

# IBM zAware - Using Analytics to Improve System z Availability

Anuja Deedwaniya  
[anujad@us.ibm.com](mailto:anujad@us.ibm.com)

Session 16077



Thanks to Garth Godfrey, zAware Development for contribution to presentation material

**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/>

## Background – Why IBM zAware



### Systems are more complex and more integrated than ever

- The rate of change of today's IT infrastructures stress the limits of IT to resolve problems quickly and accurately--while preserving SLAs
- IT is challenged to diagnose system anomalies and restore service quickly
- *Some problems are particularly...*
  - **Difficult to detect**
    - Several allowable anomalies can build up over time
    - Symptoms / problems can manifest for hours or days
    - Problem can grow, cascade, snowball
  - **Difficult to diagnose**
    - Sometimes finding the *system* in error is a challenge
    - Many times finding the *component* in error is a challenge
    - Volume of data is not humanly consumable, *especially* when seconds count
- *Need information and insight*



Complete your session evaluations online at [www.SHARE.org/Pittsburgh-Eval](http://www.SHARE.org/Pittsburgh-Eval)

# IBM System z Advanced Workload Analysis Reporter (zAware) Smarter Computing Needs Smarter Monitoring

- Cutting edge pattern recognition techniques look at the health of a system to pinpoint deviations from the 'norm'
- Proactively identifies unusual system behavior of z/OS workloads
- Improves problem diagnosis across a set of System z servers
- High speed analytics facilitates the ability to consume large quantities of message logs
- Speeds up the time to decide on appropriate corrective actions on problems before they get bigger and improve availability
- Allow establishment of procedures to prevent reoccurrence
- New technology based on Machine learning, modeling and historical data work to analyze your unique environment developed by IBM Research



- Runs in a special purpose firmware partition on zEC12 or zBC12
- Monitors zEC12 or other System z servers running z/OS v1.13 +PTFs or later
- Requires OPERLOG

# Specific Applications of IBM zAware

## ■ Identify a possible z/OS incident

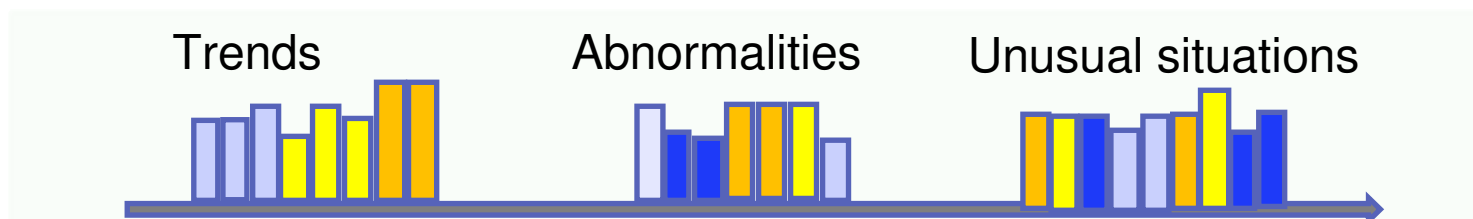
- ▶ *Which image is having a potential problem?*
  - Examines unique messages
  - High score generated by unusual messages or message patterns
- ▶ *When did this unusual behavior start?*
  - For a selected 10 minute interval either the current 10 minute interval or past intervals
    - **Which messages are unusual?**
    - **How often did the message occur?**
    - **When did the message start to occur?**
- ▶ *Were similar messages issued in the past?*
  - Understands message characteristics and message patterns

## ■ Identify behavior after a change has been made

- ▶ *Are unusual messages being issued after a change ?*
  - New software levels (operating system, middleware, applications)
  - Updated system settings or system configurations
- **Diagnose intermittent problems**
  - ▶ *Are new unusual messages being issued in advance of the problem?*
    - Are more messages issued then expected?
    - Are messages issued out of a normal pattern?

