sumo logic

Sumo Logic Fundamentals

Student Lab Guide

sumo logic

Disclaimer

This course material is Sumo Logic, Inc. confidential information. Sumo Logic, Inc. provides it as-is solely for your use and assessment as an individual partaking in the training and certification program on our Learning Portal and in specified other venues. The course material may not be reproduced, sold, or otherwise processed or transferred in any other way or for any other purpose without prior written permission from Sumo Logic. Sumo Logic owns the copyright and other intellectual property rights in the text, graphics, information, designs, data, and other content on this website (including exam materials and certifications as well as audio files and their scripts) with the exception of our partners', licensors', and other third parties' trademarks and other intellectual property. United States export control laws and regulations apply to this material, and you agree to comply with such laws and regulations.

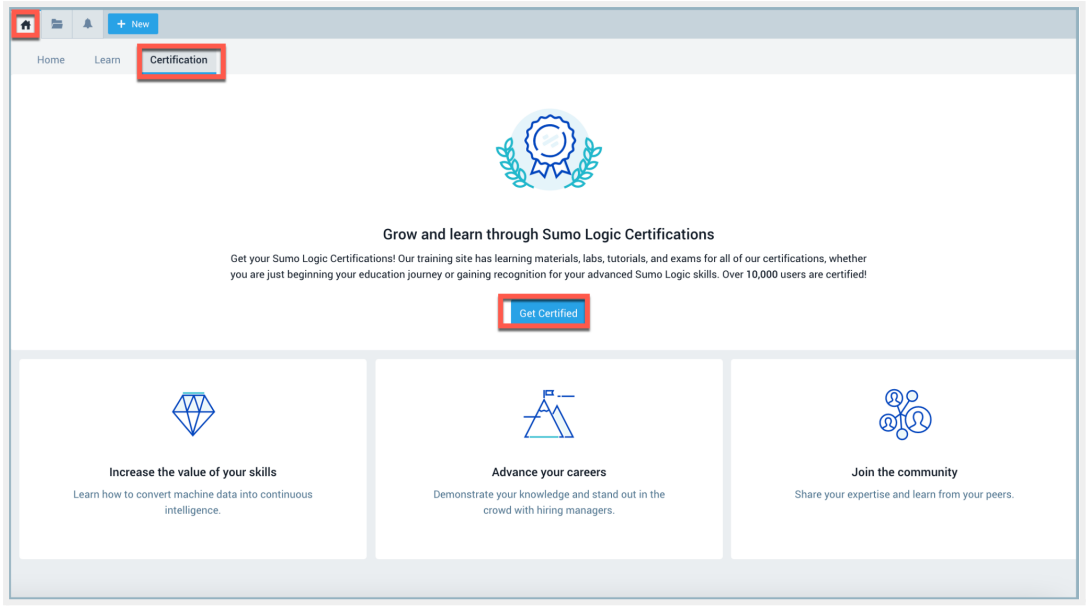
Lab 0: Log in to the training environment

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

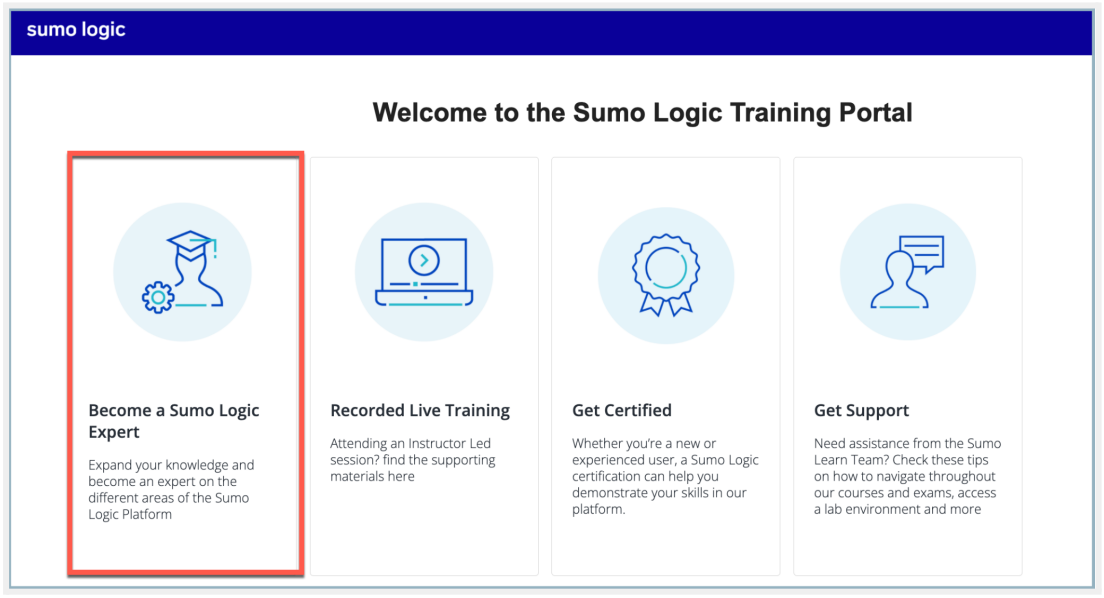
1. Open a new browser tab.
2. Go to https://service.sumologic.com.
3. Enter **training+analyst###@sumologic.com** in the **Email** field. Replace ### with a three digit number between 001 and 999.
4. Enter the **Password** provided to you by your instructor.
   Note: The password changes monthly.
5. URLs can vary based on your setup or your sign-in credentials, so check with your organization's Sumo Administrator. You begin on the **Home** page experience.

For security and compliance reasons we change our passwords every month. Specifically on the first Monday of the month. For this training, you need Analyst account and you can see the password by following the steps below:

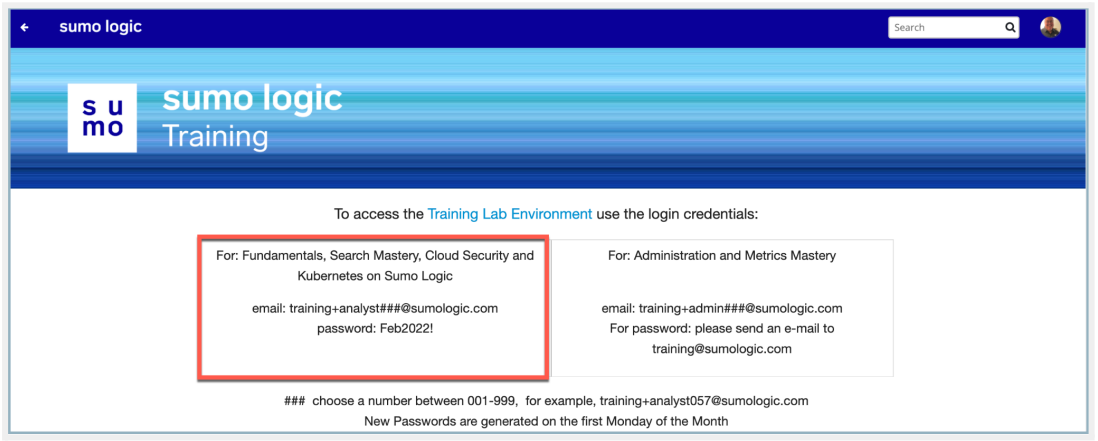
1) In your company's Sumo Logic environment, log in to your Sumo account.
2) Click on the **Home icon**, then the **certification** tab, then the **Get Certified** button:



3) Click on the section - **Become a Sumo Logic Expert**



4) You will then see the current password,



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.

Happy learning!!!

sumo logic

Lab 1: Data Collection

For this lab, we'll show you how to identify a collector, source, and metadata already set up in the environment.

Explore the data collected using Sumo Logic UI

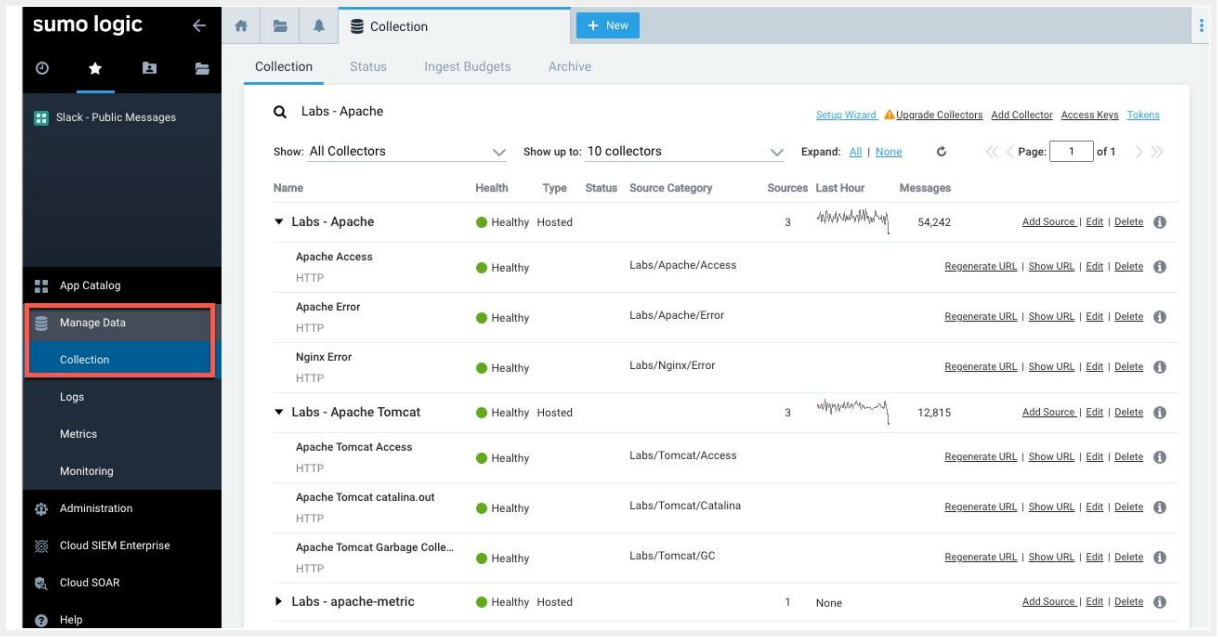
So as an Analyst, how do you know the data is ingested in the Sumo Logic app?
You need to use the **Collection** page to view all of your data, Collectors and Sources, metadata, and so on.

In this lab, you will learn to:

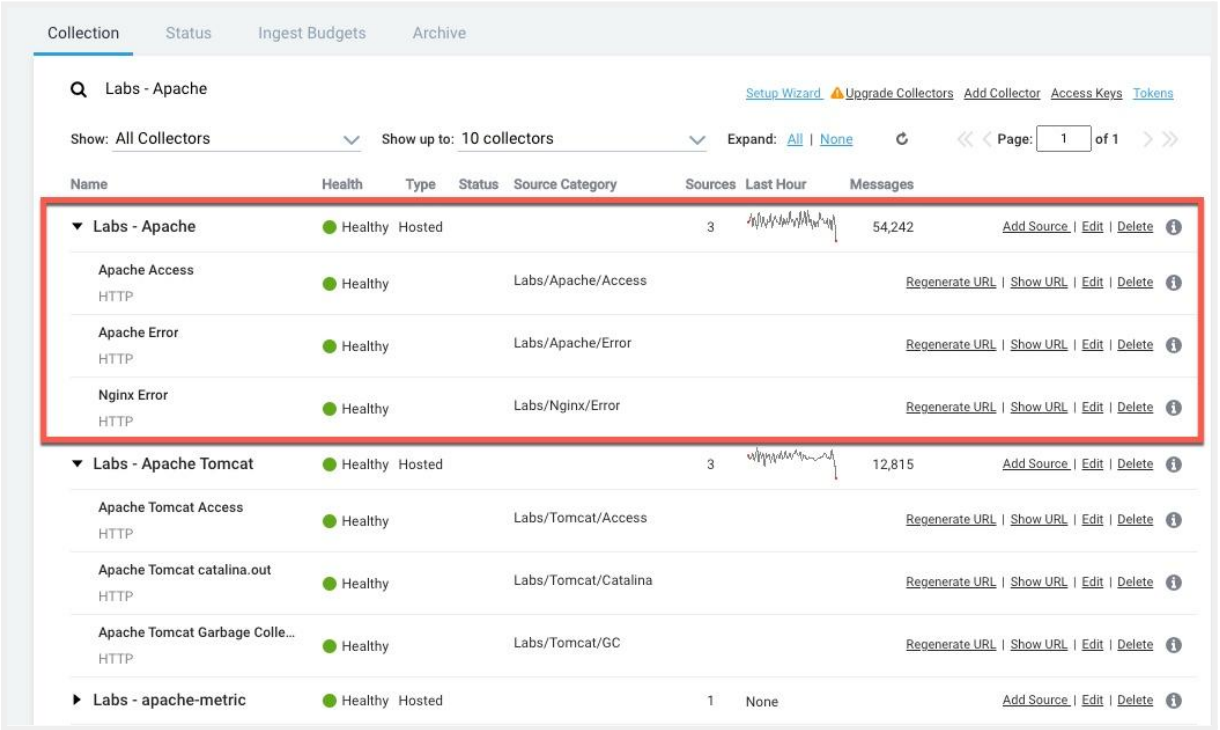
- Navigate to Manage Data > Collection page
- Identify metadata available
- Identify collectors
- Identify sources

To see what data is available to you:

1. From the left navigation pane, select **Manage Data > Collection** to access the collection page.



2. On the top, you see a search field. This allows you to search for collectors and sources by name or sourceCategory using complete keywords.
    a. To match partial keywords use a wildcard. For example, use "**Labs***".
3. For this lab, enter a complete keyword in the search field '**Labs - Apache**', and click **Search** or press Enter.
4. Expand the arrow to view details like collector name, health, status, sources, source category and so on.



5. Now, let's see what each column indicates.
    a. The **Labs - apache** collector is healthy.
        i. The **Health** of your collector is color-coded healthy.
        The column shows error, and warning states for Collectors and Sources so you can quickly determine the health of your Collectors and Sources.

    b. The type of collector is **Hosted**.
        i. You can see the **Type** here, whether the Collector is an Installed or Hosted Collector.
    c. It has 3 sources configured.
        i. From the **Status**, you get an idea of the status of Sources manually paused by users.
        ii. **Sources** column, you can see the number of Sources configured under a Collector.

    d. SourceCategory is set up as **labs/apache/access.**
        i. **Source Category** column displays the name of the configured Source Category for this Collector or Source.

    e. Shows graph
        i. **Last Hour** displays a graph of the total number of log messages ingested per minute over the past hour.

   f. 10 log messages received
      i. And the last column named **Messages**, you can view the total number of log messages ingested over the past hour.

In addition to the **Search** field, you have a couple of drop-down selections to further filter your results.

6. Can you adjust the columns displayed? ____
7. How many sources are added for each collector? ____
8. Do you see the source category set up for each Source?
9. Click the **Show** drop-down arrow? Which options do you see?
   a. All,
   b. Installed,
   c. Hosted,
   d. Running, and
   e. Stopped Collectors.
10. Check what happens on clicking the **Show up to** drop-down?
    a. It allows you to filter the number of results displayed.
11. Click **Expand** to expand or collapse the Collector's displayed Sources.

Conclusion:

In this hands-on exercise, you learned how to access the **Collection** page and view the details. You identified the collector, sources, and metadata.

sumo logic

Lab 2: Apache data app Installation

Sumo Logic apps deliver out-of-the-box dashboards, saved searches, and field extraction for popular data sources. They're the best way to start exploring a new data source on your own.

