Root Cause Analysis

Andrew Burger

Vice President

September 2001

bmcsoftware

What is RCA?

**RCA is a
problem analysis methodology to
rapidly isolate and identify the root
cause of application availability
problems across complex
technologies. Coupled with true
Service Level Management and
Predictive Modeling, this methodology
can prevent problems from impacting
service delivery**

RCA Challenges

- Environmental complexity
  - Multiple components (e.g. Network, Server, Application, Web, etc.)
  - Constant change (configuration, dynamic load balancing, etc.)
- Huge, irrelevant data volumes
  - Application, System, Network
  - Doesn't map to end user experience
- Scarce, expensive technical resources

RCA Market Needs

- Understand client view of service
  - Independent of technology underpinnings
  - Hide the data and complexity
- Rapidly identify root cause of service problem
  - "80/20 is good enough"
  - Save scarce experts for the 20!
- "Learn" to prevent problems
  - Keep from happening again
  - Ideally before they occur

RCA Technology Approaches

- Higher Understanding of "Application system"
  - E.g. Service Level Management and Fault Analysis
    - Service views of availability and responsiveness
    - Models of topology, components, application system
  - Strengths: Service view, rapid ("real time") fault isolation
  - Weaknesses: building Fault models, adapting to change, missing critical details, etc.

- Lower Understanding of "Application system"
  - E.g. Statistical Analysis and Predictive Modeling
    - Analyze time series data to determine patterns
    - Model behavioral response to change
  - Strengths: captures critical details, adapts to change
  - Weaknesses: not real-time

Higher Understanding of Application System

- Service Level Management (PATROL for SLM)
  - High level understanding of how application system works
  - Definition of, and measurement against, service levels
  - Reports for high level view/isolation of problem areas. Alerts for rapid notification

Lower Understanding of Application System

- Statistical Analysis (PATROL Dashboard, PATROL Perform, OptiTrak)
  - Complete time-series data on many/all components of the application system
  - Statistical analysis performed to identify root cause(s) with highest correlation to the problem

- Predictive Modeling (PATROL Predict)
  - Models cross-server environment using time-series data
  - Identifies impact of change in demand on utilization and responsiveness – before change occurs

BMC: A Service Centric Approach

- Enables quicker problem resolution to help improve service levels

- Evolves foundation monitoring to a service-centric approach
  - Transcends application and system boundaries
  - Provides diagnostic solution platform

- Saves resources by allowing users to address the real problem
  - Eliminates redundancy within the IT organization
  - Allows users to ignore sympathy events

- Understands how Diagnosed failures impact the environment
  - Services affected by any outage resulting from the root cause problem
  - Recommendations for repairing the outage

- Key enabler for automation/self-sufficient systems
  - If the root cause problem cannot be determined, it is impossible to initiate an automated recovery action.

- Enables customers to achieve a quick ROI

Integrated RCA solution from BMC Can:

- **Discovers the Environment**
  - Discovers the application environment and IP connectivity (L2/L3)
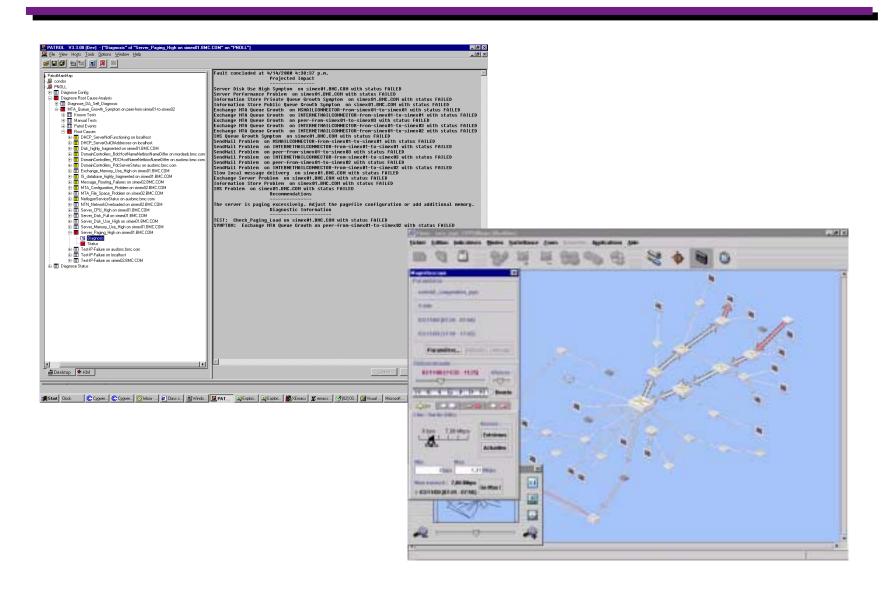 - Automatically adapts to changes

