IBM zAware – Even more aware now

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

Session 16707

#SHAREorg

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

SHARE in Seattle 2015

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

- Why IBM zAware?
- What is IBM zAware?
  - How does it identify and diagnose problems on your z/OS and Linux for z systems
- Using IBM zAware
- Operating requirements
- Integration with other management products

Background – Why IBM zAware

Systems are more complex and more integrated than ever

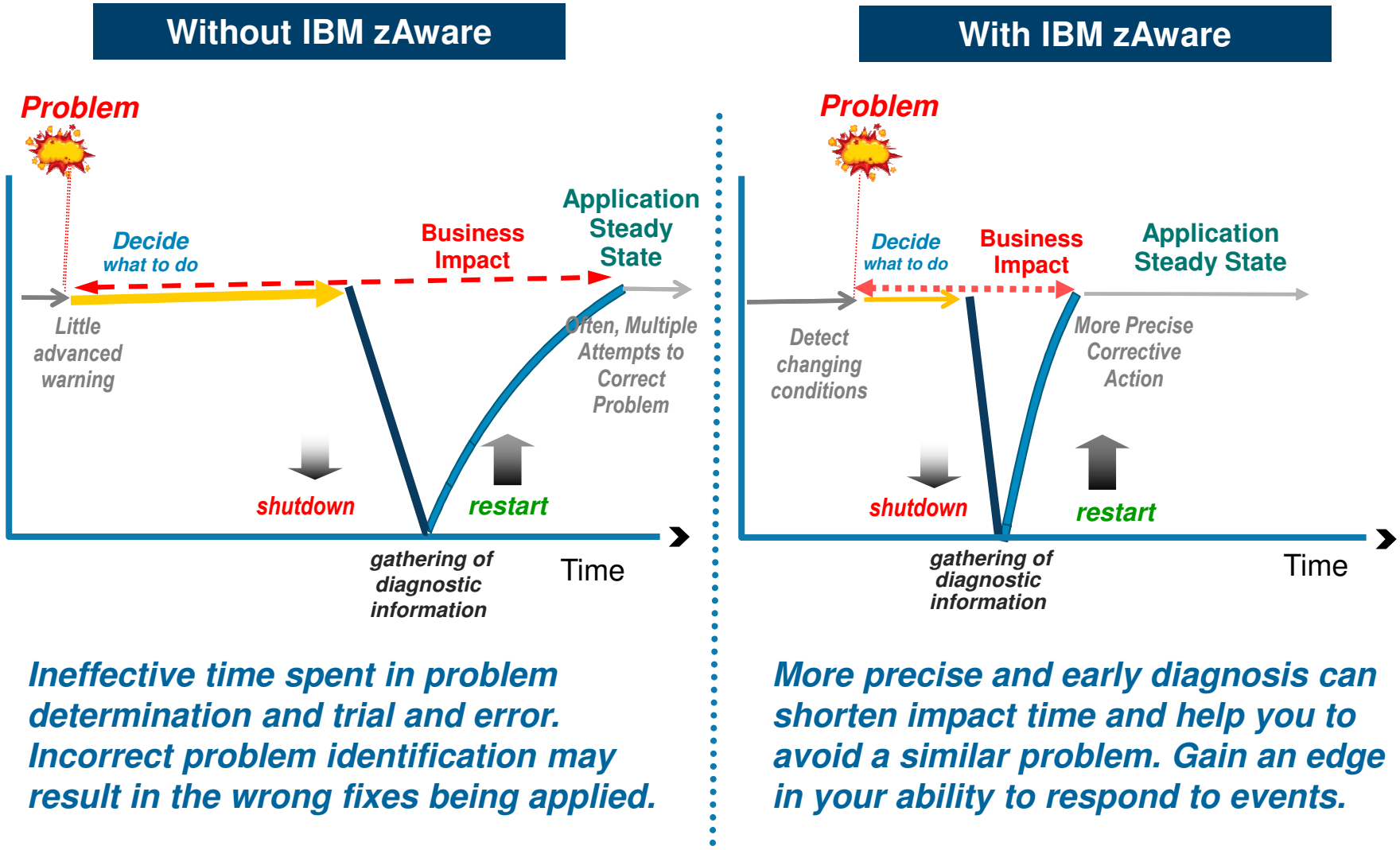
- *Errors can occur anywhere in a complex system*

- *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 timely information and insight*

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**
    - Improves problem diagnosis across a set of System z servers
- **Benefits**
  - Helps you diagnose problems quickly and more accurately to improve service recovery time
  - Particularly helpful when problems involve multiple teams
  - Easy to use graphical interface
  - Allow establishment of procedures to prevent reoccurrence

IBM zAware can reduce time to repair to improve availability



Ineffective time spent in problem determination and trial and error. Incorrect problem identification may result in the wrong fixes being applied.

More precise and early diagnosis can shorten impact time and help you to avoid a similar problem. Gain an edge in your ability to respond to events.

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?
- Easily examine prior intervals or dates

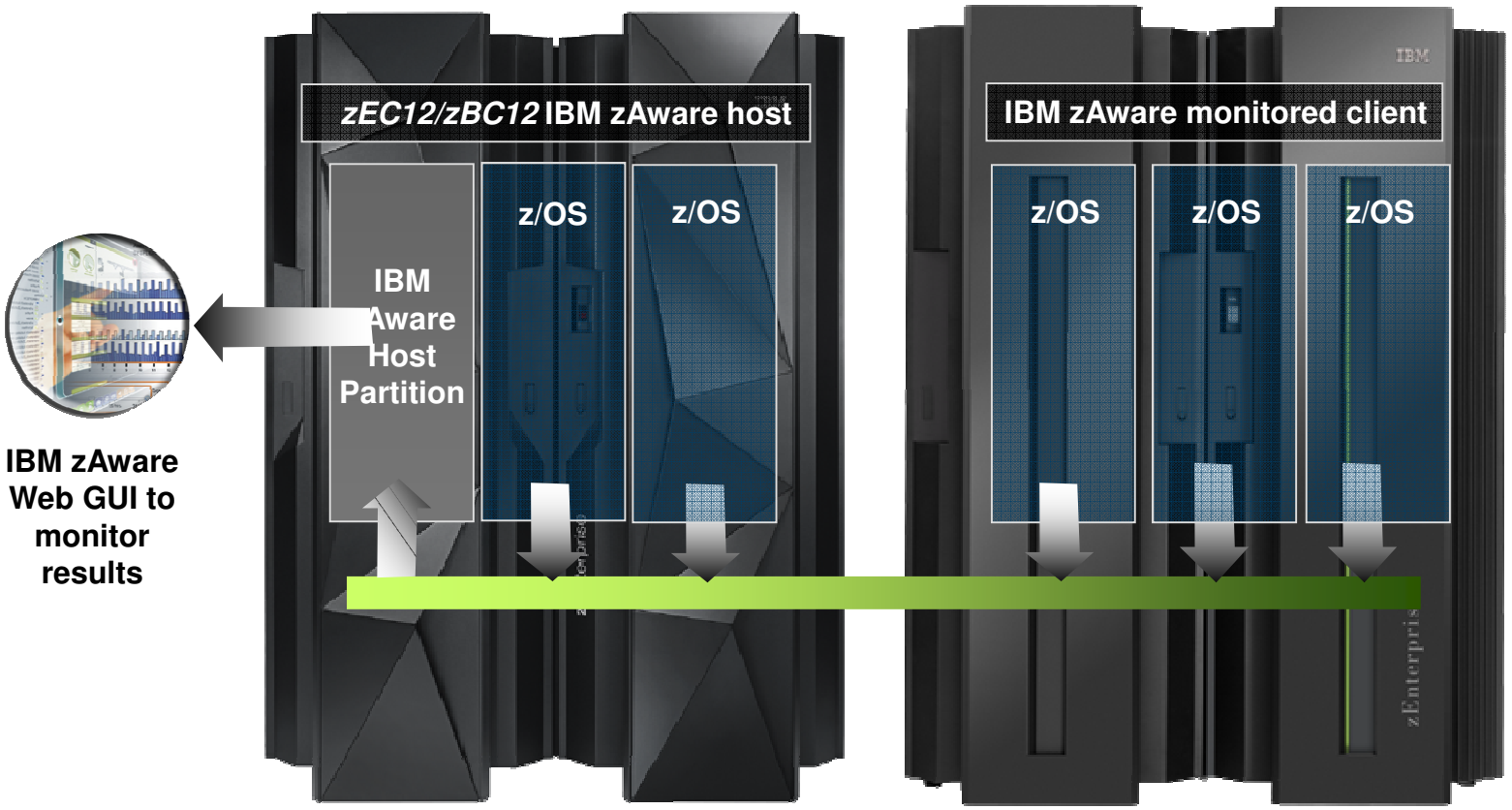
Is the unusual behavior after some maintenance or upgrade?

