sumo logic

Kubernetes on Sumo Logic

Student Lab Guide

Rev 08.16.24.K

©2024 Sumo Logic, All Rights Reserved.

sumo logic

Lab 0: Log in to the training environment

The training lab environment is separate from your other accounts. To access the training lab environment:

1. Open a new browser tab.
2. Go to https://service.sumologic.com.
3. Enter **training+analyst###@sumologic.com** in the **Email** field. Replace ### with a three digit number between 000 and 999.
4. Enter the **Password** provided to you by your instructor.
   Note: The password changes monthly.

Note: The training environment is a **shared, dynamic environment.** The data is refreshed and cleaned periodically. Other students can see the comments you make, so be careful what information you share. The dynamic updates and activities of other students may affect the data you see. Your experience will vary from one session to the next.

©2024 Sumo Logic, All Rights Reserved.

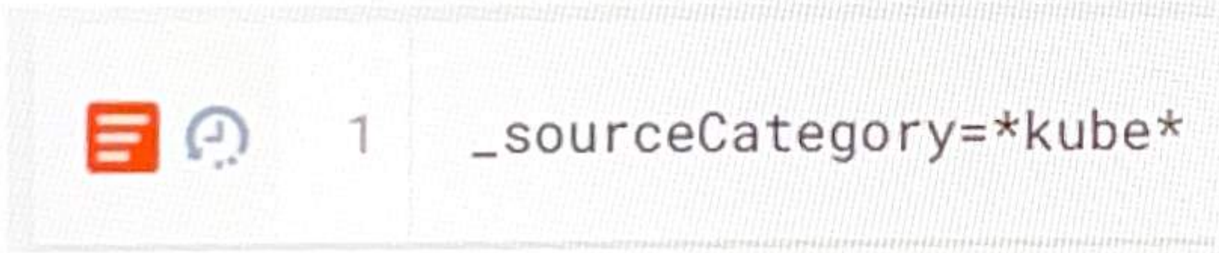
sumo logic

Lab 1: Search and visualize Kubernetes data

In this lab, we'll use the Sumo Logic query language to find and visualize Kubernetes data.

Navigate to the Sumo Logic UI if you're not already there. Refer to Lab 0 if you need help.

1. In the left nav menu, click **Logs > Log Search**.
2. Make sure you're in **Advanced Mode**. If you're not in Advanced Mode, click the **three dot icon** on the right side of the query builder. You'll be given the option to switch to **Advanced Mode**. If you're already in Advanced Mode, you'll be given the option to switch to Basic Mode.
3. Type `_sourceCategory=*kube*` into the query builder. Press **Enter** or click the **magnifying glass icon** to start the search.



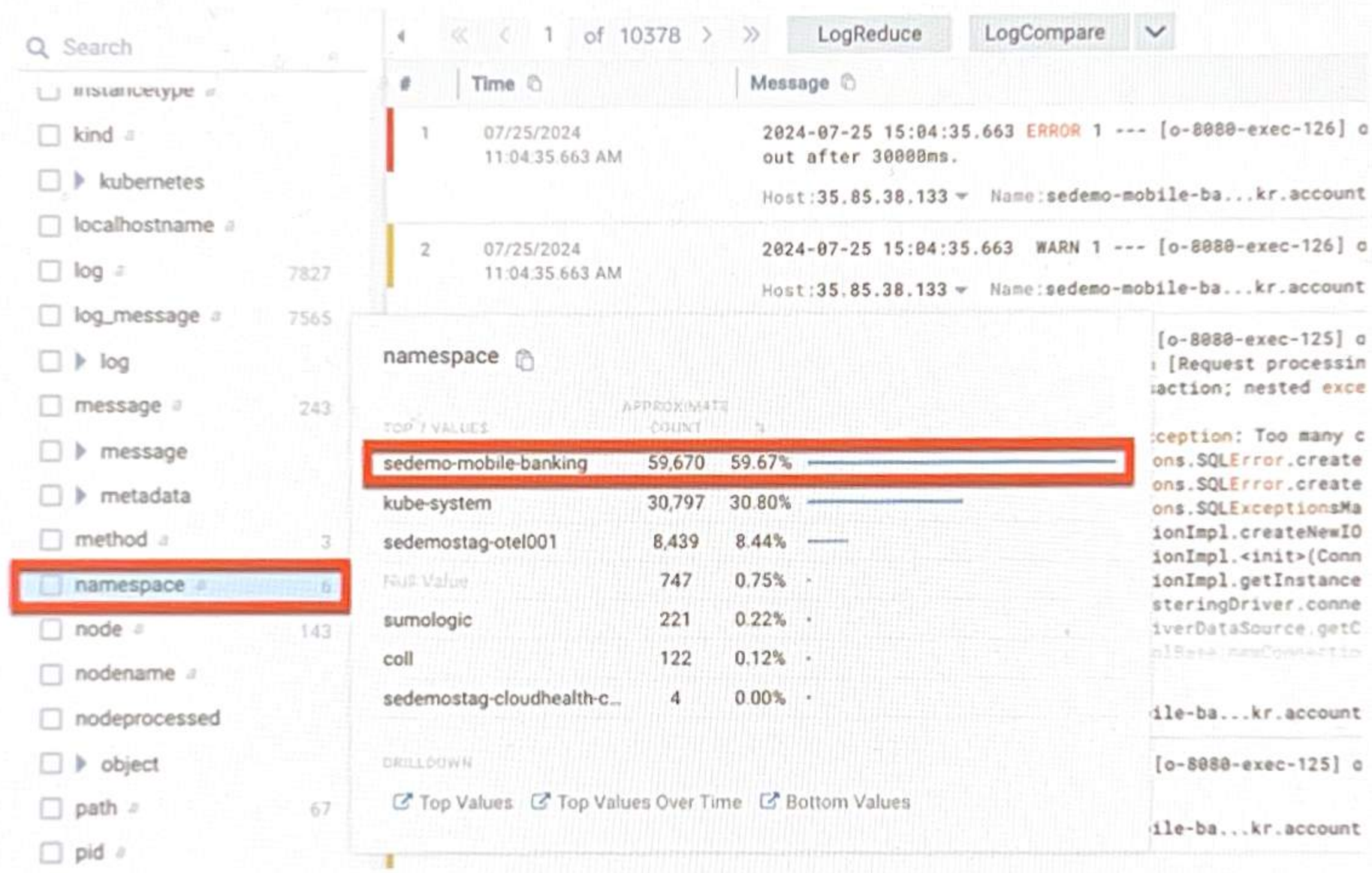
Using the asterisks as a wildcard like this will capture all Kubernetes-related data.

With this query, we might see hundreds, sometimes thousands of pages of log messages. (Your exact results will vary.) That's too many to parse through manually – let's see if we can narrow down these results further.

4. In the field browser on the left side, find and click on the **Namespace** field. You will see a popup with a list of the namespaces included in the current query. Narrow down the

©2024 Sumo Logic, All Rights Reserved.

results of the display by selecting a specific namespace (ex. **sedemo-mobile-banking**)

