HP OpenView
Network Node Manager Smart Plug-in

Network Node Manager / Route Analytics Management System Integration Module

User's Guide

Software Version: 3.5.0

for HP-UX, Solaris, and Windows® operating systems

Manufacturing Part Number : (none)

May 2005

Legal Notices

Warranty.

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company, United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices.

Trademark Notices.

Linux is a U.S. registered trademark of Linus Torvalds.

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

Netscape™ and Netscape Navigator™ are U.S. trademarks of Netscape Communications Corporation.

Contents

Contents

Support

Please visit the HP OpenView support web site at:

http://www.hp.com/managementsoftware/support

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

HP OpenView online software 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 valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter 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 log in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

http://www.managementsoftware.hp.com/passport-registration.html

1 Overview

The NNM/RAMS Integration Module integrates information from the HP OpenView Route Analytics Management System (RAMS appliance) into NNM Advanced Edition.

Overview

The integration of NNM Advanced Edition with the HP OpenView Route Analytics Management System (RAMS) gives you a powerful tool to pinpoint, analyze, and prevent problems in your OSPF, IS-IS, or BGP routing fabric.

Combining NNM's knowledge of layer-2 topology and RAMS' knowledge of layer-3 routing, this Integration Module gives you real-time and historical perspectives on important changes in your IP network.

It lets you visualize your routing environment using maps and tables built from real-time routing protocol data. These views are accessible in NNM directly from Home Base, or from the Alarms Browser menus.

The NNM/RAMS Integration Module also feeds RAMS events into the sophisticated root cause analysis of NNM Advanced Edition. You get real-time notification of changes in your routing, enhanced with layer-2 data to understand the source of the change.

Furthermore, you can monitor key routes in your network, and get immediate correlation between layer-2 faults and their layer-3 effects.

NNM/RAMS Integration Module Protocol Diagnosis gives you the ability to pinpoint OSPF router misconfigurations that can cause adjacency loss.

Use the integration of NNM Advanced Edition and RAMS to keep up with your routers as they adapt to network changes. Analyze the transitions over time, and quickly address any underlying issues.

RAMS Views

Along with root-cause analysis of routing topology events, the NNM/RAMS Integration Module creates two new Dynamic Views:

- The RAMS Path History View, which lets you see and compare current and historical routing topologies in your network.
- The RAMS IGP (Internal Gateway Protocol) View, which offers detailed OSPF or IS-IS information.

- The RAMS Neighbor View provides direct access to troubleshooting tools in the area surrounding a node with a failure alert from RAMS. (Since the RAMS appliance is always the source node, the standard Neighbor View displays the neighbors of the appliance rather than the neighbors of the failing node.)

The online help for these views has much more detail about each view, and instructions on how to make use of them. To access RAMS help, click the “Solutions” icon (building blocks) of NNM’s web-based help system (URL: `http://`*`nnm_mgmt_station`*`:3443/OvCgi/OvWebHelp.exe`)

Using the NNM/RAMS Integration Module

There are a variety of ways to use the NNM/RAMS Integration Module to troubleshoot your routing topology:

- Configure RAMS events so that you are notified about important routing changes in your network. You can monitor NNM's Status Alarms category for root-cause correlated events (for example, the loss of an OSPF adjacency, caused by a intermediary switch failure). In addition, the Route Analytics category provides a central location for all RAMS alarms. After you install the NNM/RAMS Integration Module, you can link to the appliance to enable and configure RAMS alarms:

  — Configure the Route Change event so that NNM will alert you when it detects changes in important layer-3 paths.

  — Configure the Adjacency Lost event, so that NNM will alert you when critical adjacencies are disrupted. NNM will correlate OSPF adjacency changes to the root cause faults at layer 2.

  — Configure the Prefix Origination Change event to monitor the advertisements of critical networks in your OSPF environment.

  — Configure the Prefix Flap event to monitor the reachability stability of critical networks in your OSPF environment.

  — If you are using the RAMS mBGP SPI, configure the VPN Loss Customer Reachability alarm. This alarm signifies failures of router interfaces which have an associated MPLS BGP VRF table.

  See “Configuring RAMS Events” on page 26, and Chapter 4, RAMS Alarms, for a more complete description of RAMS events and related correlations.

- For OSPF Adjacency Lost alarms not related to a layer-2 root cause failure, run Protocol Diagnosis to automatically query both end devices looking for misconfigured protocol settings in their configurations.

- Use the RAMS Path History view to monitor OSPF or IS-IS paths

  — See the current path between two nodes to verify that it meets your expectations.

  - — View differences in the path between two nodes at different points in time. This is particularly useful after you have been notified of a path change.

- Use the RAMS IGP view as a window into your network. You can see near real-time or historical data.
  - — Open the the RAMS IGP View's network map to display the logical (Layer 3) connectivity of your network.
  - — Use the IGP View's `Protocol Links` table to monitor adjacency status.
  - — Use the view's `Protocol Routers` table to track router inventory.
  - — Display the routing topology in the `Protocol Prefixes` table to better understand the IP v4 prefixes advertised by a router and route distribution configuration issues in your network.
- From any dynamic view, select a router monitored by RAMS and use the pop-up menu to access RAMS report data about the routing.
  - — The IGP Summary Report shows the system information and provides links to detail reports for Link Flaps, Link Metric Changes, All Events, Prefixes Withdrawn, and New Prefixes Advertised. The detail reports are also available from the pop-up menu.
  - — The BGP Summary Report contains system overview information such as the system type, which AS it belongs to, and its router ID.

