VMware Virtual SAN™ Backup Using VMware vSphere® Data Protection™ Advanced

SEPTEMBER 2014

vmware®

Table of Contents

Introduction 3
vSphere Data Protection Advanced Architectural Overview 4
Virtual SAN Backup Using
vSphere Data Protection Advanced 5
Test Scenarios. 5
Test Configuration 7
Test Methodology 8
Factors Affecting Backup Performance. 8
vSphere Data Protection Advanced Virtual Appliance CPU and Memory 8
CPU and Memory Utilization in NBDSSL Mode 8
CPU and Memory Utilization in HotAdd Mode 10
Virtual SAN Datastore 11
Placement of Backup Disk Components 11
Backup Workload Distribution 12
Transport Mode 14
Backup Concurrency. 14
Management Network Bandwidth. 15
Conclusion 16
References 16

Introduction

VMware Virtual SAN™ is a hypervisor-converged, software-defined storage solution for the software-defined data center (SDDC). It is the first policy-driven storage product designed for VMware vSphere® environments that simplifies and streamlines storage provisioning and management.

Virtual SAN is a distributed shared storage solution that enables the rapid provisioning of storage within VMware vCenter Server™ as part of virtual machine creation and deployment operations. It uses the concept of disk groups to pool together locally attached flash devices and magnetic disks as management constructs. Disk groups are composed of at least one flash device and several magnetic disks. The flash devices are used as read cache and write buffer in front of the magnetic disks to optimize virtual machine and application performance. The Virtual SAN datastore aggregates the disk groups across all hosts in the Virtual SAN cluster to form a single shared datastore for all hosts in the cluster.

Business continuity is a crucial component of data center operations. Virtual SAN interoperates with VMware vSphere Data Protection™ Advanced, a backup and recovery solution designed for vSphere environments and powered by EMC® Avamar®. vSphere Data Protection Advanced provides agentless backup and recovery of virtual machines running on VMware vSphere VMFS, NFS, and Virtual SAN datastores. Backups are deduplicated using a variable-length segment algorithm, resulting in a significant reduction in backup data storage capacity consumption. Backup data can also be moved offsite using reliable, secure, network-efficient replication.

vSphere Data Protection Advanced is deployed as a Linux® based virtual appliance. A vSphere Data Protection Advanced virtual appliance consists of multiple virtual disks that contain the guest operating system (OS), vSphere Data Protection Advanced application, and backup data. vSphere Data Protection Advanced routinely performs checks to verify the integrity of the virtual appliance and the backup data it contains. vSphere Data Protection Advanced can also utilize EMC Data Domain® to store backup data. The EMC DD Boost™ protocol for Avamar is used to move backup data from the vSphere Data Protection Advanced virtual appliance to the Data Domain appliance.

This paper studies two typical scenarios in which vSphere Data Protection Advanced backs up virtual machine images, one with Virtual SAN as the backup target and the other with Virtual SAN as both the backup source and the backup target. Although some might question the wisdom of storing production data and backup data in the same datastore, because this practice risks simultaneous loss of both in a disaster scenario, there are benefits such as simplicity and rapid restore to consider. To mitigate the risk, vSphere Data Protection Advanced backup data replication can be utilized to replicate the data to a vSphere Data Protection Advanced appliance deployed to another storage volume either at the same site or offsite or both. Experiments are conducted to study factors that might potentially have an impact on backup performance. Based on testing results, variables impacting backup performance are discussed and performance guidelines are provided.

vSphere Data Protection Advanced Architectural Overview

vSphere Data Protection Advanced uses VMware vSphere APIs – Data Protection, the VMware data protection framework that enables a product to back up virtual machines from a central backup server or virtual machine without requiring agents or processing to be done inside each virtual machine. To back up a virtual machine by using the vSphere APIs – Data Protection framework, the following sequence must occur:

1. Connect to the VMware ESXi™ host containing the virtual machine to be backed up. Take a snapshot of the target virtual machine by using the vSphere API.
2. The virtual machine continues to run while the snapshot view is static.
3. Capture the virtual disk data and virtual machine configuration information.
4. Open and read the virtual disk files. Copy them to backup media, along with configuration information.
5. Consolidate the backup snapshot by using the vSphere API.

In step 4 of the backup process, data is transmitted to the backup server or virtual appliance. Transmission throughput varies with different VMware transport modes. VMware supports four virtual disk transport methods: file access, Network Block Device (NBD) or encrypted Network Block Device Secure Sockets Layer (NBDSSL) over LAN, SAN transport, and SCSI HotAdd transport. vSphere Data Protection Advanced cannot use SAN transport, regardless of what storage is in use; it supports only SCSI HotAdd, NBDSSL, and NBD and in that preference order.

SCSI HotAdd involves attaching a virtual disk to the backup appliance just like attaching the disk to a virtual machine. The vSphere host on which the backup appliance resides has access to the datastore where virtual machines to be backed up are stored. During backup, the base disk of the snapshotted virtual machine becomes read only; therefore, the backup appliance is also able to mount the base disk, enabling both the target virtual machine and the appliance to read data from the virtual disk without transmitting it across the network, as shown in Figure 1. This backup mode saves substantial network bandwidth.

