为CESA配置AnyConnect NVM和Splunk

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- Cisco AnyConnect安全移动客户端 — 多于VPN
- Internet协议流信息导出(IPFIX)
- IPFIX NVM收集器
- Splunk企业

部署概述

拓扑

配置

- 为DTLS支持配置NVM
  - 证书要求
  - AnyConnect配置（4.9.3043及更高版本）
- 独立AnyConnect NVM模块
- AnyConnect NVM客户端配置文件
  - 通过ASDM配置NVM客户端配置文件
  - 通过AnyConnect配置文件编辑器配置NVM客户端配置文件
- 在Cisco ASA上配置Web部署
- 在Cisco ISE上配置Web部署
- 可信网络检测

部署

- 步骤1.在Cisco ASA/ISE上配置AnyConnect NVM
- 步骤2.设置IPFIX收集器组件（AnyConnect NVM收集器）
  - 如何安装收集器
  - DTLS支持
- 步骤3.使用CESA控制面板和TA插件设置Splunk
  - Install（安装）
  - 通过Splunk管理UI启用UDP输入

验证

- 验证AnyConnect NVM安装
- 验证收集器状态
- 验证Splunk - CESA控制面板
- 数据包流
- 流模板

故障排除

- AnyConnect客户端（NVM模块）
  - 不向收集器报告数据，也不从终端发送数据包
  - 可信网络检测(TND)

AnyConnect诊断和报告工具(DART)
收集器(在Linux/Docker计算机上：一体化或独立)
acnvmcollector安装失败
acnvmcollector无法启动
收集器日志 — 在哪里可以设置调试？
如何查找收集器的版本号？
DTLS问题
Splunk控制台（CESA控制面板）不显示数据
AnyConnect Client
收集器盒
常见问题(FAQ)
如何将数据从AnyConnect NVM发送到多个目标？
在哪里存储AnyConnect NVM DTLS的证书？
XML文件名
收集器(AnyConnect NVM)
推荐版本
相关信息

简介

本文档介绍如何在运行AnyConnect 4.7.x或更高版本的最终用户系统上安装和配置Cisco AnyConnect网络可视性模块(NVM)，以及如何安装和配置关联的Splunk企业组件和NVM收集器。

先决条件

要求

Cisco 建议您了解以下主题：

- 带NVM的AnyConnect 4.7.x或更高版本
- AnyConnect许可
- 自适应安全设备管理器(ASDM)7.5.1或更高版本
- 熟悉Splunk Enterprise以及如何安装Splunk应用和加载项

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco AnyConnect安全移动客户端4.7.x或更高版本
- Cisco AnyConnect配置文件编辑器
- 思科自适应安全设备(ASA)，版本9.5.2
- 思科自适应安全设备管理器(ASDM)，版本7.5.1
- Splunk Enterprise 7.x或更高版本(作为一体式安装在任何支持的Linux平台上；首选CentOS)

- 任何受支持的Linux安装作为收集器设备

> 注意：收集器可以在同一台服务器上运行。有关详细信息，请参阅基于Splunk Quickstart POV套件和部署指南的思科终端安全分析(CESA)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Cisco AnyConnect NVM提供高价值终端遥感勘测的持续馈送，使组织能够查看其网络上的终端和用户行为。NVM从内部和外部终端以及重要环境（如用户、应用、设备、位置和目标）收集流量。Splunk Enterprise使用遥测数据，并提供分析功能和报告。

本技术说明是采用Splunk Enterprise的AnyConnect NVM的配置示例，该配置是新的思科终端安全分析(CESA)解决方案的一部分。

- 有关使用Splunk的CESA的完整概述价值验证(POV)，请参阅基于Splunk Quickstart POV套件和部署指南的思科终端安全分析(CESA)。
- 有关Splunk上CESA NVM控制面板的指南，请参阅思科终端安全分析(CESA)控制面板概述和常见问题解答。
- 有关解决方案的详细信息，请参阅基于Splunk的思科终端安全分析。

这些组件构成了解决方案：

- 启用网络可视性模块(NVM)的Cisco AnyConnect安全移动客户端
- 适用于Splunk的思科终端安全分析(CESA)应用
- 适用于Splunk的思科终端安全分析(CESA)插件
- NVM收集器（捆绑在包含NVM TA附加模块的zip文件中）

Cisco AnyConnect安全移动客户端 — 多于VPN

Cisco AnyConnect是一个统一代理，可提供多种安全服务来保护企业。AnyConnect最常用作企业VPN客户端，但它还支持其他模块，以满足企业安全性的不同方面。附加模块支持安全功能，如状态评估、网络安全、恶意软件防护、网络可视性等。

本技术说明涉及NVM，它与Cisco AnyConnect集成，使管理员能够监控终端应用使用情况。有关Cisco AnyConnect的详细信息，请参阅Cisco AnyConnect安全移动客户端管理员指南，版本4.7。

Internet协议流信息导出(IPFIX)

IPFIX是一种IETF协议，它定义了用于各种目的（例如记帐、审计和安全性）导出IP流信息的标准。IPFIX基于Cisco NetFlow协议v9，尽管它们不直接兼容。Cisco nvzFlow是基于IPFIX协议的协议规范。根据设计，IPFIX是一种可扩展的协议，允许您定义新的参数来传达信息。Cisco nvzFlow协议扩展了IPFIX标准并定义了新的信息元素。该协议还定义了一组标准IPFIX模板，这些模板作为AnyConnect NVM使用的遥测的一部分进行传送。

有关IPFIX的详细信息，请参阅以下RFC:

- rfc5101
- rfc7011
- rfc7012
- rfc7013
- rfc7014
- rfc7015

IPFIX NVM收集器

收集器是接收和存储IPFIX数据的服务器。然后，它可以将此数据提供给Splunk。

思科提供专为nvzFlow协议设计的收集器，该收集器与CESA TA Add-On for Splunk捆绑在一起。收集器可以与Splunk服务器安装在同一机箱上（一体化），也可以安装在重型转发器上，或者安装在独立的Linux机箱上。

有关收集器的更多详细信息，请参阅思科网络可视性(NVM)收集器。

Splunk企业

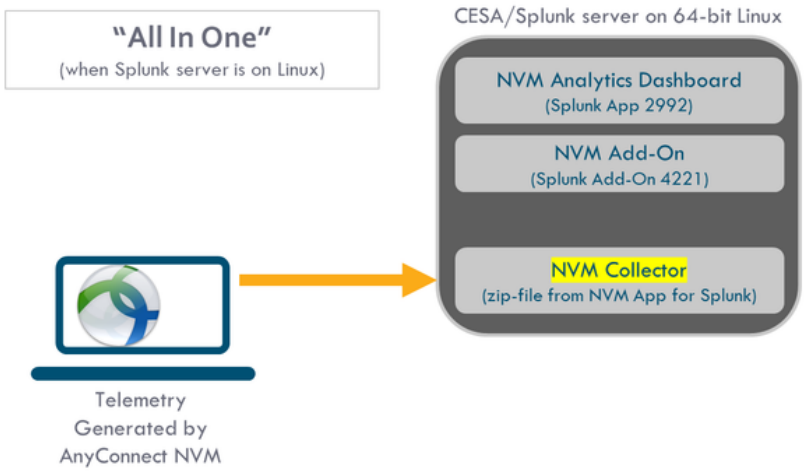
Splunk Enterprise是一个强大的工具，用于收集和分析诊断数据，从而提供有关IT基础架构的有用信息。它为管理员提供收集数据的一站式位置，帮助他们了解网络的运行状况。

