

ةعمس ةمدخ "أطخ AMP ةدوزملا ESA ىقلتت لوصولل ةلباق ريغ فلملا"

تایوتھملا

ةمدقمل

AMP ل هي قلت مت يذلا "لوصل قلباو ريغ فلملا قعمس قمدخ" أطخلات حصر
احالص او عاطخألا فاشكتسا
قلص تاذ تامولعم

ةمدقملا

ع Cisco (ESA) نم ينورتكللإا ديربلا ناماً زاهج ىلإ بوسنملأا هيبنتلا دنتسملا اذه فصي
ىلع ٰرداق ريع ٰمدخلأ نوكت ثيبح، (AMP) ٰراضلأ جماربلا نم ٰمدقتملأ ٰيامحلأا نيكمت
فـلمـلا ىـلـع فـرعـتـلـلـ 443 وـأ 32137 ذـفـنـمـلـا رـبـعـ لـاصـتـالـا.

يذلا "لوصول لبلاق ريغ فلملا ئعممس ئمداخ" أطخلا تتحص ل هيقلت مت AMP

يـنورـتـكـلـإـلـاـ دـيـرـبـلـاـ نـامـأـلـاـ AsyncOSـ نـمـ 8.5.5ـ رـادـصـ إـلـاـ يـفـ ESAـ إـلـعـ مـادـخـتـسـالـلـ AMPـ رـادـصـ إـلـاـ مـتـ صـيـخـرـتـ لـالـخـ نـمـ ـقـلـاسـرـلـاـ هـذـهـ نـوـلـوـفـسـمـلـاـ يـقـلـتـيـ ESAـ:

The Warning message is:

The File Reputation service is not reachable.

Last message occurred 2 times between Tue Jul 26 10:17:15 2015 and Tue Jul 26 10:18:16 2016.

Version: 12.5.0-066
Serial Number: 123A82F6780XXX9E1E10-XXX5DBEFCXXX
Timestamp: 07 Oct 2019 14:25:13 -0400

32137 ذفن ملا رباع ةكبش لالا ىلع لصتت ال حجرألا ىلع اهنكلو،AMP، ۆمەخ نىكەمت مەتى دق فەلملە مسا ىلع فەرعەتلل.

ربيع "فلملا ڦعمس" لاصتا هيدل نوکي ناً لوفسم راتخي ناً نكمي ،لاحلا وه اذه ناك اذا 443 ذفنملما.

نم دکأت و رمأوألا رطس ٥٥ج او نم enableConfig > advanced رمألا ليغشت بمق ، كل ذب مايقلل فلملأا ٤عمس ل (443 ذفنملأ) SSL لاصتا نيكتم ديرت له ل ٢ ديدحت [N]:

(Cluster example.com)> **ampconfig**

Choose the operation you want to perform:

- SETUP - Configure Advanced-Malware protection service.
 - ADVANCED - Set values for AMP parameters (Advanced configuration).
 - SETGROUP - Add this appliance to the group of appliances that can share File Analysis reporting details.
 - CACHESETTINGS - Configure the cache settings for AMP.

```
- CLUSTERSET - Set how advanced malware protection is configured in a cluster.  
- CLUSTERSHOW - Display how advanced malware protection is configured in a cluster.  
[]> advanced
```

Enter cloud query timeout?

[15]>

Choose a file reputation server:

1. AMERICAS (cloud-sa.amp.cisco.com)
2. AMERICAS(Legacy) (cloud-sa.amp.sourcefire.com)
3. EUROPE (cloud-sa.eu.amp.cisco.com)
4. APJC (cloud-sa.apjc.amp.cisco.com)
5. Private reputation cloud

[1]>

Do you want use the recommended analysis threshold from cloud service? [Y]>

Enter heartbeat interval?

[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]> **y**

Proxy server detail:

Server :

Port :

User :

Do you want to change proxy detail [N]>

Do you want to suppress the verdict update alerts for all messages that are not delivered to the recipient? [N]>

Choose a file analysis server:

1. AMERICAS (https://panacea.threatgrid.com)
2. EUROPE (https://panacea.threatgrid.eu)
3. Private analysis cloud

[1]>

< هلیلحتو فلملا ۃعمس > نامألا تامدخ رتخداف، ةيموسرلا مدخلتسملأا ۃھج او مدخلتسست تنك اذا
مادختسا رایتخالا ۃناخ دیدحت نم دکأت و (ۃلدرسن) ۃمدقتم تادادعإ > ۃماعلأا تادادعإا ریحـت
SSL حضـوم وـه اـمـک:

SSL Communication for File Reputation:

Use SSL (Port 443)

Tunnel Proxy (Optional):

Server: Port:

Username:

Password: 

Retype Password: 

Relax Certificate Validation for Tunnel Proxy 

نـيـوكـتـلـاـ ىـلـعـ تـارـيـيـغـتـلـاـ عـيـمـجـوـ يـأـ قـيـبـطـتـبـ مـقـ

كنـكمـيـ اـمـھـلـشـفـ وـأـ لـاصـتـالـ اوـ ۃـمـدـخـلـاـ حـاجـنـ ىـلـعـ عـالـطـالـلـ یـلـاحـلـاـ لـجـسـ عـجـارـ،ـ اـرـیـخـ اوـ
لـیـذـلـاـ رـیـبـمـأـ مـادـخـتـسـابـ (CLI) رـمـاـوـأـلـاـ رـطـسـ ۃـھـجـ اوـ نـمـ كـلـذـ قـيـقـحـتـ.

تـالـجـسـ يـفـ اـذـهـ ىـرـتـسـ تـنـكـ،ـ مـدـقـتـمـ ۢ amconfig ۢ ىـلـعـ تـارـيـيـغـتـلـاـ عـاـرـجـ اـلـبـقـ:

Mon Jan 26 10:11:16 2015 Warning: amp The File Reputation service in the cloud is unreachable.

Mon Jan 26 10:12:15 2015 Warning: amp The File Reputation service in the cloud is unreachable.

Mon Jan 26 10:13:15 2015 Warning: amp The File Reputation service in the cloud is unreachable.

تالجس يف كل ذ ٽدهاـشـمـ كـنـكـمـيـ،ـمـدـقـتـمـ >ـىـلـعـ رـيـيـغـتـلـاـ عـارـجـاـ دـعـبـ

Mon Jan 26 10:19:19 2015 Info: amp stunnel process started pid [3725]

Mon Jan 26 10:19:22 2015 Info: amp The File Reputation service in the cloud is reachable.

Mon Jan 26 10:19:22 2015 Info: amp File reputation service initialized successfully

Mon Jan 26 10:19:22 2015 Info: amp File Analysis service initialized successfully

Mon Jan 26 10:19:23 2015 Info: amp The File Analysis server is reachable

Mon Jan 26 10:20:24 2015 Info: amp File reputation query initiating. File Name = 'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain

Mon Jan 26 10:20:24 2015 Info: amp Response received for file reputation query from Cloud. File Name = 'amp_watchdog.txt', MID = 0, Disposition = file unknown, Malware = None, Reputation Score = 0, sha256 = a5f28f1fed7c2fe88bcdf403710098977 fa12c32d13bfb78bbe27e95b245f82, upload_action = 1

متـيـوـقـئـاـقـدـ 10ـ لـكـ قـبـاسـلـاـ لـاثـمـلـاـ يـفـ حـضـوـمـ وـهـ اـمـكـ amp_watchdog.txtـ فـلـمـ لـيـغـشـتـ مـتـيـسـ مـتـيـوـقـئـاـقـدـ 10ـ لـكـ قـبـاسـلـاـ لـاثـمـلـاـ يـفـ حـضـوـمـ وـهـ اـمـكـ amp_watchdog.txtـ فـلـمـ لـيـغـشـتـ مـتـيـسـ اـعـزـجـ فـلـمـلـاـ اـذـهـيـ اـعـزـجـ لـجـسـ يـفـ هـعـبـتـAMPـ.

مـتـ يـتـلـاـ تـافـلـمـلـاـ (ـعـاـونـأـ)ـ عـونـ نـمـ ٽـلـاسـرـلـبـاـقـمـ لـجـسـ يـفـ يـدـاعـ مـاـلـعـتـسـاـ يـأـ نـوـكـيـسـ ٽـلـاسـرـلـاـ ٽـذـهـلـ الـثـامـمـ فـلـمـلـاـ لـيـلـحـتـوـ فـلـمـلـاـ ٽـعـمـسـلـ اـهـنـيـوـكـتـ:

Wed Jan 14 15:33:01 2015 Info: File reputation query initiating. File Name = 'securedoc_20150112T114401.html', MID = 703, File Size = 108769 bytes, File Type = text/html

Wed Jan 14 15:33:02 2015 Info: Response received for file reputation query from Cloud. File Name = 'securedoc_20150112T114401.html', MID = 703, Disposition = file unknown, Malware = None, Reputation Score = 0, sha256 = claf8efe4eeb4e04551a8a0f5 533d80d4bec0205553465e997f9c672983346f, upload_action = 1

