

通过AnyConnect 4.2.x和Splunk安装并且配置Cisco网络公开性模块

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[背景信息](#)

[Cisco AnyConnect安全移动客户端](#)

[互联网协议流信息导出\(IPFIX\)](#)

[IPFIX收集器](#)

[Splunk](#)

[拓扑](#)

[Configure](#)

[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](#)

[配置在Cisco ASA的Web配置](#)

[配置在Cisco ISE的Web配置](#)

[可信的网络检测](#)

[配置](#)

[步骤1.配置在Cisco ASA/ISE的Anyconnect NVM](#)

[步骤2.设置IPFIX收集器组件](#)

[步骤3.与Cisco NVM App的设置Splunk](#)

[Verify](#)

[验证Anyconnect NVM安装](#)

[验证收集器状态如运行](#)

[验证Splunk](#)

[Troubleshoot](#)

[信息包流](#)

[基本排除步骤故障](#)

[可信的网络检测\(TND\)](#)

[流模板](#)

[推荐的版本](#)

[相关问题](#)

[相关链接](#)

Introduction

本文在终端用户系统描述方法安装和配置Cisco AnyConnect网络可见度模块(NVM)使用AnyConnect 4.2.x或更高。

Cisco AnyConnect NVM使用作为媒体配置安全逻辑分析方法。NVM授权组织发现终端&在他们的网络的用户行为，从终端集中流和前提与另外的上下文一起类似用户、应用程序、设备、位置和目的地。

此technote是配置示例使用AnyConnect NVM和Splunk。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- AnyConnect 4.2.01022或高与NVM
- AnyConnect尖顶许可证
- ASDM 7.5.1或更高

Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco AnyConnect安全移动性客户端4.2或以上
- Cisco AnyConnect配置文件编辑器
- Cisco可适应的安全工具(ASA)，版本9.5.2
- Cisco Adaptive Security Device Manager (ASDM)，版本7.5.1
- Splunk企业6.3
- Ubuntu 14.04.3 LTS作为收集器设备

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

背景信息

Cisco AnyConnect安全移动客户端

Cisco Anyconnect是提供多个安全服务保护企业的一个统一的代理程序。Anyconnect是最常用的作为企业VPN客户端，但是也支持迎合企业安全的不同方面的另外的模块。另外的模块enable (event)安全功能类似状态评估、Web安全、malware保护，网络可见度等等。

此technote是关于网络可见度模块(NVM)，集成Cisco Anyconnect提供管理员能力监控终端应用程序使用。

关于Cisco Anyconnect的更多信息，请参见以下：

[Cisco AnyConnect安全移动客户端管理员指南，版本4.3](#)

互联网协议流信息导出(IPFIX)

IPFIX是定义导出IP流信息一个标准的IETF协议多种目的类似记帐/审核/安全。IPFIX根据Cisco NetFlow协议v9，虽然不直接兼容。

Cisco vzFlow是根据IPFIX协议被扩大的协议规格描述。作为AC NVM一部分，IPFIX没有支持足够标准的信息要素所有参数可以收集。Cisco vzFlow协议延伸标准的IPFIX并且定义了最新信息元素以及定义了将由AC NVM使用导出IPFIX数据的标准的IPFIX模板。

关于IPFIX的更多信息，请参见[rfc5101](#)，[rfc7011](#)，[rfc7012](#)，[rfc7013](#)，[rfc7014](#)，[rfc7015](#)。

IPFIX收集器

收集器是接受并且存储IPFIX数据的服务器。它能然后供给此数据到Splunk。即Lancope。

Cisco也提供其家种的IPFIX收集器。

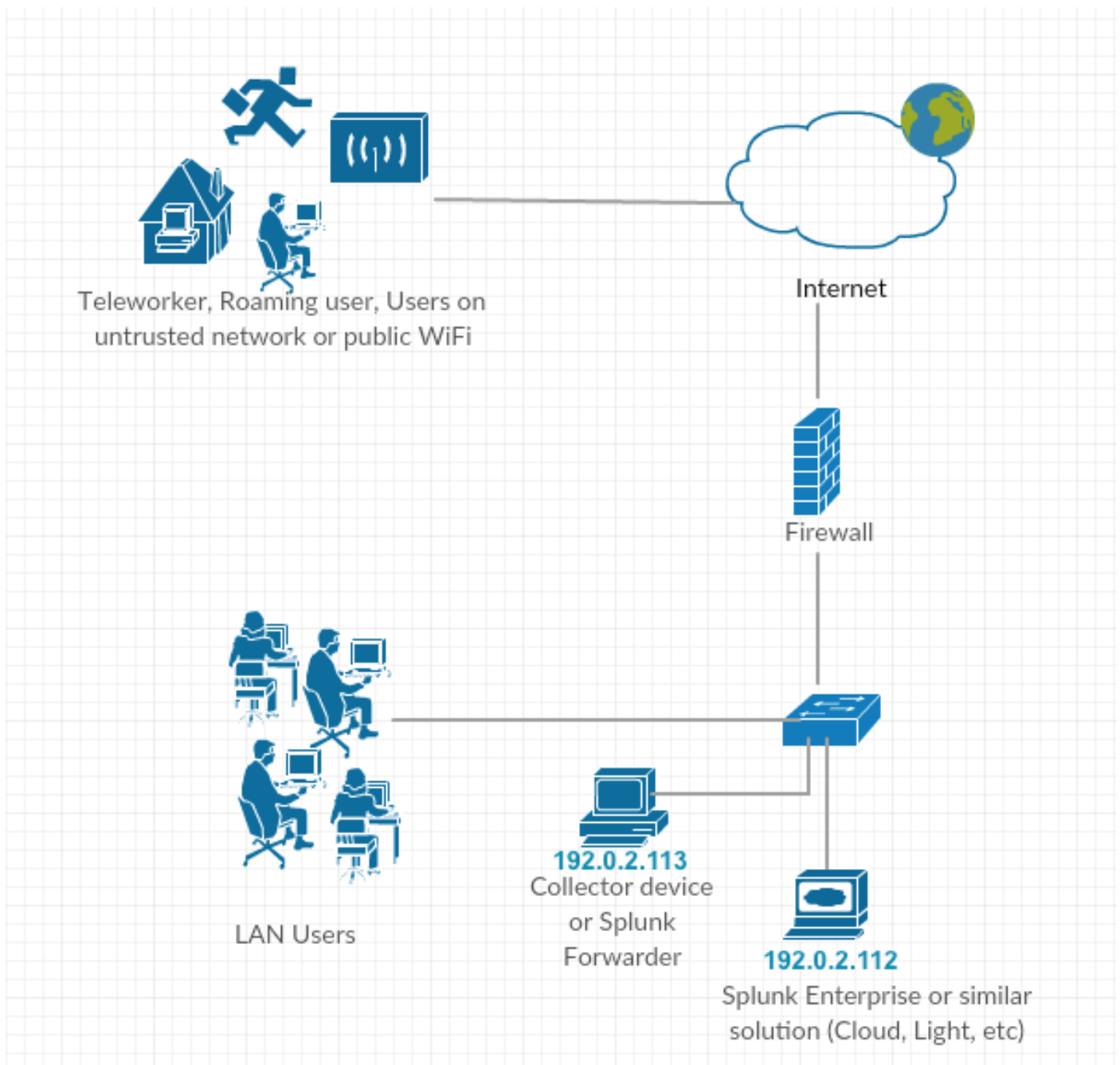
Splunk

Splunk是收集并且分析诊断数据提供关于IT基础设施的有意义的信息的一个强大的工具。它为管理员提供一个一次停顿的位置收集是关键的在了解网络的健康的数据。

Splunk没由Cisco系统拥有也没有维护，然而Cisco为Splunk提供Cisco AnyConnect NVM App。

关于怒意的更多信息，请访问他们的网站。

拓扑



在此technote的IP地址惯例：

收集器IP地址：192.0.2.123

Splunk IP地址：192.0.2.113

Configure

此部分包括Cisco NVM组件的配置。

Anyconnect NVM客户端配置文件

Anyconnect NVM配置在包含关于收集器IP地址和端口号的信息的XML文件被储存，与其他信息一起。收集器IP地址和端口号在NVM客户端配置文件需要正确地配置。