Splunk是思科合作伙伴，CESA解决方案是与他们协作创建的。有关详细信息，请参阅基于Splunk的思科终端安全分析。

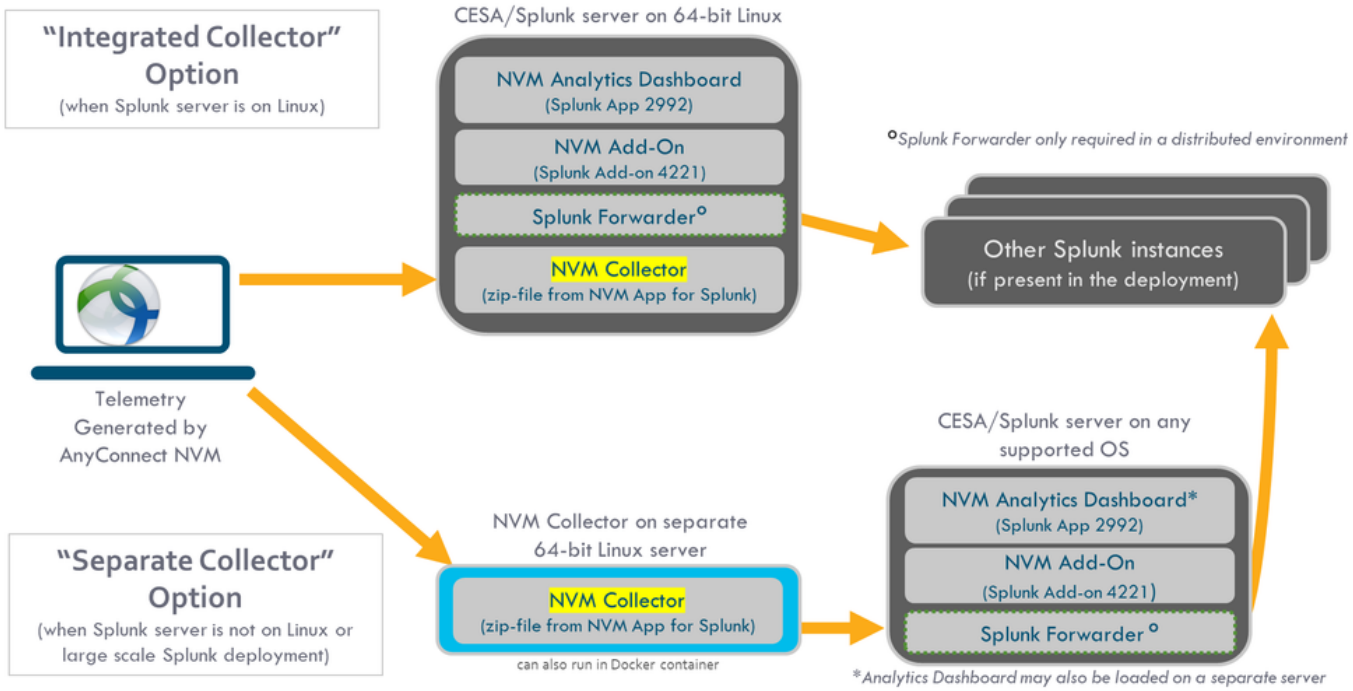
部署概述

本文档以最简单的形式简要介绍部署。这是在64位Linux上运行的一体化配置。

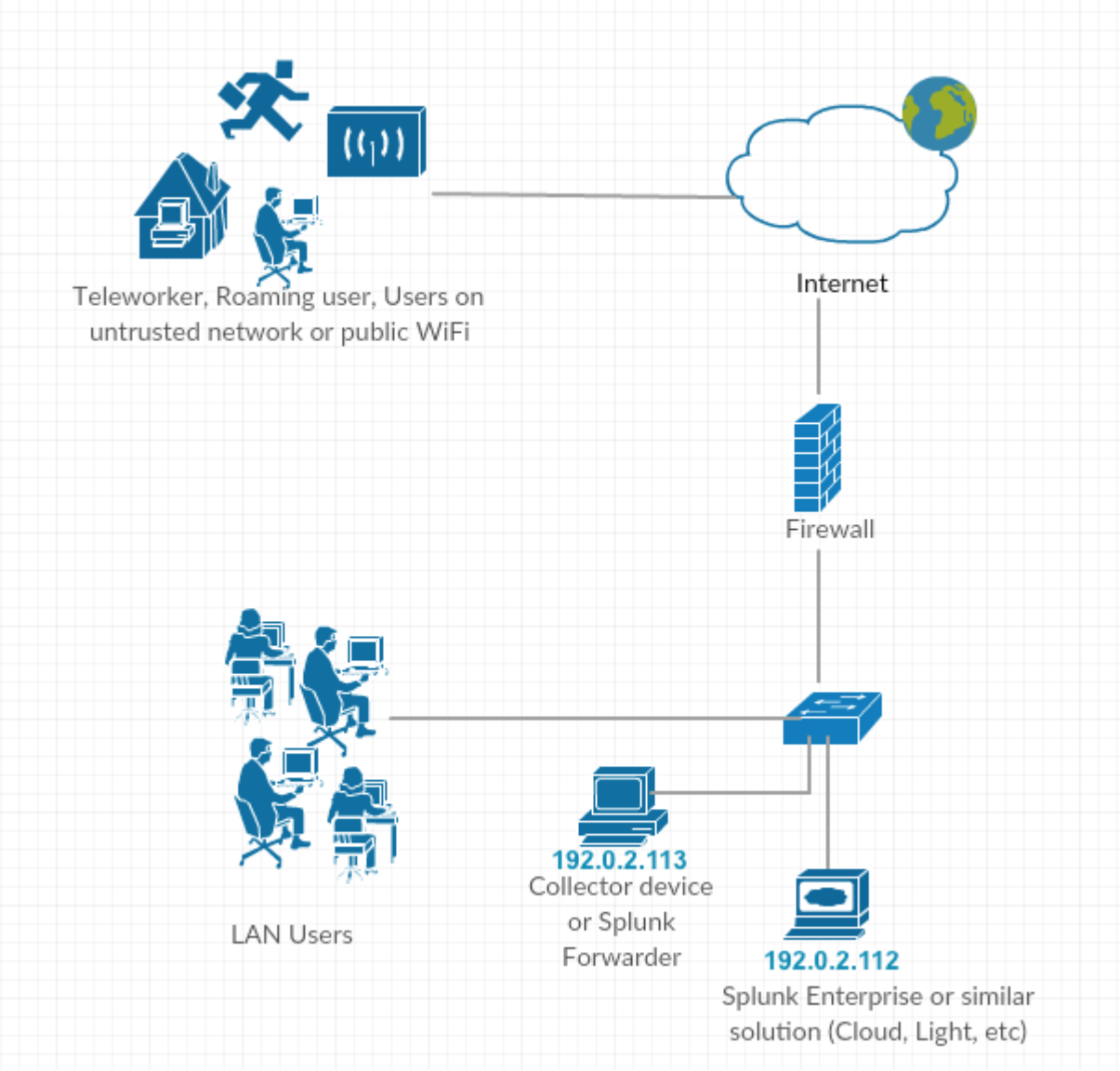
下图显示了用于大多数演示的配置。此配置在小型生产部署中也很有用。



下图显示一组更全面的选项，可用于部署。通常，生产设置是分布式的，并且有几个Splunk Enterprise节点。


"Integrated Collector" Option
(when Splunk server is on Linux)
CESA/Splunk server on 64-bit Linux
NVM Analytics Dashboard
(Splunk App 2992)
NVM Add-On
(Splunk Add-on 4221)
Splunk Forwarder°
NVM Collector
(zip-file from NVM App for Splunk)
°Splunk Forwarder only required in a distributed environment
Other Splunk instances
(if present in the deployment)
Telemetry Generated by AnyConnect NVM
"Separate Collector" Option
(when Splunk server is not on Linux or large scale Splunk deployment)
NVM Collector on separate 64-bit Linux server
NVM Collector
(zip-file from NVM App for Splunk)
can also run in Docker container
CESA/Splunk server on any supported OS
NVM Analytics Dashboard*
(Splunk App 2992)
NVM Add-On
(Splunk Add-on 4221)
Splunk Forwarder °
*Analytics Dashboard may also be loaded on a separate server

拓扑



本技术中的IP地址约定注意：

- 收集器IP地址：192.0.2.123
- Splunk IP地址：　192.0.2.113

配置

本节介绍思科NVM组件的配置。有关AnyConnect NVM部署和配置概要文件的概述，另请参阅如何实施AnyConnect网络可视性模块。

为DTLS支持配置NVM

现在，可以将NVM配置为通过DTLS将数据安全地发送到收集器。此模式可在NVM配置文件编辑器中配置。选中“安全”复选框时，NVM使用DTLS作为传输。要通过DTLS连接，终端必须信任DTLS服务器（收集器）证书。不可信的证书以静默方式被拒绝。DTLS 1.2是支持的最低版本。DTLS支持需要收集器作为CESA Splunk应用v3.1.2或更高版本的一部分。收集器只能在一个模式下工作：安全或不安全。

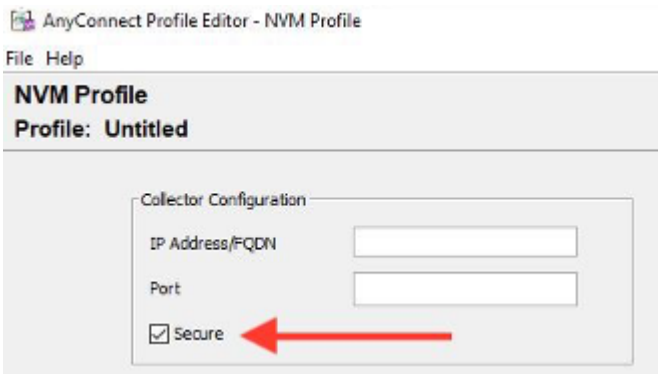
证书要求

- 收集器证书必须受客户端信任。（由于AnyConnect上没有配置，请确保证书链受信任。）
- 证书必须是PEM格式。
- 不支持证书密钥密码。注意：思科身份服务引擎(ISE)内部证书颁发机构(CA)需要一个。
- 只要AnyConnect客户端机器信任收集器(内部公钥基础设施(PKI)、众所周知等等)，就可以使用收集器上的任何证书。
- 更新配置文件后，AnyConnect NVM服务必须重新启动（用于单客户端测试）。 对于从ISE或自适应安全设备(ASA)推送的配置文件，客户端计算机必须断开与网络的连接，然后重新连接。

- AnyConnect NVM配置文件收集器配置应设置为IP或FQDN。此选择取决于证书的公用名(CN)中使用的值。如果IP地址更改，始终首选完全限定域名(FQDN)。
    - 如果使用IP地址，则收集器证书CN或主题备用名称(SAN)应具有该IP。
    - 如果您在证书中将FQDN作为CN，则NVM配置文件应与收集器具有相同的FQDN。

AnyConnect配置（4.9.3043及更高版本）

对于NVM配置文件，在收集器IP/端口下有一个名为“Secure”的新复选框。



独立AnyConnect NVM模块

独立模块需要AnyConnect 4.8.01090或更高版本。请参阅Cisco AnyConnect安全移动客户端管理员指南，版本4.9。另请参阅此独立指南：如何实施AnyConnect网络可视性模块。

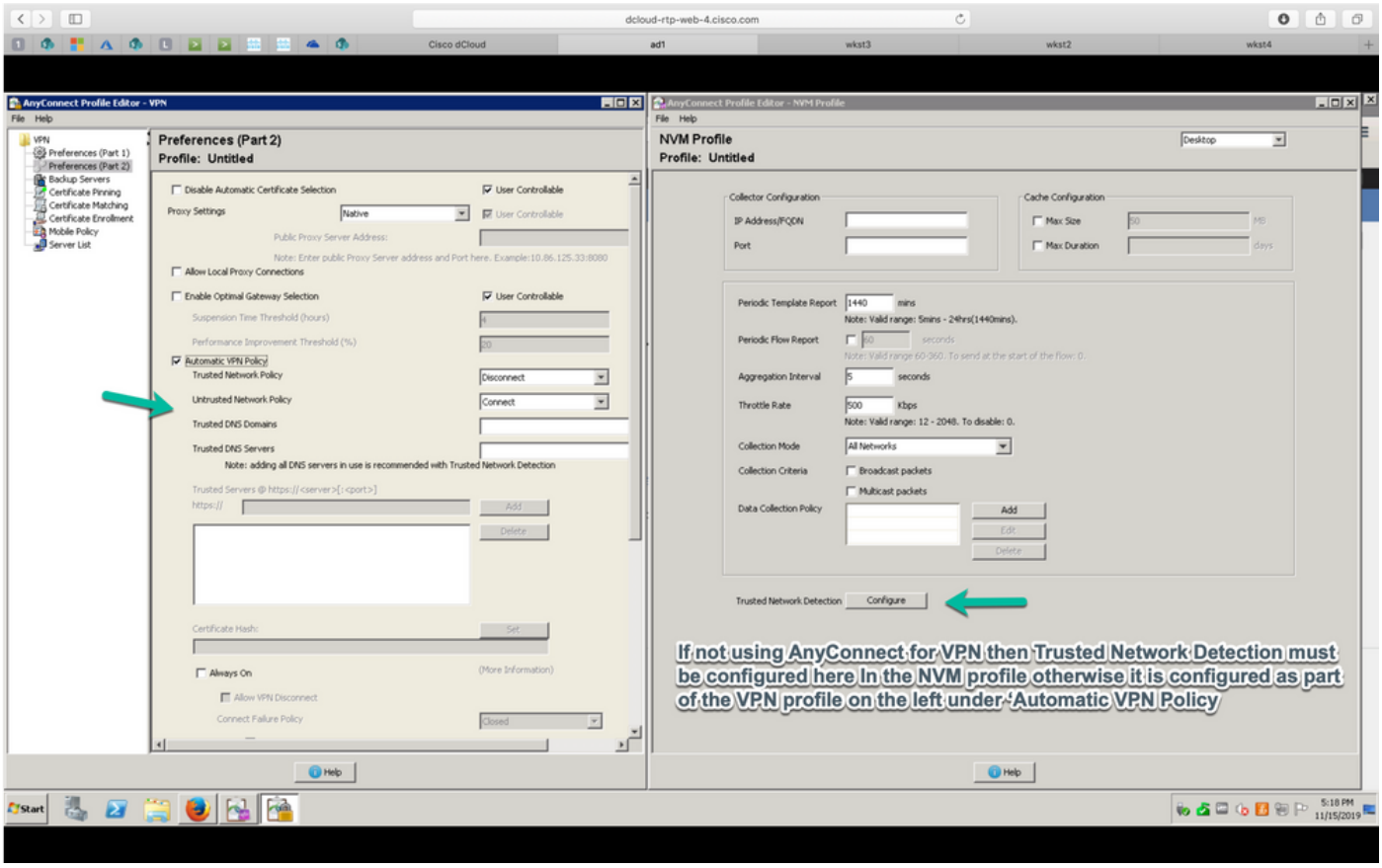
如果您没有AnyConnect部署或使用另一个VPN解决方案，则可以安装NVM独立软件包以满足您的NVM需求。此软件包独立工作，但提供的流量收集级别与当前AnyConnect NVM解决方案相同。如果安装独立NVM，活动进程(如Macintosh操作系统(macOS)上的活动监视器)将指示此用途。

独立NVM使用NVM配置文件编辑器进行配置，并且必须配置受信任网络检测(TND)。NVM使用TND配置来确定终端是否位于企业网络上，然后应用适当的策略。

故障排除和日志记录仍由AnyConnect诊断和报告工具(DART)完成，可以从AnyConnect软件包进行安装。

在独立选项可用之前，必须安装核心VPN模块才能利用TND。核心VPN图块在用户界面(UI)中可见，这会使最终用户感到困惑，尤其是如果他们使用来自其他供应商的VPN解决方案。

使用独立选项时，不使用核心VPN配置文件来配置TND。NVM配置文件现在可直接配置为TND。



AnyConnect NVM客户端配置文件

AnyConnect NVM配置保存在XML文件中，其中包含有关收集器IP地址和端口号的信息以及其他信息。必须在NVM客户端配置文件中正确配置收集器IP地址和端口号。

要正确运行NVM模块，必须将XML文件放置在此目录中：

- 对于Windows 7及更高版本:%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect安全移动客户端\NVM
- 对于Mac OSX:/opt/cisco/anyconnect/nvm

如果配置文件存在于Cisco ASA/ISE上，则它会与AnyConnect NVM部署一起自动部署。

XML 配置文件示例:

<#root>

```
<?xml version="1.0" encoding="UTF-8"?>
-<NVMProfile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="NVMPr
-<CollectorConfiguration>
<CollectorIP>
```

192.0.2.123

```
</CollectorIP>
<Port>
```

```
2055

</Port>
</CollectorConfiguration>
<Anonymize>

false

</Anonymize>
<CollectionMode>

all

</CollectionMode>
</NVMProfile>
```

