

ديدهتلا ىلع زكري يذلا ISE 2.1 NAC نيوكت (TC-NAC) عم Qualys

تايوت حمل

[عمدق مل](#)

[قيساس الابلط مل](#)

[تابلط مل](#)

[عمدخت سمل تانوك مل](#)

[نيوكت لا](#)

[ىوت سمل ىل اع قفدت طمخ](#)

[يئوض لاس مل او Qualys قاباحس نيوكت](#)

[يئوض لاس مل Qualys حسام رشن 1. ةوطخل](#)

[يئوض لاس مل Qualys حسام نيوكت 2. ةوطخل](#)

[ISE نيوكت](#)

[ISE عم لماكل ل Tune Qualys Cloud تاداعل 1. ةوطخل](#)

[TC-NAC تامدخ نيكم 2. ةوطخل](#)

[ISE VA لمع راطاب Qualys ئيهاهم لاصتا نيوكت 3. ةوطخل](#)

[VA حسام ليغشتل ليوختلا فيرعت فلم نيوكت 4. ةوطخل](#)

[ليوختلا تاسايس نيوكت 5. ةوطخل](#)

[ةحصلا نم ققحتلا](#)

[ةيوهلا تامدخ كرحم](#)

[سيلوك قاباحس](#)

[اهال صاو اعاطخل افاشكتسا](#)

[ISE ىلع اعاطخل احيحصت](#)

[ةيچذوم نلا تالكش مل](#)

[عجار مل](#)

عمدق مل

Qualys on Identity Services Engine (ISE) 2.1 نيوكت ةيفي ك دنتم سمل اذه حضوي يتلا ةكبشلا لىل لوصولا فيم كحتلا ةزيم كل حيتت 2.1. ISE نيوكت ةيفي ك دنتم سمل اذه حضوي تامس لىل اذانتسا ضيوفت تاسايس ءاشن ةيناكم (TC-NAC) ديهتلا ىلع زكترت فعضلا نم اكم و ديهتلا تائياهم نم اهلابقتسا متي يتلا فعضلا او ديهتلا.

قيساس الابلط مل

تابلط مل

ةيلاتلا عيضاوملاب قيساسا ةفرعم كيديل نوكت ناب Cisco ي صوت:

- Cisco نم ةيوهلا عمدخ كرحم
- Qualys ScanGuard

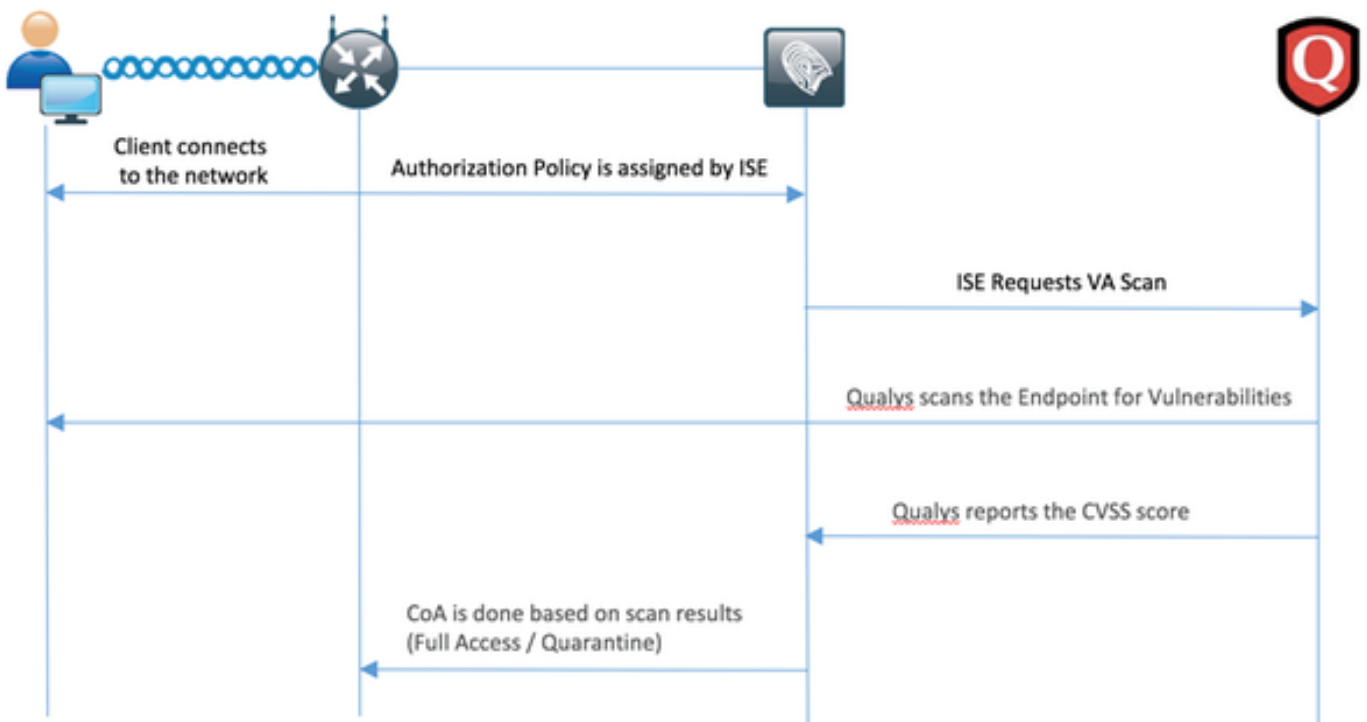
ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملا وجماربال تارادصلا ىلا دن تسملا اذه يف ةدراولا تامولعملل دن تست

- Cisco Identity Service Engine، رادصلا 2.1
- (WLC) 8.0.121.0 ةيكلسالل LAN ةكبش يف مكحتلا ةدحو
- Qualys Guard Scan 8.3.36-1، Signatures 2.3.364-2
- Windows 7 ليغشلال ماطنل 1 ةمدخللا ةمزح

نيوكتلا

ىوتسملا يلاع قفدت ططم



قفتلا وه اذه:

1. عبرمب فيرعت فلم نييعة متيو دودحم لوصوحنم متيو ةكبشلاب ليمعلا لصتي
هنيكمت متي ذللا **فعضلا نطاوم ميقت** رايتخا
2. VA حسم ناكو ةقداصملا ثودح دكؤت MNT ةدقع ىلا syslog ةلاسر PSN ةدقع لسرت
ليوختلا جهنل ةجيتن
3. Admin WebApp مادختساب (TC-NAC ةدقع ىلا ليئوضلا حسملا لاسرلاب MNT ةدقع موقت
تانايبال هذه مادختساب:
 - MAC ناووع
 - IP ناووع
 - حسملل ينمزللا لصافلا
 - يرودللا صحفال نيكمت
 - يلاصلال PSN
4. Qualys TC-NAC (ع REST API) ةباحسب لصتي (Docker ةيواح يف نمضم)
ةجالحلا دن حسملا ليغشتلا

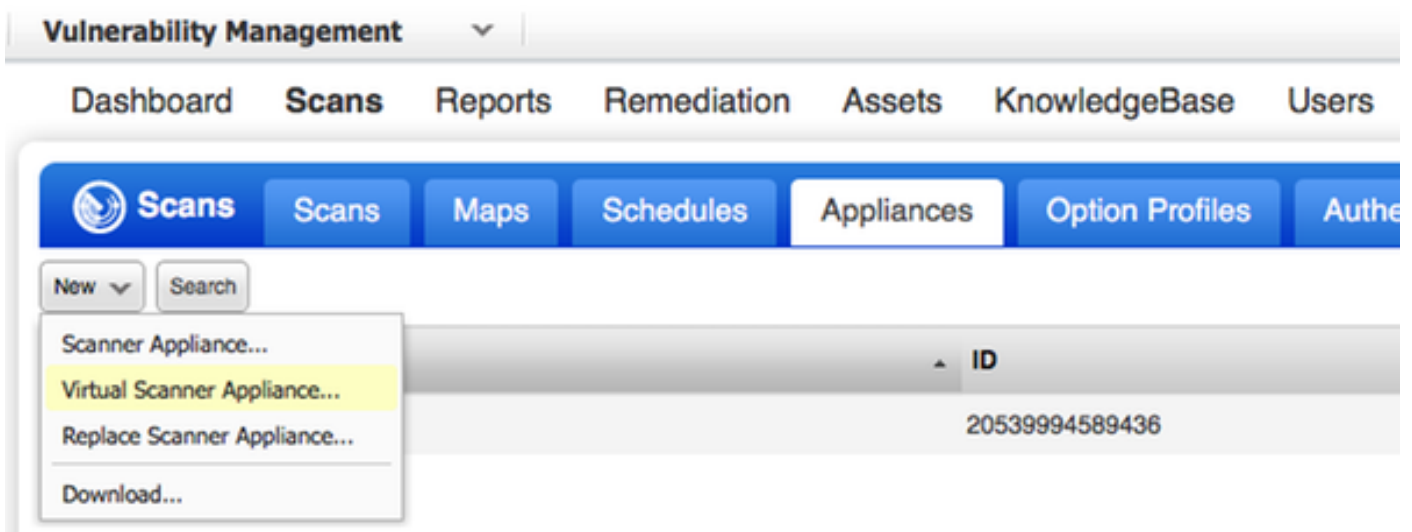
5. Qualys Cloud ةطقن حسمل Qualys Scan دشري
6. Qualys ةباحس لىل ةئوؤضلل حسملل ةئائتن ةئوؤضلل Qualys حسمل لسري
7. TC-NAC لىل ةرؤ ةرؤ صؤفلال ةئائتن لاسرل مئى:
 - MAC ناوؤن ع
 - CVSS ةئائتن ةفاك
 - (QID، ناوؤن عل، CVEIDs) فعضلل طاقن ةفاك
8. ةوطخلل نم تانايايبلل عئمع عم PAN ةئوؤضلل موقى TC-NAC
9. هئوؤؤ مئى لىل ةوؤؤلال ةهنل اقفو ةءال دن ع CoA لىل ةؤؤؤ مئى

