Troubleshoot Secure Endpoint Linux Connector Faults

Contents

Introduction

This document describes faults that the Cisco Secure Endpoint Linux connector uses to notify you of conditions that affect its proper functioning.

Background Information

The Cisco Secure Endpoint Linux connector notifies with a Fault Raised event when it detects a condition that affects the proper functioning of the connector. Similarly, a Fault Cleared event communicates that the condition is no longer present.

Secure Endpoint Linux Connector Fault Table

The table describes faults and their associated diagnostic steps.

Fault ID	Description	Troubleshooting/Resolution
5	Scan service user unavailable	The connector failed to create a user to run the file scan process. The connector uses the root user to perform file scans as a workaround. This deviates from the intended design and is not expected. If the `cisco-amp-scan-svc` user or group has been deleted, or the configuration of the user and group has been changed, then you can reinstall the connector to re-create the user and group with the necessary configurations. Additional details are available in */var/log/cisco/ampdaemon.log*. If the user group creation is restricted via the settings in **/etc/login.defs** this file must be temporarily changed while the installer is running to allow the user and group to be created. To do this, change **usergroups_enab** from no to yes. This fault can be raised in Linux connectors 1.15.1 and newer if another program modified one of the connector's directory permissions (that is /opt/cisco or a child directory). To alleviate this, the changed directory permission must be set back to default (ie. 0755), ensure that no future programs modify the /opt/cisco directory (or any child directories), and restart the connector service.

6	Scan service restarting frequently	The connector file scan process encountered repeated failures and the connector has restarted in an attempt to clear the failure. It is possible one or more files on the system causes the scan algorithm to crash when scanned. The connector continues with scans on a best-effort basis. If this fault is not automatically cleared within 10 minutes after the connector is started then this is an indication that further user intervention is required and the ability of the connector to perform scans is degraded. Review */var/log/cisco/ampdaemon.log* and */var/log/cisco/ampscansvc.log* for details.
7	Scan service failed to start	The connector's file scan process failed to start and the connector has restarted in an attempt to clear the failure. File scan functionality is disabled while this fault is raised. This failure can be triggered if an error is encountered when loading a newly installed virus definition files (.cvd files). The connector performs a number of integrity and stability checks before it activates new .cvd files to prevent this failure. On restart ,the connector removes any invalid .cvd files so that the connector can resume. If this fault is not cleared when the connector is restarted then this is an indication that further user intervention is required. If this failure repeats with each .cvd update then this is an indication that an invalid .cvd file is not being properly detected by the .cvd file integrity checks of the connector. This failure can be triggered in Linux connectors if the machine is running low on available memory and the scanner service is unable to start. Consult the "Secure Endpoint (formerly AMP for Endpoints) User Guide" for the minimum system requirements on Linux. Review */var/log/cisco/ampdaemon.log* and */var/log/cisco/ampscansvc.log* for details.
8	Realtime filesystem monitor failed to start	The kernel module that provides realtime filesystem activity monitoring was not loaded and the connector policy has "Monitor File Copies and Moves" enabled. These monitoring functions are unavailable in the connector while this fault is raised. This fault is raised when the Secure Endpoint connector is unable to load the underlying kernel module required for filesystem activity monitoring. UEFI Secure Boot must be disabled on the system. If Secure Boot is disabled, this fault can be caused by an incompatibility between the ampavflt or ampfsm kernel module provided with the Secure Endpoint connector and the system kernel or other third-party kernel modules installed on the system. Review */var/log/messages* for details. The fault can also be caused when running a kernel version that is not supported by the connector. In this case it can be cleared by building a custom ampfsm kernel module for the current running system kernel. (Applicable to Linux connector versions 1.16.0 and newer.) For more information on building custom kernel modules please see: Building Cisco Secure Endpoint Linux Connector

		Kernel Modules
9	Realtime network monitor failed to start	The kernel module that provides realtime network activity monitoring was not loaded and the connector policy has "Enable Device Flow Correlation" enabled. This monitoring function is unavailable in the connector while this fault is raised. This fault is raised when the Secure Endpoint connector is unable to load the underlying kernel module required for filesystem activity monitoring. UEFI Secure Boot must be disabled on the system. If Secure Boot is disabled, this fault can be caused by an incompatibility between the ampavflt or ampfsm kernel module provided with the Secure Endpoint connector and the system kernel or other third-party kernel modules installed on the system. Review */var/log/messages* for details. The fault can also be caused when running a kernel version that is not supported by the connector. In this case it can be cleared by building a custom ampfsm kernel module for the current running system kernel. (Applicable to Linux connector versions 1.16.0 and newer.) For more information on building custom kernel modules please see: Building Cisco Secure Endpoint Linux Connector Kernel Modules
11	Required kernel-devel package is missing	The Secure Endpoint connector uses eBPF modules to monitor filesystem, process, and network activity. The connector requires certain packages to be available on the system to load and run these eBPF modules. To resolve this fault, install the package required by your Linux distribution as described below, and restart the connector. For Red Hat based distributions, this fault is raised when the kernel-devel package is missing. Install the kernel-devel package, and restart the connector. (Applicable only to Linux connector versions 1.13.0 and newer.) For Oracle Linux UEK 6 and newer, this fault is raised when the kernel-uek-develpackage is missing. Install the kernel-uek-devel package, and restart the connector. (Applicable only to Linux connector versions 1.18.0 and newer.) For Debian based distributions, this fault is raised when the linux-headers package is missing. Install the linux-headers package, and restart the connector. (Applicable to Linux connector versions 1.15.0 and newer.) For more information please see: Linux Kernel-Devel Fault
16	Incompatible kernel	The currently running kernel is not compatible with the currently running connector and the connector policy has either "Monitor File Copies and Moves" or "Enable Device Flow Correlation" enabled. Downgrade the kernel to a supported version or upgrade the connector to a newer version that supports this kernel. For details on supported kernel versions, see: Cisco Secure Endpoint Linux Connector OS Compatibility

18	Connector event monitoring is overloaded	This fault is raised when the connector is under heavy load due to an overwhelming number system events. System protection is limited and the connector monitors a smaller set of system critical events until overall system activity is reduced. This fault could be an indication of malicious system activity or of very active applications on the system. If an active application is benign and trusted by the user then it can be added to a process exclusion set to reduce the monitoring load on the connector. This action can be enough to clear the fault. If no benign processes cause heavy load, then some investigation is required to determine if the increased activity is due to a malicious process. If the connector is under short periods of heavy load then it is possible that this fault can clear itself. If this fault is raised frequently, there are no benign processes that cause heavy load, and no malicious processes were discovered, then the system needs to be re-provisioned to handle heavier loads.
19	SELinux Policy is missing or disabled	This fault is raised when the Secure Enterprise Linux (SELinux) Policy on the system is preventing the Connector from monitoring system activity. If SELinux is enabled and in enforcing mode, the Connector requires this rule in the SELinux Policy: `allow unconfined_service_t self:bpf { map_create map_read map_write prog_load prog_run };` On Red Hat based systems, including RHEL 7 and Oracle Linux 7, this rule is not present in the default SELinux Policy. During an installation or upgrade, the Connector attempts to add this rule through the installation of a SELinux Policy Module named `cisco-secure-bpf`. If `cisco-secure-bpf` fails to install and load, or is disabled, the fault is raised. To resolve the fault, ensure the system package policycoreutils-python is installed. Reinstall or upgrade the Connector to trigger the installation of `cisco-secure-bpf`, or manually add the rule to the existing SELinux Policy and restart the Connector. For more detailed instructions on modifying the SELinux Policy to resolve this fault, see SELinux Policy Fault.