(ٽـلـاسـرـلـاـ فـرـعـمـ طـبـرـىـلـعـ اـرـدـاقـ لـوـؤـسـمـلـاـ نـوـكـيـ نـأـ بـجـيـ،ـذـهـ لـجـسـلـاـ تـاـمـوـلـعـمـ مـاـدـخـتـسـابـ دـيـرـبـلـاـ تـالـجـسـ يـفـ)

اـهـحـاـلـصـ اوـ عـاطـخـأـلـاـ فـاشـكـتـسـاـ

هـذـهـلـ لـاـصـتـاـ حـتـفـ نـاـمـضـلـ ٽـكـبـشـلـاـوـ ٽـيـاـمـحـلـاـ رـادـجـ تـاـدـادـعـاـ عـجـارـ

فـصـوـلـاـ	فـيـضـمـلـاـ مـسـاـ خـ/ـلـخـدـ ٽـكـوـتـ ٽـذـفـ ٽـرـبـلـاـ ٽـنـمـلـاـ	هـلـيـلـحـتـوـ فـلـمـلـاـ ٽـعـمـسـ >ـ نـاـمـأـلـاـ تـاـمـدـخـ يـفـ نـوـكـمـ وـهـ اـمـكـ	هـلـيـلـحـتـوـ فـلـمـلـاـ ٽـعـمـسـ >ـ نـاـمـأـلـاـ تـاـمـدـخـ يـفـ نـوـكـمـ وـهـ اـمـكـ	هـلـيـلـحـتـوـ فـلـمـلـاـ ٽـعـمـسـ >ـ نـاـمـأـلـاـ تـاـمـدـخـ يـفـ نـوـكـمـ وـهـ اـمـكـ
ٽـامـدـخـ ٽـلـاـ ٽـوـصـوـلـاـ	443 TCP جـرـاخـ ٽـمـسـقـ	،ـهـلـيـلـحـتـوـ فـلـمـلـاـ ٽـعـمـسـ >ـ نـاـمـأـلـاـ تـاـمـدـخـ يـفـ نـوـكـمـ وـهـ اـمـكـ	،ـهـلـيـلـحـتـوـ فـلـمـلـاـ ٽـعـمـسـ >ـ نـاـمـأـلـاـ تـاـمـدـخـ يـفـ نـوـكـمـ وـهـ اـمـكـ	،ـهـلـيـلـحـتـوـ فـلـمـلـاـ ٽـعـمـسـ >ـ نـاـمـأـلـاـ تـاـمـدـخـ يـفـ نـوـكـمـ وـهـ اـمـكـ
ٽـاـفـلـمـلـاـ ٽـلـوـصـوـلـاـ	32137 TCP جـرـاخـ	مـداـوـخـ عـمـجـتـ ٽـمـلـعـمـ ،ـمـدـقـتـمـلـاـ ٽـعـطـقـمـلـاـ ،ـمـدـقـتـمـلـاـ ٽـعـطـقـمـلـاـ	مـداـوـخـ عـمـجـتـ ٽـمـلـعـمـ ،ـمـدـقـتـمـلـاـ ٽـعـطـقـمـلـاـ ،ـمـدـقـتـمـلـاـ ٽـعـطـقـمـلـاـ	مـداـوـخـ عـمـجـتـ ٽـمـلـعـمـ ،ـمـدـقـتـمـلـاـ ٽـعـطـقـمـلـاـ ،ـمـدـقـتـمـلـاـ ٽـعـطـقـمـلـاـ

ربـعـ جـمـانـرـبـ رـبـعـ ٽـبـاحـسـلـاـ ٽـمـدـخـ ٽـلـاـ كـيـدـلـ ESAـ نـمـ يـسـاسـأـلـاـ لـاـصـتـاـ رـابـتـخـاـ كـنـكـمـيـ

لیلحتو تافلملا ئامس و AMP تامدخ ىلإ كيدل زاهجلال وصو ئيناكما نامضل Telnet جمانرب حاجنب تافلملا.

ههـجـاـوـىـلـعـ تـافـلـمـلـاـ لـيـلـحـتـوـ فـلـمـلـاـ ئـامـسـبـ ئـاصـلـاـ نـيـوـكـتـ مـتـيـ:ـ ئـظـاحـاـلـمـ
مدختسمـلـاـ هـهـجـاـوـنـمـ وأـقـمـدـقـتـمـ تـارـايـخـ enable config > مـادـخـتـسـابـ (CLI) رـمـأـوـالـاـ رـطـسـ
ئـمـاعـالـاـ تـادـادـعـالـاـ رـيـحـتـ > هـلـيـلـحـتـوـ فـلـمـلـاـ ئـامـسـ > نـامـأـلـاـ تـامـدـخـعـمـ (GUI) ئـيمـوسـرـلـاـ >
هـلـدـسـنـمـ)ـ قـمـدـقـتـمـ تـادـادـعـاـ.

