CA arcserve UDP vs. Symantec Backup Exec 2012

Product Review

A feature-by-feature, in-depth analysis and comparison of CA arcserve UDP and Backup Exec 2012 SP2.

Executive Summary

The following chart shows, at a glance, the significant differences between CA arcserve Unified Data Protection (UDP) and Symantec Backup Exec 2012 SP2.

	Symantec Backup Exec 2012	CA arcserve UDP
Performs faster		✓
Easier to administer		✓
Costs less		✓
High Availability (with true CDP)		✓
Supports several Hypervisors		✓
Scales better		✓
Integrates with more applications		✓
Automated, assured disaster recovery		✓
Built-in replication		✓
Global deduplication		✓
APIs for 3rd party integration		✓

CA has completely retooled CA arcserve. Symantec has, over the past two years, made extensive changes to create the current version of Backup Exec. Both vendors claim to offer the best data protection, disaster recovery and business continuity. Which vendor is correct?

Network Testing Labs has compared the two products, CA arcserve Unified Data Protection (UDP) and Backup Exec 2012 SP2. We evaluated the products' relative merits for performing backup, data recovery, replication and high availability. We examined them, feature by feature and test by test, to provide you with an objective

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

analysis. You can use this report to decide which product will best protect the data in your organization.

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

Symantec Backup Exec 2012 SP2 is a collection of tools whose components are Backup Exec 2012, Symantec System Recovery 2011, a Backup Exec 3600 Appliance and a virtual-only Backup Exec V-Ray Edition. Backup Exec 2012 initially included a Backup Exec.cloud service. However, in January, 2014, Symantec halted the service because Backup Exec.cloud lacked mobile and content-sharing features.

Also, for clarity's sake, note that Symantec has changed the name of its disk-to-disk image-based approach from *"Intelligent Disaster Recovery"* (IDR) to *"Simplified Disaster Recovery"* (SDR). Symantec's disk-to-disk component is *System Recovery 2011*.

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.
- **Data Deduplication –** An RPS can optionally use deduplication to save disk space by storing just a single copy of duplicate data in a backup.
- **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).

Backup Exec 2012 SP2's new features are

- **The New User Interface –** Replaces earlier versions' backup job orientation with a server-centric model
- **New Backup Paradigm –** Simplifies backup job scheduling
- **Guided Restore –** Uses a one-step-at-a-time Wizard to help an administrator restore data
- **Interactive Alerts –** Associates alerts with a source to help you identify a problem server, job or storage device
- **New Storage Setup Wizard –** Step-by-step help in configuring disk, tape, cloud or storage pool backups
- **Simplified Disaster Recovery –** System image (including the OS) backup and restore
- **Convert to Virtual Machine –** for Hyper-V and VMware
- **Automatic Updating of the Backup Exec Software –** Uses Symantec's "LiveUpdate"

- **Minor Reports Improvements –** Color coding, larger fonts, additional data columns and output in either HTML or PDF
- **Improved Search –** Can search for more detail in backup sets
- **New Notifications –** Email or text messages when alerts occur
- **Find Unprotected Data –** Discover data that's not backed up
- **True Image Restore –** Finds and collects latest-changed data when re-assembling a synthetic backup set
- **Checkpoint Restart –** Can restart from point of failure
- **New PowerShell interface –** Command Line Interface (CLI) works with Windows PowerShell
- **Limited Windows Server 2012 Support –** A Backup Exec Server cannot run on Windows Server 2012, the Agent for Windows doesn't work with ReFS volumes and the Agent for Windows doesn't work with a volume for which deduplication has been enabled. Backup Exec 2012 SP2 otherwise supports Windows Server 2012.
- **Windows Server 2012 Hyper-V conversion –** Backup Exec 2012 can participate in the conversion of a physical Windows Server 2012 machine to a Hyper-V host, and the Agent for Hyper-V can back up and restore Windows Server 2012 Hyper-V hosts.
- **VMware Agent –** Contains support for ESX/vSphere/vCenter 5.1.
- **Exchange Server Agent –** Works with Exchange Server 2010 SP3 and, with no granular restore ability, Exchange Server 2013 with Cumulative Update 1.
- **SQL Server Agent –** Works with SQL Server 2008 R2 SP2 and SQL Server 2012 SP1. However, the Backup Exec database cannot be a SQL Server 2012 instance, and specific availability group backup/restore is not supported.
- **SharePoint Agent –** Supports SharePoint 2013, but with no granular restore ability.

