Incident investigation

Tom Rochette <tom.rochette@coreteks.org>

June 11, 2022 — e4a94987

- Define the incident owner
- Define the incident secretary/communicator
- Create and document
  - summary
  - observations (link to metrics dashboards with absolute timestamps as much as possible)
    - screenshots
    - links to logs
  - hypotheses/theories
    - who made them
    - when
    - if they have been validated/invalidated
  - the actions taken
    - by whom
    - if it had the desired effect
  - etc.
- In the situation where an incident has been caused by the introduction of a code regression, revert the change and deploy as soon as possible
- Start by reducing/relieving the impact of the incident before searching for a root cause
- Use multiple data sources when data sources do not agree
- Diagram all the implicated systems and the relationship to one another in order to identify the potential locations where the problem might be
- Test your hypotheses to verify if they hold or not
- Develop a procedure over time that can be followed to diagnose similar issues