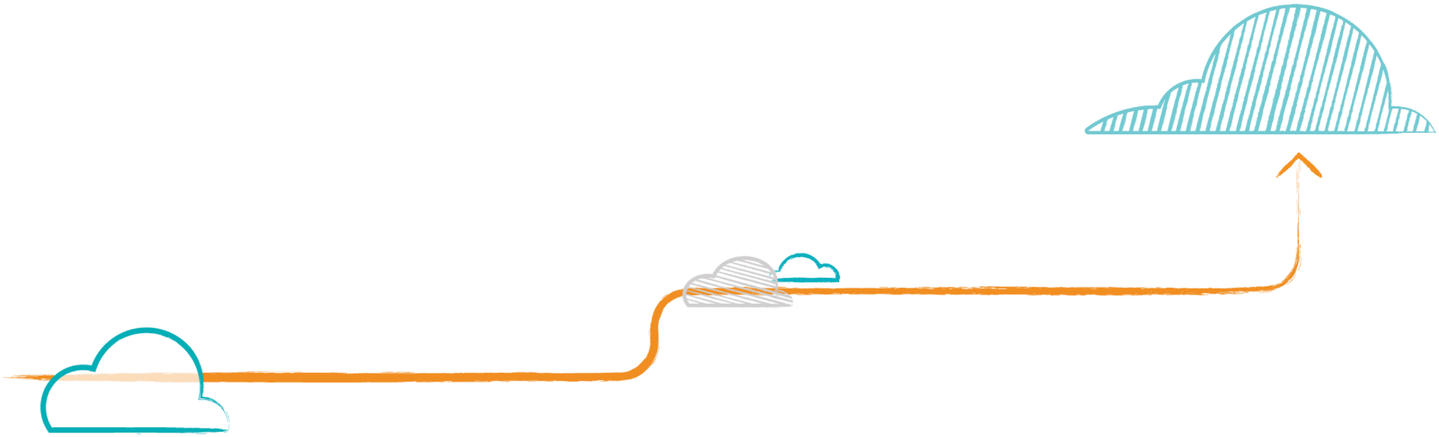
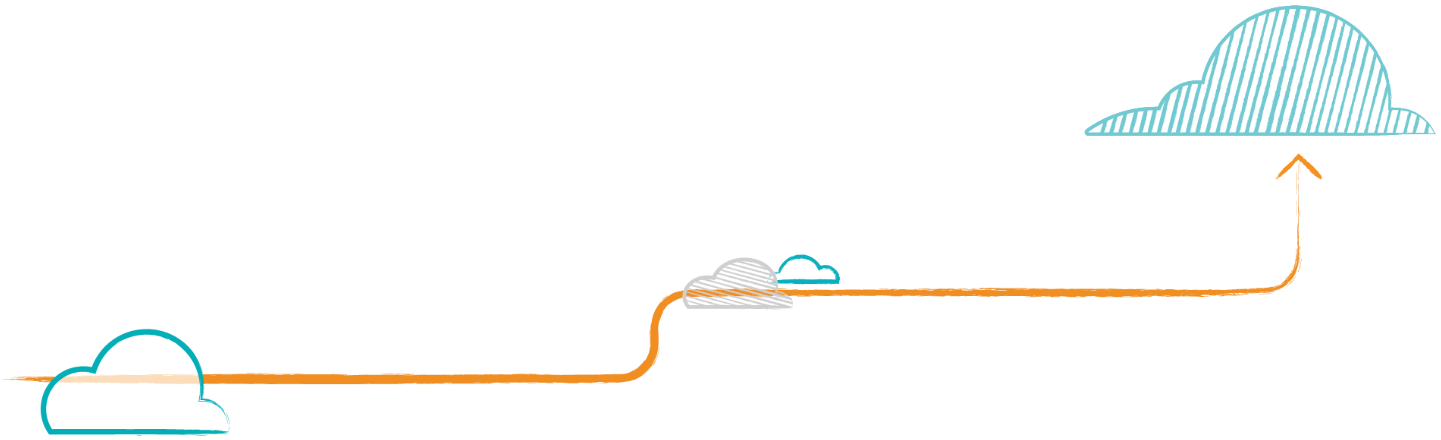
New Relic Practitioner

Lab 01 – Telemetry Data Platform



NRP: Lab 1 – Telemetry Data Platform



Introduction

This lab is intended to provide knowledge on what type of information can be verified on the New Relic Telemetry Data Platform, and where to look for each type. All the information has been instrumented up-front – on the next modules your instructor will explain how to perform the instrumentation.