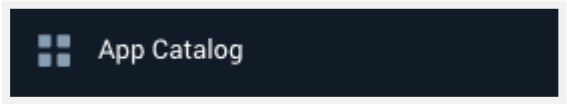
In this lab, you will learn how to:

- Install an app and view content
- Find and display shared content

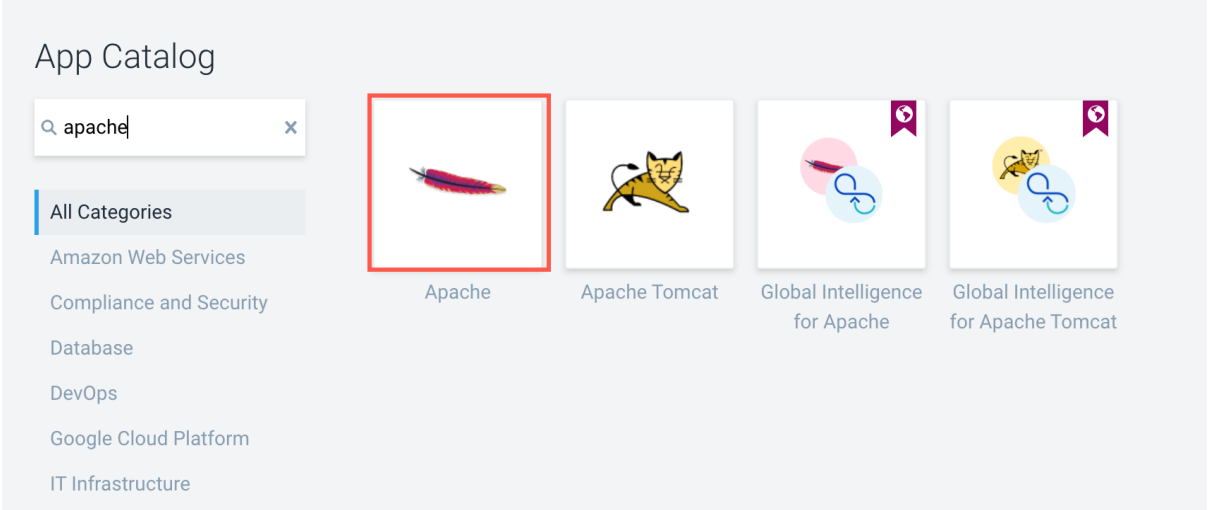
Installing an App and Viewing Content

To install the Apache Access app:

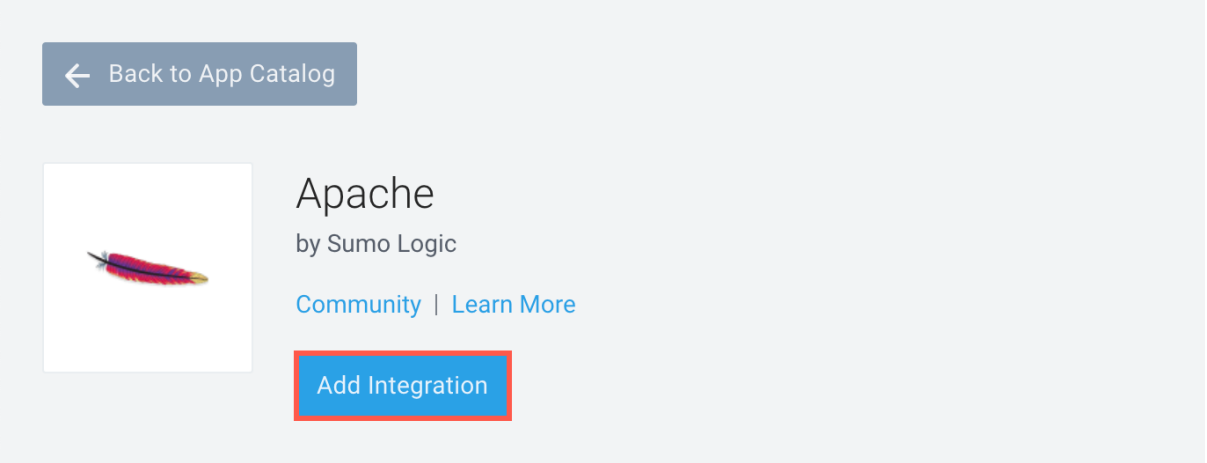
1. Click **App Catalog** in the left nav.



2. Enter **Apache** in the search field, and press Return to show the matching apps.



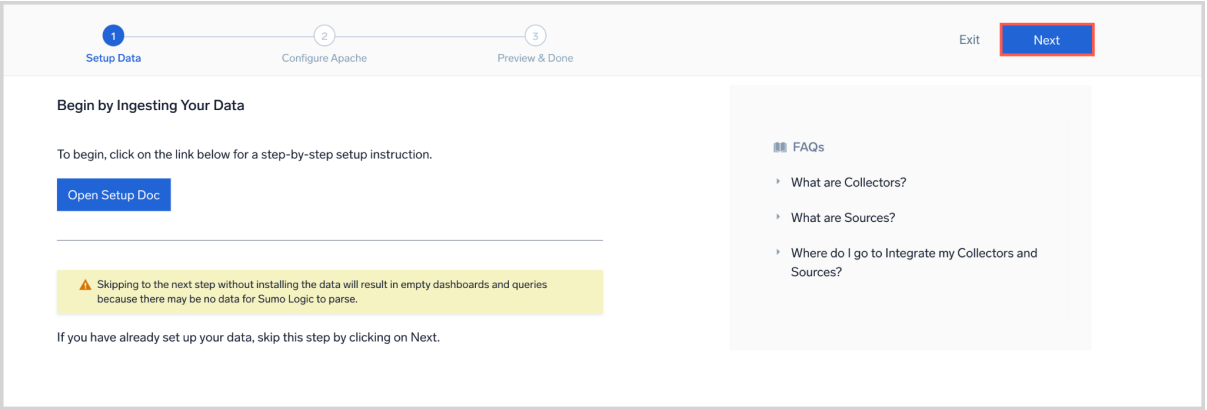
3. Double-click **Apache** to open its app page, and click **Add Integration**.



Clicking this button isn't the final installation. Instead it will launch a window with a few options for the app.

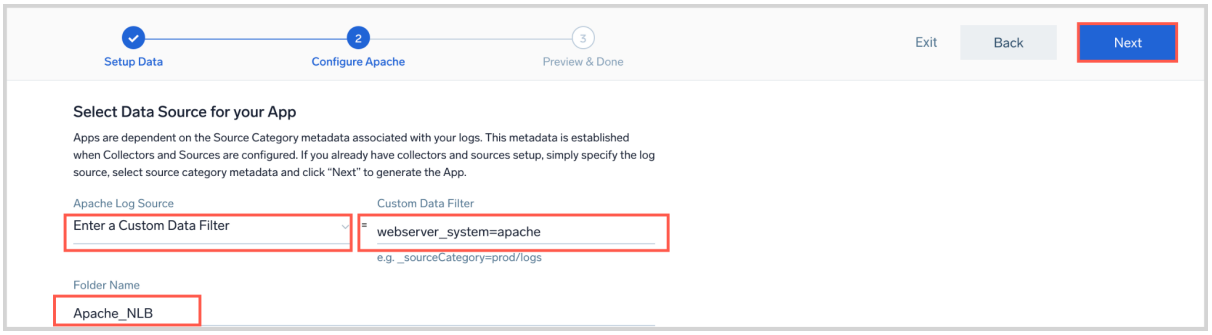
Note: You might see this information message, highlighted in yellow. It is simply pointing out that as an Analyst, you do not have the rights to create a collector. Since the collector already exists in our lab environment, you can complete this lab.

Click **Next**.



1. You can name it something else if you want more than one copy of the app in your personal folder, for example. For now, append your initials to the name **Apache_<your initials>**
2. You can choose a data source or enter a custom data filter. For now, let's choose from our existing data sources.

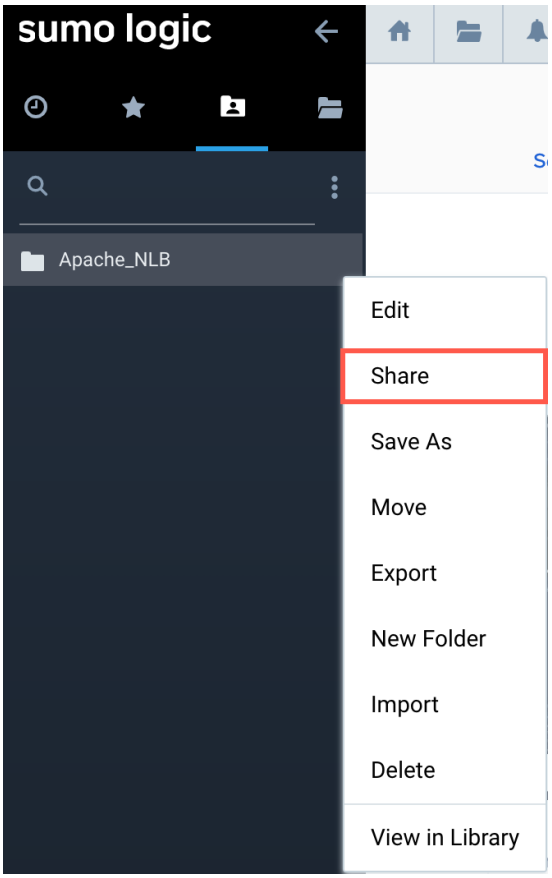
4. For the **Apache Log Source**, Select **Enter a Custom Data Filter** and type **webserver_system=apache**. This assigns a keyvalue pair to pull all apache incoming logs that contain this keyvalue pair.



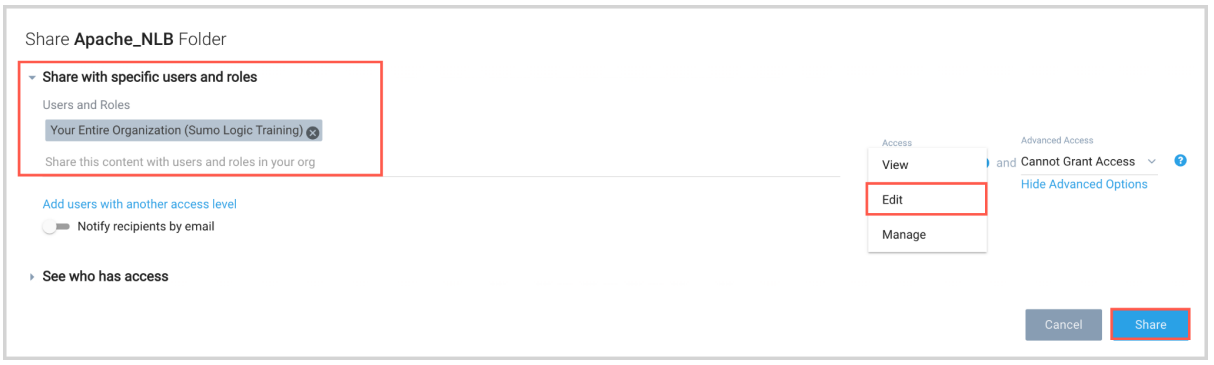
5. Click **Next** in the dialog box to confirm your selection.
   The app is added to the library. Now you can share the app with others in your organization so they can see the dashboards and saved searches for the **Apache Access** app.

6. In the left navigation panel, hover over the **Apache Access** app to display its details pane. Click the **details icon** to see the menu.

7. Select **Share** from the menu.



8. Select Your organization, Access, and then click **Share**.

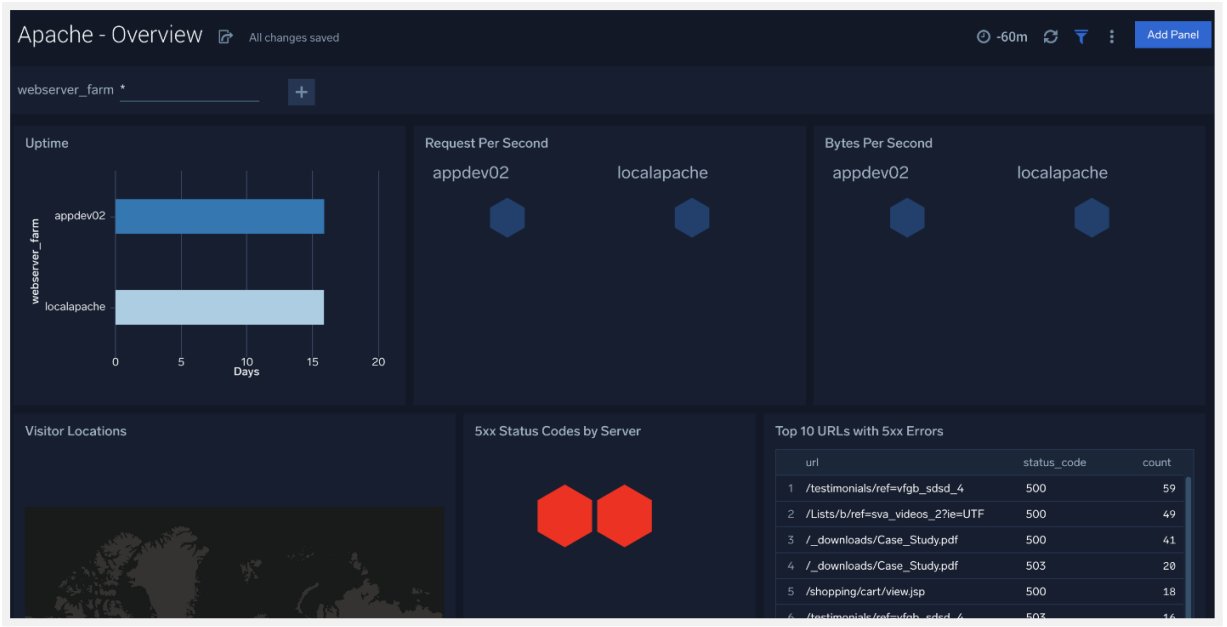


Now others in your organization will see the Apache Access app when they select the Org folder in the library.

9. Now that the app is created and shared, let's see what it contains. Click **Personal** on the left navigation panel or on the **Library** page, and double-click the Apache folder.

sumo logic

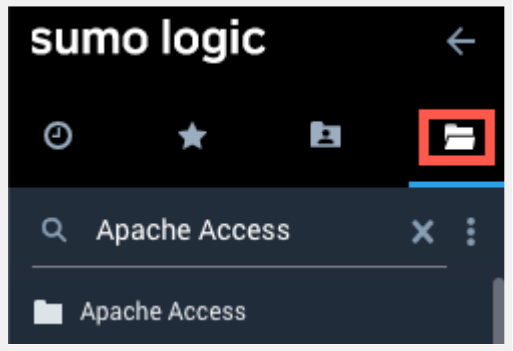
10. The app includes a bunch of predefined saved searches and dashboards. To open a dashboard, scroll down to the **Apache - Overview** dashboard, and double-click to open it. Notice the panels that are already created for you.



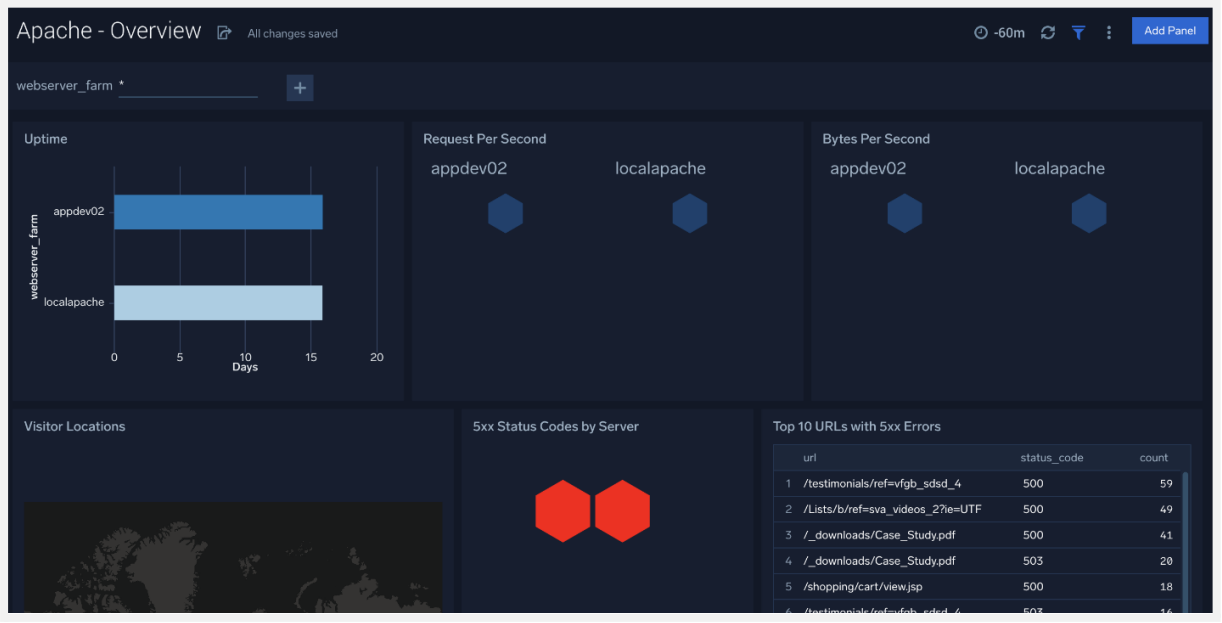
Find and display a shared dashboard

To see whether someone in your organization has shared Apache Access searches or dashboards:

1. Select **Library** from the left navigation menu, enter **Apache Access** in the search field, and press **Return**.



2. The search results include any matching saved searches or dashboards. In this case, the search finds a dashboard that's been shared by someone in your Org.
3. Click **Apache Access** and then click **Apache - Overview** to open the dashboard. The dashboard contains the panels that the owner has set up to monitor Apache Access messages in meaningful ways.



4. If the dashboard contains the information you're looking for, or something close to that, great!
5. In lab 6, you will learn how you can modify dashboards and the associated search queries to tune your results.

sumo logic

Summary

Congratulations! You've completed these tasks:

1. Installed an app, shared it with others, and opened one of the dashboards included in the app.
2. Searched for and viewed a dashboard that's been shared by someone in your organization.

Lab 3: Data Tier Exploration

Now that you know the collector is functional and successfully ingesting data in Sumo Logic, you would like to see how the data is organized. As an Analyst, it is important to know how the data is organized into data tiers, partitions so it helps to search that data easily.

