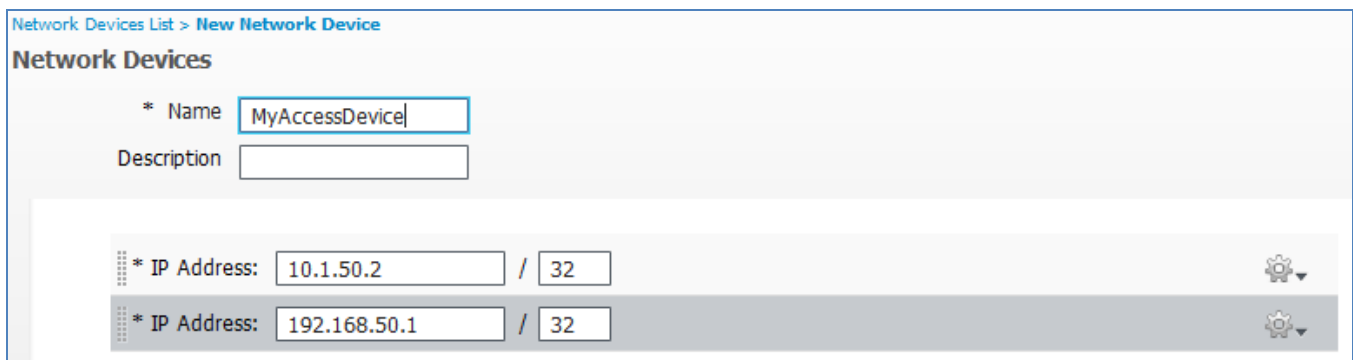
向 ISE 添加网络接入设备

通常，通过 RADIUS 对终端进行身份验证的所有网络接入设备都将在 ISE 中配置，但是使用 SNMP 陷阱探测功能通常意味着尚未为 RADIUS 配置接入设备。如果尚未配置这些接入设备，您必须添加要向 ISE 发送 SNMP 陷阱的接入设备。

步骤 1 转至 Administration → Network Resources → Network Devices 并在右侧窗点击 Add。

步骤 2 输入设备名称和 IP 地址信息（图 18）。IP 地址应包括作为 SNMP 陷阱源的 IP 地址。在简单配置中，交换机上可能只有一个管理 IP 地址。在其他情况下，可能有多个 IP 地址，并且在默认情况下 SNMP 通常会使用出口接口的 IP 地址。如有必要，请输入接入设备可能用作 SNMP 数据包源的所有可能的 IP 地址。

图 16. 网络设备配置



Network Devices List > New Network Device

Network Devices

* Name

Description

* IP Address: /

* IP Address: /

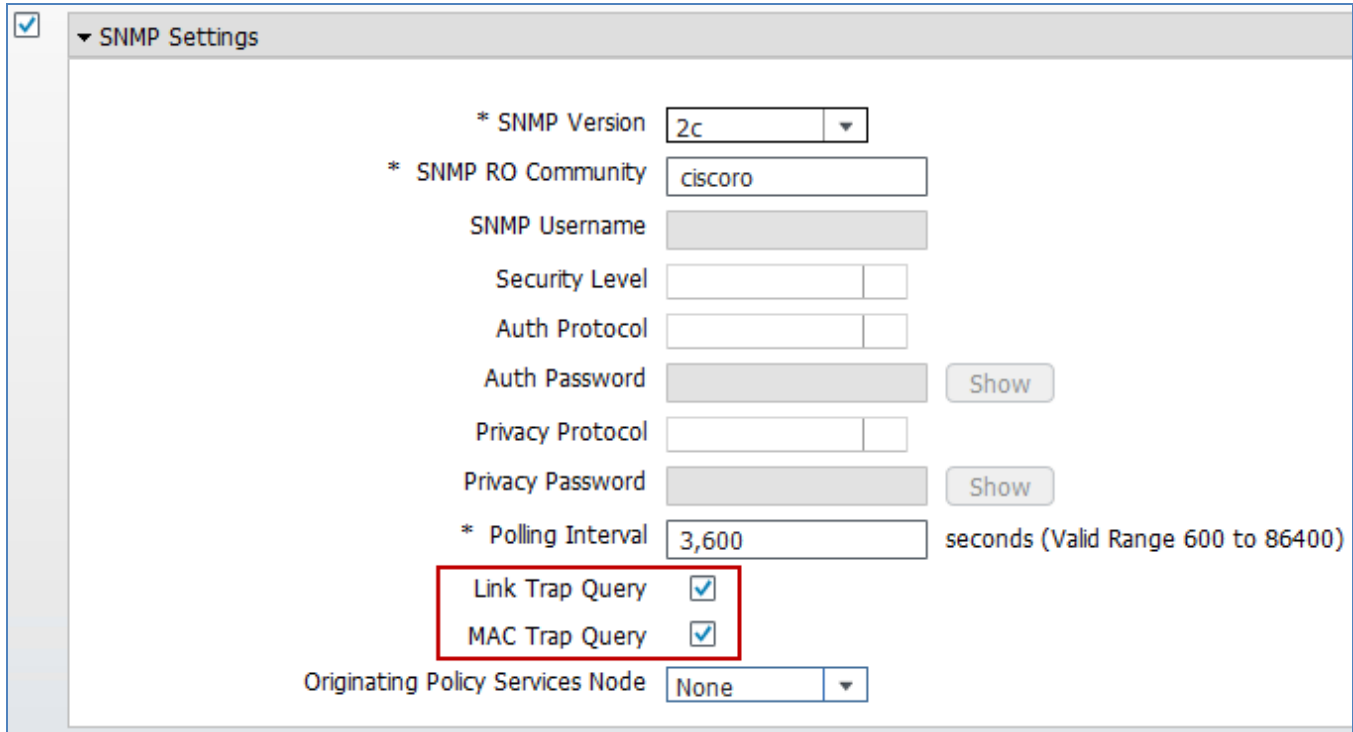
最佳实践： 如果接入设备支持，请将环回接口用于管理流量。请务必利用 source-interface 等选项，设置作为管理流量来源的具体接口和 IP 地址。这将为所有管理流量提供一个统一地址，并且如果具体接口处于关闭状态，还可以防止连接故障。

步骤 3 选中 SNMP Settings 复选框。

步骤 4 指定接入设备使用的 SNMP Version 并输入 SNMP 版本 1 和 2c 的 SNMP RO Community 字符串，否则如果适用于接入设备，也可以输入 SNMPv3 凭证和配置（图 19）。

步骤 5 验证是否已选择 Link Trap Query 和 MAC Trap Query 复选框。这些设置允许 ISE 接受或忽略从特定接入设备接收的 SNMP 陷阱，或仅接收特定类型的陷阱。

图 17. 网络设备配置 - SNMP 陷阱



SNMP Settings

* SNMP Version

* SNMP RO Community

SNMP Username

Security Level

Auth Protocol

Auth Password

Privacy Protocol

Privacy Password

* Polling Interval seconds (Valid Range 600 to 86400)

Link Trap Query

MAC Trap Query

Originating Policy Services Node

步骤 6 完成之后，请保存更改。

步骤 7 对要向 ISE 策略服务节点发送 SNMP 陷阱的每个接入设备重复以上步骤。

将接入设备配置为向 ISE 策略服务节点发送 SNMP 陷阱

步骤 1 转至接入设备的管理控制台，然后验证设备是否已配置为向运行分析服务的 ISE 策略服务节点发送 SNMP 陷阱以及设备是否已使用 SNMP 陷阱探测功能启用。

步骤 2 以下是运行思科 IOS 的 Catalyst 交换机的示例配置，通过此配置可发送 SNMP LinkUp/LinkDown 陷阱和 MAC Notification 陷阱：

```
interface <Endpoint_Interface>
 snmp trap mac-notification added
 snmp trap mac-notification removed
!
mac address-table notification change
mac address-table notification mac-move
!
snmp-server trap-source <Interface>
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification change move
snmp-server host <ISE_PSN_IP_address> version 2c ciscoro
```

注：思科 ISE 当前不支持从无线局域网控制器接收的 SNMP 陷阱。

验证 SNMP 探测功能数据

SNMP 陷阱探测功能无法单独根据 LinkUp 或 LinkDown 陷阱填充终端属性，因为在这些陷阱中没有关联的 MAC 地址。它们主要用于通知接口已建立或丢失哪个链路。但是，MAC Notification 陷阱不包含终端的 MAC 地址，因此可以为 ISE 内部终端数据库提供更新。

- 步骤 1** 从 Administration → Identity Management → Identities → Endpoints 删除终端。
- 步骤 2** 从为 SNMP 陷阱配置的接入交换机断开有线客户端，然后重新连接。
- 步骤 3** 转至 ISE Policy Administration 节点并导航至 Administration → Identity Management → Identities。
- 步骤 4** 从左侧窗格选择 Endpoints。
- 步骤 5** 查找并选择新连接的终端的 MAC 地址，以显示 SNMP 陷阱探测功能捕获的属性（图 20）。

图 18. SNMP 陷阱探测功能属性示例

Endpoint

* MAC Address **00:50:56:A0:0B:3A**

* Policy Assignment VMWare-Device

Static Assignment

* Identity Group Assignment Profiled

Static Group Assignment

Attribute List

EndPointPolicy	VMWare-Device		
EndPointProfilerServer	ise-psn-1		
EndPointSource	SNMPTrap Probe	→	EndPointSource SNMPTrap Probe
IdentityGroup	Profiled		
MACAddress	00:50:56:A0:0B:3A	→	MACAddress 00:50:56:A0:0B:3A
MacStatus	02		
MatchedPolicy	VMWare-Device		
NADAddress	10.1.50.2		
OUI	VMware, Inc.	→	OUI VMware, Inc.
PolicyVersion	22		
StaticAssignment	false		
StaticGroupAssignment	false		
TimeToProfile	19		
Timestamp	58963997		
Total Certainty Factor	10		
Vlan	10		
dot1dBasePort	1		

突出显示的关键属性包括 **EndPointSource**、**MACAddress** 和 **OUI**。

EndPointSource 确认 SNMP 陷阱探测功能是信息的来源。

注：在图 20 所示的示例中，所有其他探测功能都已禁用，并且在运行测试之前已从 ISE 数据库删除终端。

MACAddress 已从 MAC Notification 陷阱信息获得，并且通过基于 ISE 的 OUI 数据库的关联操作确定了供应商 OUI。在本例中，我们可以看到客户端运行的是使用了虚拟网络适配器的 VMware。

验证接入交换机是否正在发送 SNMP 陷阱是一项可选验证，可以通过启用调试记录查看 SNMP Link 陷阱和 MAC Notification 陷阱的发送情况进行验证。下面的输出来自启用了以下调试的 Catalyst 交换机：

- 调试 SNMP 数据包
- 调试 MAC Notification

在下面的示例中，启用连接至思科 IP 电话的交换端口和连接至该电话的 Windows 7 PC 时，系统会为该电话和 PC 将 SNMP LinkUp 陷阱发送至 ISE PSN，然后会为二者发送 MAC Notification 陷阱。仅突出显示与 MAC 地址为 00:50:56:A0:0B:3A 的 PC 相关的陷阱：

```
Apr 26 16:53:06.735: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
Apr 26 16:53:06.743: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan13, changed state to up
Apr 26 16:53:06.743: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:06.743: SNMP: V2 Trap, reqid 296, errstat 0, erridx 0
  sysUpTime.0 = 58970958
  snmpTrapOID.0 = snmpTraps.4
  ifIndex.10 = 10
  ifDescr.10 = Vlan10
  ifType.10 = 53
  lifEntry.20.10 = up

Apr 26 16:53:06.861: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:06.861: SNMP: V2 Trap, reqid 299, errstat 0, erridx 0
  sysUpTime.0 = 58970970
  snmpTrapOID.0 = snmpTraps.4
  ifIndex.13 = 13
  ifDescr.13 = Vlan13
  ifType.13 = 53
  lifEntry.20.13 = up

Apr 26 16:53:06.995: SNMP: Packet sent via UDP to 10.1.100.5
Apr 26 16:53:07.246: SNMP: Packet sent via UDP to 10.1.100.5
Apr 26 16:53:08.706: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
Apr 26 16:53:09.713: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed
state to up
Apr 26 16:53:09.713: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:09.713: SNMP: V2 Trap, reqid 302, errstat 0, erridx 0
  sysUpTime.0 = 58971255
  snmpTrapOID.0 = snmpTraps.4
  ifIndex.10101 = 10101
  ifDescr.10101 = GigabitEthernet1/0/1
  ifType.10101 = 6
  lifEntry.20.10101 = up
Apr 26 16:53:09.964: SNMP: Packet sent via UDP to 10.1.100.5
Apr 26 16:53:12.280: MN: Enqueue MAC 0050.56a0.0b3a on port 1 vlan 10
MN: New Shadow entry..

Apr 26 16:53:12.280: MN : MAC Notify event for 0050.56a0.0b3a on port 1 vlan 10

Apr 26 16:53:12.456: MN: Enqueue MAC 0030.94c4.528a on port 1 vlan 10
MN: Got the last shadow entry..Index 11

Apr 26 16:53:12.456: MN : MAC Notify event for 0030.94c4.528a on port 1 vlan 10
MN: Shadow entry for Despatch..
Despatching trap for Index 2 Time: 58971575
MN: Wrapping history queue..

Apr 26 16:53:12.925: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:12.925: SNMP: V2 Trap, reqid 305, errstat 0, erridx 0
  sysUpTime.0 = 58971577
  snmpTrapOID.0 = cmnMacChangedNotification
  cmnHistMacChangedMsg.1 =
01 00 0A 00 50 56 A0 0B 3A 00 01 01 00 0A 00 30
94 C4 52 8A 00 01 00
  cmnHistTimestamp.1 = 58971575
Apr 26 16:53:13.177: SNMP: Packet sent via UDP to 10.1.100.5
```

```

Apr 26 16:53:23.587: MN: Enqueue MAC 0030.94c4.528a on port 1 vlan 13
MN: New Shadow entry..

Apr 26 16:53:23.604: MN : MAC Notify event for 0030.94c4.528a on port 1 vlan 13
MN: Shadow entry for Despatch..
Despatching trap for Index 2 Time: 58972696
MN: Wrapping history queue..

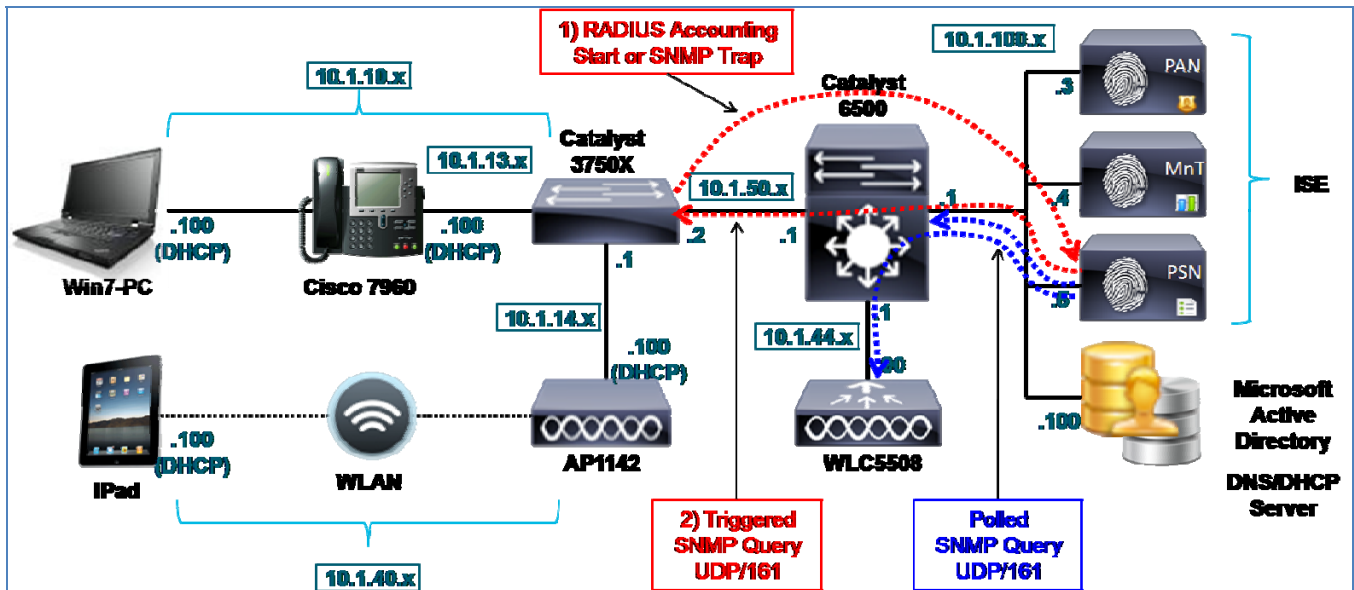
Apr 26 16:53:24.132: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:24.132: SNMP: V2 Trap, reqid 308, errstat 0, erridx 0
sysUpTime.0 = 58972697
snmpTrapOID.0 = cmnMacChangedNotification
cmnHistMacChangedMsg.1 =
01 00 0D 00 30 94 C4 52 8A 00 01 00
cmnHistTimestamp.1 = 58972696
Apr 26 16:53:24.384: SNMP: Packet sent via UDP to 10.1.100.5
    
```

作为参考，ISE 除了支持接入设备提供的调试日志记录，还支持其自身提供的调试日志记录。调试不在本指南讨论范围之内，不过还有一种替代方法可以验证 ISE 接收的信息，即使用 Operations → Troubleshoot → Diagnostic Tools → General Tools 下的内置 TCP Dump 实用工具。此工具将允许 ISE 捕获从接入设备到指定 ISE 策略服务节点接口（即 SNMP 陷阱探测功能启用的接口）的 SNMP 流量。由此可以下载并以可读的格式显示此信息，还可以采用导入 Wireshark 等常用数据包分析器所用的标准数据包捕获格式进行显示。

使用 SNMP 查询探测功能进行分析

- 步骤 1** SNMP 查询探测功能用于向接入设备和有选择地向其他基础设施设备发送查询（或 SNMP Get 请求），以收集其 SNMP MIB 中存储的相关终端数据。ISE 策略服务节点执行的 SNMP 查询有两个普通类型：
- 步骤 2** 系统查询（轮询）
- 步骤 3** 接口查询（触发）
- 步骤 4** 图 21 显示的是使用系统查询探测功能的示例拓扑。

图 19. SNMP 查询探测功能示例



系统查询

系统查询根据 ISE 的 NAD 配置中设置的轮询间隔定期执行。所轮询的 MIB 如下所示：

- IF-MIB
- SNMPv2-MIB
- IP-MIB
- CISCO-CDP-MIB
- CISCO-VTP-MIB
- CISCO-STACK-MIB
- BRIDGE-MIB
- OLD-CISCO-INTERFACE-MIB
- CISCO-LWAPP-AP-MIB
- CISCO-LWAPP-DOT11-CLIENT-MIB
- CISCO-AUTH-FRAMEWORK-MIB
- IEEE8021-PAE-MIB: RFC IEEE 802.1X
- HOST-RESOURCES-MIB
- LLDP-MIB

所收集的关键属性包括以下条目：

- 网桥、IP (ARP)
- **cdpCacheEntry** (仅有线)
- **lldpLocalSystemData** (仅有线)
- **lldpRemoteSystemsData** (仅有线)
- **cLApEntry** (仅 WLC)
- **cldcClientEntry** (仅 WLC)

如果多个策略服务节点都启用了 SNMP 查询，则会在所有可用 PSN 之间分配网络设备的 SNMP 轮询，除非特定 PSN 已配置为轮询指定网络设备。

在此轮询查询期间，还会收集地址解析协议 (ARP) 表信息，用以构建 ISE 中的 IP-MAC ARP 缓存表。在终端仅连接至第 2 层交换端口的环境中，如果上游第 3 层设备包含终端的 ARP 表信息，则可能需要将上游第 3 层设备（例如分支机构路由器或第 3 层分布交换机）配置为 ISE 网络接入设备。在未在接入设备上配置 RADIUS 或 DHCP 探测功能无法收集 IP 到 MAC 绑定数据的部署中，可能只有满足此要求，才能提供 IP 到 MAC 绑定信息。在示例拓扑（图 21）中，Cisco Catalyst 6500 系列交换机可能被轮询，从而为无线客户端或下游第 2 层交换机（图中未显示）收集 ARP 信息。

接口查询

接口查询由 RADIUS 记帐开始数据包（需要 RADIUS 探测功能）或 SNMP LinkUp/MAC Notification 陷阱（需要 SNMP 陷阱探测功能）触发。

最佳实践： 要简化部署并降低 SNMP 陷阱导致的流量开销，在可能的情况下，请使用 RADIUS 探测功能根据 RADIUS 记帐开始消息触发 SNMP 查询。

鉴于系统查询会读取接入设备 MIB，接口查询将请求获取 MIB 或仅与接收陷阱的特定接口相关的 MIB 部分。所触发的这些查询会从接入设备检索以下数据：

- 接口数据（ifIndex、ifDesc 等）
- 端口和 VLAN 数据
- 会话数据（假设接口类型是以太网）
- CDP 数据（思科设备）
- LLDP 数据

在触发的接口查询期间收集的有些关键分析属性包括思科发现协议 (CDP) 和链路层发现协议 (LLDP) 表。CDP 和 LLDP 是允许交换机动态获取所连接终端的属性的链路协议。很多设备（包括 IP 视频设备、网络基础设施和思科设备）都支持这些协议。大多数主要 IP 电话产品都支持 CDP 或 LLDP。因此，仅根据此信息即可对许多终端进行分类。此外，还可以在多种客户端操作系统上以最低的价格或免费使用许多 CDP/LLDP 代理。

以下输出显示的是使用 SNMP 查询为所连接终端收集 CDP 数据时可收集信息类型的示例。

```
cat3750x#show cdp neighbor detail
-----
Device ID: APc471.fe34.197a
Entry address(es):
  IP address: 10.1.14.100
Platform: cisco AIR-LAP1142N-A-K9 , Capabilities: Trans-Bridge
Interface: GigabitEthernet1/0/2, Port ID (outgoing port): GigabitEthernet0
Holdtime : 123 sec

Version :
Cisco IOS Software, C1140 Software (C1140-K9W8-M), Version 12.4(25e)JA, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Fri 27-Jan-12 21:45 by prod_rel_team

advertisement version: 2
Duplex: full
Power drawn: 15.400 Watts
Power request id: 1358, Power management id: 2
Power request levels are:15400 14500 0 0 0
Management address(es):
-----
Device ID: SEP003094C4528A
Entry address(es):
  IP address: 10.1.13.100
Platform: Cisco IP Phone 7960, Capabilities: Host Phone Two-port Mac Relay
Interface: GigabitEthernet1/0/1, Port ID (outgoing port): Port 1
Holdtime : 162 sec
Second Port Status: Up

Version :
P00308010100

advertisement version: 2
Duplex: full
Power drawn: 6.300 Watts
Management address(es):
-----
```

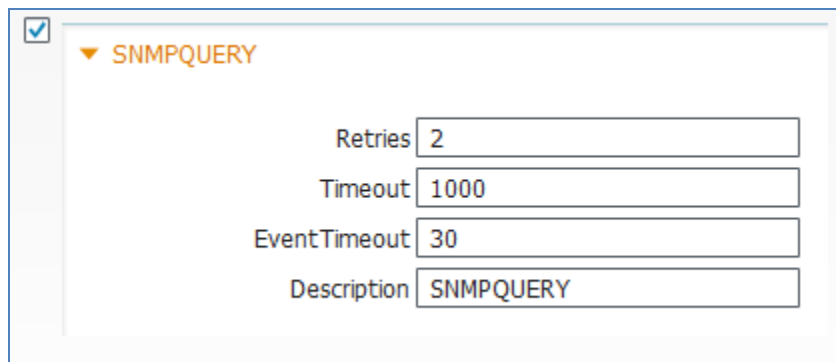

配置 SNMP 查询探测功能

要使用 SNMP 查询探测功能，网络设备必须配置为使用只读 (RO) 社区接受来自 ISE 策略服务节点的 SNMP 请求。ISE 还必须具有配置为网络设备的 SNMP 设备以及相应的 SNMP 社区字符串。要实现触发的查询，则必须启用 RADIUS 探测功能或 SNMP 陷阱探测功能，而且必须正确配置关联的组件。最后，要检索 CDP 或 LLDP 信息，终端必须支持 CDP 或 LLDP，而且必须在接入交换机上启用其中一个或两个协议。

在 ISE 中启用 SNMP 查询探测功能

- 步骤 1** 转至 Administration → System → Deployment，并从右侧窗格已部署节点的列表中选择要执行分析的策略服务节点。
- 步骤 2** 选择 Profiling Configuration 选项卡，并且选中启用 SNMP 查询探测功能的复选框（图 22）。

图 20. SNMP 查询探测功能配置



The screenshot shows the configuration for the 'SNMPQUERY' profile. A checkbox is checked. The configuration parameters are:

- Retries: 2
- Timeout: 1000
- EventTimeout: 30
- Description: SNMPQUERY

注：不需要为 SNMP 查询探测功能配置任何接口。系统将根据设备路由表向接入设备发送 SNMP 查询。

- 步骤 3** 将 Retries、Timeout 和 Event Timeout 保留默认值：
- 步骤 4** **Timeout:** 用于指定等待 SNMP 响应的的时间量（单位：毫秒）。
- 步骤 5** **Retries:** 用于指定策略服务节点在初始尝试失败之后，尝试建立 SNMP 会话的次数。
- 步骤 6** **EventTimeout:** 用于指定在 RADIUS 计帐开始或 SNMP 陷阱触发之后、向接入设备发送批量查询之前的等待时间（单位：秒）。
- 步骤 7** 对于触发的接口查询，请验证是否已启用 RADIUS 探测功能。如果在网络接入设备上未配置 RADIUS，请验证是否已启用 SNMP 陷阱探测功能。
- 步骤 8** 点击 Save 以提交更改。
- 步骤 9** 对已配置分析服务的所有其他策略服务节点重复本程序中的步骤。

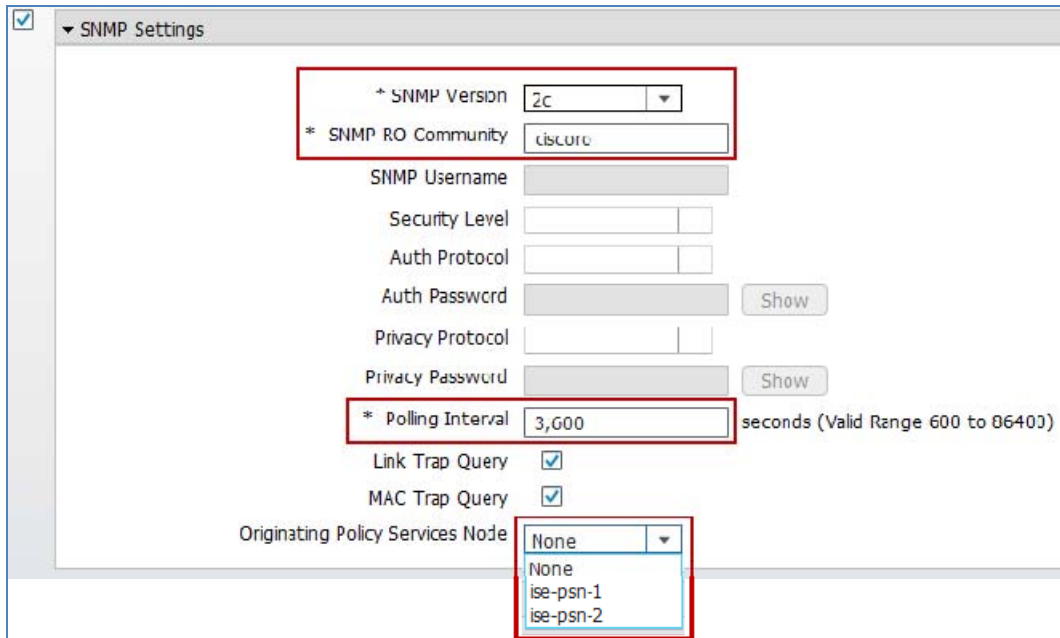
在 ISE（网络资源）中配置网络设备

通常，通过 RADIUS 对终端进行身份验证的所有网络接入设备都将在 ISE 中进行配置，因此所有必须要做的工作就是为这些接入设备逐一验证 SNMP 设置。如果为未部署 RADIUS 身份验证的网络配置 SNMP 查询探测功能，您必须向 ISE 网络设备列表添加各个接入设备，而且可以选择第 3 层设备（以获取 ARP 信息）。

- 步骤 1** 转至 Administration → Network Resources → Network Devices。如果要使用 SNMP 查询的设备已经存在，则只需从列表中选择该设备，或从右侧窗格点击 Add 即可。
- 步骤 2** 对于新设备，请输入设备名称和 IP 地址信息。

步骤 3 在 SNMP Settings 复选框中，指定接入设备使用的 SNMP 版本并输入 SNMP 版本 1 和 2c 的 SNMP RO 社区字符串，如果适用于接入设备，也可以输入 SNMPv3 凭证和配置（图 23）。

图 21. 网络接入设备配置：SNMP 查询



The screenshot shows the 'SNMP Settings' configuration page. The following fields are highlighted with red boxes:

- SNMP Version:** A dropdown menu set to '2c'.
- SNMP RO Community:** A text input field containing 'ciscoro'.
- Polling Interval:** A text input field containing '3,000' with the unit 'seconds (Valid Range 600 to 86400)'.
- Originating Policy Services Node:** A dropdown menu with options 'None', 'ise-psn-1', and 'ise-psn-2', where 'ise-psn-1' is selected.

步骤 4 对于系统（轮询）查询，请设置 Polling Interval 和 Originating Policy Services Node:

步骤 5 **Polling Interval:** 通常，在已部署 RADIUS 或 DHCP 探测功能的网络中，由于对 SRP 信息的依赖性降低，所以建议使用较长的轮询间隔。

步骤 6 **Originating Policy Services Node:** 已启用 SNMP 查询探测功能的每个 PSN 都将出现在列表中。选择执行网络设备定期轮询的最佳策略服务节点。从网络带宽角度看，这通常是距离网络设备最近的 PSN。

步骤 7 对于依赖 SNMP 陷阱的接口（触发）查询，请确保设置其中一个或两个陷阱查询选项。

注: Originating Policy Services Node 设置不适用于接口查询，因为这些查询通常是由接收 RADIUS 记帐开始或 SNMP 陷阱消息等触发器的 PSN 发送的。

步骤 8 完成之后，请保存更改。

步骤 9 为必须使用 SNMP 由 ISE 策略服务节点查询的每个接入设备重复以上步骤。

将有线接入设备配置为接受来自 ISE PSN 的 SNMP 查询

转至有线接入设备的管理控制台，然后验证设备是否已配置为支持已启用 SNMP 查询探测功能的 ISE 策略服务节点发送的 SNMP 只读请求。

以下是运行 IOS 的 Cisco Catalyst 交换机的配置示例，通过此配置可支持使用只读社区字符串 **ciscoro** 从 ISE PSN 发送的 SNMPv2c 查询：

```
snmp-server community ciscoro RO
snmp-server community ciscorw RW
```

将无线接入设备配置为接受来自 ISE PSN 的 SNMP 查询

转至无线局域网控制器的管理控制台，然后检验控制器是否已配置为支持已启用 SNMP 查询探测功能的 ISE 策略服务节点发送的 SNMP 只读请求。

- 步骤 1** 转至 Management → SNMP → Communities → SNMP v1 / v2c Community，然后配置可能查询此设备的 ISE 策略服务节点使用的一个或多个只读社区字符串。
- 步骤 2** 下图显示的 WLC 的示例配置，通过此配置可支持使用只读社区字符串 ciscoro 从 ISE PSN 发送的 SNMPv2c 查询：

图 22. 无线控制器的 SNMP 配置示例



Community Name	IP Address	IP Mask	Access Mode	Status
public	0.0.0.0	0.0.0.0	Read-Only	Enable
private	0.0.0.0	0.0.0.0	Read-Write	Enable
ciscoro	10.1.0.0	255.255.0.0	Read-Only	Enable
ciscorw	10.1.0.0	255.255.0.0	Read-Write	Enable

如果已部署 SNMPv3，请确保在 Management · SNMP · SNMP V3 Users 下配置相应的设置。

将接入设备配置为支持 CDP 和 LLDP

请确保接入设备已配置为在交换端口上接收这些协议。虽然默认情况下，思科设备上通常已启用 CDP，但 LLDP 则未启用。因此，如果想要使用 SNMP 查询探测功能收集此信息，请确保全局启用 LLDP。

```

cdp run
interface <Endpoint_Interface>
  cdp enable
!
lldp run
interface <Endpoint_Interface>
  lldp receive
  lldp transmit

```

注：对于无线客户端，无线局域网控制器不支持 CDP/LLDP。

验证 SNMP 查询探测功能数据

- 步骤 1** 从 Administration → Identity Management → Identities → Endpoints 删除终端。
- 步骤 2** 从配置为通过 ISE 进行 SNMP 访问的接入设备断开终端，然后重新连接。
- 步骤 3** 转至 ISE Policy Administration 节点并导航至 Administration → Identity Management → Identities。
- 步骤 4** 从左侧窗格选择 Endpoints。
- 步骤 5** 查找并选择新连接的终端的 MAC 地址，以显示 SNMP 查询探测功能捕获的属性。

图 25 所示示例仅使用了 SNMP 陷阱探测功能和 SNMP 查询探测，突出显示使用 SNMP 查询收集的属性。突出显示的关键属性包括 **EndPointSource**、**cdpCacheAddress** 和 **cdpCachePlatform**：

- **EndPointSource** 通知我们最后一次分析更新来自 SNMP 查询探测功能。
- **cdpCacheAddress** 提供 IP 地址并允许绑定 IP 和 MAC 地址。
- **cdpCachePlatform** 属性提供关于所连接终端的详细描述 - 在本例中所连接终端为 Cisco AIR-LAP1142N-A-K9，即 Cisco Aironet 1142N 无线接入点。

图 23. SNMP 查询探测功能属性示例

Endpoint

* MAC Address **C4:71:FE:34:19:7A**

* Policy Assignment Cisco-Access-Point

Static Assignment

* Identity Group Assignment Cisco-Access-Point

Static Group Assignment

Attribute List

EndPointPolicy	Cisco-Access-Point
EndPointProfilerServer	ise-psn-1
EndPointSource	SNMPQuery Probe
IdentityGroup	Cisco-Access-Point
MACAddress	C4:71:FE:34:19:7A
MatchedPolicy	Cisco-Access-Point
NADAddress	10.1.50.2
OUI	Cisco Systems
PolicyVersion	22
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	24
Total Certainty Factor	20
Vlan	14
VlanName	WIRELESS
cdpCacheAddress	10.1.14.100
cdpCacheCapabilities	T
cdpCacheDeviceId	APc471.fe34.197a
cdpCachePlatform	cisco AIR-LAP1142N-A-K9
cdpCacheVersion	Cisco IOS Software, C1140 Software (C1140-K9W8-M), Version 12.4(25e)JA, RELEASE SOFTWARE Copyright (c) 1986-2012 by Cisco Systems, Inc. Compiled Fri 27-Jan-12 21:45 by prod_rel_team
dot1xAuthAuthControlledPortControl	3
dot1xAuthAuthControlledPortStatus	2
ifDescr	GigabitEthernet1/0/2
ifIndex	10102
ifOperStatus	1
ip	10.1.14.100
port	2

步骤 6 要验证预期属性数据，您可以在接入交换机控制台中使用以下命令：

```
switch# show cdp neighbor detail
switch# show lldp neighbor detail
```

使用 DHCP 和 DHCP SPAN 探测功能进行分析

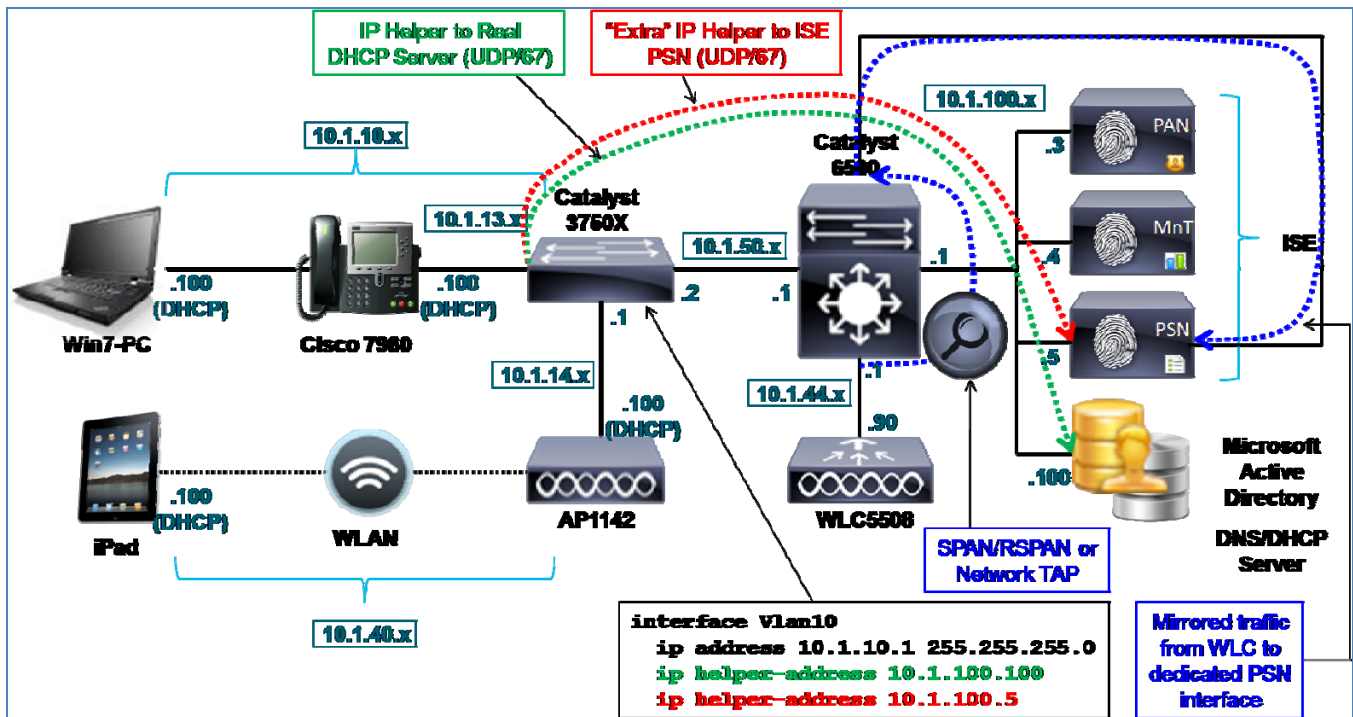
顾名思义，DHCP 探测功能是从 DHCP 数据包收集属性。可以使用以下一个或两个探测功能收集 DHCP 属性：

