HP OpenView Network Node Manager

Syslog Integration White Paper

Version: 7.0

HP-UX, Solaris

Manufacturing Part Number: None

October 2003

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.

Windows® is a U.S. registered trademark of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

5. Troubleshooting Tips

1 Introduction to the Syslog Integration Functionality

Introducing Syslog Integration Functionality

The Syslog Integration functionality provided with HP OpenView Network Node Manager (NNM) enables the management of network equipment from syslog messages. Certain types of network equipment do not have SNMP traps nor supporting MIBs for all error and warning conditions. For operators who require managing these conditions, the Syslog Integration functionality provides the ability to map syslog messages into SNMP traps for presentation or analysis.

NNM includes out-of-the-box conditions for which syslog messages are mapped to SNMP traps. You can add new conditions through the NNM Syslog Trap Mapping Configuration interface or the HP OpenView Operations message source template configuration windows, depending on your deployment mode.

Syslog Integration works with both NNM Starter Edition and NNM Advanced Edition. Syslog Integration also works with HP OpenView Operations with NNM. Syslog Integration must be configured on an NNM management station running an UNIX® operating system. See the *Release Notes* for supported software versions.

Syslog Integration Deployment Options

There are two deployment options available to you when using the Syslog Integration functionality.

- NNM standalone option
- OpenView Operations (OVO) with NNM option

NNM Standalone Configuration

The NNM standalone configuration consists of deploying an HP OpenView Operations (OVO) agent on the NNM management station. In short, the embedded OVO agent uses preconfigured templates to parse incoming syslog messages matching a certain pattern. The matched syslog messages are mapped to SNMP traps and forwarded to NNM to be displayed in the NNM alarm browser. See Figure 1-1 on page 8 for an illustration.

In this approach, the following components comprise the heart of the architecture:

- The embedded OVO agent

  When Syslog Integration is configured, an OVO agent is installed on the NNM management station. Part of the embedded OVO agent is the logfile encapsulator that is responsible for listening for syslog events from logfiles. The logfile encapsulator filters and formats syslog events according to information in configured templates. The logfile encapsulator then forwards relevant information in the form of messages to an NNM background process, `syslogTrap`, which maps the syslog messages into SNMP traps.

- The NNM management station

  When Syslog Integration is configured, the NNM management station receives formatted syslog messages from the embedded OVO agent. `syslogTrap`, a background process on the NNM management station, maps the syslog messages to OpenView SNMP traps. This process registers with the OVO agent at the message stream interface and filters all messages of message type `NNMsyslog_`.

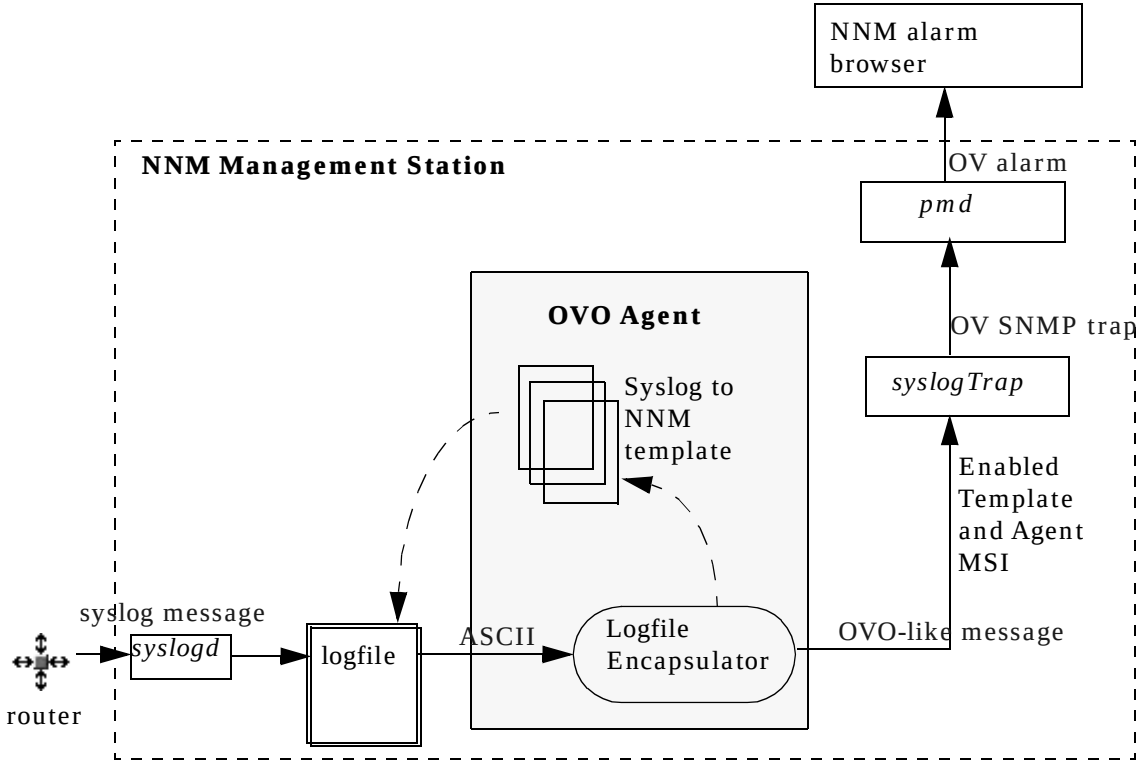
The SNMP traps are then sent to the NNM postmaster process, `pmd`, where the traps can participate in correlation or analysis. For example, the NNM Smart Plug-in for Frame Relay provides advanced correlators for frame relay traps and syslog messages. `pmd` forwards the formatted syslog messages to the NNM alarm browser.

- NNM alarm browser

  Processed syslog messages are displayed in the Status Alarm category of the NNM alarm browser.

Figure 1-1 shows the flow of events for the NNM standalone configuration. This illustration assumes that the router has been configured to forward syslog events to the NNM management station.

Figure 1-1 Flow of Events for NNM Standalone Configuration



To modify the `Syslog to NNM` template, use the NNM Syslog Trap Mapping Configuration Interface as described on page 11.

OpenView Operations with NNM Configuration

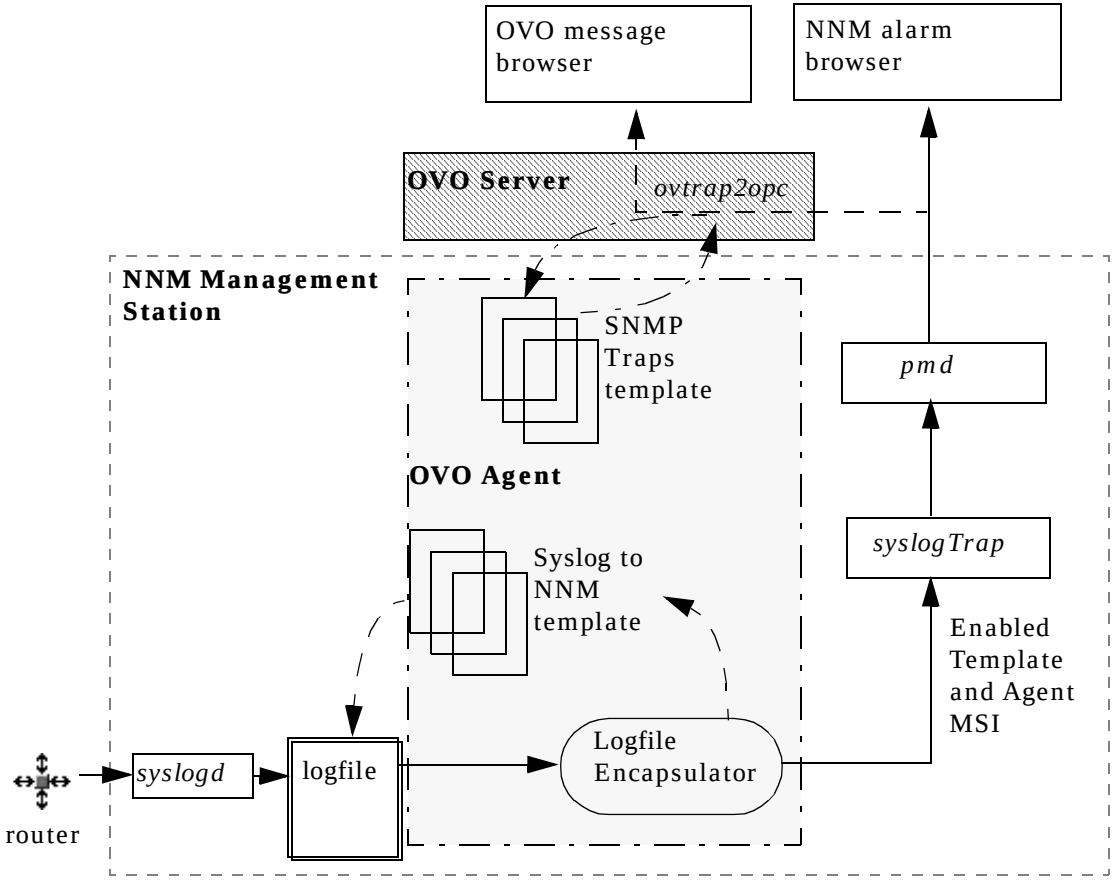
The OVO with NNM configuration option consists of deploying HP OpenView Operations with Network Node Manager. In this approach, you install an OVO agent on the NNM management station from the OVO server and use the OVO tools to configure the OVO agent to process syslog events.