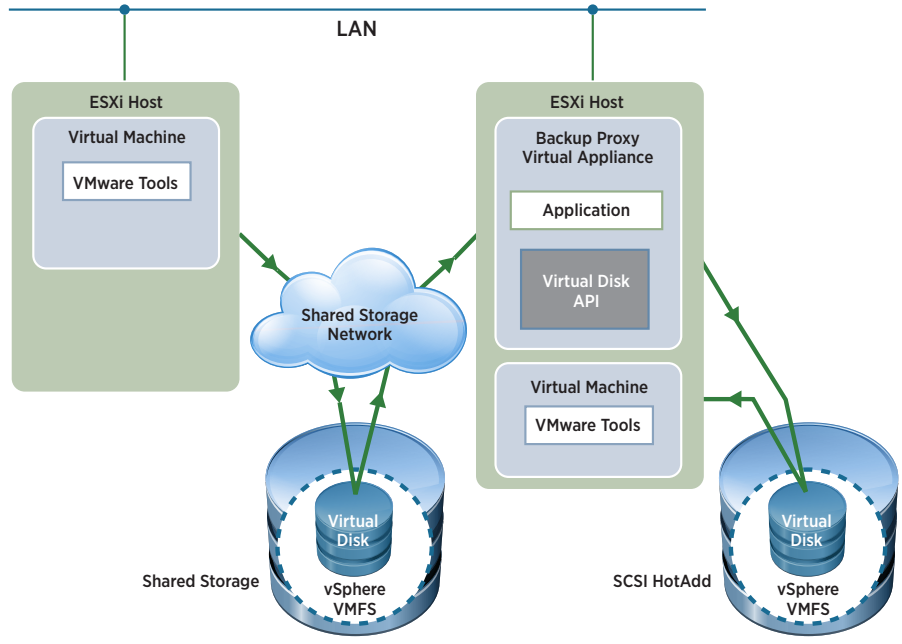


Figure 1. HotAdd Transport Mode

If the datastore containing the target virtual machine is not accessible by the vSphere host on which the vSphere Data Protection Advanced virtual appliance is running, the NBDSSL or NBD transport is used to copy data across the network to the virtual appliance. NBDSSL is the same as NBD but uses SSL to encrypt all data passed over the TCP/IP connection. During backup, the vSphere host reads data from storage and sends it across the network to the backup virtual appliance, consuming network bandwidth, as shown in Figure 2. The VMware Network File Copy (NFC) protocol is used to access virtual disks in the NBD transport mode. Each virtual disk requires one NFC connection for data transmission.

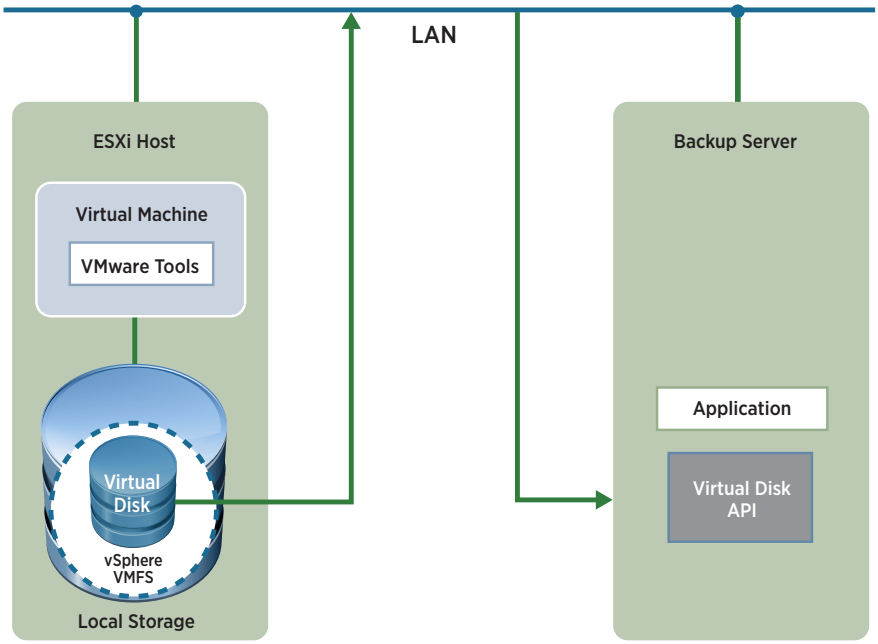


Figure 2. NBD/NBDSSL Transport Mode

Virtual machines running on vSphere hosts can track disk sectors that have changed. This feature is called Changed Block Tracking (CBT). Virtual disk block changes are tracked from outside virtual machines, in the virtualization layer. When software performs a backup, it can request transmission of only the blocks that have changed since the last backup or of the blocks in use. The CBT feature can be accessed by applications as part of vSphere APIs – Data Protection. vSphere Data Protection Advanced can use CBT to request that the VMkernel return blocks of data that have changed on a virtual disk since the last backup snapshot.

Virtual SAN Backup Using vSphere Data Protection Advanced

Test Scenarios

This study consists of two typical scenarios of backing up virtual machines in a Virtual SAN cluster using vSphere Data Protection Advanced. Backup performance, as well as system resource consumption data, is collected during testing.

Scenario 1 is depicted in Figure 3. The vSphere Data Protection Advanced virtual appliance is installed in the same Virtual SAN cluster where the virtual machines to be backed up reside. SCSI HotAdd transport mode is leveraged in this setup to improve backup performance and eliminate unnecessary network bandwidth consumption. However, because both production data and backup data are stored in the same Virtual SAN datastore, the backup workload has the potential to impact the production workload during the backup window.

This is due to I/O contention in addition to the increased risk of compromised business continuity in case of datastore failure. One solution to mitigate this risk is to use the backup data replication feature to replicate data to a secondary vSphere Data Protection Advanced appliance or to an Avamar array. Alternatively, the vSphere Data Protection Advanced appliance can send backup data to a Data Domain array by using the DD Boost protocol. Backup data can then be replicated to another vSphere Data Protection Advanced appliance and Data Domain array pair. In this configuration, the backup is usually faster, the backup window is relatively small, and the time frame for replication to a remote target is flexible.

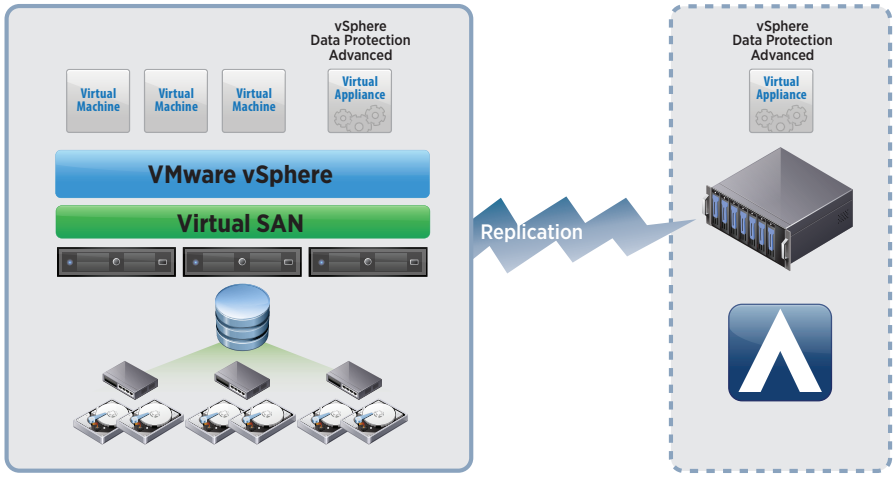


Figure 3. Backup Within the Same Virtual SAN Cluster

In scenario 2, the vSphere Data Protection Advanced virtual appliance is installed in a different Virtual SAN cluster from the one that hosts the production virtual machines to be backed up. The two Virtual SAN clusters are managed by the same vCenter Server instance. As shown in Figure 4, one is the backup source, and the other is the backup target. Backup leverages the NBD or NBDSSL transport mode, consuming the management network bandwidth. However, CBT can be utilized to minimize bandwidth consumption in incremental backups. In this configuration, backup and recovery performance can be limited by LAN performance, resulting in a relatively longer backup window.

