

Installieren und Konfigurieren von AnyConnect NVM 4.7.x oder höher und zugehörigen Splunk Enterprise-Komponenten für CESA

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Bereitstellungsübersicht](#)

[Hintergrundinformationen](#)

[Cisco AnyConnect Secure Mobility Client - Mehr als VPN](#)

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

[IPFIX NVM-Collector](#)

[Splash Enterprise](#)

[Topologie](#)

[Konfigurieren](#)

[DTLS-Unterstützung](#)

[Zertifikatanforderungen](#)

[Standalone AnyConnect NVM-Modul](#)

[AnyConnect NVM-Clientprofil](#)

[Konfigurieren des NVM-Clientprofils über ASDM](#)

[Konfigurieren des NVM-Clientprofils über den AnyConnect-Profil-Editor](#)

[Konfigurieren der Web-Bereitstellung auf der Cisco ASA](#)

[Konfigurieren der Web-Bereitstellung auf der Cisco ISE](#)

[Erkennung vertrauenswürdiger Netzwerke](#)

[Bereitstellen](#)

[Schritt 1: Konfigurieren von AnyConnect NVM auf Cisco ASA/ISE](#)

[Schritt 2: Einrichten der IPFIX Collector-Komponente \(AnyConnect NVM Collector\)](#)

[Wie wird der Collector installiert?](#)

[DTLS-Unterstützung](#)

[Schritt 3: Richten Sie Splunk mit der Cisco NVM-App \(CESA-Dashboard\) und dem TA-Add-On für Splunk ein.](#)

[Installieren](#)

[Aktivieren von UDP-Eingaben mithilfe der Splunk-Verwaltungs-Benutzeroberfläche](#)

[Überprüfung](#)

[Überprüfen der NVM-Installation von AnyConnect](#)

[Collector-Status als "Ausführen" validieren](#)

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

[Paketfluss](#)

[Flussvorlagen](#)

[Fehlerbehebung](#)

[AnyConnect-Client \(NVM-Modul\)](#)

[AnyConnect NVM - Nicht für den Collector gemeldet - CFLOW-Datenpakete verlassen nicht je Endgerät](#)

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

[Anyconnect Diagnostic and Reporting Tools \(DART\)](#)

[Collector \(auf Linux/Docker-Computer - All-in-One oder Standalone\)](#)

[Die Splunk Console \(NVM Dashboard\) zeigt keine Daten an.](#)

[AnyConnect-Client](#)

[Collector-Box](#)

[Häufige Fragen \(FAQs\)](#)

[1. Wie können Sie Daten von anyconnect NVM an mehrere Ziele senden?](#)

[2. Wo speichern Sie das Zertifikat für AnyConnect NVM DTLS?](#)

[XML-Dateinamen](#)

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

[Empfohlene Version](#)

[AnyConnect 4.9.00086 Neue Funktionen](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt die Installation und Konfiguration des Cisco AnyConnect Network Visibility Module (NVM) auf einem Endbenutzersystem mit AnyConnect 4.7.x oder höher sowie die Installation und Konfiguration der zugehörigen Splunk Enterprise-Komponenten und NVM Collector.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- AnyConnect 4.7.x oder höher mit NVM
- AnyConnect-Lizenzierung
- ASDM 7.5.1 oder höher
- Vertrautheit mit Splunk Enterprise und Installation von Splunk Apps und Add-ons

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco AnyConnect Security Mobility Client 4.7.x oder höher

- Cisco AnyConnect Profile Editor
- Cisco Adaptive Security Appliance (ASA), Version 9.5.2
- Cisco Adaptive Security Device Manager (ASDM), Version 7.5.1
- Splunk Enterprise 7.x oder höher (als All-in-One-Lösung auf jedem unterstützten Linux installiert, CentOS bevorzugt)
- Alle unterstützten Linux-Installationen als Collector-Gerät (Collector kann auch auf demselben Server ausgeführt werden; weitere Informationen finden Sie [unter cs.co/cesa-pov](http://cs.co/cesa-pov))

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

- Eine vollständige Übersicht über den POV von CESA mit Splunk finden Sie unter cs.co/cesa-pov
- Leitfaden zum CESA NVM-Dashboard auf Splunk <http://cs.co/cesa-guide>
- Weitere Informationen zur Lösung finden Sie unter www.cisco.com/go/cesa.

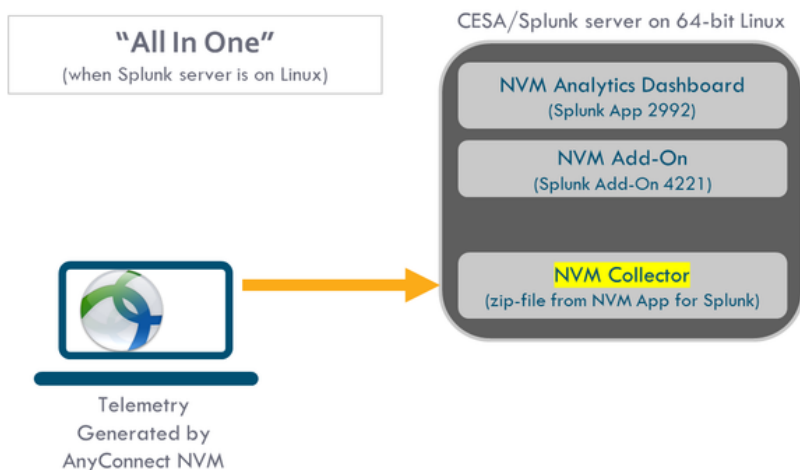
Folgende Komponenten bilden die Lösung:

- [Cisco AnyConnect Secure Mobility Client mit Network Visibility Module \(NVM\)-Aktivierung](#)
- [Cisco AnyConnect Network Visibility Module \(NVM\)-App für Splunk](#)
- [Cisco NVM-Technologie-Add-On für Splunk](#)
- NVM Collector (in einer ZIP-Datei mit dem NVM TA-Add-on gebündelt)

Bereitstellungsübersicht

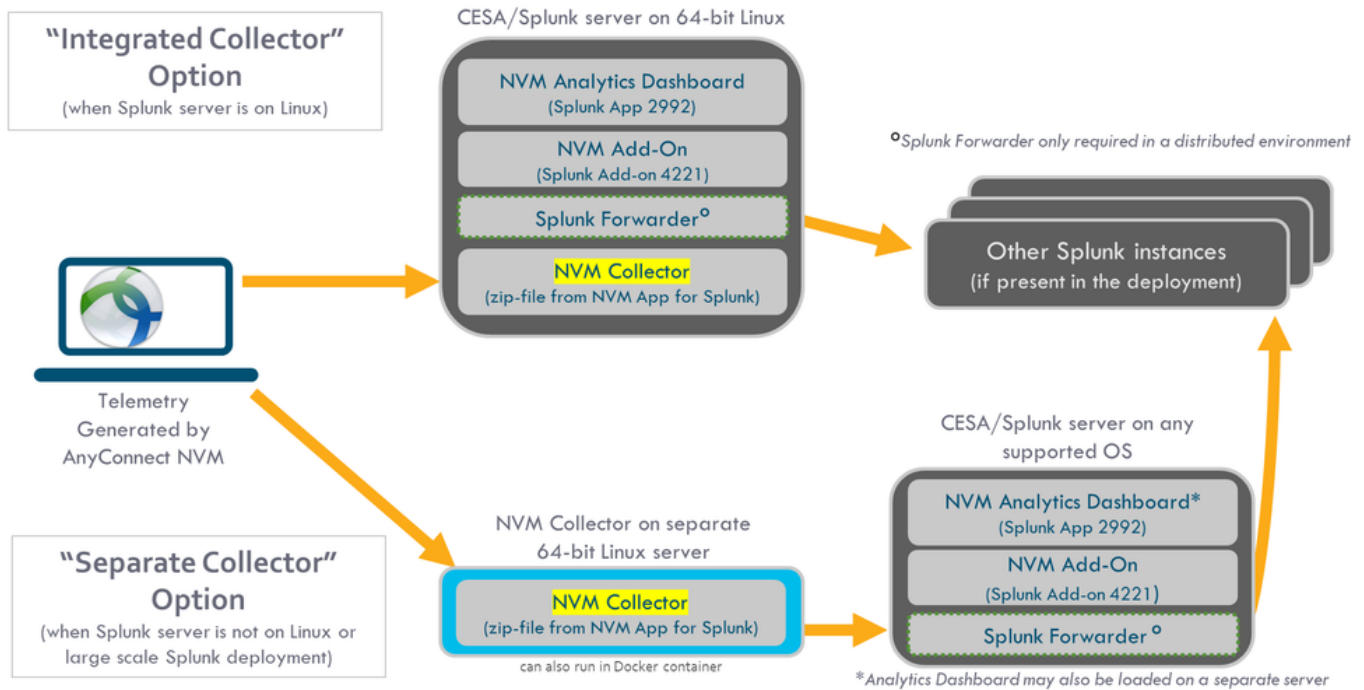
Dies ist ein allgemeiner Überblick über die Bereitstellung in ihrer einfachsten Form. Dies ist eine All-in-One-Konfiguration, die unter 64-Bit Linux ausgeführt wird.

Mit dieser Konfiguration werden die meisten Demonstrationen eingerichtet, und sie ist auch bei einer Bereitstellung in einer kleinen Produktionsumgebung hilfreich.



Dies ist ein umfassenderer Satz von Optionen, die für die Bereitstellung verfügbar sind. In der Regel ist eine Produktions-Konfiguration verteilt und verfügt über mehrere Splunk Enterprise-

Knoten.



Hintergrundinformationen

Das Cisco AnyConnect Network Visibility-Modul bietet eine kontinuierliche, hochwertige Telemetrie für Endgeräte. NVM ermöglicht es Unternehmen, das Verhalten von Endgeräten und Benutzern im Netzwerk anzuzeigen und Datenflüsse von Endgeräten sowohl am Standort als auch extern sowie wertvolle Kontexte wie Benutzer, Anwendungen, Geräte, Standorte und Ziele zu erfassen. Splunk Enterprise nutzt die Telemetriedaten und stellt Analysefunktionen und Berichte bereit.

Dieser technische Hinweis ist ein Konfigurationsbeispiel für AnyConnect NVM mit Splunk Enterprise als Teil der neuen [CESA-Lösung](#).

Cisco AnyConnect Secure Mobility Client - Mehr als VPN

Cisco AnyConnect ist ein einheitlicher Agent, der mehrere Sicherheitsservices zum Schutz des Unternehmens bereitstellt. AnyConnect wird in der Regel als VPN-Client für Unternehmen verwendet, unterstützt jedoch auch zusätzliche Module, die den unterschiedlichen Aspekten der Unternehmenssicherheit Rechnung tragen. Die zusätzlichen Module ermöglichen Sicherheitsfunktionen wie Statusüberprüfung, Web-Sicherheit, Malware-Schutz, Netzwerktransparenz und mehr.

In diesem technischen Hinweis geht es um das Network Visibility Module (NVM), das in Cisco AnyConnect integriert werden kann, um Administratoren die Überwachung der Anwendungsnutzung von Endgeräten zu ermöglichen.

Weitere Informationen zu Cisco AnyConnect finden Sie im [Administratorleitfaden zum Cisco AnyConnect Secure Mobility Client, Version 4.7](#).

Internet Protocol Flow Information Export (IPFIX)

IPFIX ist ein IETF-Protokoll, das einen Standard für den Export von IP-Flow-Informationen für verschiedene Zwecke wie Abrechnung, Audit und Sicherheit definiert. IPFIX basiert auf dem Cisco NetFlow-Protokoll v9, ist jedoch nicht direkt kompatibel. [Cisco nvzFlow](#) ist eine Protokollspezifikation, die auf dem IPFIX-Protokoll basiert. IPFIX ist ein erweiterbares Protokoll, das es ermöglicht, neue Parameter zur Informationsübermittlung zu definieren. Das Cisco nvzFlow-Protokoll erweitert den IPFIX-Standard und definiert neue Informationselemente sowie einen Standardsatz von IPFIX-Vorlagen, die als Teil der Telemetrie übertragen werden, die von AnyConnect NVM verwendet wird.

Weitere Informationen zu IPFIX finden Sie unter [RFC5101](#), [RFC7011](#), [RFC7012](#), [RFC7013](#), [RFC7014](#), [RFC7015](#).