对于NVM模块的正确的操作，在此目录要求XML文件安置：

- Windows 7及以后：%ALLUSERSPROFILE% \ Cisco \ Cisco AnyConnect安全移动客户端\ NVM
- Mac OSX：/opt/cisco/anyconnect/nvm

如果配置文件是存在Cisco ASA/Identity服务引擎(ISE)，则与Anyconnect NVM配置一起自动配置。

XML配置文件示例：

```
<?xml version="1.0" encoding="UTF-8"?>
-<NVMPProfile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="NVMPProfile.xsd">
-<CollectorConfiguration>
<CollectorIP>192.0.2.123</CollectorIP>
<Port>2055</Port>
</CollectorConfiguration>
<Anonymize>false</Anonymize>
<CollectionMode>all</CollectionMode>
</NVMPProfile>
```

使用两个不同的工具，NVM配置文件可以被创建：

- Cisco ASDM
- Anyconnect配置文件编辑器

通过ASDM配置NVM客户端配置文件

如果Anyconnect NVM通过Cisco ASA，配置此方法是更可取的。

1. 连接对Configuration>去除接入VPN >网络(客户端)访问> Anyconnect客户端配置文件

2. 点击添加

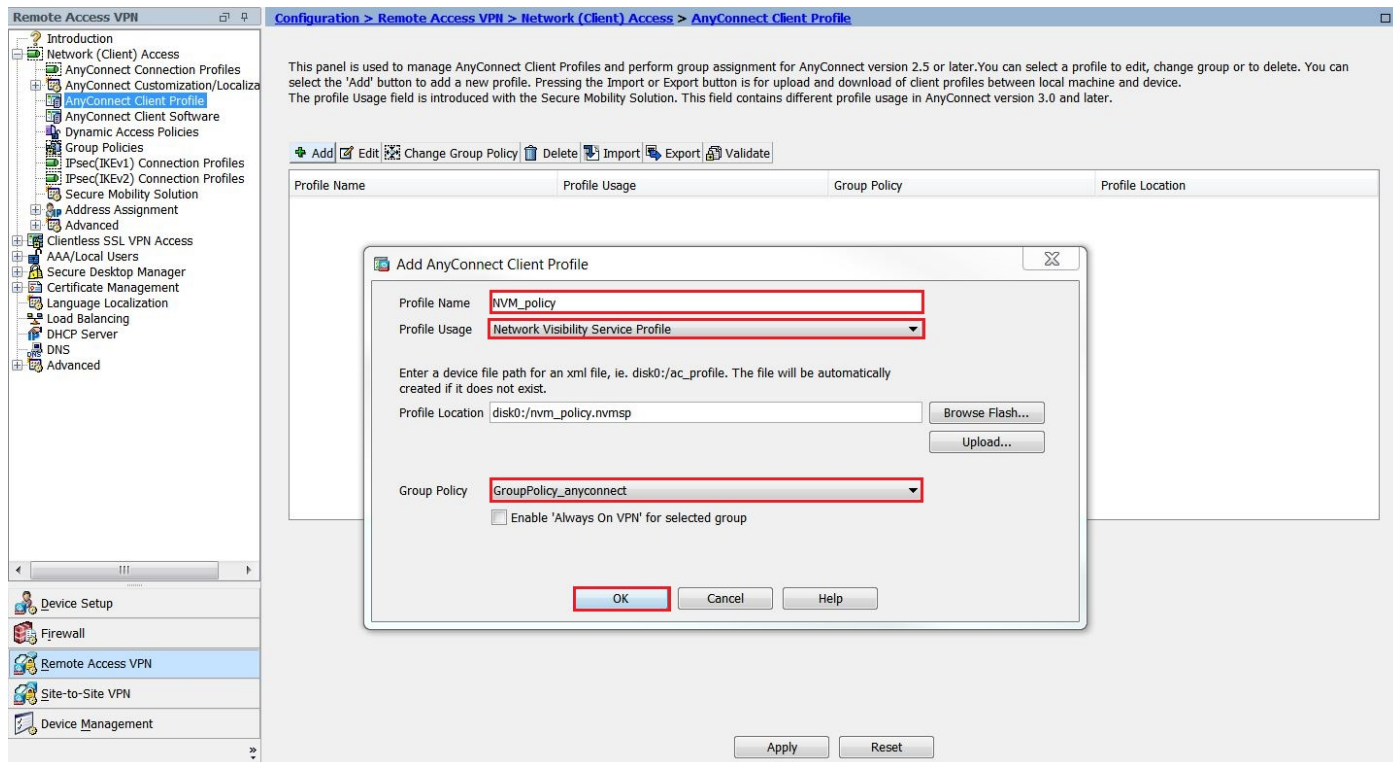
The screenshot shows the Cisco ASDM configuration interface. The breadcrumb path is Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. The main panel contains a table for managing profiles. The 'Add' button is highlighted with a red box.

