



Controlling the chaos in your Enterprise: Using log analytics and OMEGAMON

*Sarah Knowles
Strategy and Portfolio Manager for zAnalytics*

*Paul Smith (Smitty)
IBM z Systems Service Management / zAnalytics Architect*



SHARE is an independent volunteer-run information technology association that provides **education, professional networking and industry influence.**

Copyright (c) 2014 by SHARE Inc. Except where otherwise noted, this work is licensed under <http://creativecommons.org/licenses/by-nc-sa/3.0/>





Agenda

- Why IT Analytics
- Predict, Search, Optimize
- zAware
 - Capabilities
 - Interface
 - Integration with OMEGAMON
- SmartCloud Analytics – Log Analysis
 - Capabilities
 - Interface
 - Integration with OMEGAMON
- Reference Materials

Rapid growth of data from next generation technologies can be supported seamlessly on z Systems



System z scaling model and security to manage and optimize both



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

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



New Technologies like cloud and big data already challenging current Enterprise tools



- **Too long to isolate, diagnose problems in applications and infrastructure.**
 - Complex application workloads span multiple platforms
 - Increasing amounts of IT data:
 - Performance metrics, events, infrastructure logs, application logs, configuration files, traces
- **Existing IT tools inappropriate for management of Systems of Engagement**
 - 100x to 1000x explosion in data flooding existing tools.
 - New runtimes, programming languages needing complex instrumentation.
- **Reactive analytics misses critical information leading to outages**
 - Analyzing all information better for predicting problems.



Is managing IT today like sipping from a fire hose?



Analysis – The Problem

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



Where do I start??

Logs, Traces,..

```
[10/9/12 5:51:38:295
GMT+ 05:30] 0000006a
servlet E
com.ibm.ws.webcontainer.ser
vlet.ServletWrapper service
SRVE0068E:
```

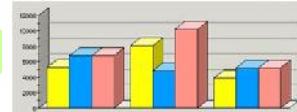
Core files

```
010001100011100001110
011000111110000110001
111111000110011100011
```

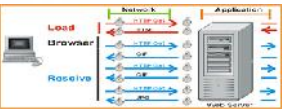
Events

Timestamp	Message	Source
10/9/12 5:51:38:295	Servlet E	com.ibm.ws.webcontainer.servlet.ServletWrapper
10/9/12 5:51:38:295	Servlet E	com.ibm.ws.webcontainer.servlet.ServletWrapper
10/9/12 5:51:38:295	Servlet E	com.ibm.ws.webcontainer.servlet.ServletWrapper
10/9/12 5:51:38:295	Servlet E	com.ibm.ws.webcontainer.servlet.ServletWrapper
10/9/12 5:51:38:295	Servlet E	com.ibm.ws.webcontainer.servlet.ServletWrapper

Metrics



Transactions



Config



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

Predict

- OMEGAMON & NetView
w/ IBM zAware

Faster Problem Resolution

Search

- IBM SmartCloud Analytics -
Log Analysis

Optimized Performance

Optimize

- IBM Capacity Management
Analytics (CMA)

Analytics is the next step in IBM value add for zEnterprise 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 system are just as bad as unavailable systems
- Next step – Enable to 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

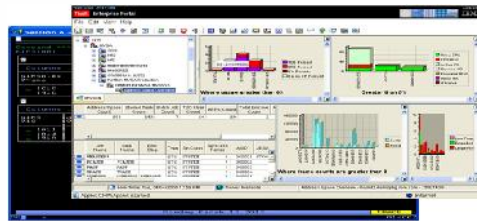
System and sub-system performance monitoring

IT Analytics

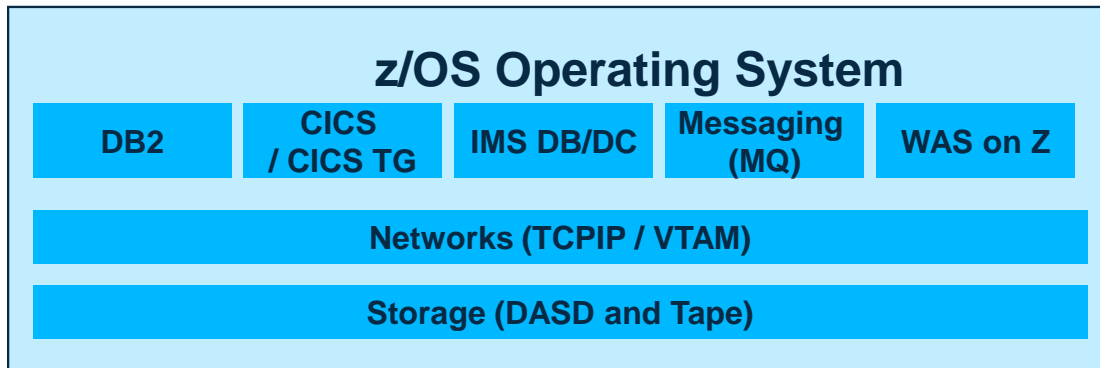
Analyze metric and log data
Predict outages
Forecast capacity, CPU, etc
Surface anomalies
Improve search techniques
Reduce MTTR
Provide expert advice
Plug into existing service management tooling



