Technical white paper

HP Network Node Manager i Software 10.00



Step-by-Step Guide to Incident Management

Table of contents

Setting up your SNMP trap	2
Dampening and the Incident Pipeline	
Customizing Incident Configurations Using Interface or Node Groups	9
Deduplication	11
Rate	14
Enrichment	
Suppression	24
More about Dampening	
Lifecycle State and Actions	28

Incident Management

This whitepaper describes the NNMi event pipeline and Incident configuration. It includes the following Incident configuration options:

- Deduplication
- Rate Correlation
- Incident Suppression
- Enrichment
- Actions

It also includes information about Dampening incidents and explains how to narrow incident customization based on Node Group and Interface Group membership.

This whitepaper uses the following terms:

Trap - an asynchronous notification from an SNMP agent on a managed node that is sent to the NNMi management server.

NNMi management event - an incident that is generated by NNMi usually as a result of a status poll. An example is the Node Down incident.

Also see the "Step-by-Step Guide to Managing SNMP Traps in NNMi".

Note

In this example scenario, a network device sends the same example SNMP trap to mean various things. The difference between the traps is the varbinds (variable bindings). This is a common practice for some devices and applications.

Setting up your SNMP trap

In this example scenario, a network device sends the same example SNMP trap to mean various things. The difference between the traps is the varbinds (variable bindings). This is a common practice for some devices and applications.

Note

Your NNMi console appearance might vary from some of the figures in this document.

The trap and its varbinds are defined below:

OID	.1.3.6.1.4.1.33333.0.1
Varbind 1:	.1.3.6.1.4.1.33333.1.1.1 (Integer)
Varbind 2:	.1.3.6.1.4.1.33333.1.2.1 (Octet String)

Varbind1 Type: Integer	Varbind1 Type Description: Status
Varbind1 Value	Description
1	Normal Status
2	Warning
3	Critical
Varbind2 Type: String	Varbind1 Type Description: Module with problem
Varbind2 Value	Description
CPU	CPU is the source of the problem
Temperature	Temperature is the source of the problem

Because this trap does not exist, no MIB defines the trap. Therefore, this example begins by creating the trap definition. However, normally, to begin, load the trap definition using the following command:

```
    First, load the MIB using:
nnmloadmib.ovpl -load <mib_file>
```

```
2. Load the trap using:
nnmincidentcfg.ovpl -loadTraps <mib_module_name>
```

To create the trap definition:

1. Navigate to the Configuration workspace, expand Incidents, and click SNMP Trap Configurations.

Figure 1.			
Ø Network Node Manager			User Name: syste
<u>Eile View Tools Actions Help</u>			
MANUTATION AND ADDRESS AND ADDRESS AND ADDRESS			
	▼ Ø ≧≅ @ Ø & ∷ □ < < ≅		
A Topology Maps	*	Atlantic osto Rebenio	
Monitoring	*	Stockholm O KETTONIA Poentug	
Troubleshooting	*	Ocean Guine Moon	
Inventory	*	O UNITED DEamans O	
Management Mode	8	RUSSIN - Mint	
🄥 Incident Browsing	*	Laber antendan Section Beckarus BELARUS	
Stream Performance Analysis	*	GERMANT POLAND	
Se Quality Assurance	×	Pratis Pratic CESOF	
Straffic Analysis	*	ERANCE Stand	
Integration Module Configuration	*	AUTTRIAND AUSTRIA DECEMBER HUNGARY ROMANIA	
Configuration Communication Configuration Discovery Monitoring Incidents Incident Configuration	×	PORTUGAL SPAIN SPAIN Of Manuel SPAIN Of MANUEL	
(SNMP Trap Configurations)	Updated: 8/4/14 04:04:05 PM	0 Nodes	
Syslog Message Configuration:	Analysis		
Management Event Configurat	Summary 🛱		
Pairwise Configurations Custom Correlation Configurati Trap Server Status Configuration	No Objects Selected		
Calus computation	1		

2. Navigate to the SNMP Traps tab and select the * icon.

Figure 2.

Network Node Manager													
ile ⊻iew <u>T</u> ools Agtions <u>H</u> elp													
V	SNMP Trap Configurations												
Incident Management 🛛 🕹	🖉 💽 🖻 🛯 🖉 🖉 🖓	n 🗙 🔛											⊠ <
Topology Maps 🛛 😵	Name 🔺	SNMP Object ID	Enabled		Deduplicat		Se (Cat F	a Author	M	lessage Format		
Monitoring ¥					on Enabled	Enabled		eg m ory y	nil				
Troubleshooting &	ArcSightEvent	1.3.6.1.4.1.11937.0.1							s HP ArcSight		1.3.6.1.4.1.11937.1.46.1		
Inventory ¥	BGPBackwardTransition		~	~ .	~				L Customer				
Management Mode 🛛 🕹	BGPBackward I ransition	.1.3.6.1.2.1.15.0.2		v .	•	1						83 (Stext(\$3)), Last Error: \$2, Neighbor: \$1	
Incident Browsing ¥	BGPEstablished	.1.3.6.1.2.1.15.0.1	~	-	÷	•	⊘ N :	≭ ⊧ 5	L Customer	B	GP Established: State \$3 (Stext	(\$3)), Last Error: \$2, Neighbor: \$1	
	CempMemBufferNotify	.1.3.6.1.4.1.9.9.221.0.1	~		÷		🕗 N 🗄	≭ ⊧ 1	C HP Network I	Noc M	emory buffer \$1 has been upda	ted	
	CiscoChassisAlarmOff	.1.3.6.1.4.1.9.5.0.6			~		0 N :	≭ ⊧	HP Network I	Not Ci	isco Chassis Alarm Off Condition	1	
Traffic Analysis 🛛 😵	CiscoChassisAlarmOn	.1.3.6.1.4.1.9.5.0.5			~		A	4.5	C. UD Mature 1		isco Chassis Alarm On Condition		
C Integration Module Configuration 🛛 😵													
Configuration	CiscoChassisChangeNotificati	.1.3.6.1.4.1.9.5.11.2.0.2		· ·	~		∆ v :	≭ F ∞	The HP Network M	Noc Ci	isco Chassis Change Notification	1	
🚰 Communication Configuration 🔺	CiscoColdStart	.1.3.6.1.6.3.1.1.5.1.1.3.6.1.4.	~	-	-	~	🛛 N 🗧	¥⊧ £	N HP Network 1	Noc Ci	isco Agent Up with Possible Cha	anges (coldStart Trap)	
* 🗀 Discovery	CiscoDemandNeighborLayer2	.1.3.6.1.4.1.9.9.26.2.0.3			~		Δ.v =	# F 🖉	L HP Network N	Noc De	emand Neighbor Layer 2 Chang	ge on interface \$1, status \$2 (\$text(\$2))	
Monitoring Definition	CiscoEnvMonFanNotification	.1.3.8.1.4.1.9.9.13.3.0.4	~				🕴 c :	≭	C HP Network 1	Noc Fa	an state change on node compo	onent \$1, state \$2 (\$text(\$2)).	
	CiscoEnvMonFanStatusChan;	.1.3.6.1.4.1.9.9.13.3.0.8	~				8 c :	#c 1	HP Network I	Noc Fa	an state change on node compo	onent \$1, state \$2 (Stext(\$2)).	
SNMP Trap Configurations	Updated: 8/4/14 04:41:15 PM					1	fotal: 125			Sele	ected: 0	Filter: OFF	
I Syslog Message Configurations	Analysis												
Management Event Configural	Summary 🛱												
m Pairwise Configurations		o Objects Selected											
Custom Correlation Configurati		o objects selected											

- 3. In the Name attribute, enter TestApp.
- 4. In the SNMP Object ID attribute, enter .1.3.6.1.4.1.33333.0.1
- 5. Click Enabled.
- 6. Click Root Cause so that these traps will display in the Key Incidents view.
- 7. In the Category attribute, select Application Status.
- 8. In the Family attribute, select Node.
- 9. In the Severity attribute, select Warning.
- 10. In the Message Format attribute, enter "TestApp \$1 \$2".
- 11. In the Author attribute, select Customer.
- 12. Click Save and Close to save the changes.

Figure 3.

	Save and Close 🖉 🗙 Delete SNMP Trap Configuration 🛛 🔛			
 Basics 			Interface Settings	Node Settings
For information ab	out troubleshooting Incidents, click here.		•	•
• Name	TestApp		NNMi enables you Group. Interface S	
	t ID (OID) attribute accepts one wildcard character (*) that must appear at the end of the	1	Settings tab.	
OID specified. NN more information.	Mi permits wildcards only in OIDs beginning with .1.3.6.1.4 (private MIBs). Click here for		* 🖻 🖉	ී 🗙
			Interface Group	Ordering
* SNMP Object II	.1.3.6.1.4.1.33333.0.1			
Enabled				
Root Cause				
 Category 	Application Status			
 Family 	Node			
 Severity 	Warning			
message use \$(var	cident message appears in the Incident view. To include Incident information in the iable_name). Select these variables from a set of valid parameters or Custom Incident e information, click here .	-		
wessage Forma				
TestApp \$1 \$2				
-		-		
TestApp \$1 \$2		-		

13. Next, use the nnmsnmpnotify.ovpl command to send the example traps:

nnmsnmpnotify.ovpl -a 10.210.109.1 localhost .1.3.6.1.4.1.33333.0.1 .1.3.6.1.4.1.33333.1.1.1 integer 2 .1.3.6.1.4.1.33333.1.2.1 OCTETSTRING CPU # nnmsnmpnotify.ovpl -a 10.210.109.1 localhost .1.3.6.1.4.1.33333.0.1 .1.3.6.1.4.1.33333.1.1.1 integer 1 .1.3.6.1.4.1.33333.1.2.1 OCTETSTRING Temperature

Note

- This command must be run from the NNMi server
- Each nnmsnmpnotify.ovpl is a single line

To confirm that NNMi has received the traps:

- 1. Navigate to the Incident Browsing workspace.
- 2. Click Open Key Incidents to confirm that the traps have been received

Note

Use the pull-down menu to change the time period if necessary.