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 Backup Exec 2012 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.

In contrast, Backup Exec 2012 offers only a server-centric focus. For example, with Backup Exec 2012's user interface, an administrator must manipulate one or several server backup jobs to add data to a backup set.

Backup Exec 2012 is labor-intensive to use. It forces the administrator to review and analyze backup status information *one server (one backup job) at a time*. Moreover, visualizing Backup Exec 2012 overall backup status requires several navigational steps.

We found navigating and operating the Backup Exec 2012 user interface unproductive and time-consuming.

The overall feature set of CA arcserve UDP far exceeds that of Backup Exec 2012. CA arcserve UDP has ***global*** deduplication, assured recovery, built-in replication, full system high availability/failover, optimized storage and bandwidth, better scalability and a comprehensive set of APIs for 3rd party integration.

Backup Exec 2012 lacks these features.

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.

Backup Exec 2012's deduplication is local, working on only one node at a time. Moreover, Symantec charges extra for Backup Exec 2012's deduplication feature. CA does not.

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.

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).

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 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 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 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.

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.

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 programmatic interface.

Pricing

The following tables show Symantec's and CA's prices for Backup Exec 2012 and CA arcserve UDP. Both products include one year of maintenance.

While the two fee schedules are structured quite differently, our analysis reveals that Backup Exec 2012 costs more yet provides far fewer features than CA arcserve UDP.

For instance, the a la carte purchases of just single (1 copy each) licenses of Backup Exec 2012 Server, System Recovery 2011, Agent for Windows, Agent for Applications and databases, Deduplication Option plus Enterprise Server Option will cost you $9,780.85.

In contrast, CA arcserve UDP Premium Edition for a 6-CPU-socket server is only $7,170, and you additionally get both virtual machine support and replication with CA arcserve UDP.

Backup Exec 2012	MSRP
Backup Exec 2012 Server	$1,162.66 per server
Symantec System Recovery 2011	$1,280
Backup Exec Small Business Edition	$1,162.66 for 3 servers
Backup Exec Agent for Windows – Small Business Edition	$928.96 per server
Backup Exec Agent for Applications and databases	$1,162.66 per server
Backup Exec agent for VMware and Hyper-V	$1,863.76
Backup Exec Capacity Edition	$10,160.11 per Terabyte
Deduplication Option	$1,746.91
Enterprise Server Option (contains ADBO)	$3,499.66
Backup Exec V-Ray Edition - 2 TO 6 CPU cores	$1,887.13
Backup Exec V-Ray Edition - 8 Plus CPU cores	$3,382.81
Backup Exec 3600 Appliance	$15,995 to $25,995
Backup Exec.cloud - hosted sub annual bill - 10GB (*Discontinued*)	$69.96

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

Note that CA arcserve includes deduplication, archiving, Active Directory granular restore and synthetic full backup at no extra charge.

In the next section, you get a detailed evaluation of the image-based backup and recovery capabilities of CA arcserve UDP and Backup Exec 2012.

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	Symantec Backup Exec 2012	CA arcserve UDP
Snapshot/image backup technology	3	5
Operating System support	3	5
Device support	5	5
Data deduplication	0	5
Virtual server & client support	4	5
Physical <–> virtual server support	3	5
Cloud support	0	5
RTO/RPO (for disaster recovery)	2	4
Granular recovery	4	5
Off-site replication of images	5	5
Bare Metal Recovery (BMR)	5	5
Virtual standby for cold-failover	0	5

Feature	Symantec Backup Exec 2012	CA arcserve UDP
Client/workstation support	5	5
Image archiving, retention and versioning	5	5
Centralized management	5	5
Centralized reporting	3	5
SaaS subscriptions with cloud storage	0	5
RMM integration for MSPs	3	5
Image-based backup features aggregate ranking	**3.1**	**4.9**

Image-based Backup Notes

CA arcserve UDP and Backup Exec 2012 can each produce – and restore from – image-based backups. Both use similar underlying technologies to intercept operating system write operations and transfer copies of written data to a destination. Both can create image-based snapshots as often as every 15 minutes.

