WHITE PAPER: DATA PROTECTION

Confidence in the connected world.

Veritas NetBackup™ for Microsoft® Exchange Server Solutions Guide

Larry Cadloff | February 2009

Contents

1.0 Goal of this paper

This paper describes a number of solutions for protecting and recovering Microsoft® Exchange Server installations. The challenges associated with protecting a Microsoft Exchange environment, as well as multiple strategies that address them, are discussed in this paper in an easy-to-comprehend format. On completion of reading this paper, you should be well positioned to describe available data protection solutions for Microsoft Exchange as provided by Veritas NetBackup™, the NetBackup for Microsoft Exchange Server agent, and the NetBackup Snapshot Client.

1.1 Intended audience

Anyone looking for information surrounding NetBackup and data protection solutions for Microsoft Exchange is encouraged to read this paper. Those with limited exposure to or experience with data protection solutions for Microsoft Exchange will benefit from the content presented.

If you've ever asked any of the following questions, you are a member of the target audience for this paper:

- Is NetBackup able to recover individual mailboxes and recover mailbox items at a granular level?
- What value and advantage does NetBackup provide for Microsoft Exchange that isn't available otherwise?
- What advantage is there to using Volume Shadow Copy Service (VSS) snapshots?
- When should off-host backups be considered?

1.2 Solution overview

NetBackup provides a comprehensive data protection solution, including centralized administration and reporting, media management, automated policy based backups, and restore. NetBackup for Microsoft Exchange Server extends the capabilities of NetBackup to include online backups and restores of Exchange databases. Additionally, NetBackup for Microsoft Exchange Server also provides a solution for protecting Exchange data at the mailbox level, facilitating granular recovery of mailboxes, messages, contacts, notes, tasks, and schedules.

An overview of the feature set provided by NetBackup for Microsoft Exchange Server includes:

- Online backups
- Full, incremental, differential, and copy-only backups
- Redirected restores
- Individual mailbox backup with granular restore
- Integrated Enterprise Client snapshot support for Volume Shadowcopy Service, off-host and backups and Instant Recovery database rollbacks.
- Continuous real-time Exchange database replication

1.3 Additional resources

A variety of additional resources are available at http://www.symantec.com/enterprise/support to assist in understanding NetBackup, NetBackup for Microsoft Exchange Server, and the NetBackup Snapshot Client, including:

- *Veritas NetBackup Administrator's Guides*
- *Veritas NetBackup for Microsoft Exchange Server Administrator's Guide*
- *Veritas NetBackup Snapshot Client Administrator's Guide*
- *Veritas NetBackup RealTime Protection Administrator's Guide*
- *Veritas NetBackup Database Agent Compatibility matrix*
- *Veritas NetBackup Snapshot Client OS Arrays and Database Compatibility matrix*

In addition, a wide variety of material is available from Microsoft, providing a vast array of information related to Exchange and Volume Shadowcopy Service. The following is an example of available resources:

- Best Practices for Using Volume Shadow Copy Service with Exchange Server 2003
  http://technet.microsoft.com/en-us/library/aa996004.aspx

- Exchange Server 2007 System Requirements
  http://technet.microsoft.com/en-us/library/1e80857c-b870-4a6d-a0f4-ff7b3a7be037.aspx

2.0 Technology issues solved with these solutions

Microsoft Exchange Server can be protected with the stock out-of-the-box Microsoft Backup utility solution that is included with Microsoft Windows Server®. The Microsoft Backup utility is also sometimes referred to as the “Windows Backup” program, or “NTBackup.” Limitations associated with the basic Microsoft Backup utility solution are numerous. Specific to protecting and recovering Microsoft Exchange Server, there is no support for mailbox-level protection, Volume Shadowcopy Service, nor off-host backups.

2.1 Granular mailbox protection

There are essentially two basic levels of Microsoft Exchange Server protection available. The first is referred to as database level protection, where Volume Shadowcopy Service (VSS) compliant snapshots or the Exchange backup API are used to perform full or incremental database backups. These backups can be used to recover individual databases within a Microsoft Exchange storage group, or an entire storage group. This method of backup is suitable for recovery from disasters or hardware failures.

The second basic type of Exchange protection is commonly referred to as a brick level backup. This type of backup uses MAPI (Messaging API) to protect Exchange mailboxes at a granular level. Mailbox backups are executed separately from Exchange storage group backups. Mailbox backups cannot be used to recover a database or storage group, but they can be used to recover individual mailboxes or mailbox content at a granular level. This method of backup is suitable for recovering accidentally deleted items.

The Microsoft Backup utility doesn’t support individual mailbox restores, or granular recovery of items within a mailbox. Microsoft does provide information detailing what a customer would need to do in order recover this data using what is referred to as recovery storage groups.

NetBackup for Microsoft Exchange Server includes the ability to perform both storage group and brick-level mailbox backups (dependent on the version of Microsoft Exchange being protected).

2.2 Volume Shadowcopy Service (VSS) snapshots

Exchange Server 2003 introduced support for backup in conjunction with Windows Server 2003 Volume Shadowcopy Service. For Exchange 2003 and 2007, Volume Shadowcopy Service acts as a mechanism for creating point-in-time copies of data that can be used for consistent Exchange storage group backup and recovery as an alternative to the older Exchange API backup method. Underlying Volume Shadowcopy Service provider components may be hardware or software assisted to improve snapshot performance and capabilities.

Additional Volume Shadowcopy Service information is available in appendix A .

NetBackup incorporates support for Volume Shadowcopy Service in conjunction with the Enterprise Client feature, detailed later in this paper.

2.3 Off-host backup

Off-host backup with respect to Exchange refers to the ability to use a copy of a Microsoft Exchange database that has been mounted on an alternate host for the purpose of performing a storage group backup. This can be accomplished in two different ways: by using the Cluster Continuous Replication feature available in Microsoft Exchange Server 2007, or by performing a Volume Shadowcopy Service compliant snapshot on the Microsoft Exchange server and transporting it via a SAN or iSCSI network to an alternate host. The alternate host, for instance, may be a NetBackup media server. In either case, the data residing on the alternate host is used as the source for the Exchange backup. This methodology removes virtually all overhead created by the backup process from the Exchange server, allowing users to send and receive email without any performance degradation.

NetBackup supports off-host backups using the snapshot feature of the Enterprise Client, and is supported for use in conjunction with NetBackup for Microsoft Exchange Server.

2.4 Instant Recovery rollbacks

As a supplement to a Microsoft Exchange backup, an administrator can elect to create one or more persistent snapshots on a server running Microsoft Exchange Server 2003 or 2007 and retain them on the Microsoft Exchange server. If a Microsoft Exchange database becomes corrupted or lost, it can be rolled back to a previous version in a matter of seconds.

NetBackup provides the ability to create and manage Instant Recovery images using the snapshot feature of the Enterprise Client.

2.5 Real-time continuous data protection

With appropriate hardware and software it is possible to continuously replicate Exchange database transactions to another location and use it for recovery purposes. NetBackup RealTime, a member of the NetBackup family, provides these capabilities. When used with NetBackup Enterprise Server, RealTime allows a backup administrator to restore data from any point in time that is present in the replicated database.

3.0 Technology overview

Protecting Microsoft Exchange Server includes backing up Microsoft Exchange databases and log files. In addition to these items, data related to the Microsoft Exchange Server installation should also be protected. Related data includes active directory information, certificate services data, system replication services data, system state data (including the IIS metabase), and any cluster information applicable to the Microsoft Exchange Server installation.

NetBackup provides a comprehensive set of data protection technologies that address the requirements and suggestions presented by Microsoft with regard to protecting Exchange environments.

3.1 Challenges addressed with this technology

Challenges in protecting and recovering Microsoft Exchange servers are numerous. This subsection provides an overview of challenges and recommends solutions architected to overcome them.

3.1.1 Standard solution

The standard solution provided by the Microsoft Backup utility (the utility provided by Microsoft) provides basic backup and recovery functionality for Exchange environments. As previously stated, the Microsoft Backup utility doesn’t provide granular mailbox recovery, support the use of Volume Shadowcopy Service snapshots with Microsoft Exchange Server, or support performing off-host backups. These limitations can become gating factors when architecting an appropriate solution for a given Exchange environment. Considerations that should be taken into account relative to the standard solution include:

- Mailbox recovery facilitates the ability to recover individual mailboxes as well as granular recovery of individual mailbox items. Some Microsoft Exchange Server administrators may desire this functionality in an effort to respond to restore requests. With the standard solution, the administrator must deny the restore request, or perform the restore by means of a recovery storage group. Using a recovery storage group to recover individual mailboxes is time-consuming, administratively intensive, and requires storage space for an entire storage group.

- Backup is all about being able to recover data based on a recovery point objective, as well as a recovery time objective. Volume Shadowcopy Service snapshots enable the ability to perform multiple daily backups of Exchange databases. Frequent backups enhance the goal of an improved recovery point objective. Additionally, Volume Shadowcopy Service snapshots also work with Instant Recovery, enabling a reduced recovery time objective. Finally, by using NetBackup RealTime, you can maintain a continuously updated replica of a Microsoft Exchange database without performing periodic backups, and perform recovery of this database from any specific point in time that is stored on the replication server.
- Off-host backups provide a method of removing the backup processing workload from the Exchange server and placing it on an alternate host, typically a NetBackup media server or the passive node of a Microsoft Exchange 2008 Continuous Cluster Replication (CCR) cluster. Exchange servers that are heavily loaded processing online transactions benefit from this technology in that users will experience the same transaction service level regardless of how frequently the Exchange databases are being protected. The possible alternatives to using this technology include reduced transactional response times for users while the Exchange server is being backed up, fewer Exchange backups (resulting in an increased recovery point), or the need to deploy additional Exchange servers in an effort to reduce overall processing workload.

The standard solution includes additional limiting factors that may be less obvious:

- Centralized administration isn't possible with the basic the Microsoft Backup utility. The requirement to protect Exchange Server System State information requires that the Microsoft Backup utility be executed locally on each Exchange server. While Exchange database backups can be performed remotely, system state backups are not able to be performed remotely with the Microsoft Backup utility.
- Reporting is less than optimal, and may incur additional administrative overhead when using the Microsoft Backup utility. Reports may need to be collated among multiple the Microsoft Backup utility instances in order to facilitate comprehensive "roll-up" reporting that reflects operational status of an environment.
- Duplicating backups performed with the Microsoft Backup utility presents another significant challenge. Tracking any duplicates that may be rotated off-site presents yet another challenge.

The limiting factors presented here aren't intended to serve as an exhaustive list. They are mentioned so that the need for enhanced solutions becomes clear. Organizations with more than a single small Exchange server can benefit from the solutions recommended in this paper.

3.1.2 Good, better, and best solutions

NetBackup is easily customized to accommodate a variety of Exchange data protection solutions. Presented in this subsection are "good," "better," and "best" solutions that extend the basic capabilities available in the standard the Microsoft Backup utility.

- Good solution

  This solution uses the NetBackup for Microsoft Exchange Server agent and provides database backup and restore functionality. Also provided is the ability to protect and recover mailboxes at a granular level. The "good" solution is superior to the standard the Microsoft Backup utility in that it provides centralized administration and reporting, the ability to use integrated NetBackup technologies such as compression, encryption, media management, storage units, and Storage Lifecycle Policies, while adding a mailbox protection strategy.

- Better solution

  The "better" solution uses NetBackup for Microsoft Exchange Server agent and supplies all the advantages of the "good" solution, with the added ability to perform off-host and Instant Recovery

Volume Shadowcopy Service snapshot backups. This added capability requires the use of Snapshot Client software, part of the NetBackup Enterprise Client.

- Best solution

  The “best” solution uses the NetBackup for Microsoft Exchange Server agent snapshots together with NetBackup RealTime to create a continuously updated replica of the Exchange server that can be recovered to any point in time.

The following table summarizes features of the standard the Microsoft Backup utility solution, as well as the recommended “good,” “better,” and “best” NetBackup solutions:

Solution Comparison				
Solution	Standard	Good	Better	Best
Recommended for	Exchange deployments with basic backup and recovery requirements.	Exchange deployments requiring centralized management and possible mailbox recovery.	Exchange deployments requiring centralized management, possible mailbox recovery, a need for frequent backups with minimal impact on the Exchange server and fast recovery.	Exchange deployments requiring centralized management, possible mailbox recovery, frequent backups with minimal impact to the Exchange server, and replication backups with true continuous coverage.
Basic Exchange database backup and recovery	✓	✓	✓	✓
Centralized management	X	✓	✓	✓
Mailbox backup with granular recovery	X	✓	✓	✓
Instant Recovery database rollback	X	X	✓	✓
Off-host backup support	X	X	✓	✓
Continuous real-time replication with point-in-time recovery	X	X	X	✓

Table 1: Solution comparison

The next table characterizes performance speed for backup and recovery, as well as the impact of backup on the Exchange server platform:

Relative Performance Comparison				
Solution	Standard	Good	Better	Best
Restore Speed	Poor	Fast	Faster	Instant
Backup Speed	Poor	Fast	Faster	Continuous
Reduced Backup Impact	X	X	✓	✓

Table 2: Performance comparison

4.0 Architecture

In this section, the “good,” “better,” and “best” solutions are examined in more detail. Insight is provided regarding the applicable Exchange environment, as well as any required hardware and software for each solution.

4.1 Good solution

The targeted Exchange environment for the “good” solution consists of:

- A range of Exchange servers beginning with a single lightly loaded server to multiple moderately loaded servers.

  Exchange database backups will place an additional processing load on these servers. Highly utilized Exchange servers will likely be impacted by backup processing to the point where transactional response times become elongated.

- A desired recovery point objective that takes into consideration the frequency at which backups can be performed.

  The time required to perform a full database backup directly correlates to possible recovery points. Take for example the case where a full backup is executed daily. In theory, if a service interruption occurred that required a restore, restoring the last full backup would take the recovery point back a maximum of 24 hours plus the time it took to perform the restore job.

- A need for centralized administration and reporting.

  The core NetBackup product provides numerous benefits that include centralized administration and reporting.

- Possible requirements for mailbox or granular mailbox recovery.

  Some customers have decided not to perform mailbox backups as they typically run much slower and longer when compared to database backups, and cannot be used to recover a database. Other customers have decided to protect a subset of mailboxes with this level of protection, usually mailboxes belonging to their executive staff.

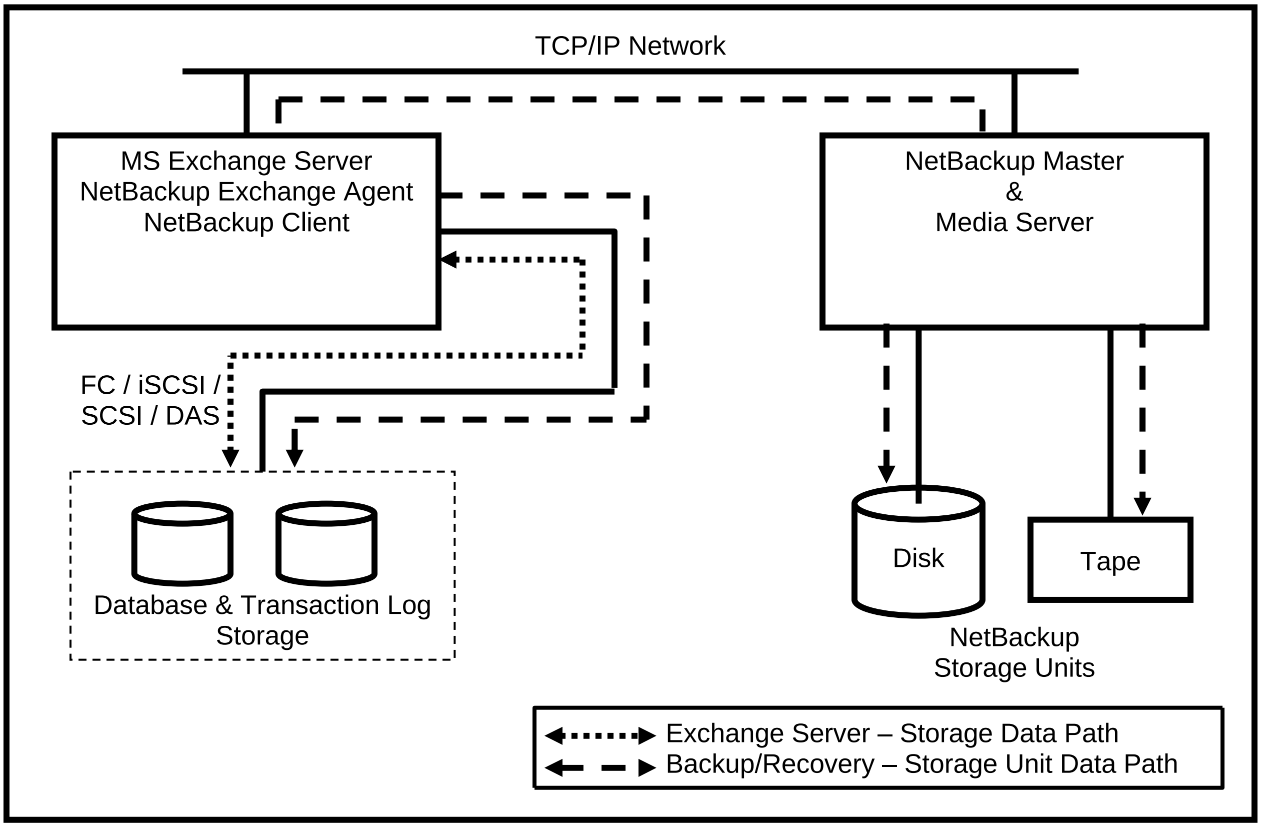
  While NetBackup still supports full and incremental mailbox backups, most Microsoft Exchange Server administrators will prefer to take advantage of its unique granular recovery feature, which allows individual mailboxes to be restored from a database backup. No “brick-level” backup is required; the same backup image can be used for both database disaster recovery and individual mail message restores.

- Possible requirements for duplication and/or offsite vaulting of backup media

  Customers that duplicate Exchange backups can benefit from the ability to duplicate backups inline (concurrent with the initial backup) or after the fact with a Storage Lifecycle Policy. Additionally, the NetBackup Vault option facilitates efficient processing and tracking of removable media sent off site for disaster recovery preparedness.

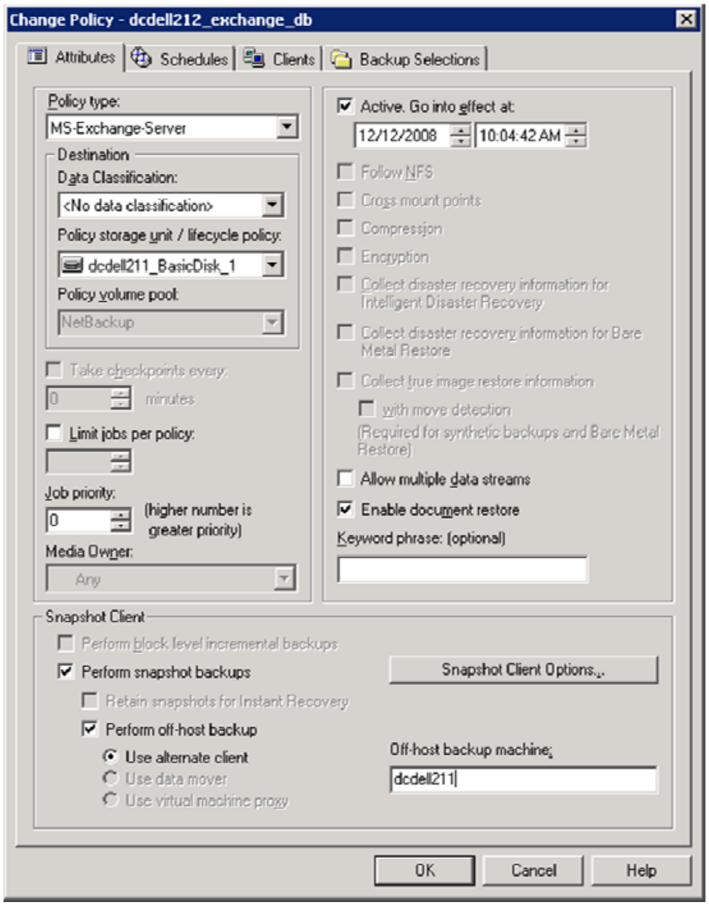
Hardware for the “good” solution includes NetBackup master and media server platforms. Both master and media server functions can be co-located on a single host, and can even be co-located on the Exchange server if desired. Also required is backup media. Disk, removable tape, and virtual tape media are all supported.

Software for the “good” solution includes NetBackup enterprise server and NetBackup for Microsoft Exchange Server software. Additional software licenses for tape or virtual tape libraries, enterprise disk foundation disk storage devices, or the NetBackup Vault option may also be required.



Graphic 1: "Good" solution block diagram

The NetBackup policy for this configuration is simple and straightforward. Select a policy type equal to “MS-Exchange-Server”, and select a suitable “Policy storage unit / lifecycle policy”:



Change Policy - dcdell212_exchange_db

Policy type: MS-Exchange-Server

Destination

Data Classification: <No data classification>

Policy storage unit / lifecycle policy: dcdell211_BasicDisk_1

Policy volume pool: NetBackup

□ Take checkpoints every 0 minutes

□ Limit jobs per policy:

Job priority: 0 (higher number is greater priority)

Media Owner: Any

☑ Active. Go into effect at: 12/12/2008 10:04:42 AM

□ Follow NFS

□ Cross mount points

□ Compression

□ Encryption

□ Collect disaster recovery information for Intelligent Disaster Recovery

□ Collect disaster recovery information for Bare Metal Restore

□ Collect true image restore information

□ with move detection

(Required for synthetic backups and Bare Metal Restore)

□ Allow multiple data streams

☑ Enable document restore

Keyword phrase: (optional)

Snapshot Client

□ Perform block level incremental backups

☑ Perform snapshot backups

□ Retain snapshots for Instant Recovery

☑ Perform off-host backup

● Use alternate client

○ Use data mover

○ Use virtual machine proxy

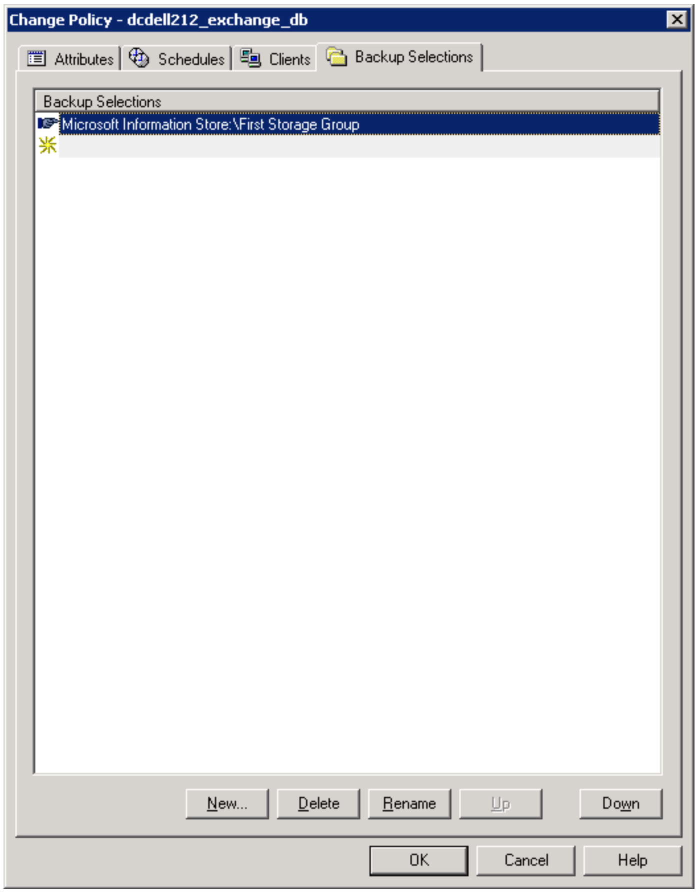
Off-host backup machine: dcdell211

Graphic 2: "Good" solution NetBackup policy attributes

Note that the “Enable document restore” checkbox is selected, and the Policy storage unit is a disk device (dcdell211_BasicDisk_1). Using these settings will make it possible to restore individual mailbox items from a database backup.

NetBackup schedules can be created to reflect when full, incremental differential or incremental cumulative backups should be executed. Retention periods for each backup type can also be selected on the schedule.

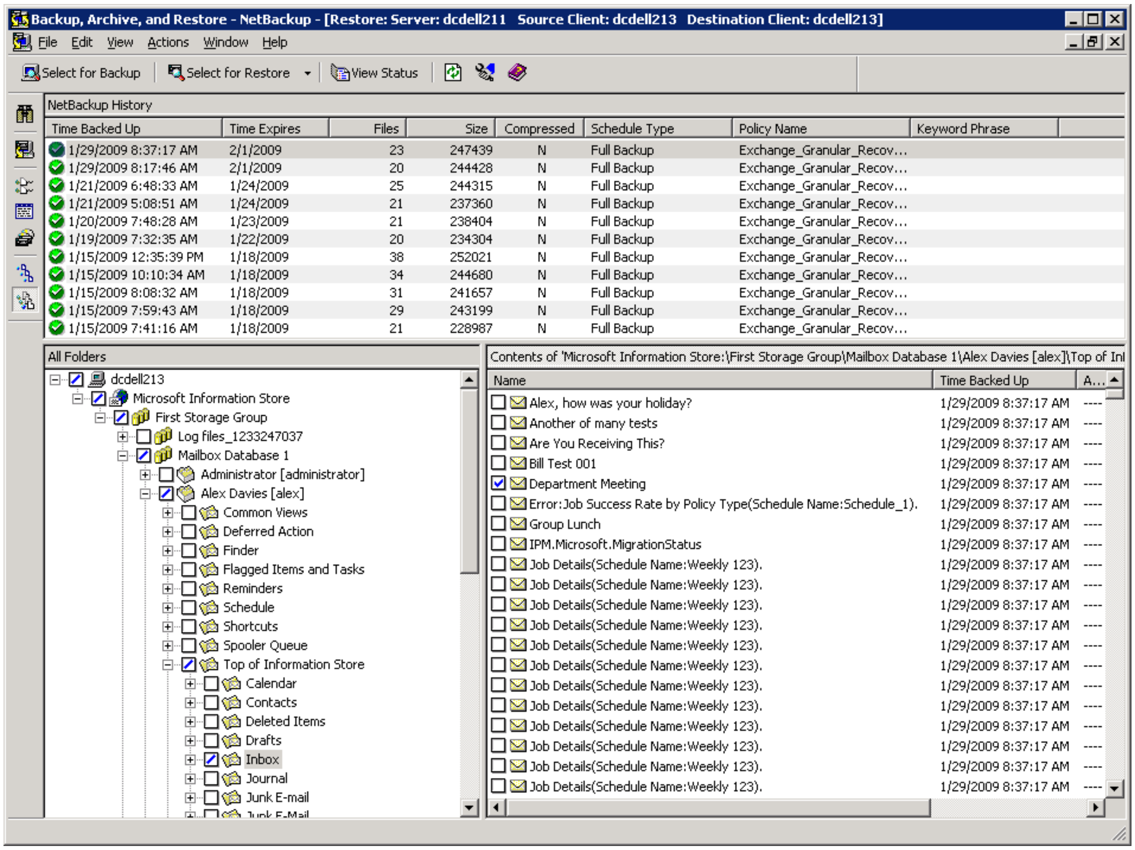
The NetBackup policy “Backup Selections” can be populated by using available directives. In this example, Microsoft Exchange databases associated with a storage group are selected for backup. A directive has been used to populate the backup selections list with “Microsoft Information Store:\First Storage Group”:



Microsoft Information Store:\First Storage Group

Graphic 3: "Good" solution NetBackup policy backup selection

During the recovery process the NetBackup administrator (or an authorized user) can restore an entire database, or drill down into the Microsoft Exchange database in order to restore individual mail items.


Backup, Archive, and Restore - NetBackup - [Restore: Server: dcdell211 Source Client: dcdell213 Destination Client: dcdell213]
File Edit View Actions Window Help
Select for Backup
Select for Restore
View Status

NetBackup History

Time Backed Up	Time Expires	Files	Size	Compressed	Schedule Type	Policy Name	Keyword Phrase
1/29/2009 8:37:17 AM	2/1/2009	23	247439	N	Full Backup	Exchange_Granular_Recov…	
1/29/2009 8:17:46 AM	2/1/2009	20	244428	N	Full Backup	Exchange_Granular_Recov…	
1/21/2009 6:48:33 AM	1/24/2009	25	244315	N	Full Backup	Exchange_Granular_Recov…	
1/21/2009 5:08:51 AM	1/24/2009	21	237360	N	Full Backup	Exchange_Granular_Recov…	
1/20/2009 7:48:28 AM	1/23/2009	21	238404	N	Full Backup	Exchange_Granular_Recov…	
1/19/2009 7:32:35 AM	1/22/2009	20	234304	N	Full Backup	Exchange_Granular_Recov…	
1/15/2009 12:35:39 PM	1/18/2009	38	252021	N	Full Backup	Exchange_Granular_Recov…	
1/15/2009 10:10:34 AM	1/18/2009	34	244680	N	Full Backup	Exchange_Granular_Recov…	
1/15/2009 8:08:32 AM	1/18/2009	31	241657	N	Full Backup	Exchange_Granular_Recov…	
1/15/2009 7:59:43 AM	1/18/2009	29	243199	N	Full Backup	Exchange_Granular_Recov…	
1/15/2009 7:41:16 AM	1/18/2009	21	228987	N	Full Backup	Exchange_Granular_Recov…	

All Folders

- ☑ dcdell213
  - ☑ Microsoft Information Store
    - ☑ First Storage Group
      - ☐ Log files_1233247037
      - ☑ Mailbox Database 1
        - ☐ Administrator [administrator]
        - ☑ Alex Davies [alex]
          - ☐ Common Views
          - ☐ Deferred Action
          - ☐ Finder
          - ☐ Flagged Items and Tasks
          - ☐ Reminders
          - ☐ Schedule
          - ☐ Shortcuts
          - ☐ Spooler Queue
          - ☑ Top of Information Store
            - ☐ Calendar
            - ☐ Contacts
            - ☐ Deleted Items
            - ☐ Drafts
            - ☑ Inbox
            - ☐ Journal
            - ☐ Junk E-mail
            - ☐ Junk E-Mail

Contents of 'Microsoft Information Store:\First Storage Group\Mailbox Database 1\Alex Davies [alex]\Top of Inl

Name	Time Backed Up	A…
☐ Alex, how was your holiday?	1/29/2009 8:37:17 AM	----
☐ Another of many tests	1/29/2009 8:37:17 AM	----
☐ Are You Receiving This?	1/29/2009 8:37:17 AM	----
☐ Bill Test 001	1/29/2009 8:37:17 AM	----
☑ Department Meeting	1/29/2009 8:37:17 AM	----
☐ Error:Job Success Rate by Policy Type(Schedule Name:Schedule_1).	1/29/2009 8:37:17 AM	----
☐ Group Lunch	1/29/2009 8:37:17 AM	----
☐ IPM.Microsoft.MigrationStatus	1/29/2009 8:37:17 AM	----
☐ Job Details(Schedule Name:Weekly 123).	1/29/2009 8:37:17 AM	----
☐ Job Details(Schedule Name:Weekly 123).	1/29/2009 8:37:17 AM	----
☐ Job Details(Schedule Name:Weekly 123).	1/29/2009 8:37:17 AM	----
☐ Job Details(Schedule Name:Weekly 123).	1/29/2009 8:37:17 AM	----
☐ Job Details(Schedule Name:Weekly 123).	1/29/2009 8:37:17 AM	----
☐ Job Details(Schedule Name:Weekly 123).	1/29/2009 8:37:17 AM	----
☐ Job Details(Schedule Name:Weekly 123).	1/29/2009 8:37:17 AM	----
☐ Job Details(Schedule Name:Weekly 123).	1/29/2009 8:37:17 AM	----
☐ Job Details(Schedule Name:Weekly 123).	1/29/2009 8:37:17 AM	----
☐ Job Details(Schedule Name:Weekly 123).	1/29/2009 8:37:17 AM	----
☐ Job Details(Schedule Name:Weekly 123).	1/29/2009 8:37:17 AM	----
☐ Job Details(Schedule Name:Weekly 123).	1/29/2009 8:37:17 AM	----

Graphic 4: Recovering a single mailbox item

Note that granular recovery of calendar, contact, draft, deleted items, journal, notes, sent items, or folders is also possible.

4.2 Better solution

The targeted Microsoft Exchange environment for the “better” solution consists of:

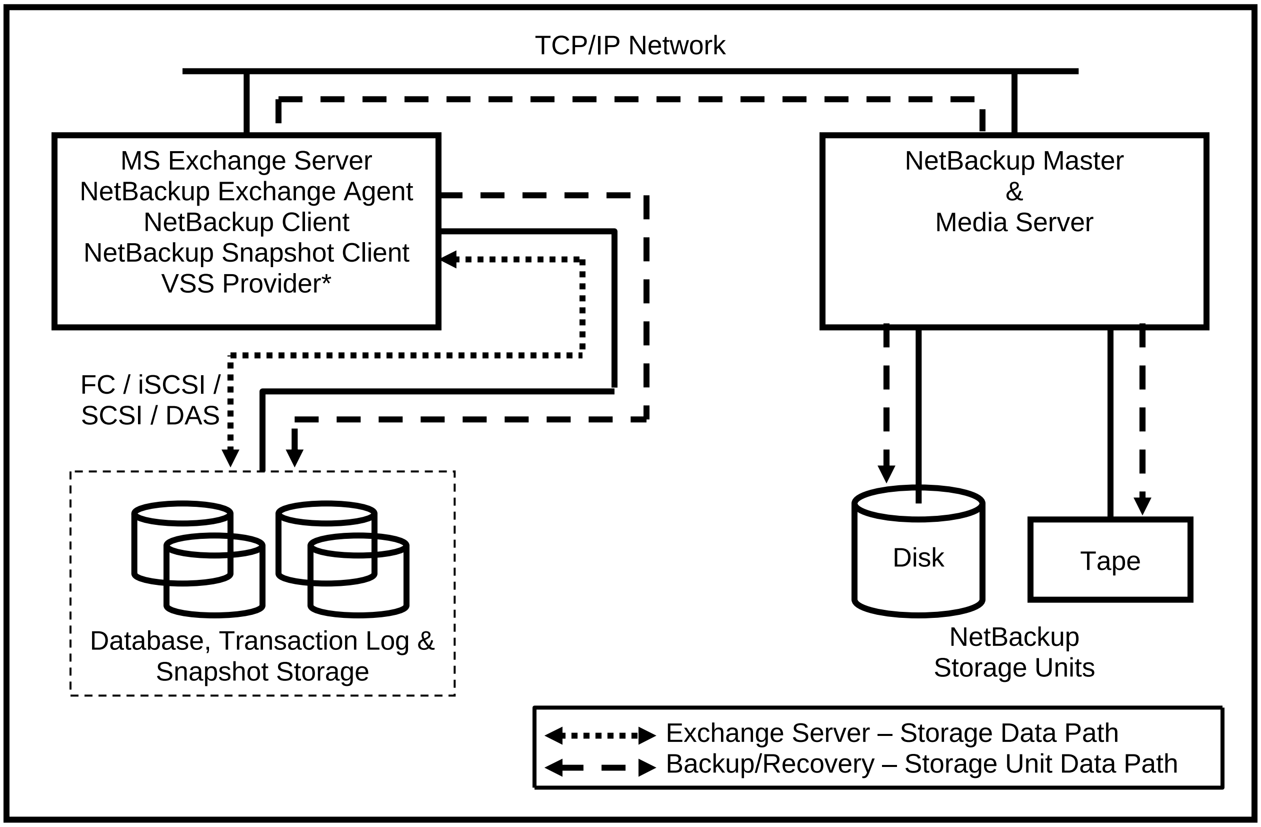
- A range of Microsoft Exchange servers beginning with a single lightly loaded server to multiple moderately loaded servers

  Dependent on the Volume Shadowcopy Service provider used, Microsoft Exchange database backups will place some additional processing load of these servers. Snapshot only backups are likely to incur a minimal increase in loading, whereas copying snapshots to a storage unit will incur a moderate increase in loading. Highly utilized Microsoft Exchange servers will likely be impacted by copying snapshots to a storage unit to the point where transactional response times become elongated.

- Recovery point and time objectives that require frequent backups and instant recovery performance.
- A need for centralized administration and reporting.
- Possible requirements for mailbox or granular mailbox recovery.
- Possible requirements for duplication and/or offsite vaulting of backup media.

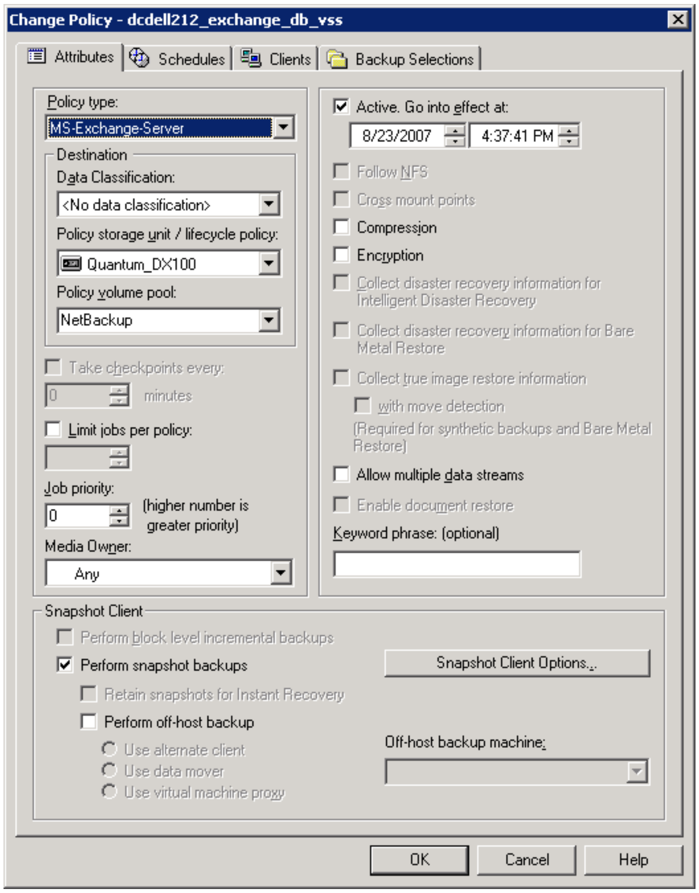
Hardware for the “better” solution includes NetBackup master and media server platforms. Both master and media server functions can be co-located on a single host, and can even be co-located on the Microsoft Exchange server if desired. Also required is backup media. Disk, removable tape, and virtual tape media are all supported. Additionally, a Volume Shadowcopy Service snapshot provider is required, which can be hardware- or software-based. Software-based Volume Shadowcopy Service providers are resident on the Microsoft Exchange server platform, while hardware Volume Shadowcopy Service providers are resident within a disk array or disk enclosure (hardware Volume Shadowcopy Service providers usually also require support software to be installed on the Microsoft Exchange server).

Software for the “better” solution includes NetBackup enterprise server and NetBackup for Microsoft Exchange Server software. A NetBackup Enterprise Client license (which includes the Snapshot Client feature) is also required in order to use Volume Shadowcopy Service snapshots. Additional software licenses for tape or virtual tape libraries, enterprise disk foundation disk storage devices, or the NetBackup Vault option may also be required.



Graphic 5: "Better" solution block diagram

The NetBackup policy for this configuration includes configuring the snapshot provider. The policy type is set to “MS-Exchange-Server”, and a “Policy storage unit / lifecycle policy” is selected. Additionally, the Snapshot Client is configured by selecting the “Perform snapshot backups” checkbox:



Change Policy - dcdell212_exchange_db_vss

Attributes | Schedules | Clients | Backup Selections

Policy type: MS-Exchange-Server

Destination

Data Classification: <No data classification>

Policy storage unit / lifecycle policy: Quantum_DX100

Policy volume pool: NetBackup

□ Take checkpoints every: 0 minutes

□ Limit jobs per policy:

Job priority: 0 (higher number is greater priority)

Media Owner: Any

☑ Active. Go into effect at: 8/23/2007 4:37:41 PM

□ Follow NFS

□ Cross mount points

□ Compression

□ Encryption

□ Collect disaster recovery information for Intelligent Disaster Recovery

□ Collect disaster recovery information for Bare Metal Restore

□ Collect true image restore information

□ with move detection

(Required for synthetic backups and Bare Metal Restore)

□ Allow multiple data streams

□ Enable document restore

Keyword phrase: (optional)

Snapshot Client

□ Perform block level incremental backups

☑ Perform snapshot backups

□ Retain snapshots for Instant Recovery

□ Perform off-host backup

○ Use alternate client

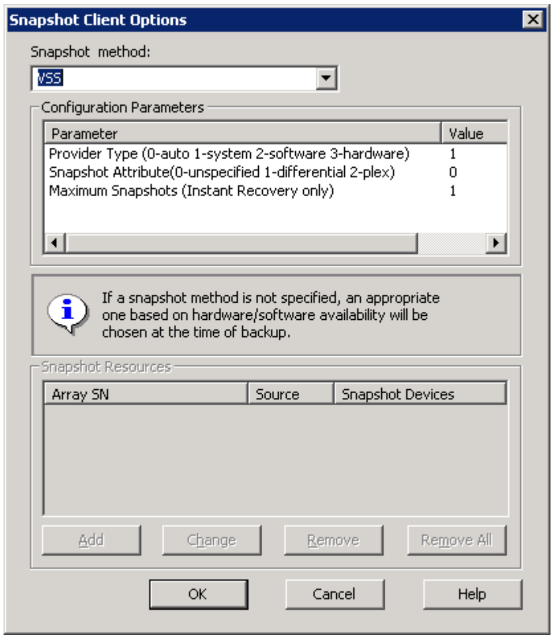
○ Use data mover

○ Use virtual machine proxy

Off-host backup machine:

Graphic 6: "Better" solution NetBackup policy attributes

Clicking the “Snapshot Client Options” button opens an additional dialog window where snapshot-specific parameters can be set:



Snapshot Client Options

Snapshot method: VSS

Configuration Parameters

Parameter	Value
Provider Type (0-auto 1-system 2-software 3-hardware)	1
Snapshot Attribute(0-unspecified 1-differential 2-plex)	0
Maximum Snapshots (Instant Recovery only)	1

If a snapshot method is not specified, an appropriate one based on hardware/software availability will be chosen at the time of backup.

Snapshot Resources

Array SN	Source	Snapshot Devices

Graphic 7: “Better” solution snapshot client options

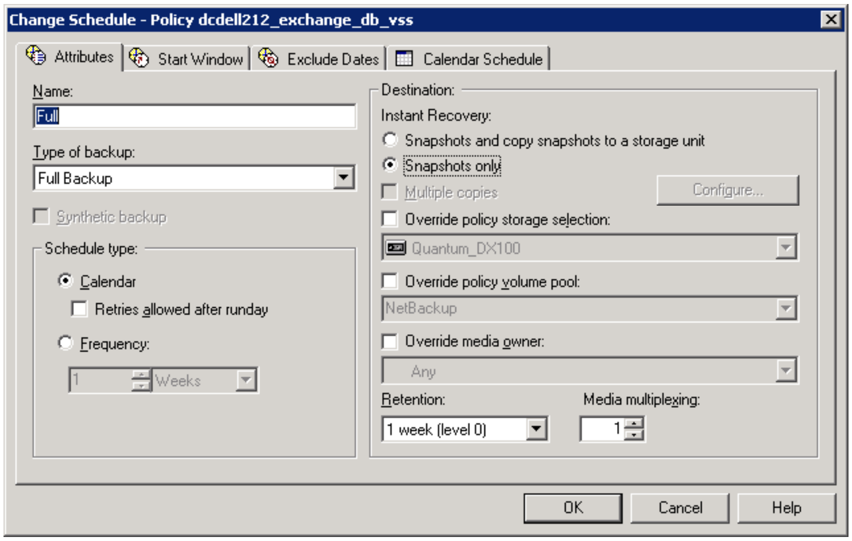
About the “Snapshot Client Options” window:

- The “Snapshot method” pull-down menu should be set to equal “VSS”.
- The “Configuration Parameters” section contains parameters and values that can be assigned to them.

Volume Shadowcopy Service Configuration Parameters		
Parameter	Value	Description
Provider Type	0–Auto	The Volume Shadowcopy Service provider is automatically selected based on the providers available for the snapshot volumes.
	1–System	The default Microsoft Volume Shadowcopy Service provider is used.
	2–Software	The Veritas Storage Foundation for Windows Volume Shadowcopy Service provider is used
	3–Hardware	A hardware Volume Shadowcopy Service provider is used.
Snapshot Attribute	0–Unspecified	The value of zero or “unspecified” indicates that this snapshot cannot be used for Instant Recovery.
	1–Differential	The value of one or “differential” implies the use of a space optimized or copy-on-write type of snapshot. An example is the EMC CLARiiON SnapView™ snapshot method.
	2–Plex	The value of two or “plex” implies the use of a mirrored type of snapshot. An example is the EMC CLARiiON SnapView clone method.
Maximum Snapshots (Instant Recovery only)	1 or more	This option defines the number of snapshots retained for instant recovery. When this threshold is reached the oldest snapshot is deleted and a new snapshot is taken.

Table 3: Snapshot Client configuration parameters

The Snapshot Client will also facilitate configuring NetBackup policy schedules such that snapshots can be used in two ways. One method is to use snapshots and also copy the snapshot to a storage unit. The second method is to use snapshots only. It is possible to have multiple schedules in the same policy. This creates great flexibility in taking regular frequent snapshots, as well as taking snapshots and copying them to a storage unit at less frequent intervals:



Change Schedule - Policy dcdell212_exchange_db_vss

Name: Full

Type of backup: Full Backup

□ Synthetic backup

Schedule type:

● Calendar

□ Retries allowed after runday

○ Frequency: 1 Weeks

Destination:

Instant Recovery:

○ Snapshots and copy snapshots to a storage unit

● Snapshots only

□ Multiple copies

□ Override policy storage selection: Quantum_DX100

□ Override policy volume pool: NetBackup

□ Override media owner: Any

Retention: 1 week (level 0)

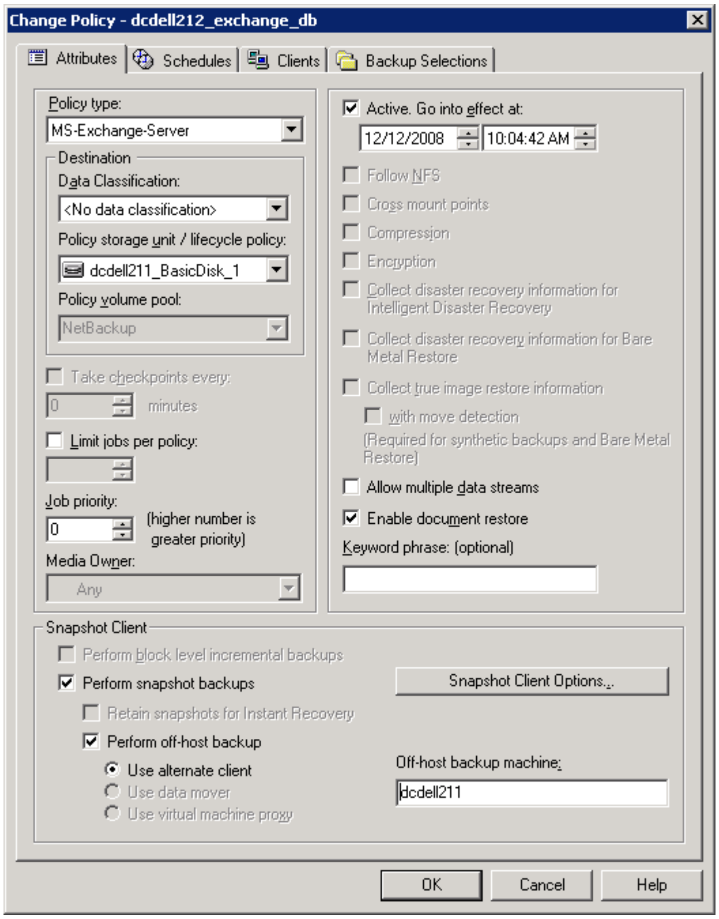
Media multiplexing: 1

Graphic 8: Schedule Instant Recovery snapshot options

Instant Recovery cannot be used in combination with granular restore. If the “Enable document restore” checkbox is selected in the policy attributes, the “Retain snapshots for instant recovery” will be grayed out and cannot be selected.

If the Microsoft Exchange database resides on a SAN device with appropriate underlying Volume Shadowcopy Service software or hardware support, it is possible to perform an off-host backup by performing a snapshot, detaching the snapshot from the Microsoft Exchange server, and attaching it to a NetBackup media server. This puts a minimal load on the Microsoft Exchange server at the beginning of a backup, and no load at all on the Microsoft Exchange server while a backup is in progress. When the backup is done, the volume is detached from the media server and re-attached and synchronized with the Microsoft Exchange server.

Configuring an off-host backup requires the addition of the name of the off-host server to the snapshot section at the bottom of the policy configuration dialog. In this case, we will be using the media server dcdell211:


Change Policy - dcdell212_exchange_db
Attributes
Schedules
Clients
Backup Selections
Snapshot Client Options...
OK
Cancel
Help

Policy type: MS-Exchange-Server

Destination

Data Classification: <No data classification>

Policy storage unit / lifecycle policy: dcdell211_BasicDisk_1

Policy volume pool: NetBackup

□ Take checkpoints every: 0 minutes

□ Limit jobs per policy:

Job priority: 0 (higher number is greater priority)

Media Owner: Any

☑ Active. Go into effect at: 12/12/2008 10:04:42 AM

□ Follow NFS

□ Cross mount points

□ Compression

□ Encryption

□ Collect disaster recovery information for Intelligent Disaster Recovery

□ Collect disaster recovery information for Bare Metal Restore

□ Collect true image restore information

□ with move detection

(Required for synthetic backups and Bare Metal Restore)

□ Allow multiple data streams

☑ Enable document restore

Keyword phrase: (optional)

Snapshot Client

□ Perform block level incremental backups

☑ Perform snapshot backups

□ Retain snapshots for Instant Recovery

☑ Perform off-host backup

● Use alternate client

○ Use data mover

○ Use virtual machine proxy

Off-host backup machine: dcdell211

Graphic 9: "Good" solution NetBackup snapshot policy with off-host backup

An off-host backup may be used in combination with other backup attributes, such as Instant Recovery and Granular Recovery. As noted above, Instant Recovery and Granular Recovery cannot both be used in the same policy.

4.3 Best solution

The targeted Microsoft Exchange environment for the “best” solution consists of:

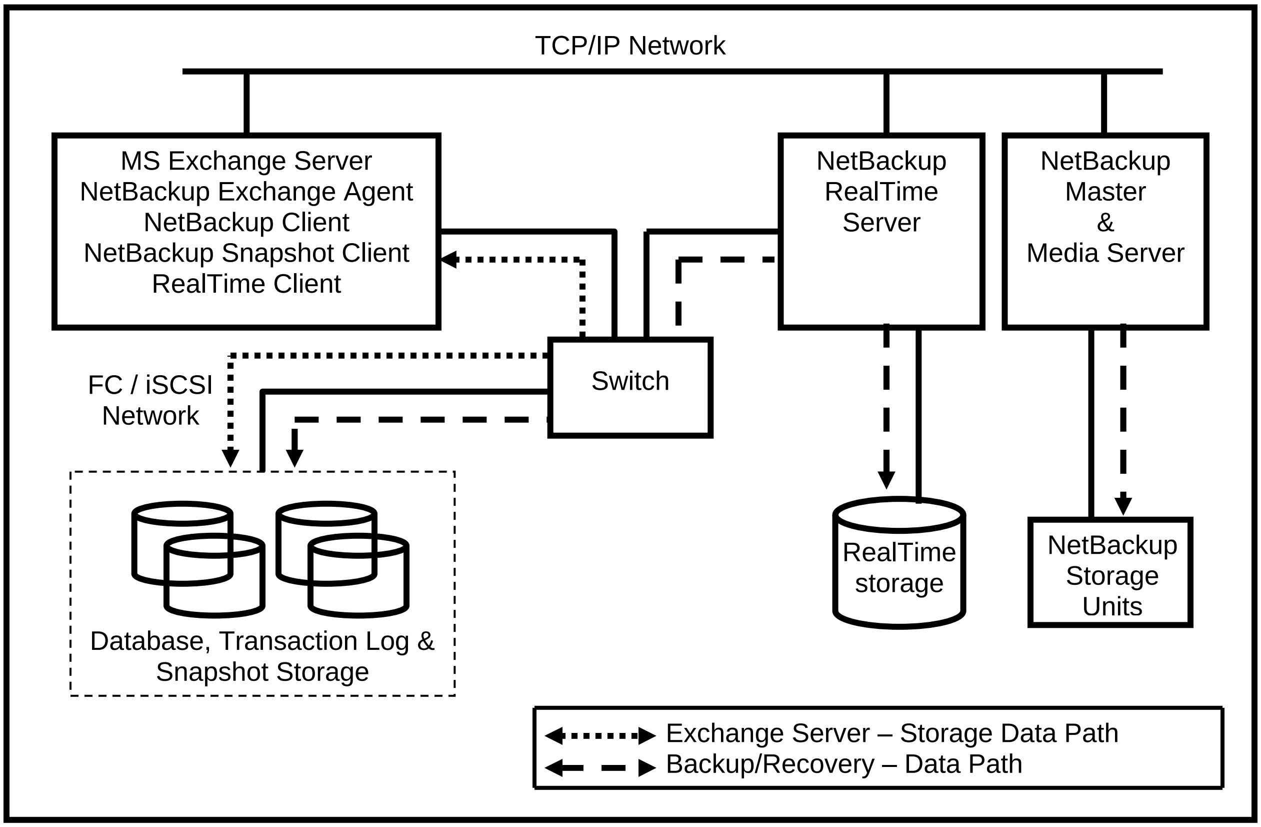
- A range of Microsoft Exchange servers that can include highly utilized servers.

- A desired recovery point objective that cannot tolerate any data loss or Microsoft Exchange server downtime.

- A need for centralized administration and reporting.

Like the “better” solution, hardware for the “best” solution includes a NetBackup master and media server platforms. Both master and media server functions can be co-located on a single host, and can even be co-located on the Microsoft Exchange server if desired. The solution also requires a dedicated machine for the RealTime Continuous Data Protection (CDP) server, as well as disk media for storage of the replicated data. The RealTime server must be on the same SAN as the Microsoft Exchange database.

Software for the “best” solution includes NetBackup enterprise server and NetBackup for Microsoft Exchange Server software. A NetBackup Enterprise Client license (which includes the Snapshot Client feature) is also required in order to use Volume Shadowcopy Service snapshots. A RealTime server license is required to enable installation of RealTime server software on the RealTime server, as well as the RealTime client software and “splitter” on the Microsoft Exchange server. Additional software licenses for tape or virtual tape libraries, enterprise disk foundation disk storage devices, or the NetBackup Vault option may also be required.


TCP/IP Network
MS Exchange Server
NetBackup Exchange Agent
NetBackup Client
NetBackup Snapshot Client
RealTime Client
NetBackup RealTime Server
NetBackup Master & Media Server
FC / iSCSI Network
Switch
Database, Transaction Log & Snapshot Storage
RealTime storage
NetBackup Storage Units
Exchange Server – Storage Data Path
Backup/Recovery – Data Path

Graphic 10: "Best" solution block diagram

NetBackup RealTime Protection uses CDP technology to deliver data protection with the best RTO and RPO possible. The RealTime client functions as a “splitter,” tapping into the I/O operations of the host to the primary disk and making a copy of every block as it is changed. Streams of changes (CDP Stream) are kept on the SAN based RealTime storage device for a predefined duration of time.

As the Microsoft Exchange server sends I/O down to its disk, the NetBackup RealTime client sends a duplicate write to the RealTime server as a CDP stream. NetBackup RealTime can then reconstruct an image or snapshot of the primary storage as it existed at any point in the recent past. With NetBackup RealTime, it is no longer necessary to keep the snapshots on the primary storage.

As part of the NetBackup platform, RealTime enables a fundamentally different method for moving data off primary storage and off-host for backups, but it retains the robust management, recovery, and application integration that NetBackup customers have relied on for years. Backup scheduling, storage lifecycle policies are all managed via the familiar NetBackup GUI or CLI exactly like a traditional NetBackup snapshot policy. In fact, NetBackup treats RealTime as a special type of snapshot, making it simple to configure a RealTime policy.

The end result is a series of snapshots that can be used for recovery from NetBackup as usual. The advantage is that the snapshots exist on secondary storage so they take up no space on the primary storage and they are already on a separate physical system protecting from failure or corruption of the primary storage.

The actual point in time for a snapshot as scheduled by NetBackup is marked by placing a marker in the CDP Stream at the same time as it catalogs an event. For example, if the CDP Stream without NetBackup Snapshot Client looks like this:

A	B	C	D	E	F						

Graphic 11: CDP data stream without RealTime

An equivalent CDP Stream with the NetBackup Snapshot Client integration looks like this:

A	B	Snap 1	C	D	Snap 2	Bkp	E	Snap 3	F		

Graphic 12: CDP data stream with RealTime

Blocks marked as letters (A,B,C, etc.) represent the changed block of data kept in historical order. Blocks named “Snap#” and “Bkp” are markers inserted by NetBackup to identify snapshots or backup events.

Because RealTime is already keeping the history of changes in its CDP Stream, it is possible to recover not only from a snapshot or a backup, but also to any time in between the marked events by requesting the data image.

With standard disk based snapshots (for example, BCVs), there is a limit of how many copies an administrator can afford to keep. Typically, administrators may keep 2–4 snapshots in addition to the daily media backup and then recycle them. A rate of four snapshots per day will leave data vulnerable for up to six hours. With RealTime, an administrator can create an infinite number of snapshots without any additional cost because each snapshot consumes no additional storage (either primary or secondary). An administrator can now afford to schedule NetBackup to perform a snapshot perhaps as frequently as every hour or more.

Just as with a standard snapshot, an image of the data can be presented to the application for immediate access after a data loss. The added benefit is that the recovery point can be chosen more granular from the timeline. In the case of data corruption, where an administrator will want to roll back to the moment before the corruption, RealTime will use the historical data to quickly restore only the changed blocks. This significantly improves restoration time. Even in the case of a database where rollback capability is built into the product, the time improvement will be significant. Instead of rolling back one change at the time, RealTime will quickly identify the image of the required block and copy over it.

RealTime enables snapshot creation on a Microsoft Exchange server by leveraging the Volume Shadowcopy Service snapshot mechanism. The RealTime client behaves like a Volume Shadowcopy Service provider. When a snapshot is requested, the RealTime client freezes the data using Volume Shadowcopy Service and places a marker in the RealTime server’s data stream. At the same time, the NetBackup server catalogs the backup in the same way it would catalog an Instant Recovery backup. A new Microsoft Exchange backup will appear in the NetBackup catalog in a few seconds or minutes, and will appear to the administrator as a conventional backup image. Optionally, the data can also be copied to a NetBackup storage unit, either disk or tape, for long-term archiving or offsite storage.

When a restore is required, the administrator can choose to recover the data in one of two ways:

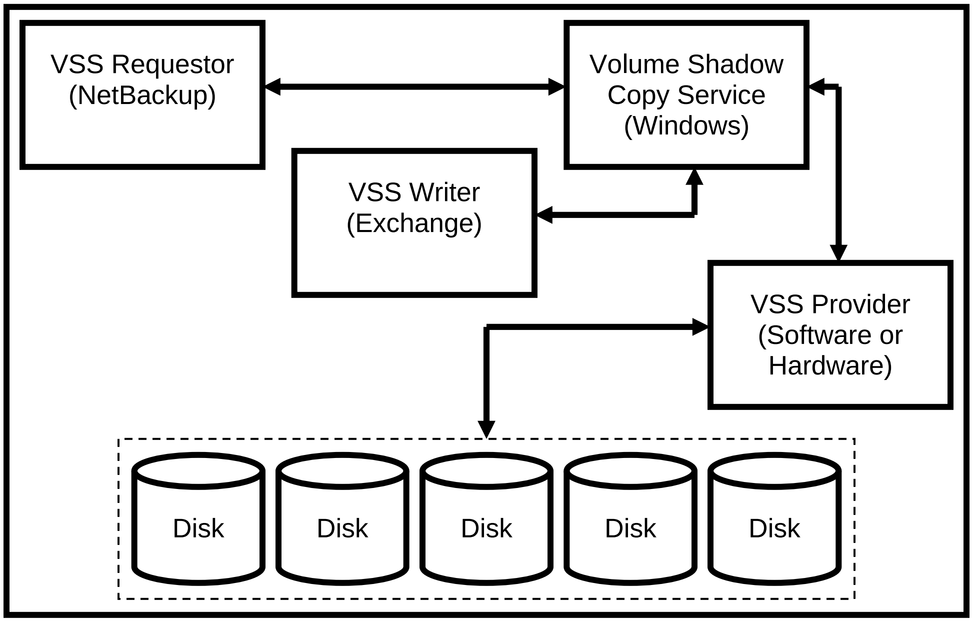
- Using snapshot for Instant Recovery—In this case the snapshot replaces the primary set of disks and makes data immediately available to the Microsoft Exchange server. Data is restored to the time when the snapshot has been taken. At this point, Microsoft Exchange logs can be applied to meet the RPO. This assumes that Microsoft Exchange logs survived the disaster. This method provides very good RPO but RTO depends on how long it will take to replay the Microsoft Exchange logs. This is where RealTime can help by allowing more frequent snapshots, thereby significantly decreasing the recovery time.
- Using an existing snapshot for full or granular data restoration—Full restore will involve re-creating the whole Microsoft Exchange server, while granular restore allows choosing individual mailboxes and messages (in 6.5.4). In both cases, the snapshot is mounted to the NetBackup client and data is copied to the primary disk. This method will restore the Microsoft Exchange server to the time of when the snapshot has been taken. If available, Microsoft Exchange logs can be applied to roll the Microsoft Exchange server forward. As with the previous method, RealTime will allow for more frequent backups and significantly reduce the recovery time. This method can also be used from the tape after a snapshot has expired. By default Snapshot Client will choose to recover from the snapshot; only after the snapshot has expired will it use the tape backup.

Using the RealTime GUI, it is possible to recover to any point in time. For more information, refer to the *Veritas NetBackup RealTime Protection Administrator's Guide*. These methods can be applied in the case of a disaster as well as in the case of data corruption. For corruption, Microsoft Exchange rollback will likely be faster than restoring from the backup.

RealTime retains information for a limited time, subject to disk space constraints, and RealTime data cannot be taken off-site. For full data protection, a NetBackup policy should be created to periodically perform a conventional backup that can be archived or duplicated to other media.

Appendix A: Volume Shadowcopy Service Overview

Volume Shadowcopy Service is a set of APIs that creates a foundation to allow backups to be performed on online volumes. Volume Shadowcopy Service components include requestors, writers, and providers. The example block diagram below puts these components in perspective:


VSS Requestor (NetBackup)
Volume Shadow Copy Service (Windows)
VSS Writer (Exchange)
VSS Provider (Software or Hardware)
Disk
Disk
Disk
Disk
Disk

Graphic 13: Volume Shadowcopy Service block diagram

In the case of a Microsoft Exchange Volume Shadowcopy Service-enabled backup, NetBackup is the Volume Shadowcopy Service requestor, the component that initiates the backup process. A Volume Shadowcopy Service writer specific to and included with Microsoft Exchange prepares databases for backup. The Volume Shadowcopy Service provider creates snapshots as directed by the Volume Shadowcopy Service requestor. A variety of Volume Shadowcopy Service providers are available and supported for use with NetBackup and Microsoft Exchange.

Volume Shadowcopy Service providers fall into two general categories in that they are typically referred to as software- or hardware-based. An example of a software-based Volume Shadowcopy Service provider would be Veritas™ Foundation Suite for Windows. NetBackup RealTime also functions as a software Volume Shadowcopy Service provider. Hardwarebased Volume Shadowcopy Service providers are based on intelligent storage devices, typically a disk array, capable of providing a Volume Shadowcopy Service compliant snapshot. Typically, you must install supporting software for hardware Volume Shadowcopy Service providers on the client machine.

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 website. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek
Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

02/09 20016957