



# **Sentra Data Collection Agents**



## Table of Contents

|   |   |
|---|---|
| Introduction.....   | 3 |
| Server and Internet Service Monitoring Agent.....                     | 3 |
| Service and Process Monitoring Agent .....                            | 3 |
| Directory Monitoring Agent.....                                       | 3 |
| Windows Event Log Agent.....  | 3 |
| Unix/Linux System Log Agent .....                                     | 4 |
| HP-NSK EMS Event Agent.....   | 4 |
| Windows Performance Counter Agent .....                               | 4 |
| Non-Windows Performance Counter Agent .....                           | 4 |
| JMX MBean Monitoring Agent .....                                      | 4 |
| Generic Log File Agent .....  | 4 |
| SQL Query Monitoring Agent.....                                       | 5 |
| XML Data Collection Agent .....                                       | 5 |
| X500 Enterprise Directory and Active Directory Monitoring Agent ..... | 5 |
| Application Response Monitoring Agent.....                            | 5 |
| WebSphere MQ Agent.....   | 5 |
| SNMP Monitoring Agent .....   | 5 |
| Syslog Protocol Monitoring Agent .....                                | 6 |
| Email Agents.....   | 6 |
| BASE24 Monitoring Agent.....  | 6 |

## **Introduction**

Sentra uses data collection agents which can be remotely installed on computers in the network in order to gather data from a variety of different sources. This document provides a brief overview of the various Sentra data collection agents that are available.

The data collected by the agents can be forwarded to a central Sentra database for reporting and analysis purposes. Captured data can also be evaluated against multiple rules. . If the captured data meets the rules criteria is met, alerts are generated. A library of pre-configured rules is shipped with the Sentra product and additional rules can be configured by users.

A separate agent is deployed for each type of data collection required from a computer. This approach is much more efficient than deploying a single monolithic collection agent. The extensive list of data types that can be collected by the agents is described below.

## **Server and Internet Service Monitoring Agent**

The server monitoring agent uses standard Internet protocols to check the availability of computers and services. The agent can check whether a computer is available on the network. Alternatively, a more specific check of the availability and response time of a service that uses an Internet protocol can be performed. The agent can monitor using FTP, HTTP, IMAP4, POP3 and SMTP protocols. Daily percentage availability and transfer rate statistics (e.g. for FTP and HTTP) are recorded for inclusion in reports. Several agents can be deployed to different geographical locations in a corporate network to gain a full picture of service performance and availability across an entire organisation. This can help in pinpointing infrastructure bottlenecks and weaknesses.

## **Service and Process Monitoring Agent**

In order to manage the data collection agents, Sentra provides a service manager process that allows agents to be installed, un-installed, started and stopped from a single console. Sentra agents can easily be deployed and configured to many machines simultaneously, from a single point. Once deployed, the service manager monitors the agents and can automatically restart or even re-install them should a problem occur. The service manager can also monitor third party processes or services and generate alerts if they fail or even attempt to re-start them. Reports can be produced to show historical outages of service or programs.

## **Directory Monitoring Agent**

The directory monitoring agent monitors files and directories on multiple computers. The agent monitors directories for changes in the number of files, the largest file size and the overall directory size. The agent also monitors the size, age and attributes of files, as well as the changes in the overall status of a file (i.e. if it is a newly created file or if a file is deleted).

## **Windows Event Log Agent**

This agent monitors the Windows event log on 32 bit and 64 bit Windows computers. The standard mode of operation is to evaluate captured data against pre-configured rules and forward those events that meet the rules criteria to the Sentra database. The agents can also be configured to forward specific event log entries to the Sentra database even if rules criteria is not met, e.g. application events that confirm the start and end of a daily backup. Events such as these are usually stored in the database for further report analysis.

## **Unix/Linux System Log Agent**

This agent monitors the system log (commonly known as the Syslog) on Unix or Linux (32 bit and 64 bit) computers. The standard mode of operation is to evaluate captured data against pre-configured rules and forward those events that meet the rules criteria to the Sentra database. The agents can also be configured to forward specific Syslog entries to the Sentra database even if rules criteria is not met, e.g. application events that confirm the start and end of a daily backup. Events such as these are usually stored in the database for further report analysis.

