Six Fairy Tales of VMware and Hyper-V Backup

UNITRENDS

7 Technology Circle
Suite 100
Columbia, SC 29203

Phone: 866.359.5411
E-Mail: sales@unitrends.com
URL: www.unitrends.com

Introduction

Cinderella. Snow White. Hansel and Gretal. VMware host-level backup works well with all deduplication strategies. These famous, and not so famous, fairy tales have one thing in common – they are fiction. In this paper we explore six fairy tales of VMware and Hyper-V backup. Like all fairy tales, our virtualization backup fairy tales are written to teach lessons in a fun way.

Our Six Virtualization Backup Fairy Tales

We've organized our six virtualization backup fairy tales as three VMware host-level backup fairy tales, two Hyper-V backup fairy tales, and one general virtualization backup pricing fairy tale.

VMware Host-Level Backup Works With All VMware Host Environments

VMware proponents often call out that the VMware vStorage APIs for Data Protection (VADP) offer a far superior backup technology when compared to any other virtualization environment. This is absolutely true. Then, some fans of VMware go one step further and state that this applies to all host-level forms of VMware. This is a fairy tale.

VADP is offered on two of the three versions of host-level VMware: ESX and licensed ESXi. One of the most common forms of host-level VMware, free ESXi, does not offer VADP. This isn't inadvertent on the part of VMware – it is a strategy designed to differentiate their paid versions of ESX and ESXi from the free version of ESXi.

If you're using free ESXi, be aware that you're not going to be using VADP or any other form of host-level protection. You're going to protect each virtual machine as if it was a physical machine. If you're licensing your backup software on a per-protected computer basis, you're going to be paying a whole lot of money for that "free" ESXi that you're using.

VMware Host-Level Backup Works Well With All Deduplication Strategies

Deduplication simply refers to the elimination of redundant data so that you get more backup storage per dollar spent. There are two primary forms of deduplication: source-level and target-level. Source-level deduplication has the advantage of potentially utilizing less network bandwidth but has the disadvantage of using much more processor, memory, and other resources from the computer that you are protecting. Target-level deduplication has the advantage of not using the resources of the computer that you are protecting but has the potential disadvantage of using more network bandwidth.

Source-level deduplication does not typically work well with VMware host-level backups. There are two reasons for this. The first is that VMware host-level backup has less redundant data through the use of CBT (Changed Block Tracking) – a technology that allows the

backup of only the changed blocks within VMware. The second, and more important, is that source-level backup takes precious resources away from the computer running VMware that is hosting the virtual machines. This is one of the reasons for the "sprawl and stall" phenomenon seen in virtualization projects today – increasing numbers of virtual machines are created, all underlying host-level computer resources are consumed, and the virtualization project grinds to a halt.

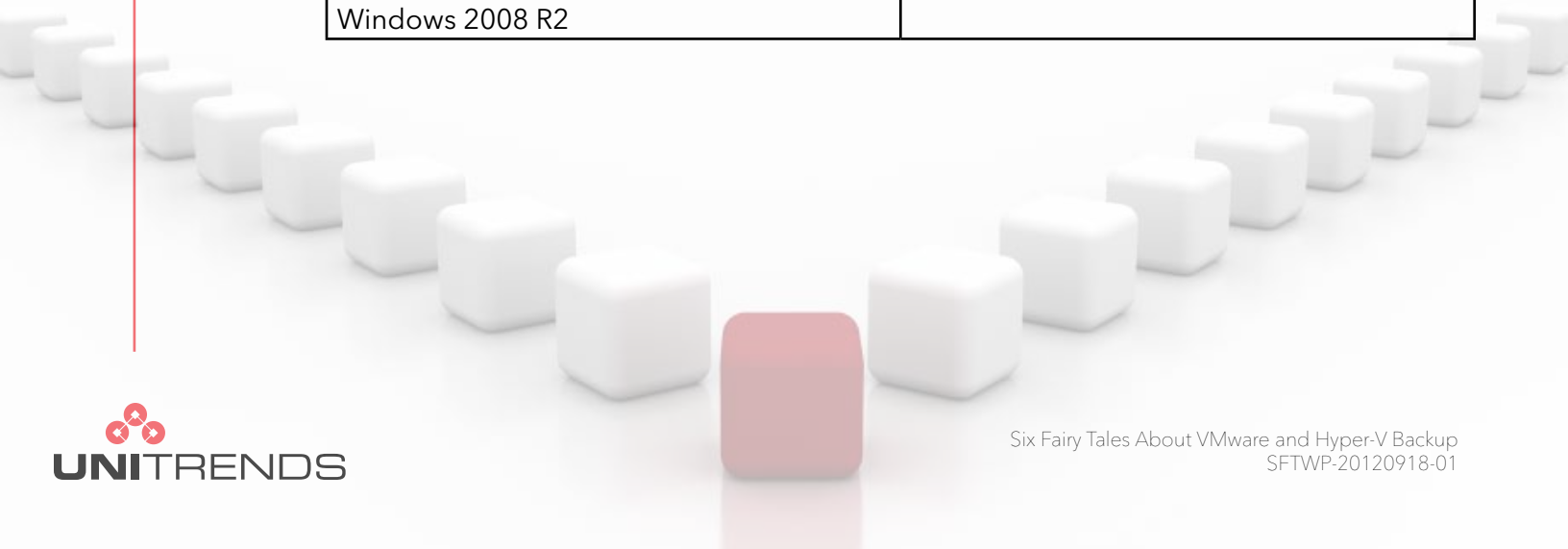
Use deduplication strategies with VMware that use less, not more, computer resources on the computer hosting VMware and you'll avoid getting eaten by the wicked witch of sprawl and stall.

