

Symantec™ Application Saver

Reliability management for enterprise applications

Symantec Application Saver is a comprehensive solution for managing the health of enterprise applications. With its ability to recognize and correct a wide range of application health problems, Application Saver is an ideal solution for eliminating frustrations resulting from intermittent, inexplicable application problems occurring in production environments. Application Saver has the ability to monitor the health of Java, .NET, VB, and C/C++ applications.

Application Saver offers additional value for users of Symantec i3™ for J2EE software. Its Java application health monitoring technology complements the performance management technologies of i3 software by supporting the ability to identify Java memory leaks. With Application Saver, operations personnel will be notified about growing Java collections and provided with rich data to identify the precise location where these collections are allocated. Application Saver metrics used to identify growing Java collections are also available directly through the i3 for J2EE user interface when the two products are installed together.

Benefits

- Maximize application availability and performance.
- Improve service levels by minimizing downtime.
- Increase return on existing IT investments.
- Facilitate rapid response time for software problems.
- Display a centralized view of application health.
- Prevent application failures by recovering leaked memory and protecting against buffer overwrites.
- Pinpoint growing collections and identifies exact the Java function responsible for allocating them.

- Protect applications against common scalability and reliability defects.
- Capture extensive forensic data for application faults.

Manage application reliability

The deployment of enterprise applications in large, complex IT infrastructures often reveals previously undetected software defects that are capable of affecting business productivity and continuity. Symantec Application Saver monitors application health in actual use and corrects common runtime faults that may not have been detected in the controlled test environment. It combines fault discovery with fault correction to manage application reliability in production environments.

Application Saver consists of three complimentary products that, together, ensure application stability and availability in real-world production environments. An extensive collection of application and system resource data makes these key components possible:

- **Actionable Alerts and Recommendations:** Near-real-time reporting on and alerting of common software errors and system resource usage issues.
- **SmarTune™:** Runtime fault suppression through automated correction of conditions that may lead to application or system degradation and possible failure.
- **Forensics:** First-fault analysis and post mortem, providing rich forensic information for high-resolution reconstruction of the chain of events leading up to application failures—the first time they occur.



Data Sheet: Application Performance Management Symantec Application Saver

These components complement each other to reduce your total cost of ownership. They minimize downtime, increase server utilization, improve application scalability, increase the productivity of your administration and technical staff, and reduce development and support costs. Considering the impact even a single software defect can have on a critical application, and the need to assign multiple administrators to manage large, complex environments, Application Saver emerges as a “must have” protective solution.

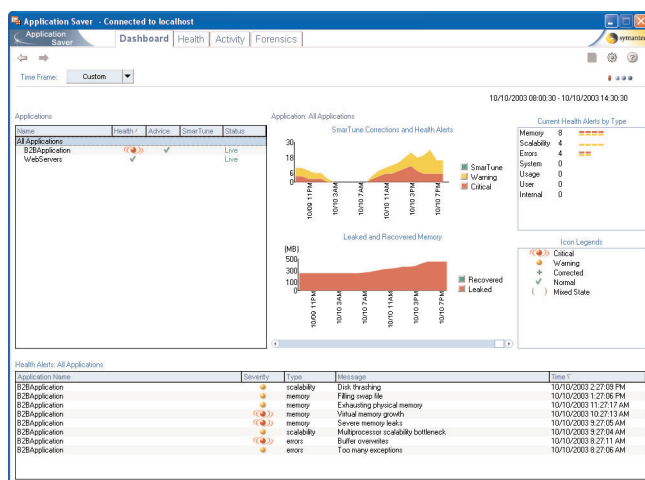


Figure 1. The Application Saver console provides timely information about the overall health of your application software, including destabilizing application faults.

Heal with SmarTune corrections

The SmarTune feature in Symantec Application Saver provides active fault correction that automatically protects your applications against common causes of runtime failure. Powerful SmarTune corrections include automatic correction of memory leaks and buffer overwrites, improved multiprocessor scalability, automatic reaping of hung processes, and much more.

Memory leaks are common in multithreaded, event-driven applications—especially in long-running application servers and batch processes. Symantec Application Saver not only identifies memory leaks and overwritten buffers, it can also be configured to safely and efficiently recover leaked memory and prevent data corruption by overwrites. You can also configure the program to increase application scalability by optimizing application memory use in multi-processor production servers.

