Windows disk drive utilization nearing capacity

Your organization's critical IT applications require space on disk to read and write to operate properly. When an application runs out of disk space, it usually results in application instability or crashing. You need a search to help detect when a disk drive is nearing capacity.

Data required

Technologies:

- Splunk Enterprise or Splunk Cloud Platform and [Splunk Add-on for Microsoft Windows](https://www.splunk.com/software/add-ons/windows/add-on) OR
- Splunk Infrastructure Monitoring and the [Splunk OpenTelemetry Connector](https://www.splunk.com/software/add-ons/open-telemetry)

Data:

- Windows event logs
- Windows update logs

Procedure

**Option 1**

1. In Splunk Enterprise or Splunk Cloud Platform, verify that you deployed the [Splunk Add-on for Microsoft Windows](https://www.splunk.com/software/add-ons/windows/add-on) add-on to your search heads, indexer, and Splunk Universal Forwarders on the monitored systems. For more information, see [About installing Splunk add-ons](https://docs.splunk.com/Documentation/Splunk/8.1.x/Introduction/GettingStarted/InstallingAddOns).

2. Run the following search. You can optimize it by specifying an index and adjusting the time range.

   ```splunk
   | mstats avg(LogicalDisk.%_Free_Space) AS "win_storage_free" WHERE index="<name of your metrics index>" host="<names of the hosts you want to check>" instance="<names of drives you want to check>" instance!="_Total" BY host, instance span=1m
   | eval storage_used_percent=round(100-win_storage_free,2)
   | eval host_dev=printf("%s:%s\",host,instance)
   | timechart max(storage_used_percent) AS storage_used_percent BY host_dev
   ```

**Search explanation**

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.
### Splunk Search

<table>
<thead>
<tr>
<th>mstats avg(LogicalDisk.%_Free_Space) AS &quot;win_storage_free&quot; WHERE index=&quot;&lt;name of your metrics index&gt;&quot; host=&quot;&lt;names of the hosts you want to check&gt;&quot; instance=&quot;&lt;names of drives you want to check&gt;&quot; instance!=&quot;_Total&quot; BY host, instance span=1m</th>
<th>Search metrics index(es) where perfmon disk space data is being collected and filter down to the desired host(s) to check.</th>
</tr>
</thead>
<tbody>
<tr>
<td>eval storage_used_percent=round(100-win_storage_free,2)</td>
<td>Convert percent storage free to percent storage used for readability.</td>
</tr>
<tr>
<td>eval host_dev=printf(&quot;%s:%s&quot;,host,instance)</td>
<td>Create a new field that combines the host and disk drive.</td>
</tr>
<tr>
<td>timechart max(storage_used_percent) AS storage_used_percent BY host_dev</td>
<td>Plot the storage used for each host and disk over time.</td>
</tr>
</tbody>
</table>

### Next steps

Create an alert based off this search so you can proactively manage potential stability issues. To alert when disk utilization is nearing max capacity, you can configure one of the following two recommendations:

- Use the SPL from this procedure to configure a Core Splunk alert.
- Build a new Vital Metric in IT Essentials Work for the desired entity type and configure vital metric alerting. Click [here](#) for an example SPL search that can be used for the vital metric search. After the vital metric has been created, configure it to alert when the disk used percentage is at or near 100.

Finally, you might be interested in other processes associated with the Maintaining Microsoft Windows systems use case.

### Option 2

1. Ensure that you have the Splunk OTEL Collector installed on the host you want to monitor.
2. In Splunk Infrastructure Monitoring, use the following SignalFlow to search the disk.utilization streaming metric, filter down to the desired hosts and mountpoints, and summarize results by counting the total number of processes found per host.

   ```
   A = data('disk.utilization', filter=filter('host', '<name of host to check>') and filter('mountpoint', '<name of disk to check>')).publish(label='A')
   ```

### Next steps

To alert when disk utilization is nearing capacity on the specified host(s) and mountpoint(s), use the SignalFlow from this procedure to configure a detector with an alert condition of "Resource Running Out" and alert settings of:

- Alert when nearing: Capacity

---

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.
• Capacity: 100
• Trigger Sensitivity: Medium

Finally, you might be interested in other processes associated with the Maintaining Microsoft Windows systems use case.