



Protecting Virtual Servers with Acronis True Image

In This Paper

Protecting Virtual Servers with Acronis True Image.....	3
Virtual Machines: The Data Protection Challenge.....	3
Mitigating Threats to Virtual Servers.....	4
Approaches to Backup.....	4
Protecting Virtual Machines in a Production Environment.....	5
Restore.....	6
Restore During Testing.....	7
The Future of Virtualization.....	8

Protecting Virtual Servers with Acronis True Image

IT organizations have discovered that virtualization technology can simplify server management and reduce total operating costs. Despite the technical and economic benefits of virtualization, though, its use in production environments can present a disaster-recovery challenge. Simply backing up a host server can be insufficient to ensure that data within virtual machines is recoverable. Acronis True Image Enterprise Server provides a comprehensive, reliable, and cost-effective data-recovery solution that backs up both a host server and all individual virtual machines on that server.

Virtualization software allows companies to deploy multiple logically distinct virtual machines, each of which runs its own "guest" operating system, on a single physical "host". Test and development groups have long used virtual machines to simplify the creation and re-creation of realistic test environments, but the introduction of products like Microsoft Virtual Server 2005 has also made it practical to apply virtualization in data-center scenarios such as server consolidation and legacy-application support.

To meet disaster recovery requirements for production systems, administrators must design and implement protection strategies that afford these virtual machines the same safeguards as traditional servers. As we will see, the architecture of virtual machine software means that simply backing up an entire physical server cannot always ensure recoverability. Thus disaster-recovery plans must be constructed with this reality in mind and must use appropriate software to fulfill these needs.

Virtual Machines: The Data Protection Challenge

Virtual machine software such as Microsoft Virtual Server 2005 runs atop a standard operating-system installation. An administrator may use the Virtual Server Administration Web site to create new virtual machines with specific hardware characteristics, including RAM, peripherals, network connections, and hard disks. These settings, and all the data needed to represent the virtual machine, are encapsulated in a small number of files on the host's physical hard disk (table 1). The administrator then starts up a virtual machine and loads a "guest" operating system and any desired applications.

Microsoft Virtual Server 2005 R2 File Type	Description
.vmc	Virtual machine configuration file. An XML file that describes the hardware and virtual hard disk(s) assigned to a virtual machine.
.vhd	Virtual hard disk file. One or more can be assigned to a virtual machine. Contains every byte of data that a virtual machine saves to its virtual hard disk. VHD files are also used for differencing disks.
.vsv	(optional file) Virtual machine saved-state file. Captures the contents of the virtual machine memory when the VM is suspended, so it can be restored to exactly the same state when restarted.
.vud	(optional file) Virtual machine undo disk file. If an undo disk is enabled, it stores any disk changes made – instead of those changes appearing in the .vhd file.

Table 1: Files Comprising a Virtual Machine

From the vantage point of the guest operating system or applications running on top of it, everything behaves as if the operating system were running on its own physical server with the hardware defined by the virtual machine configuration file. From the perspective of the host operating system, though, the virtual machine is just another application and a handful of data files.

The benefits of using virtual machines in a data center are numerous. Instead of being confined to one operating system on each physical computer, companies can leverage virtual server technology to deploy multiple environments on the same server. Companies can use virtual servers to eliminate costs of managing and upgrading legacy hardware by migrating older applications onto virtual machines running on new, reliable hardware. They can also consolidate low-use departmental servers onto a single physical server to decrease management complexity.

Virtual machines used for production purposes, like any production server, contain a constantly changing set of user data, settings, and applications that must be protected. Although virtual machines used in testing scenarios don't contain live data, creating and configuring testbed virtual machines nevertheless represents a significant investment of human time and effort -- often many hours or days of work -- and thus merits a similar degree of attention.

