DOCUMENTATION

Viewing Forensics

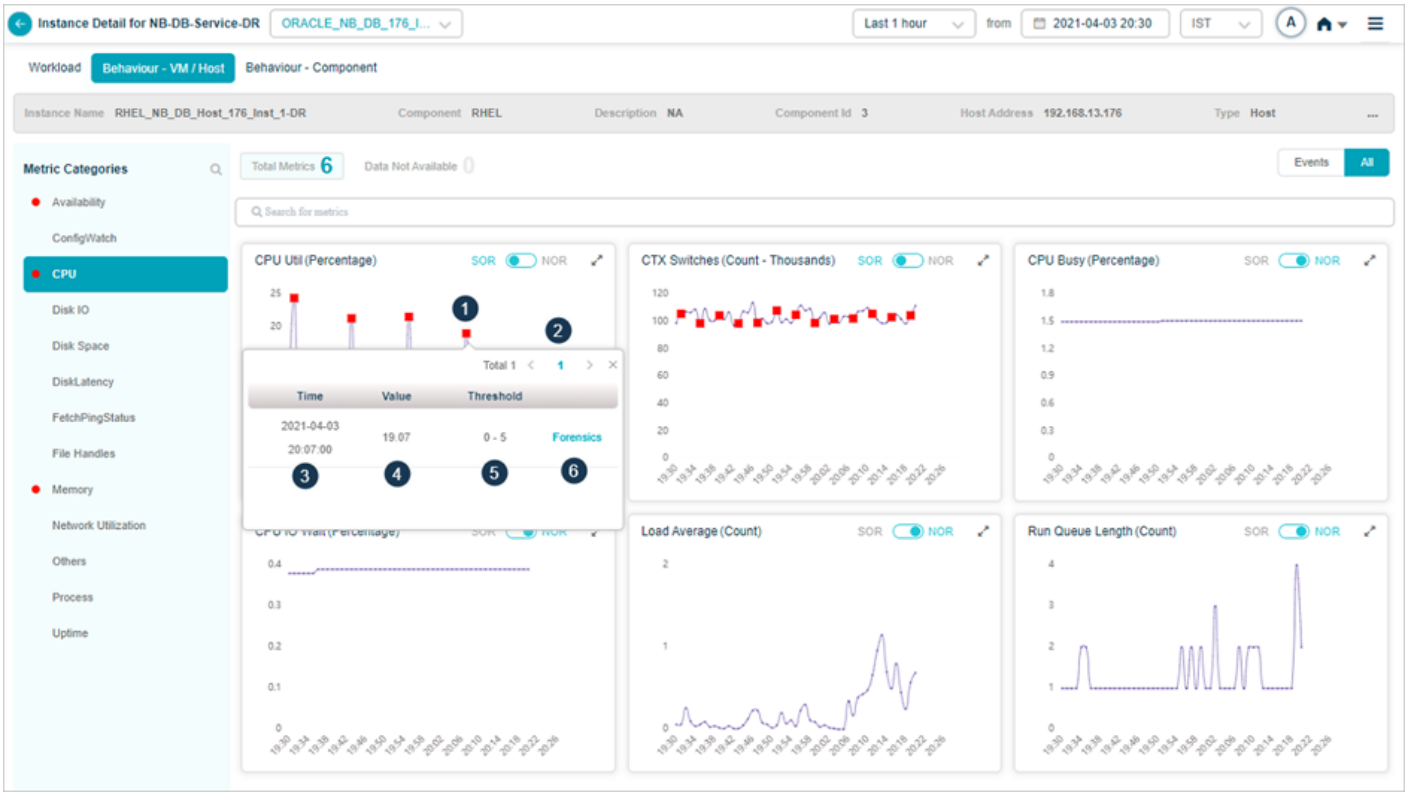
HEAL Software Inc.

Forensics provides a detailed analysis of the signal and helps in identifying the possible root cause of the signal. The HEAL application collects these forensics when an event is generated in the application and displays the data on the UI. One of the routes to value is to show customers quality and meaningful data captured related to instances where anomalies are observed to assist SMEs during signal triage further. All such data is viewed in the context of a big feature, say a problem or early warning. Data is collected through script-based forensic data (part of the supervisor package installed on the target box) or wired-in data (java deep dive code snapshots).

Forensics is useful to the application owner, ITOPs user, and product admin.

Forensics gets collected only at the instance level. Forensic collection is completely independent of the type of signal (early warning or problem). Forensics gets triggered as soon as an event occurs and not on subsequent ones in a defined time period of “n” minutes per category per instance level. This time period of “n” minutes is configurable. Forensic action on an event of the same category in the same instance is also suppressed.

