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.

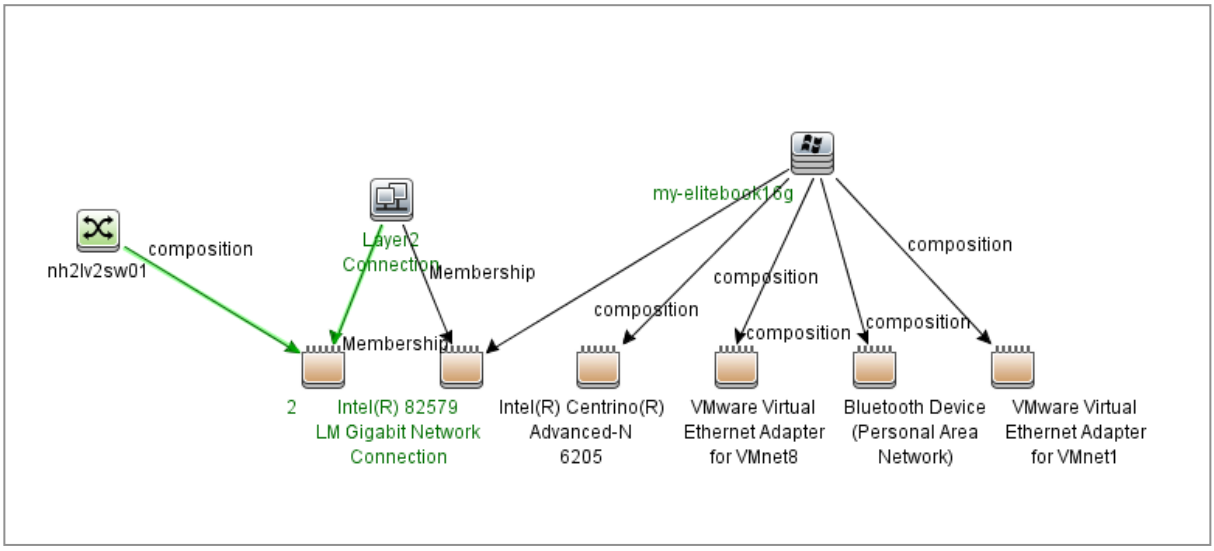
The server connected to a network switch is also monitor by the network management tool about its interface availability and performance.

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.