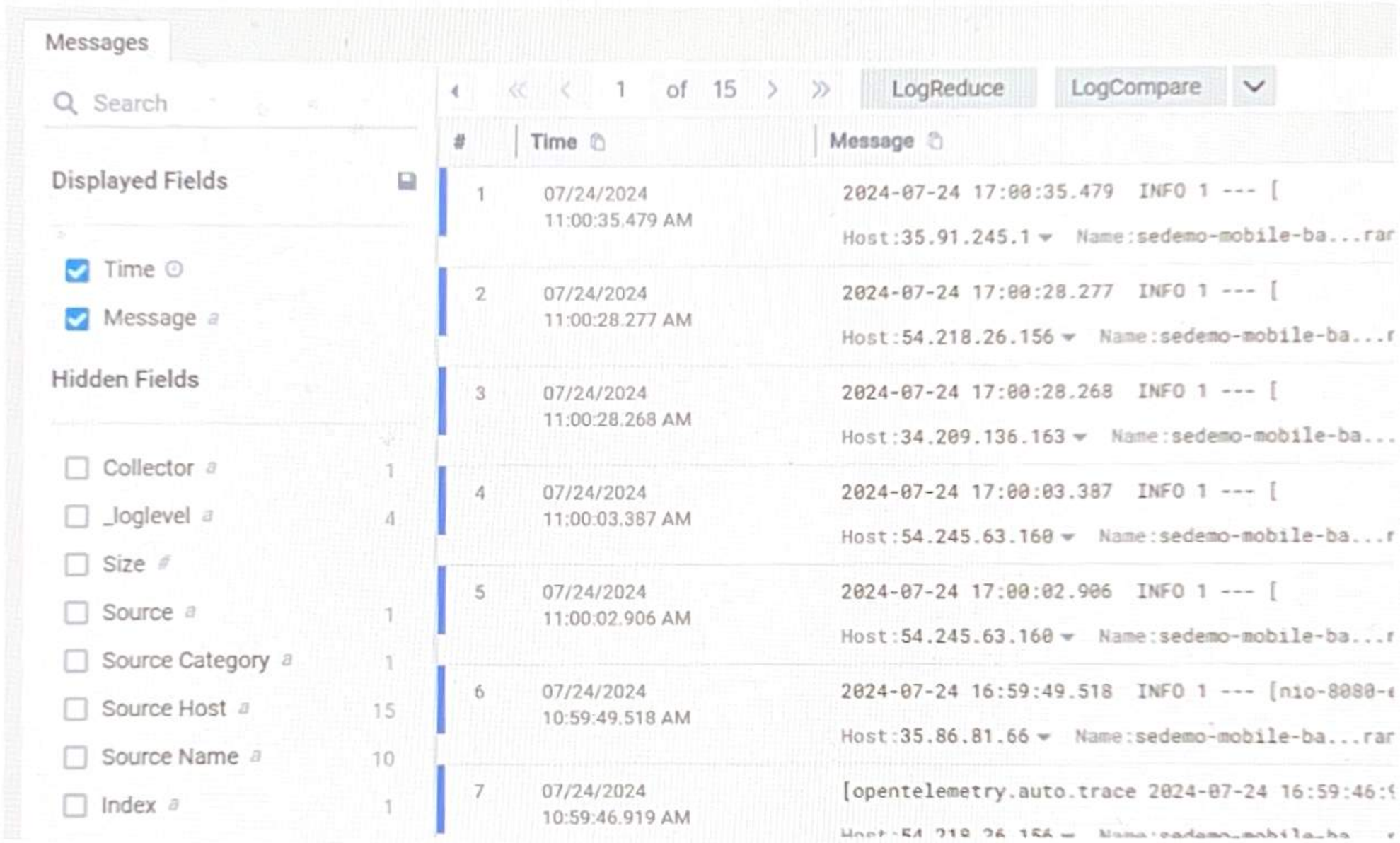


5. Do the same thing with the **container** field, selecting one of the available containers (ex. **transactions-service**).
6. You can accomplish the same data partition as in steps 4 and 5 by adding `namespace=sedemo-mobile-banking` and `container=transactions-service` to the end of your query to narrow down the results. Press **Enter** or click the **magnifying glass icon** to execute the search query this way.

```
1  _sourceCategory=*kube* namespace=sedemo-mobile-banking container=transactions-service
```

Both Sumo Logic's field browser and query language let you easily partition data, such as searching only the namespace for mobile banking looking at only transactional records. .

©2024 Sumo Logic, All Rights Reserved.



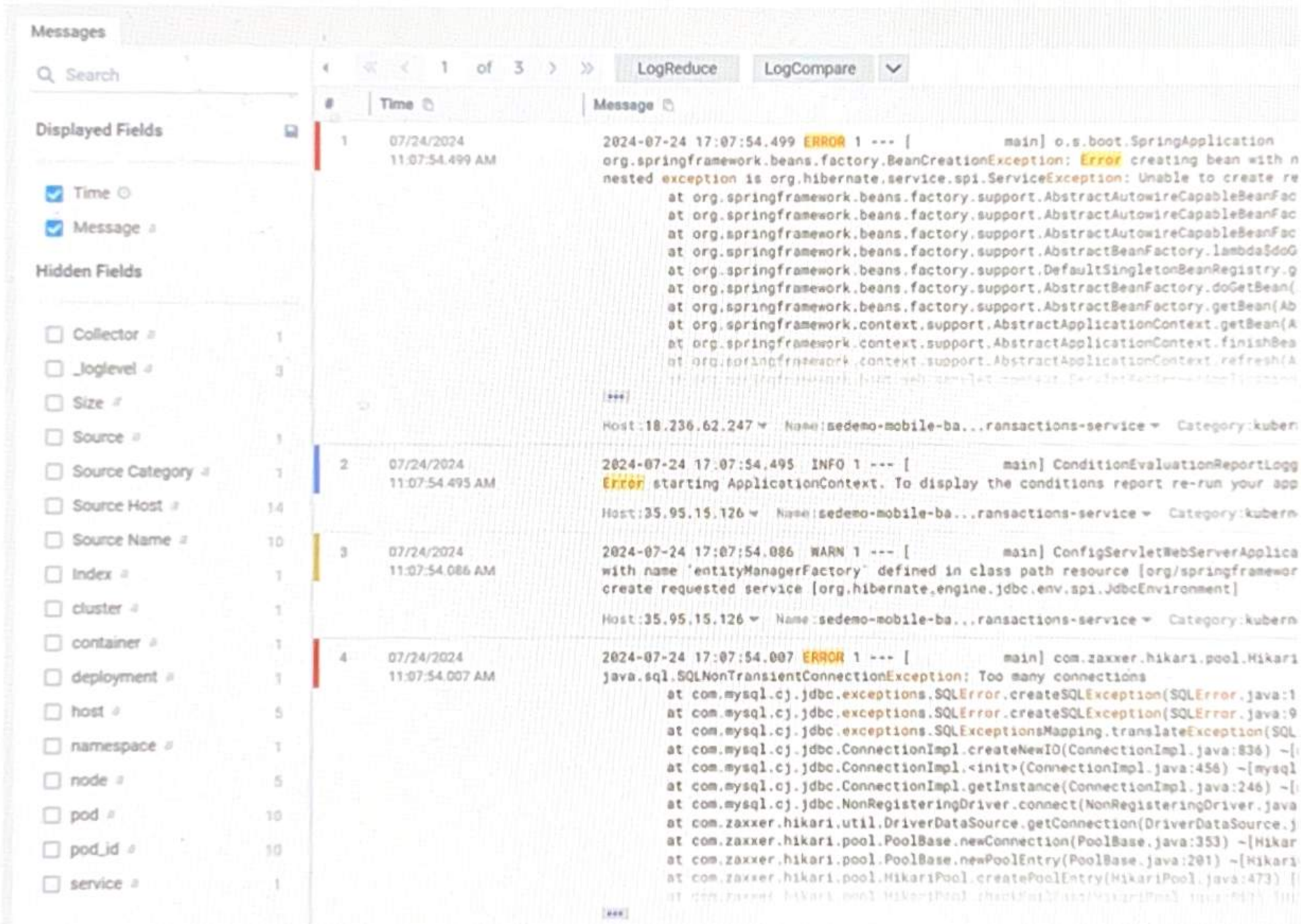
With this new query we have now reduced the previous dataset to a much smaller set of records (your exact number of data pages will vary).

7. On the right side of the histogram, click on the **error** keyword to filter the log data further by only displaying error messages.
8. You can also accomplish the same filter as step 7 by adding "`error`" to the end of your query, then pressing **Enter** or clicking the **magnifying glass icon** to redo. Alternatively, you can also click on the red portion of the histogram, or use the "_loglevel" field in the field browser to filter by errors the same way.

```
1 _sourceCategory=*kube* namespace=sedemo-mobile-banking container=transactions-service "error"
```

Using any of these methods, we can now see all the error messages produced by the mobile banking transaction service in our Kubernetes cluster.

©2024 Sumo Logic, All Rights Reserved.



At this point, we should have only a small handful of log messages to examine now. Your exact results may vary.

