SPLUNK TO DYNATRACE

QUICK START GUIDE

LEARNER AID

DATE UPDATED: 4/3/2024
OWNER: IT TRAINING

TABLE OF CONTENTS

UWM®
UNITED WHOLESALE MORTGAGE

TRANSITIONING FROM SPLUNK TO DYNATRACE

OVERVIEW

To aid in the transition from Splunk to Dynatrace, this document is a companion to the OCOE enablement session and will provide you with resources to get started searching for logs in Dynatrace. This document will contain key information about navigation, features of the new UI, and outside resources to assist you in the transition away from Splunk. Toward the end of the document, there will also be space provided to take notes during the enablement session.

BASIC NAVIGATION

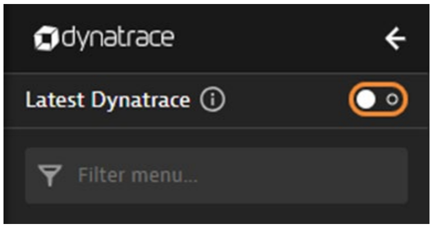
Learning how to navigate Dynatrace will help to set you up for success as you learn more advanced skills. Below you will find tips and tricks for Dynatrace navigation.

SWITCHING BETWEEN THE OLD AND NEW USER INTERFACES

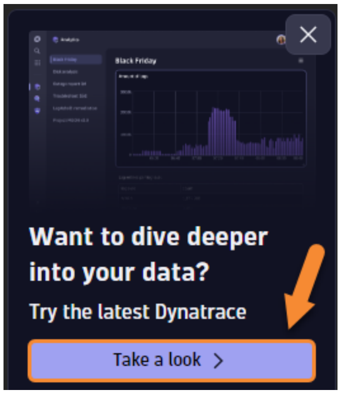
Dynatrace has an old user interface (UI) and a new UI. The new UI will be the one used most of the time, but below you will find instructions on how to toggle between the two UIs.

OLD UI TO NEW UI

1. Click the **toggle button** in the upper left corner.

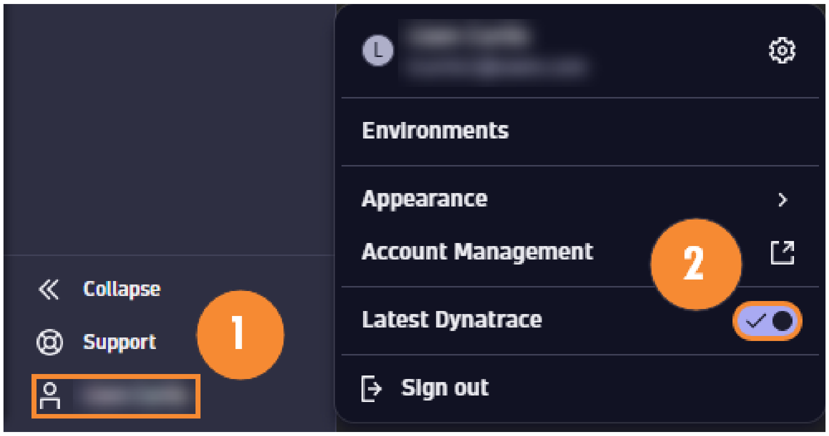


Note: If you've never accessed the new UI, the toggle will be covered with a graphic. Click **Take a look**.



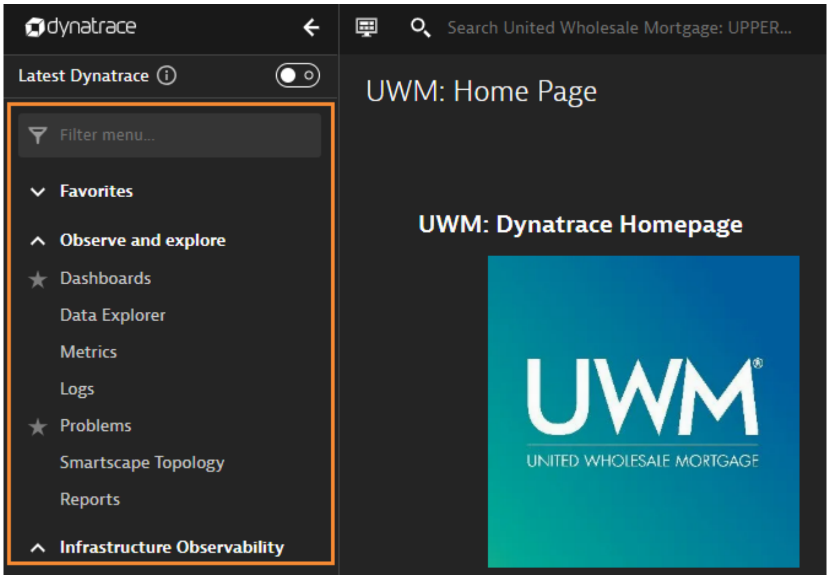
NEW UI TO OLD UI

1. Click your **account name** in the lower left corner.
2. Click the **toggle button**.



OLD UI BASIC NAVIGATION

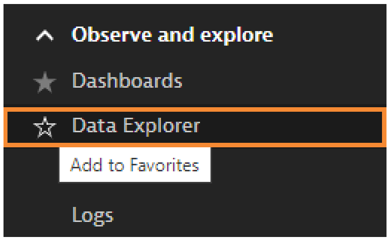
The old Dynatrace UI has a fixed left-hand menu that is used to get to different pages in Dynatrace.



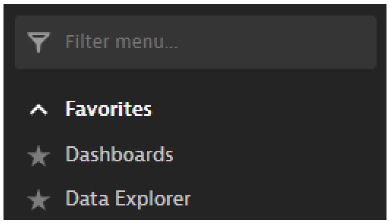
FAVORITING APPLICATIONS

You can favorite your most visited pages, which includes them in the top Favorites section for easier access.

1. Hover your mouse over the left side of the page you want to favorite then click the **star**.
   Note: You will not see the star beside the application until you hover over it.



