CA ARCserve r16 vs. Veeam Backup & Replication 6.5

Product Review

Our quest to find the best backup/restore, disaster recovery, replication and business continuity product looks at the latest versions of CA ARCserve (r16) and Veeam Backup & Replication (v6.5).

Network TESTING LABS World Class Award

Executive Summary

Top honors in this review go to CA ARCserve r16. The more mature, more reliable and more feature-complete CA ARCserve gave us both file- and image-based backup, demonstrated faster performance, had better SRM reporting, exhibited far greater uptime and availability and cost less to operate. CA ARCserve r16 is our choice as the better answer for those organizations needing quality backup/restore, replication for offsite disaster recovery and maximum high availability for business continuity.

In a virtual-only environment, CA ARCserve and Veeam Backup & Replication each have strengths. However, in contrast to Veeam Backup & Replication, CA ARCserve works equally well in both virtual and non-virtual environments.

Our testing uncovered some significant limitations with Veeam Backup & Replication:

- It only does image-based backup
- It has no support for non-virtual environments
- It works only with two VMs (VMware ESX and, with fewer features, Microsoft Hyper-V)
- It has no true High Availability component
- Its reporting & backup/network visualization features rely completely on hypervisor metrics
- It's inextricably tied to the VM hypervisor (if the hypervisor has a software error, Veeam has a software error)

CA ARCserve r16 has again earned the Network Testing Labs World Class Award for best data protection and business continuity.

CA ARCserve r16 and Veeam Backup & Replication 6.5 both offer to protect and preserve your data using a variety of backup/restore approaches. Both have many features to tempt organizations needing to protect critical data from failures, disasters and human mistakes.

How do CA ARCserve r16 and Veeam Backup & Replication 6.5 measure up? Which is best suited to your particular computing environment?

Disclosure: Production of this report funded by CA, Inc.

We decided to look closely and in detail at the abilities and shortcomings of both CA ARCserve r16 and Veeam Backup & Replication 6.5. In this report, we compare and contrast the two products, feature by feature.

Veeam Backup & Replication is only intended for and only works within virtualized environments. CA ARCserve supports both physical and virtual environments. Accordingly, to be fair to Veeam, we've divided this review into two major sections.

The first review section explains how well the products work in a virtual environment, while the second discusses physical and hybrid environments.

CA ARCserve's components are CA ARCserve Backup (file-based), CA ARCserve D2D (image-based), CA ARCserve Replication (for disaster recovery) and CA ARCserve High Availability (for rapid system failover).

Veeam Backup & Replication 6.5's components include Veeam Backup & Replication, Veeam ONE (reports), Veeam Management Pack (Microsoft monitoring helper module) and Veeam Smart Plug-in (SPI) (HP monitoring helper module). Veeam also offers some no-charge, limited-function, promotional versions: Veeam Backup Free Edition, Veeam ONE Free Edition, Veeam Extended GRL and Veeam Stencils (for Visio).

CA ARCserve's new features are

Image-based Backup Enhancements

- **Integrated Access to Cloud Storage –** Integrated configuration of the cloud connection to Amazon Simple Storage Service (Amazon S3), Microsoft Windows Azure storage and Fujitsu Global Cloud Platform
- **Backup Throttling –** Optimizes the resources allocated to each backup
- **Granular Mailbox Recovery –** Restores individual Exchange emails, attachments, files and folders from a single-pass backup
- **Desktop/Laptop Protection –** Performs Infinite Incremental snapshot backups and bare-metal restores for your desktops and notebooks
- **Encryption –** Advanced Encryption Standard (AES)-128, AES-192 and AES-256 encryption for privacy and confidentiality
- **Windows Explorer Shell Integration –** Navigate and manipulate recovery points directly from within Windows Explorer
- **Auto Update –** Downloads and painlessly installs the latest ARCserve updates, hot fixes and service packs
- **Central Protection Manager –** Web-based console for viewing and managing all protected servers and clients has automated Active Directory discovery, remote deployment, simplified policy-based administration, Storage Resource Manager (SRM) reporting, status, grouping, search and restore, basic workflow and event

logging as well as centralized manual backups, job status reporting and monitoring across all protected machines

- **Central Reporting –** Centralized, detailed reporting, with a customizable dashboard, for all devices, settings and policies (local and remote)
- **Central Host-Based VM Backup –** Backs up all Windows-based VMs on a host in a single pass
- **Central Virtual Standby –** Transforms image-based backups into runnable VMware Virtual Machine Disk (VMDK) or Microsoft Virtual Hard Disk (VHD) virtual server format and automatically registers them with the appropriate hypervisor for immediate failover in the event a production server fails (includes a “heartbeat monitor” for automatic failover)
- **Higher Integration –** Add image-backup protected servers to the file-backup Manager catalog, migrate image-based recovery points to tape and retrieve those recovery points directly from tape, replicate recovery points offsite and retrieve the offsite data as if it were local
- **Pre-flight Check --** Tests and analyzes that the VMware environment is appropriately configured prior to running a backup and provides insight by suggesting changes to help ensure a successful backup
- **SQL Server 2012 Certification**

File-Based Backup Enhancements

- **Archive Manager –** Identify and migrate data that meets specific archiving policies to less expensive storage to reduce storage costs while addressing compliance requirements
- **Integrated Cloud Storage –** Configure and use cloud storage for offsite data protection, archiving and system availability for business continuity and disaster recovery
- **Snapshot and File-level Integration –** Use combinations of image backups and file backups to restore specific data
- **Synthetic Full Backup Improvements –** Use computing resources frugally yet transparently to store incremental backups
- **Backup Images to Tape –** Copy disaster recovery disk images to tape for secondary storage
- **WinPE (Windows Preinstallation Option)-compliant Disaster Recovery –** Use Microsoft’s WinPE technology to drive bare-metal restore operations
- **Improved Tape Management –** Maximize and consolidate both disk and tape storage to lessen computing resource usage
- **SaaS Data Protection –** Image-based backup, restore and system recovery and comes bundled and integrated with Microsoft Windows Azure cloud storage