Figure 4.

Metwork Node Manager																User Name: system	NNMi Role: Adm
Ele Yiew Icols Agtions Help																	
② Dashboards		Open Key Incidents															
ncident Management	t Management 🛞 📴 😽 🕫 🦃 🔊 🌵 🗶 🗳											Last Hour V <empty c<="" th=""><th>Broup filter></th></empty>	Broup filter>				
Open Key Incidents	111	Seve	Pric	ori Life	ecj I	Last Occurrence . Ti	Assigned To	Source Node	Source Object	Cates	Fan	nil Orig	Corr	Message	Notes		
I Unassigned Open Key Incidents	4		s.[5	1	8/4/14 5:00:32 PM		ciscope6524	none			\$890	₩.	TestApp 1 Temperature			
My Open Incidents	4		5.	5	4	8/4/14 5:00:15 PM		ciscope6524	none		1	5404	Ψ	TestApp 2 CPU			

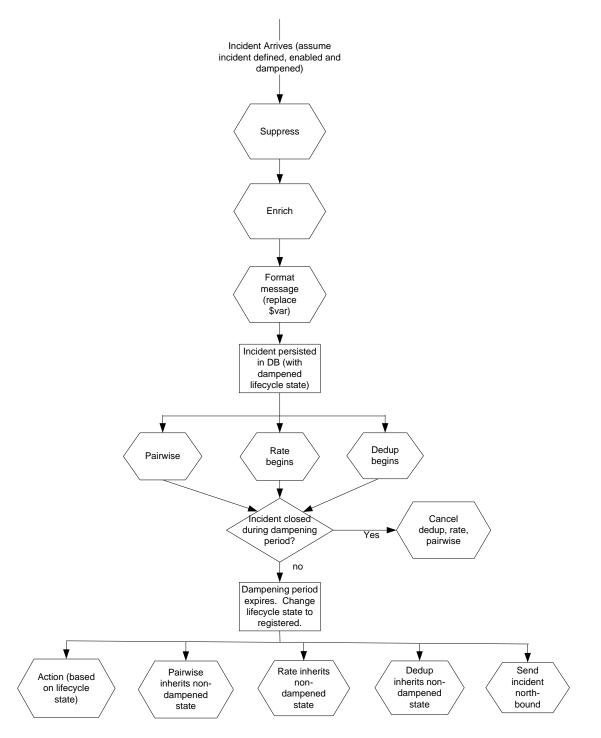
Now you are ready to begin working with these traps.

Dampening and the Incident Pipeline

NNMi provides the Incident Dampening feature to enable you to ignore network "noise" in which interfaces and nodes are down for short periods of time. With Incident Dampening, NNMi behaves as if the short outages never occurred. To identify these incidents, NNMi uses the Dampened Lifecycle State. The Dampened Lifecycle State precedes the Registered Lifecycle State.

The following flowchart provides a summary of where Dampening fits into the NNMi Incident Pipeline.

Figure 5.



As shown in the preceding flowchart, when an incident arrives, NNMi checks whether the incident can be suppressed and immediately discarded. If an incident is not suppressed, NNMi determines whether an Enrichment Configuration is enabled for the incident. (Enrichment Configuration is used to customize a subset of incident configuration attributes, such as Message Format or Priority.)

Next, NNMi replaces any parameter strings (for example \$sourceNodeName) specified in the Message Format.

If Dampening is enabled for the incident, NNMi sets the Lifecycle State to Dampened. If Dampening is not enabled for the incident, NNMi sets the Lifecycle State to Registered.

After the Lifecycle State is set, Rate and Deduplication correlations, as well as Pairwise matching takes place.

If NNMi cancels the incident and sets the Lifecycle State to Closed during this Dampening period, NNMi discards the incident and discontinues any Rate or Deduplication correlation and Pairwise matching. If the Dampening period expires, NNMi sets the Lifecycle State to Registered and continues any Rate or Deduplication correlation and Pairwise matching.

Customizing Incident Configurations Using Interface or Node Groups

Incidents can be customized based on Interface Groups or Node Groups. This feature is reflected in the incident configuration form. When a trap arrives into the Incident Pipeline (after it has cleared any filtering), NNMi compares the SNMP trap to the Interface Settings to see if the source of the trap is a member of this Interface Settings group. If NNMi finds a match on the source interface (source object), NNMi applies the Suppression, Enrichment, Dampening, and Actions specific to that Interface Group.

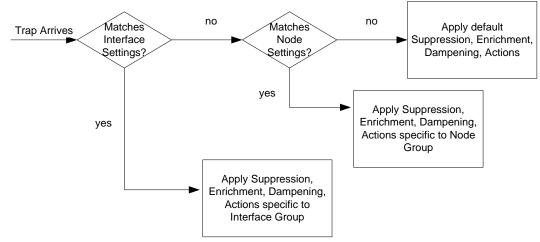
Note

If one of these tabs is disabled (for example, Enrichment), NNMi does not use the default Enrichment.

If the source interface does not match any Interface Settings, NNMi compares the source node to the Node Settings group. If NNMi finds a match on the source node, NNMi applies the Suppression, Enrichment, Dampening, and Actions specific to that Node Group.

If the source node does not match any Node Settings, then the default Suppression, Enrichment, Dampening and Actions are applied.

Figure 6.



NNMi applies Deduplication and Rate Correlation independent of Interface Settings and Node Settings.

To view the Incident Configuration options for Interface and Node Settings:

- 1. Navigate to the Configuration Workspace.
- 2. Open Incidents and select SNMP Trap Configurations.
- 3. Locate and select the TestApp trap, and then click the $\stackrel{{\scriptstyle{\bigsqcup}}}{=}$ Open button

Figure 7.

Network Node Manager												User Name: syste
ile <u>V</u> iew <u>T</u> ools Agtions <u>H</u> elp												
Dashboards 🛛 🕹	SNMP Trap Configurations											
Incident Management 🛛 🕹	🖉 * 🔁 🖉 🔊 א	🔊 🗙 🔛										
Topology Maps 🛛 🕹	Name 🔺	SNMP Object ID	Enabled	Root	Deduplicat	Rate	Se	Cat	Fa	Author	Message Format	
Monitoring ¥				Cause	ion Enabled	Enabled	ver ity	eg ory	mil v			
Troubleshooting ¥	STPNewRoot	.1.3.8.1.2.1.17.0.1	-	-	~	-		-	-	HP Network Not	STP New Root	
Inventory 😵	STPTopologyChange	.1.3.6.1.2.1.17.0.2			~			÷.,	.	HP Network Nor	STP Topology Change	
Management Mode 🛛 🕹												
Incident Browsing ¥	SiteScopeAlertEventv1	.1.3.6.1.4.1.11.15.1.4.0.1	~	-	-	-					Alert "\$.1.3.6.1.4.1.11.15.1.3.1.2" w	
Performance Analysis 🛛 💝	SiteScopeAlertEventv2	.1.3.6.1.4.1.11.15.1.4.1	~	-	-	1.0	😵 c	× F	R 🖉	HP SiteScope	Alert "\$.1.3.6.1.4.1.11.15.1.3.1.2" w	as triggered on monitor "\$.1.3.6.1.4.
Quality Assurance 🛛 💝	SyslogMessage	.1.3.6.1.4.1.9.9.41.2.0.1	-	-	-		Δv	×ε	5 I.	HP Network Not	\$1:\$3 \$4 (syslog)	
Traffic Analysis 🛛 😵	TestApp	.1.3.6.1.4.1.33333.0.1	~	~			Δv	1917 A	10 N	Customer	TestApp \$1 \$2	
Integration Module Configuration 🛛 😵	TrafficEntryExitMismatched	.1.3.6.1.4.1.8083.1.1.12.3.46	-	-	-	-		*		HP Route Analy	Entry exit mismatch between \$5/\$6	and \$9/\$10
Configuration 🔅	TrafficHighLinkUtilization	.1.3.6.1.4.1.8083.1.1.12.3.36							-	HP Route Analy	Traffic high linkUtil in \$4 for link: sro	S5 dest S6 sroType 13 destType S14
🚰 Communication Configuratio 📤	TrafficLinkCoSUtilization	.1.3.6.1.4.1.8083.1.1.12.3.38									Traffic high CoS linkUtil in \$4 for lin	
🔹 🧰 Discovery											Traffic low linkUtil in \$4 for link: src \$	
Monitoring	TrafficLowLinkUtilization	.1.3.6.1.4.1.8083.1.1.12.3.37		•	•	-						
Decidents Incident Configuration	TrafficQuantityAlert	.1.3.6.1.4.1.8083.1.1.12.3.35	1	-		1.0	V 🔍	× ₽	e e	HP Route Analy	Traffic quantity alarm: trapInfo \$4 th	reshold \$5 clearThreshold \$6
SNMP Trap Configuration	Updated: 8/6/14 07:11:24 AM					Total: 126 Selected: 1 Filter: OF						
	Analysis											
Management Event Confi	SNMP Trap Configuration St	ummary : TestApp			D	atails 🛱						
Pairwise Configurations						abled					true	
Custom Correlation Config		.1.3.6.1.4.1.33333.0.1 TestApp \$1 \$2				verity					A Warning	
Trap Server	inclouge Format					egory nily					Application Status Node	
Status Configuration						ot Cause					true	
Global Network Management					Au	hor					Customer	
User Interface												
Security												
MIBs												

The graphic below indicates how the various tabs apply to this concept

Figure 8.

