

HP Network Node Manager i Software Step- by-Step Guide to Incident Management

Release 9.23

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

CONTENTS

Setting Up Your SNMP Trap	3
Dampening and the Incident Pipeline	
Customizing Incident Configurations Using Interface or Node Groups	7
Deduplication	8
Rate	11
Enrichment	14
Suppression	19
More about Dampening	23
Lifecycle State and Actions	24

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. This is a common practice for some devices and applications.

Note: The examples presented are based on traps, but the same principles apply to management events such as Node Down.

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)

The following table describes the Varbind 1 and Varbind 2 values:

Varbind1 Type: Integer	Varbind1 Type Description: Status
Varbind1 Value	Description
1	Normal Status
2	Warning Status
3	Critical Status
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:

nnmincidentcfg.ovpl -loadTraps <mib file>

To create the trap definition:

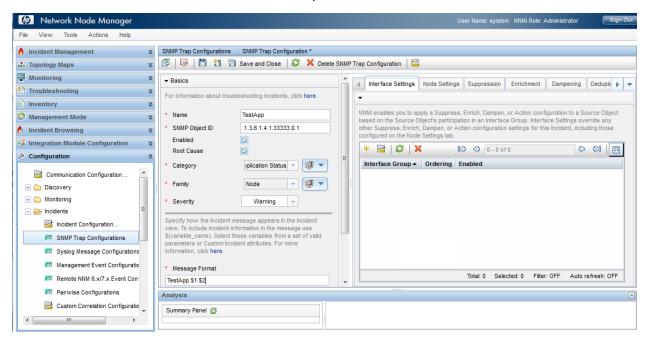
1. Navigate to the Configuration workspace, expand Incidents, and click SNMP Trap Configurations.

Metwork Node Manager			User Name: system NNMi Role: Administrator Sign O	ut
File View Tools Actions Help				
 ♦ Incident Management ※ Topology Maps ※ Monitoring ※ Proubleshooting ※ Inventory ※ Management Mode ※ Incident Browsing ※ 			Q	
Integration Module Configuration Configuration Communication Configuration Discovery	Updated: 3/18/13 03:07:58 PM	146 Nodes	Auto full refresh: 300 se	•
Monitoring	Analysis			*
🖃 🗁 Incidents	Summary 😳			٦
incident Configuration SNMP Trap Configurations Systog Message Configuration Management Event Configuratio Remote NNM 6.x/7 x Event Con Pairwise Configurations	No Objects Selected			
Cuetom Correlation Confinuentia				

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

Metwork Node Manager					
File View Tools Actions Help					
👌 Incident Management 🛛 🕹 🌾	SNMP Trap Configurations				
🛧 Topology Maps 🛛 🕹		💎 🗙 🔛			
Monitoring ×	Name New	SNMP Object ID	Enabled	Root Cause	Deduplication Enabled
Troubleshooting Inventory	ArcSightEvent	.1.3.6.1.4.1.11937.0.1	-	-	-
🕙 Management Mode 🛛 🕹 🍣	BGPBackwardTransition	.1.3.6.1.2.1.15.0.2	-	-	-
Incident Browsing	BGPEstablished	.1.3.6.1.2.1.15.0.1	-	-	-
Integration Module Configuration 🛛 🕹	CempMemBufferNotify	.1.3.6.1.4.1.9.9.221.0.1	~	-	-
	CiscoChassisAlarmOff	.1.3.6.1.4.1.9.5.0.6	-	-	~
📑 Communication Configuration 🔺					
+ 🗀 Discovery	Updated: 3/18/13 03:13:02 PM		Total: 1	25	Selected: 0
+ 🧀 Monitoring	Analysis				
- 🧁 Incidents	Summary 🙄				
lncident Configuration	No Objects	Selected			
SNMP Trap Configurations					
📖 Syslog Message Configurations					

- 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.