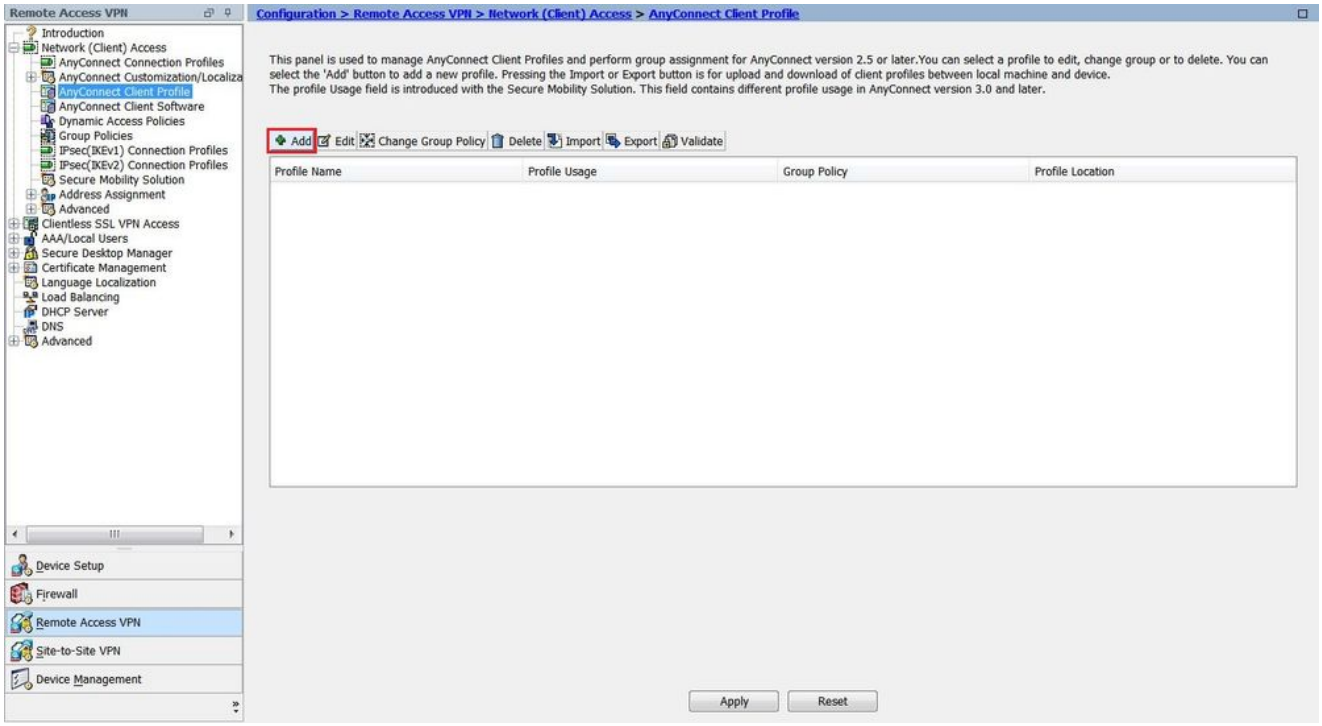
可以使用以下工具创建NVM配置文件：

- 思科ASDM
- AnyConnect配置文件编辑器
- ISE

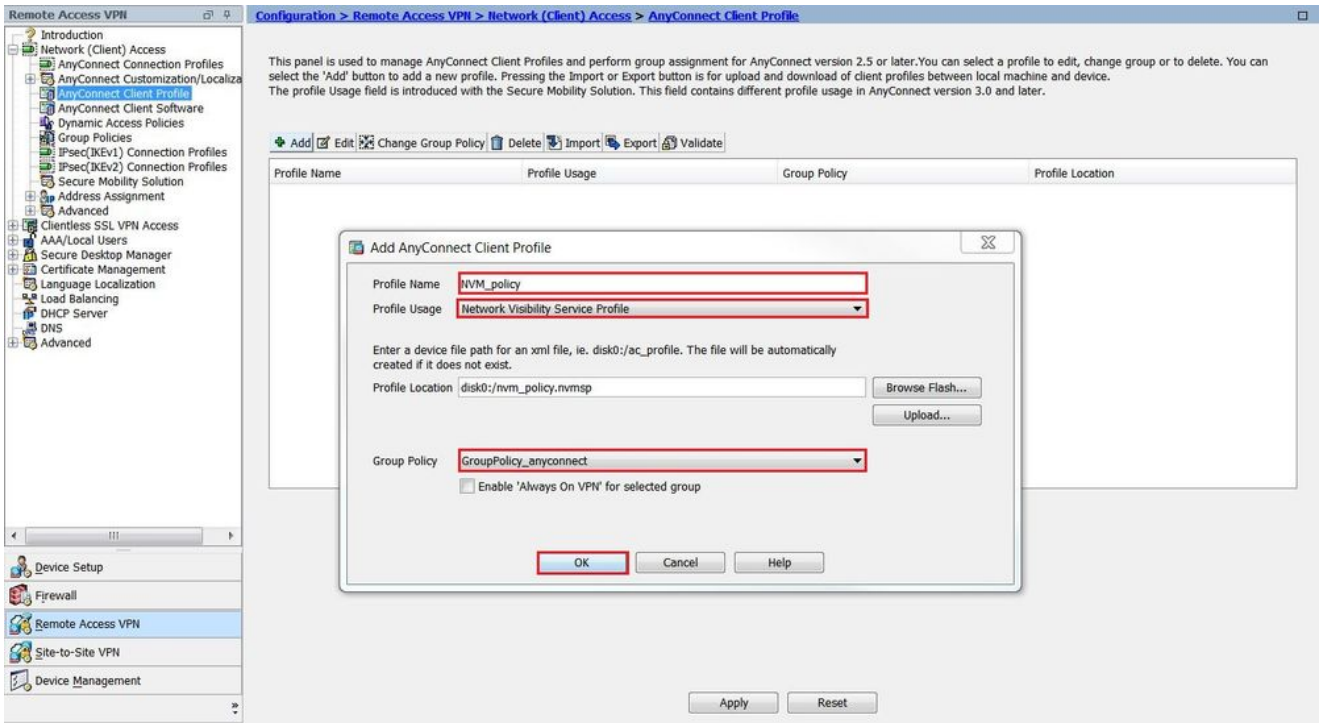
通过ASDM配置NVM客户端配置文件

如果通过Cisco ASA部署AnyConnect NVM，则首选此方法：

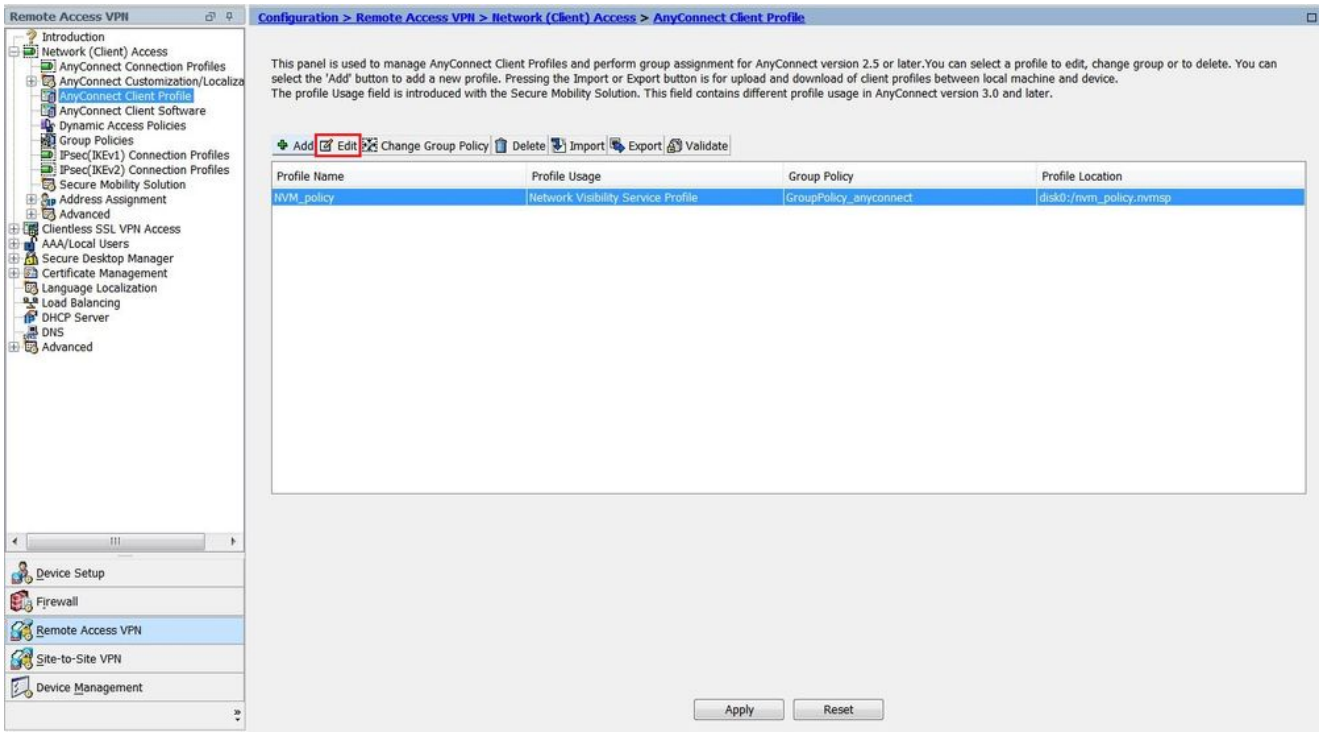
1. 导航到配置>删除接入VPN>网络（客户端）接入> AnyConnect客户端配置文件。
2. 单击Add，如图所示。



