PRODUCT DATASHEET

bradmark technologies

Surveillance DB™

Enterprise Monitoring & Event Management

From the **NORAD®** *Family of Products*

Real-Time, Proactive Solutions Ensures System Uptime

Bradmark's **Surveillance DB**™ provides best-in-class monitoring and event management technology to support simple to complex IT infrastructures. Utilizing real-time monitoring, unattended event management, and historical data analysis tools, Surveillance enables IT professionals to captures comprehensive views of overall system health, and perform comprehensive drill-downs to determine the root cause of performance bottlenecks. So whether you are running a data warehouse application, high availability online transaction system or a regular database, Surveillance delivers tangible business value by ensuring your systems are available and performing to agreed service levels.

Surveillance identifies and eliminates operational and performance issues throughout your enterprise. Execute customized rule sets and event handlers tailored to your specific requirements for immediate alert notification, or to take remedial action. Use Surveillance's Central Repository to store historical performance and utilization information for root-cause determination, capacity planning, or service-level reports. With Surveillance as your DBA assistant, you can now spend more time on day-to-day operations and less time on problem solving.

Key Benefits

View real-time data from any Oracle, Sybase, DB2 UDB and MS SQL Server environment simultaneously

Deploy an analytical "drill-down" methodology for quick problem identification

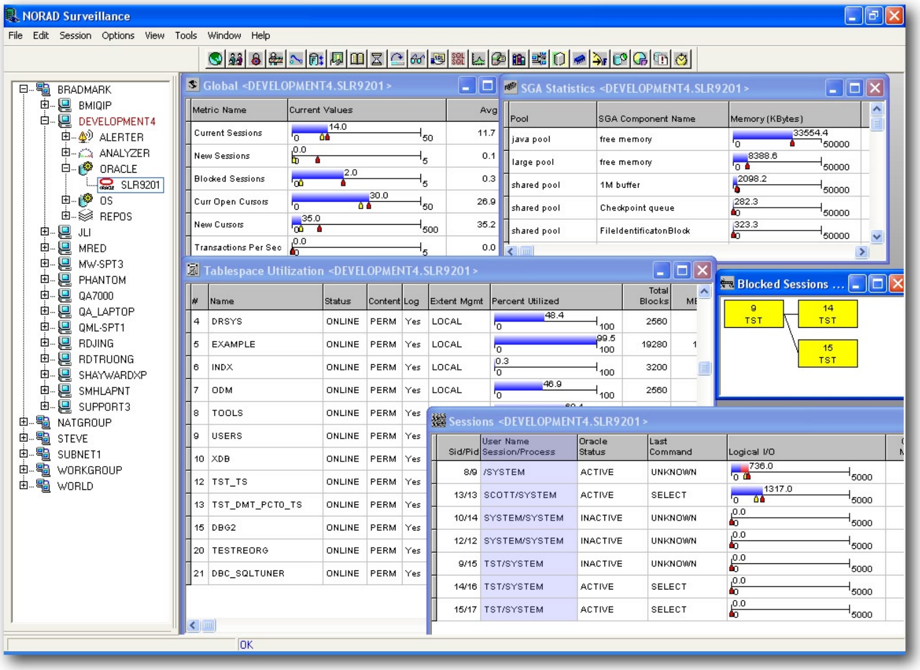
Improve data availability by reducing database downtime and troubleshooting

Flashback to view data at a select a point in time to determine the root cause of an outage

Enable proactive notification of potential problems long before systems are affected

Leverage existing IT personnel and reduce future staffing needs

Produce real-time statistics and reports for trend analysis and capacity planning



Global <DEVELOPMENT4.SLR9201>

Metric Name	Current Values	Avg
Current Sessions	14.0 (0–50)	11.7
New Sessions	0.0 (0–5)	0.1
Blocked Sessions	2.0 (0–5)	0.3
Curr Open Cursors	30.0 (0–50)	26.9
New Cursors	35.0 (0–500)	35.2
Transactions Per Sec	0.0 (0–5)	0.0