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

What is IBM zAware?

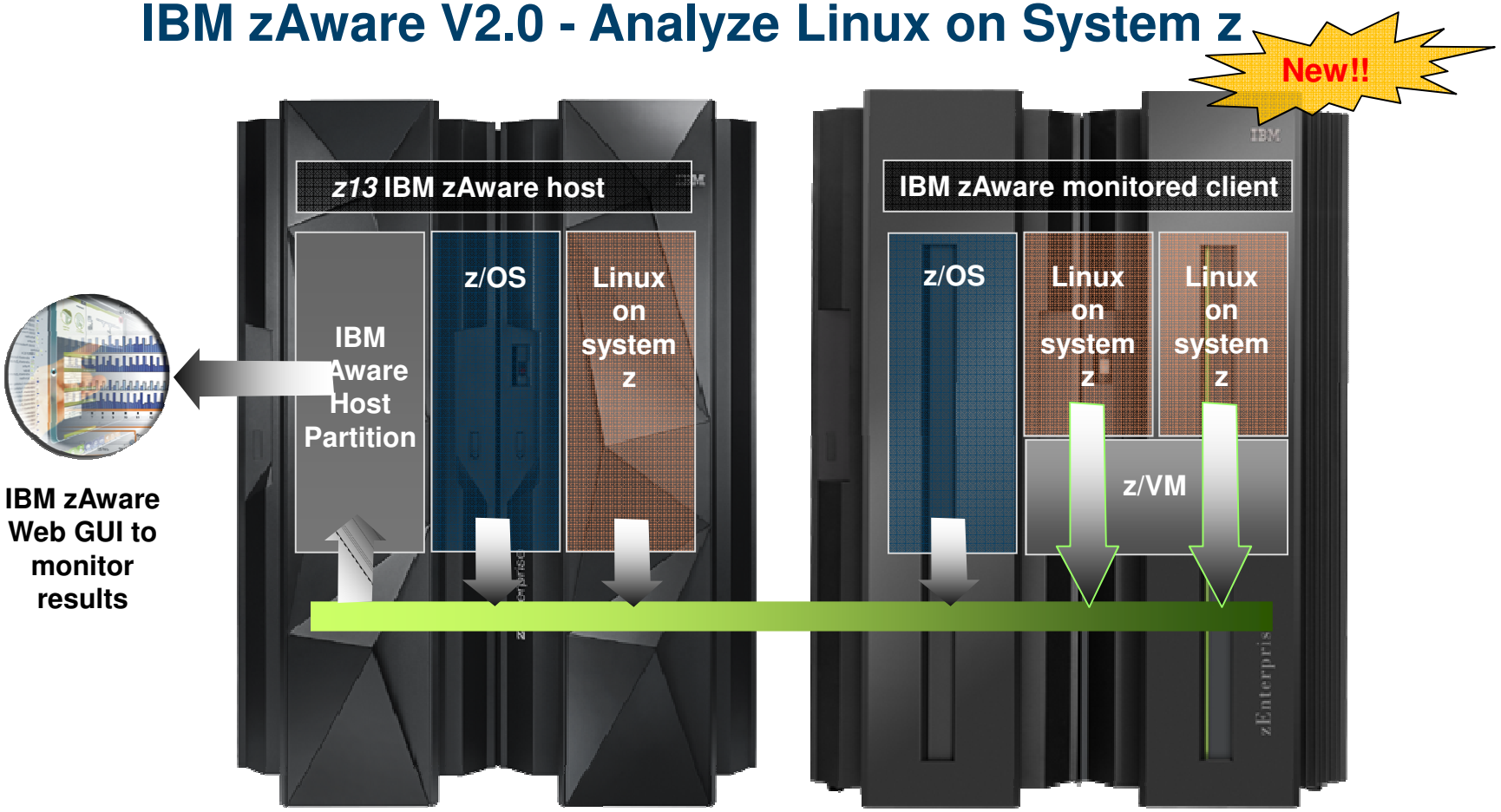
- IBM System z Advanced Workload Analysis Reporter (IBM zAware) V1 was released with the zEC12 in September 2012
- **Features**
  - Delivers cutting edge pattern recognition analytics applied to z/OS OPERLOG messages with minimal impact to z/OS workloads
    - Helps diagnose major problems while they are occurring in near real time
    - Heightens awareness of small problems before they become big problems
    - Reduces mean time to recovery
    - Reduces the time and skill required to diagnose a problem
  - A browser based view, which can show the entire z/OS footprint in one window

IBM zAware Version 1- Analyze z/OS System



- Identify unusual system behavior of zOS images
- Proactively surface anomalies in z/OS operlog

IBM zAware V2.0 - Analyze Linux on System z



- Identify unusual system behavior of Linux on system z images
  - Monitors ***syslog*** from guest or native image in real time
- Improved analytics for z/OS message logs
- Enhanced UI with heat map views

Analyzing z/OS systems

- A model of “what’s normal” is created for each system
- IBM zAware monitors and scores messages including all z/OS console messages, ISV and application generated messages
- Reports on 10 minute intervals
  - Current score is updated every 2 minutes
  - Uses a sliding 10 minute window to generate the current score
  - Uses 90 days baseline log data to build model by default (configurable)
- Detects anomalies monitoring systems miss:
  - Messages may be new, or in new patterns
  - Messages may be suppressed or rare
  - Messages may indicate a trend
  - Customer can specify message to be ignored – prevent flood of new messages from masking real problems
- XML Output is consumable through published API, can drive ISV products

