

Installeer en configureren AnyConnect NVM 4.7.x of hoger en verwante Splunk Enterprise-componenten voor CESA

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Overzicht van implementaties](#)

[Achtergrondinformatie](#)

[Cisco AnyConnect Secure Mobility Client - meer dan VPN](#)

[Internet Protocol Flow Information Exporteren \(IPFIX\)](#)

[IPFIX NVM Collector](#)

[Splunk Enterprise](#)

[Topologie](#)

[Configureren](#)

[Ondersteuning van DTLS](#)

[certificaatvereisten](#)

[Standalone AnyConnect NVM module](#)

[AnyConnect NVM-clientprofiel](#)

[NVM-clientprofiel configureren via ASDM](#)

[NVM-clientprofiel configureren via AnyConnect Profile Editor](#)

[Configuratie van WebDeployment op Cisco ASA](#)

[Configuratie van Web-Plaatsing op Cisco ISE](#)

[Trusted Network Detectie](#)

[implementeren](#)

[Stap 1. Configureer de NVM via Cisco ASA/ISE](#)

[Stap 2. Stel IPFIX Collector Component in \(AnyConnect NVM Collector\)](#)

[Hoe installeert u de Collector?](#)

[Ondersteuning van DTLS](#)

[Stap 3. Stel Splunk in met Cisco NVM App \(CESA Dashboard\) en TA Add-On voor Splunk.](#)

[Installeren](#)

[UDP-ingangen inschakelen met behulp van Splunk Management UI](#)

[Verifiëren](#)

[AnyConnect NVM-installatie valideren](#)

[Valideren van Collector status als actief](#)

[Splunk valideren - AnyConnect NVM CESA Dashboard](#)

[PacketFlow](#)

[Flow-sjablonen](#)

[Problemen oplossen](#)

[AnyConnect-client \(NVM-module\)](#)

[AnyConnect NVM - niet rapporteren aan de Collector - CFLOW-datapakketten blijven geen eindpunt achter](#)

[Trusted Network Detection \(TND\)](#)

[AnyConnect diagnostiek en rapportage-tools \(DART\)](#)

[Collector \(op Linux/Docker machine - all-in-one of standalone\)](#)

[Splunk Console \(NVM Dashboard\) geeft geen gegevens weer](#)

[AnyConnect-client](#)

[Verzamelbak](#)

[Vaak gestelde vragen \(veelgestelde vragen\)](#)

[1. Hoe kunt u gegevens van een willekeurige NVM naar meerdere bestemmingen sturen?](#)

[2. Waar slaat u het certificaatmodel op voor AnyConnect NVM DTLS?](#)

[XML-bestandsnamen](#)

[Collector \(anyconnect NVM\)](#)

[Aanbevolen release](#)

[AnyConnect 4.9.0086 nieuwe functies](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u de Cisco AnyConnect Network Visibility Module (NVM) op een eindgebruikersysteem kunt installeren en configureren met AnyConnect 4.7.x of hoger en hoe u de bijbehorende Splunk Enterprise-onderdelen en NVM Collector kunt installeren en configureren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- AnyConnect 4.7.x of hoger met NVM
- AnyConnect-licenties
- ASDM 7.5.1 of hoger
- Bekendheid met Splunk Enterprise en hoe u Splunk-apps en add-ons kunt installeren

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco AnyConnect Security Mobility Client 4.7.x of hoger
- Cisco AnyConnect-profieeditor
- Cisco adaptieve security applicatie (ASA), versie 9.5.2
- Cisco Adaptieve Security Devices Manager (ASDM), versie 7.5.1

- Splunk Enterprise 7.x of hoger (geïnstalleerd als all-in-one op een ondersteunde linux, bij voorkeur CentOS)
- Alle ondersteunde linux-installatie als een verzamelaarsapparaat (de verzamelaar kan ook op dezelfde server draaien, raadpleeg cs.co/cesa-pov voor meer informatie)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

- Voor een compleet overzicht van POV of CESA met Splunk gelieve te verwijzen naar cs.co/cesa-pov
- Voor een gids naar CESA NVM Dashboard op Splunk <http://cs.co/cesa-guide>
- Raadpleeg voor meer informatie over de oplossing www.cisco.com/go/cesa.

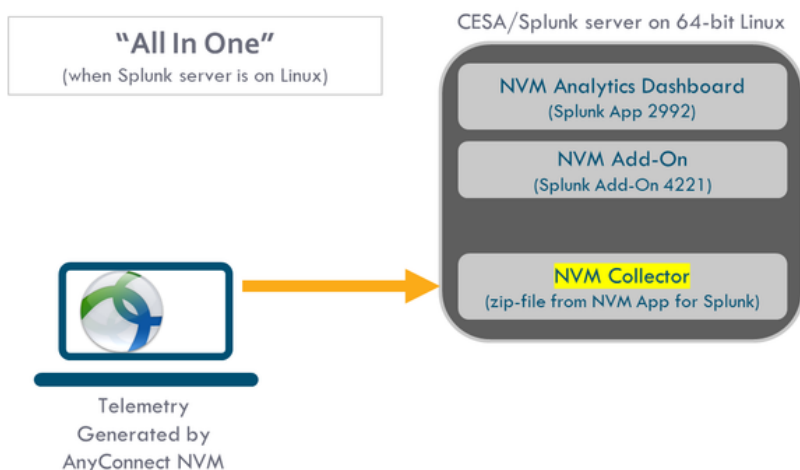
De bestanddelen van de oplossing zijn:

- [Cisco AnyConnect Secure Mobility Client met Network Visibility Module \(NVM\) ingeschakeld](#)
- [Cisco AnyConnect Network Visibility Module-app \(NVM\) voor Splunk](#)
- [Cisco NVM Technology Add-on voor Splunk](#)
- NVM Collector (gebundeld in een zip-bestand met de NVM TA Add-on)

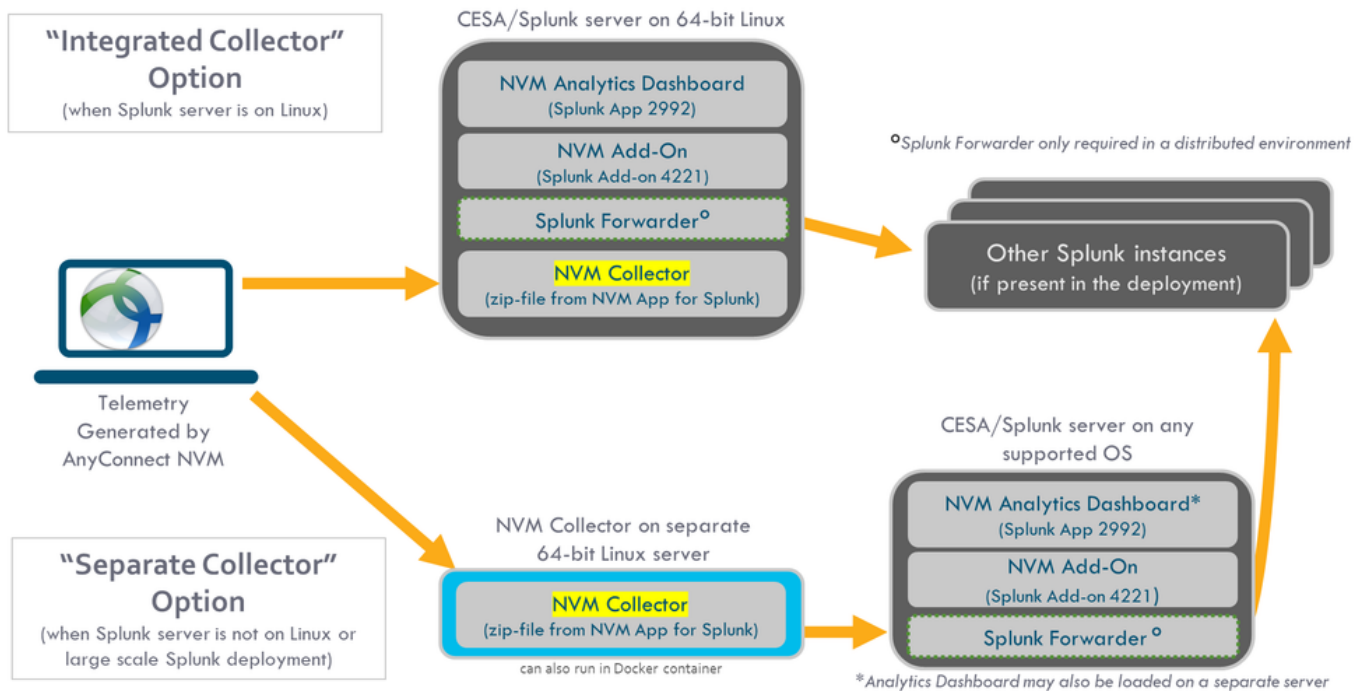
Overzicht van implementaties

Dit is een overzicht op hoog niveau van implementatie in zijn eenvoudigste vorm. Dit is een all-in-one configuratie die draait op 64-bits Linux.

Dit is hoe de meeste demonstraties worden opgezet en ook nuttig is in een kleine productie-installatie.



Dit is een uitgebreidere reeks opties die beschikbaar zijn voor plaatsing. Meestal wordt een productie-instelling gedistribueerd en heeft u verschillende knooppunten voor de onderneming.



Achtergrondinformatie

De Cisco AnyConnect Network Visibility Module biedt een continue feed met hoge-eindpunten telemetrie. NVM stelt organisaties in staat om endpoints en gebruikersgedrag op hun netwerk te zien, verzamelt stromen vanuit endpoints aan en buiten de ruimte, samen met waardevolle contexten zoals gebruikers, toepassingen, apparaten, locaties en bestemmingen. Splunk Enterprise gebruikt de telemetrie en biedt de analytische mogelijkheden en rapporten.

Deze technologie is een configuratievoorbeeld voor AnyConnect NVM met Splunk Enterprise als onderdeel van de nieuwe [CESA](#)-oplossing.

Cisco AnyConnect Secure Mobility Client - meer dan VPN

Cisco AnyConnect is een eengemaakte agent die meerdere beveiligingservices levert om de onderneming te beschermen. AnyConnect wordt meestal gebruikt als een VPN-client voor ondernemingen, maar ondersteunt ook extra modules die rekening houden met verschillende aspecten van de bedrijfsbeveiliging. De extra modules maken veiligheidskenmerken zoals beoordeling van de positie, web veiligheid, malware bescherming, netwerkzichtbaarheid en meer mogelijk.

Deze technologie gaat over Network Visibility Module (NVM), die geïntegreerd is met Cisco AnyConnect om beheerders de mogelijkheid te bieden om internetgebruik te bewaken.

Raadpleeg voor meer informatie over Cisco AnyConnect [Cisco AnyConnect Secure Mobility Client Administrator Guide, release 4.7](#)

Internet Protocol Flow Information Exporteren (IPFIX)

IPFIX is een IETF-protocol om een norm te definiëren voor het exporteren van IP-stroominformatie voor verschillende doeleinden, zoals boekhouding/controle/beveiliging. IPFIX is gebaseerd op Cisco NetFlow Protocol v9, alhoewel niet direct compatibel. [Cisco nvzFlow](#) is een protocolspecificatie die is gebaseerd op het IPFIX-protocol. Door ontwerp, is IPFIX een

uitbreidbaar protocol dat toelaat om nieuwe parameters te definiëren om informatie over te brengen. Cisco nvzFlow-protocol breidt de IPFIX-standaard uit en definieert nieuwe informatie-elementen evenals een standaardset IPFIX-sjablonen die worden verzonden als onderdeel van de telematica die door AnyConnect NVM wordt gebruikt.

Raadpleeg voor meer informatie over IPFIX [rfc5101,rfc7011,rfc7012,rfc7013,rfc7014,rfc7015](#).

IPFIX NVM Collector

Voor meer informatie over de <http://cs.co/nvm-collector>

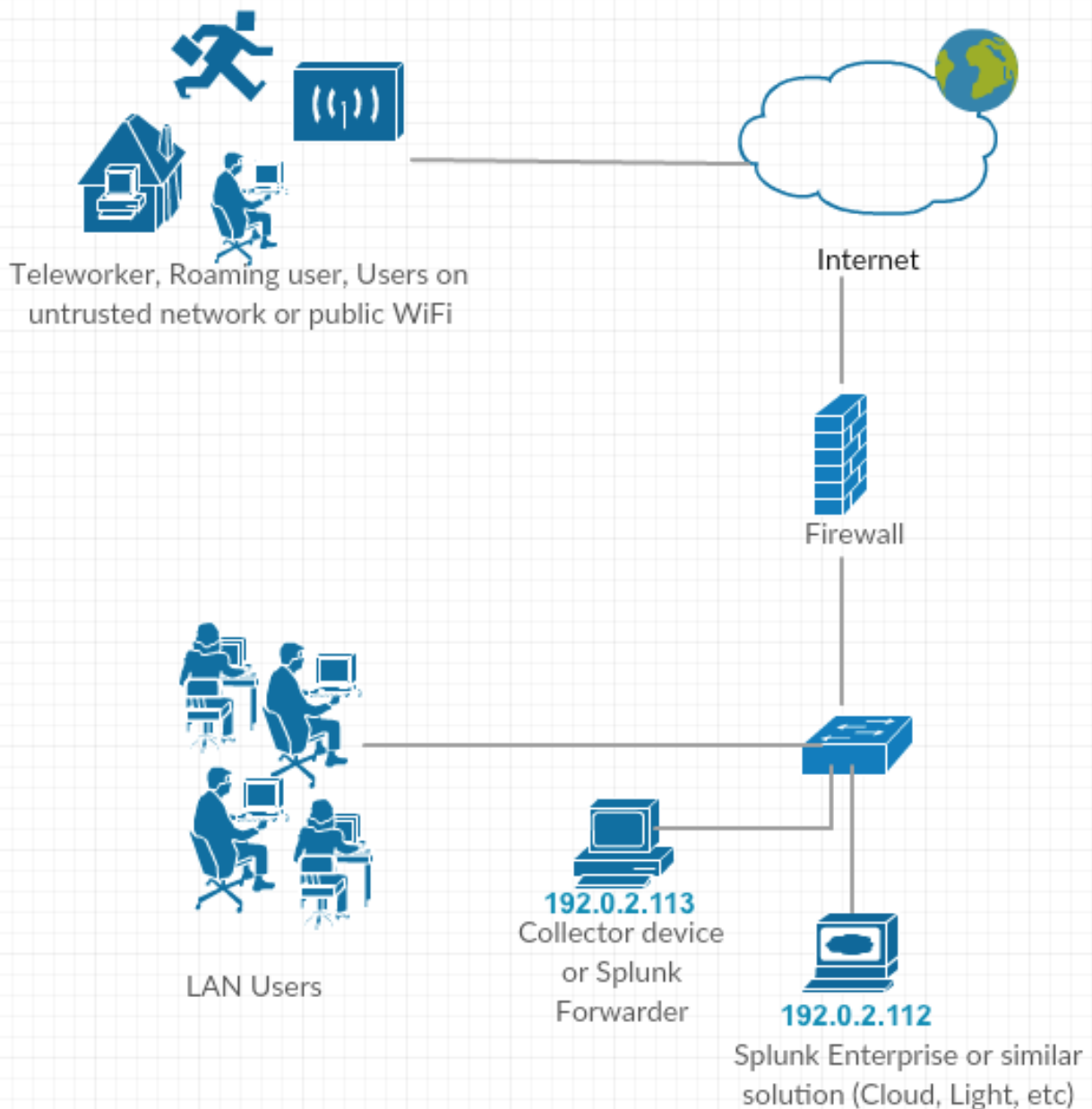
- Een verzamelaar is een server die IPFIX-gegevens ontvangt en opslaat. Het kan deze gegevens dan aan Splunk geven.
- Cisco biedt een verzamelaar die specifiek is ontworpen voor het nvzFlow-protocol en wordt gebundeld met de Splunk App (NVM TA Add-On).
- De verzamelaar kan in hetzelfde vak (all-in-one) met de Splunk-server worden geïnstalleerd. Op de vrachtwagen. Of in een standalone linux doos.

