WHITE PAPER

Top 10 Best Practices of Backup and Replication for VMware and Hyper-V

By David Davis, VMware vExpert

Virtualization changes everything for IT infrastructure administration and management. One of the many traditional, and most critical, infrastructure management processes that server virtualization breaks is backup and recovery. Once server virtualization is in place, backup and recovery systems, as well as admins, have to adapt. For example, unlike with physical servers, virtual servers can move from one host to another so you lose the host to guest OS mapping. Many virtual infrastructures were set up quickly, by admins who were new to virtualization, at a time when few best practices existed for virtualization backup and recovery.

Whether you are new to virtualization or if you have been administering a virtual infrastructure for a while, it's now time to review your virtual infrastructure backup design and backup product features in use to ensure that you are both optimally protecting your virtual infrastructure as well as taking advantage of the latest virtualization backup features which will make your life easier. Start now by learning the 10 best practices for virtual infrastructure backup and find out what you may be missing.

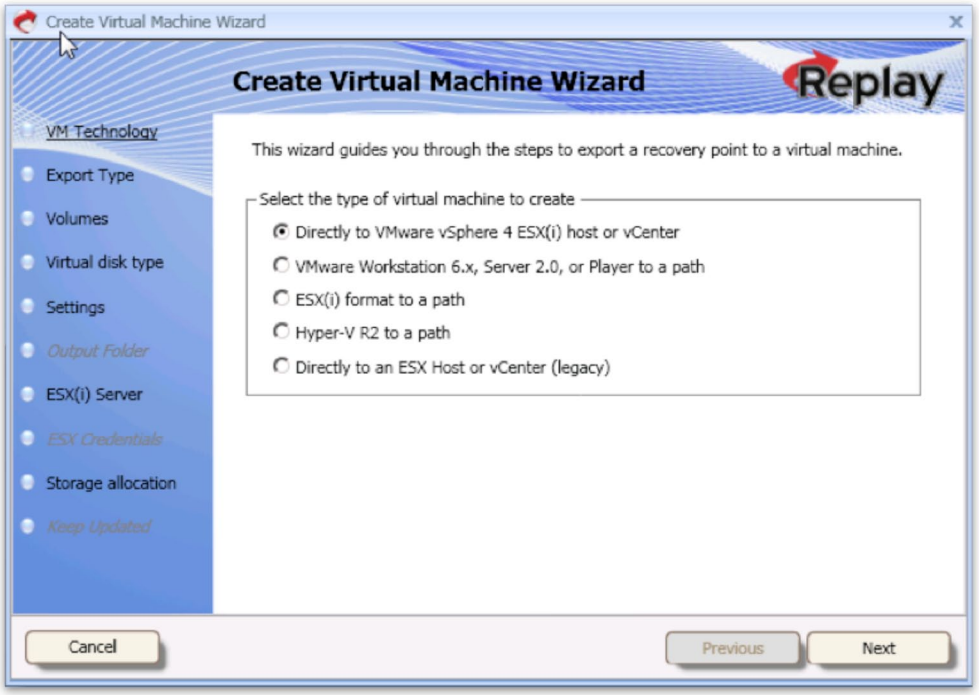
1. Use a Backup Tool that Understands your Virtual Infrastructure

Just because a backup tool says that it CAN backup your virtual infrastructure doesn't mean that it does it well (and you really want a tool that does it well). Traditional server backup tools backup virtual machines just by using the same file-based agents that they ran on physical servers. While this does perform basic file-level backups, it is very inefficient.

You'll want to select a backup tool that:

- **Does Block-Level Backups of Virtual Machines** such that only changed blocks of virtual machine disk files are backed up but those changed blocks can be combined with the original full to provide the most recent current image-level backup as well as the option to restore individual files.
- **Talks to the Hypervisor and/or Virtualization Management Tool** such that when image-level recoveries need to be done, those virtual machines can be automatically created through the hypervisor or centralized management tool using the hypervisor's API calls.

