Attention: Field /Partner Teams **Publish Date: 3/24/2010**

Announcement:

The Simpana 8.0 Virtual Server Agent iDA (VSA) is now available with the March 2010 Post-Pack which provides backup and restore of VM infrastructure on the vSphere 4.x platform using the vStorage API for Data Protection (VADP). The update is available to existing licensed/active support sites through the Maintenance Advantage download site. As with normal update release schedules it will begin as a download update category and will progressively move to an automatic update/FTP option for broad distribution around a month later.

Recommendation to Users:

This new update enables VSA users on VMWare's vSphere 4.x infrastructure to switch from the VCB tools/methods and convert to optimized VSA data protection operations using a new direct integration with the new vStorage API for Data Protection (VADP). This important change converts VSA users to the optimized configuration for higher scale/performance data protection and recovery methods, as well as aligns with VMware's new aggressive promotion campaign to drive customers to the vSphere v.4.x infrastructure. As you know, our customers have; seen recent announcements posted in the field where VMware has announced the complete elimination of the VCB tool set in near-term ESX releases.

- CommVault Simpana VSA 8.0 fully aligns and supports the preferred backup/restore methods promoted by VMware field and corporate teams.
- The CommVault VSA offers optimal protection solutions for VMware customers on 4.X virtual infrastructures with VADP and for customers on 3.5.X virtual infrastructures with VCB tools.
- The update also includes an enhancement which significantly speeds up the VM autodiscovery inquiry process used by the VSA to check with the Virtual Center server and determine if any new VMs have been added into the monitored area which meet the subclient policy discovery/auto-add selection criteria.

VADP is the second generation of optimized backup methods offered by VMware and the most important improvement is the elimination the VCB requirement to copy whole images of VMDKs/VMs to a cache area for processing by a backup server. Although the Simpana 8.0 VSA agent offered market leading features to overcome many of the complexities and operational overload conditions that quickly emerge in a VCB aligned configuration, the new VADP eliminates those challenges by switching to a snap/mount method on the –disk policies similar to the methods VSA introduced last year in –volume protection policies. The new direct integration method therefore simplifies configurations of the VSA protection node network and produces faster backup and restore jobs as indicated in the comparison table below.

New operational benefits of using VSA-VADP over VSA-VCB -disk B/R methods		
	vStorage 4.x VADP (-disk)	**VMware 3.5 VCB (-disk)**
1. Simplified VSA agent/client configurations, fewer resources needed	**Smaller** – The VSA server no longer requires additional landing free space allocation and the user should not need to repoint the Job Results folder to a dedicated volume on Faster disk. This new configuration is suitable for use in a HotAdd VM client which can serve as the virtual backup server(s).	**Larger** – The VCB proxy will require free landing space under the job results folder to serve as the disk image cache space for processing VSA backups/restores. The general recommendation is to move that folder to a dedicated volume on faster disk to improve performance.
2. Faster backup operations by eliminating copy to cache	**Shorter window, faster jobs** - With VADP integration, the data is snapped/mounted and read directly from the data store without copying it to a temporary location on the VSA Server. This results in much faster backups and eliminates the need to provision extra disk space on the VSA server.	**Longer window** - With VCB disk level backup, the virtual machine image is copied twice; first from the data store to the VCB Proxy server/VSA agent and then from the Proxy to the backup target. This doubles the amount of time taken to backup virtual machines and requires a more reserved disk space on the VSA agent cache. After processing the VMDKs are purged.

New operational benefits of using VSA-VADP over VSA-VCB -disk B/R methods		
	vStorage 4.x VADP (-disk)	**VMware 3.5 VCB (-disk)**
3. Change Block Tracking for fast incremental backup	**Faster, optimized performance** – The VADP engine employs a new Change Block Tracking method that keeps track of changed blocks within the virtual machine VMDK since the last backup. This allows the VSA agent to more quickly identify changed blocks, leading to faster incremental backups with only changed data being transferred to the backend.	**VCB optimized** - Without VADP integration, Simpana VSA can still perform incremental changed block backups. However, it uses its own algorithm based on CRC to determine changed blocks, which does add more incremental processing time. This method is most important in non-VADP environments. When VADP-CBT is available we automatically shift to that method to drive up incremental backups performance.
4. Faster restore eliminating the need for VMConverter	**Faster, direct restore performance** –Our new VADP integration allows a Virtual Machine to be directly restored into a data store leading to much faster full VM restores. This eliminates any need to use the VMConverter.	**Automatic (two step) restore method** – When restoring a full VCB VM, the data must first be restaged to the VSA proxy server so it can be used with the VMConverter to redirect the restore to the VI data store. VMConverter is not required for Container restore or granular file restore.