SGA Statistics <DEVELOPMENT4.SLR9201>

Pool	SGA Component Name	Memory (KBytes)
java pool	free memory	33554.4 (0–50000)
large pool	free memory	8388.6 (0–50000)
shared pool	1M buffer	2098.2 (0–50000)
shared pool	Checkpoint queue	282.3 (0–50000)
shared pool	FileIdentificatonBlock	323.3 (0–50000)

Tablespace Utilization <DEVELOPMENT4.SLR9201>

#	Name	Status	Content	Log	Extent Mgmt	Percent Utilized	Total Blocks	MB
4	DRSYS	ONLINE	PERM	Yes	LOCAL	48.4 (0–100)	2560	
5	EXAMPLE	ONLINE	PERM	Yes	LOCAL	99.5 (0–100)	19280	1
6	INDX	ONLINE	PERM	Yes	LOCAL	0.3 (0–100)	3200	
7	ODM	ONLINE	PERM	Yes	LOCAL	46.9 (0–100)	2560	
8	TOOLS	ONLINE	PERM	Yes				
9	USERS	ONLINE	PERM	Yes				
10	XDB	ONLINE	PERM	Yes				
12	TST_TS	ONLINE	PERM	Yes				
13	TST_DMT_PCTO_TS	ONLINE	PERM	Yes				
15	DBG2	ONLINE	PERM	Yes				
20	TESTREORG	ONLINE	PERM	Yes				
21	DBC_SQLTUNER	ONLINE	PERM	Yes				

Sessions <DEVELOPMENT4.SLR9201>

Sid/Pid	User Name Session/Process	Oracle Status	Last Command	Logical I/O
8/9	/SYSTEM	ACTIVE	UNKNOWN	736.0 (0–5000)
13/13	SCOTT/SYSTEM	ACTIVE	SELECT	1317.0 (0–5000)
10/14	SYSTEM/SYSTEM	INACTIVE	UNKNOWN	0.0 (0–5000)
12/12	SYSTEM/SYSTEM	INACTIVE	UNKNOWN	0.0 (0–5000)
9/15	TST/SYSTEM	INACTIVE	UNKNOWN	0.0 (0–5000)
14/16	TST/SYSTEM	ACTIVE	SELECT	0.0 (0–5000)
15/17	TST/SYSTEM	ACTIVE	SELECT	0.0 (0–5000)

Efficient diagnostics and effective problem identification with a real-time perspective.

Mitigating Risk Ensures Availability Demands

High availability systems, disaster recovery and back-up systems, dedicated data warehouse systems and sophisticated database monitoring and administration tools are essential for most businesses. Add the multi-platform support for most DBAs – distributed systems, mission critical applications and various operating systems, the task of the DBA is an around-the-clock challenge. And if not managed effectively, the high risk of database failure or unplanned downtime can result in disastrous financial consequences affecting the company’s bottom line. The demand for 24x7 availability also increases as databases proliferate within an environment. To help mitigate those risks, it is becomes even more essential to have monitoring, event management and reporting capabilities that deliver reliable system efficiency and scale with the environment.

The Surveillance Architecture

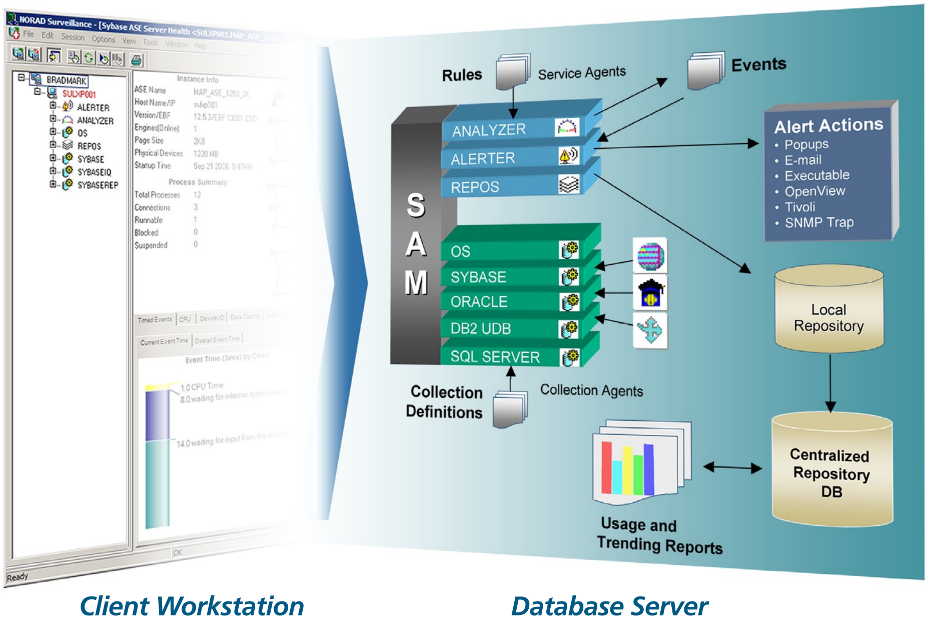
Rule-based Alerting and Event Architecture

