EMC²
where information lives®

White Paper

Backup and Recovery for VMware Using EMC Data Domain Deduplication Storage

Best Practices Planning

Abstract

VMware offers extraordinary benefits, but it can come at the cost of extra storage, backup resources, and administrative challenges. EMC® Data Domain® deduplication storage addresses this challenge by reducing redundant data across VMware data backups, operating at disk speeds, and providing cost-effective replication for fast disaster recovery (DR). This white paper reviews the best practices for architecting a backup, recovery, and DR approach for VMware using Data Domain systems, regardless of which backup software or scripts are involved.

June 2010

Part Number h7300

Table of Contents

Executive summary

VMware is the predominant method in the open systems world for creating multiple virtual machines in a physical computing system. By separating virtual systems from physical constraints, they become easier to manage, utilization is increased, and floor space is reduced. Consolidation helps take greater advantage of powerful server assets, which can contribute to supporting green initiatives.

But VMware sites also may require more storage to manage and protect than their physical counterparts. By making it much simpler to multiply servers, storage footprints tend to grow, and the implications of which become painfully apparent during backup and recovery. For example:

- Multiple similar virtual machine (VM) environments, times multiple storage image versions for protection and DR, can equal much larger storage than when servers were more expensive to clone.
- In backing up VMware environments, restore needs may include both full virtual machine disk (VMDK) images as well as individual file restores to the guest OS. Backing up both VMDKs and guest OS files can offer optimum protection, but the data is highly redundant. With tape or plain-disk backup target storage, many more tapes or that much more disk storage capacity would be consumed.

Fortunately, with EMC® Data Domain® systems as the backup target for VMware environments, those similar files would be deduplicated at high speed before being stored, minimizing storage capacity and bandwidth requirements for onsite protection and replication to a disaster recovery (DR) site. Where most file system backups result in 10 to 30 times data reduction on a Data Domain system, VMDK-inclusive backups commonly offer 40 to 60 times reduction. For more background on award-winning Data Domain deduplication storage systems in VMware environments, please see www.datadomain.com/solutions/vmware.

When using Data Domain systems with well-understood best practices for backup and snapshots in VMware, a deployment can simplify management of consistent images. Once stored, the images are ready to restore locally, or with optimized deduplicated replication at a remote DR site. This paper describes best practices for managing VMware backup and replication together.

Vendor references and script examples are included as examples only and should not be considered definitive or guaranteed by EMC.

Introduction

This white paper provides general information for using EMC Data Domain deduplication storage to back up VMs using VMware Consolidated Backup (VCB) with VMware Infrastructure 3 (VI3). Topics include an overview of VI3 components and various methods of backing up data in disk (VMDK) images and guest OS files for discrete recovery – either locally or remotely in a DR site. The central focus is on selecting the backup approach best suited to meet specific needs, and by extension, how Data Domain systems can be leveraged to assist online restoration and replication to a DR site.

This paper does not go into detail on how to use Data Domain deduplication storage in the new vSphere 4.0 vStorage API for Data Protection (VADP) environments. In contrast to VI3, VADP was introduced in vSphere 4.0 and is a replacement for VCB. Depending on what backup application is in use, VADP can be used with or without a proxy server (the proxy server may be fully integrated into the commercial backup software). Table 1 compares the differences between VADP and VCB.

Table 1. VADP compared to VCB[1]

	VADP	VCB
Additional Download and Install	No, fully integrated with the backup application	Yes
Full VM Image Backup	Yes	Yes, two-step copy; Source > VCB proxy > Target
Incremental VM Image Backup	Yes	No
File-level Backup	Yes, Windows and Linux	Yes, Windows only
Full VM Image Restore	Yes	Yes, using VMware Converter
Incremental VM Image Restore	Yes	No
File-level Restore	Yes, using Restore Agents	Yes, using Restore Agents

If commercial backup software supporting VADP is in use, the Data Domain server is simply the backup target.

For best practices on using Data Domain storage as a standard backup target in different environments, see www.datadomain.com/solutions.

NOTE: The focus of this paper is on VCB best practices, since the VI3 components are not integrated and require more planning as well as a separate proxy server to configure backups.

Audience

This white paper is intended for backup administrators, systems engineers, and EMC partners to assist them in architecting an optimized VMware backup solution for their environment. It describes how to use Data Domain deduplication storage to simplify and reduce the cost of backup and recovery of VMs and guest OS files. A basic understanding of virtualization and experience with backup and recovery software and concepts is assumed.

VMware Infrastructure 3

For a proper introduction to VMware components, terminology, and use, please refer to www.vmware.com.

