Exchange 2013 Data Protection with EqualLogic Auto-Snapshot Manager/Microsoft Edition 4.6 and PS Series Arrays

Protect Microsoft Exchange Server 2013 with online Smart Copies and recovery operations

Dell Storage Engineering

September 2013

A Dell Deployment and Configuration Guide

Revisions

The following table describes the release history of this Technical Report.

Report	Date	Document Revision
1.0	July 2010	Initial Release
2.0	December 2011	New Auto-Snapshot Manager UI
3.0	December 2012	New Auto-Snapshot Manager 4.5 Release
4.0	September 2013	New Auto-Snapshot Manager 4.6 Release

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Table of contents

Acknowledgements

Authored by: Daniel J. Curran

WWW.DELL.COM/PSseries

Preface

Dell EqualLogic™ PS Series arrays optimize resources by automating performance and network load balancing. Additionally, PS Series arrays offer all-inclusive array management software, host software, and free firmware updates.

Audience

The information in this guide is intended for administrators that have deployed Microsoft® Exchange Server® 2013 and are interested in using EqualLogic snapshots for efficient protection and recovery of Exchange server 2013.

Software information

The following table shows the software and firmware used for the preparation of this paper.

Vendor	Model	Software Revision
Microsoft®	Windows Server 2012	RTM
Microsoft®	Exchange Server 2013	RTM, CU2 (build 15.0.712.24)
Dell	PS Series Array Firmware	Version 6.0.2 and later*
Dell	Host Integration Tools – Auto-Snapshot Manager	Version 4.6 and later*

* For earlier version support see the Host Integration Tools release notes.

1 Introduction

Database protection and disaster recovery are among the top concerns for Exchange Server administrators. Requirements for reducing database backup windows and restore times continue as demands for continuous Exchange Server uptime is increasing. PS Series arrays provide administrators the ability to create volume based copies of data using snapshots, clones and replicas. These copies are known as “point-in-time” copies of volume data.

The EqualLogic Host Integration Tools (Hit Kit) Version 4.6 enhances Auto-Snapshot Manager / Microsoft Edition (ASM/ME) – adding the ability to create data and application-consistent Smart Copies of Exchange Server Databases. Auto-Snapshot Manager / Microsoft Edition is a Windows server application offering application-consistent Smart Copies of Exchange Server Databases leveraging the built-in snapshot, clone and replication facilities in PS Series arrays. With ASM/ME an Exchange Server administrator can:

- Create copies of Exchange databases, where the copy operation is coordinated with Exchange Server operations.
  - Use the management GUI or built-in scheduler to create Smart Copy sets
  - Use the command-line interface (asmcli) that enables you to perform many common tasks. GUI wizards are included to generate fully-formed command lines.
  - Set up automatic e-mail notification of events
- Allow system or Exchange administrators to perform Exchange restore operations in the following ways:
  - In-place point-in-time Database recovery (Restore All)
  - Support for doing “brick/item-level” restores using Microsoft® Exchange Recovery Mailbox Database (RDB).
  - Clone and Restore All as New feature allows you to clone a mailbox database from a source Exchange server, and then set it up as a new mailbox database on a target Exchange server.

The capabilities of ASM/ME extend the use of SAN copy facilities beyond storage administrators, to server and Exchange administrators. This raises the productivity of Exchange administrators, and allows them to leverage efficient SAN copy facilities without requiring SAN privileges. By automating data protection and recovery operations, the headaches and time-consuming day-to-day operations of managing and maintaining volume and Exchange Server uptime is minimized and data availability is increased extensively. Data availability can be maintained at a higher level of assurance using Auto-Snapshot Manager / Microsoft Edition and Smart Copy technologies with PS Series arrays.

2 ASM / ME – Exchange Server integration

Auto-Snapshot Manager/Microsoft Edition utilizes Microsoft's Volume Shadow Copy Service (VSS) architecture to provide application integration with SAN copy operations, Figure 1. During the VSS operation flow, Auto-Snapshot Manager initiates the process by requesting the Exchange Server VSS Writer to prepare a database for a Smart Copy operation. The Exchange Server VSS Writer component places the database in a consistent state and the PS Series VSS Provider service initiates the SAN copies using PS Series hardware snapshots, clones, or replication functions. The end result is a data-consistent point-in-time Smart Copy of the Exchange Server database and volumes. Smart Copies can then be used to fully restore a database or simply recover object level data using various recovery options available to the Smart Copy set.