This approach is similar to the NNM standalone configuration option. The architectural differences between the two deployment options are:

- The OVO agent is not embedded on the NNM management station; rather the OVO agent coexists with the NNM management station.
- The OVO server is used to start and configure the OVO agent on the NNM management station to process syslog messages. As an OVO administrator, you use the OVO configuration tools to upload the syslog message source templates to the OVO agent and synchronize the OVO message source templates with NNM `trapd.conf`.
- NNM forwards the SNMP traps to either (or both) the OVO message browser or the NNM alarm browser, depending on how messages are configured to be diverted through the system. The configuration instructions provided in “Sending Syslog Messages to OVO Message Browser” on page 24 show you how to forward syslog messages to the OVO message browser.

Figure 1-2 on page 10 shows the flow of events for the OVO with NNM configuration. This illustration assumes that the router has been configured to forward syslog events to the NNM management station.

Figure 1-2 Flow of Events for OVO with NNM Configuration



To construct and modify the `Syslog to NNM` message source template, use the standard OVO template editor. To launch the OVO template editor, see “OVO Message Source Templates Window” on page 11.

Configuration Tools

This section describes the tools needed to configure the NNM Syslog Integration functionality. The tools and steps required differ depending on your deployment option.

NNM Syslog Trap Mapping Configuration Interface

When you deploy the NNM standalone configuration option, you construct and modify the Syslog Integration message source template conditions through the Syslog Trap Mapping Configuration interface.

To launch the Syslog Trap Mapping Configuration interface, execute:

```
$OV_BIN/ovsyslogcfg
```

For instructions on how to use the Syslog Trap Mapping Configuration interface, see the *Syslog Trap Mapping Configuration Online Help*.

OVO Message Source Templates Window

When you deploy the OVO with NNM configuration option, you construct and modify Syslog Integration message source template conditions through the Message Source Templates configuration window.

To open the Message Source Templates configuration window, launch the OVO administrator interface (`$OV_BIN/OpC/opc`) and then click `Window:Message Source Templates`.

For instructions on how to use the Message Source Templates configuration window, see the *OVO Administrator Online Help*.

Syslog Configuration Command

The Syslog Integration functionality is not enabled when NNM is installed. To enable and deploy a syslog configuration, use the command line script, `setupSyslog.ovpl`.

Use the `-help` option to display a help message for the `setupSyslog.ovpl` command options.

In the NNM Standalone Deployment Mode

When the NNM standalone configuration option is deployed, execute the syslog configuration command with the `-standalone` option by typing: `setupSyslog.ovpl -standalone`

This command does the following on your NNM management station:

- Deploys the out-of-the-box syslog template, `Syslog to NNM`.
- Activates the embedded OVO agent.
- Activates and registers the SNMP mapping background process, `syslogTrap`.

For detailed configuration steps, see "Configuring Syslog Integration for NNM Standalone" on page 18.

The `setupSyslog.ovpl` configuration command is also used to deploy new syslog configurations. After editing syslog message source template conditions with the Syslog Trap Mapping Configuration interface, execute `setupSyslog.ovpl -standalone -deploy` to deploy the new configuration. The `-deploy` command option generates and encrypts the new template and restarts the embedded OVO agent so that the new template is reloaded.

In the OVO with NNM Deployment Mode

When the OVO with NNM configuration option is deployed, execute the syslog configuration command with the `-server` option by typing: `setupSyslog.ovpl -server`

This command create an uploadable template configuration directory for the out-of-the-box syslog template, `Syslog to NNM`.

After executing this command, other configuration steps you must perform include the following:

- Upload the `Syslog to NNM` template into the OVO database.
- Start and register the NNM mapping process, `syslogTrap`.
- Enable the template MSI and the OVO agent MSI.
- Assign and install the `Syslog to NNM` template to the OVO agent installed on the NNM management station.

For detailed configuration steps, see "Configuring Syslog Integration for OVO with NNM" on page 21.

Default Syslog Trap Mappings

NNM includes out-of-the-box template conditions for which syslog messages are mapped to OpenView SNMP traps. Each type of syslog message to be mapped is defined in one template condition. The conditions are contained in the `Syslog to NNM` template.

New OpenView traps are defined to support the out-of-the-box syslog message mappings. The list of mapped traps is described in Table 1-1.

Table 1-1 Syslog Trap Mappings

Syslog Message	OpenView Event Generated
%LINK-3-UPDOWN (down)	OV_Syslog_LinkDown
%LINK-3-UPDOWN (up)	OV_Syslog_LinkUp
%LINEPROTO-5-UPDOWN (down)	OV_Syslog_LineProtoDown
%LINEPROTO-5-UPDOWN (up)	OV_Syslog_LineProtoUp
%FR-5-DLCICHANGE (INVALID)	OV_Syslog_FrameDLCI_Inactive
%FR-5-DLCICHANGE (INACTIVE)	OV_Syslog_FrameDLCI_Inactive
%FR-5-DLCICHANGE (ACTIVE)	OV_Syslog_FrameDLCI_Active
%OSPF-5-ADJCHG (DOWN)	OV_Syslog_OSPF_Neighbor_Down
%OSPF-5-ADJCHG (FULL)	OV_Syslog_OSPF_Neighbor_Up

2 Syslog Configuration

This chapter provides the steps necessary to setup the Syslog Integration functionality in either deployment mode.

Prerequisites for Configuring Syslog

DCE Software Requirements for Syslog

NOTE Installation of DCE software prerequisites are required only for HP-UX operating systems. On Solaris operating systems, the install process automatically installs HP's lightweight DCE if a supported DCE is not found.

Part of the syslog configuration process includes installing an HP OpenView Operations (OVO) agent on the NNM management station. The OVO agent requires two pieces of software to be installed prior to configuring syslog: DCE RPC and DCE-KT-Tools. See the *Release Notes* for more information about supported software versions.

The required DCE software is available on the HP-UX Application Software CD-ROMs. To install the required DCE software, do the following:

1. Invoke the `SD Install` interface by typing: `swinstall`
2. Change the software view by clicking: `View:Change Software View->Start with Products`.
3. Install the first DCE software package by selecting `DCE-Core.DCE-CORE-RUN` and clicking `Actions:Install`.
4. Install the remaining DCE software package by selecting: `DCE-KT-Tools` and clicking `Actions:Install`.

To check whether you have properly installed the required DCE software, do the following:

1. Type: `swlist | grep DCE`
2. Look for two items in the list:
   - DCE/9000 Programming and Administration Tools
   - DCE/9000 Kernel Threads Support

Syslog Requirement in an NIS Environment

NOTE This step is required only for OVO with NNM configuration deployments.

If the NNM management station being used for syslog monitoring is a Network Information Service (NIS or NIS+) client, you need to install the default OVO user, opc_op, and user group, opcgrp, on the NIS server.

If the default OVO user, opc_op, and user group, opcgrp, are not installed on the NIS server, or at least installed locally on the managed node, you may get errors when installing agents and agent software on the managed node.