Profile Name	Profile Usage	Group Policy	Profile Location

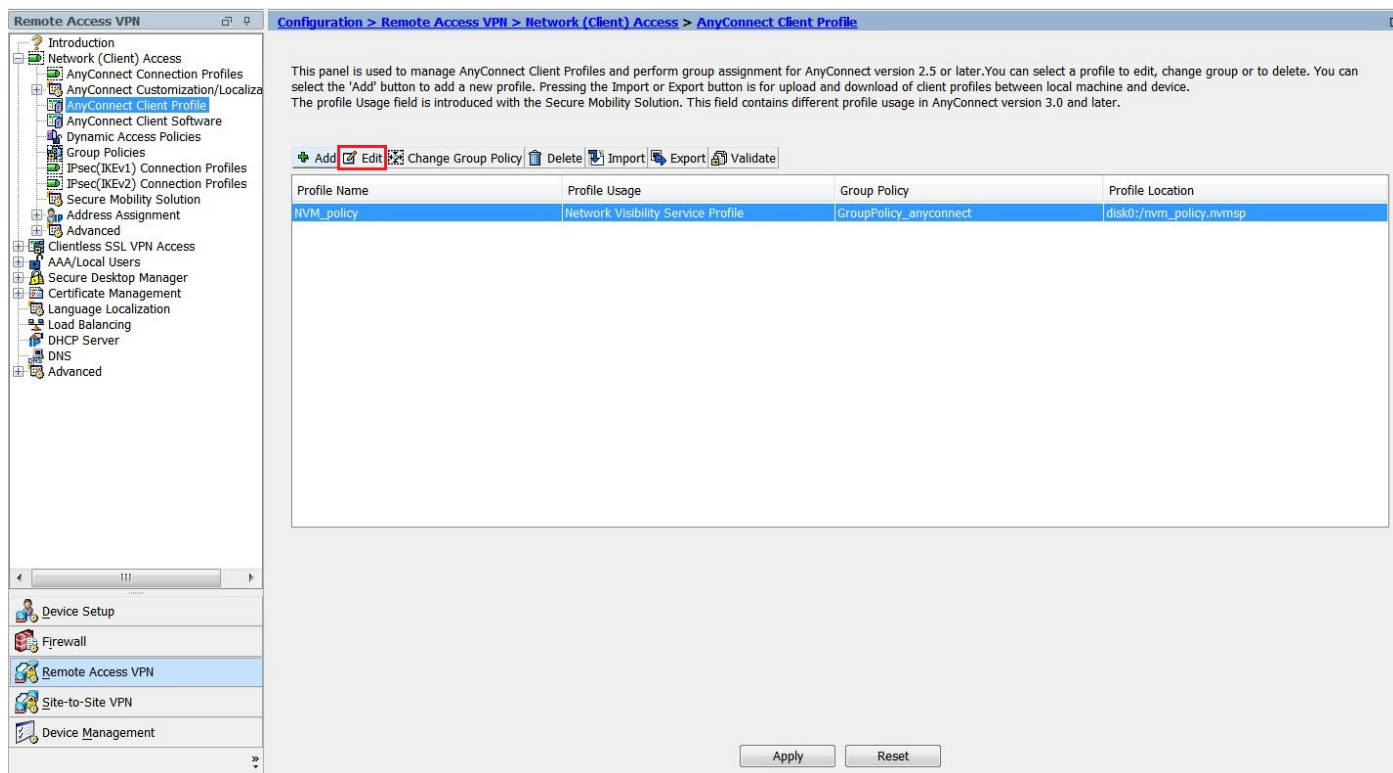
Buttons at the bottom: Apply, Reset

3. 给予配置文件一个名字。在配置文件使用方法，请选择网络可见度服务档案

4. 分配它到Anyconnect用户使用的组策略。单击 Ok。

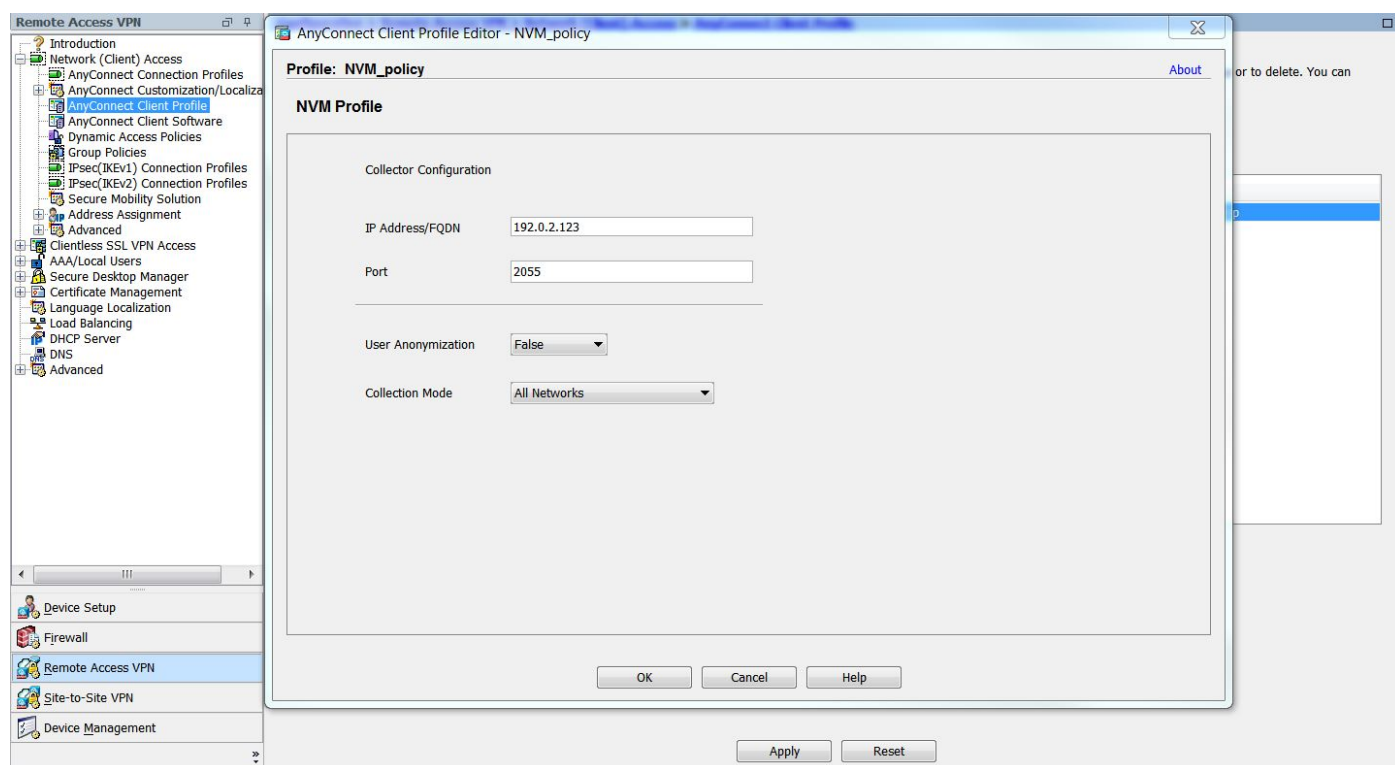


5. 新的策略被创建。点击编辑



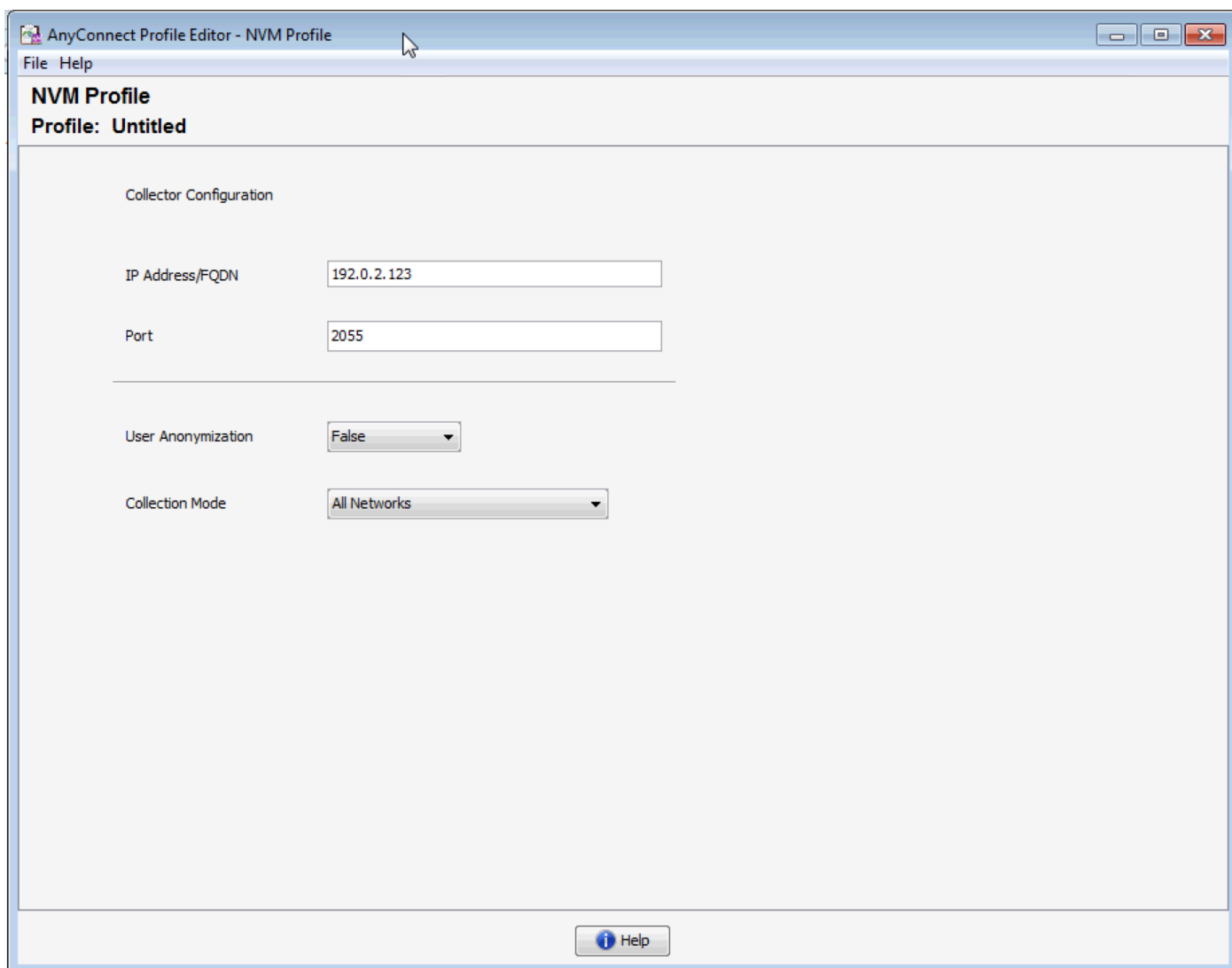
6. 填写关于收集器IP地址和端口号的信息。单击 Ok。

7. 单击 Apply。



通过Anyconnect配置文件编辑器配置NVM客户端配置文件

这是一个独立工具可用在Cisco.com。如果Anyconnect NVM通过Cisco ISE，配置此方法是更可取的。使用此工具被创建的NVM配置文件可以被加载到Cisco ISE或者被复制直接地到终端。



