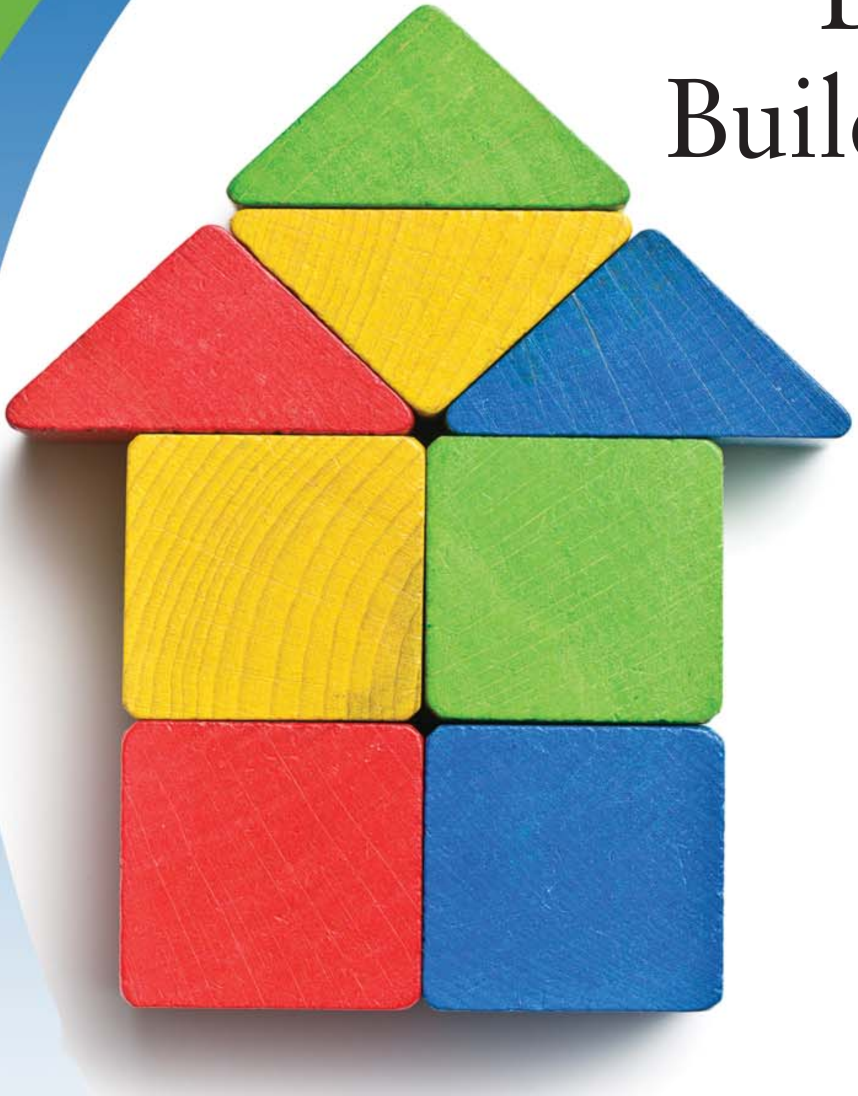
February 2015

PROSYS

Tech Outlook

Data Center Building Blocks



VMware's EVO: RAIL appliance enables the software-defined data center.

Traditional network architectures are increasingly ill-suited for modern data center workloads. An explosion of mobile devices and content, cloud services and server virtualization are placing a significant strain on the hardware-centric networking designs that have been used for nearly 30 years.

Legacy networks built on tiers of switches, routers and protocols essentially tie applications to specific servers, which require days or even weeks to reconfigure when changes are necessary. That is a major drag on operations at a time when organizations need increased agility and efficiency from their IT infrastructure.