However, CA arcserve UDP has a number of significant advantages over Backup Exec 2012. CA arcserve UDP is faster, uses less storage space, adheres better to industry standards, supports more virtualized environments, offers virtual standby, supports cloud environments and has more useful, informative reports. Moreover, CA arcserve UDP is far easier to use than Backup Exec 2012, which means administrators will be happier and Total Cost of Ownership (TCO) will be lower.

Both products offer synthetic backups, in which a full backup is assembled, or synthesized, from a baseline full backup and subsequent incremental backups.

CA arcserve UDP needs to create a full backup just once, for the first backup operation. Thereafter, CA arcserve UDP can use its patent-pending ***Infinite Incremental (I^2 Technology)*** to perform only incremental backups for all subsequent backups. I^2's sophisticated design intelligently manages the backing up of only the blocks of data that have changed since the previous backup. I^2 presents a consolidated point-in-time view of the protected volume for multiple recovery types, thus reducing recovery times and costs.

Symantec terms its synthetic backup ***Advanced Disk-based Backup Option (ADBO)***. Unfortunately, ADBO users must periodically create a new full backup (ADBO's scheduling options for starting a new recovery point set, or base, are weekly, monthly, quarterly or yearly). I^2, on the other hand, does not have this limitation – hence the name "Infinite Incremental."

The "Advanced Disk-based Option" is expensive. It's only available as part of Symantec's Enterprise Server Option (which adds $3,400 to Backup Exec's list price).

I^2 is faster than ADBO and uses less storage space. For a complete system comprising 300 GB, Figure 1 shows the relative performance of CA arcserve UDP's I^2 and Backup Exec 2012's ADBO.

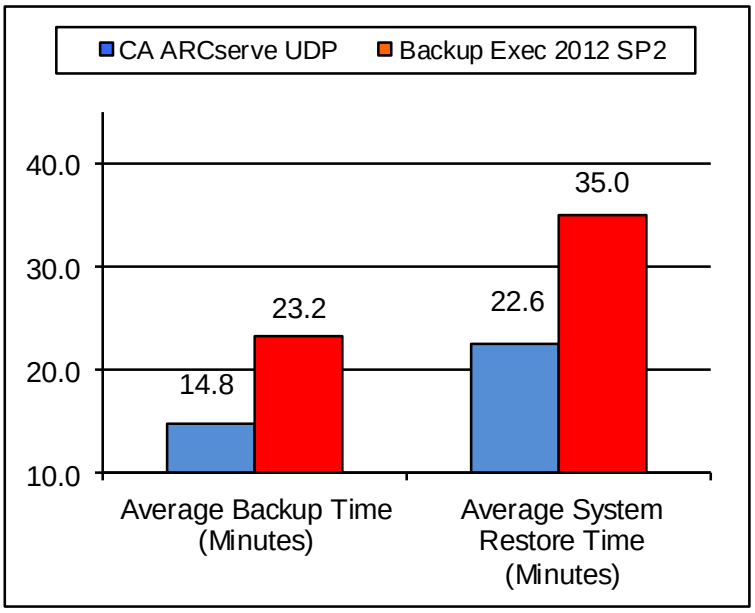

Figure 1.

I^2 vs. ADBO backup/restore performance

CA arcserve UDP also used 14% less storage space than Backup Exec 2012 (120 GB vs. 137 GB) when we tested the creation of monthly full backups and used each product's highest level of compression. (ADBO has 4 compression levels for the recovery point: None, Standard, Medium and High. I^2 has 3 levels: None, Standard and Maximum.)

