

Tech Outlook



Servers, Simplified

Automated server management with Lenovo XClarity improves efficiency and enables innovation.

Server virtualization has been embraced as a means of improving data center efficiency, delivering easily identifiable benefits such as improved server utilization, reduced hardware costs and faster application deployment. The process is not without drawbacks, however.

The ease with which virtual machines (VMs) can be generated and de-

ployed creates the risk of uncontrolled proliferation, or VM sprawl. Organizations that have underinvested in systems management and automation tools wind up employing labor-intensive management processes that result in wasted resources and significant IT burdens.

The net result that is that IT organizations use up to 80 percent of their IT budgets on basic operations and

maintenance, leaving just 20 percent for business innovation. That's simply not sustainable in today's business environment.

“Even the best IT team on the planet cannot effectively support strategic initiatives when they're constantly tied up with day-to-day tasks such as provisioning, configuration, monitoring and administration,” said Tommy Whatley, VP of Advanced Services, ProSys. “An automated server-management solution can virtually eliminate these manual processes, reducing the risk of human error and increasing IT agility.”

Lenovo XClarity is a new solution that gives IT the ability to fully automate the provisioning, configuration and management of servers, which helps control VM sprawl and improves the efficiency of the IT team. XClarity

continued on page 2

TECH OUTLOOK

PRSR T STD
U.S. POSTAGE
PAID
Tulsa, OK
Permit No. 2146

XClarity

continued from page 1

creates a “single-pane-of-glass” view of the virtualized environment with an HTML 5 dashboard that allows fast location of all resources.

Minimizing Complexity

XClarity addresses critical requirements, including the need to centralize and streamline x86 hardware resource management. It automates the discovery, monitoring, firmware updates, configuration management, and bare-metal deployment of operating systems and hypervisors across multiple systems — helping to speed deployment of both cloud and physical infrastructure.

“The automation features allow IT to cut the deployment time for server stacks from days to minutes for rapid return on investment,” said Whatley. “It also cuts the time it takes to deploy new applications or make changes to existing applications.

“By automating repetitive and error-prone manual operations, server-management automation minimizes complexity and allows IT to focus on higher-impact activities to increase the overall value for the business.”

Lenovo unveiled the solution just seven months after completing its acquisition of IBM’s x86 server business to become the third-largest global x86 server hardware supplier. The solution comes in two editions. XClarity Administrator is designed for Lenovo’s own System x servers and the Flex System converged infrastructure platform, scaling easily for up to 560 x servers or 20 Flex System chassis. XClarity Pro is designed to integrate with other widely used server solutions such as Microsoft’s System Center and VMware’s vCenter.

“We continue expanding our enterprise solutions portfolio to enable our customers to optimize infrastructure performance and reduce cost of owner-

ship, regardless of their environment,” said Darrel Ward, vice president, Lenovo’s Enterprise Systems Marketing and Enterprise Storage Business Unit. “Lenovo XClarity dramatically simplifies system management, helping organizations do more with less, while the networking solutions deliver great performance, optimized for Lenovo server and storage solutions, at an extremely attractive price point.”

Hands-Off Approach

XClarity Administrator is a virtual appliance that is quickly imported into a virtualized environment, which gives easy deployment and portability. The tool reduces complexity through out-of-band agentless management, which means managed endpoints do not need special software agents or drivers to be installed or maintained. Because it is agentless, Lenovo XClarity Administrator removes operating system (OS) dependency and is one less component to certify in the workload stack.

XClarity Pro includes the Administrator edition, along with the VMware and Microsoft integrators. The software streamlines server maintenance in cluster environments by dynamically shifting workloads from affected hosts through automated, non-disruptive rolling reboots and firmware updates. Additionally, Lenovo XClarity Pro reduces unplanned downtime by dynamically evacuating workloads from affected hosts during predicted hardware failures.

