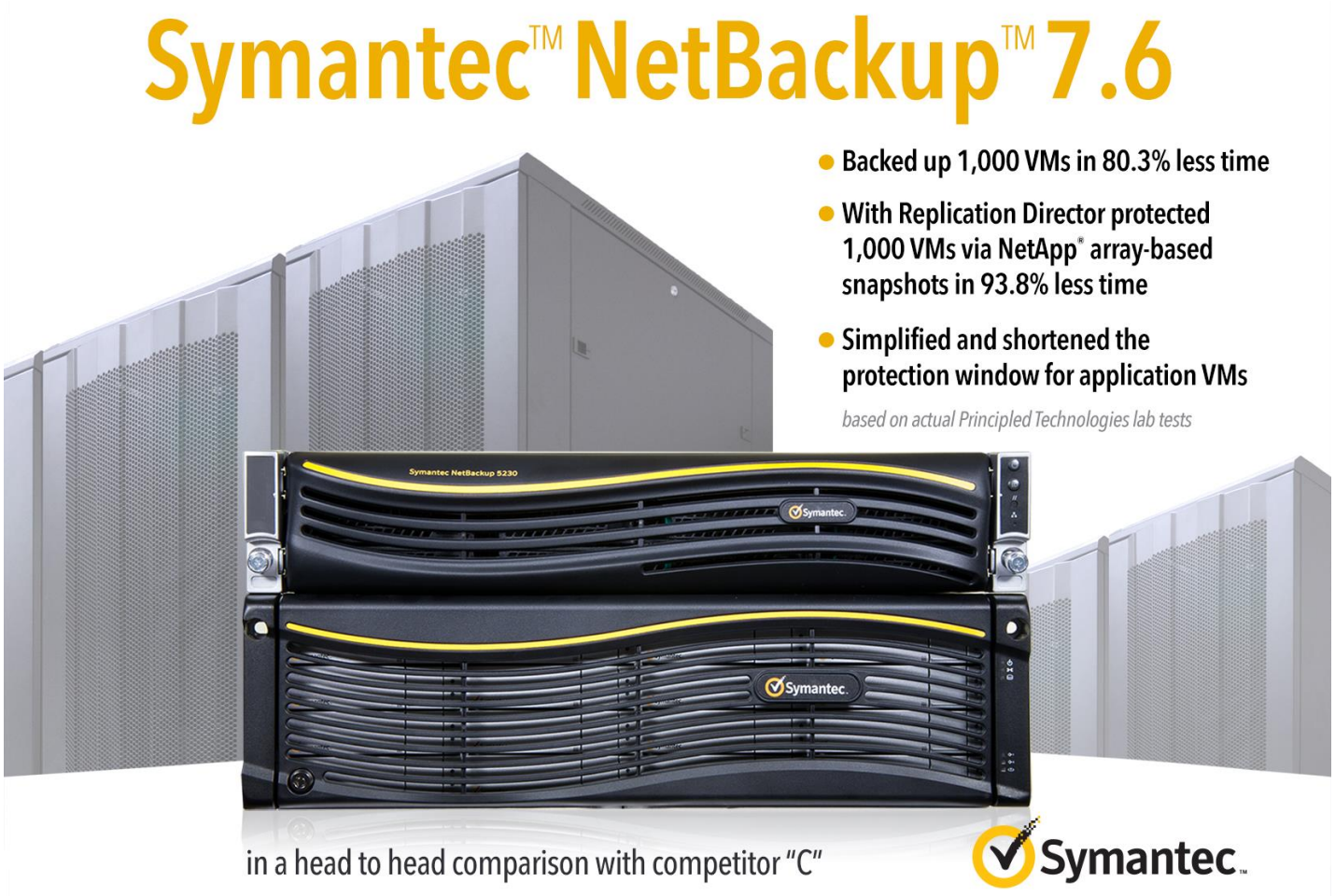
SYMANTEC NETBACKUP 7.6 BENCHMARK COMPARISON: DATA PROTECTION IN A LARGE-SCALE VIRTUAL ENVIRONMENT (PART 1)



Virtualization technology is changing the way data centers work. Technologies such as VMware® vSphere® shrink the physical footprint of computing hardware by increasing the number of virtual servers. Within the enterprise, large-scale deployments of thousands of virtual machines are now common. To protect the data on these virtual systems, enterprises employ a variety of backup methods including hardware snapshots, hypervisor-level backup (vStorage APIs for Data Protection (VADP) in the case of VMware technology), and traditional agent-in-guest methods. Enterprises that utilize both block Storage Area Network (SAN) systems and file-based Network-Attached Storage (NAS) may scale more effectively, but backup and recovery systems must fully leverage the strengths of each platform to provide efficient service with minimal impact to the production environment.

In our hands-on testing at Principled Technologies, we wanted to see how leading enterprise backup and recovery solutions handled large-scale virtual machine (VM) deployments based on vSphere. We tested a solution using industry-leading Symantec NetBackup software and the Symantec NetBackup Integrated Appliance, with NetApp FAS3200-series arrays to host the VMs, and a comparable solution from another

JULY 2014 (Revised)

A PRINCIPLED TECHNOLOGIES TEST REPORT

(First of a three-part series)

Commissioned by Symantec Corp.

leading competitor (Competitor "C"). We tested two types of scenarios: one that utilized SAN storage and one that utilized NAS storage. In both scenarios, we tested with increasing populations of VMs—as low as 100 and as high as 1,000–to see how each solution scaled as the environment grew.

We found that NetBackup 7.6 with the NetBackup Integrated Appliance, featuring capabilities such as Accelerator, Replication Director, and Instant Recovery—all for VMware vSphere—provided a more scalable solution than the Competitor "C" platform. With 1,000 VMs, NetBackup completed the SAN transport backup in a Fibre Channel SAN environment in 80.3 percent less time than the Competitor "C" solution. In the NAS scenario with 1,000 VMs, Replication Director created recovery points via NetApp array-based snapshots in 93.8 percent less time than the Competitor "C" solution.

In our tests, Symantec NetBackup with the NetBackup Integrated Appliance provided superior scalability needed to protect the largest virtual server deployments, when compared to the Competitor "C" solution.

WHAT WE COMPARED

Backup via VMware vStorage APIs for data protection

Using the NetBackup Integrated Appliance as both media server and backup storage, we tested how long it took to execute backup with virtual application protection. Using the breakdown illustrated in Figure 5, we performed full backups with application protection on groups of VMs from 100 to 1,000, measuring the backup time elapsed.

Backup via storage-array snapshots

We rebuilt our storage network and datastores as NFS and used NetBackup Replication Director to create crash-consistent backups of NAS-based NFS storage at 100-, 200-, 500-, and 1,000-VM counts, as well as a 1,000-VM application-consistent backup, and then performed the same tests on Competitor "C." We captured metrics on backup speed, hardware performance, and to determine if there was any performance degradation in the environment, as well as the administrative time required for each test.

OUR ENVIRONMENT

We set up the test environment using 20 Dell™ PowerEdge™ M420 server blades running VMware vSphere ESXi 5.5. Figure 1 shows how we configured our data network. We used this configuration universally on SAN and NAS testing. Figure 2 shows our storage network for vStorage APIs-based backup testing, and Figure 3 shows our storage network for storage-array snapshot-based backup testing.

