Sponsored by

The Essential Guide to Legacy-Free Disaster Recovery

Drop the baggage and simplify your Disaster Recovery strategy

---

Sean Clark

VCP 2, 3, 4 and VMware vExpert 2009

Executive summary

The benefits of VMware virtualization for servers are unmistakable. The last five years have seen a relentless march towards virtual being the deployment option of choice. At the VMworld 2010 keynote in San Francisco, VMware CEO Paul Maritz even quoted statistics from IDC that 2010 was the first year that servers shipped with a virtualization platform outnumbered common physical servers. This shift is due to the well-known benefits of server consolidation: lower server hardware costs, reduced datacenter power consumption, and increased efficiency of operations. But availability, disaster recovery (DR), and disaster avoidance benefits are also drivers for increased virtualization and key enablers for bringing Tier 1 business-critical workloads onto VMware platforms.

Legacy technologies are a drag on the efficiency of IT operations. The need for cautiously adopting new technology and "dipping a toe" before jumping in are well understood. But when it comes to DR planning for VMware environments, we've been a little too conservative in leaving legacy technologies and designs behind. It's like the first automobile engineers who continued the practice of placing whip holders on the frame of new automobiles (horseless carriages). It's now time to stop engineering new DR plans with their version of "whip holders." It's time to drop the legacy processes, technology, and thinking. We now have the opportunity to design a DR solution that saves money and improves recovery time and recovery point objectives (RTOs and RPOs), all while simplifying DR solutions by leveraging the latest in data protection technology.

This white paper overviews the evolution of DR strategies for x86 computing, how VMware enables new strategies but also introduces new challenges, and how adopting the latest VMware vSphere platforms along with Veeam vPower allows you to proceed confidently on the journey to a legacy-free DR solution.

Journey to DR enlightenment

The whole virtualization industry is very fond of describing a "virtualization journey" or "the journey to the cloud" computing nirvana. The journey is usually in reference to the maturity of a company's adoption of proven practices and the gradual evolution of best practices and capabilities. The journey can also mean that organizations are taking their already mature best practices and keeping pace with new evolving technologies.

There are many benefits to adopting virtualization, but availability and business continuity aren't usually the first destinations on the virtualization journey. Instead the journey starts with the issues that are dealt with every day: combating server sprawl, reducing costs associated with hardware refreshes, and greatly reducing datacenter physical costs. There is well-known ROI (return on investment) in this server consolidation phase of virtualization, but experienced virtualization technologists understand this is just the tip of the iceberg of benefits. There is a sleeping dragon of DR issues still waiting to wake up and take your business down when least expected, and virtualization provides a foundational platform to help you slay these dragons.

When it comes to DR preparedness, IT organizations are haunted by four main concerns: **Uptime, Reliability, Cost,** and **Complexity**.

4 main DR concerns

- **Uptime**—Corresponds closely to RTOs. DR solutions should offer quick restores with minimal or no manual steps after the recovery.
- **Reliability**—Corresponds closely to RPOs. Addressing database transactional consistence, avoiding corrupted file systems, and ensuring systems boot when restored are key to addressing this concern.
- **Cost**—The cost of many different software solutions or replicating storage arrays can prevent DR solutions from getting off the ground. DR solutions need to be affordable.
- **Complexity**—How many different systems are involved with the strategy? DR plans are also typically plagued by complex, thick run books that document all steps required to bring systems back online. Reducing this complexity is a chief concern.

These four concerns have not changed much since businesses created their first DR solutions, but the technology to address the concerns has grown by leaps and bounds. Virtualization with VMware enables a whole new realm of data protection technologies that frees organizations from the complexities, bottlenecks, and costs of legacy x86 data protection strategies. But are these new virtualization-aware data protection technologies enough to replace the tried and true technologies of the past? And how and when can you safely migrate to a new strategy? These questions mark the start of the journey to a legacy-free DR solution. To understand where we are going, it is wise that we first make a stop at where we started.