	Save and Close 3 X Delete				
- Basics				A Hertace Settings Node Settings Suppression Enrichment Dampening Deduptication Rate	(Actors)
For information about to	subieshooting incidents, click here				1
Name SNBP Object ID Enabled Root Cause	TestApp 1361413333301			Narrows context to specific Interfaces and Nodes to the floor Settings tell	if no
Category	Application Status	-	1.	Interfaces or N	odes
• Family	Node		9 -		
· Severity	Warning -				

Deduplication

NNMi's Deduplication feature enables you to correlate duplicate incidents under a new incident. It also deletes duplicate incidents once a specified number of duplicate incidents are generated.

This example configures Deduplication for the TestApp SNMP trap configuration.

- 1. Navigate to the **Configuration** Workspace.
- 2. Open Incidents and select SNMP Trap Configurations.
- 3. Locate and select the TestApp trap, and then click the Open 📑 button.
- 4. Click to check Enabled.
- 5. Navigate to the **Deduplication** tab.
- 6. In the **Count** attribute, enter the number of TestApp traps that NNMi should retain in the database for a particular Deduplication time period. The maximum number is 10. For this example, enter **2**.
- 7. In the **Hours**, **Minutes**, and **Seconds** attributes, specify the time that must elapse before a new duplicate incident is generated for this incident configuration. For this example, in the Minutes attribute, enter **3**
- 8. Next, in the **Parent Incident** drop-down list, select the incident that you want NNMi to generate to indicate that Deduplication has occurred. For this example, select **DuplicateCorrelation**.
- 9. Last, specify the Comparison Criteria. The Comparison Criteria specifies what attributes NNMi should use to decide what constitutes a duplicate. This example uses Name and SourceNode. This means that when two TestApp SNMP traps arrive, NNMi considers them to be duplicate if the SNMP traps have the same name (TestApp) and the same SourceNode (came from the same device in the network).

Figure 9.

🕼 Network Node Manager						User Name: sys	tem NNMiRo	le: Administrator	· s	ign Out
File View Tools Actions Help										
♠ Incident Management ¥			1 69							
A Topology Maps 🛛 🕹	🗵 📴 🖺 🎽 Save and Close 😂 🗙 Delete SNMP Tr	ap Configur	ation 📔							
Monitoring ¥	▼ Basics		Suppression	Enrichment	Dampening	Deduplication	Rate	Actions	Forward to G	b v
Troubleshooting ¥	For information about troubleshooting Incidents, click here.		Capprocolon	Lintoniton	bumponing		Tuto	, 1010110	ronnandro q	× ×
Inventory ¥										
Management Mode *	Name TestApp					uld match to dete Incident. NNMi tr				
🏠 Incident Browsing 🛛 🕹 🕹	SNMP Object ID .1.3.6.1.4.1.33333.0.1	va		as the Duplicat	e Count attribu	e. It is incremente	d on the Dupli	cate Correlation	Incident.	
Integration Module Configuration \Rightarrow	Enabled 🔽 Root Cause 🔽	(Enabled Count							
✤ Configuration	Category Application Status		Hours	2						
📑 Communication Configuration 📤	* Family Node V	_	Minutes	3						E
🛅 Discovery		=	Seconds	0						
📧 🧰 Monitoring	* Severity Warning -		Parent Incident	D	uplicateCorrela	tion			- 🗊 -	
Incidents	Specify how the Incident message appears in the Incident view. To									
Incident Configuration	include Incident information in the message use \$(variable_name).		Comparison Cr	iteria Na	Name SourceNode v					
SNMP Trap Configurations	Select these variables from a set of valid parameters or Custom Incident attributes. For more information, click here.	-	✓ Deduplication Comparison Parameters							- U
🕅 Syslog Message Configurati 🗏	A Marca - Franci		-							
🕮 Management Event Configur	* Message Format TestApp \$1 \$2		* 🖻 Ø	×		IS 🔷 0-0	of O	(> 🛛 🖻	
m Remote NNM 6.x/7.x Event C	TestApp \$1 \$2		Parameter Val	ue					•	
Pairwise Configurations	Description									
📑 Custom Correlation Configur		-								-

The following diagram depicts the following scenario:

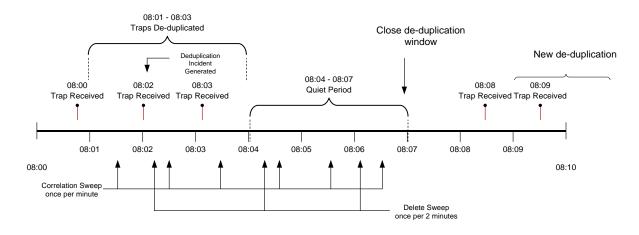
The first TestApp SNMP trap arrives at 8:00. Another trap with the same name and source node arrives at 8:02. NNMi generates a new DuplicateCorrelation incident. At 8:03 another trap arrives. In addition, every minute NNMi sweeps the incidents to determine whether to correlate duplicate incidents. At approximately 8:02:30, NNMi correlates the first two SNMP traps under the DuplicationCorrelation incident and marks them as Correlated Children. At 8:03:30, NNMi correlates the third SNMP trap as a child to the DuplicationCorrelation incident. At approximately 8:04:15, NNMi checks whether more than two TestApp SNMP traps are correlated under a single DuplicationCorrelation. NNMi deletes one of the TestApp SNMP traps because the total number is three.

Note

Although NNMi deletes the third SNMP trap from the NNMi database, the total count of 3 is retained in the DuplicateCorrelation incident as the Duplicate Count.

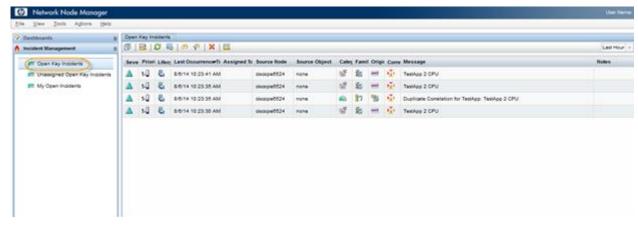
After SNMP traps stop arriving for three minutes (the time window for this Deduplication), NNMi closes the Deduplication time window. At 8:08 a new TestApp trap arrives. At 8:09 another TestApp SNMP trap arrives from the same node. This begins the cycle again. NNMi generates a new DeduplicationCorrelation incident and continues to evaluate each incident as previously described.

Figure 10.



The following image depicts how these incidents might appear in the Open Key Incidents view. Note that the times in the example below do not correspond exactly with the timeline above, but the order is similar. As shown in the example, three traps arrived and a new DuplicateCorrelation incident is generated.





When NNMi sweeps the incidents to determine whether to correlate duplicate incidents, it correlates the three traps under the DuplicateCorrelation incident as shown in the following example

Figure 12.

Open Key Incidents In	oident					
🖉 🖗 🛅 🗃 See	e and Close 💭 🗙 Delete Incident 🔚					
* Basica		÷	General Correlated Parents Correlated Children	Custom Attributes Diagnostics Regis	tration	
Message						
Duplicate Correlation for	r TexhApp: TexhApp 2 GPU		3 8 0 0			10 0 1-3#3 0 01 E
-	C		Seve Last Occurrence Type	Message	Source Node	Source Object
* Severity	Warring +		A 8/6/14 10:13:05 A De-Dup Correlation	TextApp 2 CPU	oixoope01024	none
* Priority	Note v		A 8/6/14 10:12:55 A De-Dup Correlation	TextApp 2 CPU	discope0124	none
Lifecycle State	Registered -		A 8/014 10/12/48 A De Out Correlation	TestApp 2 CPU	discopetit24	none
Source Node	discope0124	a • 1				
Source Object	none					
Assigned To		• .				
- Notes						
Notes						
			Updated: 8/6/14 10:14:21 AM	Total 3 Beleded 0	Filter, OFF	Auto rafeah: OFF
Analysis						

Next, NNMi checks whether more than two TestApp SNMP traps are correlated under a single DuplicationCorrelation and deletes one of the TestApp SNMP traps so that at most two traps are stored in the NNMi database

Figure 13.

Open Kay Incidents In	Here 7							
🖉 🖗 🛅 🕲 See	e and Close 💭 🗙 Delete Incident 🔛							
• Basia			Oeneral	Correlated Parent	a Constaned Children) (Custom Attributes Diagnostica Re	gistration	
Message								
Duplicate Correlation for	TestApp: TestApp 2 CPU						1	0 0 1-2+2 0 01 🕅
	(=		Seve: Las	d Occurrence Ten	Tope	Message	Source Node	Source Object
* Severity	Warning +				De Oup Correlation	TestApp 2 CPU	oixcope0124	none
* Priority	Note		1 20	14 10:12:55 AM	De-Dup Correlation	TestApp 2 CPU	discipation 4	none
 Lifecycle State 	Repaired							
Source Node	discipatit24	a •						
Source Object	none							
Assigned To								
• Notes								
Notes								

Finally, after no new duplicate incidents are generated within a period of three minutes, NNMi closes the Deduplication and generates a new Deduplication incident when a new TestApp SNMP trap arrives.

