SHARE in Orlando 2015

SHARE
Educate · Network · Influence

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

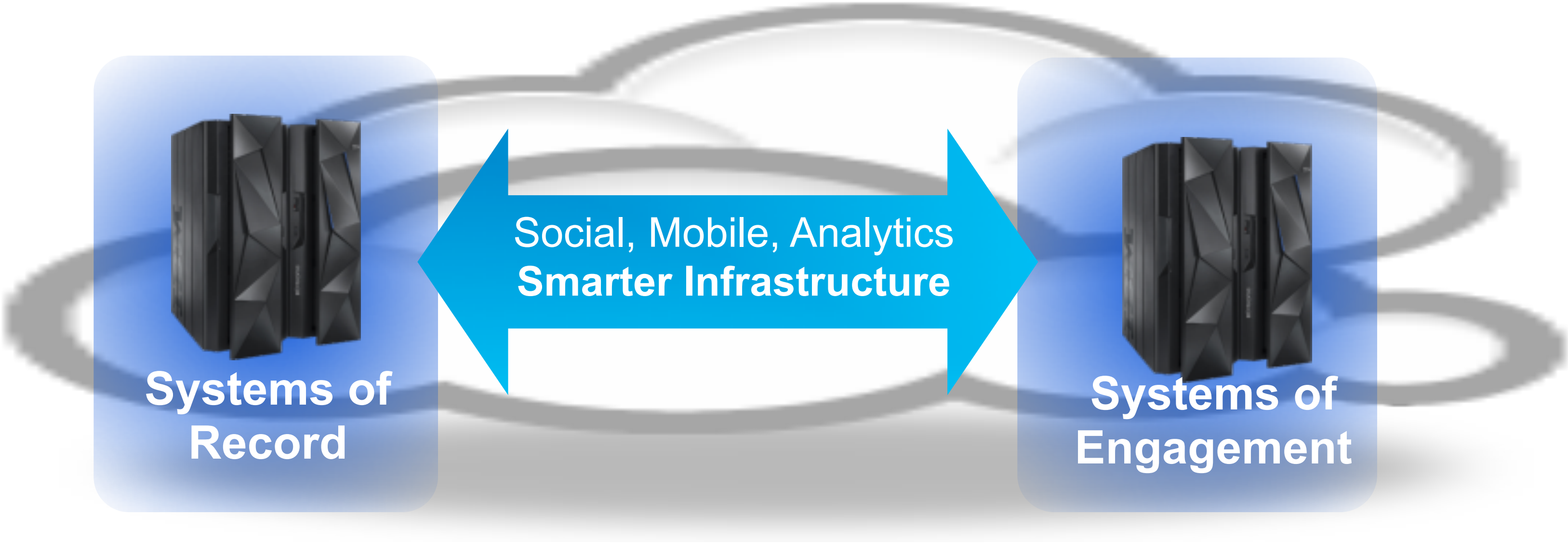
Anuja Deedwaniya (anujad@us.ibm.com)
IBM z Systems Enterprise Architect

#SHAREorg

CELEBRATING 60 ★YEARS★ OF SHARE
Influencing IT Since 1955

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

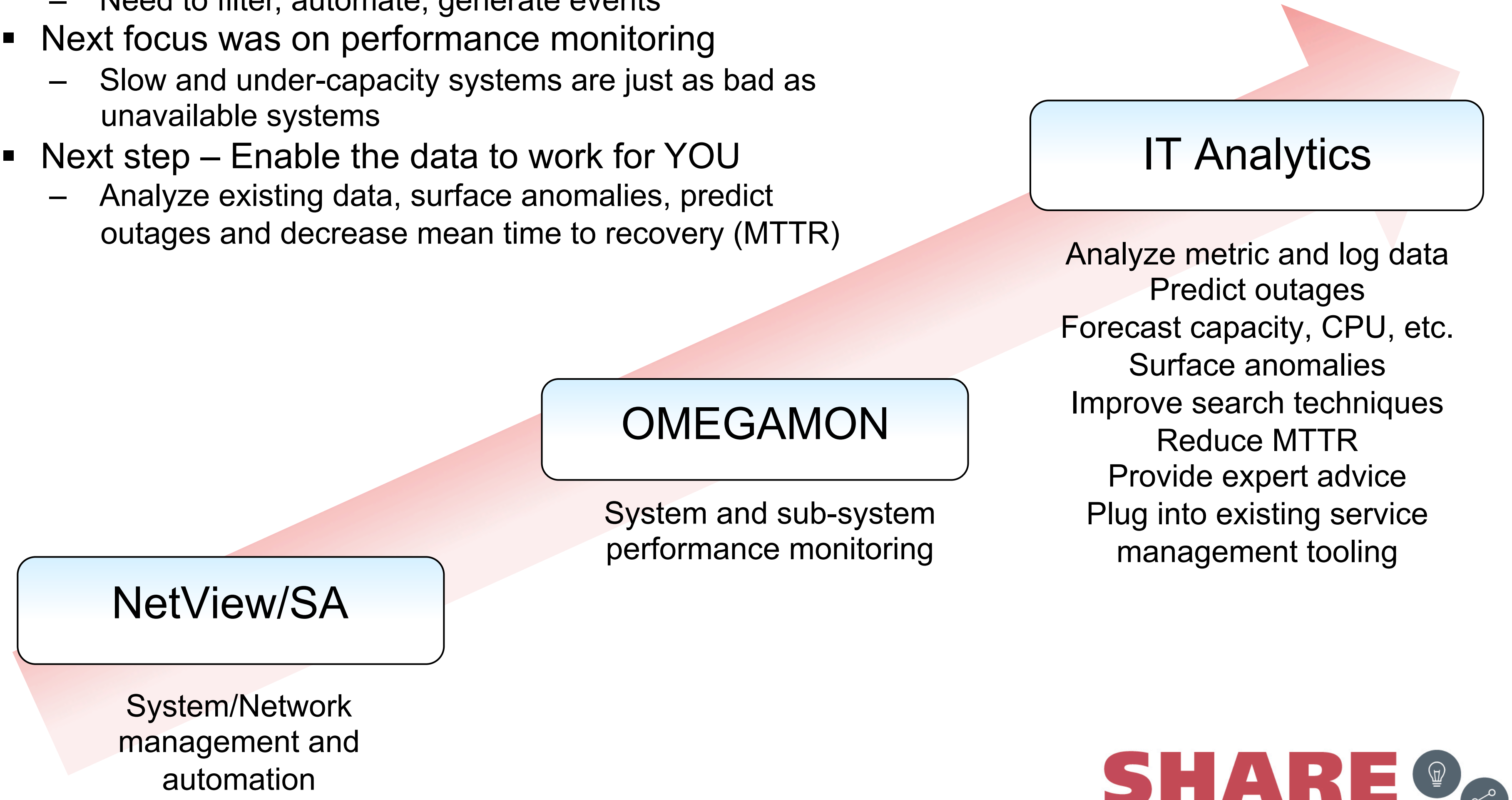
- Mobile and Social
- Dynamic
- Interactions and Collaboration
- Insight, trends, analytics