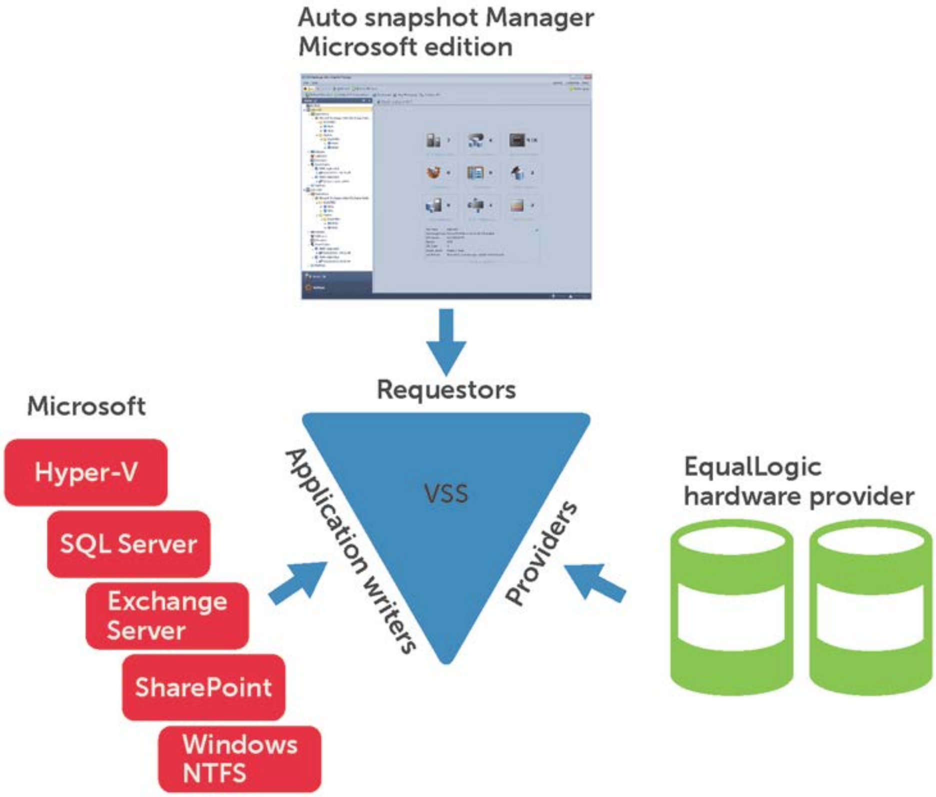


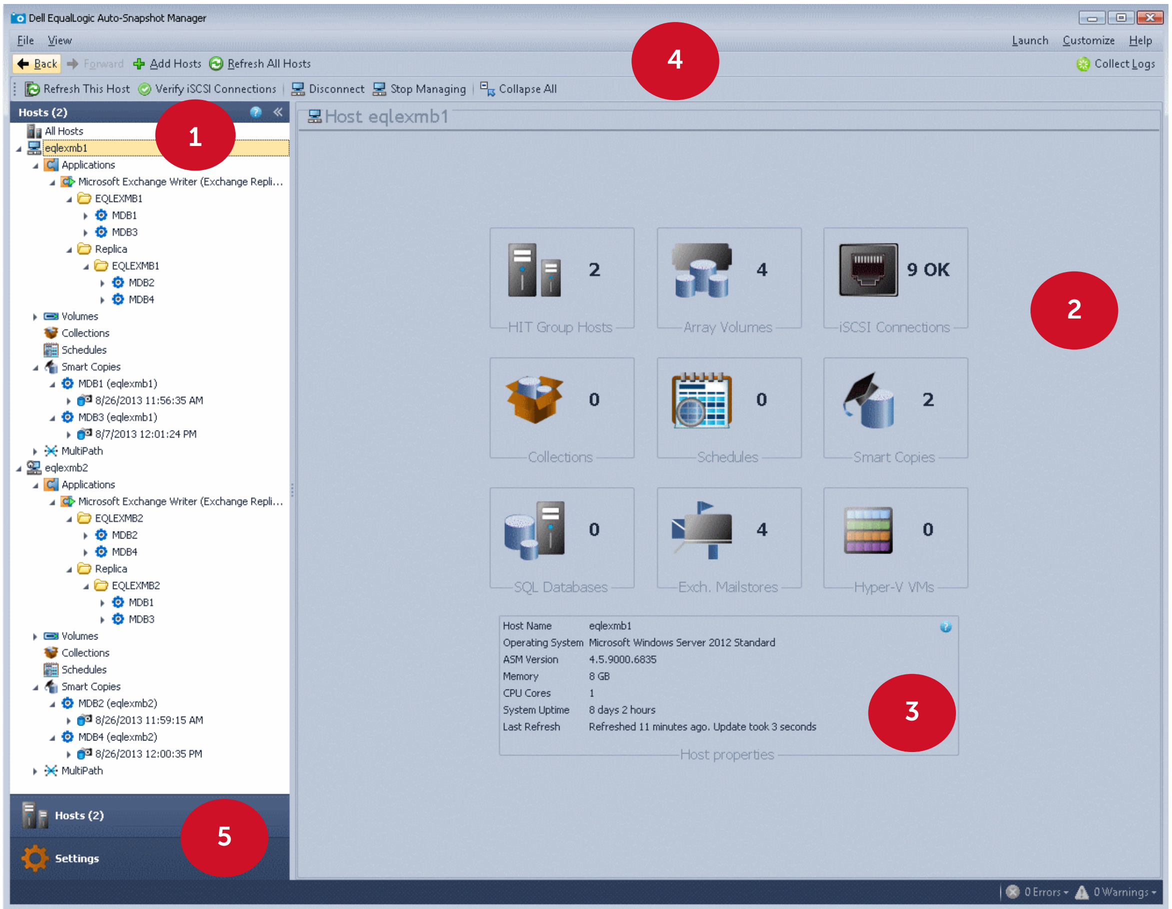
Figure 1 Volume Shadow Copy service – ASM/ME integration

The ASM/ME GUI has been redesigned in Host Integration Tools for Windows version 4.6, Figure 2. The Hosts area (1) shows the hosts that have been added to the managed HIT Group. A HIT Group is simply a group of hosts managed by that instance of ASM/ME. Each host lists supported component information including Exchange Server instances and databases, host volumes, collections, schedules, and existing Smart Copies.

The main area in the center (2 and 3) lists detailed information about the selected object, such as host information and properties, Smart Copy support options available for the selected object, volume and file information including snapshot reserve and in-use statistics, collection and schedule information, and individual Smart Copy information.

The bar (4) above the center and hosts view will list actions available for a selected object. Actions include operations including host management, schedule creation, Smart Copy creation, restore options for a Smart Copy, etc.

Users can configure property-level attributes such as the location of the Smart Copy backup documents, the CHAP authentication used to communicate with the PS Series Group, default Smart Copy settings, and alert information by choosing the Settings option (5).



Host Name	eqlexmb1
Operating System	Microsoft Windows Server 2012 Standard
ASM Version	4.5.9000.6835
Memory	8 GB
CPU Cores	1
System Uptime	8 days 2 hours
Last Refresh	Refreshed 11 minutes ago. Update took 3 seconds

Figure 2 ASM/ME user interface

3 Overview of HIT groups

A HIT Group is a group of one or more hosts that you are managing from ASM/ME. HIT Groups are useful because they allow you to manage multiple hosts from any machine that is running ASM/ME. For example, if an administrator has to manage and backup Microsoft Exchange mailbox databases residing on multiple servers, they can create a HIT Group on a single instance of ASM/ME and manage multiple servers from there.