Using infinite incrementals (one full backup at the outset and incremental thereafter) – but telling Backup Exec 2012 to continue creating monthly full backups with incrementals during the month – we saw that I^2 used about half ADBO's space at the end of two months (144 GB vs. 290 GB) and about a third of ADBO's space at the end of three months (165 GB vs. 463 GB). Figure 2 depicts the resulting storage requirements.

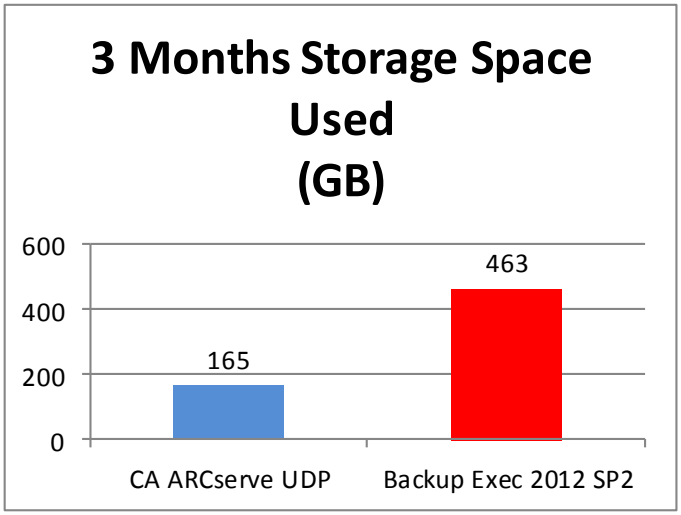

Figure 2.

I^2 vs. ADBO disk storage utilization

ADBO's administration is a bit more sophisticated than its predecessor. For instance, it has a "Limit the number of recovery point sets saved for this backup" option, which limits the number of recovery point sets that can be saved for this backup. Symantec says, "*You can limit the number of recovery point sets to reduce the risk of filling up the hard drive with recovery points. Each new recovery point set replaces the oldest set on your backup destination drive. This option appears only if you are creating a recovery point set.*" Managing older backup sets used to be a manual affair in Backup Exec 2010.

System Recovery 2011 by itself, without ADBO (via the purchase of Enterprise Server Option), can only do whole-system image backups. It can't do incremental backups. System Recovery 2011 is perhaps useful to people who make ad hoc full backups before installing or upgrading software and who perhaps use (large) flash drives as backup media. It's otherwise quite useless.

Note that Backup Exec 2012 can select only file system data for synthetic backup.

Backup Exec 2012's image-based backups use either "Symantec Volume Snapshot Provider (VSP)" or Microsoft Volume Shadow Copy Server (VSS), with "hardware provider" as a first option and "system provider" (VSS software) the secondary option. CA arcserve UDP's approach employs the industry-standard Microsoft Volume Shadow Copy Server (VSS).

Virtualization Support
While Backup Exec 2012 only supports VMWare ESX and Microsoft Hyper-V, CA arcserve UDP supports VMware ESX and vSphere, Microsoft Hyper-V, Citrix XenServer and 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 providing 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. And CA arcserve UDP's virtual standby works in either physical-to-virtual (P2V) or virtual-to-virtual (V2V) failover modes.

Backup Exec 2012 has Virtual Machine Auto-Recovery for VMware, which attempts to automatically restore a failed virtual machine in order to recover lost application services. However, this restricted-to-the-local-virtual-server action is little help in a disaster recovery situation.

Cloud Support – Backup Exec 2012's limited cloud support worked initially just with Nirvanix Storage Delivery Network. Unfortunately, Nirvanix filed for bankruptcy late in 2013. Symantec says it is looking for an alternative cloud provider. In contrast, CA arcserve UDP's data protection approach provides automated copying and archiving of critical files to Amazon's AWS S3 and Windows Azure clouds after image-based backups complete. After the first file copy to the cloud, only incremental changes are transmitted thereafter.