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

```
# nnmsnmpnotify.ovpl -a 15.2.127.135 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 15.2.121.254 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 the following:

- This command must be run from the NNMi server.
- Each nnmsnmpnotify.ovpl command 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.

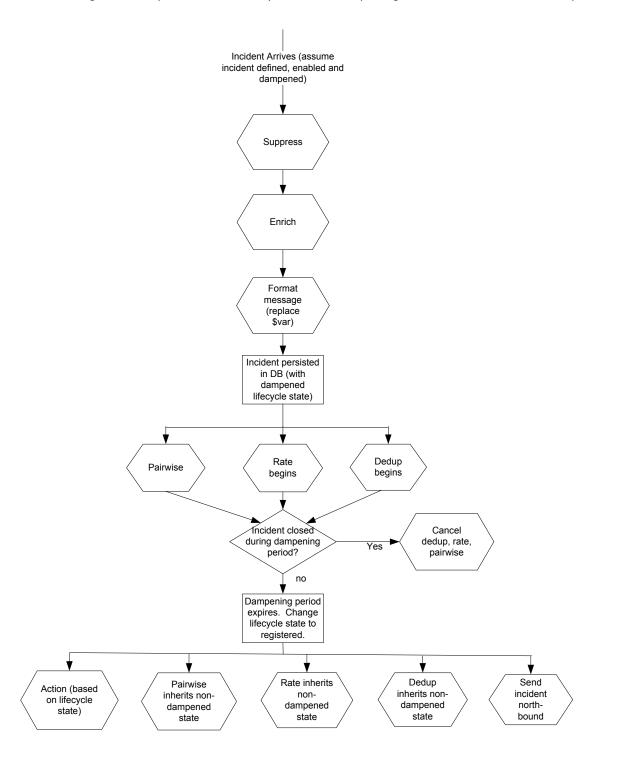
Workspaces	Incident - Open Key Incide	nts								
Incident Management	×80 (*	🗣 🖻					Last	: Week		 <set filter="" group="" node=""></set>
Open Key Incidents		Prior VLS	-Last Occurrence AT	Source Node	Source Objec	Cate	Fam	Origi	VCN	Message
My Open Incidents		5. 2.	4/9/10 11:58:07 AM	cheese	none	12	1	SNHP	PT4	TestApp 2 CPU
		5 🗸 🍓	4/9/10 11:57:14 AM	cisco6509	none	Tel:	1	SHHP	PA4	TestApp 1 Temperature

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.



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.

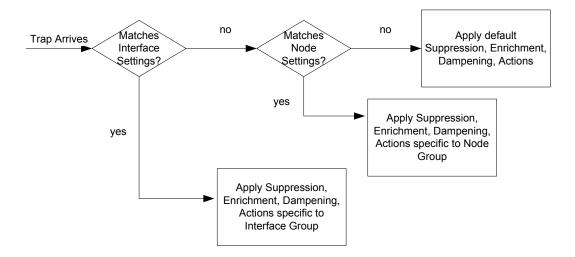
Customizing Incident Configurations Using Interface or Node Groups

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.



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 Open 📑 button.

🕼 Network Node Manager						User N	lame: sys	stem 1	NNMi F	Role: Administrator	Sign C		
File View Tools Actions Help													
👌 Incident Management 🛛 💝	SNMP Trap Configurations												
🗛 Topology Maps 🛛 🕹 😵									124 of	126	00		
Monitoring ×	Name Open •	SNMP Object ID	Enabled	Root Cause	Deduplicatio Enabled	Rate Enabled	Seve	Cate	Fam	i Author	Message Format		
Inventory ¥	SyslogMessage	.1.3.6.1.4.1.9.9.41.2.0.1	-	-	-	-	۷	🙁 F	÷ 1	HP Network Nod	\$1:\$3 \$4 (syslog		
Management Mode ¥	TestApp	.1.3.6.1.4.1.33333.0.1	~	~	-	-	Δv	₿ ⊿	ile n	Customer	TestApp \$1 \$2		
Incident Browsing ¥	TrafficEntryExitMismatched	.1.3.6.1.4.1.8083.1.1.12.3.46	-	-	-	-	Δv	🗱 F		HP Route Analyti	Entry exit misma		
🗘 Integration Module Configuration 🛛 🗧 🛠	TrafficHighLinkUtilization	.1.3.6.1.4.1.8083.1.1.12.3.36	-	-	-	-	Δv	🙁 F		HP Route Analyti	Traffic high linkU		
➢ Configuration	TrafficLinkCoSUtilization	.1.3.6.1.4.1.8083.1.1.12.3.38	-	-	-	-	Δv	🗱 F		HP Route Analyti	Traffic high CoS		
Communication Configuration							A	25	-				
The Discovery	Updated: 3/19/13 03:21:46 PM	Jpdated: 3/19/13 03:21:46 PM Total: 126 Selecte							elected: 1 Filter: OFF Auto refr				
🗄 🧰 Monitoring 🔤	Analysis												
Incidents	SNMP Trap Configuration Summ	nary : TestApp 🙄	Details 🙄										
📑 Incident Configuration	SNMP Object ID .1.3.6.1.4.1.3	3333.0.1	Enabled		true								
SNMP Trap Configurations	Message Format TestApp \$1	\$2	Severity		🛆 🗆 V	/arning							
Syslog Message Configurati			Category			on Status							
			Family		Node								
Management Event Configur			Root Cause		true								
Remote NNM 6.x/7.x Event C			Author		Customer								
m Pairwise Configurations													
· · · · · · · · · · · · · · · · · · ·													

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

SNMP Trap Configurations	SNMP Trap Configuration	
🖉 🐺 🗎 🎽 🦉	Save and Close 🛛 😂 🗙 Delete SNMP Trap Configuration	
		Interface Settings Node Settings Suppression Enrichment Dampening Deduplication Rate Actions
For information about troul	bleshooting Incidents, click here.	
Name	TestApp	Narrows context to interface Settings override any other Suppress. Otherwise, apply ings for
SNMP Object ID	.1.3.6.1.4.1.33333.0.1	specific Interfaces gured on the Node Settings tab. these settings if no
Enabled		and Nodes 🛛 🔊 💀 match is made for 👔 🖃
Root Cause		Interfaces or Nodes
* Category	Application Status	Interface Group A Ordering Enabled
* Family	Node 👻	
* Severity	Warning 💌	
	message appears in the Incident view. To include Incident e use S(variable_name). Select these variables from a set of	*

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).

🕼 Network Node Manager					User Name: system NNMi	Role: Administrator	Sign Ou	ut
File View Tools Actions Help								
👌 Incident Management 🛛 😵	SNMP Trap Configurations SNMP Trap Con	nfiguration *						
🛧 Topology Maps 🛛 🕹	🗵 📴 🛅 🎽 🕙 Save and Close	🛛 😂 🗙 Delete SNMP Trap Confi	guration					
🕎 Monitoring 🛛 🗧 🕹	▼ Basics	^	Suppression Enrichr	ment Dampening	Deduplication Rate	Actions F	orward to G 🕨 🦷	
Troubleshooting ¥	For information about troubleshooting Inciden	nts. click here.	- Suppression Ennom	Dampening	Dedupiication	Actions	Ji wald to G	
