Tivoli and IBM zAware:

Save money from enhanced analytics with Tivoli support for IBM zAware

Tivoli Telecon
January 24, 2013

Paul Smith (Smitty)
paulmsm@us.ibm.com

Agenda

- Why do we need IBM zAware?
- What is IBM zAware?
- IBM zAware complements your existing environment
- IBM zAware and Tivoli
  - Event Management
  - Automation
  - Problem Determination and MTTR
  - Traditional Performance Monitoring
  - Monitoring the IBM zAware environment

Excerpt from the IBM EC12 Announce letter

IBM zAware: With IBM zEnterprise EC12 (zEC12), IBM introduces a new technology, IBM zAware, based on machine learning developed by IBM Research. IBM zAware is designed to use near real-time continuous learning algorithms, providing a diagnostics capability intended to help you quickly pinpoint problems, which in turn, can help you to more rapidly address service disruptions. IBM zAware uses analytics to intelligently examine z/OS messages to find unusual patterns, inconsistencies, and variations.

Large z/OS operating system environments can sometimes generate more than 25 million messages per day. This can make manual analysis time-consuming and error-prone when exceptional problems occur. IBM zAware uses machine learning to help your organization gain visibility into system behavior, helping you to optimize service, respond to problems quicker, and increase availability.

IBM plans to provide **new capability within the Tivoli Integrated Service Management family of products** designed to leverage analytics information from IBM zAware, and to provide alert and event notification.

IBM zAware

Some Background

Systems are more complex and more integrated than ever

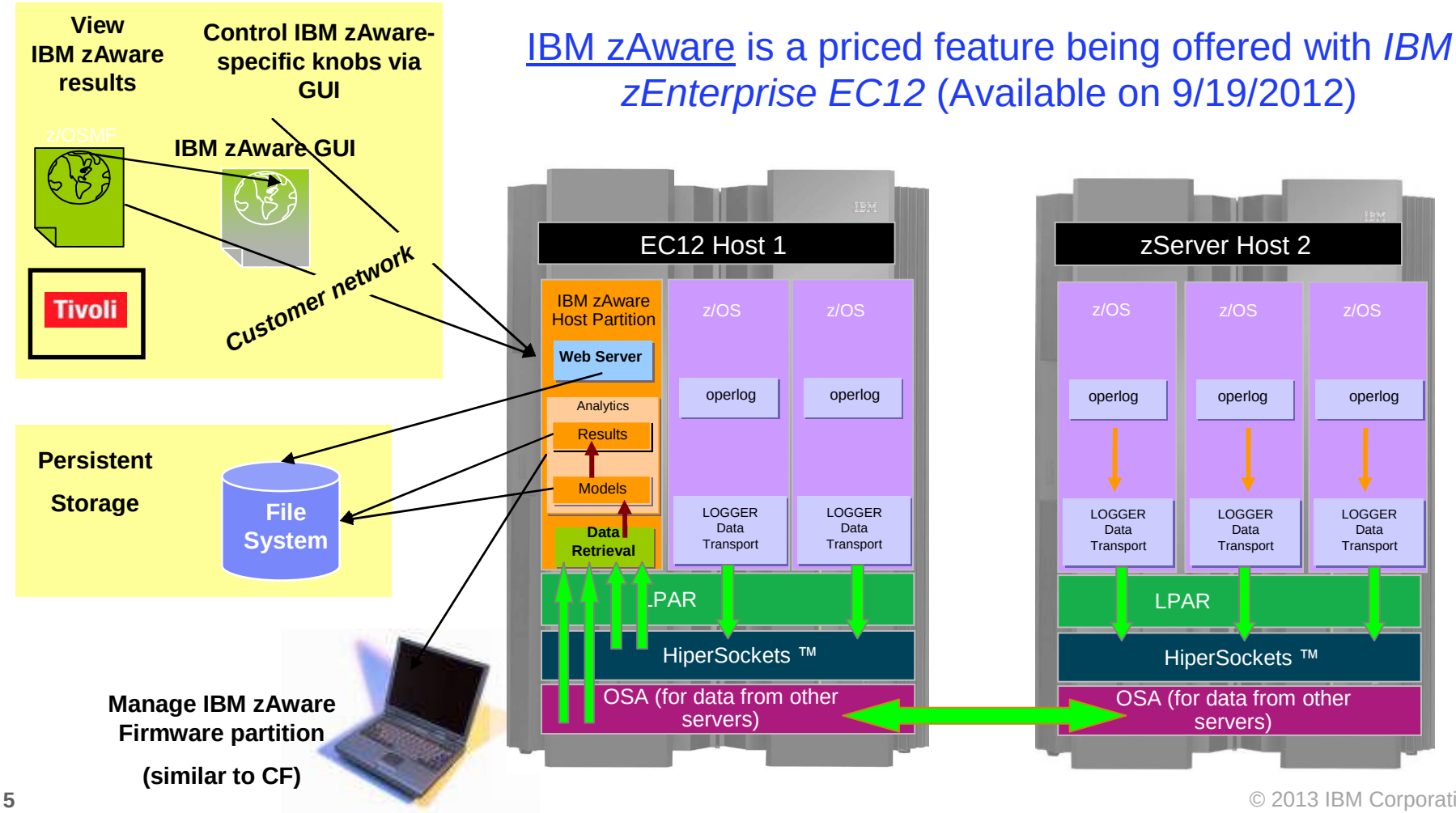
- **Errors can occur anywhere in a complex system**
- **Difficult to detect, difficult to diagnose, symptoms / problems can manifest hours/ days later**
- **Problem can grow, cascade, snowball**
- **Volume of data is unmanageable – need information and insight**
- **Systematic ‘soft failures’ (sick but not dead) much harder to detect – several anomalies can build up over time**

