為CESA配置AnyConnect NVM和Splunk

目錄

簡介

本文檔介紹如何在運行AnyConnect 4.7.x或更高版本的終端使用者系統上安裝和配置Cisco AnyConnect網路可視性模組(NVM)，以及如何安裝和配置關聯的Splunk企業元件和NVM收集器。

必要條件

需求

思科建議您瞭解以下主題：

- 帶NVM的AnyConnect 4.7.x或更高版本
- AnyConnect許可
- 自適應安全裝置管理器(ASDM)7.5.1或更高版本
- 熟悉Splunk Enterprise以及如何安裝Splunk應用和載入項

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco AnyConnect安全移動客戶端4.7.x或更高版本
- Cisco AnyConnect Profile Editor
- 思科調適型安全裝置(ASA)版本9.5.2
- 思科調適型安全裝置管理員(ASDM)版本7.5.1
- Splunk Enterprise 7.x或更高版本(作為一體式安裝在任何支援的Linux平台上；首選CentOS)

- 任何受支援的Linux安裝作為收集器裝置

> 附註：收集器可以在同一台伺服器上運行。有關詳細資訊，請參閱在Splunk快速啟動POV套件和部署指南上構建的思科端點安全分析(CESA)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Cisco AnyConnect NVM提供高價值終端遙測的持續饋送，使組織能夠檢視其網路上的終端和使用者行為。NVM從內部和外部終端以及重要環境（如使用者、應用程式、裝置、位置和目標）收集流量。Splunk Enterprise使用遙測資料並提供分析功能和報告。

本技術說明是作為新的思科端點安全分析(CESA)解決方案的一部分使用Splunk Enterprise的AnyConnect NVM的配置示例。

- 有關使用Splunk的CESA的完整概述價值驗證(POV)，請參閱在Splunk快速啟動POV工具包和部署指南上構建的思科端點安全分析(CESA)。
- 有關Splunk上CESA NVM控制面板的指南，請參閱Cisco Endpoint Security Analytics(CESA)控制面板概述和常見問題。
- 有關解決方案的詳細資訊，請參閱在Splunk構建的思科端點安全分析。

這些元件構成了解決方案：

- 已啟用網路能見性模組(NVM)的Cisco AnyConnect安全行動化使用者端
- 適用於Splunk的思科端點安全分析(CESA)應用
- 適用於Splunk的思科端點安全分析(CESA)附加模組
- NVM收集器（捆綁在zip檔案中和NVM TA載入項）

Cisco AnyConnect Security Mobility Solution — 多於VPN

Cisco AnyConnect是一個統一代理，可提供多種安全服務來保護企業。AnyConnect最常用作企業VPN客戶端，但它也支援其他模組，以滿足企業安全的不同方面。其他模組支援安全功能，如狀態評估、Web安全、惡意軟體防護、網路可視性等。

本技術說明與NVM有關，NVM與Cisco AnyConnect整合使管理員能夠監控終端應用程式使用情況。有關Cisco AnyConnect的詳細資訊，請參閱Cisco AnyConnect安全移動客戶端管理員指南，版本4.7。

網際網路通訊協定流量資訊匯出(IPFIX)

IPFIX是一種IETF協定，它定義了一個用於各種目的（如記帳、審計和安全）的IP流資訊匯出標準。IPFIX基於Cisco NetFlow協定v9，儘管它們不直接相容。Cisco nvzFlow是基於IPFIX協定的協定規範。根據設計，IPFIX是一個可擴展的協定，允許您定義傳送資訊的新引數。Cisco nvzFlow通訊協定延伸了IPFIX標準並定義新的資訊元素。該協定還定義了一組標準IPFIX模板，這些模板作為AnyConnect NVM使用的遙測的一部分進行傳送。

有關IPFIX的詳細資訊，請參閱以下RFC:

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

IPFIX NVM收集器

收集器是接收和儲存IPFIX資料的伺服器。然後，它便可以將這些資料提供給Splunk。

Cisco提供的收集器專為nvzFlow協定設計，並與CESA TA Add-On for Splunk捆綁在一起。收集器可以安裝在Splunk伺服器的同一機箱上（一體式）、重型轉發器上或獨立的Linux機箱上。

有關收集器的更多詳細資訊，請參閱思科網路能見度(NVM)收集器。

Splunk企業版

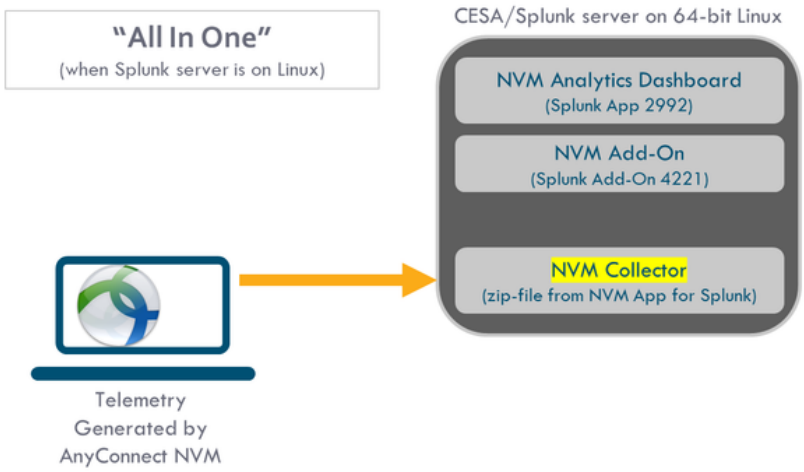
Splunk Enterprise是一個功能強大的工具，可以收集和分析診斷資料，從而提供有關IT基礎架構的有用資訊。它為管理員提供收集資料的一站式位置，幫助他們瞭解網路的運行狀況。

Splunk是思科的合作夥伴，CESA解決方案就是與他們合作建立的。有關詳細資訊，請參閱在Splunk構建的思科端點安全分析。

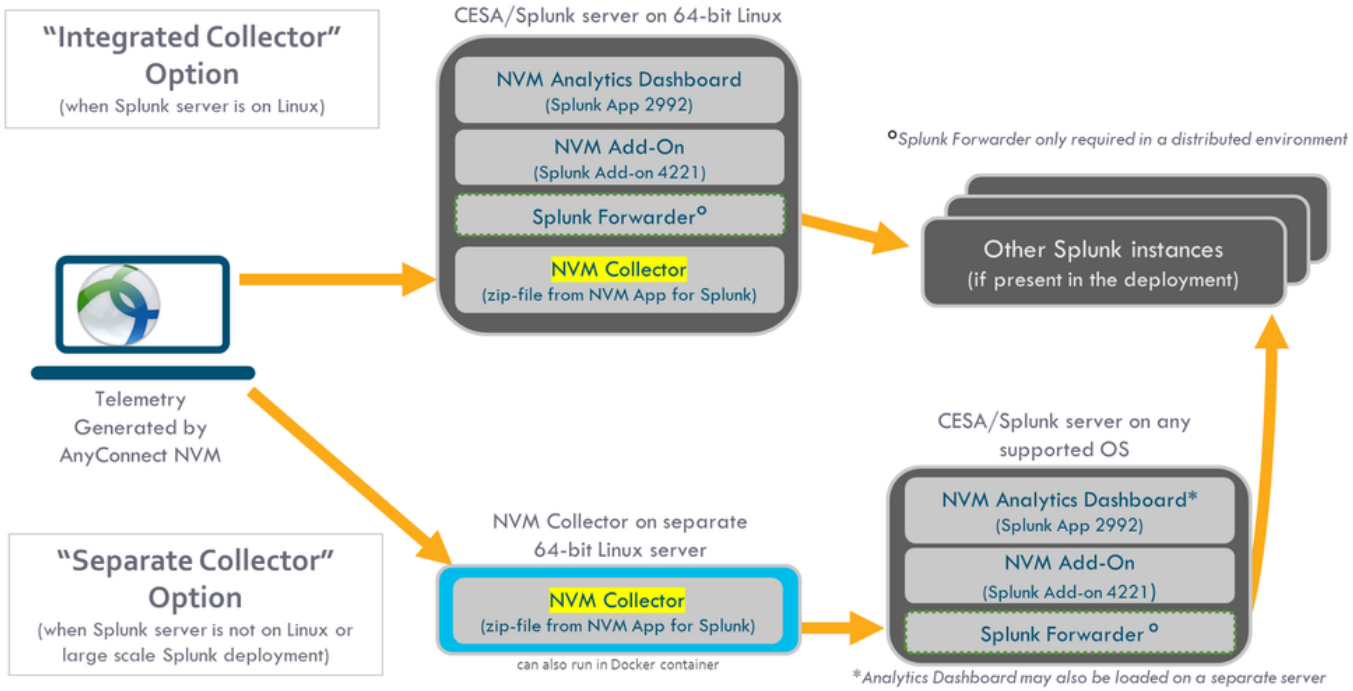
部署概述

本文檔以最簡單的形式簡要概述部署。這是在64位Linux上運行的一體化配置。

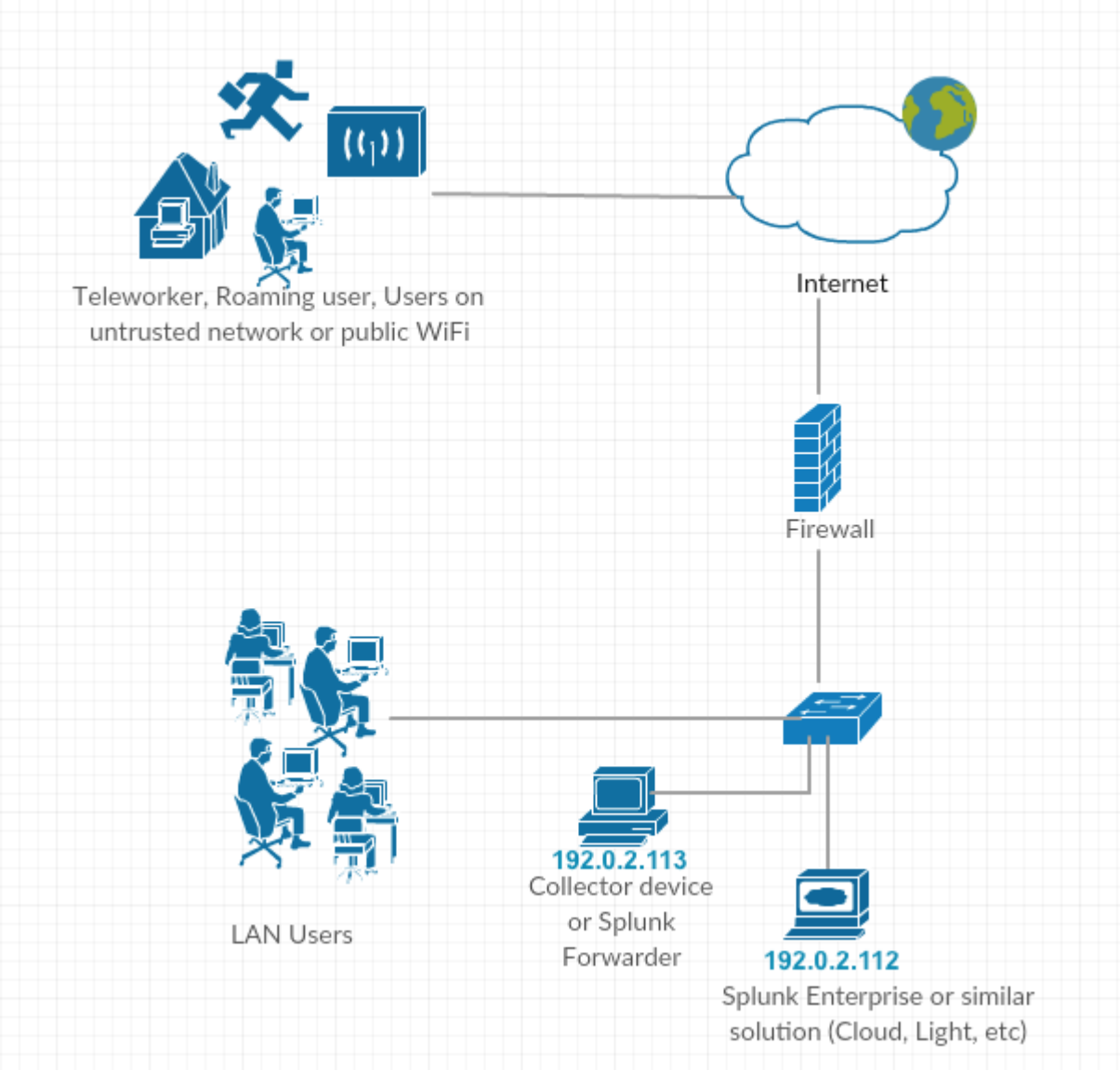
此圖顯示用於大多數演示的配置。此配置在小型生產部署中也很有用。



此圖顯示可用於部署的更全面的選項集。通常，生產設定是分散式的，並且有多個Splunk Enterprise節點。


"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

拓撲



本技術說明中的IP地址約定：

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

設定

本節介紹Cisco NVM元件的配置。有關AnyConnect NVM部署和配置檔案的概述，另請參閱如何實施AnyConnect網路可視性模組。

為DTLS支援配置NVM

現在，可以將NVM配置為通過DTLS將資料安全地傳送到收集器。此模式可在NVM配置檔案編輯器中配置。選中「安全」覈取方塊時，NVM使用DTLS作為傳輸。若要通過DTLS連線，DTLS伺服器（收集器）證書必須受終結點的信任。不信任的證書以靜默方式被拒絕。DTLS 1.2是受支援的最低版本。DTLS支援需要收集器作為CESA Splunk應用v3.1.2或更高版本的一部分。收集器只能在一個模式下工作：安全或不安全。

