Powering Business Worldwide

Thought Leadership White Paper

Powering Converged Infrastructures

By *Mike Jackson*
Product Manager
Eaton

Executive summary

Converged infrastructures utilize virtualization and automation to achieve high levels of availability in a cost-effective manner. In fact, converged infrastructures are so resilient that some IT managers believe they can be safely and reliably operated without the assistance of uninterruptible power systems (UPSs), power distribution units (PDUs) and other power protection technologies. In truth, however, such beliefs are dangerously mistaken.

This white paper explores the factors that make converged infrastructures inherently resilient, explains why robust power protection is an essential element of successful converged infrastructure deployments and describes the critical hardware and software components companies must include when designing a converged infrastructure's power protection scheme.

Table of contents

What is converged infrastructure?

Simply put, converged infrastructures are pre-integrated hardware and software bundles designed to reduce the cost and complexity of deploying and maintaining virtualized solutions. Most converged infrastructure products include these four elements:

1. Server hardware
2. Storage hardware
3. Networking hardware
4. Software (including a hypervisor, operating system, automated management tools and sometimes email systems, collaboration tools or other applications)

At present, most converged infrastructure solutions fall into one of three broad categories:

- **OEM solutions.** These are offerings in which all of the hardware and most or all of the software comes from a single vendor, such as IBM, Dell or Hewlett-Packard.
- **VCE solutions.** An independent business formed by Cisco and EMC, with investments from VMware and Intel, VCE Company LLC markets a line of converged infrastructure solutions built with hardware and software from its founding vendors.
- **Reference architecture solutions.** These converged infrastructures are based on validated design templates from one or more technology vendors. Solutions based on the VSPEX architecture, for example, combine EMC storage systems with Cisco or Brocade networking equipment and virtualization software from Citrix, Microsoft or VMware. Those same software makers also support solutions based on the FlexPod architecture, which features servers, networking and storage products from Cisco and NetApp.

Why use converged infrastructure?

According to analyst firm IDC, the worldwide market for converged infrastructure solutions will expand at a compound annual growth rate of 40 percent between 2012 and 2016, rising from $4.6 billion to $17.8 billion. Sales of non-converged server, storage and networking hardware, by contrast, will increase at a CAGR of just a little over two percent over the same period. Benefits like the following help explain why adoption of converged infrastructures is rising so sharply:

Faster, simpler deployment. Converged infrastructures are pre-integrated and tested, so they take far less time to install and configure. According to a study from analyst firm IDC, in fact, Hewlett-Packard converged infrastructures typically enable businesses to cut application provisioning time by 75 percent.

Lower costs. Converged infrastructure products usually sell for less than the combined cost of their individual components, enabling businesses to conserve capital when rolling out new solutions. Furthermore, the automated management software included with most converged infrastructure offerings decreases operating expenses by simplifying system administration. Indeed, the HP converged infrastructure users studied by IDC shifted over 50 percent of their IT resources from maintenance to innovation on average.

Enhanced agility. Thanks to their ease of deployment, affordability and scalability, converged infrastructures enable companies to add new IT capabilities or augment existing ones more quickly and cost-effectively.

Resilience in converged infrastructures

In addition to the advantages just described, converged infrastructures also give companies a potent new way to increase the resilience of their IT environment.

Traditionally, strategies for maintaining high availability have focused on an IT infrastructure's hardware layer, emphasizing the use of durable, redundant servers, networking, storage and power protection

systems. Such approaches have a long record of success and remain strong options for organizations that need uninterrupted availability 365 days a year.

However, hardware-centric resilience schemes have several drawbacks. For one, they're often difficult to modify, making them a poor fit for today's dynamic and highly virtualized infrastructures. For another, they can be expensive, as they require companies to purchase and maintain more IT equipment than they need purely for purposes of redundancy. As a result, many businesses now utilize resilience strategies emphasizing other layers of the technology stack, such as:

- **The user layer:** User-centric approaches to resilience identify user populations that can tolerate small amounts of data loss or brief service disruptions, and then deliver only as many "nines" of availability as those populations require.
- **The application layer:** Large organizations, including major cloud service providers such as Google, often increase resilience by building maximum fault tolerance into their application code. However, such schemes rely on massively distributed—and therefore costly—architectures, as well as significant investments in programming time.
- **The cloud/virtualization layer:** Rather than prevent equipment failures and power loss, resilience strategies focused on the cloud and virtualization layer mitigate the effects of such problems by either automatically restarting virtual machines or swiftly migrating them to unaffected hosts elsewhere on the network or in the cloud. As a result, they enable companies to maintain continuous or near-continuous uptime without enduring the expensive burden of deploying redundant hardware or writing fault-tolerant code.