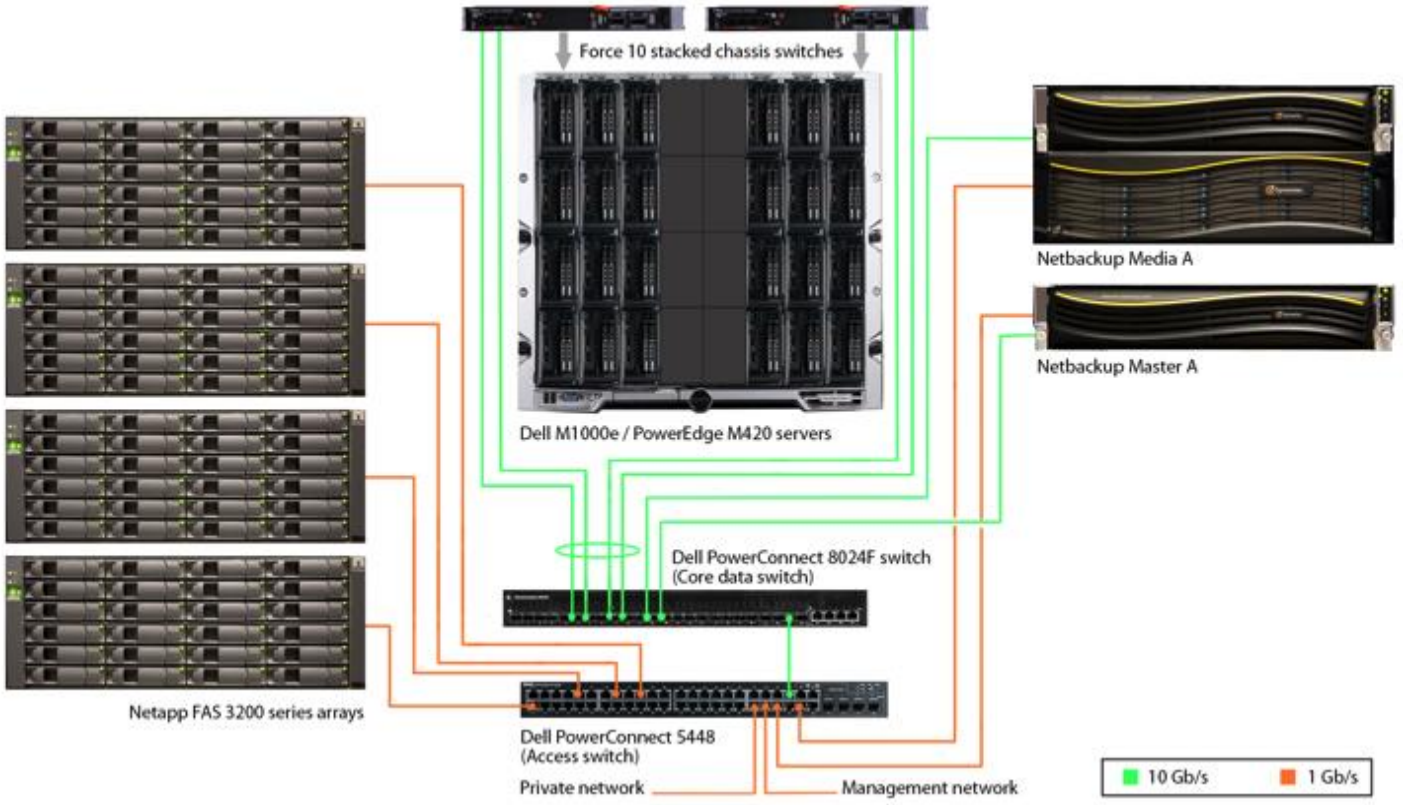


Figure 1: Detailed test bed layout: data network.

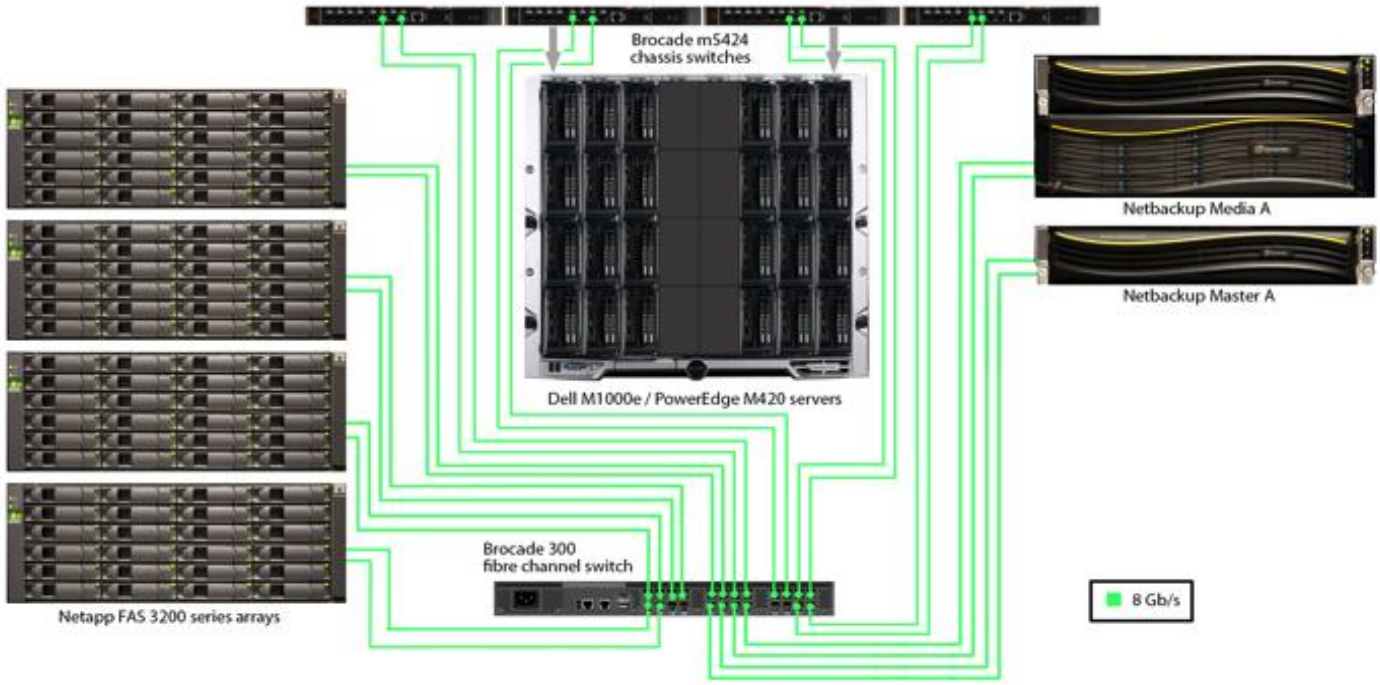


Figure 2: Detailed storage network: vStorage APIs-based backups.

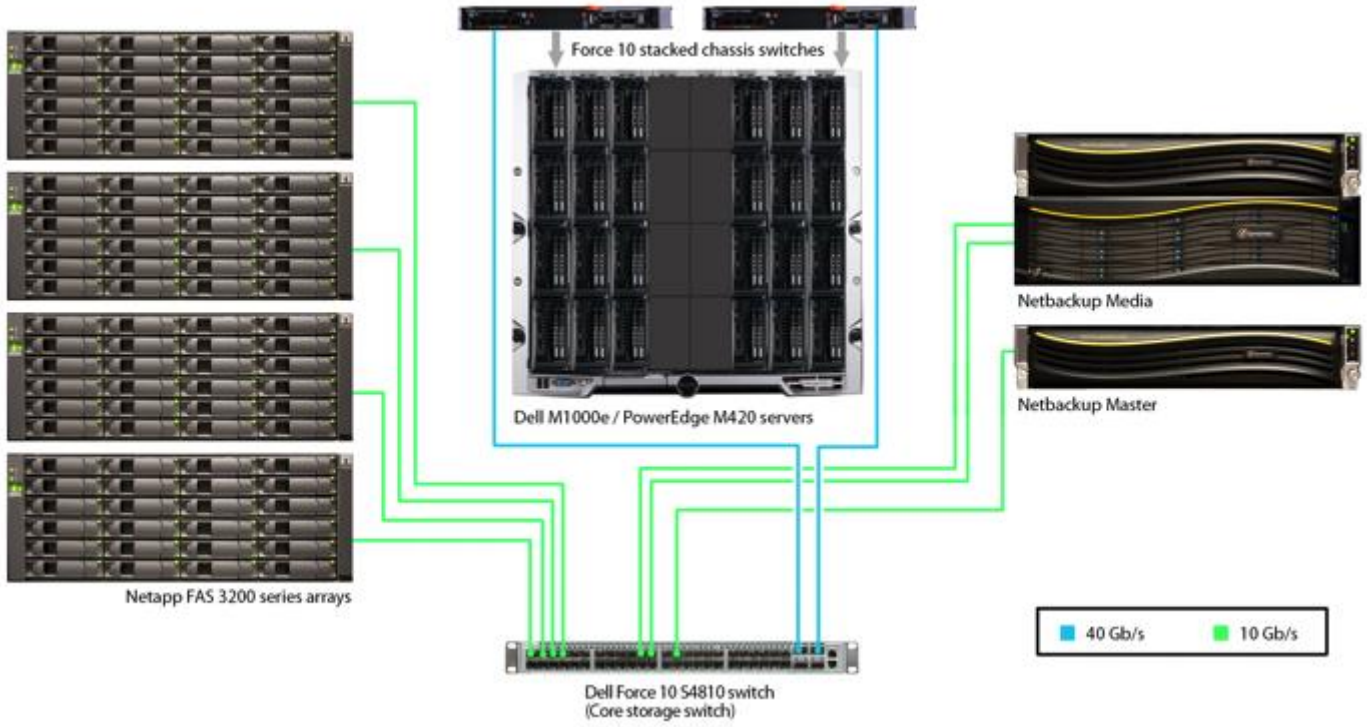


Figure 3: Detailed storage network: Storage-array snapshot-based backups.