关于Anyconnect配置文件编辑器的详细信息，请参见以下：

[AnyConnect配置文件编辑器](#)

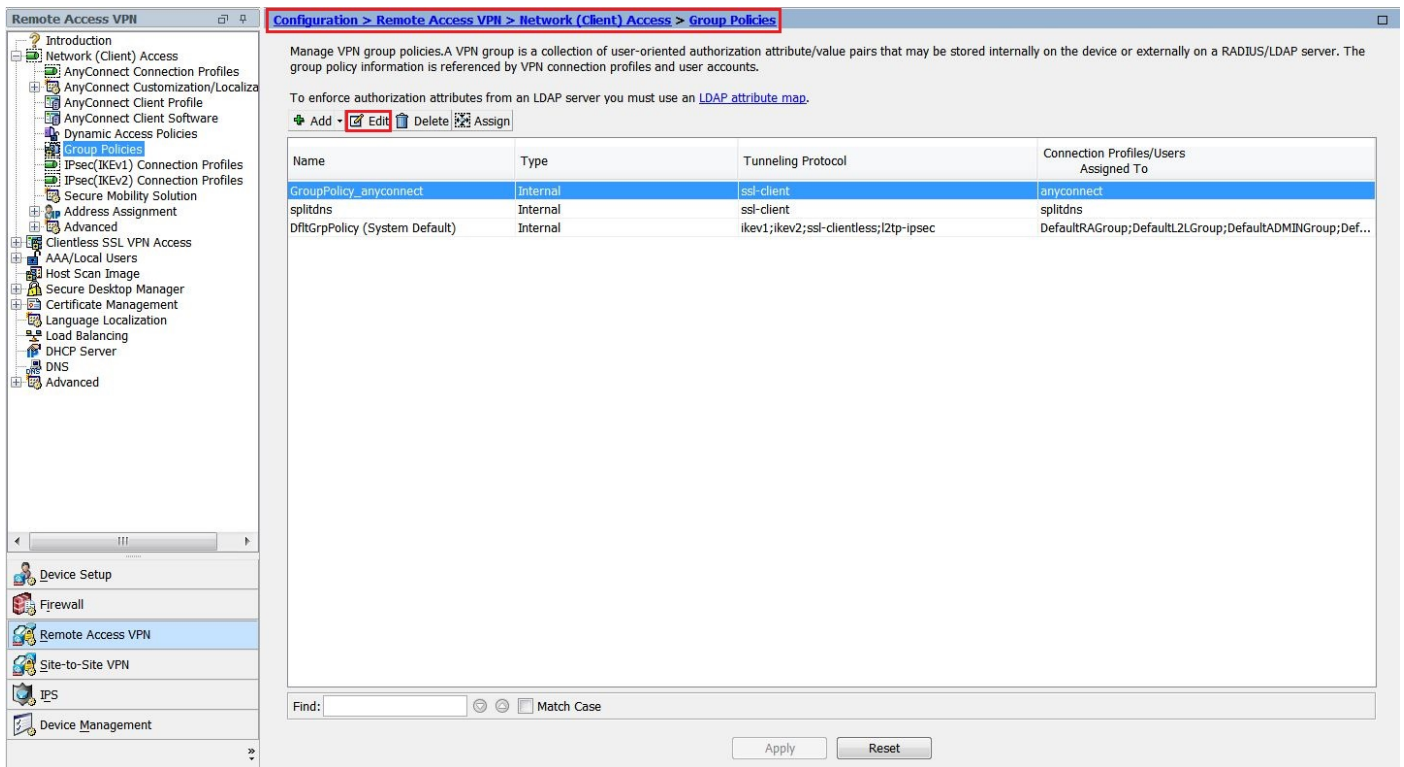
配置在Cisco ASA的Web配置

此technote假设，Anyconnect在ASA已经被配置，并且NVM仅模块配置需要被添加。关于ASA Anyconnect配置的详细信息，请参见以下：

[ASDM书3：Cisco ASA系列VPN ASDM配置指南，7.5](#)

为了enable (event)在Cisco ASA的Anyconnect NVM模块，执行这些步骤：

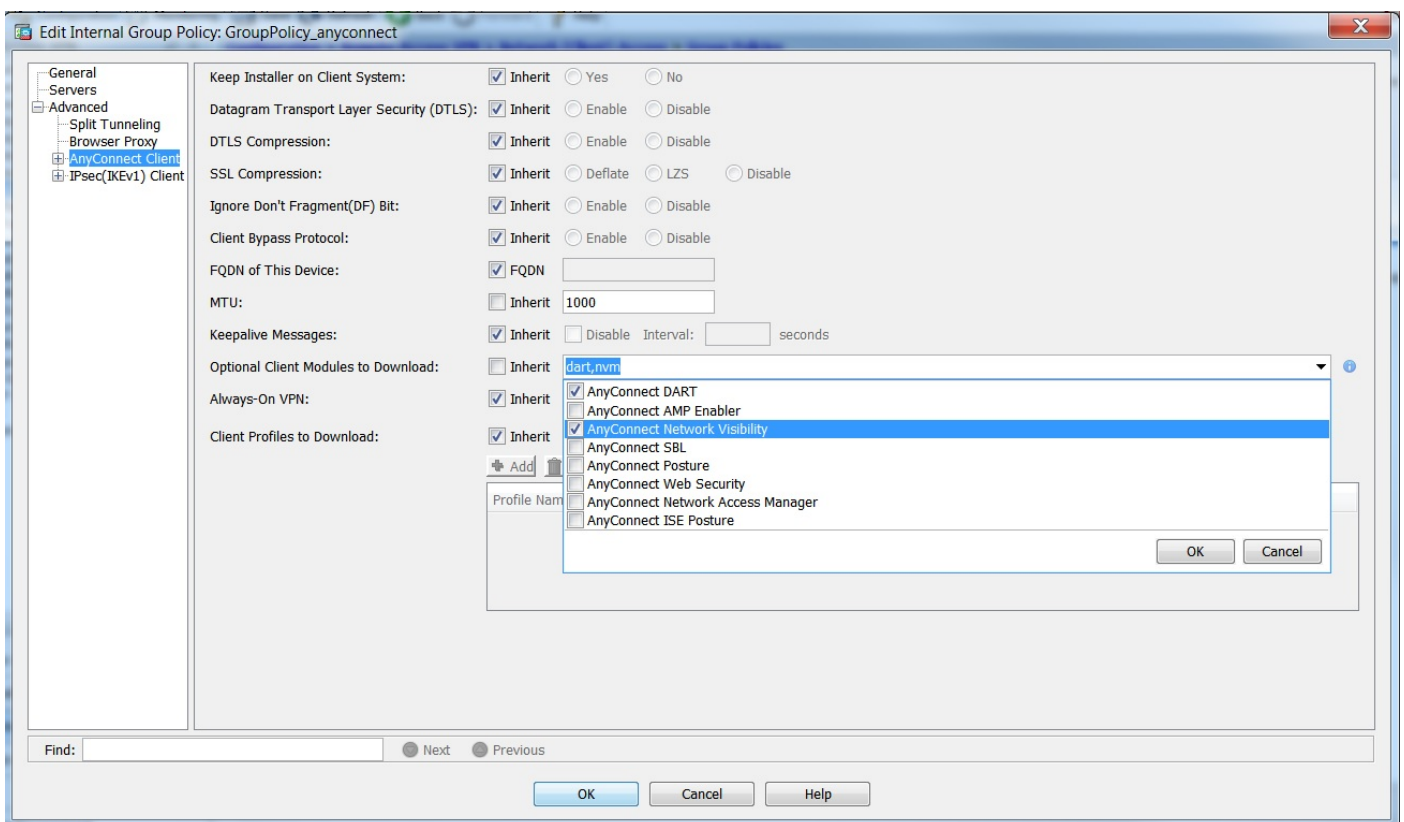
1. 连接对**Configuration>远程访问VPN >网络(客户端)访问>组策略**
2. 选择相关组策略并且点击**编辑**



