Kaseya

Our Automation. Your Liberation.™

Agent vs Probe

A review of IT Management Strategies

Contents

Introduction	3
Infrastructure View	4
Centralised Infrastructure	4
Distributed Infrastructure	4
Performance View	4
Security View	6
Summary	7
Conclusion	7

Introduction

A rapid change in IT infrastructure combined with an increased number of roaming devices is creating a more challenging environment for service managers to effectively manage and secure. The ongoing diversity of both equipment and operating systems generates gaps in service coverage, forcing manual intervention for many routine tasks such as software updates and security patches. In cost conscious times IT professionals seek to identify any processes that might be automated to save time and subsequently money. Automating routine updates (rather than have engineers drive miles to implement changes at multiple sites) is one obvious area where efficiencies may be achieved. But IT management is rarely simple and identifying a technical strategy for implementation is not straightforward.

At a grass-roots level the technology employed by various IT infrastructure management tools can have a significant impact on that strategy and heavily impact what is the right choice of tools to meet these challenges. The key two that are often discussed are probe and agent based technologies, but each of these have their own inherent character. For example management tools that use probe technology to interrogate devices can have an adverse impact on network traffic. Agent technologies can degrade individual device performance and may require additional hardware at remote sites. Common ‘free’ tools such as Microsoft SMS and Novell Zenworks which use these approaches are often unable to report on all devices, particularly if they are not running Microsoft Windows. Expensive investments in complex suites of products that use probe technology may negate operational savings.

With a need to maintain SLAs whilst implementing efficiencies, a review of the two technical solutions available to IT management is long overdue. This White Paper takes a look at the technical basis of these management options and whilst does not deliver a detailed technical comparison, comments on the main issues from an infrastructure, performance and security perspectives, hopefully giving the main points for consideration when deciding on a strategy for IT management for your business.

Infrastructure View

The type, architecture and complexity of different infrastructures has an impact on the relative performance of Agent and Probe technologies. As the scope of this paper is limited we examine two contrasting infrastructure types: centralised, with a limited number of locations and distributed, with many remote and mobile locations.

Centralised Infrastructure

Enterprises with the majority of employees in fixed and geographically concentrated locations may be supported by highly centralised infrastructures. Management of such environments may appear to be more straightforward: managers are physically closer to equipment; support may be more immediate and often more visible. In such environments selection of system tools such as SMS and Zenworks might be a sensible option. The distance (and number of hops) between device and central control points for example is limited, so that regular polling of the network might not be an issue. With the majority of devices within a fixed network, the probes ability to scan and discover equipment is often perceived as an advantage. With components in close proximity, the processing of device information may be achieved locally, and directly. Networks in centralised environments tend to have more capacity available, not relying on busy WAN links for example, enabling regular polling without loss of performance. However, NMS monitoring tools, using ICMP protocols for example, can produce false positives when the network gets heavily loaded. Agent technologies, in the centralised infrastructure might appear to be overkill; where each device has management intelligence installed. In this case it could be machine performance that can be impaired and the need for local resources on the machine to host agent applications can reduce device capability.

In centralised environments, where the network is relatively simple and most devices are fixed, probe technology, with its smaller impact upon machine performance can often be seen as a simpler approach. However, managers need to consider the number and variety of device types and operating systems to be monitored or managed. Many probe based polling systems may not be able to see or manage every aspect of a device using probes, as security policies or management interfaces may not be supported on every device.

Distributed Infrastructure

Many enterprises today have highly distributed infrastructures. Sites may be global, with employees working from a variety of locations: home, office, hotel or even a cafe. Numerous devices may be on the corporate network intermittently, creating inherent challenges. The distance between sites and number of locations means that there are likely to be many firewalls and a plethora of network equipment. Such environments are typically heterogeneous, with legacy systems and a variety of operating systems. Using probe technology to manage these environments has several disadvantages; network capability (especially to remote locations) can be limited and the ability to poll devices severely compromised and totally remote machines may give not option to probe at all. Mathematically speaking, systems need to poll at double the rate of any anticipated change in

order to 'keep up' with monitoring important changes and that is just not realistic in such environments. There may also be a requirement for multiple probes; one for each type of operating system/device on the network. In such scenarios as this, service gaps will appear.

