

ديدهتلا ىلע زكري يذلا NAC نيوك (TC-NAC) عم Qualys

تاي وتحمل

ةمدقملا

[قيس اس الاتابل طتملا](#)

[تابل طتملا](#)

[ةمدختسملا تانوكمل](#)

[نيوك تلا](#)

[يوتس ملا يلاع قفدت ططخم](#)

[يئوض لاحس امل او Qualys](#) ئياحس نيوك

[يئوض لاحس ام رشن 1. ۋوطخلا](#) Qualys

[يئوض لاحس ام نيوك 2. ۋوطخلا](#) Qualys

[نيوك](#) ISE

[عم لماكتلل Tune Qualys Cloud](#) تادادع 1. ۋوطخلا

[تامدغ نيك مت 2. ۋوطخلا](#) TC-NAC

[لمع راطاب Qualys](#) ئياهم لاصتا نيوك 3. ۋوطخلا

[حسم ليغشتلى يوختلا فيرعت فلم نيوك 4. ۋوطخلا](#) VA

[ليوختلا تاس اي س نيوك 5. ۋوطخلا](#)

[قحصلا نم ققحتلا](#)

[قيوهلا تامدغ كرحم](#)

[سيلوك ئياحس](#)

[اهالص او عاطخ الافاش كتسرا](#)

[ىلع عاطخ الاحيحصت ISE](#)

[قيجذومنلا تالكشملا](#)

[عجارملا](#)

ةمدقملا

مادختسا ب ديهتلا ىلع زكري يذلا NAC نيوك ئيفيك دنتسملا اذه حضوي يتلا ئكبشلا ىلإ لوصولا يف مكحتملا ئزيم كل حيكت Identity Services Engine (ISE) 2.1. تامس ىلإ ادانتسا ضيوفت تاس اي س عاشن ئيناكما (TC-NAC) ديهتلا ىلع زكترت فعضلا نماكمو ديهتلا تائي اهم نم اهلابقتسا متى يتلا فعضلاو ديهتلا.

ةيس اس الاتابل طتملا

تابل طتملا

ةيلاتلا عيضاوملاب ئيس اس افريم كيدل نوك نأب Cisco يصوت:

- Cisco نم ئي وهلا ئمدخ كرحم
- Qualys ScanGuard

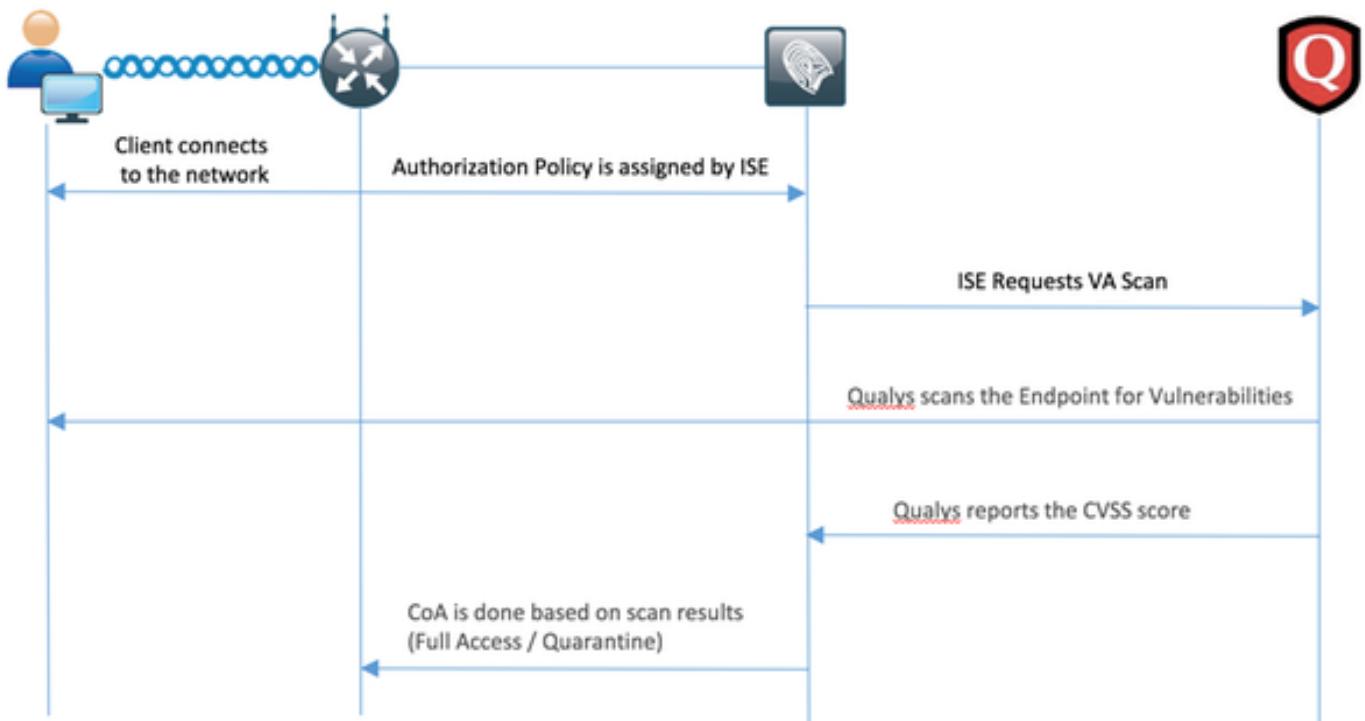
ةمدى سملات ا تانوكمل

ةييلاتلا ةي DAML ا تانوكمل او جماربلا تارادصا ىلإ دنتسملا اذه يف ةدراولما تامولعملما دنتس.

- Cisco Identity Service Engine, رادص إلـا 2.1
- ۆيكلسالـا LAN ۆكبـش يـف مـكـحـتـلـا ۆـدـحـوـ
- Qualys Guard Scan 8.3.36-1, Signatures 2.3.364-2
- ۆـمـدـخـلـا 1 ۆـمـزـحـ لـيـغـشـتـلـا مـاظـنـلـا Windows 7

نيوكتلا

ىوتسملا يلاع قفت ططخم



قفتـلـا وـهـ اـذـهـ:

1. عـبـرـمـبـ فـيـرـعـتـ فـلـمـ نـيـيـعـتـ مـتـيـ وـدـوـدـحـمـ لـوـصـوـحـنـمـ مـتـيـ وـۆـكـبـشـلـابـ لـيـمـعـلـاـ لـصـتـيـ هـنـيـكـمـتـ مـتـ يـذـلـاـ فـعـضـلـاـ نـطـاـوـمـ مـيـقـتـ رـايـتـخـاـ
2. حـسـمـ نـاـكـوـ وـقـدـاصـمـلـاـ ثـوـدـحـ دـكـؤـتـ MNTـ ۆـدـقـعـ ىـلـإـ sysـlogـ ۆـلـاسـرـ PSNـ ۆـدـقـعـ لـسـرـتـ لـيـوـخـتـلـاـ جـهـنـلـ ۆـجـيـتـنـ
3. ۆـقـدـعـ ىـلـإـ يـئـوـضـلـاـ حـسـمـلـاـ لـاـسـرـابـ Admin WebAppـ (MNTـ ۆـدـقـعـ مـوقـتـ) تـانـاـيـبـلـاـ هـذـهـ مـادـخـتـسـابـ:
 - نـاـونـعـ MAC
 - نـاـونـعـ IP
 - حـسـمـلـلـ يـنـمـزـلـاـ لـصـافـلـاـ
 - يـرـوـدـلـاـ صـحـفـلـاـ نـيـكـمـتـ
 - يـلـصـأـلـاـ PSNـ
4. Qualys TC-NAC REST API (ربـعـ Dockerـ ۆـيـواـحـ يـفـ نـمـضـمـ) ۆـبـاحـسـبـ لـصـتـيـ Qualysـ رـبـعـ

5. Qualys Cloud Scan دشري Qualys Scan
6. ئاباحس ىلا يئوضلا حسملا جئاتن يئوضلا Qualys حسام لسري
7. ىلا ئرخا ئرم صحفلا جئاتن لاسرا متي:

 - ناونع MAC
 - جئاتن ئفاك CVSS
 - فعضلا طاقن ئفاك CVEIDs، ناونعلا، (QID)

8. ۋوطخلالا نم تانايبلالا عيماج عم PAN ئيدحتب TC-NAC موقىي.
9. هنيوكت مت يذلا ليوختلا جهنهل اقفو ئجاجلا دنعل لىغشت متى.

يئوضلا حساملاو ئاباحس نيوكت

رواشتلا يجري، ئيلمعم ضارغل دنتسملا اذه يف عونتملا نيوكتلا ئارجا متي: ريدخت ميمىصلالا تارابتعالا يسدنەم عەم Qualys

يئوضلا حسام رشن 1. ۋوطخلالا

ىلا لىخدا ليجستب مق. OVA فلم نم Qualys cloud يئوضلا حساملا رشن نكمىي يرهاظلا يئوضلا حساملا زاھج > دىدج ددحو ۋەزھاجلا > حسملا تايلىمۇ ىلا لقتنا او

The screenshot shows the Qualys Vulnerability Management web interface. At the top, there's a navigation bar with tabs: Dashboard, Scans, Reports, Remediation, Assets, KnowledgeBase, and Users. Below this is another row of tabs: Scans (which is currently active and highlighted in blue), Maps, Schedules, Appliances, Option Profiles, and Authentication. On the left, there's a sidebar with buttons for New, Search, Scanner Appliance..., Virtual Scanner Appliance... (which is highlighted in yellow), Replace Scanner Appliance..., and Download... A modal window is open over the sidebar, showing the same list of options. In the main content area, there's a table with one visible row containing the ID '20539994589436'.

بسانملا عيزوتلا رتخاو طقف ۋەزھاجلا لىزنەت ددح

Add New Virtual Scanner



You have 4 virtual scanner license(s) available. Choose one of the options below to get started.

Get Started

Help me to select the right virtual image and configure my scanner.

[Start Wizard >](#)

Download Image Only

I want to download the virtual image now and configure my scanner later.

[Download](#)

I Have My Image

I'm ready to complete the configuration of my scanner.

[Continue >](#)

[Close](#)

> دى دج ديدحت و ۆزهنجا > صحفلا ۆزهنجا ىلى لاقتنالا كنكمي ، طيشنتلا زمرىل ع لوصحلل
يىت رووص ديدحت و يرها ئاظلا يىوضللا حساملا زاوج

Add New Virtual Scanner



Name Your Virtual Scanner

Virtual Scanner Name

ekorneyc_qualys



[Close](#)

[Next](#)

اقحال ھمدختسەتس يىزلا ليوختلارا زمر كەنەم مەتى ، يىوضللا حساملا مسا لاخدا دەب.

يىوضللا Qualys حسام نېوكت 2. ۆوطخىلار

اذه تلکش ، مەتى نا ام . ھراتخىت يىزلا ۆيضاارت فالا ۆاكاحملل يىساسىلارا ماظنلارا ىل ع رشن OVA دادعە ۆيلىم:

- ةكبشل ادادع (LAN)
- (نیتھج او مدخلتست تنك اذا) WAN ةھج او تادادع
- (ليکول ا مدخلتست تنك اذا) ليکول ا تادادع
- يئوضل ا حساملا اذه صيصخت



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.

اهلى زنت و عيقاوتل او جماربل ا ثدحأ ئدوجب يئوضل ا حساملا ليصوت متى 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 حسمل ا تايملع ىلإ لاقتنالا كنكمي ،يئوضلا حساملا لاصتا نم ققحتلل
ةزهجألا.

ةيُور اضيأ كنكمي ،زهاج يئوضلا حساملا نأ ىلإ راسيل라 ىلع رضخألا طبرلا قماليع ريشت
 LAN IP, WAN IP, يئوضلا حساملا رادصا.