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

IBM is focused on managing end-to-end analytics for improved performance and workload management

Predict:

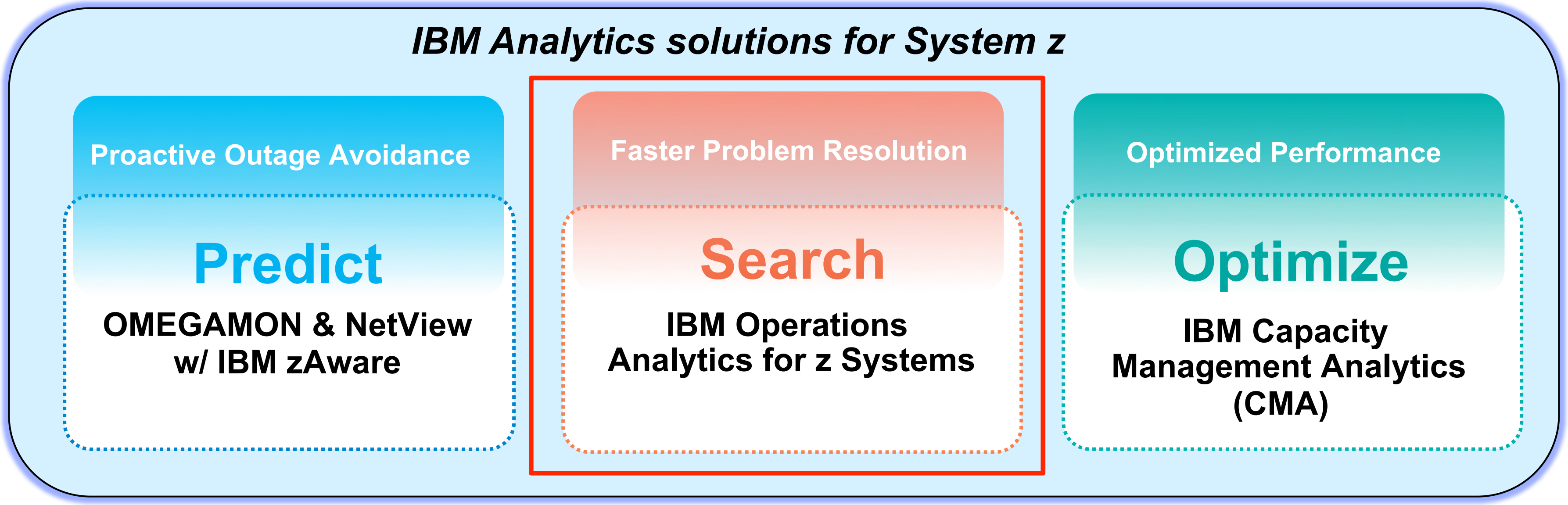
- Pro-Active Outage Avoidance
- Predict problems before they occur

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

Proactive Outage Avoidance

Predict

OMEGAMON & NetView w/ IBM zAware

Faster Problem Resolution

Search

IBM Operations Analytics for z Systems

Optimized Performance

Optimize

IBM Capacity Management Analytics (CMA)

Solution Branding – Name Change

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

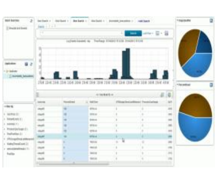
Note that the distributed product is now named

