IDERA® | Uptime Infrastructure Monitor Whitepaper

THE TRUTH ABOUT AGENT VS. AGENTLESS MONITORING

A Short Guide to Choosing the Right Monitoring Solution.

When selecting an enterprise-level IT monitoring solution, one of the first decisions the IT department needs to make is whether to look for an agent-based or agentless monitoring solution.

AGENT-BASED MONITORING

Metrics

Agent-based monitoring consists of a software component, typically a small application, which resides on the client server and collects data. The data is then returned to the monitoring station based on a policy within the local agent, or as requested by the monitoring station. In best practice situations, the agent responds with information based on requests originating from its monitoring station. This practice makes the agent very lightweight but able to access granular metrics for better monitoring, alerting and reporting, as well as deeper levels of root-cause analysis and trouble shooting.

However, some agents are very heavy consumers of resources and can stress the servers they are monitoring. For example, agents whose policy is not managed by the monitoring station, but by the agent itself, can impose heavy additional load on the client servers and reduce the overall performance of the servers and services they are supporting. Many framework solutions (like IBM Tivoli, HP Openveiw, BMC, Patrol, and CA Unicenter) employ this heavy agent model of storing data on the agent and the result is increased workload and use of disk space which can lead to poor server performance and even failure. Ironically, this effect is counter to the goal, as monitoring of performance with a heavy framework agent may actually degrade the performance of the servers.

The ideal solution is a lightweight agent (or 'invisible agent') that collects deep metrics, but doesn't introduce any recognizable load on the server. In order to get the most out of your monitoring solution, look for a product that gives you the deep monitoring you require without the negative impact on your servers. IDERA's product, Uptime Infrastructure Monitor, is one of the leading lightweight/invisible agent solutions, providing deep monitoring across many different server platforms, applications and network devices.

In these best practice agent-based solutions, the agents communicate with the monitoring station at predefined intervals, relaying the data back to a central repository for storage. Alerts are then generated if the metrics contained within the returned datasets exceed user defined thresholds.

One of the biggest benefits of using agents is the more granular data that is returned by agent-based solutions (one exception can be in the case of WMI and Windows platforms, more on that later). This allows the monitoring station to collect detailed metrics on the servers, log files, hardware and the individual processes.

This deeper level of system and service metrics provides better reporting, complete historical data for trending, smarter alerting and granular root-cause analysis capability. This translates into faster Mean-Time-To-Repair (MTTR) for service problems, more accurate capacity planning and insight into systems behavior for performance tuning. The end result is better performance, easier monitoring, less downtime and happier management.

Capabilities

By implementing an agent-based solution, advanced capabilities can be encapsulated within the agent functionality. The ability to directly interact with the client platform and its services allows the monitoring station to remotely execute automated actions for a more proactive IT delivery. Automated actions can include simple IT service recovery and maintenance tasks or more advanced actions like the spinning up and down of virtual capacity to account for fluctuating demand on IT systems. For example, a service monitor may be watching the log directory on an active Web server. When the directory exceeds a set capacity threshold, the agent can automatically compress and archive the log files, and begin a new set of logs, keeping the volume from filling and potentially crashing the Web server. Another example could include the monitoring station triggering a temporary increase in virtual capacity to meet a short-term spike in demand on the web server. The monitoring station could then have the additional virtual capacity spun down when the demand decreases, ensuring capacity resources are optimized and no virtual sprawl is created.

Agent-based solutions allow for greater flexibility with the creation of customizable service monitors. The administrator of the monitoring solution can create scripts and/or binaries that check the status of services/collect non-standard metrics from applications and hardware. These custom monitors can be used to extend the functionality of the product to support applications or services that are not covered by the monitoring station's core functionality.

Pros & Cons of Agent-Based Monitoring

PROS

- Deeper and more granular data collection for advanced monitoring, alerting and reporting.
- Proactive IT with automated actions that can avoid performance problems and downtime.
- Tighter service integration. Control applications and services on remote nodes.
- Extendibility of monitoring across non-standard metrics.
- Lower risk of downtime.

CONS

- The need to deploy and up date agents to systems.
- Internal approval for deployment on production systems in some companies.
- Up-front license cost of solution.

AGENTLESS MONITORING

Agentless monitoring is deployed in one of two ways: using a remote API exposed by the platform or service being monitored or directly analyzing network packets flowing between service components. Network packet analysis is typically implemented in addition to either an agent-based or agentless monitoring solution. Network analysis will not provide detailed metrics on the servers supporting the application services communicating over the network, but will provide data on service performance and availability. End-user experience monitoring typically includes network traffic analysis.

SNMP (Simple Network Management Protocol) is typically used to monitor servers and network devices in an agentless manner. In the case of Windows servers, WMI (Windows Management Instrumentation) is typically used and provides a much better set of metrics than can be obtained through SNMP monitoring alone. It should also be noted that VMware deployments can be deeply monitored using agentless monitors as well.

