Fast Backups in Virtual Environments

Design Blueprint and Benchmark Results

George Winter
Technical Product Manager, Veritas® NetBackup™
Symantec Corporation
May, 2009
6.0 HOW TO PROTECT 25 TB OF VIRTUAL MACHINE DATA .......................................................... 15
7.0 NETBACKUP FOR VMWARE — PERFORMANCE ADVANTAGES ............................................. 16
8.0 NETBACKUP CONFIGURATION TIPS ................................................................................. 17
   Aligning backup policies with storage ...................................................................................... 17
   Limiting simultaneous backups ................................................................................................ 17
   Tuning Backup Proxy Configuration ....................................................................................... 18
   Multiple Staging Areas ............................................................................................................. 18
   Best Practices .......................................................................................................................... 18
9.0 CONCLUSIONS AND NEXT STEPS .................................................................................. 18
10.0 APPENDICES ............................................................................................................ 19
   10.1 APPENDIX 1: HD_SPEED UTILITY ................................................................................. 19
   10.2 APPENDIX 2: GLOSSARY .............................................................................................. 20
   10.3 APPENDIX 3: ADDITIONAL RESOURCES ....................................................................... 20
Executive overview

Server virtualization is a new computing model that is transforming the world’s data centers. The economics are compelling—by using VMware infrastructure to virtualize servers and consolidate them onto high-performance computing hardware such as Sun x64 systems, organizations may:

• shrink physical server footprints
• cut power and cooling requirements
• raise server utilization to unprecedented levels
• improve service levels, respond quickly to changing business requirements, and improve business continuity and disaster recovery
• improve manageability of computing environments and make better use of skilled staff

Benefits like these are powering substantial year-over-year growth in virtualized computing solutions. But as virtualization projects make their way from development labs to production environments, pragmatic issues like deployment and maintenance, security, and data protection threaten to slow virtualization’s progress and compromise its value.

Effective management and security tools are now available with capabilities to meet the demands of virtualized enterprise production environments. But the performance of data protection solutions has remained an obstacle, in part because of the need to stage backups between virtual machines and backup storage targets without compromising server performance or extending backup windows beyond allowable limits.

Now, a groundbreaking joint effort by Sun®, Symantec™, and VMware® has combined Sun server and storage hardware, Symantec Veritas™ NetBackup™ software, and VMware virtualization solutions to deliver simplified, centralized, easy-to-manage protection for critical business information in virtualized production environments. Their combined efforts help organizations meet tight backup windows, improve storage utilization, implement flexible disaster-recovery plans, and manage the transition to virtual environments and disk-based backup—with archiving, migration, and retention capabilities ready to meet growing governance and regulatory requirements.

This paper documents production-ready performance of market-leading NetBackup software running on Sun hardware in VMware virtualized environments. It also provides detailed, point-by-point guidance that will help your staff achieve comparable performance in your own virtualized computing environment.
1.0 Solution overview

VMware introduced off-host backup technology, VMware Consolidated Backup (VCB), to its Virtual Infrastructure 3 specifically to support data protection in VMware virtual machine environments. Symantec Veritas NetBackup has supported VCB from the backup software’s 6.5.1 release.

Symantec has since enhanced its NetBackup solution with unique, patent-pending technology that raises the performance and flexibility of virtual environment data protection. NetBackup for VMware Granular File Restore is a dramatic advance that offers two efficient ways to back up Microsoft® Windows® virtual machines: full virtual machine (vmdk) restores, and individual (OS) file restores, all accomplished from a single, efficient backup pass.

Proper configuration of NetBackup for VMware using high-performance hardware such as Sun x64 servers and Sun StorageTek disk arrays eliminates bottlenecks to unlock the maximum performance potential of data protection for virtual environments.

This benchmark documents the performance, flexibility, and scalability now available for data protection in virtual environments, and recommends configurations, tests, procedures, and best practices for optimizing backup performance in your own environment.

2.0 Technology overview

Virtual machine backups involve three major components: the hardware environment, the VMware Consolidated Backup (VCB) process, and NetBackup for VMware.

2.1 Backup Proxy hardware environment

Proper testing and configuration of the hardware environment helps ensure the fastest possible backups. Initial testing also helps determine the number of virtual machines the ESX and backup proxy environment can protect. The backup proxy can be configured as a NetBackup master server, media server or client. We recommend that the backup proxy be configured as a media server, because the backup proxy processes a significant amount of backup data (see the NetBackup for VMware Best Practices guide for more information).