Please note to begin the following lab, you must have gone through the following:

- **Please ensure you have received the username and password for the demo account!**

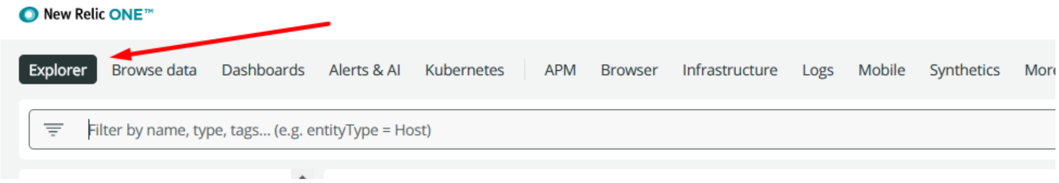
Exercise 1: Logging in and verifying the New Relic interface

Objective	*Check the New Relic user interface and get used to the main UI options.*
Context	*New Relic interface is the main point of data visualization, where every information being ingested can be easily located.*

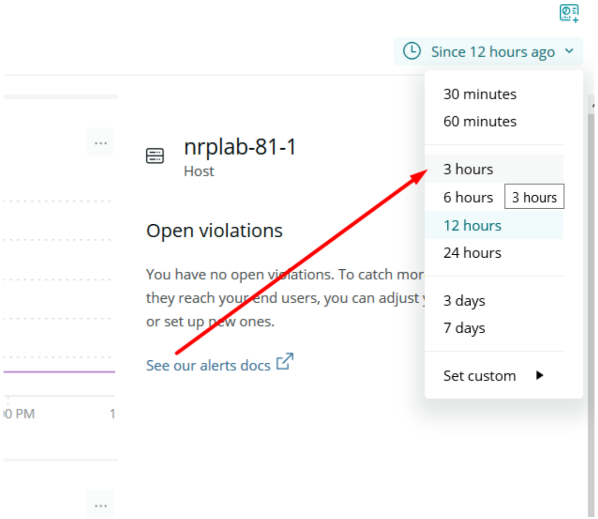
New Relic login and entities monitored

To access the New Relic UI, please proceed with the following steps:

1. From a web browser, access https://one.newrelic.com
2. Use the credentials provided by the instructor to login to the environment.
3. On the Home page, click on **Explorer**:



4. Observe the entities being monitored. Those were already added and are sending data to this specific account.
5. On the left menu, click on **Services - APM** and select any service starting with **NRP-***.
6. Observe the dashboard displayed. It shows essential information about one specific application.
7. Click on the **Explorer** menu and select **Synthetic.** Select the **Pegasus Website** monitor.
8. Observe the dashboard displayed. It shows essential information about one specific Synthetics monitor.
9. On any of the dashboards viewed, at the top right corner, select the **Time Selector** and choose another Time Period for you to observe:



nrplab-81-1
Host

Open violations

You have no open violations. To catch mor they reach your end users, you can adjust y or set up new ones.

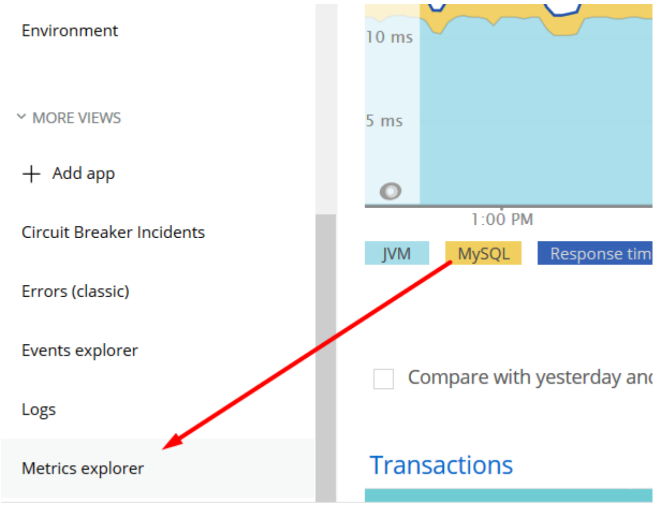
See our alerts docs

Notice the graphics will change to reflect the selected time frame and will provide information about that specific entity. Repeat this step for **Infrastructure > Hosts**.