9. Add two new lines to your query:

```
| timeslice 1m
| count by _timeslice
```

To create a new line. Use **Shift+Enter** on a Mac, or **Alt+Enter** on Windows. Remember to type a pipe **|** symbol at the beginning of each new line.

```
1 _sourceCategory=*kube* namespace=sedemo-mobile-banking container=transactions-service "error"
2 | timeslice 1m
3 | count by _timeslice
```

©2024 Sumo Logic, All Rights Reserved.

sumo logic

10. Press **Enter** or click the **magnifying glass icon** to start the search.

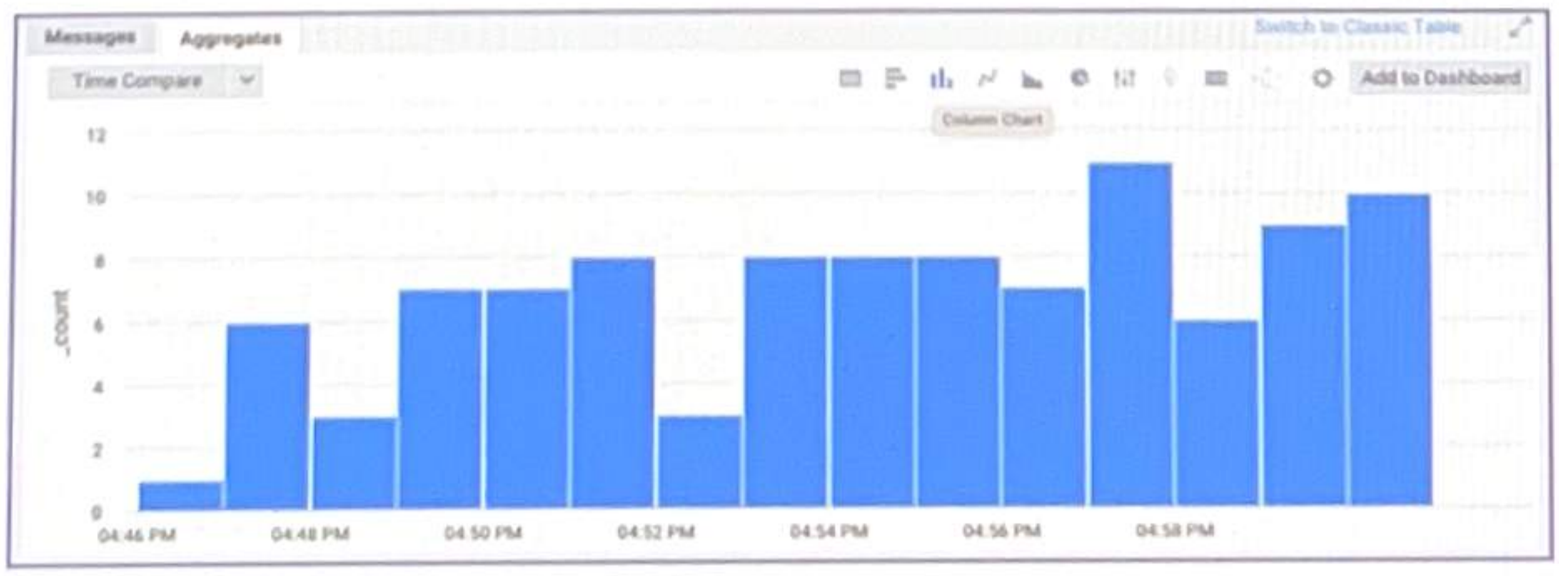
Messages | Aggregates

Page: 1 of 1 | Time Compare

#	Time	_count
1	06/27/2022 4:53:00.000 PM -0700	8
2	06/27/2022 4:48:00.000 PM -0700	3
3	06/27/2022 4:54:00.000 PM -0700	8
4	06/27/2022 4:52:00.000 PM -0700	3
5	06/27/2022 4:56:00.000 PM -0700	7
6	06/27/2022 4:57:00.000 PM -0700	11
7	06/27/2022 5:00:00.000 PM -0700	10

The `timeslice` operator groups data by chunks of time. The `count` operator then counts the number of log messages in each time slice. Here in the **Aggregates** tab we see a table showing the time range and the number of log messages.

11. Click the **Column Chart** icon in the **Aggregates** tab.



Now you can visualize the number of errors per minute.

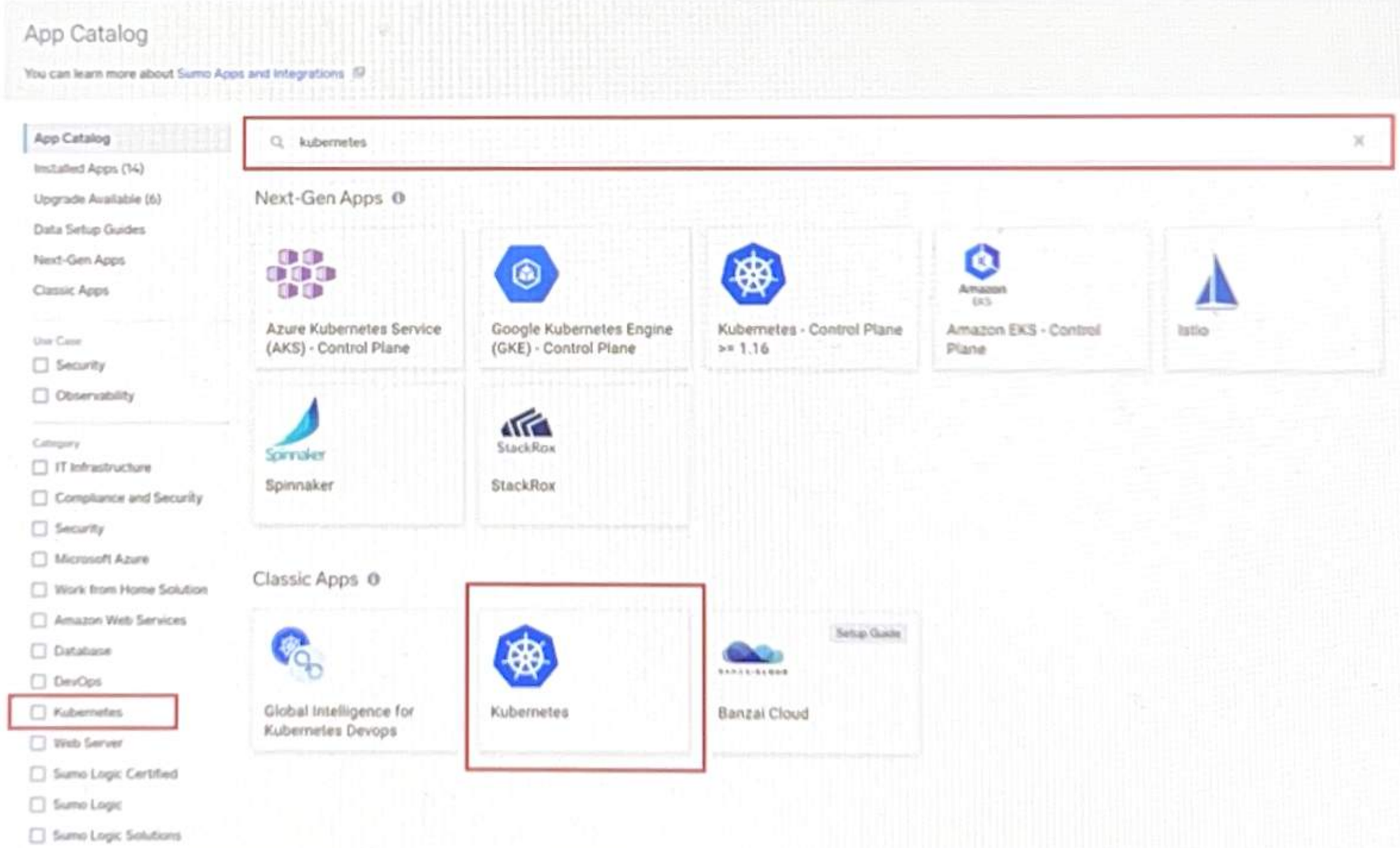
©2024 Sumo Logic, All Rights Reserved.

sumo logic

Lab 2: View pre-built dashboards

Navigate to the Sumo Logic UI if you're not already there. Refer to Lab 0 if you need help.

