

# نمآل بيولا زاهج عادأ عااخأ فاشك تسأ SHD تالچس مادختساب اهالصلإو

## تايوتحمل

[عمدقمل](#)

[عيساسال تابلطمل](#)

[تابلطمل](#)

[عمدختسمل تانوكمل](#)

[SHD تالچس يه ام](#)

[SHD تالچس دلل لوصول](#)

## عمدقمل

عادأ عااخأ فاشك تسأ عيفيكو (shd\_log) ماظنلأ عيامح جم انرب تالچس دن تسمل اذع فصي  
لچسل اذع عم اهالصلإو (SWA) نمآل بيولا زاهج.

## عيساسال تابلطمل

### تابلطمل

عيلاتل عيضاوملاب عفرعم كيدل نوك ت ناب Cisco ي صوت:

- تبت م Physical أو Virtual Secure Web Appliance (SWA)
- هتبتت أو صيخرتل طيشنت م
- ع SSH (Secure Shell) لي مع
- دادعال لعم لم تكا
- SWA دلل يرادل لوصول

### عمدختسمل تانوكمل

عني عم عي دام تانوكم وجمارب تارادصلل ع دن تسمل اذع رصتقي ال

عصاخ عي لم عم عئي بي ف دوجوملأ عزهجال نم دن تسمل اذع ي ف دراوول تامول عملا عاشنإ م  
تنك اذإ. (يضا رتفا) حوسمم نيوك تب دن تسمل اذع ي ف عمدختسملأ عزهجال عي مع تأب  
رمأ يال لم تحملل ري ثأتلل كم هف نم دكأت ف، لي غشتل دي ق ك تك تبش

## SHD تالچس يه ام

عادالاب عول عتمل تاي لم علل تاءاصح لم طعمب عم ادتسملأ عيرشبلأ عي منتلل تالچس ظف تحت  
عقي قد لك SWA ف

SHD: لجس رطس ىلع لاثم يلي اميف

Mon Jun 9 23:46:14 2022 Info: Status: CPULd 66.4 DskUtil 5.2 RAMUtil 11.3 Reqs 0 Band 0 Latency 0 Cache  
SrvConn 0 MemBuf 0 SwpPgOut 0 ProxLd 0 Wbrs\_WucLd 0.0 LogLd 0.0 RptLd 0.0 WebrootLd 0.0 SophosLd 0.0 Mc

ال (FTP) تافللملا لقن لوكوتورب نمو (CLI) رمأوالا رطس ةهجاو نم ةلوبقم SHD تالجس دعت (GUI) ةيموسرلا مدختسملا ةهجاو نم لجسلا ضرعل تاراخي دجوت

## SHD تالجس ىلإ لوصولا

رمأوالا رطس ةهجاو نم:

1. CLI في tail وأ grep بتكا.
2. مقررلا بتكاو ةمئاقلا نم FTP عالطتسا |shd\_log type: SHD Log Retrieval| نع شح ب. نرتقملا.
3. لخد شحبلل ةيداع تاريبع ةباتك كنكمي. GREP ىلإ يداعل ريبعتلا لخدإ في تقولاو خيراتلا ةباتك كنكمي، لاثملا لابس ىلع، تالجسلا يضارتفاك اذه كرت كنكمي >[Y]؟ فرحألا ةلاجل ساسح ريغ شحبللا اذه نوكي نأ ديرت له اذه ىلإ جاتحت ال SHD\_LOG في فلم يأل ةساسح ةلاجل نع شحبللا ىلإ ةجاحب تنك اذا ال راخلا.
5. اذا ال يضارتفاك رطسلا اذه طبض كنكمي >[n]؟ ةقباطم ريغ دونب نع شحبللا ديرت له ك بصاخلا يداعل GREP ريبعت ادع ام عيش لك نع شحبلل تجتحت اذه تكرت نإ، GREP نم جاتنإلا في رفوتي طقف راخي اذه >[n]؟ تالجسلا لبيذت ديرت له ي. لالجال فلملا نم رطس لوأ نم لجس SHD ل يدي وه (N) يضارتفاك لقا رماً تاجرخم اهسفن يه تاجرخم نإف، "Y" تدح اذا >[n]؟ تاجرخملا ميقرت ديرت له (عونلا) تالجسلا لخد شحبللا كنكمي اضيأ تاحفصلو رطسألا نيب لقننتلا كنكمي Q. عونلا بسح لجسلا ضرع نم جورخلل، (لاخدإلا حاتفم طغضاو ةساسألا ةملكل مث/

نم FTP:

1. تاهجالا > ةكبشلا > (GUI) ةيموسرلا مدختسملا ةهجاو نم FTP نيكمتم نم دكأت.
2. FTP ربع SWA ب لاصتالا.
3. تالجسلا ىلع SHD\_LOG دلجم يوتحي.

