Configurazione di AnyConnect NVM e Splunk per CESA

Sommario

Introduzione

In questo documento viene descritto come installare e configurare Cisco AnyConnect Network Visibility Module (NVM) su un sistema dell'utente finale con AnyConnect 4.7.x o versioni successive e come installare e configurare i componenti Splunk Enterprise associati e NVM Collector.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- AnyConnect 4.7.x o versioni successive con NVM
- Licenze AnyConnect
- Adaptive Security Device Manager (ASDM) 7.5.1 o versioni successive
- Familiarità con Splunk Enterprise e modalità di installazione di applicazioni e componenti aggiuntivi Splunk

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco AnyConnect Security Mobility Client 4.7.x o versioni successive
- Cisco AnyConnect Profile Editor

- Cisco Adaptive Security Appliance (ASA), versione 9.5.2
- Cisco Adaptive Security Device Manager (ASDM), versione 7.5.1
- Splunk Enterprise 7.x o versione successiva (installato come all-in-one su qualsiasi piattaforma Linux supportata; CentOS (scelta consigliata)
- Qualsiasi installazione Linux supportata come dispositivo di raccolta

> Nota: Un agente di raccolta può essere eseguito sullo stesso server. Per ulteriori informazioni, fare riferimento alla Cisco Endpoint Security Analytics (CESA) basata su Splunk Quickstart POV Kit & Deployment Guide.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

L'NVM di Cisco AnyConnect fornisce un flusso continuo di telemetria di alto valore degli endpoint che consente alle organizzazioni di visualizzare il comportamento degli endpoint e degli utenti sulla propria rete. La tecnologia NVM raccoglie i flussi dagli endpoint on-premise e off-premise, insieme a contesti di valore come utenti, applicazioni, dispositivi, postazioni e destinazioni. Splunk Enterprise utilizza i dati di telemetria e fornisce le funzionalità di analisi e i report.

La presente nota tecnica è un esempio di configurazione per AnyConnect NVM con Splunk Enterprise nell'ambito della nuova soluzione Cisco Endpoint Security Analytics (CESA).

- Per una panoramica completa del POV di CESA con Splunk, fare riferimento alla Cisco Endpoint Security Analytics (CESA) basata su Splunk Quickstart POV Kit e guida all'installazione.
- Per una guida al dashboard NVM CESA su Splunk, fare riferimento alla panoramica del dashboard Cisco Endpoint Security Analytics (CESA) e alle domande frequenti.
- Per ulteriori informazioni sulla soluzione, fare riferimento a Cisco Endpoint Security Analytics Built on Splunk.

Questi componenti costituiscono la soluzione:

- Cisco AnyConnect Secure Mobility Client con Network Visibility Module (NVM) abilitato
- App Cisco Endpoint Security Analytics (CESA) per Splunk
- Modulo aggiuntivo Cisco Endpoint Security Analytics (CESA) per Splunk
- NVM Collector (in bundle con un file zip con l'add-on NVM TA)

Cisco AnyConnect Secure Mobility Client - Più di VPN

Cisco AnyConnect è un agente unificato che fornisce più servizi di sicurezza per proteggere

l'azienda. AnyConnect è comunemente utilizzato come client VPN per aziende, ma supporta anche moduli aggiuntivi che soddisfano diversi aspetti della sicurezza aziendale. I moduli aggiuntivi consentono funzionalità di sicurezza quali la valutazione della postura, la sicurezza Web, la protezione da malware, la visibilità della rete e altro ancora.

La presente nota tecnica riguarda la NVM, che si integra con Cisco AnyConnect per fornire agli amministratori la possibilità di monitorare l'utilizzo delle applicazioni dell'endpoint. Per ulteriori informazioni su Cisco AnyConnect, fare riferimento al manuale Cisco AnyConnect Secure Mobility Client Administrator Guide, versione 4.7.

IPFIX (Internet Protocol Flow Information Export)

IPFIX è un protocollo IETF che definisce uno standard per l'esportazione delle informazioni sul flusso IP per vari scopi, quali contabilità, auditing e sicurezza. IPFIX è basato sul protocollo Cisco NetFlow v9, anche se non sono direttamente compatibili. Cisco nvzFlow è una specifica di protocollo basata sul protocollo IPFIX. Per progettazione, IPFIX è un protocollo estensibile che consente di definire nuovi parametri per trasmettere le informazioni. Il protocollo Cisco nvzFlow estende lo standard IPFIX e definisce nuovi elementi informativi. Il protocollo definisce anche un set standard di modelli IPFIX che vengono trasmessi come parte della telemetria utilizzata dalla NVM di AnyConnect.

Per ulteriori informazioni su IPFIX, fare riferimento alle seguenti RFC:

- rfc 5101
- rfc 701
- rfc 7012
- rfc 7013
- rfc 7014
- rfc 7015

IPFIX NVM Collector

Un agente di raccolta è un server che riceve e memorizza dati IPFIX. Può quindi inviare questi dati a Splunk.

Cisco fornisce un raccoglitore progettato specificamente per il protocollo nvzFlow e viene fornito in bundle con il componente aggiuntivo CESA TA per Splunk. Il raccoglitore può essere installato nella stessa scatola (all-in-one) con il server Splunk, sul server d'inoltro pesante o su una scatola Linux standalone.

Per informazioni più dettagliate sul collector, fare riferimento a Cisco Network Visibility (NVM) Collector.

Splunk Enterprise

Splunk Enterprise è un potente strumento che raccoglie e analizza i dati diagnostici per fornire informazioni utili sull'infrastruttura IT. Fornisce agli amministratori una posizione completa per la

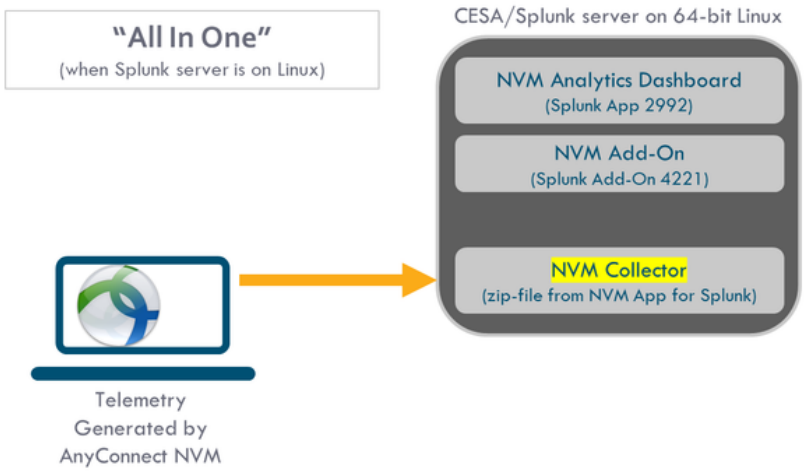
raccolta di dati che consentono di comprendere lo stato della rete.

Splunk è un partner Cisco e la soluzione CESA è stata creata in collaborazione con loro. Per ulteriori informazioni, fare riferimento a Cisco Endpoint Security Analytics Built on Splunk.

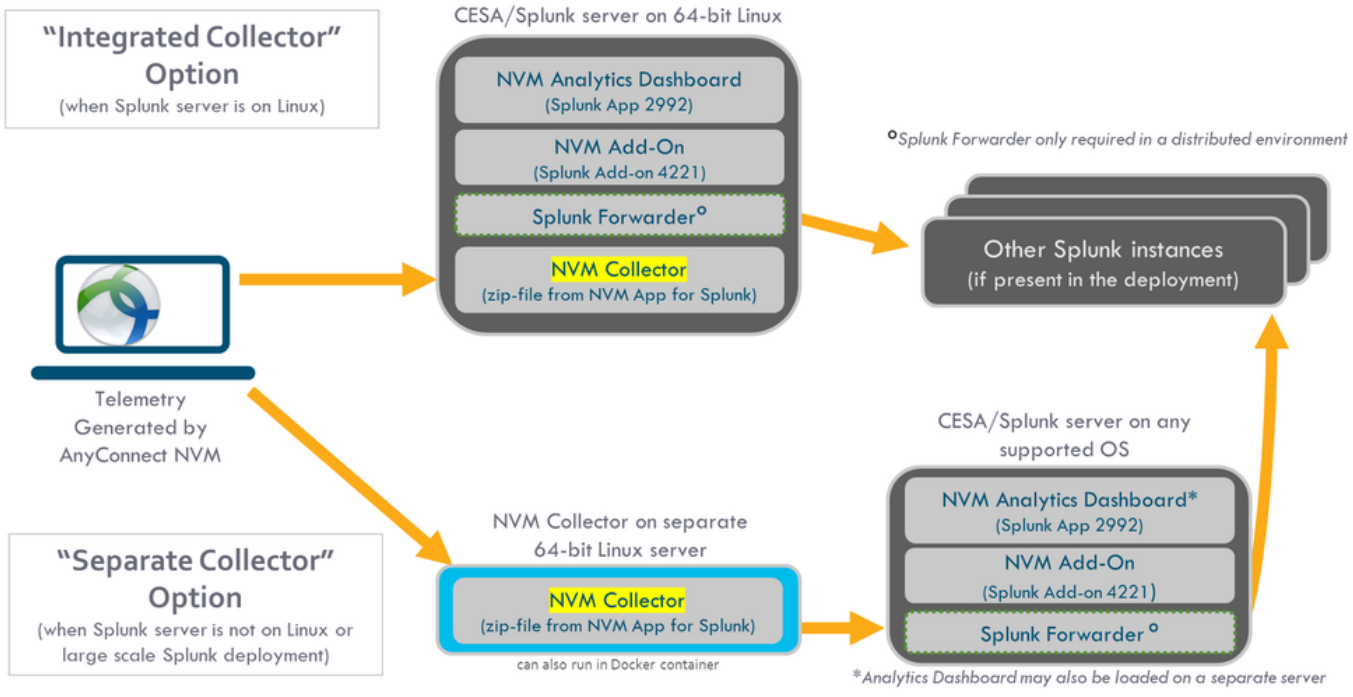
Panoramica della distribuzione

In questo documento viene fornita una panoramica di alto livello della distribuzione nella forma più semplice. Si tratta di una configurazione all-in-one eseguibile su Linux a 64 bit.

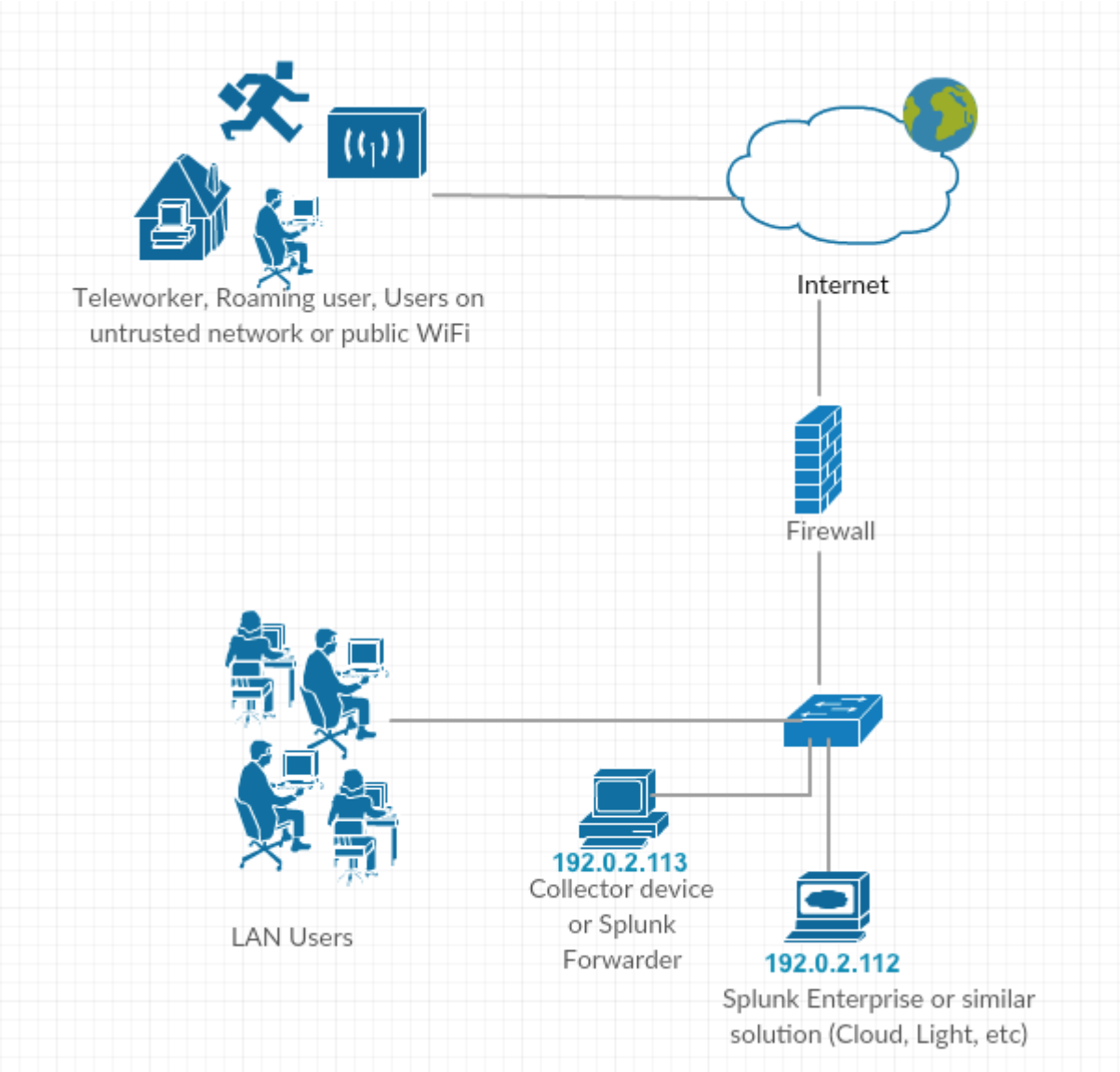
Il diagramma mostra la configurazione utilizzata per la maggior parte delle dimostrazioni. Questa configurazione è utile anche in un'installazione di produzione di piccole dimensioni.



