

PC LIFE-CYCLE MANAGEMENT

Ultimate endpoint orchestration tools

LANDesk, Altiris, Zenworks lead the way in six-vendor test

BY FRANK OHLHORST

Desktop virtualization, Web apps, software-as-a-service, and an increasingly mobile user base have created new challenges when it comes to endpoint management. Nonetheless, there are still some constants — endpoints need to be deployed, configured, patched, secured and supported.

With that in mind, we tested six PC asset management packages: Symantec's Altiris Client Management Suite, Novell Zenworks 10, LANDesk Management Suite, ScriptLogic's Desktop Authority, Dell's Kace appliance and Kaseya Small and Medium Enterprise Edition.

The tools we tested share many similarities. For the most part, they combine inventory, policy management, remote control, application provisioning and reporting into a single, cohesive management application. All use a client/server model with a software agent installed on the endpoint and a server application installed on a network server or appliance.

However, there are differences that define each product.

- Dell's Kace comes in appliance form, eliminating much of the setup work and minimizing disruption to the network during installation.
- ScriptLogic's Desktop Authority relies heavily on script-driven policies to execute tasks and manage events.
- Symantec's Altiris Client Management Suite strives to be a platform for adding additional capabilities, such as endpoint security, advanced backup and network access control (NAC).
- Novell's Zenworks 10 Configuration Management product is part of a new management architecture designed to manage multiple sites and networks using multiple servers and management zones, making the product highly scalable.
- LANDesk Management Suite has a new integrated management console in front of the company's suite of products to create a tool that appears to be more than the sum of its parts.
- Kaseya Small and Medium Enterprise (SME) Edition is a product that doesn't have all the features of the other products, but is easy to set up and operate.

All of the products have wizards, help screens, technical support and upgrades to support larger enterprises. Kaseya SME Edition favors smaller enterprises, while Novell's Zenworks seemed destined for the largest of networks, with the rest of the products falling somewhere in between.

Our Clear Choice Test winner is LANDesk's Management Suite, which proved to be one of the easiest packages to use and provided excellent documentation and support. Symantec's Altiris CMS 7.0 followed close behind and offered a robust platform for integrating additional products and showed a high level of integration. Novell's Zenworks took the third spot; although a little balky to work with, it offered one of the most robust feature sets, supported numerous client types and is highly scalable.

The fourth spot went to Dell's Kace K1100, which proved an appliance can be a viable method to quickly deploy an enterprise-level application. Dell's guided installation was second to none and the included Webex session really speeded things up. Desktop Authority showed a great deal of promise; all of the main components were there, and powerful scripting capabilities made the product very flexible. However, a product like Desktop Authority takes a commitment and introduces a significant learning curve, which is often the price of flexibility and customization. Finally, Kaseya SME Edition is an excellent product, but lacks some critical features, such as full-fledged policy management, that may give some administrators pause. Otherwise, Kaseya proves to be easy to deploy and use and is a good fit for smaller, single site deployments.

Here are the individual product reviews:

Product: Altiris Client Management Suite 7.0

Company: Symantec

This product is designed for large heterogeneous enterprise networks and offers a feature set to match, including endpoint discovery, inventory, imaging, patch management, software deployment, endpoint provisioning, remote control and reporting.

The product is designed around two primary goals — management and support. The product is very heavy into the life-cycle management portion of monitored devices, focusing on inventory, software licenses and usage. However, that does not detract from the support end of the equation,

where CMS offers software and patch management, deployment tools and remote control capabilities.

We were able to quickly deploy the client software to our test systems by using a group policy from our Windows server. Altiris offers clients for all major Windows versions, many Linux endpoints and Macintosh PCs.

We were then able to create a comprehensive inventory of devices connected to the network, deploy clients to those devices and then start to manage those devices by pushing out applications, patches, updates and other key elements. We found that the inventory discovery portion of the product was easy to use and identified all of our attached devices using a scan. We also defined additional scans to detect new devices as they were added to the network.

The product offers the ability to create images of corporate PCs and then deploy those images over the wire to new endpoints, effectively provisioning new devices (and new users) on the corporate network. We found that the imaging application did an effective job of creating base images from a reference PC; however, the imaging process can take some time and is affected by available bandwidth, as well as the size of the image. It was also simple to create a policy using a wizard to push the image to a new system.

