CA arcserve UDP vs. CommVault Simpana 10

Product Review

We test CA arcserve Unified Data Protection (UDP) and CommVault Simpana 10 to find which is best for backup/restore, disaster recovery, replication and business continuity.

Executive Summary

CA arcserve UDP performs faster, uses less storage space, costs far less, is easier to administer and offers High Availability for greater uptime and availability via Continuous Data Protection (CDP). Uniquely, CA arcserve UDP has more useful and informative SRM reporting, offers Virtual Standby for cold failover, has automated, assured disaster recovery and has a programmatic interface for third-party integration.

Whether your primary consideration is price or features, CA arcserve UDP is clearly the answer.

The following chart shows, at a glance, the significant differences between CA arcserve UDP and CommVault Simpana 10.

	CommVault Simpana 10	CA arcserve UDP
Performs faster		✓
Easier to administer		✓
Costs less		✓
Backs up virtual and physical servers	✓	✓
Has both image- and file-based backup	✓	✓
High Availability (with true CDP)		✓
Supports several virtual platforms	✓	✓
Virtual Standby for cold failover		✓
Restores Exchange folders and e-mails	✓	✓
Automated, assured disaster recovery		✓
APIs for 3rd party integration		✓

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

CA arcserve UDP vs. CommVault Simpana 10

Product Review

CA and CommVault both claim to better protect your data when disasters, failures and human mistakes occur. The vendors' products, CA arcserve UDP and CommVault Simpana 10, have many features to support these claims. Which product truly is better? Which one is best suited to your computing environment (and budget)?

We decided to look closely and in detail at the abilities and shortcomings of both CA arcserve UDP and Simpana 10. In this report, we compare and contrast the two products, feature by feature and test by test.

CA arcserve UDP is a single product with a licensing structure that unlocks such functions as replication and high availability.

Some of CommVault Simpana 10's many components are CommServe Master Server, Enterprise Data Management Server, SRM Reporting Enabler, SRM FS monitor agent, SRM NAS client, Media Agents (AIX, Linux, NetWare, Windows, etc.), Advanced Disk-Deduplication Option, 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 IntelliSnap Snapshot Enabler.

CA arcserve UDP's significant features include:

- **Recovery Point Server (RPS) –** CA arcserve UDP's brain. Generates catalogs, deletes expired backups, stores backup data sets, replicates data to other RPS machines, manages backup and restore operations and supervises CA arcserve Replication and High Availability operations.
- **True Global Deduplication –** Optionally store a single copy of data, source-side-deduplicated across all nodes, to save both disk space and network bandwidth.
- **Integrated Replication –** On a continuous basis, each RPS can optionally maintain multiple copies of backup data via replication. These backup data copies are available for virtually instantaneous use on secondary servers if a primary server fails.
- **Microsoft Hyper-V Support –** Agentless backup of data on Hyper-V virtual machines, with support for Virtual Standby (see below), incremental backups, data compression and data deduplication.
- **VMware vSphere Support –** Agentless backup of data on VMware vSphere virtual machines, with support for Virtual Standby (see below), incremental backups, data compression and data deduplication.
- **Windows and Linux Clients –** Uses a small agent to back up Windows or Linux client (workstation) data (physical or virtual).