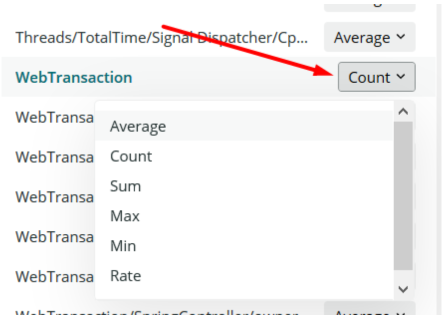
10. Now go back to the **Explorer** and select the **Synthetics** option. Select any of the checks present (Pegasus Website for example) and observe the main Dashboard. This check is verifying a specific Website for availability.
    a. Is the Website responding?
    b. What is the Website being monitored?
    c. From what locations the Website is being monitored?

Metrics analysis

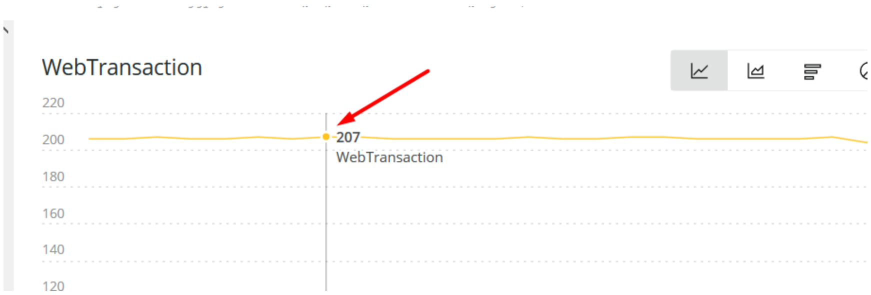
1. If not yet selected, go back again to the **Explorer** and select **Services - APM.** Choose any that starts with **NRP-*** from the list (there may be more than one). On the left side of the Service Dashboard, scroll all the way down and select, under **More Views,** the **Metrics Explorer** option:



2. Find the Metric **WebTransaction** and double click it. Select **Count** to visualize the Amount of Web Transactions executed in the period.



3. The graphic displayed will show a specific Metric that is collected from the agents installed on applications – in this case a Java application. Write down the Service name and the **count** (not average) of "WebTransaction" you see on any specific time – we will check this information later on Exercise 2.



4. Explore other metrics, for example:
    a. MySQL DB select calls
    b. Apdex
    c. Specific transactions response time (like for example "WebTransactionTotalTime/SpringController/owners")
    d. Any other metric you find interesting
5. If you have questions about any specific metric or information, ask your instructor.

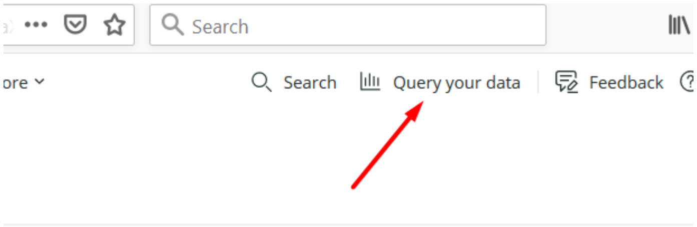
Exercise 2: Checking Events

Objective	*Learn how to see and filter/aggregate events.*
Context	*All events being sent to New Relic can be filtered, visualized, transformed and correlated to provide a better understanding on how systems are working.*

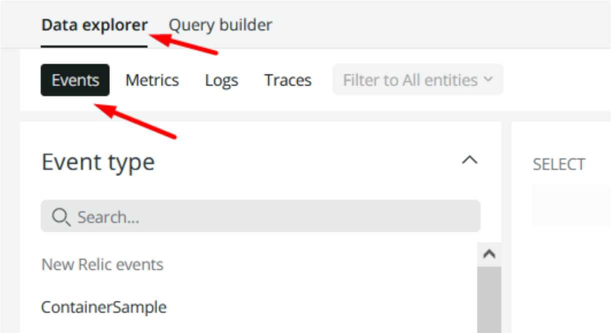
A lot of Events are captured and stored by New Relic, and can be visualized using several different ways. First, let´s take a look on the raw event information to be able to understand where those are stored.