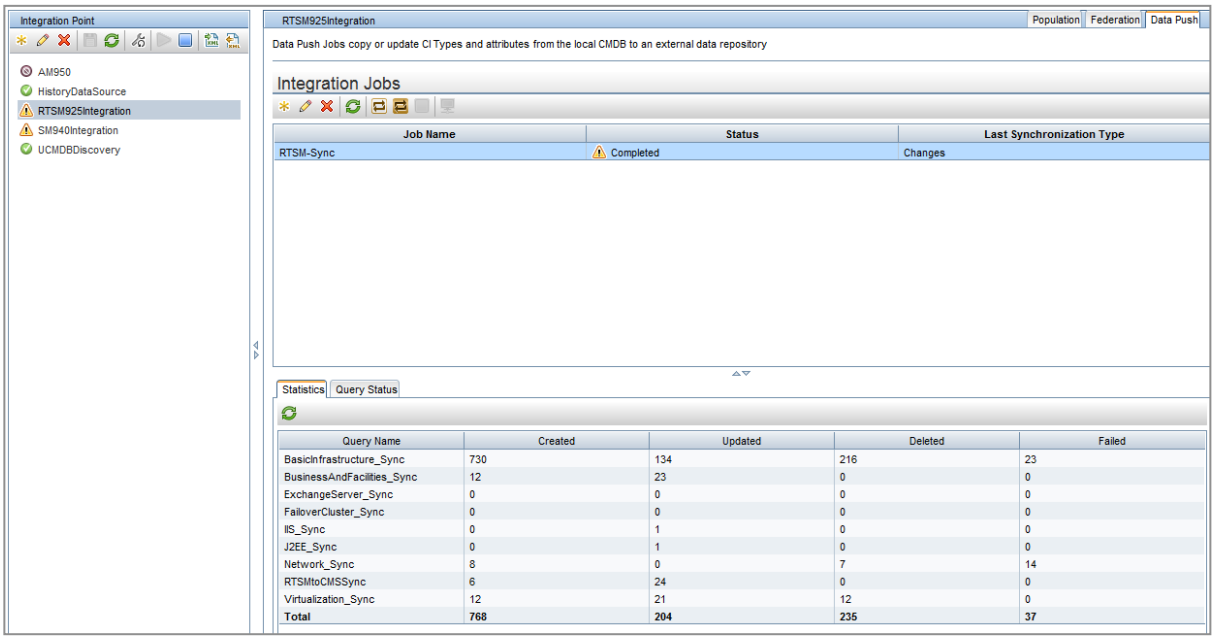


Task 1: Discover the topology

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.

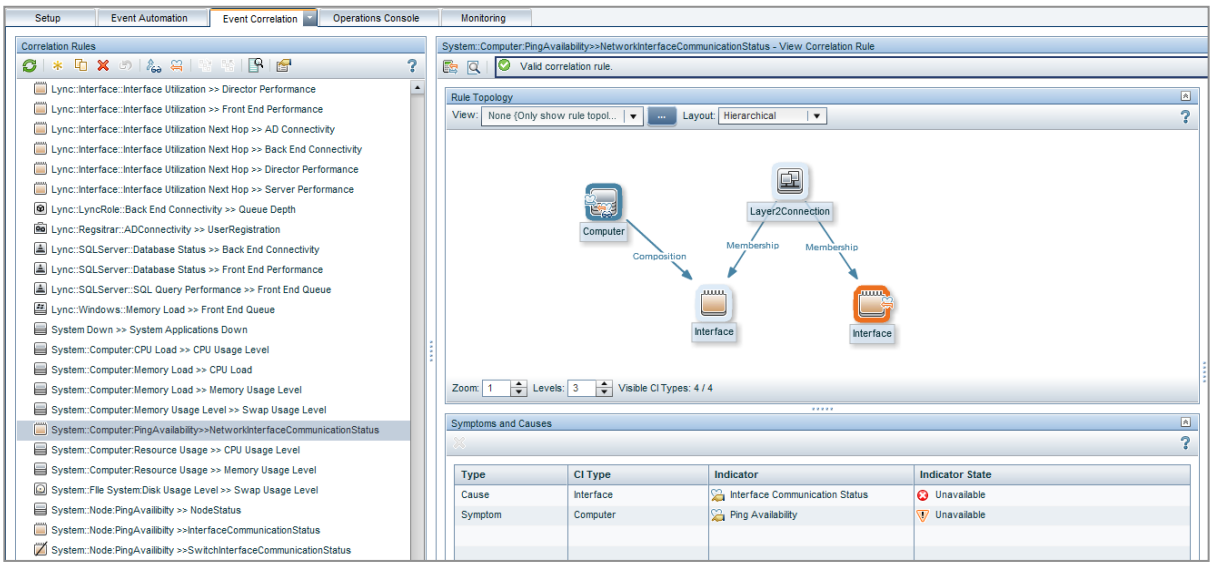

Integration Point
AM950
HistoryDataSource
RTSM925Integration
SM940Integration
UCMDBDiscovery
RTSM925Integration
Population
Federation
Data Push
Data Push Jobs copy or update CI Types and attributes from the local CMDB to an external data repository
Integration Jobs
Job Name
Status
Last Synchronization 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
IIS_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.