Analyzing Linux for z systems

- A model of “what’s normal” is created for each system or group of systems
- IBM zAware monitors and scores messages all Linux for z syslog messages, including ISV and application generated messages
- Reports on 10 minute intervals
  - Current score is updated every 2 minutes
  - Uses a sliding 60 minute window to generate the score
  - Recommend 120 days baseline data to build model by default (configurable)
  - Early models may be built with lesser data
- XML Output is consumable through published API, can drive ISV products

Analyzing Linux for z systems - details

- For Linux on System z, multiple systems can be grouped into a combined ‘model group’
- This allows multiple systems with similar operational characteristics to contribute to the generation of a single model
- ‘Model groups’ defined by the zAware admin using hostname wildcards
  - Assumes well-defined Linux host naming conventions
  - Can model systems running similar types of workload (e.g. webserver, app servers)
    - By workload (e.g. one for all web servers, one for all databases, etc.)
    - By ‘solution’ (e.g. one model for your Cloud)
    - By VM host
- Dynamic activation and deactivation of an image, common on Linux, is automatically recognized
  - The Model Group support allows for analysis to be done for a system as soon as it connects to zAware, since it can use its group model

General V2.0 Enhancements

- Enhanced analytics
  - The new generation of technology provides improved analytics to provide better results.
  - New scorers including periodicity.
- Broader scope of input data to be analyzed
  - The previous version required messages with z/OS message id format
  - zAware can process message streams that do not have message ids
  - **This opens up new possibilities going forward**

Enhanced zAware GUI

- Improved usability and GUI functional enhancements address many customer requirements
  - enhanced filtering, visualization, better use of GUI real estate,
  - improved UI navigation
  - display local time in addition to UTC time
- New improved GUIs are based on IBM One UI guidelines
- Heat map display provides a high level consolidated view with ability to drill down to detail views
  - zOS grouped by sysplex, Linux grouped by model group
  - Scores presented at the hour level
  - Quickly get to all systems in a specific group
  - See the interval summaries per system with the Bar Score view
  - Detailed messages and scores in the Interval view
- Expanded browser support with Firefox ESR 24, 31 and IE 9,10,11

zAware enhanced GUI – Heatmap

New!

admin

Analysis

Date (UTC): February 17, 2015

Analysis Source: Change Source
All monitored groups

Interval Anomaly Scores

Actions | Zoom: 24 hrs | View: Heat Map Table | Filter

No filter applied

System Group	Type	24 Hour Peak	Peak Anomaly Score Per Hour																						
			0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
SVPLEX4	Sysplex	101.0	95.5	99.7	99.6	99.3	97.3	97.5	75.1	99.6	98.2	99.3	99.1	91.1	94.2	92.3	99.0	94.7	92.8	96.8	99.6	100.0	99.9	101.0	99.8	99.5
SVPLEX7	Sysplex	101.0	101.0	101.0	92.2	88.8	101.0		99.7	75.1	91.2	94.6	87.5	99.9	101.0	101.0	99.8	101.0	99.7	101.0	101.0	101.0	95.7	101.0	92.1	93.9
UTCPLXCB	Sysplex	101.0	80.4	83.7	98.2	98.2	99.4	99.0	98.7	99.3	99.3	99.6	99.3	99.3	98.0	101.0	98.4	97.3	88.6	81.1	94.7	90.7	84.3	97.1	95.8	95.6
SVPLEX1	Sysplex	100.0	99.5	100.0																			99.4	99.8	94.9	91.8
PLEX1	Sysplex	99.9	87.4	86.6	86.6	86.6	93.2	86.6	89.8	94.6	87.6	86.6	86.6	86.6	87.4	86.6	97.1	98.0	94.2	89.3	86.6	99.9	85.7	98.0	80.2	80.2
SVPLEX3	Sysplex	99.7													99.7	98.7	99.2	98.8	96.2	95.6	98.1	96.9	96.0	96.1	92.8	94.0
SVPLEX9	Sysplex	97.7	92.8	93.9	97.7	97.7	97.7	95.4	96.6	96.6	92.1	91.2	97.3	92.1	89.3	95.7	89.2	84.9	96.9	97.3	91.2	69.1	94.3	93.1	78.0	80.0
IGNORE	Sysplex																									
SVPLEX2	Sysplex																									
SVPLEX5	Sysplex																									
SVPLEXA	Sysplex																									
CSST	Model Group																									

Aggregated analysis score for group with ability to drill down

Total: 12

Heat Map – All systems in a group

New!

