vCenter console logins

VMware vCenter Server is advanced server management software that provides a centralized platform for controlling your VMware vSphere environments, allowing you to automate and deliver a virtual infrastructure across the hybrid cloud. This search will help you to control access to the VMWare environment, including reviewing who has accessed the system and how frequently or infrequently they do so.

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.

   ```
   index=vmware-taskevent sourcetype="vmware_inframon:events"
   | stats count BY userName eventClass ipAddress userAgent _time
   ```

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=vmware-taskevent sourcetype=&quot;vmware_inframon:events&quot;</td>
<td>Search the event index where VMware vCenter task data is collected.</td>
</tr>
</tbody>
</table>
Next steps

Knowing what modifications are made to the VMware environment, when they were made, and who made them can help you identify or isolate the origin of a problem or incident. To prevent accidental misconfigurations, it might be safer to revoke access for users who access VMware infrequently. This procedure might also surface accounts created for employees who are no longer with the company or no longer in the organization where VMware access is needed.

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