Configuration d'AnyConnect NVM et de Splunk pour CESA

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Client de mobilité sécurisée Cisco AnyConnect - Plus qu'un VPN
  - IPFIX (Internet Protocol Flow Information Export)
  - Collecteur NVM IPFIX
  - Splunk Enterprise
- Présentation du déploiement
- Topologie
- Configurer
  - Configuration de NVM pour la prise en charge DTLS
    - Exigences du certificat
    - Configuration AnyConnect (4.9.3043 et versions ultérieures)
  - Module NVM AnyConnect autonome
  - Profil client AnyConnect NVM
    - Configuration du profil client NVM via ASDM
    - Configurer le profil client NVM via l'Éditeur de profil AnyConnect
  - Configurer le déploiement Web sur Cisco ASA
  - Configurer le déploiement Web sur Cisco ISE
  - Détection de réseau fiable
- Déploiement
  - Étape 1 : configuration d'AnyConnect NVM sur Cisco ASA/ISE
  - Étape 2. Configuration du composant IPFIX Collector (AnyConnect NVM Collector)
    - Comment installer le collecteur
    - Prise en charge DTLS
  - Étape 3. Configuration du Splunk avec le tableau de bord CESA et le module complémentaire TA
    - Install
    - Activer les entrées UDP via l'interface utilisateur de gestion des liaisons
- Vérifier
  - Validation de l'installation AnyConnect NVM
  - Valider l'état du collecteur
  - Valider le splunk - Tableau de bord CESA
  - Flux de paquets
  - Modèles de flux
- Dépannage
  - Client AnyConnect (module NVM)

Les données ne sont pas signalées au collecteur et les paquets de données ne sont pas envoyés à partir du terminal
TND (Trusted Network Detection)
Outils de diagnostic et de création de rapports (DART) AnyConnect
Collecteur (sur une machine Linux/Docker : tout-en-un ou autonome)
Échec de l'installation de acnvmcollector
Échec du démarrage de acnvmcollector
Journaux du collecteur : où puis-je définir le débogage ?
Comment puis-je trouver le numéro de version du collecteur ?
Problèmes DTLS
La console Splunk (tableau de bord CESA) n'affiche pas les données
Client AnyConnect
Boîte Collectrice
Questions courantes (FAQ)
Comment pouvez-vous envoyer des données d'AnyConnect NVM vers plusieurs destinations ?
Où stockez-vous le certificat pour AnyConnect NVM DTLS ?
Noms de fichiers XML
Collecteur (AnyConnect NVM)
Version recommandée
Informations connexes

Introduction

Ce document décrit comment installer et configurer le module Cisco AnyConnect Network Visibility Module (NVM) sur un système d'utilisateur final qui exécute AnyConnect 4.7.x ou version ultérieure, et comment installer et configurer les composants Splunk Enterprise et le collecteur NVM associés.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- AnyConnect 4.7.x ou version ultérieure avec NVM
- Licences AnyConnect
- Adaptive Security Device Manager (ASDM) 7.5.1 ou version ultérieure
- Connaissance de Splunk Enterprise et de l'installation des applications et modules complémentaires Splunk

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco AnyConnect Security Mobility Client 4.7.x ou version ultérieure
- Éditeur de profil Cisco AnyConnect

- Appareil de sécurité adaptatif Cisco (ASA), version 9.5.2
- Cisco Adaptive Security Device Manager (ASDM), version 7.5.1
- Splunk Enterprise 7.x ou version ultérieure (installé comme tout-en-un sur toute plate-forme Linux prise en charge ; CentOS (préféré)
- Toute installation Linux prise en charge en tant que collecteur

> Remarque : Un collecteur peut être exécuté sur le même serveur. Référez-vous à Cisco Endpoint Security Analytics (CESA) Construit sur Splunk Quickstart POV Kit & Deployment Guide pour plus d'informations.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La solution Cisco AnyConnect NVM fournit une source continue de données télémétriques sur les terminaux de grande valeur qui permet aux entreprises de voir le comportement des terminaux et des utilisateurs sur leur réseau. NVM collecte les flux à partir des terminaux sur site et hors site, ainsi que des contextes importants tels que les utilisateurs, les applications, les périphériques, les emplacements et les destinations. Splunk Enterprise utilise les données de télémétrie et fournit les fonctionnalités d'analyse et les rapports.

Cette note technique est un exemple de configuration pour AnyConnect NVM avec Splunk Enterprise dans le cadre de la nouvelle solution Cisco Endpoint Security Analytics (CESA).

- Pour une présentation complète de la preuve de valeur (PDV) de CESA avec Splunk, reportez-vous au Cisco Endpoint Security Analytics (CESA) Built on Splunk Quickstart POV Kit & Deployment Guide.
- Pour obtenir un guide du tableau de bord CESA NVM sur Splunk, reportez-vous à la présentation et à la FAQ du tableau de bord Cisco Endpoint Security Analytics (CESA).
- Pour plus d'informations sur la solution, référez-vous à Cisco Endpoint Security Analytics Built on Splunk.

Ces composants constituent la solution :

- Client Cisco AnyConnect Secure Mobility avec module de visibilité réseau (NVM) activé
- Application Cisco Endpoint Security Analytics (CESA) pour Splunk
- Module complémentaire Cisco Endpoint Security Analytics (CESA) pour Splunk
- Collecteur NVM (inclus dans un fichier zip avec le module complémentaire NVM TA)

Client de mobilité sécurisée Cisco AnyConnect - Plus qu'un VPN

Cisco AnyConnect est un agent unifié qui fournit plusieurs services de sécurité pour protéger

l'entreprise. AnyConnect est le plus souvent utilisé comme client VPN d'entreprise, mais il prend également en charge des modules supplémentaires qui répondent aux différents aspects de la sécurité d'entreprise. Les modules supplémentaires offrent des fonctions de sécurité telles que l'évaluation de la position, la sécurité Web, la protection contre les programmes malveillants, la visibilité sur le réseau, etc.

Cette note technique traite de NVM, qui s'intègre à Cisco AnyConnect pour permettre aux administrateurs de surveiller l'utilisation des applications des terminaux. Pour plus d'informations sur Cisco AnyConnect, référez-vous au Guide de l'administrateur du client Cisco AnyConnect Secure Mobility, version 4.7.

IPFIX (Internet Protocol Flow Information Export)

IPFIX est un protocole IETF qui définit une norme pour l'exportation d'informations de flux IP à des fins diverses, telles que la comptabilité, l'audit et la sécurité. IPFIX est basé sur le protocole Cisco NetFlow v9, bien qu'ils ne soient pas directement compatibles. Cisco nvzFlow est une spécification de protocole basée sur le protocole IPFIX. Par sa conception, IPFIX est un protocole extensible qui vous permet de définir de nouveaux paramètres pour transmettre des informations. Le protocole Cisco nvzFlow étend la norme IPFIX et définit de nouveaux éléments d'information. Le protocole définit également un ensemble standard de modèles IPFIX qui sont transmis dans le cadre de la télémétrie utilisée par AnyConnect NVM.

Pour plus d'informations sur IPFIX, référez-vous à ces RFC :

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

Collecteur NVM IPFIX

Un collecteur est un serveur qui reçoit et stocke des données IPFIX. Il peut ensuite transmettre ces données à Splunk.

Cisco fournit un collecteur spécialement conçu pour le protocole nvzFlow et fourni avec le module complémentaire CESA TA pour Splunk. Le collecteur peut être installé sur le même boîtier (tout-en-un) que le serveur Splunk, sur le redirecteur lourd ou sur un boîtier Linux autonome.

Pour plus d'informations sur le collecteur, référez-vous à Collecteur Cisco Network Visibility (NVM).

Splunk Enterprise

Splunk Enterprise est un outil puissant qui collecte et analyse des données de diagnostic pour fournir des informations utiles sur l'infrastructure informatique. Il fournit un emplacement unique

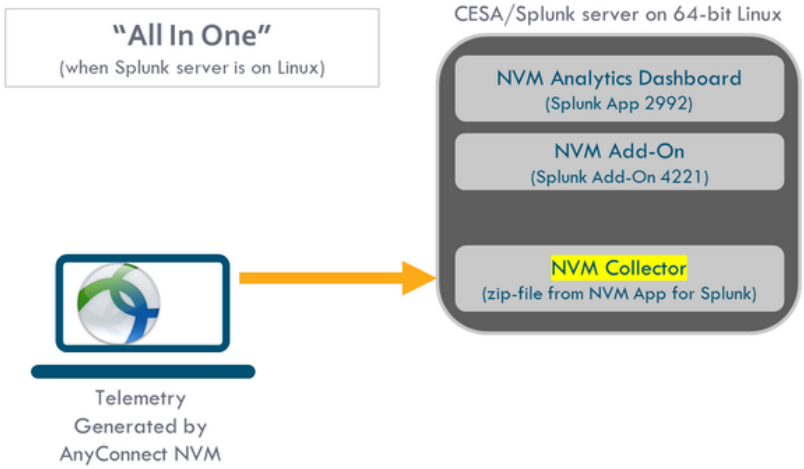
permettant aux administrateurs de collecter des données qui les aident à comprendre l'état du réseau.

Splunk est un partenaire Cisco et la solution CESA a été créée en collaboration avec lui. Pour plus d'informations, référez-vous à Cisco Endpoint Security Analytics Built on Splunk.

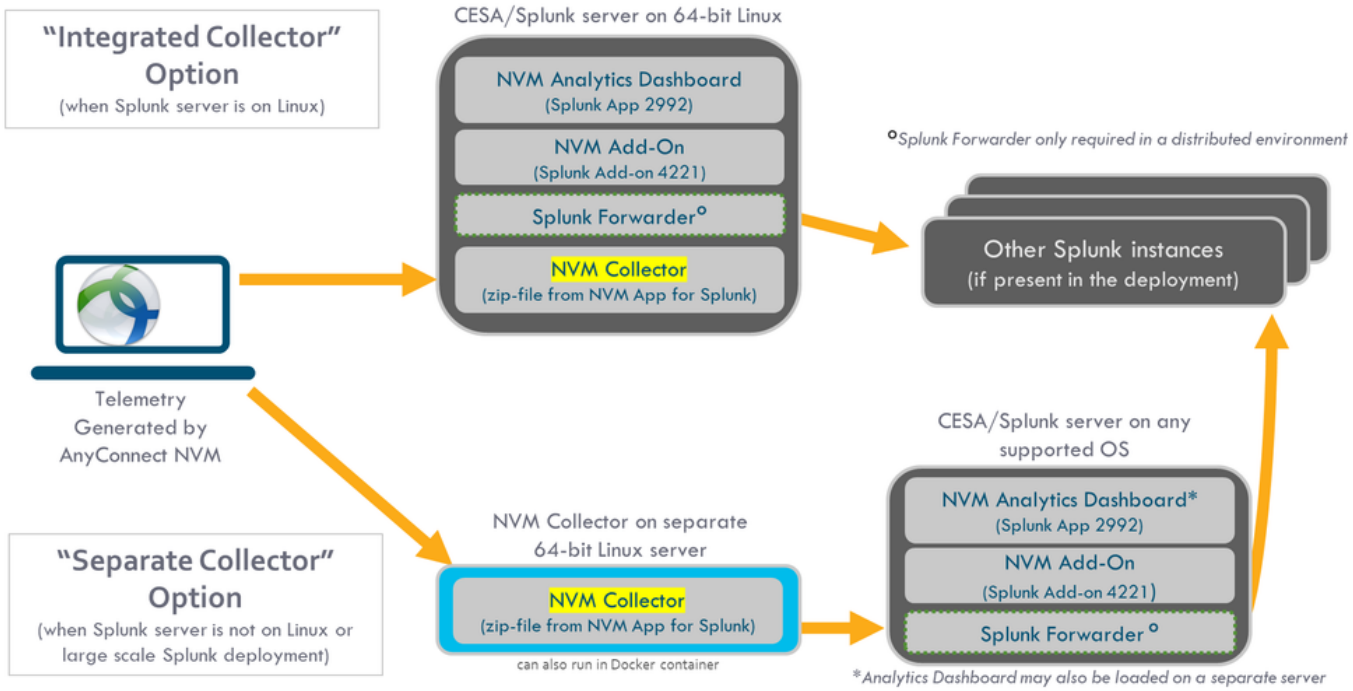
Présentation du déploiement

Ce document fournit une présentation générale du déploiement sous sa forme la plus simple. Il s'agit d'une configuration tout-en-un qui s'exécute sur Linux 64 bits.