Checking Raw event data information

1. Login to the labuser Demo account if you are not yet logged.
2. At the top menu, click "**Query your data**".



3. At this screen, you can search for any Metric, Log and Event collected by New Relic. Look for and click on **Data Explorer**, and then on **Events**.



4. Make sure the **Time Selector** is set to **30 minutes**.
5. Select the event type **ContainerSample**. On the right side, you will see a graphic, which is the event count on each specific time slice we are visualizing. If you hover the mouse cursor over the graphic, you will be able to see the count of ContainerSample events that were collected on a specific time slice (in this case, using a 30 minute timeframe, in 1 minute – this will change if you select a different timeframe, you can try it).
6. Click on the **Raw Data** button on the top right. You will see the actual events that have been recorded by New Relic. Check some aspects:
    a. The timeframes (how many per minute, is it the same amount you noticed on step 5?)
    b. Scroll right and left and check the columns title displayed (Agent Name, Command Line, Container ID, etc.). Is there any information you recognize that is being collected from a container (like IP, hostname, Image Name, etc.)?
    c. Checking one specific line (any), would you be able to tell if the container is running? And how much CPU it was using at that particular moment?
7. Select the **SyntheticCheck** Event Type on the left. Perform the same analysis (graphical, click on Raw Data, check the columns displayed).

   a. Can you see how many checks have been done in the last 30 minutes?
   b. Were they successful?

8. Select another Event Type (any other) and check the data displayed, including the Raw information.

Filtering Events

Using NRQL, Events can be easily filtered and organized in order to display the data we need. We will proceed with the most common NRQL queries to select what we need to see.

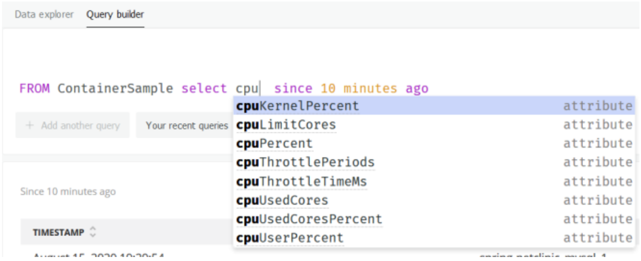
1. Click on the **Query your data** button on the top of the New Relic UI interface.
2. Select the option **Query Builder.**
3. Start by typing the following queries. This will select all event data from all container events on the last 10 minutes:

```
FROM ContainerSample select * since 10 minutes ago
```

4. The next one will get only the Container names:

```
FROM ContainerSample select name since 10 minutes ago
```

5. If you erase the word “name”, you will see an auto-complete menu. Type cpu and see the options displayed:



```
FROM ContainerSample select cpu  since 10 minutes ago
```

6. Select the option **cpuPercent**. This will show how much CPU was being used by the container at a specific time, with 1 line for each event.
7. We can perform arithmetic calculations on numbers (like the **cpuPercent** case), calculate averages, check maximums/minimums, etc. Test this by replacing **cpuPercent** by

average(cpuPercent). You should see a number with the average from the last 10 minutes.

8. If you want to see this information over time, you can add the keyword **timeseries** at the end of the NRQL sentence.
9. Try to change the time (30 mins, 2 hours, etc.) to see how the information change.
10. For now, the NRQL query should look something like this:

```
FROM ContainerSample select average(cpuPercent) since 10 minutes ago timeseries
```

11. It is possible to filter and see only one or a group of specific Events using the clause **where**. Try to add **where name=** at the end of the NRQL statement, and wait for the dropdown to help you, choosing one of the values that appear. This will change the graphic to reflect ONLY the CPU usage of the selected container.
12. We can also see the average for each entity, grouping them using the **facet <field>** keyword. Use the following NRQL to see the values broken down to each entity:

```
FROM ContainerSample select average(cpuPercent) since 10 minutes ago facet name
```