admin

Analysis

Date (UTC): February 17, 2015

Analysis Source: Change Source | Previous Group Selection

All systems in SVPLEX4

Interval Anomaly Scores

Actions | Zoom: 24 hrs | View: Heat Map Table | Filter

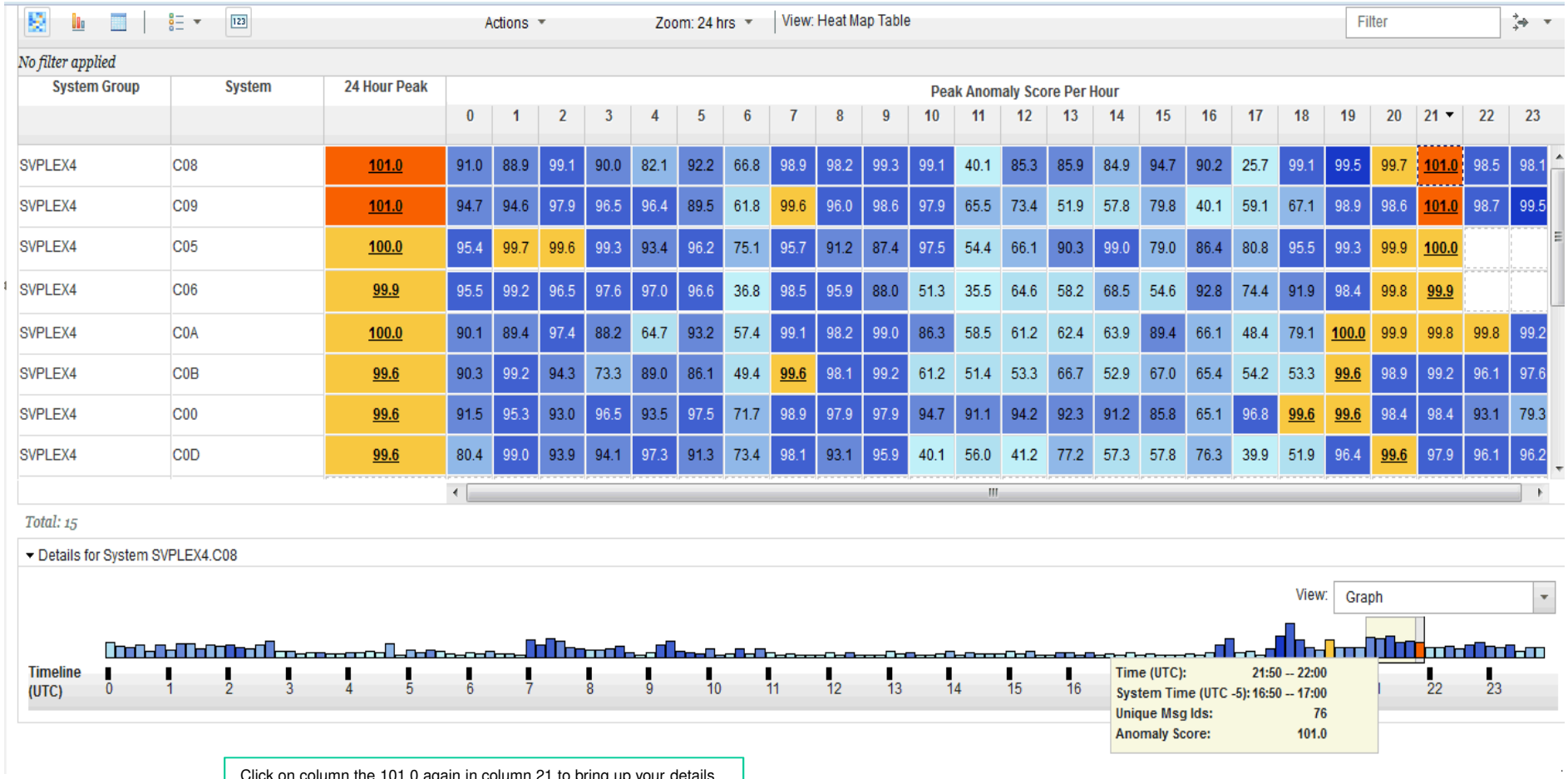
No filter applied

System Group	System	24 Hour Peak	Peak Anomaly Score Per Hour																						
			0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
SVPLEX4	C08	101.0	91.0	88.9	99.1	90.0	82.1	92.2	66.8	98.9	98.2	99.3	99.1	40.1	85.3	85.9	84.9	94.7	90.2	25.7	99.1	99.5	99.7	101.0	98.5	98.1
SVPLEX4	C09	101.0	94.7	94.6	97.9	96.5	96.4	89.5	61.8	99.6	96.0	98.6	97.9	65.5	73.4	51.9	57.8	79.8	40.1	59.1	67.1	98.9	98.6	101.0	98.7	99.5
SVPLEX4	C05	100.0	95.4	99.7	99.6	99.3	93.4	96.2	75.1	95.7	91.2	87.4	97.5	54.4	66.1	90.3	99.0	79.0	86.4	80.8	95.5	99.3	99.9	100.0		
SVPLEX4	C06	99.9	95.5	99.2	96.5	97.6	97.0	96.6	36.8	98.5	95.9	88.0	51.3	35.5	64.6	58.2	68.5	54.6	92.8	74.4	91.9	98.4	99.8	99.9		
SVPLEX4	C0A	100.0	90.1	89.4	97.4	88.2	64.7	93.2	57.4	99.1	98.2	99.0	86.3	58.5	61.2	62.4	63.9	89.4	66.1	48.4	79.1	100.0	99.9	99.8	99.8	99.2
SVPLEX4	C0B	99.6	90.3	99.2	94.3	73.3	89.0	86.1	49.4	99.6	98.1	99.2	61.2	51.4	53.3	66.7	52.9	67.0	65.4	54.2	53.3	99.6	98.9	99.2	96.1	97.6
SVPLEX4	C00	99.6	91.5	95.3	93.0	96.5	93.5	97.5	71.7	98.9	97.9	97.9	94.7	91.1	94.2	92.3	91.2	85.8	65.1	96.8	99.6	99.6	98.4	98.4	93.1	79.3
SVPLEX4	C0D	99.6	80.4	99.0	93.9	94.1	97.3	91.3	73.4	98.1	93.1	95.9	40.1	56.0	41.2	77.2	57.3	57.8	76.3	39.9	51.9	96.4	99.6	97.9	96.1	96.2
SVPLEX4	C01																									
SVPLEX4	C02																									
SVPLEX4	C03																									
SVPLEX4	C04																									

Drill down the heatmap into a particular sysplex SVPLEX4 with a high anomaly score by clicking on 101.0 in the 21st column. Now the view is drilled down and sorted by that column

Heat Map – All systems in a group w/drilldown

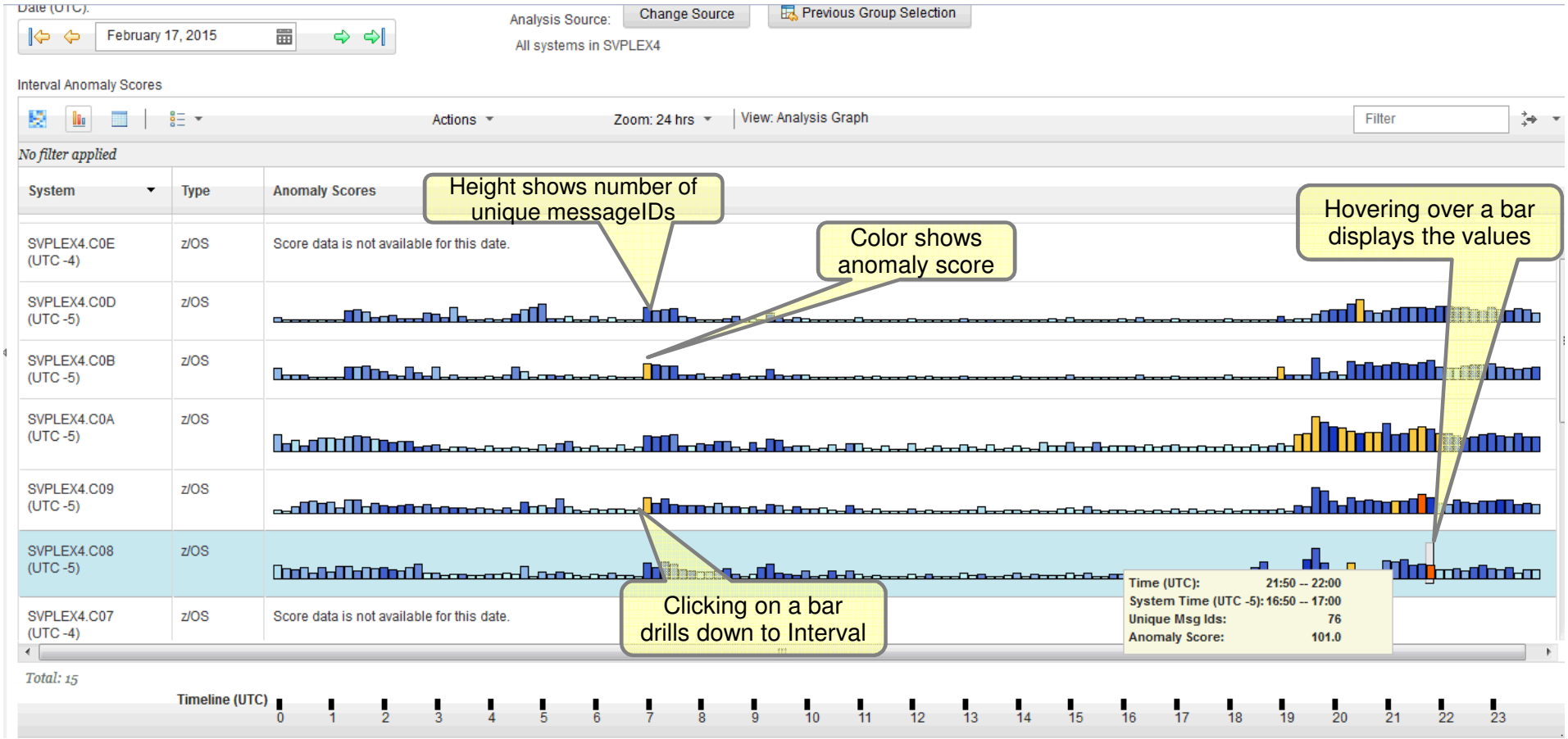
New!