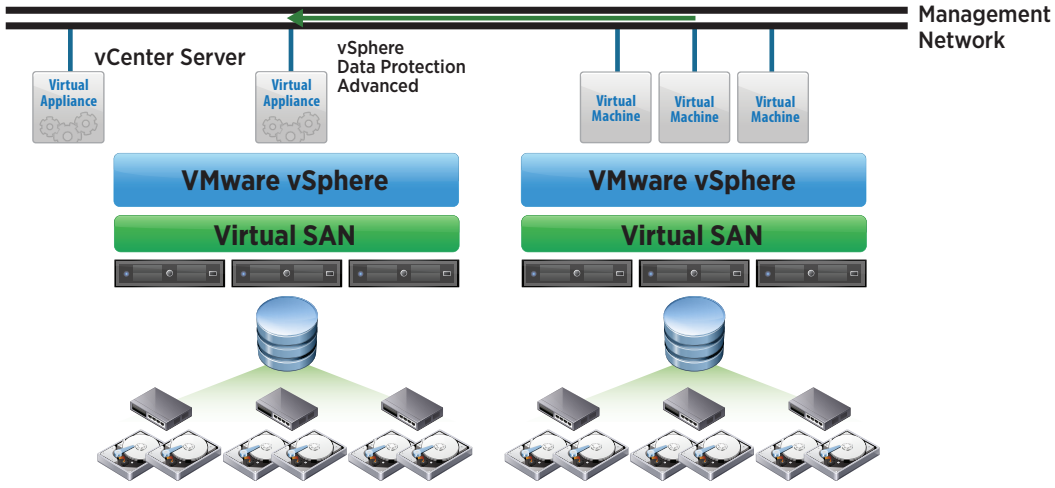


Figure 4. Backup Across Different Virtual SAN Clusters

Test Configuration

Two three-node Virtual SAN clusters are set up for the testing. The hardware configuration of these clusters is described in Tables 1 and 2 respectively.

SERVER CONFIGURATION	
Model	Dell® PowerEdge® R720
CPU	Intel® Xeon® Processor E5-2660 – 2.2GHz, 16 cores
Memory	128GB
SSD	Intel SSDSC2BB80 800GB x1
HDD	Seagate® ST1000NM0023 NL-SAS 1TB x6
Disk controller	Dell PERC H710
Network configuration	10Gb Virtual SAN network 10Gb management network

Table 1. Virtual SAN Cluster as Both Backup Source and Target in Test Scenario 1 and as Backup Source in Test Scenario 2

SERVER CONFIGURATION	
Model	Dell PowerEdge R720
CPU	Intel Xeon Processor E5-2650 – 2.0GHz, 16 cores
Memory	128GB
SSD	Intel SSDSC2BB80 800GB x2
HDD	Seagate ST91000640NS SATA 1TB x12
Disk controller	Dell PERC H710
Network configuration	10Gb Virtual SAN network 10Gb management network

Table 2. Virtual SAN Cluster as Backup Target in Test Scenario 2

vSphere 5.5 Update 1 and vSphere Data Protection Advanced 5.5.6 releases are used in testing. Table 3 lists the minimum system requirements for vSphere Data Protection Advanced to be deployed in a Virtual SAN cluster with default settings. When the vSphere Data Protection Advanced virtual appliance is deployed in a Virtual SAN datastore by using the default virtual machine storage policy, each object is mirrored with a *Number of Failures to Tolerate* setting of 1. Therefore, the vSphere Data Protection Advanced capacity requirement in a Virtual SAN deployment is twice that of a standard deployment unless the virtual appliance is applied with a customized storage policy to remove redundancy; this is not recommended unless backup data is also replicated to another vSphere Data Protection Advanced appliance or Avamar.

	2TB	4TB	6TB	8TB
Processors	Minimum four 2GHz processors	Minimum four 2GHz processors	Minimum four 2GHz processors	Minimum four 2GHz processors
Memory	6GB	8GB	10GB	12GB
Disk Space	6TB	12TB	18TB	24TB

Table 3. vSphere Data Protection Advanced Minimum System Requirements When Deployed in Virtual SAN

Test Methodology

A backup data set composed of virtual machine types specified in Table 4 is created for the testing. In each virtual machine, a mix of video and ISO files fills the virtual disk.

VIRTUAL MACHINE CONFIGURATION	
Microsoft® Windows® 7	64-bit, 40GB virtual disk
Ubuntu® 12.04	64-bit, 40GB virtual disk

Table 4. Virtual Machines to Be Backed Up

The initial full backup of a virtual machine takes some time for all of the data to be processed and then backed up. Subsequent incremental backups of the same virtual machine take significantly less time because vSphere Data Protection Advanced utilizes CBT, which reduces the amount of data copied during backup by more than 99 percent. Industry research shows that the blocks that have changed since the last backup are typically 0.5 percent to 1 percent of the average server application's data. Therefore, this study covers only full backup, also referred to as level 0 backup, the most demanding type of backup.

To minimize the influence of deduplication on backup performance, each Linux and Windows virtual machine is populated with unique video and ISO files that enable a relatively much lower deduplication ratio. A single vSphere Data Protection Advanced appliance can back up eight virtual machines concurrently; therefore, jobs of backing up one, two, four, six, and eight virtual machines are run to collect throughput performance and resource consumption data as workload increases. To minimize variation, multiple iterations are executed for each backup job to calculate the average throughput.

Factors Affecting Backup Performance

Several factors that might impact vSphere Data Protection Advanced backup performance with Virtual SAN are studied. The following sections discuss CPU and memory consumption in both test scenarios and analyze in detail Virtual SAN datastore operation and backup performance using various transport modes.

vSphere Data Protection Advanced Virtual Appliance CPU and Memory

The vSphere Data Protection Advanced virtual appliance has minimum system requirements for different capacity configurations deployed on Virtual SAN, as shown in Table 3. vSphere Data Protection Advanced leverages an inline, variable-length, block-level data deduplication process that identifies unique blocks of data. When backup workload increases, CPU and memory allocation on the appliance can become limiting factors on backup performance.