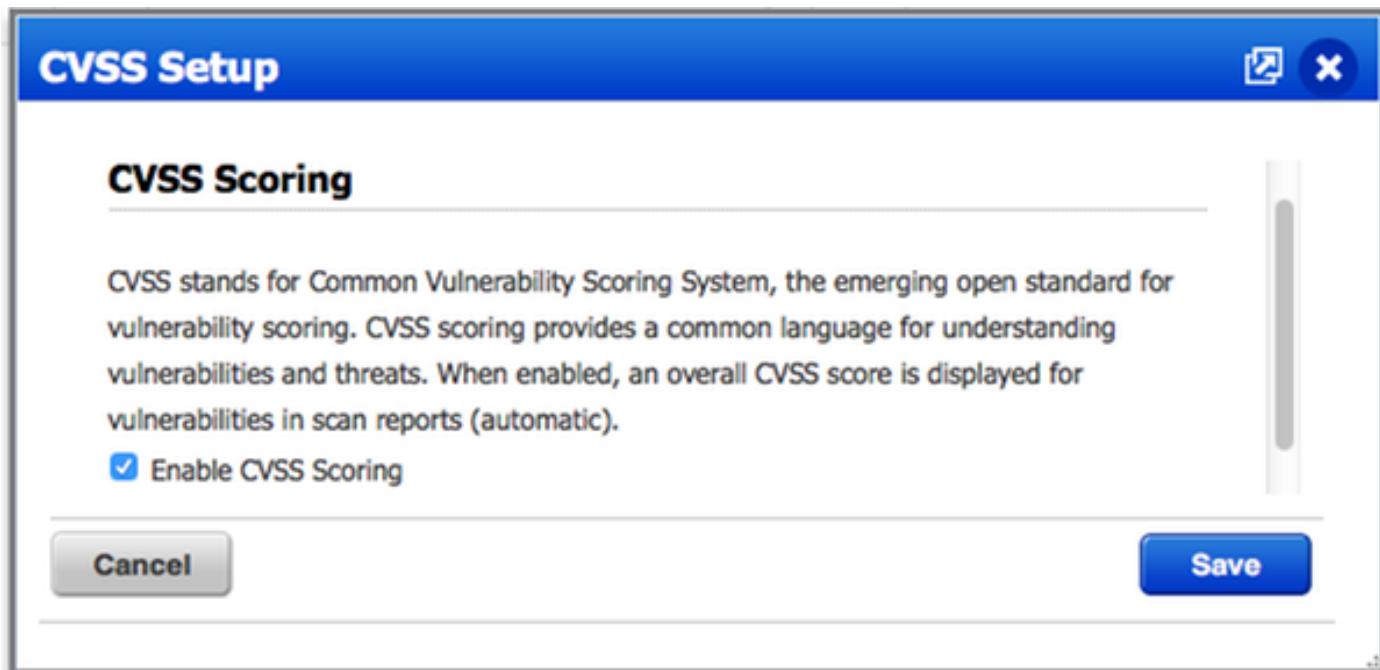
Appliance	ID	LAN IP	WAN IP	Polling	Scanner	Signatures	Last Update
ekmeyt_qualys	20536694588406	10.62.145.82	10.62.145.99	180 seconds	8.3.36-1	2.3.364-2	06/07/2016 at 23:55:30 (GMT+0400)

نويوكن ISE

تادادعإ طبض كيلع نيعتي لازي ال، Qualys Scan و Cloud نويوكن تمق كنأ نم مغرلا ىلع
لبق كلذب مايقلا بجي هنأ ظحال. ديج لكشب لماعي ISE عـمـ لـمـاـكـتـلـاـ نـأـ نـمـ دـكـأـتـلـلـ ةـبـاحـسـلـاـ
يـوـتـحـتـ يـتـلـاـ فـرـاعـمـلـاـ ةـدـعـاـقـ نـاـ ثـيـحـ،ـ (GUIـ،ـ)ـ ةـيـمـوـسـرـلـاـ مـدـخـتـسـمـلـاـ ةـهـجـاـوـ لـالـخـ نـمـ لـوـحـمـلـاـ نـيـوـكـنـ.
ةـرـمـ لـوـأـلـ لـوـحـمـلـاـ نـيـوـكـنـ دـعـبـ اـهـلـيـزـنـتـ مـتـيـ CVSSـ طـاقـنـ ىـلـعـ.

1. وةوطخل ISE عم لـمـاـكـتـلـلـ تـادـادـعـإـ Tune Qualys Cloud

- دادعإلا > ريراقتلا > فعضلا طاقن ئرادا يف CVSS طاقن ليجست نيكمنت مق طاقن ليجست نيكمنت



- دەجىن تازايتىمدا اهل لوحىملا نىوكت يىف ۋەمىتلىك مەختىسىملا تاغۇسەم نأ نم دكأت نأ بىچى. مەختىسىملا فيرعت فلم ئىلۇق رقنى اورىسىللا ئى يولۇللا ئىوازلى نم مەختىسىملا مەختىسىملا رودىيە "رىدىملار" قوقۇخ كىيدل نوکى.

The screenshot shows an 'Edit User' dialog box with a blue header. A yellow information bar at the top states: 'Information: Users must be employees or contractors of your company who are bound to confidentiality obligations as those contained in the Qualys® Service Agreement.' On the left is a sidebar with navigation links: General Information, User Role (which is selected and highlighted in blue), Options, Account Activity, and Security. The main content area is titled 'User Role' and includes fields for 'User Role: *' (set to Manager), 'Allow access to:' (checkboxes for GUI and API are checked), 'Business Unit: *' (set to Unassigned), and a 'New Business Unit' button. At the bottom are 'Cancel' and 'Save' buttons.

- مېيىقت بىلەتتىتىللا ئىاهىنلا طاقىنل ئىعەرفلى تاكىپشىللا IP نىوانع ئەفاضا نم دكأت > دىدج > ئەفيضىمىلار لوصىللا > تارغىتلار دودرمىلار ئىلار ئەتكەنلار ئەبىقۇت مەت يىتلار ئەفيضىمىلار IP ئەزەجأ



General Information: >

Host IPs >

Host Attributes >

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

IPs: *

10.62.148.1-10.62.148.128

 Add to Policy Compliance Module

(ex: 192.168.0.200,192.168.0.87-192.168.0.92)

Validate IPs through [Whois](#)[Cancel](#)[Add](#)**تامدخ نېيکم ت 2. ۋوطخلا TC-NAC**

يىتلە NAC ۋە مەدەنەت نېيکمەت صەقەف. رىيھەنلە > ۋەردىدا > رىيھەنلە > تامدخ نېيکمەت TC-NAC تامدخ نېيکمەت رايىتىخا ئەنالىخ دىدەتلى ئىلۇغ زەكتىرتى.

رىيھەنلە ئەنالىخ دىدەتلى ئىلۇغ زەكتىرتى.

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

<input checked="" type="checkbox"/> Administration	Role STANDALONE	<input type="button" value="Make Primary"/>
<input checked="" type="checkbox"/> Monitoring	Role PRIMARY	Other Monitoring Node <input type="text"/>
<input checked="" type="checkbox"/> Policy Service	<input checked="" type="checkbox"/> Enable Session Services <small>(i)</small> Include Node in Node Group None <small>(i)</small> <input checked="" type="checkbox"/> Enable Profiling Service <input checked="" type="checkbox"/> Enable Threat Centric NAC Service <small>(i)</small>	

3. ۋەطخىل اىام لاصتا نىوكت. Qualys VA ىياب را طاب

رقنا. ئەفاضى > ئېجرا خىلا تاھىلدا يىدروم > تادىدەتلىك زىرى يىذلا NAC > ئەرادىلارلىك لۇقىتنان 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 *	<input type="text" value="Qualys : VA"/>
Instance Name *	<input type="text" value="QUALYS_VA"/>
<input type="button" value="Cancel"/> <input type="button" value="Save"/>	

نىوكتل زەاج قوف رقنا، ئەلەخىلا نىوكتل زەاج ئەلەيىتمەلە تالا قىتنان ئەئىھەتب موقۇت امدىن عۆلەخىلا يىف رايىخلى.