We found that CMS also offers a comprehensive inventory module, which can create reports on every OS, application and piece of hardware associated with an endpoint.

CMS's integrated remote assistance capabilities easily allowed us to take control of remote PCs, chat with users and troubleshoot problems in real-time. We also liked the ability to blank the user's screen, allowing us to fix a system without any questions from the user. Also, we liked the ability to share the screen, which comes in handy to teach a user how to do something or for us to demonstrate a procedure.

Of course, being part of the Symantec family gives Altiris an advantage. Symantec has long developed and sold imaging software, remote control software, patch management software, and inventory management software, which has been integrated into CMS.

Integration of Symantec's various products comes across as seamless, all capabilities have a similar look and feel. All of which adds up to a reduced learning curve and a lessened need for

vendor tech support. Symantec offers several support resources, ranging from online community-based support to live chat with Symantec engineers, although due to the comprehensive documentation, you may never need to use additional support resources.

Installation was not overly complex, just time consuming, due to numerous steps and meeting the prerequisites, including a Windows server, .Net infrastructure and SQL Server.

Ease of use is another theme that permeates CMS — most chores are wizard driven or at least feature a step-by-step process that ensures even neophyte administrators should be able to get up and running quickly. We found the wizards comprehensive and easy to understand.

For those looking to follow the Symantec track, there are several other advantages offered by CMS, including the ability to integrate with other Symantec products, such as endpoint security, backup, enterprise life-cycle management and other products.

All in all, Altiris Client Management Suite is a good foundation for asset management and can prove to be a good starting point for other management and support capabilities, all while making an administrator's life a little easier.

**Product: Kaseya Small and Medium Enterprise Edition
Company: Kaseya**

Kaseya is one of the major players in the world of IT asset management, to the extent that several large managed service providers (MSP) have standardized its products. However, you don't need to sign up with a gigantic MSP to garner benefits from Kaseya's management products.

The company offers site-based solutions in the form of its Enterprise Edition and Small and Medium Enterprise Edition (SMEE) products, which offer a robust subset of capabilities formerly found only on its MSP-level products. The enterprise edition and the SMEE differ only in included tools — for example, the enterprise



edition includes elements such as a service desk, antivirus, desktop migration and data security controls, which are not found in SMEE.

We focused on SMEE because it proves to be a good fit for a smaller, single-site network, looking to keep costs down.

We found capabilities such as inventory management, patch deployment, software distribution, remote control, scripting and reporting all well represented in Kaseya's product.

We were able to step through installation of the product rather quickly. For smaller enterprises, everything (the Kaseya Server and Database) can be installed on a single server.

We used the included wizard to install the product and had no problems.

As with other PCCLM tools, you will need to install a small client application on each endpoint to enable management. We did this using the deployment wizard provided by Kaseya and it proved to be a relatively painless experience. The client installation was completely automated by the wizard. The client application handles gathering inventory, executing scripts and all of the other capabilities associated with the product.

Kaseya's biggest strength is the level of automation offered. It proved to be very easy to create scripts that offered a multitude of capabilities for administrators looking to modify a PC's settings, install applications and provision new PCs.

We only needed to define what we wanted to occur based upon triggers or policies, which force a script to execute. That helped to make applying patches and upgrades to managed systems very easy.

The product's inventory and auditing capabilities prove to be rather comprehensive. We were able to quickly identify all of the major hardware and software components on a tracked PC immediately after the inventory process completed. That information can be used to drive updates, monitor for changes or identify potential problems.

SMEE is also equipped with Kaseya's IT Systems Management Kit. The kit includes hundreds of predefined network views, report templates, third-party device monitoring, patch-approval policies, and a comprehensive set of IT automation scripts for routine maintenance, third-party software deployment and proactive alerts.

Overall ease of use is complimented by the product's browser-based console, which incorporates a dashboard with a management system that supports drill-down capabilities. We liked the dashboard's real-time view into asset functions, which can be set up to display various alerts, such as processor spikes, failed patches or access problems.

We were able to quickly troubleshoot PCs with the product's remote control capabilities. We were able to interactively control remote PCs, chat with remote users, as well as perform remote reboots and application installation. Other capabilities include some user-centric features, such as the ability to submit trouble tickets or request support.