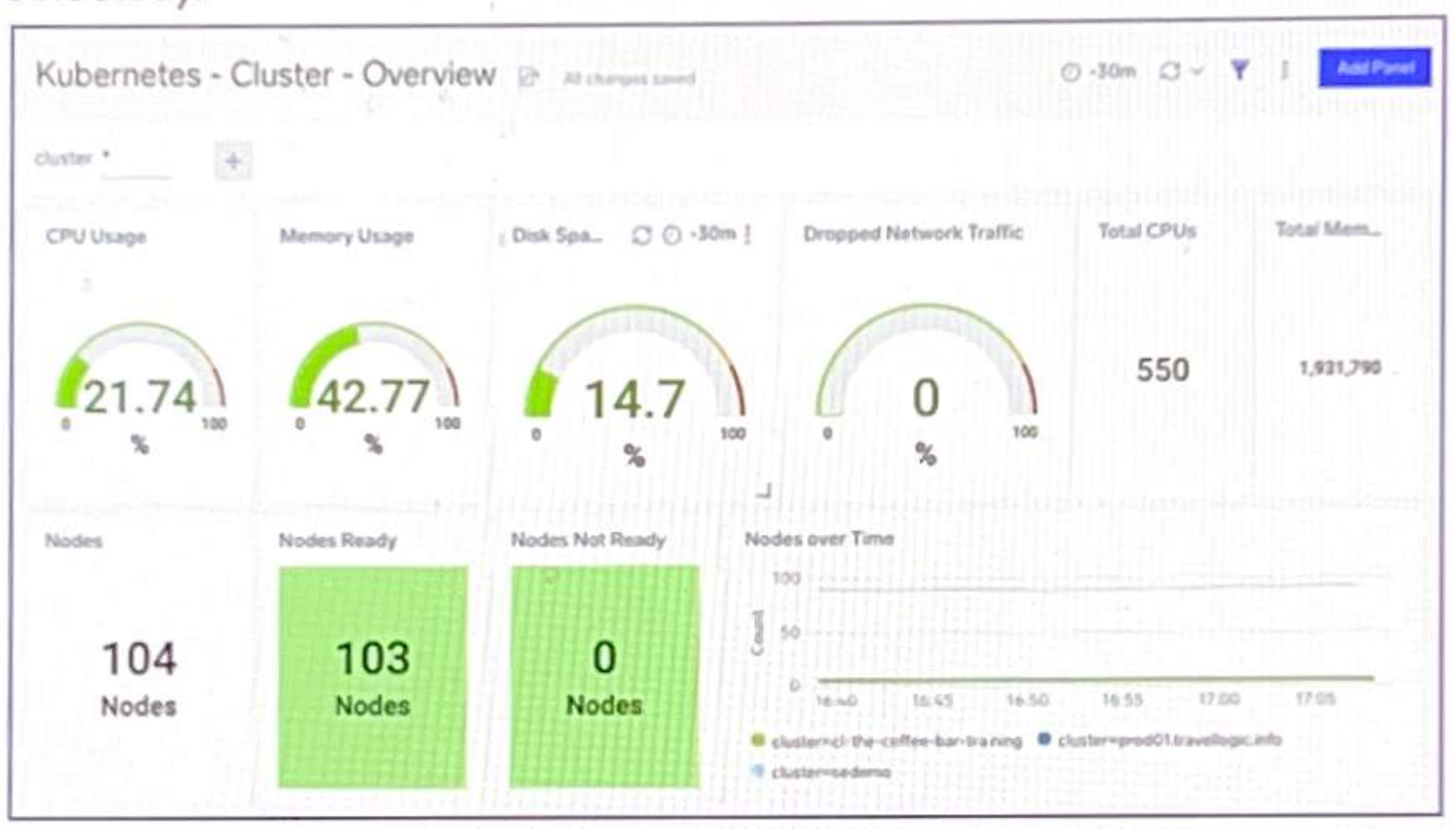
1. In the left navigation menu, click **App Catalog**.
2. In the main window, in the **Classic Apps** section, find and click the **Kubernetes** app icon. (You can find it easier by doing a search for "kubernetes" using the search bar or clicking the "Kubernetes" category checkbox on the left.)



3. Since the Kubernetes app is already installed in the training environment, finding the app in the App Catalog will display an **Explore Dashboards** button to navigate to the Kubernetes dashboards directly. (If the app is not installed in your environment you would see an install button instead). Click the **Explore Dashboards** button.
4. Select **prod** from the left menu. You should see the selected dashboard populate with data.
5. On the top of the dashboard panel to the right, there are several preconfigured dashboards to choose from. Select **Kubernetes - Cluster - Overview** (if not already

©2024 Sumo Logic, All Rights Reserved.

selected).



The dashboard will update to show only this cluster's data, rather than all the Kubernetes clusters you've ingested into Sumo Logic.

Take some time to scroll through this dashboard and look at some of the data. See if you can use this dashboard to answer these questions:

- How many nodes aren't running?
- How many pods aren't running?
- What percentage of the cluster's disk space has been used?

The answers to these questions may vary, since Kubernetes is ephemeral and always changing. Exploring these training dashboards with a curious and open mind familiarize you with them, and prepare you to monitor and troubleshoot your own clusters.

©2024 Sumo Logic, All Rights Reserved.

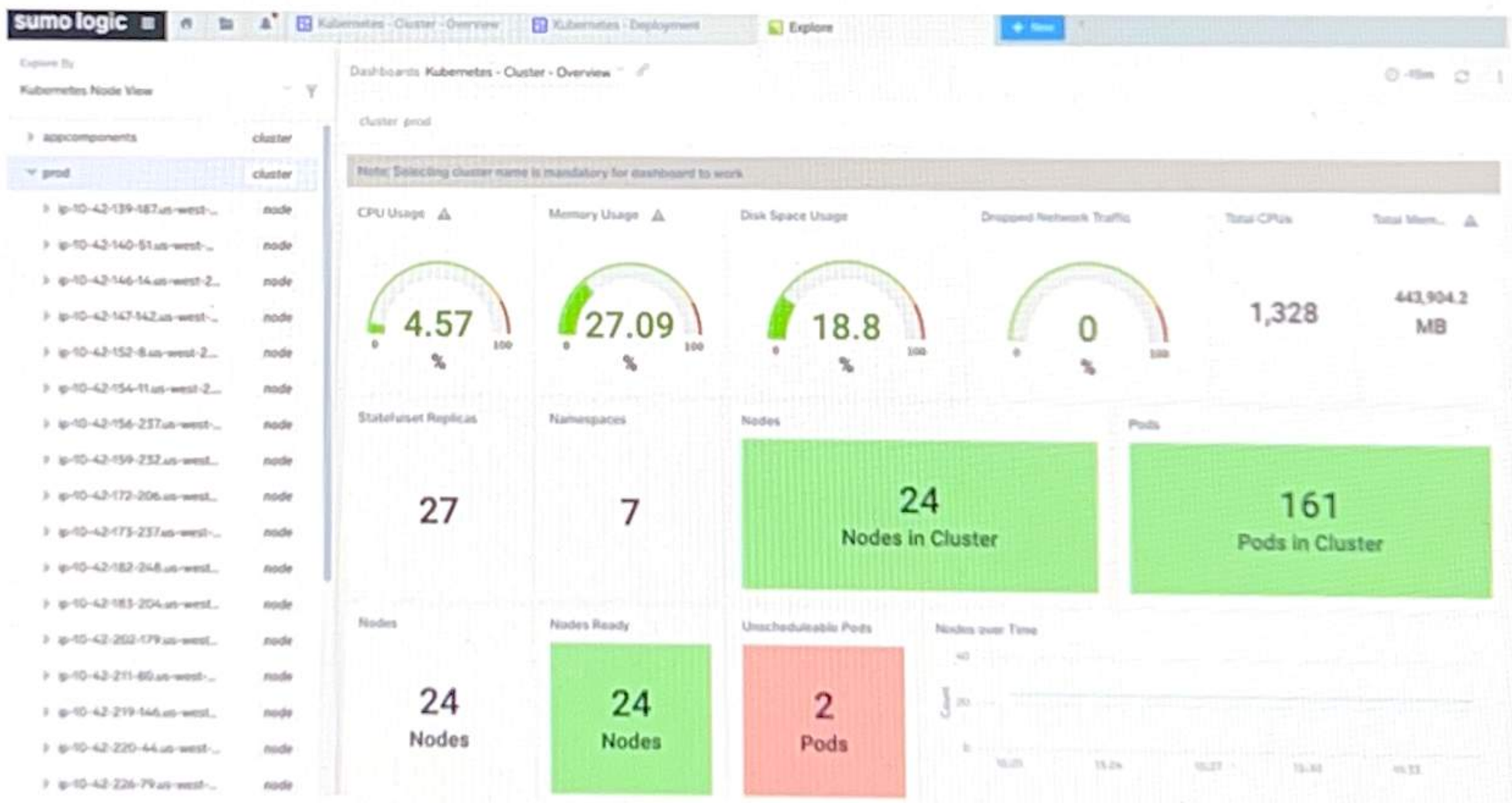
sumo logic

Lab 3: Navigate a Kubernetes cluster

In this lab, we'll use the Kubernetes Observability view to help navigate a Kubernetes hierarchy.