To add opc_op locally on the managed node, edit the /etc/passwd file to include an entry for opc_op. For example, the entry in the /etc/passwd file could read:

```
opc_op:*:777:299:OpC default operator:/home/opc_op:/usr/bin/ksh
```

Configuring Syslog Integration for NNM Standalone

NOTE DCE software requirements must be installed before configuring the Syslog Integration functionality. See "DCE Software Requirements for Syslog" on page 16.

The Syslog Integration functionality is not enabled when NNM is installed. To enable and deploy a syslog configuration, use the command line script, `setupSyslog.ovpl`.

NOTE When you execute the `ovstatus` command, a background process called `syslogTrap` is listed. Before enabling the Syslog Integration functionality, this process displays as NOT RUNNING. Do not attempt to start this process before enabling the Syslog Integration functionality.

To enable Syslog Integration for NNM standalone configurations, execute the following command on the NNM management server:
`setupSyslog.ovpl -standalone`

This command does the following on your NNM management station:

- Deploys the out-of-the-box syslog template, `Syslog to NNM`.
- Installs and activates the embedded OVO agent.
- Activates and registers the SNMP mapping process, `syslogTrap`.

NOTE On Solaris operating systems, you need to change the default location of the system logfile from `/var/adm/syslog` to `/var/adm/messages` by doing the following:

1. Start the Syslog Trap Mapping Configuration interface by executing:
   `$OV_BIN/ovsyslogcfg`
2. In the Logfile text entry box, enter: `/var/adm/messages`

3. Click **[Save]**.
4. Close the Syslog Trap Mapping Configuration window.

To customize the out-of-the-box syslog template, see "Modifying the Syslog to NNM Template" on page 19. For information about verifying your syslog configuration, see "Testing Syslog Integration" on page 19.

Modifying the Syslog to NNM Template

For customizations to the `Syslog to NNM` template, use the Syslog Trap Mapping Configuration interface. To launch the Syslog Trap Mapping Configuration interface, execute:

```
$OV_BIN/ovsyslogcfg
```

For instructions on how to use the Syslog Trap Mapping Configuration interface, see the *Syslog Trap Mapping Configuration Online Help* and "NNM Syslog Trap Mapping Configuration Interface" on page 30.

For more information about the `Syslog to NNM` template and its conditions, see "Understanding the Syslog to NNM Template" on page 33.

Testing Syslog Integration

Use the UNIX command line tool, `logger`, to write test messages to the system logfile. Read its man page for more information on how to use the command.

For example, to create a *Line Protocol status Down* syslog entry, do the following:

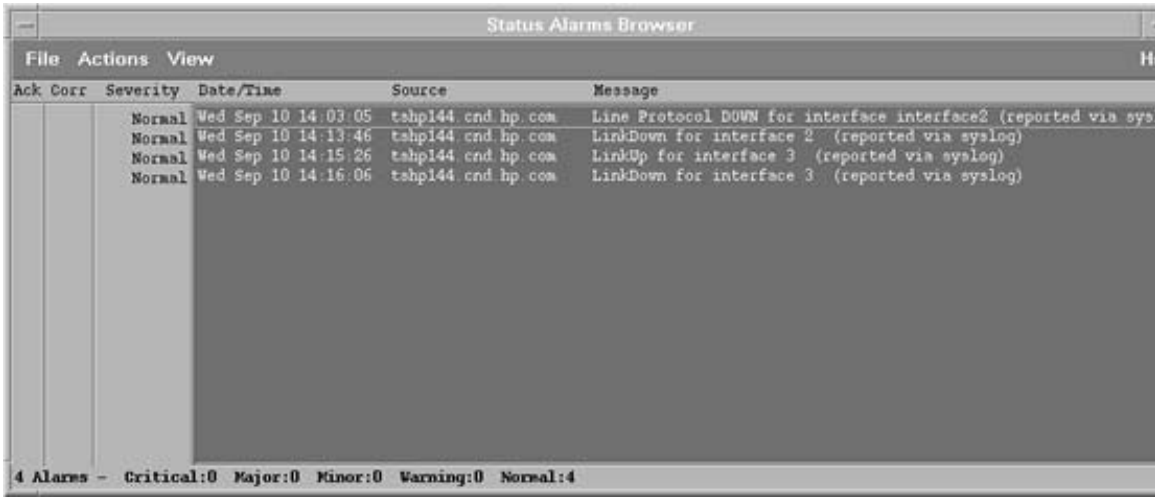
HP-UX: `logger %LINEPROTO-5-UPDOWN: Line protocol on Interface interface2, changed state to down`

Solaris: `logger -p user.err %LINEPROTO-5-UPDOWN: Line protocol on Interface interface2, changed state to down`

NOTE On Solaris operating systems, you need to change the default location of the system logfile that the `Syslog to NNM` template is monitoring. See the Note on page 18 for instructions.

When Syslog Integration is enabled, you should see syslog messages matching the conditions of the `Syslog to NNM` template forwarded to the NNM alarm browser, as shown in Figure 2-1.

Figure 2-1 Syslog Messages in the NNM Status Alarms Browser



Configuring Syslog Integration for OVO with NNM

NOTE DCE software requirements must be installed before configuring the Syslog Integration functionality. See "DCE Software Requirements for Syslog" on page 16.

The Syslog Integration functionality is not enabled when NNM is installed.

NOTE When you execute the `ovstatus` command, a background process called `syslogTrap` is listed. Do not attempt to start this process before enabling the Syslog Integration functionality.

To enable and deploy a syslog configuration, do the following on the NNM management station:

1. Execute: **`setupSyslog.ovpl -server`**

   This command creates an uploadable template configuration directory for the out-of-the-box syslog template, `Syslog to NNM`, under `/var/opt/OV/share/tmp/NNMsyslogTraps`.

2. Upload the `Syslog to NNM` template into the OVO database by typing:

   `opccfgupld NNMsyslogTraps`

3. As user `root`, start HP OpenView Operations by typing: **`$OV_BIN/OpC/opc`**

   Since the NNM process, `syslogTrap`, relies on message stream interface (MSI) to map syslog messages to SNMP traps, the MSI must be enabled on the template and the OVO agent.

4. To enable the MSI on the `Syslog to NNM` template, do the following:

   a. Open the Message Source Templates window by clicking **`Window: Message Source Templates`**.

b. Select the `Syslog to NNM` template.

c. Click **[Modify]**.

d. Click **[Advanced Options]**.

e. Check `Agent MSI` and select `Copy Messages`.

f. Click **[OK]**.

5. To enable the MSI on the OVO agent coexisting on the NNM management station, do the following:

   a. From the Node Bank, select the node containing the OVO agent coexisting on the NNM management station.

   b. Click **Actions:Node ->Modify**.

   c. From the Modify Node window, click **[Advanced Options]**.

   d. From the Node Advanced Options window, check `Enable Output` from the Message Stream Interface pane.

   e. Click **[Close]**.

   f. Click **[OK]** from the Modify Node window.

6. Assign the `Syslog to NNM` template to the OVO agent coexisting on the NNM management station by doing the following:

   a. From the Node Bank, select the node containing the OVO agent coexisting on the NNM management station.

   b. Click **Actions:Agents->Assign Templates**. This opens the Define Configuration window.

   c. Click **[Add]**. The Add Configuration window displays.

   d. Click **[Open Template Window]**.

   e. From the Message Source Templates window, select the `Syslog to NNM` template.

   f. From the Add Configuration window, click **[Get Template Selections]**.

   g. Click **[OK]** in the Add Configuration window.

   h. Click **[OK]** in the Define Configuration window.

7. Install the Syslog to NNM template on the OVO agent coexisting on the NNM management station by doing the following:

a. From the Node Bank, select the node containing the OVO agent coexisting on the NNM management station.

b. Click **Actions:Agents->Install/Update SW & Config**.

c. In the Install/Update ITO Software and Configuration window, make sure the correct managed node is listed in the Target Nodes pane.

d. Check Templates in the Components pane.

e. Click **[OK]** to cause the template to be deployed on the managed node. Afterwards, you should see a message in the OVO message browser indicating that the agent system has been updated.

8. Start the NNM mapper process, syslogTrap, by executing:
$OV_BIN/ovstart syslogTrap

9. On HP-UX operating systems, the location of the system logfile, syslog.log, that the Syslog to NNM template monitors is set to /var/adm/syslog.