DR past

IT environments have always had to navigate a complicated matrix of applications and supported operating system configurations, regardless of VMware virtualization. Before VMware virtualization became mainstream, in order to properly protect the application and its data, you had to install a software backup agent and back up the application data and settings to external media. In order to recover this application should disaster happen, you'd have to acquire a relatively similar physical server to the failed one, install the operating system following a run book that instructed you on the exact settings needed, patch the OS to the appropriate level, and reinstall the application and the backup software. As the final step, you'd attach the external media to find the backed up data and restore the data to the newly loaded server. Chances are that during this process you'd do something that was not the same as the original production server, so the application would not function properly the first time and troubleshooting would need to take place to make sure the application was ready for worthwhile use again. It was also not uncommon to discover that backups or replicated sets of data were missing, corrupted, or suffering from another malady that prevented successful restoration. Unless test recoveries were performed daily, these holes could be difficult to discover, but the cost and time needed to perform daily tests were too high.

Although traditional agent backup software solutions are tried and "true-enough" methodologies dating back to mainframes, UNIX systems, and the first x86 servers, there are also some distinct limitations with the status quo. The recovery is complex, there are many steps, and you likely won't have the staffing, equipment, or time available to complete all these recovery steps in time to meet the RTO for every server. For these reasons, RTOs of 48 hours for your critical servers and 5 days or more for the less critical servers are all too common. Even so, it's still commonplace to see companies fail to meet RTOs in DR exercises. Even with the horrendous track record of classic data protection approaches, they are still used today as part of the majority of recovery strategies because there has been no better alternative to deliver the same features for virtualized environments. But with the advent of new virtualized infrastructures, radically new and simpler server recovery methods are enabled, and the journey to legacy-free solutions can start to leave the dark ages of data protection.

Background

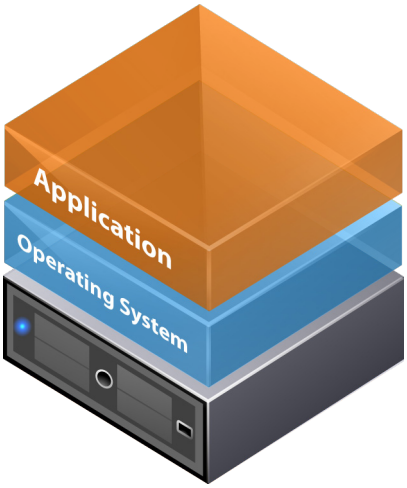
To fully appreciate the reasons for going legacy-free for your virtualized DR solution, it's helpful to step back and make sure we understand what is inherently different about virtualized platforms and protecting them. The following is a quick virtualization primer to level set newcomers to VMware virtualization and provide review for those new to virtualization-enabled data protection.

Virtualization primer

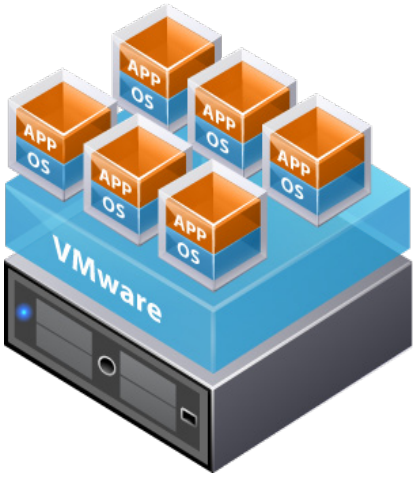
According to VMware, "a virtual machine is a tightly isolated software container that can run its own operating systems and applications as if it were a physical computer." In essence VMware delivers hardware with software virtualizations of CPU, RAM, hard disk, and network interfaces to an operating system that can't tell the difference between that and their physical counterparts. Applications running on these virtualized operating systems are also blissfully unaware of what is happening under the covers; from their perspective, as long as the OS is happy, they're happy, too.

Virtual machines (VMs) are composed entirely of software and contain no hardware components. As a result, VMs offer a number of distinct advantages over physical hardware. These include:

- **Compatibility**: VMs are compatible with all standard x86 computers
- **Isolation**: VMs are isolated from each other as if physically separated
- **Encapsulation**: VMs encapsulate a complete computing environment
- **Hardware independence**: VMs run independently of the underlying hardware



Traditional



Virtual

Three of these benefits really come into play with DR. It starts with encapsulation. Server virtualization enables standard operating systems, applications, and data to be encapsulated inside a VM, which is simply a set of discrete files that can be copied or moved anywhere. It is this hardware independence and compatibility with most standard x86 systems that allow VMs to be moved and run from anywhere. This is what is referred to as VM mobility. Today, most VMware customers leverage this mobility within their own datacenter walls. These customers use VMware Distributed Resource Scheduler (DRS) to automatically vMotion (live migrate) VMs between physical servers in order to balance the resource utilization evenly between servers and also to avoid planned server downtime due to hardware maintenance. VM mobility is also great for increasing availability of VMs. This is

exactly the case with VMware High Availability (HA), which can restart VMs from a failed physical server on remaining servers within a vSphere cluster of physical servers. All together, these technologies can help companies avoid unnecessary work in activating their DR plans if there is advanced warning.