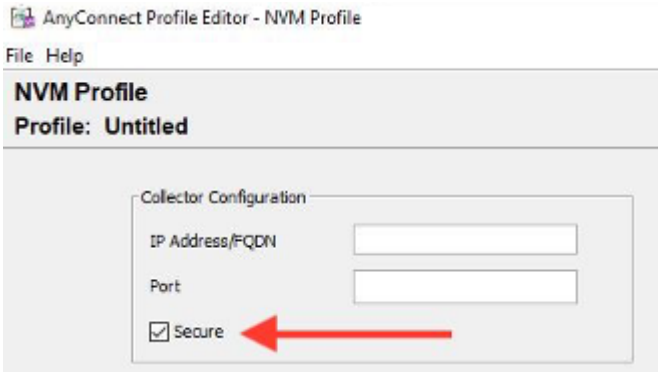
證書要求

- 客戶端必須信任收集器證書。（請確保證書鏈受信任，因為AnyConnect上沒有配置。）
- 證書必須是PEM格式。
- 不支援證書金鑰密碼。附註：思科身分識別服務引擎(ISE)內部憑證授權單位(CA)需要一個。
- 只要AnyConnect客戶端電腦信任任何證書(內部公鑰基礎架構（PKI，眾所周知等），則可以在收集器上使用任何證書。
- 更新配置檔案後，必須重新啟動AnyConnect NVM服務（用於單客戶端測試）。 對於從ISE或自適應安全裝置(ASA)推送的配置檔案，客戶端電腦必須斷開與網路的連線，然後重新連線。

- AnyConnect NVM配置檔案收集器配置應設定為IP或FQDN。此選擇取決於憑證的一般名稱(CN)中使用的是什麼值。在IP地址更改的情況下，始終首選完全限定域名(FQDN)。
    - 如果使用IP地址，則收集器證書CN或使用者替代名稱(SAN)應具有該IP。
    - 如果您的FQDN是證書中的CN，則NVM配置檔案應與收集器具有相同的FQDN。

AnyConnect配置（4.9.3043及更高版本）

對於NVM配置檔案，收集器IP/埠下有一個稱為「安全」的新覈取方塊。



獨立AnyConnect NVM模組

獨立模組需要AnyConnect 4.8.01090或更高版本。請參閱Cisco AnyConnect安全移動客戶端管理員指南4.9版。另請參閱此獨立指南：如何實施AnyConnect網路可視性模組。

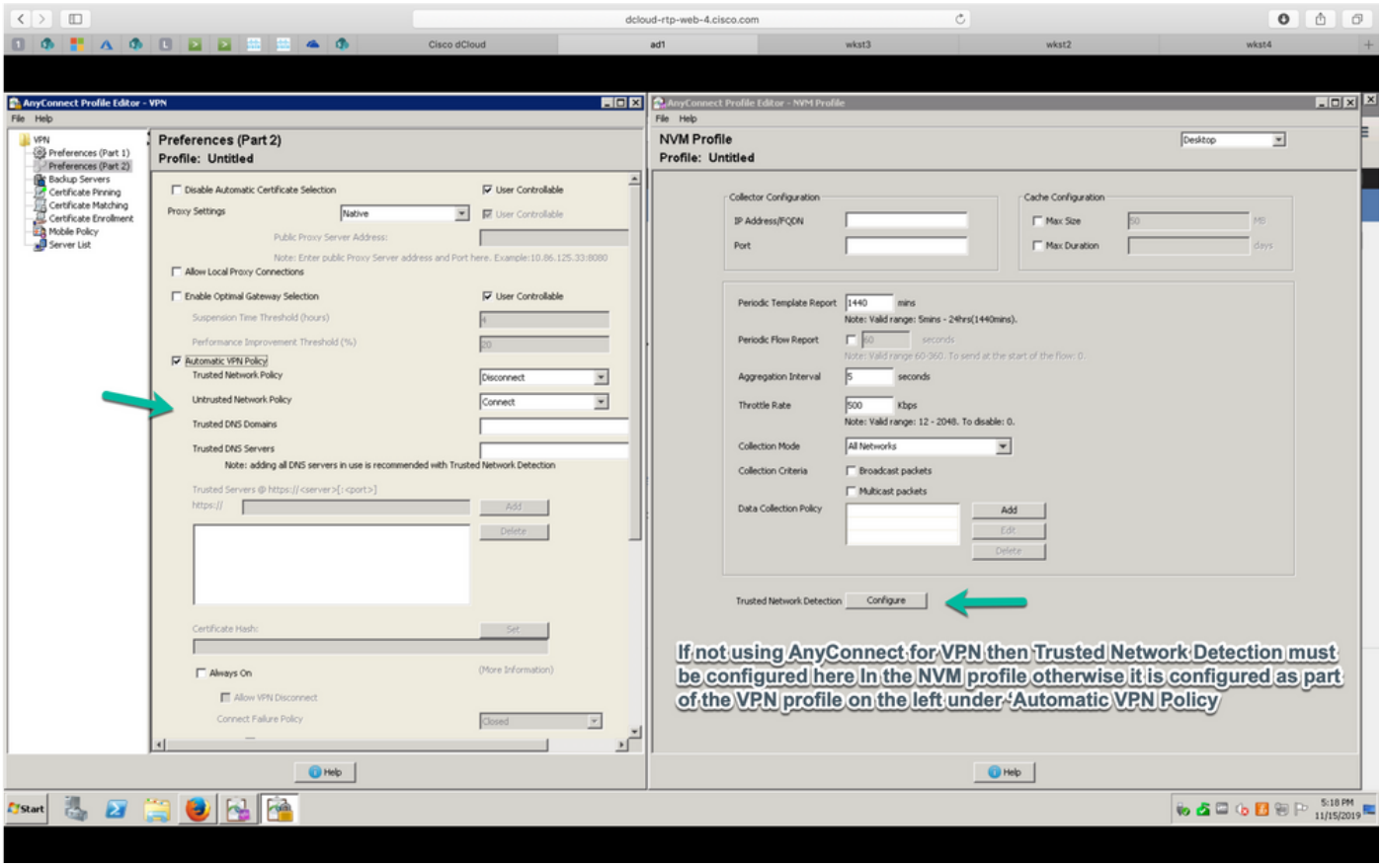
如果您沒有AnyConnect部署或使用另一個VPN解決方案，則可以安裝NVM獨立軟體包以滿足您的NVM需求。此包獨立工作，但提供的流量收集級別與當前AnyConnect NVM解決方案相同。如果安裝獨立NVM，則活動進程(如Macintosh作業系統(macOS)上的活動監視器)指示此用途。

使用NVM配置檔案編輯器配置獨立NVM，並且必須配置受信任網路檢測(TND)。NVM使用TND配置來確定終端是否位於企業網路上，然後應用適當的策略。

故障排除和日誌記錄仍由AnyConnect診斷和報告工具(DART)完成，該工具可以從AnyConnect軟體包安裝。

在提供獨立選項之前，必須安裝核心VPN模組才能充分利用TND。核心VPN圖塊在使用者介面(UI)中可見，這可能使終端使用者感到困惑，尤其是如果他們使用來自其他供應商的VPN解決方案。

使用獨立選項時，不使用核心VPN配置檔案來配置TND。NVM配置檔案現在可以直接配置為TND。



AnyConnect NVM客戶端配置檔案

AnyConnect NVM配置儲存在XML檔案中，該檔案包含有關收集器IP地址和埠號的資訊以及其他資訊。必須在NVM客戶端配置檔案中正確配置收集器IP地址和埠號。

要正確運行NVM模組，必須將XML檔案放置在此目錄中：

- 對於Windows 7及更高版本:%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect安全移動客戶端\NVM
- 對於Mac OSX:/opt/cisco/anyconnect/nvm