VMware Infrastructure 3 (VI3) is a bundled product with four components: Virtual Infrastructure Client (VI Client), License Server, Virtual Center Management Server (VC Server), and the ESX Server Console.

An ESX host, which has a hypervisor kernel (vmkernel), runs VMs. The service console is actually just a VM itself, which is granted special privileges to access the configuration of the ESX host machine. Figure 1 shows an example of a typical VI3 deployment with two VMs.

Each VM has one or more of its own VMDKs. The collection of VMDKs is managed by the VMFS file system and the ESX service console, a VM with special management privileges.

[1] VMware Storage Blog at http://blogs.vmware.com/storage/2010/02/introduction-to-vstorage-apis-for-data-protection---vstorage-apis-for-data-protection-were-introduced-in-vsphere-40-to-facil.html

VI3 also includes VMware Consolidated Backup (VCB). VCB allows a centralized approach to off-ESX-host backup, using a special purpose Windows proxy server that accesses ESX data independently. When deployed appropriately, VCB offers many scalability advantages for backing up VMs and VMDK files.

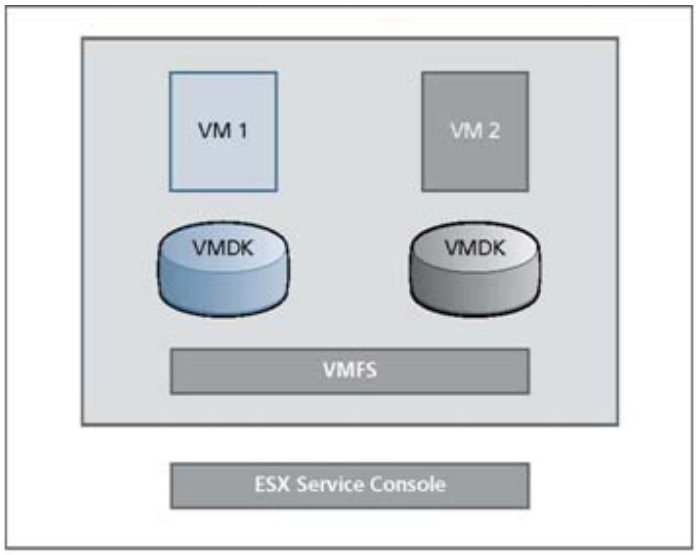

Figure 1. Typical VI3 deployment with two VMs

A specialized backup proxy server has access to shared VMDK files and their guest OS file systems. Using this proxy system, backup software can capture VMDK and guest OS file backups with low application-VM impact and only moderate impact on the ESX server. This system requires a proxy server.

VMware Infrastructure backup alternatives: Success metrics

There are a wide variety of possible methods for backing up VMware data. To achieve best practices for your site, consider the following characteristics. You will want to find the right balance of simplicity, speed, cost, and restorability in the solutions that you consider.

- **VMDK recoverability:** The method you choose should allow you to restore consistent, whole VMDK components. Because the VMDK is a portable, "bare metal" unit of storage that incorporates all guest OS settings, it is the simplest unit of recoverability for restoring a VM's state. While normally viewed as a larger form of data, discouraging some administrators from backing them up regularly, VMDKs realize huge deduplication effects when stored on a Data Domain system, making frequent backups viable.
- **Guest OS file recoverability:** According to Gartner, about 80 percent of recoveries are file recoveries. As VMware moves from lab functions to support of general server and desktop activity, single file restores for a given guest OS will predominate. Depending on the approach, finding the files to restore can be supported either by a catalog/index using traditional backup software or through a browsing method to find a file in a familiar namespace, similar to what would be done in conventional NAS file system snapshots.
- **Backup impact on application VMs:** Except in very small deployments, it is important to minimize the backup impact on production VMs. While most backup software tries to limit server impact to less than 5 percent of system resource use, if you have 10 VMs on a single ESX host backing themselves up simultaneously using the same strategies, it could tie up a substantial percentage of the physical host resources.

- **Backup impact on the ESX server running application VMs**: If the hosting ESX server slows, applications slow, even if not due to the guest OS in a particular VM. Backup best practices in general encourage non-disruption of the application ecosystem.
- **Backup performance:** Backup windows matter as much in the virtualized world as in the physical world. Faster is better.
- **Backup scalability:** Make sure the approach you choose can scale to suit your needs as you add VMs and ESX servers.

Choosing the right VMware backup method can seem complex, since there are a lot of potential alternatives. It is possible to back up:

- Within the VMs
- Within the ESX server running the VMs
- From another ESX server (either using a shared storage fabric or through a virtual LUN over Ethernet in a related ESX server) with the VI3 VMware Consolidated Backup proxy
- The underlying SAN or NAS store directly, by scripting file copies and/or snapshots
- Using commercial backup software

While the possibilities seem numerous, for most deployments there are only a few reasonable alternatives, summarized in Table 2.

