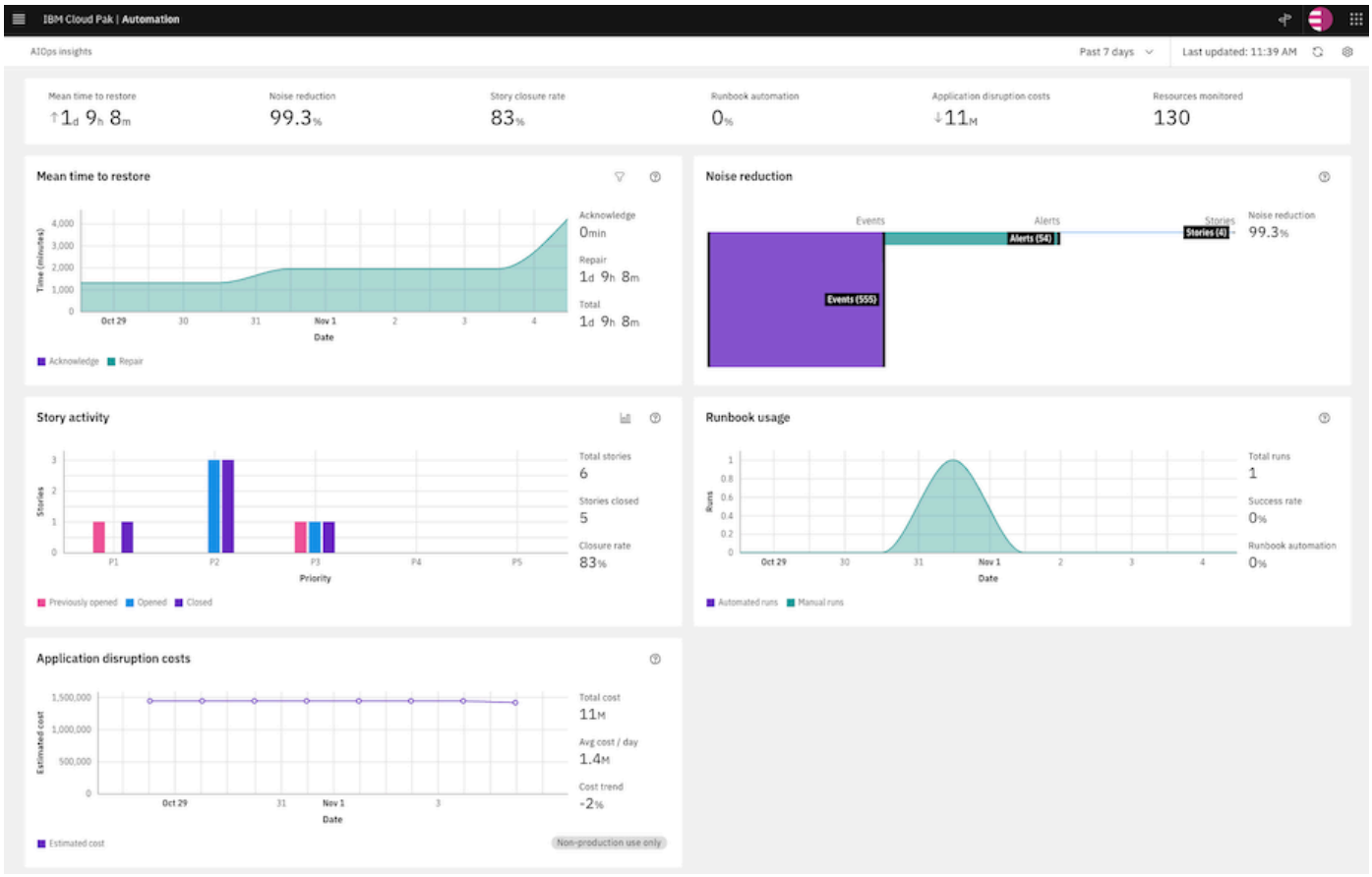
IBM AIOps

Sample Demo Script for the Click Through PPT



©2023 Włodzimierz Dymaczewski/Niklaus Hirt / IBM

1. Introduction

This script is intended as a guide to demonstrate IBM AIOps using the Click Through PPT. The script is presented in a few sections. You can utilize some or all sections depending upon your client's needs.

The script is intended to be used with the Click Through PPT.

You can watch the Demo Walkthrough video to get an idea on how to do the demo (based on 3.2).

In the demo script,

- "🚀 **Action**" denotes a setup step for the presenter.
- "📣 **Narration**" denotes what the presenter will say.
- "ℹ️ **Note**" denotes where the presenter may need to deviate from this demo script or add supplemental comments.

1.1 Key Terminology

You should be familiar with the following terminology when discussing IBM AIOps:

- **Application**: IBM IBM AIOps brings together the capability to group resources from different data types into applications. Clients can flexibly define an application to meet their business needs. With applications, you can obtain an integrated view of resources to understand inter-dependencies.
- **Event**: A point-in-time statement in IBM AIOps that tells us that something happened somewhere in a client's environment. It tells us what happened, where it happened, and when it happened. An event does not have to be exceptional or actionable, it can simply tell us something has happened.
- **Alert**: An alert in IBM AIOps represents an abnormal condition somewhere in an environment that requires resolution. It tells us what is happening, where it is happening, and when it started to happen. It may be informed by one or more events. It has a start time and end time.
- **Incident**: A incident in IBM AIOps represents an outage or reduction in service which is currently impacting customers and requires rapid remediation. It is created based on one or more trigger alerts that indicate the outage or reduction in service. Any alert of severity Major or Critical will act as a trigger alert. Other alerts that share the same cause may add context to the incident.
- **Incident**: An incident in ServiceNow is an event of interruption disruption or degradation in normal service operation. An open incident in ServiceNow implies that the customer is impacted, or it represents the business risk.
- **Topology**: A topology is a representation of how constituent parts are interrelated. In IBM AIOps, an algorithm analyzes how the event nodes are proximate to each other and groups them into a topology-based correlation.

1.2 Demonstration scenario

1.2.1 Overview

This use case shows clients how IBM IBM AIOps proactively helps avoid application downtimes and incidents impacting end-users. You play the role of an SRE/Operations person who has received a Slack message indicating that the RobotShop application is not displaying customer ratings. This is an important feature of the RobotShop application since RobotShop is the main platform from which the fictional company sells its robots.

1.2.2 Use Case

The use case demonstrates how IBM AIOps can assist the SRE/Operations team as they identify, verify, and ultimately correct the issue. The demonstration shows integration with Instana, Turbonomic, ServiceNow, and Slack. Slack is the ChatOps environment used for working on this incident.

You will demonstrate the following major selling points around IBM AIOps:

1. **Pulls data from various IT platforms**: IBM IBM AIOps monitors incoming data feeds including logs, metrics, alerts, topologies, and tickets, highlighting potential problems across incoming data, based on trained machine learning models.
2. **Utilizes AI and natural language processing**: An insight layer connects the dots between structured and unstructured data, using AI and natural language processing technologies. This allows you to quickly understand the nature of the incident.
3. **Provides trust and transparency**: Using accurate and trustworthy recommendations, you can move forward with the diagnosis of IT system problems and the identification and prioritization of the best resolution path.
4. **Resolves rapidly**: Time and money are saved from out-of-the-box productivity that enables automation and utilizes pre-trained models. A “similar issue feature” from past incidents allows you to get services back online for customers and end-users.

1.3 Demonstration flow

1. Scenario introduction
2. The Slack Incident
3. Verify the status of the Robot Shop application.
4. Understanding and resolving the incident
    1. Open the Incident
    2. Examining the Incident
    3. Acknowledge the Incident
    4. Probable Cause
    5. Similar Incidents
    6. Metric Anomalies
    7. Examine the Alerts
    8. Understand the Incident
    9. Examining the Topology
    10. Fixing the problem with runbook automation
    11. Resolve the Incident
5. Summary

1.4 Demonstration Video Walkthrough

You can watch the Demo Walkthrough video to get an idea on how to do the demo (based on 3.2).

2. Deliver the demo

2.1 Introduce the demo context

📣 **Narration**

Welcome to this demonstration of the IBM AIOps platform. In this demo, I am going to show you how IBM AIOps can help your operations team proactively identify, diagnose, and resolve incidents across mission-critical workloads.

You'll see how:

- IBM AIOps intelligently correlates multiple disparate sources of information such as logs, metrics, events, tickets and topology
- All of this information is condensed and presented in actionable alerts instead of large quantities of unrelated alerts
- You can resolve a problem within seconds to minutes of being notified using IBM AIOps' automation capabilities

During the demonstration, we will be using the sample application called RobotShop, which serves as a proxy for any type of app. The application is built on a microservices architecture, and the services are running on Kubernetes cluster.

> 🚀 **Action**
>
> Use demo introductory PowerPoint presentation, to illustrate the narration. Adapt your details on Slide 1 and 13

📣 **Narration**

Slide 2: Let' look at the environment that we have set up. Our sample application: "RobotShop" is running as a set of microservices in a Kubernetes cluster. Typically, the Operations team maintaining such application has a collection of tools through which they collect various data types.

Slide 3: Here we have several systems that are sending Events into AIOPS (slide 3), like:

- GitHub
- Turbonomic
- Instana
- Selenium
- Falcon (Sysdig)

Those Events are being grouped into Alerts to massively reduce the number of signals that have to be treated. We usually observe a ratio of about 98-99% of reduction. This means that out of 20'000 events we get about 200-300 Alerts that can be further prioritised.

Slide 4: AIOPS also ingests Logs from ElasticSearch (this could be Splunk or other Log Aggregators). The Log Anomaly detection is trained on a well running system and is able to detect anomalies and outliers. If an Anomaly is detected it will be grouped with the other Events.

Slide 5: AIOPS also ingests Metrics from Instana (this could be Dynatrace, NewRelic or others). The Metric Anomaly detection is trained on a well running system and creates dynamic baselines. Through different algorithms it is able to detect anomalies and outliers. If an Anomaly is detected it will also be grouped with the other Events.

Slide 6: Alerts that are relevant for the same Incident are packaged into a so called Incident. The Incident will be enriched and updated with information as it gets available.

Slide 7: One example is the Topology information. Not only will AIOPS tell me that I have a problem and present all relevant Events but it will also tell me where in the system topology the problem is situated.

Slide 8: Furthermore the Incident is enriched with past resolution information coming from ServiceNow tickets. I'll explain this more in detail during the demo.

Slide 9: The Stories can either be examined in the AIOPS web interface or can be pushed to Slack or Teams if your teams are using a ChatOps approach.

Slide 10: If Operations or SREs have created Runbooks, AIOPS can automatically trigger a Runbook to mitigate the problem.

ℹ️ **Note**: We are NOT using Slack in this demo.

2.2 The Slack incident

📣 **Narration**

Now let's start the demo.

> 🚀 **Action**
>
> - Click on the "Nightmare before Christmas" Tile

📣 **Narration**

In this demo I am the application SRE (Site Reliability Engineer) responsible for an e-commerce website called RobotShop, an online store operated by my company.

Imagine, it's a morning at the office, some days before Christmas and I'm just getting myself a coffe, when I receive the following slack message on my mobile, alerting me that there is some problem with the site.

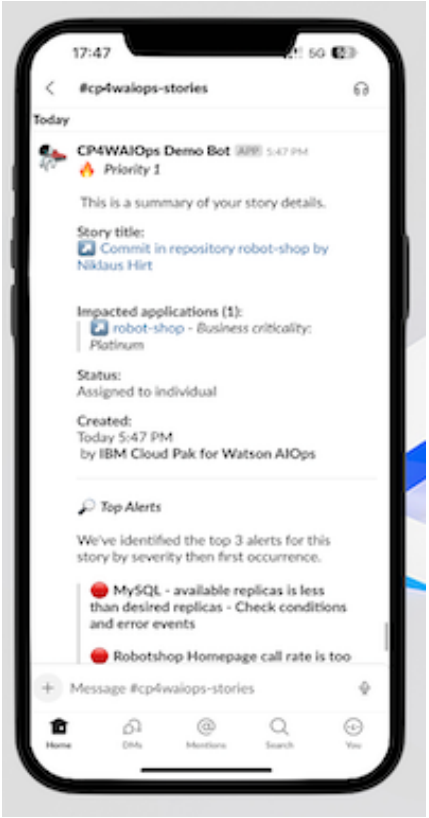
Let me check what's happening.

> 🚀 **Action**
>
> - Click on the Slack Message

📣 Narration

The Slack message has been sent from our IBM AIOps Solution, alerting me, that there is a problem with the RobotShop application, which is our online sales portal.

