

Agent vs Agentless Backup: Why it Matters

Agent-based backup is a proven technique for safeguarding physical servers.

Administrators appreciate its speed, consistency, and ease of administration when performing image-based backups for bare-metal server recovery or non-image-based backup for file recovery. But do these benefits transfer cost-effectively to virtualized environments? With multiple virtual machines (VMs) per server and mobile VMs that can migrate throughout a distributed environment, the costs of purchasing and managing a separate agent for each physical and virtual server can be prohibitive.

Agentless backup was created to retain the benefits of agent-based backup without the expense of per-server agents. Instead of installing a backup agent on each VM, the backup intelligence is centrally located and performs disk-to-disk backup from a single point of administration. Eliminating the need for individual agents in each VM clearly reduces costs and simplifies administration, but some administrators might question whether the capabilities of agentless solutions measure up to agent-based alternatives. Here are some important considerations when comparing agentless and agent-based solutions.

Agentless Backup

As virtualization proliferates throughout data centers, solutions that require an agent in every physical and virtual machine in the network become less cost-effective, more difficult to manage, and less able to provide the scalability and flexibility that agile businesses demand. While agentless backup is not truly agentless, it does require only one backup agent on one selected machine for network-wide backup. The single-agent, centralized control design offers many advantages for dynamic virtualized networks with large and changing numbers of VMs:

- **Lower Cost:** Lower cost is an important advantage of agentless backup. Without an individual agent on every VM in the network, administrators have fewer components to purchase and license, less communications to run, and lower CPU and bandwidth consumption. The need to acquire additional licenses or permissions from the software vendor as the network grows is also eliminated, which facilitates scalability and simplifies budget planning.

AGENT VERSUS AGENTLESS: FACTORS TO EVALUATE

Network Impact: The bandwidth and CPU overhead required to support an agent in every VM across the network is significant. Agentless approaches effectively eliminate this overhead.

Manageability: Centralized administration, policy-based management, and virtualization software with APIs for agentless backup make the agentless approach far easier to manage than agent-based solutions.

Investment Protection: Agentless solutions support almost all operating systems, databases, and email formats in use today, and do not require additional software or licenses as the network grows. Administrators have the financial freedom and technical flexibility to scale resources as needed.

Mixed Environments: To support mixed environments of physical and virtualized servers, administrators might elect to use both agent-based and agentless solutions. In this case, the solution should support agentless and agent-based backup from the same console, using the same file format.

- **Simplified Administration:** Agentless systems are typically implemented with a centralized management approach. The centralized approach provides a network-wide view that allows administrators to control every VM from a single point. Centralized administration eliminates the complex management scenarios that tend to result from multiple types of management software and the need to administer a separate agent on each VM. With agentless backup, the backup administrator designates network machines and data for backup, and the network-based agent transfers the designated data. Restores are equally straightforward.
- **Greater Control:** Agentless backup also lends itself to policy-based management, which helps administrators maintain greater control of backup and recovery operations with a lower time investment. Virtualization software with integrated support for agentless backup makes administration even easier. VMware® vSphere, for example, provides the vStorage API for Data Protection (VADP) for agentless backup, so no additional backup software installation is required.
- **Application Consistency:** Agentless backup implementations support snapshot technology, which makes a complete copy of a virtualized server or VM at a specific point in time. The ability to recover the snapshot allows applications to continue running without loss of data, ensuring the application consistency that is critical to business continuity. The snapshot data is not compressed for storage and can therefore be restored very quickly. Some vendors even support snapshots of data that is locked. Microsoft®, for example, provides this capability as a Windows service called the Volume Shadow Copy service.
- **Greater Flexibility:** Agentless backup architectures support almost all operating systems, databases, and email formats in use today.
- **LAN-Free Backup:** Agentless backup offers even greater efficiencies when implemented in environments that support LAN-free backup. A LAN-free backup scenario provides backup and recovery operations through the storage network rather than through the LAN. VMware vSphere provides this feature automatically through VADP. If a VMware virtual appliance (VA) is used, the VM snapshot can be mounted to the VA and data will be read directly from the snapshot as if it were a normal virtual disk. LAN-free backup can also be configured separately, but requires additional options and potentially complex configurations.