## SHD لجس لوقح

ةلصفم SHD تالجس في ةدوجوملا لوقح:

لوقحلا مقرر	مسالا	فرعملا	فصولا
8	CPULd	ةيويئملا ةبسنلا 99 ىلإ 0 نم	ةجلالعمللا ةدحو لمح ةيزكرملا

			<p>ةبس نلا يل امجإ  ةدحول ةي وئملا  ةيزك رمل اةجل املا  ةمدختسملا (CPU)  مت امك ماظنلا يل  ةطساوب هنع غالبإل  ليغشتلا ماظن</p>
10	يتوأ كسد	<p>ةي وئملا ةبس نلا  99 لىل 0 نم</p>	<p>صرقلا مادختسإ  لكشب همادختسإ مت  مسق/ لىل دعابت م  تانايبل</p>
12	ليتامار	<p>ةي وئملا ةبس نلا  99 لىل 0 نم</p>	<p>ةركاذ مادختسإ  يئاوشعلا لوصول  ةي وئملا ةبس نلا  يتلا ةرحلا ةركاذلل  اهنع غالبإل مت  ماظن ةطساوب  ليغشتلا</p>
14	بيقر	<p>يناوثل / بلطلا</p>	<p>تابلطلا  تاكرحلا ددع طسوت م  يف (تابلطلا)  ةيضامل اةقي دل</p>
16	ةباصع	<p>ةيناث/تيا ب وليك</p>	<p>قاطنلا ظفح مت  ي ددرتلا  قاطنلا طسوت م  مت يذلا ي ددرتلا  ةقي دل اةقريفون  ةيضامل  طسوت م لداع ي ام -  قاطنلا ضرع ريفون  لالخ SNMP ل ي ددرتلا  ةيضامل اةقي دل</p>
18	<sup>1</sup> لوصولا نمز	<p>يللم) ةيناث ي لل م</p>	<p>لاق تناللا نمز طسوت م</p>

		(ةيناث	<p>ي ف (ةباجتسالال تقو) ةريخالال ةقيدلال</p> <p>يناثلال لقال ذخال - لوصولال لجال ي ف راقم رهظي يذلال يذلال تقولال لاصتال هقرغتسي مدختسملال نم TCP وا WSA لال يئاهنال مدختسملال نم مداخال لال يئاهنال ك ف متي مل اذا بيولال (لاصتالال ريفشت</p> <p>صيخلتبا WSA موقت متي بلط لكل تقولال ي ف هلوخد ليجست لال لوصولال لجال ةريخالال قئاقدلال دادعأ لال هميسقتو تابلللال هذال لعل لوصولال لوصولال نمز طسولم ل SHD</p>
20	CacheHit	مقرر	<p>نيزختلال ةركاذ تغلب طسولملا تقولال ةقيدلال ي ف ةيضاملا.</p> <p>- نيزختلال ةركاذ تغلبت لوكوتوربل تقولال ةدملا طسولم SNMP ةقيدلال لال ةيضاملا</p>
22	نوكيلك	مقرر	<p>تالاصتال ددع يلامجال ةيلالالال مالعملال</p> <p>WSA لال مالعملال نم يلامجال لئفاكم - SNMP ليل مع تالاصتال ةيلالالال</p>

24	SrvConn	مقرر	تالاصت إددع يلامجإة ةيلاحلا مداخل بيو مداخل إ WSA نم يلامجال ئفاكم - SNMP مداخل تالاصتإة. ةيلاحلا
26	MemBuf <sup>2</sup>	ةيؤملا ةبس نلا 99 إ 0 نم	تقؤملا ةركاذلا نزم يلامجال رادقملا ةركاذل يلاحلا تقؤملا نيزختلا ةرفؤملا ليكولل اناجم
28	SwpPgOut	مقرر	يتلا تاحفصلا ددع امك، اهلا دب تسإ مت نم كلذ نع غالبإل مت ليغشتلا ماظن لبق فلم وأ ةحفصلا فلم ، تاحفصلا ليحرت يلع ةحاسم نع ةرابع تباثلا صرقلا كرحم اهم ادختسإ متي نيزختل تقؤم عقومك دنع تامولعمل ةركاذ مادختسإ يئاوشعلا لوصول لماك لكشب (RAM)
30	ld سكورب	ةيؤملا ةبس نلا 99 إ 0 نم	سكوربلا ةيلمع لمح عيجم ةجلا عم نع ةلوؤسم ةجلا عم ةدراول تابلطل (HTTP/HTTPS/FTP/SOCKS)
32	WBRS_WUCld	ةيؤملا ةبس نلا	ةعمس رابتخإ لمح