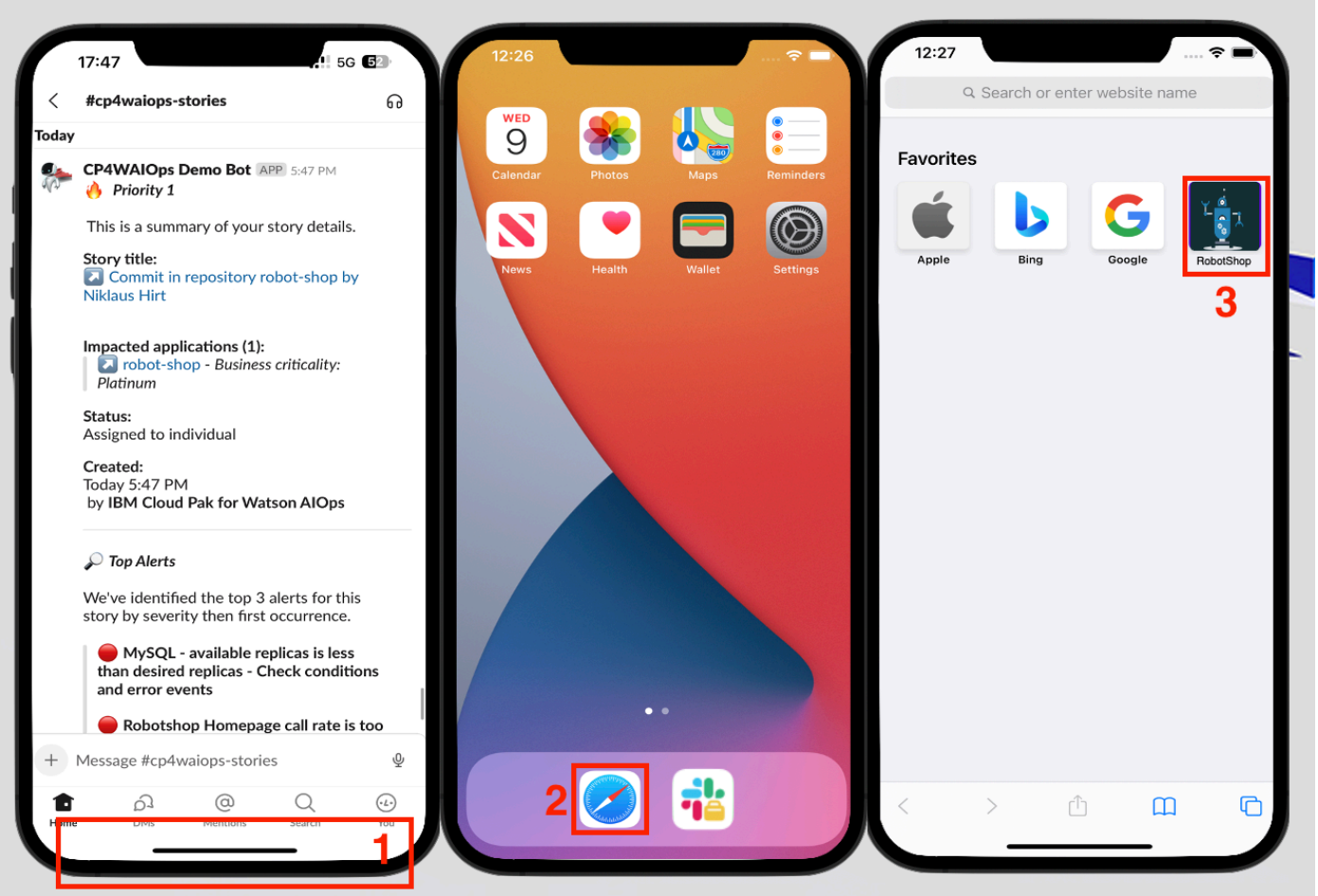
Obviously I have to make sure that the pre Christmas sales are running smoothly as this is by far the biggest quarter of the year.



2.3 Verify the status of the Robot Shop application

📣 Narration

Let me verify what's going on with the RobotShop site.



🚀 Action

- Click at the bottom of the phone (1)
- Open the Safari Browser (2)
- Click on the RobotShop bookmark (3)

📣 Narration

It seems that the application is up but displays an error that it cannot get any ratings.

📣 Narration

I know that there are many ratings for each of the products that we sell, so when none are displayed, it means that there is a likely problem with the `Ratings` service that may heavily impact client's purchasing decisions and it may well be a sign of a wider outage.

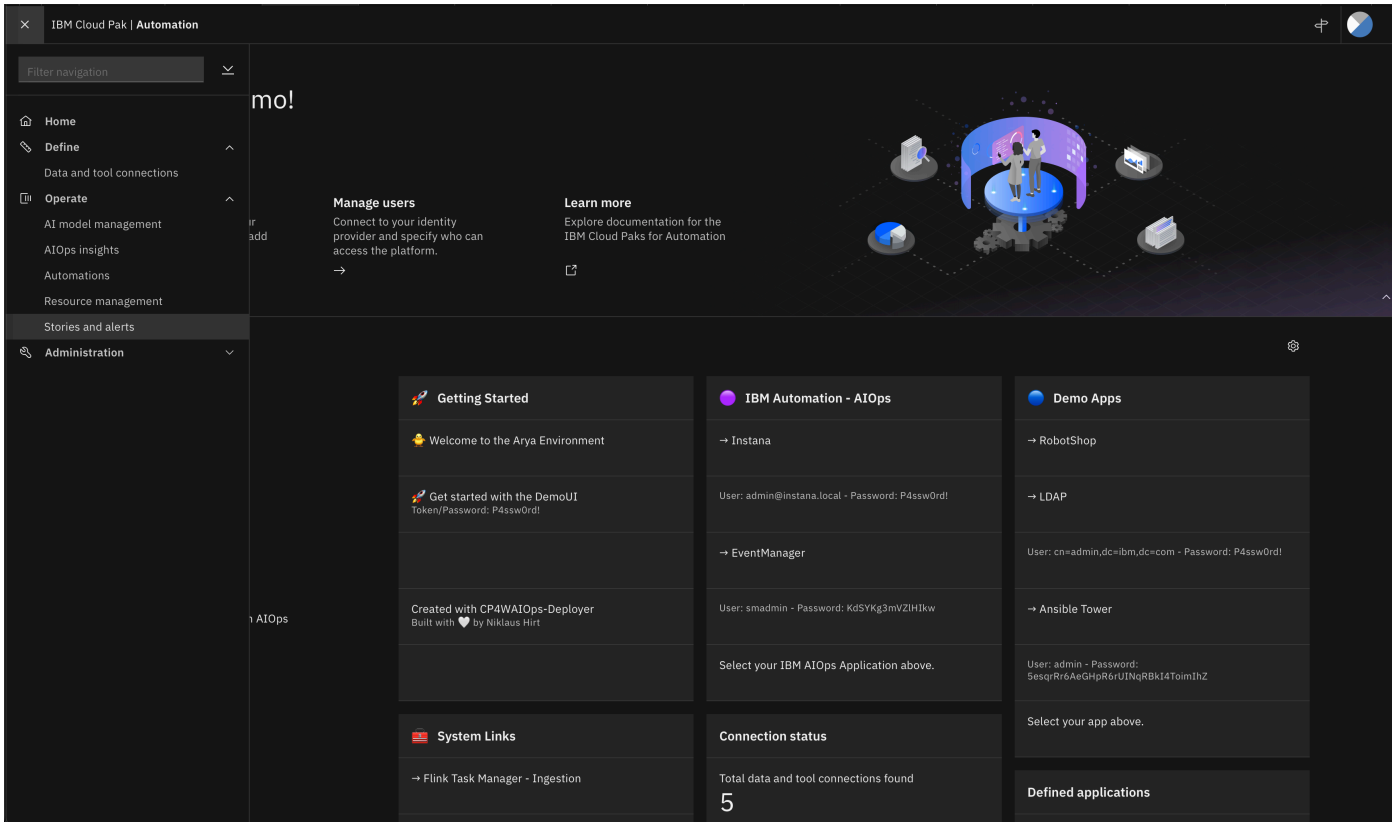
So now I'm going into my AIOps Incident Management solution to solve the problem as quickly as possible.

🚀 Action

- Click on the **IBM AIOps** icon in the left menu bar

2.4 Understanding the incident

2.4.1 Open the Incident



🚀 Action

- Click the "hamburger menu" on the upper left. Click **Stories and alerts**

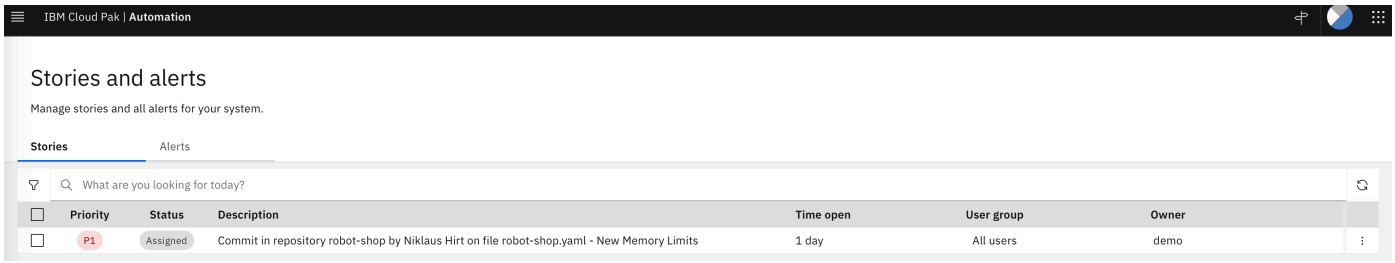
2.4.2 Examining the Incident

📣 Narration

We can see that the simulation has created a **Incident**.

The **Incident** includes grouped information related to the incident at hand. It equates to a classic War Room that are usually put in place in case of an outage.

The **Incident** contains related log anomalies, topology, similar incidents, recommended actions based on past trouble tickets, relevant events, runbooks, and more.

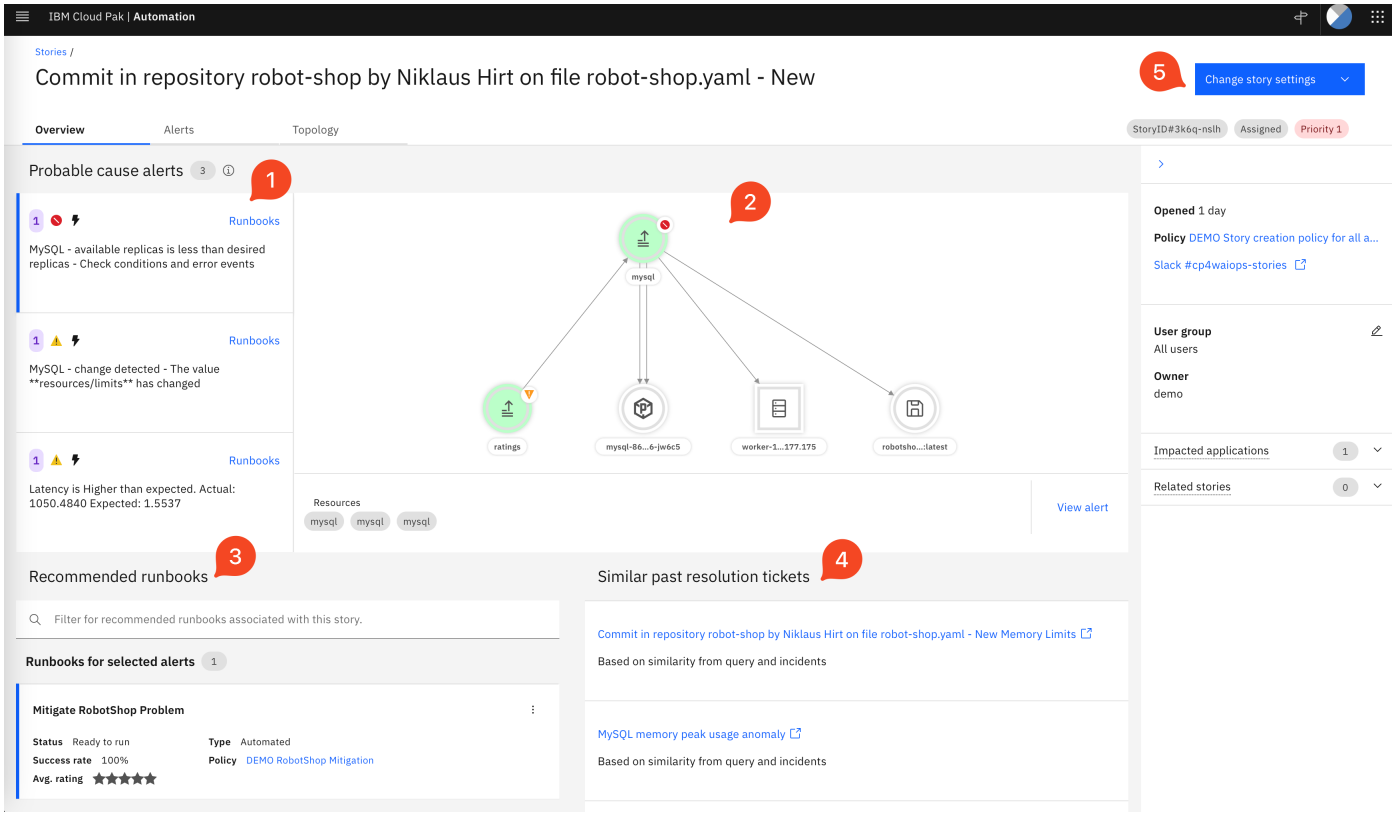


🚀 Action

- Click on the incident

📣 Narration

Now let's have a look at the **Incident**.



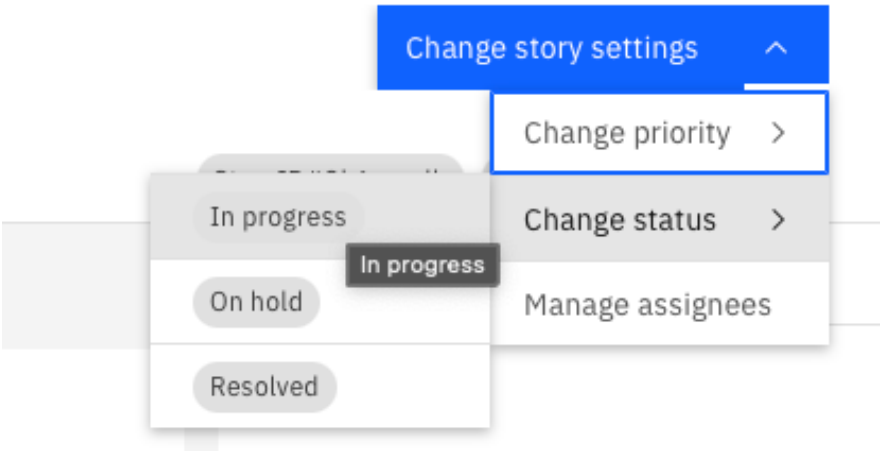
As I said before, the Incident regroups all relevant information concerning the incident at hand that have been identified by IBM AIOps.