In questo diagramma viene illustrato un insieme più completo di opzioni disponibili per la distribuzione. In genere, un'impostazione di produzione viene distribuita e dispone di diversi nodi Splunk Enterprise.



Topologia



Convenzioni degli indirizzi IP in questa nota tecnica:

- Indirizzo IP agente di raccolta: 192.0.2.123
- Indirizzo IP splunk: 192.0.2.113

Configurazione

In questa sezione viene trattata la configurazione dei componenti NVM di Cisco. Per una panoramica sull'implementazione della NVM di AnyConnect e il profilo di configurazione, consultare anche il documento sull'implementazione del Network Visibility Module di AnyConnect.

Configurazione della NVM per il supporto DTLS

La NVM può ora essere configurata per inviare i dati in modo sicuro al collector tramite DTLS. Questa modalità è configurabile in NVM Profile Editor. Quando la casella di controllo 'Secure' è selezionata, NVM utilizza DTLS come trasporto. Affinché la connessione DTLS possa passare, il

certificato del server DTLS (agente di raccolta) deve essere considerato attendibile dall'endpoint. I certificati non attendibili vengono rifiutati automaticamente. DTLS 1.2 è la versione minima supportata. Per il supporto DTLS è necessario l'agente di raccolta come parte di CESA Splunk App v3.1.2 o versioni successive. Il raccoglitore funziona solo in una modalità: protetta o non protetta.

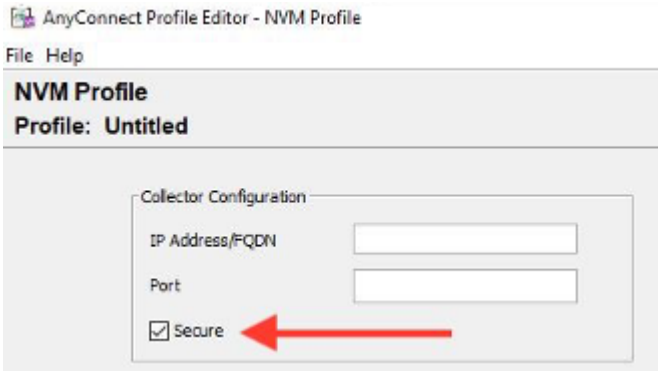
Requisiti dei certificati

- Il certificato agente di raccolta deve essere considerato attendibile dal client. Verificare che la catena di certificati sia attendibile perché non è presente alcuna configurazione in AnyConnect.
- Il certificato deve essere in formato PEM.
- Password della chiave del certificato non supportata. Nota: Per l'Autorità di certificazione (CA) interna di Cisco Identity Services Engine (ISE) è necessaria una licenza.
- È possibile usare qualsiasi certificato sull'agente di raccolta solo se è considerato attendibile dal computer client AnyConnect (infrastruttura a chiave pubblica (PKI) interna, nota e così via).
- Dopo aver aggiornato il file di configurazione, il servizio NVM AnyConnect deve essere riavviato (per test con client singolo). Per i profili push da ISE o da ASA (Adaptive Security Appliance), il computer client deve disconnettersi dalla rete e riconnettersi.

- La configurazione dell'agente di raccolta profili NVM AnyConnect deve essere impostata su IP o FQDN. Questa scelta dipende dal valore utilizzato nel nome comune (CN) del certificato. Il nome di dominio completo (FQDN) è sempre preferito in caso di modifiche all'indirizzo IP.
    - Se si utilizza un indirizzo IP, il CN del certificato del collector o il nome alternativo del soggetto (SAN) deve avere tale IP.
    - Se il nome di dominio completo (FQDN) è il nome di dominio completo (CN) nel certificato, il profilo NVM deve avere lo stesso nome di dominio completo (FQDN) di un agente di raccolta.

Configurazione AnyConnect (4.9.3043 e versioni successive)

Per il profilo NVM, è disponibile una nuova casella di controllo chiamata "Secure" (Sicuro) sotto IP/port collector (IP/porta del collettore).



Modulo NVM AnyConnect standalone

Il modulo standalone richiede AnyConnect 4.8.01090 o versioni successive. Fare riferimento alla Cisco AnyConnect Secure Mobility Client Administrator Guide, versione 4.9. Vedere anche la presente guida standalone: Come implementare AnyConnect Network Visibility Module.

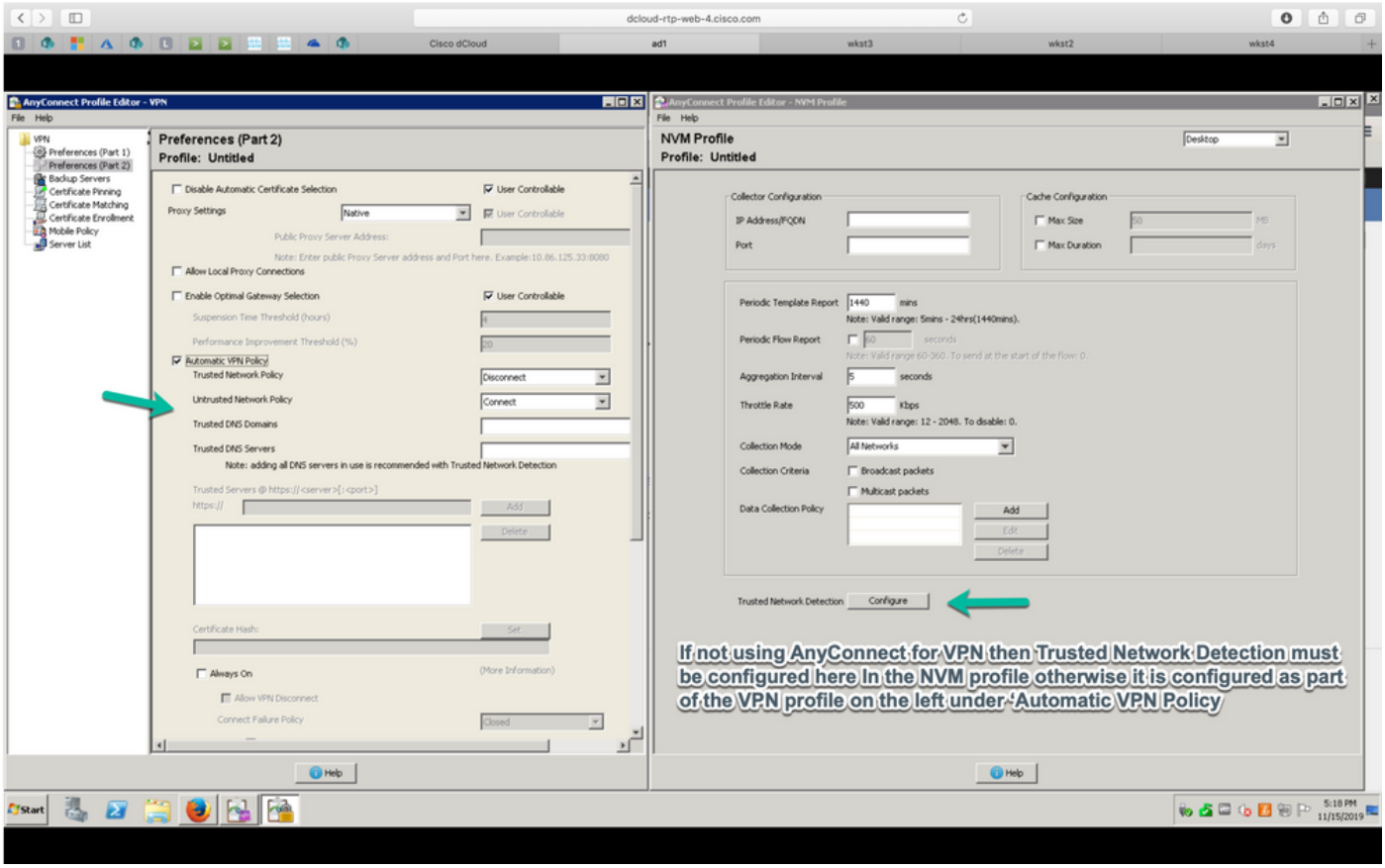
Se non si dispone di un'implementazione AnyConnect o se si utilizza un'altra soluzione VPN, è possibile installare il pacchetto NVM standalone per le proprie esigenze NVM. Questo pacchetto funziona in modo indipendente, ma offre da un endpoint lo stesso livello di raccolta del flusso della soluzione NVM AnyConnect corrente. Se si installa l'NVM standalone, i processi attivi (come Activity Monitor sul sistema operativo Macintosh (macOS)) ne indicano l'utilizzo.

L'NVM standalone è configurato con l'NVM Profile Editor, ed è necessaria la configurazione TND (Trusted Network Detection). La NVM utilizza la configurazione TND per determinare se l'endpoint si trova sulla rete aziendale, quindi applica le policy appropriate.

La risoluzione dei problemi e la registrazione vengono comunque eseguite dagli strumenti di diagnostica e report (DART) di AnyConnect, che possono essere installati dal pacchetto AnyConnect.

Prima della disponibilità dell'opzione standalone, è stato necessario installare il modulo Core VPN per trarre vantaggio da TND. La tessera VPN di base era visibile nell'interfaccia utente, il che potrebbe confondere gli utenti finali, soprattutto se usano una soluzione VPN di un altro fornitore.

Quando si utilizza l'opzione standalone, non si utilizza il profilo VPN di base per configurare TND. Il profilo NVM può ora essere configurato direttamente per TND.



AnyConnect NVM Client Profile

La configurazione di AnyConnect NVM viene salvata in un file XML contenente informazioni sull'indirizzo IP e il numero di porta del collettore, oltre ad altre informazioni. L'indirizzo IP del collector e un numero di porta devono essere configurati correttamente nel profilo del client NVM.

Per il corretto funzionamento del modulo NVM, il file XML deve essere collocato nella seguente directory:

- Per Windows 7 e versioni successive: %ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM
- Per Mac OSX: /opt/cisco/anyconnect/nvm

Se il profilo è presente su Cisco ASA/ISE, viene implementato automaticamente insieme all'implementazione di una NVM di AnyConnect.

