Troubleshoot Secure Endpoint Linux Connector Fault 18

Contents

Introduction

This document describes Fault 18 on the Secure Endpoint Linux connector.

Fault 18: Connector Event Monitoring is Overloaded

The Behavioral Protection engine improves the connectors visibility into system activity. With this increase in visibility there is an increased possibility that the connectorâ€™s system activity monitoring can be overwhelmed by the amount of activity on the system. If this happens, the connector raises fault 18 and enters degraded mode. Refer to the Cisco Secure Endpoint Linux Connector Faults article for details on fault 18. On the Linux Connector, the status command can be used in the Secure Endpoint Linux CLI to see if the connector is running in degraded mode and if any faults are raised. If fault 18 is raised, then running the status command in the Secure Endpoint Linux CLI displays the fault with one of the possible two severities:

1. Fault 18 with major severity

```
ampcli> status
Status:                  Connected
Mode:                    Degraded
Scan:                    Ready for scan
Last Scan:               2023-06-19 02:02:03 PM
Policy:                  Audit Policy for FireAMP Linux (#1)
Command-line:            Enabled
Orbital:                 Disabled
Behavioural Protection: Protect
Faults:                  1 Major
Fault IDs:      18
                ID 18 - Major: Connector event monitoring is overloaded. Investigate the most acti
```

2. Fault 18 with critical severity

```
ampcli> status
```

```
Status:                 Connected
Mode:                   Degraded
Scan:                   Ready for scan
Last Scan:              2023-06-19 02:02:03 PM
Policy:                 Audit Policy for FireAMP Linux (#1)
Command-line:           Enabled
Orbital:                Disabled
Behavioural Protection: Protect
Faults:                 1 Critical
Fault IDs:      18
                ID 18 - Critical: Connector event monitoring is overloaded. Investigate the most a
```

Connector Event Monitoring is Overloaded: Major Severity

When fault 18 is raised with major severity, this means that the connector event monitoring is overloaded but still able to monitor a smaller set of system events. The connector switches into major severity and monitors less events equivalent to the monitoring that was available in connectors older than 1.22.0. If the flood of system events is short and the event monitoring load decreases back into an acceptable range, then fault 18 is cleared and the connector resumes monitoring all system events. If the flood of system events gets worse and the event monitoring load increases to a critical amount, then fault 18 is raised with critical severity and the connector switches into critical severity.

Connector Event Monitoring is Overloaded: Critical Severity

When fault 18 is raised with critical severity, this means that the connector is experiencing an overwhelming amount of system events that puts the connector at risk. The connector switches into a more restrictive critical severity. In this state, the connector only monitors critical events to allow the connector to cleanup and focus on recovery. If the flood of events eventually decreases back into a more acceptable range then the fault is cleared entirely and the connector resumes monitoring all system events.

Fault Action Guidance

If the connector ever raises fault 18 with either major or critical severity then some steps must be taken to investigate and resolve the issue. The steps to resolve fault 18 vary depending on when and why the fault was raised:

1. Fault 18 was raised on a fresh installation of the Linux connector
2. Fault 18 was raised after recent changes to the operating system
3. Fault 18 was raised spontaneously

4. Fault 18 was raised upon re-provisioning a machine with the Linux connector already installed or updating the connector to version 1.22.0+

Case 1: Fresh Installation

If fault 18 and degraded mode are observed off of a fresh installation of the Linux connector then you must first ensure your system meets the minimum system requirements. After verifying that the requirements meet or exceed minimum requirements, if the fault persists, you must investigate the most active processes on the system. You can view the current active processes on a Linux system using the `top` command (or similar) in the terminal. If the processes consuming the highest amount of CPU are known to be benign, then you can create new process exclusions to exclude those processes from being monitored.

Example Scenario:

Suppose after fresh installation, fault 18 and degraded mode were displayed via the Secure Endpoint Linux CLI. Running the top command in a Ubuntu machine displayed these active processes:

```
Tasks: 223 total,   5 running, 218 sleeping,   0 stopped,   0 zombie
%Cpu(s): 29.4 us, 34.3 sy,  0.0 ni, 36.2 id,  0.0 wa,  0.0 hi,  0.1 si,  0.0 st
MiB Mem :   7943.0 total,   3273.9 free,   2357.6 used,   2311.5 buff/cache
MiB Swap:   2048.0 total,   2048.0 free,      0.0 used.   5141.2 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  34896 user1     20   0   18136   3292   3044 R  96.7   0.0   0:04.89 trusted_process
   4296 user1     20   0  823768  52020  38900 R  48.0   0.6   0:10.90 gnome-terminal-
    117 root      20   0       0      0      0 I  12.3   0.0   0:01.86 kworker/u64:6-events_unbound
  34827 root      20   0       0      0      0 I  10.3   0.0   0:00.47 kworker/u64:2-events_unbound
   1880 user1     20   0  353080 101600  70164 S   6.3   1.2   0:30.37 Xorg
  34576 root      20   0       0      0      0 R   6.3   0.0   0:01.46 kworker/u64:1-events_unbound
   2089 user1     20   0 3939120 251332 104008 S   3.0   3.1   0:23.25 gnome-shell
    132 root      20   0       0      0      0 I   1.3   0.0   0:02.67 kworker/2:2-events
   6951 root      20   0 1681560 213536  74588 S   1.3   2.6   0:41.30 ampdaemon
    741 root      20   0  253648  13352   9280 S   0.3   0.2   0:01.54 polkitd
    969 root      20   0  153600   3788   3512 S   0.3   0.0   0:00.36 prlshprint
   2291 user1     20   0  453636  29388  20060 S   0.3   0.4   0:03.75 prlcc
      1 root      20   0  169608  13116   8524 S   0.0   0.2   0:01.95 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 slub_flushwq
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
      8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
```

We see that there is a very active process, called trusted_process in this example. In this case I am familiar with this process and it is trusted, there is no reason for me to be suspicious of this process. To clear fault 18, the trusted process can be added to a process exclusion in the Portal. Refer to the Configure and Identify Cisco Secure Endpoint Exclusions article to learn about the best practices when creating exclusions.

Case 2: Recent Changes

If you have made recent changes to your operating system, such as installing a new program, then fault 18 and degraded mode can be observed if these new changes increase system activity. Use the same remediation strategy as outlined in the fresh installationcase, however look for processes that are related to the recent changes, such as a new process run by a freshly installed program.

Case 3: Malicious Activity

The Behavioral Protection engine increases the types of system activity that are monitored. This provides the connector with a wider perspective on the system and gives it the ability to detect more complex behavioral attacks. However, monitoring a larger amount of system activity also puts the connector at a greater risk for denial-of-service (DoS) attacks. If the connector is overwhelmed with system activity and enters degraded mode with fault 18, it still continues to monitor system critical events until overall system activity is reduced. This loss in system event visibility reduces the connectorâ€™s ability to protect your machine. It is critical that you investigate the system immediately for malicious processes. Use the top command (or similar) on your Linux system to view current active processes, and take appropriate action to remediate the situation if any possibly malicious processes are identified.

Case 4: Connector Requirements

The Behavioral Protection engine improves the ability of the connector to protect your machine activity, but to do so it must consume more resources than in prior versions. If fault 18 is raised frequently, there are no benign processes that are causing heavy load, and there doesnâ€™t appear to be any malicious processes acting on the machine, then you must ensure your system meets the minimum system requirements.

See Also

- Use the Secure Endpoint Mac/Linux CLI
- Cisco Secure Endpoint Linux Connector Faults
- Configure and Identify Cisco Secure Endpoint Exclusions
- Secure Endpoint User Guide (PDF)