We created a test environment of 1,000 Microsoft® Windows Server®-based VMs in several different configurations, depending on the test. We used Windows Server 2012 for application VMs, and Windows Server 2008 R2 Core installation for the standalone Web and idle file server VMs.

To balance the load across the ESXi hosts and storage, we created a matrix to ensure that equal load was distributed across all four NetApp filers (four volumes for the NAS testing, 40 LUNs/datastores for SAN testing) and the 20 ESXi hosts. This prevented overutilization of individual system components while others were idle, optimizing the performance of the multi-threaded backup procedures. For SAN testing, we used Symantec NetBackup's resources limits capability to eliminate the possibility of resource contention.

When we completed our NetBackup testing, we removed the NetBackup appliance, added Competitor "C" on similarly configured hardware, and retested. For Competitor "C," we performed iterative testing to determine the most effective number of streams to use in our environment, arriving at eight simultaneous streams. It is worth noting that the Competitor "C" management console advises against utilizing more than 10, due to the potential for performance issues.

For this first scenario, on SAN transport, we created 200 Windows Server 2012 application VMs running Microsoft SQL Server®, Microsoft Exchange, or Microsoft SharePoint® (10 tiles of 20 VMs each), and up to 800 idle Windows Server 2012 VMs. Figure 4 represents the grouping of VMs included in each backup job.

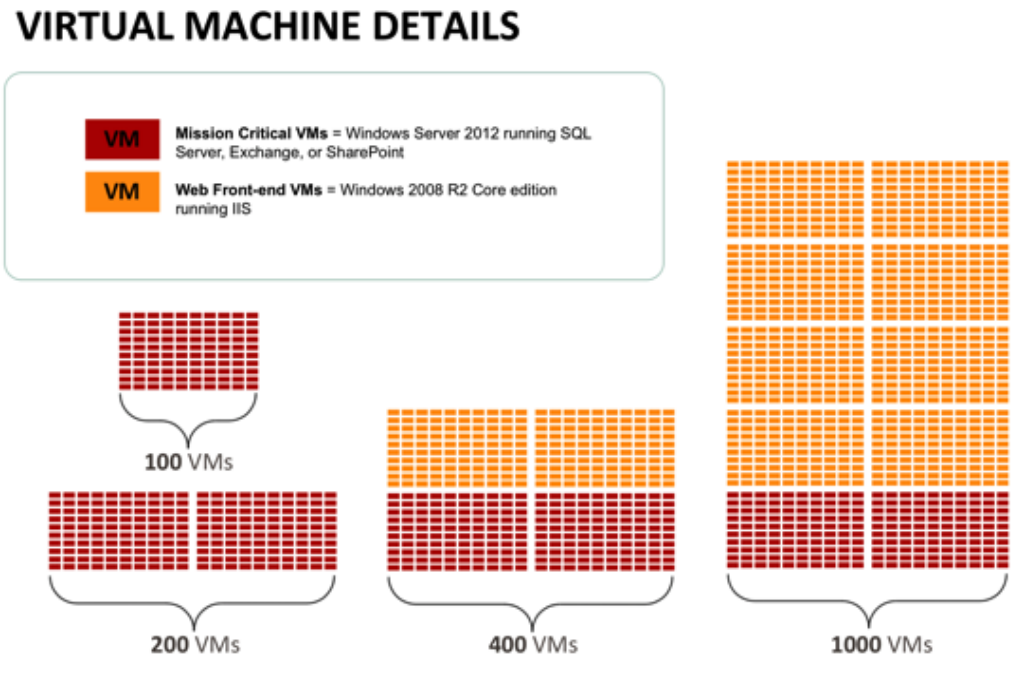


Figure 4: Backup via vStorage APIs based transport VM grouping.

Figure 5 provides the details for the sub-categories of VMs we used in this phase of testing.

Server VM type	Disk size (in GB)	VM count			
		100	200	400	1,000
Active Directory® server	55	5	10	10	10
Exchange Server	50	25	50	50	50
SharePoint Web server	55	15	30	30	30
SharePoint SQL server	160	5	10	10	10
Web application SQL server	50	50	100	100	100
Idle Web server	22			200	800

Figure 5: Production VMs on SAN storage. Color coding correponds with Figure 4.

For the NAS test phase, we created crash-consistent backups of NAS-based NFS storage at 100-, 200-, 500-, and 1,000-VM counts, as well as a 1,000-VM application-consistent backup. Figure 6 represents the groupings we used in each test category.

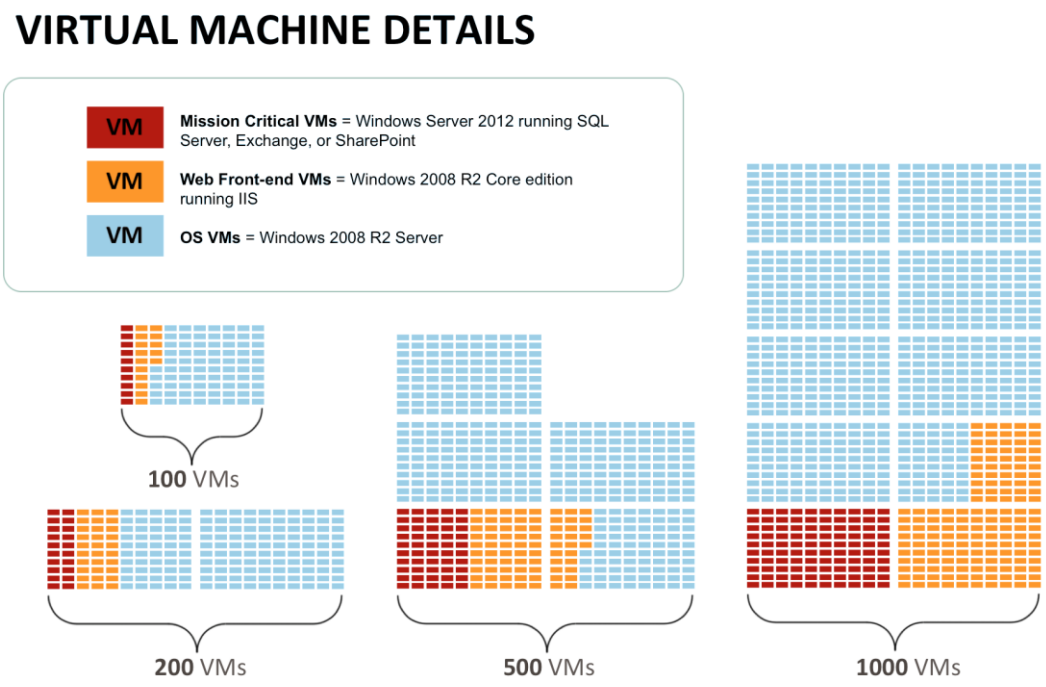


Figure 6: Backup via NAS transport VM grouping.

Figure 7 lists the details for the sub-categories of VMs we used in this phase of testing.

Server VM type	Disk size (in GB)	VM count			
		100	200	400	1,000
Active Directory server	55	1	1	3	5
Exchange Server	50	5	5	15	25
SharePoint Web server	55		3	6	15
SharePoint SQL server	160		1	2	5
Web application SQL server	50	4	10	24	50
Standalone Web server	22	15	30	75	150
OS	22	75	150	375	750

Figure 7: Production VMs on NAS Storage. Color coding correponds with Figure 6.

WHAT WE FOUND

Scenario 1 – SAN testing vs. Competitor "C"

Backup with virtual application protection via SAN transport

Using a comparable Intel® Xeon® processor-based server platform with identical memory and I/O configurations to the NetBackup Integrated Appliance as the backup target and using Competitor "C's" enterprise backup software and best practices,[1] we timed how long it took to complete an application-consistent backup of a group of VMs using SAN transport.

For this scenario, we created policies or groups containing the client VMs we wished to target, and from the GUI, instructed the orchestration server of each product to perform backups of the entire group. The NetBackup solution backed up 1,000 VMs in 80.3 percent less time than the Competitor "C" solution. In other words, the NetBackup solution completed the backup of 1,000 VMs five times faster than Competitor "C" did. Figure 8 shows the total time to complete the SAN transport backup for both solutions at every level of VM count we tested.

[1] This configuration fell within the recommendations of Competitor "C."