   On Solaris operating systems, you need to change the default location of the system logfile from /var/adm/syslog to /var/adm/messages by doing the following:

   a. Start HP OpenView Operations.

   b. Click **Window:Message Source Templates**.

   c. From the Message Source Templates window, select the Syslog to NNM template.

   d. Click **[Modify]**.

   e. In the logfile text entry box, enter: /var/adm/messages

10. Optional: Divert processed syslog messages from the NNM alarm browser to the OVO message browser. For instructions, see “Sending Syslog Messages to OVO Message Browser” on page 24.

11. Optional: Test your syslog configuration by sending sample syslog messages through the system. For instructions, see “Testing Syslog Integration” on page 24.

Sending Syslog Messages to OVO Message Browser

By default, processed syslog messages are forwarded to the Status Alarms category of the NNM alarm browser. To configure syslog messages to display in the OVO message browser, do the following:

- Execute: **`$OV_BIN/OpC/util/ovtrap2opc`**

  See the `ovtrap2opc` man page for information about this command.

- Check **`y`** when prompted to upload to `SNMP Traps` template.
- Install the `SNMP Traps` template on the OVO agent coexisting on the NNM management station. See step 6 on page page 22 for instructions on how to install templates on a managed node.

Testing Syslog Integration

Use the UNIX command line tool, `logger`, to write messages to the system logfile. Read its man page for more information on how to use the command.

For example, to create a *Line Protocol status Down* syslog entry, do the following:

HP-UX: `logger %LINEPROTO-5-UPDOWN: Line protocol on Interface interface2, changed state to down`

Solaris: `logger -p user.err %LINEPROTO-5-UPDOWN: Line protocol on Interface interface2, changed state to down`

NOTE On Solaris operating systems, you need to change the default location of the system logfile that the `Syslog to NNM` template is monitoring. See step 9 on page 23 for instructions on how to do this.

When Syslog Integration is enabled, you should see syslog messages matching the conditions of the `Syslog to NNM` template forwarded to the NNM alarm browser or the OVO message browser, depending on your configuration.

Removing Syslog Integration

Removing Network Node Manager from the system does not completely remove Syslog Integration. The OVO agent is left enabled and running on the system.

To remove the remaining Syslog Integration components, do the following:

1. Disable the Syslog Integration feature, by executing the following command:

   For NNM standalone configurations, type:
   `setupSyslog.ovpl -standalone - disable`

   For OVO with NNM configurations, type:
   `setupSyslog.ovpl -server -disable`

2. For NNM standalone configurations, remove the OVO agent software from the NNM management station by doing the following:

   a. Type: `swremove` (HP-UX) or `pkgrm` (Solaris)

      This opens the SD Remove window.

   b. Select the `ITOAgent` software package name from the Name list.

   c. Click `Actions:Remove` to remove the OVO agent from the NNM management station.

3 Customizing Message Source Templates

This chapter provides the steps necessary to create, modify, and enable Syslog Integration message source templates. The configuration tools used to modify message source templates are also described.

Overview of Message Source Templates

OVO agents are configured via message source templates. The OVO agent can only format and forward a message that is described in a message source template.

In the NNM standalone configuration, the OVO agent is embedded on the NNM management station. In the OVO with NNM configuration, the OVO agent coexists on the NNM management station. In either case, the OVO agent is configured to monitor the status of and collect information from syslog messages through the `Syslog to NNM` message source template.

Message source templates work by identifying strings within messages in message streams. When messages match the conditions defined in the message source templates, they are processed according to the rules defined in the template. When the Syslog Integration functionality is enabled, messages matching markers defined in the `Syslog to NNM` template are forwarded to the NNM `syslogTrap` process. This process maps the syslog messages to SNMP traps.

Message source templates consist of the following elements:

- Type of message source from which you want to collect messages, such as a logfile, a trap, an OVO message interface, or an action. In the case of the `Syslog to NNM` template, the message source is a logfile.
- Message conditions and suppress conditions that match a set of attributes and define responses to received messages. These conditions filter incoming messages from the message source. The conditions also determine how the “important” messages are displayed in the operator window.
- Options, such as default message logging.

Understanding the Template Configuration Tools

There are two main template editing tools used to create and modify syslog configuration template conditions. For NNM standalone configurations, use the Syslog Trap Mapping Configuration interface (see “NNM Syslog Trap Mapping Configuration Interface” on page 30). For OVO with NNM configurations, use the OVO Message Source Templates window (see “OVO Message Source Templates Window” on page 31). Details on how to use these template editing tools can be found in their respective online help volumes.

NNM Syslog Trap Mapping Configuration Interface

When the NNM standalone configuration option is deployed, you construct and modify Syslog Integration message source template conditions through the Syslog Trap Mapping Configuration interface.

To launch the Syslog Trap Mapping Configuration interface, execute:

```
$OV_BIN/ovsyslogcfg
```

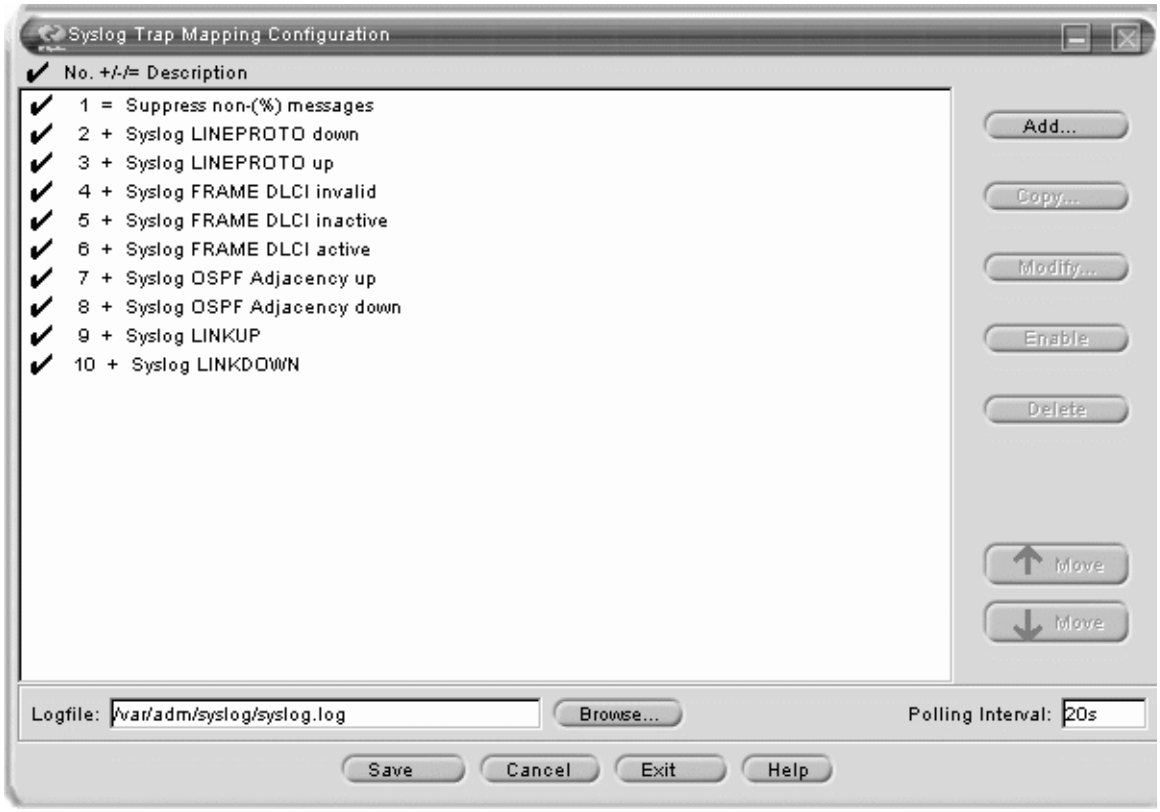
The main dialog for the Syslog Trap Mapping Configuration interface is shown in Figure 3-1 on page 31. This dialog supports the following actions:

- Add or delete template conditions.
- Modify template conditions.
- Enable and disable template conditions.
- Reorder template conditions.

For this release, ten syslog template conditions are defined. These conditions are explained in greater detail in “Understanding the Syslog to NNM Template” on page 33.

For instructions on how to use the Syslog Trap Mapping Configuration interface, see the *Syslog Trap Mapping Configuration Online Help*.

