#SHAREorg

SHARE
Technology · Connections · Results

IBM zAware

Using Analytics to Improve System z Availability

Garth Godfrey
IBM Poughkeepsie
ggodfrey@us.ibm.com

Session 13569
Wed, August 14, 2013
3:00 – 4:00

SHARE in Boston

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States, other countries, or both.

DS8000
ECKD
FICON*
GDPS*
GPFS
HiperSockets
IBM*
IBM (logo)*
InfiniBand*
Parallel Sysplex*
PR/SM
Redbooks*
System x*
System z*
System z9*
System z10*
Tivoli
WebSphere*
Z9*
z10
z10 Business Class
z10 EC
z/OS*
z/VM*
zEnterprise

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Notice Regarding Specialty Engines (e.g., zIIPs, zAAPs and IFLs):

Any information contained in this document regarding Specialty Engines ("SEs") and SE eligible workloads provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g., zIIPs, zAAPs, and IFLs). IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the “Authorized Use Table for IBM Machines” provided at

www.ibm.com/systems/support/machine_warranties/machine_code/aut.html (“AUT”).

No other workload processing is authorized for execution on an SE.

IBM offers SEs at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.

Agenda

- What is IBM zAware, and what can it detect?
  - How can it help identify problems on z/OS systems?
  - How can it help diagnose problems on z/OS systems?
- Operating requirements
- Use of the IBM zAware GUI
- Enhancements available Sept 2013
- Integration with other management products

Background

Systems are more complex and more integrated than ever

- *Errors can occur anywhere in a complex system*

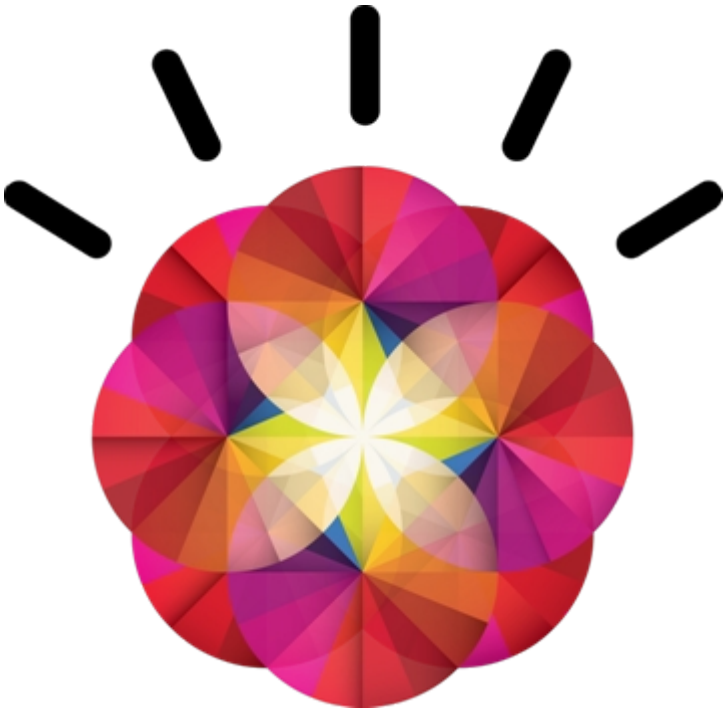
- *Some problems are particularly…*
  - **Difficult to detect**
    - Several allowable anomalies can build up over time
    - Symptoms / problems can manifest for hours or days
    - Problem can grow, cascade, snowball
  - **Difficult to diagnose**
    - Sometimes finding the *system* in error is a 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*

IBM zAware – IBM System z Advanced Workload Analysis Reporter

- Monitors **z/OS OPERLOG** including all messages written to z/OS console, including ISV and application generated messages
- Detects things typical monitoring systems miss due to:
  - Message suppression (message too common)
    Useful for long-term health issues
  - Uniqueness (message not common enough)
    Useful for real-time event diagnostics
- Color coded easy to use GUI via web browsers
- Output can be queued up to existing monitoring systems.
- Early detection and focused diagnosis can help improve time to recovery

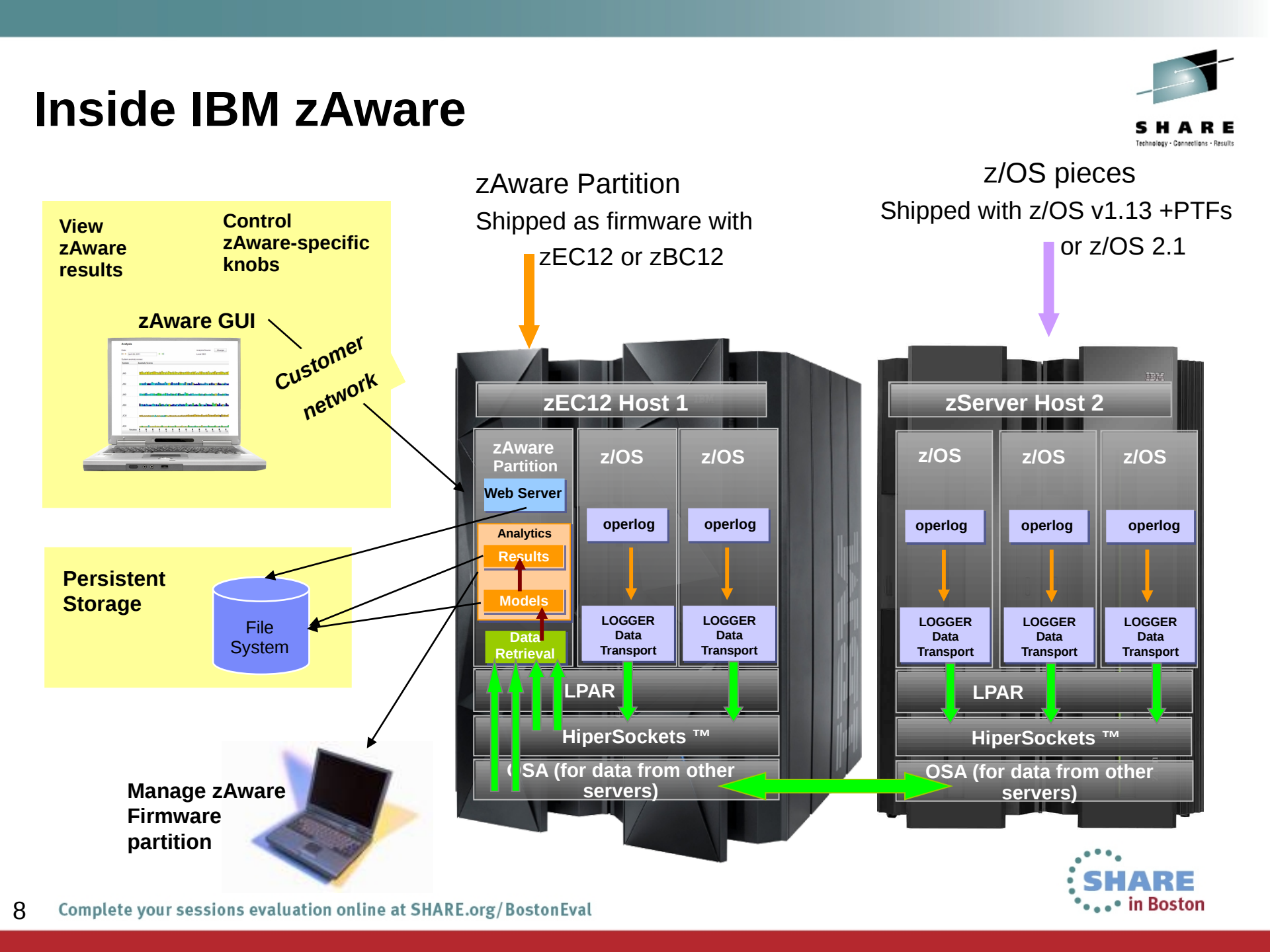
IBM zAware – Smarter Computing Needs Smarter Monitoring