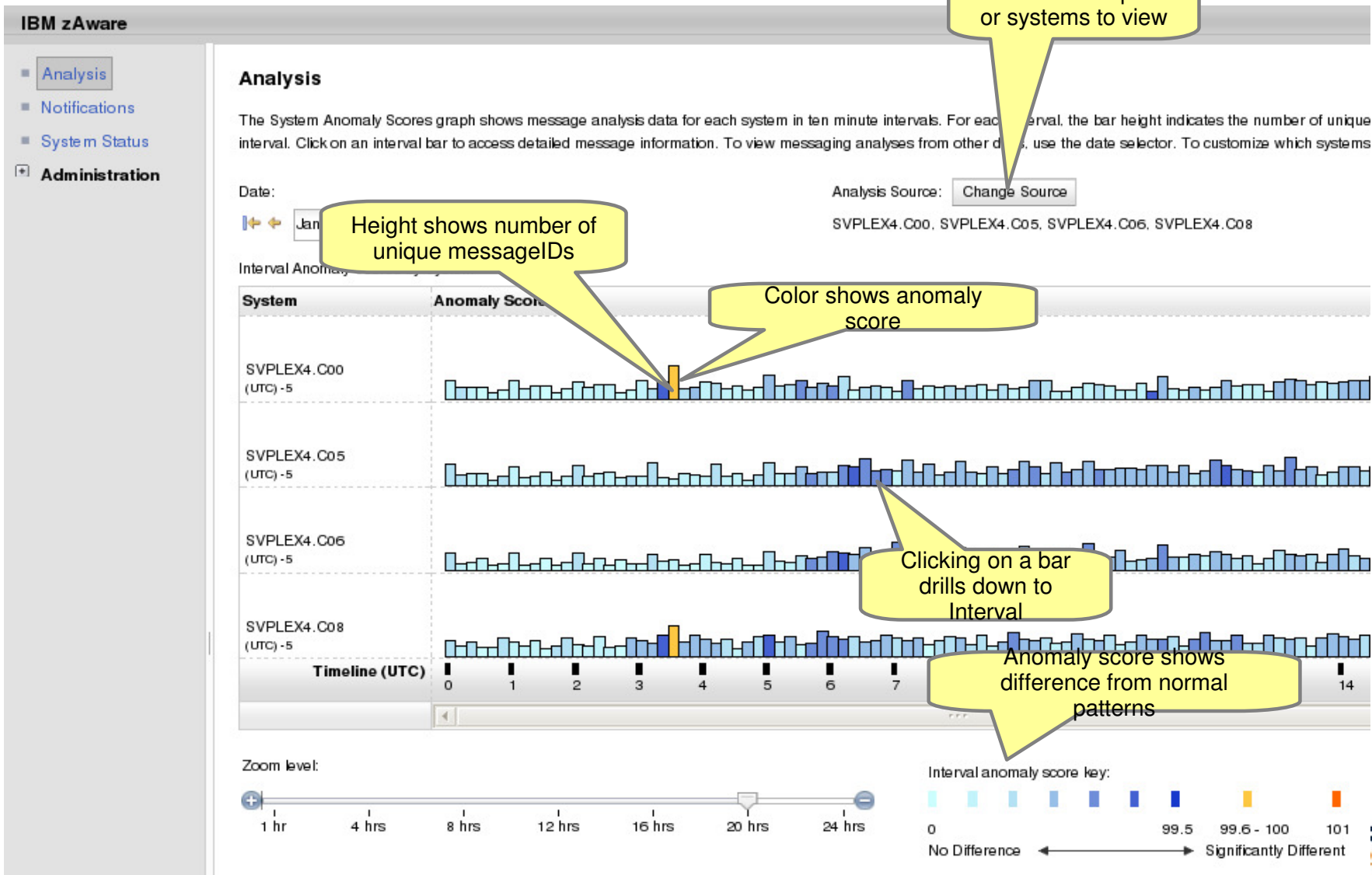
*Appeals to IT VP, Support, Operations, Systems Staff, Service Centers*

*Finds Anomalies that Would be Manually Hard to Detect*



**Reduces time and effort to identify & diagnose problematic messages**

# Analysis View



Complete your session evaluations online at [www.SHARE.org/Pittsburgh-Eval](http://www.SHARE.org/Pittsburgh-Eval)



# Interval View

IBM zAware

Analysis

Notifications

System Status

Administration

Welcome admin

Log out

IBM

Current Analysis > Interval View

Interval View for System C00

The Messages table provides detailed information for each message that occurred during the indicated time interval. To view message details for other intervals use the date and time interval selectors. Click the **Return to Analysis** button to go back to the Analysis page.