Splunk Enterprise

Splunk Enterprise is een krachtig instrument dat diagnostische gegevens verzamelt en analyseert om betekenisvolle informatie te geven over de IT-infrastructuur. Het biedt een one-stop locatie voor beheerders om gegevens te verzamelen die van cruciaal belang zijn voor het begrip van de gezondheid van het netwerk.

Splunk is een partner van Cisco en de [CESA](#) oplossing werd gemaakt in samenwerking met hen.

Topologie



IP-adresconventies in deze technologie:

IP-adres van verzamelaar: 192.0.2.123

IP-adres splitsen: 192.0.2.113

Configureren

Dit deel heeft betrekking op de configuratie van Cisco NVM-onderdelen.

Voor een overzicht van de implementatie van AnyConnect NVM en het configuratie-profiel wordt ook verwezen naar [Hoe de AnyConnect Network Visibility Module te implementeren](#)

Ondersteuning van DTLS

NVM kan nu worden ingesteld om gegevens via DTLS veilig naar de verzamelaar te sturen. Deze

modus kan worden ingesteld in de NVM Profile Editor. Wanneer het aanvinkvakje "Secure" is ingeschakeld, gebruikt NVM DTLS als transport. Voor de DTLS-verbinding die door moet gaan, dient het DTLS-servercertificaat (collector) op het eindpunt te worden vertrouwd. Onvertrouwde certificaten worden in stilte afgewezen. DTLS 1.2 is de minimale ondersteunde versie. De verzamelaar als deel van CESA Splunk App v3.1.2+ is vereist voor DTLS-ondersteuning. De verzamelaar werkt alleen in één modus, veilig of onveilig.

certificaatvereisten

- Het Collector attest moet worden vertrouwd door de klant (moet ervoor zorgen dat de certificeringsketen betrouwbaar is), er is geen configuratie op AnyConnect.
- Het certificaat moet in PEM-formaat zijn.
- ondersteunt geen wachtwoord voor certificaat en toets (Cisco ISE interne CA vereist één)
- Elk certificaat kan op de verzamelaar worden gebruikt zolang de AnyConnect-clientmachine het vertrouwt (interne PKI, bekend, enz.).
- Nadat het configuratiebestand is bijgewerkt, moet de NVM-service opnieuw worden gestart (voor één client testen). Voor profielen die vanaf ISE/ASA zijn geduwd, moet de verbinding met het netwerk worden verbroken of opnieuw worden aangesloten.
- AC NVM Profile Collector Configuration moet IP of FQDN zijn. Dit hangt af van het gebruik in de GN van het certificaat. FQDN wordt altijd geprefereerd in het geval van IP adresveranderingen. Als u een IP-adres gebruikt, dan moet het verzamelaarscertificaat CN of SAN ook dat IP hebben. Als FQDN als GN in het certificaat staat, moet het NVM-profiel dezelfde FQDN als een verzamelaar hebben.

AnyConnect Configuration (4.9.3043 en hoger) - zie Collector info

NVM-profiel is er een nieuw selectieteken onder de naam Secure voor verzamelaars IP/poort.

AnyConnect Profile Editor - NVM Profile

File Help

NVM Profile

Profile: Untitled

Collector Configuration

IP Address/FQDN	<input type="text"/>
Port	<input type="text"/>
<input checked="" type="checkbox"/> Secure	

Standalone AnyConnect NVM module

Hiervoor is AnyConnect 4.8.01090 of hoger nodig - [AnyConnect Admin Guide voor NVM](#)

Raadpleeg ook de standalone handleiding - [Hoe u de AnyConnect-netwerkzichtbaarheidsmodule implementeert](#)

Voor degenen die geen AnyConnect-implementatie hebben of een andere VPN-oplossing

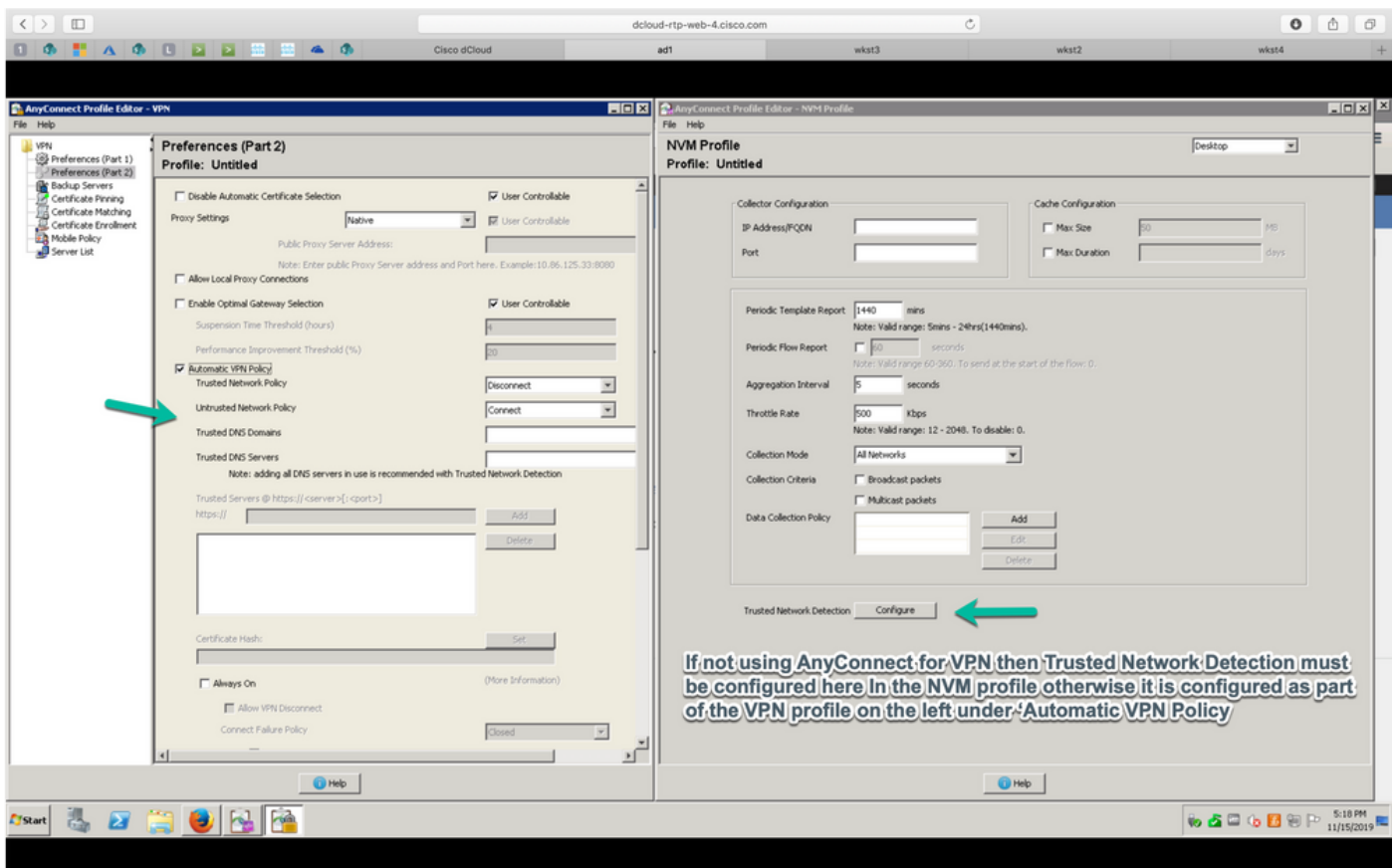
gebruiken, kunt u het NVM-standalone pakket voor uw NVM-behoefte installeren. Dit pakket werkt onafhankelijk, maar biedt hetzelfde niveau van stroomverzameling vanuit een eindpunt als de bestaande AnyConnect NVM-oplossing. Als u de standalone NVM installeert, wijzen de actieve processen (zoals de activiteitsmonitor op macOS) het gebruik aan.

Standalone NVM is ingesteld met de [NVM Profile Editor](#), en Trusted Network Detection (TND)-configuratie is verplicht. Met behulp van de TND-configuratie bepaalt NVM of het eindpunt op het bedrijfsnetwerk ligt en past zij vervolgens het juiste beleid toe.

Problemen oplossen en registreren worden nog steeds uitgevoerd door AnyConnect DART, die vanaf het AnyConnect-pakket kan worden geïnstalleerd.

Voorafgaand aan de zelfstandige, moest de Core VPN module geïnstalleerd zijn om voordeel te halen uit Trusted Network Detection, wat er ook toe leidde dat de gebruiker de kern VPN-bundel in UI zag, die de eindgebruikers in verwarring kan brengen, vooral als zij een andere verkoper VPN-oplossing gebruiken.

Wanneer u de stand-alone gebruikt, gebruikt u het core VPN-profiel niet om TND te configureren. Het NVM-profiel kan nu rechtstreeks voor TND worden ingesteld.



AnyConnect NVM-clientprofiel

AnyConnect NVM configuratie wordt opgeslagen in een XML-bestand met informatie over het IP-adres en poortnummer van de verzamelaar, samen met andere informatie. Het IP-adres van de verzamelaar en een poortnummer moeten correct worden ingesteld in het NVM-clientprofiel.

Voor een correcte werking van de NVM-module moet het XML-bestand in deze map worden geplaatst:

- Voor Windows 7 en hoger: %ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM
- Voor Mac OSX: /opt/cisco/anyconnect/nvm

Als het profiel op Cisco ASA/Identity Services Engine (ISE) aanwezig is, wordt het samen met AnyConnect NVM-implementatie automatisch ingezet.

XML-profielvoorbeeld:

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

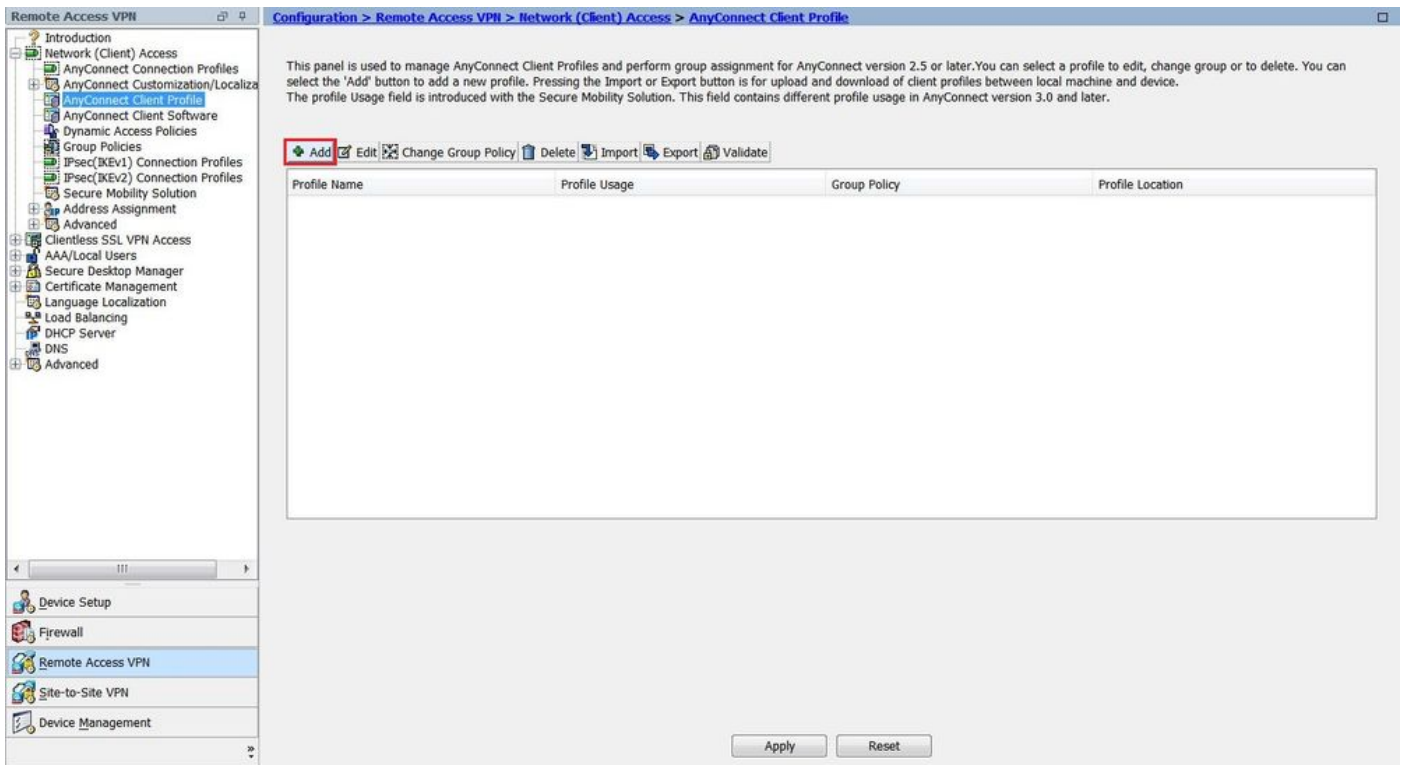
Met deze tools kan NVM-profiel worden gemaakt:

- Cisco ASDM
- AnyConnect-profiel-editor
- Identity Services Engine

NVM-clientprofiel configureren via ASDM

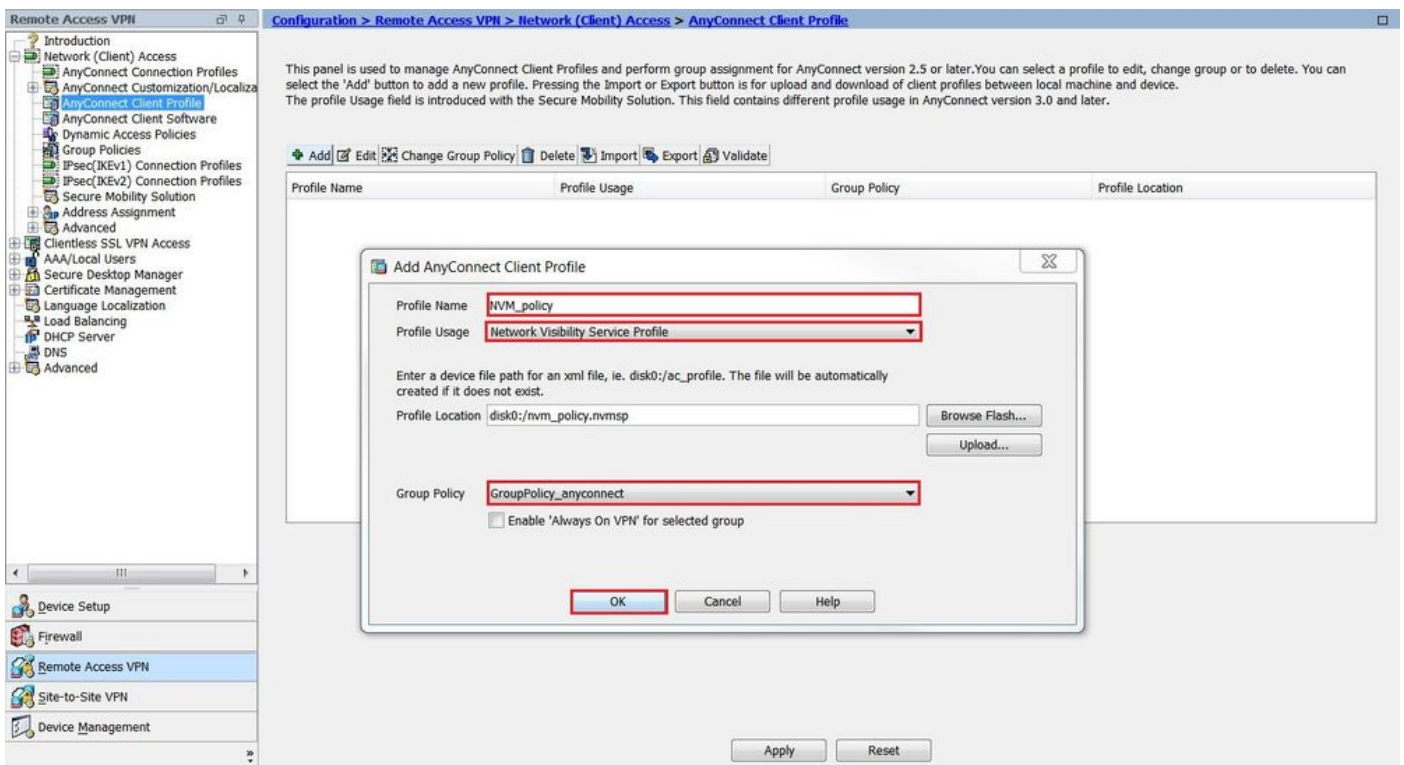
Deze methode is te verkiezen als AnyConnect NVM wordt ingezet via Cisco ASA.

1. Navigeer in op **configuratie > Toegang tot VPN > Toegang tot netwerk (client) > AnyConnect-clientprofiel verwijderen**.
2. Klik op **Add**, zoals in de afbeelding.

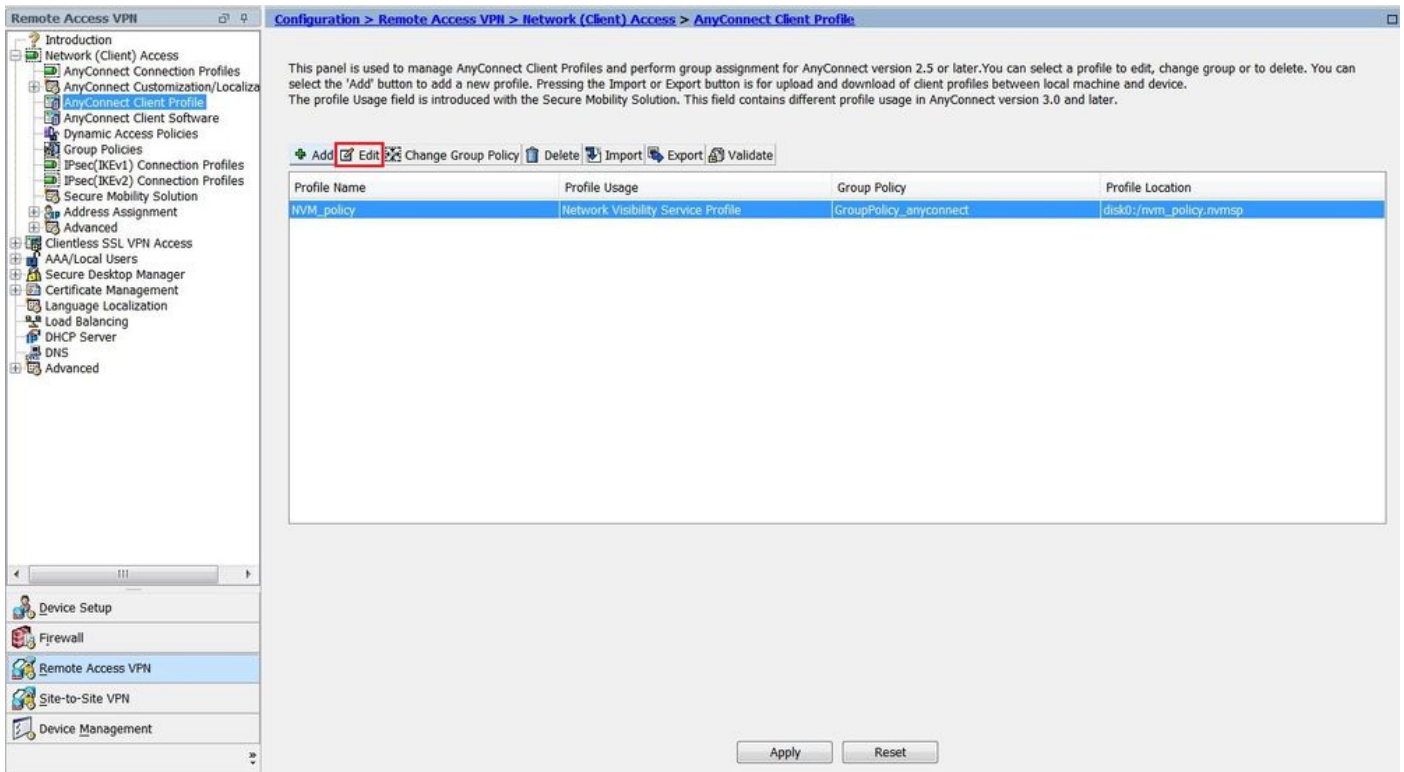


3. Geef het profiel een naam. Selecteer in **profiel gebruik** de optie **Netwerkzichtbaarheidsprofiel**.

4. Wijs het toe aan het groepsbeleid dat door AnyConnect-gebruikers wordt gebruikt en klik op **OK**, zoals in de afbeelding.

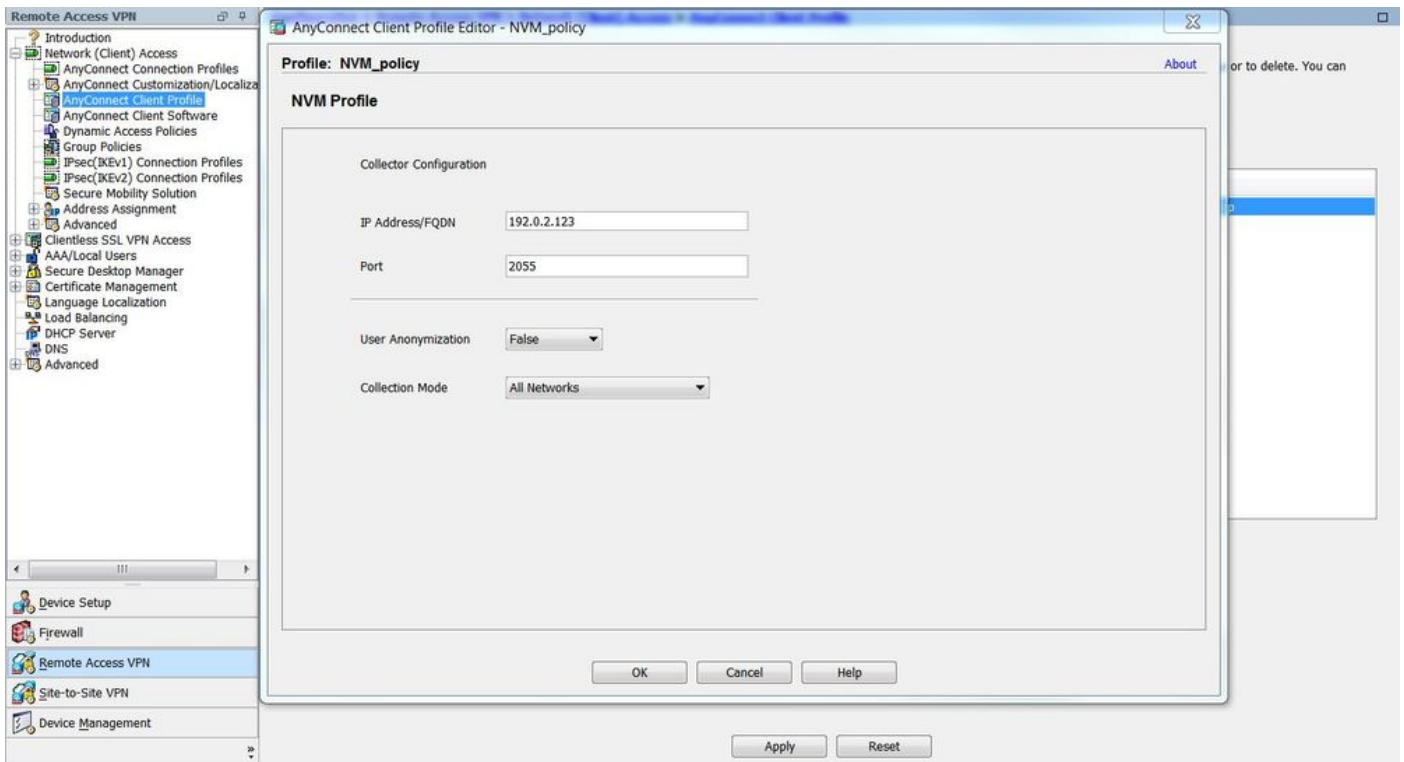


5. Klik op **Bewerken** om het nieuwe beleid te maken, zoals in de afbeelding.



6. Voer de informatie in over het IP-adres en het poortnummer van de verzamelaar en klik op **OK**.

7. Klik nu op **Toepassen**, zoals in de afbeelding.



NVM-clientprofiel configureren via AnyConnect Profile Editor

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect49/administrator/guide/b_AnyConnect_Administrator_Guide_4-9/anyconnect-profile-editor.html#ID-1430-0000061

Dit is een zelfstandige tool die beschikbaar is op Cisco.com. Deze methode is te verkiezen als AnyConnect NVM wordt uitgevoerd via Cisco ISE. Het NVM-profiel dat met dit gereedschap is gemaakt, kan naar Cisco ISE worden geüpload of rechtstreeks naar endpoints worden gekopieerd.