The online help has much more detail. To access RAMS help, click the “Solutions” icon (building blocks) of NNM’s web-based help system (URL: `http://`*`nnm_mgmt_station`*`:3443/OvCgi/OvWebHelp.exe`)

2 Installation

Preparing for Installation

Before installing the Network Node Manager / Route Analytics Management System Integration Module (NNM/RAMS Integration Module), verify that your computer meets the hardware and software requirements, and that the prerequisite hardware and software has been set up properly.

NOTE

The NNM/RAMS Integration Module replaces the OSPF view created by the Advanced Routing SPI for NNM Advanced Edition. In its place, you get the RAMS IGP view, which is similar, but far more functional, as well as many other features.

RAMS Appliance Requirements

Before installing the NNM/RAMS Integration Module, you must have your RAMS appliance installed and functioning. Without that, you can not perform even the most basic tasks with this software.

You must have purchased (at a minimum) the "OSPF Smart Plug-in for Route Analytics Management System (RAMS)" product, and installed the associated license on the RAMS appliance. Other RAMS SPIs are optional; this Integration Module does not currently make use of the functionality they provide to RAMS.

For details, see the *RAMS Appliance Setup Guide* and *RAMS User's Guide*.

Software Requirements for the Integration Module

Supported Operating Systems

The following operating systems are supported:

- HP-UX 11.0 or HP-UX 11.11
- Solaris 2.8 or Solaris 2.9
- Microsoft Windows 2000 with Service Pack 3, Windows XP, or Windows 2003 Server.

If necessary, refer to the *Network Node Manager Quick Start Installation Guide* and *Managing Your Network with NNM* for instructions on how to install and deploy NNM Advanced Edition.

Determine Which Version of NNM AE is Installed

The NNM/RAMS Integration Module requires a compatible version of NNM AE. To find out which version is installed, proceed as follows:

UNIX: **`/opt/OV/bin/ovnnmversion`**

Windows: ***`install_dir`*`\bin\ovnnmversion`**

Verify that the version is 7.5 or above.

Verify the Configuration of NNM AE

After verifying that you have a supported version of NNM Advanced Edition, verify the Extended Topology features are enabled, and that the Advanced Problem Analyzer (APA) is enabled for your IP environment.

To see if APA is enabled, run the following command with Administrator (`root`) privileges:

UNIX: **`/opt/OV/bin/apaConfig.ovpl`**

Windows: ***`install_dir`*`\bin\apaConfig.ovpl`**

If APA has been enabled, the output of this command is as follows:

```
PollNormalIP true
StatusBridgeEnabled true
```

If you get any other results, refer to the *Using Extended Topology* manual for instructions on how to enable APA.

Set the NNM Environment Variables

The following command sets the NNM environment variables:

- *UNIX* (using `sh` or `ksh`): **`. /opt/OV/bin/ov.envvars.sh`**
- *UNIX* (using `csh`): **`source /opt/OV/bin/ov.envvars.csh`**
- *Windows*: ***`install_dir`*`\bin\ov.envvars.bat`**

This step sets environment variables required by the NNM/RAMS Integration Module.

Installing the NNM/RAMS Integration Module

IMPORTANT

Before you install the NNM/RAMS Integration Module, you must first enable the Extended Topology functionality and the Advanced Problem Analyzer (APA) of NNM Advanced Edition. See “Verify the Configuration of NNM AE” on page 15 for an overview.

For specific instructions, see the guide *Using Extended Topology* that was included with NNM Advanced Edition.

Installing on a UNIX® Operating System

To install the NNM/RAMS Integration Module on a UNIX® operating system, follow these steps:

1. Log on to the NNM management station as user `root`.
2. Verify that the NNM environment variables are sourced properly. For instructions, see “Set the NNM Environment Variables” on page 15.
3. Mount the product media.
4. From the CD-ROM top-level directory, execute `setup`.

   The installation script verifies that the target system has the correct version of NNM installed. If not, the installation script exits with an error. See page 14 for pre-installation information.

5. At the prompt, follow the menus to install the NNM/RAMS Integration Module. Table 2-1 lists the menus you will see, and the actions you will need to take during the installation process.

Table 2-1 UNIX Installation Options for the NNM/RAMS Integration Module

At this Menu:	Take this Action:
List of installable product types	Enter the number of the item named "`Install the NNM Value-add Components`" and press the `Enter` key.
List of installable components	Enter the number of the item named "`Install the NNM/RAMS Integration Module`" and press the `Enter` key.

Installing on a Windows Operating System

To install the NNM/RAMS Integration Module on a Windows operating system, follow these steps:

1. Log on to the NNM management station as `Administrator`.
2. Verify that the NNM environment variables are set. For instructions, see "Set the NNM Environment Variables" on page 15.
3. Insert the product media into the CD-ROM drive.
4. The CD-ROM should start automatically. If it does not, use Windows Explorer to go to the CD-ROM top-level directory, and double-click `setup.bat`.