AppAssure Recovering a Virtual Machine Image through vSphere, vCenter, or Hyper-V

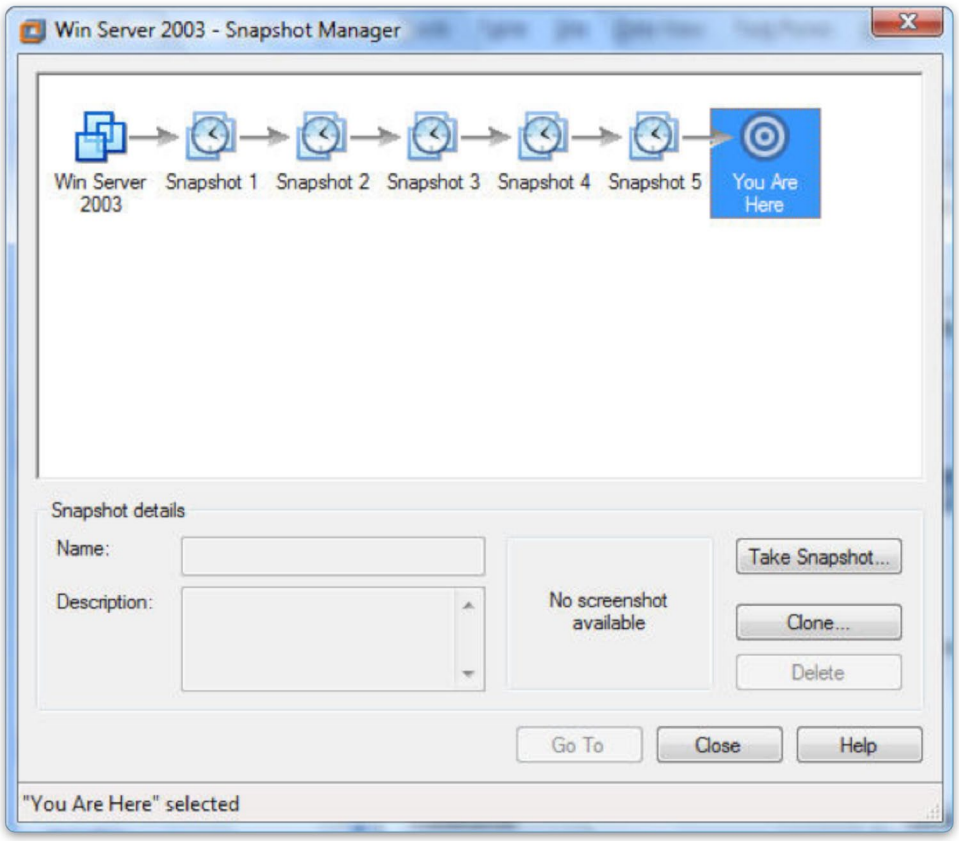


2. Don't Use Snapshots Unless Absolutely Necessary

Taking a snapshot (or multiple snapshots) using a tool like vSphere's Snapshot Manager is easily done but can take up large amounts of disk space. Additionally, there is a common misconception that snapshots can be used long term to offer you some kind of data protection. Snapshots should not be confused with virtual machine backups. Each has its own specific use case. Hypervisor snapshots are an excellent benefit and tool for virtualization Admins to use to protect you if you are performing an upgrade or changes to a critical VM.

On the other hand, virtual machine backups can be done every few minutes and are the single best choice you need to be using to protect your virtual infrastructure from data loss.