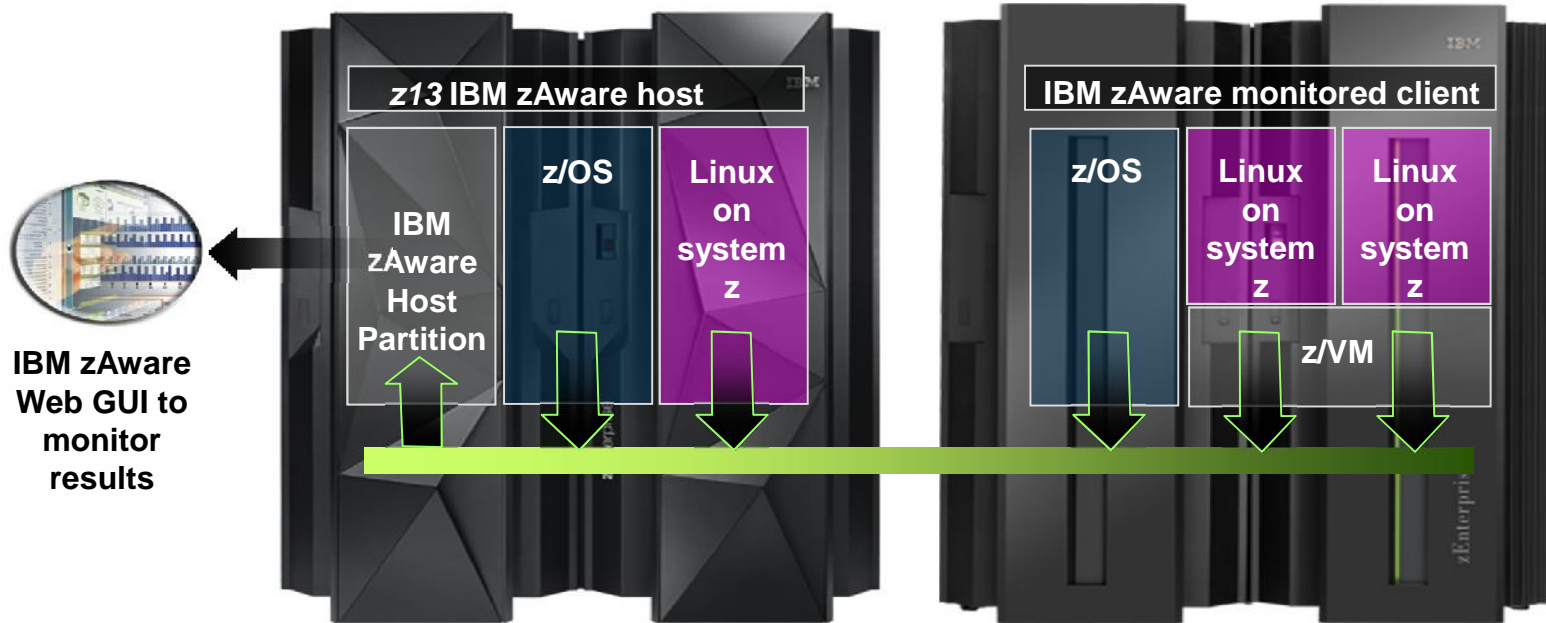
IBM OMEGAMON Performance Management Suite for z/OS



Tivoli OMEGAMON Performance Management Suite for z/OS provides an *integrated solution* with extensive capabilities to manage on-line and middleware sub-systems like CICS, DB2, IMS, WAS on z/OS and the z/OS Operating System, Networks and Storage which supports these capabilities



IBM zAware V2.0 - Analyze z/OS and Linux on z Systems



- Identify unusual system behavior of z/OS and Linux images running on z Systems
- Proactively surface log message anomalies

What can zAware do for you? *Identify unusual behavior quickly*



Which z/OS image is having unusual message patterns?

- High score generated by unusual messages or message patterns
- GUI shows all systems or selected subsets

Which subsystem or component is abnormal?