It is important to note that the following methods will not be discussed because of limitations that disqualify them as best practices.

- **Backing up or replicating the back-end data store only**. Most VMware deployments are backed by well-provisioned block storage, often on a SAN. It is possible to back up and restore just the block volumes of that storage. This is not a best practice because it is very tricky and unlikely that all the necessary steps will be taken to snapshot a consistent image prior to backing it up. It is best to back up within the logical image of ESX, the guest OS, and/or VCB.
- **Using client-based deduplicating backup software within the VM, ESX, or VCB**. The point of VMware is to optimize how much work a server can do across more workloads. Further taxing them for backup is a step backward. In addition, these specialized applications will not be generally able to support all data center backup needs, so it would create an orthogonal, extra backup administration load. Standard backup software that understands VMware well is more than efficient enough for optimized backup/restore, when paired with a good deduplication system for storage and DR.

Table 2. Backup choices

	Backup clients in both VMs and service console	VCB: VMDKs plus guest OS files	VMDK snap/copy to Data Domain system from proxy
VMDK recovery	Yes (from service console backup)	Yes	Yes
Guest OS file recovery	Yes, if in VM	Yes	Yes
File recovery method	Commercial backup software catalog	Commercial backup software catalog	Name-based browsing
Impact on application VMs	High	Low	Low
Impact on ESX server running app VMs	High	Medium	Low
Backup performance	Slow	Moderate	Fast
Scalability	Small deployments only	Scales well with proxies	Scales well with proxies
Guest OSs supported	Any	Windows only	Any

Several backup software packages have additional information on best practices for their use in a VMware environment. While they may evolve over time, these are noted as current papers for follow-up[2].

VMware:

- For information on pre-VI3 infrastructure, read the white paper *Using VMware ESX Server System and VMware Virtual Infrastructure for Backup, Restoration, and Disaster Recovery* at www.vmware.com/pdf/esx_backup_wp.pdf.
- For information on VI3 infrastructure, read the information guide *VMware Consolidated Backup: Improvements in Version 3.5* at www.vmware.com/files/pdf/vcb_35_new.pdf.
- Read the *VMware Virtual Machine Backup Guide* at http://www.vmware.com/pdf/vsphere4/r40/vsp_vcb_15_u1_admin_guide.pdf.

Enterprise backup software provider examples:

- For information on EMC NetWorker®, read the Data Sheet at http://www.emc.com/collateral/software/data-sheet/h2257-networker-ds.pdf.
- For information on EMC Avamar®, read the white paper *Optimizing Backup and Recovery for VMware Infrastructure with EMC Avamar* at http://info.emc.com/mk/get/AMA00007001_LAND_STD.
- For information on Symantec NetBackup, read the white paper *Veritas NetBackup 6.5 for VMware 3.x Best Practices* at http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_veritas_netBackup_6.5_vmware_nov2007.pdf.
- For information on IBM Tivoli Storage Manager Best Practices, go to http://www.ibm.com/developerworks/wikis/display/tivolistoragemanager/Best+Practices.

2 These are listed for the convenience of readers only and do not represent any kind of warranty from EMC on their quality or accuracy.

- Read *Using IBM Tivoli Storage Manager V5.4 and V5.5 for backup and restore operations on the VMware service console* at http://www.ibm.com/developerworks/wikis/display/tivolistoragemanager/Using+IBM+Tivoli+Storage+Manager+V5.4+and+V5.5+for+backup+and+restore+operations+on+the+VMware+service+console.
- For information on CommVault Galaxy, read the Partner Solution Brief at www.commvault.com/pdf/CV_SolutionBrief_VMWare.pdf.

Specialty VMware backup providers:

- For information on Vizioncore vRanger Pro, read the Technical Data Sheet at http://vizioncore.com/products/vRangerPro/documents/vRangerProDatasheet.pdf.
- For information on Veeam, go to http://www.veeam.com/tips_to_a_successful_veeam_backup_and_vcb_integration_rev2_wpp.pdf.

Getting started

Back up the VM guest OS files and VMDKs with a standard backup client without VCB

This method is intuitive for a backup operator and sufficient for smaller deployments. It is very straightforward, uses the same backup software as the rest of the data center, but does not scale well. It has two parts, each clear-cut, and each suited to a different path to recovery. First, by treating each VM as a physical machine, use a conventional backup client in each VM to back up the guest OS files for easy file recovery. Second, use a standard backup client in the special-purpose Linux VM that runs the service console to back up ESX configuration data and VMDKs as complete system recover points. Figure 2 illustrates the solution – backing up both VMs and the ESX server with a commercial backup agent.