  Not surprisingly, building resilience into the cloud/virtualization layer is quickly becoming the most popular approach to preserving availability. And since converged infrastructures are heavily virtualized and automated solutions ideally suited to cloud/virtualization resilience strategies, they too are rapidly gaining favor among enterprise IT managers.

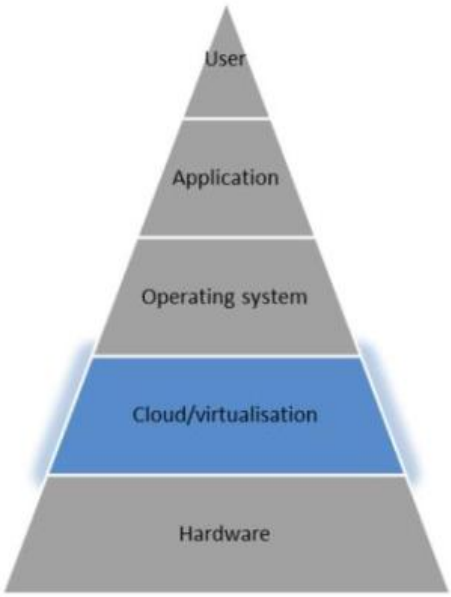

Figure 1. *Resilience strategies that target the cloud/virtualization layer deliver continuous or near-continuous uptime without forcing companies to deploy expensive redundant hardware or write fault-tolerant code.*

A dangerous delusion about power protection for converged infrastructures

Converged infrastructures are so inherently resilient that many IT managers believe they can be safely and reliably operated without the help of power protection systems. In reality, however, nothing could be further

from the truth. For all their automated, virtualized failover capabilities, converged infrastructures need robust power protection every bit as much as more traditional environments, for these reasons:

Power protection equipment plays a key role in automatically triggering virtual machine migration processes during utility outages. Converged infrastructures execute automated failover routines only when informed that there's a reason to do so. During utility failures, network connected UPSs can provide that information by notifying downstream devices that power is no longer available. At companies without UPSs, technicians must initiate the virtual machine transfer processes manually, which is far slower and less reliable.

A converged infrastructure's failover features can't function without electrical power. Even the most sophisticated converged infrastructure solutions can't transfer virtual machines instantaneously. Completing the migration process takes time, and therefore power. Unless UPSs are present, however, power becomes almost immediately unavailable during utility failures, rendering a converged infrastructure's failover capabilities useless. For example, without power there can be no networking, and without a functioning network converged infrastructures can't replicate virtual machines to a disaster recovery/backup site or to their hybrid cloud-based environment.

Converged infrastructures are vulnerable to power spikes and other electrical disturbances. Like all IT equipment, the hardware in converged infrastructures can be seriously damaged by transients, fluctuations and other power impurities. In addition, the power supplies and power factor correction solutions used by many converged infrastructure offerings require clean power for optimal performance. UPSs and PDUs have power conditioning features that shield servers, storage and networking equipment from potentially harmful electrical conditions while delivering clean, dependable power.

The fifth element of converged infrastructures: Intelligent power protection

The observations above make clear that power protection technology is so essential to the safe operation of converged architectures that IT managers should regard it as the fifth element of a complete converged infrastructure solution. More specifically, organizations should supplement a converged infrastructure's built-in hardware and software with the following additional power protection components.

