Windows memory utilization nearing capacity

Excessive memory utilization on a host, particularly abnormal or prolonged, is a sign of potential issues with the critical applications running on the host. You want to detect when an application is starved for memory resources, so you can prevent performance degradations or application instability.

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

Procedure

Option 1

1. In Splunk Enterprise or Splunk Cloud Platform, verify that you deployed the Splunk Add-on for Microsoft Windows add-on to your search heads, indexer, and Splunk Universal Forwarders on the monitored systems. For more information, see About installing Splunk add-ons.

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

   | mstats avg(Memory.Committed_Bytes) as Memory.Committed_Bytes avg(Memory.Available_Bytes) AS Memory.Available_Bytes WHERE index="<name of Windows metrics index>" AND host="<name of host to check>" span=1m BY host
   | eval total_memory=('Memory.Committed_Bytes'+"'Memory.Available_Bytes'")
   | eval percent_used=('Memory.Committed_Bytes'/total_memory*100)
   | timechart avg(percent_used) AS "% Memory Used" BY host

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(Memory.Committed_Bytes) as Memory.Committed_Bytes avg(Memory.Available_Bytes) AS Memory.Available_Bytes WHERE index=&quot;&lt;name of Windows metrics index&gt;&quot; AND host=&quot;&lt; name of host to check &gt;&quot; span=1m BY host</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>eval total_memory=('Memory.Committed_Bytes'+Memory.Available_Bytes)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>eval percent_used=('Memory.Committed_Bytes'/total_memory*100)</th>
</tr>
</thead>
</table>

| timechart avg(percent_used) AS "% Memory Used" BY host |

<table>
<thead>
<tr>
<th>Explanation</th>
</tr>
</thead>
</table>

Search metrics index(es) where perfmon memory utilization data is being collected and filter down to the desired hosts to check.

Calculate total memory.

Calculate the percent of memory used.

Plot the percent of memory used for each host over time.

### Next steps

Create an alert based on this search so you can proactively manage potential stability issues. To alert when an expected Windows process is not running, you can configure one of the following two recommendations:

- Use the SPL from this procedure to configure a Core Splunk alert.
- Configure the Average Memory Usage vital metric for the Windows entity type in IT Essentials Work to alert when the memory utilization 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 memory.utilization streaming metric and filter down to the desired hosts and processes.

```bash
A = data('memory.utilization', filter=filter('host.name', '<name of host to check>'), rollup='latest').publish(label='A')
```

### Next steps

To alert when memory utilization is nearing max capacity for the selected hosts, use the SignalFlow from this procedure to configure a detector with an alert condition of "Static Threshold" and alert settings of:

- Alert when: Above
- Threshold: 95
- Trigger sensitivity: Duration
- Duration: 5m

Finally, you might be interested in other processes associated with the [Maintaining Microsoft Windows systems](#) use case.