Introducing CA Agile Operations Analytics

Sudip Datta
Vice President of Product Management

Kiran Diwakar
Senior Director of Product Management

ca technologies

Characteristics of a Modern Operations Analytics

- Volume: Needs to *scale* to Petabytes (soon to be Exabytes) of data
- Velocity: Modern Analytics is *Dynamic* and *Real-time*
- Variety: Highly *correlative* among diverse data sources
- *Collaborative* and needs to *cater to multiple personas*: Business Users, IT Users and Developers
- *Self-Learning*

CA's Agile Operations Analytics

- Why
- What
- How
- When

WHY: Market is ripe for a combined Monitoring and Analytics offering

Gartner: Combine Log Analytics with Unified Monitoring

Modernize Your Monitoring Strategy by Combining Unified Monitoring and Log Analytics Tools

30 October 2013 G00257830

Analyst(s): *Jonah Kowall | Colin Fletcher*

"Enterprise I&O teams should combine unified monitoring and log analytics technologies to build a simpler, faster and cost-effective approach to managing the availability of today's highly complex and dynamic environments"

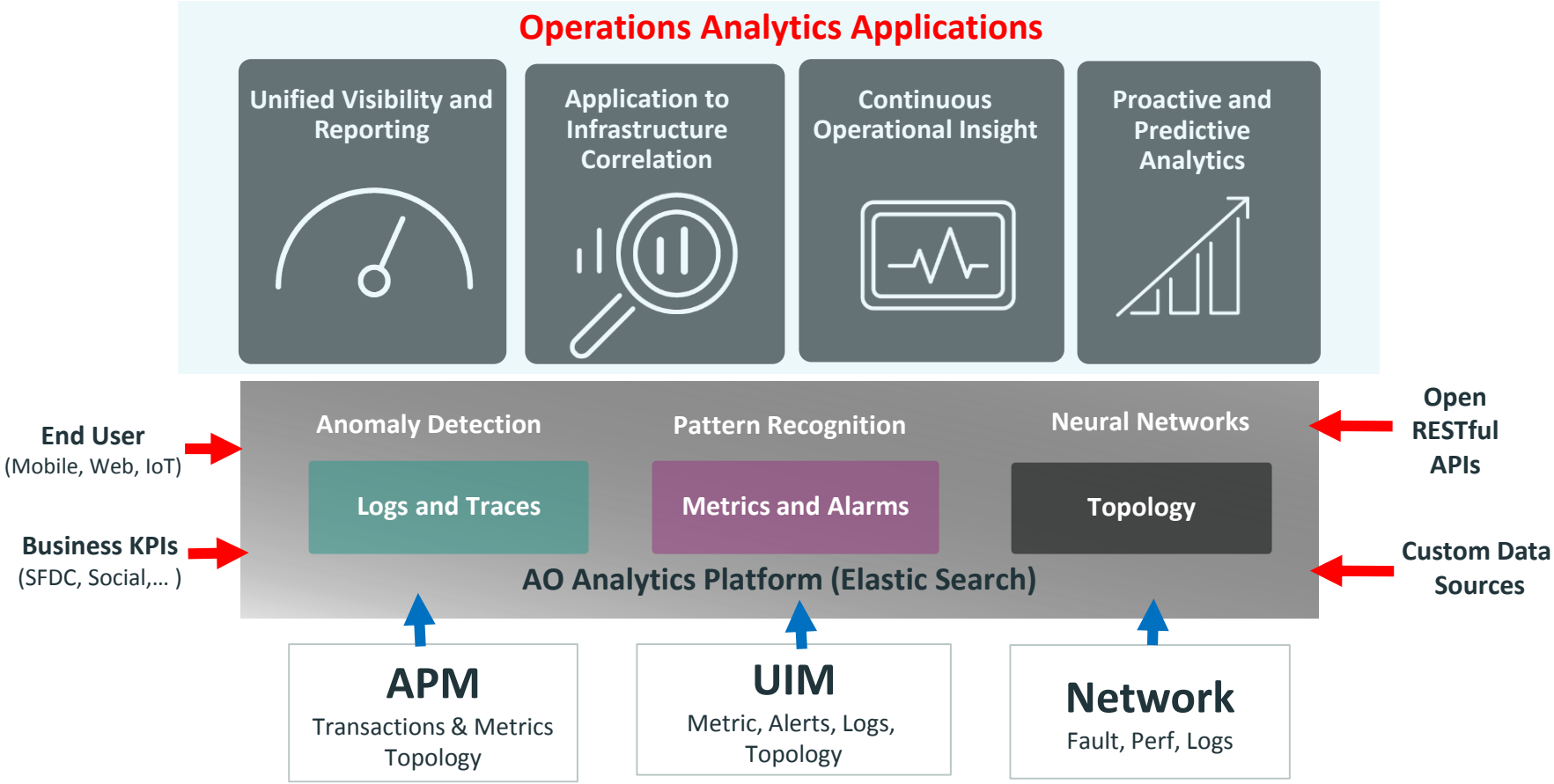
"Implement the combination of unified monitoring and log analysis tools to support availability management goals"