The advantages of agentless backup make it a very good solution for any business that wants to simplify data backup. For enterprises with large numbers of machines distributed over remote networks, these advantages become even more significant. And yet, agentless backup has some disadvantages that should be considered as well:

- **Requires a Fully-Virtualized Environment:** In networks with both physical and virtualized servers, administrators can only use agentless backup for the virtual machines. Physical machines still require agent-based backup.
- **Limited Snapshot Support:** Snapshot technology cannot be used for storage devices that are directly attached to a VM. In most cases, though, VMs use network-attached storage (NAS) instead of a direct connection to the storage device. NAS does support snapshot technology.
- **Limited Custom VM Code Execution:** Agentless backup also falls short in the area of executing custom code inside a VM. Some custom code, such as pre- and post-backup scripts and truncation of Exchange or SQL logs, cannot execute during agentless backup. Developers are working to overcome this shortcoming, but current solutions are limited.

For fully-virtualized environments, these disadvantages are minor when compared to the more costly and maintenance-intensive environment of an agent-based backup system.

Agent-Based Backup

In mixed environments of physical and virtualized servers, administrators must use some form of agent-based backup for the physical servers. In this scenario, administrators have the choice of non-image-based or image-based backup systems.

- **Non-Image-Based Backup:** Agent-based backup systems that are not image-based are designed to recover lost, deleted, or corrupted files. These systems can perform extremely granular file recovery with high performance, but cannot recover the systems on which those files run. Losing the system along with the files requires a lengthy rebuild and restore process that is not ideal for fast recovery.
- **Image-Based Backup:** Agent-based, image-based backup systems function by taking a snapshot of the entire server's drives or volumes. There is no need to reinstall the operating system and restore a patchwork of files to replicate the previous system, as is necessary with non-image-based systems. Even following a complete failure, restoring a full system image can often be accomplished in minutes. And, there is no possibility of missing critical files, as is the risk with file-level backup and restore processes.

Most of today's image-based backup systems also provide the same granular file restoration benefits as non-image-based systems. Image-based backup systems can even supplement full backup images with incremental backups, in which only those portions of the server that have changed since the previous backup are saved. Incremental backup requires much smaller backup sets and can offer more recovery points, reducing costs and supporting a fast recovery time objective (RTO). Features such as incremental backup have made image-based backup systems the standard for physical server disaster recovery.









Addressing the Reality of Mixed Environments

As data centers grow and supplement VM implementations with virtualized storage and networking, agentless backup systems will be by far the most cost-effective, scalable, and manageable solutions. But while the advantages of agentless solutions for virtualized environments are clear, many data center administrators continue to oversee mixed environments of physical and virtual servers that necessitate some use of agent-based solutions.

When considering mixed agent-based and agentless backup and recovery products, manageability implications are critical. Solutions should support agentless and agent-based backup from the same console, using the same file format. This capability gives administrators the flexibility to perform agentless backups and agent-based restores, or agent-based backups and agentless restores.

Acronis Backup and Acronis Backup Cloud solutions combine agentless and agent-based capabilities. For Hyper-V and VMware VMs, Acronis provides agentless backup and recovery of VMs running any guest operating system supported by those hypervisors. It may be easily deployed as a virtual appliance or on any server or PC running Windows, and supports file, folder, and system image backup and recovery.

While the agentless versus agent-based debate continues, practical solutions that provide efficient management of completely virtualized and mixed environments allow administrators to provide the best possible protection for their businesses today.

	Agentless backup	Agent-based (Agent for Windows/Linux)
Available for	VMware, Hyper-V, Virtuozzo (for Acronis Backup Cloud only)	VMware, Hyper-V, Citrix XenServer, RHEV, Virtuozzo, Oracle KVM
Installation	One Agent on Hyper-V host, One Agent on ESX(i) host or on a Windows machine outside of the vSphere environment	Agents on all virtual machines
What OS can be backed up?	Any operating system supported as guest by virtualization server.	Operating systems supported by Agent for Windows / Agent for Linux.
Back up selected files/folders inside virtual machine		
Back up to Online Storage		
Exclude files/folders from backup		
Recover backup to a virtual machine		
Recover backup directly to virtualization server	