- New technology based on machine learning developed by IBM Research
- Cutting edge pattern recognition techniques look at the health of a system to pinpoint deviations from the ‘norm’
- High speed analytics facilitates the ability to consume large quantities of message logs
- Improves problem diagnosis across a set of System z servers
- Speeds up the time to decide on appropriate corrective actions on problems before they get bigger
- Allow establishment of procedures to prevent reoccurrence



zAware’s capacity as a ‘watch dog’ can help to detect unusual behavior in near real time

Inside IBM zAware



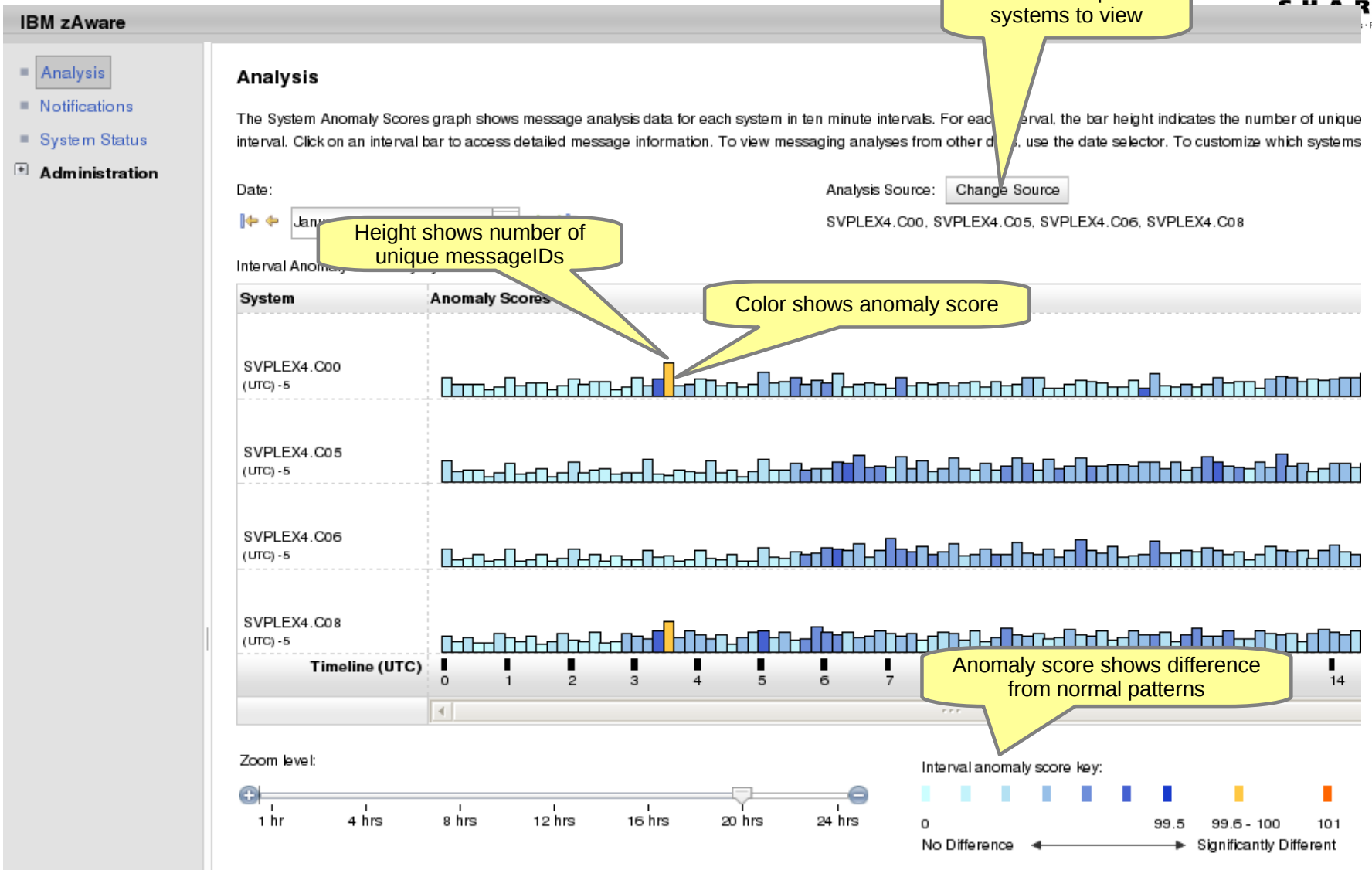
Inside IBM zAware Analytics

- 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
- z/OS utility is used to load historical logs into zAware