ةئوؤضلل حسملل او Qualys ةباحس نئوؤؤ

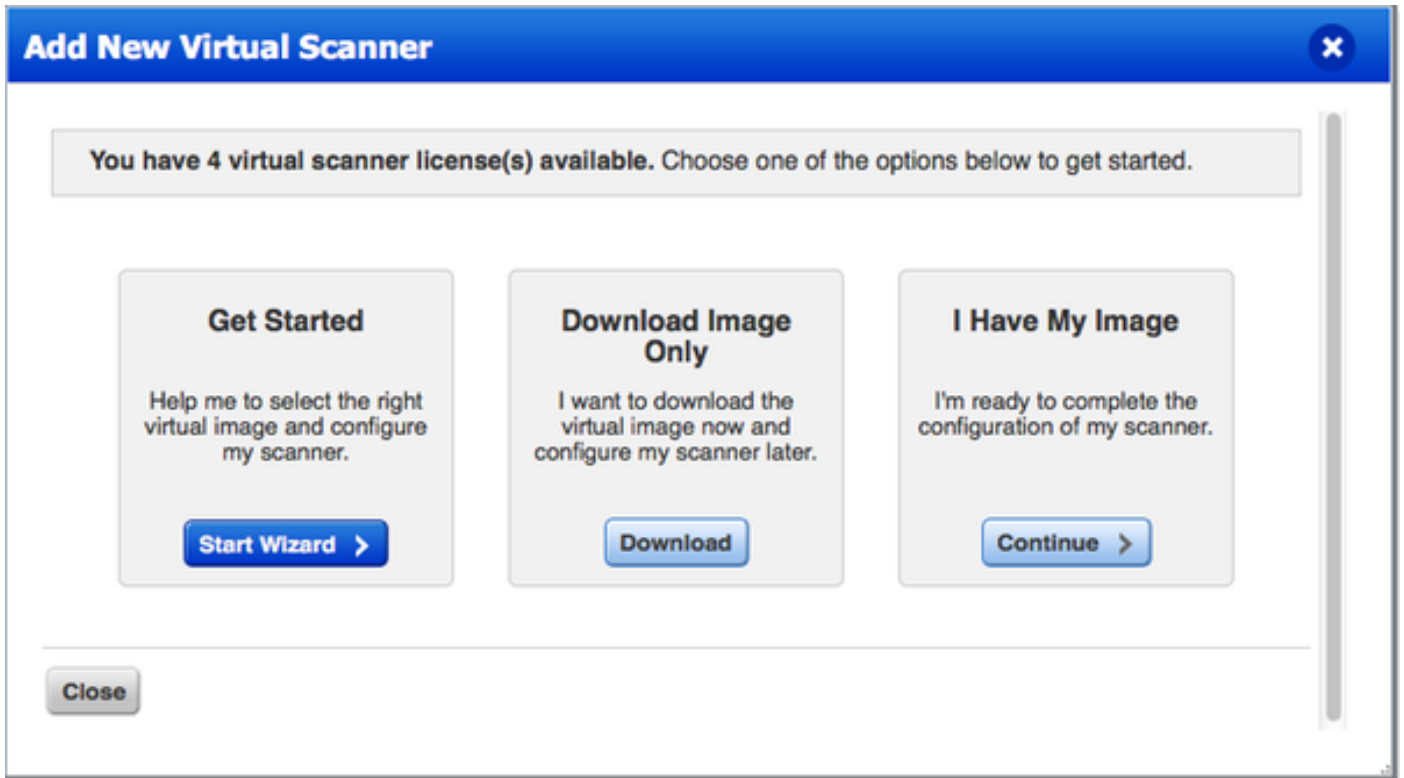
رواشتلل ةئوؤؤ، ةئوؤؤ مئى ضارؤال دن تسملل اذ ه ف ةوؤؤتتلل نئوؤؤتتلل ةارجل مئى: رىؤؤت مئى مئى صؤتتلل تارابت ع الل Qualys ةئوؤؤؤ مئى

ةئوؤضلل حسمل رشن 1. ةوطخلل

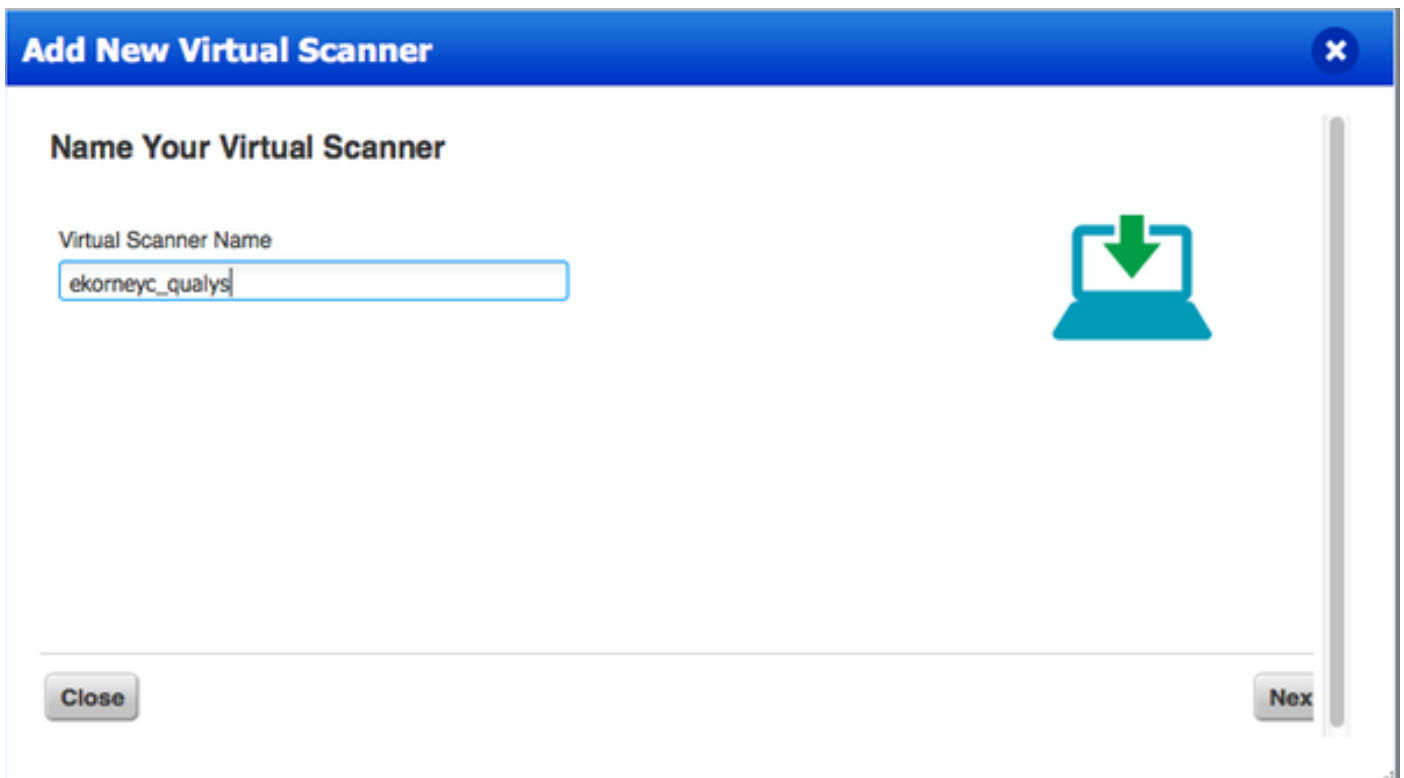
Qualys cloud لىل لوؤؤلل لىل ةئوؤؤ مئى OVA فلم نم Qualys ةئوؤضلل حسملل رشن نك مئى ىر ه اظلل ةئوؤضلل حسملل زاؤ > ةئوؤؤ ةؤؤؤؤال > حسملل تائىل مع لىل لقتن او