- DHCP 探测功能
- DHCP SPAN 探测功能

DHCP 探测功能

DHCP 探测功能旨在用于直接向 ISE 策略服务节点发送 DHCP 请求，例如作为网络中 DHCP 中继功能的结果。思科网络中常用的 DHCP 中继是应用于作为本地 DHCP 客户端网关的第 3 层接口的 `ip helper-address` 命令。图 26 显示的是使用 DHCP 探测功能的示例拓扑。

图 24. DHCP 探测功能示例



在图中，Cisco Catalyst 3750-X 有一个员工数据 VLAN 10 和一个语音 VLAN 13。在每个交换虚拟接口 (SVI) 的接口配置下都有一个 `ip helper-address` 命令，用于将 DHCP 广播数据包转发至地址为 10.1.100.100 的实际 DHCP 服务器（在图 26 中以绿色突出显示）。这是响应 DHCP 请求的服务器。在相同接口下，另一个 `ip helper-address` 命令配置为指向 DHCP 探测功能启用的 ISE PSN 接口（以红色突出显示）。ISE 策略服务节点不会回复这些数据包，目的只是为了将请求副本发送至 ISE 以解析 DHCP 属性。

可以在思科设备上将多个 IP 帮助程序目标配置为允许多个 ISE 策略服务节点接收 DHCP 请求副本。

注：ISE DHCP 探测功能可以解析来自 DHCP 中继和 DHCP 代理的流量。这些方法之间的一个主要区别是通过 `ip helper-address` 命令的 DHCP 中继能够向多个目标发送流量，因此允许多台实际 DHCP 服务器和 ISE 策略服务节点接收 DHCP 请求的副本。另一方面，DHCP 代理将只向主要 DHCP 服务器发送请求，而且只有在没有收到有效响应的情况下，才会退回其他已配置的 DHCP 目标。虽然可以将 ISE 节点配置为第一个条目，从而允许退回实际 DHCP 服务器，但是这种配置会延迟终端获取 IP 地址所需的时间。这会影响用户体验，还可能导致客户端在等待响应的时候出现超时。

DHCP SPAN 探测功能

DHCP SPAN 探测功能旨在用于使用交换端口分析器 (SPAN)、远程 SPAN (RSPAN) 或网络分流器等方法将流量镜像于 ISE 策略服务节点上的接口的情况。此方法主要用于使用 DHCP 中继的基本 DHCP 探测功能不可用或无法使用的情况。

最佳实践：对于任何给定的 DHCP 流量，都应选择一个探测功能来从该流量搜集属性。在同时使用 DHCP (IP 帮助程序) 和 DHCP SPAN 探测功能从同一 DHCP 流量收集属性方面，价值有限。

如果 DHCP 探测功能可用，建议使用 DHCP 探测功能而不要使用 DHCP SPAN 探测功能。仅通过 DHCP 中继发送 DHCP 数据包可以减少用于检查和解析来自 DHCP 数据包的属性的 ISE 策略服务节点上的总流量负载。

DHCP SPAN 探测功能也可用于从本地子网广播捕获 DHCP 流量，而使用 DHCP 探测功能只能捕获上游网关中继的 DHCP 流量。当第 3 层网关同时作为本地客户端的 DHCP 服务器时，就有这种必要。如果思科 IOS DHCP 服务器也配置成为该子网提供 DHCP 服务，则不会中继 DHCP 任何片段。

示例拓扑说明的是使用 SPAN 或网络分流器从连接 WLC 的无线客户端将数据包复制到策略服务节点上的专用接口（图 26 中以蓝色突出显示）。因为 SPAN 目标端口可能会有多个特殊属性限制收发以 PSN 为目标的正常流量，所以需要专用接口。此外，我们不希望镜像流量导致 RADIUS 等 PSN 的其他关键接口出现拥塞。使用 SPAN 方法，可能会向 SPAN 端口发送超出其处理能力的更多数据，从而导致关键流量出现丢包或延迟。

DHCP 属性

DHCP 探测功能和 DHCP SPAN 探测功能都向 ISE 提供相同的关键分析属性，包括以下一些属性：

- `dhcp-class-identifier`
- `dhcp-user-class-id`
- `dhcp-client-identifier`
- `dhcp-message-type`
- `dhcp-parameter-request-list`
- `dhcp-requested-address`
- `host-name`
- `domain-name`
- `client-fqdn`

因为 DHCP 既提供 MAC 地址 (`dhcp-client-identifier`)，又提供 IP 地址 (`dhcp-requested-address`)，所以还可以为 ISE ARP 缓存表建立 IP 到 MAC 地址绑定。这对于支持依赖 IP 地址而非 MAC 地址的其他探测功能很有用。要应用就特定终端提供的属性并将这些属性保存到 ISE 数据库中，需要根据 MAC 地址将 IP 地址与具体终端关联。

除了 **dhcp-client-identifier** 和 **dhcp-requested-address**，其他关键属性还包括 **dhcp-class-identifier**、**dhcp-user-class-id** 和 **dhcp-parameters-request-list**。类别标识符通常用于传输平台或操作系统信息。可以在 Mac OS 和 Microsoft Windows 等有些客户端操作系统上将类别标识符以及用户类别 ID 自定义为用作的分析唯一企业标识符，或供 DHCP 服务器返回唯一范围值。

dhcp-parameters-request-list 提供可能唯一的设备类型指示符，因为所请求的参数的值和序列对于单个或有限个设备类型通常是唯一的。例如 **dhcp-parameters-request-list** 值 1, 3, 6, 15, 119, 252 代表 iPad、iPod 或 iPhone 等 Apple iOS 设备。

如果为特定终端部署了标准主机名、域名或完全限定域名 (FQDN) 命名约定，可以使用这些属性对终端进行分类。例如，如果所有 Windows XP 客户端都分配了一个名称（例如 **jsmith-winxp**），则在某个条件下可以使用 **host-name** 属性或 **client-fqdn** 属性来给 Windows XP 终端进行分类。同样地，如果约定将公司终端的 **host-name** 填为 **jsmith-corp-dept** 之类的内容，则可将此属性用于验证公司资产。

必须注意，不要将配置文件属性混淆为身份，但是属性可以提高确定终端为某个类型的可信度。例如，授权策略可用于分析，拒绝向 PC 的 **host-name** 属性（如匹配的终端身份组所示）不包含预期值的员工授予完全访问权限。

一般来说，DHCP 具有很多分析优势，而且通常是任何环境中大部分终端分类的基础，因为大多数终端都提供包含详细平台信息的 DHCP “指纹”。

配置 DHCP 和 DHCP SPAN 探测功能

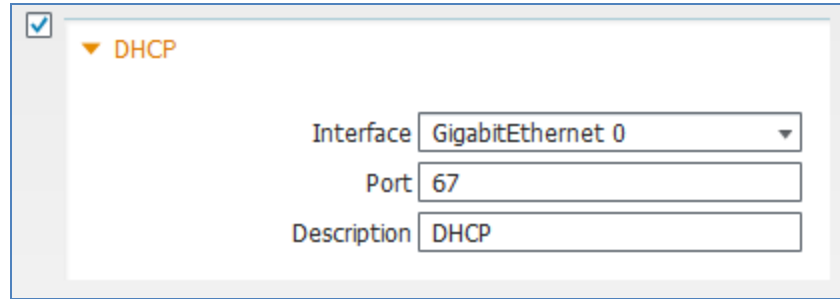
要使用 DHCP 探测功能，必须将接入设备（或仅限第 2 层的接入设备的下一跳网关）配置为向配置用于分析服务的 ISE PSN 发送 DHCP 中继或 DHCP 代理数据包。要使用 DHCP SPAN 探测功能，网络必须通过专用接口向 ISE PSN 发送多份网络流量，最好是经过过滤只包含 DHCP 的部分流量。

要使基于 DHCP 的探测功能有效，还有一个要求是相应终端必须使用 DHCP 获取其 IP 地址。这个可能看起来很明显，但是很多客户可能使用的是具有静态 IP 地址分配的无客户端设备。在这些情况下，可以部署静态 DHCP 保留，从而允许终端保持一个特定 IP 地址，同时允许对 IP 寻址进行集中管理并通过 DHCP 为 ISE 分析提供支持。

在 ISE 中启用 DHCP 探测功能

- 步骤 1** 转至 Administration → System → Deployment，并从右侧窗格已部署节点的列表中选择要执行分析的策略服务节点。
- 步骤 2** 选择 Profiling Configuration 选项卡。
- 步骤 3** 要添加对 DHCP 探测功能（例如用于 IP 帮助程序）的支持，请选中标记为 DHCP 的复选框，如图 27 左上角所示。

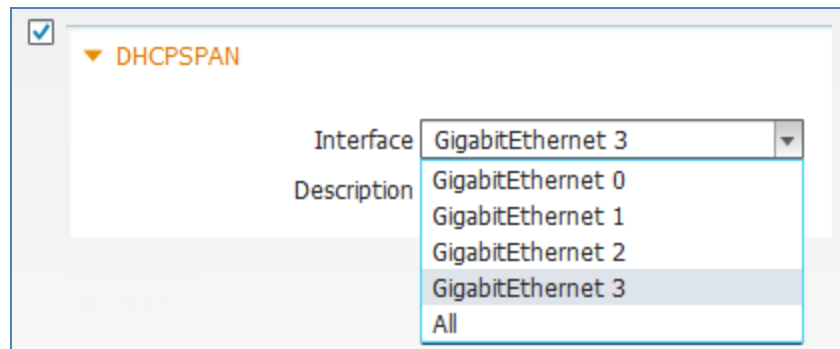
图 25. DHCP 探测功能配置



DHCP
 Interface: GigabitEthernet 0
 Port: 67
 Description: DHCP

步骤 4 要添加对 DHCP SPAN 探测功能（用于 SPAN 或其他端口镜像解决方案），请选择标记为 DHCPSPAN 的复选框（图 28）。

图 26. DHCP 探测功能配置 - 接口



DHCPSPAN
 Interface: GigabitEthernet 3
 Description: GigabitEthernet 0, GigabitEthernet 1, GigabitEthernet 2, GigabitEthernet 3, All

步骤 5 选择用于收集 DHCP 流量的接口。

要用于 IP 帮助程序（DHCP 中继），所使用的接口通常是用于会话服务的默认接口。但是，在预计会出现更高 DHCP 流量的更大型环境中，您可能需要使用专用接口 - 例如千兆以太网 1、2 或 3。

要用于镜像流量（SPAN/RSPAN/分流器），此接口应该是专用接口。

步骤 6 点击 Save 以提交更改。

步骤 7 对已配置分析服务的所有其他策略服务节点重复本程序中的步骤。

注：由于对流量镜像的要求，可能无法将多个策略服务节点配置为接收 SPAN 或这种配置不可行。如果镜像相同流量，可能无需向多个策略服务节点转发相同流量。虽然这样做可以增加一定的冗余，但是会大幅提高 ISE 节点上的负载，导致必须在所有其他节点上关联和同步的分析数据形成不必要的重复。

向 ISE（网络资源）添加网络设备

虽然支持 RADIUS 或 SNMP 的接入设备可能已经添加到 ISE 网络设备列表中（在 Administration → Network Resources → Network Devices 下），但是无需专门为向 DHCP 探测功能或 DHCP SPAN 探测功能转发 DHCP 而向 ISE 添加网络设备。

将 ISE 策略服务节点接口配置为接收 DHCP 中继数据包（仅 DHCP 探测功能）

如果已在默认千兆以太网 0 接口上启用 DHCP 探测功能，此程序即已完成。如果要使用另一个接口来接收 DHCP 中继流量，则请完成以下步骤。

步骤 1 以物理方式将所需接口与网络交换端口连接。

步骤 2 访问 ISE PSN 控制台 (CLI)。如图 29 所示，启用相应接口并分配有效的 IP 地址。

图 27. 用于接入交换机的 DHCP 中继配置示例

```
ise-psn-1/admin# conf t
Enter configuration commands, one per line. End with CNTL/Z.
ise-psn-1/admin(config)# interface GigabitEthernet 3
ise-psn-1/admin(config-GigabitEthernet)# ip address 10.1.99.100 255.255.255.0

Changing the IP may result in undesired side effects on
any installed application(s).
Are you sure you want to proceed? Y/N [N]: Y
ISE M&T Log Processor is not running.
ISE M&T Log Collector is not running.
ISE M&T Alert Process is not running.
Stopping ISE Application Server...
ISE M&T Session Database is not running.
Stopping ISE Database processes...
Starting ISE Database processes...
ISE M&T Session Database is not running.
Starting ISE Application Server...
Note: ISE Processes are initializing. Use 'show application status ise'
CLI to verify all processes are in running state.
ise-psn-1/admin(config-GigabitEthernet)# _
```

步骤 3 验证所有进程是否都按照说明运行。

步骤 4 验证新配置接口的配置并且验证是否已使用 **show running-config** 命令启用该接口，即其不是处于关闭状态（图 30）。

图 28. 验证用于接入交换机的 DHCP 中继配置示例

```
ise-psn-1/admin# show running-config
Generating configuration...
?
hostname ise-psn-1
?
ip domain-name cts.local
?
interface GigabitEthernet 0
  ip address 10.1.100.5 255.255.255.0
  ipv6 address autoconfig
?
interface GigabitEthernet 1
  shutdown
  ipv6 address autoconfig
?
interface GigabitEthernet 2
  shutdown
  ipv6 address autoconfig
?
interface GigabitEthernet 3
  ip address 10.1.99.100 255.255.255.0
  ipv6 address autoconfig
?
ip name-server 10.1.100.100
--More--
```

步骤 5 通过从需要中继 DHCP 的网络设备发送 ICMP ping，验证与新 ISE 探测功能接口的连接。

步骤 6 使用 CLI 命令 `copy running-config startup-config` 保存更改。

将 ISE 策略服务节点接口配置为接收 SPAN 流量（仅 DHCP SPAN 探测功能）

步骤 1 以物理方式将所需的接口连接至相应的 SPAN 目标端口或网络分流器接口。

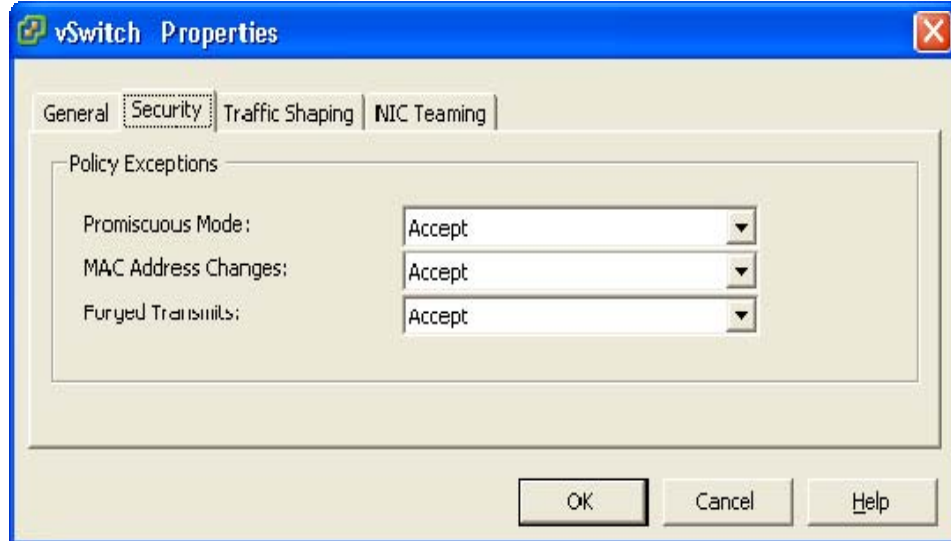
步骤 2 访问 ISE PSN 控制台 (CLI)。在所需接口的配置模式下，只需输入 `no shutdown`，即可启用相应的接口。

步骤 3 使用 ISE CLI 命令 `copy running-config startup-config` 保存更改。

注：对于在 VMware 设备上运行的策略服务节点

要为分析使用专用接口，则要求已为虚拟设备配置附加虚拟接口。如果未在安装时完成此操作，则在继续进行 ISE 配置之前，需要为所需的接口关闭 ISE 节点并更新 ESX 设备的硬件和网络配置。

此外，要接受 ISE DHCP SPAN 接口上的 SPAN/镜像流量，VMware 设备要求在虚拟交换机接口上设置混杂模式。要启用此模式，请转至 VMware Host → Configuration → Hardware → Networking → vSwitch → Security 并设置 Promiscuous Mode: Accept（默认值为 Reject），如下所示：



将有线接入设备配置为将 DHCP 数据包中至 ISE PSN（仅 DHCP 探测功能）

转至 Cisco Catalyst 交换机或路由器的管理控制台。在连接至产生 DHCP 流量的终端子网的各路由接口下，添加以下命令：

```
interface <Endpoint_VLAN>  
ip helper-address <ISE_PSN_address>
```

指定的地址应该是指向已启用 DHCP 探测功能的 PSN 接口。为了冗余，您可以添加更多 IP 帮助程序语句，将 DHCP 中继至其他策略服务节点，但是建议仅保留最低数量以降低流量重复，因为每个 PSN 都将处理所接收的流量。

将无线接入设备配置为将 DHCP 数据包中继至 ISE PSN（仅 DHCP 探测功能）

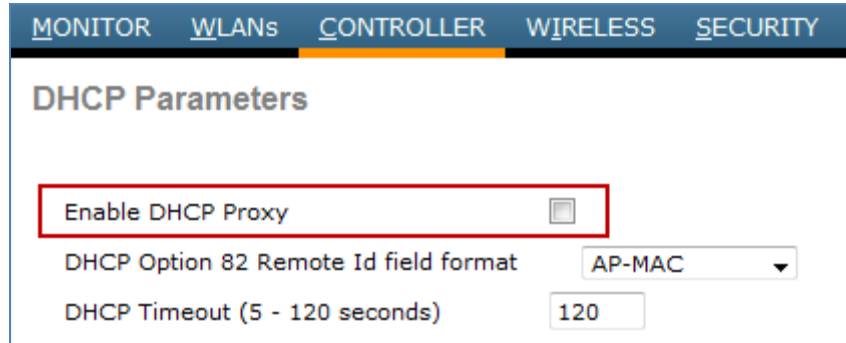
建议您在 DHCP 桥接模式而非 DHCP 代理模式下配置 WLC，这样 DHCP 数据包就将从无线客户端转发至 ISE PSN。

转至思科无线局域网控制器或无线服务模块的 Web 管理界面。

步骤 1 导航至 Controller → Advanced → DHCP → DHCP Parameters。

步骤 2 如果已选中标记为 Enable DHCP Proxy 的复选框，则取消选中此复选框（图 31）。

图 29. 无线控制器的 DHCP 中继配置示例



步骤 3 对于在使用 DHCP 的 WLC 上配置的每个 WLAN，请确保如前面的程序中所述，上游网关配置为将 DHCP 中继至 ISE 策略服务节点中。

将网络设备配置为将多份 DHCP 流量发送至 PSN（仅 DHCP SPAN 探测功能）

有多种方式可将流量镜像到 ISE 策略服务节点。本程序将介绍在 Cisco Catalyst 交换机上使用基本 SPAN 的一种常用方法。

确定将作为 DHCP 流量来源的接口或 VLAN。WLC 的出口接口或与 DHCP 服务器的连接等某些阻塞点可以作为捕获所有客户端 DHCP 数据包的理想位置。

在下面的示例中，接口千兆以太网 1/1 是思科 5500 系列无线局域网控制器的中继连接。接口千兆以太网 2/37 是连接运行 VMware ESXi 4.1 的 Cisco UCS[®] 服务器的一个交换端口连接。ESX 服务器承载配置为启用分析功能的策略服务节点的一个 ISE 虚拟设备。接口千兆以太网 2/37 连接至与作为千兆以太网 3 的 ISE PSN 链接的虚拟接口。

```
interface GigabitEthernet1/1
description WLC5508 ETH0 (Port 1)
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 40-44
switchport mode trunk

interface GigabitEthernet2/37
description UCS1 SPAN (port 3 of 4)
switchport
```

将 SPAN 配置为捕获 5500 交换机连接上的所有入站和出站流量并转发至 ISE PSN 连接。为此，接口千兆以太网 1/1 要设置为 SPAN 源并且接口千兆以太网 2/37 要设置为目标。因为 ISE 无需看见带标记的数据包，所以在交换端口上未启用 802.1Q 中继。

```
cat6500(config)# monitor session 1 source interface gigabitEthernet 1/1 both
cat6500(config)# monitor session 1 destination interface gigabitEthernet 2/37
```

确认配置并保存。

```
cat6500# show monitor session 1
Session 1
-----
Type                : Local Session
Source Ports        :
  Both              : Gi1/1
Destination Ports   : Gi2/37

Egress SPAN Replication State:
Operational mode    : Centralized
Configured mode     : Centralized (default)
```

验证 DHCP 探测功能数据

- 步骤 1** 从 Administration → Identity Management → Identities → Endpoints 删除终端。
- 步骤 2** 从网关接口拥有将 DHCP 转发至 ISE PSN 的 IP 帮助程序的接入设备断开并重新连接终端。
- 步骤 3** 转至 ISE Policy Administration 节点并导航至 Administration → Identity Management → Identities。
- 步骤 4** 从左侧窗格选择 Endpoints。
- 步骤 5** 查找并选择新连接的终端的 MAC 地址，显示 DHCP 探测功能捕获的属性（图 32）。所显示的示例仅使用 DHCP 探测功能，以突出显示使用 DHCP 收集的属性。

图 30. DHCP 探测功能属性示例

Endpoint List > 00:30:94:C4:52:8A

Endpoint

* MAC Address **00:30:94:C4:52:8A**

* Policy Assignment Cisco-IP-Phone

Static Assignment

* Identity Group Assignment Cisco-IP-Phone

Static Group Assignment

Attribute List

EndPointPolicy	Cisco-IP-Phone
EndPointProfilerServer	ise-psn-1
EndPointSource	DHCP Probe
IdentityGroup	Cisco-IP-Phone
MACAddress	00:30:94:C4:52:8A
MatchedPolicy	Cisco-IP-Phone
OUI	Cisco Systems, Inc
PolicyVersion	22
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	24
Total Certainty Factor	30
chaddr	00:30:94:c4:52:8a
ciaddr	0.0.0.0
dhcp-class-identifier	Cisco Systems, Inc. IP Phone CP-7960
dhcp-client-identifier	01:00:30:94:c4:52:8a
dhcp-message-type	DHCPDISCOVER
dhcp-parameter-request-list	1, 66, 6, 3, 15, 150, 35
dhcp-requested-address	10.1.13.100
flags	0x8000
giaddr	10.1.13.1
hlen	6
hops	1
host-name	SEP003094C4528A
htype	Ethernet (10Mb)
ip	10.1.13.100
op	BOOTREQUEST
secs	0
yiaddr	0.0.0.0

突出显示的关键属性包括：

- EndPointSource
- OUI
- dhcp-class-identifier
- dhcp-client-identifier
- dhcp-parameter-request-list
- dhcp-requested-address

EndPointSource 显示 DHCP 探测功能最后一次属性更新的来源。

dhcp-client-identifier 通常提供 MAC 地址，此地址转而通过来自 MAC Address-OUI 映射表的关联提供供应商 OUI 信息。

dhcp-requested-address 是终端请求的 IP 地址。此属性连同 **dhcp-client-identifier** 一起提供 IP 和 MAC 地址之间的绑定。

dhcp-class-identifier 通常提供唯一的平台特定属性，并且在有些情况下提供所连接终端的详细说明 - 在本例中即 Cisco Systems, Inc. IP Phone CP-7960。

dhcp-parameter-request-list 也会指示终端为思科 IP 电话，因为通常只有某些思科 IP 电话使用与 1, 66, 6, 3, 15, 150, 35, 151 一致的序列。

总之，一个或多个属性可以给使用 DHCP 给网络终端分类。如本指南下文中[设备传感器](#)章节所述，思科提供使用叫做设备传感器的一种本地分类技术收集 DHCP 和其他信息的功能。即使在无法通过 IP 帮助程序或 SPAN 技术收集 DHCP 属性的时候，仍然可以使用此功能收集 DHCP 属性。此解决方案为终端属性收集和分类提供了一种更具可扩展性的方法。

使用 HTTP 探测功能进行分析

Web 浏览器通常会通过向 Web 服务器提交特性标识明确自己的身份，包括应用程序类型、操作系统，软件供应商和软件版本。在 HTTP 中，此标识是通过叫做 **User-Agent** 的 HTTP 请求报头字段传输的。

User-Agent 是使用 HTTP 探测功能收集的主要属性。ISE 分析功能可以捕获 **User-Agent** 属性提供的 Web 浏览器信息，以及请求消息提供 HTTP 属性，并将其添加至终端属性的列表中。思科 ISE 提供很多默认配置文件，这些配置文件内置于系统之中，根据 **User-Agent** 属性标识终端。

用于向 HTTP 探测功能发送 HTTP 流量的两个方法如下：

- URL 重定向
- SPAN（和其他流量镜像方法）

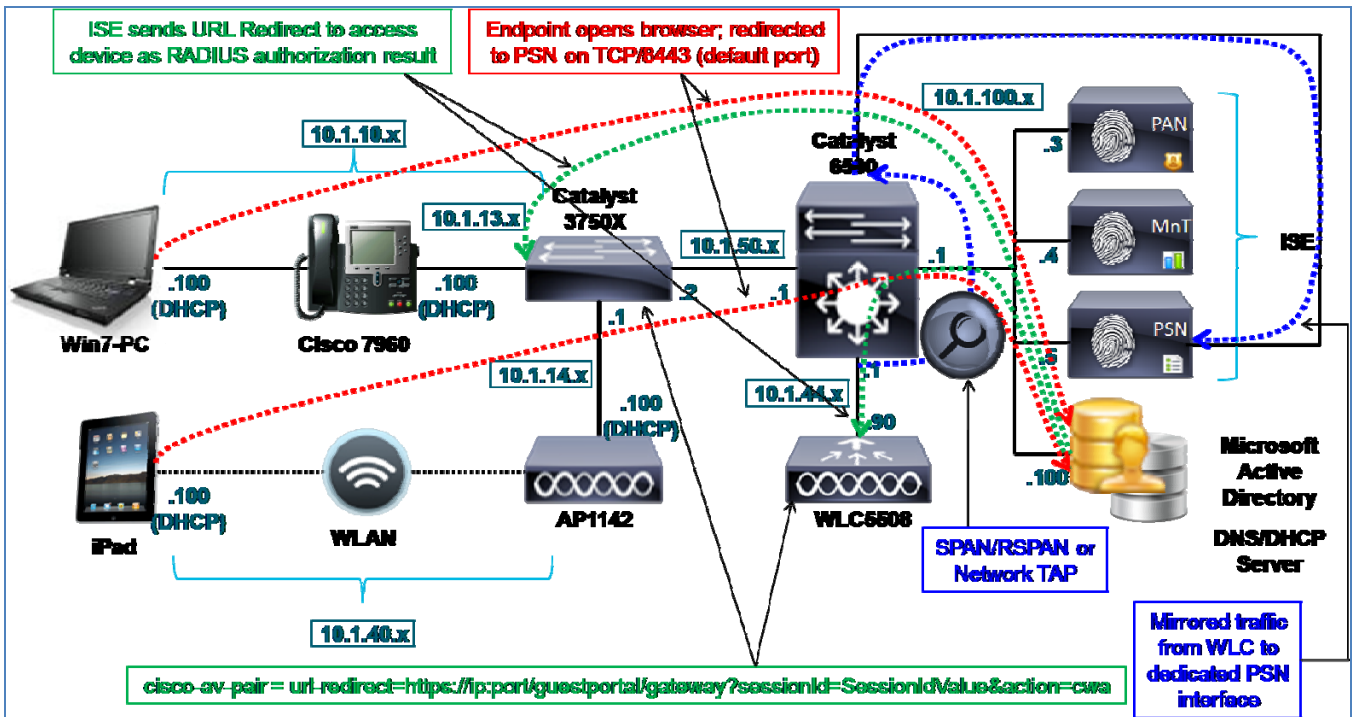
HTTP 探测功能侦听端口 80 和端口 8080 上来自 Web 浏览器的通信。URL 重定向和 SPAN 方法都向 HTTP 探测功能提供 **User-Agent** 属性。

使用 URL 重定向的 HTTP 探测功能

ISE 将 URL 重定向用于很多用户会话服务，包括集中 Web 身份验证 (CWA)、本地 Web 身份验证 (LWA)、设备注册 Web 身份验证 (DRW)、客户端调配、安全状态评估和本机请求方调配 (NSP)。在这其中每个使用案例中，终端的 Web 浏览器都被重定向至 ISE 策略服务节点。在此过程中，ISE 可以捕获 User-Agent 属性。

图 33 中的示例拓扑描述了将 URL 重定向用作终端初始授权的一部分，这样 ISE 可以向接入设备发送一个 URL 重定向（图 33 中以绿色突出显示）。当客户端打开 Web 浏览器时，将被重定向到用于集中 Web 身份验证等指定服务的策略服务节点（以红色突出显示）。

图 31. HTTP 探测功能示例



URL 重定向可以是网络接入设备 (NAD) 的一个功能。NAD 发起的重定向的一个示例是本地 Web 身份验证，其中有线交换机或无线控制器将客户端浏览器重定向至 ISE 访客门户，提供 Web 身份验证页面。

URL 重定向也可以启动作为从 ISE 到网络接入设备的一种 RADIUS 授权。由 RADIUS 授权触发的一个 URL 重定向示例即集中 Web 身份验证，其中接入设备帮助进行重定向，但是会在客户端和 ISE 策略服务节点之间建立实际会话，并且通过唯一会话 ID 跟踪此会话。

使用 SPAN 的 HTTP 探测功能

要在不使用 URL 重定向的情况下使用 HTTP 探测功能，可选的方法是使用 SPAN、RSPAN 或网络分流器等方法将 Web 流量复制或映射至 ISE 策略服务节点上的接口。此方法主要用于当 URL 重定向不可行或无法使用时。

最佳实践：在基于 RADIUS 的环境等适用情况下，URL 重定向方法优先于 HTTP SPAN。在重定向期间只捕获 **User-Agent** 属性可以减少 ISE 策略服务节点上的总体流量负载，检查和解析来自 HTTP 数据包的属性。

如果 URL 重定向不适用，例如在不使用基于 RADIUS 的身份验证的思科 NAC 设备部署中，或在尚需向接入设备部署 RADIUS 的终端发现阶段，则优先使用 SPAN 方法，因为其允许捕获 **User-Agent** 而不要求 RADIUS 或 URL 重定向。

图 33 中的示例拓扑说明的是使用 SPAN 或网络分流器从 WLC 所连接的无线客户端将数据包复制到策略服务节点上的专用接口（以蓝色突出显示）。因为 SPAN 目标端口可能会有多个特殊属性限制收发以 PSN 为目标的正常流量，所以需要专用接口。此外，我们不希望镜像流量导致 RADIUS 等 PSN 的其他关键接口出现拥塞。使用 SPAN 方法，可能会向 SPAN 端口发送超出其处理能力的更多数据，从而导致关键流量出现丢包或延迟。

HTTP 探测功能和 IP 到 MAC 地址绑定要求

因为 HTTP 流量不包括终端的 MAC 地址，因此 ISE 策略服务节点在其用于终端的 ARP 缓存表中必须已经有一个 IP 到 MAC 地址绑定，才能将发送的数据与 HTTP 探测功能正确关联。换句话说，如果 ISE 无法通过终端的 MAC 地址识别终端或没有关联的 IP 地址，则 HTTP 探测功能识别的分析数据将被废弃，因为没有终端可让它应用所识别的 **User-Agent** 属性。因此，必须在收集 HTTP 数据之前通过另一个探测功能识别 IP 到 MAC 地址绑定。可用于提供此信息的探测功能如下：

- RADIUS（通过 **Framed-IP-Address** 属性）
- DHCP（通过 **dhcp-requested-address** 属性）
- SNMP 查询（通过 SNMP 轮询）

有为 IP 到 MAC 绑定要求提供特例的特殊 HTTP 分析方案。其中包括：

- 用于客户端调配的 URL 重定向
- 用于集中 Web 身份验证的 URL 重定向

用于客户端调配的 URL 重定向

客户端调配 (CP) 是一种 ISE 会话服务，为终端提供代理和配置文件的动态下载，从而启用状态代理和本机请求方调配 (NSP) 服务。客户端调配依赖于 URL 重定向。在 CP 过程中，策略服务节点必须通过其用户代理确定客户端操作系统，从而了解要应用哪项调配策略。例如，如果终端检测为 Windows 客户端，则应该为状态支持选择 Windows 状态代理。同样，如果终端检测为一台 Android 客户端，则应该在终端上安装用于 Android 客户端的请求方调配文件。

当客户端调配服务获取 **User-Agent** 属性时，ISE 将使用此信息更新分析服务，运用这种识别。此外，由于客户端调配是活动会话的一部分，ISE 能够将此信息应用于从会话缓存检索的 MAC 地址 (**Calling-Station-ID**)。因此，可以使用这一个流程，完全分析很多终端。

用于集中 Web 身份验证的 URL 重定向

集中 Web 身份验证 (CWA) 依赖于 URL 重定向。在 CWA 过程中，HTTP 探测功能能够在策略服务节点上解密之后根据重定向的 HTTP 数据包捕获 **User-Agent** 属性。类似于客户端调配服务，访客流量是活动会话的一部分，ISE 能够通过此会话从会话缓存检索 MAC 地址 (**Calling-Station-ID**)。此过程使 HTTP 探测功能可以识别 **User-Agent** 和填充终端数据库所需的关联 MAC 地址。

总体上，HTTP 探测功能为通过 **User-Agent** 检测客户端操作系统类型提供了更高的检测精度。当要求使用基于操作系统的策略，特别是针对客户经常需要根据终端属于个人资产还是公司资产提供不同访问权限的无线环境，建议使用 HTTP 探测功能。

在使用 CP 的 URL 重定向和使用 CWA 的 URL 重定向这两种方案中，ISE 都能够将 **User-Agent** 属性应用于 MAC 地址，而无需预先设置 IP 到 MAC 地址绑定。HTTP SPAN 方法始终要求有现有的 IP 到 MAC 绑定条目，除非所镜像的流量来自邻近终端的第 2 层片段。在此特定情况下，数据包源 MAC 地址为实际终端的 MAC 地址，并且可以用于相应地更新终端数据库。

最佳实践：要获取 **User-Agent**，请使用 URL 重定向，其中将 HTTP 探测功能用于 CWA 使用情况。当要求使用状态代理或本机请求方调配服务时，系统自动执行将 URL 重定向用于客户端调配的分析功能，但是在有些情况下，即使不需要使用状态或请求方调配，仍可能需要特意触发 CP。当终端配置文件设置为 Unknown 或 Incomplete 时，可以通过重定向到 CWA（当启用状态代理时）或客户端调配和状态 (CPP) 服务（状态发现）完成此操作。其目标是捕获流程中的 **User-Agent** 并且允许生成的安全状态触发授权更改 (CoA)。重新连接之后，可根据更准确的配置文件匹配分配新的授权策略规则。

如上所述，通常 URL 重定向都优先于 HTTP SPAN，因为与镜像方法相比它允许策略服务节点通过最小的流量负载获取 **User-Agent** 属性；在有些特殊情况下还可以在不首先填充 ARP 缓存的情况下进行分析。此外，基于 RADIUS 授权的 URL 重定向可简化高可用性场景，因为重定向始终是发送到终止 RADIUS 流量的同一 PSN。

但是，在未部署 RADIUS 的接入设备等有些场景下，SPAN 方法可能是唯一可行的方案。

配置 HTTP 探测功能

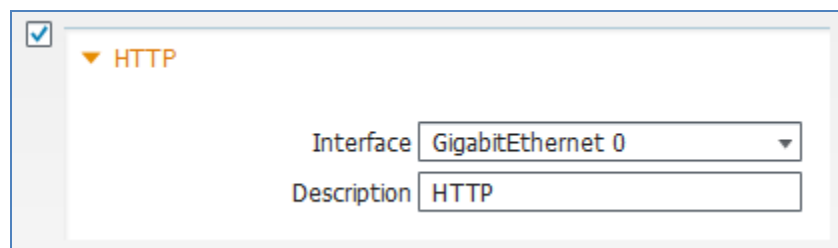
要将 HTTP 探测功能用于重定向的流量，接入设备必须能够直接（例如通过本地 Web 身份验证）或通过 RADIUS 授权将 HTTP 流量重定向至 ISE。对基于 RADIUS 的重定向，必须使用授权策略规则将 ISE 配置为返回用于 **url-redirect** 的思科属性值对 (AVP)，作为授权结果。

要在使用 SPAN 的情况下使用 HTTP 探测功能，网络必须通过专用接口向 ISE PSN 发送多份网络流量，最好是经过过滤只包含 HTTP 的部分流量。

在 ISE 中启用 HTTP 探测功能

- 步骤 1** 转至 Administration → System → Deployment，并从右侧窗格已部署节点的列表中选择要执行分析的策略服务节点。
- 步骤 2** 选择 Profiling Configuration 选项卡。要为 HTTP 探测功能添加支持，请选中标记为 HTTP 的复选框（图 34）。

图 32. HTTP 探测功能配置

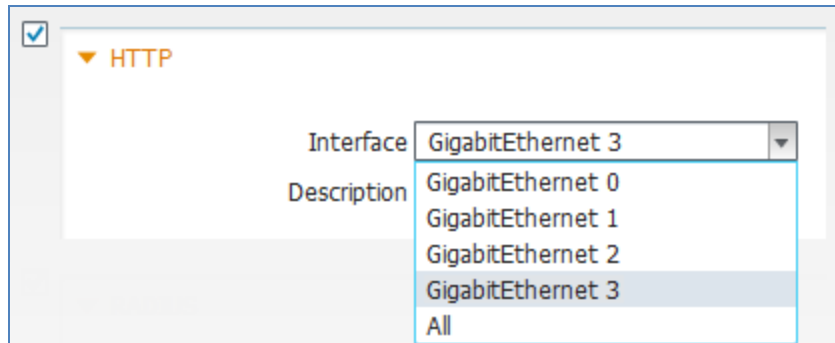


步骤 3 选择用于收集 HTTP 流量的接口。

步骤 4 要用于 URL 重定向，则所使用的接口应该为千兆以太网 0，即用于 RADIUS、Web 身份验证、安全状态等会话服务的相同接口。

步骤 5 要用于镜像流量（SPAN/RSPAN/分流器），此接口应该是专用接口（图 35）。

图 33. HTTP 探测功能配置 - 接口



步骤 6 点击 Save 以提交更改。

步骤 7 对已配置分析服务的所有其他策略服务节点重复本程序中的步骤。

注：由于对流量镜像的要求，将多个策略服务节点配置为接收 SPAN 是可能而且切实可行的。如果镜像相同流量，则可能无需向多个策略服务节点转发相同流量。虽然这样做可以增加一定的冗余，但是会大幅提高 ISE 节点上的负载，导致必须在所有其他节点上关联和同步分析数据，形成不必要的重复。