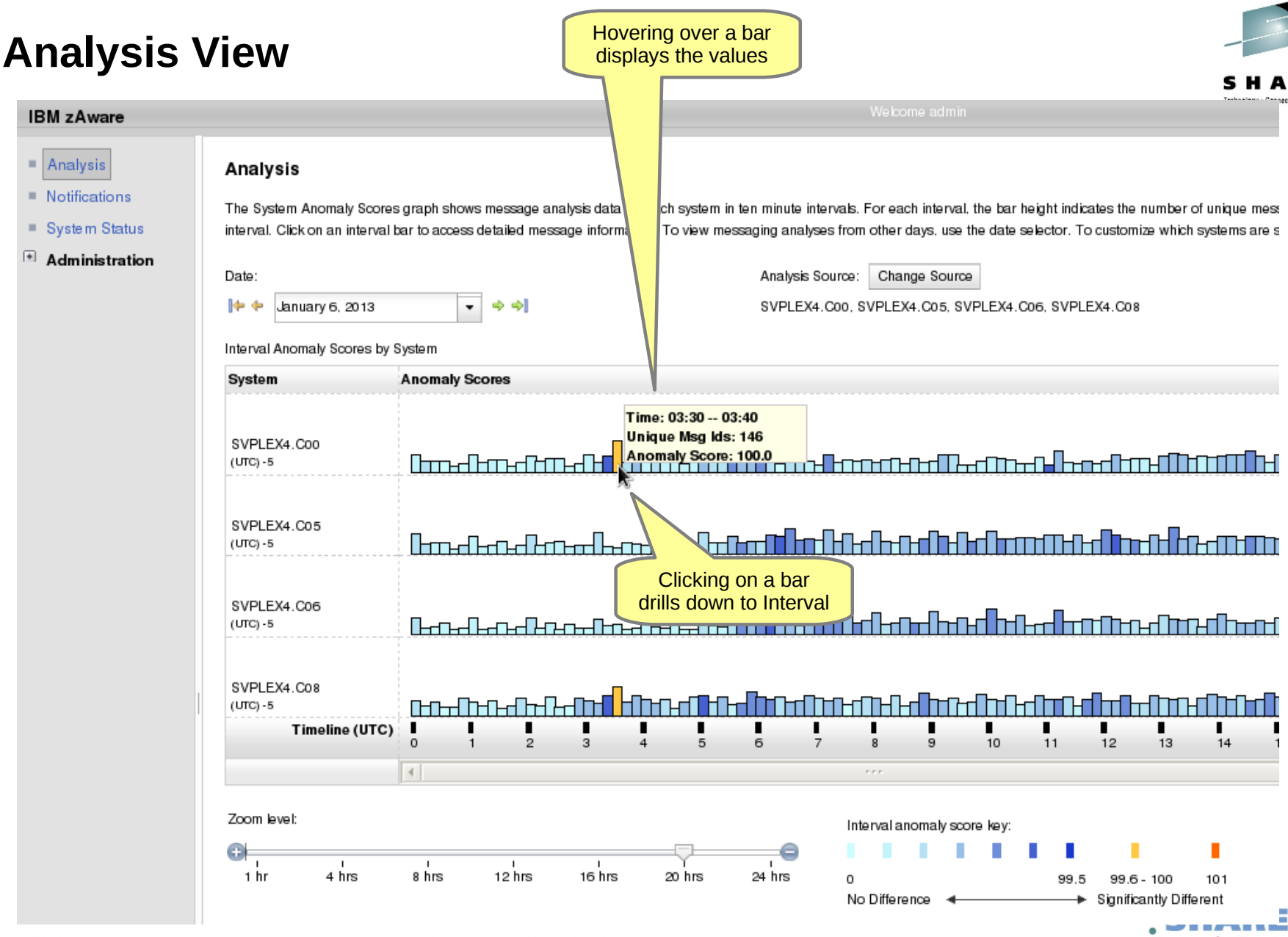
Inside IBM zAware Analytics

- 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

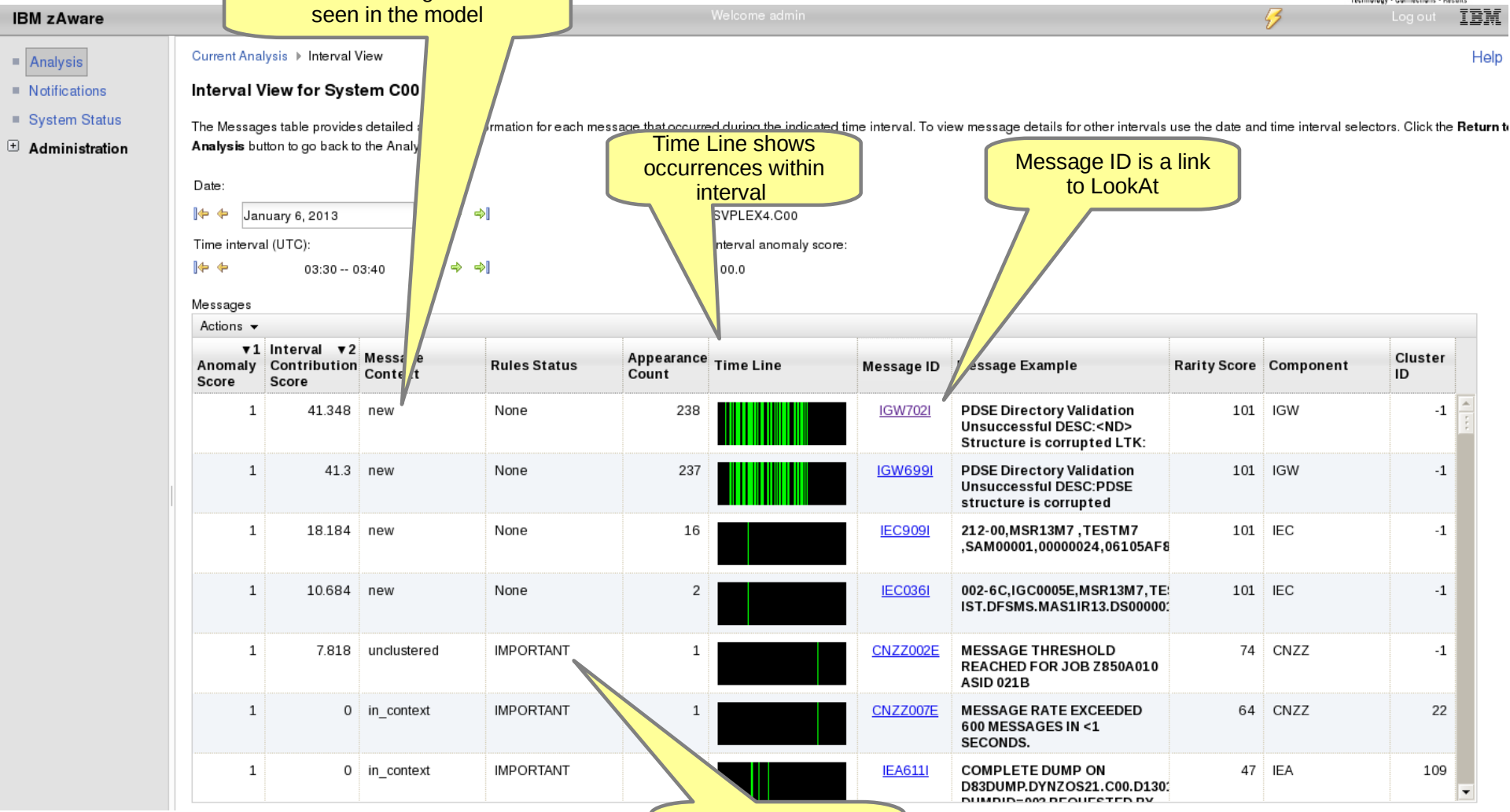
Analysis View



Analysis View



Interval View



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?

- Current 10 minute interval or earlier?
- Which messages are unusual?
- How often did the message occur?
- When did the messages start to occur?