IPFIX NVM-Collector

Weitere Informationen finden Sie unter <http://cs.co/nvm-collector>

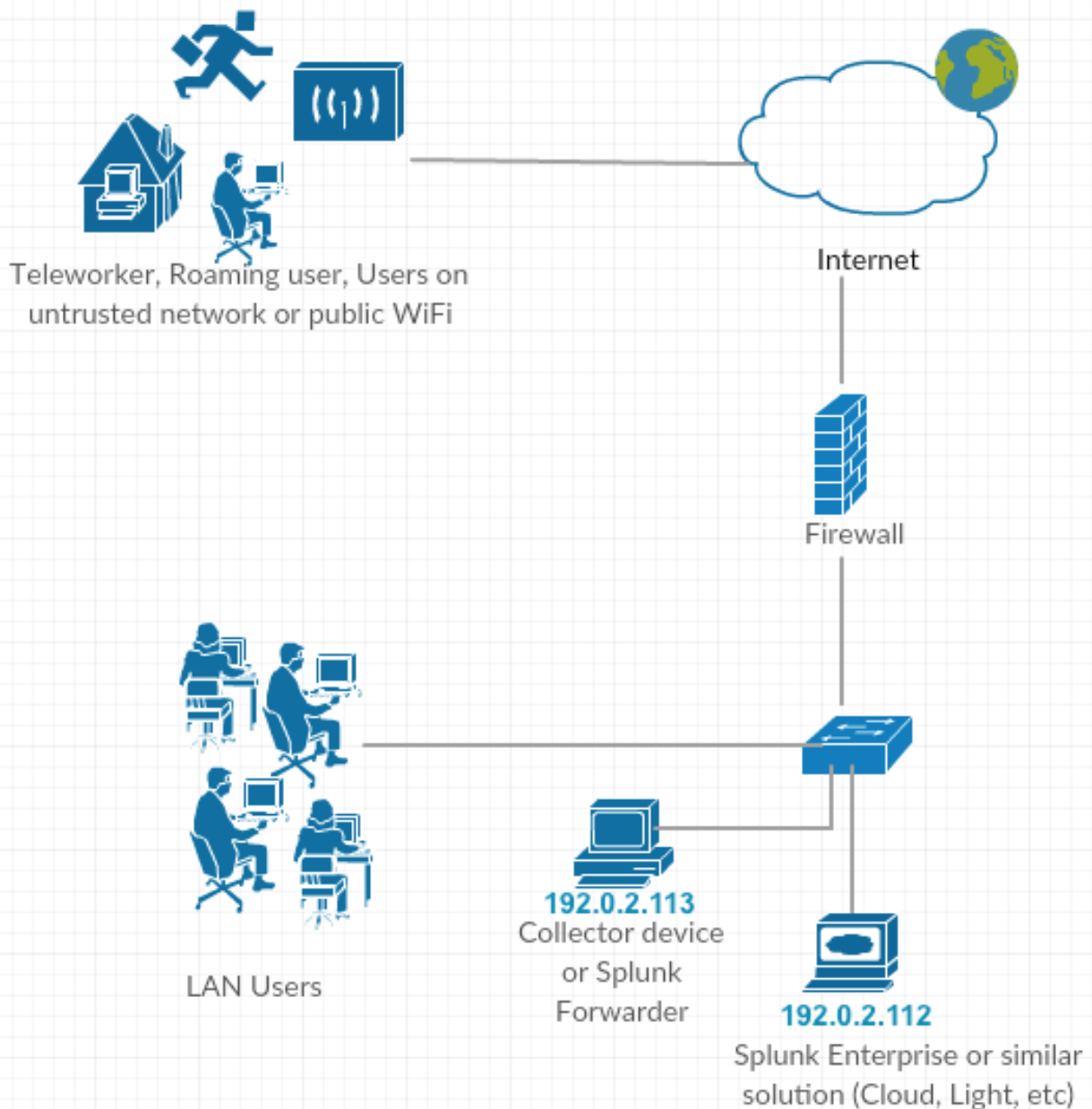
- Ein Collector ist ein Server, der IPFIX-Daten empfängt und speichert. Diese Daten können dann an Splunk weitergeleitet werden.
- Cisco stellt einen Collector bereit, der speziell für das nvzFlow-Protokoll entwickelt und mit der Splunk-App (NVM TA Add-On) gebündelt wurde.
- Der Collector kann mit dem Splunk-Server auf demselben Gerät (All-in-One) installiert werden. Auf dem Heavy Forwarder. Oder auf einer eigenständigen Linux-Box.

Splunk Enterprise

Splunk Enterprise ist ein leistungsstarkes Tool, das Diagnosedaten erfasst und analysiert, um aussagekräftige Informationen über die IT-Infrastruktur zu erhalten. Administratoren können an einem zentralen Punkt Daten sammeln, die für das Verständnis des Netzwerkzustands von entscheidender Bedeutung sind.

Splunk ist ein Partner von Cisco und die [CESA](#)-Lösung wurde in Zusammenarbeit mit diesen entwickelt.

Topologie



IP-Adresskonventionen in diesem technischen Hinweis:

Collector-IP-Adresse: 192.0.2.123

Splunk-IP-Adresse: 192.0.2.113

Konfigurieren

Dieser Abschnitt behandelt die Konfiguration von Cisco NVM-Komponenten.

Eine Übersicht zur Bereitstellung von AnyConnect NVM und Konfigurationsprofilen finden Sie auch unter [Implementieren des AnyConnect Network Visibility-Moduls](#).

DTLS-Unterstützung

NVM kann jetzt so konfiguriert werden, dass Daten sicher über DTLS an den Collector gesendet

werden. Dieser Modus kann im NVM Profile Editor konfiguriert werden. Wenn das Kontrollkästchen "Sicher" aktiviert ist, verwendet NVM DTLS als Transport. Damit die DTLS-Verbindung genutzt werden kann, muss das DTLS-Server-Zertifikat (Collector) vom Endpunkt als vertrauenswürdig anerkannt werden. Nicht vertrauenswürdige Zertifikate werden stillschweigend abgelehnt. DTLS 1.2 ist die minimale unterstützte Version. Der Collector als Teil der CESA Splunk-App v3.1.2+ ist für die DTLS-Unterstützung erforderlich. Der Collector funktioniert nur in einem Modus, entweder sicher oder unsicher.

Zertifikatanforderungen

- Das Collector-Zertifikat muss vom Client als vertrauenswürdig eingestuft werden (es muss sichergestellt werden, dass die Zertifikatkette vertrauenswürdig ist). Es gibt keine Konfiguration für AnyConnect.
- Das Zertifikat muss im PEM-Format vorliegen.
- Keine Unterstützung für Zertifikatsschlüsselkenwort (interne Zertifizierungsstelle der Cisco ISE erforderlich)
- Jedes Zertifikat kann auf dem Collector verwendet werden, solange dem Client-Computer Anyconnect vertraut (interne PKI, bekannte usw.).
- Nachdem die Konfigurationsdatei aktualisiert wurde, muss der AnyConnect NVM-Dienst neu gestartet werden (für Einzelclient-Tests). Bei Profilen, die von der ISE/ASA weitergeleitet werden, muss die Verbindung zum Netzwerk getrennt/erneut hergestellt werden.
- Die AC NVM Profile Collector-Konfiguration muss IP oder FQDN sein. Dies hängt davon ab, was in der CN des Zertifikats verwendet wird. FQDN wird bei Änderungen der IP-Adresse immer bevorzugt. Wenn Sie eine IP-Adresse verwenden, sollte das Collector-Zertifikat CN oder SAN über diese IP verfügen. Wenn das Zertifikat FQDN als CN enthält, sollte das NVM-Profil denselben FQDN wie ein Collector aufweisen.

AnyConnect-Konfiguration (4.9.3043 und höher) - siehe Collector-Info

Das NVM-Profil enthält ein neues Kontrollkästchen unter Collector IP/Port namens Secure.

AnyConnect Profile Editor - NVM Profile

File Help

NVM Profile

Profile: Untitled



Collector Configuration

IP Address/FQDN

Port

Secure 

Standalone AnyConnect NVM-Modul

Hierfür ist AnyConnect 4.8.01090 oder höher erforderlich - [AnyConnect-Administratorhandbuch für NVM](#)

Weitere Informationen finden Sie im eigenständigen Leitfaden [zur Implementierung des AnyConnect Network Visibility-Moduls](#).

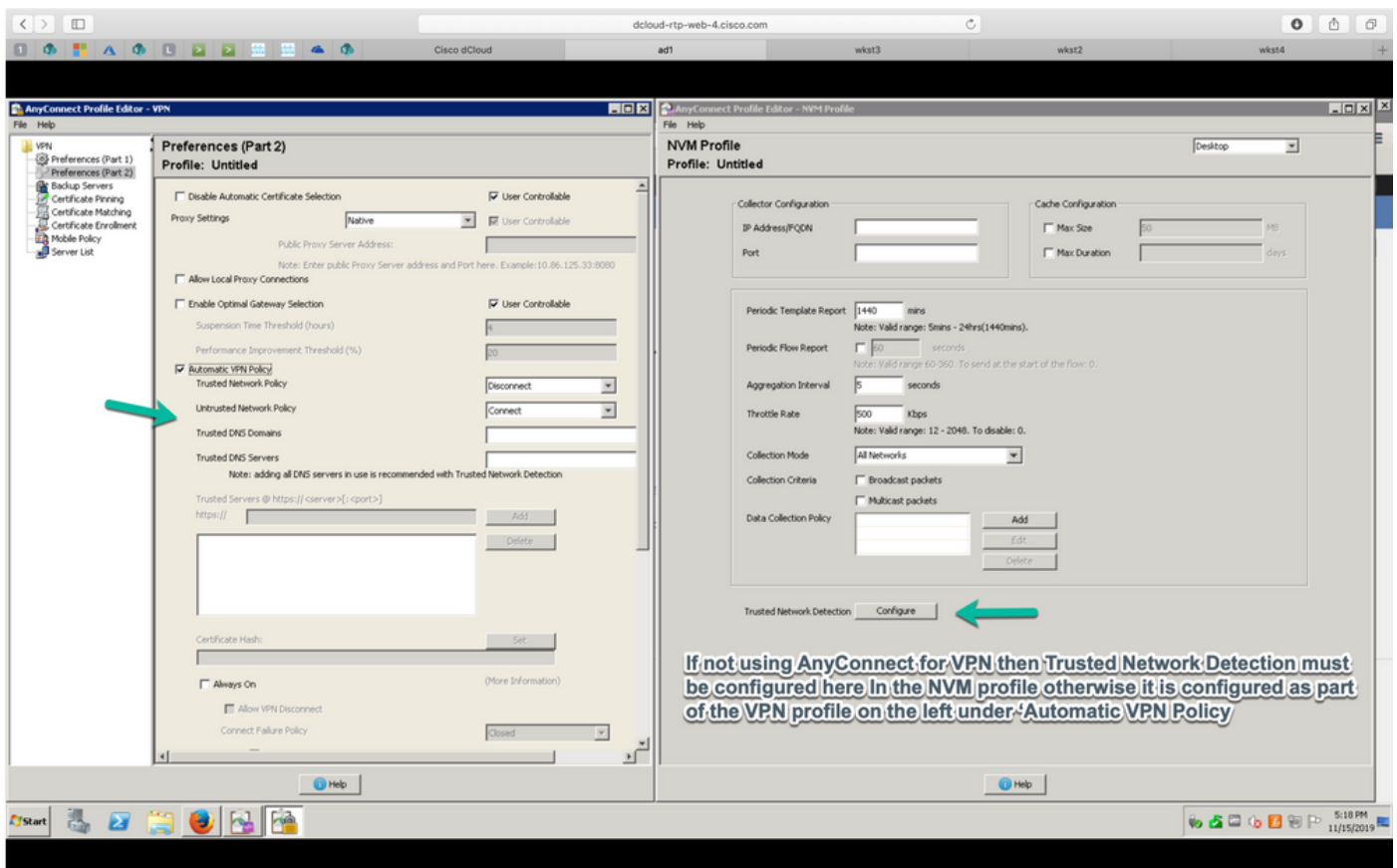
Wenn Sie keine AnyConnect-Bereitstellung haben oder eine andere VPN-Lösung verwenden, können Sie das NVM-Standalone-Paket für Ihre NVM-Anforderungen installieren. Dieses Paket arbeitet unabhängig, bietet jedoch dieselbe Ebene der Flow-Erfassung von einem Endpunkt wie die vorhandene AnyConnect NVM-Lösung. Wenn Sie die eigenständige NVM installieren, zeigen die aktiven Prozesse (z. B. die Aktivitätsüberwachung auf MacOS) die Verwendung an.

Eigenständige NVM wird mit dem [NVM Profile Editor](#) und die Konfiguration von Trusted Network Detection (TND) sind obligatorisch. Mithilfe der TND-Konfiguration ermittelt NVM, ob sich der Endpunkt im Unternehmensnetzwerk befindet, und wendet dann die entsprechenden Richtlinien an.

Fehlerbehebung und Protokollierung erfolgen weiterhin über AnyConnect DART, das über das AnyConnect-Paket installiert werden kann.

Vor der Standalone-Konfiguration musste das Core-VPN-Modul installiert sein, um Trusted Network Detection nutzen zu können. Dadurch sah der Benutzer auch die Core-VPN-Kachel in der Benutzeroberfläche, was die Endbenutzer verwirren könnte, insbesondere wenn sie die VPN-Lösung eines anderen Anbieters verwenden.

Wenn Sie das eigenständige Gerät verwenden, verwenden Sie nicht das Core-VPN-Profil, um TND zu konfigurieren. Das NVM-Profil kann jetzt direkt für TND konfiguriert werden.



AnyConnect NVM-Clientprofil

AnyConnect NVM-Konfiguration wird in einer XML-Datei gespeichert, die Informationen über die Collector-IP-Adresse und die Port-Nummer sowie weitere Informationen enthält. Die Collector-IP-

Adresse und eine Portnummer müssen im NVM-Clientprofil korrekt konfiguriert werden.

Damit das NVM-Modul ordnungsgemäß funktioniert, muss die XML-Datei in diesem Verzeichnis gespeichert werden:

- Für Windows 7 und höher: **%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM**
- Für Mac OSX: **/opt/cisco/anyconnect/nvm**

Wenn das Profil auf der Cisco ASA/Identity Services Engine (ISE) vorhanden ist, wird es zusammen mit der NVM-Bereitstellung von AnyConnect automatisch bereitgestellt.

