### HP Network Node Manager i Software

#### Step- by-Step Guide to Incident Management

Software Version 9.00



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".

#### **Contents**

Step- by-Step Guide to Incident Management	1
Setting Up Your SNMP Trap	3
Dampening and the Incident Pipeline	6
Customizing Incident Configurations Using Interface or Node Groups	8
Deduplication	10
Rate	13
Enrichment	16
Suppression	21
More About Dampening	24
Lifecycle State and Actions	25

# 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 and click Incident Configuration.

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

Metwork Node Manag	jer
File Tools Actions Help	
Workspaces	Network Overview
Incident Management	👍 🚱 😰 🗗 🍭 111 🍳 🔍
Topology Maps	
Monitoring	
Troubleshooting	
Inventory	matter.
Management Mode	
Incident Browsing	
Integration Module Configuration	cheese
Configuration	
Communication Configuration	
Discovery Configuration	
Monitoring Configuration	
Custom Poller Configuration	
Incident Configuration	
Trap Forward Configuration 🖟	
Custom Correlation Configuration	

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

File View Tools	Actions Help						
🙆 📳 😼 Save	and Close					Ir	cident Configuration
	of the columns in an Incident Configuration table, dick New Window icon. Then sort, filter, and resize the d.	SNMP		note NNM 6.x/7.x Eve	Management Even		e Configuration
NNMi Trap Handling	Settings		New	▲ Name	SNMP Object ID	Enat RC	Seve Cate
Discard Unresolved SNMP Traps				· ·	.1.3.6.1.4.1.8083.1.1 .1.3.6.1.4.1.8083.1.1		<mark>⊗</mark> c ⊯ <sub>F</sub> ^ ⊗ c ⊯ <sub>F</sub>
				· ·	.1.3.6.1.4.1.8083.1.1		⊘ N <b>≭</b> F
Registration					x .1.3.6.1.4.1.8083.1.1		🛿 C 🗱 F
Last Modified	April 1, 2010 2:05:43 PM MDT			RexVpnSiteUne	x .1.3.6.1.4.1.8083.1.1		🛛 <sub>C</sub> 🗯 <sub>F</sub>
				RMONFallingAla	1.3.6.1.2.1.16.0.2		🛇 N 端 F
				RMONRiseAlarm	.1.3.6.1.2.1.16.0.1		V M 🗱 F
				SNMPColdStart	.1.3.6.1.6.3.1.1.5.1	v -	🛇 N 🔆 F

- 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. Click Save and Close to save the changes.

File View Tools Action	ns Help						
👍 📳 🛂 Save and C	Close 🖄 X Delete SNMP Trap Configuration					SNMP '	Trap Configuration
Basics		Interface Setting	s Node Settings	Suppression	Enrichment	Dampening	Deduplication
For information about trouble	eshooting Incidents, click here.	Rate Actions	Forward to Global	Managers			
Name SNMP Object ID Enabled Root Cause Category Family Severity Specify how the Incident men Incident information in the m	TestApp .1.3.6.1.4.1.33333.0.1 ✓ Application Status Mode Warning ↓ Stage appears in the Incident view. To include vessage use \$(variable_name). Select these parameters or Custom Incident attributes. For	NNMi enables y Object based o override any of Inddent, indud Image: Second Second Image: Second Second Image: Second Second Image: Second Second Image: Second Second Image: Second Second Second Image: Second Second Second Second Second Image: Second Seco	ou to apply a Suppr n the Source Objec her Suppress, Enric ing those configure	ress, Enrich, Da t's participation d on the Node S e Group Ord	in an Interfac Action configu estimgs tab. 0 - 0 of 0 dering Ena	e Group, Inte ration setting abled	rface Settings s for this
Done							

11. 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 Management 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.

