Thresholds Module

Software Version: 5.0

HP OpenView Performance Insight

User Guide

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

Windows® and MS Windows® are US registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

OpenView is a U.S. registered trademark of Hewlett-Packard Development Company, L.P.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Support

Please visit the HP OpenView web site at:

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

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

You can also go directly to the support web site at:

http://support.openview.hp.com/

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 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://support.openview.hp.com/access_level.jsp

To register for an HP Passport ID, go to:

https://passport2.hp.com/hpp/newuser.do

Contents

1 Overview 7
Threshold Examples Package 7
Version History 8
Sources for Additional Information 8

2 Package Installation 9
Upgrading or Removing an Earlier Version 9
Software Prerequisites 9
Installing Thresholds Module 5.0 10
Testing the Thresholds Script 11
Uninstalling Thresholds Module 5.0 12

3 Defining and Maintaining Actions 13
Threshold Sub-Packages 13
Using Forms to Maintain Action Definitions 13
Supported Actions 15
Disabling an Action 27

4 Advanced Configuration 29
Threshold Procedure File 29
Scheduling Threshold Checking 29
Threshold Policy Definition File 30

5 Defining Threshold Policies 31
Threshold Policy Definition Files 31
Threshold Policy Definition File Names 31
Threshold Policy Definition File Structure 32
Examples of Threshold Policy Definitions 35

6 Troubleshooting 39
Error and Warning Messages 39
Running the thresholds.pl File 40
Debugging 40

Index 43

1 Overview

The Threshold and Event Generation Module, more commonly known as the Thresholds Module, performs the following tasks:

- Reads policy configuration files
- Creates queries against data in OVPI database tables
- Responds to any exception condition by taking one or more actions
- Records the object, the time, and the data values that triggered the exception

Each event is identified by values for Category and Severity. After all threshold exceptions have been identified, the Category and Severity of each exception are used to determine which, if any, of the following actions should occur:

- Send an SNMP trap
- Send SMTP email
- Call a user-defined program

A single event can trigger one or more actions. For example, a single event can trigger a trap, an email, and a program call. The timing of an action depends on the type of action. Although traps are sent one at a time, emails are batched together and sent later, after every exception has been processed.

Many of the reporting solutions that install on OVPI include an optional thresholds sub-package. The optional thresholds sub-package contains a thresholds policy customized for that particular set of reports. If you want to implement thresholding for that particular set of reports, install the thresholds sub-package and the Thresholds Module.

If you do not configure the Thresholds Module, a default action will be invoked when a threshold is breached and when a previous breach condition returns to normal. The default action is to send an SNMPv2 trap. The trap for breaches is *ovpiThresholdBreach*. The trap for clears is *ovpiThresholdClear*.

Threshold Examples Package

Installing the optional Threshold Examples package does two things:

- Creates new database tables populated with test data
- Installs configuration files that monitor the new database tables

Since the data in the tables is recycled, the data is always up-to-date. The threshold policies will cause several OVPI threshold SNMP traps to be sent to the local host on a regular basis. This example is intended to illustrate the operation of the Thresholds Module. Installing it is entirely optional.

Version History

Version 5.0 of the Thresholds Module was released April 2004. Version 5.0 includes the following enhancements:

- Supports Oracle as well as Sybase database management software
- Calls a perl script that provides a Java™ interface to the OVPI database

Version 5.0 was released unchanged in August 2004, November 2004, and June 2005.

Sources for Additional Information

For the latest information regarding limitations and known problems affecting the Thresholds Module, see:

Threshold and Event Generation Module 5.0 Release Statement

For information about default threshold settings in the threshold sub-package that comes with each report pack, refer to the user guide for the report pack.

Manuals for the core product, OVPI, and manuals for the reporting solutions and shared packages that run on OVPI, can be downloaded from this site:

http://www.managementsoftware.hp.com

Select **Support** > **Product Manuals** to reach the **Product Manuals Search** page. The user guides for OVPI are listed under **Performance Insight**. The user guides for report packs and datapipes are listed under **Performance Insight Reporting Solutions**.

The manuals listed under **Performance Insight Reporting Solutions** indicate the month and year of publication. If a manual is revised and reposted, the date of publication will change even if the software version number does not change. Since we post revised manuals on a regular basis, we recommend searching this site for updates before using an older manual that might not be the latest version available.

2 Package Installation

This chapter covers the following topics:

- Upgrading or Removing an Earlier Version
- Software Prerequisites
- Installing Thresholds Module 5.0
- Testing the Thresholds Script
- Uninstalling Thresholds Module 5.0

Upgrading or Removing an Earlier Version

The June 2005 report pack CD contains the latest report packs, datapipes, and shared packages. When you insert the report pack CD in the CD-ROM drive and launch the package extraction program, the install script extracts every package from the CD and copies the results to the Packages directory on your system. When the extract finishes, the install script prompts you to launch OVPI and start Package Manager.

If you are currently running Thresholds Module 4.0, upgrade to version 5.0 by installing the "4.0_to_5.0" upgrade package. If you are currently running any version earlier than 4.0, you cannot upgrade to the latest release. Instead, uninstall your current version, then re-install version 5.0.

Software Prerequisites

Make sure the following platform software is already installed before installing the Thresholds Module:

- OVPI 5.0 or higher
- Any available Service Pack for the version of OVPI (5.0 or 5.1) you are running

The Thresholds Module is itself a prerequisite for the various threshold sub-packages that come with most report packs. When you select one of these sub-packages for installation, Package Manager will install the Thresholds Module for you, automatically. However, you also have the option of using the instructions in this chapter to install or upgrade the Thresholds Module *before* you install any threshold sub-package.

Installing Thresholds Module 5.0

Perform the following tasks to install Thresholds Module 5.0:

- Task 1: Stop OVPI Timer and extract report packs and datapipes from the report pack CD
- Task 2: Use Package Manager to install Thresholds Module 5.0
- Task 3: Restart OVPI Timer

Task 1: Extract packages from the report pack CD

1. Log in to the system. On UNIX® systems, log in as root.
2. Stop OVPI Timer and wait for processes to terminate.

   On Windows, do the following:

   a. Select **Control Panel > Administrative Tools > Services**

   b. Select OVPI Timer from the list of services.

   c. From the Action menu, select **Stop**.

   On UNIX, as root, do one of the following:

   — HP-UX: **`sh /sbin/ovpi_timer stop`**

   — Sun: **`sh /etc/init.d/ovpi_timer stop`**
3. Insert the June 2005 report pack CD in the CD-ROM drive.

   Windows: The package extraction interface opens automatically.

   UNIX:

   a. Mount the CD (if the CD does not mount automatically).

   b. Navigate to the top level directory on the CD.

   c. Run **`./setup`**
4. Type **1** in the choice field and press **Enter**. The install script displays a percentage complete bar. When the copy is complete, the install script starts Package Manager. The Package Manager Welcome window opens.

Task 2: Install Thresholds Module 5.0

1. Click **Next.** The Package Location window opens.
2. Click **Install**; approve the default installation directory, or select a different directory if necessary.
3. Click **Next**. The Report Deployment window opens. Accept the option to Deploy Reports.

   The forms that come with the Thresholds Module will not deploy unless you accept the Deploy Reports option.
4. Type your username and password for the OVPI Application Server.
5. Click **Next**. The Package Selection window opens.
6. Click the check boxes next to the following items:
   - *Thresholds*

- *ThresholdExample* (optional)
- *ThresholdsRP* (optional)

7 Click **Next**. The Type Discovery window opens; disable the Type Discovery option.

8 Click **Next**. The Selection Summary window opens.

9 Click **Install**. The Installation Progress window opens. When installation is complete, a package installation complete message appears.

10 Click **Done**.

Task 3: Restart OVPI Timer.

On Windows, do the following:

a Select **Control Panel > Administrative Tools > Services**

b Select OVPI Timer from the list of services.

c From the Action menu, select **Start**.

On UNIX, as root, do one of the following:

— HP-UX: **`sh /sbin/ovpi_timer start`**

— Sun: **`sh /etc/init.d/ovpi_timer start`**

Testing the Thresholds Script

To verify that the Thresholds Modules and all the prerequisites have been installed correctly, run one of the following commands.

UNIX:

```
$DPIPE_HOME/bin/perl $DPIPE_HOME/scripts/thresholds.pl -h
```

Windows:

```
%DPIPE_HOME%\bin\perl %DPIPE_HOME%\scripts\thresholds.pl -h
```

The system returns a usage-is statement similar to the following:

```
D:/OVPI/scripts/thresholds.pl -f <rulesfile> [-d]
```

where:

`<rulesfiles>` is an XML threshold rules definition file

`-d` enables the debug mode

The default action file is `{DPIPE_HOME}/lib/threshAct.xml`

If you do not see this statement, see Chapter 6, Troubleshooting.