بس انملا ةئوؤؤلال رتؤاو طقف ةروؤؤلل لئؤؤت ةؤؤ



> ديدج ديدحتو ةزهجأال > صحفالا ةزهجأ إلى لاقانالا كنكمي ،طيشتننالا زمرىلع لوصحلل
 يتروص ديدحتو يرهاظالا يئوضالا حسامالا زاهج



اقحال همذختستس يذلا ليوختالا زمر كحنم متي ،يئوضالا حسامالا مسا لاخذإ دعب

يئوضالا Qualys حسام نيوكت 2. ةوطخلا

اذه تلكش ،متي نإ ام .هراخت يذلا ةيضارتفالا ةاكاحملل يساسأالا ماظنالا لىع OVA رشن
 دادعإ ةيلمع

- ةكبشال دادع (LAN)
- نېتهجاو مدختست تنك اذ (WAN ةهجاو تاداع)
- لېكول مدختست تنك اذ (لېكول تاداع)
- ئوضال حسامال اذه صي صخت



QualysGuard® Scanner Console

Name: ekorneyc_qualys, LAN IP: 10.62.145.82

Set up network (LAN) >

Change WAN interface >

Disable WAN interface >

Enable proxy >

Reset network config >

System shutdown >

System reboot >

Version info: 3.11.16.5.11.0

Exit this menu? (Y/N)

TIP:

This is the main (top-level) menu of the Virtual Scanner Console.

Press the UP and DOWN arrow keys to navigate the menu.

Press the RIGHT arrow or ENTER key to choose a menu item.

اهلېزنتو عي قاول او جماربلا شدا ةدوچب ئوضال حسامال لېصوت متي كلذ دعب

Personalize

Update in progress 12%

Personalize this scanner >

Enter personalization code:

Set up network (LAN) >

Downloading ml_debian_keys-1.0.0-1.noarch.rpm

Enable WAN interface >

Enable proxy >

Reset network config >

System shutdown >

System reboot >

Version info: 3.9.7.5.11.0

Exit this menu? (Y/N)

> يئوضلا حسملا تاي لمع ىلإ لاق تنال ك نكمي ، يئوضلا حسملا لاصتا نم ققحت ل ل ةزهجال .

ةيؤر اضيأ ك نكمي ، زهاج يئوضلا حسملا نأ ىلإ راسيلا ىلع رضخألا طبرلا ةمالع ريشت LAN IP ، WAN IP ، عيقاوتلاو يئوضلا حسملا رادصا .

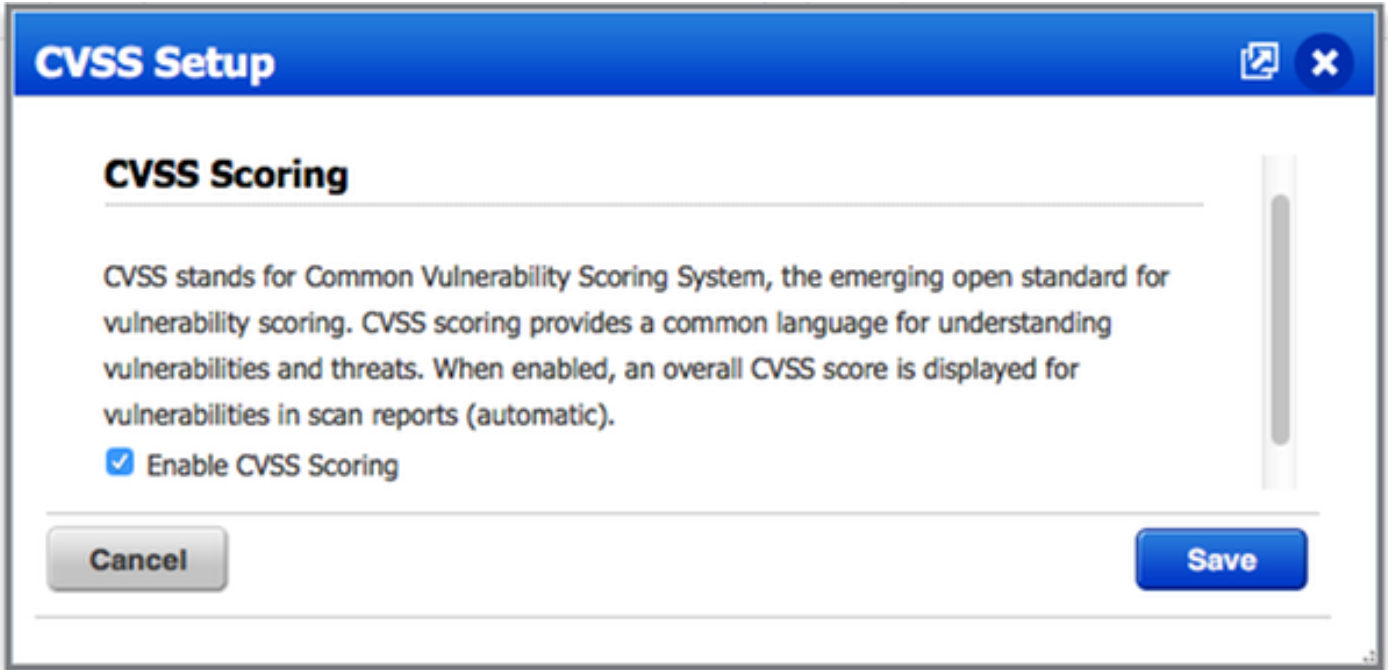


ISE نيوكت

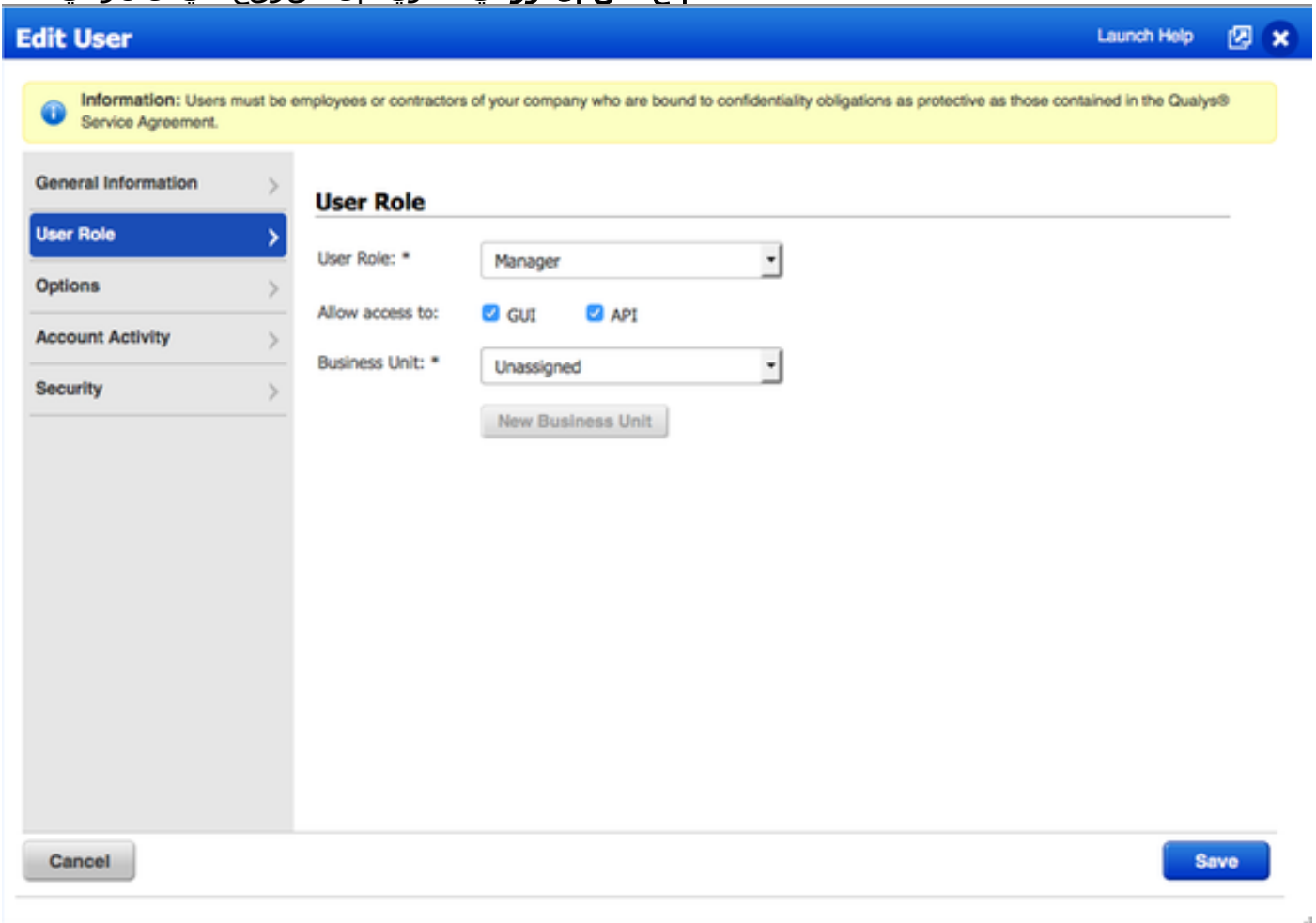
تادادعإ طبض ك يلع نيعة تي لازي ال ، Qualys Scan و Cloud نيوكت ب تمق ك نأ نم مغرلا ىلع لبق ك لذب مايقلا ب جي هنا طحال . ديچ لكشب لمعي ISE عم لمكتلا نأ نم دكأتلل ةباحسلا يوتحت تيلا فراعمال ةدعاق نإ ثيچ ، (GUI) ةيموسرلا مدختسملا ةهجاو لالخ نم لوحملا نيوكت ةرم لوأل لوحملا نيوكت دعب اهليزنت متي CVSS طاقن ىلع .