VMware provides new capabilities for DR

The same VM mobility properties that enable DRS and HA also enable some very unique new DR capabilities. But these VM mobility properties alone are not enough to provide a DR solution. For instance, consider how to solve the problem of replicating (copying) a live VM, one that is actively writing to a virtual disk.

Without leveraging assistance from an agile platform, copying virtual disk files while they are actively being written to will not yield a recoverable VM. In order to achieve a consistent replica of the original VM, a forced shutdown of the VM would be required, then a task to copy the powered-down VM, and finally a reboot of the VM at the end of the copy operation. In this state there would be a gold image for DR, but how practical is it in a 24x7 business environment? And how would critical software updates be made available to powered-down VMs?

VM snapshots

To get around this problem, VMware developed VM snapshot technology to provide a way to allow VMs to continue operation while their underlying virtual disk files are safely copied to a recovery location. When a VM snapshot is taken, the writes to the original disk are paused for a moment while a new file called a delta file or snapshot file is created to store new writes to disk. Developers and system administrators originally used this capability as a way to test new software updates and have the capability to quickly roll back to a known good state, but this technology has great DR applications as well. Since the parent virtual disks stay static and unchanged during the duration that the snapshot is open, the door is now open for brave administrators and enterprising software developers to develop the first whole virtual machine backup and recovery systems.

This first technology would simply orchestrate this snapshot technology and copy the VM in its entirety to another location. This backup could be registered with any VMware ESX(i) server with available compute resources and booted up in its entirety without any intermediary steps. These newly enabled VM backup methods worked from outside the VM and did not require a software backup agent to be installed inside every VM requiring backup. These developments dramatically lowered RTOs and offered the simplicity of one- or two-step DR plans per VM. They also greatly increased the number of organizations pursuing virtualized DR plans. Mission accomplished, right? Not exactly, as there are limitations and misconceptions to be aware of.

First-generation VMware DR – the missing manual

As compelling as the benefits of virtualization-enabled DR would be, there are some well-known deficiencies with the first iteration of VMware-aware backups. Every DR planner should be aware of these when designing or evaluating a DR solution for virtual infrastructures. These common deficiencies are:

Lack of guaranteed backups: Reliability of backed up or replicated VMs is not guaranteed, and it's a slow, manual process to verify they work.

Limited restore consistency: Replicated VMs were only crash-consistent and not fully Microsoft Volume Shadow Copy Service (VSS) aware. This result led to requiring the use of backup agents inside the VM.

Obscured access to individual files: Granularity of restores was non-existent, requiring manual, complex restores.

Bandwidth limitations: Solutions did not work efficiently over WAN links and were limited to LAN deployments.

Increased cost and complexity: First-generation VM backup technologies were fragmented from replication solutions, adding the cost and complexity of managing two VMware data protection products in addition to traditional backup software to plug other gaps.

It's these deficiencies that drove many organizations to take a "belt and suspenders" approach to DR on VMware, using both VMware-aware backup products and traditional backup software. This approach means you need to maintain two backup systems, pay for two backup software contracts, require IT support teams to learn two or more redundant data protection skills, and one extra step to complete when a disaster is declared. Although this approach ultimately provides some reliability, it does so at the expense of speed, complexity, and the cost of your DR solution. This legacy approach to DR is heavy baggage slowing you down on your journey to a legacy-free DR solution.