Metrics

SNMP Monitoring. A significantly reduced set of data is made available when compared to an agent-based or WMI monitoring approach. With SNMP, you are limited to what is exposed by the vendor, which cannot be easily extended in most cases. In agent-based monitoring, you would be able to extend the metric collection to include all the deep metrics, and not just SNMP exposed ones. Gartner strongly recommends an agent-based solution for monitoring mission critical applications and servers due to the level of metrics required to effectively monitor and manage critical services, and the potential to use agentless monitoring for non-essential servers and applications. As application and service vendors integrate management APIs into their products, this metrics gap is shrinking between agent and agentless monitoring, but this typically takes several years for the APIs to mature and several more for systems management vendors to fully support the APIs within their products.

WMI Monitoring. Windows Management Instrumentation (WMI) is a good example of how some vendors are exposing their deeper server and platform metrics for agentless monitoring consumption. For many Windows based servers and applications, agentless monitoring via the WMI gateway provides strong monitoring capabilities. However, there are some cases where an agent-based monitoring solution would be preferred. For example, a heterogeneous IT environment that includes Windows servers and additional platforms (UNIX, Linux, VMware, etc.) would be best suited for a solution that combines both agent-based and agentless monitoring together, in one dashboard.

Capabilities

Agentless SNMP solutions do not provide the same level of expansion and integration that is possible with an agent-based solution; Furthermore, agentless solutions typically do not provide the facilities to interact with the service platform being monitored with the same level of functionality as an agent-based solution. By not having an agent that can act as an arbitrator for commands being executed on the client by the monitoring station, it becomes very difficult to develop proactive and automated actions like service management and recovery scripts. Extending the monitoring capabilities of an agentless solution to include custom application and service monitors is either a very difficult development effort, or simply not possible. It should be noted that agentless monitoring via WMI (Windows only servers) or VMware (VMware only services and instances) can allow for some level of customized scripting.

Pros & Cons of Agentless Monitoring

PROS

- No client agent to deploy.
- WMI and VMware agentless monitoring is stronger than SNMP alone.
- Lower initial cost for software.
- Lightweight, no application to install or run on the client.

CONS

- No in-depth metrics for granular monitoring, alerting, reporting and analysis.
- Leave critical servers applications at risk of and performance problems and downtime.
- Can be affected by networking issues. WAN/VPN deployment can be challenging or non-functional.
- No ability to extend for custom server, service or application metric collection.

WHAT IS THE BEST SOLUTION FOR YOUR NEEDS?

Purchasing decisions for IT systems monitoring software should be made around the business metrics and SLAs that IT provides to the business in order to prove the value of IT. These higher level metrics (and SLAs) should be monitored and reported on, all the way down to the critical server and application metrics that make up the SLA.

The important concept to understand is that monitoring is one step in the IT Systems Management process; a right fit solution should include capacity planning, SLA monitoring and reporting, deep historical reporting, smart alerting functions and monitoring across all servers (UNIX, Windows, Linux, VMware, etc), applications, networks and devices within the IT environment. Not only this, but a systems monitoring solution should incorporate both agent-based and agentless monitoring options, so you can get the best monitoring fit across your datacenter, including deep agent-based monitoring for critical servers and applications and fast, easy agentless monitoring on Windows, Virtual or non-critical infrastructure and services. The solution needs to be able to handle all of this, across multiple platforms and environments at a cost that makes the CIO smile. Below is an example of how an IT monitoring solution should provide value to all levels of the IT Organization.

IT MONITORING SHOULD SHOW VALUE FOR ALL ROLES

The right choice for most enterprises is a streamlined software solution that can handle all of the important needs discussed above. It should help IT managers communicate their value to the business units (or the internal/external stakeholders consuming IT services offered by the IT department).

Look for an easy to use and cost effective IT systems monitoring solution that provides both agent-based and agentless metric collection for the best of both worlds. This allows the IT department to report on the services they are providing from an availability, performance, and reliability point of view. Having detailed metrics also allows IT to be more proactive in their service management, by analyzing the current and historical data to ensure enough capacity available to meet the current and future needs of their consumers.

The IT Food Chain

SYSTEM ADMINISTRATOR

Monitoring & Alerting. Fast Root Cause Analysis & Lower MTTR.

IT MANAGER

Proactive IT Management. Capacity Planning & Reporting.

VP/DIRECTOR OF IT

Set, Monitor & Report on SLAs. Optimize Global IT Resources.

CIO

Showcasing the Value of IT to the Executive Team

FREE IT MONITORING CHECKLIST & FEATURE/COST CALCULATOR

If you are considering evaluating IT Monitoring and Dashboard solutions, this **IT Systems Management Vendor Evaluation Checklist** and **Product/Vendor Feature and Cost Calculator** are an excellent way to start. They are designed to be vendor agnostic and customizable to help you compare different products. A free download is available here:

Download Here