z/OS Log Analysis Product Shoot-Out: CorreLog, Syncsort/Splunk and IBM

Session 17442

IBM Log Analysis

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

#SHAREorg

The Challenge

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

404 ERROR

It's SLOW!!

Where do I start??

Centralized, Distributed, Cloud, Resilient Architectures Increase Data Volume

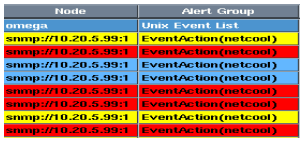
Everything is "green"

Logs, Traces,..

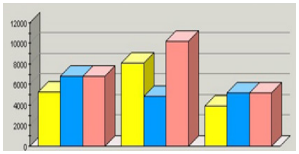
[10/9/12 5:51:38:295 GMT +05:30] 0000006a servlet E com.ibm.ws.webcontainer.servlet.ServletWrapper service

Core files

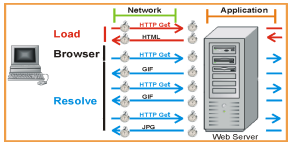
Events



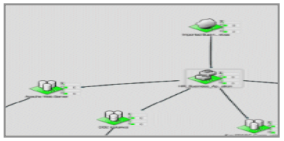
Metrics



Transaction



Config



Operational Analytics – Rationale and Approach

Analytics – Turning data into information and information into 'Insight'!

- Better/faster/more efficient/smarter processing of **very large volumes of data**; **gaining insight from data from multiple sources**; analyzing and correlating different types and sources of data to predict and prevent problems; to ultimately **Ensure availability and performance of the systems and business-critical applications in the enterprise**;
  - IBM solutions are built to **address customer challenges**. We build solutions based on expertise and real-life scenarios received from customers, system, middleware and application experts and support personnel that address and **resolve REAL client problems** for a living.
- Customers need **predictive** tools that surface anomalies, perform problem determination quickly and efficiently and optimize their enterprise applications.
- IBM analytics is NOT about collecting more data. It is about efficiently analyzing vast amounts of IT data; better; **harvesting value and insight** as close to the source as feasible with minimal processing.
- IBM can help you create a Service Management solution from scratch OR if you have an existing Services Management solution, you can use the existing data and build an integrated solution.

Move from reactive to proactive!

Avoid manual analysis and correlation of data!

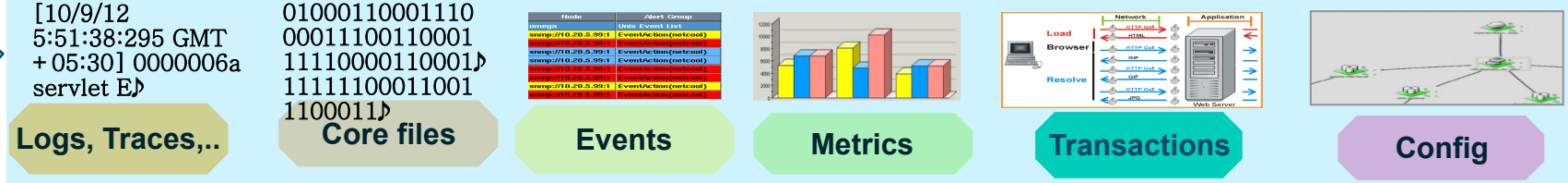
Let analytics do the heavy lifting!

Operational Analytics Integrates with your existing Service Management Solution

SHARE
Educate · Network · Influence

IBM integrates Analytics into their Service Management solutions and surfaces Insights to the management dashboards

Huge Volumes of Data; Many Types



Operational Environment

IBM Operations Analytics for the Enterprise

Avoid outages and accelerate problem isolation and identification
Reduce mean time to repair

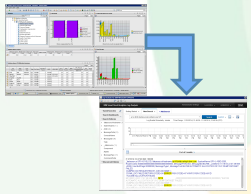
- **Analyze** various types data (logs and metrics) from multiple sources (mainframe and distributed)
- **Locate problems** from system, configuration, software logs and performance metrics using **machine learning** and **rapid index search**
- **Isolate issues** across various domains including OS, 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, etc as well as distributed systems
- **Fully customizable** to meet your needs