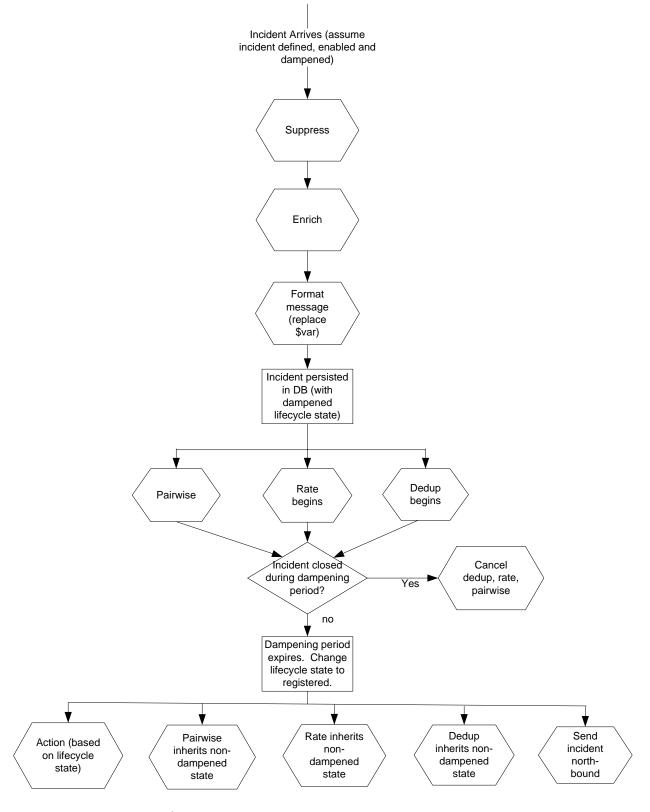
Workspaces	Incident - Open Key Inc	idents								
Incident Management	× © 0 C	۲					Last	Week		<ul> <li><set filter="" group="" node=""></set></li> </ul>
<ul> <li>Open Key Incidents</li> <li>Unassigned Open Key Incidents</li> </ul>		Se Prior VLS	Last Occurrence AT	Source Node	Source Objec	Cate	Fam	Origi	Vc	Message
My Open Incidents		5 🛛 🖏	4/9/10 11:58:07 AM	cheese	none	12 Celi	1	SNMP	PX4	TestApp 2 CPU
		5.0 🖏	4/9/10 11:57:14 AM	cisco6509	none	14	1	SHHP	P14	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 acts 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 it 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.

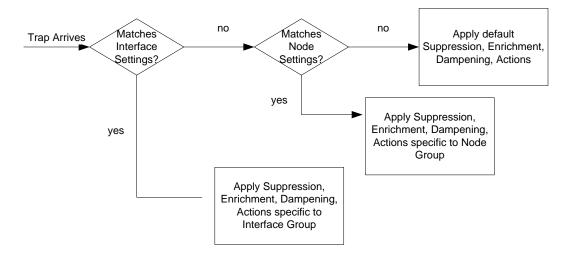
# Customizing Incident Configurations Using Interface or Node Groups

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. Select Incident Configuration.
- 3. Click the Open 🐴 icon to open the TestApp trap.

File View Tools Act	ions Help d Close							Inci	dent Co	onfigurat
To more easily view all of t the <b>5how View in Ne</b> table columns as needed.	the columns in an Incident Configuration table, click w Window icon. Then sort, filter, and resize the			NNM 6.x/7.x Ever	nts Manage	ement Even		airwise	Configu	
table columns as needed.		1	S	E#		92 - 110 (	of 110			
NNMi Trap Handling Set	tings			🔺 Name	SNMP Obj	ect ID	Enat	RC	Seve	Cate
Discard Unresolved SNMP Traps				RexVpnSitePrefix RexVpnSitePrefix				-		<b>⊭</b> ⊦ ^
SNMP Traps				RexVpnSiteUnex				-	⊘ N :	
Registration				RexVpnSiteUnex				-	<mark>8</mark> с: 8с:	
Last Modified	April 5, 2010 11:50:43 AM MDT			RMONFallingAlar			-	-	© N ⇒	
Last Modified	April 5, 2010 11:50:45 AM MD1			RMONRiseAlarm			-	-	V <sub>M</sub>	
				SNMPColdStart	.1.3.6.1.6.	3.1.1.5.1	~	-	ON 2	
				SNMPLinkDown	.1.3.6.1.6.	3.1.1.5.3	~	-	8 c	¥ F
				SNMPLinkUp	.1.3.6.1.6.	3.1.1.5.4	~	-	ØN :	#F
				SNMPWarmStart	.1.3.6.1.6.	3.1.1.5.2	~	-	🛇 <sub>N</sub> :	¥⊧
				STPNewRoot	.1.3.6.1.2.	1.17.0.1	-	-	Δ.,	¥ F
				STPTopologyCha	.1.3.6.1.2.	1.17.0.2	-	-	× N 🛆	¥ F
					.1.3.6.1.4.			-	_	×F
				TestApp	.1.3.6.1.4.		•	~		A 1
								-	-	× F
				Open HighLinkUt				-		× F
				TrafficLinkCoSUt				-		* F =
				TrafficLowLinkUt				-		<b>≭</b> F
			4	TrafficQuantityA	.1.3.6.1.4.	1.8083.1.1	-	-	<u> </u>	<u>*</u> F -
		lpdated: 4,	9/10 1	111 2:03:54  Total:	110 Selecte	ed: 0   Filte	r: OFF	Auto	refresh	: OFF
Done										