Uninstalling Thresholds Module 5.0

If you uninstall the Thresholds Module, the threshold sub-packages that depend on the Thresholds Module (for example, MPLS_VPN_Thresholds) will be selected and uninstalled automatically. Follow these steps to uninstall Thresholds Module 5.0:

1. Log in to the system. On UNIX systems, log in as root.
2. Stop OVPI Timer and wait for processes to terminate.

   On Windows, do the following:

   a. Select **Control Panel > Administrative Tools > Services**
   b. Select OVPI Timer from the list of services.
   c. From the Action menu, select **Stop**.

   On UNIX, as root, do one of the following:

   — HP-UX: **`sh /sbin/ovpi_timer stop`**
   — Sun: **`sh /etc/init.d/ovpi_timer stop`**
3. Start Package Manager. The Package Manager welcome window opens.
4. Click **Next**. The Package Location window opens.
5. Click **Uninstall.**
6. Click **Next**. The Report Undeployment window opens. Keep the defaults.
7. Click **Next**. The Package Selection window opens.
8. Click the check box next to *Thresholds Module*.

   ➤ Any sub-package that depends on the Thresholds Module (for example, MPLS_VPN_Thresholds) will be selected automatically.
9. Click **Next**. The Selection Summary window opens.
10. Click **Uninstall**. The Progress window opens. When removal is complete, a package removal complete message appears.
11. Click **Done**.
12. Restart OVPI Timer.

    On Windows, do the following:

    a. Select **Control Panel > Administrative Tools > Services**
    b. Select OVPI Timer from the list of services.
    c. From the Action menu, select **Start**.

    On UNIX, as root, do one of the following:

    — HP-UX: **`sh /sbin/ovpi_timer start`**
    — Sun: **`sh /etc/init.d/ovpi_timer start`**

3 Defining and Maintaining Actions

This chapter covers the following topics:

- Threshold Sub-Packages
- Using Forms to Maintain Action Definitions
- Supported Actions
- Disabling an Action

Threshold Sub-Packages

Most OVPI report packs are distributed with a thresholds sub-package. The thresholds sub-package contains a customized threshold policy that defines the conditions that cause exceptions to be reported. If you want to modify threshold values, do not modify the thresholds sub-package. Instead, modify threshold values by using the threshold policy that comes with the thresholds sub-package.

If you want to set new threshold limits for some or all of the objects you are monitoring, use one of the forms or the provisioning interface that comes with the report pack. Using the forms, which are described in this chapter, is easier and faster than using the provisioning interface. If you use the provisioning interface, you must export existing property data from OVPI, edit the file by inserting new values, and then re-import the file into OVPI.

Using Forms to Maintain Action Definitions

Action definitions are stored in the OVPI database. Forms are available for creating and updating action definitions. To access forms, launch the Management Console and select the **Objects** icon. Each form contains instructions for how to use it.

Update forms are easier to spot than create forms. The update forms are listed under **General Tasks**. To open a create form, select **File > New**.

All actions have Category and Severity values associated with them. These may be wildcards (*), which match any Category or any Severity. These values are used to associate actions with threshold breaches, which must have a Category and Severity associated with them.

Category Value

Category value is the name of the event category that will cause this action to occur. Category value is case sensitive. An arbitrary string value, Category value can be set to any non-null single word value *without* embedded spaces. Using special characters (punctuation marks, quotes, hash symbols) is not recommended since these characters may have special meaning for third party systems. To match all categories using a wildcard, type an asterisk (*).

Severity Value

Severity value reflects the severity of an event that will cause this action to occur. Severity level is case sensitive. An arbitrary string value, Severity value can be set to any non-null single word value *without* embedded spaces. Whenever possible, use values that match the severity levels used by other systems. For example, if you are sending traps to a network management system that assigns CRITICAL, HIGH, MEDIUM, or LOW to each trap, use these values. Using special characters (punctuation marks, quotes, hash symbols) is not recommended since these characters may have a special meaning for third party systems. To match all severities using a wildcard, type an asterisk (*).

Default Actions

Default actions are those that will occur regardless of the Category or Severity of the threshold breach that has occurred; that is, they will occur for all exceptions. Default actions have wildcards (*) for both the Category and Severity fields.

A default action is inserted into the database during package installation. The default action is to send an SNMP trap to port 162 on the local system using a community string set to “public”. If you want to send traps to a different destination, use a nonstandard SNMP port, or use a different community string, you must edit the SNMP action definitions. Do this by accessing the Update SNMP Trap Action Definition form (see Updating SNMP Trap Actions on page 17) and using it to change the values for server, port, or community.

You may choose to have additional default actions. For example, you can create a user script default action definition by typing the wildcard symbol (*) in the Category and Severity fields on the Create User Script Action Definition form (see Creating User Script Actions on page 23). Then you will have two default actions: an SNMP trap action and user script action.

Creating and Modifying Action Definitions

You can define multiple actions. For example, you may send traps to more than one system, or you may send both email and traps for the same exception. The following are the types of actions you can define:

- SNMP Trap
- SMTP Mail
- User Script

After you create an action definition, you can modify it using the Update SNMP Trap Action Definition form.

Disabling Actions

You can disable actions, but they will remain in the database in case you want to enable them in the future. For instructions, see Disabling an Action on page 27.

Supported Actions

Three actions are supported. Each action requires a set of parameters.

Action 1: SNMP-TRAP

Parameters

- Server
  - The name or address of a server to send traps to. If an address is used it must be resolvable to an IP address.
- Port
  - A numeric port number.
- Community
  - A community string.

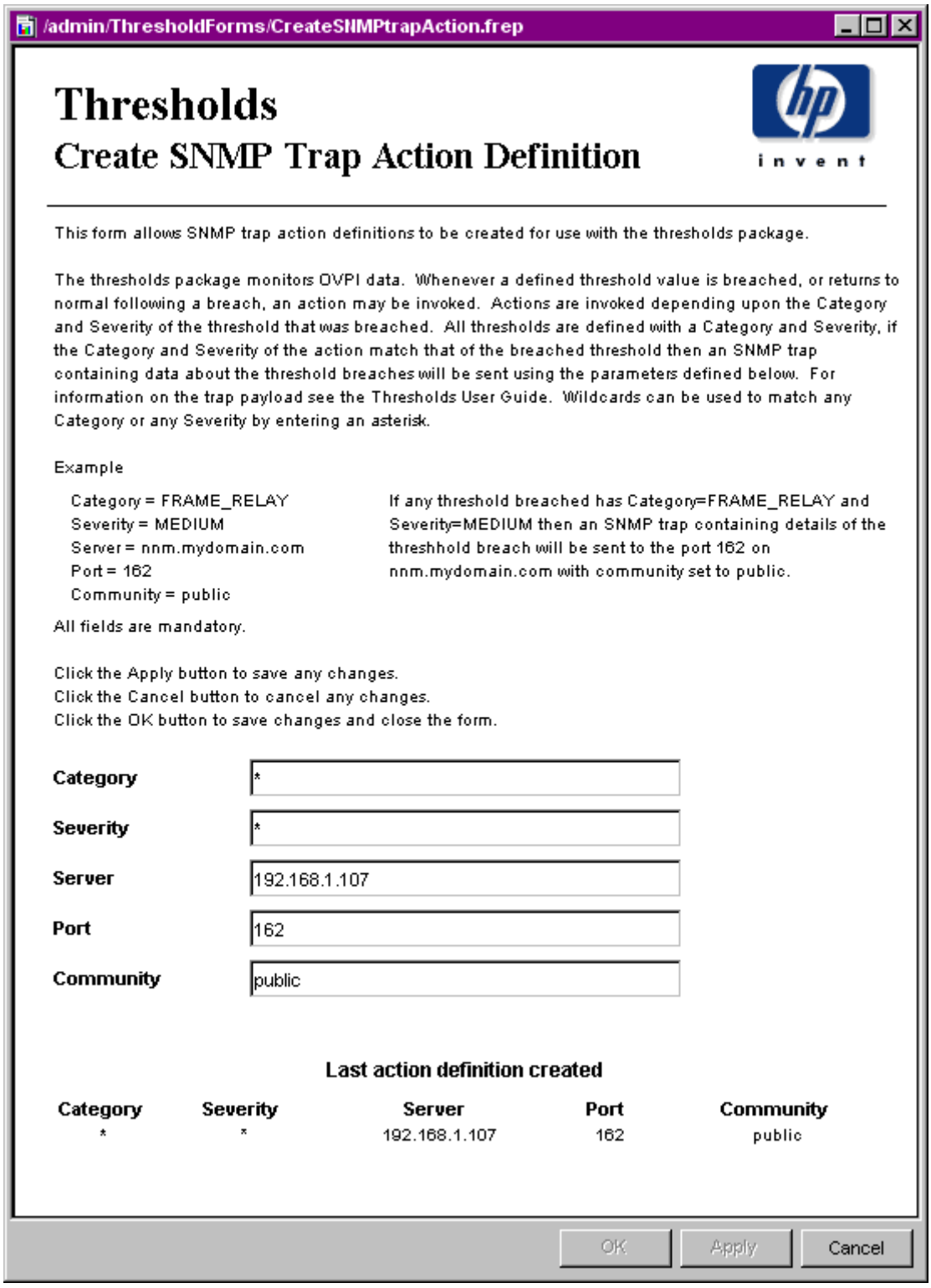
An SNMP trap is sent to the specified server and port using the specified community string.