The backup proxy also stages vmdk data as part of the VMware Consolidated Backup process. Careful configuration of this staging area (also called the holding tank) helps ensure the fastest possible backups. Additional considerations include the storage connection type (Fibre Channel, iSCSI, NAS, etc.), backup proxy system, host bus adapter placement, etc. Proper implementation of each of these components is discussed in detail below.
2.2 VMware Consolidated Backup

VMware Consolidated Backup is not itself a backup application; it provides the virtual machine snapshot and export capability NetBackup uses. Understanding VCB can help determine the I/O impact of VCB processes on the ESX datastore, locations of any performance bottlenecks, and opportunities for hardware improvements to raise backup performance.

The VCB snapshot creation and export (vmdk backup) process works as follows:

1. NetBackup requests a virtual machine snapshot from the Virtual Center (or ESX) server. This process also ensures that the virtual machine is quiesced and prepared for backup.
2. vmdk files for the virtual machine are copied to a temporary staging area (holding tank) on the backup proxy.
3. The virtual machine snapshot is deleted.
4. NetBackup backs up the vmdk files, and performs a vmdk discovery phase that supports search and restoration of individual files from a single vmdk backup pass (Windows only).

2.3 NetBackup for VMware

The entire process described above is completely controlled and automated by the third enabling component, NetBackup for VMware. Proper configuration of NetBackup and its policies helps ensure the best possible backup performance. NetBackup for VMware integrates directly with the VMware Consolidated Backup Framework, controlling every step of the virtual machine backup process without scripting. NetBackup also provides Granular File restore the ability to perform a single file or full virtual machine restore from a single backup pass.

3.0 Benchmark configuration

Hardware selection and configuration are the most important considerations for optimizing backup performance. To minimize hardware and scaling constraints, this benchmark used the Sun Fire X4600 M2 server—designed for organizations that need more raw computing power than typical four-socket servers can provide. Combining technologies from Sun, AMD®, and VMware, the Sun Fire™ X4600 M2 server is also one of the most scalable virtualization platforms, reducing backup windows and increasing the amount of data a given backup system (or proxy) can process.
3.1 Backup proxy system selection

The backup proxy is the most important hardware component in any backup environment. It offloads I/O processing that occurs on the ESX servers themselves in local backup configurations. As a result, the backup proxy must efficiently process significant amounts of offloaded I/O. Selection criteria include:

**Internal bus speed** – Data transfers cross internal buses on the backup proxy, so bus performance limits backup processing speed for virtual machine data. Every host bus adapter (HBA) connected to a system transfers data over one or more of its busses — most often the Front Side Bus (FSB) which transfers data to the CPU. The speed of the FSB can be used as an indicator of overall internal bus performance.

**I/O slot capacity** – To avoid bottlenecks, each I/O source or destination should have its own host bus adapter on the backup proxy. Examples include connections between the backup proxy and ESX datastores, the staging area (holding tank), and backup destinations (tape, disk, etc.).

**CPU and Memory** – CPU performance memory capacity are also considerations when selecting the backup proxy, but they are less likely to limit performance, especially as 2 and 3 GHz multi-core processors become commonplace and memory prices decline.

3.2 Backup proxy system configuration

This benchmark used a Sun X4600M2 backup proxy configured as outlined in Table 1:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Proxy System</td>
<td>Sun X4600M2</td>
<td></td>
</tr>
<tr>
<td>RAM</td>
<td>64 GB</td>
<td>Minimum 8 GB recommended</td>
</tr>
<tr>
<td>CPU</td>
<td>2.29 GHz AMD Opteron</td>
<td>Quad Core, 4 socket</td>
</tr>
<tr>
<td>OS</td>
<td>Windows Server 2003 R2 SP2 (32bit)</td>
<td></td>
</tr>
<tr>
<td>Fibre Channel HBA</td>
<td>QLogic QLE2462</td>
<td>4 Gb Fibre Channel</td>
</tr>
</tbody>
</table>

Table 1 - Backup Proxy Configuration

The CPU performance and RAM capacity provided by the X4600M2 makes it ideal for enterprise virtualization performance and scalability. For this specific benchmark, a two-socket quad-core Sun server with 16 GB RAM would have been adequate.
3.3 Backup proxy staging area (holding tank)

The benchmark configuration used two staging areas (holding tanks), each connected to its own storage array through a Fibre Channel host bus adapter. Staging areas were formatted to the default NTFS allocation unit size. Because staging area I/O patterns involve simultaneous reads and writes, volumes were configured as RAID 0 to optimize I/O performance.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Arrays (2)</td>
<td>Sun StorageTek 6140</td>
<td></td>
</tr>
<tr>
<td>Disk Drives</td>
<td>300 GB 15,000-rpm Fibre Channel</td>
<td></td>
</tr>
<tr>
<td>Cache size</td>
<td>4 GB data cache</td>
<td></td>
</tr>
<tr>
<td>File system</td>
<td>NTFS</td>
<td></td>
</tr>
<tr>
<td>Size</td>
<td>300 GB</td>
<td></td>
</tr>
</tbody>
</table>