如果配置檔案存在於Cisco ASA/ISE上，則它會與AnyConnect NVM部署一起自動部署。

XML配置檔案示例：

<#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>
```

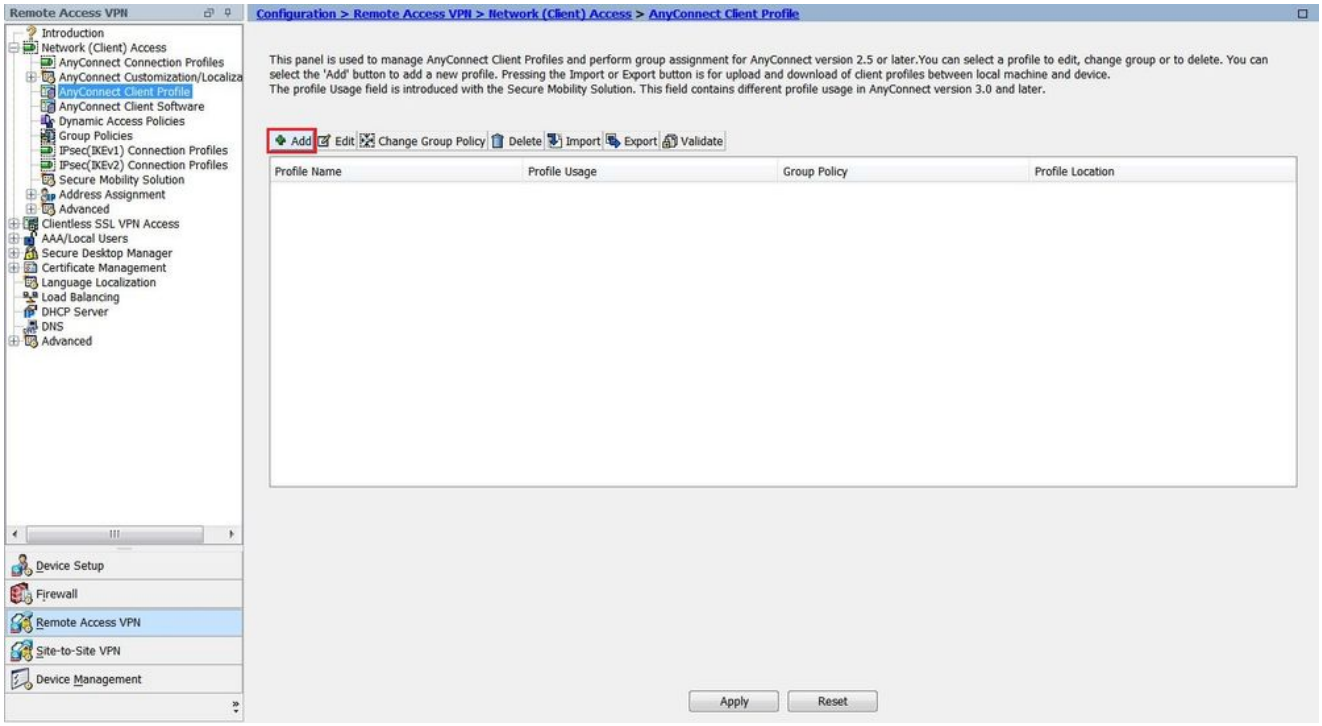
可以使用以下工具建立NVM配置檔案：

- Cisco ASDM
- AnyConnect配置檔案編輯器
- ISE

通過ASDM配置NVM客戶端配置檔案

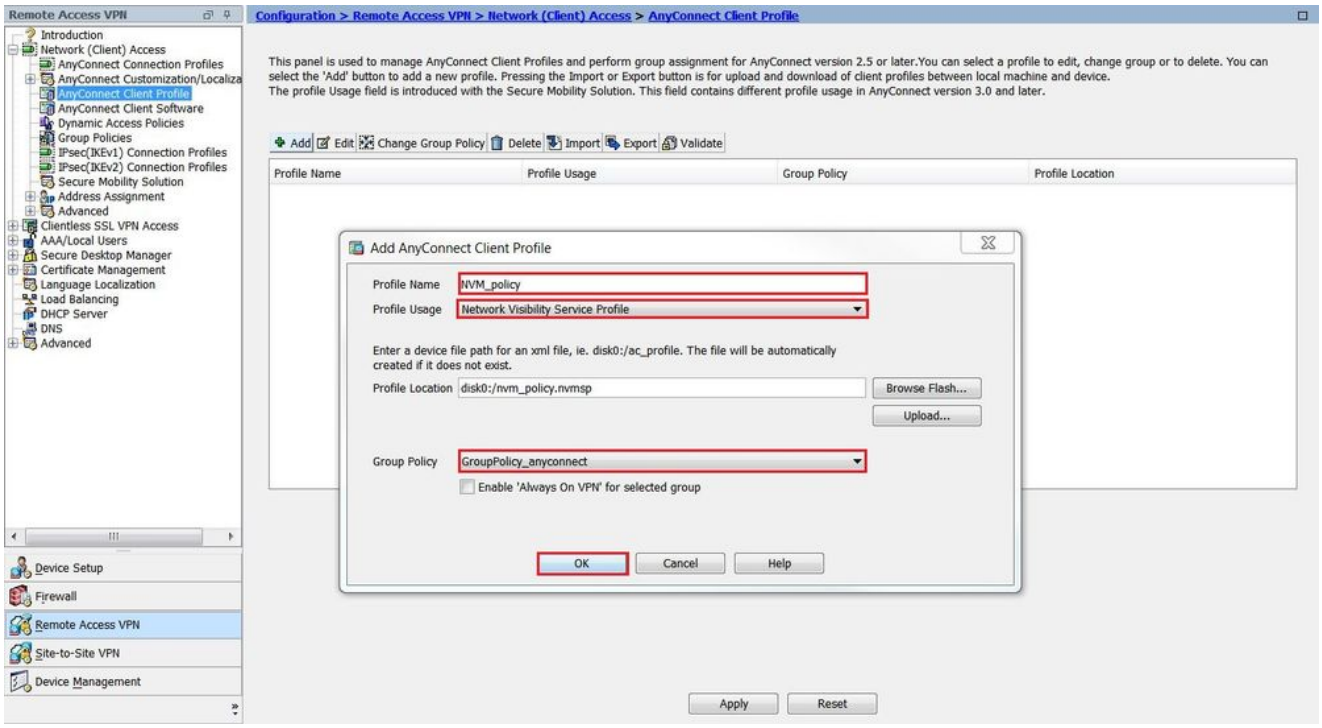
如果通過Cisco ASA部署AnyConnect NVM，則首選此方法：

1. 導航到Configuration > Remove Access VPN > Network(Client)Access > AnyConnect Client Profile。
2. 按一下「Add」，如下圖所示。

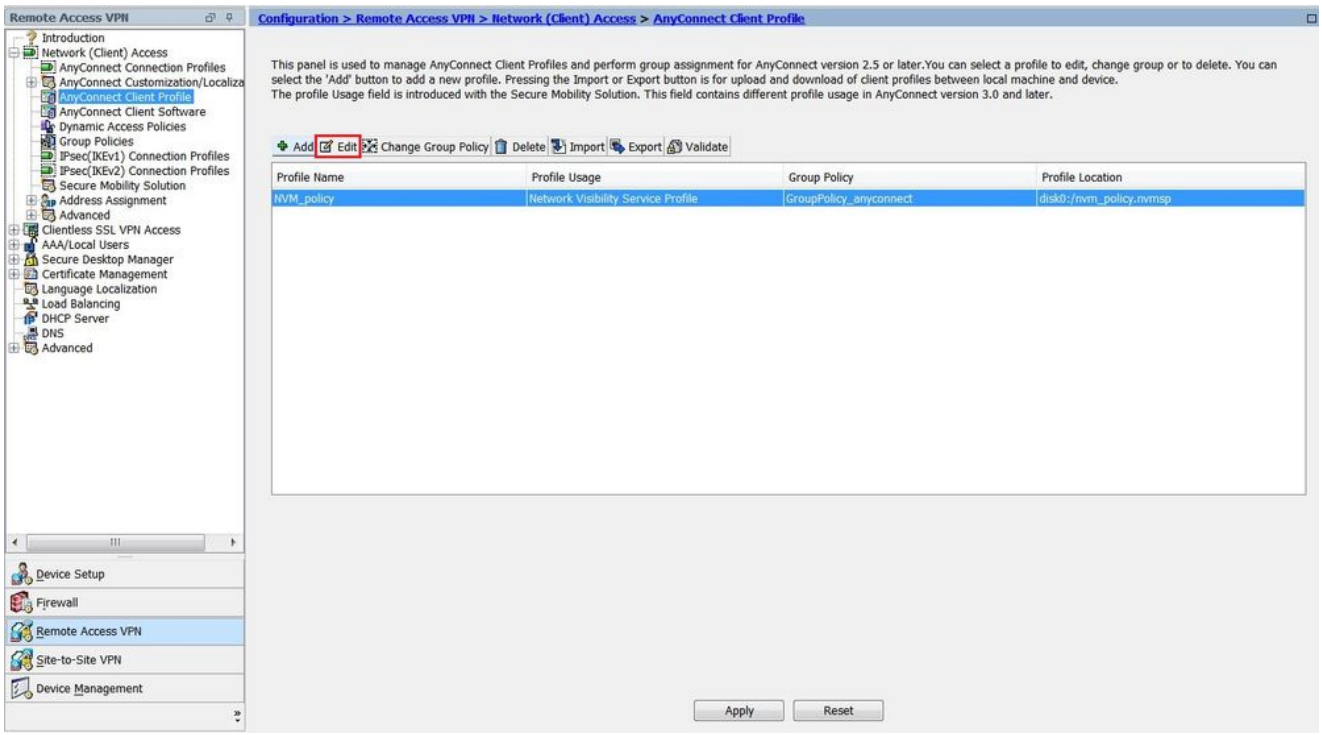


3. 為配置檔案指定名稱。在Profile Usage中，選擇Network Visibility Service Profile。

4. 將該配置檔案分配給AnyConnect使用者當前使用的組策略，然後按一下OK，如下圖所示。

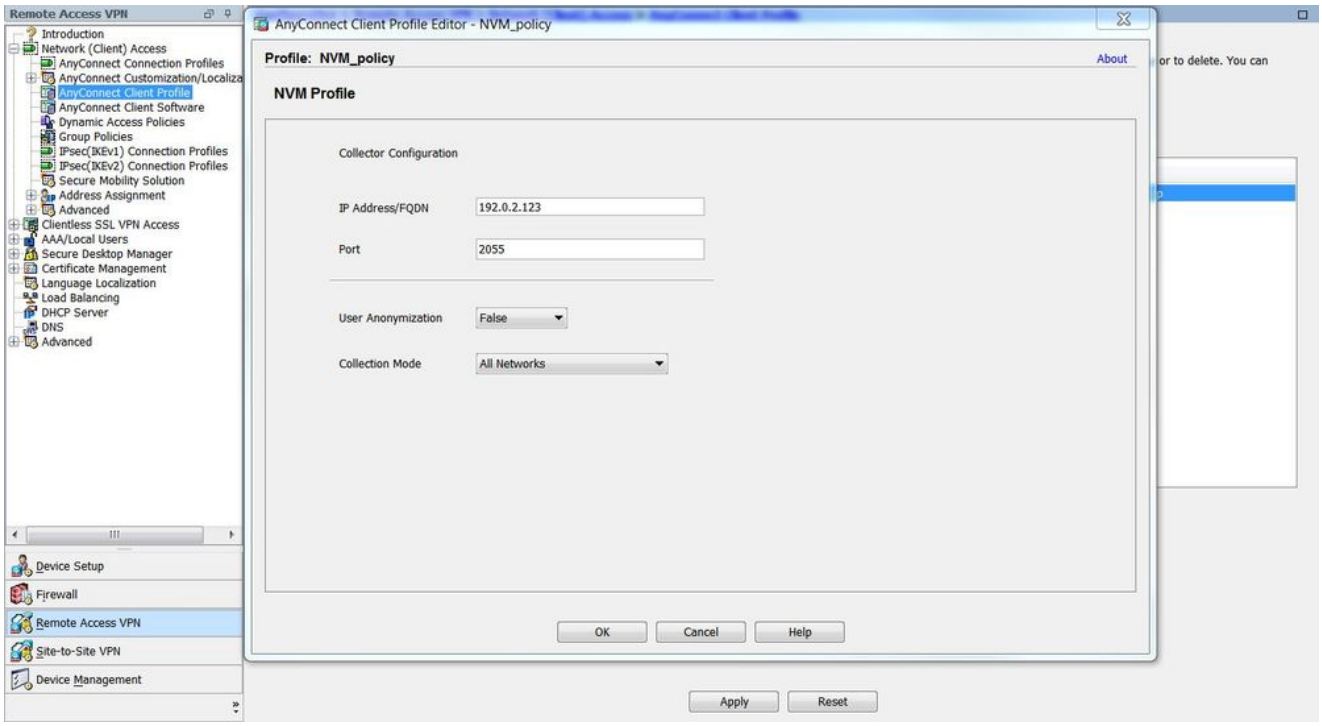


5. 建立新策略後，按一下Edit，如下圖所示。



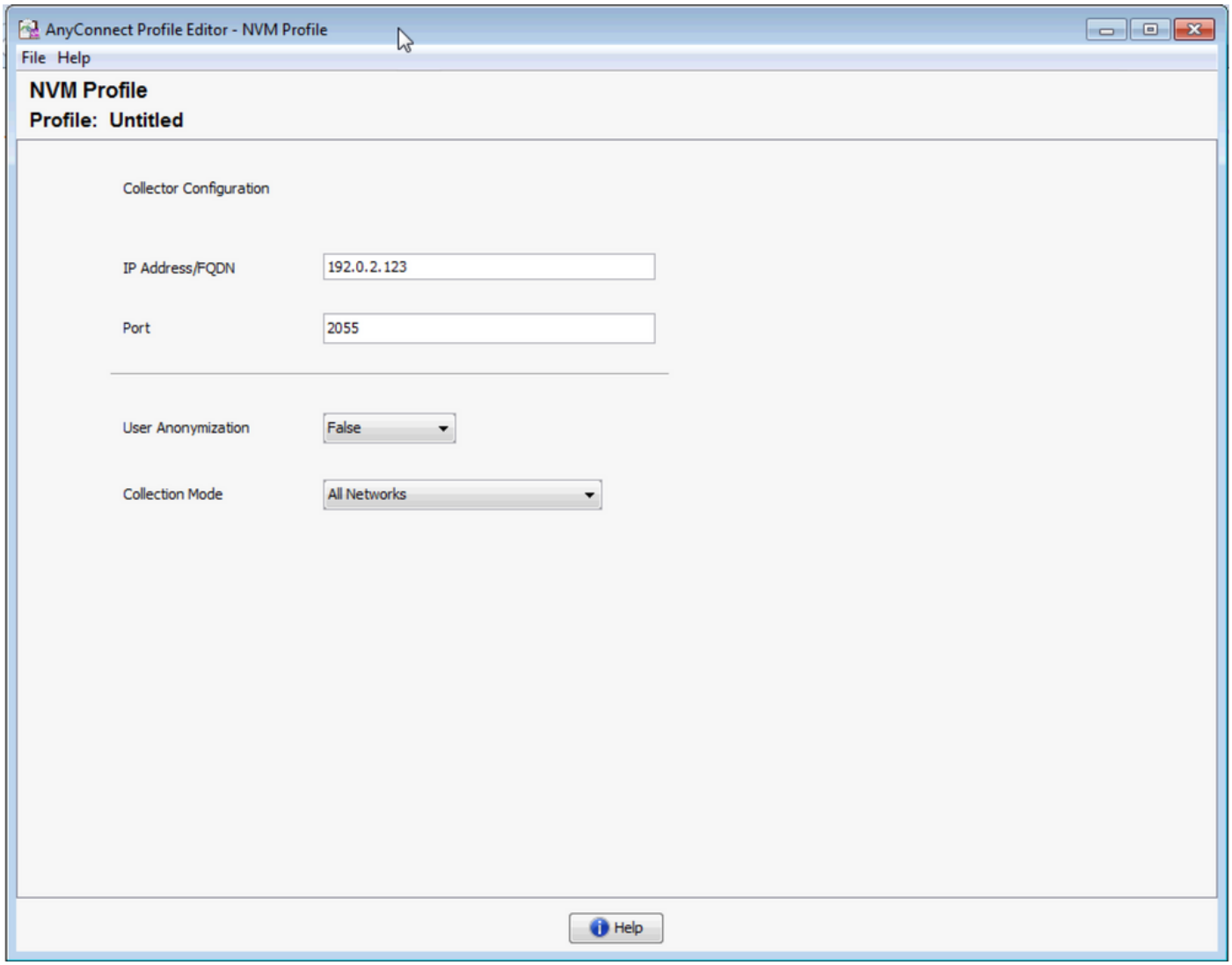
6. 輸入有關收集器IP地址和埠號的資訊；然後按一下OK。

7. 按一下「Apply」，如下圖所示。



通過AnyConnect配置檔案編輯器配置NVM客戶端配置檔案

此工具是一個獨立工具，可從Cisco.com獲得。如果通過Cisco ISE部署AnyConnect NVM，則首選此方法。通過此工具建立的NVM配置檔案可上傳到Cisco ISE，或直接複製到終端。



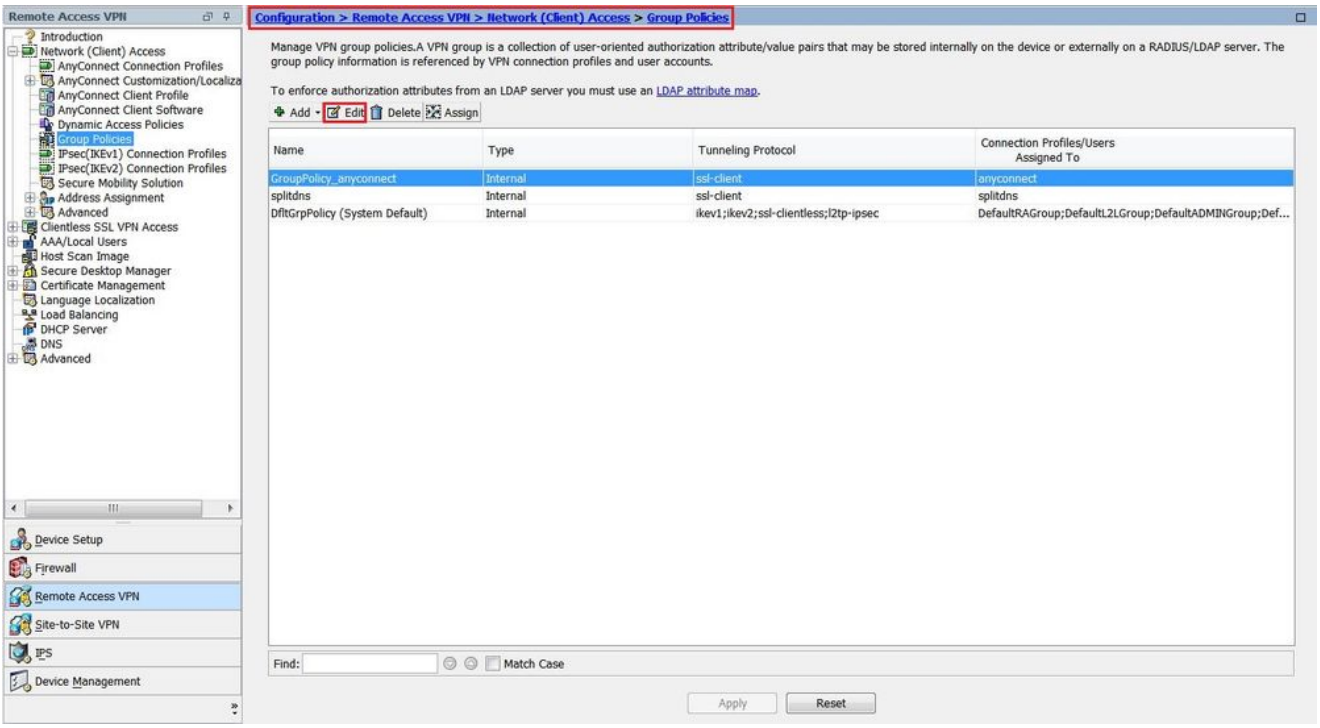
有關AnyConnect配置檔案編輯器的詳細資訊，請參閱AnyConnect配置檔案編輯器。

在Cisco ASA上配置Web部署

本技術說明假設ASA上已配置AnyConnect，並且您只需要新增NVM模組配置。有關ASA AnyConnect配置的詳細資訊，請參閱ASDM手冊3:Cisco ASA系列VPN ASDM配置指南，7.16。

要在Cisco ASA上啟用AnyConnect NVM模組，請執行以下步驟：

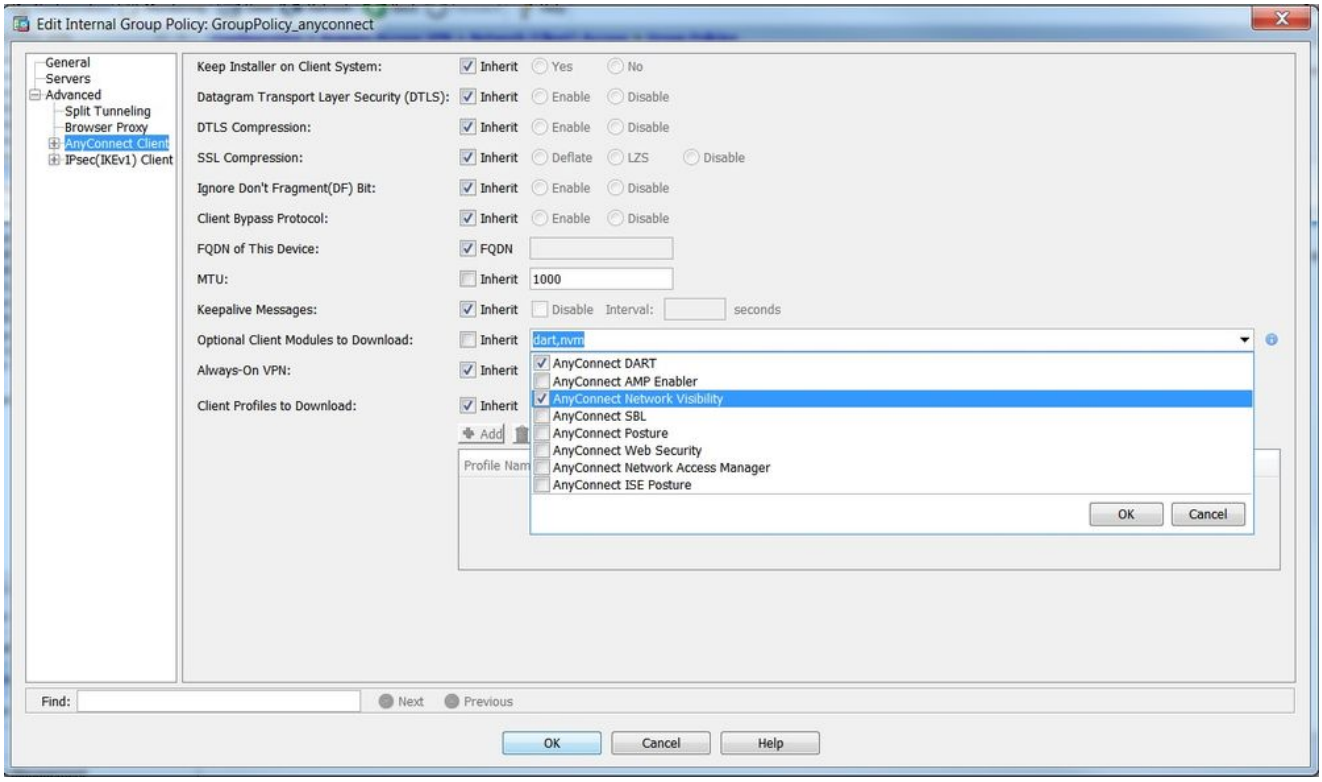
1. 導航到Configuration > Remote Access VPN > Network(Client)Access > Group Policies。
2. 選擇相關的組策略並按一下Edit，如下圖所示。



3. 在組策略彈出視窗中，導航到Advanced > AnyConnect Client。

4. 展開Optional Client Modules to Download，然後選擇AnyConnect Network Visibility。

5. 按一下「OK」並套用變更。

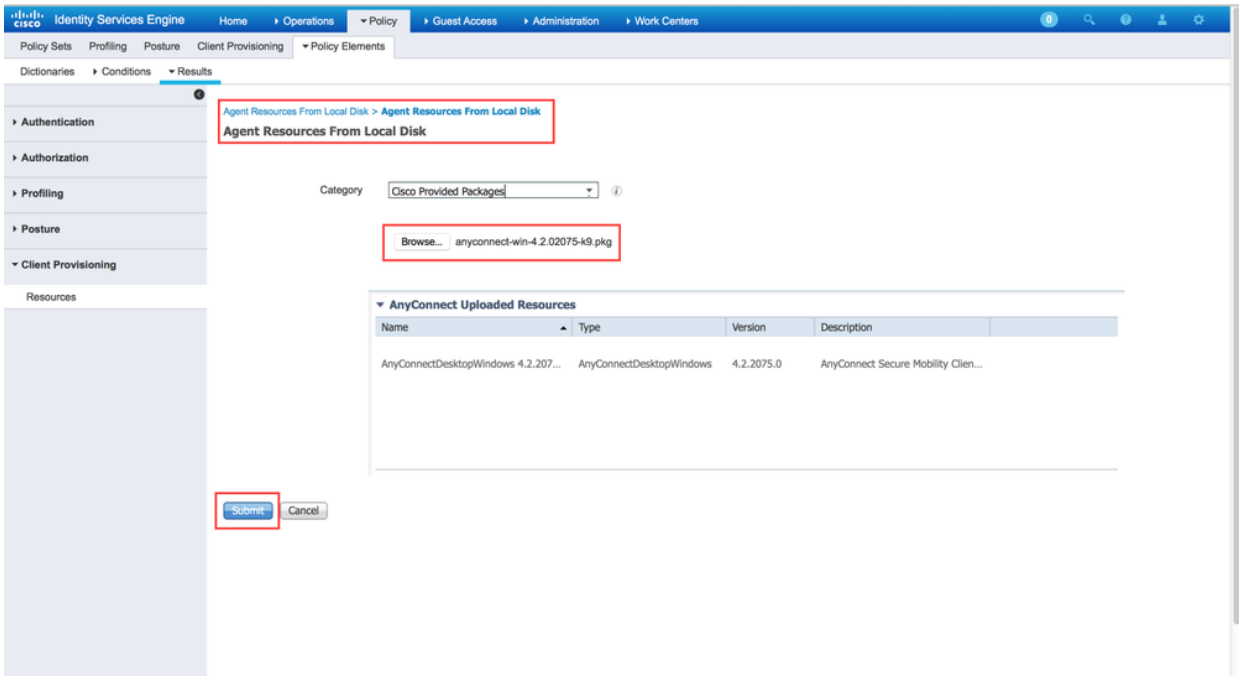


在Cisco ISE上配置Web部署

在本節中，我們將啟用AnyConnect客戶端模組、配置檔案、自定義/語言包和Opswat包。

要為AnyConnect Web部署配置思科ISE，請執行以下步驟：

1. 在Cisco ISE GUI中，導航到Policy > Policy Elements > Results。