3. 为配置文件命名。在配置文件使用中，选择网络可视性服务配置文件。
4. 将该配置文件分配给AnyConnect用户当前使用的组策略，然后单击OK，如图所示。

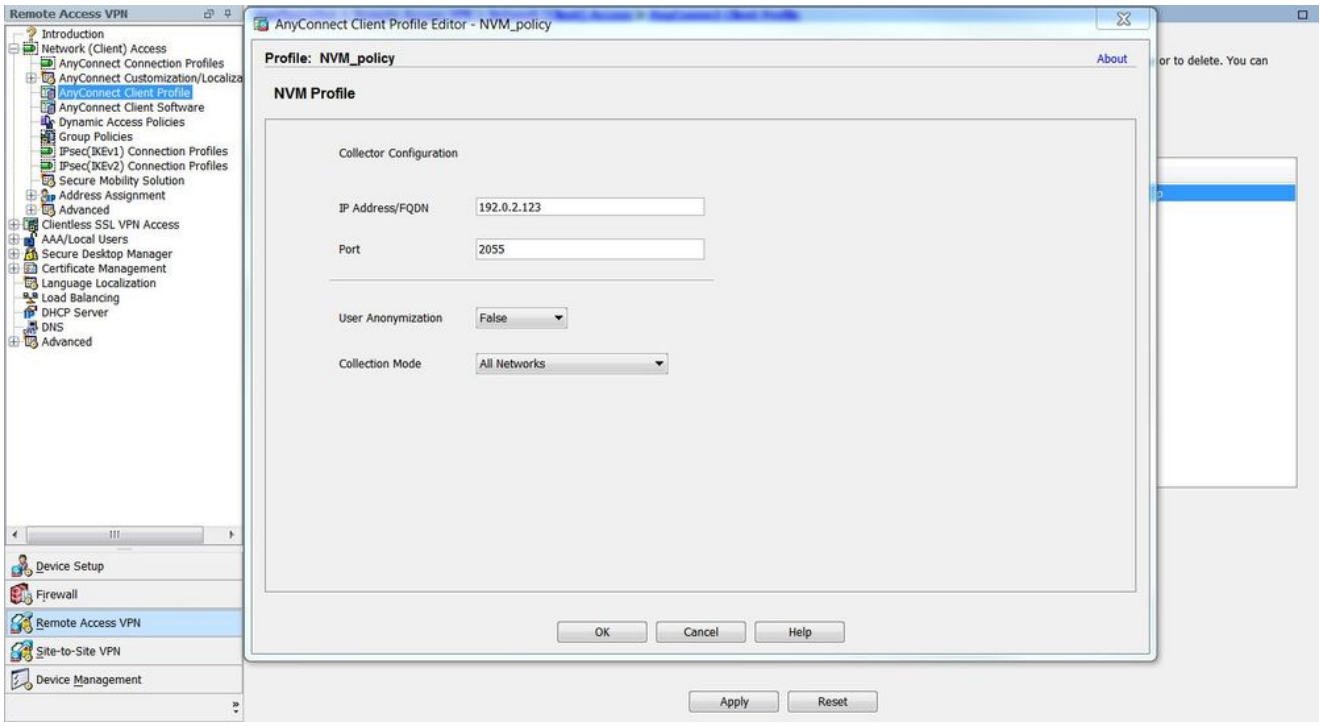


5. 创建新策略后，单击Edit，如图所示。



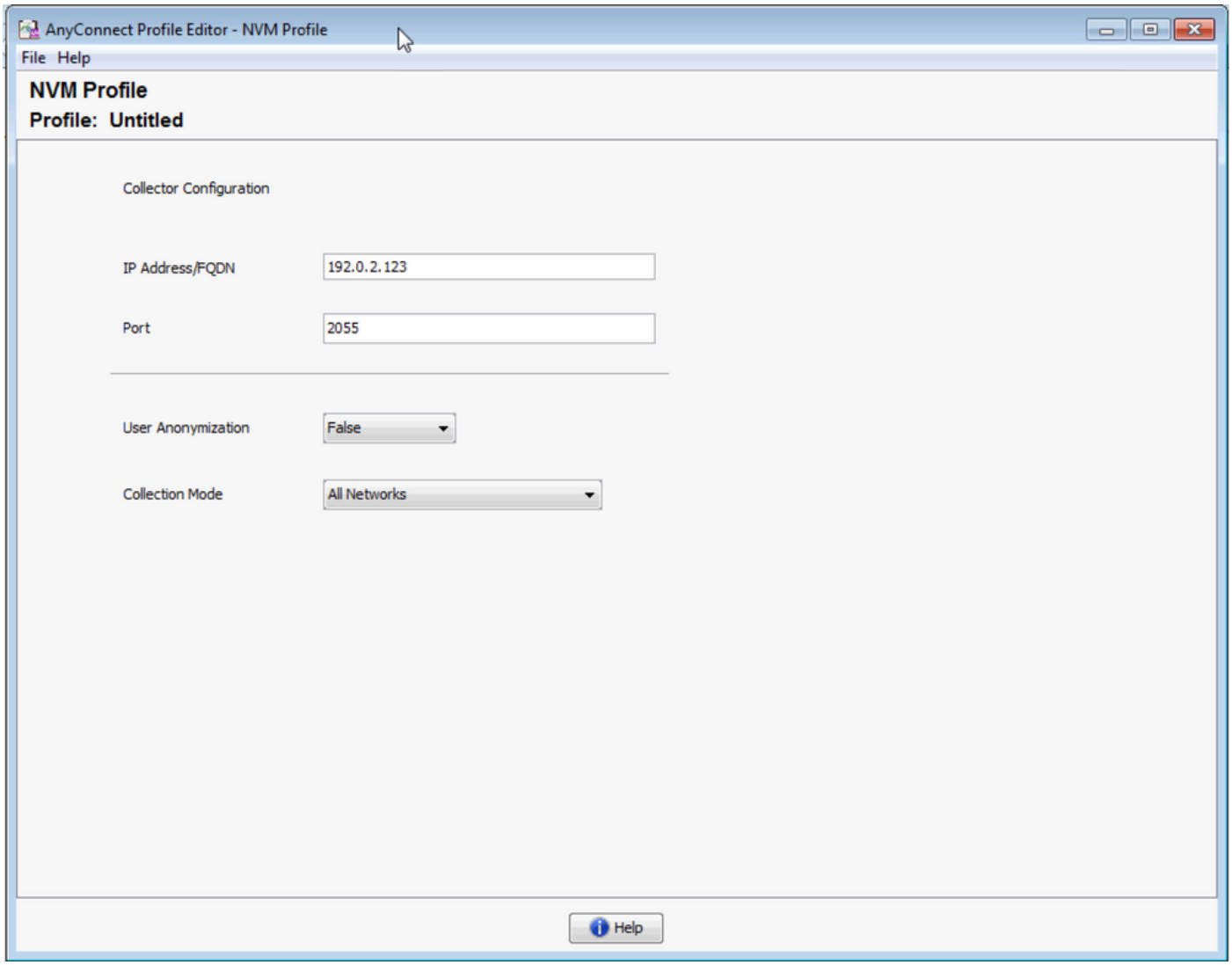
6. 输入有关收集器IP地址和端口号的信息；然后单击 OK。

7. 单击Apply，如图所示。



通过AnyConnect配置文件编辑器配置NVM客户端配置文件

此工具是一个独立工具，可在Cisco.com上找到。如果AnyConnect NVM通过思科ISE部署，则首选此方法。通过此工具创建的NVM配置文件可上传到思科ISE，或直接复制到终端。



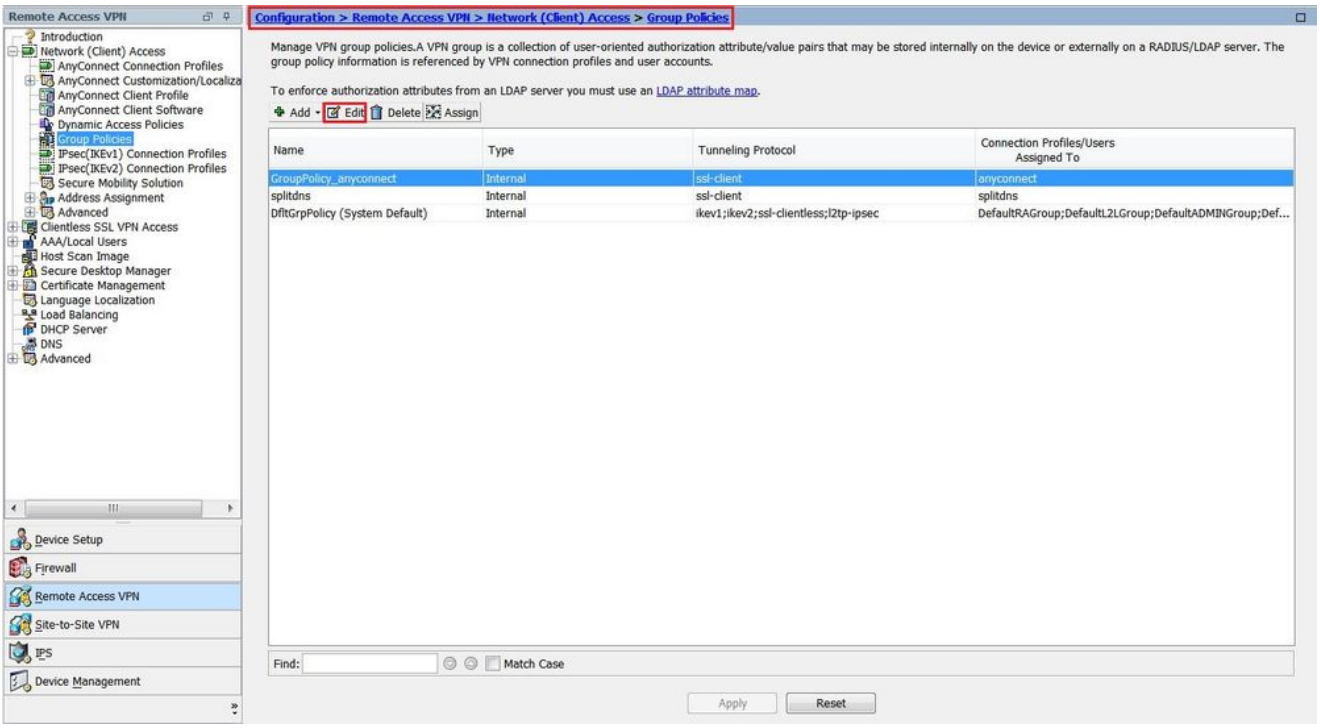
有关AnyConnect配置文件编辑器的详细信息，请参阅AnyConnect配置文件编辑器。

在Cisco ASA上配置Web部署

本技术说明假设ASA上已配置AnyConnect，并且您只需要添加NVM模块配置。有关ASA AnyConnect配置的详细信息，请参阅ASDM手册3:Cisco ASA系列VPN ASDM配置指南，7.16。

要在Cisco ASA上启用AnyConnect NVM模块，请执行以下步骤：

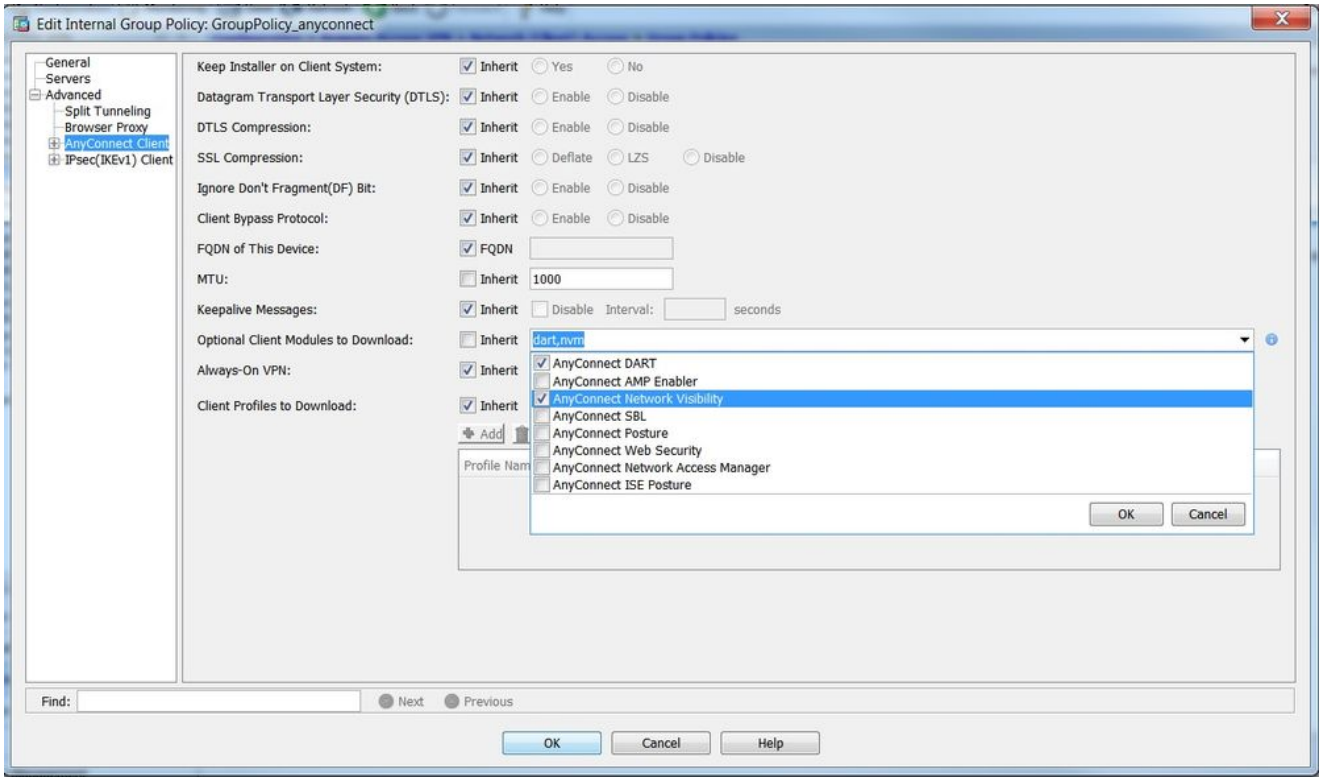
1. 导航到Configuration > Remote Access VPN > Network(Client)Access > Group Policies。
2. 选择相关的组策略并单击Edit，如图所示。



3. 在组策略弹出窗口中，导航到Advanced > AnyConnect Client。

4. 展开Optional Client Modules to Download并选择AnyConnect Network Visibility。

5. 单击OK并应用更改。

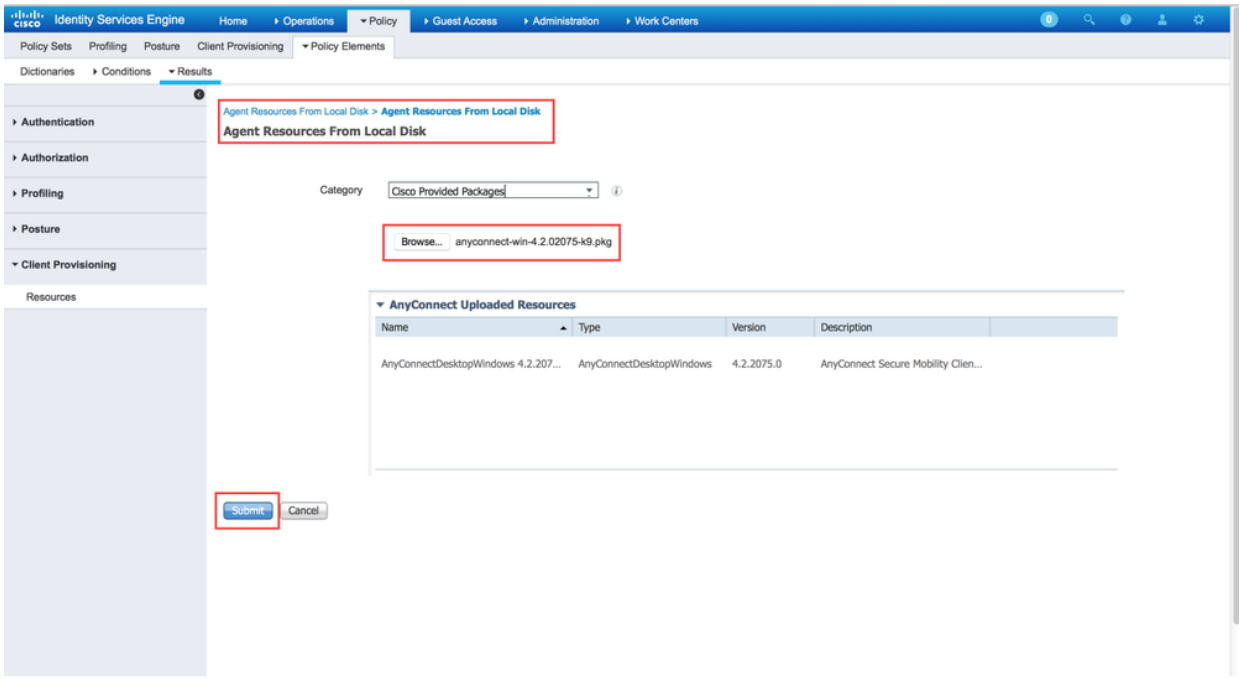


在Cisco ISE上配置Web部署

在本节中，我们将启用AnyConnect客户端模块、配置文件、自定义/语言包和Opswat包。

要为AnyConnect网络部署配置思科ISE，请执行以下步骤：

1. 在Cisco ISE GUI中，导航到Policy > Policy Elements > Results。
2. 展开客户端调配以显示资源;然后选择资源。
3. 添加AnyConnect映像：
    1. 选择Add > Agent Resources并上传AnyConnect软件包文件。



