Analytics Based Event Management in Hybrid Cloud Environments

Kristian Stewart – STSM Systems Middleware
Agenda

- Analytics for Operations: why?
- Predict / Search / Optimise
- Performance Management / Monitoring Analytics
- Event Analytics: Search
- Event Analytics: Seasonality
- Event Analytics: Related Events
- Research
The Next IT Operations Focus: Big Data

“Focus on operational objectives has seen significant uptick since 2013”

**Organizational objectives for use of data and analytics**

- **53%** Customer-centric
- **40%** Operational efficiency
- **7%** Financial/risk management
- **31%** are using data and analytics to improve customer acquisition
- **22%** are using data and analytics to improve customer experience

*Figure 1:* Respondents are primarily focused on customer-centric objectives for the use of data and analytics, but the focus on operational objectives has seen a significant uptick since 2013.

*Source:* IBM Institute for Business Value 2014 Analytics Study. n= 1036.
Operations’ Remit

Doug – the Operations Manager

I have to:
- Help maximise the availability of business-critical applications and services, and
- Minimise the cost of doing so

- Analytics
- Notification
- Automation
- Runbook

Event Management

Monitoring

Annette – Operator
Olivia – App Owner
Jim – IT SME
Alex – Network SME
Maximise availability of services/applications, and minimise the cost of doing so

Operators

Events/Tickets

SMEs

Fix here == $..
Reduce noise and correlate to lower MTTR and maximise operations efficiency.
Minimise ticket generation and event escalation.
Maximise automation.
Operators

Events

Events/Tickets

Gain Insight through examination of data

SMEs

Infrastructure and Applications
IBM IT Operations Analytics
Real Time and Historical Analytics

Real-Time

Historical

Predict
IBM SmartCloud Analytics
Predictive Insights

Search
IBM SmartCloud Analytics
Log Analysis

Optimize
IBM SmartCloud Monitoring
IBM Netcool Operations Insight

Performance Metrics
Transactions
Logs
Documentation
Alerts, Alarms & Events
IBM IT Operations Analytics
Real Time and Historical Analytics

Real-Time

Historical

Apply Insight/Models

Learn/Gain Insight

Predict
IBM SmartCloud Analytics
Predictive Insights

Search
IBM SmartCloud Analytics
Log Analysis

Optimize
IBM SmartCloud Monitoring
IBM Netcool Operations Insight

Performance Metrics
Transactions
Logs
Documentation
Alerts, Alarms & Events
Performance Analytics
I need to know when this KPI becomes abnormal
I need to know when this KPI becomes abnormal.
I think the KPI is abnormal if it crosses this threshold
~30% of these threshold events are never actioned!
Operations are wasting $$ and missing important stuff
Ok – I’ll go and adjust the thresholds
There are 100s of thresholds to define. How much is this going to cost??
Solution: Learn what is normal (baseline) and apply dynamic thresholds
• Many metrics are seasonal: what is normal for 2pm may not be for 5pm
• Reduce false positives and get early warnings
Other techniques: Learn co-variance relationships between KPIs. Report when they break down.
Other techniques: Learn co-variance relationships between KPIs. Report when they break down.
Other techniques: Detect abnormal trends and alert before a threshold breach

KPI

- No trend
- Trend begins
- Trend confirmed.
- Alarm here!
- Avoid this
Challenge: Reacting to performance thresholds is not enough. IT Staffs must become proactive to ensure mission critical applications never go down.

Automated Threshold Maintenance
No complex manual intervention to setup & maintain with 5 times faster processing

Anomaly Detection
Alerting before potential issues become service impacting, enabling IT to shift from reactive to proactive

Forecasting
Forecast anomalies and metrics to identify potential critical issues

Multivariate Analysis
Discover related KPIs for deeper insight and faster mean time to repair
Event Analytics
Maximise availability of services/applications, and minimise the cost of doing so.
Event Analytics: Why?

