Recently triggered vSphere alarms

VMware vSphere lets you author alerting rules to identify various conditions that occur in your VMware environment. Some alerts indicate problems while others are informational. You want a search that allows you to easily see all alarms so that you can review them and investigate further if necessary.

Prerequisites

- Splunk Enterprise or Splunk Cloud Platform
- Virtualization data
- System log data
- IT Essentials Work
- Splunk Add-on for VMware
- 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.

```
index="vmware-taskevent" sourcetype="vmware_inframon:events"
| spath alarm
| search alarm=*
| eval From=if(isnull('from'),"N/A","from"), To=if(isnull('to'),"N/A","to")
| stats count BY host, entity.entity.type, entity.name, From, To, fullFormattedMessage, _time
| rename host AS vCenter entity.entity.type AS "Entity Type" entity.name AS "Entity Name"
fullFormattedMessage AS "Message"
| fields - count
```

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.

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.
## Splunk Search

<table>
<thead>
<tr>
<th>Search Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>index=&quot;vmware-taskevent&quot; sourcetype=&quot;vmware_inframon:events&quot;</code></td>
<td>Search event indexes for VMWare events.</td>
</tr>
<tr>
<td>`</td>
<td>spath alarm`</td>
</tr>
<tr>
<td>`</td>
<td>search alarm=*`</td>
</tr>
</tbody>
</table>
| `| eval From=if(isnull('from'),"N/A","from'`,
To=if(isnull('to'),"N/A","to'")` | Validate that data is present. |
| `| stats count BY host, entity.entity.type, entity.name, From, To, fullFormattedMessage, _time` | Display the alarm related information. |
| `| rename host AS vCenter entity.entity.type AS "Entity Type" entity.name AS "Entity Name"
fullFormattedMessage AS "Message"` | Rename the fields as shown for better readability. |
| `| fields - count` | Remove the count field from the results. |

## Next steps

The results show the time each alarm was triggered, the host they were triggered on, the host’s previous status and current status after the alarm, and the alarm’s message. Depending on the types of rules you author and activate, it might be helpful to correlate VMware alerts with other operational and performance metrics associated with the applications running on the virtual machine.

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