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

File View Tools A	tions Help	Narrows context to specific Otherwise, apply these settings if no match is	
👍 📳 😼 Save a	nd Close 🏽 🏥 🗙 Delete SNMP Trap Confi	Interfaces and Nodes Narrows context to specific Otherwise, apply these settings if no match is made for Interfaces and Nodes	SNMP Trap Configuration
Basics		Interface Settings Node Settings Suppression Enrichment Dampening Deduplication Rate Actions F	orward to Global Managers
Name SNMP Object ID Enabled Root Cause Category Family Severity 	ubleshooting Incidents, dick here. TestApp 1.13.6.1.4.1.33333.0.1 Application Status Node Warning message appears in the Incident view. To inclu e message use §(variable name). Select these alid parameters or Custom Incident attributes. F ree.		urce Object's participation in gs for this Incident,
TestApp \$1 \$2			
Description			
Author	Customer 🚮 -	✓	Auto refresh: OFF
		opdated. 1/0/10 3/24/10 PM	Auto reiresti: OFF
Done		ŀ	

## 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. Select Incident Configuration.
- 3. Click the Open 🖾 icon to open the TestApp trap.
- 4. Navigate to the **Deduplication** tab.
- 5. 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**.
- 6. 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**.
- Next, in the Correlation Incident Config drop-down list, select the incident that you want NNMi to generate to indicate that Deduplication has occurred. For this example, select DuplicateCorrelation.
- 8. 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).

File View Tools Actions Help			
👍 📳 🛂 Save and Close 🏥 🗙	Delete SNMP Trap Configuration		SNMP Trap Configuration
Basics		Interface Settings Node	Settings Suppression Enrichment Dampening Deduplication
For information about troubleshooting Incident	s, dick here.	Rate Actions Forward	i to Global Managers
Name     TestApp       SNMP Object ID     .1.3.6.1.4.1.333       Enabled     Image: Comparison of the state of t	is	duplicate. Duplicate Incid the number of duplicates It is incremented on the Enabled Count Hours Minutes Seconds Correlation Incident Config Comparison Criteria	s what values NNMi should match to detect when an Incident is a dents are listed under a Duplicate Correlation Incident. NNMi tracks generated. This value is captured as the Duplicate Count attribute. Duplicate Correlation Incident. 2 0 3 0 DuplicateCorrelation DuplicateCorrelation Name SourceNode
Message Format		Deduplication Compa	
TestApp \$1 \$2 Description			Parameter Value
Author Customer		< Updated: 4/9/10 12:06	5:45 PM  Total: 0   Selected: 0   Filter: OFF   Auto refresh: OFF
Done			

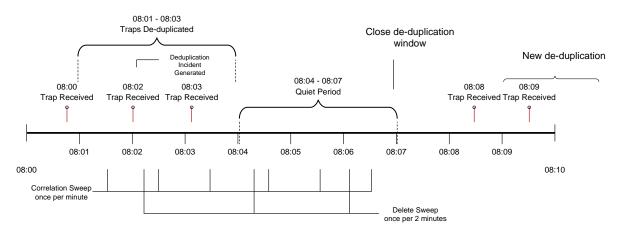
The diagram below depicts the following scenario:

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.

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



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	nt - Ope	en Key Ir	cidents										
Incident Management	X		0	جا 🔊	<b>F</b>	]				Las	t Week		<ul> <li><set filter="" group="" node=""></set></li> </ul>	
Topology Maps														
Monitoring			8	√S€ Pri	n Ar	LS - Last Occurrence AT	Source Node	Source Object	Cate	Fam	Origi	Δd	Message	
Troubleshooting				🛆 5 🗸	5	4/9/10 12:39:06 PM	cheese	none			SNMP	₽ <u>¥</u> 4	TestApp 2 CPU	
Inventory				🛆 5 🗸	2	4/9/10 12:39:03 PM	cheese	none			SNMP	₽ <u>¥</u> 4	TestApp 2 CPU	
Management Mode			<u>(</u>	🛆 5 🖵	2	4/9/10 12:39:03 PM	cheese	none		17	۳	₩ <b>4</b>	Duplicate Correlation for TestApp	
Incident Browsing				🛆 5 🖵	- Č.	4/9/10 12:39:00 PM	cheese	none			SNMP	₽ <u>¥</u> 4	TestApp 2 CPU	
Integration Module Configuration														
Configuration														
A commission conference														

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	ת <u>ו</u>	ident
Basics	General Correlated Parents Correlated Children Custom Attributes Diagnostics Registration	
Message Duplicate Correlation for TestApp	() () () () () () () () () () () () () (	
Severity Warning 👻	Seve v Last Occurrence Type Message Source Node Source Object	
Distance of the second s	📺 🖾 🛆 4/9/10 12:39:06 PM De-Dup Correlation TestApp 2 CPU cheese none	~
	📺 🔼 4/9/10 12:39:03 PM De-Dup Correlation TestApp 2 CPU cheese none	
Lifecyde State Registered 👻	📺 🔼 4/9/10 12:39:00 PM De-Dup Correlation TestApp 2 CPU cheese none	
Source Node cheese		
Source Object none		
Assigned To		
	J	
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.

