# Root Cause Analysis (RCA) using StackStorm

## 1. Introduction to StackStorm RCA

StackStorm is an event-driven automation platform that integrates with monitoring tools like SolarWinds, SCOM, Kibana, ElasticSearch, and more. It helps in automating Root Cause Analysis (RCA) and incident response.

## 2. StackStorm Architecture

StackStorm follows a modular architecture consisting of:

• Sensors: Detect external events and trigger actions.  
• Triggers: Define when actions should be executed.  
• Actions: Automation workflows executed when conditions match.  
• Rules: Define logic to correlate events and automate responses.  
• Packs: Bundled integrations with third-party tools.  
• API & CLI: Interfaces for managing and executing workflows.  
• Web UI: Graphical interface to monitor and manage automation.

## 3. Predefined Features Useful for RCA

1. Monitoring Integrations: Collect alerts from multiple sources.  
2. Event Correlation Engine: Correlate multiple alerts to find root causes.  
3. Automation Workflows: Prebuilt workflows to automate RCA processes.

## 4. RCA Rule Creation in StackStorm

Example: High CPU & API Failure RCA

A YAML rule for correlation:

name: "rca\_cpu\_api"  
description: "Identify high CPU overload as root cause of API failures"  
enabled: true  
trigger:  
 type: "stackstorm.solarwinds.cpu\_high"  
criteria:  
 server\_count:  
 type: "gt"  
 pattern: "5"  
 api\_status:  
 type: "eq"  
 pattern: "500"  
action:  
 ref: "stackstorm.create\_rca\_report"

## 5. Automating RCA Report Generation

• Create an action to generate RCA reports.  
• Store reports in Kibana / Elasticsearch.  
• Notify teams via Slack / PagerDuty.

## 6. Industry Standard SOP for RCA Using StackStorm

1. Setup StackStorm environment with required integrations.  
2. Define monitoring triggers to capture alerts.  
3. Create correlation rules based on alert severity and dependencies.  
4. Implement automated remediation actions based on predefined workflows.  
5. Test and validate RCA workflows before deployment.  
6. Deploy and monitor StackStorm RCA engine in production.  
7. Continuously optimize rules based on new incident patterns.

## 7. Conclusion

• StackStorm provides a powerful RCA framework.  
• Custom rules are needed for specific environments.  
• Seamless integration with existing monitoring tools.  
• Alternatives: Moogsoft, BigPanda (not free).