Esempio di profilo 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>
```

È possibile creare un profilo NVM con questi strumenti:

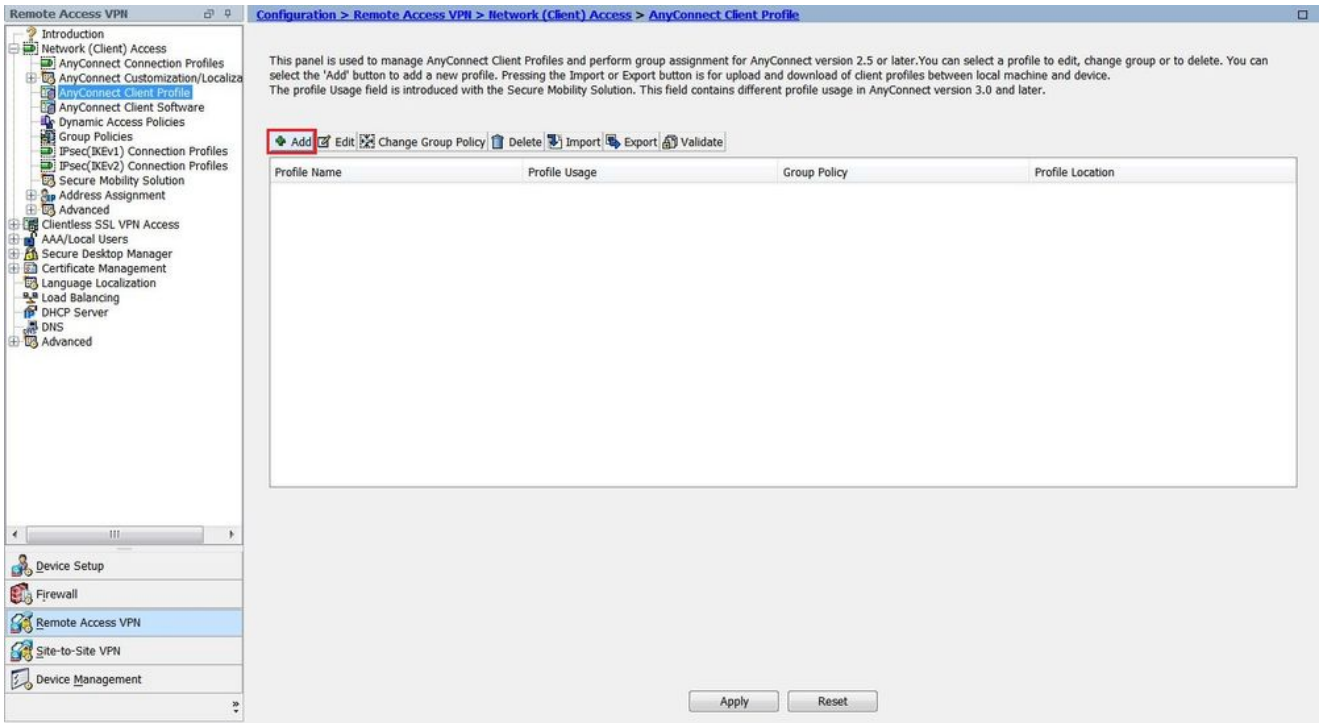
- Cisco ASDM
- Editor profili AnyConnect
- ISE

Configurazione del profilo client NVM tramite ASDM

Questo metodo è da preferire se AnyConnect NVM viene implementato tramite Cisco ASA:

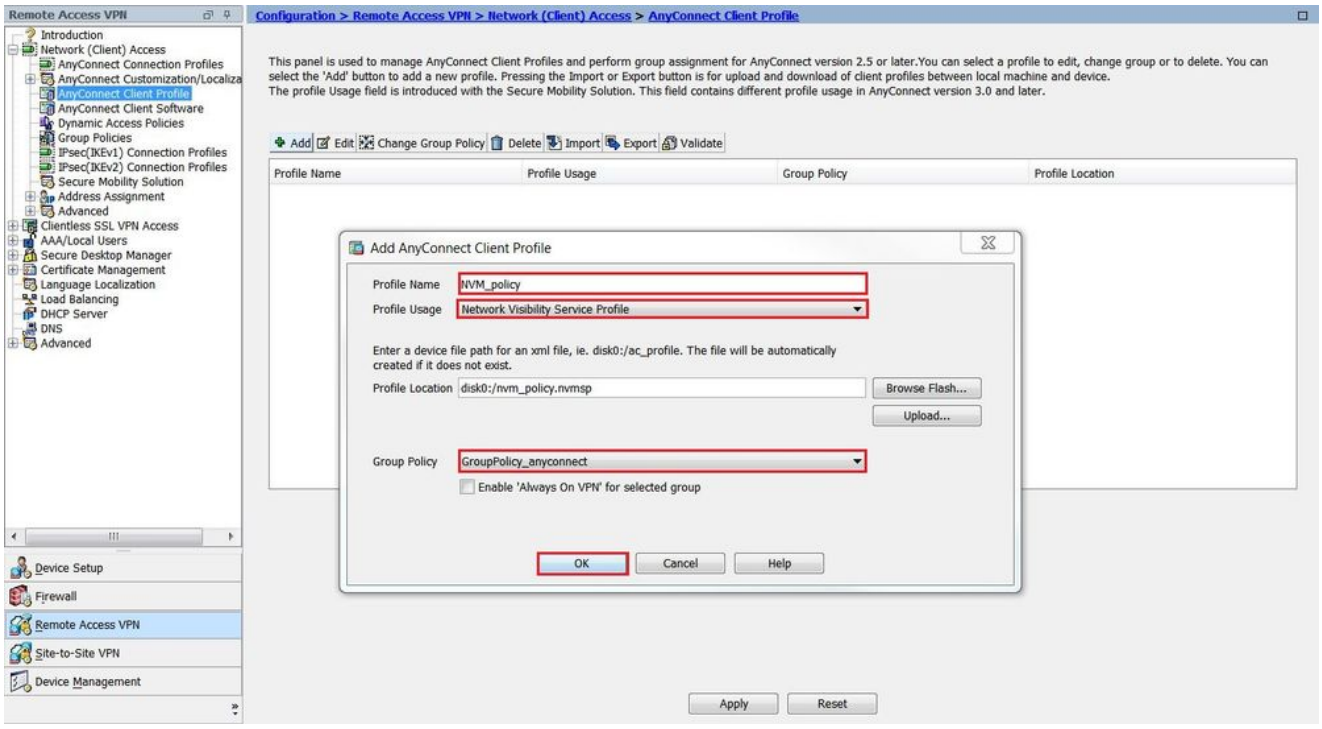
1. Selezionare Configurazione > Rimuovi VPN di accesso > Accesso di rete (client) > Profilo client AnyConnect.

2. Fare clic su Add (Aggiungi), come mostrato nell'immagine.

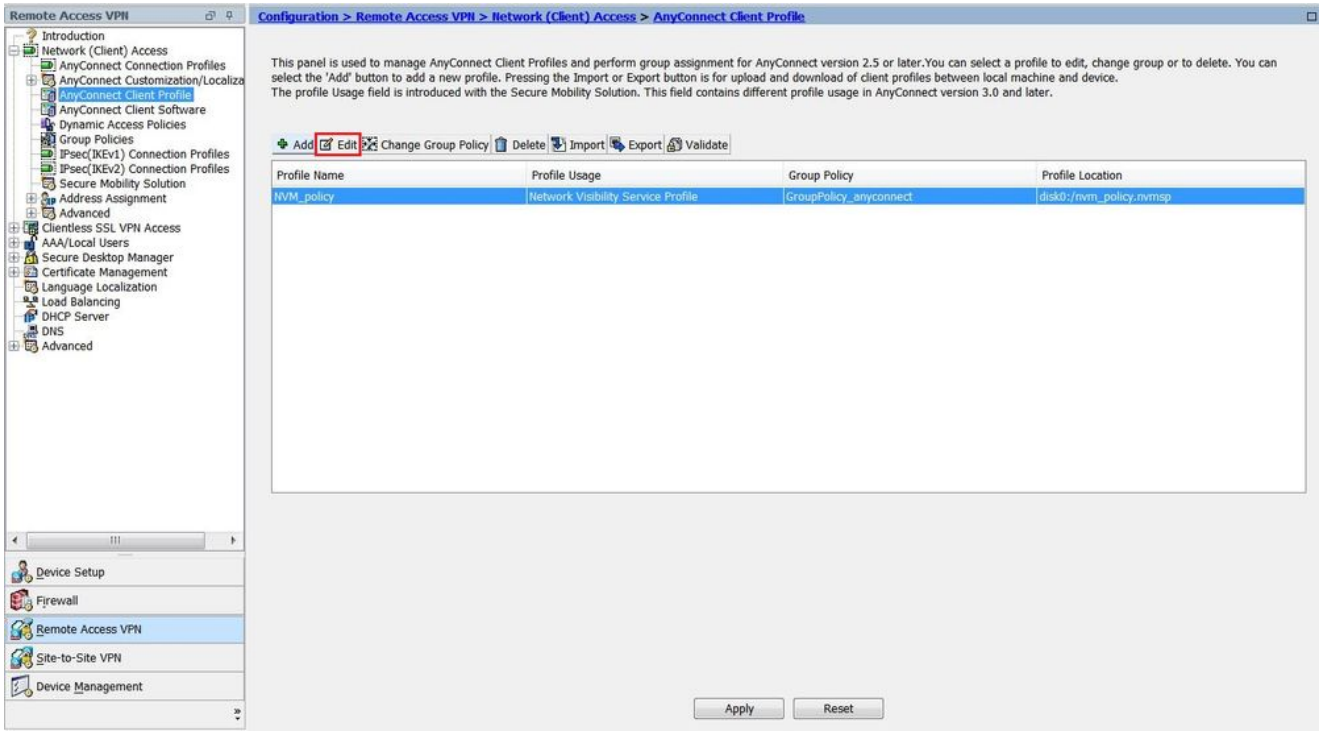


3. Dai un nome al profilo. In Utilizzo profilo, selezionare Profilo Network Visibility Service.

4. Assegnare il profilo ai Criteri di gruppo attualmente utilizzati dagli utenti di AnyConnect e fare clic su OK, come mostrato nell'immagine.

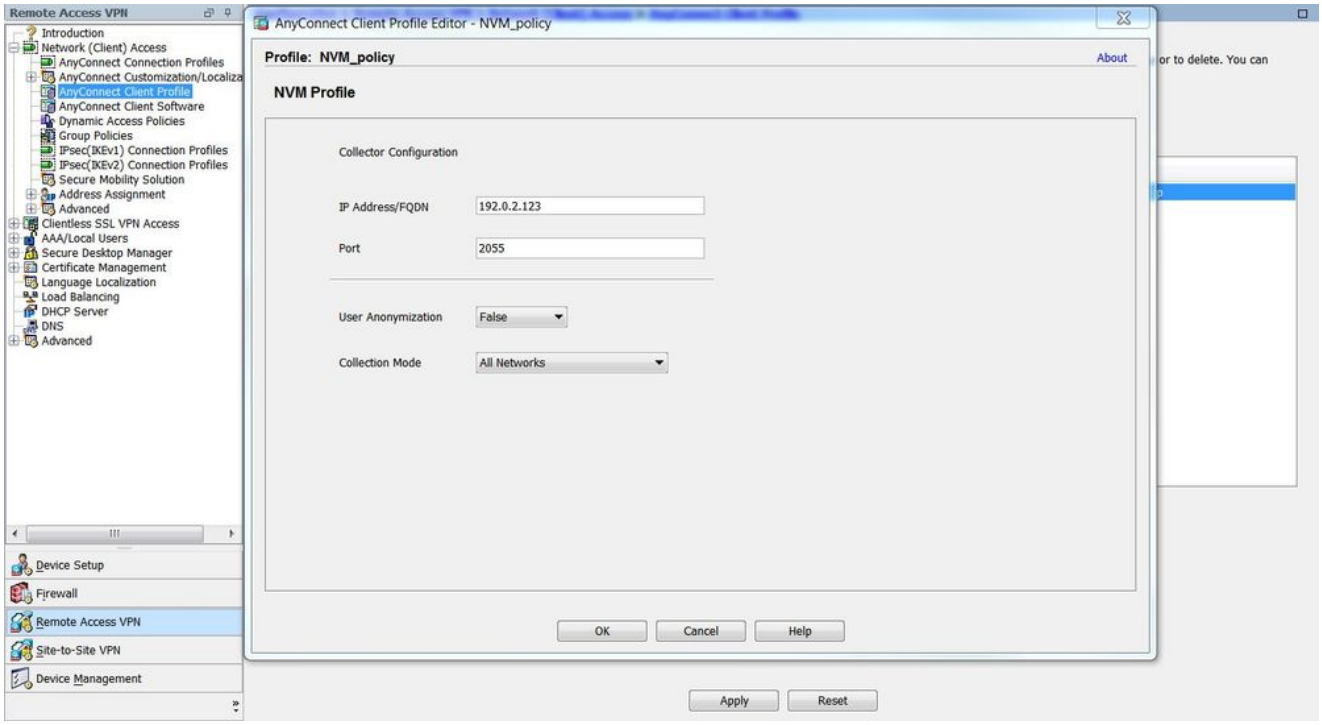


5. Dopo aver creato il nuovo criterio, fare clic su Modifica, come mostrato nell'immagine.



6. Immettere le informazioni relative all'indirizzo IP del collector e al numero di porta; quindi fare clic su OK.

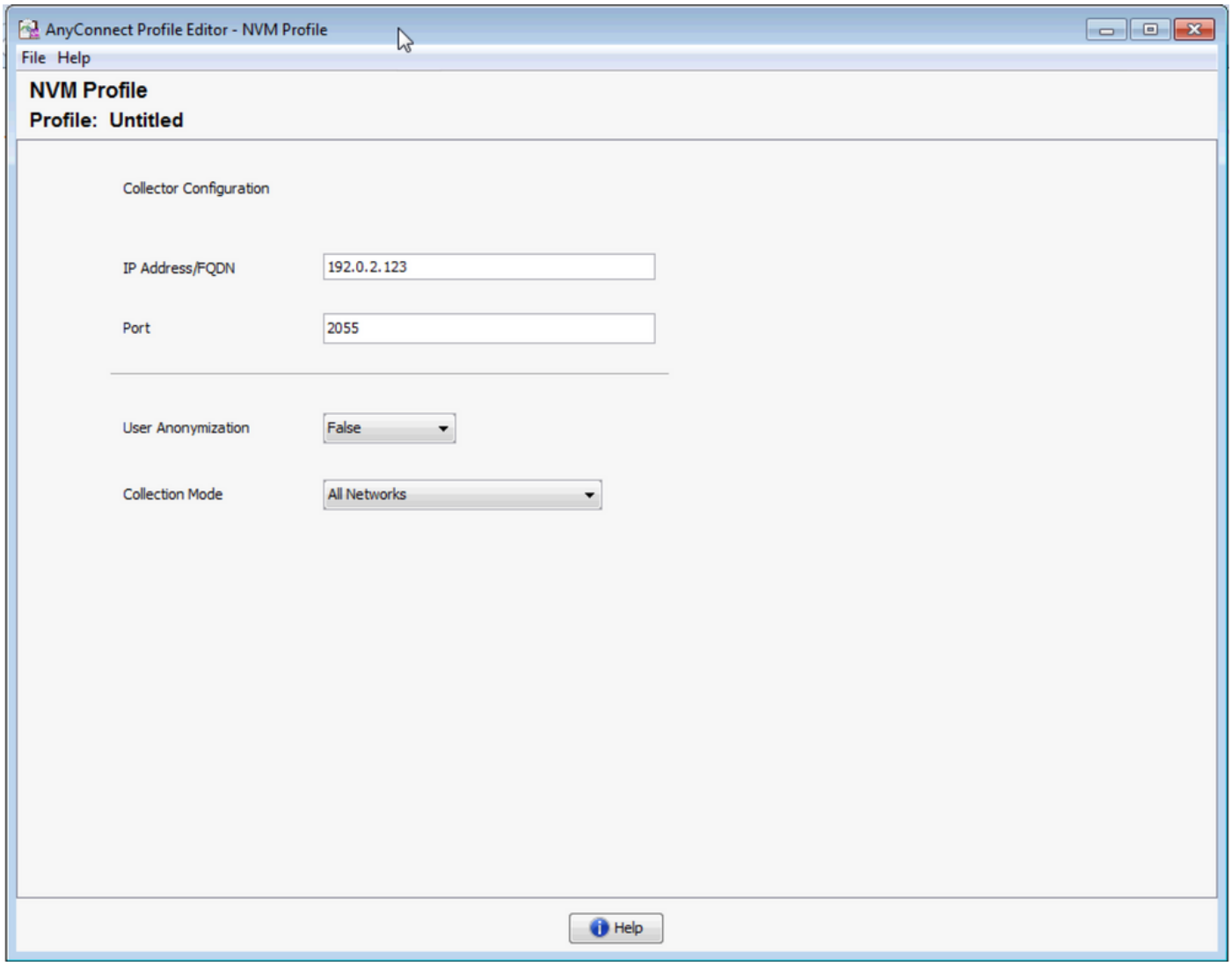
7. Fare clic su Apply (Applica), come mostrato nell'immagine.



Configurazione di NVM Client Profile con AnyConnect Profile Editor

Questo strumento è autonomo ed è disponibile su Cisco.com. Questo metodo è da preferire se AnyConnect NVM viene implementato tramite Cisco ISE. Il profilo NVM creato con questo

strumento può essere caricato in Cisco ISE o copiato direttamente sugli endpoint.



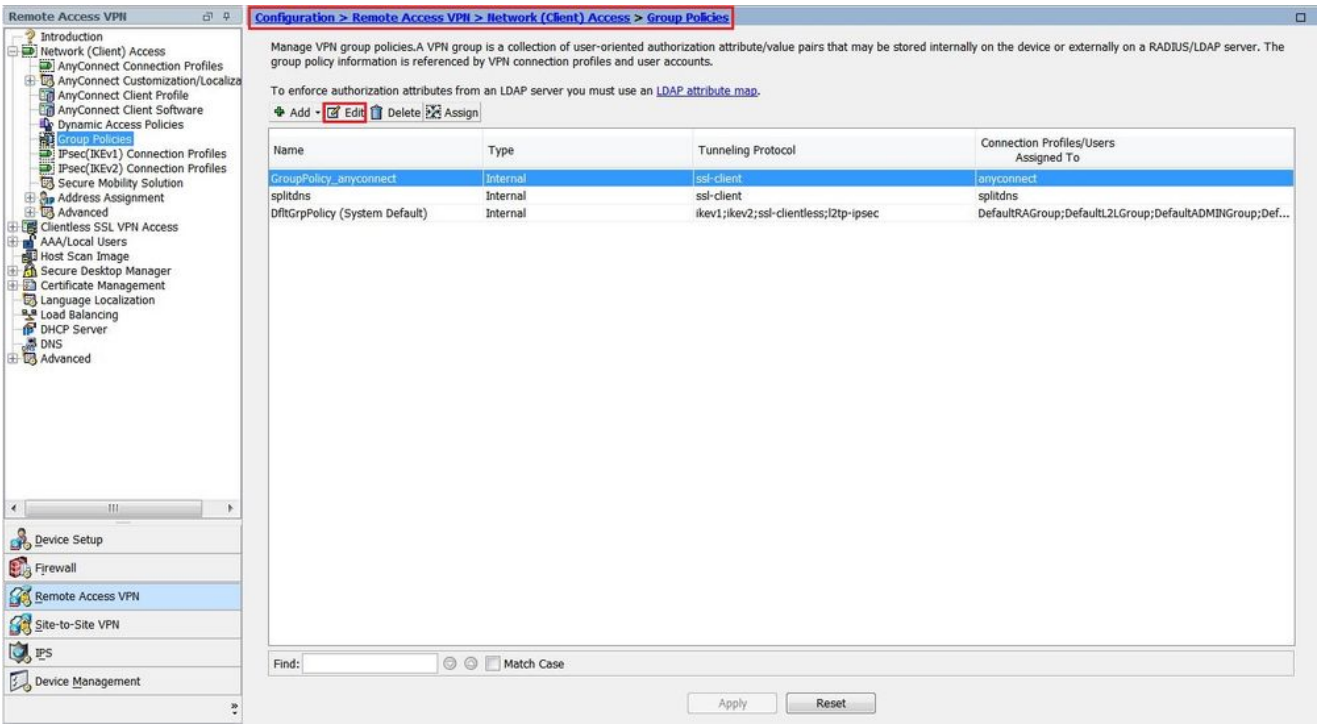
Per informazioni dettagliate sull'Editor di profili AnyConnect, consultare l'Editor di profili AnyConnect.

Configurazione della distribuzione Web su Cisco ASA

In questa nota si presume che AnyConnect sia già configurato sull'appliance ASA e che sia necessario aggiungere solo la configurazione del modulo NVM. Per informazioni dettagliate sulla configurazione di ASA AnyConnect, consultare il documento ASDM 3: Guida alla configurazione di Cisco ASA VPN ASDM, 7.16.

Per abilitare il modulo NVM AnyConnect su Cisco ASA, attenersi alla seguente procedura:

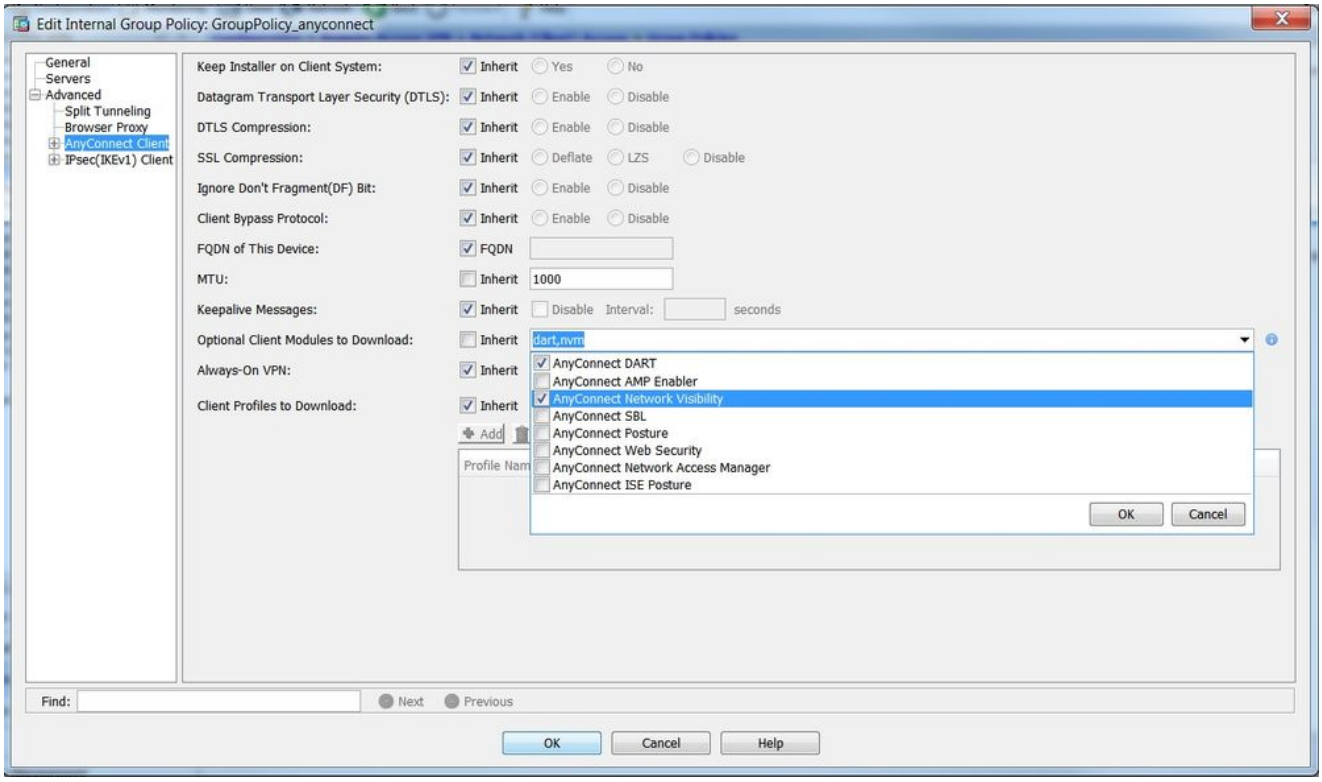
1. Selezionare Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Criteri di gruppo.
2. Selezionare il criterio di gruppo desiderato e fare clic su Modifica, come illustrato nell'immagine.



3. Nel popup di Criteri di gruppo, selezionare Advanced > AnyConnect Client.

4. Espandere Moduli client facoltativi da scaricare e selezionare AnyConnect Network Visibility.

5. Fare clic su OK e applicare le modifiche.

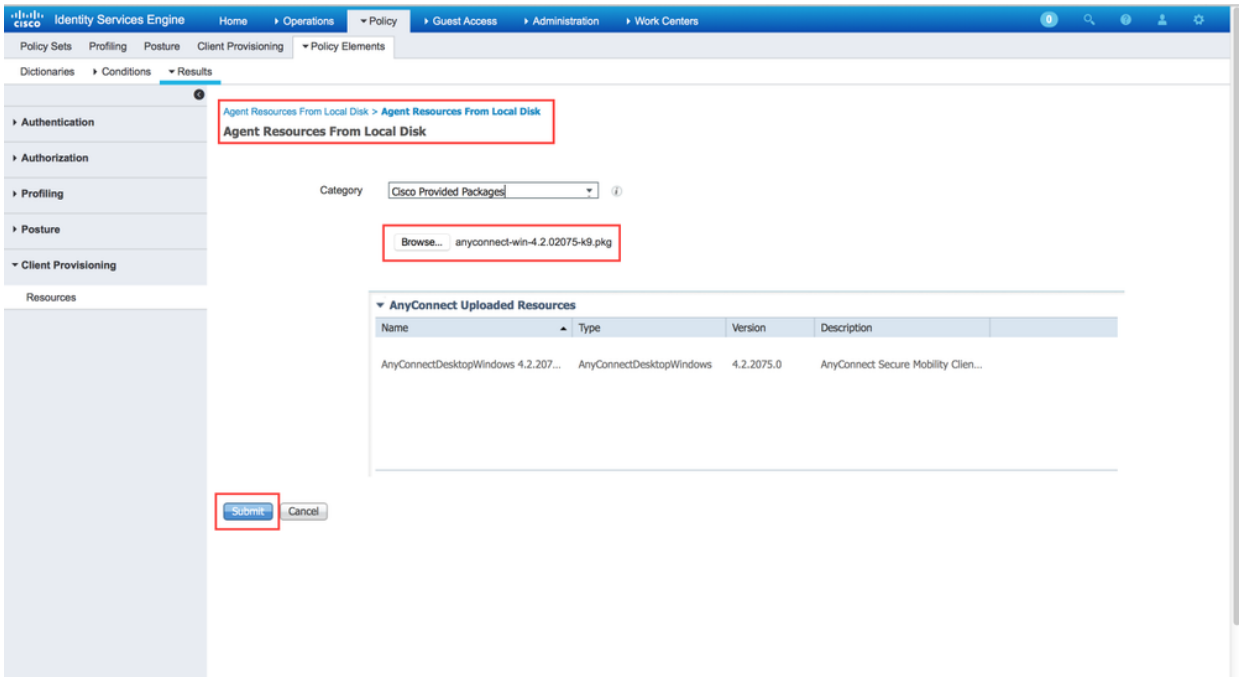


Configurazione della distribuzione Web su Cisco ISE

In questa sezione, abilitiamo i moduli AnyConnect Client, i profili, i pacchetti di personalizzazione/lingua e i pacchetti Opswat.

Per configurare Cisco ISE per la distribuzione Web di AnyConnect, attenersi alla seguente procedura:

1. Nell'interfaccia utente di Cisco ISE, selezionare Policy > Policy Elements > Results (Policy > Elementi della policy > Risultati).
2. Espandere il provisioning client per visualizzare le risorse; quindi selezionare Risorse.
3. Aggiungere l'immagine AnyConnect:
    1. Selezionare Aggiungi > Risorse agente e caricare il file del pacchetto AnyConnect.

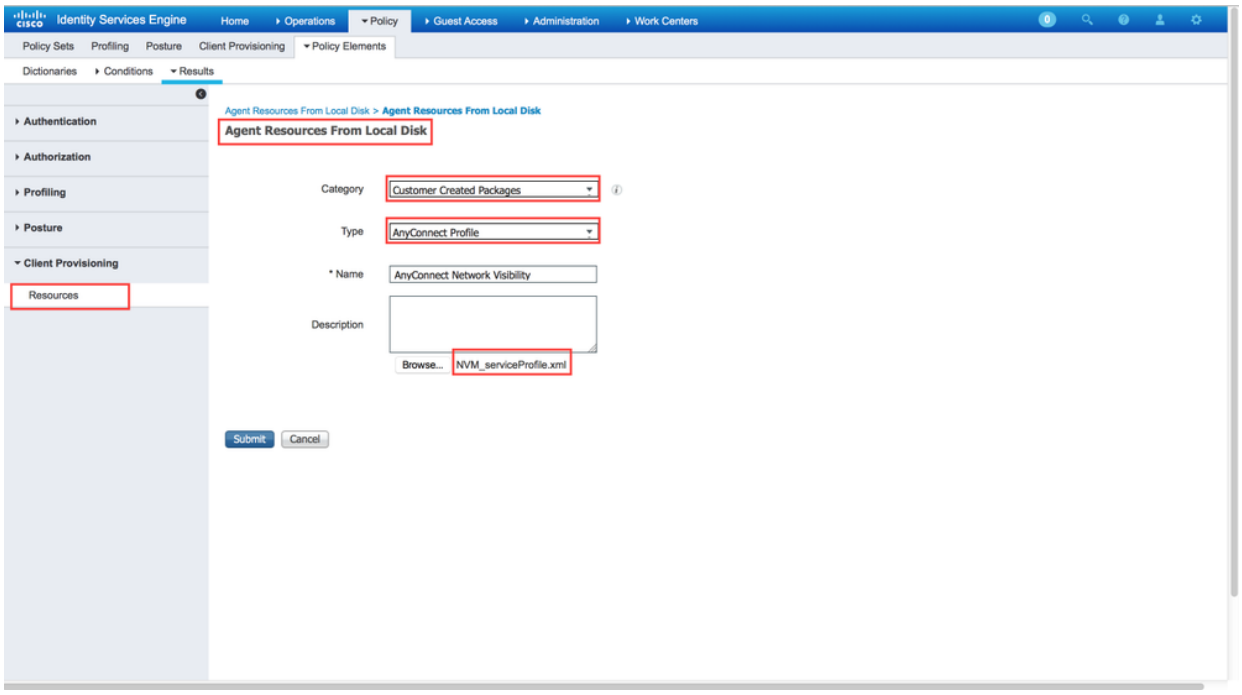


    2. Confermare l'hash del pacchetto nel popup.

        L'hash del file può essere verificato rispetto alla pagina di download Cisco.com o tramite uno strumento di terze parti.

        Questo passaggio può essere ripetuto per aggiungere più immagini AnyConnect (ad esempio, per Mac OSX e Linux OS).

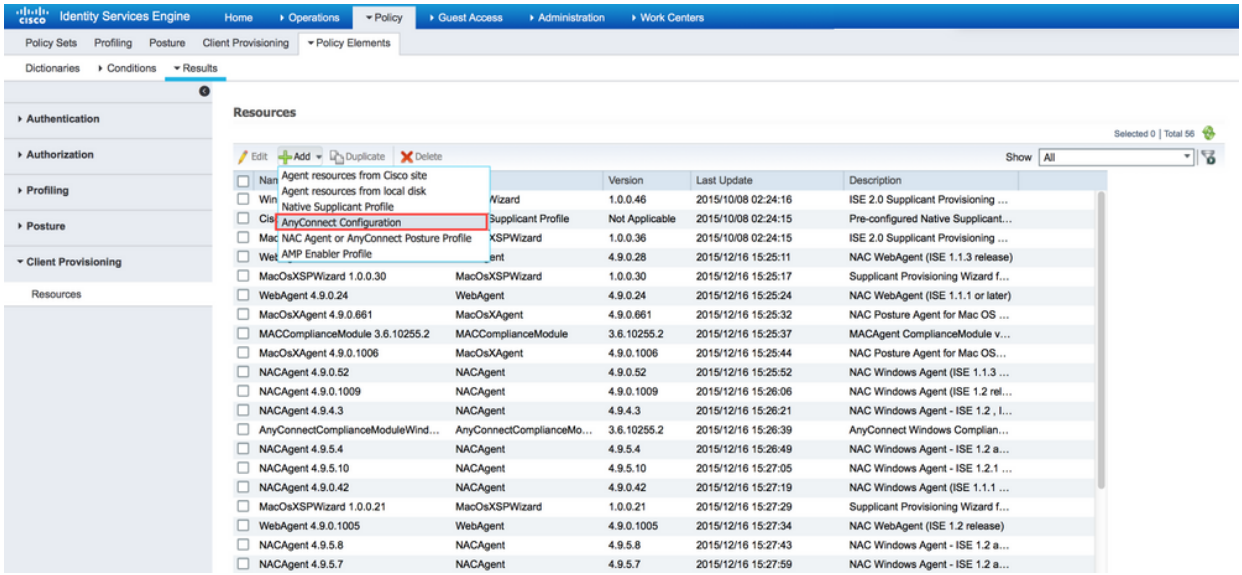
4. Aggiungere il profilo NVM di AnyConnect:
    1. Selezionare Aggiungi > Risorse agente e caricare il profilo client NVM.



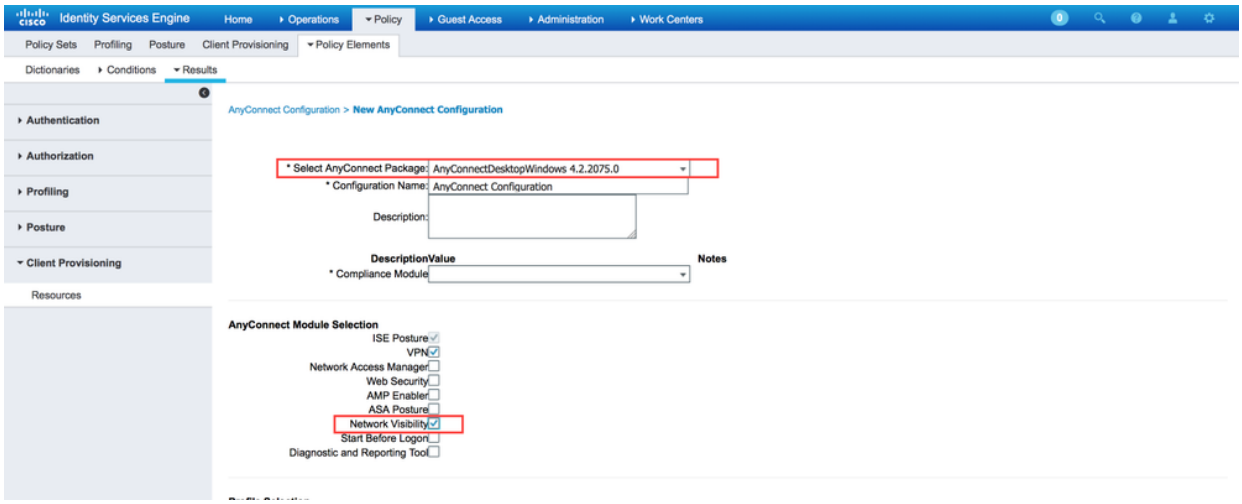
5. Aggiungere il file di configurazione AnyConnect:

    1. Fare clic su Add (Aggiungi), quindi selezionare AnyConnect Configuration (Configurazione AnyConnect).

        Selezionare il pacchetto caricato nel passaggio precedente.



    2. Abilitare NVM nella selezione del modulo AnyConnect e la policy richiesta.

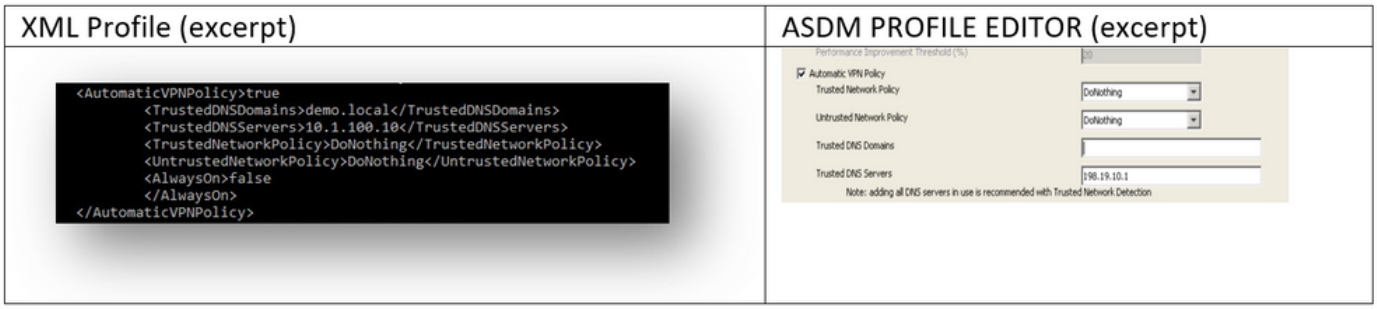


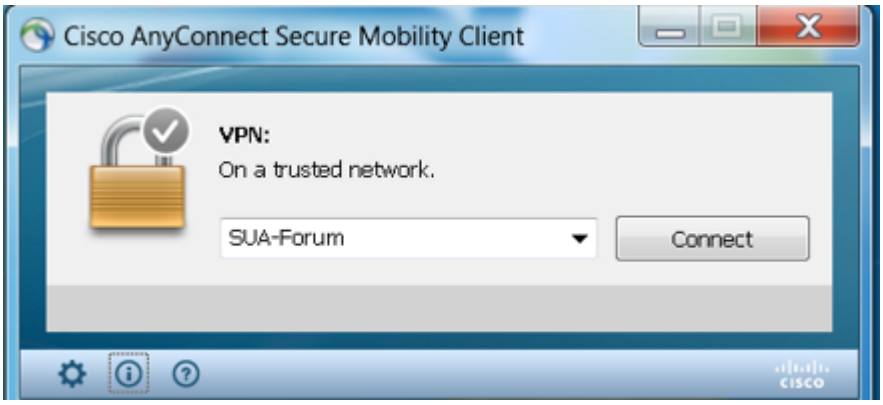
Per informazioni dettagliate sulla configurazione dell'implementazione Web su Cisco ISE, consultare il documento sulla distribuzione Web di AnyConnect.

Rilevamento di reti attendibili

AnyConnect NVM invia le informazioni sul flusso solo quando si trova su una rete attendibile. Utilizza la funzione TND del client AnyConnect per verificare se l'endpoint si trova in una rete attendibile o meno.

Il rilevamento di reti attendibili (TND, Trusted Network Detection) viene configurato nel profilo client AnyConnect (XML) utilizzato per la VPN, indipendentemente dal fatto che il componente VPN sia o meno attualmente utilizzato nell'ambiente. Il TND viene abilitato tramite la configurazione della sezione Criteri VPN automatici nel profilo. È necessario compilare almeno un singolo dominio DNS trusted o un server DNS trusted. Le azioni eseguite da AnyConnect quando il client rileva che si trova su una rete attendibile possono essere impostate sulla modalità DoNothing tramite l'elenco a discesa dei criteri di rete attendibili e non attendibili.





Per ulteriori informazioni sulla configurazione di TND, vedere Informazioni sul rilevamento di reti attendibili.

Implementazione

L'implementazione della soluzione NVM AnyConnect richiede i seguenti passaggi:

1. Configurare AnyConnect NVM su Cisco ASA/ISE.
2. Configurare il componente IPFIX Collector (NVM Collector su Linux - Disponibile nel componente aggiuntivo TA).
3. Configura Splunk con l'app CESA e il componente aggiuntivo TA.

Passaggio 1. Configurazione di AnyConnect NVM su Cisco ASA/ISE

Questo passaggio viene descritto in dettaglio nella sezione Configurazione di questo documento.

Dopo aver configurato NVM su Cisco ISE/ASA, è possibile implementarla automaticamente sugli endpoint client.

Passaggio 2. Configurazione del componente IPFIX Collector (AnyConnect NVM Collector)

Il componente Collector è responsabile della raccolta e della traduzione di tutti i dati IPFIX dagli endpoint e dell'inoltro dei dati al componente aggiuntivo Cisco Endpoint Security Analytics (CESA) per Splunk. L'NVM Collector funziona su Linux a 64 bit. Sono inclusi gli script di configurazione di CentOS, Ubuntu e Docker. Gli script di installazione e i file di configurazione di CentOS possono essere utilizzati anche nelle distribuzioni Fedora e Redhat.

In una tipica distribuzione Splunk Enterprise, il collector deve essere eseguito su un sistema Linux standalone a 64 bit o su un nodo Splunk Forwarder in esecuzione su Linux a 64 bit. Il raccoglitore può inoltre essere installato su un server autonomo senza componenti Splunk.

Nota: La soluzione può anche essere eseguita su un singolo sistema Linux a 64 bit che include i componenti NVM Collector e Splunk Enterprise da utilizzare in piccole installazioni

---

o a scopo dimostrativo. La soluzione all-in-one è più semplice da installare fino a 10.000 endpoint. Per informazioni sul dimensionamento del POV, fare riferimento al POV Real Client.

Come installare Collector

1. Copiare il file acnvmcollector.zip, che si trova nella directory /opt/splunk/etc/apps/TA-Cisco-NVM/appserver/addon/ (inclusa con il componente aggiuntivo TA), nel sistema in cui si desidera installarlo.

2. Decomprimere il file acnvmcollector.zip per estrarre i file.

Si consiglia di leggere il file $PLATFORM$_README nel bundle .zip prima di eseguire lo script install.sh. Il file $PLATFORM$_README fornisce informazioni sulle impostazioni di configurazione rilevanti che devono essere verificate e modificate (se necessario) prima dell'esecuzione dello script install.sh. È necessario configurare almeno l'indirizzo dell'istanza di Splunk a cui si inoltrano i dati. Se non si configura correttamente il sistema, l'agente di raccolta potrebbe non funzionare correttamente.

