Troubleshoot Secure Web Appliance and Advanced Malware Protection Logs (ampverdict)

Contents

Introduction

This document describes the ampverdict section in the **INFO** and **DEBUG** log level of the Advanced Malware Protection (AMP) engine of the Web Security Appliance (WSA).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- WSA Installed
- File Reputation and File Analysis enabled
- Advanced Malware Protection
- Cisco Secure Web Appliance
- SSH client

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

WSA offers integration with AMP for Endpoints and a local AMP engine. AMP provides Malware protection against zero-day malware through File reputation and File analysis features. The WSA includes a pre-classification engine that is responsible for file scans internally before public cloud checks. The logs described in the next section are related to the AMP engine on WSA not to the AMP cloud or Threat Grid.

Troubleshoot WSA AMP Logs

Access the AMP logs. Log in via CLI and tail or grep the amp logs:

1. Log in to the **CLI** through SSH Client.

2. Type the command **grep** and press **Enter** key.

3. Enter the number of the **amp_logs** as it is ordered.

4. Answer the followed options (If you run live traffic chose the option to **tail** the logs).
5. Press **Enter** key.

6. Logs are displayed.

WSA AMP logs exist in different levels of information, you can select the **INFO** level or **DEBUG** the results that have slight differences explained in the next section.

Note: AMP license needs to be installed on WSA to select the AMP logs.

AMP INFO level logs:

```
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 INFO level logs (ampverdict):

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

AMP DEBUG level logs:

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

AMP DEBUG level logs (ampverdict):

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

Detailed Field vs Value options:

Field	**Value**

Analysis_action	"0" indicates that Advanced Malware Protection did not request the upload of the file for analysis "1" indicates that Advanced Malware Protection did request the upload of the file for analysis
Scan_verdict	0: The file is not malicious 1: The file was not scanned because of its file type 2: File scan timed out 3: Scan error Greater than 3: File is malicious
Verdict_source	amp: file analysis
Disposition	1: Unknown 2: Clean 3: Malicious (amp) 4: Unscannable (unscannable)
Spyname	Empty: if the AMP outbreak policy is not used Simple_Custom_Detection: if an AMP outbreak policy is used
Upload_action	True: file is set to sandbox False: file is not sent to the sandbox
Sha256	SHA256
Threat_name	Threat name based on AMP threat types

Related Information

- **Integrate AMP for Endpoints and Threat Grid with WSA**
- **File Reputation Filtering and File Analysis**
- **Technical Support & Documentation - Cisco Systems**