- **Backup Plans –** Easy-to-administer named policies that specify exactly how to make backup copies of your data. Each plan contains instructions for copying data, replicating data, making secondary and tertiary copies of data (typically offsite), setting up and maintaining Virtual Standby machines and notifying administrators that a backup job succeeded or failed.
- **RPS Share Plan –** Establishes client backup plans, maps multiple Windows users to a plan and shares the plan with remote RPS machines.
- **Multiple Data Store Options –** CA arcserve UDP can store data on a local disk, a remote file server, a virtualized storage device or a NAS device. Compression, global data deduplication and strong encryption are settable options.
- **Sophisticated Scheduling –** Performs backup, merge, retention and replication tasks when and how you specify.
- **Virtual Standby --** Maintains an up-to-date standby (secondary) virtual server that can instantly replace a failed primary server in either physical-to-virtual (P2V) or virtual-to-virtual (V2V) mode. Automated or manual failover.
- **Useful Reports –** CA arcserve UDP tells administrators the current status and health of backup jobs and backup environment with such details as Managed Capacities, Backup Sizes, Backup Status, Virtualization Protection Status and Data Distribution on Media.
- **Multi-layer Data Recovery Options –** Recover data for an application, a specific file, an entire file system or a VM. Instant volume-level recovery for Linux.
- **Exchange Granular Restore –** Recover mail for an account, an account's mail folder, a single mail item or an entire Exchange system.
- **Bare Metal Recovery (BMR) –** Restores a Windows or Linux computer's complete operating environment, including files, settings and operating system, to a different hard disk, to a similar but different computer or to even a dissimilar computer.
- **Copy File or Recovery Point –** Saves extra copies of a particular file or an entire recovery point to the specified disk or cloud destination(s) for added data protection.
- **RPS Jumpstart –** Move large data stores to a new remote RPS via external device (e.g., USB flash drive memory).

CommVault Simpana 10's significant features include the following.

- **IntelliSnap Technology –** Automate snapshot management and application-aware recovery across a variety of hardware arrays.
- **Parallel Deduplication –** Optionally store a single copy of data, enterprise-wide, to save both disk space and network bandwidth.
- **OnePass –** Perform backup, archiving and reporting for file and email data in a single scan.
- **ContentStore –** Central repository of all Simpana-managed data.

- **Virtual Server Protection –** Discovery, installation, backup and reporting tools for VMware and Hyper-V.
- **Disaster Recovery –** Replicates backup copies to remote sites or a cloud.
- **Cloud Integration –** Support for private and public cloud storage.
- **Archive and Search –** Move least-used data to lower-cost storage; provide search tools for ContentStore data.
- **Migration Tools –** Switch from NetBackup or Tivoli Storage Manager to Simpana 10.
- **Global Reporting –** Dashboard display plus diagnostic data and backup status reports.
- **Professional Services –** Get CommVault consultants onsite.

Additionally, CommVault Simpana 10 SP6's new features are

- **Download Manager --** Create Windows or UNIX Simpana component installation packages.
- **Access Updates and Metrics Reports --** Configure an offline client to download software updates and packages from the CommVault Software Store.
- **CommVault Software Store –** Download reports, workflows and tools from the store.
- **SQL Scripts -** Software Installation components and updates
- **Capacity License Changes –** Enable client backup, archive and IntelliSnap operations for separate subclients rather than at the File System Agent level.
- **Disconnected MediaAgent NAS --** Configure NAS client with the MediaAgent when the CommServe computer does not have direct access to the file server.
- **Install SQL Server 2012 as Default Simpana Database –** Use SQL Server 2012 for new and for older Simpana installations.
- **DB2 pureScale IntelliSnap Support –** DB2 MultiNode Agent creates a point-in-time snapshot by quiescing the database, taking a snapshot and then resuming live operations.
- **AS/400 (iSeries) Backup Support –** Uses the File System Agent.
- **Access Offline Archived Emails –** Store archived emails directly on client computers to allow ContentStore Email Viewer to see offline archived emails.
- **Multiple CommCell Data Visibility –** Use Data Analytics Reports to see large or outdated backup objects across several CommCells.
- **File and Folder Sharing –** Use the Web Console to share client computer backups among users.
- **Agentless VMware Restores –** Avoid having to install a File System or Restore Only Agent in order to restore files and folders.
- **VM Archiving –** Shutdown, relocate and archive VMs during the backup process.
- **Linux VM File Recovery –** Avoid having to install a File System Agent in order to restore Linux VM files from an IntelliSnap backup.

The categories we used in this evaluation are

- Ease of use and overall features
- Pricing
- Image-based backup features
- File-based backup features
- Replication/high availability features

The first section contrasts CA arcserve UDP and CommVault Simpana 10 for ease of use and overall features.

