

将安全终端私有云与安全Web和电子邮件集成

目录

[简介](#)

[先决条件](#)

[使用的组件](#)

[在继续集成之前进行验证检查](#)

[步骤](#)

[配置安全终端私有云](#)

[配置安全网络设备](#)

[配置思科安全邮件](#)

[从安全网络和邮件获取AMP日志的步骤](#)

[测试安全网络设备和安全终端私有云之间的集成。](#)

[SWA访问日志](#)

[SWA AMP日志](#)

简介

本文档介绍将安全终端私有云与安全网络设备(SWA)和安全邮件网关(ESA)集成所需的步骤。

先决条件

Cisco 建议您了解以下主题：

- [安全终端AMP虚拟私有云](#)
- [安全Web设备\(SWA\)](#)
- [安全邮件网关](#)

使用的组件

SWA (安全Web设备) 15.0.0-322

AMP虚拟私有云4.1.0_202311092226

安全电子邮件网关14.2.0-620



注意：该文档对所有相关产品的物理和虚拟变体均有效。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

在继续集成之前进行验证检查

1. 验证是否 Secure Endpoint Private Cloud/SWA/Secure Email Gateway 具有所需的许可证。您可以验证功能密钥 SWA/Secure Email 或检查智能许可证是否已启用。
2. 如果您计划检查HTTPS流量，则必须在SWA上启用HTTPS代理。您需要解密HTTPS流量才能执行任何文件信誉检查。
3. 必须配置AMP私有云/虚拟私有云设备和所有必要的证书。请参阅VPC证书指南进行验证。

<https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/214326-how-to-generate-and-add-certificates-tha.html>

4. 产品的所有主机名都必须是DNS可解析的。这是为了避免在集成期间出现任何连接问题或证书问

题。在安全终端私有云上，Eth0接口用于管理员访问，并且Eth1必须能够与集成设备连接。

步骤

配置安全终端私有云

1. 登录到Secure Endpoint VPC admin portal。
2. 转至“Configuration” > “Services” > “Disposition Server” > Copy the disposition server hostname (也可以从第三步获取)。
3. 导航到“Integrations” > “Web Security Appliance”。
4. 立即下载“Disposition Server Public Key” & “Appliance Certificate Root”
5. 导航到“Integrations” > “Email Security Appliance”。
6. 选择ESA版本并下载“Disposition Server Public Key”和“Appliance Certificate Root”。
7. 请保证证书和密钥均安全。稍后必须将此邮件上传到SWA/安全邮件。

The screenshot shows the 'Secure Endpoint Private Cloud Administration Portal' interface. The main heading is 'Connect Cisco Web Security Appliance to Secure Endpoint Appliance'. It details two steps:

Step 1: Web Security Appliance Setup

1. Go to the Web Security Appliance Portal.
2. Navigate to `Security Services > Anti-Malware and Reputation > Edit Global Settings...`
3. Enable the checkbox for `Enable File Reputation Filtering`.
4. Click `Advanced > Advanced Settings for File Reputation` and select `Private Cloud` under `File Reputation Server`.
5. In the `Server` field paste the `Disposition Server hostname: disposition.vpc1.nanganath.local`.
6. Upload your `Disposition Server Public Key` found below and select the `Upload Files` button.

Below the instructions, there is a download button for the **Disposition Server Public Key**.

