Troubleshoot AMP in Secure Web Appliance

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Troubleshoot SWA AMP Logs

Detailed Field vs Value options

Related Content

Introduction

This document describes the ampverdict section in the **INFO** and **DEBUG** log level of the Advanced Malware Protection engine of the Secure Web Appliance.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- AMP is Enabled
- SSH Access to SWA
- SWA Installed and Licensed
- File Reputation and File Analysis Enabled

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

SWA offers integration with AMP for endpoints and a local AMP engine. AMP provides malware protection against zero-day malware through the File Reputation and File Analysis features. The SWA 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 SWA, not to the AMP cloud or Threat Grid.

Troubleshoot SWA AMP Logs

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

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

2. Run the **grep** command, then press **Enter**.

3. Enter the number for **amp_logs** as listed.

4. Answer the prompts. If you are running live traffic, choose the option to **tail** the logs.
5. Press the **Enter** key.

6. The logs are displayed.

The SWA AMP logs are available at different levels of detail. You can select the **INFO** or **DEBUG** level. The results have slight differences, which are explained in the next section

---

Note: The AMP license must be installed on SWA 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 the Advanced Malware Protection **did not** request the upload of the file for analysis. "**1**": Indicates the 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 of the file.
Threat_name	Threat name based on AMP threat types.

Related Content

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