All customers implementing CommVault's VSA on vSphere 4.x environments are requested to download the new Post-Pack/update from Maintenance Advantage and follow the instructions outlined in the associated *.readme file(s). Any field teams looking to sponsor testing, a POC or implement production sites on this combination should consult the feature support matrix listed in the following section and ensure the user/partner has access to the new media kits or installer packages outlined in this document.

Feature Support—Simpana 8.0 VSA support for VADP (as of March 2010):

The table below summarizes the available support for the VMware vStorage API (VADP) relative to the Simpana 8.0 Virtual Server agent. Formal updates to Books-On-Line (BOL) are in process and will follow the release of the new updates that are available to the general public.

VMware VSA Support	*Use-Case*	*Availability*
Certified integration with vSphere 4.X generation VADP	Optimized data protection of VMware 4.X environments using full integration with VADP (vStorage API) eliminating all VCB components from CVLT backup and restore operations • Applies to all Disk-level, Volume-level and File-level backup policy types	Supported with Post-pack March 2010 (update 16759)
	Full VSA + VADP restore support for: • Full VM Restore, Container Restore and File restore from single pass disk-level backup. • VMDK and File Level restore from volume-level backup • GH-W, File restore from file level backup	Supported with Post-pack March 2010 (update 16759)
Certified integration with VMware 3.5 generation VCB	Optimized data protection of VMware 3.5 environments using full integration with VCB (VMware Consolidated Backup tools). • Applies to all Disk-level, Volume-level and File-level backup policy types	Currently supported with 8.0, including latest updates post SP4
	Full VSA + VCB restore support for: • Full VM Restore, Container Restore and File restore from single pass disk-level backup. • VMDK and File Level restore from volume-level backup • GH-W, File restore from file level backup	Currently supported with 8.0, including latest updates post SP4
VSA-Disk backup with file level granular restore	Single pass backup with granular file restore, supported from –disk, -volume, or –file level backups of windows guest host VMs.	Currently supported with 8.0, new restore performance enhancements were added in SP4
	Extend single pass granular file restore to Linux GH from same consolidated VSA agent (installed on Windows OS).	Roadmap Planning Item
VSA – SnapProtectionEnabler (SPE) integration	Engage SBE to capture a persistent snapcopy (HW/SW) of the VMDK collection for rapid recovery and employ the VSA backup processing to work from the snapped image (cataloging, changed block extraction to secondary backup copies)	Roadmap Planning Item

Simpana 8.0 VSA Update Download / Installation Package Availability:

The new update included in the post-pack should be installed on a baseline 8.0 SP4 CommCell. After delivery of SP4 in normal release lifecycle, CommVault shifts beyond a quarterly planning period to longer cycles as the frequency of new updates begins to slow. In this phase, we normally release periodic “post-pack” rollups of specialized updates that should be applied over the most recent service pack; SP4 in this case.

Configuration Requirements for New Feature Support:

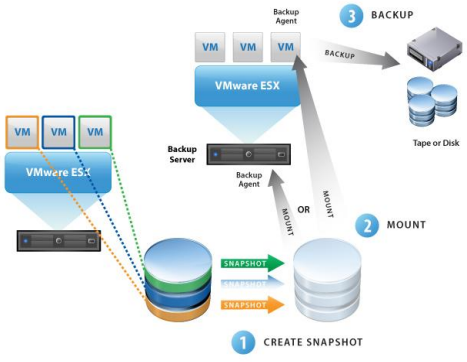
1. Media Kit – Although the VSA installer has not changed, CommVaultrecommends using the latest "R.8. Published January 2010 Edition" DVD1. The new physical media kit for isavailable all distribution outlets to the SEs, Partners and Customers including through Electronic Software Download on Maintenance Advantage. This kit includes the new installer collection and SP4.
2. Updates – Software updates are applied to the prescribed baseline installation / SP to enable new options and features in the Simpana application. Future service packs will generally roll those updates into a cumulative update package which can be used with the automatic updates option to simplify deployment across the common technology engine.