Table 2 - Backup Proxy Staging Area

3.4 Backup proxy storage units

This benchmark used Basic Disk storage units, although other NetBackup-supported storage units (disk, tape, Virtual Tape Library (VTL), and many others) would work as well. The main consideration is that the backup destination not limit end-to-end backup performance. The 4Gb Fibre Channel 6140 proved to have capacity well beyond the requirements of this benchmark—and Sun is now standardizing their entire 6000 series on 8Gb Fibre Channel. In dynamic datacenter environments, the 6000 series allows expanding the tray array without modifying the data.

3.5 ESX server environment

VMware ESX is the high-performance hypervisor now included with VMware vSphere 4. The benchmark backup environment included four VMware ESX servers, each configured with its own datastore. Virtual machines hosted on each of the ESX servers were configured with a mix of Windows and Linux virtual machines, as shown in Table 3.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESX Server</td>
<td>V3.5 U3</td>
<td></td>
</tr>
<tr>
<td>Server hardware</td>
<td>Sun Fire X4150 Server</td>
<td>64-bit</td>
</tr>
<tr>
<td>Virtual Machine OS</td>
<td>Windows 2003, 2008, RHEL 5.1</td>
<td>Both 32- and 64-bit Windows OS</td>
</tr>
<tr>
<td>Virtual Machine Sizes</td>
<td>20 GB, 50 GB, 100GB</td>
<td></td>
</tr>
<tr>
<td>Window VM File System</td>
<td>NTFS</td>
<td></td>
</tr>
<tr>
<td>Linux VM File System</td>
<td>ext3</td>
<td></td>
</tr>
<tr>
<td>Total amount of VM data</td>
<td>1 TB per ESX server</td>
<td>4 TB total VM data</td>
</tr>
</tbody>
</table>

Table 3 - ESX Server Environment
3.6 NetBackup configuration

Hardware configuration is critical, but NetBackup also requires some configuration. Out-of-the-box NetBackup buffer settings perform well in most environments, including our benchmark environment. We were able to achieve some improvement by fine-tuning settings to the values listed in Table 4. If you choose to modify settings from the NetBackup defaults, we highly recommend that you test them before implementation – it is unlikely that our benchmark settings will be optimal for your environment.

<table>
<thead>
<tr>
<th>NetBackup Setting</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetBackup Version</td>
<td>6.5.3</td>
<td></td>
</tr>
<tr>
<td>NetBackup Storage Unit Type</td>
<td>BasicDisk</td>
<td></td>
</tr>
<tr>
<td>NUMBER_DATA_BUFFERS</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>SIZE_DATA_BUFFERS</td>
<td>524288</td>
<td></td>
</tr>
<tr>
<td>NUMBER_DATA_BUFFERS_DISK</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>SIZE_DATA_BUFFERS_DISK</td>
<td>1048576</td>
<td></td>
</tr>
<tr>
<td>Number of NetBackup Policies</td>
<td>4</td>
<td>One per ESX datastore</td>
</tr>
<tr>
<td>Limit Jobs Per Policy</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Max Concurrent Jobs</td>
<td>3 per storage unit</td>
<td>Max number jobs total = 6</td>
</tr>
</tbody>
</table>

Table 4 - NetBackup Settings

To tune the “Max Concurrent Jobs” storage unit setting, we used the performance baseline numbers (Section 5.0) to estimate the hardware capabilities. We then performed a series of test backup runs, increasing the “Max concurrent jobs” setting until performance had peaked.

To eliminate I/O bottlenecks on ESX datastores, we tied the “Number of NetBackup Policies” setting to the number of datastores: one per datastore; four in all. To avoid overloading any individual datastore with backup processing, the “Limit Jobs per Policy” setting was set to two for all policies. By making sure no datastore was ever tasked with more than two backups, we spread I/O evenly across the datastores. This approach is detailed in section 1.2 of the Symantec document, *NetBackup for VMware Best Practices Guide*. 
4.0 Performance Baseline Testing

Administrators often complain that their backups are slow—but compared to what? Theoretical hardware performance is a poor indicator of real-world backup speed, and comparisons from one backup environment to another are seldom valid. Before bringing a backup environment into production, we highly recommend testing to establish an objective performance baseline—one you can use as a reference point when you evaluate new hardware or configurations, or troubleshoot the environment. This section details our own performance baseline testing in advance of the benchmark tests.