1. A list of Alerts that have been identified by IBM AIOps to be the most probable cause
2. The localization of the problem related to the Topology
3. The suggested Runbooks to automatically mitigate the incident
4. Similar Incidents that resemble the incident at hand
5. Status of the Incident - here I can change the status and priority of the incident

2.4.3 Acknowledge the Incident

📣 **Narration**

First and before I continue examining the Incident I want to let my colleagues know that I'm working on the incident. So let me set it to In Progress.



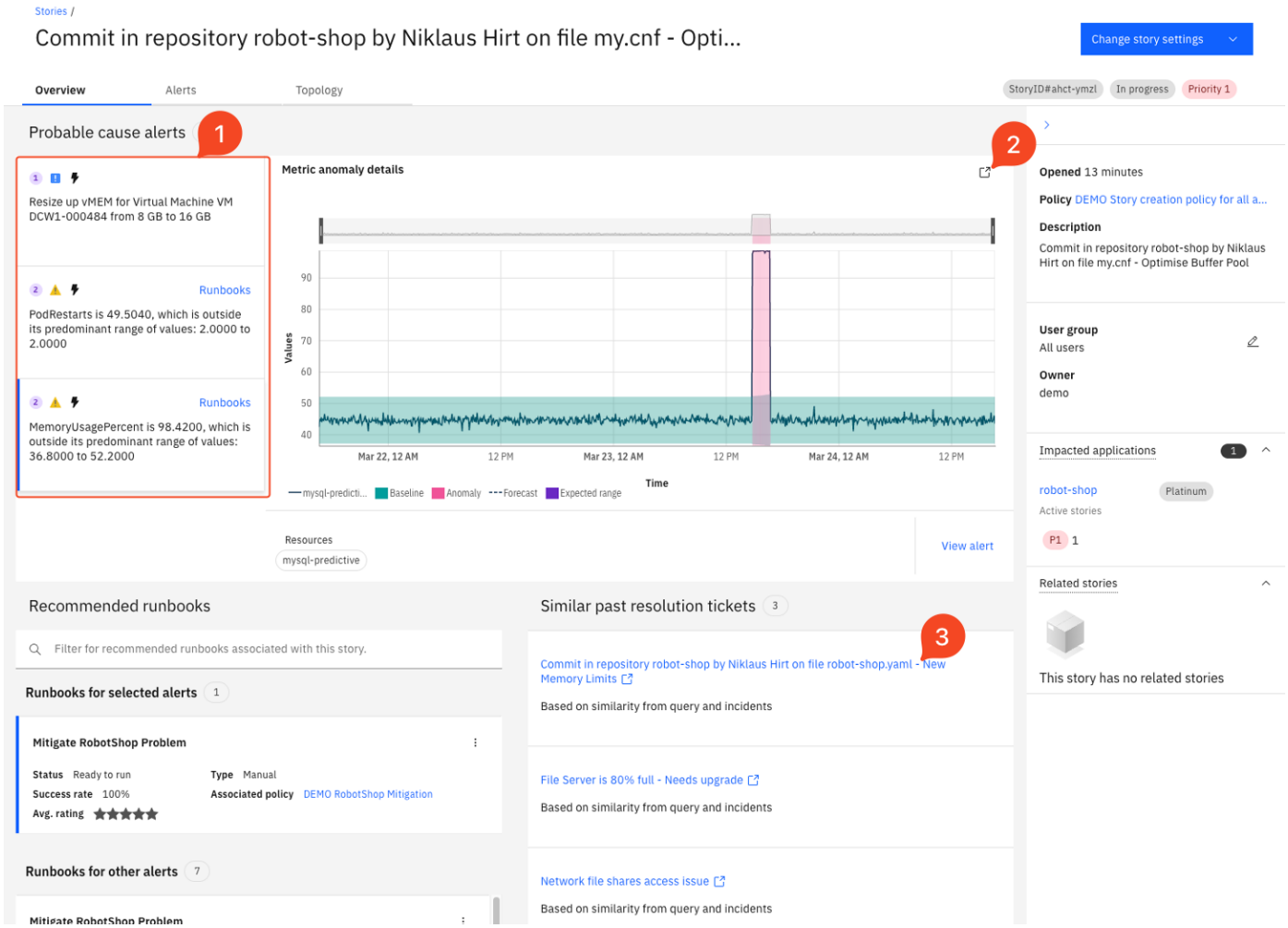
🚀 **Action**

- Click on **Change Incident Settings.**
- Select **Change Status.**
- Click on **In progress**

2.4.4 Probable Cause

📣 Narration

IBM AIOps is showing me the Alerts that are most likely to be at the heart of the Problem. We call this **Probable Cause**.



🚀 Action

- Click on **PodRestarts** in Probable Cause (1).
- Click on **Memory Usage** in Probable Cause (1).

2.4.5 Similar Incidents

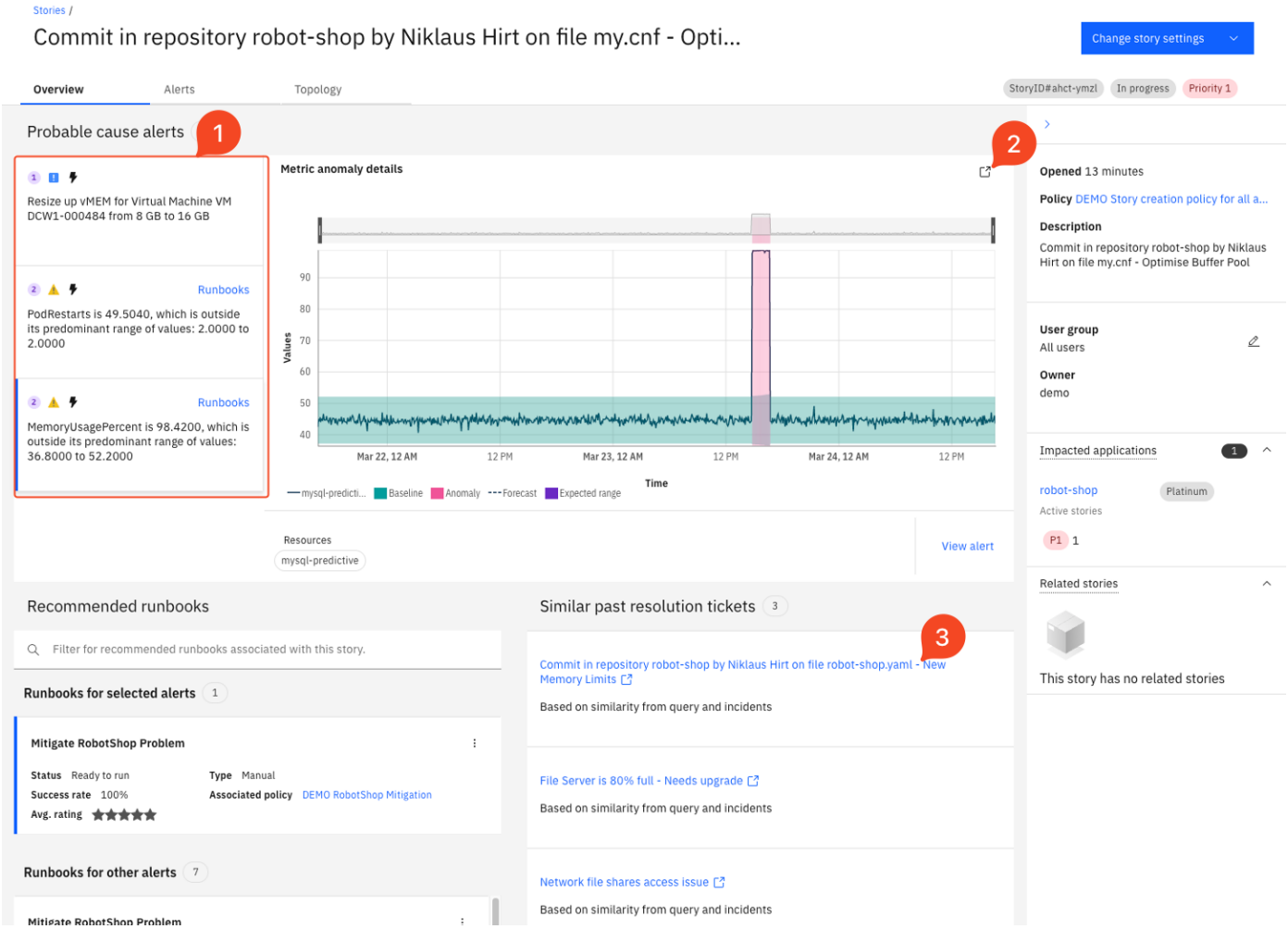
📣 Narration

Most large organizations use IT Service Management tools to govern processes around IT. Our organization is using ServiceNow for that purpose. Past incidents with resolution information are ingested and analysed by IBM AIOps to train on exisitng tickets and extracting the steps used to fix previous incidents (if documented) and recommend resolutions. This AI model helps you discover historical incidents to aid in the remediation of current problems.

So for the **Incident**, your team is presented with the top-ranked similar incidents from the past, so no need to manually search for past incidents and resolutions, which is time-consuming.

In this particular example I can see that the problem was related to a GIT Commit that massively reduced the resources on the mysql Database.

Let me check how the problem was resolved for this incident.

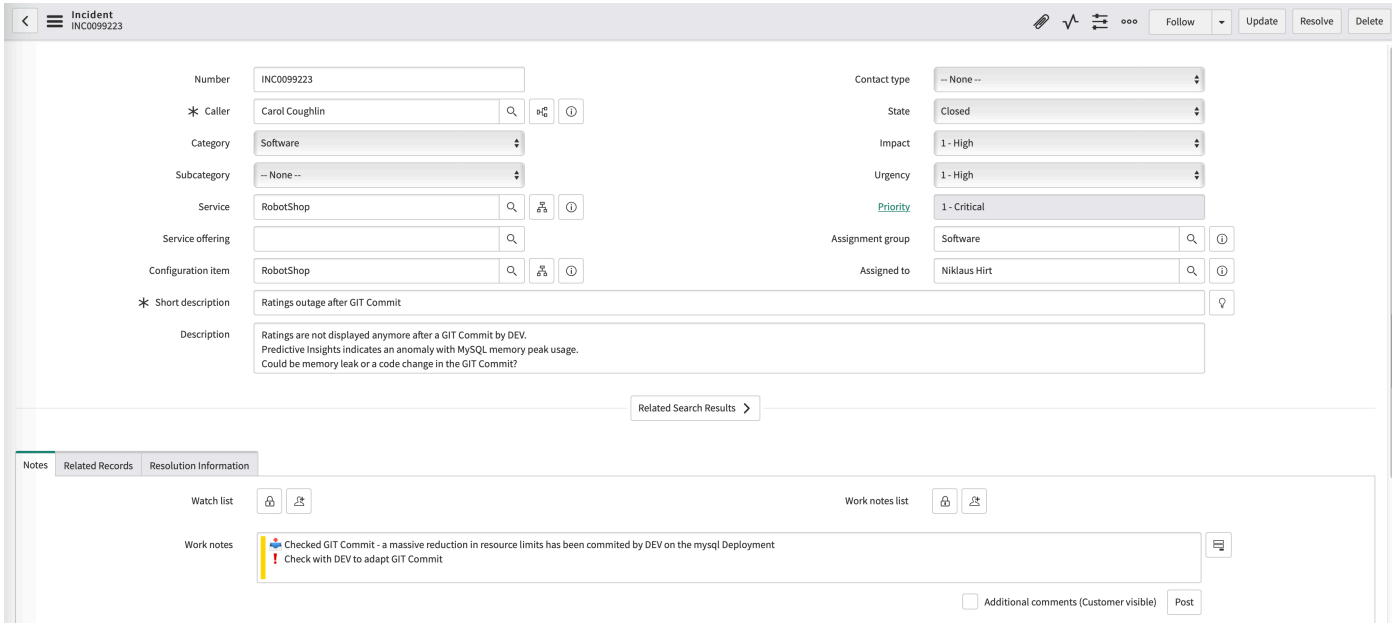


🚀 Action

- Click the first similar resolution ticket (3)

📣 Narration

When I open the ticket in ServiceNow, I see that there has been a similar problem with the the mysql database and a Runbook had been created to mitigate the problem.