向 ISE（网络资源）添加网络设备

当使用 URL 重定向方法捕获 HTTP 数据时，网络接入设备必须已经配置为支持基于 RADIUS 的身份验证，从而无需执行任何额外的步骤来添加或编辑网络接入设备。

当使用 SPAN 方法捕获 HTTP 数据时，如果不执行基于 RADIUS 的身份验证，则没有向 ISE 添加接入设备的具体要求。

将 ISE 策略服务节点接口配置为接收重定向的 HTTP 流量

当使用 URL 重定向时，应该在默认千兆以太网 0 接口上启用 HTTP 探测功能。因此，无需进行额外的接口配置。

将 ISE 策略服务节点接口配置为接收 HTTP SPAN 流量

当使用 SPAN 时，应该在专用 SPAN 接口上将 HTTP 探测功能配置为接收 HTTP 流量。要在 ISE 上配置专用 SPAN 接口，请完成以下步骤：

步骤 1 以物理方式将所需的接口连接至相应的 SPAN 目标端口或网络分流器接口。

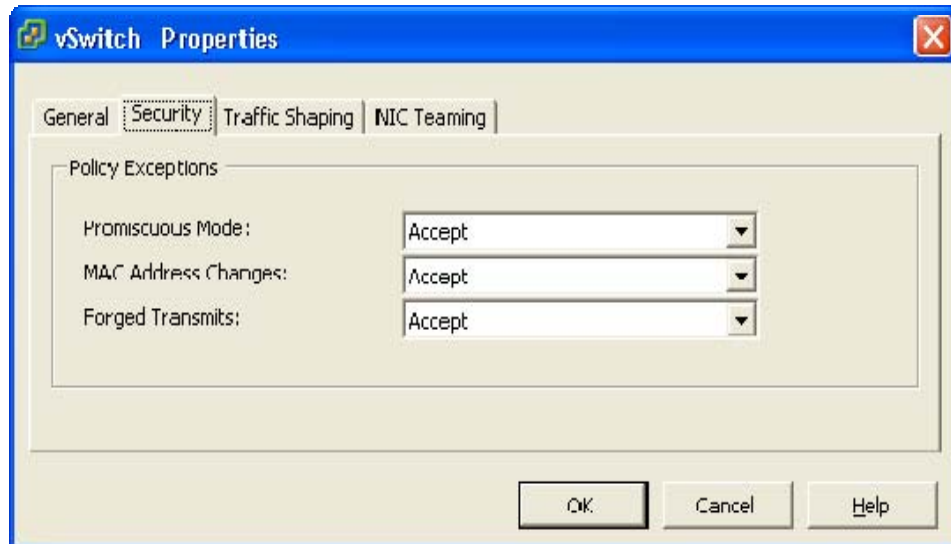
步骤 2 访问 ISE PSN 控制台 (CLI)。在所需接口的配置模式下，只需输入 **no shutdown**，即可启用相应的接口。

步骤 3 使用 ISE CLI 命令 **copy running-config startup-config**，保存更改。

注：对于在 VMware 设备上运行的策略服务节点

要为分析使用专用接口，则要求已为虚拟设备配置附加虚拟接口。如果未在安装时完成此操作，则在继续进行 ISE 配置之前，需要为所需的接口关闭 ISE 节点并更新 ESX 设备的硬件和网络配置。

此外，要接受 ISE DHCP SPAN 接口上的 SPAN/镜像流量，VMware 设备要求在虚拟交换机或接口上设置混杂模式。要启用此模式，请转至 VMware Host → Configuration → Hardware → Networking → vSwitch → Security 并设置 Promiscuous Mode: Accept（默认值为 Reject），如下所示：

**将有线接入设备配置为将 HTTP 数据包重定向至 ISE PSN**

配置接入设备，从而为 CWA、安全状态或请求方调配等具体服务提供 URL 重定向支持不在本指南内容范围之内。总之，用于使用 Cisco Catalyst 交换机根据 RADIUS 授权支持重定向的重要命令与以下内容相似：

- 在全局配置模式下，启用 HTTP 和可选的 HTTPS 服务器。
- 配置在 ISE RADIUS 授权中引用的重定向 ACL 来指定符合重定向条件的流量。

```
ip http server
ip http secure-server
ip access-list extended REDIRECT-ACL
deny tcp any any <PSN_IP_address>
permit tcp any any eq http
permit tcp any any eq https
```

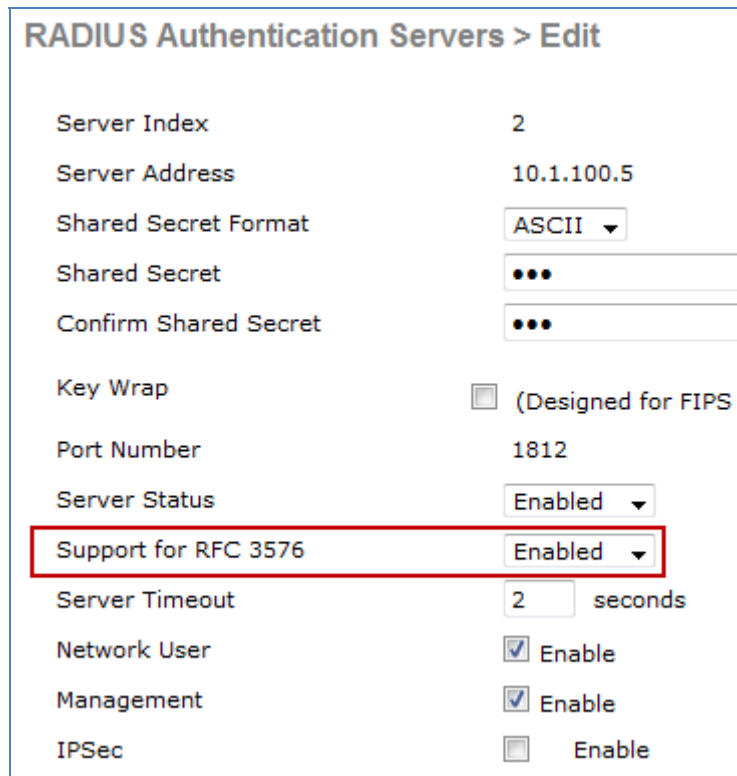
对客户端发起的流量，Catalyst 交换机可以支持 HTTP 和 HTTPS 流量的重定向。重定向至 ISE 的流量始终是 HTTPS。

将无线接入设备配置为将 HTTP 数据包重定向至 ISE PSN

配置接入设备，从而为 CWA、安全状态或请求方调配等具体服务提供 URL 重定向支持，不在本指南内容范围之内。总之，使用无线局域网控制器根据 RADIUS 授权支持重定向的重要步骤与以下内容相似：

步骤 1 在 Security → AAA → RADIUS → Authentication → (RADIUS Server) → Edit 下，确认 Support for RFC 3576 设置为 Enabled（图 36）。

图 34. 无线控制器的 CoA 配置示例

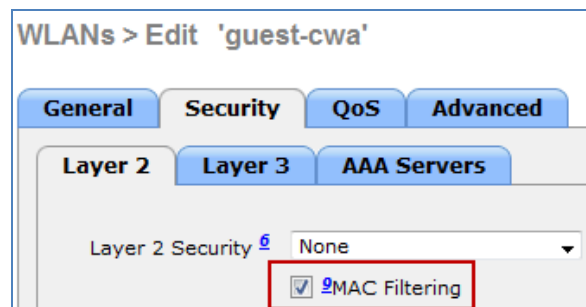


RADIUS Authentication Servers > Edit

Server Index	2
Server Address	10.1.100.5
Shared Secret Format	ASCII
Shared Secret	•••
Confirm Shared Secret	•••
Key Wrap	<input type="checkbox"/> (Designed for FIPS)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

步骤 2 在 WLANs → Edit (WLAN) → Security → Layer 2 下，为 MAC Filtering 配置 WLAN。Layer 2 和 Layer 3 Security 应设置为 None（图 37）。

图 35. 无线控制器的 MAC 过滤配置示例



WLANs > Edit 'guest-cwa'

General Security QoS Advanced

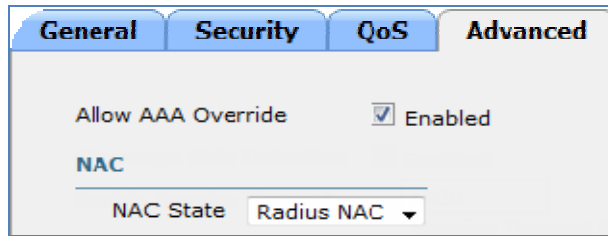
Layer 2 Layer 3 AAA Servers

Layer 2 Security [6](#) None

[9](#) MAC Filtering

步骤 3 在 Advanced 选项卡下，选择 Allow AAA Override 并将 NAC State 设置为 RADIUS NAC（图 38）。

图 36. 无线控制器的 RADIUS 授权配置示例



对于客户端发起的流量，思科无线局域网控制器仅支持重定向 HTTP 流量，不支持重定向 HTTPS 流量。重定向至 ISE 的流量始终是 HTTPS。

将 ISE 配置为执行 URL 重定向，作为 RADIUS 授权

配置 ISE，从而为 CWA、安全状态或请求方调配等具体服务提供 URL 重定向支持，不在本指南内容范围之内。总之，在 ISE 授权策略中根据 RADIUS 授权支持重定向的重要步骤与以下示例相似：

步骤 1 从 ISE 管理接口，转至 Policy → Policy Elements → Results。

步骤 2 从左侧窗格选择 Authorization → Authorization Profiles，然后从右侧窗格点击 Add，添加名称为 **Posture_Remediation** 的新授权配置文件，如图 39 所示。

图 37. 用于 URL 重定向的授权配置文件配置示例

Authorization Profiles > Posture_Remediation

Authorization Profile

* Name:

Description:

* Access Type:

▼ Common Tasks

DACL Name:

VLAN

Voice Domain Permission

Web Authentication: ACL:

Auto Smart Port

▼ Advanced Attributes Settings

Select an item = - +

▼ Attributes Details

```

Access Type = ACCESS_ACCEPT
DACL = POSTURE_REMEDIATION
cisco-av-pair = url-redirect-acl=ACL-POSTURE-REDIRECT
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cpp
    
```

在图 39 所示示例中，在 Common Task 下，选择的是 Web Authentication，其中具体重定向选择为 Posture Discovery。这将使终端重定向至客户端调配和安全状态服务或 CPP。重定向 ACL 是 POSTURE-REDIRECT，并且必须在接入设备上预先配置。所产生的 RADIUS 授权以蓝色突出显示。

步骤 1 转至 Policy → Authorization 并添加名称为 **Employee_PreCompliant** 的授权策略规则，此规则为使用工作站或 Apple iPad 类型设备的员工使用新的授权配置文件（请参阅图 40）。

图 38. 用于 URL 重定向的授权策略规则示例

<input checked="" type="checkbox"/>	Employee-Workstation	if	Workstation AND Employee	then	Employee AND SGT_Employee
<input checked="" type="checkbox"/>	Employee-iPad	if	Apple-iPad AND Employee	then	Employee_iPad AND SGT_Guest
<input checked="" type="checkbox"/>	Employee_PreCompliant	if	(Employee AND Session:PostureStatus NOT_EQUALS Compliant)	then	Posture_Remediation

在图 40 示例中，标记为 **Employee_PreCompliant** 的规则特意放在之前规则的**后面**，确保仅在员工连接网络并且设备类型与等于 **Workstation** 或 **Apple-iPad** 的明确终端身份组任一个都不匹配的情况下才匹配此规则。当经过身份验证的员工与 **Employee_PreCompliant** 规则匹配时，他们将分配到名称为 **Posture_Redirection** 的授权配置文件。这将向接入设备返回 RADIUS 授权，以执行向客户端调配和安全状态服务的 URL 重定向。

将网络设备配置为向 ISE PSN 发送多份 HTTP 流量

有多种方法可将流量镜像到 ISE 策略服务节点。本程序将介绍在 Cisco Catalyst 交换机上使用 VACL 捕获的一种常用方法。此方法有个额外的好处，就是能够仅将选中的相应流量转发至 ISE 策略服务节点。

最佳实践： 如果可用，请使用过滤器，利用支持可扩展流量镜像的智能分流器系统向 ISE 探测功能仅发送所需的流量。这包括依赖于 SPAN 方法来获取分析数据的 DHCP SPAN 和 HTTP 探测功能。更多高级分流器系统将为镜像流量提供高可用性支持。

或者，当基础设施支持时，请利用智能 SPAN 技术，例如本地交换机上的 VCL 捕获，或将 VACL 捕获/重定向与 RSPAN 相结合，允许选择性地捕获网络流量。

确定将作为 DHCP 流量来源的接口或 VLAN。WLC 的出口接口或与 DHCP 服务器的连接等某些阻塞点可以作为捕获所有客户端 DHCP 数据包的理想位置。

在下面的示例中，VLAN 40-44 被中继至思科无线局域网控制器 5500 系列。千兆以太网 2/37 是连接运行 VMware ESXi 4.1 的 Cisco UCS 服务器的一个交换端口连接。ESX 服务器承载配置为启用分析功能的策略服务节点的一个 ISE 虚拟设备。接口千兆以太网 2/37 连接至与作为千兆以太网 3 的 ISE PSN 链接的虚拟接口。

```
interface GigabitEthernet1/1
description WLC5508 ETH0 (Port 1)
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 40-44
switchport mode trunk

interface GigabitEthernet2/37
description UCS1 SPAN (port 3 of 4)
switchport
```

步骤 2 将 VACL 捕获配置为与 VLAN 40-44 的所有 HTTP 流量匹配并转发至 ISE PSN 连接。

步骤 3 将 ACL 配置为仅匹配 HTTP 流量并将另一个配置为匹配所有 IP 流量，如下所示：

```
cat6500(config)# ip access-list extended HTTP_TRAFFIC
cat6500(config-ext-nacl)# permit tcp any any eq www

cat6500(config)# ip access-list extended ALL_TRAFFIC
cat6500(config-ext-nacl)# permit ip any any
```

步骤 4 配置一个 VLAN 访问映射，其中一个序列设置匹配 HTTP_TRAFFIC ACL 的流量上的捕获位。在同一 VLAN 访问映射上配置转发所有其他流量（匹配 ALL_TRAFFIC ACL）的另一个序列。

```
cat6500(config)# vlan access-map HTTP_MAP 10
cat6500(config-access-map)# match ip address HTTP_TRAFFIC
cat6500(config-access-map)# action forward capture

cat6500(config)# vlan access-map HTTP_MAP 20
cat6500(config-access-map)# match ip address ALL_TRAFFIC
cat6500(config-access-map)# action forward
```

步骤 5 配置一个 VLAN 过滤器，将 VLAN 访问映射应用于 VLAN 40、41、42 和 43，如下所示：

```
cat6500(config)# vlan filter HTTP_MAP vlan-list 40-43
```

步骤 6 将捕获端口 (Gi2/37) 配置为包含 VLAN 40、41、42 和 43 上所有匹配的流量，包括路由至上游 VLAN 100 的流量，如下所示：

```
cat6500(config)# int Gi2/37
cat6500(config-if)# switchport capture allowed vlan 40-43,100
cat6500(config-if)# switchport capture
```

使用 URL 重定向验证 HTTP 探测功能数据（CWA 示例）

- 步骤 1** 从 Administration → Identity Management → Identities → Endpoints 删除终端。
- 步骤 2** 从配置为支持向 ISE PSN 进行 HTTP 重定向的接入设备断开终端，然后重新连接该终端。
- 步骤 3** 使用 Web 身份验证从该终端登录。
- 步骤 4** 转至 ISE Policy Administration 节点并导航至 Administration → Identity Management → Identities。
- 步骤 5** 从左侧窗格选择 Endpoints。
- 步骤 6** 查找并选择新连接的终端的 MAC 地址，显示 HTTP 探测功能捕获的属性。

图 41 中的示例显示的是仅使用 HTTP 探测功能，以突出显示使用 URL 重定向收集的属性。

图 39. 使用 URL 重定向的 HTTP 探测功能属性 - CWA 示例

* MAC Address	00:50:56:A0:0B:3A
* Policy Assignment	Windows7-Workstation
Static Assignment	<input type="checkbox"/>
* Identity Group Assignment	Microsoft-Workstation
Static Group Assignment	<input type="checkbox"/>
Attribute List	
EndPointPolicy	Windows7-Workstation
EndPointSource	HTTP Probe
IdentityGroup	Microsoft-Workstation
MACAddress	00:50:56:A0:0B:3A
MatchedPolicy	Windows7-Workstation
OUI	VMware, Inc.
PolicyVersion	20
StaticAssignment	false
StaticGroupAssignment	false
Total Certainty Factor	60
User-Agent	Mozilla/5.0 (Windows NT 6.1; rv:11.0) Gecko/20100101 Firefox/11.0

突出显示的关键属性包括：

- EndPointSource
- MACAddress
- OUI
- User-Agent

所示示例仅使用 HTTP 探测功能，以突出显示使用 URL 重定向收集的属性。此特定场景允许向内部终端数据库添加终端，即使是在没有 IP 到 MAC 地址绑定的情况下。

EndPointSource 显示 HTTP 探测功能是属性更新的最新来源。

MACAddress 是从会话缓存获取的值。

OUI 是根据 **MACAddress** 值推导的。

User-Agent 是揭示这个基于 VMware 的客户端运行的是 Windows 7 操作系统的关键数据点。

使用 URL 重定向验证 HTTP 探测功能数据（客户端调配示例）

- 步骤 1** 从 Administration → Identity Management → Identities → Endpoints 删除终端。
- 步骤 2** 从配置为支持向 ISE PSN 进行 HTTP 重定向的接入设备断开终端，然后重新连接该终端。
- 步骤 3** 尝试从终端登录。
- 步骤 4** 导航至 Administration → Identity Management → Identities 并从左侧窗格选择 Endpoints。
- 步骤 5** 查找并选择新连接的终端的 MAC 地址，显示客户端调配服务捕获的属性。

步骤 6 图 42 显示的示例中没有启用任何探测功能来突出显示在客户端调配中使用 URL 重定向收集的属性。

图 40. 使用 URL 重定向的 HTTP 探测功能属性 - 客户端调配示例

* MAC Address	7C:6D:62:E3:D5:05
* Policy Assignment	Apple-iPad
Static Assignment	<input type="checkbox"/>
* Identity Group Assignment	Apple-iPad
Static Group Assignment	<input type="checkbox"/>
Attribute List	
EndPointPolicy	Apple-iPad
EndPointProfilerServer	ise-psn-1
EndPointSource	CP
IdentityGroup	Apple-iPad
MACAddress	7C:6D:62:E3:D5:05
MatchedPolicy	Apple-iPad
OUI	Apple, Inc
PolicyVersion	20
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	26
Total Certainty Factor	30
User-Agent	Mozilla/5.0 (iPad; CPU OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9A405 Safari/7534.48.3

步骤 7 突出显示的关键属性类似于之前示例中的那些关键属性，例外的是 **EndPointSource**，其设置为 CP（客户端调配）。

使用 SPAN 验证 HTTP 探测功能数据

- 步骤 1** 从 Administration → Identity Management → Identities → Endpoints 删除终端。
- 步骤 2** 从所配置的接入设备断开终端，然后重新连接该终端。
- 步骤 3** 在终端上打开 Web 浏览器并尝试通过 http 访问任何网站。
- 步骤 4** 导航至 Administration → Identity Management → Identities 并从左侧窗格选择 Endpoints。
- 步骤 5** 查找并选择新连接的终端的 MAC 地址，显示 HTTP 探测功能捕获的属性。
- 步骤 6** 图 43 显示的是仅启用 HTTP 探测功能来突出显示使用 SPAN 收集的属性。

图 41. 使用 SPAN 的 HTTP 探测功能属性示例

Endpoint List > 7C:6D:62:E3:D5:05	
Endpoint	
* MAC Address	7C:6D:62:E3:D5:05
* Policy Assignment	Apple-iPad
Static Assignment	<input type="checkbox"/>
* Identity Group Assignment	Apple-iPad
Static Group Assignment	<input type="checkbox"/>
Attribute List	
Cookie	NID=59=eFjUh-KeyMYy3sJa6yME53u3I1LDRpolvqVVdInBu30HDIVTz PREF=ID=14254t19b36df751;U=9b71d718247b1acd;FF=0;TM=1333
EndPointPolicy	Apple iPad
EndPointProfilerServer	ise-psn-1
EndPointSource	HTTP Probe
Host	www.google.com
IdentityGroup	Apple-iPad
MACAddress	7C:6D:62:E3:D5:05
MatchedPolicy	Apple-iPad
OUI	Apple, Inc
PolicyVersion	22
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	21
Total Certainty Factor	30
User-Agent	Mozilla/5.0 (iPad; CPU OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9A105 Safari/7534.18.3
ip	10.1.41.101

关键属性包括之前示例中相同的键属性以及一些新的属性：

- **Cookie**（已截断显示）
- 主机

在初始 CWA 过程完成后，输出类似于使用 URL 重定向的输出。这些额外的属性表示捕获普通客户端浏览活动收集的其他 HTTP 报头信息。随着这些属性更改，ISE 会不断更新。显而易见，对可能未使用的属性的这种大量更新会导致对数据库更新和同步流程产生更大的影响。这再次强调了使用利用 URL 重定向的 HTTP 探测功能捕获 **User-Agent** 比 SPAN 方法高效得多。

总之，可以根据 **User-Agent** 属性所确定的终端操作系统给终端分类。可以由 HTTP 探测功能收集此属性，而且在特殊情况下可以由客户端调配服务收集此属性。收集 HTTP 流量的两个通用方法包括 URL 重定向和 SPAN 技术。一般来说，URL 重定向效率更高，但是在未启用 RADIUS 身份验证的环境中需要使用分析服务，则只能选择 SPAN。

使用 DNS 探测功能进行分析

DNS 探测功能用于在识别了现有终端的 IP 地址之后，根据来自 ISE 策略服务节点的反向 DNS 查找，获取 DNS 完全限定域名 (FQDN)。因此，除非已知 IP 地址，否则 DNS 探测功能无法运行。

以下探测功能可用于确定终端的 IP 地址：

- 通过 Framed-IP-Address 运行的 RADIUS 探测功能
- 通过 cdpCacheAddress 运行的 SNMP 探测功能
- 通过 SourceIP 运行的 HTTP 探测功能
- 通过 dhcp-requested-address 运行的 DHCP 探测功能

除了要求拥有已知 IP 地址，使用反向 DNS 查找还有很多其他要求：

- 在 DNS 中，每个终端都要求有一个地址或 **A** 记录（主机名）以及一个指针或 **PTR** 记录（IP 地址）。
- 假设终端使用 DHCP，则必须在 DHCP 服务器上配置动态 DNS (DDNS)。
- 根据 DHCP 服务器配置，终端可能需要配置为请求动态更新。
- ISE 策略服务节点必须配置为解析动态更新的 DNS 服务器提供的地址。
- 假设 DDNS 已配置并正常运行，则 DNS 探测功能可以检索 FQDN。否则，如果反向查找失败，就不会添加任何属性。

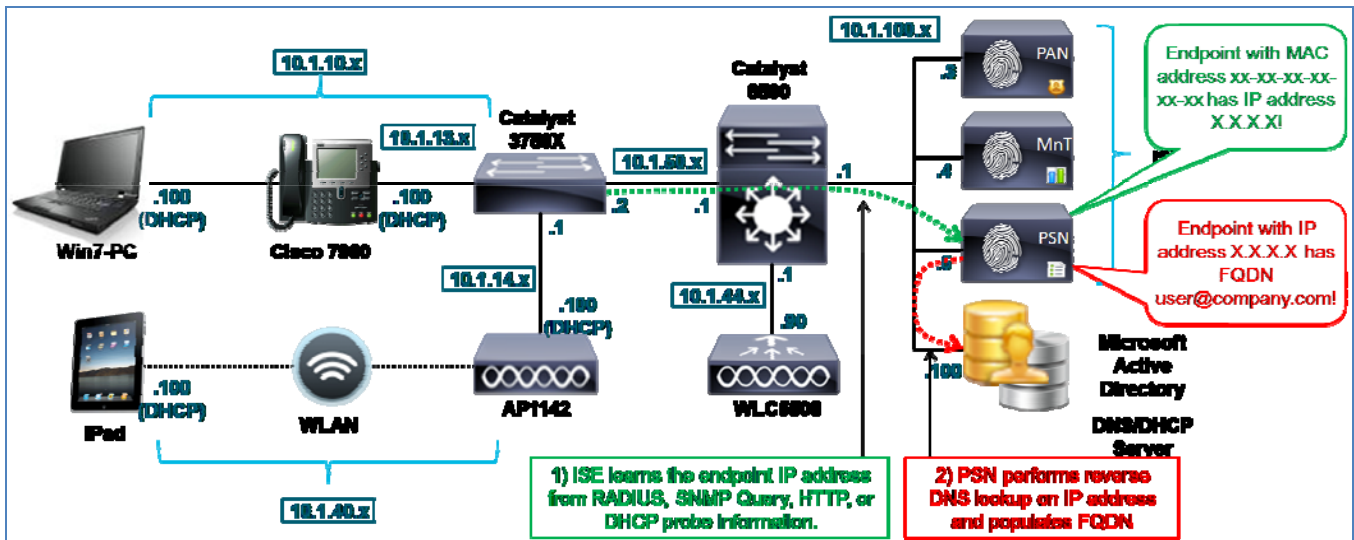
如果为特定终端部署了标准主机名、域名或 FQDN 命名约定，则可以使用这些属性对终端分类。例如，如果所有 Windows XP 客户端都分配了一个名称（例如 **jsmith-winxp**），则在某个条件下可以使用 **host-name** 属性或 **client-fqdn** 属性来给 Windows CP 终端分类。同样地，如果此约定为将公司终端的主机名填充为 **jsmith-corp-dept** 之类的内容，则可以将其用于验证公司资产。

必须注意，不要将配置文件属性混淆为身份，但是属性可以提高确定终端为某个类型的可信度。例如，授权策略可用于分析，拒绝向 PC 的 **host-name** 属性（如匹配的终端身份组所示）不包含预期值的员工授予完全访问权限。注：本指南将在后面章节论述配置文件和终端身份组之间的关系。

如此处论述所示，可能会可以使用其他探测功能收集 FQDN 或其组件。因此，如果已经可以通过其他方式获得相同的信息或部分 FQDN，则可能不必要使用 DNS 探测功能。但是，DDNS 可以配置得更安全，从而使得通过 DHCP 客户端数据包检索的信息没有向受信任的 DNS 服务器进行反向查找那么可靠。

图 44 显示的是使用 DNS 探测功能的示例拓扑。如图所示，ISE 策略服务节点使用多种方法中的一种方法识别终端的 IP 地址。然后 PSN 发起对 IP 地址的反向查找。如果收到响应，则 ISE 分析服务会使用 FQDN 属性更新终端记录。

图 42. DNS 探测功能示例



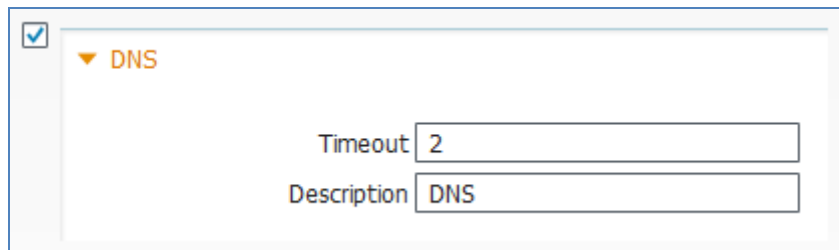
配置 DNS 探测功能

要使用 DNS 探测功能，ISE 策略服务节点引用的 DNS 必须手动地或使用 DDNS 动态地配置为包含要检索 FQDN 的每个终端的主机和反向指针记录。

在 ISE 中启用 DNS 探测功能

- 步骤 1** 转至 Administration → System → Deployment，并从右侧窗格已部署节点的列表中选择要执行分析的策略服务节点。
- 步骤 2** 选择 Profiling Configuration 选项卡。
- 步骤 3** 要为 DNS 探测功能添加支持，请选中标记为 DNS 的复选框。

图 43. 使用 SPAN 的 HTTP 探测功能属性示例



DNS 探测功能无接口选择，因为所有探测功能查询都由使用全局路由表对本地配置的 DNS 服务器进行反向查找的 ISE 策略服务节点发起。

- 步骤 4** 使 Timeout 保留默认值。此值指定 PSN 等待反向查找响应的秒数。
- 步骤 5** 点击 Save 以提交更改。
- 步骤 6** 对已配置分析服务的所有其他策略服务节点重复本程序中的步骤。

将探测功能配置为获取终端 IP 地址

注：将探测功能配置为获取终端 IP 地址，为了使 DNS 探测功能执行反向 DNS 查找，获取 FQDN，首先必须从 SNMP 查询、DHCP、DHCP SPAN、HTTP 或 RADIUS 探测功能获取终端的 IP 地址。有关这些探测功能的配置的详细信息，请参阅本指南的相应章节。

为反向地址查找配置使用 DNS 服务器的 ISE

在初始安装 ISE 设备时，一个必要的配置步骤是配置一个或多个域名服务器。

如有必要，在全局配置模式下使用 ISE CLI 命令 **ip name-server** 更新运行分析服务的 ISE 策略服务节点所使用的 DNS 服务器的列表，如图 46 所示。

图 44. ISE 策略服务节点 DNS 服务器配置示例

```
ise-pan-1/admin(config)# ip name-server ?
<A.B.C.D> Primary DNS server IP address
<A.B.C.D> DNS server 2 IP address
<A.B.C.D> DNS server 3 IP address
```

- 步骤 1** 要删除某个条目，请使用 **no name-server** 命令。
- 步骤 2** 要保存更改，请退出全局配置模式并输入命令 **copy running-config startup-config**。
- 步骤 3** 在运行分析服务的其余策略服务节点上，重复这些步骤。

验证 DNS 探测功能数据

- 步骤 1** 从 Administration → Identity Management → Identities → Endpoints 删除终端。
- 步骤 2** 从配置为支持向 ISE PSN 进行 HTTP 重定向的接入设备断开终端，然后重新连接该终端。
- 步骤 3** 转至 ISE Policy Administration 节点并导航至 Administration → Identity Management → Identities。
- 步骤 4** 从左侧窗格选择 Endpoints。
- 步骤 5** 查找并选择新连接的终端的 MAC 地址，显示 HTTP 探测功能捕获的属性。

图 47 中的示例显示仅启用 RADIUS、DHCP（IP 帮助程序）和 DNS 探测功能的情况。启用 RADIUS 和 DHCP 的目的是用作获取终端的 MAC 地址和 IP 地址的方法。选择这些探测功能还可以比较使用不同探测功能收集的相似数据。

哈希标记表示这些输出部分已被截断以进行显示。

图 45. DNS 探测功能属性示例

Endpoint List > 00:50:56:A0:0B:3A

Endpoint

* MAC Address **00:50:56:A0:0B:3A**

* Policy Assignment **Microsoft-Workstation**

Static Assignment

* Identity Group Assignment **Microsoft-Workstation**

Static Group Assignment

Attribute List

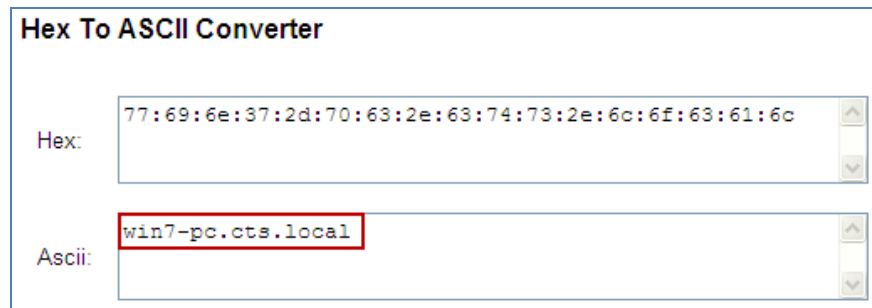
ADDomain	cts.local
AccsSessionID	ise-psn-1/121936089/19986
EndPointMACAddress	00-50-56-A0-0B-3A
EndPointMatchedProfile	VMWare-Device
EndPointPolicy	Microsoft-Workstation
EndPointProfilerServer	ise-psn-1
EndPointSource	DNS Probe
ExterralGroups	cts.local/users/employees\,cts.local/users/domain users\,cts.local/builtin/users
FQDN	win7-pc.cts.local.
Framed-IP-Address	10.1.10.100
GroupsOrAttributesProcessFailure	true
IdentityGroup	Microsoft-Workstation
chaddr	00:50:56:a0:0b:3a
ciaddr	0.0.0.0
cisco-zv-pair	audit-session-id=0A0132020000032046FD998, disc-cause-ext=No Reason, connect-pro
client-fqdn	00:00:00:77:69:6e:37:2d:7c:63:2e:63:74:73:2e:6c:6f:63:61:6c
dhcp-class-identifier	MSH-I 5.0
dhcp-client-identifier	01:00:50:56:a0:0b:3a
dhcp-message-type	DHCPREQUEST
dhcp-parameter-request-list	1, 15, 3, 6, 44, 46, 47, 31, 33, 121, 249, 43
dhcp-requested-address	10.1.10.100
flags	0x8000
giaddr	10.1.10.1
hlen	6
hops	1
host-name	win7-pc
htype	Ethernet (10Mb)
ip	10.1.10.100
op	BOOTREQUEST
secs	0
yiaddr	0.0.0.0

步骤 6 以红色突出显示的关键属性包括:

步骤 7 EndPointSource = DNS Probe

- 步骤 8** FQDN = win7-pc.cts.local
步骤 9 ip = 10.1.10.100
步骤 10 **EndPointSource** 反映终端属性的最后一个来源。
步骤 11 **FQDN** 值是使用 DNS 探测功能对 DNS 服务器成功进行反向查找的结果。
步骤 12 **ip** 属性很重要，可以强调获取此属性才能使 DSN 探测功能正常运行的要求。在本例中，RADIUS 或 DHCP 探测功能可能已更新此值。
步骤 13 以橙色突出显示的辅助属性包括：
步骤 14 ADDomain = cts.local
步骤 15 client-fqdn = 00:00:00:77:69:6e:37:2d:70:63:2e:63:74:73:2e:6c:6f:63:61:6c
步骤 16 host-name = win7-pc
步骤 17 **ADDomain** 值是使用 RADIUS 探测功能根据 RADIUS 属性识别的域名。
步骤 18 **client-fqdn** 属性是根据 DHCP 探测功能识别的终端完全限定域名，以十六进制格式表示（图 48）。

图 46. 十六进制至 ASCII 的转换示例



- 步骤 19** **host-name** 属性是根据 DHCP 探测功能识别的简单终端主机名。
步骤 20 本示例说明不同的探测功能属性可提供类似的信息。最后，策略管理员必须选择对于分析终端哪个属性最有用以及哪些探测功能最好地获取这些信息。本指南后面章节将介绍探测功能与分析方法的比较。

使用 NetFlow 探测功能进行分析

Cisco NetFlow 是从思科基于软件的 IOS 路由器和第 3 层交换机导出的一种遥感勘测。NetFlow 提供关于流过或直接流向各个启用 NetFlow 的路由器或交换机的流量的信息。启用 NetFlow 的设备收集网络流量数据并将这些数据导出至指定 UDP 端口（默认为 UDP/9996）上的收集器。流量是指给定源和目标之间的单向数据包传输流，由以下关键字段的组合唯一标识：

源 IP 地址

目标 IP 地址

源端口号

目标端口号

第 3 层协议类型

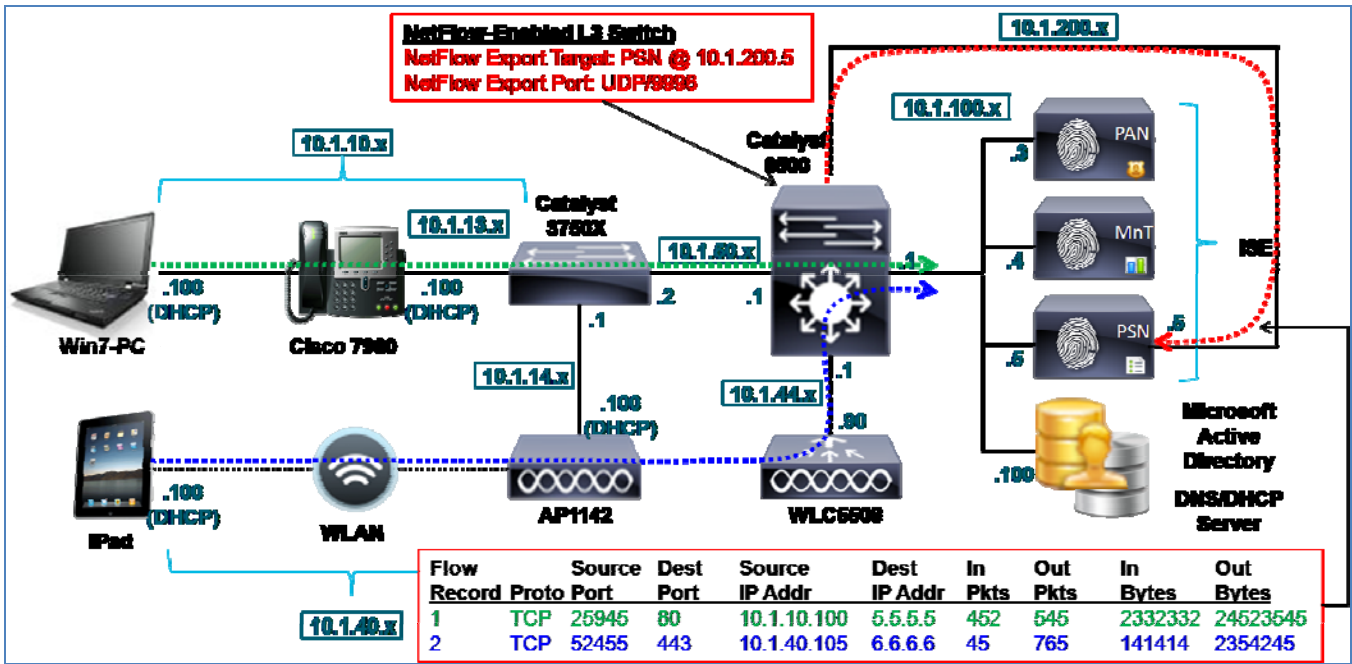
ToS 字节

输入逻辑接口 (ifIndex)