The ovpiThresholdBreach trap is sent when a threshold condition is initially breached. The ovpiThresholdClear trap is sent when the condition returns to normal. Details about the exception are stored in trap variables. The package includes a MIB that defines ovpiThresholdBreach and ovpiThresholdClear traps.

Creating SNMP Trap Actions

To create an SNMP trap action, use the Create SNMP Trap Action Definition form. Follow these steps to launch the form:

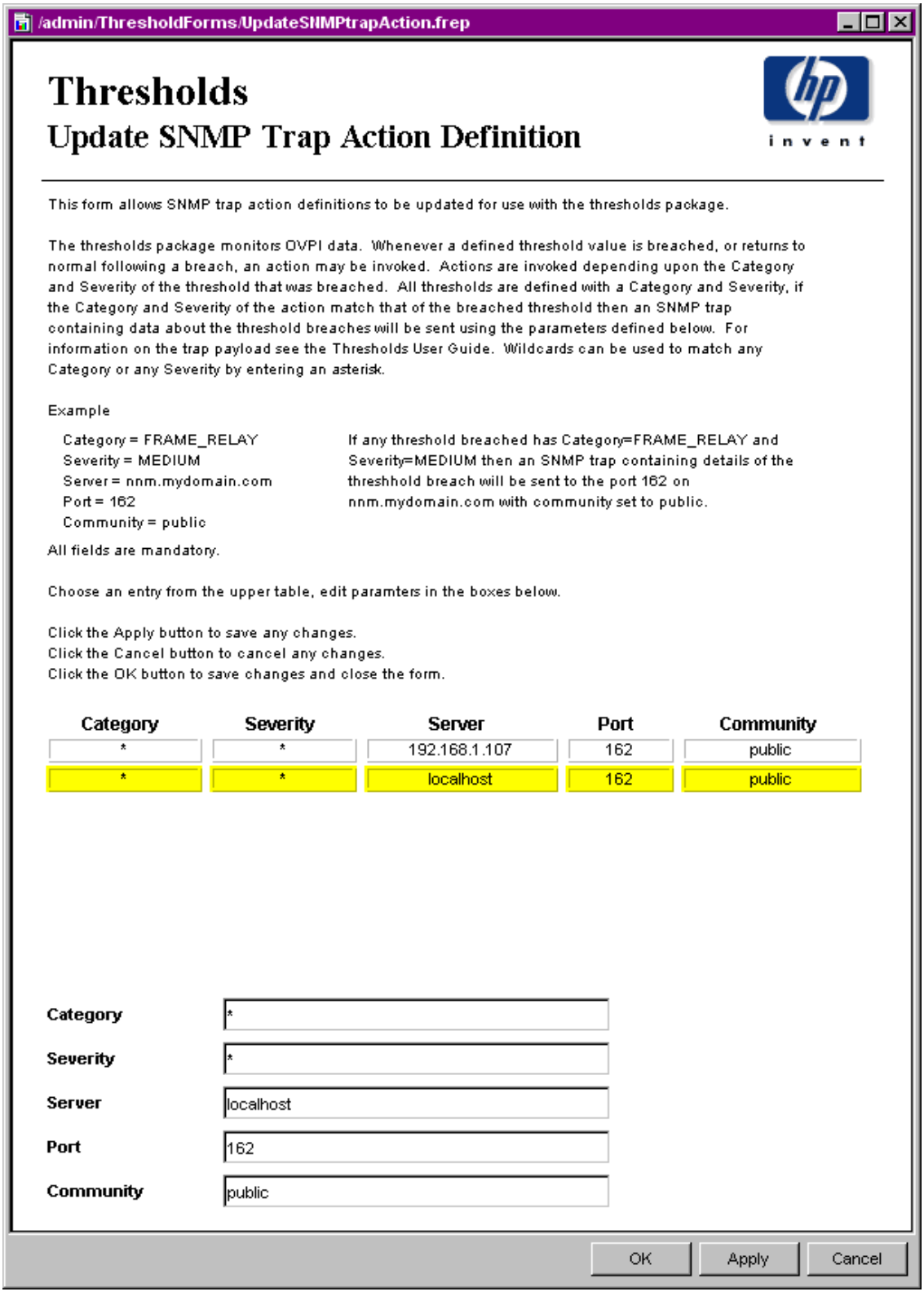
1. In the Management Console, click the **Objects** icon.
2. Select **File > New**.
3. Select **Create SNMP Trap Action** and click **Create**.
4. Follow the instructions on the form.
5. When you finish, click **OK**.


/admin/ThresholdForms/CreateSNMPtrapAction.frep
Thresholds
Create SNMP Trap Action Definition
invent
This form allows SNMP trap action definitions to be created for use with the thresholds package.
The thresholds package monitors OVPI data. Whenever a defined threshold value is breached, or returns to normal following a breach, an action may be invoked. Actions are invoked depending upon the Category and Severity of the threshold that was breached. All thresholds are defined with a Category and Severity, if the Category and Severity of the action match that of the breached threshold then an SNMP trap containing data about the threshold breaches will be sent using the parameters defined below. For information on the trap payload see the Thresholds User Guide. Wildcards can be used to match any Category or any Severity by entering an asterisk.
Example
Category = FRAME_RELAY
Severity = MEDIUM
Server = nnm.mydomain.com
Port = 162
Community = public
If any threshold breached has Category=FRAME_RELAY and Severity=MEDIUM then an SNMP trap containing details of the threshhold breach will be sent to the port 162 on nnm.mydomain.com with community set to public.
All fields are mandatory.
Click the Apply button to save any changes.
Click the Cancel button to cancel any changes.
Click the OK button to save changes and close the form.
Category
*
Severity
*
Server
192.168.1.107
Port
162
Community
public
Last action definition created
Category
Severity
Server
Port
Community
*
*
192.168.1.107
162
public
OK
Apply
Cancel

Updating SNMP Trap Actions

To modify an existing SNMP trap action, use the Update SNMP Trap Action Definition form. Follow these steps to launch the form:

1. In the Management Console, click the **Objects** icon.
2. Select an object; the General Tasks pane is updated.
3. In the list of forms under General Tasks, double-click **Update SNMP Trap Action**. The form opens.
4. Click the desired action definition from the list of actions near the center of the form. The boxes in the bottom section of the form display the action definition parameters.
5. Modify the desired parameters.
6. When you finish making changes, click **OK**.


/admin/ThresholdForms/UpdateSNMPtrapAction.frep
Thresholds
Update SNMP Trap Action Definition
invent
This form allows SNMP trap action definitions to be updated for use with the thresholds package.
The thresholds package monitors OVPI data. Whenever a defined threshold value is breached, or returns to normal following a breach, an action may be invoked. Actions are invoked depending upon the Category and Severity of the threshold that was breached. All thresholds are defined with a Category and Severity, if the Category and Severity of the action match that of the breached threshold then an SNMP trap containing data about the threshold breaches will be sent using the parameters defined below. For information on the trap payload see the Thresholds User Guide. Wildcards can be used to match any Category or any Severity by entering an asterisk.
Example
Category = FRAME_RELAY
Severity = MEDIUM
Server = nnm.mydomain.com
Port = 162
Community = public
If any threshold breached has Category=FRAME_RELAY and Severity=MEDIUM then an SNMP trap containing details of the threshhold breach will be sent to the port 162 on nnm.mydomain.com with community set to public.
All fields are mandatory.
Choose an entry from the upper table, edit paramters in the boxes below.
Click the Apply button to save any changes.
Click the Cancel button to cancel any changes.
Click the OK button to save changes and close the form.
Category
Severity
Server
Port
Community
*
*
192.168.1.107
162
public
*
*
localhost
162
public
Category
*
Severity
*
Server
localhost
Port
162
Community
public
OK
Apply
Cancel