- Post-Pack March 2010 / Update 16759 – This update is applied to the VSA agent client server to add the new VADP option. The update must be applied to a baseline 8.0 SP4 platform. The option is engaged by creating the registry key **VirtualServer\VStorageEnable** must be created (DWORD) and set to 1 to enable vStorage API method.
- This method only applies to VMs running on an vSphere 4.x ESX server which includes the VADP/vStorage SDK. Under Simpana 8.0, the SDK must be downloaded and installed manually to each the VSA server. The download is posted on Maintenance Advantage downloads under the "VDDK" package.[1] The SDK is available on all vSphere Editions with the exception of the free distribution (ESXi)[2]. BOL will provide a step-by-step recommendation.
- Consideration: To achieve the full benefits of the new supported features on the Virtual Machine backups/retores the current collection should be converted to Virtual Machine hardware version 7 types (optimized for ESX 4.0 and VMware server 2.0). Earlier VMs that are version 4 types will not exercise all of the new VM features such as CBT or VMConverter-free restores.[3] Please see the Q&A section for an example that illustrates how to change the VM hw version type.

Background—VMware vSphere 4.x VADP Architecture:

The new VADP option shifts the backup process to use a quiesce / snap / mount method that allows the Virtual Server agent to directly process the data within the Virtual Infrastucture. That eliminates the latency and complexity of the VCB copy to cache and VMConvert-oriented restores.

Figure 1: VADP vStorage Method



Under VADP, the VSA subclient will use the normal sequenced process to backup each VM in the policy using the multi-stream approach. The VM will be quiesced, triggeringthe (1) Create Snapshot action in VADP, (2) that snapped set of VM data files is then directly read by the VSA backup service and (3) we will process out the whole image on Full jobs or changed blocks on Incremental jobs, catalog/index the contents and send the data/indexes to the Storage Policy primary copy. [4]

[1] The download includes file (VMware-vix-disklib-1.1.1-2107031.i386VMware-vix-disklib-1.1.1-207031.i386.exe)

[2] Please review this link for further details on VADP - http://www.vmware.com/products/vstorage-apis-for-data-protection/

[3] Please refer to Chapter 13 Upgrading Virtual Machines for more details;
http://www.vmware.com/pdf/vsphere4/r40/vsp_40_upgrade_guide.pdf

[4] Refer to http://www.vmware.com/products/vstorage-apis-for-data-protection/ for more details on VADP

In restore operations, unlike VCB which required sub-component VMDK image files to be reassembled on the VSA for restore with the VMConverter tool, the new VADP offers a direct access, faster restore method. The VSA agent selects the contents for restore based on the user browse selections and copies through the data as it is handed back across the VADP to effect the restore. All restore options are consistent with both methods, however the VADP method is more optimized, requires less intermediary resources and produces faster results.

It is important to understand that VADP does improve portions of the data flow process but a host of operational challenges normally exist in protecting virtual environments. As environments expand their virtual infrastructures operational becomes the larger burden and scale constraint.

Virtual Environments present significant data protection challenges including

- Huge operational burden as users spend significant amount of time manually discovering new VMs and ensuring they are protected in the correct way;
- Ensuring the backup workload does not overwhelm the already optimized physical server, storage and network resources; and
- Balancing DR and Granular Recovery Needs with Long term retention while controlling storage cost and providing fast Recovery SLAs.

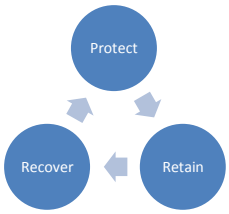


Figure 2: Data Recovery Lifecycle

While the method of copying data from the virtual platform is important, focusing too much on the copying mechanism distracts from the larger data management, retention and recovery challenges.