Replication and High Availability Enhancements

- **Full System Protection and BMR –** Replicates a complete physical or virtual Windows system (operating system, system state, applications and data) to an offline physical or virtual server via non-disruptive reverse synchronization from a Replica Server, monitors the system and application, and offers automatic and push-button failover for high availability, including hardware-independent BMR recovery and non-disruptive failback to restore the original production server – with no business downtime
- **Amazon Cloud (Amazon Web Services [AWS] and Amazon Elastic Compute Cloud [Amazon EC2]) Integration –** Use Amazon's data center resources to have a cloud-based Replica server
- **Windows Server 2008 Failover Cluster Support –** Complements a Windows Server failover cluster with data replication to any local or remote site; integrated with Microsoft System Center Operations Manager
- **Secure Communication –** 128-bit Secure Sockets Layer (SSL) encryption (no virtual private network (VPN) or IPSec tunnel necessary)
- **VMware vCenter Server v4 Support –** Replication and failover for the VMware management system
- **Network Address Translation (NAT) Support –** Allows continuous, scheduled remote replication in NAT environments through a firewall – no VPN needed
- **Recovery Point Synthesis --** Create backup sets containing all recovery points for a specified time period

The new features in Veeam Backup & Replication v6.1/v6.5 are:

- **VeeamZIP –** Version 6.1 includes a new capability for performing ad-hoc backups that functions like a zip utility for VMs
- **New console –** Uses Microsoft design standards to show only relevant management tree nodes, enable quick searching and leave vacant screen space for future enhancements
- **vPower for Hyper-V –** Can run a VM directly from a compressed and deduplicated backup file on regular backup storage
- **Intelligent load balancing –** For better backup proxy server selection, better subnet detection, recognizing excluded disks and new recognition of transformation tasks
- **Data mover agent priority –** Starts the data mover agent with BELOW NORMAL priority
- **System cache tuning –** Adjusts the low-level Windows system cache settings
- **Concurrent job limit –** The previous limit of 64 backup jobs has been removed
- **Memory consumption –** Memory consumption by the job manager process has been reduced

- **Backup proxy server replication –** The backup proxy server can now replicate itself
- **Deleted VM retention period –** No longer affects incremental backups
- **Shared backup proxy servers and repositories –** Workload balancing enhancements
- **Bottleneck analysis –** Better calculation of proxy and network processing statistics
- **Disable inline deduplication –** Now disables both target and client
- **Email notifications –** Default email notification subject redesigned
- **Backup job mapping –** Can now map a backup job to a backup created by a different v6 backup server
- **Support for rotating backup storage –** Setting the ForceCreateMissingVBK registry key creates a new full backup if previous backup files are missing
- **Omit replica suffix –** You can now configure the replica suffix to be empty
- **Edit source VM hardware –** Change VM hardware settings (such as adding a new vNIC) without having to restart the replication cycle
- **Continue replication after failback –** You can now resume replication after failback without having to replicate the full VM
- **Retrieval of VM configuration –** VM configuration files are now retrieved by the source backup proxy server, not the target
- **Overwrite existing VM files –** A VM copy job now overwrites existing VM files instead of creating a new VM copy
- **Importing backups –** You can now import backups from password-protected file servers
- **Preserve source files –** New option enables preservation of source VM files after a successful migration
- **1-Click File Restore –** Added support for restoring very large files. (Enterprise Edition only)
- **Support for ReFS volumes –** Added support for indexing ReFS volumes
- **Integration with Windows Explorer –** Can view file contents or initiate a restore from within Explorer
- **24-hour job history –** Can now see the results of all job runs in the last 24 hours
- **Delete default backup repository –** You can now delete the default backup repository
- **Synthetic full and transform progress indicators –** Can now watch the running of synthetic full and transform operations in the job grid
- **Datastore view –** Added datastore view to the virtual machine selection dialog (Enterprise Edition only)
- **Hot add (VMware only) –** Hot add performed only once for a multiple-disk VM rather than for each processed disk
- **vPower NFS (VMware only) –** Removed unnecessary logging

- **SCVMM 2012 (Hyper-V only) –** Added support for System Center 2012 Virtual Machine Manager
- **Localized servers (Hyper-V only) –** Added support for localized servers
- **VMs on backup server host (Hyper-V only) –** You can now protect VMs running on a Hyper-V host on which the Veeam backup server is installed in the parent partition
- **Changed block tracking (Hyper-V only)** – Added compatibility with some third party applications that had adversely affected changed block tracking
- **Logging –** Added current backup log compression when the size exceeds the threshold
- **Microsoft Exchange –** Exploration and recovery of elements
- **VM recovery –** from HP StoreVirtual VSA and LeftHand SAN snapshots
- **Veeam Management Suite –** Monitoring, reporting and capacity planning
- **Hypervisor support –** VMware vSphere 5.1 and Windows Server 2012 Hyper-V

The categories we used in this evaluation are:

- ❖ Image-based backup features
- ❖ File-based backup features
- ❖ Replication/high availability features

Because Veeam Backup & Replication only functions within a purely virtual environment (and then only for virtual servers), we first evaluated it and CA ARCserve using VMware ESX and vSphere, Microsoft Hyper-V, Citrix XenServer and Redhat KVM.

Next, we tested CA ARCserve in both physical and hybrid physical/virtual environments.

We also discuss pricing and usability.

For each feature, we rank the products and we explain the rankings when they're dissimilar.

The first feature chart reveals how well CA ARCserve and Veeam Backup & Replication fare in producing – and recovering from – image-based backups in a virtual environment.

Virtual Server/VM Image-based Backup

An image-based full system backup contains everything about a computer at the moment the backup copy was made – the operating system, the system's current state and the data file disk blocks. The backed up image can later be restored (termed a Bare Metal Restore operation, or BMR) either to the same computer or to another computer of different brand and type. Additionally, image-based backup products offer granular recovery at the application and file level for faster recovery.