What is IBM zAware?

IBM zAware provides:

- z/OS Log Analytics - Analysis of z/OS operlog
- Firmware appliance that runs 'out of band' (not on z/OS)
- Training period determines 'normal' message flow, volumes, etc.
- Surfaces anomalies to help detect Sick But Not Dead (SBND) scenarios

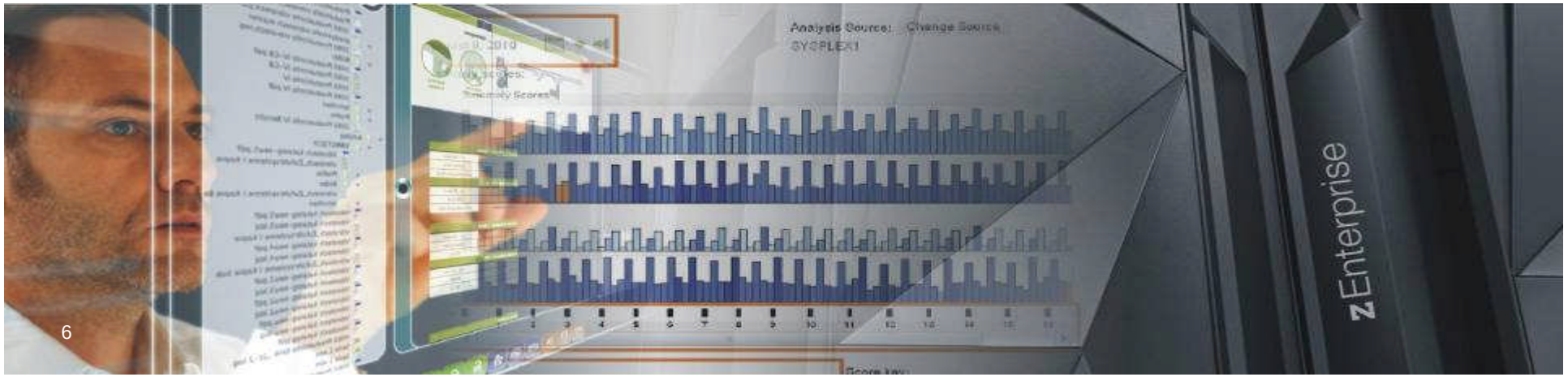
IBM zAware is a priced feature being offered with *IBM zEnterprise EC12* (Available on 9/19/2012)



IBM zAware – Identifies unusual system behavior

IBM zAware contains sophisticated analytics, applies IBM insight, and machine learning to understand your unique system

Monitoring	Detection	Frequency	Reporting
▪ Supports IBM and non-IBM middleware and applications ▪ Monitors OPERLOG in a sysplex or monoplex ▪ Assigns a message anomaly score to help identify potential issues	▪ Detects anomalies other solutions might miss ▪ Can find the rare or infrequent message ▪ Can detect an unusual number of normal messages ▪ Can detect messages issued out of context	▪ Samples every 2 minutes ▪ 10-minute interval ▪ Uses 90-day rolling baseline; a utility provided to populate baseline; flexibility provided ▪ History kept for 2 years (default)	▪ Near real-time analysis ▪ Intuitive reporting – both high level and drill down ▪ Color-coded browser display ▪ XML output can feed ISVs or processes ▪ Tivoli provides event notifications and integration with service management capabilities



How can IBM zAware Improve Problem Determination?

- **Identify messages indicating a possible z/OS incident is happening**
  - *Which image is behaving abnormally?*
    - 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 message ids** are unusual?
    - **How often** did the message occur?
    - **When** did the message start to occur?
  - *Were similar messages issued in the past?*
    - Similar characteristics, Same pattern?