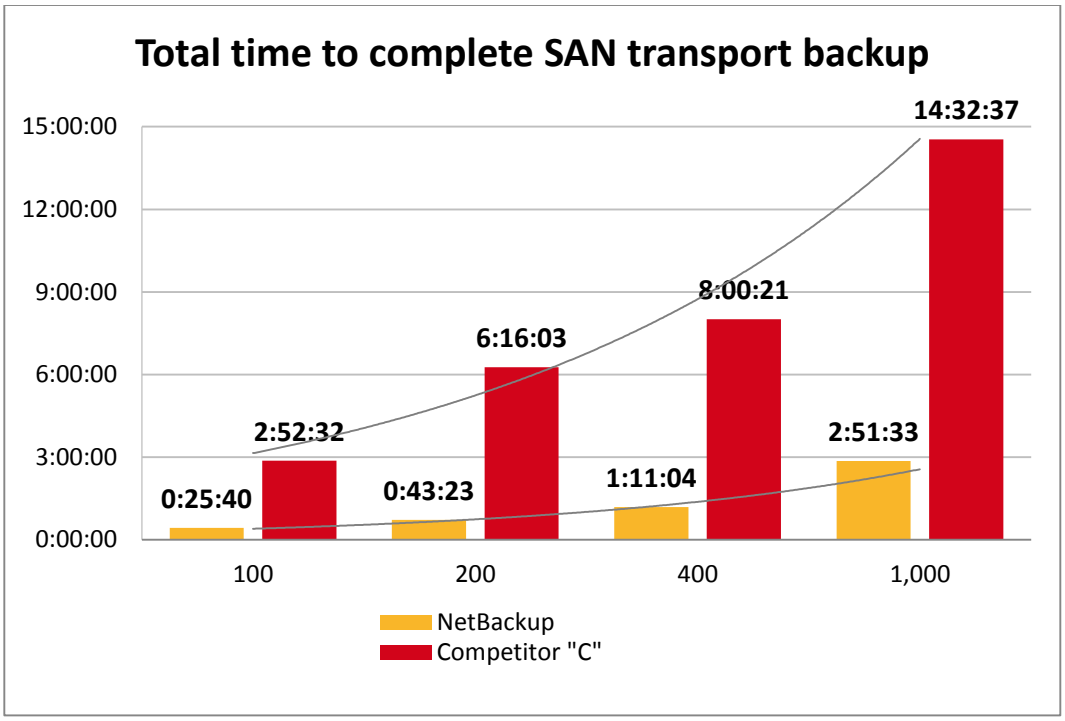


Figure 8: The total time each system took to complete vStorage APIs-based SAN transport backup in hours:minutes:seconds. Lower numbers are better.

We closely examined our infrastructure to ensure there were no bottlenecks affecting either solution's performance. After we found no evidence of bottlenecks in our test bed, we tested SAN performance by copying files from SAN volumes on our filers to local volumes on the target media servers, and again found no indications of performance issues. We re-ran our Competitor "C" test, and achieved results similar to our initial runs. Analysis of the data captured during backup runs suggested CPU saturation on the target media server, coupled with resource reservations for the backup streams contributed to the difference. When all eight streams were concurrently active, the target backup server for Competitor "C" showed CPU utilization fully saturated. Each stream utilized a finite amount of resources during the backup job. Media server CPU utilization dropped measurably when a stream was unused for backups, such as the pauses between the end of one VM backup and the beginning of the next one.

As a result, the CPU utilization on the Competitor "C" media server remained relatively high throughout the entire backup job—with spikes of 100 percent at times. The CPU utilization on the graph may not appear fully saturated due to sampling frequency (one sample every 30 seconds) and capturing "down time" between the end of one VM backup and the beginning of another. We saw this effect amplified when multiple streams were unused, as the resources remain bound to the idle streams and not shifted to active streams. See Appendix C for more details on media server CPU utilization.

Because Competitor "C" runs longer than a typical 6-to-8-hour backup window, production applications may not be able to operate at peak efficiency due to the impact of resource contention, as Figures 9 and 10 show.

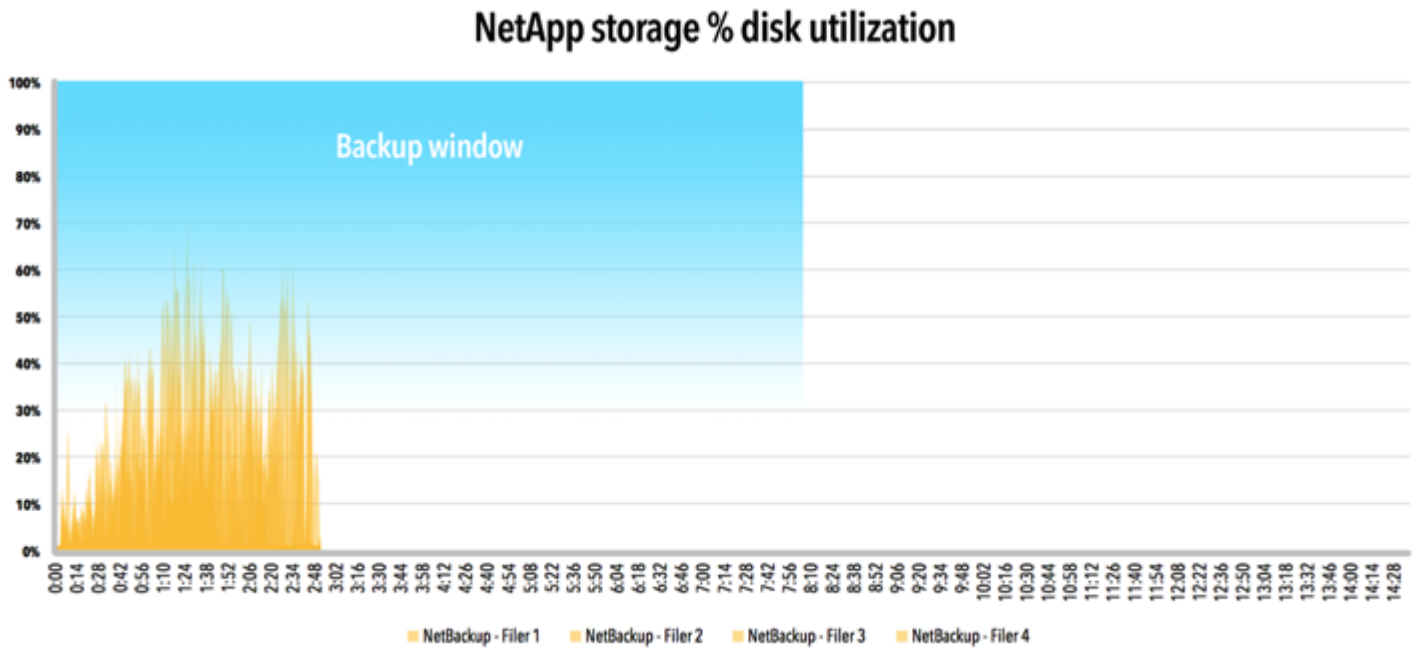


Figure 9: Average disk utilization across the four NetApp filers for Symantec NetBackup.