linventory ¥								П
S Management Mode 🛛 🕹	Name TestApp				uld match to detect when an Incident. NNMi tracks the nur			
🇞 Incident Browsing 🛛 🕹	SNMP Object ID .1.3.6.1.4.1.333	333.0.1		uplicate Count attribut	e. It is incremented on the Du	plicate Correlation Inci	dent.	
integration Module Configuration $~~$ st	Enabled 🔽 Root Cause 🔽		Enabled Count	2				
≁ Configuration \$	* Category Application St	tatus 🔻 🗃 🔻	Hours	2				
Communication Configuration	- category Application St		Minutes	3			;	Ε
Discovery	* Family Node	- 🗊 -	Seconds	0				
	* Severity Warning	-		-				
E 🗁 Incidents			Parent Incident	DuplicateCorrelat	ion		· 🗊 🔻	
📑 Incident Configuration	Specify how the Incident message appears i include Incident information in the message u		Comparison Criteria	Name SourceNode	-			
III SNMP Trap Configurations	Select these variables from a set of valid par attributes. For more information, click here.	rameters or Custom Incident	Deduplication Compariso	n Parameters				
🛅 Syslog Message Configurati				and an				
🗰 Management Event Configur	* Message Format		* 🖻 😂 🗙		😂 🔇 - 0 of 0	\diamond		
Remote NNM 6.x/7.x Event C	TestApp \$1 \$2		Parameter Value				•	
m Pairwise Configurations	Description							
📑 Custom Correlation Configur								Ŧ

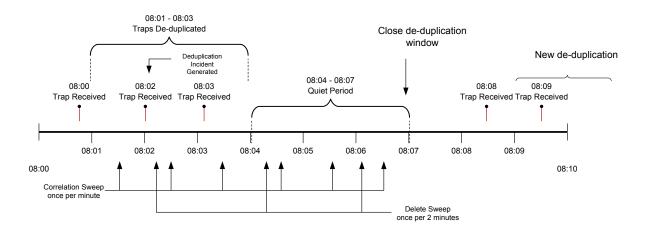
The following diagram depicts the following scenario:

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.

May 2013



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.

File Tools Actions Help														
Workspaces	Incide	ent - Op	en Key	Incider	nts									
Incident Management Topology Maps	X		0	~	P	-					Las	t Week		<set filter="" group="" node=""></set>
Monitoring				∕∕S€	Prior	γĽ	5 - Last Occurrence AT	Source Node	Source Objec	Cate	Fam	Orig		Message
Troubleshooting				Δ	5 🔒	۳,	4/9/10 12:39:06 PM	cheese	none			SHMP	₽ <u>¥</u> 4	TestApp 2 CPU
Inventory				Δ	5	2	4/9/10 12:39:03 PM	cheese	none			SHMP	Þ <u>⊼</u> ∢_	TestApp 2 CPU
Management Mode				Δ	5 🔒	е,	4/9/10 12:39:03 PM	cheese	none		17	۳	₽ <u>¥</u> 4	Duplicate Correlation for TestApp
Incident Browsing					5	۵.	4/9/10 12:39:00 PM	cheese	none	12		SNMP	₽ <u>⊼</u> 4	TestApp 2 CPU
Integration Module Configuration														
Configuration														
A														

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:

File View Tools Actions Help Image: Save and Close Image: Save and Close Image: Save and Close Image: Save and Close		Incident
Basics	General Correlated Parents Correlated Children Custom Attributes Diagnostics Registration	
Message Duplicate Correlation for TestApp		
Severity Warning 🗸	Seve - Last Occurrence Type Message Source Node Source Object	
Priority None -	📺 🚵 🔺 4/9/10 12:39:06 PM De-Dup Correlation 🛛 TestApp 2 CPU cheese none	~
Lifecyde State Registered -	📺 🖾 4/9/10 12:39:03 PM De-Dup Correlation TestApp 2 CPU cheese none	
Registered V	📺 🔼 4/9/10 12:39:00 PM De-Dup Correlation TestApp 2 CPU cheese none	
Source Node cheese		
Source Object none	6	
Assigned To		
Notes		
Notes		

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.

File View Tools Ad	ctions Help									Incident
Basics		General	Correlated	Parents	Correlated C	hildren Custom Attri	outes Diagnostics	Registration		
Message Duplicate Correlation for	Testine		-				N	1 - 2 of 2		
· · · · · · · · · · · · · · · · · · ·				ë , Last	Occurrence	Туре	Message		Source Object	
Severity	Warning 👻					De-Dup Correlation	TestApp 2 CPU	cheese	none	
Priority	None 👻			4/9/10	12:39:03 PM	De-Dup Correlation	TestApp 2 CPU	cheese	none	
Lifecycle State	Registered 👻									
Source Node	cheese 🐨 🗸									
Source Object	none 🐨 🗸									
	Hone (tight)									
Assigned To	a -									
Notes										
Notes										
										-
		•								4
		Upda	ted: 4/9/10 :	12:42:37 P	M	Total: 2	Selected: 0	Filter: OFF	Auto refres	n: OFF
Done										

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.

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.

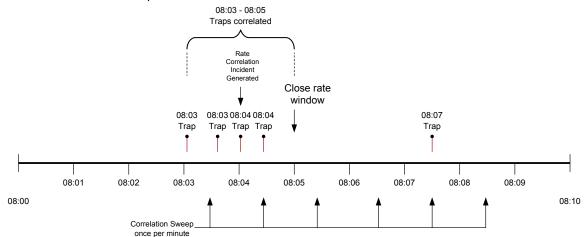
- 1. Navigate to the **Rate** tab.
- 2. Click to check **Enabled**.

- 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.

SNMP Trap Configurations SNMP Trap Configuration *											
🗵 📴 🛅 🎦 🔛 Save and Close 🞜 🗙 Delete SNMP T	rap Co	onfi	guration 🛛 🔛								
▼ Basics	^		Enrichment Da	ampening	Deduplication	Rate	Actions	Forward to Global Managers			
For information about troubleshooting Incidents, click here.			•			~					