		99 ىل 0 نم	بيولا كرحم لم ةمدختسملا ةيلمعلا يلعفل WBRS حسملا عم ليكول ةيلمع لعافتت تايلمع ءارجل reqscand ةيلمع حسم WBRS.
34	LogLd	ةيولملا ةبسنلا 99 ىل 0 نم	ليكولا لجس ليحت
36	RptLd	ةيولملا ةبسنلا 99 ىل 0 نم	كرحم ليحت ريقتلا ءاشنل نع ةلوؤسم ةيلمعلا ريراقتلا تانايب ةدعاق عم 'ReportD' لعافتتي ةدعاق ءاشنل 'hestackd' بيولا بقت تانايب.
38	WebrootLd	ةيولملا ةبسنلا 99 ىل 0 نم	Webroot لجح Antimalware
40	دلپسوفوس	ةيولملا ةبسنلا 99 ىل 0 نم	داضملا سوفوس لجح تاسوري فلل
42	McAfeeLd	ةيولملا ةبسنلا 99 ىل 0 نم	McAfee جم انرب AntiVirus Load

44	WTTLd	ةيؤئملا ةبس نللا 99 لىل 0 نم	رورم ةكرح ةطغض بيولا
46	AMLd	ةيؤئملا ةبس نللا 99 لىل 0 نم	نم ةمدقتملا ةيماحللا (AMP) تاسوري فاللا

1. ةيمنتلا تالجس يف لاقتناللا نمز يف ةيلع ةورذ ثودح عقوت نكمي نايحألا ضعب يفو .  
ىلع تابللللا نم ديدعلا كانه نكي مل اذا لاثملا لىبس ىلع ، ةمادتسملا ةيرشبللا  
لاثملا لىبس ىلع - ةليوط ةدملا لاصتالا نم ءاهتنا كانه نوكي ام ةطقن دنعو WSA  
هئاهتنا دنع ةقيقدلا كليل لوصوللا نمز ةدايز دحاولا بلللا اذهل نكمي مث .مايأ ةدع  
لوصولا تالجس يف لوخدلا لىجستو .

2. يف بوتكم وه امك :

نوكي نا نكمي لاعف لكشب working ماظنلا (RAM) يئوشعلا لوصولا ةركاذ مادختسا  
نم رخآ لكشب اهمادختسا متي ال يئوشعلا (RAM) يئوشعلا لوصولا ةركاذ نال ، 90% نم ىلعأ  
نكي مل اذا .بيولا تانئاكل تقؤملا نيزختلا ةركاذ لبق نم اهمادختسا متي ماظنلا لبق  
100% دنع ةقلعلا تسيل ةميقلال هذهو ءادألاب قلعتت ةريطخ تالكشم experiencing كماظن  
يعي ببط لكشب operating ماظنلاف .

 لوصولا ةركاذ مدختسي ادحاو انوكم ليكولل تقؤملا نيزختلا ةركاذ دعت :ةظحالم  
هذه يئوشعلا

## SHD تالجس مادختساب اهحالا صاوا عا طخألا فاشكتسا

رخآ عفترم ةجلع لمحم

تالجسلا أرقاو ةلاقملا هذه نم 1 لودجلا نم ققحتف ،اعفترم ىرخألا ةيلمعلا لمح ناك اذا  
ةيلمعلا كليل ةقلعتملا .

لاع لاقتناللا نمز

يف Proxy\_track تالجس نم ققحتلا لكيل بحج ، SHD تالجس يف عفترم لوصولا نمز تيأر اذا  
يف .يلعلا لوصولا نمز هب زي متي يذلا يئومزلا راطإلا ىلع روثعلا /data/pub/track\_stats/  
يه مسق لك مامأ ةدوجوملا ماقرألا .لوصولا نمزب ةقالع امهل نالجس كيدل ليكوللا راسم  
زمرلا اذه يف ، لاثملا لىبس ىلع .ديهمت ةداعإ رخآ ذنم راركتلا تارم ددع يلامجإ





ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومجم مادختساب دن تسمل اذه Cisco تچرت  
ملاعلاء انء عي مج ي ف ني مدختسمل معد ي وتحم مي دقتل ةيرشبل او  
امك ةقيقد نوك ت نل ةللأل ةمچرت لصف أن ةظحال م يچري. ةصاغل مه تغلب  
Cisco ي لخت. فرتحم مچرت م اهم دقي ي تلل ةي فارتحال ةمچرتل عم لاعل او  
ىل إأمئاد عوچرلاب ي صؤت و تامچرتل هذه ةقد نع اهتيل وئسم Cisco  
Systems (رفوتم طبارل) ي لصلأل يزي لچن إلال دن تسمل