

اهترادو Cyber ةيؤر زكرم مداخ ءاطخا فاشكتسا

تايوت حمل

[ةمدقم](#)

[مداخالتا تي دحت](#)

[ماظنلا ءحص](#)

[ماظنلا تالچس](#)

[ةمدقتملا تالچس](#)

[صرقلا ءحاسم](#)

[رورملا ءكز ءحص نم ققحتلا](#)

[قياسملا رادج بقعت](#)

[ةاد TCPdump](#)

ةمدقم

Cisco Cyber Vision مداخ ءنايصل اهذاختا نكمي يتلا ءفل تخملا تاوطخل دنسما اذه فص ي هتب قارمو اهالصال هءاطخا فاشكتساو.

يذغي (OT) ليغشتلا ءينقت ناما ءيعضو لىل ءقم ءتم ءرطن Cisco Cyber ءيؤر كل رفوت امم، OT، اءا ءا لوصا لوح تامول ءمب كب ءصاخلا تامول ءملا ءينقت ناما تاودا Cyber Vision كتكبش ربع نامالا تاسايس ذي فننن و رطاخملا ءراا لهسل نم لءجي.

مداخالتا تي دحت

يتلا ءديءل تازيمل او ءاطخالا حالصال تارءثلا لولح لىل لوصلل مداخال تي دحت لىل صرءا رشنل تاهويرانيس لىل اءانتسا ءمانربل ي ءهءم م تي.

ماظنلا ءحص

- ماظنلا ءيماء تاهي بنن لاسرل SNMPv3 تارابءا نيوكت

(ءيخيراتلا ءميقل نم ققحتلل) مدختسملا ءهءو نم

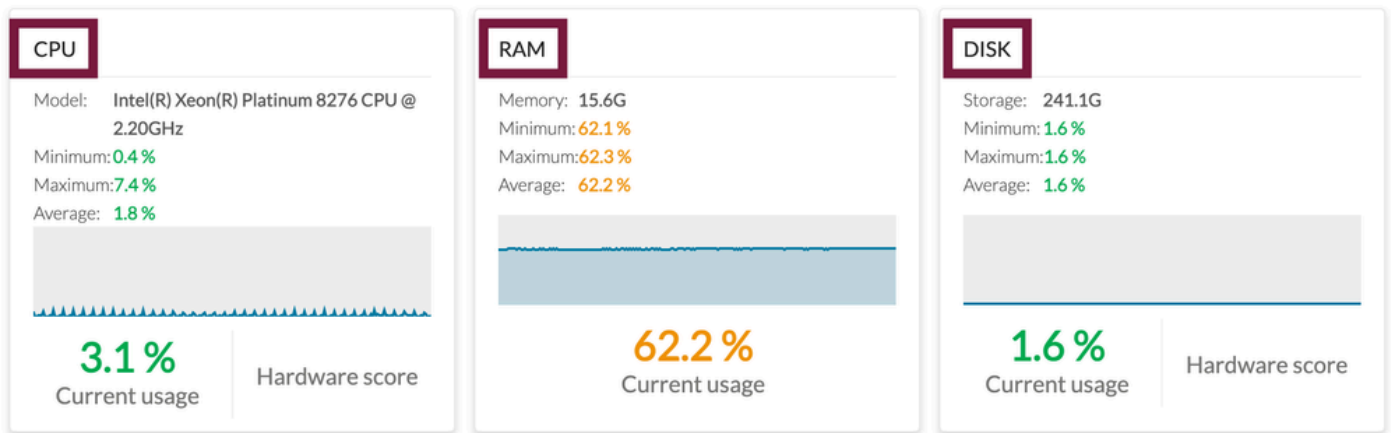
ءءو ماءءتسا نم ققحتلل (راعشتسالا ءهءا و زكرملا) ماظنلا تايءاصءا لىل لقتنا (RAM) ءيئاوشءلا لوصولا ءركا ءو (CPU) ءيؤر ءملا ءءالءملا.

- ءيئاوشءلا لوصولا ءركا ءم 600% طءء يتلا راعشتسالا ءهءا نوكت نا ءقوتمل نمو ءيءاء ءلاء ي 40% اهتبسن ءلبت يتلا (CPU) ءيؤر ءملا ءءالءملا ءءو (RAM).
- ءءو نم 50% و (RAM) ءيئاوشءلا لوصولا ءركا ءم 80% لوح زكارملا نوكت نا ءقوتمل نمو ءيءاء ءلاء ي (CPU) ءيؤر ءملا ءءالءملا.

System Health

⌚ Last hardware scoring: Jun 4, 2025 1:57:44 PM

🔄 Compute scores



نأ عقوتي نكلو، ادج ةيلاع بسن ىلإ دراومل هذه لصت نأ نكمي و. عجرمك مدختست ميقي هذه. كانه ىقبت نأ نود ةددم ةمهم زاجنإ دعب دوعت.

(CLI) رماوأل رطس ةهجاو نم:

لوصول ةركاذو (CPU) ةيتركمرل ةجلاعمل ةدحو مادختسا نم ققحتلل يولعل رمال مدختسا دراومل كلهتست يتل تايلمعل مهفل (RAM) يئوشعل.

