CA ARCserve r16 vs. CommVault Simpana 9

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 CommVault Simpana (v9).

World Class Award

Executive Summary

The more mature and reliable CA ARCserve r16 is the clear winner of this review. CA ARCserve's faster performance, much better SRM reporting, far greater uptime and availability via Continuous Data Protection and far lower cost make CA ARCserve r16 our choice as the better answer for those organizations needing quality backup/restore as well as maximum high availability and replication.

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

CA ARCserve r16 and CommVault Simpana 9 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 Simpana 9 measure up? Which is best suited to your particular computing environment?

We decided to look closely and in detail at the abilities and shortcomings of both CA ARCserve and Simpana 9. In this report, we compare and contrast the two products, feature by feature.

CA ARCserve's components are CA ARCserve Backup, CA ARCserve D2D, CA ARCserve Replication and CA ARCserve High Availability.

Some of CommVault Simpana 9's many components are CommServe Master Server, Enterprise Data Management Server, SRM Reporting Enabler, Media Agents (AIX, Linux, Windows, etc.), Consolidated Data Storage Option, Content Store, Private Cloud Storage Gateway, CommCell Disaster Recovery, Granular Recovery Mining Tool, Content Indexing Enabler Data Client Connector, Content Director Policy Enabler and Snap Protection Client-Application Server.

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

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
- **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 VMs 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
- **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

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

(Continued) CA ARCserve's new features are

- **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 –** Replicates a complete Windows system (operating system, system state, applications and data) to an offline virtual server, monitors the system and application, and offers automatic and push-button failover for high availability. Includes hardware-independent BMR recovery and non-disruptive failback to restore the original production server.
- **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

CommVault Simpana 9's new features are

Virtual Server Data Protection

- **SnapProtect for virtual environments –** Quickly backup virtual environments; can restore applications, VMs or data files
- **Supports thousands of VMs --** Scales to support thousands of VMs.
- **Auto-discovery with autoprotection –** Automatically discovers and protects VMs using pre-defined data protection policies

(continued) CommVault Simpana 9's new features are

- **Complete lifecycle management –** Policy-based management tracks data across tiers of storage
- **Off-host cataloging –** Shifts data protection workloads away from production systems to improve server performance
- **Storage vendor support –** works with Dell, EMC, HDS, HP, IBM, NetApp, Oracle/Sun/LSI
- **Integrated deduplication –** Reduces network utilization across virtual and physical environments
- **Integrated SRM for virtual and physical environments –** Reports describe physical servers and the contents of individual VMs, file-level analysis and physical resource consumption
- **Citrix Systems XEN support**

Data Reduction

- **Source-side Deduplication –** Reduces network utilization right from the backup target computer
- **Global deduplication –** Uses multiple storage policies, each with its own retention settings
- **Single-console operation –** Gives a single operational view of all deduplication policies

Modern Data Protection

- **SnapProtect platform support –** Adds Oracle/Sun/LSI, HP platforms and IBM DB2, SAP, Microsoft Exchange 2010 applications to Dell, EMC, HDS, IBM and NetApp
- **Deduplication Accelerated Streaming Hash (DASH) Backup Copies –** Allows multiple data retention periods for multiple storage tiers
- **DASH–accelerated synthetic full backups –** Transfers signatures instead of actual data to a data storage target in order to reduce synthetic full backup times
- **Content Store –** Supports SAP content storage
- **EMC Documentum Support –** Protects Documentum databases, storage areas, and full-text indexes within Oracle or DB2 on UNIX
- **NetApp Data Connector –** Imports NetApp snapshots of Exchange, SQL Server, Oracle and SAP for Oracle data
- **PostGreSQL Database Support**
- **Exchange Information Mining –** Search, browse and restore individual Exchange mailboxes or e-mail notes

(continued) CommVault Simpana 9's new features are
Simplified Administration

- **Simplified license management with dashboard visibility –** At-a-glance reminder of how much of your Simpana licensed capacity you're using
- **Automated discovery and installation –** Finds unprotected servers and installs Simpana on them
- **Automated Simpana updates**
- **New Reports –** Health checks, data protection, media management, billing charge back, capacity planning and SLA performance, computer inventory, duplicate files, server capacity, software inventory, storage aggregate and storage inventory
- **Agentless, Remote SRM –** Unobtrusively collects data on systems and files
- **Fast Pass –** Helps automate a migration from IBM TSM or Symantec NetBackup to Simpana
- **Remote Operations Management Service (ROMS) –** 30-day trial of CommVault's remote management of your data backup operations

The categories we used in this evaluation are

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

For each feature, we provide a detailed ranking of the products and we explain the rankings when they're dissimilar.