- Examine high-scoring messages

When did the behavior start?

- Which messages are unusual?
- How often did the message occur?

Were similar messages issued previously

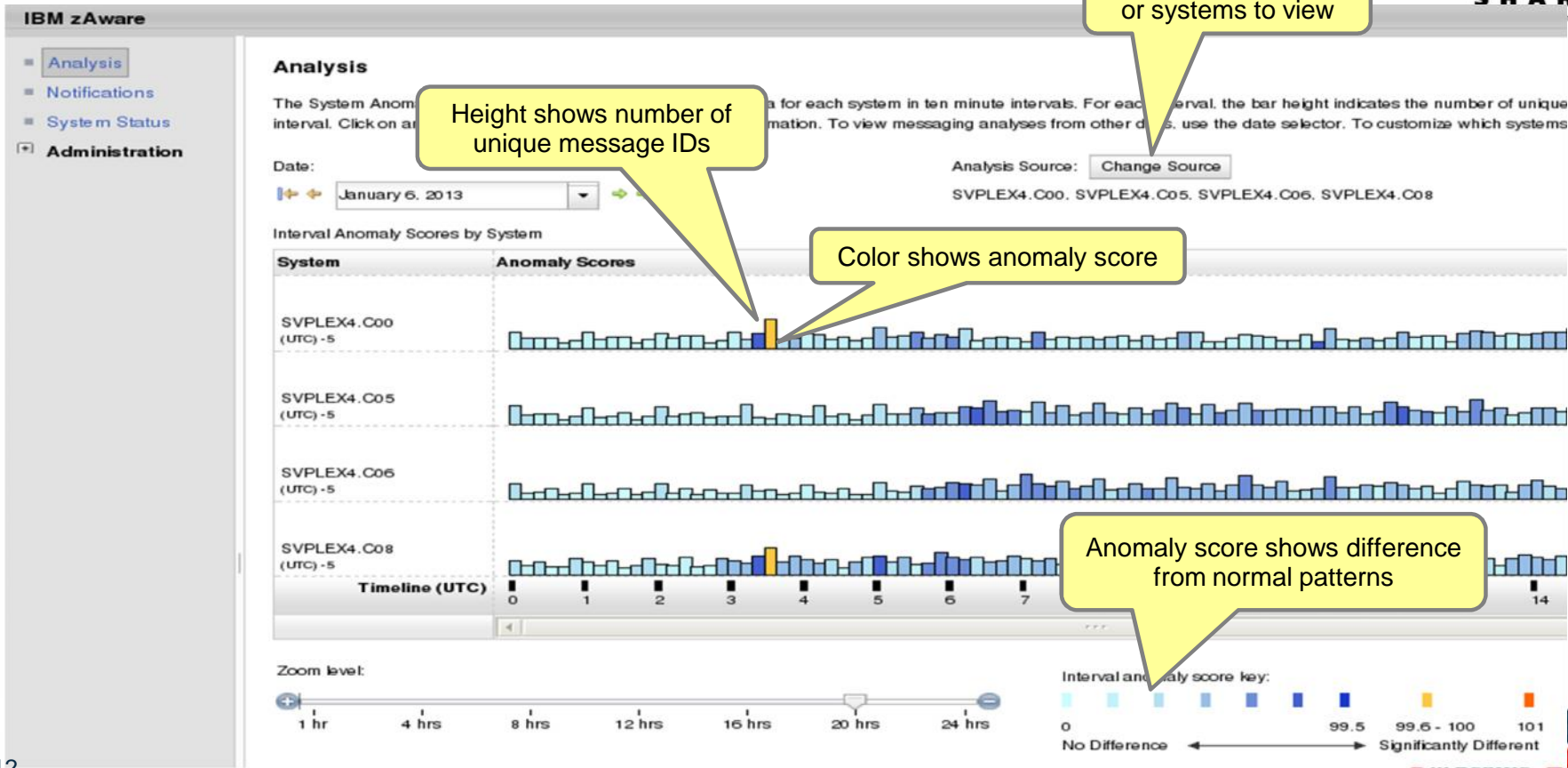
- Easily examine prior intervals or dates

Is the unusual behavior after some maintenance or upgrade?

