

NEW White Paper

7 Myths about Backup & DR in Virtual Environments

by Eric Siebert, VMware® vExpert



Eric Siebert

VMware® vExpert

Eric Siebert is an IT industry veteran, speaker, author and blogger with more than 25 years of experience who has been focused on virtualization since 2005. Siebert has published books including his most recent, "Maximum vSphere" from Pearson Publishing, and has authored training videos in the Train Signal Pro series. He also maintains his own VMware information website, vSphere-land. Siebert is a frequent speaker at industry conferences including VMworld and has been recognized as a vExpert by VMware each year since the programs inception in 2009.

Backup and disaster recovery of servers and data are two necessary areas that all companies must deal with to ensure that their most valuable assets are protected. While implementing a backup solution may seem easy it often becomes a challenge to implement and maintain an approach that you can count on to recover data when needed. Virtualization technology further complicates things, potentially disrupting your ability to protect your data center.

Many misconceptions surround backup and recovery in virtual environments. In this paper we will dispel the most common myths about backup and DR in virtual environments and help set the record straight.

Myth 1 - You shouldn't run backup agents inside a guest VM

The Fact: It's OK to run an agent inside the guest OS of a VM if that agent is "smart", i.e., aware of the virtualization layer

You've probably heard it over and over: you should never run backup agents inside the guest OS of a virtual machine. Rather, you should always back up outside the guest OS at the virtualization layer. The reasoning behind this technique is that such an approach is more efficient. Unfortunately most backup agents running in the guest OS are not aware that they are running inside a virtual machine, and therein lies a problem: the backup will consume host resources to the extent that they noticeably slow applications on the VMs. But the problem isn't that you have a backup agent running inside the VM, it's that you have a backup agent running inside the VM that isn't aware of the virtualization layer.

The fact is, it's OK to run an agent inside the guest OS of a VM if that agent is "smart", i.e., aware of the virtualization layer. Such a smart agent is optimized to work with inside the OS. Many backup applications built for virtualization do run an agent of some sort inside the guest OS. Even VMware itself runs an agent inside the guest OS with the VMware Tools application, which is designed to allow the hypervisor and guest OS to communicate with each other. By running an agent in the guest OS you ensure that applications and data are in a consistent state prior to the backup. Having an agent on the inside and backing up from within the guest OS can be just as efficient as backing a VM up from the outside. AppAssure uses smart backup agents that are optimized for virtual environments to ensure that you get the most efficient and consistent backups with very minimal resource impact (roughly a 1% - 3% load) on virtualized applications.

Myth 2 - You should always back up VMs through the virtualization layer

The Fact: It doesn't matter how you back up the data as long as it is done efficiently, with as little resource impact on your production environment as possible.

Here's another one that you hear time and again: "If you use virtualization you should always back up VMs through the virtualization layer using the special APIs that provide direct access to VMs from outside the guest OS." The theory here is that backing up from inside the guest OS is inefficient because there is extra resource overhead and you do not have direct access to the VM's virtual disk. Again, this is true if you are using backup agents designed for traditional physical server environments that are not aware of the virtualization layer.

In a virtual environment you must be sensitive to the resource requirements of other VMs on a host. You do not want the backup of one VM negatively impacting the performance of other VMs. Backing up VMs through the virtualization layer helps negate this impact, but it's also possible to reduce the impact when backing up inside the guest OS by using a backup application, like AppAssure, which is aware that it is operating in a virtualized environment. AppAssure is designed to minimize resource impact and it can intelligently and efficiently reduce the amount of data sent to the backup server. Results are what count and it doesn't matter how you back up the data as long as it is done efficiently with as little resource impact on your production environment as possible.

Myth 3 - You can't get a RTO of less than 60 minutes without storage replication

Fact: An RTO shorter than 60 minutes is no longer limited to replication with a storage array. Data can be replicated at the block level through software that runs inside the guest OS so quickly and efficiently that RTOs can be brought down to as low as 5 minutes depending on the infrastructure in use and the rate that data changes.

