



SNAPPiMON-3.6 Fact Sheet

SNAPPiMON (an IBM IPSC asset), is an enterprise monitoring tool for networks, systems, applications and databases. SNAPPiMON integrates and correlates enterprise-wide IT infrastructure information (availability and performance). SNAPPiMON allows logical and contextual grouping of IT services. Rich analytics and dashboards allow fine grained monitoring of health of various IT Services and their impact on business functions.

<p>True SNMP Polling and Monitoring</p>	<p>SNMP polling is not limited to basic SNMP commands and parameters as is the case with many monitoring systems. SNAPPiMON allows you to construct complex MIB expressions like bandwidth utilization, etc and then monitor these expressions against thresholds. Also provides ability to upload and compile new MIB's on the fly and use specific OID's or custom expressions for monitoring.</p>
<p>Event Correlation and Root Cause Isolation</p>	<p>SNAPPiMON provides a proprietary, correlation algorithm that is efficient and effective for root cause isolation. There are no complex rules to be built and managed. Events are automatically correlated to the highest parent device that has caused the failure.</p>
<p>Alarm Consolidation reduces monitoring load</p>	<p>SNAPPiMON prevents unnecessary cascading of alarms when a parent device goes down. Thus, if a root router is down, it suppresses alarms for all devices that are "logically" down due to the parent router being down.</p>
<p>Alarm Correlation eliminates unwanted spikes</p>	<p>SNAPPiMON provides an Alarm Correlation window within which events will be ignored. This helps avoid spikes and alarms which are momentary in nature and hence reduces the load on monitoring.</p>
<p>Enhanced Network Topology provides deep visualization</p>	<p>SNAPPiMON provides visualization of discovered network elements, interdependencies between various elements, configuration status, availability status, performance status, event propagation and root isolation, all within the topology map. SNAPPiMON provides auto-mapping of discovered elements and provides layer 2 views up to the systems / elements that are connected to the switches within a VLAN.</p>
<p>Easy Diagnosis and Analysis</p>	<p>SNAPPiMON provides an exhaustive list of functionality for diagnosis and analysis including Diagnosis and Analysis dashboards, diagnostics tools, root cause reports etc.</p>



Extensible, Scalable robust architecture

SNAPPiMON can be used to monitor small, medium, large and very large IT infrastructures. It allows options to install its components on one server or across multiple servers depending on the size of the infrastructure. SNAPPiMON's web based, distributed, 3 tier architecture uses client-server principles, multithreading and other enterprise design principles. SNAPPiMON's architecture framework support easy inclusion of new element families or applications for monitoring.

Customizable views and IT infrastructure visibility

SNAPPiMON provides role based access to IT infrastructure element data. Each user (technical or business) can gain access to the specific Key Performance Indicators (KPI's) of their interest and also select the mode of alerts. The home page of every user can be customized.

Out-of-the-box reporting and distribution

SNAPPiMON meets end-to-end reporting of IT infrastructure. Out-of-the box reports cover availability, performance, service levels. Features like Graphical topology, dashboards, tabular reports and trend graphs provide multiple reporting options. Highly parameterized reporting ensures accurate information delivery to every role that is defined. Reports can also be scheduled to be automatically delivered to pre-defined users in PDF, Excel or html formats.

Helps in proactive IT infrastructure planning

SNAPPiMON provides vital data needed for making critical decisions such as element relocation, server consolidation and capacity planning.

Central IT Infrastructure metrics library and templates

SNAPPiMON has inbuilt IT infrastructure library for several commonly needed KPI's. Users can define organizational specific templates using these KPI's and apply them to multiple elements having similar monitoring needs. This feature also allows for multiple polling frequencies across different class of IT elements, and an ability to schedule a "do not poll" calendar - a time frame where polling should not occur because of scheduled down time activities.

Powerful IT infrastructure discovery and configuration

SNAPPiMON provides several methods to discover the company's IT assets and also allows configuration of several parameters such as polling frequencies, alert thresholds etc.

Non-invasive monitoring

SNAPPiMON uses true agent-less monitoring technology to capture the element health and performance data for networks, servers, databases, applications, etc. This feature ensures that monitoring does not intrude on the core functionality of production servers and applications. This approach simplifies implementation complexity, reduces time taken to configure and rollout the solution.

Open unification framework for interoperability

SNAPPiMON allows addition of Bolt-on applications such as QOS manager for Cisco, File Store for centralized repository of information, IPSLA for monitoring application response, IPMeter for IP Traffic Metering, coDesk (for IT Helpdesk), etc.



