Health of critical AWS infrastructure from CloudWatch metrics

You might want to view the health of critical AWS infrastructure from CloudWatch metrics when doing the following:

- Managing an Amazon Web Services environment

Prerequisites

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

- Splunk Enterprise or Splunk Cloud Platform
- AWS description data
- Splunk Add-on for Amazon Web Services

Example

CloudWatch metrics can be collected on almost any type of AWS infrastructure and subsequently collected into a Splunk deployment. This central metric collection mechanism allows you to gain immediate visibility into the health and performance of AWS infrastructure across regions and accounts without additional instrumentation.

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

1. Ensure that your deployment is ingesting AWS data through one of the following methods:
   - Pulling the data from Splunk via AWS APIs. At small scale, pull via the AWS APIs will work fine.
   - Pushing the data from AWS into Splunk via Lambda/Firehose to Splunk HTTP event collector. As the size and scale of either your AWS accounts or the amount of data to be collected grows, pushing data from AWS into Splunk is the easier and more scalable method.

2. Run the following search:

   index=<AWS index name> sourcetype=aws:cloudwatch metric_name=<metric name> metric_dimensions=*
   | eval final=metric_dimensions."": ".metric_name
   | timechart avg(Average) AS Average BY final

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>index=&quot;&lt;AWS index name&gt;&quot;</td>
<td>Search the index(s) where AWS data is stored filtered to just the AWS description data.</td>
</tr>
<tr>
<td>sourcetype=&quot;aws:description&quot;</td>
<td></td>
</tr>
<tr>
<td>metric_name=&quot;&lt;metric name&gt;&quot;</td>
<td>Filter the metrics and resources down to a subset of the data you wish to visualize, replacing the metric name and AWS ID as needed for your metrics and resources. Multiple values and wildcards are acceptable.</td>
</tr>
<tr>
<td>metric_dimensions=&quot;*&lt;ID&gt;**&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>eval final=metric_dimensions.&quot;*.metric_name</td>
</tr>
<tr>
<td></td>
<td>timechart avg(Average) AS Average BY final</td>
</tr>
</tbody>
</table>

**Result**

With [IT Essentials - Work](#), you can configure the AWS dashboards content pack for pre-built dashboards to get even more detail about the health of your metrics.