Framework Management Layer User's Guide

Alarm-Signaling Functions

4/14/2025

Contents

- 1 Alarm-Signaling Functions
  - 1.1 Alarm Detection
  - 1.2 Default Alarm Processing

Alarm-Signaling Functions

Maintenance events that the user may want to become aware of and react to immediately are communicated as Standard-level log events that Genesys applications generate. Each log event is assigned a unique number, which identifies the situation being reported. Thus, the alarm-signaling function of the Management Layer is based on the capability to detect the log events that have been pre-configured to trigger alarms and to send them to an alarm-processing center. In addition, the Management Layer monitors certain system and SNMP variables, which you can also use for alarm signaling.

This topic describes how the Management Layer implements an alarm system, and what is required to incorporate it into your configuration. For specific instructions, refer to Alarms.

Alarm Detection

The Management Layer detects alarms by matching the following against the alarm conditions you have configured:

- Log events coming from all applications
- The thresholds of the system performance variables (such as CPU or memory usage) and of local or remote SNMP variables. (SNMP threshold monitoring is available only when you have enabled SNMP functionality.)

SCS provides the same alarm-reaction processing for both Alarm-detection mechanisms.

Using Log Events for Alarm Detection

To use a log event to trigger an alarm, you must configure an object of the Alarm Condition type and associate it with a log event ID in the Configuration Layer. When you configure an Alarm Condition, you do the following:

- Specify the log event that should trigger this alarm during runtime.
- Assign an alarm category.
- Define the source of the alarm.
- Set conditions for automatic alarm clearance.

The source of an alarm can be a specific application, all applications of a particular type, or all applications of the interaction management network. In each case, the resulting alarm message contains the application name. So, you can know the exact source of the alarm.

> **Tip**
> You can also use log events of the Standard, Interaction, or Trace levels to trigger an alarm message.

Each application that can generate an alarm must be configured with a connection to Message Server to which it is able to send log events of the appropriate level. Otherwise, the Management Layer is unable to detect the log events. Once configured, an alarm condition automatically triggers an alarm in response to an occurrence of the log event on which the alarm condition is based. If the same log event occurs subsequently while the alarm is active, the clearance timeout is reset.

As previously noted, the alarm detection takes place in Message Server, so you must connect the potential sources of alarms to Message Server for alarm signaling to operate. If you are planning to use the recommended centralized logging function, your applications should already be connected to Message Server. Otherwise, you need to set up Message Servers and configure your applications to connect to them specifically for alarm-detection purposes.

> **Tip**
> If you are using Genesys Administrator 8.1.3, you can use the by using the Alarm Condition Wizard in Genesys Administrator. For more information, see the *Framework Genesys Administrator Help*.

The Configuration Layer also provides a number of preconfigured alarm conditions based on the events that cause service degradation in any environment. Before configuring your own alarm conditions, see if they may have been predefined in the Configuration Layer. For more information about predefined alarm conditions, see Predefined Alarm Conditions.

Using System Parameters and SNMP Thresholds for Alarm Detection

The alarm-detection mechanism for thresholds for system performance variables or SNMP variables is similar in many respects to the log-event-based mechanism. In particular, you must configure certain alarm conditions in the Configuration Database that indicate the values for the Management Layer to monitor.

When you are using thresholds for system performance variables, the Management Layer detects an alarm by periodically comparing the current value of the specified performance variable with the specified limits. If a change in the variable's value exceeds the specified limit, the Management Layer triggers an alarm.

When you are using SNMP variables as thresholds, the Management Layer detects an alarm by periodically comparing the current value of the specified SNMP variable, as identified by OID, with the specified limits. Currently, the following two SNMP variables are supported for this purpose:

- **gsClientExistNum** in table **gsInfoTable**
- **tsCallsExistNum** in table **tsInfoTable**

If a change in the variable's value exceeds the maximum limit of the specified minimum to maximum value range, an alarm is triggered. When the variable's value falls below the minimum limit of the specified range, the active alarm is cleared.