Creating Snapshots in the vSphere Client

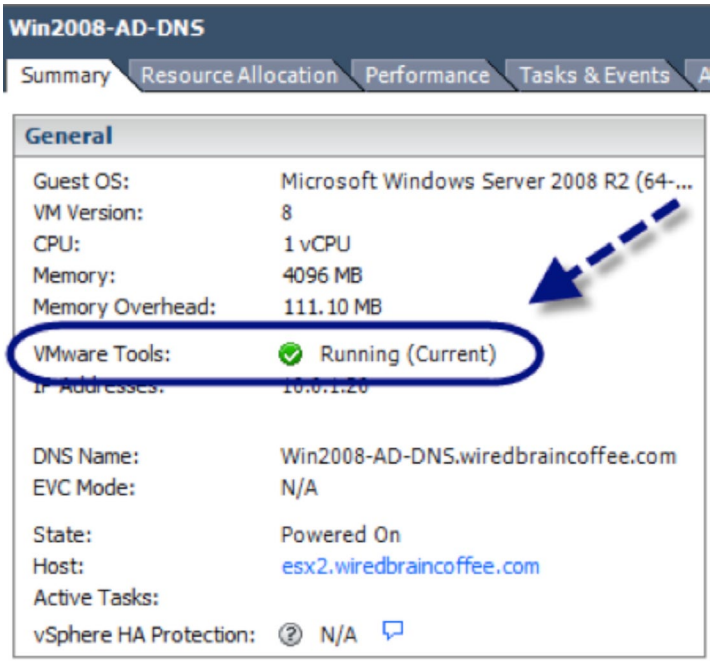


The best practice for snapshots is to use them when needed but then remove them as quickly as possible. If you need a permanent copy of a VM at a particular point in time then create a clone of that virtual machine instead. Finally, always protect your data using virtual machine backups.

3. Load Hypervisor Tools in the Guest OS

No matter the hypervisor you are running, you should install the virtual drivers, provided by the software manufacturer in each virtual machine. So, no matter whether it's the "VMware Tools", the "Hyper-V Integration Services", or the "Citrix XenServer Tools", they need to be installed in every virtual machine. These tools not only improve performance on a day to day basis of each virtual machine but they also provide the highest performance network drivers, for example, that allow a backup tool to get data in and out of the virtual machine as efficiently as possible.

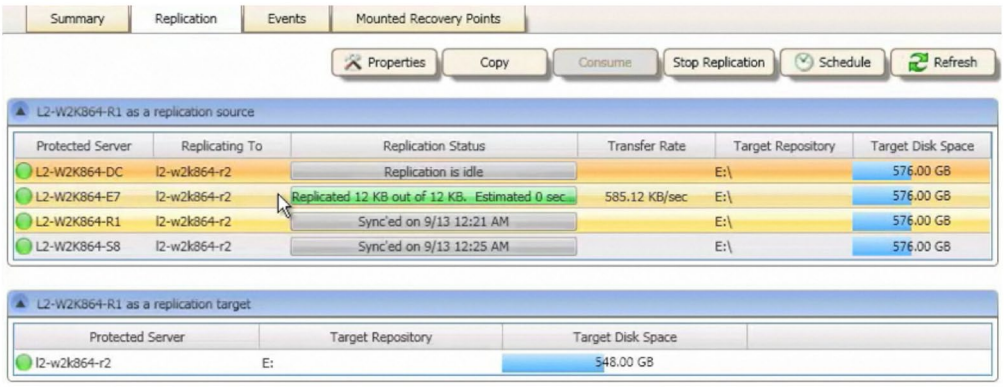
Verifiying that the VMware Tools are Running and Current



4. Use a Tool that Offers Offsite Storage and Replication

AppAssure Replicating a Virtual Machine

Most virtualization backup tools backup virtual machines (including their apps and data) to a file on a disk. While that is a great option for quick restore, it does nothing to get the data offsite in case there is a disaster. Virtualization backup tools shouldn't just end their process at leaving backup data on disk. They need to help you get that data offsite, either by going to tape or by performing replication to a remote site (or both).



Additionally, as very few companies have achieved 100% virtualization of their infrastructure, it would be extremely beneficial for a company to use a backup tool that could backup BOTH physical servers as well as virtual servers. For most companies, it would be ideal if backup data from both sources could be stored in the same repository and then that backup data could be replicated to an offsite location.

5. Ensure Your Servers Can Be Restored FAST

For any admin who administers backups, they know that they must not only test backup but, more importantly, test restores. Those restore tests should be done frequently and, no matter how frequently they are done, there is always some level of fear that when critical restore needs to be done, their backup & recovery tool may fail them or how long it would take for a large application to be restored.

