Troubleshoot Secure Endpoint Linux Connector Faults

Contents

Introduction

Secure Endpoint Linux Connector Faults

- Fault 5: Scan Service User Unavailable
  - Condition
  - Resolution
- Fault 6: Scan Service Restarting Frequently
  - Condition
  - Resolution
- Fault 7: Scan Service Failed To Start
  - Condition
  - Resolution
- Fault 8: Realtime Filesystem Monitor Failed To Start
  - Condition
  - Resolution
- Fault 9: Realtime Network Monitor Failed To Start
  - Condition
  - Resolution
- Fault 11: Required Kernel-Devel Package Is Missing
  - Condition
  - Resolution
- Fault 16: Incompatible Kernel
  - Condition
  - Resolution
- Fault 18: Connector Event Monitoring Is Overloaded
  - Condition
  - Resolution
- Fault 19: SELinux Policy Is Missing Or Disabled
  - Condition
  - Resolution

Introduction

This document describes faults that the Linux connector raises/clears to notify when conditions affecting proper functioning are detected/resolved.

Secure Endpoint Linux Connector Faults

Fault 5: Scan Service User Unavailable

Condition

The connector failed to create the *cisco-amp-scan-svc* user to run the file scan process. As a workaround, the connector has fallen back to use the root user to perform file scans. This deviates from the intended design and must be corrected.

Resolution

1. If the *cisco-amp-scan-svc* user or group has been deleted or had its configurations modified, then reinstall the connector to re-create the user and group with the necessary configurations. Review */var/log/cisco/ampdaemon.log* for details.
2. If user/group creation is restricted via settings in */etc/login.defs*, then this file must be temporarily changed while the Linux connector installer is running to allow the *cisco-amp-scan-svc* user and group to be created. To do this, change `USERGROUPS_ENAB` in */etc/login.defs* from no to yes.
3. If another program modified one of the connector's directory permissions (for example */opt/cisco* or a child directory), set the directory permissions back to default (ie. 0755). Ensure that no future programs modify the */opt/cisco* directory or any of its child directories, then restart the connector service.

Fault 6: Scan Service Restarting Frequently

Condition

The connector file scan process encountered repeated failures and the connector has restarted in an attempt to clear the failure. The connector will continue to scan on a best-effort basis.

Resolution

One or more files on the system might be causing the scan algorithm to crash when scanned. If this fault is not automatically cleared within 10 minutes after the connector is restarted then further investigation is required. The ability of the connector to perform scans will be degraded until the issue is resolved.

Review */var/log/cisco/ampdaemon.log* and */var/log/cisco/ampscansvc.log* for details.

Fault 7: Scan Service Failed To Start

Condition

The connector file scan process failed to start and the connector has restarted in an attempt to clear the failure. File scanning is disabled while this fault is raised.

Resolution

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.

1. If this fault is not cleared after the connector is restarted then further user intervention is required. If this failure repeats with each *.cvd* update then an invalid *.cvd* file is not being properly detected by the *.cvd* file integrity checks of the connector.
2. If the machine is running low on available memory then the scanner service might be unable to start.

Consult the Linux System Requirements in the Secure Endpoint User Guide Secure Endpoint User Guide.

Review /var/log/cisco/ampdaemon.log and /var/log/cisco/ampscansvc.log for details.

Fault 8: Realtime Filesystem Monitor Failed To Start

Condition

The connector is unable to load the underlying kernel module required for filesystem activity monitoring when the connector policy has "Monitor File Copies and Moves" enabled. Filesystem monitoring is unavailable while this fault is raised.

Resolution

1. Disable UEFI Secure Boot on the system.
2. If Secure Boot is disabled, there might be an incompatibility between the `ampfsm` kernel module provided with the connector and the system kernel or other third-party kernel modules installed on the system. Review */var/log/messages* for details.
3. If the connector is running on an unsupported kernel version, then either install a supported kernel version or build a custom `ampfsm` kernel module for the current running system kernel. Review Building Cisco Secure Endpoint Linux Connector Kernel Modules for more information.

Fault 9: Realtime Network Monitor Failed To Start

Condition

The connector is unable to load the underlying kernel module required for network activity monitoring when the connector policy has "Enable Device Flow Correlation" enabled. Network monitoring is unavailable while this fault is raised.

Resolution

1. Disable UEFI Secure Boot on the system.
2. If Secure Boot is disabled, there might be an incompatibility between the `ampnetworkflow` kernel module provided with the connector and the system kernel or other third-party kernel modules installed on the system. Review */var/log/messages* for details.
3. If the connector is running on an unsupported kernel version, then either install a supported kernel version or build a custom `ampnetworkflow` kernel module for the current running system kernel. Review Building Cisco Secure Endpoint Linux Connector Kernel Modules for more information.

Fault 11: Required Kernel-Devel Package Is Missing

Condition

The connector requires that one of the following is valid:

1. The current kernel has `CONFIG_DEBUG_INFO_BTF` enabled, or
2. The correct kernel header package is installed in order to monitor filesystem and network events.

If neither of these conditions are met, then this fault will be raised and the connector will monitor filesystem and network events in degraded mode.

Resolution

1. Upgrade your kernel and restart the connector. This is the preferred solution.
2. If the fault persists, then install the missing kernel header package:
    1. For RPM-based distributions, install the `kernel-devel` package.
    2. For Oracle Linux UEK distributions, install the `kernel-uek-devel` package.
    3. For Debian-based distributions, install the `linux-headers` package.
    4. For SUSE distributions, install the `kernel-default-devel` package.

Refer to Troubleshoot Secure Endpoint Linux Connector Fault 11 for more details.

Fault 16: Incompatible Kernel

Condition

The connector 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.

Resolution

Downgrade the kernel to a supported version or upgrade the connector to a newer version that supports this kernel.

Refer to the Linux System Requirements for more details on supported kernel versions.

Fault 18: Connector Event Monitoring Is Overloaded

Condition

The connector is under heavy load due to an overwhelming number system events. System protection is limited and the connector will monitor a smaller set of system critical events until overall system activity is reduced.

Resolution

This fault could be an indication of malicious system activity or of very active applications on the system.

1. 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.
2. If no benign processes cause heavy load, then some investigation is required to determine if the increased activity is due to a malicious process.
3. If the connector is under short periods of heavy load then it is possible that this fault can clear itself.
4. 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.

Refer to Troubleshoot Secure Endpoint Mac/Linux Connector Fault 18 for more details.

Fault 19: SELinux Policy Is Missing Or Disabled

Condition

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 Enterprise Linux-based systems, 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.

Resolution

To resolve the fault, ensure the `policycoreutils-python` system package is installed. Then either:

1. Reinstall or upgrade the connector to trigger the installation of `cisco-secure-bpf`, or
2. 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.