**nix: Operating system logs

*nix operating system logs are a source of data that reports on state changes in a UNIX or Linux variant operating system. This includes changes to applications, service state, and hardware events. Data collected from these different elements are written to the plain text log files hosted within the operating system. These events are used by operations and development teams to troubleshoot and mitigate errors. Security and audit events are also written to the same place, but because they serve different use cases, they are covered in the *nix security logs data source article.

The *nix operating system logs contain important events relating to applications, system services, and the operating system. The events describe errors, warnings, and other information about activity taking place on each system. This information is used to monitor and troubleshoot each system. In the Common Information Model, *nix operating system logs can be mapped to any of the following data models, depending on the field: Endpoint, Inventory, Updates, Change, Performance, Network Sessions.

**Configuration**

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). Refer to the documentation, and note the following:

- Input type: Monitored OS Logs, syslog, and scripted
- Add-on or app: Splunk Add-on for Unix and Linux
- Sizing estimate: The best way to estimate sizing is to send the data to Splunk and use the monitoring console to get ingest sizing by index or sourcetype. Data ingest will vary widely, but an estimated baseline is 250/MB per day per item.

**Validation**

The first step in validating the logs is to run a search and confirm that the index is getting data in the proper time frame and that the source types and sources are as expected. Further validation is done by inspecting the events and making sure the needed fields are seen. A search similar to the following is a good starting point:

```
index=* earliest=-15m@
|stats count by sourcetype source index
```

**Application**

When your Splunk deployment is ingesting *nix operating system logs, you can use the data to achieve the following:
• Maintaining *nix systems
• Creating a timebound picture of network activity
• Recovering lost visibility of IT infrastructure