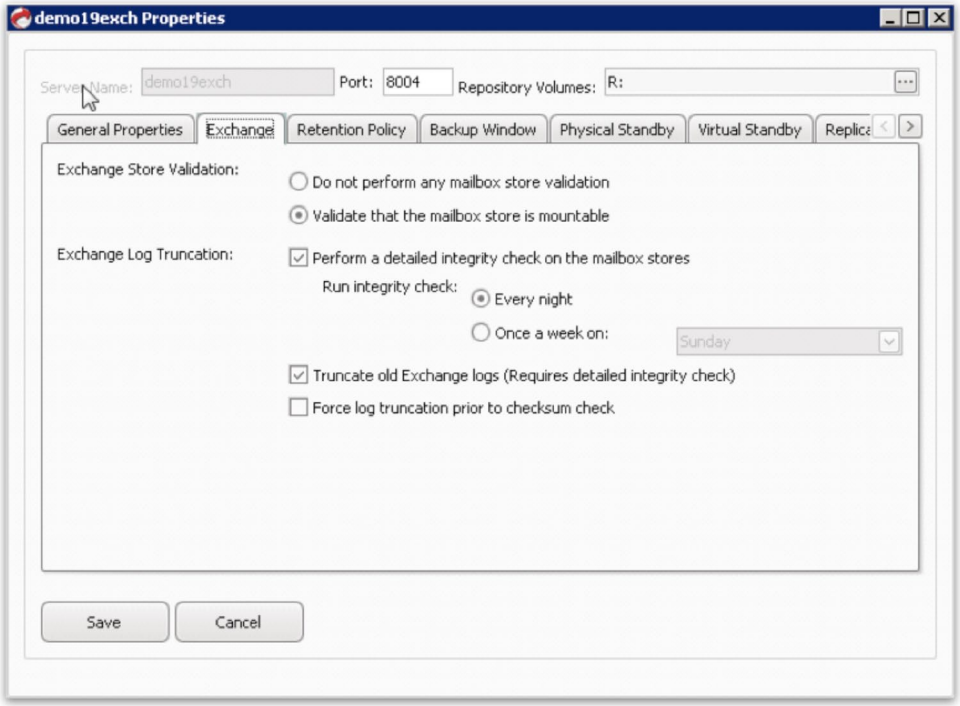
I recommend that you find a backup & recovery tool that can get your critical applications back up and running in about the time that it takes you to initiate the restore process. For example, AppAssure offers “Instant Recovery” that provides a near-zero RTO and 5 minute RPO. This works by providing files and folders indexes and metadata being recovered, to the operating system and application, before the complete block-level restore has completed. When a file is requested, the recovery job will send that file before other less critical files are recovered. The end result is that backup jobs are restored in just a few minutes vs. one or more hours.

6. Guarantee That The OS and Apps Inside a VM are Recoverable

A periodic complaint of virtualization admins is that their backup application performed a recovery but that, once the VM was recovered and booted, the OS would not boot or the applications wouldn’t run.

Today, some backup tools have matured to the point that after every backup, they perform integrity test of the data with native OS and application tools.For example, a backup application might use the native Exchange ESEUTIL.exe to verify the integrity of an Exchange database that was just backed up. Similar native application integrity checks could be done for just about any application running on physical or virtual servers.

AppAssure Gives You the Option to Test Exchange Using Native Tools, Everynight



Finally, a CHKDSK.exe could be run on each virtual machine to ensure that the native operating system sees the backup data as being valid and mountable.

Don't get a false sense of security thinking that your backup data is safe just because virtual machine backups have a status of "success". You must know that the OS and applications inside the VM have integrity and can be quickly accessed once restored.

For example, AppAssure offers "Assured Recovery" that verifies that you can 100% reliably recover both your virtual machines as well as your guest OS and applications. This ensures that application and operating system data, in physical or virtual server backups, can be restored with complete confidence, and will work, the first time.

7. Keep Options Open with Any to Any Backup and Restore

Just as you don't want a physical server backup program that will only restore backup data to the same physical server, you also don't want a virtualization backup program that will restore VM backups only to the same virtualization platform. When it comes to disaster recovery, you can plan but never quite know what will happen. That is all the more reason why you need a virtual

Graphic Thanks to http://technorati.com/technology/it/article/a-look-into-how-the-microsof

infrastructure backup program that will restore to other hypervisors OR to physical servers. Additionally, what about backing up physical servers and restoring those backups to a virtual machine in, say, vSphere or Hyper-V? Keep options open by making sure that your backup platform offers P2V, V2V, P2P, and V2P.

