Maintaining *nix systems

In your organization, you have lots of *nix systems running critical applications or services. You need to monitor these systems to ensure the health of the associated apps and services, such as basic configuration, system diagnostics, file systems, and packages. You need to log and watch all these components, and ensure that appropriate technical staff are notified as quickly as possible if problems arise. With all these different concerns, you need Splunk searches that you can save and easily run on a schedule or as needed to keep your users up and running.

You can use Splunk software to manage patches and updates to ensure all connected systems and related processes are running after the patch or update is complete. You can also use Splunk software for a number of other maintenance tasks, such as watching out for connectivity issues.

Data required

Technologies:

- Splunk Enterprise or Splunk Cloud Platform and Splunk Add-on for Unix and Linux OR
- Splunk Infrastructure Monitoring and the Splunk OpenTelemetry Connector

Data:

- *nix operating system logs
- Command line output (df, ps, iostat, etc.) via scripted inputs

How to use Splunk software for this use case

You can run many searches with Splunk software to manage *nix systems. The following procedures can be run on Splunk Enterprise, Splunk Cloud Platform, or Splunk Infrastructure Monitoring:

- *Nix CPU utilization nearing capacity
- *Nix memory utilization nearing capacity
- Expected *Nix process not running
- *Nix host stops reporting data

These additional procedures can only be run on Splunk Enterprise or Splunk Cloud Platform:

- *Nix hosts with NFS connectivity issues
- Filesystem mounts after *nix patching event
- Processes running after *nix patching event
- Package installations and upgrades on a *nix server

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Next steps

To maximize their benefit, the how-to articles linked in the previous section likely need to tie into existing processes at your organization or become new standard processes. These processes commonly impact success with this use case:

- Running regular backups
- Maintaining tooling for software provisioning
- Maintaining tooling for configuration management
- Site reliability engineering processes

Measuring impact and benefit is critical to assessing the value of IT operations. The following are example metrics that can be useful to monitor when implementing this use case:

- Mean time to resolution
- Mean time to root cause
- Reduction in defects

This use case is also included in the IT Essentials Learn app, which provides more information about how to implement the use case successfully in your IT maturity journey. In addition, these Splunk resources might help you understand and implement this use case:

- Conf Talk: Designing and deploying a Splunk hardware monitoring service at Workday
- Conf Talk: Getting the most out of logs for IT monitoring and troubleshooting
- Tech Talk: Get monitoring tricks for all your *nix Part 1
- Tech Talk: Get monitoring tricks for all your *nix Part 2