Were similar messages issued previously

- Easily examine prior intervals or dates

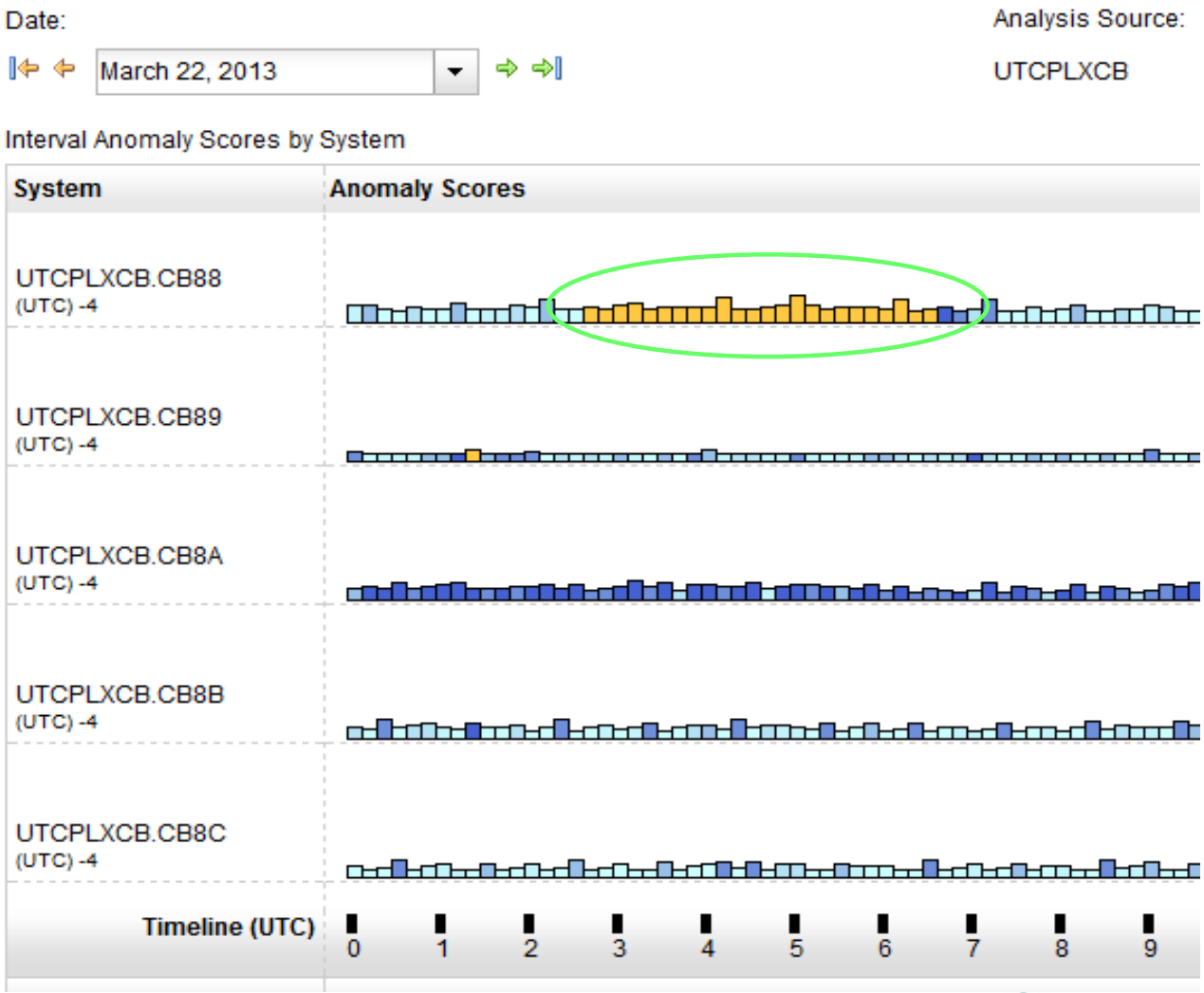
Identify unusual behavior quickly – example 1

Which z/OS image is having unusual message patterns?

- ***Yellow and dark blue on CB88***

When did the behavior start?

- ***Around 2:30***



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: March 22, 2013

Analysis Source: UTCPLXCB.CB88

Time interval (UTC): 02:40 -- 02:50

Interval anomaly score: 99.8

Messages

Actions

▼1 Anomaly Score	Interval ▼2 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		IRRC131I	(<) RACF ENCOUNTERED AN R_PROXYSERV ERROR WHILE ATTEMPTING TO CREATE AN	73	IRRC	-1
0.999	48.115	unclustered	None	932		IRRC144I	(<) RACF ENCOUNTERED AN R_PROXYSERV ERROR: SAF RETURN CODE=X'00000008',	85	IRRC	-1

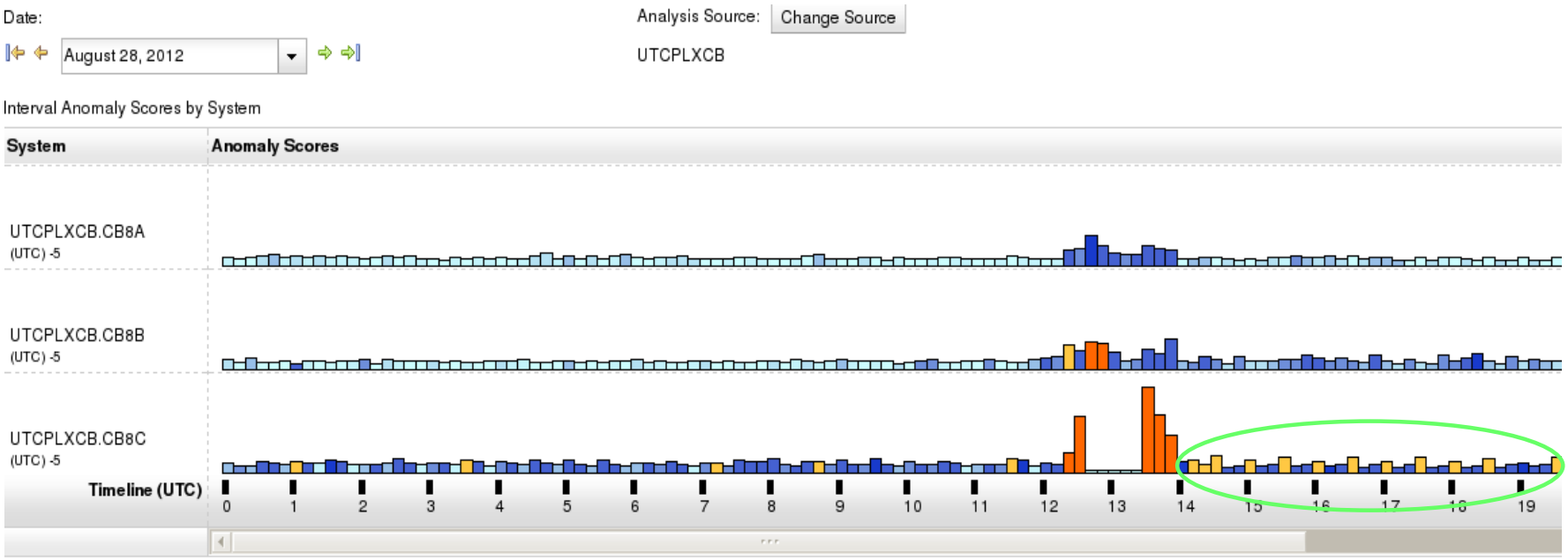
What component is having the problem?

- ***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 – example 2



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

Actions

▼1 Anomaly Score	Interval ▼2 Contribution Score	Message Context	Rules Status	Appearance Count	Time Line	Message ID	Message Example	Rarity Score	Componen
0.999	14.369	unclustered	None	2		IEE838I	TNPROC NON-CANCELABLE - ISSUE FORCE ARM	93	IEE
0.999	12.943	unclustered	None	2		EZZ0621I	AUTOLOG FORCING TNPROC, REASON: TCP/IP HAS BEEN RESTARTED	100	EZZ
0.999	9.41	unclustered	None	1		IXG601I	10.27.18 LOGGER DISPLAY 081 CONNECTION INFORMATION BY	62	IXG
0.997	6.078	unclustered	None	3		IEA631I	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?