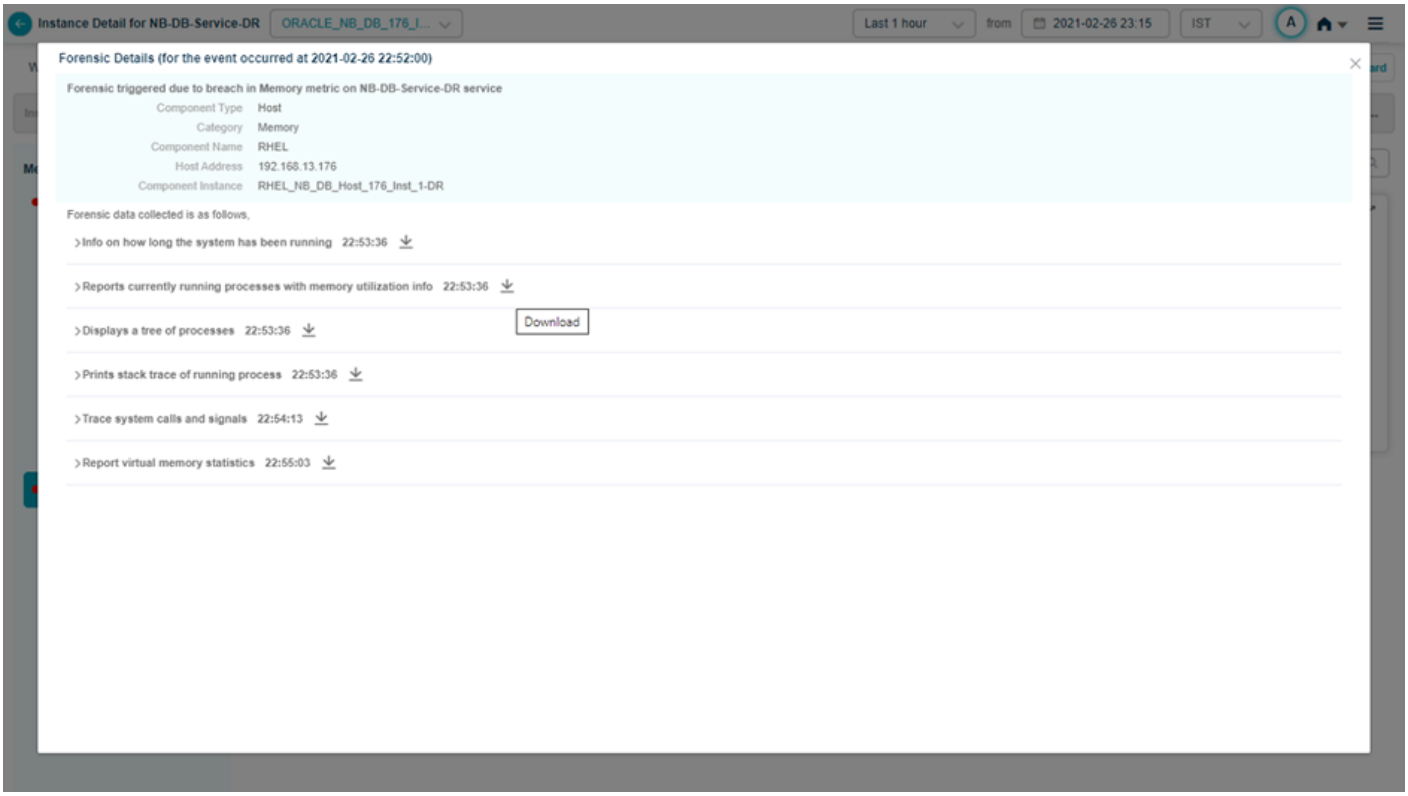
As soon as MLE triggers a NOR (Normal Operating Range) violation on a key KPI (primary indicators of service and host behavior), the associated forensic action triggers to gather just-in-time diagnostic data. MLE applies dynamic baselines on transaction response times and triggers forensics on transaction slowness. A special forensic action triggers code slowness at the Java service layer – taking code snapshots via instrumentation.



Forensic action is based on the KPI category and violating service instances.

i.e. Forensic actions are grouped at an instance and KPI category level.

1	Click on an event to view the forensic details.
2	A new pop-up arises with an option to view forensics.
3	This displays the Date and time of occurrence of an event.
4	This displays the KPI value at an event.
5	**NOR or SOR** threshold range. Either **MLE or SOR** processor triggers an event. An event indicates that the KPI value is not within the threshold range.
6	Select **Forensics** to view detailed forensics. The below screen is displayed.



Select **Download** to download specific command output. The output is in **.txt format**.

When a service is under **maintenance**, **forensics**, as well as **snapshots**, are not collected.