Virtual Server/VM Image-based Backup Features Comparison Table

(Scoring from 0 to 5, with 5 the highest)

Feature	Veeam Backup & Replication V6.5	CA ARCserve r16
Snapshot/image backup technology	5	5
Operating System/VM support	4	4
Device support	3	5
Server support	5	5
Client/Workstation support	0	5
Cloud capabilities and support	1	4
RTO/RPO (for disaster recovery)	4	4
Granular recovery	5	4
Off-site replication of images	4	3
Bare Metal Recovery (BMR)	0	5
Deduplication	4	0
Virtual standby for cold-failover	3	5
Image archiving, retention and versioning	4	5
Centralized management	4	4
Centralized reporting	4	4
Image-based backup features aggregate ranking	**3.3**	**4.1**

Virtual Server/VM Image-based Backup Notes

Technology –Both CA ARCserve and Veeam Backup & Replication offer synthetic backups, in which a full backup is assembled, or synthesized, from a baseline full backup and subsequent incremental backups.

CA ARCserve's image-based backup is built on its patent-pending ***Infinite Incremental (I^2 Technology)***. With *I^2*, users can do a full backup initially and then only perform incremental backups from that point forward. This technology leverages Windows VSS and has been designed to intelligently manage the backup of only blocks of data that have changed since the last backup and present a consolidated point-in-time view of the protected volume for multiple recovery types, thus reducing your recovery time. Veeam's synthetic backups use Veeam's proprietary virtual machine changed-block driver to detect data blocks needing backup.

CA ARCserve r16 and Veeam Backup & Replication can each create snapshots as often as every 15 minutes.

While CA ARCserve's backup targets can be just about any device, Veeam Backup & Replication backup targets must be:

- Direct Attached Storage (DAS) connected to the backup repository server
- Network Attached Storage (NAS) able to present itself as CIFS (SMB) or NFS share
- Storage Area Network (SAN), provided the backup repository server is connected directly to the SAN fabric via hardware HBA or software iSCSI initiator and the corresponding volumes are seen by Microsoft Windows Disk Management

In contrast to CA ARCserve, Veeam Backup & Replication has no file copy (D2D2D) capability. On the other hand, Veeam offers inline data deduplication at no extra charge. CA ARCserve's image-based component does not offer data deduplication.

Operating Systems; BMR – Veeam supports Linux as well as Windows, but CA ARCserve supports only Windows. However, CA ARCserve can restore Windows images onto similar or dissimilar hardware through their BMR, but Veeam cannot. To its credit, Veeam's Backup & Replication does have a virtual-only "Instant Recovery" feature (described below).

Server and Client Support –CA ARCserve protects both virtual servers and Windows workstations (clients). Veeam Backup & Replication works only with virtual servers.

Cloud Support – CA ARCserve writes initial snapshot (backup) to disk. A subsequent step copies the snapshot data to a cloud. CA ARCserve's image-based backup works with Amazon Web Services as well as Microsoft Windows Azure and Eucalyptus to store secondary or tertiary image backups. After the first image copy to the cloud, CA ARCserve transmits only incremental changes (via **I^2**) from that point forward. This makes the best use of low-speed cloud connections. Also, unlike Veeam Backup & Replication, CA ARCserve offers a SaaS subscription service with integrated Windows Azure cloud storage.

Veeam Backup & Replication's cloud support is indirect and fairly limited, available through the cloud reseller TwinStrata.

Performance and Media Usage – CA ARCserve's I^2 is faster than Veeam Backup & Replication's synthetic full backup process, and I^2 uses slightly less storage space. For a single-server system comprising 300 GB, Figure 1 shows the relative performance of CA ARCserve r16 I^2 and Veeam Backup & Replication v6.5.

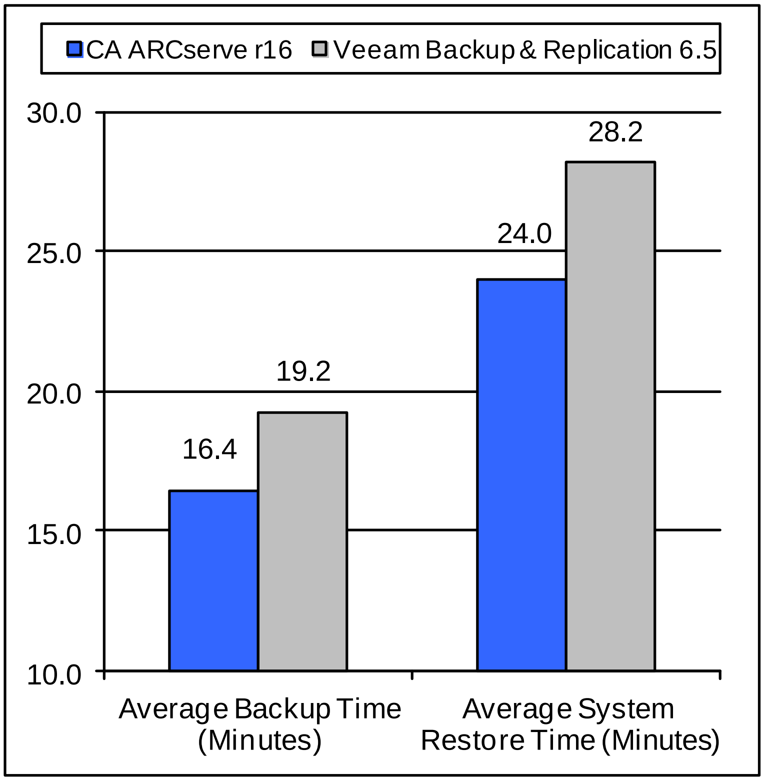

Figure 1.

CA ARCserve I^2 vs. Veeam Backup & Replication image-based backup/restore performance (no deduplication)

Testing both CA ARCserve and Veeam Backup & Replication infinite incrementals (one full backup at the outset and incremental backups thereafter), we saw that CA ARCserve's I^2 needed 8% less storage space than Veeam Backup & Replication (161 GB vs. 183 GB) when we tested the creation of daily, weekly and monthly backups over a three-month time span. Figure 3 depicts the resulting storage requirements.