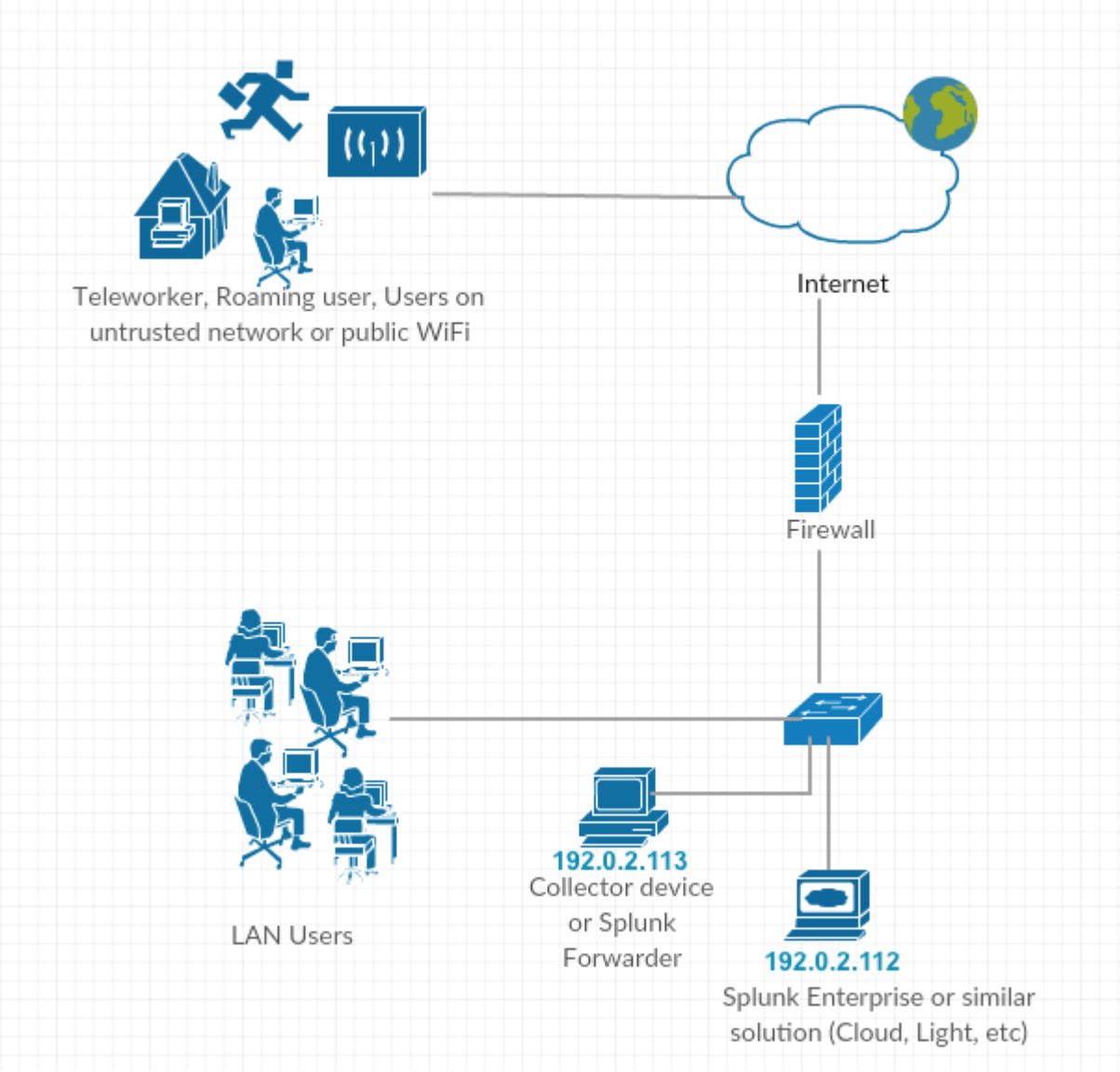
Ce schéma montre la configuration utilisée pour la plupart des démonstrations. Cette configuration est également utile dans un petit déploiement de production.



Ce schéma présente un ensemble plus complet d'options disponibles pour le déploiement. En général, une configuration de production est distribuée et comporte plusieurs noeuds Splunk Enterprise.


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

Topologie



Conventions d'adresse IP dans cette technote :

- Adresse IP du collecteur : 192.0.2.123
- Adresse IP du splunk : 192.0.2.113

Configurer

Cette section traite de la configuration des composants Cisco NVM. Pour obtenir une présentation du déploiement AnyConnect NVM et du profil de configuration, reportez-vous également à la section How to Implement the AnyConnect Network Visibility Module.

Configuration de NVM pour la prise en charge DTLS

NVM peut désormais être configuré pour envoyer des données de manière sécurisée au collecteur via DTLS. Ce mode est configurable dans l'Éditeur de profil NVM. Lorsque la case « Sécurisé » est cochée, NVM utilise DTLS comme transport. Pour que la connexion DTLS soit établie, le certificat du serveur (collecteur) DTLS doit être approuvé par le point d'extrémité. Les certificats non approuvés sont rejetés en silence. DTLS 1.2 est la version minimale prise en

charge. Le collecteur de l'application CESA Splunk App v3.1.2 ou ultérieure est requis pour la prise en charge DTLS. Le collecteur ne fonctionne que dans un mode : sécurisé ou non sécurisé.

Exigences du certificat

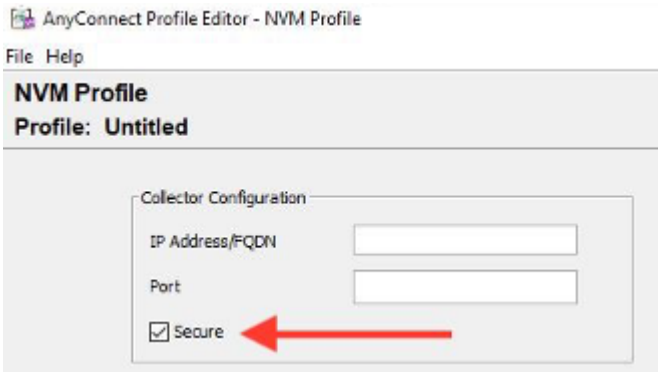
- Le certificat du collecteur doit être approuvé par le client. (Assurez-vous que la chaîne de certificats est approuvée, car il n'y a aucune configuration sur AnyConnect.)
- Le certificat doit être au format PEM.
- Ne prend pas en charge un mot de passe de clé de certificat. Remarque : L'autorité de certification (CA) interne de Cisco Identity Services Engine (ISE) en nécessite une.
- Tout certificat peut être utilisé sur le collecteur tant que la machine cliente AnyConnect l'approuve (infrastructure à clé publique (PKI) interne, bien connue, etc.).
- Une fois le fichier de configuration mis à jour, le service NVM AnyConnect doit redémarrer (pour les tests sur client unique). Pour les profils envoyés depuis ISE ou ASA (Adaptive Security Appliance), l'ordinateur client doit se déconnecter du réseau, puis se reconnecter.

- La configuration du collecteur de profils NVM AnyConnect doit être définie sur IP ou sur FQDN. Ce choix dépend de la valeur utilisée dans le nom commun (CN) du certificat. Le nom de domaine complet (FQDN) est toujours préférable en cas de changement d'adresse IP.

    - Si vous utilisez une adresse IP, le certificat collecteur CN ou le nom alternatif du sujet (SAN) doit avoir cette adresse IP.
    - Si le nom de domaine complet (FQDN) est le nom de domaine complet (CN) dans le certificat, le profil NVM doit avoir le même nom de domaine complet (FQDN) que le collecteur.

Configuration AnyConnect (4.9.3043 et versions ultérieures)

Pour le profil NVM, une nouvelle case à cocher appelée « Secure » est disponible sous Collector IP/port.



Module NVM AnyConnect autonome

Le module autonome nécessite AnyConnect 4.8.01090 ou version ultérieure. Reportez-vous au Guide de l'administrateur du client Cisco AnyConnect Secure Mobility, version 4.9. Reportez-vous également à ce guide autonome : Comment mettre en oeuvre le module de visibilité sur le réseau

AnyConnect.

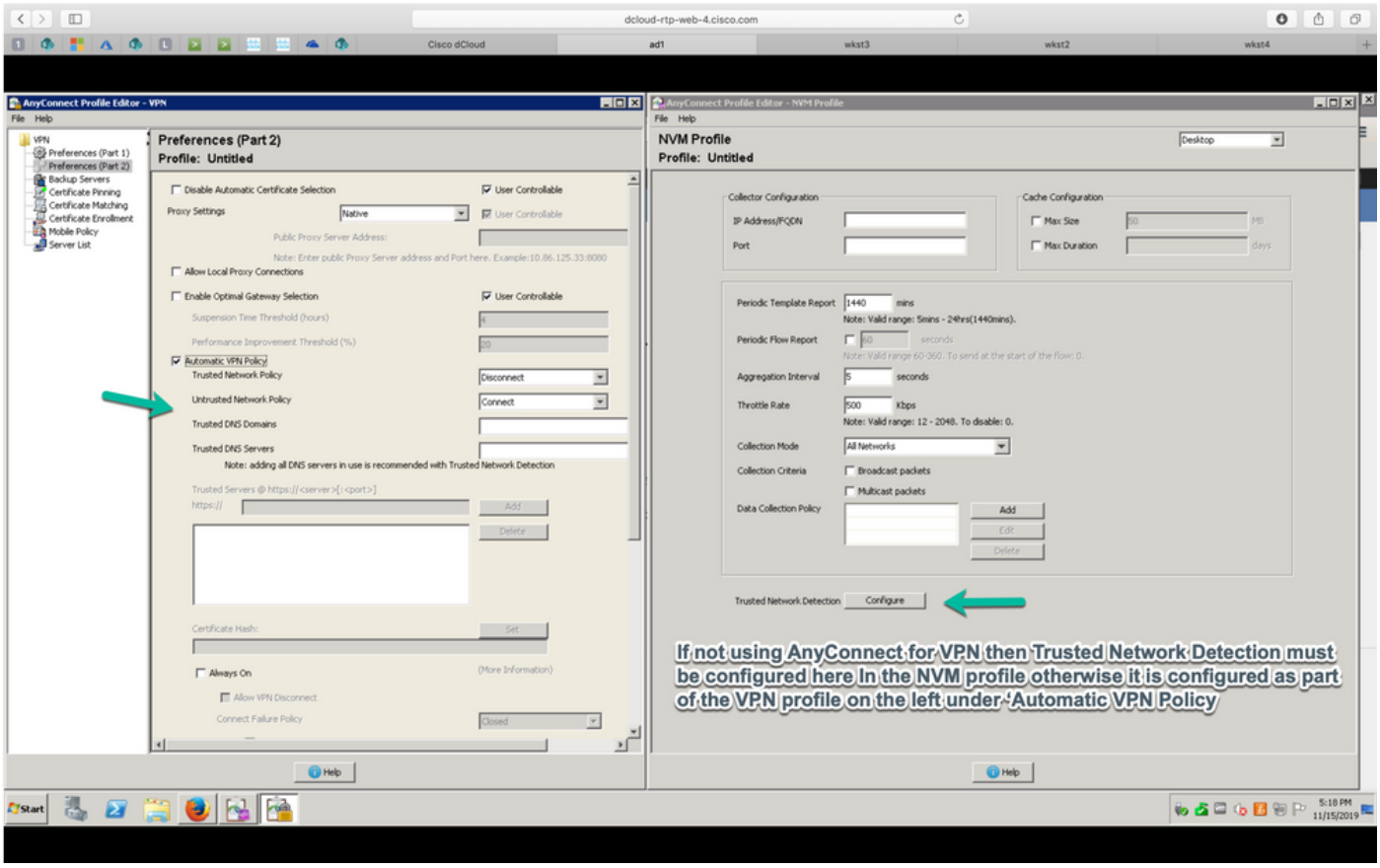
Si vous ne disposez pas d'un déploiement AnyConnect ou si vous utilisez une autre solution VPN, vous pouvez installer le package autonome NVM pour vos besoins NVM. Ce package fonctionne indépendamment, mais offre le même niveau de collecte de flux à partir d'un terminal que la solution NVM AnyConnect actuelle. Si vous installez la NVM autonome, les processus actifs (tels que Activity Monitor sur le système d'exploitation Macintosh (macOS)) indiquent l'utilisation.

La NVM autonome est configurée avec l'Éditeur de profil NVM, et la configuration TND (Trusted Network Detection) est obligatoire. NVM utilise la configuration TND pour déterminer si le point d'extrémité se trouve sur le réseau d'entreprise, puis applique les politiques appropriées.

Le dépannage et la journalisation sont toujours effectués par les outils de diagnostic et de génération de rapports (DART) AnyConnect, qui peuvent être installés à partir du package AnyConnect.

Avant la disponibilité de l'option autonome, le module VPN principal devait être installé afin de tirer parti de TND. La vignette VPN principale était visible dans l'interface utilisateur, ce qui pouvait induire en erreur les utilisateurs finaux, en particulier s'ils utilisent une solution VPN d'un autre fournisseur.

Lorsque vous utilisez l'option autonome, vous n'utilisez pas le profil VPN principal pour configurer TND. Le profil NVM peut désormais être configuré directement pour TND.



Profil client AnyConnect NVM

La configuration AnyConnect NVM est enregistrée dans un fichier XML qui contient des informations sur l'adresse IP et le numéro de port du collecteur, ainsi que d'autres informations. L'adresse IP du collecteur et un numéro de port doivent être correctement configurés sur le profil client NVM.

Pour un fonctionnement correct du module NVM, le fichier XML doit être placé dans ce répertoire :

- Pour Windows 7 et versions ultérieures : %ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM
- Pour Mac OSX : /opt/cisco/anyconnect/nvm

Si le profil est présent sur Cisco ASA/ISE, il est automatiquement déployé avec le déploiement AnyConnect NVM.