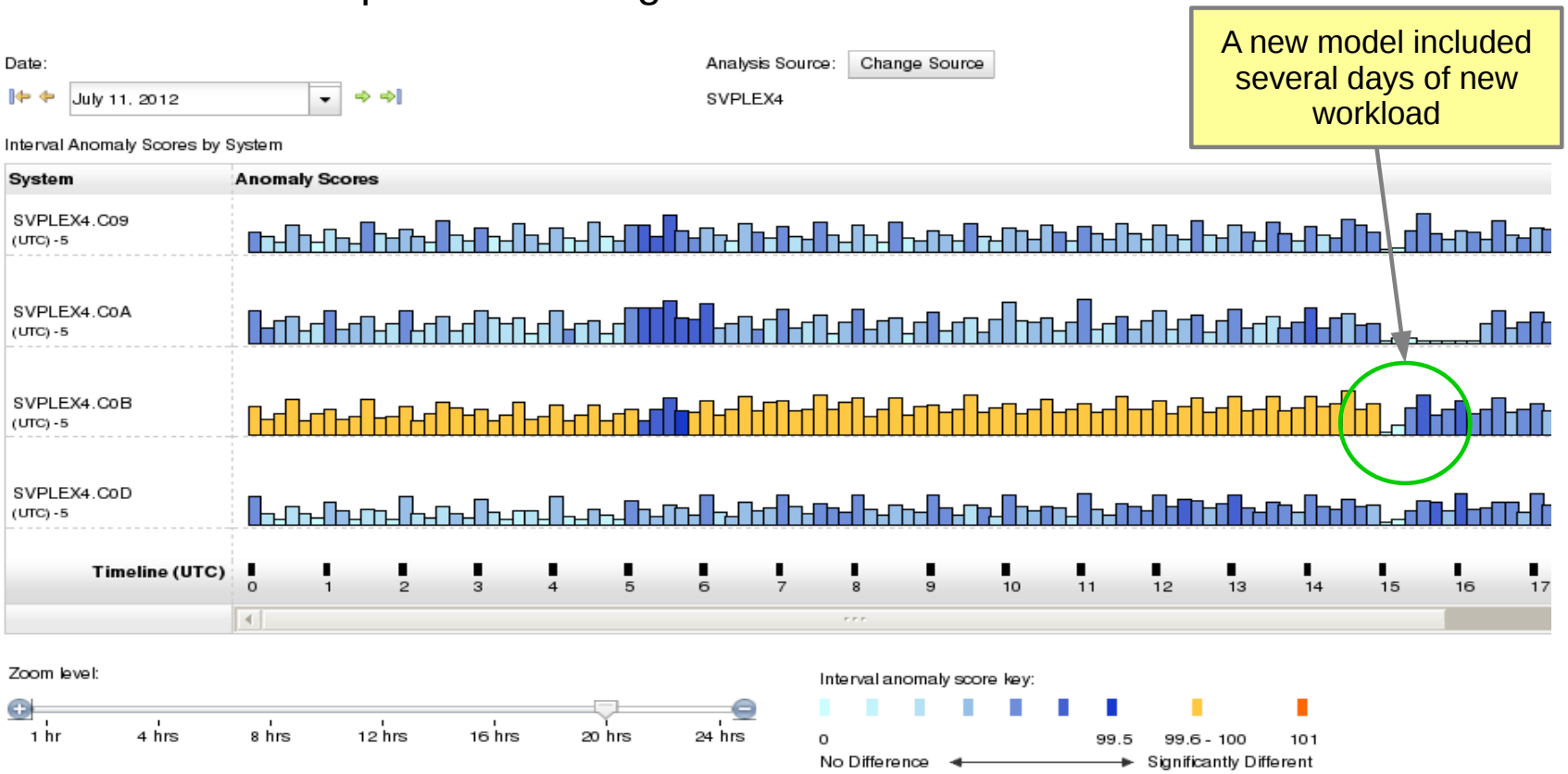
- Easily examine prior intervals or dates

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 software levels (operating system, middleware, applications)
- Updated system settings or system configurations
- Differentiate expected message traffic from side effects



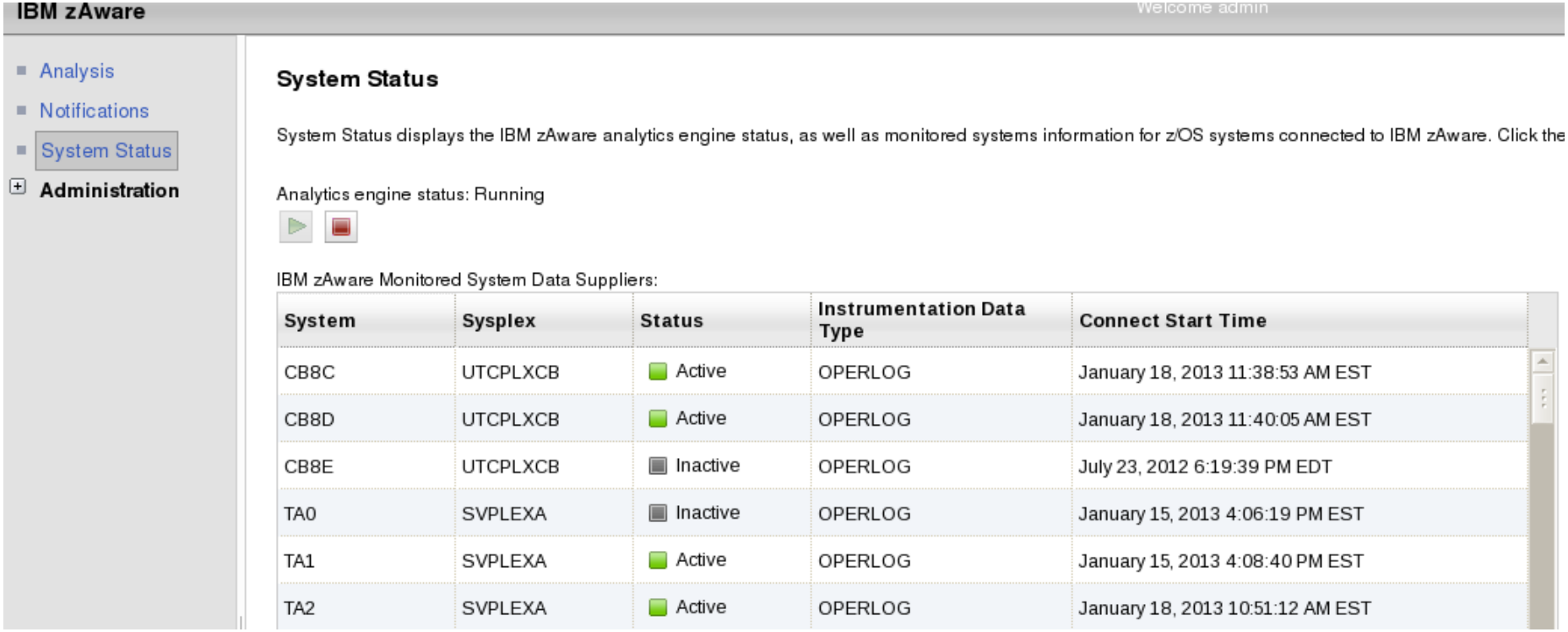
Diagnose Intermittent Problems

Are new unusual messages being issued when an intermittent problem occurs?

- Compare previous time periods
- Are more messages issued then expected?
- Are messages issued differently from the normal pattern?

