



FAULT MANAGEMENT

Introduction

Today, more than ever, managing heterogeneous networks for maximum ROI not only requires the ability to perform meaningful analysis of data derived from multiple, often geographically dispersed sources. It also relies heavily on the aptitude to detect and correct both potential and actual faults, which can arise from any single component of your mission-critical IT infrastructure. On top of an intelligent monitoring and data analysis mechanism, fault management is crucial in moving an organization forward in these highly competitive and aggressively cutthroat times.

Simply put, fault management is the ability to locate faults, determine their cause, and set appropriate corrections. This entails identifying and finding problems or irregularities within the whole gamut of the infrastructure, pinpointing the origin of the setbacks, and troubleshooting the problem elements at their source and immediate location. On an even higher plane, it also espouses the golden rule of prevention—that proactive approach of stopping negative conditions in their tracks even before they become real glitches in the system.

Using MAX's Fault Management Tools

Fault management is one of the most commonly deployed infrastructure management elements. In MAX, this core element helps detect and notify organizations of faults and service outages as and when they materialize.

MAX offers different levels of fault management with our solutions. The first level involves the generation of events/alarms logs that record all instances of events and alarms for easier tracking. The second level features event correlation capabilities, where MAX is able to instantly nail down the root cause of the problems, and speed up the effort and time to fault resolution. The third level includes the facility to incorporate additional information (comments) to events entries, facilitating the event escalation process. Here you can also customize the mode of delivery for all notification alerts to be sent to appropriate personnel—by way of email, paging, and SMS, among others.

With MAX Infrastructure Management Suite, performing fault management is made easy and convenient, helping your IT infrastructure become reliably efficient and unfailingly resilient. In a nutshell, it provides the following activities:

- Continuous monitoring and collection of statistics on networks, workstations, traffic conditions, and usage so potential faults can be forecast and avoided
- Setting threshold conditions that can alarm you of conditions that may cause failures or lead to real problems

- Setting alarms that warn of performance degradation on servers, routers, and wide area network links
- Setting alarms that warn of resource usage problems, such as a server that is almost out of disk space
- The ability to remotely control workstations and other devices, and execute batch files that address and troubleshoot known problems as a result of fault detection
- The ability to perform some or all of the preceding tasks from a single management location, which may be extremely remote from some sites

MAX: The Complete Fault Manager

MAX, through its Events and Alarms engine, empowers you to detect potential and actual faults as they occur, and better yet, before they happen and/or impact your services. At the point that these glitches materialize from any point in the whole infrastructure—network equipment, devices, workstations, servers—MAX generates an events and alarms log that, together with the notification module, can facilitate the delivery of alerts to selected personnel for prompt action. At the first hint of trouble, MAX can alert the designated personnel at once, even trigger self-remedy applications that automatically solve problems, thus reducing the *mean time to repair* (MTTR).

In MAX, events are occurrences or activities related to the monitored infrastructure, or manifestations of the inner workings of the network and its many components, which can be readily detected by MAX as having an impact to system performance and availability. Events include instances where resources are detected as either up or down, an interface is deleted, or the system is rebooted, among others. The events correlation engine is built-in within MAX, and when activated, allows related events to generate the corresponding root cause alarms and dependent alarms; you can also enter comments specific to individual events.

As part of the real-time fault management mechanism, MAX offers the root cause identification and assessment utility within the Alarms module, which is designed to isolate network issues and help ensure maximum network availability. MAX continuously applies algorithms to its object-oriented network model to detect and isolate failure points, determine the cause of failure, and correlate events across multiple resources to identify the potential impact on other elements in the chain, in particular, and within the infrastructure, in general.

MAX offers a highly intuitive, graphical user interface that ensures clear presentation of a wide range of events and information—from individual root cause alarms and network-wide failures, to notification recipients and options for notification acknowledgement and escalation. MAX is ideal for high-level to minute-detail analysis, with a self-adaptive configuration that requires very little implementation effort on the part of the user. Highly customized or complex networks will benefit from the Events and Alarms engine, an advanced root cause analysis and events correlation tool within MAX Infrastructure Management Suite.

MAX's complete fault management mechanism—from root cause identification and assessment to alerts delivery and problem resolution—deliver the following:

- Facilitates automated responses to alarms. MAX offers a broad range of automated, pre-defined responses to network events, including paging, emailing, acknowledging an alarm, and invoking user-configurable scripts that allow them to define a broader range of actions. It maintains a user-defined contact list for notifying selected personnel of alarm conditions, and supports multiple contacts

per alarm filter; notification methods include email, paging, and SMS, beep (workstation alerts), SNMP traps, and batch file execution.

- Defines dependency relationships among network elements. The events correlation engine operates by creating parent-child relationships between managed elements of the network. The selection criteria for the child elements can include the resource name, the sub-resource name, and the severity of the alarm. When alarms are triggered by events related to these child elements, automated responses include updates to alarm severity, updates to alarm message text, and script activation or notification delivery.
- Features easy-to-use GUI, requires no complicated syntax, and is completely user-configurable. MAX is easy to use for all types of users across the enterprise. Highly intuitive screens walk users through initial setup and provide a wide range of real-time information as resources are monitored and alarms are activated. It provides users with standard root cause analysis capabilities that help network managers isolate network issues, respond to them quickly, and—ultimately—provide a higher quality of service to customers.
- Integrates with OSS-driven help desk services and trouble-ticketing software. MAX provides for the flawless integration with applications and utilities using Open Source Software, which work and communicate with MAX to invoke user-configurable scripts that allow them to execute several fault resolution actions, such as putting a device into maintenance mode, and connecting to a 24-hour help desk. Additionally, fault alarms can be configured to generate trouble tickets in systems such as Remedy™ and other event notification systems. The same fault alerts can in turn be formatted as an input or hook to any events management system to automatically open trouble tickets.
- Integrates with ISS RealSecure in security-based alarms. MAX can monitor and safeguard the secure operations of intranet servers and workstations, and serve as central manager for alerts and notifications for managed firewalls/VPNs and ISS RealSecure products. Here MAX forwards alarms/events alerts—from server downtime to security violations—to the administrator by SMS, email and/or workstation pop-ups. MAX in turn sends network-based SNMP traps on one hand, and security-based SNMP traps (which contain information on events/alarms descriptions, date/time and type of violation, as generated by firewalls and ISS RealSecure) on the other. The designated personnel then receive the trap messages by SMS or pop-ups, thus informing them of security problems in near-real time. MAX integrates with many other types of intrusion detection systems (IDS) in the market.
- Features a multi-purpose SNMP trap API. As an SNMP platform, MAX has acquired the ability to receive and process SNMP traps, although converting trap information into useful data remains internal to MAX. This means that news trap from new devices, though supported by MAX, will not provide user-friendly messages. MAX will need to support more and more traps from different devices/applications in the future. To facilitate this, a standard API has been developed to enable the processing of traps and the delivery of meaningful messages. By using the standard API, the special trap converter modules can be developed independently from the core MAX software by either Equator One, your own engineers, or third parties.