ile View Tools Actions Help	. In
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 -	IIII A 4/9/10 12:39:06 PM De-Dup Correlation TestApp 2 CPU cheese none
Lifecycle State Registered 👻	IIII 🚵 🛕 4/9/10 12:39:03 PM De-Dup Correlation TestApp 2 CPU cheese none
Source Node cheese	
Source Object none	
Assigned To	
lotes	
Notes	
	۲. III ا
	Updated: 4/9/10 12:42:37 PM Total: 2 Selected: 0 Filter: OFF Auto refresh: OFF

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. Select Incident Configuration.
- 3. Click the Open 🖾 icon to open the TestApp trap.
- 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.

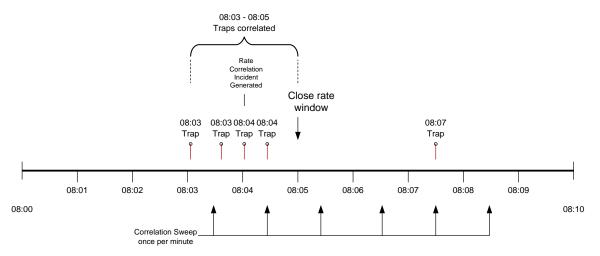
- 3. In the Count attribute, enter **3**.
- 4. In the Minutes attribute, enter 2.
- 5. In the Correlation Incident Config drop-down list, select RateCorrelation.
- 6. In the Comparison Criteria drop-down list, select Name SourceNode.
- 7. Click Save and Close to save the configuration.

File View Tools Actio	ons Help	
👍 🖪 😼 Save and	Close 🖄 🗙 Delete SNMP Trap Configuration	SNMP Trap Configurat
Basics		Interface Settings Node Settings Suppression Enrichment Dampening Deduplication
For information about troub	leshooting Incidents, click <b>here</b> .	Rate Actions Forward to Global Managers
Name SNMP Object ID Enabled Root Cause Category Family Severity Specify how the Incident me Incident information in the n	TestApp .1.3.6.1.4.1.33333.0.1 Application Status Application Status Mode Warning ssage appears in the Incident view. To include message use \$(variable_name). Select these parameters or Custom Incident attributes. For	Use Rate Configuration 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 readed, NIMI emits a Rate Correlation Incident and continues to update the Correlation Offers with the number of occurrences within that rate. Enabled Count 3 Hours 0 Minutes 2 Seconds 0 Correlation Incident Config Comparison Criteria Name SourceNode Rate Comparison Parameters
Done		

The diagram below 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.

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



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	Incide	nt - All	Incident	s												
Incident Management	X		•	<b>.</b>	<b>-4</b>							All			<ul> <li><set filter="" group="" node=""></set></li> </ul>	•
Topology Maps										4						•
Monitoring				Seve	Prio	LS		AT	Source Node	Source Objec	Cate	Fam	Orig	CN	Message	
Troubleshooting	<b></b>			$\Delta$	5	- C- 1	4/15/10 2:25:38 PM	)	cheese	none			SNMP	<b>(</b>	TestApp 2 CPU	
Inventory				$\Delta$	5	5	4/15/10 2:22:48 PM		cheese	none		17	۲.	₽ <u>⊼</u> 4	Rate Correlation for TestApp	
Management Mode				$\Delta$	5 🔒	2	9/15/10 2:22:48 PM	$\mathbf{N}$	cheese	none			SHIP /	(Jacoba)	TestApp 2 CPU	
Incident Browsing				Δ	5	5	4/15/10 2:22:15 PM		cheese	none			SHIP	<b>≧</b> ≁≏	TestApp 2 CPU	
🚥 Open Key Incidents				$\Delta$	5	5	4/15/10 2:21:55 PM		cheese	none	12 12		SNHP	<u></u>	TestApp 2 CPU	
🕅 Closed Key Incidents					5	5	4/15/10 2:21:33 PM	)	cheese	none			SHIP		TestApp 2 CPU	
Open Root Cause Incidents														$\overline{}$		
Service Impact Incidents																
All Incidents																
Custom Open Incidents																
Custom Incidents																
NNM 6.x/7.x Events																
SNMP 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 Open Key Incidents	Image: Set node group filter
Unassigned Open Key Incidents	Source Objec Cate Fam Orig VCI Message
I My Open Incidents	📄 📷 📥 5 🖳 🖏 4/15/10 2:25:38 PM dheese none 📸 🜆 🚥 🔀 TestApp 2 CPU
	📄 📷 📥 5. 🛛 💐 4/15/10 2:22:48 PM cheese none 🝙 🎁 😼 🔀 Rate Correlation for TestApp