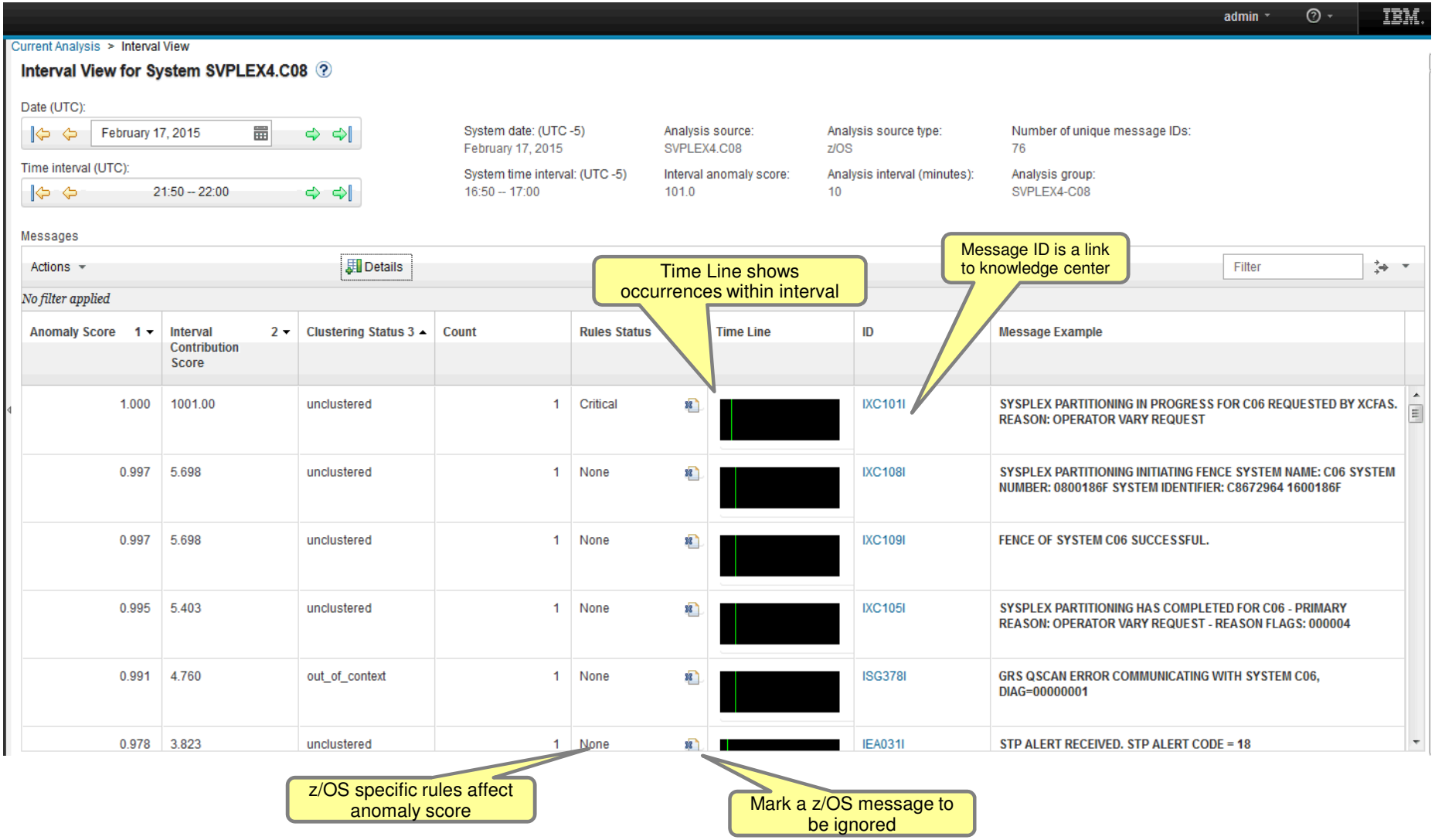
System Group	System	24 Hour Peak	Peak Anomaly Score Per Hour																						
			0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
SVPLEX4	C08	101.0	91.0	88.9	99.1	90.0	82.1	92.2	66.8	98.9	98.2	99.3	99.1	40.1	85.3	85.9	84.9	94.7	90.2	25.7	99.1	99.5	99.7	101.0	98.5	98.1
SVPLEX4	C09	101.0	94.7	94.6	97.9	96.5	96.4	89.5	61.8	99.6	96.0	98.6	97.9	65.5	73.4	51.9	57.8	79.8	40.1	59.1	67.1	98.9	98.6	101.0	98.7	99.5
SVPLEX4	C05	100.0	95.4	99.7	99.6	99.3	93.4	96.2	75.1	95.7	91.2	87.4	97.5	54.4	66.1	90.3	99.0	79.0	86.4	80.8	95.5	99.3	99.9	100.0		
SVPLEX4	C06	99.9	95.5	99.2	96.5	97.6	97.0	96.6	36.8	98.5	95.9	88.0	51.3	35.5	64.6	58.2	68.5	54.6	92.8	74.4	91.9	98.4	99.8	99.9		
SVPLEX4	C0A	100.0	90.1	89.4	97.4	88.2	64.7	93.2	57.4	99.1	98.2	99.0	86.3	58.5	61.2	62.4	63.9	89.4	66.1	48.4	79.1	100.0	99.9	99.8	99.8	99.2
SVPLEX4	C0B	99.6	90.3	99.2	94.3	73.3	89.0	86.1	49.4	99.6	98.1	99.2	61.2	51.4	53.3	66.7	52.9	67.0	65.4	54.2	53.3	99.6	98.9	99.2	96.1	97.6
SVPLEX4	C00	99.6	91.5	95.3	93.0	96.5	93.5	97.5	71.7	98.9	97.9	97.9	94.7	91.1	94.2	92.3	91.2	85.8	65.1	96.8	99.6	99.6	98.4	98.4	93.1	79.3
SVPLEX4	C0D	99.6	80.4	99.0	93.9	94.1	97.3	91.3	73.4	98.1	93.1	95.9	40.1	56.0	41.2	77.2	57.3	57.8	76.3	39.9	51.9	96.4	99.6	97.9	96.1	96.2

Click on column the 101.0 again in column 21 to bring up your details pane at the bottom with the timeline for that hour highlighted.
Hover over an interval for details