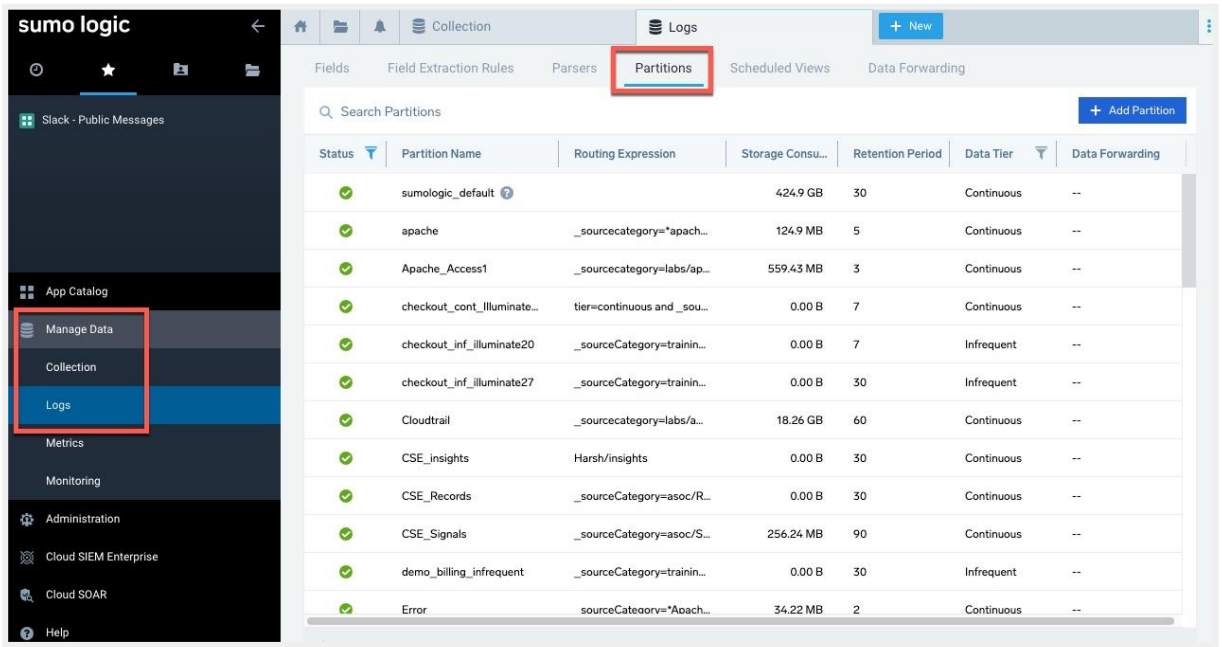
In this lab, you will learn to:

- Navigate to Manage Data > Logs > Partitions page
- Identify partitions
- Identify Data Tiers
- Click +New > Log Search > Basic Mode

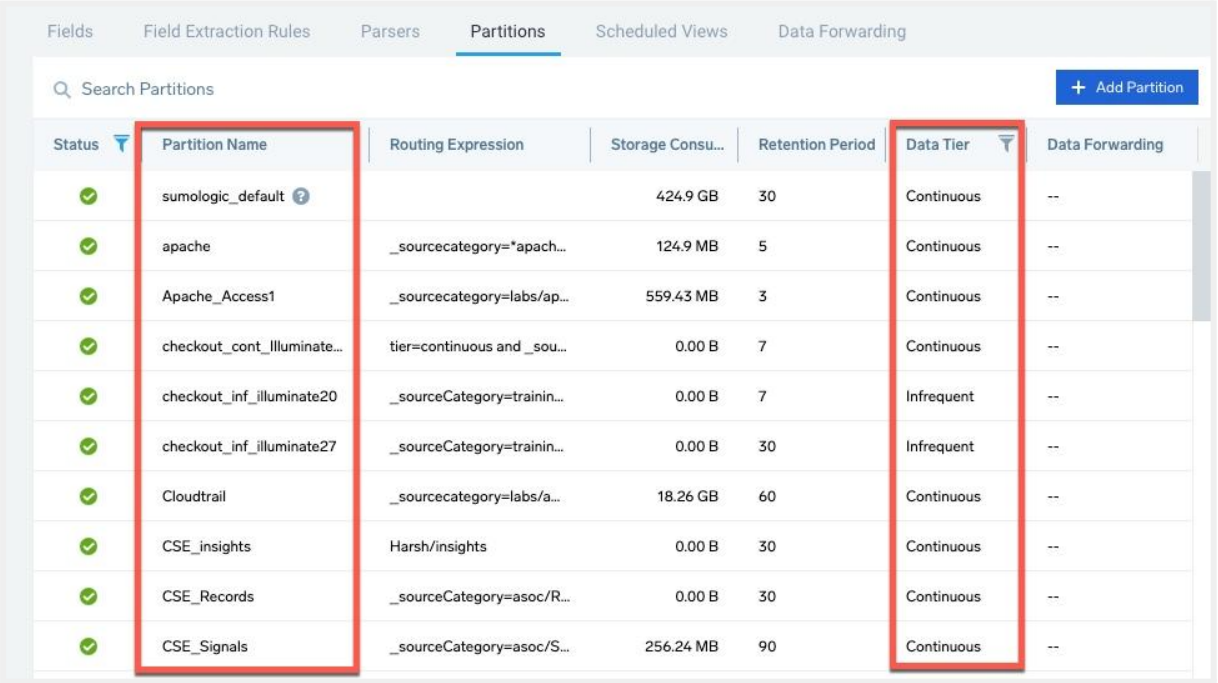
Viewing details about a Partition

Creating a partition allows you to improve search performance by searching over a smaller number of messages. Use the **Partitions** page to view and manage partitions.

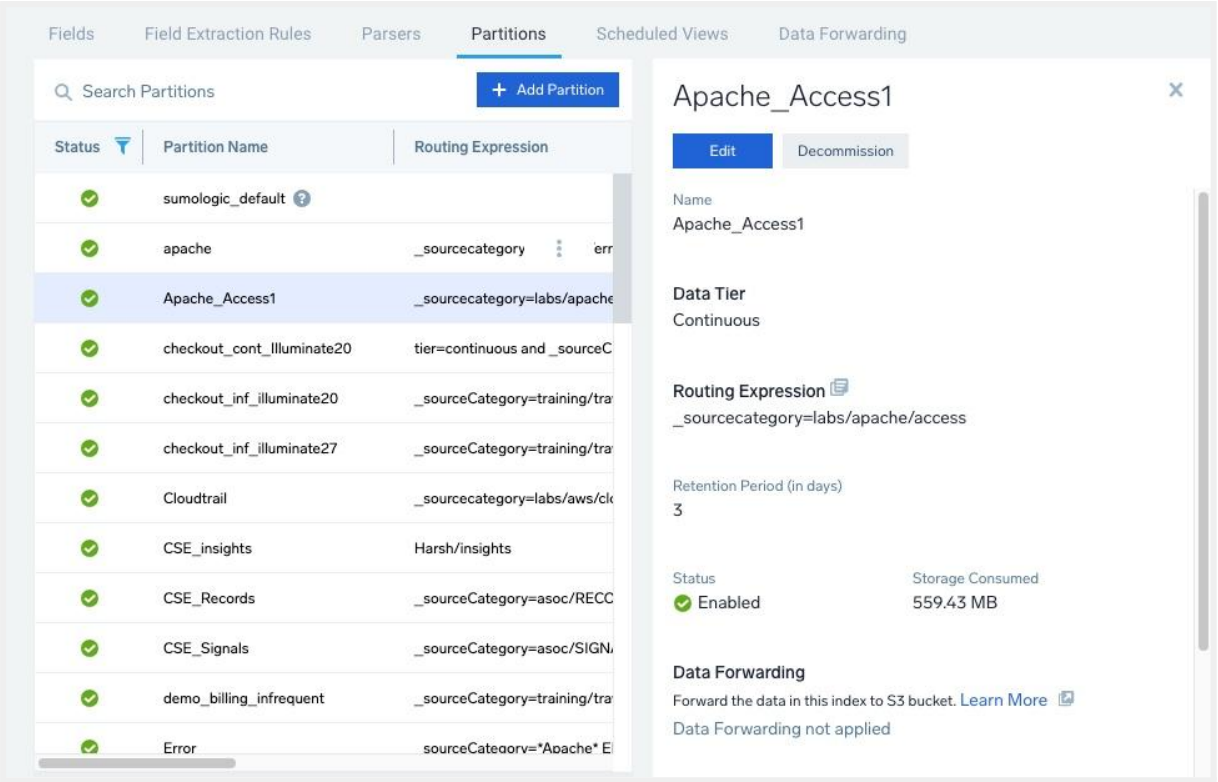
1. To access the **Partitions** page, click **Manage Data > Logs > Partitions.**



2. Review the first column, **Partition Name**. You can review the list of Partitions available in your environment.
3. Review the respective Data Tiers from the column named **Data Tiers**.



4. Click the row for a **Partition** to view its details.

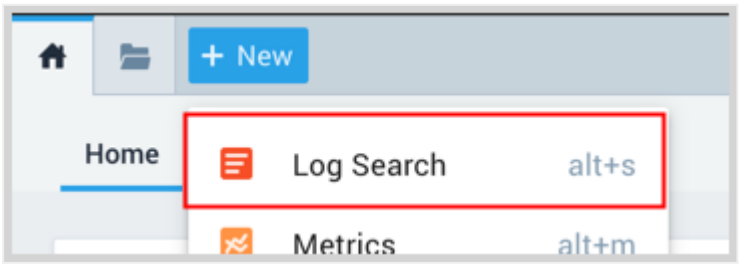


Note that the information displayed for partitions that contain CSE Records varies from

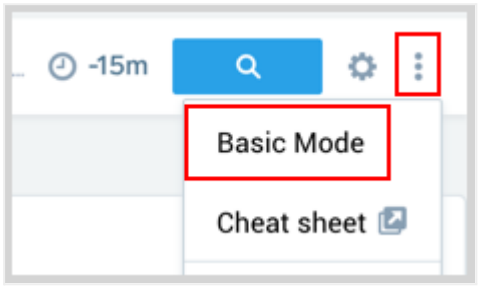
other partitions. You can tell if a partition contains CSE Records from its name: The names of the Sumo Logic partitions that contain CSE Records begin with the string sec_record_.

Searching Log Data using Basic Mode

1. Open a Log Search by clicking **+ New**, then **Log Search**.



2. Click the three-dot icon on the right of the **Search** page and select **Basic Mode**.

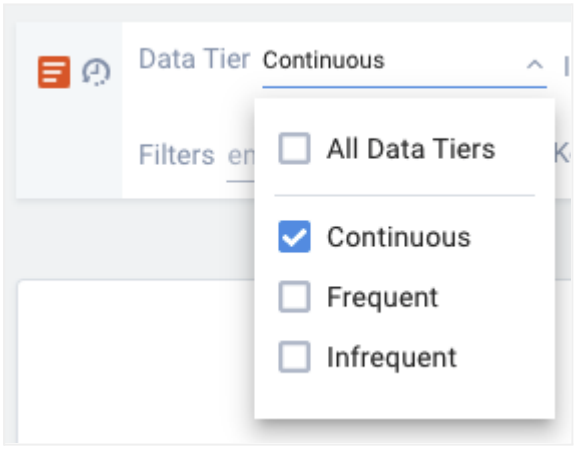


3. The Basic Mode is like a query builder. You can see the input options to build your first query.

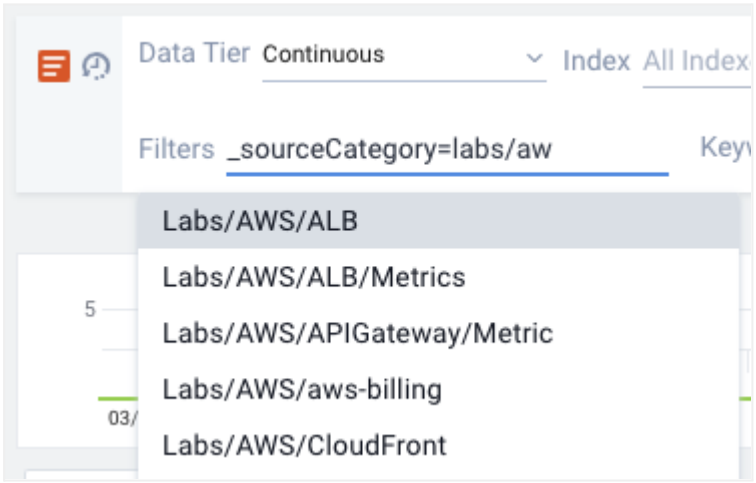
Let's take an example scenario to build your first search using Sumo Logic.

In this lab, we'll investigate a potential ongoing outage on our Amazon Web Services (AWS) Application Load Balancer (ALB).

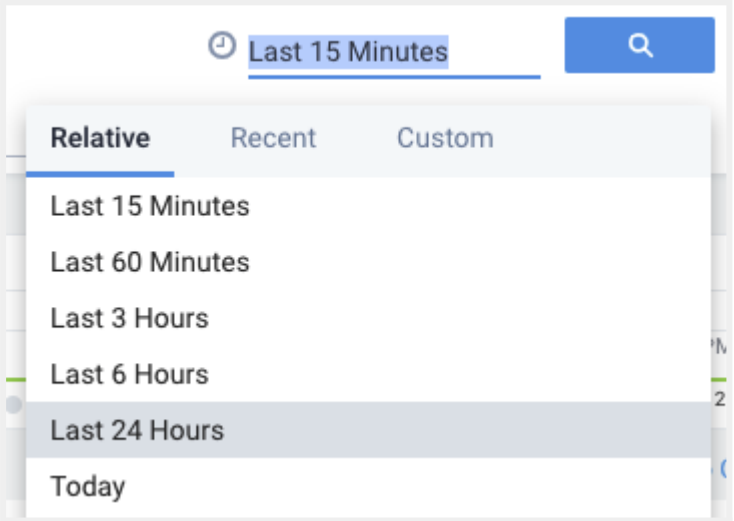
1. For **Data Tier**, select **Continuous**. Live production logs are often kept in the continuous tier. By limiting the tiers we search, our query will run faster and use fewer resources, saving us time and money.



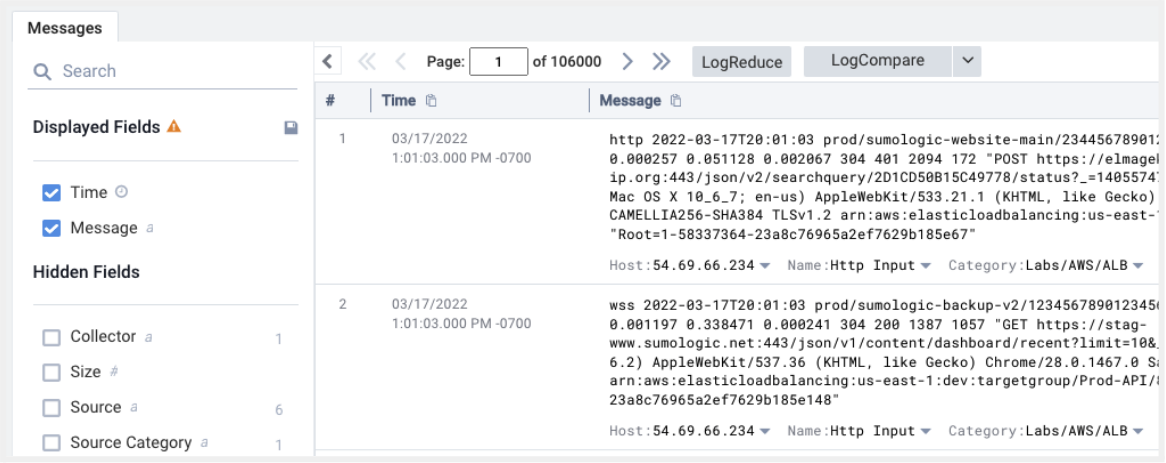
2. For **Filters**, select **_sourceCategory**, then start typing **Labs/AWS/ALB** until you see it in the dropdown menu. This will search all the training lab data from our AWS Application Load Balancer.



3. Next to the **clock icon**, select **Last 24 Hours**.

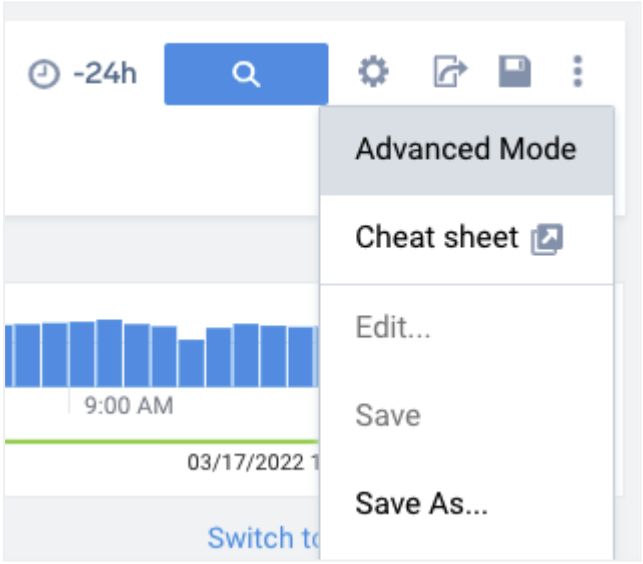


4. Click the **magnifying glass** icon to start the search. Over 100,000 pages of log messages appear. By default, each page contains 25 messages, so this is around 2.5 million logs.

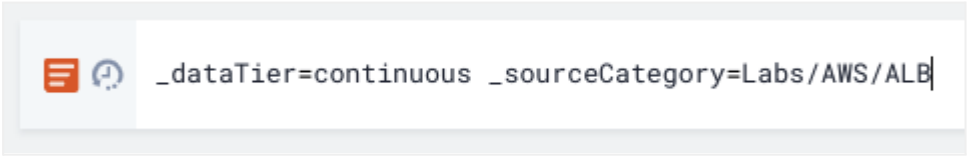


In this example, approx. 106,00 pages appear, though the exact number may vary. There's a lot of information here to start an investigation! We'll sort these and drill down further in the next labs.

