Table Of Contents

1. Log Insight Alerting
   1.1 Alert Integration into vRealize Operations Manager - Configuration Example
1. Log Insight Alerting

Log Insight for vCenter provides several terrific integration points. This section will take a look at each of those.
1.1 Alert Integration into vRealize Operations Manager - Configuration Example

Integrating Alerts into vRealize Operations Manager

- Log Insight Alert Notification Options
  - Email
  - Webhook
  - vRealize Operations Manager

- Integration allows for enhanced alerting within vRealize Operations Manager
  - Provides additional context for alerts through customizable alert Name, Description, and Recommendations
  - Adjust Criticality for the alerts
  - Control and fine tune how often alerts are created
  - Log detail immediately available as part of the vRealize Operations Manager alert

vRealize Log Insight offers several options to handle alert notifications. One of which is through vRealize Operations Manager. Integrating Log Insight’s alert notifications into vRealize Operations Manager offers several advantages. The alerts sent to vRealize Operations Manager can have customized names, descriptions, and even recommendations. These can include troubleshooting steps, links to internal or external web resources, and so forth. The alert notifications can be fine tuned so alerts are only sent when it is really necessary. The actual log detail is also sent and made available within vRealize Operations Manager. This gives users as much context and information as possible in a single location so they can make the smartest decision possible regarding their environment’s alerts.
We can take a look at an example and be able to see how each section of the vRealize Log Insight alert configuration is shown within the vRealize Operations Manager alert.

Let’s start by logging in to the vRealize Log Insight Server. You can do this by pointing your web browser to https://
Now that we are logged in, we will want to navigate to the "Interactive Analytics" page.

Once on the "Interactive Analytics" page, we can see the events received over the last 5 minutes. We will use the search box to find events related to SSH activities.
To find the exact events we’re looking for, we fine-tuned our search criteria down to "sshd accepted" events and extended the search timeline to "Latest 6 hours of data". We will then want to create an event filter to ensure we receive only events of this time. We do this by clicking on "event_type" for one of the events listed.

We’re looking for events exactly like this one. Therefore, within the popup menu, in the "Add Filter" section, we will want to select "Events Like This".
The filter will then be applied across the data Log Insight has received over the time period selected, in this case it is over the past 6 hours. We are now able to create the alert based off this filter which will be forwarded to vRealize Operations Manager. We will fire select the "Alert" option, followed by the "Create Alert from Query" option.

On the "New Alert" screen, we will want to populate all of the options available. Name: Host: SSH Session StartedDescription: An ESXi host has started an SSH session. This action should be inspected as soon as possible.Recommendation: (Input relevant information. In this case, we have input a local Sharepoint page as well as a VMware Knowledge Base page)Notify Section: Checkmark "Send to vRealize Operations Manager" and set the "Criticality"
to "Critical" Raise an alert Section: Ensure the "On any match" option has been selected. To create the new alert, click the "Save" button which is located in the bottom right-hand corner.

The new alert has been configured and we are ready to monitor vRealize Operations Manager for any potential ESXi host SSH sessions. To do this, we will login to our vRealize Operations Manager web console.
Now that we're logged in, select the "Host Systems" tab within the "Recommended Actions" dashboard.

After a period of time, we are shown a critical alert which has been sourced from Log Insight due to a SSH session having started on a ESXi host. We can click on the alert and see additional information.
We are then sent to the “Alerts” page for the ESXi host which Log Insight discovered a new SSH session on. The alert page shows us all of the information we entered from Log Insight such as the title, description, and recommendation. We can also see the exact event text which includes things like a timestamp and the source IP Address for the SSH session. vRealize Operations Manager also adds links to see additional information about the host such as its metrics, logs, and events.