Ease of Use and Overall Features

CA arcserve UDP has a new, sophisticated Web-based user interface, the ***Unified Management Console (UMC)***. The UMC is a single pane through which administrators manage, direct and control the entire breadth of CA arcserve UDP functions. The UMC is task-based, simple to use, intuitive, easy to navigate and responsive. It offers one-step-at-a-time, guided wizards for everyday operations, reporting functions, creating a new RPS, establishing backup/recovery policies and other tasks. With the UMC, an administrator is never more than a mouse-click away from seeing backup status information, producing reports, adjusting a backup schedule, or – if need be – restoring a computer to a known-to-be-good, running state.

With the UMC, an administrator can easily see and manage all servers and clients. He or she can even use a mobile device to access the UMC. As an extra bonus, a carefully-designed, well-documented programmatic interface is available that MSPs and large enterprises can use to quickly and surely integrate CA arcserve UDP into an existing complex data center environment.

CA arcserve UDP's well-formatted and configurable dashboard reveals, at a glance, the current status of your backups. Simpana also shows a dashboard display of backup/restore status information, but it's not as revealing or as configurable as CA arcserve's.

With a single click, CA arcserve UDP displays clear and highly descriptive graphical details regarding backup sets and backed up data. With Simpana, visualizing backup status requires several more navigational steps.

If you have multiple site backups, both CA arcserve and Simpana consolidate and centralize backup status information from all sites.

A Simpana dashboard meter gives you a reminder of how much of your Simpana licensed capacity you're using. If you exceed this licensed capacity, the Simpana software "phones home" to notify CommVault of the excess usage, for which you subsequently receive an invoice. To avoid unplanned budget variances, make sure that you understand CommVault's policies regarding excess usage.

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, we found navigating Simpana's Storage Policy-oriented backup reports to be labor-intensive and unproductive. Furthermore, Simpana gave us an unpleasant surprise by requiring us to periodically reorganize and re-index each of the internal CommCell databases.

The overall feature sets of CA arcserve UDP and Simpana 10 are somewhat similar. Both have BMR, global deduplication, built-in replication, optimized bandwidth usage, excellent scalability, client/workstation protection and a comprehensive set of APIs for 3rd party integration.

Some of the CA arcserve UDP features that Simpana 10 lacks include:

- Assured Recovery
- High Availability/failover
- CDP

Bare Metal Recovery – CA arcserve UDP's BMR can easily recover an entire Linux or 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 UDP's BMR can restore data from physical and virtual servers onto dissimilar hardware (P2P, P2V, V2P and V2V).

CommVault uses the term "*System State Backup/Restore*" to refer to Simpana's BMR feature. Simpana's System State Backup/Restore is less sophisticated than CA arcserve UDP's BMR. For example, when attempting a System State Restore to a different computer, the Simpana administrator typically must first install an operating system on the target and then manually exclude certain backup set elements (such as OS drivers) from the restore operation. CommVault's BMR process assumes that the target computer already has at least an operating system on it. CA arcserve UDP's BMR is truly "bare metal" – it does not assume anything about the target computer.

Global deduplication – At your option, CA arcserve UDP stores only a single copy of ***enterprise-wide*** duplicate data. The "to-all-employees" e-mail messages that everyone saves copies of, the widely-distributed documents that people file away, the videos that people like to archive and the common application files that each user has are all good examples of across-the-company duplicate data.

CA arcserve UDP maintains a global index of duplicate data. Whether the duplicate data consists of just a few users' files in one location or is spread across New York, Chicago, Los Angeles, Sydney, Tokyo, Hong Kong, Shanghai, Mumbai, Tel Aviv, Cairo, Athens, Berlin, Paris and London – CA arcserve UDP globally deduplicates your data. It carefully notes the duplicate data's different locations in its deduplication database, which CA arcserve UDP distributes among the various RPS servers. We found another feature particularly appealing: CA arcserve UDP can store its deduplication database on Solid State Disks (SSDs). The result is improved performance and reduced bandwidth utilization. Furthermore, CA arcserve UDP secures the deduplication process with encryption and per-session passwords.

CommVault Simpana 10 has a similar global deduplication feature. However, unlike CA, CommVault charges extra for its deduplication feature.