Recovery Time Objectives dictate how much time a company can afford to be without their applications. Many companies require a Recovery Time Objective (RTO) as low as possible to minimize disruption to their environment and the loss of critical data. Achieving a RTO less than 60 minutes usually requires storage replication to continuously replicate your data between storage arrays. While storage replication delivers very low RTO's all the way down to zero, for continuous availability. But those low RTO's come with a hefty price tag: you need to buy similar arrays for the source and destination that have the ability to replicate with each other.

Fortunately RTO's shorter than 60 minutes are no longer limited to replication with a storage array. Data can be replicated at the block level through software that runs inside the guest OS so quickly and efficiently that RTOs can be brought down to as low as 5 minutes depending on the infrastructure in use and the rate that data changes. AppAssure can continuously update both virtual and physical servers allowing you to create a full virtual clone for standby purposes. By doing this you get the low RTOs you need and save money; its ability to work seamlessly across dissimilar arrays eliminates the need to purchase and maintain identical equipment.

Myth 4 - You need separate backup apps to back up physical servers and virtual machines

Fact: Select a solution that handles both environments with simplified management, unified backup & replication and the ability to recover from anywhere to anywhere.

Almost every company that implements virtualization already has a backup application for their physical servers. Frequently they purchase a separate backup application that is optimized for virtual environments. One weakness of backup applications optimized for virtual: they typically only support the backup of VMs and cannot backup physical servers. Another weakness: you need to manage and maintain two separate backup systems. This can double your administrative workload.

Instead, why not choose a single application that works equally well with both physical and virtual? It is easier to manage and it provides greater flexibility and greater efficiency. You can establish backup interoperability between the two environments and easily go from virtual to physical or physical to virtual when needed. AppAssure handles both environments with simplified management, unified backup & replication and the ability to recover from anywhere to anywhere.

Myth 5 - You can't perform a bare metal restore of a VM unless you back it up at the virtualization layer

Fact: An image-level backup from within the guest OS, backed up at the block level instead of the file level, gets you the same end result as backing a VM up at the virtualization layer, with the only difference being that it occurs from within the VM.

Bare-metal restores are used to recreate a complete system including the operating system, application and settings, and they are very useful for DR/BC and for restoring point-in-time copies of a VM. Virtual machines are encapsulated into large virtual disk files that exist on a host file-system, which makes bare-metal restores much easier. A common misconception with virtualized environments is that the only way you can perform bare-metal restore of a virtual machine is to back it up from the outside through the virtualization layer. The fact is, a much more efficient method would be an image-level backup from within the guest OS, where data is backed up at the block level instead of the file level. This gets you the same end result as backing a VM up at the virtualization layer, with the only difference being that it occurs from within the VM. As a result you can perform the same bare-metal restores of a VM when you back it up from within the VM as you can do when you back it up at the virtualization layer. AppAssure provides full bare-metal restore, the flexibility of doing P2V, V2P, P2P, V2V and the ability to restore to dissimilar hardware.

Myth 6 - You can't restore application objects without using application agents

Fact: In fact, you can easily and seamlessly restore objects for critical applications without the use of agents.

Having the ability to restore application objects can make recovery much easier when you only need to restore a small subset of records to an application. Restoring individual objects from within an application, such as records from Microsoft SQL Server or Exchange, can sometimes be a challenging and time-consuming task. Typically it involves auto-installing a backup agent running inside the guest OS that understands the application that you are backing up and can read its native file structure. In many cases these application-specific backup agents require additional licensing costs.

Alternatively, some of today's 1st generation VM backup products will offer the ability to perform granular recovery, but at a cost. That cost is usually time and infrastructure. To restore an email, you may have to first launch a VM clone and extract the database, then use precious resources to run it long enough to do that extraction. Once you have the database, you then would resort to antiquated techniques to retrieve the data.