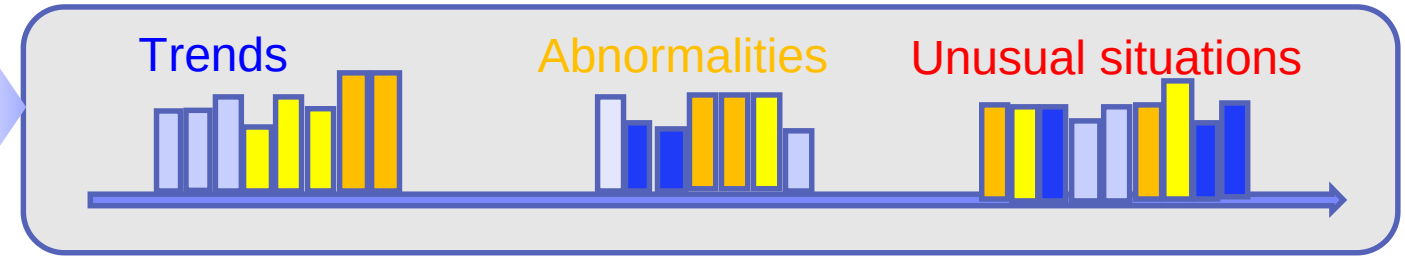
- **After a change has been made**
  - *Are unusual messages being issued following changes ?*
    - New software levels (operating system, middleware, applications)
    - Updated system settings / system configurations

- **When diagnosing the cause of an intermittent problem**
  - *Are new unusual messages being issued in advance of the problem?*
  - Are more messages issued then expected?
  - Are messages issued out of normal pattern or context?

Vertical bar shows the number of unique messages in a 10 minute interval

Scoring of messages color coded from common (blue) to rare (orange)

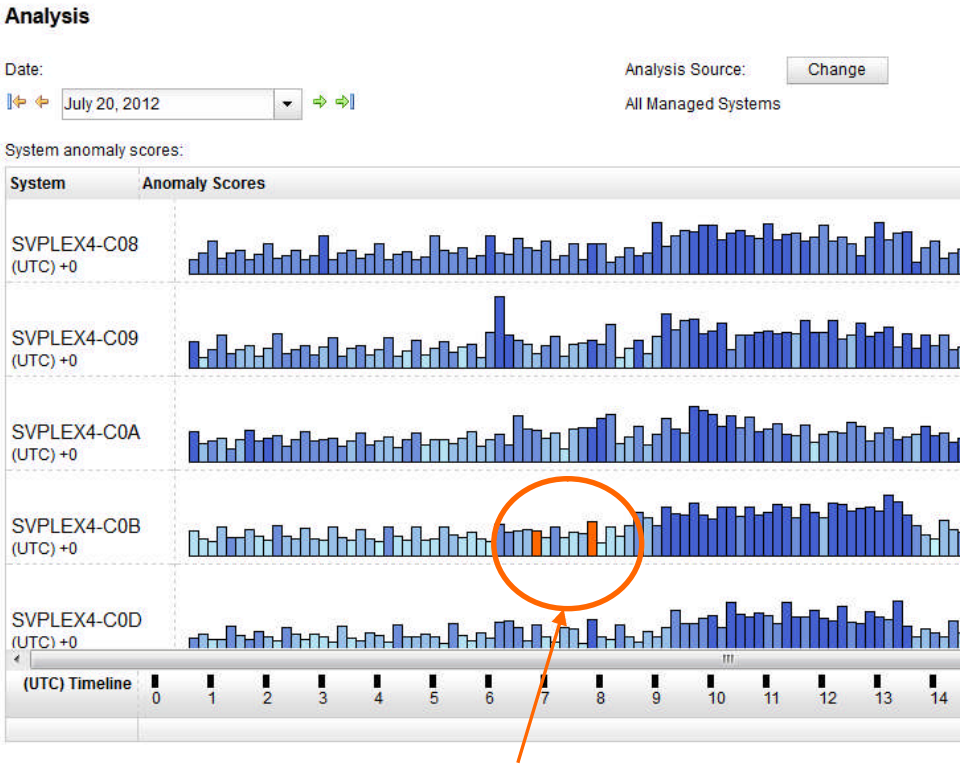
Finds Anomalies that would be Hard to Detect



IBM zAware – User Interface

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 may be too common)
    - Useful for long-term health issues
  - Uniqueness (message not common enough)
    - Useful for real-time event diagnostics
- Color-coded, easy-to-use web browser GUI
- XML Output can feed other products



Ability to drill down for details on anomalies

Sample Output - Interval View

Drill down to see JES2 resource shortage

Interval View for System CB88

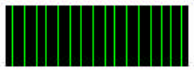
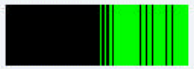
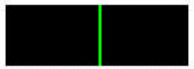
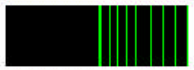
Date: July 1, 2012