A further complication of probes based on a domain such as active directory is the requirement to manage addresses, authentication and implement port mapping schemes at each site.

Agent technology, which often has the advantage of reducing network traffic can mean much more detailed information is available, as generally only differentials are reported back to the central repository for action rather than needing to scan every part of a device with each communication. However, managers can only monitor devices with agents installed; rogue devices or components that have not been properly added to the network may be missed. Management of the agent population has to be taken into account; some complex implementations may require significant resource to manage the management system themselves, an important consideration when the main goal of management systems is usually to simplify internal IT service delivery.

However, in highly complex heterogeneous environments agent technology may have the edge; where having local intelligence minimizes network load and can provide far more control over an individual device or machine.

Performance View

Examining the relative impact on performance of management systems is problematical. Different infrastructures will respond differently to either probe or agent technology. In general however, the principle that management systems should complement rather that compromise efficiency is a sensible one. Any impact on performance would have to be significantly outweighed by the benefits the technology delivers. Where performance may be impacted of course depends upon the technical solution: probes tend to adversely affect the enterprise network, agents can negatively affect the components managed.

Complex, multi-layered agent technology will take processing and physical resources from the components it manages. Some vendors have chosen an appliance approach to help mitigate performance degradation. Yet appliance solutions have their own drawbacks in terms of space, power and management, sometimes placing an appliance on every site can add an unwanted overhead.

Probe technology on the other hand will usually take minimal resources from devices but may have an adverse effect upon network components. Performance will be further degraded as the number devices or machines to be managed increases.

From a performance perspective both technologies require infrastructure resources to operate. In general terms, probe technology is more suited to centralised infrastructures and agents dispersed infrastructures. From a performance perspective the degree to which an infrastructure is either disbursed or centralised often determines the optimum technical solution.

Probe technology is more suited to centralised infrastructures and agents dispersed infrastructures

Security View

Any information transfer can compromise security and all IT management activity, requiring an interrogation of assets, represents weakness that hackers may exploit.

Most organisations first line of defence is the firewall; where the organisation physically meets the open Internet. For many service managers, compromises between security and management must be made. If a distributed infrastructure is to be managed efficiently using probe tools, then (to a degree) the firewall guard must be softened. The subsequent increased risk may not be acceptable to the business, thus increasing the reliance upon manual updating of patches and software. This in itself is flawed: the event horizon for security threats may be measured in minutes for some kinds of vulnerabilities. If it takes hours to deploy an engineer to implement a security patch at a remote site then the infrastructure could be compromised. Service managers who think that such breaches are confined to the unlucky and the dispersed may want to review articles detailing breaches in UK local authority's IT systems.

http://www.theregister.co.uk/2009/09/04/ealing_council_mystery_malware/

Agent technologies do not suffer the same issues. Firewalls do not need to be compromised in order to manage devices. As such agent technology is inherently more secure than probe solutions, as long as they do not require inbound connections to devices in order to support communication.

Summary

As infrastructures become increasingly distributed and the number of roaming devices increases, it becomes ever more difficult to secure and manage environments using only probe technology. In such conditions and under high network loads, probes can return false information. And the requirement to open ports for management tools may create increased security risk.

Agents installed on the managed device, could be taking up physical and processing resources. They may degrade performance, especially if the device is small or under resourced. The more comprehensive the management solution, the ‘heavier’ it is likely to be, which may compromise performance.