Action 2: SMTP-MAIL

Parameters

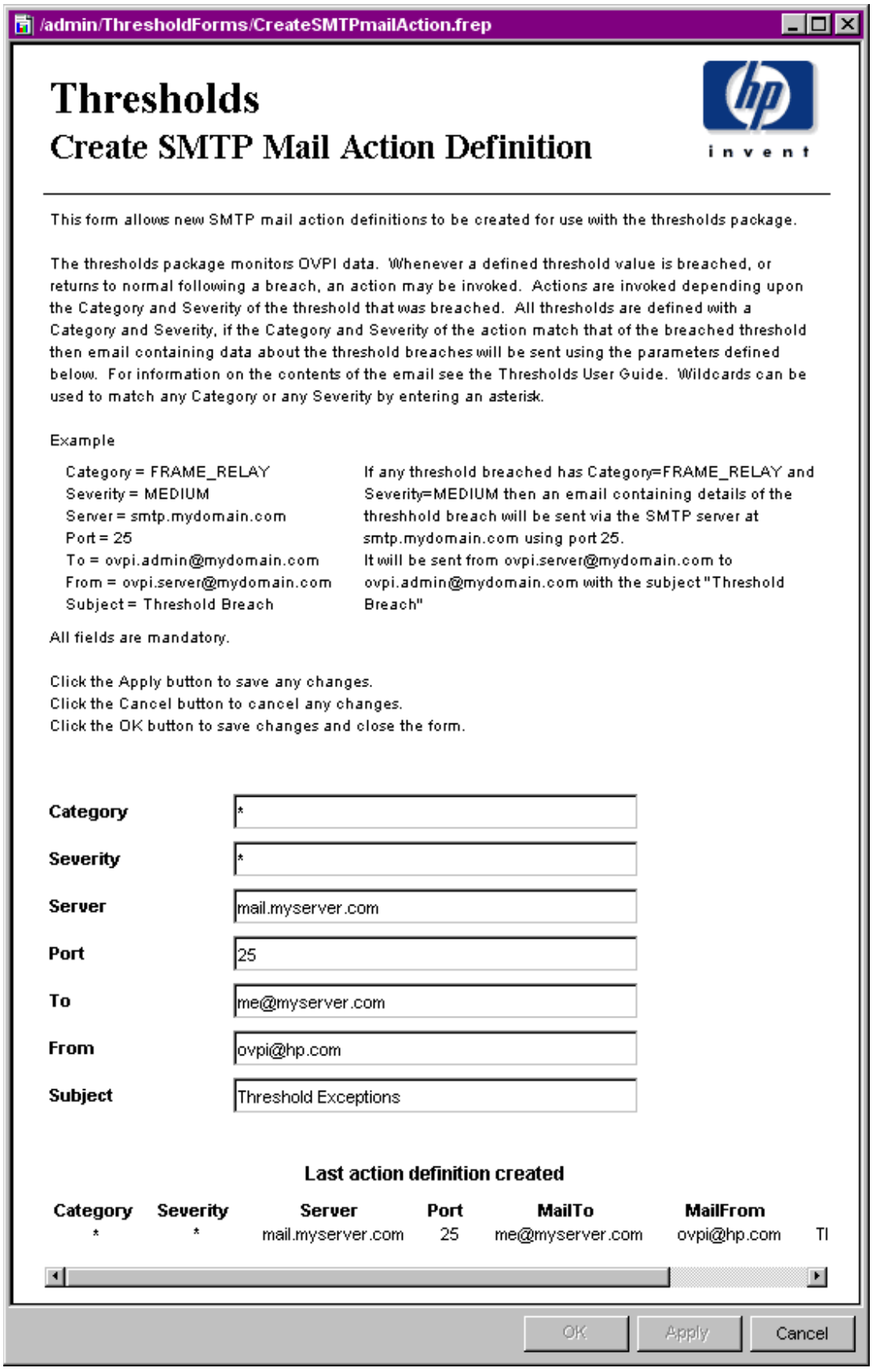
- Server
  - The name or address of an SMTP server which can be used to send email. If an address is used it must be resolvable to an IP address
- Port
  - A numeric port number. The default port for SMTP is 25 but you must check what is used by your server.
- To
  - The address to send email to. This must be a valid email address as defined by your email server, most insist on an internet style *name@domain.com* format.
  - Multiple addresses are not supported, use multiple action definitions to achieve this functionality.
  - Embedded spaces are not permitted in email addresses and may cause messages to fail.
- From
  - The address of the email sender. This must be a valid email address as defined by your email server, most insist on an internet style *name@domain.com* format.
  - Embedded spaces are not permitted in email addresses and may cause messages to fail.
- Subject
  - The subject line for the email which can be include an arbitrary string (including spaces) up to 64 characters long.

An email is sent using the specified SMTP server details. No authentication is used, because the assumption is that the SMTP server will be set up to allow unauthenticated mail from OVPI. The email contains a copy of the exception variables in a CSV-like format. One email message, containing details of all applicable breaches and clears, will be sent for each combination of category, severity and email address defined.

Creating SMTP Mail Actions

To create an SMTP mail action, use the Create SMTP Mail Action Definition form. Follow these steps to launch the form:

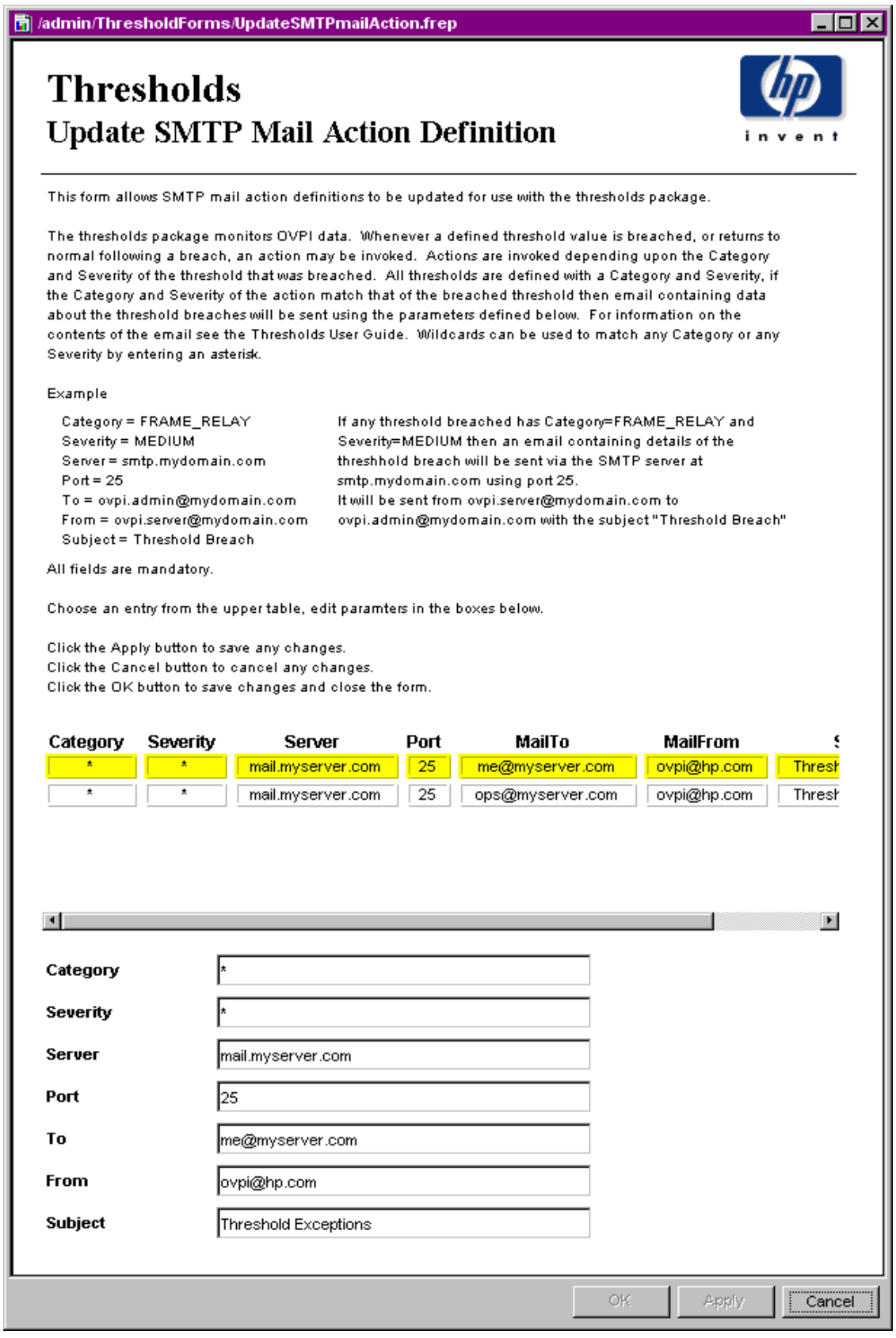
1. In the Management Console, click the **Objects** icon.
2. Select **File > New**.
3. Select **Create SMTP Mail Action** and click **Create**.
4. Follow the instructions on the form.
5. When you finish, click **OK**.


