在ESA上配置靜態檔案信譽主機或備用檔案信譽雲伺服器池

目錄

簡介

本文說明如何配置思科郵件安全裝置(ESA)，以使用高級惡意軟體防護(AMP)進行通訊並使用靜態主機或其他信譽雲伺服器池來獲取檔案信譽。

背景資訊

檔案信譽查詢是ESA上AMP兩個層中的第一層。檔案信譽在檔案通過ESA時捕獲每個檔案的指紋，並將其傳送到AMP基於雲的情報網路進行信譽判定。根據這些結果，ESA管理員可以自動阻止惡意檔案並應用管理員定義的策略。 檔案信譽雲服務託管在Amazon Web Services(AWS)上。 當您對本文檔中描述的主機名執行DNS查詢時，您會看到「.amazonaws.com」已列出。

ESA上的第二層AMP是檔案分析。 本文檔未涵蓋的內容。

檔案信譽流量的SSL通訊預設使用埠32137。在配置服務時，埠443可能用作備用埠。請參閱ESA使用手冊「檔案信譽過濾和檔案分析」一節以瞭解完整的詳細資訊。ESA和網路管理員可能需要先驗證池的IP地址、IP位置以及埠通訊(32137與443)連線，然後再繼續進行配置。

預設AMERICAS（傳統）信譽雲伺服器池(cloud-sa.amp.sourcefire.com)

在ESA上許可、啟用和配置「檔案信譽」後，預設情況下會為此信譽雲伺服器池設定它：

- 美洲（傳統）(cloud-sa.amp.sourcefire.com)

主機名「cloud-sa.amp.sourcefire.com」是DNS規範名稱記錄(CNAME)。CNAME是DNS中的一種資源記錄，用於指定域名是另一個域（即「規範」域）的別名。與此CNAME關聯的池中的關聯主機名可能類似:

- ec2-107-22-180-78.compute-1.amazonaws.com(107.22.180.78)
- ec2-54-225-142-100.compute-1.amazonaws.com(54.225.142.100)
- ec2-23-21-208-4.compute-1.amazonaws.com(23.21.208.4)
- ec2-54-83-195-228.compute-1.amazonaws.com(54.83.195.228)

可以選擇另外兩個檔案信譽伺服器選項：

- 美洲(cloud-sa.amp.cisco.com)
- 歐洲(cloud-sa.eu.amp.cisco.com)

本文檔的「靜態檔案信譽伺服器主機名(.cisco.com)」部分中介紹了這兩個伺服器。

當您運行此**dig**或**nslookup**查詢時，您可以隨時從您的網路驗證與AMERICAS cloud-sa-amp.sourcefire.com CNAME關聯的主機：

```
$ dig cloud-sa.amp.sourcefire.com +short
cloud-sa-589592150.us-east-1.elb.amazonaws.com.
107.22.180.78
54.225.208.214
23.21.208.4
54.83.195.228

$ nslookup cloud-sa.amp.sourcefire.com
Server: 208.67.222.222
Address: 208.67.222.222#53

Non-authoritative answer:
cloud-sa.amp.sourcefire.com canonical name = cloud-sa-589592150.us-east-1.elb.amazonaws.com.
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 54.225.208.214
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 54.83.195.228
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 107.22.180.78
Name: cloud-sa-589592150.us-east-1.elb.amazonaws.com
Address: 23.21.208.4
```

> **附註**：這些主機不是靜態的，建議不要將ESA文件信譽流量僅限制在這些主機上。查詢結果可能會有所不同，因為池中的主機將發生更改，恕不另行通知。

您可以通過此第三方工具驗證IP地理位置：

- http://geoiplookup.net/ip/107.22.180.78
- http://geoiplookup.net/ip/54.225.208.214
- http://geoiplookup.net/ip/23.21.208.4
- http://geoiplookup.net/ip/54.83.195.228

靜態檔案信譽伺服器主機名(.cisco.com)

2016年，思科開始為AMP的檔案信譽服務提供基於「.cisco.com」的主機名。從以下站點可獲得可用於檔案信譽的靜態主機名和IP地址：

- cloud-sa.amp.cisco.com（北美 — 美國）
- cloud-sa.eu.amp.cisco.com（歐洲 — 愛爾蘭共和國）
- cloud-sa.apjc.amp.cisco.com（亞太 — 日本）