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

File View Tools Actions Help		Incident
Basics Message Rate Correlation for TestApp	General Y Correlated Parents Correlated Children Dustom Attributes	V Diagnostics V Registration
Severity Warning  Priority None  Lifecyde State Registered	Sevi         ► Last Occurrency         Type           Image: Sevier and Sev	Message         Source Node         Source Object           TestApp 2 CPU         cheese         none         *           TestApp 2 CPU         cheese         none         *           TestApp 2 CPU         cheese         none         *
Source Node cheese  Source Object Assigned To	A 4/15/10 2:21:33 PM Rate Correlation	TestApp 2 CPU cheese none
Assigned To		

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: Constraint of the second secon			
Basics		General Correlated Parents	Correlated Children Custom Attributes Diagnostics Registration
Message Rate Correlation for TestApp		Details	
Severity Priority	Warning  Vone  Von	Name Category Family	RateCorrelation Performance Correlation
Lifecyde State Source Node	Registered  cheese	Origin Correlation Nature	NNMi Root Cause
Source Object	none	Duplicate Count RCA Active	0
Assigned To		Correlation Notes	rcidents hours, 2 minutes, 0 seconds
Notes		-	rom Thursday, April 15, 2010 2:21:33 PM MDT
Notes		to Thursday, April 15, 2010	2:22:48 PM MDT.
		First Occurrence Time	April 15, 2010 2:21:33 PM MDT April 15, 2010 2:22:48 PM MDT
		Origin Occurrence Time	April 15, 2010 2:22:33 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. Select Incident Configuration.
- 3. Click the Open 🚢 icon to open the TestApp trap.
- 4. Navigate to the Node Settings tab.
- 5. Click the New 🛍 icon.

File View Tools Action		
Basics		Interface Settings Node Settings Suppression Enrichment Dampening
For information about trouble	shooting Incidents, dick here.	NNMi enables you to apply a Suppress, Enrich, Dampen, Action, or Diagnostic
Name	TestApp	Node's participation in a Node Group. Node Settings override any other Suppr
SNMP Object ID	.1.3.6.1.4.1.33333.0.1	configuration settings for this Incident, except those configured on the Interf
Enabled		
Root Cause		New Node Group Ordering Enabled
Category	Application Status	
Family	Node 👘 🗸	
Severity	Warning -	

- 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** 한 icon.

File       View       Tools       Actions       Help         Image: Save and Close       Image	Node Settings
Basics       Node Group     Core Routers       Ordering     10       Enabled     Image: Core Routers	Suppression         Enrichment         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 enrichment configuration by selecting an Incident and choosing Actions → Incident Configuration Reports → Report Enrichments.           Enabled         ✓
	Enrichments

- 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.

	Actions Help and Close	nfiguration	Enrichment Configura
i) Changes are not c	ommitted until the top-level form is saved!		
asics		Custom Attributes Payload Filter	
Category			0 - 0 of 0
Family		Type	Custom Attribute Name Custom Inc
Severity			
Correlation Nature			
Message Format			
TestApp on Core Rou			
Assigned To	CT CT		
Description			
		✓	4
		Updated: 4/14/10 9:31:26 AM Total	I: 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. Select Incident Configuration.
- 3. Click the Open 🐴 icon to open the TestApp trap.
- 4. Navigate to the **Node Settings** tab.
- 5. Click the New 🛍 icon.

File View Tools Actions Help	
🔄 🖹 🖄 Save and Close 🏥 🗙 Delete SNMP Trap Configuration	SNMP Trap Configuration
Basics	Interface Settings Node Settings Suppression Enrichment Dampening Deduplication Rate
For information about troubleshooting Incidents, dick here.	Actions Forward to Global Managers
Name     TestApp       SNMP Object ID     .1.3.6.1.4, 1.33333.0.1       Enabled     Image: Comparison of the status of the s	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.
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	

- 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.

File     View     Tools     Actions     Help       Image: State and Close     Image: State and Close     Image: State and Close     Image: State and Close	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     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 Ca Fam Seve Prior CN AT Message Format
	Image: Vertical state     Image: Vertical state       Updated: 4/14/10 9:40:17 AM     Total: 0       Selected: 0     Filter: OFF       Auto refresh: OFF
Done	

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.
- 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         Image: Save and Close       Image	Enrichment Configuration
Basics         Category         Family         Severity         Priority         High         Correlation Nature         Message Format         TestApp on Important Server \$1 \$2         Assigned To         Description	Custom Attributes Payload Filter

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.

