CHAPTER 12

Setting Alarms Using Watchdog

Introduction

It is very useful to be able to monitor a portion of your network, or a specific network device, to determine whether a specific condition occurs. You can perform such monitoring when you suspect a fault in the segment or device, or just to be notified if it develops problems. Using TrafficDirector tools, you can monitor network variables as diverse as a rising data rate or the failure of a network device.

It is usually impractical to monitor a segment or device visually. Instead, you can use Watchdog to set alarms on the variables you want to monitor.

An *alarm* is a definition of a condition based on either rising or falling data rates, or both. When this predefined condition occurs, it is called a *trap*. When you set an alarm on a network device, the alarm detects a trap when it occurs. Then it does two things:

- It records the trap in the agent.
- It sends a notification that a trap has occurred to the TrafficDirector.

When a trap occurs, the Alert Monitor on the TrafficDirector window blinks until you acknowledge it by selecting it. You can double-click on the icon to launch the Alert Monitor application. You can also create UNIX script files that execute network or system functions when an event occurs.

Watchdog lets you establish multiple alarms on selected events associated either with an agent/domain combination, or with a resource. Then it sends you an alarm message when the data reaches the predefined threshold.

You can view a list of previous alarm messages using the Alert Monitor tool.

In this chapter, you'll learn how to start Watchdog from TrafficDirector application tools, and how you use it to set alarms. You'll also see how to view a list of existing alarms using Alert Monitor.

Starting Watchdog

You start Watchdog by launching it from any of four applications:

- Domain Manager
- Protocol Monitor
- Traffic Monitor
- Resource Manager

You launch Watchdog from Domain Manager, Protocol Monitor, and Traffic Monitor to set alarms on agent/domain combinations. You launch Watchdog from Resource Manager to set alarms on a network resource.

Starting Watchdog from Domain Manager

To start Watchdog from Domain Manager:

Step 1 Select an agent or agent group in the TrafficDirector window.

Step 2 Click on Domain Manager. The Domain Manager window appears.

Step 3 Select the Agent/Domain combination on which you want to set a alarm from the List Box in the Domain Manager window.

Step 4 Select Watchdog from the **Tools** menu. The Watchdog window appears. See "Using Watchdog to Set Alarms" for instructions on setting alarms.

Starting Watchdog from Protocol Monitor

To start Watchdog from Protocol Monitor:

Step 1 Select an agent or agent group on the TrafficDirector window.

Step 2 Start Protocol Monitor. The Protocol Monitor window appears.

Step 3 Either select Watchdog from the **Tools** menu in the Protocol Monitor window, or click on the agent for which you want to set the alarm. The Launch Application window appears.

Step 4 In the Launch Application window, select Watchdog as the application, then select the agent and domain on which you want to set an alarm.

Step 5 Click on **Launch** to bring up the Watchdog window, or **Cancel** to return to the Protocol Monitor window.

Step 6 If you selected **Launch**, the Watchdog window appears. See "Using Watchdog to Set Alarms" for instructions on setting alarms.

Starting Watchdog from Traffic Monitor

To start Watchdog from Traffic Monitor:

Step 1 Select an agent or agent group on the TrafficDirector window.

Step 2 Start Traffic Monitor. The Traffic Monitor window appears.

Step 3 Either select Watchdog from the **Tools** menu on the Traffic Monitor window, or click on the agent for which you want to set the alarm. The Launch Application window appears.

Step 4 In the Launch Application window, select Watchdog as the application, then select the agent and domain on which you want to set an alarm.

Step 5 Click on **Launch** to bring up the Watchdog window, or **Cancel** to return to the Traffic Monitor window.

Step 6 If you selected Launch, the Watchdog window appears. See "Using Watchdog to Set Alarms" for instructions on setting alarms.

Starting Watchdog from Resource Manager

When you launch Watchdog from Domain Manager, Protocol Monitor, or Traffic Monitor, you set alarms on agent/domain combinations. However, you can also use Watchdog to set alarms on network resources. To do this, you must launch Watchdog from Resource Manager.

To launch Watchdog from Resource Manager:

Step 1 On the TrafficDirector window, select the agent for which you want to view resources.

Step 2 Select Resource Manager. The Resource Manager window appears.

Step 3 Select a resource from the list that appears in the Resource Manager window.