SEARCH

ANALYZE

RESOLVE

INTEGRATE

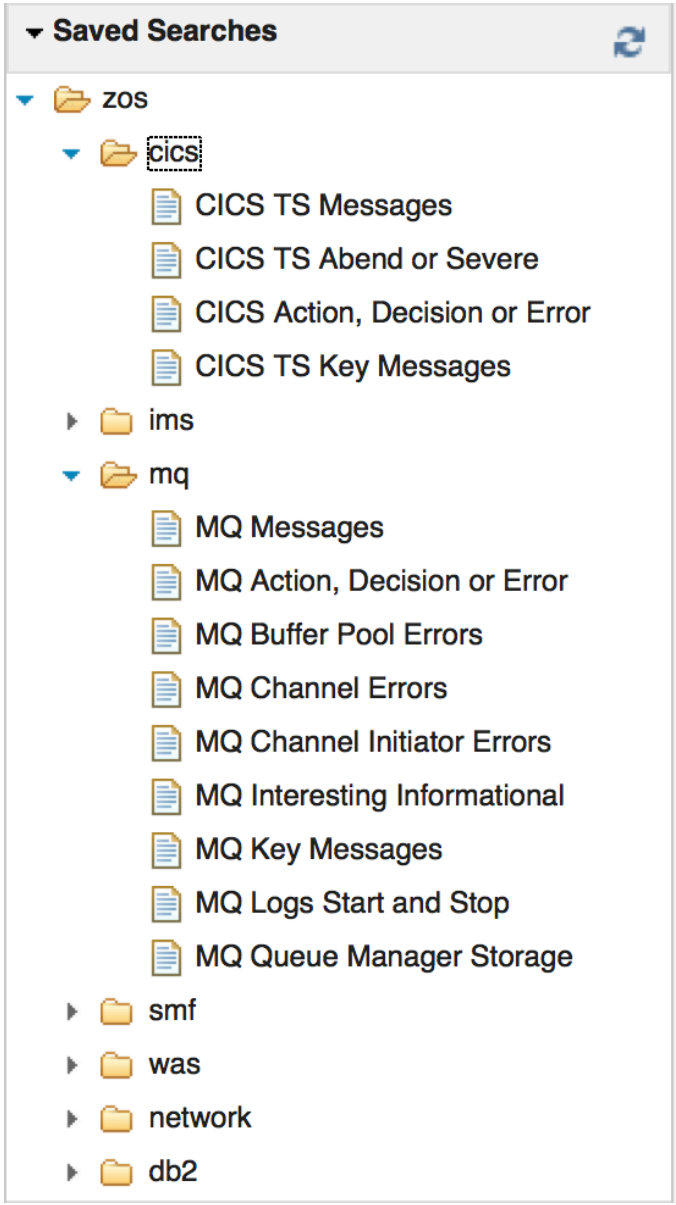


in 2015

- 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

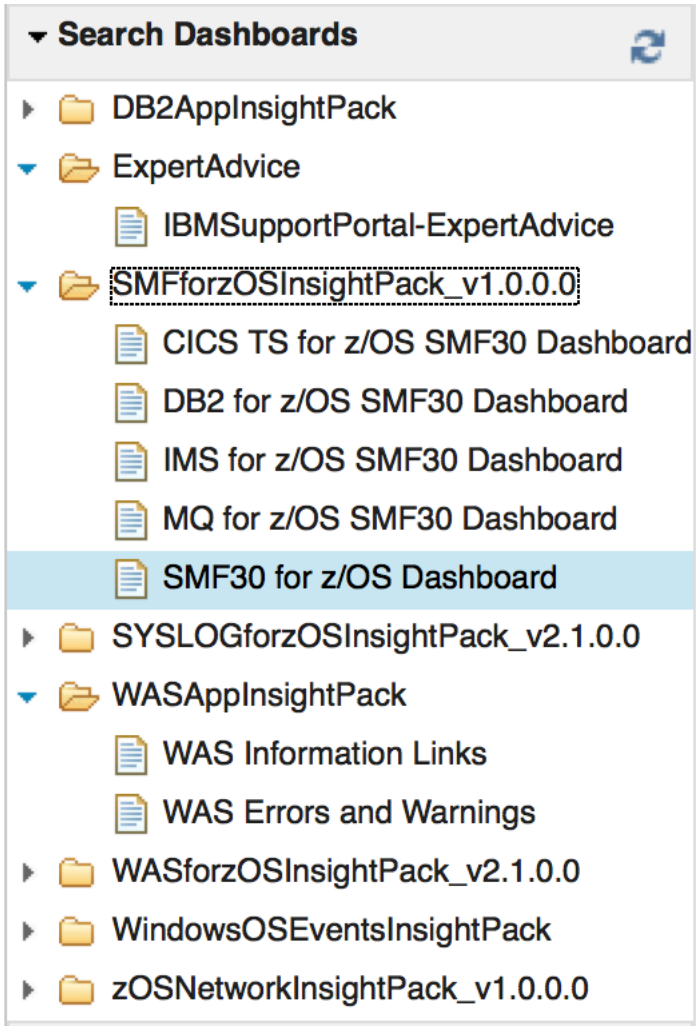
Easy to use – Quick Search

'Quick Searches' available out-of-the-box or create and save your own