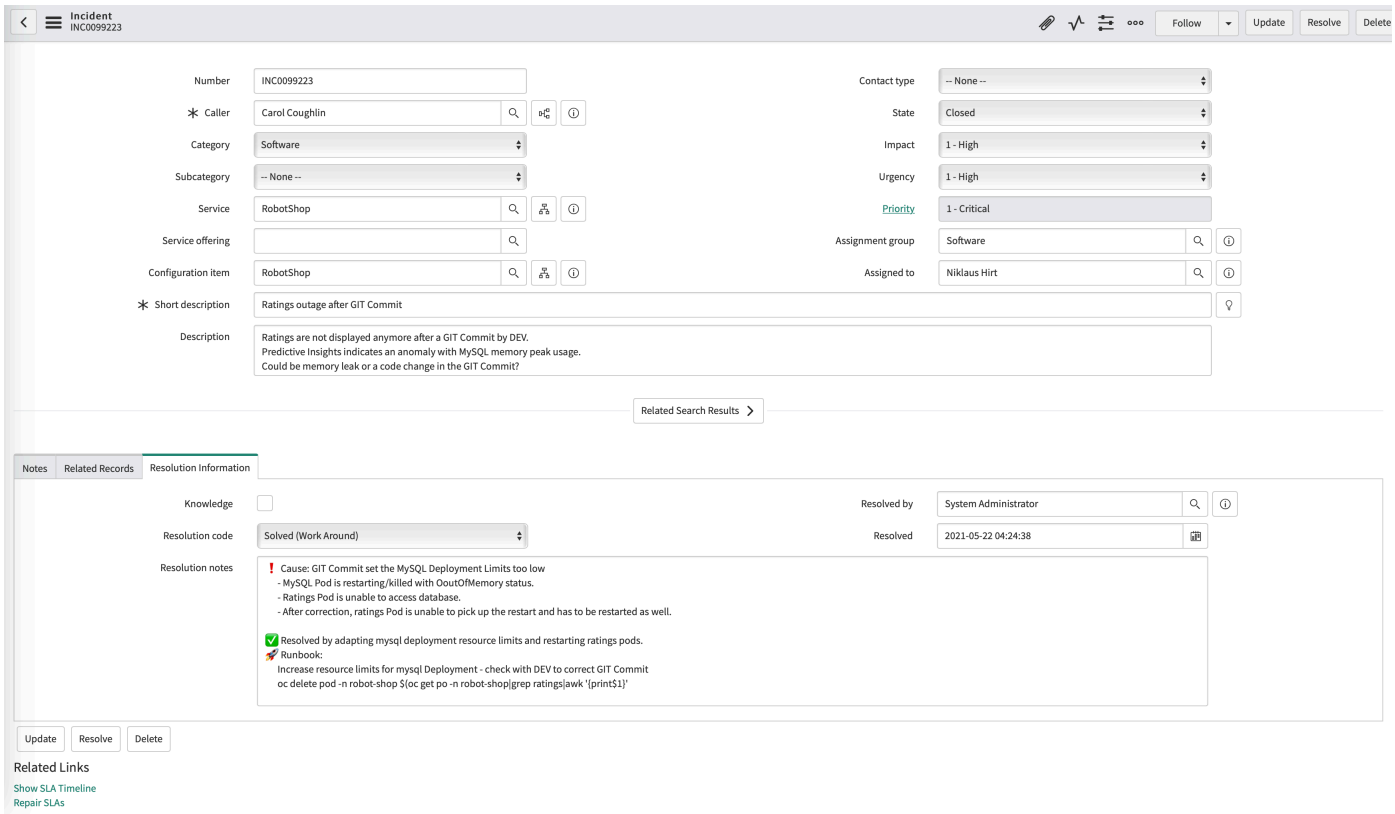


❗ **Note**: In the Robot Shop demo scenario, the integration with ServiceNow is simulated with the static content.

🚀 Action

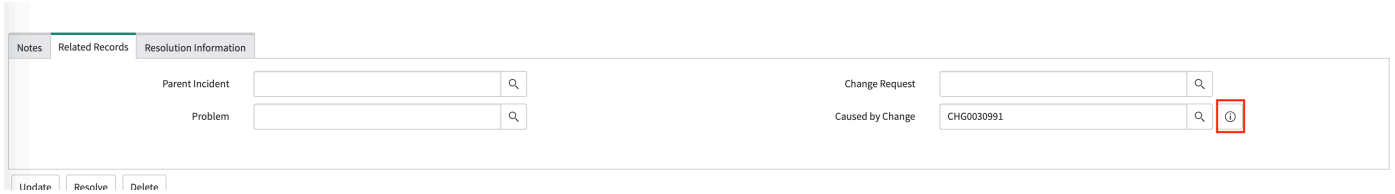
- Click on the **Resolution Information** Tab

Resolution Information



📣 Narration

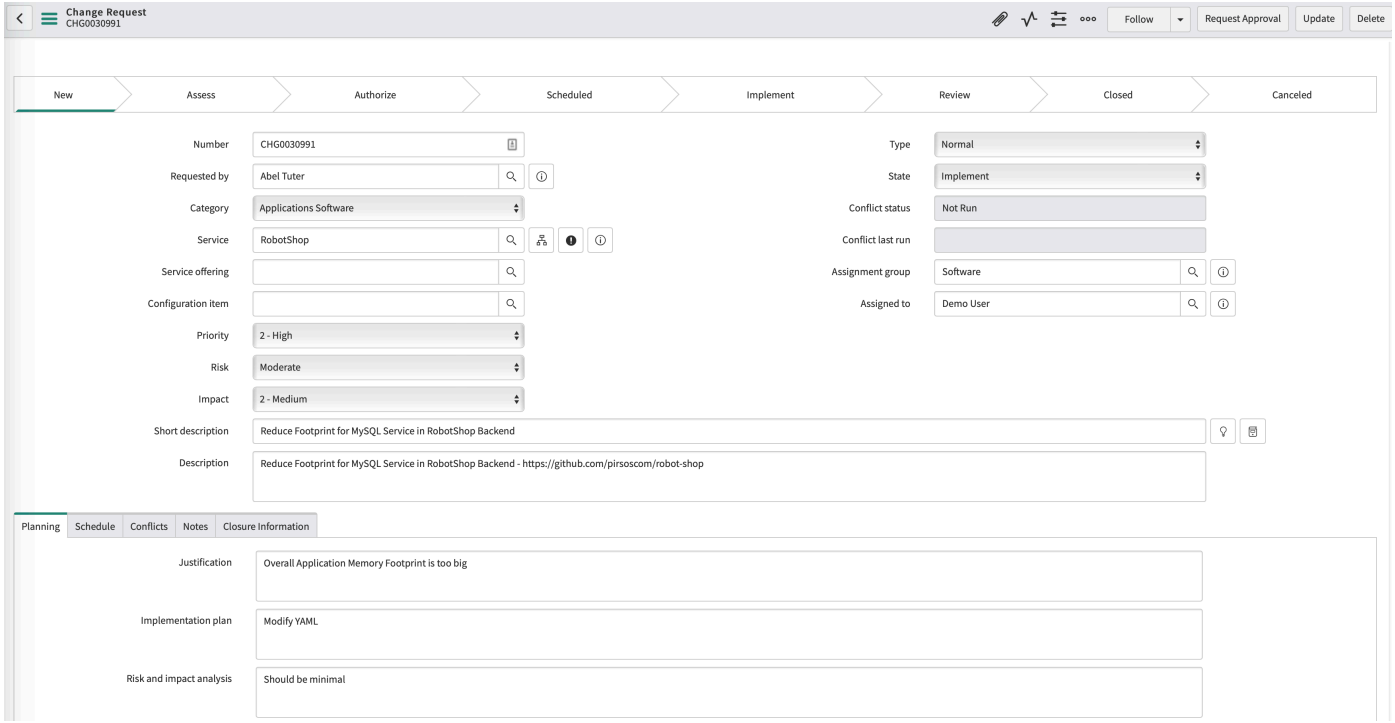
It seems that it was resolved by changing the mysql deployment and a Runbook had been created to mitigate the problem. To finish up, I will check if the incident was related to an official change.



🚀 Action

- Click on the **Related Records** Tab
- Click on the **i** Button next to **Caused by Change**

Examine the Change



📣 Narration

Ok, so now I can see that the problem is related to a Change that aims to reduce the footprint of the mysql database.

As it's still ongoing, chances are high, that the development team recreated a similar problem.

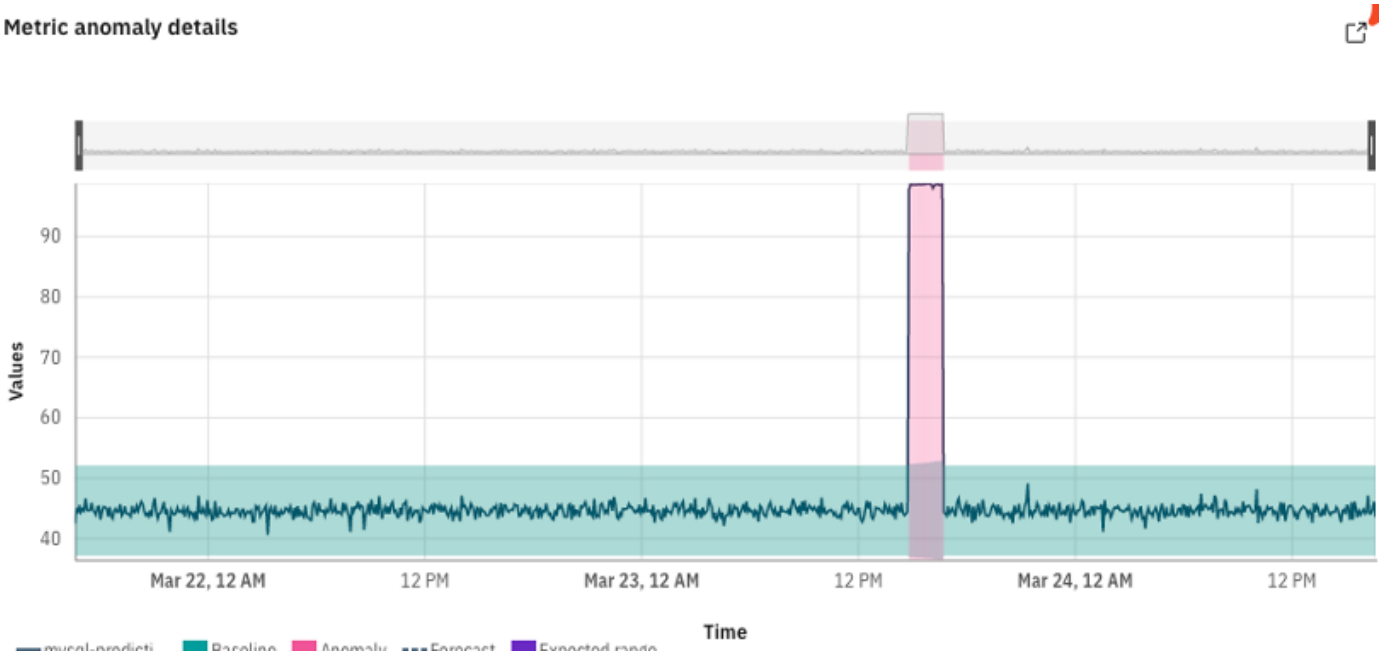
Obviously, in real life I would now start the Runbook to see if it resolves the problem.
But for the sake of the demo, let's dig a little deeper first.

So let me go back to the incident.

🚀 Action

- Close the ServiceNow page by clicking the **IBM AIOps** Icon.

2.4.6 Metric Anomalies



📣 Narration

- IBM AIOps is capable of collecting metrics from multiple sources and detecting **Metric Anomalies**. It was trained on hundreds or thousands of metrics from the environment and constructs a dynamic baseline (shown in green). The graphic suddenly turns red which relates to detected anomaly when the database is consuming a higher amount of memory than usual.

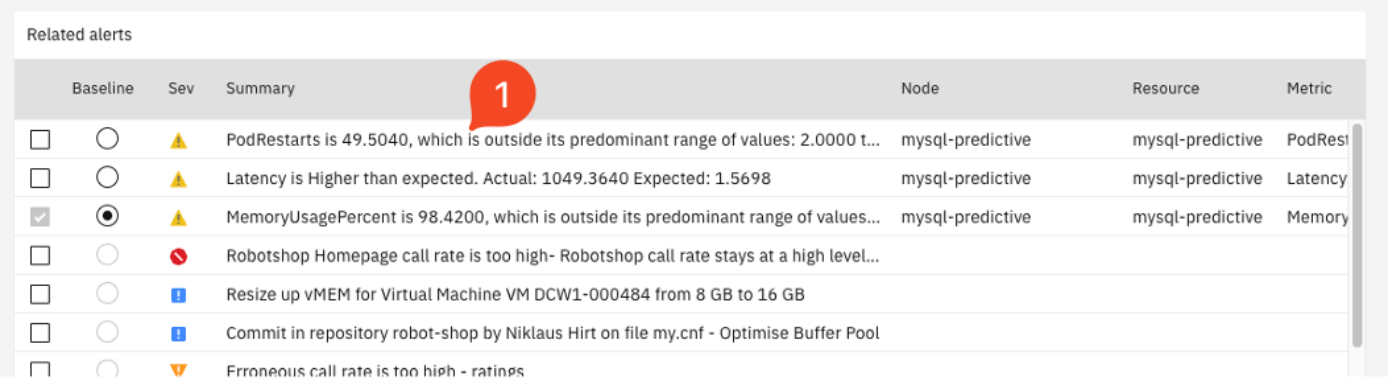
Let's see the details of what is wrong with my metrics.

🚀 Action

- Click on the button (2) in the upper right of the metrics graph.