   The installation script verifies that the target system has the correct version of NNM installed. If not, the installation script exits with an error. See page 14 for pre-installation information.
5. Follow the instructions on the screen to install the NNM/RAMS Integration Module. Table 2-2 lists the decisions you will be asked to make during the installation process.

Table 2-2 Windows Installation Options for the NNM/RAMS Integration Module

At this Menu:	Take this Action:
List of installable product types	Enter the number of the item named "`Install the NNM Value-add Components`" and press the `Enter` key.
List of installable components	Enter the number of the item named "`Install the NNM/RAMS Integration Module`" and press the `Enter` key.

Disabling the NNM/RAMS Integration Module

Disabling the NNM/RAMS Integration Module makes the following changes in NNM Advanced Edition:

- Removes the RAMS Path History view
- Removes the RAMS IGP view and restores the standard OSPF view
- Removes the RAMS tab from the NNM AE Extended Topology configuration utility
- Stops the event reduction that is performed on arriving RAMS events
- Stops the root cause analysis of RAMS events

After disabling the NNM/RAMS Integration Module, any RAMS events that come to NNM are delivered to the Status Alarms category, without root cause analysis.

Note that disabling the NNM/RAMS Integration Module does *not* remove the Route Analytics event category.

To disable the NNM/RAMS Integration Module, use Administrator (`root`) privileges to execute the following command:

UNIX: **`/opt/OV/support/NM/setupRAMS.ovpl -disable`**

Windows: ***`install_dir`*`\support\NM\setupRAMS.ovpl -disable`**

NOTE

Disabling the NNM/RAMS Integration Module does not actually remove the software. By running the above command with the **`-enable`** switch instead, you can re-enable the NNM/RAMS Integration Module.

To remove the NNM/RAMS Integration Module software entirely, execute **`setupRAMS.ovpl -uninstall`**.

3 Configuration

After installing the NNM/RAMS Integration Module, a few initial configuration steps are required. Some of these steps are done on the RAMS appliance, and others are done within NNM Advanced Edition.

Essential Configuration of the RAMS Appliance

This section gives high-level steps for performing the essential configuration of your RAMS appliance.

NOTE

This section explains only the steps that are required to permit full use of the NNM/RAMS Integration Module. It does not cover other features or functionality of the RAMS product.

You will want to familiarize yourself with all the features of the RAMS product, but they are not discussed here. See the *Route Analytics Management System User's Guide*.

Follow these steps to configure your RAMS appliance to work with the NNM RAMS Integration Module:

1. Launch your web browser, and load the RAMS Administration web-based interface (URL: `http://`*`appliance_name`*`/`, or `http://`*`appliance_IP_address`*`/`)
2. Click the `Administration` tab. When prompted, enter the Administrator's name ("`admin`") and password. The default password is also "`admin`", but this can and should be changed for obvious security reasons. (After logging in the first time, use the `Change Password` tab to set a new Administrator's password).
3. Click the `Queries` tab, and set the Queries password. Make a note of this password, as you will need it when configuring the Integration Module.
4. Click the `System` tab, and within that tab, click the `Time and Date` tab.

   If the time is not already set correctly, do so now. Either use an available NTP server, or set the time manually. Be sure to set the time zone correctly, using Standard (not Daylight) time.
5. Click the `Route Recorder Configuration` tab.
6. Click the `Networks` icon at the left, and from the pop-up menu, select `Add->Administrative Domain`.

An **Administrative Domain** is a collection or grouping of routers under common management. For best results, HP recommends that you create a single Administrative Domain for all OSPF protocol instances.

Type the name of your Administrative Domain in the space provided (e.g., `CorporateNet`). You will need to know this name during the configuration of the NNM RAMS Integration Module.

7. Click the new domain in the list, and from the pop-up menu, select `Add->OSPF Instance`.
8. The resulting dialog lets you create an OSPF Protocol Instance, which is a database to hold RAMS data. For simplicity, HP recommends that you create a single OSPF Protocol Instance for all OSPF areas you want to manage.

   The main body of this dialog lets you specify which interfaces or GRE tunnels will supply data to this Protocol Instance. (See the Tip below.)

   If you are following the above recommendation, you should add all available physical interfaces and GRE tunnels to the Active list. Otherwise, add only those that you want to belong to this Protocol Instance. Select items in the `Not Active` list, and use the left-arrow button to move items to the `Active` list.

TIP

A physical interface or GRE tunnel has—by virtue of the router it is connected to—an area associated with it. For example, if you plugged Slot 0/Port 1 into a Backbone router, the RAMS appliance would, as you expect, collect Backbone area data from that interface.

The physical interfaces of your RAMS appliance should be connected to different areas that you want to monitor. To reach additional or more distant areas, you can configure GRE tunnels.

If you need to configure GRE tunnels, or OSPF authentication, see the *RAMS User's Guide* for details.

9. Press the `Start Recording` button.

At this point, the RAMS appliance begins participating in the routing protocols. Over time, it discovers your routing topology and logs historical data about it for forensic analysis when troubleshooting.

Configuring the NNM RAMS Integration Module

After configuring the RAMS appliance as described in “Essential Configuration of the RAMS Appliance” on page 23, you can proceed with configuring the NNM RAMS Integration Module itself.

