

# CESA J Splunk و AnyConnect NVM نيوكت

## تايوت حمل

[قمدقم](#)

[قيساس ألأا تابل طتم](#)

[تابل طتم](#)

[قمدخت سمل تانوكم](#)

[قيساس أ تامول عم](#)

[VPN نم رثكأ - Cisco AnyConnect Secure Mobility Client](#)

[\(IPFIX\) تثر تنال لوكوت ورب قفدت تامول عم ري دصت](#)

[عمجم IPFIX NVM](#)

[Splunk قس سؤم](#)

[رشنلأا ىلع قماع قرظن](#)

[ططخم](#)

[نيوكت](#)

[DTLS م عدل NVM نيوكت](#)

[قدهشلأا تابل طتم](#)

[\(ثدج ألأا تارادصلأا 4.9.3043\) AnyConnect نيوكت](#)

[قلقت سمل AnyConnect NVM قي طم نلأا قدهولأا](#)

[AnyConnect NVM لي مع في رعت فلم](#)

[ASDM ربع NVM لي مع في رعت فلم نيوكت](#)

[AnyConnect في رعت فلم برجم لالغ نم NVM لي مع في رعت فلم نيوكت](#)

[Cisco ASA ىلع بيولأا ربع رشنلأا نيوكت](#)

[Cisco ISE ىلع بيولأا ربع رشنلأا نيوكت](#)

[وب قوؤوملأا قكبشلأا فاشتك](#)

[رشنلأا](#)

[Cisco ASA/ISE ىلع AnyConnect NVM نيوكت 1. قوطخ](#)

[\(AnyConnect NVM عمجم\) IPFIX عمجم نوكم دادعأ 2. قوطخ](#)

[تانايبلأا عمجم تي بئثت قي فيك](#)

[معد DTLS](#)

[قي فاضأ TA ة في طوؤو CESA تامول عم قحول مادخت ساب ميسقت دادعأ 3. قوطخ](#)

[Install رمألأا](#)

[Splunk قراڈا مدخت سم قهچا و ربع UDP تالاد نيوكم](#)

[قحصلأا نم ققحت](#)

[AnyConnect NVM تي بئثت قحص نم ققحت](#)

[عمجملأا قلاح قحص نم ققحت](#)

[CESA تامول عم قحول - Splunk قحص نم ققحت](#)

[قمنجلأا قفدت](#)

[قفدت بلأوق](#)

[اهجالص او عا طخ ألأا فاشكت س](#)

[\(NVM قدهو\) AnyConnect لي مع](#)

[قطقن نم تانايبلأا مزح لاس را متي الو تانايبلأا عمجم ىلأا تانايبلأا نع غالبالأا متي ال قياهنلأا](#)

[\(TND\) هب قوٲوملا ةكبشلا فاشنلا](#)

[AnyConnect ل \(DART\) ريراقتلا دادعلاو صيخشلا تاودا](#)

[\(لقتسم وا دحاو يف لئلا Linux/Docker زامج ىلع\) عمجم](#)

[acnvmcollector تيبتت لشف](#)

[عديلا يف AcnvmCollector لشف](#)

[ءاطخألا حىحصت نييغت يئتنكمي نيأ - عمجملا تالجم](#)

[ءماقراألا عمجم صاخلا رادصلا مقري ىلع روٲعلا يئتنكمي فيك](#)

[DTLS لئلاشم](#)

[تانايبلا ضرعت ال \(CESA تامولعم ؤحول\) Splunk مكحت ؤحول](#)

[AnyConnect لييمع](#)

[عيمجت قودنص](#)

[ةعئاشلا قلئسألا](#)

[ةددعتم تاهجو ىلا AnyConnect NVM نم تانايبلا لئسلا كنكمي فيك](#)

[AnyConnect NVM DTLS ؤداهش نييختب موقت نيأ](#)

[XML تافللم ءامسأ](#)

[\(AnyConnect NVM\) عمجم](#)

[هب ىصوملا رادصلا](#)

[قلص تاذا تامولعم](#)

## ةمدقملا

نم (NVM) ةكبشلا ةيؤر ةيئناكمال ةيظمنلا ؤحول تيبثت ةي فيك دنتسمل اذه حضوي AnyConnect 4.7.x لغشي يذلا يئئاھنلا مدختسمل ماظن ىلع اھنيوكتو Cisco AnyConnect 4.7.x اھنيوكتو NVM عمجت مو ؤلصل تاذا Splunk ؤسسؤم تانوكم تيبثت ةي فيكو ،ثدحأ رادصا

## ةيساسألا تابلطتملا

### تابلطتملا

ةيلال عيضاوملاب ؤفرعم كي دل نوكت نأب Cisco ي صوت:

- AnyConnect 4.7.x واً رادصا واً NVM عم ثدحأ رادصا
- AnyConnect صيخرت
- Adaptive Security Device Manager (ASDM) 7.5.1 واً رادصا واً
- اھتافاضا و Splunk تاقيبطت تيبثت ةي فيكو Splunk Enterprise ىلع فرعتلا

### ةمدختسمل تانوكملا

ةيلال ةي داملا تانوكملا وجماربلا تارادصا ىلا دنتسمل اذه يف ؤدراولا تامولعمل دنتست:

- Cisco AnyConnect Security Mobility Client 4.7.x واً رادصا واً
- Cisco نم AnyConnect فيرعت فلم ررحم
- Cisco Adaptive Security Appliance (ASA) ؤلدعمل نامألا ؤزهجأ 9.5.2 رادصا واً
- Cisco Adaptive Security Device Manager (ASDM) 7.5.1 رادصا واً

- يألل ع تاناكملإل ددعتم زاهك هتېبثت م (ثدأ رادصل وأ Splunk Enterprise 7.x جم انرب (لصفم ال CentOS لىغشتل ماطن: Linux نم ةم ودم ال لىغشتل ةمظنأ نم
- عمجم زاهك م ودم Linux تېبثت ي



[ةطقنلأ نامأ تاليلحت](#) عجار. مداخل س فن ىل ع عمجم لىغشت نكمي: ةطال م رشنلأ لىلدو [Splunk QuickStart POV Kit](#) ىل ع ةمئاقلأ Cisco نم (CESA) ةيفرطلأ تامولعملأ نم ديزم ىل ع لوصلل

ةصاخ ةيلمعم ةئيب ي ف ةدوجوملأ ةزهجألأ نم دنتسملأ اذه ي ف ةدراولأ تامولعملأ عاشنإ م تناك اذإ. (يضا رتفا) حوسمم نيوكتب دنتسملأ اذه ي ف ةمدختسملأ ةزهجألأ عيمج تأدب رملأ يأل لمحتملأ ريثأتلل كمهف نم دكأتف، لىغشتلأ دي ق ك تكبش

## ةيساسأ تامولعملأ

ةميقلأ ةيلاع ةياهنلأ طاقن عبتت تانايبل ةرمتسم ةيذغت Cisco AnyConnect NVM رفوي عمجت. مهتكبش ىل ع مدختسملأ كولسو ةياهنلأ ةطقن ةيؤر نم تاسسؤملأ نكمت يتلأ لثم ةميقلأ تاقايسلأ ىل ةفاضلأب، عقوملأ جراحو لخد ةياهنلأ طاقن نم تاقفدتلأ NVM تانايب Splunk Enterprise كل هتسي. تاهجولأو عقولأو ةزهجألأو تاقيبطتلأو نيمدختسملأ ريراقتلأو تاليلحتلأ تانايكملأ رفويو مادختسالأ عبتت تانايب تانايب

لح نم عزجك Splunk Enterprise عم AnyConnect NVM ل نيوكتب لاثم يه ةينقتلأ ةطاللملأ هذه Cisco نم ديدجلأ (CESA) ةيفرطلأ ةطقنلأ نامأ تاليلحت

- مادختساب CESA نم (POV) ةميقلأ تابثإ لىلد ىل ع ةلماك ةماع ةرطن ىل ع لوصلل [Splunk ىل ع ةمئاقلأ Cisco نم \(CESA\) ةيفرطلأ ةطقنلأ نامأ تاليلحت](#) ىل ع عجار، [رشنلأ لىلدو Splunk QuickStart POV Kit](#).
- [ىل ع ةماع ةرطن](#) ىل ع عجار، Splunk ىل ع Cisco NVM تامولعملأ ةحولل لىلد ىل ع لوصلل [ةلوادتملأ ةلئسلأو \(CESA\) ةيفرطلأ ةطقنلأ نامأ تاليلحت تامولعملأ ةحول](#).
- Cisco نم ةيفرطلأ ةطقنلأ نامأ تاليلحت ىل ع عجار، لال لولح تامولعملأ نم ديزمل [Splunk ىل ع ةينبم](#).

للال لكشت تانوكملأ هذه:

- [ةيؤر ةينكاملأ ةيظمنلأ ةدحولأ نيكمت عم Cisco AnyConnect Secure Mobility Client \(NVM\) ةكبشلأ](#)
- [Splunk ل Cisco نم \(CESA\) ةيفرطلأ ةطقنلأ نامأ تاليلحت قيبطت](#)
- [Splunk ل Cisco نم \(CESA\) ةيفرطلأ ةطقنلأ نامأ تاليلحتلأ ةيفاضلأ ةفيظولأ](#)
- NVM TA ةيفاضلأ ةفيظولأ عم zip فلم ي ف نمضم) NVM عمجم

## VPN نم رثكأ - Cisco AnyConnect Secure Mobility Client

امابلأغ. ةسسؤملأ ةيامل ةددعتم نامأ تامدخ رفوي دحوم لىكو نع ةرابع Cisco AnyConnect اضيأ م عدي هنكلو، تاسسؤملأب ةصاخلأ VPN ةكبشل لىم عك AnyConnect مادختسالأ متي تادحولأ حيتت. تاسسؤملأ نامأل ةفلتخملأ بناوجلل بيحتست يتلأ ةيفاضلأ تادحولأ ةينكاملأو ةراضلأ جماربلأ ةياملحو بيولأ نامأو عضولأ مبيقت لثم نامأل تازيم ةيفاضلأ

ريثك ال ك ل ذ ري غ و ة ك ب ش ل ا ة ي ؤر .

Cisco AnyConnect عم ا ه ج م د م ت ي ي ت ل ا و ، NVM ة ق ا ط ب ب ة ي ن ق ت ل ا ة ط ح ا ل م ل ا ه ذ ه ق ل ع ت ت ن م د ي ز م ل . ة ي ا ه ن ل ا ة ط ق ن ق ي ب ط ت م ا د خ ت س ا ة ب ق ا ر م ي ل ع ن ي ل و و س م ل ل ة ر د ق ل ا ر ي ف و ت ل [Cisco AnyConnect Secure Mobility لوؤس م ل ي ل د](#) ي ل ا ع ج ر ا ، Cisco AnyConnect ل و ح ت ا م و ل ع م ل ا [4.7 ر ا د ص ا ل ا ، Client](#).

(IPFIX) ت ن ر ت ن ا ل ل و ك و ت و ر ب ق ف د ت ت ا م و ل ع م ر ي د ص ت

ل ث م ة د د ع ت م ض ا ر غ أ ل IP ق ف د ت ت ا م و ل ع م ر ي د ص ت ل ا ر ا ي ع م د د ح ي IETF ل و ك و ت و ر ب و ه IPFIX ر ي غ ا م ه ن ا م غ ر ، Cisco NetFlow v9 ل و ك و ت و ر ب ي ل ع IPFIX د م ت ع ي . ن ا م أ ل ا و ة ع ج ا ر م ل ا و ة ب س ا ح م ل ا IPFIX ل و ك و ت و ر ب ي ل ا د ن ت س ت ل و ك و ت و ر ب ت ا ف ص ا و م ي ه [Cisco NVZflow](#) . ة ر ش ا ب م ن ي ق ف ا و ت م ل ق ن ل ة د ي د ج ت a م ل ع م د ي د ح ت ب ك ل ح م س ي ع ي س و ت ل ل ل ب ا ق ل و ك و ت و ر ب و ه IPFIX ، م ي م ص ت ل ل ا ب ر ص ا ن ع ف ر ع ي و IPFIX ر ا ي ع م ع ي س و ت ي ل ع Cisco NVZflow ل و ك و ت و ر ب ل م ع ي . ت a م و ل ع م ل ا ه ل ق ن م ت ي ي ت ل ا IPFIX ب ل ا و ق ن م ة ي س ا ي ق ة ع و م ج م ل و ك و ت و ر ب ل a د د ح ي ا م ك . ة د ي د ج ل a ت a م و ل ع م ل a AnyConnect NVM ا م د خ ت س ي ي ت ل a م a د خ ت س a ل a ع ب ت ت ت a ن a ي ب ن م ع ن ج ك

RFCs: ا ذ ه ، IPFIX ي ل ع ة م و ل ع م ر ي ث ك ل ت ل ح ا

- [RFC5101 ر ا ي ع م ل ا](#)
- [RFC7011 ر ا ي ع م ل ا](#)
- [RFC7012 ر ا ي ع م ل ا](#)
- [RFC7013 ر ا ي ع م ل ا](#)
- [RFC7014 ر ا ي ع م ل ا](#)
- [RFC7015 ر ا ي ع م ل ا](#)

IPFIX NVM ع م ج م

ت a ن a ي ب ل a ه ذ ه ة ي ذ غ ت ك ل ذ د ع ب ن ك م ي و . ا ه ن ز خ ي و IPFIX ت a ن a ي ب ل ب ق ت س ي م د a خ و ه ت a ن a ي ب ل a ع م ج م ل ل Splunk .

م a د خ ت س a ب ه ع ي م ج ت م ت ي و NVZflow ل و ك و ت و ر ب ل ا ص ي ص خ ه م ي م ص ت م ت ع م ج م Cisco ر ف و ت ع ب ر م ل a س ف ن ي ل ع ت a ن a ي ب ل a ع م ج م ت ي ب ث ت ن ك م ي . CESA TA ل Splunk ة ي ف ا ض ا ل ا ة ف ي ط و ل a ل ق ت س م Linux ع ب ر م ي ل ع و ا ل ي ق ث ل a ل ي م ح ت l a ز ا ه ج ي ل ع و ا Splunk م د a خ ع م ( ت a ن a ك م l a د د ع ت م )

(NVM) ة ك ب ش ل a ة ي ؤر ع م ج م ي ل a ع ج ر a ، ت a ن a ي ب ل a ع م ج م ل و ح ة ي ل ي ص ف ت l a ت a م و ل ع م ل a ن م د ي ز م ل [Cisco](#) ن م .

