4h Oct 24, 6:03 pm – Oct 24, 10:03 pm

Open Notebook in Datadog

Azure Incident Response

Created by **Ryan MacLean MacLean** on Oct 24

Azure Incident Response with Datadog

1. Intro

In this *quick* section we'll set up a test, assign a metric as a monitor, then go through a quick incident.

If you're reading this as a readme on GitHub, you can import the notebook's JSON file from `json_import.json` in the repository, and import it from the create notebook link in Datadog after creating a new notebook, then importing it from the top-right share icon.

> Note: if ever you need to export a notebook, from the same menu you can download as PDF or markdown (.md) or export the JSON file.

Overview

2. Synthetic Testing

In order to test the site we created earlier in the lab, we'll set up a synthetic monitor.

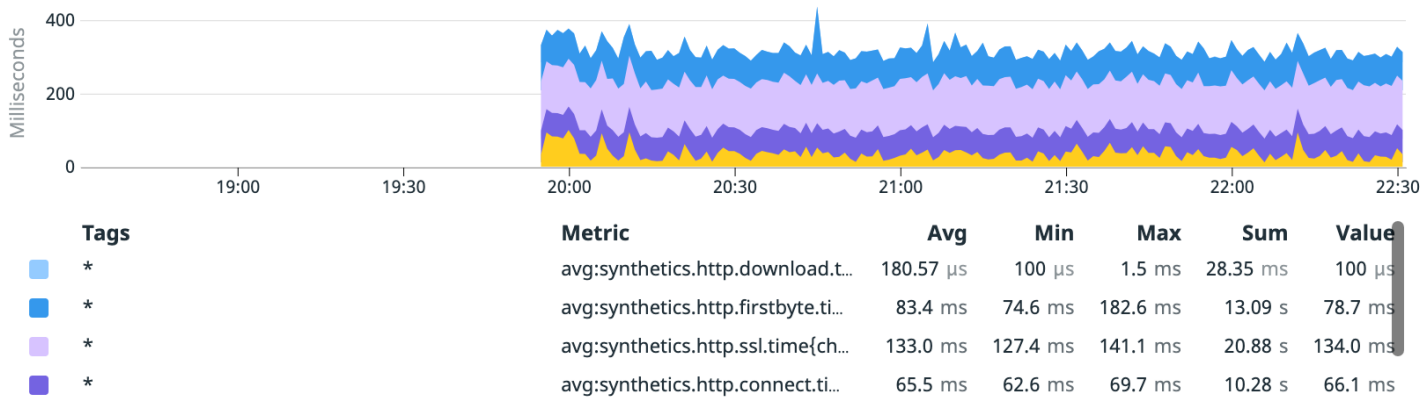
You can do that by following this link to create a multi-step syntethic test.

In a different tab, we'll need to retrieve the URL for our app service from the Azure App Services page.

After running a few tests - you can export the metrics or graphs to a dashboard (new or existing) or even add one to a notebook, as seen below!

Once you see the Network Timings graph below fill up, please proceed to the next section.

Network timings (averaged)



Tags	Metric	Avg	Min	Max	Sum	Value
*	avg:synthetics.http.download.t...	180.57 µs	100 µs	1.5 ms	28.35 ms	100 µs
*	avg:synthetics.http.firstbyte.ti...	83.4 ms	74.6 ms	182.6 ms	13.09 s	78.7 ms
*	avg:synthetics.http.ssl.time{ch...	133.0 ms	127.4 ms	141.1 ms	20.88 s	134.0 ms
*	avg:synthetics.http.connect.ti...	65.5 ms	62.6 ms	69.7 ms	10.28 s	66.1 ms

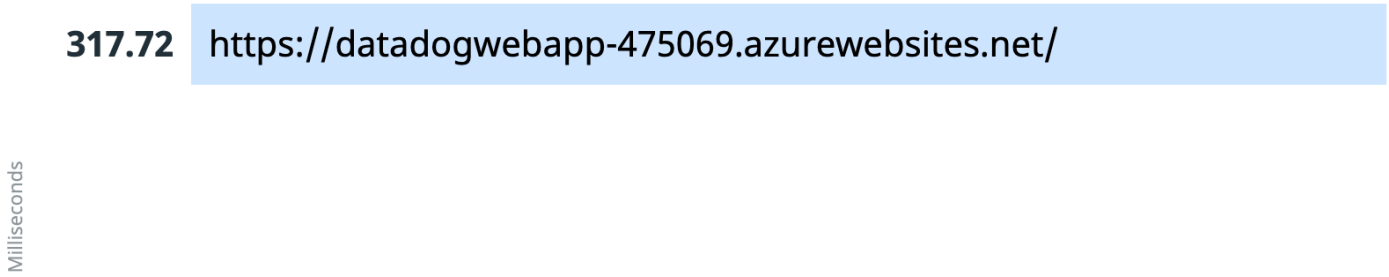
3. Monitors

Next we'll head over to the Monitors section of Datadog in order to have a look at the automatically-created monitor from our synthetic test.

It might be red, but don't panic - we're only setting things up in our development environment 😅

Because we set our alert to `@all`, everyone in our company would have received this alert. That could have been via Teams, email, or other services you've set up in order to receive alerts or notifications.

