

سوري ف فيرعت تاراخي: ةياهنلا طاقنل AMP Linux ليغشتل ماظن في ClamAV

تاوت حمل

[ةمدقملا](#)

[ةقباسلا تارادصلال عم قفاوتلا](#)

[ClamAV سوريف تافيرعت راخي ريغت](#)

[ةياهنلا ةطقن في ديوجل دادعلا نم ققحتلا](#)

ةمدقملا

ةئيهتل نيراخي نال ةياهنلا طاقنل AMP رفوت، Linux ل صوم نم 1.11.0 رادصلال نم اءب ClamAV سوريف فيرعت:

1. طقف سكونيل
2. ClamAV ل مأك

مادختساب تافل ملسب سكونيل ل صوم ماق، احاتم طقف سكونيل راخي حبصي نأ لب ق ةراض جمارب تاعيقوت ةومجمل هذه نمضتت. ClamAV سوريف ل ةلماكل فيرعتلا ةومجمل ةيطغت رفوي كلذ نأ نم مغلرا يلعو. Windows و Android و MacOS و Linux ليغشتل ماظنل ةيزكرملا ةجلعلا ةدحو تقو لثم) ليغشتل تقول ةريبك دراوم اضيا بلطتي هنا ال، ةلماش ةومجمل مادختسال AMP نيوكت نم ةدافتسال سكونيل ةمظنأ ضعبل نكمي. (ةركاذلو طقف سكونيل ماظن مدختست يتلا ةريغصل ClamAV تاسوريف تافيرعت.

مادختسا يدوي. ةلماكل ةومجمل نم 10% نم لقا Linux ل طقف سوريفلا فيرعت فلم مجح لوكوتورب ليغشت نكمملا نم لعجي امك، ةبسوخل تافورصم ليلقت يلا رغصا ةومجمل ةيطغتلا ليلقت نأ ال، اءال تازيم نم مغلرا يلع. ةدودحمل دراوملا تاذه ةمظنأ ال يلع AMP ضعبل ابسانم نيوكتلا اذه لعجي Linux ليغشتل ماظن فالخب ةراضلا جماربلل نخت/فيضتست يتلا تامقللمل ةمئالم نوكتس، لاثملا ليلبس يلع. طقف تاقيبطتلا يتلا تامقللمل ةبسانم نوكت نل اهنكل (تاقيبطتلا تامقللمل لثم) طقف Linux تافللم تامقللمل لثم) Linux ليغشتل ماظنل ةصاخلا ريغ تافللمل نيزخت/ةفاضتساب اضيا موقت رايتخال ةضياقمل هذه ةنزاوم ماظنلا لوؤسم يلع بجي. (SMB و ديربلال او FTP تافللمل تاسوريفلا تافيرعت نم ةبسانملا ةومجمل.

اماه

ثدح رادصلال و ل صوملا نم 1.11.0 رادصلال يلا ةياهنلا طاقنل عيمج ةيقربتب ةدشب ي صوي نيح في. طقف Linux ليغشتل ماظن يلع ديوجل سوريفلا فيرعت راخي مادختسا لب ق ضعبل في اهكولس نأ ال، ديجل راخيلا لبقت مدقألا تارادصلال او 1.10.x ل صوم تارادصلال نأ يلع لوصحلل ةقباسلا تارادصلال عم قفاوتلا مسق عجار. ايهي دب نوكتي نل تالاجل ليلصافت.

ةقباسلا تارادصلال عم قفاوتلا

ةياهنلا طاقنل نيوكت لب ق رابتعالا نيعب اهذأل ةمهم ي عجارت قفاوت ةلكشم كانه

قېبېت رمت سېس Linux لېغش تال ماظن ىل ع دېدج ل سوري فال فيرعت راځ مادخت سال ة لمال ة عومج مالا ليزنت مت اذا مدق ال تال صوم ل او 1.10.x ىل ع سوري فال ل مالكل فيرعت ال ، طقف سكونيل ىل ع دېدج ل سوري فال فيرعت راځ مادخت سال هنيوكت مت اذا . ل ع فال اب ، شي دحت ب موقېس و لمالكل اب تاسوري فال فيرعت ة عومج م شي دحت فاقېب ل صوم ل موقېس مادخت سال ىل ك ل ذ ي دوې نأ نكمي . ك ل ذ ع هنيي عت مت ي ذل طقف سكونيل سوري فال فيرعت و Windows و MacOS تافيرعت نكل و ة شي دح ل Linux تاسوري فال تافيرعت ة ياهن ل ة طقن ة م يدق Android .