Automated Disaster Recovery (DR) and Assured Recovery – You can instruct CA arcserve UDP to automatically fail over to an alternate set of servers (likely at a remote site or hosting provider) when disaster strikes. Without disrupting your business or the flow of data in your organization, CA arcserve UDP will even periodically test the failover process. The test produces a detailed report that you (and compliance auditors) can use as evidence of system recoverability. Quick, worry-free disaster recovery is a hallmark of CA arcserve UDP.

CommVault's disaster recovery approach is somewhat short-sighted. The vendor 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.

Replication – CA arcserve UDP can send a copy of each and every data output (i.e., write) operation to a secondary destination. The replication destination can be, for example, a separate RPS, a secondary server or a cloud. The replication destination is an instantly-available secondary resource in case of disaster. Intelligently, CA arcserve UDP uses compression, encryption, WAN optimization and bandwidth throttling to give you control over the replication process, including network bandwidth utilization and thus costs. The replication feature uses HTTP tunneling to avoid firewall and Network Address Translation (NAT) issues. CA arcserve UDP can replicate in a one-to-one, one-to-many or many-to-one fashion. CA arcserve UDP keeps the replicated server(s) perfectly synchronized with the primary (source) server(s).

CommVault Simpana 10 also has a data replication feature.

High Availability/Failover – CA arcserve UDP's HA achieves virtually 100% uptime for servers you designate by monitoring applications and background services running on a

server. If a service fails, CA arcserve UDP attempts to restart it. If the restart fails, the system can be set to automatically fail over to a 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 manual push-button failover.

CA arcserve UDP can monitor a single server, group of servers, 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 UDP 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 the failover happened.

CommVault Simpana 10 has no High Availability feature, and it does not provide Continuous Data Protection (CDP).

Scalability – CA arcserve UDP's architecture is eminently scalable. To save money, a small company might add RPS functionality to an existing file server. At the other end of the spectrum, a large enterprise might install individual CA arcserve UDP elements on a variety of dedicated servers throughout the organization's data centers. CA arcserve UDP can support any server or application topology. Simpana 10 also scales well.

APIs for 3rd party integration – Managed Service Providers (MSPs) and large enterprises can easily integrate CA arcserve UDP into their existing organizational structures via a comprehensive, simple-to-use and clearly documented Web-API programmatic interface.

CommVault Simpana 10's Automated Management feature can run scripts that instruct Simpana to perform repetitive or complex data backup/restore tasks. While the scripting engine is fairly rudimentary – it merely feeds script entries to Simpana's Command Line Interface (CLI) – the feature does have a highly visual, drag-and-drop graphical environment for script creation.

Pricing

The following tables show CommVault's and CA's prices for Simpana 10 and CA arcserve UDP. CA arcserve UDP includes one year of maintenance. For Simpana 10 maintenance, add 21% to net license price (alternately, purchase CommVault's Software Assurance option for $575,000).

While the two fee schedules are structured very differently, our analysis reveals that CommVault Simpana 10 costs much more yet provides far fewer features than CA arcserve UDP.

For instance, a basic CommVault Simpana 10 license to protect 2 Terabytes of data will cost you $10,000. In contrast, CA arcserve UDP Standard Edition is only $7,553.14.

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

CommVault Simpana 10 Pricing

	MSRP
Two Terabytes of basic managed capacity	$10,000
One Terabyte of Application Data Management (ADM)	$7,000
(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 NAS client, per proxy 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 – One Terabyte	$3,000
Consolidated Data Storage Option – One Terabyte	$5,000
Tape Drive Management Software (priced per drive)	$1,950
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 (1-500 clients)	$4,000
Virtual Environment Bundle, Tier 4 (Up to 500 VMs)	$42,500
Partitioned Windows/Linux DB Bundle (per physical host) (50 clients)	$60,000
Data Replication for Unix – 1 node	$1,750
Data Replication for Windows – 1 node	$1,150
Software Support – Software Assurance Annual Cost	$575,000