Can your virtualization backup & recovery tool backup from Hyper-V and restore to vSphere (or vice-versa?)

AppAssure calls this any to any physical and virtual recovery “Universal Recovery”.

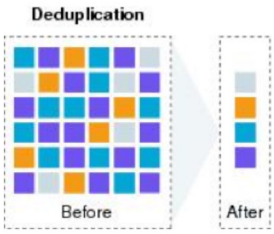
8. Make Sure It Supports “The Cloud”

More and more companies are using cloud infrastructure to host their company’s enterprise servers – both for disaster recovery and production. Just about every vendor is trying to say that their application is “cloud compatible”, in some way.

When it comes to backup and recovery, you want to be able to backup virtual machines running on a hosted cloud infrastructure, recover them, and even recover your current physical or virtual infrastructure to a hosted cloud platform when disaster occurs. Ensure that your infrastructure backup solution gives you the flexibility you may need now, and in the future.

For example, AppAssure can run on any infrastructure, physical or virtual, no matter where it's located (local or in a public cloud), giving you the ability to keep options open.

9. Use Deduplication and Compression



Graphic Thanks to http://virtualaleph.blogspot.com

As virtual machines multiple, a great strain is put on storage capacity. Besides the increased number of virtual machines, storage capacities are pushed by numerous virtual machine snapshots and virtual machine clones. Virtual machines running the same guest OS will typically be 80% identical so when deduplication is used on those virtual machines, tremendous storage capacity can be gained.

For these reasons, it is imperative that compression and deduplication are employed to reduce the size of backup data repositories.

10. Safeguard Your Company's Applications

Microsoft® Exchange Server 2010

Virtualization backup tools can be most effective if they know something about your applications. At the lowest level, a virtualization backup tool should use Microsoft's volume shadow service (VSS) to be able to quiesce the Windows file system, inside a virtual machine, to ensure that backups of files have integrity. From there, they could take it another level and ensure that Microsoft applications inside the VM (such as SQL Server and Exchange) are quiesced when the backup is performed to ensure that application data (not just files) have integrity that they will require when you restore them.

Once the virtualization backup tool is at least using VSS, you could take this a step further and the same tool could offer specialized backup agents that understand how an application works and how to backup (and recover) data blocks from its database. For example, besides virtualization backup tools, AppAssure also offers backup products specialized for SQL, Exchange Server, SharePoint, and SQL.

Conclusion

Ensure that the virtualization backup solution you are using now, and in the future, is going to provide the advanced features demanded by your growing virtual infrastructure. Features like replication and file level recovery have become common-place over the last year. Today, look for a growing list of features that make your virtualization backup tool more intelligent and flexible. Not all virtualization backup tools are the same. Make sure you take advantage of free evaluations to see which tool best fits the needs of your company.

About the Author

David Davis is a VMware vExpert and is the author of the best-selling VMware vSphere video training library from TrainSignal. He has written hundreds of virtualization articles on the Web, is also a VCP, VCAP-DCA, and CCIE #9369 with more than 18 years of enterprise IT experience. His personal Website is VMwareVideos.com.

AppAssure®

#1 BACKUP AND REPLICATION TO YOUR CLOUD

About AppAssure Software

AppAssure, the global leader in complete server, data and application protection for virtual, physical and cloud infrastructures, delivers customer-proven backup and replication software that assures the recovery of applications in minutes. AppAssure's groundbreaking technology uniquely guarantees instant and 100% reliable application recovery from your server to your datacenter – to your cloud. AppAssure goes beyond protecting data, to protecting entire applications enabling service providers and enterprises to adopt a cloud model to deliver fast, reliable and secure data protection. With 3,450% growth over the past three years and more than 5,000 customers, partners and service providers in over 50 countries, AppAssure is the world's fastest growing backup and replication software company, ranked by Inc. Magazine.

© 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.

www.appassure.com