Figure 3-1 Syslog Trap Mapping Configuration Dialog



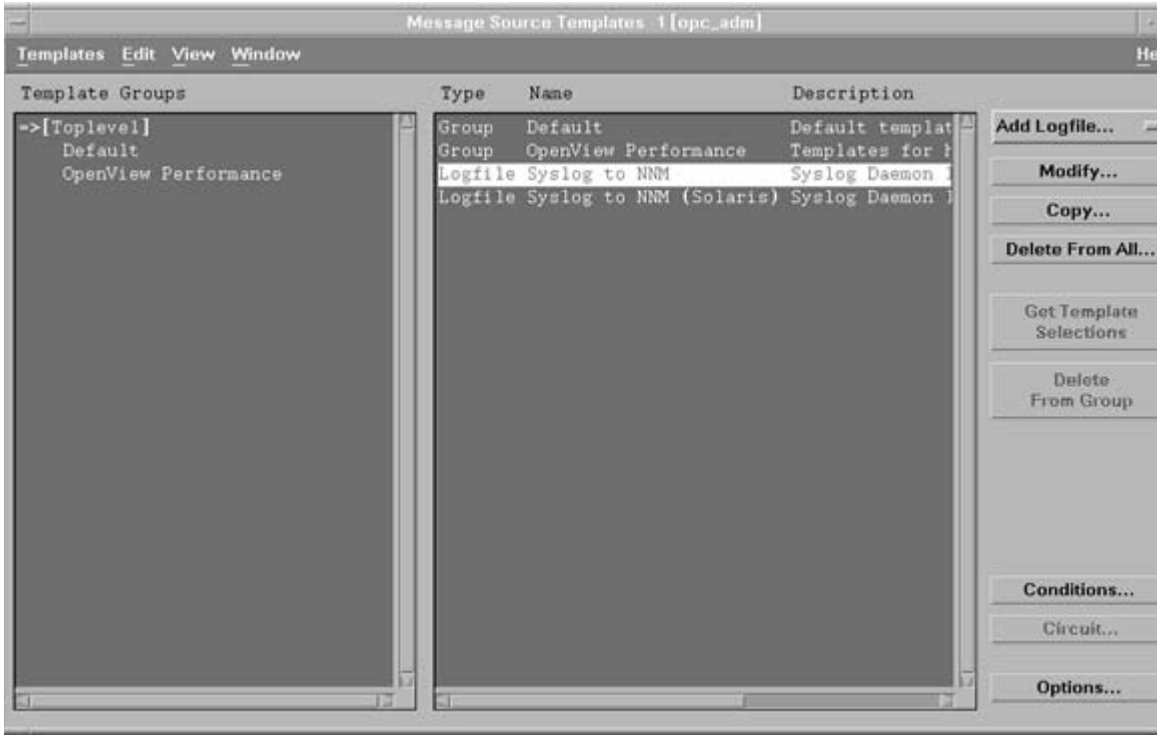
OVO Message Source Templates Window

When the OVO with NNM configuration option is deployed, you construct and modify Syslog Integration message source template conditions through the Message Source Templates configuration window.

To open the Message Source Templates configuration window, launch HP OpenView Operations (`$OV_BIN/OpC/opc`) as an Administrator and then click `Window:Message Source Templates`.

The Message Source Templates window is shown in Figure 3-2 on page 32. The `Syslog to NNM` template for HP-UX operating systems and `Syslog to NNM (Solaris)` template for Solaris operating systems contain the conditions that map syslog message to OpenView SNMP traps.

Figure 3-2 OVO Message Source Templates Window



With the `NNM to Syslog` template for your operating system selected, you can use this dialog to perform the following actions:

- Modify the properties of the template by clicking `[Modify]`.
- Modify the template conditions by clicking `[Conditions]`.

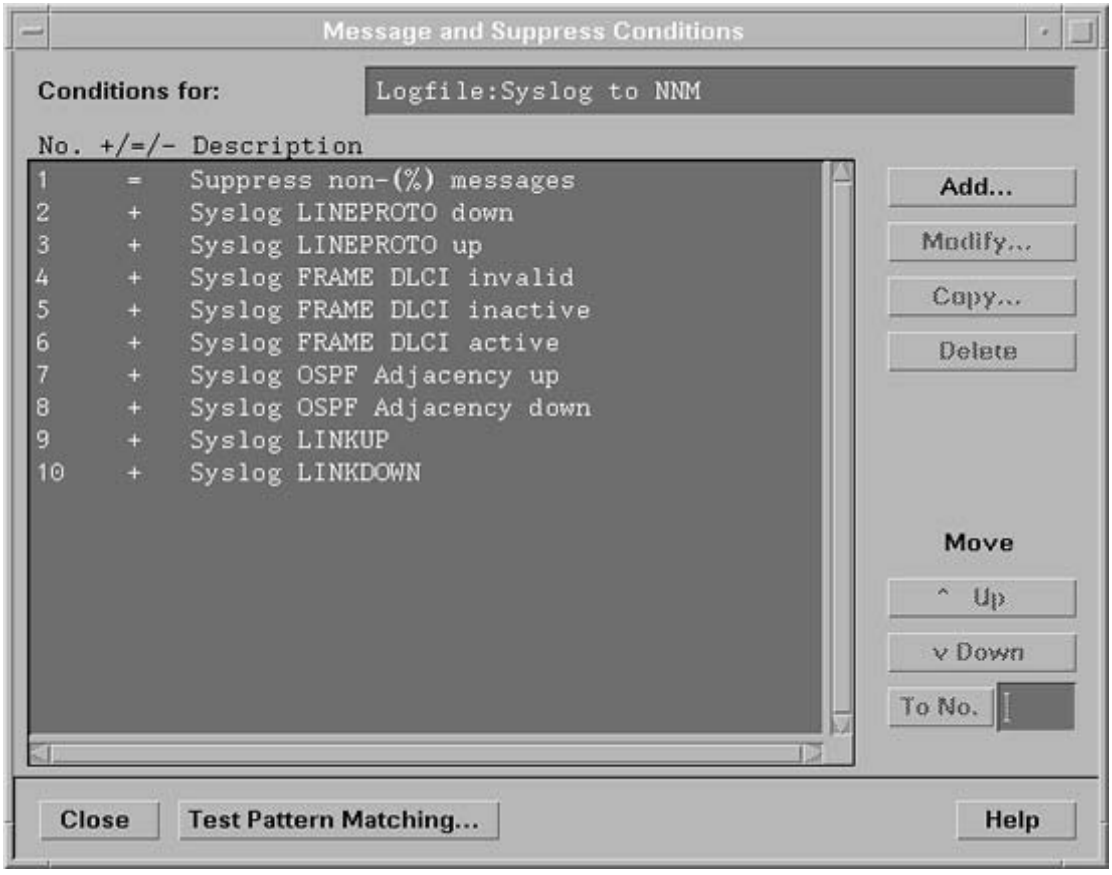
For instructions on how to use the Message Source Templates window, see the *OVO Administrator Online Help*.

Understanding the Syslog to NNM Template

NNM includes out-of-the-box template conditions for which syslog messages are mapped to OpenView SNMP traps. Each type of syslog message to be mapped is defined in one template condition. The conditions are contained in the Syslog to NNM template.

The Syslog to NNM template contains ten out-of-the-box conditions. Figure 3-3 lists the template conditions as they appear in the OVO Message and Suppress Conditions window.

Figure 3-3 Syslog to NNM Template Conditions



In both the OVO template editor windows and the NNM Syslog Trap Mapping Configuration interface, the order of the conditions is important for pattern matching. The patterns are tested in the order that they are listed, and the first pattern to match is executed.

NOTE Since ordering of template conditions matters, it is important to place suppression patterns first and more specific patterns at the beginning of the list. More general patterns should go last.

The first condition is a suppress unmatched condition, meaning the pattern will exclude any message that does not conform to its pattern. In this case, the pattern matches only those syslog messages with the % character as the leading non-white space character in the message (specifically, Cisco syslog message types). This pattern does not functionally perform anything, but is significant as an optimization tool, since all other conditions in this template will execute only on Cisco syslog messages.

The remaining conditions look for Cisco syslog messages matching defined patterns as identified in Table 3-1.