This section shows you how to set up communication between the NNM management station and the RAMS appliance. It also shows you how to configure the RAMS events for use in NNM.

All the tasks in this section are done using the Extended Topology web-based configuration utility of NNM Advanced Edition.

Configuring Communication between NNM and RAMS

To configure communications between NNM and the RAMS appliance, follow these steps:

1. Launch your web browser, and load the Extended Topology web-based configuration utility (URL: `http://<nnm_mgmt_station>:7510/topology/etconfig`)
2. Click the `RAMS` tab, and within that tab.
3. In the `RAMS IP/DNS Address` field, enter the hostname or IP address of your RAMS appliance.
4. In the `RAMS Query Password` field, enter the password you set in Step 3 on page 23.
5. In the `RAMS Database Name` field, enter the name of the Administrative Domain you set in Step 6 on page 23.
6. Select the `Preferred Protocol` to be used to resolve hostnames to IP addresses for Route Change event watch lists.
7. Press the `Apply` button to set the new configuration values on the RAMS appliance.

Configuring RAMS Events

After configuring communications between NNM and the RAMS appliance, you can enable any of several RAMS events. The following subset are used by the root-cause analysis engine in NNM:

Adjacency Lost	This event indicates that an adjacency is lost between two routers in the network. This event is normally used to monitor key adjacencies, like adjacencies between areas, adjacencies between a router and a server farm, and point-to-point links to remote areas on the backbone.
Route Change	This event indicates that the route between an explicitly configured source and destination has changed. This alert provides an early indication of service degradation or even of an outage.
Prefix Origination Change	This event is sent when a prefix has been withdrawn or is newly advertised. A prefix withdrawal indicates that services have been disrupted which could present a number of possible problems such as dropped packets, slowed service, etc.
Prefix Flap	This event indicates that a prefix is flapping, or being advertised by different routers in quick succession. This gives you an early indication of a service becoming unavailable.
BGP Lost Redundancy	This event indicates that a redundant link is lost, which can be an early indicator of a reduction in service level or higher cost for service. The event is issued when redundant prefixes are reduced to a single available next hop. The calculation uses a baseline derived from an average redundancy for a prefix sampled over the last 7 days.

BGP Route Flap	This event is issued when a route is repeatedly updated or withdrawn from the BGP table. The event provides an early indication of a critical service becoming unavailable or degrading in performance.
BGP Prefix Drought **BGP Prefix Flood**	These two events are received when a routing table size increases or decreases respectively by a significant amount relative to a baseline. The baseline is calculated based on an average sampled over a one week period (last 7 days). The event may indicate a router misconfiguration or a security breech has occurred.
Customer Reachability by PE	This event is issued when an interface which has an associated VRF table fails. An interface failure signifies that the customer's VPN connection is down on the provider edge router and the customer can no longer reach the VPN. Enable this event when you are integrating the RAMS mBGP SPI. (This event is configured in the Event Configuration sub-menu of VPN Explorer rather than the Alert Configuration menu.)

Refer to your *Route Analytics Management System User's Guide* for a complete listing of possible alerts to forward to NNM.

In general, configuring a RAMS event is a simple procedure:

1. Launch your web browser, and load the Extended Topology web-based configuration utility (URL: `http://<nnm_mgmt_station>:7510/topology/etconfig`)
2. Click the `RAMS` tab, and within that tab, click the `Rams Event Configuration` link to alert configuration on the RAMS system.
3. Refer to the *HP OpenView Route Analytics Management System User's Guide* chapter on Alerts for detailed configuration instructions..

4. If desired, or required, use the provided fields to register one or more entries in the Watch List for the event.

About Watch Lists

A Watch List is essentially a filter on an event, a way to ensure that the only events that get sent are those which meet the criteria of the Watch List. For performance reasons, you may want to limit your number of entries in a Watch List to 12. Some events require that you configure a Watch List (for example, Route Change). For all other events, a Watch List is optional (for example, Adjacency Lost). See Table 3-1 for details.

Table 3-1 Event Watch List Requirement

Event	Watch List
Adjacency Lost	Optional
Route Change	Required
Prefix Origination Change	Optional
Prefix Flap	Required

NOTE

When a Watch List is optional and is *not* set, *all events* of that type are sent. In other words, with no filter in place, all events pass. As soon as a Watch List is configured, however, RAMS sends only events that match the Watch List.

For example, if you do not configure a Watch List for the Adjacency Lost event, then all Adjacency Lost events are sent to NNM. However, if you configure one entry in the Watch List for the Adjacency Lost event, then NNM will get alarms for only that adjacency. Therefore, you should either configure the Watch List to specify all the adjacencies of interest, or configure no Watch List at all.

There are two kinds of Watch Lists:

Node-based — A node-based Watch List filters the events based on specific nodes. For example, the Adjacency Lost event uses a node-based Watch List to specify which routers have an adjacency of interest. For Route Change

events, you can configure the Watch List using hostnames or IP addresses. All other Watch Lists are configured using IP addresses.

Network-based — A network-based Watch List filters the events based on prefixes (or networks) and masks. For example the Prefix Origination Change event uses a network-based Watch List. What triggers the event is a change in the prefix advertisement, which is not specific to a router.

