DOCUMENTATION

Viewing Forensics

HEAL Software Inc.

Table of Contents

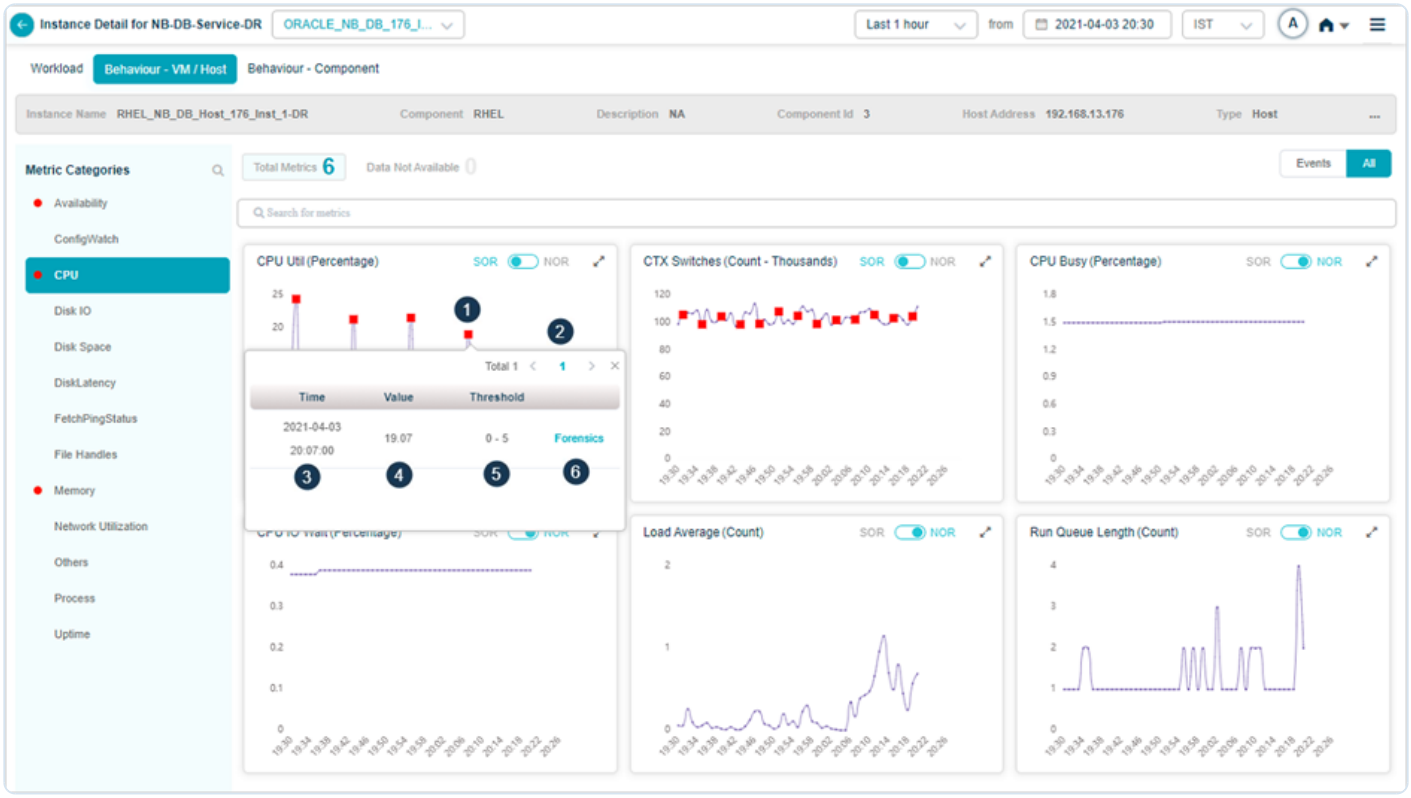
Forensics gives you a detailed look at the data HEAL captures around an event so you can identify the root cause faster. Useful for application owners, IT Ops, and product admins.

How forensic data is collected

HEAL collects forensics through script-based actions (part of the supervisor package on the target box) and wired-in data (Java deep-dive code snapshots). Both flow into the UI in the context of a Problem or Early Warning.

Forensics is collected only at the instance level, regardless of signal type. The action triggers as soon as the first event in a category occurs, then suppresses for the next “n” minutes per category and instance. The “n” minutes interval is configurable.

> **When forensics fires.** As soon as the MLE flags a NOR (Normal Operating Range) violation on a key KPI, the matching forensic action runs to gather just-in-time diagnostic data. Dynamic baselines on transaction response times also trigger forensics on transaction slowness, and a special action takes Java code snapshots through instrumentation.