The next feature chart reveals how well CA ARCserve and Simpana 9 fare in producing – and recovering from – image-based backups.

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.

Image-based Backup Features Comparison Table

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

Feature	CommVault Simpana 9	CA ARCserve r16
Snapshot/image backup technology	3	5
Operating System support	5	4
Device support	3	5
Virtual server support	5	5
Physical <–> virtual server support	5	5
Cloud capabilities and support	4	3
RTO/RPO (for disaster recovery)	5	5
Granular recovery	4	5
Off-site replication of images	5	5
Bare Metal Recovery (BMR)	4	5
Virtual standby for cold-failover	0	5
Client support	5	5
Image archiving, retention and versioning	5	5
Centralized management	3	5
Centralized reporting	4	5
SaaS subscriptions with cloud storage	5	5
RMM integration for MSPs	3	4
Image-based backup features aggregate ranking	**4.0**	**4.8**

Image-based Backup Notes

Technology – CA ARCserve r16 offers true infinite incremental snapshot/image-based backups onto virtually any disk drive. CA ARCserve's image-based backup/restore component is easy to install, a breeze to use, relatively inexpensive to buy and highly protective of your data. CA ARCserve's disk-to-disk image-based backup supports myriads of hardware combinations.

CA ARCserve's image-based backup is built on its patent-pending ***Infinite Incremental (I^2 Technology)*** that enables users to only perform a full backup once (the first time it's used) and then only perform incremental backups from that point forward. This technology 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.

Both CA ARCserve and Simpana offer synthetic backups, in which a full backup is assembled, or synthesized, from a baseline full backup and subsequent incremental backups. Simpana users must periodically create a new full backup. CA ARCserve's I^2, on the other hand, does not have this limitation – hence the name *Infinite Incremental*.

Simpana's design of its synthetic full backup methodology uses what the vendor terms ***Deduplication Accelerated Streaming Hash (DASH)*** to reduce the time needed for synthetic full backup operation. To minimize disk I/O, DASH transfers only data signatures instead of actual data to the target.

We were deeply disappointed by CommVault's disk image processing module, ***SnapProtect***. It's difficult and time-consuming to install, it's expensive and – the worst part – it's engineered poorly when it comes to protecting your data. CommVault admits that installing SnapProtect requires 4 weeks of effort. CommVault also says you'll need to research and either update or adjust several environment details: Firmware versions on the array, device types, modes of access, security configurations, operating systems that access the storage array and application layout on the storage array LUNs. SnapProtect can record hardware-based snapshots onto (within) just Dell, EMC HDS, HP, IBM or NetApp hardware arrays.

SnapProtect writes its backup/snapshot file (your first line of data disaster defense) ***onto the same hardware array filesystem that you're afraid may fail***. Later, the CommCell's CommServer schedules a subsequent operation to tell a proxy server to mount the hardware array, copy the image files to secondary storage and, after the secondary file copy finishes, unmount the hardware array. SnapProtect itself merely halts the application, triggers the hardware array to produce a snapshot right within the array and then restarts the application. We find these extra operations and steps to be a risky and poorly-designed engineering approach to protecting critical data.

CommVault imposes a number of other limitations and restrictions on SnapProtect. These include but are not limited to:

- *Once a backup copy is performed and the snapshot is copied to media, the same snapshot cannot be re-copied again*
- *If a previously selected snapshot has not been copied to media, the current SnapProtect job will complete without creating the backup copy and you will need to create an offline backup copy for the current backup*
- *If the Storage Policy or the disk library being used by the subclient is updated, the subclient should be recreated*
- *SnapProtect backups support online virtual machines only with NetApp file servers. Other storage array vendors use the traditional backup method. To perform a SnapProtect backup, the virtual machine must be offline.*

CA ARCserve r16 and Simpana 9 can each create snapshots as often as every 15 minutes.