13. Now do the same steps 1-12 done previously, but use the entity **SyntheticsCheck** and perform arithmetic operations over a numeric field, like **duration.** Ask your instructor for help if you can´t find the correct NRQL syntax.
14. As a last step, execute the following query to check how many transactions from a specific service are being recorded in the last minute. Replace <SERVICE_NAME> by the service observed on the Exercise 1. Check if the information is the same (or very similar) – if not, check with your instructor:

```
FROM Transaction select count(*) where appName='<SERVICE_NAME>' since 1 minute ago
```

15. On the top right, click the **Close** button to exit the **Query your data** screen.

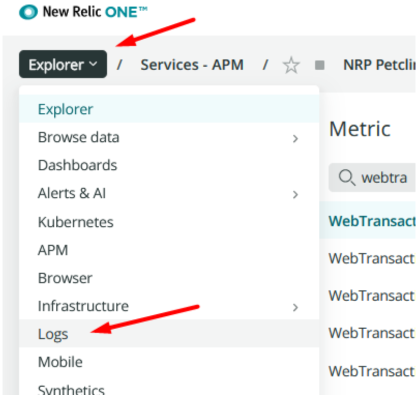
Exercise 3: Verifying log entries

Objective	*Learn how to check logs ingested by New Relic.*
Context	New Relic offer the ability to capture any type of plain text logs generated by any tool, and the logs can be visualized from a single interface. On top of this, log entries can be correlated, counted and filtered in order to generate a better comprehension of what is happening in a specific system or a group of systems

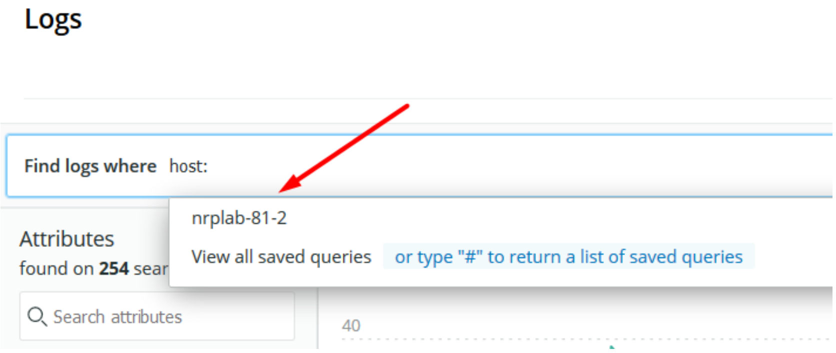
Querying logs in NRDB

Logs can be visualized from a specific interface on New Relic. To do so, use the following instructions:

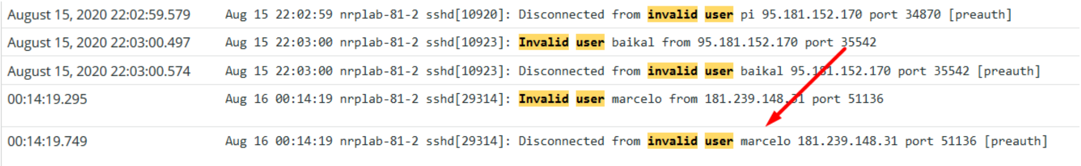
1. On the New Relic UI homepage, click on **Explorer** and the on **Logs**.



2. On the top right, at the **Time Selector** select 3 hours.
3. You will observe the logs will be displayed in the middle of the page.
4. In the **Find logs where** box, type “docker” and click on **Query logs**. You will notice that only logs containing the word “docker” will appear, and this word will be highlighted. Also, on the graphic that appears above the logs, you will see how many times this string appeared in each log.
5. Erase the word “docker” from the search, and type “host:”. You will see a dropdown box that will allow the host selection. Choose any that appears, and notice the logs will be filtered only for entries generated by that specific host.



6. Add to the search the word “service_name:”. You will notice some services that are feeding logs to New Relic. Select the <HOSTNAME>:auth service and hit enter. Now only the logs from that specific service and that specific host will be displayed.
7. Add to the search the string “Invalid user”. This will look for all SSH login attempts being made by SSH bots over the internet to that server (and hopefully failing).



```
August 15, 2020 22:02:59.579    Aug 15 22:02:59 nrplab-81-2 sshd[10920]: Disconnected from invalid user pi 95.181.152.170 port 34870 [preauth]
August 15, 2020 22:03:00.497    Aug 15 22:03:00 nrplab-81-2 sshd[10923]: Invalid user baikal from 95.181.152.170 port 35542
August 15, 2020 22:03:00.574    Aug 15 22:03:00 nrplab-81-2 sshd[10923]: Disconnected from invalid user baikal 95.181.152.170 port 35542 [preauth]
00:14:19.295                    Aug 16 00:14:19 nrplab-81-2 sshd[29314]: Invalid user marcelo from 181.239.148.31 port 51136

00:14:19.749                    Aug 16 00:14:19 nrplab-81-2 sshd[29314]: Disconnected from invalid user marcelo 181.239.148.31 port 51136 [preauth]
```