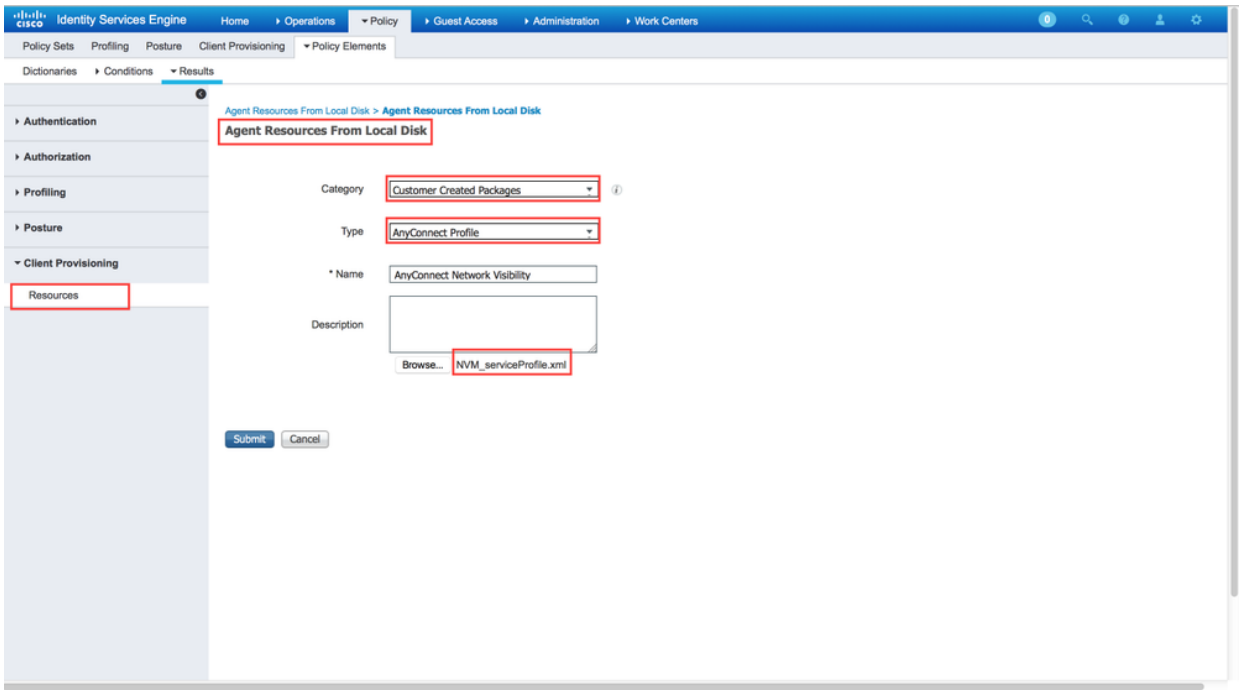
    2. 在弹出窗口中确认软件包的散列。

        文件哈希可以通过Cisco.com下载页面或第三方工具进行验证。

        可重复此步骤以添加多个AnyConnect映像（例如，适用于Mac OSX和Linux OS）。



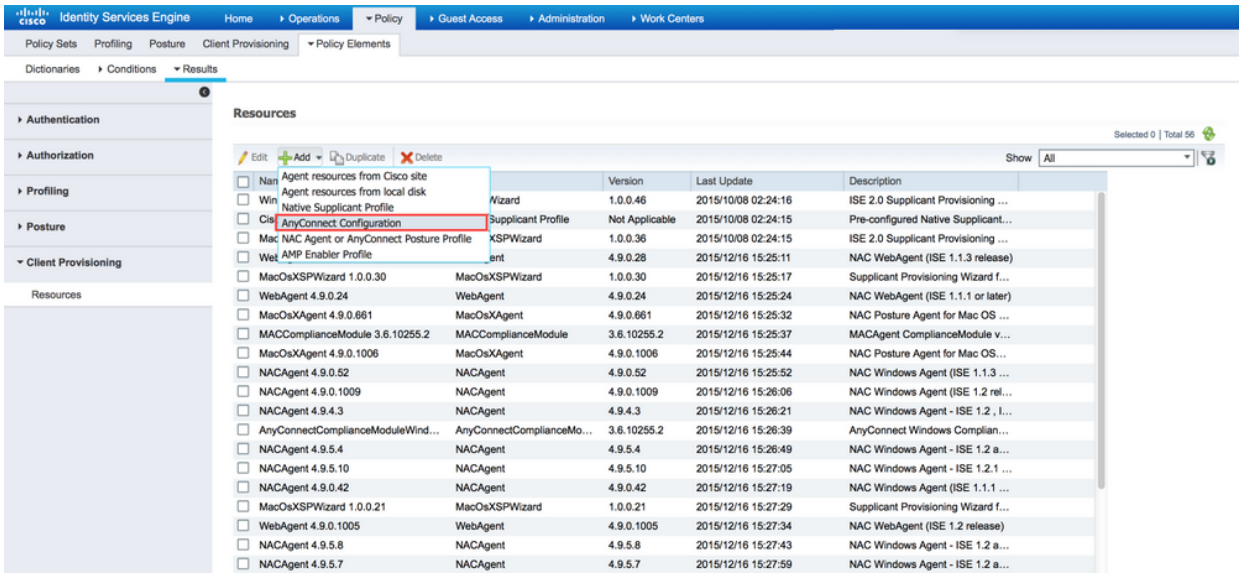
4. 添加AnyConnect NVM配置文件：
    1. 选择Add > Agent Resources，然后上传NVM客户端配置文件。



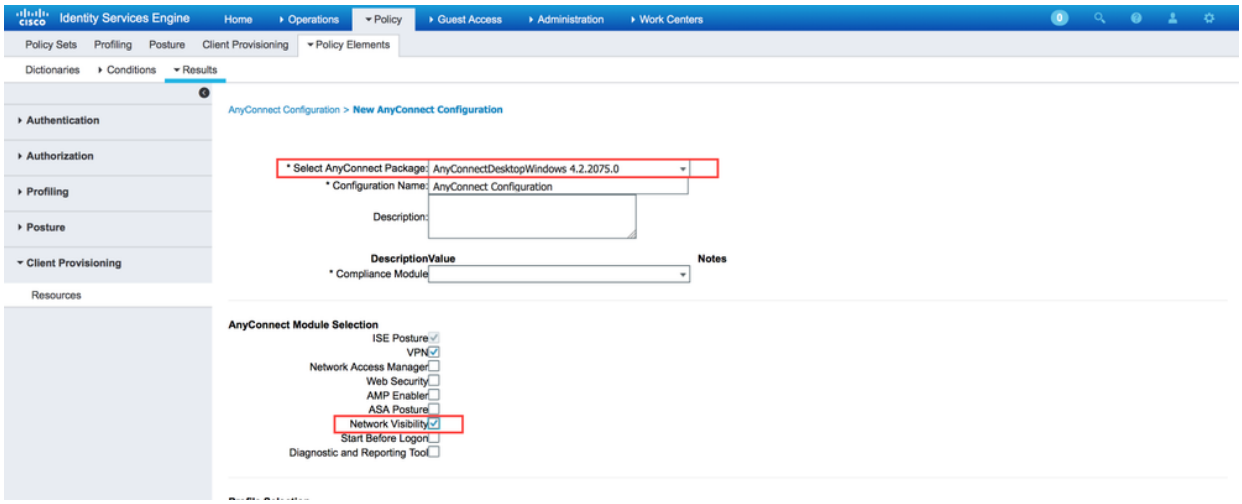
5. 添加AnyConnect配置文件：

    1. 单击Add并选择AnyConnect Configuration。

        选择您在上一步中上传的数据包。



    2. 在AnyConnect Module Selection中启用NVM，同时启用所需的策略。

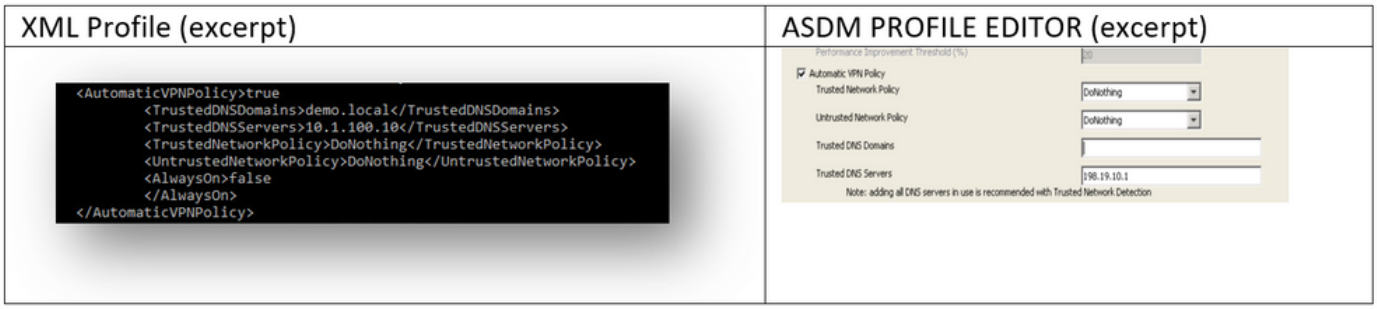


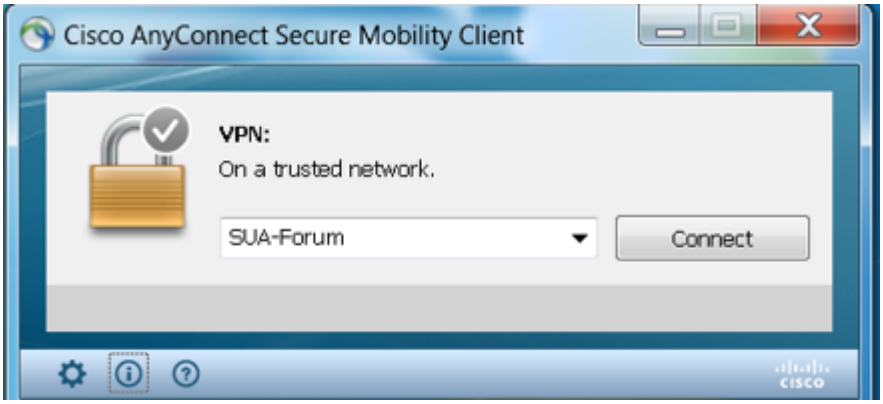
有关思科ISE上的Web部署配置的详细信息，请参阅Web部署AnyConnect。

可信网络检测

AnyConnect NVM仅在处于受信任网络时发送流信息。它使用AnyConnect客户端的TND功能来了解终端是否处于受信任网络中。

受信任网络检测(TND)在用于VPN的AnyConnect客户端配置文件(XML)中配置，而不管环境中当前是否使用VPN组件。TND通过配置配置文件中的Automatic VPN Policy部分启用。至少必须填充一个受信任DNS域或受信任DNS服务器。AnyConnect在客户端确定它处于受信任网络时采取的操作可以通过受信任和不受信任网络策略的下拉菜单设置为DoNothing模式。





有关TND配置的其他详细信息，请参阅关于受信任网络检测。

部署

部署AnyConnect NVM解决方案需要以下步骤：

1. 在Cisco ASA/ISE上配置AnyConnect NVM。
2. 设置IPFIX收集器组件（Linux上的NVM收集器 — 打包在TA插件中）。
3. 使用CESA应用和TA附加设备设置Splunk。

步骤1.在Cisco ASA/ISE上配置AnyConnect NVM

本文档的配置部分详细介绍了此步骤。

在Cisco ISE/ASA上配置NVM后，可将其自动部署到客户端终端。

步骤2.设置IPFIX收集器组件（AnyConnect NVM收集器）

收集器组件负责从终端收集和转换所有IPFIX数据，并将数据转发到适用于Splunk的思科终端安全分析(CESA)插件。NVM收集器在64位Linux上运行。包括CentOS、Ubuntu和Docker配置脚本。CentOS安装脚本和配置文件也可以用于Fedora和Redhat发行版中。

在典型的分布式Splunk Enterprise部署中，收集器应在独立的64位Linux系统上运行，或在64位Linux上运行的Splunk Forwarder节点上运行。收集器还可以安装在没有Splunk组件的独立服务器上。

注意：该解决方案也可以在包含NVM收集器和Splunk Enterprise组件的单个64位Linux系统上运行，用于小型部署或演示目的。对于多达10,000个终端，一体化解决方案最简单。有关POV大小信息，请参阅实际客户端POV。

如何安装收集器

1. 将acnvmcollector.zip文件(位于/opt/splunk/etc/apps/TA-Cisco-NVM/appserver/addon/目录（随TA插件提供）复制到要安装它的系统。
2. 解压缩acnvmcollector.zip文件以解压缩文件。

建议在执行install.sh脚本之前读取.zip捆绑包中的$PLATFORM$_README文件。$PLATFORM$_README文件提供执行install.sh脚本之前需要验证和修改（如有必要）的相关配置设置的信息。至少需要配置将数据转发到的Splunk实例的地址。无法正确配置系统可能导致收集器无法正确运行。