Operating Systems, BMR – Simpana supports UNIX flavors as well as Windows, but CA ARCserve supports only Windows. Simpana, like CA ARCserve, can restore Windows images onto dissimilar hardware, but imposes significant constraints on its UNIX BMR operations.

Cloud Support – Both Simpana and CA ARCserve write the initial snapshot (backup) to disk. A subsequent step copies the snapshot data to a cloud. For secondary storage (via its proxy backup/restore component), Simpana 9 can interface with the cloud vendors Amazon, Azure, EMC (Atmos), Iron Mountain, Meseo, Nirvanix and Rackspace. CA ARCserve's D2D feature works with Amazon and Azure 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.

Remote Management via Managed Service Providers (MSPs) – Several MSPs have embraced CA ARCserve, and the list is growing. CommVault is currently just beginning to get MSPs to consider supporting Simpana.

Performance and Media Usage – CA ARCserve's I^2 is faster than Simpana 9's synthetic full backup process (its Deduplication Accelerated Streaming Hash notwithstanding), and I^2 uses less storage space. For a complete system comprising 300 GB, Figure 1 shows the relative performance of CA ARCserve r16 I^2 and Simpana 9.

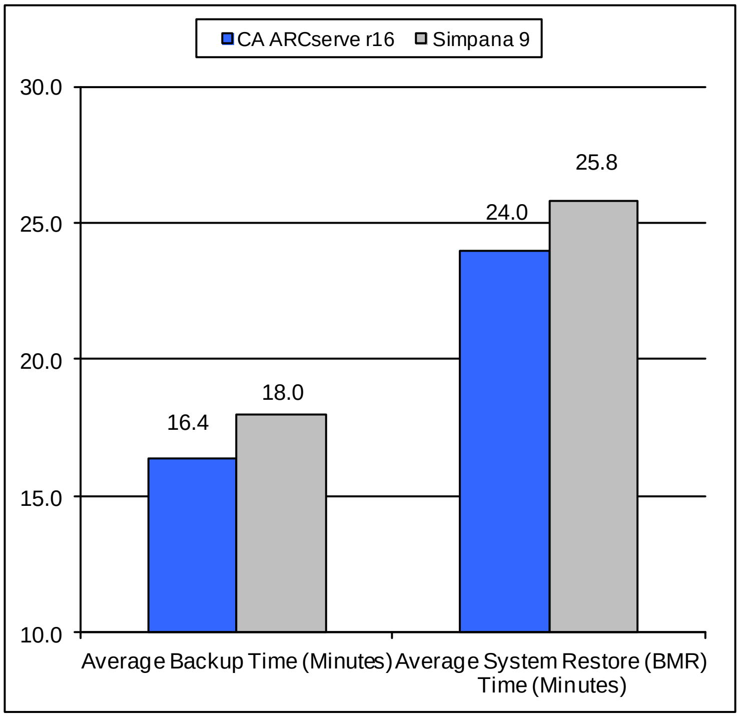

Figure 1.

CA ARCserve I^2 vs. Simpana 9 image-based backup/restore performance

CA ARCserve also needed 8% less storage space than Simpana 9 (120 GB vs. 131 GB) when we tested the creation of monthly full backups and selected each product's highest level of compression.

In our tests, CA ARCserve's I^2 utilized only small, incremental amounts of backup storage after the initial full backup. In contrast, Simpana 9's need to perform periodic full backups caused it to consume considerable backup storage, overwhelming any advantage of Simpana's (interim) synthetic full backups.

Using infinite incrementals (one full backup at the outset and incremental thereafter) – but telling Simpana 9 (as CommVault recommends) to continue creating monthly full backups with incrementals during the month – we saw that I^2 used about half Simpana's space at the end of two months (144 GB vs. 268 GB) and a little more than a third of Simpana's space at the end of three months (161 GB vs. 420 GB). Figure 2 depicts the resulting storage requirements.