ISE عم لمكتلا ل Tune Qualys Cloud تادادعإ 1. ةوطخلا

- > CVSS > دادعإلا > ريراقتلا > فعضلا طاقن ةرادإ ي CVSS طاقن ليحست نيكم تب مق • CVSS طاقن ليحست نيكم تب



- ددح ري دم تا زاي تما اهل لوح م لا ني وكت في م دختس م لا م دختس م لا تا غوس م نا ن م دكات ن ا ب جي . م دختس م لا في رعت فلم يل ع ر ق نا و ي ر س ي ل ا ة ي و ل ع ل ا ة ي و ا ز ل ا ن م م دختس م لا م دختس م لا ر و د في " ري دم لا " ق و ق ح ك ي د ل ن و ك ي .



- م ي ي ق ت ب ل ط ت ي ت ل ا ة ي ا ه ن ل ا ط ا ق ن ل ا ة ي ع ر ف ل ا ت ا ك ب ل ل / IP ني و ا ن ع ة ف ا ض ا ن م دكات ن ا ب جي > ة في ض م لا ل و ص ا ل ا > ل و ص ا ل ا > ت ا ر غ ث ل ا ة ر ا د ا د ن ع د و د ر م لا ي ل ا ر ث ا ت ل ا ة ي ل ب ا ق ا ه ب ق ع ت م ت ي ت ل ا ة في ض م لا IP ة ز ه ج ا

New Hosts Launch Help ✕

General Information: >

Host IPs >

Host Attributes >

Host IPs

Enter IPs and ranges in the field below. See the [Help](#) for proper formatting.

IPs: *

Add to Policy Compliance Module

(ex: 192.168.0.200,192.168.0.87-192.168.0.92)

Validate IPs through [Whois](#)

Cancel

Add

TC-NAC تامدخ نيكمت 2. ةوطخال

يتال NAC ةمدخ نيكمت صحف. ريرحتال ةدقع > رشنال > ةرادال تحت TC-NAC تامدخ نيكمت رايخا ةناخ ديهتال ال ع زكترت.

رشن ةيلمع لكل طقف ةدحاو TC-NAC ةدقع كانه نوكت نا نكمي: ةطحال

Edit Node

General Settings

Profiling Configuration

Hostname **ISE21-3ek**
 FQDN **ISE21-3ek.example.com**
 IP Address **10.62.145.25**
 Node Type **Identity Services Engine (ISE)**

Personas

Administration Role **STANDALONE**

Monitoring Role **PRIMARY** Other Monitoring Node

Policy Service

Enable Session Services Include Node in Node Group **None**

Enable Profiling Service

Enable Threat Centric NAC Service

ISE VA لمع رابط Qualys لاصتا نيوكت 3. ةوطخل

رقنا. ةفاضل > ةيچراخل تاهجل ي دروم > تاديدهتل لىل ع زكري يذل NAC > ةرادل لىل لقتنا
 ظفح قوف.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > PassiveID > Threat Centric NAC

Third Party Vendors

Vendor Instances > New
 Input fields marked with an asterisk (*) are required.

Vendor *

Instance Name *

نيوكتل زهاج قوف رقنا، ةلاجل نيوكتل زهاج لىل ليثمل تالاقتنا ةئي هتب موقت ام دنع
 ةلاجل ي ف رايل.

Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
AMP_THREAT	AMP	THREAT	https://api.amp.sourcefire.com	Connected	Active
QUALYS_VA	Qualys	VA		Disconnected	Ready to configure

دجوي شيح، Qualys Cloud ل هم دختست يذال فيضم ال وهو REST API فيضم نوكي نأ بجي
 ك.ك باسح qualysguard.qg2.apps.qualys.com - ل اثم ال اذه في .

ي.لالتل قوف رونا، Manager، تازايتما كل مې يذال وهو باسح ال نوكي نأ بجي

Vendor Instances > QUALYS_VA

Enter Qualys Configuration Details

Enable CVSS Scoring in Qualys (Reports->Setup->CVSS Scoring->Enable CVSS Scoring) and add the IP address of your endpoints in Qualys (Assets > Host Assets)

REST API Host

 The hostname of the Qualys platform where your account is located.

REST API Port

 The port used by the REST API host.

Username

 User account with Manager privileges to the Qualys platform.

Password

 Password of the user.

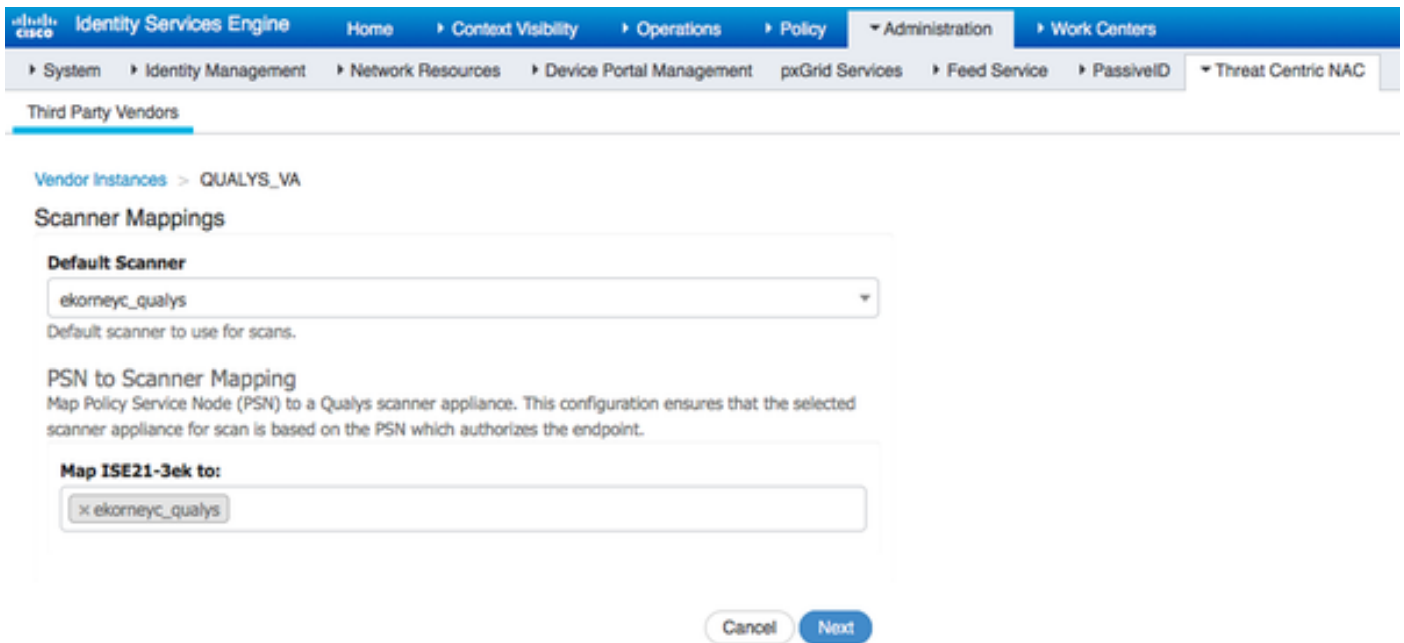
HTTP Proxy Host

 Optional HTTP Proxy Host. Requires proxy port also to be set.