"Networks have customarily been built on a box-by-box basis, with devices added as needed, configured independently and managed manually," said Matt Merriman, VP of Professional Services, ProSys. "That's just not practical anymore. Years of continually adding servers, storage devices and networking gear to meet evolv-

continued on page 2

Data Center Building Blocks

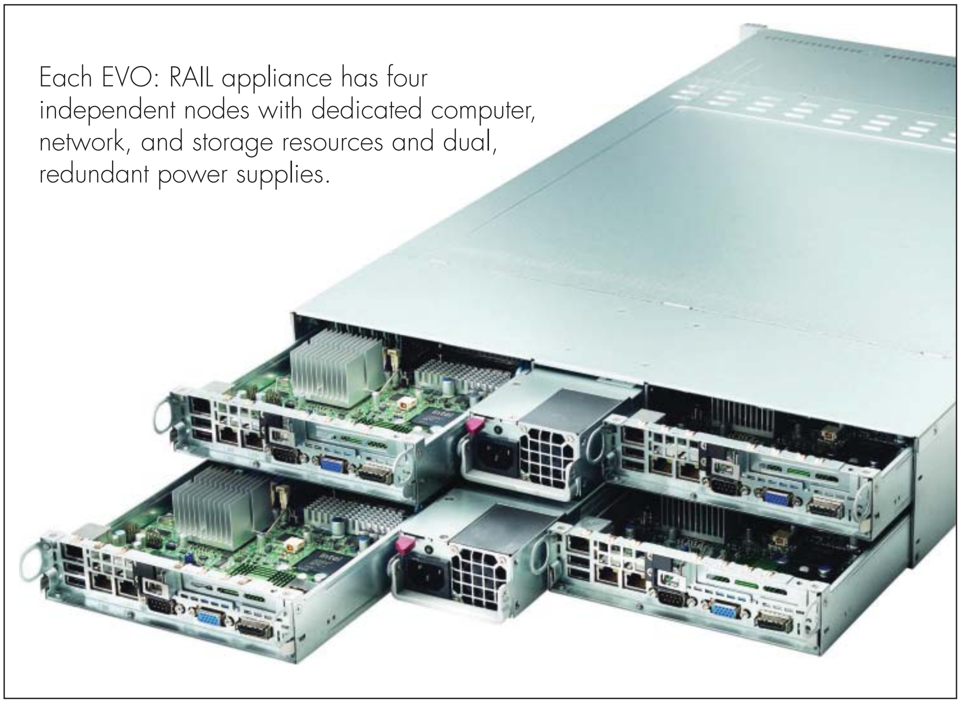
continued from page 1

ing business needs has resulted in IT infrastructures so large and complex as to be nearly unmanageable.

"This is why we're seeing a rapid shift to a more software-centric approach. Data center architects are finding new ways to use software to control the physical network and improve agility through increased levels of programmability and automation."

Focus on Software

This is the aim of the software-defined data center (SDDC), an architectural approach in which all necessary computing, storage and security resources are pooled and abstracted through software, and hosted on virtual machines running on scale-out commodity hardware. That makes it far easier to add or reconfigure devices, dramatically simplifies management, reduces operational costs and increases the speed of service delivery.



Each EVO: RAIL appliance has four independent nodes with dedicated computer, network, and storage resources and dual, redundant power supplies.

VMware, among the early proponents of SDDC, has made it easier for organizations to adopt such a strategy with the release last year of EVO: RAIL, an infrastructure appliance featuring a pretested, pre-integrated VMware software stack optimized for commodity hardware from several key partners.

EVO: RAIL software includes VMware vSphere, VMware Virtual SAN, VMware vCenter Log Insight, and the new EVO: RAIL engine — all integrated with hardware from select partners including HP, Dell, EMC, Fujitsu and more. EVO: RAIL simplifies appliance deployment and configuration, as well as on-going management, patching and upgrading of the software. The appliance features a new intuitive user interface that will streamline previously manual processes of creating and managing virtual machines, along with the associated networks and data stores.

EVO: RAIL is among the first products designed around the concept of "hyper convergence," an approach that has evolved from the converged infrastructures developed in recent years as simple, flexible and fast solutions for data center bloat.