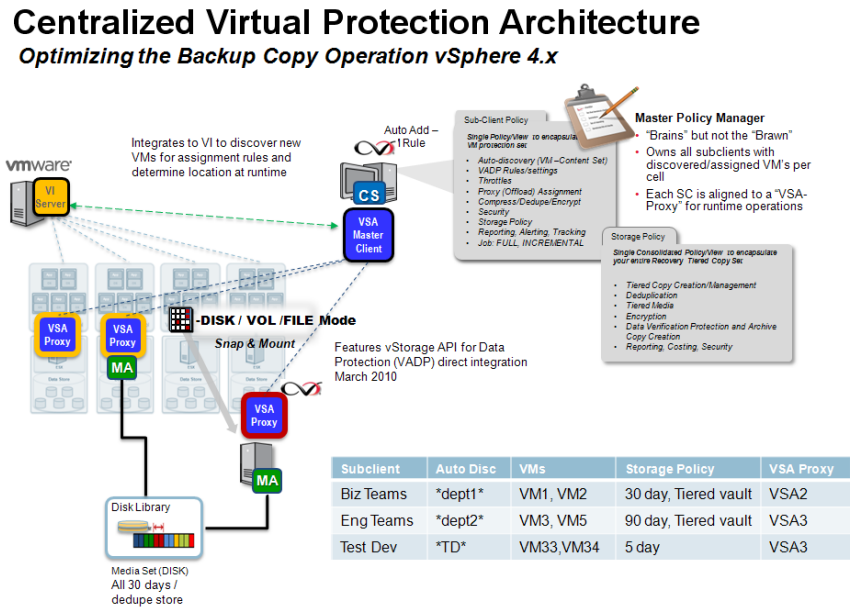
CommVault Simpana, and the Virtual Server Agent, implements a solution framework that spans an end-to-end data protection lifecycle to meet recovery objectives and operational budget constraints with maximum efficiency. The data recovery lifecycle is a measureable, repeatable process composed of three interrelated elements; **backup phase**, **retention phase** and **recovery phase**. The Simpana Virtual Server Agent transcends a simple backup job and touches all the dimensions that drives higher efficiency at each phase, reduce operational complexity, and flexibly scales with business needs for higher returns on investment.
CommVault Simpana software and the Universal Virtual Server Agent help organizations protect critical virtual server information assets, while reducing operational overhead, improving manageability and scalability, simplifying granular and DR recovery operations and enhancing backup storage utilization:

- Auto-discovery combined with auto-protection, helps ensure virtual machines are fully protected with minimal administrator intervention;
- Leverage high resiliency and concurrency for scalable backup operations within shrinking backup windows. Built-in protection options distribute backup workload across physical servers, datastores and networks for optimal resource utilization;
- Flexible, centralized virtual machine protection, without having to install client software on individual virtual machines.
- Utilize Granular Recovery or Full VM recovery from single pass backup to meet Service Level Agreements – which includes rapid granular restore from any backup tier (disk/tape/cloud) without needing to restage entire VM images in temporary disk caches.
- Optimized backup storage utilization through the use of innovative features, such as block-level incremental image level backup and embedded deduplication

Best-Practice—Simpana 8.0 Virtual Server Agent

Use-case: VMware Centralized Protection Policies

One of the unique features of the Simpana VSA agent is the ability to deploy in a hierarchial relationship where one master VSA client is deployed centrally and uses auto discovery against the Virtual Center server to find VMs and assign them to an appropriate backup subclient policy based on the classification/collection rules. That subclient can be used to associate groups of VMs under distinct protection policies that may have different security needs, retention rules, data processing options – such as deduplication, encryption, compression – and assign that group to a secondary VSA server to run the actual backup jobs.



The master VSA server consolidates policy administration and controls the assignment of the operational workloads to the secondary VSA server. The master VSA server can even be installed on the CommServe server to take full advantage of the availability / failover used on that server. The VSA-master is a policy-only agent, all backup data movement paths run through the secondary VSA clients. This minimizes the burden of managing a fluid virtual infrastructure by employing subclient/discovery/collection policies.

The secondary VSA servers can be viewed as a coordinated collection of virtual backup server nodes that are now best suited to use HotAdd VM-W to host the VSA agents, when matched with VADP integration to deliver high performance and scalability. In this configuration, the secondary VSA agents do not have any local subclient policies configured. Rather they are are tethered to the subclients defined under the master VSA server.

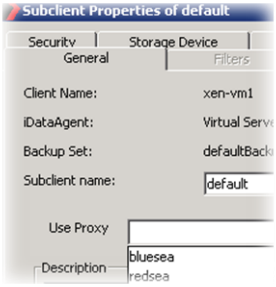


Figure 2: VSA Subclient - Proxy designation

Each subclient policy offers the standard VSA operational tuning controls, such as the number concurrent readers threshold that are used to balance the number of parallel VM backed up simultaneously when the subclient job runs. With VADP eliminating the VCB copy to cache step, the VM backup collection will process much faster since each VM is snapped/mounted/read directly by the VSA agent reducing the span of the operational window. As the subclient backup job is executed, the agent will start selecting sets of VMs to process up to the number of readers, as a VM finishes the backup operation, the agent will select the next VM and automatically work down the content list in the subclient policy. This feature simplifies the administration of backup policies as VMs can be grouped based on

business or retention/ recovery needs while ensuring the operation runs efficiently with normal restartabilty, reporting and alerting conditions.