HIT Groups allow you to create and manage Smart Copies and Smart Copy schedules on all your hosts, and simultaneously edit settings on multiple hosts. When a new host is added to a HIT Group, the Host Integration Tools get installed on the host. If you've already created a HIT Group, ASM/ME will display a message if any of the hosts are not running a version of Host Integration Tools greater than or equal to the version running on the local host. You can then use the Add Hosts wizard to remotely upgrade the Host Integration Tools on the other hosts.

4 HIT groups in non-DAG environments

In non-DAG environments, HIT Groups are host-specific. That is, adding host B to the ASM/ME instance on host A does not automatically add host A to the ASM/ME instance on host B. A HIT Group can also consist of one host. Adding multiple hosts to manage is optional; you can also just run ASM/ME from a single host and manage that local host.

5 HIT groups in DAG environments

In DAG environments, all DAG nodes in a HIT Group have a reciprocal relationship. That is, adding DAG node B to the ASM/ME instance on DAG node A will automatically add DAG node A to the ASM/ME instance on DAG node B. You must always add an entire DAG to a HIT Group as opposed to a subset of DAG nodes. ASM/ME will then automatically set up the trust relationship between each DAG node. If you only add a subset of DAG nodes to a HIT Group, then data restoration, schedule, and Smart Copy operations could result in fatal errors. If you run ASM/ME from a DAG node, ASM/ME will warn you if you haven't created a HIT Group that includes all the other DAG nodes.

For more information on Dell EqualLogic Host Integration Tools for Microsoft, please refer to the *Dell EqualLogic Host Integration Tools/Microsoft Edition - Installation and User's Guide – Version 4.6* and the *Dell EqualLogic Host Integration Tools for Microsoft Windows® – Release Notes – Version 4.6* on the Dell EqualLogic Customer Support site at https://support.Dell.com/EqualLogic.

5.1 Smart Copy options and backup types

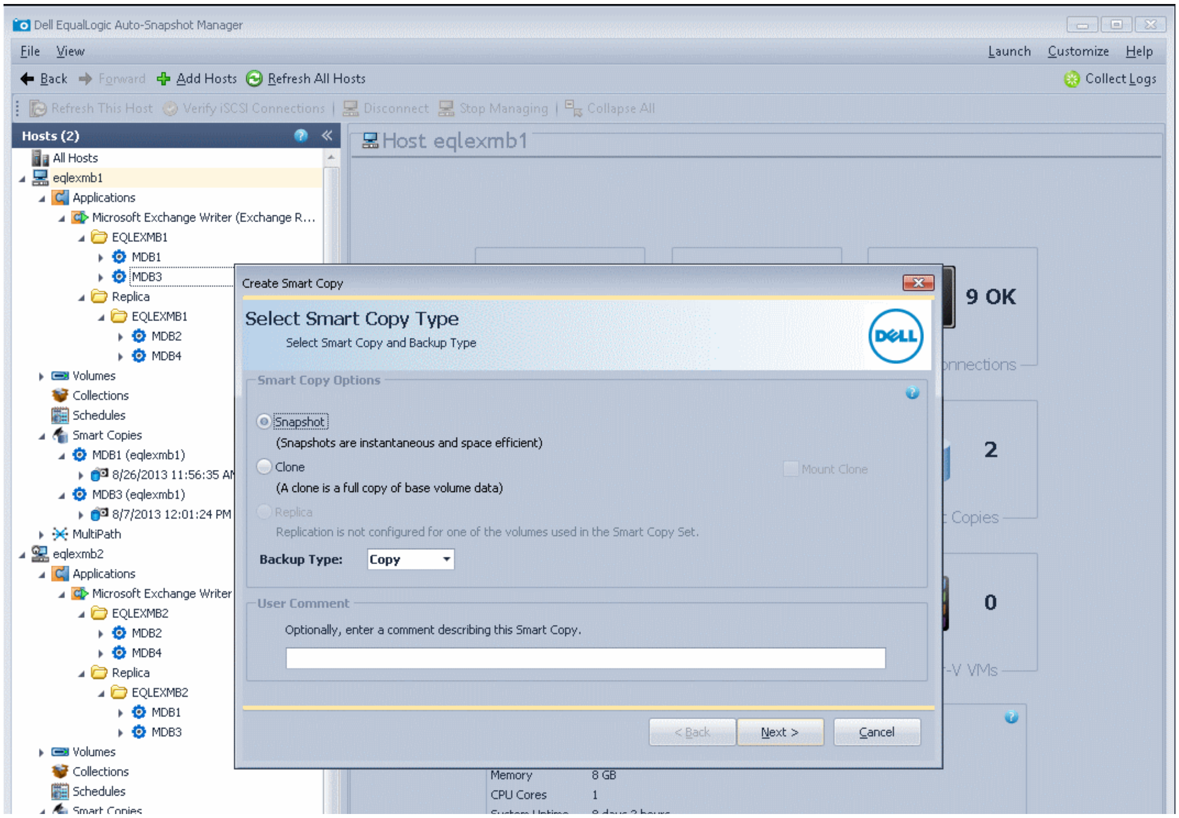
Auto-Snapshot Manager / Microsoft Edition (ASM/ME) creates Smart Copy snapshots, clones, and replicas (see Figure 3). These Smart Copies leverage the built-in PS Series SAN copy facilities.