Mitigating Threats to Virtual Servers

Virtual servers are subject to the same variety of loss scenarios as traditional servers, as well as some additional ones that arise from the nature of the virtualization technology. These loss scenarios include:

- Complete hardware loss due to theft, fire or flooding, or similar disasters
- Hard-disk corruption or failure
- Compromise of host operating system, whether by virus or similar malware, software failure, intentional hacking, or human error
- Compromise of guest operating system, by any of the mechanisms that can compromise the host OS
- Human error, including accidental deletion or modification of a virtual machine or virtual hard disk or its files on the host

Acronis True Image Enterprise Server protects virtual servers and virtual machines against these and other loss scenarios. Acronis True Image's real-time disk-to-disk imaging solution lets administrators protect the operating system, applications, settings, and data for the host operating system and for each virtual machine in a manner that is faster, more comprehensive, and simpler than traditional file-by-file backup to tape devices. The resulting backup images can be stored on a separate physical drive attached to the virtual server, on a hidden partition on each virtual machine called the Acronis Secure Zone, or on any network-accessible drive.

Additionally, Acronis products support all of the host and guest operating systems supported under Microsoft Virtual Server 2005 R2 (including Linux) so each and every virtual machine can be protected. Administrators can choose on-demand image creation or scheduled jobs for periodic full, incremental, or differential imaging.

Approaches to Backup

Two mechanisms for protecting the virtual server are possible in principle. One is to back up the files that comprise the virtual machines from "outside" -- that is, from the host operating system. The other is to back up the virtual machines from "inside", treating each virtual machine like a distinct physical server that needs to be backed up independently.

In practice, backing up production virtual machines from outside is insufficient. Because running virtual machines keep state information in memory, simply backing up the .VMC, .VHD, and other files cannot reliably capture the complete state of a running virtual machine. It is possible to back up virtual machines when they are not running, but that would mean shutting them down during the backup cycle -- rarely a realistic option in a production environment.

Backing up virtual machines from within each virtual machine is thus the preferred approach in a production environment. Since these virtual machines may be running server operating systems such as Microsoft Windows Server 2003 or Microsoft Windows 2000 Server, the backup solution must be designed and licensed to run on these operating systems. (Many desktop backup solutions simply don't work on server operating systems.)

Acronis True Image Server products are both designed and licensed to back up all operating systems supported by Microsoft Virtual Server 2005 R2, including Linux. Since Acronis True Image Enterprise Server backs up live and running servers, it has no problem backing up running virtual machines in production environments.

Protecting Virtual Machines in a Production Environment

Acronis True Image Enterprise Server can run on the host and within each virtual machine to ensure that both the host system and all individual virtual machines are backed up. Administrators can back up on demand or schedule backups for the host and each virtual machine as desired.

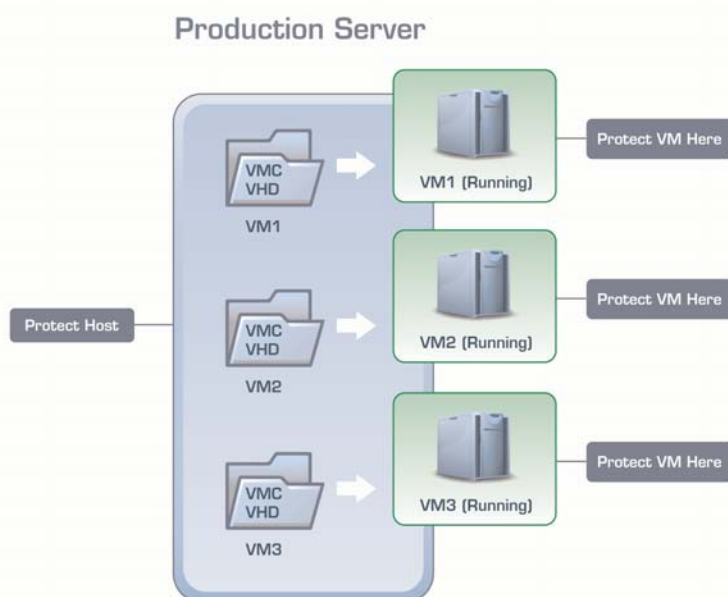


Figure 2: Running virtual machines in the production environment must be protected from inside the guest operating system.