Main Configuration Diagram

Figure 1 diagrams the backup environment we used to establish baseline performance. We measured four main data transfer points:

- Read performance of each ESX datastore
- Read performance of each staging area (holding tank)
- Write performance of each staging area
- Write performance of the destination Storage Unit (in this case, disk)

We took each measurement from the perspective of the backup proxy, and designed the tests to include the smallest possible number of hardware components for maximum granularity, so we could identify, isolate and repair performance bottlenecks quickly. We used the free “HD_Speed” utility to determine the performance of our I/O subsystems during basic read-write I/O testing (see section 8.0 for details).
4.1 Datastore read performance

During the VMware Consolidated Backup process, virtual machine data is read from the ESX datastore and sent to the backup proxy staging area. Datastores are typically designed and configured separately from the backup environment, so even if datastore read performance is a constraint, backup administrators may be unable to do anything about it. But administrators should still understand and measure datastore performance so they can set expectations for backup performance.

This first test used the HD_Speed utility (see Appendix 1: HD_Speed Utility) to determine the baseline read performance of each datastore. We used the utility’s nondestructive I/O read tests, which simulate the frequent reads of virtual machine files during the VCB process, to measure read I/O capacity of each ESX datastore. Because we performed this test from the backup proxy, its I/O pattern didn’t precisely match VCB process I/O. But it does provide an accurate assessment of the datastore read performance. Table 5 shows the results:

<table>
<thead>
<tr>
<th>ESX Storage</th>
<th>Read Performance</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datastore 1</td>
<td>219MB/sec</td>
<td>RAID 1+0</td>
</tr>
<tr>
<td>Datastore 2</td>
<td>221MB/sec</td>
<td>RAID 1+0</td>
</tr>
<tr>
<td>Datastore 3</td>
<td>224MB/sec</td>
<td>RAID 1+0</td>
</tr>
<tr>
<td>Datastore 4</td>
<td>218MB/sec</td>
<td>RAID 1+0</td>
</tr>
</tbody>
</table>

Table 5 - ESX Datastore Read Performance

4.2 Staging area configuration and performance

The staging area — also called the holding tank — is the most performance-critical component of a VMware Consolidated Backup configuration. Proper staging area design pays significant dividends in backup performance. This list outlines recommendations for improving staging area performance, and details the staging area configuration used in the benchmark:

**Size** — Staging areas should be kept under 1 TB: larger staging areas consume excessive system memory without adding much value. Staging areas should be dedicated partitions, and free of other data to avoid file-system fragmentation that could hurt performance. Our benchmark used two staging areas, each configured as a 300 GB partition, to accommodate the largest virtual machine (100 GB).

**File system** — We used the default file system allocation unit size for the staging area: 4096 for a 300 GB partition (http://support.microsoft.com/kb/140365).

**RAID Configuration** — The staging area should be configured across as many dedicated (i.e., unused by other I/O processes) spindles as possible. We recommend RAID 0 to balance performance and affordability. Staging areas are not permanent data stores, so moderate availability levels can generally be tolerated — however, RAID 1+0 (RAID 10) is a good choice when a highly available staging area is required. For the benchmark, we configured each staging area as a RAID 0 LUN on top of 8 dedicated spindles.

**Connectivity** — To eliminate I/O bottlenecks, we highly recommend following our practice of using a separate host bus adapter for each individual datastore, staging area, storage unit, or other major component.
4.2.1 Staging area write I/O

The VMware Consolidated Backup process reads or copies virtual machine (vmdk) data from the ESX datastore and writes it to the backup proxy staging area(s) for temporary storage. Our second test determined the maximum write performance of the backup proxy staging area. We ran the HD_Speed utility from the backup proxy as before, but configured it to perform sustained writes to the staging area. Write operations are much more “expensive” (in terms of time and system resources) than reads, so we expected significantly lower I/O performance. The results of this test are shown in Table 6.

Please note that HD_Speed write tests are destructive: this test wipes out the staging area file system. When this test is complete, you will need to recreate the NTFS file system for the staging area. We urge extreme caution when running this test, and recommend you perform it on pre-production systems only.

4.2.2 Staging area read I/O

Once the VCB process has finished writing virtual machine (vmdk) data to the staging area, the data is copied to the NetBackup destination storage unit. This phase of the VCB process is characterized by a high volume of staging area disk reads. Our third series of tests configured HD_Speed to perform sustained (non-destructive) disk reads, again from the backup proxy, to test staging area read performance. These results are also listed in Table 6.

