SPONSORED CONTENT
Redmond MAGAZINE

Highlights from a recent webcast on Managing Virtual and Cloud Environments

NEED FOR SPEED: DATA RECOVERY IN A NON-STOP WORLD

Jon Toigo, managing principal, Toigo Partners International, and Kris Patton, Inside Sales Engineer, Quest Software, discuss the IT management dilemma faced by organizations implementing virtualization and cloud technologies.

IT management including security, backup and recovery will all be easier, better, faster once you adopt virtualization and cloud technologies.

Or maybe not, says Jon Toigo, managing principal, Toigo Partners International.

"I'm a skeptic because I talk to a lot of companies where the virtualization project has been less than ideal," he told the audience for a recent webcast.

Toigo allows that virtualization and cloud have an upside including:

Virtualization

- Less expensive infrastructure
- Leaner staffing requirements
- Easier provisioning to workloads
- Workload balancing

Cloud

- Access anywhere
- Lower OPEX/CAPEX
- Insulation from tech change

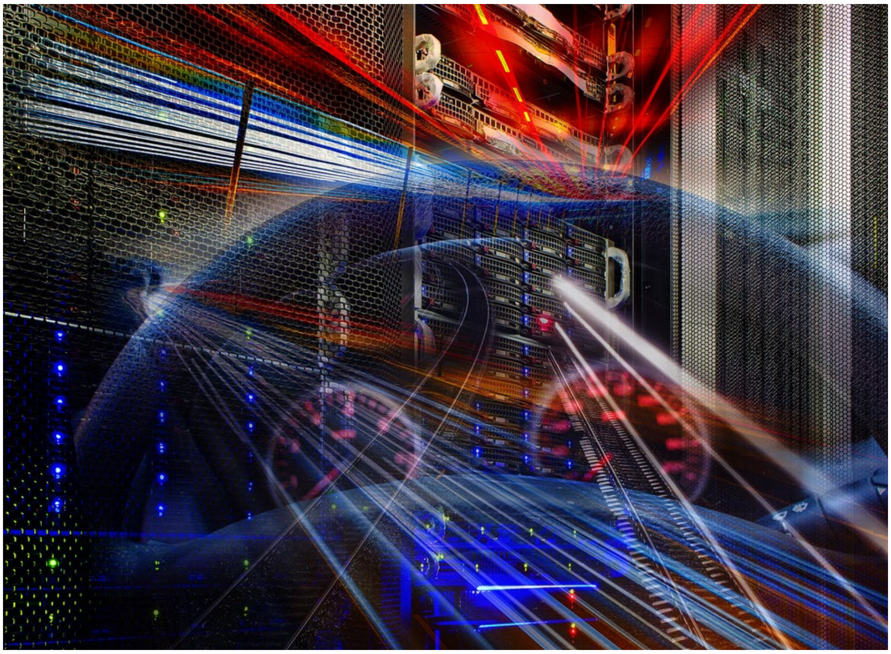
However, there is a downside:

Virtualization

- Lack of standards, interoperability between hypervisor stacks and kits
- Lagging orchestration/administration tools
- Silo'ing and virtual sprawl

Cloud

- Bandwidth and access issues
- "Resiliency" (predictability of service)
- Cost and outage frequency



The Heterogeneous Problem

As has been true of the software and hardware world for decades, most organizations embrace heterogeneity when implementing virtualization and cloud technology, Toigo said. Far from simplifying IT management heterogeneity adds complexity. The analogy he uses is herding cats. In the old days when hardware and software were only on premises, maybe you had hardware from a couple different vendors and software from several vendors. At that point, you only had a few cats to herd. Now you still have some hardware and software in house but you also have virtual technology from VMware, Microsoft and others. You are utilizing Amazon Web Services, Microsoft Azure and other cloud vendors. Now, you've got a lot of cats to round up and herding is not so simple.

Another dilemma faced by IT departments with heterogeneous environments is what Toigo calls silo'ing by the vendors. Seeking to lock in customers, vendors do not make it easy for their virtual technology to play nice with ones from a rival vendor. IT finds itself faced with the problem of managing a mixture of legacy, virtual server/SDS and hyper-converged infrastructure (HCI) appliances.

Timofeev Vladimir/Shutterstock.com

"That's the bane of existence for disaster recovery," Toigo told his audience. "It's a pain to manage, administer and test."

> "It helps if you have a third-party backup solution that allows you to apply different strategies to data protection to different data targets." —Jon Toigo

Avoid the Crisis that Turns Into a Disaster

The mixture of real metal machines and virtual machines with apps and data located both on-premises and off in the cloud makes for a problematic recovery scenario.

Toigo uses the term "time to data" when calculating whether the crisis of a system's interruption due to a natural or human caused event becomes a disaster that may damage or destroy a business.

"The difference between a crisis and a disaster is measured in time to data," he told the webcast audience. "If you can measure it with a stopwatch, it's a crisis that is quickly resolved. If it is measured with a sundial, it is a disaster and you may go out of business."

With stories of phishing and ransomware showing up on the nightly news, security threats now account for substantial downtime, Toigo noted. In this threat environment, it's no longer valid to separate security from continuity planning. But doing that job is harder now because what he calls "cloudification and virtualization" increase the "attack surface" IT is being tasked to protect.

While security vendors search for technology fixes that will fend off ransomware and other malware, Toigo told the IT pros listening to the webcast: "Despite our best efforts, security breaches will occur."

How are you going to recover quickly enough to make sure the immediate crisis does not become a disaster? A recovery plan needs to make sure you have an uncorrupted copy of your data, and a backup to tape or to the cloud. Toigo recommends a continuous data protection plan that will facilitate point-in-time restore, so you can quickly get your systems back up and running with data and applications as they were before the virus or corruption or disruption event happened.

"Achieving the goal of continuous data protection can be very expensive and requires upfront analysis of business processes and data to determine which apps and data are mission critical and require such rigorous protection," Toigo said.

Sometimes lost in the discussion of recovering data is the need to also restore the application that was used to create and interact with that data. Toigo pointed out that Quest Software recognized years ago that to restore email so it could be worked on by end users, it was important to restore Outlook and the settings those users needed to access their business communications.

Ultimately the ability to identify, continuously protect and speedily restore mission critical data and applications can make the difference between a short-time crisis and a long-term and perhaps terminal disaster.

"It helps if you have a third-party backup solution that allows you to apply different strategies to data protection to different data targets based on the criticality of the data," Toigo said.

Quest Solution for Data Protection

The Quest Data Protection solution makes it possible for organizations that have suffered a natural disaster or malware attack to resume operations quickly and smoothly, explained Kris Patton, Inside Sales Engineer at Quest Software. The goal is a "zero impact recovery" allowing a company to continue normal business operations as if the outage never happened. The Quest solution:

- Recovers the OS volume to the new target machine.
- Works across multiple hypervisors.
- Works across monitoring vendors, management vendors, and data protection vendors.
- Presents data volumes to the restored OS as accessible disk/files so that requesting apps and users can access the data immediately.
- Data requested by users is restored to the target machine first, so the outage is transparent to the app and users.

Patton said that this results in users back to work in less than 15 minutes with little-to-no data loss.