/admin/ThresholdForms/CreateSMTPmailAction.frep
Thresholds
Create SMTP Mail Action Definition
invent
This form allows new SMTP mail action definitions to be created for use with the thresholds package.
The thresholds package monitors OVPI data. Whenever a defined threshold value is breached, or returns to normal following a breach, an action may be invoked. Actions are invoked depending upon the Category and Severity of the threshold that was breached. All thresholds are defined with a Category and Severity, if the Category and Severity of the action match that of the breached threshold then email containing data about the threshold breaches will be sent using the parameters defined below. For information on the contents of the email see the Thresholds User Guide. Wildcards can be used to match any Category or any Severity by entering an asterisk.
Example
Category = FRAME_RELAY
Severity = MEDIUM
Server = smtp.mydomain.com
Port = 25
To = ovpi.admin@mydomain.com
From = ovpi.server@mydomain.com
Subject = Threshold Breach
If any threshold breached has Category=FRAME_RELAY and Severity=MEDIUM then an email containing details of the threshhold breach will be sent via the SMTP server at smtp.mydomain.com using port 25. It will be sent from ovpi.server@mydomain.com to ovpi.admin@mydomain.com with the subject "Threshold Breach"
All fields are mandatory.
Click the Apply button to save any changes.
Click the Cancel button to cancel any changes.
Click the OK button to save changes and close the form.
Category
*
Severity
*
Server
mail.myserver.com
Port
25
To
me@myserver.com
From
ovpi@hp.com
Subject
Threshold Exceptions
Last action definition created
Category
Severity
Server
Port
MailTo
MailFrom
*
*
mail.myserver.com
25
me@myserver.com
ovpi@hp.com
TI
OK
Apply
Cancel

Updating SMTP Mail Actions

To modify an existing SMTP mail action, use the Update SMTP Mail Action Definition form. Follow these steps to launch the form:

1. In the Management Console, click the **Objects** icon.
2. Select an object so that the General Tasks pane is updated.
3. In the list of General Tasks, double-click **Update SMTP Mail Action**. The form opens.
4. Click the desired action definition from the list of actions near the center of the form. The boxes in the bottom section of the form display the action definition parameters.
5. Modify the desired parameters.
6. When you finish making changes, click **OK**.


/admin/ThresholdForms/UpdateSMTPmailAction.frep
Thresholds
Update SMTP Mail Action Definition
invent
This form allows SMTP mail action definitions to be updated for use with the thresholds package.
The thresholds package monitors OVPI data. Whenever a defined threshold value is breached, or returns to normal following a breach, an action may be invoked. Actions are invoked depending upon the Category and Severity of the threshold that was breached. All thresholds are defined with a Category and Severity, if the Category and Severity of the action match that of the breached threshold then email containing data about the threshold breaches will be sent using the parameters defined below. For information on the contents of the email see the Thresholds User Guide. Wildcards can be used to match any Category or any Severity by entering an asterisk.
Example
Category = FRAME_RELAY
Severity = MEDIUM
Server = smtp.mydomain.com
Port = 25
To = ovpi.admin@mydomain.com
From = ovpi.server@mydomain.com
Subject = Threshold Breach
If any threshold breached has Category=FRAME_RELAY and Severity=MEDIUM then an email containing details of the threshhold breach will be sent via the SMTP server at smtp.mydomain.com using port 25. It will be sent from ovpi.server@mydomain.com to ovpi.admin@mydomain.com with the subject "Threshold Breach"
All fields are mandatory.
Choose an entry from the upper table, edit paramters in the boxes below.
Click the Apply button to save any changes.
Click the Cancel button to cancel any changes.
Click the OK button to save changes and close the form.
Category
Severity
Server
Port
MailTo
MailFrom
* * mail.myserver.com 25 me@myserver.com ovpi@hp.com Thresh
* * mail.myserver.com 25 ops@myserver.com ovpi@hp.com Thresh
Category *
Severity *
Server mail.myserver.com
Port 25
To me@myserver.com
From ovpi@hp.com
Subject Threshold Exceptions
OK
Apply
Cancel

Action 3: USER-SCRIPT

Parameters

A CSV file is created for each combination of Category and Severity. Each CSV file contains details about every applicable breach and clear. Every time a file is created, the user script program is called and the filename is passed as a parameter.

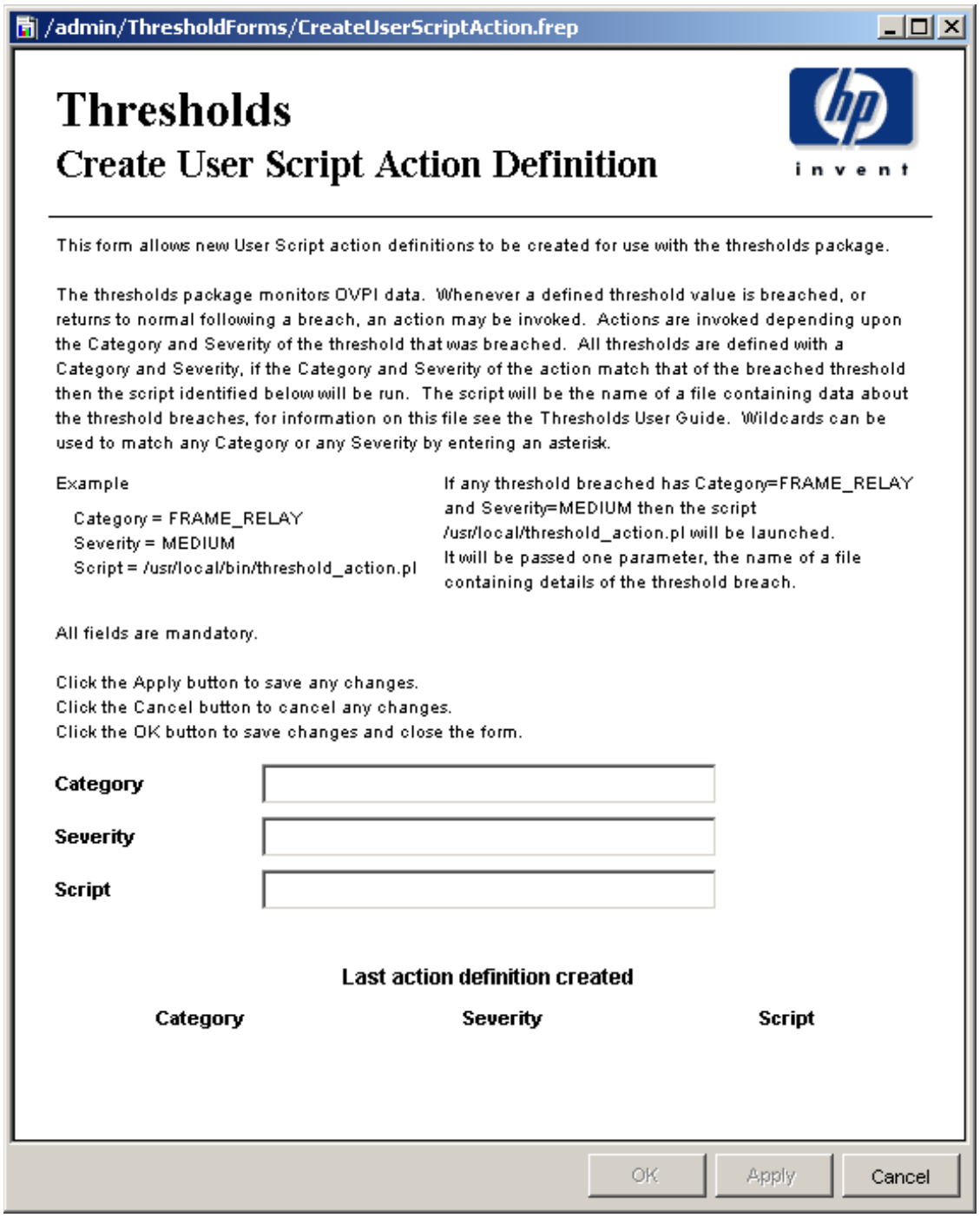
The user script program is called using the supplied command line. If the program is not on the user's path, an appropriate path name should be included. In addition, the user must have suitable permissions to run the program. Responsibility for managing the files created belongs to the program; the thresholding package does not archive these files or delete them.

The program is launched independent of the thresholding package and may outlive the instance that invokes it. Be careful when calling processes that require user intervention. If a backlog of processes develops, OVPI may slow down or even crash. For this reason, it is good practice to call processes that run to completion automatically.