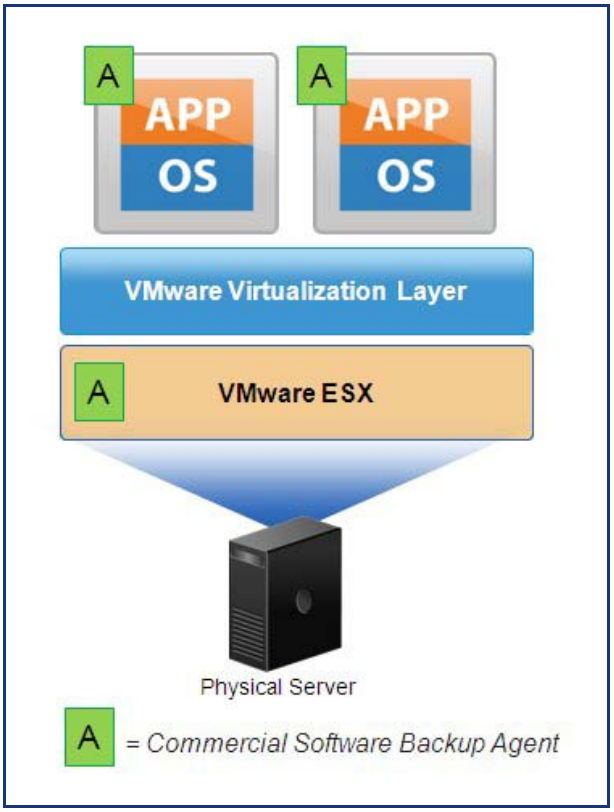

Figure 2. Back up VMs and ESX with Commercial Agent

Method 1: Backing up the VM guest OS files

This technique is the most well known and probably most direct way of backing up an operating system running within VMware. A standard backup client is installed on a VM. The guest OS backup on the VM is then scheduled and file-level backups are performed as with a physical machine. File restores are the same as for any standard client. The backup infrastructure can be shared as just one more component of a standard backup deployment, and it needs no additional hardware.

Using this guest VM-based approach also allows for a simple solution for VMs that may be running an application (for example, SQL Server, Oracle). The backup application being used will likely have a special agent for these situations that can be used to ensure a consistent, point-in-time backup of the application.

Benefits

File-level backups are typically done by the same technique as with other backup clients in the environment. Backups and restores occur just as if the guest OS was hosted on a physical, not virtual, machine. As long as the guest OS is supported by the backup software and VMware, the OS can be backed up safely. File-level restores are supported. Data Domain systems fit well for this method, providing excellent data reduction and WAN-optimized replication for disaster recover (DR) purposes. The technique is straightforward to implement. It also allows for the backup of not only the VM, but also application data that resides on different, non-VM controlled storage partitions (such as "raw disk" or NAS).

Considerations

First, managing the sheer number of VMs that can proliferate quickly can be difficult with this method. Second, if a number of clients are backed up concurrently, backups can quickly overrun CPU, memory, and other resources on the ESX host. To avoid potential resource overload, IT managers have to be very selective about how many and which virtual systems they back up at the file level using this approach. The "guest OS" technique simply does not scale or have a feasible management solution for medium-to-large VMware installations.

With this step alone, you cannot back up an ESX host that contains the ESX service console or the VMDK images. To do so, you would need to follow Method 2.

Method 2: Backing up ESX and VMDKs

Each VMware guest OS has at least one disk file and other associated configuration files within the directory [DataStoreName]/ VMname under /vmfs/volumes, stored on the ESX host. VMware places the files on top of VMFS and adds a "vmdk" extension to each file. The files can be backed up and restored as standard files. Think of this as a whole VM image backup that can be used for DR (bare metal restore). For this configuration, a Linux backup agent is installed on the VMware service console. Restoring a virtual machine requires restoring the individual VM folder that contains the VMDK disk files; that is, restoring an image of the VM from the point in time it was shut down.

Data Domain systems can take advantage of this method with excellent data reduction effects for local storage as well as WAN replication for DR purposes. Note that service console backup only enables the backup and restore of data that resides on the same storage area (such as "disk") as the VM. Application data may reside on a separate filesystem.