Tip

The longer the time period, the more Deduplication NNMi can track.

Note

Please note that the "Correlation Nature" of a Duplicate Correlation incident is decided based on the correlation nature of the underlying child incidents. For example, if an 'Origin' is "SNMP Trap" or "Syslog" for a particular incident (trap or syslog) and if this incident is configured as "Root Cause" in the Incident Configuration then "Duplicate Correlation" incident's Correlation Nature will be set to "Root Cause" else it will be set to "Dedup Stream Correlation".

Once correlated, underlying correlated children events' Correlation Nature is marked as "Symptoms" if it was "Root Cause" before correlation.

Rate

Rate configuration enables you to track incident patterns based on the number of incident reoccurrences within a specified time period. After the count within the specified time period is reached, NNMi emits a Rate Correlation incident and continues to update the Correlation Notes with the number of occurrences within that rate. NNMi correlates the incidents under the Rate Correlation incident while they are within the specified time period. Unlike Deduplication, Rate Correlation never deletes incidents from the database.

This example configures the Rate so that NNMi generates a Rate incident when three or more TestApp SNMP traps occur within a two-minute time period.

First, disable the Deduplication Incident Configuration

- 1. Navigate to the Configuration Workspace.
- 2. Open Incidents and select SNMP Trap Configurations.
- 3. Locate and select the TestApp trap, and then click the Open button.
- 4. Navigate to the Deduplication tab.
- 5. Click to clear Enabled

Next, specify the Rate configuration for the TestApp SNMP trap incident.

- 1. Navigate to the Rate tab.
- 2. Click to check Enabled.
- 3. In the Count attribute, enter 3.
- 4. In the Minutes attribute, enter 2.
- 5. In the Parent Incident drop-down list, select RateCorrelation.
- 6. In the Comparison Criteria drop-down list, select Name SourceNode.
- 7. Click Save and Close to save the configuration

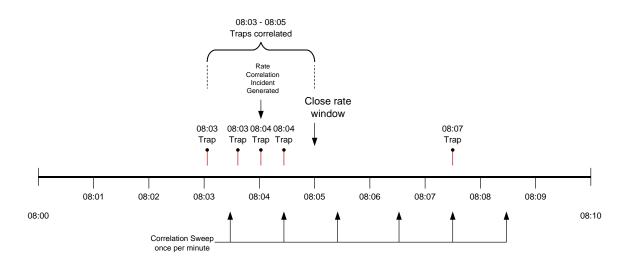
Figure 14.

- Basics		Â		Enrichment	Dampening	Deduplication	Rate	Actions	Forward to Global Managers
For information about tr	oubleshooting incidents, click here.		-	•					
Name SNMP Object ID	TestApp .1.3.6.1.4.1.33333.0.1			specified time pr	eriod. After th	e count within the	specified time	period is reach-	dent reoccurrences within a ed, NNMI emits a Rate Correlation turrences within that rate
Enabled			1	Enabled		2			
Root Cause	a			Count		3			
 Category 	Application Status 👻 🎼 💌			Hours		0			
. Fresh	Node 👻 🕼 🔻			Minutes		2			
 Family 	Node			Seconds		0			
 Severity 	Warning	. 11		Parent Incide	nt	RateCorrelation			- 🐲 -
include Incident information	nt message appears in the Incident view. To tion in the message use \$(variable_name). from a set of valid parameters or Custom			Comparison (Oriteria	Name SourceNode	•		
	more information, click here.			· Rate Comparis	son Paramete	rs			
Message Format				* 🖬 🕻	x		000-0	of	
TestApp \$1 \$2				Parameter V	1				
Description		- Ш		Parameter	alue				-

The following diagram depicts the following scenario:

The same network device generates four TestApp SNMP traps, each about 20 seconds from the previous one. Because these traps fit within the two-minute time window, when three TestApp SNMP traps occur within a two-minute time period, NNMi generates a new RateCorrelation incident. During the two-minute period, NNMi correlates all TestApp SNMP traps from this same source. After two minutes, NNMi closes the Rate time period. When another TestApp SNMP trap arrives outside of this time period, NNMi does not correlate the incident as part of this Rate correlation

Figure 15.



Similar to Deduplication, NNMi only checks for Rate correlations once per minute. Eventually the incident views show all the TestApp SNMP traps within the time period specified and they are correlated under the RateCorrelation incident.

The following image depicts how these incidents might appear in the All Incidents view. As shown in the following example, NNMi correlates the first four traps under the Rate Correlation incident because they are within the two-minute window. When another TestApp SNMP trap arrives outside of the two-minute window, NNMi does not correlate the incident.

Figure 16.

Dashboards	¥ Al I	ndidenti										
Incident Management	. 3	8	0	တ ကု 🗶 🔛								
L. Topology Maps	8 Sev	Prio	ri Lifer	c Last Occurrence/Ti Assigned 1	ls Source Node	Source Object	Cale	Fami	i Orig	Corr	Message	Notes
Monitoring	*	5.0	3	8 10 14 10 53 49 AM	ciscopett24	none	15	影	int.	6	TextApp 2 CPU	
Boubleshooting	*	s.Q	3	8/0/14 10:52 20 AM	discope6524	none		17	-	4	Rate Correlation for TestApp: TestApp 2 CPU	
Management Mode	- A	5.0	3	8/0/14 10 52 20 AM	discepett24	none	10	影	-	-	TestApp 2 CPU	
Incident Browsing		5.0	3	8/8/14 10:51:54 AM	oiscepett24	none	1		-	3-	TestApp 2 CPU	
Coen Key Incidents		sQ	3	8-6/14 10:51:23 AM	ciscope0024	none	12	彩	-	3-1	TextApp 2 CPU	
Closed Kay Incidenta		5.0	3	8-0/14 10:51:00 AM	ciscope0624	none	1	影	-	3	TextApp 2 CPU	
Open Root Cause Incidents Service Impact Incidents All Incidents												
Custom Open Incidents	1											
Custom Incidents												
NNM 6.x/7.x Events												
E Syslog Messages												

As shown in the following example, because they are not Root Cause incidents, these correlated incidents do not appear in the Open Key Incidents view.

Figure 17.

Yiew Jools Agtions Help		-									
Dashboards &		cidenta (1. C	X X	eR.			_	_	_	_	
ncident Management A			Last Occurrence Ta		Source Node	Source Object	Calles	Famil	Origi	Corre	Message
Unassigned Open Key Incidents	s.J	ε,	8/6/14 10:53:49 AM		oiscope0524	none	5	能	-	4	TestApp 2 CPU
My Open Incidents	s.	з,	8/6/14 10:52:20 AM		ciscope0524	none	6	17	3	r.	Rate Correlation for TestApp: TestApp 2 CPU

To view the Correlated Children, open the Rate Correlation incident and navigate to the Correlated Children tab

Figure 18. Open Key Inddents Inddent | • Basics General Corel Ibutes Diagnostics Registration melated Children Message ٠ Rate Correl on for TestApp: TestApp 2 CPU 3 😫 🛛 🔿 0 0 1-4040 Seve Last Occur Source Object Source Node renae Type Message Severity Warning A 8/6/14 10:52:26 A Rate Correlation TestApp 2 CPU discope6524 none None 8/5/14 10:51:54 A Rate Correlation TestApp 2 CPU oiscope0524 none Lifecycle Registered ۸ 8/6/14 10:51 23 A Rate Correlation TestApp 2 CPU discope0524 A 8/6/14 10 51 00 A Rate Correlation Source ciscope6524 TestApp 2 CPU damentt24 Source Object - 1 Assigned To · Notes No

Navigate to the General tab to see information about the rate correlation in the Correlation Notes. The Correlation Notes are updated throughout the Rate time period that is specified.

Figure 19.

Open Kay Insident Insident	
🕑 😳 🛅 🛐 Save and Close 💋 🗙 Delete Incident 🔛	
+ Basics	General Correlated Parents Correlated Children Custom Attributes Diagnostics Registration
Message	* Details
Rate Correlation for TestApp 2 CPU * Seventy * Dirolity None • Lifesyde State	Name RateCorrelation Category Performance Family Completion Origin NMAI Correlation Root Cause
Source Node discopetit24	Duplicate Count 0 RCA Assive Comelation Notes
Source Object none Assigned To	Configured rate acurit: 3 incidents Configured rate internat: 0 hours, 2 minutes, 0 seconds Incident coourred 4 times from Wednesday, August 6, 2014 10:51:00 AM IST to Wednesday, August 6, 2014 10:52:26 AM IST.
• Notes	First Occurrence Time August 6, 2014 10:51 00 AM IST Last Occurrence August 6, 2014 10:52 26 AM IST Origin Occurrence August 6, 2014 10:51 00 AM IST

Note

Please note that the "Correlation Nature" of a Rate Correlation incident is decided based on the correlation nature of the underlying child incidents. For example, if an 'Origin' is "SNMP Trap" or "Syslog" for a particular incident (trap or syslog) and if this incident is configured as "Root Cause" in the Incident Configuration then "Rate Correlation" incident's Correlation Nature will be set to "Root Cause" else it will be set to "Rate Stream Correlation".

Once correlated, underlying correlated children events' Correlation Nature is marked as "Symptoms" if it was "Root Cause" before correlation.

