Optimal Alert Management Strategies for System z and Beyond

Ed Woods
IBM Corporation

Session 9776
Monday, August 8th
9:30 – 10:30 AM
Agenda

- Alerts
  - Why Alerts? What are the benefits?
  - What are the challenges?
- Types of alerts
  - Typical sources of alert information
- How alerts may be presented
  - Visualization and notification
- How alerts may be managed and correlated
- Forging an integrated alert management methodology
  - Integration and event correlation
    - Examples using IBM OMEGAMON, TBSM and OMNIbus
- Recommendations And Road Map
  - Putting it all together
Why Alerts?
What Are The Benefits?

- If you don’t measure it, you can’t manage it
  - Ongoing measurement of system/application activity, availability and performance is important to consistent results

- Many issues are anecdotal
  - What happened? Where? When?
  - How much? How often? How severe?
  - What’s the technical and business impact?

- Meaningful alert management enables fast and efficient problem isolation and root cause analysis
  - Become more proactive

- Gather measurement data and use to craft meaningful alerts
  - Select and publish ongoing performance metrics
Islands Of Automation Complicate Management

Potentially many consoles, screens, and technologies to monitor and manage
Common Alert Challenges
Islands Of Automation

- Many technical platforms, components and core technologies to manage
  - Often times each with it’s own group of Subject Matter Experts (SMEs)
  - Each with it’s own set of management tools

- The problems
  - Complex SME tools with different User Interfaces
  - SME tools that do not integrate or share information
    - More difficult to navigate
    - More difficult to do problem identification, isolation, and resolution
  - More challenging to automate corrective actions without clearly defined integration
    - More reliance on manual intervention
Common Alert Challenges
Islands Of Automation And Tools Ownership

- Islands of automation pose challenges when trying to become more proactive
  - Sophisticated ‘composite’ applications drive the need for a more integrated methodology
  - Often necessary to more effectively integrate tools and technologies to become more proactive

- Tools ownership
  - Installation and management of the tools
  - Centralized management
  - Management dispersed among multiple groups
  - Recommendation – where feasible try for a centralized approach
Categories Of Typical Alerts

When planning an alert infrastructure, consider each category of alerts:

**Availability**
- Application availability
- Essential infrastructure availability
- Subsystem availability

**Performance**
- Subsystem performance
- Application performance
- Identification of performance issues

**Resource**
- Subsystem resource utilization
- Application resource utilization

Examples of typical alerts:

- Application availability
- Essential infrastructure availability
- Subsystem availability
- Subsystem performance
- Application performance
- Identification of performance issues
- Subsystem resource utilization
- Application resource utilization
Alert Notification Types And Options

- **Visual View – Custom Views – Enterprise View**
  - Red/Yellow indicators and icons in a GUI interface, such as Tivoli Enterprise Portal or TBSM displays

- **Console messages**
  - Example - Issuing messages and commands to the z/OS console
  - Use this as a mechanism to feed other automation

- **Paging and emails**
  - Issue commands to feed paging systems
  - Use 3rd party tools such as Postie to issue emails from the command prompt
  - Console messages may be used to feed email systems

- **SNMP traps and alerts**
  - Issue SNMP traps from the command prompt using situations or policies

- **Event correlation engine – example Netcool/OMNIbus events**
  - OMNIbus may act as an event correlation engine
  - May receive events via traps or the EIF interface

- **Alerts to 3rd party tools**
Sources Of Alert Information
Various Examples

- **Operating System Performance monitoring technology**
  - z/OS monitoring – example OMEGAMON XE For z/OS
  - Distributed OS monitoring – example IBM Tivoli Monitoring

- **Database monitoring technology**
  - z/OS Examples – OMEGAMON XE For DB2, OMEGAMON XE For IMS
  - IBM Tivoli Monitoring for Distributed databases, IBM Optim

- **Network monitoring technology**
  - Examples – OMEGAMON XE For Mainframe Networks, NetView
  - IBM Netcool OMNIbus, SNMP alert managers

- **Application level monitoring**
  - Examples – ITCAM for Application Diagnostics, OMEGAMON XE For Messaging
  - Application error messages

- **Console Automation and workload scheduling**
  - Console messages and resource status
  - Job and workload status
### Setting Alerts At The 3270 Level

**Example - OMEGAMON Classic Exceptions**

<table>
<thead>
<tr>
<th>Command</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISPLAY Parameters:</td>
<td>State=ON</td>
<td>Threshold=1</td>
</tr>
<tr>
<td>BOX Parameters:</td>
<td>Boxchar=NONE</td>
<td>Boxattr=NONE</td>
</tr>
</tbody>
</table>