🛆 🗒 😼 Save and Close 🏨 🗙 Delete Node Settings 🚱 Node Set	
Image: Save and Close     Image: Save and Close <td< th=""><th>ings</th></td<>	ings
(i) Changes are not committed until the top-level form is saved!	
Basics (Suppression) Enrichment Dampening Actions Diagnostic Selections	
Node Group       Important Servers       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       Enabled       Enabled       Enabled         Payload Filter       A Payload Filter enables you to further define the filters to be used for selecting the Incident 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 v = v Append Insert Replace	
There is currently no filter defined.  Append AND OR Delete Filter String	] ] ]
Done	

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 Mana	ger User Name: system User Role: Administrator	Sign out
File Tools Actions Help		
Workspaces	Incident - Open Key Incidents	
Incident Management	X         Image: Set node group filter>         ✓         Image: Set node group filter         ✓         Image: Set node group fi	
Topology Maps		
Monitoring	Source Nobel Source Objec Cate Fam Origi VCh Message	Notes
Troubleshooting	📗 🔚 🖾 🛆 11 🛃 4/20/10 10:52:13 PM TJ 🛛 cisco6509 none 🙀 🌆 📟 💦 TestApp onCore Route? 2 CPU	~
Inventory	📗 🔚 🖾 🛆 24 🖉 🦉 4/20/10 10:52:10 PM 🖉 cheese none 🛛 🙀 🖅 🔤 👾 🏹 TestApp on Important Server 3 CPU	
Management Mode		
Incident Browsing		
Integration Module Configuration	2	
Configuration		

### 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.

File View Tools Actions Help	
🔄 📓 Save and Close 🏥 🗙 Delete SNMP Trap Configuration	SNMP Trap Configuration
Basics	Interface Settings Node Settings Suppression Enrichment Dampening Deduplication
For information about troubleshooting Incidents, click here.	Rate Actions Forward to Global Managers
Name     TestApp       SNMP Object ID     .1.3.6.1.4.1.33333.0.1       Enabled     ✓       Root Cause     ✓       Category     Application Status       Family     Node       Family     Node       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	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. Node Group Ordering Enabled Core Routers 10 Den Important Servers 20 Open

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

- 1. Navigate to the Configuration Workspace.
- 2. Select Incident Configuration.
- 3. Click the Open 🐴 icon to open the TestApp trap.
- 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: Save and Close         Image: Save and Close <th image<="" th=""><th>Node Settings</th></th>	<th>Node Settings</th>	Node Settings
$({\bf \hat{j}})$ 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     IV	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.	
	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         ciaName       =         Append         Insert         Replace	
	OR       Append         - AND       AND         - ciaName = .1.3.6.1.4.1.33333.1.1.1       OR         - ciaName = .1.3.6.1.4.1.33333.1.1.1       Delete         - 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	

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, click the Open 🚢 icon that precedes the incident of interest.
- 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	
👍 🖪 🖥 s	Node Actions	Incident
	IP Address Actions	
Basics	Node Group Map	ren Custom Attributes Diagnostics
Message	Path View Registration	
TestApp on Core R	Source Node Details	
Severity	Source Object Node Group Members TestApp	
Priority	Cotecerv Automatical	-
Lifecycle State	Graph Custom Polier Results	
	Delete Origin SNMP Trap	
Source Node	Change Lifecycle Correlation Nature Root Cause	
Source Object	Incident Configuration Reports	
-	Open Incident Configuration     Dampen Results     Report Enrichments	
Assigned To	Kun Diagnostics (ISP1 NET only) (Evaluation) Global Manager Forwarding	
	Suppression Results	
Notes		
Notes		

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.

3

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
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.

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

Metwork Node Mana	ger User Name: system User Role: Administrator	Sign out
File Tools Actions Help		
Workspaces	Incident - Open Key Incidents	
Incident Management	Last Week + <set filter="" group="" node=""> +</set>	
Topology Maps		
Monitoring	Source Nobe Source Objec Cate Fam Origi VCt Message	Notes
Troubleshooting	📗 🔄 🚵 🔺 🖞 🛃 4/20/10 11:36:09 PM TJ cisco6509 none 📑 🌆 뺆 🔀 TestApp on Core Router 3 CPU	-
Inventory		
Management Mode		
Incident Browsing		
Integration Module Configuration		
Configuration	N N	
Communication Configuration	13 13 13 13 13 13 13 13 13 13 13 13 13 1	
Discovery Configuration		