The VADP configuration is best suited to employ virtualized Windows guest host servers for each VSA server which reduces the infrastructure cost of the protection solution. The initial sizing recommendation for typical VM infrastructures suggests using a 50 VM to 1 VSA Server ratio to begin. This ratio may be increased as you deploy the solution and run/measure it under production loads by adding more VMs to the VSA Server subclient or by associating multiple subclients to the same VSA agent. As with any good architecture process the design should consider data volumes, change rates, concurrent streams/readers, operational loads in context of the user's environment.

Note: When using legacy VCB, sizing recommendation is 25 VM to 1 VSA server ratio when the VSA server is on a virtual machine. Also recommend a 2 VSA to 1 MA ratio in this config.The ratio is higher when the VSA is a physical box.

Depending on the environment, resource availability, and throughput needs, MediaAgents can either be virtual or physical servers. The Virtual Protection bundles in the Pricebook include all components necessary to protect virtual environments, regardless of which configuration is selected for implementation.

In an all virtual environment, MediaAgents can be collocated on the VM hosting the VSA servers. When the MediaAgent is a virtual machine, it is critical that the virtual server meets the prescribed CPU, memory and network requirements as described in BOL. When deduplication is added, the DDB volume is a critical component to design for performance. The DDB can be hosted on dedicated physical MediaAgents that function as DDB managers. Alternately, in smaller deployments, DDBs can be hosted on virtual MAs, however, it is important to ensure that the DDB volume meets performance requirements as detailed in the Dedupe Architecture Guide. In general, RDM volumes perform better as DDB volumes vs. VMFS volumes. Always run the deduplication simulator tool to determine a more accurate estimate of the DDB volume performance. At this time, it is not recommended to perform backups to tape when MA is a virtual machine, due to incompatibilities between tape hardware and virtual servers. Additional guidance on connecting tape drives to virtual servers will be provided in the future as the option becomes more prevalent.

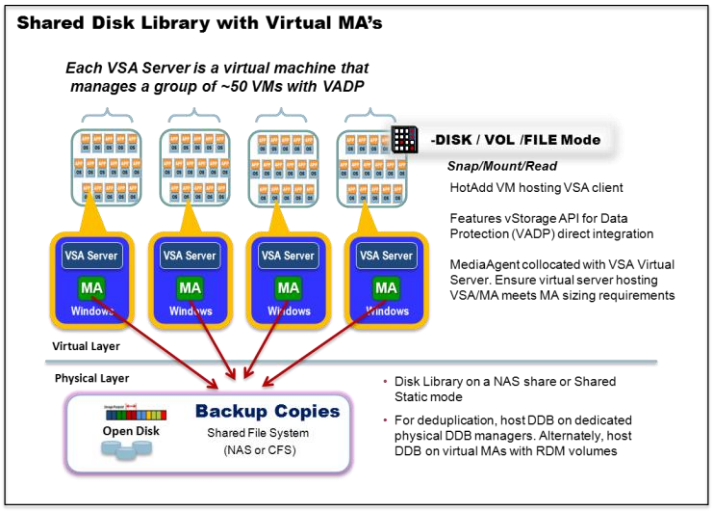


Figure 3: VSA and MediaAgents on virtual servers

The MediaAgent can also be hosted on dedicated physical servers. In this configuration, many VSA servers can write to a single MediaAgent. When configured in this manner, the VSA agents leverage VADP to read the VM data from the data stores and transfer it over the LAN to the physical MediaAgent. A dedicated vLAN/vSwitch is recommended to isolate backup traffic from other data on the network.

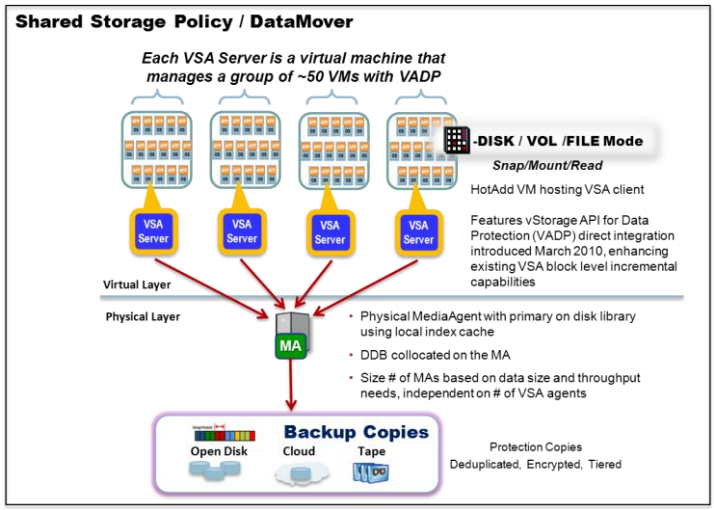


Figure 4: VSA on virtual servers, MediaAgent on physical server

The number of MediaAgents required will follow the usual MA sizing considerations that depend on the amount of data being transferred, the backup window available and the total throughput desired. The physical MA can also host DDBs if appropriately configured DDB volumes are available. Refer to Deduplication architecture guide for more details.

