SmartCloud Analytics – Log Analysis

Clyde Richardson  (richarcl@us.ibm.com)
Technical Sales Specialist

Anuja Deedwaniya (anujad@us.ibm.com)
IBM z Systems Enterprise Architect

Paul Smith (Smitty) (paulmsm@us.ibm.com)
IBM z Systems Service Management / zAnalytics Architect
Agenda

• Problem Diagnosis and Resolution – Finding a needle in a haystack
• Predict, Search, Optimize
• SmartCloud Analytics – Log Analysis
  – Capabilities
  – Interface
  – Integration with your Service Management Tooling
  – Coming Soon … Join the Beta
  – Reference Materials
  – Solution Demo
Centralized, Distributed, Cloud, Resilient Architectures Increase Data Volume

Analysis – The Problem

Find the right needle in one of many haystacks – QUICKLY!

Where do I start??

Logs, Traces,..

Core files

Events

Metrics

Transactions

Config

Everything is “green”

404 ERROR

It’s SLOW!!


010001100011100001110110001111100001100011100011

Find the right needle in one of many haystacks – QUICKLY!
IBM focused on managing end-to-end analytics for improved performance and workload management

**Predict:**
- Pro-Active Outage Avoidance
- Predict problems before they occur

**Search:**
- Quickly search large volumes of log data from a single search bar
- Perform log analysis while searching
- Correlate messages from multiple logs for end-to-end problem diagnosis

**Optimize:**
- Improve performance across IT Infrastructure

---

**IBM Analytics solutions for System z**

**Proactive Outage Avoidance**
- OMEGAMON & NetView w/ IBM zAware

**Faster Problem Resolution**
- IBM SmartCloud Analytics - Log Analysis

**Optimized Performance**
- IBM Capacity Management Analytics (CMA)
Search for and rapidly analyze unstructured data to assist in and accelerate problem identification, isolation and repair

**SmartCloud Analytics – Log Analysis**

**Differentiating Capabilities**

Locate **component error messages** from system, configuration, software and event logs **via rapid indexed search**

- Search logs and events across multiple platforms (distributed and mainframe), LPARs, CECs, applications, middleware, subsystems

Isolate issues and provide insights across various domains including WebSphere, DB2, CICS, IMS, MQ, OS, etc

Link support documentation and operations notes **dynamically** to log messages and events to resolve problems quickly

Visualize search results with analytic tools to rapidly **perform root cause analysis**
Search for and rapidly analyze unstructured data to assist in and accelerate problem identification, isolation and repair

**SmartCloud Analytics – Log Analysis**

**Delivering Business**

Reduce mean time to repair by identifying and isolating service impacting issues quickly

Resolve problems more efficiently with faster access to all pertinent information

Reduce effort by consolidating, analyzing information in real-time

Improve service availability by leveraging expert knowledge of applications and infrastructure

Built on IBM’s leading Big Data platform
IBM expertise built-in
Download and install in minutes for quick time-to-value
Customer Experiences

Large Insurance Company
• Experienced an application outage that resulted in the team working around the clock for 29 hours pouring through logs and traces to determine the root cause of the issue. After the issue was resolved, the logs were captured and sent to IBM lab for analysis using SCA-LA. Within minutes, the IBM team was able to see the scope of the issues, and find the relevant PTF to resolve the issue through the integrated expert advice.

State Agency
• Were able to download, install, configure and use SCA-LA to search their logs in 2.5 hours.

Numerous Customers
• Errors lurking in logs that are never examined because they don’t necessarily cause SLA or performance problems. For example, SCA-LA found over 4,000 invalid login attempts in a three day period that had otherwise gone unnoticed.
IBM SmartCloud Analytics – Log Analysis z/OS Insight Packs & SCA-LA Server

- z/OS Log Forwarder is installed on each z/OS LPAR to enable Log Search
- The SCA-LA server is installed on z Systems (or System x) running Linux (64 bit)
- z/OS Insight Packs for WebSphere and SYSLOG are installed on the SCA-LA server

Arrows show flow of data from logs to SCA-LA user interface.
Simple free form searches can be performed
- Search for “error” for example
- OR is the default operator
- AND or + is the AND operator:
  - +MessageType:"E" + MessageID:"CSQX599E"
  - MessageType:"E" AND MessageID:"CSQX599E"
- Exclude terms with the NOT or – operator:
  - +MessagePrefix:"CSQ" NOT MessageType:"I"
  - +MessagePrefix:"CSQ" – MessageType:"I"
- Quotes can be used for phrases containing spaces:
  - “ended abnormally”
- Parentheses for grouping:
  - (+MessagePrefix:"CSQ" +MessageType:"E") OR (+MessagePrefix:"CNZ"+MessageType:"E")
- Field designator to restrict search to a particular field:
  - MessagePrefix:"CSQ"