Date:

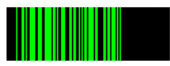



January 6, 2013

Time interval (UTC):

03:30 -- 03:40

Messages

Actions

▼1 Anomaly Score	▼2 Interval Contribution Score	Message Context	Rules Status	Appearance Count	Time Line	Message ID	Message Example	Rarity Score	Component	Cluster ID
1	41.348	new	None	238		<a href="#">IGW702I</a>	PDSE Directory Validation Unsuccessful DESC:<ND> Structure is corrupted LTK:	101	IGW	-1
1	41.3	new	None	237		<a href="#">IGW699I</a>	PDSE Directory Validation Unsuccessful DESC:PDSE structure is corrupted	101	IGW	-1
1	18.184	new	None	16		<a href="#">IEC909I</a>	212-00,MSR13M7 ,TESTM7 ,SAM00001,00000024,06105AF8	101	IEC	-1
1	10.684	new	None	2		<a href="#">IEC036I</a>	002-6C,IGC0005E,MSR13M7,TE:IST.DFSMS.MAS1IR13.DS00000:	101	IEC	-1
1	7.818	unclustered	IMPORTANT	1		<a href="#">CNZZ002E</a>	MESSAGE THRESHOLD REACHED FOR JOB Z850A010 ASID 021B	74	CNZZ	-1
1	0	in_context	IMPORTANT	1		<a href="#">CNZZ007E</a>	MESSAGE RATE EXCEEDED 600 MESSAGES IN <1 SECONDS.	64	CNZZ	22
1	0	in_context	IMPORTANT	4		<a href="#">IEA611I</a>	COMPLETE DUMP ON D83DUMP.DYNZOS21.C00.D130: DUMPID=003 REQUESTED BY	47	IEA	109

Complete your session evaluations online at [www.SHARE.org](http://www.SHARE.org)

# Inside IBM zAware Analytics

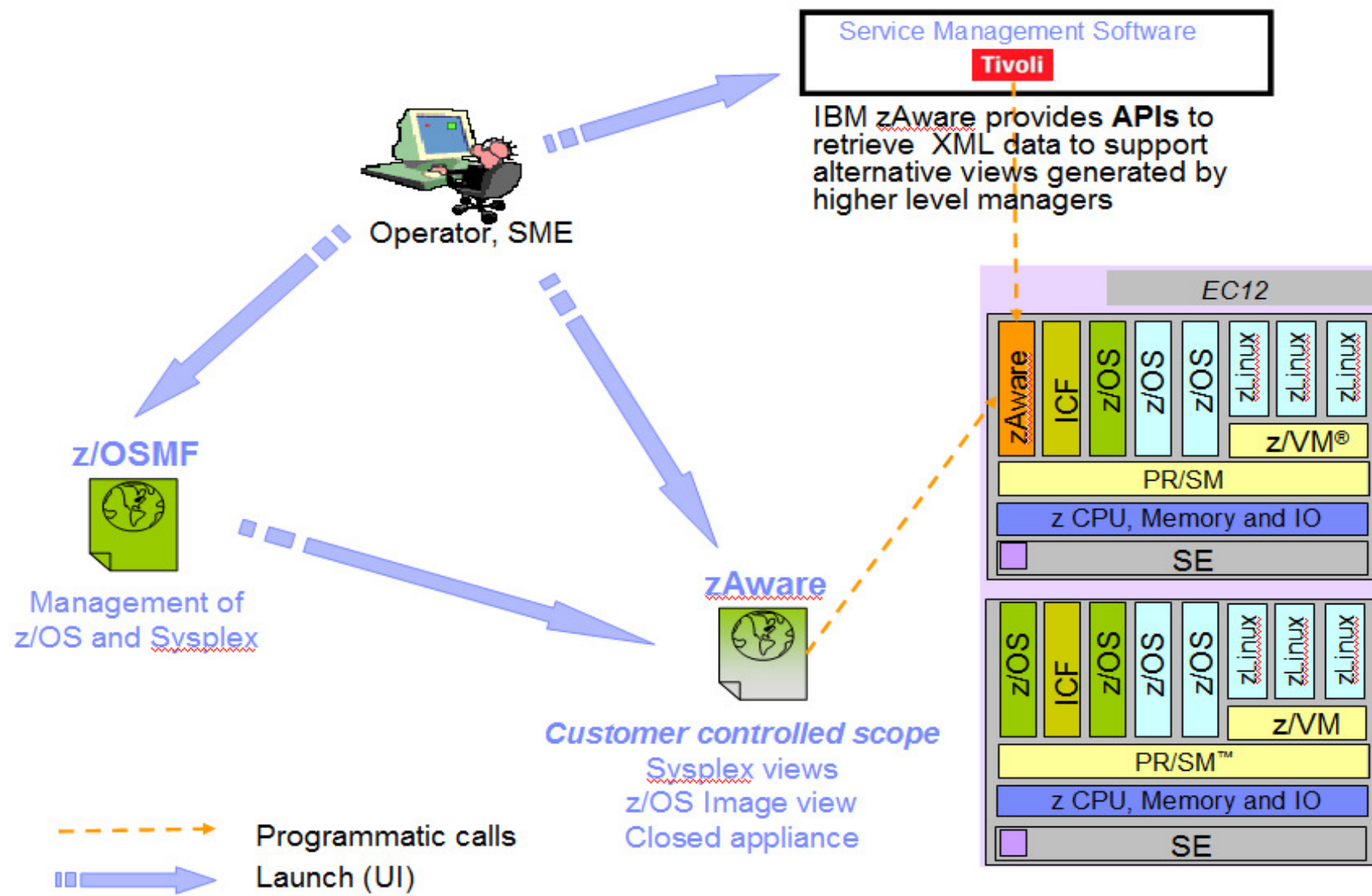
- OPERLOG is processed per-system
- zAware recognizes any well-formed message IDs,
  - including IBM and non-IBM products and customer applications
- zAware summarizes the common message text and records the occurrences
- zAware builds a **model** of normal behavior based on the last 90 days
  - Called “Training”
  - Automatically trains every 30 days
  - Can be forced manually
  - Customizable
  - Unusual days can be excluded from future models
  - Support for excluding messages from training
- z/OS utility is used to load historical logs into zAware