Name TestApp SNMP Object ID .1.3.6.1.4.1.33333.0.1			specified time period	e Rate Configuration to track Incident patterns based on the number of Incident reoccurrences within a scified time period. After the count within the specified time period is reached, NNMi emits a Rate Correlation Ident and continues to undate the Correlation Notes with the number of occurrences within that rate							
Enabled 🔽 Root Cause 🔽			Enabled Count		2						
Category Application Status			Hours)						
* Family			Minutes Seconds		2						
* Severity Warning v			Parent Incident		RateCorrelation						
Specify how the Incident message appears in the Incident view. To include Incident information in the message use S(variable_name). Select these variables from a set of valid parameters or Custom			* Comparison Criter	ria	Name SourceNode	•					
Incident attributes. For more information, click here.			 Rate Comparison F 	Parameter	s						
* Message Format			* 🖻 🞜	×	K) 🔷 0-0	of O				
TestApp \$1 \$2			Parameter Value	•				•			
Description	+										

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.



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.

Workspaces	Incider	nt - All	Inciden	ts												
Incident Management			(~									All			Cot and a server filters	- [
Topology Maps		2													 <set filter="" group="" node=""></set> 	- 1
Monitoring				Seve	Prior	LS	- Last Occurrence	AT .	Source Node	Source Objec	Cate	Fam	Orig	CN	Message	
Troubleshooting				Δ	5 📮	<mark>ال</mark> ال	4/15/10 2:25:38 PM		cheese	none			SNMP	E	TestApp 2 CPU	
Inventory				Δ	5	۵.	4/15/10 2:22:48 PM		cheese	none		17	۲	₽₩₫	Rate Correlation for TestApp	
Management Mode				Δ	5	۵.	9/15/10 2:22:48 PM		cheese	none			SHIP	\$	TestApp 2 CPU	
Incident Browsing				Δ	5	5	4/15/10 2:22:15 PM		cheese	none			SHIP	€~	TestApp 2 CPU	
🕮 Open Key Incidents					5	5	4/15/10 2:21:55 PM		cheese	none			SHMP	2	TestApp 2 CPU	
🕮 Closed Key Incidents				$\overline{\Delta}$	5	5	4/15/10 2:21:33 PM		cheese	none			SHMP	€~	TestApp 2 CPU	
Open Root Cause Incidents				_	-								,	U		
Service Impact Incidents																
All Incidents																
Custom Open Incidents																
Custom Incidents																
 NNM 6.x/7.x Events SNMP Traps 																
- Sime traps																

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.

File Tools Actions Help	
Workspaces	Incident - Open Key Incidents
Incident Management	X 2 O C P T Last Week V <set filter="" group="" node=""></set>
Unassigned Open Key Incidents	Source Nobel Source Objec Cate Fam Orig VC Message
I My Open Incidents	📄 📷 🖾 🛓 5 🛛 🖏 4/15/10 2:25:38 PM cheese none 🔡 🌆 🚥 🔀 TestApp 2 CPU
	📄 📠 🖾 🛆 5 🗸 🖏 4/15/10 2:22:48 PM cheese none 🕋 🎁 💑 Rate Correlation for TestApp
a 1	1

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

	Actions Help and Close									Incider
Basics		G	General	Correlated P	Parents Correlated	Children Custom Attribu	utes Diagnostics Reg	istration		
Message Rate Correlation for Tes	stApp		8					▲ 1 - 4 of 4		
Severity	Warning 👻			Seve	- Last Occurrenc	Туре	Message	Source Node	Source Object	
Priority	None 👻			🔼 🛆	4/15/10 2:22:48 PM	Rate Correlation	TestApp 2 CPU	cheese	none	
Lifecycle State	Registered -			I 🔼 🛆	4/15/10 2:22:15 PM	Rate Correlation	TestApp 2 CPU	cheese	none	
enceyde blate	Registered V			🔼 🛆	4/15/10 2:21:55 PM	Rate Correlation	TestApp 2 CPU	cheese	none	
Source Node	cheese 🗃 🗸			🔼 🛆	4/15/10 2:21:33 PM	Rate Correlation	TestApp 2 CPU	cheese	none	
Source Object	none 🗊 🗸									
Assigned To										
Notes										

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.

File View Tools Action Image: Construction of the second sec			
Basics		General Correlate	ed Parents Correlated Children Custom Attributes Diagnostics Registration
Message Rate Correlation for TestAp Severity Priority Lifecycle State Source Node	Warning None Registered Cheese	Details Name Category Family Origin Correlation Nature Duplicate Count	RateCorrelation Performance Correlation NNMi re Root Cause 0
Source Object Assigned To	none @ ·	RCA Active Correlation Notes	s count: 3 incidents
Notes		-	interval: 0 hours, 2 minutes, 0 seconds
Notes		to Thursday, Apr	kd 4 times from Thursday, April 15, 2010 2:21:33 PM MDT ril 15, 2010 2:22:48 PM MDT.
		First Occurrence 1 Last Occurrence T Origin Occurrence Time	Time April 15, 2010 2:22:48 PM MDT