- Easily pinpoint changes caused by new software levels, configuration settings



Analysis View

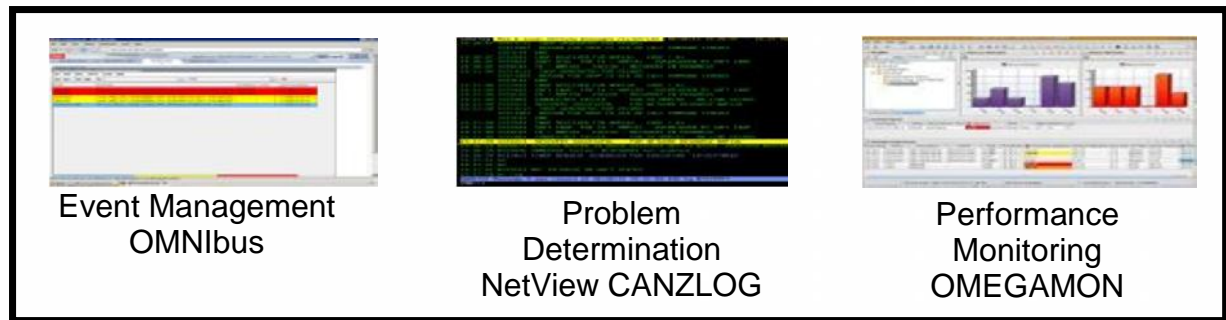


Predictive Analysis integrating IBM zAware's Anomaly Detection and Performance Monitoring



- Save money ensuring z/OS availability. Highlight potential system health problems which will improve service and reduce business risk.
- Transition to a Problem Management platform with integration to NetView and/or OMEGAMON

Predict



Surface Anomalies

“What’s different today?”



Search for and rapidly analyze unstructured data to assist in and accelerate problem identification, isolation and repair



SmartCloud Analytics – Log Analysis



Differentiating Capabilities

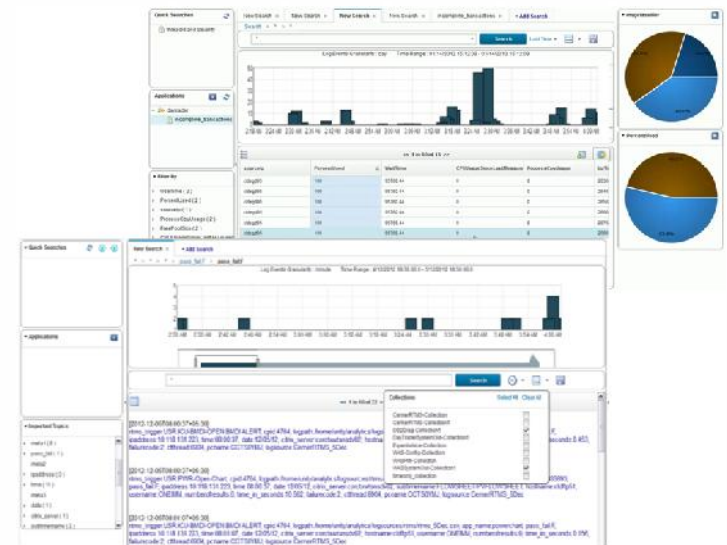
Locate **component error messages** from system, configuration, software and event logs **via rapid indexed search**

- 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**.