Splunk ة س س ؤ م

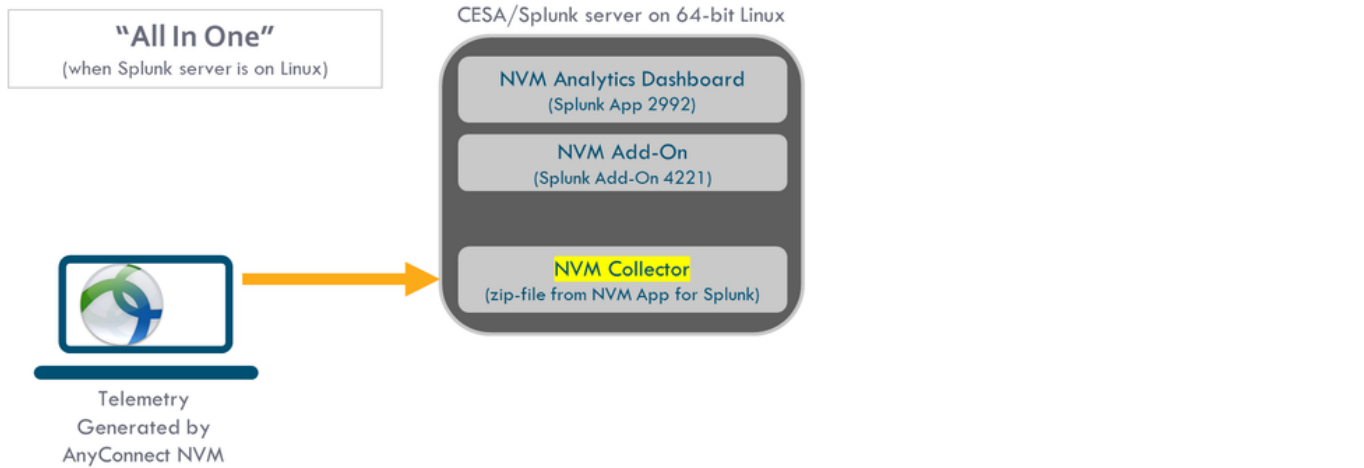
ة د ي ف م ت a م و ل ع م ر ي ف و ت ل ا ه ل ل ح ت و ص ي خ ش ت l a ت a ن a ي ب ع م ج ت ة ل a ع ف ا د ا Splunk Enterprise د ع ت ن ي ل و و س م ل l a ل م a ك ت م a د ح a و ا ع ق و م ر ف و ي و ه و . ت a م و ل ع م l a ة ي ن ق ت l ة ي س a س a ل a ة ي ن ب l a ل و ح ة ك ب ش l a ة م a ل س م ه ف ي ل ع م ه د ع a س ت ي ت l a ت a ن a ي ب l a ع م ج ل

ي ل a ع ج ر a ، ت a م و ل ع م l a ن م د ي ز م ل . م ه ع م ن و ا ع ت l a ب CESA ل ح ا ش ن ا م ت و Cisco ك ي ر ش و ه Splunk [Splunk ي ل ع ة ي ن ب م Cisco](#) ن م ة ي ف ر ط l a ة ط ق ن l a ن a م ا ت a ل ي ل ح ت

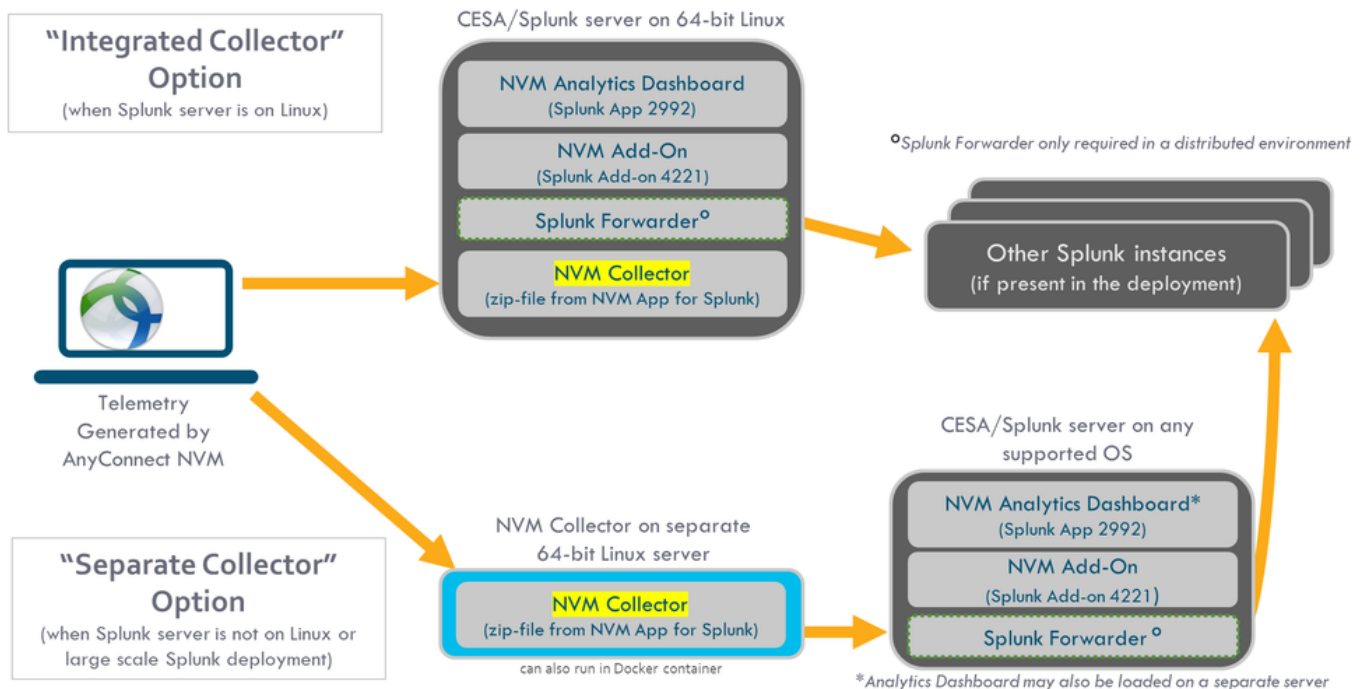
## رشننلا ىلع ةماع ةرظن

هذه. اهروص طسبأ يف رشننلا ةيلمع ىلع ىوتسملا ةعيفر ةماع ةرظن ةقيثولا هذه رفوتو تب 64 رادصا Linux ليغشتلا ماظن ىلع لمعت تاناكلال ةددعتم ةئيهت

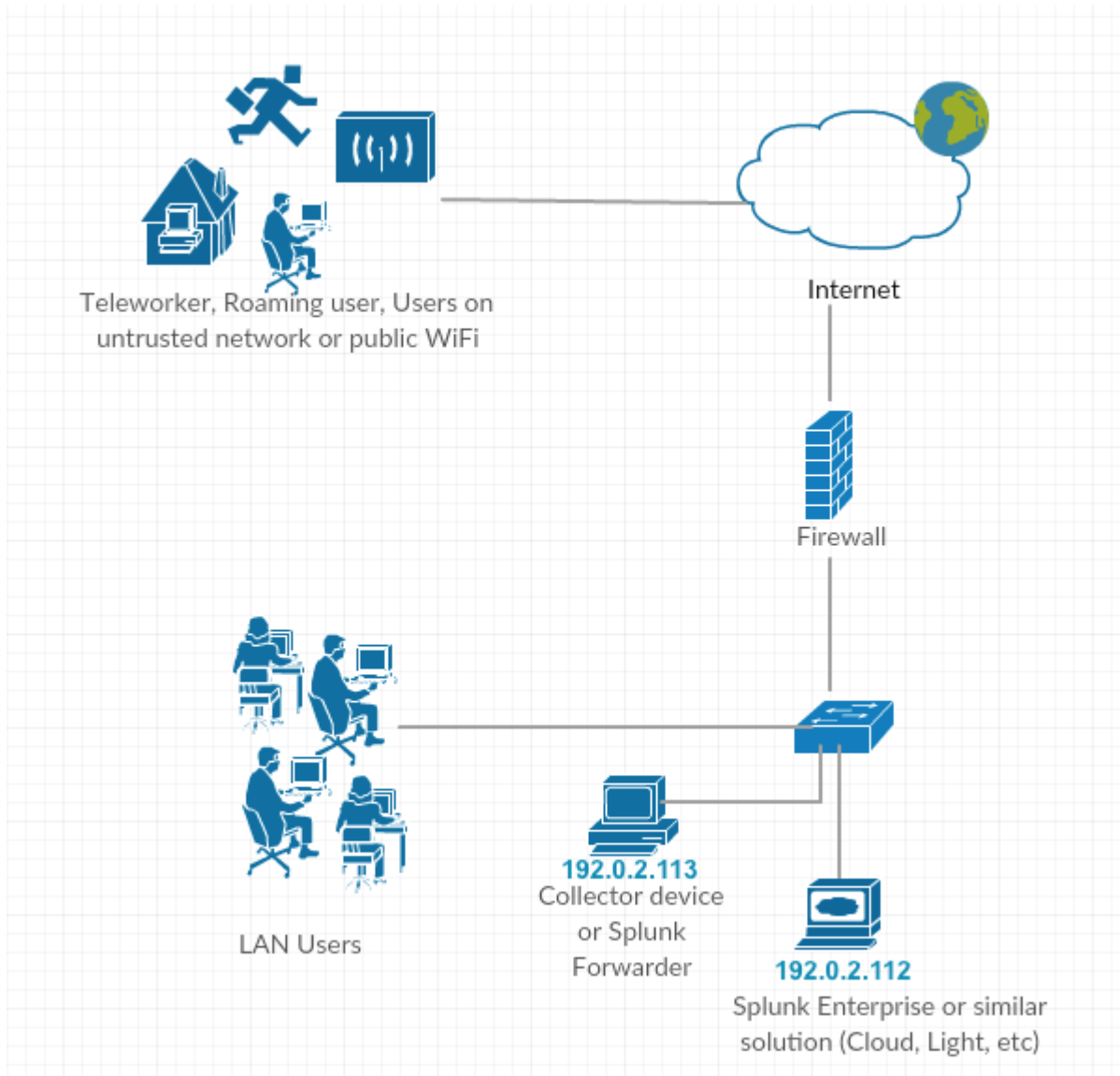
ايفم نيوكتلا اذه نوكيو. ضرع بلغال تلمعتسا نوكي نأ ليكشتلا ينايب مسر اذه يدبي ريغص جاتنا رشن يف اضيا



م تي، يجذومن لكشبو. رشننل ةرفوتملا تارايلال نم الومش رثكأ ةعومجم ططخمل اذه حضوي Splunk Enterprise دقع نم ديدعل ىلع ىوتحي وجاتنا لاداع عيزوت



## ططخمل



ة:نقنقالتة طحالمالهذه ف IP ننيوانع تاحالطصا

- عمحملل IP ناوع 192.0.2.123
- مي سقتب صالخال IP ناوع 192.0.2.113

## نيوكتال

AnyConnect رشن ىلع ةماع ةرظن ىلع لوصحلل Cisco NVM. تانوكم نيوكت مسقلا اذه يطغي [ةيؤر ةينك مال ةي طمنلا ةدحول اذيفنت ةيفيك](#) ىلا اضيا عجرا ،نيوكتال فيرعت فلمو NVM [ةكش AnyConnect](#).

## DTLS معدل NVM نيوكت

اذه DTLS ربع تانايبال عمحمل ىلا نم آ لكشب تانايبال لاسرال نآال NVM نيوكت نكمي مدختسي ،"نمآ" رايتخاللا ةناخ ديدحت دنع NVM فيرعت فلم ررحم في نيوكتلل لباق عضولا قوئوم (عمحمل) DTLS مداخ ةداهش نوكت نأ بجي ،هلع رورم لل DTLS لاصتال .لقنك NVM DTLS وه DTLS 1.2 .تمص في اهب قوئومال ريغ تاداهشل ضفر متي .ةياهنلا ةطقن لبق نم اهب ثدحأ رادصا وأ Splunk v3.1.2 قيبطت نم عزجك عمحمل رفوت مزلي .دمتعل رادصلل ىندأل دحل

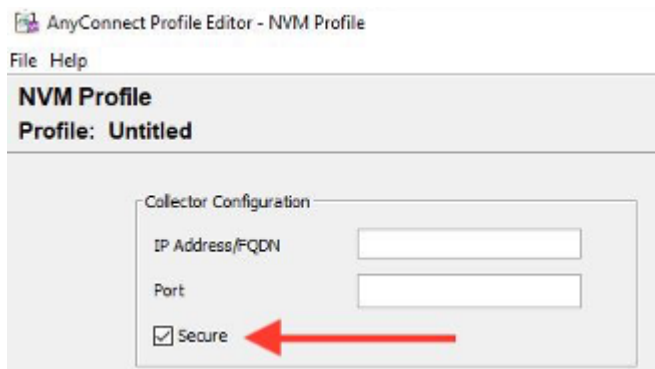
ة.نم آريغ وأ ةنم آما :طقف دحاو عضو ي ف تانا يبال عمجم لمعي .DTLS معدل CESA نم

ةداهشال تابلطتم

- ةلسلس نأ نم دكأت) .لعمعال لبق نم هب اقوئوم عمجمال صيخرت نوئي نأ بجي (AnyConnect.) لىل نيوكت دجوي ال هنأل اهب قوئوم تاداهشال
- PEM قيسنتب ةداهشال نوكت نأ بجي .
- كرحمل (CA) يلخادل ةداهشال عجرم بلطتي :ةظحال م .ةداهش حاتفم رورم ةم لك معدل ال دحاو دوجو Cisco نم (ISE) ةيوهال تامدخ
- اهب قثي AnyConnect ليمع زاهج ناك املاط عمجمال لىل ةداهش يأ مادختسإ نكمي (كلذلإ امو ،ةفورعم ،(PKI) يلخادل ماعال حاتفم لل ةيساسأل ةينبال)
- تارابتخا ءارجإل AnyConnect NVM ةمدخ ليغشت ةداعا بجي ،نيوكتال فلم ثيدحت دعب لبالل نامأل زاهج وأ ISE نم اهعفدم تي يتال تافيصوتلل ةبسنبالاب .(دحاوال ليمعال لاصلال ديعي مث ةكبشال نع ليمعال زاهج لصفني نأ بجي ،(ASA) فيكتلل
- اذه دمتعي .FQDN وأ IP لىل AnyConnect NVM فيرعت تافل عمجم نيوكت نييعت بجي ليضفت امئاد متي .ةداهشلل (CN) عئاشال مسال ي ةمدختسمال ةميقلال لىل رايلخا IP ناوئع تاريغي ةلاح ي (FQDN) لمكالل لهؤمل لاجمال مسا
- عوضومال مسا وأ CN عمجمال ةداهشل نوئي نأ بجي ي ،IP ناوئع مدختست تنك اذلإ IP. كلذل (SAN) ليابل
- NVM فيرعت فلم يوتحي نأ بجي ي ،ةداهشال ي CN ةكبشك FQDN كي دل ناك اذلإ عمجمك هسفن FQDN لىل

ثدحال تارادصلال او 4.9.3043 AnyConnect نيوكت

Collector نمض "Secure" مسمت ةديج رايتخا ةناخ كانه ،NVM فيرعت فلمل ةبسنبالاب IP/Port.