- **Profile member**

- **XACB command**

- **XACB LIST=XREP**

- **Settings are stored in a profile member – may have multiple profiles**
- **XACB command sets threshold ON or OFF or sets threshold level, enables XLF logging facility, and automated screen facility**

---

- Each Classic OMEGAMON (MVS, IMS, DB2, CICS) has a set of pre-defined exceptions
  - Note – OMEGAMON for Mainframe Networks and Storage do not have Classic interface

---

**Optimal Alert Management Strategies for System z and Beyond**

© 2011 IBM Corporation
Monitoring Interfaces With Automation For Alert Processing – example OMEGAMON and IBM SA

IBM System Automation

OMEGAMON can view the console and issue commands

Automation may check for classic exceptions
Automation may issue OMEGAMON commands

Automation provides a bidirectional interface with the z/OS console

- IBM System Automation and AF/Operator provides a bi-directional interface with OMEGAMON
- Automation may detect OMEGAMON classic exceptions
- Automation may run execs to send traps to Netcool/OMNibus
Visualization Options
3270 Interface Versus GUI Interface Options

- **3270 Interface**
  - 3270 green screen is high speed and detailed
  - 3270 interfaces well with console automation tools
  - Works well for SME deep dive analysis and problem resolution
  - z/OS centric views

- **GUI interfaces**
  - Flexible and useful for ‘big picture’ views
    - Most customizable for different audiences
  - Works well for ‘end to end’ integrated views and methodologies
    - Incorporate Linux/UNIX/Windows platforms
    - Incorporate network, application, database and middleware
  - Works well for business application views
    - Correlate the impact of events on the business
GUI Interface Example - Tivoli Enterprise Portal Provides An Integrated Alert Management Interface
<table>
<thead>
<tr>
<th>Component</th>
<th>IBM Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>z/OS Health check</td>
<td>z/OS Management Console</td>
</tr>
<tr>
<td>z/OS &amp; USS</td>
<td>OMEGAMON XE on z/OS</td>
</tr>
<tr>
<td>NetView for z/OS</td>
<td>IBM Tivoli NetView for z/OS V5.3</td>
</tr>
<tr>
<td>Network</td>
<td>OMEGAMON XE for Mainframe Networks</td>
</tr>
<tr>
<td>DB2</td>
<td>OMEGAMON XE for DB2 PE/PM</td>
</tr>
<tr>
<td>CICS</td>
<td>OMEGAMON XE for CICS</td>
</tr>
<tr>
<td>IMS</td>
<td>OMEGAMON XE for IMS</td>
</tr>
<tr>
<td>Storage</td>
<td>OMEGAMON XE for Storage</td>
</tr>
<tr>
<td>WebSphere MQ</td>
<td>OMEGAMON XE for Messaging</td>
</tr>
<tr>
<td>WebSphere Appl Server</td>
<td>ITCAM for WAS</td>
</tr>
<tr>
<td>z/VM &amp; Linux on z</td>
<td>OMEGAMON XE on z/VM and Linux</td>
</tr>
<tr>
<td>Distributed Monitoring</td>
<td>IBM Tivoli Monitoring (ITM) &amp; ITCAM</td>
</tr>
<tr>
<td>Automation</td>
<td>SA for z/OS</td>
</tr>
<tr>
<td>DFSMS Audit</td>
<td>Advanced Audit for DFSMSHsm</td>
</tr>
<tr>
<td>Catalog Management</td>
<td>Advanced Catalog Management for z/OS</td>
</tr>
<tr>
<td>SMF trend analysis Reports</td>
<td>Tivoli Decision Support for z/OS</td>
</tr>
</tbody>
</table>
Benefits Of An Integrated Alert Management Methodology

- **Improved ability to manage increasingly complex composite applications**
  - Enables an integrated approach to the management of subsystems, platforms, and application components

- **Reduce time to problem resolution**
  - Identify potential issues more rapidly

- **Improved event management and problem isolation**
  - More meaningful and useful problem alerts

- **Improved event correlation and management**
  - Eliminate the “noise” and focus on key issues
Important Characteristics Of An Integrated Alert Management Methodology

- **Integration**
  - Pull critical information together to the “single pane of glass”
    - Gather essential information from a variety of sources
    - End to end views for complex composite business applications

- **Flexibility**
  - Different views for different audiences
    - Management and Line of business/end users
    - Operations
    - Help desk
    - Technical Subject Matter Expert (SME) views
  - Optimize the views as the environment or requirements change