5. Click the three dot icon to the right of the query builder, then select **Advanced Mode**.



A traditional SQL-like query is built from your dropdown selections. If you run this query, the same results should return.



Congratulations!

You've built a simple query using Sumo Logic's Basic Mode search, then converted it to an **Advanced Mode** query.

sumo logic

Lab 4: Data Searching

In this lab, we'll show you how to use the Search page to search for, parse, and aggregate log data, and save the results.

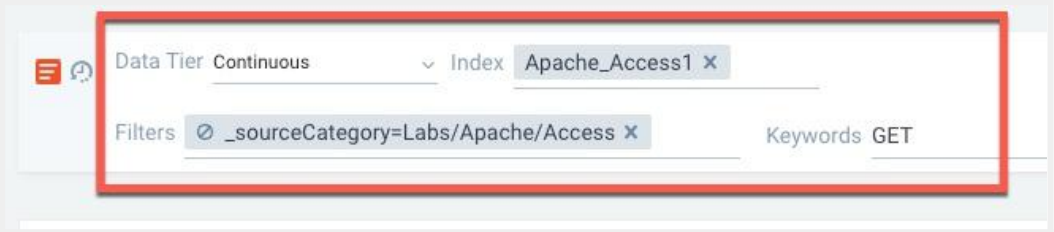
1. Build a query in Basic mode.
2. Parse and aggregate the results.
3. Save the search results.

Build a query in Basic Mode

From lab 1, you know that you have access to Apache Access data. Let's search for log messages within that source category that include the keyword GET.

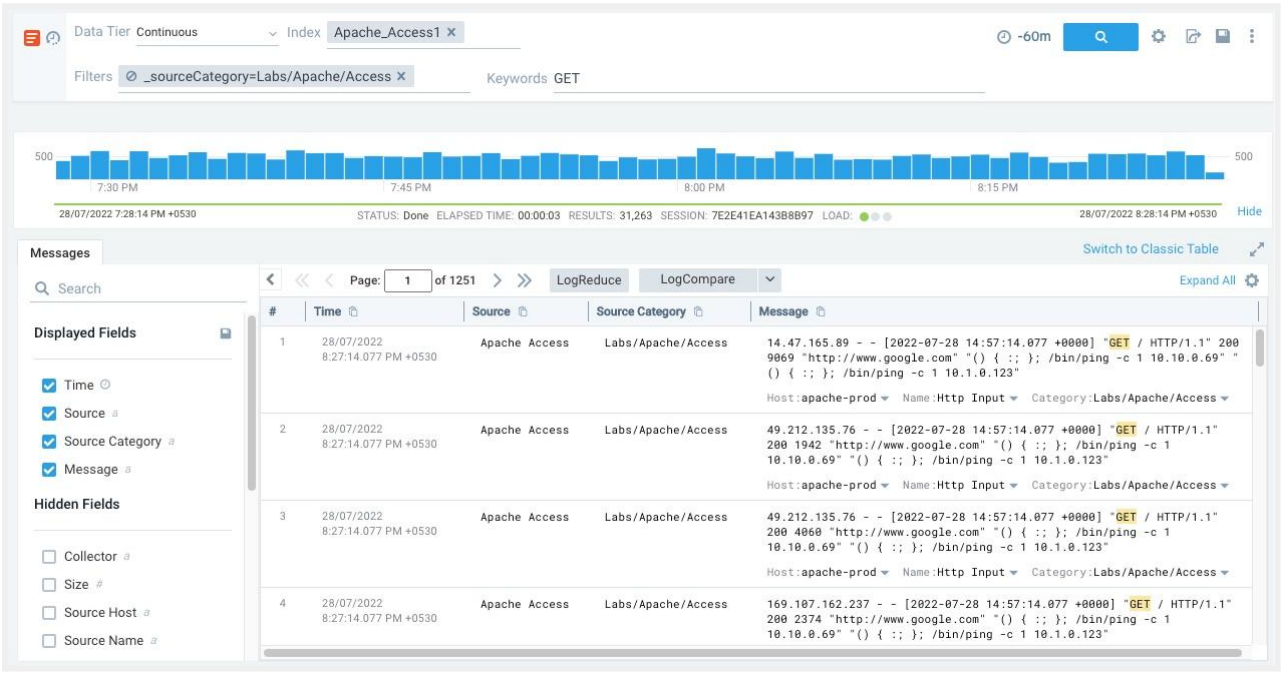
1. If the **Search** page isn't already open, click **+New** on the top tab bar, and select **Log Search**. By default, Advanced Mode opens. You need to switch to Basic Mode.
2. In the query area, select the following:
   Data Tier as **Continuous**
   Index as **Apache_Access1**
   Filters as **_sourceCategory=Labs/Apache/Access**
   keyword as **GET**

   Keep in mind that keywords are not case sensitive.



4. You can select a pre-configured time range from the drop-down menu, enter a relative time range such as -1d to -12h, or enter an absolute time range, such as 3/08/2022 11:00 AM to 3/08/2022 11:00 PM. For our purposes, let's select **Last 60 Minutes** from the drop-down menu.

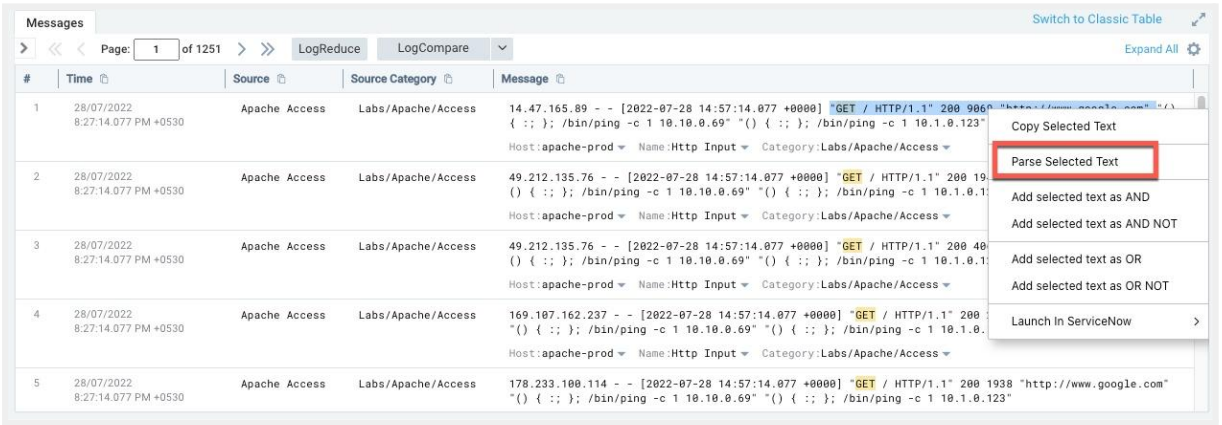
5. Click **Start** to execute the search and display results. In the **Messages** tab, notice that the keyword GET is highlighted, and the number of pages found is displayed.



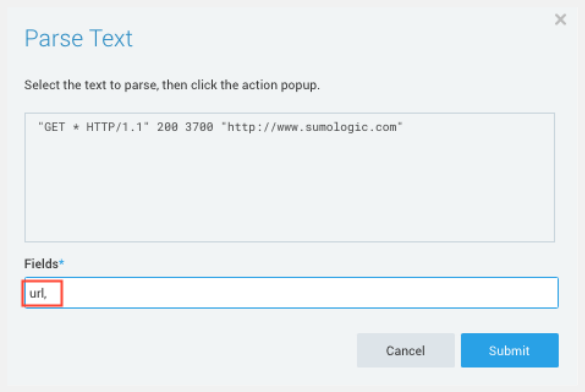
Parse the messages

Parsing makes search results much easier to scan and interpret. Let's parse the log messages for the information that follows the GET and build a new query. We'll parse for URL, status code, size, and referrer. (Your first search result may not be exactly the same, but that's OK.)

1. In the first result message, select/highlight GET and everything after that, including the URL, the status code, the size, and the referrer. After highlighting, right-click the highlighted text. From the menu that appears, select **Parse selected text**.



2. The Parse Text dialog opens. This is where you can select text to be parsed and replaced by fields. The fields are added to the search box to build your search query.
3. Highlight the URL and select **Click to extract this value**.
4. In the **Fields** box, enter URL and a comma to separate the values.



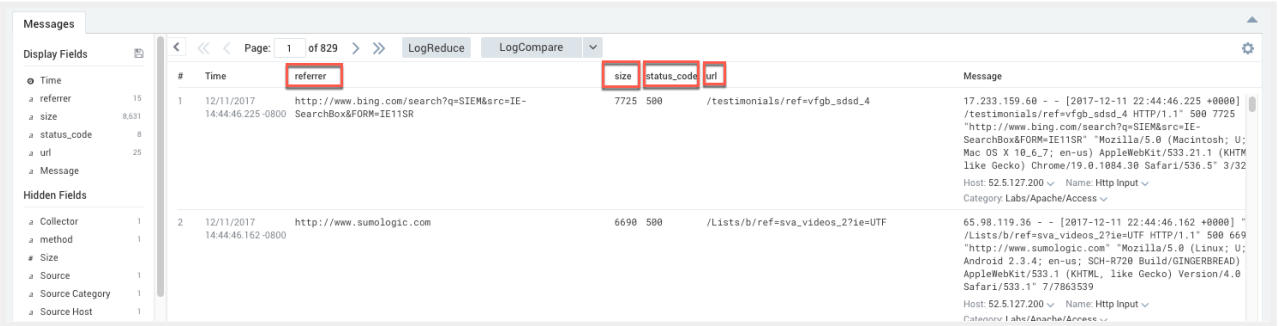
5. Next, highlight the status code 200 and select **Click to extract this value**.
6. In the **Fields** box, add status_code and a comma. Following best practices for naming, use an underscore to connect the words to name the field.
7. Next, highlight the file size and select **Click to extract this value**.
8. In the **Fields** box, enter size and a comma.
9. Finally, highlight the referring URL, but not the quotation marks that surround it. Select **Click to extract this value**.
10. In the **Fields** box, add a referrer, and click **Submit**.
11. The parsing information has been added to our query. You could have typed into the search box yourself, but using the Parse Text dialog is an easy way to build a query without having to remember the syntax.

Remember that you can run this query ONLY in Advanced Mode.
So now our query is:

```
_sourceCategory=Labs/Apache/Access and GET

| parse "\"GET * HTTP/1.1\" * * \"*\" " as
    url,status_code,size,referrer
```

12. Click **Start** to run the query.
13. In the **Messages** pane, notice that the fields that you parsed are now extracted from the raw messages: referrer, size, status_code, and URL. The **Message** text is still available as well.



Save the search

Before going any further, let's save the search so you can easily return to it later.

1. Click the **More Action** icon, then click **Save As**.
2. Enter a name for your search. We entered Apache Status Codes. The description is optional. Notice that the query and time range are filled in automatically. You can change either of them when saving the search if you want to.

3. By default, the saved search is added to your **Personal** folder. You can select one of the subfolders that's listed, or click **+ New Folder** to add a new subfolder.
4. Click **Save** to save your search and add it to the library. Notice that the name is also shown on the top tab bar.

Summary

Pat yourself on your back! As you completed this lab successfully, you

1. Created a search query.
2. Parsed the message so they're easier to scan and interpret.
3. Saved your search.

In the next session, you'll add to your query, chart some results, and create a dashboard.

sumo logic

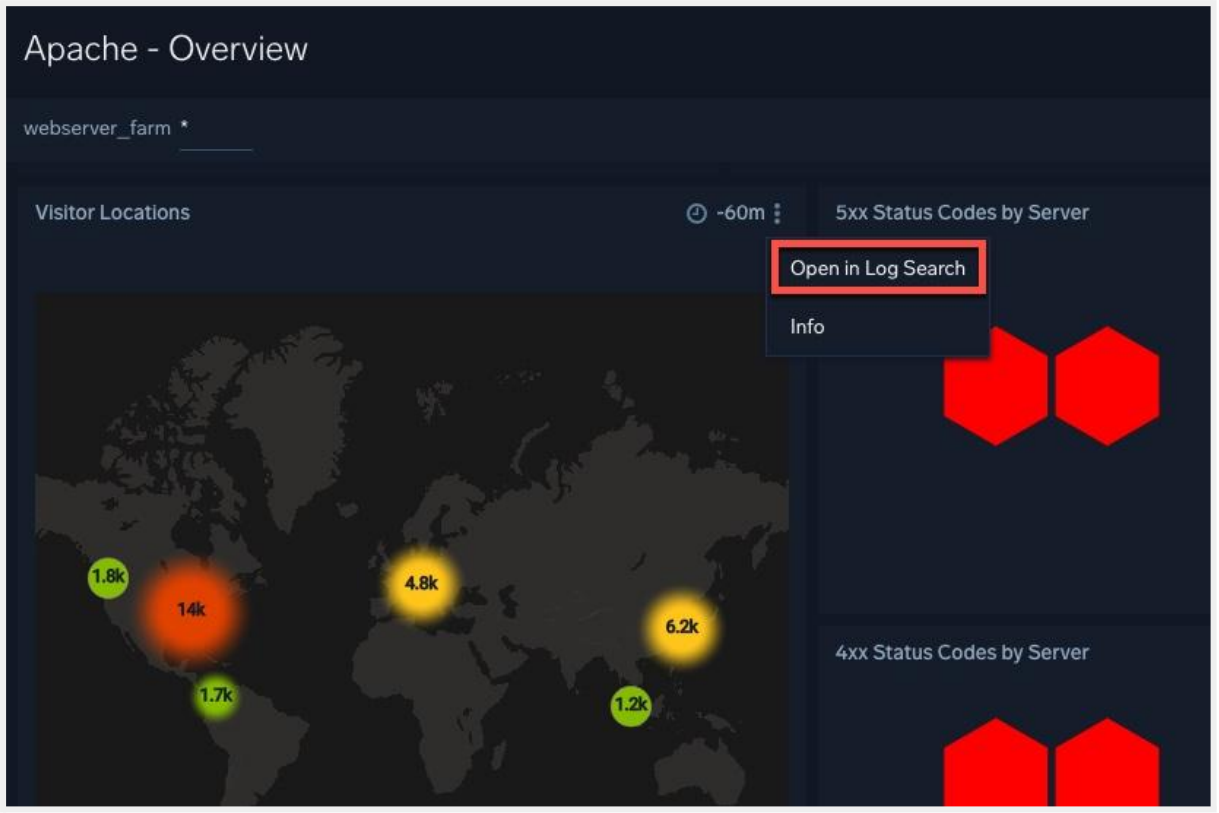
Lab 5: Data Monitoring

Now that you know how to search through data and understand your data, we can create an alert. Alerts allow you to monitor trends in your data.

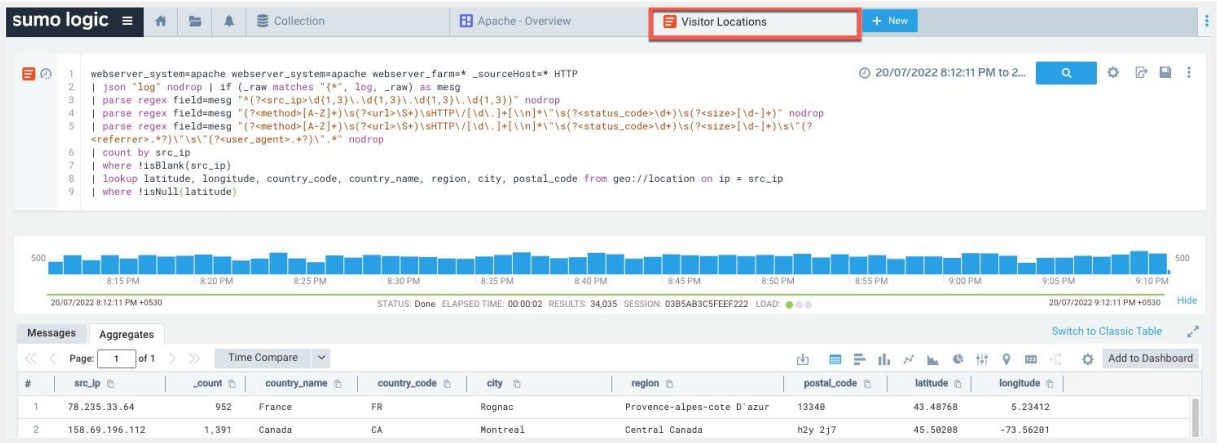
For the purposes of this lab, let's create an email alert. To do that we'll schedule the search we just created.

