Troubleshooting

Troubleshooting

Security Analytics and Logging (OnPrem) General Troubleshooting Information

On the Manager, the following log files contain troubleshooting information related to Security Analytics and Logging (OnPrem):

- `/lancope/var/logs/containers/sal.log` - general app logging information (Manager only deployment only)
- `/lancope/var/logs/sal_preinstall.log` - information specific to the app installation process

On the Flow Collector, the following log files contain troubleshooting information related to Security Analytics and Logging (OnPrem) Data Store deployment:

- `lancope/var/sw/today/logs/sw.log` - information specific to telemetry logging
- `/lancope/var/logs/containers/svc-db-ingest.log` - information specific to event ingestion and the database

Security Analytics and Logging (OnPrem) Configuration Using Flow Collector Advanced Settings (Data Store Only)

If you configured your Flow Collector(s) to not store Firewall Logs during First Time Setup, you can update your ingest settings using the Flow Collector Advanced Settings page. To access Advanced Settings:

1. Log in to your Flow Collector (formerly known as Appliance Administration (Admin) interface).
2. Click **Support** > **Advanced Settings**.
3. In the **enable_sal** field, enter 1 to enable ingest of Firewall event logs.
4. If you want to change the port for Firewall logs, enter the new value in the **sal_syslog_port** field (default port is 8514).
5. Click **Apply** and then click **OK**.

Security Analytics and Logging (OnPrem) App Install Failure on Manager Only Deployment

We support installing the app on an Manager as a standalone appliance (Manager only), or an Manager that manages Flow Collector(s) and Data Node(s) (Data Store). You cannot install the app on a Manager if it manages one or more Flow Collectors and does not manage a Data Store. If you attempt to install the app in this situation, then the installation fails. To verify that this is the cause, review the log file at `/lancope/var/logs/sal_preinstall.log`. If you see the following message or similar, then the installation detected a managed Flow Collector:

```
Checking flow collectors...
1 Flow Collector(s) detected
Flow Collector(s) are present in inventory -- aborting installation.
```

To install the app, remove all managed Flow Collectors from the Central Manager Appliance Inventory, then try again.

⚠

Caution If you have a Manager only deployment, uninstalling the Security Analytics and Logging (OnPrem) app removes all related information, including event data, from your Manager, and removes the standalone Manager restriction. After you uninstall the Security Analytics and Logging (OnPrem) app, you can then manage one or more Flow Collectors with your Manager as part of a traditional Secure Network Analytics deployment to inspect traffic.

Security Analytics and Logging (OnPrem) App Dropping Events

The app may drop events in the following situations:

- You export all event types in syslog, instead of only connection, file, malware, and intrusion events.
- Your average events per second (EPS) ingest rate or burst EPS ingest rate exceeds the recommended specifications in the Secure Network Analytics Resource Allocation section.

For Manager only deployment, review the information in the Manager `/lancope/var/logs/containers/sal.log` log file to determine whether the app is dropping events. Search the file for entries containing "`events_dropped:`".

For Data Store deployment, review the information in the Flow Collector `lancope/var/sw/today/logs/sw.log` log file to determine whether the app is dropping events. Search the file for entries containing "`sal_event`".

Contact Cisco Support if this behavior persists.

Security Analytics and Logging (OnPrem) App Crash

If the Security Analytics and Logging (OnPrem) app crashes (due to an excessive ingest rate, for example), restart the Manager. This also restarts the app.

⚠

Caution Do not unistall the app. If you have a Manager only deployment, uninstalling the Security Analytics and Logging (OnPrem) app removes all related information, including event data, from your Manager.