- **Provided with every z/OS Insight Pack**
- Provided by **subject matter experts, support teams and customers**
- **Immediate value** out of the box
- Easy to modify or create and **save your own**

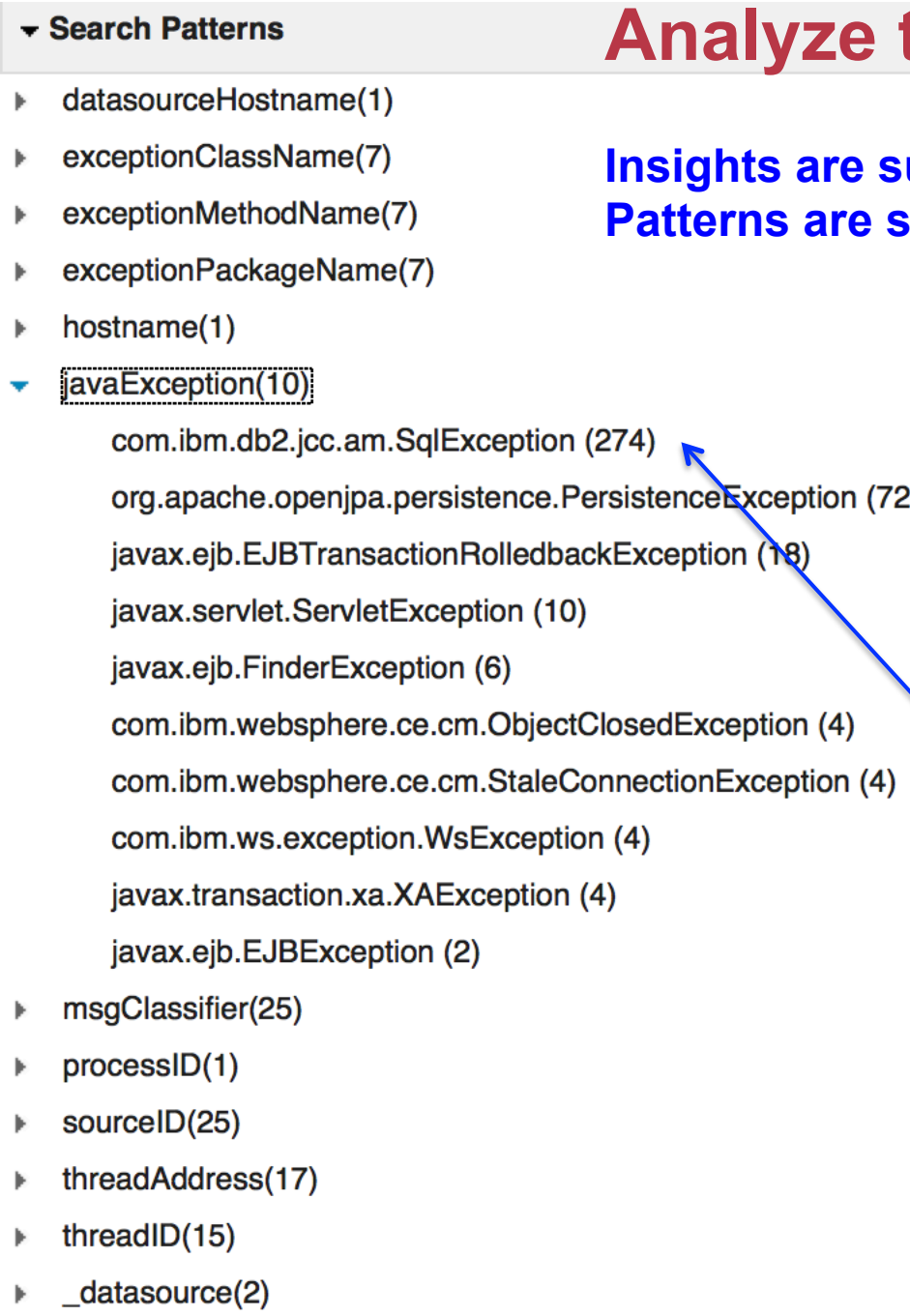
Dashboards, Information Links and Expert Advice