Exemple de profil XML:

<#root>

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

192.0.2.123

</CollectorIP>
<Port>

2055

</Port>
</CollectorConfiguration>
<Anonymize>

false

</Anonymize>
<CollectionMode>

all

</CollectionMode>
</NVMProfile>
```

Un profil NVM peut être créé à l'aide des outils suivants :

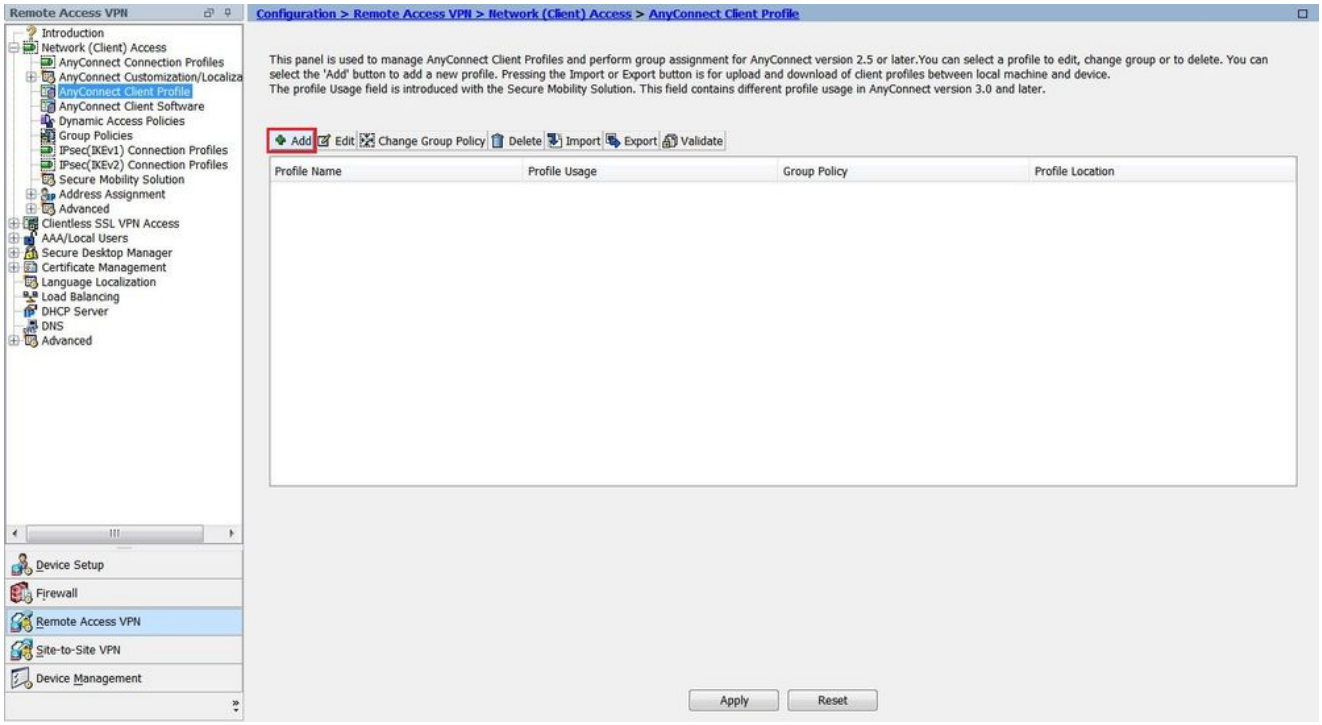
- Cisco ASDM
- Éditeur de profil AnyConnect
- ISE

Configuration du profil client NVM via ASDM

Cette méthode est préférable si AnyConnect NVM est déployé via Cisco ASA :

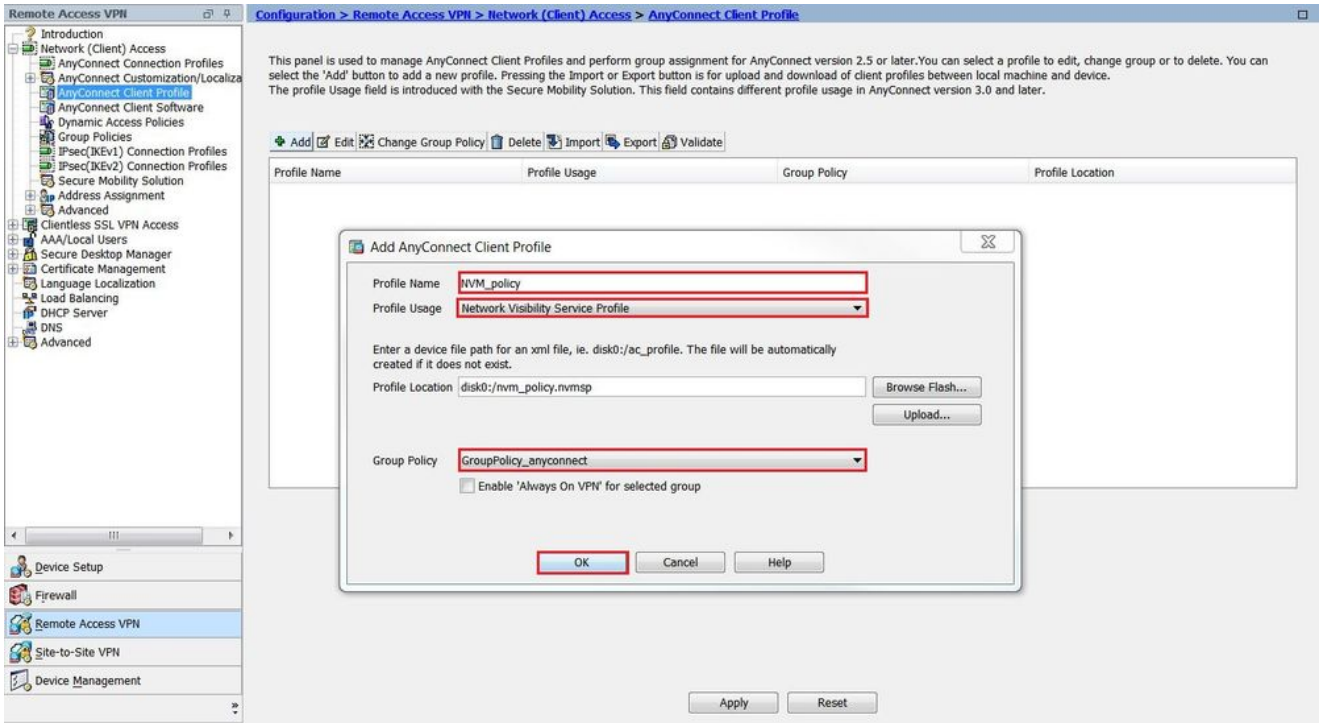
1. Accédez à Configuration > Remove Access VPN > Network (Client) Access > AnyConnect Client Profile.

2. Cliquez sur Add, comme illustré dans l'image.

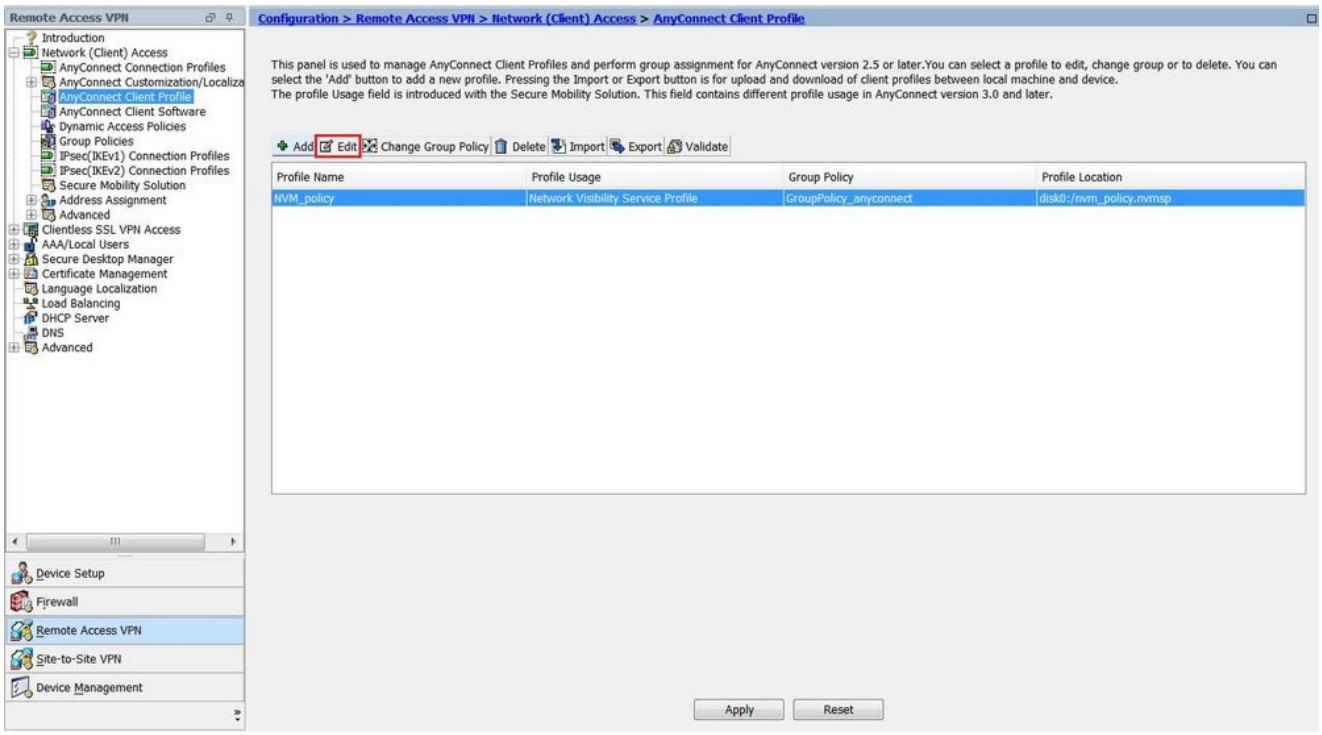


3. Donnez un nom au profil. Dans Utilisation du profil, sélectionnez Profil de service de visibilité réseau.

4. Attribuez le profil à la stratégie de groupe actuellement utilisée par les utilisateurs AnyConnect et cliquez sur OK, comme illustré dans l'image.

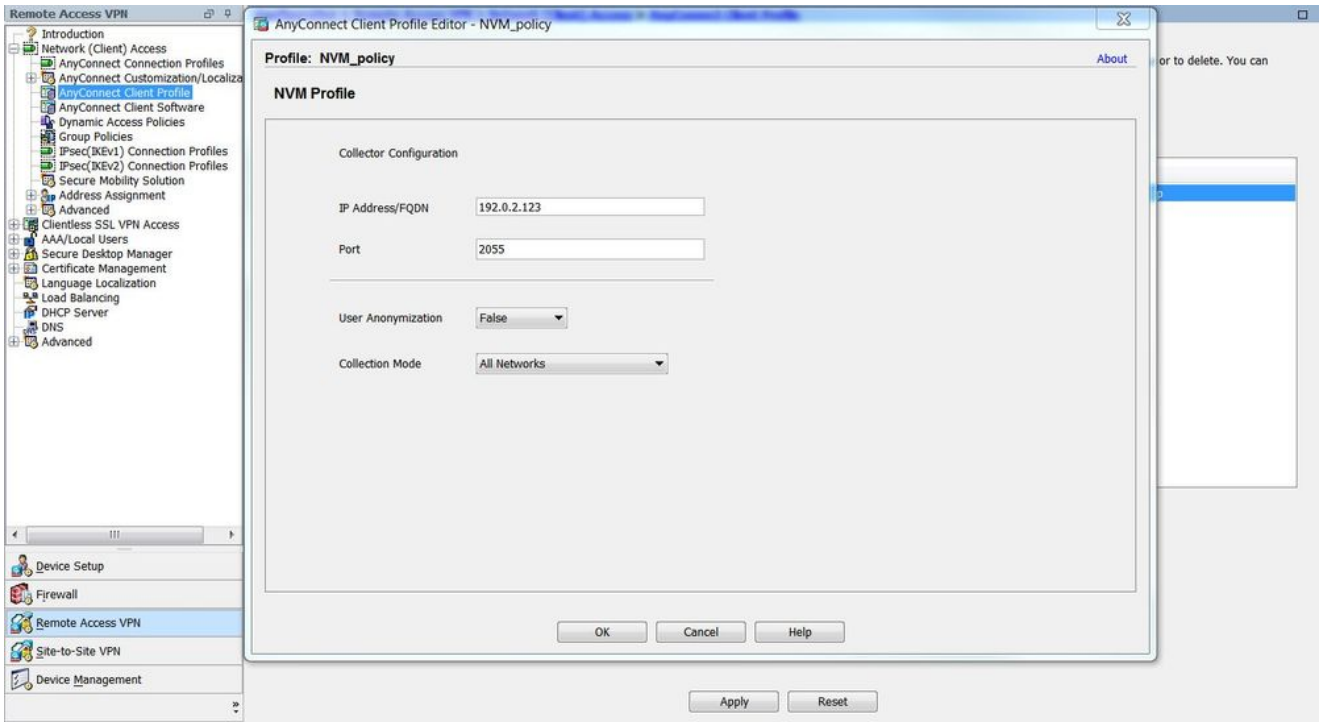


5. Une fois la nouvelle stratégie créée, cliquez sur Edit, comme indiqué dans l'image.



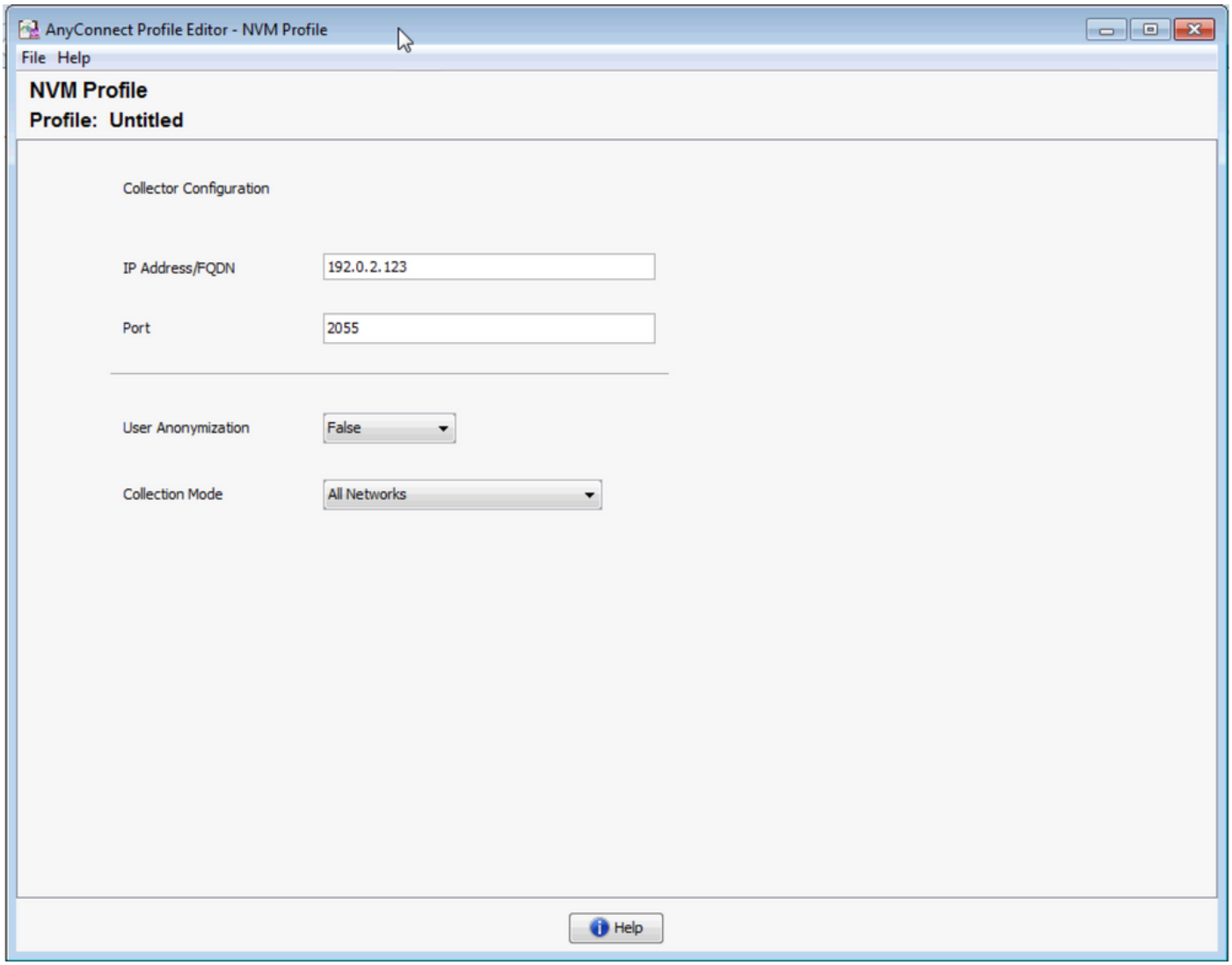
6. Saisissez les informations relatives à l'adresse IP et au numéro de port du collecteur ; puis cliquez sur OK.

7. Cliquez sur Apply, comme illustré dans l'image.



Configurer le profil client NVM via l'Éditeur de profil AnyConnect

Cet outil est un outil autonome disponible sur le site Cisco.com. Cette méthode est préférable si AnyConnect NVM est déployé via Cisco ISE. Le profil NVM créé à l'aide de cet outil peut être téléchargé vers Cisco ISE ou copié directement vers les terminaux.



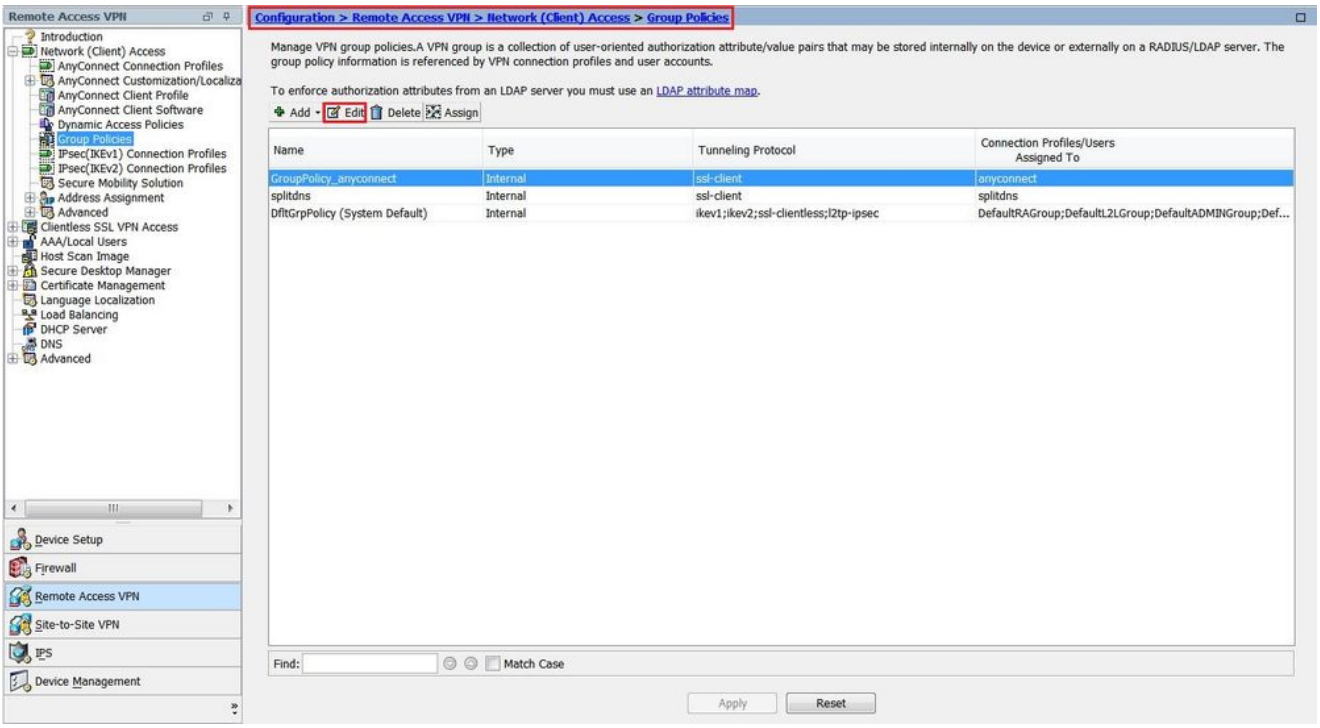
Pour plus d'informations sur l'Éditeur de profil AnyConnect, reportez-vous à Éditeur de profil AnyConnect.

Configurer le déploiement Web sur Cisco ASA

Cette note technique suppose qu'AnyConnect est déjà configuré sur l'ASA et que vous devez ajouter uniquement la configuration du module NVM. Pour obtenir des informations détaillées sur la configuration d'ASA AnyConnect, reportez-vous au livre 3 d'ASDM : Guide de configuration de l'ASDM VPN de la gamme Cisco ASA, 7.16.

Afin d'activer le module AnyConnect NVM sur Cisco ASA, effectuez ces étapes :

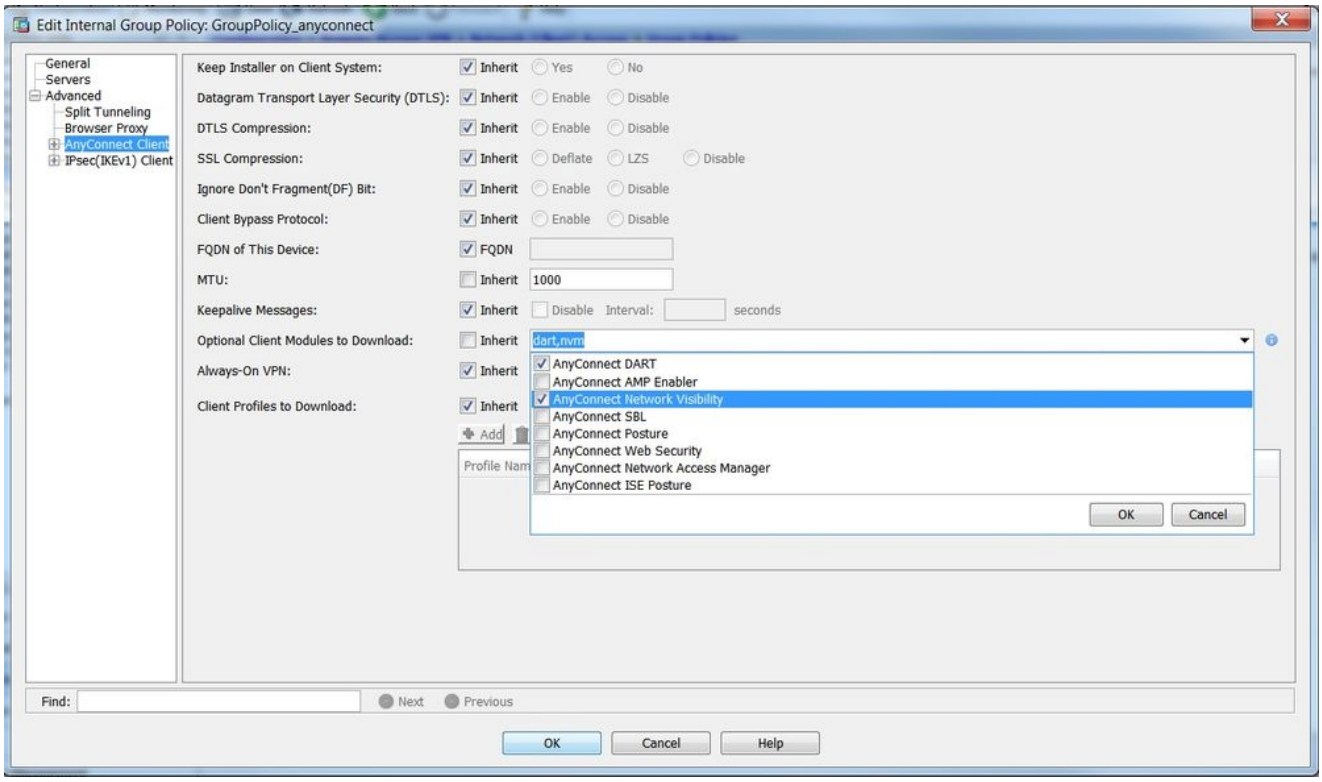
1. Accédez à Configuration > Remote Access VPN > Network (Client) Access > Group Policies.
2. Sélectionnez la stratégie de groupe appropriée et cliquez sur Edit, comme indiqué dans l'image.



3. Dans la fenêtre contextuelle de stratégie de groupe, accédez à Advanced > AnyConnect Client.

4. Développez Optional Client Modules to Download et sélectionnez AnyConnect Network Visibility.

5. Cliquez sur OK et appliquez les modifications.

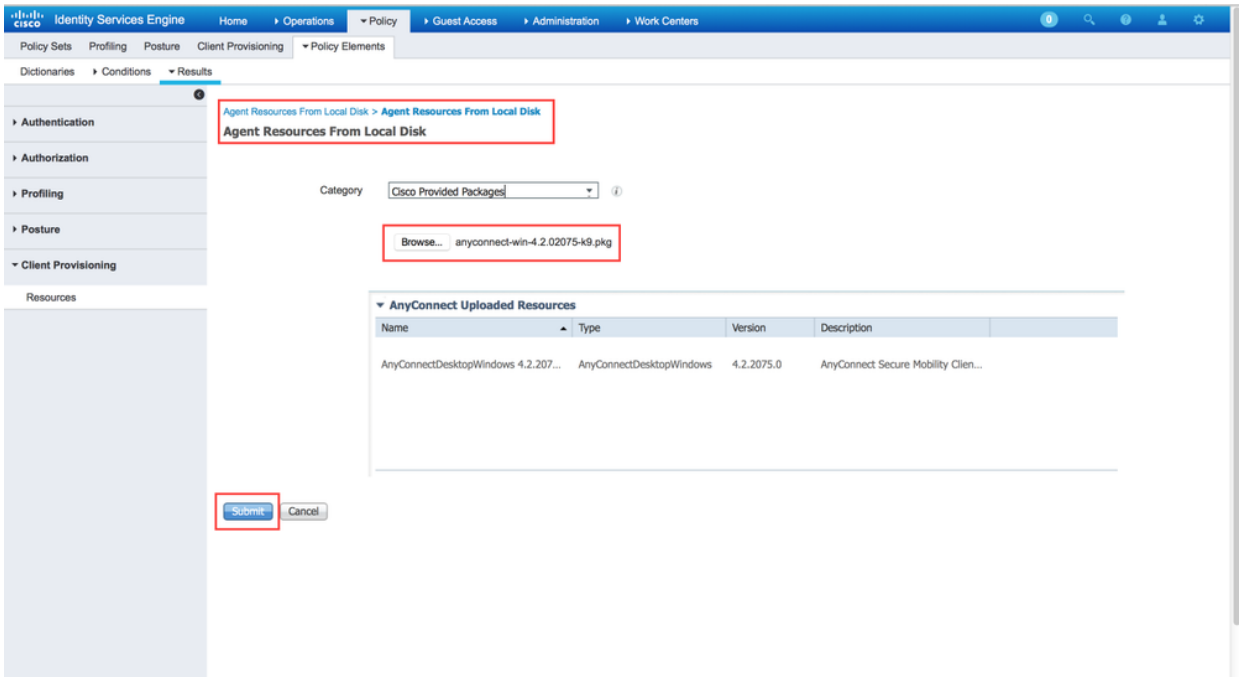


Configurer le déploiement Web sur Cisco ISE

Dans cette section, nous activons les modules AnyConnect Client, les profils, les packages de personnalisation/langue et les packages Opswat.

Pour configurer Cisco ISE pour AnyConnect Web-Deployment, procédez comme suit :

1. Dans l'interface utilisateur graphique de Cisco ISE, accédez à Policy > Policy Elements > Results.
2. Développez Client Provisioning pour afficher Resources ; puis sélectionnez Ressources.
3. Ajoutez l'image AnyConnect :
    1. Sélectionnez Add > Agent Resources et téléchargez le fichier de package AnyConnect.



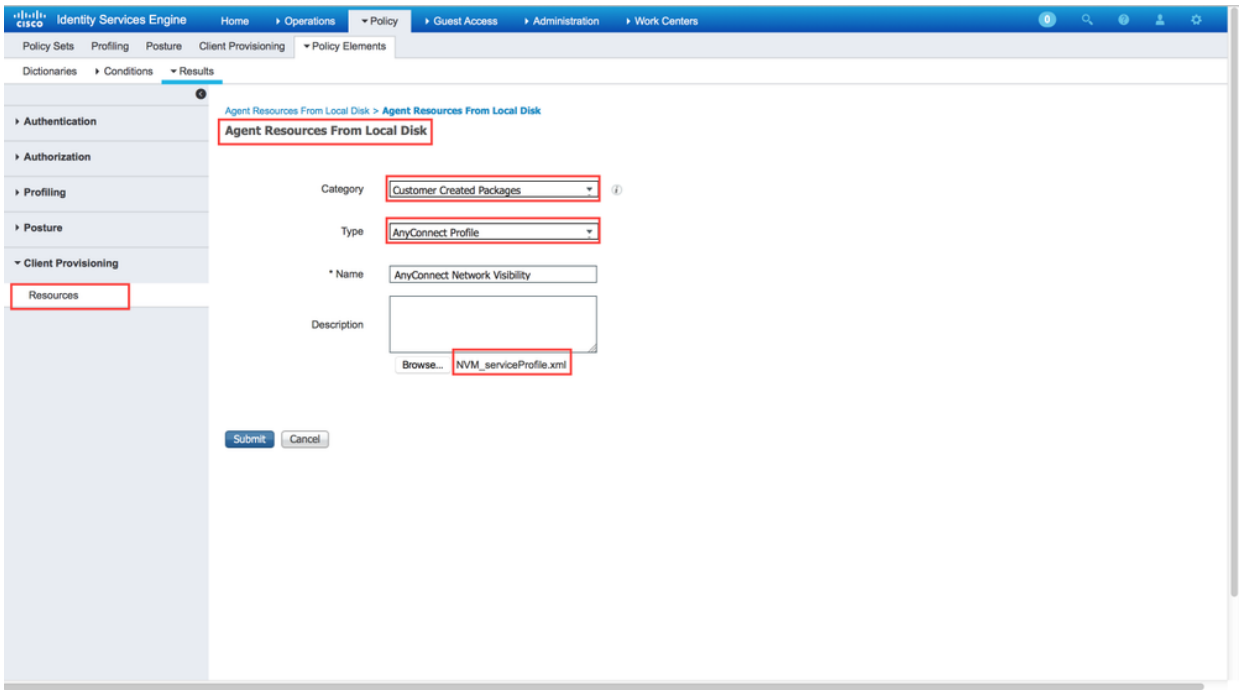
    2. Vérifiez le hachage du package dans la fenêtre contextuelle.

        Le hachage du fichier peut être comparé à la page de téléchargement Cisco.com ou via un outil tiers.

        Cette étape peut être répétée pour ajouter plusieurs images AnyConnect (par exemple, pour Mac OSX et Linux OS).



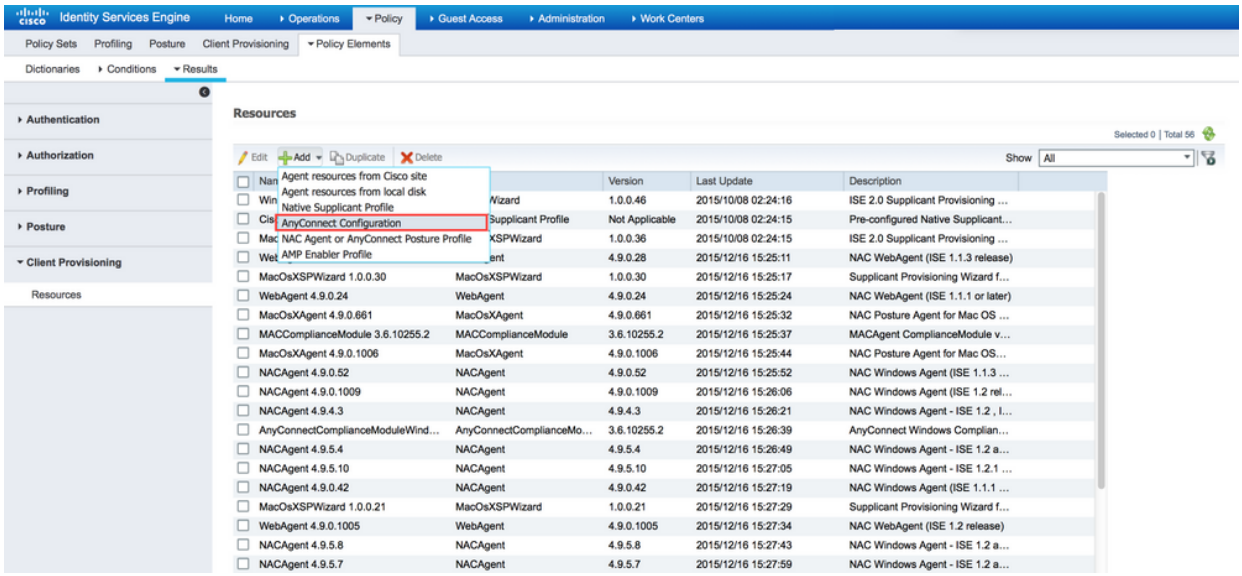
4. Ajoutez le profil NVM AnyConnect :
    1. Sélectionnez Add > Agent Resources et téléchargez le profil client NVM.