Synthetics Response Time by URL



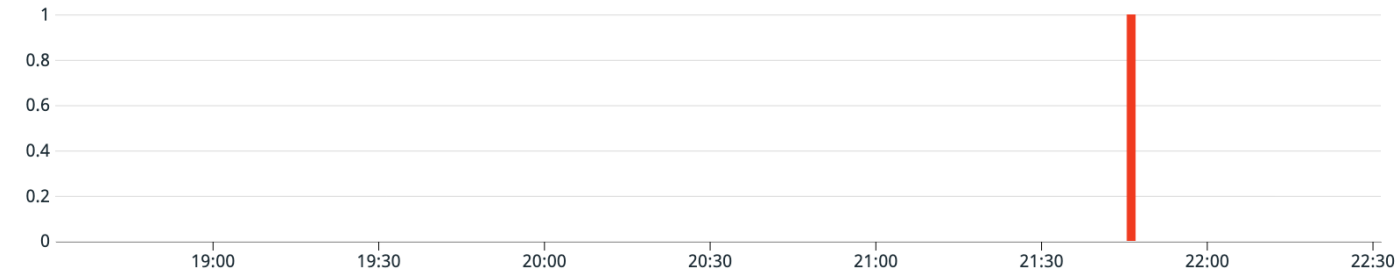
4. Creating an Incident

From the dashboard we created by exporting the Synthetics metric, we'll declare an incident.

In the incident declaration, you can set a title/summary, the severity level, pick an audience for notifications as well as context and signals (ours will be pre-filled as we created the incident from a graph).

Once the incident has been created, it will appear in the following graph of Active Incidents.

Active Incidents



Tags	Metric	Avg	Min	Max	Sum	Value
*	count[state:active]	0	0	0	0	0
commander:Ryan MacLean MacLean,state:active	count[state:active]	8e-3	0	1	1	0

5. Updating the Incident

Throughout the incident lifecycle, we'll want to update the status in order to keep team team and stakeholders up-to-date on the progress.

Note that you can also link to both live chat as well as video chat - say for example you've set up a new Teams channel programmatically in order to deal with the incident, but also a live Teams video meeting muster point (or "war room"). Both can be added as links so that others can join and get updated with one click from the header on the incident's page. *ADD IMAGE HERE*

Next we'll go over adding an update, as well as sending out a notification from within the Incident Response section of Datadog.

To do so, first add an update from the Incident Response *timeline*.

Once it has been updated, on the top-right of the Incident Response page, we'll send out a notification: *ADD IMAGE HERE*

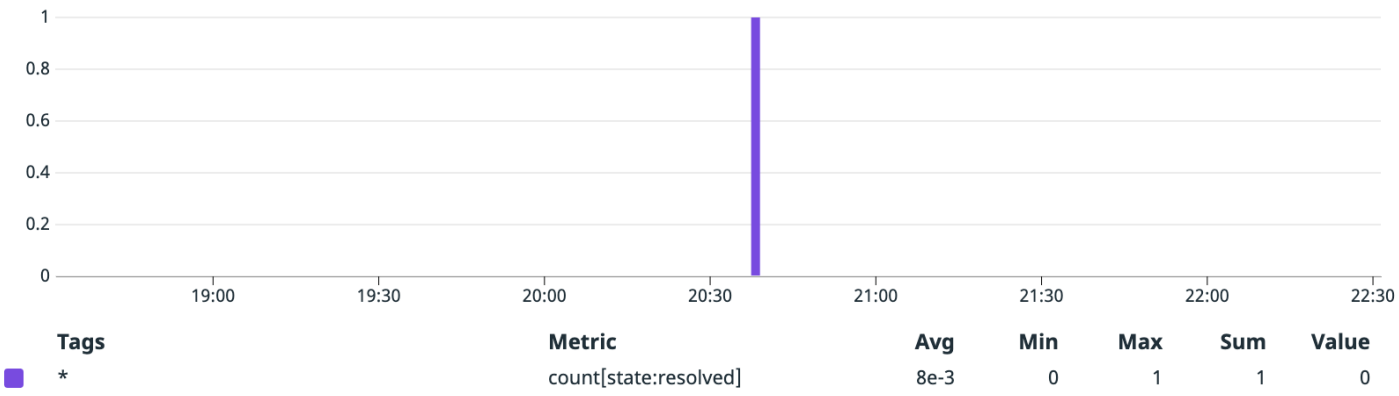
Next we'll add a task to the incident. This is like a to-do list for the team. You can assign tasks to team members as well as add a deadline, if required.

After adding a task to the incident, the Datadog Events query should show an entry for the Incident update.

6. Resolving the Incident

Once we've addressed the causes of the incident, for example via a subsequent deployment, we can then resolve it, via the status on the top-left of the Incident Resolution page.

Resolved Incidents



Tags	Metric	Avg	Min	Max	Sum	Value
*	count[state:resolved]	8e-3	0	1	1	0

7. Blameless Postmortem

Once the incident has been resolved, you would normally start the blameless postmortem process.

This means collecting a timeline of events, things that were tried, any dashboards related to the incident, etc. Since we collected these as we went along, when the postmortem is created in Datadog, it will collect all of these for you, and collect it in a notebook. Once the postmortem notebook has been created, you can then export it as markdown, JSON and/or PDF.

Link to first postmortem

8. Markdown Fun!

While working with Datadog notebooks, sometimes having a cheat-sheet handy can be helpful for those unfamiliar with Markdown, as well as to serve as a quick reminder to you while on-call.

Some Handy Markdown

Title

Sub-title

Sub-sub-title

> Note

Emphasis

Use either `_` or `*`:

bold / **bold**

italics / *italics*

Code Snippets

Single line / inline `code`

Multiline

```
for i in {1..100};
  do echo "hi from Datadog!";
done
```

Links

link

Tables

AZURE SERVICE	MONITOR
App Service	Throughput
VM	Uptime

Checklists

- [x] Checklist Item
- [ ] Unchecked

Bullets

- Bullet
- List

Numbered Lists

1. This is the first item
2. This is the second!