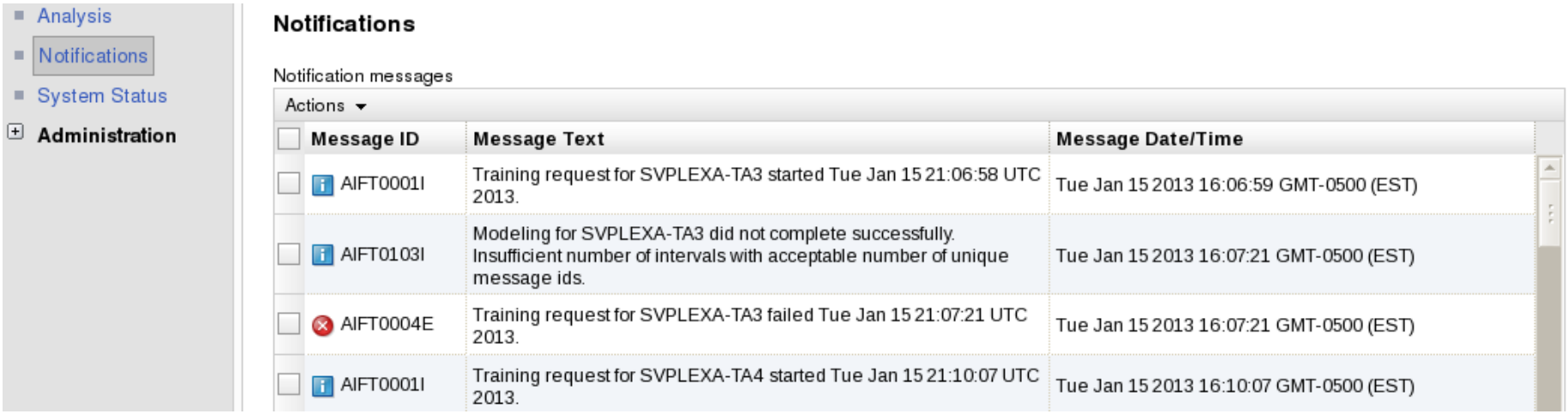
Connection Status

- *Which z/OS Monitored clients are connected?*



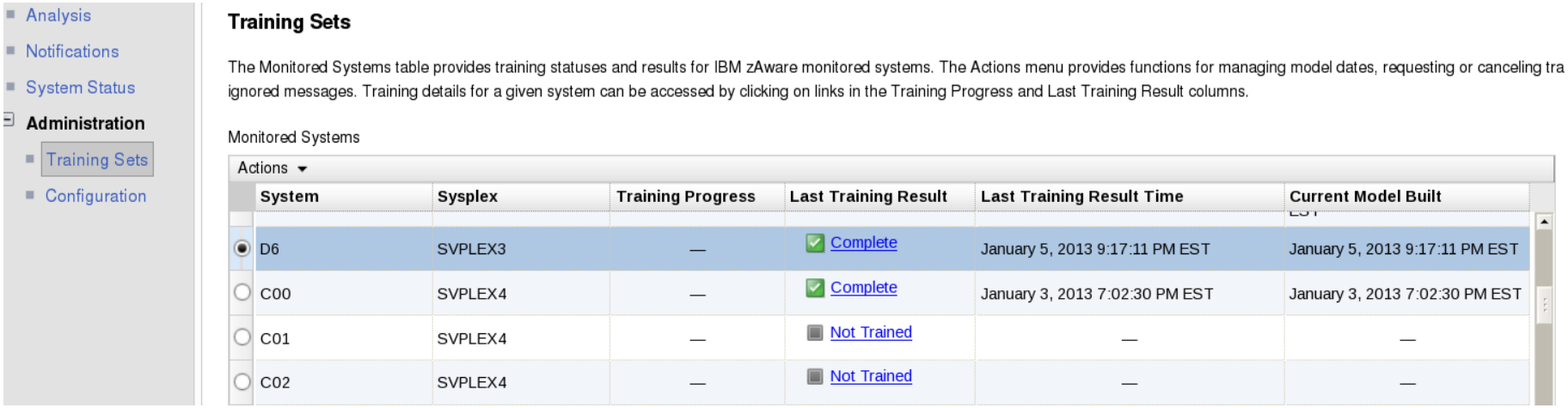
Notifications

- zAware messages for asynchronous events
  - Storage, Training, Bulk load, ...
- Viewable by all users
- Persistent, until removed by an admin
- New ones indicated by  in header



Training Sets

- Admins can view
  - Model training status
  - Dates included in the current model and next model
- Admins can take action
  - Request training
  - Exclude days from the next model



Operating Requirements – IBM zAware Server

- Logical partition on a **zEC12 or zBC12** server
  - Runs on **IFL**s or general purpose **CP**s – 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)
- Network resources
  - HiperSockets or shareable OSA ports or IEDN
  - IP address for partition
- Browsers
  - Internet Explorer 9
  - Firefox ESR 10

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%

New function available Sept 20 2013

Customer added domain knowledge – Ignore messages

- When a new workload is added to a system monitored by zAware
  - Generates messages that are not in the zAware model
  - Flagged as anomalous
    - *Orange bars on zAware Analysis*
    - *High anomaly scores on the Interval View*

Review of these messages is needed to improve the scoring

A) If a **real** problem is indicated, **fix the problem** on the monitored system
- Check subsequent zAware Analysis to confirm 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**
- *In subsequent analysis, the ignored messages will **not** contribute to the anomaly scores*
- *At the next training for this system, these messages will be built into the model, and removed from the system's ignored list*

Ignore messages continued

C) If you examine high scoring messages, and determine they are always **ok**

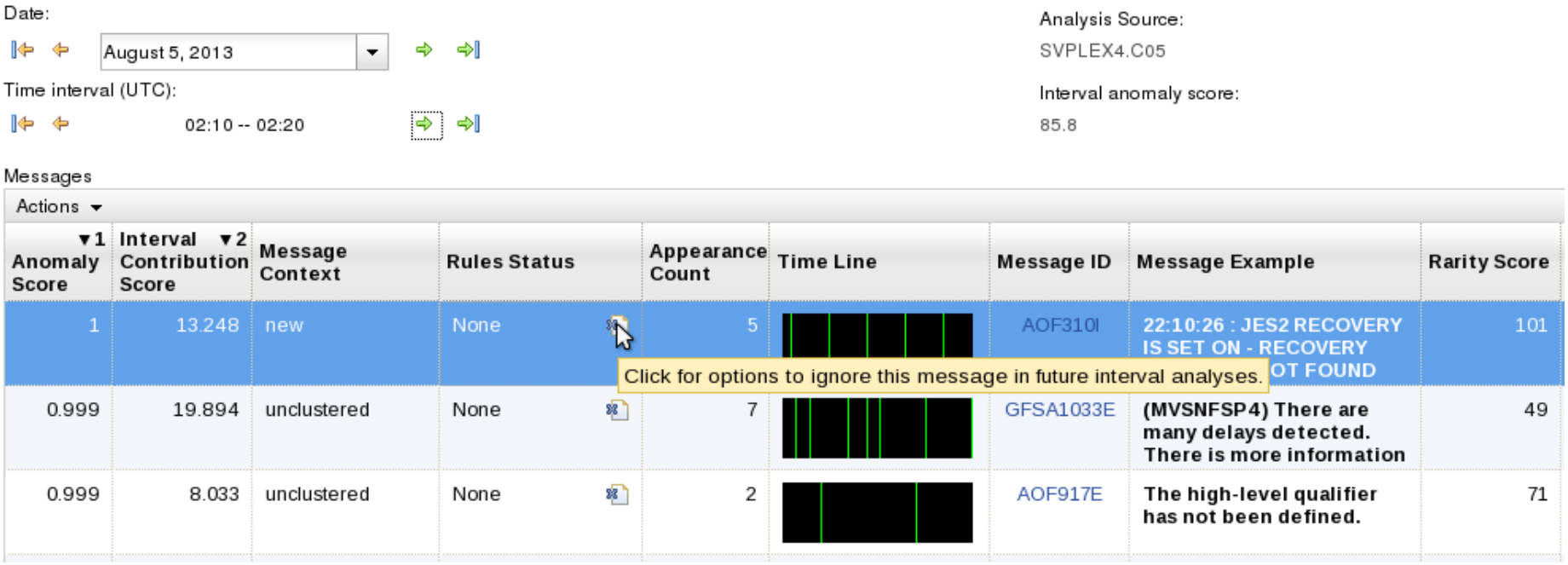
- Mark these as **Ignore until manually restored**
  - In subsequent analysis, the ignored messages will not contribute to the anomaly scores
  - This setting will **persist** after trainings
  - This **reduces false positives**, based on user input, so real problems are not masked

- This feature is the first phase in giving the user input into the IBM zAware rules.