Converged infrastructures consist of pre-racked and cabled computing, storage and networking hardware components integrated into a unified system based upon a validated reference architecture. This approach shortens deployment time, improves management and delivers one-throat-to-choke support. However, there are drawbacks. The hardware-centric nature of these platforms create vendor lock-in, and rigid configuration rules severely limit provisioning and expansion.

Hyper convergence promises to resolve these limitations through a focus on software. In this approach, commodity x86 hardware components can function as a single, shared resource pool through hypervisor technology. Building on key virtualization concepts, hyper convergence allows distinct hardware components to be integrated while maintaining a high degree of scalability.

"Converged infrastructure solutions are essentially separate components engineered to work together. They definitely bring a new level of simplicity to the data center, but they have some limitations," said Merriman. "Most converged infrastructure products give you a standard form factor with a standard maximum number of disks, CPUs and RAM, and there is no way to deviate from that.

"This is where hyper-converged systems like EVO: RAIL really shine. These are modular designs that can scale out quickly by adding additional modules. That flexibility is important because it provides a building-block approach for those who are moving toward a software-defined data center and a more agile and efficient IT infrastructure."

Scalability Benefits

EVO stands for "evolution," while RAIL refers to a design in which the appliance slides into a 2U rack server space on a rail. Each appliance features four independent server nodes, which combine to deliver at least 100GHz of CPU resources, 768GB of memory resources and 14.4TB of storage capacity — as well as 1.6TB of flash capacity for storage acceleration services.

EVO: RAIL appliances can be deployed in clusters of up to four appliances for a total of 16 nodes as IT infrastructure needs grow. New appliances added to an existing VMware EVO: RAIL cluster will be automatically discovered, requiring only a few mouse clicks to get started.

Appliance deployment and configuration are simple. VMware claims it only takes 15 minutes to get a preconfigured EVO: RAIL appliance up and running, and about the same time to add appliances to an existing cluster.

A single appliance will support approximately 100 general-purpose virtual machines or 250 virtual desktops and will feature a VMware Virtual SAN data store with a capacity of 13TB. EVO: RAIL scales linearly to offer customers predictability in design, performance and cost.

Users also have the ability to manage, patch and upgrade software from one location. The increased efficiency of creating and managing virtual machines, networks and data stores will reduce operational costs as there will be no downtime when performing patches and updates.

EVO: RAIL is aimed at use cases in the midmarket and enterprise segments. With VMware Virtual SAN as key enabling software, VMware says EVO: RAIL is ideally suited for use cases such as virtual desktop infrastructure (VDI) as well as remote office/branch office for industries such as financial services, government, healthcare, higher education, insurance, oil and gas, and retail. Based upon VMware vSphere, the appliance can coexist with customers' existing VMware vSphere environments as well as serve as an on-ramp to VMware vCloud Air.

"Customers expect IT solutions to deliver immediate value — not in days, weeks or months," said Raghu Raghuram, executive vice president, VMware. "VMware EVO: RAIL is a new building block for software-defined data center environments, taking the guesswork out of building, deploying, scaling and managing software-defined infrastructure services. With the help of our partners, we are bringing the simplicity of consumer appliances to the world of enterprise infrastructure."

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@prosysis.com

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

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

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

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

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

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

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

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

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

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

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

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

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

Tampa, FL
Phone: 813-440-2410
800-891-8123
lspivack@prosysis.com

Beware of the Three Faces of Ransomware

CryptoWall, CryptoLocker and CoinVault promise to destroy data if ransom demands are not met.

"Ransomware" has been making news lately due to the rise of CryptoWall – a nasty combination of malware and extortion that encrypts files and demands money in exchange for the key. If the ransom isn't paid by a certain deadline, data will be lost forever. The only way to regain access to the files is to pay the ransom or restore from a recent backup that was not actively connected to the infected machine.

CryptoWall ransomware infected millions of users in September and October of this year. Hackers infiltrated the advertising networks that delivered ads to a number of reputable, high-profile websites such as AOL, Yahoo and Match.com as part of a sophisticated "malvertising" campaign. Users didn't even have to click the ads to be infected. CryptoWall was automatically downloaded to user computers when pages with malicious ads loaded. Although the ad networks compromised in these attacks claim to have addressed the problem, an even more serious threat lurks on the horizon.