All Smart Copies are transportable, and can be mounted on the same or a different server. All servers on the SAN with ASM/ME installed and access to the Smart Copy backup documents can mount (restore) a Smart Copy.

5.2 Smart Copy behavior with Exchange Server

With all Smart Copy types there is only one backup type (Figure 3) for use with Exchange. The following backup type is available with Auto-Snapshot Manager GUI:

- Copy – This backup type creates a copy of the Exchange Server Database with associate logs, and specifies an out-of-band backup operation that has no effect on application log files or backup operations.
- For more information on Exchange Server recovery models see Exchange Server TechCenter document: Exchange Server Disaster Recovery: Disaster Recovery.



Create Smart Copy

Select Smart Copy Type

Select Smart Copy and Backup Type

Smart Copy Options

● Snapshot

(Snapshots are instantaneous and space efficient)

○ Clone □ Mount Clone

(A clone is a full copy of base volume data)

○ Replica

Replication is not configured for one of the volumes used in the Smart Copy Set.

Backup Type: Copy

User Comment

Optionally, enter a comment describing this Smart Copy.

< Back | Next > | Cancel

Figure 3 Smart Copy behavior options

5.3 Snapshot Smart Copy

Snapshot Smart Copies are point-in-time copies of Exchange Database and log files at the time of the Smart Copy operation. Snapshots are the most space-efficient form of a Database Smart Copy and therefore multiple copies of snapshots can be stored and used for restore operations. In the PS Series Group Manager GUI, snapshot Smart Copies are shown under each base volume from which they were created. Snapshot Smart Copies are most useful as point in-time copies of the original Database.

Using ASM/ME, Smart Copy snapshots can be created and applied to restore the original Database, restore the snapshot Smart Copy to an Exchange Recovery Mailbox Database allowing Brick / Item level restores.

5.4 Clone Smart Copy

Clone Smart Copies are exact duplicates of the original volume including all the data on the volume and the full size of the volume. Clones are treated and shown as separate volumes in the PS Series Group Manager GUI. Clone Smart Copies are most useful to recreate the original Database environment such as test or development scenarios.

With ASM/ME, smart copy clones can be used for restoring to an Exchange Recovery Mailbox Database allowing Brick / Item level restores, or create exact copies of Database environments for testing and development scenarios.

5.5 Replica Smart Copy

Replicas can be used to offload Smart Copy storage as well as checksum and soft recovery operations to the remote site.

Note: Replicas cannot be used to restore the original volume (Restore All).

Replica Smart Copy options are available if replication is configured in the PS Series group for the volume or volumes that make up an Exchange Server Database(s). Replicas are point in time copies that are sent from a primary site and stored on a replication partner. The first replication process will always be a complete copy of the base volume. Subsequent replication operations will only send the changes since the last replication operation. When using replica Smart Copies it is important to manage ASM/ME's backup documents so that they can be used to recover replicas.