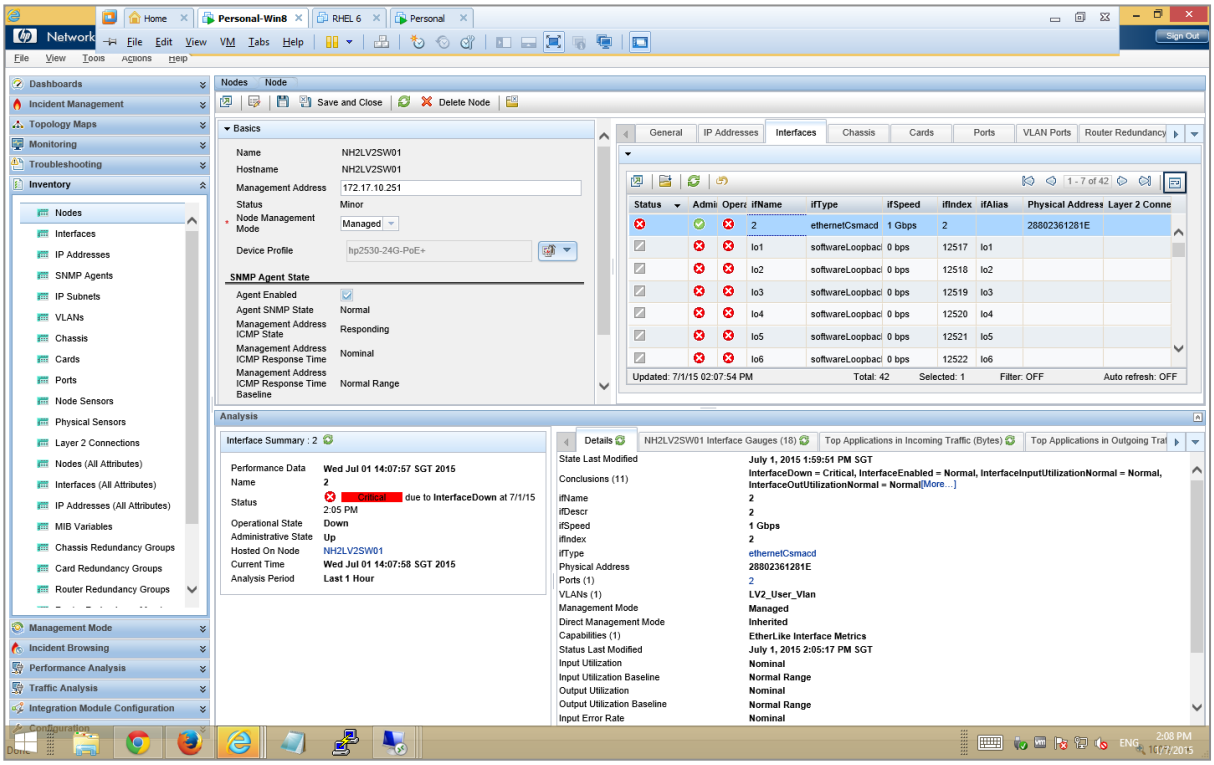
This directs the cause event to the network team to investigate.