IBM Operations Analytics – Log Analysis

IBM Operations Analytics for z Systems

Accelerate problem isolation and identification
Reduce mean time to repair

- **Analyse** 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



SEARCH

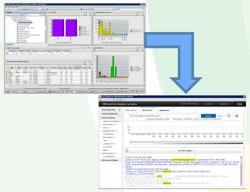
ANALYZE

CPU Utilization by Task over Last Day

WSKeyStore CWPKI0041W warning message is found in the SystemOut.log file

RESOLVE

INTEGRATE

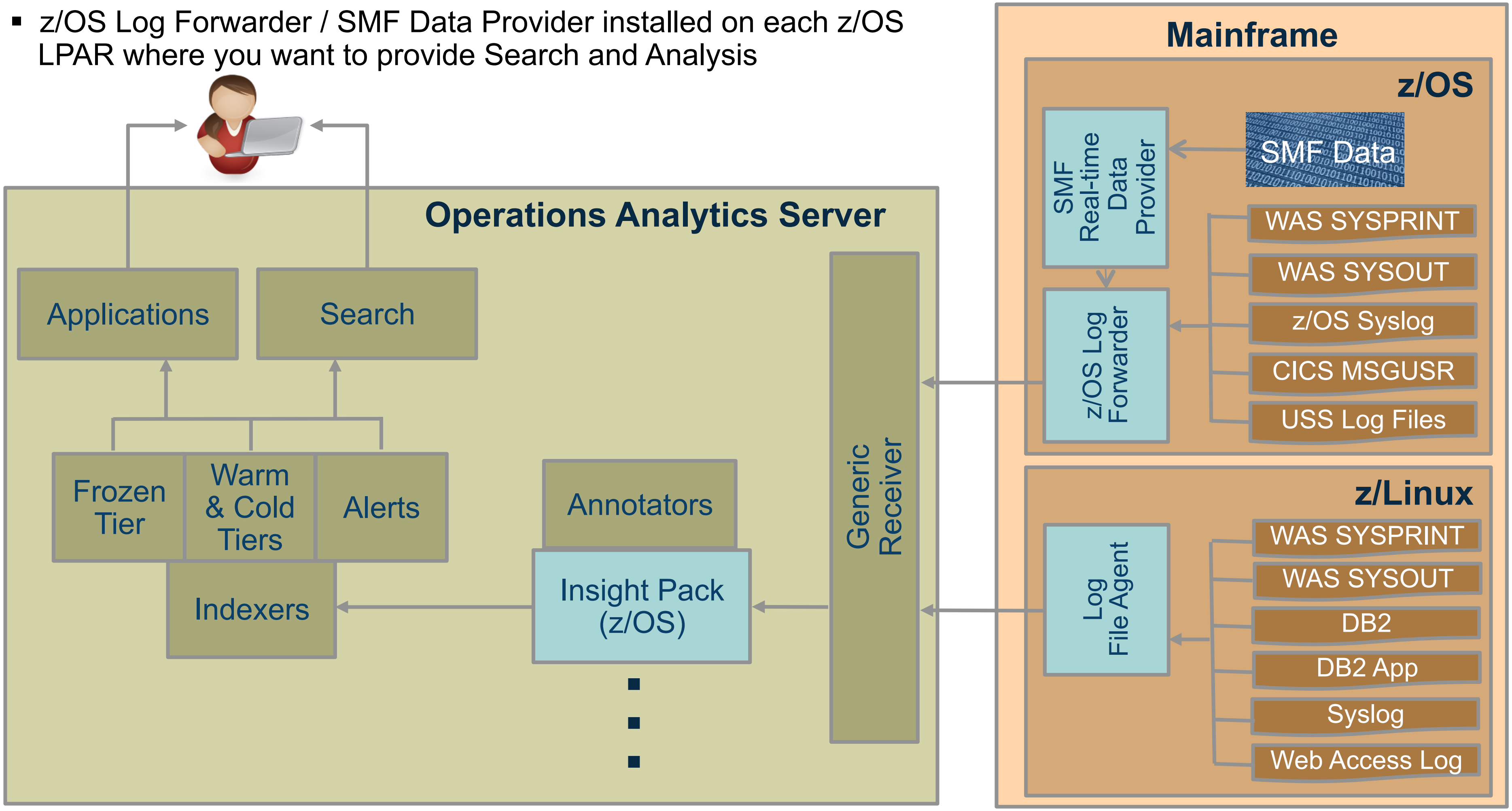


in 2015

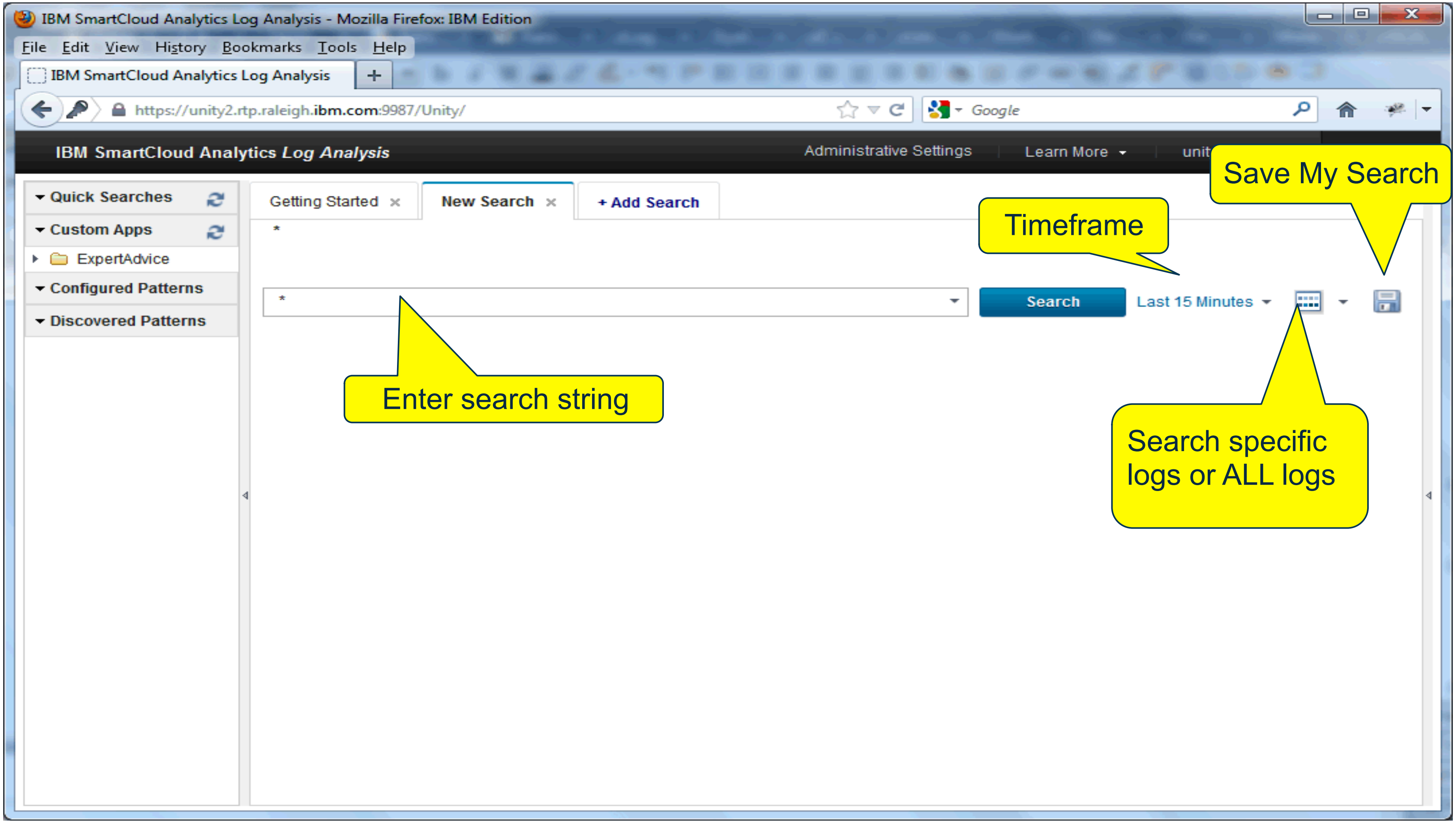
- Network Insights
- Event notification
- Hadoop Support
- Analysis of Performance Metrics (new SMF real time Data Provider)
- Integration with ITM/OMEGAMON and Netcool Operations Insight, Service Management Unite, Trouble Ticketing

