ESXi hosts with sustained high swapping

When an ESXi host can't reclaim necessary memory through ballooning, the host begins to swap memory to disk. Memory swapping on the host is a strong indication that the host is over provisioned and experiencing significant memory pressure. The latency introduced by the swapping has a noticeable performance impact on the virtual machines running on the host. You want to monitor and investigate hosts with high memory swapping.

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Splunk Enterprise or Splunk Cloud Platform
  OR
  Splunk Infrastructure Monitoring and the Splunk OpenTelemetry Connector
- Virtualization data
- System log data
- IT Essentials Work
- Splunk Add-on for VMware ESXi Logs
- Splunk Add-on for vCenter Logs
- Splunk Add-on for VMware Metrics

Procedure

Option 1

To optimize the search shown below, you should specify an index and a time range.

1. In Splunk Enterprise or Splunk Cloud Platform, ensure that you have installed the IT Essentials Work app to onboard VMware data and provide the various VMware entity type configurations and dashboards.
2. Ensure that you are collecting VMware data through one or more Data Collection Nodes, which are essentially Splunk heavy forwarders with specific VMware collection configurations.
3. Run the following search. You can optimize it by specifying an index and adjusting the time range.

```
| mstats max(vsphere.esxihost.mem.llSwapUsed) AS vsphere.esxihost.mem.llSwapUsed WHERE (index=vmware-perf-metrics) BY name moid | stats max(vsphere.esxihost.mem.llSwapUsed) AS max_p_average_mem_llSwapUsed_kiloBytes BY name moid | eval is_high_swapping = if(max_p_average_mem_llSwapUsed_kiloBytes > 5000, 1, 0) | eventstats mean(max_p_average_mem_llSwapUsed_kiloBytes) AS mean_host_population stdev(max_p_average_mem_llSwapUsed_kiloBytes) AS stdev_host_population
```
| eval stdev_from_host_population = (max_p_average_mem_llSwapUsed_kiloBytes - mean_host_population) / stdev_host_population
| sort - stdev_from_host_population
| table name moid max_p_average_mem_llSwapUsed_kiloBytes is_high_swapping stdev_from_host_population mean_host_population stdev_host_population

**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.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mstats max(vsphere.esxihost.mem.llSwapUsed) AS vsphere.esxihost.mem.llSwapUsed WHERE (index=vmware-perf-metrics) BY name moid</td>
<td>Calculate the average of llSwapUsed, which is the amount of space used for caching swapped pages in the host cache, in kilobytes, for each managed object ID (MOID).</td>
</tr>
<tr>
<td>eval is_high_swapping = if(max_p_average_mem_llSwapUsed_kiloBytes &gt; 5000, 1, 0)</td>
<td>Create the is_high_swapping field for results where more than 5,000 kilobytes of space are used.</td>
</tr>
<tr>
<td>eventstats mean(max_p_average_mem_llSwapUsed_kiloBytes) AS mean_host_population stdev(max_p_average_mem_llSwapUsed_kiloBytes) AS stdev_host_population</td>
<td>Calculate the average and standard deviation of the results.</td>
</tr>
<tr>
<td>eval stdev_from_host_population = (max_p_average_mem_llSwapUsed_kiloBytes - mean_host_population) / stdev_host_population</td>
<td>Calculate a running total of how many standard deviations away each MOID is from the average amount of space used and put the result in a field called stdev_from_host_population.</td>
</tr>
<tr>
<td>sort - stdev_from_host_population</td>
<td>Sort results with the largest standard deviation first.</td>
</tr>
<tr>
<td>table name moid max_p_average_mem_llSwapUsed_kiloBytes is_high_swapping stdev_from_host_population mean_host_population stdev_host_population</td>
<td>Display the results in a table with columns in the order shown.</td>
</tr>
</tbody>
</table>

**Next steps**

Sample results for this search are shown in the table below. None of the hosts have crossed the swapping threshold set...
in the search. You can see the average KB of memory swapped and which hosts are under some memory pressure and which are less so. From that information, you can determine if and where to move load from and to in order to better balance load.

<table>
<thead>
<tr>
<th>moid</th>
<th>Avg Mem swapped (KB)</th>
<th>Swapping</th>
<th>Mean Host Pop.</th>
<th>Stdev of Host Pop</th>
<th>Stdev Across Host Pop</th>
</tr>
</thead>
<tbody>
<tr>
<td>host-26</td>
<td>1000</td>
<td>No</td>
<td>325</td>
<td>471.699</td>
<td>1.431</td>
</tr>
<tr>
<td>host-11</td>
<td>300</td>
<td>No</td>
<td>325</td>
<td>471.699</td>
<td>-0.053</td>
</tr>
<tr>
<td>host-10</td>
<td>0</td>
<td>No</td>
<td>325</td>
<td>471.699</td>
<td>-0.689</td>
</tr>
<tr>
<td>host-20</td>
<td>0</td>
<td>No</td>
<td>325</td>
<td>471.699</td>
<td>-0.689</td>
</tr>
</tbody>
</table>

Finally, you might be interested in other processes associated with the Monitoring VMware virtual machine performance use case.

**Option 2**

1. Ensure that you have the Splunk OTEL Collector installed on the host you want to monitor. After installation, complete the following additional steps:
   1. Configure the receiver in agent_config.yaml. Note the extra groups.

   ```yaml
   receivers:
     smartagent/vsphere:
       type: vsphere
       host: "vcenterexample.local"
       username: "administrator"
       password: "mypassword"
       insecureSkipVerify: true
       extraGroups:
         - cpu
         - mem
   
   2. Configure the service pipeline in agent_config.yaml (smartagent/vsphere).

   ```yaml
   service:
     ...
     metrics:
       receivers: [hostmetrics, otlp, signalfx, smartagent/signalfx-forwarder, smartagent/vsphere]
   
   3. Restart the agent after configuration changes:

   systemctl restart splunk-otel-collector
2. In Splunk Infrastructure Monitoring, use the following SignalFlow to search the vsphere.mem_swapin_rate_kbs and vsphere.mem.swapout_rate_kbs streaming metrics and calculate the mean by host.

\[
A = \text{data('vsphere.mem_swapin_rate_kbs', filter=filter('object_type', 'HostSystem'))}.\text{publish}(label='A', \text{enable=False}) \\
B = \text{data('vsphere.mem_swapout_rate_kbs', filter=filter('object_type', 'HostSystem'))}.\text{publish}(label='B', \text{enable=False}) \\
C = (A+B).\text{mean(by=['esx_ip'])}.\text{publish}(label='C')
\]

**Next steps**

To alert when the swap rate suddenly changes on an ESXi host, you can use the SignalFlow from this procedure to configure a detector with the following configurations:

- Alert condition: Sudden change
- Alert when: Too high
- Trigger sensitivity: Medium

Finally, you might be interested in other processes associated with the Monitoring VMware virtual machine performance use case.