Enrichment

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

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 enriched so that the Priority is High. The Message Format of the incident for this Node Group is also customized.

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.

SNMP Trap Configurations SNMP Trap Configuration												
💯 📴 🛅 🎒 Save and Close 🧭 🗙 Delete SNMP Trap Configuration 🖺												
▼ Basics	Â	4	Interface Settings	Node Settings	Suppression	Enrichment	Dampening	Deduplication	Rate	Actions	Forward to	• G 🕨 🔫
For information about troubleshooting Incidents, click here.		•										
Name TestApp SNMP Object ID .1.3.6.1.4.1.3333.0.1		p	INMi enables you to ap articipation in a Node C acident, except those c	Group. Node Sett	ings override an	y other Suppre						
Enabled 🔽 Root Cause 🔽			* 🖉 🗱					Ø ♦ 0.	- 0 of 0		0 0	-
* Category Application Status 👻			New New	Ordering E	nabled							
* Family Node 👻	E											
* Severity Warning -												
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						Total: 0	Selecte	d:0 Fi	iter: OFF		Auto refresh	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.

File View Tools Actions Help									
Node Settings *									
😼 📔 🎦 🖾 Save and Close 🛛 🞜 🗙 Delete Node Settings 🛛 🔛									
$({f i})$ Changes are not committed until the top-level form is saved!									
	Suppression Enrichment Dampening Actions Diagnostic Selections								
Node Group Core Routers Ordering 10 Enabled	Suppression Einforment Dampening Actions Diagnostic Selections 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 enrichments. Enabled Enrichments Enrichments Seve Prior Corr Assigned Tr Message Format Description								

11. In the **Priority** drop-down list, select **Top**.

- 12. In the Message Format attribute, enter TestApp on Core Routers \$1 \$2.
- 13. 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.

File View Tools Actions Help								
Enrichment Configuration *								
📴 🛅 🎦 🔄 Save and Close 🞜 🗙 Delete Enrichment Config	juration	n 🖴						
$(\mathbf{\hat{i}})$ Changes are not committed until the top-level form is saved!								
	Cu	stom Attri	outes	Payload	d Filter			
Category	-							
Family 💌 🐨		* 🖻	8	×	K	🗘 🔷 0 - 0 of	0	
SeverityChoose One 🔻		Туре		Cu:	stom Attribute Name		Custom Incider	nt Attribute Name
Priority Top								
Correlation NatureChoose One V								
Message Format								
TestApp on Core Routers \$1 \$2								
Assigned To TJ 💌 🖼 🔻								
•								
Description								
					Total	0 Selected:	0 Filter: OFF	Auto refresh: OFF

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.

SNMP Trap Configurations	SNMP Trap Configuration *								
2 😼 🗎 🎽 🖄	Save and Close 🛛 🖉 💢 Delete SNMP T	rap Configuration 🛛 🔛							
			^		Node Setting	Suppression	Enrichment	Dampening	Deduplication
For information about troubl	eshooting Incidents, click here.			•		U	1		
Name	TestApp			NNMi enables you to					
SNMP Object ID	.1.3.6.1.4.1.33333.0.1			participation in a Nod Incident, except thos				ss, Enrich, Dan	ipen, Action, or Dia
Enabled Root Cause				🍾 🖬 🖉	×				1-
	Application Status	- 🗊 -			Ordering	Enabled			
* Category	Application Status			Core Routers	10	~			
* Family	Node	-	=						
* Severity	Warning -								
the message use \$(variable	essage appears in the Incident view. To includ _name). Select these variables from a set of For more information, click here .								
TestApp \$1 \$2									
Description									
* Author	Customer		-				Total: 1	Selecte	d: 0 Filt

- 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 粩 icon.

File View Tools Actions Help	
Node Settings *	
🕼 📋 🎦 Save and Close 🛛 🧭 🗶 Delete Node Settings 🗎	<u>کا</u>
(i) Changes are not committed until the top-level form is saved!	
▼ Basics	Suppression Enrichment Dampening Actions Diagnostic Selections
* Node Group Important Servers 💌 🕅 🔻	▼
Ordering 20 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 New mil Seve Prior Corr Assigned To 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.

File View Tools Actions Help		
Enrichment Configuration *		
🞼 💾 🎦 🔄 Save and Close 🧭 X Delete Enrichment Configu	ation 🛛 🖾	
$(\hat{\mathbf{j}})$ Changes are not committed until the top-level form is saved!		
▼ Basics	Custom Attributes Payload Filter	
Category	•	
Family	* 😫 🞜 🗙 🔯 🖓 0-0 of 0	
SeverityChoose One	Type Custom Attribute Name Custo	m Incident Attribute Name