Nota: Verificare che i firewall di rete e host siano configurati in modo da consentire il traffico UDP per le porte e gli indirizzi di origine e di destinazione. I firewall devono consentire il traffico IPFIX (CFLOW) in arrivo dai client AnyConnect all'agente di raccolta e i dati UDP in uscita da Splunk.

Una singola istanza del collector NVM può gestire un minimo di 5000 flussi al secondo su un sistema di dimensioni appropriate, o fino a 35.000-40.000 endpoint. L'agente di raccolta deve essere configurato e in esecuzione prima di poter utilizzare la NVM Splunk e l'app TA-Add on.

Per impostazione predefinita, l'agente di raccolta riceve i flussi dagli endpoint NVM di AnyConnect sulla porta UDP 2055.

Inoltre, il raccoglitore genera tre feed di dati per Splunk:

- Dati per flusso sulla porta UDP 20519
- Dati identità endpoint sulla porta UDP 20520
- Dati interfaccia endpoint sulla porta UDP 20521

È possibile modificare le porte di ricezione e di feed dei dati. A tale scopo, modificare il file acnvm.conf e riavviare l'istanza del raccoglitore. Verificare che tutti i firewall host/di rete tra gli endpoint e l'agente di raccolta o tra l'agente di raccolta e i sistemi Splunk siano aperti per le porte e gli indirizzi UDP configurati. Inoltre, verificare che la configurazione della NVM AnyConnect corrisponda alla configurazione del collector.

Dopo l'installazione e l'esecuzione di tutti i componenti, fare riferimento alla sezione dei file della Guida dall'applicazione Splunk per informazioni dettagliate sui report preconfigurati, sul modello di dati e sugli elementi informativi creati dalla soluzione.

È possibile riavviare uno degli endpoint AnyConnect e verificare che il traffico venga inviato alla soluzione. Ad esempio, è possibile utilizzare youtube.com per eseguire un flusso di dati costante.

Queste informazioni devono essere configurate nel file di configurazione acnvm.conf:

- syslog_server_ip (server d'inoltro o istanza Splunk): È possibile puntare a 127.0.0.1 (non utilizzare LOCALHOST) se si trova sulla stessa scatola.
- Porta di ascolto per l'agente di raccolta (dati IPFIX in ingresso): Il valore predefinito è okay.

Nota: netflow_collector_ip è omesso dal file di configurazione. Utilizza l'interfaccia pubblica predefinita e deve essere modificata solo per sostituire il valore predefinito con un indirizzo IP locale specifico.

Le porte Dati per flusso, Dati identità endpoint, Dati interfaccia endpoint e Porta agente di raccolta sono preconfigurate per le impostazioni predefinite nel file di configurazione. Se si utilizzano porte non predefinite, è necessario modificare questi valori.

Queste informazioni vengono aggiunte nel file di configurazione: /opt/acnvm/conf/acnvm.conf

Supporto DTLS

Nota: Per ulteriori informazioni, vedere Configurare NVM per il supporto DTLS in questo documento.

Attenersi alla seguente procedura nella casella che ospita l'agente di raccolta:

- Crea questa directory: /opt/acnvm/certs.
- Per applicare il certificato all'agente di raccolta, salvare il certificato e la chiave nella directory /opt/acnvm/certs.
- Modificare il proprietario e il gruppo della cartella in acnvm:acnvm con questo comando:sudo chown -R acnvm:acnvm certs/:
- Questa sezione per acnvm.conf deve essere configurata con il certificato e la chiave.
- Dopo aver inserito la configurazione e il certificato, riavviare l'agente di raccolta:sudo systemctl restart acnvm.service
- Controllare lo stato dell'agente di raccolta:sudo systemctl status acnvm.service

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

Di seguito è riportata la parte restante della configurazione:

```
"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
}
```

- Eseguire lo script install.sh con privilegi di utente avanzato (sudo ./install.sh).

> Nota: Per eseguire lo script install.sh e le autorizzazioni per l'account del servizio acnvm sono necessarie le autorizzazioni sudo per l'account root.

Per ulteriori informazioni, fare riferimento all'app Cisco Endpoint Security Analytics (CESA) per Splunk (dettagli).

Passaggio 3. Configurare Splunk con il dashboard CESA e il componente aggiuntivo TA

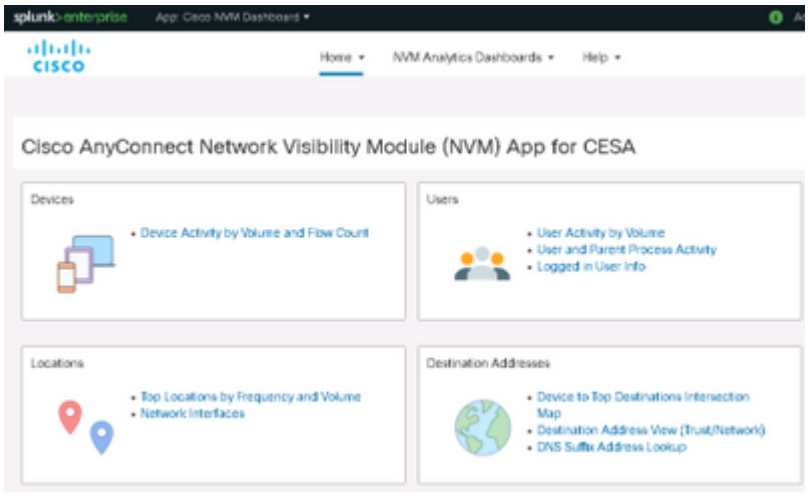
L'app Cisco AnyConnect NVM per Splunk è disponibile su Splunkbase. Questa app fornisce report e dashboard predefiniti che presentano dati IPFIX (nvzFlow) dagli endpoint in report utilizzabili che aiutano a correlare il comportamento di utenti ed endpoint.

> Nota: Per le distribuzioni cloud, entrambe le app sono installate nell'istanza cloud. Solo la scheda è installata in sede (con il server d'inoltro). Il raccoglitore viene installato in sede con il server d'inoltro o su una scatola Linux/Docker separata.

Per un'installazione in sede, è possibile installare tutti i componenti e le app in un'unica scatola o in caselle separate. Vedere i diagrammi nella sezione Panoramica distribuzione di questo documento.

Scarica i seguenti file:

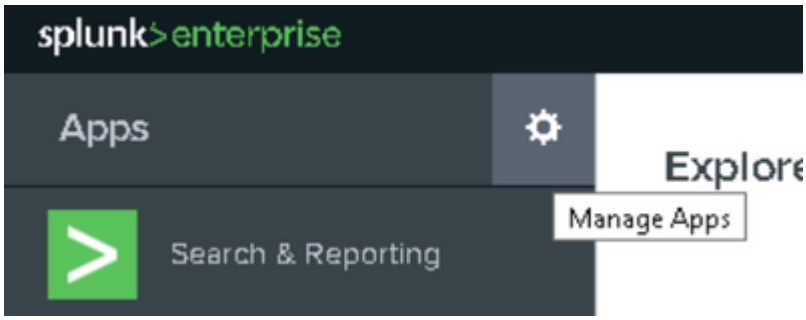
- App Cisco Endpoint Security Analytics (CESA) per Splunk



- [Modulo aggiuntivo Cisco Endpoint Security Analytics (CESA) per Splunk]

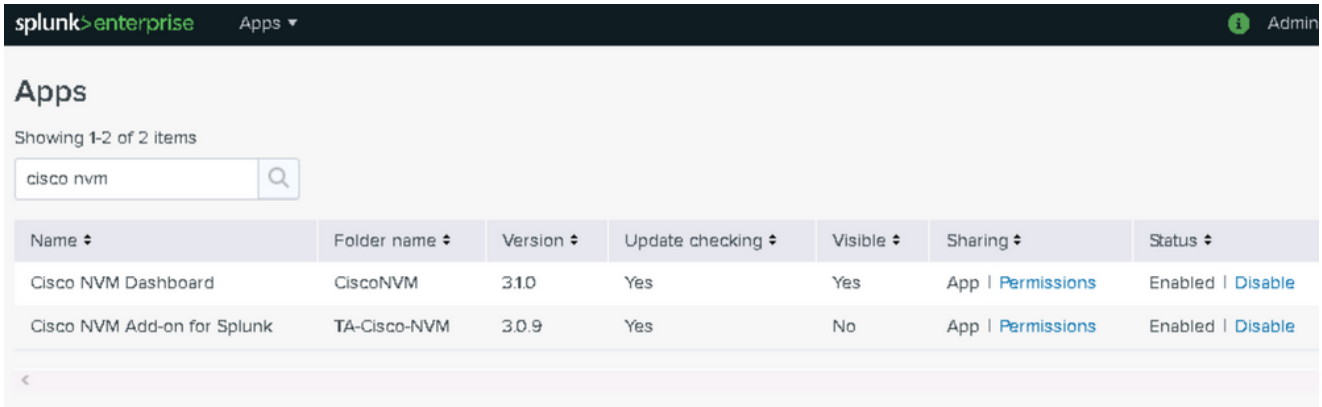
Install

1. Passare a Splunk > App. Fare clic sull'ingranaggio e installare il file tar.gz scaricato da Splunkbase oppure eseguire una ricerca all'interno della sezione Apps.



2. Installare il componente aggiuntivo con lo stesso processo.

3. Visualizzare la pagina Splunk Apps per confermare che siano installati sia il Cisco NVM Dashboard che il Cisco NVM Add-On per Splunk.



La configurazione predefinita riceve tre feed di dati per Splunk (vedere [Abilitare gli input UDP tramite l'interfaccia utente di gestione di Splunk] in questo documento).

- Per Flusso di dati sulla porta UDP 20519

- Dati identità endpoint sulla porta UDP 20520
- Dati interfaccia endpoint sulla porta UDP 20521

Il componente aggiuntivo esegue quindi il mapping di questi feed di dati a Splunk, rispettivamente ai tipi di origine cisco:nvm:flowdata, cisco:nvm:sysdata e cisco:nvm:ifdata.

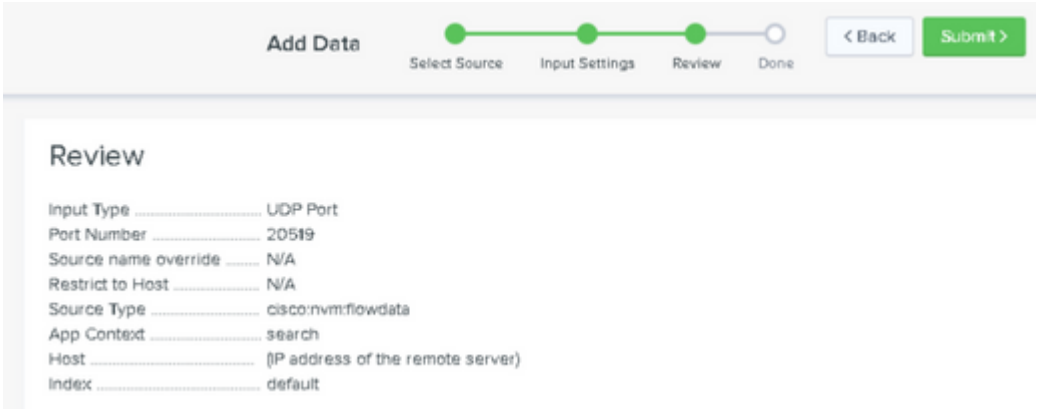
Abilitare gli input UDP tramite l'interfaccia utente di gestione dello splunk

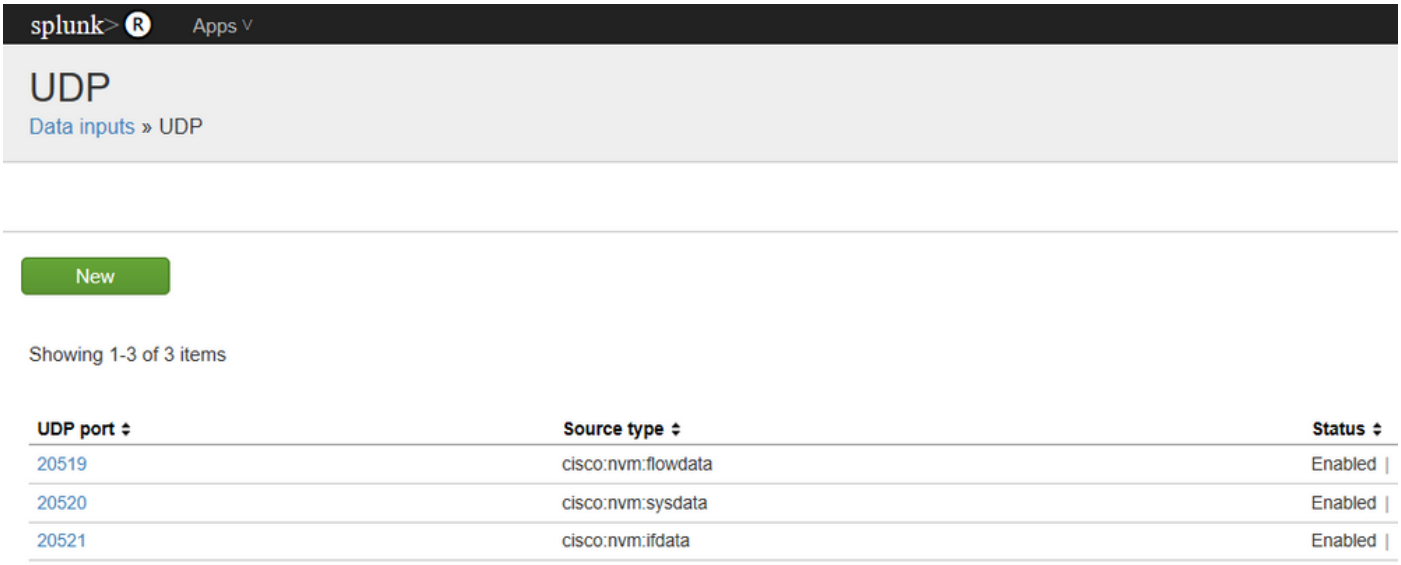
---

Nota: È inoltre possibile abilitare gli ingressi UDP tramite un file input.conf. Questo metodo è spiegato nell'interfaccia utente dell'app Cisco NVM Dashboard (sotto Guida).

Non è necessario riavviare il software Splunk.

1. Passare a Splunk > Impostazioni > Input dati > UDP.
2. Fare clic su New Local UDP > Enter port # missing > Fare clic su Next > Selezionare il tipo di origine corrispondente > Fare clic su Review > Fare clic su Submit.
3. Ripetere l'operazione per le altre due porte. È possibile utilizzare un clone.

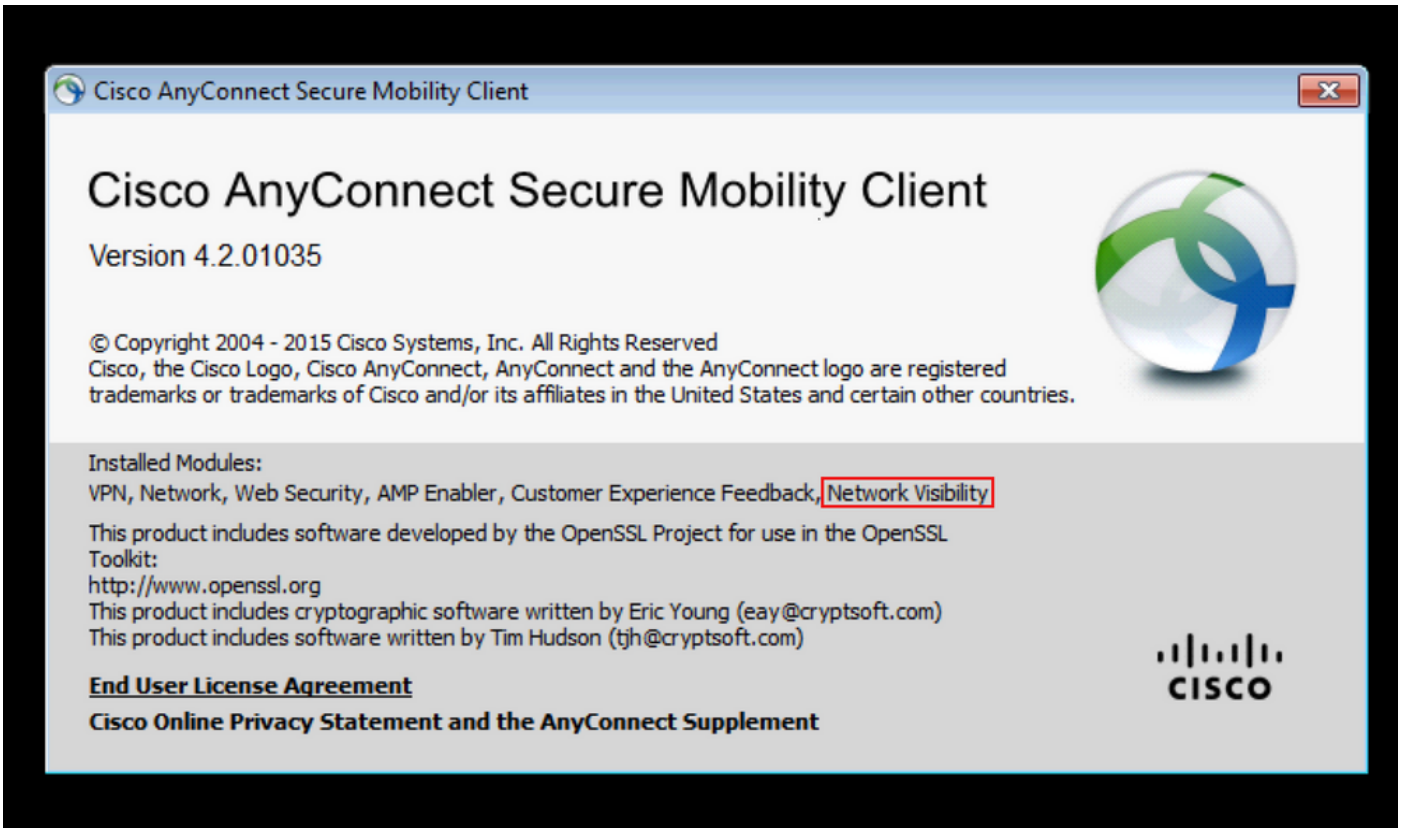




Verifica

Convalida dell'installazione di AnyConnect NVM

Dopo aver completato l'installazione, Network Visibility Module deve essere elencato nella sezione Moduli installati, all'interno della sezione Informazioni di AnyConnect Secure Mobility Client.



Verificare inoltre che il servizio nvm sia in esecuzione sull'endpoint e che il profilo sia presente nella directory richiesta.

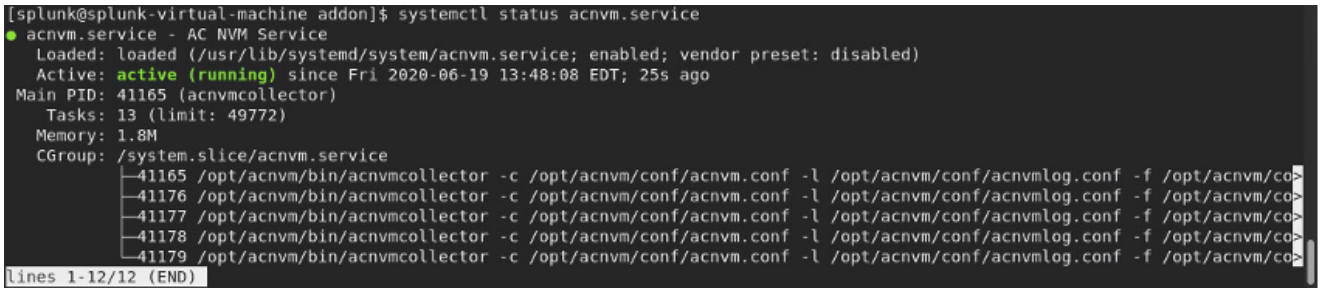
Convalida stato agente di raccolta

Confermare che lo stato dell'agente di raccolta sia "attivo (in esecuzione)". Questo stato garantisce che l'agente di raccolta riceva sempre IPFIX/cflow dagli endpoint. Se lo stato dell'agente di raccolta non è attivo, verificare che le autorizzazioni dell'account acnvm per il file ne consentano l'esecuzione:

- /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/

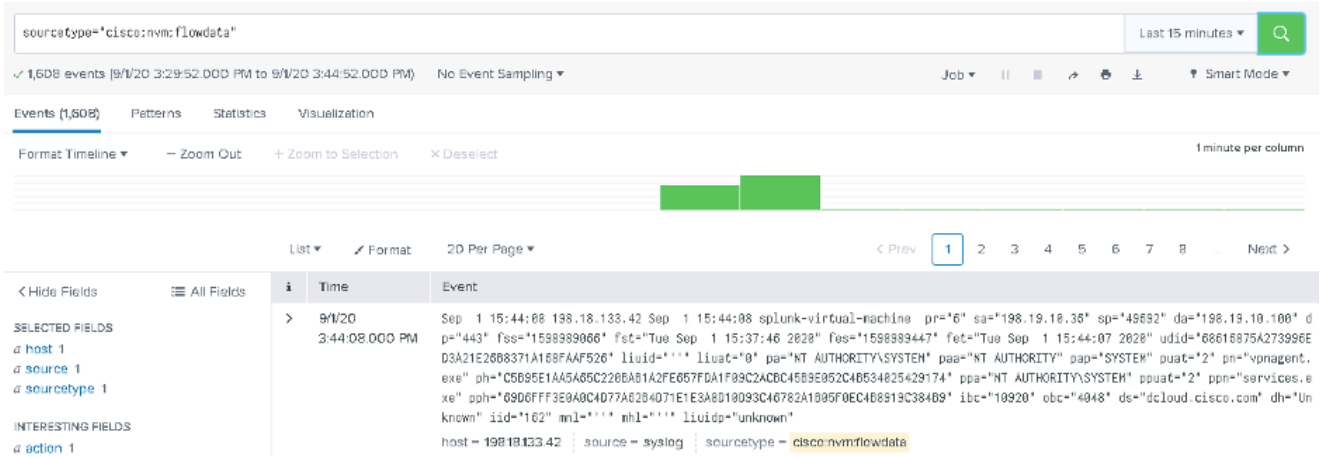


Convalida Splunk - Dashboard CESA

Verificare che Splunk e i relativi servizi siano in esecuzione. Per la documentazione su come risolvere i problemi relativi a Splunk, consultare il sito Web Splunk.

I dashboard per CESA vengono aggiornati solo cinque minuti dopo la ricezione dei dati iniziali, a causa di uno script di automazione. È tuttavia possibile eseguire immediatamente una ricerca manuale per verificare che i dati vengano ricevuti:

1. Dal dashboard Splunk principale, fare clic su Ricerca e report.
2. Nella schermata successiva, impostare l'intervallo corretto per popolare i dati desiderati.
3. Nel campo di ricerca, immettere: sourcetype="cisco:nvm:flowdata"



Dopo i primi cinque minuti, verificare che il quadro comandi CESA riceva i dati:

1. Dal dashboard Splunk principale, fare clic su Cisco Endpoint Security Analytics Dashboard.
2. Fare clic su Attività dispositivo per volume e conteggio flusso se si desidera mantenere le impostazioni correnti.
3. Fare clic su Invia. Il quadro comandi visualizza i dati e gli elementi grafici.

Flusso dei pacchetti

1. I pacchetti IPFIX vengono generati sugli endpoint client dal modulo NVM di AnyConnect.
2. Gli endpoint client inoltrano i pacchetti IPFIX all'indirizzo IP del collector.

3. Il raccoglitore raccoglie le informazioni e le inoltra a Splunk.

4. L'agente di raccolta invia il traffico a Splunk su tre flussi diversi: Dati per flusso, Dati endpoint e Dati interfaccia.

Tutto il traffico è basato su UDP, quindi non vi è conferma nel flusso del pacchetto che i dati sono stati ricevuti.

Porte predefinite per il traffico:

- Dati IPFIX 2055
- Dati per flusso 20519
- Dati endpoint 20520
- Dati interfaccia 20521

Il modulo NVM memorizza nella cache i dati IPFIX e li invia a un raccoglitore su una rete attendibile. Questo comportamento si verifica quando il notebook è connesso alla rete aziendale (in locale) o quando è connesso tramite VPN.

È possibile verificare che l'agente di raccolta stia ricevendo pacchetti dal modulo NVM. A tale scopo, eseguire un'acquisizione dei pacchetti su porte UDP specifiche, in base alla configurazione, per verificare se i pacchetti vengono ricevuti. Questa convalida viene eseguita tramite il sistema operativo Linux Splunk.

Modelli di flusso

I modelli di flusso IPFIX vengono inviati all'agente di raccolta all'inizio della comunicazione IPFIX. Questi modelli consentono all'agente di raccolta di dare un senso ai dati IPFIX.