VMware Host-Level Backup Has Problems When You Use Microsoft Windows Guest Operating Systems

Prior to VMware 4.1, Microsoft applications running within a Windows virtual machine hosted by VMware had an issue with respect to something called application-level quiescing. This simply meant that when you used VADP to protect your VMware environment that the backup did not produce in all cases crash-consistent backups for applications, such as Exchange or SQL. This meant that when you wanted to recover applications within these virtual machines that you'd have to perform integrity tests and repair in order to attempt to recover data for these applications.

VMware 4.1 supports application-level quiescing. The table below depicts the details of this:

Guest Operating System	Quiescing Type Used
Windows XP 32-Bit Windows 2000 32-Bit Windows Vista 32-Bit/64-Bit Windows 7 32-Bit/64-Bit	File system-consistent quiescing
Windows 2003 32-Bit/64-Bit	Application-consistent quiescing
(Pre-VMware ESX 4.1 Hosts) Windows 2008 32-Bit/64-Bit Windows 2008 R2	File system-consistent quiescing



Guest Operating System	Quiescing Type Used
(VMware ESX 4.1 and Later Hosts) Windows 2008 32-Bit/64-Bit Windows 2008 R2	Application-consistent quiescing. For application consistent quiescing to be available, three conditions must be met: • The UUID attribute must be enabled. This is enabled by default on virtual machines created on ESX 4.1 hosts. For virtual machines created on other hosts, see below. • The virtual machine must use only SCSI disks. For example, application-consistent quiescing is not supported for virtual machines with IDE disks. There must be as many free SCSI slots in the virtual machine as the number of disks. For example, if there are 8 SCSI disks on SCSI adapter 1, there are not enough SCSI slots free to perform application quiescing. • The virtual machine must not use dynamic disks.
Other Guest Operating Systems	• Crash-consistent quiescing

Hyper-V Host-Level Backup Is Efficient

Hyper-V host-level backup will be efficient one day – but it's not now. The reason is because of the underlying technology that Microsoft uses to protect all of its operating systems and applications. This technology, which is known as VSS (Volume Shadow Copy Service), is also used to protect Hyper-V environments.

Unfortunately, VSS for Hyper-V at the host-level only supports full backups at the time this paper was being written. This means that protecting Hyper-V is currently better done by protecting each Hyper-V virtual machine as if it were a physical system, as well as protecting the underlying Hyper-V physical system using the same technique.

Source-Level Deduplication Is an Effective Technique to Use With Hyper-V Environments

A consequence of each VSS-based Hyper-V backup being a full backup means that if you're using Hyper-V host-level backup then you are generating a tremendous amount of redundant information. This makes sense, right? After all, the reason that modern backup systems don't use full backups all the time is to perform data protection more efficiently by eliminating redundant data.

In order for the glass slipper of data protection to fit with respect to Hyper-V, some vendors recommend using source-level deduplication so that at least both the network over which

these backups have to travel and the storage used to store the backup will be burdened less. The problem, of course, is that by using source-level deduplication, you are consuming more resources on the Hyper-V physical computer; thus, you are lowering the ability of that computer to effectively host more virtual machines.

The answer is the same as described in the previous section: to protect all Hyper-V physical and virtual machines as if they were physical machines.

You Have to Pay for Advanced Virtualization Backup Services

This is true for most backup, archiving, and disaster recovery services. However, Unitrends supports not only virtualization but other advanced features, such as deduplication, using an all-in-one licensing methodology in which you don't pay for either the feature nor do you pay each time you want to add physical or virtual machines.

Conclusion

Virtualization is a powerful technology – you just have to make sure that you understand not only the rewards but the consequences of uninformed choices. Protecting virtual environments isn't difficult nor does it have to be expensive if you make the right decisions before starting your virtualization project. On the other hand, virtualization can become a figurative tar pit of a problem if you either ignore virtualization protection or try to spend your way out of your problems.

About Unitrends

Unitrends offers a family of affordable, all-in-one, on-premise backup appliances that support virtual and physical system backup and disaster recovery via disk-based archiving as well as electronic vaulting to private- and public-clouds. Unitrends is customer-obsessed, not technology-obsessed, and is focused on enabling its customers to focus on their business rather than on backup.

For more information, please visit www.unitrends.com or email us at sales@unitrends.com.

7 Technology Circle, Suite 100
Columbia, SC 29203

Phone: 866.359.5411
E-Mail: sales@unitrends.com
URL: www.unitrends.com