AnyConnect Profile Editor - NVM Profile

File Help

NVM Profile
Profile: Untitled

Collector Configuration

IP Address/FQDN 192.0.2.123

Port 2055

User Anonymization False

Collection Mode All Networks

Help

Raadpleeg voor meer informatie over AnyConnect Profile Editor het volgende:

[De AnyConnect-profiel-editor](#)

Configuratie van WebDeployment op Cisco ASA

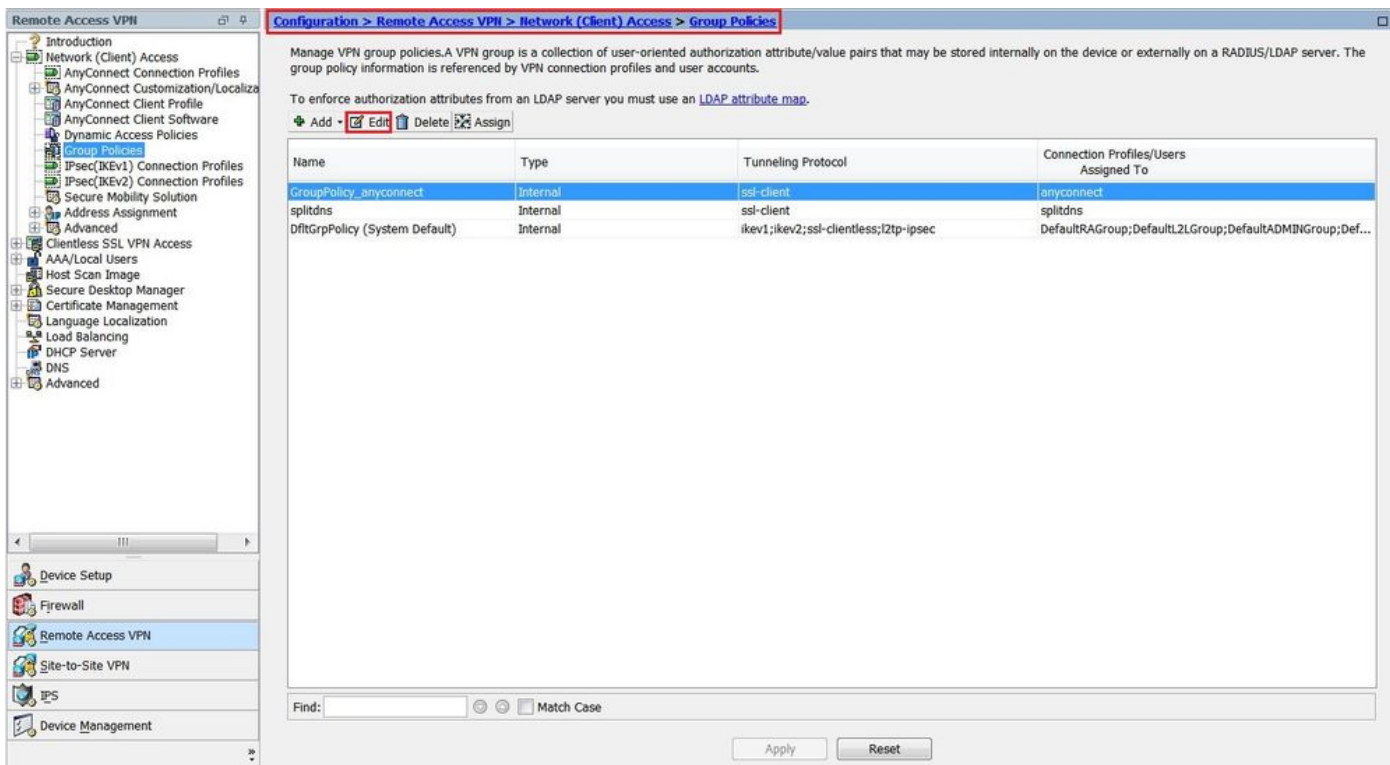
Deze technologie gaat ervan uit dat AnyConnect al op de ASA is geconfigureerd en dat alleen de configuratie van de NVM-module moet worden toegevoegd. Raadpleeg voor meer informatie over ASA AnyConnect-configuratie:

[ASDM Boek 3: Cisco ASA Series 5000 Series VPN ASDM-configuratiegids, 7.5](#)

Voer de volgende stappen uit om AnyConnect NVM-module op Cisco ASA in te schakelen:

1. Navigeer naar **Configuration > Remote Access VPN > Network (Client) Access > Group Policy**.

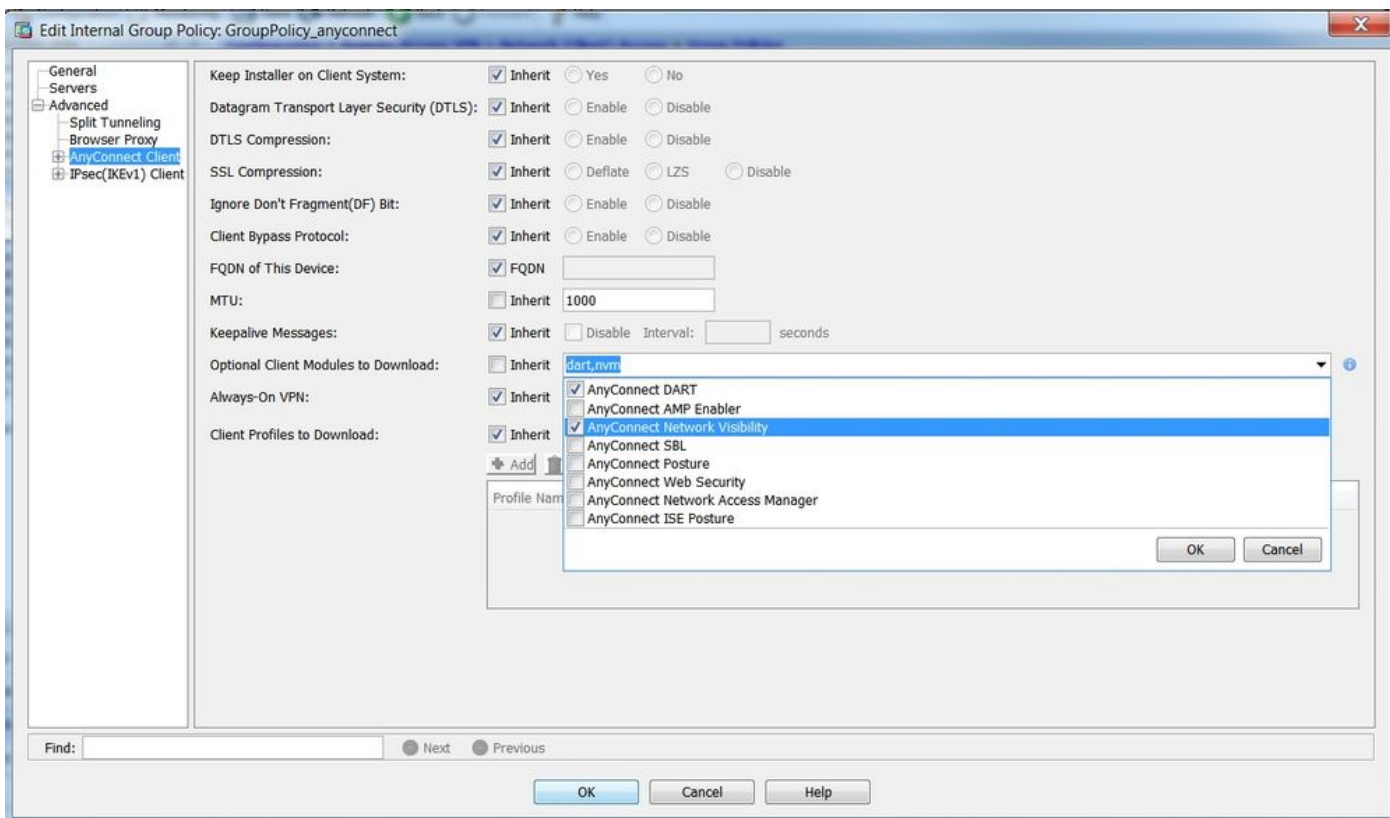
2. Selecteer het betreffende groepsbeleid en klik op **Bewerken**, zoals in de afbeelding.



3. In de pop-up met groepsbeleid, navigeer naar **Advanced > AnyConnect Client**.

4. **Optionele clientmodules** uitvouwen om te downloaden en **Any-connect netwerkzichtbaarheid** te selecteren.

5. Klik op **OK** en pas wijzigingen toe.



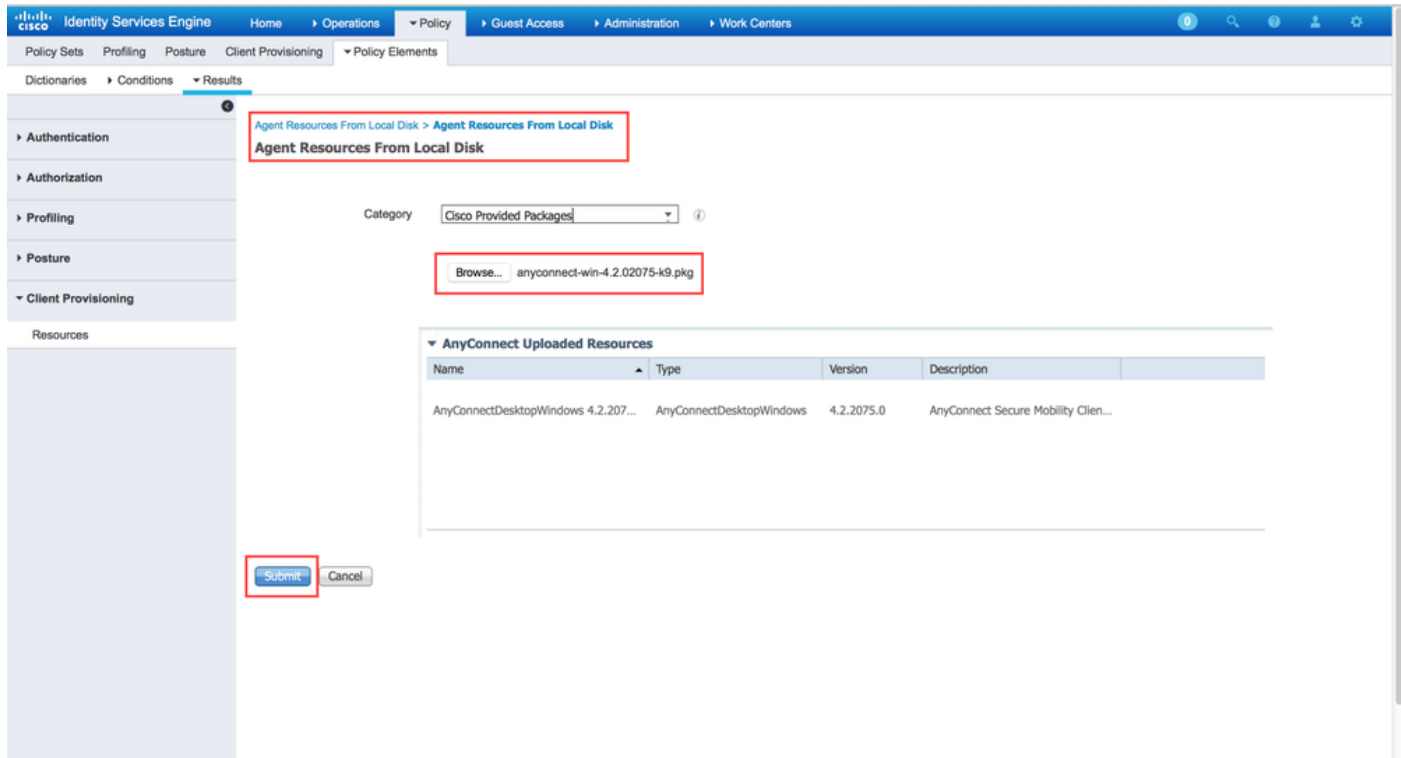
Configuratie van Web-Plaatsing op Cisco ISE

Om Cisco ISE voor AnyConnect Web-Deployment te configureren voert u deze stappen uit:

1. In Cisco ISE GUI, navigeer naar **Beleid > Elementen van het Beleid > Resultaten**.
2. **Clientprovisioning** uitvouwen om **bronnen** weer te geven en **bronnen** te selecteren.

Afbeelding toevoegen:

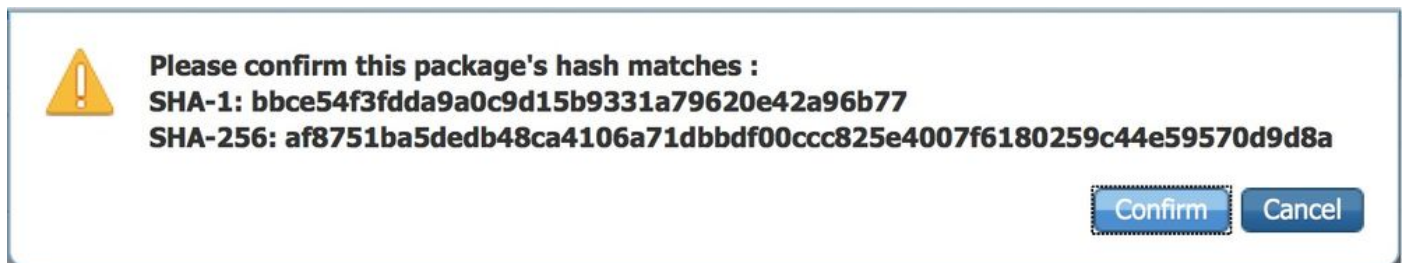
Stap 1. Selecteer **Add > Agent Resources** en uploaden het Any Connect pakketbestand.



Stap 2. Bevestig de hash van de verpakking in de pop-up.

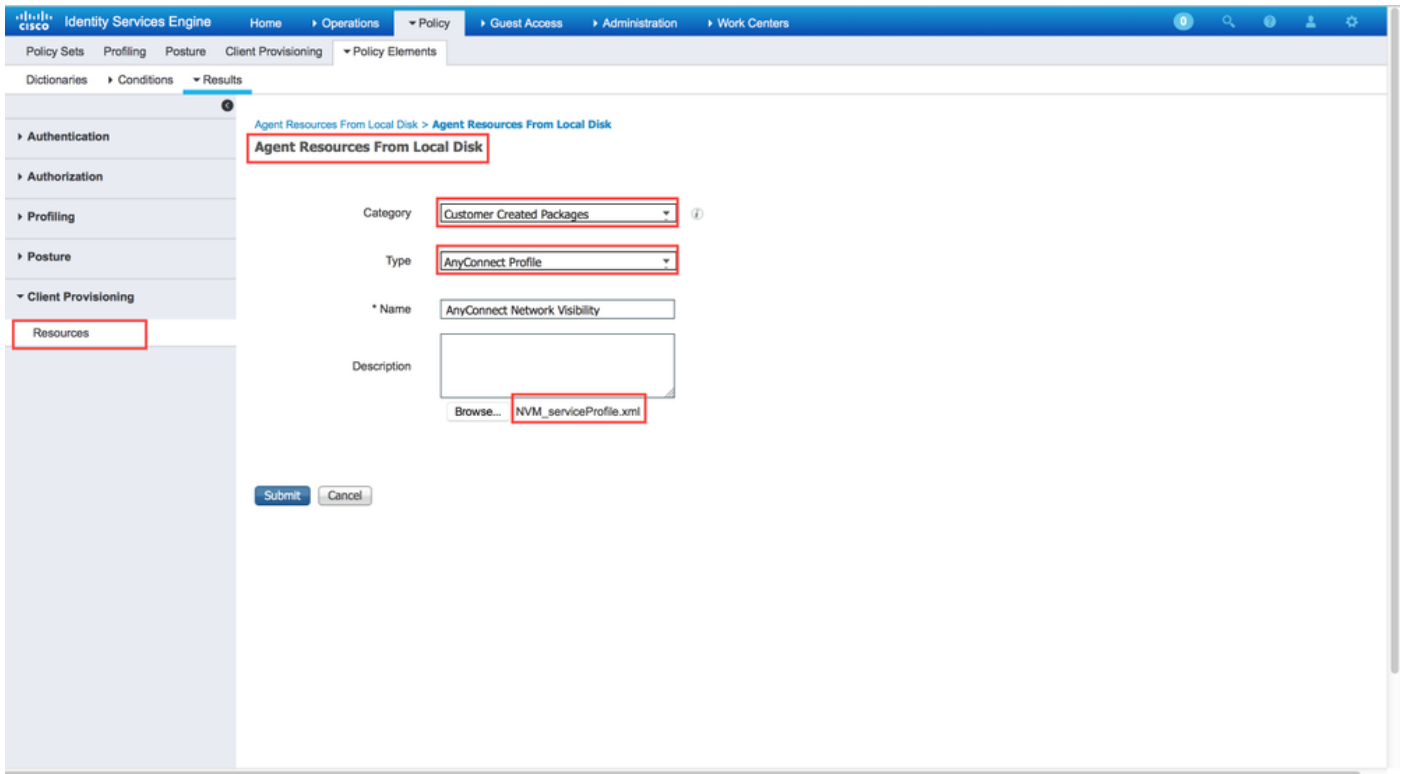
Het bestand-hash kan worden geverifieerd via de downloadpagina van Cisco.com of met een gereedschap van derden.