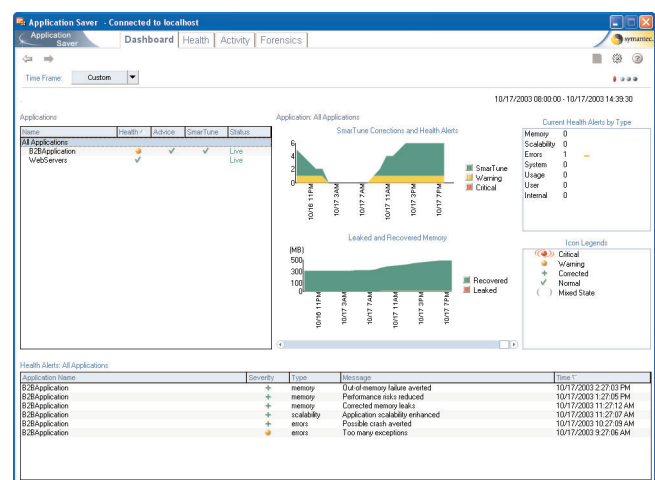


Figure 2. SmarTune corrections reverse destabilizing application faults to ensure maximum application reliability.

Respond to failures rapidly

Application Saver Forensics allows support and engineering teams to identify the root cause of application failures in development, testing, and production. By monitoring program execution and system information, the Forensics module pinpoints the exact source of the failure. It helps you rapidly recover from problems, minimize debugging time, and eliminate the need to re-create problems.



Data Sheet: Application Performance Management Symantec Application Saver

The Forensics module works by automatically inserting lightweight agents into applications through a process called instrumentation. As the instrumented program runs, the Forensics module continually monitors it, capturing relevant system information and the exact sequence of statement execution across all threads. When an exception, error, or termination occurs in the instrumented application or through an external command, the Forensics module generates files that capture a detailed history of source statement execution. The forensic data is presented in an easy-to-use graphical interface that tells you exactly what led to the failure, and enables you to quickly fix the problem without needing to re-create the failure in a test environment.

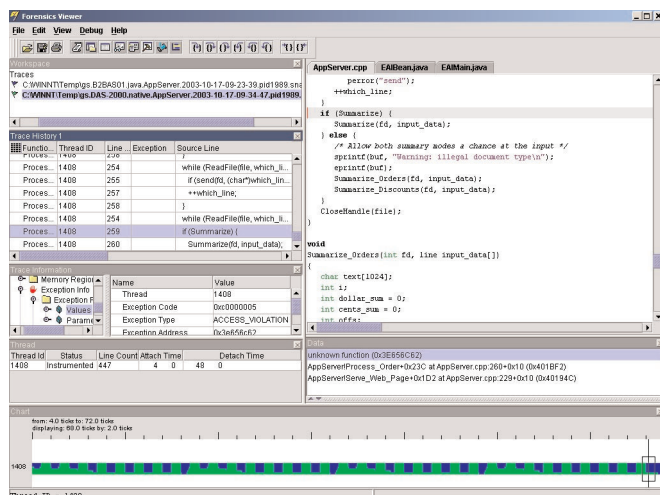


Figure 3. The Forensic Viewer in Applications Saver enables rapid root-cause analysis of application failures.

System requirements

Consult <http://support.veritas.com> for detailed operating system, environment, and console version support information.

Managed servers

Operating Systems	App Bits	Compilers	Forensics
AIX (5.1, 5.2 and 5.3)	32, 64	VA5, VA6	Java
HP-UX (11i)	32, 64	aCC, v3.5	Java
Solaris (7, 8 and 9)	32, 64	VW6, S1S8, GCC 3.0, 3.2-3.4*	Java C/C++
RedHat (7.2, 8.0, 9.0 and AS3.0)	32	GCC 3.0, 3.2-3.4	Java C/C++
Windows (2000, XP and 2003 SP1)	32	VC6, VC7, VB6,* VS2003	C#, VB .NET, Java, C/C++

Environment	App Bits*	Compilers
.NET CLR 1.1	32	VS7, VS2001, VS2003
JRE 1.2.2+, 1.3x, 1.4x (on OS's above)	32, 64	Javac, jikes

*GCC Forensics is 32-bit only

*SmarTune applies to VB apps when COM Code is invoked

*SmarTune applies when native/unmanaged code is invoked

Console support

- Windows 2000, Windows XP and Windows 2003 SP1

Symantec Corporation World Headquarters

20330 Stevens Creek Boulevard

Cupertino, CA 95014 USA

1 (408) 517 8000

1 (800) 721 3934

www.symantec.com