However, the elephant in the room with SMEE is the concern over whether or not the product includes everything an administrator needs or is it just a stepping stone to one of Kaseya's MSP-based solutions. For those with smaller networks that are not experiencing exponential growth, the answer is no — simply because combining SMEE with native network management tools should provide all of the management smarts needed to effectively pull off PCCLM chores. But should you have to self-integrate tools when so many other PCCLM options are available on the market?

NETRESULTS

Product name	LANDesk Management Suite 9	Altiris Client Management Suite 7.0	ZENworks 10 Configuration Management	Kace K1000 Series	ScriptLogic Desktop Authority 8	Kaseya Small and Medium Enterprise Edition (SMEE)
Company	LANDesk Software	Symantec	Novell	Dell	Quest Software	Kaseya
Cost	\$48 per node.	\$47 per node.	\$69 per user for 1,000 users.	\$8,900 for 100 nodes; additional nodes \$39 each.	Starts at \$43 a seat	About \$50,000 for 1,000-seat license, depending on configuration.
Pros	Comprehensive feature set; excellent management tools.	Strong feature set; focus on life-cycle management; platform for adding endpoint tools.	Comprehensive feature set; platform-based approach.	Appliance-based easy install; intuitive interface; helpful wizards.	Close tie-in with Windows systems, script-centric approach.	Simple install, comprehensive feature set for SMBs.
Cons	Installation can be complex.	May be overkill for some networks.	Can be complex to install; difficult to use.	Limited upgrade, resiliency options; capital expense; app deployment can be complex.	Patch management, imaging not included in base package.	No service desk, policy management, or integrated anti-virus.
Score	4.6	4.1	4	3.875	3.7	3.5

SCORECARD

Product	LANDesk LMS	Altiris CMS	ZENworks 10	Kace K1000	Desktop Authority	Kaseya SMEE
Feature set (35%)	5	4.5	5	3.5	4	3
Dashboard and console (15%)	5	4	3	4	4	4
Ease of use/deployment (15%)	4	3.5	3	5	3	4
Additional features (15%)	4	4	5	3	3	3
Reports and alerts (10%)	5	4	4	3.5	4	4
Documentation and support (10%)	4	4	2	5	4	4
Total	4.6	4.1	4	3.875	3.7	3.5

SCORING KEY: 5: EXCEPTIONAL; 4: VERY GOOD; 3: AVERAGE; 2: BELOW AVERAGE; 1: SUBPAR OR NOT AVAILABLE

Product: LANDesk Management Suite
Company: LANDesk Software

LANDesk Management Suite consists of four separate but integrated products:

- LANDesk Inventory Manager.
- LANDesk Power Manager.
- LANDesk System Manager.
- LANDesk Server Manager.

The combination of these four products enables LANDesk Management Suite to offer the capabilities needed for effective PC asset management. Although each tool can operate independently, LANDesk has created a singular interface that we found very easy to use, with each element grouped together by function.

During our testing, we found that LANDesk has gone to great lengths to create client discovery and deployment options then ensure any attached PC is discovered and included in client distribution. LANDesk offers the typical capabilities including, discovery and inventory, patch and application distribution, imaging and deployment, remote control and policy creation, and reporting.

However, LANDesk puts a little more oomph behind some of its native capabilities. For example, once we set up the hardware discovery process, we were offered options for the process to run constantly, which identifies a new PC as soon as it attaches to the network. Most other products rely on a scheduled sweep to detect new hardware.

That discovery process proves to be the key to deploying the LANDesk client. We were able to define policies that auto launch scripts to stream the client down to new assets, whenever a new PC is detected. The product's management console lends itself well to the creation of policies, executing events and running reports; it was easy to navigate and policy creation was simplified with step-by-step help. The console supports full drill-down capabilities and is customizable; we were able to easily create groups, change sort orders or track customized fields associated with assets.

When it comes to provisioning a new PC, the

ability to image a master copy of a deployed OS proves to be of utmost importance, since that image represents a predefined enterprise desktop. The included imaging tool can be used to quickly capture a master image, which is then stored for later distribution.

We were impressed with the fact that you are not tied down to a single imaging product; LANDesk allows you to use third-party imaging (or migration) tools as well, which means you can automate the tools that you are already familiar with and leverage images that may be already created.