- Existing solutions are fragmented. Monitoring vendors (BMC, Nagios, New Relic…) lack sophisticated analytics. Analytics vendors (Splunk, Sumologic) lack monitoring and diagnostic capabilities. Solarwinds (with Papertrail) has both, but Analytics is too nascent and limited.
- Existing tools offer either Log Analytics or IT Operational Analytics, but hardly both

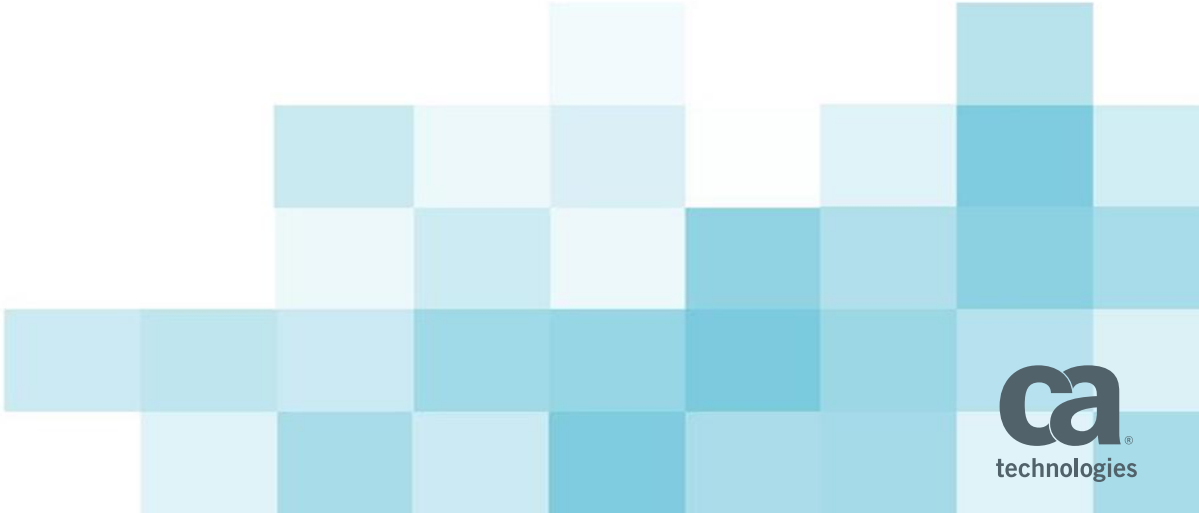
CA's Strategic Advantage

- Leader in infrastructure monitoring
  - Millions of assets monitored across **1000+** customers
  - **~150** Probes covering on-prem and cloud assets including apps
- Leader in Applications Monitoring
  - Ability to capture and anchor around business metrics
  - AXA has already been a forerunner in App Experience Analytics
- Powerful open-standards, open-source based analytics platform

WHAT: Overall Picture



How: (some UIs are conceptual)