Benefits

This method works with all off-the-shelf backup software that supports Linux-based (ESX) clients. It is easier to manage than the prior approach as only one Linux client exists for each ESX host. You can easily back up the entire ESX host itself if desired. It involves moderate load on the ESX server, but since larger files can be streamed at a much faster rate than smaller files, it can have less impact than a guest OS file backup. This method can also help manage the load on any given ESX server because under normal circumstances, the VDMK files will be backed up serially rather than concurrently.

Considerations

This method is essentially a disk image backup, which has inherent limitations for recovery granularity. No guest OS file-level restores are enabled from the backup software catalog. One other important consideration is the need to snapshot the VM system whose VMDK file and folder are being backed up; this requires appropriate commands or scripting to ensure image consistency. Separately, some backup applications may not support Linux. Finally, the process of scheduling VM shutdowns, shutting down VMs, and scheduling the backups can be a management challenge as the number of VMs increase. However, scripting or the ability to shut down all VMs on an ESX server at the same time can lessen the burden.

If you add VMotion to the configuration, the location of the guest OS is not fixed in the system, and this option becomes even more challenging to manage, especially if you only want to back up selected VMs.

Method 3: Using VMware Consolidated Backup

Using VCB with commercial backup software not supporting VADP

If commercial backup software supporting the vStorage API is not available, an alternative method utilizes a Windows 2003+ host as a backup proxy that is a source for backups. The storage to be backed up is shared with the backup proxy host. It may either use a storage array that is shared by the ESX servers and the proxy, or, as of ESX 3.5's Virtual LUN construct, the proxy can use a LAN connection to another ESX server to access the storage. For Windows systems, the VCB proxy server can also mount the shared storage for backup access at the file system level if desired. It supports only Windows guest OS. Figure 3 depicts the VMware VCB configuration.

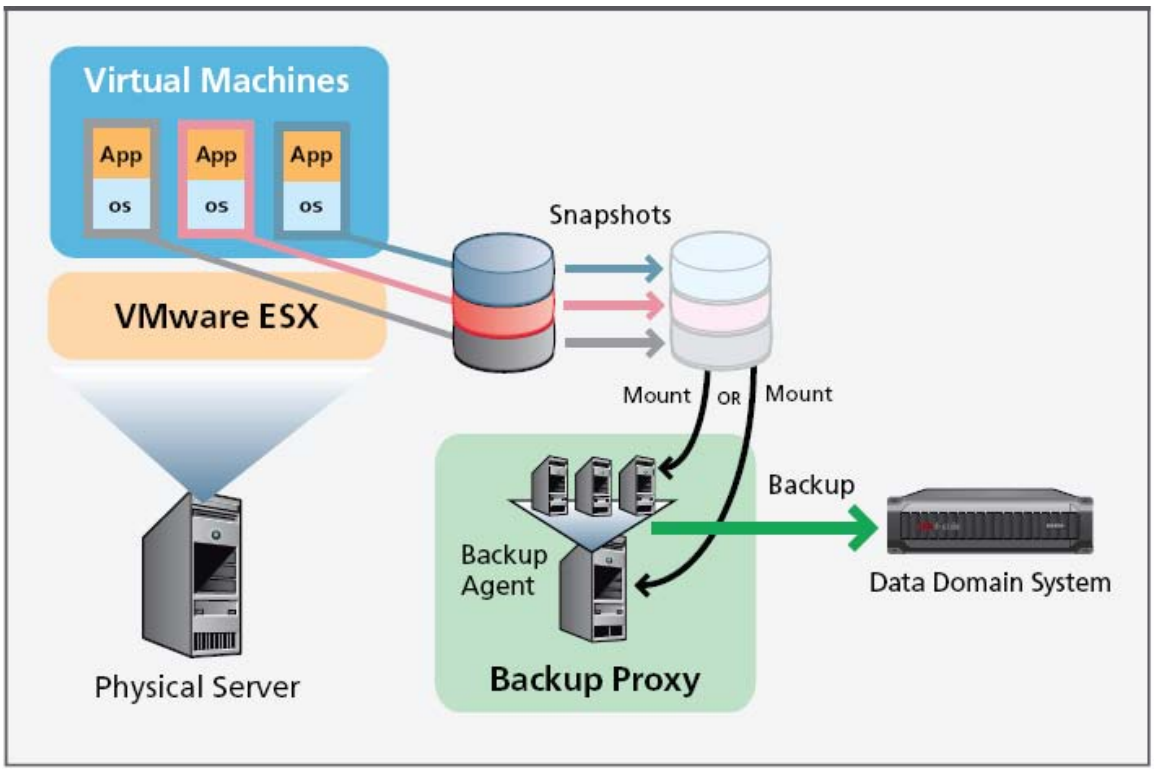

Figure 3. VMware Consolidated Backup with a Data Domain system

The consolidated backup agent, installed as a separate package on the Windows 2003 proxy host, takes a snapshot of an individual VMware virtual machine (or if scripted, multiple VMs), and copies the data to a temporary folder. The data is then used as the source for backups.