Creating User Script Actions

To create a user script action, use the Create User Script Action Definition form. Follow these steps to launch the form:

1. In the Management Console, click the **Objects** icon.
2. Select **File > New**.
3. Select **Create User Script Action Definition** and click **Create**.
4. Follow the instructions on the form.
5. When you finish, click **OK**.



Updating User Script Actions

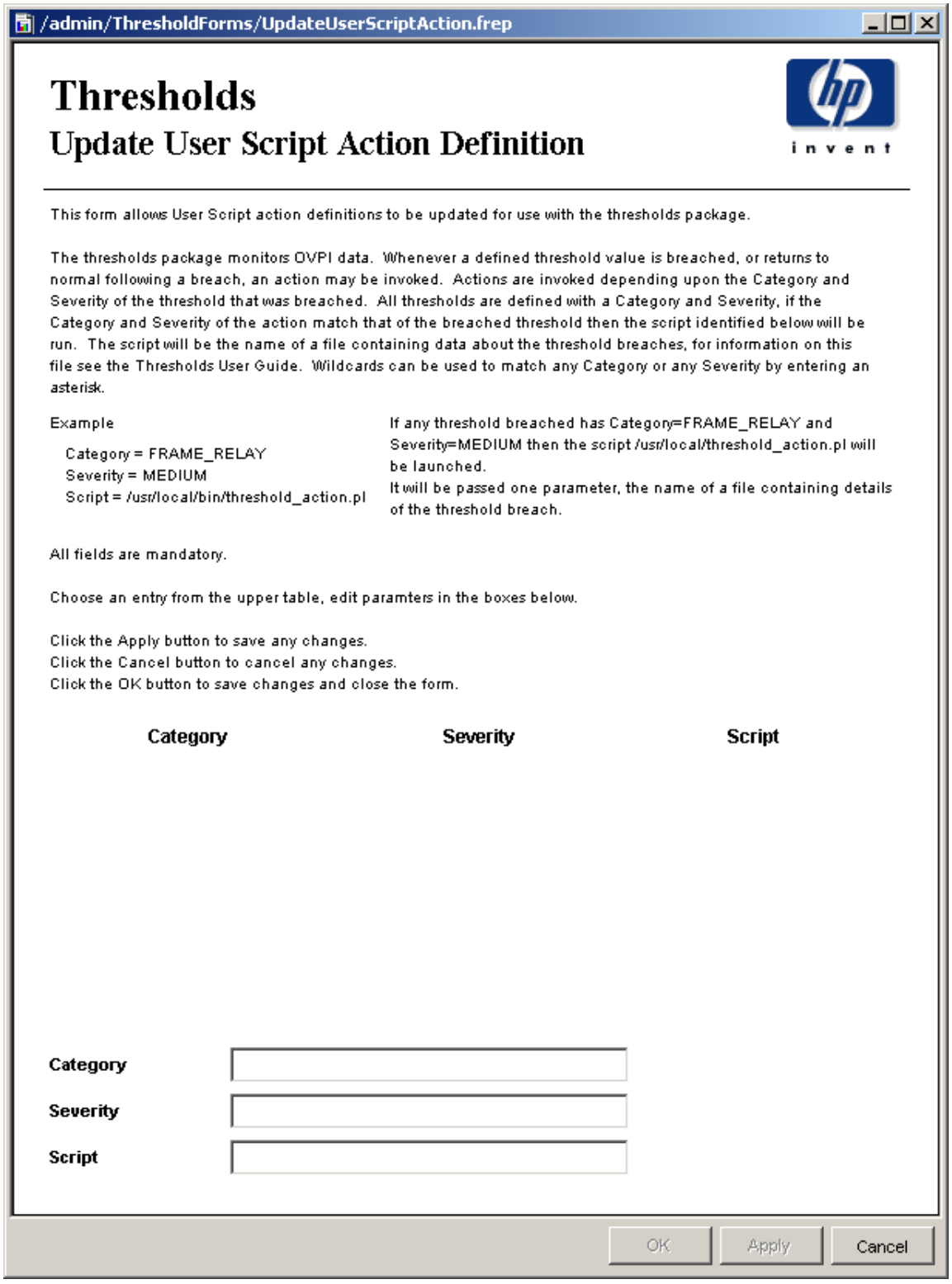
To modify an existing user script action, use the Update User Script Action Definition form. Follow these steps to launch the form:

1. In the Management Console, click the **Objects** icon.
2. Select an object so that the General Tasks pane is updated.
3. In the list of General Tasks, double-click **Update User Script Action Definition**. The form opens.

4 Click the desired action definition from the list of actions near the center of the form. The boxes in the bottom section of the form display the action definition parameters.

5 Modify the desired parameters.

6 When you finish making changes, click **OK**.


/admin/ThresholdForms/UpdateUserScriptAction.frep
Thresholds
Update User Script Action Definition
invent
This form allows User Script action definitions to be updated for use with the thresholds package.
The thresholds package monitors OVPI data. Whenever a defined threshold value is breached, or returns to normal following a breach, an action may be invoked. Actions are invoked depending upon the Category and Severity of the threshold that was breached. All thresholds are defined with a Category and Severity, if the Category and Severity of the action match that of the breached threshold then the script identified below will be run. The script will be the name of a file containing data about the threshold breaches, for information on this file see the Thresholds User Guide. Wildcards can be used to match any Category or any Severity by entering an asterisk.
Example
Category = FRAME_RELAY
Severity = MEDIUM
Script = /usr/local/bin/threshold_action.pl
If any threshold breached has Category=FRAME_RELAY and Severity=MEDIUM then the script /usr/local/threshold_action.pl will be launched.
It will be passed one parameter, the name of a file containing details of the threshold breach.
All fields are mandatory.
Choose an entry from the upper table, edit paramters in the boxes below.
Click the Apply button to save any changes.
Click the Cancel button to cancel any changes.
Click the OK button to save changes and close the form.
Category
Severity
Script
Category
Severity
Script
OK
Apply
Cancel

Disabling an Action

You can disable actions, but they will remain in the database in case you want to enable them in the future. Do the following to disable an action:

1. In the Management Console, click the **Objects** icon.
2. Select an object; selecting an object updates the General Tasks pane.
3. In the list of forms under General Tasks, double-click the desired Update Action Definition form. The form opens.
4. Click the desired action definition from the list of actions near the center of the form. The boxes in the bottom section of the form display the action definition parameters.
5. Change Category and/or Severity to a value that will not occur (for example, “NOT_IN_USE” or “RESERVED”) to ensure that the action will not take place.
6. Click **OK**.

4 Advanced Configuration

To configure the more advanced features of the Thresholds Module, it helps to be familiar with the components of the threshold sub-package. A threshold sub-package contains:

- A procedure file that calls the Threshold Module with appropriate configuration files
- trendtimer.sched file entries that control timing of threshold checking
- A threshold policy definition

Threshold Procedure File

A threshold procedure file is an OVPI procedure (`.pro` file) and typically consists of a single call to the Thresholds Module within a single block. A single procedure file could also be used to check multiple thresholds across multiple tables by simply inserting multiple calls to the Thresholds Module, either in the same block or another block. For more information about OVPI procedure files, refer to the *Performance Insight Reference Guide*.

A call to the Thresholds Module within a procedure file looks like this:

```
begin: checkThreshold
{DPIPE_HOME}/bin/perl {DPIPE_HOME}/scripts/thresholds.pl -f policy.xml
end: checkThreshold
```

`policy.xml` should be replaced with a full path to the desired configuration file.

Scheduling Threshold Checking

To check thresholds on a regular basis, you should set up an entry in the `trendtimer.sched` file to call an appropriate procedure file. You should check thresholds at a frequency that is less than or equal to the frequency at which data is inserted into the table you are checking. For example, if data is collected and inserted into the table every 15 minutes, you should not check thresholds more often than every 15 minutes. For more information about OVPI `trendtimer.sched` entries, refer to the *Performance Insight Reference Guide*.

Here is an example of a `trendtimer.sched` entry that calls a thresholds procedure every 15 minutes:

```
15 - - {DPIPE_HOME}/bin/trend_proc -f {DPIPE_HOME}/scripts/thresh.pro
```

Threshold Policy Definition File

Any call to the Thresholds Module must include a valid policy definition file. Policy definition files are written in XML, specifying the data to be checked and the threshold values for that data. The file also assigns a Category value and a Severity value to any threshold breaches (events). For details about the structure and content of policy definition files, see Chapter 5, Defining Threshold Policies.

5 Defining Threshold Policies

This chapter covers the following topics:

- Threshold Policy Definition Files
- Threshold Policy Definition File Names
- Threshold Policy Definition File Structure
- Examples of Threshold Policy Definitions

Threshold Policy Definition Files

A threshold definition file establishes a threshold policy. It provides the rules necessary to construct queries against a single database table or view and an associated property table. A view may span multiple data and property tables.