Priority High Correlation NatureChoose One		
Message Format TestApp on Important Server \$1 \$2		
Assigned To		
Description		
	Total: 0 Selected: 0 Fil	Iter: OFF Auto refresh: OFF

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.

File View Tools Node Settings * Image: Setting the setting setting the setting setting setting the setting set	Actions Help Save and Close 🥔 🗙 Delete Node Setti	ngs E
(i) Changes are no	ot committed until the top-level form is saved!	
		Suppression Enrichment Dampening Actions Diagnostic Selections
Node Group * Ordering Enabled	Important Servers 20	 Suppress Configuration enables you to discard the Incident so that it does not appear in an Incident view and is not stored in the NNMi database. Enabled Payload Filter A Payload Filter enables you to further define the filters to be used for selecting the Incidents that should participate in an operation, for example, be suppressed, enriched, dampened, run actions, or participate in pairwise. A Payload Filter selects incoming Incidents based on Custom Incident Attribute names (ciaName) and values (ciaValue). For more information, click here. Filter Editor Attribute Operator Value CiaName I = Append Insert Replace
		Append AND OR 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.

🕼 Network Node Manag	ger User Name: system User Role: Administrator	Sign out
File Tools Actions Help		
Workspaces	Incident - Open Key Incidents	
Incident Management	Last Week V Set node group filter V	
Topology Maps		
Monitoring	Source Nobel Source Objec Cate Fam Origi 🖓 Message	Notes
Troubleshooting	📄 📠 🖾 🛕 🛱 🧸 4/20/10 10:52:13 PM TJ 🛛 cisco6509 none 📓 🌆 뺆 🔀 TestApp onCore Router? 2 CPU	~
Inventory	📗 🔚 🚵 🛕 🖓 💐 4/20/10 10:52:10 PM 🖉 cheese none 📑 🏗 🚥 🔀 TestApp on (important Server)3 CPU	
Management Mode		
Incident Browsing	N	
Integration Module Configuration		
Configuration	II	

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.

SNMP Trap Configurations	SNMP Trap Configuration	
🗵 😼 💾 🎦 🖄	Save and Close 🥔 🗙 Delete SNMP Trap (Configuration 🛛 🖾
Basics For information about trouble	eshooting Incidents, click here .	Interface Settings Node Settings Suppression Enrichment Dampening Deduplication Rate
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 Source Node based on the Source Node's participation in a Node Group. Node Settings override any other Suppress, Enrich, Dampen, Action, or Diagnostics Selection configuration settings for this Incident, except those configured on the Interface Settings tab.
Root Cause Category	Application Status	
* Family * Severity	Node v Warning v	E Important Servers 20 V
Incident information in the m	essage appears in the Incident view. To include essage use \$(variable_name). Select these parameters or Custom Incident attributes. For	
* Message Format		
TestApp \$1 \$2		
Description		Total: 2 Selected: 1 Filter: OFF Auto refresh: OFF
		v

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.
- I. Click AND.
- m. In the Attribute drop-down list, select **ciaName**.
- n. In the Operator attribute, select =.
- o. 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.

File View Tools Actions Help Image: Comparison of the second sec	Node Settings
$({\bf j})$ Changes are not committed until the top-level form is saved!	
Basics Node Group Core Routers Ordering 10 Enabled	Suppression Enrichment Dampening Actions Diagnostic Selections Suppress Configuration enables you to discard the Incident so that it does not appear in an Incident view and is not stored in the NNMi database. Enabled Image: Configuration enables you to discard the Incident so that it does not appear in an Incident view
	Payload Filter A Payload Filter enables you to further define the filters to be used for selecting the Incidents that should be suppressed, enriched, or dampened. A Payload Filter selects incoming Incidents based on Custom Incident Attribute names (ciaName) and values (ciaValue). For more information, click here. Filter Editor Attribute Operator Value ciaName =
	OR Append - AND AND - ciaName = .1.3.6.1.4.1.33333.1.1.1 OR Delete Delete AND - ciaName = .1.3.6.1.4.1.33333.1.1.1 - ciaName = .1.3.6.1.4.1.33333.1.1.1 Delete Filter String Image: CiaName = .1.3.6.1.4.1.33333.1.1.1 ((ciaName = .1.3.6.1.4.1.33333.1.1.1 AND ciaName = .1.3.6.1.4.1.33333.1.1.1

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.