2. 展開客戶端調配以顯示資源;然後選擇Resources。
3. 新增AnyConnect映像：
    1. 選擇Add > Agent Resources，然後上傳AnyConnect軟體包檔案。

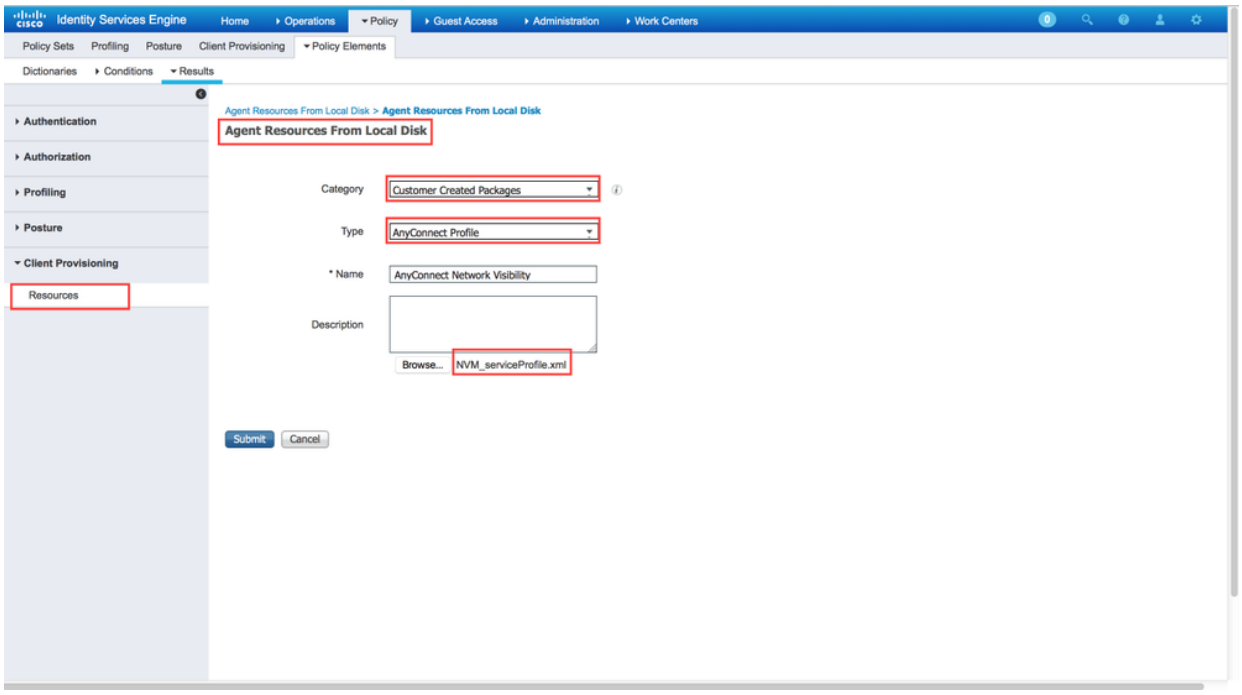


    2. 在彈出視窗中確認包的雜湊。

        可通過Cisco.com下載頁面或第三方工具驗證檔案雜湊。

        可重複此步驟以新增多個AnyConnect映像（例如，Mac OSX和Linux OS）。

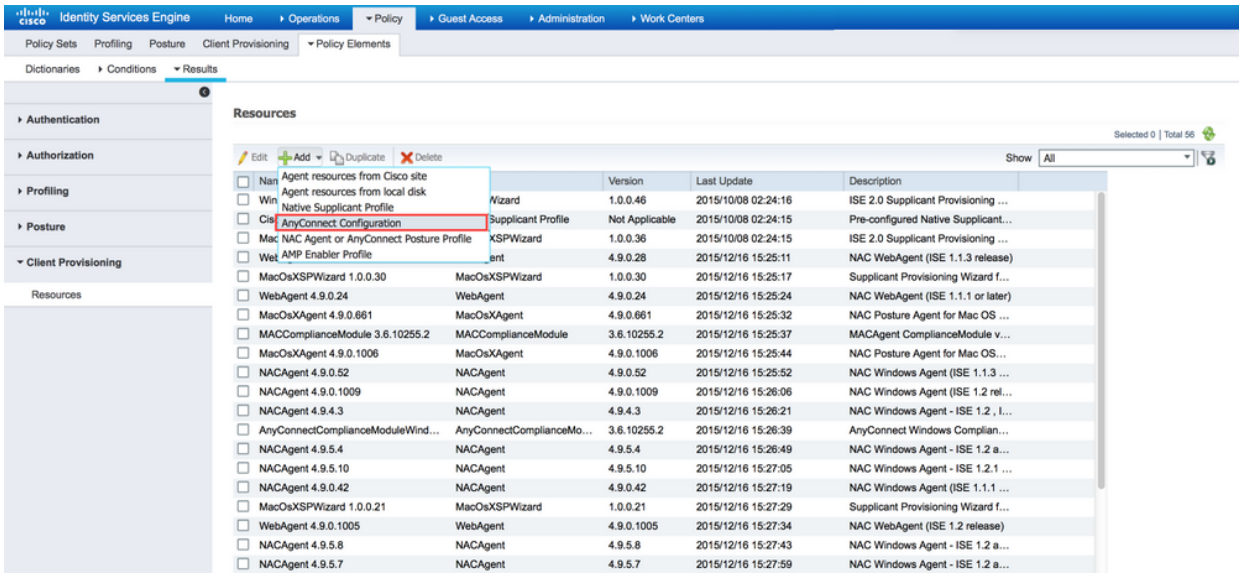
4. 新增AnyConnect NVM配置檔案：
    1. 選擇Add > Agent Resources，然後上傳NVM客戶端配置檔案。



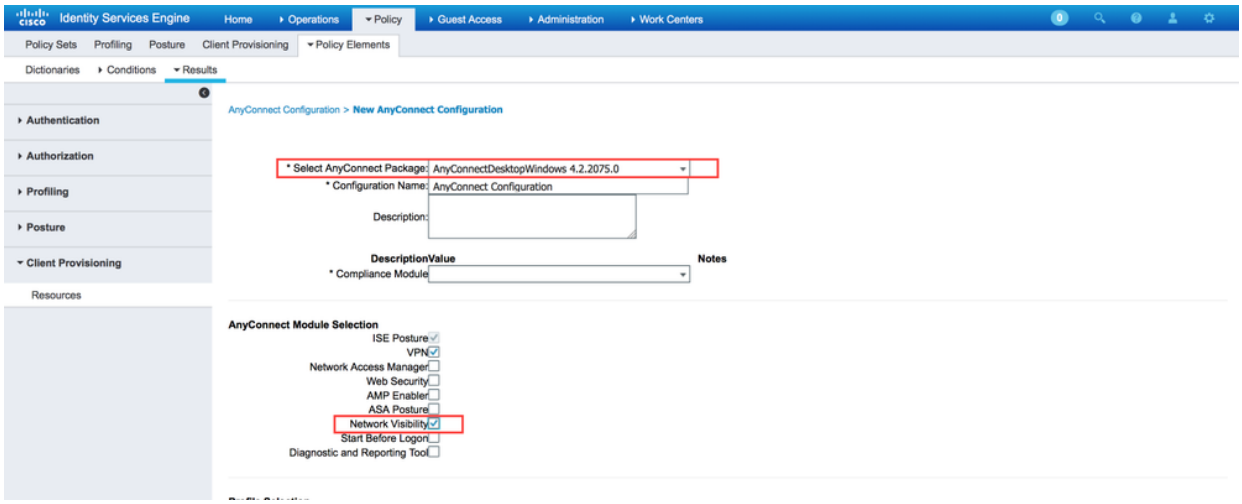
5. 新增AnyConnect配置檔案：

    1. 按一下Add並選擇AnyConnect Configuration。

        選擇您在上一步中上載的包。



    2. 在AnyConnect Module Selection中啟用NVM，同時啟用所需的策略。

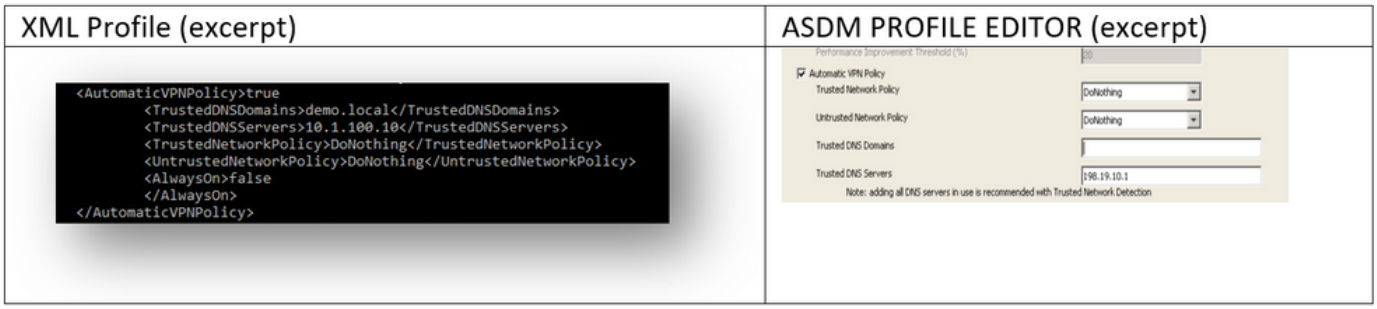


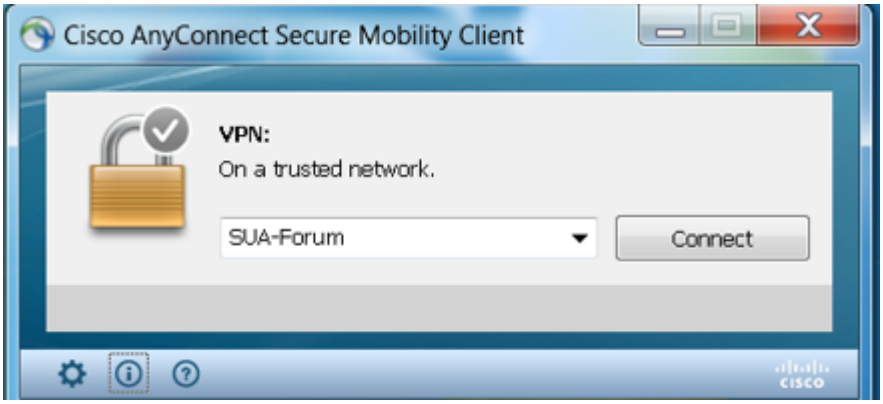
有關思科ISE上的Web部署配置的詳細資訊，請參閱Web部署AnyConnect。

可信網路檢測

AnyConnect NVM僅在流資訊位於受信任網路時才傳送流資訊。它使用AnyConnect客戶端的TND功能來瞭解端點是否位於受信任網路中。

可信網路檢測(TND)在用於VPN的AnyConnect客戶端配置檔案(XML)中配置，而不管環境中當前是否使用VPN元件。通過配置檔案中自動VPN策略部分的配置啟用TND。至少必須填充單個受信任DNS域或受信任DNS伺服器。當客戶端確定它位於受信任網路時，AnyConnect執行的操作可以通過受信任和不受信任網路策略的下拉選單設定為DoNothing模式。





有關TND配置的其他詳細資訊，請參閱關於受信任網路檢測。

部署

部署AnyConnect NVM解決方案需要以下步驟：

1. 在Cisco ASA/ISE上配置AnyConnect NVM。
2. 設定IPFIX收集器元件（Linux上的NVM收集器 — 打包在TA附加模組中）。
3. 使用CESA應用和TA附加模組設定Splunk。

步驟1.在Cisco ASA/ISE上配置AnyConnect NVM

本檔案設定一節中將詳細介紹此步驟。

在Cisco ISE/ASA上配置NVM後，可以將其自動部署到客戶端終端。

步驟2.設定IPFIX收集器元件（AnyConnect NVM收集器）

收集器元件負責從終端收集和轉換所有IPFIX資料，並將資料轉發到Cisco Endpoint Security Analytics(CESA)Add-On for Splunk。NVM收集器在64位Linux上運行。包括CentOS、Ubuntu和Docker配置指令碼。CentOS安裝指令碼和配置檔案也可以用於Fedora和Redhat發行版中。

在典型的分散式Splunk Enterprise部署中，收集器應在獨立的64位Linux系統上運行，或在64位Linux上運行的Splunk Forwarder節點上運行。收集器還可以安裝在沒有Splunk元件的獨立伺服器上。

附註：該解決方案還可以運行在包含NVM收集器和Splunk Enterprise元件的單個64位Linux系統上，用於小型部署或演示目的。對於多達10,000個終端來說，一體化最簡單。有關POV調整資訊，請參閱Real Client POV。