注意：确保您的网络和主机防火墙配置为允许源、目标地址和端口的UDP流量。防火墙必须允许从AnyConnect客户端到收集器的传入IPFIX(CFLOW)流量，以及传出UDP数据到Splunk。

单个NVM收集器实例在大小适当的系统上每秒可处理至少5000个流，或最多35,000到40,000个终端。必须先配置收集器并运行收集器，然后才能使用Splunk NVM和TA-Add on App。

默认情况下，收集器在UDP端口2055上接收来自AnyConnect NVM终端的流量。

此外，收集器为Splunk生成三个数据源：

- UDP端口20519上的每流数据
- UDP端口20520上的终端身份数据
- 终端接口数据UDP端口20521

可以更改接收端口和数据馈送端口。为此，请更改acnvm.conf文件并重新启动收集器实例。确保终端与收集器之间或收集器与Splunk系统之间的任何主机/网络防火墙对配置的UDP端口和地址都是开放的。此外，请确保AnyConnect NVM配置与收集器配置匹配。

安装并运行所有组件后，请参阅Splunk应用程序中的“帮助文件”部分，以获取有关预配置报告、数据模型和解决方案所创建信息元素的详细信息。

您可以重新启动其中一个AnyConnect终端并验证流量是否正在发送到解决方案。例如，您可以使用youtube.com运行稳定的数据流。

此信息必须在acnvm.conf配置文件中配置：

- syslog_server_ip（转发程序或Splunk实例）：可以指向127.0.0.1（请勿使用LOCALHOST）（如果它位于同一框中）。
- 收集器的侦听端口（传入IPFIX数据）：默认值为OK。

注意：从配置文件中省略netflow_collector_ip。它使用默认公共接口，只有通过特定本地IP覆盖默认值时才应进行更改。

Per Flow Data Port、Endpoint Identity Data Port、Endpoint Interface Data和Collector Port已预配置为配置文件中的默认设置。如果使用非默认端口，则必须更改这些值。

此信息将添加到配置文件中：/opt/acnvm/conf/acnvm.conf

DTLS支持

注意：有关详细信息，请参阅本文档中的为DTLS支持配置NVM。

在托管收集器的机箱上执行以下步骤：

- 制作此目录：/opt/acnvm/certs。
- 要将证书应用到收集器，请将证书和密钥保存到/opt/acnvm/certs目录中。
- 使用以下命令，将文件夹的所有者和组更改为acnvm:acnvm:sudo chown -R acnvm:acnvm certs/:
- acnvm.conf的此部分必须使用证书和密钥进行配置。
- 放置配置和证书后，重新启动收集器：sudo systemctl restart acnvm.service

- 检查收集器状态：sudo systemctl status acnvm.service

```
{
"security" :{
   "dtls_enabled": true,
   "server_certificate":"/opt/acnvm/certs/public.cer",
   "server_pkey":"/opt/acnvm/certs/private.key"
   },
```

以下是配置的其余部分：

```
"syslog_server_ip" : "192.0.2.113",
"syslog_flowdata_server_port" : 20519,
"syslog_sysdata_server_port" : 20520,
"syslog_intdata_server_port" : 20521,
"netflow_collector_port" : 2055
}
```

- 使用超级用户权限()执行install.shsudo ./install.sh脚本。

> 注意：帐户需要sudo权限或root权限才能运行install.sh脚本，并需要acnvm服务帐户的权限。

有关详细信息，请参阅适用于Splunk的思科终端安全分析(CESA)应用（详细信息）。

步骤3.使用CESA控制面板和TA插件设置Splunk

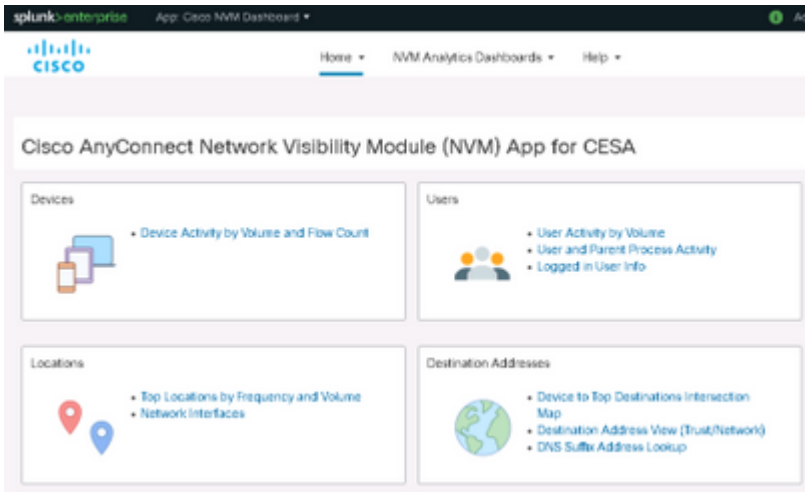
适用于Splunk的Cisco AnyConnect NVM应用在Splunkbase上可用。此应用提供预定义的报告和控制面板，在帮助关联用户和终端行为的可用报告中显示来自终端的IPFIX(nvzFlow)数据。

> 注意：对于云部署，两个应用都安装在云实例中。只有TA安装在内部（与转发器）。 收集器随转发器一起安装在内部或安装在单独的Linux/Docker机箱上。

对于内部安装，您可以在一个机箱或单独的机箱上安装所有组件和应用。（请参阅本文档的部署概述部分中的图。）

下载以下文件：

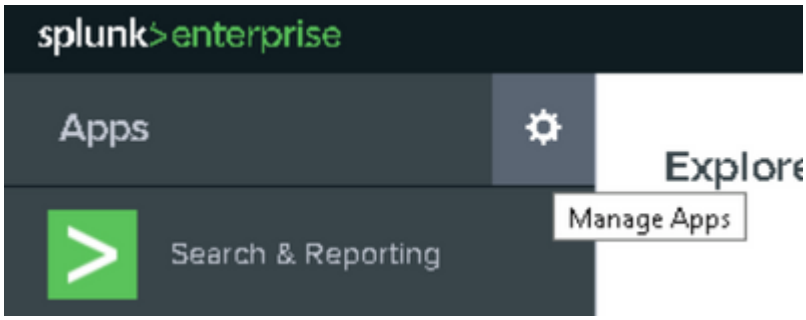
- 适用于Splunk的思科终端安全分析(CESA)应用



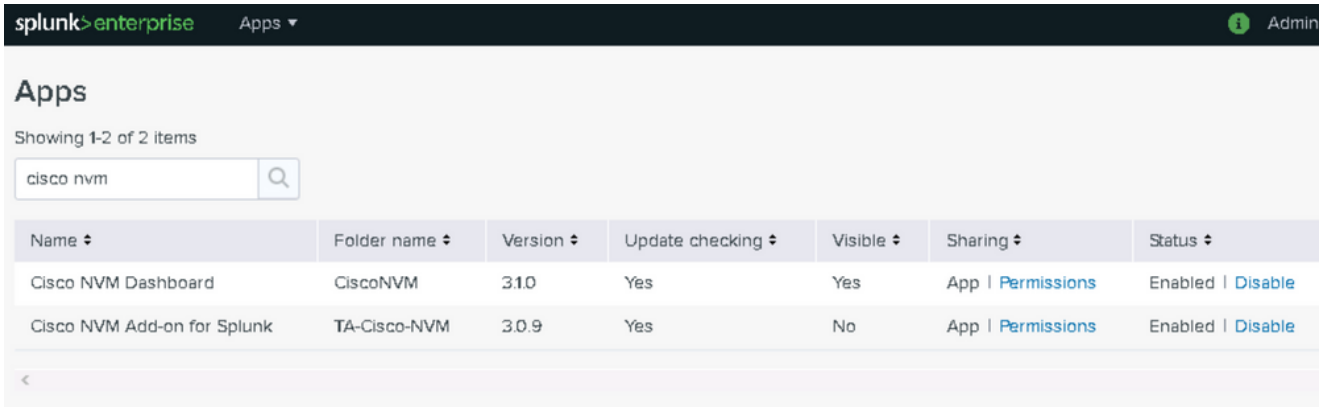
- [适用于Splunk的思科终端安全分析(CESA)插件]

Install（安装）

1. 导航到Splunk > Apps。单击齿轮并安装从Splunkbase下载的tar.gz文件，或在“应用”部分中进行搜索。



2. 使用相同的流程安装Add-On。
3. 查看Splunk Apps页，以确认已安装Cisco NVM控制面板和适用于Splunk的Cisco NVM加载项。



默认配置接收Splunk的三个数据馈送（请参阅本文档中的通过Splunk管理UI启用UDP输入）。

- UDP端口20519上的每数据流
- UDP端口20520上的终端身份数据

- UDP端口20521上的终端接口数据

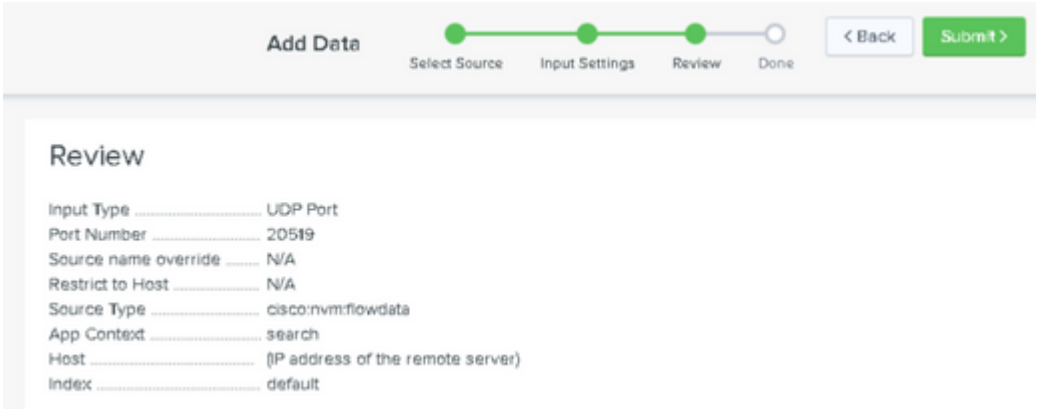
然后，加载项将这些数据源分别映射到Splunk源类型cisco:nvm:flowdata、cisco:nvm:sysdata和cisco:nvm:ifdata。

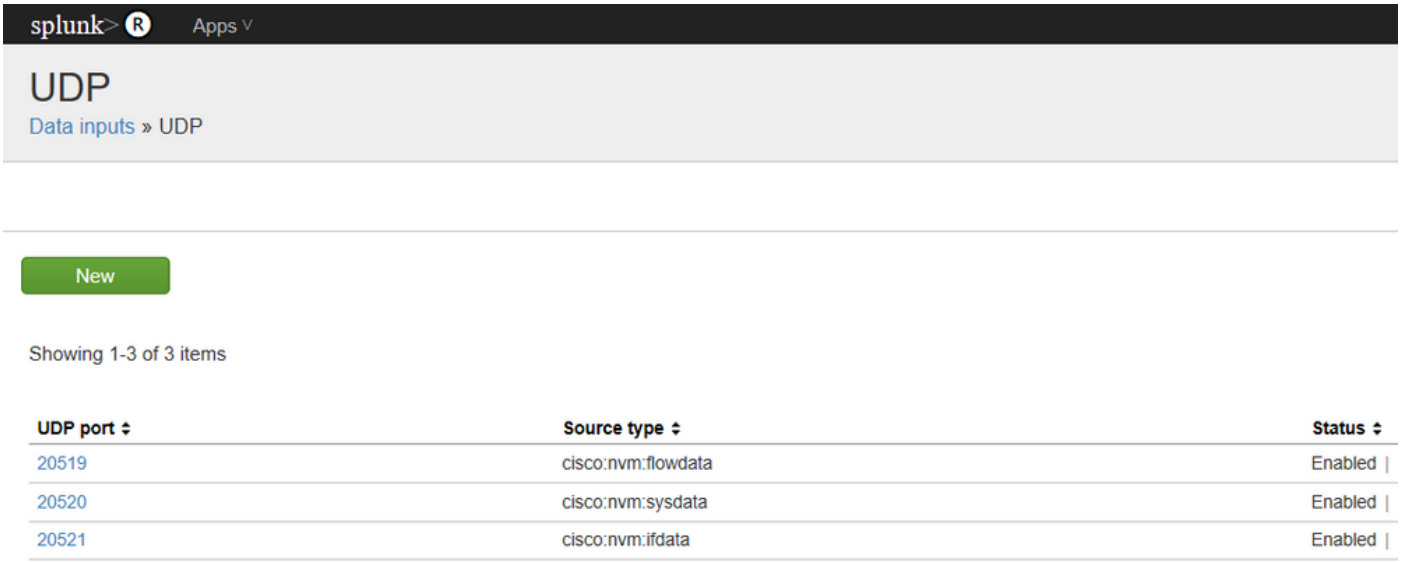
通过Splunk管理UI启用UDP输入

注意：您还可以通过input.conf文件启用UDP输入。此方法在Cisco NVM控制面板应用GUI(在“帮助”(Help)下)中说明。

您无需重新启动Splunk软件。

1. 导航到Splunk > Settings > Data Input > UDP。
2. 点击New Local UDP > Enter port # missing > Click Next >选择相应的源类型>点击Review >Click Submit。
3. 对另外两个端口重复上述步骤。（您可以使用克隆。）