<table>
<thead>
<tr>
<th>Component</th>
<th>Performance</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staging area 1</td>
<td>Read = 225 MB/sec, Write = 85 MB/sec</td>
<td>RAID 0 across 8 disks</td>
</tr>
<tr>
<td>Staging area 2</td>
<td>Read = 225 MB/sec, Write = 85 MB/sec</td>
<td>RAID 0 across 8 disks</td>
</tr>
</tbody>
</table>

Table 6 - Staging area Performance

4.2.3 Storage unit performance

NetBackup supports many storage unit types: simple disks, tape drives, virtual tape drives, deduplication targets, and more. To simulate them, this benchmark configured two disk storage units, each connected to the backup proxy through its own host bus adapter and configured using RAID 1+0. One unit was configured over 8 striped spindles, the other over 12 spindles. Backups write data to both units, so we tested their using HD_Speed as before. These results are shown in Table 7.

<table>
<thead>
<tr>
<th>Component</th>
<th>Performance</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Storage Unit 1</td>
<td>Write = 85 MB/sec</td>
<td>RAID 1+0 across 8 disks</td>
</tr>
<tr>
<td>Disk Storage Unit 2</td>
<td>Write = 130 MB/sec</td>
<td>RAID 1+0 across 12 disks</td>
</tr>
</tbody>
</table>

Table 7 – Disk Storage Unit Performance
4.3 Additional performance tests

The tests described above help estimate performance and uncover configuration problems. Additional tests can further isolate performance issues, and more accurately simulate the real-world performance of virtual machine backup proxy systems:

4.3.1 Between ESX datastore and proxy staging area

The vcbMounter.exe command runs from the backup proxy, and executes the same data transfer process that occurs during VCB. Running vcbMounter simultaneously tests the read performance of the ESX datastore, the transfer rate of the connection (here 4 Gb Fibre Channel) between datastore and backup proxy, and the write capabilities of the backup proxy staging area. This test very closely simulates actual operating conditions during VMware Consolidated Backups.

4.3.2 Between the staging area and the NetBackup storage unit

Our first test of staging area read performance used the HD_Speed utility and did not involve NetBackup. However, a full end-to-end test of performance between the staging area and NetBackup storage unit is easy to configure: put file data in a folder on the staging area, create a NetBackup Policy to back up the data, and measure how long execution takes. By inserting NetBackup itself into the performance equation, this test helps expose performance issues from improper NetBackup configuration.

4.3.3 Simultaneous backup and restore of the staging area

VMware Consolidated Backups write data to the Staging Area while copying data from the Staging Area to the NetBackup storage unit. These simultaneous operations can create a significant I/O load on the staging area. This test accurately measures the total I/O performance available from the staging area:

1. Run a vcbMounter.exe command from the backup proxy. This initiates copying of virtual machine data to the staging area.
2. As soon as vcbMounter.exe is running, initiate the standard file system policy (created in section 4.3.2 above).

With both vcBMounter.exe and the standard file system policy running, data is being written to the staging area, and simultaneously read from it, testing whether the Staging Area can process these simultaneous I/O requests. Since the Staging Area is typically the slowest device in the entire VMware Consolidated Backup I/O path, it will determine the maximum performance obtainable by the backup proxy system as a whole.
5.0 Benchmark results

Backups in virtual environments differ in several important ways from typical backups. The most important practical difference is time to complete. In physical environments, backup processes read data from a source and stream it to a destination. VMware Consolidated Backups involve an additional step, in which data are first written or “staged” to an intermediate disk device (staging area, or holding tank). Even when the entire process is under full automated control of NetBackup, two-stage backups necessarily take longer than otherwise equivalent one-stage backups.

We will report two sets of performance benchmarks. The first uses the default configuration described above; it applies directly to today’s established backup environments and processes. The second set of performance benchmarks uses new internal NetBackup cache settings included in the NetBackup 6.5.4 release. These settings significantly accelerate virtual machine backups in VCB environments using NetBackup.

5.1 Results – default configuration

Using the configuration as described in section 3.0, the overall backup performance measured:

Default Configuration Backup Performance = 227.1 GB/hour

If virtual machines in a backup environment average 20 GB of data, a single backup proxy can protect more than 545 of them, assuming a) a 48-hour (weekend) backup window and b) all backups are full backups. NetBackup’s unique incremental backup technology can extend coverage even further, as discussed below.

5.2 Results – enhanced cache settings

In an effort to boost backup performance in virtual environments, NetBackup engineering has incorporated a new internal cache setting specific to VMware Consolidated Backup environments. This benchmark test increased the NetBackup for VMware cache setting to 2048kB from the default 512kB, for a 30% improvement in overall backup performance:

Enhanced Cache Setting Backup Performance = 285.1 GB/hour

Using this new setting, a single backup proxy can protect more than 700 20GB virtual machines with full backups during a 48-hour weekend backup window.