To replicate many Databases and volumes, make sure to configure sufficient replication space. For more information on PS Series replication and sizing replication space, see the Dell EqualLogic Technical Report, *Understanding Data Replication Between Dell EqualLogic PS Series Groups*, at the following URL: http://en.community.dell.com/dell-groups/dtcmedia/m/mediagallery/19861448/download.aspx.

5.6 Smart Copy Schedules

You can create schedules to create Smart Copy sets at various intervals (Figure 4). The ASM/ME scheduler is based on the Microsoft Windows schedule service and supports Smart Copy schedule period as often as 5 minutes apart. ASM/ME also supports a "keep count" parameter that retains only the specified number of active Smart Copies for an object. This ensures that storage resources are maintained while data recovery remains highly available. You can create schedules by right-clicking an object or using the Actions pane of ASM/ME. See Appendix B – Command Line Options for instructions on creating schedules in a script.

Note: ASM/ME and Windows scheduling service can process only one scheduled task at a time. A scheduled Smart Copy operation may fail if there is another Smart Copy process occurring at the same time on a server system.

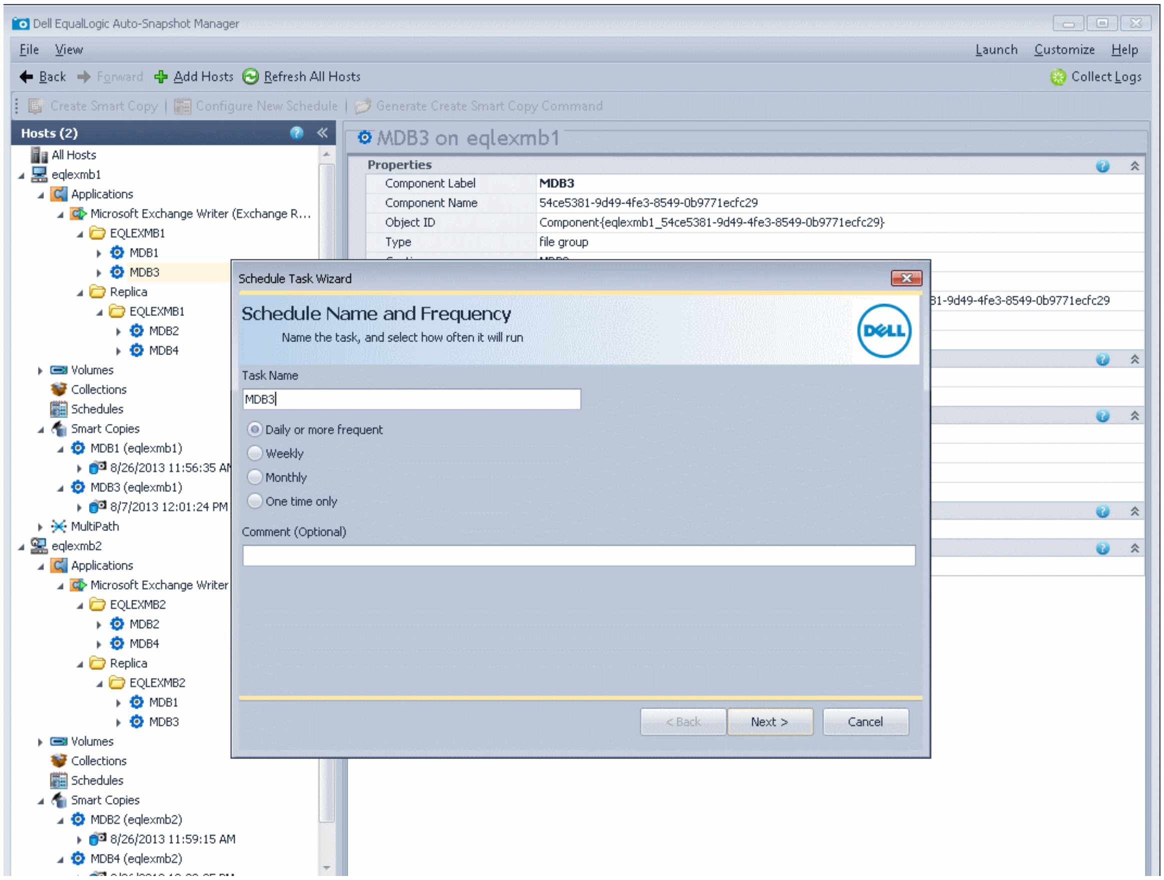
6 Setup and Configuration Best Practices

This section details some best practices for using Auto-Snapshot Manager with PS Series groups and Exchange Server.