Bar Score view with interval summaries

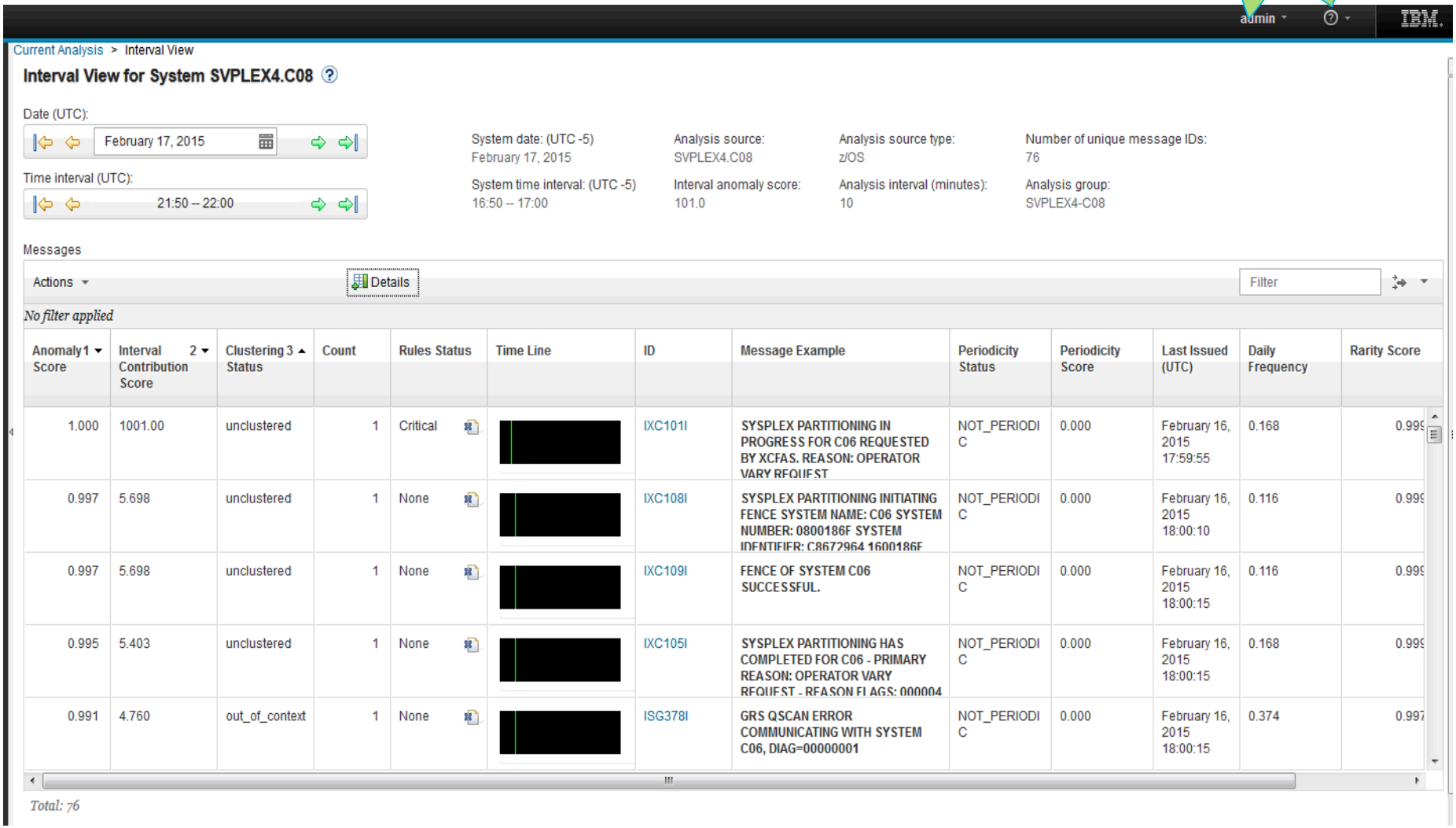


Interval View



Interval View with details

Enhanced!



admin

Current Analysis > Interval View

Interval View for System SVPLEX4.C08

Date (UTC): February 17, 2015

Time interval (UTC): 21:50 -- 22:00

System date: (UTC -5) February 17, 2015

Analysis source: SVPLEX4.C08

Analysis source type: z/OS

Number of unique message IDs: 76

System time interval: (UTC -5) 16:50 -- 17:00

Interval anomaly score: 101.0

Analysis interval (minutes): 10

Analysis group: SVPLEX4-C08

Messages

Actions | Details | Filter

No filter applied

Anomaly 1 Score	Interval 2 Contribution Score	Clustering 3 Status	Count	Rules Status	Time Line	ID	Message Example	Periodicity Status	Periodicity Score	Last Issued (UTC)	Daily Frequency	Rarity Score
1.000	1001.00	unclustered	1	Critical		IXC101I	SYSPLEX PARTITIONING IN PROGRESS FOR C06 REQUESTED BY XCFAS. REASON: OPERATOR VARY REQUEST	NOT_PERIODIC	0.000	February 16, 2015 17:59:55	0.168	0.999
0.997	5.698	unclustered	1	None		IXC108I	SYSPLEX PARTITIONING INITIATING FENCE SYSTEM NAME: C06 SYSTEM NUMBER: 0800186F SYSTEM IDENTIFIER: C8672964 1600186F	NOT_PERIODIC	0.000	February 16, 2015 18:00:10	0.116	0.999
0.997	5.698	unclustered	1	None		IXC109I	FENCE OF SYSTEM C06 SUCCESSFUL.	NOT_PERIODIC	0.000	February 16, 2015 18:00:15	0.116	0.999
0.995	5.403	unclustered	1	None		IXC105I	SYSPLEX PARTITIONING HAS COMPLETED FOR C06 - PRIMARY REASON: OPERATOR VARY REQUEST - REASON FLAGS: 000004	NOT_PERIODIC	0.000	February 16, 2015 18:00:15	0.168	0.999
0.991	4.760	out_of_context	1	None		ISG378I	GRS QSCAN ERROR COMMUNICATING WITH SYSTEM C06, DIAG=00000001	NOT_PERIODIC	0.000	February 16, 2015 18:00:15	0.374	0.997

Total: 76

Inside IBM zAware Analytics -- *Modeling*

- OPERLOG (z/OS) or syslog (Linux for z) is processed
- zAware recognizes any well-formed message IDs for z/OS
  - recognizes similar message text and generates a message ID for Linux for z,
  - 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 recent baseline data
  - Called “Training”
  - Automatically trains every 30 days (configurable)
  - Training can be forced manually
  - Training period is configurable
  - Unusual days can be excluded from future models
  - For z/OS,
    - Each system has its own model
    - Messages can be excluded from analysis scoring
  - For Linux for z,
    - Systems are grouped into a combined model
- z/OS utility, or a Linux command, may be used to load historical logs into zAware

Inside IBM zAware Analytics -- *Analysis*

- Real-time log data from each system 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
  - Periodicity
- Uses z/OS knowledge to influence the z/OS scores
- Generates an **interval anomaly** score bar per 10 minute interval
  - z/OS based on last 10 minutes
  - Linux for z based on last 60 minutes
  - 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

Sample Use cases

- ***A client compared it to an Airbag in the car – it reacts when something is wrong;***
- *It learns as time progresses, situations happen and identifies things we know would not have been identified by normal monitoring products - Allows to fix before it becomes a real problem;*

