



eHealth® Live Health™

eHealth® Live Health™, in conjunction with the eHealth E2E Console, provides real-time fault management across applications, systems and networks. Live Health analyzes SNMP traps and identifies potential outages for real-time fault correction.

Product Benefits

- Identify current and potential issues quickly through high-level, personalized business views
- Ensure availability and peak performance across applications, systems, and networks
- Reduce mean time to repair by associating alarms with elements and enabling drill downs to eHealth's historical and real-time reports
- eHealth Suite integration provides real-time fault and performance management with an underlying historical and business context

If your existing real-time monitoring and Network Management System (NMS) solutions are generating hundreds of alarms a day, it's impossible to know which problems are real and which are false. With CA's Live Health™ product—featuring Live Status® diagram, Live Exceptions browser, and Live Trend application—you now have access to integrated fault and performance management for rapid problem diagnosis by drilling down to historical and real-time reports from network, system, application, and response information.

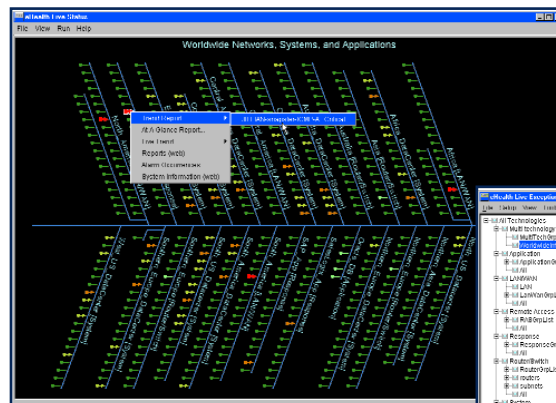


Figure 1. Live Status highlights your business topology with current alarm status and is a navigation point to drill down into real-time and historical reports.

Technical Specifications for eHealth 5.7 English Standalone
eHealth® E2E Console required.
Minimum System Requirements
UNIX

Workstation

- Sun SPARCstation or UltraSPARC
- HP-9000 Series

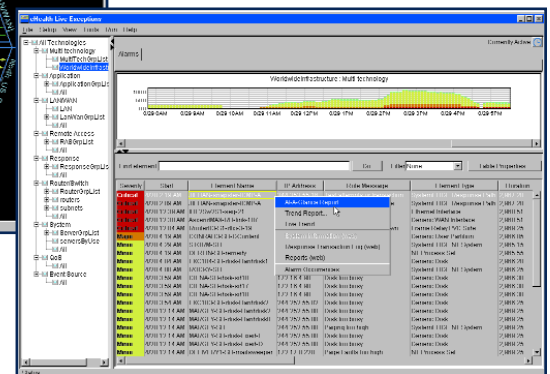
Operating Systems

- Solaris 8, 9 (32 and 64-bit)
- HP-UX 11.i (64-bit)

Windows Manager

- OpenWindows, OSF/Motif, CDE

Figure 2. The Live Health browser identifies what is at risk for an outage or degradation by delivering correlated impact analysis by customers, services, technologies, and regions.



The Live Status diagram is a high-level, personalized business view of the current status of key elements in your IT environment. The Live Exceptions browser gives you a detailed list of alarms. Both of them show you the performance alarms and hard faults on a single console. They identify who is at risk for an outage or service degradation by delivering correlated impact analysis organized by customers, services, technologies, and geographies. Live Health automatically notifies appropriate IT personnel about the alarms via email, pager, by forwarding alarms to a NMS, or by invoking any user-specified action. Moreover, you can annotate alarms to document the results of your investigation.

Memory

- 2 GB

Free Disk Space

- 3.5 GB—eHealth and apps
 - Oracle - 2400 MB
 - eHealth 5.6 - 1200 MB
- 2.5 GB—Minimum Database Size
- 1.5 GB—System swap space

Web Browser

- Mozilla 1.6 (or higher)

Minimum System Requirements

Windows

Workstation

- Intel Pentium III processor, 1 GHz (or higher) or equivalent

Operating Systems

- Windows 2000: Professional Server, Advanced Server/Windows 2003: Standard, Enterprise

Memory

- 2 GB

Free Disk Space

(NTFS Format)

- 2.6 GB—eHealth files and apps
 - Oracle - 2400 MB
 - eHealth 5.6 - 835 MB
 - NutC - 80 MB
 - Acrobat - 12 MB
- 2.5 GB—Minimum Database
- 1.5 GB—System swap space

Web Browser

- Netscape Communicator 7.0 (or higher)
- Internet Explorer 6 (or higher)
- Mozilla 1.6 (or higher)

With Live Trend you can seamlessly launch real-time monitoring on affected elements to view performance patterns of your internet infrastructure. Because Live Health leverages CA's strength in historical data collection, you can understand the context to raw data.

Live Health is simple to install and deploy. It provides out-of-the-box profiles that detect "brownouts" and service delays, eliminating the need to configure complicated rules. You have the flexibility not only to monitor your infrastructure at user-defined intervals on specified days, but also to "un-monitor" specified devices, systems, and applications depending on your needs.

Integration with Existing Operational Tools

Live Health adds complementary value to your existing management systems by delivering fewer, but more intelligent, alarms. These intelligent alarms can then be forwarded to your other management systems—enhancing the value of your current investments. It also adds a business and historical perspective while preserving and conforming to your existing workflow.

Powerful Algorithms for Predicting and Preventing Problems

Embedded intelligence and powerful algorithms enable you to be proactive by resolving potential issues before they affect the business. Five key algorithms are used to understand exceptions and to evaluate traps in historical context:

Time Over Threshold—This algorithm compares the value of a variable to a pre-defined threshold at each poll and reports if the value has been "too wrong for too long." Rather than generating a trap each time the threshold is crossed, the historical data is leveraged to watch for real, persistent problems.

Deviation From Normal—This algorithm takes advantage of Live Health's ability to baseline the performance of your end-to-end internet infrastructure. Instead of comparing current performance to a fixed threshold, Live Health uses historical data to establish what is normal for a specific day and time. It then assesses whether the current behavior is deviating from what is normally seen for that period.

Event State—This algorithm generates an alarm whenever a specific type of trap is received. For example, if a process fails, it generates a single intelligent alarm on this first process-down trap only.

Event Rate—This algorithm is applied when you want an alarm generated after an event occurs too many times over a fixed interval. For example, if a login failure trap occurs more than 3 times in 1 hour, an alarm is generated indicating that an intruder may be trying to access your system.

Event Time Over Threshold—This algorithm generates an alarm when the rate of traps received exceeds a threshold rate for a period of time. For example, network links frequently go up and down, so you don't want an alarm generated every time this happens across all of your network links. However, if the network link has gone down for 10 minutes in the last hour, then availability is impacted and you want an alarm generated to start investigating the "bouncing circuit" problem.