In an effort to reduce Veeam Backup & Replication's storage space consumption, we enabled the product's data deduplication feature. Unfortunately, because Veeam's data deduplication is extremely CPU-intensive, backup and recovery times unacceptably nearly doubled with the option turned on. Figure 2 graphically shows the relative performance of the two products.

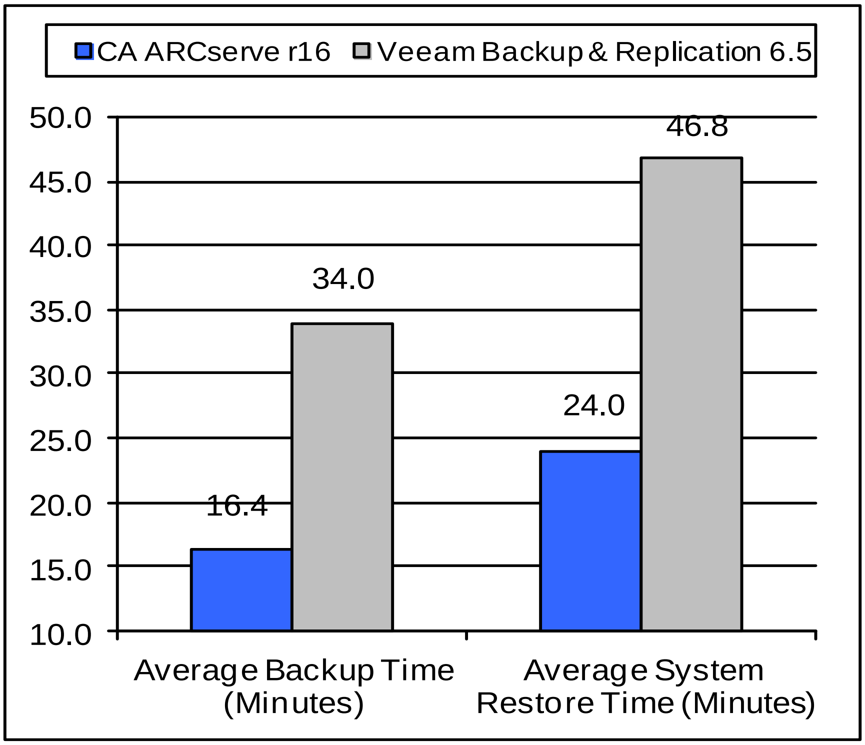

Figure 2.

CA ARCserve I^2 vs. Veeam Backup & Replication image-based backup/restore performance, with Veeam's deduplication feature enabled

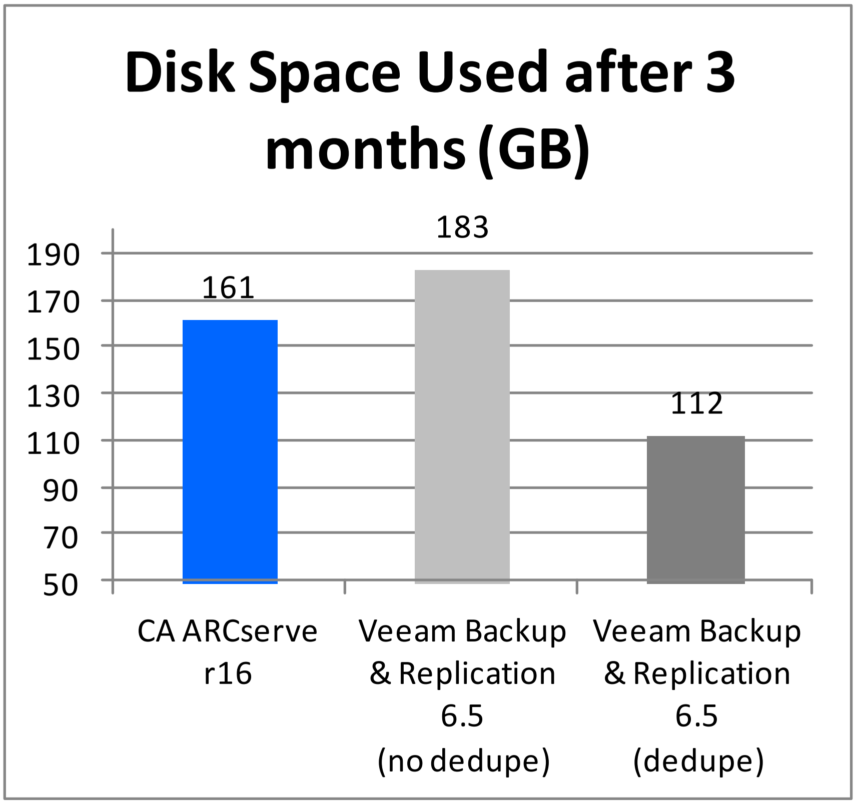

Figure 3.

CA ARCserve I^2 vs. Veeam Backup & Replication image-based disk storage utilization

Virtualization Support -- CA ARCserve supports more virtualization platforms than Veeam Backup & Replication, including VMware ESX and vSphere, Microsoft Hyper-V, Citrix XenServer and Redhat KVM. Until recently, Veeam Backup & Replication only supported VMware but now supports VMware ESX/vSphere (including V5.1) and Microsoft Hyper-V (including Windows Server 2012 Hyper-V).

Note that Veeam Backup & Replication does not fully support Hyper-V. Missing features for Hyper-V are application object recovery (such as an Exchange mailbox), verification of recovery point integrity and Veeam Explorer for SAN Snapshots.

CA ARCserve protects the entire Hyper-V hypervisor host, while Veeam Backup & Replication does not. CA ARCserve can thus recover an entire virtual host, as a single entity.

Virtual Standby – CA ARCserve offers Virtual Standby, a feature wherein up-to-date copies of backup images (recovery points) are available for immediate use in case of a system outage, thus offering near-instantaneous system recovery. CA ARCserve's Virtual Standby feature automatically converts recovery points into VMDK and VHD formats and automatically registers with the hypervisor. It offers automated and manual failover. Furthermore, CA ARCserve's virtual standby works in either physical-to-virtual (P2V) or virtual-to-virtual (V2V) failover modes.