# Inside IBM zAware Analytics

- Real-time OPERLOG data is compared to the model
- Assigns a **message anomaly** score to indicate deviation from the model
  - Rare messages
  - Out of context from normal patterns
  - High counts
- Uses z/OS-specific knowledge to influence the scores
- Generates an **interval anomaly** score per 10 minute interval
  - Current interval is updated every 2 minutes
  - GUI shows number of unique message IDs (bar height)
  - GUI shows interval anomaly score (bar color)
- Drill down on interval shows the message scores
- XML output available via HTTP APIs to drive alerting



# IBM zAware Complements Your Existing Environment



# Backup

# IBM System z Advanced Workload Analysis Reporter (IBM zAware) Using Analytics to Improve System z Availability

- **The complexity and rate of change of today's IT infrastructures stress the limits of IT to resolve problems quickly and accurately--while preserving SLAs**
- **IT is challenged to diagnose system anomalies and restore service quickly**
  - ▶ Systems often experience problems which are difficult or unusual to detect
  - ▶ Existing tools do little to identify messages preceding system problems
  - ▶ Some incidents begin with symptoms that remain undetected
  - ▶ Manual log analysis is skills-intensive, and prone to errors
- **IBM zAware with Expert System Diagnostics Gets it Right, Fast**
  - ▶ IBM zAware helps improve problem determination in *near real time* – helps rapidly and accurately **identify problems** and **speed time to recovery**
    - Analyzes **massive amounts of data** to identify problematic messages, providing information to enable faster corrective action
    - Analytics on log data provides a near real time view of current system state
    - Cutting edge pattern recognition examines system behavior to help you pinpoint deviations
    - Machine learning, modeling and historical data work to analyze **your unique environment**
- **Benefits**
  - ▶ Can reduce problem determination and troubleshooting
  - ▶ Particularly helpful when problems involve multiple teams
  - ▶ Helps you diagnose problems quickly and more accurately to improve service recovery time
  - ▶ Easy to use graphical interface



Complete your session evaluations online at [www.SHARE.org/Pittsburgh-Eval](http://www.SHARE.org/Pittsburgh-Eval)