ةلقئسمال AnyConnect NVM ةيظمنال ةدحوال

ليلىلإ عجرا .ثدحال رادصلأ وأ AnyConnect 4.8.01090 دوجو ةلقئسمال ةيظمنال ةدحوال بلطتت لىل دلل اذه لىل اضيأ عجرا .4.9 رادصلال ،Cisco AnyConnect Secure Mobility Client لوؤسم AnyConnect ةكبش ةيؤر ةيناكل ةيظمنال ةدحوال ذي فنت ةي فيك :لقئسمال

ةمزح تيبتت كنكمي ي ،رخآ VPN لح مدختست تنك اذلأ وأ AnyConnect ل رشن كي دل نكي مل اذلأ لققسم لكشب ةمزال هذه لمعت .كب ةصاخال NVM تاجايحتل ةبلتل ةلقئسمال NVM

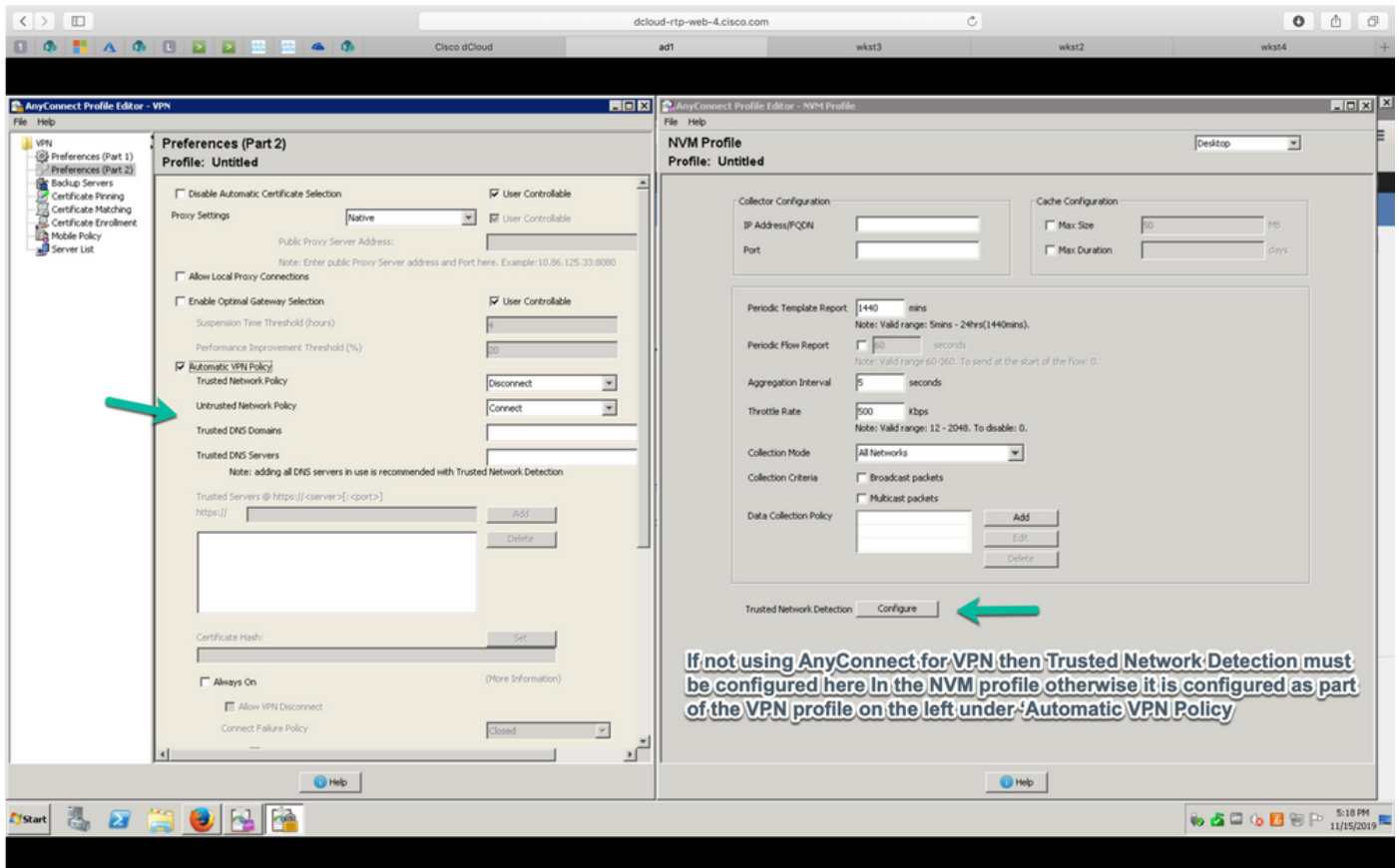
AnyConnect NVM لثمة عيانه عطقن نم قفدتال عومجم يوتسم سفن رفوت اهنكلو  
 دلج Activity Monitor لثمة) عطقننل تايلمعل اناف، لقتسمال NVM تيبتب تمق اذا. ليالجل  
 مداخلتسال لريشت (Macintosh (MacOS)) ليغشتال ماطن

فاشتك نيوكت نوكيو، [NVM فيرعت فلم برجم](#) مداخلتساب لقتسمال NVM نيوكت متي  
 عطقن تناك اذا ام ديدحتل TND نيوكت NVM مدختست. ايمازل (TND) هب قوومال كبشال  
 عبسانملا تاسايسال قيبطتب موقت م، عكرشال كبش دلج عيانهال

دادع او صيخشتل تاودا عطساوب متي ليحستل او احوال ص او اطاخال فاشكتس لازي ال  
 AnyConnect. عمزح نم اهتيبتب نكمي يتل او، AnyConnect، نم (DART) ريراقتال

عدافتسال لجا نم عيطمنال Core VPN عدحو تيبتب بجي ناك، لقتسمال رايل رفو لبق  
 مدختسمال عجاوي فايئرم ياساسال (VPN) عيره اظلال عاخال كبشال عبرم ناك. TND نم  
 ل نومدختسي اوناك اذا عساو، نيئيانهال ني مدختسمال اكابر ببسي دق ام وهو، (UI)  
 رجا دروم نم (VPN) عيره اظلال عاخال كبشال

نيوكتل ياساسال VPN فيرعت فلم مدختست ال كن اناف، لقتسمال رايل مدختست ام دنع  
 TND. ل عرشابم NVM فيرعت فلم نيوكت نال نكمي.



## AnyConnect NVM لي مع فيرعت فلم

عجمجلل IP ناونع لوح تامولعم دلج يوتحي XML فلم في AnyConnect NVM نيوكت ظفح متي  
 لكشب ذفنم مقرر عجمجلل IP ناونع نيوكت بجي. رخا تامولعم للافاضالاب، ذفنملا مقرر  
 NVM لي مع فيرعت فلم دلج عيحص

ليلدل اذه في XML فلم عضو بجي، عيطمنال NVM عحول عيحصال عيلمعل اعجال

- Windows 7 لي غشتال ماظنل ةبس نلاب : %ALLUserProfile%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM
- Mac OSX: /opt/cisco/anyconnect/nvm

رشن عم ايئاقلت هرشن م تي سف ، Cisco ASA/ISE ىل ع ادوجوم فيرعتال فلم ناك اذا AnyConnect NVM.

XML: فيرعت فلم لاثم

<#root>

<?xml version="1.0" encoding="UTF-8"?>

-<NVMProfile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="NVMP

-<CollectorConfiguration>

<CollectorIP>

**192.0.2.123**

</CollectorIP>

<Port>

**2055**

</Port>

</CollectorConfiguration>

<Anonymize>

**false**

</Anonymize>

<CollectionMode>

**all**

</CollectionMode>

</NVMProfile>

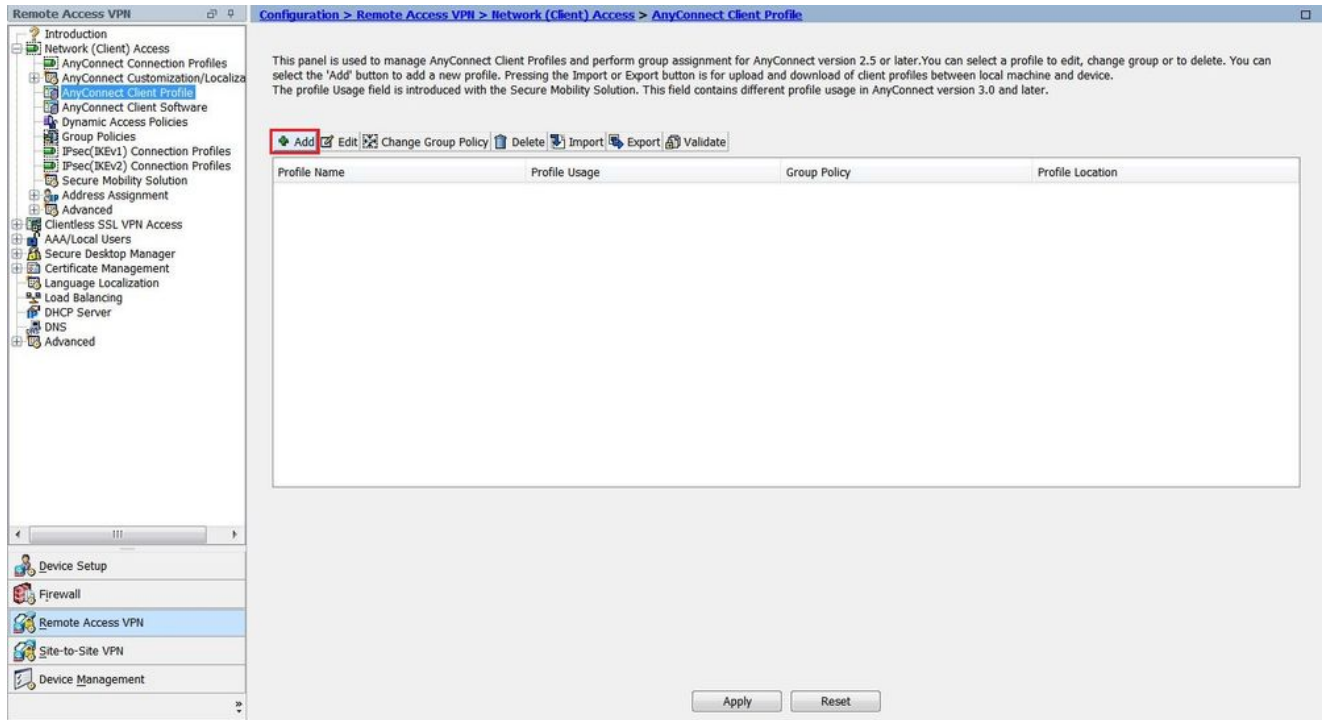
ةيالاتل تاودال مادختساب NVM فيرعت فلم عاشن نكمي:

- Cisco ن ASDM
- AnyConnect فيرعت فلم ررحم
- (ISE) ةيوهال فشك تامدخ كرحم

ASDM ربع NVM لي مع فيرعت فلم نيوكت

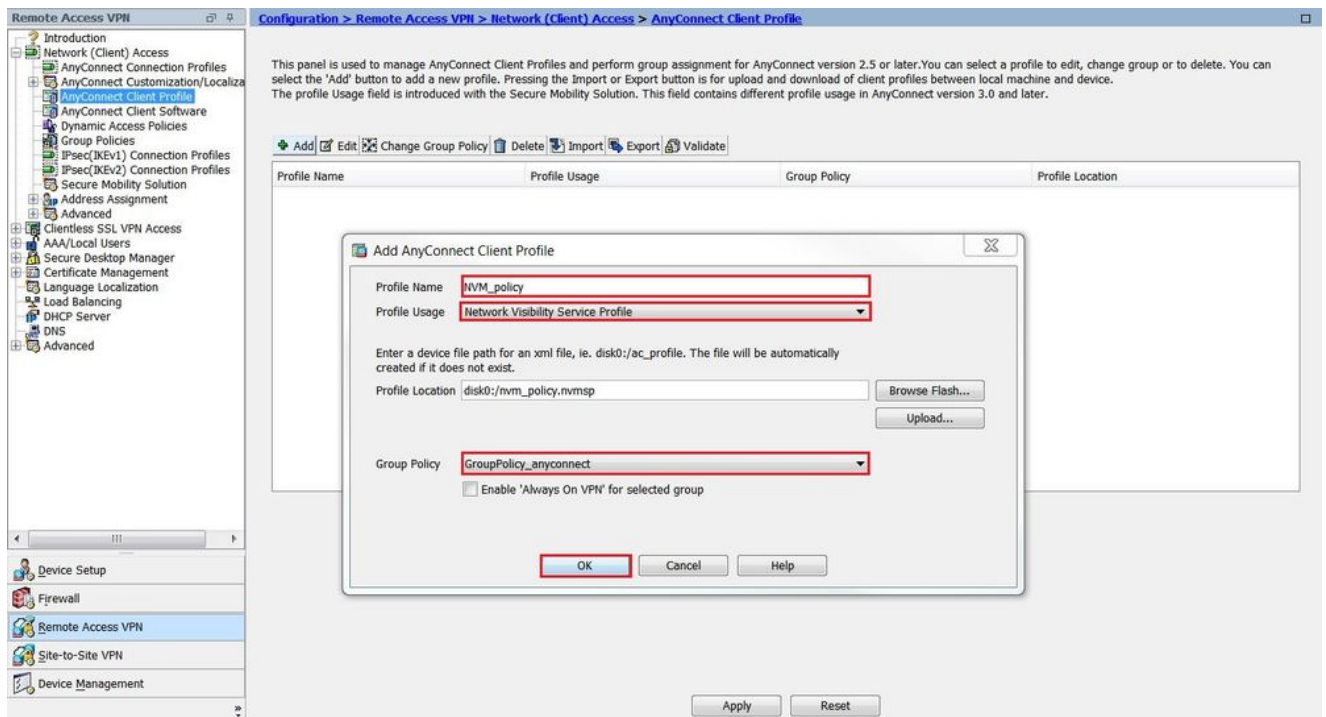
Cisco ASA ربع AnyConnect NVM رشن مت اذا بولسأل اذه لصف ي

1. AnyConnect Client Profile > Network (Client) Access > Access VPN ةلازا > نيوكتال ىل لقتنا Profile.
2. ةروصلال ي فضوم وه امك ، ةفاضل رقنا.