Deze stap kan worden herhaald om meerdere AnyConnect-afbeeldingen toe te voegen. (voor Mac OSX en Linux OS)



NVM-profiel toevoegen:

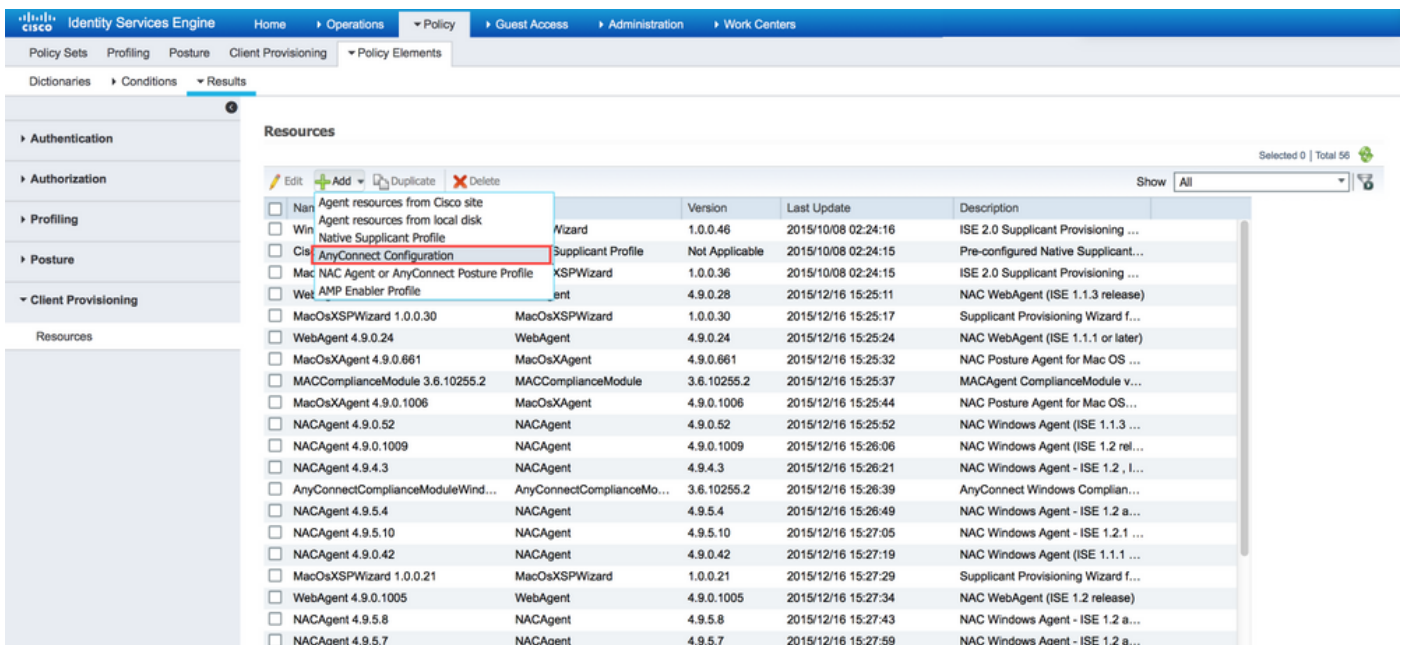
Stap 1. Selecteer **Add > Agent Resources** en uploadt het NVM-clientprofiel.



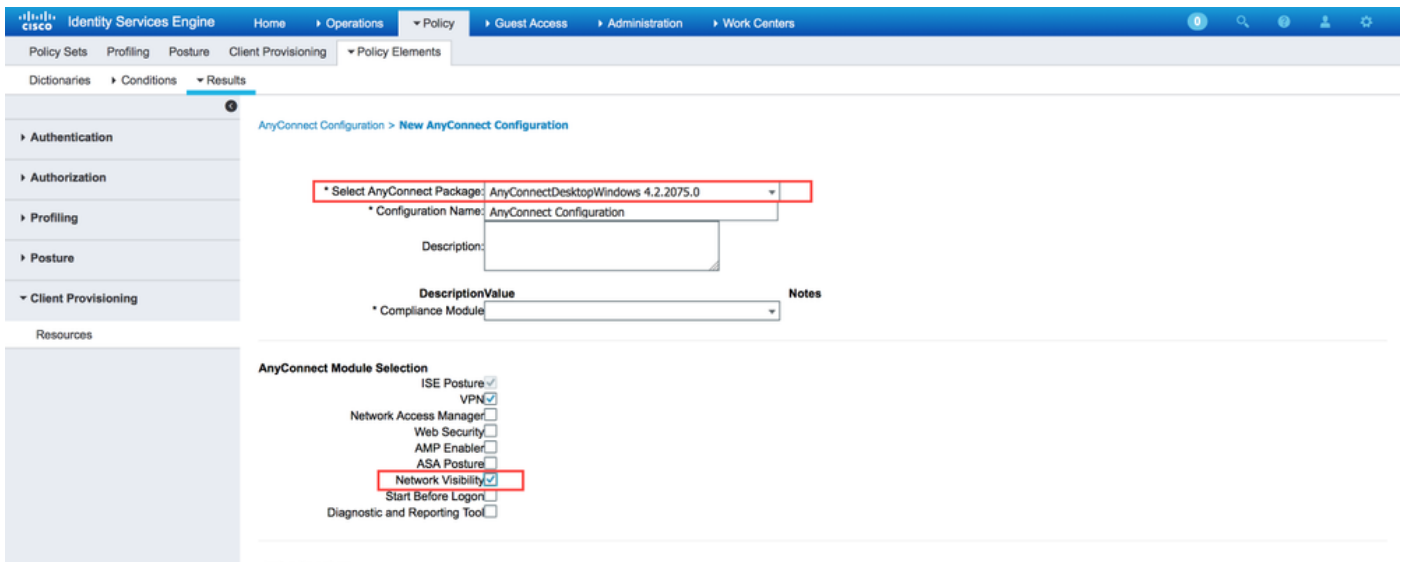
Geef configuratie bestand toe:

Stap 1. Klik op **Add** en kies **AnyConnect Configuration**

Selecteer het pakket dat in de vorige stap is geüpload.



Stap 2. Schakel NVM in de selectie van AnyConnect Module samen met het gewenste beleid.



In dit gedeelte kunnen we AnyConnect-clientmodules, profielen, customization/taalpakketten en de Opswat-pakketten inschakelen.

Raadpleeg voor gedetailleerde informatie over de configuratie van webimplementatie op Cisco ISE:

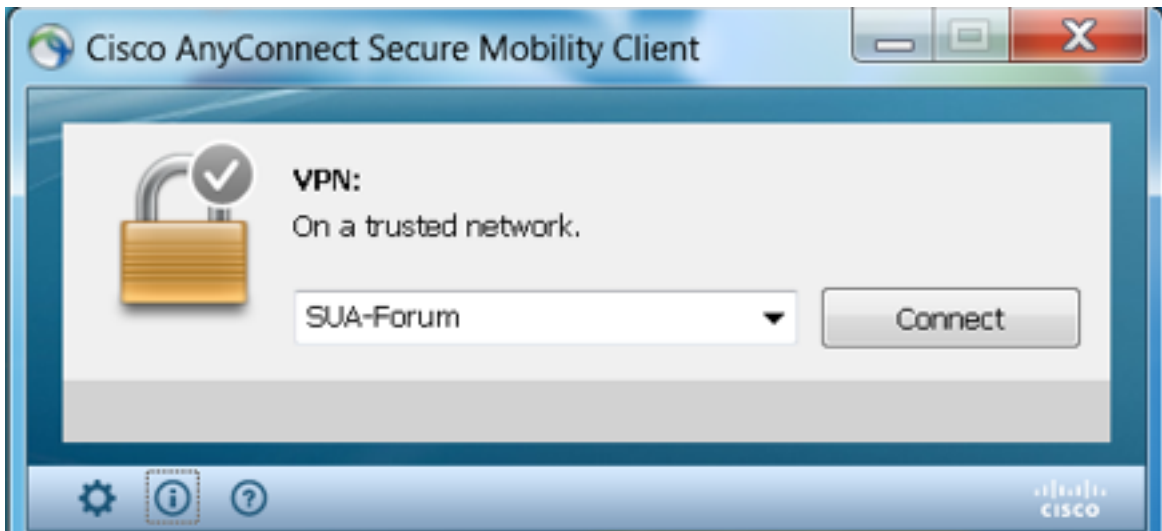
[Web-implementering van AnyConnect](#)

Trusted Network Detectie

AnyConnect NVM verstuurt alleen stroominformatie als deze op een betrouwbaar netwerk is geïnstalleerd. Het gebruikt de TND-functie van AnyConnect-client om te weten of het eindpunt in een vertrouwd netwerk zit of niet.

Trusted Network Detectie is ingesteld in AnyConnect Client Profile (XML) dat voor VPN wordt gebruikt, ongeacht of de VPN-component in de omgeving is gebruikt of niet. TND is ingeschakeld door de sectie Automatisch VPN-beleid in het profiel te configureren. minimaal moet één Trusted DNS-domein of Trusted DNS-server worden ingevuld. De acties van AnyConnect wanneer de client heeft bepaald dat deze op een betrouwbaar netwerk is uitgevoerd, kunnen worden ingesteld op **DoNiets** Mode met behulp van de pull-down voor het Trusted en Unvertrouwde Network Policy.

XML Profile (excerpt)	ASDM PROFILE EDITOR (excerpt)
<pre data-bbox="162 1594 778 1742"><AutomaticVPNPolicy>>true <TrustedDNSDomains>demo.local</TrustedDNSDomains> <TrustedDNSServers>10.1.100.10</TrustedDNSServers> <TrustedNetworkPolicy>DoNothing</TrustedNetworkPolicy> <UntrustedNetworkPolicy>DoNothing</UntrustedNetworkPolicy> <AlwaysOn>>false </AlwaysOn> </AutomaticVPNPolicy></pre>	



Raadpleeg voor meer informatie over de TND-configuratie:

[Trusted Network Detectie configureren](#)

implementeren

Deployment Any Connect NVM-oplossing omvat de volgende stappen:

1. Configureer de NVM met AnyConnect op Cisco ASA/ISE.
2. Stel IPFIX Collector component (NVM Collector op Linux in - Packaged in the TA Add-On) in.
3. Stel Splunk in met Cisco NVM App en TA Add-On.

Stap 1. Configureer de NVM via Cisco ASA/ISE

Deze stap is in detail behandeld in de sectie Configure.

Als NVM eenmaal is ingesteld op Cisco ISE/ASA, kan deze worden geautomatiseerd naar client-endpoints.

Stap 2. Stel IPFIX Collector Component in (AnyConnect NVM Collector)

De Collector Component is verantwoordelijk voor het verzamelen en vertalen van alle IPFIX-gegevens van de endpoints en het doorsturen naar de [Splunk Add-On](#). De NVM collector draait op 64-bits Linux. De configuratiescripts van CentOS, Ubuntu en Docker zijn opgenomen. De installatie scripts en configuratiebestanden van CentOS kunnen ook in Fedora en Redhat distributions worden gebruikt.

In een typische gedistribueerde plaatsing van Splunk Enterprise zou de verzamelaar moeten worden uitgevoerd op of een standalone 64-bits Linux-systeem of [Splunk Forwarder](#)-knooppunt dat op 64-bits Linux wordt gebruikt. Het kan ook op een standalone server zonder splunkcomponenten worden geïnstalleerd.

Opmerking: De oplossing kan ook worden uitgevoerd op één enkel 64-bits Linux-systeem dat de NVM-verzamelaar en Splunk Enterprise-componenten bevat voor gebruik in een kleine implementatie of voor demonstratiedoeleinden. all-in-one is het makkelijkst voor tot

10.000 eindpunten - zie [CESA POV, grootte van informatie](#).

Hoe installeert u de Collector?

1. Kopieer de **adapter.zip**file, bevindt zich in de **/opt/splunk/etc/apps/\$APP_DIR\$/appserver/addon/** (meegeleverd met de TA Add-On)-map voor het systeem waarop u de map wilt installeren.
2. Extraceer de bestanden (unzip acnvmCollector.zip)

Het wordt aanbevolen het **\$PLATFORM\$_README**-bestand in de bundel.zip te lezen voordat het **install.sh** script uitvoert. Het **\$PLATFORM\$_README**-bestand bevat informatie over de relevante configuratie-instellingen die moeten worden geverifieerd en aangepast (indien nodig) voordat het **install.sh** script wordt uitgevoerd. U moet ten minste het adres van de Splunk-instantie configureren waarnaar u gegevens doorstuurt. Wanneer u het systeem niet correct instelt, kan dit ertoe leiden dat de verzamelaar niet correct werkt.