ISE NetFlow 探测功能可从启用 NetFlow 版本 5 和版本 9 的设备接收流量记录，从而可以为进行分析解析关键信息。

图 49 中的示例拓扑显示已通过兼容 NetFlow 的交换机（Cisco Catalyst 6500 系列）建立流量的两个不同终端。6500 系列配置为将流量导出至 UDP/9996 上 IP 地址为 10.1.200.5 的专用接口上的 ISE 策略服务节点。此接口与终止 RADIUS 和 Web 身份验证等用户会话服务的接口分开。

图 47. NetFlow 探测功能示例



您可以从拓扑中发现，在相应流量的路径中的路由器或交换机上必须启用 NetFlow。例如，如果必须收集远程分支中的片段之间的流量，则集线器或中心位置部署的 NetFlow 将不提供必要的可视性。此外，为了收集特定流量流，必须首先在网络上允许该流量通过。因此，如果网络接入取决于依赖 NetFlow 数据的某个配置文件，您需要确定如何充分限制访问，同时仍然允许完成分析所需的流量通过。

NetFlow 属性

表 4 显示 NetFlow 探测功能收集的某些属性。

表 4. NetFlow 探测功能属性

IN_BYTES	IN_PKTS	FLAWS
PROTOCOL	SRC_TOS	TCP_FLAGS
L4_SRC_PORT	IPV4_SRC_ADDR	SRC_MASK
L4_DST_PORT	IPV4_DST_ADDR	DST_MASK
IPV4_NEXT_HOP	LAST_SWITCHED	FIRST_SWITCHED
OUT_BYTES	OUT_PKTS	IPV6_SRC_ADDR
IPV6_DST_ADDR	IPV6_SRC_MASK	IPV6_DST_MASK
IPV6_FLOW_LABEL	ICMP_TYPE	DST_TOS
IN_SRC_MAC	OUT_DST_MAC	SRC_VLAN
DST_VLAN	IP_PROTOCOL_VERSION	DIRECTION

在 ISE 分析服务中，NetFlow 通常用于根据终端生成的流量识别终端。反过来，当特定终端生成不具有该终端特点的流量时，它可以提供关于异常行为的指示。例如，如果 NetFlow 属性反映一开始分析为 IP 电话的终端开始突然启动与端口 443 上的远程目标通信，则可能表示存在异常情况和潜在欺骗威胁。但是，请注意，将 NetFlow 用于 ISE 分析服务不可视为一种反欺骗功能或解决方案。

NetFlow 专注于对终端的积极分类，在将普通硬件用于任务特定功能的情况下最为有用，在此情况中给终端唯一分类的唯一信息与流量相关。这些类型的设备示例包括用于制造或医疗行业的设备。例如，医院使用的心脏监护器可能会使用利用标准硬件技术嵌入的 Windows 操作系统或加固型 Linux 内核，但是可以运行在特定协议、端口和目标上进行通信的协议。对于这些类型的终端，NetFlow 可能是唯一可行的选择。

步骤 1 一般来说，不建议随意启用 NetFlow 和/或将 NetFlow 用作通用分析方法。如果不谨慎部署，NetFlow 可能会对设备资源产生负面影响，具体取决于所使用的平台以及 NetFlow 配置和流量大小。如果从一个或多个来源持续发送大量流量，则 NetFlow 还可能会在 ISE 策略服务节点上生成高负载。不同于其他 ISE 探测功能，NetFlow 探测功能不支持优化数据收集和数据库效率的属性过滤器。

步骤 2 如果 NetFlow 版本 9 在网络设备上可用，为了将 NetFlow 导出至 ISE 策略服务节点，建议使用 NetFlow 版本 9，而不要使用版本 5。版本 9 支持 Flexible NetFlow 和各种增强功能，可过滤收集和导出至 NetFlow 探测功能的流量数据。虽然采样的 NetFlow 可以降低总流量，但是采样可能会无法满足所有分析要求，因为有些情景可能要求 NetFlow 探测功能查看所有流量。

NetFlow 探测功能和 IP 到 MAC 地址绑定要求

步骤 1 NetFlow 记录以源和目标 IP 地址之间的通信为基础。因为 NetFlow 流量不包括源或目标终端的 MAC 地址，因此 ISE 策略服务节点在其用于终端的 ARP 缓存表中必须已经有一个 IP 到 MAC 地址绑定，才能正确关联发送至 NetFlow 探测功能的数据。换句话说，如果 ISE 无法通过终端的 MAC 地址识别终端或没有关联的 IP 地址，则 NetFlow 探测功能识别的分析数据将被废弃，因为没有终端可让它应用所识别的流量属性。因此，必须在收集 NetFlow 数据之前通过另一个探测功能识别 IP 到 MAC 地址绑定。可用于提供此信息的探测功能如下：

步骤 2 RADIUS（通过 Framed-IP-Address）

步骤 3 DHCP（通过 dhcp-requested-address）

步骤 4 SNMP 查询（通过 SNMP 轮询）

步骤 5 值得注意的是，NetFlow 版本 9 支持将源和目标 MAC 地址包含在流量记录中，而版本 5 则不支持。但是，所报告的这些 MAC 地址是路径中相邻节点（通常为第 3 层路由器和交换机）的 MAC 地址，而不是距离超过一跳的终端的 MAC 地址。除非终端系统直接连接至 NetFlow 设备，否则此功能没有多大价值。

最佳实践：将 NetFlow 用于分析会导致可能向用于解析的 ISE 发送大量数据。仅限在其他探测功能不足以满足要求的情况下使用 NetFlow。如有必要，建议使用 NetFlow 版本 9，从而充分利用 Flexible NetFlow 中的过滤增强功能。虽然 ISE 不会阻止使用默认接口，但我们强烈建议将 NetFlow 导出至专用于 NetFlow 探测功能的 ISE PSN 接口。

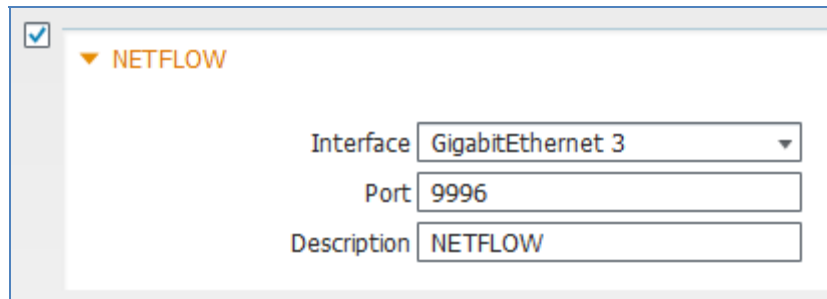
配置 NetFlow 探测功能

步骤 1 要使用 NetFlow 探测功能，则与相应流量流串联的网络设备必须兼容 NetFlow 并且支持 NetFlow 版本 5 或版本 9。将要作为 NetFlow 数据的目标的各个 ISE PSN 上应该使用专用接口。

在 ISE 中启用 NetFlow 探测功能

- 步骤 1** 转至 Administration → System → Deployment，并从右侧窗格已部署节点的列表中选择要执行分析的策略服务节点。
- 步骤 2** 选择 Profiling Configuration 选项卡，并且选中启用 NetFlow 探测功能的复选框（图 50）。
- 步骤 3** 选择用于收集 NetFlow 流量的接口，这应该是带可路由 IP 地址的一个专用接口（图 50）

图 48. NetFlow 探测功能配置



- 步骤 4** 选择 UDP 端口侦听导出的 NetFlow。此值应与 NetFlow 导出设备上配置的值相同。默认端口为 UDP/9996。
- 步骤 5** 点击 Save 以提交更改。
- 步骤 6** 对已配置分析服务的所有其他策略服务节点重复本程序中的步骤。

注：很多支持 NetFlow 功能的路由器和交换机都仅支持将单个目标用于 NetFlow 导出。因此，必须考虑高可用性问题。此外，我们还建议由同一个策略服务节点接收特定节点的所有配置文件数据。由于网络配置和其他限制，通常很难实现这一点。

向 ISE（网络资源）添加网络设备

接入设备也可能支持 NetFlow，但无明确要求将能够向 NetFlow 探测功能发送 NetFlow 流量的其他网络设备都配置为 ISE 中的网络设备。

将 ISE 策略服务节点接口配置为接收 NetFlow 流量

应该在专用接口上将 NetFlow 探测功能配置为接收 NetFlow 流量。要在 ISE 上配置专用 NetFlow 接口，请完成以下步骤：

- 步骤 1** 以物理方式将所需接口与网络交换端口连接。
- 步骤 2** 访问 ISE PSN 控制台 (CLI)。如图 51 所示，启用相应接口并分配有效的 IP 地址。

图 49. ISE 探测功能专用接口配置示例

```
ise-psn-1/admin# conf t
Enter configuration commands, one per line. End with CNTL/Z.
ise-psn-1/admin(config)# interface GigabitEthernet 3
ise-psn-1/admin(config-GigabitEthernet)# ip address 10.1.99.100 255.255.255.0

Changing the IP may result in undesired side effects on
any installed application(s).
Are you sure you want to proceed? Y/N [N]: Y
ISE M&T Log Processor is not running.
ISE M&T Log Collector is not running.
ISE M&T Alert Process is not running.
Stopping ISE Application Server...
ISE M&T Session Database is not running.
Stopping ISE Database processes...
Starting ISE Database processes...
ISE M&T Session Database is not running.
Starting ISE Application Server...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise-psn-1/admin(config-GigabitEthernet)# _
```

步骤 3 验证所有进程是否都按照说明运行。

步骤 4 验证新配置接口的配置并且验证是否已使用 **show running-config** 命令启用该接口，即其不是处于关闭状态（图 52）。

图 50. ISE 探测功能专用接口验证示例

```
ise-psn-1/admin# show running-config
Generating configuration...
?
hostname ise-psn-1
?
ip domain-name cts.local
?
interface GigabitEthernet 0
  ip address 10.1.100.5 255.255.255.0
  ipv6 address autoconfig
?
interface GigabitEthernet 1
  shutdown
  ipv6 address autoconfig
?
interface GigabitEthernet 2
  shutdown
  ipv6 address autoconfig
?
interface GigabitEthernet 3
  ip address 10.1.99.100 255.255.255.0
  ipv6 address autoconfig
?
ip name-server 10.1.100.100
--More--_
```

- 步骤 5** 通过从需要导出 NetFlow 数据的网络设备发送 ICMP ping，验证与新探测功能接口的连接。
- 步骤 6** 使用 CLI 命令 `copy running-config startup-config` 保存更改。
- 步骤 7** 以物理方式将所需的接口连接至相应的 SPAN 目标端口或网络分流量器接口。

注：对于在 VMware 设备上运行的策略服务节点

要为分析使用专用接口，则要求已为虚拟设备配置附加虚拟接口。如果未在安装时完成此操作，则在继续进行 ISE 配置之前，需要为所需的接口关闭 ISE 节点并更新 ESX 设备的硬件和网络配置

将支持 NetFlow 的交换机/路由器配置为将 NetFlow 导出至 ISE PSN

NetFlow 配置特定于支持 NetFlow 的设备。本程序包括 Catalyst 6500 系列交换机的一个配置示例。

- 步骤 1** 在全局配置模式下，启用 NetFlow，配置 NetFlow 版本 9 支持作为 NetFlow 数据的来源的接口 IP 地址，以及导出数据的策略服务节点。注意，ISE 默认端口指定为 UDP 9996。

```
mls netflow interface
mls flow ip interface-full
mls nde sender
mls nde interface
ip flow-cache timeout active 1
ip flow-export source Vlan100
ip flow-export version 9
ip flow-export destination 10.1.100.5 9996
```

注：在前面的示例中，Catalyst 6500 系列交换机有一个管理引擎 720，在此引擎中策略功能卡 (PFC) 执行基于硬件的 NetFlow，在软件中执行流向多层交换机功能卡 (MSFC) 的流量。必须使用 `mls nde sender` 命令将 PFC 配置为执行 NetFlow 数据导出 (NDE)。

- 步骤 2** 可选择配置捕获过滤器，如下所示：

```
ip flow-capture ttl
ip flow-capture vlan-id
ip flow-capture ip-id
ip flow-capture mac-addresses
```

- 步骤 3** 在入口接口（面向终端的接口）上启用 NetFlow，如下所示：

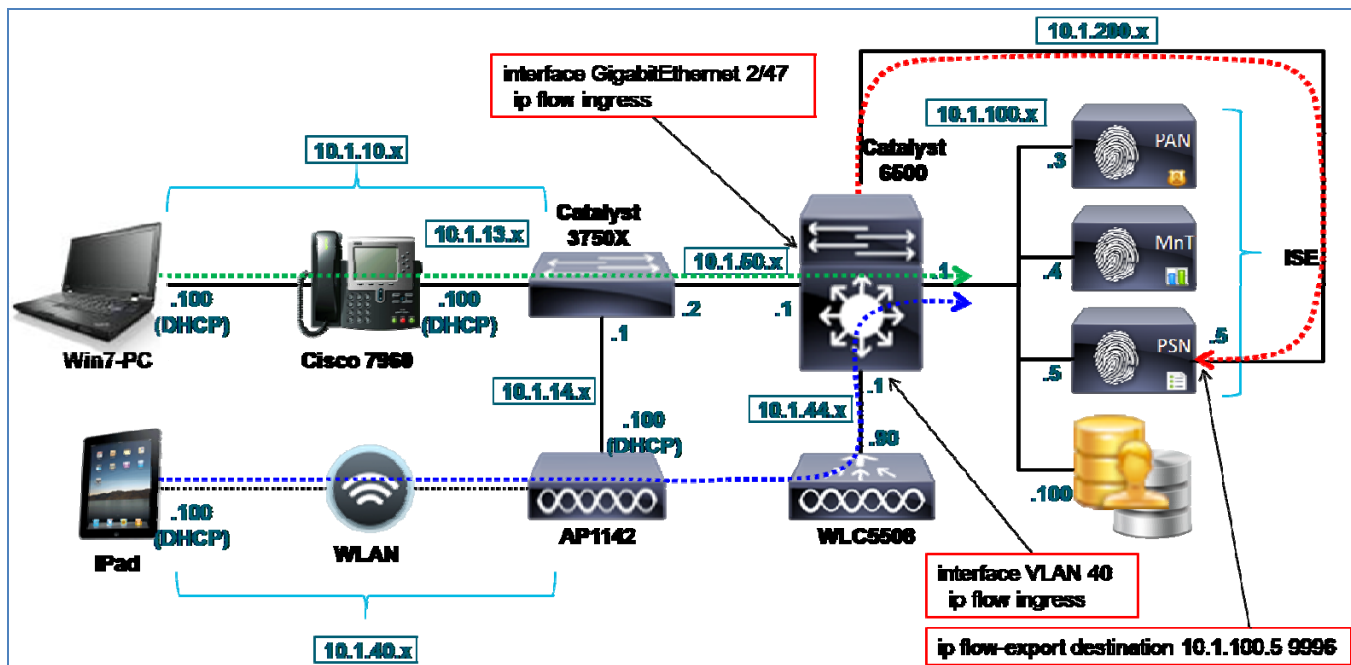
```
interface GigabitEthernet 2/47
description To cat3750x
ip address 10.1.50.1 255.255.255.0
ip flow ingress
!
interface Vlan40
description EMPLOYEE
ip address 10.1.40.1 255.255.255.0
ip helper-address 10.1.100.100
ip helper-address 10.1.100.5
ip flow ingress
!
interface Vlan41
description GUEST
ip address 10.1.41.1 255.255.255.0
```

```
ip helper-address 10.1.100.100
ip helper-address 10.1.100.5
ip flow ingress
```

此外，还显示 IP 帮助程序命令，以突出显示支持 DHCP 探测功能的配置，此探测功能用于获取 IP 到 MAC 地址绑定信息。这会允许 NetFlow 探测根据匹配的 IP 属性应用各种属性。

图 53 说明了应用 NetFlow 的接口以及 NetFlow 数据导出 (NDE) 的目标。其目的是从通过 Cisco Catalyst 3750-X 系列交换机连接的有线终端以及通过 Cisco 5500 系列无线局域网控制器连接的无线终端捕获流量。

图 51. NetFlow 导出示例



验证 NetFlow 探测功能数据

- 步骤 1 从 Administration → Identity Management → Identities → Endpoints 删除终端。
- 步骤 2 从接入设备断开终端，然后重新连接该终端。
- 步骤 3 从该终端登录并尝试生成样本流量，例如尝试使用浏览器进行 Web 访问。
- 步骤 4 转至 ISE Policy Administration 节点并导航至 Administration → Identity Management → Identities。
- 步骤 5 从左侧窗格选择 Endpoints。
- 步骤 6 查找并选择新连接的终端的 MAC 地址，显示 NetFlow 探测功能捕获的属性（图 54）。
- 步骤 7 图 54 中的示例突出显示使用 NetFlow 导出功能收集的属性。此外，还已启用 RADIUS 和 DHCP 探测功能以确保获取 IP 到 MAC 绑定来支持 NetFlow 探测功能。

图 52. NetFlow 属性示例

Endpoint List > 00:50:56:A0:0B:3A

Endpoint

- * MAC Address **00:50:56:A0:0B:3A**
- * Policy Assignment
- Static Assignment
- * Identity Group Assignment
- Static Group Assignment

Attribute List

EndPointProfilerServer	ise-psr-1
EndPointSource	NETFLOW Probe
ExternalGroups	cts.local/users/contractors\,cts.local/users/domain users\,cts.local/builtin/users
FIRST_SWITCH_ID	137839523
FLOW_SAMPLER_ID	0
FQDN	win7-pc.cts.local
FragmentOffset	0
Framed-IP-Address	10.1.10.100
GroupsOrAttributesProcessFailure	true
INPUT_SNMP	49
IN_BYTES	1869
IN_PKTS	6
IPV4_DST_ADDR	173.37.144.208
IPV4_NEXT_HOP	172.16.1.1
IPV4_SRC_ADDR	10.1.10.100
IdentityGroup	Microsoft-Workstation
IdentityPolicyMatchedRule	Default
L4_DST_PORT	80
L4_SRC_PORT	53149
LAST_SWITCHED	137839715
Location	Location#All Locations#North_America#RTP
MACAddress	00:50:56:A0:0B:3A
MatchedPolicy	Windows7-Workstation
MessageCode	3002
NAS-IP-Address	10.1.50.2
NAS-Port	50101
NAS-Port-Id	GigabitEthernet1/0/1
NAS-Port-Type	Ethernet
NetworkDeviceGroups	Device Type#All Device Types#Wired, Location#All Locations#North_America#RTP
NetworkDeviceName	cat3750x
OUI	VMware, Inc.
OUTPUT_SNMP	52
PROTOCOL	6

以红色突出显示的关键属性包括：

- EndPointSource = NetFlow Probe
- IPV4_DST_ADDR = 173.37.144.208 (cisco.com)
- IPV4_SRC_ADDR = 10.1.10.100 (win7-pc)
- L4_DST_PORT = 80 (HTTP)
- L4_SRC_PORT = 53149
- PROTOCOL = 6 (TCP)

如果使用流量捕获语句，您可以看到以下附加属性：

- DST_VLAN/SRC_VLAN
- IN_SRC_MAC/OUT_DST_MAC
- MAX_TTL/MIN_TTL

要验证是否在收集 NetFlow 数据，您可以使用 **show ip cache flow** 和 **show mls netflow ip** 命令。以下示例使用的是 **show ip cache flow** 命令：

```

cat6503#show ip cache flow
-----
Displaying software-switched flow entries on the MSFC in Module 1:

IP packet size distribution (348128 total packets):
 1-32  64   96  128  160  192  224  256  288  320  352  384  416  448  480
 .548 .342 .077 .005 .000 .000 .000 .000 .000 .000 .015 .000 .000 .000 .000

   512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
 .000 .000 .007 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
 2 active, 4094 inactive, 15760 added
251284 age polls, 0 flow alloc failures
Active flows timeout in 1 minutes
Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 33992 bytes
 6 active, 1018 inactive, 47280 added, 15760 added to flow
 0 alloc failures, 2775 force free
 1 chunk, 24 chunks added
last clearing of statistics never
Protocol      Total      Flows      Packets Bytes  Packets Active(Sec) Idle(Sec)
-----
              Flows      /Sec      /Flow  /Pkt  /Sec    /Flow    /Flow
TCP-Telnet    44         0.0        91     42    0.0     14.4     7.8
TCP-WWW       1361       0.0        22     45    0.0     0.0      14.2
TCP-other     1602       0.0        25     51    0.0     0.1      13.6
UDP-DNS       128        0.0        1      70    0.0     0.0      15.4
UDP-NTP       1375       0.0        1      76    0.0     0.0      15.5
UDP-other     2880       0.0        3     338   0.0     3.8      15.4
ICMP          6985       0.0        34     30    0.0     0.4      13.4
IP-other      1383       0.0        13     65    0.0     58.3     2.0
Total:        15758      0.0        22     46    0.0     6.0      13.0

SrcIf      SrcIPAddress  DstIf      DstIPAddress  Pr SrcP DstP  Pkts
-----
Gi2/47     10.1.50.2     Null       224.0.0.10    58 0000 0000   4
Gi2/47     10.1.13.1     Null       10.1.100.7    11 0043 0043   3
-----

```

```

Displaying hardware-switched flow entries in the PFC (Active) Module 1:
SrcIf          SrcIPAddress  DstIf          DstIPAddress  Pr SrcP DstP  Pkts
-----
Gi2/47         10.1.50.1     Gi2/47         10.1.50.2     58 0000 0000   0
Gi2/47         10.1.50.2     ---           10.1.100.1    11 007B 007B   0
Gi2/47         10.1.50.2     ---           10.1.50.1     58 0000 0000   0
Gi2/47         10.1.100.1    Gi2/47         10.1.50.2     11 007B 007B   0
Gi2/47         10.1.50.2     V1100         10.1.100.5    11 CC9B 00A2   15
Gi2/47         10.1.13.1     V1100         10.1.100.100  11 0043 0043  124
Gi2/47         10.1.13.1     V1100         10.1.100.5    11 0043 0043  124
Gi2/47         10.1.13.1     V1100         10.1.100.6    11 0043 0043  124
Gi2/47         10.1.50.2     ---           224.0.0.10    58 0000 0000   84
V140           10.1.40.1     ---           224.0.0.10    58 0000 0000   0
Gi2/47         10.1.50.2     V1100         10.1.100.4    11 C8D5 5022   30
Gi2/47         10.1.13.1     ---           10.1.100.7    11 0043 0043   0
Gi2/47         10.1.10.100   V1100         10.1.100.100  11 CA72 0035   1
Gi2/47         10.1.50.2     V1100         10.1.100.5    11 066E 0715  128
V141           10.1.41.1     ---           224.0.0.10    58 0000 0000   0
Gi2/47         10.1.50.2     V1100         10.1.100.5    11 06A4 7195   2
Gi2/47         10.1.50.2     V1100         10.1.100.6    11 E6D7 00A2   15
Gi2/47         10.1.50.2     ---           10.1.100.7    11 C748 00A2   0
Gi2/47         10.1.50.2     V1100         10.1.100.5    11 066D 0714   6
Gi2/47         10.1.10.100   V1100         10.1.100.100  11 E5CC 0035   1
Gi2/47         10.1.10.100   V1100         10.1.100.100  11 DA8B 0035   1
Gi2/47         10.1.10.100   V1100         10.1.100.100  11 C114 0035   1
Gi2/47         10.1.10.100   V1100         10.1.100.100  11 FC03 0035   1
Gi2/47         10.1.10.100   V1100         10.1.100.100  11 D295 0035   1
Gi2/47         10.1.10.100   V1100         10.1.100.100  11 ED48 0035   1
Gi2/47         10.1.10.100   V1100         10.1.100.100  11 E7E8 0035   1
Gi2/47         10.1.10.100   V1100         10.1.100.100  11 D770 0035   1
Gi2/47         10.1.10.100   V1100         10.1.100.100  11 D5AB 0035   1
--            0.0.0.0       ---           0.0.0.0       00 0000 0000  31K

```

步骤 8 以下示例使用的是 `show mls netflow ip`:

```

at6503#show mls netflow ip
Displaying Netflow entries in Active Supervisor EARL in module 1
DstIP          SrcIP          Prot:SrcPort:DstPort  Src i/f          :AdjPtrPkts      Bytes
Age   LastSeen  Attributes
-----
10.1.50.2      10.1.100.1    udp :ntp      :ntp      Gi2/47          :0x00            0
43    20:26:48  L2 - Dynamic
10.1.44.90     10.1.14.100   udp :16792    :5246     Gi2/47          :0x03            359
35    20:27:26  L3 - Dynamic
10.1.100.100   10.1.13.1     udp :67       :67       Gi2/47          :0x04            1846
32    20:27:30  L3 - Dynamic
10.1.100.5     10.1.50.2     udp :52379    :162      Gi2/47          :0x015           2734
335   20:23:02  L3 - Dynamic
10.1.100.4     10.1.50.2     udp :51413    :20514    Gi2/47          :0x030           5286
334   20:23:58  L3 - Dynamic
10.1.100.5     10.1.50.2     udp :1646     :1813     Gi2/47          :0x04            2680
32    20:27:30  L3 - Dynamic
10.1.100.100   10.1.10.100   udp :51826    :dns      Gi2/47          :0x01            61
211   20:24:00  L3 - Dynamic
10.1.44.90     10.1.14.100   udp :16792    :5247     Gi2/47          :0x06            901
30    20:27:30  L3 - Dynamic
224.0.0.10     10.1.41.1     88  :0         :0        V141            :0x00            0
426   20:27:27  Multicast
10.1.100.5     10.1.50.2     udp :1700     :29077    Gi2/47          :0x02            132
335   20:23:56  L3 - Dynamic
10.1.100.6     10.1.50.2     udp :59095    :162      Gi2/47          :0x015           2734
335   20:23:02  L3 - Dynamic

```


10.1.100.7	10.1.50.2	udp	:51016	:162	Gi2/47	:0x00	0
335	20:23:02	L3 - Dynamic					
10.1.100.5	10.1.50.2	udp	:1645	:1812	Gi2/47	:0x06	1365
270	20:23:56	L3 - Dynamic					
10.1.100.100	10.1.10.100	udp	:54699	:dns	Gi2/47	:0x01	64
211	20:24:00	L3 - Dynamic					
10.1.100.1	10.1.50.2	udp	:ntp	:ntp	Gi2/47	:0x00	0
43	20:26:48	L3 - Dynamic					
17.172.232.209	10.1.40.101	tcp	:61858	:443	Vl40	:0x02	173
17	20:27:14	L3 - Dynamic					
17.172.232.209	10.1.40.101	tcp	:61858	:443	Vl40	:0x00	0
17	20:27:14	L2 - Dynamic					
10.1.40.101	17.172.232.209	tcp	:443	:61858	Vl40	:0x00	0
17	20:27:14	L2 - Dynamic					
0.0.0.0	0.0.0.0	0	:0	:0	--	:0x032283	20941051
1573	20:27:31	L3 - Dynamic					

步骤 9 要验证 NetFlow 导出配置以及是否正在向 ISE 策略服务节点发送流量，请使用 **show ip flow export** 命令，如下所示：

```
cat6503# sh ip flow export
Flow export v9 is enabled for main cache
Export source and destination details :
VRF ID : Default
Source(1)      10.1.100.1 (Vlan100)
Destination(1) 10.1.99.5 (9996)
Version 9 flow records
20408 flows exported in 7635 udp datagrams
0 flows failed due to lack of export packet
0 export packets were sent up to process level
0 export packets were dropped due to no fib
0 export packets were dropped due to adjacency issues
0 export packets were dropped due to fragmentation failures
0 export packets were dropped due to encapsulation fixup failures
0 export packets were dropped enqueueing for the RP
0 export packets were dropped due to IPC rate limiting
0 export packets were dropped due to Card not being able to export
```

使用网络扫描 (NMAP) 探测功能进行分析

网络扫描探测功能以嵌入式开源网络映射器实用工具为基础。网络映射器 (NMAP) 用于扫描所连接终端的大型网络，然后对各个主机执行扫描，检测其操作系统、操作系统版本和服务（应用名称和版本）。

其他 ISE 探测功能被视为“被动”探测功能，因为它们不是直接查询终端本身，而是依赖于数据收集的间接方法，例如解析设备生成的数据或来自其他网络设备的数据。网络扫描探测功能被视为“主动”评估机制，因为它直接与终端通信，从源头获取信息。

NMAP 探测功能扫描操作

当 NMAP 探测功能进行扫描时，它可以执行以下一项或多项操作：

- 操作系统扫描
- SNMP 端口扫描
- 通用端口扫描

操作系统扫描用于检测终端的操作系统和版本。这是一项密集型操作。

SNMP 端口扫描会尝试检测 UDP 端口 161（SNMP 后台守护程序）和 162（SNMP 陷阱）是否已打开。如果已打开，则会使用社区字符串 **public** 向终端发起 SNMP 查询，从系统 MIB 和其他来源收集关于终端的其他信息。事实证明，在使用默认社区字符串 **public** 默认启用 SNMP 的网络打印机之类的终端中，此探测功能就特别有用。

注：NMAP 探测功能只能使用默认社区字符串 **public** 直接查询终端。此值当前不可配置。此探测功能不可与 SNMP 查询探测功能混淆，SNMP 查询探测功能查询网络设备而不查询终端并且在网络设备设置下拥有可配置的 SNMP 设置。

通用端口扫描对 15 个通用 TCP 和 UDP 端口执行扫描，如表 5 所示：

表 5. NMAP 探测功能通用端口扫描：TCP 和 UDP 端口

TCP 端口		UDP 端口	
端口	服务	端口	服务
21/tcp	ftp	53/udp	域
22/tcp	ssh	67/udp	dhcpc
23/tcp	telnet	68/udp	dhcpc
25/tcp	smtp	123/udp	ntp
53/tcp	域	135/udp	msrpc
80/tcp	http	137/udp	netbios-ns
110/tcp	pop3	138/udp	netbios-dgm
135/tcp	msrpc	139/udp	netbios-ssn
139/tcp	netbios-ssn	161/udp	snmp
143/tcp	imap	445/udp	microsoft-ds
443/tcp	https	500/udp	isakmp
445/tcp	microsoft-ds	520/udp	route
3306/tcp	mysql	631/udp	ipp
3389/tcp	ms-term-serv	1434/udp	ms-sql-m
8080/tcp	http-proxy	1900/udp	upnp

注：所扫描的通用端口的列表当前不可配置。

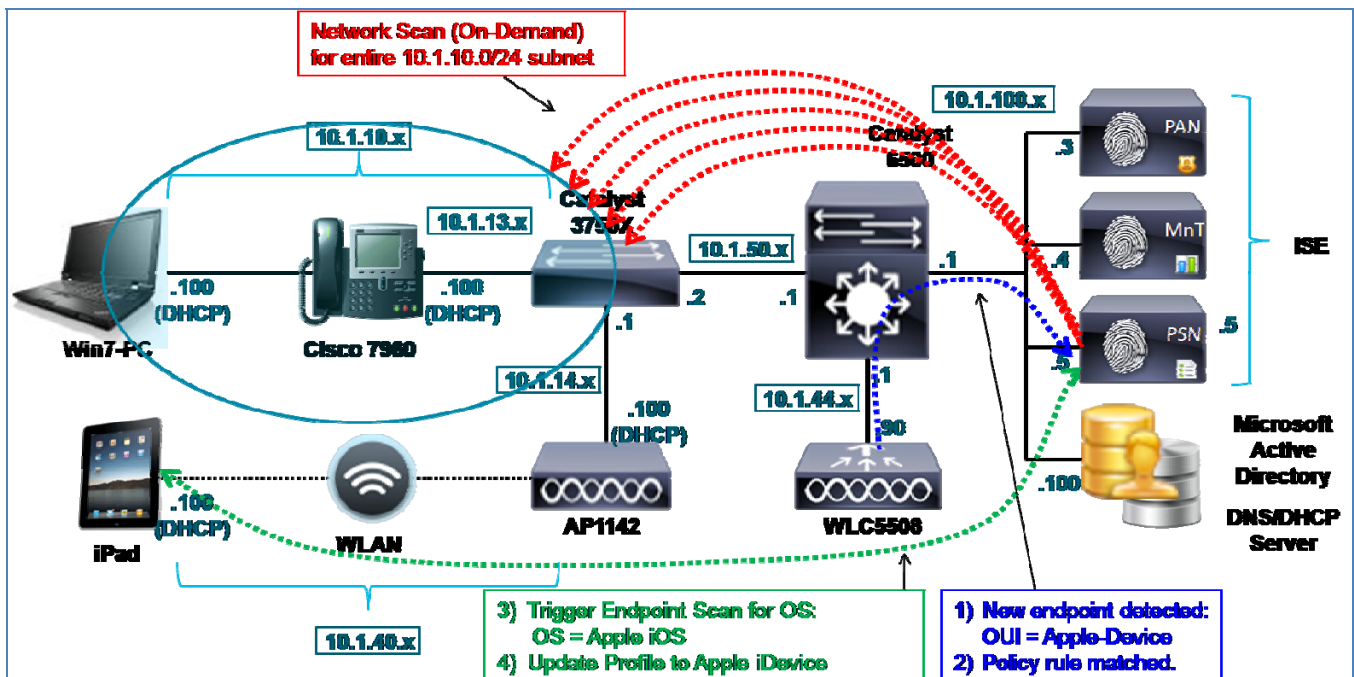
管理员可以选择根据终端运行的服务对终端进行分配和提供安全保护。例如，运行 Web 服务的 Windows 服务器可能会要求应用特定授权策略（dACL、VLAN、SGT），确保其免受非 HTTP 请求干扰。相反，运行 Web 服务器的 Windows 或 Linux 工作站可能需要使用类似的授权方法拒绝访问或进行隔离。

使用以下两种方法之一可启动 NMAP 探测功能：

- 网络扫描
- 终端扫描

图 55 中的示例拓扑描述的是在整个 10.1.10/24 子网上发起的网络扫描（以红色突出显示）。

图 53. NMAP 探测功能示例



NMAP 探测功能网络扫描

网络扫描是对一个或多个网络终端进行的按需扫描。它由管理员用户从 ISE 管理节点手动启动。此探测功能甚至无需在策略服务节点上启用，即可运行手动网络扫描。管理员用户只需指定要扫描的 IP 子网并点击 **Run Scan** 按钮。

网络扫描同时执行 SNMP 端口和操作系统扫描。因为大型网络扫描比较耗时并且会给策略服务节点增添负载，所以建议认真选择子网的范围。启动扫描后，管理员用户可以点击链接，导航至显示结果的页面。

NMAP 探测功能终端扫描

终端扫描是对单个终端触发的扫描。根据分析策略中匹配的规则自动启动此扫描。要运行所触发的扫描，终端必须与分析策略和分配网络操作的具体条件相匹配。网络扫描操作可根据配置文件规则进行配置，其定义要执行的具体扫描操作。

默认情况下，可以分配三种 NMAP 操作，作为对匹配的配置文件条件的响应：

- **CommonPortsAndOS-scan**（通用端口 + 操作系统扫描）
- **OS-scan**（仅操作系统）
- **SNMPPortsAndOS-scan**（SNMP 端口 + 操作系统扫描）

图 55 中的示例拓扑描述了此过程。最近的探测功能活动检测出了一个新终端（显示为蓝色）。根据所收集的配置文件数据，基于来自其 MAC 地址的 OUI 已得出该终端为一台 Apple 设备，但是不知道此终端是 Mac OS X 工作站、Apple iDevice 还是其他 Apple 终端。其与对 Apple 设备进行针对性操作系统扫描的策略规则匹配（显示为绿色）。结果发现终端运行的是 Apple iOS，并且其配置文件已更新为移动 Apple 设备的配置文件。

与未知配置文件匹配的终端会使用 SNMP 端口和操作系统扫描自动进行扫描。此响应不可配置。其旨在使 ISE 分析快速获得关于已发现但却未分析的任何终端的更多信息。

注：有些终端已启用个人防火墙或其他代理软件，这会阻止尝试扫描终端。这些终端只能生成少量或根本不生成任何 NMAP 数据。此外，限制网络访问的任意终端都可能无法接收或响应 NMAP 操作。

NMAP 探测功能和 IP 到 MAC 地址绑定要求

NMAP 以已知 IP 地址为基础。如果 NMAP 探测功能收集了终端的属性，但却无法将其与具体 MAC 地址关联，则会丢弃那些数据。如果策略服务节点位于其所扫描的终端相同的片段上，则可以根据其本地 ARP 缓存识别 IP 到 MAC 地址绑定并将该终端直接添加至内部终端数据库。因此，必须在收集 NMAP 数据之前通过另一个探测功能识别 IP 到 MAC 地址绑定。可用于提供此信息的探测功能如下：

- RADIUS（通过 Framed-IP-Address）
- DHCP（通过 dhcp-requested-address）
- SNMP 查询（通过 SNMP 轮询）

思科最佳实践：在 ISE 部署的发现阶段中当 ISE 尚未对终端进行身份验证时，可以对大型网络块进行网络扫描，从而扫描和检测终端以及任何相关操作系统和终端信息。此外，建议在此阶段，对存储终端 ARP 表信息的所有网络设备都启用 SNMP 查询探测功能。这将允许发现终端 MAC 和 IP 地址，包括静态寻址的终端。这反过来可以支持 NMAP 探测功能收集，因为 PSN 此时应该获取了在网络扫描期间发现的各个 IP 地址的 MAC 地址。

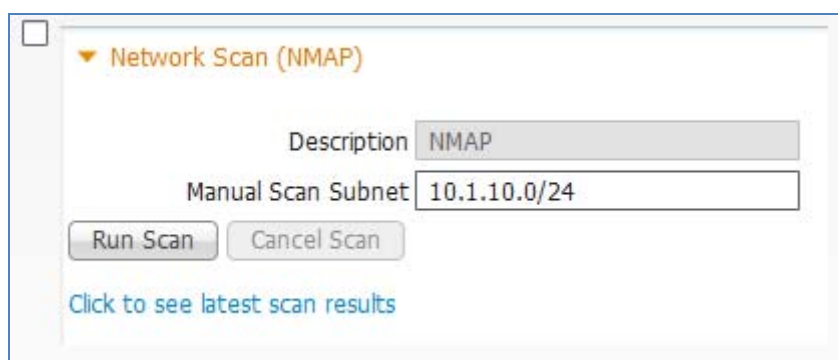
配置 NMAP 探测功能

如上所述，有两种运行 NMAP 探测功能的方法，一种是作为手动按需网络扫描，另一种是作为单个终端的自动触发扫描事件。下文将分别介绍使用这两种方法的程序。

运行网络扫描

- 步骤 1** 转至 Administration → System → Deployment 并从右侧窗格已部署节点的列表中选择要执行网络扫描的策略服务节点。
- 步骤 2** 选择 Profiling Configuration 选项卡。
- 步骤 3** 要运行网络扫描，请选择 Network Scan (NMAP) 选项，展开其内容（图 56）。


图 54. NMAP 探测功能



注：如图 56 所示，不一定要启用探测功能才能执行手动网络扫描。

- 步骤 4** 输入 IP 子网地址和掩码，从而以示例所示形式进行扫描。示例显示输入的是 C 类子网 (10.1.10.0) 以及 C 类子网的掩码位 (24) 的相应位数。
- 步骤 5** 可选择其他子网大小，但是必须考虑选择之后涵盖的网络范围和终端数量，减少执行扫描的总时间和负载。
- 步骤 6** 点击 Run Scan。
- 步骤 7** 要取消活动扫描，请点击 Cancel Scan。否则，请选择“Click to see latest scan results”，直接导航至 Administration → Identity Management → Identities 页面。即使您导航离开此页面，系统仍将继续扫描直到完成。
- 步骤 8** 在 Identities 页面，从左侧窗格选择 **Latest Network Scan Results**。根据扫描的进度，会在右侧窗格显示拥有确定扫描结果的终端（图 57）。

图 55. NMAP 网络扫描结果示例

Latest Network Scan Results Endpoints				
 Edit				
<input type="checkbox"/>	Endpoint Profile	MAC Address	Profiler Server	Static Assignment
<input type="checkbox"/>	Cisco-Device	1C:DF:0F:8F:60:42	ise-psn-1	false
<input type="checkbox"/>	VMWare-Device	00:50:56:A0:0B:3A	ise-psn-1	false

步骤 9 按照 MAC 地址点击终端条目可查看相应结果。

图 56. 网络扫描提供的 NMAP 探测功能属性示例

Endpoint List > 00:50:56:A0:0B:3A

Endpoint

* MAC Address **00:50:56:A0:0B:3A**

* Policy Assignment

Static Assignment

* Identity Group Assignment

Static Group Assignment

Attribute List

EndPointMACAddress	00-50-56-A0-0B-3A
EndPointMatchedProfile	VMWare-Device
EndPointPolicy	VMWare-Device
EndPointProfilerServer	ise-psn-1
EndPointSource	NMAP Probe
NmapSubnetScanID	4
OUI	VMware, Inc.
ip	10.1.10.100
operating-system	Microsoft Windows general purpose 2008

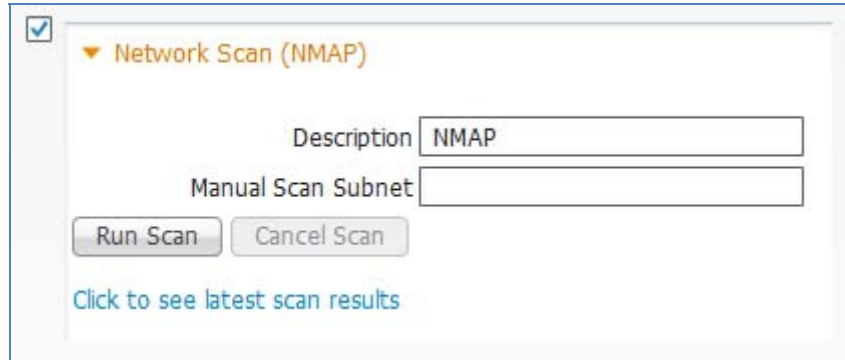
所选终端是 Windows 7 PC。您可以从手动网络扫描的输出中看到，NMAP 检测出通用操作系统类别（Windows 7 和 Windows 2008 共享通用代码库），但是不足以提供充分的信息来进一步对超出当前基于与 OUI 条件的匹配的 VMware 配置文件范围的终端进行分类。EndPointSource 显示为 NMAP Probe。ScanID 指分配给手动网络扫描事件的 ID。

注：需要禁用默认 Windows 7 防火墙设置，才能实现从 NMAP 探测功能成功进行扫描。

为终端扫描配置 NMAP 探测功能

- 步骤 1** 转至 Administration → System → Deployment，并从右侧窗格已部署节点的列表中选择要执行分析的策略服务节点。
- 步骤 2** 选择 Profiling Configuration 选项卡，并且选中标记为 Network Scan (NMAP) 的复选框（图 59）。

图 57. NMAP 探测功能配置



步骤 3 点击 Save 以提交更改。

步骤 4 对已配置分析服务的所有其他策略服务节点重复本程序中的步骤。

检查网络扫描 (NMAP) 操作

步骤 1 转至 Policy → Policy Elements → Results 并从左侧窗格选择 Profiling → Network Scan (NMAP) Actions。

步骤 2 查看默认 NMAP 操作（图 60）。

图 58. NMAP 扫描操作

The screenshot shows a table titled 'Network Scan Actions'. At the top of the table, there are three buttons: 'Edit' (with a pencil icon), '+ Add', and 'X Delete'. The table has two columns: 'Network Scan (NMAP) Action Name' and 'Description'. There are four rows of data, each with a checkbox in the first column.