CPU and Memory Utilization in NBDSSL Mode

Both CPU and memory usage gradually increase as backup workload grows. At a certain point, however, utilization jumps sharply to deliver enough processing power. Figure 5 shows utilization data in the NBDSSL backup mode across two Virtual SAN clusters.

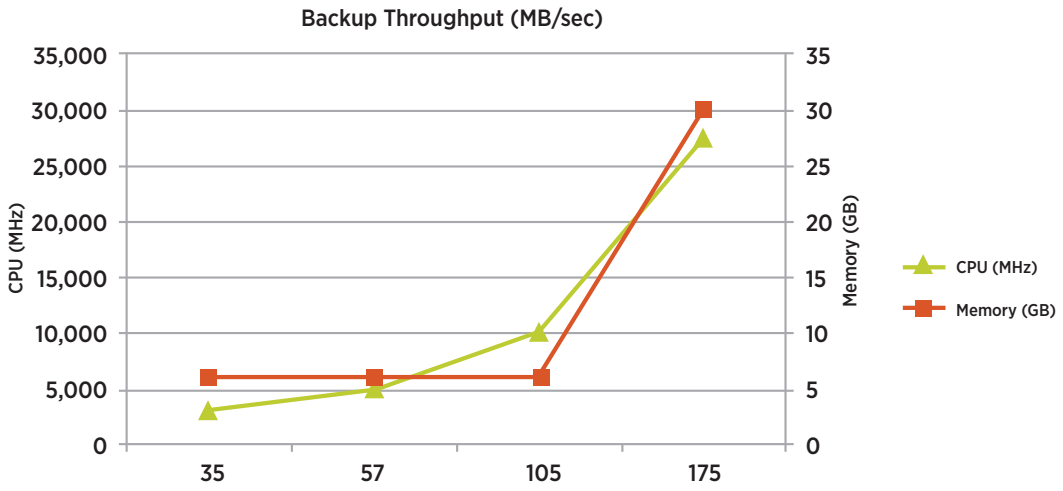


Figure 5. CPU and Memory Utilization in NBDSSL Backup Mode

In the test, memory is initially set to 12GB, with four vCPUs totaling 8000MHz, both recommended configurations for a default vSphere Data Protection Advanced appliance deployment. Memory and CPU utilization soon reach 100 percent, becoming bottlenecks. The backup throughput is only approximately 60MB/sec. Memory is then increased to 32GB and CPU increased to 16000MHz on the appliance. While memory is no longer a bottleneck, CPU utilization still reaches nearly 100 percent, with the backup throughput at approximately 120MB/sec. To improve performance, CPU allocation is increased to 24000MHz. Consequently, throughput rises to approximately 170MB/sec while average CPU utilization is at more than 80 percent. Further increasing CPU allocation, however, does not yield higher throughput. At this point, CPU utilization stabilizes at approximately 60 percent. This implies that CPU is no longer the backup performance bottleneck. Figure 6 illustrates that to eliminate the possibility of CPU's being the bottleneck, it is important to find the minimum CPU allocation in a specific backup environment; overcommitting CPU to the virtual appliance is not necessary.

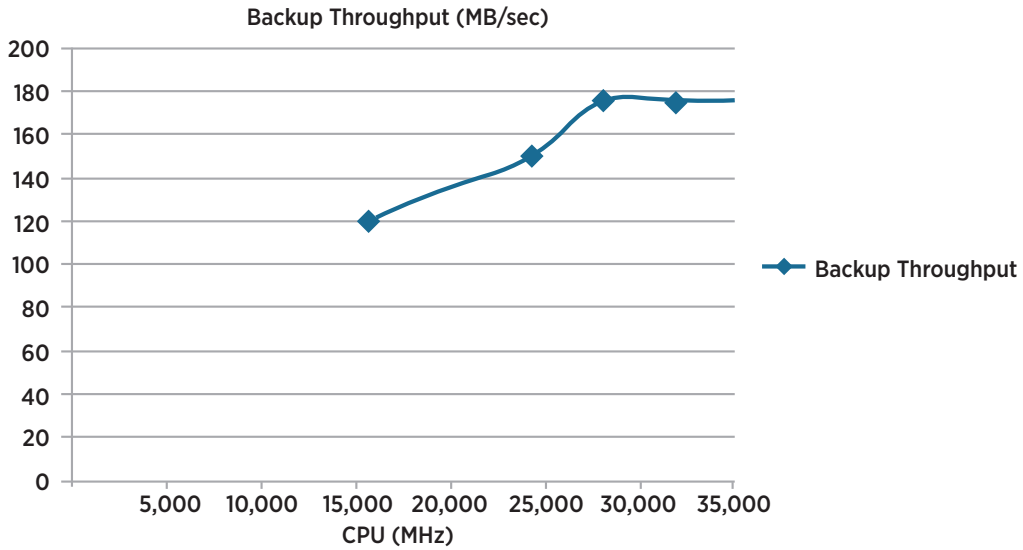


Figure 6. CPU Impact on Backup Throughput

CPU and Memory Utilization in HotAdd Mode

When backing up virtual machines in the same Virtual SAN cluster by using SCSI HotAdd, the vSphere Data Protection Advanced appliance consumes more CPU and memory as compared to backing up across clusters by using NBDSSL. Moreover, as backup workload increases, memory and CPU utilization rise more rapidly. In our testing, when backup throughput exceeds 174MB/sec, the ESXi host's entire CPU capacity is consumed by the virtual appliance. However, Figure 7 demonstrates that vSphere Data Protection Advanced can continue delivering higher throughput even though CPU is fully utilized, which suggests that backup is very CPU intensive in HotAdd mode. If not controlled, vSphere Data Protection Advanced can consume all available CPU resources; the recommendation is to create separate resource pools for the production virtual machines and the vSphere Data Protection Advanced virtual appliance, combined with shares to prioritize production workload over backup workload during resource contention.