Opmerking: Zorg ervoor dat de netwerk- en host-firewalls correct zijn geconfigureerd om het UDP-verkeer voor de bron- en doeladressen en -poorten toe te staan. Het IPFIX (flow) verkeer dat van de om het even welke klanten aan de verzamelaar en de uitgaande UDP gegevens aan Splunk (hier) komt.

Een enkele NVM-verzamelaar kan een minimum van 5000 stromen per seconde verwerken op een goed gesorteerd systeem. Of tot 35-40.000 eindpunten. De verzamelaar moet worden geconfigureerd en actief voordat de Splunk NVM en TA-Add op App kunnen worden gebruikt.

De standaardinstelling is dat de verzamelaar stromen ontvangt van AnyConnect NVM endpoints op UDP-poort 2055.

Daarnaast produceert de verzamelaar drie gegevensfeeds voor Splunk, Per Flow Data, Endpoint Identity Data en Endpoint Interface Data op UDP-poorten 20519, 20520 en 20521.

De poorten voor ontvangen en gegevensinvoer kunnen worden gewijzigd door het **acnvm.conf**-bestand te wijzigen en de verzamelaarsinstantie te herstarten. Zorg ervoor dat elke host/netwerk firewall tussen endpoints en de verzamelaar of tussen de verzamelaar en het Splunk-systeem(s) open is voor de geconfigureerde UDP-poorten en -adressen. Zorg er ook voor dat de configuratie van AnyConnect NVM overeenkomt met de configuratie van uw verzamelaar.

Nadat alle onderdelen zijn geïnstalleerd en uitgevoerd, raadpleegt u het gedeelte Help-bestanden vanuit de Splunk-toepassing voor meer informatie over de vooraf ingestelde rapporten, het gegevensmodel en de informatie-elementen die door de oplossing zijn gemaakt.

U kunt één van uw AnyConnect-eindpunten opnieuw opstarten en valideren dat gegevens naar de oplossing worden verzonden. Start een vaste gegevensstroom met behulp van YouTube.

De informatie moet in het configuratiebestand worden geconfigureerd - acnvm.conf

- **syslog_server_ip** (expediteur of splunk instantie) kan naar 127.0.0.1 (gebruik LOCALHOST niet) wijzen als deze op hetzelfde doosje staat
- Het standaard poort voor de verzamelaar (inkomende IPFIX-gegevens) is niet geschikt.

OPMERKING: netflow_Collector_ip wordt weggelaten van het configuratiebestand (het gebruikt de standaard openbare interface), het zou slechts moeten worden veranderd om met een specifiek lokaal IP te omzeilen

Per Flow Data-poort, Endpoint Identity Data-poort, Endpoint Interface Data en Collector Port zijn vooraf ingesteld op standaardinstellingen in het configuratiebestand. Zorg ervoor dat deze waarden worden gewijzigd indien niet-standaard poorten worden gebruikt.

Deze informatie wordt toegevoegd in het configuratiebestand - **/opt/acnvm.conf**

Ondersteuning van DTLS

(zie NVM DTLS-informatie voor meer informatie)

Dit gebeurt in het doosje waarin de verzamelaar wordt getoond.

- Maak folder **/opt/acnvm/certs**.
- Om het certificaat toe te passen op de verzamelaar, slaat u het op met de toets in de directory **opt/acnvm/certs**
- wijzig de eigenaar en de groep van de map in **acnvm:acnvm** met deze opdracht: **sudo chown -R acnvm:acnvm certs/**:
- Dit gedeelte voor **acnvm.conf** moet worden geconfigureerd met de cert en de toets
- Nadat de configuratie en cert zijn geplaatst, start de verzamelaar - **sudo systemctl start acnvm.service**
- Controleer de status van verzamelaar - **sudo systemctl status acnvm.service**

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

Hier is de rest op de configuratie.

```
"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, "correlate_data": false }
```

3. het install.sh script uitvoeren met superuser privileges (zoals ./install.sh)

Opmerking: De account heeft aangepaste rechten of wortel nodig om de install.sh en de toegangsrechten voor de ACM Service Account te kunnen uitvoeren.

Raadpleeg voor meer informatie <https://splunkbase.splunk.com/app/2992/#/details>

Stap 3. Stel Splunk in met Cisco NVM App (CESA Dashboard) en TA Add-On voor Splunk.

Cisco AnyConnect NVM App voor Splunk is beschikbaar op de Splunkbasis. Deze app helpt met vooraf gedefinieerde rapporten en dashboards om IPFIX (nvzFlow)-gegevens te gebruiken van endpoints in bruikbare rapporten en correleert gebruiker- en endpointgedrag.

Opmerking: Voor cloudimplementaties worden beide apps geïnstalleerd in de cloudinstantie.

Alleen de technische bijstand is op het gebouw geïnstalleerd (met de expediteur). De verzamelaar wordt op het gebouw met de expediteur of op een afzonderlijk linux/docker vakje geïnstalleerd.

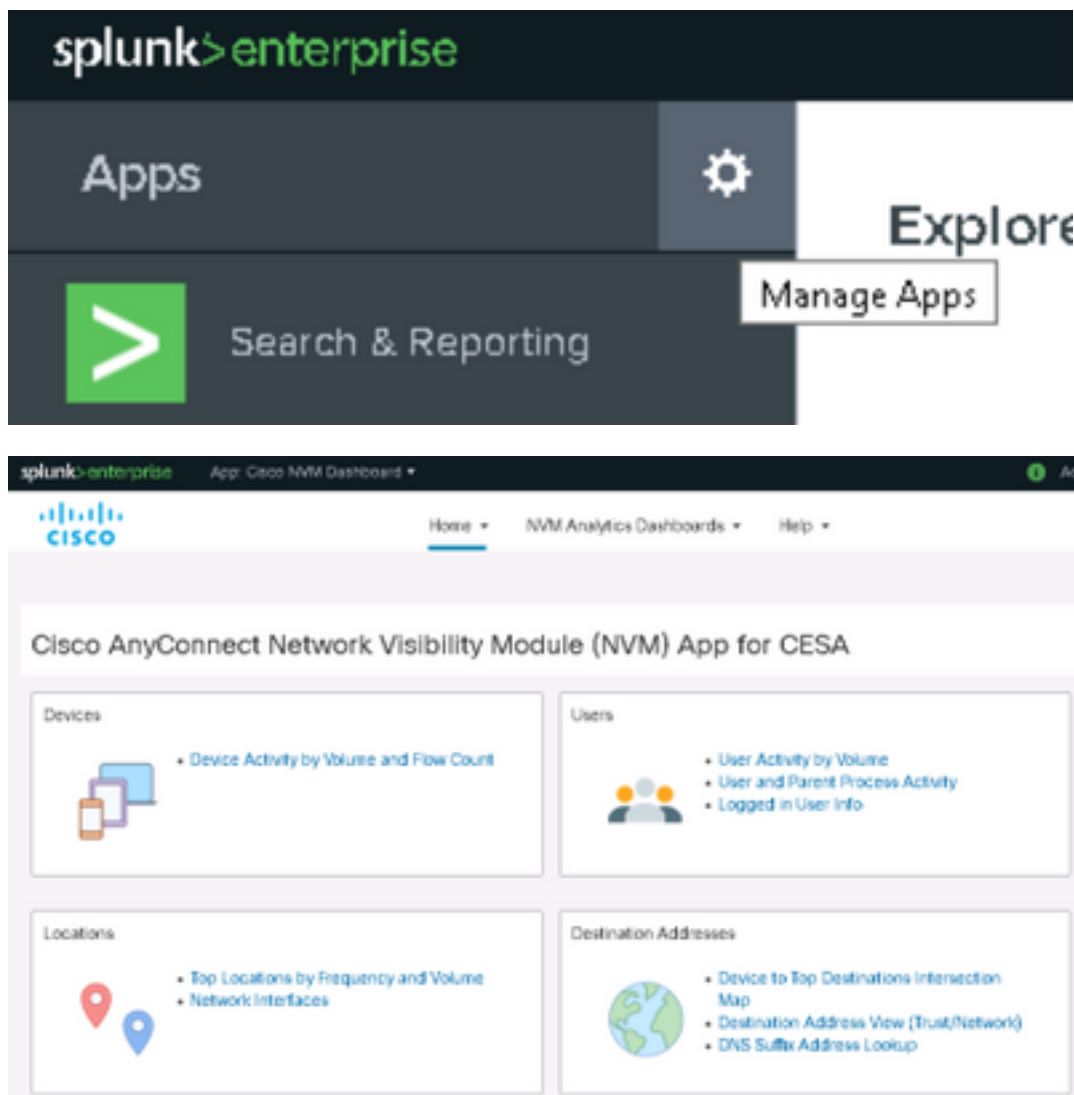
Voor een aanmelding kunt u alleen alle onderdelen en apps in één vak installeren (of afzonderlijk) zie diagrammen

Download deze bestanden:

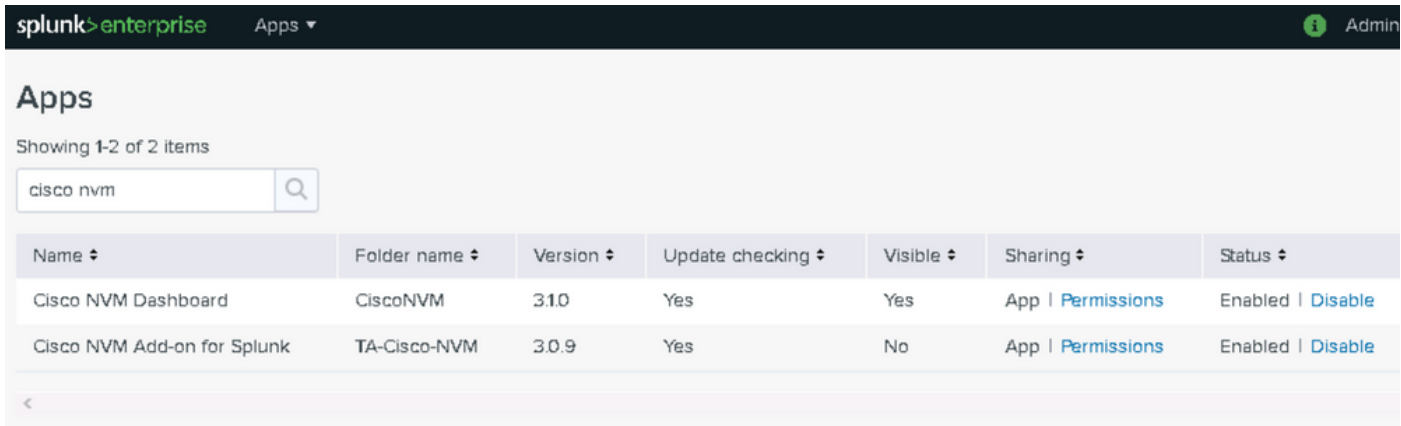
- Cisco NVM App voor Splunk op Splunkbase: <https://splunkbase.splunk.com/app/2992/>
- Cisco NVM Add-on voor Splunk op Splunkbase: <https://splunkbase.splunk.com/app/4221/>

Installeren

Stap 1. Navigeer naar **Splunk > Apps** en klik op het gereedschap en installeer het bestand **tar.gz** dat u hebt gedownload van de Splunkbasis of zoekopdracht in het Apps-gedeelte.



Stap 2. Daarna moet u de **Add-On** installeren met hetzelfde proces. Controleer of beide geïnstalleerd zijn door de pagina **Splunk Apps** te bekijken:



De standaardconfiguratie ontvangt drie gegevensfeeds voor Splunk, Per Flow Data, Endpoint Identity Data en Endpoint Interface Data, respectievelijk op UDP-poorten 20519, 20520 en 20521 (zie Stap 2)

De add-on zet deze dan in kaart aan Splunk source **Cisco:nvm:stroomgegevens**, **Cisco:nvm:sysgegevens** en **Cisco:nvm:ifgegevens**.

UDP-ingangen inschakelen met behulp van Splunk Management UI

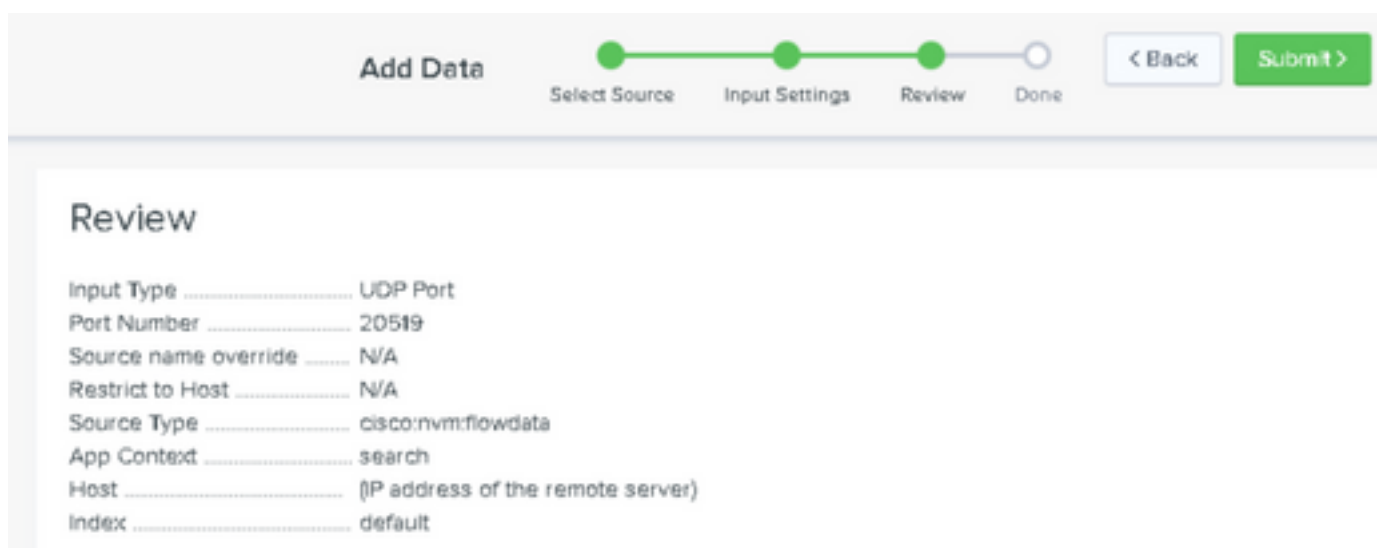
Opmerking: Dit kunt u ook doen met een input.conf-bestand. Dit wordt uitgelegd in de Cisco NVM Dashboard-app in de Help-functie

U hoeft de software van Splunk niet opnieuw te starten.