Identity Services Engine		Home	> Context Visibility	> Operations	> Policy	> Administration	> Work Centers	> Threat Centric NAC
> System		> Identity Management	> Network Resources	> Device Portal Management	pxGrid Services	> Feed Service	> PassiveID	
Third Party Vendors								
Vendor Instances								
<input type="button" value="Refresh"/>	<input type="button" value="Add"/>	<input type="button" value="Trash"/>	<input type="button" value="Edit"/>			<input type="button" value="Filter"/>		
<input type="checkbox"/> Instance Name	Vendor Name	Type	Hostname	Connectivity	Status			
<input type="checkbox"/> AMP_THREAT	AMP	THREAT	https://api.amp.sourcefire.com	Connected	Active			
<input type="checkbox"/> QUALYS_VA	Qualys	VA		Disconnected	Ready to configure			

دجوی ثیح، REST API فیضم نوکی نأ بجي Qualys Cloud، لـ Qualysguard.qg2.apps.qualys.com اذه يف. كباسح لاثملـا - qualysguard.qg2.apps.qualys.com

يـلاتـلا قـوف رـقـنـا، تـازـاـيـتـمـا كـلـمـي يـذـلـا وـه بـاسـحـلـا نـوـكـي نـأ بـجـي.

Identity Services Engine		Home	> Context Visibility	> Operations	> Policy	> Administration	> Work Centers	> Threat Centric NAC
> System		> Identity Management	> Network Resources	> Device Portal Management	pxGrid Services	> Feed Service	> PassiveID	
Third Party Vendors								
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								
<input type="text" value="qualysguard.qg2.apps.qualys.com"/>								
The hostname of the Qualys platform where your account is located.								
REST API Port								
<input type="text" value="443"/>								
The port used by the REST API host.								
Username								
<input type="text" value="csc2ek"/>								
User account with Manager privileges to the Qualys platform.								
Password								
<input type="password" value="*****"/>								
Password of the user.								
HTTP Proxy Host								
<input type="text"/>								
Optional HTTP Proxy Host. Requires proxy port also to be set.								
HTTP Proxy Port								
<input type="text"/>								
Optional HTTP Proxy Port. Requires proxy host also to be set.								
<input type="button" value="Cancel"/> <input type="button" value="Next"/>								

كـنـكـمـي، ةـبـاحـسـبـ ةـلـصـتـمـلـا ةـيـئـوـضـلـا تـاحـسـاـمـلـا لـوحـ تـامـوـلـعـمـلـا لـيـزـنـتـبـ ISE Qualys، حـسـاـمـلـا ءـاقـتـنـا نـمـضـيـ هـنـا. ةـحـفـصـلـا هـذـهـ يـلـعـ يـئـوـضـلـا حـسـاـمـلـا طـيـطـخـتـ لـلـا PSN نـيـوـكـتـ، ةـيـاهـنـلـا ةـطـقـنـ لـوـخـيـ يـذـلـا PSN يـلـعـ عـانـبـ يـئـوـضـلـا.

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 > QUALYS_VA

Scanner Mappings

Default Scanner

ekomeyc_qualys

Default scanner to use for scans.

PSN to Scanner Mapping

Map Policy Service Node (PSN) to a Qualys scanner appliance. This configuration ensures that the selected scanner appliance for scan is based on the PSN which authorizes the endpoint.

Map ISE21-3ek to:

x ekomeyc_qualys

Cancel Next

ىلע روثرلا نكمي و، ISE 2.1 لؤوسنم ليلد يف ديج لكشب ئمدقتمنا تادادع إلأ قي ثوت مت تاي لم مع حي ضوت . زاجن او كلذ دع ب قوف تقطق ط . دنتسملا اذه يف عجارملما مسق يف طابترالا فراعملما ئدع اق ليزنت عدب و ئطشنلما ئلاحلا ئلا لي ثملا لي وخت.

رشن ئيلمع لك دح او Qualys لي ثم يو س كانه نوك ي نأ نكمي ال : ئظحالم.

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

Refresh	Add	Trash	Edit	Filter	?
Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
AMP_THREAT	AMP	THREAT	https://api.amp.sourcefire.com	Connected	Active
QUALYS_VA	Qualys	VA	qualysguard.qg2.apps.qualys.com	Connected	Active

Knowledge base download in-progress

حسم ليغشتل لي وختلا فيرعت فلم نيكوت . 4. ئوطخلما

لي وختلا تافي صوت > لي وختلا > جئاتنلا > ئاسايسلما ئلا لقتننا . تارغثلا مي ييق ت راي ت خالا ئناخ ددح ئكرتشملا ما هملما تحت . ديدج فيرعت فلم ئفاضن . ئكبشلما ميم مصتل اقفو بطللا بسح حسم للي نمزلا لصافلا ديدحت بجي .

جاؤزا ئلع لي وختلا فيرعت فلم 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

يقييق حلا ضراغلا نأ نم مغرلا ىلع ،لوصولا لوبق ةمزح لخاد ةكبشلا ةزهجأ ىلإ اهلاسرا متيو
لاصتالل TC-NAC MNT ڈدقع دشري .صحفلال ليغشت ڈرورضب MNT ڈدقع مالعا وه اهنم
ةبااحسب Qualys.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The Policy tab is selected. Below it, the Policy Elements section is open, showing sub-options like Dictionaries, Conditions, and Results. The Results tab is selected. On the left, a sidebar lists categories: Authentication, Authorization, Profiling, Posture, Client Provisioning, and a collapsed section. The main content area is titled 'Authorization Profiles > New Authorization Profile'. It contains fields for Name ('VA_Scan'), Description (empty), Access Type ('ACCESS_ACCEPT'), Network Device Profile ('Cisco'), Service Template (unchecked), Track Movement (unchecked), and Passive Identity Tracking (unchecked). A 'Common Tasks' section below includes a checked checkbox for 'Assess Vulnerabilities', an 'Adapter Instance' dropdown set to 'QUALYS_VA', and a 'Trigger scan if the time since last scan is greater than' field set to '48' hours. There is also an unchecked checkbox for 'Assess periodically using above interval'.