Time interval (local time): 04:00 AM -- 04:10 AM

Analysis Source: All Managed Systems

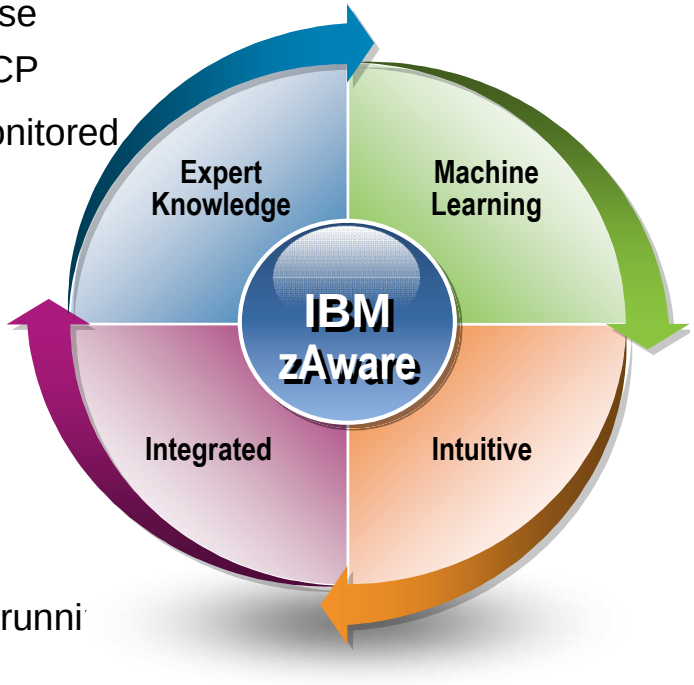
Interval anomaly score: 99.7

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
1	0.226	new	None	1		EYUXS1004W	M88CM88 Interval Timing queue element shortage detected	101	EYUXS	-1
1	0.226	new	None	1		EYUXS1005I	M88CM88 Interval Timing queue element shortage relieved	101	EYUXS	-1
1	0	in_context	IMPORTANT	16		HASP050	JES2 RESOURCE SHORTAGE OF TGS - 100% UTILIZATION REACHED	50	HASP	102
0.999	10.974	unclustered	None	57		IEE043I	A SYSTEM LOG DATA SET HAS BEEN QUEUED TO SYSOUT CLASS M	2	IEE	-1
0.998	6.706	unclustered	None	7		EYUCL0016I	M88CM88 Send Link Task terminated for MRO Network connection with CMAS M8ACM8A.	74	EYUCL	-1
0.998	6.519	unclustered	None	4989		ITP136I	ADSWCB G2APA001 G2LUA001-1 LU IS NOW INACTIVE 00.02.50.86	27	ITP	-1
0.987	4.427	unclustered	None	40		IEC070I	209-220,NETVIEW,NETVIEW,DSILOGS,683C,NE	12	IEC	-1

IBM zAware Operating Requirements

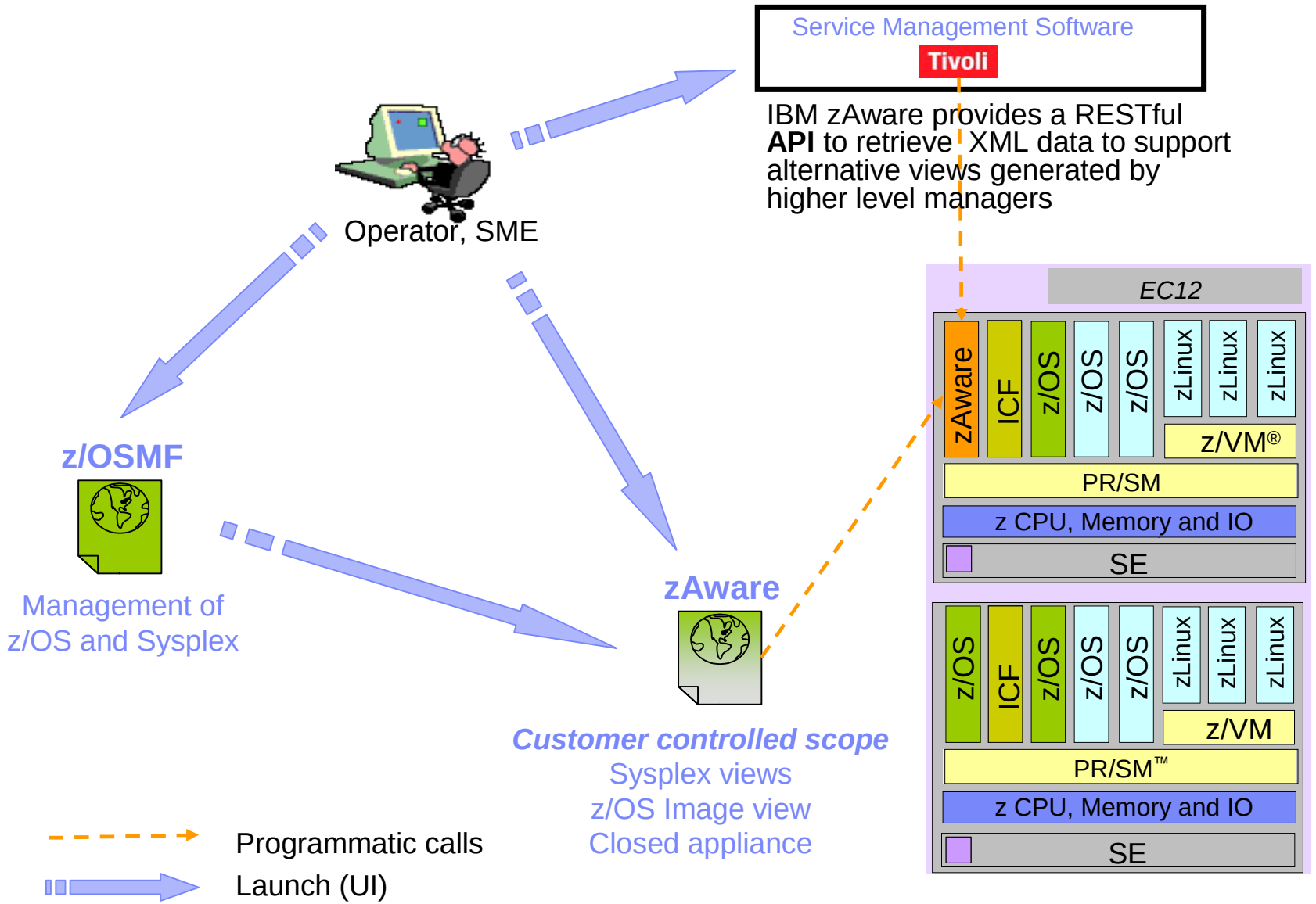
- **zEC12 to host IBM zAware Server**
  - IBM zAware requires it's own LPAR and runs it's own self-contained firmware stack.
    - This will reduce the number of LPARs available for customer use
  - IBM zAware processor resources can be IFL or General Purpose CP
  - Memory and DASD resources are dependent on the number of monitored clients, amount of message traffic, length of time data retained
    - Memory - Min 6GB + 256 MB
    - DASD ~ 500GB (ECKD or FC)
  - Network: HiperSockets or OSA ports – for both gathering of instrumentation data, and outbound alerting/communications
    - Need dedicated IP address for partition