All available out-of-the-box

- **Provided with every Insight Pack**
- **Expert Advice**
- **Dashboard views** created by subject matter experts, support teams and customers
- Immediate value out of the box
- Easy to modify or create and save your own

Analyze the log as you Search



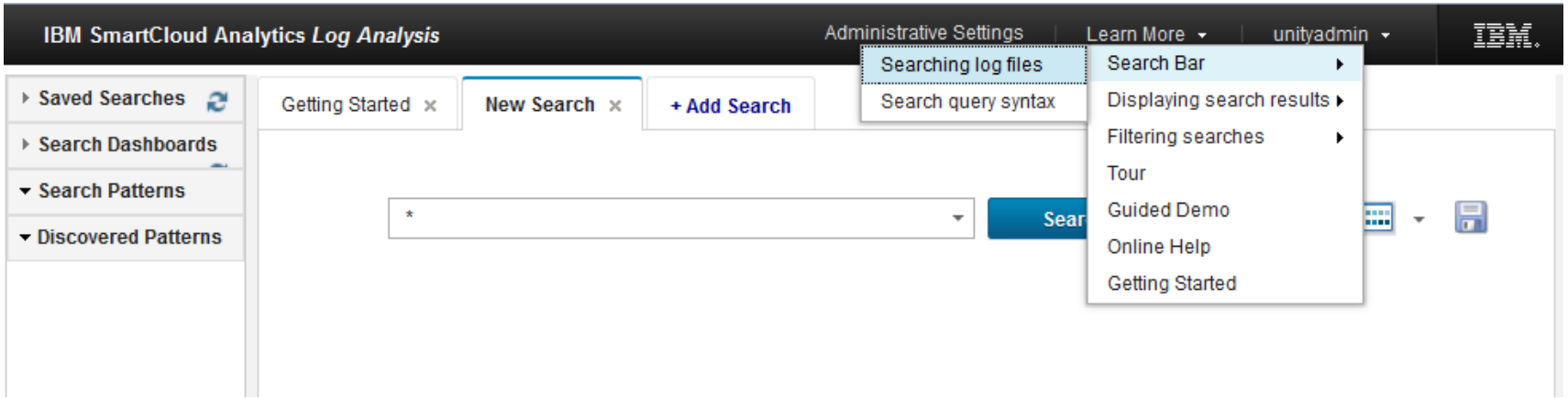
Insights are surfaced automatically as you search.
Patterns are surfaced based on the log type.

- **Provided with every Insight Pack**
- Logs are **analyzed automatically**
- Log data is **categorized** by hostname, datasource, message type, message source, etc
- **Patterns/Insights** are surfaced to help you **focus on the source of the problem.**
  For example, log analysis automatically surfaces java exceptions in application logs.
- Perform searches and analyze **multiple logs, organized per the needs of your enterprise**.