如何安裝收集器

1. 將acnvmcollector.zip檔案(位於/opt/splunk/etc/apps/TA-Cisco-NVM/appserver/addon/目錄（隨TA附加模組提供）複製到要安裝它的系統。
2. 解壓縮acnvmcollector.zip檔案以解壓縮檔案。

建議在執行install.sh指令碼之前，閱讀.zip套件組合中的$PLATFORM$_README檔案。$PLATFORM$_README檔案提供有關在執行install.sh指令碼之前需要驗證和修改（如有必要）的相關配置設定的信息。至少需要配置將資料轉發到的Splunk例項的地址。無法正確配置系統可能導致收集器無法正確運行。

附註：請確保將網路和主機防火牆配置為允許源、目標地址和埠的UDP流量。防火牆必須允許從AnyConnect客戶端到收集器的傳入IPFIX(CFLOW)流量，以及傳出UDP資料到Splunk。

單個NVM收集器例項在大小適當的系統上可以每秒處理至少5000個流，或者最多可以處理35,000到40,000個端點。必須先配置收集器並運行收集器，然後才能使用Splunk NVM和TA-Add on App。

預設情況下，收集器從UDP埠2055上的AnyConnect NVM終端接收流。

此外，收集器還會為Splunk生成三個資料饋送：

- UDP埠上的每個流數20519
- UDP埠上的端點身份數20520
- 終端介面資料UDP埠20521

可以更改接收埠和資料饋送埠。為此，請更改acnvm.conf檔案並重新啟動收集器例項。確保端點與收集器之間或收集器與Splunk系統之間的所有主機/網路防火牆均已針對配置的UDP埠和地址開啟。此外，請確保AnyConnect NVM配置與收集器配置匹配。

安裝並運行所有元件後，請參閱Splunk應用程式中的「幫助檔案」部分，以獲取有關預配置報告、資料模型和解決方案所建立資訊元素的詳細資訊。

您可以重新啟動其中一個AnyConnect終端並驗證正在向解決方案傳送流量。例如，您可以使用youtube.com運行穩定的資料流。

此資訊必須在acnvm.conf配置檔案中配置：

- syslog_server_ip（轉發程式或Splunk例項）：可以指向127.0.0.1（不使用LOCALHOST）（如果它位於同一框中）。
- 收集器的偵聽埠（傳入IPFIX資料）：預設值為OK。

附註：配置檔案中省略netflow_collector_ip。它使用預設公共介面，僅應進行更改以便使用特定本地IP覆蓋預設值。

Per Flow Data Port、Endpoint Identity Data Port、Endpoint Interface Data和Collector Port已預配置為配置檔案中的預設設定。如果您使用非預設連線埠，必須變更這些值。

此資訊將新增到組態檔中：/opt/acnvm/conf/acnvm.conf

DTLS支援

附註：有關詳細資訊，請參閱本文檔中的為DTLS支援配置NVM。

在託管收集器的框上執行以下步驟：

- 製作此目錄：/opt/acnvm/certs。
- 若要將憑證套用到收集器，請將憑證和金鑰儲存在/opt/acnvm/certs目錄中。
- 使用以下命令將資料夾的所有者和組更改為acnvm:acnvm:sudo chown -R acnvm:acnvm certs/:
- acnvm.conf的此部分必須配置有證書和金鑰。
- 放置配置和證書後，重新啟動收集器：sudo systemctl restart acnvm.service
- 檢查收集器狀態：sudo systemctl status acnvm.service

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

以下是其餘的組態：