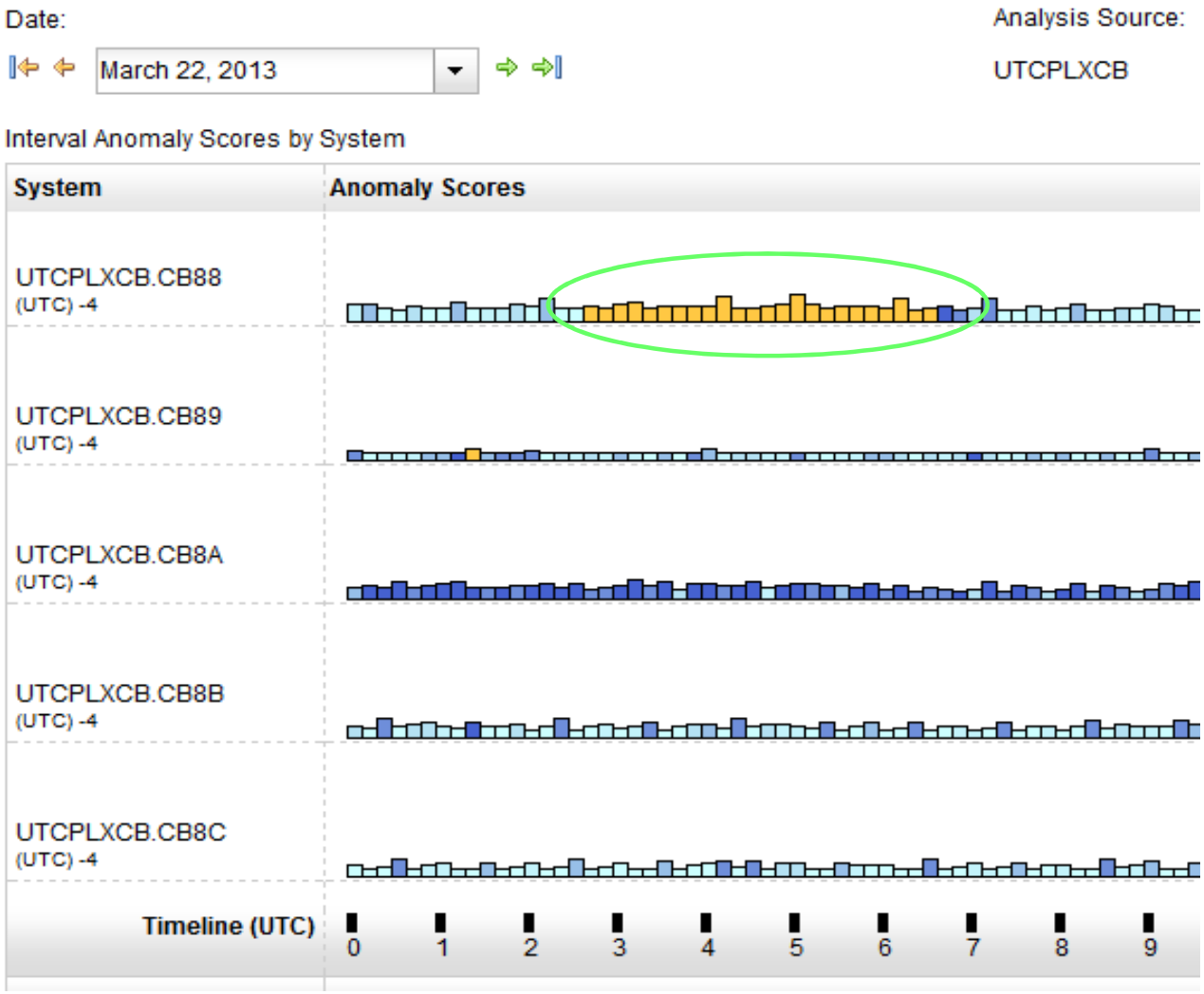
Identify unusual behavior quickly

Which z/OS image is having unusual message patterns?

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

When did the behavior start?

- ***Around 2:30***



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

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

Analysis Source: UTCPLXCB.CB88

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.***

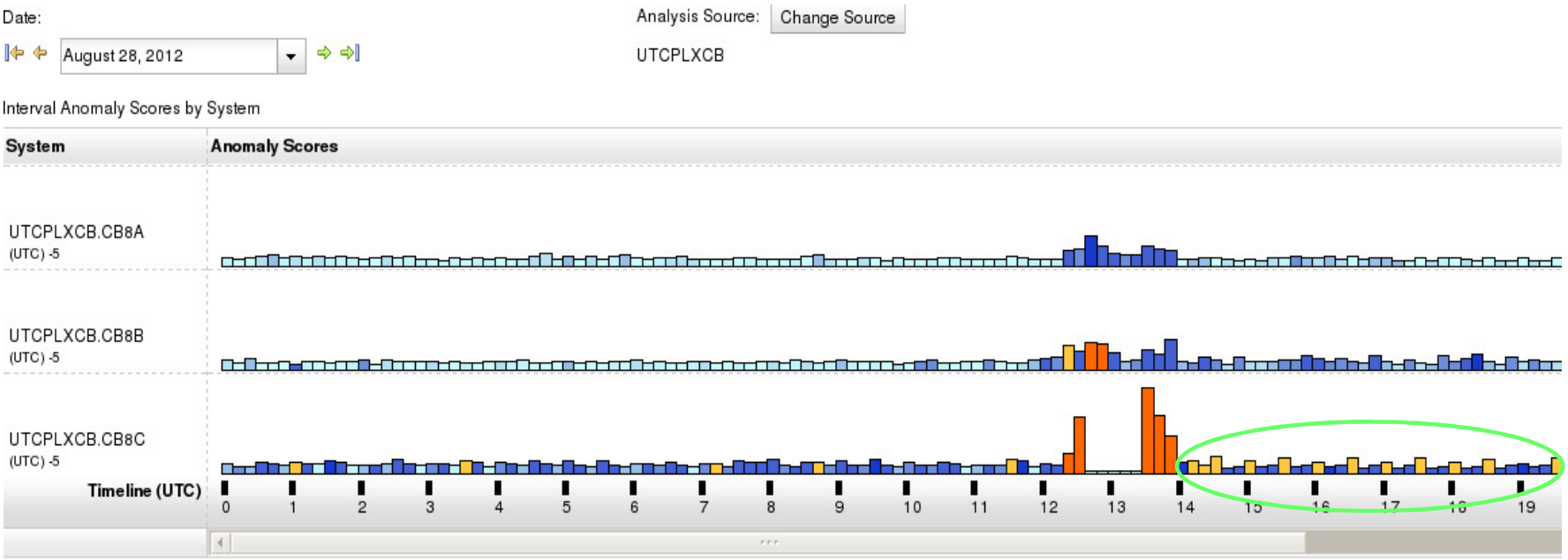
Impact

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

When did the behavior start?

- ***Around 2:30***

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

Time interval (UTC): 14:20 -- 14:30

Analysis Source: UTCPLXCB.CB8C

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 / 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.”