CA arcserve UDP

	MSRP
CA arcserve Unified Data Protection Standard Edition Includes Limited Tape Functionality and RPS Replication	$3,776.57 per Terabyte
CA arcserve Unified Data Protection Advanced Edition Includes Limited Tape Functionality and RPS Replication	$4,724.57 per Terabyte
CA arcserve Unified Data Protection Premium Edition* Includes Complete Tape Functionality and RPS/File-level Replication	$7,870.51 per Terabyte
CA arcserve Unified Data Protection Premium Plus Edition* Includes Complete Tape Functionality and Complete RHA Functionality	$13,810.51 per Terabyte
CA arcserve Unified Data Protection Standard Edition Includes Limited Tape Functionality and RPS Replication	$595 (per socket)
CA arcserve Unified Data Protection Advanced Edition Includes Limited Tape Functionality and RPS Replication	$745 (per socket)
CA arcserve Unified Data Protection Premium Edition Includes Complete Tape Functionality and RPS/File-level Replication	$1,195 (per socket)
CA arcserve Unified Data Protection Premium Plus Edition Includes Complete Tape Functionality and Complete RHA Functionality	$1,795 (per socket)
CA arcserve Unified Data Protection	$445.20 For five clients

- Terabyte Volume Tiers: 1TB, 2-5TB, 6-15TB, 16-25TB, 26-50TB, 51-100TB, and 100+TB
- Per Socket prices apply to both hypervisors and physical servers
  A Per-Socket "Essentials" version available for up to six sockets for VMware Essentials & Windows SBS/Essentials Servers at a 20% discount
- Workstation Volume Tiers: 5, 10, 25, 50, 100, 250, and 500 clients

In the next section, you get a detailed evaluation of the image-based backup and recovery capabilities of CA arcserve UDP and CommVault Simpana 10.

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 10	CA arcserve UDP
Snapshot/image backup technology	3	5
Operating System support	5	5
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)	4	5
Granular recovery	5	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	4	5
Centralized reporting	4	5
RMM integration for MSPs	3	5
Image-based backup features aggregate ranking	**4.0**	**4.9**

Image-based Backup Notes

Technology – CA arcserve UDP offers true infinite incremental snapshot/image-based backups onto virtually any disk drive. CA arcserve's image-based backup/restore 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***, which 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.

CommVault Simpana also offers synthetic backups, in which a full backup is assembled, or synthesized, from a baseline full backup and subsequent incremental backups. However, CommVault recommends that Simpana users periodically create a new full backup, typically once a week or at least once a month. 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, not the actual data, to the backup target.

CommVault's snapshot management component, ***IntelliSnap***, supports the following hardware arrays:

- Dell Compellent, EqualLogic, PowerVault MD
- EMC Celerra, CX, DMX, VMAX, VNX
- HDS AMS, HUS, USP/VSP
- HP 3PAR, EVA, XP
- IBM DS Series, N-Series, SVC & XIV
- Fujitsu ETERNUS
- NetApp E-Series, FAS
- Nimble CS Series
- Oracle/SUN LSI

Note that, before you can begin to use IntelliSnap, you'll need to research and either update or adjust several hardware array environmental details, including array firmware, device types, modes of access, security configurations, operating systems that access the storage array and application layout on the storage array LUNs.

IntelliSnap 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. IntelliSnap itself merely halts the application, triggers the hardware array to record a snapshot and then restarts the application.

CA arcserve UDP and Simpana 10 can each create snapshots as often as every 15 minutes.

Operating Systems, BMR – Both CA arcserve UDP and Simpana 10 support UNIX, Linux and Windows. Simpana 10, like CA arcserve UDP, can restore Windows images onto dissimilar hardware. However, Simpana imposes significant constraints on its UNIX BMR operations. Simpana 10's BMR, which the vendor terms "System State Backup/Restore," also assumes that an administrator has already installed an operating system on the target computer.

Cloud Support – Both Simpana and CA arcserve write the initial snapshot (backup) to disk. A subsequent step can copy snapshot data to a cloud. For secondary storage (via its proxy backup/restore component), Simpana 10's cloud support includes Microsoft Windows Azure, Amazon Web Services, NetApp, Rackspace and HDS. CA arcserve UDP works with Amazon and Azure to store 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 or expensive cloud connections.

Performance and Media Usage – CA arcserve UDP's I^2 is faster than Simpana 10'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 UDP I^2 and Simpana 10.