- **zAware Monitored Clients**
  - IBM zAware monitored clients can be on any System z Server runni
    z/OS 1.13 + PTFs
    - IBM zEnterprise 196 (z196), IBM zEnterprise 114 (z114), etc., and can share log files via IP network with IBM zAware server

- **90 days historical syslog or OPERLOG data to initially prime IBM zAware**

IBM zAware Complements Your Existing Environment



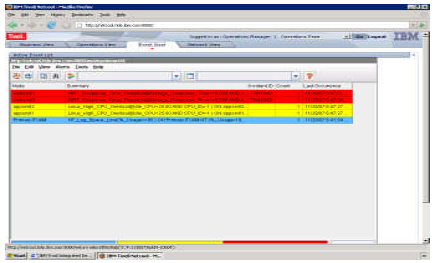
IBM zAware and Tivoli Service Management - A powerful Combination

Get the more from the zAware feature by **integrating** with **Tivoli Service Management.** Tivoli will utilize the zAware API to integrate log analysis with existing service management capabilities.

- Provide visibility into IBM zAware anomalies via Event Management
- Improve MTTR through integration with existing problem determination and performance monitoring tools
- Identify system errors and eliminate subsequent occurrences thru automation and more sophisticated analysis

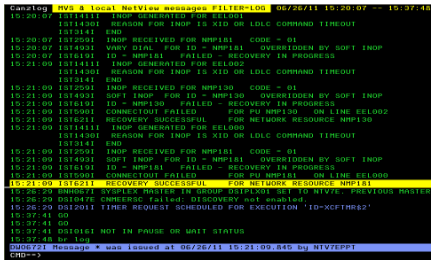
IBM zAware is NOT a replacement for traditional performance and availability monitoring tools. It's just the opposite. When used in conjunction with existing service management tools, it can provide a VERY powerful combination to help achieve 24/7 uptime, improve MTTR when problems occur and help avoid subsequent problems.

IBM zAware, Automation, Event Management and PD Tools



View event in Active Event List
Generate trouble ticket

Operator, SME



Browse NetView CANZLOG
Perform PD for anomaly

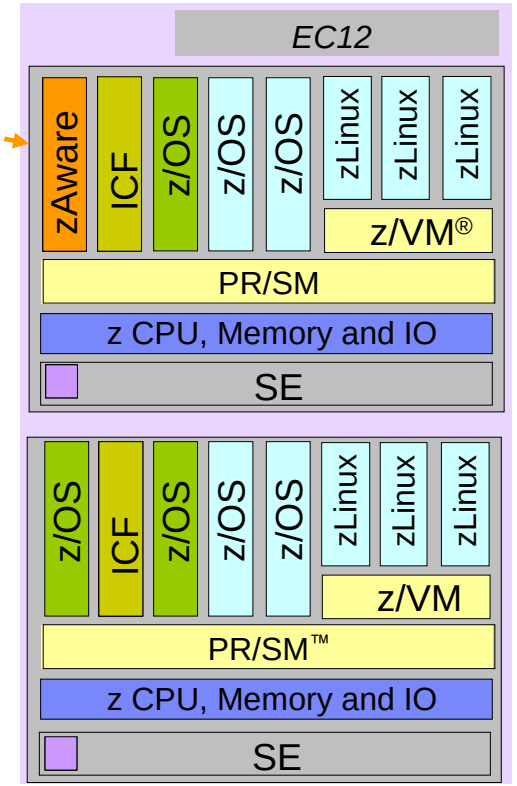
z/OS

Logger

Tivoli **NetView**

NetView processing …

- Query zAware (10 minute interval)
- If anomaly detected
  - Generate ‘anomaly’ message
  - Generate Event
- SME - Browse NetView CANZLOG to perform problem determination