📣 Narration

You can display several alerts at the same time to better understand the temporal dependencies

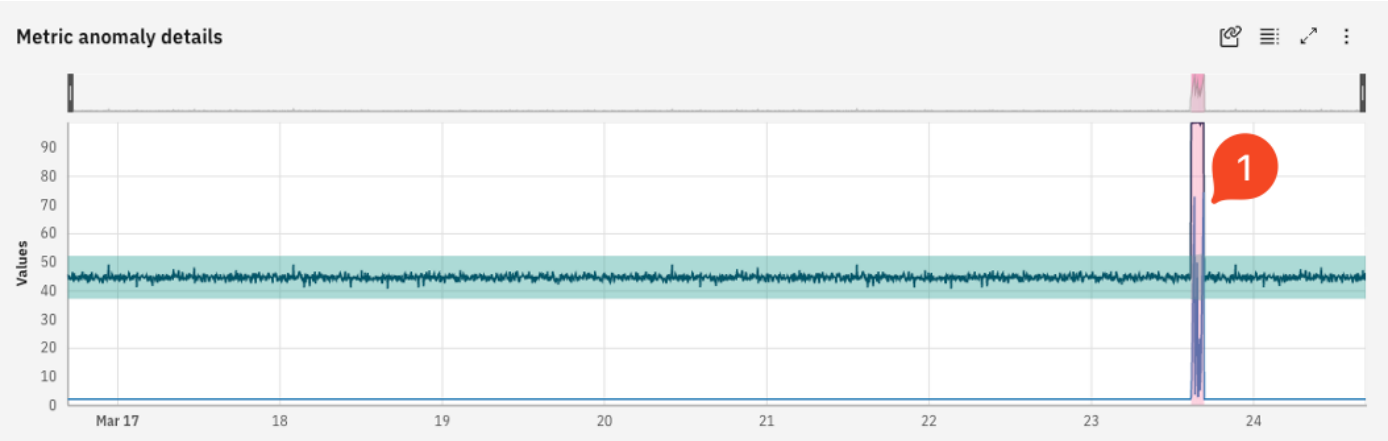


🚀 Action

- In **Related Alerts** click on the line **PodRestarts** to add an additional alert.

📣 Narration

Now let's zoom in to better see the anomalies

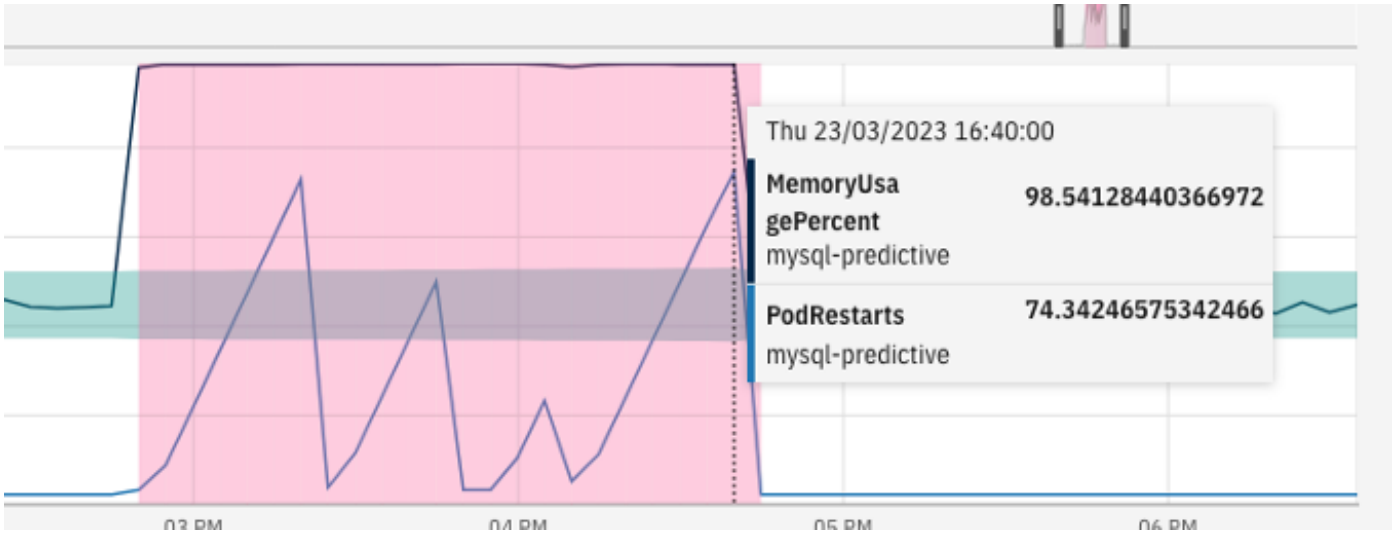


🚀 Action

- Click on the anomaly in the graph to zoom in
- Click on the anomaly a second time to show the values

📣 Narration

I can clearly see that the incident caused the **Memory Usage** to skyrocket and the **Pods** have been continuously restarte. This is yet another confirmation of the source of the problem.



🚀 Action

- Close the Metric anomaly details view by clicking on the cross in the upper right corner.

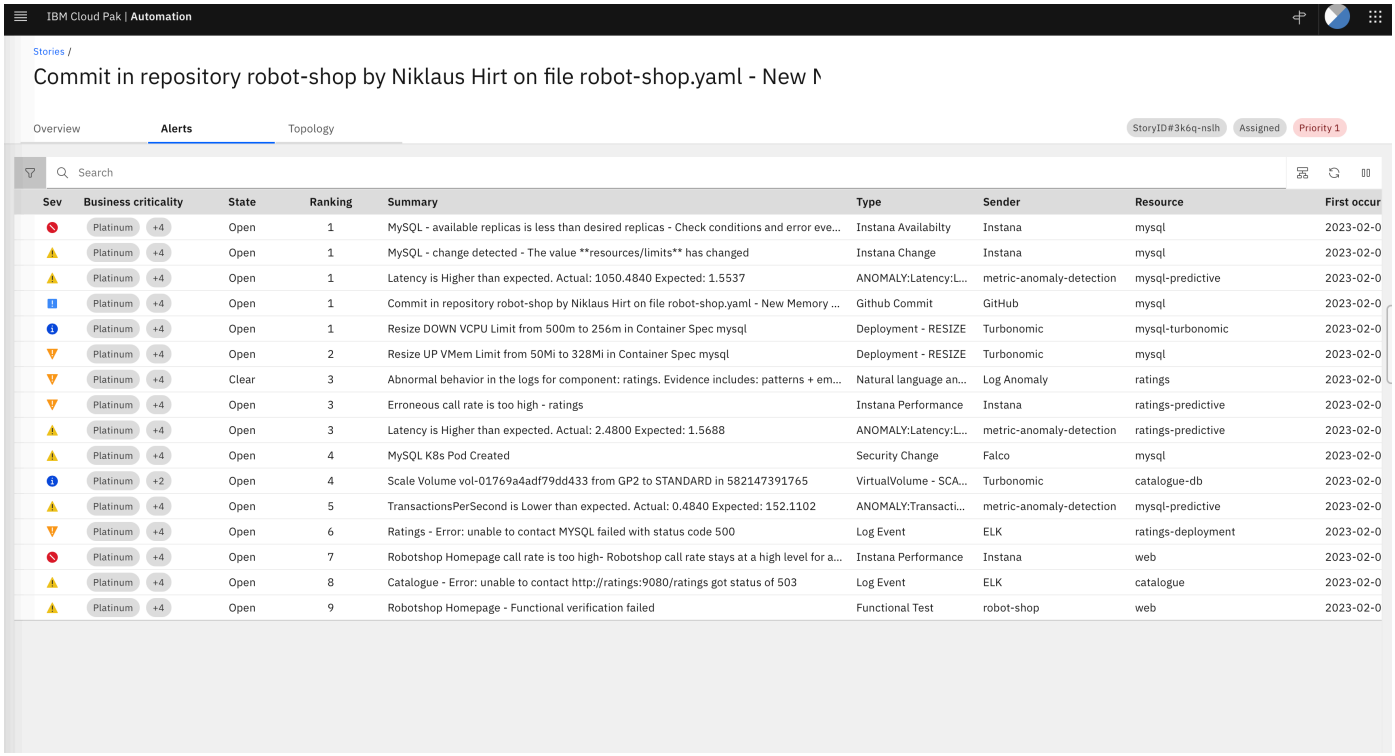
2.4.7 Examine the Alerts

📣 Narration

Let's have a look at the Alerts.

🚀 Action

- Click on the **Alerts** Tab
- Click on the first **Alert Group** to expand it



📣 Narration

Notice, that alerts are not sorted by severity, but the AI engine ranked them by relevance. The ones that are likely related to the root cause are at the top. Let's look at the first row for some more details.

🚀 Action

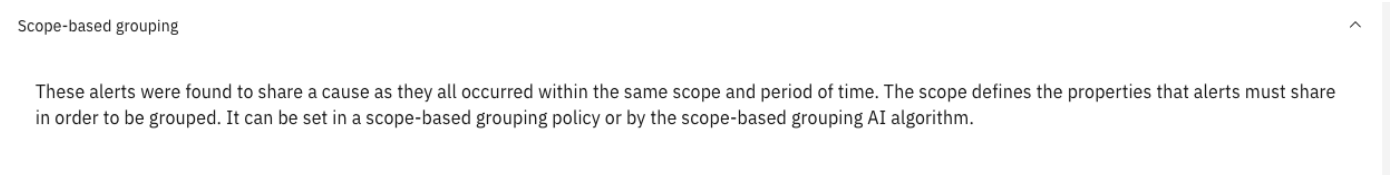
- Click on the first Alert in the list.

📣 Narration

In the **Alert details,** you can see different types of groupings explaining why the specific alert was added to the incident.

Scope based grouping

> 🚀 **Action**
>
> - Click **Scope-based grouping**.

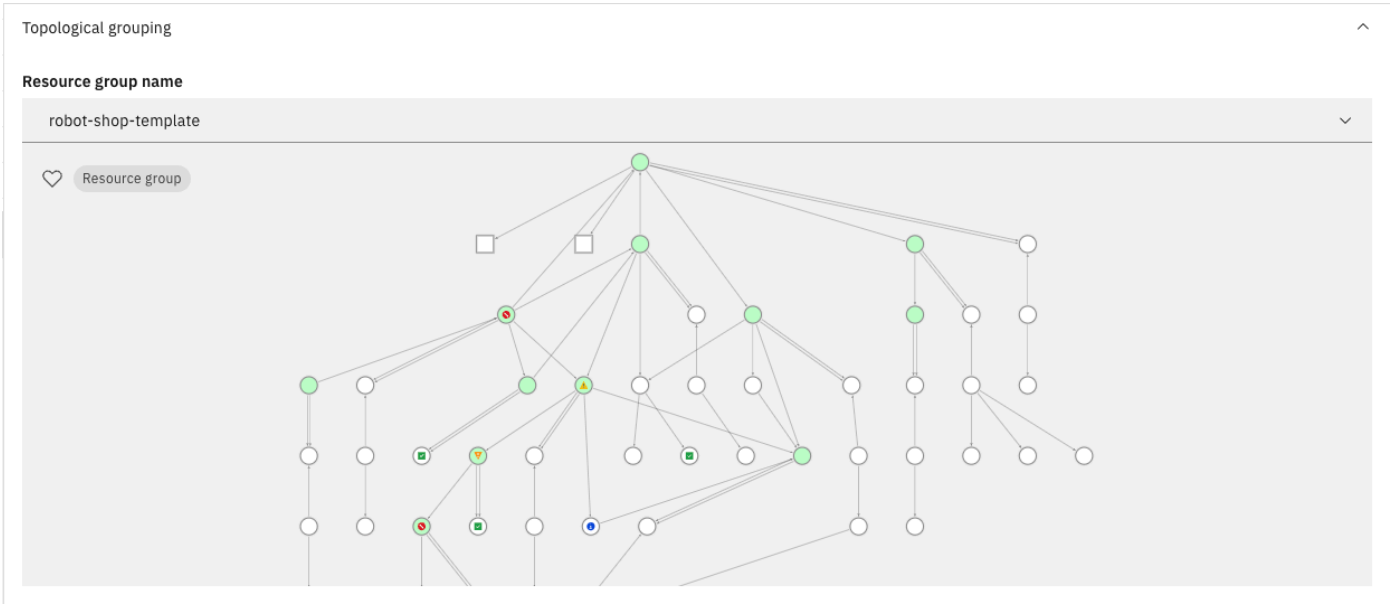


📣 Narration

Some alerts were added to the incident because they occurred on the same resource within a short period (default is 15 minutes)

Topological grouping

> 🚀 **Action**
>
> - Click **Topological grouping**.



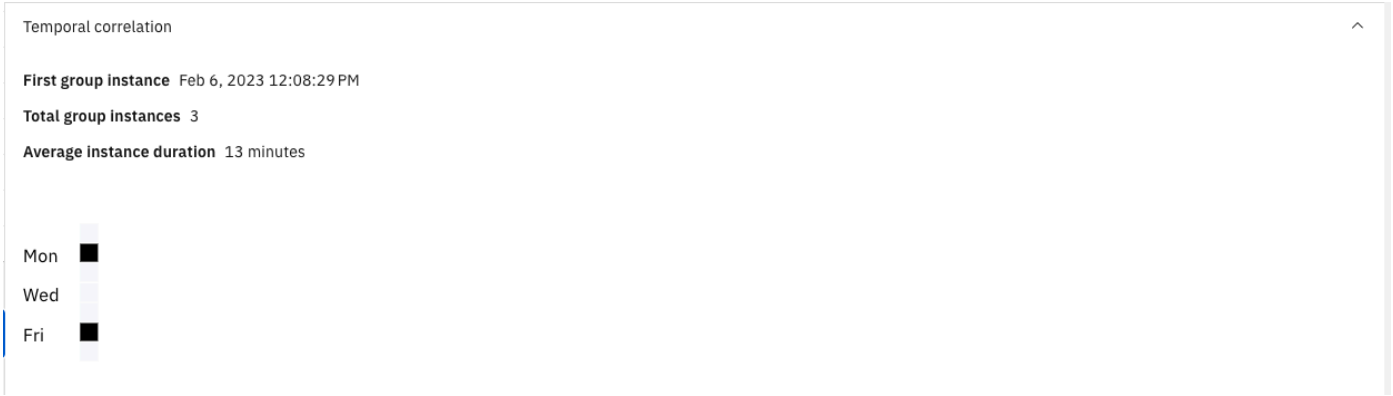
📣 Narration

Other alerts were grouped because they occurred on the logically or physically related resources. This correlation is using the application topology service that stitches topology information from different sources.