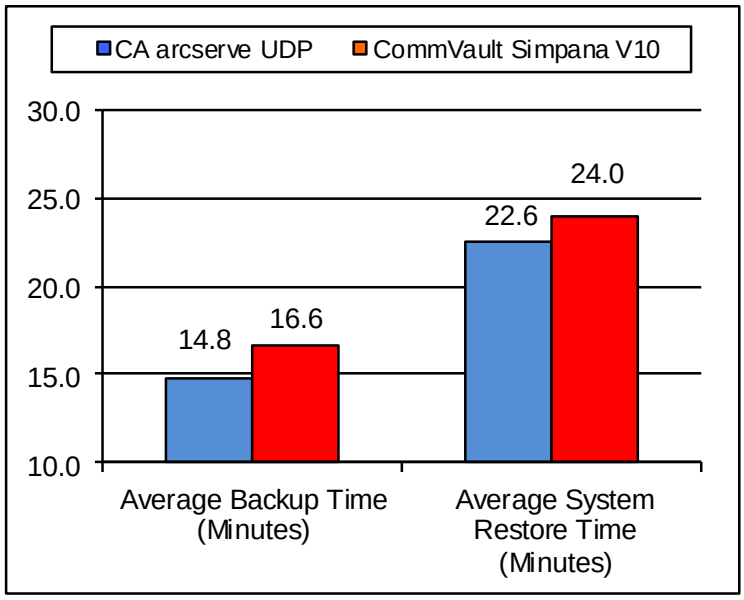

Figure 1.

CA arcserve UDP I^2 vs. Simpana 10 image-based backup/restore performance

CA arcserve also needed 8% less storage space than Simpana 10 (118 GB vs. 128 GB) when we tested the creation of monthly full backups and selected each product's highest level of compression.

In our tests, CA arcserve UDP's I^2 utilized only small, incremental amounts of backup storage after the initial full backup. In contrast, Simpana 10'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 10 (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 (165 GB vs. 447 GB). Figure 2 depicts the resulting storage requirements.

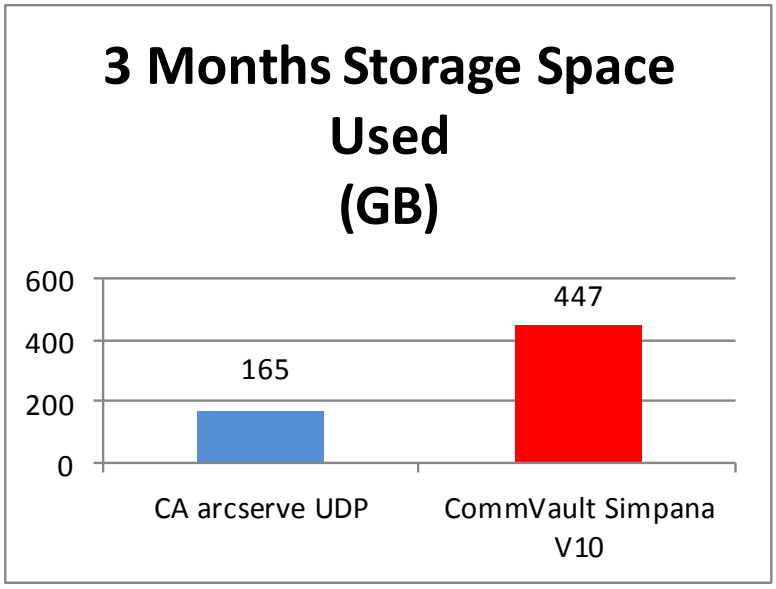

Figure 2.

CA arcserve UDP I^2 vs. Simpana 10 image-based disk storage utilization

Virtualization Support -- Both CA arcserve UDP and Simpana 10 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 UDP 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 UDP'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 UDP's virtual standby works in either physical-to-virtual (P2V) or virtual-to-virtual (V2V) failover modes.

Simpana 10 lacks an automated virtual standby feature. As a substitute, CommVault offers "Virtualize Me," an automated process that can create a VM from a backup copy. "Virtualize Me" is a P2V operation that copies backup data to a VM and then activates that VM.