HTTP Proxy Port

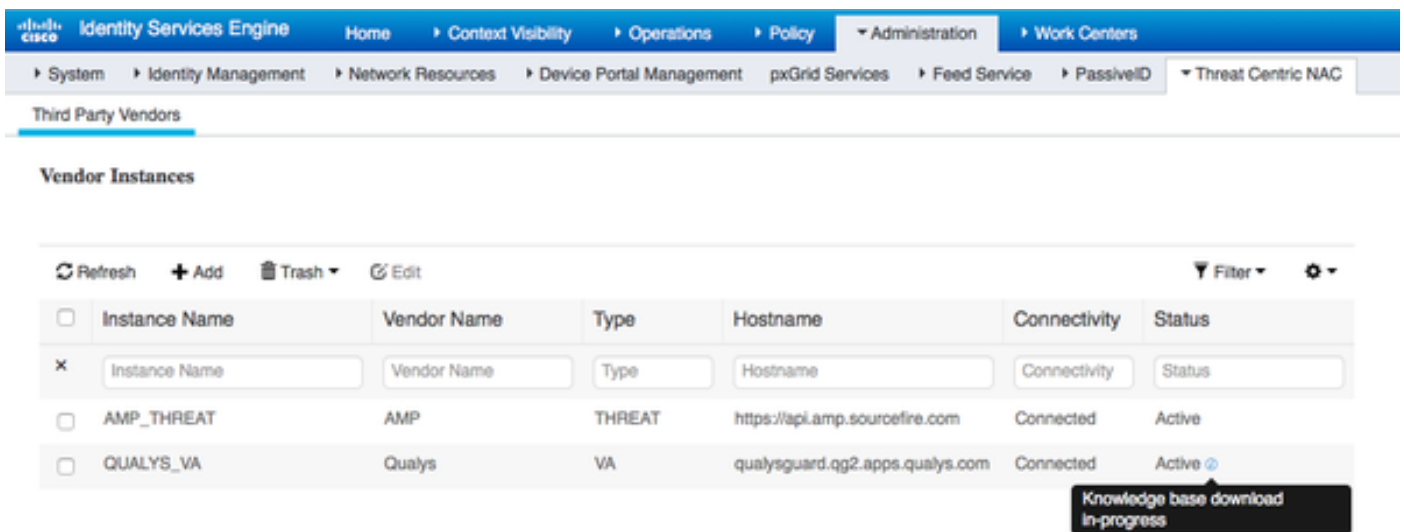
 Optional HTTP Proxy Port. Requires proxy host also to be set.

كنكمي، Qualys، ةباحسب ةلصتلم ةيئوضلا تاحسامل لوح تامولعمل ليزنن تب ISE موقت
 حسامل اقاتنا نمضي هنإ. ةحفصل هذه يلع يئوضلا حسامل طي طخت لىل PSN نيوكت
 ةياهنل ةطقن لوخي يذال PSN لىل انب يئوضلا



يلع روثع ال نكمي و، ISE 2.1 لوؤسم ليلد في ديچ لكش ب ةم دقتم ل اتاداع ال قيثوت مت تايلمع حيضوت. زاجن او كلذ دعب قوف تقطقط. دنن سمل اذه في عجارم ل مسق في طابترال ا فراعمال ةدعاق ليزنت ادب و ةطشنل ال ةلاح ال ال ليثم ل ليوت

رشن ةيلمع لك ل دحاو Qualys ليثم يوس كانه نوكي نأ نكمي ال : ةظحالم



VA حسم ليغشتل ليوختل فيرت فلن نيوك ت. 4 ةوطخل

ليوختل تافيصوت > ليوختل > چئاتنل > ةسايسل رصانع > ةسايسل ال لقتنا. تارغلل مبيقت رايختال ةناخ دح ةكرتشم الماهم ل تحت. ديچ فيرت فلن ةفاض. ةكبش الم ميمصتل اق فو بلطل بسح حسم لل ينمزل ل صافل ديحت بچي.

هذه AV جاوزا يلع ليوختل فيرت فلن يوتحي

cisco-av-pair = on-demand-scan-interval=48

Cisco-av-pair = Periodic-scan-enabled=0

cisco-av-pair = va-adapter-instance=796440b7-09b5-4f3b-611-199fb81a4b99

يقيقحلا ضرغلا نأ نم مغرلا يلع ،لوصولا لوبق ةمزح لخاد ةكبشلا ةزهجأ ىلإ اهلاسرا متي و لاصتال TC-NAC ةدقع MNT دشري .صحفلا ليغشت ةرورضب MNT ةدقع مالعإ وه اهنم ةباحسب Qualys.

ليوختلا تاسايس نيوكت 5 ةوطخلا

- في هنيوكت مت يذلا ديدجلا ليوختلا فيرعت فلم مادختسال ليوختلا جهن نيوكتب مق ةدعاق عقوم ددحو ،ليوختلا جهن > ضيوفت > جهن ىلإ لقتنا 4. ةوطخلا نم تانوذألا رييغتب مق .(ريحت) Edit قوف رقنا مٲ ،basic_authenticated_access صحف ءارجإ ىلإ ك لذ يدؤي .اٲيدح هؤاشنإ مت يذلا Standard VA_Scan ىلإ PermitAccess ظفح قوف رقنا .نيمدختسملا ةفاكل تارغٲلا
- جهن > ليوخت > جهن ىلإ لقتنا .اهيلع يحيص ربح ضرّف مت يتلا ةزهجالل دامتعا جهن ءاشنإ ديدج طرش ءاشنإ > طورش قوف رقنا .ءانٲٲسإ ةدعاق ءاشنإب مق و تاءانٲٲسإ > ليوخت ددحو ديدٲٲلا ةمس عيسوتب مق .ديدٲٲ ددحو لفسأل قلزنا ،ةمس ددح > (مدقتم رايخ) ةميق لاخداب مقو نم ربكأ ىلإ ليغشتلا لماع رييغتب مق .Qualys-CVSS_BASE_SCORE صحف ءارجإ جهن لاقفو الوصو يحيصل ربحلا ضيوفت فيرعت فلم يقطع نأ بچي .كب صاخلا نامألا جهن لاقفو .يحمملا ريغ زاوجل ادودحم

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Exception Rule	if ThreatQualys-CVSS_Base_Score GREATER 8	then Quarantine
Standard			
✓	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
⊘	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess
⊘	Employee_EAP-TLS	if (Wireless_802.1X AND BYOD_Is_Registered AND EAP-TLS AND MAC_in_SAN)	then PermitAccess AND BYOD
⊘	Employee_Onboarding	if (Wireless_802.1X AND EAP-MSCHAPv2)	then NSP_Onboard AND BYOD
✓	Wi-Fi_Guest_Access	if (Guest_Flow AND Wireless_MAB)	then PermitAccess AND Guests
✓	Wi-Fi_Redirect_to_Guest_Login	if Wireless_MAB	then Cisco_WebAuth
✓	Basic_Authenticated_Access	if Network_Access_Authentication_Passed	then VA_Scan
✓	Default	if no matches, then	DenyAccess