Just before the snapshot is made, /usr/sbin/pre-freeze-script or C:\Windows\pre-freeze-script.bat is run. Once the backup is complete, /usr/ sbin/post-thaw-script or C:\Windows\post-thaw-script.bat is run.

Taking a snapshot only takes a few minutes so, as an example, you could use the scripts to quiesce or stop your database. The entire snapshot and copy process needs to be understood to automate the process. Variables include size of the disk file and the amount of ESX server resources in use.

A VMDK "snapshot" involves the creation of special VMDK files with the extension .redo, which become the writeable disk file, while the main .vmdk file is now closed for writing (and locked by VMFS) and therefore can be backed up from the service console. While not shown, using the Data Domain system as a virtual tape library is also possible.

Benefits

The most important benefit with VCB is that once the systems are quiesced and the VM snapshot taken, the VMs can be up and running during the actual backup, and the backup processing has minimal impact on their performance. Both VMDK images and guest OS file images are available for copying to a safe place using scripting or backup software. Multiple virtual machines can be backed up at once with limited load on VMs or an ESX host. This approach is vastly simpler and more scalable, so most of the larger VMware deployments running VI3 tend to prefer it. Data Domain systems can take advantage of this method with excellent local storage deduplication and WAN-optimized replication for DR purposes.

Considerations

The tradeoffs when considering VMware Consolidated Backup are:

- Consolidated backup requires some manual command line configuration and implementation. The process can be automated using VMware-supplied scripts.

Note: The new vStorage API (VADP) eliminates the need for manual scripting.

- If using shared, SAN-attached storage, LUNs must have the same LUN numbers assigned to the proxy and to the ESX host. Both the proxy and ESX host must also be on the same SAN.

The VMware VI3 Consolidated Backup framework requires a Windows 2003 host as proxy; no other OS is supported.

Method 4: Consolidated backup with Data Domain systems

This is an example of how to set up a consolidated backup proxy and integrate it with a Data Domain system. The example assumes that the backup software is installed on a separate host configured for file system backups and that the Data Domain system is properly installed. The connectivity assumes the layout in Figure 3.

Proxy installation

A requirement is a Windows 2003 server with the VMware Consolidated Backup framework installed that is directly plugged in to a SAN along with one or more ESX servers. Both must directly see all the VM images sitting in the VMFS LUNs.

The Windows host is called a backup proxy, or proxy for short. The first time a consolidated backup occurs through the proxy host, the VMs must be powered on.

After configuration, the proxy talks to the ESX server(s), takes a snapshot, and makes a copy of it to locally attached disk. The process is manual and lends itself to scripting. VMware does provide scripts that let you tie in to some commercial backup products such as EMC NetWorker or Symantec NetBackup.

Advanced best practices

Snap/Copy VMDK images to Data Domain systems from ESX or VCB, and restore guest OS file copies via browsing

In the prior methods, commercial backup software was used to identify, move, catalog, and restore guest OS files, VMDKs, and even the ESX system itself. They provide complete protection in different levels of scalability. There is one other important approach that is normally used only with scripting. Some backup software providers have begun to offer it as a software package that links well into VMware Infrastructure as well as Data Domain systems for local and remote/DR restores.

In this method, only VMDKs are actually copied for protection to the Data Domain system. This may be done from either a service console or from a VCB proxy. If these copied VMDK files are named with simple characteristics that allow them to be found easily (such as a combination of VM name, ESX server name, time and date), they can be stored to a network share on a Data Domain system (for example, using NFS). This would enable simple VMDK recovery, locally or remotely. Once copied to the network share, the data is fully protected. Recovery of a given VMDK back to the ESX storage is just another file copy request.

This method also enables file recovery, without guest OS file backup. Using the random access properties of the Data Domain system, a new VM can boot from the saved VMDK on the Data Domain system. Once running, a user can browse into its guest OS file system, find the file in question, and just copy it back to a production VM's guest OS. Using Storage VMotion, the whole data image of the VM may be migrated to a primary store if it requires a high rate of interaction (IOPS). Figure 4 depicts this configuration.

Benefits

This approach has the least impact on running VMs and ESX infrastructure, and it enables the fastest backups of all the methods because there is no requirement for guest OS file system backups in order to restore discrete files. It is simpler to administer over time because there are fewer files to manage. From a help-desk standpoint, the critical files to track are only the larger VMDKs. Unlike VCB, this approach supports any guest OS, including Linux, Solaris, and NetWare.