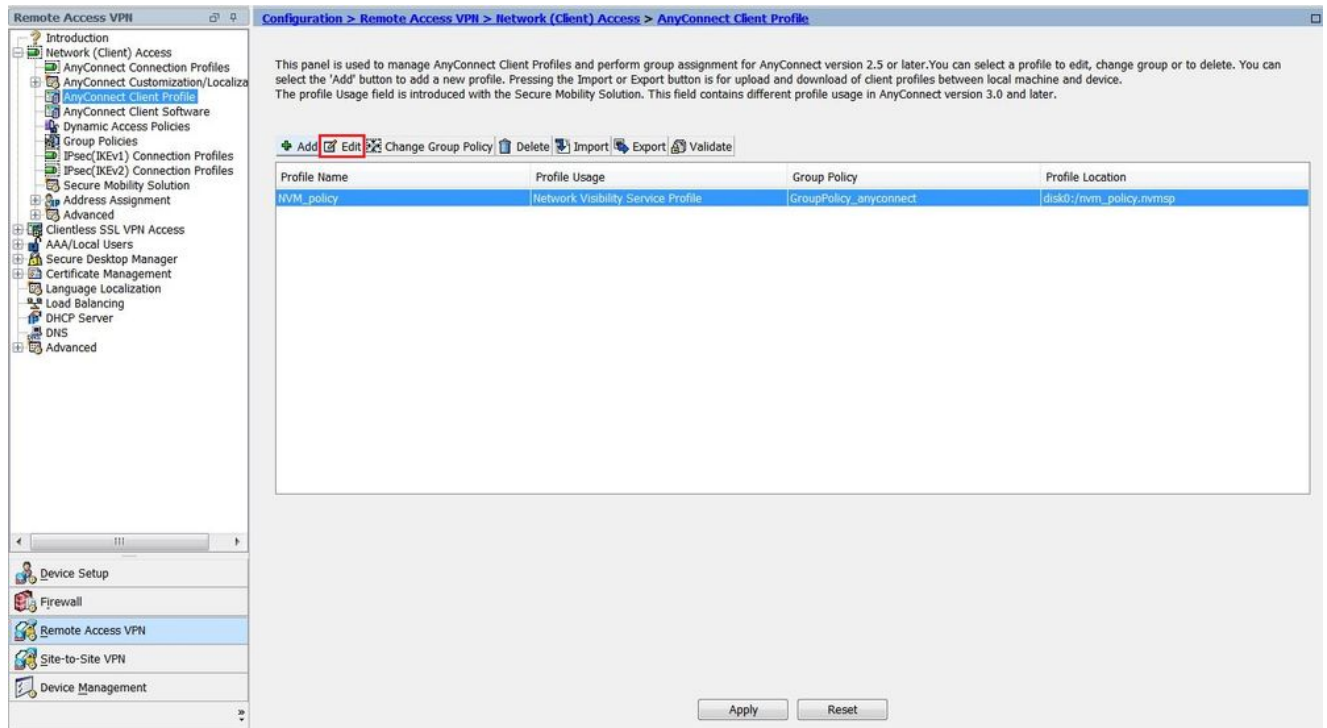


3. ةيؤرم دڤي صوت ددڤ ، تاف ي صوت ل م ادڤتس إ ي ف . م س اب في ر ع ت ل ا ف ل م ة ي م س ت ب م ق . ة ك ب ش ل ل .

4. ي م د خ ت س م ل ب ق ن م ا ي ل ا ح ة م د خ ت س م ل ا ة و م ج م ل ا ة س ا ي س ل ف ي ر ع ت ل ا ف ل م ن ي ي ع ت ب م ق . ة ر و ص ل ا ي ف ح ض و م و ه ا م ك ، ق ف ا و م ق و ف ر ق ن ا و AnyConnect .

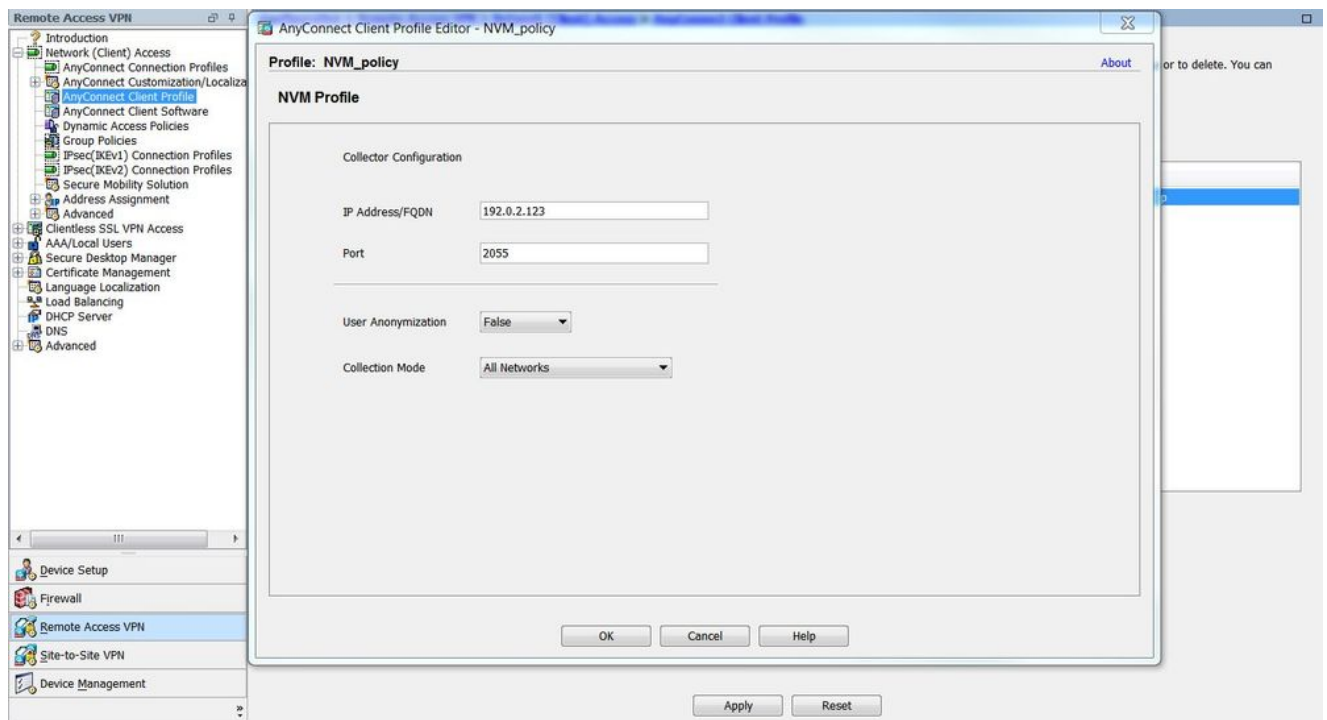


5. ة ر و ص ل ا ي ف ح ض و م و ه ا م ك ، ر ي ر ت ق و ف ر ق ن ا ، د ي د ج ل ا ج ه ن ل ا ء ا ش ن إ د ع ب .



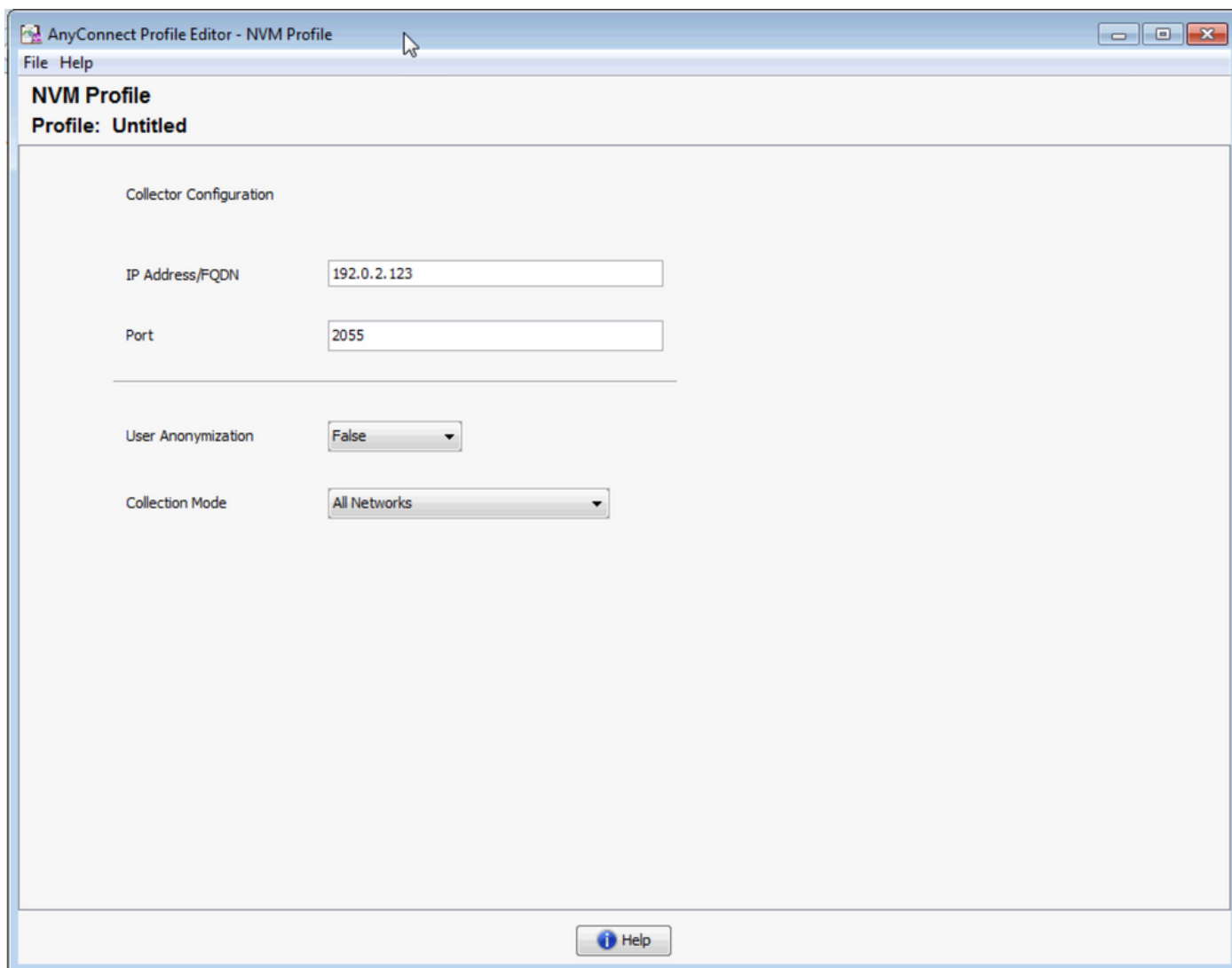
6. OK قوف رقنا مٲ ؛ذفنم الم مقروم مجمل ل IP ناونع لوح تام ول عمل لخدأ .

7. ةروصل ال ي ف حضوم وه امك ، قي بطت قوف رقنا .



AnyConnect في رعت فلم ررحم لال خ نم NVM لي م في رعت فلم نيوكت

م اذ ة قيرطال اذه لصف يو . Cisco.com بي ول ع قوم يلع رفوت ة لقت سم ةادأ يه ةادأل هذه ربع هؤاشن ا م تي يذل NVM في رعت فلم لي م حن نكمي . Cisco ISE ربع AnyConnect رشن ةي اهنال طاقن ال ةرشابم مخسن وأ ، Cisco ISE ال ةادأل هذه



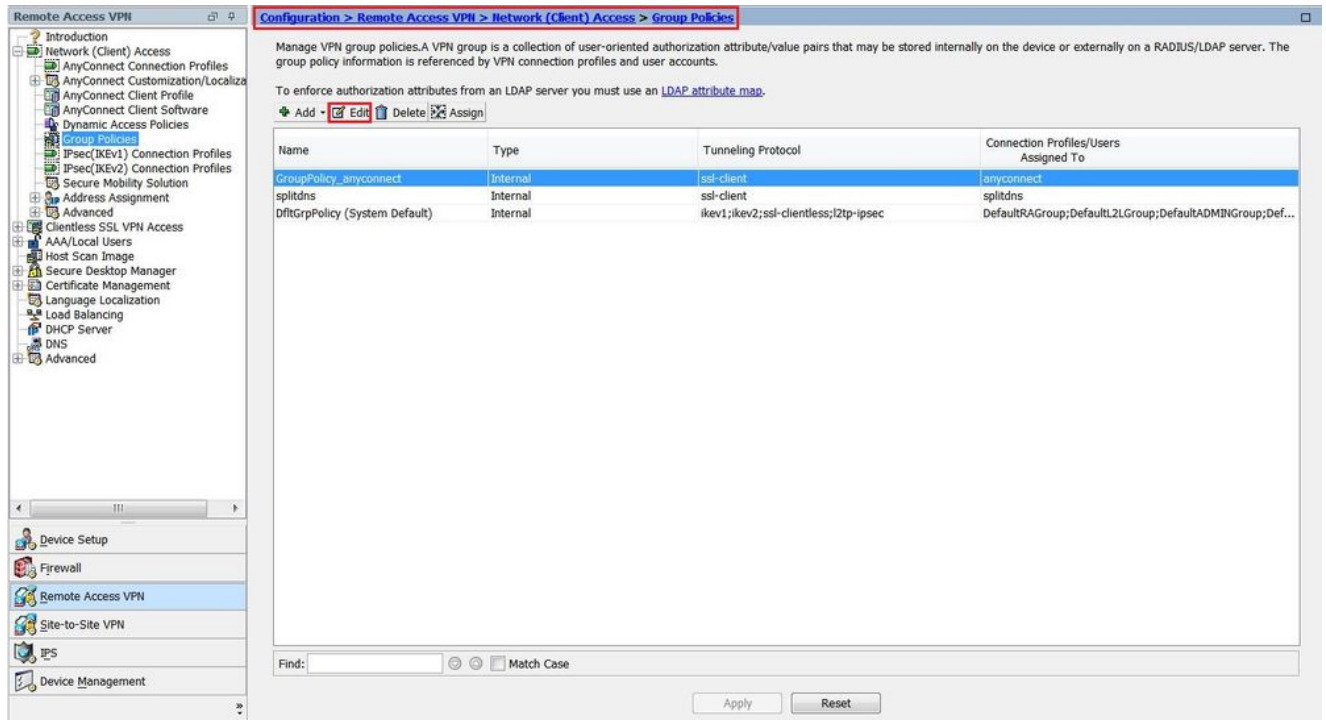
في رعت فلم ررحم ىل ع ةلي صفت تامول عمل تلحأ [AnyConnect](#).

## Cisco ASA ىل ع بيول ربع رشنل نيوكت

جاتحت كنأو، ASA ىل ع لعفلاب هنيوكت مت AnyConnect نأ ةينفلا ةطحالما هذه ضررت لوح ةلي صفت تامول عم ىل ع لوصحلل. طقف ةيطنل NVM ةدحو نيوكت ةفاضإ ىل [Cisco ASA Series VPN نيوكت لىلد: 3 مقر ASDM باتك](#) ىل ع جرا، AnyConnect، ASA نيوكت [7.16 رادصلال ASDM](#).