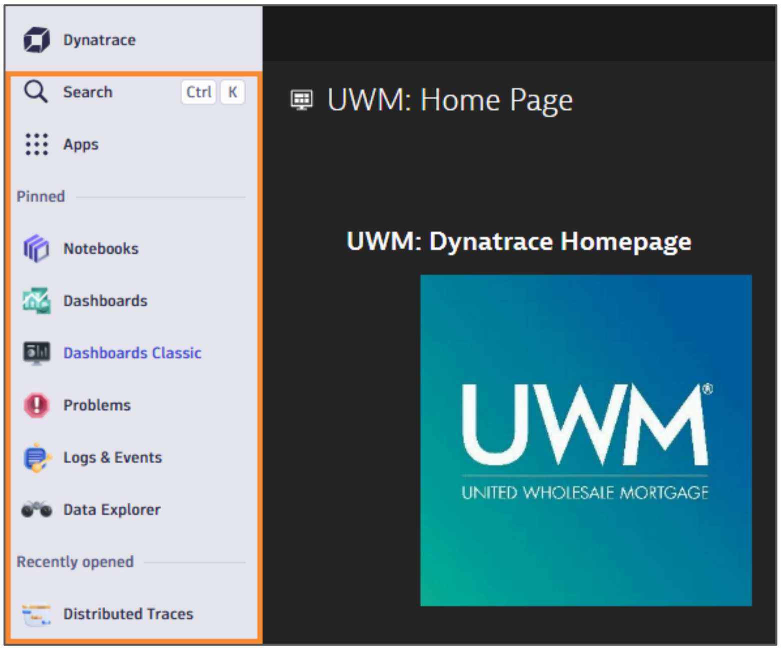
2. To access any favorited pages, expand the **Favorites** section under the filter menu field.



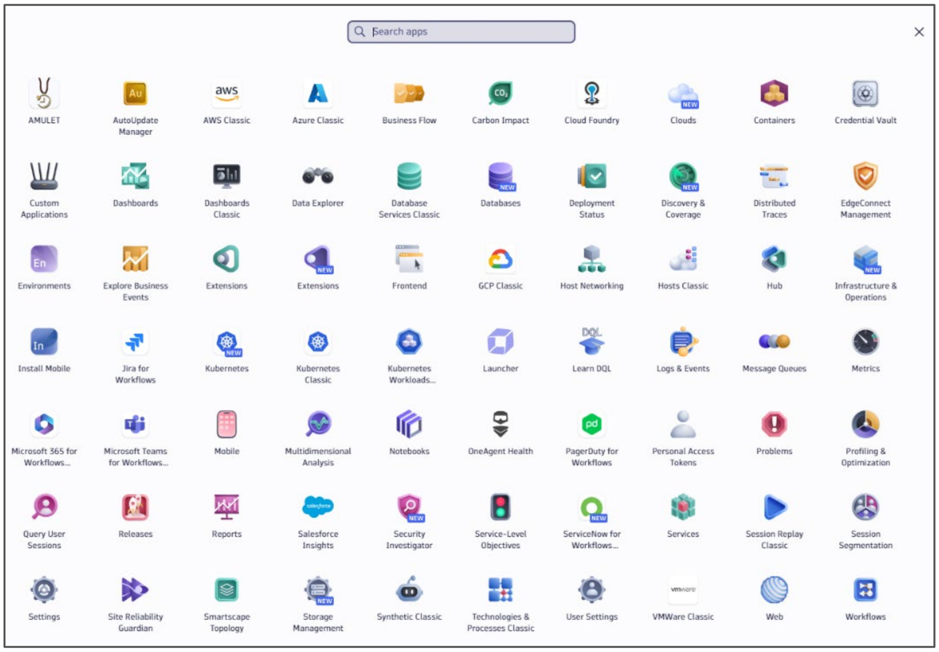
NEW UI BASIC NAVIGATION

To modernize, Dynatrace is developing a new UI alongside their old UI. This new UI is live, and you are encouraged to use it as much as possible to utilize the better layout and new features. The new UI uses applications instead of pages and to access these applications Dynatrace uses an app drawer for navigation, as well as the ability to pin your most used apps to the left-hand side of the UI.

Below is the left-hand navigation where you can pin applications for quick access:



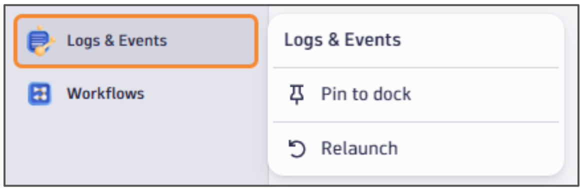
Below is the app drawer:



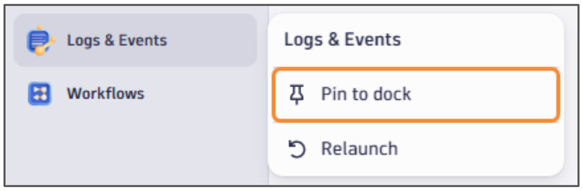
PINNING APPLICATIONS

You can pin your most used apps to the left sidebar in the new UI. Rather than having all pages displayed like the old UI, the new UI enables you to curate your own menu with the apps most important to you.

1. Under the Recently Opened section, hover your cursor over the **app you'd like to pin**.
   Note: You cannot pin an application from the App Drawer. You must open the app first.



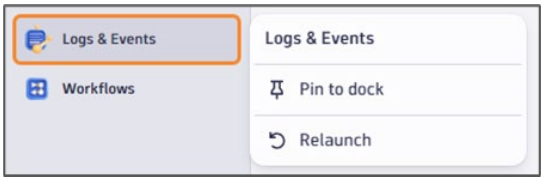
2. Click **Pin to dock**.



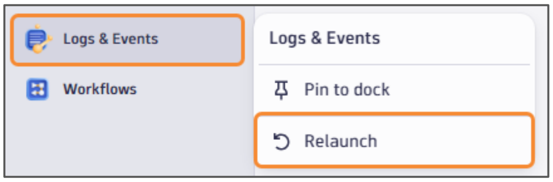
RELAUNCHING APPLICATIONS

Occasionally, while using an application in Dynatrace, you may find yourself stuck on a screen and unable to navigate away. If this happens, you can relaunch the application to its default starting point. Follow the steps below to relaunch an application in Dynatrace.