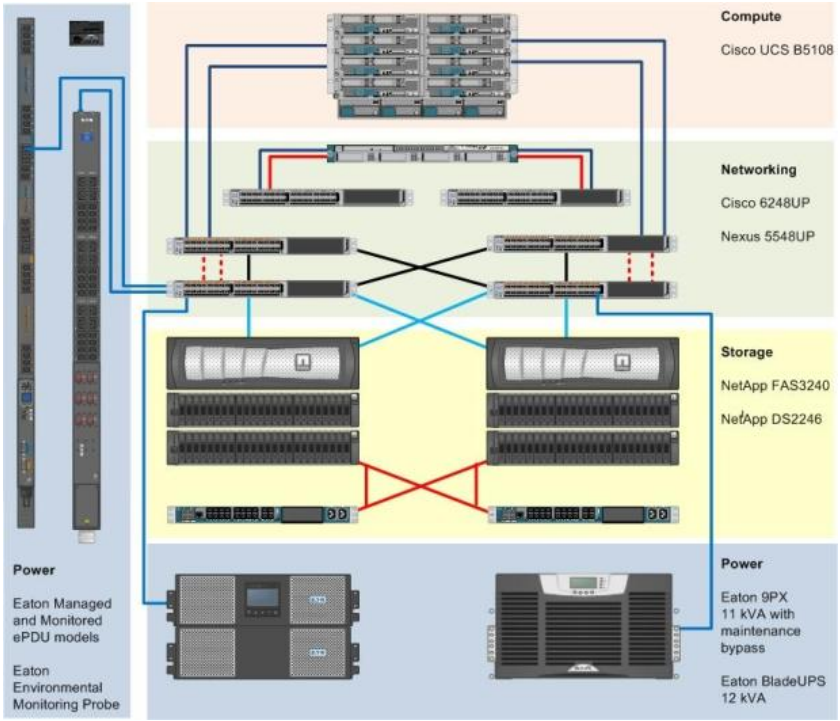

Figure 2. *Sample converged infrastructure based on the FlexPod reference architecture.*

PDUs

Power distribution units suitable for use with converged infrastructures do more than simply distribute power. They also enable technicians to:

- **Remotely switch power outlets on and off.** Advanced PDUs come with switching functionality that administrators can use to turn individual power outlets on or off remotely. Utilizing that feature, managers can execute a “hard reboot” of a malfunctioning converged infrastructure component without the costly and time-consuming inconvenience of visiting it on foot, an especially big advantage for technicians who remotely manage facilities located many miles away.
- **Monitor power outlets individually.** Sophisticated PDUs collect power consumption data on an outlet-by-outlet basis. Drawing on that information, administrators can analyze usage trends and reduce downtime by performing predictive maintenance. For example, a sharp increase in power utilization by a specific outlet is often evidence of an impending power supply failure. Monitoring power usage data can help technicians perform repairs before downtime occurs.
- **Manage and control downstream devices.** In addition to distributing power downstream, the most sophisticated PDUs also feed information about power status, power quality and other issues upstream to network management systems, giving administrators real-time visibility into issues that can critically affect the performance and availability of converged infrastructures.

Management software

Most converged infrastructure solutions come with built-in system management software that helps make them highly resilient. Adding VM-centric power management software increases resilience even further by enabling technicians to do the following:

Manage all of their converged IT and power protection assets through a single console. Advanced power management systems integrate seamlessly with major virtualization management products, including VMware vCenter Server and Citrix XenCenter. As a result, they increase IT managers’ productivity and effectiveness by enabling them to view, monitor and control power protection equipment through the same familiar console they use to administer a converged infrastructure’s other components.

Respond to power anomalies automatically. Using power management software that integrates with other management platforms also enables companies to:

- Preserve uptime by automatically initiating automated disaster recovery processes during power outages.
- Extend standby power during utility failures by using load shedding functionality to shut down low-priority virtual machines quickly and gracefully.
- Increase power system availability, by automatically notifying technicians via text message, email or other communication tools when temperature spikes, vibrations or other issues indicate that power protection equipment may require immediate maintenance.

Manage power protection systems remotely. The latest VM-centric power management solutions allow administrators to monitor and manage their UPSs and PDUs remotely from any device with a browser and Internet connection.

UPSs

UPS equipment performs three vital functions in a converged infrastructure power protection strategy:

- Notify converged infrastructures of utility failures, causing their automated management systems to initiate business continuity measures.
- Give converged infrastructures the emergency power they need to complete virtual machines migrations before gracefully shutting down servers and storage systems.
- Safeguard converged hardware from potentially hazardous power impurities.