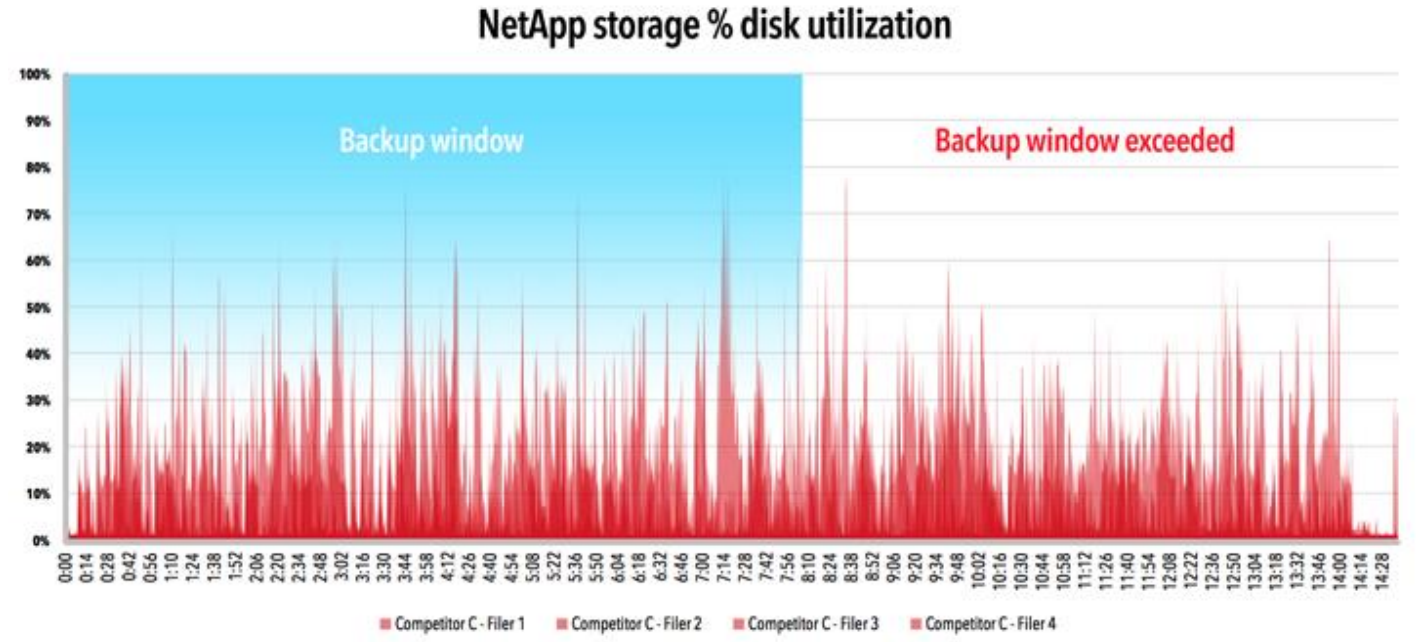


Figure 10: Average disk utilization across the four NetApp filers for Competitor "C."

Scenario 2 – Storage-array snapshot-based backup testing vs. Competitor "C"

Backup testing via NAS array-based snapshot

Our second scenario tested the ability to integrate with NetApp array-based snapshots to create recovery points in a high-VM-count environment. First, we ran Symantec NetBackup Replication Director and the comparable software from Competitor "C" on 100 application VMs. We found that at the 100-VM level, integration with crash-consistent recovery points with the NetBackup solution took 69.8 percent less time than the Competitor "C" solution. Next, we ran Replication Director and the comparable software from Competitor "C" on 200, 500, and then 1,000 VMs. At the 1,000-VM level, integration with application-consistent and crash-consistent recovery points with the NetBackup solution took up to 93.8 percent less time than the Competitor "C" solution.

As we increased our VM count from 100 to 1,000, the total integration times with NetBackup Replication Director increased slightly, from 5 minutes and 4 seconds with 100 VMs to 8 minutes and 29 seconds with 1,000 VMs. The total recovery-point integration times with comparable software from Competitor "C" increased at a much larger rate, from 16 minutes and 45 seconds with 100 VMs to 2 hours, 15 minutes, and 48 seconds with 1,000 VMs. Figure 11 shows the total time to complete array-based snapshots for both solutions at every level of VM count we tested.

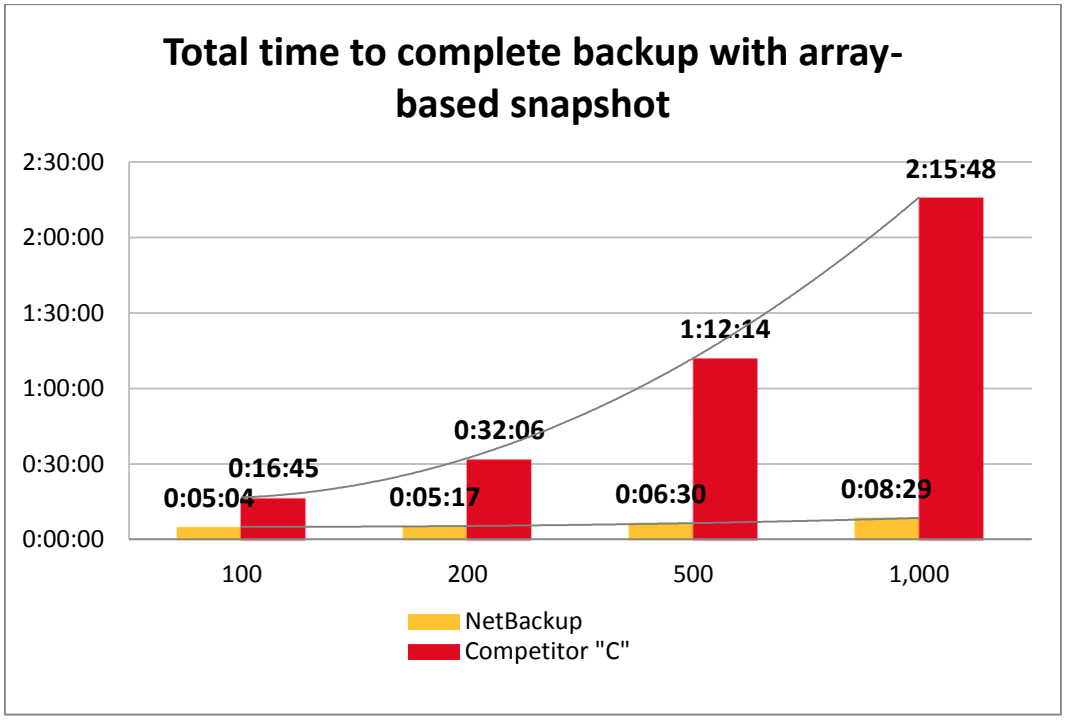


Figure 11: The total time each system took to complete a storage array-based snapshot backup in hours:minutes:seconds. Lower numbers are better. Note: For all testing, we did not enable snapshot indexing or make copies of the array-based snapshots.

We measured integration with application-consistent recovery points at 1,000 VMs and crash-consistent recovery points for both systems at four VM counts: 100, 200,

500, and 1,000. There was no noteworthy I/O activity on the storage or the backup targets to measure or report because our testing measured hardware-based snapshots without indexing. For application-consistent recovery points at the 1,000 VM level, the Symantec NetBackup solution took 77.5 percent less time than the Competitor "C" solution. Figure 12 shows the application-consistent and crash-consistent times for both solutions.

	100 VMs	200 VMs	500 VMs	1,000 VMs
Application-consistent recovery points				
Symantec NetBackup Integrated Appliance with NetBackup Replication Director				00:38:22
Competitor "C" with snapshot integration technology				02:50:21
Crash-consistent recovery points				
Symantec NetBackup Integrated Appliance with NetBackup Replication Director	0:05:04	0:05:17	0:06:30	00:08:29
Competitor "C" with snapshot integration technology	0:16:45	0:32:06	1:12:14	02:15:48

Figure 12: The times to complete application- and crash-consistent recovery points for both solutions in hours:minutes:seconds. Lower numbers are better.

The value of granular recovery and the required protection window to ensure it

In the case of file corruption or VM deletion, a system administrator can run a recovery job to recreate a VM from a previously captured backup image stored on the media server or media server equivalent. There are times, however, that recovering an entire VM is very inefficient—for example, when all that really needs recovery is an individual application file. In the case of a SQL database application, an administrator may only need to recover an individual database.

In addition to the backup job used to protect a virtual machine, Competitor "C" utilizes a SQL agent and requires an additional application specific job in order to allow granular recovery of the SQL application files. This backup job runs across the data network, rather than by SAN transport.

By contrast, the NetBackup solution offered a simplified and shortened protection window. During the virtual machine backup job, the NetBackup client installed on the application VM captures the application data in a manner that allows recovery of only application specific data as well as an entire VM, so no additional backup jobs are necessary. As Figure 13 shows, in our testing, the Symantec NetBackup solution needed just 4 minutes and 46 seconds to create a backup image that supports granular restore. Competitor "C" required 15 minutes and 24 seconds and required 14

additional steps to make the same image. Symantec NetBackup's strategy results in a 69.0 percent reduction in the time required for complete protection of a single application VM.