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



Simple Search Interface – Easy to Customize

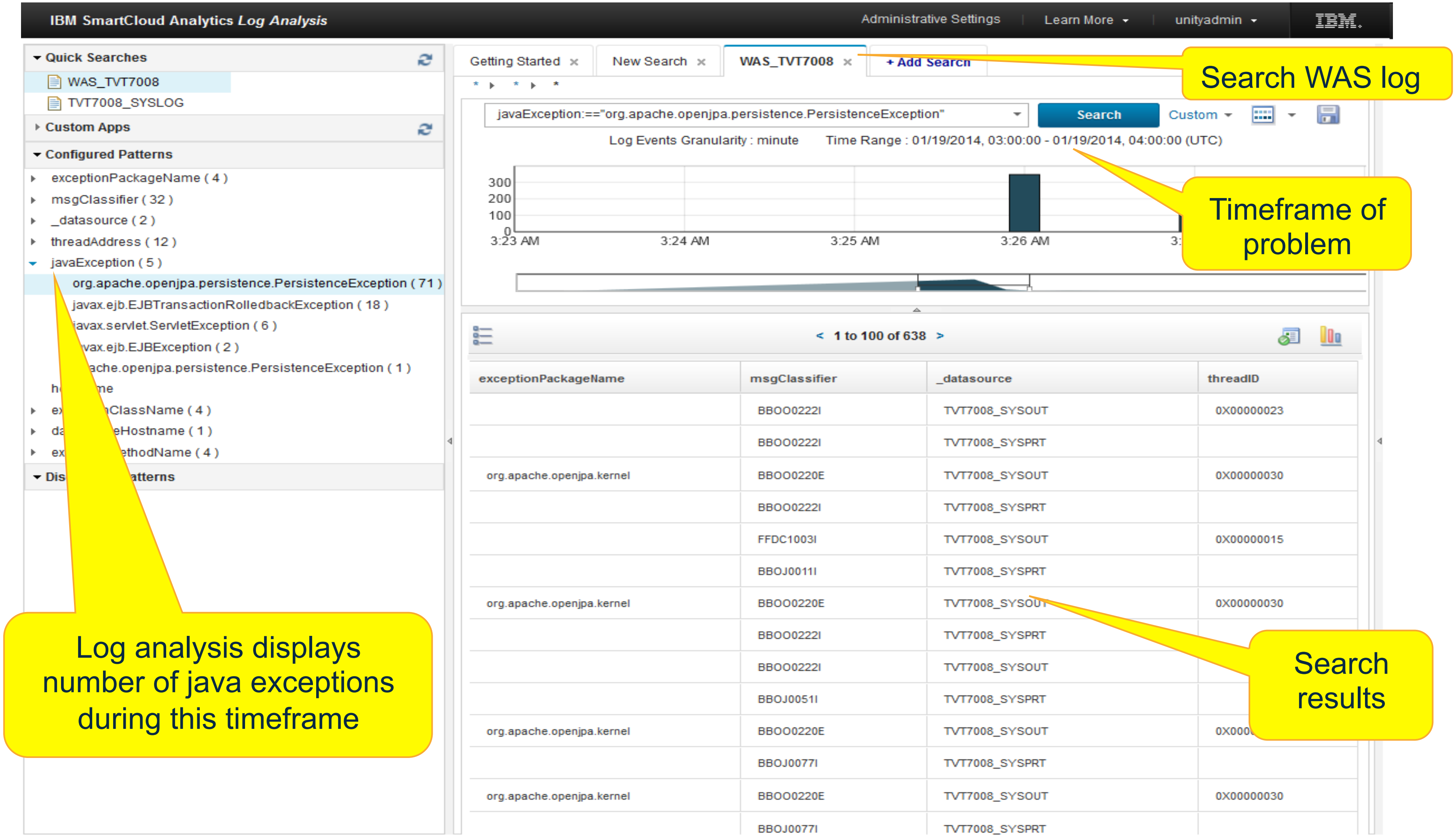


IBM SmartCloud Analytics Log Analysis - Mozilla Firefox: IBM Edition
File Edit View History Bookmarks Tools Help
IBM SmartCloud Analytics Log Analysis
https://unity2.rtp.raleigh.ibm.com:9987/Unity/
Google
IBM SmartCloud Analytics Log Analysis
Administrative Settings
Learn More
unit
Quick Searches
Custom Apps
ExpertAdvice
Configured Patterns
Discovered Patterns
Getting Started
New Search
+ Add Search
*
*
Search
Last 15 Minutes
Save My Search
Timeframe
Enter search string
Search specific logs or ALL logs

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



- Quick Searches
  - WAS_TVT7008
  - TVT7008_SYSLOG
- Custom Apps
- Configured Patterns
  - exceptionPackageName (4)
  - msgClassifier (32)
  - _datasource (2)
  - threadAddress (12)
  - javaException (5)
    - org.apache.openjpa.persistence.PersistenceException (71)
    - javax.ejb.EJBTransactionRolledbackException (18)
    - javax.servlet.ServletException (6)
    - vax.ejb.EJBException (2)
    - ache.openjpa.persistence.PersistenceException (1)
  - h me
  - ex nClassName (4)
  - da eHostname (1)
  - ex ethodName (4)
- Dis atterns

javaException:=="org.apache.openjpa.persistence.PersistenceException"

Log Events Granularity : minute   Time Range : 01/19/2014, 03:00:00 - 01/19/2014, 04:00:00 (UTC)