File View Tools Actions Help							
Node Actions							
Interface Actions							
Topology Maps IP Address Actions	, ave and Close 🛛 💋 💥 Delete Incident 🛛 🔛						
🕎 Monitoring 💦 Maps	General Correlated Parents Correlated Children Custom Attributes Diagnostics Registration						
Troubleshooting 🔤 Source Node							
Inventory Source Object	✓ Details						
Node Group Members	Vn Name NodeOrConnectionDown						
Management Mod Graph Custom Poller Results							
Node Access	Critical V Category Fault V						
Open Key Inci X Delete	None Family Node						
Change Lifecycle	Origin NNMi Penieterant Correlation Nature Root Cause						
Closed Key In Assign	Registered						
Incident Configuration Reports	Action Results Duplicate Count 0						
🕮 Service Impac 🜌 Open Incident Configuration	Dampen Results RCA Active						
All Incidents	ion) Report Enrichments Correlation Notes						
Source Object	Global Manager Forwarding Incident duration: 3 minutes, 33 seconds, 264 ms						
Custom Open Incidents	Suppression Results In Time incident detected: Friday, March 29, 2013 2:34:32 AM MDT.						
Custom Incidents Assigned To	I lime incident resolved: r haday, March 29, 2013 2:38:05 AM MDI. Incident cancelled by: NodeUp.						
MNM 6.x/7.x Events							
Votes Votes	First Occurrence Time March 29, 2013 2:34:32 AM MDT						
Notes	 Last Occurrence Time March 29, 2013 2:34:32 AM MDT 						
Analysis	SNMP Iraps						
Incident Summa	/: NodeOrConnectionDown 😨 📄 🔄 Detais 😳 Custom Attributes 😳 Children (1) 😳 atlanta-ce1 MIB Values 😳 Source Node atlanta-ce1 😳 🕨 💌						
Integration Module Configuration *	Node or Connection Down Incident duration: 3 minutes, 33 seconds, 264 ms Time incident detected:						
Severity	Severity 🔇 Critical Contention Notes Friday, waren 29, 2015 2:54:52 AM MDT. Time incident resolved: Friday, waren 29,						
Je Configuration 😵	T 2013 2:38:05 AM MDT. Incident cancelled by: NodeUp.						

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

Report Suppression

Node cisco6509.cnd.hp.com found match within nodeGroup Core Routers. Suppression performed for Core Routers for the incident TestApp. This incident will be suppressed / dropped.

2

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

nnmsnmpnotify.ovpl -a 15.6.96.97 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 15.6.96.97 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 15.6.96.97 localhost .1.3.6.1.4.1.33333.0.1 .1.3.6.1.4.1.33333.1.1.1

nnmsnmpnotify.ovpl -a 15.6.96.97 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.

🕼 Network Node Man	iger User Name: system User Role: Administrator Sign
File Tools Actions Help	
Workspaces	Incident - Open Key Incidents
Incident Management	X 3 0 C P
Topology Maps	
Monitoring	□ ∇sc Prio ∇LS → Last Occurrence AT Source Node Source Objec Cate Fam Orig ∇ch Message Notes
Troubleshooting	📗 📺 🖾 🛕 🖞 🛃 4/20/10 11:36:09 PM TJ disco6509 none 🙀 🌆 🔤 🔤 🥳 🔏 TestApp on Core Router 3 CPU
Inventory	
Management Mode	
Incident Browsing	
Integration Module Configuration	
Configuration	N N
Communication Configuration	6

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 6 minutes. 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:

Management Event Configurations Management Event Configuration *									
🗵 📴 🎽 🎦 Save and Close 🞜 🗙 Delete Management B	Event	t Configuration 🛛 🔛							
Basics For information about troubleshooting incidents, click here. Name InterfaceDown SNMP Object ID .1.3.6.1.4.1.11.2.17.19.2.0.19 Enabled		Interface Settings	t actions. lents within Incid	ent views.	g:	Dampening Dedupi	ication Rate	Þ	•
Category Faut Family Interface Critical Specify how the Incident message appears in the Incident view. To include	III	Enabled Use a maximum of 60 * Hours * Minutes * Seconds	minutes for the Da	ampen interval.					ш
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 Interface Down		an operation; for exan	ple, be suppress	ed, enriched, dar	mpened, run actio	electing the Incidents the ons, or participate in pa (ciaName) and value	irwise. A Payload		
Description This incident indicates that the interface is not responding to polls.		Filter Editor Attribute	Operat	tor	Value		Arrend	-	
* Author HP Network Node Manager 👻 🚳 🔻	-	ciaName	✓ !=		•		Append		Ŧ

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:
```

```
#!/usr/bin/ksh
echo $1 $2 $3 >> /tmp/serverscript.txt
```