1. Hover your cursor over the **app** you need to restart.



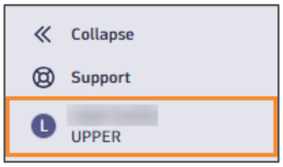
2. Click **Relaunch**.



SWITCH TO DARK MODE

For those of you who prefer dark mode, follow the steps below to switch to dark mode.

1. Click on your **name** in the lower left corner.

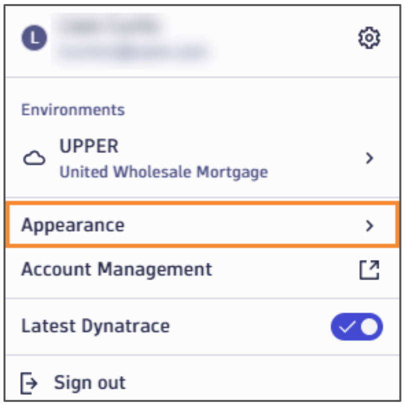


Collapse

Support

L [redacted]
UPPER

2. Click **Appearance**.



L [redacted]

Environments

UPPER
United Wholesale Mortgage

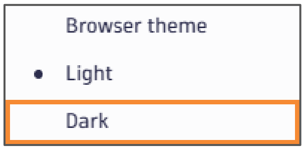
Appearance

Account Management

Latest Dynatrace ✓

Sign out

3. Select **Dark**.



Browser theme

● Light

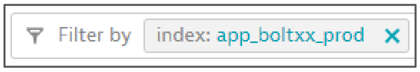
Dark

LOGS AND EVENTS

Logs and Events is the application you will use to write queries and search for logs. The following tips are not exhaustive but will help you get started with using the Logs and Events application instead of Splunk.

USE INDEXES IN YOUR SEARCH

When writing your queries, always search by index. You can find the list of indexes on this KB page: Index Glossary[1]

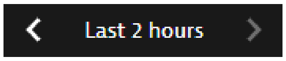


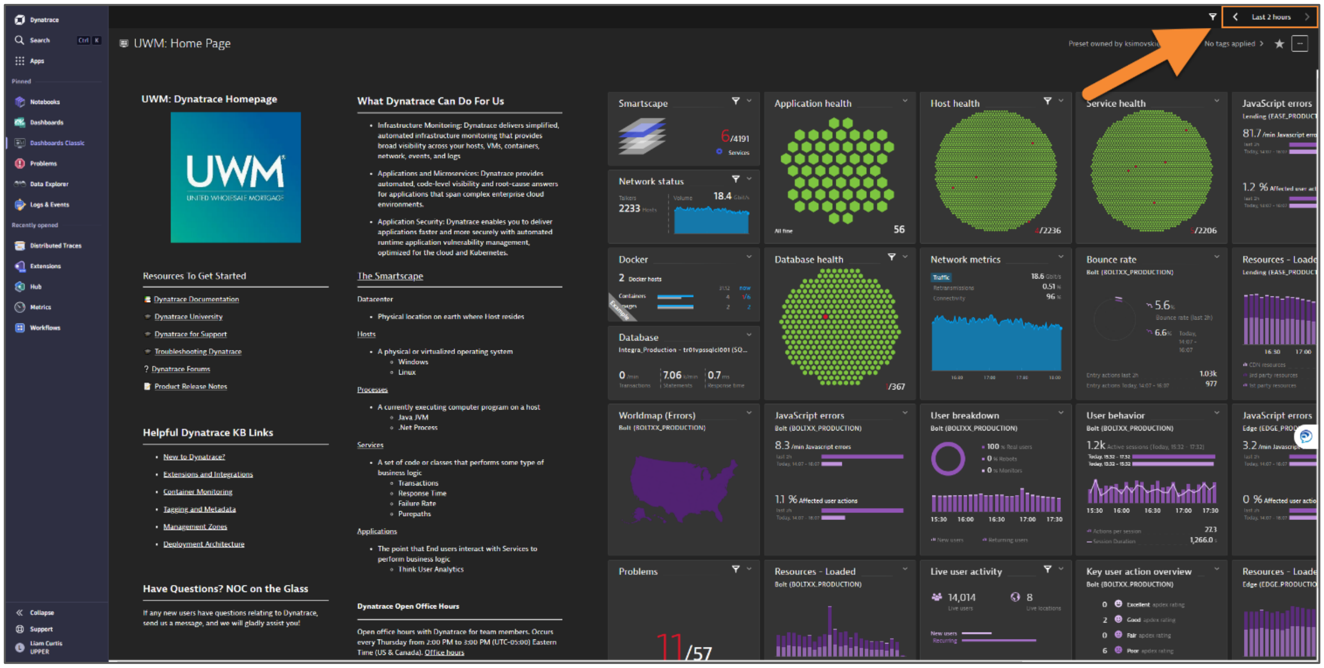
Filter by index: app_boltxx_prod ✕

NARROW YOUR TIMEFRAME

When writing your queries, keep the timeframe narrow to begin with. When querying large data sets, using smaller timeframes will result in faster results. It is best practice to start with a timeframe of 2 hours. Follow the steps below to set your timeframe.

1. Click the **timeframe** button in that upper left corner. By default, it says Last 2 hours.





UWM: Home Page

UWM: Dynatrace Homepage

What Dynatrace Can Do For Us

- Infrastructure Monitoring: Dynatrace delivers simplified, automated infrastructure monitoring that provides broad visibility across your hosts, VMs, containers, network, events, and logs
- Applications and Microservices: Dynatrace provides automated, code-level visibility and root-cause answers for applications that span complex enterprise cloud environments.
- Application Security: Dynatrace enables you to deliver applications faster and more securely with automated runtime application vulnerability management, optimized for the cloud and Kubernetes.