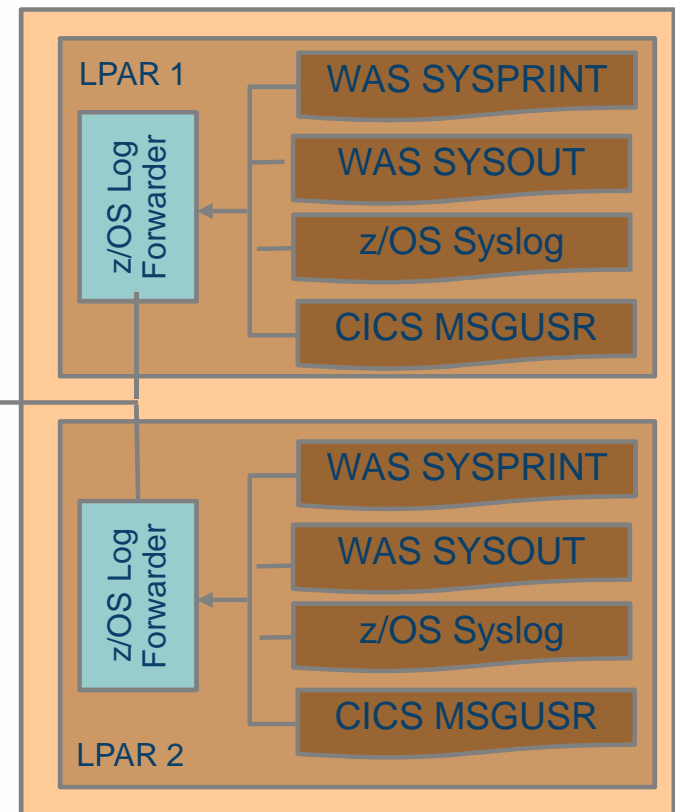
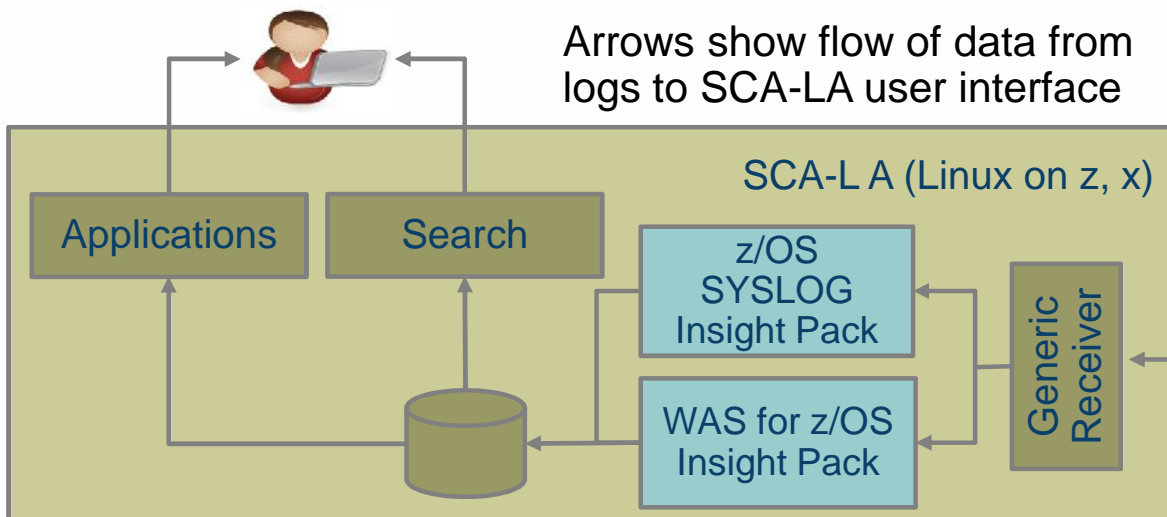
Numerous Customers