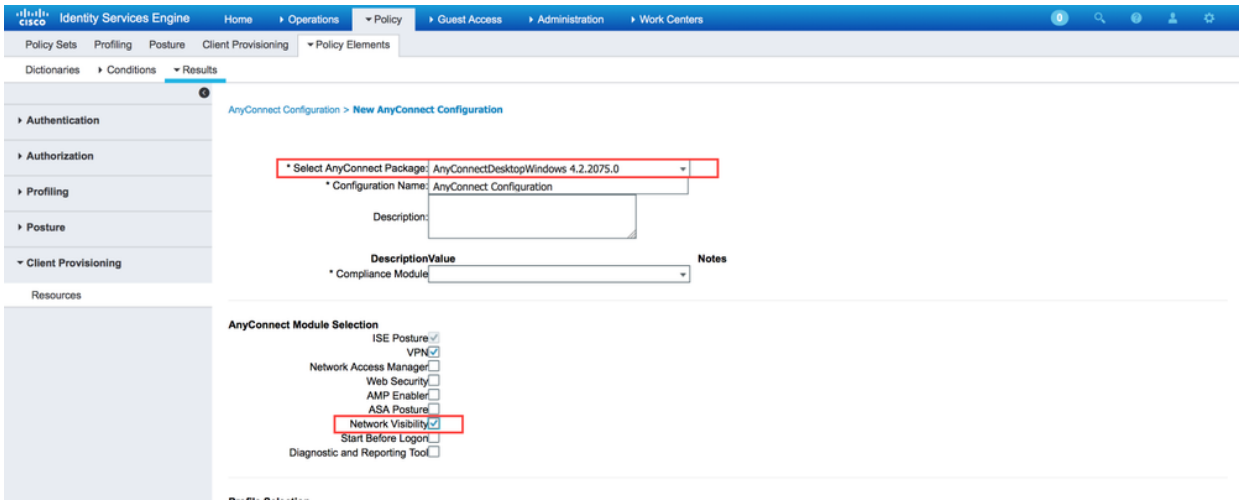
5. Ajoutez le fichier de configuration AnyConnect :

    1. Cliquez sur Add et choisissez AnyConnect Configuration.

        Sélectionnez le package que vous avez téléchargé à l'étape précédente.



    2. Activez NVM dans la sélection de module AnyConnect, ainsi que la politique requise.

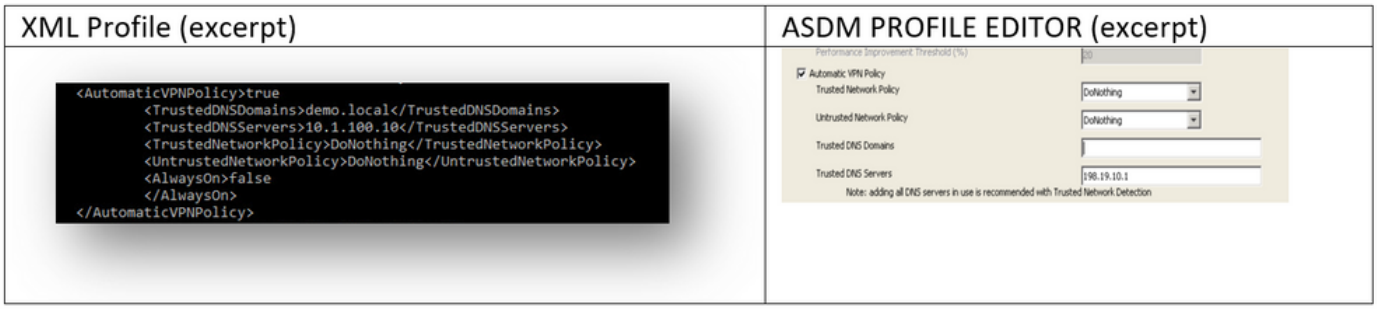


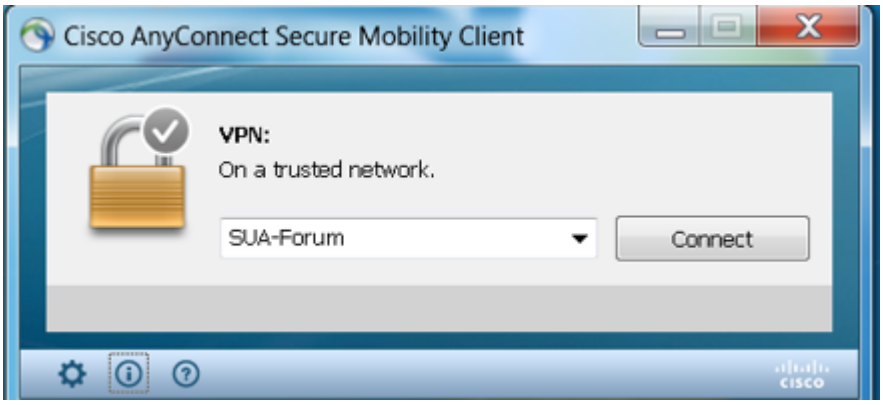
Pour obtenir des informations détaillées sur la configuration du déploiement Web sur Cisco ISE, reportez-vous à Déploiement Web d'AnyConnect.

Détection de réseau fiable

AnyConnect NVM envoie des informations de flux uniquement lorsqu'il se trouve sur un réseau de confiance. Il utilise la fonction TND du client AnyConnect pour savoir si le point d'extrémité se trouve ou non dans un réseau approuvé.

TND (Trusted Network Detection) est configuré dans le profil client AnyConnect (XML) utilisé pour le VPN, que le composant VPN soit actuellement utilisé dans l'environnement ou non. TND est activé via la configuration de la section Automatic VPN Policy dans le profil. Au minimum, un seul domaine DNS approuvé ou serveur DNS approuvé doit être renseigné. Les actions entreprises par AnyConnect lorsque le client a déterminé qu'il se trouve sur un réseau approuvé peuvent être définies sur le mode DoNothing via la liste déroulante pour la politique de réseau approuvé et non approuvé.





Pour plus de détails sur la configuration TND, référez-vous à À propos de la détection de réseau de confiance.

Déploiement

Le déploiement de la solution AnyConnect NVM nécessite les étapes suivantes :

1. Configurez AnyConnect NVM sur Cisco ASA/ISE.
2. Configurez le composant IPFIX Collector (NVM Collector sur Linux - fourni avec le module complémentaire TA).
3. Configurez Splunk avec l'application CESA et le module complémentaire TA.

Étape 1 : configuration d'AnyConnect NVM sur Cisco ASA/ISE

Cette étape est traitée en détail dans la section Configurer de ce document.

Une fois la NVM configurée sur Cisco ISE/ASA, elle peut être automatiquement déployée sur les terminaux clients.

Étape 2. Configuration du composant IPFIX Collector (AnyConnect NVM Collector)

Le composant Collecteur est responsable de la collecte et de la traduction de toutes les données IPFIX à partir des terminaux, et de la transmission des données au module complémentaire Cisco Endpoint Security Analytics (CESA) pour Splunk. Le collecteur NVM fonctionne sous Linux 64 bits. Les scripts de configuration CentOS, Ubuntu et Docker sont inclus. Les scripts d'installation et les fichiers de configuration de CentOS peuvent également être utilisés dans les distributions Fedora et Redhat.

Dans un déploiement distribué type de Splunk Enterprise, le collecteur doit être exécuté sur un système Linux 64 bits autonome ou sur un noeud Splunk Forwarder qui s'exécute sur Linux 64 bits. Le collecteur peut également être installé sur un serveur autonome sans composants Splunk.

Remarque : La solution peut également être exécutée sur un seul système Linux 64 bits qui inclut le collecteur NVM et les composants Splunk Enterprise pour une utilisation dans un

---

petit déploiement ou à des fins de démonstration. Le tout-en-un est le plus facile pour un maximum de 10 000 terminaux. Référez-vous à PDV client réel pour les informations de dimensionnement de PDV.

Comment installer le collecteur

1. Copiez le fichier acnvmcollector.zip, situé dans le répertoire /opt/splunk/etc/apps/TA-Cisco-NVM/appserver/addon/ (inclus avec le module complémentaire TA), sur le système où vous souhaitez l'installer.

2. Décompressez le fichier acnvmcollector.zip pour extraire les fichiers.