Veeam vPower is legacy-free DR

With the recent release of Veeam Backup & Replication v5 with vPower, VMware customers finally have all the features they need to confidently transition to legacy-free DR strategies. The mature features like advanced VSS support, instant file-level recovery, and inline deduplication have provided the solid foundation for a legacy-free DR solution since the version 1.0 product. These features closed the gaps in virtualization backup and allowed customers to implement legacy-free DR solutions for large portions of their environment. Since the 1.0 product release, Veeam has added VMware vStorage API integration coupled with new patent-pending capabilities like SureBackup™ Recovery Verification, U-AIR™ (Universal Application-Item Recovery), and SmartCDP™, which greatly address DR concerns and eliminate the shortcomings of traditional VMware backup solutions.

vPower addresses DR concerns

DR strategies must address the four main concerns identified earlier: uptime, reliability, cost, and complexity. Veeam Backup & Replication addresses these concerns like no other product before it.

Uptime—The name of the game in DR is uptime. Once a disaster is declared, the race is on to meet the RTO. With InstantRestore™, restores of full VMs, files or application items can happen instantly without intermediary steps. vPower allows a VM to run directly from a compressed and deduplicated backup file. This means a VM can be restored at the speed a VM takes to be booted from the backup file. In addition, SmartCDP allows the option to have RPOs in the minutes. SmartCDP leverages VMware vStorage integration to enable the fastest VM replication ever and provide near-continuous data protection (near-CDP).

Reliability—Without reliability, features developed to increase uptime are really just a hurry-up-and-wait approach to DR. VM backups and replicas must be reliable before a restore can meet an RTO, and RPOs will be affected if you have to go too far back in time to find a quality backup. vPower includes advanced VSS support to ensure backups and replicas provide application consistency and are restorable the first time. Even with this advanced feature, it is still necessary to test backups to verify recoverability. SureBackup Recovery Verification provides an additional level of protection by verifying each and every VM backup is restorable. Back in the old days you would verify that you got all the bits backed up correctly, SureBackup goes beyond that to actually boot up the VM and verify recoverability with every backup.

Cost—Providing unprecedented reliability, uptime, and granularity for VMware data protection allows customers to sunset the use of traditional in-guest backup agents. This reduces the cost of maintaining two or more different data protection systems. Granularity is addressed by U-AIR features that allow the restoration of objects from any virtualized application and also has wizards to support recovery from Microsoft Active Directory, SQL Server and Exchange. Veeam also supports instant file-level recovery from any OS and file system. It's this granularity coupled with reliability features that finally kick the in-guest backup agent to the street.

Another key cost saver is that VM backup, replication, and granular recovery features are implemented in a single product. Other solutions require a dizzying array of software, agents, and hardware to provide the same functionality. With Veeam, you use one software product and your choice of commodity server and storage hardware. In addition to software and hardware costs, Veeam can save you money on network bandwidth to your recovery sites by using WAN bandwidth efficiently. This allows replication over slower links than typically required for large data transfers seen in a backup solution.

Complexity—Veeam Backup & Replication is a single product that provides VM-level, file-level, and application-level protection, eliminating the complexity of providing protection at different levels with different products. By removing the need for backup software inside the VM, VMs become more lightweight and consume less CPU and memory. Lack of agents simplifies the VM image used to provide the initial load. Agent-less protection streamlines the provisioning of data

protection services to a VM. The protection can be configured by placing the VM on a protected host or folder or by configuring Veeam Backup & Replication to protect the specific VM. DR exercises are also greatly simplified and accelerated due the features provided by InstantRestore and SureBackup. InstantRestore technologies save DR teams time testing since VMs can be run directly from backup files and files and application objects can be restored instantly from the same VM backup file. SureBackup can help remove the complexity from DR exercises by automating testing that would be cost-prohibitive to have a human being conduct manually. Veeam Backup & Replication also allows DR teams to create an on-demand virtual lab of a set of VMs that comprise an application. This sandbox can be provisioned quickly and isolated from the production network in order to troubleshoot and perfect your DR plan for complex multi-tier applications or applications with many dependencies. These technologies allow companies to be more proactive about their DR testing and create a repeatable, provable DR plan that exceeds RTOs and RPOs.

Time for a Veeam-first DR strategy

Whether you are planning for a new greenfield deployment of VMware and DR systems, or if you are a seasoned VMware shop, the time is right to adopt a Veeam-first data protection strategy. The technology is proven and ready to address your data protection needs. In order to fully realize the benefits, a strategy needs to be adopted to ensure Veeam Backup & Replication is fully leveraged to simplify your environment and reduce costs associated with DR. This strategy is called Veeam-first, and it requires Veeam Backup & Replication to be used as the sole data protection method for your VMs.