Table 3-1 Template Conditions and Corresponding Syslog Messages

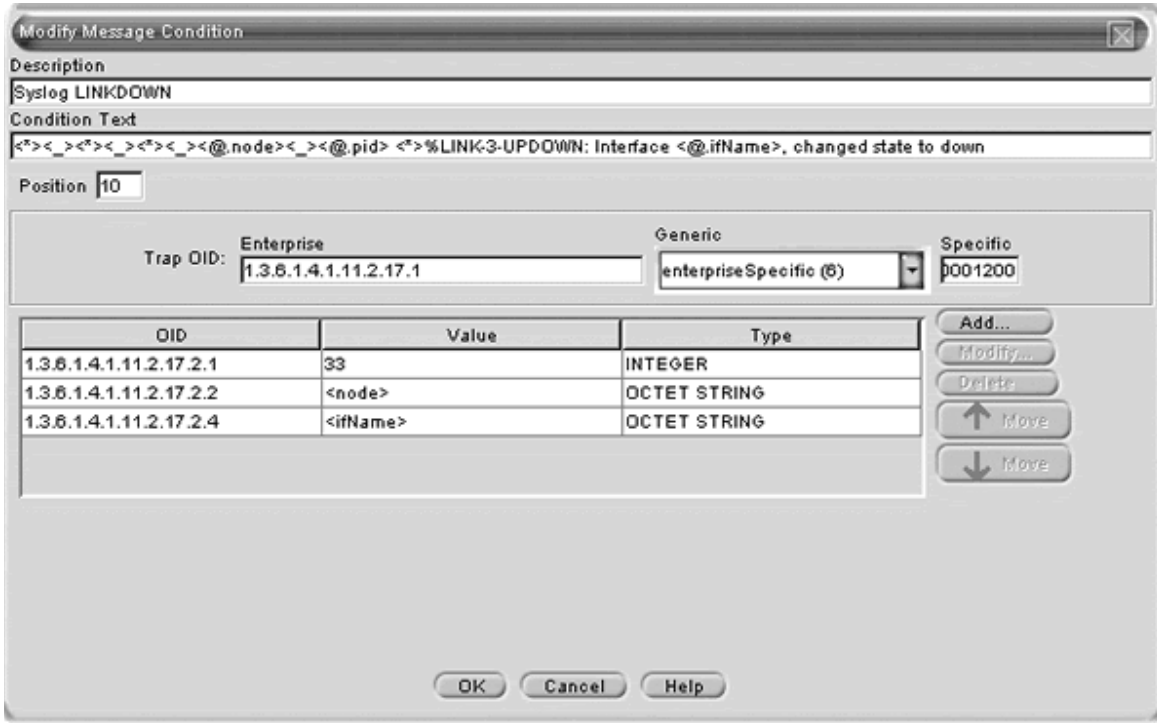
Template Condition Name	Syslog Message Format
Syslog LINEPROTO down	`%LINEPROTO-5-UPDOWN (down)`
Syslog LINEPROTO up	`%LINEPROTO-5-UPDOWN (up)`
Syslog FRAME DLCI Invalid	`%FR-5-DLCICHANGE (INACTIVE)`
Syslog FRAME DLCI Inactive	`%FR-5-DLCICHANGE (INACTIVE)`
Syslog FRAME DLCI Active	`%FR-5-DLCICHANGE (ACTIVE)`
Syslog OSPF Adjacency up	`%OSPF-5-ADJCHG (UP)`
Syslog OSPF Adjacency down	`%OSPF-5-ADJCHG (DOWN)`
Syslog LINKUP	`%LINK-3-UPDOWN (up)`
Syslog LINKDOWN	`%LINK-3-UPDOWN (down)`

How Syslog to NNM Conditions Function in the NNM Standalone Configuration

Figure 3-4 shows a condition window to modify a Syslog to NNM template condition definition. The window is divided into two logical parts: a condition text field to match patterns and a set of attributes that define the SNMP trap to be generated.

The Condition Text field uses syntax similar to a regular expression. It identifies the pattern to match and names any subexpressions in the pattern to be used in the mapping to an SNMP trap. See the *NNM Syslog Trap Mapping Configuration Online Help* for more information about pattern matching.

Figure 3-4 Modify Message Condition Window for Syslog LINKDOWN



The Position field identifies the location of the condition with respect to the other conditions of the template.

The Trap OID is defined by the enterprise, generic, and specific fields. The trap OID is used to determine the type of OpenView event to be generated in response to a message matching the condition pattern.

The varbinds of the trap are defined in the lower table, as shown in Figure 3-4.

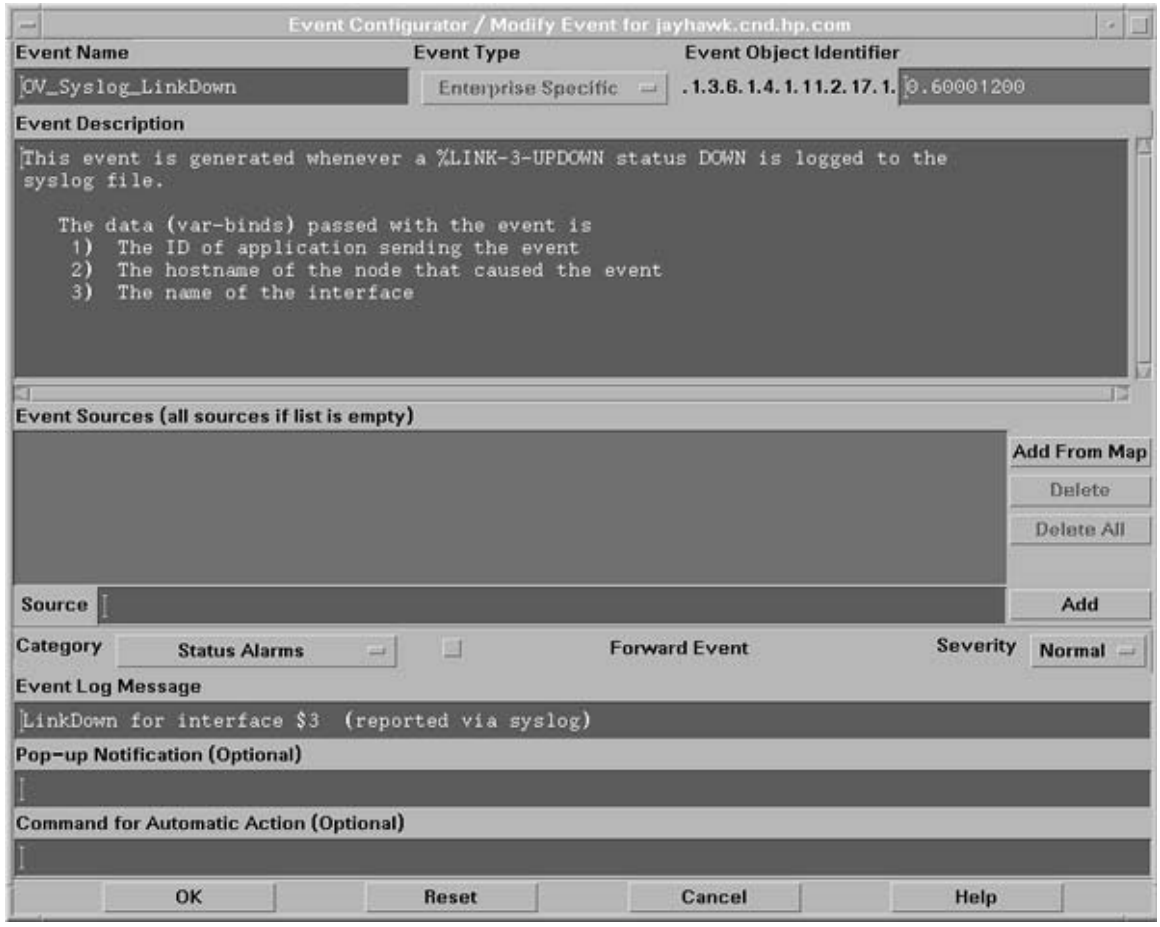
You can edit the Condition Text and the Trap OID fields. You can also modify and reorder any of the varbinds. See the *NNM Syslog Trap Mapping Configuration Online Help* for more information about modifying these fields.