XML-Profilbeispiel:

```
<?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>
```

Das NVM-Profil kann mit den folgenden Tools erstellt werden:

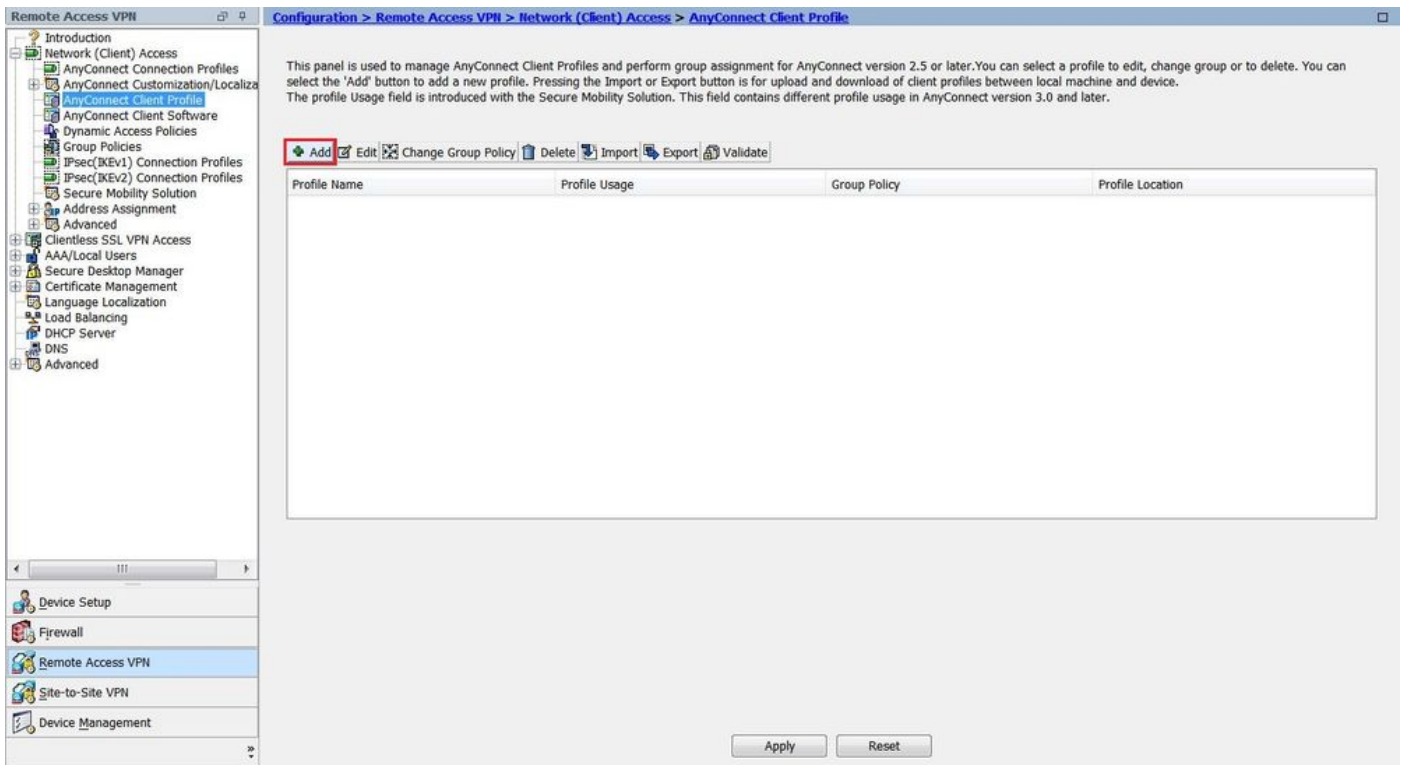
- Cisco ASDM
- AnyConnect-Profil-Editor
- Identity Services Engine

Konfigurieren des NVM-Clientprofils über ASDM

Diese Methode ist vorzuziehen, wenn AnyConnect NVM über Cisco ASA bereitgestellt wird.

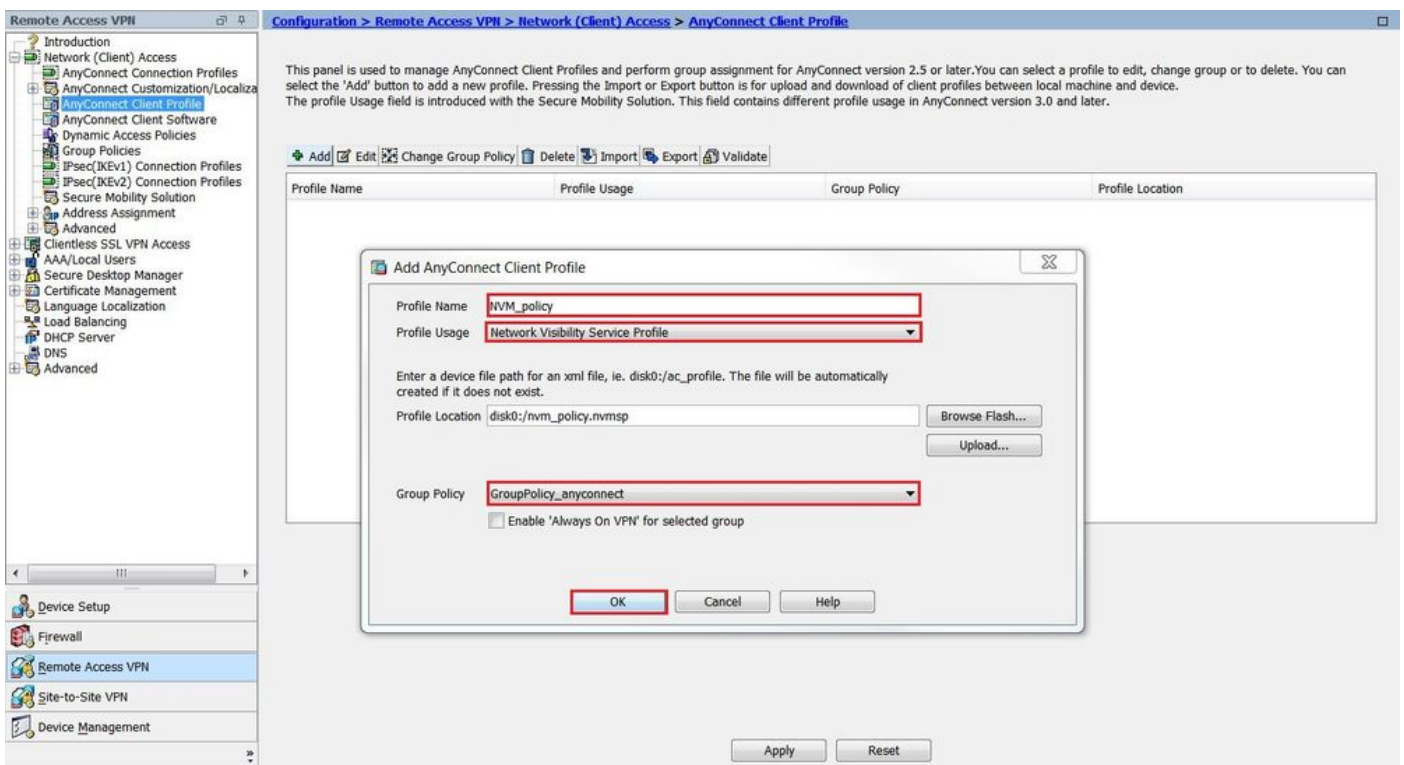
1. Navigieren Sie zu **Konfiguration > Access VPN entfernen > Network (Client) Access > AnyConnect Client Profile**.

2. Klicken Sie auf **Hinzufügen**, wie im Bild gezeigt.

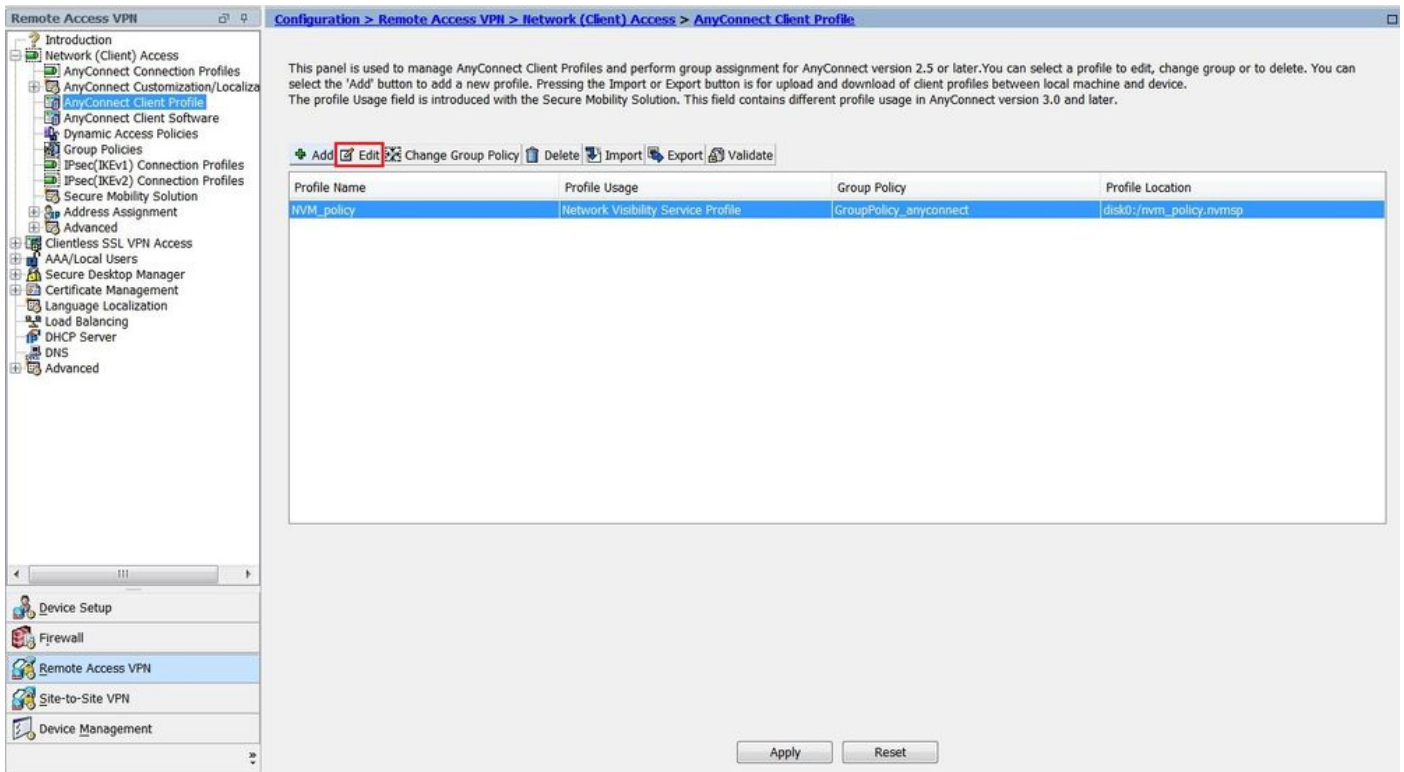


3. Geben Sie dem Profil einen Namen. Wählen Sie in **Profilverwendung** die Option **Network Visibility Service Profile**.

4. Weisen Sie sie der Gruppenrichtlinie zu, die von AnyConnect-Benutzern verwendet wird, und klicken Sie auf **OK**, wie im Bild gezeigt.

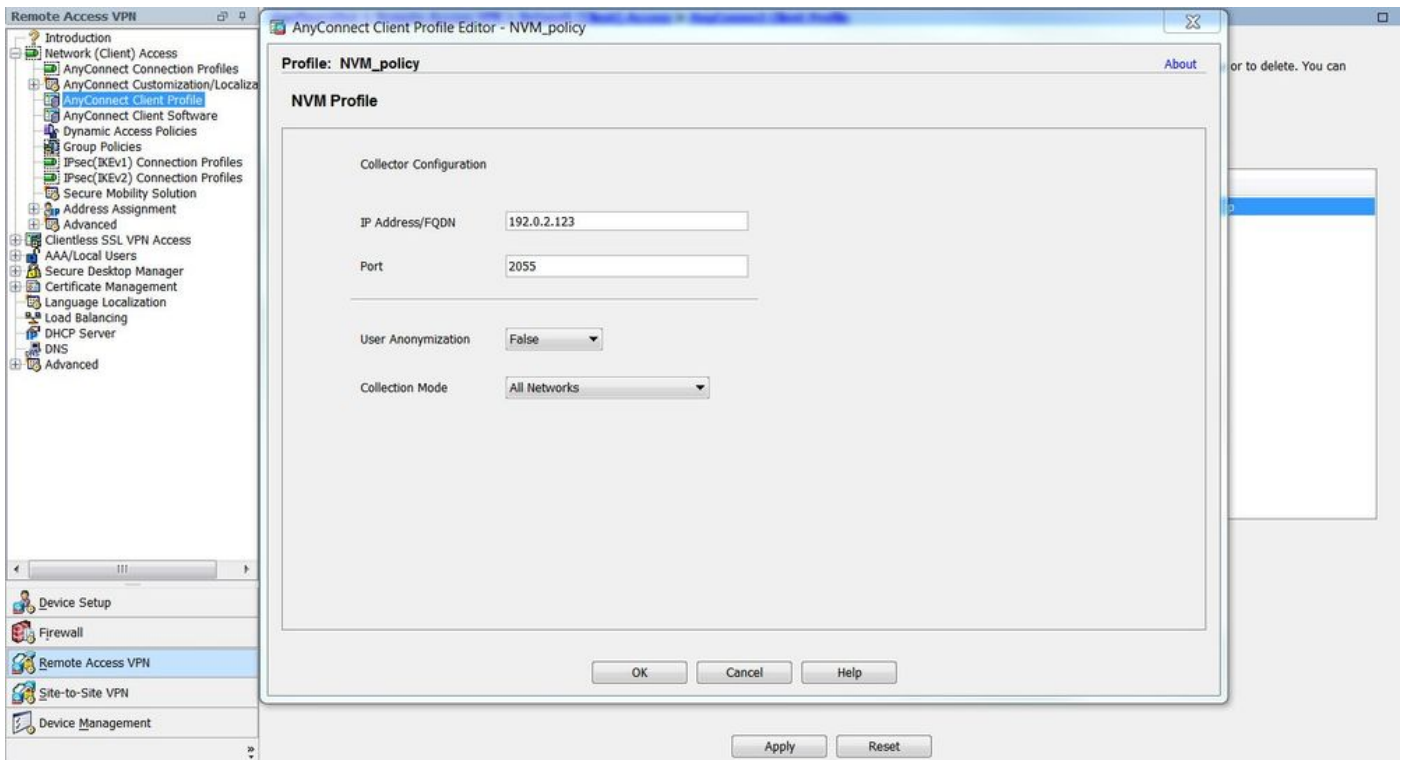


5. Die neue Richtlinie wird erstellt. Klicken Sie auf **Bearbeiten**, wie im Bild gezeigt.



6. Geben Sie die Informationen zur Collector IP-Adresse und Portnummer ein, und klicken Sie auf **OK**.

7. Klicken Sie nun auf **Apply**, wie im Bild gezeigt.



Konfigurieren des NVM-Clientprofils über den AnyConnect-Profil-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-

[00000061](#)

Dieses eigenständige Tool ist auf Cisco.com verfügbar. Diese Methode ist vorzuziehen, wenn AnyConnect NVM über die Cisco ISE bereitgestellt wird. Das mit diesem Tool erstellte NVM-Profil kann auf die Cisco ISE hochgeladen oder direkt auf Endpunkte kopiert werden.