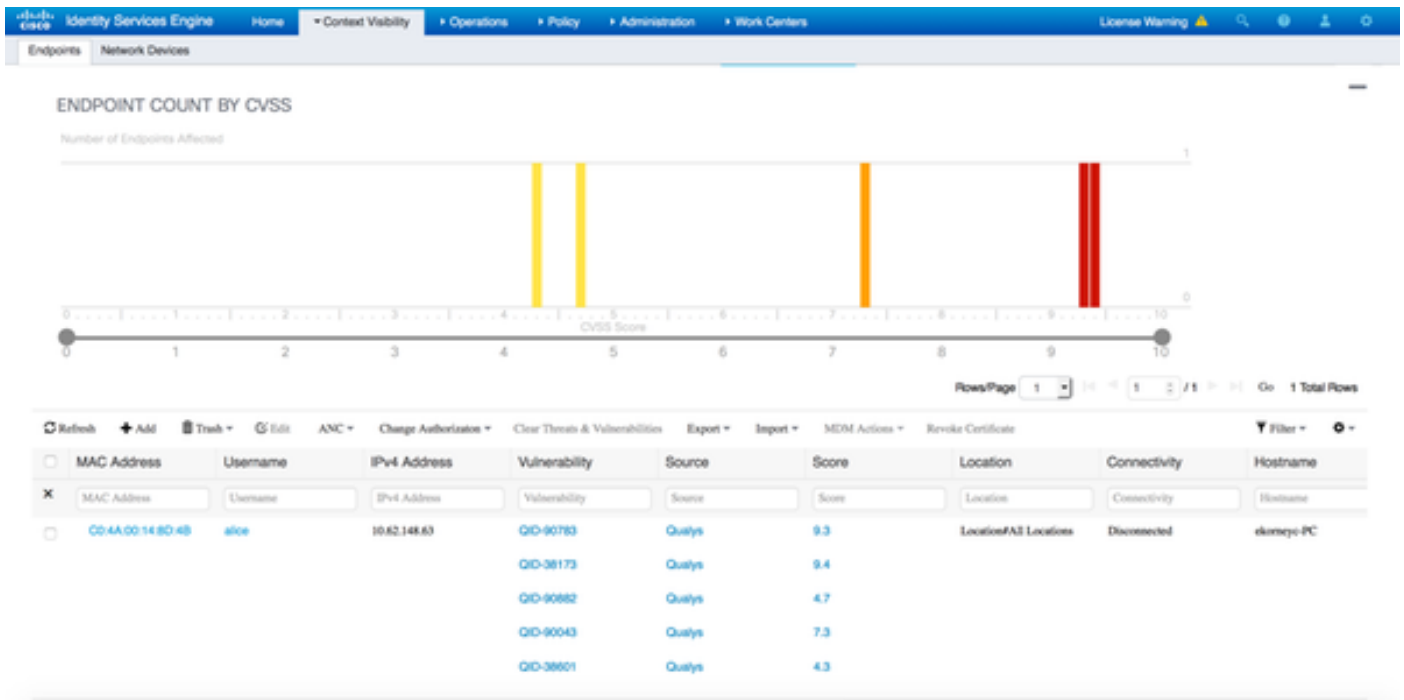
تحصلنا من ققحتنا

هوهنا تامدخ كرحم

لدينا مشتمة، صحفنا اءاتنا دنع VA. لئو وضلنا حسمنا لئو غشتمب لوالنا لاصتالنا موقو هتقبطاطم ةلا ح ي ف دئج جهن قئببطلنا CoA ةقداصم ةداعا.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizati
Jun 28, 2016 07:25:10:971 PM	Auth Pass			alice	CO-4A:00:14:8D:4B	Microsoft-Wo...	Default >> Dot1X >> Default	Default >> Exception Rule	Quarantine
Jun 28, 2016 07:25:07:065 PM	Auth Pass			alice	CO-4A:00:14:8D:4B				
Jun 28, 2016 07:06:23:437 PM	Auth Pass			alice	CO-4A:00:14:8D:4B	TP-LINK De...	Default >> Dot1X >> Default	Default >> Basic_Authenticated_Access	VA_Scan

طاقن > قئببطلنا ةئو ةئنا كملنا لئو لئو قئنا، اءافاشتمنا كملنا فعضلنا نمنا كملنا نم ققحتنا لئو لئو نم اءح نم مئنا لئو طاقننا عم ةئنا هتقطن لئو لئو فعضلنا طاقننا نم ققحتنا. ةئنا هءنا لئو Qualys.



في ام ب، فعرض عطقن لك لوح لى صافات ل نم ديزم ل رهظي، ةني عم ةياهن عطقن دي دجت دن ع CVEID و ناونع ل ك ل ذ

The screenshot shows the details for endpoint C0:4A:00:14:8D:4B. The endpoint profile is Microsoft-Workstation, and the current IP address is 10.62.148.63. The location is not specified. Below the endpoint details, there is a tab for 'Vulnerabilities' which lists the following vulnerabilities:

- QID-90783**
 Title: Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)
 CVSS score: 9.3
 CVEIDS: CVE-2012-0002, CVE-2012-0152,
 Reported by: Qualys
 Reported at:
- QID-38173**
 Title: SSL Certificate - Signature Verification Failed Vulnerability
 CVSS score: 9.4
 CVEIDS:
 Reported by: Qualys
 Reported at:

لباقم ةميدقلا لي وختلا تاسايس ةيؤر كنكمي ، ةرشابملا TC-NAC تالجس > تايلملا ي CVSS_BASE_SCORE. يل لصافتلاو ةقبطملا ةديدل

يواس تيتلاو ، CVSS_BASE_SCORE. يل اذانتسا لي وختلا طورش ذي فننت متي : ةظالم ةياهنلا ةطقن يل ءهع فشكلا متي تال ءعضلا طاقن يل

Time	Endpoint ID	Username	Incident type	Ven...	Old Authorization p...	New Authorization ...	Authorization rule matched	Details
Thu Jun 28 2016 12:25:32 GMT+05...	CO-4A:00:14:8D:4B	alice	vulnerability	Qualys	VA_Scan	Quarantine	Exception Rate	CVSS_Base_Score: 9.4 CVSS_Temporal_Score: 7.7

سيلوك ةباحس

ةصاخلا TC-NAC Qualys راطتنا مئاوق ةطساوب VA ل ئي وضللا حسملا لي غشت متي امدنع حسملا تايلمع > ئي وضللا حسملا تايلمع يف هضرع كنكمي ، ئي وضللا حسملا ب

Title	Targets	User	Reference	Date	Status
IseScan	10.62.148.63	Eugene Komeychuk	scan/1467134073.04090	06/28/2016	Queued

حسام يل تاميلعت تردصأ دق Qualys ةباحس نأ ينعي امم ، لي غشتلا يل لقتني كلذ دعب يل ءفل ئي وضللا حسملا اءارءال Qualys

Title	Targets	User	Reference	Date	Status
IseScan	10.62.148.63	Eugene Komeychuk	scan/1467134073.04090	06/28/2016	Running

"...ئي وضللا حسملا" ىرت نأ بجي ، ئي وضللا حسملا اءارءال ئي وضللا حسملا موقبي امنبي Qualys Guard نم ايلعلا ينميلا ةيوازلا يل لوخدلا لي جست

QualysGuard® Scanner Console

Name: ekorneyc_qualys, LAN IP: 10.62.145.82

TIP:
Press ENTER to access the menu.

في جئاتنللا ضرع كنكمي . "ةيهتنم" ةلاجلال لىل لقتني هناف ،صحفال م تي نأ درجم ب ضرع وأ صخلمللا ضرع قوف رقن او بولطمال صحفال دح ،يئوض حسم > يئوض حسم تاي لمع جئاتنللا.

QUALYS ENTERPRISE

Vulnerability Management

Dashboard Scans Reports Remediation Assets KnowledgeBase Users

Scans Scans Maps Schedules Appliances Option Profiles Authentication Search Lists Setup

Title	Targets	User	Reference	Date	Status
IseScan	10.62.148.63	Eugene Korneychuk	scan/1467134073.04090	06/28/2016	Finished
IseScan	10.201.228.107	Eugene Korneychuk	scan/1467132757.03987	06/28/2016	Finished
IseScan	10.201.228.102	Eugene Korneychuk	scan/1467131435.03655	06/28/2016	Finished
IseScan	10.62.148.89	Eugene Korneychuk	scan/1464895232.91271	06/02/2016	Finished
IseScan	10.62.148.71	Eugene Korneychuk	scan/1464855593.86436	06/02/2016	Finished
IseScan	10.62.148.71	Eugene Korneychuk	scan/1464850315.85548	06/02/2016	Finished
IseScan	10.62.148.71	Eugene Korneychuk	scan/1464847674.85321	06/02/2016	Finished
IseScan	10.62.148.71	Eugene Korneychuk	scan/1464841736.84337	06/02/2016	Finished
IseScan	10.62.148.71	Eugene Korneychuk	scan/1464836454.83651	06/02/2016	Finished

Preview

Vulnerability Scan - IseScan
Target: 1 IP(s)

Scan launched by Eugene Korneychuk (sc2bk) | Start: 06/28/2016 at 21:18:55 (GMT+0400) | Ended: 06/28/2016 at 21:22:17 (GMT+0400) | Scan Finished (00:05:22)

Summary Scanner(s) are finished. Results from this scan have been processed.

Total Hosts Alive	Total appliances used	Aggregate Vulnerabilities
1	1	7

[View Summary](#) | [View Results](#)

فعضاللا طاقن ضرع م تي شيح ،ةيلصفتللا جئاتنللا ةيؤر كنكمي هسفن ريرقتللا في ةفشتكماللا.