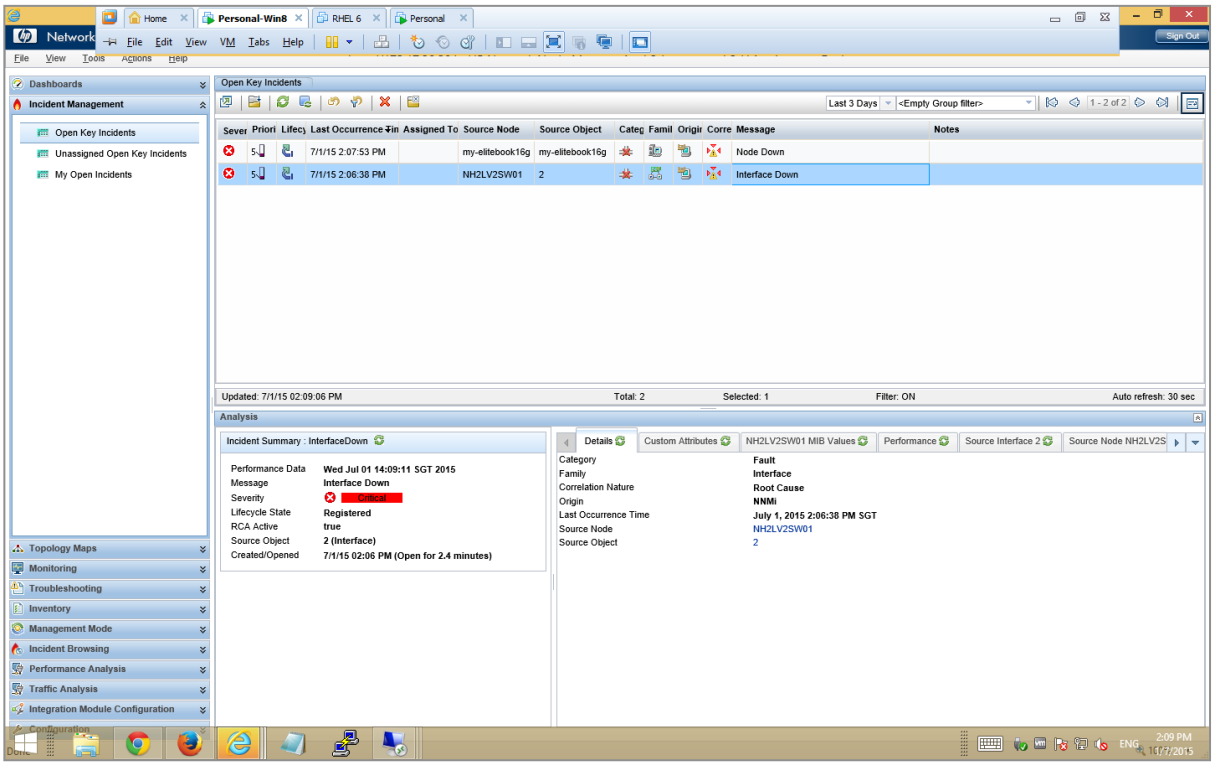
Task 3: NNMi Monitors the Switch Interface

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 unplug in the scenario, NNMi will detected the unavailable of the interface.