Step 4 Select Watchdog, either from the **Tools** menu or by clicking on the **Watchdog** button. The Watchdog window appears. See “Using Watchdog to Set Alarms” for instructions on setting alarms.

Using Watchdog to Set Alarms

Once you have launched Watchdog from one of the four applications, you can set alarms for the agent, agent group, or resource you selected. When you want to set an alarm, follow these steps:

Step 1 Select the agent, agent group, or resource on which you want to set the alarm and launch Watchdog as described in the previous section. The Watchdog window appears. The selected agent and domain names appear at the top of the window.

Step 2 Use the **Variable** menu to select the variable on which you want to set the alarm. Your choices depend on whether you selected an Ethernet segment or a Token Ring segment. You must choose a variable, there is no default. Choices that do not apply to the type of network segment are grayed out. The **Variable** menu choices are:

- Ethernet statistics
- Token Ring Promiscuous Stats (token ring segments only)
- Token Ring MAC Stats (token ring segments only)
- FDDI Stats (FDDI segments only)
- WAN Stats (WAN segments only)
- Host Stats (host windows only)
- Conversation Stats (host windows only)
- Miscellaneous
- Proxy Variables

Step 3 Fill in the fields in the Watchdog window. The fields are described below, in the section “Watchdog Selection Fields.”

Step 4 Click on the **Add** button. TrafficDirector adds the new alarm.

When the variable you’ve selected exceeds the thresholds you set in the Watchdog window, the agent or proxy resource sends a trap to the TrafficDirector. This triggers the Alert Monitor (see ”Viewing a List of Traps Using Alert Monitor”) and executes a script file, if you specified one in the Watchdog alarm set up (see “Using Traps to Execute UNIX Script Files”).

Watchdog Selection Fields

This section lists and describes the Watchdog fields you fill in when you want to add an alarm to an agent or proxy resource.

Selection Field	What it Displays or Selects
Variable	Indicates the variable you selected with the **Variable** menu (described above). This field is filled in automatically.
Sample Type	Selects **Per Second Rate**, **Delta Value,** or **Absolute Value**. This determines whether the alarm is triggered on the data rate, such as packets per second, a change in data rate, or on an absolute value, such as the number of packets counted. The default sample type is **Per Second Rate**.
Sample Interval (secs)	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. The value must be a decimal number. The allowed range is 1 - 3600 seconds.
Generate Trap When	Selects **Rising Threshold**, **Falling Threshold**, or **Either**. Values must be in decimal form and must be within the range of the variable being monitored. The default threshold is **Rising Threshold**. • **Rising Threshold.** When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was *less than* this threshold, the agent generates a single event. It does not generate another such event until the sampled value falls below this threshold and reaches the Falling Threshold. • **Falling Threshold**. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was *greater than* this threshold, the agent generates a single event. It does not generate another such event until the sampled value rises above this threshold and reaches the Rising Threshold. • **Either**. The agent generates an event when either the rising or the falling threshold is reached.
Trap Community	Watchdog sends trap messages to each host registered for that community. The host from which a trap is installed is automatically registered when you create the trap. You can register additional hosts to receive traps for the community using the **dvwatch** utility (see Chapter 15, “Using Command Line Utilities”). The default trap community string is **public**.
Threshold Type Rising/Falling	These fields let you define rising and falling trap thresholds.

Selection Field	What it Displays or Selects
	• **Trap Descriptions.** When a rising or falling alarm condition is reached, Watchdog transmits the text message entered in this field as part of the trap message to the reporting console. The default descriptions are **Rising threshold reached** and **Falling threshold reached**. • **Value**. The value that triggers the trap. Values must be decimal. The allowed ranges depend on the variable you select. • **Severity**. A relative rating of the severity of the trap. The value range is from 0 - 999, decimal. The severity rating of a trap appears as part of the trap information in the Alert Monitor. You can also use the severity rating of a trap in script files. (See Program Info.) These scripts let you use trapping events to trigger actions in TrafficDirector or in UNIX. • **Program Info**. You can write UNIX script files and use traps to execute the scripts. In this way, you can use a trap to trigger actions in TrafficDirector or in UNIX. You can write different script files for rising or falling thresholds. You enter the script name in the Program Info field. Writing UNIX script files is discussed in the section "Using Traps to Execute UNIX Script Files."
Last Sample	The system fills in the value of the parameter selected for the last sample period.
Last Rising Trap	The system fills in the date and time of last trap condition caused by reaching the rising threshold.
Last Falling Trap	The system fills in the date and time of last trap condition caused by reaching the falling threshold.