Create your own – Queries, Dashboards, Feeds

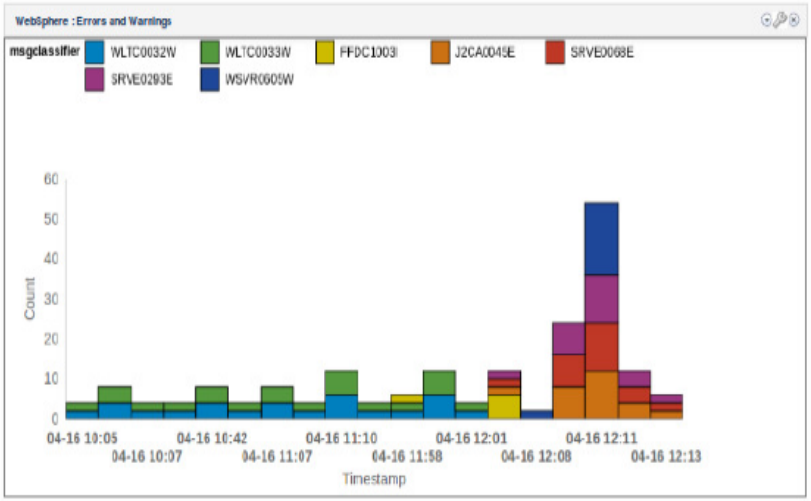
The Out-of-the-Box capabilities provide immediate value.
Additionally, IOA can easily be tailored to your specific needs.

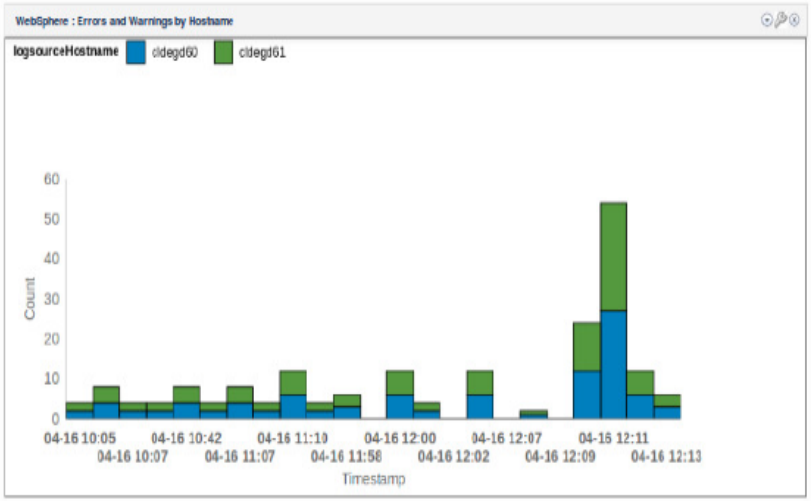
- Perform simple free-form searches using the standard set of search keywords and operators
- Build complex queries with range searches and *DateMath* functions
- To learn more, consult Online Help available from the **Learn More → Search Bar → Search query syntax** menu:

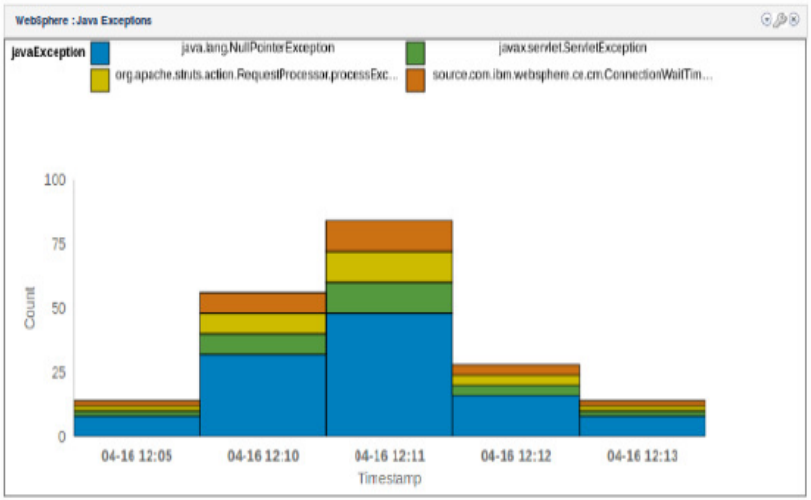


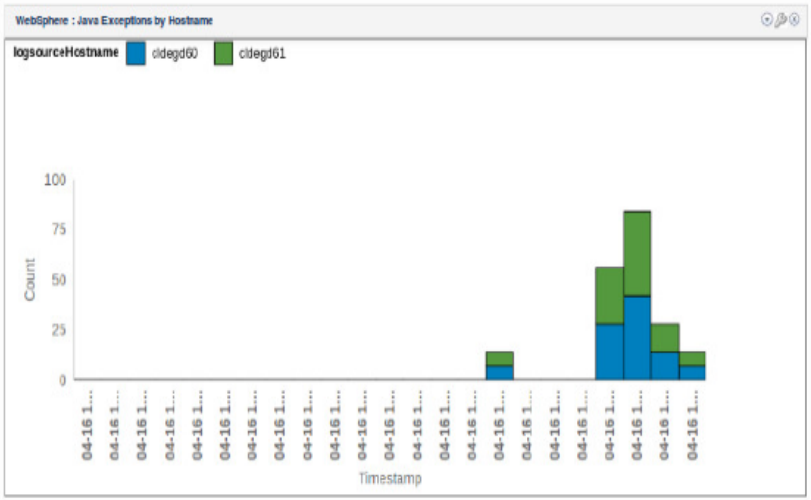
- BYOD – Bring your own Data – The z/OS Log Forwarder can be configured to forward your text logs to enable the Search capability.
- BYOIP – Build your own Insight Pack
- BYOV – Build your own Views

Multiple charting options – WebSphere Example









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

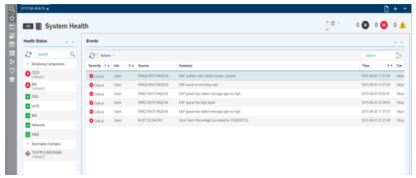
Integration with Event Management

Network Operations Insight + IOA – Search and Analyze Events

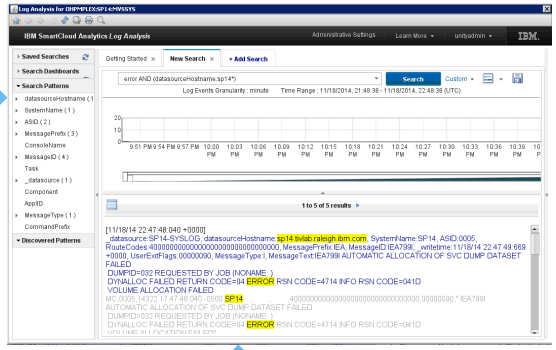
Event Analytics – for Seasonal Event Identification

- 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



Service Management Unite



Event Management OMNIbus/Netcool Operations Insight

Problem Determination NetView CANZLOG

Performance Monitoring ITM/OMEGAMON

Search and analyze logs, metrics and events

Surface anomalies

IBM zAware

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

Summary

IBM Hardware. IBM Software. IBM Middleware. IBM Insights

Quicker Problem Diagnosis	• **Rapid index search to enable quick search of large volumes of data across the Enterprise** • **Real-time insights to identify pertinent messages and filter out noise** • Real time anomaly detection for proactive analysis

Time to Value	• Easy install and quick configuration gets customers up and running in a few hours.
	• Out-of-the-box capabilities provide immediate return on investment
	  • Reports, Optimized searches
	  • Application views and dashboards
	  • All built on expert knowledge from industry experts (customers, SMEs and support)

Extensibility	• Can be customized to meet your needs:
	  • Perform simple or complex searches in seconds
	  • Build application views to meet your needs (for example ‘before’ and ‘after’ views)
	  • Save and share your searches
	  • Define additional data sources (Logs, Events, Trouble Tickets, Documentation, etc)

Integration	• Re-use your existing data • Tightly integrated with existing Service Management Solutions (Event Management, APM, Availability and Performance Monitoring, Automation, Trouble Ticketing, etc) • IT Analytics is about much more than just logs. IBM’s Log Analysis tools also include analysis of metrics, files, events, and much more, The tooling is designed for IT Analytics .. Not just Log Analysis.
On Platform	• Keep data on the mainframe by running the Analytics engine on zLinux
Expert Advice	• Connect directly to IBM Support Portal to leverage knowledge of applications and infrastructure • Connect to your company Knowledge Base or Runbooks

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


धन्यवाद
Hindi
多謝
Traditional Chinese
ขอบคุณ
Thai
Спасибо
Russian
Gracias
Spanish
Thank You
English
شكراً
Arabic
Obrigado
Brazilian Portuguese
多谢
Simplified Chinese
Danke
German
Bedankt
Dutch
Grazie
Italian
Merci
French
நன்றி
Tamil
ありがとうございました
Japanese
감사합니다
Korean