Navigate to the Sumo Logic UI if you're not already there. Refer to Lab 0 if you need help.

1. In the left nav menu, click **Observability > Kubernetes**..
2. In the right pane, at the top, select **Kubernetes Node View**.
3. Click the expand arrow next to the **prod** cluster to reveal the nodes inside the cluster.
4. Click the expand arrow next to one of the nodes to reveal the pods inside the node.
5. Click the expand arrow next to one of the pods to reveal the containers inside the pods.
6. Select one of the containers you revealed.



Because Kubernetes is ephemeral, the container names may vary from instance to instance. Selecting any container should work for this activity.

Help! There's no data!

You might see an error that says "No Data to Display!" in your dashboard, like this:

©2024 Sumo Logic, All Rights Reserved.

sumo logic

CrashLoopBackOff? -6h

No Data to Display

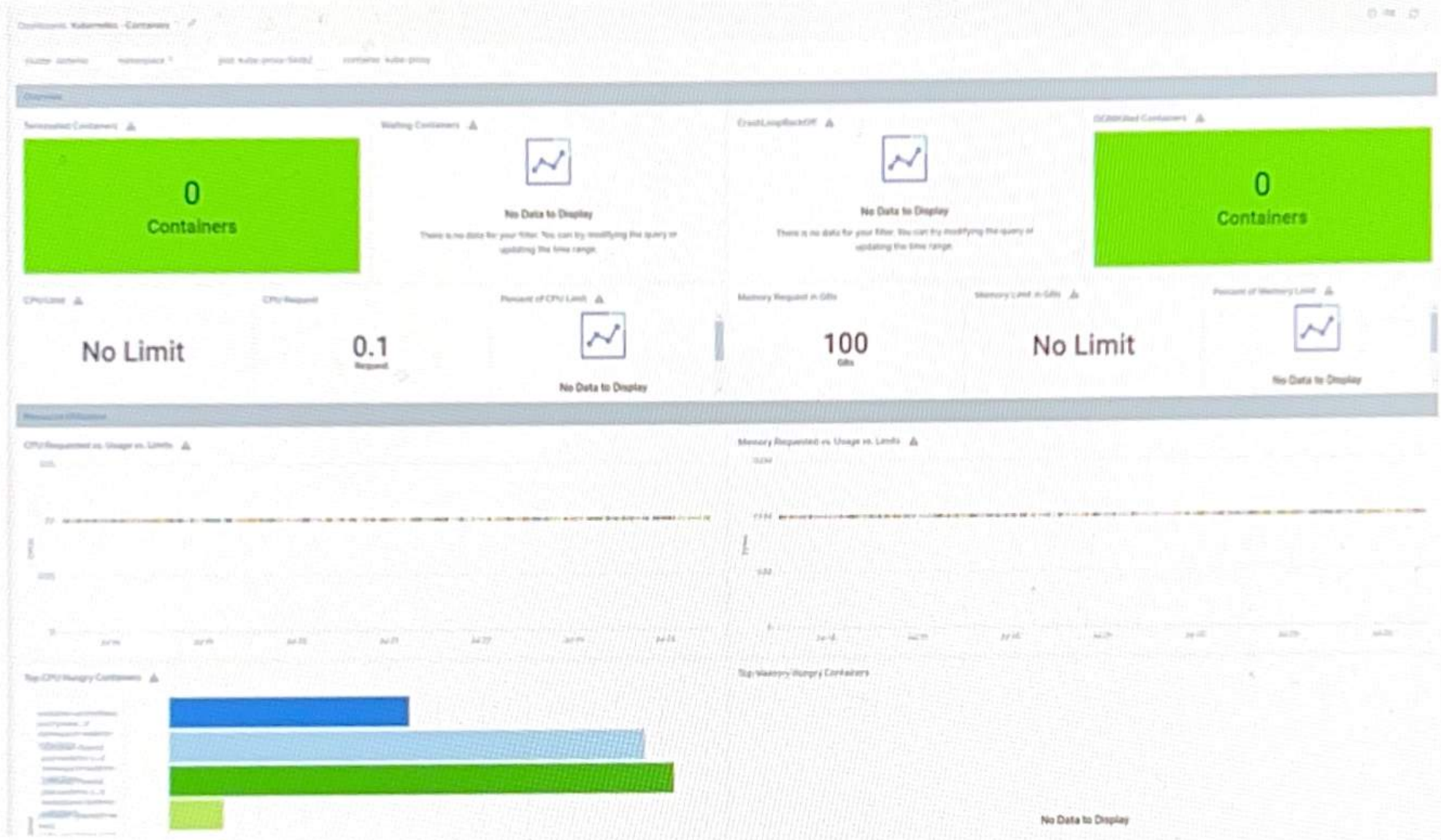
There is no data for your filter. You can try modifying the query or updating the time range.

This isn't necessarily bad! This just means there isn't any data for this category for the time period selected. You can try exploring a different pod or container. Or you can adjust the time period displayed by the dashboard widget – a larger time period means a larger scope to find relevant data to display.

In the top right of each dashboard panel, you might see **-15m** next to the clock icon. That means the dashboard is only displaying the last 15 minutes of data, which is the default. Try selecting **Last 7 days** or **Last 24 hours** next to the clock icon. Experiment to see if longer time periods show some data for those "empty" dashboard sections.

7. In the right pane at top, select **Dashboards > Kubernetes - Containers**. This will bring up a dashboard that shows detailed information like resource utilization about the container you selected.

©2024 Sumo Logic, All Rights Reserved.



In this example, we can see no containers have errors. Your data may vary.

Great! Now you've dug into a Kubernetes hierarchy using the Sumo Logic UI!

©2024 Sumo Logic, All Rights Reserved.