About the Watch List Operation of the Adjacency Lost Event The Watch List for the Adjacency Lost event includes an Operation field. This sets conditions for when the event is issued, as follows:

Table 3-2 Operation in Watch List

Operation	Meaning
`and`	The `and` operation indicates that an event should be sent when the adjacency from the Source router to the Destination router is lost. You must specify both the Source and Destination.
`or`	The `or` operation provides a compact way to specify multiple adjacencies of interest. It indicates that an event should be sent if either of the following occurs: • An outbound adjacency from the specified Source router to any other router is lost. • An inbound adjacency from any router to the specified Destination router is lost. You must specify both Source and Destination. You can use the same router in both fields, to watch all adjacencies involving that router.
`none`	The `none` operation is exactly like the `or` operation, except that it requires you to specify either the Source or Destination, but *not both*. Use the `none` operation like the `or` operation, but in those cases where you want to monitor a limited set of adjacencies (inbound or outbound) on one router.

4 RAMS Alarms

About RAMS Alarms

If you configured RAMS events as described in "Configuring RAMS Events" on page 26, several changes are made in NNM to respond to these new events:

- A new `Route Analytics Alarms` category is added to the Alarm Browser tab of Home Base.

  RAMS alarms appear in the Route Analytics category with APA alarms correlated under them.

- The Advanced Problem Analyzer of NNM Advanced Edition begins to perform root-cause analysis on incoming RAMS events to find the root cause of the RAMS alarm.

  If NNM determines the root cause of a RAMS alarm the APA alarm appears in the Status alarm category.

In addition, the RAMS administrator can configure additional RAMS events. These may be correlated, as described above, or given other event-reduction treatment to reduce clutter in the alarms browsers.

NOTE See "Correlation Composer Correlators for RAMS" on page 35 for detailed information on the correlation and event reduction that NNM applies to incoming RAMS events.

You can view a RAMS alarm in the Route Analytics category, where it is correlated to a root cause.

A RAMS alarm has several fields that can help you analyze it and troubleshoot a problem. Table 4-1 on page 33 lists the fields available for each RAMS alarm.

Table 4-1 Reading the Key RAMS alarms

Alarm Field	Alarm			
	Adjacency Lost	**Route Flap**	**Prefix Origination Change**	**Prefix Flap**
1	Source IP address	Source IP address	Prefix network address	
2	Source Node type[1]	Destination IP address	Prefix subnet mask	
3	Destination IP address	Time stamp[2]	Router that is now the originator of this prefix	Time stamp[2]
4	Destination Node type[1]	-	Time stamp[2]	-
5	Time stamp[2]	-	-	-

1. A value of zero (0) means “Router”; a value of one (1) means “Pseudonode”. A pseudonode, as defined by the IS-IS protocol, is a virtual node that models multiaccess links.
2. Useful to distinguish closely spaced similar alarms (milliseconds from epoch)

Other RAMS Alarms

In addition to the above, several other events may be enabled by the RAMS administrator. These would also appear in the NNM Alarms Browser, with formats and fields similar to the key alarms already described:

- `Adjacency Established`: all fields are identical to `Adjacency Lost` alarm

- `Adjacency Flap`: all fields are identical to `Adjacency Lost` alarm
- `Prefix Change`: all fields are identical to `Prefix Origination Change` alarm
- `Routing Event`: RAMS software version; time stamp; alarm severity according to RAMS appliance
- `Excess Net Churn`: Current churn number; time stamp
- `Peering Change`: IP address of the peering neighbor; time stamp
- `Duplicate Interface IP`: The duplicate IP address; time stamp
- `BGP Prefix Drought`: Peer IP address ; time period in days used for baselining; baseline RIB size (number of peer routes which are in baseline); current RIB Size; percent change in size of Current Peer RIB from Baseline Peer RIB
- `BGP Prefix Flood`: Peer IP address; time period in days used for baselining; baseline RIB size (number of peer routes which are in baseline); current RIB size; percent change in size of current peer RIB from baseline peer RIB
- `BGP Route Flap` Prefix IP; prefix mask ; peer IP address; peer AS number; next hop IP; next hop AS; route status (such as Withdrawn or Announced)
- `BGP Lost Redundancy` Prefix IP; prefix mask; route source AS; baseline number of next hops; current number of next hops
- `Customer Reachability by PE` The first two fields are unused. The third field contains the trap severity; the fourth contains the Route Target or customer; the fifth contains the associated PE router

To learn more about these RAMS events, see the *HP OpenView Route Analytics Management System User's Guide*

Correlation Composer Correlators for RAMS

The following section provides an explanation of the correlators that function when you enable the NNM/RAMS Integration Module. These correlators are defined using HP OpenView Correlation Composer. For further information on correlators and NNM, see *Managing Your Network with NNM*.

RAMS Built-In Correlators

The RAMS-enabled correlators are contained within three namespaces:

- The `OV_RAMS` namespace contains a set of correlators that listen for RAMS events and perform additional processing on the events before releasing them to the NNM alarm browser. Since the incoming RAMS events are protocol-independent, the correlators operate across all supported protocols.
- The `OV_RAMS_BGP` namespace correlators process BGP events from the RAMS appliance.
- The `OV_RAMS_2547` namespace correlators process multicast protocol 2547 events from the RAMS appliance. The `OV_RAMS_2547` (MPLS BGP) namespace contains two correlators that work in concert. Both must be enabled or both must be disabled. Only the second of the two correlators, OVRAMS_POLL_VPN_2 is modifiable.