Ignore messages continued
GUI selection

New

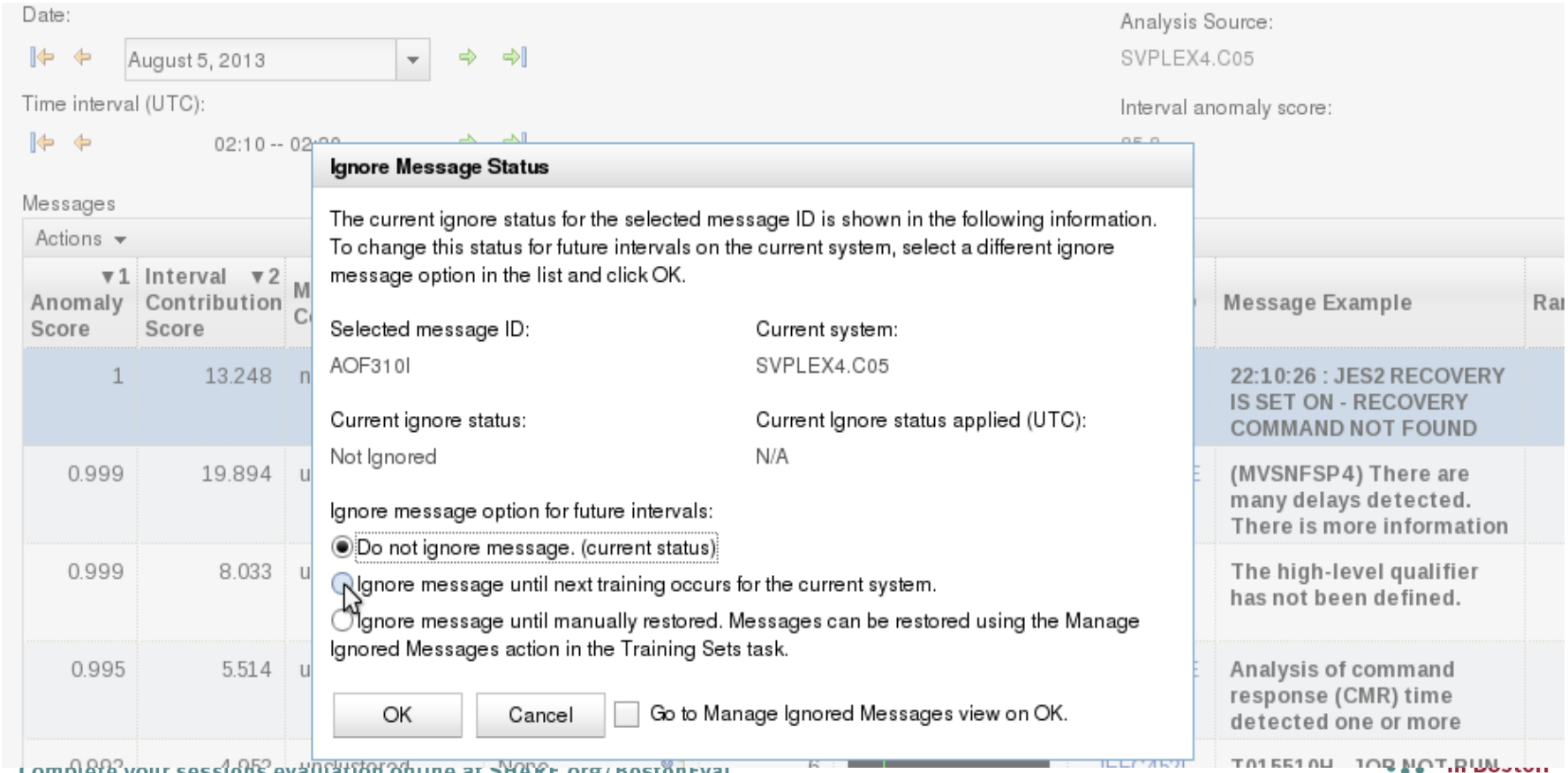
- From the Interval View
- When logged in as Admin
- When no IBM Rule (Rules Status is None)



Ignore messages continued
GUI selection

New

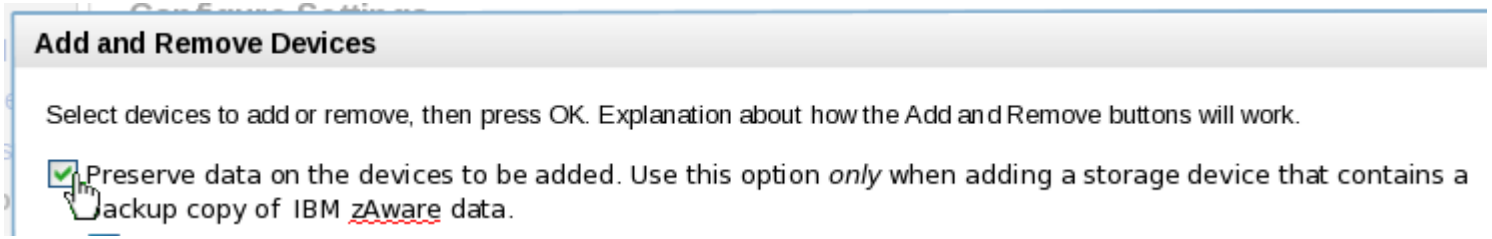
- Choose duration specific to this message, on this monitored system
- Takes effect on next analysis interval. Shows in Rules Status
- Lists available from Training Sets > Actions > Manage Ignored Messages



New function available Sept 20 2013
Alternate Data Storage Set

- Addition of DASD volumes without formatting
- Allow a backup copy of zAware data to be added after a failure.
  - DASD CU failure – Restore backup to zAware
  - Partition failure – Switchover to an alternate zAware with backed up copy of data

- Replication is not handled by zAware (Use IBM FlashCopy, DFSMS XRC, PPRC, …)
- Manage the primary devices and the backup devices as separate, but equivalent sets
  - Same number of devices, same sizes



Integration with other System Management products

- **z/OSMF**
  - 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

- **API**s
  - 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
  - Can use the APIs to get 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** and raise **alerts** on anomaly score.

- **Announced July 2013**, Tivoli Integrated Service Management products use of IBM zAware results.
  - Omegamon XE on z/OS (including predefined situations)