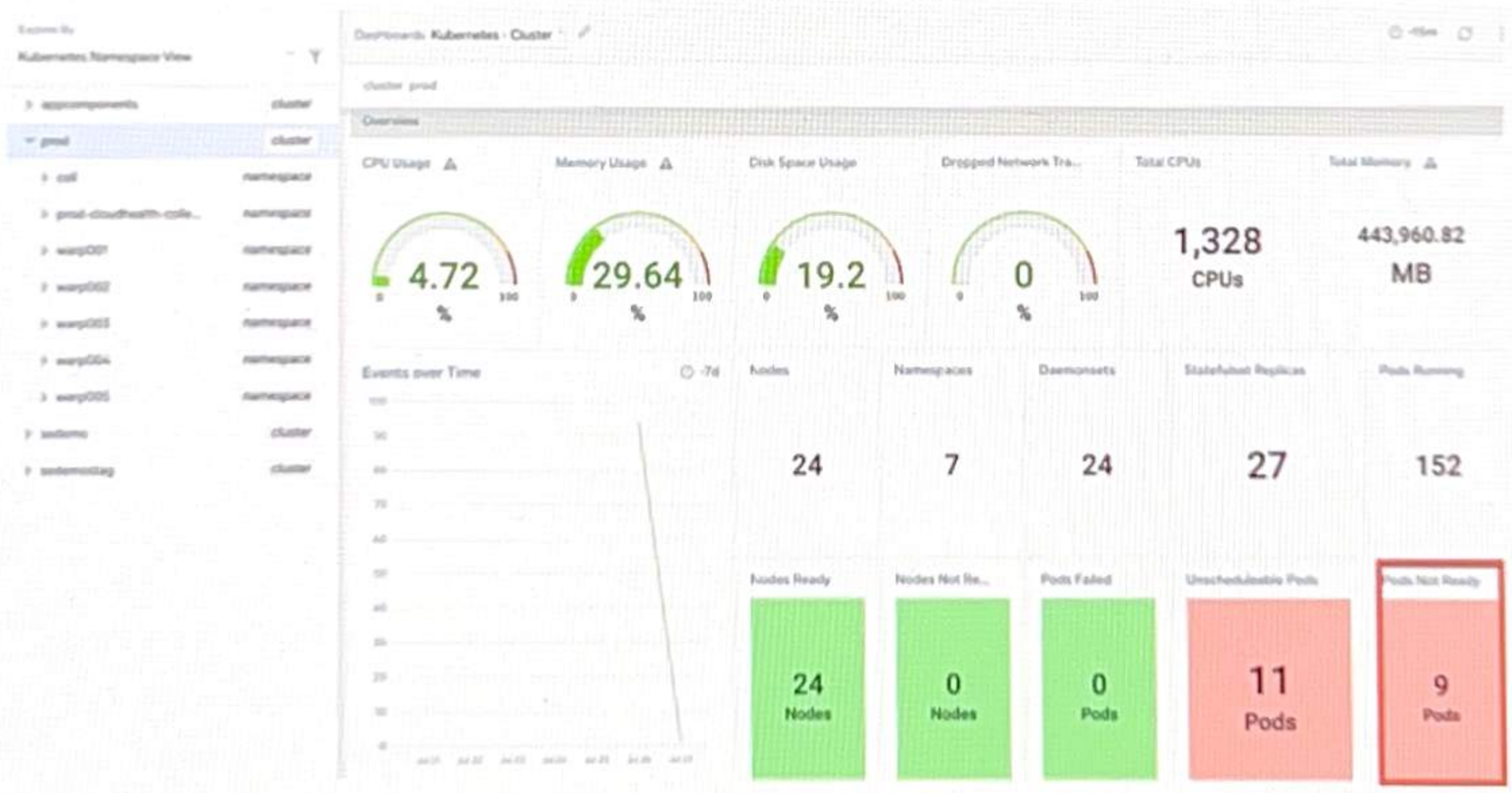
sumo logic

Lab 4: Create a metrics alert

While using Kubernetes to provide your application services, you've become worried about pod failure. Rather than check your dashboards daily, you decide you want an email sent to you if more than 10 pods have been down for over an hour.

Navigate to the Sumo Logic UI if you're not already there. Refer to Lab 0 if you need help.

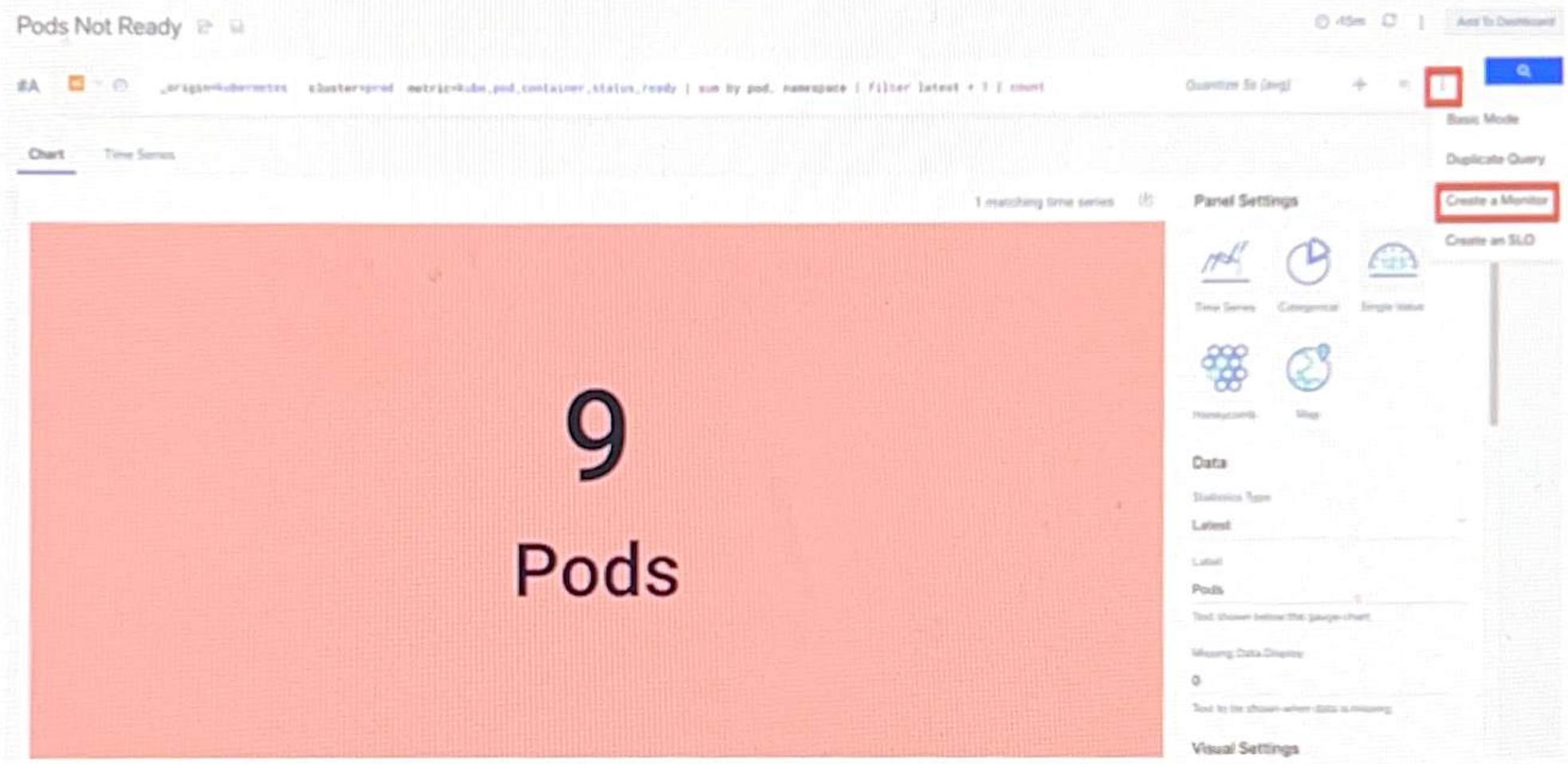
1. In the Kubernetes dashboard view, select the **prod** cluster in the left navigation pane
2. In the right pane, select the **Kubernetes - Cluster** dashboard.
3. Find the "Pods Not Ready" panel (typically in the lower right corner)



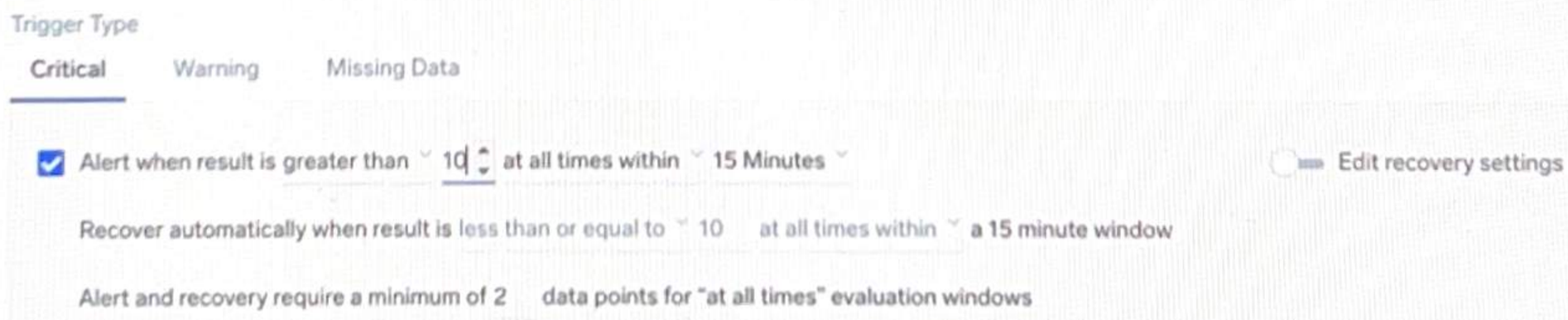
4. When you mouse over that panel, you'll see a button with three vertical dots (known as the "More Actions" icon). Click this and select **Metrics > Open in Metrics** to open the query that creates the data behind this dashboard panel in metric explorer.