Create an email alert

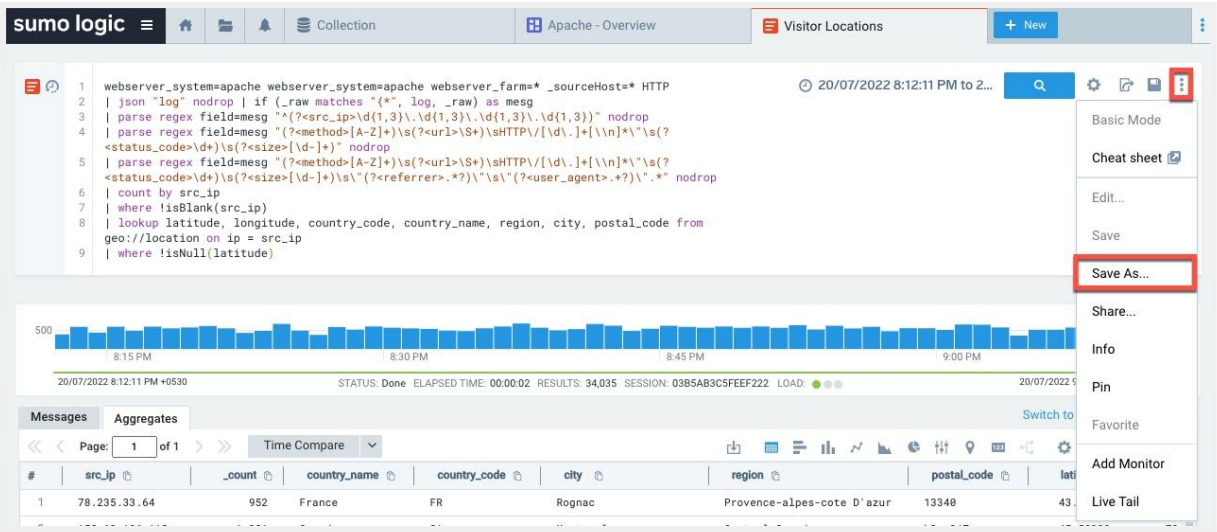
1. In the Apache Overview dashboard, go to the **Visitor Locations** panel, click the details icon  and select **Open in Search** as shown below:



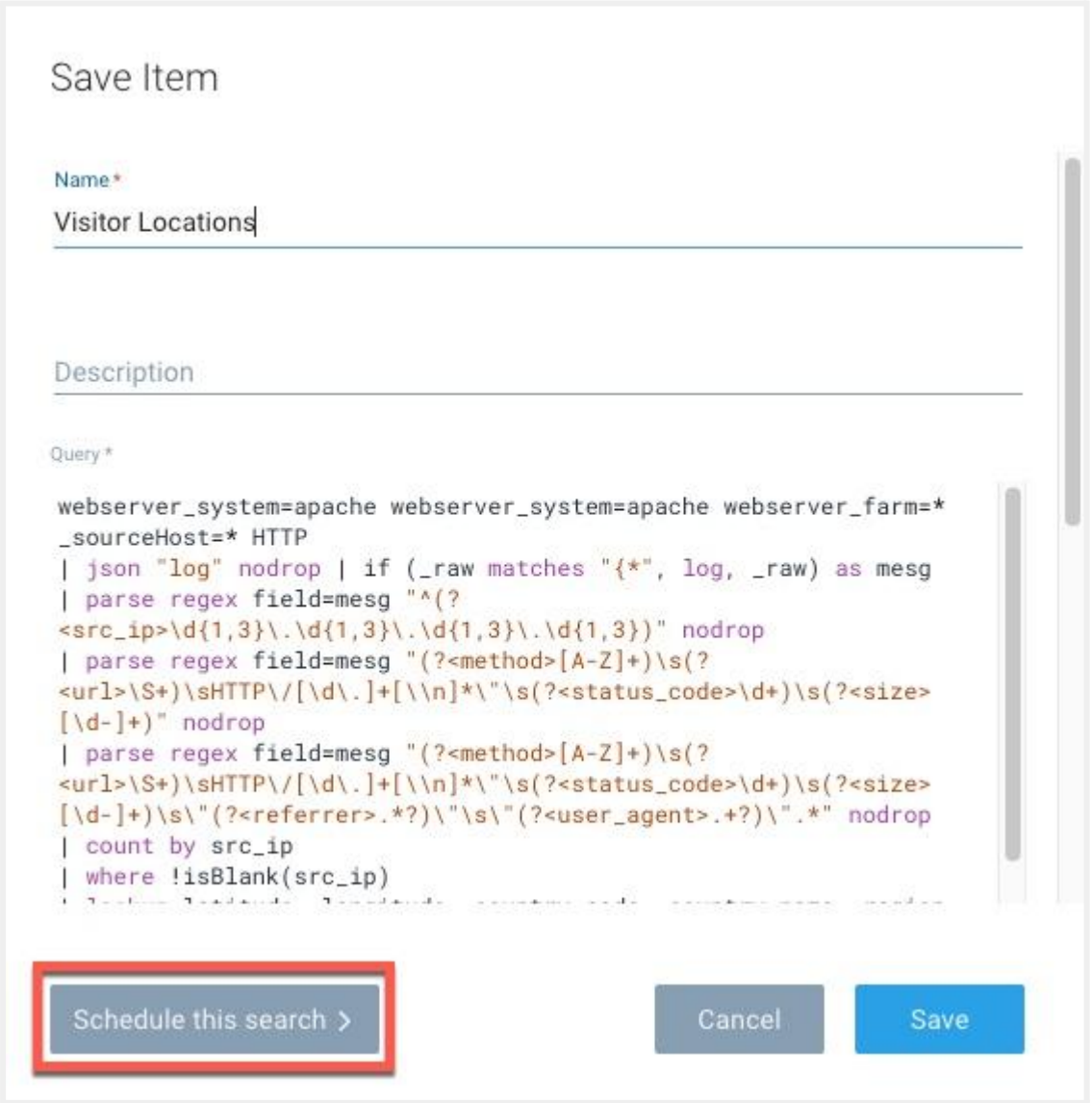
2. Let's select our **Visitor Locations** Search tab.



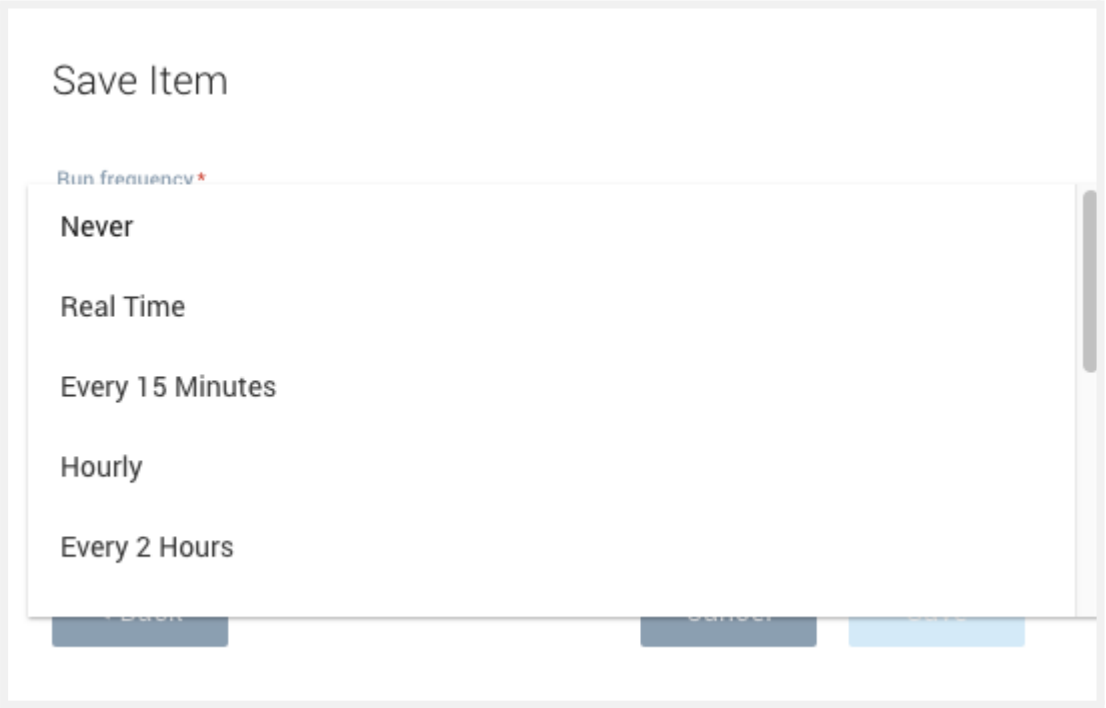
and click on the **More Actions** icon  then click **Save As**.



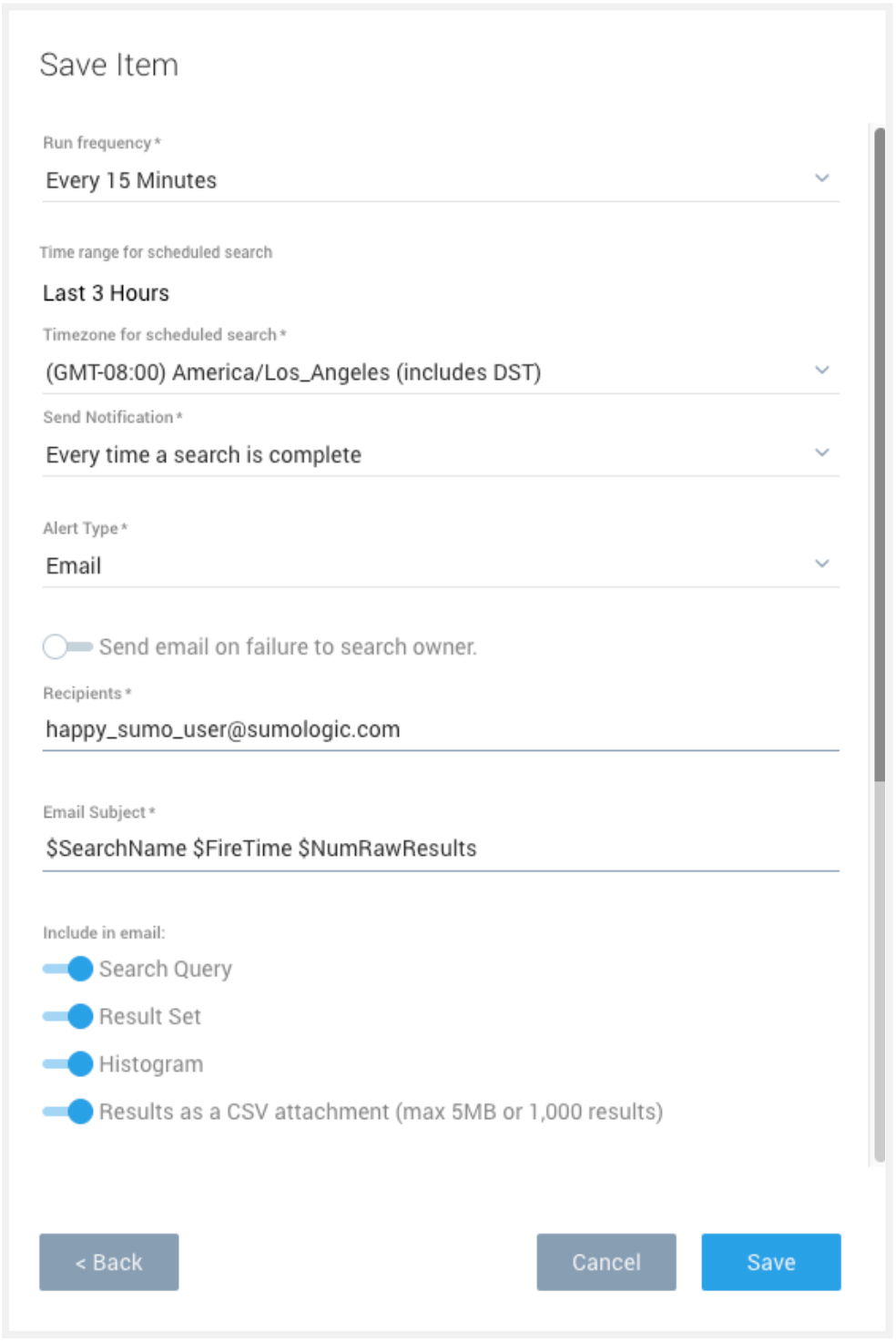
3. Let's keep the default settings, and click **Schedule this Search**.



4. Next, select **Every 15 minutes** as the **Run Frequency**.



5. You will see the options for alerts in the **Save Item** window.



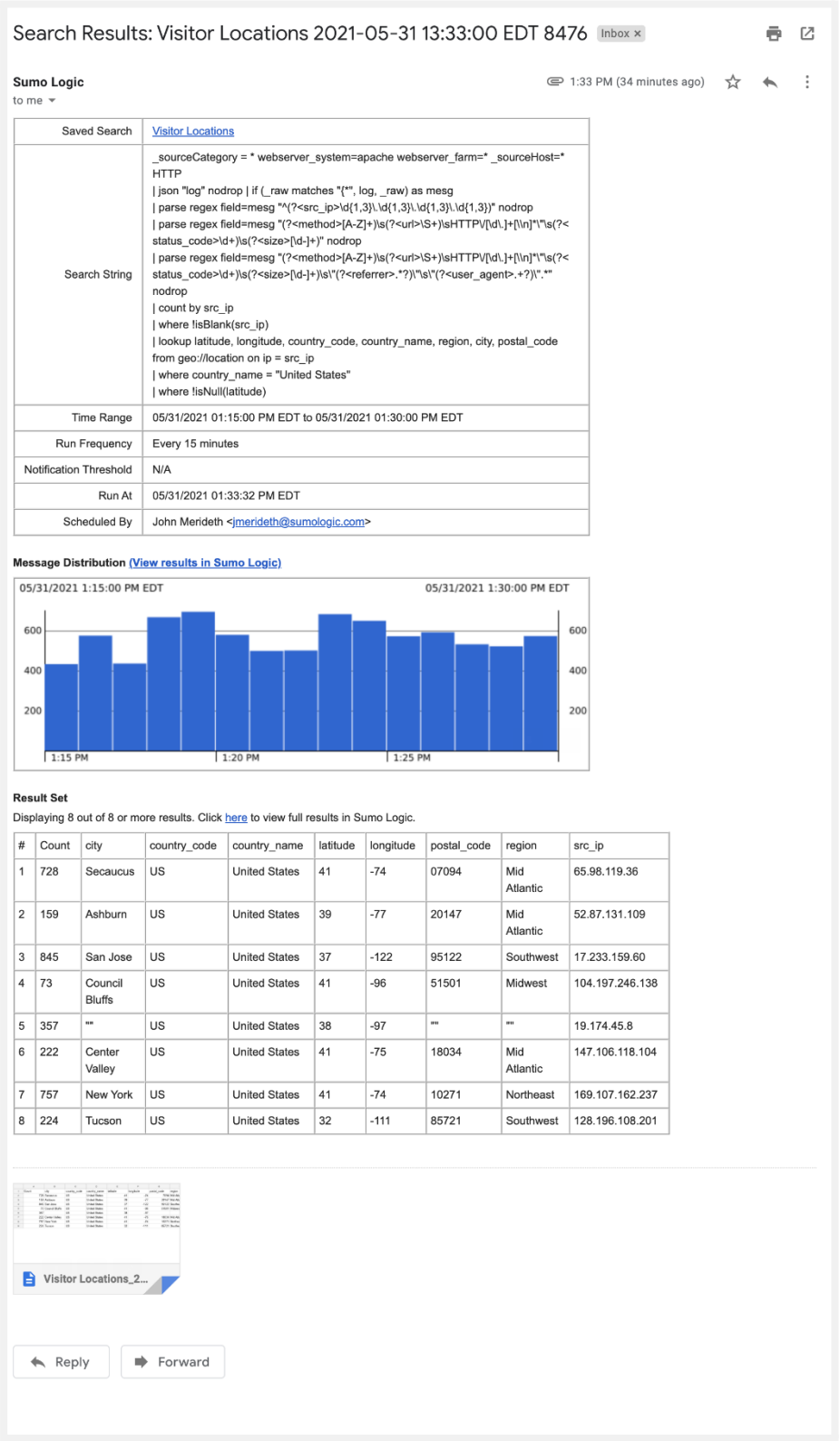
6. Set the following fields:
   a. **Run Frequency. Every 15 minutes.** The search will run every 15 minutes at :00, :15, :30, and :45
   b. **Time range for scheduled search.** Let's set this for **Last 3 Hours**.

c. **Timezone for scheduled search.** This option is great when your source logs are in another timezone but for now, let's leave this at GMT-8:00.
d. **Send Notification. Select Every time a search is complete.** You will get an email with search results every 15 minutes based on the selection you made in **Run frequency.**
e. **Alert Type.** Select **Email**.
f. **Send email on failure to search owner.** This option is selected by default, but let's unselect the option for this tutorial.
g. **Recipients**. Put your own email address. Don't copy my happy_sumo_user@sumologic.com address.
h. **Email Subject**. Let's use some variables to make the subject meaningful to you:

> **{{SearchName}} {{FireTime}} {{NumRawResults}}**

i. This will give you a subject line with the name of the saved search, the time that the search ran, and the number of raw messages returned by the search.
j. **Include in email.** Choose **Results as a CSV attachment** to get a CSV file of the results to go with your alert. (The maximum CSV file size allowed is 5MB or 1,000 results.)