- 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

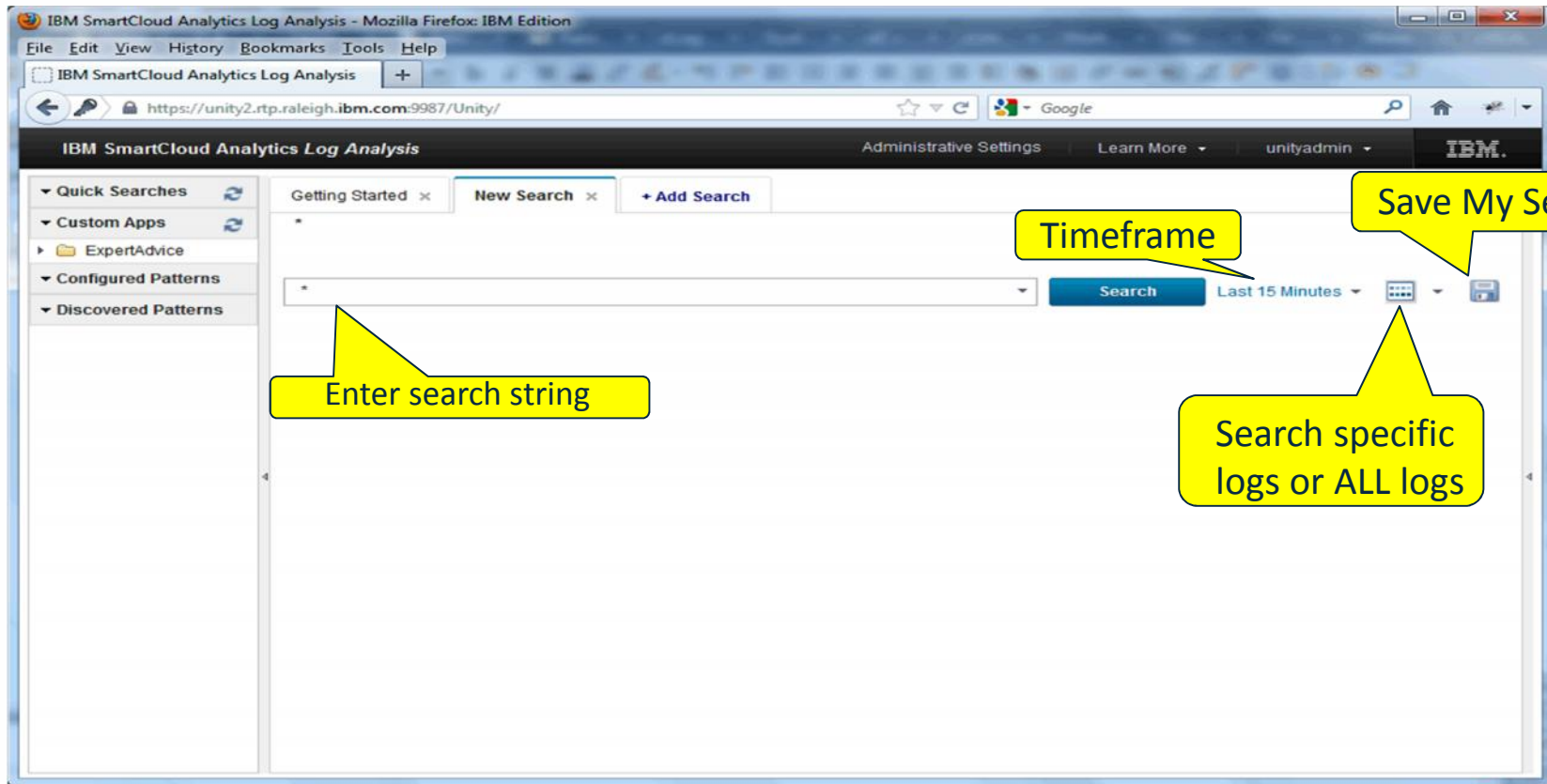


z/OS Systems



- 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

Simple Search Interface – Easy to Customize



WebSphere Application Server Search – java Exception pattern

Example of search capabilities plus insights



The screenshot shows the IBM SmartCloud Analytics Log Analysis interface. On the left, a sidebar lists 'Configured Patterns' with 'org.apache.openjpa.persistence.PersistenceException (71)' selected. The main area shows a search query: 'javaException:=="org.apache.openjpa.persistence.PersistenceException"'. A bar chart above the results table shows a spike in log events at 3:26 AM. A table below displays search results with columns: exceptionPackageName, msgClassifier, _datasource, and threadID.

exceptionPackageName	msgClassifier	_datasource	threadID
	BB000222I	TVT7008_SYSOUT	0X00000023
	BB000222I	TVT7008_SYSVRT	
org.apache.openjpa.kernel	BB000220E	TVT7008_SYSOUT	0X00000030
	BB000222I	TVT7008_SYSVRT	
	FFDC1003I	TVT7008_SYSOUT	0X00000015
	BBOJ0011I	TVT7008_SYSVRT	
org.apache.openjpa.kernel	BB000220E	TVT7008_SYSOUT	0X00000030
	BB000222I	TVT7008_SYSVRT	
	BB000222I	TVT7008_SYSOUT	
org.apache.openjpa.kernel	BB000220E	TVT7008_SYSOUT	0X00000030
	BBOJ0051I	TVT7008_SYSVRT	
org.apache.openjpa.kernel	BB000220E	TVT7008_SYSOUT	0X00000030
	BBOJ0077I	TVT7008_SYSVRT	
org.apache.openjpa.kernel	BB000220E	TVT7008_SYSOUT	0X00000030
	BBOJ0077I	TVT7008_SYSVRT	