©2024 Sumo Logic, All Rights Reserved.

5. To the right of the metric query, click on the **More Actions** (triple dot) icon again, and select **Create a Monitor**.



6. You will be taken to a new monitor page where you can modify the various monitor settings (some settings like Monitor Type, Query, and Alert Grouping have already been set for you).
7. Scroll down to **Trigger Type** to set the thresholds for your alert. Under **Critical**, select **greater than 10 and at any time within 15 minutes**.



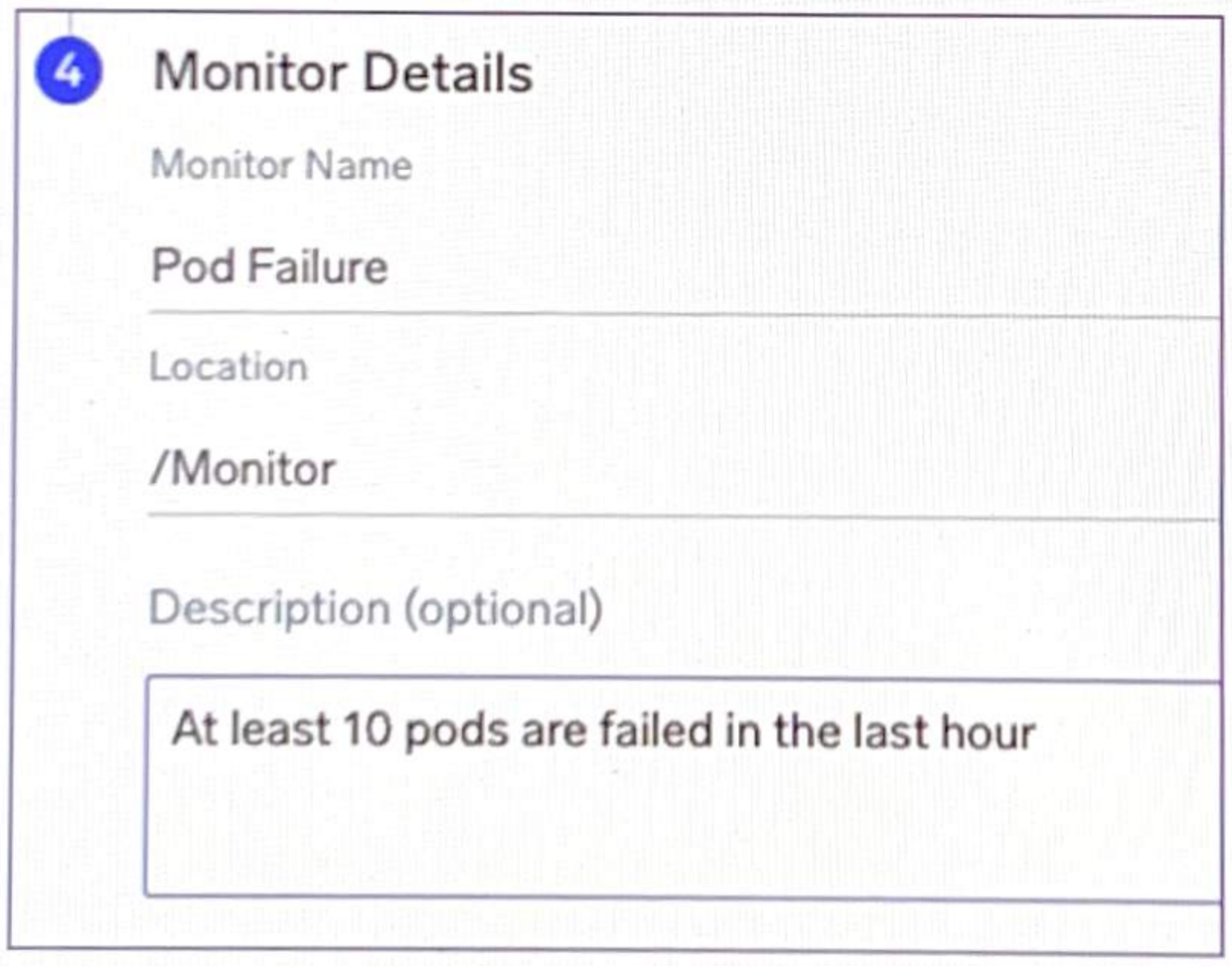
8. On the **Warning** tab, check the box and set it to **greater than 7 within 15 minutes**.
9. On the **Missing Data** tab, check the box and set the value for **5 minutes**.
10. Skip **Advanced Settings** for now.
11. Under **Notifications**, select **Email**, then enter a valid email address. You can use your training+analyst####@sumologic.com address. Make sure you check at least one

©2024 Sumo Logic, All Rights Reserved.

sumo logic

notification type, such as **Critical Alert**.

12. Give your alert a **Monitor Name** and **Monitor Description**. This way, people will know what to do if your alert is triggered.



13. When you're done, click **Save** near the top of the page.

Congratulations! You've set up a custom Kubernetes alert based on a dashboard panel!

©2024 Sumo Logic, All Rights Reserved.

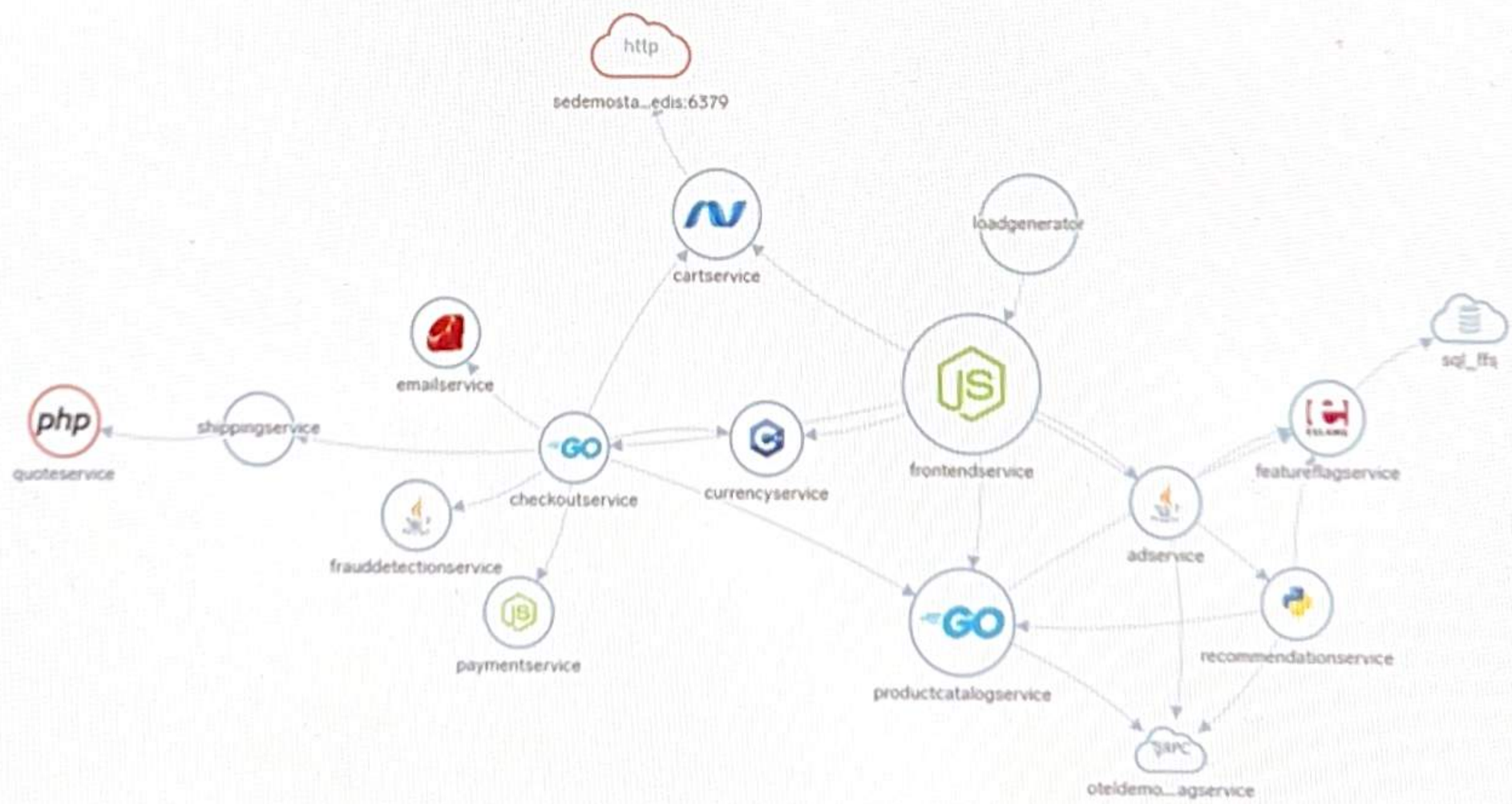
sumo logic

Lab 5: Troubleshoot with Traces and the Service Map

Traces help you see the time between one log and another, so you can see the path of information as it goes down the pipeline of an application. You can use traces to drill down and find the source of a bottleneck and the true root cause of a problem.