- **Ease of Use**
  - Eliminate the clutter and tune out the “noise”
  - Focus on critical metrics
Integrate Information To Consolidate Alerts And Analysis

Take advantage of the Tivoli Portal GUI to integrate information and alerts

Multiple z/OS LPARs

Key alerts
Forming An Alert Management Strategy

- **High level analysis**
  - Integrated event management and event correlation
  - Integrated business application topology analysis

- **Integrated technical view**
  - End to end technical analysis
  - Alerts for problem isolation and automation

- **Technical detail view**
  - Technical deep dive analysis
  - Alerts for problem isolation and automation
Different Views May Be Required For Different Audiences - A Few Examples

- The integrated alert management overview
- The integrated Subject Mater Expert (SME) view
- The SME technical graphic overview
- The SME application specific view
- Management by exception view
- The Integrated technical view
- The end to end business application view
- The Integrated Operational view
- The Help Desk view
- The End User or Line of Business view
Example
An Integrated Operational View

- CICS Status
- DB Status
- z/OS Status

OMEGAMON Networks
System Automation
Tivoli Workload Scheduler
OMEGAMON z/OS

Alerts
Operational Alerts
Network Status

Optimal Alert Management Strategies for System z and Beyond © 2011 IBM Corporation 20
The focus of this view is technical and hardware/platform specific in nature. Target audience may be systems or operations.
The Tivoli Enterprise Portal enables integrated end to end views and dramatically expands alert management capabilities.

Icons highlight a problem.

Customizable graphic overview
User-definable drill downs for detail
Combine information from multiple sources

Add...
CICS
DB2, IMS
Middleware
Network Storage
z/OS plex
Distributed
z/OS
z/VM
Linux on z
Alerts Are Defined Using Situations
Boolean Logic Capability Makes Event Management More Meaningful And Powerful

**OMEGAMON** alerts are based upon a mechanism called a situation

Situations are created with an easy to use GUI editor

Using boolean logic allows the alert to be more meaningful and useful

For example - A single OMEGAMON DB2 situation can handle multiple application or subsystem scenarios

Any item of information monitored by OMEGAMON may be used in a situation
Situations Highlight Alert Scenarios And Provide Drill Down Detail For Analysis

Icons highlight alerts

Click to see alert detail

Alert details
Alerts

General Recommendations And Rules Of Thumb

- Make alerts Meaningful, Actionable, and Useful
- Meaningful alerts
  - Alert should be flexible – make the names understandable
  - Adopt an alert naming convention
    - Makes it easier to identify customer created versus product provided situations
- Actionable alerts
  - Have appropriate notification
    - A workspace with an alert icon, command/message notification
  - As a standard have expert advice
  - Have pre-defined take actions where appropriate
- Useful alerts
  - Eliminate phony alert indicators – tune out the noise
  - If an alert fires it should indicate an actual issue
    - An alert, an owner, and a consequence
Considerations For Event Correlation

- Event correlation helps to improve the ability to manage increasingly sophisticated composite applications
  - Applications are more complex
  - Infrastructure is more complex
  - Alerts are more complex

- Event correlation helps to eliminate the “noise” and focus on key issues
  - Tune out false alerts and focus on root cause analysis
  - Identify potential issues more rapidly
  - Reduce time to problem resolution

- Event correlation helps to enable an integrated approach to the management of subsystems, platforms, and application components
Components To Enable Event Correlation Example - Tivoli Netcool/OMNibus

- IBM Tivoli Netcool/OMNibus is the cornerstone of the IBM Tivoli Consolidated Operations Management solution
  - Delivers real-time, centralized monitoring of complex networks, IT domains
  - Event processing scalability that can exceed over 100 million events per day
- Netcool/OMNibus includes over two hundred out-of-the-box probes (and more than 25 vendor alliances)
  - Enables the ability to include events from virtually any management system or device in the network or IT environment
- Provides manager-of-manager capabilities
  - Depth and breadth of event coverage and correlation
  - Software failover for highly available consolidated operations management
  - Event-processing efficiency resulting in cost savings and scalability
An Example Of Integration And Correlation
How Does Monitoring And Automation Integrate With OMNIbus?

Integration enables customer to forward events reported by OMEGAMON XE monitoring agents and System Automation to Netcool/Omnibus.

OMEGAMON situations may feed information to automation and/or send events to OMNIbus.