A Veeam-first DR strategy is a similar approach to the first VMware virtual-first strategies that were employed to help create some tactical guidance to the strategic goal of fully virtualizing your datacenter. A virtual-first policy means that application owners have to use VMware VMs as the platform for new applications or as part of hardware refreshes. This was a great method to contain the previously unbounded proliferation of physical servers in datacenters and to help start to chip away at the cost of managing large physical server environments. Without the virtual-first policies, application owners and other server huggers would be reluctant to virtualize and would have an easier path to choosing more costly physical server platforms. This virtual-first strategy allowed operational efficiency savings along with power and cooling savings to begin accumulating sooner than if workloads remained on costly, inflexible physical server platforms. The impact of an aggressively implemented virtualization strategy is reaching a lower TCO (total cost of ownership) sooner and realizing an ROI faster. For this reason, many virtual-first strategies began with a large P2V (physical to virtual) migration effort to achieve that ROI faster. A similar effort should also be considered when implementing a Veeam-first strategy in order to begin fully leveraging the cost-saving benefits and capabilities of the Veeam vPower vision.

But operating a successful virtual-first policy takes more than policies and big sticks to motivate application owners to go along with a Veeam-first DR strategy. It means that virtualization engineers need to be solution providers to make sure availability and DR capabilities are the same or better on VMware platforms. I

think it's clear that Veeam Backup & Replication can best address the availability and DR needs of these critical applications, providing more features, best RPOs and RTOs, at the lowest cost. Features like SureBackup, InstantRestore, and on-demand sandbox all allow Veeam-first strategy adopters to verify that their strategy is working day in and day out. It's this verification that allows customers to confidently begin their journey to legacy-free DR with Veeam.

About the Author

Sean is a ten-year IT veteran with a background in software development, database administration, security coordination, and IT management. The last five years, he has focused on developing his expertise in VMware virtualization and surrounding technologies. He has kept current VMware Certified Professional (VCP) status on VI 2.5, VI 3.5 and vSphere 4. In 2009 Sean was awarded VMware vExpert status, one of 300 globally to receive the award recognizing their contribution to the virtualization community. Since then, Sean has been an active member of the virtualization community as a notorious Twitter contributor with the handle of @vSeanClark, as co-instigator of the popular vmunderground.com community party at VMworld, and as a random blogger at http://seanclark.us. He has provided guidance on virtualization strategy to businesses of all sizes and from all industries, and is currently a virtualization consultant with TEKsystems working on a long-term cloud computing project for a Fortune 500 company.

About Veeam Software

Veeam Software, an Elite-level VMware Technology Alliance Partner, develops innovative software to manage VMware vSphere. Veeam vPower™ provides advanced Virtualization-Powered Data Protection™ and is the underlying technology in Veeam Backup & Replication™, the #1 VMware backup solution. Veeam ONE™ provides a single solution to optimize the performance, configuration and utilization of VMware environments and includes: Veeam Reporter™—VMware capacity planning, change management, and reporting and chargeback; Veeam Business View™—VMware business service management and categorization; and a choice of VMware monitoring options including the nworks Management Pack™—VMware management in Microsoft System Center, the nworks Smart Plug-in™—VMware management in HP Operations Manager, and Veeam Monitor™—framework-independent VMware monitoring. Learn more about Veeam Software by visiting www.veeam.com.

VEEAM

BEST OF vmworld 2010 BEST OF SHOW

BEST OF vmworld 2010 GOLD AWARD NEW TECHNOLOGY

WINNER 2011 VIRTUALIZATION

#1 VMware Backup

100% Reliability | Best RTOs | Best RPOs

SureBackup™ | InstantRestore™ | SmartCDP™

vPower™
Virtualization-Powered Data Protection™

5 Patents Pending!

VMware vSphere

5 Patents Pending!

NEW Veeam Backup & Replication™ v5

vPower enables these game-changing capabilities in Veeam Backup & Replication v5:

- **Instant VM Recovery**—restore an entire virtual machine IN MINUTES by running it directly from a backup file
- **U-AIR™ (Universal Application-Item Recovery)**—recover individual objects from ANY application, on ANY OS
- **SureBackup™ Recovery Verification**—automatically verify the recoverability of EVERY backup, of EVERY virtual machine, EVERY time

To learn more, visit www.veeam.com/vPower