```
"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
}
```

- 以超級使用者許可權()執行install.shsudo ./install.sh指令碼。

> 附註：帳戶需要sudo許可權或root才能運行install.sh指令碼，並需要acnvm服務帳戶的許可權。

如需詳細資訊，請參閱適用於Splunk的Cisco端點安全分析(CESA)應用（詳細資訊）。

步驟3.使用CESA控制面板和TA附加模組設定Splunk

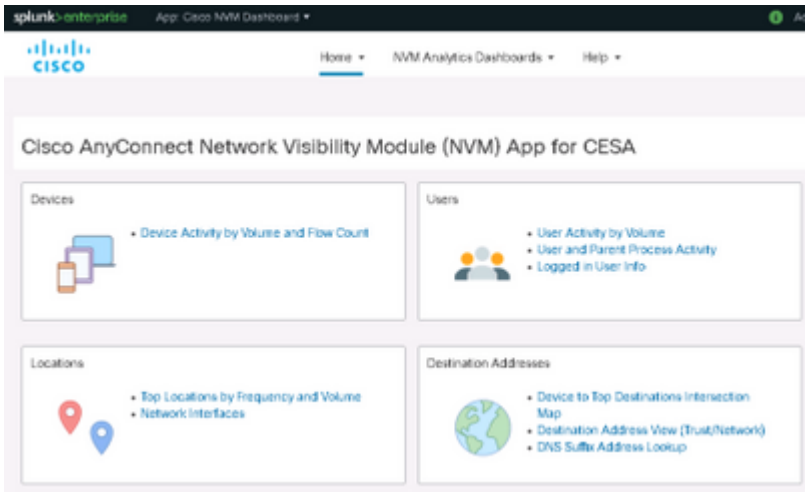
Splunkbase提供適用於Splunk的Cisco AnyConnect NVM應用。此應用提供預定義的報表和儀表板，這些報表和儀表板在幫助關聯使用者和終端行為的可用報表中顯示來自終端的IPFIX(nvzFlow)資料。

> 附註：對於雲部署，這兩個應用都安裝在雲例項中。只有TA安裝在內部（與轉發器一起）。收集器隨轉發器一起安裝在內部或安裝在單獨的Linux/Docker盒上。

對於內部安裝，您可以在一個機箱或單獨的機箱上安裝所有元件和應用。(請參閱本文檔的部署概述部分中的圖。)

下載以下檔案：

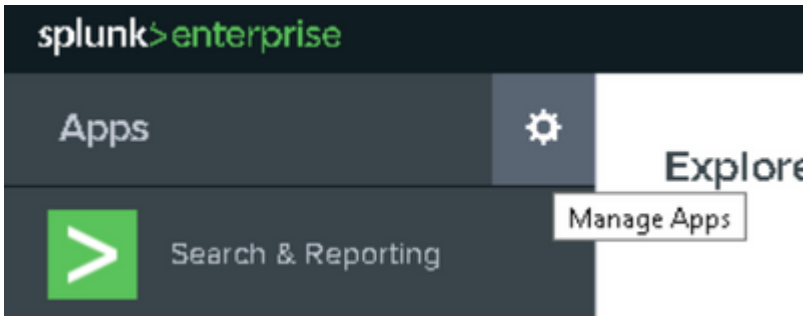
- 適用於Splunk的思科端點安全分析(CESA)應用



- [適用於Splunk的思科端點安全分析(CESA)附加模組]

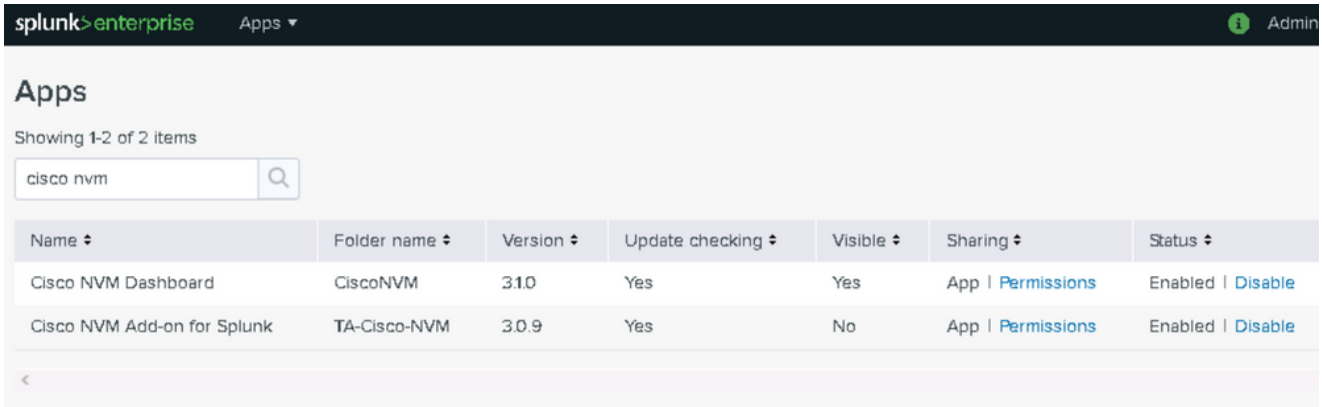
安裝

1. 導航到Splunk > Apps。按一下齒輪並安裝從Splunkbase下載的tar.gz檔案，或在「應用」部分中搜尋。



2. 使用相同的進程安裝載入項。

3. 檢視Splunk Apps頁面，以確認已安裝Cisco NVM控制面板和適用於Splunk的Cisco NVM載入項。



預設配置接收Splunk的三個資料饋送(請參閱本文檔中的[通過Splunk管理UI啟用UDP輸入])。

- UDP埠上的每個資料流數20519
- UDP埠上的端點身份數20520

- UDP埠上的端點介面數20521

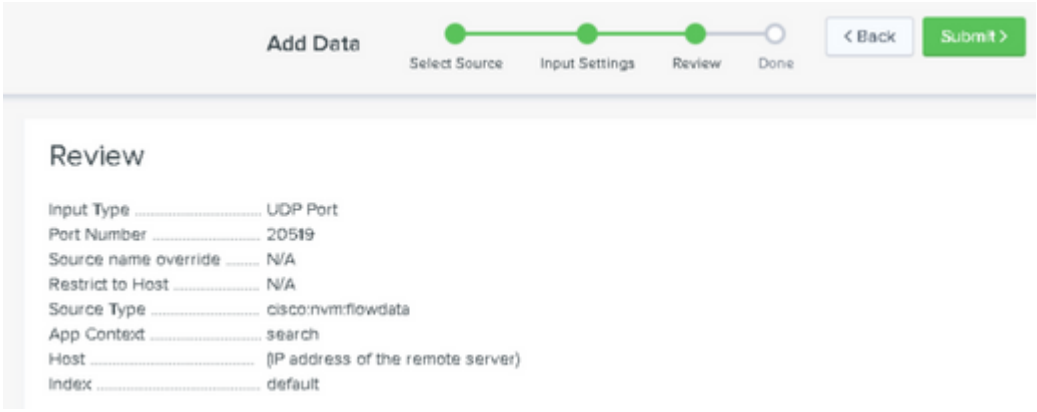
然後，載入項將這些資料來源分別對映到Splunk源型別cisco:nvm:flowdata、cisco:nvm:sysdata和cisco:nvm:ifdata。

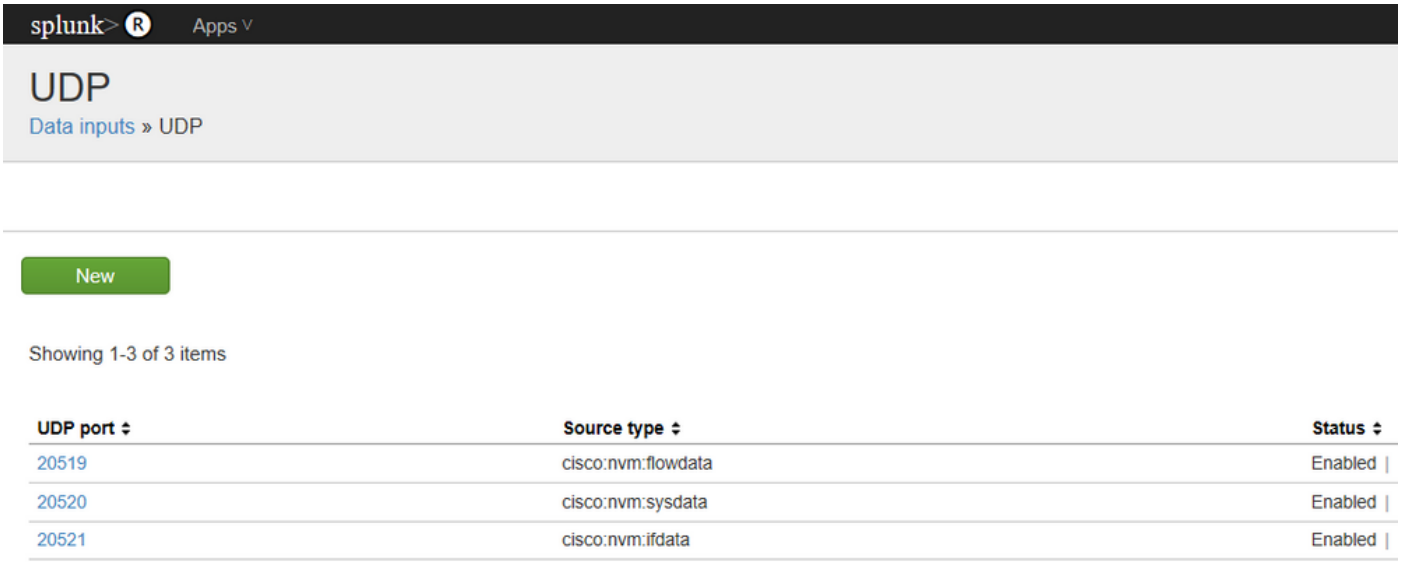
通過Splunk Management UI啟用UDP輸入

附註：您還可以通過input.conf檔案啟用UDP輸入。此方法在Cisco NVM控制面板應用GUI（在「幫助」下）中說明。

您無需重新啟動Splunk軟體。

1. 導覽至Splunk > Settings > Data Input > UDP。
2. 按一下New Local UDP > Enter port # missing > Click Next > Select the corresponding Source Type >按一下Review >按一下Submit。
3. 對另外兩個連線埠重複上述步驟。（可以使用克隆。）

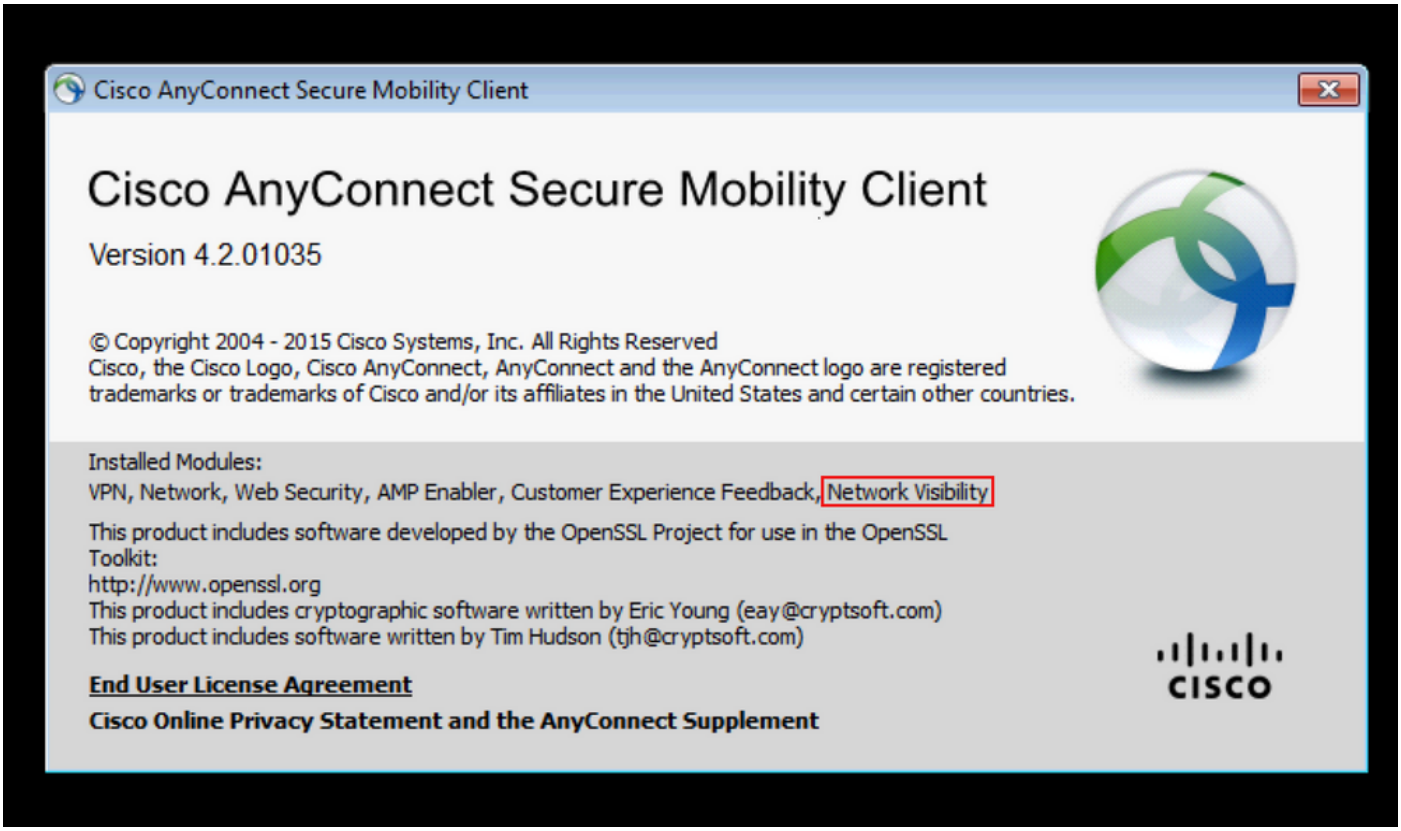




驗證

驗證AnyConnect NVM安裝

成功安裝後，網路可視性模組應在AnyConnect安全移動客戶端的資訊部分的已安裝的模組中列出。



此外，請驗證nvm服務是否正在終端上運行，以及配置檔案是否位於所需目錄中。

驗證收集器狀態

確認收集器狀態為「活動（運行）」。 此狀態確保收集器始終從終端接收IPFIX/cflow。如果收集器狀態為非活動狀態，請確保檔案的acnvm帳戶許可權允許其執行：

- /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/

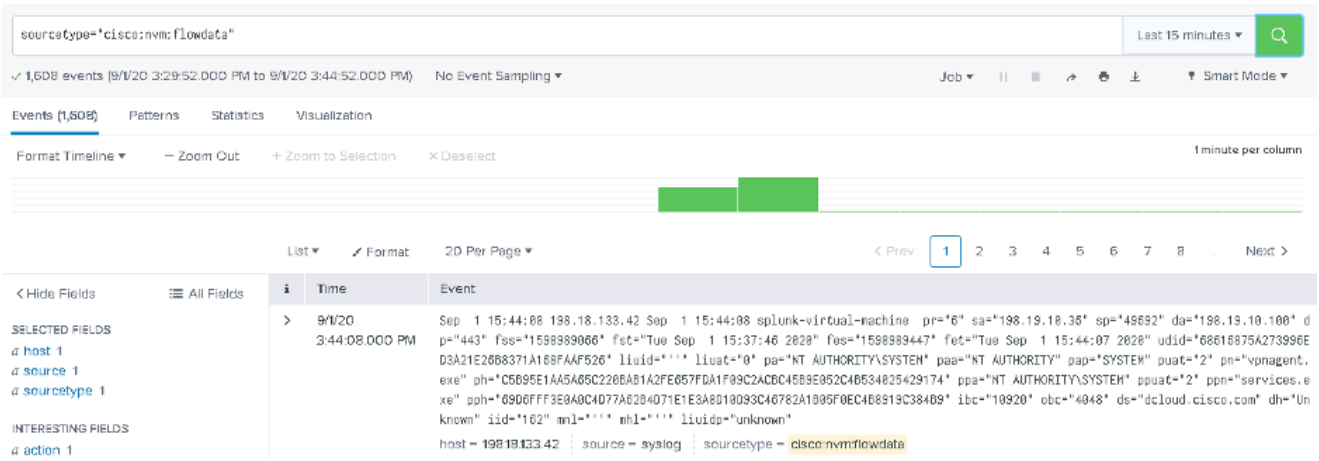
```
[splunk@splunk-virtual-machine addon]$ systemctl status acnvm.service
● acnvm.service - AC NVM Service
   Loaded: loaded (/usr/lib/systemd/system/acnvm.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2020-06-19 13:48:08 EDT; 25s ago
 Main PID: 41165 (acnvmcollector)
    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)
```

驗證Splunk - CESA儀表板

確保Splunk及其相關服務正在運行。有關如何對Splunk問題進行故障排除的文檔，請參閱Splunk網站。

由於使用了自動化指令碼，CESA的控制面板只有在收到初始資料五分鐘後才會更新。但是，您可以立即運行手動搜尋以驗證是否正在接收資料：

1. 在Splunk主控制面板中，按一下Search & Reporting。
2. 在下一個螢幕中，設定正確的範圍，以便填充所需資料。
3. 在搜尋欄位中，輸入： sourcetype="cisco:nvm:flowdata"



在最初的五分鐘後，驗證CESA控制面板是否正在接收資料：

1. 在Splunk主控制面板中，按一下Cisco Endpoint Security Analytics Dashboard。
2. 如果要保留當前設定，請按一下Device Activity by Volume and Flow Count。
3. 按一下「Submit」。操控板顯示資料和圖形。

封包流量

1. IPFIX資料包由AnyConnect NVM模組在客戶端終端上生成。
2. 客戶端終端將IPFIX資料包轉發到收集器IP地址。
3. 收集器收集資訊並將其轉發給Splunk。

4. 收集器通過三個不同的流向Splunk傳送流量：每個流資料、終端資料和介面資料。

所有流量都基於UDP，因此資料包流中不會確認已收到資料。

流量的預設連線埠：

- IPFIX資料2055
- 每個流資料流20519
- 終端資料20520
- 介面資料20521

NVM模組快取IPFIX資料，並在資料處於受信任網路時將其傳送到收集器。當筆記型電腦連線到公司網路（內部網路）或通過VPN連線時，會發生此行為。

您可以驗證收集器是否正在從NVM模組接收資料包。為此，請根據您的配置，在特定的UDP埠上運行資料包捕獲，以檢查是否正在接收資料包。此驗證將通過Splunk系統Linux OS完成。

流模板

IPFIX流模板會在IPFIX通訊開始時傳送到收集器。這些模板有助於收集器理解IPFIX資料。

收集器還會預載入模板，以確保即使客戶端尚未傳送模板，也可以分析資料。如果客戶端的較新版本發佈時發生了協定更改，則收集器會使用客戶端傳送的新模板。

在以下情況下傳送模板：

1. NVM客戶端配置檔案發生更改。
2. 發生網路更改事件。
3. Nvmagent服務已重新啟動。
4. 終端已重新啟動/重新啟動。
5. 按照NVM配置檔案中配置的定期更新（預設值=24小時）。

在極少數情況下，收集器無法找到模板。如果發生這種情況，您會看到以下症狀之一：

- 在端點上的資料包捕獲中找不到模板
- 或收集器日誌中沒有flowset的模板

若要解決此問題，請重新啟動其中一個端點。

疑難排解

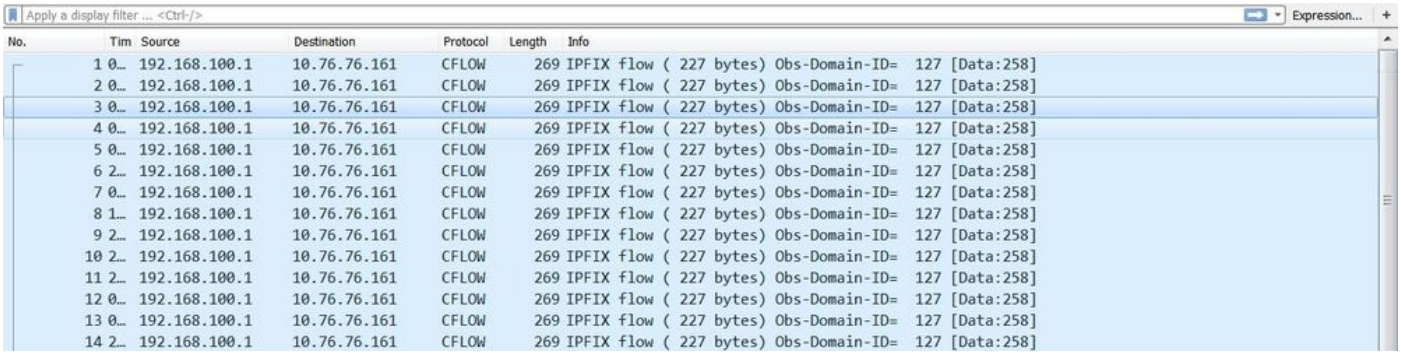
以下是進行疑難排解的基本步驟：

1. 確保客戶端終端和收集器之間的網路連線。
2. 確保收集器和Splunk之間的網路連線。
3. 確保在客戶端終結點上正確安裝NVM。
4. 在終端上應用捕獲，檢視是否正在生成IPFIX流量。
5. 在收集器上應用捕獲，檢視它是否收到IPFIX流量，以及它是否將流量轉發到Splunk。
6. 在Splunk上應用捕獲，檢視它是否收到流量。

7. 對於DTLS:
    - 確認AnyConnect客戶端信任收集器證書。
    - 確認NVM配置檔案已啟用「安全」選項。
    - 確認收集器已配置證書。

IPFIX流量（如Wireshark所示）：

附註：如果在客戶端和收集器之間運行DTLS，則必須過濾DTLS流量。



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

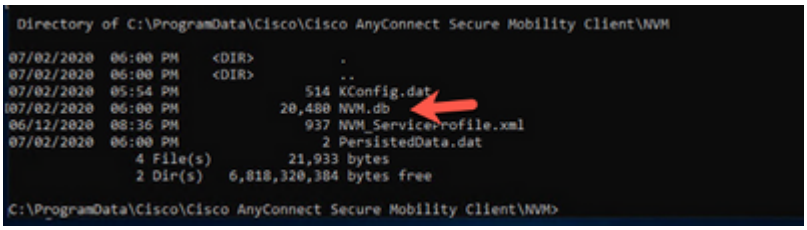
No.	Tim	Source	Destination	Protocol	Length	Info
1	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
2	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]
3	0…	192.168.100.1	10.76.76.161	CFLOW	269	IPFIX flow (227 bytes) 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客戶端（NVM模組）

不向收集器報告資料，也不從端點傳送資料包

在C:\%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM目錄中，NVM資料庫檔案(NVM.db)的大小是否繼續增加？該行為表示AnyConnect NVM客戶端沒有向收集器傳送資料包。

附註：有關快取進程和可用快取控制的資訊，請參閱Cisco AnyConnect安全移動客戶端管理員指南4.9版。



