

# اهحال صإو ISE لماكت ءاطخأ فاشكتسأ

## تايوت حمل

[قمدقملا](#)

[تاسرامملا لصفأ نع ةمماع ةحمل - ايناث](#)

[CCV-ISE يوتسملا يلإع قفدت ططخم](#)

[اهحال صإو ءاطخأ فاشكتسأ تاداشرا](#)

[اهعيمجت بولطملا تاناي بلا](#)

[ةعقوتملا لجسلا لئاسر](#)

[ةلص تاذ تامولعم](#)

## ةمدقملا

ISE لماكتل اهل صإو CyberVision Center ءاطخأ فاشكتسأ تاوطخ دنتسملا اذه فصبي

## تاسرامملا لصفأ نع ةمماع ةحمل - ايناث

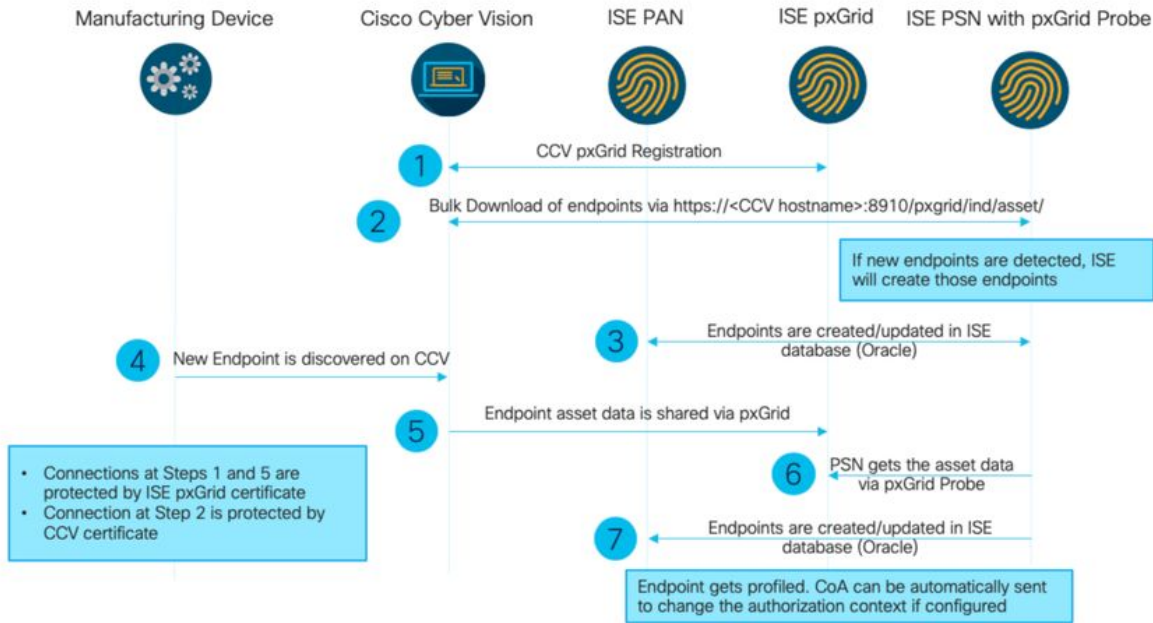
ليغشتلا نامضل اهتاعارم كيلع بجي يتلا اهب يصوملا تاوطخلا يه تاسرامملا لصفأ  
تايصوتلا. ماظنلا نيوكتل حيحصل

- نم (ISE) ةيوهلا تامدخ كرحم رادصإ تاظحالمو، Cisco Cyber Vision رادصإ تاظحالم عجار  
تاريذحتلاو دودحلل او ةيهيحوتلا ئدابملاو تازيمل شذأ يلع لوصحلل Cisco،
- اهذيفنت دعب اهل صإو اهئاطخأ فاشكتسأو ةديج نيوكتل تاريغيغت ي نم ققحتلا

## CCV-ISE يوتسملا يلإع قفدت ططخم

## Configure

### High-Level Flow Diagram



## اهحال صإو عاطخأل فاشك تسأ تاداشرا

اهحال صإو عاطخأل فاشك تسأ راسم دي دحت كنكمي، عم داقال ةلئسأل ىل عباإال لال خ نم ةلا ح دي دحتل ةيلال ةلئسأل ىل ع درل. عاصقتسالا نم ديزم ىل اجاتحت يتل تانوكمل او تيبتل:

- دوجوم تيبتل مأ اثيدح تبتل ماظن اذه له
- ISE ةيؤر نم CyberVision تنكمت له

systemctl status pxgrid-agent رمال مادختساب pxGrid تامدخ ةلا ح نم ققحت

```
root@center:~# systemctl status pxgrid-agent
● pxgrid-agent.service - Agent for interfacing with pxGrid
   Loaded: loaded (/lib/systemd/system/pxgrid-agent.service; enabled)
   Active: active (running) since Wed 2021-03-17 20:12:15 UTC; 17min ago
     Process: 28434 ExecStop=/usr/bin/lxc-stop -n pxgrid-agent (code=exited, status=0/SUCCESS)
    Main PID: 28447 (lxc-start)
      CGroup: /system.slice/pxgrid-agent.service
              └─28447 /usr/bin/lxc-start -F -n pxgrid-agent

Mar 17 20:12:15 center lxc-start[28447]: lxc-start: cgfsng.c: create_path_for_hierarchy: 1306 Path "/sys/fs/cgroup/pids//lxc/pxgrid-agent-6" already existed.
Mar 17 20:12:15 center lxc-start[28447]: lxc-start: cgfsng.c: cgfsng_create: 1363 File exists - Failed to create /sys/fs/cgroup/pids//lxc/pxgrid-agent-6: File exists
Mar 17 20:12:15 center lxc-start[28447]: pxgrid-agent Center type: standalone [caller=postgres.go:290]
Mar 17 20:12:16 center lxc-start[28447]: pxgrid-agent HTTP server listening to: '169.254.0.90:2027' [caller=main.go:135]
Mar 17 20:12:16 center lxc-start[28447]: pxgrid-agent RPC server listening to: '/tmp/pxgrid-agent.sock' [caller=main.go:102]
Mar 17 20:12:16 center lxc-start[28447]: pxgrid-agent Account activated [caller=pxgrid.go:81]
Mar 17 20:12:16 center lxc-start[28447]: pxgrid-agent Service registered, ID: 3d7bee0f-3840-4dc7-a121-a8740f86fa06 [caller=pxgrid.go:99]
Mar 17 20:13:19 center lxc-start[28447]: pxgrid-agent API: getSyncStatus [caller=sync_status.go:34]
Mar 17 20:13:19 center lxc-start[28447]: pxgrid-agent Cyber Vision is in sync with ISE [caller=assets.go:67]
Mar 17 20:23:19 center lxc-start[28447]: pxgrid-agent API: getSyncStatus [caller=sync_status.go:34]
```

- ةلا ع رفوت يي pxGrid ليغشتب ISE موق ي له
- لكاشم ثودح يي تاقيبطتل ادبت نأ لبق ةرشابم ةماعال ةيساسأل ةينبال يي وأ نينوكتل يي ريغت يذل ام

اهحال صإو ةكبشال عاطخأ فاشك تسال ةماعال تاوطخل مدختسأ، ةكبشال يي ةلكشم فاشك تال

ISE نم CyberVision زكرم ل فيضمل مسا رابتخا كنكمي له 1. ةوطخل

```

ESCISE2/admin# ping center
PING center (10.2.3.138) 56(84) bytes of data.
64 bytes from 10.2.3.138: icmp_seq=1 ttl=64 time=1.53 ms
64 bytes from 10.2.3.138: icmp_seq=2 ttl=64 time=1.73 ms
64 bytes from 10.2.3.138: icmp_seq=3 ttl=64 time=1.87 ms
64 bytes from 10.2.3.138: icmp_seq=4 ttl=64 time=1.80 ms

--- center ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.539/1.737/1.878/0.125 ms

```

فيضم الم مسا ةفاض او Secure Shell (SSH) م ادخ تساب ISE CLI ب لاصت ال اب مق ف ، لاصت ال ا رابتخ | رذعت اذا

```

ESCISE2/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ESCISE2/admin(config)# ip host 10.2.3.138 center
Add Host alias was modified. You must restart ISE for change to take effect.
Do you want to restart ISE now? (yes/no) yes

```

CyberVision؟ زكرم نم ISE فيضم الم مسا لاصت ا رابتخ | كنكمي له 2. ةوطخ ل

```

root@center:~# ping ESCISE2.ccv.local
PING ESCISE2.ccv.local (10.2.3.118) 56(84) bytes of data.
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=1 ttl=64 time=2.04 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=2 ttl=64 time=1.88 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=3 ttl=64 time=1.75 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=4 ttl=64 time=1.98 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=5 ttl=64 time=2.02 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=6 ttl=64 time=1.97 ms
^C
--- ESCISE2.ccv.local ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 1.754/1.945/2.045/0.109 ms
root@center:~#

```

زكرم ل ي ف ل ل م ل /data/etc/hosts لى ISE فيضم م سا ةفاض | لواحف ، ةحاسم كانه نكت مل اذاو

```

root@Center:~# cat /data/etc/hosts
127.0.0.1        localhost.localdomain        localhost

# The following lines are desirable for IPv6 capable hosts
::1            localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.1.1 center
10.48.60.131 ise31-tm2.cisco.com