Step 2: Proxy Setting

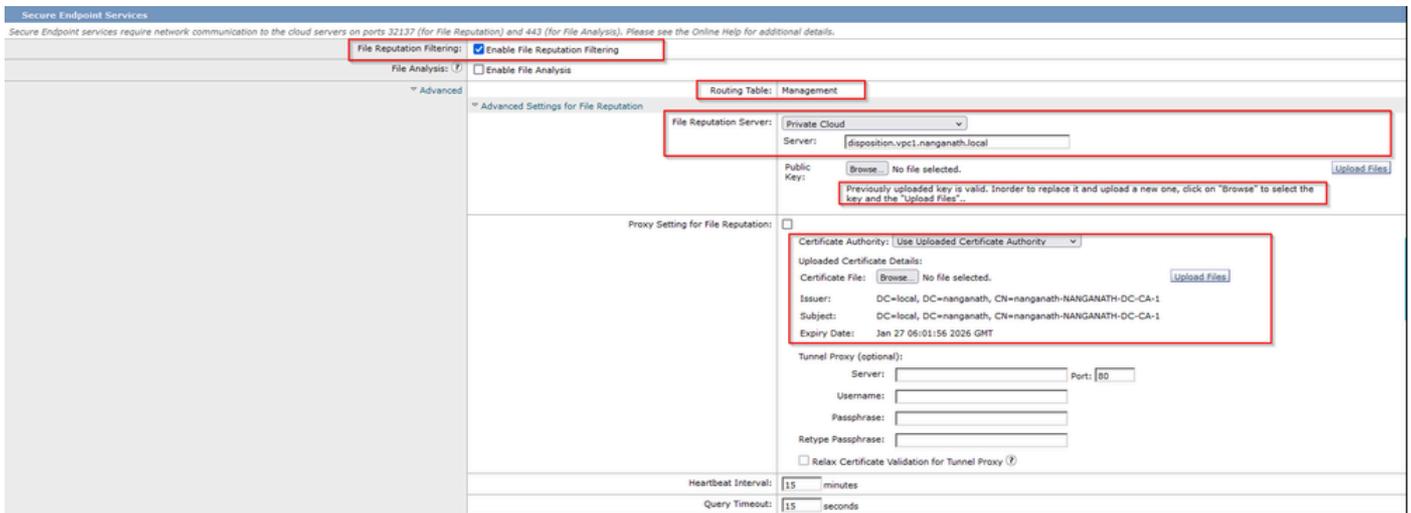
1. Continuing from Step 1 above, find the `Proxy Setting for File Reputation` section.
2. Choose `Use Uploaded Certificate Authority` from the `Certificate Authority` drop down.
3. Upload your `Appliance Certificate Root` found below and select the `Upload Files` button.
4. Click the `Submit` button to save all changes.

Below the instructions, there is a download button for the **Appliance Certificate Root**.

配置安全网络设备

1. 导航至 SWA GUI > “Security Services” > “Anti-Malware and Reputation” > Edit Global Settings
2. 在“Secure Endpoint Services”部分，您可以看到选项“Enable File Reputation Filtering”，并且“Check”此选项显示新字段“Advanced”
3. 在文件信誉服务器中选择“私有云”。
4. 将私有云安全状态服务器主机名提供为“Server”。
5. 上传您之前下载的公钥。点击“上传文件”(Upload Files)。

6. 可以选择上传证书颁发机构。从下拉菜单中选择“使用上传的证书颁发机构”(Use Uploaded Certificate Authority)并上传您之前下载的CA证书。
7. 提交更改
8. 提交更改