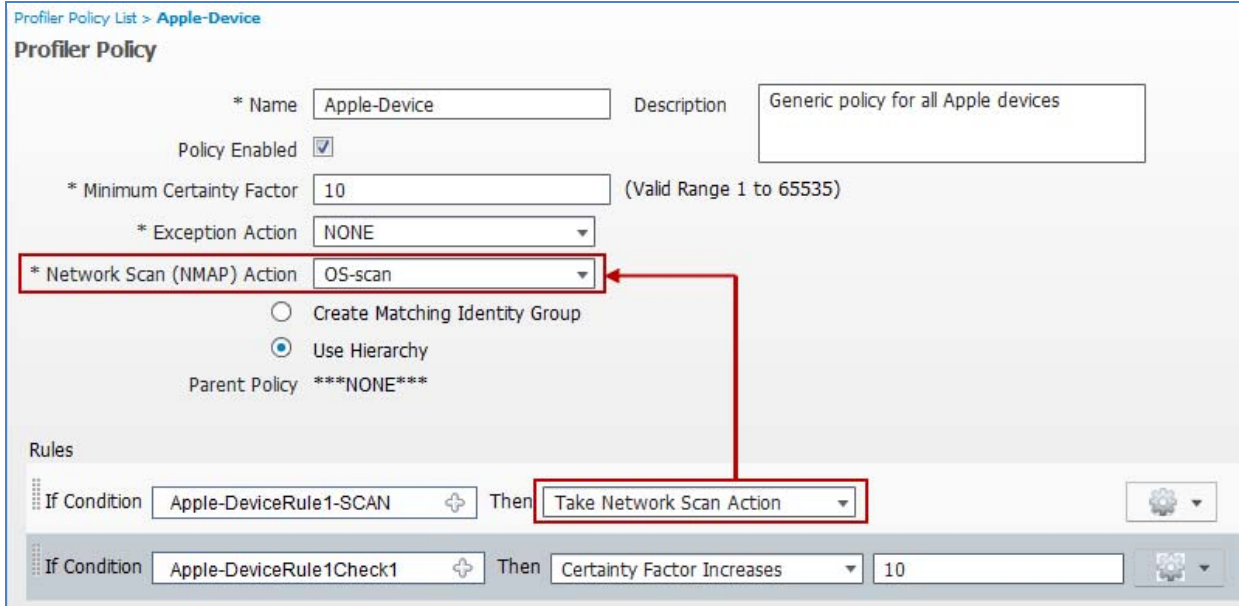
Network Scan (NMAP) Action Name	Description
<input type="checkbox"/> CommonPortsAndOS-scan	Perform operating system and common ports detection (not SNMP).
<input type="checkbox"/> OS-scan	Perform operating system detection.
<input type="checkbox"/> SNMPPortsAndOS-scan	Perform operating system and SNMP ports detection. Used for 'Unknown' endpoints.

步骤 3 如有必要，可以定义其他 NMAP 操作，不过已经配置最常用的选项。例如，可以创建名称为 **CommonPorts** 或 **SNMPPorts** 的新扫描操作，从而仅执行通用端口或 SNMP 端口扫描，作为所触发响应的一部分。

检查配置，向分析策略条件分配 NMAP 操作

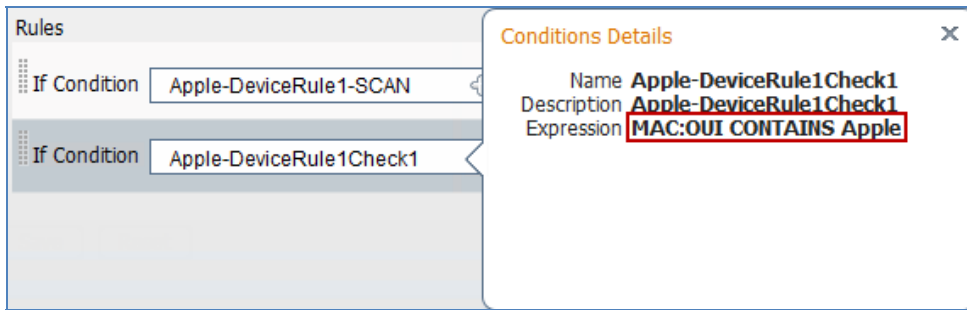
步骤 1 转至 Policy → Profiling 并从右侧窗格的列表中选择 Apple-Device 配置文件（图 61）。

图 59. 使用 NMAP 扫描操作的分析策略示例



步骤 2 Apple 设备配置文件有两个条件。在第二个条件名称右侧点击查看规则条目的内容（图 62）。

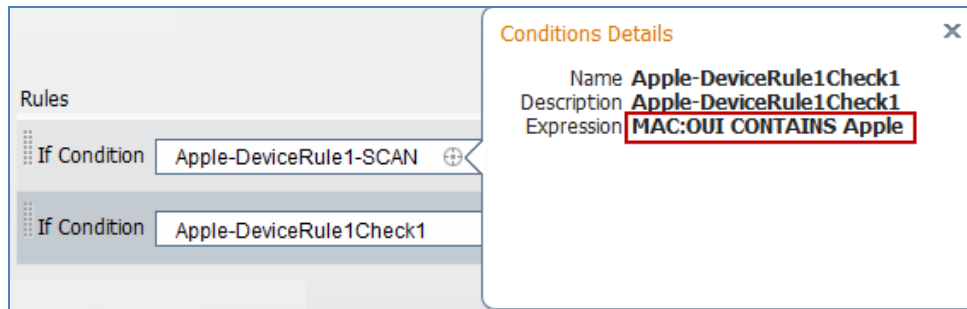
图 60. NMAP 扫描分析策略规则示例 1



此规则通过提高可信度 (CF)，将终端与此配置文件进行匹配。如果 MAC 地址提供的 OUI 与“Apple”匹配，则符合该条件。

步骤 3 在第一个条件名称右侧点击查看其内容（图 63）。

图 61. NMAP 扫描分析策略规则示例 2



此规则用于触发终端扫描。第一个条件与第二个规则中使用的条件相同。因此，根据第二个条件与此配置文件匹配的任何终端都将自动匹配第一个规则并触发所选的网络扫描操作，即操作系统扫描。

可通过点击现有规则表右侧的齿轮图标，添加或删除各规则条目。

步骤 4 当您完成查看或更改后，请点击页面底部的 **Save**，提交更改。

此程序旨在查看可以如何根据匹配的条件将网络扫描操作应用于配置文件。在[配置分析策略](#)章节将详细介绍分析策略配置。

根据触发的终端扫描操作验证 NMAP 探测功能数据

- 步骤 1** 从 Administration → Identity Management → Identities → Endpoints 删除终端。
- 步骤 2** 从配置为支持使用 NMAP 探测功能进行分析的接入设备断开终端，然后重新连接该终端。
- 步骤 3** 转至 ISE Policy Administration 节点并导航至 Administration → Identity Management → Identities。
- 步骤 4** 从左侧窗格选择 Endpoints。
- 步骤 5** 查找并选择新连接的终端的 MAC 地址，显示 HTTP 探测功能捕获的属性。
- 步骤 6** 在示例中，除 NMAP 之外，仅启用了 RADIUS 和 DHCP（IP 帮助程序）。这两个额外的探测功能用于发现新终端并将其与相应的 MAC 地址和 IP 地址信息一起添加至内部终端数据库。这有助于确保正确应用而不丢弃 NMAP 探测功能数据。

图 62. 终端扫描提供的 NMAP 探测功能属性示例 1

Endpoint List > 7C:6D:62:E3:D5:05

Endpoint

* MAC Address **7C:6D:62:E3:D5:05**

* Policy Assignment

Static Assignment

* Identity Group Assignment

Static Group Assignment

Attribute List

MACAddress	7C:6D:62:E3:D5:05
MatchedPolicy	Apple-Device
MessageCode	3001
NAS-IP-Address	10.1.44.90
NAS-Identifier	Cisco_0c:99:a4
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
NetworkDeviceGroups	Device Type#All Device Types#Wireless, Location#All Locations#
NetworkDeviceName	wlc5508
NmapScanCount	1
OUI	Apple, Inc

所截取的输出显示已对该终端 (**NmapScanCount**) 进行初始扫描，但是对 Apple 设备的配置文件分配仍是基于 OUI。此扫描是根据适用于 Apple 设备的匹配配置文件条件而触发的。

经过短暂的时间之后，就应已完成操作系统扫描。退出并重新选择相同终端，查看任何已更新的分析属性（图 65）。

突出显示的关键属性包括：

- EndPointPolicy
- LastNmapScanTime
- NmapScanCount
- OUI
- operating-system

图 63. 终端扫描提供的 NMAP 探测功能属性示例 2

Endpoint List > 7C:6D:62:E3:D5:05

Endpoint

* MAC Address **7C:6D:62:E3:D5:05**

* Policy Assignment

Static Assignment

* Identity Group Assignment

Static Group Assignment

Attribute List

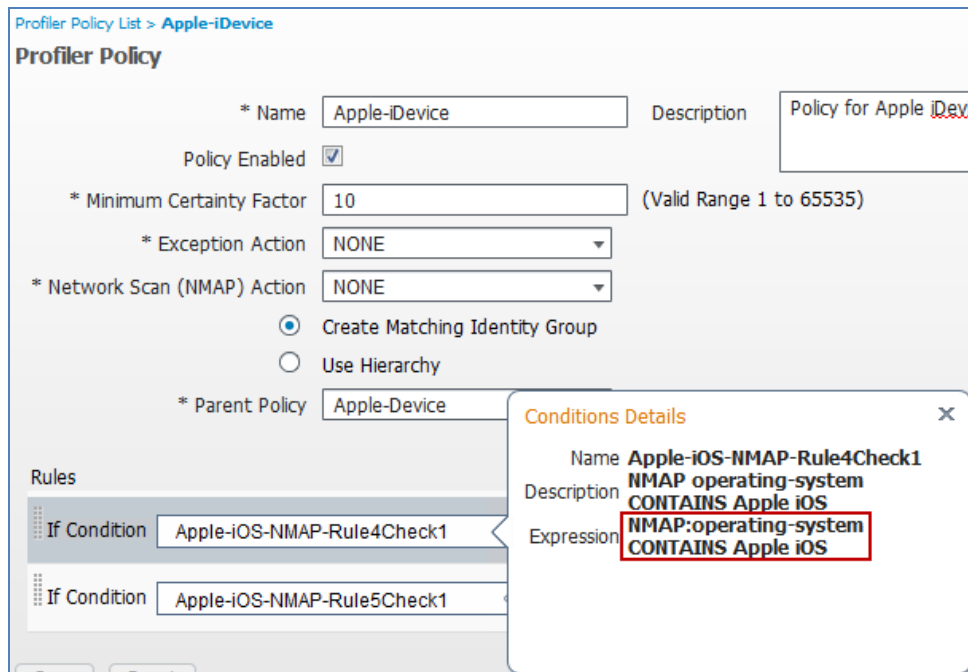
EndPointMACAddress	7C-6D-62-E3-D5-05
EndPointMatchedProfile	Apple-iDevice
EndPointPolicy	Apple-iDevice
EndPointProfilerServer	ise-psn-1
EndPointSource	RADIUS Probe
ExternalGroups	cts.local/users/employees\,cts.local/users/domain users\
Framed-IP-Address	10.1.40.101
IdentityAccessRestricted	false
IdentityGroup	Apple-iDevice
IdentityPolicyMatchedRule	Default
LastNmapScanTime	2012-May-03 05:59:56 UTC
Location	Location#All Locations#North_America#RTP
MACAddress	7C:6D:62:E3:D5:05
MatchedPolicy	Apple-iDevice
NAS-Port-Type	Wireless - IEEE 802.11
NetworkDeviceGroups	Device Type#All Device Types#Wireless, Location#All L
NetworkDeviceName	wlc5508
NmapScanCount	2
OUI	Apple, Inc
PolicyVersion	22
PostureAssessmentStatus	NotApplicable
host-name	Apple-Ipad
htype	Ethernet (10Mb)
ip	10.1.40.101
op	BOOTREQUEST
operating-system	Apple iOS general purpose 4.X (accuracy 93%)
secs	0

在本例中，明显已完成 NMAP 扫描。**EndPointSource** 属性表示执行最后一次更新的 RADIUS。这是可行的，因为随着不同来源提供分析数据，该值会不断变化。

LastNmapScanTime 和 **NmapScanCount** 属性对于设备分类并不十分重要，但是已突出显示以显示由 NMAP 探测功能添加的属性。

OUI 属性是 **Apple**，但现在所分配的配置文件为 **Apple-iDevice** 而不是更通用的 **Apple-Device** 的配置文件。这是因为与已触发的 NMAP 扫描的结果匹配，此结果揭示终端操作系统为 **Apple iOS**。如果您在 **Policy** → **Profiling** 下查看 **Apple-iDevice** 配置文件的内容，您会发现此配置文件可以根据 NMAP 操作系统扫描结果与两个条件之一匹配（图 64）。

图 64. Apple iDevice 的分析策略



步骤 7 如果 NMAP 扫描返回包含 **Apple iOS** 或 **Apple iPhone OS** 的 **operating-system** 属性值，则与此配置文件匹配。在本例中，它匹配的是 **Apple iOS**。

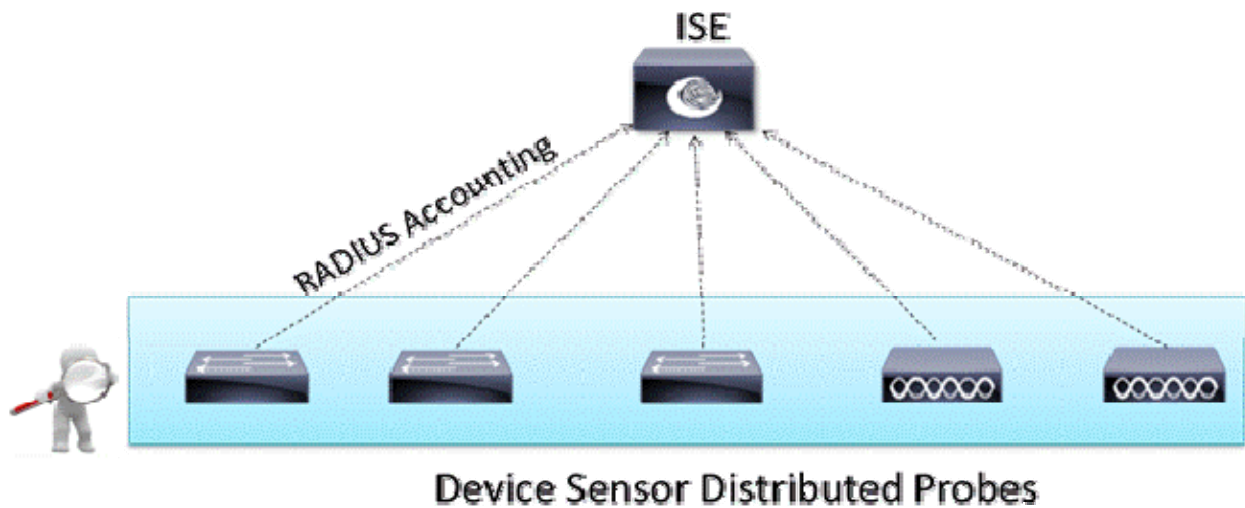
步骤 8 总之，在根据由操作系统扫描确定的终端操作系统对终端进行分类时，NMAP 探测功能很有用。许多无客户端设备都支持可以接收设备分类查询的 **SNMP** 代理。其他设备可根据其开放端口进行分类，而且策略可以控制运行特定服务的某些设备应该获得更多还是更少的限制权限。无论授权策略分配情况如何，每个探测功能都会增加可视性，这对于整个网络的运行和安全管理都有价值。

设备传感器

设备传感器概述

设备传感器是思科接入交换机和无线控制器（例如 Cisco Catalyst 3650 和 3750 系列以及 4500 系列交换机）当前支持的接入设备功能。设备传感器从通过各种协议（例如思科发现协议 (CDP)、链路层发现协议 (LLDP) 和动态主机配置协议 (DHCP)）连接的终端收集网络信息并将这些信息转发至 RADIUS 计费数据包中的 ISE PSN（图 67）。ISE 能够仅使用 RADIUS 探测功能收集和解析分析数据。

图 65. 设备传感器概述



设备传感器详细信息

设备传感器从网络设备收集原始终端数据。所收集的终端信息有助于完成交换机分析功能。接入设备的分析功能由以下两部分组成：

收集器 - 收集来自网络设备的终端数据

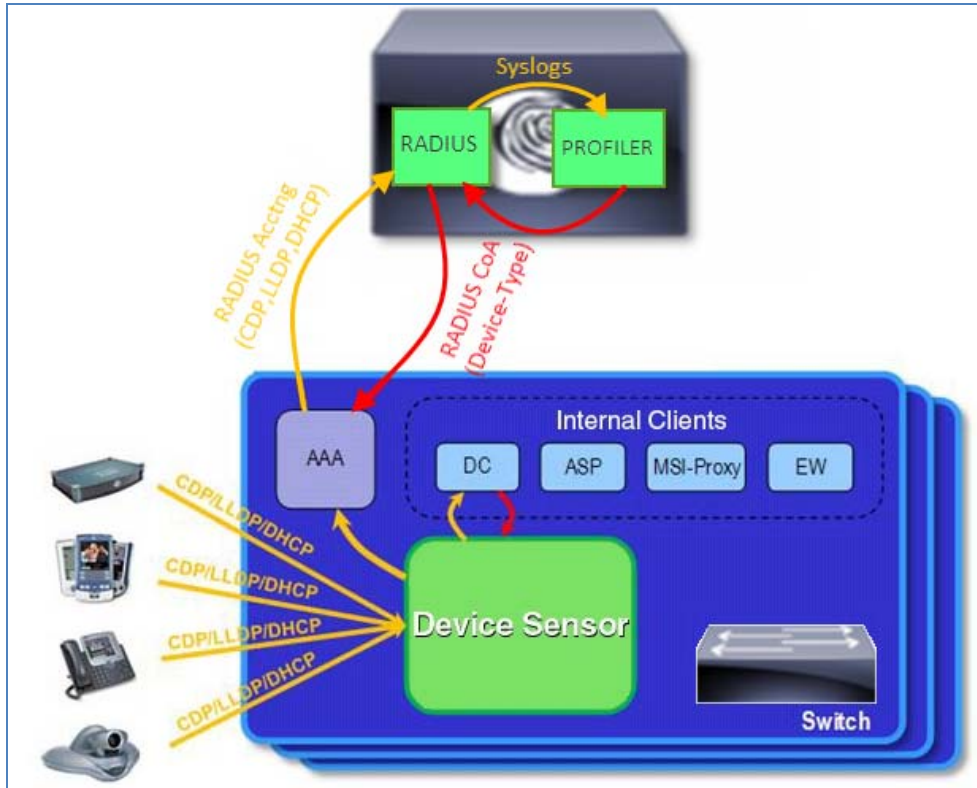
分析器 - 处理这些数据并确定设备的类型

设备传感器代表接入设备（例如 Cisco Catalyst 交换机或思科无线局域网控制器）的嵌入式收集器功能。图 68 显示分析系统情景中的传感器并且描述了传感器数据的其他可能的使用者。

具备传感器功能的交换机或无线控制器可从使用 CDP、LLDP 和 DHCP 等协议的网络设备收集终端信息，经过静态配置的过滤器筛选，并将这些消息提供给访问会话情景中的注册客户端。访问会话表示与网络设备的终端连接。

设备传感器拥有内部和外部客户端。内部客户端包括嵌入式设备分类器（DC 或本地分析器）、Cisco Auto SmartPorts (ASP)、MSI-Proxy 和 Cisco EnergyWise™ (EW) 等组件。设备传感器使用 RADIUS 记账功能将数据发送到外部客户端（如身份服务引擎分析 (ISE) 分析用“分析器”）。

图 66. 设备传感器操作详细信息



此功能会生成客户端通知、包含分析数据的记帐消息以及会话事件和其他会话相关的数据（例如 MAC 地址和入口端口数据）并将其发送至内部和外部客户端 (ISE)。默认情况下，对于每个支持的对等协议，只有在传入数据包包含在特定会话中之前未被接收的分析属性或类型长度值 (VLT) 的情况下，才会生成客户端通知和记帐事件。您可以为所有 TVL 更改启用客户端通知和记帐事件，而无论是接收了新 TLV 还是之前接收的 TLV 使用 CLI 命令接收了不同的值。

传感器将监控会话的最大设备数量限制为每个端口（访问端口和中继端口）32 台设备。换句话说，每个端口上最多可以监控 32 个终端。非活动计时器会断开持续时间超出 12 小时的会话。

设备传感器要求

表 6 按接入设备和版本汇总了设备传感器协议支持。

表 6. 设备传感器要求

平台	CDP	LLDP	DHCP	HTTP	mDNS
Catalyst 3560/3750 系列交换机	15.0(1)SE1	15.0(1)SE1	15.0(1)SE1	-	-
Catalyst 4500 系列交换机	15.1(1)SG IOS-XE 3.3.0SG	15.1(1)SG IOS-XE 3.3.0SG	15.1(1)SG IOS-XE 3.3.0SG	-	15.1(1)SG IOS-XE 3.3.0SG
WLC/WiSM2 无线控制器	-	-	7.2.110.0	7.3	-

注：请务必为您的平台引用适用的版本说明，以确认软件版本和功能支持。例如，有很多 Catalyst 3560 和 3750 交换机未满足思科 IOS 软件版本 15.0(1)SE1 和设备传感器功能的要求。

思科 IOS 软件版本 15.0(2)SE 提供对 Catalyst 3560-C 和 3560-CG 系列交换机的设备传感器功能的支持。

当在思科无线控制器上部署设备传感器时，系统会为连接配置用于感测的 WLAN 的所有客户端启用 DHCP 分析。客户端 DHCP 请求支持 DHCP 代理和桥接模式。在 7.2MR1 中的限制包括：

不支持独立接入点。

不支持对本地交换的本地身份验证。

总之，设备传感器为 ISE 分析服务提供扩展收据收集方面的显著优势。使用设备传感器，数据收集会广泛分布于接入层、最接近终端的点和数据源中。在来源点会对信息进行选择性过滤，然后使用 RADIUS 计帐数据包将这些信息传输至集中式策略服务节点以进行分析和分类。与使用传统 ISE 探测功能捕获这些相同的数据相比，这样可以减少很多设计挑战和基础设施要求。

为 ISE 分析配置设备传感器

设备分类器从 MAC-OUI 以及 CDP、LLDP 和 DHCP 等协议收集信息并识别设备。要收集 CDP 和 LLDP 信息，必须在 Catalyst 交换机上启用 CDP 和 LLDP。要使 DHCP 选项信息可用于设备分类器，必须在交换机上启用 DHCP 搜索功能。思科无线局域网控制器目前仅支持 DHCP 数据。然后可以定义过滤器，其指定要发送至分析器 (ISE) 的特定属性和选项。要将传感器数据发送至 ISE，接入设备必须启用 RADIUS 计帐。ISE 必须启用并正确配置 RADIUS 探测功能。

注：需要使用 RADIUS 计帐功能才能将传感器数据转发至 ISE。但是，无需 RADIUS 身份验证和授权即可收集传感器数据并将其发送至 ISE。因此，当组织尚未准备好启用 RADIUS 身份验证时，即使是在仅监控模式下，在网络发现阶段都可以将设备传感器用于 ISE 预部署。此支持可扩展至将 ISE 分析服务用于未部署 RADIUS 访问控制的思科 NAC 设备的部署中。

在 ISE 中启用 RADIUS 探测功能

- 步骤 1** 在[配置 RADIUS 探测功能](#)章节详细介绍了启用 RADIUS 探测功能的步骤。请参阅该章节，了解如何正确启用和配置 RADIUS 探测功能。
- 步骤 2** 该章节提供的说明中有一种例外情况，即在未使用基于 RADIUS 的身份验证和授权的部署中使用设备传感器。在此场景中，应该未向 ISE 添加接入设备，但是由于它们需要向 ISE 沟通 RADIUS 计帐信息，因此需要在 Administration → Network Resources → Network Devices 下添加支持设备传感器的所有接入设备。
- 步骤 3** 请确保在 ISE 中输入的 IP 地址与接入设备捕获到的用于发送 RADIUS 的值匹配。此外，请确保 RADIUS 共享密钥与接入设备上配置的值匹配。需要执行这些步骤才能支持从设备传感器接收 RADIUS 计帐数据包。

在思科有线交换机上启用分析协议

要从终端收集 CDP、LLDP 或 DHCP 属性，接入交换机需要启用这些协议以允许它读取和收集关联属性。

- 步骤 1** 访问支持设备传感器的接入交换机的命令控制台。
- 步骤 2** 启用交换机，支持 CDP。
- 步骤 3** 默认情况下，思科交换机上会全局启用 CDP。如已禁用，请使用此全局命令启用：

```
cat3750x(config)# cdp run
```

- 步骤 4** 默认情况下，各个交换端口都会启用 CDP。如已禁用，请使用以下接口命令启用：

```
cat3750x(config-if)# cdp enable
```

- 步骤 5** 如下所示，使用 `show cdp neighbors` 命令，验证交换机上 CDP 是否正常运行：

```
cat3750x# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID         Local Intrfce   Holdtme    Capability   Platform   Port ID
APc471.fe34.197a  Gig 1/0/2      137        T            AIR-LAP11  Gig 0
SEP003094C4528A  Gig 1/0/1      150        H P M       IP Phone   Port 1
cat6503.cts.local
                  Gig 1/0/24      140        R S I       WS-C6503   Gig 2/47
```

以下是详细视图:

```
cat3750x# show cdp neighbors detail
-----
Device ID: APc471.fe34.197a
Entry address(es):
  IP address: 10.1.14.100
Platform: cisco AIR-LAP1142N-A-K9 , Capabilities: Trans-Bridge
Interface: GigabitEthernet1/0/2, Port ID (outgoing port): GigabitEthernet0
Holdtime : 133 sec

Version :
Cisco IOS Software, C1140 Software (C1140-K9W8-M), Version 12.4(25e)JA, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Fri 27-Jan-12 21:45 by prod_rel_team

advertisement version: 2
Duplex: full
Power drawn: 15.400 Watts
Power request id: 21756, Power management id: 2
Power request levels are:15400 14500 0 0 0
Management address(es):
-----
Device ID: SEP003094C4528A
Entry address(es):
  IP address: 10.1.13.100
Platform: Cisco IP Phone 7960, Capabilities: Host Phone Two-port Mac Relay
Interface: GigabitEthernet1/0/1, Port ID (outgoing port): Port 1
Holdtime : 147 sec
Second Port Status: Up

Version :
P00308010100

advertisement version: 2
Duplex: full
Power drawn: 6.300 Watts
Management address(es):
-----
Device ID: cat6503.cts.local
Entry address(es):
  IP address: 10.1.50.1
Platform: cisco WS-C6503, Capabilities: Router Switch IGMP
Interface: GigabitEthernet1/0/24, Port ID (outgoing port): GigabitEthernet2/47
Holdtime : 136 sec

Version :
Cisco IOS Software, s72033_rp Software (s72033_rp-ADVIPSERVICESK9_WAN-M), Versio
n 12.2(33)SXJ2, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Wed 14-Dec-11 19:51 by prod_rel_team

advertisement version: 2
VTP Management Domain: 'cts'
Duplex: full
Management address(es):
  IP address: 10.1.50.1
```

步骤 6 Enable the switch to support LLDP.

步骤 7 默认情况下，思科交换机会全局禁用 LLDP。要启用它，请输入以下全局命令：

```
cat3750x(config)# lldp run
```

步骤 8 默认情况下，各个交换端口都会启用 LLDP。如已禁用，请使用以下接口命令启用：

```
cat3750x(config-if)# lldp receive
```

步骤 9 如下所示，使用 **show lldp neighbors** 命令，验证交换机上 LLDP 是否正常运行：

```
cat3750x# show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID Local Intf Hold-time Capability Port ID
AVA4FF00E Gi1/0/9 120 B 0004.0d4f.f00e
AVAEC8C79 Gi1/0/10 120 B 0004.0dec.8c79
AVAF694AC Gi1/0/15 120 B 0004.0df6.94ac
AVAEC8C79 Gi1/0/17 120 B 0004.0dec.8c79

Total entries displayed: 4
```

以下是详细视图：

```
cat3750x# show lldp neighbors detail
-----
Chassis id: 10.6.104.29
Port id: 0004.0d4f.f00e
Port Description - not advertised
System Name: AVA4FF00E
System Description - not advertised

Time remaining: 106 seconds
System Capabilities: B,T
Enabled Capabilities: B
Management Addresses:
IP: 10.X.104.29
OID:
1.3.6.1.4.1.6889.1.69.1.5.
Auto Negotiation - supported, enabled
Physical media capabilities:
Symm Pause(FD)
Pause (FD)
100base-TX (FD)
100base-TX (HD)
10base-T (FD)
10base-T (HD)
Media Attachment Unit type: 16
Vlan ID: - not advertised

MED Information:
```



```
MED Codes:
(NP) Network Policy, (LI) Location Identification
(PS) Power Source Entity, (PD) Power Device
(IN) Inventory

H/W revision: 4620D01B
F/W revision: b20d01b2_9_1.bin
S/W revision: a20d01b2_9_1.bin
Serial number: 051606020284
Manufacturer: Avaya
Model: 4620
Capabilities: NP, IN
Device type: Endpoint Class III
Network Policy(Voice): VLAN dot1p, tagged, Layer-2 priority: 6, DSCP: 46
Power requirements - not advertised
Location - not advertised

----<snip>----

Total entries displayed: 4
```

步骤 10 启用交换机，搜索 LLDP。在全局配置模式下输入以下命令，启用对选择的接入 VLAN 的 DHCP 搜索功能：

```
cat3750x(config)# ip dhcp snooping
cat3750x(config)# ip dhcp snooping vlan <VLANs>
```

步骤 11 列表中至少应包含连接要分析的终端的接入 VLAN。

步骤 12 要信任从直接或间接连接至受信任 DHCP 服务器的接口发送的 DHCP 信息，请使用以下接口配置命令：

```
cat3750x(config)# interface <interface_to_DHCP_Server>
cat3750x(config-if)# ip dhcp relay information trusted
```

步骤 13 如下所示，使用 **show ip dhcp snooping** 命令，验证是否已在交换机上启用 DHCP 搜索：

```
cat3750x# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10-14
DHCP snooping is operational on following VLANs:
10-14
Smartlog is configured on following VLANs:
无
Smartlog is operational on following VLANs:
无
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: 1cdf.0f8f.6000 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
```

Interface	Trusted	Allow option	Rate limit (pps)
-----	-----	-----	-----

步骤 14 如下所示，使用 **show ip dhcp snooping binding** 命令，验证 DHCP 搜索功能在交换机上是否正常运行（已为 DHCP 客户端创建绑定表）：

```
cat3750x# show ip dhcp snooping binding
-----
MacAddress      IpAddress      Lease(sec)    Type           VLAN  Interface
-----
00:30:94:C4:52:8A  10.1.13.100    691187        dhcp-snooping  13   GigabitEthernet1/0/1
00:50:56:A0:0B:3A  10.1.10.100    653260        dhcp-snooping  10   GigabitEthernet1/0/1
C4:71:FE:34:19:7A  10.1.14.100    653068        dhcp-snooping  14   GigabitEthernet1/0/2
Total number of bindings: 3
```

步骤 15 保存对交换机配置的更改。

在思科有线交换机上配置设备传感器

步骤 1 定义选择数据收集要包含或排除的 CDP、LLDP 或 DHCP 属性的过滤器。

步骤 2 在全局配置模式下开始为 CDP 属性定义过滤器：

```
cat3750x(config)# device-sensor filter-list cdp list <my_cdp_list>
cat3750x(config-sensor-cdplist)# tlv name device-name
cat3750x(config-sensor-cdplist)# tlv name address-type
cat3750x(config-sensor-cdplist)# tlv name capabilities-type
cat3750x(config-sensor-cdplist)# tlv name platform-type
cat3750x(config)# device-sensor filter-spec cdp include list <my_cdp_list>
```

步骤 3 可以按照名称或编号输入 CDP TLV 值。CDP TLV 名称如下：

address-type	地址类型
capabilities-type	功能类型
cos-type	COS 类型
device-name	设备名称
duplex-type	双工类型
external-port-id-type	外部端口 ID 类型
ipprefix-type	IP 前缀类型
mgmt-address-type	管理地址类型
mtu-type	MTU 类型
native-vlan-type	本征 VLAN 类型

platform-type	平台类型
port-id-type	端口 ID 类型
power-available-type	可用电源类型
power-request-type	外部端口 ID 类型
power-type	电源类型
protocol-hello-type	协议欢迎类型
trigger-type	触发器类型
trust-type	信任类型
twoway-connectivity-type	双向连接类型
unidirectional-mode-type	单向模式类型
version-type	版本类型
vtp-mgmt-domain-type	VTP 管理域类型
vvid-type	VVID 类型

步骤 4 在全局配置模式下开始为 LLDP 属性定义过滤器：

```
cat3750x(config)# device-sensor filter-list lldp list <my_lldp_list>
cat3750x(config-sensor-lldp-list)# tlv name system-name
cat3750x(config-sensor-lldp-list)# tlv name system-description
cat3750x(config)# device-sensor filter-spec lldp include list <my_lldp_list>
```

步骤 5 可以按照名称或编号输入 LLDP TLV 值。LLDP TLV 名称如下：

chassis-id	机箱 ID	机箱 Id
end-of-lldpdu	LLDP 结束	
management-address	管理地址	
port-description	端口说明	
port-id	端口 ID	
system-capabilities	系统功能	
system-description	系统说明	
system-name	系统名称	
time-to-live	有效时间	

步骤 6 在全局配置模式下开始为 DHCP 属性定义过滤器：

```
cat3750x(config)# device-sensor filter-list dhcp list my_dhcp_list
cat3750x(config-sensor-dhcplist)# option name host-name
cat3750x(config-sensor-dhcplist)# option name default-ip-ttl
cat3750x(config-sensor-dhcplist)# option name requested-address
cat3750x(config-sensor-dhcplist)# option name parameter-request-list
cat3750x(config-sensor-dhcplist)# option name class-identifier
cat3750x(config-sensor-dhcplist)# option name client-identifier
cat3750x(config)# device-sensor filter-spec dhcp include list my_dhcp_list
```

步骤 7 可以按照名称或编号输入 DHCP 选项。相关的一些常用选项如下：

class-identifier	类别标识符
client-fqdn	客户端 FQDN
client-identifier	客户端标识符
default-ip-ttl	默认 IP 有效时间
domain-name	域名
host-name	主机名
server-identifier	服务器 ID
user-class-id	用户类别 ID
...	