您可以驗證來自網路的主機和關聯的IP地址，並運行**dig**或**nslookup** 查詢：

北美洲（美國）：

```
$ dig cloud-sa.amp.cisco.com +short
52.21.117.50
```

歐洲（愛爾蘭共和國）：

```
$ nslookup cloud-sa.eu.amp.cisco.com
Server: 208.67.222.222
Address: 208.67.222.222#53

Non-authoritative answer:
Name: cloud-sa.eu.amp.cisco.com
Address: 52.30.124.82
```

亞太地區（日本）：

```
 $ dig cloud-sa.apjc.amp.cisco.com +short
52.69.39.127
```

您可以通過此第三方工具驗證IP地理位置：

- http://geoiplookup.net/ip/52.21.117.50
- http://geoiplookup.net/ip/52.30.124.82
- http://geoiplookup.net/ip/52.69.39.127

目前，尚未計畫停用「.sourcefire.com」主機名。

Alternative EUROPE信譽雲伺服器池(cloud-sa.eu.amp.sourcefire.com)

對於需要向僅基於歐盟的伺服器和資料中心傳送特定流量的基於歐盟(EU)的客戶，管理員可以將ESA配置為指向歐盟靜態主機或歐盟信譽雲伺服器池：

- cloud-sa-eu.amp.cisco.com
- cloud-sa.eu.amp.sourcefire.com

與預設主機名「cloud-sa.amp.sourcefire.com」類似，主機名「cloud-sa.eu.amp.sourcefire.com」也是CNAME。與此CNAME關聯的池中的關聯主機名可能類似於：

- ec2-54-217-245-97.eu-west-1.compute.amazonaws.com(54.217.245.97)
- ec2-54-247-186-153.eu-west-1.compute.amazonaws.com(54.247.186.153)
- ec2-176-34-122-245.eu-west-1.compute.amazonaws.com(176.34.122.245)

可以從您的網路中驗證與EUROPEAN cloud-sa.eu.amp.sourcefire.com CNAME關聯的主機，並運行**dig**或**nslookup** 查詢：：

```
$ dig cloud-sa.eu.amp.sourcefire.com +short
cloud-sa-162723281.eu-west-1.elb.amazonaws.com.
54.217.245.97
54.247.186.153
```

```
176.34.122.245

$ nslookup cloud-sa.eu.amp.sourcefire.com
Server: 208.67.222.222
Address: 208.67.222.222#53

Non-authoritative answer:
cloud-sa.eu.amp.sourcefire.com canonical name = cloud-sa-162723281.eu-west-1.elb.amazonaws.com.
Name: cloud-sa-162723281.eu-west-1.elb.amazonaws.com
Address: 54.247.182.97
Name: cloud-sa-162723281.eu-west-1.elb.amazonaws.com
Address: 176.34.122.245
Name: cloud-sa-162723281.eu-west-1.elb.amazonaws.com
Address: 54.247.186.153
```

> **附註**：這些主機不是靜態的，建議不要僅基於這些主機來限制ESA檔案信譽流量。查詢結果可能會有所不同，因為池中的主機將發生更改，恕不另行通知。

您可以通過此第三方工具驗證IP地理位置：

- http://geoiplookup.net/ip/176.34.122.245
- http://geoiplookup.net/ip/54.247.186.153
- http://geoiplookup.net/ip/54.217.245.97

在ESA上配置靜態檔案信譽主機或備用檔案信譽雲伺服器池

可以通過ESA上的GUI或CLI配置檔案信譽。本文檔中列出的配置步驟將演示CLI配置。但是，可以通過GUI應用相同的步驟和資訊(「安全服務」(Security Services)>「檔案信譽和分析」(File Reputation and Analysis)>「編輯全域性設定……」(Edit Global Settings...)>「檔案信譽高級設定」(Advanced Settings for File Reputation))。

AsyncOS 10.x及更高版本

AsyncOS 10.x的新功能允許將ESA配置為使用私有信譽雲（本地檔案信譽伺服器）或基於雲的檔案信譽伺服器。通過此更改，AMP配置不再提示使用「輸入信譽雲伺服器池」步驟輸入主機名。您必須選擇將其他檔案信譽伺服器設定為私有信譽雲並提供該主機名的公鑰。