Search WAS log

Timeframe of problem

Log analysis displays number of exceptions during this timeframe

Search results



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



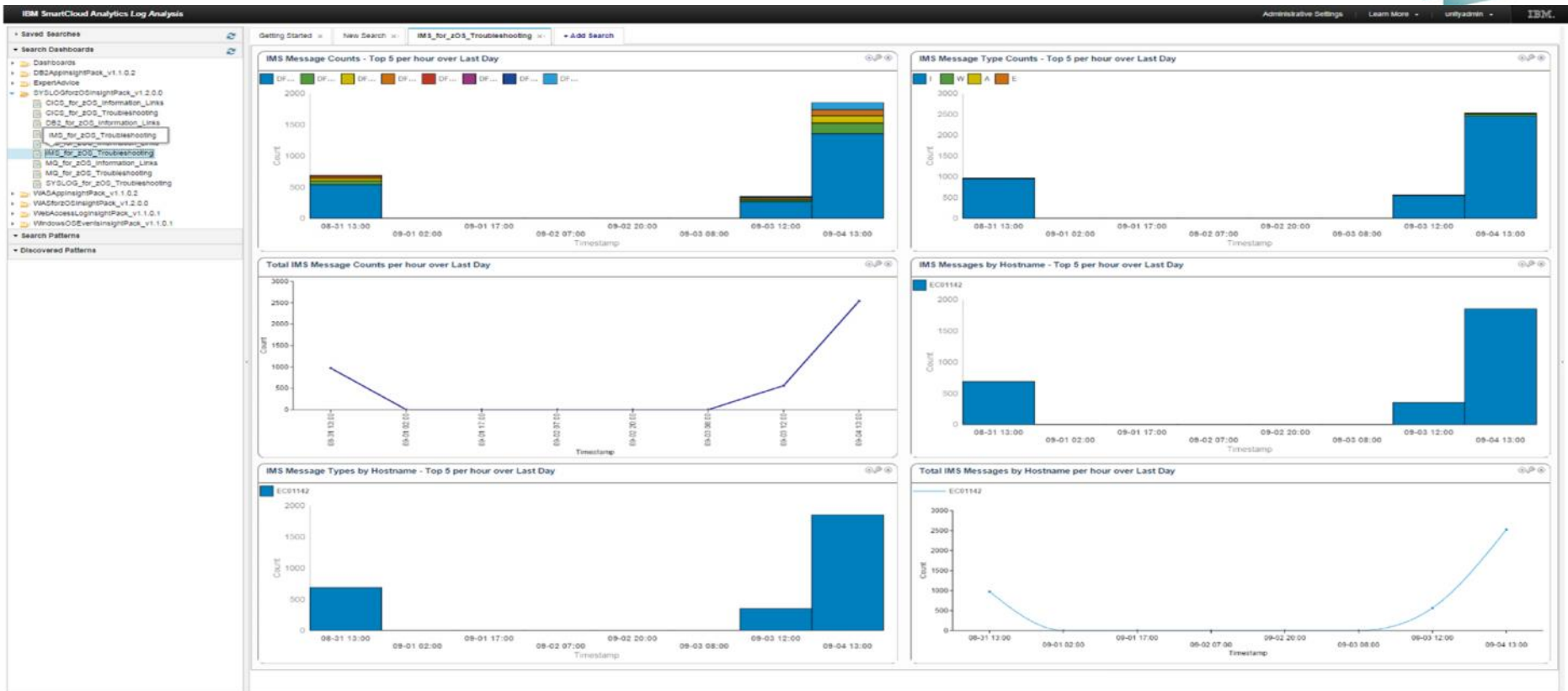
Search for expert advice with the click of a button

All IBM support site documents that reference messages from search results

The screenshot shows the IBM Support Portal interface. On the left, there is a navigation pane with sections like 'Quick Searches', 'Custom Apps', 'ExpertAdvice', 'Configured Patterns', and 'Discovered Patterns'. The main content area displays search results for 'WebSphere Application Server V8: Administration and Configuration Guide'. A specific result is highlighted with a yellow callout box: 'I205682: ADMIN TASK RECONFIGURE TAM PORT CONFLICT'. Below this, there are several other search results, including one for 'CWPKI0041W warnings in WebSphere Application Server V7.0 log files'. A red arrow points from this result to a detailed article page. The article page is titled 'WSKeyStore CWPKI0041W warning message is found in the SystemOut.log file' and includes sections for 'Technote (troubleshooting)', 'Problem(Abstract)', 'Cause', 'Resolving the problem', and 'Using the administrative console'. A yellow callout box with the text 'Launch to Technote' points to the article title. The article page also features a 'Rate this page' section, 'Add comments', and 'Document information'.



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



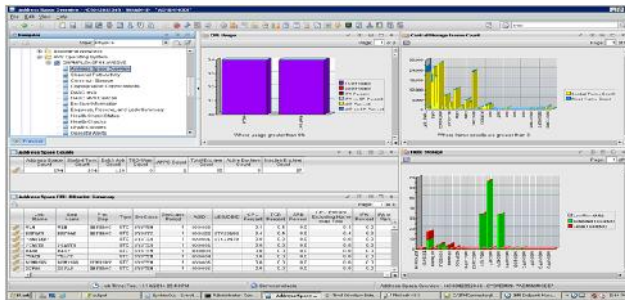
Integration with Performance Monitoring



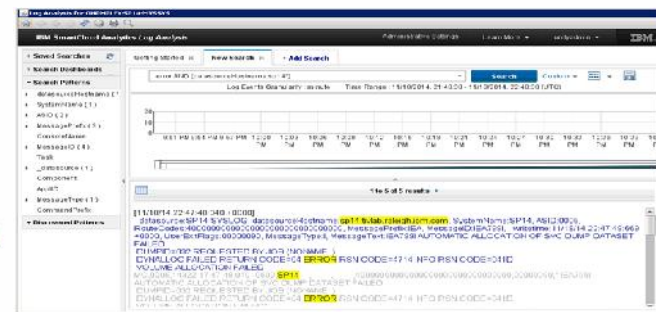
OMEGAMON + SCA-LA – Launch in Context from TEP