Enrichment

This example uses Group Settings with Enrichment. The Node Groups used for the Node Group Settings are named Core Routers and Important Servers Node.

The Enrichment feature enables you to modify an incident when it is processed by NNMi. The types of items that you can modify for a selected incident configuration include:

- Category
- Family
- Severity
- Priority
- Correlation Nature
- Message
- Assigned To
- Custom Attributes

In this example, when the TestApp trap arrives from a router in the Core Routers Node Group, the Incident is enriched so that the Priority is Top. The Message Format is also customized and the incident is assigned to the user (TJ) who is in charge of the Core Routers. When the TestApp trap arrives from a server in the Important Servers Node Group, the incident is

To edit the Enrichment configuration for the TestApp SNMP trap incident:

- 1. Navigate to the Configuration Workspace.
- 2. Open Incidents and select SNMP Trap Configurations.
- 3. Locate and select the TestApp trap, and then click the 📴 **Open** button.
- 4. Navigate to the Node Settings tab.
- 5. Click the * New icon.

Figure 20.

SNMP Trap Configurations SNMP Trap Configuration		
🎯 🗟 🛅 🐮 🕲 Save and Close 🖉 🗙 Delete SNMP Trap Configuration 🔛		
Basics for information about troubleshooting incidents, click here.	C Interface Settings Node Settings Suppression Enrichment Dampening Deduptication Rate Actions Forward	1 to 🤇 🕨 🔫
Name TestApp SNMP Object D . 1.3.6.1.4.1.33333.0.1 Enabled	NMM enables you to apply a Suppress, Enrich, Dampen, Action, or Disgnostics Selection configuration to a Source Node based on the Source No participation in a Node Group, Node Settings override any other Suppress, Enrich, Dampen, Action, or Disgnostics Selection configuration setting incident, except those configured on the Interface Settings tab.	a for this
Enabled Root Cause Category Application Status	New Yap A Ordering Enabled	
* Famiy Node * 🕃 * a		
Specify how the incident message appears in the incident view. To include incident information in the message use §(variable_name). Select these variables from a set of valid parameters or Custom incident attributes. For more information, click here .		
* Message Format		
TestApp \$1 \$2		
Description		
• Author Customer • 🐨 💌 •	Total 0 Selected 0 Filter: OFF Auto refree	ah: OFF

- 6. In the Node Group drop-down list, select the Core Routers Node Group.
- 7. In the **Ordering** attribute, enter 10.

Note

The Ordering attribute determines which Node Settings are applied to a node that is a member of more than one Node Group.

- 8. Click to check Enabled.
- 9. Navigate to the **Enrichment** tab.
- 10. Click the *** New** icon.

Figure 21.

- gare = ···	
File View Tools Actions Help	
Node Settings *	
😼 🛅 🎦 Save and Close 🞜 🗙 Delete Node Settings 🖥	
Changes are not committed until the top-level form is saved!	
▼ Basics	Suppression Enrichment Dampening Actions Diagnostic Selections
* Node Group Core Routers 👻 🕼 💌	▼
* Ordering 10 Enabled 💟	Enrichment enables you to do the following: Change an Incident configuration's Category, Family, Severity, Priority, Correlation Nature, Message Format, and Assigned To values. Add Custom Incident Attributes to the Incident before it is stored in the NNMi database. Test enrichment configuration by selecting an Incident and choosing Actions → Incident Configuration Reports → Report Enrichments. Enabled
	▼ Enrichments
	K K S K K K K K K K K K K K K K K K K K
	C New Prior Corr Assigned To Message Format Description

- In the Priority drop-down list, select Top.
 In the Message Format attribute, enter TestApp on Core Routers \$1 \$2.
- In the Assigned To attribute, select Quick Find to select a user from the list. In this example, TJ is a valid user.
- 14. Click Save and Close to return to the SNMP Trap Configuration Form.
- 15. Click Save and Close to save your changes

Figure 22.

iguic LL.											
File View Tools Ad	ctions Help										
Enrichment Configuration *	K										
😼 🖹 🎦 🖄 Save	and Close 😂 🗙 De	lete Enrichment Configu	ration	E							
		-									
Changes are not as	mmitted until the top-level fo	rm is saved									
T changes are not co	minited until the top-level it	ininis saveu:									
• 545/05				stom Attr	ibutes	Payload F	Filter				
Category		- 🗊 -	•								
Family		-		* 📑	0	×	Ø	0 - 0 of ()	0 01	=
Course to	Choose One 🔻			Туре		Custo	om Attribute Name		Custom Incider	nt Attribute Nam	е
Severity											
Priority	Тор										
Correlation Nature	Choose One 🔻										
Message Format											
TestApp on Core Routers	\$1 \$2										
Assigned To	TJ	- 🗊 -)									
-											
Description											
							Total:	0 Selected: () Filter: OFF	Auto refresh:	OFF
					_		Total.	Selected. (Auto renesil.	

Next, configure Node Settings for the Important Servers Node Group.

- 1. Navigate to the **Configuration** Workspace.
- 2. Open Incidents and select SNMP Trap Configurations.
- 3. Locate and select the TestApp trap, and then click the 📴 **Open** button.
- 4. Navigate to the **Node Settings** tab.
- 5. Click the * New icon

Figure 23.

SNMP Trap Configuration	s SNMP Trap Configuration *										
2 😼 💾 🎽	🔄 Save and Close 🛛 😂 🗙 Delete SNMP Tr	rap Configuration 🔛									
- Basics			^	4	Interface Settings	Node Setting	Suppression	Enrichment	Dampening	Deduplication	T
For information about tr	oubleshooting Incidents, click here.			•			u				
Name	TestApp				NMi enables you to articipation in a Node						
SNMP Object ID	.1.3.6.1.4.1.33333.0.1				cident, except those				aa, Ennon, Dan	ipen, Action, or t	510
Enabled					* 🖬 🖉	×				K 🔄 1	-
Root Cause					No New Pup	Ordering	Enabled				
* Category	Application Status	- 🗊 -			Core Routers	10	~				
* Family	Node	-	=			10					
* Severity	Warning 👻										
the message use \$(vari	nt message appears in the Incident view. To includ iable_name). Select these variables from a set of es. For more information, click here .										
* Message Format											
TestApp \$1 \$2											
Description											
								Total: 1	Selecte	d: 0	Fil
* Author	Customer	- 🗊 -	-					Total. 1	00.0010		

6. In the Node Group drop-down list, select the Important Servers Node Group.

- 7. In the Ordering attribute, enter 20.
- 8. Click to check Enabled.
- 9. Navigate to the Enrichment tab.
- 10. Click the * New icon

Figure 24.

File View Tools Actions Help	
Node Settings *	
🔯 💾 🎦 Save and Close 🧭 🗙 Delete Node Settings 🖺	
 Changes are not committed until the top-level form is saved! Basics 	Suppression Enrichment Dampening Actions Diagnostic Selections
 Node Group Important Servers Ordering Enabled 	Enrichment enables you to do the following: Change an Incident configuration's Category, Family, Severity, Priority, Correlation Nature, Message Format, and Assigned To values. Add Custom Incident Attributes to the Incident before it is stored in the NNMi database. Test enrichment configuration by selecting an Incident and choosing Actions → Incident Configuration Reports → Report Enrichments. Enabled Enrichments
	Image: Sever Prior Corr Assigned Te Message Format Description

Next, set the priority to High and change the Message Format.

- 11. In the Priority attribute drop-down list, select High.
- 12. In the Message Format attribute, enter TestApp on Important Server \$1 \$2.
- 13. Click Save and Close to return to the SNMP Trap Configuration form.
- 14. Click Save and Close to save your changes.

Figure 25.

igure Lo.			
File View Tools	Actions Help		
Enrichment Configuration *	3		
😼 📔 🎦 🕲 Sav	e and Close 🛛 😂 🗙 De	lete Enrichment Configu	uration 🔛
() Changes are not o	committed until the top-level fo	orm is saved	
- Basics			Custom Attributes Payload Filter
Category		- 🖉 -	•
Family		- 🖉 -	🖂 KA 🗢 0100-0 🗢 🖾 🗶 🖏 🖼 🛊
Severity	Choose One 👻		Type Custom Attribute Name Custom Incident Attribute Name
Priority	High		
Correlation Nature	Choose One 👻		
Message Format			
TestApp on important Se	rver \$1 \$2		
Assigned To		- 🗊 -	
-			
Description			
			Total: 0 Selected: 0 Filter: OFF Auto refresh: OFF
L			

Note

When you specify Interface Settings or Node Settings, all of the Incident Configuration tabs apply for that Interface or Node Group. For example, if the Suppression configuration is not enabled, NNMi does not use the global setting for Suppression. Instead, Suppression does not occur for that incident.

Figure 26.

ode Settings * 법 법 법 원 :	Save and Close 💋 🗙 Dek	te Node Settings	1			
(i) Changes are n	of committed until the top-level for	m is saved				
Basics			Suppression Enric	chment Dampening	Actions Diagnostic Sel	ections
Node Group	Important Servers					
Ordering	20				d the incident so that it does n	of appear in an incident view
Enabled	20		and is not stored in I	the NNMi database.		
			Enabled			
			· Payload Filter			
			participate in an ope pairwise. A Payload	ration; for example, be su	pressed, enriched, dampene dents based on Custom Incid	ting the incidents that should d, run actions, or participate in ent Attribute names (cialiame)
			ciaName	w [te	3	Append
						insert
						Replace
						Append +
						AND
						OR
			There is currently n	o filter defined.		NOT
						EXISTS
						NOT EXISTS
						Delete

Next, send a trap from each node to see the results.