RTO/RPO Performance Testing – To measure CA arcserve UDP's and Simpana 10'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 2008, 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 UDP in one test and Simpana 10 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 UDP administrator needed just 46 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 10 administrator needed one hour and two minutes** (62 minutes) to accomplish the same thing – **16 minutes longer**. If time is money in your data center, CA arcserve UDP is clearly the tool of choice when disaster strikes.

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 Reporting – CA arcserve UDP's Central Reporting produces much more useful and informative reports regarding disk image recovery points than does Simpana 10.

In the next chart, we take a detailed look at basic, fundamental CA arcserve UDP and Simpana 10 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 10	CA arcserve UDP
Tape device support; integration	5	5
Application support	5	5
Tape archiving, retention and versioning	5	5
Virtual machine protection	5	5
Application-specific granular recovery	5	5
SRM reporting	3	5
Basic backup reporting	4	5
Infrastructure visualization	2	5
Central management	4	5
Deduplication	5	5
Public and private cloud support	5	4
File archiving	5	5
Integration with image-based backups	5	5
Synthetic full backups	3	5
File-based backup features aggregate ranking	**4.3**	**4.9**

File-based Backup Notes

CA arcserve UDP and Simpana 10 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.

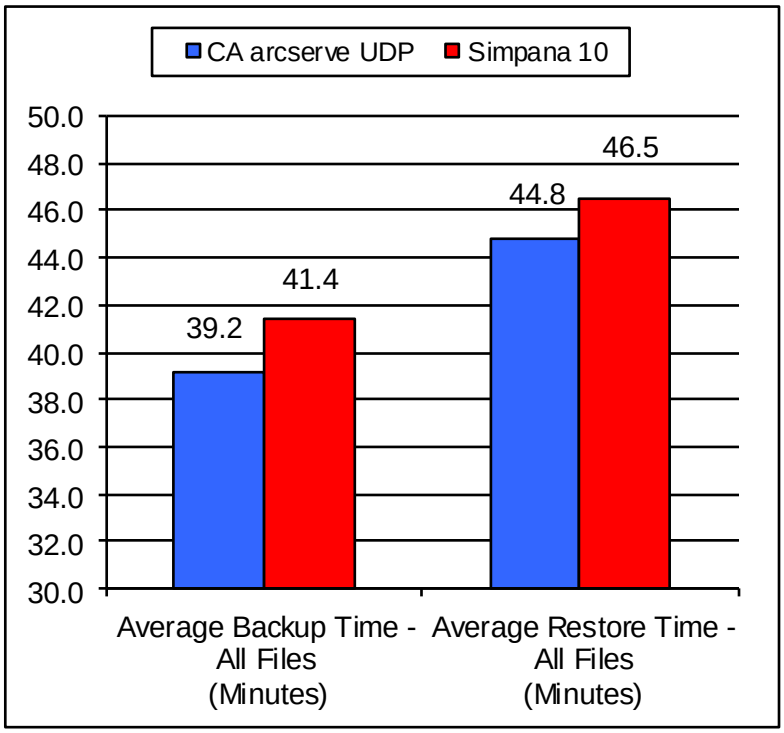

Figure 3.