8. Clear the search and check if you can find anything related to the containers visualized on the previous Exercise 2.

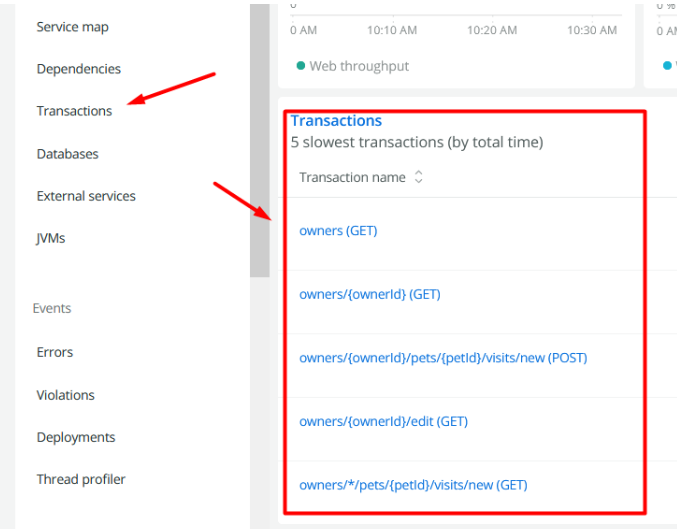
Exercise 4: Finding and analyzing traces

Objective	*Understand where to find application traces and what information is stored on it.*
Context	*When an application is being monitored, it can generate and send traces to New Relic – usually when some performance problem or slowness is observed on the execution of the application.*

Finding the transactions that will generate traces

In order to find transaction traces, we need to navigate to a specific service/application being monitored by New Relic agents or using Opentelemetry to send data.

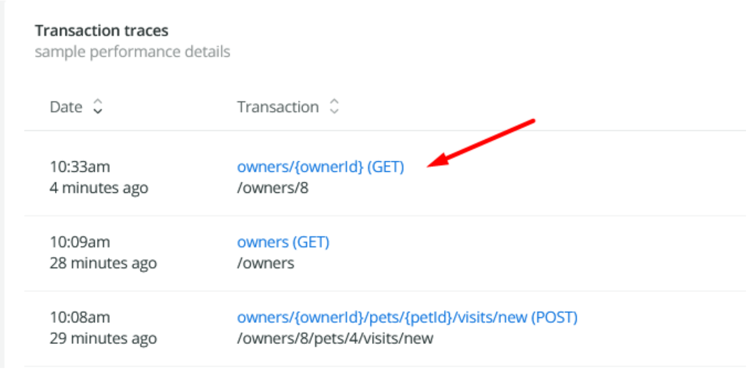
1. On the New Relic UI, click on the **Explorer**, and then on **APM.** Find and click on one of the services starting with “NRP” reporting to this account.
2. See the main dashboard. Scroll down until you find a **Transactions** section showing the Top 5 transactions on this Service. Click on **Transactions,** or you can also find the **Transactions** option on the left menu.



Transactions
5 slowest transactions (by total time)

Transaction name
owners (GET)
owners/{ownerId} (GET)
owners/{ownerId}/pets/{petId}/visits/new (POST)
owners/{ownerId}/edit (GET)
owners/*/pets/{petId}/visits/new (GET)