最佳实践：针对 CDP、LLDP 和 DHCP 显示的示例，过滤器提供了对于大多数使用情况来说合理的选择。要了解哪些属性可用，请使用适用于 CDP 和 LLDP 的 show 命令来查看网络中终端显示的是哪些 TLV 并确定任何特定属性是否会协助对终端进行唯一分类。也可以在 Administration → Identity Management → Identities 下，在无过滤器的情况下对设备传感器进行初始部署，查看向 ISE 显示哪些属性。可以根据被确定为匹配客户端分析条件所需的那些过滤器来应用相应的过滤器。

注：输入特定 TLV 或选项值并不表示终端在传输此信息。根据终端向交换机或网络显示的属性应用过滤器。例如，如果过滤器选择包含 DHCP 选项 client-fqdn，但是 DHCP 客户端未请求该选项，则有关该选项的任何信息对于设备传感器或 ISE 都不可用。

步骤 8 如下所示，在 RADIUS 计帐中启用要发送的传感器数据：

```
cat3750x(config)# device-sensor accounting
cat3750x(config)# device-sensor notify all-changes
```

步骤 9 禁用本地分析器，防止向 ISE 发送重复的更新：

```
cat3750x(config)# no macro auto monitor
cat3750x(config)# access-session template monitor
```

默认情况下，思科交换机会启用嵌入式设备分类器，此分类器会通过程序启用设备传感器。因此，默认情况下，也会启用设备传感器。当启用 RADIUS 身份验证和记帐功能，向 ISE 发送传感器数据时，对于各项 TLV 更改，可能会发送一个重复的 RADIUS 记帐数据包。这是由于本地分析器执行的会话监控导致的。要防止发送重复的记帐消息，必须禁用本地分析器。

如果禁用 RADIUS 身份验证（例如，在处于 ISE 预部署/发现阶段或已使用思科 NAC 设备实施 ISE 分析服务的网络中），如果禁用本地分析器，则不会发送任何传感器数据。要允许在不受本地分析器影响的情况下，发送传感器数据，请使用 **access-session template monitor** 命令。

步骤 10 将交换机配置为使用 RADIUS 记帐功能向 ISE 发送会话记帐信息。

步骤 11 如果已经配置 RADIUS 身份验证和授权，此步骤应已完成。有关配置交换机以与 ISE 通信的其他详细信息，请参考[配置 RADIUS 探测功能](#)章节。

步骤 12 如果尚未部署 RADIUS/802.1X，请务必在交换机配置中包含以下命令：

```
cat3750x(config)# aaa new-model
cat3750x(config)# aaa accounting dot1x default start-stop group radius
cat3750x(config)# radius-server host <PSN_ip> auth-port <port> acct-port <port> key <shared-secret>
cat3750x(config)# radius-server vsa send accounting
```

步骤 13 验证设备传感器是否在收集分析数据。

如下所示，使用 **show device-sensor cache** 命令，验证设备传感器是否在正常运行：

```
cat3750x# show device-sensor cache all
Device: 0050.56a0.0b3a on port GigabitEthernet1/0/1
-----
Proto Type:Name                               Len Value
dhcp 55:parameter-request-list                14 37 0C 01 0F 03 06 2C 2E 2F 1F 21 79 F9 2B
dhcp 60:class-identifier                        10 3C 08 4D 53 46 54 20 35 2E 30
dhcp 12:host-name                              9 0C 07 77 69 6E 37 2D 70 63
dhcp 50:requested-address                      6 32 04 0A 01 0A 64
dhcp 61:client-identifier                      9 3D 07 01 00 50 56 A0 0B 3A

Device: 0012.d9e3.427e on port GigabitEthernet1/0/24
-----
Proto Type:Name                               Len Value
cdp 4:capabilities-type                       8 00 04 00 08 00 00 00 29
cdp 2:address-type                            17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A 01 32 01
cdp 6:platform-type                          18 00 06 00 12 63 69 73 63 6F 20 57 53 2D 43 36 35 30 33
cdp 1:device-name                            21 00 01 00 15 63 61 74 36 35 30 33 2E 63 74 73 2E
                                                6C 6F 63 61 6C

Device: c471.fe34.197a on port GigabitEthernet1/0/2
-----
Proto Type:Name                               Len Value
cdp 4:capabilities-type                       8 00 04 00 08 00 00 00 02
cdp 2:address-type                            17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A 01 0E 64
cdp 6:platform-type                          30 00 06 00 1E 63 69 73 63 6F 20 41 49 52 2D 4C 41
                                                50 31 31 34 32 4E 2D 41 2D 4B 39 20 20 20
cdp 1:device-name                            20 00 01 00 14 41 50 63 34 37 31 2E 66 65 33 34 2E 31 39 37
61
dhcp 50:requested-address                      6 32 04 0A 01 0E 64
dhcp 60:class-identifier                      16 3C 0E 43 69 73 63 6F 20 41 50 20 63 31 31 34 30
dhcp 55:parameter-request-list                10 37 08 01 06 0F 2C 03 21 96 2B
dhcp 12:host-name                              18 0C 10 41 50 63 34 37 31 2E 66 65 33 34 2E 31 39 37 61
dhcp 61:client-identifier                      9 3D 07 01 C4 71 FE 34 19 7A
```

```

Device: 0030.94c4.528a on port GigabitEthernet1/0/1
-----
Proto Type:Name                               Len Value
cdp     2:address-type                          17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A 01 0D 64
cdp     6:platform-type                          23 00 06 00 17 43 69 73 63 6F 20 49 50 20 50 68 6F
        6E 65 20 37 39 36 30
cdp     4:capabilities-type                    8 00 04 00 08 00 00 04 90
cdp     1:device-name                          19 00 01 00 13 53 45 50 30 30 33 30 39 34 43 34 35 32 38 41
dhcp    50:requested-address                    6 32 04 0A 01 0D 64
dhcp    55:parameter-request-list             9 37 07 01 42 06 03 0F 96 23
dhcp    60:class-identifier                    39 3C 25 43 69 73 63 6F 20 53 79 73 74 65 6D 73 2C
        20 49 6E 63 2E 20 49 50 20 50 68 6F 6E 65 20 43
        50 2D 37 39 36 30 00
dhcp    12:host-name                          18 0C 10 53 45 50 30 30 33 30 39 34 43 34 35 32 38 41 00
dhcp    61:client-identifier                   9 3D 07 01 00 30 94 C4 52 8A

```

在思科无线控制器上配置设备传感器

可以使用 CLI 或 Web 管理界面在支持的无线控制器上为 DHCP 启用设备传感器。

步骤 1 要通过 CLI 在思科无线控制器上配置设备传感器，请输入以下命令：

```
> config wlan profiling radius enable <wlan-id>
```

在指定 WLAN 的所有无线客户端上启用设备传感器。

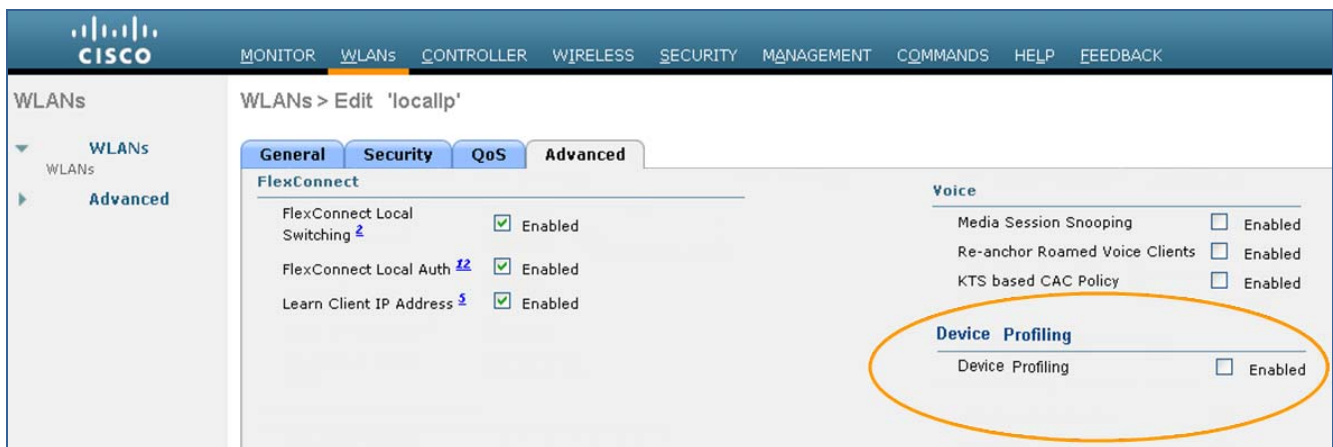
步骤 2 将无线控制器配置为使用 RADIUS 计帐功能向 ISE 发送会话计帐信息。

步骤 3 如果已经配置 RADIUS 身份验证和授权，此步骤应已完成。

步骤 4 有关配置无线控制器以与 ISE 进行 RADIUS 通信的其他详细信息，请参考[配置 RADIUS 探测功能](#)章节。

步骤 5 从 WLC Web 界面，转至 WLANs → (WLAN-id) → Edit。图 69 中的屏幕显示内容显示在何处启用设备传感器。

图 67. 无线控制器的设备传感器配置示例



使用设备传感器验证分析

- 步骤 1** 从 Administration → Identity Management → Identities → Endpoints 删除终端。
- 步骤 2** 从配置为支持使用 NMAP 探测功能进行分析的接入设备断开终端，然后重新连接该终端。
- 步骤 3** 转至 ISE Policy Administration 节点并导航至 Administration → Identity Management → Identities。
- 步骤 4** 从左侧窗格选择 Endpoints。
- 步骤 5** 查找并选择新连接的终端的 MAC 地址，显示 HTTP 探测功能捕获的属性。

在图 70 中，在 ISE 策略服务节点上仅启用了 RADIUS 探测功能。突出显示的关键属性包括：

EndPointPolicy

EndPointSource

OUI

CDP 属性（cdpCacheAddressType、cdpCacheCapabilities、cdpCacheId、cdpCachePlatform）

DHCP 属性（dhcp-class-identifier、dhcp-client-identifier、dhcp-parameter-request-list、dhcp-requested-address、host-name）

图 68. 设备传感器属性示例

Endpoint

* MAC Address **00:30:94:C4:52:8A**

* Policy Assignment **Cisco-IP-Phone-7960**

Static Assignment

* Identity Group Assignment **Cisco-IP-Phone**

Static Group Assignment

Attribute List

AcsSessionID	ise-psn-1/125323864/12755
AuthState	Authenticated
CPMSessionID	0A010A01000000900036DFC
Called-Station-ID	1C-DF-0F-8F-60-01
Calling-Station-ID	00-30-94-C4-52-8A
Device IP Address	10.1.50.2
Device Type	Device Type#All Device Types#Wired
EndPointPolicy	Cisco-IP-Phone-7960
EndPointProfilerServer	ise-psn-1
EndPointSource	RADIUS Probe
Framed-IP-Address	10.1.13.100
IdentityGroup	Cisco-IP-Phone
Location	Location#All Locations#North_America#RTP
MACAddress	00:30:94:C4:52:8A
MatchedPolicy	Cisco-IP-Phone-7960
MessageCode	3002
NAS-IP-Address	10.1.50.2
NAS-Port	50101
NAS-Port-Id	GigabitEthernet1/0/1
NAS-Port-Type	Ethernet
NetworkDeviceGroups	Device Type#All Device Types#Wired, Location#All Locations#North_America#RTP
NetworkDeviceName	cat3750x
OUI	Cisco Systems, Inc.
PolicyVersion	22
RequestLatency	12
SelectedAccessService	Default Network Access
Service-Type	Framed
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	24
Total Certainty Factor	145
attribute-151	A4117E8D
cdpCacheAddressType	00:00:00:01:01:01:cc:00:04:0a:01:0d:64
cdpCacheCapabilities	H;P;M
cdpCacheDeviceId	SEP003094C4528A
cdpCachePlatform	Cisco IP Phone 7960
audit-session-id=0A010A01000000900036DFC, connect-progress=Call Up, cdp-tlv=cdpCacheAddressType=00:00:00:01:01:01:cc:00:04:0a:01:0d:64; cdp-tlv=cdpCachePlatform=Cisco IP Phone 7960, cdp-tlv=cdpCacheCapabilities=00:00:04:90, cdp-tlv=cdpCacheDeviceId=SEP003094C4528A, dhcp-address=10.1.13.100, dhcp-option=dhcp-parameter-request-list=1, 66, 6, 3, 15, 150, 35, dhcp-option=dhcp-class-identifier=Cisco Systems, Inc. IP Phone CP-7960, dhcp-option=dhcp-client-identifier=01:00:30:94:c4:52:8a	
dhcp-class-identifier	Cisco Systems, Inc. IP Phone CP-7960
dhcp-client-identifier	01:00:30:94:c4:52:8a
dhcp-parameter-request-list	1, 66, 6, 3, 15, 150, 35
dhcp-requested-address	10.1.13.100
host-name	SEP003094C4528A
ip	10.1.13.100

如果我们在将 **EndPointSource** 设置为 RADIUS 探测功能的情况下单独使用设备传感器，可以发现 **EndPointPolicy** 正确地与 Cisco-IP-Phone-7960 匹配。从促使配置文件匹配的设备传感器接收的分析属性包含 **OUI = Cisco Systems, Inc.**、**cdpCachePlatform = Cisco IP Phone 7960** 并且 **dhcp-class-identifier = Cisco Systems, Inc, IP Phone CP-7960**。

请注意，CDP 和 DHCP 属性仅包含过滤器指定的那些属性，其中过滤器会显示已如何优化数据收集。策略服务节点无需在 ISE 部署中的所有管理和策略服务节点中解析和同步不必要的属性。根据设备传感器配置，仅在发生变更时才会接收到更新。另一方面，SNMP 查询和 DHCP 探测功能在每次查询或 DHCP 更新时都会更新属性。

最佳实践： 在可能的情况下，请使用设备传感器部署 ISE 分析，从而最大程度地提高可扩展性并简化整体管理和分析配置。对于通过 RADIUS 身份验证的环境和其他类型的部署（例如 ISE 预发现阶段或与 NAC 设备集成），都可以在有线接入交换机和无线控制器上部署设备传感器。

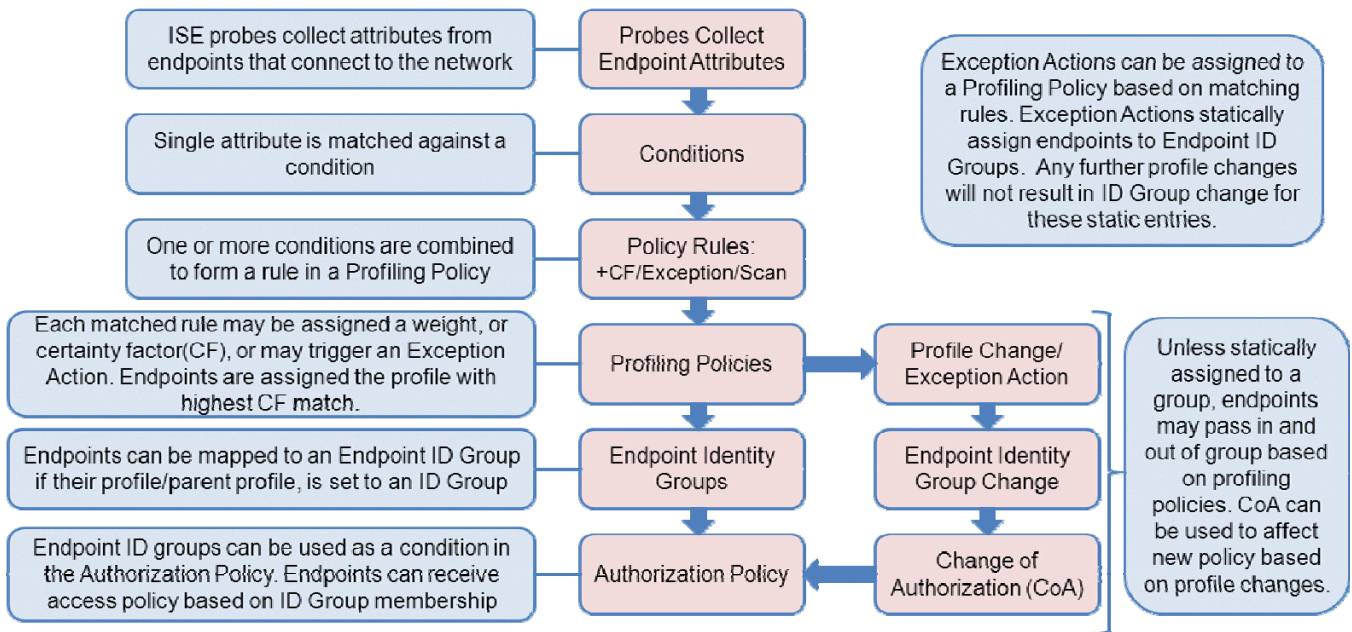
配置分析策略

分析策略配置概述

在本指南中前面部分，我们已经介绍 ISE 分析服务的高级架构，如图 71 所示，这还可以用作 ISE 分析配置和整个流程的一般指导原则。

我们刚刚完成流程中的第一部分，即配置探测功能以收集终端属性。在本部分，我们将继续介绍其余部分，配置分析策略和授权策略以满足客户分析要求。

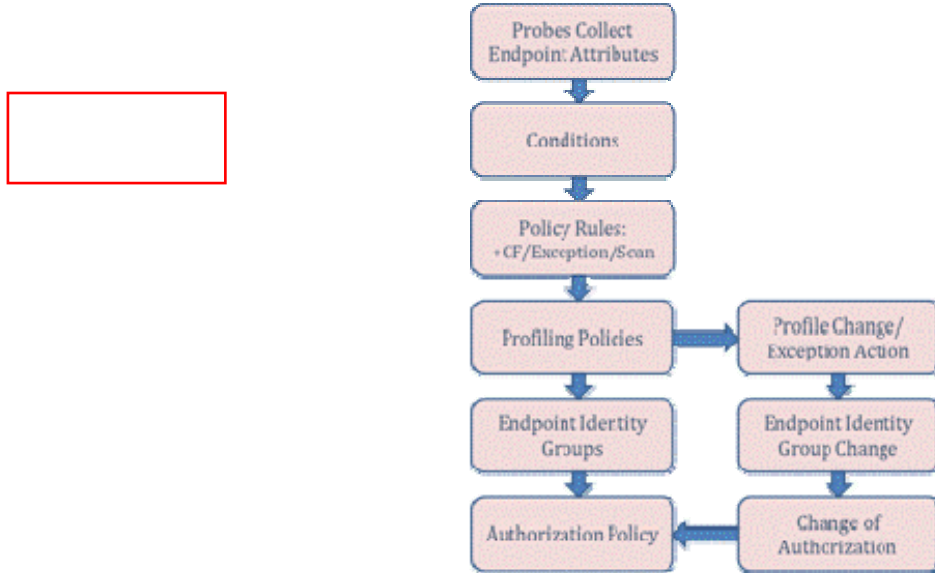
图 69. ISE 分析策略配置流程



分析条件

很多分析属性都可以通过各种 ISE 探测功能收集。ISE 策略服务节点收集了属性之后，分析过程的下一步是将这些属性与分析条件进行匹配（图 72）。每个条件代表与 Policy → Policy Elements → Dictionary 下 System Dictionary 中列出的受支持属性的一个匹配项。

图 70. 配置流程：分析条件



字典属性

表 7 表示 Policy → Policy Elements → Dictionary 下 System Dictionary 中列出的属性。当在 Policy → Policy Elements → Conditions → Profiling 中创建或修改分析条件时，这些属性是可选的。

表 7. 字典属性

RADIUS	MAC	SNMP	CDP	NetFlow	NMAP
Acct-Authentic	MACAddress	cafSessionAuthorizedBy	cdpCacheAddress	MAX_PKT_LENGTH	110-tcp
Acct-Delay-Time	OUI	cafSessionAuthUserName	cdpCacheCapabilities	MAX_TTL	123-udp
Acct-Input-Octets		cafSessionAuthVlan	cdpCacheDeviceId	MIN_PKT_LENGTH	135-tcp
Acct-Input-Packets		cafSessionClientMacAddress	cdpCachePlatform	MIN_TTL	135-udp
Acct-Interim-Interval		cafSessionDomain	cdpCacheVersion	nexthop	137-udp
Acct-Link-Count		cafSessionStatus	LLDP	OUT_BYTES	138-udp
Acct-Multi-Session-Id		clApIfMacAddress		OUT_PKTS	139-tcp
Acct-Output-Octets	IP	clApName	LLDP	output	139-udp
Acct-Output-Packets		clApNameServerAddress		OUTPUT_SNMP	143-tcp
Acct-Session-Id	EndpointSource	clApNameServerAddressType	lldpCacheCapabilities	prot	1434-udp
Acct-Session-Time	FQDN	clApSshEnable	lldpCapabilitiesMapSupported	sampling_interval	161-udp
Acct-Status-Type	Host	clApSysMacAddress	lldpChassisId	source_id	162-udp
Acct-Terminate-Cause	ip	clApTelnetEnable	lldpManAddress	src_as	1900-udp
Acct-Tunnel-Connection	mask	clApTertiaryControllerAddress	lldpPortDescription	SRC_MAC	21-tcp
Acct-Tunnel-Packets-Lost	PortalUser	clApTertiaryControllerAddress	lldpPortId	SRC_MASK	22-tcp
Callback-ID	User-Agent	clApUpTime	lldpSystemCapabilitiesMapEnabled	SRC_TOS	23-tcp
Callback-Number	DHCP		lldpSystemDescription	SRC_VLAN	25-tcp
				lldpSystemName	srcaddr

(不完整列表)	boot-file client-fqdn client-identifier device-class dhcp-class-identifier dhcp-client-identifier dhcp-message-type dhcp-parameter-request-list dhcp-requested-address dhcp-user-class-id domain-name host-name name-servers pxe-client-arch pxe-client-machine-id pxe-client-network-id server-identifier vendor-class	(不完整列表)			
---------	--	---------	--	--	--

配置分析条件

思科 ISE 在交付时即已预置大量分析条件，用于在分析策略中构建一个大型配置文件库。有时候可能需要创新新自定义条件或修改现有条件，从而满足特定终端和特定环境的要求。

配置自定义（用户定义）分析条件。

- 步骤 1** 转至 Policy → Policy Elements → Conditions 并从左侧窗格选择 Profiling。滚动浏览条件列表，了解用于创建条件的常用属性（例如 **OUI**、**dhcp-class-identifier**、**host-name**、**User-Agent**）以及 SNMP MIB 数据（例如 **cdpCachePlatform**、**lldpSystemDescription** 和 **hrDeviceDescr**）。
- 步骤 2** 为了说明创建自定义分析条件的流程，我们将使用一个真实的示例。在 Endpoints → Identities 的列表下列出了显示以下内容的终端（图 73）：

图 71. 未知终端示例

Endpoints			
Edit Add Delete Import Export			
	Endpoint Profile	MAC Address	Static Assignment
<input type="checkbox"/>	Unknown	00:C0:B7 65:1F:BC	false
<input type="checkbox"/>	Unknown	00:C0:B7 68:31:E1	false

步骤 3 图中的两个条目均显示为 Unknown 配置文件；此外，它们拥有相同的 MAC 前缀。查看第一个终端的详细属性会揭示以下信息（图 74）：

图 72. 终端扫描提供的 NMAP 探测功能属性示例 1

MACAddress	00:C0:B7:65:1F:BC
MatchedPolicy	Unknown
MessageCode	3000
NAS-IP-Address	10.1.50.2
NAS-Port	50108
NAS-Port-Id	GigabitEthernet1/0/8
NAS-Port-Type	Ethernet
NetworkDeviceGroups	Device Type#All Device Types#Wired, Location#All Locations#North_America#RTP
NetworkDeviceName	cat3750x
OUI	AMERICAN POWER CONVERSION CORP

步骤 4 其可以通过直接检查连接至 GigabitEthernet1/0/8 的终端确定，也可以根据 OUI (American Power Conversion Corp) 简单推断得出：这些终端为用于实验室数据中心安装的 APC 不间断电源系统 (UPS) 的 SNMP 网络管理连接。因为对于这些终端，库中没有默认条件，我们将进行创建并最终构建一个新的策略，从而在整个网络中支持所有这些设备。

步骤 5 从右侧窗格点击 Add。

步骤 6 在本例中，名称 **APC-OUICheck** 用于指示供应商和检查类型。

步骤 7 在本例中，输入说明 **Custom OUI check for American Power Conversion Corp**。我们建议您添加一个唯一标识符，本例中添加的是单词“Custom”，以便快速过滤和显示所创建的所有用户定义条件。

步骤 8 在 Type 下有很多类别。对于此检查，Type 为 **Mac**（图 75）。

图 73. 用户定义的分析器条件示例 1

步骤 9 Attribute Name 为 **OUI**。

步骤 10 Operator 为 **EQUALS**。

步骤 11 Attribute Value 为分配给 OUI 的供应商名称。在本例中此值为 **AMERICAN POWER CONVERSION CORP**。

注：当指定 Attribute Value 时，请务必使用准确的大小写。

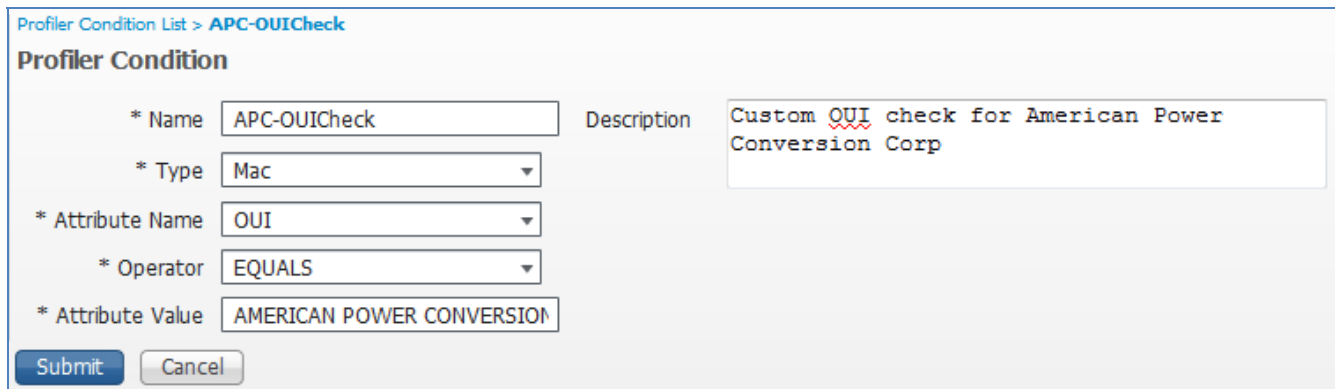
在所给示例中，可以选择使用运算符 MATCH 并将 Attribute Value 设置为“AMERICAN POWER”或“AMERICAN POWER CONVERSION”，代替使用完全匹配运算符 (EQUALS)。

如果 OUI 数据库缺少适用于特定 MAC 地址前缀的条目，则可以使用以下设置为未知 OUI 创建一个条件：

- Type = Mac
- Attribute Name = MACAddress
- Operator = CONTAINS
- Attribute Value = XX:XX:XX（MAC 地址的 3 字节前缀）

步骤 12 图 76 显示用户定义的配置文件的最终表单。

图 74. 用户定义的分析器条件示例 2



Profiler Condition List > APC-OUICheck

Profiler Condition

* Name: APC-OUICheck Description: Custom OUI check for American Power Conversion Corp

* Type: Mac

* Attribute Name: OUI

* Operator: EQUALS

* Attribute Value: AMERICAN POWER CONVERSION

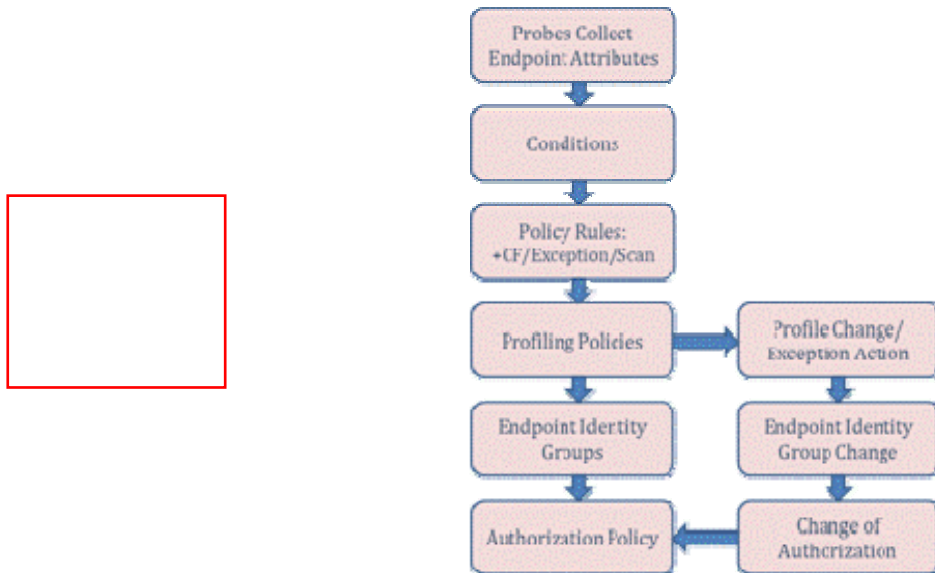
Submit Cancel

步骤 13 点击 Submit 按钮（如果是连续编辑，则点击 Save 按钮），提交更改。

分析策略和规则

分析策略或配置文件定义终端要被视为与配置文件匹配必须符合的策略规则。此策略规则包含一个或多个条件。如果符合规则的所有条件（使用 AND 运算符）或符合规则的一个条件（使用 OR 运算符），则会执行指定的操作。图 77 显示分析策略配置流程。

图 75. 配置流程：分析策略和规则



分析策略规则操作

受支持的三个分析策略规则操作如下：

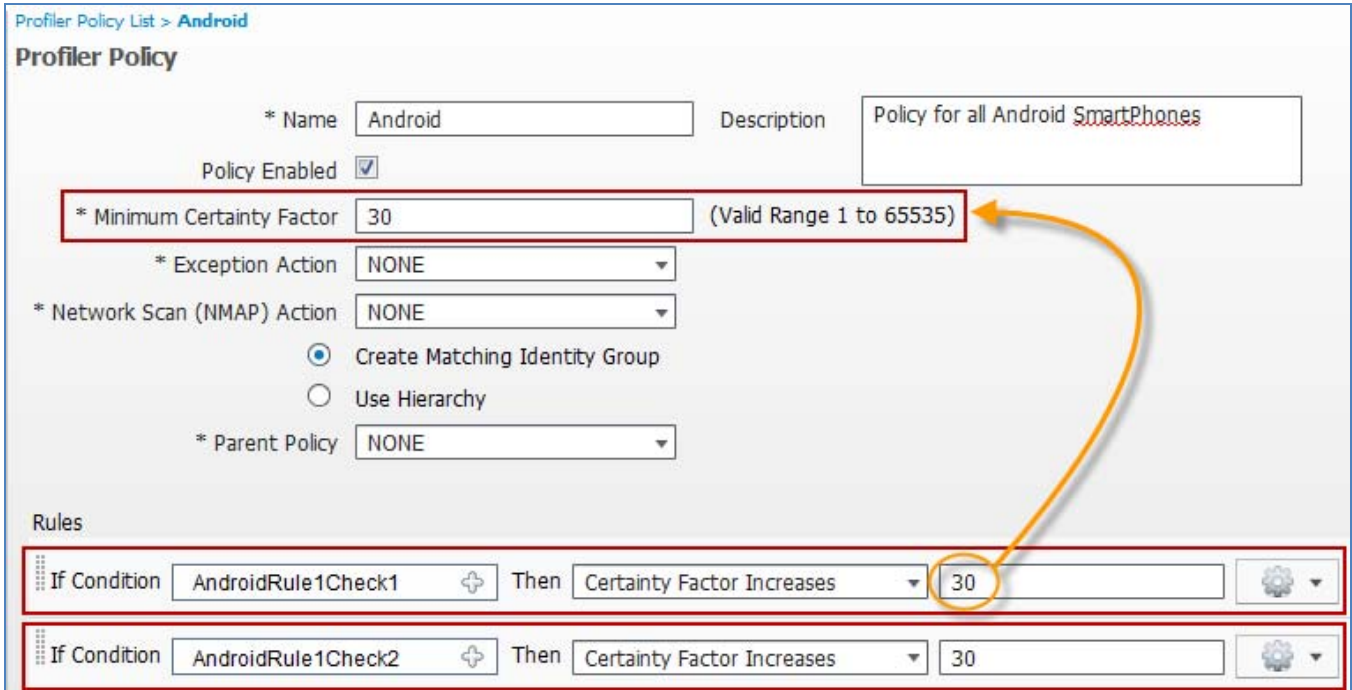
- 可信度增加 <X>
- 执行例外操作
- 执行网络扫描操作

可信度 (CF)

图 78 显示名称为 Android 的简单分析策略。此策略包含两个规则。每个规则都有一个条件，如果满足这些条件，则会执行“可信度增加 30”的操作。CF 用于提供依据匹配的条件终端与配置文件正确匹配的一般权重或相对可信程度。

对于 Android 配置文件，本例将 Minimum Certainty Factor 设置为 30。因此，如果匹配任一规则，则该终端就可分配给此配置文件。由于终端可以匹配多个条件，因而可以同时匹配多个配置文件，所以必须根据匹配的配置文件计算累计 CF 值。

图 76. 分析策略示例



有四个分析策略分配标准。如果满足以下所有条件，则终端将被分配至配置文件：

必须启用策略。（必须选中/启用 Policy Enabled 复选框。）

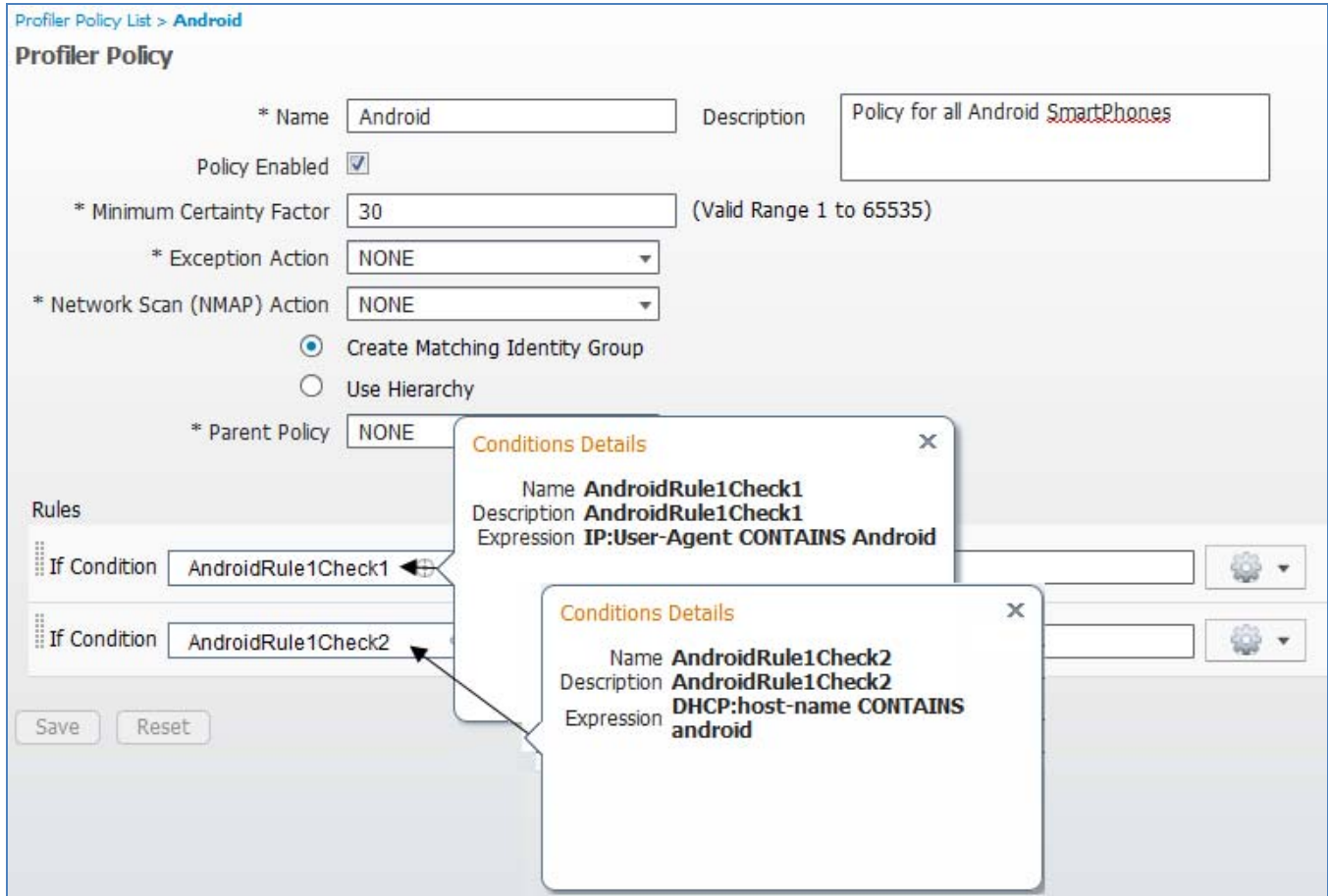
配置文件的终端累计 CF 值达到最低可信度值。

配置文件的 CF 评分高于任何其他配置文件，同时达到第 1 和 2 条标准。

（如果配置文件是层次结构的一部分）终端达到父配置文件的最低 CF 值。

根据图 79 中显示的 Android 策略示例中的第一个规则，如果终端的 **User-Agent** 包含字符串“Android”，其对于此配置文件的 CF 值将增至 30。如果终端与第二条规则匹配（DHCP **host-name** 值包含字符串“Android”），则也会使其对于此配置文件的 CF 增至 30。如果与两个规则的条件都匹配，其 CF 将为 60。