L'agente di raccolta precarica inoltre i modelli per garantire che i dati possano essere analizzati, anche se il client non li ha inviati. Se viene rilasciata una versione più recente del client con modifiche al protocollo, l'agente di raccolta utilizza i nuovi modelli inviati dal client.

Un modello viene inviato alle seguenti condizioni:

1. È stata apportata una modifica al profilo del client NVM.
2. Evento di modifica della rete.
3. Il servizio nvmagent è stato riavviato.
4. L'endpoint viene riavviato.
5. Periodicamente (predefinito = 24 ore), come configurato nel profilo NVM.

In rari casi, l'agente di raccolta non è in grado di trovare un modello. Se si verifica questa situazione, si verificherà uno dei seguenti sintomi:

- Nessun modello trovato in un'acquisizione pacchetto sull'endpoint
- Oppure nessun modello per il set di flussi nei registri dell'agente di raccolta

Per risolvere il problema, riavviare uno degli endpoint.

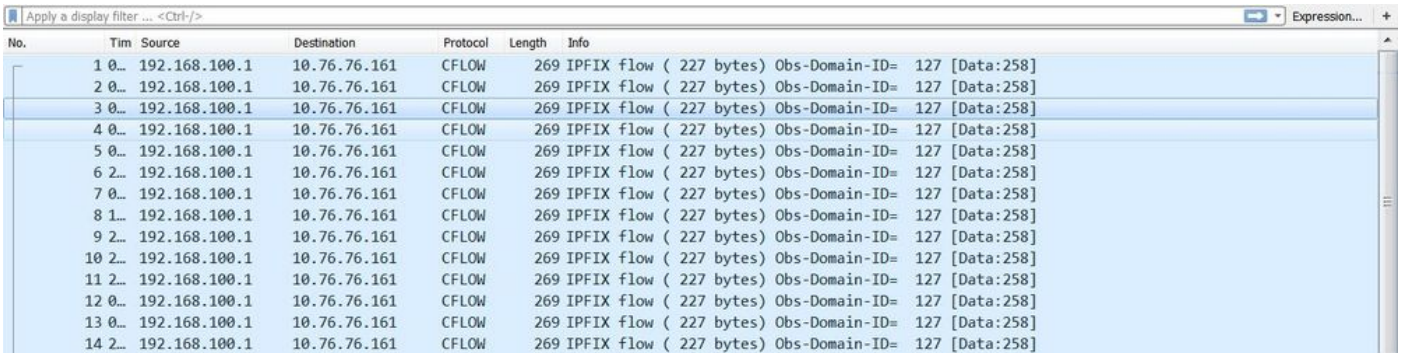
Risoluzione dei problemi

Di seguito sono riportati i passaggi di base per la risoluzione dei problemi:

1. Verificare la connettività di rete tra l'endpoint client e l'agente di raccolta.
2. Verificare la connettività di rete tra l'agente di raccolta e Splunk.
3. Verificare che NVM sia installato correttamente sull'endpoint client.
4. Applicare le clip sull'endpoint per verificare se il traffico IPFIX è stato generato.
5. Applicare le acquisizioni su un agente di raccolta per verificare se riceve il traffico IPFIX e se inoltra il traffico a Splunk.
6. Applica le clip su Splunk per vedere se riceve il traffico.
7. Per DTLS:
    - Confermare che i client AnyConnect considerino attendibile il certificato dell'agente di raccolta.
    - Confermare che l'opzione "secure" sia abilitata nel profilo NVM.
    - Verificare che l'agente di raccolta sia configurato per i certificati.

Traffico IPFIX come rilevato su Wireshark:

Nota: Se si esegue il protocollo DTLS tra il client e l'agente di raccolta, è necessario filtrare il traffico DTLS.

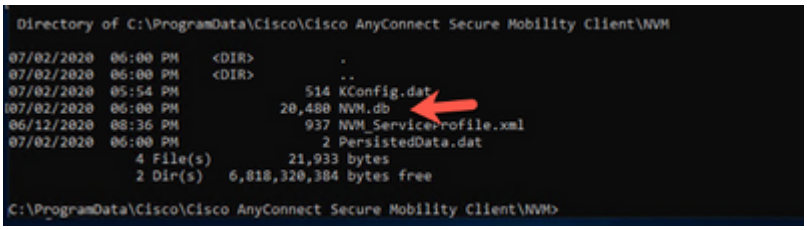


Client AnyConnect (modulo NVM)

I dati non vengono segnalati all'agente di raccolta e i pacchetti di dati non vengono inviati dall'endpoint

Le dimensioni del file del database NVM (NVM.db) continuano ad aumentare nella directory C:\%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM? Questo comportamento indica che il client NVM AnyConnect non sta inviando pacchetti di dati all'agente di raccolta.

Nota: Per informazioni sui processi della cache e sui controlli della cache disponibili, consultare la Guida dell'amministratore di Cisco AnyConnect Secure Mobility Client, versione 4.9.



TND (Trusted Network Detection)

Avviare l'interfaccia utente di AnyConnect e verificare che si trovi su una rete attendibile. NVM si affida a TND per rilevare quando l'endpoint si trova all'interno di una rete attendibile. Una configurazione TND errata causa problemi con la NVM. NVM dispone di una propria configurazione TND, che funziona sull'impronta digitale del certificato TLS del server configurato. Il NVM TND può essere configurato nell'NVM Profile Editor.

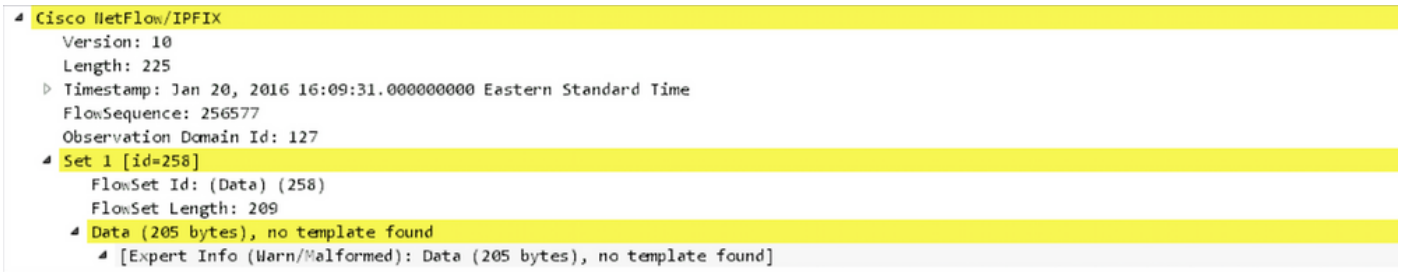
Se NVM TND non è configurato, NVM si basa sulla configurazione TND del modulo VPN. Il TND del modulo VPN funziona in base alle informazioni ricevute tramite DHCP: server DNS (Domain-name System). Se il server DNS e/o il nome di dominio corrispondono ai valori configurati, la rete viene considerata attendibile. La VPN supporta anche il rilevamento TND basato sui certificati TLS.

- Verificare che la configurazione TND sia corretta. NVM esporta solo quando si trova su una rete attendibile.

Nota: Se la configurazione TND non è corretta, NVM non esporterà i dati. Ad esempio, se nel client sono configurati tre server DNS, ma nella configurazione TND non sono impostati tutti e tre i server DNS, NVM non esporterà i dati.

- Rimuovere il dominio trusted dalla configurazione VPN TND.
- Problemi di rete:
  - Per il tunneling suddiviso, includere sempre l'indirizzo IP dell'agente di raccolta nella configurazione "split include" per la VPN. Se l'indirizzo IP dell'agente di raccolta non fa parte della configurazione attendibile del tunnel suddiviso, i dati verranno inviati all'interfaccia pubblica.
- Verificare che CollectionMode sia configurato per la raccolta nella rete corrente (trusted/untrusted).
- Assicurarsi che i file VPN.xml e NVM_ServiceProfile.xml si trovino nelle cartelle corrette; quindi riavviare.
- Avviare e arrestare tutti i servizi AnyConnect.
- Rimbalza la rete connessa all'interno che dispone di una connessione al server DNS.

Acquisizione pacchetti:



Strumenti di diagnostica e report (DART) di AnyConnect

Per risolvere i problemi relativi alle azioni AnyConnect, eseguire DART sui componenti NVM. Fare riferimento alla sezione Risoluzione dei problemi di AnyConnect.

- Tutti i registri necessari per NVM vengono gestiti da DART. DART raccoglie file di registro, configurazione e così via.
- Registri di Windows: Gli eventi non si trovano in un'unica posizione. Nel Visualizzatore eventi di NVM di AnyConnect è presente un'altra foglia.
- macOS/Linux: Filtra i registri per nvmagent.

Collector (Su computer Linux/Docker: all-in-one o standalone)

Impossibile installare acnvmcollector

Durante l'installazione dell'agente di raccolta e l'esecuzione dello script di installazione (Sudo ./install_ubuntu.sh)

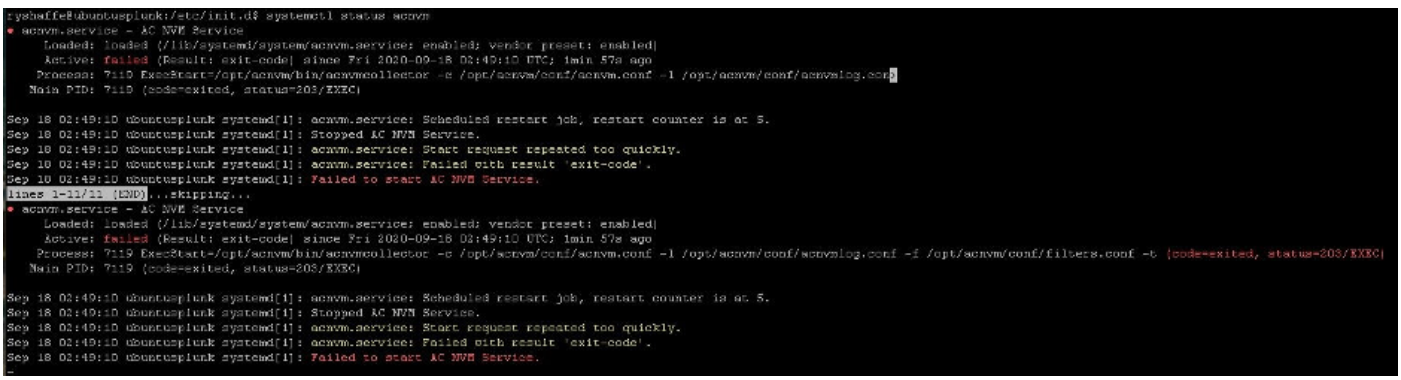
questo errore si verifica in /var/log/syslog: "Acnvm.conf error: line number 17 : expected key string"

Il problema può essere causato da una virgola aggiuntiva o da una virgola in una posizione non valida.

Impossibile avviare acnvmcollector

Questo problema era un problema su Ubuntu (ma forse su tutti i Linux). Impossibile eseguire il codice sul file acnvmcollector: /opt/acnvm/bin/acnvmcollector.

L'utente e il gruppo acvnm non disponevano eXecute di per acnvmcollector.



Registri dell'agente di raccolta - Dove è possibile impostare il debug?

È possibile impostare il livello di log nel file ACMNVMLOG.conf. Il livello di log fa parte della configurazione inviata all'agente di raccolta all'avvio. Dopo una modifica, riavviare il raccoglitore.

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
```