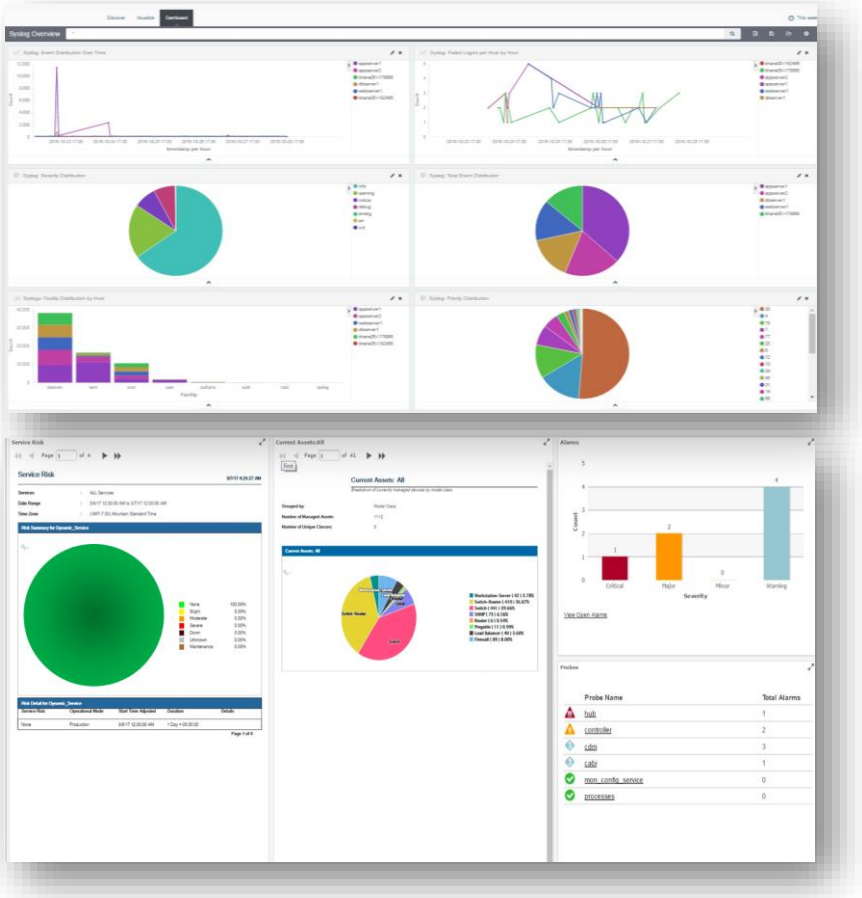


Unified Visibility and Reporting: Dashboards

Multi-source aggregation with modern dashboards

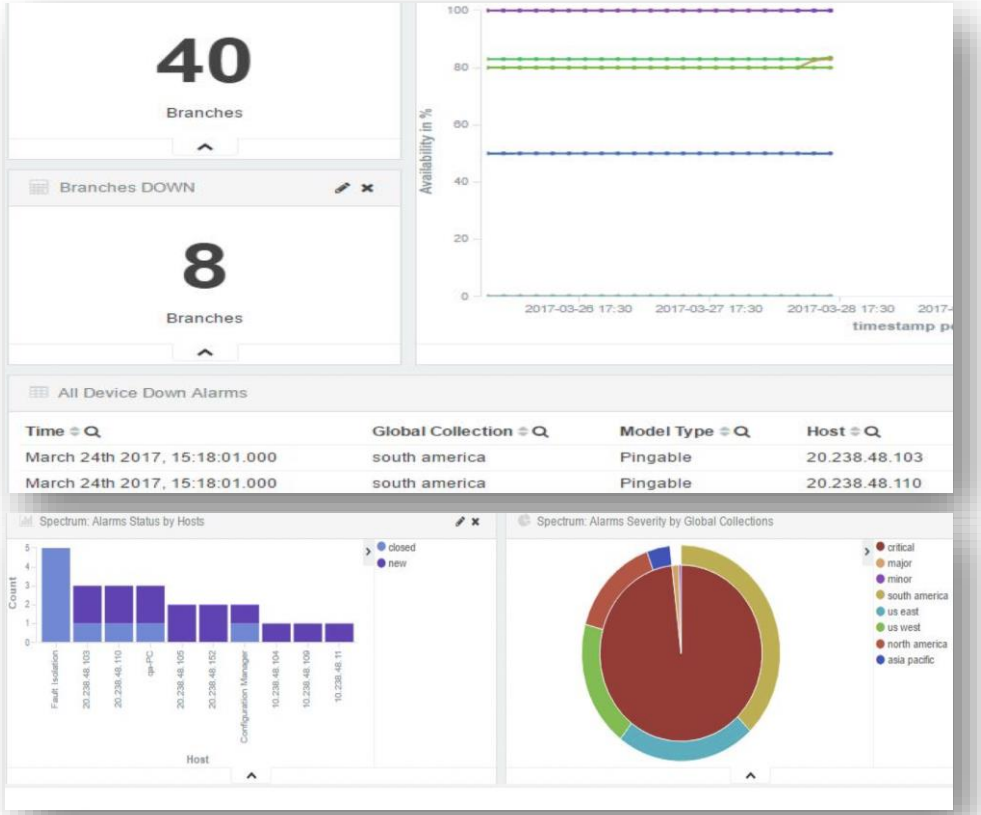
Out-of-box reports for inventory, SLA and Top-n Alarms