رمال مادختساب اهنم ققحتلل نكمي:

'top -n 1 -b' | دي ه -n 5

اذه مادختسا متي. لشف يذل رمال — systemCTL رمال مادختساب ماطنل تايلمع نم ققحت مل يتل تادحول وأ تامدخل ديدحتل اهحالصإو ءاطخأل فاشكتسا ضارغل ءئاش لكشب رمال عقوتم ريغ لكشب تفقوت وأ أدبت.

ماظنل تالجس

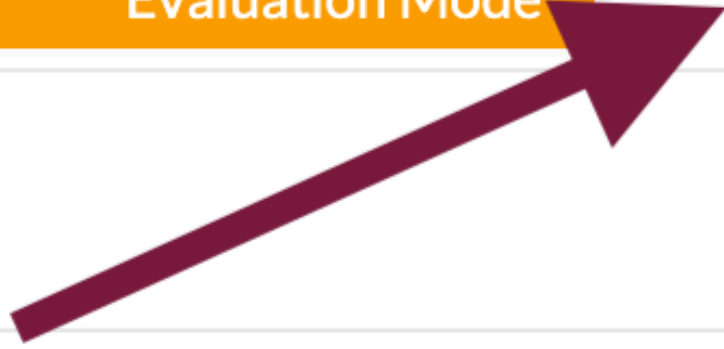
يساسأل ماطنل ىلع تالجس ةدع رفوت:

مدختسمل ةهجاو نم:

رقناو (راعشتسالا ةزهجأ وأ زكرملا) ماطنل تايئاصحإ ىلإ لقتنا. يصيخشتم فلم ءاشنإ يصيخشتم ءاشنإ قوف.

**16**

days remaining
Evaluation Mode



Diagnostic

Last diagnostic generated: Jun 4, 2025 11:33 AM



Download diagnostic



Generate diagnostic

رم أوأال رطس ةهجاو نم:

يرذجال مدختسمال عضو إلى لوصولل sudo -i رمال مدختسأ

مماظنل تالچس بقعتل JournalCTL رمال مدختسأ

journalCtl -r (-r * يسكع)

JournalCTL — 2015-01-11 03:00" ىتح وأ "2015-01-10" ذنم

JournalCtl -u <مسا> ةلمعال

JournalCTL -f (-f * ةعباتم)

JournalCtl -p (مماظنل ي فءاطخأ) أطاخ

sbs-diag رمال لمعتسي تقلطأ تنك عيطتسي ةمزح صيخشتل، اضيأ

ةمدقتملا تالچسلا

تامدخلا هذهل CLI نم ةمدقتملا تالچسلا طيشنت نكمي

ةيفلخلا-SBS

وروب-سإ ي ب سإ

تومرام-سإ ي ب سإ

SBS-LSYNCD-Gather

SBS-Isynd-communication

SBS-gsyncd

SBS-nad

SBS-aspic

ي ك ب ش ه ب ش لماع

يرذجل مدختسملا عضو لىا لوصولل sudo -i رمألا مدختسأ

اهمدختسإ بجي، يلاتلابو، لئاسرلاب ماطنلا قارغا لعفلاب ةمدقتملا تالچسلا هذهل نكمي TAC. قيرف عم لمعل دنع طقف

صرقلا ةحاسم

- ةدعاق ي ف اهنيزخت متي راعشتسالا ةزهجأ لبق نم ةللحمل او ةدراولا تانايبلا عي مج . تانايبلا
- df -h رمألا مادختساب تانايبلا مسق ي ف ةرفوتملا ةحاسملا بقار
- rm -rf رمألا مدختسأ . /data/tmp/capture/ تحت ةكبشلا طاقنلا فيظنتب مق . /data/tmp/capture/* اذ طاقنلا تاي لمع عي مج فذل
- ةميدقلا صيخشنتلا تافل م ةفاك فذل
- رمألا مادختساب تانايبلا ةدعاق ي ف اهي ف بوغرمل ريغو ةميدقلا تانايبلا ةلازاب مق sbs-db purge-xxxxx.

رورملا ةكرح ةحص نم ققحتلا

رورملا ةكرح قفدت عبتت TCPdump و IPTABLES مادختسإ

ةيامحل رادج بقعت

ك اهطاقسإ مت ي تال مزحل ليجست متي . مداخل لىا IPTABLES ةيامح رادج ني كمت مت "DropInput و DropForward".

(GREP ةلسلس | iptables -L -n -v) اهيلع ةطقسملا مزحل صحتل IPTABLES تادادع نم ققحت

(لېصاصافتالو لىلىع ةملاع رظن | JournalCTL) لجسلا يف اهطاقسا مت يتا مزحل نغ ثحبل

٤ TCPdump

ههڄاويلع اههالصالواهيئاڻڀڻا فاش ڪتس او تان اڀال رورم ڪڙهه ڦارمل همادختسا ڪمي
مداخلي ڦه ڪڙهه ڦارمل همادختسا ڪمي

طاق تالالەي لمع فاقيل Ctrl+C ىلغ طغضا، رورمالە كرح تقررغ اذا.

ةلثمألا

123 : عانيم NTP (UDP/TCP 123): tcpdump -i [ethX] تاقفت عقب قارمل

1.2.3.4 فيض الم tcpdump -i [ethX] : فيضم نم ةرداصل/ةدراول رورملا ةكرح ةبقارمل

PCAP: فلم ي ف طاقت لال ا ظ ف حل

```
tcpdump -i [ethX] 1.2.3.4 -r /data/tmp/your_file.pcap
```

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 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