Incident investigation

Tom Rochette <tom.rochette@coreteks.org>

September 21, 2022 — a9642824

- 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
      - Who took the screenshot
      - Link to get the graph/data
      - Associated conclusions
    - 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
- Write down a list of improvement suggestions in order for the incident not to reproduce itself in the future or to lessen its impact
- Once the incident is completed, have a summary of the conclusions at the top of the document with a link to the sections in the document explaining the rationale behind the conclusions