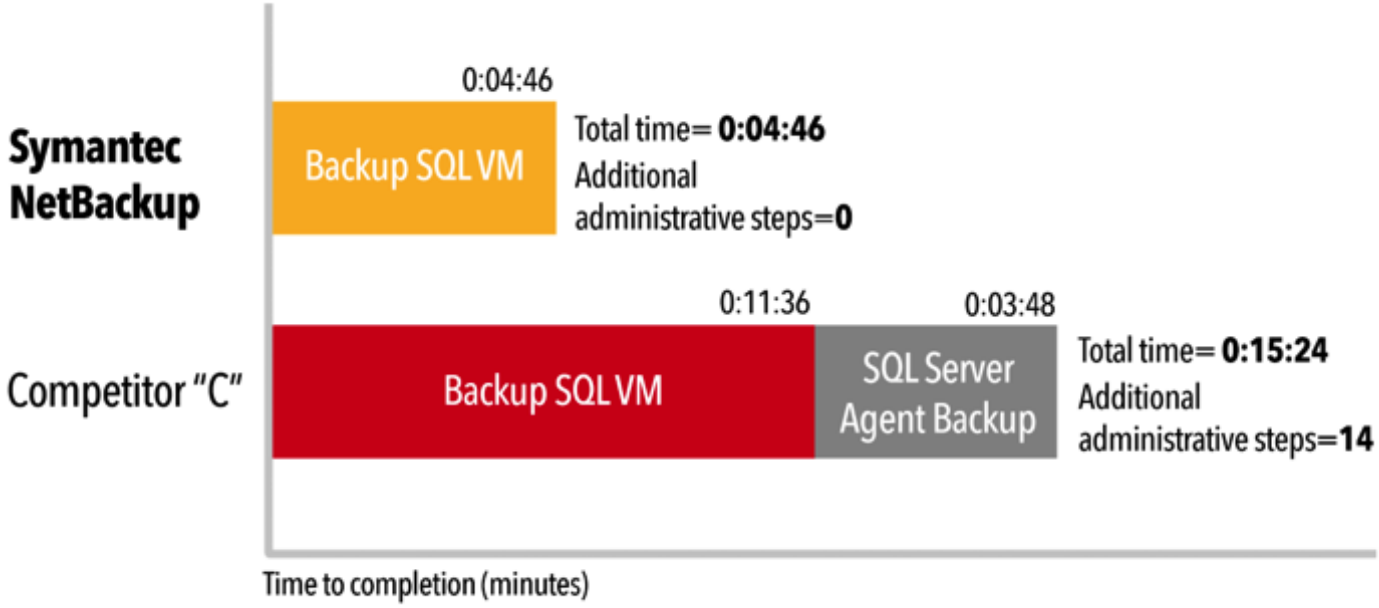


Figure 13: The additional time and steps needed to create the backup necessary to enable granular recovery.

CONCLUSION

In an enterprise environment, a data center VM footprint can grow quickly; large-scale deployments of thousands of virtual machines are becoming increasingly common. Risk of failure grows proportionally to the number of systems deployed and critical failures are unavoidable. Your ability to offer data protection from a backup solution is critical to business continuity. Elongated, inefficient protection windows can create resource contention with production environments, therefore, it is critical to execute system backup in a finite window of time.

The Symantec NetBackup Integrated Appliance running NetBackup 7.6 offered application protection to 1,000 VMs in 80.3 percent less time in SAN testing and used NetApp array-based snapshots to create recovery points in 93.8 percent less time than Competitor "C." In addition, the Symantec NetBackup Integrated Appliance with NetBackup 7.6 created backup images that offered granular recovery without additional steps and in a backup window 69.0 percent shorter than the backup window needed for Competitor "C." These time savings can scale as your VM footprint grows, allowing you to execute both system protection and user-friendly, simplified recovery.

APPENDIX A – SYSTEM CONFIGURATION INFORMATION

Figure 14 lists the information for the server from the NetBackup solution.

System	Dell PowerEdge M420 blade server (vSphere host)
Power supplies (in the Dell PowerEdge M1000e Blade Enclosure)	
Total number	6
Vendor and model number	Dell A236P-00
Wattage of each (W)	2,360
Cooling fans (in the Dell PowerEdge M1000e Blade Enclosure)	
Total number	9
Vendor and model number	Dell YK776 Rev. X50
Dimensions (h x w) of each	3.1” x 3.5”
Volts	12
Amps	7
General	
Number of processor packages	2
Number of cores per processor	8
Number of hardware threads per core	2
System power management policy	Performance
CPU	
Vendor	Intel
Name	Xeon
Model number	E5-2420
Stepping	2S
Socket type	FCLGA1356
Core frequency (GHz)	1.9
Bus frequency	7.2
L1 cache	32 KB + 32 KB (per core)
L2 cache	256 KB (per core)
L3 cache	15 MB
Platform	
Vendor and model number	Dell PowerEdge M420
Motherboard model number	0MN3VC
BIOS name and version	1.2.4
BIOS settings	Default, Performance profile
Memory module(s)	
Total RAM in system (GB)	96
Vendor and model number	Samsung® M393B2G70BH0-YH9
Type	PC3L-10600R
Speed (MHz)	1,333
Speed running in the system (MHz)	1,333
Timing/Latency (tCL-tRCD-tRP-tRASmin)	9-9-9-36
Size (GB)	16

System	Dell PowerEdge M420 blade server (vSphere host)
Number of RAM module(s)	6
Chip organization	Double-sided
Rank	Dual
Operating system	
Name	VMware vSphere 5.5.0
Build number	1209974
File system	VMFS
Kernel	VMkernel 5.5.0
Language	English
Graphics	
Vendor and model number	Matrox® G200eR
Graphics memory (MB)	16
RAID controller	
Vendor and model number	Dell PERC H310 Embedded
Firmware version	20.10.1-0084
Driver version	5.1.112.64 (6/12/2011)
Cache size (MB)	0 MB
Hard drive	
Vendor and model number	Dell SG9XCS1
Number of disks in system	2
Size (GB)	50
Buffer size (MB)	N/A
RPM	N/A
Type	SSD
Ethernet adapters	
Vendor and model number	2 x Broadcom® BCM57810 NetXtreme® II 10 GigE
Type	LOM
USB ports	
Number	2 External
Type	2.0

Figure 14: Detailed information for the server we tested from the NetBackup solution.

Figure 15 lists the information for the NetApp storage from the NetBackup solution.

System	NetApp FAS3240
Platform	
Vendor and model number	4 x NetApp FAS3240
OS name and version	NetApp Release 8.1.3 (7-Mode)
Hard drives	
Number of drives	24
Size (GB)	560
RPM	15K
Type	SAS

System	NetApp FAS3240
Network adapters	
Vendor and model number	2 x 10Gbps
Type	Integrated
Fiber adapters	
Vendor and model number	2 x 8Gbps
Type	PCI-E

Figure 15: System configuration information for the NetApp storage array.

Figure 16 details the configuration of the NetBackup integrated appliance and the Competitor "C" media server.

System	NetBackup 5230 integrated appliance	Competitor "C" media server
General		
Number of processor packages	2	2
Number of cores per processor	6	6
Number of hardware threads per core	2	2
System power management policy	Default	Default
CPU		
Vendor	Intel	Intel
Name	Xeon E5-2620	Xeon E5-2620
Model number	E5-2620	E5-2620
Socket type	FCLGA2011	FCLGA2011
Core frequency (GHz)	2 GHz	2 GHz
Bus frequency	7.2 GT/s	7.2 GT/s
L1 cache	32 KB + 32 KB per core	32 KB + 32 KB per core
L2 cache	1.5 MB (256 KB per core)	1.5 MB (256 KB per core)
L3 cache	15 MB	15 MB
Platform		
Vendor and model number	Symantec NetBackup 52 30 Integrated Appliance	N/A
Memory module(s)		
Total RAM in system (GB)	64	64
Vendor and model number	Ventura Tech® D3-60MM104SV-999	Ventura Tech D3-60MM104SV-999
Type	PC3-10600	PC3-10600
Speed (MHz)	1,333	1,333
Speed running in the system (MHz)	1,333	1,333
Timing/Latency (tCL-tRCD-tRP-tRASmin)	9-9-9-27	9-9-9-27
Size (GB)	8	8
Number of RAM module(s)	8	8
Chip organization	Double-sided	Double-sided
Rank	Dual rank	Dual rank

System	NetBackup 5230 integrated appliance	Competitor "C" media server
Operating system		
Name	NetBackup Appliance 2.6.0.2	Windows Server 2012
Build number	2.6.32.59-0.7-default-fsl	N/A
RAID controller		
Vendor and model number	Intel RMS25CB080	Intel RMS25CB080
Firmware version	23.9.0-0025	23.9.0-0025
Cache size (MB)	1024	1024
Hard drives		
Vendor and model number	Seagate Constellation ES ST1000NM0001	Seagate Constellation ES ST1000NM0001
Number of drives	10	10
Size (GB)	1,000	1,000
RPM	7.2K	7.2K
Type	SAS	SAS
Storage shelf		
Vendor and model number	HGST HUS723030ALS640	HGST HUS723030ALS640
Number of drives	16	16
Size (GB)	3,000	3,000
RPM	7.2K	7.2K
Type	SAS	SAS
Ethernet adapters		
Vendor and model number	Intel X520 10Gbps dual-port Ethernet adapter	Intel X520 10Gbps dual-port Ethernet adapter
Type	PCI-E	PCI-E

Figure 16: Detailed information on the media server from each solution.