5.3 Results – incremental backups

In Windows environments, file-level incremental backups are another way to extend backup proxy performance. File-level incremental backups are unique to NetBackup, the only backup application that discovers, indexes and catalogs all files during full vmdk backups and allows full granular file-level restoration. During vmdk scans, the file discovery process catalogs and indexes all attributes of every virtual machine file—information NetBackup uses as the basis for its full backup. Later backups use VMware Consolidated Backup’s file-level backup capability to send the backup proxy only new or changed files.
By replacing full vmdk backups with efficient file level incremental backups, NetBackup allows a single backup proxy to protect many more virtual machines. File level incremental backups are especially effective in VCB environments because file-level virtual machine image mount and file backup processes are extremely fast and efficient: once files have been discovered, they can be transferred directly to the backup destination without first being copied to the backup proxy staging area. Eliminating file staging removes a major obstacle to backups in virtual environments, and significantly improves backup processing performance. Neither full vmdk backups nor file-level incremental backups require installation of client software on virtual machines.

We tested file-level incremental backups by changing data in 10% of all virtual machines before running a single streamed backup job. Performance measured 24.3 MB/sec — marginally slower than a vmdk-level backup because incremental backups require a full scan of the files in every virtual machine. But this was only a single stream: multiple incremental backup jobs can be run simultaneously. If we ran the same 6 data streams for incremental backups that we used during full VM backups, we calculate incremental backup performance at:

\[
\text{Incremental file-level backup performance} = 173.5 \text{ GB/hour}
\]

This approach avoids copying all vmdk files for a Windows virtual machine to protect minor changes. The size of the virtual machine doesn’t even matter — the amount of new or changed data, not the size of the virtual machine, determines backup speed. Thus 10 GB of new data can be protected as quickly on a 500GB virtual machine as on a 100 GB machine. Our tests prove that these backup times are extremely fast: we were able to perform an incremental (10% data change) backup of a 100 GB virtual machine in just 7 minutes.

### 6.0 How to protect 25 TB of virtual machine data

NetBackup 6.5.2 introduced file-level incremental backup technology for Windows virtual machines. The approach updates full backups performed at the vmdk level using incremental backups performed at the file level — dramatically expanding the amount of virtual machine data a single backup proxy can protect. In this section, we illustrate how to configure a backup proxy to protect as much as 25 TB of virtual machine data.

This sizing exercise assumes:
- backup proxy performance as measured in the benchmark
- full backups scheduled in two-week rotation, i.e., full backups every two weeks
- backup windows of 10 hours on weeknights; 48 hours on weekends
- data change between backups (churn) averaging 5%

Using enhanced NetBackup cache settings and 6 data streams for incremental backups, the preceding section gave us these performance data (backup rates):

- Backup rate (full): 285.1 GB/hr
- Backup rate (incremental): 173.5 GB/hr
We multiply backup rates by the time scheduled for full and incremental runs to determine the amount of data a single proxy can protect:

\[
\text{Backup rate (GB/hr) x backup window (hr) = protected virtual machine data (GB)}
\]

For full backups:

\[
(285.1 \text{ GB}) \times (48 \text{ hours}) = 13,685 \text{ GB} = 13.6 \text{ TB of protected data}
\]

With the capacity to protect 13.6 TB of virtual machine data in a single 48-hour weekend backup window, a single proxy can provide full backups for more than 25 TB over a two-week rotation.

For incremental backups:

\[
(173.5 \text{ GB}) \times (10 \text{ hours}) = 17,350 \text{ GB} = 1.7 \text{ TB of protected data}
\]

With the capacity to protect 1.7 TB of new data in a 10-hour weeknight shift, one backup proxy can easily accommodate the 5% “churn” of an average day (25TB x .05 = 1.25 TB).

The combination of NetBackup for VMware Granular File Restore and VMware file-level backup protects more than 25 TB of virtual machine data with daily incremental backups and full backups every two weeks.

### 7.0 NetBackup for VMware — performance advantages

Performance is an important consideration when selecting technology for virtual machine backups. Another is the load imposed by backup processes on ESX servers while their virtual machines are being protected. High-performance ESX servers can support large numbers of virtual machines. The Sun Fire X4600 M2 servers used in this benchmark, for example, through processor adds and upgrades, can scale as high as eight sockets of enhanced Quad-Core AMD Opteron processors. Such an ESX server can manage more than twice the number of active virtual machines as a four-socket system with Third-Generation Quad-Core AMD Opteron processors — a total of 114 virtual machines.