Drag-and-Drop creation, easy to publish and share



Unified Visibility and Reporting: Representative Use Cases

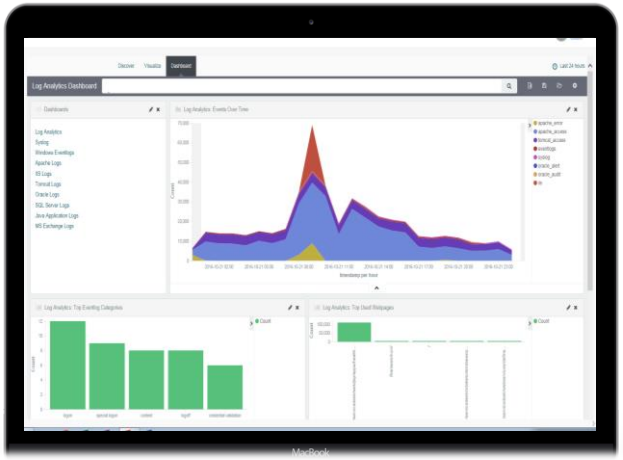
- Show the overall availability for the targets in each Geographic Location and for each location list the top-n offending targets
- List all the Linux targets across my IT estate grouped by location (AWS, On-Prem) and sub-grouped by Production versus Test
- For an MSP, find the most common operating system and database versions across multiple tenants and notify customers whose versions are reaching end-of-life



App-to-Infra Correlation: Log Analytics

Contextual Insights for rapid issue identification

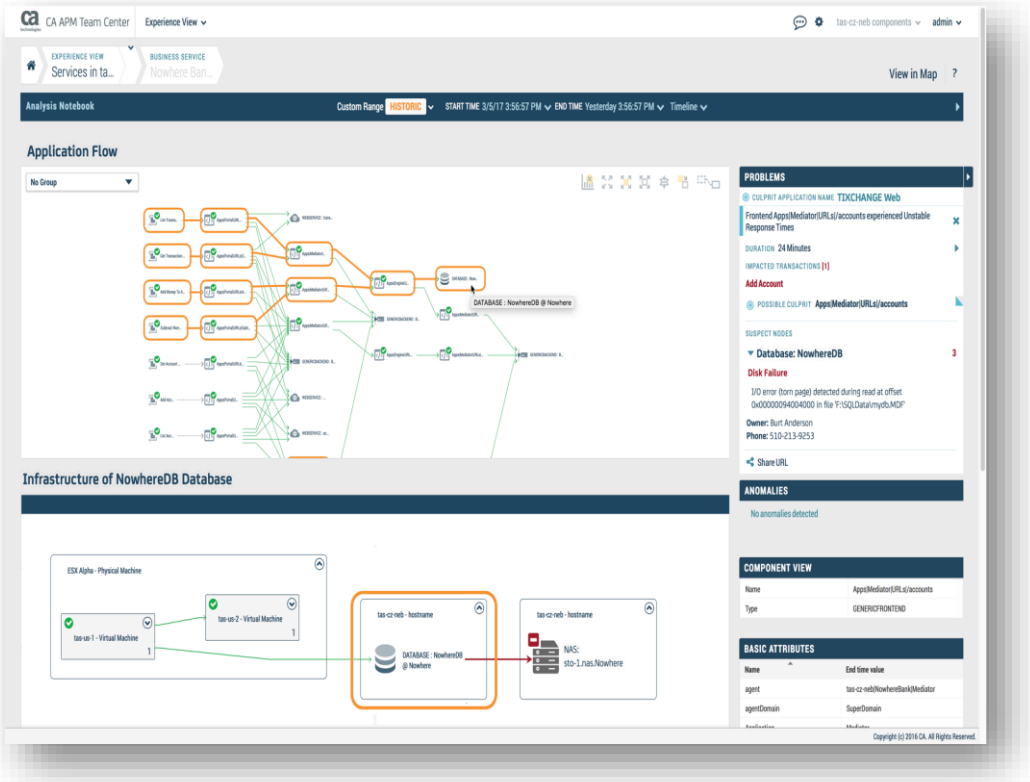
- Multi-source aggregation with out of the box dashboards and reports
- Search and ad-hoc analysis
- Contextual Alerting
- Ability to correlate different events
- Unified, template based configuration