Detailed Results

10.62.148.63 (ekorneyc-pc.example.com, EKORNEYC-PC)

Vulnerabilities (6)

- 5 Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)
- 3 SSL/TLS use of weak RC4 cipher
- 3 Windows Remote Desktop Protocol Weak Encryption Method Allowed
- 2 NetBIOS Name Accessible
- 2 SSL Certificate - Signature Verification Failed Vulnerability
- 1 ICMP Timestamp Request

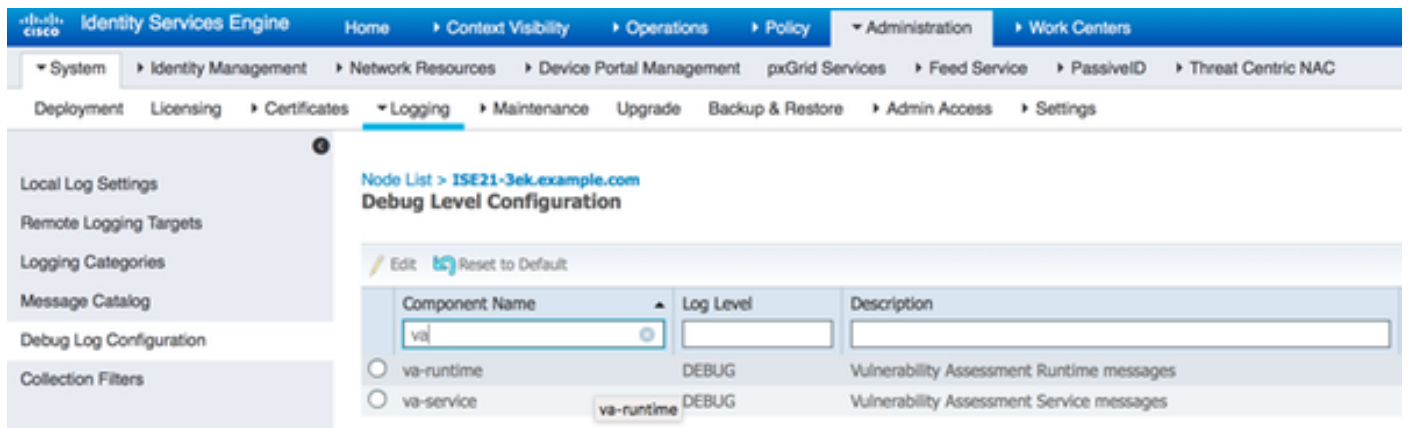
Potential Vulnerabilities (1)

Information Gathered (26)

اهحال صا وءاطخ ال فاشك ت سا

ISE لى عءاطخ ال حى حصت

لجس نيوكت > ليجستال > ماظنل > ةرادال لى للاقن ال ISE لى عءاطخ ال حى حصت نيكم تل
va-service و va-runtime لجس ال يوتسم نوكم ريغت ب مقو TC-NAC ةدق دح، ءاطخ ال حى حصت
ءاطخ ال حى حصت لى



رطس ةهجاو نم ةرشابم اه لى ع لوصح ال كنكم ي. varuntime.log - اه صحف بولطم ال تالجس لى
ISE رما و:

```
ISE21-3ek/admin# varuntime.log tail
```

ة ني عم ة ياهن ة طقن ل صحف ال ءارج ل تاداشرا TC-NAC Docker لى قلت

```
2016-06-28 19:06:30823 [Thread-70][ ] va.runtime.admin.mnt.EndpointFileReader -:::- VA: Read  
Va Runtime.  
[{"operationType":1"macAddress":"C0:4A:00:14:8D:4B"ondemandScanInterval":"48"isPeriodicScanEna  
bled":false"periodicScanEnabledString":"0"vendorInstance":"79640b7-09b5-4f3b-611-  
199fb8a4b99"psnHostName":"21-3ek"heartBeatTime":0"lastScanTime":0}]  
2016-06-28 19:06:30824 [Thread-70][ ] va.runtime.admin.vaservice.VaServiceRemotingHandler -  
:::- VA: MNT:
```

```
{ "operationType": 1, "macAddress": "c0:4a:00:14:8d:4b", "ondemandScanInterval": "48", "isPeriodicScanEnabled": false, "PeriodicScanScan4 String": "0", "vendorInstance": "796440b7-09b5-4f3b-611-199fb81a4b99", "psnHostName": "ISE21-3ek", "heartBeatTime": 0, "lastScanTime": 0 }
```

قاي س ل ل ل ي د ي ف ة ي ن م أ ل ا ت ا ر غ ث ل ل ا ن ا ي ب ع ي م ج ن ي ز خ ت م ت ي ، ة ج ي ت ن ل ل م ا ل ت س ا د ر ج م ب و

```
2016-06-28 19:25:02020 DEBUG [pool-311-thread-8][ ]
va.runtime.admin.vaservice.VaServiceMessageListener -:::- VaService:
[{"macAddress": "c0:4a:00:14:8d:4b", "ipAddress": "10.62.148.63", "lastScanTime": 1476
: [{"VulnerabilityId": "QID-90783", "cveIds": "CVE-2012-0002 CVE-2012-
0152", "cvssBaseScore": "9.3", "cvssTemporaryScore": "7.7", "VulnerabilityTitle": "Windows
Remote Desktop Protocol Remote Execution Vulnerability (MS12-
020)", "VulnerabilityVendor": "Qualys"} {"VulnerabilityId": "QID-
38173", "cveIds": "CVSSbaseScore": "9.4", "cvssTemporaryScore": "6.
9", "VulnerabilityTitle": "SSL -
", "VulnerabilityVendor": "Qualys"} {"VulnerabilityId": "QID-
90882", "cveIds": "CVSSbaseScore": "4.
7", "cvssTemporaryScore": "4", "VulnerabilityTitle": "Windows Remote Desktop
", "VulnerabilityVendor": "Qualys"} {"VulnerabilityID": "QID-
90043", "cveIds": "CVSSbaseScore": "7.3", "cvssTemporaryScore": "6.
3", "vulnerabilityTitle": "SMB SMB
", "vulnerabilityVendor": "Qualys"} {"vulnerabilityID": "QID-38601", "CVEid": "CVE-2013-
2566 CVE-2015-
2808", "cvssBaseScore": "4.3", "cvssTemporaryScore": "3.7", "VulnerabilityTitle": "SSL/TLS
RC4", "VulnerabilityVendor": "Qualys"}]]]
2016-06-28 19:25:02127 [pool-311-thread-8][ ]
va.runtime.admin.vaservice.VaServiceMessageListener -:::- VA: db LastscanTime: 1467134394000
mac: c0:4a:00:14:8d:4b
2016-06-28 19:25:02268 [pool-311-thread-8][ ] va.runtime.admin.vaservice.VaAdminServiceContext
-:::- VA: json pri-lan
2016-06-28 19:25:02272 [pool-311-thread-8][ ] va.runtime.admin.vaservice.VaPanRemotingHandler -
:::- VA: {C0:4a:00:14:8d:4b=[{"vulnerabilityId": "QID-90783", "cveIds": "CVE-2012-02-0202
02 CVE-2012-0152", "cvssBaseScore": "9.3", "cvssTemporaryScore": "7.7", "vulnerabilityTitle": "Microsoft
Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-
020)", "vulnerabilityVendor": "Qualys"} {"vulnerabilityID": "QID-38173", "cveIds": "CVSSbaseScore": "
9.4", "cvssTemporaryScore": "6.9", "VulnerabilityTitle": "SSL -
", "VulnerabilityVendor": "Qualys"} {"VulnerabilityId": "QID-
90882", "cvssBaseScore": "4.7", "cvssTemporaryScore": "4", "VulnerabilityTitle": "
Windows", "QualityVendor": "ys"} {"vulnerabilityId": "QID-
90043", "cveIds": "CVSSbaseScore": "7.3", "cvssTemporaryScore": "6.3", "vulnerabilityTitle": "SMB
Signature Disabled SMB Signature Not Required", "vulnerabilityVendor": "Qualys"}
{"vulnerabilityID": "QID-38601", "cveIds": "CVE-2013-223-23 66 CVE-2015-
2808", "cvssBaseScore": "4.3", "cvssTemporaryScore": "3.7", "vulnerabilityTitle": "SSL/TLS RC4
", "vulnerabilityVendor": "qualys"}]]
```

ة ه ج ا و ن م ة ر ش ا ب م ا ه ي ل ع ل و ص ح ل ا ك ن ك م ي . Catalyervice.log - ا ه ص ح ف م ت ي س ي ت ل ا ت ا ل ج س ل ل ا ر م ا و ا ر ط س ISE:

```
ISE21-3ek/admin# server.log tail
```

ل و ح م ل ا ل ا ف ع ض ل ا م ي ي ق ت ب ل ط ل ا س ر ا م ت

```
2016-06-28 17:07:13200 DEBUG [endpointPollerScheduler-3][ ] cpm.va.service.util.VaServiceUtil -
:::- VA SendSyslog systemMsg : [{"systemMsg": "91019", "isAutoInsertSelfAcInstance": true}, {"TC-
NAC.ServiceName": "TC-NAC", "Status": "VA", "Details": "VA", "TC-
NAC.MACAddress": "C0:4a:00:14:8d:4b", "TC-NAC.IPAddress": "10.62.148.63", "TC-
NAC.AdapterInstanceUid": "79640B-003 9b5-4f3b-611-199fb81a4b99", "TC-NAC.VendorName": "Qualys", "TC-
NAC.AdapterInstanceName": "QUALYS_VA"}]]
```