This consolidation of virtual machines onto physical hosts carries a downside. A physical system hosting 50 virtual machines needs to back up 50 separate operating systems with all their associated data. The VMware Consolidated Backup API was designed to address this issue.
To assess the impact of VMware Consolidated Backup processes on ESX server performance, we measured system resources consumed by an ESX server during a standard backup run. Figure 2 shows utilization of the ESX server CPU as reported by the Virtual Center Server, with the start and finish of a backup run indicated by arrows (the periodic peaks are caused by background processes unrelated to backup activity).

Next, we measured the impact of VMware Consolidated Backup processes on ESX datastores, as shown in Figure 3. Snapshot creation and deletion are visible in the CPU usage history. But from the perspective of the ESX server, backups have little I/O impact on the ESX datastore. This emphatically does not mean that datastore I/O is limited—in fact, during the transfer of vmdk files to the backup proxy, a considerable amount of I/O occurs.

Loads on the backup proxy system itself are another potential issue, at least in theory. We measured peak system loads on the backup proxy during a VMware Consolidated Backup run (Figure 4). These were very low, based both on CPU measurements and system memory requirements. These results reinforce the *NetBackup for VMware Best Practices* recommendation that in selecting and configuring a backup proxy I/O capacity, not processor or memory loads, should be the primary consideration.

![CPU Load During Backups and Memory Consumption During Backups](image)

**Figure 4 – Backup Proxy System Load**

### 8.0 NetBackup configuration tips

Up to this point we have considered primarily the hardware aspects of virtual machine backups. Proper configuration of NetBackup can also accelerate backups. Incremental backups do this by minimizing daily backup volume. Other NetBackup configuration methodologies used in this benchmark include:

**Aligning backup policies with storage**—our benchmark configuration used four ESX datastores. We configured policies that associated every virtual machine with a specific datastore, controlling the number of backups occurring against any datastore, and minimizing I/O impacts.

**Limiting simultaneous backups**—most environments will support between 3 and 6 simultaneous backups.

**These are just guidelines**—you should determine actual numbers for your environment during your initial testing to establish a performance baseline. We recommend establishing and observing a limit, because too many simultaneous backups can slow overall backup speed.
Tuning Backup Proxy Configuration — your VMware backup proxy may be configured as a NetBackup master server, media server or enterprise client—we recommend configuring it as a media server. The backup proxy is a natural focal point for backup-related I/O, with backup proxy access to VM files through a fast Fibre Channel or iSCSI connection (NetBackup 6.5.2 also supports a NAS-based datastore). In most configurations, it makes sense to avoid configuring the backup proxy as a NetBackup enterprise client, since this forces all VM backup data through the NetBackup client network, which is typically a slow, shared resource.

Multiple Staging Areas — the staging area (holding tank) can be an I/O bottleneck. Additional staging areas spread out I/O, allowing significantly faster backups. If you add a staging area to your environment, be sure your backup proxy’s internal bus structure can support the I/O it will require.

Best Practices — this benchmark used information provided in section 1.2 of the Symantec document NetBackup for VMware Best Practices, available from the Symantec Web site. We highly recommend that you use the information and recommendations in this document when configuring your own VMware Consolidated Backup environment.

9.0 Conclusions and Next Steps

Concerns about data protection need no longer interfere with virtualization initiatives to consolidate servers, reduce costs, and improve IT agility. As this benchmark study has demonstrated:
• the combined technologies of VMware, Symantec, and Sun are more than equal to the requirements of protecting data in enterprise-scale virtualized environments
• careful attention to configuration of the backup proxy system — especially I/O processing — can overcome performance limits that once looked insurmountable
• new features including powerful Sun server and storage hardware and increased NetBackup buffer capacity and other capabilities are constantly expanding the range of possibilities
• based on the results of this benchmark study, a single backup proxy is adequate to protect even 25 TB of virtual machine data under real-world production conditions
• improvements in backup performance need not come at the expense of ESX server performance or backup proxy system CPU load and memory consumption

This benchmark document, together with its Symantec companion document NetBackup for VMware Best Practices Guide, are your first steps toward unlocking the full benefits of virtualization in your computing environment, without risking the critical data on which your business depends.
10.0 Appendices

10.1 Appendix 1: HD_Speed Utility

Disk manufacturers publish I/O performance data for their hard drives are based on tests in perfect, controlled circumstances; these can overestimate performance in real operating environments. Local factors that can impact performance include connection type (IDE/SCSI/SATA), disk and host controller cache, OS type, file system type, internal bus on host, and more.

We wanted to measure the performance we could expect from I/O devices operating in our backup environment, not calculate theoretical performance from manufacturer performance figures. We used HD_Speed, an I/O performance testing utility available at http://www.steelbytes.com.