RTO/RPO Performance Testing – To measure CA arcserve UDP's and Backup Exec 2012'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 UDP and Backup Exec 2012 made 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 Backup Exec 2012 in another test, the 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 administrator needed just 45 minutes to restore data to the servers and resume the OLTP application using CA arcserve UDP. With Backup Exec 2012, the administrator needed one hour and eight minutes (68 minutes) to accomplish the same thing – 23 minutes longer. If time is money in your data center, CA arcserve is clearly the tool of choice when disaster strikes.

Note that Backup Exec 2012's user interface for dealing with disk images is cumbersome. Also, CA arcserve UDP's Central Reporting produces much more useful and informative reports regarding disk image recovery points than does Backup Exec 2012's Central Administration Server. However, both products integrate with Windows Explorer to show the contents of an image file as a mountable drive letter.

Backup Exec 2012's image-based component has a few other limitations we found annoying. When recovering a Backup Exec 2012 server, the Recover This Computer Wizard could not restore data from a local deduplication storage device. And SDR could not recover a deduplication storage folder.

If you use SDR to recover a Backup Exec server that contains a deduplication storage folder:

- Any existing backup sets that were sent to the deduplication storage folder after it was backed up cannot be restored
- The deduplication storage folder may not be in an operational state after the recovery

Crucially, backups from previous versions of Backup Exec cannot be restored using SDR.

In the next chart, we take a detailed look at basic, fundamental CA arcserve UDP and Backup Exec 2012 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	Symantec Backup Exec 2012	CA arcserve UDP
Tape device support	5	5
Application support	5	5
Tape integration	4	5
Tape archiving, retention and versioning	5	5
Virtual machine protection	4	5
Support for application-specific granular recovery	5	5
SRM reporting	2	5
Basic backup reporting	3	5
Infrastructure visualization	1	5
Central management	3	5
Deduplication	3	5
Cloud support	0	4
File archiving	5	5
Integration with image-based backups	5	5
Synthetic full backups	5	5
File-based backup features aggregate ranking	**3.7**	**4.9**

File-based Backup Notes

CA arcserve UDP and Backup Exec 2012 have similar file-based backup features. They both support the same operating systems, applications and backup devices. CA arcserve UDP has advantages over Backup Exec 2012, however, in its reporting, its infrastructure visualization, its central management console and its sophisticated backup job scheduling. CA arcserve UDP was also faster than Backup Exec 2012 in our

tests, and its data deduplication was more efficient. Figures 3 and 4 graph the relative performance of the two products.

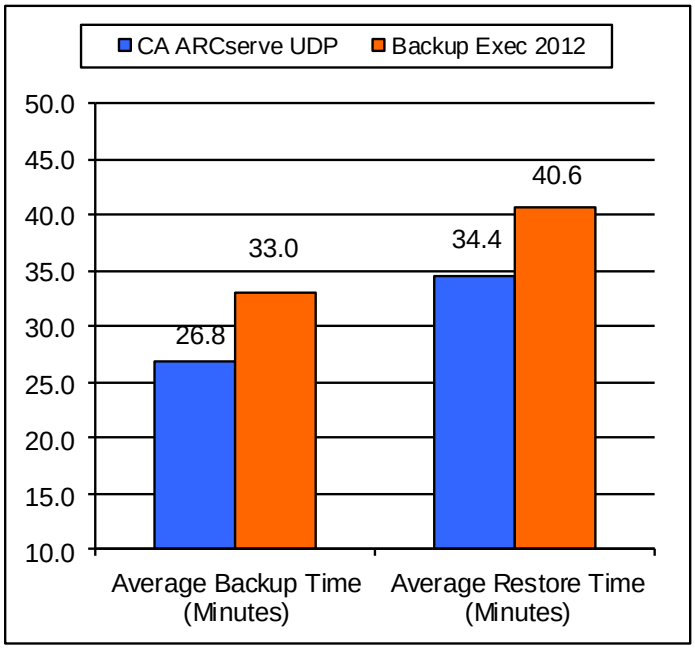

Figure 3.