Threshold configuration files are written in XML. To modify them you can use an XML editor or any text editor.

When modifying XML files, make sure that you use special characters correctly. For example, in XML the less-than (<) and greater-than (>) signs indicate the start and end of tags. If you want symbols for less-than and greater-than, use **`&lt`** and **`&gt`**. If you want to add a comment, use this format:

<*!-- This is a comment --*>

Most web browsers know when an XML file is correctly constructed. Load the edited file into your browser to verify it is well constructed.

The threshold policy definition file contains a number of clauses. Some are mandatory and some are optional, but the structure is fixed.

Threshold Policy Definition File Names

A threshold definition file name cannot exceed 27 characters in length (ignoring the final period and any extension following the period). The name of the threshold definition file is used to build an OVPI data table that stores data required by the Thresholds Module. Exceeding this character limit may cause errors when the data table is built and when the data table is used.

Threshold Policy Definition File Structure

The threshold policy definition file consists of a single all-encompassing OVPI clause. The OVPI clause contains a single “ThresholdPolicy” clause.

A “ThresholdPolicy” clause consists of several clauses; a “MaxAge” clause, a “DataTable” clause, a “Constraint” clause and a “Thresholds” clause. It may optionally include “Variables” and “UserDefs” clauses.

A “Constraint” clause contains a single “SQL” clause.

An “SQL” clause contains an optional “Name” clause, a “PropertyTable” clause, and an optional SQL constraint “Clause” clause.

A “Variables” clause contains a number of “Variable” clauses.

A “Variable” clause contains a “Data” clause.

A “UserDefs” clause contains up to five numbered “UserDefX” clauses.

A “Thresholds” clause consists of a number of “Threshold” clauses.

A “Threshold” clause contains a “Rule” clause, identified by a “Name” and a “Severity”. It may also optionally be identified as being an “SLA” and may optionally contain a “Display” clause.

A “Rule” clause contains a “Data” clause.

A “Display” clause contains a “Data” clause.

This is shown below:

```
<OVPI>
  <ThresholdPolicy Category="CATEGORY-NAME">
    <MaxAge>
      <DeltaTime Value="MAXIMUM-AGE" Units="HOURS"/>
    </MaxAge>
    <DataTable>tableName</DataTable>
    <Constraint Type="SQL">
      <SQL>
        <Name>CONSTRAINT-NAME</Name>
    <!-- The Name clause is optional -->
        <PropertyTable>PROPERTY-TABLE</PropertyTable>
        <Clause>SQL-CONSTRAINT</Clause>
    <!-- The SQL constraint Clause clause is optional -->
      </SQL>
    </Constraint>
    <Variables>
      <Variable Name="VARIABLE-NAME">
        <Data>VARIABLE-SQL</Data>
      </Variable>
    </Variables>
    <UserDefs>
```

```
    <UserDef1>USERDEF-SQL</UserDef1>
     <!-- Include up to five USERDEF tags -->
  </UserDefs>
  <Thresholds>
    <Threshold Name="THRESHOLD-NAME" Severity="SEVERITY" SLA="SLA-FLAG">
      <Rule>
        <Data>THRESHOLD-SQL</Data>
      </Rule>
      <Display>
        <Data>DISPLAY-SQL</Data>
      </Display>
    </Threshold>
     <!-- Include as many additional Threshold tags as desired -->
  </Thresholds>
 </ThresholdPolicy>
</OVPI>
```

Required values, appearing in italics above, are defined below.

CATEGORY_NAME

The name of the category to which any events defined in this threshold policy belong. Category name is an arbitrary string value and can be set to any single word value, however do not use spaces. The use of special characters (for example, quotes or hash symbols) is not advised since these can have special meaning for third party software packages that integrate with the Thresholds Module. If you are integrating OVPI with NNM and wish to launch OVPI reports from NNM, you must set this value to a category that is registered with NNM.

MAXIMUM-AGE

The maximum age of data that will trigger an event. Must be entered in HOURS. This value can be used to suppress testing data that is “too old” which might in turn cause event storms.

The maximum age value will not normally be exceeded since only data which is more recent than the previous test will now be tested. For example, if data is inserted into a table on a fifteen minute polling cycle, and thresholds are checked every fifteen minutes, you might use a maximum age of one hour. The first time you invoke this threshold test, there is no previously tested data. So rather than testing all the data in the table, only data up to the maximum age is tested.

Set the parameter to at least one poll period. For heavily populated tables (“rate” tables, for example) keep the value as low as possible; for lightly populated tables it can be set higher since any impact is smaller.

DATA-TABLE

The data table to be checked. The table must be a valid OVPI data table or view.

CONSTRAINT-NAME

The name of the constraint applied to data to be checked. Constraint-name is an arbitrary string value and can be set to any single word value (i.e. do not use spaces). The use of special characters (e.g. quotes or hash symbols) is not advised. The constraint name does not get passed on from the thresholds module; thus, it is not externally visible. The name can be used to provide a description of what the constraint does, for example:

- "DOMESTIC-US-CIRCUITS-ONLY"
- "FRAME-RELAY-PORTS"

PROPERTY-TABLE

The property table that is being checked. This must be related to the DATA-TABLE and exist in OVPI's dictionary tables.

SQL-CONSTRAINT

An SQL clause that constrains the query. The query built by the threshold module is ANDed with this clause. Columns from property and/or data tables may be used. Prefix columns from the property table with "**p.**"; prefix columns in the data table with "**d.**". For example, if the property table being checked contained a column for if_type, it would be possible to check thresholds for a particular if_type by using a constraint clause similar to the following:

```
<Clause>d.if_type = 17</Clause>
```

SQL is checked only when it is passed to the database server. Invalid SQL clauses will result in errors being returned from the database, which in turn will be logged by the Thresholds Module.

VARIABLE-NAME

The name by which the variable will be known. Variable names must be unique within the definition file. Variables defined within this XML clause can be used in the DISPLAY-STRING (see below).

VARIABLE-SQL

An SQL clause that will be evaluated to provide a value for the variable. Columns from property and/or data tables may be used. Prefix columns from the property table with "**p.**"; prefix columns in the data table with "**d.**".

USERDEF-SQL

An SQL clause that will be evaluated and passed directly to output. Columns from property and/or data tables may be used. Prefix columns from the property table with "**p.**"; prefix columns in the data table with "**d.**".

Up to five user defined SQL clauses can be used and allow passing of data which is not directly part of the threshold query to third party systems via any actions defined (e.g. SNMP trap or SMTP mail).

SLA-FLAG

If this tag is present, the threshold is considered an SLA threshold which can be used to determine any breaches that affect a Service Level Agreement. The value itself is ignored, for example, the presence of SLA="Yes" or SLA="True" has the same effect. The tag should be omitted if the threshold does not form part of an SLA.

DISPLAY-SQL

An SQL clause that will be evaluated and passed to output. Columns from property and/or data tables may be used as well as variables (defined above). Prefix columns from the property table with "**p.**"; prefix columns in the data table with "**d.**", prefix variables with "**v**". The use of variables allows for some "nesting" of the results of queries which can be used to greatly simplify what is presented to the users via actions.

THRESHOLD NAME

The name of this threshold. Name is an arbitrary string value and can be set to any single word value (i.e. do not use spaces). The use of special characters (e.g. quotes or hash symbols) is not advised.

SEVERITY

The severity of the event defined in the particular threshold-policy. Severity is an arbitrary string value and can be set to any single word value (i.e. do not use spaces). The use of special characters (e.g. quotes or hash symbols) is not advised since these can have special meaning for third party software packages (e.g. SMTP servers) which integrate with the thresholds module. Using values that match with the severity levels used by other systems is recommended. For example, if you are sending traps to a network management system that assigns traps to severities CRITICAL, HIGH, MEDIUM, or LOW, use these values.

THRESHOLD-SQL

SQL clauses that constitute the main body of the threshold query. Columns from property and/or data tables may be used. Prefix columns from the property table with "**p.**"; prefix columns in the data table with "**d.**". For example, if the property table being checked contained a column for CIR, and the data table contained a column for bytes_transmitted, it would be possible to determine if the bytes_transmitted exceeded the CIR by using the following SQL clause:

```
<Data>d.bytes_transmitted &gt; p.cir</Data>
```

Examples of Threshold Policy Definitions

A number of examples of policy definition files are included with the thresholds module. You can find them in the following directories:

UNIX

```
$DPIPE_HOME/packages/Thresholds/ThresholdExamples.ap/xml
```

Windows

```
%DPIPE_HOME%\pacakges\Thresholds\ThresholdExamples.ap/xml
```

Understanding Policy Definitions

This section contains a sample policy definition and explanation.