As shown in the following example, the traps are enriched based on Node Group membership.

Figure 27.

ine Xien Ioola Albour Helb											
Dashboards W	Open	Keyle	odenti								
Incident Management	0	81	0.1	8 0 V X E							
Coen Key Insidents	Seve	m	Lifes	Last Occurrence Ti Assigned To	Source Node	Source Object	Categ	Fami	(Origi	Corte	Message
E Unassigned Open Key Indidents		2	ē,	8/6/14 11:12:30 AM	lptom10	none	12	わ	-	121	TestApp on Important Servers 2 CPU
My Open Incidents		12	E.	8-014 11 13 02 AM TJ	oixcope0524	none	1	診	-	121	TextApp on Core Routers 2 CPU
540 B 4050		9									

Suppression

Suppression enables you to discard traps based on specified filter values. For example, you can discard the TestApp SNMP trap incidents when the varbind value that stores Status is set to Normal or Warning for traps received from the Core Routers Node Group. This requires configuring Node Settings and Suppression.

Using the Payload Filter configuration feature, this example suppresses the trap if Varbind1=1 (Normal) or Varbind1=2 (Warning).

Tip

Use the absolute OID (Object Identifier) to specify the Varbind rather than position. For example, for Varbind1 you would specify 1.3.6.1.4.1.33333.1.1.1.

Figure 28.

SNMP Trap Configurations	SNMP Trap Configuration		
🗵 😼 💾 🎦 🗳	Save and Close 🛛 😂 💥 Delete SNMP Trap (Configuration 🖼	
Basics For information about trouble	leshooting Incidents, click here.	Interface Settings Node Settings Suppression Enrichment Dampening Deduplication Rat	e 🕨 🔻
Name SNMP Object ID Enabled	TestApp .1.3.6.1.4.1.33333.0.1	NNMi enables you to apply a Suppress, Enrich, Dampen, Action, or Diagnostics Selection configuration to a Sourn based on the Source Node's participation in a Node Group. Node Settings override any other Suppress, Enrich, D Action, or Diagnostics Selection configuration settings for this Incident, except those configured on the Interface tab.)ampen,
Root Cause * Category	Application Status	★ ★ ★ ★ ★ ★ ★ ★ ↓	
* Family * Severity	Node v Warning v	Important Servers 20	
Incident information in the m variables from a set of valid more information, click here	essage appears in the Incident view. To include essage use \$(variable_name). Select these d parameters or Custom Incident attributes. For		
* Message Format			
TestApp \$1 \$2			
Description			
		Total: 2 Selected: 1 Filter: OFF Auto refres	h: OFF

To edit the Suppression configuration for the TestApp SNMP trap incident:

- 1. Navigate to the Configuration Workspace.
- 2. Open Incidents and select SNMP Trap Configurations.
- 3. Locate and select the TestApp trap, and then click the Open button.
- 4. Navigate to the Suppression tab.
- 5. Click to check Enabled.
- 6. In the Payload Filter, do the following:

Note

You must use a top level OR operator in an expression that is two levels deep as shown in this example.

- A. Make sure Append appears as the selection in the drop-down list.
- B. Click OR.
- C. Click AND.
- D. In the Attribute drop-down list, select ciaName.
- E. In the Operator attribute, select =.
- F. In the Value attribute, enter .1.3.6.1.4.1.33333.1.1.1
- G. Click Append.
- H. In the Attribute drop-down list, select ciaValue.
- I. In the Operator attribute, select =.
- J. In the Value attribute, enter 1.
- K. Click Append.
- L. Click AND.
- M. In the Attribute drop-down list, select ciaName.

- N. In the Operator attribute, select =.
- 0. In the Value attribute, enter .1.3.6.1.4.1.33333.1.1.1
- P. Click Append.
- Q. In the Attribute drop-down list, select ciaValue.
- R. In the Operator attribute, select =.
- S. In the Value attribute, enter 2.
- T. Click Append
- 7. Click Save and Close to return to the SNMP Trap Configuration form.
- 8. Click Save and Close to save your changes.

Figure 29.

Eile View Iools	Agtions Help					
Node Settings *						
😺 💾 🐮 🕲 s	Save and Close 💋 💢 D	lete Node Settings	-			
(i) Changes are r	not committed until the top-le	el form is saved!				
▼ Basics			Suppression Enrich	ment Dampening	Actions Diagnostic Se	lections
Node Group	Core Routers	*	·	ion enables usu to discu	of the Incident so that it do	es not appear in an Incident
Ordering	10			id in the NNMi database.	o the incident so that it do	es not appear in an incident
Enabled			Enabled			
			▼ Payload Filter			
					ts incoming Incidents base more information, click her Value	id on Custom Incident Attribute e.
			ciaValue	-	▼ 2	Append
						Insert
						Replace
						Append 🗸
			OR			AND
			- daValue =	1		OR
				.1.3.0.1.4.1.33333.1.1.1		NOT
			L AND	2		EXISTS
				.1.3.0.1.4.1.33333.1.1.1		NOT EXISTS
			Either Steine			Delete
			Filter String ((ciaValue = 1 AND ciaName = .1.3.0.1		3333.1.1.1) OR (ciaValue	= 2 AND

To determine whether an SNMP trap incident is being suppressed, examine one of the SNMP traps in the NNMi database that has already been sent and not suppressed:

- 1. From an incident view, select the incident of interest and then click the Open button.
- 2. Select Actions->Incident Configuration Reports->Suppression Results.

The Suppression Results report displays the results of processing the incident using the Suppression configuration specified for that incident as if the incident was generated.

Note

The Suppression Results report does not actually execute the rules, but instead reports on how the Suppression configuration would be executed. This report is useful to determine whether the Suppression configuration matches any incidents. You can use the same approach for Actions, Dampen, and Enrichment configurations as well.

Figure 30.											
Network No.	še Manoger			(ne ferre press) WHI Risk Altorodous							
for Yes Jam	Aplans (Hrs										
 Datificants Incident Managerea 	Table Adlants Interface Adlants IP Address Adlants	and Instant	ans (Holes) 3 See and Doe D. X. Does houses III.								
Coon Key Ind	Marca .	•		Beneral Completer Parente Completer Culture Attributes Degranite Registration							
ett Unsegned Op ett My Open Inse		ione Routens 2 CPU		Coloris Norma Sectors Colory Aspirater Statul +							
	Court: Lister: Polar Read gode Acces Traffic Maps Quality Accessors	Tarring + Tarring +		Family Rote Organ SIMP Two Consistion Native Root Cause							
	X Detete	· mainter	(a)(*)	RCA Addres							
	Openge Lifesysie Belgin Het NAM JOHN Partsmanne	-		Completion Netwo							
	Materi Configurator Ben Configurator Differencia Scaluetor Internetia Inte	n Demperi Resulta Report Envidmenta	- (# ¥)	Free Oppurence Time: August 5, 2014 11 12 82 AM IST Les Dopurence Time: August 5, 2014 11 13 82 AM IST Origin Oppurence: August 5, 2014 11 13 82 AM IST Time: August 5, 2014 11 13 82 AM IST							
	Analysis										
	Parto	t Summery Teaches () menas Data - Mard Aug DE 11 18 28 187 2014	Desers (3) Category Yamity	Contrart Altriantes (D) consequent(2) A MRI Variant (D) Parlamentos (D) Savara Naria consequent(2) A (D) Savara (12) (D) Applications Nation Nation							
J. Samar Mars	E MAA	ny Altanoing Constraints and an and a second an and a second an and a second and an and a second	Comulation 1 Origin Last Occurre Sources factor	SMMM* Tray man Time August 6, 2014 11 A3 03 AM 101							
Management Made	Bourse Orga	e Otject none (Configuration News)									

The following example verifies that a match is made and this trap would be suppressed if received.

Figure 31.

Report Suppression

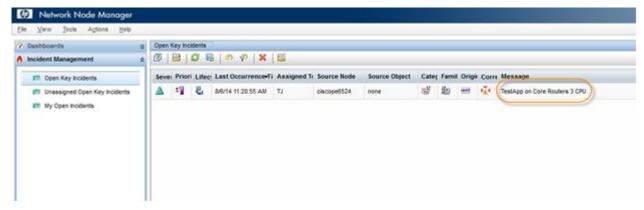
Node ciscope6524.ind.hp.com found match within nodeGroup Core Routers. Suppression performed for Core Routers for the incident TestApp. This incident will be suppressed / dropped.

To fully test the Suppression configuration, send the trap three times, each with a different Varbind value (1, 2, and 3):

```
# nnmsnmpnotify.ovpl -a 10.210.109.1 localhost .1.3.6.1.4.1.33333.0.1
.1.3.6.1.4.1.33333.1.1.1 integer 1 .1.3.6.1.4.1.33333.1.2.1 OCTETSTRING CPU
# nnmsnmpnotify.ovpl -a 10.210.109.1 localhost .1.3.6.1.4.1.33333.0.1
.1.3.6.1.4.1.33333.1.1.1 integer 2 .1.3.6.1.4.1.33333.1.2.1 OCTETSTRING CPU
# nnmsnmpnotify.ovpl -a 10.210.109.1 localhost .1.3.6.1.4.1.33333.0.1
.1.3.6.1.4.1.33333.1.1.1 integer 3 .1.3.6.1.4.1.33333.1.2.1 OCTETSTRING CPU
```

Notice that only the TestApp SNMP trap with Varind1=3 appears in the Open Key Incidents view. NNMi suppresses the other two TestApp SNMP trap incidents.

