Agent-based and Agentless Monitoring - Primer

General Information

- Neither agent-based nor agentless approach to monitoring is superior. Both have their strengths.
- Most organizations choose a mix of agent-based and agentless data collection.
- For cost reasons, the majority of availability and performance monitoring will use agentless data collection and use agent-based data collection will focus on mission-critical applications.

Agent-Based Data Collection (Overview)

- Agent-based software resides on an IT element (such as a server) that collects data based on policy set centrally by the management server. These agents observe the state of IT objects, and communicate any detected state changes to the management server, where management policy is set. They can also collect, aggregate and analyze performance data that causes an event to be issued when a threshold is breached.
- Typically, the agents communicate with the management server only if policy breaches are detected (for example, when a performance or storage capacity threshold is exceeded) or at prescheduled times to upload historical data. Thus, the impact on the management server is much lower than on an agentless management server and, thus, the impact on the network (no constant polling for data) is also lower. (An agentless management server typically does all the polling, data filtering and threshold analysis.) However, there is a performance impact on the server being monitored due to the processing power the resident agent consumes. Depending on the vendor architecture, agent-based architectures can require an additional configuration effort associated with centrally setting policy, and deploying and updating the agents.
- Agent-based products can provide a level of IT management autonomy. Agents execute an action, such as restarting a process, based on a policy set by the central management server, even if the management server or its connection is lost. In addition, the agent can cache collected data, and then send the data once communication with the management server is restored, preserving the complete set of performance data for historical trend analysis or service-level reporting. Thus, the agent can take action regardless of the management server's communication availability.

Agentless Data Collection (Overview)

- Agentless monitoring can be approached in two ways:
- Data is made available via remote APIs — for example, Simple Network Management Protocol (SNMP) Management Information Base (MIB) for network devices or Windows Management Instrumentation (WMI) on Windows devices — thereby negating the need to deploy an agent to a server.
- Agentless monitoring is done by analyzing packet flow across the corporate network infrastructure with a sensing system (hardware or software) located at a strategic point in the infrastructure's topology. The system captures information about response time, availability and other flow-oriented functions as traffic goes by the sensing point. This approach is in line with monitoring end-user response times and with root-cause analysis.
- Although the industry historically has opted for placing agents on the servers they are intended to monitor, there are many companies that choose to use agentless approaches, which are easier to implement and administer for monitoring. Much of the data that companies seek is available via remote APIs. Typically, an agentless approach doesn't consume as many resources on a server being monitored, although remote polling has some impact on the server and more so on the network.

Agentless

Pros	Cons
• Dominant monitoring technology today • As vendors continue to add management functionality via APIs, there will be less need for agents on servers (at least for more mature platforms) • Lower license costs • Better implementation speed • Lower maintenance • Minimal impact on server load • Solution for "locked down" servers (where nothing can be loaded on server in addition to core application) • •Good option for less-mission-critical applications	• Increases performance demands on server, network – consume network resources (poor solution for clients with slow/remote network lines) • If high-availability not designed in: if server fails or network suffers connectivity issues, then agentless tool will stop collecting data and issues will not be detected. • If resilience is important, must ensure no single points of failure

Agent-Based

Pros	Cons
• Higher level of granularity: much higher polling rates down to sub-second levels versus typical 5-minute to 15-minute polling intervals for agentless approaches. • Less dependence on network being up: monitoring may still be accomplished autonomously when the network connection to server is disrupted. • Less network impact	• Affects monitored server resources • Administration management overhead • Longer deployment/implementation