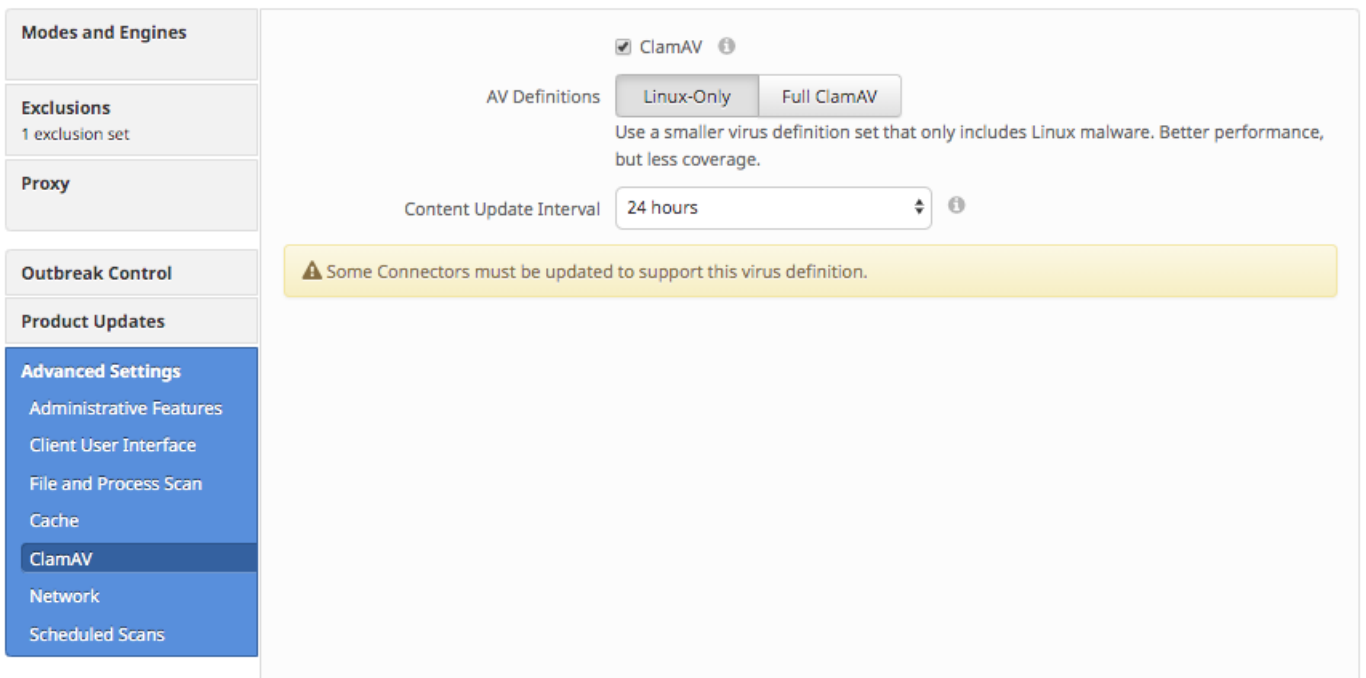
نال متحم نارارق كانه:

1. ش دح ا رادص ا و 1.11.0 ىل ل صوم ل ة يقرت ب مق .
2. لمالكل ClamAV ىل ل ر خ ا ةرم ClamAV سوري فال فيرعت دادع ا ر ي غت ب مق .