Resources To Get Started

- Dynatrace Documentation
- Dynatrace University
- Dynatrace for Support
- Troubleshooting Dynatrace
- ? Dynatrace Forums
- Product Release Notes

The Smartscape

Datacenter

- Physical location on earth where Host resides

Hosts

- A physical or virtualized operating system
  - Windows
  - Linux

Processes

- A currently executing computer program on a host
  - Java JVM
  - .Net Process

Services

- A set of code or classes that performs some type of business logic
  - Transactions
  - Response Time
  - Failure Rate
  - Purepaths

Applications

- The point that End users interact with Services to perform business logic
  - Think User Analytics

Helpful Dynatrace KB Links

- New to Dynatrace?
- Extensions and Integrations
- Container Monitoring
- Tagging and Metadata
- Management Zones
- Deployment Architecture

Have Questions? NOC on the Glass

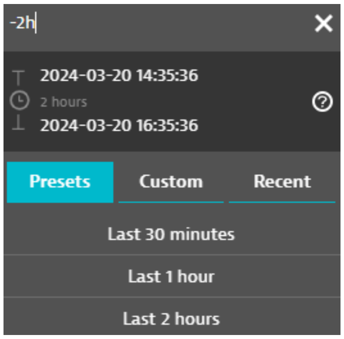
If any new users have questions relating to Dynatrace, send us a message, and we will gladly assist you!

Dynatrace Open Office Hours

Open office hours with Dynatrace for team members. Occurs every Thursday from 2:00 PM to 3:00 PM (UTC-05:00) Eastern Time (US & Canada). Office hours

[1] Index Glossary

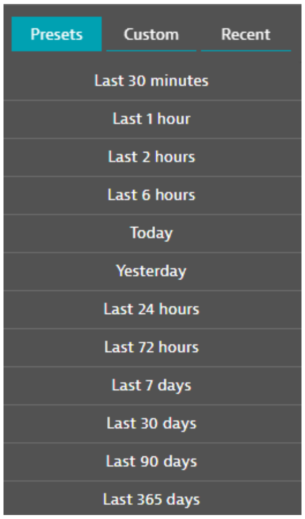
2. Adjust the **timeframe** as needed.



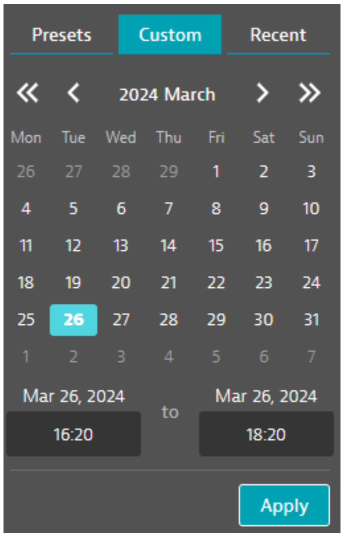
-2h

2024-03-20 14:35:36
2 hours
2024-03-20 16:35:36

Presets: Dynatrace comes with presets times built in such as last 30 minutes, 1 hour, last 2 hours, today, last 365 days, etc.



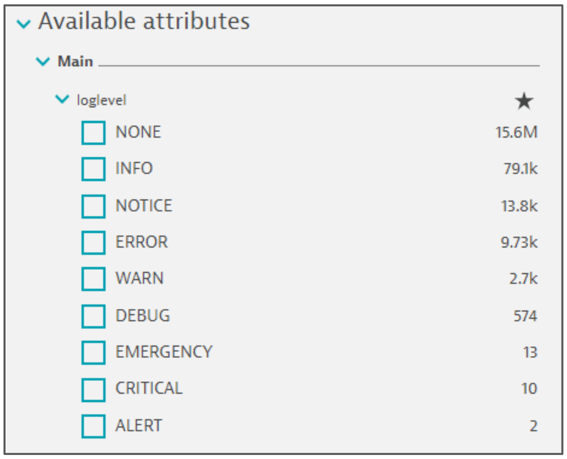
Custom: The custom tab enables you to choose the exact month, day, year, and time you want to query.



Mar 26, 2024
16:20
to
Mar 26, 2024
18:20

USE ATTRIBUTES

Using attributes can help narrow your queries and make them more precise. Some of the more common attributes you'll search for are the loglevel attributes such as error.



Available attributes

Main

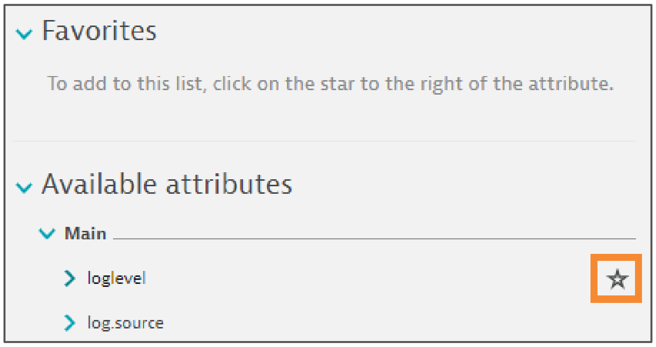
loglevel ★

□ NONE	15.6M
□ INFO	79.1k
□ NOTICE	13.8k
□ ERROR	9.73k
□ WARN	2.7k
□ DEBUG	574
□ EMERGENCY	13
□ CRITICAL	10
□ ALERT	2

FAVOURITE ATTRIBUTES

Follow the steps below to favorite your most used attributes.

1. Hover over the attribute you would like to favorite and click the star.
   Note: The star will not appear until you hover over the attribute.



Favorites

To add to this list, click on the star to the right of the attribute.