對於10.0.x及更高版本，配置備用AMP信譽伺服器時，可能需要輸入與該主機名關聯的公鑰。

所有AMP信譽伺服器使用相同的公鑰：

```
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEchIap1VqPuGibM2n3wjfhqQZdzC9
WI1Z7QZ2Q7VesLe+A53TxYujeo7fCDKJEQKrPjU6kI36PSZusObr9Cur/g==
-----END PUBLIC KEY-----
```

此示例將幫助您將備用檔案信譽伺服器設定為cloud-sa.eu.amp.sourcefirce.com:

```
my11esa.local > ampconfig

NOTICE: This configuration command has not yet been configured for the current cluster mode
(Machine 122.local).

What would you like to do?
```

```
1. Switch modes to edit at mode "Cluster Test_cluster".
2. Start a new, empty configuration at the current mode (Machine 122.local).
3. Copy settings from another cluster mode to the current mode (Machine 122.local).
[1]>

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
Appliance Group ID/Name: Not part of any group yet


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.
- CLEARCACHE - Clears the local File Reputation cache.
- 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.sourcefire.com)
2. Private reputation cloud
[2]>

Enter AMP reputation server hostname or IP address?
[]> cloud-sa.eu.amp.sourcefire.com

Do you want to input new public key? [N]> y

Paste the public key followed by a . on a new line
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEchIap1VqPuGibM2n3wjfhqQZdzC9
WI1Z7QZ2Q7VesLe+A53TxYujeo7fCDKJEQKrPjU6kI36PSZusObr9Cur/g==
-----END PUBLIC KEY-----
.
Enter cloud domain?
[a.immunet.com]>

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

Enter heartbeat interval?
[15]>

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

Please make sure you have added the Amp onprem reputation server CA certificate in certconfig-
>CERTAUTHOROTIES->CUSTOM
Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>
```

```
Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private analysis cloud
[1]>
```
提交所有配置更改。

AsyncOS 9.7.x及更低版本

此有關適用於郵件安全的AsyncOS 9.7.2-065的示例將幫助您將備用信譽雲伺服器池升級到cloud-sa.eu.amp.sourcefirce.com:

```
my97esa.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
Appliance Group ID/Name: Not part of any group yet


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.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Enter cloud domain?
[a.immunet.com]>

Enter reputation cloud server pool?
[cloud-sa.amp.sourcefire.com]> cloud-sa.eu.amp.sourcefire.com

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

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private Cloud
[1]>

Enter heartbeat interval?
[15]>

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

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>
```
提交所有配置更改。

內部部署檔案信譽伺服器（FireAMP私有雲）

本地檔案信譽服務器（也稱為FireAMP私有雲）的使用從用於郵件安全的AsyncOS 10.x開始。

如果您在網路中部署了Cisco AMP虛擬私有雲裝置，則現在您可以查詢郵件附件的檔案信譽，而無需將它們傳送到公共信譽雲。要將裝置配置為使用本地檔案信譽伺服器，請參閱《ESA使用手冊》或聯機幫助中的「檔案信譽過濾和檔案分析」一章。

驗證

使用本節內容，確認您的組態是否正常運作。

若要檢視傳遞到已配置的靜態主機或信譽雲伺服器池的檔案信譽流量，請使用指定的過濾器從ESA執行資料包捕獲，以捕獲埠32137或埠443流量。

在本示例中，使用cloud-sa.eu.amp.sourcefire.com雲伺服器池和SSL通訊並使用埠443...