XClarity delivers fast time-to-value through automatic discovery of existing or new network endpoints, including rack servers or converged system inventory. These discovered assets can be viewed via the XClarity dashboard almost immediately, reducing hardware inventory time from days to seconds. The dashboard instantly provides a centralized view of any events or alerts generated from managed endpoints.

For simpler and faster provisioning of systems, XClarity uniquely deploys operating systems or hypervisors onto

bare metal servers. VMware ESXi, Windows Server and Red Hat Linux images can be imported and held in a repository for images, with as many as 28 OS images able to be deployed concurrently.

Security and More

XClarity includes several security features, including the ability to implement NIST SP 800-131A and FIPS 140-2 compliance. It supports self-signed SSL certificates and external SSL certificates to establish secure connections, and includes an audit log that provides a historical record of user actions, such as logging on, creating users, or changing user passwords.

XClarity also features extensive REST APIs that provide deep visibility and control over hardware resources from external, higher-level cloud orchestration and service management software tools from Microsoft, Red Hat, VMware, IBM and others. For example, developers can exploit the REST APIs to centrally orchestrate both the virtual and physical infrastructures to make cloud resources available to tenants faster.

Configuration management is where XClarity really shines. Lenovo has developed system configuration patterns and templates that can be saved and reapplied to multiple servers and compute nodes to substantially reduce the time and headaches involved in deployment.

“IT staff can become bogged down fighting fires instead of focusing on innovative services that can drive business value,” said Whatley. “This fire-fighting approach pulls resources from strategic project work, and creates both direct costs and indirect opportunity costs. Server automation with Lenovo XClarity will improve IT operations by automating routine, repetitive tasks prone to human error, and these improvements will translate directly into cost savings and increased innovation.”

News Briefs

Much Security Spending Wasted

As much as 60 percent of security software in some organizations is “shelfware,” products that are either underutilized or not used at all, according to a recent Osterman Research survey conducted on behalf of Trustwave.

Osterman surveyed 172 small, midsize and large enterprises from multiple industries. The study found the average organization spent \$115 per user on security-related software in 2014, but \$33 of it — 28 percent — was underutilized or not used at all.

Examples of technologies being underutilized included firewalls that were installed but never properly configured with the right rule sets, database monitoring tools that were implemented but never looked at later, and data leak preventing tools with few policies for monitoring data loss.

Thirty-five percent of survey respondents said that software was sitting on the shelf because IT was too busy to implement it properly, while 33 percent said that IT didn't have enough resources and 19 percent said IT did not understand the software well enough. Eighteen percent cited insufficient vendor support.

Study: IT Hiring Challenges to Persist

IT industry executives anticipate that filling technical positions will continue to be a challenge in the coming year, according to CompTIA's recently released “IT Industry Outlook 2015.” In the survey of executives from nearly 650 IT companies, 68 percent of respondents said they expect to face a challenging or very challenging hiring environment for technical positions this year.

Meanwhile, the U.S. Bureau of Labor Statistics reports an unemployment rate for computer and mathematical occupations at less than half the national rate, further confirming the strong demand for IT workers.

“Companies across our industry are delivering affordable, creative technology solutions for businesses and consumers alike, but the persistent shortage of workers educated, trained and certified in the latest technologies threatens to stall the pace of innovation,” said Todd Thibodeaux, president and CEO, CompTIA.

A net 43 percent of U.S. IT companies report having job openings. Another 36 percent say they are fully staffed, but would like to make new hires to support business expansion and growth. One in five companies have postponed or canceled projects due to understaffing.

Technicians and IT support and service personnel top the list of positions IT companies expect to pursue in 2015. Other in-demand skills include application development, cloud expertise, security expertise, network engineering and data and analytics expertise.

Tech Outlook

Copyright © 2015 CMS Special Interest Publications. All rights reserved.

Editorial Correspondence:

7360 E. 38th St.,
Tulsa, OK 74145
Phone (800) 726-7667
Fax (918) 270-7134

Change of Address: Send corrected address label to the above address.