6.1 Database File Layout

To create Exchange Server Database Smart Copies with ASM/ME, all of the Database files must reside on PS Series storage so that ASM/ME recognizes all the underlying volumes that make up the Database object.

PS Series groups create volume-based data copies. All the volume data will be protected during a Smart Copy operation. By default, ASM/ME creates an application-consistent Smart Copy of the object or Exchange Database chosen. If more than one Exchange Database shares the same volume, it could result in a" torn" Smart Copy set. To avoid torn Smart Copies and selective restore scenarios, Dell recommends placing Exchange Server Database files on their own PS Series volumes. This allows for much faster restore times by taking advantage of the PS Series snapshot restore technologies.



Properties	
Component Label	**MDB3**
Component Name	54ce5381-9d49-4fe3-8549-0b9771ecfc29
Object ID	Component{eqlexmb1_54ce5381-9d49-4fe3-8549-0b9771ecfc29}
Type	file group

Schedule Name and Frequency

Name the task, and select how often it will run

Task Name: MDB3

● Daily or more frequent
○ Weekly
○ Monthly
○ One time only

Comment (Optional):

Figure 4 Create Smart Copy schedules

6.2 Storage resource management

This section describes how ASM/ME and Smart Copies use storage resources and suggests some best practices for monitoring and managing space used by Smart Copy sets on the PS Series group.

- Snapshot Smart Copies use the snapshot reserve space allocated to the volume. You can monitor and change the snapshot reserve value for each volume that makes up an Exchange Server Database.

When a snapshot smart copy is restored as a Recovery Mailbox Database, the snapshot continues to exist, and continues to use the snapshot reserve for the volumes that make up the Smart Copy.

Best Practice: Maintain “keep counts” for Snapshot Smart Copy schedules to minimize overuse of snapshot reserve. Recovery Mailbox Database restore of Snapshot Smart Copies are best used as temporary copies of Databases and cleaned up as soon as the data is restored and confirmed.

- Clone Smart Copies use the same amount of storage as the original volume or volumes. When you create a clone Smart Copy, a new volume appears in the Group Manager GUI with the date and timestamp of the Smart Copy operation. Clone Smart Copies can be brought online through ASM/ME by using the Mount option. We recommend that you mount your volumes read-only if you don’t need to make any changes to the data contained in the Smart Copy. If you mount the volumes read-write and make changes to your data, you will lose the ‘point in time’ nature of the Smart Copy.

Best Practice: Clone Smart Copies are complete copies of Exchange Database objects and should be cleaned up after use to avoid storage resource consumption.

- Replica Smart Copies are created if replication is configured for a volume or volumes that make up Exchange Server Databases. Replication requires a replication partner to store the replica set, and must be set up on the PS Series group. The first replication always replicates the total volume data for an Exchange Server Database or PS Series volume. Each subsequent replication operation only replicates the data that changed for the volume or volumes since the last replication operation. You can monitor and increase the replication reserve through the PS Group Manager GUI at any time.

Additionally, the Mount as Read-only Smart Copy option halts all replication activity on that Smart Copy replica set until the replica is un-mounted and demoted. See “Restoring Exchange Server Databases with Smart Copies” in this document for more information.

- The time it takes to replicate data can vary due to the amount of data being replicated and the bandwidth of the network between the partner groups. For more information on replication see the PS Series Technical Documents at: http://www.equallogic.com/resourcecenter/documentcenter.aspx

Best Practices: Size replication space and network bandwidth according to your network needs. Only use the Mount as Read-only option for temporary use and be sure to un-mount and demote when finished to continue replication on that Smart Copy Set.