A third configuration is to co-host the Virtual Server and the MediaAgent on a separate physical server. In this configuration, the VSA agent leverages VADP to quiesce the VMs, creates a snapshot and reads the data blocks in the snapshot directly over the SAN from the physical VSA server. All data is transferred directly over the SAN with no impact on LAN. The number of VSA/MediaAgent physical servers required follows the usual sizing guidelines for MediaAgents that depends on the amount of data to be transferred, the backup window available and the I/O and throughput characteristics of the physical server.

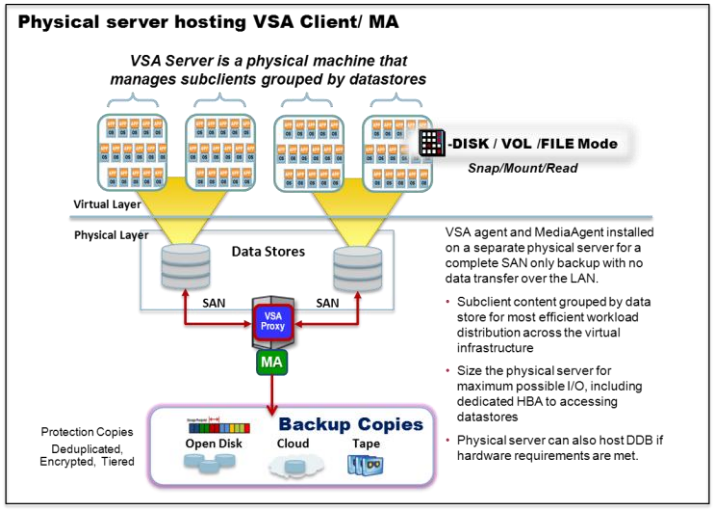


Figure 5: VSA and MediaAgent on physical server

For best performance, it is recommended to create subclients on the VSA server aligned with the datastores inside the virtual infrastructure. This ensures that the data read operations are distributed equally across all datastores for maximum cumulative throughput and performance. It is also recommended to have a dedicated HBA on the physical VSA server to optimize access to the datastores for fast read operations. The physical server can also host a DDB when deduplication is enabled, provided the hardware requirements as detailed in the Dedupe Architecture Guide are met.

One of the key usability benefits of the consolidated design relates to the browse and restore options. With all the subclients existing under the VSA master client, browse and restore is consolidated into a single node for the entire environment. The VADP option offers the full VSA restore options, including the the ability to restore single files form the single backup pass on windows guest host clients.

Roadmap Planning Items

Please stay tuned for future announcements regarding additional enhancements and special features related to Virtual Server Agent / vSphere integration that may be part of the Simpana beta program or future release programs. Key concepts that we are evaluating:

1. Simplified configuration and management by automatically installing the VADP SDK components automatically with the VSA client installation.
2. Incorporating persistent hardware snapshots with the VSA protection strategy to afford rapid recovery of the VMs.
3. Extending granular recovery of files from Linux guest host VSA backups, from the same VSA/Windows client
4. Individual reporting on Virtual Machines of job results and focused SRM views that profile both the VM characteristics and the file level contents of the guest host system.

Frequently Asked Questions

Q: How do you protect virtual machines on ESX 3.5 or environments with a combination of ESX 3.5 and ESX 4.0?

A: Virtual machines running on ESX 3.5 can be protected using VCB framework with VSA.

In environments with a mixture of ESX 3.5 and ESX 4.0, virtual machines running on ESX 3.5 servers are protected using VCB and VADP can be used for protecting VMs on ESX 4.0. This will require, at the minimum two sets of VSA agents, one set uses VCB to backup VMs on 3.5 and the other set uses VADP to protect virtual machines on ESX 4.0. As the organization transitions entirely away from the ESX 3.5 servers they can migrate all the VMs over to the ESX 4.0 VSA clients.