# Ignore messages - High scoring message review



**A)** If a **real problem** is indicated,

- **Fix the problem** on the monitored system
- Check subsequent zAware Analysis to confirm the resolution
- Do **not** mark these messages as ignored

**B)** If the messages are **normal messages** from the new workload,

- Mark these as **Ignore until next training**
- At the next training for this system, these messages will be built into the model, and removed from the system's ignored list

**C)** If the messages are **always ok** (normal, but infrequent)

- Mark these as **Ignore until manually restored**
- In subsequent analysis, the ignored messages will not contribute to the anomaly scores
- This setting will **persist** after trainings
- This **reduces false positives**, based on user input, so real problems are not masked

This gives the user input into the IBM zAware rules.

Complete your session evaluations online at [www.SHARE.org/Pittsburgh-Eval](http://www.SHARE.org/Pittsburgh-Eval)



# Sample Use cases

## Identify unusual behavior quickly

Which z/OS image is having unusual message patterns?

- **Yellow and dark blue on CB88**

When did the behavior start?

- **Around 2:30**

Date:



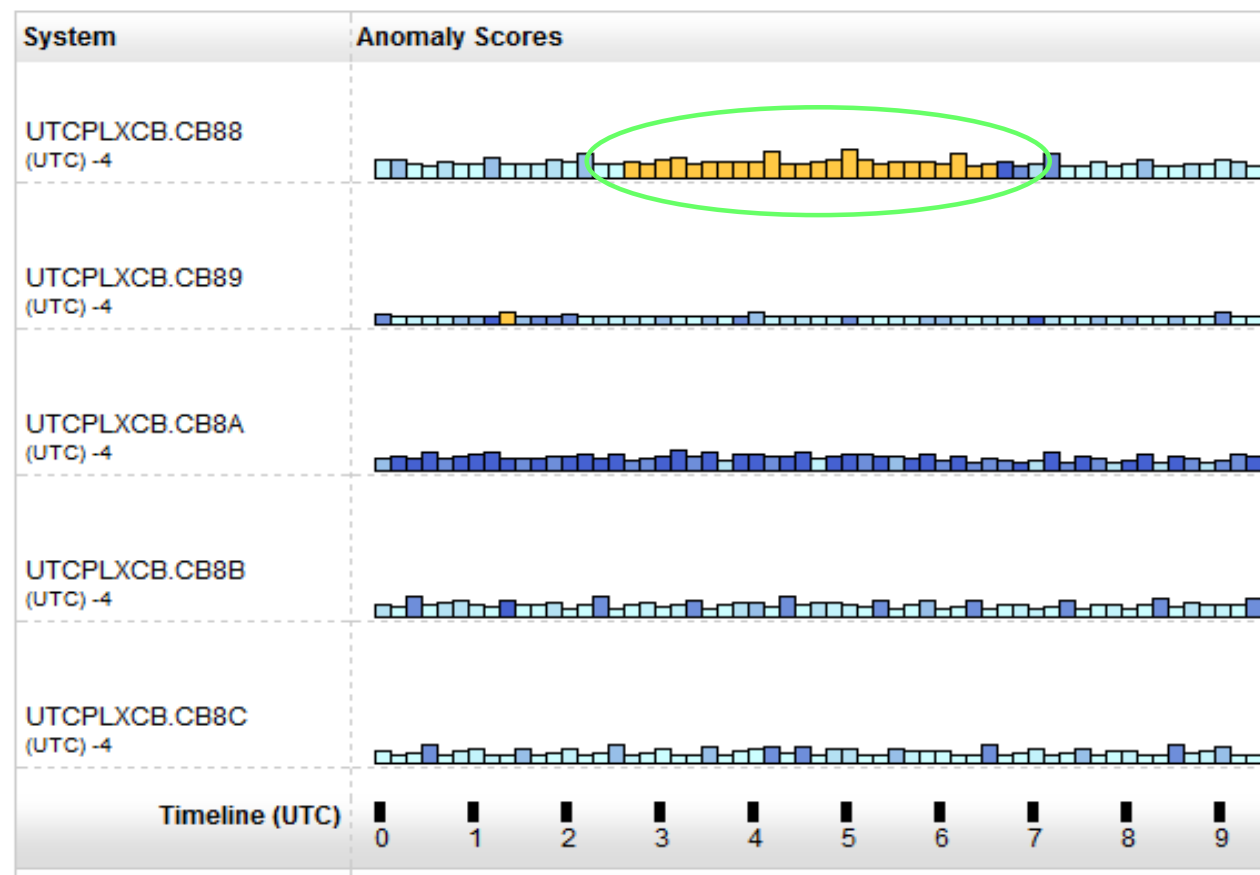
March 22, 2013



Analysis Source:

UTCPLXCB

Interval Anomaly Scores by System

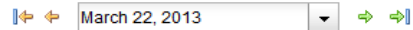


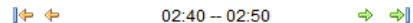


# Identify unusual behavior quickly – Configuration Error

## Interval View for System CB88

The Messages table provides detailed analysis information for each message that occurred during the indicated time interval. To view message details for other intervals use the date and time interval selectors. Click the Re



Date:  

Time interval (UTC):  

Analysis Source:  
UTCPLXCB.CB88

Interval anomaly score:  
99.8

### Messages

Actions ▼										
▼1 Anomaly Score	▼2 Interval Contribution Score	Message Context	Rules Status	Appearance Count	Time Line	Message ID	Message Example	Rarity Score	Component	Cluster ID
0.999	196.275	unclustered	None	898		<a href="#">IRRC131I</a>	(<) RACF ENCOUNTERED AN R_PROXYSERV ERROR WHILE ATTEMPTING TO CREATE AN	73	IRRC	-1
0.999	48.115	unclustered	None	932		<a href="#">IRRC144I</a>	(<) RACF ENCOUNTERED AN R_PROXYSERV ERROR: SAF RETURN CODE=X'00000008',	85	IRRC	-1

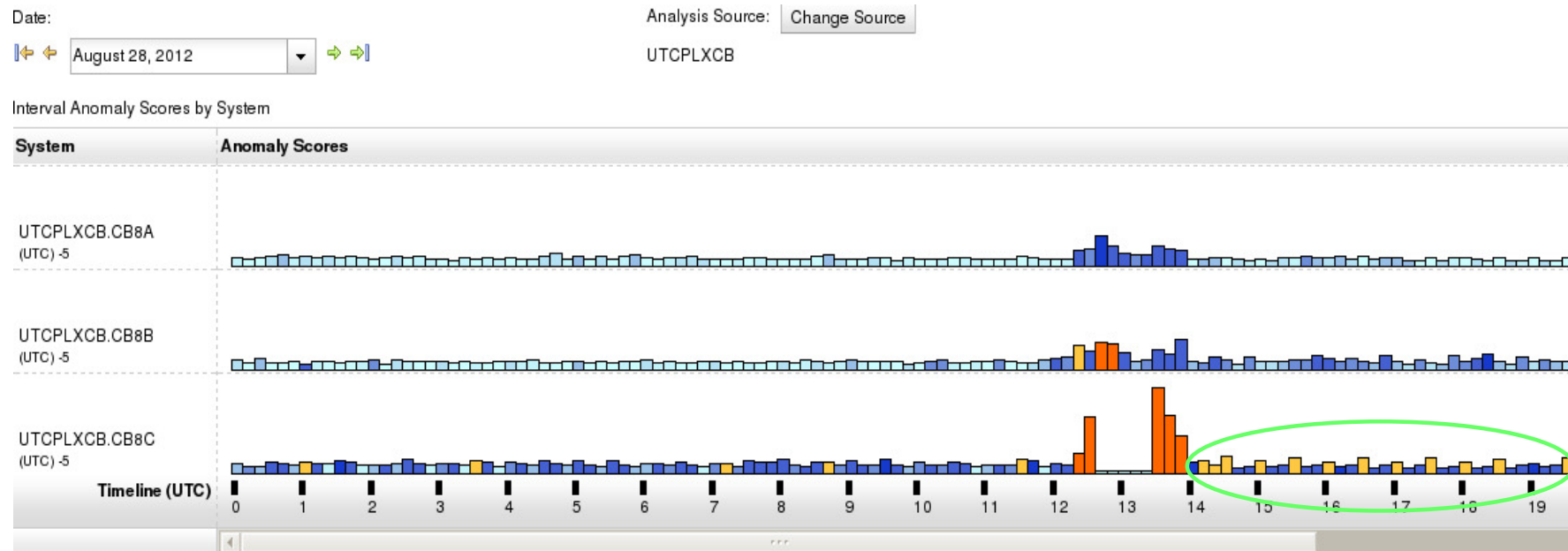
## What component is having the problem?