App to Infra Correlation: Providing in-context drill-downs

Detect Anomalies in Application Context. Example: Intermittent database errors leading to lower payment processing compared to seasonal transactional volume

Contextual funneling and drill-down into respective domain-specific tool to diagnose the root-cause



App-to-Infra Correlation: Outlier Detection, Dynamic Baselining and Anomaly Detection

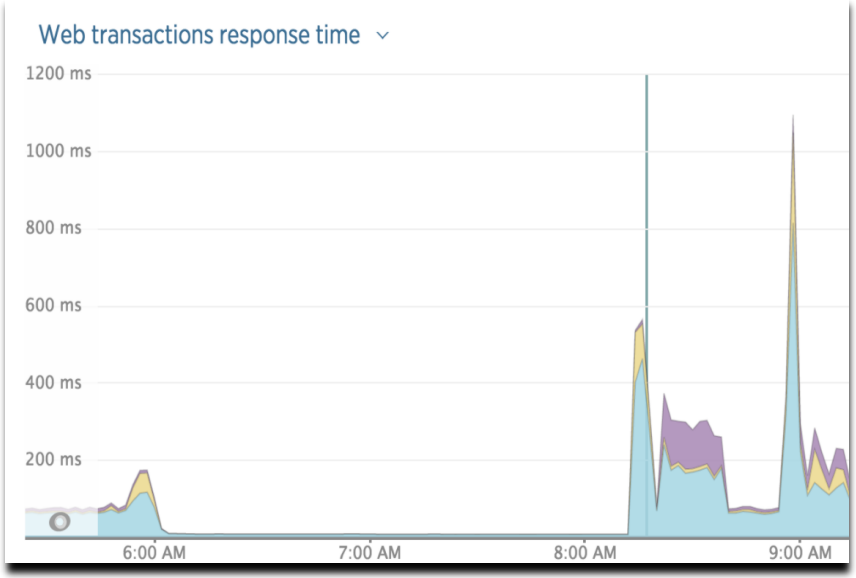
Detect outliers based on a range of metric value.

- Example: Of all the webservers in a pool of webservers, find the one with abnormally high error count

Dynamic Baselining based on range, seasonality and machine learning

Anomaly Detection. Example:

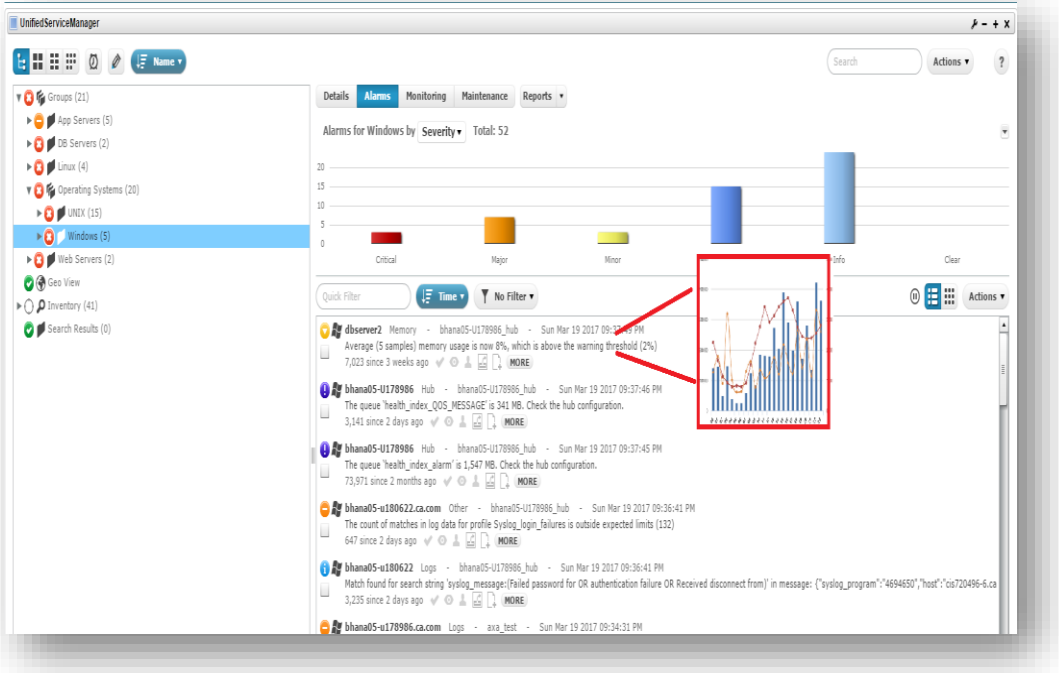
- Month-end payroll application taking longer to complete than usual and causing I/O spikes