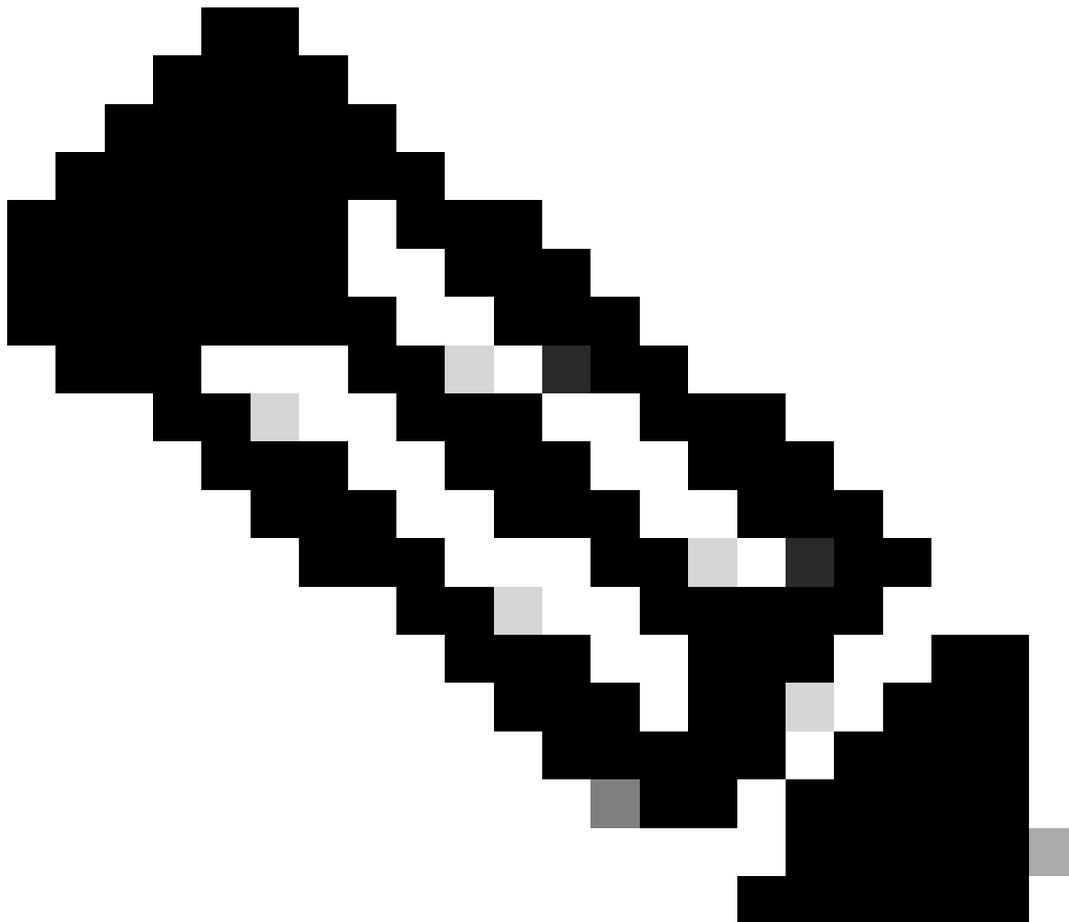


配置思科安全邮件

1. 导航至 Secure Email GUI > Security Services” > “File Reputation and Analysis” > Edit Global Settings > “Enable” or “Edit Global Settings”
2. 在文件信誉服务器中选择“私有云”
3. 将私有云安全评估服务器的主机名提供为“服务器”。
4. 上传我们之前下载的公钥。点击“上传文件”(Upload Files)。
5. 上传证书颁发机构。从下拉菜单中选择“使用上传的证书颁发机构”(Use Uploaded Certificate Authority)并上传您之前下载的CA证书。
6. 提交更改
7. 确认更改

Edit File Reputation and Analysis Settings

Advanced Malware Protection	
<i>Advanced Malware Protection services require network communication to the cloud servers on ports 443 (for File Reputation and File Analysis). Please see the Online Help for additional details.</i>	
File Reputation Filtering:	<input checked="" type="checkbox"/> Enable File Reputation
File Analysis: (?)	<input type="checkbox"/> Enable File Analysis
▼ Advanced Settings for File Reputation	File Reputation Server: Private reputation cloud Server: disposition.vpc1.nanganath.local Public Key: <input type="button" value="Browse..."/> No file selected. <input type="button" value="Upload File"/> <i>A valid public key has already been uploaded. To upload a new one, click on "Browse" to select the key and then the "Upload File".</i>
	SSL Communication for File Reputation: Use SSL (Port 443) Tunnel Proxy (Optional): Server: <input type="text"/> Port: <input type="text"/> Username: <input type="text"/> Passphrase: <input type="text"/> Retype Passphrase: <input type="text"/> <input type="checkbox"/> Relax Certificate Validation for Tunnel Proxy (?)
	Heartbeat Interval: <input type="text" value="15"/> minutes
	Query Timeout: <input type="text" value="20"/> seconds
	Processing Timeout: <input type="text" value="120"/> seconds
	File Reputation Client ID: cb1b31fc-9277-4008-a396-6cd486ecc621
	File Retrospective: <input type="checkbox"/> Suppress the verdict update alerts (?)
▸ Cache Settings	<i>Advanced settings for Cache</i>
▸ Threshold Settings	<i>Advanced Settings for File Analysis Threshold Score</i>