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

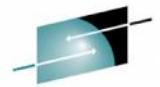


Launch SCA-LA from OMEGAMON performance monitoring workspaces to search logs in context



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

Search will be done in context of LPAR

Specify search time frame

Specify search string

The screenshot displays the OMEGAMON Address Space Overview interface. At the top, a search bar contains the text 'error'. The interface is divided into several sections:

- Navigator:** A tree view on the left showing the system hierarchy, with 'Address Space Overview' selected.
- Address Space Counts:** A table showing counts for various metrics.

Address Space Count	Started Task Count	Batch Job Count	TSO User Count	APPC Count	Total Enclave Count	Active Enclave Count	Inactive Enclave Count
274	154	118	0	2	30	3	27
- Address Space CPU Utilization Summary:** A table listing jobs and their CPU utilization.

Job Name	Step Name	Proc Step	Type	SvcClass	SvcClass Period	ASID	JESJOBID	CPU Percent	TCB Percent	SRB Percent	CPU Percent Excluding Home SRB Time	IFA Percent	IFA or Perc
WLM	WLM	IEFFPROC	STC	SYSTEM	1	0x000B		0.4	0.4	0.0	0.4	0.0	
RMFGAT	RMFGAT	IEFFPROC	STC	SYSSTC	1	0x02EE	STC20186	0.4	0.4	0.0	0.4	0.0	
MASTER			STC	SYSTEM	1	0x0001	STC19479	0.0	0.0	0.0	0.0	0.0	
PCAUTH	PCAUTH		STC	SYSTEM	1	0x0002		0.0	0.0	0.0	0.0	0.0	
RASP	RASP		STC	SYSTEM	1	0x0003		0.0	0.0	0.0	0.0	0.0	
TRACE	TRACE		STC	SYSTEM	1	0x0004		0.0	0.0	0.0	0.0	0.0	
DUMPSRV	DUMPSRV	DUMPSRV	STC	SYSTEM	1	0x0005		0.0	0.0	0.0	0.0	0.0	
XCFAS	XCFAS	IEFFPROC	STC	SYSTEM	1	0x0006		0.0	0.0	0.0	0.0	0.0	
- Central Storage Frame Count:** A bar chart showing frame counts for various storage devices. The legend includes Central Frame Count (yellow) and Fixed Frame Count (blue).
- Fixed Storage:** A bar chart showing storage usage in MB. The legend includes Low Fixed (Mb) (purple), Extended Fixed (Mb) (green), and Large Fixed (Mb) (red).

Launch SCA-LA (in context of LPAR) from OMEGAMON Workspace

Search results displayed in SCA-LA



The screenshot shows the IBM SmartCloud Analytics Log Analysis application. The search query is "error AND (datasourceHostname:sp14*)". The results show a single log event with the message: "DYNALLOC FAILED RETURN CODE=04 ERROR RSN CODE=4714 INFO RSN CODE=041D". The interface includes a search bar, a search button, and a list of search results.

Notice there is only 1 SystemName (LPAR)

Search string provided from OMEGAMON workspace

Insights surfaced during search

Search results with search strings highlighted



Additional Reference Material



- Analytics Overview Video
 - <https://www.youtube.com/watch?v=OQJapWiQECs>
- SCA-LA z/OS Insight Packs videos:
 - 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
 - SYSLOG: <http://www.ibm.com/support/knowledgecenter/SS9M7K>
 - IBM WAS: <http://www.ibm.com/support/knowledgecenter/SS9MBD>
- SCA-LA Product Documentation
 - Service Management Connect
 - <http://www.ibm.com/developerworks/servicemanagement/ioa/log/index.html>
 - Knowledge Center
 - <http://www.ibm.com/support/knowledgecenter/SSPFMY>



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/>



zSCA-LA v.Next Early Access and Beta Program



The **IBM SmartCloud Analytics - Log Analysis for z/OS V.next Early Access and Beta Program** was announced on January 29, 2015.

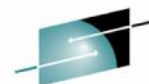
In 2015, we will build on the strong foundation established over the past months by providing insights into additional domains, as well as by enhancing existing insights through integration of performance metrics.

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>





SHARE
Educate • Network • Influence

Thank
You