Il est recommandé de lire le fichier $PLATFORM$_README dans le bundle .zip avant d'exécuter le script install.sh. Le fichier $PLATFORM$_README fournit des informations sur les paramètres de configuration pertinents qui doivent être vérifiés et modifiés (si nécessaire) avant l'exécution du script install.sh. Au minimum, vous devez configurer l'adresse de l'instance Splunk vers laquelle vous transférez les données. Si le système n'est pas correctement configuré, le collecteur risque de ne pas fonctionner correctement.

Remarque : Assurez-vous que vos pare-feu réseau et hôte sont configurés pour autoriser le trafic UDP pour les adresses et ports source et de destination. Les pare-feu doivent autoriser le trafic IPFIX entrant (CFLOW) des clients AnyConnect vers le collecteur et les données UDP sortantes vers Splunk.

Une seule instance de collecteur NVM peut gérer un minimum de 5 000 flux par seconde sur un système correctement dimensionné, ou jusqu'à 35 000 à 40 000 terminaux. Le collecteur doit être configuré et en cours d'exécution avant que la NVM Splunk et le TA-Add sur l'application puissent être utilisés.

Par défaut, le collecteur reçoit les flux des points d'extrémité NVM AnyConnect sur le port UDP 2055.

En outre, le collecteur produit trois sources de données pour Splunk :

- Données par flux sur le port UDP 20519
- Données d'identité du terminal sur le port UDP 20520
- Données d'interface de terminal sur port UDP 20521

Les ports de réception et de flux de données peuvent être modifiés. Pour ce faire, modifiez le fichier acnvm.conf et redémarrez l'instance du collecteur. Assurez-vous que les pare-feu hôte/réseau entre les points d'extrémité et le collecteur ou entre le collecteur et le ou les systèmes Splunk sont ouverts pour les ports et adresses UDP configurés. Assurez-vous également que votre configuration AnyConnect NVM correspond à celle de votre collecteur.

Une fois tous les composants installés et en cours d'exécution, reportez-vous à la section Fichiers d'aide de l'application Splunk pour obtenir des informations détaillées sur les rapports

préconfigurés, le modèle de données et les éléments d'information créés par la solution.

Vous pouvez redémarrer l'un de vos terminaux AnyConnect et valider l'envoi du trafic vers la solution. Par exemple, vous pouvez utiliser youtube.com pour exécuter un flux continu de données.

Ces informations doivent être configurées dans le fichier de configuration acnvm.conf :

- syslog_server_ip (instance de redirecteur ou de liaison) : Peut pointer vers 127.0.0.1 (n'utilisez pas LOCALHOST) s'il se trouve sur la même boîte.
- Port d'écoute du collecteur (données IPFIX entrantes) : La valeur par défaut est OK.

Remarque : netflow_collector_ip est omis du fichier de configuration. Il utilise l'interface publique par défaut et ne doit être modifié que pour remplacer la valeur par défaut par une adresse IP locale spécifique.

Les paramètres par port de données de flux, par port de données d'identité de point de terminaison, par port d'interface de point de terminaison et par port de collecteur sont préconfigurés avec les paramètres par défaut dans le fichier de configuration. Vous devez modifier ces valeurs si vous utilisez des ports autres que les ports par défaut.

Ces informations sont ajoutées dans le fichier de configuration : /opt/acnvm/conf/acnvm.conf

Prise en charge DTLS

Remarque : Voir Configurer NVM pour la prise en charge DTLS dans ce document pour plus de détails.

Procédez comme suit sur le boîtier qui héberge le collecteur :

- Créez ce répertoire : /opt/acnvm/certs.
- Afin d'appliquer le certificat au collecteur, enregistrez le certificat et la clé dans le répertoire /opt/acnvm/certs.
- Modifiez le propriétaire et le groupe du dossier en acnvm:acnvm avec cette commande :sudo chown -R acnvm:acnvm certs/:
- Cette section pour acnvm.conf doit être configurée avec le certificat et la clé.
- Une fois la configuration et le certificat placés, redémarrez le collecteur :sudo systemctl restart acnvm.service
- Vérifiez l'état du collecteur :sudo systemctl status acnvm.service