< 1 to 100 of 638 >

exceptionPackageName	msgClassifier	_datasource	threadID
	BBOO0222I	TVT7008_SYSOUT	0X00000023
	BBOO0222I	TVT7008_SYSPRT	
org.apache.openjpa.kernel	BBOO0220E	TVT7008_SYSOUT	0X00000030
	BBOO0222I	TVT7008_SYSPRT	
	FFDC1003I	TVT7008_SYSOUT	0X00000015
	BBOJ0011I	TVT7008_SYSPRT	
org.apache.openjpa.kernel	BBOO0220E	TVT7008_SYSOUT	0X00000030
	BBOO0222I	TVT7008_SYSPRT	
	BBOO0222I	TVT7008_SYSOUT	
	BBOJ0051I	TVT7008_SYSPRT	
org.apache.openjpa.kernel	BBOO0220E	TVT7008_SYSOUT	0X000
	BBOJ0077I	TVT7008_SYSPRT	
org.apache.openjpa.kernel	BBOO0220E	TVT7008_SYSOUT	0X00000030
	BBOJ0077I	TVT7008_SYSPRT	

Search WAS log

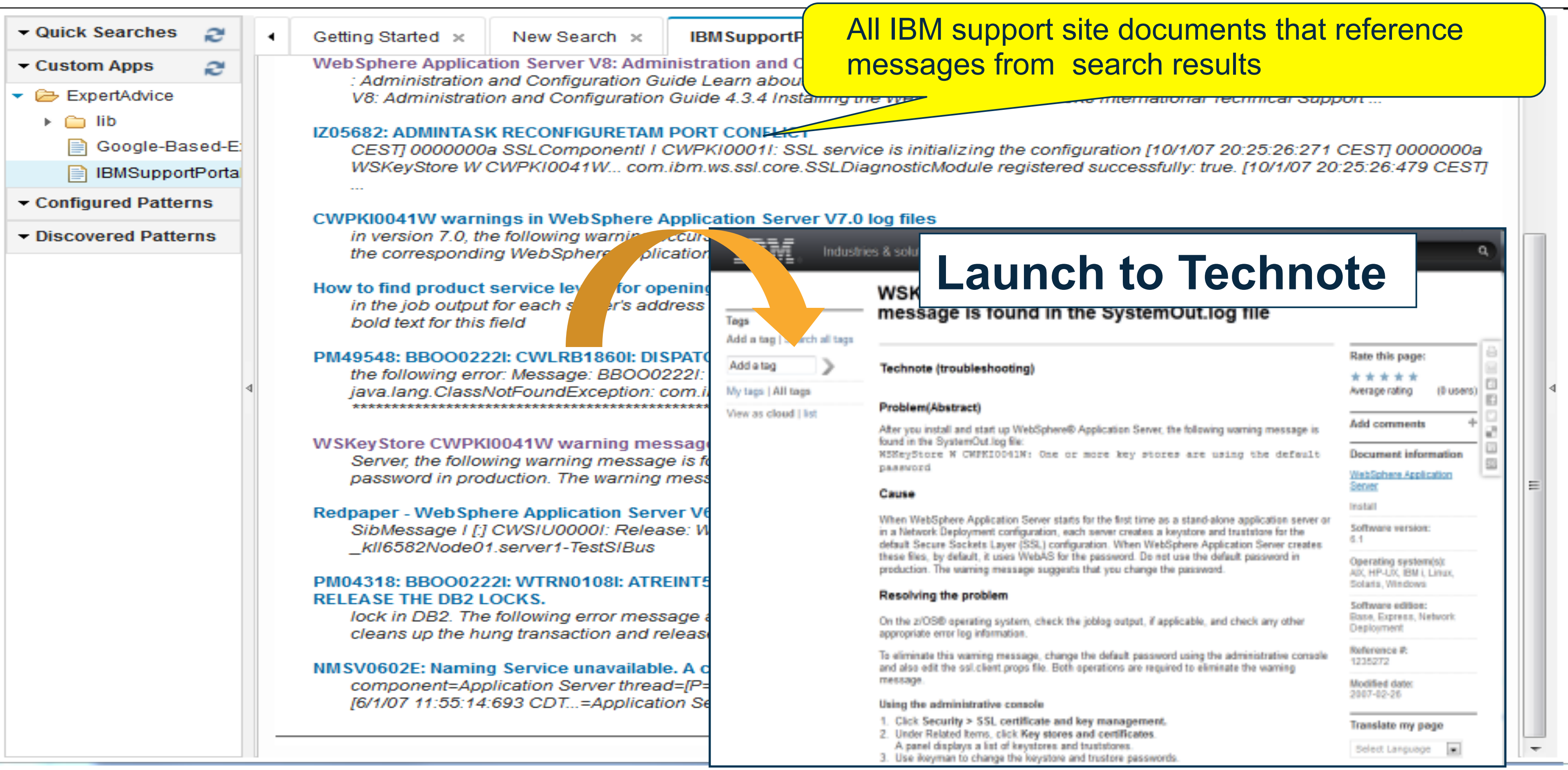
Timeframe of problem

Log analysis displays number of java 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

WebSphere Application Server V8: Administration and C
: Administration and Configuration Guide Learn abou
V8: Administration and Configuration Guide 4.3.4 Installing the We ... International Technical Support ...

IZ05682: ADMINTASK RECONFIGURETAM PORT CONFLICT
CEST] 0000000a SSLComponentI I CWPKI0001I: SSL service is initializing the configuration [10/1/07 20:25:26:271 CEST] 0000000a WSKeyStore W CWPKI0041W... com.ibm.ws.ssl.core.SSLDiagnosticModule registered successfully: true. [10/1/07 20:25:26:479 CEST]
...

CWPKI0041W warnings in WebSphere Application Server V7.0 log files
in version 7.0, the following warnin occur
the corresponding WebSphere Application

How to find product service lev for opening
in the job output for each s er's address
bold text for this field

PM49548: BBOO0222I: CWLRB1860I: DISPATC
the following error: Message: BBOO0222I:
java.lang.ClassNotFoundException: com.i
****

WSKeyStore CWPKI0041W warning messag
Server, the following warning message is f
password in production. The warning mess

Redpaper - WebSphere Application Server V6
SibMessage I [:] CWSIU0000I: Release: W
_kll6582Node01.server1-TestSIBus

PM04318: BBOO0222I: WTRN0108I: ATREINT5 RELEASE THE DB2 LOCKS.
lock in DB2. The following error message
cleans up the hung transaction and releas

NMSV0602E: Naming Service unavailable. A c
component=Application Server thread=[P=
[6/1/07 11:55:14:693 CDT...=Application Se

Launch to Technote

WSK
message is found in the SystemOut.log file

Technote (troubleshooting)

Problem(Abstract)

After you install and start up WebSphere® Application Server, the following warning message is found in the SystemOut.log file:

```
WSKeyStore W CWPKI0041W: One or more key stores are using the default
password
```

Cause

When WebSphere Application Server starts for the first time as a stand-alone application server or in a Network Deployment configuration, each server creates a keystore and truststore for the default Secure Sockets Layer (SSL) configuration. When WebSphere Application Server creates these files, by default, it uses WebAS for the password. Do not use the default password in production. The warning message suggests that you change the password.