Navigate to the Sumo Logic UI, if you're not already there. Refer to Lab 0 if you need help.

1. In the left nav menu, click **Observability > Services**.
2. In the top right of the Services view, select **Map**
3. For **Application Name**, select the entry that starts with **otel-app-sedemo**.

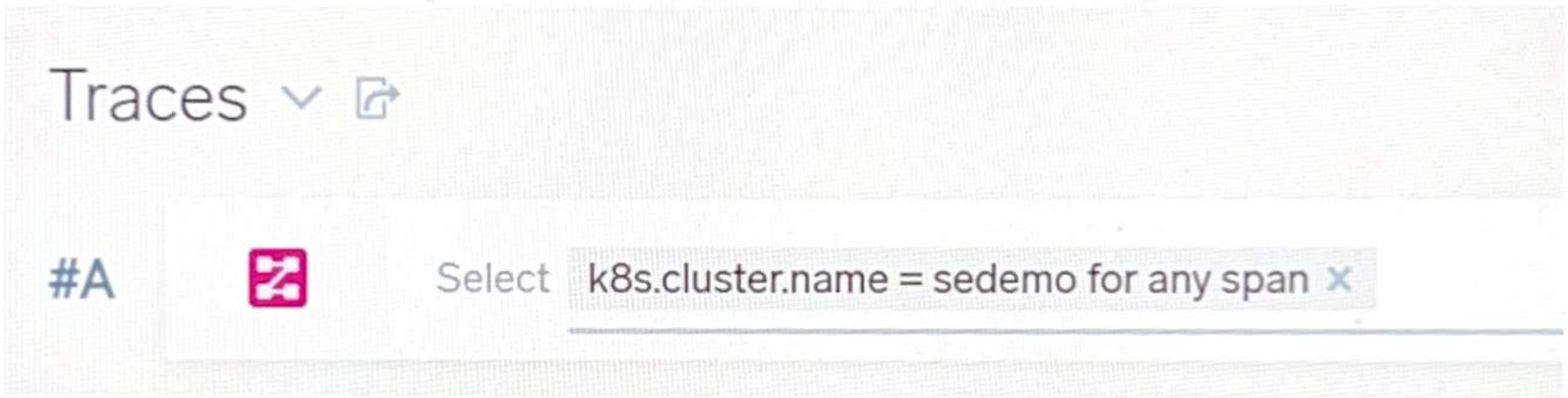


Here you can visualize all the services used in this application. You can scroll or use the magnifying glass icons to zoom in on the different services. You can see how all the services are connected and dependent on each other. You can hover over each service to learn more about them.

4. Any services outlined in red indicate that there are anomalies. Select a service in red and click on it to open the right sidebar with more information about that service.

©2024 Sumo Logic, All Rights Reserved.

5. The sidebar view has an "Open In" button to dive into the log search again for logs related to that service. We can use this to move automatically into the "Traces" view.
6. Click **Open In > Traces.** (Alternately, in the left nav menu, you can click **Observability > Transaction Traces**.)
7. If you came here from the Service Map, the "Select" field will already be populated based on the service chosen. If you came here from the left nav menu, next to **Select**, start typing **k8s.cluster.name=sedemo for any span** and select it from the dropdown.



8. Click the **Duration** column to sort the results by duration from high-to-low.

The exact durations and number of errors you'll see may vary, since Kubernetes is ephemeral and always changing. You may notice that the traces with longer durations also tend to have more errors. While some errors and some latency is expected with any application, we don't want your ecommerce customers to wait too long.

9. Click a trace that has one or more errors. (You can go back to the Service Map and select another service outlined in red if you want a different dataset. You can also click on the "Number of Errors" column to sort by error number.)
10. Enable **Error Spans Only** to show only the spans that have errors in this trace.

©2024 Sumo Logic, All Rights Reserved.

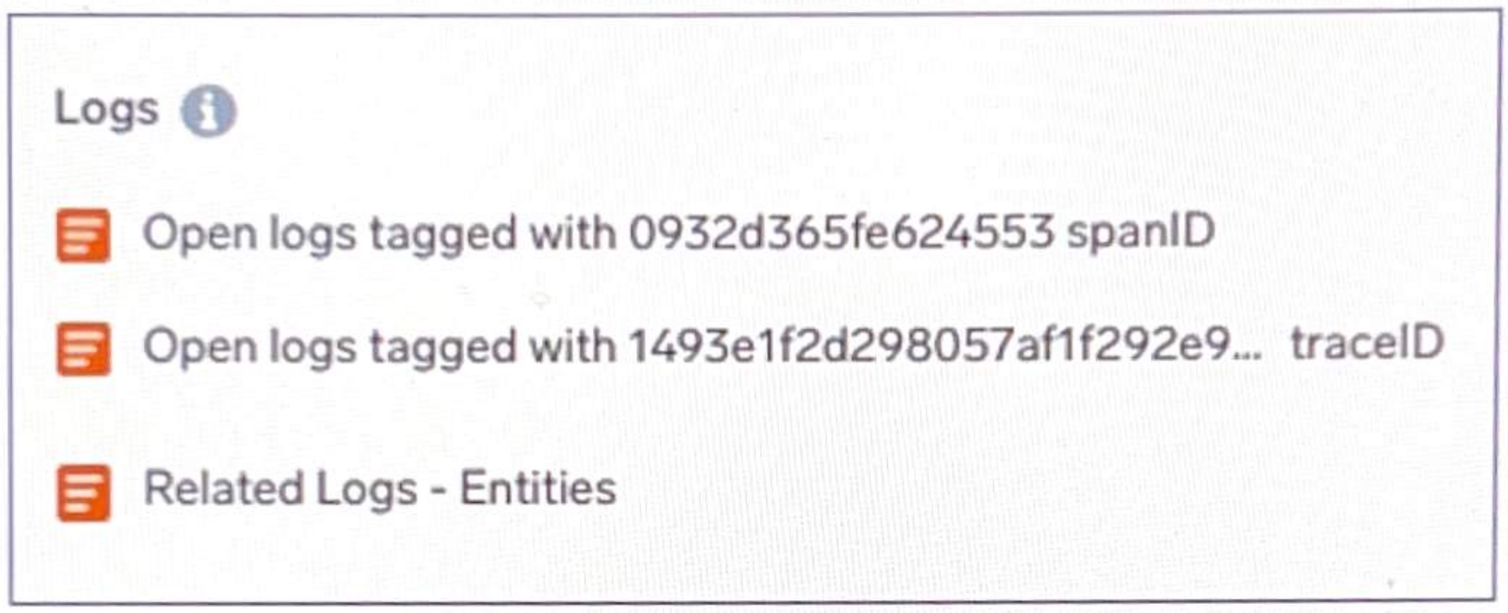
11. Use the **magnifying glasses** to zoom in until you can find the root cause of the bottleneck. You can also use the scroll function on your mouse or track pad to zoom in or out.

The service with an error you find may vary from instance to instance depending on the trace you selected.

12. Click the service with the error. This will open up the right sidebar with more info.

©2024 Sumo Logic, All Rights Reserved.

13. In the right pane, click **Open logs tagged with... span ID**.



A new log search tab will open. Here, we'll see any logs related to the selected span. By narrowing down the logs based on span, we should have a reasonable number of log entries to parse through to find the root cause of our errors.

©2024 Sumo Logic, All Rights Reserved.