Forensic actions are grouped at the instance and KPI category level.

Open forensics for an event

1. Click an event to see its forensic details.

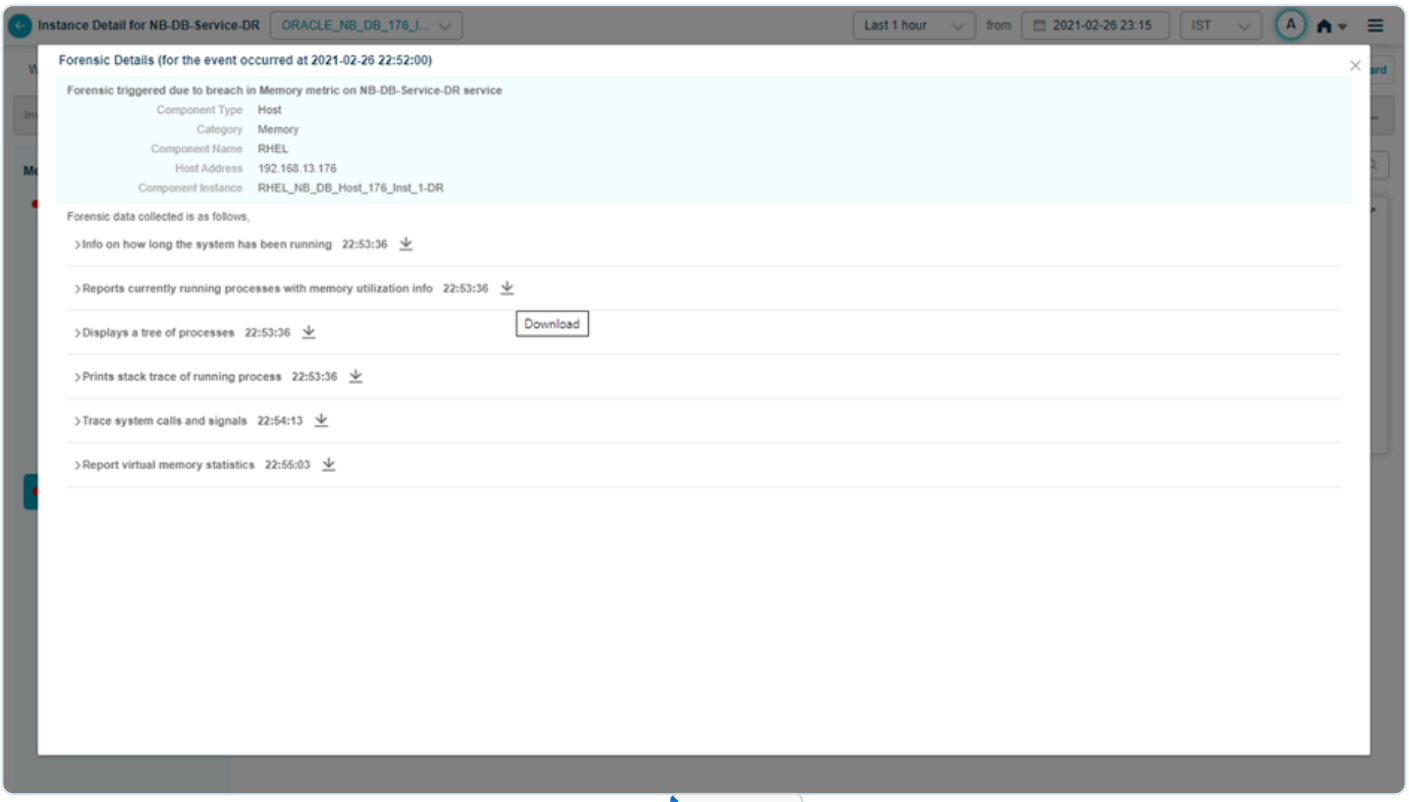
2. A popup opens with the option to view forensics.

3. Date and time of the event.

4. KPI value at the moment of the event.

5. NOR or SOR threshold range. The MLE or SOR processor triggered the event because the value went outside the range.

6. Click Forensics to open the detailed forensic data.



Click **Download** to save command output as a `.txt` file.

> **Heads up.** When a service is under maintenance, neither forensics nor code snapshots are collected.

Next

- View Problem Report . open one Problem.
- Root Cause Analysis . trace the cause of a signal.
- Viewing Request Dashboard . workload request details.