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

Ausführliche Informationen zu AnyConnect Profile Editor finden Sie unter:

[Der AnyConnect Profile Editor](#)

Konfigurieren der Web-Bereitstellung auf der Cisco ASA

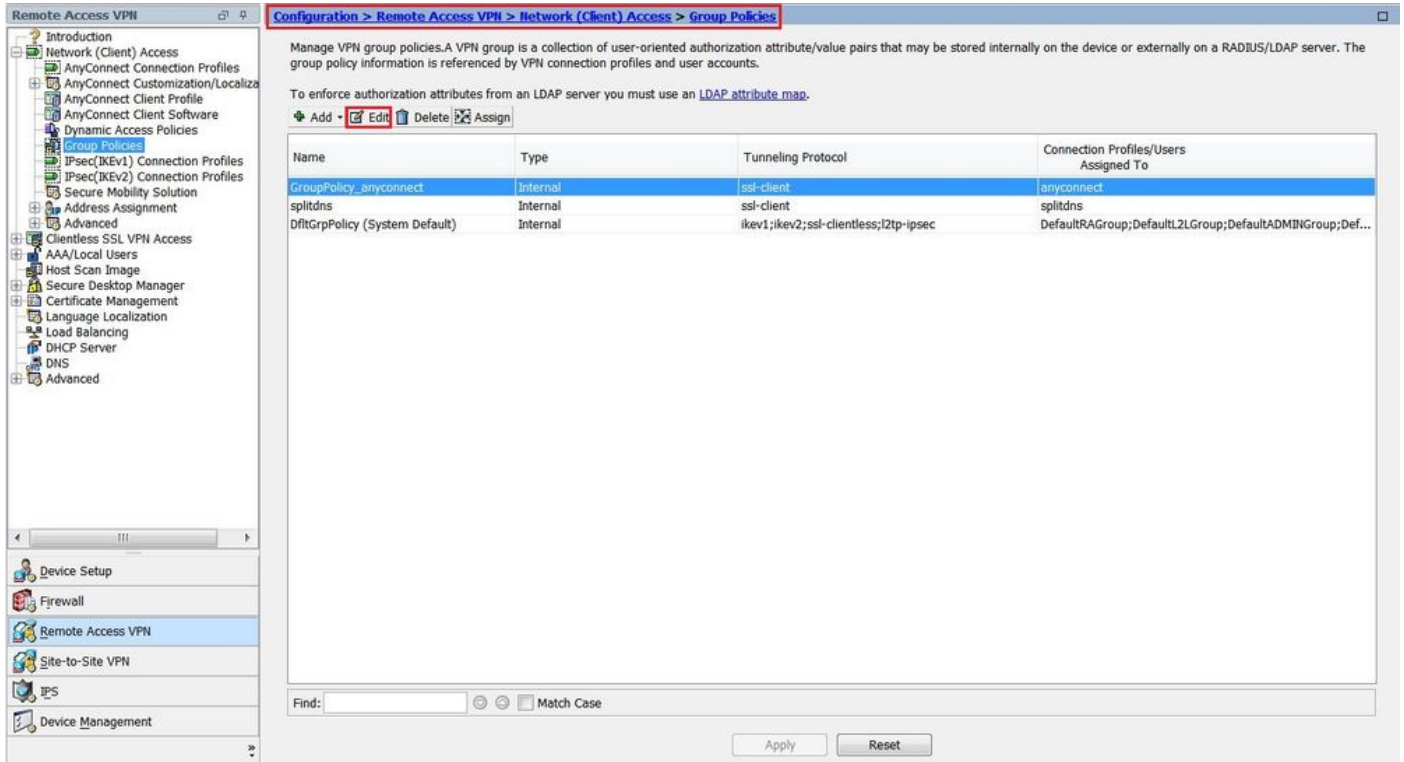
In diesem technischen Hinweis wird davon ausgegangen, dass AnyConnect bereits auf der ASA konfiguriert ist und nur die NVM-Modulkonfiguration hinzugefügt werden muss. Detaillierte Informationen zur ASA AnyConnect-Konfiguration finden Sie unter:

[ASDM-Buch 3: Cisco ASA VPN ASDM Configuration Guide, 7.5](#)

So aktivieren Sie das AnyConnect NVM-Modul auf der Cisco ASA:

1. Navigieren Sie zu **Configuration > Remote Access VPN > Network (Client) Access > Group Policies (Konfiguration > Remote Access VPN > Netzwerk-(Client-)Zugriff > Gruppenrichtlinien.**

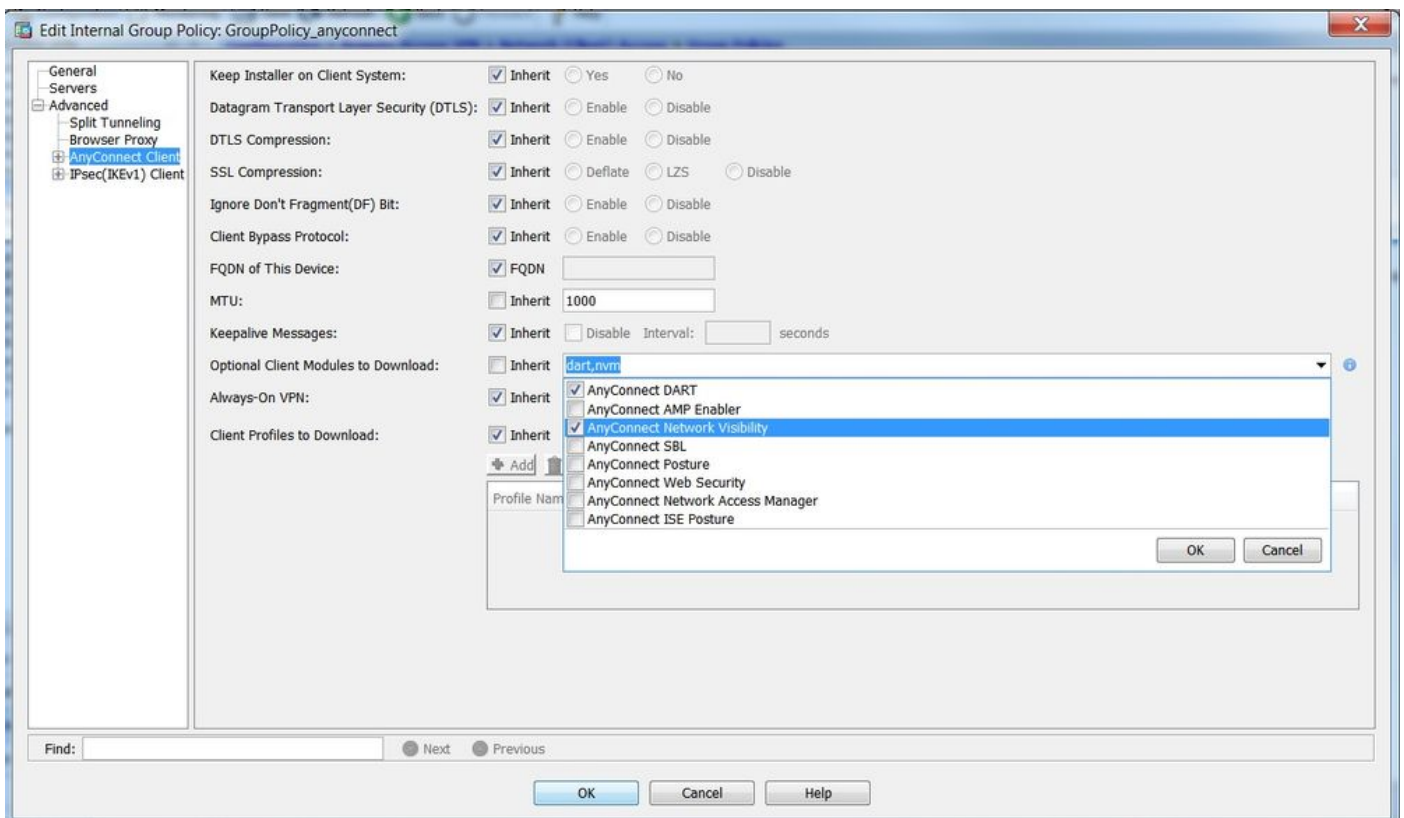
2. Wählen Sie die entsprechende Gruppenrichtlinie aus, und klicken Sie auf **Bearbeiten**, wie im Bild gezeigt.



3. Navigieren Sie im Gruppenrichtlinien-Popup zu **Erweitert > AnyConnect-Client**.

4. Erweitern Sie **Optional Client Modules (Optionale Client-Module)**, um sie herunterzuladen, und wählen Sie **AnyConnect Network Visibility** aus.

5. Klicken Sie auf **OK** und übernehmen Sie die Änderungen.



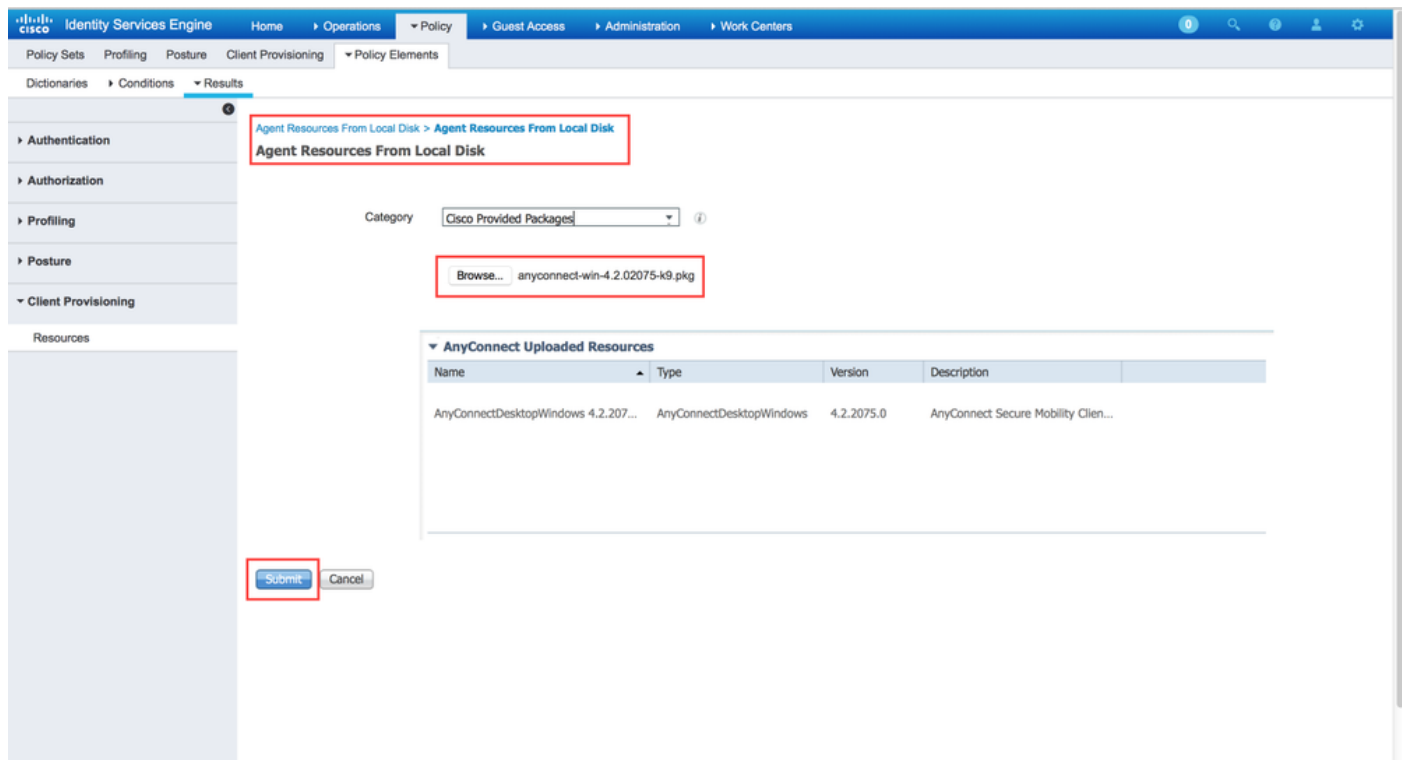
Konfigurieren der Web-Bereitstellung auf der Cisco ISE

So konfigurieren Sie die Cisco ISE für AnyConnect Web Deployment:

1. Navigieren Sie in der Cisco ISE-GUI zu **Richtlinien > Richtlinienelemente > Ergebnisse**.
2. Erweitern Sie **Client Provisioning**, um **Ressourcen** anzuzeigen, und wählen Sie **Ressourcen aus**.

AnyConnect-Image hinzufügen:

Schritt 1: Wählen Sie **Add > Agent Resources**, und laden Sie die AnyConnect-Paketdatei hoch.



The screenshot shows the Cisco Identity Services Engine (ISE) GUI. The navigation path is: Home > Operations > Policy > Guest Access > Administration > Work Centers > Policy Elements > Client Provisioning > Policy Elements > Results. The 'Agent Resources From Local Disk' section is highlighted with a red box. Below it, the 'Category' is set to 'Cisco Provided Packages'. The file 'anyconnect-win-4.2.02075-k9.pkg' is selected in the 'Browse...' field, also highlighted with a red box. Below this, the 'AnyConnect Uploaded Resources' table is visible, showing the uploaded package details:

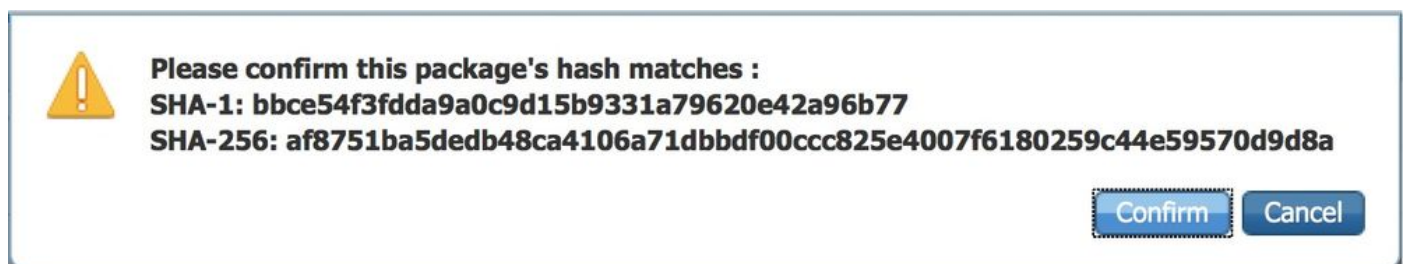
Name	Type	Version	Description
AnyConnectDesktopWindows 4.2.207...	AnyConnectDesktopWindows	4.2.2075.0	AnyConnect Secure Mobility Clien...