CA arcserve UDP vs. Backup Exec 2012 file-based backup/restore performance

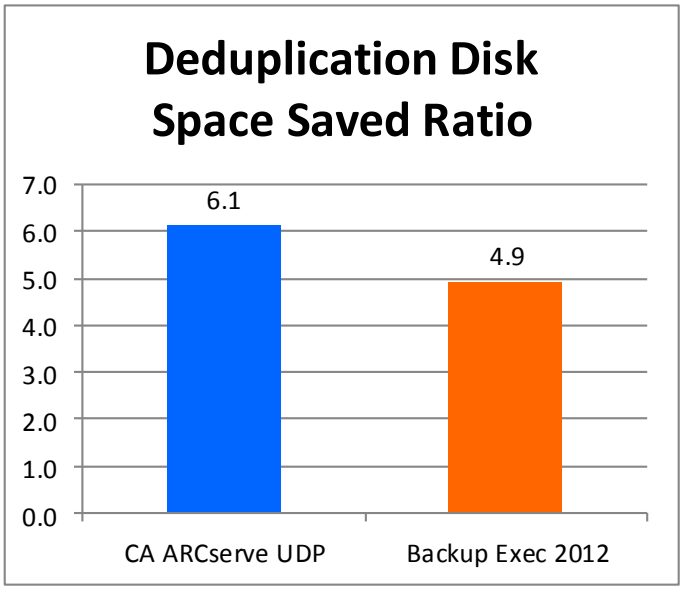

Figure 4.

CA arcserve UDP vs. Backup Exec 2012 data deduplication ratios (higher is better)

CA arcserve UDP and Backup Exec 2012 both have native D2T and D2D2T support, but Backup Exec 2012 offers only rudimentary scheduling options. For example a Backup Exec 2012 customer cannot schedule tiered jobs over time. CA arcserve UDP offers advanced tape management and scheduling options.

CA arcserve UDP'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. Unfortunately, Backup Exec 2012's unremarkable SRM reporting is lackluster and little-changed from the previous version, Backup Exec 2010.

Backup Exec 2012's basic reporting capabilities are the same as Backup Exec 2010's, with very minor changes (color highlighting of titles, larger fonts, a few new data columns and output in either HTML or PDF format). In contrast, CA arcserve UDP provides global views, administration and reporting on all devices, settings and policies (both on-site and off-site) protected by CA arcserve UDP. It gives both detailed reports and a summary report view that clearly show the overall status as well as individual details for any and all backup operations.

While Backup Exec 2012 has virtually no infrastructure visualization capability, CA arcserve UDP's topology map clearly and intuitively displays a customer's infrastructure. By node, virtual machine or device, CA arcserve UDP graphically presents a hierarchical picture of data backup sets.

Backup Exec 2012 can perform data deduplication only locally, at either a server or a client node. CA arcserve UDP's deduplication is global, across all nodes. Moreover, Backup Exec 2012's deduplication feature is an extra-charge option. CA arcserve UDP includes deduplication at no extra charge.

Backup Exec 2012's job scheduling is far less sophisticated than CA arcserve UDP's.

For example, suppose a user needs to set up the following backup schedule:

- Daily incremental backups, Monday throught Thursday, at 6 PM
- Weekly full backups on Friday at 6 PM
- Monthly full backups on the last Friday of the month at 6 PM

In this example, the user wants to schedule duplicate-to-tape jobs on Monday at 6 AM following the last full backup. (The user doesn't want to have D2D and D2T jobs competing for I/O and thus prolonging the backup jobs). Backup Exec 2012's new server-centric user interface has no facility for scheduling the duplicate jobs to run on the Monday following the last full backup. CA arcserve UDP's advanced scheduling feature handles this situation with ease.