Some parts of this publication may be reprinted or reproduced in nonprofit or internal-use publications with advance written permission. Tech Outlook is published monthly by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.

ProSys locations

Atlanta, GA
(Headquarters)
Phone: 678-268-1300
Toll-Free: 888-337-2626
chash@prosys.com

Atlanta, GA
(Integration Center)
Phone: 678-268-9000
Toll Free: 888-337-2626
twheless@prosys.com

Austin, TX
Phone: 512-658-5847
Toll Free: 888-337-2626
jwestmoreland@prosys.com

Birmingham/Montgomery, AL
Phone: 205-314-5746
Toll-Free: 800-863-9778
birminghamsales@prosys.com

The Carolinas
Toll-Free: 888-337-2626
chash@prosys.com

Knoxville, TN
Phone: 865-310-8843
Toll-Free: 800-863-9778
pmadden@prosys.com

Lexington, KY
Phone: 859-887-1023
Toll-Free: 800-863-9778
dclmmons@prosys.com

Louisville, KY
Phone: 502-719-2101
Toll-Free: 800-863-9778
dclmmons@prosys.com

Miami, FL
Phone: 305-256-8382
Toll-Free: 800-891-8123
lspivot@prosys.com

Mid-Atlantic
Phone: 800-634-2588 ext 2
midatlantic@prosys.com

Nashville, TN
Phone: 615-301-5200
Toll-Free: 800-863-9778
dclmmons@prosys.com

New England
Toll Free: 800-634-2588 ext 1
newengland@prosys.com

New York/Metro
Toll Free: 800-634-2588 ext 3
nymetro@prosys.com

Seattle
Phone: 425-939-0342
sballantyne@prosys.com

Tampa, FL
Phone: 813-440-2410
800-891-8123
lspivot@prosys.com



Unified communications (UC) once was viewed as a way to reduce costs and simplify administration by bringing together communications tools for telephony, email, text, instant messaging, videoconferencing and presence into a single platform. However, UC quickly evolved into a valuable, strategic resource, capable of boosting productivity and innovation by enhancing the quality of collaboration and improving access to data and services.

Today, the technology is evolving once again with the migration of UC applications and services to the cloud, allowing organizations to take advantage of a Unified Communications-as-a-Service (UCaaS) delivery model. The ability to deliver a set of business communications services through a highly scalable IP communications infrastructure makes UCaaS an increasingly attractive alternative to on-premises communication platforms.

“There’s a growing preference for cloud-based services, particularly in mid-to-large enterprises, and UCaaS is riding that demand,” said Bill Haskins, Senior

Analyst & Partner for Massachusetts-based Wainhouse Research. “Putting unified communications in the cloud makes great economic sense: the infrastructure is there, the support mechanisms are in the place, the training program is ready. Plus, fewer IT and purchasing resources are required to manage it.”

UC in the Cloud

Rapid growth of subscription-based unified communications expected.

Cost Savings and More

In a recent report on the global UCaaS market, Wainhouse Research noted that all signs point to rapid growth in the industry as both telephony and non-telephony service providers compete for market share. While there are hundreds of providers currently in the market, analysts expect a great deal of consolidation over the next few years. Key players now include Cisco, Avaya, Alcatel-Lucent, Microsoft, IBM, HP, CSC, Voss, Verizon Communication and Polycom. Wainhouse Research predicts the market will be worth approximately \$5.3 billion by 2018, with a five-year compound annual growth rate of 24 percent.

Not surprisingly, the cost factor makes UCaaS attractive to many organizations. Instead of purchasing, configuring, deploying and managing an on-premises solution, those costs and responsibilities are assumed by the service provider. For a monthly fee, users can simply access enterprise-class UC technology and applications on any Internet-connected device. Users enjoy a consistent UC experience anytime, anywhere, which allows for greater business agility and productivity.

