Troubleshoot Linux Connector Compatibility on RHEL CentOS Oracle Linux

Contents

Introduction

Environment

- Connector Version
- Operating System
- Kernel Version

Issue

- Symptoms

Resolution

- Connector Upgrade

Related Content

- Linux OS Compatibility
- Linux User Guide

Introduction

This document describes an incompatibility between Cisco Secure Endpoint Linux connector versions 1.12.4 and earlier.

Environment

On these platforms, the connector can appear to operate normally but does not detect File Rename and Network Events, Red Hat Enterprise Linux, CentOS, and Oracle Linux 7.8. Upgrade to connector version 1.12.5 or later to restore full event detection.

This issue applies to the connector versions, operating systems, and kernel versions described in the next sections.

Connector Version

The affected connector versions are:

- 1.12.4 and earlier

Operating System

The affected operating systems are:

- Red Hat Enterprise Linux 7.8
- CentOS 7.8
- Oracle Linux 7.8 (RHCK)

Note: Oracle Unbreakable Enterprise Kernel (UEK) is supported in connector versions 1.18.0 and later.

Kernel Version

The affected kernel versions are:

- 3.10.0-1127.el7.x86_64 or later

Issue

On Red Hat Enterprise Linux, CentOS, and Oracle Linux 7.8 with kernel version 3.10.0-1127.el7.x86_64 or later, Cisco Secure Endpoint Linux connector versions 1.12.4 and earlier do not detect File Rename and Network Events.

Symptoms

Use these symptoms to confirm the issue:

- In the Cisco Secure Endpoint Console, File Rename and Network Events are not detected by the connector and do not appear in Device Trajectory.
- From a terminal window, run the command **sudo cat /var/log/messages | grep "kernel: ampnetworkflow: <info> _msg_send_offset: peer disconnected"**. The command returns multiple results, indicating a failure in the ampnetworkflow kernel module used by the connector.

```
sudo cat /var/log/messages | grep "kernel: ampnetworkflow: <info> _msg_send_offset: peer disconnected"
```

Resolution

Connector Upgrade

Complete these steps to confirm the issue, upgrade the connector, and confirm the fix:

1. Confirm the installed connector version on the endpoint. If the connector version is 1.12.4 or earlier, continue to the next step.
2. Confirm the running kernel version:

   From a terminal window, run the command **uname -r**.

   ```
   uname -r
   ```

   The command returns 3.10.0-1127.el7.x86_64 or a later kernel version. If the command returns this version or later, continue to the next step.

3. Upgrade the Cisco Secure Endpoint Linux connector to version 1.12.5 or later.
4. After the upgrade, confirm that File Rename and Network Events are detected again and appear in Device Trajectory.
5. Confirm that the ampnetworkflow error no longer appears in the system log:

   ```
   sudo cat /var/log/messages | grep "kernel: ampnetworkflow: <info> _msg_send_offset: peer disconnec
   ```

Related Content

Linux OS Compatibility

- Open the Cisco Secure Endpoint Linux Connector OS Compatibility documentation

Linux User Guide

- Open the Cisco Secure Endpoint Linux Connector User Guide