Veeam Backup & Replication lacks an automated virtual standby feature. It does have, however, "***vPower***," which consists of essentially two capabilities: (1) Publishing a backup as a VMDK file and (2) running a VM directly from a backup, without having to first restore the VM (this is Veeam's "***Instant Recovery***"). Veeam Backup & Replication can perform a VM recovery from HP StoreVirtual VSA and LeftHand SAN devices.

RTO/RPO Performance Testing – To measure CA ARCserve's and Veeam Backup & Replication's Recovery Time Objective (RTO) and Recovery Point Objective (RPO) performance, we simulated the destruction of four Windows Server computers containing a total of 300 GB in a small data center. One of these computers ran SQL Server 2005, one ran Internet Information Server (IIS), one ran an OLTP business application and the fourth was the backup server. All the computers ran VMware ESX.

Both CA ARCserve and Veeam Backup & Replication took snapshots every fifteen minutes and transferred backups to a remote location. Four computers at the remote location stood by, waiting to go to work in case of a disaster. We measured the minutes needed to recover data and resume operations.

Using CA ARCserve image-based backup in one test and Veeam Backup & Replication in another test, an administrator at the remote location restored the transferred data onto the waiting secondary servers. The test concluded when the administrator had restored all servers and had brought the OLTP application back online.

The CA ARCserve administrator needed just 49 minutes to restore data to the (virtual machine) servers and resume the OLTP application. The Veeam Backup & Replication administrator needed slightly less time (48 minutes) to accomplish the same thing.

Note that the testing depicted earlier in Figures 1 and 2 occurred on a single computer, while our RTP/RPO testing used two sets of four computers. Also, the earlier charts show only the time to complete a backup job. They do not include times for such other disaster recovery tasks as restarting applications.

Central Management – Working with disk images is easy and painless with CA ARCserve's Web 2.0-based management console, but replication of image backups is managed separately using the replication component's user interface. Veeam's user interface spans both backup and replication and, although less responsive and intuitive than CA's, is also a point-and-click affair.

Central Reporting –CA ARCserve's Central Reporting produces much more useful and informative reports regarding disk image recovery points than does Veeam Backup & Replication, but reporting for replication jobs is managed separately using the replication component user interface. Veeam reporting spans both backup and replication. Both products integrate with Windows Explorer to show the contents of an image file as a mountable drive letter. Veeam Backup & Replication, like CA ARCserve, displays a useful dashboard of backup job status information. Both Veeam Backup & Replication and CA ARCserve offer reports for backup job monitoring and capacity planning.

CA ARCserve's image-based backup component offers far better management and reporting than Veeam Backup & Replication, but Veeam Backup & Replication does offer a single user interface through which to manage both backup and replication. CA ARCserve's image backup and replication components are separately managed. It should be noted that CA ARCserve's file-based backup and replication/high availability components do share a common interface.

Granular Recovery – Uniquely, Veeam Backup & Replication can restore nearly any object or sub-object within a virtual environment to a "sandbox" environment. While CA ARCserve can recover entire SQL Server databases or other file-level objects, its finer granularity is limited to Microsoft Exchange databases – mailboxes, e-mail notes and attachments. In contrast, Veeam Backup and Replication can even restore individual SQL Server tables.

To use Veeam Backup & Replication's granular recovery, an administrator first chooses the desired restore point and starts the target application on a special recovery VM (the "sandbox"). Once the object is recovered in the sandbox, the administrator can then copy application objects to the production VM instance. The administrator uses a Windows Explorer-like interface to retrieve specific Microsoft Exchange elements from a Veeam Backup & Replication backup set.

However, see our note, below, regarding the restoration of individual SQL Server tables.

NOTE: Restoring SQL Server Tables Can Be Risky

Suppose you add customer ABC to the SQL Server database on Monday. ABC becomes a new row in the Customer Table. On Tuesday, customer ABC places order #111, which becomes a new row in the Order Table. On Wednesday, customer ABC places order #222, which also becomes a new row in the Order Table. On Thursday, a sysadmin restores the Order Table to late Tuesday (or early Wednesday).

You then have database errors/omissions/inconsistencies.

The scenario in which you delete customer ABC and his orders but then restore the Order Table to a point in time at which ABC's orders still existed is even worse. You then have no Customer Table entry for ABC, but you have ABC's orders in the Order Table. (How would you feel if your bank were able to restore individual tables relating to your bank account balances?)

Practically speaking, you never want to be able to restore only part of a SQL Server database. It's far too risky.

Not all IT organizations use image-based backup technology and many still rely on file-based backup, especially if they want to use a direct-to-tape backup strategy. In the next section, we had planned to compare CA ARCserve r16 and Veeam Backup & Replication file-based backup and restore capabilities in a virtual environment, but Veeam does not offer file-based backup, only image-based backup. Therefore Veeam did not achieve any scores in this section.

Virtual Server/VM File-based Backup

A file-based backup contains copies of applications and data files you designate, file by file and directory by directory. The backup process automatically and regularly creates the latest backup copy onto whatever media you specify – tape, disk, USB memory or other device. You can archive older backup copies offsite, for safekeeping. Restoring the data copies it back to the source machine or other computer that typically already has an operating system installed on it. However, most file-based backup products also offer some type of bare metal restore (BMR) for system recovery.

Virtual Server/VM File-based Backup Features Comparison Table

(Scoring from 0 to 5, with 5 the highest)

Feature	Veeam Backup & Replication V6.5	CA ARCserve r16
Tape device support	0	5
Application support	0	5
Tape integration	0	5
Tape archiving, retention and versioning	0	5
Virtual machine protection	0	5
Application-specific granular recovery	0	5
SRM reporting	0	5
Basic backup reporting	0	5
Infrastructure visualization	0	5
Central management	0	4
Deduplication	0	4
Public and private cloud support	0	4
File archiving	0	5
Integration with image-based backups	0	5
Synthetic full backups	0	5
File-based backup features aggregate ranking	**0.0**	**4.8**

Virtual Server/VM File-based Backup Notes

CA ARCserve r16 has a wealth of file-based backup features. Moreover, it's fast, reliable and frugal in its use of storage space, offering built-in data deduplication at no additional cost. Because it's integrated with CA ARCserve's image-based backup/recovery component, you can migrate image-based backups to tape for archive and compliance purposes.