App to Infra Correlation: Representative Use cases for Metric-Log Correlation

- Correlate a metric event (such as a spike in network activity) with a log event (multiple login attempts) using a single timeline

- Correlate multiple log events to an alarm that followed immediately after, example: multiple disk errors preceding a database crash

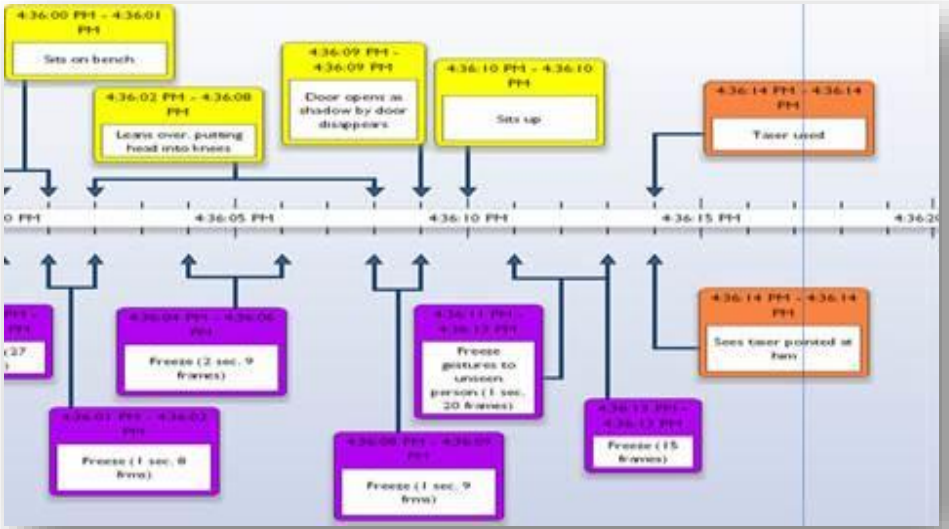


Continuous Operational Insight: Simpler Visualization under a Single Pane

Timeline representation of alarms, open tickets and related CIs

Color coded alarms to denote source (UIM, Spectrum, ..) of the alarm to help in deep-dive diagnosis