HD_Speed is small (<100 KB) Windows utility that measures sustained and burst data transfer rates of disk drives, and provides a real-time graphic display of results (Figure 5). An alternative to HD_Speed is Iometer (http://www.iometer.org), created by Intel Corporation and now available from SourceForge.net. Iometer supports other OS types as well as Windows.

We used HD_Speed to stress-test I/O subsystems before running any benchmarks. The tests helped us find and correct performance and hardware configuration issues to help us rule out I/O performance issues that would have complicated our analysis of backup environment performance.

WARNING: No matter which utility you use, we strongly recommend that I/O testing be performed only on non- or pre-production systems. Testing I/O writes with HD_Speed destroys all data on tested devices. Before running any tests, make sure you understand their implications, and take necessary steps to avoid destruction of valuable data.
10.2 Appendix 2: Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Proxy</td>
<td>System designated as the off-host backup. At a minimum, the Backup Proxy includes the VMware Consolidated Backup Framework and NetBackup client.</td>
</tr>
<tr>
<td>Datastore</td>
<td>The ESX server storage. Virtual machine (vmdk) files are created here.</td>
</tr>
<tr>
<td>Holding Tank</td>
<td>Staging Area, see below</td>
</tr>
<tr>
<td>Staging Area</td>
<td>An NTFS-formatted disk volume created on the backup proxy that stores virtual machine (vmdk) files temporarily as part of the VMware Consolidated Backup process.</td>
</tr>
<tr>
<td>Sync Driver</td>
<td>Installed via VMware Tools to flush OS buffers (Windows only) prior to VMware Consolidated Backup snapshots. See also VSS Writer, below.</td>
</tr>
<tr>
<td>VCB</td>
<td>VMware Consolidated Backup Framework, see below.</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Software that creates a virtualized environment between the computer platform and its operating system, so that the end user can install and operate software on an abstract machine. Note that the virtual machine designation does not imply any specific operating system version.</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine, see above.</td>
</tr>
<tr>
<td>VMDK</td>
<td>The collection of files that make up a VMware virtual machine, called “vmdk” from their file extension.</td>
</tr>
<tr>
<td>VMware Consolidated Backup Framework</td>
<td>Backup API created by VMware to offload backup processing from the ESX server.</td>
</tr>
<tr>
<td>VMware Tools</td>
<td>Set of utilities installed in virtual machines to enhance their performance and add backup functionality.</td>
</tr>
<tr>
<td>VSS Writer</td>
<td>Volume Shadow Copy Service writer — replaces Sync Driver beginning with the ESX 3.5 U2 release.</td>
</tr>
</tbody>
</table>

10.3 Appendix 3: additional resources

**Sun**

Proven Virtualization Scalability – Consolidate More on Sun. An introduction to advanced hardware solutions engineered for high performance and scalability in virtualized environments

**Sun Fire X4150 Server Data Sheet**
http://www.sun.com/servers/x64/x4150/datasheet.pdf

**Sun Fire X4600 M2 Server Data Sheet**
http://www.sun.com/servers/x64/x4600/datasheet.pdf

**Sun StorageTek 6140 Array Data Sheet**

**Sun StorageTek 2540 Array Data Sheet**
Symantec


Veritas NetBackup 6.5.2 Documentation Updates. Chapter 2 details how to configure and use the NetBackup for VMware feature set – http://support.veritas.com/docs/302438

Veritas NetBackup 6.5.3 Documentation Updates. Includes detailed information specific to NetBackup for VMware – http://support.veritas.com/docs/305408

Veritas NetBackup™ Snapshot Client Configuration. Discusses supported components in a NetBackup for VMware environment – http://support.veritas.com/docs/288300

Veritas NetBackup™ Backup Planning and Performance Tuning Guide. Provides significant detail related to NetBackup Media Server (and the Backup Proxy) – http://support.veritas.com/docs/307083

VMware

VMware Hardware Compatibility Guide. A Web-based searchable guide to compatibility with systems, SAN, I/O devices, etc. – http://www.vmware.com/resources/compatibility/search.php


Third-party

About Sun

Sun Microsystems develops the most innovative products and services that power the network economy. Guided by a singular vision, “The Network is the Computer”, Sun drives network participation through shared innovation, community development and open source leadership. Headquartered in Santa Clara, Calif., Sun maintains operations in more than 100 countries. For more information, please visit www.sun.com

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

About VMware

VMware is the global leader in virtualization solutions from desktop to datacenter, with a wide range of award-winning virtualization products, that help its customers reduce capital and operating expenses, ensure business continuity, strengthen security and go green. Headquartered in Palo Alto, Calif., VMware is one of the fastest growing public software companies. For more information, please visit www.vmware.com.