CA ARCserve supports a myriad of operating systems, applications and backup devices, including tape and Virtual Tape Library (VTL). CA ARCserve has superior reporting, its infrastructure visualization feature is unequalled and its central management console is responsive and intuitive.

CA ARCserve Central Reporting provides global views, administration and reporting on all devices, settings and policies (running on-premise and off-premise) protected by CA ARCserve. It gives both detailed reports and a summary Dashboard report view that clearly show the overall status as well as individual details for any and all backup operations.

CA ARCserve's topology map clearly and intuitively displays a customer's infrastructure. By node, virtual machine or device, CA ARCserve graphically presents a hierarchical picture of data backup sets. CA ARCserve's SRM reporting is revealing, comprehensive and helpful. A person can monitor the status of any and all backup operations, identify long-running backup operations, locate backed up data, discover whether data is encrypted, know the company's disaster recovery status and track volume, disk and memory usage on each server.

In the last features table, let's examine the huge differences between CA ARCserve and Veeam Backup & Replication in the areas of replication and high availability.

Virtual Server/VM Replication and High Availability

The Replication process continuously copies changes made to one (master) computer's files to a secondary (replica) computer. The replica computer is always an exact copy of the master (provided that all byte-level changes made on the master computer are successfully transmitted across the LAN or WAN to the replica).

High Availability manages the relationship between the master and replica computers in a way that makes the replica computer almost instantly assume the role of master if the master computer suffers a problem. Users are automatically redirected to the replica as part of the failover process. The result is a file, application or database server that's virtually always available.

Multiple master and replica computers are possible, and Replication can be configured for one-to-one, many-to-one and one-to-many scenarios.

Virtual Server/VM Replication and High Availability Features Comparison Table

(Scoring from 0 to 5, with 5 the highest)

Feature	Veeam Backup & Replication V 6.5	CA ARCserve r16
Replication	4	5
True high availability (hot failover)	1	5
Server support	5	5
Operating System and application support	5	5
RTO/RPO (for disaster recovery)	2	5
Cloud Integration	2	3
Continuous Data Protection (CDP)	2	4
Offline synchronization	5	5
Replication and HA recovery testing	2	5
Network optimization	5	5
Replication and backup integration	5	4
Assessment mode utility	2	5
Application aware replication	5	5
Replication and high availability features aggregate ranking	**3.5**	**4.7**

Virtual Server/VM Replication and High Availability Notes

CA ARCserve's replication component may be used in a scheduled manner to migrate backups offsite and in a real-time, continuous manner. CA ARCserve provides true continuous data protection to complement periodic backups of critical data.

For companies needing maximum system uptime and availability, CA ARCserve has a High Availability (HA) component. Veeam has a replication feature but does not offer high availability.

Both CA ARCserve's and Veeam Backup & Replication's replication components perform asynchronous replication and support Windows, Linux and UNIX environments. They may be deployed onsite, offsite and/or linked to a cloud. Basically, CA ARCserve's and Veeam Backup & Replication's replication features clone each I/O operation and send the cloned copy to a secondary destination of your choice.

Uniquely, CA ARCserve can replicate between physical and virtual servers (P2P, P2V and even V2P). CA ARCserve can also replicate between virtual server platforms (V2V).

Veeam Backup & Replication can replicate only between virtual servers (V2V).

CA ARCserve's HA component includes all the functions of the replication component and adds the ability to monitor one or more background services running on a server. If a service fails, CA ARCserve will attempt to restart it. If the restart fails, the system can be set to automatically fail over to the replica (or failover) server. Alternately, the administrator can set the system to not automatically failover, thus allowing the administrator to investigate the problem. The administrator can then choose to use push-button failover if he or she deems it necessary. Veeam Backup & Replication lacks all these features.

Veeam Backup & Replication's replication feature lacks true high availability and delivers only "Near CDP:"

- Veeam's Instant Recovery technology is slower, because it requires manual intervention on the part of an administrator when a data disaster occurs
- Instant Recovery is an incomplete, poor substitute for high availability, because it doesn't have the system monitoring, service-level restart and automated failover capabilities of CA ARCserve's HA component

Veeam's Instant Recovery, which is somewhat similar to CA ARCserve's image-based Virtual Standby, is used to manually start a VM at a remote location.

With Veeam Backup & Replication, you still run the risk of significant outages and stoppages in the running of your business when you need to recover data and start up replacement servers.

CA ARCserve can monitor a single server, group of servers, entire server farm or specific applications, such as Microsoft Exchange, SQL Server, SharePoint, IIS and Dynamics CRM, thus ensuring maximum availability. When a hardware or application failure occurs, CA ARCserve automatically activates the replica server(s). It gives the replica servers IP addresses and host names during activation to make failover transparent to end users, many of whom will never even know an outage occurred. Again, Veeam Backup & Replication lacks these abilities.

CA ARCserve's HA component is perfect for distributed applications like Microsoft SharePoint and Dynamics CRM, which typically have a multi-tier architecture consisting of separate Web, application and database servers. CA ARCserve replicates, monitors and fails over all the servers, not just the database server. And with group management, all component servers can be failed over even if only one fails. This is especially useful when the replica servers are kept at a distant remote location. CA ARCserve offers sophisticated push-button failover and failback for the highest possible level of automated availability. Veeam Backup & Replication's replication feature requires that an administrator manually start the application(s) that will access the replicated data.

CA ARCserve comes with many pre-built replication and high availability scenarios. Furthermore, it provides application-aware replication and failover for Exchange, SQL Server, SharePoint, and IIS, as well as Oracle and Blackberry. In other words, CA ARCserve already knows what specific directories and files to replicate and when – you just indicate which applications to protect. Furthermore, the CA ARCserve high availability component supports virtually all third party or in-house-developed Windows-based applications – administrators can easily create custom scenarios that specify which application services to monitor.