ليوطخلا تاسايس نيوكت 5. ةوطخلا

- يف هنيوكت مت يذلا ديوجلا ليوطخلا فيريعت فلم مادختسال ليوطخلا جهن نيوكت بمقدار عقوم ددحو، ليوطخلا جهن > ضيوفت > جهن ىلإ لقتنا 4. ةوطخلا نم تانوذالا رعيغتب مق. (ريوحـت) Edit قوف رقـنـا مـثـ، basic_authenticated_access، PermitAccess ىـلـا Standard VA_Scan ىـلـا كـلـذـيـ دـوـيـ. اـثـيـ دـحـ هـؤـاشـنـاـ مـتـ يـذـلـاـ صـحـفـ عـارـجـاـ ىـلـاـ ظـفـحـ قـوـفـ رـقـنـاـ. نـيـمـدـخـتـسـمـلـاـ ةـفـاكـلـ تـارـغـثـلـاـ.
- جـهـنـ > ليـوطـخـ > جـهـنـ ىـلـاـ لـقـتـنـاـ. اـهـيـلـعـ يـحـصـ رـجـحـ ضـرـفـ مـتـ يـتـلـاـ ةـزـهـجـأـلـلـ دـامـتـعـاـ جـهـنـ عـاـشـنـاـ دـيـدـجـ طـرـشـ عـاـشـنـاـ > طـورـشـ قـوـفـ رـقـنـاـ. عـاـنـثـتـسـاـ ةـدـعـاـقـ عـاـشـنـاـبـ مـقـوـ تـاءـانـثـتـسـاـ > ليـوطـخـ دـدـحـ وـدـيـدـهـتـلـاـ ةـمـسـ عـيـسـوـتـبـ مقـ. دـيـدـهـتـ دـدـحـ وـلـفـسـأـلـ قـلـزـنـاـ، ةـمـسـ دـدـحـ > (مـدـقـتـمـ رـايـخـ) ةـمـيـقـ لـاخـدـابـ مـقـوـنـمـ رـبـكـأـ ىـلـاـ ليـغـشـتـلـاـ لـمـاعـ رـيـيـغـتـبـ مقـ. Qualys-CVSS_BASE_SCORE الـلوـصـوـيـحـصـلـاـ رـجـحـلـاـ ضـيـوفـتـ فـيـرـعـتـ فـلـمـ يـطـعـيـ نـأـ بـجـيـ. كـبـ صـاخـلـاـ نـاـمـأـلـاـ جـهـنـلـ اـقـفـوـ يـمـحـمـلـاـ رـيـغـ زـاهـجـلـلـ اـدـوـدـحـمـ.

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

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

Exceptions (1)

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Exception Rule	If Threat.Qualys-CVSS_Base_Score GREATER 8	then Quarantine

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	If Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	If Cisco-IP-Phone	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	If Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
<input checked="" type="checkbox"/>	Compliant_Devices_Access	If (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess
<input checked="" type="checkbox"/>	Employee_EAP-TLS	If (Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then PermitAccess AND BYOD
<input checked="" type="checkbox"/>	Employee_Onboarding	If (Wireless_802.1X AND EAP-MSCHAPv2)	then NSP_Onboard AND BYOD
<input checked="" type="checkbox"/>	Wi-Fi_Guest_Access	If (Guest_Flow AND Wireless_MAB)	then PermitAccess AND Guests
<input checked="" type="checkbox"/>	Wi-Fi_Redirect_to_Guest_Login	If Wireless_MAB	then Cisco_WebAuth
<input checked="" type="checkbox"/>	Basic_Authenticated_Access	If Network_Access_Authentication_Passed	then VA_Scan
<input checked="" type="checkbox"/>	Default	If no matches, then DenyAccess	

QQ حصلنا نم ققحتلا

ئي وهلا تامدخ كرحم

لېغشت متي، صحفىلا ئاهتندا دنۇن ل يىوضلى جىمىلا لېغشتىپ لەئەلا لاصىتالا موقىي تىقىباتىم ئەلەح يىف دىدج جىھن قىبىطتلل CoA ۋىداصىم ۋىداعى.

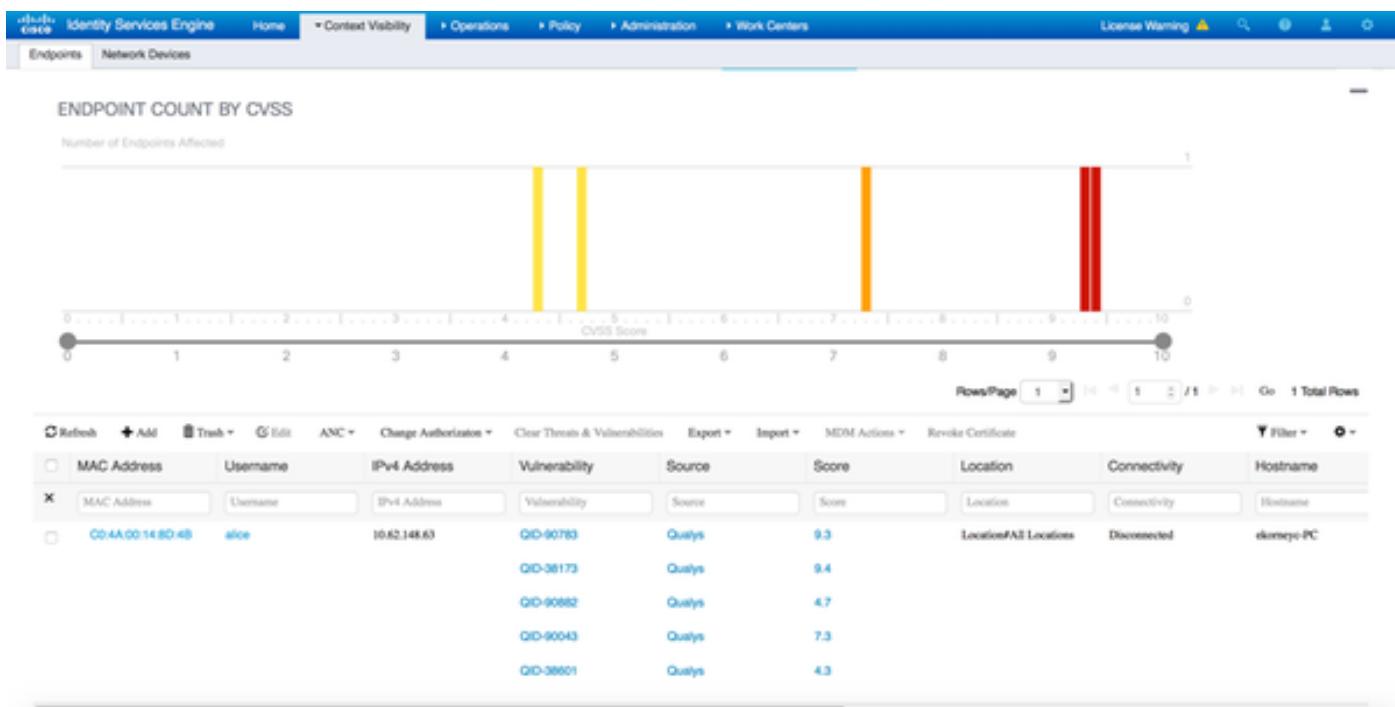
Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Live Logs Live Sessions