APPENDIX B – HOW WE TESTED

We set up hardware and software for Competitor "C" according to administrative best practices.

Creating a storage lifecycle policy with NetBackup 7.6

1. Open a connection to the NetBackup machine.
2. If the Symantec NetBackup Activity Monitor is not open, open it.
3. Log into nbu-master-a with administration credentials.
4. Go to Storage→Storage Lifecycle Policies.
5. Right-click in the right pane, and select New Storage Lifecycle Policy.
6. Enter a name for your SLP.
7. Click Add.
8. In the New Operation window, change the operation to Snapshot, and select primary-snap as your destination storage.
9. Click OK.

Creating a policy with NetBackup 7.6

1. Open a connection to the NetBackup machine.
2. If the Symantec NetBackup Activity Monitor is not open, open it.
3. Log into nbu-master-a with administration credentials.
4. Go to Policies.
5. Right-click the All Policies area, and select New Policy.
6. Under Add a New Policy, enter your policy name, and click OK.
7. Change Policy type to VMware.
8. Click the Policy storage drop-down menu, and select the policy you created earlier.
9. Check Use Replication Director, and click Options.
10. In the Replication Director options, change Maximum Snapshots to 1,000, and make sure that Application Consistent Snapshot is Enabled.
11. Click the Schedules tab.
12. In the Schedules tab, select New.
13. In the Attributes window, enter a name for your scheduled backup, click Calendar, and click the Calendar Schedule tab.
14. In the Calendar Schedule tab, select a date as far away as you deem reasonable, and click OK.
15. Click the Clients tab.
16. Click Select automatically through query. If a warning window appears, click Yes.
17. Choose the VMs you wish to backup through queries (for example, if you want to back up all VMs on a drive, choose Datastore in the Field category, and enter the drive you want to pull all VMs from in quotes in the Values field.

Running a test with NetBackup 7.6

1. Open a connection to the NetBackup machine.
2. If the Symantec NetBackup Activity Monitor is not open, open it.
3. Log into nbu-master-a with administration credentials.
4. Go to Policies.
5. Right-click the policy you wish to run, and select Manual Backup.
6. Click OK.

Note: In the case of the NAS backups, we had two separate policies as each one targets the opposite VMs. Make sure to run the even and odd backup.

Backing up VM hosts in NetBackup 7.6

1. Select Policies.
2. Under All Policies, right-click and select New Policy.
3. Provide a policy name and click OK.
4. On the Attributes tab, use the pull-down menu for Policy type and select VMware.
5. For Destination, use the pull-down menu and select your target storage. We selected media-msdp.
6. Check the box for Disable client-side deduplication.
7. Check the box for Use Accelerator.
8. On the Schedules tab, create a backup schedule based on the desired parameters.
9. On the Clients tab, choose Select automatically through query.
10. Select the master server as the NetBackup host to perform automatic virtual machine selection.
11. Build a query to select the correct VMs required for the backup job.
12. Click Test Query to ensure the correct VMs are properly selected.
13. Start the backup.

NetBackup 7.6 Exchange Instant Recovery

1. Start LoadGen test load.
2. Force-power-down all VMs once 50 LoadGen operations complete.
3. Initiate the Exchange infrastructure restore job/start timer.
    a. Establish a connection to the master server via SSH.
    b. Log in with administrator credentials.
    c. Type `support` and press Enter.
    d. Type `maintenance` and press Enter.
    e. Enter the administrator credentials.
    f. Type `elevate` and press Enter.
    g. Type the following:

    ```
    nbrestorevm -vmw -ir_activate -C client_DNS_name -temp_location
    temporary_restore_LUN -vmproxy restore_host_FQDN -vmpo
    ```

    This will restore, activate, and power-on the VM.
    h. Repeat Step g for each of the four VMs to restore.
    i. Stop the LoadGen test run.
4. When restores complete, restart the LoadGen test.
5. Once 100 LoadGen operations complete successfully, stop the timer.

NetBackup 7.6 Exchange restore via command line

Initiate Exchange infrastructure restore job

1. Establish a connection to the master server via SSH.
2. Log in with administrator credentials.
3. Type `support` and press Enter
4. Type `maintenance` and press Enter.
5. Enter the administrator credentials
6. Type `elevate` and press Enter.
7. Type the following:

```
nbrestorevm -vmw -ir_activate -C client_DNS_name -temp_location
temporary_restore_LUN -vmproxy restore_host_FQDN -vmpo
```

This will restore, activate, and power-on the VM.

8. Repeat step 7 for each of the four VMs to restore.

NetBackup 7.6 Exchange Instant Recovery

1. Start the LoadGen test load.
2. Force-power-down all VMs once 50 LoadGen operations complete.
3. Initiate the Exchange infrastructure restore job/start timer.
    a. Establish a connection to the master server via SSH.
    b. Log in with administrator credentials.
    c. Type `support` and press Enter.
    d. Type `maintenance` and press Enter.
    e. Enter the administrator credentials.
    f. Type `elevate` and press Enter.
    g. Type the following:

    ```
    nbrestorevm -vmw -ir_activate -C client_DNS_name -temp_location
    temporary_restore_LUN -vmproxy restore_host_FQDN -vmpo
    ```

    This will restore, activate, and power-on the VM.
    h. Repeat step g for each of the four VMs to restore.
    i. Stop the LoadGen test run.
4. When restores complete, restart the LoadGen test.
5. Once 100 LoadGen operations complete successfully, stop the timer.

Launching collectors and compiling data for NetBackup 7.6

The following two tasks (Launch the collectors & Compile the data) should be executed from the domain\administrator login on INFRA-SQL.

Launching the collectors

Note: If this is a first run collection, skip to step 2.

1. Double-click the collector job (located in C:\Scripts) associated with the number of VMs you want to collect.
2. In the PuTTY session launched for the media server collection, enter the following sequence:

    ```
    Support
    Maintenance
    (P@ssw0rd)
    iostat -d 30
    ```
3. RDP into the Backup-Test server.
4. On the NetBackup Console, expand nbu-master-a→NetBackup Management→Policies.
1. Right click the Policy you want to start, and select Manual Backup.
5. To start the job, click OK.
6. Open the Activity Monitor on the NetBackup Administration Console.
7. The Backup job will execute and spawn four different kinds of jobs for each target VM:
    a. Application State Check
    b. VM Snapshot
    c. Backup
    d. Image Cleanup

Compile the data

In the following steps, ### represents the number of VMs you're testing, and # represents the test number.

1. At job completion, double-click the StopCollection.bat file (located in C:\Scripts).

2. Capture screenshots of the Main Backup Job (both Tabs) and sub jobs for a SQL server, an Exchange Server, and a SharePoint server.
    a. Save each screenshot in:
    E:\Symantec Test Results\01 Backup Test\### VM Results Repository\Test #\
    b. If this is a first run, return to step 1 above.
3. On the menu at the top of the NetBackup Console, select File→Export.
4. Select All Rows, and export to *<Test#.xls>.* Click Save.
5. Manually select all the rows in the activity monitor and delete them.
6. Open WinSCP.
7. Select My Workspace on the left panel and click Login. This will open a connection and automatically log into each of the ESX servers undergoing data collection.
    a. In the left panel, browse for the correct job folder:
    \### VM Results Repository\Test #\esxtop\
    b. In the right panel, select the esxout file (which may be of considerable size) and drag it into the esxtop directory.
    c. Once the file transfer is complete, delete the esxtop from the server (right panel).
    d. Repeat steps a-c for each of the esx servers.
8. Close WinSCP.
9. On the INFRA-SQL server, open E:\Putty Output.
10. In a separate window, open:
    E:\Symantec Test Results\01 Backup Test\### VM Results Repository\Test #\sysstats.
11. Move all the files from E:\Putty Output to the Test folder you selected in the previous step.
12. Close all Explorer windows.
13. Return to step 1 above.

General concurrent restore procedure

1. Delete restore target VM(s) from disk in vCenter.
2. Launch the data collector script.
3. Execute a restore job using one of the following methods:
    a. For NetBackup:
        i. Open a PuTTY session to the NBU master server (172.16.100.100).
            1. Log in as `admin/P@ssw0rd`
            2. Type `support` and press Enter.
            3. Type `maintenance` and press Enter.
            4. Enter the maintenance password `P@ssw0rd`
            5. Type `elevate` and press Enter.
        ii. Copy the commands to be executed from a text file and paste them into the command line interface on the NetBackup master server.
4. Determine the time by determining the difference between the time the first job begins and the end-time of the last job to complete.
5. Export the NBU job log to disk and copy it to the results folder.
6. Stop the collection script.
7. Transfer the relevant data collector output into the test folder.

APPENDIX C – CPU UTILIZATION

Figure 17 shows the CPU utilization for the NetBackup solution.

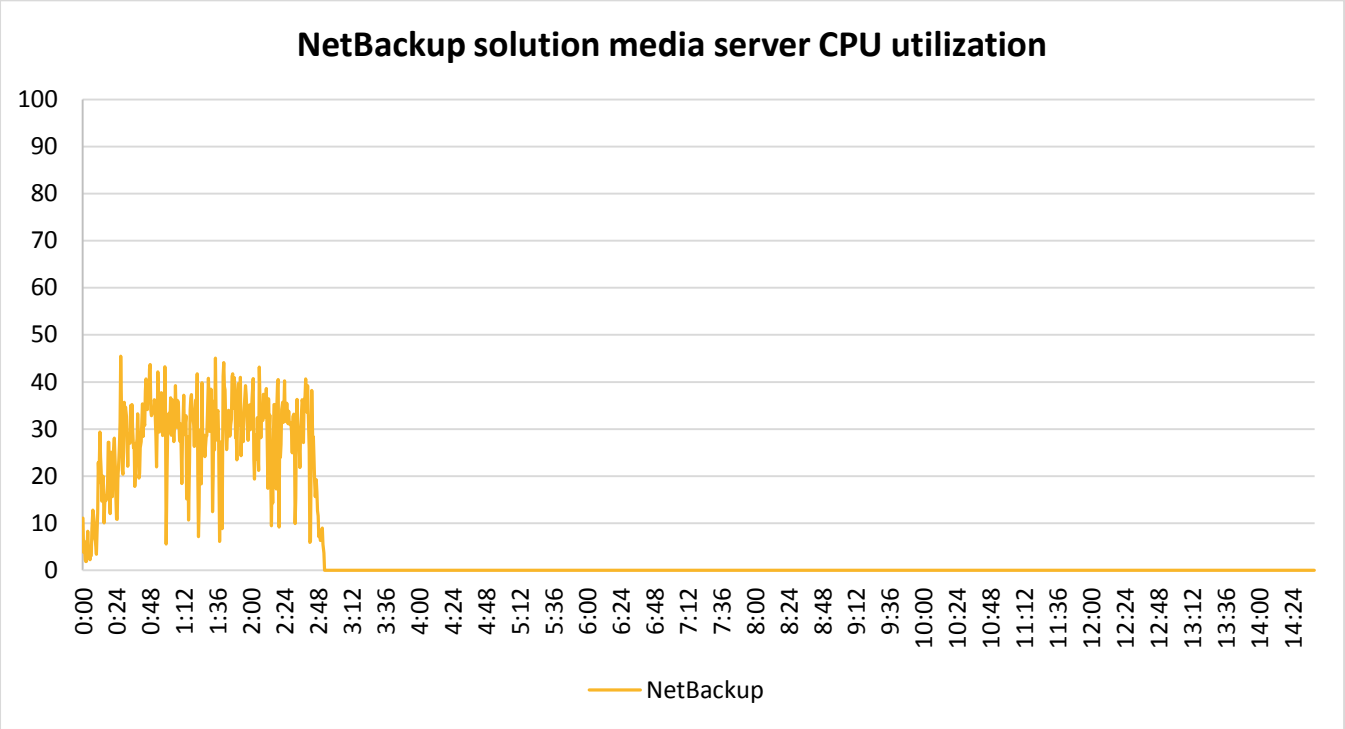


Figure 17: CPU utilization for the NetBackup solution using the NetApp media server.

Figure 18 shows the CPU utilization for the Competitor "C" solution.

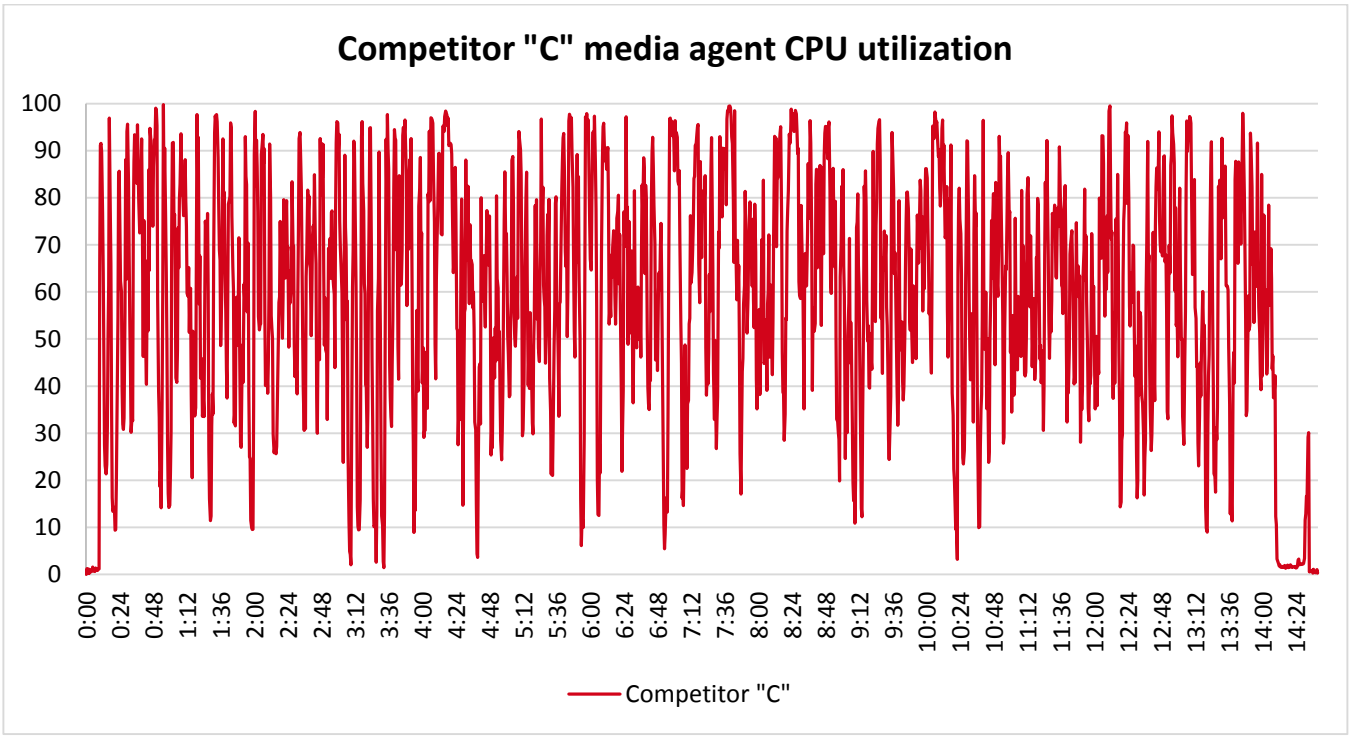


Figure 18: CPU utilization for the Competitor "C" solution using the media agent.

ABOUT PRINCIPLED TECHNOLOGIES

Principled Technologies, Inc.
1007 Slater Road, Suite 300
Durham, NC, 27703
www.principledtechnologies.com

We provide industry-leading technology assessment and fact-based marketing services. We bring to every assignment extensive experience with and expertise in all aspects of technology testing and analysis, from researching new technologies, to developing new methodologies, to testing with existing and new tools.

When the assessment is complete, we know how to present the results to a broad range of target audiences. We provide our clients with the materials they need, from market-focused data to use in their own collateral to custom sales aids, such as test reports, performance assessments, and white papers. Every document reflects the results of our trusted independent analysis.

We provide customized services that focus on our clients' individual requirements. Whether the technology involves hardware, software, Web sites, or services, we offer the experience, expertise, and tools to help our clients assess how it will fare against its competition, its performance, its market readiness, and its quality and reliability.

Our founders, Mark L. Van Name and Bill Catchings, have worked together in technology assessment for over 20 years. As journalists, they published over a thousand articles on a wide array of technology subjects. They created and led the Ziff-Davis Benchmark Operation, which developed such industry-standard benchmarks as Ziff Davis Media's Winstone and WebBench. They founded and led eTesting Labs, and after the acquisition of that company by Lionbridge Technologies were the head and CTO of VeriTest.