3. 在组策略上推内，请连接对先进> Anyconnect客户端。

4. 扩展可选的客户端模块下载和选择Anyconnect网络可见度。

5. 点击OK键并且应用更改。



配置在Cisco ISE的Web配置

- 为了配置Anyconnect Web配置的Cisco ISE，请执行这些步骤：

- 在Cisco ISE GUI中，请连接对策略>Policy元素>结果
- 扩展客户端设置显示资源，并且选择资源

添加Anyconnect镜像

选择Add>代理程序资源，并且加载Anyconnect程序包文件。

The screenshot shows the Cisco ISE GUI interface. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers. The main menu includes Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements. The 'Results' tab is selected, showing 'Agent Resources From Local Disk'. A file named 'anyconnect-win-4.2.02075-k9.pkg' is selected. Below, a table titled 'AnyConnect Uploaded Resources' shows the file details. A 'Submit' button is highlighted.

Name	Type	Version	Description
AnyConnectDesktopWindows 4.2.207...	AnyConnectDesktopWindows	4.2.2075.0	AnyConnect Secure Mobility Clien...

确认在上推的程序包的哈希。

FILE HASH可以被验证Cisco.com下载页或使用第三方工具。

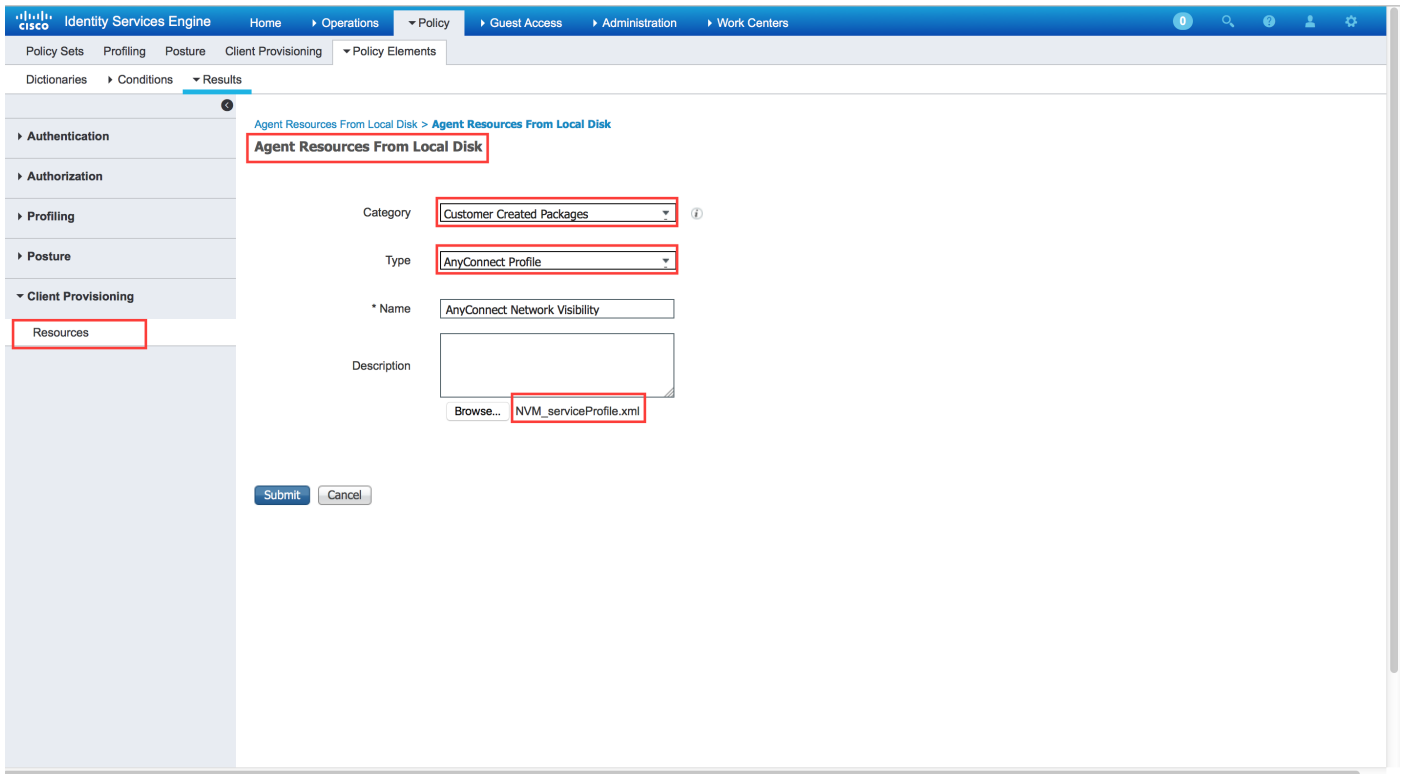
此步骤可以被重复添加多个Anyconnect镜像。(Mac OSX和Linux OS)

Please confirm this package's hash matches :
SHA-1: bbce54f3fdda9a0c9d15b9331a79620e42a96b77
SHA-256: af8751ba5dedb48ca4106a71dbbdf00ccc825e4007f6180259c44e59570d9d8a

