Topology of a VMware environment

Visualizing the VMware environment in a topology view provides an intuitive way for analysts and administrators to better understand the current distribution of resources. A topology view may uncover misconfigurations such as high availability VMs deployed to the same ESXi host, or co-mingled prod and non-prod systems. Additionally, you can use the time picker to review prior topology views to aid in troubleshooting or understand how resources have shifted over time.

Prerequisites

- Splunk Enterprise or Splunk Cloud Platform
- 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

1. 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.

```splunk
index="vmware-inv" source="VMInv:Hierarchy" type=*
| dedup moid
| eval parent_moid=coalesce('changeSet.runtime.host.moid','changeSet.parent.moid'), name='changeSet.name'
| appendpipe [ stats count BY moid, name=changeSet.name' 
| rename moid AS parent_moid, name AS parent_name 
| table parent_*)
| eventstats values(parent_name) AS parent_name BY parent_moid
| top useother=true limit=5 name BY parent_name type
| table parent_name name percent
| rename parent_name AS parent, name AS child
```
## 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><code>index=&quot;vmware-inv&quot; source=&quot;VMInv:Hierarchy&quot; type=*</code></td>
<td>Search index and sourcetype for for VMware hierarchy data.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>`</td>
<td>dedup moid`</td>
</tr>
<tr>
<td>`</td>
<td>eval parent_moid=coalesce('changeSet.runtime.host.moid','changeSet.parent.moid'), name='changeSet.name'`</td>
</tr>
<tr>
<td>`</td>
<td>appendpipe [ stats count BY moid, name</td>
</tr>
<tr>
<td>`</td>
<td>eventstats values(parent_name) AS parent_name BY parent_moid`</td>
</tr>
<tr>
<td>`</td>
<td>top useother=true limit=5 name BY parent_name type`</td>
</tr>
<tr>
<td>`</td>
<td>table parent_name name percent`</td>
</tr>
<tr>
<td>`</td>
<td>rename parent_name AS parent, name AS child`</td>
</tr>
</tbody>
</table>

## Next steps

You can use this information on-demand during troubleshooting or periodically during general environment checks to monitor your environment.

The SPL in this sample provides one meaningful way of rendering the hierarchy of the environment, however, many other ways may exist as well. For instance, you may want to filter the results per the type field in a dashboard and render a greater number of nodes in the tree. You should modify the SPL to provide a hierarchical rendering that fits your needs.

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