7. Click **Save**.
   Soon, you should see your first email alert:



Search Results: Visitor Locations 2021-05-31 13:33:00 EDT 8476 Inbox ×

Sumo Logic
to me

1:33 PM (34 minutes ago)

Saved Search	Visitor Locations
Search String	_sourceCategory = * webserver_system=apache webserver_farm=* _sourceHost=* HTTP | json "log" nodrop | if (_raw matches "{*", log, _raw) as mesg | parse regex field=mesg "^(?<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})" nodrop | parse regex field=mesg "(?<method>[A-Z]+)\s(?<url>\S+)\sHTTP\/[\d\.]+[|\n]*\"\s(?<status_code>\d+)\s(?<size>[\d-]+)" nodrop | parse regex field=mesg "(?<method>[A-Z]+)\s(?<url>\S+)\sHTTP\/[\d\.]+[|\n]*\"\s(?<status_code>\d+)\s(?<size>[\d-]+)\s\"(?<referrer>.*?)\"\s\"(?<user_agent>.+?)\".*" nodrop | count by src_ip | where !isBlank(src_ip) | lookup latitude, longitude, country_code, country_name, region, city, postal_code from geo://location on ip = src_ip | where country_name = "United States" | where !isNull(latitude)
Time Range	05/31/2021 01:15:00 PM EDT to 05/31/2021 01:30:00 PM EDT
Run Frequency	Every 15 minutes
Notification Threshold	N/A
Run At	05/31/2021 01:33:32 PM EDT
Scheduled By	John Merideth <jmerideth@sumologic.com>

Message Distribution (View results in Sumo Logic)

Result Set

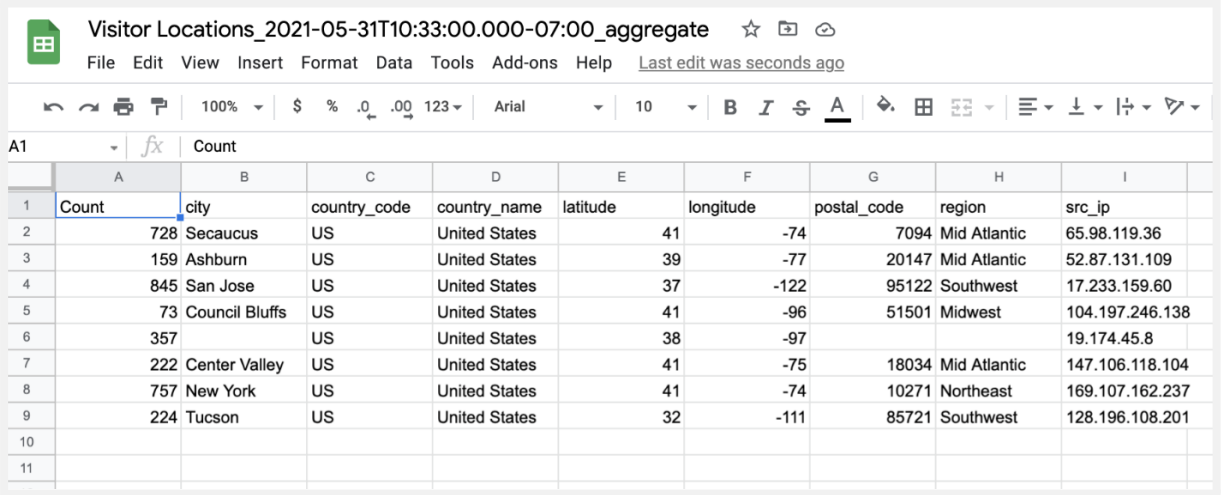
Displaying 8 out of 8 or more results. Click here to view full results in Sumo Logic.

#	Count	city	country_code	country_name	latitude	longitude	postal_code	region	src_ip
1	728	Secaucus	US	United States	41	-74	07094	Mid Atlantic	65.98.119.36
2	159	Ashburn	US	United States	39	-77	20147	Mid Atlantic	52.87.131.109
3	845	San Jose	US	United States	37	-122	95122	Southwest	17.233.159.60
4	73	Council Bluffs	US	United States	41	-96	51501	Midwest	104.197.246.138
5	357	""	US	United States	38	-97	""	""	19.174.45.8
6	222	Center Valley	US	United States	41	-75	18034	Mid Atlantic	147.106.118.104
7	757	New York	US	United States	41	-74	10271	Northeast	169.107.162.237
8	224	Tucson	US	United States	32	-111	85721	Southwest	128.196.108.201

Visitor Locations_2...

Reply Forward

And, also a CSV file named with the search name and timestamp:



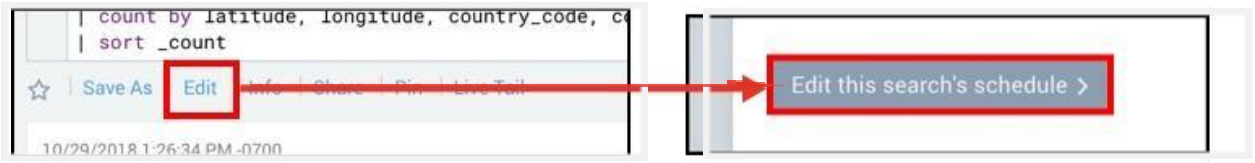
Visitor Locations_2021-05-31T10:33:00.000-07:00_aggregate

File Edit View Insert Format Data Tools Add-ons Help Last edit was seconds ago

A1 Count

	A	B	C	D	E	F	G	H	I
1	Count	city	country_code	country_name	latitude	longitude	postal_code	region	src_ip
2	728	Secaucus	US	United States	41	-74	7094	Mid Atlantic	65.98.119.36
3	159	Ashburn	US	United States	39	-77	20147	Mid Atlantic	52.87.131.109
4	845	San Jose	US	United States	37	-122	95122	Southwest	17.233.159.60
5	73	Council Bluffs	US	United States	41	-96	51501	Midwest	104.197.246.138
6	357		US	United States	38	-97			19.174.45.8
7	222	Center Valley	US	United States	41	-75	18034	Mid Atlantic	147.106.118.104
8	757	New York	US	United States	41	-74	10271	Northeast	169.107.162.237
9	224	Tucson	US	United States	32	-111	85721	Southwest	128.196.108.201
10									
11									

8. To turn the alert off, open the corresponding query in the Search view, select **Edit**, then **Edit this Search's Schedule**:



9. Select **Never** from the Run frequency dropdown selector, and **Update** to confirm the changes:

sumo logic

Lab 6: Data Visualization

Dashboards are a powerful forensic tool that allow you to visualize key search results at a glance and view related results in a single graphical display.

Dashboard allows you to view log and metric data on the same dashboard in an integrated and seamless view. This gives you the same control over how your metrics and log data are visualized. Dashboard template capabilities provide for easier data scoping and intuitive chart creation.

In this lab, you will learn how to:

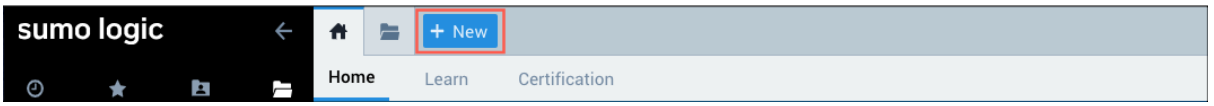
- Create and modify a dashboard.
- Create a panel and add it to a dashboard.
- Modify content of the panels from your dashboard.

Create a Dashboard

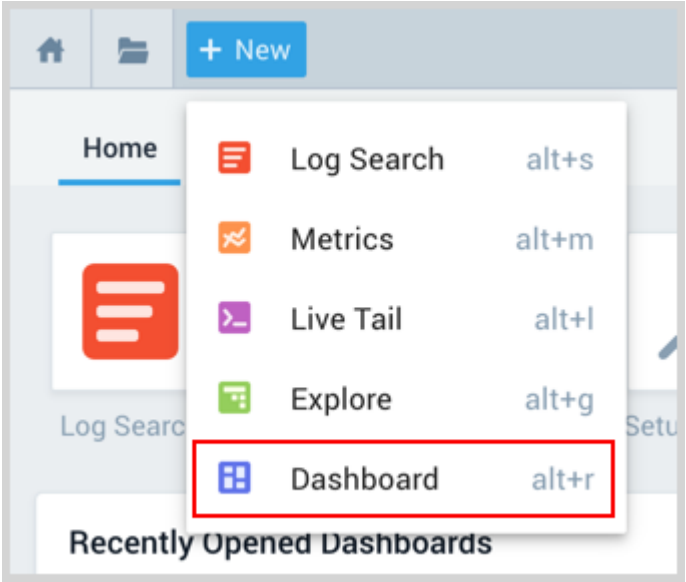
In this lab, you create a Dashboard, to which you will add panels and customize charts in later steps. You can use the +New button or create a Dashboard directly from the Log Search, Metrics page.

To create a Dashboard:

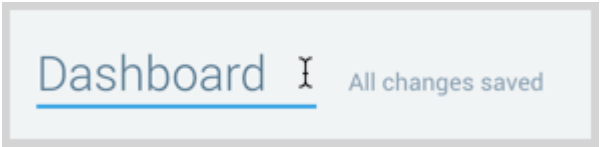
1. On the Home page, click **+ New**.



2. Select Dashboard from the drop-down list.



3. Select the Dashboard text field at the top of the window and enter a unique name for your new dashboard.



4. Let's name it 'Apache <yourname> Status'. After you enter the dashboard name, the dashboard will be automatically saved to your **Personal** folder. If you don't see it listed immediately then you may need to refresh your browser page to have it appear.

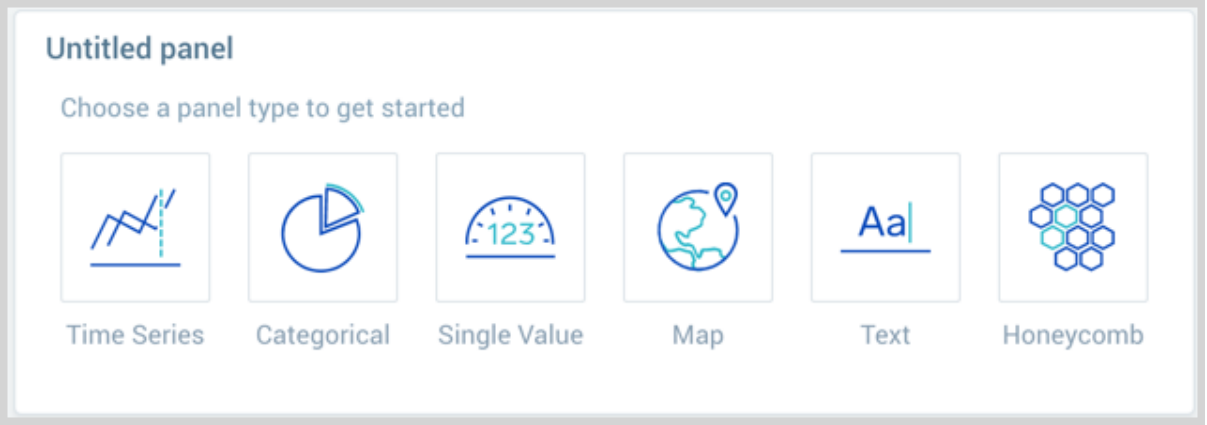
5. You can then choose to move your new dashboard to, say, your **Apache** folder by clicking on the details icon  , selecting **Move** from the pop-up menu presented and then following the prompts presented in the dialogue.

Add a 'Time Series' panel

Now that you've created a new Dashboard, you can populate it with panels that visually display your data. This task shows you how to add a panel to your new dashboard and customize the display.

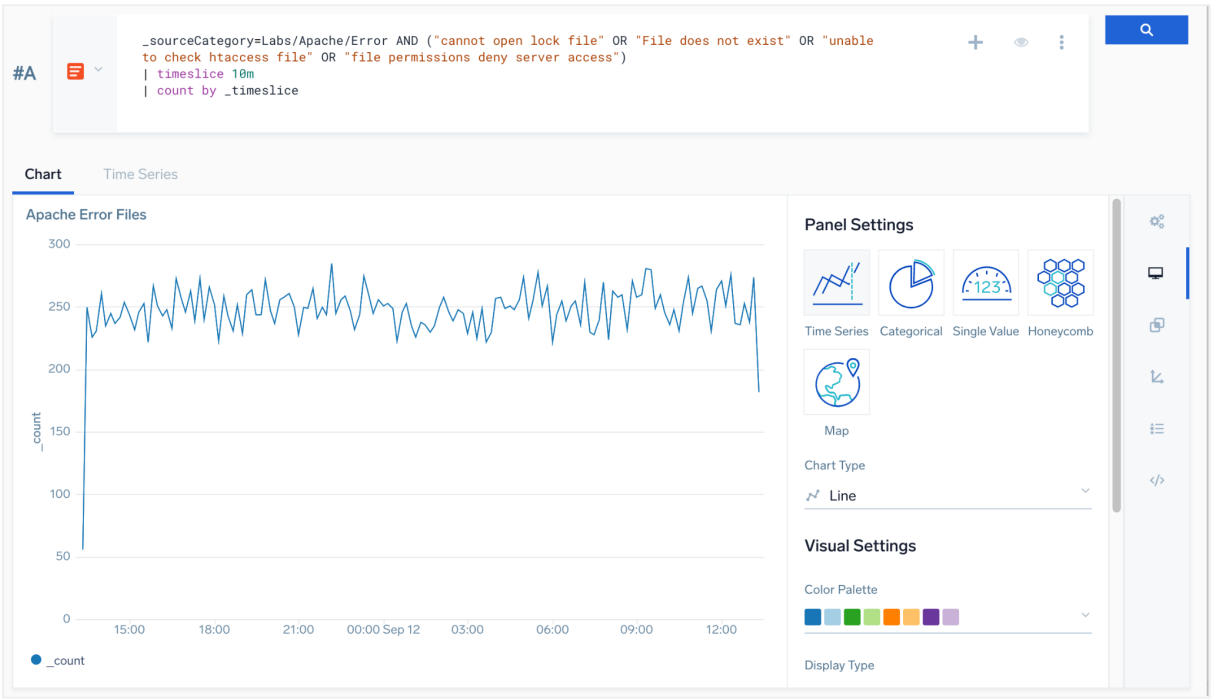
To add a panel to a new Dashboard:

1. Select a panel type 'Time Series' by clicking the icon. See choosing a panel type for details.



2. You will be prompted to provide a query. You can create Log and Metric queries on the same panel.
3. By default, the query builder is set to Logs.
4. Let's enter the search query in the input field, set the Time Range to -24h and press enter.

```
_sourceCategory=Labs/Apache/Error AND ("cannot open lock
file" OR "File does not exist" OR "unable to check htaccess
file" OR "file permissions deny server access")
| timeslice 10m
| count by _timeslice
```

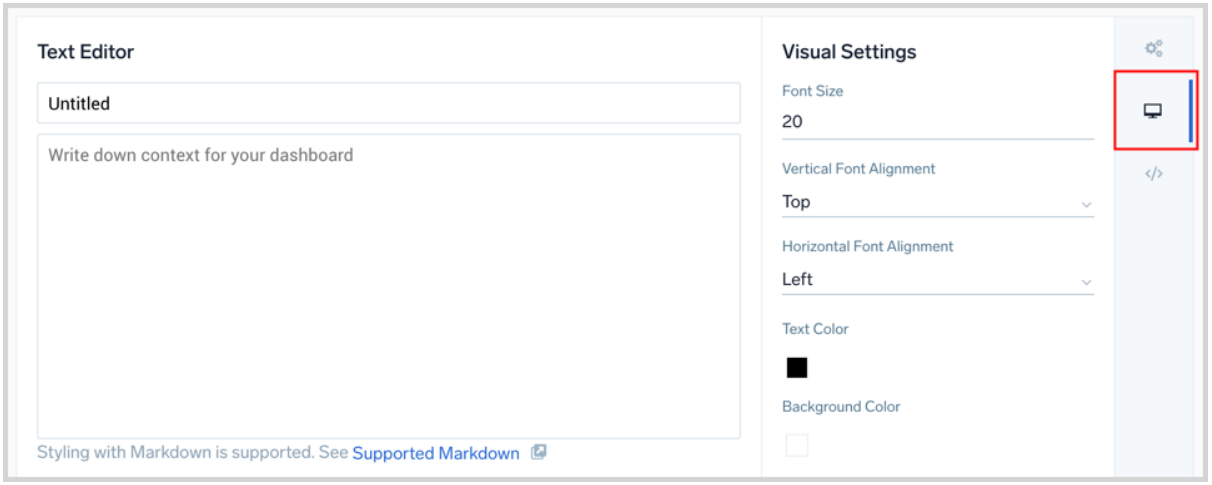
5. 

6. Assign a name to the new panel. For this example query, let's call the panel "Apache File Errors"
7. Click **Add to Dashboard**. The panel is added to the dashboard.

