The Medium is the Message: Improving Message Handling in HP Operations

Mike Peckar

Fognet Consulting

Abstract

One of the key objectives of any HPOM implementation should be to best leverage the tool to increase service availability. With that goal in mind, this session will focus on practices for shaping the tool so it can better shape us. Specific, proven methods and ongoing processes to reduce message volume and increase message quality will be covered, such as building customized policy dumps, top “n” reports and segregating internal messages from production message views. Both windows-based and UNIX-based HPOM administrators seasoned and new will benefit from this session and will walk away with specific practices they can immediately implement to increase product ROI and lift their organization’s level of IT maturity.

Welcome!

- Audience
  - Focus is on the HP Software Operations Manager product
  - Presentation will take about 2 hours
  - Both OMW (Windows) and OMU (UNIX) is covered
  - Session is technical – target is HPOM product administrators
  - Assumes basic administrator level knowledge of the products and of system administration
- Presenter
  - Mike Peckar, Principal, Fognet Consulting, www.fognet.com
    - Independent consultant since leaving HP in 1998
    - Have worked continuously with HPOM products since 1995
    - Last 2 years: Deployed HPOM on 3 networks in Iraq for coalition forces
    - Author Fognet’s Field Guide OpenView Network Node Manager

Outline

- Holistic Approach
  - People, Process, Technology
- Ongoing Process
  - Service Oriented Approach
- Message Volume Reduction
  - Traditional methods covered only briefly
- Mapping Messages to Services
  - Mapping instrumentation to services via top n reporting
- Message Quality Improvements
  - Policy data dumps
- Internal Messages
  - Messages related to monitoring “don’t count”

Products Covered

- Acronyms used in this presentation
  - HPOM refers to HP Operations Manager software
    - This is HP’s umbrella for it’s event & perf mgmt software
    - OM An equivalent generic acronym
  - OMW refers to Ops Mgr for Windows
    - OMW Typically 8.x+
    - OVOW Typically 7.x-
  - OMU refers to Ops Mgr for UNIX
    - OMU Typically 9.x and 8.x
    - OML OM for Linux
    - OVOU Typically 8.x and below
  - Legacy Acronyms: OVO, VPO, ITO, OpC

Holistic Approach

Marshall McLuhan

- *“The medium is the message. This is merely to say that the personal and social consequences of any medium - that is, of any extension of ourselves - result from the new scale that is introduced into our affairs by each extension of ourselves, or by any new technology. “*
- *“We shape our tools and afterwards our tools shape us.”*

Holistic Approach

- The tool itself is a not the solution
  - Every business has different monitoring requirements based on a unique corporate mission
  - Tools tuned to meet only the most popular needs
  - Default instrumentation intended to provide examples of monitoring capabilities and potential
  - SPIs add intelligent instrumentation but require deeper investment to map to service objectives
  - Tools typically over-inform on exceptions (duplicates)
  - Autodiscovery policies assume more alerts = better

OVO provides great flexibility and customization entry points but must be "socialized" into the organization order to be effective

Holistic Approach

- "Socialize" the tool
  - Apply People, Process, Technology approach
  - Empower entire staff to engage in event reduction process
  - Create ongoing process to improve instrumentation and reduce message volume
  - Technology should build out on business needs, not product capabilities -Tie monitoring tasks to requirements for service availability
  - Ongoing process should evangelize proactive processes and approaches such as ITIL

Reducing the number of events is easy, but increasing the intelligence of those events at the same time requires close interaction with the owners of the services being managed

Ongoing Process

Ongoing Process

- People - Empower Staff
  - Engage service owners in monitoring improvement
  - Enforce consistent and appropriate methods
  - Encourage quantitative reporting
  - Educate them on Event/Incident/Problem mgmt processes
  - Recognize multivariate aspects of analyses (Tufte)
  - Regular (weekly?) meetings
    - Track action items and assign owners
    - Rotate involvement through various stakeholders

Don’t meet for meeting’s sake – meet to advance the process

Ongoing Process

- Process - Map monitoring requirements to services
  - Establish baseline metrics tied to services
  - Establish event review process inputs and outputs
  - Tie costs for internal processing of events/incidents
  - Review/Update monitoring requirements/SLAs
  - Establish lines of communication with customer
  - Establish goals and set up rewards

Ongoing Process

- Process - Map monitoring requirements to SLAs
  - Are SLA’s tied to KPIs? Are KPIs baselined?
  - Example baselines for analysis
    - Number of alarms being generated (including duplicates) by tools
    - Number of tickets automatically generated
    - Ratio of proactive vs reactive alarms & tickets (use samples)
  - Project ROI
    - Assign a cost to ticket handling and alarm handling
      - Take baseline numbers and estimate overall cost of handling baseline
      - Extra credit: do this for separately for proactive and reactive alarms
    - Determine target message/ticket volume
    - Do the math

Ongoing Process

- Process - Map reporting requirements to SLAs
  - Develop reports that support ongoing processes
    - Reports that relate event mgmt with problem & incident mgmt
    - Top n reports
    - Policy dumps for monitoring instrumentation reviews
  - Service owners should want to be involved.
    - If not, process should be adjusted to show value to them

A good practice is to group or re-word closure codes in the incident management tools to flag proactive versus reactive incidents, then set specific goals for proactive service management

Ongoing Process

- Process - Example Baseline Metrics
  - Events per day
    - What’s really important is events that require action.
  - Example:
    - NNM generates 1000 traps/day, but only node down events launch trouble tickets –all other events are not even looked at in a systems management operation.
  - Distinguish events by time investment (cost)
    - Separate events that launch trouble tickets
    - Separate events that are duplicates or correlated
    - Separate log-only events
    - Separate events related to monitoring (Internal events)

Ongoing Process

- Process - Example Baseline Metrics
  - Events per day
    - What’s really important is events that require action.
  - Example:
    - NNM generates 1000 traps/day, but only node down events launch trouble tickets –all other events are not even looked at in a systems management operation.
  - Distinguish events by time investment (cost)
    - Separate events that launch trouble tickets
    - Separate events that are duplicates or correlated
    - Separate log-only events
    - Separate events related to monitoring (Internal events)

Ongoing Process

- Technology – Prioritize investment in tools
  - Top n reports typically reveal need for adjustments to instrumentation
  - Traditional Message Volume Reduction
    - Deduplication, Message Keys and correlation
  - Mapping service level objectives to instrumentation
    - Policy dumps for mapping monitoring to SLOs reviews
  - Segregate msgs that don’t reflect service availability
    - Filtering out internal messages

Message Volume Reduction

Message Volume Reduction

- Message volume reduction –Tradition methods
  - Server-based duplicate handling (browser config)
    - OOB settings are good
  - Policy-based duplicate message suppression
    - Suppress messages at agent
    - OOB settings not great
  - Message Keys
    - OOB settings OK, but inconsistent across SPIs
    - Biggest opportunities in customized instrumentation
  - Message Storm Handling
    - OOB settings too forgiving of Critical events

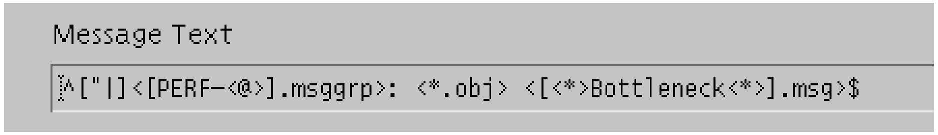
All this is very well documented

Message Volume Reduction

- Message volume reduction –Tradition methods
  - Message Keys
    - Set global de-duplication settings under server config
    - Set message keys for every condition
    - Set message key acknowledgements on clearing and reset conditions
  - Unmatched Messages
    - Consider template settings to not forward them
    - Start by not sending unmatched messages to TT/notif
    - Review unmatched messages in ongoing process

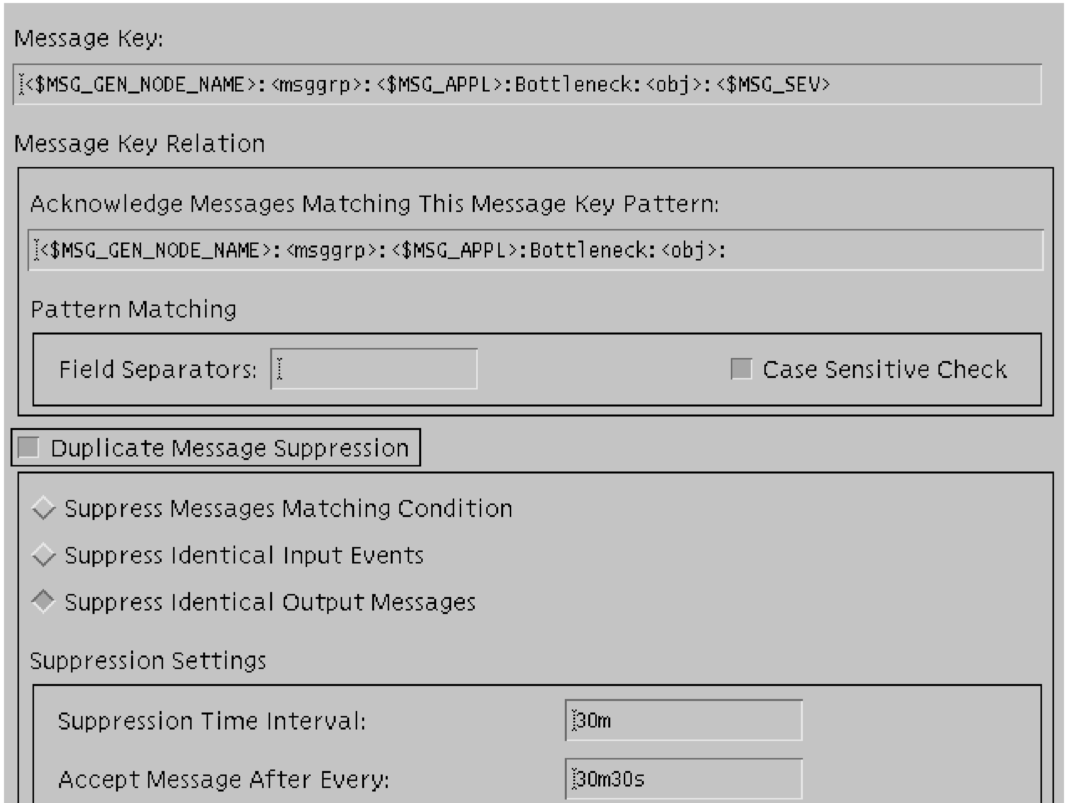
Message Volume Reduction

- OMU Traditional Message volume reduction
  - Traditional message correlation example



Message Text

```
^["|]<[PERF-<@>].msggrp>: <*.obj> <[<*>Bottleneck<*>].msg>$
```



Message Key:

```
<$MSG_GEN_NODE_NAME>:<msggrp>:<$MSG_APPL>:Bottleneck:<obj>:<$MSG_SEV>
```

Message Key Relation

Acknowledge Messages Matching This Message Key Pattern:

```
<$MSG_GEN_NODE_NAME>:<msggrp>:<$MSG_APPL>:Bottleneck:<obj>:
```

Pattern Matching

Field Separators:

□ Case Sensitive Check

□ Duplicate Message Suppression

◇ Suppress Messages Matching Condition

◇ Suppress Identical Input Events

◆ Suppress Identical Output Messages

Suppression Settings

Suppression Time Interval: 30m

Accept Message After Every: 30m30s

Mapping Messages to Services

Mapping Messages to Services

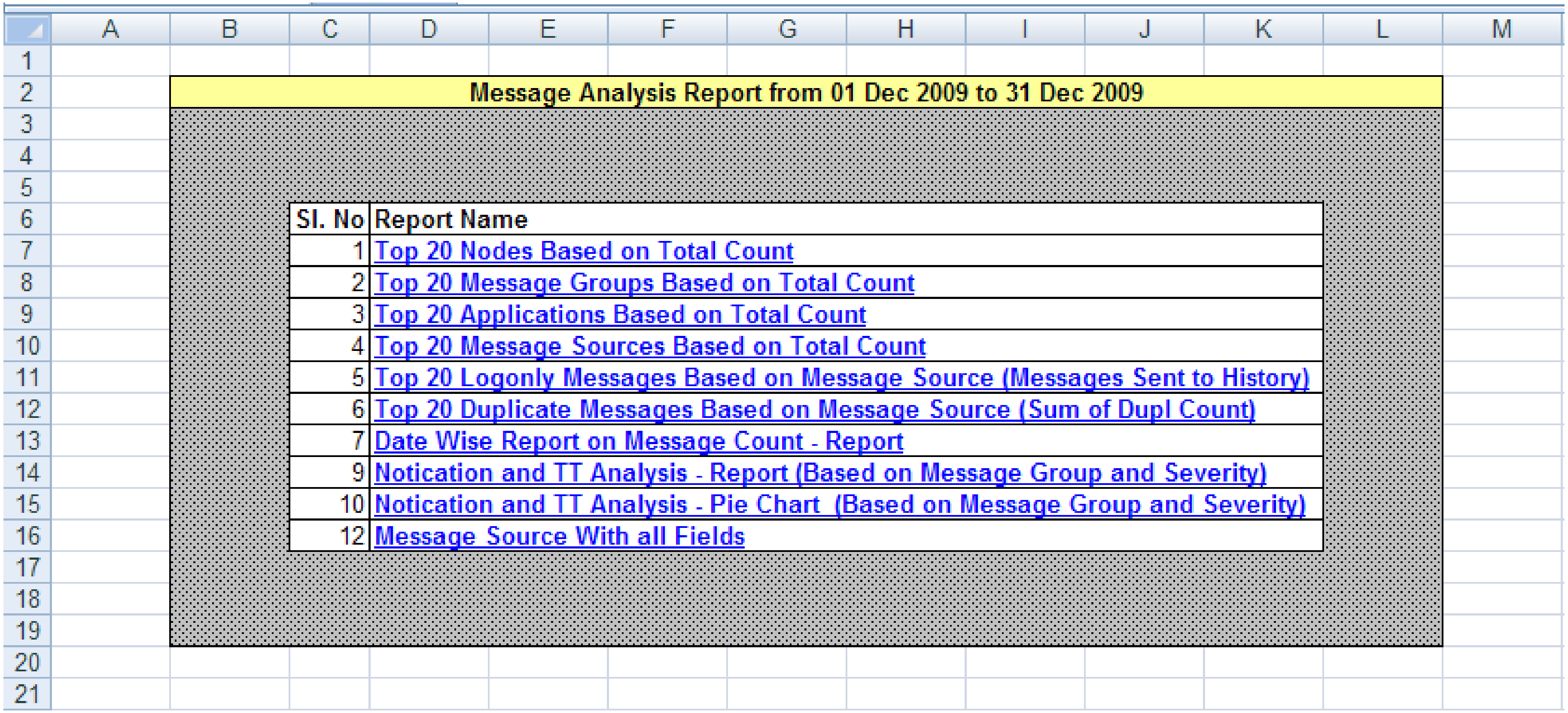
Top n Message Dumps

- Top n Nodes
  - IDs the specific servers generating the most exceptions
- Top n Message Sources (Policies)
  - ID’s the instrumentation responsible for the most msgs
- Top n Duplicate message sources
  - ID’s potential issues with threshold settings
  - IDs excessively verbose logging rules
- Top n Notification/TT generators
  - Chart by Msg Group or Severity or Msg Source

Mapping Messages to Services

Top n Dumps

- Format message dumps in Excel – Summary page

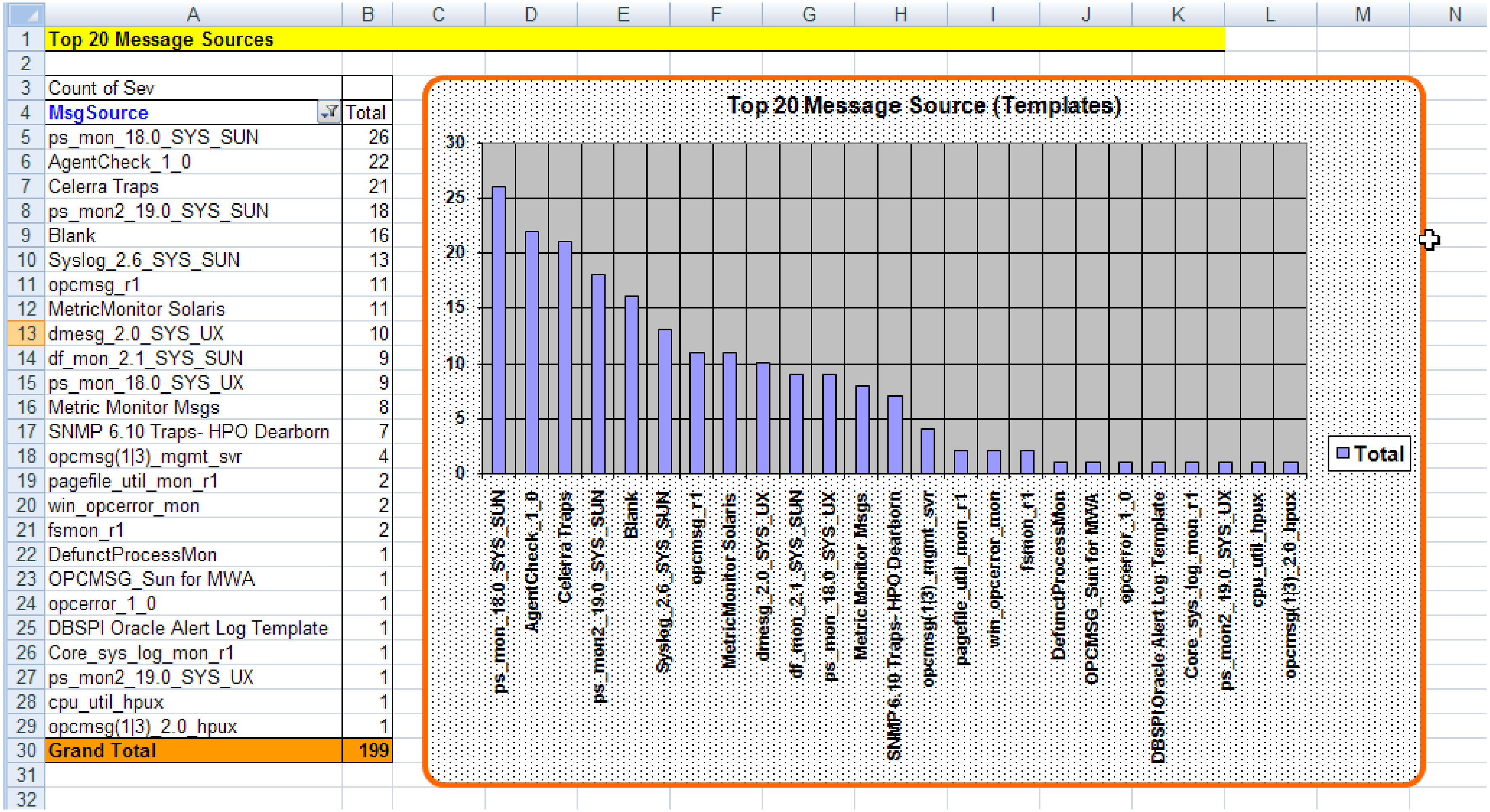


Message Analysis Report from 01 Dec 2009 to 31 Dec 2009

Sl. No	Report Name
1	Top 20 Nodes Based on Total Count
2	Top 20 Message Groups Based on Total Count
3	Top 20 Applications Based on Total Count
4	Top 20 Message Sources Based on Total Count
5	Top 20 Logonly Messages Based on Message Source (Messages Sent to History)
6	Top 20 Duplicate Messages Based on Message Source (Sum of Dupl Count)
7	Date Wise Report on Message Count - Report
9	Notication and TT Analysis - Report (Based on Message Group and Severity)
10	Notication and TT Analysis - Pie Chart (Based on Message Group and Severity)
12	Message Source With all Fields

Mapping Messages to Services

Top n Dumps - Excel example by MsgSource



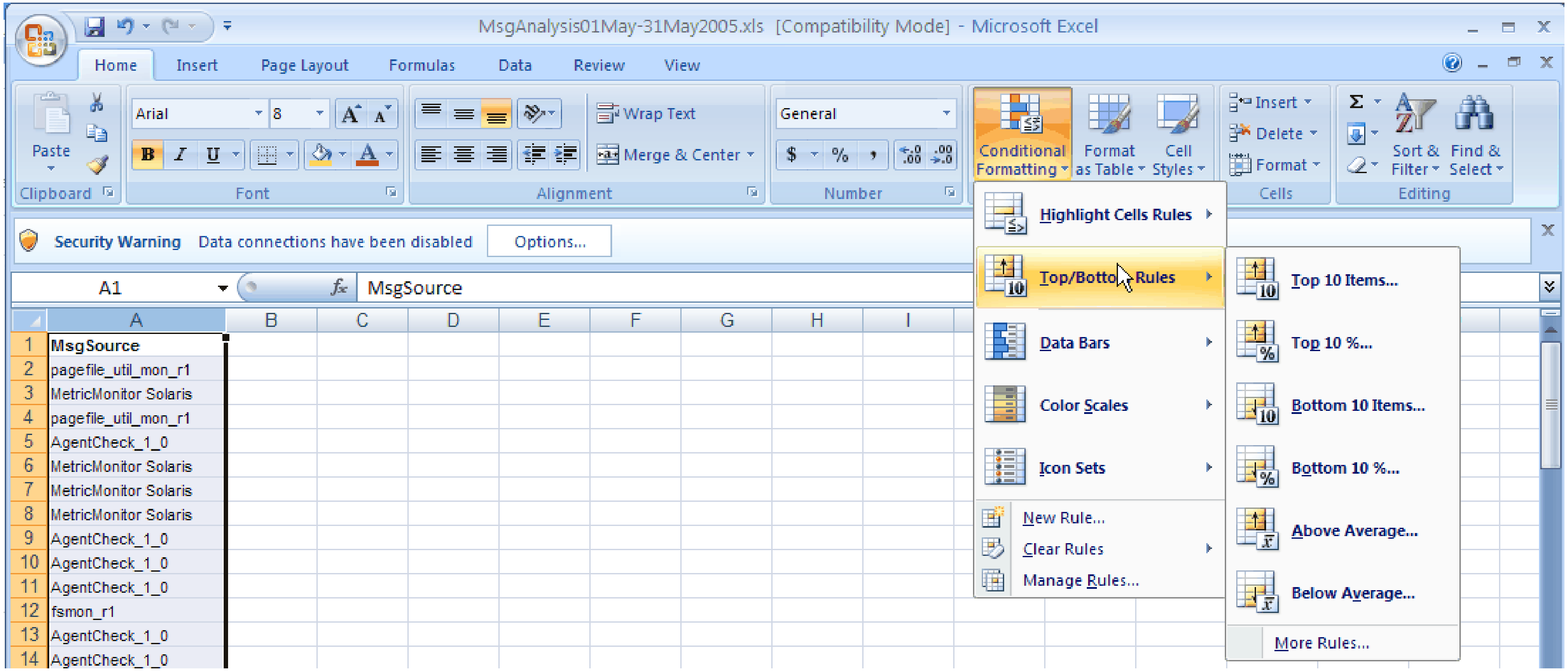
Top 20 Message Sources

Count of Sev	
MsgSource	Total
ps_mon_18.0_SYS_SUN	26
AgentCheck_1_0	22
Celerra Traps	21
ps_mon2_19.0_SYS_SUN	18
Blank	16
Syslog_2.6_SYS_SUN	13
opcmsg_r1	11
MetricMonitor Solaris	11
dmesg_2.0_SYS_UX	10
df_mon_2.1_SYS_SUN	9
ps_mon_18.0_SYS_UX	9
Metric Monitor Msgs	8
SNMP 6.10 Traps- HPO Dearborn	7
opcmsg(1|3)_mgmt_svr	4
pagefile_util_mon_r1	2
win_opcerror_mon	2
fsmon_r1	2
DefunctProcessMon	1
OPCMSG_Sun for MWA	1
opcerror_1_0	1
DBSPI Oracle Alert Log Template	1
Core_sys_log_mon_r1	1
ps_mon2_19.0_SYS_UX	1
cpu_util_hpux	1
opcmsg(1|3)_2.0_hpux	1
Grand Total	**199**

Mapping Messages to Services

Top n Dumps

- Format message dumps in Excel – Top 20
  - Home – Conditional Formatting – Top/Bottom Rules



MsgAnalysis01May-31May2005.xls [Compatibility Mode] - Microsoft Excel

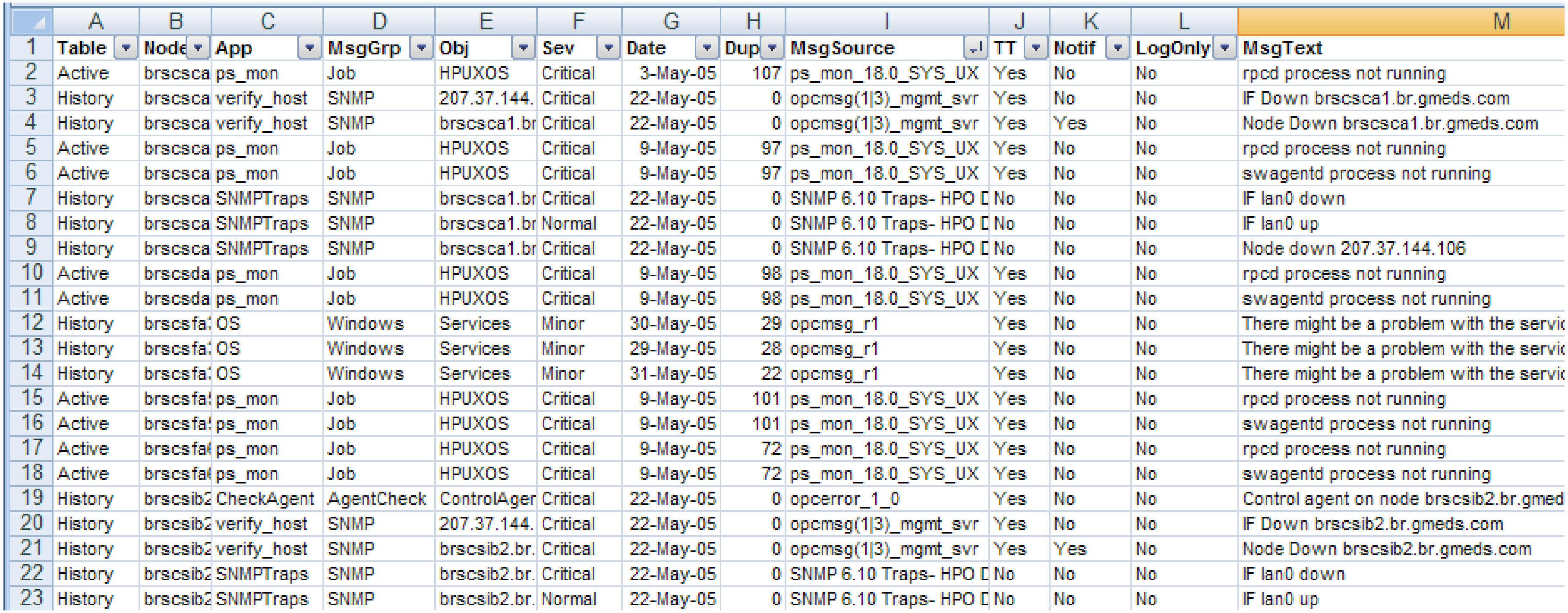
Security Warning Data connections have been disabled

A1 MsgSource

	A
1	MsgSource
2	pagefile_util_mon_r1
3	MetricMonitor Solaris
4	pagefile_util_mon_r1
5	AgentCheck_1_0
6	MetricMonitor Solaris
7	MetricMonitor Solaris
8	MetricMonitor Solaris
9	AgentCheck_1_0
10	AgentCheck_1_0
11	AgentCheck_1_0
12	fsmon_r1
13	AgentCheck_1_0
14	AgentCheck_1_0

Mapping Messages to Services

- Top n Dumps Excel – example raw data set
  - Table, Node, Appl, MsgGrp, Obj, Sev, Date, Duplicates, Msg Source, TT Flag, Notif Flag, LogOnly flag, Msg Text



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Table	Node	App	MsgGrp	Obj	Sev	Date	Dup	MsgSource	TT	Notif	LogOnly	MsgText
2	Active	brscsca	ps_mon	Job	HPUXOS	Critical	3-May-05	107	ps_mon_18.0_SYS_UX	Yes	No	No	rpcd process not running
3	History	brscsca	verify_host	SNMP	207.37.144.	Critical	22-May-05	0	opcmsg(1|3)_mgmt_svr	Yes	No	No	IF Down brscsca1.br.gmeds.com
4	History	brscsca	verify_host	SNMP	brscsca1.br	Critical	22-May-05	0	opcmsg(1|3)_mgmt_svr	Yes	Yes	No	Node Down brscsca1.br.gmeds.com
5	Active	brscsca	ps_mon	Job	HPUXOS	Critical	9-May-05	97	ps_mon_18.0_SYS_UX	Yes	No	No	rpcd process not running
6	Active	brscsca	ps_mon	Job	HPUXOS	Critical	9-May-05	97	ps_mon_18.0_SYS_UX	Yes	No	No	swagentd process not running
7	History	brscsca	SNMPTraps	SNMP	brscsca1.br	Critical	22-May-05	0	SNMP 6.10 Traps- HPO D	No	No	No	IF lan0 down
8	History	brscsca	SNMPTraps	SNMP	brscsca1.br	Normal	22-May-05	0	SNMP 6.10 Traps- HPO D	No	No	No	IF lan0 up
9	History	brscsca	SNMPTraps	SNMP	brscsca1.br	Critical	22-May-05	0	SNMP 6.10 Traps- HPO D	No	No	No	Node down 207.37.144.106
10	Active	brscsda	ps_mon	Job	HPUXOS	Critical	9-May-05	98	ps_mon_18.0_SYS_UX	Yes	No	No	rpcd process not running
11	Active	brscsda	ps_mon	Job	HPUXOS	Critical	9-May-05	98	ps_mon_18.0_SYS_UX	Yes	No	No	swagentd process not running
12	History	brscsfa	OS	Windows	Services	Minor	30-May-05	29	opcmsg_r1	Yes	No	No	There might be a problem with the servic
13	History	brscsfa	OS	Windows	Services	Minor	29-May-05	28	opcmsg_r1	Yes	No	No	There might be a problem with the servic
14	History	brscsfa	OS	Windows	Services	Minor	31-May-05	22	opcmsg_r1	Yes	No	No	There might be a problem with the servic
15	Active	brscsfa	ps_mon	Job	HPUXOS	Critical	9-May-05	101	ps_mon_18.0_SYS_UX	Yes	No	No	rpcd process not running
16	Active	brscsfa	ps_mon	Job	HPUXOS	Critical	9-May-05	101	ps_mon_18.0_SYS_UX	Yes	No	No	swagentd process not running
17	Active	brscsfa	ps_mon	Job	HPUXOS	Critical	9-May-05	72	ps_mon_18.0_SYS_UX	Yes	No	No	rpcd process not running
18	Active	brscsfa	ps_mon	Job	HPUXOS	Critical	9-May-05	72	ps_mon_18.0_SYS_UX	Yes	No	No	swagentd process not running
19	History	brscsib2	CheckAgent	AgentCheck	ControlAger	Critical	22-May-05	0	opcerror_1_0	Yes	No	No	Control agent on node brscsib2.br.gmed
20	History	brscsib2	verify_host	SNMP	207.37.144.	Critical	22-May-05	0	opcmsg(1|3)_mgmt_svr	Yes	No	No	IF Down brscsib2.br.gmeds.com
21	History	brscsib2	verify_host	SNMP	brscsib2.br.	Critical	22-May-05	0	opcmsg(1|3)_mgmt_svr	Yes	Yes	No	Node Down brscsib2.br.gmeds.com
22	History	brscsib2	SNMPTraps	SNMP	brscsib2.br.	Critical	22-May-05	0	SNMP 6.10 Traps- HPO D	No	No	No	IF lan0 down
23	History	brscsib2	SNMPTraps	SNMP	brscsib2.br.	Normal	22-May-05	0	SNMP 6.10 Traps- HPO D	No	No	No	IF lan0 up

Mapping Messages to Services

Top n Dumps Excel – example SQL – UNIX - Active

```
SET HEADING ON ECHO OFF PAGESIZE 0 LINESIZE 1000
 SET FEEDBACK OFF VERIFY OFF NEWPAGE 0
 SELECT 'Active' || '@@'|| m3.node_name || '@@' || m1.application || '@@'
         || m1.message_group || '@@' || m1.object || '@@'
         || DECODE(m1.severity,1,'Unknown',2,'Normal',4,'Warning',8,
            'Critical',16,'Minor',32,'Major') || '@@'
         || to_char(m1.local_receiving_time, 'DD-Mon-YYYY') || '@@'
         || m1.dupl_count || '@@' || m1.msg_source_name || '@@'
         || DECODE(m1.trouble_tick_flag,1,'Yes',0,'No') || '@@'
         || DECODE(m1.notification_flag,1,'Yes',0,'No') || '@@'
         || 'No' || '@@' || substr(m2.text_part,1,60)
 FROM opc_op.opc_act_messages m1, opc_op.opc_msg_text m2,
      opc_op.opc_node_names m3
 WHERE  m1.message_number = m2.message_number and m1.node_id = m3.node_id
        AND to_char(m1.local_receiving_time, 'DD-Mon-YYYY')
        BETWEEN to_date('&1') AND to_date('&2')
 ORDER BY to_char(m1.local_receiving_time, 'DD-Mon-YYYY');
 EXIT;
```

Mapping Messages to Services

Top n Dumps Excel – example SQL – UNIX - History

```
SET HEADING ON ECHO OFF PAGESIZE 0 LINESIZE 1000
SET FEEDBACK OFF VERIFY OFF NEWPAGE 0
SELECT 'History' || '@@` || m3.node_name || '@@` || m1.application || '@@'
       || m1.message_group || '@@` || m1.object || '@@'
       || DECODE(m1.severity,1,'Unknown',2,'Normal',4,'Warning',8,
          'Critical',16,'Minor',32,'Major') || '@@'
       || to_char(m1.local_receiving_time, 'DD-Mon-YYYY') || '@@'
       || m1.dupl_count || '@@` || m1.msg_source_name || '@@'
       || DECODE(m1.trouble_tick_flag,1,'Yes',0,'No') || '@@'
       || DECODE(m1.notification_flag,1,'Yes',0,'No') || '@@'
       || DECODE(m1.log_only_flag,1,'Yes',0,'No') || '@@'
       || substr(m2.text_part,1,60)
   from   opc_op.opc_hist_messages m1, opc_op.opc_hist_msg_text m2,
          opc_op.opc_node_names m3
WHERE m1.message_number = m2.message_number AND m1.node_id = m3.node_id
      AND to_char(m1.local_receiving_time, 'DD-Mon-YYYY')
      BETWEEN to_date('&1') and to_date('&2')
ORDER BY to_char(m1.local_receiving_time, 'DD-Mon-YYYY');
EXIT;
```

Mapping Messages to Services

Top n Dumps Excel – example SQL – Windows

```
SELECT CASE State WHEN 2 THEN 'Active' WHEN 4 THEN 'History' END,
   SUBSTRING(b.object_text,PATINDEX('%PrimaryNodeName%',
      b.object_text) + 19, PATINDEX('%;%',SUBSTRING(b.object_text,
      PATINDEX('%PrimaryNodeName%', b.object_text) + 19, 253)) - 2),
   Application, MessageGroup, Object,
   CASE Severity WHEN 1 THEN 'Unknown' WHEN 2 THEN 'Normal'
      WHEN 4 THEN 'Warning' WHEN 8 THEN 'Critical' WHEN 16 THEN 'Minor'
      WHEN 32 THEN 'Major‘  END,
    TimeCreatedTimeStamp, NumberOfDuplicates, Source,
    CASE DoNotification WHEN 0 THEN 'No' WHEN 1 THEN 'Yes' END,
    CASE LogOnly WHEN 0 THEN 'No' WHEN 1 THEN 'Yes' END, Text
FROM dbo.OV_MS_Message a, ovms_admin.sto_ov_managednode b
WHERE a.NodeName = b.name
   and TimeCreated > $Start and TimeCreated < $EndTime
   ORDER BY a.TimeCreated
```

```
sqlcmd -S .\OVOPS -E -d openview -h -1 -W -s "@@" -Q "$SQL"
```

Mapping Messages to Services

Top n Reports via SQL instead of Excel

- Top 20 Policies by Message Volume (Active)

Windows (Sequel)

```
SELECT top 20 Source, count(distinct id)
FROM ov_ms_message
WHERE State = 2
GROUP BY Source ORDER BY 2 DESC;
```

UNIX (Oracle)

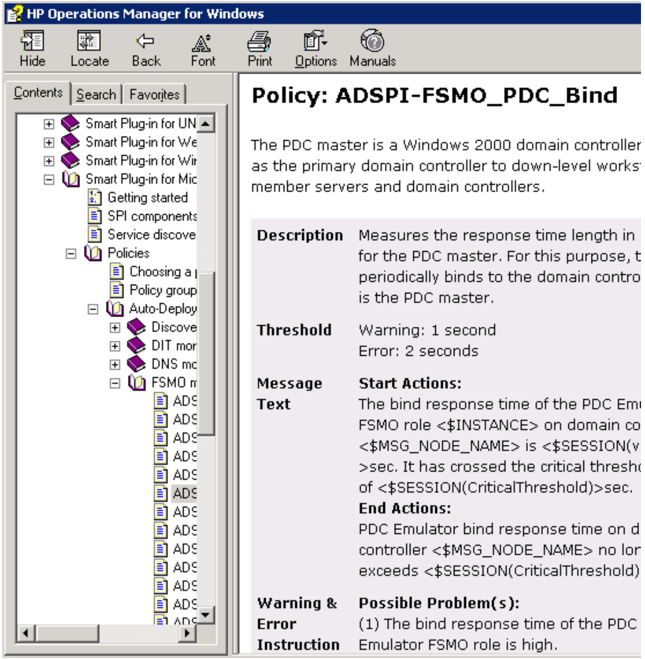
```
SELECT msg_source_name, COUNT(msg_source_name)
FROM (SELECT msg_source_name FROM opc_op.opc_act_messages
ORDER BY COUNT(msg_source_name) DESC)
WHERE ROWNUM <= 20;
```

Message Quality Improvements

Message Quality Improvements

- Policy Data Dumps - Windows
  - Available in online help but Inconsistent across SPIs
  - Granularity variable (no details on conditions/rules)
  - Static – OOB, not reflective of customizations

ADSPI



Policy: ADSPI-FSMO_PDC_Bind

The PDC master is a Windows 2000 domain controller
as the primary domain controller to down-level works
member servers and domain controllers.

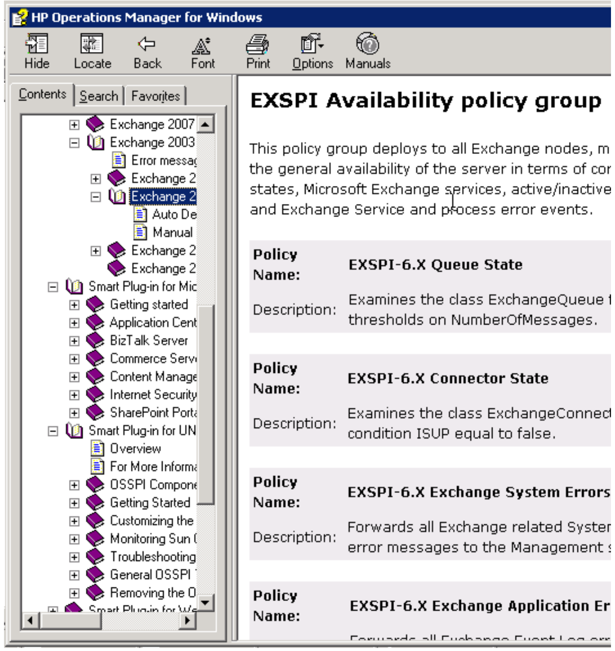
Description Measures the response time length in
for the PDC master. For this purpose, t
periodically binds to the domain contro
is the PDC master.

Threshold Warning: 1 second
Error: 2 seconds

Message Text **Start Actions:**
The bind response time of the PDC Em
FSMO role <$INSTANCE> on domain co
<$MSG_NODE_NAME> is <$SESSION(
>sec. It has crossed the critical thresh
of <$SESSION(CriticalThreshold)>sec.
End Actions:
PDC Emulator bind response time on d
controller <$MSG_NODE_NAME> no lo
exceeds <$SESSION(CriticalThreshold)

Warning & Error Instruction **Possible Problem(s):**
(1) The bind response time of the PDC
Emulator FSMO role is high.

EXSPI



EXSPI Availability policy group

This policy group deploys to all Exchange nodes, m
the general availability of the server in terms of co
states, Microsoft Exchange services, active/inactive
and Exchange Service and process error events.

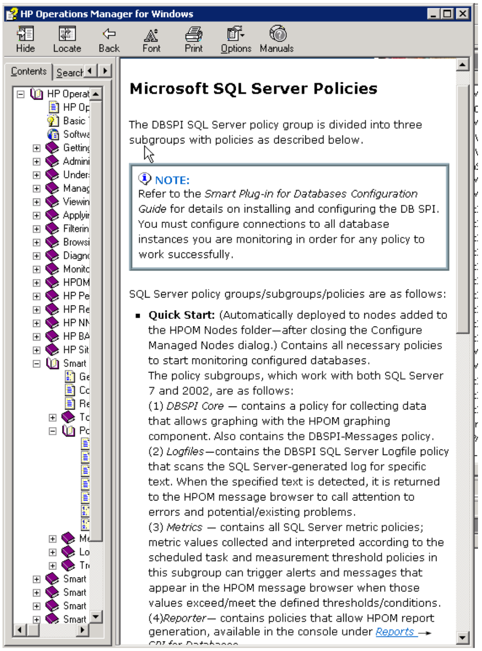
Policy Name: **EXSPI-6.X Queue State**
Description: Examines the class ExchangeQueue
thresholds on NumberOfMessages.

Policy Name: **EXSPI-6.X Connector State**
Description: Examines the class ExchangeConnec
condition ISUP equal to false.

Policy Name: **EXSPI-6.X Exchange System Errors**
Description: Forwards all Exchange related Syste
error messages to the Management

Policy Name: **EXSPI-6.X Exchange Application Er**

DBSPI



Microsoft SQL Server Policies

The DBSPI SQL Server policy group is divided into three subgroups with policies as described below.

NOTE:
Refer to the *Smart Plug-in for Databases Configuration Guide* for details on installing and configuring the DB SPI. You must configure connections to all database instances you are monitoring in order for any policy to work successfully.

SQL Server policy groups/subgroups/policies are as follows:

- **Quick Start:** (Automatically deployed to nodes added to the HPOM Nodes folder—after closing the Configure Managed Nodes dialog.) Contains all necessary policies to start monitoring configured databases.
  The policy subgroups, which work with both SQL Server 7 and 2002, are as follows:
  (1) *DBSPI Core* — contains a policy for collecting data that allows graphing with the HPOM graphing component. Also contains the DBSPI-Messages policy.
  (2) *Logfiles*—contains the DBSPI SQL Server Logfile policy that scans the SQL Server-generated log for specific text. When the specified text is detected, it is returned to the HPOM message browser to call attention to errors and potential/existing problems.
  (3) *Metrics* — contains all SQL Server metric policies; metric values collected and interpreted according to the scheduled task and measurement threshold policies in this subgroup can trigger alerts and messages that appear in the HPOM message browser when those values exceed/meet the defined thresholds/conditions.
  (4)*Reporter*— contains policies that allow HPOM report generation, available in the console under Reports →

Message Quality Improvements

- OM Policy Dumps – Why are they important?
  - Excellent templates for defining service metrics
    - KPI’s should be tied to real service availability measures
  - Key resource for proactive service management
    - Process: Map policy rules to reactive/historical incidents
    - Service Owners can better understand monitoring capabilities
  - Documentation
    - Dumps show exactly what is and what isn’t being monitored
    - OM admins can use dumps to baseline or track changes

Message Quality Improvements

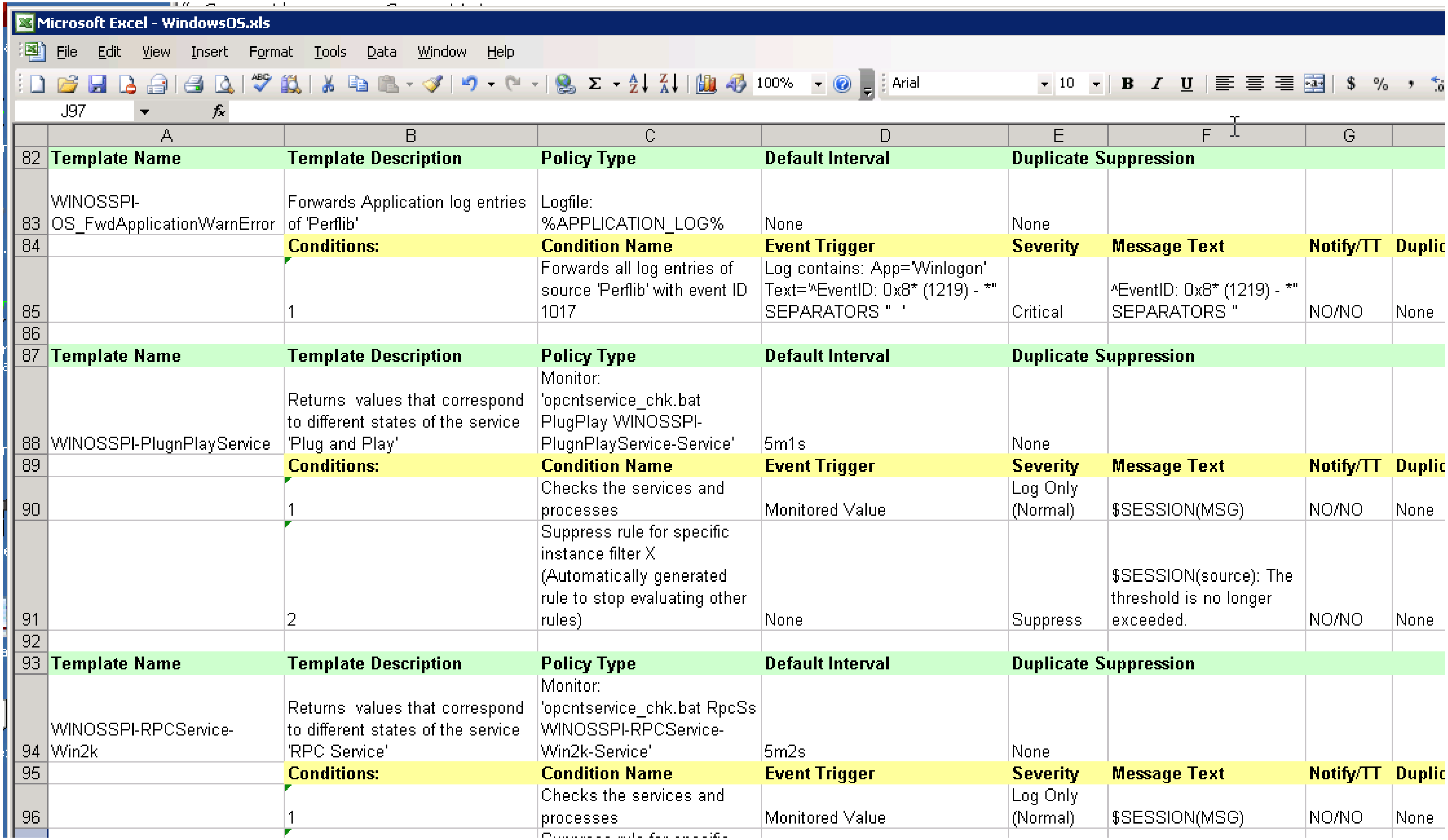
- OM Policy Dumps – Use in Ongoing Processes
  - Service Owner's Tasks
    - Suppress rules of no concern/Add rules of great concern
    - Suggest updates to thresholds/intervals to reduce volume
    - Map criticality to service availability and/or proactiveness
    - Identify rules that should launch Tickets or Notifications
    - Suggest automated/Operator actions & Operator Instructions
  - OM Admin Tasks
    - ID rules needing duplicate message suppression
    - ID rules needing Message Keys
    - IF rules needing more complex correlation

Message Quality Improvements

- OM Policy Dumps – Why are they problematic?
  - Instrumentation nearly impossible to report on
    - Many policies are based on dynamic scripts
    - Different policy types have different attributes
    - There are a gazillion attributes
  - Admins change policies frequently

Message Quality Improvements

Example Script-based Policy Dump



	A	B	C	D	E	F	G	
82	**Template Name**	**Template Description**	**Policy Type**	**Default Interval**	**Duplicate Suppression**			
83	WINOSSPI-OS_FwdApplicationWarnError	Forwards Application log entries of 'Perflib'	Logfile: %APPLICATION_LOG%	None	None			
84		**Conditions:**	**Condition Name**	**Event Trigger**	**Severity**	**Message Text**	**Notify/TT**	**Duplic**
85		1	Forwards all log entries of source 'Perflib' with event ID 1017	Log contains: App='Winlogon' Text='^EventID: 0x8* (1219) - *" SEPARATORS " '	Critical	^EventID: 0x8* (1219) - *" SEPARATORS "	NO/NO	None
86								
87	**Template Name**	**Template Description**	**Policy Type**	**Default Interval**	**Duplicate Suppression**			
88	WINOSSPI-PlugnPlayService	Returns values that correspond to different states of the service 'Plug and Play'	Monitor: 'opcntservice_chk.bat PlugPlay WINOSSPI-PlugnPlayService-Service'	5m1s	None			
89		**Conditions:**	**Condition Name**	**Event Trigger**	**Severity**	**Message Text**	**Notify/TT**	**Duplic**
90		1	Checks the services and processes	Monitored Value	Log Only (Normal)	$SESSION(MSG)	NO/NO	None
91		2	Suppress rule for specific instance filter X (Automatically generated rule to stop evaluating other rules)	None	Suppress	$SESSION(source): The threshold is no longer exceeded.	NO/NO	None
92								
93	**Template Name**	**Template Description**	**Policy Type**	**Default Interval**	**Duplicate Suppression**			
94	WINOSSPI-RPCService-Win2k	Returns values that correspond to different states of the service 'RPC Service'	Monitor: 'opcntservice_chk.bat RpcSs WINOSSPI-RPCService-Win2k-Service'	5m2s	None			
95		**Conditions:**	**Condition Name**	**Event Trigger**	**Severity**	**Message Text**	**Notify/TT**	**Duplic**
96		1	Checks the services and processes	Monitored Value	Log Only (Normal)	$SESSION(MSG)	NO/NO	None
			Suppress rule for specific					

Message Quality Improvements

Policy dump scripts

- Outline of script functions
  - Example (last slide) (Win): www.fognet.com/ovowDumpPol.pl
  - Windows:
    - ovpmutil cfg pol dnl <targetDir> /p \<PolicyGroupName>
    - ovpmutil PCV \/x \"<file>\“ on each binary dump file\
  - UNIX:
    - Use opcpolicy in 9.x+ Use opctempl or opccgfdwn in 8.x and below
  - Massage text data & output to Excel .xlsx (Requires 2003+)
- Advantages/Disadvantages

  + Customizable to the fields of most interest

  + Shows an entire policy group’s instrumentation details

  - Doesn’t capture details embedded in launched scripts

  - Almost impossible to present so much data cleanly

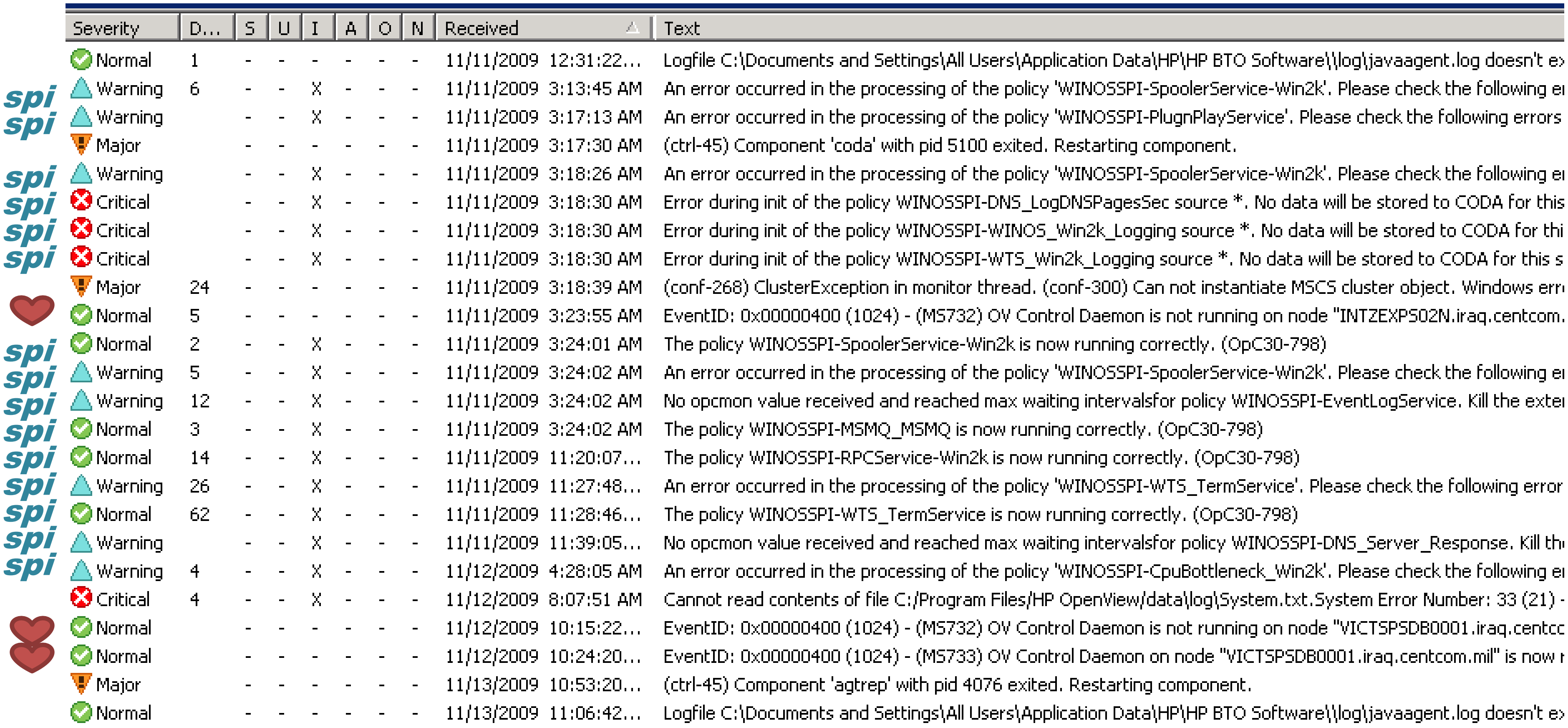
Internal Messages

Internal Messages

- Service Management challenges
  - Need to separate events related to monitoring infrastructure from service-related events
  - SLA, top n and other message-related reports skewed by excessive alerts related to monitoring infrastructure
- Operations challenges
  - Operators focus on infrastructure exceptions vs. production because internal alerts show up in their views
  - OM Administrators have difficulties because of mixing of internal alerts with production alerts
- Solution
  - Filter out and redirect internal alarms
    - Only OM admins see internal alarms
    - Internal messages can then be eliminated from reports

Internal Messages

- Example OMW OOB Messages - Internal Messages



	Severity	D...	S	U	I	A	O	N	Received	Text
	✓ Normal	1	-	-	-	-	-	-	11/11/2009 12:31:22...	Logfile C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\\log\javaagent.log doesn't ex
spi	Warning	6	-	-	X	-	-	-	11/11/2009 3:13:45 AM	An error occurred in the processing of the policy 'WINOSSPI-SpoolerService-Win2k'. Please check the following er
spi	Warning		-	-	X	-	-	-	11/11/2009 3:17:13 AM	An error occurred in the processing of the policy 'WINOSSPI-PlugnPlayService'. Please check the following errors
	Major		-	-	-	-	-	-	11/11/2009 3:17:30 AM	(ctrl-45) Component 'coda' with pid 5100 exited. Restarting component.
spi	Warning		-	-	X	-	-	-	11/11/2009 3:18:26 AM	An error occurred in the processing of the policy 'WINOSSPI-SpoolerService-Win2k'. Please check the following er
spi	☒ Critical		-	-	X	-	-	-	11/11/2009 3:18:30 AM	Error during init of the policy WINOSSPI-DNS_LogDNSPagesSec source *. No data will be stored to CODA for this
spi	☒ Critical		-	-	X	-	-	-	11/11/2009 3:18:30 AM	Error during init of the policy WINOSSPI-WINOS_Win2k_Logging source *. No data will be stored to CODA for thi
spi	☒ Critical		-	-	X	-	-	-	11/11/2009 3:18:30 AM	Error during init of the policy WINOSSPI-WTS_Win2k_Logging source *. No data will be stored to CODA for this s
	Major	24	-	-	-	-	-	-	11/11/2009 3:18:39 AM	(conf-268) ClusterException in monitor thread. (conf-300) Can not instantiate MSCS cluster object. Windows err
♥	✓ Normal	5	-	-	-	-	-	-	11/11/2009 3:23:55 AM	EventID: 0x00000400 (1024) - (MS732) OV Control Daemon is not running on node "INTZEXPS02N.iraq.centcom.
spi	✓ Normal	2	-	-	X	-	-	-	11/11/2009 3:24:01 AM	The policy WINOSSPI-SpoolerService-Win2k is now running correctly. (OpC30-798)
spi	Warning	5	-	-	X	-	-	-	11/11/2009 3:24:02 AM	An error occurred in the processing of the policy 'WINOSSPI-SpoolerService-Win2k'. Please check the following er
spi	Warning	12	-	-	X	-	-	-	11/11/2009 3:24:02 AM	No opcmon value received and reached max waiting intervalsfor policy WINOSSPI-EventLogService. Kill the exter
spi	✓ Normal	3	-	-	X	-	-	-	11/11/2009 3:24:02 AM	The policy WINOSSPI-MSMQ_MSMQ is now running correctly. (OpC30-798)
spi	✓ Normal	14	-	-	X	-	-	-	11/11/2009 11:20:07...	The policy WINOSSPI-RPCService-Win2k is now running correctly. (OpC30-798)
spi	Warning	26	-	-	X	-	-	-	11/11/2009 11:27:48...	An error occurred in the processing of the policy 'WINOSSPI-WTS_TermService'. Please check the following error
spi	✓ Normal	62	-	-	X	-	-	-	11/11/2009 11:28:46...	The policy WINOSSPI-WTS_TermService is now running correctly. (OpC30-798)
spi	Warning		-	-	X	-	-	-	11/11/2009 11:39:05...	No opcmon value received and reached max waiting intervalsfor policy WINOSSPI-DNS_Server_Response. Kill th
spi	Warning	4	-	-	X	-	-	-	11/12/2009 4:28:05 AM	An error occurred in the processing of the policy 'WINOSSPI-CpuBottleneck_Win2k'. Please check the following er
	☒ Critical	4	-	-	X	-	-	-	11/12/2009 8:07:51 AM	Cannot read contents of file C:/Program Files/HP OpenView/data\log\System.txt.System Error Number: 33 (21) -
♥	✓ Normal		-	-	-	-	-	-	11/12/2009 10:15:22...	EventID: 0x00000400 (1024) - (MS732) OV Control Daemon is not running on node "VICTSPSDB0001.iraq.centco
♥	✓ Normal		-	-	-	-	-	-	11/12/2009 10:24:20...	EventID: 0x00000400 (1024) - (MS733) OV Control Daemon on node "VICTSPSDB0001.iraq.centcom.mil" is now r
	Major		-	-	-	-	-	-	11/13/2009 10:53:20...	(ctrl-45) Component 'agtrep' with pid 4076 exited. Restarting component.
	✓ Normal		-	-	-	-	-	-	11/13/2009 11:06:42...	Logfile C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\\log\javaagent.log doesn't ex

Internal Messages

Internal Message Handling Strategies - Windows

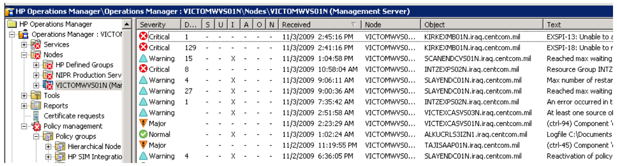
1. **Internal filtering based on Msg Groups**
   - User roles have explicit list of valid Message Groups
   - Easiest to set up and maintain
   - Problems with missed messages, ongoing admin & customizations
2. **Internal filtering based on WMI Policy**
   - Internal messages redirected to a non-production Node
   - Or, internal messages automatically acknowledged
   - Server WMI Policy filters all agent and server-based internal msgs
   - Agents are NOT individually configured to filter internal messages
   - Fewer problems with missed msgs & future customizations
   - Initial setup harder but ongoing administration is easier

Internal Messages

Internal Message Handling Strategies - UNIX

1. **Internal filtering based on Msg Groups**
   - User roles have explicit list of valid Message Groups
   - Easiest to set up and maintain
   - Problems with missed messages, ongoing admin & customizations
2. **Internal filtering based on Agent Config/opcmsg policy**
   - Internal messages redirected to a non-production Node
   - Or, internal messages automatically acknowledged
   - Server and agents configured to filter internal messages
   - Customized opcmsg policy defines event handling
   - Fewer problems with missed msgs & future customizations
3. **Server-based ECS Circuit – Requires ECS Designer**

Internal Messages

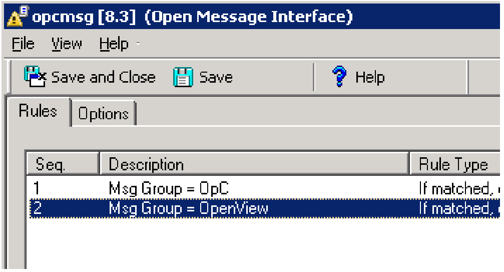


HP Operations Manager\Operations Manager : VICTOMWVS01N\Nodes\VICTOMWVS01N (Management Server)

- HP Operations Manager
  - Operations Manager : VICTO
    - Services
    - Nodes
      - HP Defined Groups
      - NIPR Production Serv
      - VICTOMWVS01N (Mar
    - Tools
    - Reports
    - Certificate requests
    - Policy management
      - Policy groups
        - Hierarchical Node
        - HP SIM Integratio

Severity	D...	S	U	I	A	O	N	Received	Node	Object	Text
Critical	1	-	-	-	-	-	-	11/3/2009 2:45:16 PM	VICTOMWVS0...	KIRKEXMB01N.iraq.centcom.mil	EXSPI-13: Unable to a
Critical	129	-	-	-	-	-	-	11/3/2009 2:41:16 PM	VICTOMWVS0...	KIRKEXMB01N.iraq.centcom.mil	EXSPI-18: Unable to r
Warning	15	-	-	X	-	-	-	11/3/2009 1:04:58 PM	VICTOMWVS0...	SCANENDCVS01N.iraq.centcom.mil	Reached max waiting
Critical	8	-	-	-	-	-	-	11/3/2009 10:58:04 AM	VICTOMWVS0...	INTZEXPS02N.iraq.centcom.mil	Resource Group INTZ
Warning	4	-	-	X	-	-	-	11/3/2009 9:06:11 AM	VICTOMWVS0...	SLAYENDC01N.iraq.centcom.mil	Max number of restar
Warning	27	-	-	X	-	-	-	11/3/2009 9:00:36 AM	VICTOMWVS0...	SLAYENDC01N.iraq.centcom.mil	Reached max waiting
Warning	1	-	-	X	-	-	-	11/3/2009 7:35:42 AM	VICTOMWVS0...	INTZEXPS02N.iraq.centcom.mil	An error occurred in t
Warning		-	-	X	-	-	-	11/3/2009 2:51:58 AM	VICTOMWVS0...	VICTEXCASVS03N.iraq.centcom.mil	At least one source of
Major		-	-	-	-	-	-	11/3/2009 2:23:29 AM	VICTOMWVS0...	VICTEXCASVS01N.iraq.centcom.mil	(ctrl-94) Component '
Normal		-	-	X	-	-	-	11/3/2009 1:02:24 AM	VICTOMWVS0...	ALKUCRLS3IZN1.iraq.centcom.mil	Logfile C:\Documents
Major		-	-	-	-	-	-	11/2/2009 11:19:55 PM	VICTOMWVS0...	TAJISAAP01N.iraq.centcom.mil	(ctrl-45) Component '
Warning	4	-	-	X	-	-	-	11/2/2009 6:36:05 PM	VICTOMWVS0...	SLAYENDC01N.iraq.centcom.mil	Reactivation of policy

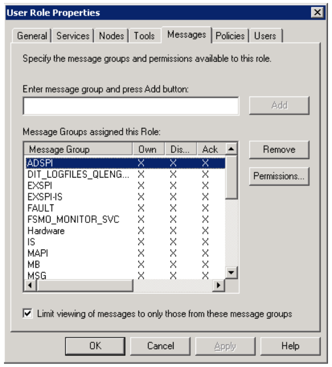
Filtered internal message view



opcmsg [8.3] (Open Message Interface)

Seq.	Description	Rule Type
1	Msg Group = OpC	If matched,
2	Msg Group = OpenView	If matched,

Internal msg filter & opcmsg policy



User Role Properties

Specify the message groups and permissions available to this role.

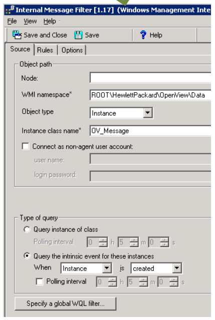
Enter message group and press Add button:

Message Groups assigned this Role:

Message Group	Own	Dis...	Ack
ADSPI	X	X	X
DIT_LOGFILES_QLENG...	X	X	X
EXSPI	X	X	X
EXSPI-IS	X	X	X
FAULT	X	X	X
FSMO_MONITOR_SVC	X	X	X
Hardware	X	X	X
IS	X	X	X
MAPI	X	X	X
MB	X	X	X
MSG	X	X	X

☑ Limit viewing of messages to only those from these message groups

User roles based on msg groups



Internal Message Filter [1.17] (Windows Management Inte

Object path

Node:

WMI namespace* ROOT\HewlettPackard\OpenView\Data

Object type Instance

Instance class name* OV_Message

☐ Connect as non-agent user account:

user name:

login password:

Type of query

○ Query instance of class

Polling interval 0 h 5 m 0 s

● Query the intrinsic event for these instances

When Instance is created

☐ Polling interval 0 h 5 m 0 s

WMI Policy

or

Server only

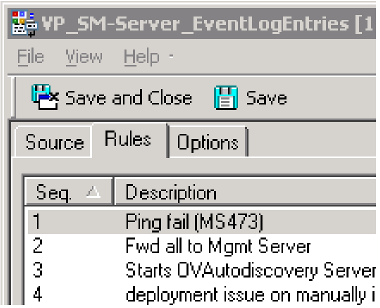
OMW

or

All agents

OMU

Server only



VP_SM-Server_EventLogEntries [1

Seq.	Description
1	Ping fail (MS473)
2	Fwd all to Mgmt Server
3	Starts OVAutodiscovery Server
4	deployment issue on manually i

Event Log Policy

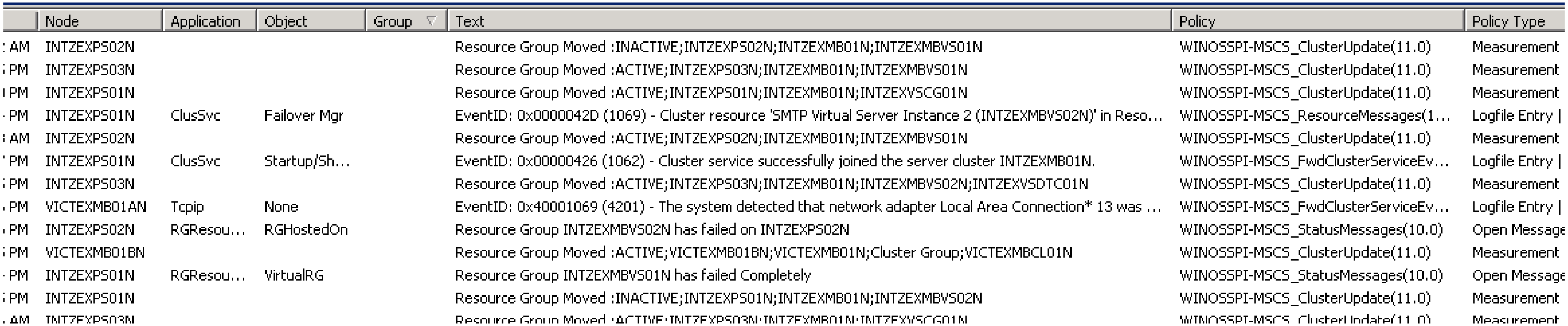
Server only

Heartbeat msgs

Internal Messages

Internal filtering with user roles based on Msg Groups

- Advantages
  - Simply configure user roles with all Msg Groups except OpC & OpenView
- Disadvantages (none of these are show stoppers)
  - May miss messages from msg Groups not configured in user roles
  - Custom DB queries must include list of valid production message groups
  - Operations Admins must monitor all node groups for internal msgs
  - Counterexample: non-internal OOB SPI messages with no Msg Group:



	Node	Application	Object	Group	Text	Policy	Policy Type
AM	INTZEXPS02N				Resource Group Moved :INACTIVE;INTZEXPS02N;INTZEXMB01N;INTZEXMBVS01N	WINOSSPI-MSCS_ClusterUpdate(11.0)	Measurement
PM	INTZEXPS03N				Resource Group Moved :ACTIVE;INTZEXPS03N;INTZEXMB01N;INTZEXMBVS01N	WINOSSPI-MSCS_ClusterUpdate(11.0)	Measurement
PM	INTZEXPS01N				Resource Group Moved :ACTIVE;INTZEXPS01N;INTZEXMB01N;INTZEXVSCG01N	WINOSSPI-MSCS_ClusterUpdate(11.0)	Measurement
PM	INTZEXPS01N	ClusSvc	Failover Mgr		EventID: 0x0000042D (1069) - Cluster resource 'SMTP Virtual Server Instance 2 (INTZEXMBVS02N)' in Reso…	WINOSSPI-MSCS_ResourceMessages(1…	Logfile Entry |
AM	INTZEXPS02N				Resource Group Moved :ACTIVE;INTZEXPS02N;INTZEXMB01N;INTZEXMBVS01N	WINOSSPI-MSCS_ClusterUpdate(11.0)	Measurement
PM	INTZEXPS01N	ClusSvc	Startup/Sh…		EventID: 0x00000426 (1062) - Cluster service successfully joined the server cluster INTZEXMB01N.	WINOSSPI-MSCS_FwdClusterServiceEv…	Logfile Entry |
PM	INTZEXPS03N				Resource Group Moved :ACTIVE;INTZEXPS03N;INTZEXMB01N;INTZEXMBVS02N;INTZEXVSDTC01N	WINOSSPI-MSCS_ClusterUpdate(11.0)	Measurement
PM	VICTEXMB01AN	Tcpip	None		EventID: 0x40001069 (4201) - The system detected that network adapter Local Area Connection* 13 was …	WINOSSPI-MSCS_FwdClusterServiceEv…	Logfile Entry |
PM	INTZEXPS02N	RGResou…	RGHostedOn		Resource Group INTZEXMBVS02N has failed on INTZEXPS02N	WINOSSPI-MSCS_StatusMessages(10.0)	Open Message
PM	VICTEXMB01BN				Resource Group Moved :ACTIVE;VICTEXMB01BN;VICTEXMB01N;Cluster Group;VICTEXMBCL01N	WINOSSPI-MSCS_ClusterUpdate(11.0)	Measurement
PM	INTZEXPS01N	RGResou…	VirtualRG		Resource Group INTZEXMBVS01N has failed Completely	WINOSSPI-MSCS_StatusMessages(10.0)	Open Message
PM	INTZEXPS01N				Resource Group Moved :INACTIVE;INTZEXPS01N;INTZEXMB01N;INTZEXMBVS02N	WINOSSPI-MSCS_ClusterUpdate(11.0)	Measurement
AM	INTZEXPS03N				Resource Group Moved :ACTIVE;INTZEXPS03N;INTZEXMB01N;INTZEXVSCG01N	WINOSSPI-MSCS_ClusterUpdate(11.0)	Measurement

Internal Messages

Internal filtering with user roles based on Msg Groups

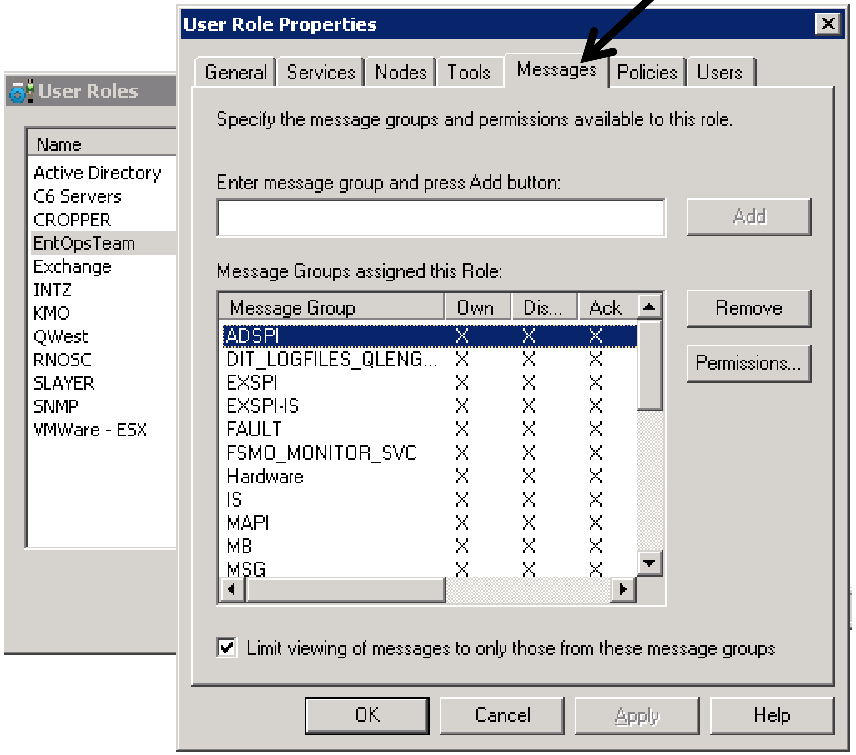
- Add Message Groups except OpC & OpenView to User Roles
- Extract all Msg Groups in DB (results are only from active/history msgs) :

```
Windows:       SELECT distinct MessageGroup from OV_MS_Message
UNIX:          SELECT distinct name from opc_message_groups
```

- Output (Windows with OS, EX, & AD SPIs):

```
WINOSSPI-MS_SYSTEMS_MGMT_SERVER,
MAPI, EXSPI-FAULT, MSG, PF, Hardware,
WINOSSPI-MS_CLUSTER_SERVER, EXSPI-IS,
WINOSSPI-MS_MESSAGE_QUEUE_SERVER,
EVENT-ONLINE, DIT_DIT_QUEUELENGTH,
DSACCESS, WINOSSPI-MS_INDEX_SERVER,
<$MSG_GROUP>, WINOSSPI-INTERNET_SERVICE,
FAULT, OpenView, IS, OWA, MTA, MB, PERF,
VP_SM_DB, VP_SM, OpC, EVENT-OFFLINE,
DIT_LOGFILES_QLENGTH, FSMO_MONITOR_SVC,
WINOSSPI-MS_TRANSACTION_SERVER,
REPLICATION_MONITOR_REP, WINOSSPI-CORE,
SMTP, WINOSSPI-MS_TERMINAL_SERVER,
Service, EXSPI, REPLICATION-SYSVOL,
RESPONSETIME_SVC, WINOSSPI_CORE

(38 rows affected)
```



User Roles

Name
Active Directory
C6 Servers
CROPPER
EntOpsTeam
Exchange
INTZ
KMO
QWest
RNOSC
SLAYER
SNMP
VMWare - ESX

User Role Properties

Specify the message groups and permissions available to this role.

Enter message group and press Add button:

Message Groups assigned this Role:

Message Group	Own	Dis...	Ack
ADSPI	X	X	X
DIT_LOGFILES_QLENG...	X	X	X
EXSPI	X	X	X
EXSPI-IS	X	X	X
FAULT	X	X	X
FSMO_MONITOR_SVC	X	X	X
Hardware	X	X	X
IS	X	X	X
MAPI	X	X	X
MB	X	X	X
MSG	X	X	X

☑ Limit viewing of messages to only those from these message groups

Internal Messages

Internal filtering with user roles based on Msg Groups

– Use this Method to mine *all potential* msg groups from all policies:

1. Windows: `ovpmutil cfg pol dnl <Target Directory>`

   UNIX: `opccfgdwn <spec file> <target dir>`

2. PERL script to extract all Message Group assignments from policy dump:

   (Path to embedded PERL on OMW server is %OvInstallDir%\nonOV\perl\a\bin\perl.exe)

```
#!/bin/perl
$Dir = $ARGV[0];
@Files = `dir \/D \/S \/B \"$Dir\"`;
foreach (@Files) {
   if ((! -d $_) && ($_ !~ /config\.mm/)) { # excludes dirs & config.mm file
      open (POL, "<$_");
      my @pol = <POL>;
      @b = grep (/MSGGRP/, @pol); # array of all MSGGRP matches in the file
      foreach $j (@b) {
         $j =~ s/.*MSGGRP |"//g; # strips unwanted chars
         next if $j =~ /\$WBEM/; # excludes <$WBEM:TargetInstance.MessageGroup>
         print "$j" unless grep (/$j/, @a);
         push (@a, $j) unless grep (/$j/, @a); # use @a to get unique matches
      }
   }
}
```

Internal Messages

Internal filtering based on opcmsg policy - UNIX

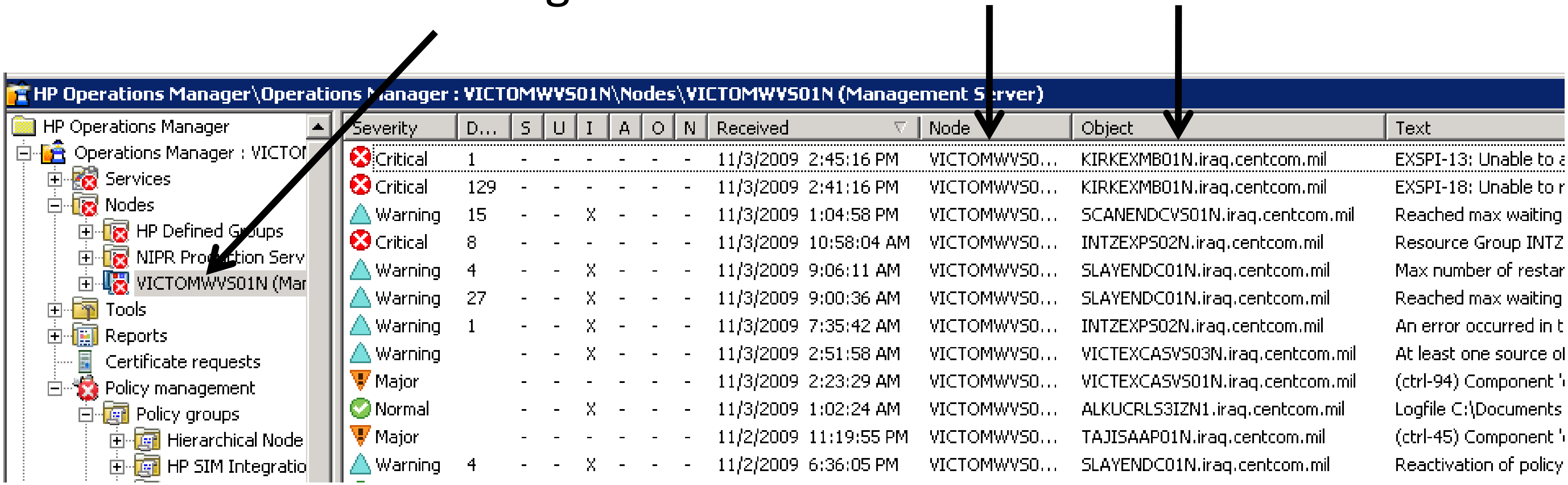
– Outline of activities

1. Enable internal message filtering in agent and server configs
    1. Server: `ovconfchg -ovrg <server> -ns opc -set OPC_INT_MSG_FLT TRUE`
    2. Agent: `ovconfchg -ns eaagt OPC_INT_MSG_FLT TRUE`
    3. Pre OVOU V8: Set in opcsvinfo/nodeinfo files
2. Define internal message handling strategy
    1. Send all internal msgs to Acknowledged msgs browser
        1. Easier to implement but makes the job of Operations Admins harder
    2. Redirect all internal msgs to Mgmt Server with node in Object field
        1. This method is shown in subsequent slides
        2. Operations Admins can more easily handle internal msgs
        3. Internal messages can be easily isolated from production node groups
3. Modify default opcmsg policy and distribute to all agents

Internal Messages

Redirect internal messages to Management Server

- A one-stop shop for OpenView Admins for internal messages
- Assumes Ops Admin is Ops Server admin, too
  - Could be any node, even a dummy External node instead
- Example screenshot showing internal agent-based msgs redirected to mgmt server node:



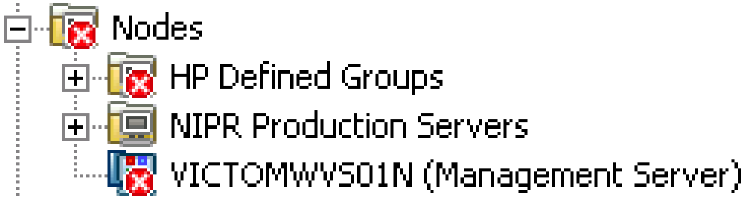
HP Operations Manager\Operations Manager : VICTOMWVS01N\Nodes\VICTOMWVS01N (Management Server)

Severity	D...	S	U	I	A	O	N	Received	Node	Object	Text
Critical	1	-	-	-	-	-	-	11/3/2009 2:45:16 PM	VICTOMWVS0...	KIRKEXMB01N.iraq.centcom.mil	EXSPI-13: Unable to a
Critical	129	-	-	-	-	-	-	11/3/2009 2:41:16 PM	VICTOMWVS0...	KIRKEXMB01N.iraq.centcom.mil	EXSPI-18: Unable to r
Warning	15	-	-	X	-	-	-	11/3/2009 1:04:58 PM	VICTOMWVS0...	SCANENDCVS01N.iraq.centcom.mil	Reached max waiting
Critical	8	-	-	-	-	-	-	11/3/2009 10:58:04 AM	VICTOMWVS0...	INTZEXPS02N.iraq.centcom.mil	Resource Group INTZ
Warning	4	-	-	X	-	-	-	11/3/2009 9:06:11 AM	VICTOMWVS0...	SLAYENDC01N.iraq.centcom.mil	Max number of restar
Warning	27	-	-	X	-	-	-	11/3/2009 9:00:36 AM	VICTOMWVS0...	SLAYENDC01N.iraq.centcom.mil	Reached max waiting
Warning	1	-	-	X	-	-	-	11/3/2009 7:35:42 AM	VICTOMWVS0...	INTZEXPS02N.iraq.centcom.mil	An error occurred in t
Warning		-	-	X	-	-	-	11/3/2009 2:51:58 AM	VICTOMWVS0...	VICTEXCASVS03N.iraq.centcom.mil	At least one source of
Major		-	-	-	-	-	-	11/3/2009 2:23:29 AM	VICTOMWVS0...	VICTEXCASVS01N.iraq.centcom.mil	(ctrl-94) Component '
Normal		-	-	X	-	-	-	11/3/2009 1:02:24 AM	VICTOMWVS0...	ALKUCRLS3IZN1.iraq.centcom.mil	Logfile C:\Documents
Major		-	-	-	-	-	-	11/2/2009 11:19:55 PM	VICTOMWVS0...	TAJISAAP01N.iraq.centcom.mil	(ctrl-45) Component '
Warning	4	-	-	X	-	-	-	11/2/2009 6:36:05 PM	VICTOMWVS0...	SLAYENDC01N.iraq.centcom.mil	Reactivation of policy

Internal Messages

Redirect internal msgs to an alternative node – UNIX

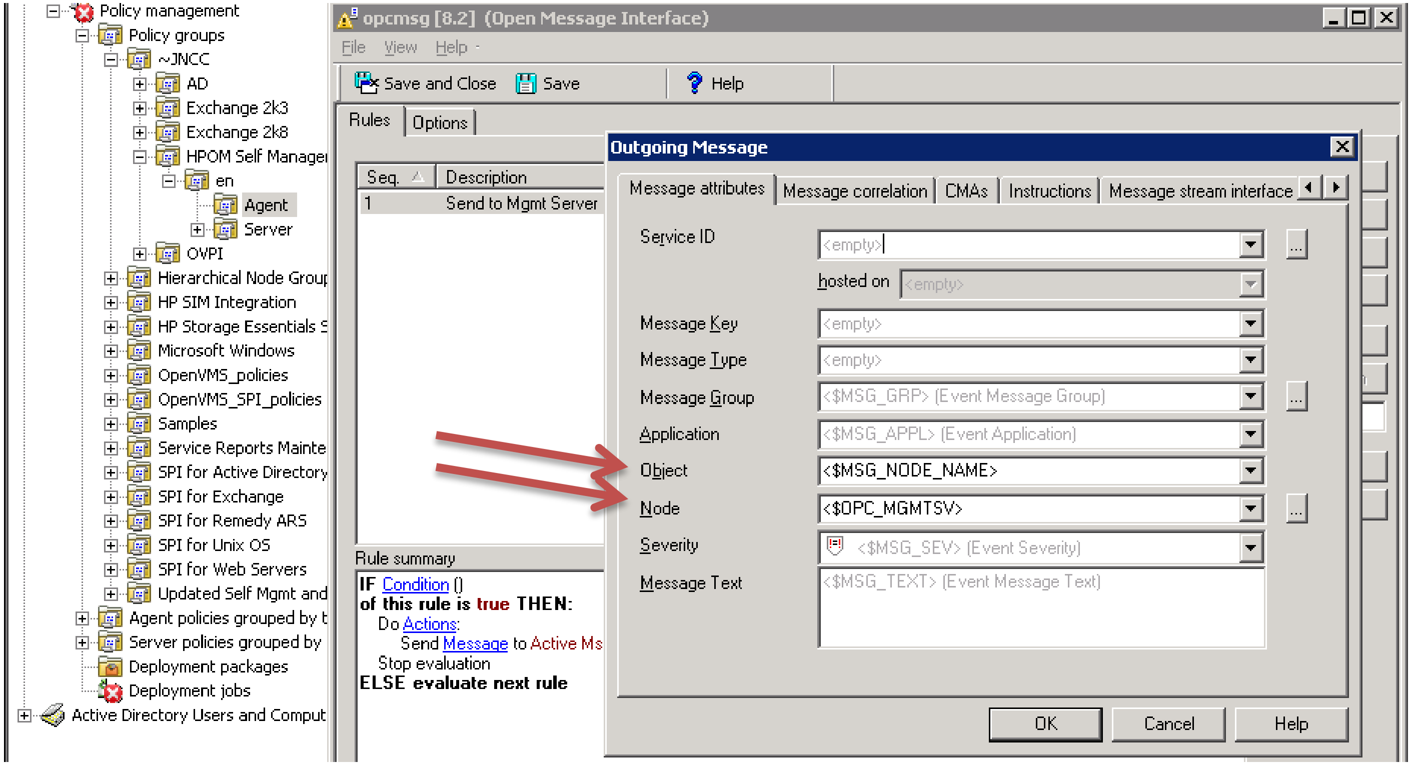
1. Move Mgmt Server out of production node group



2. Configure User Roles based on production Node Groups
    1. Optional – not required.
3. Set up opcmsg policy rule and distribute to all agent nodes

Internal Messages

opcmsg policy to direct internal msgs to mgmt server



Seq.	Description
1	Send to Mgmt Server

Rule summary

IF Condition ()
of this rule is true THEN:
Do Actions:
Send Message to Active Ms
Stop evaluation
ELSE evaluate next rule

Service ID: <empty>
hosted on: <empty>
Message Key: <empty>
Message Type: <empty>
Message Group: <$MSG_GRP> (Event Message Group)
Application: <$MSG_APPL> (Event Application)
Object: <$MSG_NODE_NAME>
Node: <$OPC_MGMTSV>
Severity: <$MSG_SEV> (Event Severity)
Message Text: <$MSG_TEXT> (Event Message Text)

1. Set rule to filter on Msg Group OpC & OpenView
2. Set outgoing msg Node to mgmt server
3. Set object to agent node name
4. Save and distrib to all agents

Internal Messages

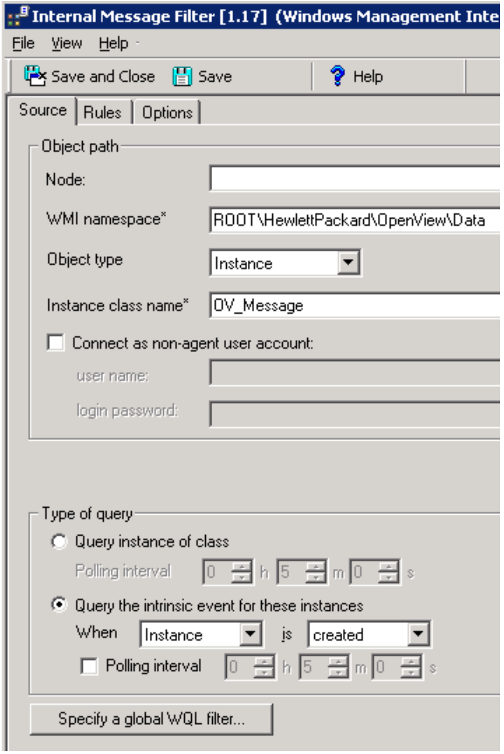
Internal filtering based on WMI policy - Windows

– Outline of activities

1. Do NOT Enable internal message filtering in agent configs
2. Define internal message handling strategy
    1. Send all internal msgs to Acknowledged msgs browser
        1. Easier to implement but makes the job of Operations Admins harder
    2. Redirect all internal msgs to Mgmt Server with node in Object field
        1. This method is shown in subsequent slides
        2. Operations Admins can more easily handle internal msgs
        3. Internal messages can be easily isolated from production node groups
3. Set up Server-based WMI policy

Internal Messages

- Internal filtering based on WMI policy - Windows
  - WMI Policy Screen Shots



Internal Message Filter [1.17] (Windows Management Inte

Object path

Node:

WMI namespace* ROOT\HewlettPackard\OpenView\Data

Object type Instance

Instance class name* OV_Message

□ Connect as non-agent user account:

user name:

login password:

Type of query

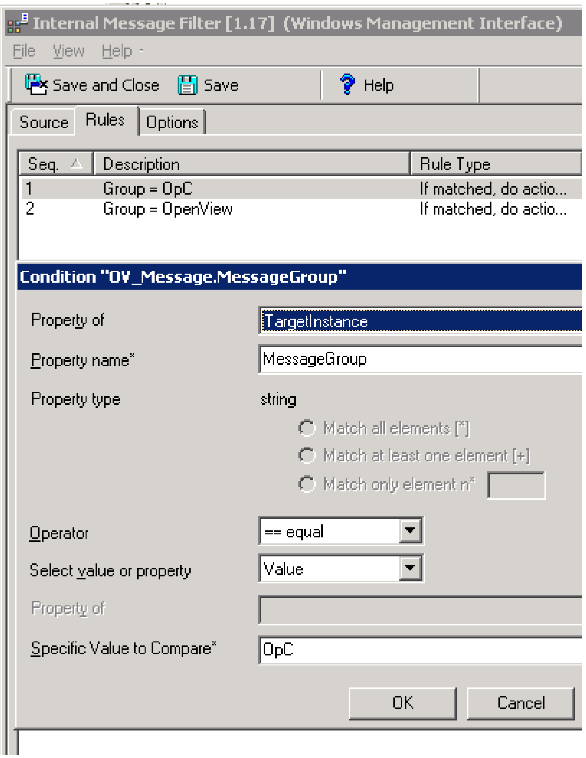
○ Query instance of class

Polling interval 0 h 5 m 0 s

● Query the intrinsic event for these instances

When Instance is created

□ Polling interval 0 h 5 m 0 s



Internal Message Filter [1.17] (Windows Management Interface)

Seq.	Description	Rule Type
1	Group = OpC	If matched, do actio...
2	Group = OpenView	If matched, do actio...

Condition "OV_Message.MessageGroup"

Property of TargetInstance

Property name* MessageGroup

Property type string

○ Match all elements [*]

○ Match at least one element [+]

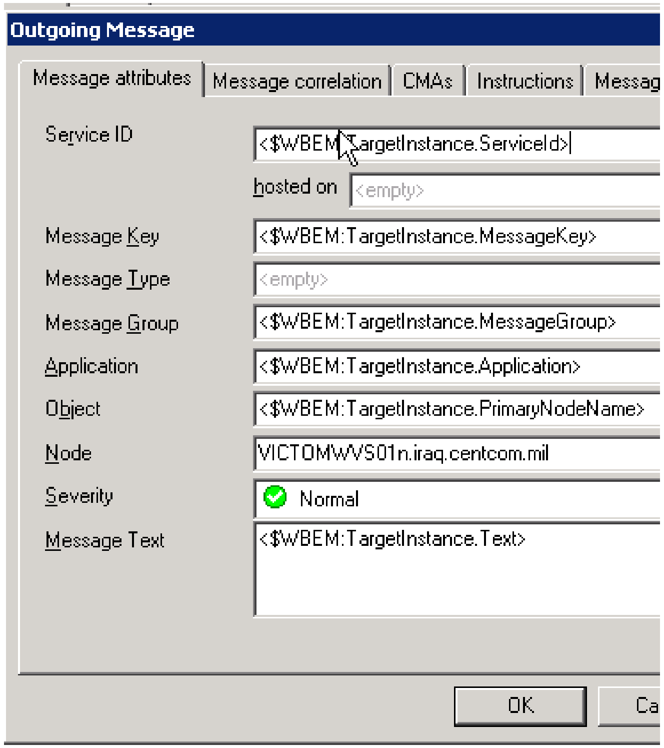
○ Match only element n°

Operator == equal

Select value or property Value

Property of

Specific Value to Compare* OpC



Outgoing Message

Service ID <$WBEM:TargetInstance.ServiceId>

hosted on <empty>

Message Key <$WBEM:TargetInstance.MessageKey>

Message Type <empty>

Message Group <$WBEM:TargetInstance.MessageGroup>

Application <$WBEM:TargetInstance.Application>

Object <$WBEM:TargetInstance.PrimaryNodeName>

Node VICTOMWVS01n.iraq.centcom.mil

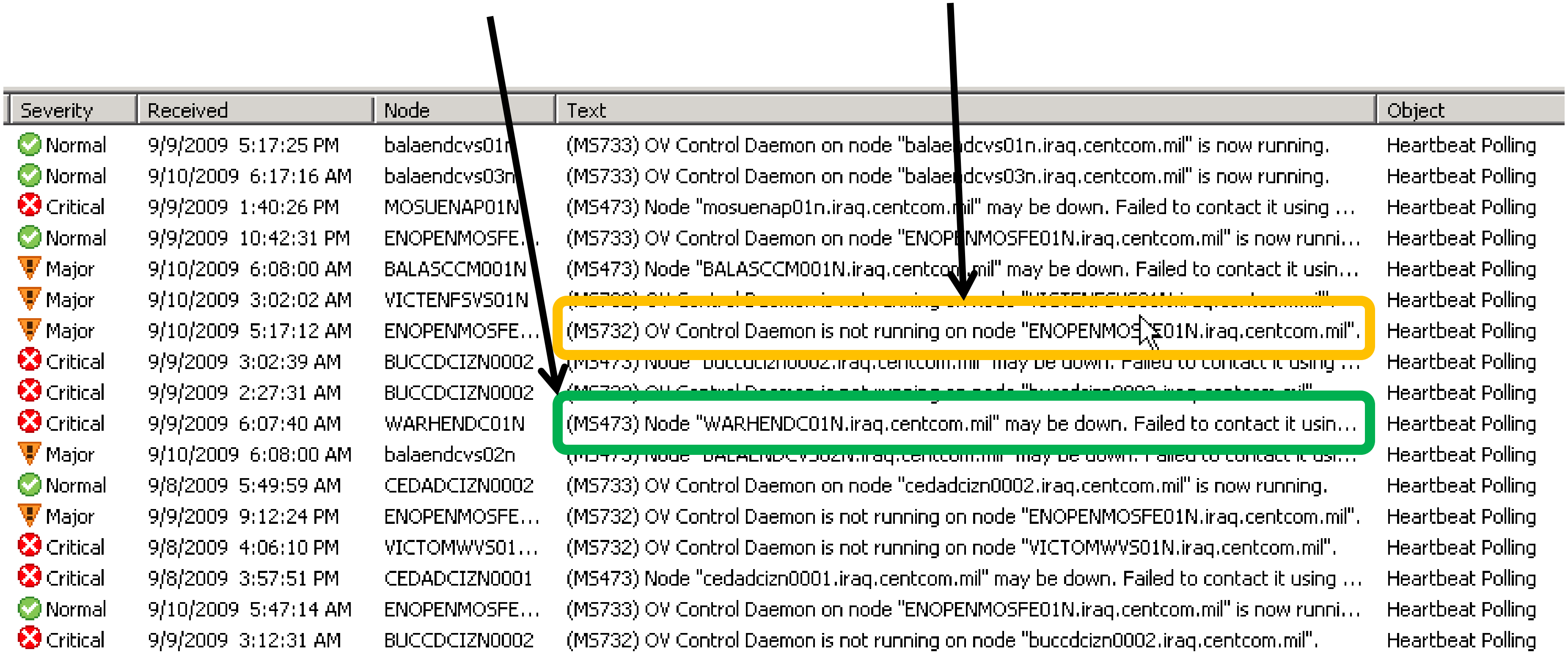
Severity ✓ Normal

Message Text <$WBEM:TargetInstance.Text>

Internal Messages

Internal filtering of Heartbeat Messages

- Most Heartbeat Messages relate to OM agent status
  - Separate hard failure from agent-related messages

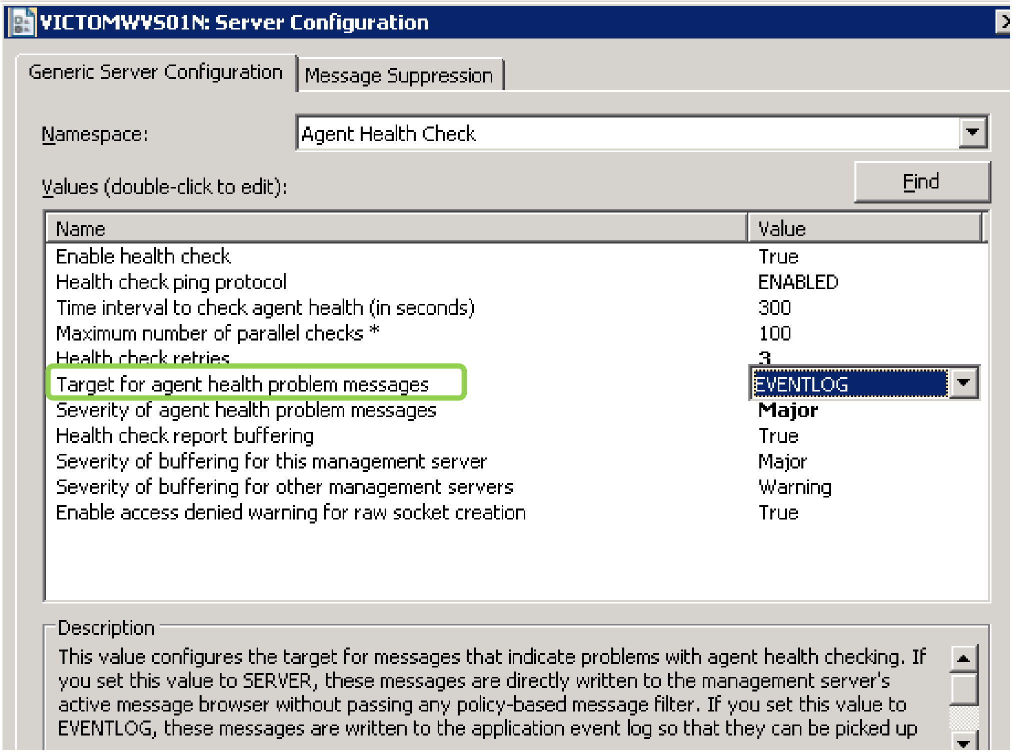


Severity	Received	Node	Text	Object
Normal	9/9/2009 5:17:25 PM	balaendcvs01n	(MS733) OV Control Daemon on node "balaendcvs01n.iraq.centcom.mil" is now running.	Heartbeat Polling
Normal	9/10/2009 6:17:16 AM	balaendcvs03n	(MS733) OV Control Daemon on node "balaendcvs03n.iraq.centcom.mil" is now running.	Heartbeat Polling
Critical	9/9/2009 1:40:26 PM	MOSUENAP01N	(MS473) Node "mosuenap01n.iraq.centcom.mil" may be down. Failed to contact it using ...	Heartbeat Polling
Normal	9/9/2009 10:42:31 PM	ENOPENMOSFE...	(MS733) OV Control Daemon on node "ENOPENMOSFE01N.iraq.centcom.mil" is now runni...	Heartbeat Polling
Major	9/10/2009 6:08:00 AM	BALASCCM001N	(MS473) Node "BALASCCM001N.iraq.centcom.mil" may be down. Failed to contact it usin...	Heartbeat Polling
Major	9/10/2009 3:02:02 AM	VICTENFSVS01N	(MS732) OV Control Daemon is not running on node "VICTENFSVS01N.iraq.centcom.mil".	Heartbeat Polling
Major	9/10/2009 5:17:12 AM	ENOPENMOSFE...	(MS732) OV Control Daemon is not running on node "ENOPENMOSFE01N.iraq.centcom.mil".	Heartbeat Polling
Critical	9/9/2009 3:02:39 AM	BUCCDCIZN0002	(MS473) Node "buccdcizn0002.iraq.centcom.mil" may be down. Failed to contact it using ...	Heartbeat Polling
Critical	9/9/2009 2:27:31 AM	BUCCDCIZN0002	(MS732) OV Control Daemon is not running on node "buccdcizn0002.iraq.centcom.mil".	Heartbeat Polling
Critical	9/9/2009 6:07:40 AM	WARHENDC01N	(MS473) Node "WARHENDC01N.iraq.centcom.mil" may be down. Failed to contact it usin...	Heartbeat Polling
Major	9/10/2009 6:08:00 AM	balaendcvs02n	(MS473) Node "BALAENDCVS02N.iraq.centcom.mil" may be down. Failed to contact it usi...	Heartbeat Polling
Normal	9/8/2009 5:49:59 AM	CEDADCIZN0002	(MS733) OV Control Daemon on node "cedadcizn0002.iraq.centcom.mil" is now running.	Heartbeat Polling
Major	9/9/2009 9:12:24 PM	ENOPENMOSFE...	(MS732) OV Control Daemon is not running on node "ENOPENMOSFE01N.iraq.centcom.mil".	Heartbeat Polling
Critical	9/8/2009 4:06:10 PM	VICTOMWVS01...	(MS732) OV Control Daemon is not running on node "VICTOMWVS01N.iraq.centcom.mil".	Heartbeat Polling
Critical	9/8/2009 3:57:51 PM	CEDADCIZN0001	(MS473) Node "cedadcizn0001.iraq.centcom.mil" may be down. Failed to contact it using ...	Heartbeat Polling
Normal	9/10/2009 5:47:14 AM	ENOPENMOSFE...	(MS733) OV Control Daemon on node "ENOPENMOSFE01N.iraq.centcom.mil" is now runni...	Heartbeat Polling
Critical	9/9/2009 3:12:31 AM	BUCCDCIZN0002	(MS732) OV Control Daemon is not running on node "buccdcizn0002.iraq.centcom.mil".	Heartbeat Polling

Internal Messages

Internal filtering of heartbeat messages – Windows 8+

- Direct Heartbeat messages to Appl. Event Log
  - Server Configuration (right click, Configure -> Server)



VICTOMWVS01N: Server Configuration

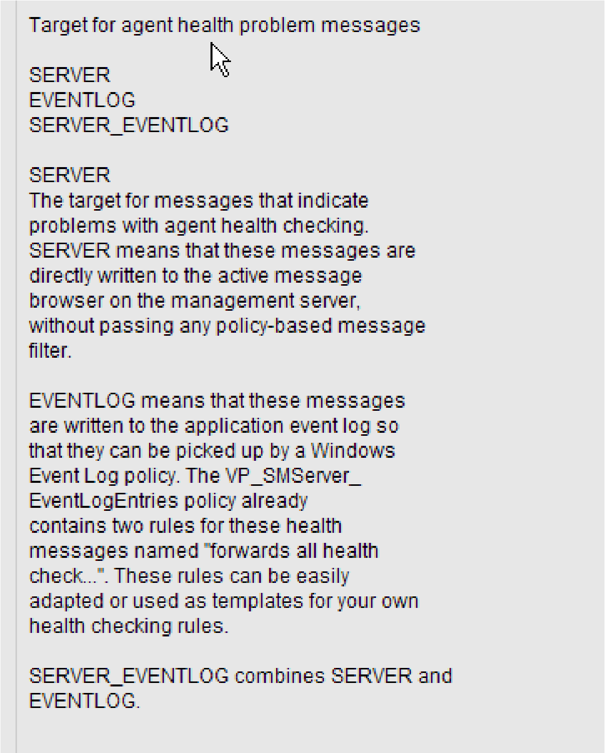
Namespace: Agent Health Check

Values (double-click to edit):

Name	Value
Enable health check	True
Health check ping protocol	ENABLED
Time interval to check agent health (in seconds)	300
Maximum number of parallel checks *	100
Health check retries	3
Target for agent health problem messages	EVENTLOG
Severity of agent health problem messages	**Major**
Health check report buffering	True
Severity of buffering for this management server	Major
Severity of buffering for other management servers	Warning
Enable access denied warning for raw socket creation	True

Description

This value configures the target for messages that indicate problems with agent health checking. If you set this value to SERVER, these messages are directly written to the management server's active message browser without passing any policy-based message filter. If you set this value to EVENTLOG, these messages are written to the application event log so that they can be picked up



Target for agent health problem messages

SERVER
EVENTLOG
SERVER_EVENTLOG

SERVER
The target for messages that indicate problems with agent health checking. SERVER means that these messages are directly written to the active message browser on the management server, without passing any policy-based message filter.

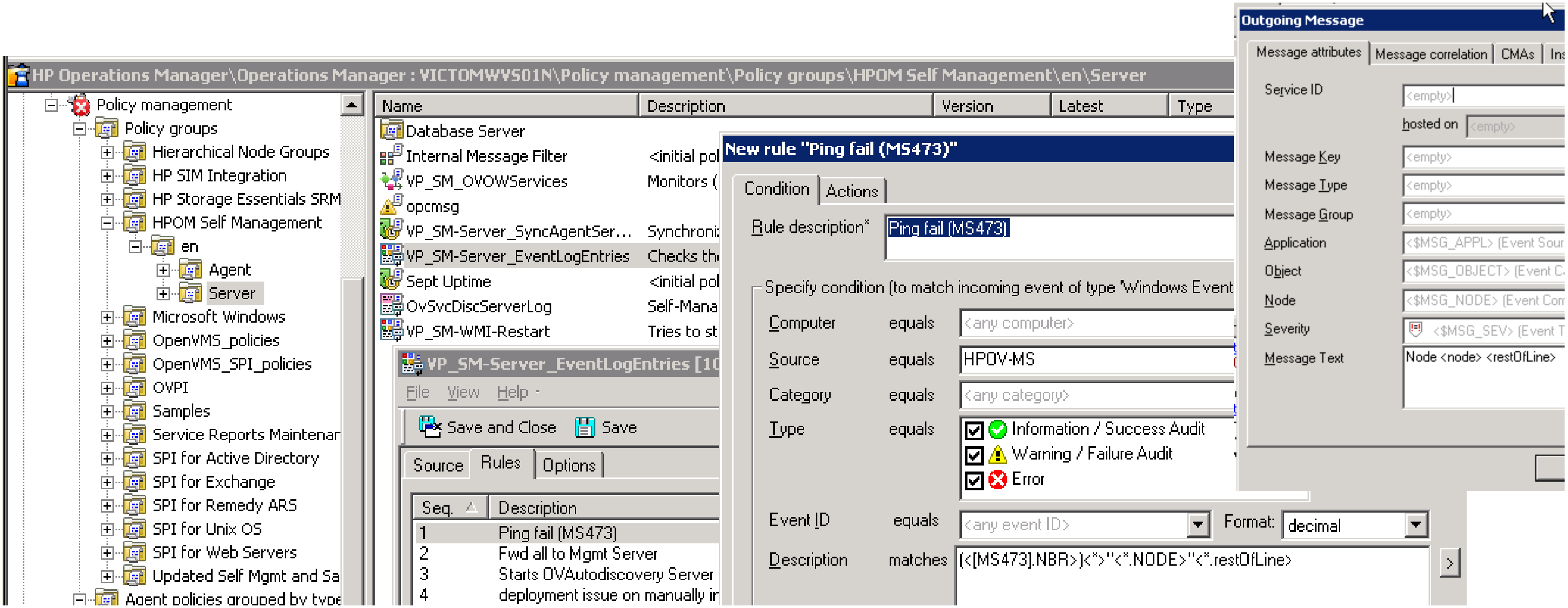
EVENTLOG means that these messages are written to the application event log so that they can be picked up by a Windows Event Log policy. The VP_SMServer_EventLogEntries policy already contains two rules for these health messages named "forwards all health check...". These rules can be easily adapted or used as templates for your own health checking rules.

SERVER_EVENTLOG combines SERVER and EVENTLOG.

Internal Messages

Internal filtering of heartbeat messages - Windows

- Customize VP_SMServer_EventLogEntries policy
  - Add condition for Ping Fail (filter IN)
  - Note: OMW_00051 updated version of this policy



HP Operations Manager\Operations Manager : VICTOMWVS01N\Policy management\Policy groups\HPOM Self Management\en\Server

- Policy management
  - Policy groups
    - Hierarchical Node Groups
    - HP SIM Integration
    - HP Storage Essentials SRM
    - HPOM Self Management
      - en
        - Agent
        - Server
    - Microsoft Windows
    - OpenVMS_policies
    - OpenVMS_SPI_policies
    - OVPI
    - Samples
    - Service Reports Maintenar
    - SPI for Active Directory
    - SPI for Exchange
    - SPI for Remedy ARS
    - SPI for Unix OS
    - SPI for Web Servers
    - Updated Self Mgmt and Sa
  - Agent policies grouped by type

Name	Description	Version	Latest	Type
Database Server				
Internal Message Filter	<initial pol			
VP_SM_OVOWServices	Monitors (			
opcmsg				
VP_SM-Server_SyncAgentSer...	Synchroni:			
VP_SM-Server_EventLogEntries	Checks th			
Sept Uptime	<initial pol			
OvSvcDiscServerLog	Self-Mana			
VP_SM-WMI-Restart	Tries to st			

VP_SM-Server_EventLogEntries [10

Seq.	Description
1	Ping fail (MS473)
2	Fwd all to Mgmt Server
3	Starts OVAutodiscovery Server
4	deployment issue on manually ir

New rule "Ping fail (MS473)"

Rule description* Ping fail (MS473)

Specify condition (to match incoming event of type 'Windows Event

Computer	equals	<any computer>
Source	equals	HPOV-MS
Category	equals	<any category>
Type	equals	☑ Information / Success Audit ☑ Warning / Failure Audit ☑ Error
Event ID	equals	<any event ID> Format: decimal
Description	matches	(<[MS473].NBR>)<*>"<*.NODE>"<*.restOfLine>

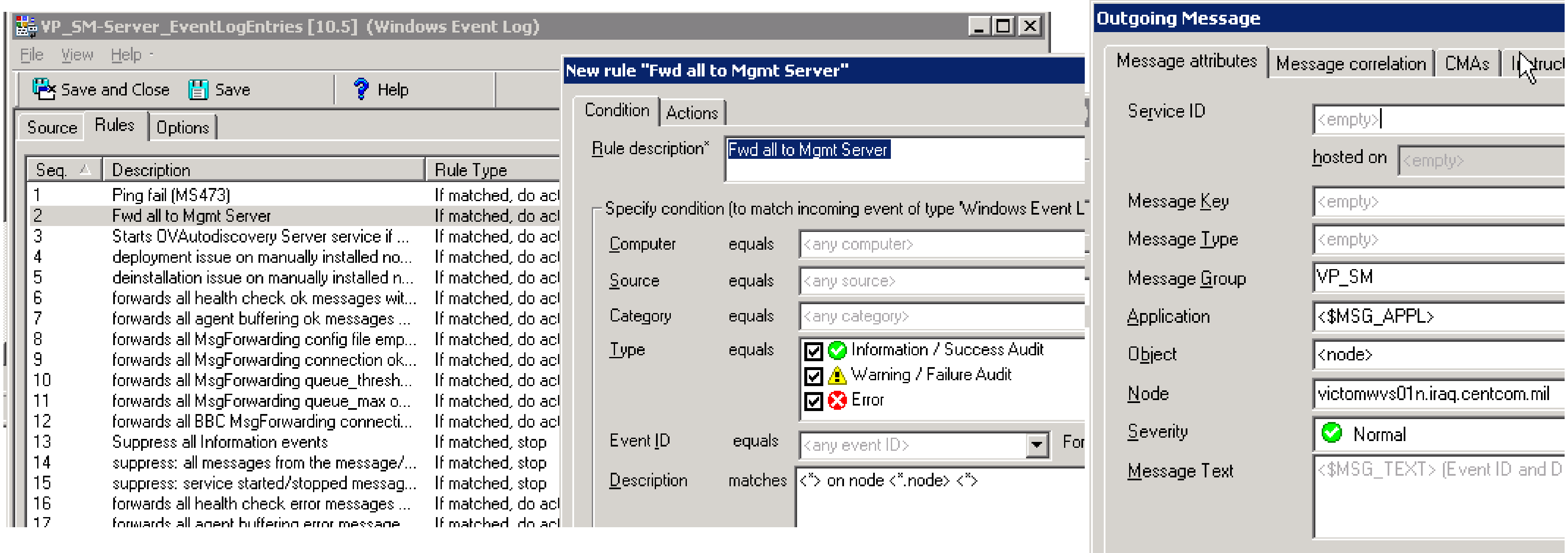
Outgoing Message

Service ID	<empty>
hosted on	<empty>
Message Key	<empty>
Message Type	<empty>
Message Group	<empty>
Application	<$MSG_APPL> (Event Sour
Object	<$MSG_OBJECT> (Event C
Node	<$MSG_NODE> (Event Con
Severity	<$MSG_SEV> (Event T
Message Text	Node <node> <restOfLine>

Internal Messages

Internal filtering of heartbeat messages - Windows

- Customize VP_SMServer_EventLogEntries policy
  - Add condition To redirect remaining heartbeat messages (filter OUT)
  - Windows default heartbeat msg group: VP_SM



Seq.	Description	Rule Type
1	Ping fail (MS473)	If matched, do act
2	Fwd all to Mgmt Server	If matched, do act
3	Starts OVAutodiscovery Server service if ...	If matched, do act
4	deployment issue on manually installed no...	If matched, do act
5	deinstallation issue on manually installed n...	If matched, do act
6	forwards all health check ok messages wit...	If matched, do act
7	forwards all agent buffering ok messages ...	If matched, do act
8	forwards all MsgForwarding config file emp...	If matched, do act
9	forwards all MsgForwarding connection ok...	If matched, do act
10	forwards all MsgForwarding queue_thresh...	If matched, do act
11	forwards all MsgForwarding queue_max o...	If matched, do act
12	forwards all BBC MsgForwarding connecti...	If matched, do act
13	Suppress all Information events	If matched, stop
14	suppress: all messages from the message/...	If matched, stop
15	suppress: service started/stopped messag...	If matched, stop
16	forwards all health check error messages ...	If matched, do act
17	forwards all agent buffering error message	If matched, do act

Rule description* Fwd all to Mgmt Server

Specify condition (to match incoming event of type 'Windows Event L

Computer	equals	<any computer>
Source	equals	<any source>
Category	equals	<any category>
Type	equals	☑ Information / Success Audit ☑ Warning / Failure Audit ☑ Error
Event ID	equals	<any event ID> For
Description	matches	<*> on node <*.node> <*>

Service ID	<empty>
hosted on	<empty>
Message Key	<empty>
Message Type	<empty>
Message Group	VP_SM
Application	<$MSG_APPL>
Object	<node>
Node	victomwvs01n.iraq.centcom.mil
Severity	✓ Normal
Message Text	<$MSG_TEXT> (Event ID and D

Internal Messages

Internal filtering of heartbeat messages - UNIX

- Customize Server-side opcmsg template
    - No need for additional msg conditions in template
        - Heartbeat messages use Message Group: OpC
    - Set up condition to filter IN msgs related to ping failure
    - Heartbeat ping fail (OpC40-436) message attributes:

Application:	*HP OpenView Operations*
Object:	*ovoareqsdr* (Request Sender)
Message Group:	*OpC*
Message Text:	*Node <node> is probably down. Contacting it with ping packages failed*

Summary

- You are what you eat
  - No effort into instrumentation = poor IT health
- Defaults are not best practices
- Reducing/improving events must involve all business stakeholders
- Reducing/improving events can save lots of money and directly affects SLA compliance

Last words

Marshall McLuhan:

- *“…we live habitually in a state of information overload. There's always more than you can cope with.“*

- *“I don't necessarily agree with everything I say.”*