VMware does not recommend moving VMs across ESX servers of different versions, hence it is unlikely that VMotion will cause VMs to move between ESX 3.5 and ESX 4.0 thus causing the same VM to be backed up with two different methods.

Q: What transport modes are supported with VADP?

A: VADP supports all the modes supported by VCB. Simpana VSA supports 3 different modes, HotAdd mode where the VSA is in a VM, **SAN mode** for backup over SAN and **NBD mode** for backup over the LAN. Simpana VSA attempts all 3 transport modes in the above order. A registry key is available that forces VSA to use a specific protocol. Books Online outlines the registry key options.[5]

Q: Does Simpana VSA with VADP support VMs running on NFS volumes?

A: Yes, VSA with VADP leverages the NBD mode to protect VMs running on NFS volumes. This will cause data to flow over the LAN. However, incremental backups minimize data transfer over the LAN.

Q: With the VADP integration when would VCB be used?

A: VSA with VCB is used in the following scenarios

- To protect virtual machines running on ESX 3.5 or ESX 3.0

5 http://documentation.commvault.com/commvault/release_8_0_0/books_online_1/english_us/features/backup/virtual_server.htm#Registry_Keys_for_Virtual_Server_iDataAgent_Backups

- When Volume Level backup is necessary. Volume level backup is necessary when you need to filter out volumes/files from the virtual machine
- When File level backup is necessary to upload the backup data into content indexing jobs for offline CI. At this time, although –disk and –volume level backups support one-pass backup with granular file level restore on GH-W, offline CI is not supported.
- When the VMs are at hardware version 4 and incremental backups are required

Q: How much extra disk space is required on the VSA agent?

A: When using VSA with VADP, you only need to provision enough space on the VSA agent to accommodate the contents of the job results folder. Refer to Books Online for guidelines on space recommendations for job results. As there is no requirement to copy the VM snapshot to the VSA agent, no additional space is required.

On the data store containing the VM being backed up, sufficient space is required to maintain changes to the virtual machine while it is being backed up. Depending on the change rate on the VM, this space can be as high as 10% of the virtual machine size. Refer to VMware documentation on sizing recommendations when creating snapshots of virtual machines. Recall that the snapshot is reserved only to support the backup process in this case, so the space is recycled.

Q: Should we only consider using physical servers to support the VSA with VADP?

A: No, although the VSA agent can installed and run from a physical or a virtual machine – with the new VADP integration we expect most environments to use virtual machines. The HotAdd mode can be used to host the VM with the VSA client. We are recommending sites to consider that combination as the best practice approach with VADP.

Refer to BOL for more details on setting up VSA in HotAdd mode.[6]

Q: Does the licensing of VSA change with VADP?

A: No, VSA with VADP is licensed exactly in the same manner as today. There are two options:

- For medium to larger sites or new installations we would recommend the Virtual Environment protection bundles that are sized in modules around the number of protected VMs. These bundles include sets of VSA clients, FS base clients, MediaAgents, GridStor and Standard Disk Capacity that is optimized for either HotAdd VSA virtual backup server clients or physical VSA host servers. The bundles can be combined into blocks to combine the components/capacity to meet the needs of larger configuration designs while advanced options such as deduplication and data encryption can be easily be added on.
- For established CTE environments, the individual VSA agent licensing model remains available based on the number of ESX host servers.

Q: Can VSA with VADP protect applications that are running inside virtual machines?

A: Potentially yes, VMware tools deployed on Windows Guest Host VMs include a VSS requestor. VADP invokes this FS VSS requestor for every snapshot request to ensure that the snapshot is crash consistent.

When this option is enabled in VMWare tools, the applications inside the VM will be crash consistent when backed up with VSA. However, since the VSS requestor does not communicate specifically with the applications VSS writer, the image may not be application-consistent meaning that it may not restore in a fully usable mode. This is a VMware limitation.

[6] http://documentation.commvault.com/commvault/release_8_0_0/books_online_1/english_us/features/restore/use_case/vs_hot_add.htm

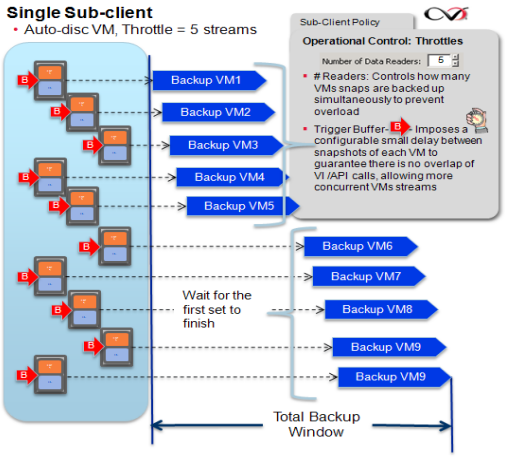
With this method, you will create crash-consistent file backups of the system running the application but you do not get the application-aware protection benefits such as log truncation or granular recovery of application data (individual database, individual datastore, etc.).