Surveillance uses an extensive alerting and alarming facility that comes with a library of ready-to-use predefined rules. Rules are needed to activate the Session Agent Manager (SAM) which gathers data information, creates alerts based on requested thresholds and writes records to the local repository. Rules can be assigned for any supported database and OS. Additionally User Defined Collections (UDCs) can be created for files and non-standard databases to utilize all of Surveillance’s SAM functionality. To ensure the network traffic is planned around peak system traffic loads, the information gathered is written to a local repository and remains until a scheduled request to copy to the central repository is made for reporting and trend analysis (See Fig. 1).

Surveillance is composed of two major components: the Server Agent and the Console.

The Console is the set of programs the end user runs to view real-time performance data, configure the connectionless monitoring, alerting, and historical collection of performance data.

The Server Agent is the set of programs used to collect data and automate analysis of the database servers

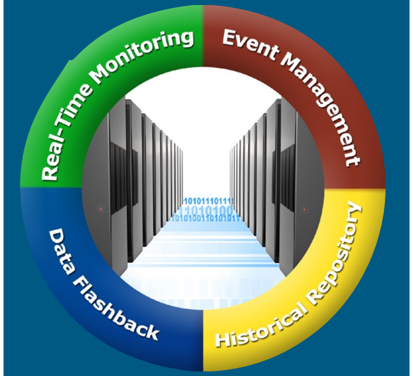


(Fig. 1)

Multi-Tier Deployment Architecture

Surveillance’s tier deployment architecture allows for maximum flexibility in setting up monitoring databases, applications and the environment. Simply put, it allows a single database to be managed separately, a set of databases (maybe an application) to be managed separately, the whole environment to be managed as a single entity – or any combination of the above to meet security or organizational requirements (See Fig. 2).

The Surveillance Core Feature Set



Real-Time Monitoring
Monitors real-time performance statistics through the Surveillance GUI. Surveillance is helpful when checking on a current issue such as long running SQL to see the actual statement/plan.

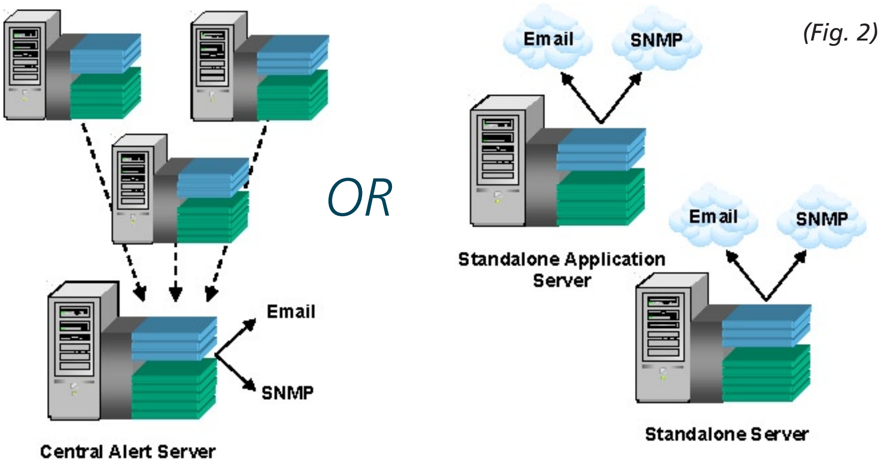
Proactive Event Management
Sends alerts to notify DBAs when a threshold has been exceeded. This means no one has to be watching a GUI to look for problems. You only look when notified.