Regrettably, Symantec has dropped support in Backup Exec 2012 for:

- Earlier versions of Windows
- One Button Disaster Recovery
- Symantec Online Storage for Backup Exec (SOSBE)
- Replication Exec
- Backup Exec Continuous Protection Server
- Agent for SAP
- A variety of reports
- Macintosh OS 10.4
- Some user interface features (barcode, media labeling and copying jobs to other media servers), which are now available only via the command line interface

In the last features table, let's examine the huge differences between CA arcserve UDP and Backup Exec 2012 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	Symantec Backup Exec 2012	CA arcserve UDP
Replication	0 (Not available in or integrated with Backup Exec 2012)	5
True high availability (hot failover)	0	5
Physical and virtual server support	0	5
Operating System and application	0	5

Feature	Symantec Backup Exec 2012	CA arcserve UDP
support		
RTO/RPO (for disaster recovery)	0	5
Cloud Integration	0	4
Continuous Data Protection (CDP)	0	5
Offline synchronization	0	5
Replication and HA recovery testing	0	5
Network optimization	0	5
Replication and backup integration	0	5
Assessment mode utility	0	5
Application aware replication	0	5
Replication and high availability features aggregate ranking	**0**	**4.9**

Replication and High Availability Notes

Backup Exec 2012 completely lacks replication or high availability and thus scores zero for this entire category.

CA arcserve UDP's replication may be used in a scheduled manner to migrate backups offsite and may be used in a real-time, continuous manner for continuous data protection (CDP). Additionally, for companies needing maximum system uptime and availability, a High Availability (HA) feature is available.

CA arcserve UDP's replication performs asynchronous replication and supports both Windows and Linux environments. It may be deployed onsite, offsite and linked to Amazon's (AWS/EC2) cloud.

CA arcserve UDP's High Availability includes replication and adds the ability to monitor one or more 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 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 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 it happened.

CA arcserve UDP 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 UDP 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 UDP offers push-button failover and failback for the highest possible level of availability.

CA arcserve UDP replication and High Availability protect both physical and virtual servers. They offer host-level and VM-level protection for Hyper-V and offer VM-level protection for VMware and XenServer. Furthermore, CA arcserve UDP can replicate between physical and virtual servers (P2P, P2V, V2V and V2P) and even between virtual server platforms.

CA arcserve UDP 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 UDP already knows what specific directories and files to replicate and when – you just indicate which applications to protect. Moreover, CA arcserve UDP supports DAS, NAS and SAN, and it can replicate data in a variety of ways – one-to-one, one-to-many and many-to-one.

When we measured RTO/RPO by performing the same disaster recovery test with CA arcserve UDP's High Availability feature that we'd done with CA arcserve UDP's image-based feature (*see RTO/RPO section above under Image-based Backup), **CA arcserve UDP needed just six seconds to automatically restart the OLTP application** at the remote backup site. Backup Exec 2012 has no high availability feature and thus forfeited the test.

CA arcserve UDP also includes an easy-to-use assessment mode tool for performing "what if" dry runs to assure you have adequate bandwidth for replication. It also offers an automated recovery testing feature, CA arcserve UDP Assured Recovery, that 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.

CA arcserve UDP can perform cloud-based data replication or cloud-based full system replication. Fully integrated with Amazon's AWS EC/2 for disaster recovery, CA arcserve UDP can use the cloud for storage and then, upon failover, "stand up" a virtual machine with current data and the current system state.

Rankings Summary

	Backup Exec 2012	**CA arcserve UDP**
Ease of Use; Overall Features	3.0	5.0
Pricing	3.0	4.0
Image-based backup	3.1	4.9
File-based backup	3.7	4.9
Replication, High Availability	0	4.9
Total score	**2.6**	**4.7**

Conclusion

CA arcserve UDP is an integrated, reliable, easy-to-use and scalable answer when disaster happens. It works with more operating systems, more virtual environments and more applications. It supports cloud data storage. CA arcserve UDP is less expensive, and, as you've seen, is far more feature-complete.

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

Vendor Contacts

CA 800-225-5224	www.arcserve.com
Symantec 800-721-3934	www.symantec.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 2000/2003/2012 and Windows Vista/7/8, 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 consisted of VMware, XenServer and Microsoft Hyper-V.

A group of four Compaq Proliant ML570 computers, each with four 900 Mhz CPUs, 2G bytes RAM and 1.3 T bytes hard disks and 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.