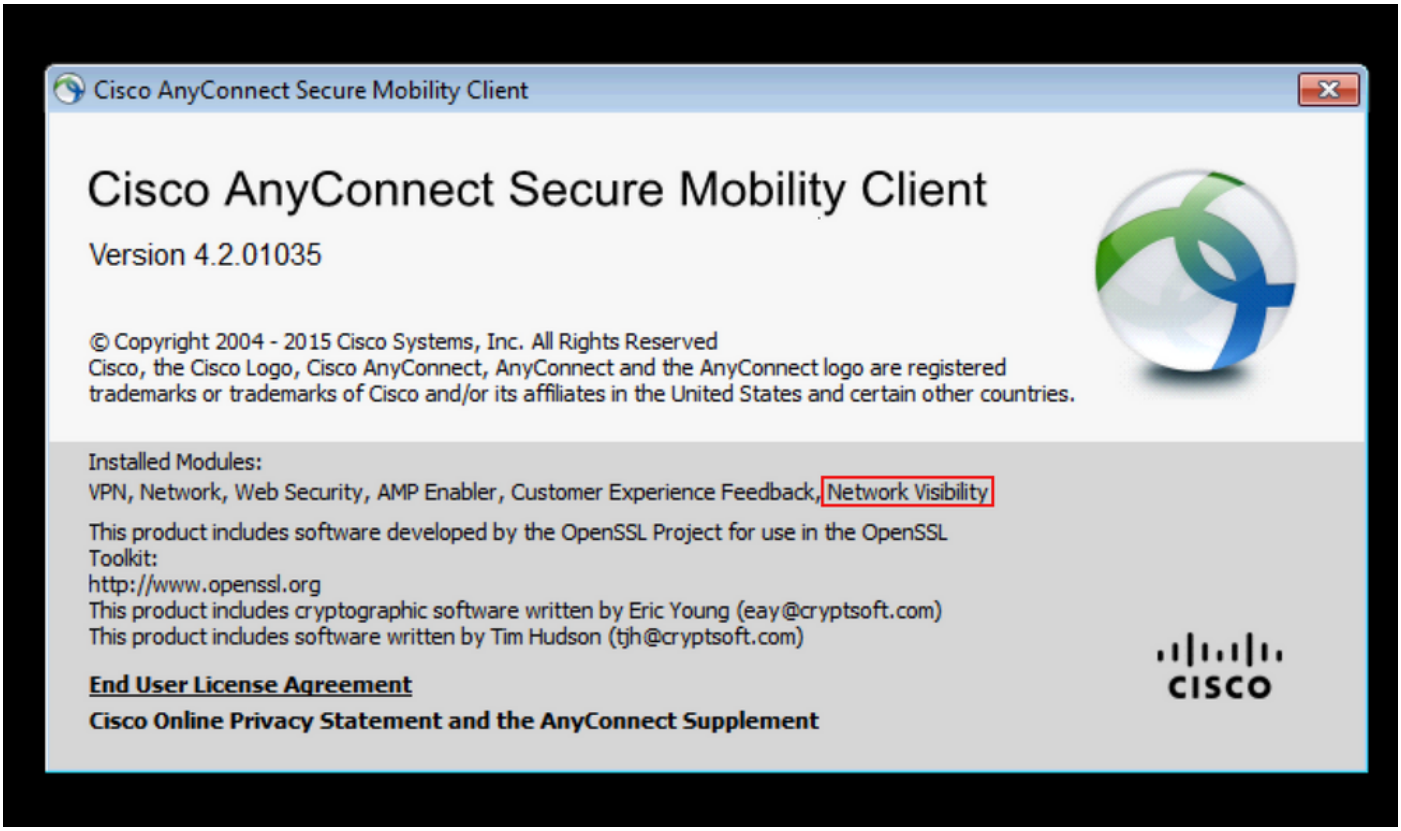




验证

验证AnyConnect NVM安装

成功安装后，网络可视性模块应列在AnyConnect安全移动客户端的信息部分的已安装的模块中。



此外，验证nvm服务是否在终端上运行，且配置文件存在于所需目录中。

验证收集器状态

确认收集器状态为“活动（运行）”。 此状态确保收集器始终从终端接收IPFIX/cflow。如果收集器状态为非活动状态，请确保文件的acnvm帐户权限允许其执行：

- /opt/acnvm/bin/acnvmcollector

```
root@ubuntu-splunkcollector:~$ /etc/init.d/acnvmcollectord status
 * acnvmcollector is running
root@ubuntu-splunkcollector:~$
```

- /opt/splunk/etc/apps/TA-Cisco-NVM/appserver/addon/

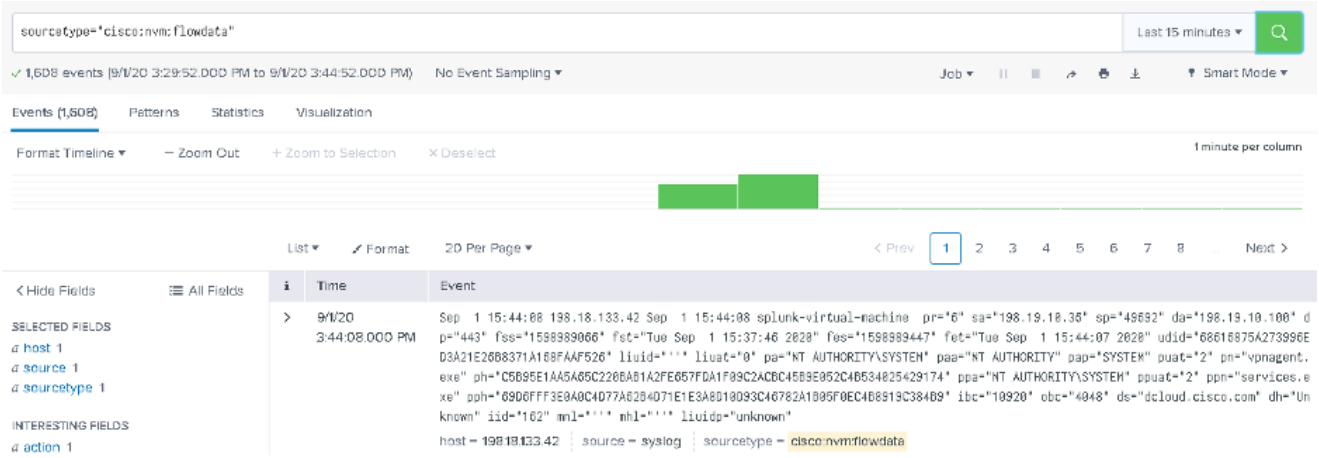
```
[splunk@splunk-virtual-machine addon]$ systemctl status acnvm.service
● acnvm.service - AC NVM Service
   Loaded: loaded (/usr/lib/systemd/system/acnvm.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2020-06-19 13:48:08 EDT; 25s ago
 Main PID: 41165 (acnvmcollector)
    Tasks: 13 (limit: 49772)
   Memory: 1.8M
   CGroup: /system.slice/acnvm.service
           ├─41165 /opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/co>
           ├─41176 /opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/co>
           ├─41177 /opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/co>
           ├─41178 /opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/co>
           └─41179 /opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/co>
lines 1-12/12 (END)
```

验证Splunk - CESA控制面板

确保Splunk及其相关服务正在运行。有关如何排除Splunk问题的文档，请参阅Splunk网站。

由于使用自动化脚本，CESA的控制面板在收到初始数据五分钟后才会更新。但是，您可以立即运行手动搜索以验证是否正在接收数据：

1. 在Splunk主控制面板中，单击Search & Reporting。
2. 在下一个屏幕中，设置正确的范围，以填充所需数据。
3. 在搜索字段中，输入： sourcetype="cisco:nvm:flowdata"



在最初的五分钟后，验证CESA控制面板是否正在接收数据：

1. 在Splunk主控制面板中，单击Cisco Endpoint Security Analytics Dashboard。
2. 如果要保留当前设置，请单击Device Activity by Volume and Flow Count。
3. 单击 submit。控制面板显示数据和图形。

数据包流

1. IPFIX数据包由AnyConnect NVM模块在客户端终端上生成。
2. 客户端终端将IPFIX数据包转发到收集器IP地址。
3. 收集器收集信息并将其转发到Splunk。
4. 收集器通过三个不同的流向Splunk发送流量：每个流数据、终端数据和接口数据。

所有流量都基于UDP，因此数据包流中不会确认已收到数据。

流量的默认端口：

- IPFIX数据2055
- 每流数据流20519
- 终端数据20520
- 接口数据20521

NVM模块缓存IPFIX数据，并在数据处于受信任网络中时将其发送到收集器。当笔记本电脑连接到公司网络（内部）或通过VPN连接时，会发生此行为。

您可以验证收集器是否正在从NVM模块接收数据包。为此，请根据您的配置在特定UDP端口上运行数据包捕获，以检查是否收到数据包。此验证将通过Splunk系统Linux操作系统完成。

流模板

IPFIX流量模板会在IPFIX通信开始时发送到收集器。这些模板有助于收集器理解IPFIX数据。

收集器还会预加载模板，以确保即使客户端未发送模板，也可以解析数据。如果客户端的更新版本发布时协议发生更改，收集器将使用客户端发送的新模板。

在以下情况下发送模板：

1. NVM客户端配置文件中有更改。
2. 发生网络更改事件。
3. Nvmagent服务已重新启动。
4. 终端已重新启动/重新启动。
5. 按照NVM配置文件的配置，定期（默认值为24小时）。

在极少数情况下，收集器无法找到模板。如果发生这种情况，您将看到以下症状之一：

- 在终端上的数据包捕获中找不到模板
- 或者收集器日志中没有flowset的模板

要解决此问题，请重新启动其中一个终端。

故障排除

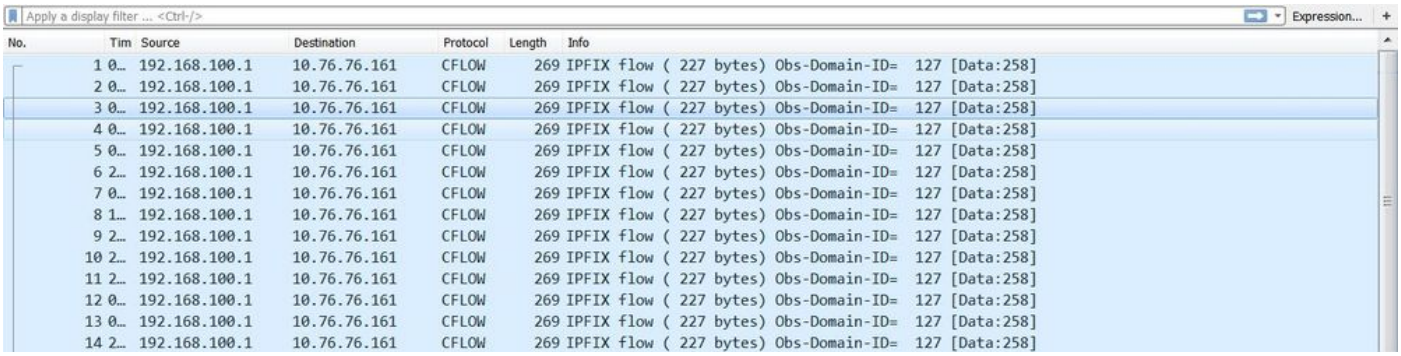
以下是故障排除的基本步骤：

1. 确保客户端终端和收集器之间的网络连接。
2. 确保收集器和Splunk之间的网络连接。
3. 确保NVM已正确安装在客户端终端上。
4. 在终端上应用捕获，以查看是否正在生成IPFIX流量。
5. 在收集器上应用捕获，以查看它是否接收IPFIX流量，以及它是否将流量转发到Splunk。
6. 在Splunk上应用捕获以查看它是否收到流量。
7. 对于DTLS:

- 确认AnyConnect客户端信任收集器证书。
- 确认NVM配置文件已启用“安全”选项。
- 确认已为证书配置收集器。

IPFIX流量，如Wireshark所示：

注意：如果在客户端和收集器之间运行DTLS，则必须过滤DTLS流量。



Apply a display filter ... <Ctrl-/> Expression... +

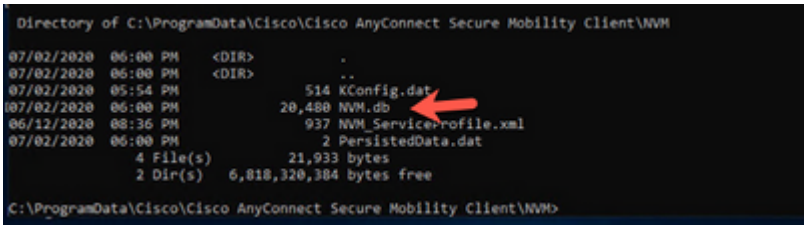
No.	Tim	Source	Destination	Protocol	Length	Info
1	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
2	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
3	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
4	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
5	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
6	2…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
7	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
8	1…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
9	2…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
10	2…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
11	2…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
12	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
13	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
14	2…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]