UCaaS provides the flexibility to quickly scale services up or down according to business needs, creating operational efficiency by enabling organizations to pay only for what they need. Service provider data centers typically have more resiliency and redundancy than customer environments, making it possible to maintain high levels of performance and minimize the risk of downtime and data loss. Similarly, UC support is handled by the service provider's team of IT specialists, which often improves the speed and quality of support.

Weighing Options

It's important to recognize that UCaaS is one approach to UC, and organizations need to determine if cloud-based UC is the right fit. Many IT managers are leery of moving mission-critical applications to the cloud, especially when dealing with increasingly complex regulatory compliance requirements. Organizations need to make sure the service provider understands and is capable of maintaining compliance.

In addition to regulatory compliance, existing technology investments must be considered. UCaaS makes the most sense in new facilities that have no communications service, or when a total overhaul is needed. Otherwise, organizations should make sure their UCaaS strategy is compatible with existing applications and user equipment. Employees should also be ready to embrace a new communications system, which should be trialed and tested before making a final decision.

Still, there is a widespread perception among telecommunication experts and industry analysts that UCaaS will inevitably overtake on-premises solutions as the platform of choice for organizations of all sizes.

"As the use of mobile devices within organizations grows, employees need the ability to collaborate from any device and from any connected location," said Audrey William, Frost & Sullivan's head of research for information and communications technologies. "Many organizations are reluctant to continue investing in on-premises solutions, which often have multi-year contract agreements. There is a significant shift toward third-party hosted and managed models, and service providers are playing an important role in the overall UC market."



Stay connected and productive

Enable your users to access applications anytime, anywhere, and at a fixed cost. Take advantage of voice, video, mobility tools, and more. Cisco Powered collaboration cloud services are best-in-class, flexible and scalable cloud services designed to help you achieve faster time-to-value. You will benefit from superior levels of service, security, and 24-hour support from Cisco partners who undergo rigorous certification and a third-party auditing of their solutions.

Contact ProSys to learn more



www.prosys.com 888-337-2626

© 2015 Cisco. All Rights Reserved. CIS-120



Mobile App Security

Organizations must take steps to ensure mobile applications don't create security and privacy risks.

It's all about the apps.

Mobile devices such as tablets and smartphones have fundamentally changed business processes over the past few years by providing unprecedented connectivity and driving new levels of productivity, efficiency and job satisfaction. What makes these devices powerful business tools rather than just fun electronic toys is the ever-expanding ecosystem of mobile applications.

Billions of purpose-built apps are downloaded each year, allowing users to access real-time business data, auto-

mate key processes and gain powerful insights. Equally important, organizations have greatly expanded efforts to create mobile versions of all the enterprise apps they've been using for years.

However, the growth of mobile apps is matched with an inevitable rise in security issues.

Attackers are increasingly seeking — and finding — vulnerabilities in mobile apps that can expose both business and personal data to risk. According to Gartner analysts, 75 percent of mobile apps fail the most basic of security tests.

“Most enterprises are inexperienced in mobile application security,” said Dionisio Zumerle, principal research analyst at Gartner. “Even when application security testing is undertaken, it is often done casually by developers who are mostly concerned with the functionality of applications, not their security.”

Mobile Malware Increasing

Other studies seem to support Gartner's findings. A recent report from Alcatel-Lucent's Motive Security Labs division says that malware infections in mobile devices increased by 25 percent in 2014. The firm estimates that 16 million mobile devices worldwide have been infected.

The report claims mobile malware is increasing in sophistication, with more robust command and control protocols. Six of the top 20 mobile threats in 2014 were mobile spyware apps designed to track a device's location, monitor incoming and outgoing calls and text messages, monitor emails and track the victim's Web browsing.

Malware growth continues to be aided by the fact that the vast majority of mobile device owners do not take proper device security precautions. The Motive Security Labs survey found that 65 percent of subscribers expect their service provider to protect both their mobile and home devices.