AppAssure natively understands many popular application file formats so you do not need to install and license a special backup agent in order to restore application objects. This is a key capability as the cause of many restores tends to be from deleted records instead of deleted files. With AppAssure you can easily and seamlessly restore objects for critical applications without disrupting user access to the application. It restores application objects, files and entire virtual machines all from one software product.

Myth 7 - The only way to verify your backups is to perform a full restore

Fact: Solutions like AppAssure automatically test and verify the recoverability of your backups without performing a full restore.

While having good backups is important, having the ability to successfully restore data when needed is even more important. Backups are useless if you cannot restore data properly and backup verification is necessary to prove that you can. But verification is more than just checking for media errors. If there is something wrong with your source data that will carry over to your target as well. This can be caused by things like corrupt, open or missing files and improper quiescing. Traditionally, to perform this verification, you need to carry out a full restore, then boot the VM, login and verify access key files and applications. This can be very time-consuming task, and doing it on an ongoing basis is a real challenge.

Automated backup verification makes life much easier and ensures that every backup is verified without having to perform a full restore and verifying it manually. AppAssure solves this challenge with its innovative Assured Recovery technology which automatically tests and verifies the recoverability of your backups without performing a full restore. This ensures that critical data from key applications like SQL and Exchange can be recovered when necessary and no surprises await you when you try to recover them.

Summary

Make sure you have your facts straight when looking for software to protect your virtual environment. Virtualization is still relatively new technology and there is often a lot of confusion with it as it represents a drastic change from traditional server architectures. Removing the mystery that sometimes surrounds virtualization will help you make informed choices when choosing a backup product. Data protection requires you to understand the technologies and methods needed to implement the product to ensure that it does more than just meet your requirements. It should exceed them and provide you with extra value and efficiency. AppAssure was designed to deliver that and more with unified data protection for your virtual, physical and cloud infrastructure.

About AppAssure Software

AppAssure is the #1 unified backup & replication software for virtual, physical and cloud environments. This multiple award-winning and customer-proven software recovers virtual and physical servers, applications and data in minutes instead of days or hours. AppAssure's innovative and groundbreaking technologies assure 100% reliability of recovery and goes beyond just protecting data to protecting entire applications. It also supports multi-hypervisor environments including VMware vSphere / ESXi, Microsoft Hyper-V and Citrix XenServer. AppAssure is an Elite VMware Technology Alliance Partner and Microsoft Gold Certified Partner. With more than 6,000 customers, partners and service providers in over 50 countries and over 3,000% growth in three years, AppAssure is the world's fastest growing backup software company as ranked by Inc. Magazine.

AppAssure's 3 Innovative and Groundbreaking Backup Technologies:

1. Live Recovery™

Instant restore of VMs or Servers – near-zero recovery time (RTO) & 5-minute RPO

2. Recovery Assure™

Assurance of 100% Reliability of Recoverability

3. Universal Recovery™

Anywhere to Anywhere Restore – to any VM or dissimilar hardware with Granular Object Level Recovery

WINNER OF 10 TOP INDUSTRY AWARDS



5 Reasons to Try AppAssure – Get a FREE Trial Now!

1. Ultra-Fast Backup & Recovery – near-zero Recovery Time & 5-minute RPO
2. Recovery Auto-Testing and Auto-Verification - 100% Recoverability
3. Unified Backup & Replication from One Single Pane of Glass
4. Recovery Anywhere to Anywhere (P2V, V2V, V2P, P2P)
5. True Global Deduplication

www.appassure.com/Free-Trial



#1 BACKUP
VM, Physical & Cloud

AppAssure Software, Inc. 1925 Isaac Newton
Square East, Suite 440, Reston, VA 20190
Americas: 1-866-459-6653
EMEA: 44-1306-888864

Connect with AppAssure:
<http://www.appassure.com/facebook>
www.appassure.com/twitter
www.appassure.com/blog

© 2012. AppAssure Software. All Right Reserved.

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.