Event Correlation In OM And OMi

Analysis From A Technology Standpoint

Speaker: Alfred Hermann, HP
Event Correlation: Why Is It So Important?

Benefits

- Reduced MTTR, faster resolution of problems
- Faster isolation of causal events, simplify event streams
- Increase operator efficiency, optimize the use of IT staff resources, have them work on what matters to the business
- Reduced OPEX
## Summary of OM/i Event Correlation Technologies

<table>
<thead>
<tr>
<th>Event Correlation Feature</th>
<th>OM Agent</th>
<th>OM Server</th>
<th>OMi Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignoring short term peaks</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Duplicate event suppression</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced threshold monitoring</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Baselining</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event storm detection and suppression</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event de-duplication</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>State based event correlation</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Event Correlation Interfaces</td>
<td>X</td>
<td>X</td>
<td>EPI</td>
</tr>
<tr>
<td>ECS: Event Correlation Circuits</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TBEC: Topology Based Event Correlation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Technologies:**
- Message Stream Interface (MSI)
- Event Processing Interface (EPI)
Discussion Of The Different Event Correlation Techniques In OM / OMi
Ignoring Short-Term Peaks
Setting On OM Agent Policy

**Technology**
OM allows you to define a minimum time over which the monitored value must exceed the threshold before it generates a message.

**Benefits**
Since it may not be reasonable to create a message when a threshold is exceeded only for a short time...

---

See backup section of this deck for an explanation of these qualifiers.
Duplicate Event Suppression
Setting On OM Agent Policy

Technology
Logic can work based on a count of events, on a time interval, or on a combination of \#events / per time

Benefits
Identical messages occurring in very short order will be suppressed, only the first one of a series will be forwarded to the management server and will draw the operator's attention.
Advanced Threshold Monitoring  
Combine Multiple Metrics

**Technology**

With the help of scripts (Visual Basic, Perl, Jscript) you can retrieve monitored values, combine them, apply arithmetic operations and fire events. Values can be compared against and/or stored in the embedded performance component (EPC) of the agent.

**Benefits**

In many cases a single metric crossing a threshold is not a sufficient indication of a misbehaving system. Instead, you need to look at multiple metrics in combination.

![Diagram](image-url)
Baselining
Historical Data Used To Calculate Baseline Of „Normal“ Range

Technology
Messages sent when current value (red line) is above or below the “normal” value.
Severity is assigned based on the distance from the “normal” for that time period (one, two or three StdDev from average).

Use Cases
- Metrics with recurring time patterns, e.g. weekly or time-of-day
- Not ideal for slowly creeping value changes, e.g. free space of a disk filling up over months

Benefits
Free-up operations staff to solve top issues rather than prioritizing them.
Reduces “false” alarms by 95%: Only alarms for “abnormal” behavior at a given time.
Message Storm Detection And Suppression Setting On OM Server

**Technology**

Once a message storm is detected, a high priority internal message will be placed in the browser indicating the message storm. Newly incoming messages will optionally be suppressed. Automatic and/or operator initiated action is available, e.g. to stop the agent.

**Benefits**

Keeps OM management server operable even though there is a high incoming flood of events.

**Use Cases**

Too many messages created from a specified node in a specified time interval, e.g. more than 100 events in 5 minutes.
Event De-Duplication

Goal: Do Not Fill The Event Browser With Duplicate Events

Technology

Combine similar events identified by message key, ETI or other attributes. A counter indicates number of duplicates. Individual events attached as annotations and/or available in event history.

Benefits

Only a single, consolidated message in the message browser instead of 100's of duplicates repeated using a lot of real estate, adding noise and competing for the attention of the operator.
State Based Event Correlation (OM)
Pairwise Correlation - Automatic Acknowledgement Per Key

Technology
Message properties enhanced by a "message key" and an "acknowledge key". Once an abnormal condition is solved the "bad" message along with the corresponding "good" message are automatically placed in the event history.

Benefits
As a result, the event browser only shows still existing problems, and service status is automatically reset. Reduces clutter in active event browser.
State Based Event Correlation (OMi)
Automatic Acknowledgement Per Message Key Or ETI

**Technology**

Same as OM state based event correlation (previous slide) but in addition to message keys also based on Event Type Indicators (ETIs). Events can be correlated with same related CI, same health-contributing ETI, but different ETI value.

**Benefits**

Same as OM state based event correlation. Especially useful if OMi processes events from 3rd party domain managers per BSM Integration Adapter.
Event Correlation Interfaces
Fully Customizable Event Correlation And Enrichment

Technology
Open interfaces to modify event while traversing the event pipeline. OM offers MSI interface with copy/divert, OMi offers EPI interfaces. Both of them are very similar. They are general in nature and can be used for non-correlation purposes as well, eg. event enrichment. The diagram below depicts how EPI interfaces in OMi can be plugged into the event flow at various stages of server processing.

Benefits
Allows script based event enrichment or manipulation, e.g. enrichment from an external DB, or to plug-in further EC technologies, eg. ECS.
ECS Designer And Composer
Correlation Per Circuits

**Technology**
Event processing engine running as an external process and plugged-into MSI. ECS Designer (add-on product) allows to create new circuits while ECS Composer uses a pre-defined circuit and is parameterized per fact store, data store and perl functions.

**Benefits**
ECS Designer supports creation of very complex logic while ECS Composer is more easy to use, and bundled with the OM media. Support for OM for Windows added with version 9.0, or alternatively OMW 8.1x plus patch OMW_00090.

**Use Cases**
- Combine events, issue only one message when a single point of failure causes multiple events
- Can retain messages for a certain time before they are issued to the console (or removed, modified)
- Remove transient messages
  - Example: 2 bad su followed by 1 good su -> no message generated
- Rate correlator, eg. detect DNS outage by correlating lookup failures
  - Suppress isolated DNS lookup failure
  - Raise an event when more than 5 failures occur for all agents within 10 seconds

**OM**
- Add-On
- Agent / Server
- Reduction
- Static
1. Something goes wrong in your environment
2. Monitoring reports multiple problems via events
3. Usually just one of the events describes the *CAUSE* of the problem
4. Others are just *SYMPTOMS*
5. Fix the *CAUSE* and also the *SYMPTOMS* go away

**Technology**
HP labs developed causal engine to correlate events based on Event Type Indicators (ETIs) & topology in the RTSM. Automatic "chaining" of correlation rules to cover cross-domain scenarios. Rules can be created directly from events in the browser.

**Benefits**
Operators can quickly identify cause events in the browser. They work on cause events instead of wasting time on multiple symptom events. Fewer invalid escalations to cross-domain tier 2/3 specialists. As discovery changes topology, rules are auto adapted.
Combining Event Correlation Techniques
Effective Combination Of Multiple Layers Of Correlation Techniques
The Effect Of Stacking Up Multiple Layers Of Correlation Techniques

OMi Server
Topology Based Event Correlation

OM Server Based Correlation

OM Agent Based Correlation

BSM Integration Adapter

... duplicate suppression
... automatically closing events

OMi Server Based Correlation

Site-Scope

ECS

M SI

MSL

ECS
Event Flow And MTTR Analysis

- Detect ALL events
- Categorize
- Impact Analysis
- Diagnose
- Rectify

**Magnitude of events**
- Fast / low effort
- Incorrect impact = delays in fixing
- Manual activity = slow
- Fast (potentially!)

**Monitor and Detect**
- Adaptive
- Filter
- Smart monitors
- Duplicate suppression

**Classify and Notify**
- ECS
- Duplicate counts
- Auto acknowledge

**Prioritize**
- Topology Based Event Correlation
Classification / Qualifiers
Of Event Correlation Techniques
Event Reduction Or Setting Up Relationships Between Events

<table>
<thead>
<tr>
<th>Event Reduction</th>
<th>Event Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignoring short term peaks</td>
<td>X</td>
</tr>
<tr>
<td>Duplicate event suppression</td>
<td>X</td>
</tr>
<tr>
<td>... based on time, frequency, and combination of both</td>
<td>X</td>
</tr>
<tr>
<td>Advanced threshold monitoring</td>
<td>X</td>
</tr>
<tr>
<td>... consolidate multiple event sources</td>
<td>X</td>
</tr>
<tr>
<td>Baselining</td>
<td>X</td>
</tr>
<tr>
<td>Event storm detection and suppression</td>
<td>X</td>
</tr>
<tr>
<td>Event de-duplication</td>
<td>X</td>
</tr>
<tr>
<td>... per message counters</td>
<td>(X)</td>
</tr>
<tr>
<td>State based event correlation</td>
<td>(X)</td>
</tr>
<tr>
<td>... per message key</td>
<td>X</td>
</tr>
<tr>
<td>Event Correlation Interfaces</td>
<td>X</td>
</tr>
<tr>
<td>... plug into event stream</td>
<td>X</td>
</tr>
<tr>
<td>ECS: Event Correlation Circuits</td>
<td>X</td>
</tr>
<tr>
<td>... Designer and Composer</td>
<td>X</td>
</tr>
<tr>
<td>TBEC: Topology Based Event Correlation</td>
<td>X</td>
</tr>
</tbody>
</table>

Insert Name
Title Goes Here

ECS: Event Correlation Circuits
... Designer and Composer

TBEC: Topology Based Event Correlation
## What Correlation Technologies Are Built-in?

<table>
<thead>
<tr>
<th>Built-in</th>
<th>Add-On</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Agent based message correlation</td>
<td>- ECS designer</td>
</tr>
<tr>
<td>- Correlation per message key / EPI</td>
<td>- TBEC: a separate OMi license</td>
</tr>
<tr>
<td>- Adaptive Baselining as technology, and deployed with Infrastructure SPI</td>
<td>- Adaptive Baselining with add-on SPIs, eg. SPI for AD</td>
</tr>
<tr>
<td>- MSI/EPI interfaces</td>
<td></td>
</tr>
<tr>
<td>- ECS composer (included with Operations Manager for Windows and Unix/Linux)</td>
<td></td>
</tr>
</tbody>
</table>
Where Do You Correlate Events?

On The Agent
- De-centralized: Split the load/effort through distributed processing
- Close to the source: the earlier in the event lifecycle you correlate, the less resources are needed/wasted for further handling
- Autonomous, no interaction with server needed, even in case of a network outage / disconnect this logic is applied

On The Server
- Central: Single place to maintain
- Across heterogeneous environments: This allows correlation logic that connects the dots across multiple source systems, e.g. in composite applications or cross-domain
- Correlation for agent-less event sources, e.g. events coming from SiteScope
- Combining events from different systems, HP and 3rd party, OM and other domain managers
What Correlation Technologies Are Adaptive?

Static
- Message Key Correlation
- MSI/EPI interfaces
- ECS

Adaptive - Self learning
- Adaptive baselining will adjust the thresholds based on past experience
- TBEC is self-adjusting based on dynamic topology. As new CIs and relationships are automatically discovered, the TBEC rules are adapted. Experts define the rules ONCE and do NOT have to go back and update when the infrastructure changes.
Conclusions
1. HP offers a rich portfolio of available event correlation capabilities, out of the box and as add-on products.
2. It is assumed that 80% event reduction can be achieved by effectively applying out of the box capabilities.
3. Baselining and TBEC are self-adjusting and reduce maintenance effort. TBEC correlation capabilities are unmatched in the industry.
4. There is not ONE correlation method that is the best, a variety of techniques are available to satisfy specific purposes.
5. Optimize your system and apply correlation techniques in combination.
6. There is no either-or OM vs. OMi positioning. Rather use OM and OMi in combination.
Event Correlation & Analysis 2010

HP is the ONLY vendor providing a complete event management solution that includes topology-based event correlation, run-book automation, integrated performance management, along with end-user monitoring and advanced application diagnostics.

HP in leader’s quadrant for 4th consecutive time.