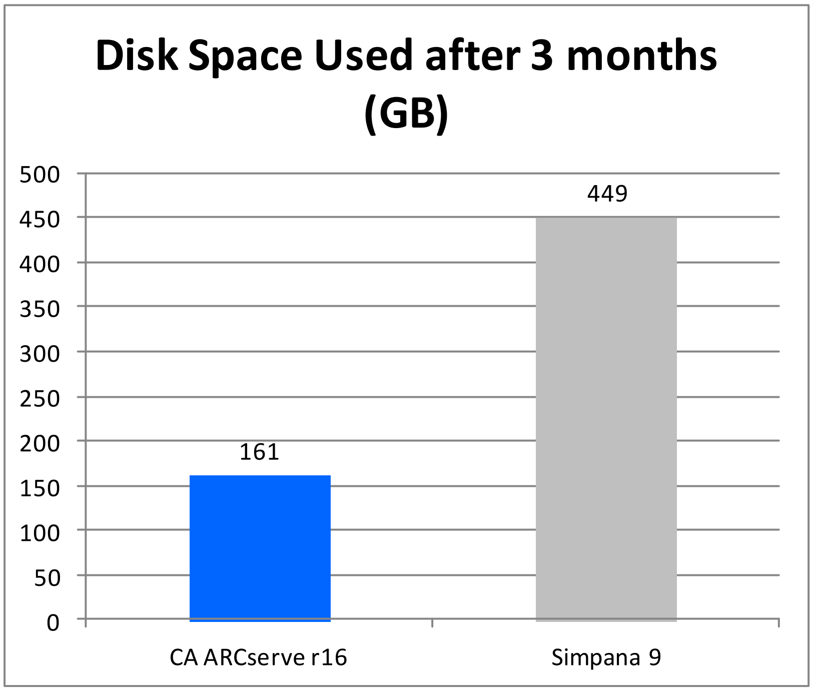

Figure 2.

CA ARCserve I^2 vs. Simpana 9 image-based disk storage utilization

Virtualization Support -- Both CA ARCserve and Simpana 9 are champions of virtualization, supporting VMware ESX and vSphere, Microsoft Hyper-V and Citrix XenServer. CA ARCserve additionally supports Redhat KVM.

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.

Unfortunately, Simpana 9 lacks an automated virtual standby feature.

RTO/RPO Performance Testing – To measure CA ARCserve's and Simpana'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. In our tests, both CA ARCserve and Simpana took snapshots every fifteen minutes and transferred backup material 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 Simpana 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 47 minutes** to restore data to the servers and resume the OLTP application. Primarily because of the complexity of its user interface (and despite its use of the term "1-Touch" to describe the process), the **Simpana administrator needed one hour and fifteen minutes** (75 minutes) to accomplish the same thing – **28 minutes longer**. If time is money in your data center, CA ARCserve is clearly the tool of choice when disaster strikes.

Central Management – Working with disk images is easy and painless with CA ARCserve's Web 2.0 based management console. Simpana's user interface for dealing with image-based backups is comparatively awkward, despite its "1-Touch" name.

Central Reporting – Similarly, CA ARCserve's Central Reporting component produces much more useful and informative reports regarding disk image recovery points than does Simpana 9. Both products integrate with Windows Explorer to show the contents of an image file as a mountable drive letter.

In the next chart, we take a detailed look at basic, fundamental CA ARCserve r16 and Simpana 9 file-based backup and restore capabilities.

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.

File-based Backup Features Comparison Table

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

Feature	CommVault Simpana 9	CA ARCserve r16
Tape device support	5	5
Application support	5	5
Tape integration	5	5
Tape archiving, retention and versioning	5	5
Virtual machine protection	5	5
Application-specific granular recovery	5	5
SRM reporting	4	5
Basic backup reporting	3	5
Infrastructure visualization	3	5
Central management	3	4
Deduplication	5	4
Public and private cloud support	5	4
File archiving	5	5
Integration with image-based backups	5	5
Synthetic full backups	4	5
File-based backup features aggregate ranking	**4.5**	**4.8**

File-based Backup Notes

CA ARCserve r16 and Simpana 9 have similar file-based backup features. They both support the same operating systems, applications and backup devices. CA ARCserve has advantages over Simpana, however, in its reporting, its infrastructure visualization and its central management console. CA ARCserve was also faster than Simpana in our tests, and its data deduplication was more efficient.