## **HP-NSK EMS Event Agent**

The HP-NSK operating system and its applications are richly instrumented through EMS events. This agent monitors EMS event logs. The standard mode of operation is to evaluate captured data against pre-configured rules and forward those events that meet the rules criteria to the Sentra database. The agents can also be configured to forward specific EMS event entries to the Sentra database even if rules criteria is not met, e.g. EMS events that confirm the start and end of a daily backup. Events such as these are usually stored in the database for further report analysis.

## **Windows Performance Counter Agent**

This agent can capture data from any Windows performance counter. An extensive library of pre-configured rules is shipped with Sentra, e.g. to monitor issues such as high CPU usage and low virtual memory availability. 'Data-thinning' techniques are used to average the performance counter data in the database into summaries as the data becomes older. This allows recent data to retain its detail whilst long term trends can be still be seen without filling the database.

## **Non-Windows Performance Counter Agent**

On non-Windows platforms key performance indicators such as CPU usage and disk space can be collected into performance counter format. Sentra is therefore able to monitor performance metrics across multiple platforms and operating system types.

## **JMX MBean Monitoring Agent**

Many Java-based programs instrument their performance metrics using JMX. Java-based applications such as BEA WebLogic and IBM WebSphere provide a whole series of performance monitoring metrics via JMX. The Sentra JMX agent can monitor JMX counters and treat the captured data in the same way as Windows performance counters. Rules can be configured to evaluate captured JMX data and generate alerts if the rules criteria are met.

## **Generic Log File Agent**

Sentra uses a general purposes 'Generic' log file agent that can collect data from any structured text log files. The Sentra Windows console enables a user to configure a new agent and specify the format of the data that the agent is required to capture. For example, a new agent can rapidly be configured to capture the contents of any CSV file. Sentra ships with some pre-configured setups for some common structured log files, e.g. the Microsoft ISA Firewall log file, the Microsoft ISA Packet Filter log file, the BEA WebLogic log file and Tuxedo log file.

As with all Sentra agents, rules can be configured to evaluate captured data. Alerts will be generated if the rules criteria are met.

## **SQL Query Monitoring Agent**

The Sentra SQL agent can be configured to schedule execution of queries of the Sentra database or any other ODBC-compliant database, including SQL Server, ORACLE, DB2 and MySQL. This agent is typically used to store summary information from a number of database sources so that long term trends can be summarised and alerts generated if any rules are broken. For example this could be used to produce an escalation of a problem if the number of alerts for a server broke a nominated limit. This agent has been used to monitor a high-performance payment system that used an ORACLE database. The agent issued scheduled queries to monitor payment volumes; if the payment volume fell below a preset threshold, an alert was generated.

## **XML Data Collection Agent**

A general purpose XML agent can be configured to parse any xml data into a hierarchical structure of SQL tables and fields. This makes the information much easier to process and report on, whilst maintaining the relationships between the XML elements. The agent can be configured by specifying an XSD schema or (where a schema is not available) by loading examples of the xml structure to be captured. The agent can collect XML data from files, MQ queues or from TCP/IP socket-based messages sent directly to it. XML agents can be configured to monitor any ISO20022-compatible payment or transaction.

A series of these XML agents can be deployed to key monitoring points (waypoints) within a payment processing infrastructure to monitor transaction volumes and trends, payment volumes and trends and end-to-end processing times. Rules can be configured to monitor service level compliance and abnormal processing volumes.

## **X500 Enterprise Directory and Active Directory Monitoring Agent**

The enterprise directory monitoring agent monitors the availability and performance of X500 or Windows Active Directory based enterprise directories. Statistics such as percentage availability and directory query response time can be recorded. Agents can be deployed to multiple locations around a network to determine the availability and responsiveness of the enterprise directory from across the whole organisation.

## **Application Response Monitoring Agent**

This agent can be configured to invoke a program or script file and measure the time taken for execution to complete. Statistics for the average response time and last response time are collected. For example, the agent could be configured to perform an SQL query to monitor a trend of long-term degradation of database performance. The agent has in the past been used to monitor the performance of SAP transactions in a corporate environment, by launching a program that issues a SAP transaction and waits for a confirmation reply.