Resolving the problem

On the z/OS® operating system, check the joblog output, if applicable, and check any other appropriate error log information.

To eliminate this warning message, change the default password using the administrative console and also edit the ssl.client.props file. Both operations are required to eliminate the warning message.

Using the administrative console

1. Click **Security > SSL certificate and key management.**
2. Under Related Items, click **Key stores and certificates**.
   A panel displays a list of keystores and truststores.
3. Use ikeyman to change the keystore and trustore passwords.

Document information

WebSphere Application Server

Install

Software version:
6.1

Operating system(s):
AIX, HP-UX, IBM i, Linux, Solaris, Windows

Software edition:
Base, Express, Network Deployment

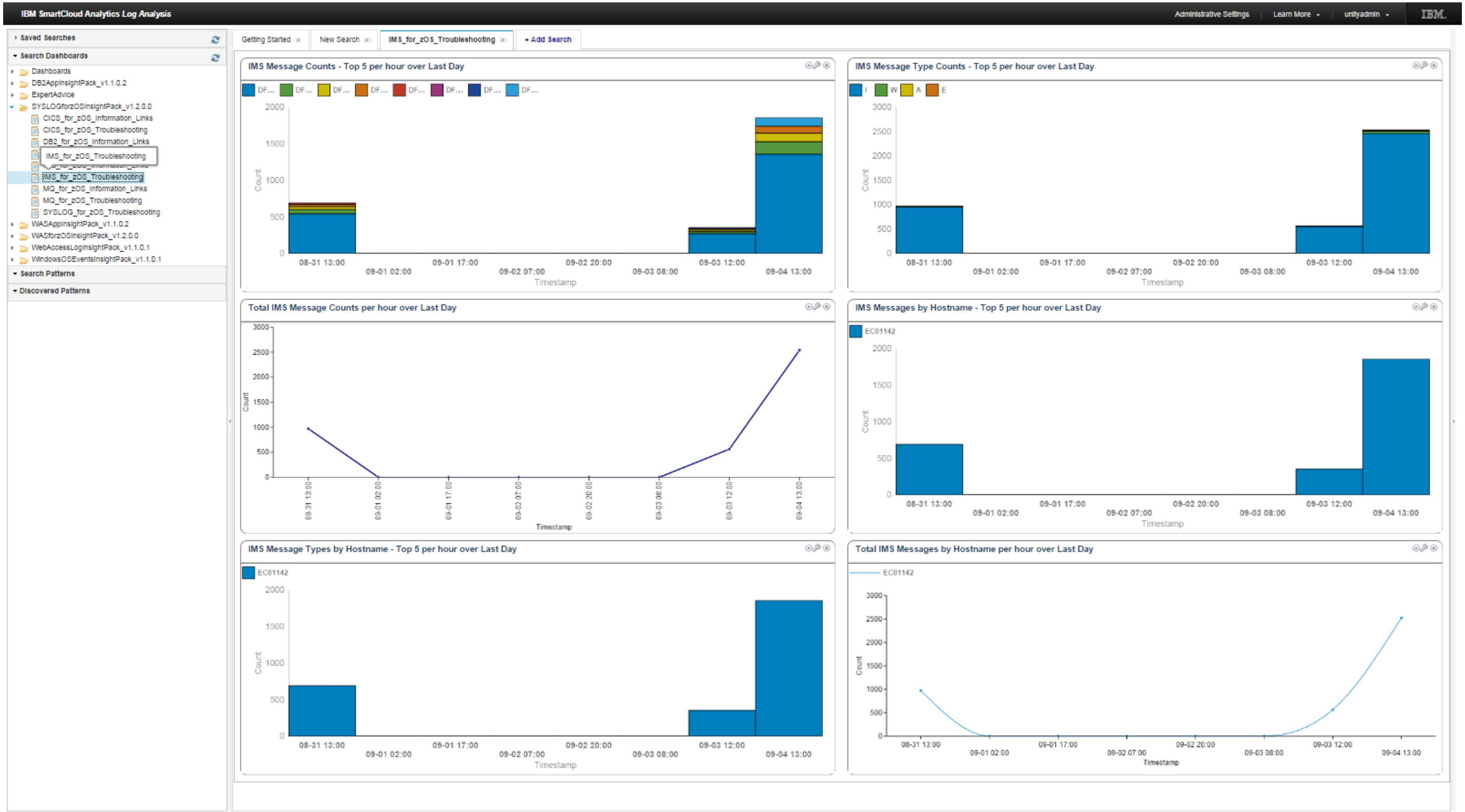
Reference #:
1235272

Modified date:
2007-02-26

Translate my page

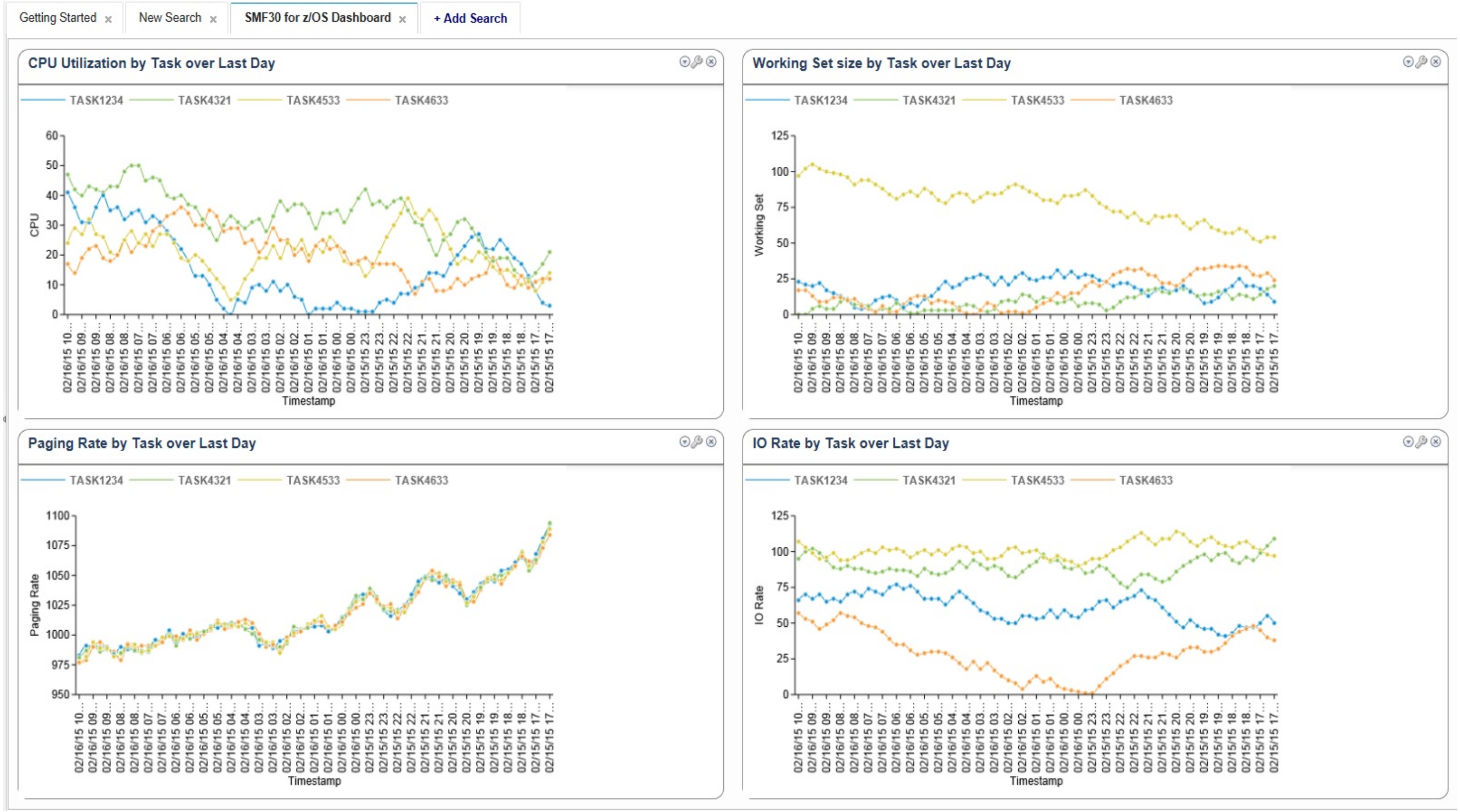
Select Language

Sample dashboard – View your log and metric data however you like



IBM SmartCloud Analytics Log Analysis
Administrative Settings
Learn More
unityadmin
IBM.
Saved Searches
Search Dashboards
Dashboards
DB2AppInsightPack_v1.1.0.2
ExpertAdvice
SYSLOGforzOSInsightPack_v1.2.0.0
CICS_for_zOS_Information_Links