While both CA ARCserve and Veeam Backup & Replication support virtual computing environments, CA ARCserve's HA component goes much further than Veeam Backup & Replication. CA ARCserve offers high availability for VMware vSphere, Microsoft Hyper-V and Citrix XenServer. Veeam Backup & Replication can perform replication in a VMware or Hyper-V environment, but it does not have high availability support for any of these virtual platforms.

CA ARCserve has high availability support for Windows server clusters. Veeam Backup & Replication can replicate data onto clustered Windows servers, but an administrator must activate the secondary servers within the cluster to complete/finish a failover operation.

CA ARCserve's Replication and High Availability components include an easy-to-use assessment mode tool for performing "what if" dry runs to assure you have adequate bandwidth for replication. CA ARCserve also offers an Assured Recovery testing feature you can use to perform scheduled or ad-hoc recovery testing at the hardware, application and data levels on the replica server, without affecting the production server or impacting the continuous data protection and monitoring. Veeam Backup & Replication's SureBackup feature can verify the integrity of recovery points, but only for VMware, not Hyper-V.

Simply put, Veeam Backup & Replication lacks CA ARCserve's feature-rich, mature ability to replicate, monitor and automatically fail over critical servers.

When we measured RTO/RPO by performing the same disaster recovery test with CA ARCserve's High Availability component that we'd done with CA ARCserve's image-based feature (*see RTO/RPO section above under Image-based Backup), **CA ARCserve needed just six seconds to automatically restart the OLTP application** at the remote backup site. **Veeam Backup & Replication's replication feature required the same 48 minutes** as in the previous (image-based) test to recover from the simulated disaster. Veeam Backup & Replication's slower RTO/RPO was primarily a result of the administrator having to perform many manual tasks in order to make the application available from the remote site.

Physical Server Image Backup, File Backup and Replication and High Availability

If you have a hybrid physical/virtual environment, Veeam Backup & Replication forces you to license two different vendor's backup and recovery products – one physical, the other virtual. The two-vendor approach doesn't make sense because it's more expensive and less productive. Veeam Backup & Replication's "Total Cost of Ownership" (TCO) is always going to be higher than if you'd licensed your backup/recovery from a single vendor.

CA ARCserve is a single answer for IT organizations that need both physical server and virtual server backup and recovery. It offers image- and file-based backup, replication and true high availability for both physical and virtual environments. And CA ARCserve can also backup Windows-based clients (workstations).

Veeam Backup & Replication only supports virtual servers (and then only VMware and Hyper-V). Moreover, Veeam Backup & Replication is purely image-based.

Notably, CA ARCserve's Virtual Standby feature can convert backups from both physical and virtual servers to VMs for near instantaneous recovery. Veeam Backup & Replication's server-to-server data exchanges, even for its *Instant Recovery* feature, must occur strictly within a virtual environment.

CA ARCserve's BMR can easily recover an entire Windows machine (server or client), including hidden Registry files and system status information, thus putting a computer quickly back to work even after a hard drive failure. Furthermore, CA ARCserve's BMR can restore data from physical and virtual servers onto dissimilar hardware (P2P, P2V, V2P and V2V). Veeam Backup & Replication operates only in the virtual world and cannot perform BMR.

Because it spans physical and virtual environments, CA ARCserve offers both physical-to-virtual and virtual-to-physical replication and high availability. Veeam Backup & Replication lacks this capability. Impressively, CA ARCserve's image-based backup and high availability components can also be used to quickly and easily perform physical-to-virtual migrations. Veeam Backup & Replication lacks this capability, too.

CA ARCserve's support for both physical and virtual environments extends into the cloud – including physical-to-cloud backup migration, replication and high availability. Again, Veeam Backup & Replication lacks these features.

Ease of Use and Pricing

CA ARCserve's well-formatted and configurable dashboard reveals, at a glance, the current status of your backups. Veeam Backup & Replication also shows a configurable dashboard display of backup/restore status information. However, with Veeam Backup & Replication, visualizing backup status requires several more navigations steps. If you have multiple site backups, both CA ARCserve and Veeam Backup & Replication consolidate and centralize backup status information from all sites.

Data visibility is crucial to data backup reliability. With a single click, CA ARCserve displays a clear and highly descriptive graphical view of backup sets and backed up data. Veeam Backup & Recovery uses Microsoft design standards and Microsoft user interface guidelines to present a tree view of backup sets and objects.

Navigating Veeam Backup & Replication's backup job reports, we found, is time-consuming and tedious.

CA ARCserve's image-based backup component has a Web 2.0 interface that provides real-time access to the latest documentation updates, invaluable technical data, helpful tips and online user communities. Impressively, CA ARCserve's Web 2.0 interface even gives customers virtually direct access to the CA ARCserve development staff – and they actually listen to customer suggestions and ideas. Veeam Backup & Replication's user interface, which is not intuitive and which requires much more user input to accomplish the same tasks, pales in comparison.

CA ARCserve's Web 2.0 interface has meaningful icons, a grasp-at-first-glance view of network objects and pop-up windows for object-specific tasks. It strategically uses multi-level drop-down menus and tabs to organize tasks in a way that aligns perfectly with a network administrator's workflow. Every backup and restore operation is within easy reach of just a few mouse clicks.

CA ARCserve makes extensive use of the Ajax (***Asynchronous JavaScript and XML***) multipurpose browser-based framework of tools, widgets, controls and methods. CA ARCserve's interface offers a rich set of widgets that resemble elements of native desktop applications. For example, it has built-in support for keyboard navigation, focus and tab handling and drag & drop.

CA ARCserve's Web 2.0 interface gave us the ability to remotely access all our protected servers, change configuration settings, check the status of our backups and restores, initiate backup jobs and launch remote recoveries – all via the Internet.