```

تاداهش ل لكاشم فاشتك ا 3. ةوطخ ل

CyberVision. زكرم نم openssl s\_client -connect YourISEHostname:8910 رمألا لخدأ



اهعيمجت بولطمملا تانايبلا

ةكبشلا لكاشملا:

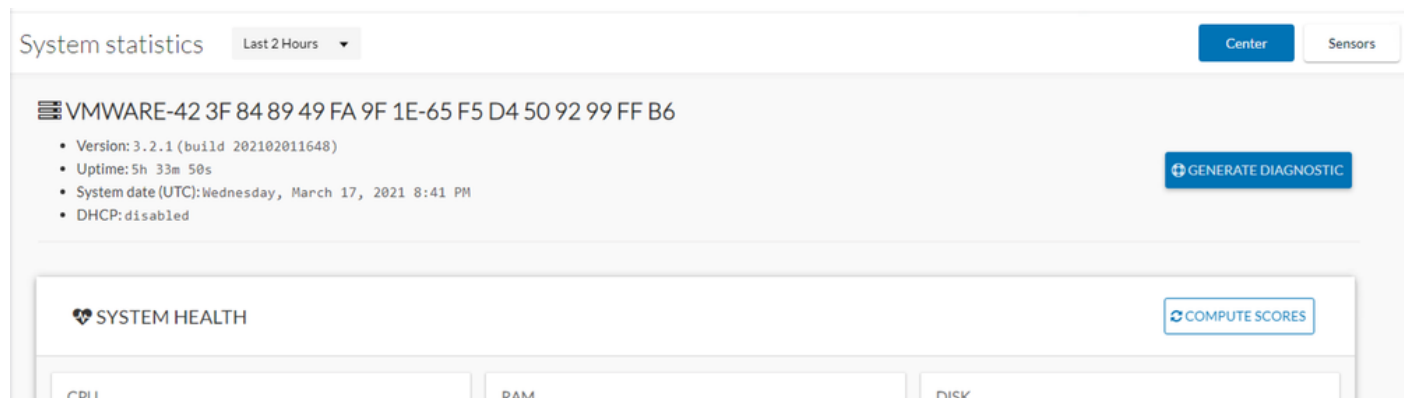
- ةيرامعملل ةسدنهلل

ديفم رما ISE و زكرملا نيب ليصافتلا كلت حضوي ططخم دوجو نإ

- ةياملحل رادج دعاوق
- ةتباثلا تاراسملا
- ةباوبلا نيوكت
- VLAN تانايبوكت

- ISE لكاشم عيمجل اهعيمجت بولطمملا تالاجسلا:

.تانايبلا نادقف بنجت Center صيخشنت فلم عيمجتب ءدبلا كنكمي



ءارجالا اذه مادختساب زكرملا ىلع ةمدقتملا تالاجسلا طيشنتب مق مث

/data/etc/sbs. دلجملل في نيفلم ءاشنإ

ىوتحمللا ىلع هئوتحاو listener.conf لوألا فلملا ةيمست بجي

(.لجسلا يوتسم مامأ ةئدابلا ءحاسملا طحال)

```
root@Center:~# cat /data/etc/sbs/listener.conf
configlog:
loglevel: debug
root@Center:~#
```

يوتحميل الى عهئاوتحاو pxgrid-agent.conf يناثال فلمل اةيمست بجي

(لجسلا يوتسم مام اةئدابلا ءحاسملا طحال)

```
root@Center:~# cat /data/etc/sbs/pxgrid-agent.conf
configlog:
loglevel: debug
```

تامءءال sbs-burrow pxgrid-agent لئغشت ءءاعاب مق واء زكرملا لئغشت ءءاعاب مق ،نئفللملا الك اءشنل ءرءمب

```
Restart service using the command:
#systemctl restart sbs-burrow
#systemctl restart pxgrid-agent
```

(زكرملا نم تالءسلا رئءصتل تافللملا لقن تاوءا مءءتسأ) pxGrid تالءس عئمءتب مق مء

```
root@Center:~# journalctl -u pxgrid-agent > /data/tmp/pxgridLogs.log
```

ISE و زكرملا نئب لاصتالا قءءل لئلءتل tcpdump طاقتل عئمءتب مق

```
root@Center:~# tcpdump -i eth0 -n host CCV_IP and host ISE_IP -w /data/tmp/ccv_ise.pcap
```