Change the look and feel of the dashboard

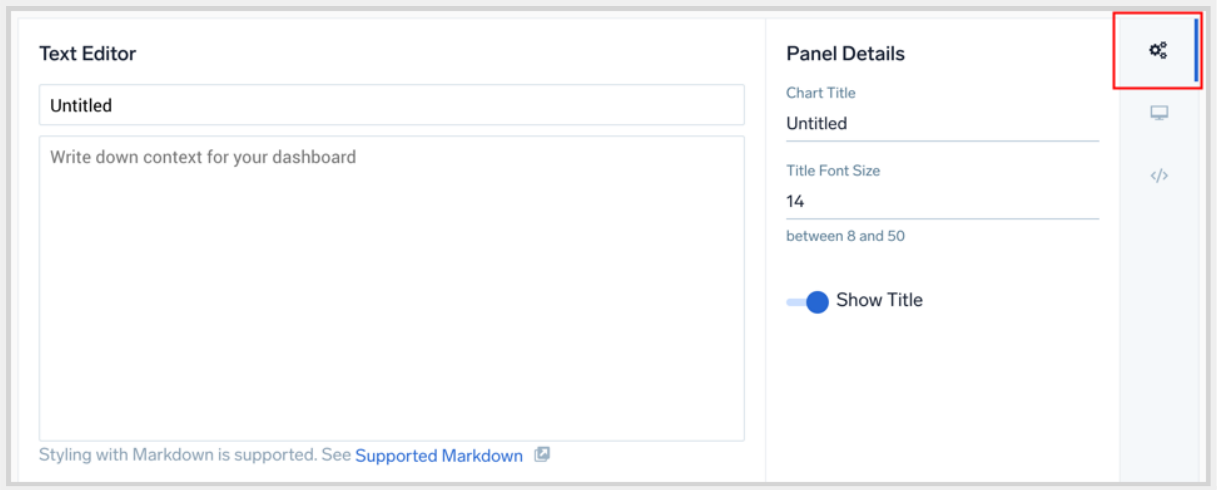
1. Try adding the text panel next to the time-series panel.
2. With the Dashboard open, click the **Add Panel** button.

3. Choose **Text** as the Panel Type**.**
4. The **Text Editor** and **Visual Settings** are displayed.



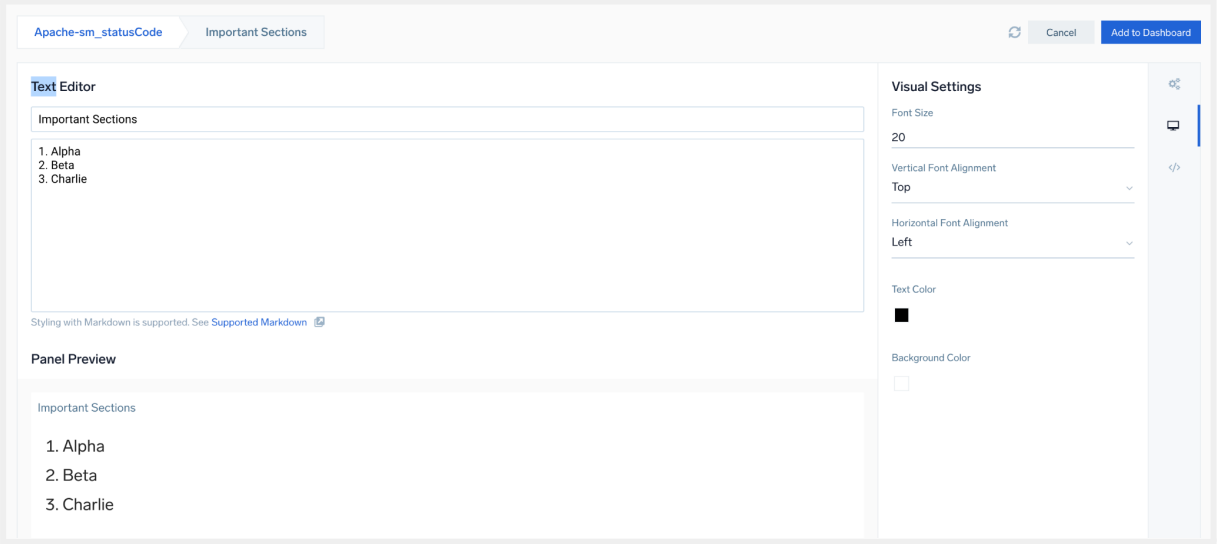
   a. Input your **Text** or **Markdown** syntax in the **Text Editor** pane. See Markdown Syntax for details on what is supported.
   b. The **Visual Settings** options allow you to adjust the font, colors, and alignment of your data.
   c. A title is optional, you can toggle its visibility in the **Panel Details** covered in the next section.

5. Next, to set a Title, select the **General** menu icon to open the **Panel Details** pane.

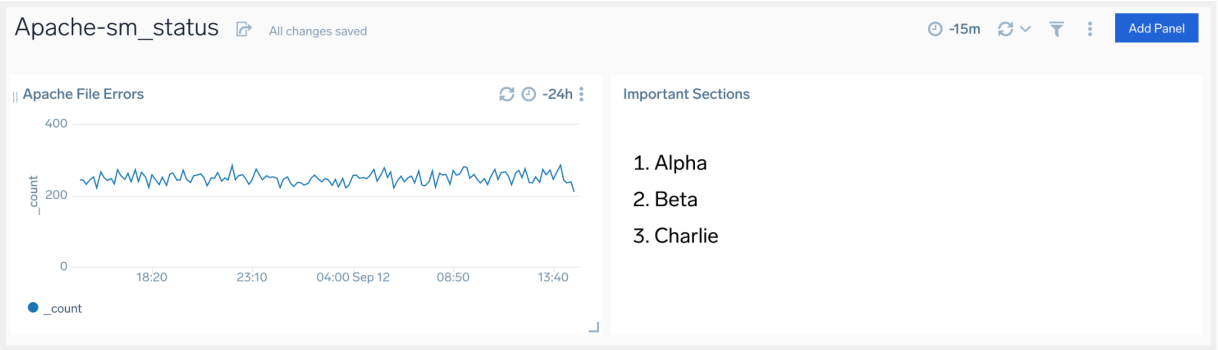


   a. A title is optional. Use the toggle switch labeled **Show Title** to set if the title is displayed. If desired, enter a title and set the font size.

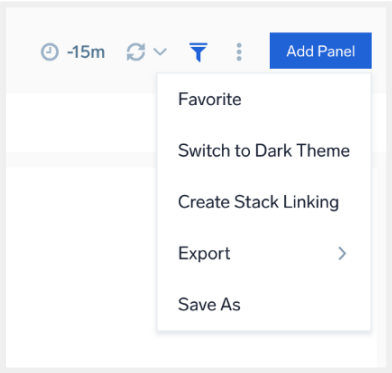
6. The **Panel Preview** section displays your text panel based on your settings.



7. When you're done, click **Add to Dashboard** at the top of the window.
8. If the panel is set to show its title then you can drag the panel by clicking and dragging the panel title. If the title is hidden then you need to point your mouse at the top left corner to show the multi-arrow icon. That's your signal that you can drag the panel to reposition it.
9. Let's resize the text panel so it's easier to see. Drag the lower right corner of the panel to resize it. As before, you might have to reposition both panels to arrange the panels in your dashboard so you can see the most valuable information at a glance.



10. Click the **More Actions** (three dots) icon to the left of the **Add Panel** button.



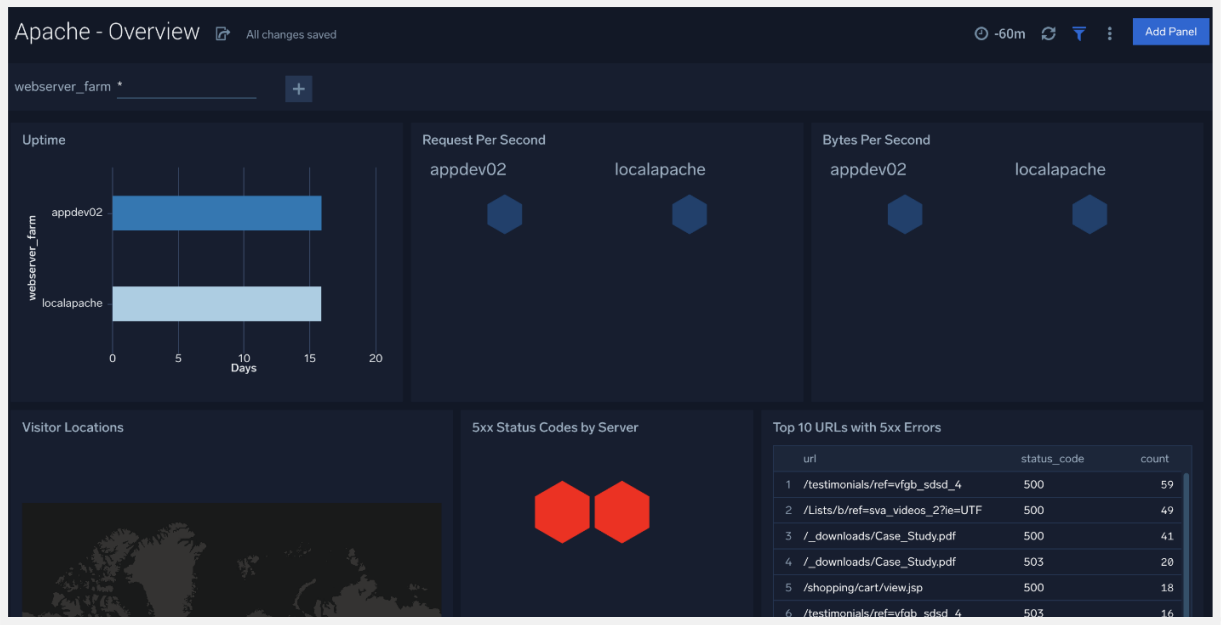
11. Select **Switch to Dark Theme** to change the dashboard to the dark theme.

Modify your dashboard

Now that you know how to create a dashboard and change the look and feel, let's see how you can change the content of the data panels.

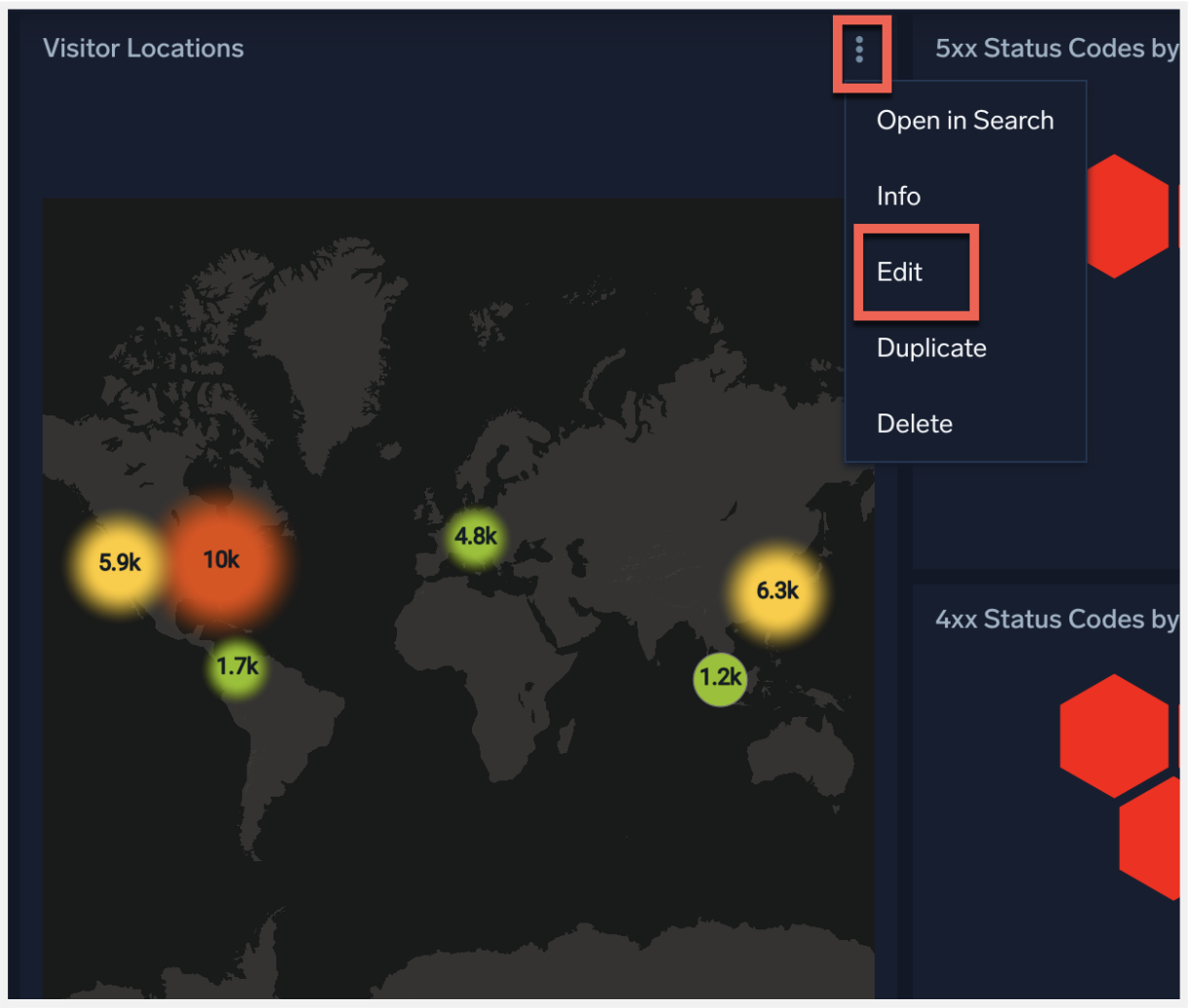
Let's start with the Apache Overview dashboard, which is included in the Apache Access app.

1. In the left navigation panel, click **Apache - Overview** in your Personal folder.

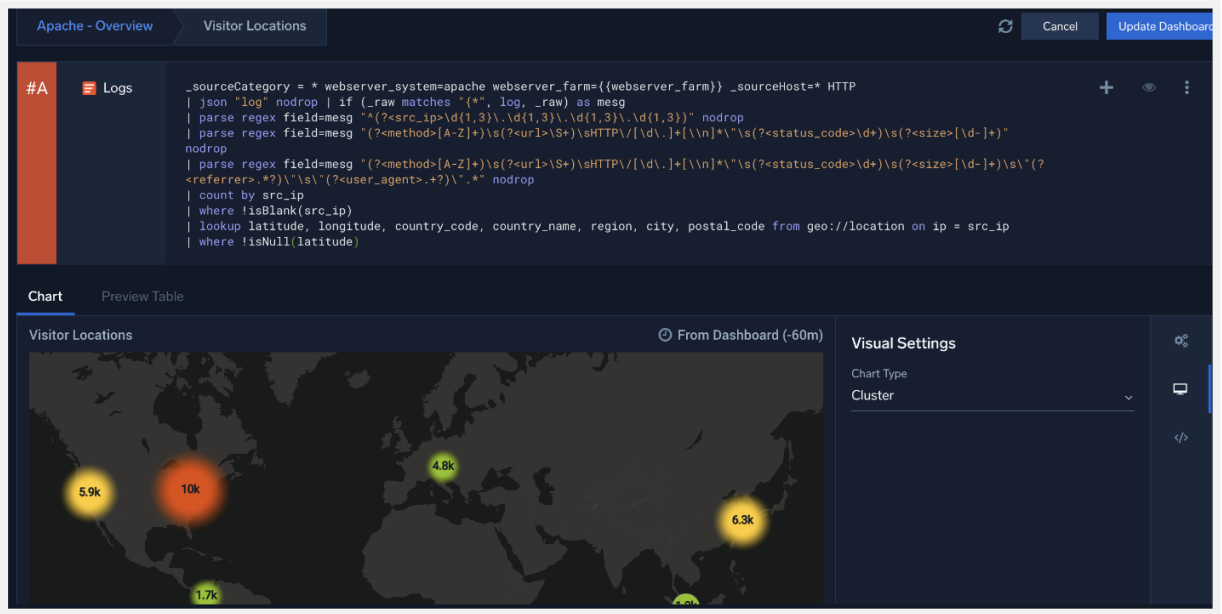


Notice that the Visitor Locations panel includes all worldwide locations. Let's change the panel to zero-in on the U.S. locations.

2. In the Visitors Locations panel, click the details icon  , then click **Edit** to show the search that was used to generate this panel.



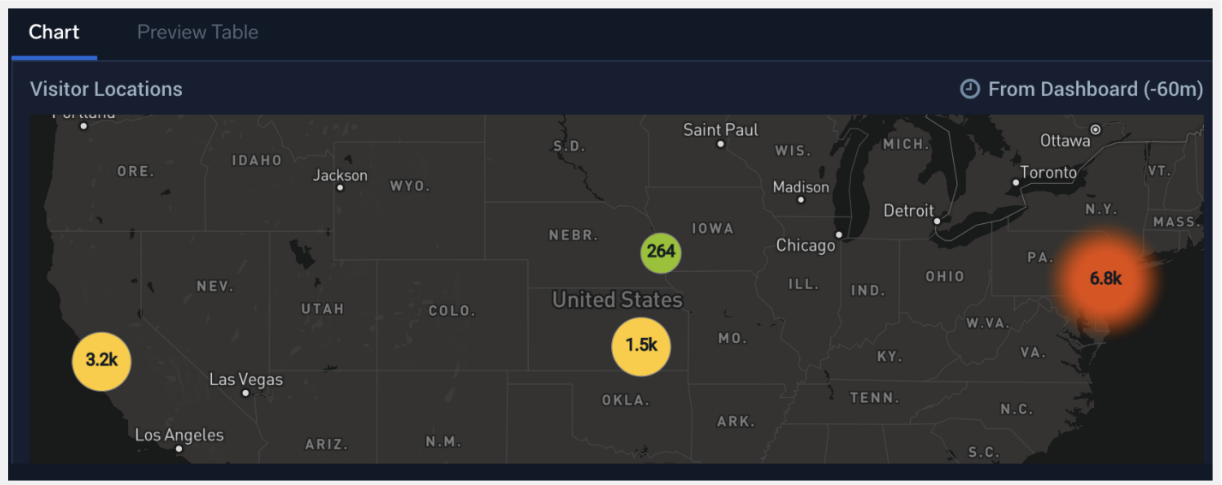
The page includes all the information for the search, including the query and the chart.