Considerations

Commercial backup software stores the backup images on disk in their respective formats (for example, tar). While some of these are well understood, they can obscure the internal data from view without use of the catalog or backup application for a restore. As a result, most backup packages, which never fully simplified the scripting requirements of VCB, are not suitable for backups in Method 3. It must be scripted, using the conventions recommended by VMware for creating snapshots and restarting VMs for consistent backups. A link to the papers discussing this from VMware's point of view is on page 8.

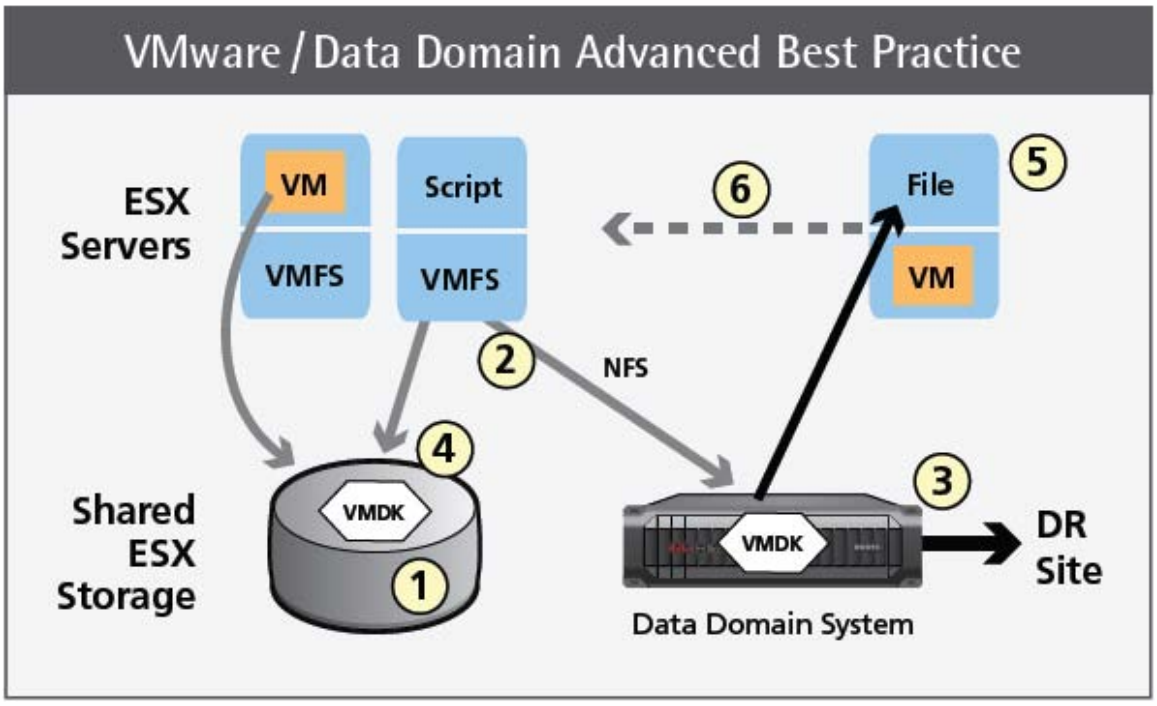

Figure 4.Snap/Copy VMDK images to Data Domain deduplication storage from ESX or VCB. Restore guest OS file copies via browsing

The six steps in Figure 4 show the following:

1. Snap a VMDK image
2. Copy VMDK to the Data Domain system
3. Store / Replicate

The following occur locally or at the DR site.

4. Restore VMDK from the Data Domain system
5. Restore the file to the guest OS at the DR site
6. VMotion to the primary store

vSphere's VADP with commercial backup software

As mentioned in the introduction, one of the simplest methods for backing up and restoring virtualized environments makes use of backup software supporting vSphere's vStorage API. Software packages supporting the vStorage API provide centralized management of full, differential, and incremental VM backups and restores without having to manage tasks from within each VM or ESX server.

Benefits

The key benefit of using backup software supporting the vStorage API is that users do not need to have a separate process or software agents on each individual VM. Users simply use one VM or physical system with backup software installed to back up and restore all discovered VMs in a given ESX server. In addition to simplifying backups, using standard backup software to manage the process reduces backup windows by avoiding the need to load ESX servers with the task of managing VM backups.

Considerations

Not all backup software packages support the vStorage API. While support for it is growing over time, this option may not be available to all users at this time. Users must judge whether simplifying their backup tasks warrants conversion to another backup software application or whether using an alternative backup method for their VMs is preferable.

