

Author: Sidney Lim

Date: 1st July, 2015

OMi – Infrastructure (System-Network) Domain

Description:

OMi positions as an Operation Bridge to achieve better efficiency in event management by consolidating events from all sources. During the consolidation of events, it should provide a central repository of event management and it must help operation team quickly in determining the cause rather than complicating the IT operation in handling consolidated event.

This use case demonstrates 2 events collected from 2 different domain tools and it gets consolidated to identify a cause and a symptom type of event. This helps the operation team quickly react on a cause event instead of wasting time investigating on symptom event.

Use Case Scenario:

A server that is monitor by a system management tool, like Sitescope, is constantly checking on the heartbeat by pinging the server in a regular interval.

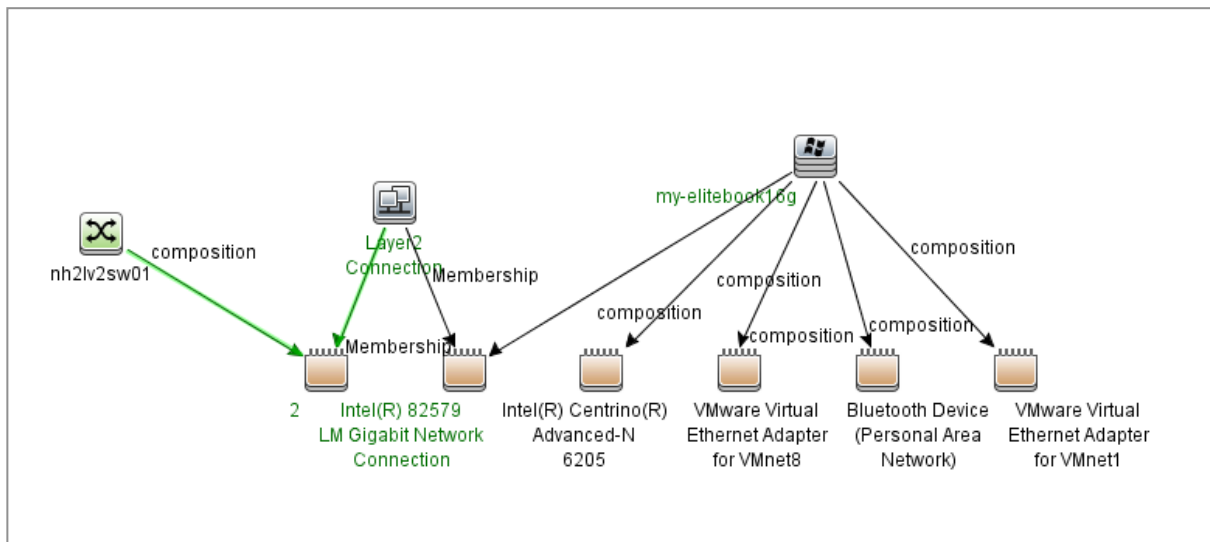
The server connected to a network switch is also monitor by the network management tool about its interface availability and performance.

This use case simulation is by disconnecting the network cable from the switch. There will be 2 events collected in OMi Event Console. One event is recorded by System Management Tool and another by Network Management tool.

Scenario Prerequisites:

A complete topology mapping about how the server is connected to a switch provides the true value to help identify the cause and symptom of event.

The server (my-elitebook16g) has a layer 2 connection to the switch (nh2lv2sw01) via the 2 end-points of interfaces (interface 2 and Intel(R) 82579). This topology can be discovered and it is extremely difficult to maintain manually.



Task 1: Discover the topology

UCMDB/UD Discovery helps to discover the above topology automatically. The sequence of the discovery for the above topology mapping is:

- Network Infrastructure > Range IPs by ICMP
 - This will discover both the server and the switch IP address in the network
- Host Connection by WMI/SNMP/Shell
 - This will discover both the server and the switch components details like interfaces, bridge, type of network equipment etc
- Host Resources by WMI/SNMP/Shell
 - This will discover additional details about nodes like HBA, Filesystem etc
- Layer 2 Topology Bridge-based by SNMP
 - This will discover switches details about is physical ports, MAC address that the server is connected to the port (Port Next MAC) and forming a Layer 2 Connection
 - This is the essential details that we can used to formulate the Cause and Symptom event

The result of the discovery is stored in UCMDB Database and this forms the single truth about the configuration details in production environment. The topology mapping in UCMDB can be extended to other system and in this use case scenario, it is extended to RTSM so that RTSM can leverage on this topology to correlate cause-symptom event.

