Protecting Exchange Server 2007 with NetApp SnapManager for Exchange

Brad Garvey, Network Appliance, Inc.

NetApp®

Microsoft®
GOLD CERTIFIED
Partner

Table of Contents

1.0 Introduction

Microsoft Exchange Server has become a vital source of communication as well as repository for business critical data.

Because of the increasing importance of Microsoft Exchange Server, data protection, disaster recovery, and high availability play a critical role in Exchange Server deployments. As the importance of Exchange Server within the organization increases, companies expect quick recovery times with little or no data loss. With Exchange databases growing rapidly in size every day, it is increasingly difficult to complete time-consuming backup operations in a reasonable amount of time. When an outage occurs, it can take days to restore service from slower media such as tape, even assuming that all of the backup tapes are available and error free.

Network Appliance offers a comprehensive suite of data management solutions that enable organizations to keep pace with the increasing data availability demands of an ever-expanding Exchange Server environment, as well as scale to accommodate future needs while reducing cost and complexity.

1.1 Purpose and Scope

Since there are many different solutions that leverage Microsoft Volume Shadow Copy Services (VSS) for Exchange Server, it is important not only to understand the implementation but also to test performance, capacity and recovery implications of your solution to ensure that it meets your corporate messaging needs and meets SLA requirements.

The purpose of this paper to is to test performance implications of NetApp SnapManager for Exchange in an Exchange Server 2007 environment.

1.2 Intended Audience

The audience of this paper should be familiar with the following products.
- Exchange Server backup and recovery solutions
- NetApp storage solutions
- Microsoft Volume Shadow Copy Services (VSS) technology

2.0 Snapshot Overview

Exchange Server 2007 supports Microsoft VSS, which supports shadow copies that can be executed via a software or hardware provider. Generally, it takes much less time to restore a backup that was taken using a hardware-based snapshot. Therefore, depending on the hardware and software that was used in the solution, restoring Exchange data from these types of backups may make it easier to meet the requirements of aservice level agreement (SLA) that relate to the time required to restore Exchange databases. Because larger databases can be restored more quickly, hardware-based snapshot restores can help support larger database sizes and still meet SLAs for restoring Exchange data.

VSS in Microsoft Windows Server 2003 provides an infrastructure that enables third-party storage management programs, and hardware providers to create and manage shadow copies of Microsoft Exchange Server utilizing the VSS API.

The Volume Shadow Copy service coordinates communication between *Requestors* (backup applications), *Writers* (applications in Windows services like Exchange Server 2007), and *Providers* (system, software or hardware components that create the shadow copies, such as NetApp storage systems). To use the Volume Shadow Copy service feature to backup Exchange Server 2007, the backup program must include an Exchange Server 2007-aware Volume Shadow Copy service requestor. Because the backup program that is bundled with Windows Server has no such requestor, organizations must use third-party backup applications.

2.1 Components of a VSS Snapshot

VSS ensures the consistency and integrity of a Snapshot by orchestrating Freeze/Thaw, flushing outstanding I/O to disk, and ensuring that all related LUNS are brought together into a single, consistent Snapshot.

There are four key components present in the snapshot process.

1. **Volume Shadow Copy Service:** Volume Shadow Copy Service (VSS) is the Windows Server 2003 service that coordinates among other VSS components to provide snapshot-based backups and restores.

2. **VSS Requestor:** The VSS requestor is a backup application, such as NetApp SnapManager for Exchange. It initiates, or 'requests' VSS backup and restore operations. The requestor also specifies snapshot attributes for the backups it initiates.

3. **VSS Writer:** The VSS writer owns and manages the data to be captured in the snapshot. In this case, the VSS writer is Exchange Server 2007.

4. **VSS Provider:** The VSS provider integrates storage array-specific snapshot and cloning functionality into the VSS framework. A provider can be either a hardware or a software provider. In this case, the NetApp hardware provider is installed as part of the SnapDrive software installation.

When the Exchange server receives a backup request, the Exchange writer prepares Exchange databases for backup. The writer does this by suspending all disk write I/O to the databases for up to 20 seconds. This is referred to as "freezing the databases". The provider must be able to complete the shadow copy within this window or the backup will be aborted. After the backup is completed, the writer *thaws* the databases and resumes regular I/O operations. For more information about requestors, writers, and providers, see Basic VSS Concepts. For additional information on VSS implementation in Exchange Server, see http://www.microsoft.com/technet/prodtechnol/exchange/2003/vssbp.mspx

Each VSS-compliant backup must contain the following components.
1. Exchange databases and transaction logs must be backed up through the Exchange VSS writer.
2. The backup application must validate the integrity of the the backup set.
3. Restores must be done through the Exchange VSS writer.

2.2 VSS Backup Methods

Below is an overview of VSS Backup Methods

- Clone Shadow Copies
- Snapshot Shadow Copies
- Considerations for using VSS backups

Clone Shadow Copies
A "clone shadow copy" is a full copy of the volumes in a shadow copy set. A clone is a completely independent copy of the original data set.

Unlike clone copy, a Shadow Copy is not an independent copy of the original data. A *shadow copy set* is a group of volume shadow copies that are synchronized at the same point in time.

Snapshot Shadow Copies
Generically, snapshots are created by defining a marker at a point in time and making sure that the data can be rolled back to that point in time. Multiple snapshots can be kept, and snapshots typically require much less additional disk space than clones.

Snapshots can be created in several different ways. The most common method is called *copy-on-write*. The copy-on-write method defines a snapshot at a point in time, and then monitors the original dataset for changes. If a change is made to a block, the original contents of the block are copied to a separate location before the block is updated. Over time, the size of a snapshot can continue to grow, especially when a snapshot is made of a quickly-changing dataset.

Benefits of Snapshot Backups
- VSS snapshots provide the ability to backup large amounts of data in a backup window
- Faster restore times

Considerations for Using Copy-on-write Snapshot Backups
- During the Snapshot process, performance degradation can occur.
- As additional snapshots are taken and kept available, performance degradation can occur.
- Deleting snapshot copies can negatively impact performance.

2.3 NetApp Snapshot technology

NetApp Snapshots are unique in that they have all the benefits of snapshot technology without additional performance overhead.

NetApp Snapshot technology is a feature of the WAFL® (Write Anywhere File Layout) storage virtualization technology that is a part of Data ONTAP®.   A NetApp Snapshot is a frozen, read-only view of a WAFL volume that provides easy access to old versions of files, directory hierarchies, and/or LUNs.

NetApp Snapshot technology is very efficient as it only stores block-level changes between each incremental snapshot. There can be up to 255 snapshots per file system with little to no impact on performance.

How NetApp Snapshots differ from other snapshot solutions
Most snapshot shadow copy implementations use a method called "copy-out snapshots". The principle behind copy-out snapshots is to preserve snapshot data by relocating it from an active file system or LUN to a "special" pre-allocated copy-out area. After a snapshot is taken, when a data block in the active file system or LUN is about to be overwritten by new data, the following steps are taken:

1. The original data (that is about to be overwritten) is read from the underlying disks.
2. The original data is written to the copy-out area in order to preserve it.
3. The new data is written over the original data on the disks.

This process <u>triples</u> the I/O burden when data is being copied out (each new write operation becomes a read operation and two write operations) and typically results in a performance penalty of as much as 30-50%.

NetApp SnapManager for Exchange utilizes NetApp Snapshot technology as a basis for snapshots. NetApp Snapshots differ from other vendors' snapshot technology as it is not a copy-on-first-write implementation. This allows NetApp Snapshots to store up to 255 snapshots per volume witout incurring additional performance overhead.

When a Snapshot is created on a NetApp storage system it does not copy changed blocks. It instead identifies all blocks as belonging to both the active file system and the snapshot. As data changes, data is written to new disk blocks. This creates two copies of the changed data: the newly written copy in the active file system and the old data in the Snapshot copy.

This enables the NetApp storage system to create near-instantaneous snapshot copies without incurring additional performance overhead.

2.4 SnapManager For Exchange

Network Appliance™ SnapManager for Microsoft Exchange 4.0 software is available for Microsoft Exchange Server 2003 and 2007. SnapManager 4.0 for Exchange (SME) has achieved a "Certified for Windows" logo

for Windows® Server 2003 Standard and Enterprise editions. SME is also a "Microsoft SimpleSAN" designated and a Windows Server 2003 certified backup and recovery solution for Exchange Server. SME istightly integrated with Microsoft Exchange, which allows for consistent online backups of Exchange environments while leveraging NetApp Snapshot™ copy technology. SnapManager 4.0 for Exchange supports Microsoft Volume Shadow Copy Services (VSS), Virtual Disk Services (VDS), and other Microsoft storage technologies. (For details on VSS, see Microsoft KB article 822896.) SME is a VSS (Snapshot copy) requestor, which means that it uses the Microsoft-supported VSS subsystem to initiate backups. SME provides a complementary feature set for the new Microsoft Exchange 2007 data replication features. SME works with Local Continuous Replication (LCR) and Cluster Continuous Replication (CCR) replica databases and provides a rich feature set to leverage these new technologies.

Benefits at a glance:
- Quickly backup and restore entire Exchange Storage Groups using NetApp Snapshot technology.
- Exchange data stored in snapshots can be mirrored to one or more locations for archival or disaster recovery purposes.

3.0 Test Overview

To validate the use of NetApp Snapshots in an Exchange Server 2007 environment, a test scenario was built using Microsoft Exchange Load Generator (LoadGen) to simulate a 3,000-user environment. LoadGen is a simulation tool that tests Exchange servers to see how they respond to email loads.

Multiple runs of LoadGen testing were completed during the testing periods. The first day was run without any scheduled snapshots for baseline performance. Over subseqent days, SME Snapshots were scheduled every two hours with 24 Snapshots retained. Snaphots were verified nightly using a separate verification server.

During the simulation, data was collected using Windows Performance Monitor (perfmon).   Upon completion of the test, the data was analyzed to determine affects of Snapshots on server performance and to ensure that server response times remained within acceptable limits.

The following sections detail server and storage configurations used in the test environment.

Storage:
- (1) NetApp FAS3050C storage system
  - Composed of 2 FAS3050 storage controllers configured as an Active/Active cluster
- Data ONTAP 7.1
- A total of 12 Disk Shelves (DS14 MK2) were used (6 per storage controller)
- 15K 144GB Drives (See Table 1 for total number of disks used in each configuration)

Servers:
- 1 Hewlett Packard Proliant DL 385 with (2) dual-core AMD Opteron processors and 8GB RAM
- Windows Server 2003 Enterprise Edition (64-bit) Service Pack 1
- (2)1 GbE iSCSI connections per server
- Intel Pro/1000 MT driver version 8.1.8.0

Software:
- Microsoft iSCSI Software Initiator v2.02
- Microsoft Exchange Server 2007
- NetApp SnapDrive for Windows 4.1 with MPIO (NetApp multipathing I/O solution)
- NetApp SnapManager for Exchange version 4.0

Network:
- (1) NetGear GSM7224 GbE Ethernet switches (Jumbo Frames enabled)

3.1 Exchange Storage Layout

Storage layout was sized according to NetApp best practices. The FAS3050 storage controller was configured with separate aggregates for database and transaction log volumes. Each database aggregate on the storage controller contained two NetApp FlexVol volumes (one volume for each storage group.) Both volumes were configured as RAID DP volumes. Each volume contained one LUN on which mailbox databases were located. The transaction log aggregate on each storage controller contained one FlexVol volume with three LUNs (one LUN per storage group).

The following table shows the storage configuration used in each test:

Aggregate	# of Drives in Aggr.	Volume	Total Space Available	Used Space
DBAGGR	39	DB	3600GB	2880GB
LOGAGGR	9	LOGVOL	340GB	272GB

Table 1) Storage Layout

3.2 SnapManager for Exchange Configuration

SME backups were scheduled every two hours during the test, providing a recovery point of two hours. The backup job was configured to complete a full backup of all storage groups and mailbox databases. A retention period of seven days was maintained. A separate verification server was set up in order to isolate database checksum I/O from the active server.

Each SME backup was configured to do a full backup of all three storage groups, with up to the minute recovey capability. When up to the minute recovery is used, trasaction logs corresponding to the current backup set are moved to the SnapInfo location. In addition to corresponding transaction log files the SnapInfor directory contains information regarding each backup taken. The SnapInfo directory in contained on the same volume as the transaction logs.

When the transaction log directory resides on the same NTFS volume as the SnapInfo directory, SME will utilize NTFS hard links to avoid the file copy operation and maximize storage utilization. During the backup process, SME will edit the file pointers for a given transaction log. SME inserts a pointer to the SnapInfo directory and removes the pointer to the Exchange transaction log directory. As a result, it will appear as if a transaction log was moved from one directory to the other. However, a physical move operation was not performed, and no I/O overhead was incurred on the Exchange server. Only the pointers for a transaction log file were updated, thus saving the additional space required to copy the transaction log files into the SnapInfo directory.

3.3 LoadGen Configuration

The following configuration was used during LoadGen testing:

Exchange Server 2007
- 3,000 mailboxes
- 3 Storage Groups
- 1 Mailbox database per storage group

Mailbox Characteristics
- 1,000 Users/Mailbox database
- Average mailbox size of 225MB

- Heavy mailbox usage profile

For detailed information mailbox profiles please refer to
http://www.microsoft.com/technet/prodtechnol/exchange/2007/plan/hardware.mspx

4.0 Results

Analysis of the data collected shows the following performance characteristics.

4.1 Baseline performance Characteristics

In order to establish baseline performance characterestics, Exchange server performance while under LoadGen testing was observed without performing any snapshot backups. LoadGen tests were run for 10 hours. In order to gather consistant data points, the following charts display the last four hours of the test period.

RPC-Averaged Latency
Average RPC latency is a measure of the average amount of time it takes for a server to respond to a client request. Under normal circumstances, this number should be below 50ms. RPC latencies above 50 milliseconds can cause Outlook clients to temporarily lose connectivity to the Exchange Server.

The RPC-averaged latency during the baseline testing period was nine milliseconds.
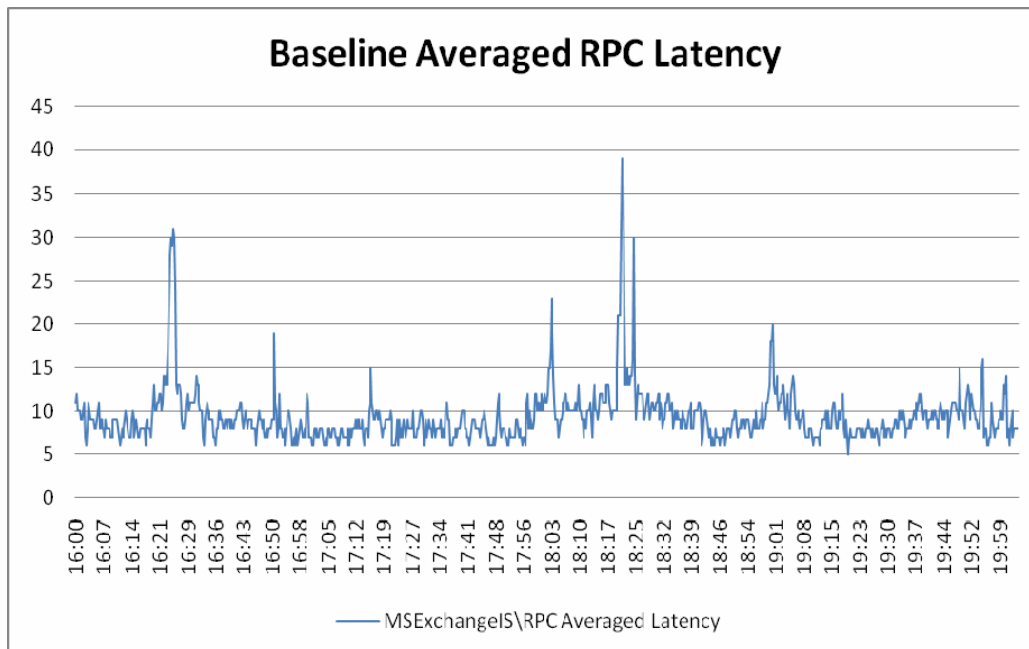

Database Read Latency

In an Exchange Server environment, disk read latency equates to degraded system performance. Microsoft recommends that average read latency for Exchange 2007 servers remain under 20ms, and that latency spikes over 50ms should not last more than a few seconds.

The chart below shows average database read latency of the database LUNS during the 10-hour test period. Average database read latency on the database LUNS was 8ms on the G drive and 9ms on the R drive. Graph of average read latency to ensure performance is within acceptable limits during the entire test.

Baseline Database Read Latency

PhysicalDisk(4 R:)\Avg. Disk sec/Read
PhysicalDisk(1 G:)\Avg. Disk sec/Read
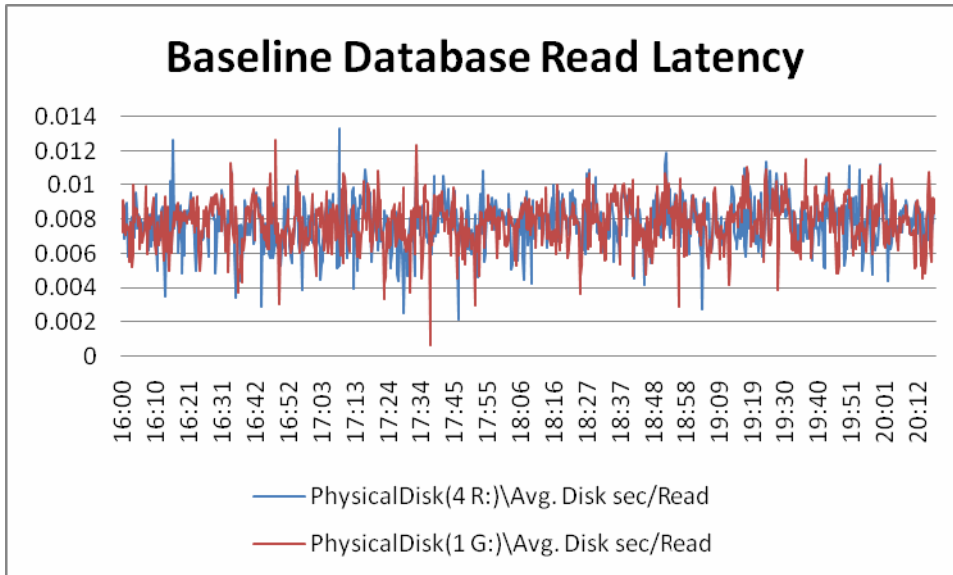
CPU Utilization
For an optimal Exchange Server environment, CPU utilization should average below 70%. The following chart shows CPU utilization during a baseline run of 10 hours. During the baseline run, with no scheduled snapshots, the average CPU utilization was 19%.

9

% Processor Time
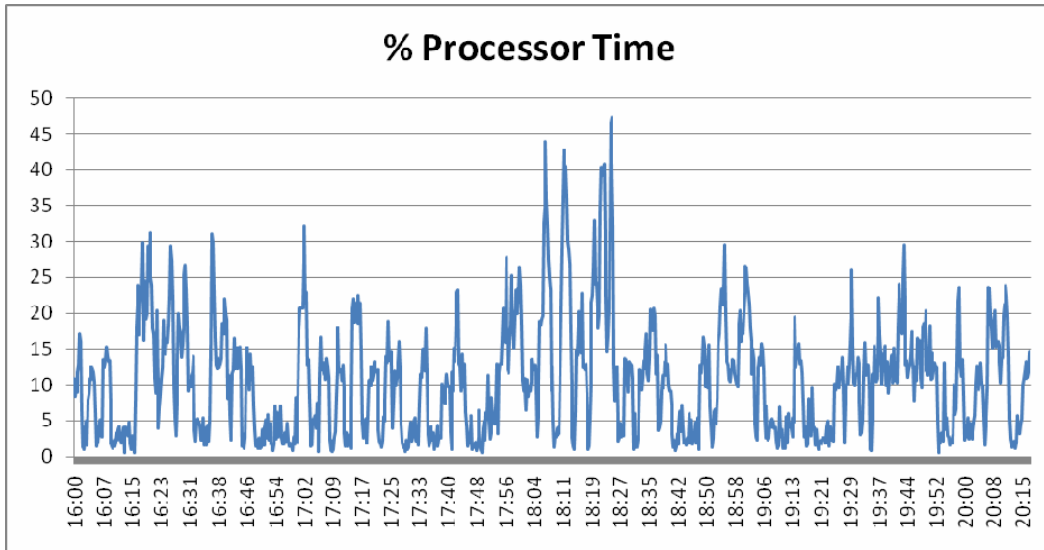
5.0 Performance Impact of NetApp Snapshots

The following charts show the impact NetApp Snapshots have on Exchange Server performance. During the 10-hour test period, SnapManager for Exchange was scheduled to take a snapshot backup every two hours with 24 snapshots kept online. The shaded areas in the charts below indicate periods where snapshots took place.

> **NOTE:** Verification times and performance were not a part of the testing performed. For additional information, as well as best practices on database checksum verification, refer to Chapter 10 of the SME Installation and Administration Guide.
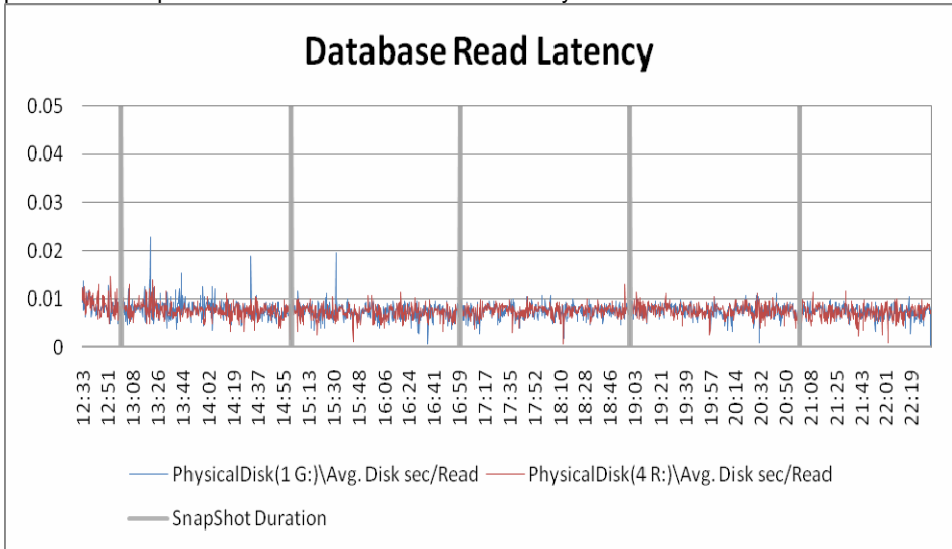
RPC Latency
The following chart shows RPC average latency with snapshots occurring every two hours. No significant changes were apparent in averaged PRC latency numbers. With Snapshot backups occurring every two hours, averaged RPC latency is still well within acceptable ranges, with no sustained spikes occurring during the Snapshot backup process.

Averaged RPC Latency
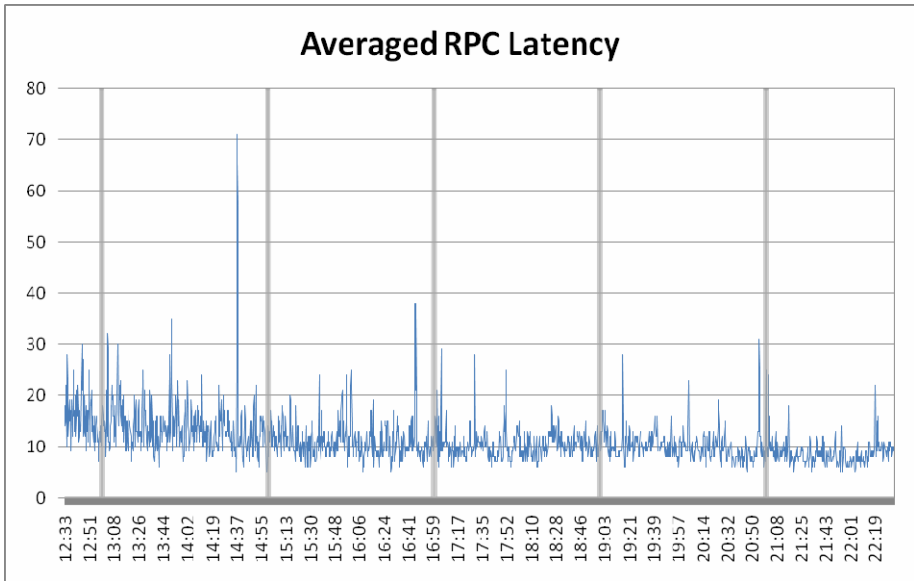
Database Read Latency
The following chart shows the database read latency with snapshots occurring every two hours. During the specified run period, database read latencies were eight milliseconds on average with a maximum spike of up to 22 milliseconds. Note that during the duration of the Snapshot backup operations, no sustained performance spikes occured in database read latency.

Database Read Latency

PhysicalDisk(1 G:)\Avg. Disk sec/Read   PhysicalDisk(4 R:)\Avg. Disk sec/Read
SnapShot Duration

CPU Utilization
The following chart shows the CPU utilization during the testing period. Average CPU utilization during this testing period was 11% with a maximum spike of 51%.

% Processor Time
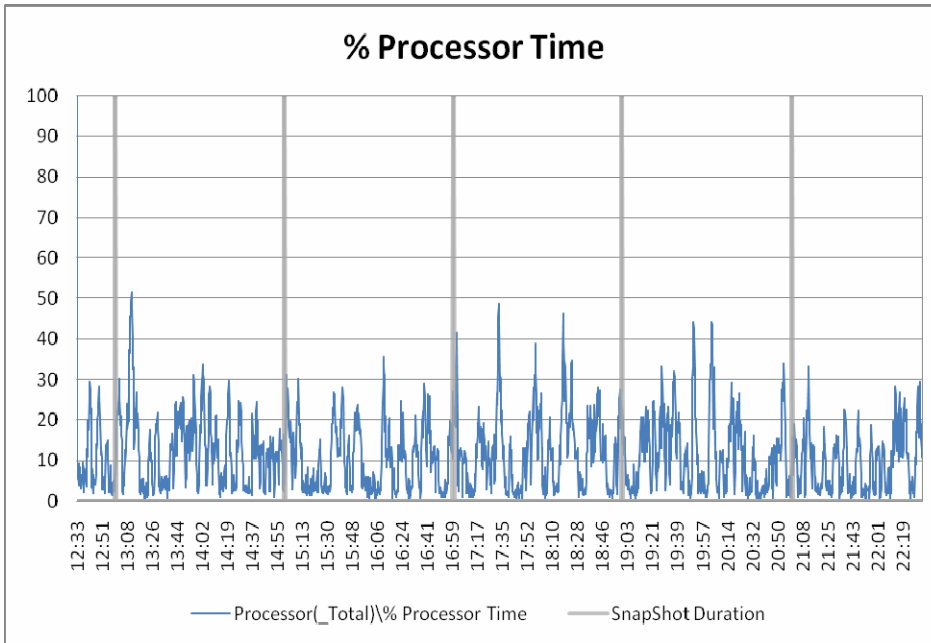
6.0 Performance Impact of Deleting Snapshots

Tests were configured to keep a total of 24 snapshots online. Once the number of online snapshots threshold is met, the oldest snapshot is deleted after successful completion of the next snapshot backup operation. This sections examines Exchange Server performance characteristics when deleting a VSS snapshot.

A base of 24 Snapshots were kept online to provide a base for this testing period. SnapManager for Exchange was configured to keep a total of 24 Snapshot backups online.

As part of a scheduled database backup job, backup deletion criteria (based on Snapshot copy age or quantity) can be specified. SnapManager automatically deletes the oldest backups for that storage group and backup management group after the backup is finished.

In order to determine any impact deleting Snapshots may have on performance, the impact NetApp Snapshots have on performance, performance counters were examined for a period of 4 minutes before and 20 minutes after each Snapshot operation The following charts show the performance characteristics of keeping 24 Snapshot backups online. All counters examined showed no dramatic increase while deleting the SnapShot backups.

6.1 Averaged RPC Latency

The chart below shows a representative sample of Averaged RPC latency surrounding a snapshot backup. The graph below shows temporary increases in RPC latency after the backup was performed and deleting the snapshot after it was completed. It is important to note that while a temporary increase is shown that Averaged RPC latency did not go beyond the 50 millisecond threshold.

RPC Average Latency

Snapshot — RPC Average Latency (Milliseconds)

13
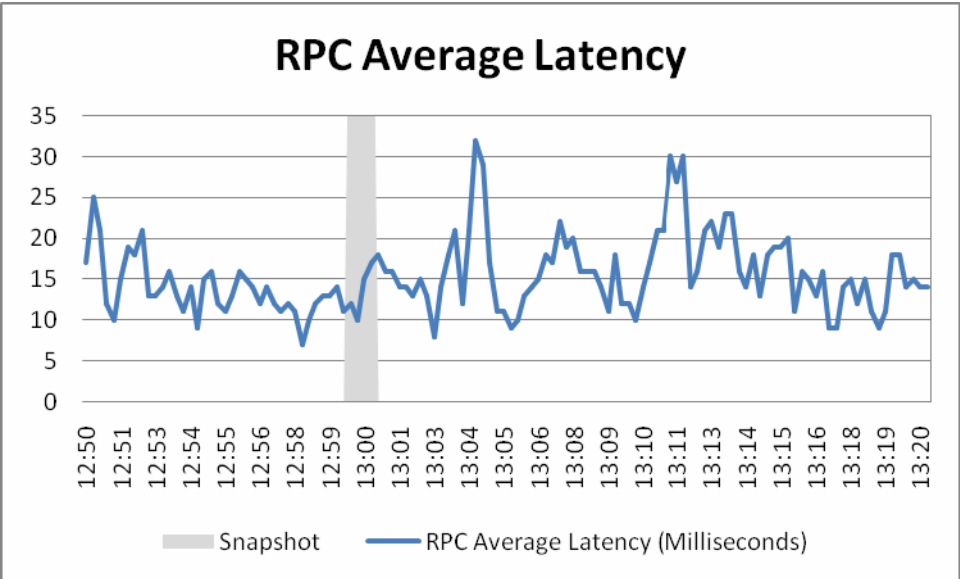
6.2 Database Read Latencies

The chart below shows a representative sampling of read latencies of the database LUNs. No sustained increase in database read latency is experienced as part of deleting the snapshot backup.

Database Read Latency
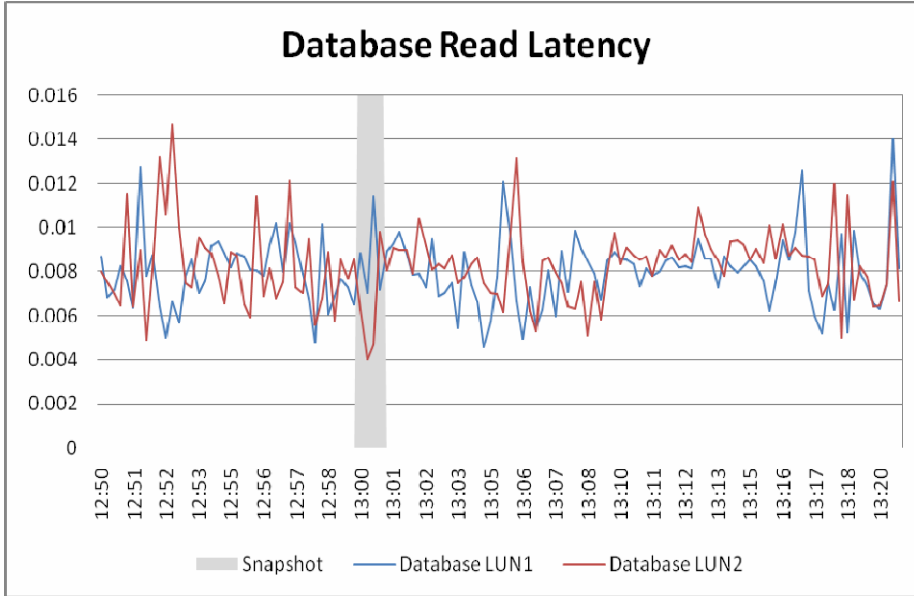
6.3 CPU Utilization

The chart below shows a temporary increase in CPU utilization in the minutes after the snapshot process. CPU utilization increased to a maximum of 50% then returned to the normal range.

% CPU Utilization
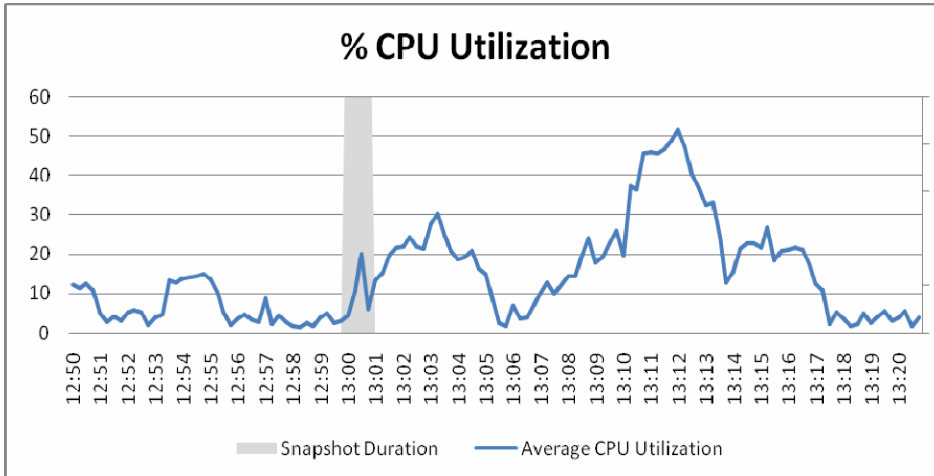
7.0 Conclusion

After examining Exchange Server 2007 performance characteristics during periods using NetApp Snapshot backups, it is clear that there is no performance impact on an Exchange Server. All performance counters, on average, remained virtually unchanged. It is also important to note that while running the test scenario with 24 Snapshot backups kept online, performance not only remained consistant but also well within accepted performance thresholds and Microsoft best practices

The combined features of Exchange Server 2007 and Network Appliance SnapManager for Exchange provide unparallelled ease of use and performance results. They also provide IT departments a method of meeting the backup demands of ever-increasing Exchange mailbox databases.