Confirm Cancel

添加Anyconnect NVM配置文件：

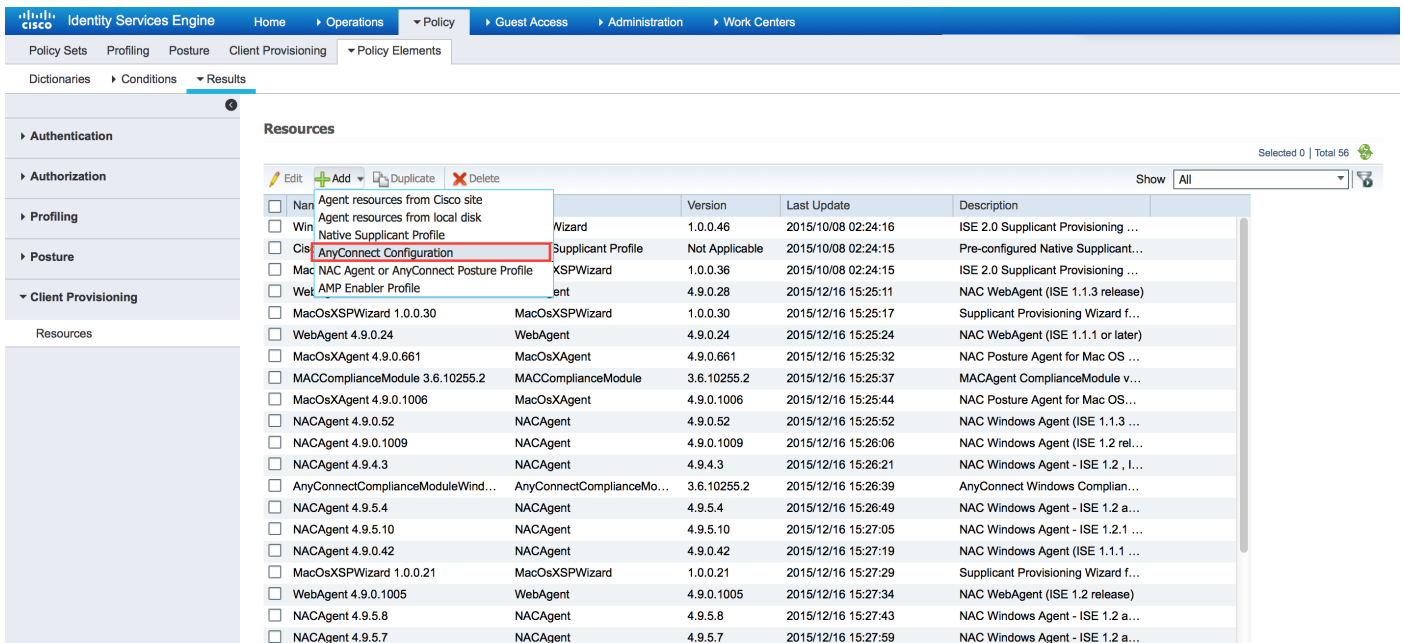
选择Add>代理程序资源，并且加载NVM客户端配置文件。



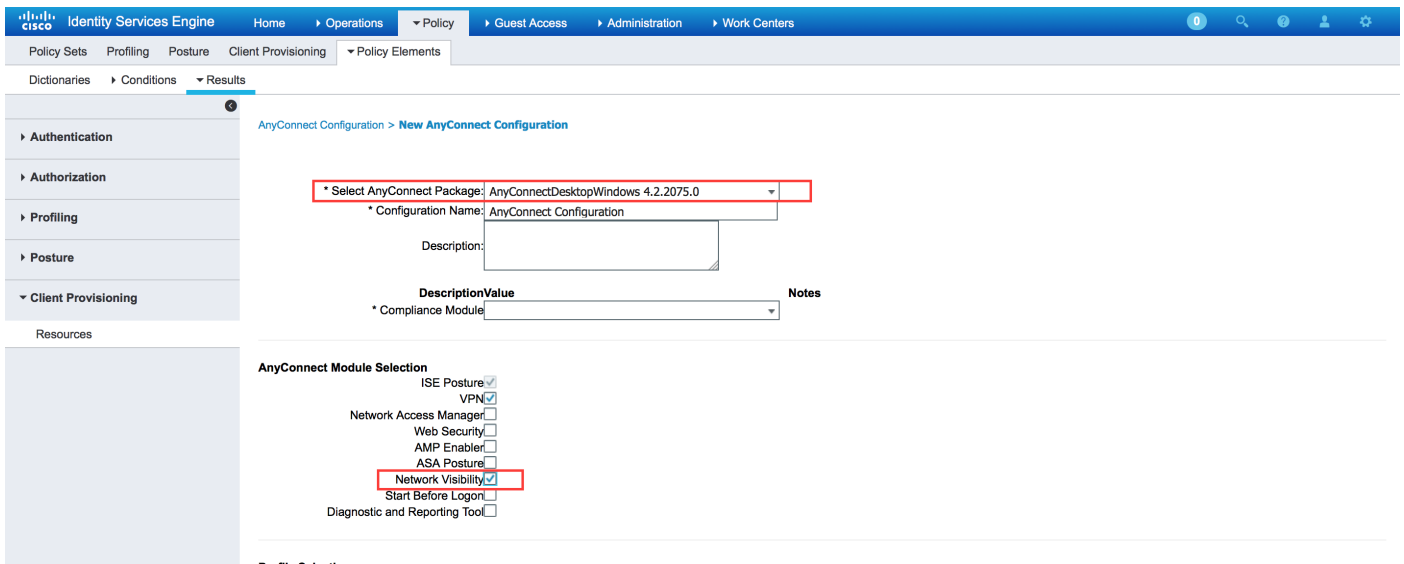
添加Anyconnect配置文件：

选择Add> AnyConnect配置

选择在上一步加载的程序包。



在AnyConnect模块选择的Enable (event) NVM与需要的策略一起。



在上述部分，我们enable (event) AnyConnect客户端模块，配置文件、定制/语言程序包和Opswat程序包。

关于在Cisco ISE的Web配置配置的详细信息，请参见以下：

[Web配置AnyConnect](#)

可信的网络检测

只有当在一个可信的网络时，NVM发送流信息。它使用Anyconnect客户端TND功能了解终端是否在一个可信的网络。TND使用DNS/domain信息确定终端是否在一个可信的网络。当VPN被连接时，认为在一个可信的网络，并且流信息被发送到收集器。

TND需要为正确作用NVM正确地被配置。关于在TND配置的资料，请参见以下：

[配置可信的网络检测](#)

配置

配置Anyconnect NVM解决方案包括这些步骤：

1. 配置在Cisco ASA/ISE的Anyconnect NVM
2. 设置IPFIX收集器组件
3. 设置Splunk和Cisco NVM App

步骤1.配置在Cisco ASA/ISE的Anyconnect NVM

此步骤在配置部分详细报道了。

一旦NVM在Cisco ISE/ASA被配置，可以自动配置到客户端终端。

步骤2.设置IPFIX收集器组件

收集器组件对收集和转换所有IPFIX数据从终端和转发它负责到Splunk App。有可用多种第三方收集器的工具，并且Cisco NVM是与了解IPFIX的所有收集器兼容。此technote使用运行在64位Linux的Cisco本地出产的收集器工具。CentOS和Ubuntu配置脚本被包括在splunk应用程序中。CentOS安装脚本和配置文件可能也用于浅顶软呢帽和Redhat分配。在运行在64位Linux的一个独立64位Linux系统或Splunk转发器应该运行收集器。

为了安装您将需要复制在CiscoNVMCollector_TA.tar文件的应用程序的收集器，位于\$APP_DIR\$/appserver/addon/目录对您计划安装它的系统。

Splunk，此technote的，在E的Windows工作站上安装：驱动。

CiscoNVMCollector_TA.tar文件可以位于以下目录：

```
E:\Program Files\Splunk\etc\apps\CiscoNVM\appserver\addon\
```

抽出在您计划安装收集器和执行install.sh脚本有超级用户权限的系统的TAR文件。推荐在执行install.sh脚本前读在.tar套件的\$PLATFORM\$_README文件。\$PLATFORM\$_README文件在需要确认并修正的相关配置设置提供信息(如果需要)，在install.sh脚本被执行前。

在Ubuntu服务器的收集器目录：

```
root@ubuntu-splunkcollector:~/Downloads/CiscoNVMCollector_TA$ ls
acnvmcollector  CENTOS_README          libboost_log.so.1.57.0
acnvmcollectord  install_centos.sh      libboost_system.so.1.57.0
acnvm.conf      install.sh              libboost_thread.so.1.57.0
acnvm.conf~     install_ubuntu.sh      UBUNTU_README
acnvm.service   libboost_filesystem.so.1.57.0
root@ubuntu-splunkcollector:~/Downloads/CiscoNVMCollector_TA$
```

信息需求在配置文件(acnvm.conf)被配置：

1. IP地址和Splunk实例监听端口。
2. 收集器的(流入IPFIX数据)监听端口。

每个流数据端口，终端身份数据端口和收集器端口预先配置对在配置文件的默认设置。保证更改这些值，如果使用非默认端口。

此信息在配置文件(acnvm.conf)被添加：

```
GNU nano 2.2.6                               File: acnvm.conf

{
"syslog_server_ip" : "192.0.2.113",
"syslog_flowdata_server_port" : 20519,
"syslog_sysdata_server_port" : 20520,
"netflow_collector_port" : 2055,
"log_level" : 7
}
```