Integration Point

AM950

HistoryDataSource

RTSM925Integration

SM940Integration

UCMDBDiscovery

RTSM925Integration

Population Federation Data Push

Data Push Jobs copy or update CI Types and attributes from the local CMDB to an external data repository

Integration Jobs

Job Name

Status

Last Synchronization Type

RTSM-Sync

Completed

Changes

Statistics

Query Status

Query Name	Created	Updated	Deleted	Failed
BasicInfrastructure_Sync	730	134	216	23
BusinessAndFacilities_Sync	12	23	0	0
ExchangeServer_Sync	0	0	0	0
FailoverCluster_Sync	0	0	0	0
IS_Sync	0	1	0	0
J2EE_Sync	0	1	0	0
Network_Sync	8	0	7	14
RTSMtoCMSSync	6	24	0	0
Virtualization_Sync	12	21	12	0
Total	768	204	235	37

Task 2: Build a Correlation Rule

OMi allows building topology-based event correlation rule. Defining a rule that:

- If the switch interface is detected with “Interface Communication Status” indicator; and
- The server connected to the switch also detected with “Ping Availability” indicator, then
- The event from Network Management tool is a Cause; and
- The event from System Management tool is a Symptom.

This directs the cause event to the network team to investigate.

The screenshot displays the OMi Event Correlation tool interface. On the left, a list of correlation rules is shown, with "System:ComputerPingAvailability>>NetworkInterfaceCommunicationStatus" selected. The main area shows the "Rule Topology" for this rule, which is a hierarchical diagram. It starts with a "Computer" node, which has a "Composition" relationship to an "Interface" node. This "Interface" node is part of a "Layer2Connection" node, which in turn has "Membership" relationships to two other "Interface" nodes. Below the diagram, a "Symptoms and Causes" table is visible.

Type	CI Type	Indicator	Indicator State
Cause	Interface	Interface Communication Status	Unavailable
Symptom	Computer	Ping Availability	Unavailable

Task 3: NNMi Monitors the Switch Interface

Network Management tool will monitor the production network devices like switches and routers. It should also monitor the critical servers that connected to network from the network perspective. Network monitoring will monitor the availability and performance of the interface that server connected.

When the network cable is unplugged in the scenario, NNMi will detect the unavailability of the interface.

The screenshot displays the Network Management (NNMi) interface. The left sidebar shows a navigation tree with categories like Dashboards, Incident Management, Topology Maps, Monitoring, Troubleshooting, and Inventory. The main window is divided into several panes:

- Nodes Node:** Shows details for node NH2LV2SW01, including Hostname, Management Address (172.17.10.251), Status (Minor), and Device Profile (hp2530-24G-PoE+).
- SNMP Agent State:** Shows the state of the SNMP agent, including Agent Enabled, Agent SNMP State (Normal), Management Address (ICMP State), and Management Address (ICMP Response Time).
- Interfaces:** A table listing interfaces for node NH2LV2SW01. The table has columns: Status, Admin, Oper, ifName, ifType, ifSpeed, ifIndex, ifAlias, Physical Address, and Layer 2 Connection. The interfaces listed are lo1 through lo6, all of which are in a 'Down' state.
- Interface Summary:** Shows performance data for the selected interface, including Name, Status, Operational State, Administrative State, Hosted On Node, Current Time, and Analysis Period.
- Details:** Shows detailed information for the selected interface, including State Last Modified, Conclusions, ifName, ifDescr, ifSpeed, ifIndex, ifType, Physical Address, Ports, VLANs, Management Mode, Direct Management Mode, Capabilities, Status Last Modified, Input Utilization, Input Utilization Baseline, Output Utilization, Output Utilization Baseline, and Input Error Rate.

Unavailability of the interface will create an Incident in NNMi console.

The screenshot displays the HP Network Management Console (NNMi) interface. The top navigation bar includes 'Dashboards', 'Incident Management', 'Topology Maps', 'Monitoring', 'Troubleshooting', 'Inventory', 'Management Mode', 'Incident Browsing', 'Performance Analysis', 'Traffic Analysis', and 'Integration Module Configuration'. The 'Incident Management' section is active, showing a list of 'Open Key Incidents'.