Deployment example

A financial services, Fortune 500 company with revenues in excess of $5.5 billion (2009) deployed Data Domain with VMware and EMC storage.

The project was a complete redesign of their continuity plan for their largest global office that employs over 1,000 people. They replaced their fragmented backup and recovery approach with consolidated and consistent protection of both virtual and physical infrastructure assets.

They are now backing up more than 60 TB of data and replicating to the disaster recovery site. Three tape silos were displaced with the solution and backups are now stable and operations run smoothly. Figure 5 is a diagram of the Data Domain solution as deployed.

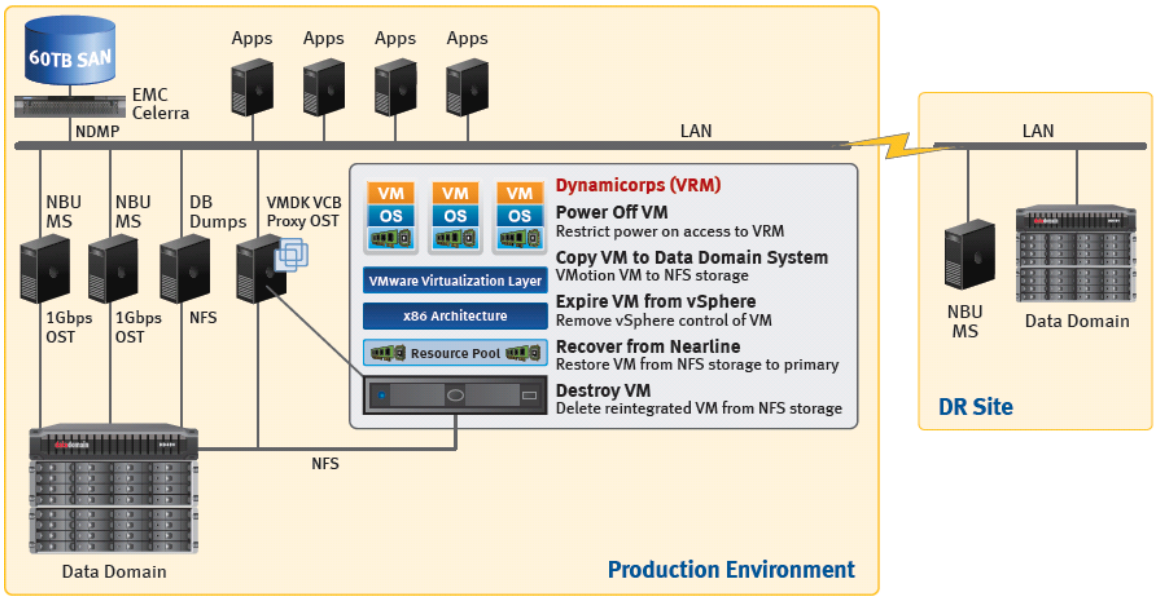

Figure 5. Deployment example of a financial services company

VMDK files are moved in their native format (template, archive, mount, boot). VMware Storage VMotion is used for live migration of VMDK files. Disaster recovery testing has become simple in the new environment.

Conclusion

In this paper, we presented the predominant approaches to link Data Domain deduplication storage systems to the VMware environment for simplicity, speed, and safety of backup retention, recovery, and replication.

To gain the benefits of VMware, storage (especially backup storage) often is forced to grow. Through efficient use of Data Domain deduplication storage, backup time can be well managed, and backup storage and replication bandwidth for DR can be brought back under control. While in normal file system backups and retention periods, Data Domain can offer 10 to 30 times data reduction, and a VMware environment can often result in 40 to 60 times data reduction.

Be clear about your goals, and consider one of the following choices:

- To get started, consider using a traditional backup client in each guest OS, though this will not scale well.
- For a professional IT deployment that will be supported by most backup software over time, with Windows virtualization, consider VI3 VCB.
- For optimum scalability and efficiency, but with some scripting required in most cases, consider copying consistent VMDKs to a Data Domain system. For VM restore, copy back the VMDK directly or through Storage VMotion. For file restore, boot the VM from the VMDK on the Data Domain system, and either copy the file to primary storage or again, use Storage VMotion while the VM is running.
- For optimum scalability with no scripting required, consider using backup software that supports the vStorage API. Also, with the use of the vStorage API, there is no need to have backup agents installed on all existing VMs, as all that is needed is a single VM or physical server with the backup agent installed managing all the backups and restores for the whole VM environment.

There are a lot of possible choices, but only a few real best practices. For further reading, please visit www.datadomain.com/solutions/vmware.