At the bottom, the 'Submit' button is highlighted with a red box.

Schritt 2: Bestätigen Sie den Hash des Pakets im Popup-Fenster.

Der Datei-Hash kann auf der Download-Seite von Cisco.com oder mit einem Drittanbieter-Tool verifiziert werden.

Dieser Schritt kann wiederholt werden, um mehrere AnyConnect-Bilder hinzuzufügen. (für Mac OSX und Linux OS)

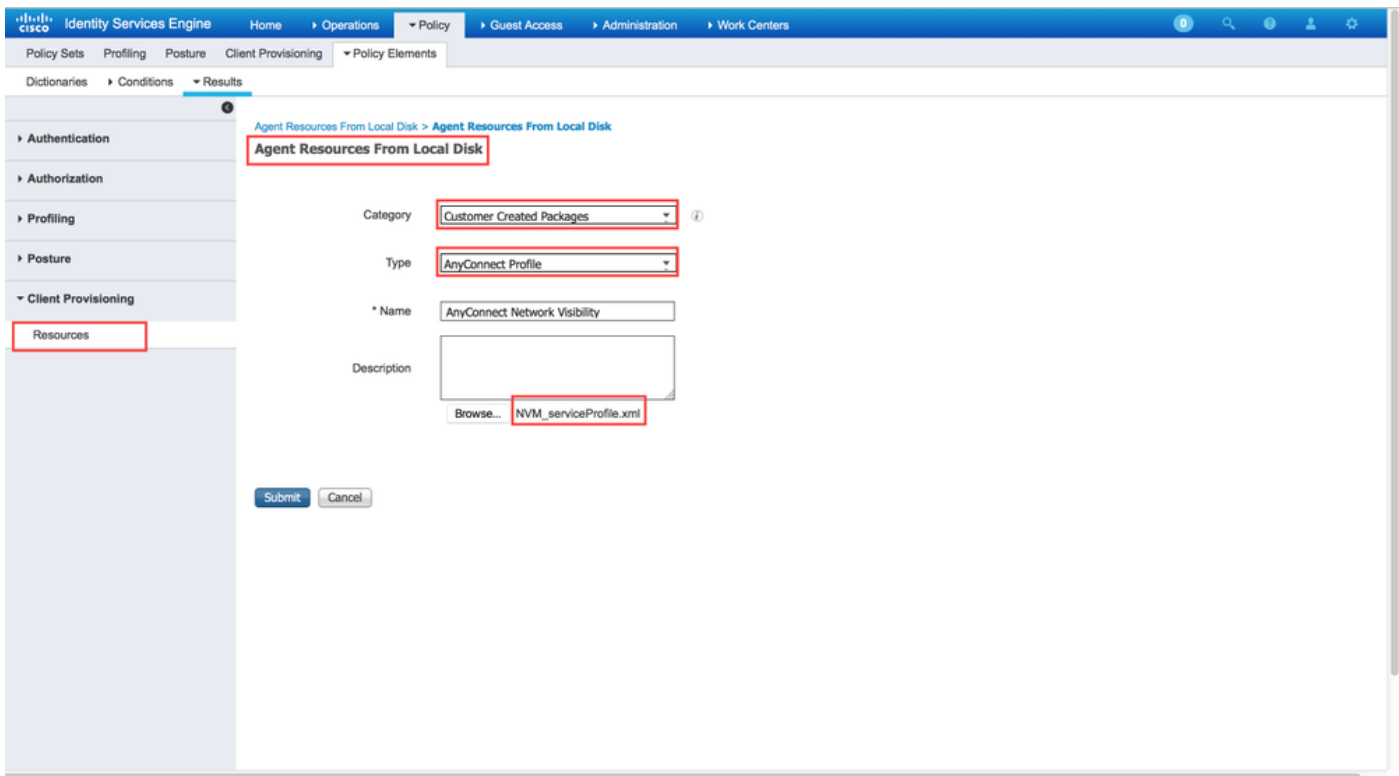


Please confirm this package's hash matches :
SHA-1: bbce54f3fdda9a0c9d15b9331a79620e42a96b77
SHA-256: af8751ba5dedb48ca4106a71dbbdf00ccc825e4007f6180259c44e59570d9d8a

Confirm **Cancel**

NVM-Profil für AnyConnect hinzufügen:

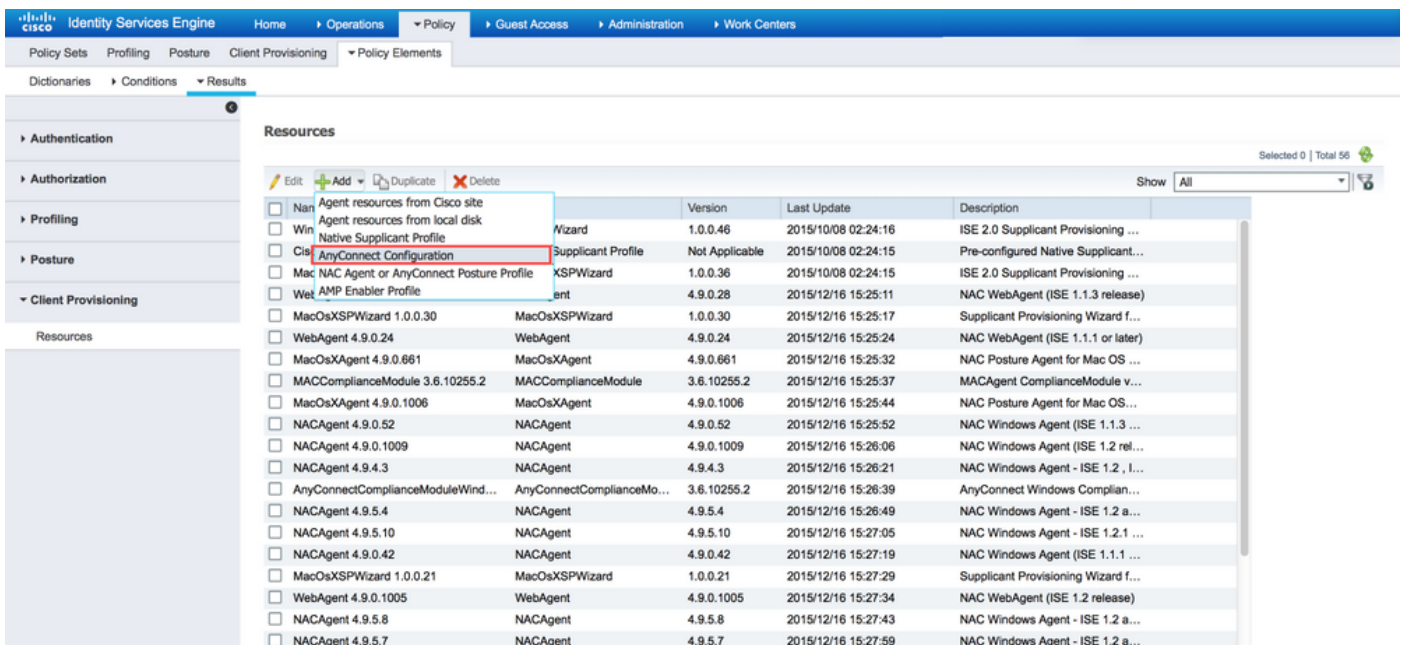
Schritt 1: Wählen Sie **Add > Agent Resources**, und laden Sie das NVM-Clientprofil hoch.



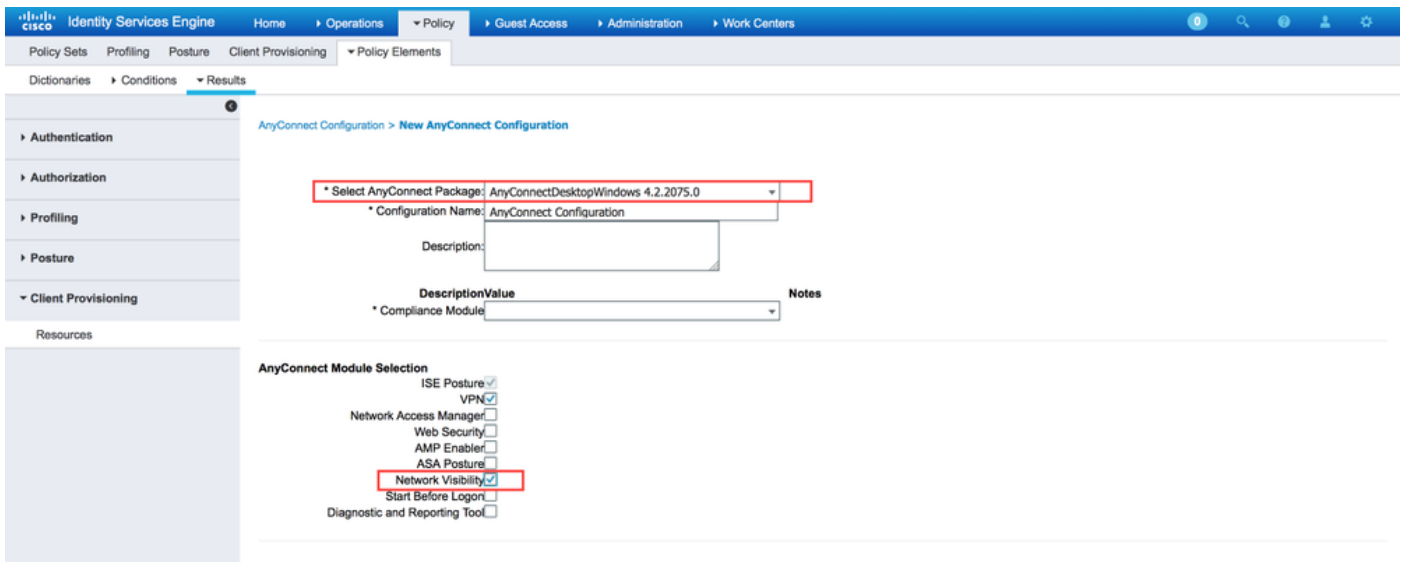
AnyConnect-Konfigurationsdatei hinzufügen:

Schritt 1: Klicken Sie auf **Hinzufügen**, und wählen Sie **AnyConnect-Konfiguration** aus.

Wählen Sie das im vorherigen Schritt hochgeladene Paket aus.



Schritt 2: Aktivieren Sie **NVM** in der **AnyConnect-Modulauswahl** zusammen mit der erforderlichen Richtlinie.



In diesem Abschnitt aktivieren wir AnyConnect Client-Module, Profile, Anpassungs-/Sprachpakete und die Opwat-Pakete.

Detaillierte Informationen zur Konfiguration der Web-Bereitstellung auf der Cisco ISE finden Sie unter:

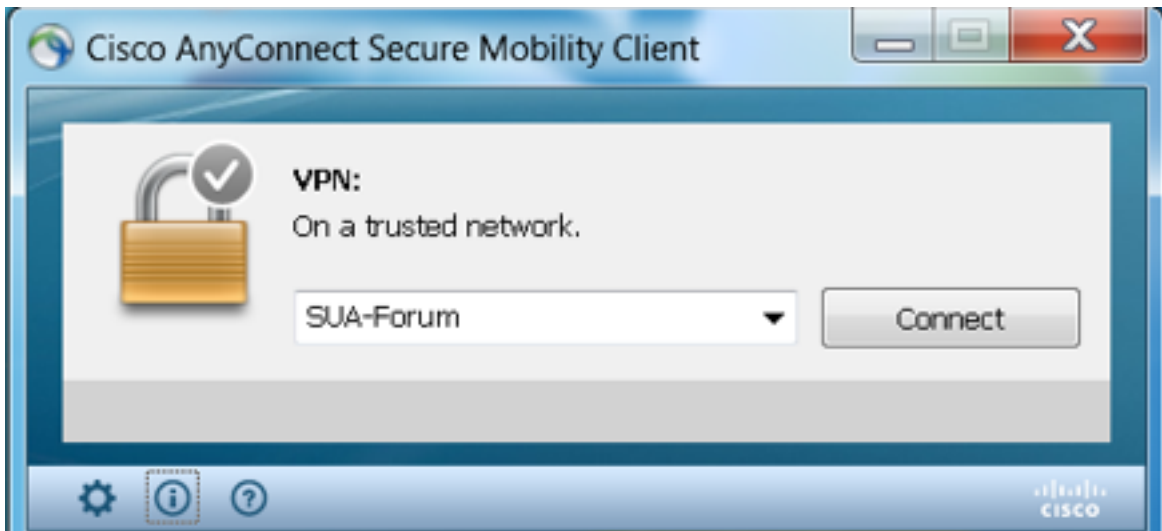
[Web-Bereitstellung von AnyConnect](#)

Erkennung vertrauenswürdiger Netzwerke

AnyConnect NVM sendet Flow-Informationen nur in einem vertrauenswürdigen Netzwerk. Mithilfe der TND-Funktion des AnyConnect-Clients wird ermittelt, ob sich das Endgerät in einem vertrauenswürdigen Netzwerk befindet.

Trusted Network Detection wird im für VPN verwendeten AnyConnect Client Profile (XML) konfiguriert, unabhängig davon, ob die VPN-Komponente in der Umgebung verwendet wird oder nicht. TND wird aktiviert, indem der Abschnitt "Automatic VPN Policy" (Automatische VPN-Richtlinie) im Profil konfiguriert wird. Mindestens eine vertrauenswürdige DNS-Domäne oder ein vertrauenswürdiger DNS-Server muss eingetragen werden. Für die von AnyConnect durchgeführten Aktionen, wenn der Client festgestellt hat, dass er sich in einem vertrauenswürdigen Netzwerk befindet, kann mithilfe des Pulldowns für die Richtlinie für vertrauenswürdige und nicht vertrauenswürdige Netzwerke der **DoNothing**-Modus festgelegt werden.