Messages matching the pattern defined in the Condition Text field cause the OpenView event identified by the Trap OID to be generated. For example, when a %LINK-3-UPDOWN status DOWN message is logged to the syslog file, the message is intercepted, since the Syslog LINKDOWN condition looks for this pattern (as shown in the Condition Text field of Figure 3-4). In that same condition, a trap OID is identified, which corresponds to the OpenView event, OV_Syslog_LinkDown, as shown in Figure 3-5 on page 37. This event is then generated.

To view or identify the corresponding OpenView event to be generated, do the following:

1. Start NNM by typing: **ovw**
2. From the Root window, click **Options: Event Configuration**.
3. Select OpenView from the Enterprise Name list. A list of OpenView events displays in the bottom pane.
4. Locate the trap OID from the Event Identifier list.
5. Double-click the event or click **Edit:Modify Event** to display the Event Configurator/Modify Event window. An example is shown in Figure 3-5 on page 37.

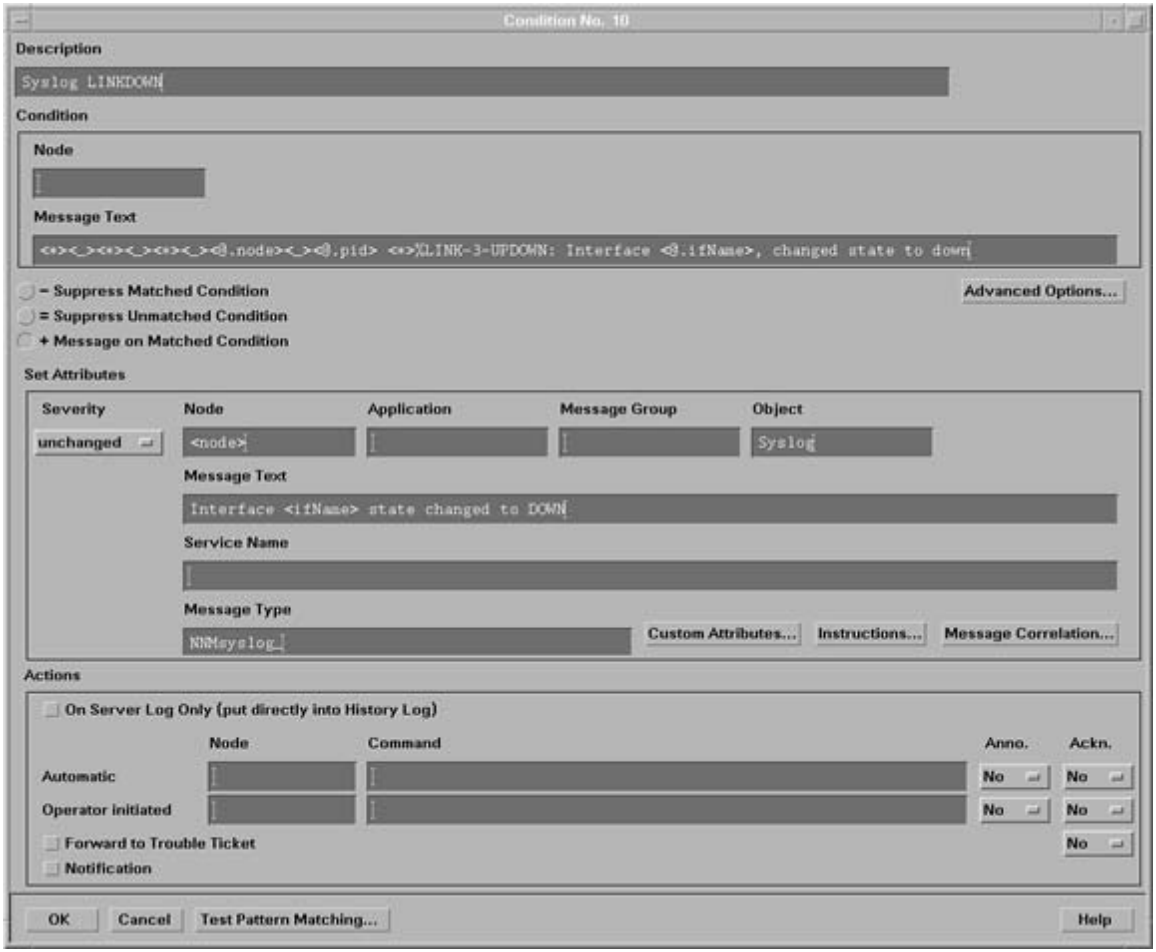
Figure 3-5 OV_Syslog _LinkDown Event Configuration Window



How Syslog to NNM Templates Function in the OVO with NNM Configuration

Figure 3-6 shows a condition window to modify a Syslog to NNM template condition definition. The window is divided into three logical parts: input section, condition matching section, and message output section.

Figure 3-6 OVO Condition Editing Window



The top part contains the input section. Messages are matched according to values stored in the fields listed in Table 3-2.

Table 3-2 Input Fields for OVO Template Conditions

Field	Description	Size
Node	Course-grained identifier for the source of a message, such as software.hp.com.	254
Message Text	Content and/or description of a message. Use OVO's regular expression-like syntax to define the Message Text. Right-click in the field to view a short list of acceptable regular expressions. For example, if you want to match messages on the string "`Switch1`", then define the Message Text field to be `<*>Switch1<*>`. See the *OVO Administrator Online Help* for more information on writing pattern matching expressions.	512

The matching conditions section describes how the conditions are to be treated. The options are listed in Table 3-3.

Table 3-3 Matching Conditions for OVO Template Conditions

Option	Description
Suppress Matched Condition	Suppresses all messages matching condition fields in the input section. Messages are stored in a log file, rather than displaying in the OVO message browser. Identified by the – symbol.

Table 3-3 Matching Conditions for OVO Template Conditions (Continued)

Option	Description
Suppress Unmatched Condition	Suppresses all messages not matching condition fields in the input section. Messages are stored in a log file, rather than displaying in the OVO message browser. Identified by the = symbol.
Message on Matched Condition	Forwards all messages matching condition fields in the input section to the OVO message browser. Identified by the + symbol.

The lower portion contains the output section. The fields in this section correspond to columns in the message browser. Use these fields to reformat the original message into a more readable format for end users. When any of these fields are unspecified, values are copied from the original message. Table 3-4 lists the key message fields, their intended usage, and their size limitations.

NOTE If the value of an output field is a named subexpression from the Message Text input field, it must be enclosed in angle brackets (<>).

Table 3-4 Output Fields of OVO Template Conditions

Field	Description	Size
Node	Identifies the source of a message. In the `Syslog to NNM` template conditions, the value of this field is pulled from the incoming syslog message. Its value is stored in the variable `node`.	254

Table 3-4 Output Fields of OVO Template Conditions (Continued)

Field	Description	Size
Application	Medium-grained identifier for a message source. For example, Oracle.	32
Message Group	Group of alarms to which a message belongs.	32
Object	Fine-grained message source identifier. For example, Syslog.	32
Message Text	Contains the description text of a message.	2048
Service Name	Identifier used to associate a message with a service.	254
Message Type	Identifier of a subgroup of a message group. In order for syslog messages to be forwarded to the NNM `syslogTrap` process, `NNMsyslog_` is required to be entered in this field.	32