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

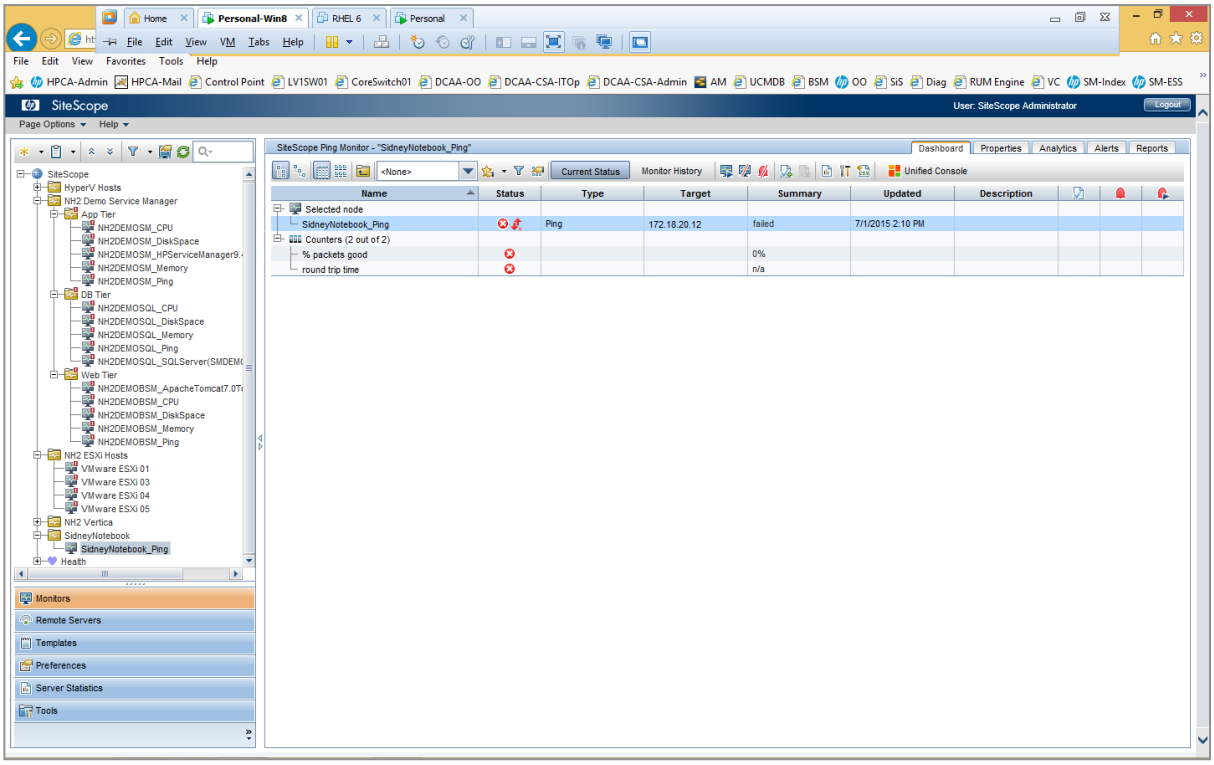


This incident will be recorded in OMI Event Console (Consolidated Event Console)

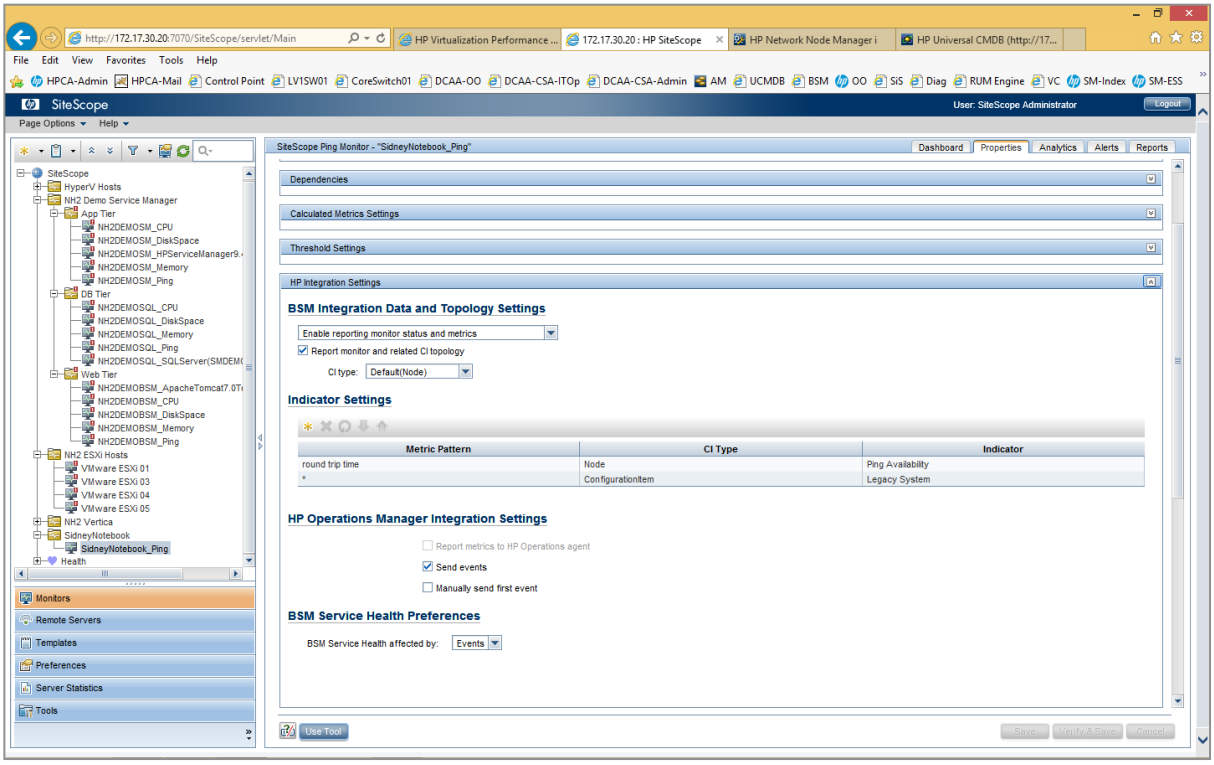
Task 4: Sitescope Monitors server by pinging