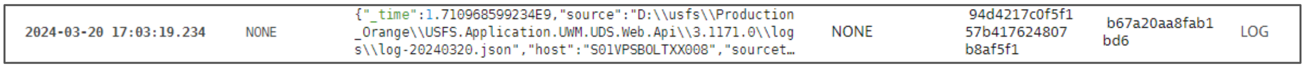
Available attributes

Main

VIEW TRACE

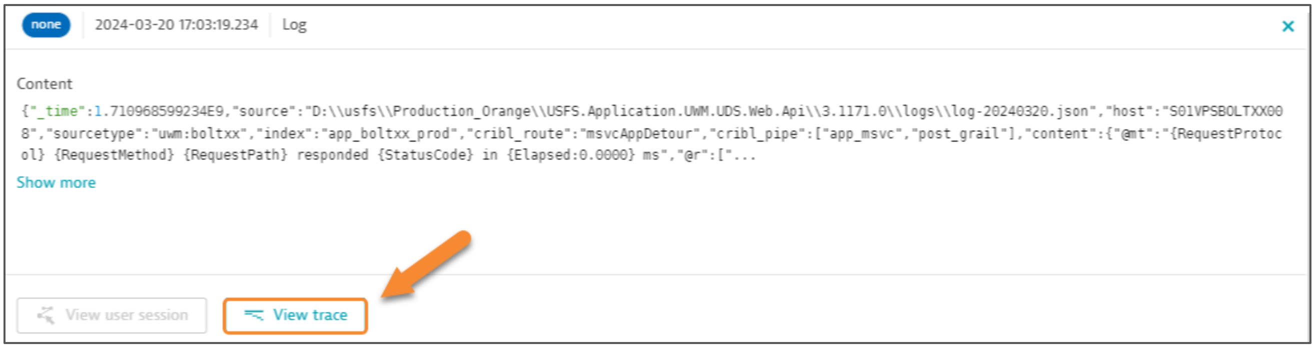
The view trace function will take you to a log's distributed trace, which can give you a more in-depth overview and enable you to dig down into code level.

1. Click the **log** you want to view.



2024-03-20 17:03:19.234	NONE	{"_time":1.710968599234E9,"source":"D:\\usfs\\Production_Orange\\USFS.Application.UWM.UDS.Web.Api\\3.1171.0\\logs\\log-20240320.json","host":"S01VPSBOLTXX008","sourcet…	NONE	94d4217c0f5f157b417624807b8af5f1	b67a20aa8fab1bd6	LOG

2. Click **View trace**.



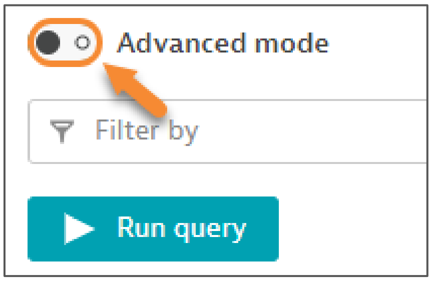
Content

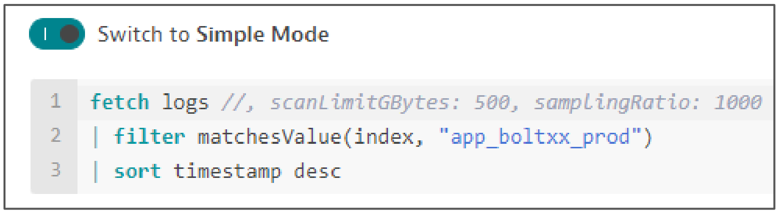
```
{"_time":1.710968599234E9,"source":"D:\\usfs\\Production_Orange\\USFS.Application.UWM.UDS.Web.Api\\3.1171.0\\logs\\log-20240320.json","host":"S01VPSBOLTXX008","sourcetype":"uwm:boltxx","index":"app_boltxx_prod","cribl_route":"msvcAppDetour","cribl_pipe":["app_msvc","post_grail"],"content":{"@mt":"{RequestProtocol} {RequestMethod} {RequestPath} responded {StatusCode} in {Elapsed:0.0000} ms","@r":["...
```

ADVANCED MODE

Advanced mode allows you to switch from the simple search mode to using DQL. DQL is Dynatrace's querying language. Writing a query using the simple search and then clicking the toggle button will automatically translate your simple search query into a DQL query. When you save a query to a notebook, it will save as a DQL query, so you'll want to familiarize yourself with the language. (See 'Open With Button' section below on how to save a query to a notebook. See the 'DQL Links' section under 'More Resources' if you'd like to learn more about DQL.)

1. Click the **toggle** next to Advanced mode.



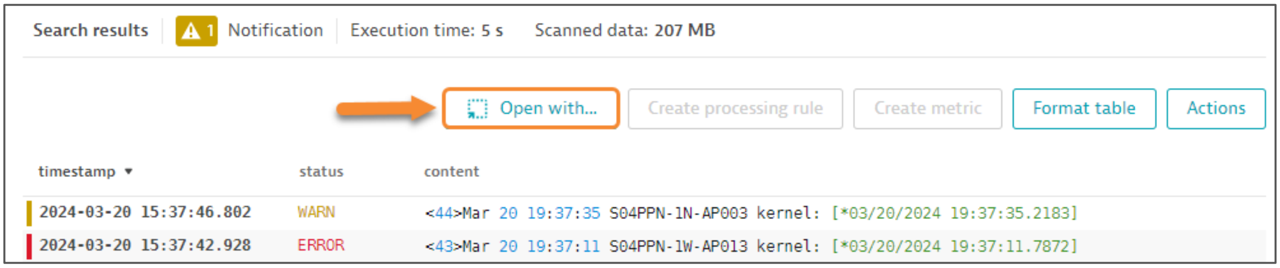


```
fetch logs //, scanLimitGBytes: 500, samplingRatio: 1000
| filter matchesValue(index, "app_boltxx_prod")
| sort timestamp desc
```

'OPEN WITH' BUTTON

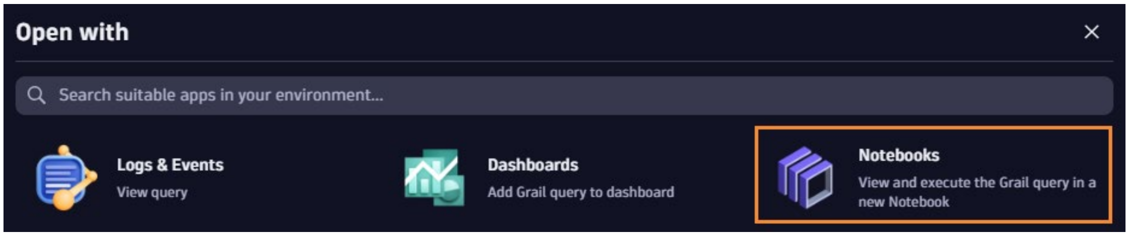
One feature in the Logs and Events page is the 'open with' button. You can use the 'Open with…' button to add log queries to your dashboard or notebooks. You will learn more about notebooks in the next section.