3. Now you can modify the query to zoom on the U.S. portion of the map. Add a soft return (hold shift + return) right after the lookup line, to specify the country:

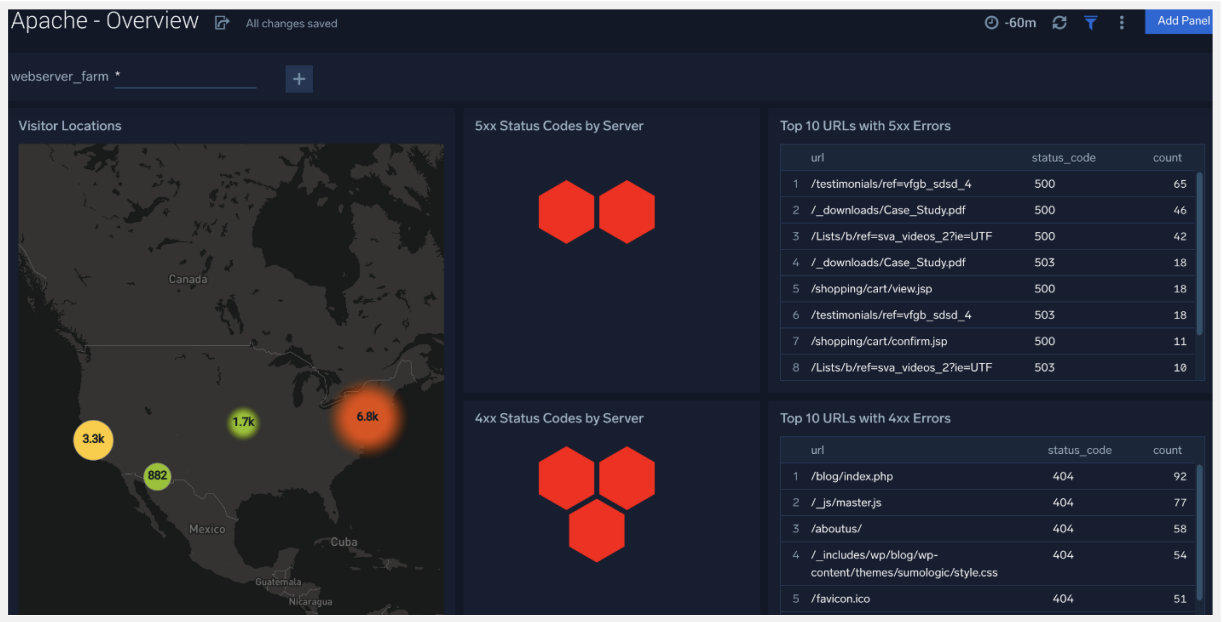
```
| where country_name="United States"
```

4. Click **Search** or hit **Enter** to run the query. The results chart now shows just the United States.



5. To show the modified panel in your dashboard, click **Update Dashboard**.

6. You will now see the dashboard with the updated panel.



Now that you know how to move between the dashboard and the Search tab, you can adjust any of the search settings for a dashboard panel.

Good job! You've completed the following tasks:

1. Created a dashboard from your search results
2. Added a panel
3. Changed the look and feel of the dashboard.

Moving on to the last lab, you'll learn about the number of resources and stay connected with the Sumo Logic community.

sumo logic

Lab 7 – Get help

Get Help with Sumo Logic

Now that you know the basics, you can focus on using Sumo Logic to get the results you want from your data.

But when you have a question, you can reach out to us in a number of ways.

- Check out the Release Notes
- Search DocHub
- Visit the Learn Page
- Post a question on the Sumo Logic Community
- Try our Customer Slack channel
- Contact Support

Check out the Release Notes

Using Sumo day to day you will find most of the updates you need in the Service Release Notes. These release notes cover all the Sumo features and fixes that impact your data analytics.

There are also Collector Release Notes that cover updates to our data ingest tools. Usually these updates are of more interest to Sumo admins.

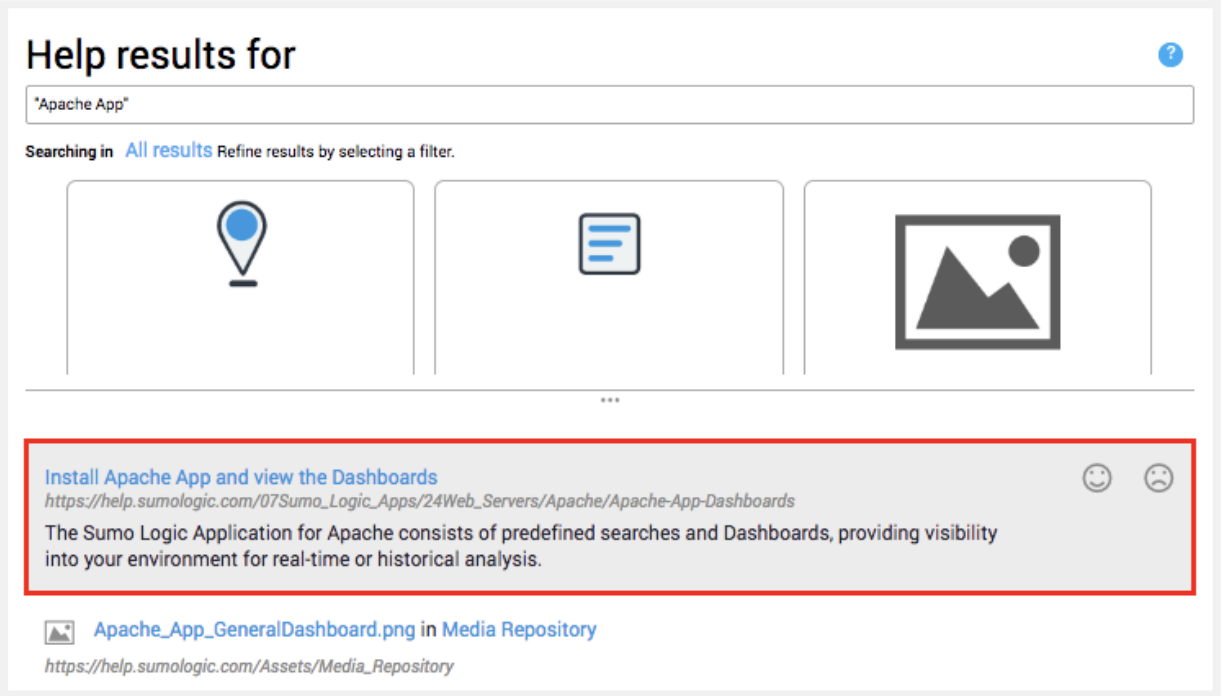
To find the Release Notes, choose the Release Notes link from any DocHub Page:

Search DocHub

DocHub contains hundreds of articles on how to use Sumo. Let's look for Apache Access app documentation.

1. In the search bar for DocHub, enter "Apache app".

2. The Help results for returns several links, let's click the top one **Apache App Dashboards**.



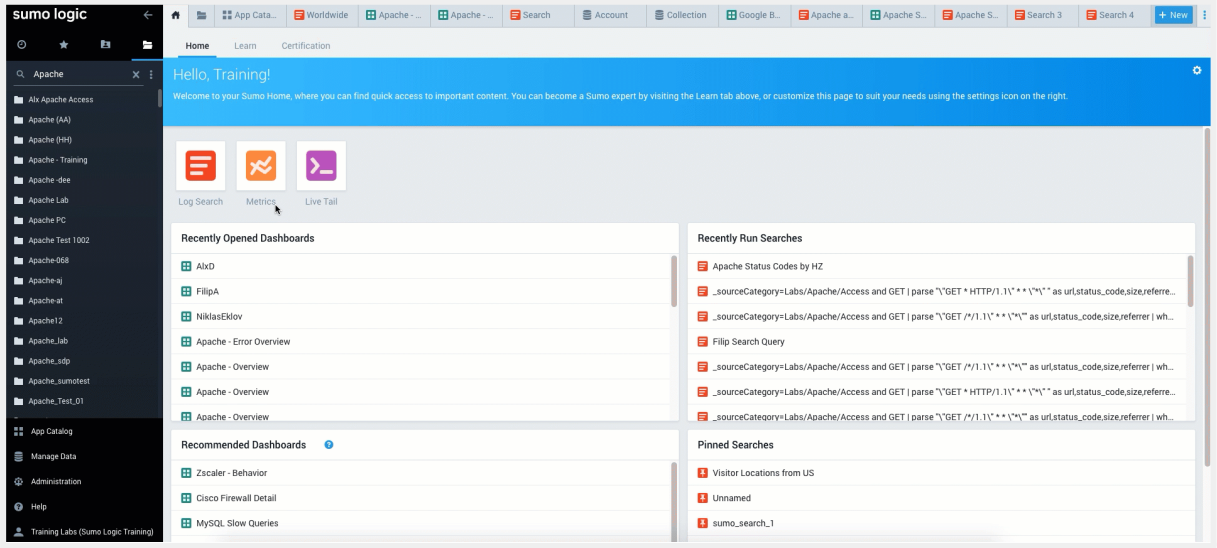
3. Click Apache App Dashboards, help will take you to the descriptions of the out-of-the-box Dashboards for Apache.

Visit the Learn Page in Sumo

Find out more about Sumo by clicking Learn from the **Home** page. Learn is designed to help you discover Sumo resources quickly by providing direct links to:

- Important how-to videos
- Tutorials on setting up and using Sumo for the first time
- Support ticket interface
- Product documentation

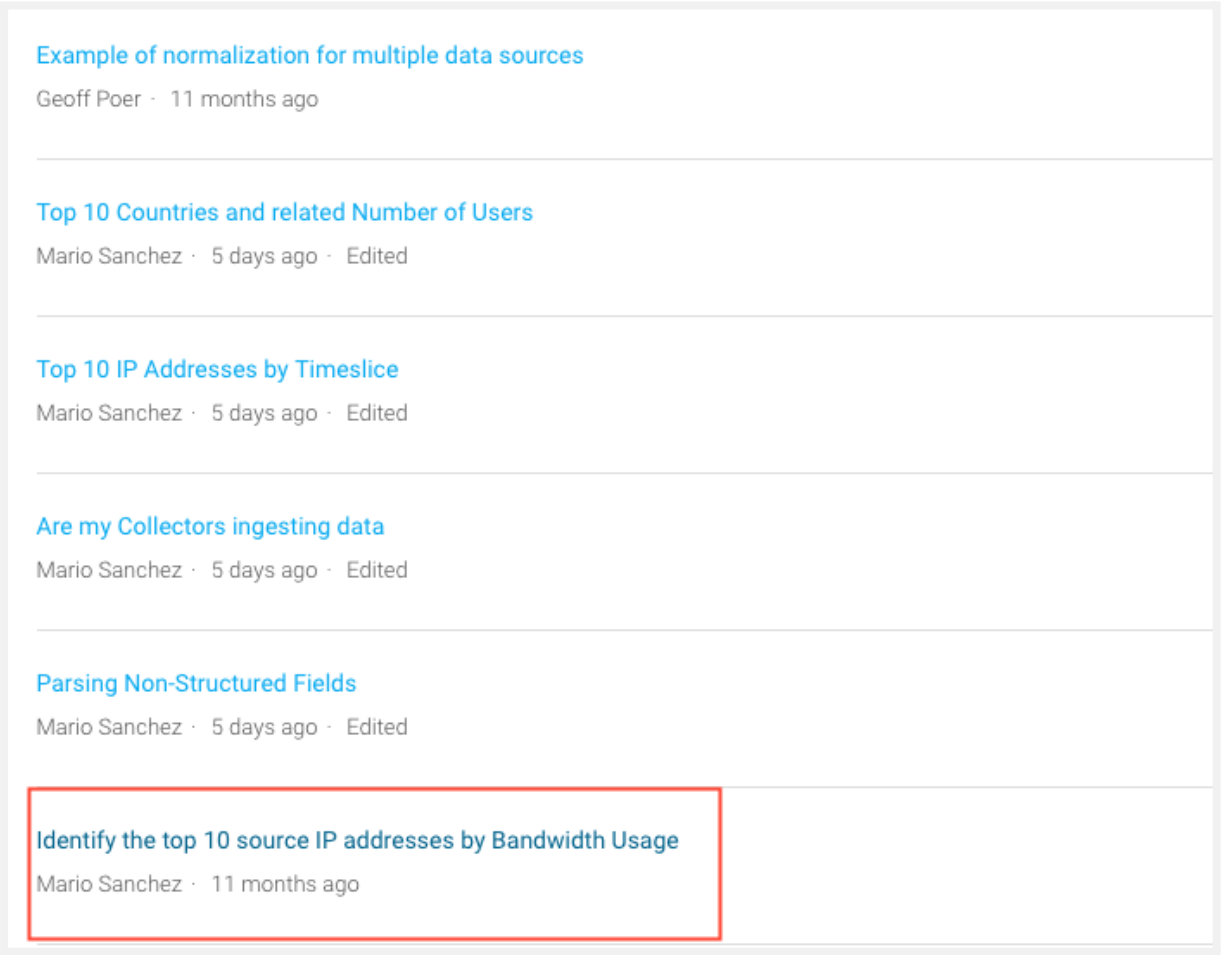
- Available training webinars
- Cheat Sheet
- Sumo Community
- What's New page with the latest product announcements



Post a question on the Sumo Community

Our Community is the best way to find help for Beta Features and answers to puzzling questions, but you can also find templates to help you use Sumo more effectively. The **Query Library** is a series of posts available in the community that give you basic query templates to help you search Sumo more effectively.

1. Go to the Sumo Community.
2. Select Query Library.
3. All the posts here list available queries. Let's pick one to help you with your Apache Access data from the previous tutorials. Select **Identify the top 10 source IP addresses by Bandwidth Usage**.



4. You can copy the query template and create a new search:

Try our Customer Slack channel

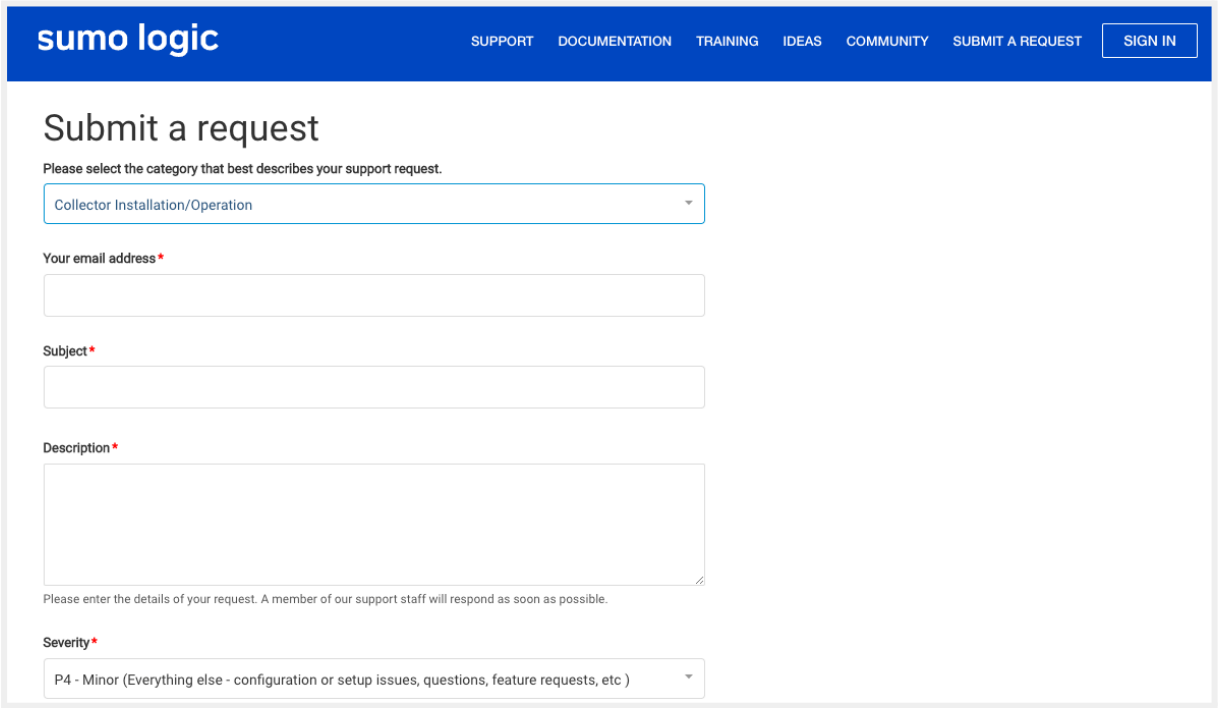
Need to talk to an expert? Most of our developers make themselves available on our customer-facing Slack channel. Slack is a very popular chat channel, and if your question isn't time-bound:

1. Register for the channel at slack.sumologic.com
2. Log in and join us

Most of the time we're able to respond quickly to your question.

Log a Support Ticket

If you need an answer to a time-bound question, log a Support ticket.



Congrats! You've reached the end of the labs. If you want more training, you can visit our Training Site.