```
{
"security" :{
```

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

Voici le reste de la configuration :

```
"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
}
```

- Exécutez le script install.sh avec des privilèges de superutilisateur (sudo ./install.sh).

> Remarque : Le compte a besoin d'autorisations sudo ou root pour exécuter le script install.sh, ainsi que d'autorisations pour le compte de service acnvm.

Pour plus d'informations, référez-vous à Application Cisco Endpoint Security Analytics (CESA) pour Splunk (détails).

Étape 3. Configuration du Splunk avec le tableau de bord CESA et le module complémentaire TA

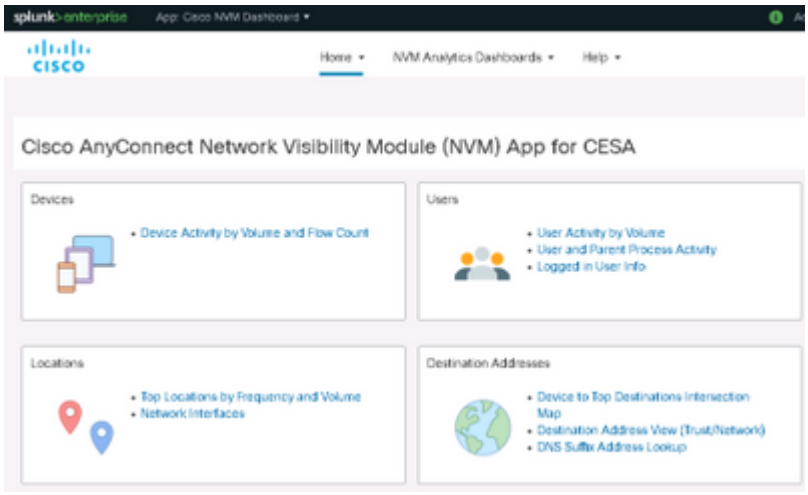
L'application Cisco AnyConnect NVM pour Splunk est disponible sur Splunkbase. Cette application fournit des rapports et des tableaux de bord prédéfinis qui présentent les données IPFIX (nvzFlow) des terminaux dans des rapports utilisables qui permettent de corréler le comportement des utilisateurs et des terminaux.

> Remarque : Pour les déploiements cloud, les deux applications sont installées dans l'instance cloud. Seul le TA est installé sur site (avec le redirecteur). Le collecteur est installé sur site avec le redirecteur ou sur un boîtier Linux/Docker séparé.

Pour une installation sur site, vous pouvez installer tous les composants et applications sur un seul boîtier ou sur des boîtiers distincts. (Reportez-vous aux diagrammes de la section Présentation du déploiement de ce document.)

Téléchargez ces fichiers :

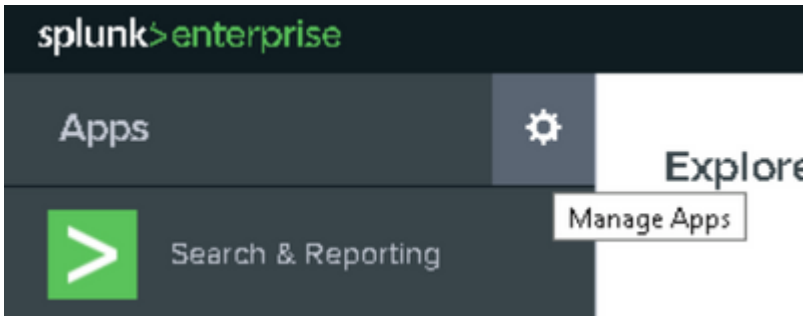
- Application Cisco Endpoint Security Analytics (CESA) pour Splunk



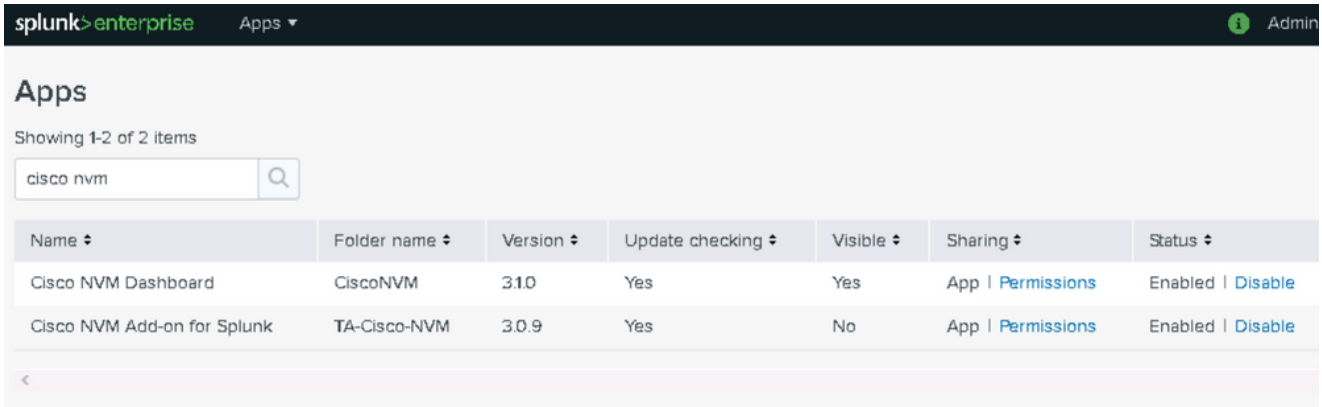
- [Module complémentaire Cisco Endpoint Security Analytics (CESA) pour Splunk]

Install

1. Accédez à Splunk > Apps. Cliquez sur l'engrenage et installez le fichier tar.gz qui a été téléchargé à partir de Splunkbase, ou recherchez dans la section Apps.



2. Installez le module complémentaire avec le même processus.
3. Consultez la page Splunk Apps afin de confirmer que le tableau de bord Cisco NVM et le module complémentaire Cisco NVM pour Splunk sont installés.



La configuration par défaut reçoit trois sources de données pour le Splunk (voir [Activer les entrées UDP via l'interface utilisateur de gestion du Splunk] dans ce document).

- Par flux de données sur le port UDP 20519

- Données d'identité du terminal sur le port UDP 20520
- Données d'interface de terminal sur le port UDP 20521

Le module complémentaire mappe ensuite ces flux de données vers les types de source Splunk cisco : nvm : flowdata, cisco : nvm : sysdata et cisco : nvm : ifdata, respectivement.

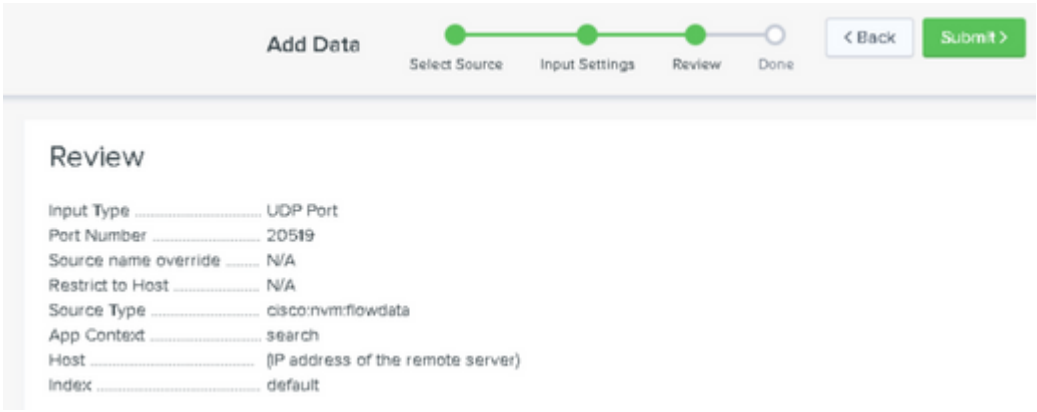
Activer les entrées UDP via l'interface utilisateur de gestion des liaisons

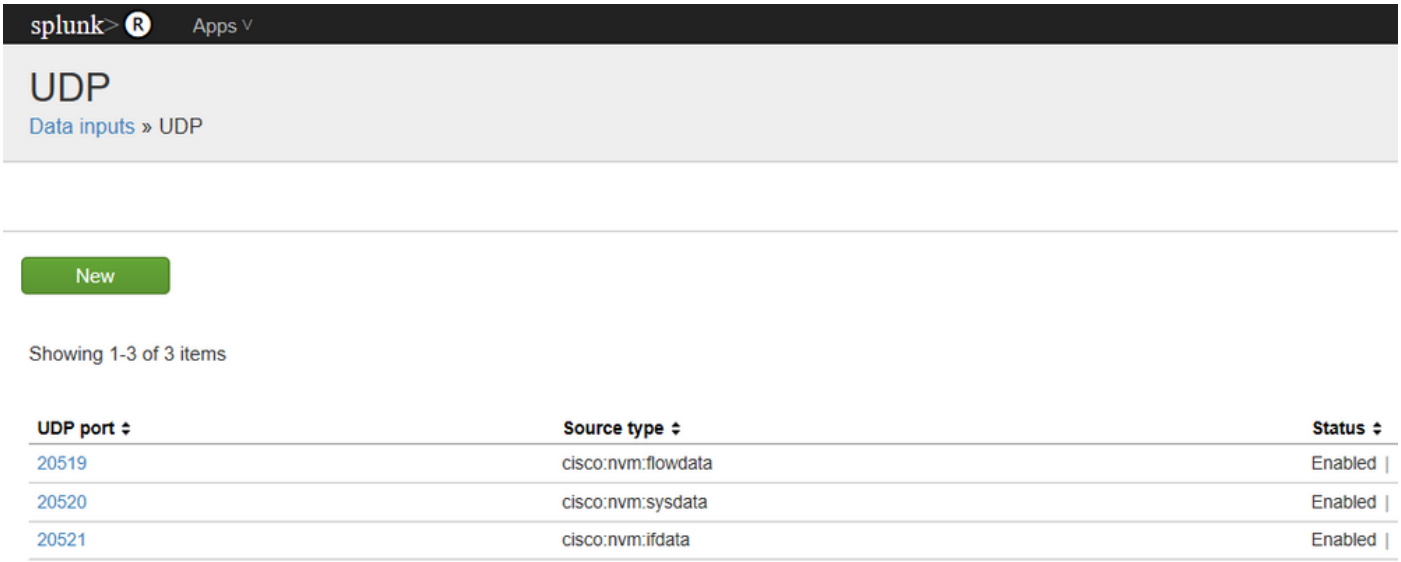
---

Remarque : Vous pouvez également activer les entrées UDP via un fichier input.conf. Cette méthode est expliquée dans l'interface utilisateur graphique de l'application Cisco NVM Dashboard (sous Aide).

Vous n'avez pas besoin de redémarrer le logiciel Splunk.

1. Accédez à Splunk > Settings > Data Input > UDP.
2. Cliquez sur New Local UDP > Enter port # missing > Cliquez sur Next > Sélectionnez le type de source correspondant > Cliquez sur Review > Cliquez sur Submit.
3. Répétez l' pour les deux autres ports. (Vous pouvez utiliser un clone.)

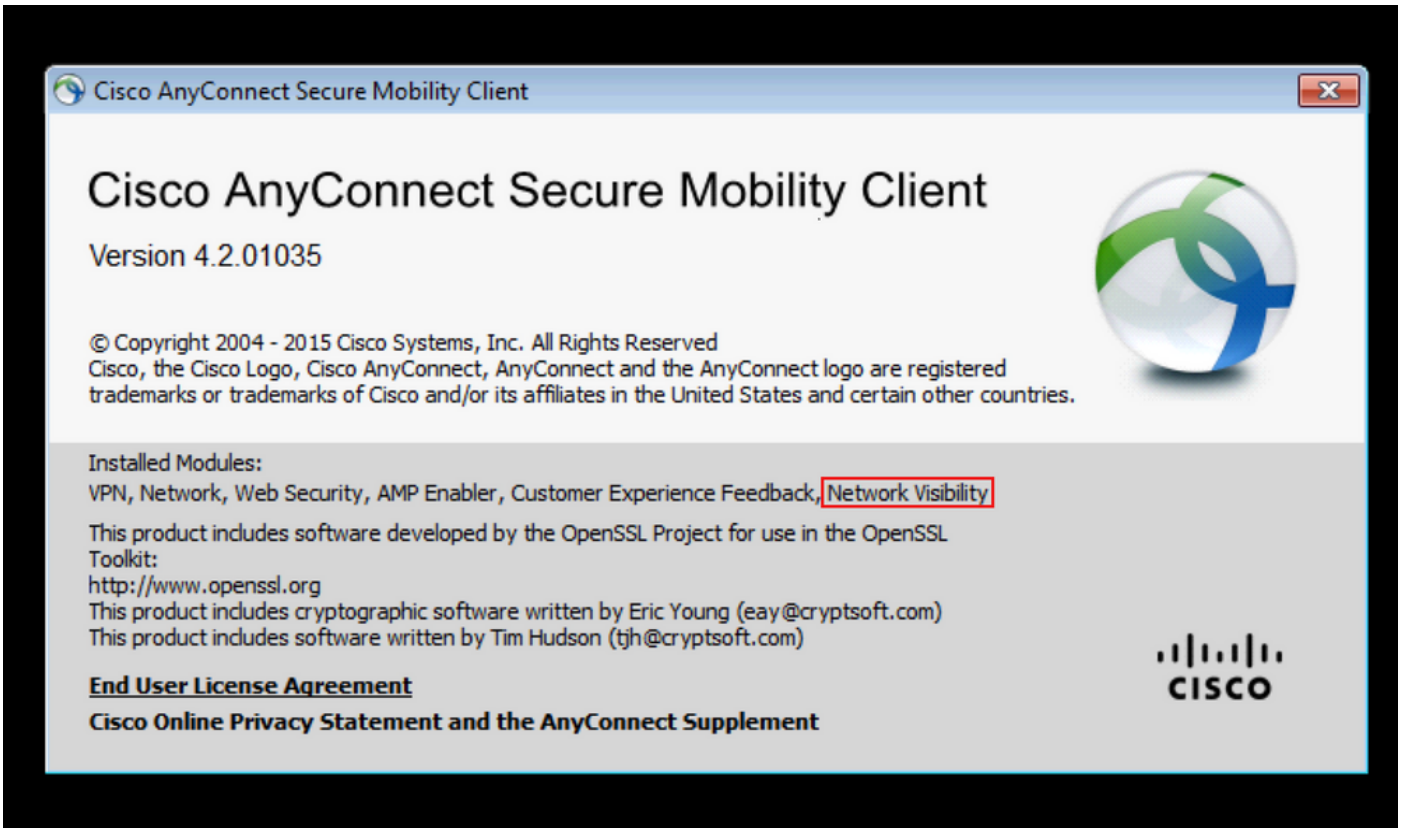




Vérifier

Validation de l'installation AnyConnect NVM

Une fois l'installation terminée, le module de visibilité réseau doit être répertorié dans Modules installés, dans la section Information du client AnyConnect Secure Mobility.



Vérifiez également que le service nvm est en cours d'exécution sur le point d'extrémité et que le profil est présent dans le répertoire requis.

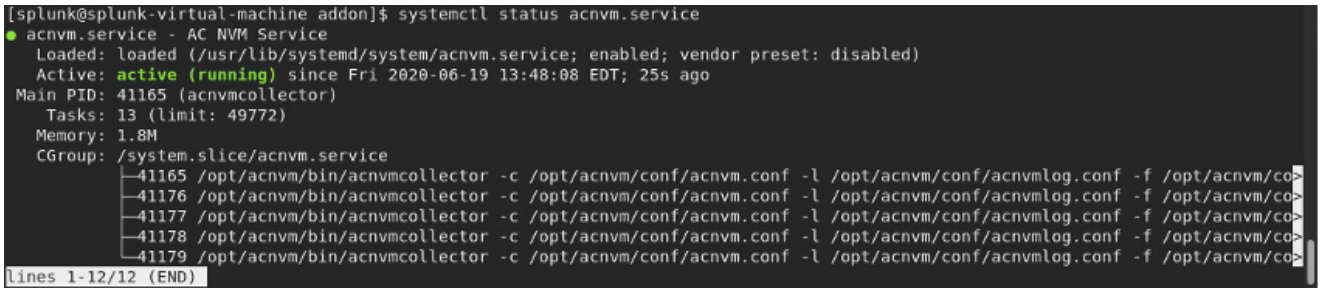
Valider l'état du collecteur

Vérifiez que l'état du collecteur est « actif (en cours d'exécution) ». Cet état garantit que le collecteur reçoit en permanence IPFIX/cflow des points d'extrémité. Si l'état du collecteur n'est pas actif, vérifiez que les autorisations du compte acnvm pour le fichier lui permettent de s'exécuter :

- /opt/acnvm/bin/acnvmcollector

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

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

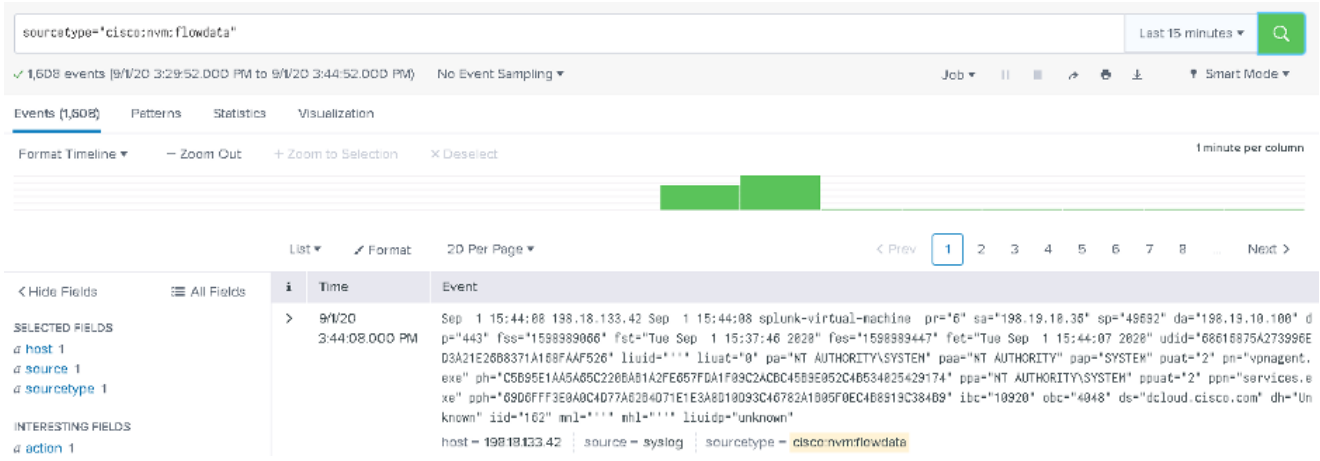


Valider le splunk - Tableau de bord CESA

Assurez-vous que Splunk et ses services pertinents sont en cours d'exécution. Pour obtenir de la documentation sur le dépannage des problèmes Splunk, reportez-vous au site Web Splunk.

Les tableaux de bord de CESA ne sont mis à jour que cinq minutes après la réception des données initiales, en raison d'un script d'automatisation. Cependant, vous pouvez lancer une recherche manuelle immédiatement afin de valider que les données sont reçues :

1. Dans le tableau de bord principal du Splunk, cliquez sur Search & Reporting.
2. Dans l'écran suivant, définissez la plage correcte afin de renseigner les données souhaitées.
3. Dans le champ de recherche, saisissez : sourcetype="cisco:nvm:flowdata"



Après les cinq premières minutes, vérifiez que le tableau de bord CESA reçoit les données :

1. Dans le tableau de bord principal Splunk, cliquez sur Cisco Endpoint Security Analytics Dashboard.
2. Cliquez sur Device Activity by Volume and Flow Count si vous souhaitez conserver les paramètres actuels.
3. Cliquez sur Submit. Le tableau de bord affiche des données et des graphiques.

Flux de paquets

1. Les paquets IPFIX sont générés sur les terminaux clients par le module NVM AnyConnect.

2. Les terminaux clients transmettent les paquets IPFIX à l'adresse IP du collecteur.

3. Le collecteur collecte les informations et les transmet à Splunk.

4. Le collecteur envoie le trafic au Splunk sur trois flux différents : Données par flux, données de point de terminaison et données d'interface.

Tout le trafic est basé sur le protocole UDP, de sorte qu'il n'y a pas d'accusé de réception dans le flux de paquets indiquant que les données ont été reçues.

Ports par défaut pour le trafic :

- Données IPFIX 2055
- Données par flux 20519
- Données de terminal 20520
- Données d'interface 20521

Le module NVM met en cache les données IPFIX et les envoie à un collecteur lorsqu'il se trouve dans un réseau de confiance. Ce comportement se produit lorsque l'ordinateur portable est connecté au réseau de l'entreprise (sur site) ou lorsqu'il est connecté via un VPN.