The RAMS correlators perform several main functions:

- "Trigger APA Polling" on page 36

  (A set of two correlators) When a RAMS `Adjacency Lost` or `Route Change` event is received, a new, enhanced alarm is generated containing the corresponding router IP address. The new (LOG-ONLY) alarm causes APA to begin analysis on the specified router IP address.

- "Reduce Repeated RAMS Routing and Prefix Events" on page 37

  (a set of six correlators) Listens for repeated events, including `Prefix Flap`, `Prefix Change`, `Prefix Origination Change` and `Routing` events. The first event of its kind is forwarded to the alarm browser. Subsequent events received within a specified time window are correlated under the first event.

- "Correlate APA Events under RAMS Alarms" on page 38

  (a set of five correlators) Listens for several RAMS events, and for APA alarms. When one of the supported RAMS events arrive, the correlators store information from the event in a queue for two minutes for further analysis. When an APA alarm is received, the correlators compare its information to the information in the queue. When information from a RAMS event matches the information of an APA alarm, the APA event is nested under the RAMS alarm in the Route Analytics Alarm Browser. The APA alarm also shows in the Status Alarm Browser.

  The RAMS events that can be correlated with APA events are as follows:

  — `Route Change` event

  — All "`Adjacency` ..." events

  — All "`Prefix` ..." events

- "Correlate BGP Events to APA Root Cause Alarms" on page 40

  (a set of three correlators) Listens for several RAMS BGP events, and for APA alarms. When one of the supported RAMS events arrive, the correlators store information from the event in a queue for two minutes for further analysis. When an APA alarm is received, the correlators compare its information to the information in the queue. When information from a RAMS event matches the information of an APA alarm, the APA event is nested under the RAMS alarm in the Route Analytics Alarm Browser. The APA alarm also shows in the Status Alarm Browser.

  The RAMS events that can be correlated with APA events are as follows:

  — BGP events

- "Cleanup Correlation Composer Queue" on page 43

  This correlator is an internal utility that prevents the Correlation Composer queue from growing too large. The queue is erased after a threshold is reached (default: 50 alarms).

Trigger APA Polling

Triggers an immediate APA poll on a router that is the root cause of an `Adjacency Lost` or `Route Change` event.

Behavior APA is configured to receive certain events immediately, but other events and messages require further processing before a poll is requested. The `OV_RAMS_TRIGGER_POLL_ADJ_LOST` and `OV_RAMS_TRIGGER_POLL_ROUTE_CHANGE` correlators perform this additional processing and generate the appropriate poll trigger request for certain RAMS events.

When a RAMS `Adjacency Lost` or `Route Change` event is received, the `OV_RAMS_TRIGGER_POLL_ADJ_LOST` and `OV_RAMS_TRIGGER_POLL_ROUTE_CHANGE` correlators generate a new event containing the corresponding router IP address that causes APA to begin analysis on the specified router IP address.

Configurable Parameters No parameters for either correlator are configurable.

Reduce Repeated RAMS Routing and Prefix Events

Correlates RAMS `Route Change`, `Prefix Change`, `Prefix Flap`, and `Prefix Origination Change` events under the first event of its kind.

Behavior Certain RAMS events can occur in large numbers, such as `Routing` and `Prefix Origination Change` events. For example, multiple routers may send out `Prefix Origination Change` events for the same prefix (indicating another router will be forwarding packets to the prefix). These correlators detect a repetitive situation and nest the repeated alarms under the first alarm of its kind.

In particular, the following seven correlators detect repetitive routing and prefix events by determining if the events originated from the same router or are for the same prefix.

- The `OV_RAMS_ROUTING_REDUCE` correlator nests RAMS `Routing` events that originate from the same router and are received within a specified time window (default: 1 hour).
- The `OV_RAMS_FLAP_REDUCE` correlator nests RAMS `Prefix Flap` events that are from the same prefix and are received with a specified time window (default: 5 minutes).
- The `OV_RAMS_ADJ_REDUCE` correlator nests RAMS `Adjacency Lost` events that are from the same source IP address and are received with a specified time window (default: 5 minutes).

- The `OV_RAMS_PREFIX_REDUCE` correlator nests RAMS `Prefix` ... events that originate from the same router and are received with a specified time window (default: 5 minutes).
- The `OV_RAMS_PREFIX_REDUCE_PREFIX` correlator nests RAMS `Prefix` ... events that are for the same prefix and are received with a specified time window (default: 5 minutes).
- The `OV_RAMS_CHANGE_REDUCE` correlator nests RAMS `Prefix Origination Change` events that originate from the same router and are received with a specified time window (default, five minutes).
- The `OV_RAMS_CHANGE_REDUCE_PREFIX` correlator nests RAMS Prefix Origination Change events that are for the same prefix and are received with a specified time window (default: 5 minutes).