CICS_for_zOS_Troubleshooting
DB2_for_zOS_Information_Links
IMS_for_zOS_Troubleshooting
MQ_for_zOS_Information_Links
MQ_for_zOS_Troubleshooting
SYSLOG_for_zOS_Troubleshooting
WASAppInsightPack_v1.1.0.2
WASforzOSInsightPack_v1.2.0.0
WebAccessLogInsightPack_v1.1.0.1
WindowsOSEventsInsightPack_v1.1.0.1
Search Patterns
Discovered Patterns
Getting Started
New Search
IMS_for_zOS_Troubleshooting
+ Add Search
IMS Message Counts - Top 5 per hour over Last Day
DF... DF... DF... DF... DF... DF... DF... DF...
IMS Message Type Counts - Top 5 per hour over Last Day
I W A E
Total IMS Message Counts per hour over Last Day
IMS Messages by Hostname - Top 5 per hour over Last Day
EC01142
IMS Message Types by Hostname - Top 5 per hour over Last Day
EC01142
Total IMS Messages by Hostname per hour over Last Day
EC01142
Count
Timestamp
0
500
1000
1500
2000
2500
3000
08-31 13:00
09-01 02:00
09-01 17:00
09-02 07:00
09-02 20:00
09-03 08:00
09-03 12:00
09-04 13:00

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



CPU Utilization by Task over Last Day

Working Set size by Task over Last Day

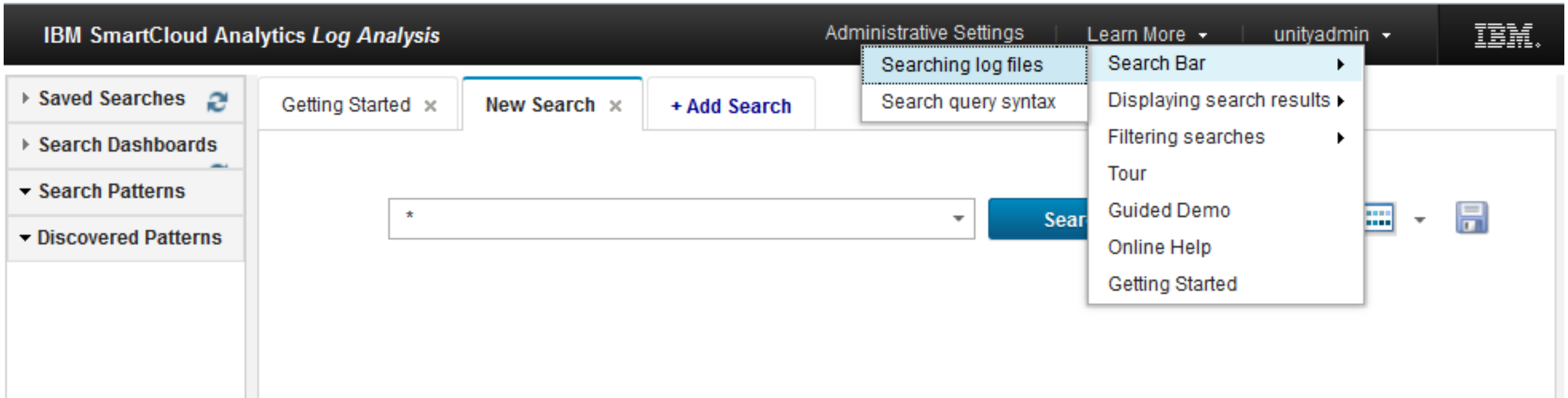
Paging Rate by Task over Last Day

IO Rate by Task over Last Day

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

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.