注意：思科安全网络设备和思科安全邮件网关基于AsyncOS，并且在初始化文件信誉时共享几乎相同的日志。可以在安全网络设备或安全邮件网关AMP日志中观察AMP日志（两台设备中的类似日志）。这仅表示服务已在SWA和安全邮件网关上初始化。它并不表示连接完全成功。如果存在任何连接或证书问题，则在“File Reputation initialized”（文件信誉已初始化）消息后您会看到错误。大多数情况下，它表示“Unreachable error”或“certificate Invalid”错误。

从安全网络和邮件获取AMP日志的步骤

1. 登录到SWA/安全邮件网关CLI并键入命令 "grep"
2. 选择 "amp" or "amp_logs"
3. 保留所有其他字段原样，然后键入“Y”以跟踪日志。跟踪日志以显示实时事件。如果您正在查找旧事件，则可以在“正则表达式”中键入日期

```
Tue Feb 20 18:17:53 2024 Info: connecting to /tmp/reporting_listener.sock.root [try #0 of 20]
Tue Feb 20 18:17:53 2024 Info: connected to /tmp/reporting_listener.sock.root [try #0 of 20]
Tue Feb 20 18:17:53 2024 Info: File reputation service initialized successfully
Tue Feb 20 18:17:53 2024 Info: The following file type(s) can be sent for file analysis: Executables, Document,
Microsoft Documents, Database, Miscellaneous, Encoded and Encrypted, Configuration, Email, Archived and compressed.
To allow analysis of new file type(s), go to Security Services > File Reputation and Analysis.
```

测试安全网络设备和安全终端私有云之间的集成。

没有直接选项可用于从SWA测试连接。您必须检查日志或警报，以验证是否存在任何问题。

为简单起见，我们测试的是HTTP URL而不是HTTPS。请注意，您需要对HTTPS流量进行解密，以进行任何文件信誉检查。

配置在SWA访问策略中完成，并强制执行AMP扫描。

注意：请查看SWA[用户指南](#)，了解如何在Cisco Secure Web设备上配置策略。

Access Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	AP.Users Identification Profile: ID.Users All identified users	(global policy)	(global policy)	Monitor: 342	(global policy)	Web Reputation: Enabled Secure Endpoint: Enabled Anti-Malware Scanning: Disabled	(global policy)		

Access Policies: Anti-Malware and Reputation Settings: AP.Users

Web Reputation and Anti-Malware Settings

Define Web Reputation and Anti-Malware Custom Settings

Web Reputation Settings

Web Reputation Filters will automatically block transactions with a low Web Reputation score. For transactions with a higher Web Reputation score, scanning will be performed using the services selected by Adaptive Scanning.

If Web Reputation Filtering is disabled in this policy, transactions will not be automatically blocked based on low Web Reputation Score. Blocking of sites that contain malware or other high-risk content is controlled by the settings below.

Enable Web Reputation Filtering

Secure Endpoint Settings

Enable File Reputation Filtering and File Analysis

File Reputation Filters will identify transactions containing known malicious or high-risk files. Files that are unknown may be forwarded to the cloud for File Analysis.

File Reputation	Monitor	Block
<input checked="" type="checkbox"/> Known Malicious and High-Risk Files	<input type="checkbox"/>	<input checked="" type="checkbox"/>

试图通过思科安全网络设备从互联网下载恶意文件“Bombermania.exe.zip”。日志显示恶意文件已被阻止。

SWA访问日志

可以通过以下步骤获取访问日志。

1. 登录SWA并键入命令 "grep"
2. 选择 "accesslogs"
3. 如果要添加任何“正则表达式”，如客户端IP，请予以说明。
4. 键入“Y”跟踪日志

```
1708320236.640 61255 10.106.37.205 TCP_DENIED/403 2555785 GET
http://static1.1.sqspcdn.com/static/f/830757/21908425/1360688016967/Bombermania.exe.zip?token=gsF
- DEFAULT_PARENT/bg11-lab-wsa-2.cisco.com application/zip BLOCK_AMP_RESP_12-
AP.Users-ID.Users-NONE-NONE-NONE-DefaultGroup-NONE <"IW_comp", 3.7,1, "-", -, -, -,
-, -, -, -, 1"-", "-", "-", -, -, "IW_comp", -, "AMP高风险", "计算机和互联网", "-", "未知
", "未知", "-", "-", 333.79,0, "-", "-
", 37, "Win.Ransomware.Protected : : Trojan.Agent.talos", 0,0, "Bombermania.exe.zip", "46ee42fb7
3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8", 3, -, "-", -, -> -
```

