ManageEngine
OpManager

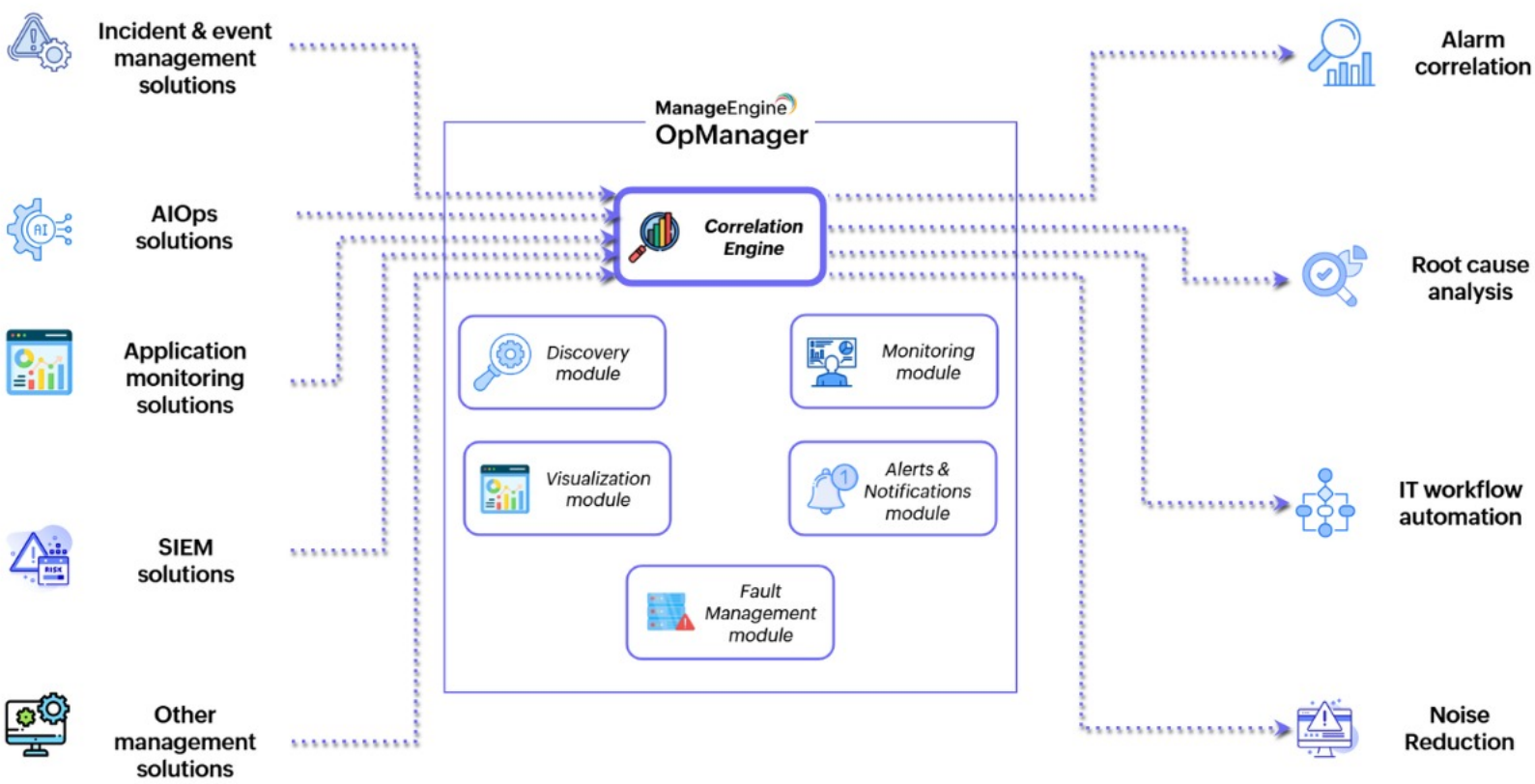
Cross-domain event correlation using OpManager APIs

A guide on how to ingest and correlate events from various third-party solutions using OpManager's RESTAPI.

The need for cross-domain event correlation

An enterprise infrastructure comprises multiple devices with multiple tools and IT teams trying to make sense of the jargon that the infrastructure spews out. Given the siloed environments in which these teams and tools work in, contextual correlation of various metrics from these environments is needed to:

1. Gain comprehensive visibility into the entire IT stack
2. Uncover the root cause of critical IT issues
3. Reduce MTTR through instant fault management
4. Ensure adherence to SLOs across all levels of IT



By ingesting events across different spectrums of your network, correlating them under a single console, and automating the fault remediation measures to be taken place, OpManager's REST API capabilities can help you identify the root cause and remediate them, making your entire incident management lifecycle seamless.

OpManager's addEvent API - enabling seamless cross-event correlation

With OpManager's addEvent REST API, you can ingest various events such as alerts, syslogs traps and event logs and correlate them under a single console. The addEvent API in OpManager allows you to retrieve the events from the respective data source. All you have to do is configure the following API URL from the respective data source.

```
https://localhost:8060/api/json/events/addEvent?source=Test_Dev
ice_MoName&severity=1&message=Sample_Critical_Message&ala
rmCode=Sample_AlarmCode&entity=Sample_Entity&apiKey=***
```

The API comprises the following information.

- **apikey** = <The API key to access OpManager's server>
- **source** = <The name of the source>
- **severity** = <Severity mapping of the alarm, ranging anywhere from 1 to 5>
- **message** = <Message of the alarm>
- **alarmCode** = <The alarm code of the respective alarm>
- **entity** = <Unique value for the generated alarm>
- **eventType** = <Event type of the alarm, used to identify the group of alerts >

Once you have configured this API, the respective events will automatically be sent to OpManager.