- NetView samples provided to generate anomaly message and event(s) - Available for download from Service Management Connect
- NetView integration referenced from IBM zAware Redbook
- IBM Services (optional) available to install and configure zAware and NetView

NetView CANZLOG – Browse in zAware context

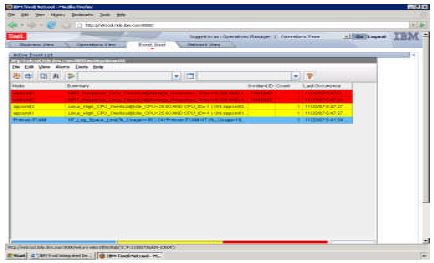
- Browse NetView CANZLOG in context of zAware anomaly
- Set filter and timeframe to view related messages in CANZLOG (consolidated log)
- Perform problem determination in context of timeframe of the anomaly

Set appropriate filters?

Launch to proper Timeframe

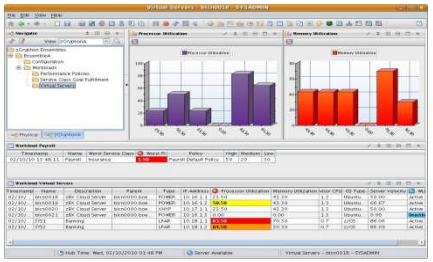
```
Canzlog  MVS & local NetView messages FILTER=LOG  11/06/12 16:50:04 -- 16:50:04
16:50:04 ZAI0001I Interval Results.
          System   :                    UTCPLXSB-SP0
          Interval:       2012-09-25T09:30:00.000Z
          Anomaly :                            72.0
         ------------------------------------------------------------------------
         Anomaly   Message   Count       Cluster          Contribution  Rarity
         0.997000   CSQE008I   6       UNCLUSTERED           6.425       76.0
         0.987000   CSQX209E   2       UNCLUSTERED           4.452       50.0
         0.987000   CSQX501I   6       UNCLUSTERED           4.419       38.0
         0.959000   CSQX191I   1       UNCLUSTERED           3.217       26.0
         0.939000  FPEV0511I   1       UNCLUSTERED           2.809       39.0
         0.939000    IEC070I  52       UNCLUSTERED           2.808       16.0
         0.929000   CSQX202E   2       UNCLUSTERED           2.664       28.0
         0.888000   DFS2864I  28       UNCLUSTERED           2.199        8.0
         0.878000   CSQX004I   1       UNCLUSTERED           2.107       28.0
         0.807000    IGD104I   1       UNCLUSTERED           1.648       12.0
         0.795000   CNZ4100I   1       UNCLUSTERED           1.588       20.0
         0.770000    IEF237I   1       UNCLUSTERED           1.473        3.0
         0.767000    AOF313I   5       UNCLUSTERED           1.458        2.0
                          ------------------- END OF DATA --------------------
16:50:04 ZAIGET - Starting
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
CMD==>
```