TCP_DENIED/403 —> SWA拒绝此HTTP GET请求。

BLOCK_AMP_RESP —>由于AMP响应，HTTP GET请求被阻止。

Win.Ransomware.Protected : : Trojan.Agent.talos —>威胁名称

Bombermania.exe.zip —>我们尝试下载的文件名

46ee42fb79a161bf3763e8e34a047018bd16d8572f8d31c2cdecae3d2e7a57a8 —>文件的SHA值

7 DISP_UNSEEN文件性质未知，这是我们第一次看到该文件。

13 DISP_BLOCK文件不能执行。

14 DISP_IGNORE XXX

15 DISP_CLEAN_PARENT认为该文件是良性的，因此它创建的任何恶意文件都必须被视为未知文件。

16 DISP_CLEAN_NFM认为文件是良性的，但客户端必须监控其网络流量。

测试安全邮件和AMP私有云之间的集成

没有直接选项可用于测试来自安全邮件网关的连接。您必须检查日志或警报，以验证是否存在任何问题。

在安全邮件传入邮件策略中完成配置以实施AMP扫描。

Incoming Mail Policies

Find Policies									
Email Address:				<input checked="" type="radio"/> Recipient <input type="radio"/> Sender		Find Policies			
Policies									
Add Policy...									
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	amp-testing-policy	Disabled	Disabled	File Reputation Malware File: Drop Pending Analysis: Deliver Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	(use default)	(use default)	(use default)	(use default)	

Mail Policies: Advanced Malware Protection

Advanced Malware Protection Settings	
Policy:	amp-testing-policy
Enable Advanced Malware Protection for This Policy:	<input checked="" type="radio"/> Enable File Reputation <input checked="" type="checkbox"/> Enable File Analysis <input type="radio"/> Use Default Settings (AMP and File Analysis Enabled) <input type="radio"/> No
Message Scanning	
	<input checked="" type="checkbox"/> (recommended) Include an X-header with the AMP results in messages
Unscannable Actions on Message Errors	
Action Applied to Message:	Deliver As Is
Advanced	Optional settings for custom header and message delivery.
Unscannable Actions on Rate Limit	
Action Applied to Message:	Deliver As Is
Advanced	Optional settings for custom header and message delivery.
Unscannable Actions on AMP Service Not Available	
Action Applied to Message:	Deliver As Is
Advanced	Optional settings for custom header and message delivery.
Messages with Malware Attachments:	
Action Applied to Message:	Drop Message
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Drop Malware Attachments:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING: MALWARE DETECTED]
Advanced	Optional settings.
Messages with File Analysis Pending:	
Action Applied to Message:	Deliver As Is
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Drop Message Attachments with File Analysis Verdict Pending : (?)	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING: ATTACHMENT(S) MAY CONTAIN
Advanced	Optional settings.