OMNIbus Probes

Events

OMNIbus Event Mgmt Server

Events

OMNIbus events

Automation

EIF Probe

ITM Server

Situation Events

Situation Policies

Automation/ Trouble tickets

TEP

Event Viewer
The Next Phase Of Event Correlation Business Application View – What’s The Impact?

- Enabling the management of performance and availability from the perspective of key business applications
- Business Application Views
  - Manage performance and availability from an application perspective
  - Target the critical path performance and availability components of an application
    - Focus on specific components (platforms, databases, transactions)
    - Choose mission critical business applications
- How to get there
  - Start with event management and migrate to business application management
Alert Considerations
Managing Events Versus Understanding The Business Impact

Events
Manage and correlate events from a variety of sources

Business Perspective
Determine the source of business service disruptions
Expanding The Perspective Business Application View

- **Components of a Business Application View**
  - **Availability**
    - Is the application and its infrastructure components available?
    - Are users able to access the application?
    - Are SLAs being met?
  - **Performance**
    - How well is the application performing?
    - What is the end user experience?
    - Are Key Performance Indicators (KPIs) being met?
  - **Alerts**
    - Notification when issues occur
    - Real time and Historical information available
    - The ability to trend and analyze over time
Example Of A Business Application View Using IBM TBSM

IBM Tivoli Business Service Manager (TBSM) provides a GUI interface designed for business views.

Displays that show business metrics, KPIs, and SLA.

Business application overview.

Business application resource component relationship and status.
What Makes Up A TBSM Solution?

**Visualize & Inform**
- Business & Operational Dashboards
- Realtime Views & Metrics:
  - Balanced scorecards & KPIs
  - Charts, Graphs, Maps
  - Service Topology
  - Event Views
  - SLA Metrics
  - Custom Data Views

**Analyze & Automate**
- Service Correlation & Automations
  - Business impact and root cause analysis -- KPI and SLA calculation & tracking
  - enrichment & escalation -- Automated actions

**Collect**
- Dependency
  - IBM & 3rd Party
- Event & Perf.
  - IBM & 3rd Party
- Data
  - IBM & 3rd Party

**Service Infrastructure**
- Applications
- Systems
- Wireless
- Network
- Voice
- Security
- Mainframe
- Storage
- Business
- Other
What’s Required To Create A Business Application View?

- **Events**
  - Meaningful and useful alerts from a variety of sources – monitoring, automation, network management, database management and more…

- **Correlation**
  - Correlate alerts to eliminate noise and remove duplicate events
  - Correlate events to application infrastructure
    - Discovery and mapping of application components

- **Visualization**
  - KPIs and SLAs
    - Define Key Performance Indicators and Availability objectives (SLAs)
  - Map and display KPIs and SLAs
  - Drive notification
TBSM
Events
Correlation
Visualization

TADDM
- Create/Maintain application maps
- Maintain dependencies and configuration values
- Stitch relationships between z/OS and distributed resources
- Maintain change history

TBSM
- Model and visualize business services
- Custom business views & dashboards
- Real-time service status from events & external sources
- Dynamic key performance indicators (KPIs)
- Advanced numeric rules for calculations
- Service definition from TADDM
- Real-time Service Level Tracking

Discovery
z/OS

TADDM Sensors

Auto Disc
z/OS DLA
TMS DLA
TMS DLA
ITCAM DLA
Auto Disc

TBSM Server

Netcool/OMNibus Server

TBSM Dashboard

Status Events
z/OS

Netcool/OMNibus EIF Probe

Distributed

Distributed and z/OS Monitoring

TADDM

Auto Disc
z/OS DLA
TMS DLA
ITCAM DLA

TEC
ITM v5
ITM v6
ITM v6
ITMCAM

TEC
ITM v5
ITM v6
ITMCAM

OMEGAMON XE

OMEGAMON XE

Event Pump for z/OS

z/OS
IMS
CICS
DB2
SA

z/OS
IMS
CICS
DB2
SA
The Roadmap
Pulling It All Together

- Begin with event management
  - Define meaningful, actionable, useful alerts
    - Establish standards and conventions for alerts
  - Determine visualization/notification of events
    - Optimize views for target audiences
- Grow the infrastructure
  - Determine an integration approach for alert management
  - Implement event correlation
    - Expand event information sources and eliminate background noise
- Expand to business application management
  - Define KPIs and SLAs
  - Define the mapping of application infrastructure
  - Correlate events to application performance and availability
Thank You!
Check Out My Blog
http://tivoliwithaz.blogspot.com

Visit my blog on IBM Tivoli performance and availability management of System z. Lots of information on OMEGAMON, Automation, and many things Tivoli...