The Rising Threshold, which triggers an alarm when crossed *only if the value is rising*, must be a higher number than the Falling Threshold, which clears the alarm when crossed *only if the value is falling*. For example, if the Rising Threshold is 300 then the Falling Threshold must be less than 300.

This mechanism provides alarm signaling with both local SNMP variables—that is, variables from the Genesys MIB file, implemented locally in SCS—and with remote SNMP variables—that is, variables provided by third-party SNMP agents.

To monitor a variable of either type, use Genesys Administrator to create:

- An Alarm Detection Script
- A new Alarm Condition based on the Alarm Detection Script

For more information, see *Framework Genesys Administrator Help*.

Default Alarm Processing

Once it detects an alarm, Message Server sends it to Solution Control Server for processing. SCS processes the detected alarm in this way:

1. Stores the alarm in the system as active until it is removed manually, expires based on the configurable timeout, or is cleared by another log event, which you can optionally define in the Alarm Condition object as an automatic removal condition.
2. Generates log messages about every alarm detection and its removal.
3. Passes the alarm information and a list of all the running solutions that the alarm may affect to Genesys Administrator to display them for the user. SCS only passes alarm information about objects (such as applications or hosts) that the user currently logged in to Genesys Administrator has permissions to view. If necessary, the user can then take the appropriate action.

For alarm processing to take place, you must connect SCS to the Message Servers that detect the alarms.

Whenever you start Genesys Administrator, it automatically displays all active alarms currently registered in SCS as long as you have permissions to view the objects associated with the active alarms.

For more information, see *Genesys Administrator Help*.

Customized Alarm Processing

In addition to relying on the default alarm-processing actions, you can configure other actions (called Alarm Reactions) that the Management Layer is to take when it detects a specified alarm, such as:

- Shutdown a specified application.

- Start up a specified application.
- Restart the application that reported the alarm.
- Start up a specified solution.
- Send an email message with detailed information about the alarm to specified Internet addresses.
- Switchover operations from the application that reported the alarm to its backup application, for applications running in primary, backup, or either mode.
- Send an SNMP trap with detailed information about the alarm to a general-purpose network management system.
- Execute an operating system command.
- Change the value of a configuration option of a specified application, including the application that reported the alarm. (If the proposed change to an option is for a section or option that does not exist, the system creates both.)

Most of these reactions do not require any special arrangements. However, the switchover reaction type requires that the application in question have a backup application configured and running. The application restart and switchover mechanisms are described in detail in Fault Management Functions.

If you wish to use SNMP trap capabilities, you must install an SNMP Master Agent and configure your Solution Control Server to connect to it. You can use Genesys SNMP Master Agent or a third-party SNMP Master Agent you already have within you network management system—as long as it is compliant with the AgentX protocol. For instructions on these procedures and for detailed specification of the SNMP trap to which the Management Layer converts the alarms, see SNMP Support.

Though the Management Layer itself does not provide paging notifications, you can arrange these through the supported email or SNMP interfaces using your email server or network management system, respectively.

An alarm reaction is configured in the Configuration Database as a Script object of the Alarm Reaction type. For runtime execution of a particular alarm, you must associate the alarm reaction with the corresponding Alarm Condition object. You can configure any combination of supported reactions with respect to any alarm condition. The easiest way to do this is by using the Alarm Condition Wizard in Genesys Administrator.

You can configure alarms in the Management Layer that execute alarm reactions not only at alarm activation, but also at alarm clearance. To achieve this, add the alarm reaction Scripts that should be executed when the alarm is cleared to the Clearance Scripts list of the corresponding Alarm Condition object. You can also use the Alarm Condition Wizard in Genesys Administrator to accomplish this.

You can also use the mlcmd utility to clear all active alarms raised by an application or on the basis of a specified Alarm Condition.