IBM zAware, Event Management and Traditional Performance Monitoring



View event in Active Event List
Generate trouble ticket

Operator, SME



Perform PD for anomaly using association with traditional monitoring KPIs

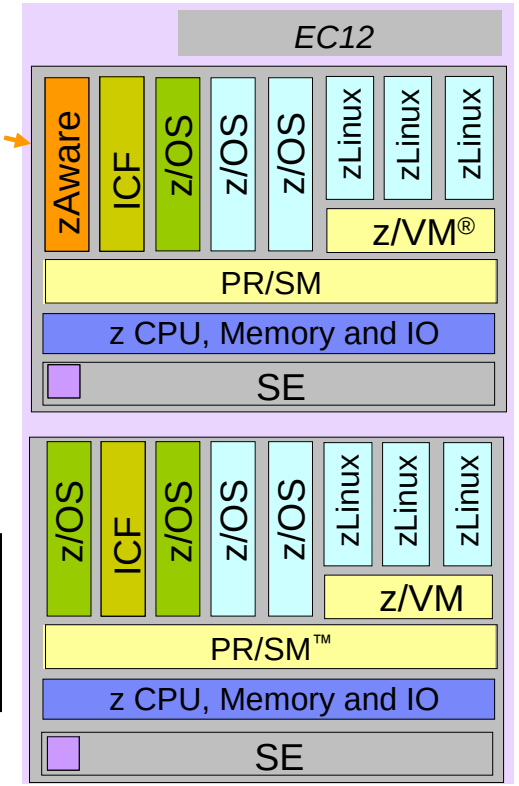
z/OS Logger

Tivoli **Performance Monitoring**

Processing …

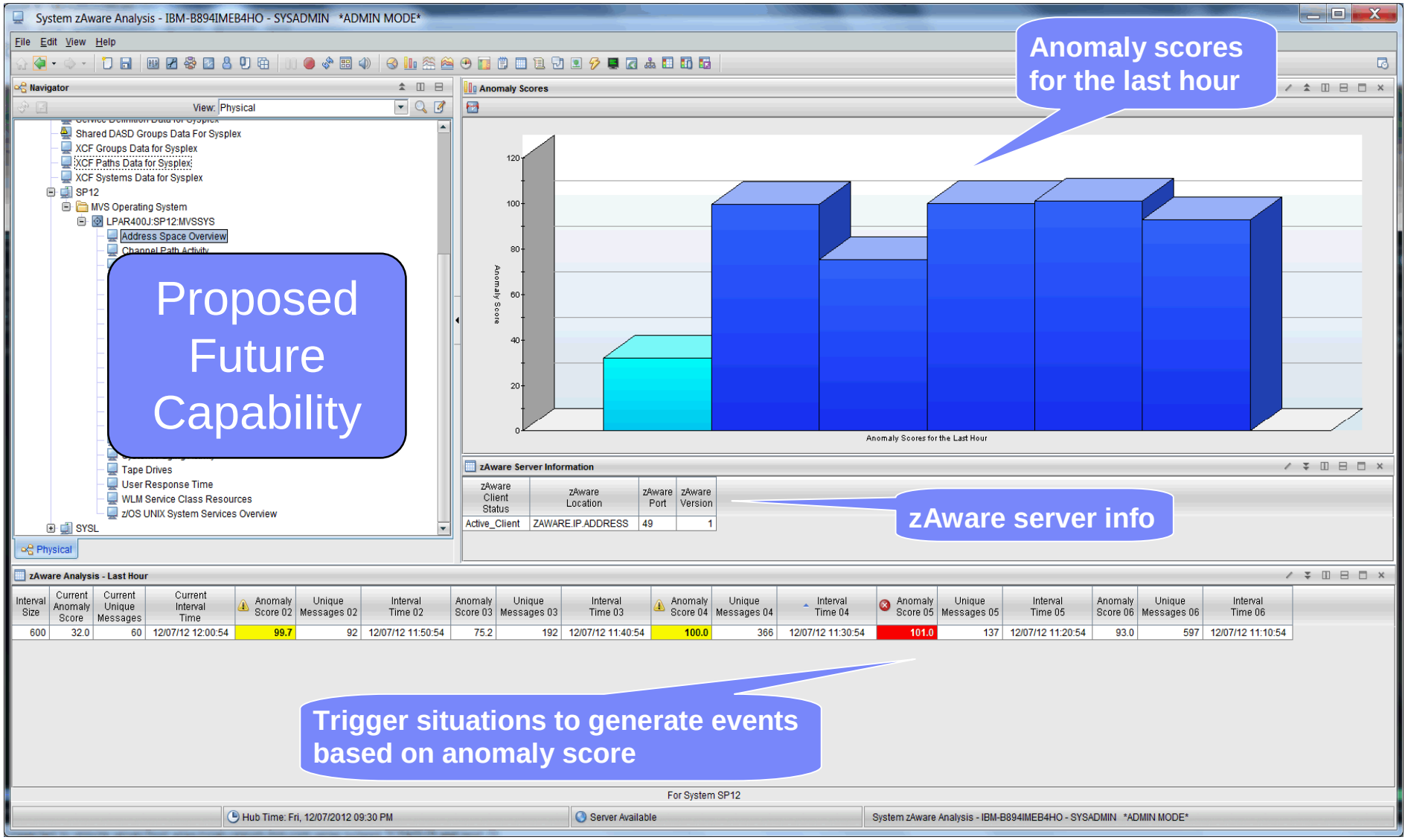
- Query zAware (10 minute interval)
- If anomaly detected
  - Trigger situation to Generate Event when anomaly is surfaced
  - Include zAware insights in performance monitoring views