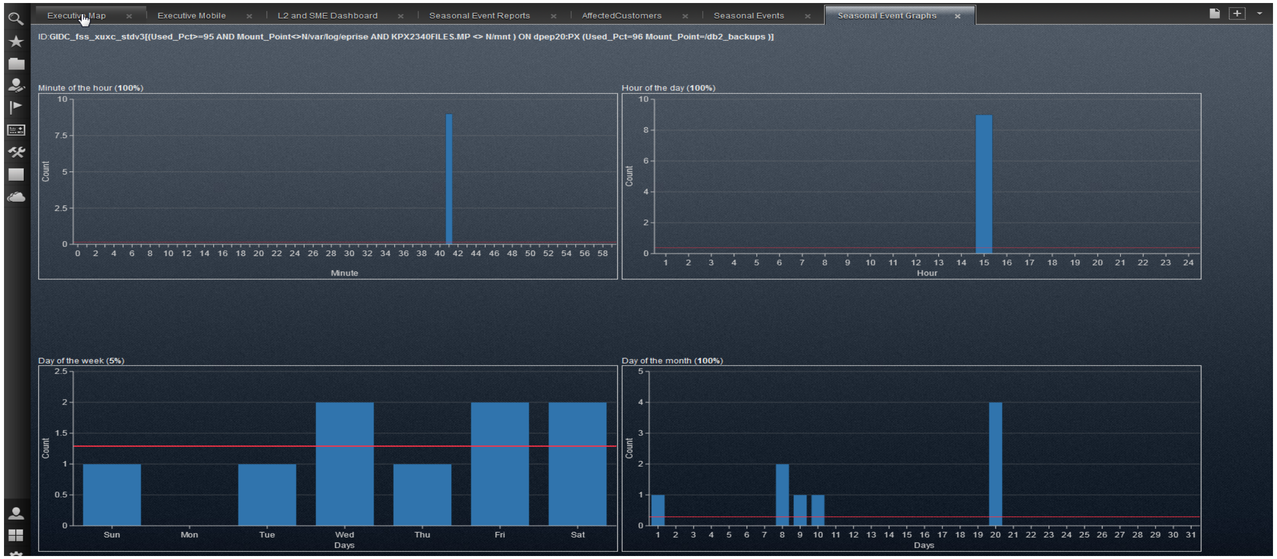
Integration with Service Management Solutions

Integration with Event Management

Network Operations Insight + IOA – Search and Analyze Events

Event Analytics – for Seasonal Event Identification

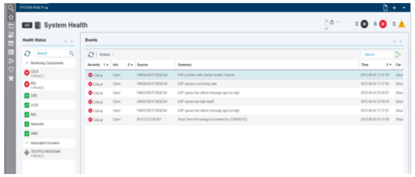
- Easily identify ‘related’ Events that may be candidates for suppression
- Identify “difficult to spot” seasonal events that often result in regular periodic problems
- Leverage visualizations that help you quickly isolate more severe and significant problems.



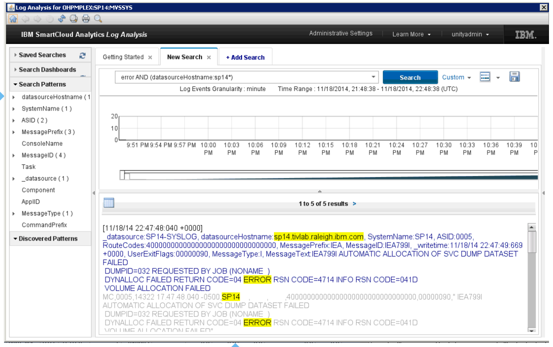
ID:GIDC_fss_xuxc_stdv3[(Used_Pct>=95 AND Mount_Point<>N/var/log/eprise AND KPX2340FILES.MP <> N/mnt) ON dpep20:PX (Used_Pct=96 Mount_Point=/db2_backups)]

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

Log Analysis Integration with existing Service Management Solutions



Service Management Unite



error AND (datasourceHostname:sp14*)

Log Events Granularity : minute   Time Range : 11/18/2014, 21:48:38 - 11/18/2014, 22:48:38 (UTC)

```
[11/18/14 22:47:48:040 +0000]
_datasource:SP14-SYSLOG, datasourceHostname:sp14.tivlab.raleigh.ibm.com, SystemName:SP14, ASID:0005,
RouteCodes:4000000000000000000000000000000, MessagePrefix:IEA, MessageID:IEA799I, _writetime:11/18/14 22:47:49:669
+0000, UserExitFlags:00000090, MessageType:I, MessageText:IEA799I AUTOMATIC ALLOCATION OF SVC DUMP DATASET
FAILED
 DUMPID=032 REQUESTED BY JOB (NONAME  )
 DYNALLOC FAILED RETURN CODE=04 ERROR RSN CODE=4714 INFO RSN CODE=041D
 VOLUME ALLOCATION FAILED
MC,0005,14322 17.47.48.040 -0500,SP14     ,        ,        ,4000000000000000000000000000000,00000090," IEA799I
AUTOMATIC ALLOCATION OF SVC DUMP DATASET FAILED
 DUMPID=032 REQUESTED BY JOB (NONAME  )
 DYNALLOC FAILED RETURN CODE=04 ERROR RSN CODE=4714 INFO RSN CODE=041D
 VOLUME ALLOCATION FAILED"
```

Search and analyze logs, metrics and events

Event Management
OMNIbus/Netcool
Operations
Insight

Problem
Determination
NetView
CANZLOG

Performance
Monitoring
ITM/OMEGAMON

Surface anomalies

IBM zAware

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

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

IOA for z Systems Early Access and Beta Program

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

Thank
You