If a RAMS `Route Change`, `Prefix Change`, `Prefix Flap`, or `Prefix Origination Change` event arrives and no other events have previously been seen of this type (and for the same prefix, if it is a prefix event), a new interval is started. Moreover, this event is posted in the Route Analytics Alarms Browser.

All subsequent RAMS `Route Change`, `Prefix Change`, `Prefix Flap`, or `Prefix Origination Change` events of the same type (and for the same prefix, if it is a prefix event), received within the specified time window are nested under the first alarm.

The suppressed RAMS alarms can be viewed from the Route Analytics Alarms Browser by selecting a RAMS alarm and selecting `Actions:Show Details`.

After the interval expires, the process begins again.

Configurable Parameters The only configurable parameter is:

- Window Period

For instructions on how to modify this parameter, see “Setting Parameters” on page 43.

Correlate APA Events under RAMS Alarms

Correlates the APA root cause alarm under the RAMS alarm.

Behavior It is desirable to see the root cause APA alarm in the alarm browser related to the RAMS alarms. These correlators help achieve that.

- The `OV_RAMS_QUEUE_ROUTE` correlator listens for RAMS `Route Change` events and stores the event information in a queue.
- The `OV_RAMS_QUEUE_ADJ` correlator listens for RAMS `Adjacency Lost`, `Adjacency Flap`, or `Adjacency Established` events and stores the event information in a queue.
- The `OV_RAMS_QUEUE_PREFIX` correlator listens for RAMS `Prefix` ... events and stores the event information in a queue. This correlator is disabled by default because the number of these types of events can be large. For more information about the queue, see “Cleanup Correlation Composer Queue” on page 43.
- The `OV_RAMS_APA_1` correlator listens for APA alarms with one endpoint, such as an APA `Node Down` alarm.
- The `OV_RAMS_APA_2` correlator listens for APA alarms with two endpoints, such as an APA `Connection Down` alarm.

The correlators perform two functions. First, the correlators listen for RAMS events and store the UUID, router address, and subnet mask values in a queue.

Second, the correlators correlate RAMS events with the appropriate APA root cause alarm. When an APA alarm is received, its information is compared to the RAMS events that have been received. If they match, the RAMS event is correlated with the APA alarm in the NNM alarm browser.

Either the APA event or the RAMS events may arrive first, and in any order. Events within a specified time window are evaluated to determine if the APA alarm is the root cause of the RAMS event.

The following steps demonstrate in more detail how the correlators function.

1. The RAMS appliance forwards a RAMS event to the NNM management station.

2. The UUID, router address, and subnet mask values are extracted from the RAMS alarm, given the alarm is a `Route Change`, an `Adjacency Lost`, `Adjacency Flap`, an `Adjacency Established`, a `Prefix Change`, a `Prefix Origination Change`, or a `Prefix Flap` alarm.
3. The UUID, router address, and subnet mask values are held in a queue for two minutes.
4. The RAMS alarm is posted to the Route Analytics Alarms category in the NNM alarm browser.
5. Either before or after a RAMS event arrives, a root cause alarm is generated by APA and posted to the Status Alarms category of the NNM alarm browser.
6. The UUID, router address, and subnet mask values of the APA alarm are stored in a queue.
7. The UUID, router address, and subnet mask values of the APA alarm are compared to the UUID, router address, and subnet mask values of the RAMS events stored in a queue.
8. The matching APA alarm is nested under the RAMS alarm in the Route Analytics Alarm Browser.

The correlated root cause APA alarm can be viewed from the Route Analytics Alarms Browser by looking at correlated events for the RAMS alarm.

Configurable Parameters No parameters for these correlators are configurable.

Correlate BGP Events to APA Root Cause Alarms

Correlates the APA root cause alarm under the RAMS BGP alarm. In these events RAMS identifies its BGP peer that is experiencing the flood (or drought). The flood or drought may be due to the BGP peer losing connectivity with its peer. For example, RAMS is connected to BGP1 and BGP1 is connected to BGP2. If connectivity is lost between BGP1 and BGP2, BGP1 would experience a drought, conversely when the connectivity is re-established, it would cause a flood on BGP1.

Behavior It is desirable to see the root cause APA alarm in the alarm browser related to the RAMS BGP alarms. These correlators help achieve that.

- The `OV_RAMS_QUEUE_BGP_DROUGHT` correlator listens for RAMS `BGP Prefix Flood` and `BGP Prefix Drought` events and stores the event information in a queue for correlation with APA events.
- The `OV_RAMS_QUEUE_BGP_FLAP` correlator listens for RAMS `BGP Route Flap` events and stores them in a queue for correlation with APA events.
- The `OV_RAMS_QUEUE_BGP_LOST` correlator listens for RAMS `BGP Lost Redundancy` events and stores them in a queue for correlation with APA events.
- The `OV_RAMS_APA_1` correlator listens for APA alarms with one endpoint, such as an APA `Node Down` alarm.
- The `OV_RAMS_APA_2` correlator listens for APA alarms with two endpoints, such as an APA `Connection Down` alarm.

The correlators perform two functions. First, the correlators listen for RAMS events and store the UUID, router address, and subnet mask values in a queue.

Second, the correlators correlate RAMS events with the appropriate APA root cause alarm. When an APA alarm is received, its information is compared to the RAMS events that have been received. If they match, the RAMS event is correlated with the APA alarm in the NNM alarm browser.