Vous pouvez vérifier que le collecteur reçoit des paquets du module NVM. Pour ce faire, exécutez une capture de paquets sur des ports UDP spécifiques, selon votre configuration, pour vérifier si les paquets sont reçus. Cette validation serait effectuée via le système d'exploitation Linux Splunk.

Modèles de flux

Les modèles de flux IPFIX sont envoyés au collecteur au début de la communication IPFIX. Ces modèles aident le collecteur à comprendre les données IPFIX.

Le collecteur précharge également les modèles pour s'assurer que les données peuvent être analysées, même si le client n'a pas envoyé les modèles. Si une version plus récente du client est publiée avec des modifications de protocole, le collecteur utilise les nouveaux modèles envoyés par le client.

Un modèle est envoyé dans les conditions suivantes :

1. Le profil du client NVM a été modifié.
2. Il y a un événement de modification du réseau.
3. Le service d'intégration est redémarré.
4. Le point de terminaison est redémarré/redémarré.
5. Périodiquement (par défaut = 24 heures), comme configuré dans le profil NVM.

Dans de rares cas, le collecteur ne trouve pas de modèle. Si cette situation se produit, vous verrez l'un des symptômes suivants :

- Soit aucun modèle trouvé dans une capture de paquets sur le point d'extrémité
- Ou aucun modèle de jeu de flux dans les journaux du collecteur

Afin de résoudre ce problème, redémarrez l'un des points d'extrémité.

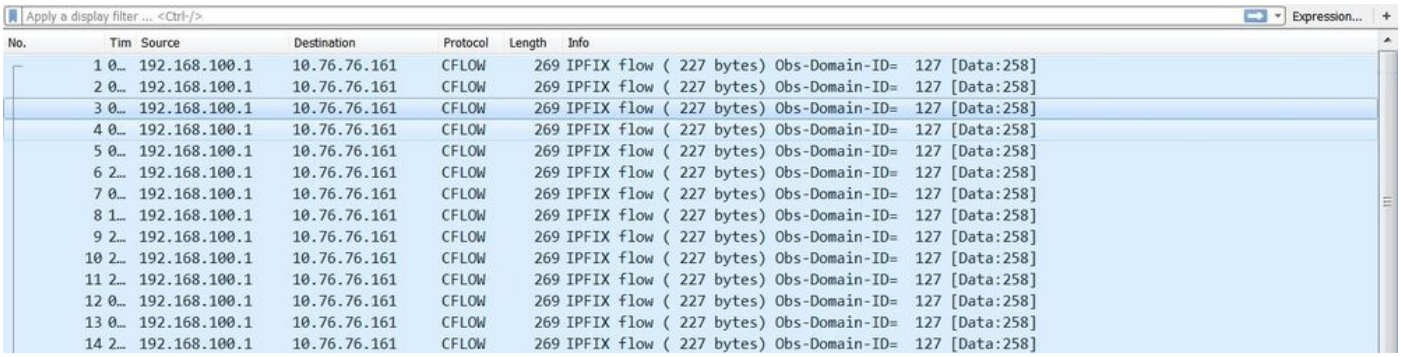
Dépannage

Voici les étapes de base du dépannage :

1. Assurez la connectivité réseau entre le point d'extrémité client et le collecteur.
2. Assurez la connectivité réseau entre le collecteur et le Splunk.
3. Assurez-vous que NVM est correctement installé sur le terminal client.
4. Appliquez des captures sur le terminal pour voir si le trafic IPFIX est généré.
5. Appliquez les captures sur un collecteur pour voir s'il reçoit le trafic IPFIX et s'il transfère le trafic vers le Splunk.
6. Appliquez les captures sur le Splunk pour voir s'il reçoit du trafic.
7. Pour DTLS :
    - Vérifiez que les clients AnyConnect font confiance au certificat du collecteur.
    - Vérifiez que l'option « secure » est activée sur le profil NVM.
    - Vérifiez que le collecteur est configuré pour les certificats.

Trafic IPFIX tel qu'il apparaît dans Wireshark :

Remarque : Si vous exécutez DTLS entre le client et le collecteur, vous devez filtrer le trafic DTLS.

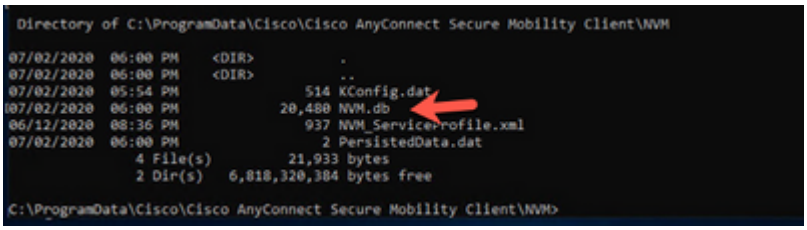


Client AnyConnect (module NVM)

Les données ne sont pas signalées au collecteur et les paquets de données ne sont pas envoyés à partir du terminal

La taille du fichier de base de données NVM (NVM.db) continue-t-elle d'augmenter dans le répertoire C:\%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM ? Ce comportement indique que le client NVM AnyConnect n'envoie pas de paquets de données au collecteur.

Remarque : Pour plus d'informations sur les processus de cache et les contrôles de cache disponibles, référez-vous au Guide de l'administrateur du client Cisco AnyConnect Secure Mobility, version 4.9.



TND (Trusted Network Detection)

Lancez l'interface utilisateur AnyConnect et assurez-vous qu'elle se trouve sur un réseau approuvé. NVM s'appuie sur TND pour détecter si le point d'extrémité se trouve dans un réseau approuvé. Une configuration TND incorrecte entraîne des problèmes avec NVM. NVM possède sa propre configuration TND, qui fonctionne sur l'empreinte de certificat TLS du serveur configuré. Le TND NVM peut être configuré dans l'Éditeur de profil NVM.

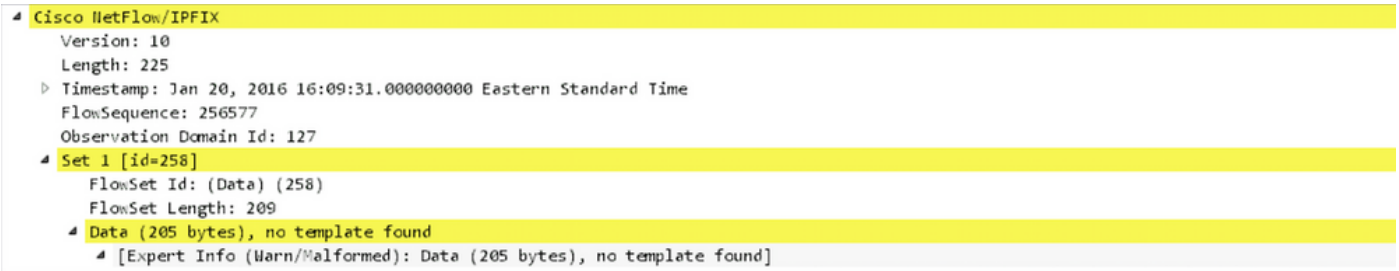
Si NVM TND n'est pas configuré, NVM s'appuie sur la configuration TND du module VPN. Le TND du module VPN fonctionne sur la base des informations reçues via DHCP : nom de domaine et serveur DNS (Domain Name System). Si le serveur DNS et/ou le nom de domaine correspondent aux valeurs configurées, le réseau est considéré comme fiable. VPN prend également en charge la détection TND basée sur les certificats TLS.

- Assurez-vous que la configuration TND est correcte. NVM exporte uniquement lorsqu'il se trouve sur un réseau approuvé.

Remarque : Si la configuration TND est incorrecte, NVM n'exportera pas les données. Par exemple, si trois serveurs DNS sont configurés sur le client, mais que les trois serveurs DNS ne sont pas définis dans la configuration TND, NVM n'exportera pas les données.

- Supprimez le domaine approuvé de la configuration VPN TND.
- Problèmes réseau :
  - Pour la transmission tunnel partagée, incluez toujours l'adresse IP du collecteur dans la configuration « split include » pour le VPN. Si l'adresse IP du collecteur ne fait pas partie de la configuration approuvée du tunnel partagé, les données sont envoyées à l'interface publique.
- Assurez-vous que CollectionMode est configuré pour collecter sur le réseau actuel (approuvé/non approuvé).
- Assurez-vous que les fichiers VPN.xml et NVM_ServiceProfile.xml se trouvent dans les dossiers appropriés ; puis redémarrez.
- Démarrer-arrêter tous les services AnyConnect.
- Renvoi du réseau connecté à l'intérieur qui a une connexion au serveur DNS.

Capture de paquets:



Outils de diagnostic et de création de rapports (DART) AnyConnect

Afin de dépanner les actions AnyConnect, exécutez DART sur les composants NVM. Référez-vous à Dépanner AnyConnect.

- Tous les journaux nécessaires à NVM sont gérés par DART. DART collecte les fichiers journaux, la configuration, etc.
- Journaux Windows : Les événements ne se trouvent pas au même endroit. Il existe un leaf distinct dans l'observateur d'événements pour NVM sous AnyConnect.
- macOS/Linux : Filtrer les journaux par invmagent.

Collecteur (sur une machine Linux/Docker : tout-en-un ou autonome)

Échec de l'installation de acnvmcollector

Lors de l'installation du collecteur et de l'exécution du script d'installation (Sudo ./install_ubuntu.sh),

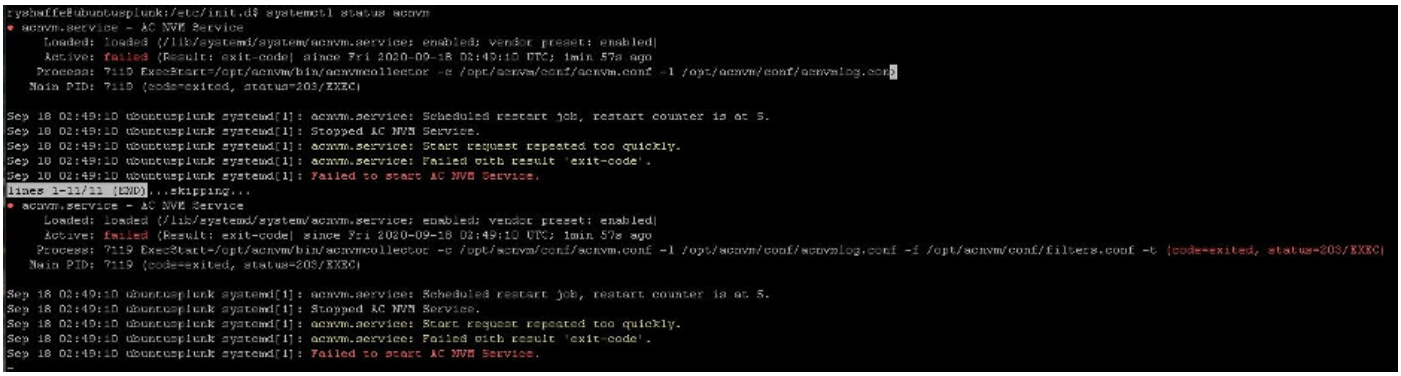
cette erreur se produit dans /var/log/syslog : "Acnvm.conf error: line number 17 : expected key string"

Ce problème peut être causé par une virgule supplémentaire ou par une virgule dans une position non valide.

Échec du démarrage de acnvmcollector

Ce problème était un problème sur Ubuntu (mais peut-être pour tous les Linux). Échec de l'exécution du code sur le fichier acnvmcollector : /opt/acnvm/bin/acnvmcollector.

L'utilisateur et le groupe acvnm n'avaient pas de eXecute pour le collecteur acnvm.



Journaux du collecteur : où puis-je définir le débogage ?

Vous pouvez définir le niveau de journalisation dans le fichier ACMNVMLOG.conf. Le niveau de journalisation fait partie de la configuration qui est envoyée au collecteur au démarrage. Après une modification, redémarrez le collecteur.

