

Agent vs. Agentless Systems Management

Agent-Based Solutions Provide Better Availability and Security Benefits

No politician ever said, "It's all about the architecture, stupid," but maybe they should have. The fact is, the way your IT systems management solution is engineered does matter. Today's business environment is putting unprecedented pressure on IT organizations to manage increasingly mobile and diverse devices. When they're architected correctly, IT systems management solutions are better able to detect these remote, diverse machines, perform more powerful executions on them and ease much configuration pain for the IT staff.

The goal, of course, is to find the right tool for your individual business needs.

While there are appliances, cloud services and point products, the debate really boils down to agent-based solutions versus agentless solutions. Both provide the feature set required by any-sized organization from a 20-user mom and pop to a large enterprise with 5,000 employees, allowing administrators to monitor, maintain, update, back up and secure distributed machines. But agentless and agent-based solutions go about providing visibility into and control over managed systems through two distinct methods.

Agent-based IT systems management solutions deploy agents on managed systems that execute commands directly from the remote computer's hard drive. A connection to a central server is required, but most of the processing is completed locally. Conversely, agentless management solutions don't require that software be deployed on each system. Instead, the software probes computers and executes commands from a central server through a network connection or over the Internet.

Because all software requires IT resources, both architectures do have an effect on performance. Agent-based solutions can degrade individual device performance while agentless solutions sap network bandwidth. The key is to mitigate their impact on performance without limiting management functionality.

It's safe to say that performance degradation is pretty much a wash. We can argue degrees of impairment, but productivity is impacted either way. However, there are other critical differences in agent-based versus agentless solutions that do make a difference—namely availability and security.

Since data collection and processing occurs over the network, agentless solutions are essentially rendered useless if the network goes down.

The Case for Availability

The ability to manage devices at all times—regardless of network status—is important when choosing an IT systems management solution for your organization.

Stored and run on the managed machine, agents are protected from outside influence and can continue to operate when non-agent based software may be effected by network, authentication or configuration issues. Agentless solutions, on the other hand, are at risk from network outages, requiring a robust network connection between the system and a central management server. Since data collection and processing occurs over the network, agentless solutions are essentially rendered useless if the network goes down, taking away visibility into the network and inhibiting the ability to manage systems just when you need those capabilities the most.

Conversely, agent-based solutions can still perform automated tasks from the remote computer's hard drive if the network fails, giving administrators the tools they need to address outages and continue managing devices.

The Case for Security

Maintaining a consistent and robust security strategy across the entire organization is an increasingly critical issue as systems continue to become more mobile and more diverse. IT organizations typically have to manage systems on separate, disparate networks with varying IT and security policies and often are forced to work around multiple firewalls.

This is a huge disadvantage of agentless IT systems management solutions. It is difficult to probe machines through a firewall without complex configuration or additional hardware on the client side. As a result, many organizations are forced to make security compromises in order to give them the visibility and control around the firewall. If the security compromises are unacceptable, automated processes are virtually impossible, and administrators are forced to rely more heavily on manual maintenance.

On the contrary, firewalls do not have to be compromised in order to manage devices with an agent-based IT systems management solution because commands are executed from the individual systems' hard drive. As a result, the environment is inherently more secure without sacrificing automation or management functions.

The Bottom Line

The performance degradation of agentless and agent-based IT systems management solutions is essentially the same. However, agent-based solutions provide inherent availability and security benefits, including the ability to manage systems during a network outage and the ability to manage systems around firewalls with no additional configuration.

Maybe, it is all about the architecture, stupid.
Just don't tell the other guys.

**...agent-based solutions
provide inherent
availability and security
benefits, including the
ability to manage systems
during a network outage
and the ability to manage
systems around firewalls...**

Contact Kaseya Today

Remote access and remote control of managed devices needs to be integrated within a single management framework, allowing you to conduct powerful maintenance on distributed machines without putting the firm at risk and without disrupting users. Kaseya provides this level of integration, consolidating remote systems management on a single pane of glass.

Contact Kaseya today for more information and to request a live demo of our powerful IT Systems Management solution.

www.kaseya.com | facebook.com/KaseyaFan

About Kaseya

Kaseya is the leading global provider of IT Systems Management software. Kaseya solutions empower virtually everyone — from individual consumers to large corporations and IT service providers — to proactively monitor, manage and control IT assets remotely, easily and efficiently from one integrated Web-based platform.

©2011 Kaseya. All rights reserved. Kaseya and the Kaseya logo are among the trademarks or registered trademarks owned by or licensed to Kaseya International Limited. All other marks are the property of their respective owners.