Figure 32.



More about Dampening

The Dampening feature is useful for incidents that NNMi closes automatically when the condition is cleared rather than the simple traps included in the previous examples. For example, NNMi closes the InterfaceDown incident when the status of the interface goes to Normal. If this were to occur during the Dampening period, NNMi does not display the incident in any Incident Management or Incident Browsing views.

By default, NNMi dampens the Management Events it provides for a period of 1 minute. Dampening can be configured to a maximum of one hour to allow two polling cycles to occur before NNMi sets the Lifecycle State to Registered.

To disable the Dampening for an incident configuration, click to clear Enabled on the incident configuration form.

You can also use the nnmsetdampenedinterval.ovpl command line tool to set the Dampening period and enable Dampening for all incidents.

To disable Dampening for all incident configurations use nnmsetdampenedinterval.ovpl as shown in the following example:

nnmsetdampenedinterval.ovpl -hours 0 -minutes 0 -seconds 0

An example of the dampening for the InterfaceDown incident is shown below:

Figure 33.

and the second se	gurations Management Event Configuration *		
- Basics		Interface Settings Node Settings Suppression Enrichment Desuplication Rate	Actions
Name	wbesheding incidents, click here InterfaceDown	Dampen configuration enables you to delay the following Decident actions.	
	E) altibute accepts one wildcard character (") that must appear at the end of i permits wildcards only in ODs beginning with: 1.3.6.1.4 (private MBs). Click an. 1.3.6.1.4.1.11.2.17.19.2.6.19	Appearance of Incidents within Incident views. Execution of Diagnostics (VIBI 2014 Network Engineering Toolest bely). Enabled Use a maximum of 60 minutes for the Campon Interval.	
Enabled	2	* Hours 0	
* Category	Faut - 🗊 💌	Elevies 1	
* Family	interface +	* Seconda 0	
* Severity	Critical +	✓ Payload Filter	
message use T/variable attributes. For more info * Nessage Format	It message appears is the incident vew. To include incident information in the energy_Select these variables from a ant of valid parameters or Custom incident metion, click here.	A Payted Filter enables you to turber define the filters to be used for selecting the incidents that should participate in suppressed, serviced, deepender, run actione, or participate in participate in participate in (calibration) and values (calibbar). For more actionmetric, cick here Filter Editor Attribute Operator Value	
Interface Down		cahane + h	
Description This incident indicates t	that the interface is not responding to polls.		
• Author	HP Network Node Manager		

Lifecycle State and Actions

NNMi has four common Lifecycle States: Registered, In Progress, Completed, and Closed. It is important to understand Lifecycle State changes because these state changes are the triggers for actions in NNMi.

It is also important to understand that NNMi changes the Lifecycle State to Closed based on the "Down" incident. For example, when an interface goes down, an Interface Down incident is generated and, if the incident is not Dampened, NNMi sets the Lifecycle State to Registered. When the interface comes back up again, NNMi changes the Lifecycle State to Closed, but does not generate an additional Interface Up incident.

This example uses two command line scripts that can be run as actions. One script (ServerScript.ksh) is to be run for TestApp traps that arrive from the Important Servers group. The other script (RouterScript.ksh) is to be run on traps that arrive from the Core Routers group. Each script is passed Source Node Name (\$snn) as well as the Varbind1 and Varbind2 values.

```
The two scripts are as follows:

ServerScript.ksh:

    #!/bin/ksh

    echo $1 $2 $3 >> /tmp/serverscript.txt

RouterScript.ksh:

    #!/bin/ksh

    echo $1 $2 $3 >> /tmp/routerscript.txt
```

1. Place the scripts into the following directory and make sure they are executable:

```
Windows:
%NnmDataDir%\shared\nnm\actions
```

```
UNIX: /var/opt/OV/shared/nnm/actions
```

- 2. Navigate to the **Configuration** Workspace
- 3. Open Incidents and select SNMP Trap Configurations.
- 4. Locate and select the TestApp trap, and then click the 📴 Open button.
- 5. Navigate to the Node Settings tab.
- 6. Select Core Routers and then click the 📑 Open button.
- 7. In the **Node Group** drop-down list, select the **Core Routers** Node Group.
- 8. In the **Ordering** attribute, enter **10**.
- 9. Click to check Enabled.
- 10. Navigate to the Actions tab.
- 11. Click to check Enabled.
- 12. Click the ⊁ New icon.

Figure 34.

File View Tools Actions Help	
Node Settings *	
😼 📋 🎦 Save and Close 😂 X Delete Node Settings 🗄	
(i) Changes are not committed until the top-level form is saved!	
▼ Basics	Suppression Enrichment Dampening Actions Diagnostic Selections
Node Group Core Routers	▼
* Ordering 10	You configure actions to automatically run at any point in the Incident lifecycle. For example, when an Incident is
Enabled	generated (Registered), you might want to automatically open a trouble ticket, send email, or page your network operator. NNMi supports running a Jython file, executable, or script as an action.
	Note: Your configured actions are disabled until you click Enabled and Save this form.
	✓ Lifecycle Transition Actions
	L New primand Type Command

Next, specify the action to be run and the arguments to pass it.

You can specify Varbinds, using the full OID (as shown below) or using a position number, such as \$1 and \$2. The advantage to using the full OID is that the action can be re-run on an "already received trap". NNMi does not store the Varbind position, but if you use the OID specification, it properly re-runs the action as demonstrated in this example.

To configure a Lifecycle Transition Action:

- 1. In the Lifecycle State drop-down list, select Registered.
- 2. In the **Command Type** drop-down list, select **ScriptOrExecutable**.
- 3. In the **Command** attribute, enter the following command:

/var/opt/OV/shared/nnm/actions/RouterScript.ksh \$snn \$.1.3.6.1.4.1.33333.1.1.1 \$.1.3.6.1.4.1.33333.1.2.1

Tip

Include the full path to the action script.

4. Click Save and Close to save your changes.

Figure 35.

-		
File View Tools Actions Help		
Lifecycle Transition Action *		
😼 📔 🎦 🎦 Save and Close) 😂 X Delete Lifecycle Transit	tion Action	
(i) Changes are not committed until the top-level form is saved!		
•	Payload Filter	
Enter the Java Jython file, executable, or script to run when an Incident	▼	
changes to the specified Lifecycle State. You can pass Incident attribute values as parameters into each. See Help → Using the Lifecycle	A Payload Filter enables you to further define the filters to be used for selecting the Inci	idents that should
Transition Action form.	participate in an operation; for example, be suppressed, enriched, dampened, run action	ns, or participate in
	pairwise. A Payload Filter selects incoming Incidents based on Custom Incident Attribute values (ciaValue). For more information, click here.	e names (ciaName) and
* Lifecycle State Registered -		
* Command Type ScriptOrExecutable 💌	Filter Editor	
Command	Attribute Operator Value	
/var/opt/OV/shared/nnm/actions/RouterScript.ksh \$snn	ciaName 💌 !=	Append
\$.1.3.6.1.4.1.33333.1.1.1 \$.1.3.6.1.4.1.33333.1.2.1		Insert
		Replace
		Append -
		AND
		OR
	There is currently no filter defined.	NOT
		EXISTS
		NOT EXISTS
		Delete
	Filter String	
	There is currently no filter defined.	
1		

Next configure the action for the Important Servers Node Group.

- 1. Navigate to the **Configuration** Workspace.
- 2. Open Incidents and select SNMP Trap Configurations.
- 3. Locate and select the TestApp trap, and then click the 📑 Open button.
- 4. Navigate to the **Node Settings** tab.
- 5. In the Node Group list, select the Important Servers Node Group and click the 📴 Open button.
- 6. In the **Ordering** attribute, enter **20**.
- 7. Click to check **Enabled**.
- 8. Navigate to the Actions tab.
- 9. Click the * New icon.
- 10. Click to check Enabled.
- 11. In the Lifecycle State drop-down list, select Registered.
- 12. In the **Command Type** drop-down list, select **ScriptOrExecutable**.
- 13. In the **Command** attribute, enter the following command: /var/opt/OV/shared/nnm/actions/ServerScript.ksh \$snn \$1 \$2
- 14. Click Save and Close.

Figure 36.

File View Tools Actions Help Node Settings * Image: Comparison of the settings and the settings of	N
	Suppression Enrichment Dampening Actions Diagnostic Selections
Node Group Important Servers * Ordering 20 Enabled Important	You configure actions to automatically run at any point in the Incident lifecycle. For example, when an Incident is generated (Registered), you might want to automatically open a trouble ticket, send email, or page your network operator. NNMi supports running a Jython file, executable, or script as an action. Note: Your configured actions are disabled until you click Enabled and Save this form. Enabled
	Lifecycle Transition Actions * E * * * * * * * * * * * * * * * * * * *

- 15. Click Save and Close to save your changes.
- 16. Click **Save and Close** again to save your changes.

To confirm that action is configured properly:

- 1. From an incident view, select an incident of interest and then click the 📴 Open button.
- 2. Select Actions->Incident Configuration Reports-> Action Results.