LANDesk's software distribution capability offers some impressive features, such as the ability to deploy software packages from multiple package servers. That allowed us to create a distributed model for deploying applications, locating the resources as close as physically possible to the user. The net result is a reduction in installation times and network traffic. We found that makes software deployments, upgrades, patch management and other distribution-related procedures less painful.

We used a wizard driven, step-by-step procedure to capture the software installation process, which in turn is used to create a deployment package. We were able to distribute that package using a distribution script, which we also created using a wizard.

For troubleshooting and help desk purposes, LANDesk incorporates an integrated remote control package. We were able to quickly seize control of remote PCs. We were able to then blank the screen (if needed), reboot the remote system and chat with the user. One advantage offered by LANDesk is the ability to view inventory data (hardware and software), as well as the PC's history during a remote control session.

The product also offers comprehensive inventory, status and usage reports, which we found helpful during management tasks, allowing us to quickly track down elements that can affect perfor-

mance or dictate a system's compatibility with applications. The inventory capabilities can also be used to determine budgets and plan for upgrades.

We were impressed with the product's dashboard, which offered a quick way to view the status and health of monitored PCs in real-time.

Installation was rather complex and time consuming, although LANDesk does provide adequate step-based installation instructions that guided us through the process. However, there are numerous elements that must be addressed — ranging from the number of management servers, software deployment servers and the types of clients to be managed. Basically, the product works using a Windows Server, SQL Server and the associated hardware. The roles, features and software must not be installed on what the company refers to as a "core server" (the server running the management engine, or a domain controller) and other elements, such as ASP.NET and Web Services Enhancements 3.0 must be included during the installation.

Overall, LANDesk is our Clear Choice winner because of its sophisticated, well-integrated feature set and its excellent management tools.

Product: Desktop Authority 8
Company: ScriptLogic

Desktop Authority 8 offers all of the major features one would require to manage desktop PCs.

However, we were surprised to find that some common features, normally found in a PCCLM tool, were absent. Critical capabilities, such as patch management and imaging, are only offered as options to the base package.

Initially, that does help to lower costs, and it does shift the onus of patch management back to the tools normally found in operating systems. However, in the end, it proves to be easier to manage a desktop environment with all of the tools centralized into a single product.

We found no surprises during the installation

of Desktop Authority, which for the most part was very simple. There are some minimal prerequisites that must be addressed; however, those requirements prove to be almost inconsequential. The product uses two SQL databases — one to store inventory and configuration information, and the other to store reporting data.

The product offers several strengths, including the ability to leverage existing group policies, login scripts and user directories. Desktop Authority seems to combine server and PC management in a way that develops a symbiotic relationship with the Windows Server operating system. Those looking to tighten that relationship can choose Desktop Authority System Center Edition, which fully integrates into Microsoft's System Center management infrastructure.

Much of the product's capabilities comes from the login script process, where native login scripts can be replaced by Desktop Authority created scripts to deploy clients, applications, change settings and so on. Desktop Authority also offers a Wake on LAN (WoL) capability, which can boot a PC remotely and apply settings and changes to that PC once it boots.

Application deployment is primarily handled by MSI (Microsoft installer) packaging and associated scripts. That retains much of the native application installation process, which can reduce incompatibilities and eliminates the need to build different MSI packages for different hardware or OS versions. However, MSI-based installations do need user input to succeed. To counter that requirement, Desktop Authority offers auto scripting, which in most cases can turn an MSI-based installation into an unattended event.

Much of the functionality of the product relies on a Boolean logic engine that examines endpoints to determine what should happen as part of a management event. Although that sounds complicated, Script Logic has endowed Desktop Authority with a technology called Validation Logic. In short, administrators can quickly create scripts based upon Validated Logic using wizards that define what should happen on each PC, when and why. The Validation Logic database contains thousands of elements that can be used to determine a course of action, ranging from detected registry settings to major OSs to PC types.

The idea is to bring a level of granularity to PC management that is appropriate for environments with thousands of PCs. For example, an administrator can define a script that only affects Windows XP PCs in a single department, which have a particular application installed.