# 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:

File View Tools Actions Help			
🔄 🖹 🖄 Save and Close 🏥 🗙 Delete Management Event Config	guration	Management Ev	ent Configuration
Basics	Interface Settings Node Settings	Suppression Enrichment Dampening	Deduplication
For information about troubleshooting Incidents, click here.	Rate Actions	<u> </u>	
Name       InterfaceDown         SNMP Object ID       .1.3.6.1.4.1.11.2.17.19.2.0.19         Enabled           Category       Fault         Family       Interface         Severity       Critical         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         Interface Down         Description         This incident indicates that the interface is not responding to polls.         Author           Method	Enabled Use a maximum of 60 minutes for th Hours 0 Minutes 6 Seconds 0 Payload Filter A Payload Filter enables you to furt Incidents that should be suppresse	Incident views. SPI Network Engineering Toolset only), he Dampen Interval ther define the filters to be used for selectir id, enriched, or dampened. A Payload Filter m Incident Attribute names (ciaName) and v ick here.	ppend insert eplace
Done			

### 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 script 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. Select Incident Configuration.
- 4. Click the Open 🚢 icon to open the TestApp trap.
- 5. Navigate to the **Node Settings** tab.
- 6. In the **Node Group** drop-down list, select the **Core Routers** Node Group.
- 7. In the Ordering attribute, enter 10.
- 8. Click to check **Enabled**.
- 9. Click the New 🛍 icon.

File         View         Tools         Actions         Help           Image: Comparison of the setting s	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	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.
	Lifecycle Transition Actions
	New LS Command 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.

File View Tools A	Actions Help	n 🛛	]			Lifecycle Transition Action
Enter the Java Jython fi changes to the specified values as parameters int Action form. Lifecycle State Command Type Command	mmitted until the top-level form is saved! ile, executable, or script to run when an Incident d Lifecycle State. You can pass Incident attribute to each. See Help → Using the Lifecycle Transition Registered ScriptOrExecutable	Paylo A P Inci inca (cia Fil	Payload Filter Payload Filter enables idents that should be oming Incidents base avalue). For more infi <b>Iter Editor</b>	e suppressed, enrich d on Custom Incide	ne the filters to be used for red, or dampened. A Paylo t Attribute names (ciaNar Value	oad Filter selects
Var jopt/UV isnared,inn	m/actions/RouterScript.ksh \$snn \$.1.3.6.1.4.1.333	ть гы	ere is currently no fil lter String ere is currently no fil			Append Insert Replace Append AND OR Delete

Next configure the action for the Important Servers Node Group.

- 1. Navigate to the **Configuration** Workspace.
- 2. Select Incident Configuration.
- 3. Click the Open 🚢 icon to open the TestApp trap.
- 4. Navigate to the Node Settings tab.
- 5. In the **Node Group** drop-down list, select the **Important Servers** Node Group.
- 6. In the Ordering attribute, enter 20.
- 7. Click to check Enabled.
- 8. Click the New 🛍 icon.
- 9. In the Lifecycle State drop-down list, select Registered.
- 10. In the Command Type drop-down list, select ScriptOrExecutable.
- 11. In the Command attribute, enter the following command: /var/opt/OV/shared/nnm/actions/ServerScript.ksh \$snn \$1 \$2
- 12. Click **Save and Close** to return to the SNMP Trap Configuration form.
- 13. Click Save and Close to save your changes.

File View Tools Actions Help	
🕍 📓 🖾 Save and Close 🎼 🗙 Delete Node Settings	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     ✓	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

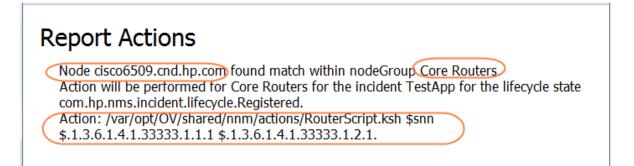
To confirm that action is configured properly:

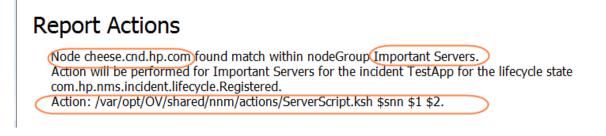
- 1. From an incident view, click the Open 🚢 icon that precedes the incident of interest.
- 2. Select Actions->Incident Configuration Reports-> Action Results.

File View Tools	Actions Help				
👍 📳 😼 Sav	Interface Actions			Incid	ident
Basics	IP Address Actions		General Correlated Parents	Correlated Children Custom Attributes Diagnostics	
Message	🦻 Path View		Registration		
TestApp on Core Rou	4		Details		
Severity	Source Object Node Group Members		Name	TestApp	
Priority	Graph Custom Poller Results		Category	Application Status 👻	
Lifecycle State	X Delete		Family	Node	
Source Node	Change Lifecycle		Origin Correlation Nature	SNMP Trap Root Cause	
Source Object	Incident Configuration Reports	Actio	n Results		
	Open Incident Configuration	Damp Repo	pen Results	0	
Assigned To	Run Diagnostics (ISPI NET only) (Evaluation)	Globa	al Manager Forwarding pression Results		
			Correlation Notes		
Notes					
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.