1. After writing a query, click **Open with…**.



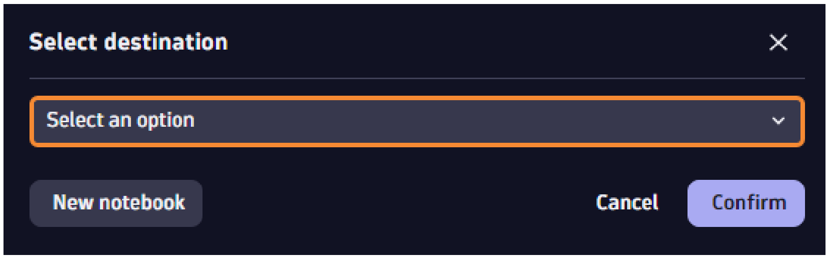
timestamp ▾	status	content
2024-03-20 15:37:46.802	WARN	<44>Mar 20 19:37:35 S04PPN-1N-AP003 kernel: [*03/20/2024 19:37:35.2183]
2024-03-20 15:37:42.928	ERROR	<43>Mar 20 19:37:11 S04PPN-1W-AP013 kernel: [*03/20/2024 19:37:11.7872]

2. Click **Notebooks**.

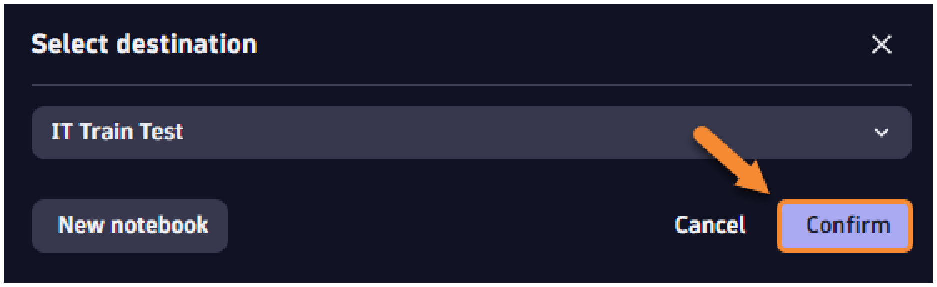


Open with
Search suitable apps in your environment...
Logs & Events
View query
Dashboards
Add Grail query to dashboard
Notebooks
View and execute the Grail query in a new Notebook

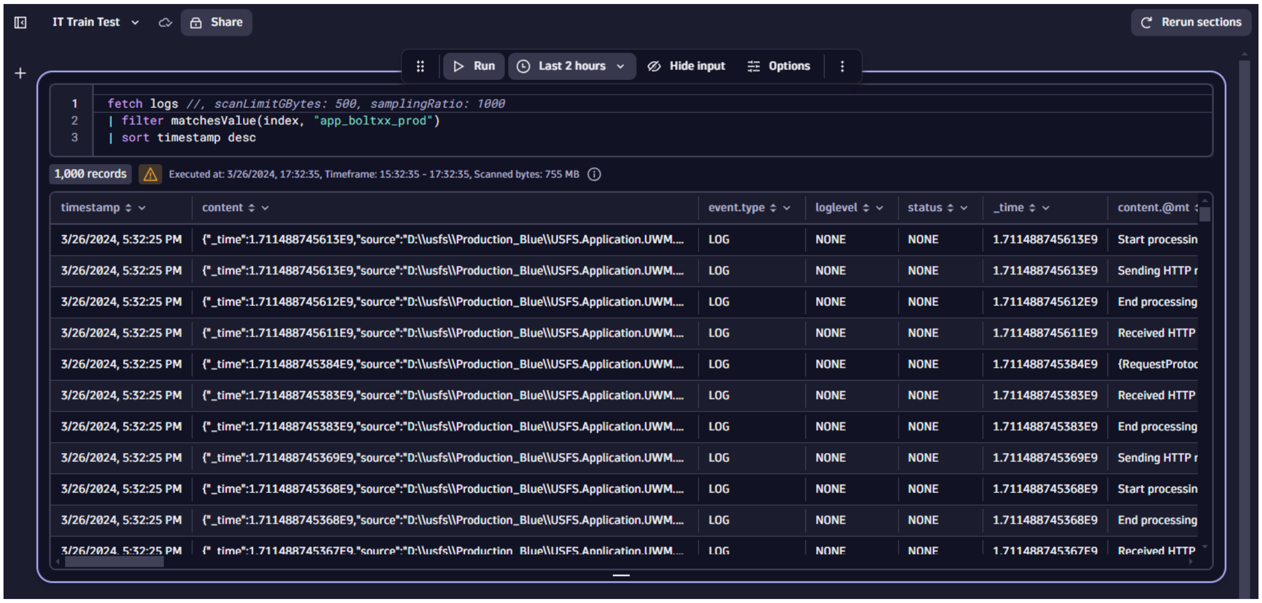
3. Select which **notebook** you'd like to add your query to (or create a new notebook).