- **As an Operations specialist (Annette) I can**
  - see events in the *context of the business problem* they are causing, and
  - see the *most likely causes* of business affecting problems

  **So that I can**
  - resolve the problems the business cares most about first, and
  - Minimise the mean-time-to-diagnose/repair

- **As an Operations Administrator/SME (Barbara/Jim) I can**
  - leverage historical events, and
  - leverage domain knowledge and topological models

  **So that I can**
  - *reduce and correlate events*, prior to presentation to Annette and Jim, *without having to do any programming*

- **As an Operations Manager (Doug) I can**:
  - determine which events cost operations the most to deal with
  - determine which faults have the greatest impact on the business
  - determine which events distract my team from solving problems
  - determine which events are indicative of insidious problems

  **So that I can**
  - Identify and improve/eliminate bottlenecks in my Service Assurance procedures
  - Apply my staff to the problems the business cares about

**So that we can** Maximise the availability of Services and minimise the cost of doing so
Event Analytics Delivery Programme

1) Event Search Analytics – Shipped in Netcool Operations Insight 1.1
What? : Provide flexible search and ad-hoc reporting on active and historical events
For Whom? : SMEs, Ops Managers, Operators…
Why? :
  • Reveal event hotspots
  • Search for root causes in otherwise discarded events

2) Event Seasonality Analysis – Shipped in Netcool Operations Insight 1.2
What? : Detect which events are generated in non-random patterns over time
For Whom? : Rules Authors/Admins, Ops Managers, Operators, SMEs…
Why? :
  • Reveal recurring underlying problems
  • Suggest candidate events for suppression or automation
  • Reveal poorly tuned thresholds

3) Related Event Analysis – Shipped in Netcool Operations Insight 1.3
What? : Determine which events are highly likely to occur together
For Whom? : Rules Authors/Admins, Ops Managers, Operators, SMEs…
Why? :
  • Reveal relationships between events and between managed entities
  • Identify candidate correlation rules
  • Identify candidate prediction rules

WHY? : Maximise availability of services and minimise the cost of doing so
Event Management and Log Analysis – Complementary Disciplines

- Correlation/Reduction/Filtering
- Aggressive Filtering/Normalization

Launch in Context

Correlation/Reduction/Filtering
- Annette – L2 Operator
- Notification

Successive Search/Drill Down

Agents and Probes
- Logfile Adaptors

Indexing

Agents and Probes

Logfile Adaptors
Event Search Analytics for Operational Effectiveness and Efficiency

Accelerate Problem isolation, identification and resolve for greater operations agility

- Identify problems within seconds with insight to your near real-time and historical event data
- Isolate problems faster by bringing relevant events data into problem investigations
- Repair problems quicker with the right details quickly to hand.

Turn your historical event data into insight for higher operational efficiency

- Identify Event Hot Spots that impact your workload with simple visualization
  - Top Nodes, Top Locations, Top Managers, Top Events with Tickets and more
- Easily see related Events that may be candidates for supression
- Leverage visualizations to quickly isolate the problems that will make more difference to your environment

Look at events a whole different way

What are they?
Why are they there?
How many are there?
Are they accurate?
Are they actionable?
Are they valid?

Provides rapid interactive line of sight to opportunities for improving efficiency, making Operations task simpler
Event Search with launch in context from Netcool

Keyword and pattern search on OMNIbus events

Clickable results distributed by important fields

Distribution of matching events over time
Event Statistics provide quick identification of root causes

Optional tabular display for sorting and field comparison

On-the-fly charting of event data for hotspot identification
Quick search results allows an iterative process to find the root cause

Pin point issues with search refinement and drill down
Report on event history identifies seasonal events sorted by confidence level and frequency.

Drill down shows time distributions of events ...investigate peaks.

Can better align thresholds to seasonal peaks reducing events.