```
 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>
```

可信網路偵測(TND)

啟動AnyConnect UI並確保它位於受信任的網路中。NVM依靠TND檢測終端何時位於受信任網路中。TND配置不正確會導致NVM問題。NVM具有自己的TND配置，該配置在已配置伺服器的TLS證書指紋上工作。可以在NVM配置檔案編輯器中配置NVM TND。

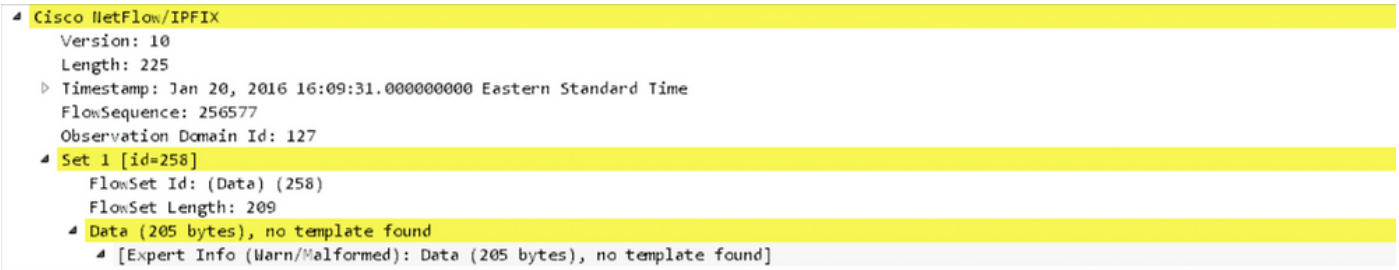
如果未配置NVM TND，則NVM依賴於VPN模組的TND配置。VPN模組的TND基於通過DHCP接收的資訊工作：網域名稱和網域名稱系統(DNS)伺服器。如果DNS伺服器和/或域名與配置的值匹配，則認為網路受信任。VPN還支援基於TLS證書的TND檢測。

- 確保TND配置正確。NVM僅在位於受信任網路時才匯出。

> 附註：如果TND配置不正確，NVM將不會匯出資料。例如，如果在客戶端上配置了三個DNS伺服器，但所有三個DNS伺服器均未在TND配置中設定，則NVM不會匯出資料。

- 從TND VPN配置中刪除受信任域。
- 網路問題：
  - 對於拆分隧道，始終在VPN的「拆分包括」配置中包括收集器的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，則資料將從公共介面發出。
- 確保將CollectionMode配置為在當前網路上收集（受信任/不受信任）。
- 確保VPN.xml和NVM_ServiceProfile.xml檔案位於正確的資料夾中；然後重新啟動。
- 啟動 — 停止所有AnyConnect服務。
- 退回連線到DNS伺服器連線的內部網路。

封包擷取：



AnyConnect診斷和報告工具(DART)

若要對AnyConnect操作進行故障排除，請在NVM元件上運行DART。請參閱AnyConnect故障排除。

- NVM所需的所有日誌都由DART處理。DART收集日誌檔案、配置等。
- Windows日誌：事件未位於單一位置。AnyConnect下的NVM事件檢視器中有一個單獨的枝葉。
- macOS/Linux:按nvmagent過濾日誌。

收集器(在Linux/Docker電腦上：一體化或獨立)

acnvmcollector安裝失敗

安裝收集器並運行安裝指令碼(Sudo ./install_ubuntu.sh)時，

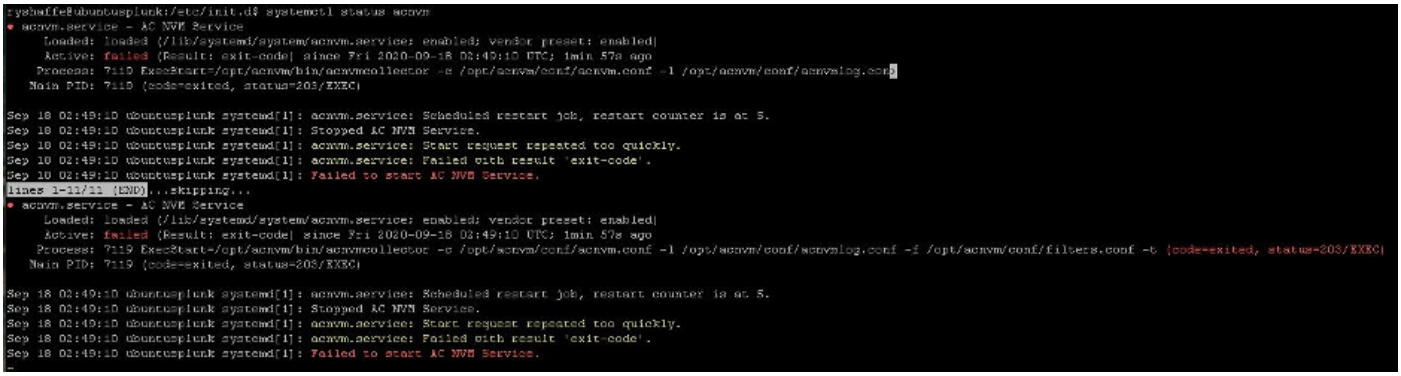
此錯誤出現在/var/log/syslog: "Acnvm.conf error: line number 17 : expected key string"

此問題可能由額外的逗號或無效位置的逗號引起。

acnvmcollector無法啟動

此問題發生在Ubuntu上（但可能適用於所有Linux）。 未能對acnvmcollector檔案執行代碼：/opt/acnvm/bin/acnvmcollector。

acvnm使用者和組沒有用於eXecuteacnvmcollector的。



收集器日誌 — 在哪裡可以設定調試？

您可以在ACMNVMLOG.conf檔案中設定日誌記錄級別。日誌記錄級別是啟動時傳送到收集器的配置的一部分。更改後，重新啟動收集器。

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
```