log4cplus.rootLogger=DEBUG, STDOUT, NvmFileAppender

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

Comment puis-je trouver le numéro de version du collecteur ?

Afin de trouver la version du collecteur, exécutez la acnvmcollector commande avec l' -vindicateur :

Exemple 1 :

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

Exemple 2 :

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

Sortie :

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

Problèmes DTLS

- Le message « DTLS not configured » signifie que DTLS n'est pas configuré dans le fichier acnvm.conf.
- Le message « server key is invalid » s'affiche lorsqu'une combinaison de clés de mot de passe n'est pas prise en charge.

La console Splunk (tableau de bord CESA) n'affiche pas les données

Client AnyConnect

- Utilisez youtube.com pour générer des données. Vous pouvez également naviguer jusqu'à quelques sites Web.
- Le client AnyConnect peut-il envoyer des informations via UDP 2055 au serveur collecteur ? (En d'autres termes, existe-t-il des pare-feu entre le client AnyConnect et le serveur collecteur ?)
    - Essayez d'établir une connexion Telnet entre l'ordinateur client et l'ordinateur collecteur.
- Exécutez Wireshark pour confirmer que le client envoie des données de trafic (2055 CFLOW) au collecteur.

Boîte Collectrice

- Vérifiez que le boîtier collecteur reçoit le trafic NVM AnyConnect :
    - Effectuez un tcpdump et vérifiez que vous voyez des paquets du client vers le serveur sur 25001 à 2055. Par exemple, cette commande affiche les 100 premiers paquets provenant de l'adresse IP de l'hôte client :`Sudo tcpdump -I any -c100 -nn host 10.1.110.7`

      Remarque : Pour plus d'informations, référez-vous à Comment puis-je capturer tous les paquets UDP en utilisant tcpdump ?
    - Assurez-vous que le collecteur AnyConnect NVM est en cours d'exécution (voir Prise en charge DTLS dans ce document).
    - Recherchez les erreurs de format, les guillemets manquants, les virgules, etc. dans le fichier acnvm.conf.
    - Interface utilisateur Splunk - TA - Les entrées de données UDP et les types de source sont-ils configurés sur l'interface utilisateur graphique Splunk ou via input.conf ?
        - Redémarrez Splunk sous UI > settings > server controls.

Questions courantes (FAQ)

Comment pouvez-vous envoyer des données d'AnyConnect NVM vers plusieurs destinations ?

Ce scénario est utilisé pour les situations de haute disponibilité ou pour l'envoi vers plusieurs plates-formes (par exemple, Splunk et StealthWatch).

Pour plus d'informations, référez-vous à Cisco Endpoint Security Analytics (CESA) Built on Splunk Quickstart POV Kit & Deployment Guide.

Où stockez-vous le certificat pour AnyConnect NVM DTLS ?

Cette situation peut se produire lors de tests de TP où aucun certificat connu n'est installé sur le collecteur.

- Fenêtres: Installez le certificat du collecteur dans les certificats de confiance Windows.
- Mac OSX : Utilisez le processus standard pour installer le certificat racine via la chaîne de clés. Vous pouvez utiliser l'outil de chaîne de clés pour importer le certificat et l'ajouter en tant que certificat approuvé.
- Linux RHEL : Suivez ces étapes d'importation RHEL Root CA :
    1. Copiez le certificat ca dans /etc/pki/ca-trust/source/anchors.
    2. sudo update-ca-trust enable
    3. sudo update-ca-trust extract
- Linux Ubuntu : Suivez ces étapes d'importation de CA racine Ubuntu :
    1. Convertissez le fichier .cer en fichier .crt avec cette commande : openssl x509 -inform PEM -in RootCA.cer -out rootCa.crt
    2. Copiez le fichier .crt dans le répertoire /usr/local/share/ca-certificates.
    3. Exécutez la commande : sudo update-ca-certificates

Noms de fichiers XML

Lorsque vous utilisez l'éditeur de profil local, le nom de profil XML du module VPN principal n'a pas d'importance. Toutefois, vous devez enregistrer le profil de service sous le nom NVM_ServiceProfile.xml. Si vous utilisez un nom différent pour le profil de service, NVM ne parvient pas à collecter et à envoyer des données.

Collecteur (AnyConnect NVM)

Application Cisco Endpoint Security Analytics (CESA) pour Splunk (détails)

- Un répertoire fournisseur peut-il être créé sous la racine, puis la propriété peut-elle être fournie à un autre compte ?

  Vous pouvez d'abord créer /opt/acnvm tant que le script d'installation a l'autorisation d'y copier des fichiers.

- Autorisations de fichier : Le fichier install.sh doit être autorisé à s'exécuter en tant que racine.
- Comptes de service :
  - La useradd -rcommande et la -s /bin/falsecommande sont requises, car un compte de service est un compte non interactif qui n'a pas de répertoire d'accueil.
  - Il n'est pas obligatoire que les comptes non interactifs aient un répertoire de base, et il est d'usage que le compte de service n'ait pas de répertoire de base à garder propre.
  - Tous les utilisateurs ont uid/guid, qu'ils aient ou non un répertoire de base.
- OS du collecteur : Le collecteur s'exécute sur CentOS ou Ubuntu ; il peut également être exécuté sur RedHat, car RedHat utilise le script CentOS.
- Vous pouvez modifier le script d'installation, si nécessaire :
  - Le script d'installation doit être exécuté en tant que root ou avec des droits SUDO parce qu'il crée un nouvel utilisateur appelé acnvm et place tout dans le répertoire /opt/acnvm.

    Remarque : Vous pouvez également créer un script personnalisé pour effectuer les actions appropriées en fonction de vos besoins. Ce script peut utiliser un autre utilisateur qui existe déjà sur le système, mais cet utilisateur doit disposer des droits SUDO pour exécuter l'installation.
- Pour rechercher la version du collecteur, exécutez cette commande avec l'-vindicateur : ./opt/acnvm/bin/acnvmcollector -v

Version recommandée

Nous vous recommandons toujours d'utiliser la dernière version logicielle disponible d'AnyConnect. Pour plus d'informations, référez-vous aux Notes de version pour le client Cisco AnyConnect Secure Mobility v4.x.

Informations connexes

- Cisco Endpoint Security Analytics (CESA) basé sur le kit POV et le guide de déploiement Splunk Quickstart
- Présentation du tableau de bord Cisco Endpoint Security Analytics (CESA) et FAQ
- Application Cisco Endpoint Security Analytics (CESA) pour Splunk
- Application Cisco Endpoint Security Analytics (CESA) pour Splunk (documentation)
- Guides de l'administrateur client pour Cisco AnyConnect Secure Mobility Client v4.x
- Notes de version du client Cisco AnyConnect Secure Mobility v4.x
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.