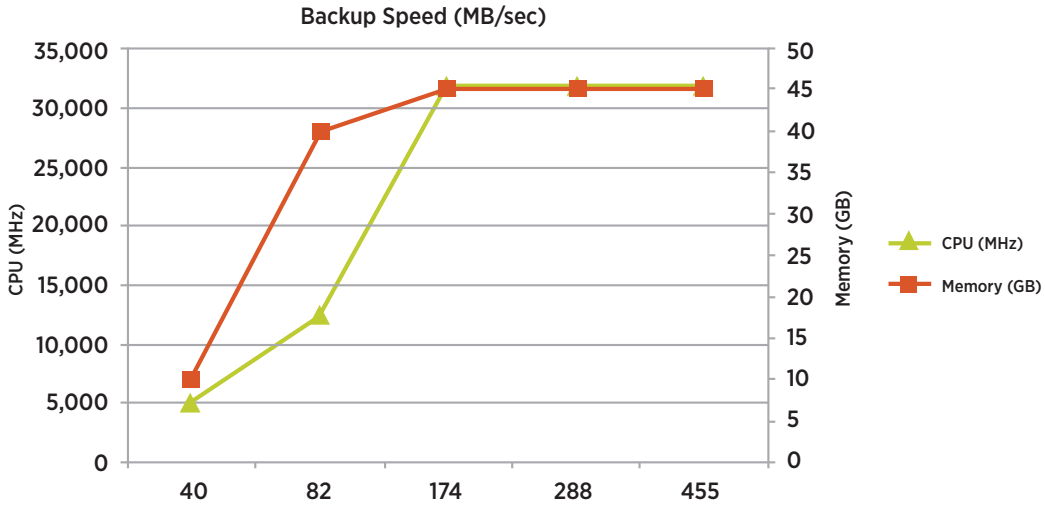


Figure 7. CPU and Memory Utilization in the HotAdd Backup Mode

SCSI HotAdd backup mode requires substantial computing resources to deliver high performance. However, our testing results reveal that for any individual backup job, CPU and memory demands are in an inverse relationship, as shown in Figure 8.

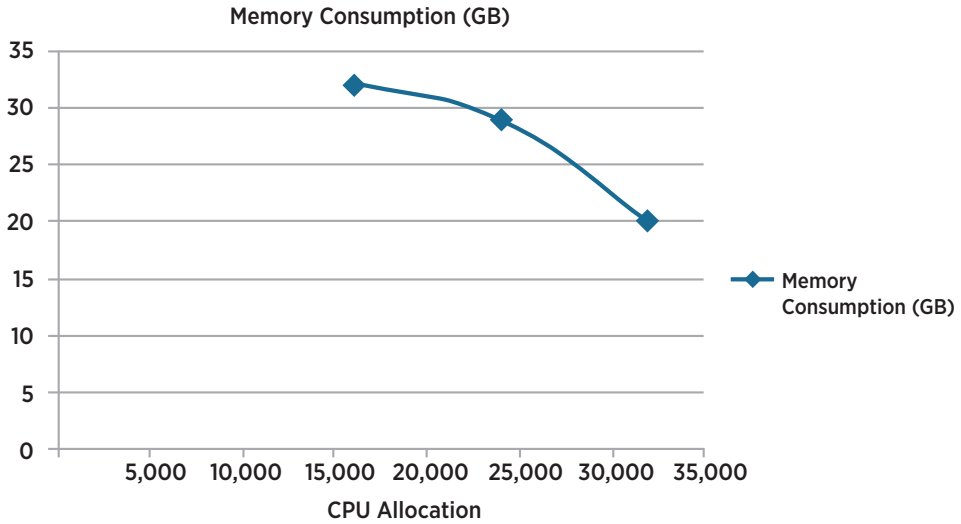


Figure 8. Relationship Between CPU and Memory Utilization in a Backup Job

In this example of backing up four virtual machines, if CPU allocation is 16000MHz, memory consumption is 32GB. As more CPU is allocated to the appliance, less memory is consumed during backup. When CPU allocation reaches 32000MHz, memory consumption drops to only 20GB. The same inverse relationship can be observed in all other backup jobs of different numbers of virtual machines.

Virtual SAN Datastore

At the storage layer, the Virtual SAN datastore plays a critical role in determining vSphere Data Protection Advanced backup performance and capacity planning.

Placement of Backup Disk Components

The vSphere Data Protection Advanced virtual appliance is deployed in the Virtual SAN datastore by using the default virtual machine storage policy through Storage Policy Based Management (SPBM), which sets *Number of Failures to Tolerate* at 1, meaning that each of the virtual machine objects is mirrored in the datastore. Any object larger than 255GB is split into multiple components that are distributed in the datastore.

The ideal component placement is that all components are distributed into different disk groups so that more SSDs are leveraged and each component resides on a different HDD. It helps performance when writes are destaged from SSDs to more disk spindles to minimize disk contention. For instance, the vSphere Data Protection Advanced 2TB configuration contains four virtual disks: virtual disk 1 for the guest OS, virtual disk 2 and virtual disk 3 for backup data, and virtual disk 4 for creating and managing checkpoints. Due to its 1TB size, each backup data disk object is split into five components. Overall, each backup data disk has two replicas and each replica consists of five components residing on different physical HDDs to result in high performance. Figures 9 and 10 show detailed placement information.

