Exploiting IT Log Analytics to Find and Fix Problems Before They Become Outages

Session 17595

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

Anuja Deedwaniya (anujad@us.ibm.com)
IBM z Systems Enterprise Architect
Rapid growth of data from latest technologies can be supported seamlessly on z Systems.

*z Systems scaling model and security to manage and optimize both*

- Business Transactions
- Quality of Service
- Command & Control
- Facts and data “source of truth”
- z/OS Systems

- Mobile and Social
- Dynamic
- Interactions and Collaboration
- Insight, trends, analytics

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
Analytics for System z addresses rapid growth of data and next generation technology

• Much greater amount of critical IT operational data (SMF, log, journal) than distributed-only environments.
  • Focus on problem determination and time to resolution while placing premium on availability of services and applications.
    ▪ 100x to 1000x explosion in data flooding existing tools.
    ▪ New runtimes, programming languages needing complex instrumentation.
• By 2016, 40% of Global 2000 enterprises will have IT operations analytics architecture in place, up from < 1% in 2014, looking to integrate across their enterprise to reduce outages (Gartner).
• 90% of the Fortune 1000 companies are running z and have ‘Systems of Record’ dependencies for transactional processing and data serving applications.
Operations Analytics is the next step in IBM value add for enterprise performance and availability management

- This journey started with NetView/SA
  - Too many messages
  - Need to filter, automate, generate events
- Next focus was on performance monitoring
  - Slow and under-capacity systems are just as bad as unavailable systems
- Next step – Enable the data to work for YOU
  - Analyze existing data, surface anomalies, predict outages and decrease mean time to recovery (MTTR)

NetView/SA
System/Network management and automation

OMEGAMON
System and sub-system performance monitoring

IT Analytics
- Analyze metric and log data
- Predict outages
- Forecast capacity, CPU, etc.
- Surface anomalies
- Improve search techniques
- Reduce MTTR
- Provide expert advice
- Plug into existing service management tooling

Note that NetView/SA and OMEGAMON are NOT required for IT Analytics

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
IBM is 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 data from a single search bar
- Perform log and performance 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**

- **Predict**
  - OMEGAMON & NetView w/ IBM zAware

- **Search**
  - IBM Operations Analytics for z Systems

- **Optimize**
  - IBM Capacity Management Analytics (CMA)

---

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
This solution was previously branded as ‘IBM SmartCloud Analytics - Log Analysis’.

The support to search and analyze z/OS logs was initially provided in March, 2014 under the following product names:

- IBM SmartCloud Analytics - Log Analysis z/OS - Insight Packs – SYSLOG V1.1
- IBM SmartCloud Analytics - Log Analysis z/OS - Insight Packs - IBM WebSphere® Application Server V1.1

Subsequent releases were named with the SmartCloud brand until April, 2015 when Version 2 of the product was rebranded to

**5698-AAP IBM Operations Analytics for z Systems V2.1.0**

Note that the distributed product is now named **IBM Operations Analytics – Log Analysis**
IBM Operations Analytics for z Systems

Accelerate problem isolation and identification
Reduce mean time to repair

- **Analyze** various types data (logs and metrics) from multiple sources (mainframe and distributed)
- **Locate problems** from system, configuration, software logs and performance metrics using **rapid index search** and **pattern analysis**
- **Isolate issues** across various domains including OS, Middleware, applications, etc
- **Leverage Expert Advice** via links to support documentation and operations notes to resolve problems quickly
- **Visualize** search results with analytic tools to **rapidly determine root cause**
- **Out-of-the-box analysis and insights** for z/OS, WebSphere, DB2, CICS, IMS, MQ, Network as well as distributed systems
- **Fully customizable** to meet your needs

**New in 2015**
- Network Insights
- Event notification
- Hadoop Support
- Analysis of Performance Metrics (new SMF real time Data Provider)
- Integration with ITM/OMEGAMON and Netcool Operations Insight, Service Management Unite, Trouble Ticketing
IBM Operations Analytics for z Systems

- The IBM Operations Analytics server is installed on z System (or x System) running Linux (64 bit)
- z/OS Insight Packs are installed on the IBM Operations Analytics server
- z/OS Log Forwarder / SMF Data Provider installed on each z/OS LPAR where you want to provide Search and Analysis

Operations Analytics Server

Applications
Search
 Frozen Tier
Warm & Cold Tiers
Alerts
Indexers

Annotators
Insight Pack (z/OS)