- Drill down indicates 900 IRRC131I and IRRC144I messages per interval. A review of SYSLOG showed that this was the result of work being performed in the LDAP address spaces. Further analysis showed that the LDAP PC Callable Interface was not enabled. At 6:40, the function was enabled, and the 131I and 144I messages are no longer generated.

## Impact

- Unnecessary messages blocking ability to see anything else. Impacts ability to look at the console.

## Identify unusual behavior quickly



**Which z/OS image is having unusual message patterns?**

- **Recurring yellow and dark blue on CB8C**

**When did the behavior start?**

- **After an IPL at 13:30**

# Identify unusual behavior quickly – Configuration Error

## Interval View for System CB8C

The Messages table provides detailed analysis information for each message that occurred during the indicated time interval. To view message details for other intervals use the date and time interval **Return to Analysis** button to go back to the Analysis view.

Date:

August 28, 2012

Analysis Source:

UTCPLXCB.CB8C





Time interval (UTC):

14:20 -- 14:30

Interval anomaly score:

99.6

Messages

▼1 Anomaly Score	Interval Contribution Score	Message Context	Rules Status	Appearance Count	Time Line	Message ID	Message Example	Rarity Score	Component
0.999	14.369	unclustered	None	2		<a href="#">IEE838I</a>	TNPROC NON-CANCELABLE - ISSUE FORCE ARM	93	IEE
0.999	12.943	unclustered	None	2		<a href="#">EZZ0621I</a>	AUTOLOG FORCING TNPROC, REASON: TCP/IP HAS BEEN RESTARTED	100	EZZ
0.999	9.41	unclustered	None	1		<a href="#">IXG601I</a>	10.27.18 LOGGER DISPLAY 081 CONNECTION INFORMATION BY	62	IXG
0.997	6.078	unclustered	None	3		<a href="#">IEA631I</a>	OPERATOR GTHOMPS NOW INACTIVE, SYSTEM=CB8C , LU=TCP8C003	31	IEA

**Which subsystem or component is abnormal?**

- Examine high-scoring messages

**When did the behavior start?**

- When did the messages start to occur?

**Were similar messages issued previously?**

- Easily examine prior intervals or dates

Complete your session evaluations online at [www.SHARE.org/Pittsburgh-Eval](http://www.SHARE.org/Pittsburgh-Eval)

Moving left and right by interval shows messages due to TNPROC being cancelled by TCP/IP

## Identify behavior after a change

### Are unusual messages being issued after a change?

- New / updated workload (OS, middleware, apps) was introduced
- Detected as yellow bars
- Once messages confirmed as ok, can rebuild your system model, and workload now understood as “normal.”



# References

- IBM System z Advanced Workload Analysis Reporter (IBM zAware) Guide SC27-2623-00

<http://www.ibm.com/systems/z/os/zos/bkserv/r13pdf/#E0Z>

or IBMResourceLink Library → zEC12 → Publications

- Redbook: Extending z/OS System Management Functions with IBM zAware SF24-8070-00

<http://www.redbooks.ibm.com/abstracts/sg248070.html?Open>

- IBM Mainframe Insights blog [www.ibm.com.systemz](http://www.ibm.com.systemz)

- The Journey to IBM zAware

[http://www.ibm.com/connections/blogs/systemz/entry/zaware?lang=en\\_us](http://www.ibm.com/connections/blogs/systemz/entry/zaware?lang=en_us)

- zAware Installation and Startup

[http://www.ibm.com/connections/blogs/systemz/entry/zaware\\_installation?lang=en\\_us](http://www.ibm.com/connections/blogs/systemz/entry/zaware_installation?lang=en_us)

- Top 10 Most Frequently Asked Questions About IBM zAware

[http://www.ibm.com/connections/blogs/systemz/entry/zawarefaq?lang=en\\_us](http://www.ibm.com/connections/blogs/systemz/entry/zawarefaq?lang=en_us)