ةيلاتل تاوطخل اءارجاب مق، Cisco ASA ىل ع AnyConnect NVM ةيطنل ةدحول نيكم تل:

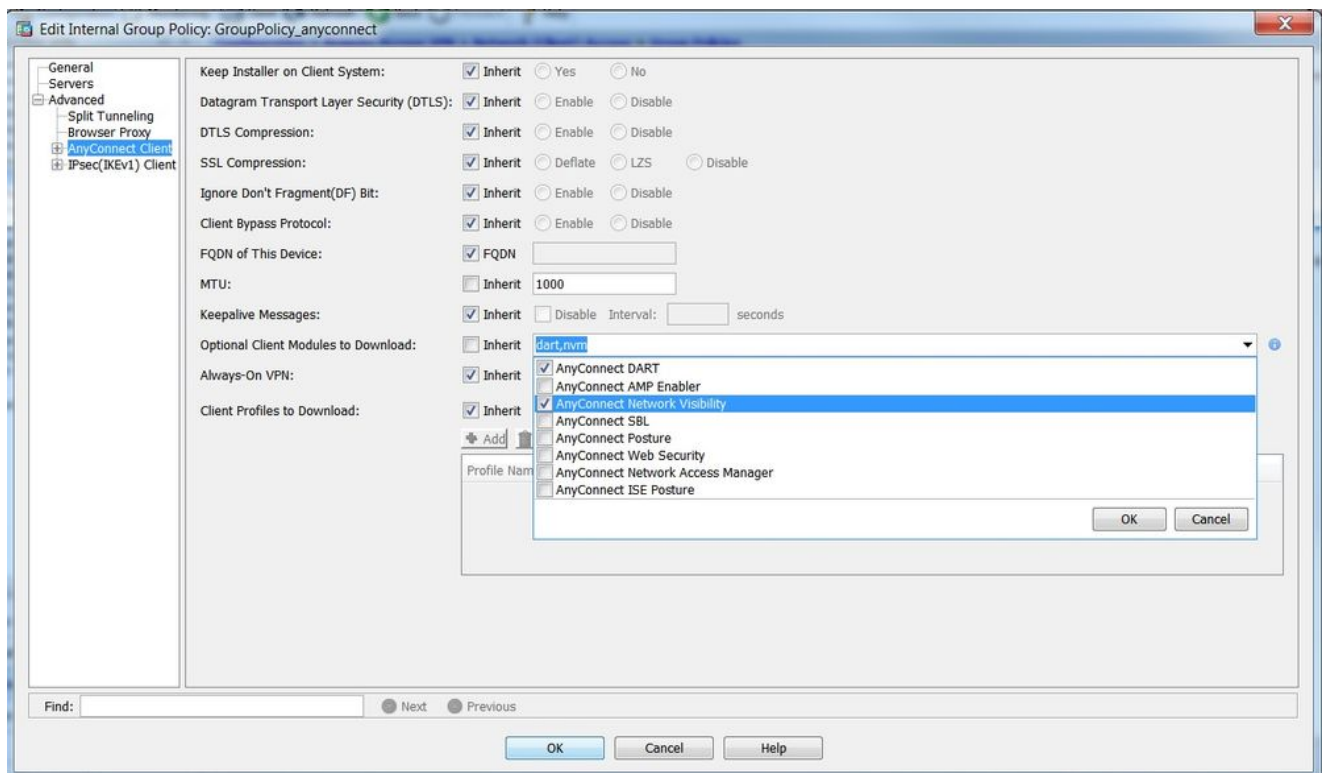
1. (للمعمل) Network > (ةكبشلا ىل لوصول) Remote Access VPN > نيوكتل ىل لقتنا Access > Group Policies.
2. ةروصلال يف حضوم وه امك، ريرحت قوف رقناو ةلصلال تاذه عومحمل ةسايس دح.



3. AnyConnect Client > م دق ت م ي ل ل ق ت ن ا ، ق ث ب ن م ل ا ة و م ج م ل ا ه ن ر ا ط ا ن م ض .

4. ة ي و ر ة ي ن ا ك م ا د ي د ح ت و ل ي ز ن ت ل ي ر ا ي ت خ ا ل ا ل ي م ع ل ل ة ي ط م ن ل ا ت ا د ح و ل ا ع ي س و ت ب م ق .  
AnyConnect ة ك ب ش .

5. ر ي غ ت ق ب ط و o k ة ق ط ق ط .



Cisco ISE ي ل ع ب ي و ل ا ر ب ع ر ش ن ل ا ن ي و ك ت

م ز ح و ا ه ت ا ف ي ص و ت و AnyConnect ل ي م ع ت ا د ح و ن ي ك م ت ب م و ق ن ، م س ق ل ا ا ذ ه ي ف

4. AnyConnect NVM فيرت فلم ةفاض:
1. NVM لي مع فيرت فلم لي محتو لي كول دراوم > ةفاض دح.

Identity Services Engine

Home Operations Policy Guest Access Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Profiling

Posture

Client Provisioning

Resources

Agent Resources From Local Disk > Agent Resources From Local Disk

Agent Resources From Local Disk

Category: Customer Created Packages

Type: AnyConnect Profile

Name: AnyConnect Network Visibility

Description:

Browse... NVM\_serviceProfile.xml

Submit Cancel

5. AnyConnect نيوكت فلم ةفاض:

1. AnyConnect نيوكت رتخاو ةفاض قوف رقنا.

ةقباسلا ةوطخلا يف اهلي محتب تمق يتلا ةمزال دح

Identity Services Engine

Home Operations Policy Guest Access Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Profiling

Posture

Client Provisioning

Resources

Resources

Selected 0 | Total 56

| Name                                        | Version        | Last Update         | Description                         |
|---------------------------------------------|----------------|---------------------|-------------------------------------|
| Agent resources from Cisco site             | 1.0.0.46       | 2015/10/08 02:24:16 | ISE 2.0 Supplicant Provisioning ... |
| Agent resources from local disk             | Not Applicable | 2015/10/08 02:24:15 | Pre-configured Native Supplicant... |
| Native Supplicant Profile                   | 1.0.0.36       | 2015/10/08 02:24:15 | ISE 2.0 Supplicant Provisioning ... |
| AnyConnect Configuration                    | 4.9.0.28       | 2015/12/16 15:25:11 | NAC WebAgent (ISE 1.1.3 release)    |
| Mac NAC Agent or AnyConnect Posture Profile | 1.0.0.30       | 2015/12/16 15:25:17 | Supplicant Provisioning Wizard f... |
| WebAMP Enabler Profile                      | 4.9.0.24       | 2015/12/16 15:25:24 | NAC WebAgent (ISE 1.1.1 or later)   |
| MacOsXSPWizard 1.0.0.30                     | 4.9.0.661      | 2015/12/16 15:25:32 | NAC Posture Agent for Mac OS ...    |
| WebAgent 4.9.0.24                           | 3.6.10255.2    | 2015/12/16 15:25:37 | MACAgent ComplianceModule v...      |
| MacOsXAgent 4.9.0.661                       | 4.9.0.1006     | 2015/12/16 15:25:44 | NAC Posture Agent for Mac OS...     |
| MACComplianceModule 3.6.10255.2             | 4.9.0.52       | 2015/12/16 15:25:52 | NAC Windows Agent (ISE 1.1.3 ...    |
| MacOsXAgent 4.9.0.1006                      | 4.9.0.1009     | 2015/12/16 15:26:06 | NAC Windows Agent (ISE 1.2 rel...   |
| NACAgent 4.9.0.52                           | 4.9.4.3        | 2015/12/16 15:26:21 | NAC Windows Agent - ISE 1.2, I...   |
| NACAgent 4.9.0.1009                         | 3.6.10255.2    | 2015/12/16 15:26:39 | AnyConnect Windows Complian...      |
| NACAgent 4.9.4.3                            | 4.9.5.4        | 2015/12/16 15:26:49 | NAC Windows Agent - ISE 1.2 a...    |
| AnyConnectComplianceModuleWind...           | 4.9.5.10       | 2015/12/16 15:27:05 | NAC Windows Agent - ISE 1.2.1 ...   |
| NACAgent 4.9.5.4                            | 4.9.0.42       | 2015/12/16 15:27:19 | NAC Windows Agent (ISE 1.1.1 ...    |
| NACAgent 4.9.5.10                           | 1.0.0.21       | 2015/12/16 15:27:29 | Supplicant Provisioning Wizard f... |
| NACAgent 4.9.0.42                           | 4.9.0.1005     | 2015/12/16 15:27:34 | NAC WebAgent (ISE 1.2 release)      |
| MacOsXSPWizard 1.0.0.21                     | 4.9.5.8        | 2015/12/16 15:27:43 | NAC Windows Agent - ISE 1.2 a...    |
| WebAgent 4.9.0.1005                         | 4.9.5.7        | 2015/12/16 15:27:59 | NAC Windows Agent - ISE 1.2 a...    |
| MacOsXAgent 4.9.5.8                         |                |                     |                                     |
| NACAgent 4.9.5.7                            |                |                     |                                     |

2. ةسايسلا ىلإ ةفاضلاب، ةيظمنلا AnyConnect ةدحو ديحت يف NVM نيوكت محتب مق. ةبولطملا

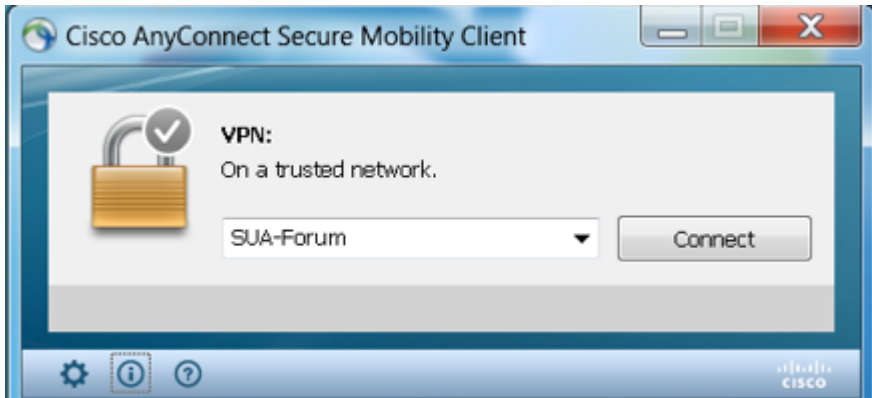
**رشن** ىلا عجرا Cisco ISE، ىلع بيولا رشن نيوكت لوح ةيليصف تاملولعم ىلع لوصحلل [بيولا ىلع AnyConnect](#).

## ه ب قووثومل ةكبشلل فاشتكا

وهو. اه ب قووثوم ةكبش ىلع نوكل ام دنع طقف قفدتل تاملولعم AnyConnect NVM لسري يف ةياهنل ةطقن تناك اذا ام ةفرعمل AnyConnect ليمعب ةصاخل TND ةزيم مدختسي ال ما اه ب قووثوم ةكبش.

AnyConnect ليمعب فيرعت فلم يف "TND) اه ب قووثومل ةكبشلل فاشتكا" نيوكت متي دي ق VPN ةكبش نوكم ناك اذا امع رظنل اضغب، VPN ةكبشل همادختسا متي يذلا (XML) ةسايس "مسق نيوكت لال خ نم TND نيكم متي. ال ما ةئيبل يف ايلاح مادختسالال DNS لاجم رشن بجي. فيرعتل فلم يف "ةيئاقللتل (VPN) ةيراهظال ةصاخل ةكبشلل اهذختي يتل تاءارجال نييغت نكمي. لقأل ىلع ه ب قووثوم DNS مداخ وادحاو قووثوم لال خ نم DoNothing عضو ىلا اه ب قووثوم ةكبش ىلع هنأ ليمعل ددحي ام دنع AnyConnect ه ب قووثومل ريغو ه ب قووثومل ةكبشلل جهنل بحسلال.

| XML Profile (excerpt)                                                                                                                                                                                                                                                                                                                                                                  | ASDM PROFILE EDITOR (excerpt) |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| <pre> &lt;AutomaticVPNPolicy&gt;true &lt;TrustedDNSDomains&gt;demo.local&lt;/TrustedDNSDomains&gt; &lt;TrustedDNSServers&gt;10.1.100.10&lt;/TrustedDNSServers&gt; &lt;TrustedNetworkPolicy&gt;DoNothing&lt;/TrustedNetworkPolicy&gt; &lt;UntrustedNetworkPolicy&gt;DoNothing&lt;/UntrustedNetworkPolicy&gt; &lt;AlwaysOn&gt;false &lt;/AlwaysOn&gt; &lt;/AutomaticVPNPolicy&gt; </pre> |                               |



هـ. [قوتوملا ءكبشلا فاشتكا لوح](#) عجار ،TND نيوكت لوح ءيفاضا لى صافات ىل ع لوصحلل

## رشنلا

ءىلاتلا تاوطخل AnyConnect NVM لى رشن بلطتى

1. Cisco ASA/ISE لى AnyConnect NVM نيوكت .
2. ءيفاضالا ءفىظولا فى همزح مئى - Linux لى AnyConnect NVM عمجم IPFIX عمجم نوكم دادعاب مق (TA).
3. TA ءيفاضالا ءفىظولا و CESA قىببطت مادختساب Splunk دادعاب مق .

### Cisco ASA/ISE لى AnyConnect NVM نيوكت . 1 ءوطخل

ءنئسملا اءه فى [نىوكتلا](#) مسق فى لى صفتلاب ءوطخل هءه ءىطغت تمئ

ءالمئل ءىهانلا طاقن ىل ائىائلئ رشن نكمى ،Cisco ISE/ASA لى AnyConnect NVM نيوكت ءعب

### (AnyConnect NVM عمجم IPFIX عمجم نوكم دادعاب) 2 ءوطخل

نعو ،ءىهانلا طاقن نم اهئمئرتو IPFIX تاناىب ءىمءى نمء الوؤسم عمجملا نوكم ءعى [نم \(CESA\) ءىفرطلا ءطقنلا ناما تالىلئ ءىفاضالا ءفىظولا](#) ىل تاناىبال هئءوئ ءءاع نئمضئ مئى . تب 64 راءصا Linux لى ءىغشئلا ماظن لى AnyConnect NVM عمجم لمءى . [Cisco ل Splunk](#) لى ءىغشئلا ماظن تىبئئ ءمارب مادختسا نكمى امك . CentOS و Ubuntu و Docker ءىغشئلا ماظن لى CentOS ءمارب Fedora و Redhat ءمارب فى نىوكتلا تافلمو ءىصنلا CentOS

ماظن ىل ع اما عمجملا لى ءىغشئ بءى ،ئاسؤسملا ىوتسم ىل ع ءوزوم ءىءؤمن رشن ءىلمء فى نكمى امك . تب 64 Linux ماظن ىل ع لمءئ ىل ع [Splunk for Order](#) ءءق و لئقئسم تب 64 Linux Splunk تانوكم نوئب لئقئسم مءاخ ىل ع عمجملا تىبئئ

 NVM عمجم نمضئى تب 64 راءصا ءحاو Linux ماظن ىل ع لءلا لى ءىغشئ نكمى امك :ءظءالم ضرءلا ضارءال و ءرىغص رشن تالىلمء فى مادختسالل Splunk Enterprise تانوكمو ءطقن 10000 ىل لى لى ءلوهسلا ءىاغ فى تاناكمالا ءىمء ربئعى . ءىءىضوئلا POV مءء ءىءئ تامولعم ىل ع لوصحلل [Real Client POV](#) ىل عجار . ءىهان

## تانايايبل عمجم تيبتت ةيفي

1. ديري تايح ماظنلإ إلإ، (TA ةيفاضإلإ ةيفيظولأ عم نمضم) ليلد NVM/appserver/addon/ acnvmcollector.zip فلم خسنا 1. هتيتبتت.

2. تافللمل جارختسال acnvmcollector.zip فلم طغض اغللإب مق.

ذيفنتب موقوي نأ لباق zip. ةمزح في \$PLATFORM\$\_README فلم ةءارق نسحتسمل نم تادادعإ نع تامولعم \$PLATFORM\$\_README فلمل رفوي. install.sh يصنلإ جمآنربلل جمآنربلل ذيفنت لباق (رملأل مزل إذا) اهلديعتو اهنم ققحتلل مزل في تلال ةلصلل تاذا نيوكتلل هيحوت ةءاعإب موقت فيذل Splunk ليثم ناوئع نيوكتل إلل لقلأل لعل جاتحت. install.sh يصنلإ عمجملل ليغشت في حيحص لكشب ماظنل نيوكتل في لشلل ببست في دق. هيلإ تانايايبلل حيحص ريغ لكشب.

 UDP رورم ةكرحب حامسلل ةفيضملا ةيامحلل نارذو كتكبش نيوكتل نم دكأت: ةطحال IPFIX رورم ةكرحل ةيامحلل نارذو حمست نأ بجي. ذفانملاو ةهوجلل و ردصملا نيوانعل إلل ةرداصل UDP تانايايبلو تانايايبل عمجم إلل AnyConnect ءالمع نم ةدراول (CFLOW) Splunk.