Historical Repository
Creates reports from the central repository to identify trending usage changes and point out most used objects and many other useful management statistics.

Data Flashback
Determines the root cause of database issues/problems by moving back and forth through past performance data stored in the repository… just like it was happening in real time to detect root causes.

The Session Agent Manager (SAM) can be implemented as the Central Alert Service (CAS) where standard monitoring can be managed from a central location or have application level Alert Service for security sensitive or uniquely managed applications. Alerting (i.e. popups, emails, SNMP traps) and heartbeat monitoring can be centrally configured, or configured uniquely for applications or even a single database. If central alerting is selected, the non-CAS SAMs can be implemented to forward events to the CAS.

For large, complex installations, the Surveillance **Enterprise Deployment** feature provides a simple, standard way to deploy across the enterprise.



(Fig. 2)

Real-Time Monitoring
View Statistics Across Multiple RDBMSs

Without reliable tools as an intricate component of your IT infastructure, work stoppage will continue until the DBA is notified by the user community or help desk that there is a performance problem. Once available, the DBA has to then write and/or run scripts that query a multitude of performance statistics to determine the cause of the problem before the work stoppage can be eliminated.

Surveillance **Real-Time Monitoring** displays exactly what is currently happening in the database. With an extensive set of predefined windows available, Surveillance can provide an immediate global view of database activity and up to 2500 detailed performance metrics such as session/process activity, locks, batch contention, file I/O, and much more.

Real-time data from multiple RDBMS can be viewed simultaneously. Data from each window can be sorted or filtered while most statistics can be graphed over time. In addition, each window or graph can be configured to refresh at either the default collection interval or its own refresh interval.

Use data from Real Time Diagnostics to obtain a real-time perspective when Event Management detects and alerts technical professionals that conditions negatively impacting performance or availability. DBAs can also use real-time data to establish baselines for threshold values in Event Management's rule definitions.

Blocking Instance
Example:

If Surveillance alerts the DBA that a user is blocking other users for an extended period of time – causing a work stoppage, Real-time Diagnostics can identify the user's session that is causing the problem. Drilling down to session details reveals that the user's session has issued an exclusive lock on the LEDGERS table that is preventing other users from entering general ledger records. The DBA is also able to determine that the user has selected data for update purposes, but has neglected to save or abort the update, causing other users to wait. The DBA can then request that the user save or abort the data. If the user can't be found, the DBA could decide to kill the user's session, allowing other users to enter general ledger records. If the DBA is not available, a pre-configured rule in Event Management can kill the session automatically – the work stoppage will be eliminated without intervention from technical professionals.

Proactive Management Quickly Detect Problems and Notify Multiple DBAs

Event Management

Surveillance **Event Management** is used to provide peace of mind whose sole purpose is to continually monitor the database for conditions which have a negative impact on performance and/or availability and alert technical professionals before conditions gets out of control. To accomplish this, Surveillance uses its extensive alerting and alarming facility that comes with a large set of predefined rules.

To begin, the DBA adjusts default threshold values and collection intervals before turning on the rules to be monitored. The DBA then defines how the alerts are to be sent when an incident occurs. Surveillance DB can be easily configured to notify multiple DBAs or technical professionals by e-mail, pager, HP Openview or Tivoli alerts, pop-up windows, or record the error in the Windows Event Log.

Surveillance also provides unattended event monitoring. As long as the Surveillance Server Agent is running, continuous monitoring of the rules that the DBA has explicitly turned on occurs, even if the Surveillance console is not connected.

Alert Notification
Example:

*In most RDBMS environments, blocked users can cause performance to quickly degrade. Surveillance DB can monitor for blocked users, and if a user is found to be blocking other users for an extended period of time, Surveillance DB can notify IT staff via an e-mail. If the problem is not resolved in a designated period of time, Surveillance DB can then page the entire DBA staff, e-mail DBA management, and execute SQL*Plus to kill the offending user's process or session before it affects system response time or prevents other users from entering data.*

Go Back in Time to Analyze and Report on Historical Data

Historical Repository

The benefit of establishing an historical repository is to provide a vehicle through which to analyze events that happened in the past. The Surveillance **Historical Repository** is used to determine new trends that have been occurring in the environment, or where the peaks and valleys are within the daily workload.