XML Profile (excerpt)	ASDM PROFILE EDITOR (excerpt)
<pre data-bbox="159 1713 778 1859"><AutomaticVPNPolicy>true <TrustedDNSDomains>demo.local</TrustedDNSDomains> <TrustedDNSServers>10.1.100.10</TrustedDNSServers> <TrustedNetworkPolicy>DoNothing</TrustedNetworkPolicy> <UntrustedNetworkPolicy>DoNothing</UntrustedNetworkPolicy> <AlwaysOn>false </AlwaysOn> </AutomaticVPNPolicy></pre>	



Weitere Informationen zur TND-Konfiguration finden Sie unter:
[Konfigurieren der Erkennung vertrauenswürdiger Netzwerke](#)

Bereitstellen

Die Bereitstellung der AnyConnect NVM-Lösung umfasst folgende Schritte:

1. Konfigurieren Sie AnyConnect NVM auf Cisco ASA/ISE.
2. Richten Sie die IPFIX Collector-Komponente ein (NVM Collector auf Linux - im TA-Add-On verpackt).
3. Richten Sie Splunk mit der Cisco NVM-App und dem TA Add-On ein.

Schritt 1: Konfigurieren von AnyConnect NVM auf Cisco ASA/ISE

Dieser Schritt wurde im Abschnitt Konfigurieren ausführlich behandelt.

Sobald NVM auf der Cisco ISE/ASA konfiguriert ist, kann sie automatisch auf Client-Endpunkten bereitgestellt werden.

Schritt 2: Einrichten der IPFIX Collector-Komponente (AnyConnect NVM Collector)

Die Collector-Komponente ist für die Erfassung und Übersetzung aller IPFIX-Daten von den Endpunkten und deren Weiterleitung an das [Splunk-Add-On](#) zuständig. Der NVM Collector wird unter 64-Bit Linux ausgeführt. Konfigurationsskripte für CentOS, Ubuntu und Docker sind im Lieferumfang enthalten. Die CentOS-Installationsskripte und -Konfigurationsdateien können auch in den Distributionen Fedora und Redhat verwendet werden.

In einer typischen verteilten Splunk Enterprise-Bereitstellung sollte der Collector entweder auf einem eigenständigen 64-Bit-Linux-System oder einem [Splunk Forwarder](#)-Knoten ausgeführt werden, der unter 64-Bit-Linux ausgeführt wird. Es kann auch auf einem eigenständigen Server ohne Splunk-Komponenten installiert werden.

Anmerkung: Die Lösung kann auch auf einem einzigen 64-Bit-Linux-System ausgeführt werden, das die NVM Collector- und Splunk Enterprise-Komponenten enthält, um sie in

einer kleinen Bereitstellung oder zu Demonstrationszwecken einzusetzen. Das All-in-One-Gerät ist für bis zu 10.000 Endgeräte am einfachsten - siehe [CESA POV-Bedarfsbestimmungsinformationen](#).

Wie wird der Collector installiert?

1. Kopieren Sie die Datei **acnvmcollector.zip** im Verzeichnis **/opt/splunk/etc/apps/\$APP_DIR\$/appserver/addon/** (im Lieferumfang des TA Add-On enthalten) in das System, auf dem Sie die Installation planen.
2. Extrahieren Sie die Dateien (entpacken **acnvmcollection.zip**)

Es wird empfohlen, die Datei **\$PLATFORM\$_README** im **.zip**-Paket zu lesen, bevor das Skript **install.sh** ausgeführt wird. Die Datei **\$PLATFORM\$_README** enthält Informationen zu den relevanten Konfigurationseinstellungen, die vor der Ausführung des **install.sh**-Skripts überprüft und ggf. geändert werden müssen. Sie müssen mindestens die Adresse der Splunk-Instanz konfigurieren, an die Sie Daten weiterleiten. Wenn das System nicht richtig konfiguriert wird, kann dies dazu führen, dass der Collector nicht ordnungsgemäß arbeitet.

Anmerkung: Stellen Sie sicher, dass Netzwerk- und Host-Firewalls ordnungsgemäß konfiguriert sind, um den UDP-Datenverkehr für die Quell- und Zieladressen und -Ports zuzulassen. Der IPFIX-Datenverkehr (cflow), der von den anyconnect-Clients zum Collector eingeht, und die ausgehenden UDP-Daten zu Splunk (hier).

Eine einzelne NVM-Collector-Instanz kann mindestens 5.000 Flows pro Sekunde auf einem entsprechend großen System verarbeiten. oder bis zu 35.000-40.000 Endpunkte. Der Collector muss konfiguriert und ausgeführt werden, bevor Splunk NVM und TA-Add on App verwendet werden können.

Standardmäßig empfängt der Collector Flows von AnyConnect NVM-Endpunkten auf dem UDP-Port 2055.

Darüber hinaus erstellt der Collector drei Datenfeeds für Splunk, Per Flow Data, Endpoint Identity Data und Endpoint Interface Data für die UDP-Ports 20519, 20520 bzw. 20521.

Die Empfangs- und Datenfeed-Ports können geändert werden, indem die Datei **acnvm.conf** geändert und die Collector-Instanz neu gestartet wird. Stellen Sie sicher, dass alle Host-/Netzwerk-Firewalls zwischen Endpunkten und dem Collector oder zwischen dem Collector und den Splunk-Systemen für die konfigurierten UDP-Ports und -Adressen offen sind. Stellen Sie außerdem sicher, dass Ihre AnyConnect NVM-Konfiguration mit Ihrer Collector-Konfiguration übereinstimmt.

Wenn alle Komponenten installiert und ausgeführt sind, finden Sie im Abschnitt Hilfedateien innerhalb der Splunk-Anwendung detaillierte Informationen zu den vorkonfigurierten Berichten, Datenmodellen und Informationselementen, die von der Projektmappe erstellt werden.

Sie können einen Ihrer AnyConnect-Endpunkte neu starten und überprüfen, ob Daten an die Lösung gesendet werden. Führen Sie einen stetigen Datenstrom mit youtube aus.

Die Informationen müssen in der Konfigurationsdatei konfiguriert werden - acnvm.conf.

- syslog_server_ip (Forwarder- oder Splunk-Instanz) kann auf 127.0.0.1 verweisen (LOCALHOST darf nicht verwendet werden), wenn es sich im selben Gerät befindet
- Der Listening-Port für den Collector (eingehende IPFIX-Daten) ist standardmäßig ok.

HINWEIS: netflow_collector_ip wird in der Konfigurationsdatei nicht berücksichtigt (sie verwendet die öffentliche Standardschnittstelle), sollte sie nur so geändert werden, dass sie mit einer bestimmten lokalen IP überschrieben wird.

Pro Datenfluss-Port, Endpunkt-Identitätsdatenport, Endpunkt-Schnittstellendaten und Collector-Port sind in der Konfigurationsdatei auf Standardeinstellungen vorkonfiguriert. Stellen Sie sicher, dass diese Werte geändert werden, wenn nicht standardmäßige Ports verwendet werden.

Diese Informationen werden der Konfigurationsdatei hinzugefügt: **/opt/acnvm.conf**

DTLS-Unterstützung

(Weitere Informationen finden Sie unter Anyconnect NVM DTLS Information.)

Dies erfolgt auf der Box, die den Collector hostet.

- Machen Sie Verzeichnis **/opt/acnvm/certs**.
- Um das Zertifikat auf den Collector anzuwenden, speichern Sie es zusammen mit dem Schlüssel im Verzeichnis **/opt/acnvm/certs**.
- Ändern Sie den Besitzer und die Gruppe des Ordners in **acnvm:acnvm** mit dem folgenden Befehl: **sudo chown -R acnvm:acnvm certs/**:
- Dieser Abschnitt für **acnvm.conf** muss mit "cert" und "key" konfiguriert werden.
- Nachdem die Konfiguration und das Zertifikat platziert wurden, starten Sie den Collector neu - **sudo systemctl restart acnvm.service**
- Erfassungsstatus überprüfen - **sudo systemctl status acnvm.service**

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

Der Rest ist die Konfiguration.

```
"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. Ausführen des install.sh-Skripts mit Superuser-Berechtigungen (sudo ./install.sh)

Anmerkung: Das Konto benötigt sudo-Berechtigungen oder root, um das install.sh-Konto und die Berechtigungen für das acnvm-Dienstkonto auszuführen.

Weitere Informationen finden Sie unter <https://splunkbase.splunk.com/app/2992/#/details>

Schritt 3: Richten Sie Splunk mit der Cisco NVM-App (CESA-Dashboard) und dem TA-Add-On für Splunk ein.

Die Cisco AnyConnect NVM-App für Splunk ist auf SplunkBase verfügbar. Diese App unterstützt vordefinierte Berichte und Dashboards bei der Verwendung von IPFIX-Daten (nvzFlow) von

Endpunkten in nutzbaren Berichten und der Korrelation von Benutzer- und Endpunktverhalten.

Anmerkung: Bei Cloud-Bereitstellungen werden beide Apps in der Cloud-Instanz installiert. Nur der TA wird vor Ort installiert (mit dem Forwarder). Der Collector wird vor Ort mit dem Forwarder oder auf einer separaten Linux/Docker-Box installiert.

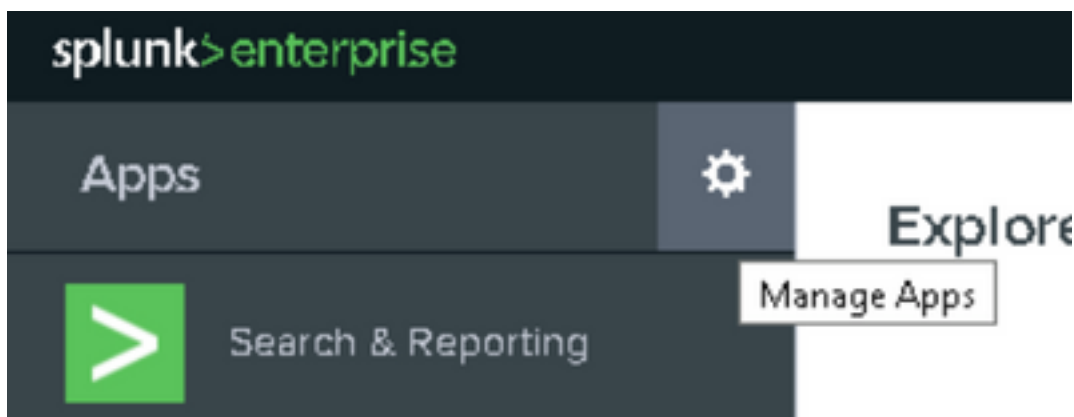
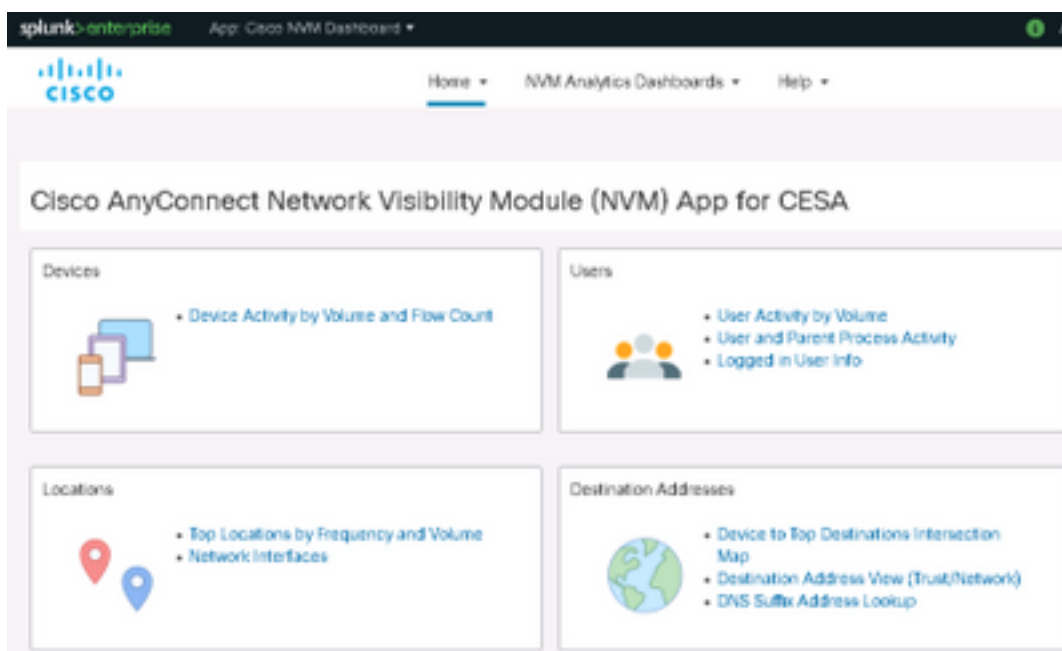
Für die Installation am Standort können nur alle Komponenten und Anwendungen auf einem Gerät (oder separat) installiert werden. Siehe Diagramme

Laden Sie diese Dateien herunter:

- Cisco NVM-App für Splunk auf Splunkbase: <https://splunkbase.splunk.com/app/2992/>
- Cisco NVM-Add-On für Splunk auf SplunkBase: <https://splunkbase.splunk.com/app/4221/>

Installieren

Schritt 1: Navigieren Sie zu **Splunk > Apps**, klicken Sie auf das Gerät, und installieren Sie die **tar.gz**-Datei, die Sie aus der Splunkbase heruntergeladen haben, oder suchen Sie im Apps-Abschnitt.



Schritt 2: Als Nächstes müssen Sie das **Add-On** mit demselben Prozess installieren. Vergewissern Sie sich, dass beide installiert sind, indem Sie die Seite **Splunk-Apps** anzeigen:

splunk>enterprise Apps Admin

Apps

Showing 1-2 of 2 items

Name	Folder name	Version	Update checking	Visible	Sharing	Status
Cisco NVM Dashboard	CiscoNVM	3.1.0	Yes	Yes	App Permissions	Enabled Disable
Cisco NVM Add-on for Splunk	TA-Cisco-NVM	3.0.9	Yes	No	App Permissions	Enabled Disable

Die Standardkonfiguration empfängt drei Datenfeeds für Splunk, Pro Flow Data, Endpoint Identity Data und Endpoint Interface Data auf den UDP-Ports 20519, 20520 bzw. 20521. (siehe Schritt 2)

Das Add-On ordnet diese dann Splunk-Quelletypen zu. `cisco:nvm:flowdata`, `cisco:nvm:sysdata` und `cisco:nvm:ifdata`.

Aktivieren von UDP-Eingaben mithilfe der Splunk-Verwaltungs-Benutzeroberfläche

Anmerkung: Sie können dies auch mit einer `input.conf`-Datei tun. Dies wird in der Cisco NVM Dashboard-App-GUI im Hilfe-Pulldown-Menü erläutert.

Sie müssen Splunk-Software nicht neu starten.

Navigieren Sie zu **Splunk > Settings > Data Input > UDP**, wie im Bild gezeigt.

1. Klicken Sie auf Neues lokales UDP > Port-Nummer fehlt > Klicken Sie auf Weiter > Wählen Sie den korrespondierenden Quelltyp aus > Klicken Sie auf **Prüfen** > Klicken Sie auf Senden.

2. Wiederholen Sie die Schritte für die anderen 2 Ports (versuchen Sie, Klon zu verwenden).

Add Data

Select Source
 Input Settings
 Review
 Done

[< Back](#) [Submit >](#)

Review

Input Type UDP Port
 Port Number 20519
 Source name override N/A
 Restrict to Host N/A
 Source Type cisco:nvm:flowdata
 App Context search
 Host (IP address of the remote server)
 Index default

UDP

Data inputs » UDP

New

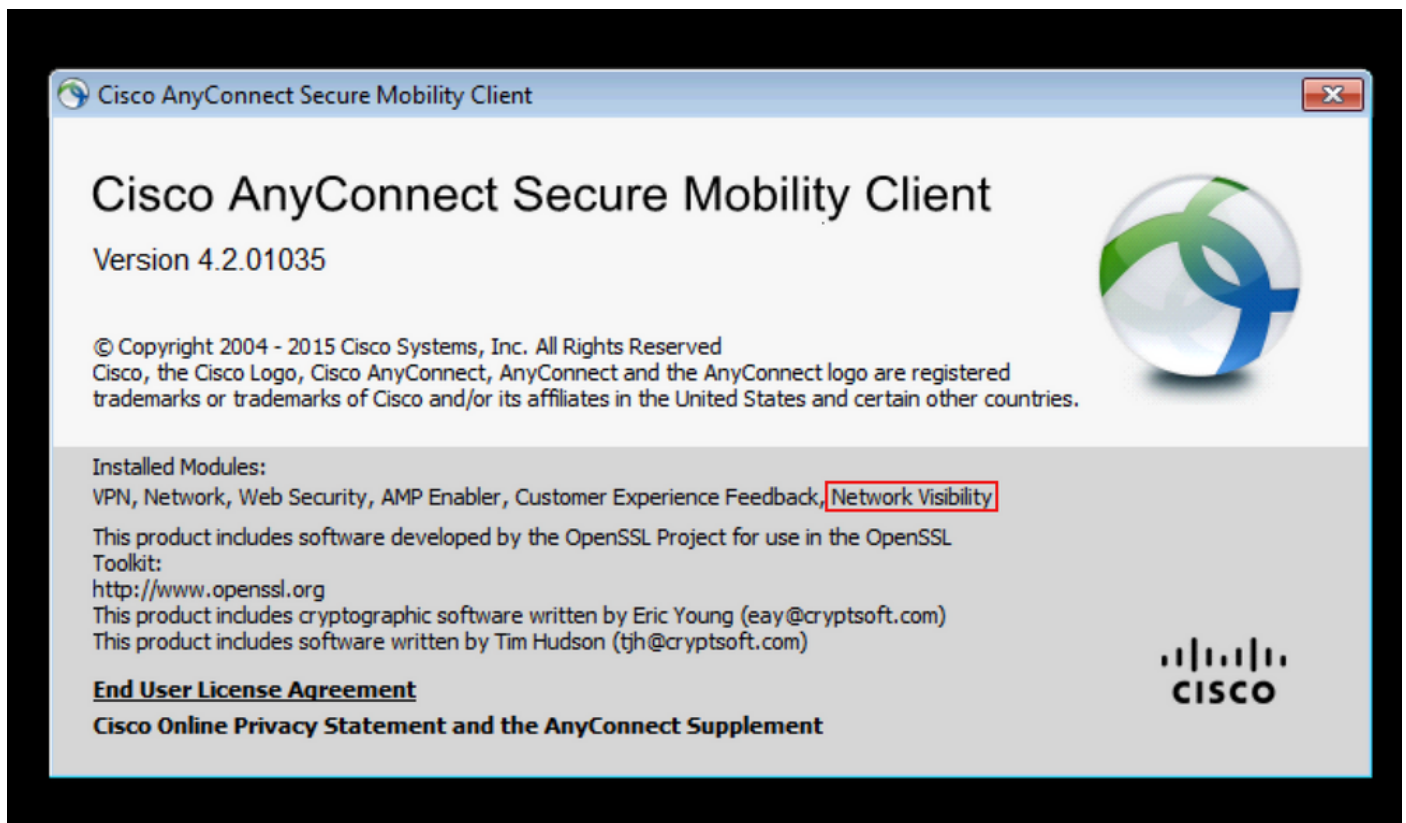
Showing 1-3 of 3 items

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

Überprüfung

Überprüfen der NVM-Installation von AnyConnect

Nach erfolgreicher Installation sollte das Network Visibility-Modul unter **Installierte Module** im Abschnitt **"Informationen"** des AnyConnect Secure Mobility Client aufgeführt werden.



Überprüfen Sie außerdem, ob der nvm-Dienst auf dem Endpunkt ausgeführt wird und sich das Profil im erforderlichen Verzeichnis befindet.

Collector-Status als "Ausführen" validieren

Stellen Sie sicher, dass der Collector-Status ausgeführt wird. Dadurch wird sichergestellt, dass der

Collector IPFIX/cflow von den Endpunkten immer empfängt. Wenn sie nicht ausgeführt wird, stellen Sie sicher, dass die ACNVM-Kontoberechtigungen für die Datei die Ausführung zulassen:
`/opt/acnvm/bin/acnvmcollector`

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