حيحص ماظنل لعل ةيناثلل في قفدت 5000 نع لقي إلل ام ةجلاعم دحاو NVM عمجم ليثمل نكمي لباق هليغشتو عمجملل نيوكتل بجي. ةياهن ةطقن 4000 إلل 35000 إلل لصي ام وأ، مءجلل ققبتتال إلل TA-Add و NVM Splunk مادختسا.

لعل NVM AnyConnect ةياهن طاقن نم تاقفدتال عمجملل لبقتسي، فيضارتفا لكشبو UDP 2055 ذفنم.

ميسقتلل تانايايبل تازجوم ةثالث تانايايبل عمجم جتن في، كلذل إلل ةفاضلإابو

- UDP 20519 ذفنم لعل قفدت لكل تانايايبل
- UDP 20520 ذفنم لعل ةيفرطال ةطقنل ةيوة تانايايبل
- UDP 20521 ةيفرطال ةطقنل ةهجاو تانايايبل ذفنم

acnvm.conf فلم ريغيغتب مق، كلذب مايقلل. تانايايبلل زجومو فيقلتلل ذفانم ريغيغت نكمي طاقن نيبل ةكبشلل/فيضملل ةيامحلل نارذو نأ نم دكأت. تانايايبلل عمجم ليثم ليغشت دءأو فيتلل نيوانعلو UDP ذفانم ءحوتف Splunk (ةمظنأ) ماظنو عمجملل نيبل وأ عمجملاو ةياهنل تانايايبل عمجم نيوكتل قباطي كيذل AnyConnect NVN نيوكتل نأ نم اضيأ دكأت. اهن نيوكتل مت كيذل.

ققبتت لءاذا نم تاميللعتال تافللم مسق إلل عءرا، اهلديغشتو تانوكملل عيمج تيبتت دعب تانايايبلل جذومنو اقابس م ءنوكملل ريقاتل لول ةيليصفت تامولعم لعل لوصحلل Splunk لءال ةطساوب اهؤاشن مت فيتلل تامولعملل رصانعو.

تانايايبلل رورم ةكرح لاسرا نم ققحتللو AnyConnect ةياهن طاقن يءا ليغشت ةءاعإ كنكمي نم تباث قفدت ليغشتل youtube.com مادختسا كنكمي، لاثملل لبس لعل. لءال إلل تانايايبلل.

acnvm.conf نيوكت فلم ي ف تامولعمل هذه نيوكت بجي:

- syslog\_server\_ip (سپلنك و اردصم ليثم) 127.0.0.1 ىل اءراشال نكمي: (LOCALHOST) ع برمل سفن ىل ع ناك اذا.
- اءب ساء ال ءيضا رءفال ءميقل: (ءءراول IPFIX ءانايب) ع مءمل عامءسال اءفنم.

 ءمءال ءهءاول مءءءسي وهو. نيوكتل فلم نم netflow\_collector\_ip فءء مءي: ءءءالم يلى م IP مءءءساب ءيضا رءفال ءميقل زواء لء نم طقف هريءي ء بجي و ءيضا رءفال اءءءم.

ءطقن ءهءاول ءانايب و ءيها نل ءطقن ءي وه ءانايب اءفنم و قءء لك ءانايب اءفنم نيوكت مء ءريء يءبني ءنأ. نيوكتل فلم ي ف ءيضا رءفال ءاءاءل اقبسم ع مءم و ءيها نل اءريصقء ريء ءانيم ءنأ لمءءسي نل ءميقل اءه.

ءءم لىكشءل ي ف ءمولعم اءه ءفضأ: /opt/acnvm/conf/acnvm.conf

ءءم DTLS

 نم ءيزم ىل ع لوصءلل ءنءسم ال اءه ي ف [NVM ل DTLS مءء نيوكت](#) عءار: ءءءالم لىصافءل.

ع مءم ال فىضا ءسي نأ قوءءصل ال ىل ع steps اءه ءءءنأ:

- /opt/acnvm/certs: لىلءل اءه لءء.
- لىلء ي ف ءاءفم لاء ءءاءش ل طفاء، ءاءاءش ل ع مءم ىل ع ءءاءش ل قىببء لء نم /opt/acnvm/certs.
- sudo: رمأل اءه مءءءساب acnvm:acnvm ىل ءاءلءم ل ءومءم و ءلءم لك لالم ريءي ءب مق chown -R acnvm:acnvm certs/:
- ءاءفم لاء ءءاءش ل مءءءساب acnvm.conf ل مسقل اءه نيوكت بجي.
- sudo systemctl restart: ءانايب ل ع مءم لىءشء ءءاءب مق، ءءاءش لاء نيوكتل ءضو ءعب acnvm.service
- sudo systemctl status acnvm.service: ءانايب ل ع مءم ءلء نم ققءء

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

نيوكتل ءيقب يلى امي ف:

```
"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
}
```

- `(sudo ./install.sh)` زيمتم الم مدختسم الم تازايتما ب `install.sh` رمأل ذي فنتب مق



ي صننل جم انربل لي غشتل رذل و ا تانوذأل هذه ل باسحل جاتحي :عظالم `install.sh` م د خ باسحب ة صاخل تانوذأل و `ACNVM`.

Cisco نم (CESA) ة ف رطل ا ة طقنل ا نام ا تاليلحت قي بط ل ل ع ج را ، تامولعمل نم دي زم ل (ل ي ص اف ت ل ل) Splunk ل ع ل و ص ح ل ل .

ة ف ا ض ا TA ة ف ي ط و و CESA تامولعمل ة ح و ل م اد خ ت س اب م ي س ق ت دادع ل 3 ة و ط خ ل

ر ي ر ا ق ت ق ي ب ط ت ل ا ذ ه ر ف و ي . Splunkbase ل ع Splunk ل AnyConnect NVM ق ي ب ط ت ر ف و ت ي ر ي ر ا ق ت ي ف ة ي ا ه ن ل ط ا ق ن نم IPFIX (NVZflow) ت ا ن ا ي ب م د ق ت تامولعمل ت ا ح و ل و ا ق ب س م ة د د ح م . ة ي ا ه ن ل ة ط ق ن و م د خ ت س م ل ك و ل س ط ب ر ل ع د ع ا س ت م اد خ ت س ل ل ل ب ا ق

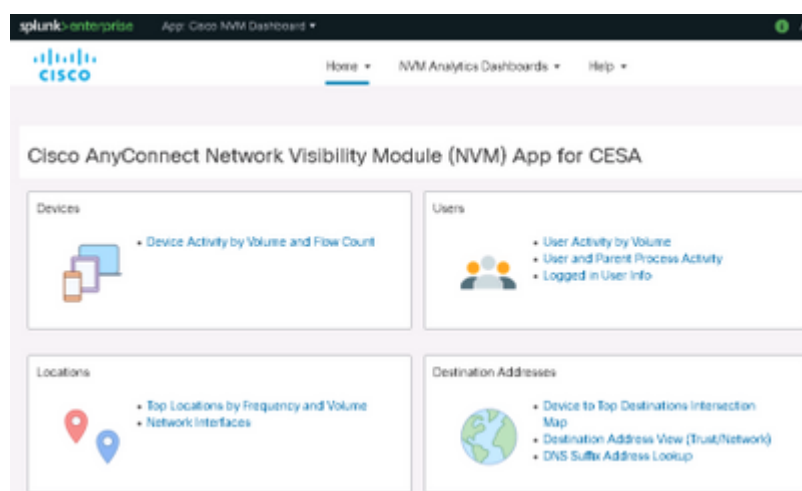


ي ف ن ي ق ي ب ط ت ل ا ل ك ت ي ب ث ت م ت ي ، ع ا ر ط ن ل ا ة و م ح م ر ش ن ت ا ي ل م ع ل ة ب س ن ل ا ب : ع ظ ا ل م ت ي ب ث ت م ت ي . ( ه ج و م ل م ) ع ق و م ل ي ف ط ق ف TA ت ي ب ث ت م ت ي . ع ا ر ط ن ل ا ة و م ح م ل ي ث م ل . ص ف ن م Linux/Docker ع ب ر م ل ع و ا ه ج و م ل م اد خ ت س اب ع ق و م ل ي ف ع م ح م ل

ل ع و ا د ح و ع ب ر م ي ف ت ا ق ي ب ط ت ل ا و ت ا ن و ك م ل ا ة ف ا ك ت ي ب ث ت ك ن ك م ي ، ي ل ح م ل ت ي ب ث ت ل ل ( د ن ت س م ل ا ذ ه ي ف ر ش ن ل ا ل ع ة م ا ع ق ر ط ن ) م س ق ي ف ت ا ط ط خ م ل ع ج ا ر . ة ل ص ف ن م ت ا ع ب ر م

ت : اف ل م ل ا ذ ه ل ي ز ن ت ب مق

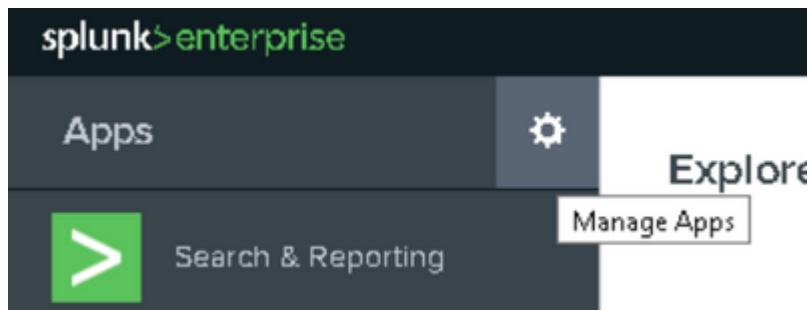
- [Splunk ل Cisco نم \(CESA\) ة ف رطل ا ة طقنل ا نام ا تاليلحت قي بط ل](#)



- [Cisco ل Splunk \(CESA\) ةف رطال ةطقنل نام ةال لحتل ةف فاضل ةف رطال](#)

## Install رمال

1. هليزنت مت يذل tar.gz فلم تي ب ثب مق و زاهل قوف رقنا Splunk > Apps ل ل قتنا .  
"تاقب طال" مسق ل خاد ثحبأ و Splunkbase نم



2. ةلم عل س فن ب ةف فاضل ةف رطال تي ب ثب مق .
3. Cisco NVM تامول عم ةحول نم لك تي ب ثب دي كأتل Splunk تاقب طت ةحفص ضرع  
Cisco NVM ةفاضل Splunk.

| splunk>enterprise Apps                 |              |         |                 |         |                                   |                                   |
|----------------------------------------|--------------|---------|-----------------|---------|-----------------------------------|-----------------------------------|
| Apps                                   |              |         |                 |         |                                   |                                   |
| Showing 1-2 of 2 items                 |              |         |                 |         |                                   |                                   |
| <input type="text" value="cisco nvm"/> |              |         |                 |         |                                   |                                   |
| Name                                   | Folder name  | Version | Update checking | Visible | Sharing                           | Status                            |
| Cisco NVM Dashboard                    | CiscoNVM     | 3.1.0   | Yes             | Yes     | App   <a href="#">Permissions</a> | Enabled   <a href="#">Disable</a> |
| Cisco NVM Add-on for Splunk            | TA-Cisco-NVM | 3.0.9   | Yes             | No      | App   <a href="#">Permissions</a> | Enabled   <a href="#">Disable</a> |

ربع UDP [تالخدم ني كم ت](#) عجار Splunk ل تانايب زجوم ةثالث يضا رتفال ني وكتال ملتسي (دنتسمال اذه يف [SPLUNK ةرادا مدختسم ةهجاو](#)).

- UDP 20519 ذفنم يل ع تانايب قفدت لكل
- UDP 20520 ذفنم يل ع ةف رطال ةطقنل ةي وه تانايب
- UDP 20521 ذفنم يل ع ةي هالنل ةطقن ةهجاو تانايب

Splunk sourcetypes ل هذ تانايب ل تازجوم ني عتب لك لذ دب ةف فاضل ةف رطال موقتو  
cisco:nvm:flowData، وCisco:nvm:sysdata، وCisco:nvm:ifdata، يل لاولتال.

Splunk ةرادا مدختسم ةهجاو ربع UDP تال خاد ني كم ت

هذه حرش متي .دربم conf.لخدم قي رط نع لخدم UDP تنكم اضيأ عي طتسي تنأ :ةظحال  
نم NVM تامول عمل ةحول قي بطتل (GUI) ةي موسرل مدختسمال ةهجاو يف قي رطال  
(تاميل لعل لسأ) Cisco.

Splunk. جمانرب ليغشت ةداعإ ىلإ جاتحت ال

1. UDP > تانايبلا لادإ > تادادعإ > Splunk ىلإ لقتنا .
2. لثامي لا ددح > كلذ دعب تقطقط > دوقفم # ءانيم لخدي > يلحم UDP ديدج تقطقط .  
لاسرا ةقطقط > ةعجارم ةقطقط > عون ردصم .
3. (ةخسن مادختسا كنكمي) .نيرخآلا نيدفنملل ررك .