## **WebSphere MQ Agent**

This agent collects information on the state of MQ managers, queues and channels. The MQ message header is also captured. Rules can be configured e.g. to monitor the change in run status of queues and channels or to monitor the size or number of entries on a particular queue. Sentra also provides management of MQ queues such as starting and stopping queue managers, queues and channels.

## **SNMP Monitoring Agent**

The Sentra SNMP agent can listen for and report the occurrence of SNMP traps. The agent can also be configured to perform periodic SNMP read requests to query particular values on remote SNMP-enabled devices such as routers or switches.

## Syslog Protocol Monitoring Agent

Sentra can be configured to monitor devices that support the Syslog protocol. A Syslogd service can be configured to forward Syslog protocol events to the Windows event log, which is monitored by another Sentra agent, as discussed earlier in this document. This technique enables the status of devices such as printers to be monitored.

## Email Agents

Sentra collects email message events from a wide range of e-mail system vendors and transforms them into a unified format in the Sentra database. Agents are provided for capture of both SMTP and X400 mail system tracking log files. This allows messages to be tracked across multiple vendors and between X400 and SMTP environments and through mail gateways.

Typical mail systems supported on a variety of different operating systems include:

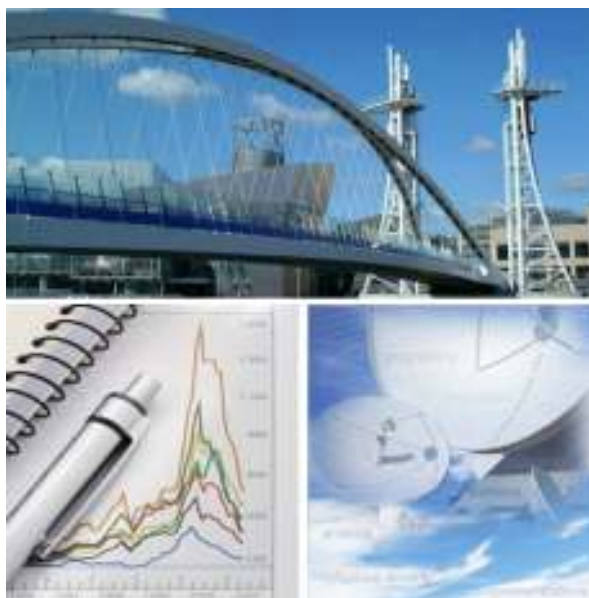
- Microsoft Exchange 5.5, 2000, 2003, 2007
- Boldon James X400 Bridgehead Connector for Microsoft Exchange 2007
- Lotus Notes/Domino
- Sendmail
- Clearswift
- Nexor
- Isode MSwitch
- InfoNet

In many cases mail queues can also be monitored for messages that have been stuck for specified period of time, providing an early warning of potential performance or connectivity problems.

For Microsoft Exchange 2003 and 2007, mailboxes activity can be monitored for events such as messages being deleted before they are read, copying of messages to another folder, and delegate user logins.

## BASE24 Monitoring Agent

Capture of BASE24 ATM and POS transactions is available and has proved to be able to capture the complete contents of the TLF and PTLF logs from the HP-NSK platform to a SQL Server database. This provides real time alerting capabilities as well as the ability to do ad-hoc queries, which are otherwise not possible. Even with high data processing volumes ~1000 transactions/sec the impact on the host HP-NSK machine was minimal.



Insider Technologies is a UK-based software and services company quality certificated to ISO 9001:2008 and TickIT. Operating in the Financial and Messaging markets, it provides Service Management, Tracking, Bespoke Software and Information Mediation solutions.

A cross section of our customers would include Banking and Financial Services, Telecommunications Providers and Government and Military Institutions.

For details about the full range of products and services available from Insider Technologies Limited, please contact our Product Development Centre in Salford Quays (home to MediaCityUK), at:

Insider Technologies Limited  
 Spinnaker Court  
 Chandlers Point  
 Broadway  
 Salford Quays  
 MANCHESTER, M50 2YR  
 United Kingdom

Tel: +44 (0)161 876 6606  
 Fax: +44 (0)161 868 6666

e-mail: [support@insidertech.co.uk](mailto:support@insidertech.co.uk)  
 Website: <http://www.insidertech.co.uk>



business partner



ISV/Software Solutions