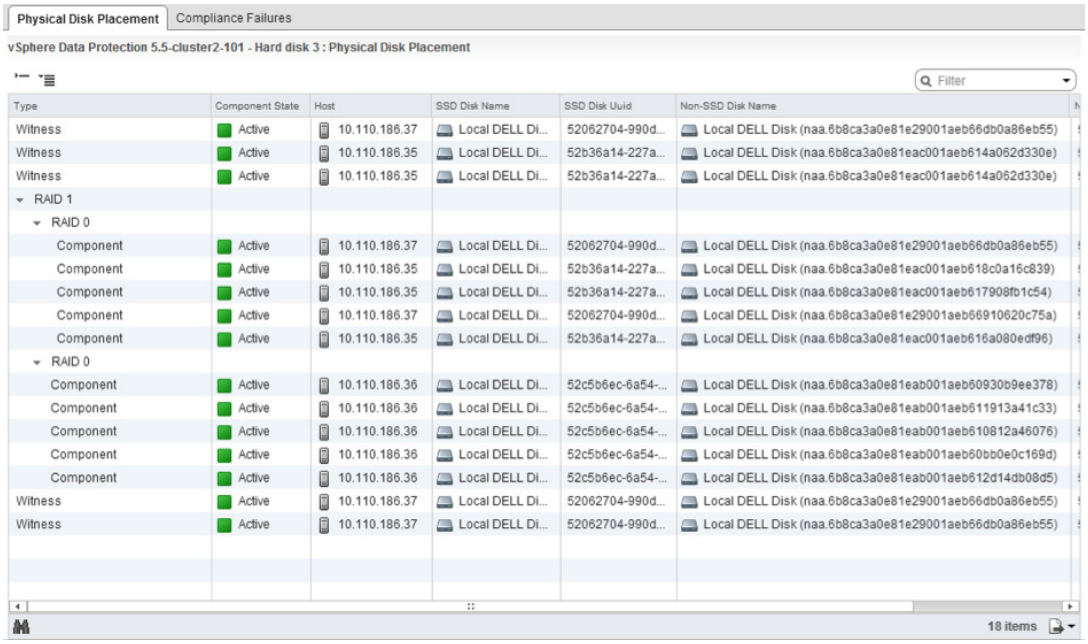


Figure 9. Physical Placement View of Backup Disk Components

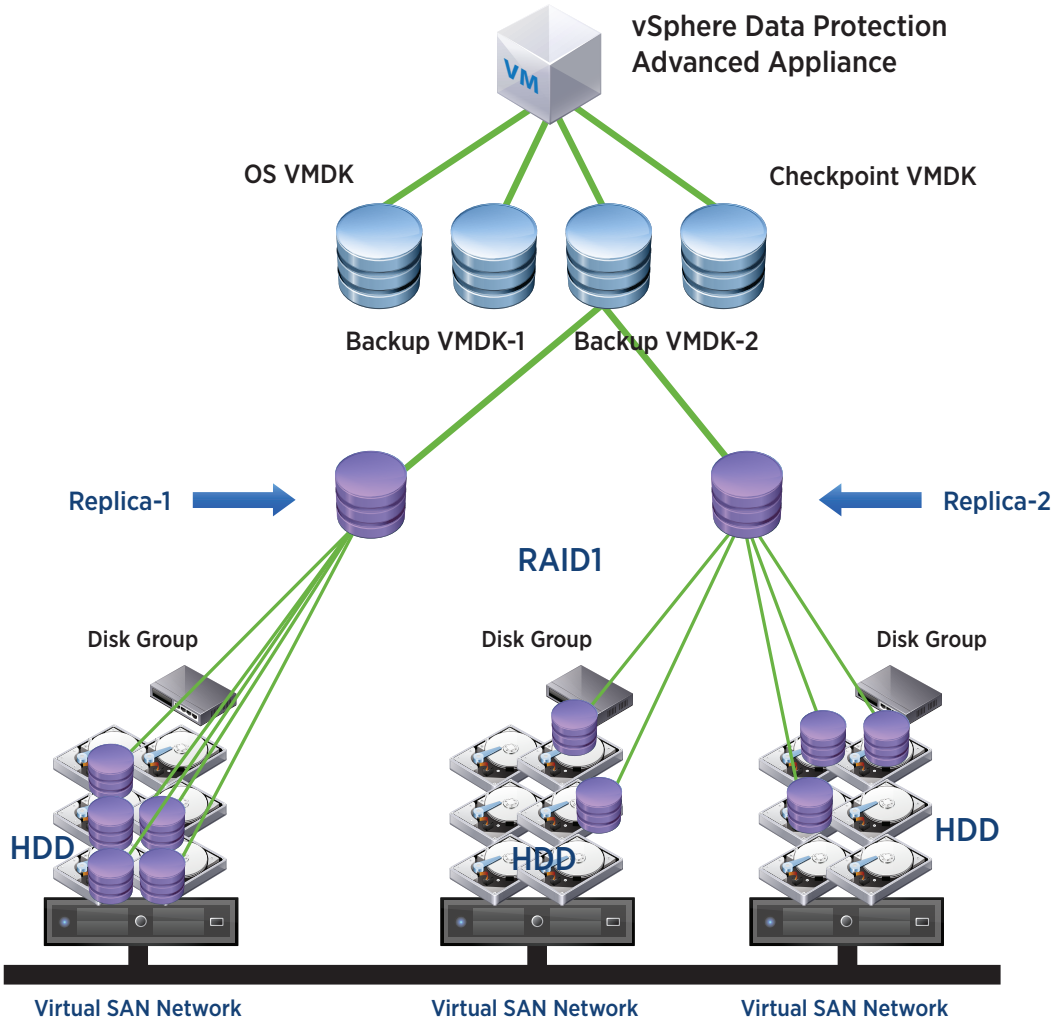


Figure 10. Logical Placement View of Backup Disk Components

Backup Workload Distribution

Backup workload is distributed to all SSDs in disk groups where the backup disk components are stored. Figure 11 shows Virtual SAN observer performance data of a disk object that contains five components, each placed on a different HDD in the same disk group. All components achieve similar IOPS performance because data is simultaneously destaged to those HDDs. In this case, increasing *Number of Disk Stripes per Object* in the storage policy might not improve overall performance because most disk spindles are already utilized.

When multiple components are stored on the same physical disk, disk contention arises during destaging. In this situation, adding more disks to better distribute components is effective in improving backup performance. Our testing verified that when increasing the number of HDDs from two to six for each host of the Virtual SAN cluster in the vSphere Data Protection Advanced 2TB configuration test of backing up eight virtual machines, backup performance improves greatly from 255MB/sec to 500MB/sec in SCSI HotAdd mode.

On the other hand, if the number of HDDs is much larger than the number of components, increasing *Number of Disk Stripes per Object* to place smaller components onto more disks is a viable solution for improving backup performance until the number of disk spindles is no longer a bottleneck.