-	-			-	-	
ы	Π	ur	-ρ	-≺	1	
	ч	u	۰.	-		٠

Ø	Net	work N	ode	Ma	nage	er																				User Name:	system	NNMI	Role: Administrator
Eile	View	Tools	A	tions	He	lp																							
 Das Inci 		ds Managerr		Node Interfa	ce Ac				> 💻	idents	Incid		se 💋	🗙 Delete Incident 🔛															
		n Key Inc		Maps				ı	•								^	General	Co	orrelated	Parents	Correlated C	hildren Cus	om Attrib	outes	Diagnostics	Registrat	ion	
1	Una	ssigned O	E	Sourc	e Nod	e			je									- Details											
	🛲 My Open Incid 📑 Source Object					n	Core Ro	outers 2	2 CPU						Name			TestAr											
						Membe	ers																						
	Graph Custom Poller Results Node Access				sults	V Warning V								Category Family Origin		Application Status - Node													
													E				SNMP Trap												
				Traffi	Maps	5			۶.									Correla	ation Nat	iture	Root C	ause							
				Qualit	Ass	urance			•	State		Reg	istered	*				Duplice	ate Cour	at	0								
	Change Lifecycle		Ne	ode		cisco	pe6524			•		RCA A			Ē														
				۶.									Correla	ation Not	ites														
				Assig	n				• 01	bject		none																	
						Perform			•	_																			
						-	_	eports I	Action Results Dampen Results									First Occurrence Time August 6, 2014 11:13:02 AM IST				3:02 AM IST							
			2	Open	Incide	nt Confi	igura	tion				sults hments					-											_	
			S	Run D	iagnos	stics (E)	valua	tion)				nments aer Forw	ardina																
								ncident	s			n Results	aroing			Details	8	Custom Attri	ibutes 🕻	Cise	cope6524	MIB Values 🕻	Performa	nce 😂	Source	ce Node cisco	pe6524 🗭	Simila	r (13) 😂
								Perforr Messa Severit	ge ty			Wed Au TestApp	p on Core Warning			Category Family Correlation		ire				Application Node Root Cause SNMP Trap	Status						
и, Тор	ology	Maps				×		Priority		toto		com.hp Registe		ident.priority.Top		Last Occ		e Time					014 11:13:02	AM IST					
🕎 Mo	nitorir	ng				×		RCA A				false	ieu			Source N	lode					ciscope6524							
🐴 Tro	ubles	hooting				×		Assign				TJ																	
👔 Inv	entory	,				×		Source						ition Item)															
🔅 Ma	nagen	nent Mod	le			×		Create	a/Up	ened		8/6/14 11	1:13 AM (Open for 1.2 hours)															
🏡 Inci	ident l	Browsing	1			*																							

The Action Results report displays whether a Node Group match occurred for that particular trap and if the action would have been run.

Note

Run the Action Results report for a node in the Core Routers group and for a node in the Important Servers group.

Figure 38.

Report Actions

Node ciscope6524.ind.hp.com found match within nodeGroup Core Routers.

Action will be performed for Core Routers for the incident TestApp for the lifecycle state com.hp.nms.incident.lifecycle.Registered. Action: /var/opt/OV/shared/nnm/actions/RouterScript.ksh \$snn \$.1.3.6.1.4.1.33333.1.1.1 \$.1.3.6.1.4.1.33333.1.2.1

Action(s) do not exist for the incident TestApp for the lifecycle state com.hp.nms.incident.lifecycle.lnProgress.

Action(s) do not exist for the incident TestApp for the lifecycle state com.hp.nms.incident.lifecycle.Completed.

Action(s) do not exist for the incident TestApp for the lifecycle state com.hp.nms.incident.lifecycle.Closed.

Figure 39.

Report Actions

Node iptcm10.ind.hp.com found match within nodeGroup Important Servers. Action will be performed for Important Servers for the incident TestApp for the lifecycle state com.hp.nms.incident.lifecycle.Registered. Action: /var/opt/OV/shared/nnm/actions/ServerScript.ksh \$snn \$1 \$2.

Action(s) do not exist for the incident TestApp for the lifecycle state com.hp.nms.incident.lifecycle.lnProgress.

Action(s) do not exist for the incident TestApp for the lifecycle state com.hp.nms.incident.lifecycle.Completed.

Action(s) do not exist for the incident TestApp for the lifecycle state com.hp.nms.incident.lifecycle.Closed.

Next, send one of the traps.

After the trap is sent, check the Incident Actions log for a message indicating the action was run.

Figure 40.

	Cools Actions Help	_												
shboar	Find Node	Open	Key Inc	idents	3									
cident N 🔍	Find Attached Switch Port	2	2	0	e 🔊 🖗 🗙	E							Last 8 Hours 👻 <empty group<="" th=""><th>filter> -</th></empty>	filter> -
m Oper	MIB Browser	Seve	Prior	Lifeo	Last Occurrence-Ti	Assigned 1	Source Node	Source Object	Cate	Famil	Origi	Corn	Message	Notes
🕅 Unas	NNMi Status Status Distribution Graphs		1	3	8/6/14 12:29:10 PM	тл	ciscope6524	none		Ŀ	5009	₽ <u>₩</u> 4	TestApp on Core Routers 1 CPU	
🕅 My C	NNMi Self-Monitoring Graphs	0	5	5	8/6/14 12:27:58 PM		cisco6506pe1	BLRFTCTCPTest	*	Qualit	1	₽ <u>¥</u> 4	Service type TCP Connect is down on target address 15.218.54.252	
	Trap Analytics	0	5	5	8/6/14 12:07:44 PM		memphis-p1	removed		1	۰	14	Power supply on memphis-p1 is malfunctioning	
5	Visio Export		1	5	8/6/14 11:20:55 AM	тJ	ciscope6524	none			18040	P <u>1</u> 4	TestApp on Core Routers 3 CPU	
47	Incident Actions Log		2/	5	8/6/14 11:13:30 AM		iptcm10	none			18940	P <u>1</u> 4	TestApp on Important Servers 2 CPU	
	Security Reports		1	5	8/6/14 11:13:02 AM	тJ	ciscope6524	none			999	₽ <u>∓</u> 4	TestApp on Core Routers 2 CPU	
	NNMi Audit Log	\wedge	5.	5	8/6/14 10:53:49 AM		ciscope6524	none			9999	P <u>1</u> 4	TestApp 2 CPU	
			5	5	8/6/14 10:52:26 AM		ciscope6524	none		î٦	2	<u>14</u> 4	Rate Correlation for TestApp: TestApp 2 CPU	

Figure 41.

6, 2014 12:29:50.628 FM [ThreadID:1] FINE: com.hp.ov.nms.events.action.log.ActionLogger addActionResponseToCompletedList: Command) */var/opt/OF/shared/nms/actions/Bout
Recotion Status: Finished execution; Kan for 27836 milliseconds
Aug 4, 2014 12:29:50.429 PM [ThreadID:1] FINE: com.hp.ov.nms.events.sction.log.ActionEcogper addActionResponseToCompletedList:
Command: "/var/opt/DV/shared/nom/actions/BouterScript.Xsh" "classpe4524" "1" "CPU"
Started at 0/4/16 12:29 FM
Incident Name: TestApp
Incident UUID: d5%cfbbl=Tass=feac-bdl5=fbs5bl%b8bca
Command Type: ScriptOrfxecutable
lifecycle state: com.hp.nms.iscident.lifecycle.Registered
Exit Code: 126
Standard Output:
Standard Error: /bin/sh: /vaz/opt/09/shared/nnm/actions/RouterScript.ksh: Permission denied
Execution Status: Finished execution
Ran for 27,634 milliseconds

You can also check the results of the action as shown in the following example:

cat /tmp/serverscript.txt
cheese 2 CPU

To practice running the action from an already received incident:

- 1. From an incident view, select an incident of interest and then click the Open button.
- 2. Change the Lifecycle State attribute to a different state.
- 3. Click Save and Close.
- 4. Change the Lifecycle State attribute value back to the Registered State.
- 5. Click Save and Close.

Note

NNMi processes the varbinds values in the proper order when the trap first arrives, but it does not do so in subsequent runs when the Lifecycle State is changed and the varbinds are identified using position number. Therefore, use the full OIDs for the varbinds when forcing a Lifecycle State change.

File View Tools Actions Help	Inciden
Basics	General Correlated Parents Correlated Children Custom Attributes Diagnostics
Message TestApp on Core Router 3 CPU	Registration Details
Severity Warning Priority Top Ulfecycle State Registered Source Node In Progress Completed Closed Notes Notes Notes	Name TestApp Category Application Status Family Node Origin SNMP Trap Correlation Nature Root Cause Duplicate Count 0 RCA Active
	First Occurrence Time May 10, 2010 10:03:33 PM MDT Last Occurrence Time May 10, 2010 10:03:33 PM MDT Origin Occurrence May 10, 2010 10:03:33 PM MDT Time

Figure 42.

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

© Copyright 2009–2014 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft[®] and Windows[®] are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX[®] is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

For the full Oracle license text, see the license-agreements directory on the NNMi product DVD.

Acknowledgements

This product includes software developed by the Apache Software Foundation.

(http://www.apache.org)

This product includes software developed by the Indiana University Extreme! Lab.

(http://www.extreme.indiana.edu)

Support

Visit the HP Software Support web site at:

www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches and associated patch documentation
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Sign up for updates hp.com/go/getupdated

© Copyright 2009-2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.



We appreciate your feedback!

If you have comments about this document, you can <u>contact the documentation team by email</u>. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line: Feedback on White Paper (Network Node Manager i Software 10.00)

Just add your feedback to the email and click send. If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to docfeedback@hp.com.