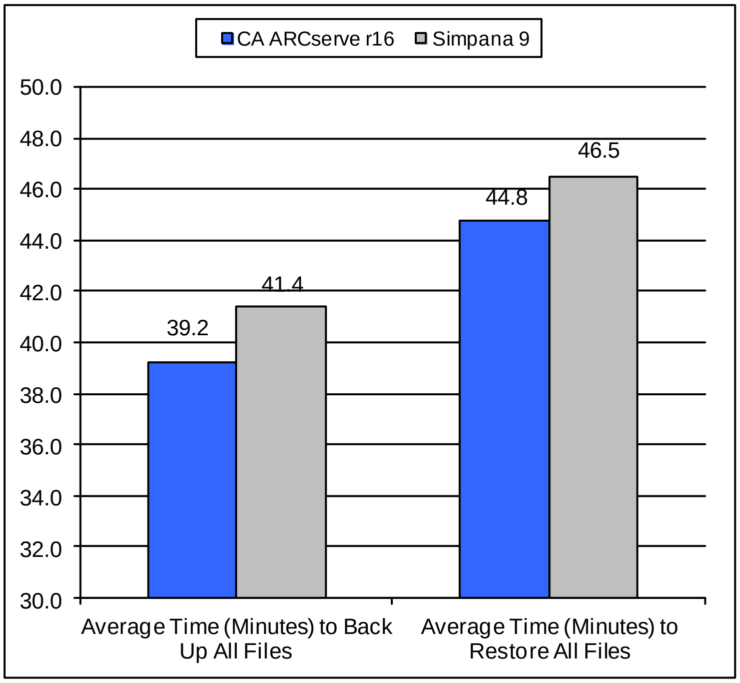

Figure 3.

CA ARCserve r16 vs. Simpana 9 backup/restore performance

Figures 3 and 4 graph the relative performance of the two products.

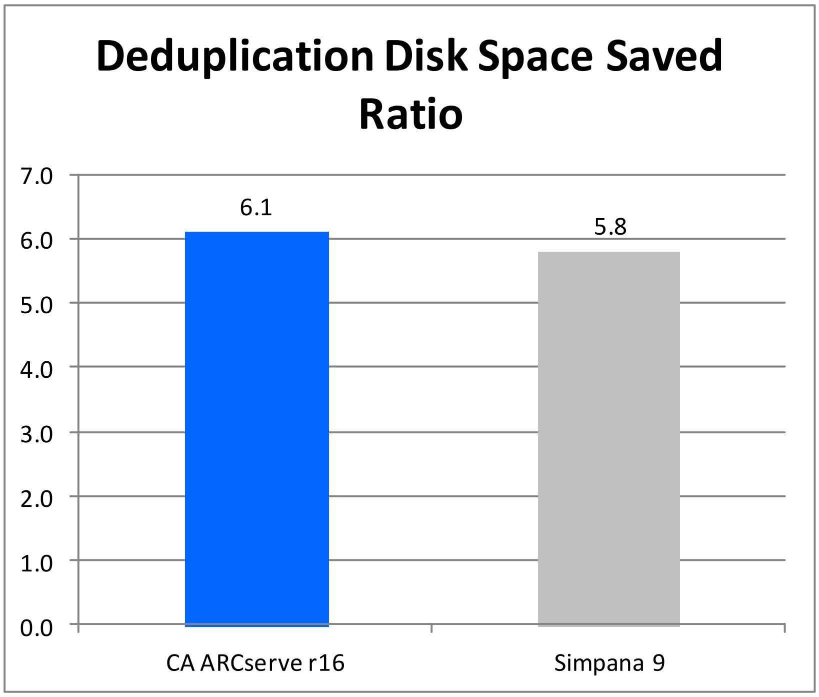

Figure 4.

CA ARCserve r16 vs. Simpana 9 data deduplication ratios (higher is better)

Separately for each Storage Policy, Simpana's basic reports show details on backup histories, retentions and storage media usage. In contrast, 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.

With its reports on physical servers and the contents of individual VMs, file-level analysis and physical resource consumption, Simpana 9 exhibits a modicum of SRM capability. In stark contrast, 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.

Simpana 9 can perform data deduplication at either the server or the client, while CA ARCserve's deduplication is server-only. On the other hand, Simpana's deduplication feature is an extra-charge option. CA ARCserve includes deduplication at no extra charge.