Either the APA event or the RAMS events may arrive first, and in any order. Events within a specified time window are evaluated to determine if the APA alarm is the root cause of the RAMS event.

The following steps demonstrate in more detail how the correlators function.

1. The RAMS appliance forwards a RAMS event to the NNM management station.
2. The UUID, router address, and subnet mask values are extracted from the RAMS alarm.
3. The UUID, router address, and subnet mask values are held in a queue for two minutes.
4. The RAMS alarm is posted to the Route Analytics Alarms category in the NNM alarm browser.

5. Either before or after a RAMS event arrives, a root cause alarm is generated by APA and posted to the Status Alarms category of the NNM alarm browser.
6. The UUID, router address, and subnet mask values of the APA alarm are stored in a queue.
7. The UUID, router address, and subnet mask values of the APA alarm are compared to the UUID, router address, and subnet mask values of the RAMS events stored in a queue.
8. Get the Extended Topology database OID of the BGP IP address. Compare the BGP OID to the Extended Topology database OID of the APA source node. If they match, correlate them.
9. Compare the BGP OID to the APA destination node OID. If they match, correlate them.
10. Find the Layer 3 neighbors of the BGP node. If a Layer 3 neighbor database OID matches the APA source node database OID or the APA destination node database OID, then correlatethem.
11. Find the Layer 2 neighbors of the BGP node. If a Layer 2 neighbor OID matches the APA source node OID or the APA destination node OID, then correlate them.
12. Get the Layer 2 interface on the neighbor node. If the neighbor interface OID matches the APA source interface OID or the APA destination interface OID, then correlate them.
13. The matching APA alarm is nested under the RAMS alarm in the Route Analytics Alarm Browser.

The correlated root cause APA alarm can be viewed from the Route Analytics Alarms Browser by looking at correlated events for the RAMS alarm.

Configurable Parameters No parameters for these correlators are configurable.

Trigger APA Polling for MPLS BGP Events

Triggers an APA Poll of the MPLS PE Router when a VPN loss event is received. this event is defined as the Customer reachability by PE event in VPN Explorer. This is a 2 part correlator.

Behavior When certain events are received from a network device, an APA poll and analysis should be scheduled immediately instead of waiting until the next poll cycle. APA is configured to receive certain traps immediately, but other events require further processing before a poll is requested. The following correlators perform this additional processing and generate the appropriate poll trigger request.

- OVRAMS_POLL_VPN_LOST_1: When a customer VPN loss trap is received from the RAMS appliance, pass through the original trap and send a new trap to signify an APA poll should be initiated for this device. No parameters of this correlator are configurable.
- OVRAMS_POLL_VPN_LOST_2: This correlator listens for traps sent from OVRAMS_POLL_VPN_LOST_1. If multiple events arrive with in a 30 second (default) time period and the events are for the same device (PE), only one APA poll is initiated.

Configurable Parameters The only user-modifiable parameter is the time window, which defaults to 30 seconds.

Cleanup Correlation Composer Queue

The OV_RAMS_CLEANUP and OV_RAMS_CLEANUP2 correlators are internal utility correlators that prevent the queue from growing too large.

Behavior The RAMS correlators use a queue to store the UUID, router address, and subnet mask values from RAMS events. To prevent the queue from growing too large, the queue has a threshold of 50 event entries. Once the threshold is reached, the queue is erased.

Configurable Parameters No parameters for this correlator are configurable.

Setting Parameters

Complete the following steps if you want to review parameter definitions or modify parameters contained within a Correlation Composer correlator.

TIP There are several ways to access the event correlation features. For more information, from any view, select `Tools:HP OpenView Launcher`. Select the `[?]` (Help) tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any view, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, select the `'default'` stream. Then, highlight `Composer` in the correlation table and select `Modify`. The `Correlation Composer` window appears in your web browser.
4. In the `Correlation Composer` window, select the `OV_RAMS` namespace from the NameSpace table. Its correlators are displayed in the Correlator Store.
5. Double-click the correlator to display the `Description` tab.
6. Carefully read the information in the `Description` tab.

   The configurable parameters are listed in the `Description` tab.
7. Click the `Definition` tab to access the configurable parameter setting. Click `[Help]` for information about each field.
8. After making the desired change, click `[OK]` and close the correlator configuration window and return to the `Correlation Composer` main window.
9. Save your change by clicking `File:Save`. This updates the correlator fact store file associated with the namespace.
10. To activate your change, click `File:Close` and then click `Correlations:Deploy`.
11. Exit the `Correlation Composer` main window.

Correlator Fact Store File

The RAMS fact store file, `RAMS.fs`, is located in the following directory:

UNIX: `$OV_CONF/ecs/CIB/`

Windows: *`install_dir`*`\ecs\CIB\`

If you are planning to make experimental changes to the correlator parameter settings, you may wish to make a backup of the fact store file before proceeding.

Troubleshooting Information

For troubleshooting information about the HP OpenView Correlation Composer or the NNM correlators, see the following references:

- Access the following PDF format manuals from the NNM main window, select `Help:Documentation:`
  - — *HP OpenView Correlation Composer's Guide*
  - — *Managing Your Network with NNM*

Index

Index