يہتني ىتح ٲئوضلا حسملا ةلاح نم قئاقء 5 لك AdapterMessageListener ققحتي

```
2016-06-28 17:09:43459 [SimpleAsyncTaskExecutor-2][[]
cpm.va.service.processor.AdapterMessageListener -:::- :
{"AdapterInstanceName":"Qualys_VA"AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-627f30248ad0"
VendorName:"Qualys"OperationMessageText":
: 1 : 0 : 0"}
2016-06-28 17:14:43760 DEBUG [SimpleAsyncTaskExecutor-2][[]
cpm.va.service.processor.AdapterMessageListener -:::- :
{"AdapterInstanceName":"Qualys_VA"AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-627f30248ad0"
VendorName:"Qualys"OperationMessageText":
: 0 : 0 : 1"}
2016-06-28 17:19:43837 [SimpleAsyncTaskExecutor-2][[]
cpm.va.service.processor.AdapterMessageListener -:::- :
{"AdapterInstanceName":"Qualys_VA"AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-627f30248ad0"
VendorName:"Qualys"OperationMessageText":
: 0 : 0 : 1"}
2016-06-28 17:24:43867 [SimpleAsyncTaskExecutor-2][[]
cpm.va.service.processor.AdapterMessageListener -:::- :
{"AdapterInstanceName":"Qualys_VA"AdapterInstanceUid":"a70031d6-6e3b-484a-adb0-627f30248ad0"
VendorName:"Qualys"OperationMessageText":
: 0 : 0 : 1"}
```

CVSS تامالع عم بئج لىل ابئج CVE راي عم و (QID) دروملا ةئف فرعم لىل لوجملا لصرحي

```
2016-06-28 17:24:57556 [SimpleAsyncTaskExecutor-2][[]
cpm.va.service.processor.adapterMessageListener -:::- :
{"RequestedMacAddress":"C0:4a:00:14:8D:4B"scanStatus":"Assessment_SUCCESS"lastScanLong":146713
449 000"ipAddress":"10.62.148.63" "":[{"VulnerabilityId":"QID-
38173"cvssBaseScore":"9.4"cvssTemporaryScore":"6.9"VulnerabilityTitle":" SSL -
"VulnerabilityVendor":"Qualys"}{"VulnerabilityID":"QID-90
43"cvssBaseScore":"7.3"cvssTemporaryScore":"6.3"vulnerabilityTitle":"SMB Signature Disabled
SMB Signature Not Required"vulnerabilityVendor":"Qualys"}{"vulnerabilityId":"QID-
90783"cveIds":"CVE-2012-002CVE-2012-012-512
2"cvssBaseScore":"9.3"cvssTemporaryScore":"7.7"vulnerabilityTitle":"Microsoft Windows Remote
Desktop Protocol Remote Execution Vulnerability (MS12-
020)"vulnerabilityVendor":"Qualys"}{"vulnerabilityId":"QID-38601"cveIds":"CVE-2013-2566CVE-
2015-22 08"cvssBaseScore":"4.3"cvssTemporaryScore":"3.7"vulnerabilityTitle":"SSL/TLS RC4
"vulnerabilityVendor":"Qualys"}{"vulnerabilityId":"QID-
90882"cvssBaseScore":"4.7"cvssTimerScore":"4"VulnerabilityTitle":
"VulnerabilityVendor":"Qualys"}]}
2016-06-28 [SimpleAsyncTaskExecutor-2] [] cpm.va.service.processor.adapterMessageListener -
:::- IRF {"C0:4a:00:14:8d:4b":[{"
":{"CVSS_Base_Score":9.4"CVSS_Temporal_Score":7.7}timestamp-4":1 67134394000"""":"Qualys"}]}
2016-06-28 17:25:01853 DEBUG [endpointPollerScheduler-2][[] cpm.va.service.util.VaServiceUtil -
:::- VA SendSyslog systemMsg : [{"systemMsg":"91019"isAutoInsertSelfAcsInstance":true"":["TC-
NAC.ServiceName" " TC-NAC.Status"VA "TC-NAC.Details"VA : 5"TC-
NAC.MACAddress"C0:4a:00:14:8D:4B"TC-NAC.IpAddress"10.62.148.63"TC-
NAC.AdapterInstanceUid"796440B-0Address 9b5-4f3b-611-199fb81a4b99"TC-
NAC.VendorName"Qualys"TC-NAC.AdapterInstanceName"QUALYS_VA"}]}
```

ةجذومنللا تالكشمل

و 0.0 نم CVSS_BASE_SCORE عم تارغثلا ريرقت لىل لصرحي 1. ةلأسمل
فعضللا طاقن لىل Qualys Cloud ريرقت يوتحي امنب، 0.0 نم CVSS_TEMPORAL_SCORE
ةفشكتملا.

ةلكشمل:

عم و، ةفشكتملا فعضللا طاقن ةيؤر كنكمي Qualys Cloud نم ريرقتلا نم ققحتلا ءانثا
ISE لىل اهارة ال كلذ.

catalyervice.log في ءاطخألا حيحصت ضرع م ت

```
2016-06-02 08:30:10323 [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.adapterMessageListener -:::- IRF
{"c0:4a:00:15:75:c8":[{"Vulnerability":{"CVSS_Base_Score":0.0"CVSS_Temporal_Score":0.0}"stamp-
4":1 6485905000"title":" "":"Qualys"}]}
```

الحل:

متي مل CVSS ةمالع نأ وأ فعض طاقن اهل سي ل نأ ام| وه رفض CVSS ةجرد نوك ءارو ب بس لل
ليزنت متي . UA لال خ نم لوحمل نيوك تب موقت نأ لب بق Qualys Cloud يف اهنيك مت
نيوك دع ب اهنيك مت مت يتي ال CVSS طاقن ليجست ءزي م يل ع يتحت يتي ال KnowledgeBase
ءاشن| مت ثي ح ، لب بق نم CVSS طاقن ليجست نيك مت نم دكأت ال ك يل ع ب جي . ءرم لوأل لوحمل
> دادعإل > ريراق تل > فعض ال طاقن ءراد| تحت كلذب ماي قل نك مي . ISE يل ع لوحمل لي ثم
CVSS > طاقن ليجست نيك مت > CVSS

جهن قي ببط نم مغرل ال ع ، Qualys Cloud ةومجم نم جئاتن يل ع ISE لصحي ال . 2 ءلأسمل
ححص ال ليوخت ال .

ءل كشمل:

هذه نم مغرل اب . VA صحف لي غشت يل ديؤي نأ ب جي ي ذل ، ححصم ليوخت ال جهن ءق باطم تمت
صحف ي ءارج متي ال ، ءق ق الح

catallyervice.log يف ءاطخ ال حي حصت ضرع مت

```
2016-06-28 16:19:15401 DEBUG [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::- :
(:'[B@6da5e620([311)]'MessageProperties [=({} timestamp=null messageId=null userId=null
appId=null clusterId=null type=null correlationId=null Null =Null =application/octet-stream
contentEncoding=null contentLength=0 deliveryMode=PERSISTENT expiration=null priority=0
redelivered=false receiveExchange=irf.topic.va-reports receiveRoutingKey= deliveryTag=9830
messageCount=0])
2016-06-28 16:19:15401 [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::- :
{"requestedMacAddress":"24:77:03:3d:CF:20"scanStatus":"scan_error"scanStatusMessage":"
1904: IP . "lastScanTimeLong":0"ipAddress":"10.201.228.102"}
2016-06-28 16:19:15771 [SimpleAsyncTaskExecutor-2][]
cpm.va.service.processor.AdapterMessageListener -:::- Macaddress:24:77:03:3d:CF:20
IP(DB): 10.201.228.102
2016-06-28 16:19:16336 DEBUG [endpointPollerScheduler-2][] cpm.va.service.util.VaServiceUtil -
:::- VA SendSyslog systemMsg : [{"systemMsg":"91008" isAutoInsertSelfAcsInstance":true"}: [{"TC-
NAC.ServiceName" " TC-NAC.Status"VA Failure"TC-NAC.Details" : 1904:
IP . "TC-NAC.MACAddress" "24:77:03:3d:CF:20"TC-NAC.IPAddress"10.201.28.12"TC-
NAC.AdapterInstanceUuid" "79640b7-09b5-4f3b-611-199fb81a4b99"TC-NAC.VendorName"Qualys"TC-
NAC.AdapterInstanceName"QUALYS_VA"}]}
```

الحل:

ي ءوض ال حسم لل لهؤم ريغ ءي اه ن ال ءطقن ب صاخ ال IP ناو نع نأ يل Qualys Cloud ري شي
ل وصال > ل وصال > تارغ ثل ءراد| يل ءي اه ن ال ءطقن لل IP ناو نع ءفاض| نم دكأت ال ءارل
IP Track Host > دي دج > ءفي ضم ال

عجارم ال

- [2.1 رادصال ، Cisco نم ءي و ال تام دخ كرحم لوؤسم لي ل د](#)
- [Cisco Systems - تادنت سمل او ي نقت ال م عدل](#)
- [Qualys عم 2.1 ISE : و ي دي ف ال](#)

- [Qualys قېښوت](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء نأ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل ة مچرت ل ض ف أن ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ئ ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل ج ن إ ل ا دن تسمل ا