“With malware attacks on devices steadily rising with consumer ul-

tra-broadband usage, the impact on customer experience becomes a primary concern for service providers,” said Patrick Tan, General Manager of Network Intelligence at Alcatel-Lucent. “As a result, we’re seeing more operators take a proactive approach to this problem by providing services that alert subscribers to malware on their devices along with self-help instructions for removing it.”

Proactive Testing is Key

Still, businesses can’t afford to depend solely upon software vendors and service providers for the security of their mobile computing environment. Gartner says it is imperative that organizations develop their own methods and technologies for mobile application security testing and risk assurance.

Gartner expects existing static application security testing (SAST) and dynamic application security testing (DAST) vendors will modify and adjust these technologies to address mobile application cases and meet mobile application security testing challenges. Although SAST and DAST have been used for the past six to eight years and have become reasonably mature, mobile testing is a new space, even for these technologies.

In addition to SAST and DAST, a new type of test — behavioral analysis — is emerging for mobile applications. The testing technology monitors a running application to detect malicious or risky behavior in the background. For example, this test would raise a red flag if an active audio player accesses a user’s contact list or geolocation and initiates data transmission to some external IP address.

Testing the Server Layer

Testing the client layer — the code and graphical user interface — of the mobile application that runs on the mobile device is not enough.

The server layer should be tested as well. Mobile clients communicate with servers to access an enterprise’s applications and databases. Failure to protect a server creates the potential for highly damaging database breaches. Code and user interfaces of these server-side applications should therefore be tested with SAST and DAST technologies.

Gartner predicts that through 2017, 75 percent of mobile security breaches will be the result of application misconfigurations rather than deeply technical attacks on mobile devices. A classic example of misconfiguration is the misuse of personal cloud service through apps residing on smartphones and tablets. When

used to convey enterprise data, these apps lead to data leaks that typically go undiscovered.

“Today, more than 90 percent of enterprises use third-party commercial applications for their mobile BYOD strategies, and this is where current major application security testing efforts should be applied,” said Zumerle. “App stores are filled with applications that mostly prove their advertised usefulness. Nevertheless, enterprises and individuals should not use them without paying attention to their security. They should download and use only those applications that have successfully passed security tests conducted by specialized application security testing vendors.”

Agency Develops Guide for Vetting Mobile Apps

A new publication from the National Institute of Standards and Technology (NIST) provides guidance for organizations to improve security for mobile devices and apps. The guide, “Vetting the Security of Mobile Applications,” outlines strategies for assessing the security and privacy risks associated with mobile apps, whether developed in-house or downloaded from mobile app marketplaces. The publication is also a guide for developers seeking to understand the types of vulnerabilities that can be introduced during an app’s software development cycle.

The guide offers plans for implementing the vetting process and considerations for developing app security requirements, and describes the types of app vulnerabilities and the testing methods to use to detect them.

The document also provides guidance for determining if an app is acceptable for an organization to use. The guide says organizations should develop security requirements that specify, for example, how data used by an app should be secured, the environment in which an app will be deployed, and the acceptable level of risk for an app.

The NIST guide says vetting mobile apps involves “a sequence of activities that aims to determine if an app conforms to an organization’s security requirements.” The process of vetting an application consists of careful testing and looking at the results to either approve or reject the app.

The NIST guide is available at <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf>.

redefine

what's

possible

Automation drives innovation. Lenovo's XClarity automated server management solution enables administrators to deploy infrastructure faster and with less effort. Systems management also becomes less complex. Relieved of responsibility for many time-consuming manual processes, the IT organization is freed to devote more time and focus on innovative technologies that can drive business value.

Contact your ProSys representative to learn more.

SIMPLIFY MANAGEMENT

INCREASE EFFICIENCY

CONSOLIDATE INFRASTRUCTURE

IMPROVE AGILITY



www.prosysis.com 888-337-2626