- مءءلا ءمزه عئمءتو ISE لئع اءاءأال ءئءصت نئكمءتب مق

نئئعءتب مق . Administration > System > Logging > Debug Log Configuration لئلقننا ، ISE لئع اءاءأال ءئءصت نئكمءتل  
ئئلئ ام لئلجسلا تاؤوتسم

| فلملا<br>بولطملا<br>هنم ققءتل | لئءستلا يوتسم | نوكملا مسا | انوسرب       |  |
|-------------------------------|---------------|------------|--------------|--|
| ئشنم<br>تافل<br>log.فئرعءتل   | اءاءأال ءئءصت | للءم       | PAN (ئراؤءا) |  |

|                            |        |                |                                  |  |
|----------------------------|--------|----------------|----------------------------------|--|
| PSN PxGrid ني كمت عم Probe | للحم   | ءاطخأل احي حصت | ئشنم<br>تافل م<br>log.فيري رعتال |  |
| PxGrid                     | pxgrid | رثأ            | pxgrid-server.log                |  |

ةعقوتمل لجسل لئاسر

Cisco و ،ةلجسمل ةمدخل او ،هلي غشت ادب متي يذال ليكولل زكرم ال في pxGrid ليكوب ةصاخال ءاطخأل احي حصت تالجس رهظت  
Cyber Vision (CCV) ءاشن | ءي سب لاصتا ءاشن (ISE) عم (STOMP) ةهجوم ال ةلصارمل لوكوتوربل (قف د وأ) طي سب لاصتا ءاشن |  
تاتنوكمل/الوصأل دحل اشي دحت:

<#root>

Jul 11 13:05:02 center systemd[1]:

Started Agent

for interfacing with pxGrid.  
Jul 11 13:05:02 center pxgrid-agent[5404]: pxgrid-agent Center type: standalone [caller=postgres.go:543]  
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent RPC server listening to: '/tmp/pxgrid-agent.sock'  
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent HTTP server listening to: '169.254.0.90:2027' [caller=pxgrid.go:544]  
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/AccountActivate body={\"username\":\"root\", \"password\":\"root\"} [caller=pxgrid.go:545]  
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent

Account activated

[caller=pxgrid.go:58]  
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/ServiceRegister body={\"name\":\"pxgrid\", \"description\":\"pxgrid\", \"icon\":\"\", \"url\":\"\", \"assetTopic\":\"/topic/com.cisco.endpoint.asset\"}  
, \"restBaseUrl\":\"https://Center:8910/\"  
Jul 11 13:05:04 center pxgrid-agent[5404]: pxgrid-agent

Service registered

, ID: c514c790-2361-47b5-976d-4a1b5ccfa8b7 [caller=pxgrid.go:76]  
Jul 11 13:05:04 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/ServiceLookup body={\"name\":\"pxgrid\", \"description\":\"pxgrid\", \"icon\":\"\", \"url\":\"\", \"assetTopic\":\"/topic/com.cisco.endpoint.asset\"}  
Jul 11 13:05:05 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/AccessSecret body={\"username\":\"root\", \"password\":\"root\"}  
Jul 11 13:05:06 center pxgrid-agent[5404]: pxgrid-agent

Websocket connect url

=wss://labise.aaalab.com:

8910

/pxgrid/ise/pubsub [caller=endpoint.go:129]  
Jul 11 13:05:07 center pxgrid-agent[5404]: pxgrid-agent

STOMP CONNECT host

=10.48.78.177 [caller=endpoint.go:138]  
Jul 11 13:06:59 center pxgrid-agent[5404]: pxgrid-agent

STOMP SEND destination

```
"opType": "UPDATE"
```

تحتوي مجموعة الأصول assetGroup على سلسلة من الأصول التي تم دمجها مع بعض الأصول التي لا يتم دمجها مع أي أصول أخرى. يتم دمج الأصول التي لا يتم دمجها مع أي أصول أخرى مع الأصول التي يتم دمجها مع بعض الأصول التي لا يتم دمجها مع أي أصول أخرى.

&lt;#root&gt;

```
{"key": "assetGroup", "value": ""}
```

```
, {"key": "assetCustomName", "value": "test"}, {"key": "assetGroupPath", "value": ""}], "assetConnectedLinks": []
```

مل اذاو، تامسلا لاسرلاب موقى CyberVision Center نأ دكؤى اذهو. (حضور وه امك، ةميقب AssetGroup) عقوتملا لئاسرلا قيسنت كلذك ISE عم قيقحتلا كىلعل بچىف، يفاضا لكشب ISE بناج ىلع كلذك سىكعنى

&lt;#root&gt;

```
{"key": "assetGroup", "value": "test group"}
```

```
, {"key": "assetCustomName", "value": "test"}, {"key": "assetGroupPath", "value": "test group"}], "assetConnecte
```

قلص تاذا تاملعم

- [لحلل انجومي ISE و CCV](#)
- [Cisco ISE مادختساب ةيكي ماني دلا ةري غصلا ةي نجلتلا ري فوتل Cisco Cyber ةي فور مادختسا Demo Lab ج ذومت](#)
- [CCV و ISE ي حيضوتلا ضرعلا](#)
- [ISE لم اكات لي لد](#)
- [Cisco نم تالي زينتل او ينفل ا 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