对安全网络设备中的AMP进行故障排除

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

排除SWA AMP日志故障

详细字段与值选项

相关内容

简介

本文档介绍安全Web设备的高级恶意软件防护引擎的信息和调试日志级别中的ampverdict部分。

先决条件

要求

Cisco 建议您了解以下主题：

- AMP已启用
- 对SWA的SSH访问
- SWA安装和许可
- 已启用文件信誉和文件分析

使用的组件

本文档不限于特定的软件和硬件版本。

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。

背景信息

SWA提供与面向终端的AMP和本地AMP引擎的集成。AMP通过文件信誉和文件分析功能提供针对零日恶意软件的恶意软件防护。SWA包括一个预分类引擎，用于在公共云检查之前进行内部文件扫描。下一部分中描述的日志与SWA上的AMP引擎相关，而不是AMP云或Threat Grid。

排除SWA AMP日志故障

访问AMP日志。通过CLI登录并跟踪或更新amp日志：

1.通过SSH客户端登录CLI。

2.运行grep命令，然后按Enter。

3.输入列出的amp_logs的编号。

4.回答提示。如果您运行实时流量，请选择跟踪日志选项。
5.按Enter键。

6.显示日志。

SWA AMP日志提供不同级别的详细信息。可以选择INFO或DEBUG级别。结果略有差异，将在下一节进行说明

注意：AMP许可证必须安装在SWA上才能选择AMP日志。

AMP信息级别日志：

```
Wed Apr 27 12:21:26 2022 Info: Txn 18210 Binary scan on instance[0] Id[1345]: AMP allocated memory = 0,
Wed Apr 27 12:21:35 2022 Info: Binary scan on instance[0] id[1345]: filename[npp.8.4.Installer.x64.exe]
Wed Apr 27 12:22:28 2022 Info: File uploaded for analysis. Server: https://panacea.threatgrid.com, SHA2
```

AMP信息级别日志(ampverdict):

```
ampverdict[(1, 1, 'amp', '', 0, 0, True)]
(analysis_Action, scan_verdict, 'verdict_source', 'spyname', malware_verdict, file_reputation, upload_a
```

AMP调试级别日志：

```
Fri Apr 29 01:38:40 2022 Debug: Binary scan: proxid[3951] filename[favicon.ico] len[41566b] readtime[10
```

AMP调试级别日志(ampverdict):

```
ampverdict[(1, 1, 'amp', '', 0, 0, False)]
ampverdict[(analysis_action, scan_verdict,disposition, ‘spyname: policy name if amp registered with con
```

详细字段与值选项

字段	价值
Analysis_action	"0":表示高级恶意软件保护未请求上传文件进行分析。 "1":表示高级恶意软件防护已请求上传文件进行分析。
Scan_verdict	"0":该文件不是恶意。 "1":由于文件类型，未扫描该文件。 "2":文件扫描超时。 "3":扫描错误。 大于 3:文件是恶意的。
Verdict_source	amp:文件分析.
处置	"1":未知。 "2":干净。 "3":恶意(amp)。 "4":不可扫描（不可扫描）。
Spyname	空:如果未使用AMP爆发策略。 Simple_Custom_Detection:如果使用AMP爆发策略。
Upload_action	正确:文件设置为沙盒。 错误:文件不会发送到沙盒。
Sha256	SHA256。
Threat_name	基于AMP威胁类型的威胁名称。

相关内容

- 将面向终端的AMP和Threat Grid与SWA集成
- 文件信誉过滤和文件分析

- 技术支持和文档系统

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）。