It can also be used for preventative maintenance, as in the case of tables that are filling up at an alarming rate, resulting in a demand for more disc storage; or determining applications that are eating up inordinate CPU utilization or disc I/O and perhaps should be reviewed for performance improvement.

All these would be difficult to determine without the use of a central repository. Long-term historical data (minutes to years of data) for Reporting is kept in a Central Repository Database, like Sybase Adaptive Server Enterprise (ASE). The delivery of historical information is via ODBC drivers and thus can be of any RDBMS platform. (See Fig. 3)

EXAMPLE:

Reports on Collected Historical Data

A heterogeneous environment that has Oracle, Sybase, DB2 Universal Database, and Microsoft SQL Server can all report history to a single ASE database. The appropriate license is required for the instance of ASE to hold the long-term historical data. Reporting is done against the Central Repository Database for storage trending, CPU activity, etc., and produces reports in PDF, HTML, and other formats.

Avoid Future Outbreaks by Determining Past Problem Root Cause

Data Flashback

A key benefits of a repository is in isolating the cause of incidents that occurred behind the scenes, when the DBA is not available to experience it first hand. Many times a user calls-in to complain about the system performing sluggishly; but, when the DBA gets a chance to look at the system, the problem has already resolved itself. So, what next? In the past, the only option was to wait until the problem reoccurred and hope that there was enough time to find the cause before it disappeared again. Through the use of a repository, this dilemma becomes easily resolved.

The Surveillance **Data Flashback** feature used in conjunction with the repository, allows you to review the period of time in which the problem occurred as if it were in real-time. This is often referred to as simulated real-time of the environment. Generally, within a very short period of time, the problem is solved and the culprit is found. This is not a substitute for rules-based alarming and alerting. Alarming and alerting determines that there is a problem, where "flashback" helps to isolate the cause and resolve the problem.

Product Summary

Be Proactive vs. Reactive... Detect and resolve problems before a crisis can affect availability by setting rules for violations combined with unattended alerting when a threshold has exceeded.

Maximize Performance and Availability... Avoid an outage by identifying problems quickly with an immediate global view of database activity and detailed performance metrics without writing scripts.

Determine Root Cause... Go back to review the period of time in which a problem occurred as if it were in real-time.

Plan for the Future... Use trend performance and space utilization data to support system upgrades and/or decisions regarding additional disk space.

Maximize Scarce Resources... The DBA can concentrate on improving performance and developing new databases rather than looking for problems.

System Requirements

Console Requirements:	• Windows 2000 or later • 600 MHz Pentium Processor • 128 MB of RAM • 100 MB free hard disk space
Agent Requirements:	• Platforms: Windows Server 2003 or later, AIX, HP-UX PA-RISC, HP-UX Itanium, Linux x64 - x86, Linux POWER, Solaris SPARC, Solaris x64, Tru64 • Full 64-bit support on UNIX and Linux • 200 MB disk space, plus repositories
RDBMS Requirements:	• Oracle v 7.3.4, 8.0.x, 8i, 9i-9.2, 10.1-10.2 and 11G • Sybase ASE v 12.0 or later • Sybase Replication Server v 12.6 or later • Sybase IQ Server v 12.6 or later • Microsoft SQL Server v 7.0, 2000-08 • DB2 UDB version 7.2, 8.1-8.2 and 9.1

About Bradmark

A privately held company founded in 1981, Bradmark Technologies, Inc, is a leading developer of software solutions for major RDBMS enterprise environments. Bradmark solutions manage all three major components of the enterprise environment: the database, the operating system and the network to ensure data integrity.

To order, or for more information on other Bradmark products:

Phone: **(800) 621-2808** or outside the U.S.: (713) 621-2808
Fax: (713) 621-1639

Or visit: **www.bradmark.com**

Bradmark Regional Offices:

Bradmark EMEA
Tel: +31 (0) 251 268 248

Bradmark Technologies UK Ltd.
Tel: +44 (0) 870 240 6285

Bradmark Deutschland
Tel: +49 (0) 211 52391 154

Bradmark Asia
Tel: +86 10 8458 0860

bradmark technologies