對安全Web裝置和高級惡意軟體防護日誌(ampverdict)進行故障排除

目錄

簡介

本檔案介紹網路安全裝置(WSA)進階惡意軟體防護(AMP)引擎的**資訊**和**DEBUG**日誌層級中的ampverdict一節。

必要條件

需求

思科建議您瞭解以下主題：

- 已安裝WSA
- 已啟用檔案信譽和檔案分析
- 高級惡意軟體防護
- 思科安全網路裝置
- SSH客戶端

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

WSA提供與面向終端的AMP和本地AMP引擎的整合。AMP通過檔案信譽和檔案分析功能提供針對零日惡意軟體的惡意軟體防護。WSA包括一個預分類引擎，該引擎負責在公共雲檢查之前進行內部檔案掃描。下一部分中描述的日誌與WSA上的AMP引擎相關，而與AMP雲或Threat Grid無關。

排除WSA AMP日誌故障

訪問AMP日誌。通過CLI登入並跟蹤或登入amp日誌：

1.通過SSH客戶**端**登入到CLI。

2.鍵入命令**grep**，然後按**Enter**鍵。

3.輸入**amp_logs** 的訂購編號。

4.回答以下選項(如果運行即時流量，則選擇**尾隨**日誌的選項)。
5.按**Enter**鍵。

6.顯示日誌。

如果AMP日誌存在於不同級別的資訊中，則可以選擇**INFO**級別或**DEBUG**結果，這些結果在下一部分中會有細微差異。

附註：需要在WSA上安裝AMP許可證以選擇AMP日誌。

AMP資訊級別日誌：

```
Wed Apr 27 12:21:26 2022 Info: Txn 18210 Binary scan on instance[0] Id[1345]: AMP allocated
memory = 0, AMP used memory = 0, Scans in flight = 1, Active faster connections = 1, Active
slower connections = 0
Wed Apr 27 12:21:35 2022 Info: Binary scan on instance[0] id[1345]:
filename[npp.8.4.Installer.x64.exe] filemime[application/x-dosexec] file_extension[exe]
length[4493047b] ampverdict[(1, 1, 'amp', '', 0, 0, True)] scanverdict[0] malwareverdict[0]
spyname[] SHA256[ecdcf497418a1988ebf20c647acadc9eca7bc8569fd980713582acd0de011ba1] From[Cloud]
uploadreason[Enqueued in the local queue for submission to upload] verdict_str[FILE UNKNOWN]
is_slow[0] scans_in_flight[0] Active faster connections[0] Active slower connections[0]
Wed Apr 27 12:22:28 2022 Info: File uploaded for analysis. Server:
https://panacea.threatgrid.com, SHA256:
ecdcf497418a1988ebf20c647acadc9eca7bc8569fd980713582acd0de011ba1, Filename:
npp.8.4.Installer.x64.exeTimestamp: 1651044116 sampleid[]
```

AMP資訊級別日誌(AMPVERDICT):

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

AMP調試級別日誌：

```
Fri Apr 29 01:38:40 2022 Debug: Binary scan: proxid[3951] filename[favicon.ico] len[41566b]
readtime[109.721680ms] scantime[2.205322ms] ampverdict[(1, 1, 'amp', '', 0, 0, False)]
scanverdict[0] malwareverdict[0]
SHA256[e7a2345c75a03e63202b12301c29bb8b6bae7cef9e191ed58797ec028def7c4f] From[Cloud]
FileName[favicon.ico] FileMime[application/octet-stream]
```

AMP調試級別日誌(ampverdict):

```
ampverdict[(1, 1, 'amp', '', 0, 0, False)]
ampverdict[(analysis_action, scan_verdict,disposition, ‘spyname: policy name if amp registered
with console’, file_reputation, upload_action, ‘sha256', ‘threat_name’)]
```

詳細欄位與值選項：

欄位	價值
Analysis_action	「0」表示高級惡意軟體防護未請求上傳檔案進行分析 「1」表示高級惡意軟體防護已請求上傳檔案進行分析
Scan_verdict	0:該檔案不是惡意的 1:由於檔案型別，未掃描該檔案 2:檔案掃描超時 3:掃描錯誤 大於3:檔案是惡意的
Verdict_source	amp:檔案分析
處置	1:未知 2:清除 3:惡意(amp) 4:不可掃描（不可掃描）
Spyname	空：如果未使用AMP爆發策略 Simple_Custom_Detection:如果使用AMP爆發策略
Upload_action	真：檔案設定為沙盒 錯誤：檔案未傳送到沙盒
Sha256	SHA256
威脅名稱	基於AMP威脅型別的威脅名稱

相關資訊

- 將面向終端的AMP和Threat Grid與WSA整合
- 檔案信譽過濾和檔案分析
- 技術支援與檔案 — Cisco 系統