Network Node Manager							User Name: system User Role: Administ	rator Sign
	nt - All Incidents							
cide 🕅 Find Attached Switch Port	5			All 👻	Set node grou	p filter>	• • • • • • • • • • • • • • • • • • •	
nite Load MIB	Seve Prior	LS - Last Occurrence	e AT Source Nod	e Source Objec		CN	Message	Notes
Upload Local MIB File	🛅 🔼 🔺 📫	4/24/10 3:57:22 PM	TJ cisco6509	none	RE SHP	- Þ <u>⊼</u> ∢	TestApp on Core Router 3 CPU	
en Restore All Default View Settings	🛅 🖾 🔺 📫	4/24/10 3:55:21 PM	TJ cisco6509	none	RE SHP	- Þ <u>⊼</u> 4	TestApp on Core Router 3 CPU	
nac NNMi Status NNMi System Health Report	[III] [III] [III] [IIII] [IIIII] [IIIIII] [IIIIIII] [IIIIII] [IIII	4/24/10 3:55:18 PM	cheese	none	SINHP	- <b>b</b> <u>⊼</u> 4	TestApp on Important Server 2 CPU	
cide Status Distribution Graphs								
O NNMi Self-Monitoring Graphs Trap Analytics (iSPI NET only)								
d								
Ose Signed In Lisers								
Sign In/Out Audit Log								
Incident Actions Log								
Custom Open Incidents								
pr 24, 2010 3:55:39.693						gger	addActionResponseToCompl	.etedList:
pr 24, 2010 3:55:39.693						gger	addActionResponseToCompl	etedList
pr 24, 2010 3:55:39.693 Command: "/var/opt/OV/shi incident Name: TestApp	ared/nnm/actions	s/ServerScript.				gger	addActionResponseToCompl	.etedList:
pr 24, 2010 3:55:39.693 Command: "/var/opt/OV/shi incident Name: TestApp incident UUID: 07bf0b23-1	ared/nnm/actions	s/ServerScript.				gger	addActionResponseToCompl	.etedList
pr 24, 2010 3:55:39.693 command: "/var/opt/0V/sh. incident Name: TestApp incident UUID: 07bf023-1 command Type: ScriptOrEx.	ared/nnm/actions b81a-4281-8081-f ecutable	s/ServerScript.	.ksh" "cheese'			gger	addActionResponseToCompl	.etedList;
pr 24, 2010 3:55:39.693 command: "/var/opt/OV/shi ncident Name: TestApp ncident UUID: 07bf0b23-1 ormmand Type: ScriptOrEx. difecycle state: com.hp.1	ared/nnm/actions b81a-4281-8081-f ecutable	s/ServerScript.	.ksh" "cheese'			gger	addActionResponseToCompl	etedList
Apr 24, 2010 3:55:39.693 Command: "/var/opt/OV/shi Incident Name: TestApp Incident UUID: 07bf0b23-1 Command Type: ScriptOrEx. Lifecycle state: com.hp.: Exit Code: 0	ared/nnm/actions b81a-4281-8081-f ecutable	s/ServerScript.	.ksh" "cheese'			gger	addActionResponseToCompl	.etedList;
pr 24, 2010 3:55:39.693 command: "/var/opt/0V/shi incident Name: TestApp incident UUID: 07bf0b23-1 command Type: ScriptOrExd ifccycle state: com.hp.1 xit Code: 0 tandard Output:	ared/nnm/actions b81a-4281-8081-f ecutable	s/ServerScript.	.ksh" "cheese'			gger	: addActionResponseToCompl	etedList;
Apr 24, 2010 3:55:39.693 Command: "/var/opt/0V/sh. Incident Name: TestApp Incident UUID: 07bf0b23-J Command Type: ScriptOrEx. Lifecycle state: com.hp.: Exit Code: 0 Standard Output: Standard Error:	ared/nnm/actions b91a-4281-8081- ecutable nms.incident.lis	s/ServerScript.	.ksh" "cheese'			gger	addActionResponseToCompl	.etedList;
	ared/nnm/actions b91a-4281-8081- ecutable nms.incident.lis	s/ServerScript.	.ksh" "cheese'			gger	addActionResponseToCompl	.etedList;

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, click the Open 🖾 icon that precedes the incident of interest.
- 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. HP Network Node Manager i Software Step- by-Step Guide to Incident Management

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