Options for resilience

Using advanced power protection technologies gives businesses greater flexibility in how they ensure the resilience of converged infrastructures. Specifically, companies that deploy state-of-the-art UPSs, PDUs and power management systems in conjunction with converged infrastructures have these three options for protecting data and preserving uptime automatically during utility failures:

1. **Transfer all virtual machines to an infrastructure or site where power remains available.**

   Once that process is complete, the converged infrastructure's power management system can perform a graceful shutdown of the hypervisor and a controlled power down of the physical servers and storage systems. With this option, full IT service remains available throughout the utility failure, though users are likely to experience somewhat slower performance than usual during the virtual machine migration process.

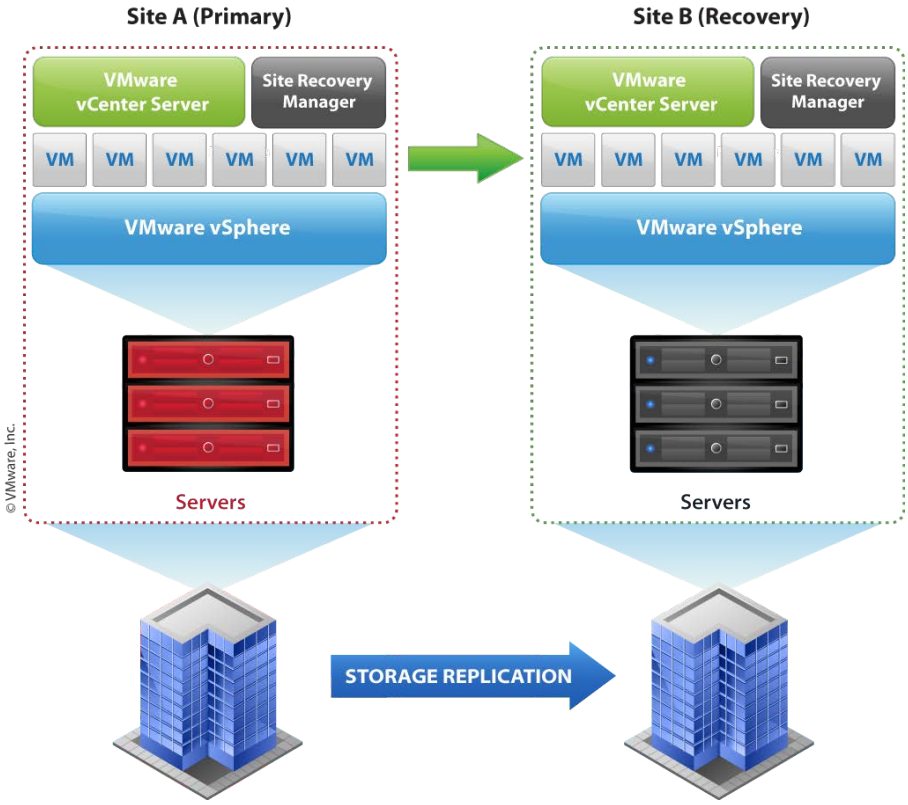

Figure 3. *During utility outages, converged infrastructures equipped with power protection technologies can automatically transfer mission-critical virtual machines to an infrastructure or site where power remains available and gracefully shut down all remaining virtual machines.*

2. **Transfer mission-critical virtual machines to an infrastructure or site with functioning power, gracefully shut down the remaining virtual machines and then power down the physical host servers.**

   In this scenario, depicted in Figure 3 below, services provided by non-critical virtual machines will be unavailable until utility power is restored. For some companies, however, that's an acceptable price to pay in exchange for a shorter and simpler migration process that also costs less because it doesn't require as much disaster recovery capacity. For example, manufacturers must typically halt production lines during power outages anyway, so shedding production-related workloads poses no additional threat to profitability.

