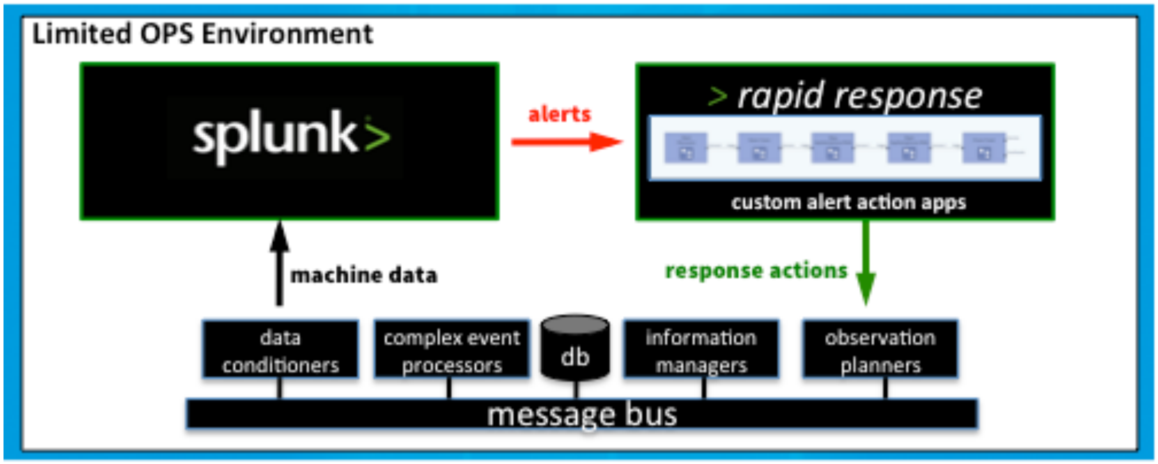
>*rapid response* for Splunk® in Action

Increasing Mission Assurance in IC Limited Operations Environment

>*rapid response* was originally conceived for an IC customer conducting advanced systems and technology R&D for next generation intelligence capabilities. The ongoing research program has achieved remarkable technology and tradecraft advances, many of which have already transitioned into a limited-ops environment - with its attendant mission availability requirements.

Challenges

The advanced technology requires continuous operation to acquire and maintain custody of real-world entities of interest. However, the limited ops environment is presently only staffed 5 x 8. Therefore an outage occurring at 1800 on a Friday may not be addressed until 0800 Monday. During this down time, intel observations are backlogged and/or missed altogether, which directly degrades mission performance.



Solution

We developed >*rapid response* for Splunk specifically to mitigate the impacts of off-hours outages on mission performance. Splunk and >*rapid response* team up to keep a constant watch over the limited-ops environment. Splunk generates alerts when it detects system anomalies – and the alerts trigger >*rapid response* composed custom alert action workflows to automatically recover mission operations.

>*rapid response* Recovery Strategies

Recovering from single point failures is generally straightforward. But some of the advanced technology elements employed in the limited ops environment are strongly interdependent. In other words, a failure in one element may precipitate subsequent downstream failures. Recovering from such 'cascade failures' often requires a 'closed loop' strategy that orchestrates initial recovery actions, measures their results, and escalates as necessary. >*rapid response* empowered operations specialists to quickly and easily compose, test and verify comprehensive custom recovery strategies, and then track and where necessary control their execution in real time. The team is in the process of implementing a wide range of response strategies for the following types of anomaly cases:

- Cross-Tier (JBoss-Oracle) connector hang
- Resource over-limits
- Excessive message broker CLOSE-WAITs
- DNS server lockup
- Extended WAN outage

Available through carahsoft. optensity.com/rapid-response-splunk *Powered by* AppSymphony
sales@carahsoft.com 1-(844)-37RAPID