Sever	Priori	Life	Last Occurrence	Assigned To	Source Node	Source Object	Categ	Famil	Origin	Corre	Message	Notes
5	1	1	7/1/15 2:07:53 PM		my-elitebook16g	my-elitebook16g					Node Down	
5	1	1	7/1/15 2:06:38 PM		NH2LV2SW01	2					Interface Down	

Below the table, the 'Analysis' section provides details for the selected incident:

Incident Summary : InterfaceDown

Performance Data: Wed Jul 01 14:09:11 SGT 2015
 Message: Interface Down
 Severity: Critical
 Lifecycle State: Registered
 RCA Active: true
 Source Object: 2 (Interface)
 Created/Opened: 7/1/15 02:06 PM (Open for 2.4 minutes)

Details

Category: Fault
 Family: Interface
 Correlation Nature: Root Cause
 Origin: NNMi
 Last Occurrence Time: July 1, 2015 2:06:38 PM SGT
 Source Node: NH2LV2SW01
 Source Object: 2

This incident will be recorded in OMI Event Console (Consolidated Event Console)

Task 4: SiteScope Monitors server by ping

System Management will monitor all critical servers and its service components like processes and services. The system availability of a server is easily checked by “pinging” the server.

SiteScope will monitor the server with Ping Monitor on a regular interval.

The screenshot displays the SiteScope Ping Monitor interface for the 'SidneyNotebook_Ping' monitor. The left sidebar shows a tree view of monitored hosts, including HyperV Hosts, App Tier, DB Tier, Web Tier, and NH2 ESXi Hosts. The main panel shows the 'Current Status' tab with a table of monitor details.

Name	Status	Type	Target	Summary	Updated	Description
SidneyNotebook_Ping	Failed	Ping	172.18.20.12	failed	7/1/2015 2:10 PM	
Counters (2 out of 2)						
% packets good	0%					
round trip time	n/a					

Whenever an error is detected, the Ping Monitor is integrated to OMi by sending it as an Event to OMi and mapped it Ping Availability Indicator for the server

The screenshot displays the SiteScope web interface for configuring the 'SidneyNotebook_Ping' monitor. The left-hand navigation pane shows a tree structure of monitors, including 'NH2 DEMO Hosts', 'App Tier', 'DB Tier', 'Web Tier', 'NH2 ESXi Hosts', and 'NH2 Vertica'. The main content area is titled 'SiteScope Ping Monitor - "SidneyNotebook_Ping"' and contains several configuration sections:

- Dependencies**: A section for defining dependencies.
- Calculated Metrics Settings**: A section for configuring calculated metrics.
- Threshold Settings**: A section for setting thresholds.
- HP Integration Settings**: A section for integrating with HP tools.
- BSM Integration Data and Topology Settings**: A section for configuring BSM integration.
- Indicator Settings**: A section for defining indicators, including a table with columns for Metric Pattern, CI Type, and Indicator.
- HP Operations Manager Integration Settings**: A section for integrating with HP Operations Manager.
- BSM Service Health Preferences**: A section for configuring BSM service health preferences.

The 'Indicator Settings' section contains the following table:

Metric Pattern	CI Type	Indicator
round trip time	Node	Ping Availability
*	ConfigurationItem	Legacy System

The 'HP Operations Manager Integration Settings' section includes checkboxes for 'Report metrics to HP Operations agent', 'Send events', and 'Manually send first event'. The 'BSM Service Health Preferences' section includes a dropdown menu for 'BSM Service Health affected by' set to 'Events'.

Task 5: Working on OMi Console

When both events from Network and System arrived in the OMi Event Console, it gets processed by correlation engine and based on the rule defined earlier, it marks the event from Network as Cause Event and event from System as Symptom Event.

The screenshot displays the HP Business Service Management (BSM) Operations Management console. The interface includes a top navigation bar with tabs for Event Perspective, Health Perspective, and Performance Perspective. The main area is divided into several panes:

- Model Explorer:** A tree view on the left showing the hierarchy of network components, including NNM_Layer2, hyper-vdemo01, hyper-vdemo02, lefthand01, lefthand02, my-ellerebook16g, and various network interfaces like nh2ap01_v1, nh2ap01_v2, nh2ap02_v1, nh2ap02_v2, nh2ap02_v3, nh2csw01, nh2csw02, nh2demosql.nh2d.biz, nh2fw001, nh2v1sw01, nh2v2sw01, nh2v3sw01, and nh2msupport.
- Event Browser:** A central table displaying a list of events. The table has columns for Severity, Priority, Category, Incident, Acknowledged, Unresolved, Status, Time Received, Title, and Related CI. The events listed are:

Sev	Prio	C	I	A	U	D	Sta	Time Received	Title	Related CI
Warning	Low						Open	7/1/15 02:40:34 PM	Metric '% packets good' changed status from	my-ellerebook16g: SiteScope:13.607379
Warning	Low						Open	7/1/15 02:40:34 PM	Metric 'round trip time' changed status from	my-ellerebook16g: SiteScope:13.607380
Critical	High						Open	7/1/15 02:37:44 PM	Interface Down	2
- Interface Down - Event Details:** A pane at the bottom showing detailed information for the selected 'Interface Down' event. It includes fields for ID (9es46ef0-1fb-71e5-0312-ac111e1c0000), Severity (Critical), Lifecycle State (Open), Priority (Medium), Assigned Group, Assigned User, Category (SNMP), Subcategory, and Control Transferred. It also shows related CI (2 Interface), Node (nh2v2sw01 [Switch]), Source CI (Operations-agent on NH2DEMONNM /HP Operat), Time Created (7/1/15 02:37:18 PM), Time Received (7/1/15 02:37:44 PM), Time State Changed, Event Type Indicator (Interface Communication Status: Unavailable), Duplicate Count (0), and Type (BSMC_Message).
- Actions:** A pane on the right showing a list of actions that can be performed on the event, such as 'Show Performance Graphs', 'Ping node from NNMi server', 'Show Layer 2 Neighbors', 'Show Layer 3 Neighbors', 'Show NNMi console', 'Show NNMi server status', 'Show node information', 'Show related NNMi incident', 'Show related NNMi node', 'Traceroute to node from N...', and 'Traceroute to node from N...'. The actions are filtered by 'All'.

Diagram below shows the result for Correlation Rule of
System::Node:PingAvailability>>NodeStatus

The screenshot displays the HP Business Service Management (BSM) Operations Management console. The interface includes a top navigation bar with 'Business Service Management - Operations Management' and a 'Full Screen View' button. Below the navigation bar, there are tabs for 'Event Perspective', 'Health Perspective', and 'Performance Perspective'. The 'Event Perspective' is active, showing a list of events in the 'Event Browser' pane. The 'Model Explorer' on the left shows a tree structure of nodes, with 'my-ellebook16g' selected. The 'Event Browser' pane displays a table of events:

Sev	Prio	C	I	A	U	D	Sta...	Time Received	Title	Related CI	Us
7/1/15	02:08:50 PM								Interface Down	2	
7/1/15	02:08:31 PM								Node Down	my-ellebook16g	
7/1/15	02:00:38 PM								Metric '% packets good' changed status from my-ellebook16g: SiteScope:13.607379		
7/1/15	02:00:35 PM								Metric 'round trip time' changed status from my-ellebook16g: SiteScope:13.607380		

The 'Node Down - Event Details' pane at the bottom provides more information about the selected event:

- ID:** 8927c7b0-1fb7-71e5-0312-ac111e1c0000
- Severity:** Critical
- Lifecycle State:** Open
- Priority:** Medium
- Assigned Group:**
- Assigned User:**
- Category:** SNMP
- Subcategory:**
- Control Transferred:**
- Related CI:** my-ellebook16g [Windows]
- Node:** my-ellebook16g [Windows]
- Source CI:** Operations-agent on NH2CEMOMNM (HP Operat...
- Time Created:** 7/1/15 02:08:04 PM
- Time Received:** 7/1/15 02:08:31 PM
- Event State Changed:**
- Event Type Indicator:** Node Status: Down
- Duplicate Count:** 0
- Type:** BSMC_Message

The 'Actions' pane on the right lists various actions available for the event, such as 'Show Performance Graphs', 'Ping node from NMI server', 'Show Layer 2 Neighbors to r...', 'Show Layer 3 Neighbors to r...', 'Show Layer 3 Neighbors to r...', 'Show NMI console', 'Show NMI console (https)', 'Show NMI server status', 'Show NMI server status (...)', 'Show node information in NMI', 'Show node information in NN...', 'Show related NMI incident', 'Show related NMI node', 'Show related NMI node (...)', 'Traceroute to node from NMI...', and 'Traceroute to node from NNM...'.