4. Click **Confirm**.



5. After clicking confirm, the notebook you chose will open and you will see your new section with the query and logs displayed.



```
fetch logs //, scanLimitGBytes: 500, samplingRatio: 1000
| filter matchesValue(index, "app_boltxx_prod")
| sort timestamp desc
```

1,000 records ⚠ Executed at: 3/26/2024, 17:32:35, Timeframe: 15:32:35 - 17:32:35, Scanned bytes: 755 MB

timestamp	content	event.type	loglevel	status	_time	content.@mt
3/26/2024, 5:32:25 PM	{"_time":1.711488745613E9,"source":"D:\\usfs\\Production_Blue\\USFS.Application.UWM....	LOG	NONE	NONE	1.711488745613E9	Start processin
3/26/2024, 5:32:25 PM	{"_time":1.711488745613E9,"source":"D:\\usfs\\Production_Blue\\USFS.Application.UWM....	LOG	NONE	NONE	1.711488745613E9	Sending HTTP r
3/26/2024, 5:32:25 PM	{"_time":1.711488745612E9,"source":"D:\\usfs\\Production_Blue\\USFS.Application.UWM....	LOG	NONE	NONE	1.711488745612E9	End processing
3/26/2024, 5:32:25 PM	{"_time":1.711488745611E9,"source":"D:\\usfs\\Production_Blue\\USFS.Application.UWM....	LOG	NONE	NONE	1.711488745611E9	Received HTTP
3/26/2024, 5:32:25 PM	{"_time":1.711488745384E9,"source":"D:\\usfs\\Production_Blue\\USFS.Application.UWM....	LOG	NONE	NONE	1.711488745384E9	{RequestProtoc
3/26/2024, 5:32:25 PM	{"_time":1.711488745383E9,"source":"D:\\usfs\\Production_Blue\\USFS.Application.UWM....	LOG	NONE	NONE	1.711488745383E9	Received HTTP
3/26/2024, 5:32:25 PM	{"_time":1.711488745383E9,"source":"D:\\usfs\\Production_Blue\\USFS.Application.UWM....	LOG	NONE	NONE	1.711488745383E9	End processing
3/26/2024, 5:32:25 PM	{"_time":1.711488745369E9,"source":"D:\\usfs\\Production_Blue\\USFS.Application.UWM....	LOG	NONE	NONE	1.711488745369E9	Sending HTTP r
3/26/2024, 5:32:25 PM	{"_time":1.711488745368E9,"source":"D:\\usfs\\Production_Blue\\USFS.Application.UWM....	LOG	NONE	NONE	1.711488745368E9	Start processin
3/26/2024, 5:32:25 PM	{"_time":1.711488745368E9,"source":"D:\\usfs\\Production_Blue\\USFS.Application.UWM....	LOG	NONE	NONE	1.711488745368E9	End processing
3/26/2024, 5:32:25 PM	{"_time":1.711488745367E9,"source":"D:\\usfs\\Production_Blue\\USFS.Application.UWM....	LOG	NONE	NONE	1.711488745367E9	Received HTTP

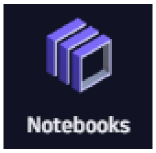
NOTEBOOKS

A new feature of the new UI, Notebooks in Dynatrace are a great resource for saving and sharing information, such as queries and visualizations. Below you will find some tips on how to use this feature. Remember, the tips shown below are not exhaustive and are just meant to get you started. Play around and look at other notebooks to see how others are utilizing them!

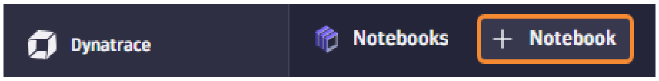
Note: It is recommended that you pin the Notebooks application.

CREATE A NEW NOTEBOOK

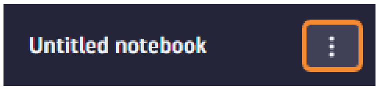
1. From the app drawer, open the **Notebooks** application.



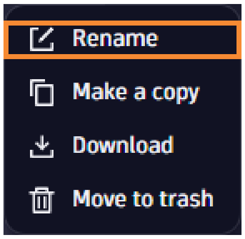
2. Click **+ Notebook**.



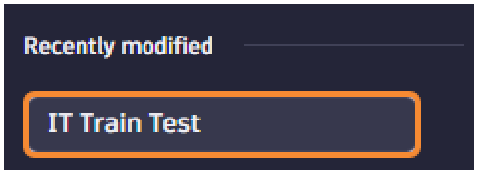
3. Click the **three dots** to the right of the notebook you just created.
Note: You must hover over the notebook to see the dots.



4. Click **Rename**.



5. **Name** your notebook.
Note: It will appear on the left under Recently Modified.

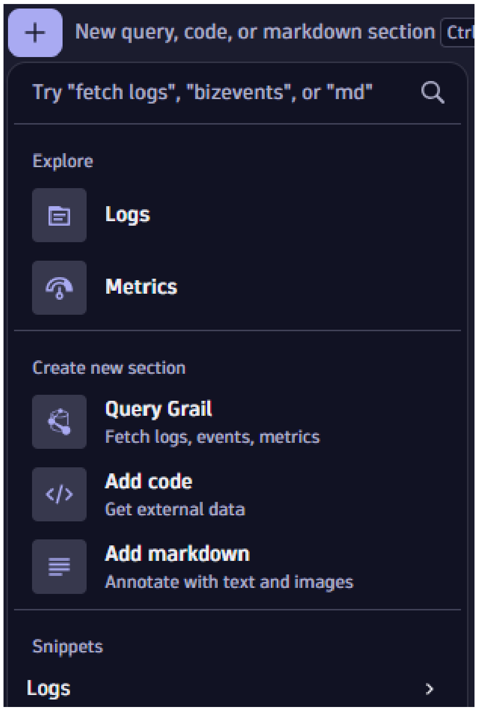


ADD SECTIONS TO AN EXISTING NOTEBOOK

You can add many different types of information to an existing notebook including markdown, queries, code, logs, metrics, etc. To add sections to your notebook, follow the steps below.

1. Click the **plus (+)** button within the notebook you want to add to.

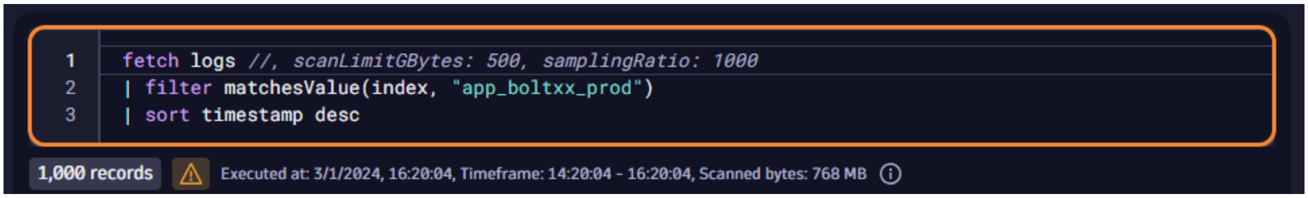
2. Pick what you would like to **add** to that section.