```
* acnvmcollector is running
```

```
root@ubuntu-splunkcollector:~$
```

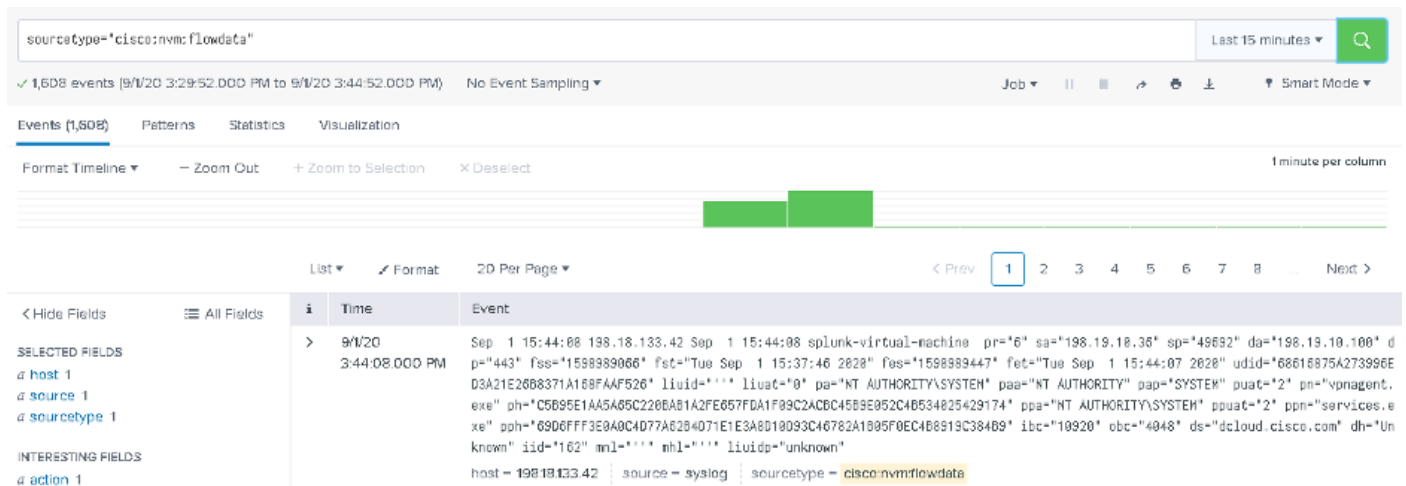
```
[splunk@splunk-virtual-machine addon]$ systemctl status acnvm.service
● acnvm.service - AC NVM Service
   Loaded: loaded (/usr/lib/systemd/system/acnvm.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2020-06-19 13:48:08 EDT; 25s ago
   Main PID: 41165 (acnvmcollector)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

Splunk validieren - AnyConnect NVM CESA Dashboard

Stellen Sie sicher, dass Splunk und die zugehörigen Services ausgeführt werden. Dokumentation zur Fehlerbehebung für Splunk finden Sie auf deren Website.

Die Dashboards für CESA werden erst fünf Minuten nach dem Empfang der ersten Daten aufgrund eines Automatisierungsskripts aktualisiert. Führen Sie eine manuelle Suche aus, um sofort zu validieren:

Klicken Sie im Haupt-Dashboard auf "Suchen und Berichten". Legen Sie im nächsten Bildschirm den korrekten Bereich fest, um die gewünschten Daten einzutragen. Geben Sie dort "Suchbegriff hier eingeben.." ein. Geben Sie "sourcetype=cisco:nvm:flowdata" ein.



Überprüfen Sie das Splunk-Dashboard, um sicherzustellen, dass Sie zu Splunk wechseln, auf **Cisco NVM Dashboard** klicken, auf **Device Activity by Volume and Flow Count** klicken, wenn Sie die aktuellen Einstellungen beibehalten möchten, und klicken Sie auf **Submit (Senden)**. Es zeigt Daten in den Grafiken an.

Paketfluss

1. IPFIX-Pakete werden auf Client-Endpunkten vom AnyConnect NVM-Modul generiert.

2. Die Client-Endpunkte leiten IPFIX-Pakete an die Collector-IP-Adresse weiter.
3. Der Collector erfasst die Informationen und leitet sie an Splunk weiter.
4. Collector sendet Datenverkehr an Splunk in drei verschiedenen Streams: Pro Datenfluss, Endpunktdaten und Schnittstellendaten.

Der gesamte Datenverkehr ist UDP, da der Datenverkehr nicht bestätigt wird.

Standard-Port für Datenverkehr:

IPFIX-Daten 2055

Pro Datenfluss 20519

Endgerätedaten 20520

Schnittstellendaten 20521

Das NVM-Modul speichert IPFIX-Daten und sendet diese an einen Collector, wenn es sich in einem vertrauenswürdigen Netzwerk befindet. Dies kann entweder der Fall sein, wenn der Laptop mit dem Unternehmensnetzwerk verbunden ist (am Standort), oder wenn er über VPN verbunden ist.

Sie können überprüfen, ob der Collector Pakete vom NVM-Modul empfängt, indem Sie eine Paketerfassung auf bestimmten UDP-Ports gemäß Ihrer Konfiguration ausführen, um zu überprüfen, ob die Pakete empfangen werden. Dies erfolgt über das Splunk-System-Linux-Betriebssystem.

Flussvorlagen

IPFIX-Flussvorlagen werden zu Beginn der IPFIX-Kommunikation an den Collector gesendet. Diese Vorlagen helfen dem Collector, die IPFIX-Daten sinnvoll zu nutzen.

Der Collector lädt außerdem Vorlagen vorab, um sicherzustellen, dass die Daten auch dann analysiert werden können, wenn der Client sie nicht gesendet hat. Wenn eine neuere Version des Clients mit Protokolländerungen freigegeben wird, werden die vom Client gesendeten neuen Vorlagen verwendet.

Unter den folgenden Bedingungen wird eine Vorlage gesendet:

1. Das NVM-Clientprofil ändert sich.
2. Es tritt ein Netzwerkänderungsereignis auf.
3. Der Dienst "nvmagent" wird neu gestartet.
4. Der Endpunkt wird neu gestartet/neu gestartet.
5. Periodisch (Standard = 24 Stunden), wie im NVM-Profil konfiguriert.

In seltenen Fällen kann eine Vorlage nicht gefunden werden. Dies kann durch einen Neustart eines der Endpunkte auf einfache Weise behoben werden.

Das Problem kann identifiziert werden, indem **keine Vorlage** in einer Paketerfassung des Endpunkts beobachtet wird, oder **keine Vorlagen für den Flow** in den Collector-Protokollen.

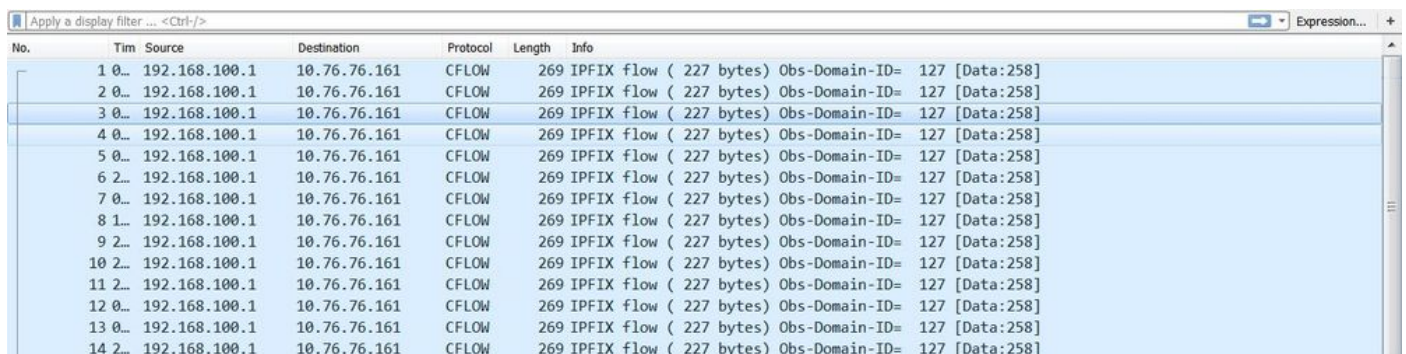
Fehlerbehebung

Dies sind die grundlegenden Schritte zur Fehlerbehebung:

1. Stellen Sie die Netzwerkverbindung zwischen Client-Endgerät und Collector sicher.
2. Stellen Sie die Netzwerkverbindung zwischen Collector und Splunk sicher.
3. Stellen Sie sicher, dass NVM korrekt auf dem Client-Endpunkt installiert ist.
4. Übernehmen Sie auf dem Endpunkt eine Erfassung, um festzustellen, ob IPFIX-Datenverkehr generiert wird.
5. Übernehmen Sie die Erfassung eines Collectors, um festzustellen, ob er IPFIX-Datenverkehr empfängt und Datenverkehr an Splunk weiterleitet.
6. Tragen Sie in Splunk Captures ein, um zu überprüfen, ob der Datenverkehr empfangen wird.
7. Für DTLS anyconnect clients vertrauen dem Collector-ZertifikatDas NVM-Profil ist sicher aktiviert.Collector ist für Zertifikate konfiguriert

IPFIX-Datenverkehr wie in Wireshark dargestellt:

Anmerkung: Wenn DTLS zwischen Client und Collector ausgeführt wird, muss der DTLS-Datenverkehr gefiltert werden.



