Maintaining Microsoft Windows systems

In your organization, you have many applications and services hosted on Microsoft Windows that are critical to the support of the business. Because of the reliance on these critical applications and services by workers and management, you need to monitor availability and performance to make sure that the functionality is there when needed. In order to do this, you need to search application and infrastructure logs for key indicators of failures and potential performance degradation, which are often disparate. Because it is easy to get data into Splunk and then search and alert on key indicators, you are motivated to onboard data. After the data is available, you want to develop and save searches that help you achieve this type of monitoring efficiently. You can use Splunk software to monitor a large number of Windows system management tasks and events, such as patch management, software deployment, inventory tracking, remote access availability, and more.

Data required

Technologies:

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

Data:

- Windows event logs
- Windows update logs

How to use Splunk software for this use case

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

- Windows disk drive utilization nearing capacity
- Windows CPU utilization nearing capacity
- Windows memory utilization nearing capacity
- Expected Windows process not running
- Windows host stops reporting data

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

- Windows availability problems
- Microsoft recommended application log events
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:

- Active directory administration, which is closely related to Windows Maintenance
- The use of cloud services, such as Azure, to cover Windows maintenance requirements
- Integration with ticketing systems used for the service desk
- The use of any other related applications, such as MS SQL Server, IIS, Exchange, and O365, which can all affect a Windows environment

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:

- Availability of service: Percentage of agreed service time to down time
- Maintainability of service: Mean time to repair (MTTR) and mean time between failure (MTBF)
- Additional metrics: Page load times, average response time, and operations per second

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:

- Blog: Peeping through Windows (logs)
- Blog: Splunking Microsoft Azure Monitor Data Part - 2 - Splunk Setup
- Docs: Monitoring Windows event log data
- Blog: What the WEF... Choosing Windows Event Forwarding or Splunk UF
- Tech Talk: My start will go on: Splunk’s TA for Windows Part 1
- Tech Talk: My start will go on: Splunk’s TA for Windows Part 2