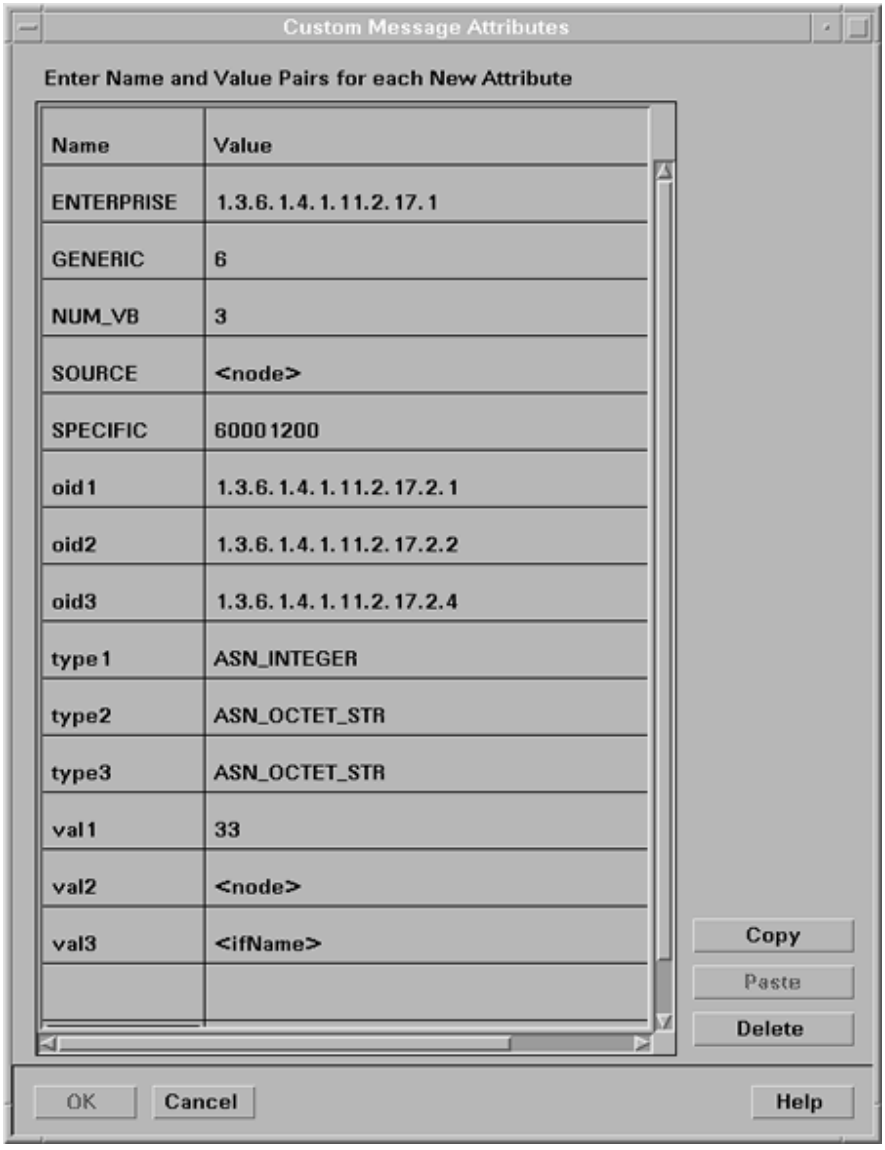
NOTE Be aware that Node, Application, Message Group, and Object fields are used by administrators to create filtered views in the OVO interface. Consistent use of these fields is paramount to enabling operators to effectively monitor equipment for which they are responsible.

From the OVO condition editing window, as shown in Figure 3-6 on page 38, you add, delete, or modify custom message attributes (CMAs). Custom message attributes allow you to add your own attributes to a message. This means that in addition to the default message attributes, you can extend OVO with attributes of your choice.

To assign custom message attributes to a message, use the Custom Message Attributes window. To open, click `[Custom Attributes]` from the OVO condition editing window. For example, Figure 3-7 shows a list of defined custom message attributes for the `syslog LINKDOWN` condition.

The Name field defines the name of the attribute that is displayed as an additional column in the message browser. The Value sets the value of the attribute. The value can contain either hard-coded text or a variable defined in the Message Text input field.

Figure 3-7 OVO Custom Message Attributes



If you have enabled the display of custom message attributes in your OVO message browser, they appear as additional columns in your OVO message browser.

4 Maintaining Syslog Integration

This section provides instructions for tasks that an NNM administrator would need to perform to maintain the working of the Syslog Integration functionality.

Administrative Tasks for NNM Standalone Configurations

Deploying Syslog to NNM Template

After editing syslog message source template conditions with the Syslog Trap Mapping Configuration interface, execute

```
setupSyslog.ovpl -standalone -deploy
```

to deploy the new configuration.

The `-deploy` command option generates and encrypts the new template and restarts the embedded OVO agent so that the new template is reloaded.

Testing Patterns in Template Conditions

Before you redeploy the `Syslog to NNM` template, you can verify the syntax of any template condition by executing:

```
opcpat
```

Read the man page for `opcpat` for instructions on how to use the command.

Disabling Syslog Integration Functionality

To disable the syslog functionality, execute:

```
setupSyslog.ovpl -standalone -disable
```

This command stops the embedded OVO agent processes and the NNM `syslogTrap` process. The OVO agent software remains on the NNM management station. To remove the OVO agent software, see “Removing Syslog Integration” on page 25.

You can re-enable the Syslog Integration functionality, by executing:
`setupSyslog.ovpl -standalone`

Administrative Tasks for OVO with NNM Configurations

Disabling Syslog Integration Functionality

To disable the Syslog Integration functionality, execute:

```
setupSyslog.ovpl -server -disable
```

Starting and Stopping syslogTrap

To start the NNM `syslogTrap` process, execute:

```
ovstart -c syslogTrap
```

NOTE This process is not registered with NNM until you execute the `setupSyslog.ovpl` configuration script. Therefore, you cannot start this process until you have run the `setupSyslog.ovpl` script.

To stop the `syslogTrap` process, execute:

```
ovstop -c syslogTrap
```

5 Troubleshooting Tips

Here are some troubleshooting tips for the Syslog Integration functionality.

System Logfiles

On HP-UX operating systems, syslog entries are logged to `/var/adm/syslog/syslog.log`.

On Solaris operating systems, syslog entries are logged to `/var/adm/messages/syslog.log`.

By default, the `Syslog to NNM` template is set to monitor syslog entries in `/var/adm/syslog`. So, on Solaris operating systems, you need to change the location of the logfile. For instructions for NNM standalone configurations, see the Note on page 18. For instructions for OVO with NNM configurations, see configuration step 9 on page 23.

Performance

The Syslog Integration functionality is not intended for high volume syslog message systems.

Some performance issues may arise as the syslog messages from the managed network elements can become extremely abundant. Sufficient tuning of the `Syslog to NNM` template conditions may need to be done for exclusion patterns to improve performance. Additionally, you may need to add some filtering mechanism to the NNM background process (`syslogTrap`) that maps the syslog message to an SNMP trap.

Configuration

Error starting syslogTrap process:

You must have the Syslog Integration functionality enabled before starting the `syslogTrap` background process.

To enable the Syslog Integration functionality in NNM standalone configurations, see "Configuring Syslog Integration for NNM Standalone" on page 18.

To enable the Syslog Integration functionality in OVO with NNM configurations, see "Configuring Syslog Integration for OVO with NNM" on page 21.

To start the `syslogTrap` process, execute:
`ovstart syslogTrap`

Seeing Duplicate Syslog Messages in Message Browser:

This could be caused by a number of reasons, including one of the following:

- In OVO with NNM configurations, you must enable the message stream interface for both the `Syslog to NNM` template and the OVO agent on the NNM management station in order for syslog messages to be processed as documented. However, in OVO, there are a multitude of combinations for diverting messages through the system. For example, you can enable the message stream interface for individual conditions of a template to copy messages as well as enabling the message stream interface for the template to copy messages. This will produce multiple messages in the message browser.
- Templates are not ordered, meaning that if messages match conditions of multiple templates, multiple messages are displayed in the message browser. For example, if a wildcard template is assigned and installed on a system, then every message entering the agent is forwarded to the message browser. Furthermore, if additional templates are assigned and installed on a system, then those messages matching the conditions of the templates are also forwarded to the message browser. Thus, duplicate messages appear in the message browser, formatted according to rules in the templates.

Not Seeing Syslog Messages in Message Browser

This could be caused by many reasons, including one of the following:

- The `Syslog to NNM` template is not installed or enabled on the OVO agent system (on the NNM management station). To verify that the `Syslog to NNM` template is installed and enabled on the OVO agent, execute:
  `$OV_BIN/OpC/opctemplate`

  This command lists all templates with the type, name, and status (enabled or disabled). This command is helpful to check whether a template you have assigned to an agent node has successfully been installed on that agent system. Be aware that this command does not indicate which version of the template has been deployed. If you have made modifications to any assigned templates, you must reinstall the templates on the managed nodes.

- For OVO with NNM configurations, the message stream interface is not enabled for either the `Syslog to NNM` template or the OVO agent on the NNM management station.

  To isolate the problem, you can turn on XPL tracing for the `syslogTrap` process. If you see no activity in incoming messages, it usually means that the message stream interface has not been enabled in all places that must be enabled.