CA arcserve UDP vs. Simpana 10 backup/restore performance

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

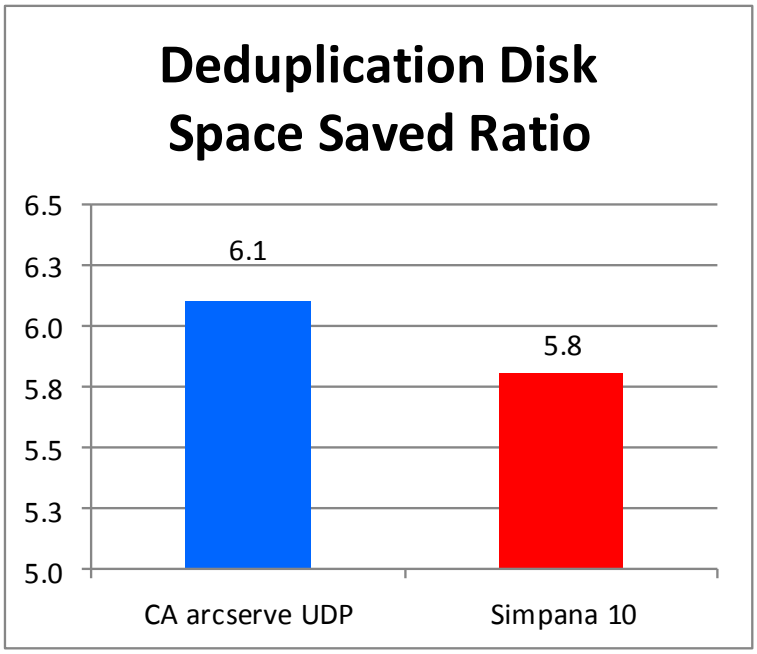

Figure 4.

CA arcserve UDP vs. Simpana 10 data deduplication ratios (higher is better)

Separately for each Storage Policy, Simpana's reports show basic details on backup histories, retentions and storage media usage. The more comprehensive CA arcserve reports provide global views, administration and reporting on all devices, settings and policies (running on-premise and off-premise) that are protected by CA arcserve. These include 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.

For an extra SRM license fee, Simpana 10 produces reports on physical servers and the contents of individual VMs, file-level analysis and physical resource consumption. In 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. And CA does not charge extra for its SRM reports.

In the last features table, let's examine the differences between CA arcserve UDP and Simpana 10 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 10	CA arcserve UDP
Replication	5	5
True high availability (hot failover)	0	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)	2	5
Offline synchronization	5	5
Replication and HA recovery testing	3	5
Network optimization	4	5
Replication and backup integration	5	5
Assessment mode utility	1	5
Application aware replication	5	5
Replication and high availability features aggregate ranking	**3.8**	**4.9**

Replication and High Availability Notes

CA arcserve UDP's replication feature can migrate and manage offsite backups in a scheduled manner. In a real-time, continuous manner, CA arcserve UDP provides true Continuous Data Protection (CDP).

In contrast, Simpana 10's replication feature, Continuous Data Replication (CDR), delivers only "Near CDP" by allowing disaster recovery copies of backup/archive data to be created over a LAN or WAN on a continuous basis. 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 UDP has a High Availability (HA) feature. Simpana 10 can perform replication but does not offer high availability.

Both CA arcserve UDP's and Simpana 10's replication functions perform asynchronous replication and support both Windows 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).

Uniquely, CA arcserve UDP's HA feature includes all the functions that are part of CA arcserve replication and adds the ability to monitor one or more background services running on a server. If a service fails, CA arcserve attempts 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.

Because Simpana's "Near CDP" does not offer high availability, 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 UDP HA 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 related 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 UDP HA goes much further. CA arcserve UDP offers high availability for VMware vSphere, Microsoft Hyper-V and Citrix XenServer. Simpana can merely replicate among 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 manually activate servers within the cluster to complete/finish a failover operation.

CA arcserve UDP Replication and High Availability 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 UDP High Availability 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 **two minutes, 11 seconds** – 131 seconds – to recover from the simulated disaster, after which the administrator had to manually restart the OLTP application.

Rankings Summary

	Simpana 10	CA arcserve UDP
Ease of Use; Overall Features	4.0	5.0
Pricing	2.0	4.0
Image-based backup	4.0	4.9
File-based backup	4.3	4.9
Replication, High Availability	3.8	4.9
Total score	**3.6**	**4.7**

Conclusion

CA arcserve UDP is an integrated, reliable, easy-to-use and scalable answer when disaster happens. CA arcserve UDP 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 UDP costs far less than Simpana 10.

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 T1 and T3 frame relay 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/Win8, 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, Windows 2008 and Windows 2012 servers).

Our virtual computing environments used VMware, XenServer, Red Hat KVM and Microsoft Hyper-V.

A group of four Compaq Proliant ML570 computers, running Windows 2003 Server, Windows 2008 Server, Windows 2012 Server and Red Hat Enterprise Linux, was our test platform for all the products' server modules. A second group of four similar 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.