Refresh Every 1 minute Show Latest 20 records Within Last 24 hours Filter

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizati...
Jan 28, 2016 07:25:10:971 PM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Auth Pass	alice	C0:4A:00:14:8D:4B	Microsoft-Wi...	Default >> Dot1X >> Default	Default >> Exception Rule	Quarantine
Jan 28, 2016 07:25:07:060 PM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			C0:4A:00:14:8D:4B				
Jan 28, 2016 07:06:23:437 PM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		alice	C0:4A:00:14:8D:4B	TP-LINK-De...	Default >> Dot1X >> Default	Default >> Basic_Authenticated_Access	VA_Scan

طاقدن < قايىسىلا ئيور ئيناكما ئىلى لىقتىندا، اهفاشتىكىمەت يىتلى فىعاضلى ئاماكىم نم ققحتلى لېقىن نم اوهىنەم مەت يىتلى طاقىنلا عم ئيادىن ئەطقىن لەكل فىعاضلى طاقىن نم ققحت. ئيادىنلا Qualys.



يـ اـمـ بـ ، فـعـضـ ةـطـقـنـ لـكـ لـوـحـ لـيـصـاـفـتـلـاـ نـمـ دـيـزـمـلـاـ رـهـظـيـ ، ةـنـيـعـمـ ةـيـاهـنـ ةـطـقـنـ دـيـدـحـتـ دـنـعـ وـنـاـوـنـعـلـاـ كـلـذـ

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Endpoints Network Devices

Endpoints > C0:4A:00:14:8D:4B

C0:4A:00:14:8D:4B

MAC Address: C0:4A:00:14:8D:4B
Username: alice
Endpoint Profile: Microsoft-Workstation
Current IP Address: 10.62.148.63
Location:

Attributes Authentication Threats 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:

لباقام ئەم يىدىقلارلىق ختلا تاسايس ئىيۇر كنكمىي، ئەرشابىملار TC-NAC تالجىس > تايىلمۇلا يىف ئىلۇغشىتلا او قىبىطىملا CVSS_BASE_SCORE.

يواستىتلا او CVSS_BASE_SCORE، ادانتسا لىيۇختىلا طورش ذې فنت مىتى: **ظحالىم** ئىاهنلا ئەطقن ئىلۇغ اهنۇ فشكىلا مىت يىتلار فاعضىلار ئاقۇن ئىلۇغ.

The screenshot shows a log entry from the Threat Centric NAC LiveLog. The entry details a scan by endpoint ID 00:AA:00:14:8D:4B (alice) on June 28, 2016, at 12:25:32 GMT+05:00. The incident type is 'vulnerability' and the vendor is 'Qualys'. The old authorization profile was 'VA_Scan' and the new authorization profile is 'Quarantine'. An exception rule was applied. The log also notes CVSS_Base_Score: 9.4 and CVSS_Temporal_Score: 7.7.

سېلىوك ئەباحس

ئەصالى TC-NAC Qualys را ئەلتىنامىا وق ئەتساوب VA لىيۇضىلار حسمىلار لىيۇغشتىمىتى امدىن حسمىلار تايىلمۇع > يىۋىضىلار حسمىلار تايىلمۇع يىۋىضىلار حسمىلاب

The screenshot shows the Qualys Enterprise Vulnerability Management interface. It displays a list of scans, including one named 'IsleScan' with target 10.62.148.63, user Eugene Komeychuk, reference scan/1467134073.04090, and date 06/28/2016. The status is 'Queued'.

حسام ئىلار تامىلىمعت تردصا دق Qualys ئەباحسى نأ يىنعمى امم، لىيۇغشتىلا ئىلار لىقتىنى كىلدۈپ يىلۇغلىك ئىۋىضىلار حسمىلار ئارچالى

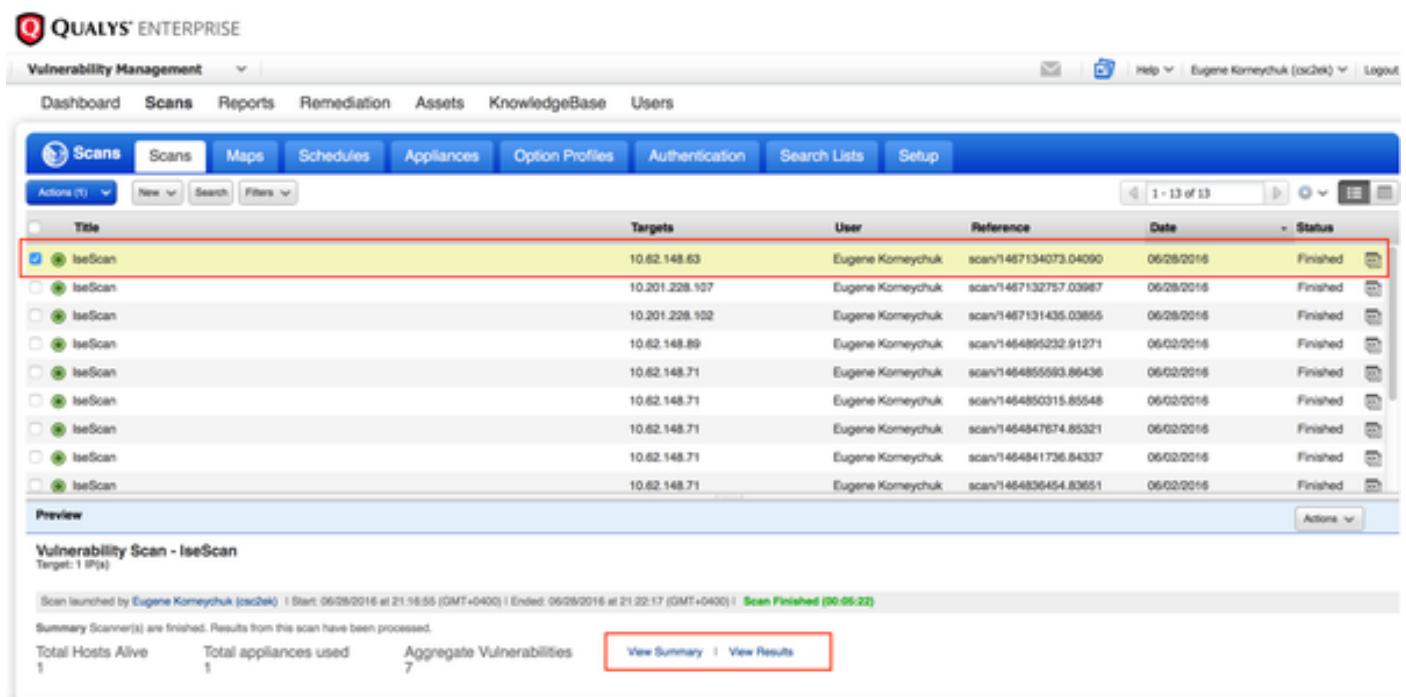
The screenshot shows the Qualys Enterprise Vulnerability Management interface. It displays a list of scans, including one named 'IsleScan' with target 10.62.148.63, user Eugene Komeychuk, reference scan/1467134073.04090, and date 06/28/2016. The status is 'Running'.