已使用非恶意文件测试ESA。这是CSV文件。

Secure Email mail_logs

```

Tue Feb 20 11:55:58 2024 Info: New SMTP ICID 43855 interface Management (10.106.39.193) address 10.110.172.122 reverse dns host unknown verified no
Tue Feb 20 11:55:58 2024 Info: ICID 43855 ACCEPT 5G UNKNOWNLIST match sbrs[none] SBRS rfc1918 country not applicable
Tue Feb 20 11:55:58 2024 Info: Start MID 660 ICID 43855
Tue Feb 20 11:55:58 2024 Info: MID 660 ICID 43855 From: <ajayra@gmail.com>
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: CSC0-W-PF253NKG, env-from: gmail.com, header-from: Not Present, reply-to: Not Present
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain: gmail.com
Tue Feb 20 11:55:58 2024 Info: MID 660 ICID 43855 RID 0 To: <ajayra@cisisco.com>
Tue Feb 20 11:55:58 2024 Info: MID 660 Subject: testing amp private cloud
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo: CSC0-W-PF253NKG, env-from: gmail.com, header-from: gmail.com, reply-to: Not Present
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain: gmail.com
Tue Feb 20 11:55:58 2024 Info: MID 660 SDR: Tracker Header : 65d445f6_TdY46k/XzoIL66+HhA4cFJo0192j3QSDhLDnEkX9DPClxVhx3o3lC136to+TzXqIaVVP6hX+cND+5IQ=
Tue Feb 20 11:55:58 2024 Info: MID 660 ready 5467 bytes from <ajayra@gmail.com>
Tue Feb 20 11:55:58 2024 Info: MID 660 attachment: Training Details.csv
Tue Feb 20 11:55:58 2024 Info: MID 660 matches all recipients for per-recipient policy amp-testing-policy in the inbound table
Tue Feb 20 11:56:59 2024 Warning: graymail [RPC CLIENT] MID 660 Graymail scan timed out
Tue Feb 20 11:57:01 2024 Info: MID 660 AMP file reputation verdict : UNKNOWN (File analysis pending)
Tue Feb 20 11:57:01 2024 Info: MID 660 SHA-90381C261f80e3e9330710ab96647358c461f6834c0ca001408e40decdf19dbe filename Training Details.csv queued for possible file analysis upload
Tue Feb 20 11:57:01 2024 Info: MID 660 Outbreak Filters: verdict negative none
Tue Feb 20 11:57:01 2024 Info: MID 660 Message-ID : <99221a1xwexs1.nanganath.local>
Tue Feb 20 11:57:01 2024 Info: MID 660 queued for delivery
Tue Feb 20 11:57:01 2024 Info: New SMTP ICID 542 interface 10.106.39.193 address 173.37.147.230 port 25
Tue Feb 20 11:57:02 2024 Info: Delivery start DCID 542 MID 660 to RID [0]
Tue Feb 20 11:57:04 2024 Info: Message done DCID 542 MID 660 to RID [0]
Tue Feb 20 11:57:04 2024 Info: MID 660 RID [0] Response: ok: Message 142767851 accepted
Tue Feb 20 11:57:04 2024 Info: Message finished MID 660 done
Tue Feb 20 11:57:09 2024 Info: DCID 542 close
Tue Feb 20 11:57:23 2024 Info: ICID 43855 lost
Tue Feb 20 11:57:23 2024 Info: ICID 43855 close
    
```

安全邮件AMP日志

2024年2月20日星期二11:57:01 2024信息：从云端接收的文件信誉查询响应。文件名=培训详细信息.csv，MID = 660，性质=文件未知，恶意软件=无，分析分数= 0，sha256 = 90381c261f8be3e933071dab96647358c461f6834c8ca0014d8e40dec4f19dbe，upload_action =建议发送文件进行分析， verdict_source = AMP，suspected_categories = None

安全终端私有云事件日志

```
{"pv": 3, "ip": "10.106.72.238", "si": 0, "ti": 14, "tv": 6, "qt": 42, "pr": 1, "ets": 1708410419, "t": "9277-4008-a396-6cd486ecc621", "ai": 1, "aptus": 295, "ptus": 2429102, "spero": {"h": "00", "fa": 0, "fs": 0, "ft": 0, "hd": 1}, "sha256": {"h": "90381c261f8be3e933071dab96647358c461f6834c8ca0014d8e40dec4f19dbe", "fa": 0, "fs": 0, "ft": 0, "hd": 1}, "hord": [32,4], "rd": 1, "ra": 1, "n": 0}
```

rd - 1 DISP_UNKNOWN。文件性质未知。

已观察到的导致集成失败的常见问题

1. 在SWA或安全邮件中选择错误的“路由表”。集成设备必须能够与AMP私有云Eth1接口通信。
2. VPC主机名在SWA或安全邮件中无法进行DNS解析，从而导致连接建立失败。
3. VPC处置证书中的CN（通用名称）必须与VPC主机名以及SWA和安全邮件网关中提到的主机名匹配。
4. 不支持使用私有云和云文件分析。如果使用的是内部设备，则文件分析和信誉必须是内部服务器。
5. 确保AMP私有云与SWA、安全邮件之间不存在时间同步问题。
6. SWA DVS引擎对象扫描限制默认为32 MB。如果要扫描较大的文件，请调整此设置。请注意，它是一个全局设置，会影响所有扫描引擎，如Webroot、Sophos等。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。