- IBM zAware Demo

[http://www.ibm.com/connections/blogs/systemz/entry/zawaredemo?lang=en\\_us](http://www.ibm.com/connections/blogs/systemz/entry/zawaredemo?lang=en_us)

IBM zAware

# Operating Requirements



# Operating Requirements – IBM zAware Server

- Logical partition on a **zEC12** or **zBC12** server
  - Runs on **IFLs** or general purpose **CPs** – may be dedicated or shared
  - Runs its own self-contained firmware stack
  - Recommended 2 partial engines
    - Initial priming and training: 25-80% of 1 **zEC12** IFL (30-95% of 1 **zBC12** IFL)
    - Analysis: 20-40% of 1 IFL (zEC12 or zBC12)
- Memory and DASD resources are dependent on the number of monitored clients, amount of message traffic, length of time data retained
  - Minimum Memory is **4 GB** for 6 clients with light message traffic (500 msgs/sec)  
For > 6 clients + **256 MB per client** required
  - Estimated DASD storage is **500 GB (ECKD) + 5GB per client**
- Network resources
  - HiperSockets or shareable OSA ports or IEDN
  - IP address for partition
- Browsers
  - Internet Explorer 9
  - Firefox ESR 17

Complete your session evaluations online at [www.SHARE.org/Pittsburgh-Eval](http://www.SHARE.org/Pittsburgh-Eval)

# Operating Requirements – z/OS Monitored Clients

- System z servers supported as IBM zAware monitored clients
  - zEC12
  - zBC12
  - IBM zEnterprise™ 196 (z196) or z114,
  - IBM System z10™ EC or BC
  - Prior generations that meet the OS and configuration requirements
- Running **z/OS 1.13 + PTFs** or **z/OS 2.1**
  - APAR OA38747
  - APAR OA38613
  - APAR OA39256
  - APAR OA42095
- System needs to be configured as a monoplex, system in a multisystem sysplex, or a member of a parallel sysplex
- Using operations log (**OPERLOG**) as the hardcopy medium
- Sysplex name + system name must uniquely identify system
- Requires an OSA or IEDN or HiperSocket for IP network connection
- z/OS zAware monitored client MIPs usage ~ 1%

Complete your session evaluations online at [www.SHARE.org/Pittsburgh-Eval](http://www.SHARE.org/Pittsburgh-Eval)

## Integration with z/OSMF

- **Using the z/OSMF GUI**
  - **Configure a new external link**
    - to access IBM zAware from z/OSMF
  - **Administration > Links > Actions > New**
    - Provide link name, SAF suffix, **zAware GUI URL**
    - Category – recommend Problem Determination
    - Define authority required to use the link

## Integration with other System Management products

- **APIs**
  - Provides **XML** equivalent to GUI
    - Analysis page
    - Interval View page
  - Requires HTTPS
    - From z/OS, use AT-TLS
  - HTTP GET/POST requests
    - **Connect and authenticate** to IBM zAware server
      - *UserID known as a zAware user (e.g. LDAP)*
    - **Retrieve analysis** for a monitored client
      - **LPAR** *Interval scores for date*
      - **INTERVAL** *Message scores for a 10-minute interval*

# Integration with other System Management products

- IBM Tivoli **NetView** for z/OS
  - Use the APIs to pull the IBM zAware results
  - Sample programs are available from <https://www.ibm.com/developerworks/mydeveloperworks/wikis/home/wiki/Tivoli%20System%20z%20Monitoring%20and%20Application%20Management/page/Integration%20Scenarios%20for%20Tivoli%20NetView%20for%20zOS?lang=en>
  - Described in detail in the Redbook:
    - **Extending z/OS System Management Functions with IBM zAware**
  - The samples can be tailored to drive NetView message **automation** for high anomaly scores:
    - Generate a message
    - Generate an event
  - CANZLOG – Browse consolidated logs for PD
- **Announced July 2013**, Tivoli Integrated Service Management products use of IBM zAware results.
  - Omegamon XE on z/OS (including predefined situations)
- Other products can exploit the XML format results
  - Rexx exec sample can be obtained from IBM

# Omegamon XE on z/OS – July 2013