在AMP日誌中將此記錄到ESA:

```
Sun Mar 26 21:17:45 2017 Info: File reputation query initiating. File Name =
'contract_604418.doc', MID = 463, File Size = 139816 bytes, File Type = application/msword
Sun Mar 26 21:17:46 2017 Info: Response received for file reputation query from Cloud. File Name
= 'contract_604418.doc', MID = 463, Disposition = MALICIOUS, Malware = W32.8A78D308C9-95.SBX.TG,
Reputation Score = 99, sha256 =
8a78d308c96ff5c7158ea1d6ca25f3546fae8515d305cd699eab2d2ef3c08745, upload_action = 2
```

運行ESA資料包跟蹤捕獲了此會話：

```
1060 28.504624 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 74 51391
443 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 WS=64 SACK_PERM=1 TSval=198653388 TSecr=0
1072 28.594265 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 74 443
51391 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=142397924
TSecr=198653388 WS=256
1073 28.594289 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=1 Ack=1 Win=16384 Len=0 TSval=198653478 TSecr=142397924
1074 28.595264 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com SSL 502
Client Hello
1085 28.685554 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 66 443
51391 [ACK] Seq=1 Ack=437 Win=30208 Len=0 TSval=142397947 TSecr=198653478
1086 28.687344 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 1434
Server Hello
1087 28.687378 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=437 Ack=1369 Win=15040 Len=0 TSval=198653568 TSecr=142397947
1088 28.687381 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 146 [TCP
segment of a reassembled PDU]
1089 28.687400 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=437 Ack=1449 Win=14912 Len=0 TSval=198653568 TSecr=142397947
1090 28.687461 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 1434 [TCP
segment of a reassembled PDU]
1091 28.687475 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=437 Ack=2817 Win=13568 Len=0 TSval=198653568 TSecr=142397947
1092 28.687479 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 1346 [TCP
segment of a reassembled PDU]
```

```
1093 28.687491 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=437 Ack=4097 Win=12288 Len=0 TSval=198653568 TSecr=142397947
1094 28.687614 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 [TCP
Window Update] 51391  443 [ACK] Seq=437 Ack=4097 Win=16384 Len=0 TSval=198653568 TSecr=142397947
1096 28.711945 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 1120
Certificate
1097 28.711973 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=437 Ack=5151 Win=15360 Len=0 TSval=198653594 TSecr=142397953
1098 28.753074 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TLSv1 392
Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1099 28.855886 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 348 New
Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1100 28.855934 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=763 Ack=5433 Win=16128 Len=0 TSval=198653740 TSecr=142397989
1101 28.856555 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TLSv1 252
Application Data, Application Data
1104 28.952344 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 252
Application Data, Application Data
1105 28.952419 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=949 Ack=5619 Win=16192 Len=0 TSval=198653837 TSecr=142398013
1106 28.958953 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TLSv1 300
Application Data, Application Data
1107 29.070057 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 268
Application Data, Application Data
1108 29.070117 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=1183 Ack=5821 Win=16192 Len=0 TSval=198653951 TSecr=142398043
1279 59.971986 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TLSv1 103
Encrypted Alert
1280 59.972030 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=1183 Ack=5858 Win=16320 Len=0 TSval=198684848 TSecr=142405768
1281 59.972034 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 66 443
51391 [FIN, ACK] Seq=5858 Ack=1183 Win=33280 Len=0 TSval=142405768 TSecr=198653951
1282 59.972044 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [ACK] Seq=1183 Ack=5859 Win=16320 Len=0 TSval=198684848 TSecr=142405768
1283 59.972392 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TLSv1 103
Encrypted Alert
1284 59.972528 my11esa.local -> ec2-176-34-122-245.eu-west-1.compute.amazonaws.com TCP 66 51391
443 [FIN, ACK] Seq=1220 Ack=5859 Win=16384 Len=0 TSval=198684848 TSecr=142405768
1285 60.062083 ec2-176-34-122-245.eu-west-1.compute.amazonaws.com -> my11esa.local TCP 66 443
51391 [ACK] Seq=5859 Ack=1221 Win=33280 Len=0 TSval=142405791 TSecr=198684848
```

您看到流量通過埠443進行通訊。從我們的ESA(my11esa.local)，它與hostname ec2-176-34-122-245.eu-west-1.compute.amazonaws.com通訊。此主機名與IP地址176.34.122.245關聯：

```
$ dig ec2-176-34-122-245.eu-west-1.compute.amazonaws.com +short
176.34.122.245
```

IP地址176.34.122.245是cloud-sa.eu.amp.sourcefire.com的CNAME的池成員：

```
$ dig cloud-sa.eu.amp.sourcefire.com +short
cloud-sa-162723281.eu-west-1.elb.amazonaws.com.
54.217.245.200
54.247.186.153
176.34.122.245
```

