Kaseya White Paper

Eight Keys to Cloud Friendly Systems Management

www.kaseya.com

At the same time that organizations are moving many of their IT assets to the cloud, the problem of how to manage all of an organization's IT assets has, in many ways, become more complex. Scenarios include public cloud, private cloud, hybrid cloud, BYOD, the mobile workforce, software-by-subscription, and more — in most cases existing side-by-side with legacy LAN-based client/server architectures that look a lot like they did in the 1990s.

Meanwhile, systems management models, by and large, have not kept up — leaving IT managers with a hodgepodge of domain-based point solutions they must cobble together in order to get even a fragmented view of what's happening in their environment. The result is often unused software, unmet user requests, lack of agility, and unending firefighting. Managers are too preoccupied at coping with "routine" issues, they have little time to focus on strategic initiatives that can actually move the business forward.

This is not why organizations move to the cloud. To make a cloud migration "work" they need systems management solutions based on a model specifically aligned to cloud objectives such as scalability, capital preservation, and agility — recognizing that "the cloud" itself typically means a blended environment with some very un-cloudlike features. Cloud migrations will not be successful if organizations can't deal with the "real" cloud rather than the one they see in TV commercials.

Here are eight keys to such a "cloud friendly" systems management model and why they are important given the reality organizations face:

1. SaaS-based

Besides simply being intuitive, there are many technical and business reasons why systems management should itself be in the cloud, if what you're looking for are cloud benefits — scalability, agility, pay as you need, and the rest. Of course, just hosting the service on a remote server doesn't necessarily guarantee the service will be "cloud like" — it must be designed to be — which brings us to the other seven keys.

2. Hybrid Cloud Architecture

The premise of the cloud is that it offers a very fluid environment in which components, services and even use-cases can be mixed and matched without the friction that comes from operating across silos. A hybrid cloud architecture encompasses cloud and non-cloud based IT assets alike under a single management layer so that reports, audits, monitors, configuration controls, policy automation, and other management features apply equally everywhere as enabled from a single point of control by the system administrator.

A potential barrier to implementing this type of architecture is how difficult it is to connect new sites with the cloud server (hosting the management layer) whenever the IT organization wishes to do so. Ideally, those connections are completely secure and allow systems to be fully managed "out of band." In other words there is no requirement for address management, implementation of port mapping schemes at each site, the establishment of cumbersome VPNs to all the sites, or any other forms of IT "overhead." All you should need is a standard outbound port such as might be used for any Internet connection — web browsing, for example.

Kaseya

3. Full scope

Fixing the "hodgepodge" problem requires an all-in-one (but not a one-size-fits-all) solution. The solution must be both wide and deep. That's wide, meaning it addresses the full spectrum of management needs and pain points, such as inventory, anti-virus, backup and patch management. And deep, meaning not just covering those needs but covering them in a feature-rich way — as in deployment, configuration, execution, update, log, reporting, monitoring and automated remediation.

One measure of a system management solution's scope is the number of IT management reports it provides and the ease with which it provides them. (If the solution can't report or alert on an item, how else would it help you to manage it?) Some obvious management reports would include:

- Hardware and Software Inventory
- Asset Change
- Windows and 3rd party Patch Status
- Security Status
- Capacity Management
- Systems Utilization
- Policy Compliance
- Availability Management
- Network Usage and Statistics
- Event and Log Management
- File Share Audit

To illustrate the depth required, taking the File Share Audit as an example, such audits might include reports on what file shares have been created on all the computers within the environment, regardless of location, whether the platform was desktop or mobile or whether the file was in the cloud or on one of the computers in a local network — and would include accessibility to those files. The security status report would include endpoint security settings on all computers, including AV engine(s) installed, active status and date of last update.

4. Well integrated

One of the main reasons for the success of ERP was that everything came in the box and everything, more or less, talked to each other. A cloud-friendly systems management model would offer this same value proposition, but without the long implementation effort, time and expense ERP has often required.

One sign that your system management integrates your various systems and platforms (both cloud and non-cloud) is in your ability to keep up with and apply security or software changes throughout your environment. This task is becoming increasingly challenging as your networks span ever more locations, include ever more domains, traverse ever more firewalls and includes more and more remote and home users. And it's not just because you have to scan for and apply fixes. Often patches must be deployed in a test environment, undergo an approval process and otherwise require multiple steps to deploy. Different types of tools (hopefully automated) are required to accomplish those steps — in the right order, based on predefined policies, and work across silo boundaries such as the aforementioned locations, networks, domains, firewalls and mobile users.