Primarily delivered via email attachments, CryptoWall 2.0 has been enhanced to fortify "deficiencies" that allowed security professionals to stop the earlier version in recent months.

Simply put, enhancements to CryptoWall 2.0 make it more difficult for users to recover data and easier for hackers to compromise computers and receive ransom payments.

CryptoWall 2.0 copies and encrypts data and securely deletes the original data files, forcing users to recover data from backups or pay the ransom. CryptoWall 2.0 also assigns user-specific bitcoin payment addresses for each victim, which prevents victims from stealing another victim's payment and using it to pay their own ransom. Gateway servers through the Tor anonymization network are now being used for ransom payments in order to stay hidden from authorities and control access to their servers.

CryptoLocker Locks Down Data

Although CryptoWall made headlines as part of a widespread malvertising campaign, most ransomeware such as CryptoLocker is spread via phishing emails designed to look as if they come from legitimate businesses, or through phony UPS and FedEx tracking notices. CryptoLocker has also shown up on computers attacked by a separate botnet infection.

Typically, the emails have a malicious attachment in the form of a .zip file that contains an executable program disguised as a PDF. When the victim clicks on the file, it installs itself in the Documents and Settings folder. After contacting one of the hackers' command-and-control servers to generate an encryption key, it encrypts all documents, graphics and other files on the victim's internal and external hard drives, removable media, and any shared network drives.

Once the files are encrypted, CryptoLocker displays a message demanding payment of $300 within 72 hours in order to obtain the private key needed to decrypt the files. Recently, the developers launched a new "service" in which victims can get their files decrypted after the deadline has passed. Reportedly, the cost is more than $2,000. So far, CryptoLocker has eluded antivirus software, Microsoft security updates and firewalls. That's because it continually morphs into new variants that are difficult to detect. Even if antivirus software is able to detect it, it will already have begun encrypting files.

Law enforcement officials from the U.S. and other countries have managed to seize servers used for the CryptoLocker ransomware, although recent activity has been reported. According to the U.S. Department of Justice, Cryptolocker had infected nearly a quarter-million computers by April 2014, mostly in the U.S., with victims estimated to have paid more than $27 million in ransom in the first two months after the malware emerged.

CoinVault Adds Mind Games to the Equation

Cybercriminals have introduced a psychological component into a new form of ransomware called CoinVault. Like CryptoWall and CryptoLocker, CoinVault is a program that encrypts data and stores the key on a remote server. It also eliminates the Windows Volume Shadow Copy Service, making it impossible for users to restore the most recent autosaved version of the file.

CoinVault is different in that it shows the victim a list of encrypted files and allows the user to choose one file to have decrypted for free. Some security experts believe this functionality is offered to prove that files can actually be decrypted. CoinVault even shows a clock that counts down to the payment deadline. If the clock reaches zero and a bitcoin payment hasn't been made, the cost for the key increases.

Although many hackers using these three ransomware programs have provided the key needed to decrypt files after the ransom is paid, some victims have reported that they did not receive the decryption key. Because there is no guarantee that criminals will live up to their end of the deal, US-CERT is urging victims not to give in to extortion but rather to report the incident to the FBI's Internet Crime Complaint Center.

Limiting the Damage from Ransomware

Victims of a ransomware attack should immediately disconnect their computers from wired or wireless networks in order to stop the infection from spreading. More importantly, organizations should take these steps to prevent an attack:

- Inform users about the seriousness of this threat and remind them to never click links or download files from any unknown or suspicious sources.
- Ensure that antivirus software is current and all systems and applications have the last security patches.
- Configure the network firewall to prevent executable programs from being downloaded.
- Utilize email and web filtering defenses.
- Configure PCs and servers to control the damage from this threat — for example, use role-based folder permissions to stop an infected PC from encrypting other users' files.
- Implement a reliable backup system for all data stored within the organization, and ensure that files can be recovered quickly if needed.