For virtual server environments, CA ARCserve's RPO socket-based pricing (which includes file- and image-based backup, file replication and one year of maintenance) is less expensive than Veeam Backup & Replication. CA ARCserve's RPO-RTO socket pricing is slightly higher, but it adds full application and data replication along with true high availability. Note that CA ARCserve offers component-, server- and capacity-based pricing, too. Also note that Veeam Backup & Replication only supports virtual server environments.

Veeam Backup & Replication Pricing

Standard Edition MSRP	$699 per socket
One year of regular maintenance (1-6 cores)	$128 per socket
One year of premium maintenance (1-6 cores)	$203 per socket
One year of regular maintenance (7-12 cores)	$192 per socket
One year of premium maintenance (7-12 cores)	$305 per socket
Enterprise Edition MSRP	$1,099 per socket
One year of regular maintenance (1-6 cores)	$200 per socket
One year of premium maintenance (1-6 cores)	$320 per socket
One year of regular maintenance (7-12 cores)	$300 per socket
One year of premium maintenance (7-12 cores)	$478 per socket

CA ARCserve r16 Pricing

	MSRP
CA ARCserve Backup for Windows	$818.40/server
CA ARCserve D2D for Windows Server Standard Edition	$732.00/server
CA ARCserve Replication for Windows Standard OS with Assured Recovery	$1,600.50/server
CA ARCserve High Availability for Windows Standard OS with Assured Recovery	$3,250.50/server
CA ARCserve Backup for Windows Essentials File Server Module with D2D and Replication	$2,005.20/server
CA ARCserve Backup for Windows Standard Database Module with D2D and Replication	$2,610.00/server
CA ARCserve Backup Advanced Email Module with D2D and Replication	$2,730.00/server
CA ARCserve Backup for Windows Enterprise Application Module with D2D and Replication	$3,228.00/server
RPO Managed Capacity: Recover your data in minutes CA ARCserve Backup + CA ARCserve D2D Advanced Server + Central Applications + file-only CA ARCserve Replication	$9,540/Terabyte
RTO Managed Capacity: Recover applications in seconds CA ARCserve Backup + CA ARCserve D2D + Central Applications + CA ARCserve Replication + CA ARCserve High Availability	$16,740/Terabyte
Virtual Environment RPO Per Socket Solution: Recover your data in minutes CA ARCserve Backup + CA ARCserve D2D Advanced Server + Central Applications + file-only CA ARCserve Replication	$795/socket (unlimited cores)
Virtual Environment RPO-RTO Per Socket Solution: Recover applications in seconds CA ARCserve Backup + CA ARCserve D2D +Central Applications + CA ARCserve Replication + CA ARCserve High Availability	$1,995/socket (unlimited cores)

* All CA ARCserve pricing includes 1 year of Enterprise support/maintenance

Rankings Summary – Virtual Server Environment

	Veeam Backup & Replication 6.5	**CA ARCserve r16**
Image-based backup	3.3	4.1
File-based backup	0.0	4.8
Replication, High Availability	3.5	4.7
Usability	4.0	4.5
Total score	**2.7**	**4.5**

Conclusion

We've shown that even in a virtual-only environment – if such an animal exists – CA ARCserve and Veeam Backup & Replication each have strengths. However, in complete contrast to Veeam Backup & Replication, CA ARCserve is equally at home in both physical and virtual environments.

CA ARCserve is an integrated, reliable, easy-to-use and scalable answer when disaster happens. CA ARCserve offers both comprehensive file-based and image-based backup, offers much better SRM reporting and provides far greater uptime and availability with its virtual standby and high availability capabilities. Moreover, in many cases, CA ARCserve r16 costs less than Veeam Backup & Replication 6.5.

We recommend CA ARCserve without reservation. In fact, we use it in our own shop.

Vendor Contacts

CA 800-225-5224	www.arcserve.com
Veeam 678-353-2140	www.veeam.com

Testbed and Methodology

Virtually all our testing took place across 512 kb/s frame relay, T1 and T3 WAN links. The testbed network consisted of six Fast Ethernet subnet domains routed by Cisco routers. Our lab's 150 clients consisted of computing platforms that included Windows 2000/2003/XP/Vista/Win7, Macintosh 10.x and Red Hat Linux (both server and workstation editions).

The relational databases on the network were Oracle, IBM DB2 Universal Database, Sybase Adaptive Server 12.5 and both Microsoft SQL Server 2008 and 2012. The network also contained two Web servers (Microsoft IIS and Apache), three e-mail servers (Exchange, Notes and Sendmail) and several file servers (Windows 2003 and Windows 2008 servers).

Our virtual computing environments consisted of VMware, XenServer and Microsoft Hyper-V.

A group of four Compaq Proliant ML570 computers, running Windows 2003 Server, Windows 2008 Server and Red Hat Enterprise Linux, was our test platform for all the products' server components. A second group of four computers simulated our backup site for disaster recovery.

About the Author

Barry Nance is a networking expert, magazine columnist, book author and application architect. He has more than 29 years experience with IT technologies, methodologies and products. Over the past dozen years, working on behalf of Network Testing Labs, he has evaluated thousands of hardware and software products for ComputerWorld, BYTE Magazine, Government Computer News, PC Magazine, Network Computing, Network World and many other publications. He's authored thousands of magazine articles as well as popular books such as *Introduction to Networking (4th Edition)*, *Network Programming in C* and *Client/Server LAN Programming*.

He's also designed successful e-commerce Web-based applications, created database and network benchmark tools, written a variety of network diagnostic software utilities and developed a number of special-purpose networking protocols.

You can e-mail him at barryn@erols.com.

About Network Testing Labs

Network Testing Labs performs independent technology research and product evaluations. Its network laboratory connects myriads of types of computers and virtually every kind of network device in an ever-changing variety of ways. Its authors are networking experts who write clearly and plainly about complex technologies and products.

Network Testing Labs' experts have written hardware and software product reviews, state-of-the-art analyses, feature articles, in-depth technology workshops, cover stories, buyer’s guides and in-depth technology outlooks. Our experts have spoken on a number of topics at Comdex, PC Expo and other venues. In addition, they've created industry standard network benchmark software, database benchmark software and network diagnostic utilities.