Service Management and Business Impact Management provide business to technology mapping

SNAPPiMON provides a very powerful analytical view for IT Service Management and Business Impact Management. . IT administrators and operation managers can understand the impact each error or incident has on the business. This feature allows IT administrators to prioritize critical errors and incidents that are affecting vital business functions SNAPPiMON provides end-to-end service health measurement with ability to define services and service groups and monitor the overall health of a service group and its associated services. IT Service views provide a very high level of visibility and insight into IT Infrastructure to the entire organization and presents the mapping of IT to business.

Fine Grained Access Control

Ability to create new roles and assign users, assign navigation specific permissions for roles and assign module specific permissions for roles.

Real-Time Event Console

Single console to view ALL events (Availability, Performance Threshold breaches, etc). This is useful for the IT administrator to monitor the entire IT infrastructure on a single screen.

Top N / Bottom N – Attention Dashboard

Multiple dashboards for specific element type (e.g. Databases, Routers, etc) can be created by end user. Allows administrators to focus on top/bottom N elements of a specific type.

Log File Monitoring

Allows monitoring of ASCII/text log files for ANY application, database, etc. Provides ability to monitor for specific tokens including those specified by regular expressions. Provides ability to include and exclude tokens from monitoring. Provides email notifications and historical reporting when token matches occur.

Element support

Availability and performance monitoring for all SNMP v1/v2/v3 based network devices (Routers, Switches, WAN links, Bridges, servers and printers), Systems (Windows 2003/2000/NT/98, Linux 2.4.20.8,Solaris 5,8, HPUX 11i, AIX 5.x, Open VMS 7.3.x), databases (Sybase, Oracle 8i/9i/10g, MS SQL 7.0/2000/2005, DB2 UDB 8.x/9.x), Applications (IIS, MS Exchange 5.5/2000/2003, Lotus Domino 6.x,WebSphere 6.x, WebLogic, WebSphere MQ Series, .NET applications, Apache Tomcat 5.x, , Windows DNS, Windows DHCP, Windows ADS), add on services (Custom log parser, SQL Query Response Time, HTTP URL Response Time, Port Process, Services), Cisco Pack including Cisco Ping, Cisco QoS and Cisco IPSLA. Support for on-demand reporting of PIX, IDS and Checkpoint log files for security analysis.

Automated Action Engine

Automated action engine provides the ability to execute custom scripts, programs, and shell/batch files when an alarm is generated. Alarms can be generated for multiple events including Node Up, Node Down, KPI breaches, SNMP traps, etc. Scripts can take corrective or preventive actions; e.g disabling login access, dynamically increasing resources available or raise Help Desk tickets. The engine is based on a high performance and



scalable architecture that can support multiple simultaneous events. Also, actions can be executed by distributed Action Servers.

Automated Script Engine

This feature can be used to monitor custom business processes and activities. The engine allows ability to remotely or locally execute custom, external scripts and commands, periodically on any server using SSH or Telnet. The output of these scripts can be compared against pre-defined thresholds. Email notifications and escalations are possible for threshold breaches. Further, the KPIs can be included in all dashboards, historical reports, IT Service Management, etc.

Enhanced Scalability and Flexibility

SNAPPiMON is a modular framework that supports very high scalability. The components include the SNAPPiMON Manager; the RDBMS based database engine, one or more Proxy agents and plugins based on elements being monitored. All the components can be implemented on a single system for a small enterprise and the Proxy agents can be distributed for very large scalability.

Integration with IPMeter and coDesk

SNAPPiMON provides out of the box integration with other Netsol tools like IPMeter for IP Traffic analysis (using Cisco Netflow or software based Sniffer). SNAPPiMON also provides bi-direction integration for incident management with coDesk.

Support for multiple tenancy for Service Providers

SNAPPiMON can be used in a service provider environment where multiple instances of SNAPPiMON can be resident on the same server. Each of these instances could monitor separate customer environments. This allows for server consolidation and ease of manageability for service providers.

Self Health Check - Watch Dog feature

SNAPPiMON provides a separate watchdog facility that ensures smooth running of SNAPPiMON. This facility can notify IT administrators in case a specific element cannot be polled for various reasons. It will be possible to view the health of SNAPPiMON processes and components in real time. This allows for excellent, independent manageability option for IT administrators.

Typical Platform Requirements

SNAPPiMON Manager - Microsoft Windows 2000/2003 or RedHat Enterprise Linux, Release 3/4. (Kernel 2.4.x or above), Solaris 5.8
SNAPPiMON Agent - Microsoft Windows 98/XP/2000/2003 or RedHat Enterprise Linux, Release 3/4. (Kernel 2.4.x or above), Solaris 5.8
Database - Microsoft SQL Server 2000/2005 Standard/Enterprise or Oracle 9i/10g.
Browser - Microsoft Internet Explorer 6 or above.
Others - Sun Java Runtime 1.5.0_10 or above.