图 77. 分析策略规则示例



即使 CF 达到 60，从技术角度看，终端仍可能与另一个 CF 值高于 60 的策略的条件匹配。如果满足所有其他条件，终端会被分配至该配置文件，即使它满足 Android 策略的所有条件。

通常，应将预定义策略的 CF 值保留为默认值。有时候需要修改默认值，从而确保根据网络策略或首选项特定策略优先于其他策略。在那种情况下，请在首选策略中将适用规则的 CF 值增加最小量，从而满足您所需的分析目标。

同样，如果您创建新配置文件，请将初始 CF 值设置为相对低的值（例如 10 或 20），然后监控策略分配，验证是否得到想要的结果。如果初始值设置得太高，当与其他策略相比，某个配置文件的规则设置的 CF 值异常高时，根据 CF 计算值可能无法应用与实际终端可能更接近的其他配置文件。

例如，如果某个终端与自定义配置文件 A 的单个规则匹配，导致 CF 值增至 100，即使该终端与配置文件 B 的四条规则匹配，但是每个匹配项仅将 CF 值提高 20，该终端始终无法分配至配置文件 B。甚至有可能，配置文件 A 中的规则与配置文件 B 中的规则完全一样，但是分配的 CF 值却不一致。因此，一般都建议在所有策略规则中使用一致的 CF 评分。

思科最佳实践：一般都建议将 CF 值保持默认设置。如果需要修改默认设置，从而确保特定配置文件分配享有优先权，仅将首选配置文件中规则的值增加至影响所需策略分配的最低值即可。

如果创建自定义配置文件，请保持较低的 CF 初始值，或将其设置为与其他配置文件相同的值。

例外和 NMAP 操作

匹配的规则的另两个可能的操作包括执行网络扫描操作和执行例外操作。执行网络扫描操作将允许策略服务节点依据 Network Scan (NMAP) Action 字段的设置对终端触发 NMAP 扫描。[使用网络扫描 \(NMAP\) 探测功能进行分析](#) 章节详细介绍了此功能。

执行例外操作允许 ISE 根据 Exception Action 字段的设置，将终端静态分配至某个策略。[例外操作](#) 章节详细介绍了此功能。

只有在终端与策略匹配并且匹配指定条件的情况下，才会同时触发这两项操作。如果条件匹配，但终端与配置文件策略不匹配，则不执行操作。

另请注意，也可能匹配策略中的多个规则，导致执行多项操作。例如，其可能匹配一条规则，使得 CF 值增加 10，并且在也匹配该策略的前提下，还与执行例外操作或执行网络扫描操作等另一个规则匹配。

配置自定义（用户定义）分析策略

- 步骤 1** 在此程序中，将使用之前配置的条件，为实验室 APC UPS 设备创建一个自定义分析策略。
- 步骤 2** 转至 Policy → Profiling。从右侧窗格菜单点击 Add。
- 步骤 3** 输入配置文件名称 APC-UPS。
- 步骤 4** 输入说明 **Custom profile for APC UPS Network Management module**。与 APC 自定义条件的说明相似，可以通过使用关键字 **Custom**，根据此字符串对所有用户定义策略进行简单过滤。
- 步骤 5** 使 Minimum Certainty Factor 保留默认值 10。
- 步骤 6** 选择单选按钮 Use Hierarchy，而不要选择默认设置 Create Matching Identity Group。
- 步骤 7** 在 Rules 下，点击 Condition 旁边的 + 符号，然后选择 Select Existing Condition from Library。
- 步骤 8** 在 Condition Name → Select Condition 下，选择 APC-OUICheck。

注：也可以首先创建 Profiling Condition，然后在单独任务中创建 Profiling Condition，而且还可以使用选项 Create New Condition (Advanced Option) 从 Profiling Policy 本身内创建新条件。创建之后，新条件在策略规则中将显示为已命名条件。

- 步骤 9** 保留默认规则操作 Certainty Value Increases，其值为 10（图 80）。

图 78. 用户定义的分析策略示例

Profiler Policy List > APC-UPS

Profiler Policy

* Name: APC-UPS Description: Custom profile for APC UPS Network Management module

Policy Enabled:

* Minimum Certainty Factor: 10 (Valid Range 1 to 65535)

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

Create Matching Identity Group
 Use Hierarchy

* Parent Policy: NONE

Rules

If Condition: APC-OUICheck Then: Certainty Factor Increases 10

步骤 10 点击 Submit，保存更改。

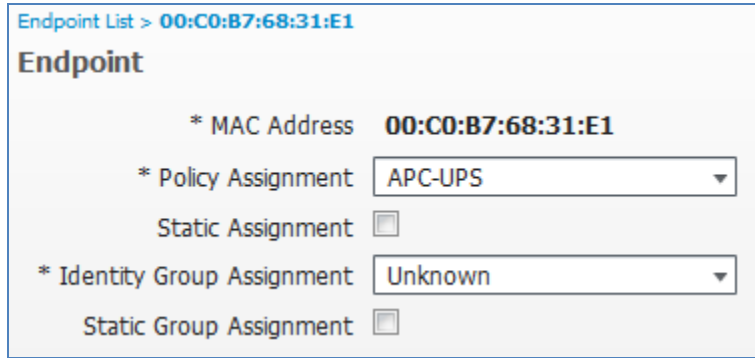
步骤 11 转至 Administration → Identity Management → Identities 并从左侧窗格选择 Endpoints。如图 81 所示，在列表中 APC 设备应不再显示为 Unknown，而是显示新匹配的分析策略分配。

图 79. 使用用户定义配置文件的终端的示例

Endpoints			
Edit Add Delete Import Export			
	Endpoint Profile	MAC Address	Static Assignment
<input type="checkbox"/>	APC-UPS	00:C0:B7:68:31:E1	false
<input type="checkbox"/>	APC-UPS	00:C0:B7:65:1F:BC	false

步骤 12 点击列表中一个终端的 APC-UPS（图 82）。

图 80. 使用用户定义的配置文件的终端详细信息示例



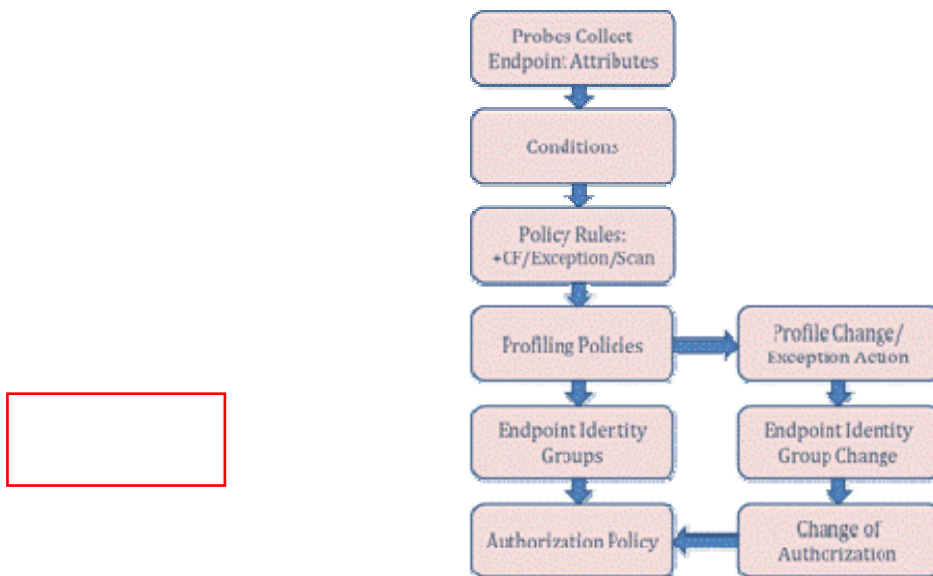
请注意，Policy Assignment 为 APC-UPS，但是 Identity Group Assignment 设置为 Unknown。这是在配置文件中将默认设置从 Create Matching Identity Group 改为 User Hierarchy 的决策导致的。我们故意选择了此选项，以便说明 Profiling Policy 和 Endpoint Identity Groups 之间的关系。

终端身份组

对于网络和安全管理员而言，设备分析是更好地了解哪些类型的设备正在连接网络的一个宝贵工具。除了获得可视性之外，为了根据终端的设备分类或分析策略分配制定授权策略决策，需要将配置文件与终端身份组关联。ISE 授权策略目前不接受以原始分析属性或策略分配作为条件，但是可以创建映射至分析策略分配的终端身份组。这样，授权策略就可以间接将终端的分析策略分配引用为规则条件。

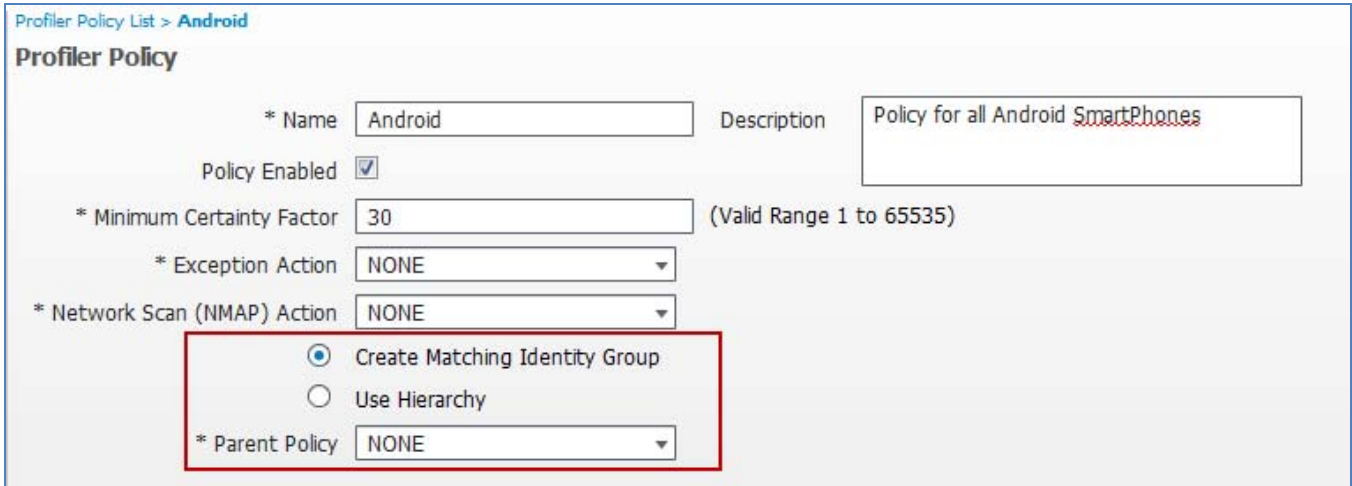
图 83 显示的是终端身份组的配置流程。

图 81. 配置流程：终端身份组



要将一个分析策略映射到终端身份组，请在如图 84 所示的配置文件中选择单选按钮 Create Matching Identity Group。

图 82. 分析策略 - 创建匹配的身份组示例

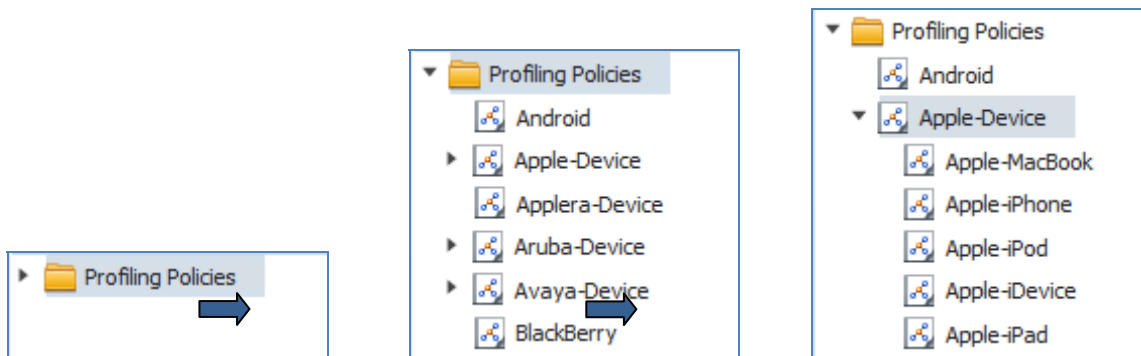


选择 Create Matching Identity Group 选项意味着手动排除大多数预置配置文件的默认选择 Use Hierarchy 设置。在图 84 中的 Android 策略示例中，默认设置已改为根据策略名称创建终端身份组。用户定义的配置文件的默认设置是创建匹配的身份组。

分析策略层次结构

匹配分析策略的最后一个标准是终端达到父策略的最低 CF 值。本部分介绍分析策略中的层次结构这一主题。在 Android 配置文件中，Parent Policy 设置为 NONE，但与之不同的是，如图 84 所示，Apple-iPad 和 Apple-iPhone 等配置文件为子配置文件，其父配置文件为 Apple-Device。要查看策略层次结构，请导航至 Policy → Profiling。从左侧窗格展开 Profiling Policies，方法是点击标签前面的向右箭头符号 (▶)。这样将显示所有第一级策略（图 85）。

图 83. 分析策略层次结构



具体条目前面的向右箭头表示那些配置文件存在子策略。根据上图，Android 策略没有子级，而 Apple-Device 为父策略。点击该箭头可显示 Apple 设备的子策略。

层次结构在组织策略的显示和管理方面很有用。它还提供一种为多个子策略定义一组共同条件的方法，这样匹配的子策略就意味着父级的一个匹配项，而无需重复在更细化的规则下定义那些高级条件。

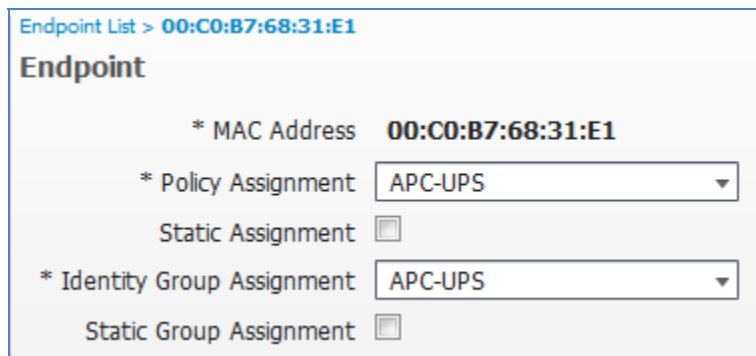
层次结构一般用于匹配 OUI。例如，所有 Apple 设备都有一个等于 Apple 的 OUI。因此，不必为 iPad、iPod、iPhone 等重复此条件。要与 Apple-iPhone 配置文件匹配，就要求该终端也有一个 Apple OUI。这就是为什么使用名称为 User Agent Switch 的简单 Firefox 浏览器插件（其将单独模拟其他浏览器 **User-Agent** 字符串）将不会达到 Apple iPhone 的配置文件条件的原因。没有 Apple MAC 地址，父条件无法通过测试。如本指南前文所述，分析并不是一种防监听解决方案，但是此解决方案的有些功能确实可以自然地消除某些监听活动。

层次结构也有利于简化身份组分配的匹配。如果父策略映射至身份组，则不必将所有子策略都映射至身份组。例如，对于思科 IP 电话就有很多预置配置文件。通过为思科 IP 电话（默认设置）创建匹配的身份组，可以根据其父级创建授权策略，而无需为每个子策略逐一创建身份组。这可以大幅简化授权策略规则。除非具体型号的 IP 电话要求特殊处理，否则都可以通过引用父配置文件和身份组分配统一处理。

为分析策略创建匹配的身份组

- 步骤 1** 在本程序中，为用户定义的配置文件策略创建了一个名称为 **APC-UPS** 的身份组。
- 步骤 2** 转至 Policy → Profiling 并从配置文件列表选择 APC-UPS。
- 步骤 3** 选择选项 Create Matching Identity Group，然后点击 Save，提交更改。
- 步骤 4** 返回 Administration → Identity Management → Identities → Endpoints 下的 Internal Endpoints 列表，再从已分配至 APC-UPS 配置文件的终端中选择一个终端（图 86）。

图 84. 用户定义的配置文件的终端身份组示例

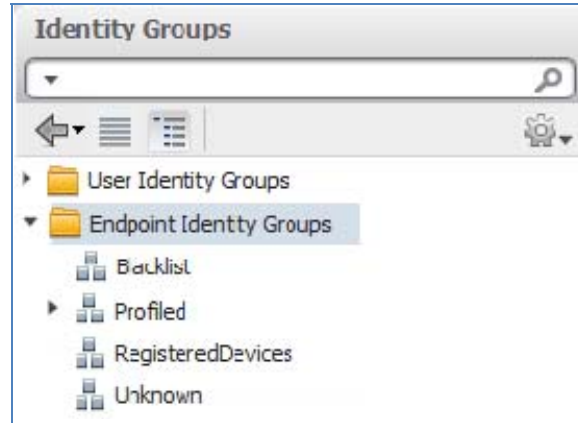


Endpoint List > 00:C0:B7:68:31:E1	
Endpoint	
* MAC Address	00:C0:B7:68:31:E1
* Policy Assignment	APC-UPS
Static Assignment	<input type="checkbox"/>
* Identity Group Assignment	APC-UPS
Static Group Assignment	<input type="checkbox"/>

注：Identity Group Assignment 已从 Unknown 改为 APC-UPS。

- 步骤 5** 转至 Administration → Identity Management → Groups，然后在左侧窗格中点击 Endpoint Identity Groups 左边的箭头(▶)，展开其内容，如图 87 所示。

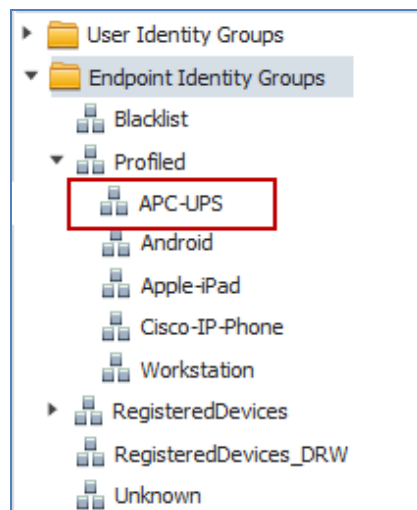
图 85. 查看终端身份组示例 1



步骤 6 此列表显示的是默认顶级身份组名称。默认情况下，分配至**没有**匹配身份组的分析策略的所有终端都会成为 **Unknown** 身份组的成员。分配至具有匹配身份组的分析策略的所有终端都会在父身份组 **Profiled** 下显示为该身份组的成员。**Blacklist** 和 **RegisteredDevices** 组是特殊组。**Blacklist** 用于识别被拒绝接入网络的终端。**RegisteredDevices** 由 MyDevicesPortal 和 Native Supplicant Provisioning 用于指定网络接入用户注册的终端。

步骤 7 点击 **Profiled** 左侧的 ▶ 即可展开其内容（图 88）：

图 86. 查看终端身份组示例 2

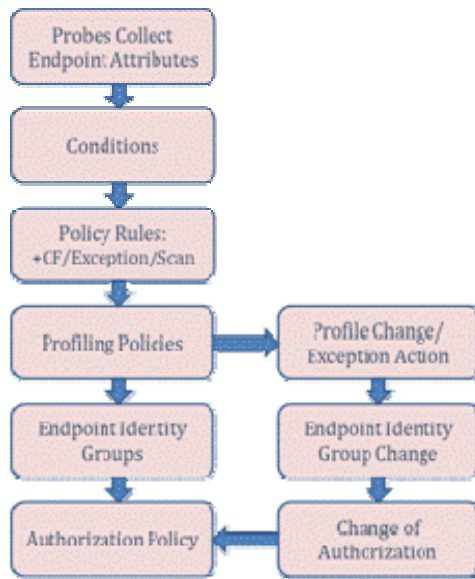


步骤 8 请注意，默认情况下，有些分析策略拥有匹配的身份组，包括 Cisco-IP-Phone 和 Workstation。APC-UPS 也出现在 Endpoint Identity Groups 列表下，现在可以将其选择作为授权策略规则中的一个匹配条件。

分析和授权策略

授权策略根据匹配的规则为连接至网络的终端定义访问权限。授权策略规则指定在分配特定权限之前终端必须满足的条件。要根据分析向终端分配策略，则终端必须分配给具有匹配的身份组的分析策略。图 89 显示的是授权策略的配置流程。

图 87. 配置流程：授权策略



使用 ISE 分析服务给设备分类并将其分配给身份组，可以使 ISE 向使用 MAB 的打印机或 IP 电话等非身份验证终端应用不同的策略，或在使用 iPad 等个人设备而非公司工作站进行连接时向通过身份验证的员工应用不同的策略（图 90）。

图 88. 授权策略示例

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Employee_Personal_Device	if Android OR Apple-iPad AND Employee	then Guest
✓	Employee_Corp_Device	if Workstation AND Employee	then Employee

步骤 1 如示例授权策略中所示，名称为 Cisco-IP-Phone 的身份组用于向被分析为思科 IP 电话的终端分配特殊电话授权。这些终端都使用 MAB 进行身份验证。使用分层策略还允许此策略应用于任意思科 IP 电话，而无论配置文件与特定 IP 电话型号的匹配情况。

步骤 2 授权策略还突出使用分析功能向使用个人设备（那些分类为 Apple-iPad 或 Android 的设备）进行连接的员工唯一授予“仅互联网访问权限”，同时通过工作站连接的员工则获得完全访问权限（员工权限）。

在授权策略中使用终端身份组

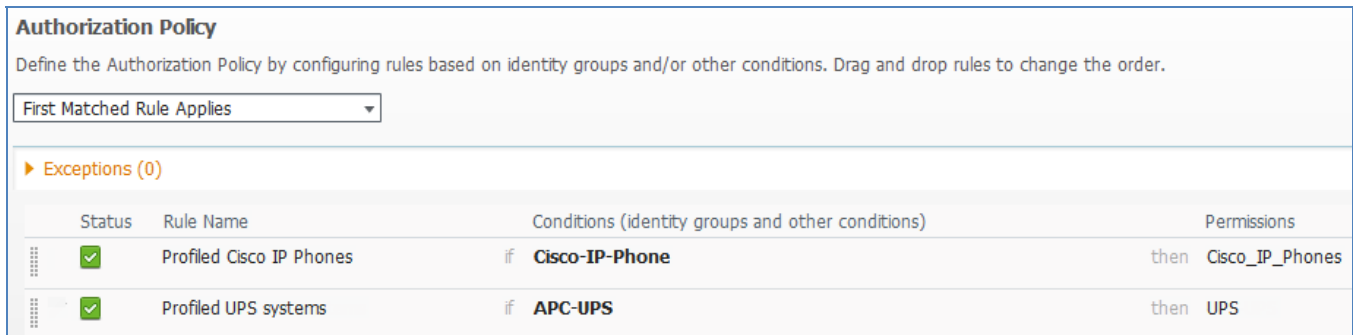
步骤 1 在本程序中，被分析为 APC UPS 设备的终端将根据 MAB 身份验证和授权策略规则与名称为 APC-UPS 的身份组的匹配，获得特殊权限。

步骤 2 转至 Policy → Authorization 并在 Profiled Cisco IP Phones 规则下插入名称为 Profiled UPS Systems 的新规则。

步骤 3 在身份组情况下，导航到 Endpoint Identity Groups → Profiled，选择 APC-UPS。

步骤 4 在 Permissions，选择 UPS 等相应的授权配置文件，然后点击 Save，提交更改。策略规则看起来应类似于图 91。

图 99. 授权策略配置示例 1



Authorization Policy
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

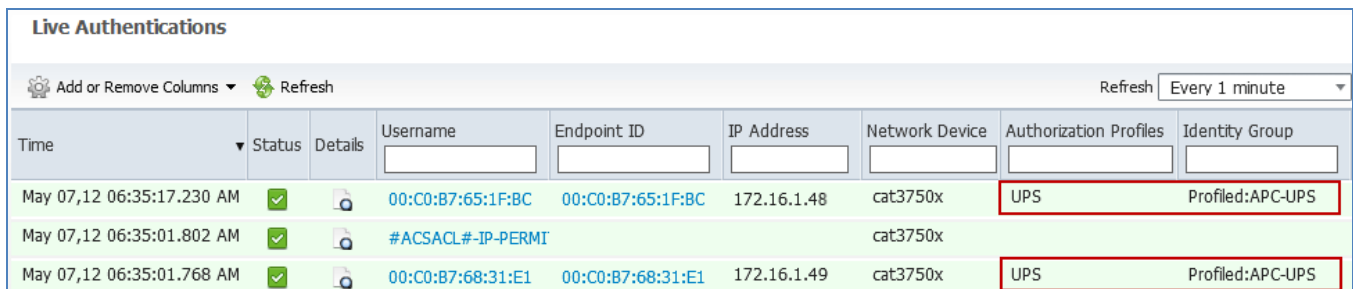
▶ Exceptions (0)

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Profiled UPS systems	if APC-UPS	then UPS

步骤 5 通过断开并重新连接 UPS 设备连接，或只需通过在相应接口下发出 **shut / no shut** 命令重置连接的交换端口，验证授权策略是否正常运行。

步骤 6 转至 Operations → Authentications，查看 Live Authentications 日志。所显示的条目应该类似于下图 92 中所示的那些条目。

图 90. 授权策略配置示例 2



Live Authentications

Add or Remove Columns Refresh Refresh Every 1 minute

Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Authorization Profiles	Identity Group
May 07,12 06:35:17.230 AM	✓		00:C0:B7:65:1F:BC	00:C0:B7:65:1F:BC	172.16.1.48	cat3750x	UPS	Profiled:APC-UPS
May 07,12 06:35:01.802 AM	✓		#ACSACL#-IP-PERMI			cat3750x		
May 07,12 06:35:01.768 AM	✓		00:C0:B7:68:31:E1	00:C0:B7:68:31:E1	172.16.1.49	cat3750x	UPS	Profiled:APC-UPS

步骤 7 日志显示被分析为 APC-UPS 的两个终端正在使用名称 UPS 的授权配置文件进行身份验证和授权。在本例中，在第一个终端获得授权后会向交换机发送可下载的 ACL (dACL)。第二个终端重新使用已下载的 dACL，所以不会发送第二个 dACL。

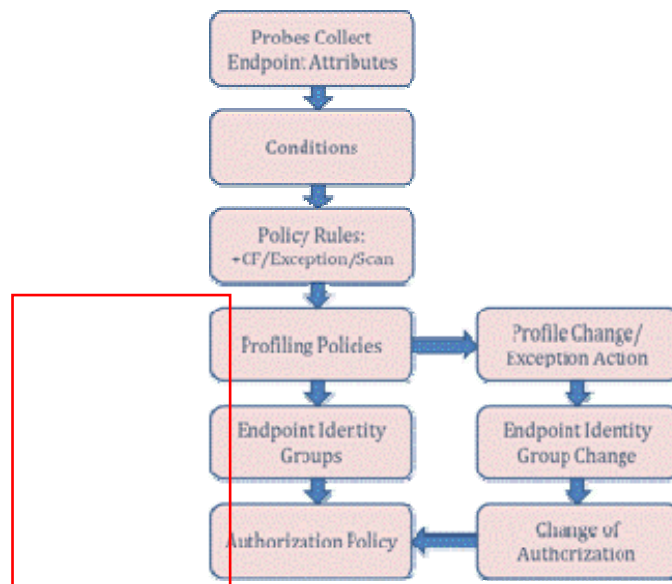
配置文件转变和授权更改

通过分析过程，终端可以从未知身份组转变为 Apple-Device 等更具体的配置文件。在有些情况下，其将直接转变为 Apple-iPad 等身份组，但是在从网络收集新配置文件数据的步骤中也可能会出现转变。虽然不常见，但是终端的“负面”分析数据有可能导致从更具体的配置文件转变为不那么具体的父配置文件或完全不同的配置文件。

无论配置文件转变的类型如何，在终端身份组分配中通常会有相关变更，其将在匹配的终端向网络进行身份验证时应用不同的授权策略规则。其所面临的挑战是如何为已经向网络接受身份验证和授权的终端施行新的授权。

图 93 显示配置文件转变和授权更改 (CoA) 的配置流程。

图 91. 配置流程：配置文件转变和 CoA



授权更改 (CoA)

CoA 是一种基于标准的 RADIUS 功能 (RFC 3576)，其在发生特定状态或策略变化时，允许 RADIUS 服务器 (ISE) 向网络接入设备 (RADIUS 客户端) 发起主动通信，为终端更新其访问策略。无需终端发起重新身份验证，即可实现这种更新。

在两种主要情况下 ISE 分析服务会触发 CoA：

配置文件转变触发例外操作。

配置文件转变导致基于授权策略规则的终端访问权限变更。

例外操作

默认情况下，有三种预定义的非可配置例外操作。转至 Policy → Policy Elements → Results → Profiling → Exception Action，查看列表（图 94）。

图 92. 例外操作

<input type="checkbox"/> Profiler Action Name ▲	Description
<input type="checkbox"/> EndpointDelete	When endpoint is deleted or reassigned to the unknown profile.
<input type="checkbox"/> FirstTimeProfile	When an endpoint profile changes from unknown to known for the first time.
<input type="checkbox"/> StaticAssignment	When an endpoint has connected to the network and is now statically assigned.

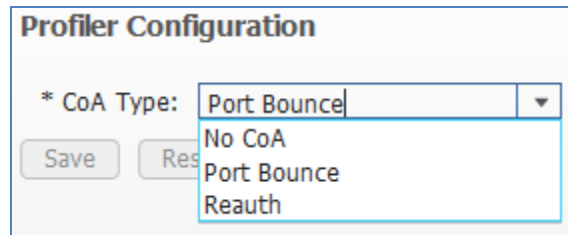
EndpointDelete 在终端被删除或从已分析配置文件转变为未知配置文件（无分析策略匹配项）时发送 CoA。

FirstTimeProfile 在终端从未知分析文件转变为具体的分析策略分配时生成 CoA。如果终端是在已知配置文件之间转变（例如从 Apple-Device 转变成 Apple-iPod），则此例外操作不会触发 CoA。

如果终端从动态配置文件分配静态分配至某个配置文件，则 **StaticAssignment** 会导致生成 CoA。分配至静态策略分配之后，就无法再分配新的终端分析策略，即使分析属性通常会指示可以转变。

对于各项例外操作，所发送的默认 CoA 类型在全局设置中在 **Administration → System → Settings → Profiling** 下进行配置（图 95）。

图 93. 全局分析器 CoA 配置



Profiler Configuration

* CoA Type: Port Bounce ▼

Save Res

No CoA
Port Bounce
Reauth

本指南中[配置全局分析设置](#)章节详细介绍了全局分析设置的配置。当通过同一交换端口连接多个会话时，Port Bounce 设置降低为 Reauth 设置，以最大程度地减少对其他会话的干扰。

系统定义的例外操作不可配置，且无法分配为分析策略下的操作。它们会根据所定义的转变自动触发。但是，管理员可以定义自定义例外操作。这些用户定义的例外操作可用于分析策略中，以应用静态分析策略分配和指定是否发送 CoA。

如果授权策略更改，自动在配置文件转变时发送 CoA

在思科 ISE 软件版本 1.1.1 之前，例外操作通常用于为配置文件内的转变（也就是从一个已知配置文件转变为另一个已知配置文件）强制实施 CoA，通常会对向分析策略静态分配终端产生不利负面影响。从 ISE 1.1.1 开始，只要配置文件转变导致依据授权策略规则更改终端访问权限，ISE 策略服务节点就会发送 CoA。其判定逻辑以终端身份组的变更为基础，其中此身份组用于授权策略规则中。此增强功能消除了使用例外操作处理为配置文件内转变发送 CoA 的要求。此外，它还允许终端维护动态配置文件分配，从而允许根据分析属性和策略配置进行额外转变。

用户定义的例外操作适用于在满足特定条件之后向首选策略分配静态分配终端，也可用于防止在策略分配时发送 CoA。一个使用情况示例是制造工厂过程控制终端等关键网络设备或医疗机构的联网医疗设备。在这些示例中，管理员可能希望向策略和关联身份组静态分配终端。通过例外操作执行的静态分配可以预防伪造的配置文件数据和终端配置文件影响其网络连接的风险。

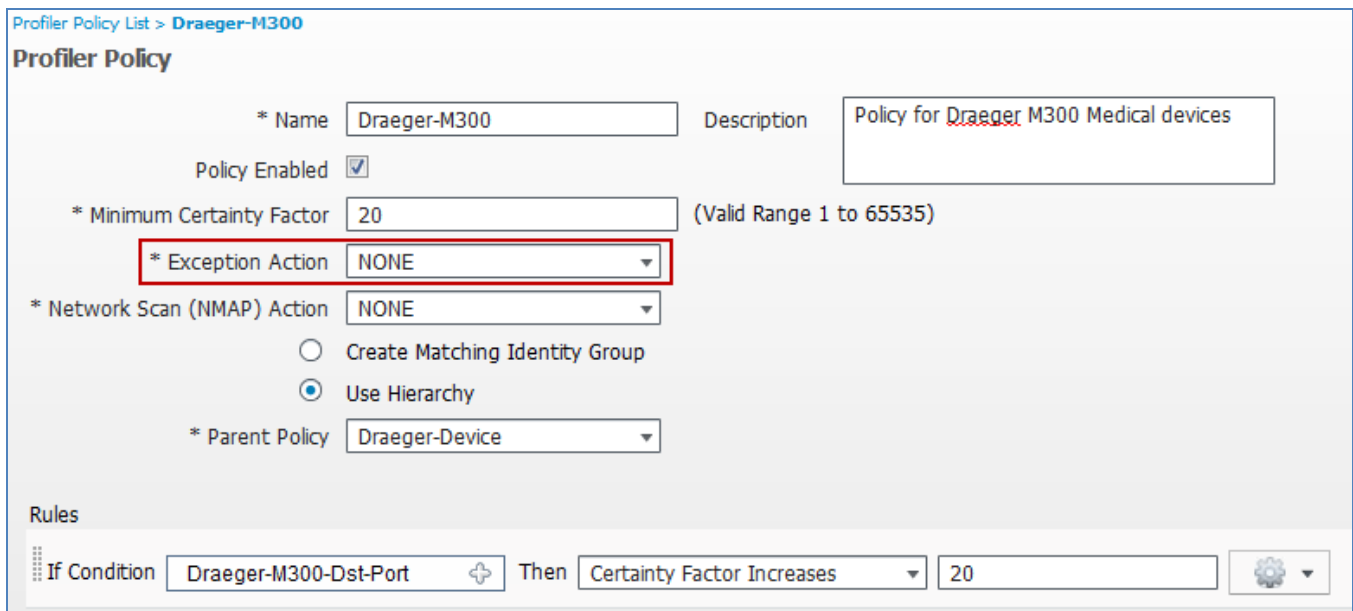
配置自定义（用户定义）例外操作

步骤 1 在本程序中，为某医疗设备配置了一个例外操作，从而在符合指定条件时，将其分配给静态分析策略。示例设备为 Draeger M300，一种便携式无线心脏监护器。

注意： 由于医疗保健解决方案所涉及的固有合规性因素，此示例的目的是严格阐明自定义例外操作的使用情况，而不是验证 ISE 分析服务用作保护医疗设备网络访问安全的方法的恰当性。

步骤 2 转至 Policy → Profiling 并从列表选择 Draeger-M300。默认情况下，此配置文件不包括引用例外操作的规则。此外，尚未定义例外操作（图 96）。

图 94. Draeger-M300 分析策略示例



Profiler Policy List > Draeger-M300

Profiler Policy

* Name: Draeger-M300 Description: Policy for Draeger M300 Medical devices

Policy Enabled:

* Minimum Certainty Factor: 20 (Valid Range 1 to 65535)