Easily create and save your own search string and application views!
SCA-LA: Search syntax …

- * wildcard for multiple characters:
  - test* might return test, tests or tester.
- ? wildcard for any single character:
  - te?t might return text or test

Easily create simple or advanced queries.
- Online Help available from the Learn More → Search Bar → Search query syntax menu:
Integration with Performance Monitoring

OMEGAMON + SCA-LA – Launch in Context from TEP

The **One Two – Punch**: Combine two very powerful tools to ensure performance and high availability of your enterprise.

- **Perform log analysis in context of OMEGAMON workspaces** – This approach enables OMEGAMON users to perform in-context log analysis while doing problem determination
  - From your OMEGAMON workspace, use the SCA-LA search bar to search logs (using LPAR or Sysplex as the default context)
  - Easy to implement - Configure TEP to display the SCA-LA search bar

Launch SCA-LA from OMEGAMON performance monitoring workspaces to search logs in context
Integration with Event Management

Network Operations Insight + SCA-LA – Search and Analyze Events

Event Analytics – for Seasonal Event Identification (New)

Provides opportunities for event reduction thus improving operational efficiency.

- Easily identify ‘related’ Events that may be candidates for suppression
- Identify “difficult to spot” seasonal events that often result in regular periodic problems
- Leverage visualizations that help you quickly isolate more severe and significant problems.

Also, SCA-LA can generate notifications based on data (logs messages, data, etc)
In Beta Now

- Analyze your SMF data AND your log data for a complete view of the enterprise.

- Also, Search and provide network Insights with our new Network Insights Pack
The IBM SmartCloud Analytics - Log Analysis for z/OS V.next Early Access and Beta Program was announced on January 29, 2015.

In 2015, we will build on the strong foundation established over the past months by providing insights into additional domains, as well as by enhancing existing insights through integration of performance metrics.

We are looking for customers and business partners worldwide who would like to test the new capabilities and help shape the content of the release under development.

To see the full program announcement, and to learn how to sign up, please visit us in our developerWorks community at:

https://ibm.biz/BdEkZV
Additional SCA-LA Reference Material

- Analytics Overview Video
  - [https://www.youtube.com/watch?v=OQJapWiQECs](https://www.youtube.com/watch?v=OQJapWiQECs)

- SCA-LA z/OS Insight Packs videos:
  - [http://www.youtube.com/watch?v=2oDgX_Ydr18](http://www.youtube.com/watch?v=2oDgX_Ydr18)
  - There are several YouTube videos – search for ‘SmartCloud Analytics – Log Analysis’

- SCA-LA z/OS Insight Pack Documentation
  - Knowledge Centers

- SCA-LA Product Documentation
  - Service Management Connect
  - Knowledge Center
Send us your logs!

- Request a product demo using logs from your own test, development or production environments

- IBM will load your logs into a SCALA server, then demo the results back to you
  - A secure, dedicated drop box will be assigned to you
  - You will be sent detail upload instructions via email
  - Any file uploaded will be automatically moved to a dedicated SCALA environment within 24 hours
  - All log data will be purged from the SCALA environment within 48 hours after the demo event

To request your hosted demo, visit: http://services-useast.skytap.com:18280/WebDemo/
Demo
Thank You
Backup slides in case you can’t do the demo
Launch SCA-LA (in context of LPAR) from OMEGAMON Workspace

LPAR Scenario - OMEGAMON user searches for the word ‘error’ in the LPAR’s logs

SCA-LA search bar now available in TEP

Specify search string

Specify search time frame

Search will be done in context of LPAR
Launch SCA-LA (in context of LPAR) from OMEGAMON Workspace...

Search results displayed in SCA-LA

Notice there is only 1 SystemName (LPAR)

Insights surfaced during search

Search string provided from OMEGAMON workspace

Search results with search strings highlighted
Simple Search Interface – Easy to Customize

- Enter search string
- Search specific logs or ALL logs
- Timeframe
- Save My Search
WebSphere Application Server Search – java Exception pattern

Example of search capabilities plus insights

Log analysis displays number of exceptions during this timeframe

Search WAS log

Timeframe of problem

Search results
Quickly and easily access IBM Support Portal based Expert Advice from Log Analysis

Search for expert advice with the click of a button

All IBM support site documents that reference messages from search results

Launch to Technote
Sample dashboard – Out-of-the-Box or Build your Own!