欲知更多信息，请参见以下：

<https://splunkbase.splunk.com/app/2992/#/documentation>

步骤3.与Cisco NVM App的设置Splunk

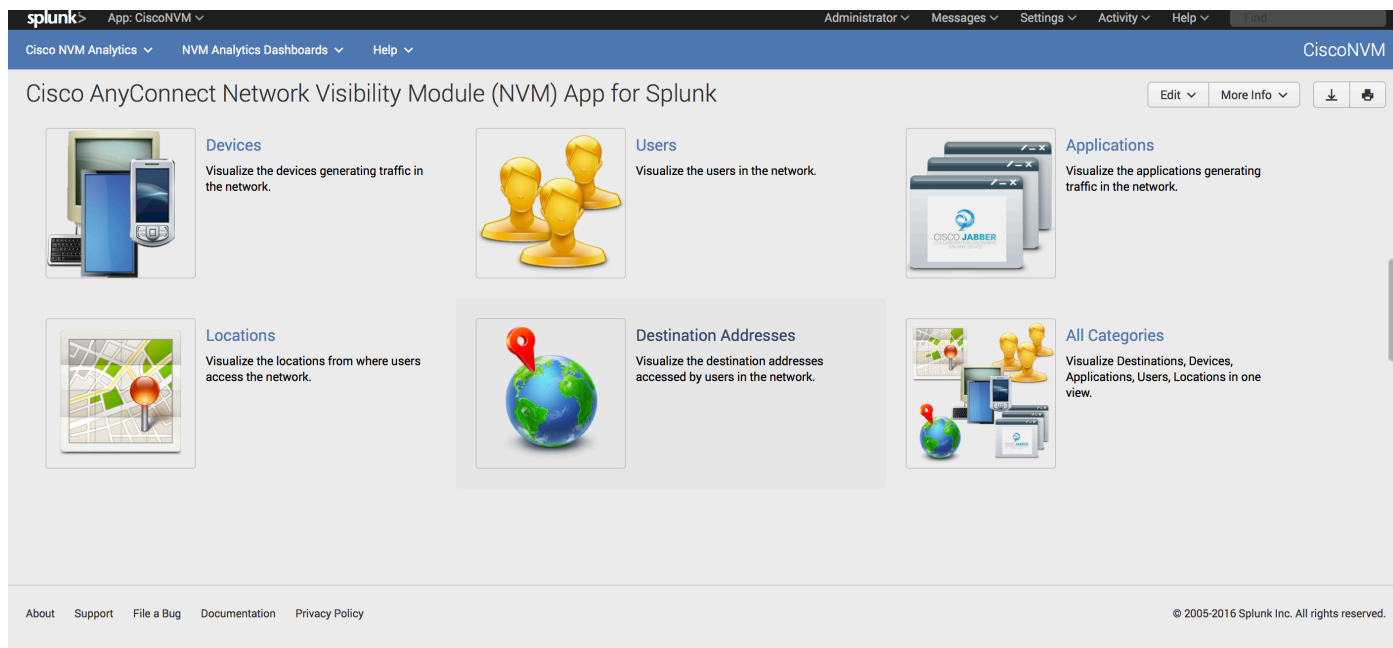
Cisco AnyConnect Splunk的NVM App是可用的在Splunkbase。此app在可用的报道帮助与预定义的报告和显示板使用从端点的IPFIX (nvzFlow)数据，并且关联用户和终端工作情况。

Cisco的在Splunkbase的NVM App链路：

<https://splunkbase.splunk.com/app/2992/>

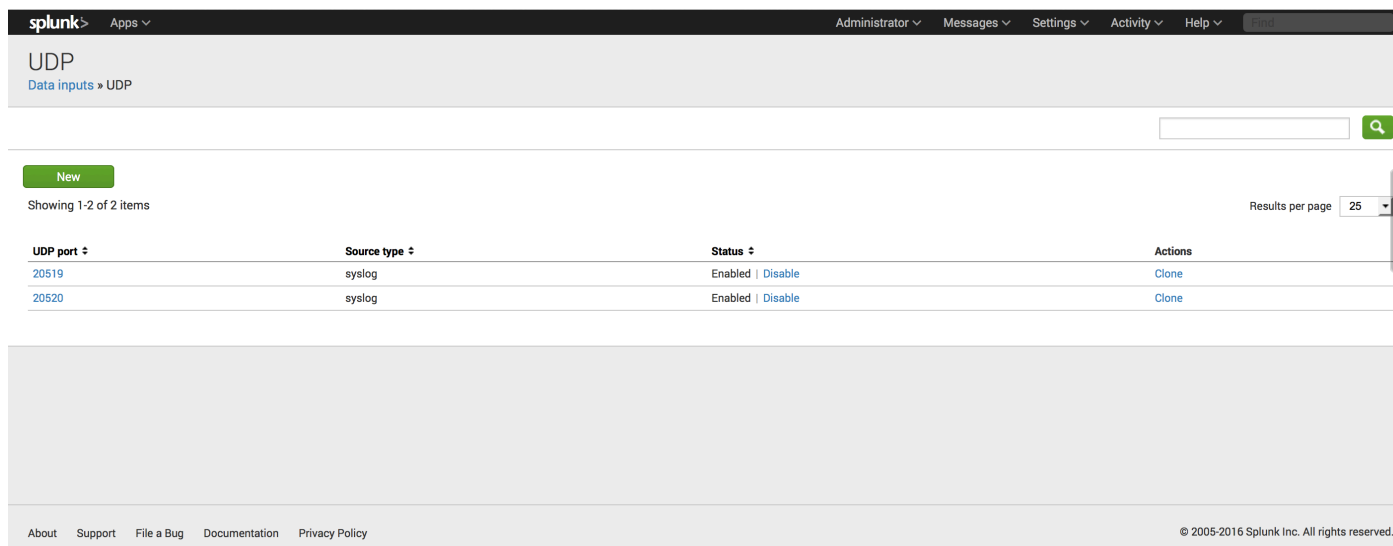
安装：

连接对Splunk > Apps并且安装从Splunkbase下载的tar.gz文件或搜索在Apps部分内。



默认情况下， Splunk分别接受每流数据和终端身份数据的两数据输入结转，关于UDP端口20519和20520。默认情况下收集器组件发送在这些端口的这些结转。默认端口在splunk可以更改，但是相同端口在收集器配置也需要指定(请参阅第2)步