Add Data

< Back

Submit >

Select SourceInput SettingsReviewDone

Review

Input Type

UDP Port

Port Number

20519

Source name override

N/A

Restrict to Host

N/A

Source Type

cisco:nvm:flowdata

App Context

search

Host

(IP address of the remote server)

Index

default

splunk> R Apps ▾

UDP

Data inputs » UDP

New

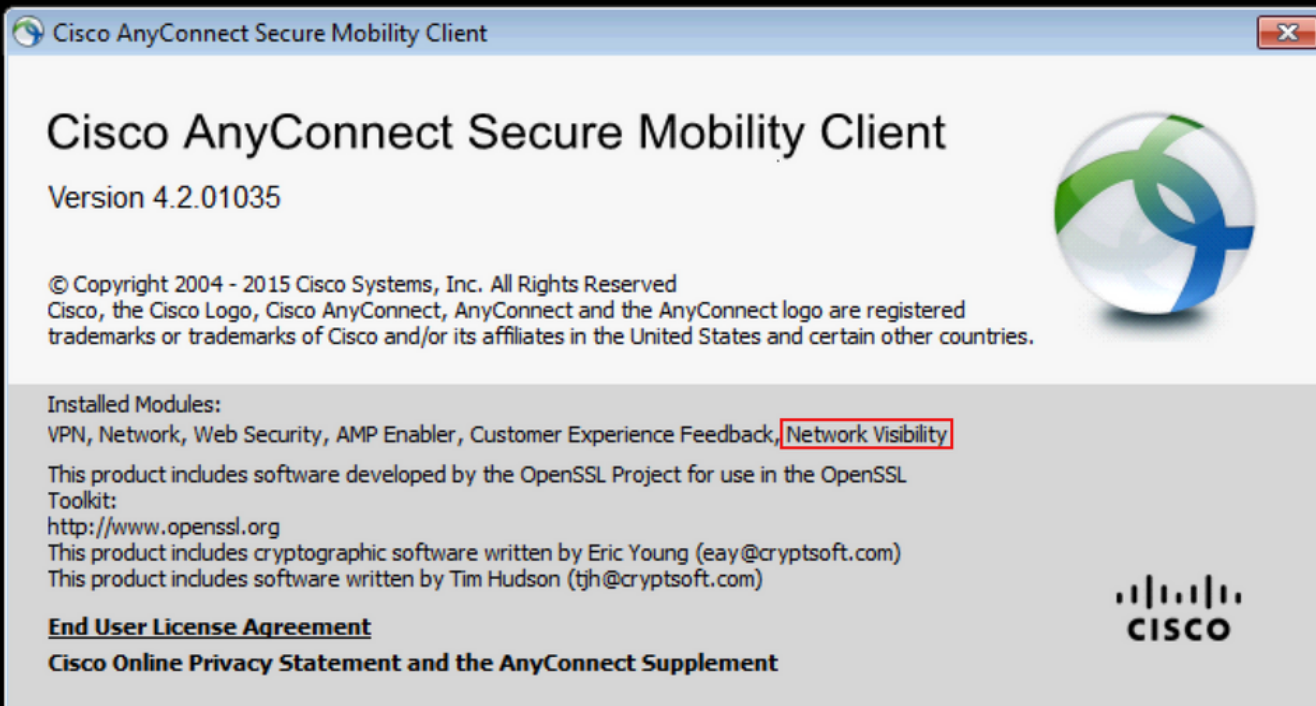
Showing 1-3 of 3 items

| UDP port ⇅ | Source type ⇅      | Status ⇅ |
|------------|--------------------|----------|
| 20519      | cisco:nvm:flowdata | Enabled  |
| 20520      | cisco:nvm:sysdata  | Enabled  |
| 20521      | cisco:nvm:ifdata   | Enabled  |

## ةحصل نم ققحتلا

### AnyConnect NVM تيبتت ةحص نم ققحتلا

تادحول اي ف ةكبشلا ةيؤر ةيناكمإل ةيظمنلا ةدحولا جاردإ بجي ،حجانلا تيبتتلا دعب  
AnyConnect Secure Mobility Client اي تامولعمل مسق لخاد ،ةبثمل ةيظمنلا



ليدل في فيرعت الت فلم دوجو نمو ويةهالنل ةطقن ىلع NVM ةمدخ ليغشت نم اضيأ ققحت بولطملم.

## عمجمملا ةلاح ةحص نم ققحتل

لبقتسي عمجمملا نأ ةلاحل هذه نمضت ". (ليغشتل ديق) ةطشن" عمجمملا ةلاح نأ نم دكأت ةطشن ريغ تانايبل عمجم ةلاح تناك اذا. تاقوالا عيجم في ويةهالنل طاقن نم IPFIX/cflow، ذيفنتلاب هل حمست فلملل لوصولو باسح تانوذأ نأ نم دكأتف:

- /opt/acnvm/bin/acnvmcollector

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

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

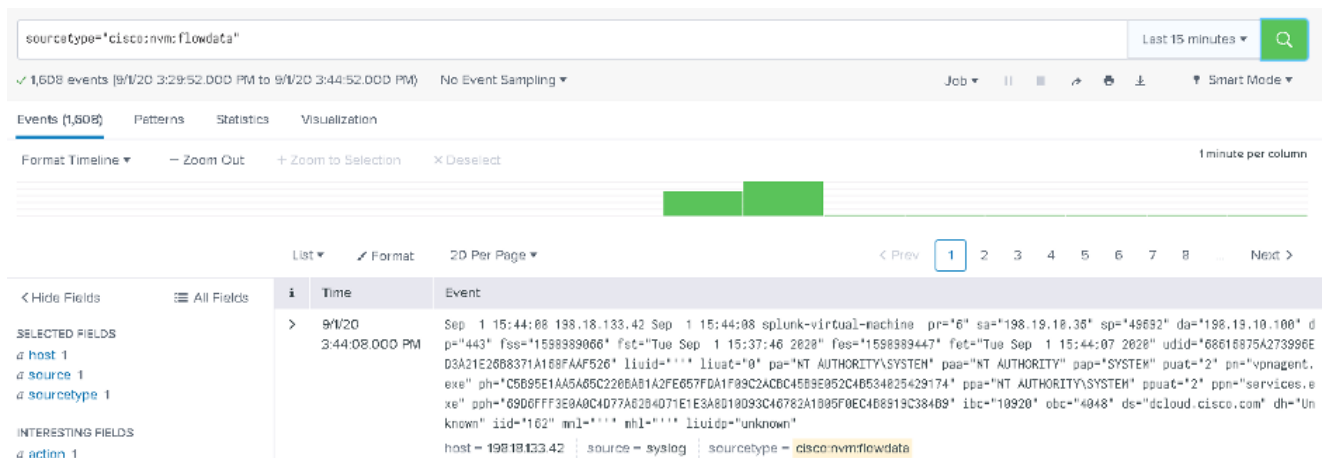
```
[splunk@splunk-virtual-machine addon]$ systemctl status acnvm.service
● acnvm.service - AC NVM Service
   Loaded: loaded (/usr/lib/systemd/system/acnvm.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2020-06-19 13:48:08 EDT; 25s ago
     Main PID: 41165 (acnvmcollector)
        Tasks: 13 (limit: 49772)
       Memory: 1.8M
      CGroup: /system.slice/acnvm.service
              └─41165 /opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/co>
                 41176 /opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/co>
                 41177 /opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/co>
                 41178 /opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/co>
                 41179 /opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/co>
lines 1-12/12 (END)
```

## CESA تامولعم ةحول - Splunk ةحص نم ققحتلا

فاشكتسأ ةيفيك لوح قئاتو ىلع لوصحلل .ةلصلل اذامدخو Splunk ليغشت نم دكأت ببول ىلع Splunk عقوم ىلا عجرا ،اهالصلو Splunk اطاخأ

،ةلولأا تانايبلا مالئسإ دعب قئاتد سمخ ىتح CESA ل تامولعمل تاحول ثيدحت متي ال اروف يودي ثحب ليغشت كنكمي ،كلذ عمو .يئاقلل ليغشتلل يصن جم انرب ببسب كلذو :تانايبلا يقلت نم ققحتلل

1. ريراقت دادعإو ثحب قوف رقنا ،ميسقتلاب ةصاخلا ةيسيئرلا تامولعمل ةحول نم .
2. ةبولطملا تانايبلا علمل حيحصلا قاطنلا نييعتب مق ،ةيلاتلا ةشاشلا يف .
3. sourcetype="cisco:nvm:flowdata" :لخدأ ،ثحبلا لقح يف .



:تانايبلا يقلت CESA تامولعم ةحول نأ نم ققحت ،ةلولأا سمخل قئاتدل دعب

1. تاليلحت تامولعم ةحول ىلع رقنا ،ميسقتلاب ةصاخلا ةيسيئرلا تامولعمل ةحول نم . Cisco نم ةيفرطلا ةطقنل نامأ
2. ةيلاتلا تادادعإلاب ظافتحالا ديرت تنك اذا قفدتلاو مچحل بسح زاهجلا طاشن ىلع رقنا .
3. تاموسرلاو تانايبلا تامولعمل ةحول ضرعت .لاسرا قوف رقنا .

### ةمزلحلا قفدت

1. AnyConnect ةيطمنلا ةحوللا ةطساوب ليمعلا ةياهن طاقن ىلع IPFIX مزح عاشنإ متي . NVM.
2. عجمحمل IP ناوئع ىلا IPFIX مزح لاسرلاب ليمعلا موقوي .
3. Splunk ىلا اوهيجوت ةداعإو تامولعمل عيمجتب عجمملا موقوي .
4. لك تانايب :ةفلتخم تاقفدت ةثالث ىلع Splunk ىلا تانايبلا رورم ةكرح عجمملا لسري . ةهجاولا تانايبو ةياهنلا ةطقن تانايبو قفدت .

مت تانايبلا نأب ةمزلحلا قفدت يف رارقإ دجوي ال كلذل ،UDP ىلا رورملا ةكرح عيمج دنتست

اهل ابلقتسا.

رورملا ةكرحل ةيضا رتفالال ذفانملا:

- IPFIX 2055 تانايب
- 20519 تانايب قفدت لكل
- 20520 ةياهنلا ةطقن تانايب
- 20521 ةهجالا تانايب

يف نوكت امدنع عمجم ىل اهل اسرلاو IPFIX تانايب ني زختب NVM ل ةيظمنلا ةدحولل موقت ةكبش ب الصتم لومحمل رتوي بمكلال نوكي امدنع كولسلال اذه ثدحي. اهب قووثوم ةكبش VPN. ةكبش ربع الصتم نوكي امدنع وا (ايلاح) ةكرشلال

مق، كلذب مايقلل. ةيظمنلا NVM ةدحو نم مزحلل لبقتسي عمحمل نا نم ققحتل كنكمي نم ققحتلل، كب صاخلا نيوكتل بسح، ةني عم UDP ذفانم ىلع ةمزحلل طاقنلا ليغشتب، Splunk System Linux OS ماظن لالخنم ققحتل اذه عارجا متي و. مزحلل مالتسا

## قفدت بلالوق

هذه دعاست. IPFIX لاصتا ةيادب يف تانايب عمجم ىل IPFIX قفدت بلالوق لاسرا متي IPFIX تانايب مهف ىلع عمحمل بلالوقلا

مل اذا ىتح، تانايبلا عيزوت ةيناكم نامضل اقبس م بلالوقلا لي محتب عمحمل موقبي امك، لوكوتوربلل تاريغيغت عم ليمعلا نم ثدحاً رادصاً رادصاً قلاحي يف. بلالوقلا ليمعلا لسري، ليمعلا ةطساوب اهل اسرلا متي يتلا ةديجلال بلالوقلا عمحمل مدختسي

طورشلال هذه بجومب بلالوق لاسرا متي:

1. NVM ليمع فيرعت فلم يف ريغيغت كانه.
2. ةكبشلا يف ريغيغت ثدح كانه.
3. NetPoint ةمدخ ليغشت ةداعا تمت.
4. ةياهنلا ةطقن ليغشت ةداعا/ليغشت ةداعا متي.
5. NVM فيرعت فلم يف نوكم وه امك، (ةعاس 24=يضا رتفالال) يرود لكش ب.

هذه دحاً دهاشتس ف، فقوملا اذه ثدح اذا. بلالوق ىلع روثلعل عمحمل ىلع رذعتي، ةردان فورظ يف ضارعال:

- ةياهنلا ةطقن ىلع ةمزحلل طاقنلا يف بلالوق ىلع روثلعل متي مل هنأ ام
- تانايبلا عمجم تالچس يف قفدتلا ةومحمل بلالوق دجوتال وأ

.ةياهنلا طاقن ىدح ليغشت ةداعا ب مق، ةلكشملا هذه حالصال

## اهحالصا واطخالال فاشكتسا

اهحالصا واطخالال فاشكتسال ةيساسالال تاوطخالال يه هذه:

1. عمحمل او ليمعلا ةياهنلا ةطقن ني ب ةكبشلا لاصتا نامض.
2. اهميسقتو تانايبلا عمجم ني ب ةكبشلا لاصتا نامض.

3. لي م عمل اة ياهن ة طقن ىل ع حي حص لكشب NVM تي ب ثت نم دكأت .
4. IPFIX رورم ة كرح عاشنإ م تي ناك اذا ام ة فر عمل اة ياهنل ة طقن ىل ع طاقتل ا ق ي ب ط ت .
5. ناك اذا امو IPFIX رورم ة كرح ملت سي ناك اذا ام ة فر عمل م جم ىل ع طاقتل ا ق ي ب ط ت م ق . م ي س ق ت ل ا ىل ا رورم ل ة كرح ه ي ج و ت ة د ا ع ا ب م و ق ي .
6. رورم ة كرح ملت سي ناك اذا ام ة فر عمل Splunk ىل ع طاقتل ا ق ي ب ط ت .
7. ل DTLS:
  - ع م جم ل ا ة د ا ه ش ي ف ن و ق ث ي AnyConnect ا ل م ع ن ا نم دكأت .
  - NVM ف ي ر ع ت ف ل م ي ف "نمآ" ر ا ي خ ن ي ك م ت نم دكأت .
  - ت ا د ا ه ش ل ل ع م جم ل ا ن ي و ك ت نم دكأت .

Wireshark ي ف ح ض و م و ه ا م ك IPFIX رورم ة كرح

 ىل ع ة ي ف ص ت ل ا ك ي ل ع ب ج ي ف ، ع م جم ل ا و ل ي م ع ل ا ن ي ب DTLS ل ي غ ش ت ب ت م ق اذا : ة ط ح ا ل م DTLS رورم ة كرح .

| No. | Time | Source        | Destination  | Protocol | Length | Info                                                  |
|-----|------|---------------|--------------|----------|--------|-------------------------------------------------------|
| 1   | 0... | 192.168.100.1 | 10.76.76.161 | CFLOW    | 269    | IPFIX flow ( 227 bytes) Obs-Domain-ID= 127 [Data:258] |
| 2   | 0... | 192.168.100.1 | 10.76.76.161 | CFLOW    | 269    | IPFIX flow ( 227 bytes) Obs-Domain-ID= 127 [Data:258] |
| 3   | 0... | 192.168.100.1 | 10.76.76.161 | CFLOW    | 269    | IPFIX flow ( 227 bytes) Obs-Domain-ID= 127 [Data:258] |
| 4   | 0... | 192.168.100.1 | 10.76.76.161 | CFLOW    | 269    | IPFIX flow ( 227 bytes) Obs-Domain-ID= 127 [Data:258] |
| 5   | 0... | 192.168.100.1 | 10.76.76.161 | CFLOW    | 269    | IPFIX flow ( 227 bytes) Obs-Domain-ID= 127 [Data:258] |
| 6   | 2... | 192.168.100.1 | 10.76.76.161 | CFLOW    | 269    | IPFIX flow ( 227 bytes) Obs-Domain-ID= 127 [Data:258] |
| 7   | 0... | 192.168.100.1 | 10.76.76.161 | CFLOW    | 269    | IPFIX flow ( 227 bytes) Obs-Domain-ID= 127 [Data:258] |
| 8   | 1... | 192.168.100.1 | 10.76.76.161 | CFLOW    | 269    | IPFIX flow ( 227 bytes) Obs-Domain-ID= 127 [Data:258] |
| 9   | 2... | 192.168.100.1 | 10.76.76.161 | CFLOW    | 269    | IPFIX flow ( 227 bytes) Obs-Domain-ID= 127 [Data:258] |
| 10  | 2... | 192.168.100.1 | 10.76.76.161 | CFLOW    | 269    | IPFIX flow ( 227 bytes) Obs-Domain-ID= 127 [Data:258] |
| 11  | 2... | 192.168.100.1 | 10.76.76.161 | CFLOW    | 269    | IPFIX flow ( 227 bytes) Obs-Domain-ID= 127 [Data:258] |
| 12  | 0... | 192.168.100.1 | 10.76.76.161 | CFLOW    | 269    | IPFIX flow ( 227 bytes) Obs-Domain-ID= 127 [Data:258] |
| 13  | 0... | 192.168.100.1 | 10.76.76.161 | CFLOW    | 269    | IPFIX flow ( 227 bytes) Obs-Domain-ID= 127 [Data:258] |
| 14  | 2... | 192.168.100.1 | 10.76.76.161 | CFLOW    | 269    | IPFIX flow ( 227 bytes) Obs-Domain-ID= 127 [Data:258] |

## NVM (ة د ح و) AnyConnect ل ي م ع

ة طقن نم ت ا ن ا ي ب ل م ر ح ل ا س ر ا م ت ي ا ل و ت ا ن ا ي ب ل ا ع م جم ىل ا ت ا ن ا ي ب ل ا ن ع غ ا ل ب ا ل ا م ت ي ا ل اة ياهنل

ل ي ل د ي ف ة د ا ي ز ل ا ي ف (NVM.db) NVM ت ا ن ا ي ب ة د ع ا ق ف ل م م ج ح ر م ت س ي ل ه ك و ل س ل ا ا ذ ه ر ي ش ي و C:\ProgramData\Cisco\Cisco\AnyConnect Secure Mobility Client\NVM؟ ت ا ن ا ي ب ل ا ع م جم ىل ا ت ا ن ا ي ب ل ا م ر ح ل ا س ر ي ا ل AnyConnect NVM ل ي م ع ن ا ىل ا .