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.



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



Task 5: Working on OMi Console

When both events from Network and System arrived in the OMi Event Console, it get processes 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.

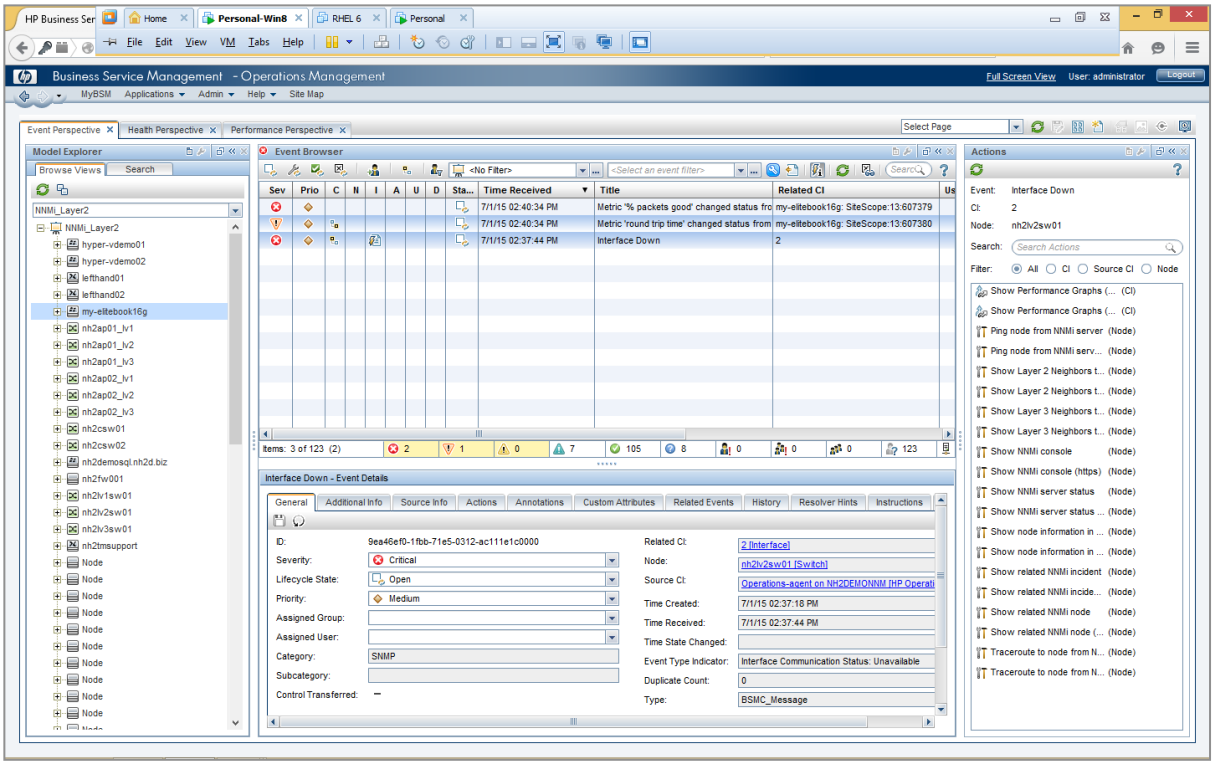


Diagram below shows the result for Correlation Rule of System::Node:PingAvailability>>NodeStatus