在本例中，通訊由配置的信譽雲伺服器池cloud-sa.eu.amp.sourcefire.com定向和接受。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

使用Telnet測試連線

若要驗證到檔案信譽雲的埠級別連線，請使用已配置的信譽雲伺服器池的主機名，然後使用**telnet**測試埠32137或埠443（如已配置）。

```
my97esa.local> telnet cloud-sa.amp.sourcefire.com 443

Trying 23.21.208.4...
Connected to ec2-23-21-208-4.compute-1.amazonaws.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

與歐盟的完全連線，通過埠443成功：

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 443

Trying 176.34.113.72...
Connected to ec2-176-34-113-72.eu-west-1.compute.amazonaws.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

與EU的完全連線，無法通過埠32137:

```
my97esa.local> telnet cloud-sa.eu.amp.sourcefire.com 32137

Trying 176.34.113.72...
telnet: connect to address 176.34.113.72: Operation timed out
telnet: Unable to connect to remote host
```

您可以使用相同的telnet測試方法使用埠32137或埠443，對信譽雲伺服器池的CNAME後面的直接IP或主機名進行telnet測試。如果無法成功telnet至主機名和埠，則可能需要檢查ESA外部的網路連線和防火牆設定。

驗證本地檔案信譽伺服器的telnet成功將通過如下所示的相同過程完成。

公鑰的輸入

當您在運行AsyncOS 10.x及更高版本的ESA上輸入公鑰時，請確保已成功貼上或載入公鑰。公鑰中的任何錯誤都會顯示在配置輸出中：

```
Do you want to input new public key? [N]> y

Paste the public key followed by a . on a new line
-----BEGIN PUBLIC KEY-----
MEAwEAYHKoZIzj0CAQYFK4EEAAEDLAAEAIHPMkqCH057gxeQK6aUKqmpqk+1AW0u
vxOkpuI+gtfLICRijTx3Vh45
-----END PUBLIC KEY-----
.
Failed to save public key
```

如果收到錯誤，請重試配置。有關持續錯誤，請與思科支援聯絡。

檢視AMP日誌

當您檢視ESA上的AMP日誌時，請確保您看到檔案信譽查詢時指定的「來自雲的檔案信譽查詢」：

```
Sun Mar 26 11:28:13 2017 Info: File reputation query initiating. File Name =
'billing_fax_271934.doc', MID = 458, File Size = 143872 bytes, File Type = application/msword
Sun Mar 26 11:28:14 2017 Info: Response received for file reputation query from Cloud. File Name
= 'billing_fax_271934.doc', MID = 458, Disposition = MALICIOUS, Malware = W32.50944E2888-
100.SBX.TG, Reputation Score = 0, sha256 =
50944e2888b551f41f3de2fc76b4b57cb3cd28e718c9265c43128568916fe70f, upload_action = 2
```

如果您看到這種情況，查詢將從本地ESA快取提取響應，而不是從配置的信譽雲伺服器池提取響應:

```
Sun Mar 26 11:30:18 2017 Info: File reputation query initiating. File Name =
'billing_fax_271934.doc', MID = 459, File Size = 143872 bytes, File Type = application/msword
Sun Mar 26 11:30:18 2017 Info: Response received for file reputation query from Cache. File Name
= 'billing_fax_271934.doc', MID = 459, Disposition = MALICIOUS, Malware = W32.50944E2888-
100.SBX.TG, Reputation Score = 0, sha256 =
50944e2888b551f41f3de2fc76b4b57cb3cd28e718c9265c43128568916fe70f, upload_action = 2
```

其他錯誤和警報

ESA管理員可能會收到此通知。如果收到此資訊，請重新執行配置和驗證過程。

```
The Warning message is:

amp The previously selected regional server cloud-sa.eu.amp.sourcefire.com is unavailable.
Server cloud-sa.amp.sourcefire.com has been selected as default.

Version: 11.0.0-028
Serial Number: 1111CEE15FF3A9F9A1111-1AAA2CF4A1A1
Timestamp: 26 Mar 2017 11:09:29 -0400
```

相關資訊

- 正確AMP操作所需的伺服器地址
- 技術支援與文件 - Cisco Systems