IBM zAware
Operating Requirements

Operating Requirements – **IBM zAware Server**

- Logical partition on a **zEC12 or zBC12** server or **z13** (soon)
  - 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) **+ 5GB per client**
- Network resources
  - HiperSockets or shareable OSA ports or IEDN
  - IP address for partition
- Browsers
  - Internet Explorer 9, 10, 11
  - Firefox ESR 24, 31

Operating Requirements – **z/OS Monitored Clients**

- System z servers supported as IBM zAware monitored clients
  - z13
  - 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%

Linux for System z Setup

Monitoring Linux on System z ‘syslog’ data

- Where ‘syslog’ is well-known, standardized, UNIX syslog data (e.g. /var/log/messages), from Linux on System z
  - Note this data is different than z/OS SYSLOG
  - Note this does not include zVM hypervisor data.
- Uses existing syslog daemon interface to send data to IBM zAware
  - Configuration of syslog daemon is required for Linux on system z images
  - Linux syslog daemon (rsyslog, syslog-ng) configured to send RFC 5424 format
- No Linux client / agent software is needed
- Each Linux for System z system connects to IBM zAware, without a syslog relay

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

- **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
      - **Analysis** ***Analysis data generated***
      - **INTERVAL** *Message scores for a 10-minute interval*
      - **LPAR** *Interval scores for date (deprecated, replaced by analysis)*

Note: API compatible with existing callers (z/OS); V2 required for Linux. Adds new attributes.

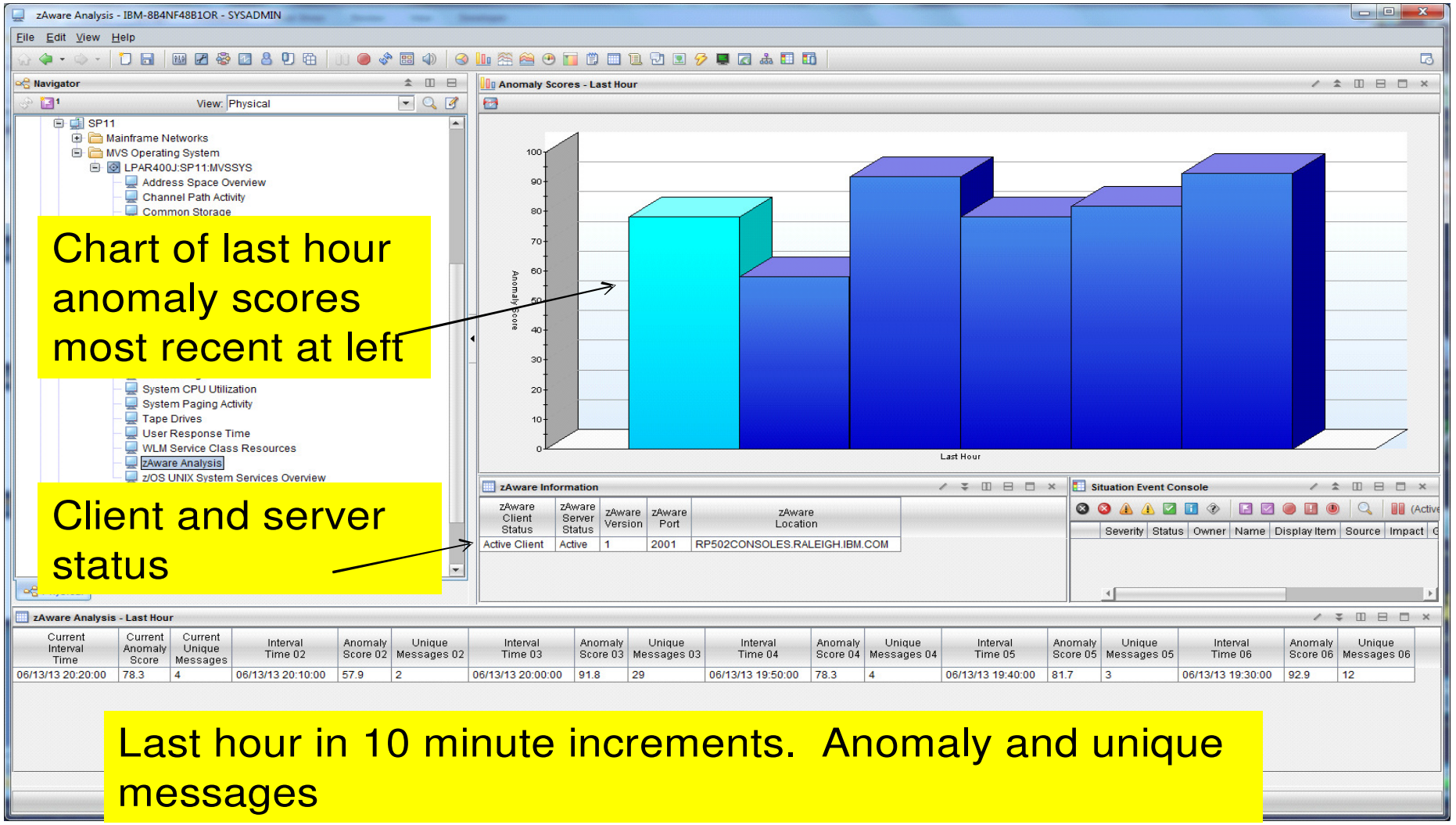
Integration with other System Management products

- 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

- 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

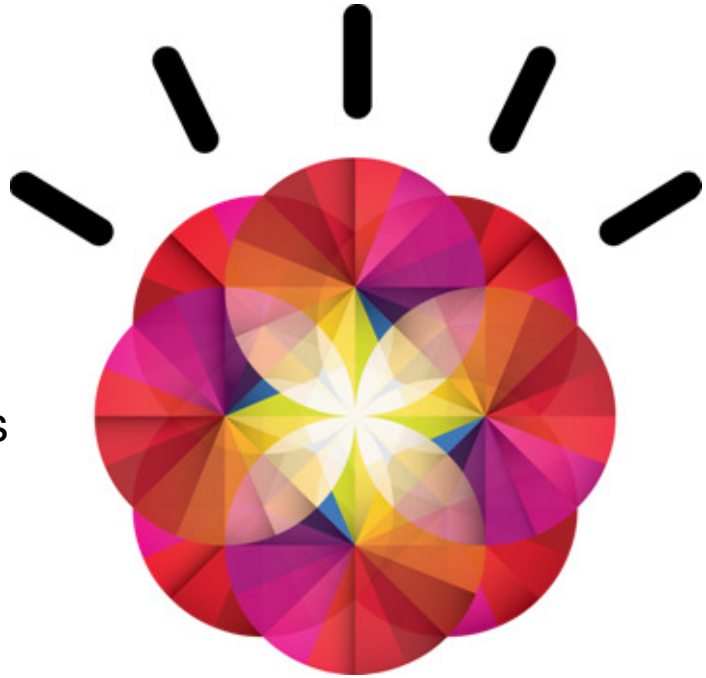


Summary
IBM zAware – Smarter Computing Needs Smart Monitoring

IBM zAware is a self learning, integrated solution that analyzes messages in near real time to provide insight into the behavior of your system.

Benefits

- Helps diagnose problems quickly and more accurately to **improve service recovery time**
- **Reduces risk** by identifying "what changed" after maintenance.
- Helpful when problems involve multiple teams
- Easy-to-use graphical interface
- Integrates with existing alerting environment



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

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**
  - 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

धन्यवाद
Hindi

多謝
Traditional Chinese

ขอบคุณ
Thai

Спасибо
Russian

Gracias
Spanish

Thank You
English

شكرا
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