By creating and verifying complete images of live hard disks and partitions, administrators can be certain that all data, settings, applications, and operating system files are protected. In a typical scenario, an administrator might schedule a full image creation for each virtual machine once each week and incremental images daily throughout the week. An administrator can, of course, schedule incremental or differential images or perform backups more or less frequently as desired.

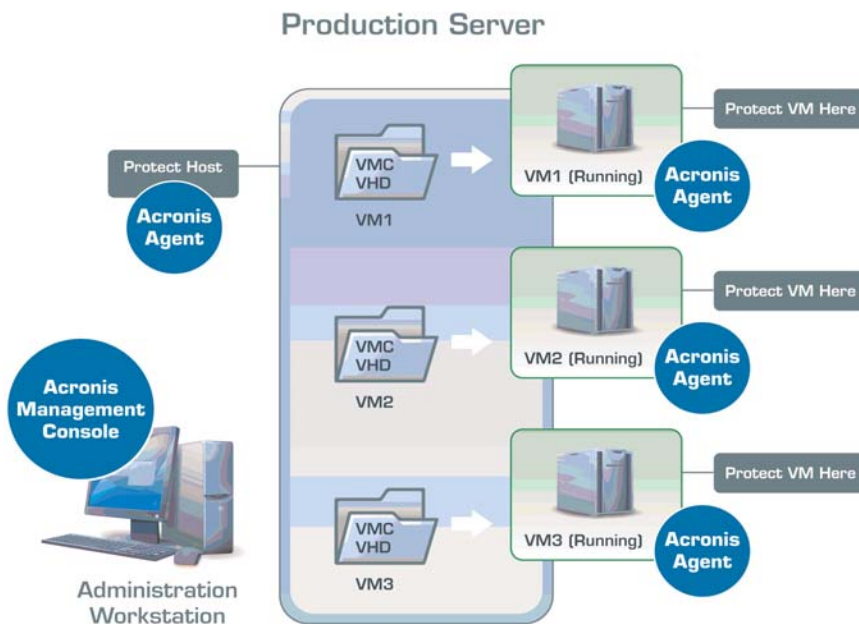


Figure 3: The Acronis True Image Enterprise Server agent architecture provides a convenient approach to protecting large numbers of virtual machines.

For convenience in protecting multiple virtual machines on one or more physical servers, Acronis True Image Enterprise Server uses lightweight distributed agents, as shown in Figure 3. One agent runs on each virtual machine; a central management console controls on-demand and scheduled image creation on any virtual machine or physical server with an agent installed.

To simplify the installation of agents on virtual machines, companies can include the agent software on the base virtual hard disk they use as a replica source for creating other virtual machines. Additionally, Microsoft's Systems Management Server can be used to distribute the agent across the network. This Microsoft product can be used to distribute all MSI-based programs to networked computers.

Restore

When any part of a production virtual machine fails, administrators need fast and simple recovery steps. Acronis delivers a number of options designed to get the production virtual machines up and running again. Several recovery options are available:

- For data and non-system partitions within a virtual machine, administrators can recover the partition in minutes using the installed Acronis software and pointing to the latest image file for that partition.
- For individual files within a virtual machine, Acronis provides selective file restore from any Acronis image.
- For system partitions within a virtual machine, administrators can restore the partition easily from the bootable Acronis Secure Zone (if one was created) or by using a bootable rescue CD or disk and then pointing to the latest image file.
- In the case of full system loss, administrators can restore the host operating system from an Acronis Secure Zone (if one was created) or by using the bootable rescue media, then restore each running virtual machine as outlined above.
- If you use the Acronis Recovery Manager, you can boot a system by selecting the F11 key – you don't necessarily need bootable media

In application-development and test environments, virtual machines make it fast and practical to test and re-test against different operating systems, applications, or settings. Companies may use virtual machines, for example, to confirm their migration or upgrade plans, to test new third-party software, or to test new versions of their own software.