如何查詢收集器的版本號？

要查詢收集器版本，請運行帶acnvmcollector有標誌的命-v令：

範例 1：

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

範例 2：

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

輸出：

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

DTLS問題

- 消息「DTLS not configured」表示未在acnvm.conf檔案中配置DTLS。
- 不支援密碼金鑰組合時，將顯示消息「伺服器金鑰無效」。

Splunk控制檯（CESA控制面板）不顯示資料

AnyConnect客戶端

- 使用youtube.com生成資料。您還可以瀏覽一些網站。
- AnyConnect客戶端是否可以通過UDP 2055將資訊傳送到收集器伺服器？（換句話說，AnyConnect客戶端和收集器伺服器之間是否存在任何防火牆？）
  - 嘗試從客戶端電腦telnet到收集器電腦。
- 運行wireshark以確認客戶端正在向收集器傳送流量(2055 CFLOW)資料。

收集器盒

- 驗證收集器盒是否正在接收AnyConnect NVM流量：
  - 執行tcpdump並確認您看到從Client到2055的伺服器發25001的資料包。例如，此命令顯示來自客戶端主機IP地址的前100個資料包：Sudo tcpdump -I any -c100 -nn host 10.1.110.7

    附註：有關詳細資訊，請參閱如何使用tcpdump捕獲所有UDP資料包？
  - 確保AnyConnect NVM收集器正在運行(請參閱本文檔中的DTLS支援)。
  - 檢查acnvm.conf檔案是否存在格式錯誤、缺少引號、逗號等。
  - Splunk UI - TA — 在Splunk GUI上或通過input.conf設定UDP資料輸入和源型別？
    - 在UI > settings > server controls下重新啟動Splunk。

常見問題（常見問題）

如何將資料從AnyConnect NVM傳送到多個目標？

此方案用於高可用性情況或傳送到多個平台（例如Splunk和Stealthwatch）。

有關詳細資訊，請參閱在Splunk快速啟動POV套件和部署指南上構建的思科端點安全分析(CESA)。

在哪裡儲存AnyConnect NVM DTLS的證書？

在收集器上沒有安裝公認證書的實驗室測試中，可能會出現這種情況。

- Windows:將收集器證書安裝到Windows受信任證書中。
- Mac OSX:使用標準過程通過金鑰鏈安裝根證書。您可以使用金鑰鏈工具匯入證書，並將其新增為受信任證書。
- Linux RHEL:請按照以下RHEL根CA匯入步驟操作：
    1. 將ca cert複製到/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匯入步驟操作：
    1. 使用以下命令將.cer檔案轉換為.crt檔案： openssl x509 -inform PEM -in RootCA.cer -out rootCa.crt
    2. 將.crt檔案複製到/usr/local/share/ca-certificates目錄。
    3. 執行命令： sudo update-ca-certificates

XML檔名

使用本地配置檔案編輯器時，核心VPN模組XML配置檔名稱並不重要。但是，您必須將服務配置檔案另存為NVM_ServiceProfile.xml。如果對服務配置檔案使用不同的名稱，NVM將無法收集和傳送資料。

收集器(AnyConnect NVM)

適用於Splunk的思科端點安全分析(CESA)應用（詳細資訊）

- 是否可以在根下建立供應商目錄，然後將所有權提供給其他帳戶？

  您可以先建立/opt/acnvm，只要安裝指令碼具有將檔案複製到其中的許可權。
- 檔案許可權：install.sh檔案需要許可權才能作為根目錄執行。
- 服務帳戶：

- 需要useradd -r該命令和-s /bin/false該命令，因為服務帳戶是不具有主目錄的非互動式帳戶。
- 對於非互動式帳戶來說，擁有主目錄並不是一項要求，服務帳戶沒有主目錄是保持乾淨的標準做法。
- 所有使用者都具有uid/guid（無論他們是否具有主目錄）。

- 收集器作業系統：收集器運行在CentOS或Ubuntu上；它也可以在RedHat上運行，因為RedHat使用CentOS指令碼。
- 如果需要，可以修改安裝指令碼：
  - 安裝指令碼必須以root使用者身份或具有SUDO許可權運行，因為它建立一個名為acnvm的新使用者，並將所有內容放入/opt/acnvm目錄。

> 附註：或者，您可以建立自定義指令碼，以便根據要求執行適當的操作。此指令碼可以使用系統上已存在的其他使用者，但此使用者必須具有SUDO許可權才能運行安裝。

- 要查詢收集器版本，請運行帶有標誌的以下-v命令： ./opt/acnvm/bin/acnvmcollector -v

建議版本

我們始終建議您使用最新可用軟體版本的AnyConnect。如需詳細資訊，請參閱Cisco AnyConnect安全行動化使用者端v4.x的版本說明。

相關資訊

- 在Splunk快速啟動POV工具包和部署指南上構建的思科端點安全分析(CESA)
- Cisco Endpoint Security Analytics(CESA)控制面板概述和常見問題
- 適用於Splunk的思科端點安全分析(CESA)應用
- 適用於Splunk的思科端點安全分析(CESA)應用（檔案）
- Cisco AnyConnect安全移動客戶端v4.x客戶端管理員指南
- Cisco AnyConnect安全移動客戶端v4.x版本說明
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。