3. **Maximize standby power by gradually shutting down virtual machines rather than migrating them offsite.**

   This option utilizes the power management system's load shedding functionality to shut down virtual machines sequentially, starting with the least mission-critical ones and ending with the most. Throughout that process, the virtualization management system automatically consolidates remaining workloads onto fewer and fewer physical devices, allowing companies to extend their backup power by progressively shutting down unused host machines. In addition to shedding the lower priority loads, the IT manager may also invoke [server] power capping to further extend battery run time. If utility power is still unavailable when standby power reaches critically low levels, the power management and virtualization management systems can execute a controlled shut down of the few remaining virtual and physical servers. This option leaves organizations vulnerable to service disruptions but also spares them the expense of maintaining offsite disaster recovery resources.

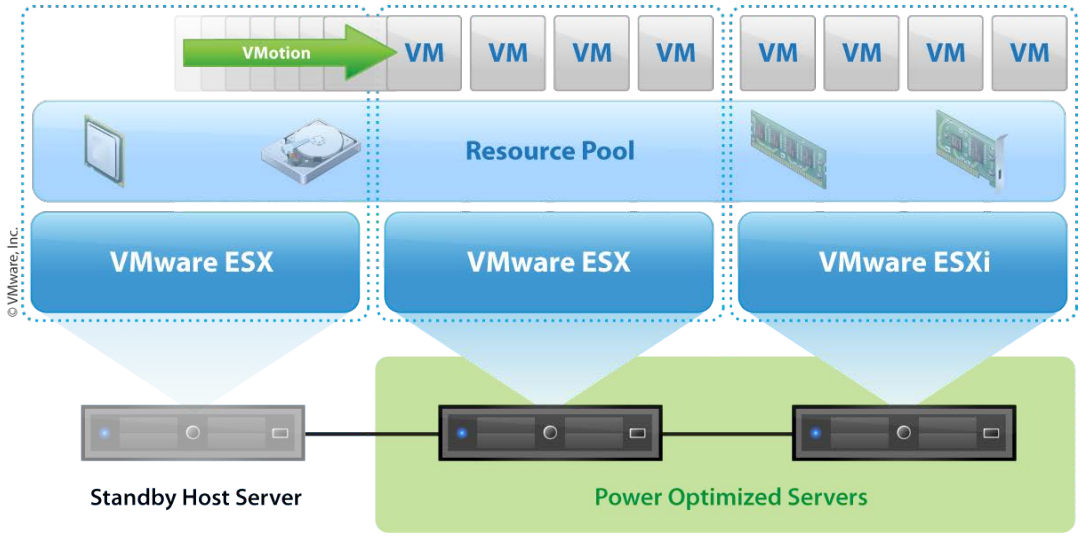

***Figure 4**. Virtual Machine consolidation for maximized backup time.*

Note that all three of these options hinge on tight integration between the converged infrastructure and a comprehensive power protection solution that includes networked UPSs and PDUs as well as sophisticated power management software.

Conclusion

Leveraging virtualization and automated management systems, converged infrastructures make IT environments dramatically more resilient—*if* they're backed by advanced UPSs, PDUs and power management software. Companies that don't use power protection technologies in conjunction with their converged infrastructures expose themselves to increased risk of data loss and unnecessary downtime. When planning converged infrastructure implementations, therefore, IT managers should treat power protection as the all-important fifth element of a complete solution, alongside servers, storage, networking and software.

About Eaton

Eaton is a diversified power management company providing energy-efficient solutions that help our customers effectively manage electrical, hydraulic and mechanical power. With 2012 sales of $16.3 billion, Eaton is a global technology leader in electrical products, systems and services for power quality, distribution and control, power transmission, lighting and wiring products; hydraulics components, systems and services for industrial and mobile equipment; aerospace fuel, hydraulics and pneumatic systems for commercial and military use; and truck and automotive drivetrain and powertrain systems for performance,

fuel economy and safety. Eaton acquired Cooper Industries plc in 2012. Eaton has approximately 103,000 employees and sells products to customers in more than 175 countries. For more information, visit www.eaton.com.

About the author

Mike Jackson is Product Manager for Single Phase UPS systems in Eaton's Distributed Power Quality Division in Raleigh, North Carolina. He has been in the power quality industry since 2007, with experience in power distribution and power quality solutions for datacenter, commercial and IT applications. Besides product management, Mike has held various roles in operations and sales for Eaton. He can be reached at MikeJackson@eaton.com.