The level of granularity is impressive and proves to be a great way to migrate PCs or create commonality among environments by only impacting the PCs that fall outside of an accepted configuration.

Extensive configuration capabilities round out

the product's management capabilities. Administrators can quickly define basic settings, such as drive mappings, printer selections, user accounts and so on, due to the product's ability to work closely with group policies.

And there's the advantage of being much easier to use than tools bundled in with the network operating system. That ease of management is further extended with comprehensive reporting, where administrators can quickly define reports to see what policies and scripts are in place and what endpoints will be affected by those elements. What's more, a comprehensive inventory report helps track physical assets, identify problem areas and offers rudimentary change management capabilities.

Desktop Authority meets the support mission with remote control capabilities, where administrators can fully control remote endpoints, even in the off hours, by using the product's WoL capabilities.

Desktop Authority takes a different approach, relying heavily on scripting and triggering. There is nothing wrong with that and many administrators may feel more comfortable with scripts that offer detailed information, instead of policies that hide much of the mechanics behind the scenes.

Desktop Authority's tight integration with existing Windows networking technologies as well as its script-centric approach makes the product a good fit for established, enterprise networks that are heterogeneous in nature. Administrators preferring granularity over commonality may find Desktop Authority a refreshing approach to asset management.

Product: ZENworks 10 Configuration Management Company: Novell

ZENworks has been around in one form or another for close to 20 years. In its early days, Novell offered ZENworks as a PC configuration management application for Novell Netware-based networks, running DOS or Windows 3.1 clients.

ZENworks has evolved into a full-fledged PCCLM tool that works with multiple OSs and endpoints. ZENWorks 10 Configuration Management is very different from previous versions of ZENWorks, featuring a completely new architecture and design.

ZENWorks 10 strives to think of everything an administrator could need, at least when it comes to managing a diverse ecosystem of IT assets. However, that can make the product very complex and difficult to use, especially if you are trying to leverage all of the various features and capabilities. Novell offers extensive training and support options to counter some of the inherent complexity that may arise when using the product on multisite, enterprise networks.

Nonetheless, ZENworks 10 Configuration

Management (ZCM) was relatively simple to install, due to a wizard-driven installation program. However, the prerequisite planning can become a little complicated when integrating multiple management servers, external databases, satellite servers and different management zones.

To help tame the installation process, a 90-page installation guide (PDF) proves to be an excellent point of reference. However, it is probably a good idea to set aside several hours to go through the manual, prep your systems and perform the actual install.

For smaller implementations, both the ZCM management and database servers can be installed on a single Windows 2003 or 2008 server. Other requirements include installation of the Microsoft .Net framework and several management ports to be opened on the corporate firewall. For larger networks, you can choose to set up additional management servers, satellite servers, management zones and so on — all in all, ZCM proves to be very robust for large, multisite networks.

With Zenworks, deployment of the client can be automated using policies.

Management of the product (and the associated assets) occurs via a browser-based management console. The layout, which is divided up by assorted tabs, was quite easy to master. The GUI offers drill-down menus, tips and associated help files, and Novell has tried to use plain English or simplified menu descriptions, making it a little easier to plod through the numerous choices.

The inventory module was very well executed — inventory is gathered by the agent and stored in the database, while the inventory management menu acts as a portal into that information. We were able to search through various inventory items, create reports and drill down into specifics with ease. The ability to customize reports and filter the results is a nice touch, allowing us to quickly group together systems by CPU or OS or most any other inventoried item. A powerful inventory module proves to be very important, because it can become the basis for generating scripts and policies based upon detected settings.

For example, when we created a policy-driven script to install Service Pack 3 on Windows XP systems, the inventory provided the information for which systems were running Windows XP, but not SP3.

We also found the application deployment capabilities very robust, allowing us to define almost any installation element associated with an application installation. For example, we were able to capture the installation changes made by MS Office and then create a script to deliver those changes (and others) down to a subject PC. To do that we used an application creation wizard to build a deployment package, created some automated responses to drive the application installation and then defined a policy to determine where



PC LIFE-CYCLE MANAGEMENT

(and when) to push the application package down to a client system.

For the most part, the process proved straightforward, although, if you are working with multiple OSs, you may have to tweak the install policy to deal with the nuances of those different OSs. Fortunately, Novell provides a number of tools to fine tune application packages and to experiment with the results before going live.