Deleting an Alarm

You can delete an existing alarm by filling in the information for that alarm in the Watchdog window, then clicking on the **Delete** button.

Getting Agent Information

To get system and interface information for the agent you selected when you launched Watchdog, do the following:

Step 1 Either select **Agent Info** from the **Tools** menu, or click on the **Agent Info** button. The Agent Information window appears.

Step 2 When you are finished viewing the agent information, click on **OK** to exit the Agent Information window.

Exiting Watchdog

To exit the Watchdog window:

Step 1 Select the **File** menu.

Step 2 Click on **Exit**.

Viewing a List of Traps Using Alert Monitor

Traps can be generated by any agent in the network, even agents that are not related to TrafficDirector. The Alert Monitor's trap listing shows all traps sent to the IP address of your TrafficDirector console, even if they are not RMON-related traps.

The trap list displays all the messages sent on the date shown in the date field at the top of the Alert Monitor window. Each local agent also logs traps, and you can gain access to them through an inquiry to the specific agent.

When an alarm occurs, the Alert Monitor alarm clock icon at the bottom of the TrafficDirector main window flashes until you acknowledge it by clicking on the icon. Click on the icon a second time to display the Alert Monitor window.

To view a list of traps:

Step 1 Select **Alert Monitor** from the TrafficDirector main window. The Alert Monitor window appears.

Step 2 Using the date field buttons at the top of the Alert Monitor window, select the date for which you want to view traps. A list of traps recorded for that day appears in the list box.

When you select a specific trap in the list box, information on that trap appears in the box beneath the list box.

Refreshing the Alert Monitor Display

You can update the information in the list box to show new traps. To do so, click on the **Refresh** button.

Printing Trap Information

You can print the contents of the Alert Monitor list box for future reference. To print the contents of the list box:

Step 1 Select the **File** menu.

Step 2 Click on **Print**. TrafficDirector prints the list box information on your default printer.

Exiting the Alert Monitor

To exit the Alert Monitor window:

Step 1 Select the **File** menu.

Step 2 Click on **Exit**.

Using Traps to Execute UNIX Script Files

When an alarm condition occurs, the alarm generates a trap. The agent sends the trap to TrafficDirector, which causes the Alert Monitor icon on the TrafficDirector Main window to blink repeatedly until you click on it to display the Alert Monitor window.

You can also use traps to execute UNIX script files. These script files can perform Alarm functions, such as sending mail messages or printing the trap information. They can also perform actions in the network, such as changing the speed of a router.

You can pass two variables from the trap to your UNIX script file, the agent name, and the severity of the trap.

For example, you may want to automatically change the speed of a WAN router if utilization reaches a certain threshold. You can write a script to change the router speed if an alarm based on utilization triggers a trap.

As a second example, you can generate a snapshot of the network if a certain threshold is reached. You can do this by writing a script file that runs the command line utility **dvsnap** when a certain threshold is reached.

Finally, you might want UNIX to sound an audible alarm and flash a screen message if a Severity 1 trap occurs.

This sample script file sends a mail message when a trap is received:

```
#
# Sample shell script to be executed upon trap reception
#
# This sends a mail message to the user showing the top hosts & conversations
#
echo High utilization trap received from agent $1, priority $2 > temp.$$
echo Top 10 hosts: >> temp.$$
$NSHOME/bin/dvsnap $1 ALL HOST 30 10 >> temp.$$
echo Top 10 conversations: >> temp.$$
$NSHOME/bin/dvsnap $1 ALL CONV 30 10 >> temp.$$
mail ‘whoami‘ < temp.$$
rm temp.$$
```

To use traps to execute UNIX script files:

Step 1 Write the UNIX script file. Remember that you can use both the agent name and the severity level from the trap you want to use to execute the script file.

Step 2 Create the alarm in Watchdog as described in this chapter (see "Using Watchdog to Set Alarms"). Enter the name of the script file in the appropriate **Program Info** field (see "Watchdog Selection Fields"). You can have two separate **Program Info** files, one for a rising threshold and one for a falling threshold.

Step 3 Add the alarm. The script file will execute each time the alarm creates a trap.