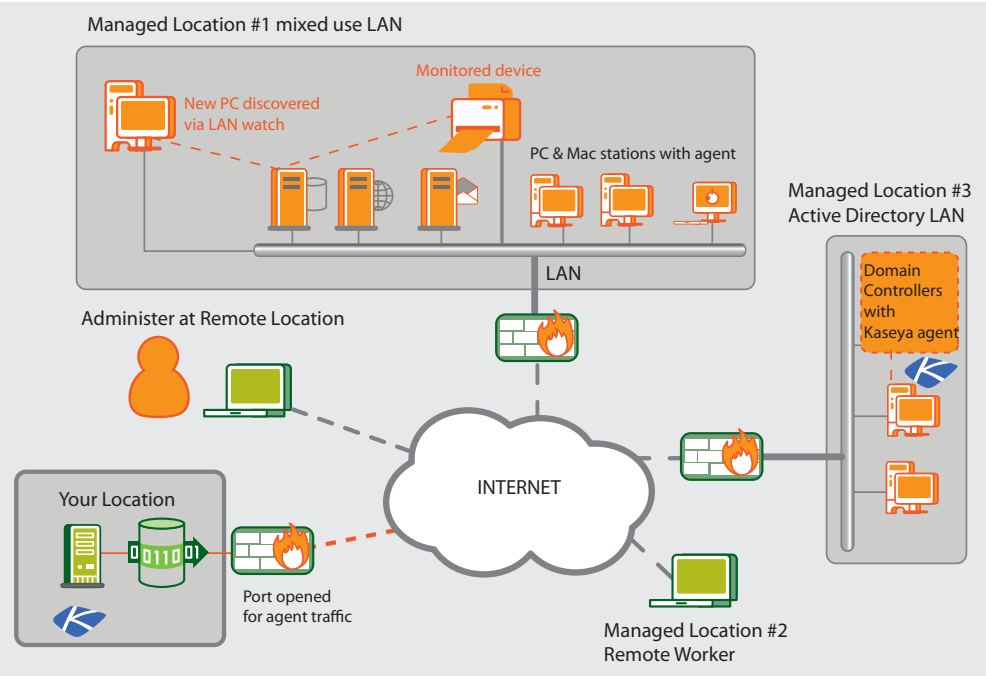
Probe and agent technology offer significantly different approaches for delivering IT management. It might appear that no one management strategy is ‘better’ than another, both provide benefits and both have weaknesses.

In general terms however, probe technology is better suited to homogeneous, geographically concentrated environments, whereas distributed environments might benefit from an ‘agent’ approach. The answer is not clear cut. Business need, the number of different devices, operating systems and the infrastructure itself needs to be taken into account.

Do we have to accept compromise?

Conclusion

The lack of a clear winner surely means that all solutions involve a degree of compromise, exposure to risk and sub-optimal efficiency. Should service managers simply accept less than perfect tools to do their job?



The obvious solution to ensure the best of both worlds and limit both performance overhead and risk is to use a Hybrid approach of agents on devices which need the stronger management ethos and can sustain the small overhead of running a local management application, and use a probe based approach on devices that sit within the bounds of a higher performance and more secure environment, thereby negating the weaknesses of each but benefiting from the obvious advantages of each.

The same can be said of how this fits into the different environmental challenges faced in managing network environments, where within a LAN on a controlled environment, dependency on know conditions such as available bandwidth, network settings and authentication, probes can be effective and allow communication with non-agent devices such as specialist hardware, or network devices.

By splitting the approach and using agents with specific device capabilities and probes where advantageous, the agents can be much more lightweight than traditional heavier agents which might negatively impact machine performance. In this way probes are also only deployed as needed and from within the environment and can be much more targeted to local need, reducing the network overhead and management of standard probe based approaches.

In an increasingly diverse and complex IT world, the day of the Hybrid management platform has arrived.

About Kaseya

Kaseya is a global provider of IT automation software for IT Service Providers and Public and Private Sector IT organisations. The Kaseya® IT Automation™ Framework allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

Kaseya

Our Automation. Your Liberation.™