5. Manages platform diversity

You could also say, "manage non-Windows devices," or "includes MDM (mobile device management)." The issue is dealing with an increasingly diverse and mobile environment populated with different operating systems and with devices outside traditional organizational and geographic boundaries.

The days of the "Windows only" enterprise are long gone. Linux is well established as a server operating system, and you are likely to find individual Mac users throughout the organization. That's in addition to those traditional "Mac preferred" departments such as marketing where Macs still reign in many organizations.

Mobile is probably the poster child for platform diversity — including Android (which itself has many variants), iOS, Windows Phone 7 and Blackberry. These differences make it hard, for example, to have a desirable level of visibility into a device, including serial number, operating system, firmware status, installed applications and other inventory data. Bandwidth limitations, meanwhile, require that any management clients installed on the device be able to run autonomously without a live connection to the Internet — and that they can be installed via a simple web link or text message.

Sys admins may also want a little platform diversity of their own when it comes to which browser they'll use to access the cloud-based system management solution: Internet Explorer, Chrome, Firefox or Safari. Rather than be forced into a one-size-fits-all administration experience — they'll want to use the browser they prefer.

6. Value-added content

Another benefit of going to the cloud is its "click-to-deploy" advantage. Ideally, organizations would want to set up their systems management in minutes, not weeks. One key to doing that is having out-of-the-box content such as predefined templates, scripts, and policies based on actual years of real-world systems experience that could also be easily and quickly tailored to an organization's specific needs.

Policy setting and enforcement is one area in particular where organizations can often use a jump-start. If you run IT, you are probably expected to know each machine by name and category and be able to provide IT costing and inventory information for each user department. Without policy automation that covers all policy categories (e.g., inventory, remote access, monitors) accomplishing this task for more than a few machines can be daunting. But it can also be daunting even with policy automation when you set up your automation scripts the first time if you have to do so without some "out-of-the-box" scripts to guide you. Such "out of the box" system management can, for example:

- Assign multiple policies to each machine
- Determine which policies are obeyed or ignored if a conflict arises
- Check that each machine assigned one or more policies is in compliance
- Show policy status across the organization on a consolidated dashboard
- Enable manual policy overrides

7. Scalable pricing

Scalable computing means consuming (and paying for) only as much or as little as you need when you need it. The transition to cloud computing has brought with it commensurate pricing models that allow organizations on both sides of the relationship (provider and customer) to benefit. Providers (including cloud-based systems management providers) get to "prove themselves" while customers get to try out services with less risk.

8. Multi-tenant management

A cloud-based solution or service may consist of many individual applications, platforms or even service providers that are brought together under a single branded offering — either for internal users or for commercial resale. To leverage costs, a single provider may also support multiple use-cases or multiple organizations. Such "multi-tenant" scenarios call for a systems management views right sized to specific user domains — whether a managed service provider or corporate IT organization.

Organizations moving to the cloud will only achieve the benefits they seek if they take into account the system management issues that can come with a cloud migration. Solutions that were designed to manage less diverse environments are proving they are not up to the task — and can undermine the very purpose of a cloud migration before it even starts. That's why organizations should assess the cloud readiness of their systems management solution just as they would any other aspect of their cloud strategy.

The Ultimate Solution

Kaseya SaaS is the ultimate solution for providing complete network management, automating recurring IT tasks and aligning IT with business goals from a reliable and secure web-based platform.

The unique Cloud based architecture of Kaseya means that no site servers, dedicated hardware or appliances are required. IT administrators can easily manage systems on small or large, local or remote sites and even roaming machines with no need for VPN's or special configuration.

With industry leading FIPs certification, the Kaseya system uses an AES encrypted connection over a single TCP port to the Cloud infrastructure to create a highly secure connection and provide complete peace of mind.

Through a simple lightweight download, Kaseya delivers high value services with less required resources on your managed systems. And whether you have multiple or single domains [or none at all], Kaseya fits easily into your existing environment.

For more information, please visit www.kaseya.com/solutions/saas-products.aspx

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.

Kaseya

www.kaseya.com