- **Performs Analysis**
  - Identifies key problem symptoms
  - Analyzes events to determine the root cause of failures
  - Enables service-oriented fault isolation for the entire application stack

- **Presents Results**
  - Presents impact analysis of failed service
  - Provides an audit trail for analysis involved with diagnosis
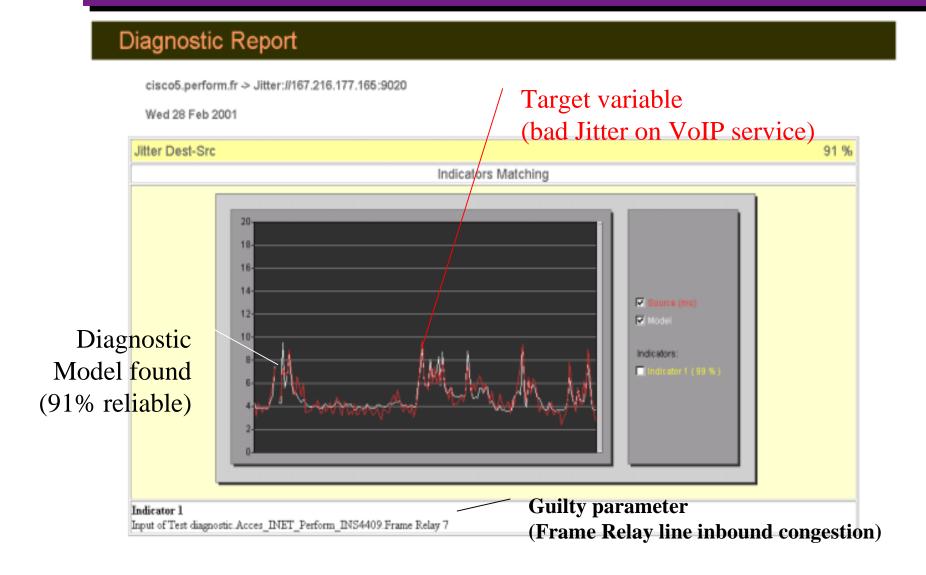 - Provides recommendations for corrective actions

L2 Topology Root Cause Analysis

Statistical Analysis

- Use single variable and multi-variable time series correlation analysis to identify the root cause.

  - "Response was fine at 1:00 PM and terrible at 1:30 PM. Which change between 1:00 PM and 1:30 has the highest correlation to the change in response time?"

- When the pattern begins again, we can alert on a pending problem and its probable root cause.

  - As problems and their root causes tend to repeat, a pattern of change in certain components that precedes a problem can be identified

DashBoard Diagnostics

Diagnostic Report

cisco5.perform.fr -> Jitter://167.216.177.165:9020

Wed 28 Feb 2001

Jitter Dest-Src   91 %

Indicators Matching

**Target variable
(bad Jitter on VoIP service)**

Diagnostic
Model found
(91% reliable)

☑ Source (ms)
☑ Model

Indicators:
☐ Indicator 1 (99 %)

Indicator 1
Input of Test diagnostic.Acces_INET_Perform_INS4409.Frame Relay 7

**Guilty parameter
(Frame Relay line inbound congestion)**

Integrated RCA solution from BMC

- With PATROL, all data (event, historical, analysis) shares namespace and repository for all solutions to populate and consume
  - PATROL
  - PATROL for Service Level Management
  - PATROL Perform/Predict
  - PATROL Dashboard
- Statistical Analysis input to Fault and Predict models to improve capabilities
  - Intelligent, automated thresholding
  - Predictive alerting
- Greater automation of Fault Modeling and Statistical Analysis