Large Bank

7% of Priority 1 Tickets were raised by events that were highly seasonal

30% of lower severity tickets
Report shows seasonal events, with confidence

<table>
<thead>
<tr>
<th>Summary</th>
<th>Maximum Severity</th>
<th>Minimum Severity</th>
<th>Confidence Level</th>
<th>Review</th>
<th>Reviewed by others</th>
</tr>
</thead>
<tbody>
<tr>
<td>GIDC_fes_xuic_stav3(Usd_Pot=55 AND Mount_Point&lt;&gt;N\NAS\fileprise AND KPX2.340\FILES MP &lt;&gt; N\mnt) ON dpep20\PX (Usd)</td>
<td>5</td>
<td>5</td>
<td>100%</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Link Down (Device 800) (Enterprise 13614.1.1.1.1)</td>
<td>3</td>
<td>3</td>
<td>100%</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>UNIX_CMD_Runaway_Process[CPU_Utilization&gt;95 AND User_ID&lt;&gt;0 AND Execution_State=Runnable OR Execution_State=Active]</td>
<td>4</td>
<td>4</td>
<td>100%</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>MS_Offline(Status=OFFLINE AND Reason&lt;&gt;FA) ON E0 00-17-00-00-00-18-CA-CD 1.HUM (Status=OFFLINE Reason=)</td>
<td>5</td>
<td>5</td>
<td>100%</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>UNIX_HIGH_CPU[CPU_Utilization&gt;95 &amp; Time &gt; 5 Mins ]</td>
<td>5</td>
<td>4</td>
<td>100%</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Pct Peak free memory very low - risk of crash</td>
<td>4</td>
<td>4</td>
<td>100%</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>MQ Queue down Node TME10999d</td>
<td>5</td>
<td>5</td>
<td>100%</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MQ Queue down Node TME10999card</td>
<td>5</td>
<td>5</td>
<td>100%</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>UNIX_HIGH_CPU[CPU_Utilization&gt;75 &amp; Time &gt; 5 Mins ]</td>
<td>5</td>
<td>5</td>
<td>100%</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>MS_Offline(Status=OFFLINE AND Reason&lt;&gt;FA) ON JW-A02_01_WAH_102_01_BK.WAS (Status=OFFLINE Reason=)</td>
<td>4</td>
<td>4</td>
<td>97%</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Interface GigabitEthernet2/0/16 changed state to down</td>
<td>2</td>
<td>2</td>
<td>97%</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>GIDC_fes_xuic_stav3(Usd_Pot=55 AND Mount_Point&lt;&gt;N\NAS\fileprise AND KPX2.340\FILES MP &lt;&gt; N\mnt) ON dpep21\PX (Usd)</td>
<td>3</td>
<td>3</td>
<td>98%</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>MS_Offline(Status=OFFLINE AND Reason&lt;&gt;FA) ON JW-A01_01_WAH_127_01_B.K.WAS (Status=OFFLINE Reason=)</td>
<td>3</td>
<td>3</td>
<td>98%</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Event occurred four times over several weeks, always at the same time of day and same day of the week

Action > Investigate underlying cause
Event occurs consistently in the same two hours of the day, and in a consistent time window over the hour.

Action > Batch/cron job or some other temporal cause. Investigate cause or lower threshold.
Non-seasonal by the minute of hour or day
Occurs consistently in the same time window each day
Action > Raise threshold or provision more resource
Failures can lead to cascade of events

Today clients can solve this with event correlation rules but this requires Specialist Knowledge and has to be maintained

Automatic Grouping events that are related can significantly improve Operational Efficiency

Multiple operators working different events, but the same problem!

Multiple tickets raised, leading to inefficient use of SMEs

Identifying Root Cause requires greater skill and takes more time

Higher cost and lower operational efficiency

Grouped events

Auto generated or out of the box Correlation rules
What events have a causal relationship?
What events have a causal relationship?

Use Machine Learning to find out
Use the learned model: Group new instances
Use the learned model: Group new instances
Related Events Grouping

Relationships I know about

Known Event Analysis Grouping and Correlation providing powerful situation management of active events

- Out of the box domain expertise for known event relationships
- Vendor and technology dependent
- Significant reduction of incidents presented to the operator
- Extendable by Business Partners and clients with no coding required

Grouped by scope under a synthetic situation event and single ticket
Cause/symptom reprioritised by weighting factors as the situation develops
Weighted by the likelihood of being probable cause and/or service impacting
Event Analytics – Related Event Analytics

Relationships I don’t know about

Improve efficiency - Reduce actionable events by grouping events that always occur together

Automatic detection of event clusters

Review

Take action

Out of the box – no coding required!

“It is very beneficial to have a tool that can turn historical event data into an event group with a single root event. It helps us turn the data into logic”

Leverages machine learning to analyze historical event archive and identify groups of events that always occur together

- Presents identified relationship to the Administrator
- Presents proposed automated actions
  - Watch, Deploy, Archive or Do nothing
- Groups events in the Event Viewer

Increase operator efficiency by up to 90% with out-of-the-box alert reduction and advanced alert analytics
Making Insight Actionable

I can investigate the history and context of this seasonal event

This seasonal event is noise – I’ll suppress it

If this event does not occur when it is expected, I’ll raise an alarm
Futures
Research – Complement Discovered Topology with Analytically Derived Relationships

Events

Logs

Analytics

Metrics

Visualise and Correlate
Research – Use Discovered Topology to Inform Analytics
Research – Significant Event Classification

- I can characterise events that:
  - Take a long time to resolve
  - Go away by themselves
  - Always get manually ticketed
  - Never get acknowledged
  - Occur predictably

- I can:
  - suppress
  - filter
  - auto-ticket
  - delete these events without writing any rules

- I can:
  - unsuppress
  - escalate
  - ticket an event when its lifecycle deviates from the norm

I’ve got a lot less noise to deal with