tMonitor™
Planning and Considerations

SLM tMonitor™

The Insight:SLM tMonitor measures transaction response time for both the server environment and network down to the user workstation. It also collects both network and server environment availability information for all end-users. tMonitor is a stand-alone Unix/Linux based device running the InsightETE transaction filter (tFilter™) to measure network and server environment time and availability filters (tsAvail™ and tnAvail™) to track network and server availability. It is typically placed in the network segment where the production servers reside.

The tMonitor watches transaction traffic from every end-user and creates a transaction audit trail for every system it is designated to watch. This audit trail consists of information for each 'end-user' transactions from the end-user view. To an end-user, a transaction response time is the time from when a request is started, usually when an enter key or mouse click is hit, until the response returns and is displayed on the user's workstation. tMonitor gathers the 'what', 'when', 'where', 'who' and 'time' for each transaction. This detail consists of the begin and end timestamp for the transaction, the time spent on the network, time spent in the server environment, the client IP address, the network segment where the end-user resides, the server IP address, the Transaction ID, the User ID, return code for the transaction, and additional information depending on the type of application (i.e. entity tags for BPM, software release, etc).

Because of the passive, non-intrusive way it is deployed, tMonitor can work with any type of system, no matter what platforms are used in the application environment, including mainframe, Unix, Tandem, and Microsoft based platforms. Any 'client-server' type system can be readily and instantly monitored. Many protocols, using both UDP and TCPIP based transports, have additional capabilities including *Bank ATMs, Argo Data, Spectrum, MQ Series, CICS, DB2, Oracle, SQL Server, Jacada*, Lexmark, MicroMedia Flex, etc. tMonitor can easily be configured for any 'home grown' type application as well.

tMonitor Placement

tMonitors must have at least two attachments to the network.

1. Regular network attachment with an IP address such that it can communicate with the Insight:SLM server. This attachment can be on an internal network just like all other servers in the production environment.
2. Span-port connection. This connection is used for monitoring network traffic (packet traffic) such that a transaction audit trail can be produced for the servers designated to be monitored.

tMonitor span-port connection and configuration is key to getting all of the data needed to monitor every end-user, identify their geographic location, get the functions they are performing and get their userID.

Careful planning is required so that the tMonitors are placed properly in the network environment such that all of the appropriate network traffic can be seen and parsed by the tMonitor.

tMonitors are also used to gather the appropriate data from the back-end tiers of an application system to analyze problems and alerts. This ability may require additional network connections on the tMonitor or additional tMonitors.

tMonitor Planning

- Create a document containing all of the servers in an application environment that are to be monitored. Include the 'server' ports that are presented by each server on behalf of the application in this document. Also identify the protocol for each of these server ports.

  - If only Insight:SLM is licensed for the application system, only the servers that are involved in communicating with the 'end-users' of the system are to be monitored.
  - If Insight:Analyzer is licensed for this application system, then all servers in the system need to be set up for monitoring including all of the application servers, database servers, etc.
- Obtain system diagrams from an application view.
- Obtain network diagrams with switches, servers, and firewall placement, or work with the network group to find appropriate switches to plug into to monitor targeted servers.
- Plan the tMonitor connectivity and placement with the network, server, application, security, and infrastructure groups.
- Make tMonitor and their associated span-ports part of the application system change control process.

tMonitor Considerations

- The use of tMonitor for constant monitoring may require a cultural change in some technical groups. This will likely be the first time that a 'span-port' becomes a production resource. Network groups typically use span-ports for testing, temporary analysis, and trouble shooting. Modern technology allows for span-port connections to be multiplied such that at least one on each network switch can be designated as a 'production' port for the permanent monitoring required by a tMonitor.
- tMonitors should be placed as close to the servers they're designated to monitor as possible.
- For monitoring end-users, tMonitors should be placed in front of any device that might 'nat' the client IP address. This is commonly a Cisco Pix device. If placed behind the Pix device, the user locations will not be available for the InsightETE Reporting and analysis.
- Plan for implementation of InsightETE SSL support or place tMonitors behind SSL and IPSEC translation devices. These devices de-encrypt encrypted network packets. If tMonitors are placed where it sees encrypted packets, then the transID, userID, BPM tags and perhaps accurate measurement of true end-user response time may be compromised.
- tMonitors are capable of monitoring 10s of millions of transactions per day. The same tMonitor can and should be set up to monitor many servers across many different application systems with many different protocols. Be sure there are enough network connections in the tMonitor for multiple span-port connections if needed.
- Be sure the span-port is set up for packet traffic in both directions. If a separate port is required, be sure there are enough network cards in the tMonitor to handle the connection.
- Consider extra network cards for each tMonitor for backup and future connectivity. Be sure the network cards match the speed of the network to be monitored.
- Consider redundant tMonitors, or at least a backup spare if monitoring is considered mission critical.