Navigeer naar **Splunk > Instellingen > Data Input > UDP** zoals in de afbeelding.

1. Klik op New Local UDP > Voer poort in # ontbrekend > Klik op Volgende > selecteer corresponderend brontype > Klik op **Review** > Klik op Inzenden

2. Doe dit met de andere 2 poorten (probeer de kloon te gebruiken)



UDP

Data inputs » UDP

[New](#)

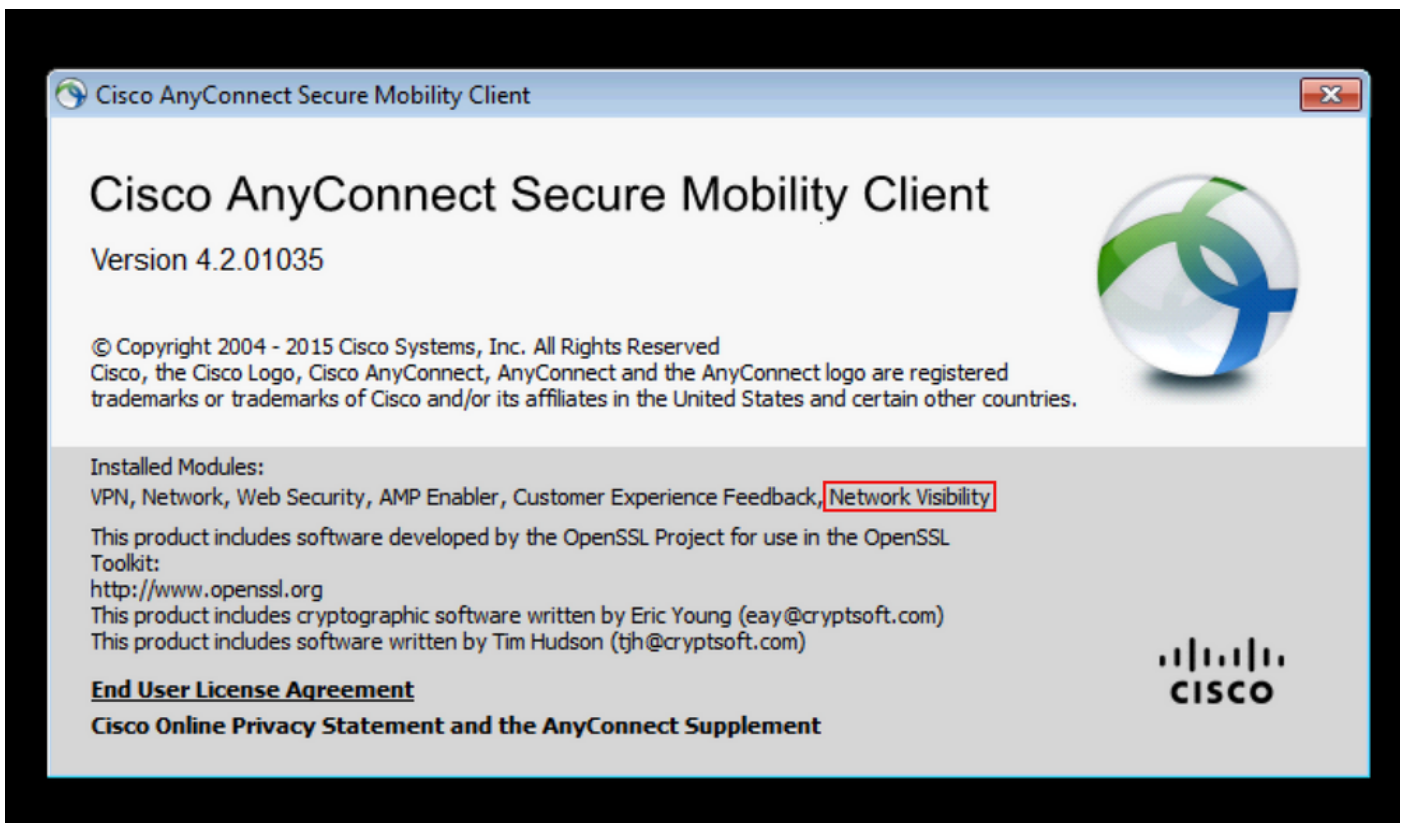
Showing 1-3 of 3 items

UDP port ↕	Source type ↕	Status ↕
20519	cisco:nvm:flowdata	Enabled
20520	cisco:nvm:sysdata	Enabled
20521	cisco:nvm:ifdata	Enabled

Verifiëren

AnyConnect NVM-installatie valideren

Na een succesvolle installatie moet de netwerkzichtbaarheidsmodule worden opgenomen in **geïnstalleerde modules**, in het gedeelte **Informatie** van de client voor Any Secure Mobility.



Controleer ook of de nvm-service op het eindpunt wordt uitgevoerd en het profiel in de vereiste map staat.

Valideren van Collector status als actief

Zorg ervoor dat de status van de verzamelaar actief is. Dit waarborgt dat de verzamelaar te allen

tijde IPFIX/flow uit de eindpunten ontvangt. Als deze niet actief is, zorg er dan voor dat de cnvm account rechten voor het bestand het uitvoeren toestaan: `/opt/acnvm/bin/acnvmcollector`

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

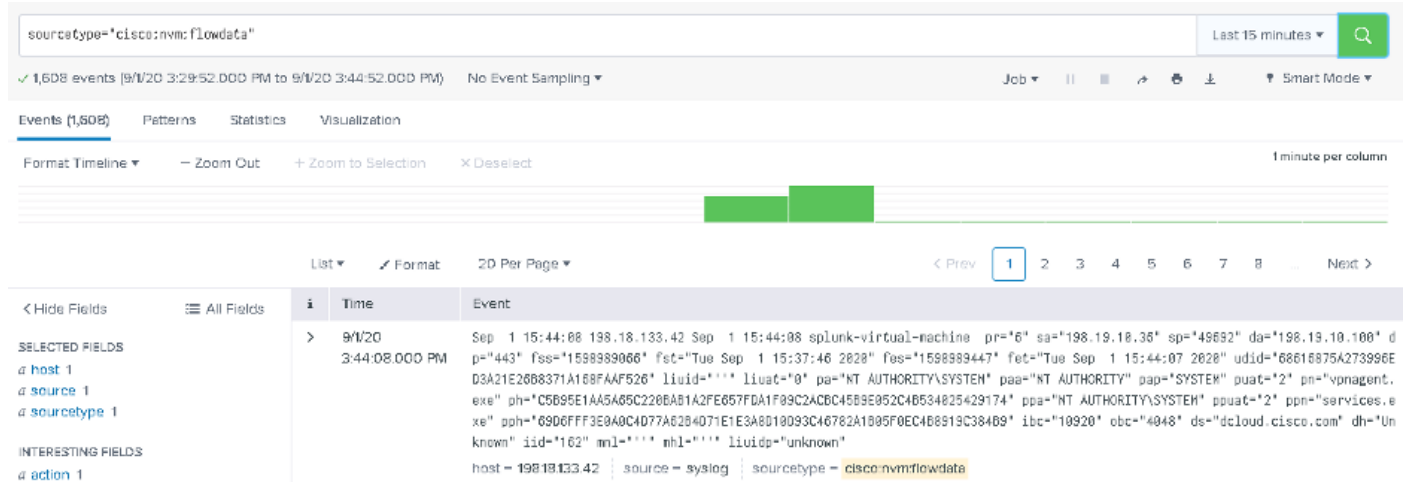
```
[splunk@splunk-virtual-machine addon]$ systemctl status acnvm.service
● acnvm.service - AC NVM Service
   Loaded: loaded (/usr/lib/systemd/system/acnvm.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2020-06-19 13:48:08 EDT; 25s ago
     Main PID: 41165 (acnvmcollector)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

Splunk valideren - AnyConnect NVM CESA Dashboard

Zorg ervoor dat Splunk en zijn relevante services actief zijn. Raadpleeg hun website voor documentatie over het oplossen van problemen met Splunk.

Niet de dashboards voor CESA zullen niet worden bijgewerkt tot 5 minuten nadat de eerste gegevens zijn ontvangen vanwege een automatiseringsscript. Start een handmatige zoekopdracht om direct te valideren:

Klik vanaf het hoofddashboard op "Zoeken en rapporteren". Stel in het volgende scherm het juiste bereik in om de gewenste gegevens op te geven en waar er op staat: "Typ hier zoekopdracht...". Voer "sourcetype=cisco:nvm:flow data" in



Controleer het Splunk Dashboard om ervoor te zorgen dat Ga naar Splunk, klik op **Cisco NVM Dashboard**, klik op **Apparaatactiviteit door volume en Flow Count** als u de huidige instellingen wilt behouden en klik op **Inzenden**. Het geeft gegevens in de illustratie weer.

PacketFlow

1. IPFIX-pakketten worden gegenereerd op client-endpoints door AnyConnect NVM-module.
2. De client-eindpunten sturen IPFIX-pakketten naar het IP-adres van de verzamelaar.

3. De verzamelaar verzamelt de informatie en stuurt deze naar Splunk.

4. Verzamelaar stuurt op drie verschillende stromen verkeer naar Splunk: Per Flow data, endpointgegevens en interfacegegevens.

Al het verkeer is UDP dat is gebaseerd op de afwezigheid van ontvangstbevestiging.

Standaardpoort voor verkeer:

IPFIX-gegevens 2055

Per Flow Data 2019

Endpoint Data 20520

Interfacegegevens 20521

NVM-module slaat IPFIX-gegevens op en stuurt deze naar een verzamelaar wanneer deze zich in Trusted Network bevindt. Dit kan zijn wanneer de laptop is aangesloten op het bedrijfsnetwerk (on-prem) of wanneer hij via VPN is verbonden.

U kunt valideren dat de verzamelaar pakketten ontvangt van de NVM-module door een pakketvastlegging op specifieke UDP-poorten uit te voeren, zoals in uw configuratie wordt aangegeven om te controleren of de pakketten worden ontvangen. Dit gebeurt via het Splunk-systeem linux OS.

Flow-sjablonen

De IPFIX-stroomsjablonen worden naar de verzamelaar gestuurd aan het begin van de IPFIX-communicatie. Deze sjablonen helpen de verzamelaar om de IPFIX-gegevens te begrijpen.

De verzamelaar voegt ook sjablonen toe om er zeker van te zijn dat zelfs als de klant ze niet heeft verstuurd, de gegevens kunnen worden geparseerd. Als een nieuwere versie van de client wordt vrijgegeven met protocolwijzigingen, worden de nieuwe sjablonen gebruikt die door de client worden verstuurd.

Een sjabloon wordt onder deze voorwaarden verzonden:

1. Er is een verandering in het NVM-clientprofiel.
2. Er is een evenement voor netwerkverandering.
3. De spoeddienst is opnieuw gestart.
4. Het eindpunt wordt herstart/herstart.
5. Periodiek (standaard=24 uur) zoals ingesteld in het NVM Profile.

In zeldzame gevallen is er mogelijk geen sjabloon gevonden. Dit kan eenvoudig worden verholpen door een van de eindpunten opnieuw te starten.

De kwestie kan worden geïdentificeerd door het observeren van **geen sjabloon die is gevonden** in een pakketvastlegging op het eindpunt of **geen sjablonen voor stromen die zijn ingesteld** in de collector logs.

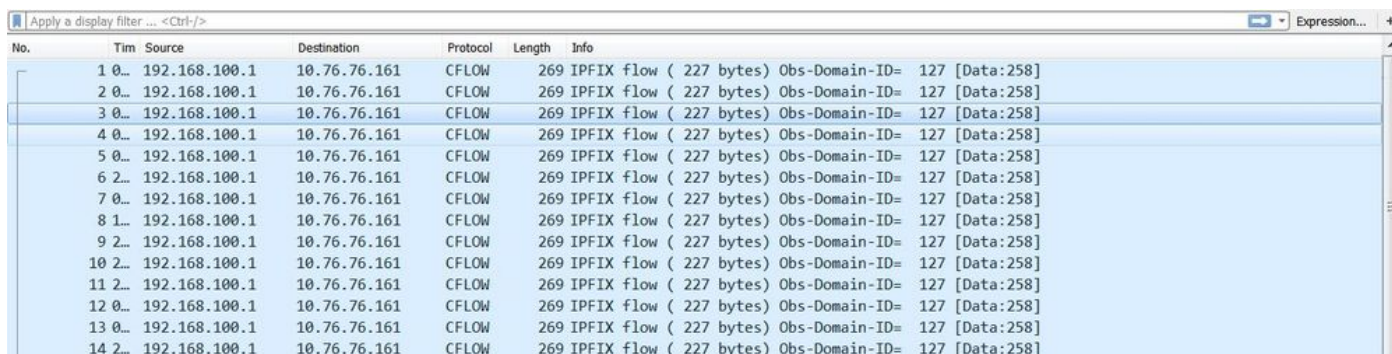
Problemen oplossen

Dit zijn de basisstappen voor probleemoplossing:

1. Zorg voor netwerkconnectiviteit tussen client-eindpunt en verzamelaar.
2. Zorg voor netwerkconnectiviteit tussen verzamelaar en splunk.
3. Zorg ervoor dat NVM op de juiste manier op het cliënteindpunt is geïnstalleerd.
4. Pas opnames op het eindpunt toe om te zien of het IPFIX verkeer wordt gegenereerd.
5. Toepassen opnames op een verzamelaar om te zien of het IPFIX verkeer ontvangt en of het verkeer naar Splunk doorgeeft.
6. Toepassen opnames op Splunk om te zien of het verkeer ontvangt.
7. Voor DTLS alle klanten die vertrouwen op het verzamelaarscertificaat NVM-profiel is beveiligd verzamelaar is ingesteld voor certs

IPFIX-verkeer zoals in Wireshark gezien:

Opmerking: Als u DTLS tussen de client en de verzamelaar gebruikt, moet u een filter op DTLS-verkeer filteren



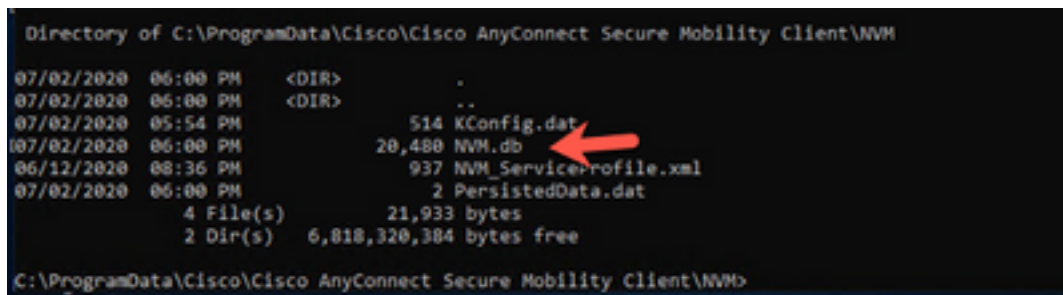
The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of 14 IPFIX flow records. Each record has a 'No.' column, a 'Time' column, a 'Source' IP address (192.168.100.1), a 'Destination' IP address (10.76.76.161), a 'Protocol' of 'CFLOW', a 'Length' of 269 bytes, and an 'Info' column containing 'IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]'. The interface includes a filter bar at the top and a packet list on the left.

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]

AnyConnect-client (NVM-module)

AnyConnect NVM - niet rapporteren aan de Collector - CFLOW-datapakketten blijven geen eindpunt achter

Groeit het NVM database bestand onder C:\%ProgramData%\Cisco\Cisco Anyconnect Secure Mobility Client? Als het blijft groeien betekent dit dat de logboeken niet van de klant worden verstuurd. Als je onder de NVM-map kijkt, zie je dat de sql-database groeit, dan is de nvm.db niet gedocumenteerd, maar we praten uitgebreid over hoe we caching in de [NVM-gids](#) en de controles rond caching in [de NVM-gids](#). Als je dat ziet, stuurt het de gegevens niet naar de verzamelaar.



The screenshot shows a Windows command prompt window with the following output:

```
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_Service_Profile.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>
```

A red arrow points to the 'NVM.db' file in the directory listing.

Trusted Network Detection (TND)

Start AnyConnect UI en zorg ervoor dat dit op een betrouwbaar netwerk gebeurt. NVM is

afhankelijk van TND voor het detecteren van het eindpunt in een betrouwbaar netwerk. Als de TND-configuratie niet correct is, levert dit problemen op met NVM. NVM heeft zijn eigen TND-configuratie, die werkt op de TLS-certificaatvingerafdruk van de geconfigureerde server. Dit kan worden ingesteld in de NVM Profile Editor.

Als NVM TND niet is geconfigureerd, is NVM afhankelijk van de TND-configuratie van de VPN-module. VPN's TND werkt op basis van informatie die via DHCP wordt ontvangen: domeinnaam en DNS-server. Als de DNS-server en/of de domeinnaam overeenkomen met de ingestelde waarden, wordt het netwerk als betrouwbaar beschouwd. VPN ondersteunt ook TLS op certificaat gebaseerde TND-detectie.

- Zorg ervoor dat de Trusted Network Detectie-configuratie juist is. NVM exporteert alleen wanneer dit op een betrouwbaar netwerk gebeurt, d.w.z. een ongeldige TND-configuratie (bijvoorbeeld: als u 3 DNS-servers hebt, hebt u 3 gedefinieerd) nodig.
- Verwijder het vertrouwde domein van de TND VPN-configuratie
- Netwerkkwesties: gesplitste tunneling (het IP-adres van de verzamelaar maakt geen deel uit van de gesplitste tunnel die wordt vertrouwd, zodat de gegevens worden verzonden naar de openbare interface). Zorg ervoor dat de IP van de verzamelaar altijd in de splitsingen zit, ook voor VPN.
- Zorg ervoor dat de Collector is ingesteld om deze op het huidige netwerk te verzamelen (vertrouwde/onvertrouwde).
- Zorg ervoor dat de mappen VPN.xml en NVM_ServiceProfile.xml in de juiste mappen staan en opnieuw starten
- Start-stop alle aansluitingsservices
- Staak het netwerk dat op de binnenkant is aangesloten en dat een verbinding met de DNS server heeft.

PacketCapture:

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

AnyConnect diagnostiek en rapportage-tools (DART)

Om een oplossing te vinden doet AnyConnect [DART](#) uitvoeren op de NVM-onderdelen.

- Alle logbestanden die nodig zijn voor NVM worden door DART verwerkt, worden opgeslagen, geconfigureren, enzovoort.
- Windows logs - Evenementen zijn niet op één locatie, er is een apart blad in de eventviewer voor NVM onder AnyConnect.
- macOS/linux - filterbestanden per medium

Collector (op Linux/Docker machine - all-in-one of standalone)

acnvmCollector is niet geïnstalleerd :

Terwijl u verzamelaar installeert en het script installeert

```
Sudo ./install_ubuntu.sh
```

Ik krijg een fout in de var/log/syslog. "Acnvm.conf-fout: regel nummer 17 : verwacht belangrijke string" dit was omdat er een komma was waar je niet zou moeten zijn, misschien nog een extra

acnvmCollector kan niet starten :

Dit was een probleem op Ubuntu (maar mogelijk voor alle linux). Ik merkte op dat de code niet in het collectorbestand is uitgevoerd: `/opt/acnvm/bin/acnvmcollector`.

De actieve gebruiker en de groep hadden geen eXecute voor de adapter

```
csaxena@ubuntu-splunk:/etc/init.d$ systemctl status acnvm
● acnvm.service - AC NVM Service
   Loaded: loaded (/lib/systemd/system/acnvm.service; enabled; vendor preset: enabled)
   Active: failed (Result: exit-code) since Fri 2020-09-18 02:49:10 UTC; 1min 57s ago
   Process: 7119 ExecStart=/opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf
   Main PID: 7119 (code=exited, status=203/EXEC)

Sep 18 02:49:10 ubuntu-splunk systemd[1]: acnvm.service: Scheduled restart job, restart counter is at 5.
Sep 18 02:49:10 ubuntu-splunk systemd[1]: Stopped AC NVM Service.
Sep 18 02:49:10 ubuntu-splunk systemd[1]: acnvm.service: Start request repeated too quickly.
Sep 18 02:49:10 ubuntu-splunk systemd[1]: acnvm.service: Failed with result 'exit-code'.
Sep 18 02:49:10 ubuntu-splunk systemd[1]: Failed to start AC NVM Service.
lines 211/211 (200) / skipping...
● acnvm.service - AC NVM Service
   Loaded: loaded (/lib/systemd/system/acnvm.service; enabled; vendor preset: enabled)
   Active: failed (Result: exit-code) since Fri 2020-09-18 02:49:10 UTC; 1min 57s ago
   Process: 7119 ExecStart=/opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/conf/filters.conf -b [code=exited, status=203/EXEC]
   Main PID: 7119 (code=exited, status=203/EXEC)

Sep 18 02:49:10 ubuntu-splunk systemd[1]: acnvm.service: Scheduled restart job, restart counter is at 5.
Sep 18 02:49:10 ubuntu-splunk systemd[1]: Stopped AC NVM Service.
Sep 18 02:49:10 ubuntu-splunk systemd[1]: acnvm.service: Start request repeated too quickly.
Sep 18 02:49:10 ubuntu-splunk systemd[1]: acnvm.service: Failed with result 'exit-code'.
Sep 18 02:49:10 ubuntu-splunk systemd[1]: Failed to start AC NVM Service.
```

Collector logs

Hoe kan ik verificaties van de verzamelaar verkrijgen?

```
./nvmcollector -v
```

Waar kan ik het debug instellen?

U kunt het logniveau in ACMNVMLOG.conf instellen - het gedeelte van de configuratie dat naar het opstartbeeld van de computer wordt verzonden. Start na een verandering de verzamelaar opnieuw op.

log4cplus.rootLogger=DEBUG, STDOUT, NVMFileAppender < dit is te vinden in **ACNVMLOG.conf**-bestand

```
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
```

DTLS-kwesties:

- DTLS niet ingesteld (middelen zijn niet gezien in het acnvm.conf-bestand)
- De servertoets is ongeldig (dit was een toetsencombinatie met het wachtwoord dat niet wordt

ondersteund)

Splunk Console (NVM Dashboard) geeft geen gegevens weer

AnyConnect-client

- Gegevens genereren met behulp van YouTube en misschien browsen naar een paar website
- Kan een client informatie via UDP 2055 naar de verzamelserver sturen (zijn er daartussen firewalls?) probeert telnet van clientmachine naar verzamelmachine
- Draai draadloos shark om er zeker van te zijn dat de client verkeer (2055 cflow) gegevens naar de verzamelaar stuurt

Verzamelbak

- Waarderen van het ontvangen van AnyConnect NVM-verkeer Voer een bom uit (en zorg ervoor dat u pakketten van client tot server op 25001 tot 2055 ziet) Sudo tcPDump -l any-c100-nn host 10.1.10.7 (dit betekent dat eerst 100 pakketten afkomstig zijn van IP-clienthost)[Hoe wordt TCPDUMP op tellers gebruikt](#)
- Zorg ervoor dat de NVM-verzamelaar van anyconnect actief is (zie bovenaan informatie met behulp van het systeem)
- Controleer cnvm.conf op de opmaak, ontbrekende quotes, komma's enz
- **Splunk UI** - TA - zijn de UDP-gegevensinvoer en de productie van brongegevens die zijn ingesteld op de Splunk GUI of via Input.conf
Start opnieuw op onder **UI > Instellingen > servercontroles**

Vaak gestelde vragen (veelgestelde vragen)

1. Hoe kunt u gegevens van een willekeurige NVM naar meerdere bestemmingen sturen?

Dit wordt gebruikt voor een hoge beschikbaarheid of voor het verzenden naar Splunk en Stealthwatch.

Zie voor meer informatie <http://cs.co/cesa-pov>

2. Waar slaat u het certificaatmodel op voor AnyConnect NVM DTLS?

Dit zou voor laboratoriumtesten zijn waar geen bekende cert geïnstalleerd is op de verzamelaar.

- Windows

Installeer het certificaat van de verzamelaar in de Windows Vertrouwde certificaten

- Mac OSX

Voor het installeren van het wortelcertificaat is het proces standaard en duidelijk gedefinieerd voor macOS dat via een sleutelketen verloopt, kunnen we Trefkettengereedschap gebruiken om te

importeren en toe te voegen zoals u wilt.

- Linux - verschillend voor elke distro (Ubuntu en RHEL).

RHEL Root CA-IMPORTSTAPPEN:

1. Kopieer de **cabine** naar **enz/pki/ca-trust/bron/ankers**
2. **sudo update-ca trust**
3. Ten slotte **sudo update-ca-trust extract**

Ubuntu Root CA IMPORT STAPS :

1. K-bestand converteren naar .crt-bestand. openssl x509 - stelt PEM-in RootCA.cer-out rootCa.crt
2. Kopieer het .crt-bestand naar **/usr/local/share/ca-certificaten**
3. Start de opdracht **sudo update-ca-certificaten**

XML-bestandsnamen

Wanneer u de lokale profieleditor gebruikt. De XML-profielnaam van de kern VPN-module doet er niet toe. "Sla het profiel op als NVM_ServiceProfile.xml. U moet het profiel met deze exacte naam opslaan, anders kan NVM gegevens niet verzamelen en verzenden."

Collector (anyconnect NVM)

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

- Kan een folder onder wortel worden gemaakt en daarna het eigendom aan een andere rekening worden verstrekt? U kunt eerst **een NVM maken/opteren/nvm maken** zolang het installatiescript toestemming heeft om bestanden te kopiëren
- Bestandsrechten - **install.sh** moet toegangsrechten om als root te implementeren
- dienstrekeningen: Waarom **gebruiker add -r**, en waarom **s/bin/vals** omdat het een niet interactieve account zonder adresdirectory isHet is geen vereiste dat een adresboekje en de standaardpraktijk van de dienstrekening geen "clean"-account hebbenAlle gebruikers hebben uid/gids of zij al dan niet een huisfolder hebben.
- Verzamelaar OS - stelt CentOS, Ubuntu, Redhat kunnen gebruiken CentOS script.
- Installeer het script - kan indien nodig worden aangepast. Moet worden uitgevoerd als root of met SUDO rechts omdat het een nieuwe gebruiker creëert die **acnvm** heet en alles in een **opt/acnvm** directory plaatst.Algemene opmerking: U kunt ook uw eigen script maken om te doen wat u volgens uw vereisten moet doen. Dit script kan een andere gebruiker gebruiken die al op het systeem actief is, maar deze gebruiker heeft SUDO-rechten nodig om de installatie te kunnen uitvoeren.
- De collector versie werkt met -v flag **./opt/acnvm/bin/acnvmcollector-v**

Aanbevolen release

Cisco raadt altijd de nieuwste softwareversie van AnyConnect aan op het moment van gebruik of update. Wanneer u de AnyConnect-versie kiest, gebruikt u de nieuwste 4.9.x-client of hoger. Dit levert de meest recente verbeteringen met betrekking tot NVM.

AnyConnect 4.9.0086 nieuwe functies

Dit is een belangrijke release die deze functies bevat en updates ondersteunt, en die de tekortkomingen oplost die in [AnyConnect 4.9.0086](#) worden beschreven

- NVM-uitbreiding om stroom- en endpointgegevens te verrijken, inclusief nieuwe NVM Collector, gecoördineerd met Splunk-app 3.x en een tijdstempel voor stroominformatie.

Gerelateerde informatie

- [Cisco Endpoint Security Analytics op Splunk \(Quick Start Guide\)](#)
- [Cisco AnyConnect Network Visibility and \(NVM\) app voor Splunk](#)
- [Splunk Documentatie over Splunk Collector Setup en het installeren van collector scripts](#)
- [Cisco AnyConnect Secure Mobility Client-beheergids](#)
- [Releaseopmerkingen van AnyConnect 4.x](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)