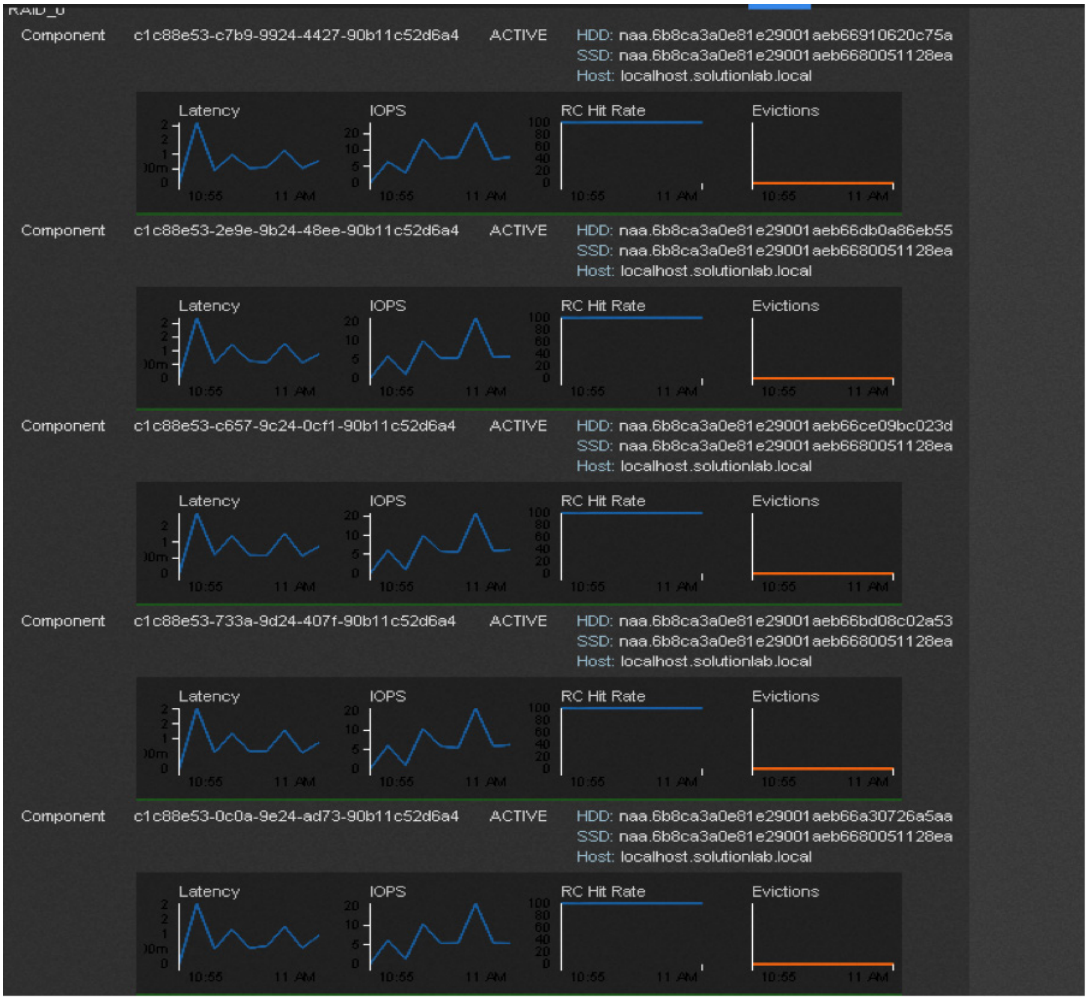
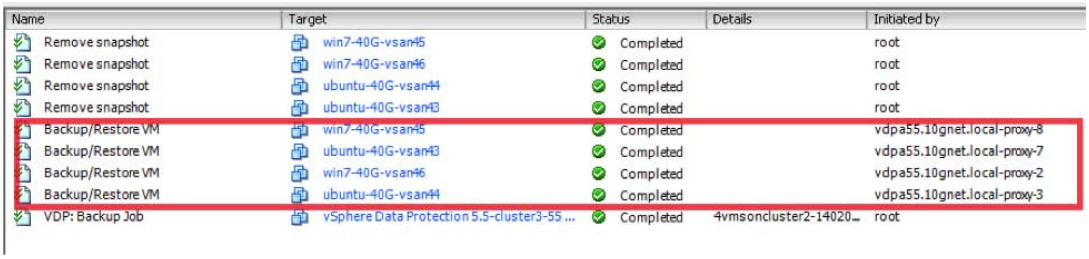


Figure 11. Workload Distribution Within Disk Group

Transport Mode

Concurrent backup improves overall backup throughput. A backup proxy is allocated for each virtual machine being backed up. vSphere Data Protection Advanced can back up eight virtual machines simultaneously, so if more virtual machines are selected for backup, the remaining ones will be queued. As many as 10 vSphere Data Protection Advanced appliances can be deployed to a vCenter Server environment when needed to increase concurrency. Figure 12 illustrates that there are four proxies in a backup job of four virtual machines.



Name	Target	Status	Details	Initiated by
Remove snapshot	win7-40G-vsan45	Completed		root
Remove snapshot	win7-40G-vsan46	Completed		root
Remove snapshot	ubuntu-40G-vsan44	Completed		root
Remove snapshot	ubuntu-40G-vsan43	Completed		root
Backup/Restore VM	win7-40G-vsan45	Completed		vdpa55.10gnet.local-proxy-8
Backup/Restore VM	ubuntu-40G-vsan43	Completed		vdpa55.10gnet.local-proxy-7
Backup/Restore VM	win7-40G-vsan46	Completed		vdpa55.10gnet.local-proxy-2
Backup/Restore VM	ubuntu-40G-vsan44	Completed		vdpa55.10gnet.local-proxy-3
VDP: Backup Job	vSphere Data Protection 5.5-cluster3-55 ...	Completed	4vmsoncluster2-14020...	root

Figure 12. Backup Proxies

Backup Concurrency

vSphere Data Protection Advanced overall backup throughput increases as the number of virtual machines to be backed up increases. Under the same backup workload, aggregated backup throughput is higher in HotAdd mode than in NBD/NBDSSL mode, as shown in Figure 13.

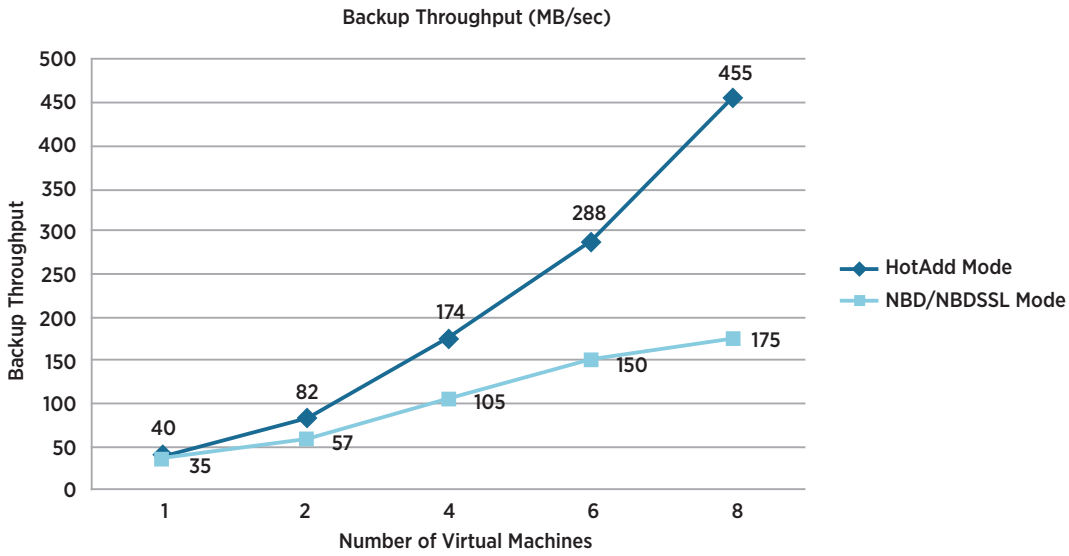


Figure 13. Aggregated Backup Throughput in Various Transport Modes

In NBD/NBDSSL mode, the NFC protocol is used to read virtual disks. As the degree of concurrency increases, backup throughput scales up nearly linearly. This implies that each NFC access stream has a certain performance constraint and is the determining factor for overall backup performance.