Session 14077: Improve Service Levels with Enhanced Data Analysis

Paul Smith Thurs, Aug 15 1:30 Room 200

- Other products can exploit the XML format results

Omegamon XE on z/OS – July 2013

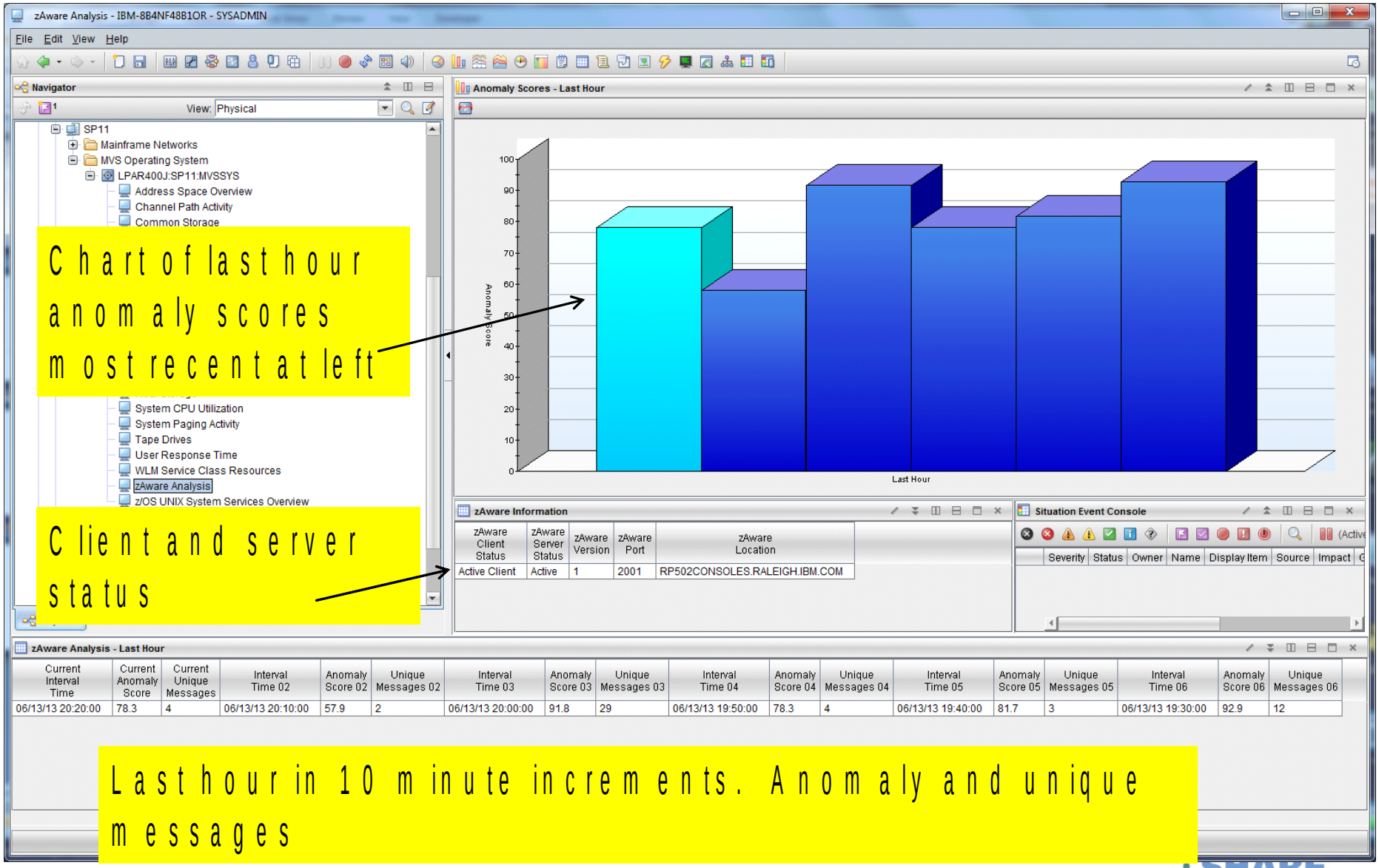
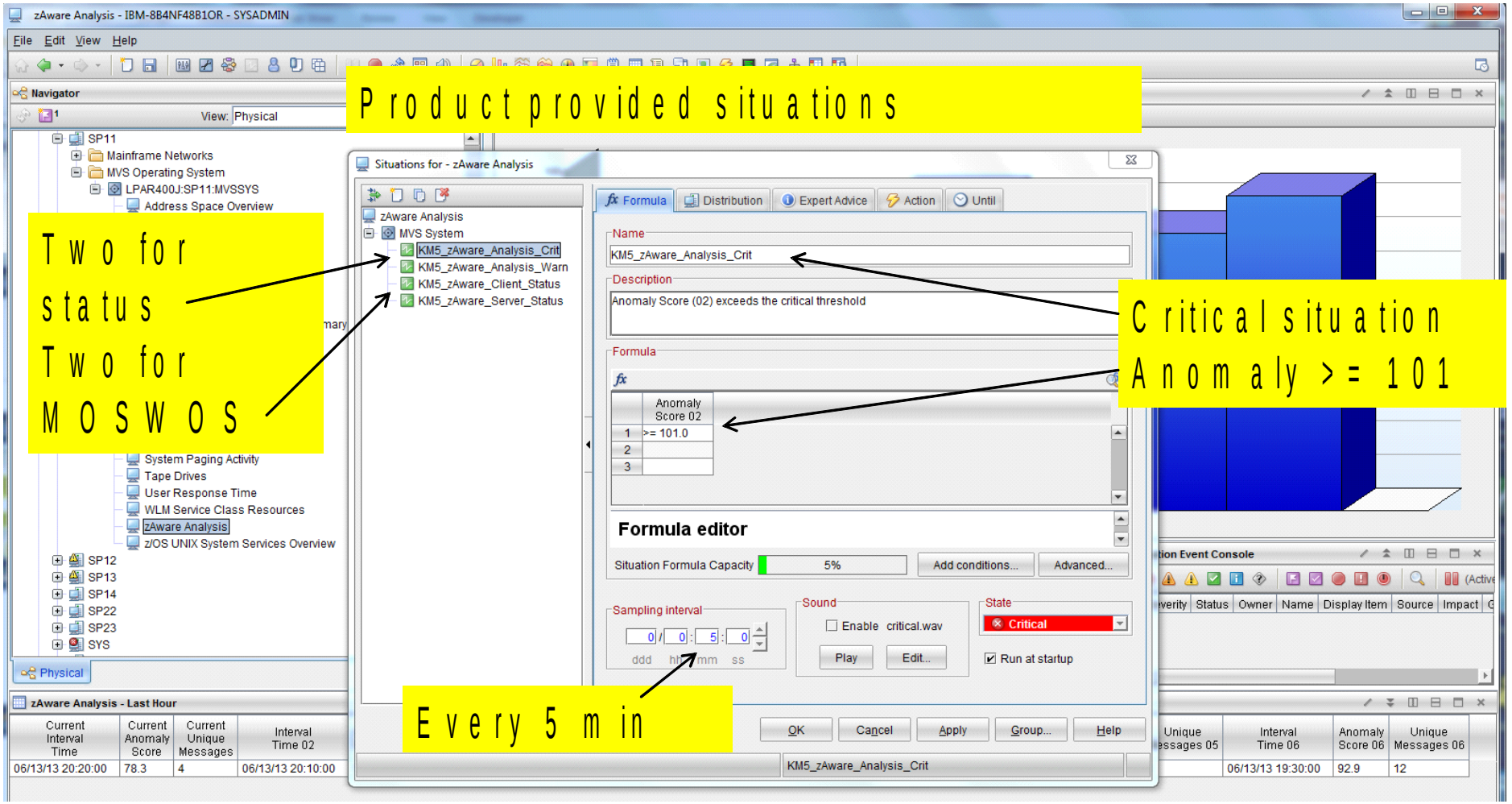


Chart of last hour anomaly scores most recent at left

Client and server status

Last hour in 10 minute increments. Anomaly and unique messages

Omegamon XE on z/OS – July 2013



Summary

You should now understand

- What IBM zAware is, and what can it detect
- How can it help identify problems on z/OS systems
- How can it help diagnose problems on z/OS systems
- Operating requirements
- Use of the IBM zAware GUI
- Integration with other management products

Questions?

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

- 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**
  - The Journey to IBM zAware
    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
  - Top 10 Most Frequently Asked Questions About IBM zAware
    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