ClamAV سوري فال تافيرعت راځ ري غت

ىل ع ة ياهن ل طاقن ة اب و ل AMP مادخت س اب ClamAV سوري فال فيرعت راځ نېوكت نكمي ىل ل ل ا ق ت نال ا ق ي ر ط ن ع ج ه ن ل ل راځ ل راځ ري غت نكمي . ب ي و ل ا :

ClamAV > ة مدق مت تادادع ا > ريرحت > [Linux ة ساي س] > تاساي س ل ا > ة راد ا ل ا



The screenshot shows the ClamAV configuration interface. On the left is a sidebar with navigation options: Modes and Engines, Exclusions (1 exclusion set), Proxy, Outbreak Control, Product Updates, and Advanced Settings (highlighted). Under Advanced Settings, there are sub-options: Administrative Features, Client User Interface, File and Process Scan, Cache, ClamAV (selected), Network, and Scheduled Scans. The main panel shows 'ClamAV' is checked. Under 'AV Definitions', 'Linux-Only' is selected over 'Full ClamAV'. A note states: 'Use a smaller virus definition set that only includes Linux malware. Better performance, but less coverage.' The 'Content Update Interval' is set to '24 hours'. A yellow warning banner at the bottom says: 'Some Connectors must be updated to support this virus definition.'

شي دحت ل ا ي ف ة ياهن ل طاقن ىل ع دېدج ل دادع ا ل ر س ي ، AV تافيرعت ج ه ن دادع ا ر ي غت د ع ج ه ن ل ا دادع ا ل ل ا خ ن م ر ي خ ا ت ل ا ا ذ ه ي ف م ك ح ت ل ا م ت ي . تاسوري فال فيرعت ل ل و دج م ل ا ي ل ا ت ل ا "ىوتحم ل ا شي دحت" ي ل خ ا د ل ا .

ي ف "ا ذ ه سوري فال فيرعت م عدل ا ه شي دحت ب ج ي ي ت ل ا تال صوم ل ا ض ع ب" ر ي ذ ح ت ل ا ر ه ظ ي د ق ة ط س ا و ب ه ت ر ا د ا م ت ل ل ق ا ل ا ىل ع د ح ا و ل صوم كانه ن ا ك اذا ة مدق مت ل ClamAV تادادع ا ة ش ا ش تال صوم ل ا شي دحت ب ة دش ب ى صوي . Linux ل صوم ن م ق ف ا و ت م ر ي غ ر ا د ص ا ل ي غ ش ت ب موقې ج ه ن ل ا . طقف Linux ل ي غ ش ت ل ا ماظن ب ة ص ا خ ل ا تافيرعت ل ا دادع ا مادخت سال ل ب ق ر ي ذ ح ت ل ا ا ذ ه ل و ح و

ة ياهن ل ا ة طقن ي ف دېدج ل ا دادع ا ل ن م ق ق ح ت ل ا

ة ر ك ا ذ ل ا م ج ح نو ك ي نأ ب ج ي ، طقف Linux ل ي غ ش ت ل ا ماظن تافيرعت مادخت سال هنيوكت دن ع

ت.ي.اباچيم 100 نم لقا AMP Connector يتيلمع نم لك لع مجملا مي قملا

ي.لاتلا رمألا مادختساب كلذ صحف نكمي

```
top -p `pidof ampdaemon` -p `pidof ampscansvc`
```

ت.اخ م لم نم ةني ع يلي امي فو

```
top - 23:52:51 up 15:11, 7 users, load average: 0.36, 1.10, 0.83
Tasks:  2 total,  0 running,  2 sleeping,  0 stopped,  0 zombie
%Cpu(s):  2.5 us,  0.5 sy,  0.0 ni, 97.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem : 3861508 total, 309220 free, 1732560 used, 1819728 buff/cache
KiB Swap: 2097148 total, 2064116 free,  33032 used. 1629348 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
88910	root	20	0	1323172	32904	6752	S	0.7	0.9	3:20.16	ampdaemon
88937	cisco-a+	20	0	258764	8400	2704	S	0.0	0.2	1:23.73	ampscansvc

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيد نوك تنل ةللأل ةمچرت لصف انءمچال مچرئى. ةصاغل متهتبل ب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لاعل او
ىل اءءاد ةوچرلاب يصوت و تامچرتل هذه ةقد نع اهتيل وئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزىلچنل دن تسمل