بلطي دقـفـ ،ـ فـلـمـلـاـ ئـامـسـ (ـمـداـوـخـ)ـ مـداـخـوـ ESAـ نـيـبـ قـفـنـ لـيـكـوـ مـدـخـتـسـتـ تـنـكـ اـذـاـ:ـ ئـظـاحـاـلـمـ
مـتـيـ .ـ قـفـنـلـاـ لـيـكـوـلـ ـةـدـاهـشـلـاـ ـةـحـصـ نـمـ قـقـحـتـلـاـ هـيـلـمـعـ فـيـفـخـتـ رـايـخـ نـيـكـمـتـ كـنـمـ
عـيـقـوـتـ مـتـيـ مـلـ اـذـاـ هـيـسـاـيـقـلـاـ ـةـدـاهـشـلـاـ ـةـحـصـ نـمـ قـقـحـتـلـاـ يـطـخـتـلـ رـايـخـلـاـ اـذـهـ رـيـفـوـتـ
لـاـثـمـلـاـ لـيـبـسـ ـىـلـعـ ESAـ.ـ لـبـقـ نـمـ ـهـ بـ قـوـثـومـ رـذـجـ عـجـرمـ لـبـقـ نـمـ قـفـنـلـاـ لـيـكـوـ مـداـخـ ـةـدـاهـشـ
قـوـثـومـ يـلـخـادـ قـفـنـ لـيـكـوـ مـداـخـ ـىـلـعـ اـيـتـاـذـ ـةـعـقـوـمـ ـةـدـاهـشـ مـدـخـتـسـتـ تـنـكـ اـذـاـ رـايـخـلـاـ اـذـهـ دـدـحـ
بـ5ـ.

فـلـمـلـاـ ئـامـسـ لـاـثـمـ:

```
10.0.0-125.local> telnet cloud-sa.amp.sourcefire.com 443
```

```
Trying 23.21.199.158...
Connected to ec2-23-21-199-158.compute-1.amazonaws.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

فـلـمـلـاـ لـيـلـحـتـ لـاـثـمـ:

```
10.0.0-125.local> telnet panacea.threatgrid.com 443
```

```
Trying 69.55.5.244...
Connected to 69.55.5.244.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

قـفـتـلـلـ لـيـكـوـ دـجـوـيـ الـوـ ،ـ فـلـمـلـاـ ئـامـسـ مـداـخـ ىـلـإـ Telnetـ جـمـانـرـبـ لـاسـرـاـ ـىـلـعـ اـرـدـاقـ ESAـ نـاـكـ اـذـاـ
هـكـبـشـ مـادـخـتـسـابـ قـيـبـطـتـلـاـ لـيـجـسـتـ ـةـدـاعـاـ مـزـلـيـ دقـفـ ،ـ لـاـصـتـالـاـ رـيـفـشـتـ كـفـ ـىـلـعـ لـمـعـيـ
يـفـخـمـ رـمـأـ كـانـهـ (CLI)ـ رـمـأـوـاـ رـطـسـ هـهـجـاـوـىـلـعـ .ـ تـادـيـدـهـتـلـاـ:

```
10.0.0-125.local> diagnostic
```

```
Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- SERVICES - Service Utilities.
[]> ampregister
```

```
AMP registration initiated.
```

ةلص تاذ تامولع

- ةراضـلا جـمـارـبـلا نـم ـقـمـدـقـتـمـلـا ةـيـامـحـلـلـ رـابـتـخـا (AMP)
- ESA مـدـخـتـسـمـ ةـلـدـأـ
- وـأـ (ICID) نـقـحـلـا لـاـصـتـاـ فـرـعـمـ وـأـ (MID) ةـلـاسـرـلـا فـرـعـمـ وـهـ اـمـ: لـوـحـ ةـلـوـادـتـمـلـا ةـلـئـسـأـلـاـ (DCID)؟ـ
- ـىـلـعـ دـيـرـبـلـا تـالـجـسـ ضـرـعـ وـثـجـبـلـا يـنـنـكـمـيـ فـيـكـ (ESA)ـ
- ـتـادـنـتـسـمـلـاـوـيـنـقـتـلـاـ مـعـدـلـاـ Cisco Systemsـ

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).