Also note that Simpana 9 has some quirky and somewhat confusing restrictions on the use of incremental backups, as exemplified by the following Simpana 9 documentation excerpt.

> ***Incremental Storage Policy Considerations***
>
> - *You cannot enable a storage policy as an incremental storage policy if that storage policy already has an incremental storage policy enabled.*
> - *The incremental storage policy option is only available for a Standard storage policy.*
> - *If you are using a different MediaAgent for an incremental storage policy than the MediaAgent used for a full storage policy, one of the following conditions must be met:*
>   - *The primary copies of both this storage policy and the selected incremental storage policy use a shared index cache.*
>   - *The primary copies of both this storage policy and the selected incremental storage policy are set to use preferred data paths.*
> - *If an incremental storage policy is de-associated from a storage policy, the most recent incremental backup may be pruned before the next full backup occurs.*

In the last features table, let's examine the huge differences between CA ARCserve and Simpana 9 in the areas of replication and high availability.

Replication and High Availability

Replication 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.

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.

Multiple master and replica computers are possible. The result is a file, application or database server that's virtually always available.

Replication and High Availability Features Comparison Table

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

Feature	CommVault Simpana 9	CA ARCserve r16
Replication	5	5
True high availability (hot failover)	3	5
Physical and virtual server support	5	5
Operating System and application support	5	5
RTO/RPO (for disaster recovery)	4	5
Cloud Integration	5	4
Continuous Data Protection (CDP)	3	5
Offline synchronization	5	5
Replication and HA recovery testing	3	5
Network optimization	3	5

Feature	CommVault Simpana 9	CA ARCserve r16
Replication and backup integration	5	5
Assessment mode utility	2	5
Application aware replication	5	5
Replication and high availability features aggregate ranking	**4.0**	**4.9**

Replication and High Availability Notes

CA ARCserve's replication component may be used in a scheduled manner to migrate and manage offsite backups. In a real-time, continuous manner, CA ARCserve provides true Continuous Data Protection (CDP). In contrast, Simpana's replication feature, Continuous Data Replication (CDR), delivers "Near CDP" by allowing disaster recovery copies of backup/archive data to be created over a LAN or WAN on a continuous basis. However, Simpana's approach requires manual intervention on the part of an administrator when a data disaster occurs.

For companies needing maximum system uptime and availability, CA ARCserve has a High Availability (HA) component. Simpana 9 has a replication feature but does not offer high availability.

Both CA ARCserve's and Simpana'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 Simpana's replication features clone each I/O operation and send the cloned copy to a secondary destination of your choice.

Both CA ARCserve and Simpana can replicate between physical and virtual servers (P2P, P2V and V2P) and even between virtual server platforms (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. Simpana lacks all these features.

With Simpana's "Near CDP" and absence of a high availability component, 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, Simpana 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. Simpana'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. Simpana comes with far fewer pre-built scenarios, and for just some of the most popular applications – Oracle, Microsoft Exchange, Microsoft SharePoint and Microsoft SQL Server.

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

CA ARCserve is also unique in its high availability support for Windows server clusters. Simpana can replicate data onto clustered Windows servers, but an administrator must activate servers within the cluster to complete/finish a failover operation.

CA ARCserve's Replication and High Availability components also 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 application level on the replica server, without affecting the production server or impacting the continuous data protection and monitoring. Simpana's less automated approach requires manual intervention and, unfortunately, requires rebooting the server.

Simply put, Simpana 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. Simpana's replication feature required an **interminable 93 seconds** – over a minute and a half – to recover from the simulated disaster, after which the administrator had to manually restart the OLTP application.

Ease of Use and Pricing

CA ARCserve's well-formatted and configurable dashboard reveals, at a glance, the current status of your backups. With Simpana, visualizing backup status requires several more navigations steps. If you have multiple site backups, both CA ARCserve and Simpana consolidate and centralize backup status information from all sites.

Simpana also shows a dashboard display of backup/restore status information, but it's not as revealing nor as configurable as CA ARCserve's.