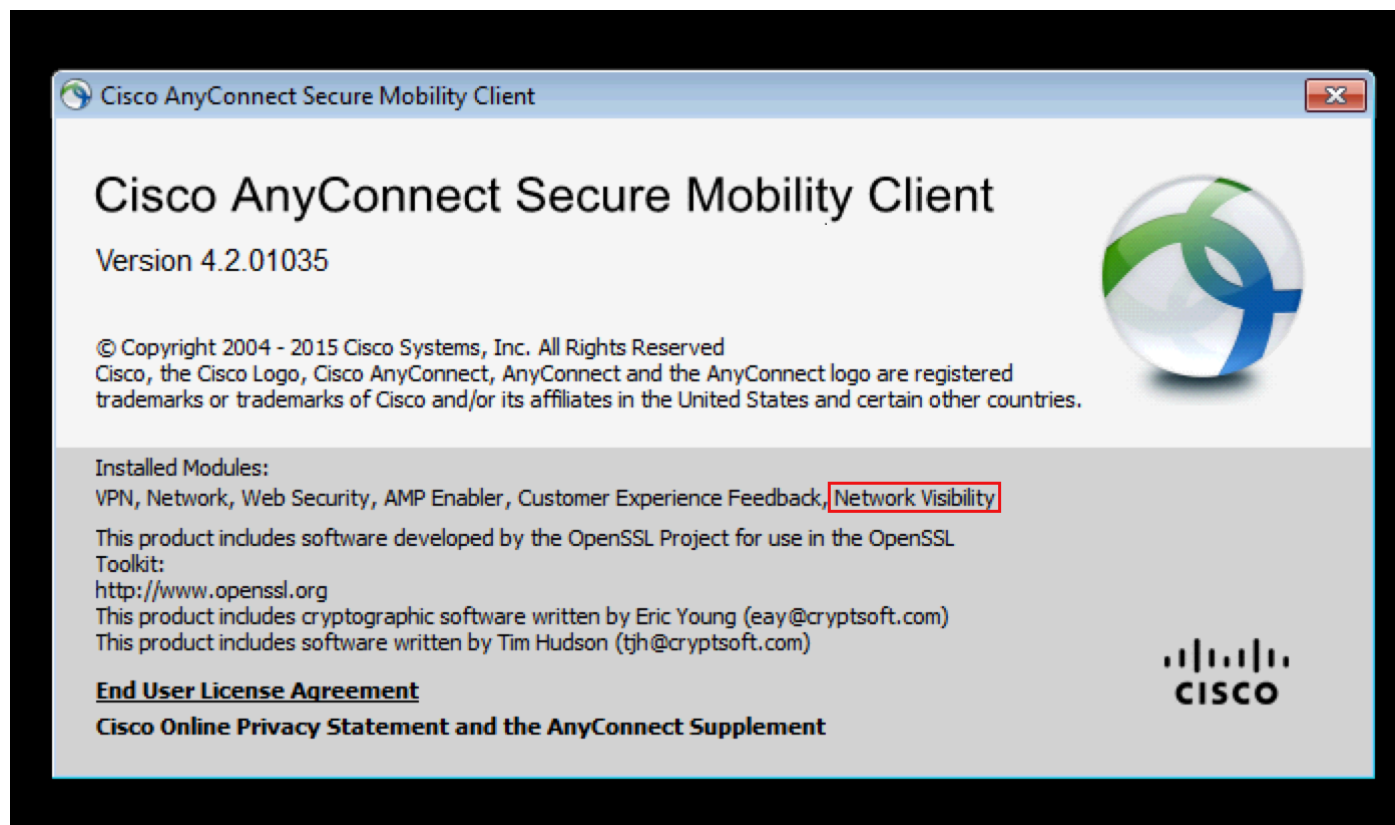
为了更改默认端口，请连接对Splunk >设置>数据输入> UDP



Verify

验证Anyconnect NVM安装

在成功的安装以后，在**安装模块**应该列出网络可见度模块，内在Anyconnect安全移动性客户端的信息部分。



并且，请验证nvm服务是否在终点运行，并且配置文件在必需的目录里。

验证收集器状态如运行

保证收集器状态运行。这保证收集器从终端一直接受IPFIX/cflow。

```
GNU nano 2.2.6                               File: acnvm.conf

{
"syslog_server_ip" : "192.0.2.113",
"syslog_flowdata_server_port" : 20519,
"syslog_sysdata_server_port" : 20520,
"netflow_collector_port" : 2055,
"log_level" : 7
}
```

验证Splunk

保证Splunk和其相关服务运行。关于在排除Splunk故障的文档，请参见他们的网站。

Troubleshoot

信息包流

1. IPFIX信息包在客户端终端生成由Anyconnect NVM模块。
2. 客户端终端转发IPFIX信息包到收集器IP地址
3. 收集器收集信息并且寄它给Splunk
4. 收集器发送数据流到在两不同的流的Splunk：每流数据和终端身份数据

所有数据流是基于的UDP那里是没有数据流的确认。

数据流的默认端口：

IPFIX数据2055

每流数据20519

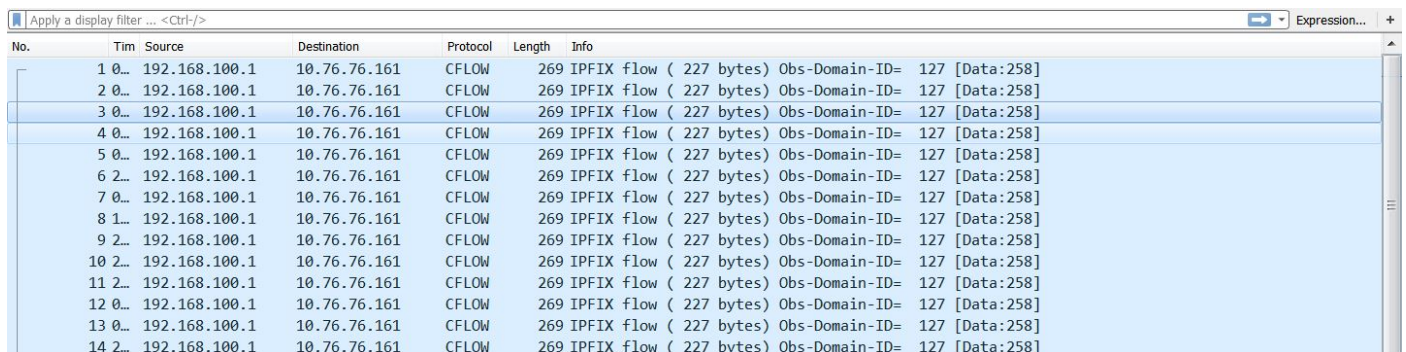
每流数据20520

当在可信的网络时，NVM模块缓存IPFIX数据并且发送它到收集器。这可以二者之一是，当膝上型计算机被连接到公司网络时(在prem)或，当通过VPN时被连接。

基本排除步骤故障

- 保证客户端终端和收集器之间的网络连通性。
- 保证收集器和splunk之间的网络连通性。
- 保证NVM在客户端终端上正确地安装。
- 适用在终端的捕获发现IPFIX数据流是否生成。
- 适用在收集器的捕获发现是否收到IPFIX数据流，并且是否寄数据流给Splunk。
- 适用在Splunk的捕获发现是否收到数据流。

如在Wireshark中看到的IPFIX数据流：



The image shows a Wireshark packet capture window with a display filter set to 'Apply a display filter ... <Ctrl-/>'. The packet list pane shows 14 packets, all of which are IPFIX flow records. Each record is 269 bytes long and originates from 192.168.100.1 and is destined for 10.76.76.161. The protocol is CFLOW. The information field for each packet is '269 IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]'. The packet bytes pane is currently empty.

No.	Time	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]

可信的网络检测(TND)

当终端在可信的网络内时，NVM依靠发现的TND。如果TND配置是不正确的，这将导致NVM的问题。

根据信息的TND工作获得通过DHCP : domain-name和DNS服务器。如果DNS服务器和domain-name匹配配置的值，则网络视为委托。

如果NVM不寄数据流给收集器，则它可能是TND的一个问题。

流模板

IPFIX流模板被发送到收集器在IPFIX通信的开始。这些模板帮助收集器有意义IPFIX数据。如果此信息没有被发送到收集器，则收集器不能收集IPFIX数据。这导致数据收集的问题。

这样问题被看到是否以后配置收集器，或者最初的少数IPFIX信息包是否在网络被丢弃(普通在VPN)。为了缓和此，其中一个下面的事件应该发生：

1. 有在NVM客户端配置文件上的一个变化。
2. 有网络更改事件。
3. nvmagent服务被重新启动。
4. 重新启动终点/被重新启动。

此问题可以通过重新启动终端或者重新连接VPN恢复。

问题不可以由观察在终点的信息包获取找到的模板，或者flowset的没有模板确定在收集器日志。

信息包获取

```
└─ Cisco NetFlow/IPFIX
  Version: 10
  Length: 225
  └─ Timestamp: Jan 20, 2016 16:09:31.000000000 Eastern Standard Time
    FlowSequence: 256577
    Observation Domain Id: 127
    └─ Set 1 [id=258]
      FlowSet Id: (Data) (258)
      FlowSet Length: 209
      └─ Data (205 bytes), no template found
        └─ [Expert Info (Warn/Malformed): Data (205 bytes), no template found]
```

收集器日志：

```
GNU nano 2.2.6                               File: acnvm.conf

{
"syslog_server_ip" : "192.0.2.113",
"syslog_flowdata_server_port" : 20519,
"syslog_sysdata_server_port" : 20520,
"netflow_collector_port" : 2055,
"log_level" : 7
}
```

推荐的版本

Cisco在使用或更新时总是推荐AnyConnect最新的软件版本。当选择AnyConnect版本时，请使用最新的4.2.x或4.3.x客户端。这将产生与reselect NVM的最新的增进，故障修正，并且缓和与Microsoft的最近更改请编码签署的证书实施。[这里更多详细资料。](#)

相关问题

1. [CSCva21660](#) - Anyconnect NVM把柄/acnvmagent.exe*32进程的泄漏

相关链接

1. Cisco AnyConnect网络可见度(NVM) Splunk的App
: <https://splunkbase.splunk.com/app/2992/>
2. 在Splunk收集器设置和安装收集器脚本的Splunk文档
: <https://splunkbase.splunk.com/app/2992/#/documentation>
3. [Cisco AnyConnect安全移动客户端管理员指南，版本4.3](#)
4. [版本注释AnyConnect 4.3](#)