Come è possibile trovare il numero di versione del collector?

Per trovare la versione dell'agente di raccolta, eseguire il acnvmcollector comando con il -v flag:

Esempio 1:

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

Esempio 2:

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

Uscita:

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

Problemi DTLS

- Il messaggio "DTLS not configure" indica che DTLS non è configurato nel file acnvm.conf.
- Quando la combinazione di tasti non è supportata, viene visualizzato il messaggio "server key is invalid".

La console Splunk (dashboard CESA) non visualizza i dati

Client AnyConnect

- Utilizzare youtube.com per generare i dati. È inoltre possibile passare a un numero limitato di siti Web.
- Il client AnyConnect può inviare informazioni tramite UDP 2055 al server di raccolta? (In altre parole, esistono firewall tra il client AnyConnect e il server di raccolta?)
  - Provare a eseguire il telnet dal computer client al computer di raccolta.
- Eseguire wireshark per confermare che il client sta inviando dati relativi al traffico (2055 CFLOW) all'agente di raccolta.

Casella di raccolta

- Verificare che la cassetta di raccolta riceva il traffico AnyConnect NVM:
  - Eseguire un dump tcp e verificare che siano visualizzati i pacchetti dal client al server dal 2501 al 2055. Ad esempio, questo comando visualizza i primi 100 pacchetti provenienti dall'indirizzo IP dell'host del client:Sudo tcpdump -I any -c100 -nn host 10.1.110.7

    Nota: Per ulteriori informazioni, consultare il documento sulla cattura di tutti i pacchetti UDP tramite tcpdump.

  - Verificare che AnyConnect NVM Collector sia in esecuzione (vedere Supporto DTLS in questo documento).
  - Controllare il file acnvm.conf per verificare la presenza di errori di formato, virgolette mancanti, virgole e così via.
  - Splunk UI - TA - Gli input e i tipi di origine dei dati UDP sono configurati nell'interfaccia utente di Splunk o tramite input.conf?
    - Riavviare Splunk in UI > impostazioni > controlli server.

Domande frequenti (FAQ)

Come è possibile inviare dati da AnyConnect NVM a più destinazioni?

Questo scenario viene utilizzato per situazioni di elevata disponibilità o per l'invio a più piattaforme (ad esempio, Splunk e Stealthwatch).

Per ulteriori informazioni, fare riferimento alla Cisco Endpoint Security Analytics (CESA) Built on Splunk Quickstart POV Kit & Deployment Guide (in lingua inglese).

Dove memorizzare il certificato per AnyConnect NVM DTLS?

Questa situazione può verificarsi nei test di laboratorio in cui non è installato un certificato noto sull'agente di raccolta.

- Windows: Installare il certificato dell'agente di raccolta nei certificati attendibili di Windows.
- Mac OSX Utilizzare il processo standard per installare il certificato radice tramite il portachiavi. È possibile utilizzare lo strumento keychain per importare il certificato e aggiungerlo come certificato attendibile.
- Linux RHEL: Attenersi alla procedura di importazione della CA radice RHEL seguente:
    1. Copiare il certificato ca in /etc/pki/ca-trust/source/anchors.
    2. sudo update-ca-trust enable
    3. sudo update-ca-trust extract
- Ubuntu Linux: Attenersi alla procedura di importazione della CA radice Ubuntu seguente:
    1. Convertire il file .cer in un file .crt con questo comando: openssl x509 -inform PEM -in RootCA.cer -out rootCa.crt
    2. Copiare il file .crt nella directory /usr/local/share/ca-certificates.
    3. Eseguire il comando: sudo update-ca-certificates

Nomi file XML

Quando si utilizza l'editor dei profili locali, il nome del profilo XML del modulo VPN di base non ha importanza. Tuttavia, è necessario salvare il profilo del servizio come NVM_ServiceProfile.xml. Se si utilizza un nome diverso per il profilo del servizio, NVM non è in grado di raccogliere e inviare i dati.

Collector (AnyConnect NVM)

App Cisco Endpoint Security Analytics (CESA) per Splunk (dettagli)

- È possibile creare una directory fornitore nella directory radice e quindi fornire la proprietà a un altro account?

  È possibile creare /opt/acnvm prima di tutto se lo script di installazione ha l'autorizzazione per copiare i file in esso.
- Autorizzazioni file: Il file install.sh richiede l'autorizzazione per l'esecuzione come root.
- Account del servizio:
    - Il useradd -rcomando e il -s /bin/falsecomando sono necessari perché un account

del servizio è un account non interattivo che non dispone di una home directory.

- Non è necessario che gli account non interattivi dispongano di una home directory, ed è normale che gli account del servizio non dispongano di una home directory da mantenere pulita.
- Tutti gli utenti dispongono di un uid o di un guid, indipendentemente dal fatto che dispongano o meno di una home directory.

- Sistema operativo del collector: Il collector funziona su CentOS o Ubuntu; può anche essere eseguito su RedHat perché RedHat utilizza lo script CentOS.
- Se necessario, è possibile modificare lo script di installazione:
  - Lo script di installazione deve essere eseguito come root o con diritti SUDO perché crea un nuovo utente chiamato acnvm e inserisce tutto nella directory /opt/acnvm.

> Nota: In alternativa, è possibile creare uno script personalizzato per eseguire le azioni appropriate in base alle proprie esigenze. Questo script può utilizzare un utente diverso già esistente nel sistema, ma questo utente deve disporre dei diritti SUDO per eseguire l'installazione.

- Per trovare la versione dell'agente di raccolta, eseguire questo comando con il -vflag: ./opt/acnvm/bin/acnvmcollector -v

Versione consigliata

Si consiglia sempre di usare la versione software più recente di AnyConnect. Per ulteriori informazioni, fare riferimento alle note sulla versione di Cisco AnyConnect Secure Mobility Client v4.x.

Informazioni correlate

- Cisco Endpoint Security Analytics (CESA) basato su Splunk Quickstart POV Kit e Guida all'installazione
- Panoramica del dashboard Cisco Endpoint Security Analytics (CESA) e domande frequenti
- App Cisco Endpoint Security Analytics (CESA) per Splunk
- App Cisco Endpoint Security Analytics (CESA) per Splunk (documentazione)
- Guide per l'amministratore dei client per Cisco AnyConnect Secure Mobility Client v4.x
- Note sulla versione di Cisco AnyConnect Secure Mobility Client v4.x
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).