Note that one of the Simpana dashboard indicators gives you an at-a-glance reminder of how much of your Simpana licensed capacity you're using. If you exceed that licensed capacity, even for just a moment, the Simpana software "phones home" to notify CommVault of the "excess usage." You see the result in a bill from CommVault, and the size of the bill may astonish you … CommVault's charges for excess usage are quite high.

We were also disappointed and dismayed to find that CommVault, both in its documentation and in its approach to data protection, considers "disaster recovery" to be the restoration of a failed Simpana server rather than the recovery of a customer's critical data. To our minds (and perhaps to yours), this is the wrong perspective.

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. In contrast, navigating Simpana's Storage Policy-oriented backup reports can be time-consuming and unproductive. Furthermore, Simpana gave us an unpleasant surprise by requiring us to periodically reorganize and re-index each of the internal CommCell databases.

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. Simpana’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.

CommVault’s pricing for Simpana 9 is significantly higher than that of CA ARCserve, as shown in the following tables. (Except for the managed capacity offerings, CA ARCserve pricing includes one year of maintenance. For Simpana 9 maintenance, add 21% to net license price.) Be aware that the “a la carte” Simpana pricing can save you money, but you must know exactly which modules and components you need – a daunting challenge.

CommVault Simpana 9 Pricing

	MSRP
Per Terabyte of managed capacity	$8,000 - $10,000
(a la carte)	**MSRP**
CommServe Master Server, Enterprise Edition	$5,000
Enterprise Data Management Server, Enterprise Edition	$9,500
SRM Reporting Enabler	$4,500
SRM Exchange Server agent, per server	$1,195

SRM SharePoint Server agent, per server	$1,195
SRM MS SQL DB agent, per server	$1,395
SRM Oracle DB agent per server	$1,395
SRM VMware Agent, per VSA client	$500
SRM Unix/Linux FS agent, per server	$225
SRM Windows FS agent, per server	$225
SRM NAS agent (up to 6 TB), per server	$1,995
Media Agent (AIX)	$7,500
Media Agent (Linux)	$2,350
Media Agent (Solaris)	$7,500
Media Agent (Windows)	$2,350
Advanced Disk-Deduplication - Disk Library Capacity License	$3,000
Consolidated Data Storage Option	$5,000
Conversion license per TB - upgrade Std Disk capacity to CDSO capacity	$4,200
Content Store, Private Cloud Storage Gateway	$5,000
Tape Drive Management Software (priced per drive)	$1,950
CommCell Disaster Recovery License (200+ clients)	$8,500
Secondary Copy Data Encryption enabler per MediaAgent	$7,500
CommCell Data Erase Enabler	$2,500
Granular Recovery Mining Tool pack (Granular Recovery of Exchange, SharePoint and Active Directory)	$5,000
External Data Connector (Tier 3)	$10,000
Content Indexing Enabler Data Client Connector (10 pack), per host	$40,000
Content Director Policy Enabler per CI Index Node	$10,000
Virtual Environment Bundle, Tier 4 (Up to 500 VMs)	$42,500
Partitioned Unix DB Bundle per host, Tier 4 (50 clients)	$60,000
Snap Protection Client-Application Server, per Win/Linux host, choice of Application option, 25 client pack (Media storage capacity not included)	$60,000
Snap Protection Client-Application Server, per Unix host, choice of Application option, 25 client pack (Media storage capacity not included)	$125,000
Data Replication for Unix	$2,930
Data Replication for Windows	$1,955
Software Support – Software Assurance Annual Cost	$262,500

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

Note that CA ARCserve includes deduplication, archiving, Active Directory granular restore and synthetic full backup in its basic product, at no extra charge.

Rankings Summary

	Simpana 9	**CA ARCserve r16**
Image-based backup	4.0	4.8
File-based backup	4.5	4.8
Replication, High Availability	4.1	4.9
Usability	4.0	4.5
Total score	**4.2**	**4.8**

Conclusion

CA ARCserve is an integrated, reliable, easy-to-use and scalable answer when disaster happens. CA ARCserve offers comprehensive file-based and image-based backup, performs backups and restores faster, offers much better SRM reporting and provides far greater uptime and availability. Moreover, CA ARCserve r16 costs far less than Simpana 9.

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

Vendor Contacts

CA 800-225-5224	www.arcserve.com
CommVault 888-746-3849	www.commvault.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.