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

Create Matching Identity Group

Use Hierarchy

* Parent Policy: Draeger-Device

Rules

If Condition: Draeger-M300-Dst-Port Then: Certainty Factor Increases 20

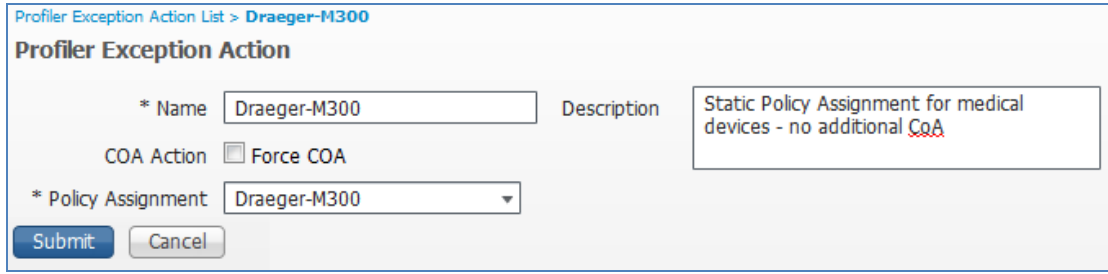
步骤 3 添加新的例外操作。

步骤 4 转至 Policy → Policy Elements → Results 并在左侧窗格的 Profiling 左侧点击箭头 (▶)，展开其内容。

步骤 5 从左侧窗格选择 Exception Actions，然后从右侧窗格菜单中点击 Add。

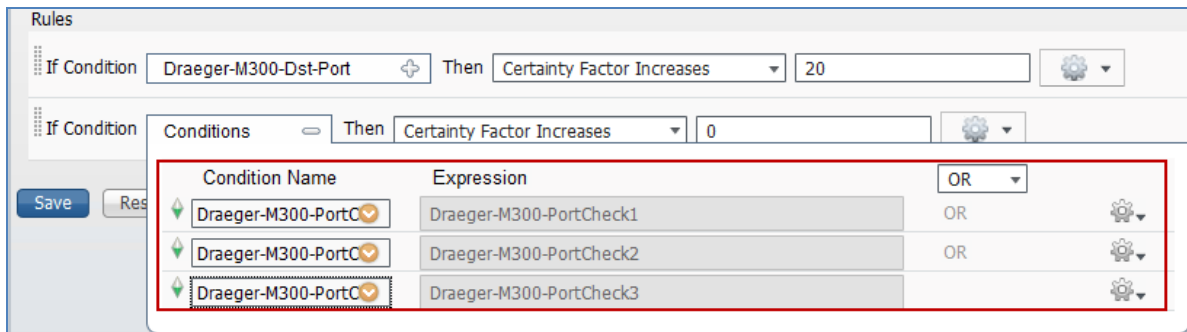
步骤 6 即已使用图 97 中所示的值添加新的例外操作。

图 95. 用户定义的例外操作示例



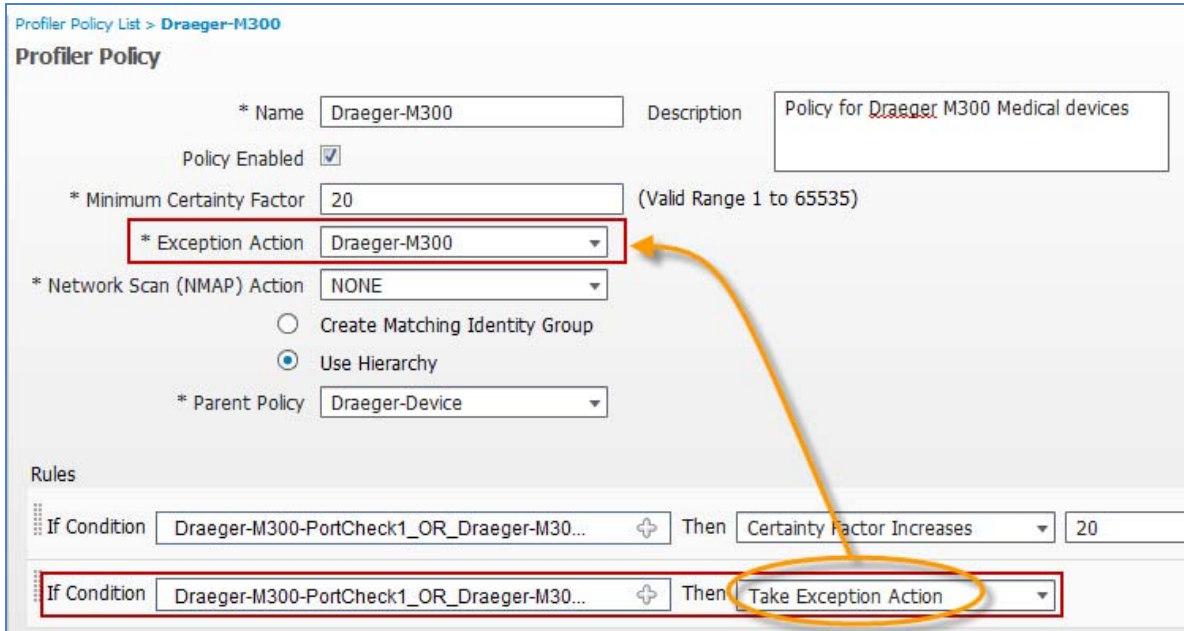
- 步骤 7** 在本例中，向配置文件 Draeger-M300 进行静态策略分析时不会发送附加 CoA。这是与之前显示相同的配置文件。
- 步骤 8** 在 Policy → Profiling 下返回 Draeger-M300 Profiling Policy，完成以下步骤，为配置文件定义例外操作：
- 步骤 9** 将 Exception Action 设置为 Draeger-M300。
- 步骤 10** 利用与用于匹配配置文件的现有规则完全一样的条件，创建一个新规则（图 98）。

图 96. 使用用户定义的例外操作的分析策略规则示例 1



- 步骤 11** 将操作 (Then) 从默认值 Certainty Factor Increases 改为 Take Exception Action。所生成的分析策略应看起来与图 99 所示的分析策略类似。

图 97. 使用用户定义的例外操作的分析策略规则示例 2



步骤 12 保存更改。

步骤 13 在此示例策略中，我们使用了与用于将策略分配给终端的相同条件，从而也静态地将终端分配至该策略。授权策略还可以利用名称为 **Draeger-Device** 的父策略具有匹配的身份组这一事实。否则，此策略可以分配一个身份组，其中授权策略将应用此具体配置文件。

步骤 14 将有线交换机配置为支持 CoA。如下所示，在全局配置模式下使用 **aaa server radius dynamic-author** 命令：

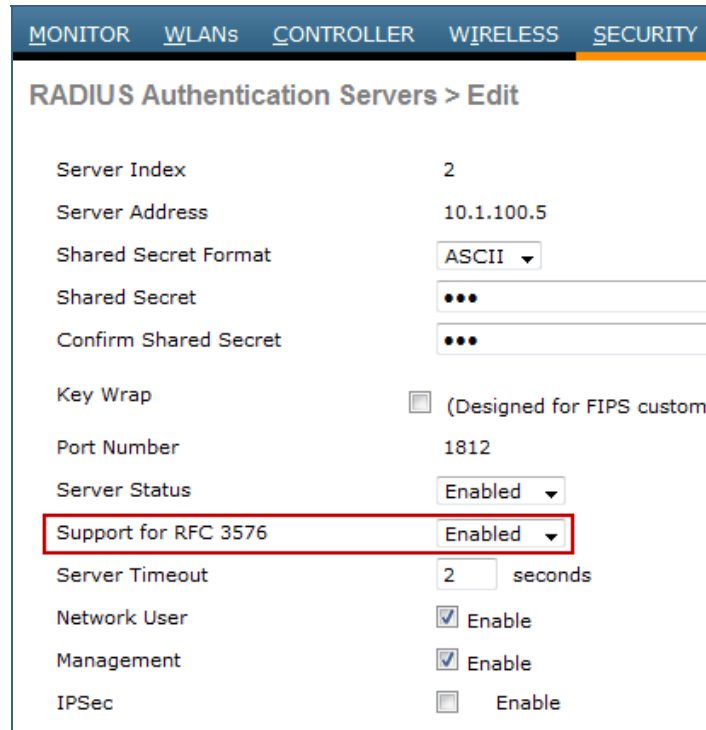
```
cat3750x(config)# aaa server radius dynamic-author
cat3750x(config-locsvr-da-radius)# client <ISE_PSN_IP_address> server-key <secret-key>
```

步骤 15 为要通过 RADIUS 与交换机通信的各个 ISE 策略服务节点添加一个单独的客户端条目。

步骤 16 将无线控制器配置为支持 CoA。

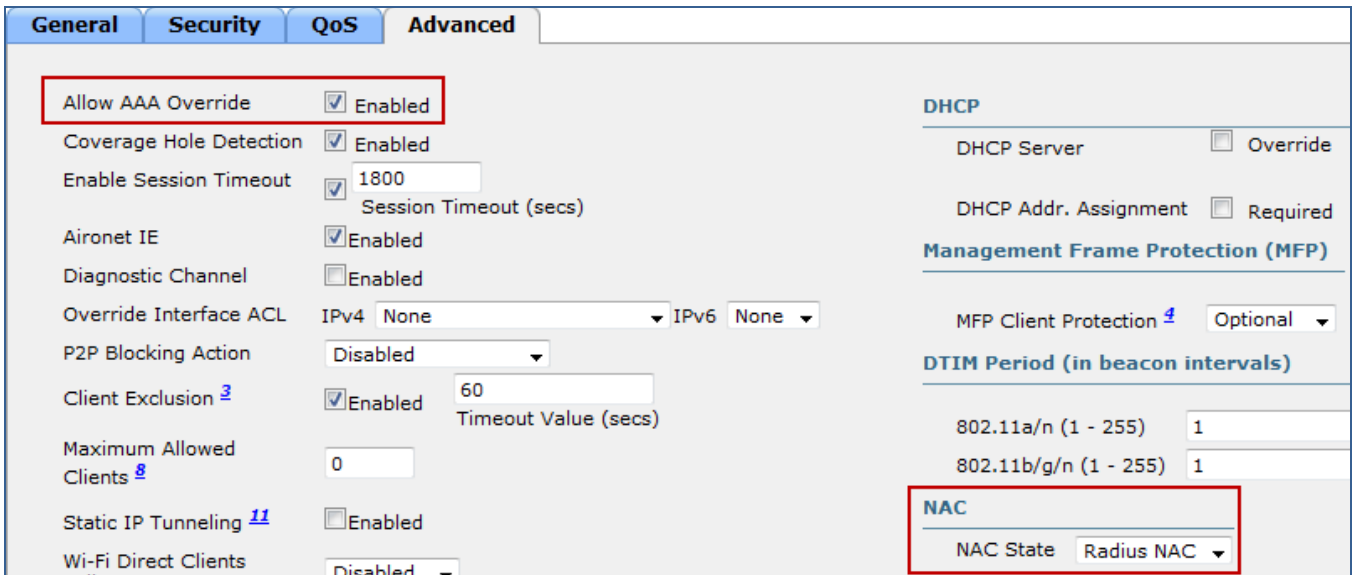
步骤 17 在 WLC web 管理接口下，转至 Security → AAA → RADIUS → Authentication。如图 100 所示，在 RADIUS 服务器定义下，确保启用对 RFC 3576 的支持。

图 98. 无线控制器的 CoA 配置示例 1



步骤 18 转至 WLANs → (WLAN) → Edit → Advanced。要使每个 WLAN 支持 CoA，请将 Allow AAA Override 设置为 Enabled 并且将 NAC State 设置为 RADIUS NAC，如图 101 所示。

图 99. 无线控制器的 CoA 配置示例 2



步骤 19 保存对每个平台的更改。

分析设计和最佳实践

本节介绍适用于各种部署和使用情况的一般分析设计以及最佳实践建议。

分析设计注意事项

当规划 ISE 分析要求时，首先必须了解需要分类的终端的类型，才能支持网络访问策略。例如，如果您知道很多特定类型的网络设备不支持 802.1X 或基于 Web 的身份验证，则很可能这些设备要求根据设备分类通过授权进行 MAB 身份验证。必须列出可能需要为网络访问进行分析的所有已知设备类型。

分析已知设备类型

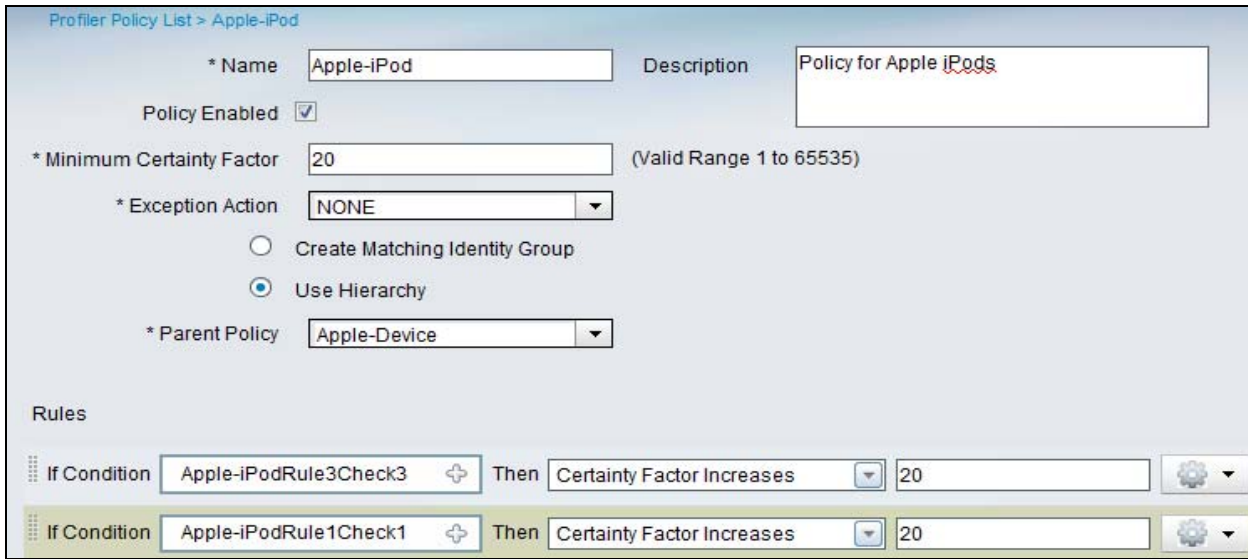
在 ISE 规划阶段，请确定需要进行设备分类的终端（根据配置文件属性进行授权）并确定分析这些终端所需的属性。如果已知要求授权的设备类型，接下来就要确定充分分析这些设备所需的属性和相关探测功能。

大多数常见终端在 ISE 配置文件库中都有预置的策略。通过查看这些默认 ISE 配置文件确定属性和探测功能要求。例如，了解配置文件 X 包含条件 A、B 和 C，您就可以推断出所需的属性和收集该数据所需的探测功能。如果配置文件库中没有特定匹配项，请参考相似类型的设备的配置文件。通常，类似类型的设备具有类似的分析要求。

如果无现有配置文件，可以临时启用探测功能以收集关于终端的属性。通常通过重置终端或断开然后重新连接网络，管理员可以捕获在正常启动时可用于设备的属性。ISE 中显示的属性通常会揭示可以给终端进行唯一分类的相关属性。某些设备可能需要执行数据包捕获等流量分析，从而确定用于 OUI、DHCP 选项、用户代理、TCP/UDP 端口或 DNS 命名的唯一属性。

以下示例（图 102）显示如何查找用于匹配 Apple iPod 配置文件的属性。可以看出该配置文件是基于 DHCP 属性或 **User-Agent**。因此，为了分析 Apple iPod，建议使用 DHCP 和 HTTP。

图 100. Apple-iPod 的分析条件示例



Profiler Policy List > Apple-iPod

* Name Description

Policy Enabled

* Minimum Certainty Factor (Valid Range 1 to 65535)

* Exception Action

Create Matching Identity Group

Use Hierarchy

* Parent Policy

Rules

If Condition Then

If Condition Then

查看配置文件库（在 Policy → Profiling 下）并且查看分析器条件（在 Policy → Policy Elements → Conditions → Profiling 下）（图 103），可以充分了解所使用的属性和分析那些终端或类似终端所需的探测功能。

图 101. 探测功能和分析器条件



已知关键分析属性之后，请从可用的探测功能中确定收集所需配置文件数据的最佳探测功能和其他收集方法。有关支持每个类型的探测功能的具体要求，请参阅关于 ISE 探测功能配置的各个章节。本节结尾处将提供有关探测功能选择最佳实践的其他建议。

分析未知设备类型

要分析的终端的列表可以包括网络打印机、传真机、电话、摄像头、存储设备，或任意数量支持 IP 的终端。有时候会已知关键设备的列表，例如在拥有大型 IP 电话部署的环境中。在其他情况下，可能会有各种未知主机，有必要首先发现这些终端。分阶段的 ISE 部署通常是最佳实践，首先从监控模式开始。这使得管理员可以了解连接至网络的终端的类型和在已将交换端口设置为强制模式的情况下可能已被拒绝访问网络的终端的类型。

无线接入没有“监控模式”，但是仍可将无线分析用于为使用 802.1X、Web 身份验证或 MAC 过滤功能的终端进行分类。从思科无线局域网控制器软件版本 7.0.116.0 开始，ISE 支持分析无线 802.1X 终端。从 WLC 版本 7.2.103.0 开始，ISE 支持分析使用 MAC 过滤的无线终端，包括使用集中 Web 身份验证进行身份验证的那些终端。这是因为这些 WLAN 身份验证方法都引入了 CoA 支持。

在 7.2.103.0 之前，仍可以分析无线客户端，但是 ISE 无法为配置文件转变应用 CoA。不过，它可以给终端分类并可选择将其分配给终端身份组以用于资产（可视性）用途。此外，终端重新连接无线网络时，可以根据当前身份组分配向终端应用授权策略。如果在活动会话期间检测到配置文件更改，则无法更改授权。

最佳实践： 确保如上图所示，将 Call Station ID Type 设置为 **System MAC Address** 以允许分析非 802.1X 客户端。这样可以确保 ISE 能够将终端添加到数据库中并根据已知 MAC 地址将所接收的其他配置文件数据与同一终端关联。

如果可能，请在部署的早期阶段部署 ISE 分析。ISE 可以分析有线终端，无需网络身份验证或授权即可开始执行发现过程。这样在可视性和了解尝试连接至网络的终端的类型方面，可以提供巨大的优势。在这些早期阶段，如果不确定需要为访问网络进行分析的特定终端类型，可以开始形成 ISE 分析策略。

访问策略和设备配置对分析的影响

根据所使用的 802.1X 部署模式（开放式身份验证与封闭模式）以及接入设备上配置的身份验证方法的顺序/优先级，分析结果有所不同。例如，如果端口处于封闭模式，在端口获得授权之前都无法发送 DHCP 数据包。如果没有发送某些流量，探测功能可能无法收集制定分析决策所需的数据。使用开放式身份验证（监控模式和低影响模式）可能允许某些流量在端口授权之前通过。在这任一种情况下都可以调整分析，但是必须明白具体部署模式对于收集属性的能力和时间的影响。

在灵活身份验证 (FlexAuth) 的情况下，身份验证方法的顺序也会影响收集属性的时间和在授权时分配的配置文件。例如，如果其顺序设置为首先执行 MAB 身份验证，在监控或低影响模式下执行 802.1X，则 ISE 可能无法获得充分的配置文件数据来在初始连接时分配所需的策略。当执行 MAB 查找时，终端可能仍处于未知或普通已分析身份组。如果其顺序设置为首先执行 802.1X，则在 802.1X 超时之前可以收集 DHCP 和其他分析属性。然后，可以根据在初始连接期间收集的其他属性，利用正确的配置文件，成功完成 MAB 查找。

注： 对终端的影响通常仅在于与网络的第一次连接。一旦终端已完全分析，ISE 可以使用其身份组分配来对后续与网络的重新连接进行即时策略匹配。

还应注意向端口初始应用的或在中间或最后授权阶段应用的全局访问策略。例如，当终端首次连接至网络时，可能会根据端口 ACL（假设是低影响模式）或初始 VLAN 获得访问权限。如果终端未知并且 MAB 查找失败或其安全状态未知，则可能会继续进行集中 Web 身份验证或进入安全状态，这会在端口上设置新的 ACL 或进行 VLAN 分配。Web 身份验证或修复成功之后，端口可能获得新的 ACL 或 VLAN。在每个状态下，将有不同级别的网络访问权限。如果分析要求收集某些数据，则必须授予该权限。

一个简单的例子是 DHCP。如果不启用 DHCP，则依赖来自 DHCP 探测功能的数据的分析可能会不可用。如果使用网络扫描，但是端口阻止访问 NMAP 探测功能查询的端口，则该信息也会不可用于制定分析决策。这包括对 SNMP 端口的访问，即使其在终端上已启用。此外，终端本身也必须允许该流量。常见示例是使用 NMAP 执行操作系统扫描。如果个人防火墙阻止尝试扫描终端，则探测功能不会生成任何结果。

NetFlow 探测功能的使用尤其具有挑战性，因为必须允许终端访问网络通信，才能收集 NetFlow 数据。因此，策略必须允许数据的初始收集，而无需获得任何终端的完全网络访问权限。一个可能的解决方案是在 VLAN A 中分析终端，VLAN A 禁止访问处于安全保护下的资源，但并不阻止对指定端口的一般访问。根据匹配的流量分析终端之后，可以向 VLAN B 重新授权终端，VLAN B 允许对处于安全保护下的资源进行特权访问。

还有一种方案是在一开始允许流量，但是在检测出异常流量之后，匹配更改端口授权的更具体配置文件。例如，如果某个过程控制终端与意外端口通信，则可以应用特例操作，将端口分配至隔离身份组和策略。再次申明，ISE 分析的目的并不是用作反监听解决方案，但是可以用于根据异常流量或其他分析属性强制执行策略。在包含关键设备的环境中，通常会锁定或将访问限制于已知的一系列终端。在这些情况下，分析的值可能是为了获得可视性，确保匹配特定分析策略的所有终端显示与那些设备类型一致的属性。

在需要执行静态策略分配的情况下，使用特例操作不失为一种方法。但是，请注意终端被静态分配至某个配置文件后，就只有管理员可以更改那种分配。

探测功能选择最佳实践

对于每种部署，可以使用不同的探测功能。本节重点介绍每个探测功能可以提供的信息并根据部署类型在探测功能选择过程方面提供指导。

探测功能属性

在确定在网络中启用哪些探测功能时，最好要了解每个探测功能可以收集哪些属性。表 8 总结了不同的探测功能所收集的关键属性以及合适的使用案例。

表 8. 探测功能和关键属性

探测功能	关键分析属性	常见终端分析使用案例
RADIUS	<ul style="list-style-type: none"> • MAC 地址 (OUI) • IP 地址 	MAC Address → OUI = 指示设备供应商。如果供应商只制造特定设备，则可以单独使用此属性分析某些终端。例如：第三方 IP 电话、移动设备、游戏控制台；MAC 至 IP 绑定和探测功能支持。
带设备传感器的 RADIUS	<ul style="list-style-type: none"> • CDP/LLDP • DHCP 	有关 CDP/LLDP 信息，请参阅 SNMP 探测功能。 有关 DHCP 信息，请参阅 DHCP 探测功能。
SNMP	<ul style="list-style-type: none"> • MAC 地址/OUI • CDP/LLDP • ARP 表 	对于使用 CDP/LLDP 的任何供应商非常有价值。例如，思科 IP 电话、摄像头、接入点、设备。 DHCP（参阅 DHCP 探测功能信息） MAC 地址（参阅 RADIUS 探测功能） 设备 ARP 表的轮询填充 ISE MAC 至 IP 绑定。
DHCP	<ul style="list-style-type: none"> • DHCP 	硬件和软件的唯一供应商 ID。操作系统检测的 DHCP 指纹。通用名称模式的主机名/FQDN 可能会指示操作系统或设备类型。额外提供 MAC 至 IP 绑定以支持其他探测功能。

NMAP	<ul style="list-style-type: none"> • 操作系统 • 通用端口 • 终端 SNMP 数据 	<p>如果网络/客户端固件不阻止扫描，则执行操作系统检测。</p> <p>对运行网络打印机之类 SNMP 代理的终端提供分类。</p> <p>适用于检测侦听通用 UDP/TCP 端口的终端。</p>
DNS	<ul style="list-style-type: none"> • FQDN 	<p>值取决于主机名/DNS 是否使用通用命名约定。</p>
HTTP	<ul style="list-style-type: none"> • User-Agent 	<p>操作系统检测；Chrome 等有些浏览器可能会掩饰实际操作系统。</p>
NetFlow	<ul style="list-style-type: none"> • 协议 • 源/目标 IP • 源/目标/端口 	<p>适用于检测使用唯一流量模式或使用通用硬件/软件的任务特定端口。</p> <p>可以检测特定终端的异常流量。</p>

表 9 提供了每个探测功能更详细的关键属性列表。每个探测功能可能还可以提供其他属性，但是以下列表突出强调对于典型部署最常用或最有用的属性。

表 9. 探测功能和分析属性详细信息

探测功能	关键分析属性
RADIUS	<ul style="list-style-type: none"> • Calling-Station-ID (OUI) • Framed-IP-Address
带设备传感器的 RADIUS	<ul style="list-style-type: none"> • cdpCachePlatform • cdpCacheAddress • cdpCacheCapabilities • lldpSystemDescription • lldpSystemName • dhcp-requested-address • dhcp-class-identifier • dhcp-client-identifier • dhcp-parameter-request-list • host-name • domain-name • client-fqdn

SNMP 查询	<ul style="list-style-type: none"> • MACAddress(OUI) • MAC-IP (ARP) • cdpCachePlatform • cdpCacheAddress • cdpCacheCapabilities • lldpSystemDescription • lldpSystemName
DHCP	<ul style="list-style-type: none"> • dhcp-requested-address • dhcp-class-identifier • dhcp-client-identifier • dhcp-parameter-request-list • host-name • domain-name • client-fqdn
NMAP	<ul style="list-style-type: none"> • operating-system • tcp-x • udp-x • SNMP 属性
DNS	<ul style="list-style-type: none"> • FQDN
HTTP	<ul style="list-style-type: none"> • User-Agent
NetFlow	<ul style="list-style-type: none"> • IPV4_DST_ADDR • IPV4_SRC_ADDR • PROTOCOL • L4_SRC_PORT • L4_DEST_PORT • MIN_TTL • MAX_TTL
其他	<ul style="list-style-type: none"> • PortalUser • EndPointSource • DeviceRegistrationStatus

探测功能选择的非官方指南

当您考虑为特定使用情况选择哪个探测功能时，根据回答以下问题的通用指标给各个探测功能评级可能会有帮助：

哪些探测功能部署起来最简单或最难？

哪些探测功能对我的网络影响最小或最大（在流量开销、ISE 服务器负载或支持的其他组件方面）？

此探测功能对于我分析我的终端的能力总体价值如何？

表 10 提供了对表 11、12 和 13 中使用的指标和评级的说明，帮助对不同使用情况进行探测功能选择。

表 10. 探测功能评级的说明

指标		评级		
名称	说明	1	2	3
DDI	部署难度系数	容易	中等	困难
NII	网络影响指数	低影响	中等影响	高影响
PVI	探测功能价值指数	高价值	中等价值	低价值

发现阶段 - 探测功能最佳实践

表 11 为 ISE 部署的发现阶段中探测功能的选择提供了最佳实践和指导。其假设尚需为 RADIUS 端口身份验证和授权配置网络接入设备。因此，RADIUS 探测功能等关键探测功能无法收集与网络身份验证相关的数据。

这些建议适用于没有启用 RADIUS 身份验证的其他部署情况，例如需要集成 ISE 分析服务的思科 NAC 设备安装情况。

表 11. 探测功能选择 - 发现阶段

探测功能（方法）	EDI	NII	PVI	关键分析属性	备注
RADIUS	-	-	-	• N/A	不适用，因为 ISE 不属于身份验证控制层面。
带设备传感器的 RADIUS	2	1	1	• CDP/LLDP • DHCP	如果网络支持设备传感器，无论身份验证控制层面如何，您都可以使用 RADIUS 记帐。
SNMPTrap	1	1	1	• LinkUp/Down 陷阱 • MAC 通知陷阱 • 告知	检测终端连接/触发 SNMP 查询探测功能。
SNMP 查询	1	2	1	• MAC 地址 (OUI) • CDP/LLDP • ARP 表	设备 ARP 表的轮询填充 ISE MA 至 IP 绑定。请注意，由于重新身份验证或临时更新，大量 RADIUS 记帐更新会触发高 SNMP 查询流量。
DHCP (帮助程序)	2	1	1	• DHCP	提供 MAC 至 IP 绑定。网络影响通常很低，但是请注意低 DHCP 租赁计时器。
DHCP SPAN	2	3	1	• DHCP	提供 MAC 至 IP 绑定。
NMAP	1	2	2	• 操作系统 • 通用端口 • 终端 SNMP 数据	SNMP 数据采取 UDP/161 开放和公共字符串。NMAP 的相对值取决于客户网络以及操作系统检测在有线访问策略中是否属于重要因素。
DNS	1	1	2	• FQDN	价值取决于是否使用通用命名约定。
HTTP (重定向)	-	-	-	• N/A	不适用，因为 ISE 不属于身份验证控制层面。
HTTP (SPAN)	2	3	2	• User-Agent	考虑使用智能 SPAN/分流器解决方案和/或 VACL 捕获的服务器或互联网边缘之类的关键 HTTP 阻塞点的 SPAN。
NetFlow	3	3	2	• 协议 • 源/目标 IP • 源/目标端口	仅建议用于特定使用情况，并非通用分析。

有线网络 - 探测功能最佳实践

表 12 为有线网络中部署的探测功能提供最佳实践建议和指导。

表 12. 探测功能选择 - 有线网络

探测功能（方法）	EDI	NII	PVI	关键分析属性	备注
RADIUS	1	1	1	<ul style="list-style-type: none"> MAC 地址 (OUI) IP 地址 用户名、其他 	用于设备检测和启用其他探测功能的基本探测功能。
带设备传感器的 RADIUS	2	1	1	<ul style="list-style-type: none"> CDP/LLDP DHCP 	如果运行具有设备传感器支持的 3000 或 4000 系列接入交换机，则此探测功能是收集选定属性的理想和优化方法。
SNMPTrap	1	1	3	<ul style="list-style-type: none"> LinkUp/Down 陷阱 MAC 通知陷阱 告知 	检测终端连接/触发 SNMP 查询探测功能。
SNMP 查询	1	2	1	<ul style="list-style-type: none"> MAC 地址 (OUI) CDP/LLDP ARP 表 	设备 ARP 表的轮询填充 ISE MAC 至 IP 绑定；注意，由于重新身份验证或临时更新，大量 RADIUS 计帐更新会触发高 SNMP 查询流量。
DHCP（帮助程序）	2	1	1	<ul style="list-style-type: none"> DHCP 属性 	提供 MAC 至 IP 绑定；注意低 DHCP 租赁计时器。
DHCP SPAN	2	3	1	<ul style="list-style-type: none"> DHCP 属性 	提供 MAC 至 IP 绑定。
NMAP	1	2	2	<ul style="list-style-type: none"> 操作系统 通用端口 终端 SNMP 数据 	SNMP 数据采取 UDP/161 开放和公共字符串。
DNS	1	1	2	<ul style="list-style-type: none"> FQDN 	价值取决于是否使用通用命名约定。
HTTP（重定向）	2	1	2	<ul style="list-style-type: none"> 用户代理 	值取决于操作系统对于有线接入的相对重要性。
HTTP (SPAN)	2	3	2	<ul style="list-style-type: none"> 用户代理 	考虑互联网边缘等关键 HTTP 阻塞点的 SPAN；如有可能，利用智能 SPAN 解决方案和 VACL 捕获。
NetFlow	3	3	2	<ul style="list-style-type: none"> 协议 源/目标 IP 源/目标端口 	仅建议用于特定使用情况，并非通用分析。

无线网络 - 探测功能最佳实践

表 13 为无线网络中部署的探测功能提供最佳实践建议和指导。

表 13. 探测功能选择 - 无线网络

探测功能（方法）	EDI	NII	PVI	关键分析属性	备注
RADIUS	1	1	1	<ul style="list-style-type: none"> MAC 地址 (OUI) IP 地址 用户名、其他 	用于设备检测和启用其他探测功能的基本探测功能。
带设备传感器的 RADIUS	2	1	1	<ul style="list-style-type: none"> CDP/LLDP DHCP 	如果运行具有设备传感器支持的 3000 或 4000 系列接入交换机，则此探测功能是收集选定属性的理想和优化方法。
SNMPTrap	1	1	3	<ul style="list-style-type: none"> LinkUp/Down 陷阱 MAC 通知陷阱 告知 	检测终端连接/触发 SNMP 查询探测功能。
SNMP 查询	1	2	1	<ul style="list-style-type: none"> MAC 地址 (OUI) CDP/LLDP ARP 表 	设备 ARP 表的轮询填充 ISE MAC 至 IP 绑定。请注意，由于重新身份验证或临时更新，大量 RADIUS 计帐更新会触发高 SNMP 查询流量。
DHCP（帮助程序）	2	1	1	<ul style="list-style-type: none"> DHCP 	提供 MAC 至 IP 绑定。注意低 DHCP 租赁计时器。
DHCP SPAN	2	3	1	<ul style="list-style-type: none"> DHCP 	提供 MAC 至 IP 绑定。
NMAP	1	2	2	<ul style="list-style-type: none"> 操作系统 通用端口 终端 SNMP 数据 	SNMP 数据采取 UDP/161 开放和公共字符串。
DNS	1	1	2	<ul style="list-style-type: none"> FQDN 	价值取决于是否使用通用命名约定。
HTTP（重定向）	2	1	2	<ul style="list-style-type: none"> 用户代理 	值取决于操作系统对于有线接入的相对重要性。
HTTP (SPAN)	2	3	2	<ul style="list-style-type: none"> 用户代理 	考虑互联网边缘等关键 HTTP 阻塞点的 SPAN；如有可能，使用智能 SPAN 解决方案和 VACL 捕获。
NetFlow	3	3	2	<ul style="list-style-type: none"> 协议 源/目标 IP 源/目标端口 	仅建议用于特定使用情况，并非通用分析。

分析计划

在检查因可视性或基于设备类型的网络访问而要求进行设备分类的不同类型终端并且就收集所需数据的最佳探测功能达成一致意见之后，下一步是制定分析计划。至少，此计划应包括要分析的所有设备，以及如何将分析数据用于授权网络访问。该计划还应包括给每个终端分类所要求的唯一属性、用于捕获这些属性的探测功能或方法，以及收集方法的具体信息。例如，是否使用 URL 重定向或 SPAN 来捕获 HTTP？在哪里捕获这些数据？哪些 PSN 将接收数据？该计划的另一个重要方面是如何部署可扩展性和冗余。

注：分析高可用性和可扩展性，包括负载均衡，不在本文档的讨论范围之内。

表 14 显示某示例公司的基本分析计划。

表 14. 示例分析计划

设备配置文件	在身份验证策略规则中什么地方使用？	唯一属性	使用的探测	收集方法
思科 IP 电话	思科 IP 电话 (MAB)	OUI	RADIUS	RADIUS 身份验证
		CDP	SNMP 查询	由 RADIUS 开始触发
IP 摄像机	思科 IP 摄像头 (MAB)	OUI	RADIUS	RADIUS 身份验证
		CDP	SNMP 查询	由 RADIUS 开始触发
打印机	打印机 (MAB)	OUI	RADIUS	RADIUS 身份验证
		DHCP 类标识符	DHCP	从本地第 3 层交换机 SVI 使用 IP 帮助程序
销售点 (PoS) 站点 (静态 IP)	POS (MAB)	MAC 地址	RADIUS (MAC 地址发现)	RADIUS 身份验证
		MAC 至 IP 映射的 ARP 缓存	SNMP 查询	由 RADIUS 开始触发
		DNS 名称	DNS	由 IP 发现触发
Apple iDevice	员工个人 (802.1X/CWA)	OUI	RADIUS	RADIUS 身份验证
		浏览器用户代理	HTTP	授权策略安全状态重定向至中心策略服务节点集群
		DHCP 类标识符和 MAC 至 IP 映射	DHCP	从本地第 3 层交换机 SVI 使用 IP 帮助程序

设备 X	关键设备 X (MAB)	MAC 地址	RADIUS (MAC 地址 发现)	RADIUS 身份验证
		MAC 至 IP 映射所要求的 IP 地址	DHCP	DHCP 服务器端口的 RSPAN 至本地策略服务节点
		可选，用于获取 MAC 至 IP 映射的 ARP 缓存	SNMP 查询	由 RADIUS 计帐开始触发
		流量至目标端口/IP	NetFlow	从 Distribution 6500 交换机至中心策略服务节点的 NetFlow 导出

分析最佳实践和建议总结

以下是对 ISE 分析的最佳实践建议的总结：

尽可能使用设备传感器以优化数据收集。

- 如果可能，请确保特定终端的配置文件数据发送至同一策略服务节点。否则，多个 PSN 可能导致终端数据大量更新。
- 在很多情况下，ISE 会自动处理此问题：
- SNMP 查询将由接收 RADIUS 计帐开始或 SNMP 陷阱数据包的相同 PSN 发出。
- URL 重定向导致的 HTTP 流量发送至处理 RADIUS 会话的 PSN。
- 可以向不止一个 PSN 发送 DHCP 帮助程序，因此建议发送至与为特定接入设备的 RADIUS 配置相同的 PSN。
- DNS 查询由收集 IP 地址的同一 PSN 发送。此 PSN 通常是处理 RADIUS 会话的那个 PSN，其来自 RADIUS 计帐的 Framed-IP-Address 或来自 DHCP 的 dhcp-requested-address 接收 IP 地址，或从 cdpCacheAddress 的已触发 SNMP 查询获取 IP 地址。
- 已触发的 NMAP 扫描由接收策略规则匹配中产生的分析数据的同一 PSN 收集。例如，如果根据 OUI 匹配向配置文件规则条件分配某个 NMAP 操作，则通过 RADIUS、DHCP 或其他探测功能接收终端 MAC 地址的第一个 PSN 将是收集 NMAP 扫描的那个 PSN。
- 在其他情况下，例如使用 DHCP SPAN、HTTP SPAN 或 NetFlow 的情况，无法始终确保流量到达分布式部署中的相同 PSN。

HTTP 探测功能：

- 使用 URL 重定向而不是 SPAN 集中收集并减少与 SPAN/RSPAN 相关的流量负载。
- 总之，尽量避免使用 HTTP SPAN 收集数据。如果使用：
- 查找关键流量阻塞点，例如互联网边缘或无线控制器连接。
- 使用智能 SPAN/分流器选项或 VACL 捕获限制向 IS 发送的数据量。
- 无智能网络分流器基础设施，可能难以为 SPAN 提供高可用性。

DHCP 探测功能:

- 尽可能使用 DHCP 中继（IP 帮助程序）。
- 总之，尽量避免使用 DHCP SPAN 收集数据。如果使用，请确保探测功能捕获流向中心 DHCP 服务器的流量。
- 请注意，服务 DHCP 的第 3 层设备不会为相同网络中继 DHCP。
- 无智能网络分流器基础设施，可能难以为 SPAN 提供高可用性。
- SNMP 探测功能:
- 注意由于高重新验证率（低会话/重新身份验证计时器）或频繁的临时计帐更新，所触发的 RADIUS 计帐更新会形成高 SNMP 流量。
- 对于轮询查询，注意不要将轮询间隔设置得太低。请确保为 ISE 网络设备配置中的轮询设置最优 PSN。
- SNMP 陷阱主要适用于与 NAC 设备集成之类的非 RADIUS 部署，而不适用于使用基于 RADIUS 的身份验证和授权的网络。
- NetFlow：仅适用于特定使用情况。NetFlow 在网络设备和 PSN 上具有产生高负载的可能性。

附录 A：参考

Cisco TrustSec 系统：

<http://www.cisco.com/go/trustsec>

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

设备配置指南：

思科身份服务引擎用户指南：

http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

有关思科 IOS 软件、思科 IOS XE 软件和思科 NX-OS 软件版本的更多信息，请参阅以下 URL：

对于 Cisco Catalyst 2900 系列交换机：

http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 3000 系列交换机：

http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 3000-X 系列交换机：

http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 4500 系列交换机：

http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 6500 系列交换机：

http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html

对于 Cisco ASR 1000 系列路由器：

http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

对于无线局域网控制器：

http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/wlc_cg70MR1.html