Proposed Future Capability



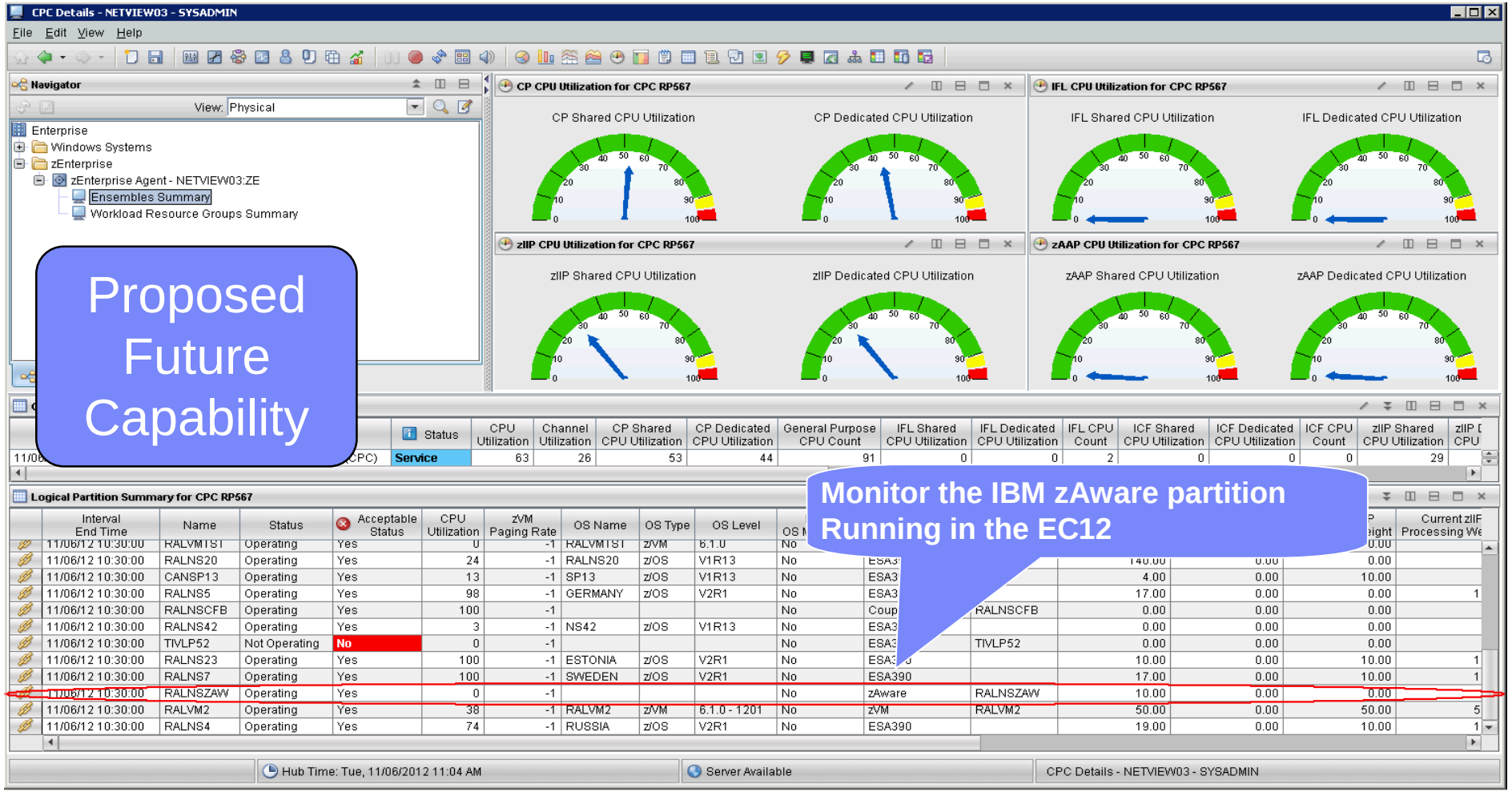
- Performance monitoring scenarios currently being developed per Tivoli's statement of direction
- Customer input welcome

Performance monitoring view including IBM zAware anomalies



Monitoring the zAware Server

- The Tivoli zEnterprise Monitoring Agent already monitors the logical partitions in the CEC as shown in the ‘Logical Partitions Summary’ table in the zEnterprise Ensemble Summary workspace.



IBM zAware and Tivoli – more Information

IBM zAware Publications:

System z Advanced Workload Analysis Reporter (IBM zAware) Guide - SC27-2623-00
https://www-304.ibm.com/support/docview.wss?uid=isg24f9114255d7d1f3285257a6a0077c2ca&aid=1

IBM zAware Demo:

https://www-304.ibm.com/connections/blogs/systemz/entry/zawaredemo?lang=en_us

IBM zAware Redbook:

Extending z/OS System Management Functions with IBM zAware
http://www.redbooks.ibm.com/abstracts/sg248070.html?Open

Service Management Connect:

NetView wiki page to download zAware integration samples and documentation
https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20System%20z%20Monitoring%20and%20Application%20Management/page/Integration%20Scenarios%20for%20Tivoli%20NetView%20for%20zOS

Learn more about IBM's entire Tivoli System z portfolio at upcoming Pulse Conference

Register at:

http://www-01.ibm.com/software/tivoli/pulse/

- *Receive Tivoli for System z information updates on a regular basis:*
  - *IBM Software Newsletter*

Thank You for Joining Us today!

Go to www.ibm.com/software/systemz/events/calendar **to:**

- Replay this teleconference
- Replay previously broadcast teleconferences
- Register for upcoming events