We were also impressed by Novell's remote control capabilities, which not only included all of the normal bells and whistles, but also offered the ability to silently watch activity on remote systems. That may sound a little like spying (and in fact it is), but that can be a powerful tool to determine if a system is being used properly.

Other notable capabilities include the ability to quickly define pre- and post-installation scripts, which can be used to further automate patch application and application delivery. One thing to note is that the patch management component requires a subscription service, but that service includes predefined patching policies for more than 70 vendors. That takes most of the pain out of patch management and we were able to create patching chores with just a few mouse clicks. In addition, there are several predefined reports that offer compliance information, making it a little easier to determine if the subject endpoints meet the latest compliance requirements.

Novell's ZCM 10.3 may very well be the most comprehensive PCCLM tool on the market, thanks to the company's platform approach.

Product: Kace K1000 series

Company: Dell

The typical PC Configuration Life Cycle Management (PCCLM) tool comes with deployment challenges that can make an IT administrator cringe. Critical questions, such as what server to install, or what database is needed, can lead to additional effort, cost and management burdens.

With Kace, IT administrators take a different approach to systems management — one that starts with plugging in a new piece of hardware (an appliance) and then configuring the

management capabilities. That methodology offers several advantages, such as no interruption in existing services, no lengthy installations, no configuration or compatibility challenges and no customization of the existing infrastructure.

However, an appliance-based solution is not without its downsides, including managing a piece of proprietary hardware, additional costs of the hardware and limited upgrade or resiliency choices. Nevertheless, appliances are still an attractive way to quickly solve most IT problems.

The Kace appliance incorporates all of the critical functions that an IT administrator needs to manage desktop assets in the enterprise. The Kace K1000, which is a 1U rack mount appliance, includes device discovery and inventory, patch management, configuration and policy management, application management, remote control and asset reporting capabilities. The Kace appliance is available in two versions: the K1100, which supports as many as 3,000 endpoints, and the K1200, which supports as many as 20,000 endpoints.

The Kace appliance has a simplified setup, in part due to Dell, which bundles in Webex-based training services. The Dell technician was able to walk us through the installation process and help us to define our initial policies, as well as perform our first inventory and deploy the desktop client.

Administrators of any skill level should be able to deploy a K1000 series with little hassle. Easy setup is only part of the product's overall ease of use.

We used the product's Web-based dashboard and management console to manage our test systems, as well as deploy applications, patches and clients. One of the first things we noticed is that the interface is intuitive and offers easy-to-understand context-sensitive help. However, we really liked the product's comprehensive wizards, which could help us through most any procedure.

We found it quite easy to install the client application with Kace's push technology, which automatically deploys the client application to newly detected endpoints. If you want to have a little more control over the process, you can use a number of manual methods, ranging from group

policies to login scripts to Kace's own manual installation, which can be accessed via a Web page.

Once an endpoint is equipped with the client, the real management magic begins to happen. Kace offers a plethora of tools, policies and wizards that ease deployment and management for the endpoints. Patch management is handled by an integrated version of Patchlink Technologies' patch management product. We were able to automatically push out patch packages with policies created using a wizard.

Application deployment takes a little more finesse, because each application is virtualized, using a methodology called "Virtual Containers". Virtual Containers take a lot of the pain out of installing apps, since they contain all the supporting dynamic link libraries and other files needed by each application. The technology also virtualizes registry changes, which prevents conflicts with other applications. However, there is a downside — we needed to create a Virtual Container for every application we wanted to deploy for every operating system supported. For example, if you want to deploy MS Office to Windows XP, Windows Vista, Windows 7 32-bit and Windows 7 64-bit, you will need to create four Virtual Containers. Although the process is straightforward, it becomes more complex and time consuming as more operating systems are supported.

We also took a look at Kace's remote control application and found that it covers the basics of support adequately. A robust selection of add-ons helps to extend the product's value with help desk integration, server management and security auditing. All things considered, Kace does succeed in bringing simplicity to the complex chore of managing IT assets and perhaps no other product can get administrators started as quickly and easily. ■

Ohlhorst is a technology journalist and IT business consultant with more than 20 years of experience with enterprise IT systems. He can be reached at fohlhorst@gmail.com.