For virtual machines that are running smaller, less critical applications, protecting the VM using the VSA may be a sufficient level of protection. Customers should make that choice and potentially conduct recovery tests to see if it will serve their needs. For larger or mission critical applications, CommVault recommends employing the specific application agent locally inside the virtual machine and conducting a networked, application-aware backup to take full advantage of application specific capabilities and support full application-consistent recovery. That delivers an application-consistent backup, log management and simplified application restore – including features such as No Loss Restore on Exchange.

- Simpana Exchange DB No Loss Restore: After a restore operation has been performed, if the No Loss Restore option on the Restore Options dialog was selected, the log files that have been created since the last backup will be appended to the restored data. This will bring the database to the most current possible state.

Q: Do all the subclient operational tuning controlls apply to VADP too?

A: Yes, the same features such as the # readers and trigger buffers apply to the subclient operations working in the VADP or VCB modes. With VADP the elimination of the VCB copy can dramatically improve performance, resulting in a shorter backup window.



Q: Can we provide granular object recovery of Exchange, Sharepoint or AD from a VSA –disk backup?

A: Yes, the granular file restore options available on all VSA backups can be used to restore the database files to a server hosting the Simpana offline recovery tools[7]. Those tools can be used to recover individual messages, documents or AD objects. Please refer to BOL for more details.

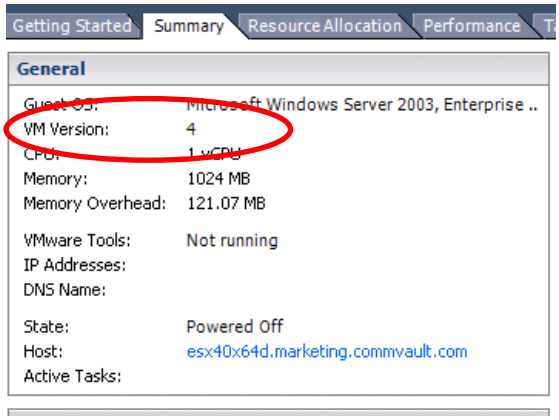
Q: Does VSA with VADP require VMware Data Recovery (VDR) tool?

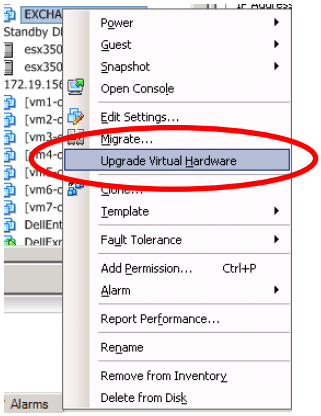
A: No, the VMware Data Recovery (VDR) tool is a separate backup tool provided by VMware for protecting VMs in small environments. It leverages VADP under the covers to create on disk based VM backups from a HotAdd appliance running the VDR tool, as such it is limited to vSphere 4.0 and above. Althought the tool is promoted as internal alternative to 3rd party backup, such as Simpana VSA, it requires a large amount of manual administration, operational limitations and sub-optimal performance. Example discussion from VMware user group (http://communities.vmware.com/thread/258878) where even smaller collections running sequentially can take 10-20 hours per cycle. After customers and prospects begin to understand the broader complexities of managing the protection and recovery of a virtual server environment they quickly see the value of embracing a leading, innovative solution such as the Simpana Virtual Server Agent.

[7] We are shifting the name from the original "Offline Mining Tools" to "Offline Recovery Tools" to better describe the functions

Q: How do I know if a customer is using Version 4 or Version 7 machines?

A: The hardware version of the virtual server can be seen in the summary tab of the virtual server properties. To take advantage of all the features available in VADP, including CBT, the virtual machine needs to be at Hardware Version 7. To update the hardware version, right click on the virtual machine in the vCenter client and select **"Update Virtual Hardware"** option. The virtual server needs to be powered off for this option to be visible. Refer to VMware 4.0 documentation for more details on the benefits of hardware version 7 and how to convert existing VMs to the optimized format.





Please send any additional questions to Products@Commvault.com.