Temporal grouping

🚀 Action

- Click **Temporal correlation**.



📣 Narration

Finally, the temporal correlation adds to the incident events that previously, in history, are known to occur close to each other in the short time window. What is most important here is the fact that all these correlations happen automatically – there is no need to define any rules or program anything. In highly dynamic and distributed cloud-native applications this is a huge advantage that saves a lot of time and effort.

🚀 Action

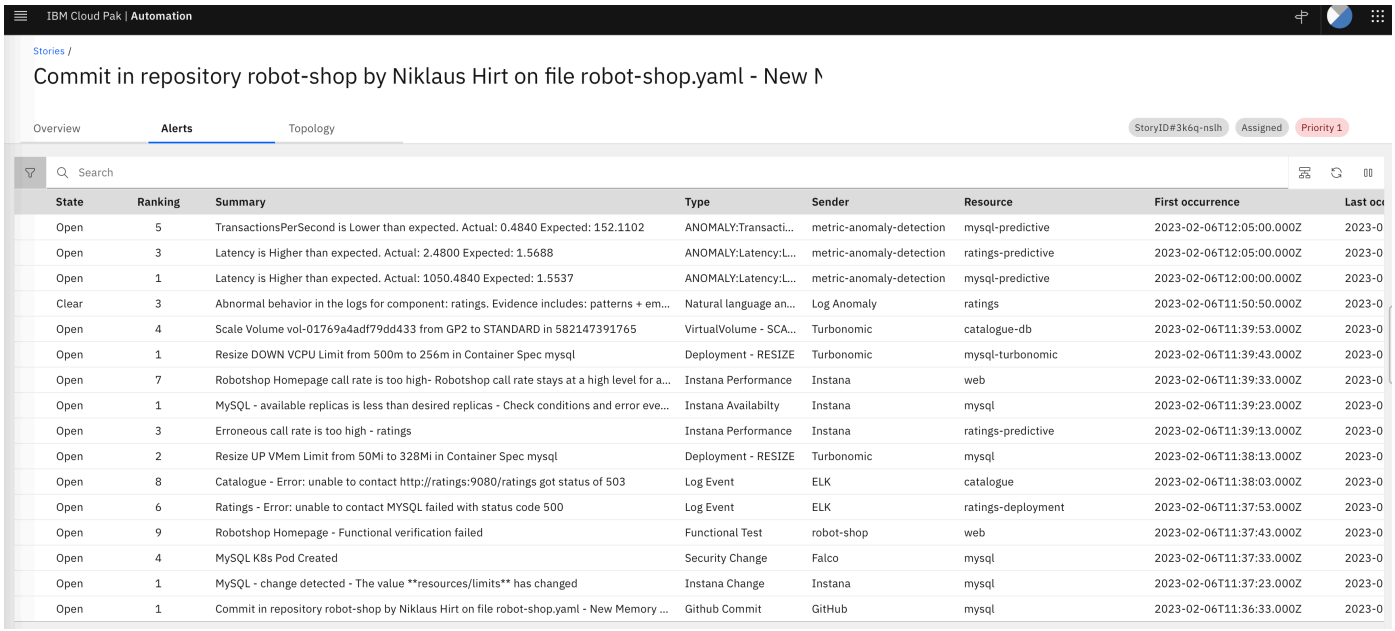
- **Close** the Alert details window.

2.4.8 Incident timeline

🚀 Action

- Click on **Summary** in the Header.

Result: The "Commit in repository robot-shop by Niklaus Hirt on file robot-shop.yaml" should be at the bottom



State	Ranking	Summary	Type	Sender	Resource	First occurrence	Last oc
Open	5	TransactionsPerSecond is Lower than expected. Actual: 0.4840 Expected: 152.1102	ANOMALY:Transacti...	metric-anomaly-detection	mysql-predictive	2023-02-06T12:05:00.000Z	2023-0
Open	3	Latency is Higher than expected. Actual: 2.4800 Expected: 1.5688	ANOMALY:Latency:L...	metric-anomaly-detection	ratings-predictive	2023-02-06T12:05:00.000Z	2023-0
Open	1	Latency is Higher than expected. Actual: 1050.4840 Expected: 1.5537	ANOMALY:Latency:L...	metric-anomaly-detection	mysql-predictive	2023-02-06T12:00:00.000Z	2023-0
Clear	3	Abnormal behavior in the logs for component: ratings. Evidence includes: patterns + em...	Natural language an...	Log Anomaly	ratings	2023-02-06T11:50:50.000Z	2023-0
Open	4	Scale Volume vol-01769a4adf79dd433 from GP2 to STANDARD in 582147391765	VirtualVolume - SCA...	Turbonomic	catalogue-db	2023-02-06T11:39:53.000Z	2023-0
Open	1	Resize DOWN VCPU Limit from 500m to 256m in Container Spec mysql	Deployment - RESIZE	Turbonomic	mysql-turbonomic	2023-02-06T11:39:43.000Z	2023-0
Open	7	Robotshop Homepage call rate is too high- Robotshop call rate stays at a high level for a...	Instana Performance	Instana	web	2023-02-06T11:39:33.000Z	2023-0
Open	1	MySQL - available replicas is less than desired replicas - Check conditions and error eve...	Instana Availabilty	Instana	mysql	2023-02-06T11:39:23.000Z	2023-0
Open	3	Erroneous call rate is too high - ratings	Instana Performance	Instana	ratings-predictive	2023-02-06T11:39:13.000Z	2023-0
Open	2	Resize UP VMem Limit from 50Mi to 328Mi in Container Spec mysql	Deployment - RESIZE	Turbonomic	mysql	2023-02-06T11:38:13.000Z	2023-0
Open	8	Catalogue - Error: unable to contact http://ratings:9080/ratings got status of 503	Log Event	ELK	catalogue	2023-02-06T11:38:03.000Z	2023-0
Open	6	Ratings - Error: unable to contact MYSQL failed with status code 500	Log Event	ELK	ratings-deployment	2023-02-06T11:37:53.000Z	2023-0
Open	9	Robotshop Homepage - Functional verification failed	Functional Test	robot-shop	web	2023-02-06T11:37:43.000Z	2023-0
Open	4	MySQL K8s Pod Created	Security Change	Falco	mysql	2023-02-06T11:37:33.000Z	2023-0
Open	1	MySQL - change detected - The value **resources/limits** has changed	Instana Change	Instana	mysql	2023-02-06T11:37:23.000Z	2023-0
Open	1	Commit in repository robot-shop by Niklaus Hirt on file robot-shop.yaml - New Memory ...	Github Commit	GitHub	mysql	2023-02-06T11:36:33.000Z	2023-0

📣 Narration

When trying to understand what happened during the incident, I sort the Alerts by occurence. This allows me to understand the chain of events.

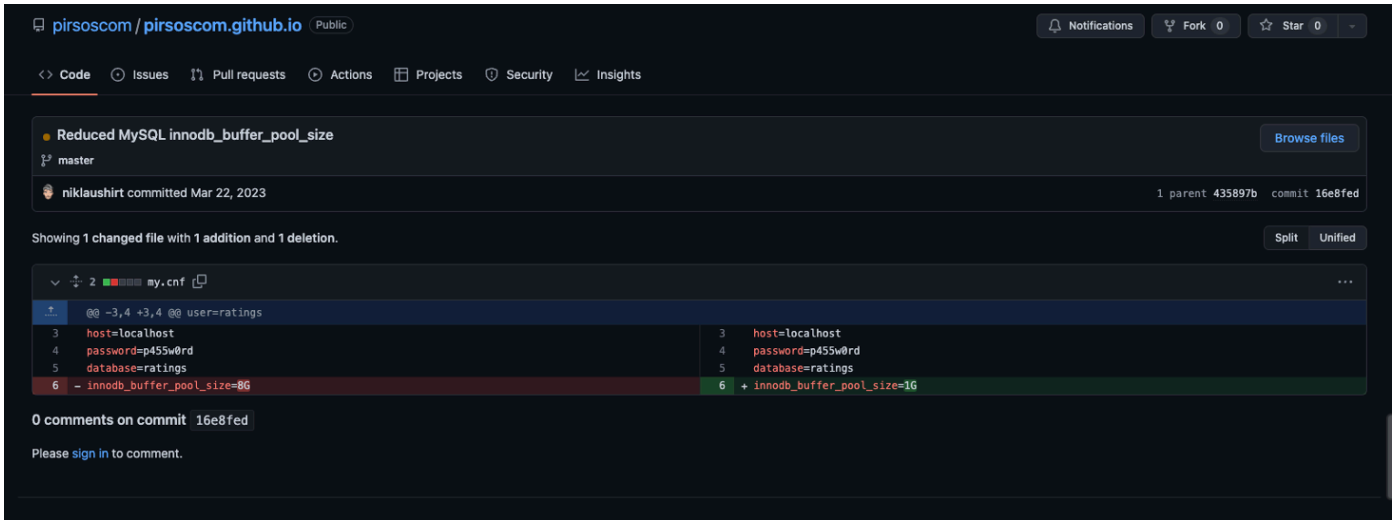
- I can see that the first event was a code change that had been commited to **GitHub**.

🚀 Action

- Click on the Alert line that has **Commit in repository** in the Summary.
- Click on **Open Link**

📣 Narration

I have now confirmation that the Dev team has massively reduced the Buffer Pool Size of my MySQL Database.



🚀 Action

- Click anywhere in the Git screen to go back

📣 Narration

Other events are confirming the hypothesis:

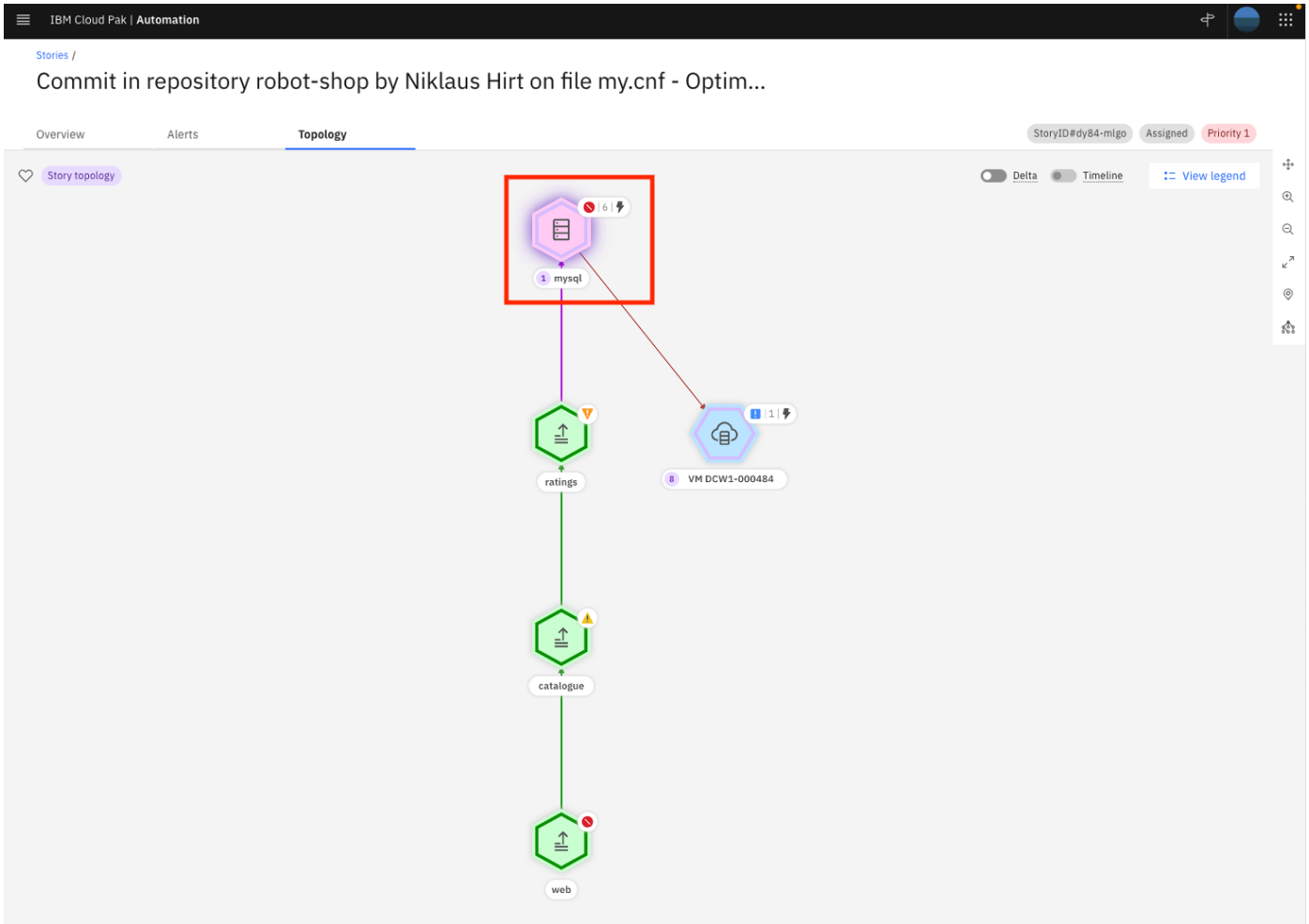
- I can then see the CI/CD process kick in and deploys the code change to the system detected by the Security tool and
- **Instana** has has detected the memory size change.
- Then **Functional Selenium Tests** start failing and
- **Turbonomic** tries to scale-up the mysql database.
- **Instana** tells me that the mysql Pod is not running anymore, the replicas are not matching the desired state.