"...يىۋىضىلار حسمىلار" ئىرت نأ بجي، يىۋىضىلار حسمىلار ئارچاب يىۋىضىلار حساملىا موقۇي امنىييەت نم اىلۇغلى ئىنمەيلە ئىوازىلا ئىلار لىوخدىلار لىيچىسىنىڭ

QualysGuard® Scanner Console
Name: ekorneyc_qualys, LAN IP: 10.62.145.82
TIP:

Press ENTER to access the menu.

يُف جئاتنلا ضرع كنكمي .ةيـهـتـنـم "ـةـلـاحـلـاـىـلـاـلـقـتـنـيـهـنـافـ،ـصـحـفـلـاـمـتـيـنـأـدـرـجـمـبـ
ضرـعـوـأـصـخـلـمـلـاـضـرـعـقـوـفـرـقـنـأـوـبـولـطـمـلـاـصـحـفـلـاـدـدـ،ـيـئـوضـحـسـمـ>ـيـئـوضـحـسـمـتـاـيـلـمـعـ
جـئـاتـنـلـاـ.



The screenshot shows the QualysGuard Enterprise interface under the 'Vulnerability Management' tab. The main content area displays a table of scan results. One row is highlighted with a red border, corresponding to the scan titled 'IseScan'. The table columns include Title, Targets, User, Reference, Date, and Status. All scans listed are marked as 'Finished'. The 'Actions' button at the top left of the table is also highlighted with a red border.

Title	Targets	User	Reference	Date	Status
<input checked="" type="checkbox"/> IseScan	10.62.148.63	Eugene Komeychuk	scan/1467134073.04090	06/28/2016	Finished
<input type="checkbox"/> IseScan	10.201.228.107	Eugene Komeychuk	scan/1467132757.03987	06/28/2016	Finished
<input type="checkbox"/> IseScan	10.201.228.102	Eugene Komeychuk	scan/1467131435.03985	06/28/2016	Finished
<input type="checkbox"/> IseScan	10.62.148.89	Eugene Komeychuk	scan/1464895232.91271	06/03/2016	Finished
<input type="checkbox"/> IseScan	10.62.148.71	Eugene Komeychuk	scan/1464855593.86436	06/03/2016	Finished
<input type="checkbox"/> IseScan	10.62.148.71	Eugene Komeychuk	scan/1464850315.85548	06/03/2016	Finished
<input type="checkbox"/> IseScan	10.62.148.71	Eugene Komeychuk	scan/1464847674.85321	06/03/2016	Finished
<input type="checkbox"/> IseScan	10.62.148.71	Eugene Komeychuk	scan/1464841736.84307	06/03/2016	Finished
<input type="checkbox"/> IseScan	10.62.148.71	Eugene Komeychuk	scan/1464836454.83651	06/03/2016	Finished

Preview

Vulnerability Scan - IseScan
Target: 1 IP(s)

Scan launched by Eugene Komeychuk (os2ek) | Start: 06/28/2016 at 21:18:55 (GMT+0400) | Ended: 06/28/2016 at 21:22:17 (GMT+0400) | Scan Finished (00:03:22)

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

Total Hosts Alive: 1 | Total appliances used: 7 | Aggregate Vulnerabilities: 7

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

فعـضـلـاـ طـاقـنـاـ ضـرـعـ مـتـيـثـيـحـ،ـةـيـلـيـصـفـتـلـاـجـئـاتـنـلـاـ ةـيـفـرـكـنـكـمـيـهـسـفـنـرـيـرـقـتـلـاـ يـفـ
ةـفـشـتـكـمـلـاـ.

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) []

اهحالص او عاطخألا فاشكتسا

ISE ىلع عاطخألا حيحيحصت

لچس نويوكن > ليچستلا > ماظنلا > ةرادإلا ىلإ لاقتنالا ISE ىلع عاطخألا حيحيحصت نيكملت لچسلا ىوتسم نوكم ريمغتب مقو TC-NAC ڈدقع ددج، عاطخألا حيحيحصت va-runtime و va-service عاطخألا حيحيحصت ىلإ

Component Name	Log Level	Description
va		
va-runtime	DEBUG	Vulnerability Assessment Runtime messages
va-service	DEBUG	Vulnerability Assessment Service messages

رطس ٰهنجاو نم ٰرشابم اهيلع لوصحلان كنكمي varuntime.log. - اهصحف بولطملا تالجسلى ISE رماوأ:

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

ةنيعم ٰيامن ٰطقنل صحفلا عاجإا تاداشرا TC-NAC Docker ىقلت.

```
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","isPeriodicScanEnabled":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}
```

قايسل ليلديف ئينمألا تارغىللا تانايىب عيىمج نيزخت متي، ۋەجىتنلا مالتسا درجمبۇ.

```
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 - SMB\", \"VulnerabilityVendor\": \"Qualys\", \"VulnerabilityId\": \"QID-90882\", \"cveIds\": \"\", \"cvssBaseScore\": \"4\", \"cvssTemporaryScore\": \"4\", \"VulnerabilityTitle\": \"Windows Remote Desktop Vulnerability (Qualys)\", \"VulnerabilityID\": \"\", \"VulnerabilityVendor\": \"Qualys\", \"VulnerabilityId\": \"QID-90043\", \"cveIds\": \"\", \"cvssBaseScore\": \"7.3\", \"cvssTemporaryScore\": \"6.3\", \"vulnerabilityTitle\": \"SMB\", \"vulnerabilityVendor\": \"Qualys\", \"vulnerabilityID\": \"QID-38601\", \"CVEid\": \"CVE-2013-2566CVE-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-2012-02-020202CVE-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 - SMB", "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 66CVE-2015-2808", "cvssBaseScore": "4.3", "cvssTemporaryScore": "3.7", "vulnerabilityTitle": "SSL/TLS RC4", "vulnerabilityVendor": "qualys"}]
```