The screenshot shows a Wireshark interface with a display filter set to 'Apply a display filter ... <Ctrl-/>'. The main pane displays a list of network packets. The columns are: No., Tim, Source, Destination, Protocol, Length, and Info. The packets are all CFLOW protocol, 269 bytes long, and contain IPFIX flow data. The source IP is 192.168.100.1 and the destination IP is 10.76.76.161. The info field for each packet indicates 'IPFIX flow (227 bytes) Obs-Domain-ID= 127 [Data:258]'.

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-Client (NVM-Modul)

AnyConnect NVM - Nicht für den Collector gemeldet - CFLOW-Datenpakete verlassen nicht je Endgerät

Steigt die NVM-Datenbankdatei unter C:\%ProgramData%\Cisco\Cisco Anyconnect Secure Mobility Client? Wenn es weiter wächst, bedeutet das, dass die Protokolle nicht vom Kunden gesendet werden. Wenn Sie unter dem Ordner NVM schauen, können Sie sehen, dass die SQL-Datenbank wächst, die nvm.db ist nicht dokumentiert, aber wir sprechen ausführlich darüber, wie wir zwischenspeichern und die Steuerelemente rund um das Caching im [NVM-Handbuch](#). Wenn Sie sehen, dass die Daten nicht an den Collector gesendet werden.

```

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             20,488 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>

```

Trusted Network Detection (TND)

Starten Sie die Benutzeroberfläche von AnyConnect, und stellen Sie sicher, dass sie sich in einem vertrauenswürdigen Netzwerk befindet. NVM benötigt TND, um zu ermitteln, wann sich der Endpunkt in einem vertrauenswürdigen Netzwerk befindet. Wenn die TND-Konfiguration falsch ist, führt dies zu Problemen mit NVM. NVM verfügt über eine eigene TND-Konfiguration, die auf dem TLS-ZertifikatsFingerabdruck des konfigurierten Servers arbeitet. Dies kann im NVM Profile Editor konfiguriert werden.

Wenn NVM TND nicht konfiguriert ist, verlässt sich NVM auf die TND-Konfiguration des VPN-Moduls. Der TND des VPNs basiert auf Informationen, die über DHCP empfangen wurden: Domänenname und DNS-Server. Wenn der DNS-Server und/oder der Domänenname mit den konfigurierten Werten übereinstimmen, gilt das Netzwerk als vertrauenswürdig. VPN unterstützt auch die auf TLS-Zertifikaten basierende TND-Erkennung.

- Stellen Sie sicher, dass die Konfiguration der vertrauenswürdigen Netzwerkerkennung korrekt ist. NVM exportiert nur in einem vertrauenswürdigen Netzwerk, d.h. ungültige TND-Konfiguration (Bsp.: Wenn Sie über 3 DNS-Server verfügen, benötigen Sie 3 definiert).
- Entfernen Sie die vertrauenswürdige Domäne aus der TND VPN-Konfiguration.
- Netzwerkprobleme: Split-Tunneling (die IP-Adresse des Collectors ist nicht Teil des Split-Tunnels und vertrauenswürdig, sodass die Daten über die öffentliche Schnittstelle gesendet werden). Stellen Sie sicher, dass die IP-Adresse des Collectors immer in die Split-Include-Konfiguration für VPN einbezogen wird.
- Stellen Sie sicher, dass CollectionMode für das Erfassen im aktuellen Netzwerk konfiguriert ist (vertrauenswürdig/nicht vertrauenswürdig).
- Vergewissern Sie sich, dass die Ordner VPN.xml und NVM_ServiceProfile.xml im richtigen Ordner sind, und starten Sie den Computer neu
- Anhalten aller AnyConnect-Services
- Bounce das Netzwerk, das mit dem internen Netzwerk verbunden ist, das eine Verbindung zum DNS-Server hat.

Paketerfassung:

```

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]

```

Anyconnect Diagnostic and Reporting Tools (DART)

Um eine Fehlerbehebung für das, was Anyconnect tut, durchzuführen Sie [DART](#) auf den NVM-Komponenten.

- Alle für NVM erforderlichen Protokolle werden von DART verarbeitet, Protokolldateien werden gesammelt, konfiguriert usw.
- Windows-Protokolle - Ereignisse sind nicht an einem zentralen Ort, es gibt ein separates Blatt in der Ereignisanzeige für NVM unter AnyConnect.
- macOS/linux - Filter-Protokolle nach nvAGENT

Collector (auf Linux/Docker-Computer - All-in-One oder Standalone)

acnvmCollector kann nicht installiert werden:

beim Installieren des Collectors und Ausführen des Installationskripts

```
./install_ubuntu.sh
```

Ich erhalte einen Fehler in /var/log/syslog - "ACNVM.conf-Fehler: Zeilennummer 17: erwartete Schlüsselzeichenfolge" war, weil es ein Komma gab, wo es nicht sein sollte, vielleicht ein zusätzliches

acnvmCollector startet nicht:

Dies war ein Problem unter Ubuntu (aber möglich für alle Linux). Ich bemerkte, dass der Code in der acnvmCollector-Datei nicht ausgeführt werden konnte: `/opt/acnvm/bin/acnvmcollector`

Der Benutzer und die Gruppe "acnvm" verfügten nicht über eXecute für den ACNVMCollector.

```
rysh@fife@ubuntu:~/bin$ 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:plunk systemd[1]: acnvm.service: Scheduled restart job, restart counter is at 5.
Sep 18 02:49:10 ubuntu:plunk systemd[1]: Stopped AC NVM Service.
Sep 18 02:49:10 ubuntu:plunk systemd[1]: acnvm.service: Start request repeated too quickly.
Sep 10 02:49:10 ubuntu:plunk systemd[1]: acnvm.service: Failed with result 'exit-code'.
Sep 10 02:49:10 ubuntu:plunk systemd[1]: Failed to start AC NVM Service.
lines 1-11/22 (END) ...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 -t {code=exited, status=203/EXEC}
   Main PID: 7119 (code=exited, status=203/EXEC)

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

Collector-Protokolle

Wie erhalte ich verifizierte vom Collector?

```
./nvmCollector -v
```

Wo kann ich den Debugger einstellen?

Sie können die Protokollierungsebene in ACMNVMLOG.conf festlegen - Der Teil der Konfiguration, der an den Collector-Systemstart gesendet wird. Nach einem Neustart wird der Collector neu gestartet.

log4cplus.rootLogger=DEBUG, STDOUT, NvmFileAppender < dies ist in der Datei

ACNVMLOG.conf.

```
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 tolength=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-Probleme:

- DTLS nicht konfiguriert (d. h. in der Datei "acnvm.conf" nicht sichtbar)
- Der Serverschlüssel ist ungültig (dies war eine Kennwortschlüsselkombination, die nicht unterstützt wird)

Die Splunk Console (NVM Dashboard) zeigt keine Daten an.

AnyConnect-Client

- Generieren Sie Daten mithilfe von YouTube, und navigieren Sie ggf. zu einigen Websites.
- Kann ein AnyConnect-Client Informationen über UDP 2055 an den Collector-Server senden (gibt es dazwischen irgendwelche Firewalls?) Telnet vom Client-Computer zum Collector-Gerät testen
- Ausführen von Wireshark, um sicherzustellen, dass der Client Daten (2055 cflow) an den Collector sendet

Collector-Box

- Überprüfen des empfangenden AnyConnect-NVM-Datenverkehrs Tcpcdump durchführen (und sicherstellen, dass Pakete von Client zu Server für die Jahre 2501 bis 2055 angezeigt werden) Sudo tcpdump -l any -c100 -nn host 10.1.110.7 (dabei werden die ersten 100 Pakete von der Client-Host-IP kommen)[Verwendung von TCPDUMP auf Centos](#)
- Stellen Sie sicher, dass der AnyConnect NVM Collector ausgeführt wird (siehe Informationen oben unter Verwendung von systemctl).
- Überprüfen Sie acnvm.conf auf Formatierung, fehlende Anführungszeichen, Kommas usw.
- **Splunk-Benutzeroberfläche** - TA - Sind die UDP-Dateneingaben und -Souretarten auf der Splunk-GUI oder über input.conf konfiguriert?
Splunk unter der **Benutzeroberfläche** neu starten > **Einstellungen** > **Serversteuerelemente**

Häufige Fragen (FAQs)

1. Wie können Sie Daten von anyconnect NVM an mehrere Ziele senden?

Diese Funktion wird für hohe Verfügbarkeit oder das Senden an Splunk und Stealthwatch verwendet.

Weitere Informationen finden Sie unter <http://cs.co/cesa-pov>

2. Wo speichern Sie das Zertifikat für AnyConnect NVM DTLS?

Dies wäre für Labortests, bei denen kein bekanntes Zertifikat auf dem Collector installiert ist.

- Windows

Installieren Sie das Collector-Zertifikat in den vertrauenswürdigen Windows-Zertifikaten.

- Mac OSX

Für die Installation des Root-Zertifikats ist der Prozess Standard und gut definiert für MACOS, das über die Schlüsselkette ist, können wir Keychain Tool zu importieren und als vertrauenswürdig hinzufügen.

- Linux - unterschiedlich für jede Distribution (Ubuntu und RHEL).

RHEL Root CA-IMPORTSCHRITTE:

1. Kopieren Sie das **CA-Zertifikat** in `/etc/pki/ca-trust/source/anchors`.
2. **sudo update-ca-trust enable**
3. Schließlich **sudo update-ca-trust extrahieren**

Ubuntu Root CA-IMPORTSCHRITTE:

1. Konvertieren Sie die Datei `.cer` in die Datei `.crt`. `openssl x509 -notify PEM-in RootCA.cer -out rootCa.crt`
2. Kopieren Sie die Datei `.crt` in `/usr/local/share/ca-Certificates`
3. Führen Sie den Befehl **sudo update-ca-Certificates aus**.

XML-Dateinamen

Wenn Sie den lokalen Profil-Editor verwenden. Der XML-Profilname des Core-VPN-Moduls spielt keine Rolle. "Speichern Sie das Profil als `NVM_ServiceProfile.xml`. Sie müssen das Profil mit genau diesem Namen speichern, oder NVM kann keine Daten erfassen und senden."

Collector (AnyConnect NVM)

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

- Kann ein Anbieterverzeichnis unter "root" erstellt werden, und dann kann der Eigentümer für ein anderes Konto bereitgestellt werden? Sie können zuerst erstellen `/opt/acnvm`, solange das Installationsskript die Berechtigung zum Kopieren von Dateien besitzt.
- Dateiberechtigungen - **install.sh** benötigt Berechtigungen, um als root auszuführen
- Dienstkonten: Warum **userAdd -r** und wieso - **s /bin/false**, weil es ein nicht interaktives Konto ohne ein Home-Verzeichnis ist. Es ist nicht erforderlich, dass ein Home-Verzeichnis und sein Standardverfahren, dass ein Dienstkonto nicht über ein solches verfügt, um sauber zu bleiben. Alle Benutzer haben uid/guid, unabhängig davon, ob sie ein Home-Verzeichnis haben oder nicht.
- Collector OS - führt CentOS, Ubuntu und Redhat das CentOS-Skript aus.
- Installationsskript - kann bei Bedarf geändert werden. Muss als root oder mit SUDO Recht ausgeführt werden, da ein neuer Benutzer namens **acnvm** erstellt wird und alles in das

`/opt/acnvm`-Verzeichnis einordnet. Allgemeine Anmerkung: Sie können auch ein eigenes Skript erstellen, um entsprechend Ihren Anforderungen das zu tun, was Sie benötigen. Dieses Skript könnte einen anderen Benutzer verwenden, den Sie bereits auf dem System ausgeführt hatten, aber dieser Benutzer müsste SUDO-Rechte haben, um die Installation ausführen zu können.

- So suchen Sie, ob die Collector-Version mit dem `-v`-Flag ausgeführt wird
`./opt/acnvm/bin/acnvmcollection v`

Empfohlene Version

Cisco empfiehlt zum Zeitpunkt der Verwendung oder Aktualisierung stets die neueste Softwareversion von AnyConnect. Wenn Sie die AnyConnect-Version auswählen, verwenden Sie bitte den neuesten 4.9.x-Client oder höher. Dies bietet die neuesten Erweiterungen im Hinblick auf NVM.

AnyConnect 4.9.00086 Neue Funktionen

Dies ist eine Hauptversion, die diese Funktionen enthält und Updates unterstützt und die in [AnyConnect 4.9.0086](#) beschriebenen Fehler behebt.

- NVM-Erweiterung zur Anreicherung von Flow- und Endpunktdaten, einschließlich des neuen NVM Collector, koordiniert mit der Splunk-App 3.x und einem Zeitstempel für Flow-Informationen.

Zugehörige Informationen

- [Cisco Endpoint Security Analytics für Splunk \(Schnellstartanleitung\)](#)
- [Cisco AnyConnect Network Visibility \(NVM\)-App für Splunk](#)
- [Splunk-Dokumentation zur Splunk Collector-Installation und Installation von Collector-Skripten](#)
- [Cisco AnyConnect Secure Mobility Client - Administrationsleitfaden](#)
- [Versionshinweise von AnyConnect 4.x](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)