RouterScript.ksh:

```
#!/usr/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

To configure these scripts as actions for the TestApp SNMP trap incident configuration:

- 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.

File View Tools Actions Help Node Settings *)						
 Image: Save and Close Ima						
▼ Basics	Suppression Enrichment Dampening Actions Diagnostic Selections					
Node Group Core Routers • Ordering 10 Enabled Image: Core Routers	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					

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.

File View Tools Actions Help						
Lifecycle Transition Action *						
💷 💾 🎦 🚰 Save and Close 🖉 💥 Delete Lifecycle Transition 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 Transition Action form. * Lifecycle State Registered * Command Type Command	A Payload Filter enables you to further define the filters to be used for selecting the Incidents that should participate in an operation; for example, be suppressed, enriched, dampened, run actions, or participate in pairwise. A Payload Filter selects incoming Incidents based on Custom Incident Attribute names (ciaName) and values (ciaValue). For more information, click here. Filter Editor Attribute Operator Value					
/var/opt/OV/shared/nnm/actions/RouterScript.ksh \$snn	ciaName v != 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.					

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.

File View Tools Actions Help						
Node Settings * 🗍 🐻 Save and Close 🖉 🗶 Delete Node Settings 🗳						
(i) Changes are not committed until the top-level form is saved!						
▼ Basics	Suppression Enrichment Dampening Actions Diagnostic Selections					
Node Group Important Servers • Ordering 20 Enabled Important Servers	Ordering 20 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					
	* Image: SeriptOrExecutable /var/opt/OV/shared/nnm/actions/ServerScript.ksh \$snn \$1 \$2					

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

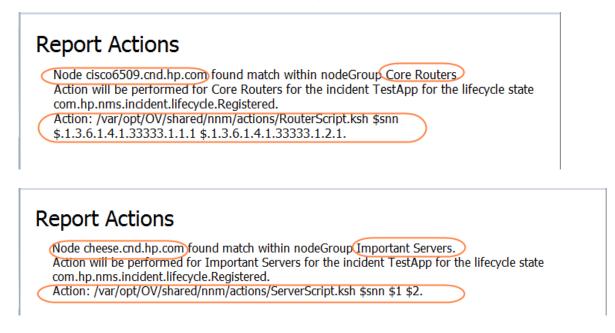
To confirm that action is configured properly:

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

File View Tools Actions Help								
Node Actions	•	8						
Incident Managem Interface Actions	•							
A Topology Maps IP Address Actions	s 🕨 🕨	ave and Close 🛛 🧭 X Delete Incide	nt 🛛 🔛					
Monitoring 🎇 Maps	•			General Correlated I	arents Correlated Children	Custom Attributes	.	
Troubleshooting 📑 Source Node					arents Correlated Children	Custom Attributes	Diagnostics	Registration
Inventory				✓ Details				
Management Mod	ers			Name	InterfaceDown			
Graph Custom Pole	er Results			Category	Fault 👻			
Node Access	•	Critical						
🗰 Open Key Inci 🔀 Delete		None 🔻		Family Origin	Interface NNMi			
Change Lifecycle	•	Registered		Correlation Nature	Root Cause			
Closed Key In Assign	•	Registered						
Open Root Ca Incident Configuration		Action Results		Duplicate Count	0			
🗰 Service Impac 🜌 Open Incident Conf				RCA Active				
All Incidents	SPINET only) (Evaluation) Source Object	Report Enrichments	T	Correlation Notes				
Custom Open Incidents		Clobal manager For Marang	-33°					
		Suppression Results						
Custom Incidents	Assigned To		T	First Occurrence Time	March 29, 2013 12:45:35 Pl			
NNM 6.x/7.x Events				Last Occurrence Time	March 29, 2013 12:45:35 Pl	N MDT		
Syslog Messages	▼ Notes			Origin Occurrence Time	March 29, 2013 12:45:35 Pl	M MDT		
III SNMP Traps	Notes							

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.



Next, send one of the traps.

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

Metwork Node Manager					User Name: system User Role: Administrator	Sign out	
File Tools Actions Help							
	nt - All Incidents						
Incide 🕅 Find Attached Switch Port	2 💎 🗣 🔁		All 👻	<set filt<="" group="" node="" td=""><td>r> - 1-3 of 3</td><td></td></set>	r> - 1-3 of 3		
Topole MIB Browser Monite Load MIB	Seve Prior LS v La	st Occurrence AT Source No	le Source Objec (Cate Fam Orig Cl	l Message	Notes	
Troub Upload Local MIB File	[III]	10 3:57:22 PM TJ cisco6509	none	12 III) SHHE 🔰	 TestApp on Core Router 3 CPU 	~	
Inven Restore All Default View Settings	🛅 🔼 🛕 11 🛃 4/24/	10 3:55:21 PM TJ cisco6509	none	👬 🌆 she 🕅	 TestApp on Core Router 3 CPU 		
Manag NNMi Status NNMi System Health Report	A 21 4/24/	10 3:55:18 PM cheese	none	📸 💼 🖬 😽	 TestApp on Important Server 2 CPU 		
Incide Status Distribution Graphs							
NNMi Self-Monitoring Graphs Trap Analytics (ISPI NET only)							
In Sign In/Out Audit Log							
Incident Actions Log	\square						
· · · · · · · · · · · · · · · · · · ·							
Apr 24, 2010 3:55:39,693	PM [ThreadID:10] FINE	com.bp.ov.nms.even	ts actionlog	ActionLogg	er addActionResponseToComplet	edList:	
				*			
Command: "/var/opt/OV/sh	ared/nnm/actions/Serve	erScript.ksh" "cheese	" "2" "CPU"				
Incident Name: TestApp							
Incident UUID: 07bf0b23-	b81a-4281-8081-bd08626	688b9					
Command Type: ScriptOrEx	ecutable						
Lifecycle state: com.hp.:	nms.incident.lifecycle	Registered					
Exit Code: 0							
Standard Output:							
Standard Error:							
Execution Status: Finished execution							
				-			

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		Incident
Save and Close X Delete Incident		Incluent
Basics	General Correlated Parent	ts Correlated Children Custom Attributes Diagnostics
Message	Registration	
TestApp on Core Router 3 CPU	Details	
Severity Warning 🗸	Name	TestApp
Priority Top 👻	Category	Application Status 👻
Lifecyde State	Family	Node
Registered	Origin	SNMP Trap
Source Node In Progress Completed	Correlation Nature	Root Cause
Source Object	Duplicate Count	0
Assigned To	RCA Active	
Assigned To	Correlation Notes	
Notes		
Notes		
Notes		
	First Occurrence Time	May 10, 2010 10:03:33 PM MDT
	Last Occurrence Time	May 10, 2010 10:03:33 PM MDT
	Origin Occurrence Time	May 10, 2010 10:03:33 PM MDT

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 2009–2013 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

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

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

 $\mathsf{UNIX} \ensuremath{\mathbb{R}}$ 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