Management Network Bandwidth

In NBD/NBDSSL mode, backup data is transmitted over the management network. The management network bandwidth can be a limiting factor when backup workload increases. In our test environment, the management network is 10GbE. Figure 13 clearly illustrates that the aggregated backup throughput can exceed the bandwidth of a 1GbE network. Figure 14 shows network throughput during a backup job of four virtual machines. Therefore, when using the NBD/NBDSSL transport mode for backup, it is necessary to estimate backup workload and allocate sufficient bandwidth to the management network.

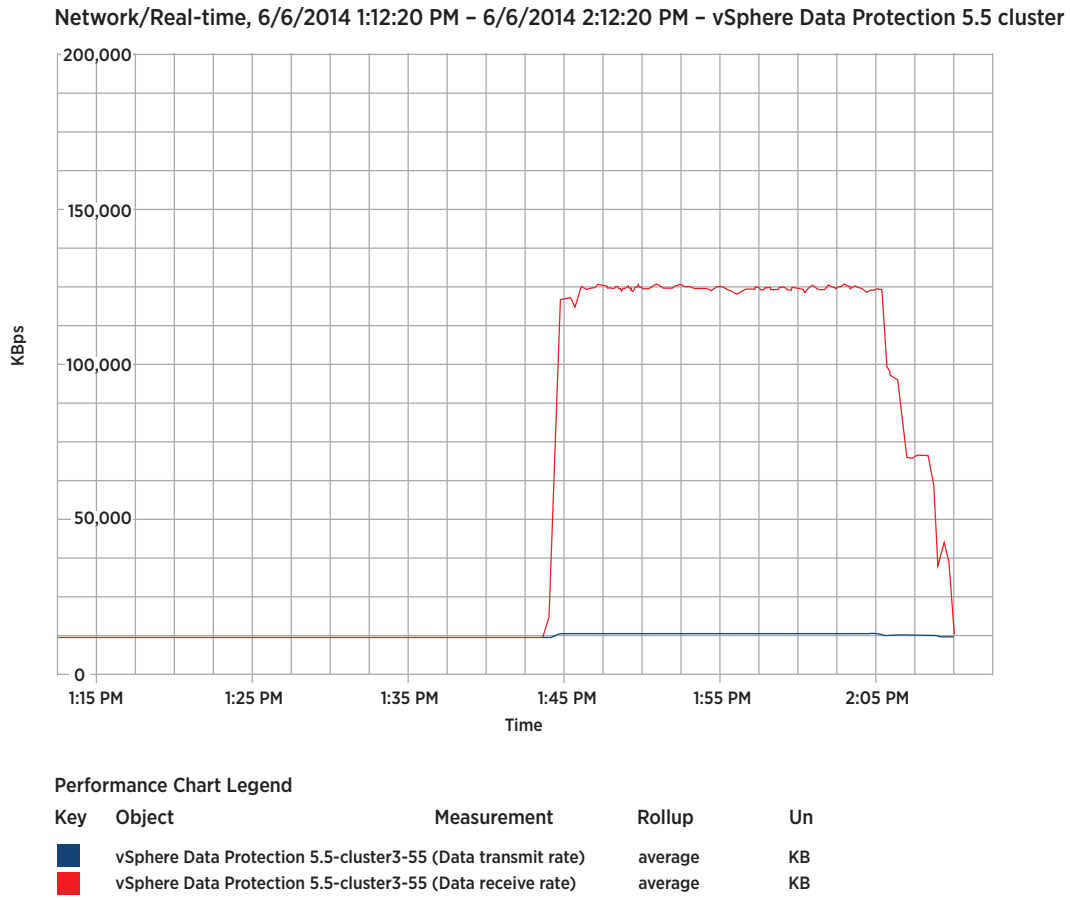


Figure 14. Network Throughput in the NBD/NBDSSL Mode

Conclusion

VMware Virtual SAN fully interoperates with VMware vSphere Data Protection Advanced. Virtual SAN can both be protected by vSphere Data Protection Advanced and be used as the vSphere Data Protection Advanced backup storage.

When planning for backup, it is important to understand where the potential bottlenecks might lie. Configuration of the vSphere Data Protection Advanced virtual appliance has impact on backup performance. When Virtual SAN is used as the backup target, it is beneficial to distribute components of the virtual appliance's backup disks onto more HDDs and SSDs in the Virtual SAN datastore.

In general, having more concurrent backup jobs helps improve the overall backup performance, but backup transport mode is an important factor to consider. SCSI HotAdd mode is usually faster than NBD/NBDSSL mode. In this mode, however, production data and backup data are stored in the same Virtual SAN datastore. It is recommended that backup data be replicated to a remote target to improve business continuity. The NBD/NBDSSL mode is slower and adds significant traffic to the VMware ESXi management network. Because a separate Virtual SAN cluster is used for backup, this mode has less performance impact on the production environment.

References

1. http://www.vmware.com/products/virtual-san/
2. *vSphere Data Protection Administration Guide* – http://pubs.vmware.com/vsphere-55/topic/com.vmware.ICbase/PDF/vmware-data-protection-administration-guide-555.pdf
3. Virtual Disk Development Kit Documentation – http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vddk.pg.doc%2FvddkDataStruct.5.5.html
4. *Essential Virtual SAN: Administrator's Guide to VMware Virtual SAN* by Cormac Hogan and Duncan Epping
5. *Backing up Virtual Machines on Virtual SAN with vSphere Data Protection Advanced and Data Domain* – http://blogs.vmware.com/vsphere/2014/03/backing-up-vsan-vdpa-data-domain.html

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

 Item No: VMW-WP-vSAN-BK-vSPHR-Dta-Prot-Adv-USLET-103 Docsource: OIC-FP-1193