AnyConnect客户端（NVM模块）

不向收集器报告数据，也不从终端发送数据包

NVM数据库文件(NVM.db)在C:\%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM目录中的大小是否继续增加？此行为表示AnyConnect NVM客户端没有向收集器发送数据包。

注意：有关缓存进程和可用缓存控制的信息，请参阅Cisco AnyConnect安全移动客户端管理员指南，版本4.9。



```
 Directory of C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM

07/02/2020  06:00 PM    <DIR>          .
07/02/2020  06:00 PM    <DIR>          ..
07/02/2020  05:54 PM               514 KConfig.dat
07/02/2020  06:00 PM            20,480 NVM.db
06/12/2020  08:36 PM               937 NVM_ServiceProfile.xml
07/02/2020  06:00 PM                 2 PersistedData.dat
               4 File(s)         21,933 bytes
               2 Dir(s)   6,818,320,384 bytes free

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM>
```

可信网络检测(TND)

启动AnyConnect UI并确保它位于受信任的网络中。NVM依赖TND检测终端何时处于受信任网络中。不正确的TND配置会导致NVM出现问题。NVM具有自己的TND配置，该配置在已配置服务器的TLS证书指纹上工作。可以在NVM配置文件编辑器中配置NVM TND。

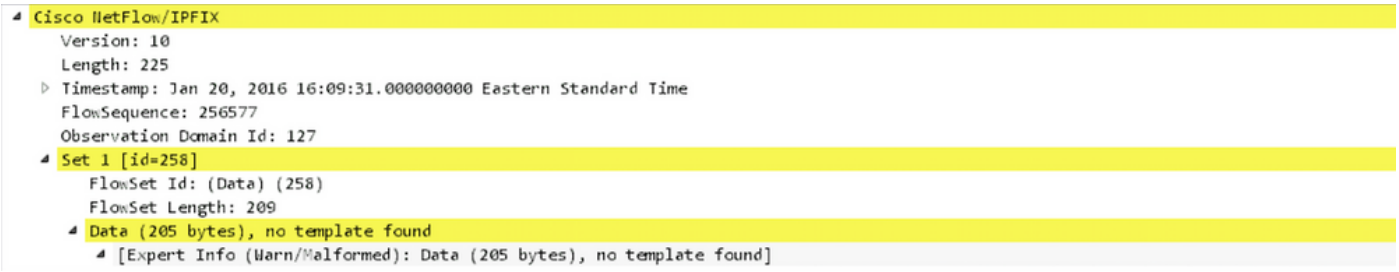
如果未配置NVM TND，则NVM依赖于VPN模块的TND配置。VPN模块的TND基于通过DHCP接收的信息工作：域名和域名系统(DNS)服务器。如果DNS服务器和/或域名与配置的值匹配，则网络被视为受信任。VPN还支持基于TLS证书的TND检测。

- 确保TND配置正确。NVM仅在位于受信任网络中时导出。

> 注意：如果TND配置不正确，NVM不会导出数据。例如，如果在客户端上配置了三个DNS服务器，但所有三个DNS服务器均未在TND配置中设置，则NVM不会导出数据。

- 从TND VPN配置中删除受信任域。
- 网络问题：
  - 对于拆分隧道，始终在VPN的“拆分包括”配置中包含收集器的IP地址。如果收集器的IP地址不是拆分隧道受信任配置的一部分，则数据将从公共接口发送出去。
- 确保将CollectionMode配置为在当前网络上收集（受信任/不受信任）。
- 确保VPN.xml和NVM_ServiceProfile.xml文件位于正确的文件夹中；然后重新启动。
- 启动 — 停止所有AnyConnect服务。
- 退回连接到DNS服务器连接的内部网络。

数据包捕获:



AnyConnect诊断和报告工具(DART)

要对AnyConnect操作进行故障排除，请在NVM组件上运行DART。请参阅AnyConnect故障排除。

- NVM所需的所有日志都由DART处理。DART收集日志文件、配置等。
- Windows日志：事件不在同一个位置。AnyConnect下的NVM事件查看器中有一个单独的枝叶。
- macOS/Linux:按nvmagent过滤日志。

收集器(在Linux/Docker计算机上：一体化或独立)

acnvmcollector安装失败

安装收集器并运行安装脚本()Sudo ./install_ubuntu.sh时，

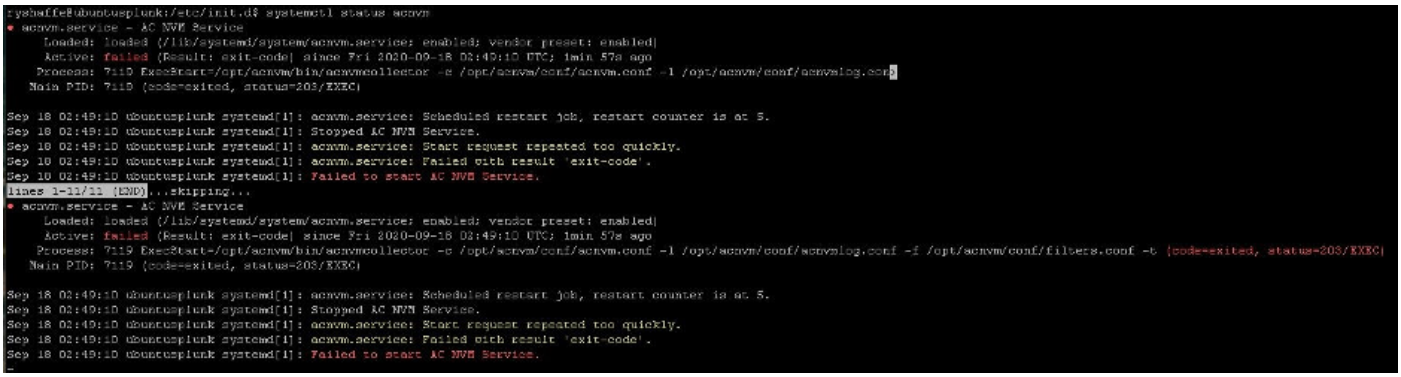
此错误出现在/var/log/syslog中： "Acnvm.conf error: line number 17 : expected key string"

此问题可能由额外的逗号或无效位置的逗号引起。

acnvmcollector无法启动

此问题是Ubuntu的问题（但可能适用于所有Linux）。 未能对acnvmcollector文件执行代码：/opt/acnvm/bin/acnvmcollector。

acnvmcollector没有acvnm用eXecute户和组。



收集器日志 — 在哪里可以设置调试？

您可以在ACMNVMLOG.conf文件中设置日志记录级别。日志记录级别是启动时发送到收集器的配置的一部分。更改后，重新启动收集器。

log4cplus.rootLogger=DEBUG, STDOUT, NvmFileAppender

```
Jan 20 12:48:54 csaxena-ubuntu-splunkcollector NVMCollector: no templates
for flowset 258 for 10.150.176.167 yet
Jan 20 12:48:55 csaxena-ubuntu-splunkcollector NVMCollector:
HandleReceivedIPFIX: exporter=10.150.176.167 bytes_recvd=234 totlength=234
Jan 20 12:48:55 csaxena-ubuntu-splunkcollector NVMCollector:
=================> flowsetid=258 flowsetlen=218
Jan 20 12:48:55 csaxena-ubuntu-splunkcollector NVMCollector: no templates
for flowset 258 for 10.150.176.167 yet
```

如何查找收集器的版本号？

要查找收集器版本，请运行带有acnvmcollector以下标志的-v命令：

示例 1：

```
./opt/acnvm/bin/acnvmcollector -v
```

示例 2：

```
/opt/acnvm/bin
[root@splunk-virtual-machine bin]# ./acnvmcollector -v
```

输出：

```
Cisco AnyConnect Network Visibility Module Collector (version 4.10.02086 release)
Copyright (C) 2004-2021 All Rights Reserved.
```

DTLS问题

- 消息“DTLS not configured”表示acnvm.conf文件中未配置DTLS。
- 当不支持密码密钥组合时，将显示消息“服务器密钥无效”。

Splunk控制台（CESA控制面板）不显示数据

AnyConnect Client

- 使用youtube.com生成数据。您还可以浏览一些网站。
- AnyConnect客户端能否通过UDP 2055将信息发送到收集器服务器？（换句话说，AnyConnect客户端和收集器服务器之间是否存在任何防火墙？）
  - 尝试从客户端计算机telnet至收集器计算机。
- 运行wireshark确认客户端正在向收集器发送流量(2055 CFLOW)数据。

收集器盒

- 验证收集器盒是否正在接收AnyConnect NVM流量：
  - 执行tcpdump并确认您在25001 to 2055上看到从客户端到服务器的数据包。例如，此命令显示来自客户端主机IP地址的前100个数据包：Sudo tcpdump -I any -c100 -nn host 10.1.110.7

    注意：有关详细信息，请参阅如何使用tcpdump捕获所有UDP数据包？
  - 确保AnyConnect NVM收集器正在运行（请参阅本文档中的DTLS支持）。
  - 检查acnvm.conf文件是否存在格式错误、缺少引号、逗号等。
  - Splunk UI - TA — 是通过Splunk GUI或input.conf设置UDP数据输入和源类型？
    - 在UI > settings > server controls下重新启动Splunk。

常见问题(FAQ)

如何将数据从AnyConnect NVM发送到多个目标？

此方案用于高可用性情况或发送到多个平台（例如Splunk和Stealthwatch）。

有关详细信息，请参阅基于Splunk Quickstart POV套件和部署指南的思科终端安全分析(CESA)。

在哪里存储AnyConnect NVM DTLS的证书？

在收集器上未安装已知证书的实验室测试中，可能会出现这种情况。

- Windows 窗口版本:将收集器证书安装到Windows受信任证书中。
- Mac OSX:使用标准流程通过密钥链安装根证书。您可以使用密钥链工具导入证书，并将其添加为受信任证书。
- Linux RHEL:按照以下RHEL根CA导入步骤操作：
    1. 将ca cert复制到/etc/pki/ca-trust/source/anchors。
    2. sudo update-ca-trust enable
    3. sudo update-ca-trust extract
- Linux Ubuntu:按照以下Ubuntu根CA导入步骤操作：
    1. 使用以下命令，将.cer文件转换为.crt文件： openssl x509 -inform PEM -in RootCA.cer -out rootCa.crt
    2. 将.crt文件复制到/usr/local/share/ca-certificates目录。
    3. 运行以下命令： sudo update-ca-certificates

XML文件名

使用本地配置文件编辑器时，核心VPN模块XML配置文件名称并不重要。但是，您必须将服务配置文件另存为NVM_ServiceProfile.xml。如果为服务配置文件使用其他名称，NVM将无法收集和发送数据。

收集器(AnyConnect NVM)

适用于Splunk的思科终端安全分析(CESA)应用（详细信息）

- 是否可以在根目录下创建供应商目录，然后将所有权提供给其他帐户？

  只要安装脚本具有将文件复制到其中的权限，您就可以首先创建/opt/acnvm。
- 文件权限：install.sh文件需要权限才能作为根目录执行。
- 服务帐户：

- 命令useradd -r和命令是-s /bin/false必需的，因为服务帐户是不具有主目录的非交互式帐户。
- 对于非交互式帐户来说，不要求具有主目录，服务帐户没有主目录是保持干净的标准做法。
- 所有用户都有uid/guid，无论他们是否有主目录。

- 收集器操作系统：收集器运行在CentOS或Ubuntu上；也可以在RedHat上运行，因为RedHat使用CentOS脚本。
- 如果需要，可以修改安装脚本：
  - 安装脚本必须以root用户身份或具有SUDO权限运行，因为它会创建一个名为acnvm的新用户，并将所有内容都放入/opt/acnvm目录。

> 注意：或者，您可以创建自定义脚本，以便根据要求执行适当的操作。此脚本可以使用系统上已存在的其他用户，但此用户必须具有SUDO权限才能运行安装。

- 要查找收集器版本，请运行带有以下标志的此-v命令： ./opt/acnvm/bin/acnvmcollector -v

推荐版本

我们始终建议您使用最新可用软件版本的AnyConnect。有关详细信息，请参阅Cisco AnyConnect安全移动客户端v4.x发行版本注释。

相关信息

- 基于Splunk Quickstart POV套件和部署指南的思科终端安全分析(CESA)
- 思科终端安全分析(CESA)控制面板概述和常见问题
- 适用于Splunk的思科终端安全分析(CESA)应用
- 适用于Splunk的思科终端安全分析(CESA)应用（文档）
- Cisco AnyConnect安全移动客户端v4.x的客户端管理员指南
- Cisco AnyConnect安全移动客户端v4.x版本说明
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。