Generic Receiver

Mainframe

z/OS

SMF Real-time Data Provider

z/OS Log Forwarder

WAS SYSPRINT
WAS SYSOUT
z/OS Syslog
CICS MSGUSR
USS Log Files

z/Linux

Log File Agent

WAS SYSPRINT
WAS SYSOUT
DB2
DB2 App
Syslog
Web Access Log

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
Simple Search Interface – Easy to Customize

- Enter search string
- Search specific logs or ALL logs
- Timeframe
- Save My Search

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
WebSphere Application Server Search – java Exception pattern

This is just one example of many

Log analysis displays number of java exceptions during this timeframe

Search WAS log

Timeframe of problem

Search results

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
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

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
Sample dashboard – View your log and metric data however you like

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
Analyze your SMF data AND your log data for a complete view of the enterprise
Create your own – Queries, Dashboards, Feeds

The Out-of-the-Box capabilities provide immediate value. Additionally, IOA can easily be tailored to your specific needs.

- Perform simple free-form searches using the standard set of search keywords and operators
- Build complex queries with range searches and DateMath functions
- To learn more, consult Online Help available from the Learn More → Search Bar → Search query syntax menu:

- BYOD – Bring your own Data – The z/OS Log Forwarder can be configured to forward your text logs to enable the Search capability.
- BYOIP – Build your own Insight Pack
- BYOV – Build your own Views

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
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 IOA for z Systems. 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 IOA for z Systems 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, IOA for z Systems found over 4,000 invalid login attempts in a three day period that had otherwise gone unnoticed.
Integration with Service Management Solutions

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
Event Analytics – for Seasonal Event Identification

- 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.
Log Analysis Integration with existing Service Management Solutions

Event Management OMNIbus/Netcool Operations Insight
Problem Determination NetView CANZLOG
Performance Monitoring ITM/OMEGAMON

Search and analyze logs, metrics and events

POWerful tools integrate to ensure performance and high availability of your Enterprise.

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
Send us your logs!

- Request a product demo using logs from your own test, development or production environments
  - IBM will load your logs into an IBM Operations Analytics 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 IBM Operations Analytics environment within 24 hours
    - All log data will be purged from the IBM Operations Analytics environment within 48 hours after the demo event

To request your hosted demo, visit:
http://services-useast.skytap.com:18280/WebDemo/

Or take the product for a test drive using IBM-provided sample data at:
http://zscala.ibmzoperationsanalytics.com:9182/ZLALiveDemo
Announcing the IBM Operations Analytics for z Systems Early Access and Beta Program!

In 2015, we are building on the strong foundation established over the past months as we develop and implement our product roadmap.

We are looking for customers and business partners worldwide who would like to help influence our roadmap and test new capabilities. The program is open-ended; interested participants may join at any time and stay on as long as they wish. That said, it is our desire to establish a set of “customer sponsor” relationships that will become instrumental in shaping the future of our offering.

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
Summary

- IBM has various solutions for IT analytics that address different use cases.
  - **IBM zAware** for proactive anomaly detection and faster diagnosis
  - **Operations Analytics for z Systems** for faster problem diagnosis with search, analysis and expert advice.
  - **Capacity Management Analytics (CMA)** to enable optimal use of z Systems and Distributed Systems capacity by managing and predicting consumption of IBM® z Systems® and Distributed infrastructure resources
IT Analytics SHARE Presentations

Monday - 12:30pm-1:30pm - Southern Hemisphere 3
Lunch & Learn - IT Operations Analytics Solutions for z Systems
Speaker: Paul Smith, z Systems Service Management Architect

Thursday – 11:15am-12:15pm - Southern Hemisphere 5
Session 17595 – Exploiting IT Log Analytics to Find and Fix Problems Before They Become Outages
Speaker: Paul Smith, z Systems Service Management Architect

Thursday – 1:45pm-2:45pm - Europe 2
Session 17442 - z/OS Log Analysis Product Shoot-Out: CorreLog, Syncsort/Splunk and IBM
Speaker: Paul Smith, z Systems Service Management Architect

Thursday – 4:30pm – 5:30pm - Southern Hemisphere 1
Session 17879 - Taking z System Resiliency to New Heights with IT Analytics
Speaker: Anuja Deedwaniya, z Systems Architect

Complete your session evaluations online at www.SHARE.org/Orlando-Eval