You can also add other APIs to further simplify your incident management lifecycle process. Click here to know about the various other REST APIs that OpManager provides.

Usecase : Putting OpManager's AddEvent API into action

Consider that your organization has deployed an application performance monitoring solution to monitor your front-end java applications and back-end MongoDB servers. The MongoDB server infrastructure are also being monitored by OpManager.

Now, consider the following scenario.

I. IT team detects **subpar user experience**

II. On further analysis, you detect **higher query processing time** in database servers, which increases latency

III. **Higher utilization levels** of the server on which the database is hosted

IV. Issue with the cooling units, causing the **server to overheat, causing performance throttling**, a phenomenon wherein higher temperature decreases the CPU and GPU speeds and the clock frequency.

The solution - API implementation steps

In the scenario described above, here's how to configure REST API in OpManager for event ingestion. Additionally, OpManager also provides several built-in APIs for event ingestion, correlation, and automatic fault remediation.

Learn more about REST API implementation in OpManager.

1. Get the REST API Key in OpManager from ***Quicklinks → REST API key*** and use the key to setup **addEvent API** in your APM tool (refer to page #3 of this document for the API template)

2. As soon as the solution detects higher query performance time, it relays the same to OpManager via the configured addEvent API

3. The relayed event is received as an alert and automatically associated to the corresponding database server in OpManager.

4. Now, using OpManager's root cause analysis feature, you can correlate the database server's query processing times, its utilization, and temperature. This helps you identify the correlation.

5. You can also configure an alarm correlation rule. to correlate multiple events received from the API. This also helps you arrive at the right root cause without further analysis.

6. The alarmCode and eventType parameters from the API call are matched to trigger the corresponding workflow in OpManager, automating fault remediation and eliminating manual intervention

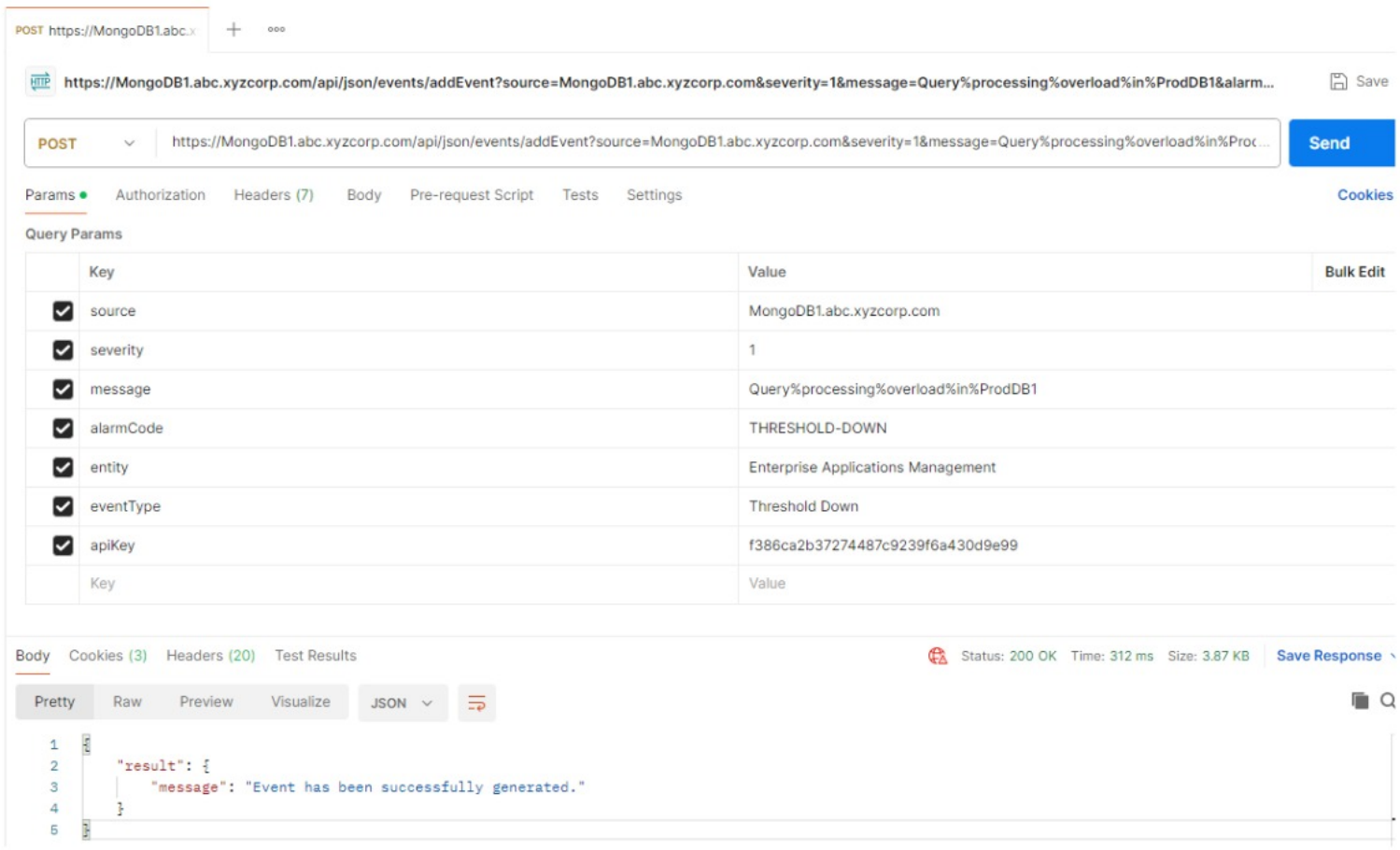


Fig: API implementation using Postman

Still having queries ?

Write to us at **opmanager-support@manageengine.com**