- IBM AIOps has learned the normal, good patterns for logs coming from the applications. The Incident contains a **Log Anomaly** that has been detected in the ratings service that cannot acces the mysql database.

2.5 Working with Topology

2.5.1 Examining the Topology

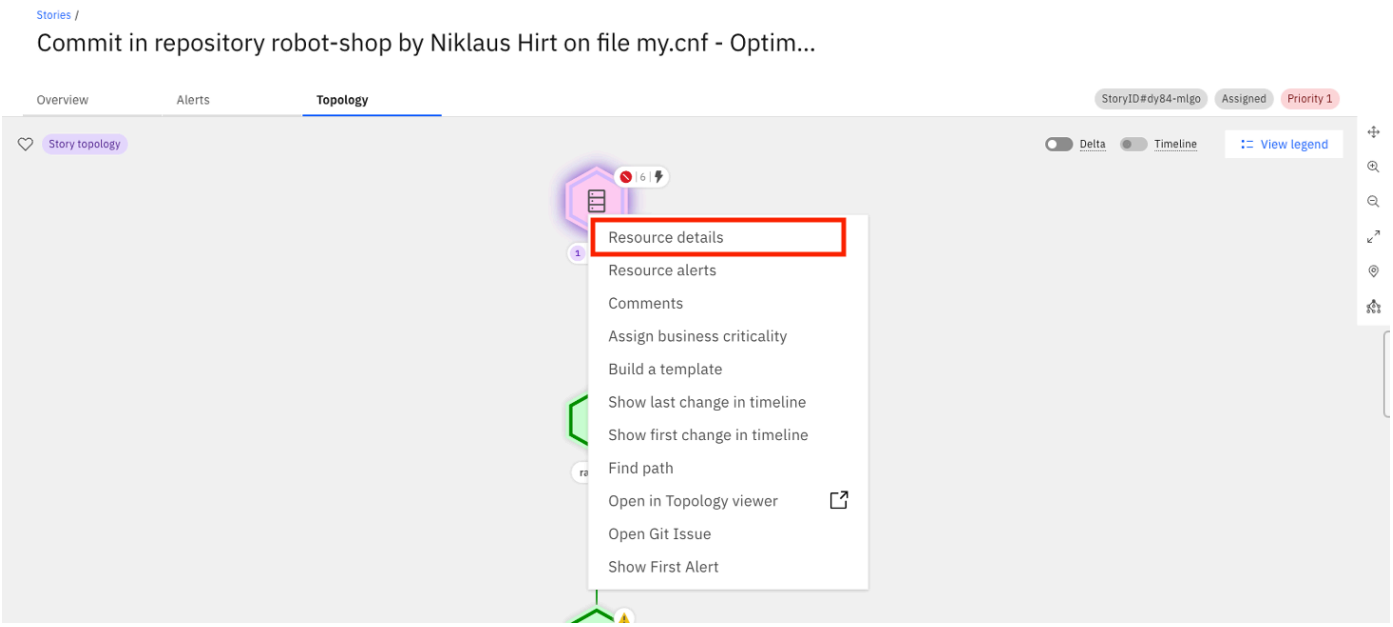
> **Action**
>
> - Click the **Topology** Tab.



Narration

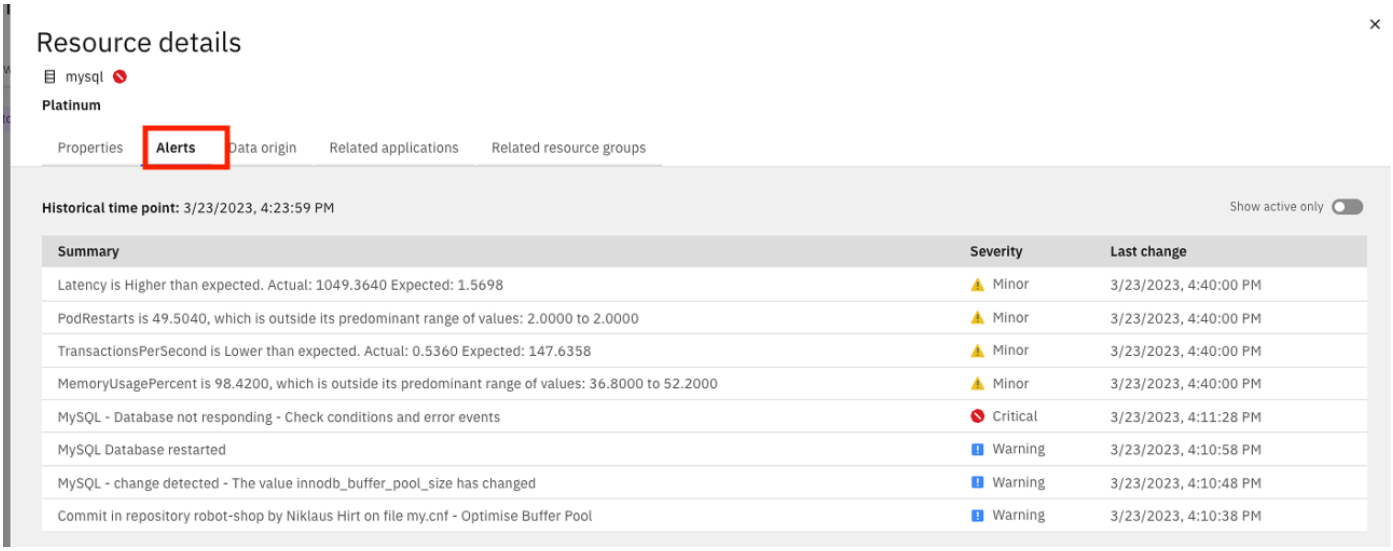
The interface shows the **topology** of the application that is relevant to the incident. IBM IBM AIOps' topology service delivers a working understanding of the resources that you have in your environment, how the resources relate to each other, and how the environment has changed over time.

You can see that there are some statuses attached to the different resources, marked with colorful dots. Let's view the details and status of the **mysql** resource with red status.



🚀 Action

- Click on the resource which displays resource name “**mysql**”
- Then, click and select **Resource details.**
- Click on Tab **Alerts**



📣 Narration

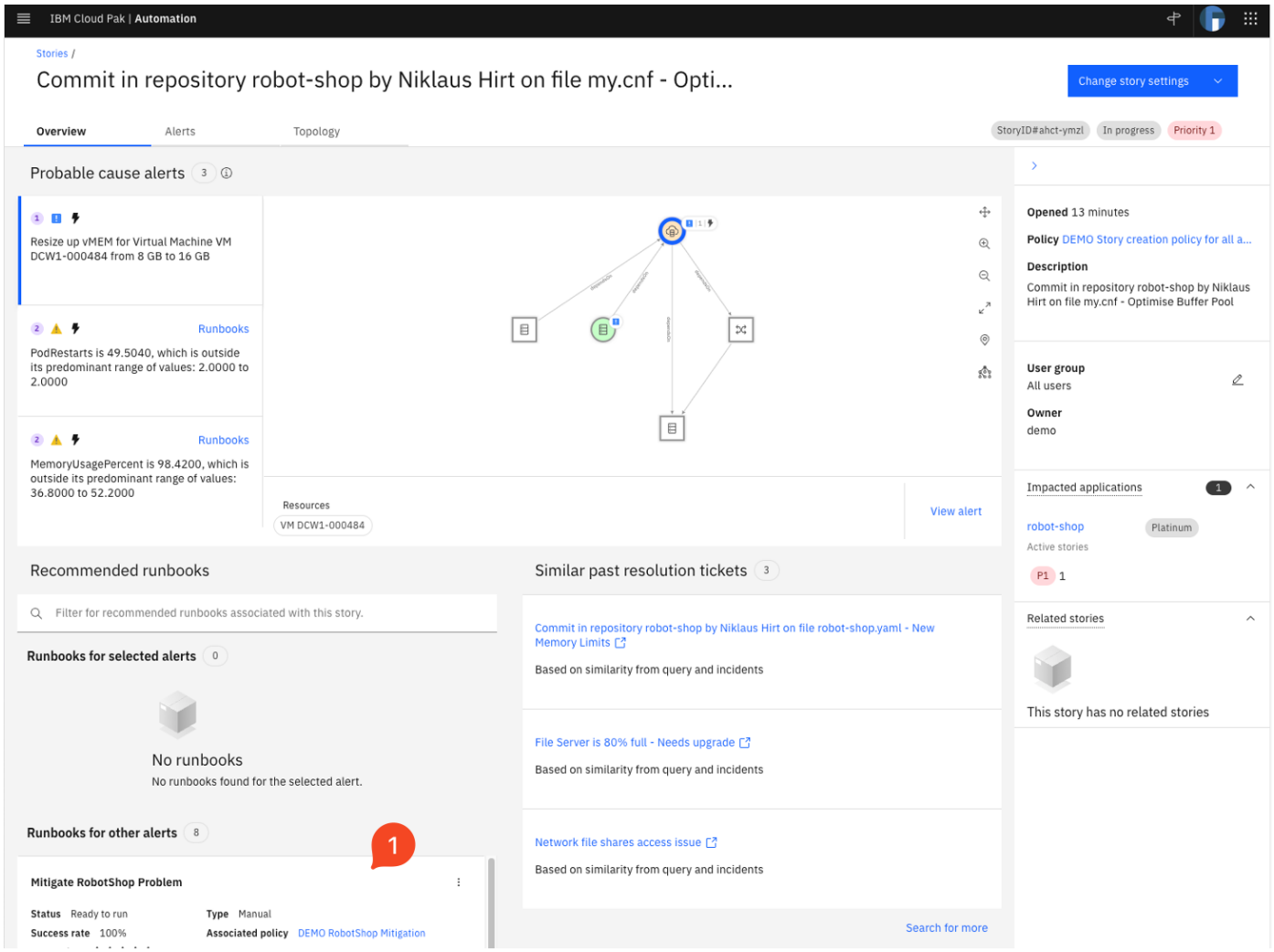
The topology service provides operations teams with complete up-to-date visibility over dynamic infrastructure, resources, and services. The topology service lets you query a specific resource for details, and other relevant information. Here I can see all Alerts for the mysql database resource for example.

🚀 Action

- Click the cross in the upper right corner to close the details view.
- Click on the **Overview** Tab.

2.6 Resolving the incident

2.6.1 Fixing the problem with runbook automation



📣 Narration

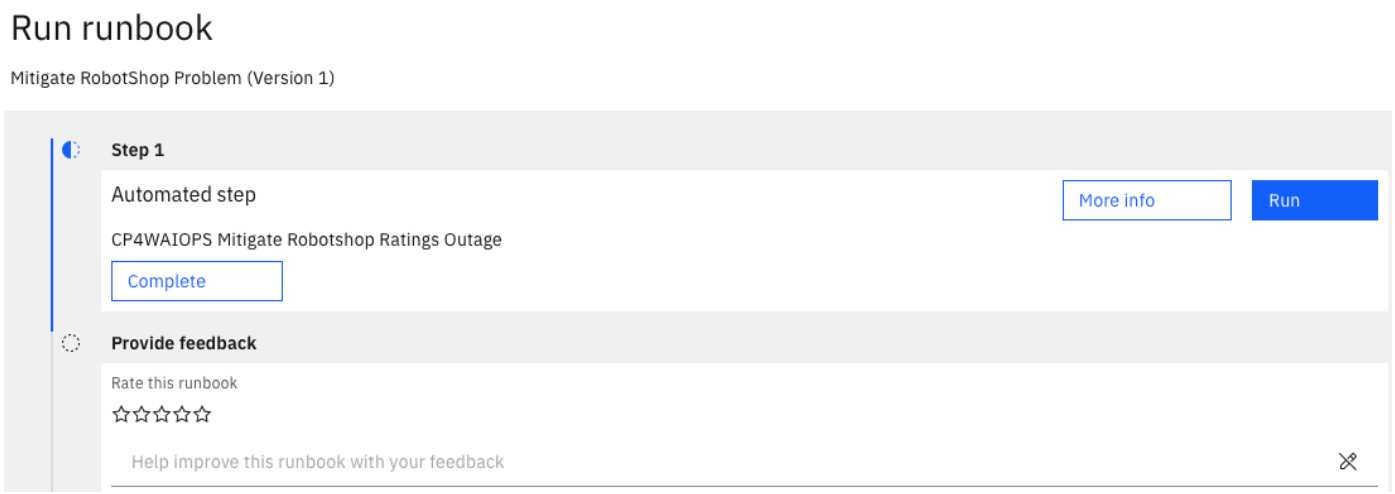
Now that we know what the problem is, let's correct what has happened. A runbook has been automatically identified but have not been executed. Runbooks are guided steps that IT operations teams use to troubleshoot and resolve problems. Some organizations might call these standard operating procedures or playbooks. When an incident occurs, IBM IBM AIOps matches an appropriate runbook to the problem. The runbook can be set to run automatically when it is matched to an incident, or it can run with user approval and participation.

📣 Narration

Let's execute the Runbook.