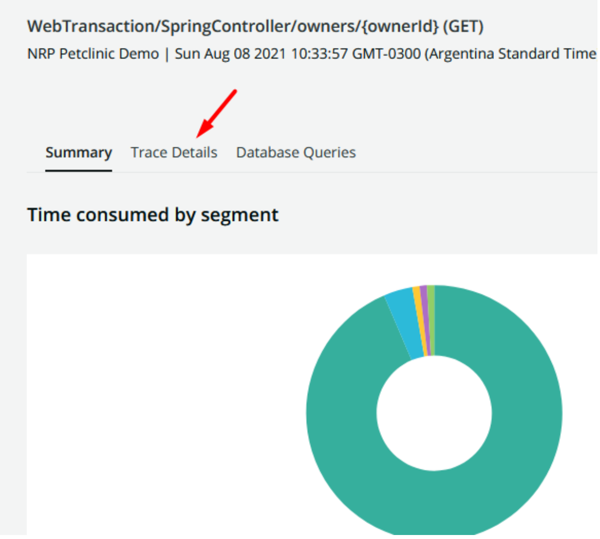
3. You will notice a more complete list of transactions for this service. On the bottom of this screen (you may need to scroll down) there will be Transaction traces listed, with the name of the transaction being clickable. If you can´t find any traces, increase the Time Selector until you find one (you may need to use 1 hour or more to see a trace – our service may be behaving just fine and not generating traces) – ask your instructor for help if you can´t find any.



Transaction traces
sample performance details

Date	Transaction
10:33am 4 minutes ago	owners/{ownerId} (GET) /owners/8
10:09am 28 minutes ago	owners (GET) /owners
10:08am 29 minutes ago	owners/{ownerId}/pets/{petId}/visits/new (POST) /owners/8/pets/4/visits/new

4. Click on one of the traces. You will notice a colored graphic showing what are the main code functions/methods executing, and how much time each one is taking. This is helpful for a DevOps admin or a Developer to understand what part of the code is taking more time or having problems.
5. On the top of the trace, click on **Trace details.**



WebTransaction/SpringController/owners/{ownerId} (GET)

NRP Petclinic Demo | Sun Aug 08 2021 10:33:57 GMT-0300 (Argentina Standard Time

Time consumed by segment

6. At this point, there is a complete breakdown of the actions executed on this transaction. This breakdown has several information, let´s try to respond some questions:
   a. What is the method/function that is taking more time?
   b. Can you see any database SQL call? If not, choose another Trace and check if you can see one.

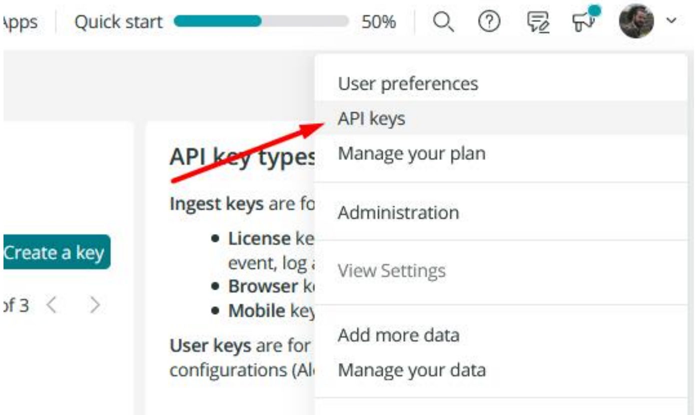
Exercise 5: Creating your own New Relic account

Objective	*Create a free New Relic account to use on the labs and to monitor systems in the future.*
Context	*Next labs will include instrumentation, so an account is needed to host all the information. We will see how to create an account for the next labs.*

If you don´t have an account yet, of if you do but can´t use this for labs, create a free account for the upcoming labs. IMPORTANT: don´t use the email you already use for an existing account (if any). If needed, create an email on some free service (Gmail, Outlook, Yahoo, etc.) to use on this account.

1. Connect to https://newrelic.com/signup?partner=NR+Partner+Program+Trials1
2. Create a login with your personal email (or using an account created as suggested).
3. Select the region where you want to store data – don´t forget it, **we will need the region for the subsequent labs.**

4. Complete the required information and proceed to the New Relic UI.
5. On the UI, click at the top right menu (with your name), and select **API keys.**



6. On this screen, you can see some all keys needed for the subsequent labs. Click on the "…" icon for the **INGEST – LICENSE** and copy it, we will be using it on next labs.
7. Explore the account, for example, on the **Manage your data** section, where you will be able to see on the next days the amount of data being sent to New Relic. You have a free limit of 100GB of data to be ingested.

What´s next?

Tell your instructor you have reached the end of Lab 1. We will be checking next how to generate all the information seen at this lab, and more.