+ New query, code, or markdown section Ctrl
Try "fetch logs", "bizevents", or "md"
Explore
Logs
Metrics
Create new section
Query Grail
Fetch logs, events, metrics
Add code
Get external data
Add markdown
Annotate with text and images
Snippets
Logs ›

OPTIONS

Within your notebook, you can change the view of your logs more to your liking.

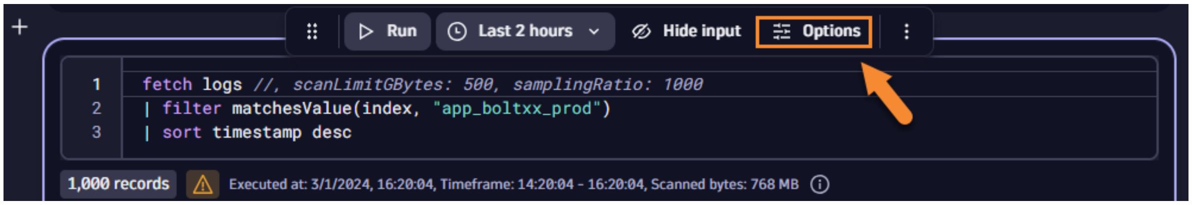
1. Click **within the query** within your notebook that you'd like change the view of.



```
fetch logs //, scanLimitGBytes: 500, samplingRatio: 1000
| filter matchesValue(index, "app_boltxx_prod")
| sort timestamp desc
```

1,000 records ⚠ Executed at: 3/1/2024, 16:20:04, Timeframe: 14:20:04 - 16:20:04, Scanned bytes: 768 MB ⓘ

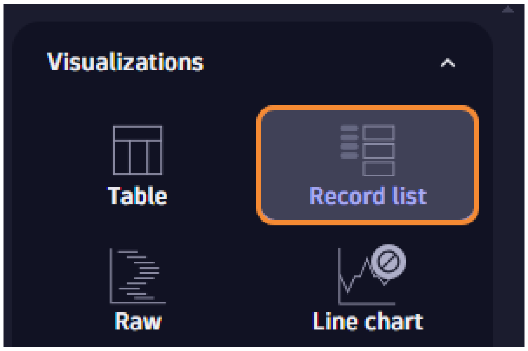
2. Click **Options**.



```
fetch logs //, scanLimitGBytes: 500, samplingRatio: 1000
| filter matchesValue(index, "app_boltxx_prod")
| sort timestamp desc
```

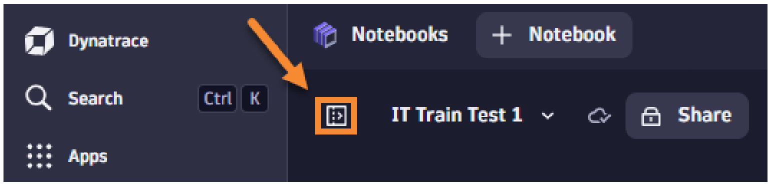
1,000 records ⚠ Executed at: 3/1/2024, 16:20:04, Timeframe: 14:20:04 - 16:20:04, Scanned bytes: 768 MB ⓘ

3. Select how you'd like to **visualize** your logs.
Note: The Record list view is closest to viewing Splunk logs.



HIDE SIDEBAR

If you are attempting to create a new notebook or switch to a different one, and the recently modified list isn't visible, click the button show below.



ADDITIONAL RESOURCES

Below you will find additional resources to support your transition from Splunk to Dynatrace.

INDEX GLOSSARY

When building a search in the Logs and Events app in Dynatrace, it is a best practice to always use indexes to narrow your search. The list of UWM indexes can be found here: Index Glossary[1]

DYNATRACE COMMUNITY OF PRACTICE (COP)

The Dynatrace CoP is a collaborative space to create an avenue for people to interact, pool resources, and work in partnership to better understand and utilize Dynatrace. The KB page is where you can go for established resources, while the Teams Channel can be leveraged to ask questions and start discussions about Dynatrace.

Dynatrace CoP KB Page[2]

Dynatrace CoP Teams Channel[3]

DQL LINKS

The simple search for Logs and Events may not be the most efficient for querying large data sets. For more advanced querying, you can leverage Dynatrace's query language DQL. Below are some resources to help you get started using DQL.

DQL Comparison (Splunk to DQL Examples)[4]

DQL Start Guide[5]

DQL Best Practices[6]

DQL Commands[7]

DQL Functions[8]

DOCUMENT HYPERLINKS

[1] https://kb.uwm.com/display/Observ/Index+Glossary

[2] https://kb.uwm.com/pages/viewpage.action?pageId=1120043979

[3] HTTPS://TEAMS.MICROSOFT.COM/L/CHANNEL/19%3AA4FD4483820D4D8D83704BF67FC810F4%40THREAD.TACV2/DYNATRACE%20COP?GROUPID=10D34A17-A496-4190-9D1B-54B7E057DDA4&TENANTID=13D3189D-22A4-4F96-BBC9-2AF46C222581

[4] https://docs.dynatrace.com/docs/platform/grail/dynatrace-query-language/dql-comparison

[5] https://docs.dynatrace.com/docs/platform/grail/dynatrace-query-language/dql-guide

[6] https://docs.dynatrace.com/docs/platform/grail/dynatrace-query-language/dql-best-practices

[7] https://docs.dynatrace.com/docs/platform/grail/dynatrace-query-language/commands

[8] https://docs.dynatrace.com/docs/platform/grail/dynatrace-query-language/functions

NOTES

Use the space given below to take any notes during your enablement session.

If you have any questions or concerns, please reach out to GRP-D-IT Observability via email.