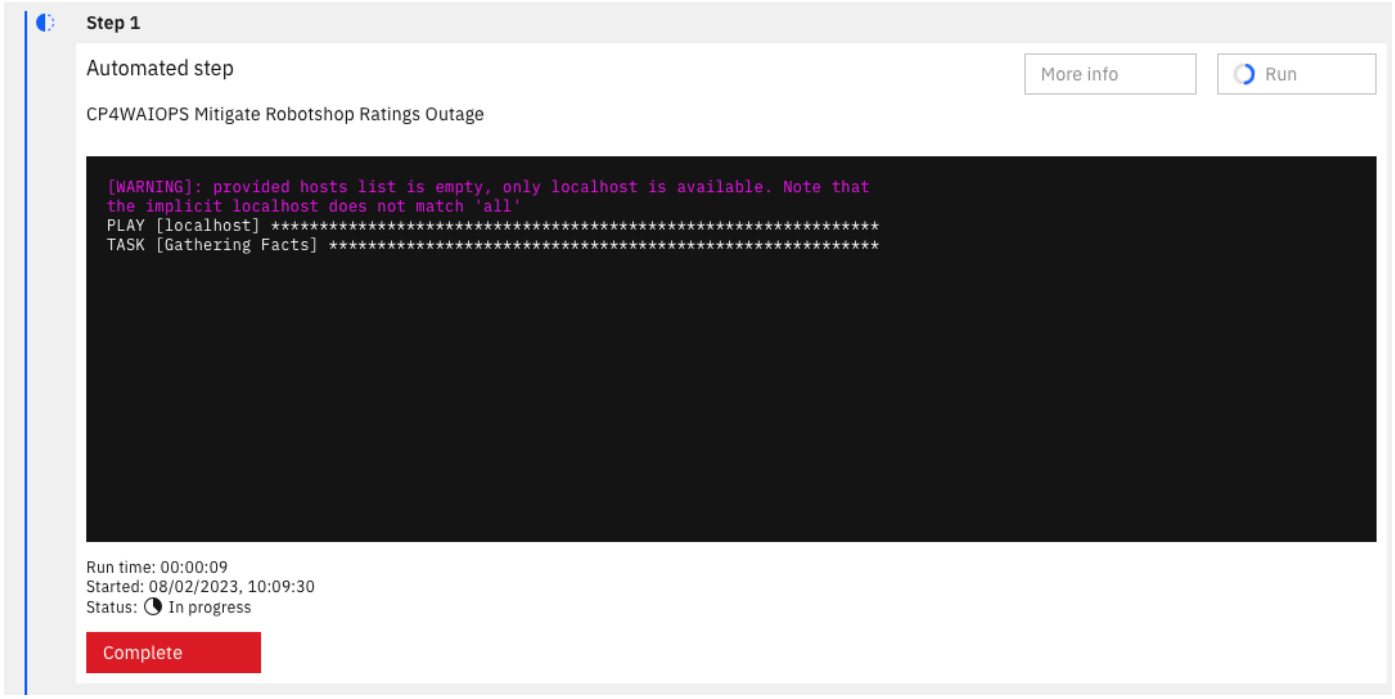
🚀 Action

- Click on the Runbook (1)
- Click **Start Runbook**.



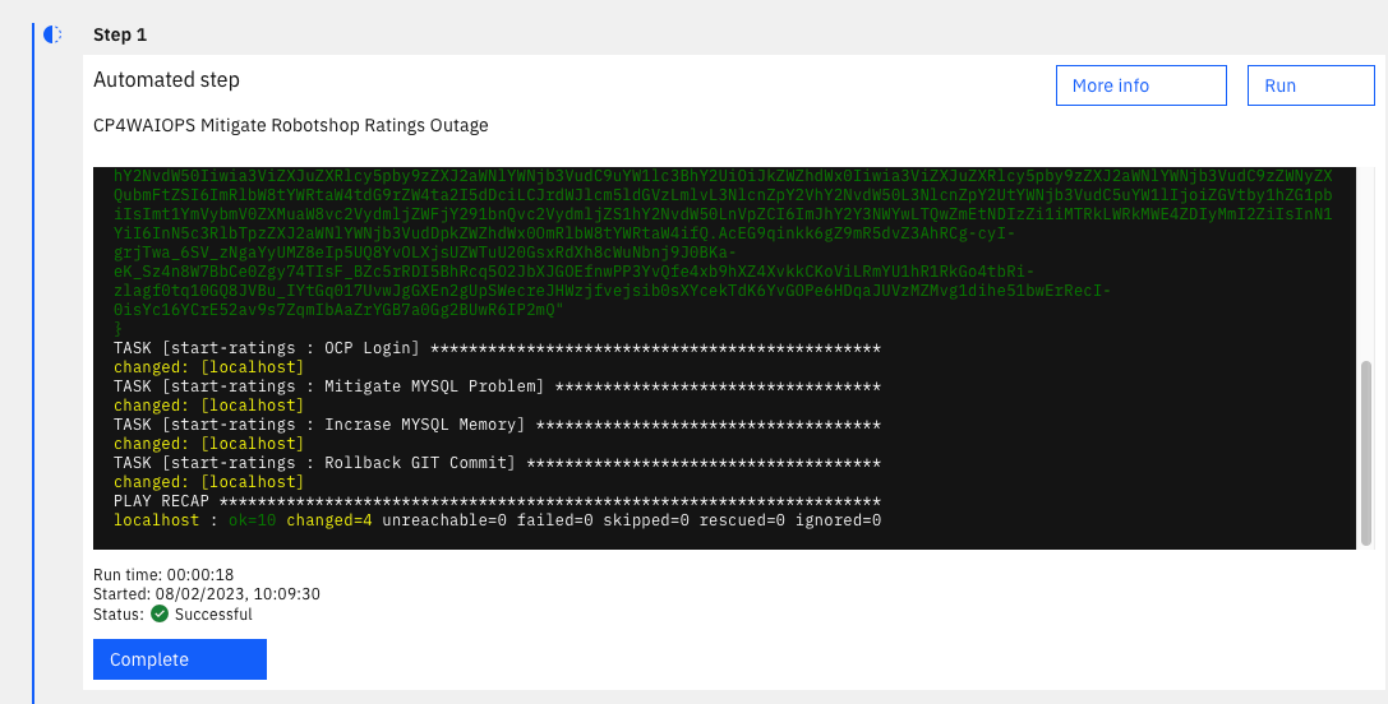
🚀 Action

- Click **Run** in Step 1.



📣 Narration

The Runbook that I just started kicks off a Playbook on Ansible Tower. I can follow the execution as it connects to the cluster and then scales up memory for the MySQL deployment.

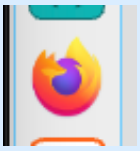


📣 Narration

Before confirming that the runbook worked as expected, I should check the RobotShop application to see if it is working as expected.

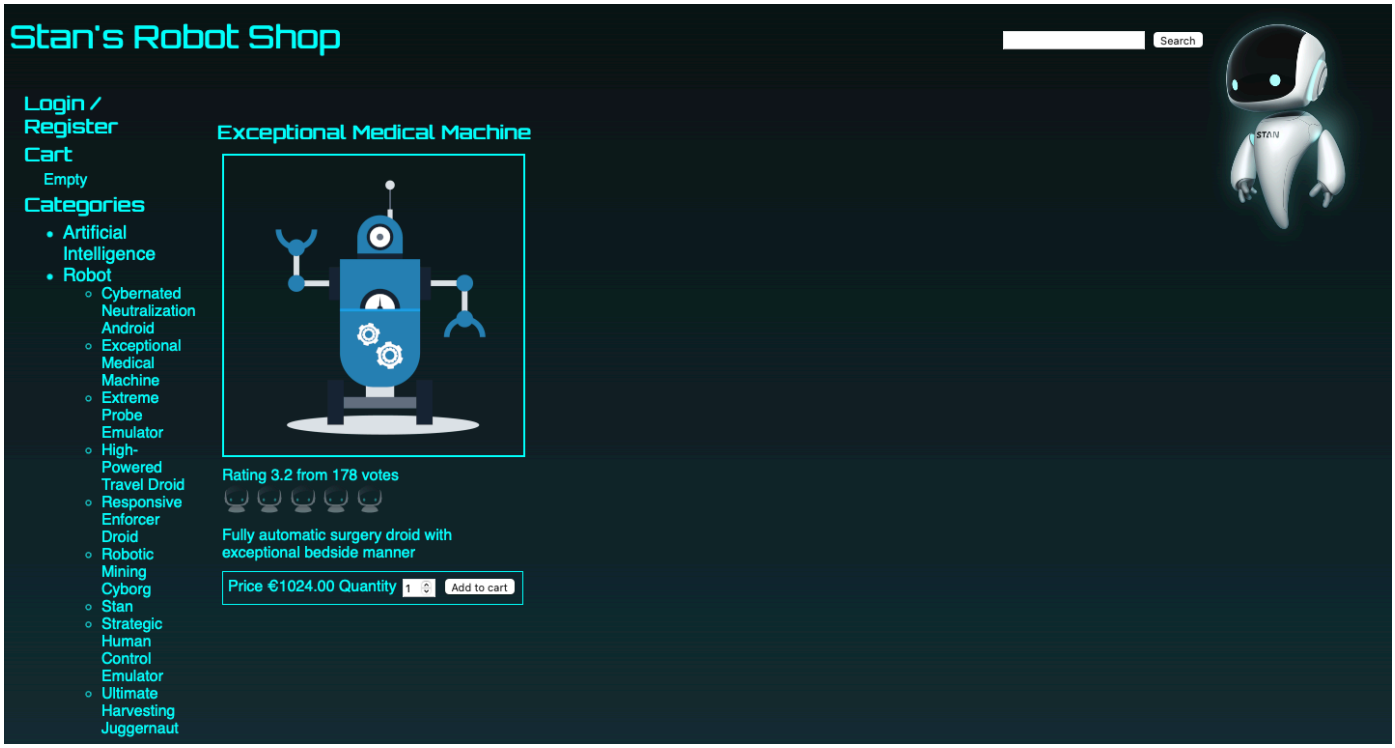
🚀 Action

- When finished, click **Complete**.
- Open the RobotShop application by clicking on the **Firefox** Icon in the left menu



🚀 Action

- Click on any Robot
- Show that ratings are correctly shown

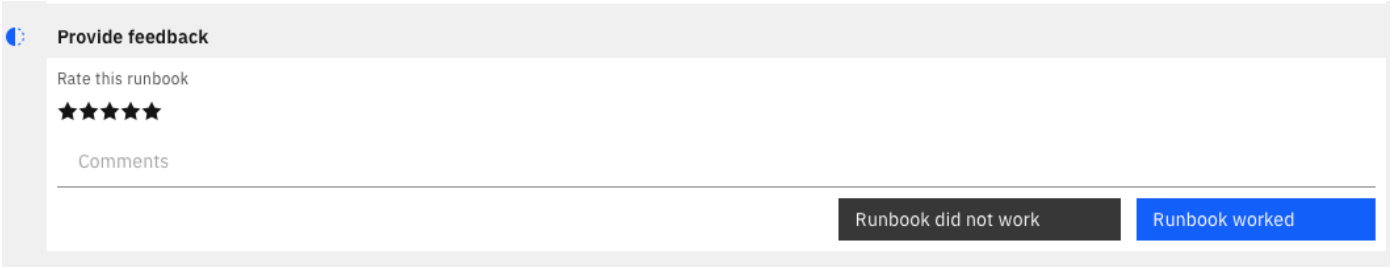


🚀 Action

- Go back by clicking on the **IBM AIOps** Icon in the left menu

📣 Narration

So the runbook has resolved the problem. When I tell IBM AIOps that the Runbook worked, it will learn over time to prioritize and suggest more relevant Runbooks.



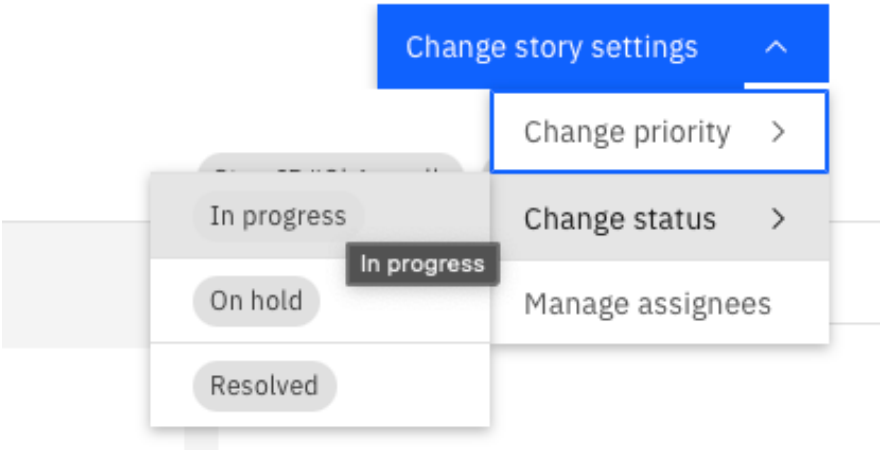
🚀 Action

- Rate the Runbook
- Then click **Runbook Worked**.

2.6.2 Resolve the Incident

🚀 **Action**

- Click on **Change Incident Settings.**
- Select **Change Status.**
- Click on **Resolved**



📣 **Narration**

So now as we have resolved the problem, I will inform the development team of the problem by reopening the ServiceNow ticket and by closing the Incident.

🚀 **Action**

- Click anywhere to go back to the list of Incidents
- Click anywhere to conclude the demo

Demonstration summary

📣 **Narration**

Today, I have shown you how IBM AIOps can assist the SRE/Operations team to identify, verify, and ultimately correct an issue with a modern, distributed application running in a cloud-native environment. The presented solution provides automatic application topology discovery, anomaly detection both with metrics and logs, and sophisticated methods of correlation of events coming from different sources.