ۋەجىن ئىچىلىكلىك كىنكمى - اهصحف متييس يىتللا تالجىسىلنىڭ ئىچىلىكلىك كىنكمى Catalyervice.log. ISE: رەم او رەطس

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

لۇحەملىلى فەعەضلى مىيىقت بىلەت لاسرا مت

```
2016-06-28 17:07:13200 DEBUG [endpointPollerScheduler-3] [] cpm.va.service.util.VaServiceUtil - ::::- VA SendSyslog systemMsg : [{"systemMsg": "91019", "isAutoInsertSelfAcsInstance": true}, {"TC-NAC.ServiceName": "TC-NAC.Status", "VA": "TC-NAC.Details", "VA": "TC-NAC.MACAddress", "C0:4a:00:14:8D:4B": "TC-NAC.IPaddress", "10.62.148.63": "TC-NAC.AdapterInstanceId", "79640B-003": "TC-NAC.VendorName", "Qualys": "TC-NAC.AdapterInstanceName", "QUALYS_VA": ""}]
```

يەتنى يەتح ققحتى AdapterMessageListener لەن قىاقد 5 حسملە ئەلا

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

CVSS لەچىلە بىنچىلىق فرعىم ئەلە DVOM (QID) رايىم و اپنج تامالع

```
2016-06-28 17:24:57556 [SimpleAsyncTaskExecutor-2] []
cpm.va.service.processor.adapterMessageListener -::::- :
{ "RequestedMacAddress": "C0:4a:00:14:8D:4B" "scanStatus": "Assessment_SUCCESS" "lastScanLong": 146713449 000 "ipAddress": "10.62.148.63" ":[ {"VulnerabilityId": "QID-38173" "cvssBaseScore": "9.4" "cvssTemporaryScore": "6.9" "VulnerabilityTitle": " SSL - " "VulnerabilityVendor": "Qualys" } {"VulnerabilityID": "QID-9043" "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" "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.AdapterInstanceId" "796440B-0Address 9b5-4f3b-611-199fb81a4b99" "TC-NAC.VendorName" "Qualys" "TC-NAC.AdapterInstanceName" "QUALYS_VA" } ] }
```

تالكش مەلە ئەجذۇمنلە

و 0.0 نم CVSS_BASE_SCORE تارغىلە رىرقىت ئەلا ISE لىصەي 1. ئەلسەملە CVSS_TEMPORAL_SCORE فەصلە طاقن ئەلا Qualys Cloud رىرقىت يوتىرىپ 0.0 نم فەشتكمە.

تالكش مەلە:

عەم و ئەفشتكمە ئەلا فەصلە طاقن ئەيەر كەن كەمەي Qualys Cloud نم رىرقىتلە ئەنۋە ئەلا ISE ئەلا اهارت ئەل كەلذ.

يەقىن ئەلا catalysercive.log:

```
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" } ] }
```

لحل:

متى مل CVSS ةماليع نأ وأ فعوض طاقن اهل سيل نأ اما و رفص CVSS لايزنـت متـي UI لـالـخـ نـمـ لـوحـمـلاـ نـيـوـكـتبـ مـوقـتـ نـأـ لـبـقـ Qualys Cloud يـفـ اـهـنـيـكـمـتـ نـيـوـكـتبـ دـعـبـ اـهـنـيـكـمـتـ مـتـ يـتـلـاـ CVSSـ طـاقـنـ لـيـجـسـتـ ةـزـيـمـ يـلـعـ يـوـتـحـتـ يـتـلـاـ KnowledgeBaseـ عـاـشـنـاـ مـتـ ثـيـحـ ،ـلـبـقـ نـمـ CVSSـ طـاقـنـ لـيـجـسـتـ نـيـكـمـتـ نـمـ دـكـأـتـلـاـ كـيـلـعـ بـجـيـ .ـةـرـمـ لـوـأـلـ لـوـحـمـلـاـ > دـادـعـاـلـاـ > رـيـرـاـقـتـلـاـ > فـعـضـلـاـ طـاقـنـ لـيـجـسـتـ نـيـكـمـيـ ISEـ اـلـيـلـعـ لـوـحـمـلـاـ لـيـثـ CVSSـ طـاقـنـ لـيـجـسـتـ نـيـكـمـتـ

جهنـ قـيـبـطـتـ نـمـ مـغـرـلـاـ يـلـعـ Qualys Cloudـ ،ـ حـصـصـلـاـ لـيـفـخـتـلـاـ جـهـنـ صـحـفـ يـاـ اـلـ 2ـ ةـلـأـسـمـلـاـ حـصـصـلـاـ لـيـفـخـتـلـاـ.

ملـكـشـمـلـاـ:

هـذـهـ نـمـ مـغـرـلـاـبـ VAـ صـحـفـ لـيـغـشـتـ يـلـاـ يـدـؤـيـ نـأـ بـجـيـ يـذـلـاـ ،ـ حـصـصـمـلـاـ لـيـفـخـتـلـاـ جـهـنـ ةـقـبـاطـمـ تـمـتـ صـحـفـ يـاـ اـعـارـجـاـ مـتـ يـاـ اـلـ ،ـ قـيـقـحـلـاـ.

يفـ ءـاطـخـأـلـاـ حـيـحـصـتـ ضـرـعـ مـتـ catalyervice.log:

```
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.AdapterInstanceId" "79640b7-09b5-4f3b-611-199fb81a4b99" "TC-NAC.VendorName" "Qualys" "TC-  
NAC.AdapterInstanceName" "QUALYS_VA" } ] }
```

لـحلـاـ:

يـوـضـلـاـ حـسـمـلـلـلـهـفـمـ رـيـغـ ةـيـاهـنـلـاـ ةـطـقـنـبـ صـاخـلـاـ IPـ نـاـونـعـ نـأـ يـلـاـ Qualys Cloudـ رـيـشـيـ
لـوـصـأـلـاـ > لـوـصـأـلـاـ > تـارـغـثـلـاـ ةـرـادـإـ يـلـاـ ةـيـاهـنـلـاـ ةـطـقـنـلـ IPـ نـاـونـعـ ةـفـاضـاـ نـمـ دـكـأـتـلـاـ عـاـجـرـلـاـ
ديـدـجـ > IP Track Hostـ

عـاجـارـمـلـاـ

- [رادـصـاـلـاـ نـمـ ةـيـوهـلـاـ تـامـدـخـ كـرـحـمـ لـوـفـسـمـ لـيـلـدـ Cisco 2.1](#)
- [تـادـنـتـسـمـلـاـوـيـنـقـتـلـاـ مـعـدـلـاـ Cisco Systems](#)
- [عـمـ ISE 2.1ـ وـيـدـيـفـلـاـ Qualys](#)

- قيثوت Qualys

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).