Collaboration among multiple Admins

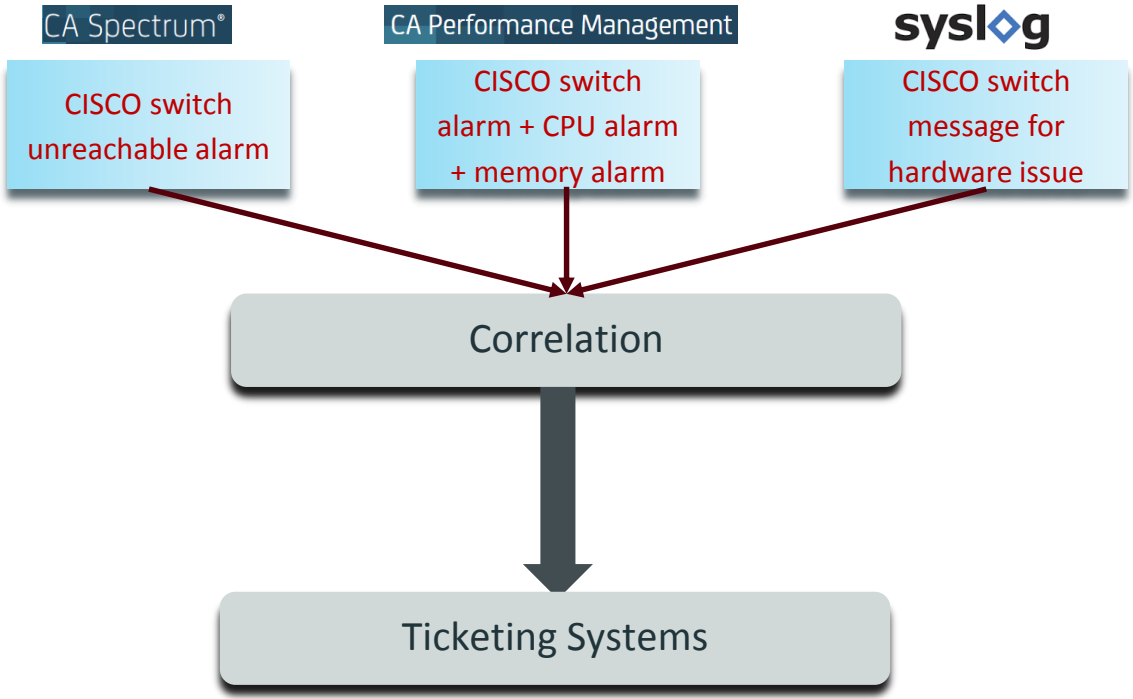


Continuous Operational Insight: Noise Reduction

Noise Reduction: Minimize the number of tickets by combining multiple events from disparate data sources into a single alarm. Example:

> For an alarm generated in Spectrum, review the SYSLOG and CAPM events and combine them into a single outgoing ticket

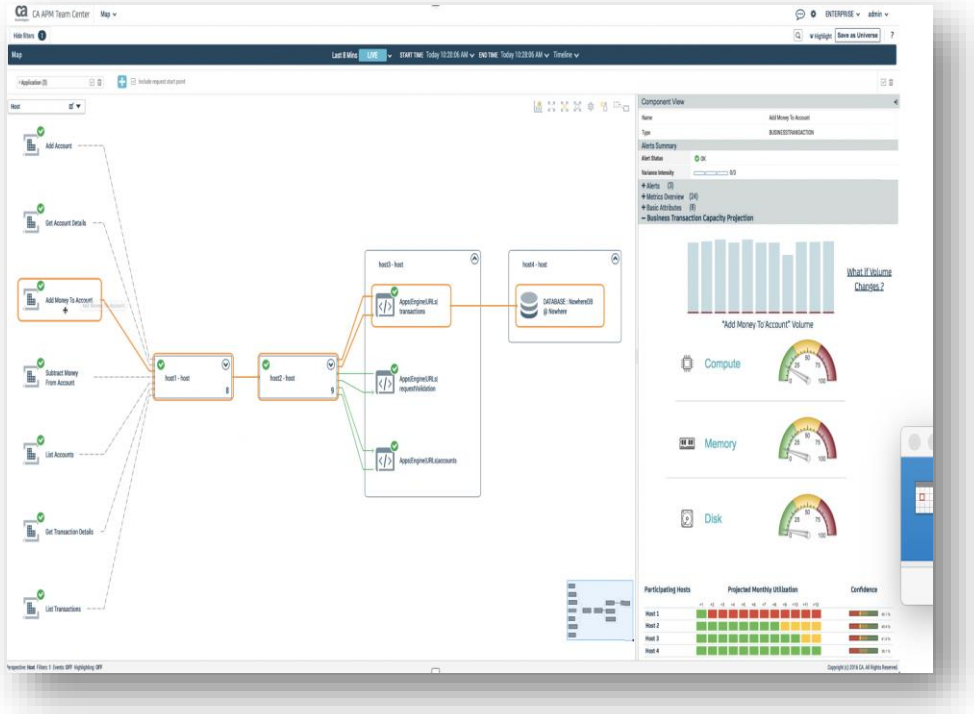
Root-Cause Detection: If Multiple alarms precede a major alarm or outage, the Timeline view helps in associating them to the eventual outage. Example: Several network packet drops before a router actually going down



Proactive and Predictive Analytics: Capacity Planning

Predict possible saturation of IT resources based on trends in application transaction volume

What-if analytics to gauge the impact of transaction volume to actual IT capacity



Based on current trends, predict if the SAN storage needs additional capacity to accommodate a 20% increase in transaction volume

CA Agile Operations

Analytics Deliver Insights
for Flawless Digital Experiences