App Containers

Lightweight application packages create new levels of portability.

The development of containerized shipping in the 1950s revolutionized the freight transport industry by improving efficiency, curtailing waste and cutting costs. These standardized metal boxes made it possible to move tons of cargo from ship to rail to truck in a matter of hours. Before that, it might take a team of 20 men working two shifts a day a week or more to load or unload that much cargo piece by piece.

There are parallels with today's heterogeneous computing environment. Deploying applications across a wide variety of hardware environments has proven to be a time- and labor-intensive process for IT staff. Depending on where the app is running — whether on bare-metal or virtualized servers in public, private or hybrid clouds — it can have wildly different operating system, security, storage and network requirements.

As with the freight industry example, containerization is emerging as an effective solution. By packaging an app and all the resources it needs to run in a lightweight and portable bundle, application containerization allows IT to easily move applications among a variety of machines and systems without modifying any code.

Alternative to VMs

Industry analysts say a key benefits of containerization is the ability to package applications in a more uniform way. Like shipping containers, app containers can have a wide variety of contents but the external packaging remains the same. As such, the apps and resources within the container can be written in any language or built on any particular framework.

"Container-based development is becoming essential for DevOps teams because it enables application development to move more quickly and efficiently," said Al Hilwa, program director, application development software, IDC. He added that workflow containerization solutions "will ultimately lead to better software quality."

A company called Docker has led the surge in app container technology, building off a decade-old open source technology called Linux containers. Using resource isolation features of the Linux kernel, Docker allows containerized apps to access the CPU, memory, block I/O and network resources of the host operating system. These resource-sharing features make containerization an attractive alternative to the use of virtual machines (VMs) to package apps

VMs are created by hypervisors that virtualize at the hardware level, which means the VM must also include a full OS installation along with virtualized device drivers, memory management, etc. Because containers virtualize at the OS level and share the resources of the host, they are more lightweight, flexible and quicker to install than VMs. Additionally, this resource isolation helps ensure that apps don't get slowed down by other apps running on the same host server.

Fostering Agile Development

The containerization approach drives developer productivity and agility by allowing application code changes to move from development to production in minutes, enabling real-time change. However, developers, enterprises, service providers and ISVs are also exploring containerization for application delivery because it cleanly separates applications from infrastructure, resulting in faster application lifecycles and the "write once, run anywhere" ability to move applications between endpoint devices, data centers and clouds.

With the growing popularity of both Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS), app containers also help prevent cloud lock-in. By separating infrastructure services from the application, containerized applications can move freely between not only different clouds, but also physical and virtual environments, consuming only the needed services and delivering upon the extreme flexibility promised by the open hybrid cloud.

Some of the biggest players in technology have embraced the container philosophy. Red Hat was an early booster, and Microsoft has signed on to deliver Docker solutions that can be used with either Linux or Windows Server. Google, IBM and Amazon Web Services have announced deals to deliver container services in their cloud platforms. Even VMware has partnered with Docker to integrate containers into its virtualization software lineup.

"Just as virtual machines replaced individual servers, we believe there will be another 10-to-1 consolidation in the data center thanks to containers," said Bryan Cantrill, CTO of Joyent, a cloud infrastructure company closely aligned with Docker.

Infrastructure at the Speed of Innovation

Meet accelerating business demands by simplifying infrastructure design with VMware EVO:RAIL, which combines VMware compute, networking, and storage resources into a hyper-converged infrastructure appliance.

EVO:RAIL is complete and ready to be configured with your networking details for rapid deployment. Easy to size and scale, each appliance supports approximately 100 general purpose virtual machines or up to 250 Horizon View virtual desktops, allowing IT to leverage a pay-as-you-grow model.

Simple deployment, configuration and management with the intuitive user interface, reducing OpEx so IT can focus on strategic initiatives, applications and business growth.

CONTACT YOUR PROSYS REPRESENTATIVE TO LEARN MORE

PROSYS

www.prosysis.com 888-337-2626