Protecting virtual machines in a test environment presents different challenges than protecting production virtual machines. Although virtual machines used for testing scenarios don't contain user data, their creation still represents a significant investment of human time and effort. Instead of having a number of virtual machines running nonstop, as is common in production environments, test environments more typically have a large selection of virtual machines, of which only a small number (possibly none at all) are running at any given time. Since virtual machines used in the test environment can be stopped without incident and, it's most common to protect them from "outside" by backing up the small number of files that describe them, rather than backing them up from within the guest operating system (figure 4). As these files are likely to be stored locally on the virtual server machine, storing the backup image on a separate hard disk or network-accessible drive is often desirable.

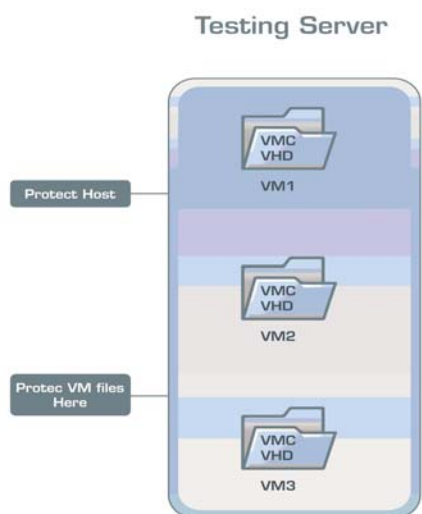


Figure 4: In a testing environment, virtual machine files can be protected from the host operating system.

When a virtual machine is not running -- and thus not accessing its virtual hard disk -- administrators can back up its files from the host operating system just like any other files. If testers can conveniently stop virtual machines, then the entire server can be protected with a single instance of the Acronis software running on the host operating system. If a test machine must remain up and running, for example, when performing a duration test, the backup techniques suitable for live production servers can be used instead. Either way, administrators can instruct Acronis True Image software to create full or incremental images on demand or on any desired schedule.

Restore During Testing

Human error in a test environment can easily erase or corrupt a virtual hard disk file. By protecting these files with Acronis, testbed configurations can be recovered in a few minutes instead of requiring tedious and error-prone reconstruction from scratch.

If virtual machine files or folders are lost during the testing process (perhaps as a result of human error), administrators can quickly recover these files. These files can be selectively restored from the latest Acronis image if desired -- a full image restore is not required. Also, if the entire host is lost, it can be restored to the same or another server in a matter of minutes. Acronis adds an important measure of protection that allows testers to quickly and confidently move forward with a large number of virtual machine configurations knowing that if something happens to a virtual machine, it can quickly be restored.

The Future of Virtualization

Virtualization provides major cost and management benefits for corporate data centers. With advances in 64-bit hardware and multi-processor servers and the accompanying increase in CPU power and RAM capacity, servers will increasingly be capable of supporting larger number of virtual machines. Additionally, virtualization is becoming an increasingly important aspect of the Windows Server System family of products, and Microsoft has announced its intentions to include virtualization technology within its next version of Windows Server.

Acronis technologies and products enable IT managers to provide these virtual machines with the same protection as physical servers, so they can rest assured their data, settings, applications, and operating systems are protected against disaster.

To find out more about Acronis True Image products:

Call +1 877 669-9749
E-mail sales@acronis.com

For OEM inquiries:
Call +1 650 875-7593
E-mail oem@acronis.com

Copyright © 2000–2005 Acronis, Inc. All rights reserved. “Acronis”, “Acronis Compute with Confidence”, “Secure Zone”, “Recovery Manager”, “Snap Restore” and the Acronis logo are trademarks of Acronis, Inc. Windows is a registered trademark of Microsoft Corp. Linux is a registered trademark of Linus Torvalds. All other names mentioned are trademarks, registered trademarks or service marks of their respective owners. Printed in USA.