 ت ق و م ل ا ن ي ز خ ت ل ا ة ر ك ا ذ م ك ح ت ر ص ا ن ع و ت ق و م ن ي ز خ ت ت ا ي ل م ع ل و ح ة م و ل ع م ل ت ل ح ا : ة ط ح ا ل م 4.9 ر ا د ص ل ا ، cisco AnyConnect Secure Mobility Client Administrator ل ا ، ة ح ا ت م ل ا

```

Directory of C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM
07/02/2020 06:00 PM <DIR> .
07/02/2020 06:00 PM <DIR> ..
07/02/2020 05:54 PM      514 KConfig.dat
07/02/2020 06:00 PM 20,480 NVM.db
06/12/2020 08:36 PM    937 NVM_Service_Profile.xml
07/02/2020 06:00 PM      2 PersistedData.dat
               4 File(s)      21,933 bytes
               2 Dir(s)  6,818,320,384 bytes free

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\NVM>

```

(TND) ه ب ق و ث و م ل ا ة ك ب ش ل ا ف ا ش ت ك ا

دمتعت .اهب قوٲوم ةكبش ىلع ةدو؁وم اهانم دكأتو AnyConnect مدختسم ةه؁او لىغشتب مق نىوكت ببسى .اهب قوٲوم ةكبش نمض ةياهنل ةطقن نوكت ىتم فاشتكال TND ىلع NVM ةمصب ىلع لمعى ىذللو ،اهب صاخ TND نىوكت NVM ىدل .NVM عم لكاشم حىحص رى؁ TND NVM فىرعت فلم ررحم فى TND NVM نىوكت نكمى .هنىوكت مت ىذل مداخلل TLS ةداهش

لمعى .ةىطمنل VPN ةدحول TND نىوكت ىلع دمتعى NVM نإف ،NVM TND نىوكت متى مل اذإ مداخ :DHCP ربع اهلابقتسا متى ىتلا تامولعمل اىلإ ادانتسا ةىطمنل VPN ةدحول TND مت ىتلا مىلل لاجمل مسا وأ/و DNS مداخ قباط اذإ .لاجمل مساو (DNS) لاجمل مسا ماضن اىلإ دنتسمل TND فاشتكال VPN معدت امك .اهب قوٲوم ةكبش ل رابتعإ متىسف ،اهنىوكت TLS ةداهش

- اهب قوٲوم ةكبش ىلع نوكتى امदन طقف NVM ردصى .TND نىوكت ءحص نم دكأت



ىلع .تانايبل رىدصتب NVM موى نلف ،حىحص رى؁ TND نىوكت ناك اذإ :ةطخالمل مل نكلو ،لىمعل ىلع اهنىوكت مت DNS مداوخ ةثال كىدل ناك اذإ ،لاثل لىبس NVM موقت نلف ،TND نىوكت فى ةثالثل DNS مداوخ عىم نىعت متى .تانايبل رىدصتب

- لىكشت TND VPN ل نم لاجم قوٲوم ل تلزأ .
- ةكبشل لكاشم :
  - صاخل IP ناونع نىمضتب امئاد مق ،مسقنمل ىقفنل لاصللل ةبسنللاب اذإ . "نمضتى مسقنمل" نىوكتل فى (VPN) ةىرهاطل ةصاخل تاكبشل عجمب ،مسقمل قفنلل هب قوٲومل نىوكتل نم اعزج عجملاب صاخل IP ناونع نكى مل .ةماعل ةه؁اول نم تانايبل لاسرا متىسف
- قوٲوم رى؁/هب قوٲوم) ةىللل ةكبشل ىلع عىمجتلل CollectionMode نىوكت نم دكأت (هب).
- مٲ :ءحىصلل تادلجمل فى ةدو؁وم NVM\_ServiceProfile.xml و VPN.xml تافل نم دكأت لىغشتل د؁ .
- AnyConnect تامدخ عىم لىغشت فاقى .
- DNS مداخب لاصلتا اهل ىتل لخالللاب ةلصتمل ةكبشل دترا .

منزل طاقتل:

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

AnyConnect ل (DART) رىراقتل داد؁او صىخشتل تاودأ

عجرا NVM. تانوكم ىلع DART ليغشتب مق ،اهجالصاوا AnyConnect تاءارجا عاطاخأ فاشكتسال  
[اهجالصاوا AnyConnect عاطاخأ فاشكتسا](#) ىلا

- عي مجتب DART موقى. DART طساوب NVM ل ةبولطملا تالجسلا عي مج ةجلالعم متت  
كلذ ىلا امو نيوكتلاو لجسلا تافلّم
- ل ثادحأل ضراع ي ةلصفنم ةقرو كانه. دحاو ناكم ي ف ثادحأل دجوت ال Windows تالجس  
AnyConnect نمض NVM
- NVMAGENT بسح تالجسلا ةيفصت MacOS/Linux ليغشتلا ماظن .

(لقتسم وأ دحاو ي ف لك ال Linux/Docker: زاهج ىلع) عمجم

acnvmcollector تيبتت لشف

(Sudo ./install\_ubuntu.sh) تيبتت لل يصننلا جم انربلا ليغشتو عمجملا تيبتت ءانثأ

"/var/log/syslog: "Acnvm.conf error: line number 17 : expected key string" ال ي ف أطخ اذه عقي

ريغ عضو ي ةلصاف ببسب وأ ةيفاضا ةلصاف ببسب ةلكشملا هذه ثدحت نأ نكمي  
حلص.

ءدبلا ي ف AcnvmCollector لشف

ي ف زمربلا ذيفنت لشف .(سكنيل لكل امبر نكل) وتنوبوأ ي ف ةلكشم ةلكشملا هذه تناك  
acnvmcollector: /opt/acnvm/bin/acnvmcollector. فلم

acnvmcollector ل acnvm eXecute ل ةومجملاو مدختسملا ىدل نكي مل

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

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

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

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

ءاطاخأل حيحصت نييعت ي نكنمي نيأ - عمجملا تالجس

ليجستلا ىوتسم .دربم ACMNVMLOG.conf ال ي ف ىوتسم ليجستلا تبتت عي طتسي تنأ  
مق ،رييغت ءارجا دعب .ليغشتلا ادب دن عمجملا ىلا هلاسا متي ي ذل نيوكتلا نم عزج وه  
تانايابلا عمجم ليغشت ةداعإ

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
```

؟م اقرألا ع م جم ب ص ا خ ل ا ر ا د ص إ ل ا م ق ر ي ل ع ر و ث ع ل ا ي ن ن ك م ي ف ي ك

نوع: `acnvmcollector` رمال لي غشت ب مق ، عمجم رادصا يلع روثعلل

### 1: لاثم

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

## 2: لاثم

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

## ج: تانجا

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

## DTLS لكاشم

- acnvm.conf فلم ي ف اهن ي و ك ت م ت ي م ل DTLS ن أ ي ن ع ت "DTLS ني و ك ت م ت ي م ل" ة ل اس ر ل ا
- ري غ ر و ر م ل ا ة م ل ك ح ي ت ا ف م ة ع و م ج م ن و ك ت ا م د ن ع "ح ل ا ص ر ي غ م د ا خ ل ا ح ا ت ف م" ة ل اس ر ل ا ر ه ط ت ة م و ع د م .

## تانايا بـالـا ضرعت ال (CESA تامول عم ةحول) Splunk مـكـحت ةدحو

## AnyConnect لىمى

- نم ليلق ددع ىلإ ضارعتسالا اضيأ كنكمي . تانايبلا عاشنإل youtube.com مدختسا ببول عاوم .
- مداخ ىلإ UDP 2055 لوكوتورب ربع تامولعمل لاسرر AnyConnect لىمعل كنكمي له .

- تالاصتال عمجم زاهج ىل لىمعال زاهج نم Telnet جم انرب مادختسا لواح

- ## عیمجت قودنص

- ✍ UDP مزح عي مج طاقت لا ةي فيك ى لا عجرا ، تامول عمل لا نم دي زملا : ةظحال م  
[tcpdump؟ مادختساب](#)

- ## ةعئاشلا ةلئسألا

؟ددعتم تاهجو ىلا AnyConnect NVM نم تاناىبلا لاسرا كنكمى فىك

[Cisco](#) نم (CESA) [قېفرطاللا ةطوقنلا نامأ تاليلحت](#) ىلا عجرا ، تامولعمل نم ديزمل  
رشنلا ليلدو Splunk Quickstart POV Kit ىلع قمئاقلا .

## AnyConnect NVM DTLS؟ نی زخت ب موقت نی

- "اهب قوتومل Windows تاداهش" يف عمجمل ةداهش تيبتب مق Windows:
- رذجل ةداهشل تيبتب تل ةيسايل ةيلعمل مدختسأ: Mac OSX ليغشتل ماظن

داري تسال حيتافم الةلسلس اءا مءءءسإ كنكمي .حيتافم الةلسلس رب ع  
اهب قوؤوم ءءاهشك هتفاضاؤ صيؤرتال

- ءيلاتال رءال قءصم ال عؤرم ال ءاري تسإ تاوؤؤ عبتا :Linux RHEL لئغشتال ماضن  
RHEL ب ءصاؤال

1. /etc/pki/ca-trust/source/links إلى قءصم ال عؤرم ال ءءاهشؤ سنال .

2. sudo update-ca-trust enable

3. sudo update-ca-trust extract

- رءال Ubuntu قءصم عؤرم ءاري تسإ تاوؤؤ عبتا :Linux Ubuntu لئغشتال ماضن  
ءيلاتال:

1. openssl x509 -inform PEM -in رمال اءه مءءءسإ اب .crt فلم إلى .cer فلم لئوؤت  
RootCA.cer -out rootCa.crt

2. /usr/local/share/ca-certificates/ لئل ء إلى .crt فلمؤ سنال .

3. sudo update-ca-certificates رمال لئغشتب مق .

## XML تافل مءامسا

ءءولل XML فئرت فلم مسا ناف ،ئلؤم ال فئرتال فلم رؤم مءءءست امءنع  
هنا إلى ءمءءال فئرت فلم ظفؤ بؤئ ،كل ءؤ ءمؤ .مهم رئؤ ءئساسال VPN ءئطمنال  
NVM لشفئ ،ءمءءال فئرت فلمل رؤا امسا مءءءست تنك اءا .NVM\_ServiceProfile.xml  
اهل اسراؤ تانا ئابل ءئؤئ فئ

## مؤمؤ (AnyConnect NVM)

[\(لئصافئال\) Splunk ل Cisco نم \(CESA\) ءئفرطال ءطقنال ناما ئالئلؤت قئبؤت](#)

- رؤا باسؤ إلى ءئكللم ال رئفؤؤ مؤئ مؤ رءال ئؤ ءرؤم لئل ءاشنإ كنكمي له
- مؤ ئلؤئ صننال ءمانربال نا املاؤ الؤ VM إلى لوصولال/رائؤؤا/ ءاشنإ كنكمي  
هئل ئافللملؤ سنل نءال هئل هئبؤت
- رءؤك ءئفنئلل نءا إلى install.sh فلمل ءاؤئ :فلمل تانؤا
- تاملءال تاباسؤ:
  - رئؤ باسؤ وه ءمءءال باسؤ نال نابولطم -s /bin/false رمالاؤ useradd رمال  
ئسئئر لئل ءلؤؤئ ال لئلؤت
  - نمو ؛ئسئئر لئل ءلؤؤت رئؤ باسؤ ءلؤؤئ نا ئرورؤال نم سئلو  
ئلؤ ظافؤلل ئسئئر لئل ءمءءال باسؤ ءلؤؤئ ال ءءاءم ال تاسرامم ال  
هتفاؤن
  - لئل مءئل ناك ءاؤس ؛ئمؤمؤ ءئرف فرؤم/فرؤم نئمءءءسم ال ءئؤؤ ءلؤ

ال. مأ يسيئر

- يلغ هليغشت نكمي امك: Ubuntu و CentOS يلغ عمجم ل لمعي: عمجم ليغشت ماظن CentOS. جم انرب مدختسي RedHat نأل RedHat.
- رمال مزل اذ، تيبتل لي صننل جم انربل لي دعت كنكمي:
  - هنأل SUDO قوقح عم وأ رذك تيبتل لي صننل جم انربل ليغشت بجي ليلدي في ش لك عضوي و acnvm يمس ي ديج مدختسم عاشناب موق ي /opt/acnvm.



ذيفنتل صصخم يذيفنت صن عاشن كنكمي، كلذ نم الدب: عطلال جم انربل اذهل نكمي. كاتابلطتم يلغ انب عبسانملا تايلمعل نكلو، ماظنل يلغ لعفلاب دوجوم فلتخم مدختسم مادختسا ي صننل. تيبتل ليغشتل SUDO قوقح مدختسملا اذه كلمي نأ بجي.

- عمالعلل -v- مادختساب رمال اذه ليغشتب مق، عمجملا رادصل يلغ روثلل ./opt/acnvm/bin/acnvmcollector -v

## هب ي صوملا رادصلال

تامولعمل نم ديزمل. AnyConnect نم رفوتم جمارب رادصل اذحأ مادختساب امئاد ي صون 4.x رادصلال Cisco AnyConnect Secure Mobility Client بة صاخلا رادصلال تا طاحالم يلغ عجرا

## ةلص تا ذ تامولعم

- [Splunk QuickStart يلغ عي ن ب Cisco نم \(CESA\) عي فرطلا طقنل نامأ تاليلحت رشنل ليلدو POV Kit](#)
- [Cisco نم \(CESA\) عي فرطلا طقنل نامأ تاليلحت تامولعم قحول يلغ عماع قرظن قلوادت ملل قليئسألاو](#)
- [Cisco ل Splunk نم \(CESA\) عي فرطلا طقنل نامأ تاليلحت قيبطت](#)
- [Cisco ل Splunk نم \(CESA\) عي فرطلا طقنل نامأ تاليلحت قيبطت \(قئاثولا\)](#)
- [4.x رادصلال Cisco AnyConnect Secure Mobility Client ل ليمعلل لوؤسم قلدأ](#)
- [4.x رادصلال Cisco AnyConnect Secure Mobility Client بة صاخلا رادصلال تا طاحالم](#)
- [Cisco Systems - تادنت سمل او ينقتل معدلا](#)

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems ( ر ف و ت م ط ب ا ر ل ا ) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا