PATROL® Diagnose:
A ModelingApproach to Root-Cause Analysis

Contents

Overview

According to studies, 50% to 80% of system downtime is spent diagnosing problems to identify their root causes. This results in time wasted and revenue lost. The solution is to offer a system that helps operators pinpoint the root causes or that decreases the number of root-cause candidates. BMC Software's PATROL Diagnose solutions do just that.

PATROL by BMC Software provides operators of enterprise computing environments with astonishing amounts of observation information. While this information provides an incredibly powerful tool for monitoring large systems, in many cases, the number of managed objects creates an environment that becomes too difficult for operators to manage effectively.

Additionally, maintaining the availability of systems is a huge and demanding role. Quickly and decisively identifying the root cause of a service loss or outage takes time, and any given application outage can be masked by hundreds of sympathetic events and alarms. This makes it difficult for even a skilled administrator to determine the root cause. Further complicating the matter is that multiple, closely timed events can appear to be a single stream of events when in fact, they can be totally independent, unrelated failures, all with different root causes.

Many IT organizations rely on experts from multiple domains (such as network, database, or operating systems) to manage each specific area of their enterprise. Prior to fixing a problem or failure, these experts must determine in which domain the problem resides. As each expert researches and responds, the clock is ticking. The unfortunate and unnecessary results include redundant work, increased maintenance, increased costs and extended downtime.

BMC Software's PATROL Diagnose Solution

PATROL Diagnose solutions are created using a highly adaptable, fundamental and generic technology from which many application-specific solutions can be derived. By automatically isolating the root cause of availability and performance problems, PATROL Diagnose solutions let you quickly diagnose problems and rapidly restore system performance into compliance with defined service-level agreements. This translates into less time spent reacting to symptoms and more time fixing the problem.

PATROL Diagnose solutions address intelligent diagnosis of the root cause of a loss of service by:

- Diagnosing the root causes of failures related to applications, operating systems, middleware, RDBMSs and network connectivity problems
- Displaying the services affected by a failure

- Distinguishing true root causes from sympathetic symptoms
- Dynamically adapting to network changes
- Providing optional tests that can be executed directly from the console

PATROL Diagnose solutions go beyond simple problem identification by actually automating resolution. They let you create tasks that perform corrective actions; these tasks are executed based on the outcome of the root-cause diagnosis.

How BMC Software's Root-Cause Analysis (RCA) Solution Works

PATROL Diagnose solutions use the following information to determine the service or application failure's root cause:

- Preconfigured proprietary cause-and-effect models
- PATROL events
- PATROL-discovered application topology

The RCA solution analyzes the alarms generated by PATROL, diagnoses the root causes of these alarms and displays the results in the PATROL Console. To diagnose root causes, PATROL Diagnose solutions use fault propagation models developed by domain experts for managed objects. For example, the PATROL for Microsoft Exchange Server – Diagnose uses three models: IP device accessibility, Microsoft Windows NT domain servers and Microsoft Exchange application servers.

The flow of root-cause analysis modeling

Root-cause analysis is initiated by certain PATROL alarms or by IP accessibility failures. If a PATROL alarm triggers a root-cause analysis, PATROL Diagnose acknowledges the alarm within the PATROL application and creates a diagnosis manager instance, which is displayed within the PATROL Console. The diagnosis manager instance contains all of the information that PATROL Diagnose gathers about the PATROL event, as well as the system failure it represents. This includes a list of faults that are suspected to be the root cause as determined by the modeling.

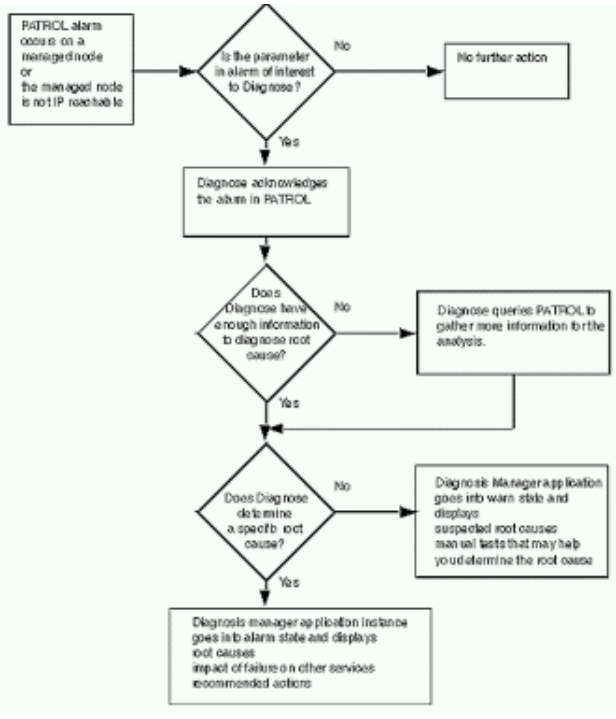

Figure 1 – This diagram depicts the logical flow of control for completing a root-cause analysis.

After creating the diagnosis manager instance, PATROL Diagnose uses its sophisticated cause-and-effect models to begin root-cause analysis. During the analysis, PATROL Diagnose may query the PATROL Agents on the managed nodes using predefined tests for more information.

If a suspected root cause cannot be eliminated or verified, it remains a suspect.

The PATROL Console is used to convey events to users using the PATROL hierarchical tree view of nodes, applications, instances and parameters. PATROL Diagnose displays the diagnosis manager as an instance in the PATROL Console under the Root-Cause Analysis application branch of the tree. This is shown in Figure 2. All the relevant information pertaining to a diagnosis manager instance is held in branches beneath it. The Known Tests branch contains any predefined tests that were executed to gather more information to complete the diagnosis. The Manual Tests branch contains tests that are not automatically executed because they are too intrusive or because the test requires operator input.

Figure 2 – This screen shot displays an exploded view of a diagnosis manager instance in the PATROL Console window.

Listed beneath the PATROL Events branch are symptoms that contain a parameter listing the text from the PATROL event initiating the analysis and a time stamp of when the event was received by PATROL Diagnose.

Displayed under the Root Causes branch are the root-cause instances that PATROL Diagnose has evaluated. Under each root-cause instance are two parameters: 1) the root-cause instance's status parameter, which displays the alarm state information; and 2) the root-cause instance's diagnosis parameter, which contains a time stamp of when the diagnosis was concluded. The projected impact of the failure, the recommended actions (if any) and the names of the known events that led to the diagnosis are also included.

The known events include the symptom that initiated the analysis and the name of the test that implicated the root cause. The projected impact can include information about the devices, services and applications affected by the failure.

If no specific root cause is found, PATROL Diagnose displays the suspected root causes in a warning state. It then suggests manual tests that can help determine the specific root cause. Because some of these tests consume system resources, PATROL Diagnose provides the option of executing the tests when they will not adversely affect the efficient operation of the enterprise. Tests can be executed directly from the PATROL Console.

In general, the diagnosis manager instance remains in an alarm state until the originating PATROL parameter returns to a non-alarm state, or until the IP accessibility failure is cleared. If an IP accessibility failure root cause is cleared, PATROL Diagnose re-examines other related root causes. This is done to ensure a complete diagnosis, which may not have been possible while the Agents involved were inaccessible. When the diagnosis manager

returns to a normal state, it remains displayed in the PATROL Console. The diagnose parameter displays the recovery time and the name of the PATROL event that led to recovery.

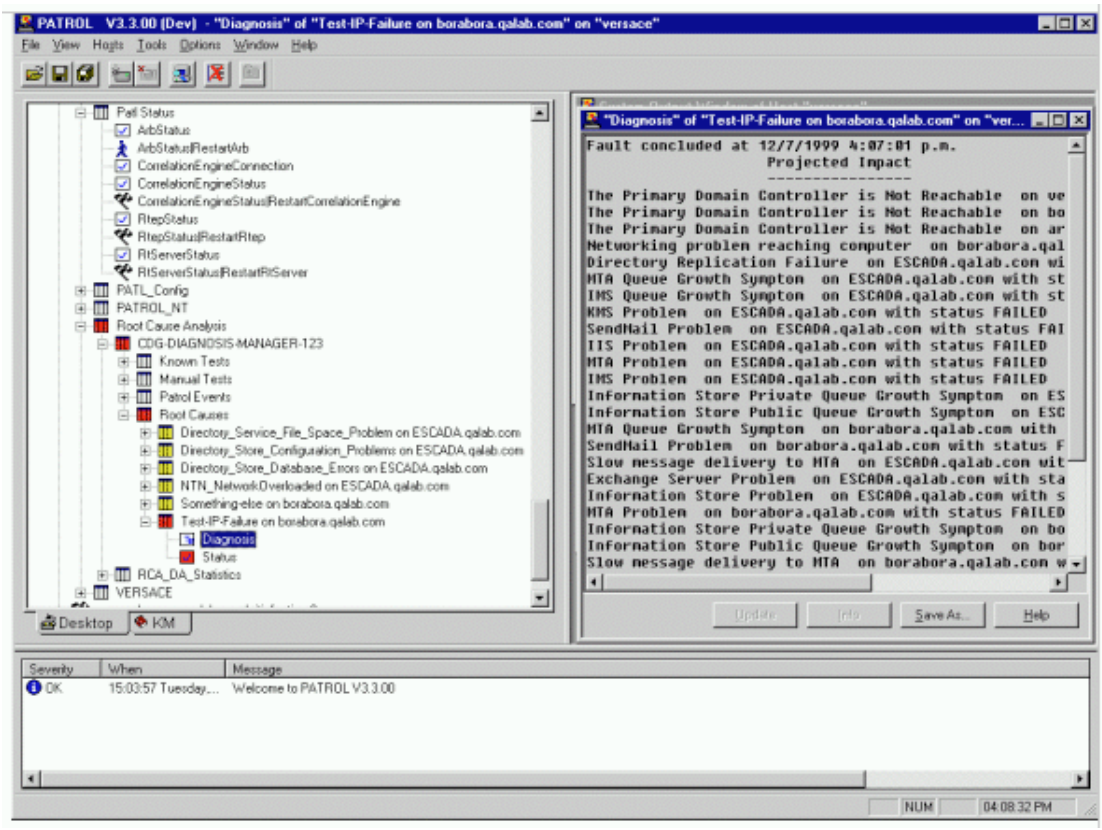

Figure 3 – All root-cause diagnoses are displayed as events in the PATROL Console.

Impact Analysis

When PATROL diagnoses the root cause of a failure, it also displays what services and managed objects are affected by the failure. PATROL alarms generated independently by the failure of these services can be treated as sympathetic alarms and ignored.

Operators can use PATROL to create a recovery action that automatically notifies the staff affected by the devices, as well as the person responsible for fixing the problem. This feature helps staff reduce recovery time by eliminating unnecessary troubleshooting.

Dynamic Updating of Topology

PATROL Diagnose uses dynamic discovery to update the enterprise topology (domain) map. The topology map used by the correlation engine during root-cause analysis consists of the topology information about network devices, operating systems and applications. As servers or applications are added or removed from the network, PATROL Diagnose detects these changes and automatically updates the map.

This unique capability makes it possible for PATROL Diagnose solutions to install and work correctly “out of the box,” regardless of the physical enterprise topology. Moreover, the ability to automatically respond to physical topological changes means that PATROL Diagnose will always correctly understand the interdependencies and interrelationships between managed objects.

Record Keeping

PATROL Diagnose provides an audit trail of the analysis process used to diagnose the root cause or causes of a system failure. The root causes and the analysis record are provided under the root-cause analysis application container. If a specific root cause cannot be diagnosed, PATROL may provide a list of suspected root causes and recommend tests that can be executed to help narrow the list. Operators can choose to execute these tests directly from the PATROL Console to verify that the problem has been fixed.

PATROL also lists the tests that were performed automatically during the analysis. From the PATROL Console, operators can see which tests have been performed and whether each test passed or failed. For example, as part of its analysis, PATROL Diagnose may query PATROL to determine whether the CPU use is high. If PATROL reports that it is, this is reported as a failed test. If CPU use is not high, it is reported as a passed test.

Component Architecture

PATROL Diagnose uses one computer – called the mid-level agent – to gather information about the system and about the monitored computers. The monitored computers are called managed nodes and are used as the important servers in the system. Figure 4 shows a simplified view of the product architecture. The mid-level agent collects data from multiple managed nodes, performs root-cause analysis and then sends the analysis results to the PATROL Console. The PATROL Console is also used to configure the mid-level agent. The PATROL Console and the mid-level agent can be located on the same computer.

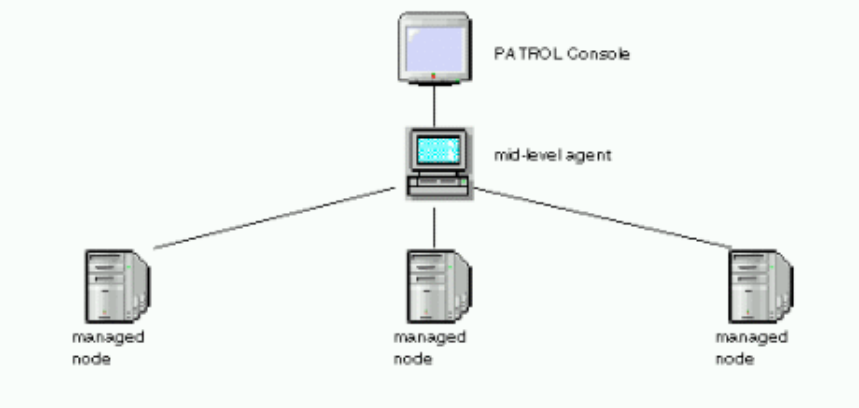

Figure 4 – Locally managed PATROL agents integrate with the mid-level RCA agent.

Mid-Level Agent Function

The mid-level agent is the machine that collects and analyzes the data from PATROL Agents running on managed nodes. The term *mid-level agent* can also refer to the PATROL Agent running on the mid-level agent machine. Although more than one mid-level agent can be configured, it is highly scalable and even very large enterprises will only require one.

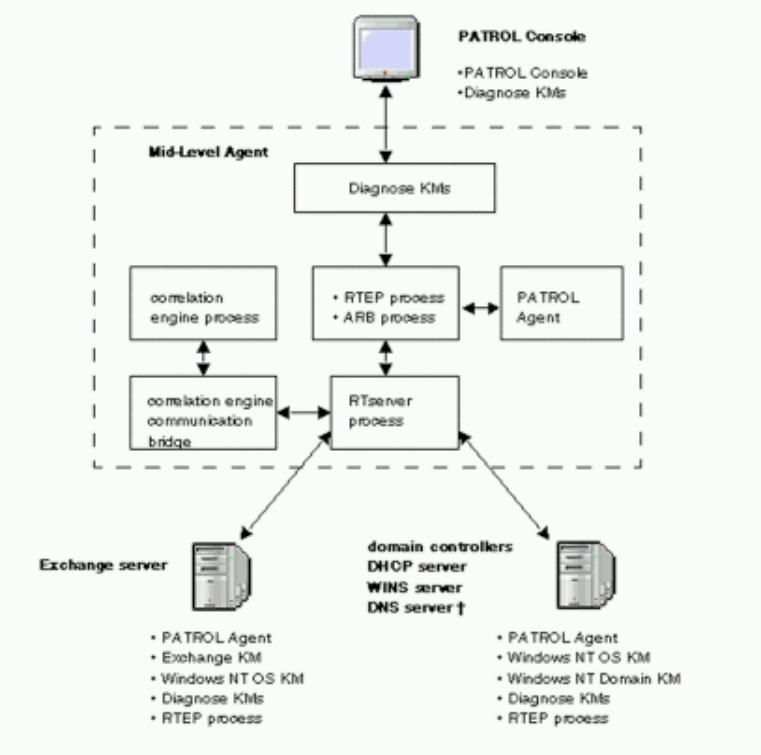

Figure 5 – This diagram gives an in-depth view of the mid-level agent architecture.

Managed Node Function

A managed node is a machine that is monitored by the mid-level agent to obtain information required for root-cause analysis. Servers that perform certain functions must be established as managed nodes for PATROL Diagnose to determine the root causes of system failures. For example, the Microsoft Exchange Server must be a managed node.

PATROL Diagnose Solution Models

An applied example of root-cause analysis is the BMC Software solution for Microsoft Exchange. This PATROL Diagnose solution is composed of three distinct, yet interrelated models:

- Exchange Server services model
- Windows NT services and components model
- IP networking model

Exchange Server services model

PATROL diagnoses the root causes of problems that are related to the following Exchange Server services:

- System attendant
- Directory service
- Information store (IS)
- Message transfer agent (MTA)
- Key management server
- Internet mail service
- Event service
- Server performance
- Internet information service

PATROL also handles faults associated with the PATROL for Exchange Server round-trip mail monitoring applications, Send_Mail and Remote_Server.

Windows NT services and components model

PATROL diagnoses problems related to the following Microsoft Windows NT services and components:

- Domain controllers
- Dynamic Host Configuration Protocol (DHCP)
- Broadcasts
- LMHOST

- HOSTS
- Domain Name Service (DNS)
- Windows Internet Name Service (WINS)

IP networking model

PATROL Diagnose also polls network devices to determine accessibility. If a device is unreachable, PATROL alerts staff and displays the network nodes that are affected by the device failure. PATROL's additional polling features are:

- Monitor single- or multi-path networks
- Handle multiple, simultaneous failures
- Predict the impact of failures on services and applications
- Poll managed nodes on a regular basis
- Enable or disable the polling of a device
- Provide an adjustable polling frequency

Flexible and Scalable

Whether scalability is measured in terms of managed systems or number of events, PATROL Diagnose solutions are highly scalable, capable of managing thousands of objects from systems that generate millions of events daily. No hard-coded rules mean users do not have to cope with managing the mayhem resulting from endless rule combinations; the significant reduction in event/message traffic to the enterprise console allows users to concentrate on matters that are most critical to the business.

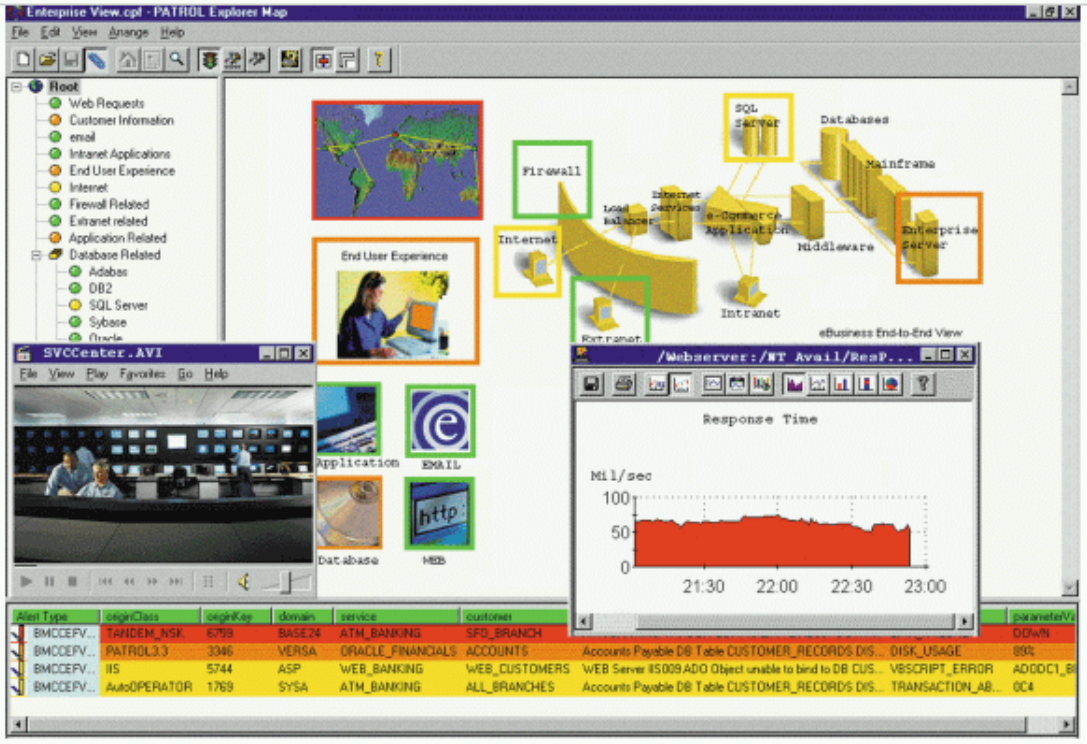

Figure 6 – PATROL manages applications from one point of control through a "business process view."

ROI Benefits Across the Enterprise

BMC Software's PATROL solutions maximize your uptime while letting you invest only in the management tools you need. The result is faster return on investment than would typically be seen from other vendor solutions. Other significant benefits include:

- Increased availability of business-critical applications
- Improved service-level management
- Dramatically reduced operational complexity and cost
- Dynamic and easily quantifiable service-level agreements for end users
- Reduced support costs due to automatic event notification and recovery
- Expanded service capabilities without requiring additional staff

Conclusion

In summary, BMC Software's PATROL Diagnose solutions provide the unique ability to automate true root-cause analysis, optimize availability and performance, and reduce implementation and maintenance costs. This translates into service-agreement compliance, maximized profit, internal and external customer satisfaction, and minimal cost of ownership.

About BMC Software

BMC Software is one of the world's largest independent software vendors. We deliver the most comprehensive e-business systems management software with the fastest guaranteed implementation. We help companies achieve greater availability, performance and recoverability of their business-critical applications. Companies who are members of BMC Software's OnSite™ program demonstrate their ability to deliver optimal service to their customers and partners. This certification program conveys that our customers' e-business applications or service offerings are managed by BMC Software technology and have undergone rigorous performance testing.

BMC Software is a Forbes 500 company and a member of the S&P 500, with fiscal year 2000 revenues exceeding $1.7 billion. The company is headquartered in Houston, Texas, with offices worldwide.

For more information visit BMC Software on the Web at www.bmc.com

100035719 01/01