Sample Definition

```
<OVPI>
  <ThresholdPolicy Category="THRESHOLD-EXAMPLE">

    <MaxAge>
      <DeltaTime Value="1" Units="HOURS"/>
    </MaxAge>

    <DataTable>R_threshEg</DataTable>

    <Constraint Type="SQL">
      <SQL>
        <PropertyTable>K_threshEg</PropertyTable>
      </SQL>
    </Constraint>

    <Variables>
      <Variable Name="utilisation">
        <Data>((d.ifinoctets * 8 * 1000) / (60 * (1+ d.delta_time)))</Data>
      </Variable>
    </Variables>

    <UserDefs>
      <UserDef1>d.received_usec</UserDef1>
    </UserDefs>

    <Thresholds>
      <Threshold Name="EXAMPLE1" Severity="HIGH" SLA="True">

        <Rule>
          <Data>(d.ifinoctets * 8 * 1000) / (60 * (1+ d.delta_time)))
                                              &gt; p.util_threshold)</Data>
        </Rule>

        <Display>
          <Data>Utilisation = v.utilisation, limit = p.util_threshold</Data>
        </Display>

      </Threshold>

    </Thresholds>
  </ThresholdPolicy>
</OVPI>
```

Explanation

The statements above define a threshold in the category THRESHOLD-EXAMPLE. The category is an arbitrary name that can be used (with Severity) to identify groups of thresholds. This mechanism is used to associate threshold breaches (or clears) with actions.

The maximum age of data that will cause an exception is set to one hour. Data samples are checked only once at most. If a sample is either older than the last sample checked (for a particular object) or the sample is older than the maximum age specified in this clause, it will be ignored.

Data from the table “R_threshEg” will be checked. The table has a related property table: “K_threshEg”.

A variable called “utilisation” is defined. Any variables defined can be used in “display” clauses (described below).

A user defined field is created. This is passed directly to output.

A single threshold rule, EXAMPLE1, is defined. The severity associated with this threshold is HIGH and, because the SLA tag is defined, any actions generated by this rule will have the SLA flag set to True.

The rule checks whether the calculated value for circuit utilisation is greater than the limit stored in the property table. Different objects can have different limits.

A display clause is defined and contains the variable defined above, some text, and the limit value from the property table. If the threshold is breached, the resulting string will look similar to this:

“`Utilisation = 93, limit = 90`”

6 Troubleshooting

This chapter explains how to:

- Troubleshoot error and warning messages
- Troubleshoot problems caused by the thresholds.pl file not running

In OVPI 5.0, the thresholds functionality logs to the website.log file. The perl script thresholds.pl will continue to log to the trend.log file, but you can usually obtain more detailed data from the website.log file.

Error and Warning Messages

The following table, sorted alphabetically by message, provides recommended responses to specific error messages.

Message	Type	Suggested Action
Cannot find system information Error code: 10	FATAL	Use the system manager component in the Management Console to identify a database system as the default collector database. Usually this is the local host.
Failed to lock rules file (another instance may be running) Error code: 11	FATAL	The requested policy is still in use. Wait and try again.
Invalid property table Error code: 12	FATAL	Make sure the key table specified in the policy file matches the key table defined in the database.
Some threshold actions reported errors. See log file for more details. Error code: 99 Reason: The threshold action (SNMP, User-Script, or Mail) reported an error during processing	FATAL	You can find additional information in the `website.log` file. Verify that the thresholds policy file and threshold actions are correctly formatted and that the required statistics appear in the key and data tables.

Message	Type	Suggested Action
Unknown error has occurred at <LOCATION> Error code: 99 This error code is usually followed by a reason message and line number that HP Technical Support can use to help you resolve the problem.	FATAL	You can find additional information in the `website.log` file. Verify that the thresholds policy file and threshold actions are correctly formatted and that the required statistics appear in the key and data tables.

Running the thresholds.pl File

On UNIX systems, check that execute permission has been granted to the files in the Scripts directory, located beneath the $DPIPE_HOME directory. Run the following command:

```
ls -l $DPIPE_HOME/scripts/thresholds.pl
```

If execute permission has been granted, a message similar to this message appears:

```
-rwxr-x--x 1 trendadm adm 25591 Aug 24 19:42 thresholds.pl
```

Execute permission for the current user is shown by the fourth letter in the permission string ("`-rwxr-x--x`" in the example above) and must be set to "`x`".

Debugging

Log entries directly from the threshold module are written to trend.log, however, the module calls functions located in OVPI's Java based engine. Any error logging from these calls is written to website.log.

If a threshold definition is not working as it should you should check the following:

- Is the OVPI server running?
  - For Unix systems check the daemon is running, on Windows check the service is running.
- Are all actions correctly defined?
  - Ensure that "category" and "severity" identifiers do not contain spaces or special characters (e.g. quotes or hash symbols).
  - Ensure that servers are identified using a valid IP address or resolvable name.
  - Ensure that validly formatted email addresses are used for both "from" and "to" parameters.
- Are all XML definitions correctly constructed?
  - Check that the XML file be loaded into an XML editor or browser
  - Ensure that all clauses, tags and values meet the requirements described in this document.

If after checking these you are still experiencing problems the following may help:

1. Comment out all thresholds entries in trendtimer.sched file.
2. Deactivate all actions using the “modify” forms to change the category to “NOT_IN_USE” or some other suitable string.
3. Identify any status tables used by the threshold module. These will all appear under the thresholds category and be named “RTH*”.
4. Delete any TEEL files associated with the “RTH*” tables identified above found in `$DPIPE_HOME/lib` (UNIX) or `%DPIPE_HOME%\lib` (Windows).
5. Drop the tables identified above using table manager from the OVPI console.
6. Truncate the E_threshExcept table using table manager from the OVPI console.
7. From the command line, start the thresholds module using the same command as found within the .pro which you commented out of trendtimer.sched.

If this is successful, you should restore desired actions one at a time, repeating steps 4 through 7 after each.

Index

Symbols

&gt (greater-than symbol), 31

&lt (less-than symbol), 31

A

actions
- Category values, 13
- default, 14
- defining, 13
- disabling, 27
- maintaining, 13
- Severity values, 13
- SMTP-MAIL, 19
- SNMP-TRAP, 15
- supported, 15
- USER-SCRIPT, 23

asterisk (wildcard), 13

C

category, defined, 14

CATEGORY_NAME value, 33

community string, changing, 14

configuration files, installing, 7

configuring advanced features, 29

CONSTRAINT-NAME value, 34

CSV file, 23

D

database tables, creating, 7

DATA-TABLE value, 33

default actions, 14
- modifying, 14

DISPLAY-SQL value, 35

E

e-mail, 19

error messages, 39

F

forms for maintaining action definitions, 13

G

greater-than symbol, 31

I

installation
- prerequisites, 9
- Thresholds Module, 10
- verifying, 11

J

Java interface, 8

L

less-than symbol, 31

M

MAXIMUM-AGE value, 33

messages, troubleshooting, 39

O

Oracle, 8

OVPI clause, 32

ovpiThresholdBreach traps, 15

ovpiThresholdClear traps, 15

OVPI Timer
- starting, 11, 12
- stopping, 10, 12

P

perl script, 8

Product Manuals Search (web page), 8

PROPERTY-TABLE value, 34

R

removing Thresholds Module, 12

S

severity, defined, 14

SEVERITY value, 35

SLA-FLAG value, 35

SMTP mail actions
- creating, 19
- updating, 21

SNMP port, changing, 14

SNMP-TRAP actions
- creating, 15
- updating, 17

software prerequisites, 9

SQL clauses
- in a threshold query, 35
- passed to output, 35

SQL-CONSTRAINT value, 34

Sybase, 8

T

tables, creating, 7

Threshold Examples package, 7

THRESHOLD-NAME value, 35

ThresholdPolicy clause, 32

thresholds
- checking, 29
- configuration files, 31
- policy
  - recommendation, 13
- policy definition files, 31
  - construction of, 31, 32
  - contents of, 30
  - examples, 35
  - naming, 31
- procedure file, 29
- scheduling checks, 29
- sub-packages, 13
  - components, 29
- testing script, 11

thresholds.pl file, 39, 40

THRESHOLD-SQL value, 35

trap destination, changing, 14

traps, ovpiThreshold, 15

trend.log file, 39

trendtimer.sched file, 29

troubleshooting, 39

U

uninstalling Thresholds Module, 12

upgrading Thresholds Module, 10

USERDEF-SQL value, 34

user script actions
- creating, 23
- updating, 24

V

VARIABLE-NAME value, 34

VARIABLE-SQL value, 34

verifying installation, 11

W

website.log file, 39

wildcards, for Category and Severity, 13

X

XML files, advice for modifying, 31