7 Creating Exchange Server database Smart Copies

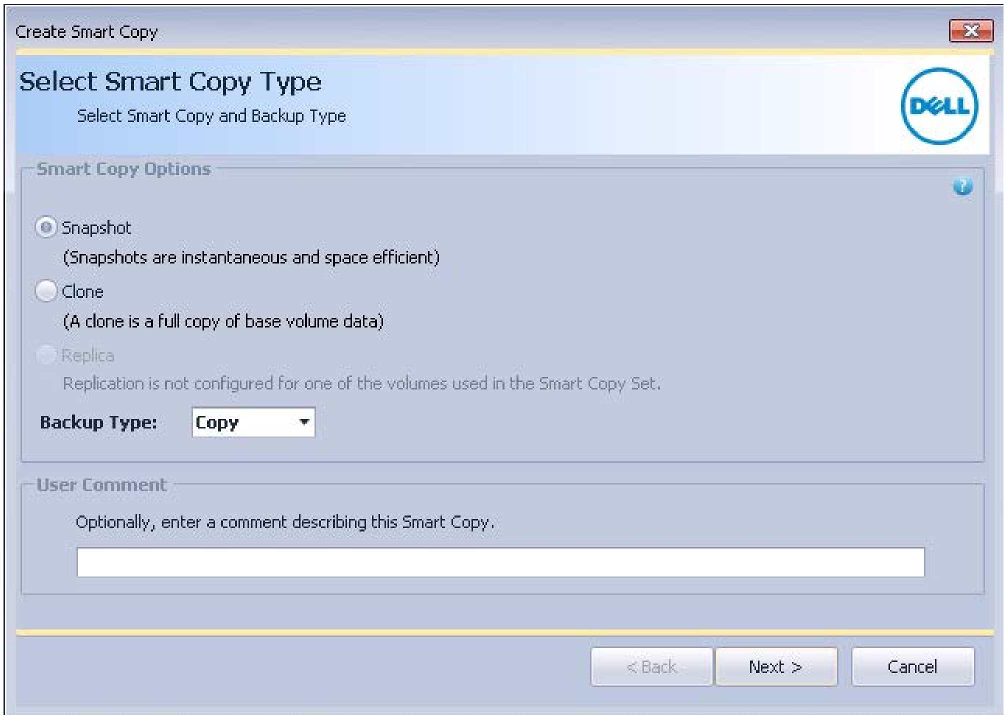
Your business needs will determine the type of Smart Copy to create using ASM/ME.

- If the objective is fast recovery of Exchange Server Databases, use snapshot Smart Copies because they consume minimal storage resources and can be used to quickly roll back the original database volumes for a complete recovery strategy.
- If the objective is to create a copy of an Exchange Server Database for longer duration use clone Smart Copies because volume clones do not consume snapshot reserve and are treated as normal volumes in the PS Series group.

If there is a remote array available and you want to store the latest version of Exchange Server Database information, use replica Smart Copies.

7.1 Steps to create Smart Copy sets

All Smart Copies can be created using the same wizard (Figure 5) either by right-clicking an object or using the Actions pane. The wizard will display options allowed by the object based on what type of Smart Copy operation is supported (snapshot, clone, or replica).



Create Smart Copy

Select Smart Copy Type

Select Smart Copy and Backup Type

Smart Copy Options

● Snapshot
(Snapshots are instantaneous and space efficient)

○ Clone
(A clone is a full copy of base volume data)

○ Replica
Replication is not configured for one of the volumes used in the Smart Copy Set.

Backup Type: Copy

User Comment

Optionally, enter a comment describing this Smart Copy.

Figure 5 Create Smart Copy window

1. Unless you have a database availability group (DAG) that has two or more copies the recommended configuration is to keep Database files on their own volumes separate from logs, see: Understanding Exchange LUN Architecture. Choose the Smart Copy type and the behavior based on the planned usage of the Smart Copy (Database restore, Recovery Mailbox Database, or another use).

Note: ASM/ME does not support torn Smart Copies. If any components of other Exchange Databases are included in the smart copy set, ASM/ME displays an error dialog. Torn Smart Copies mean that there were additional object components (Database files) on the volume you selected for the Smart Copy. For more information see "Restoring Exchange Server Databases with Smart Copies".

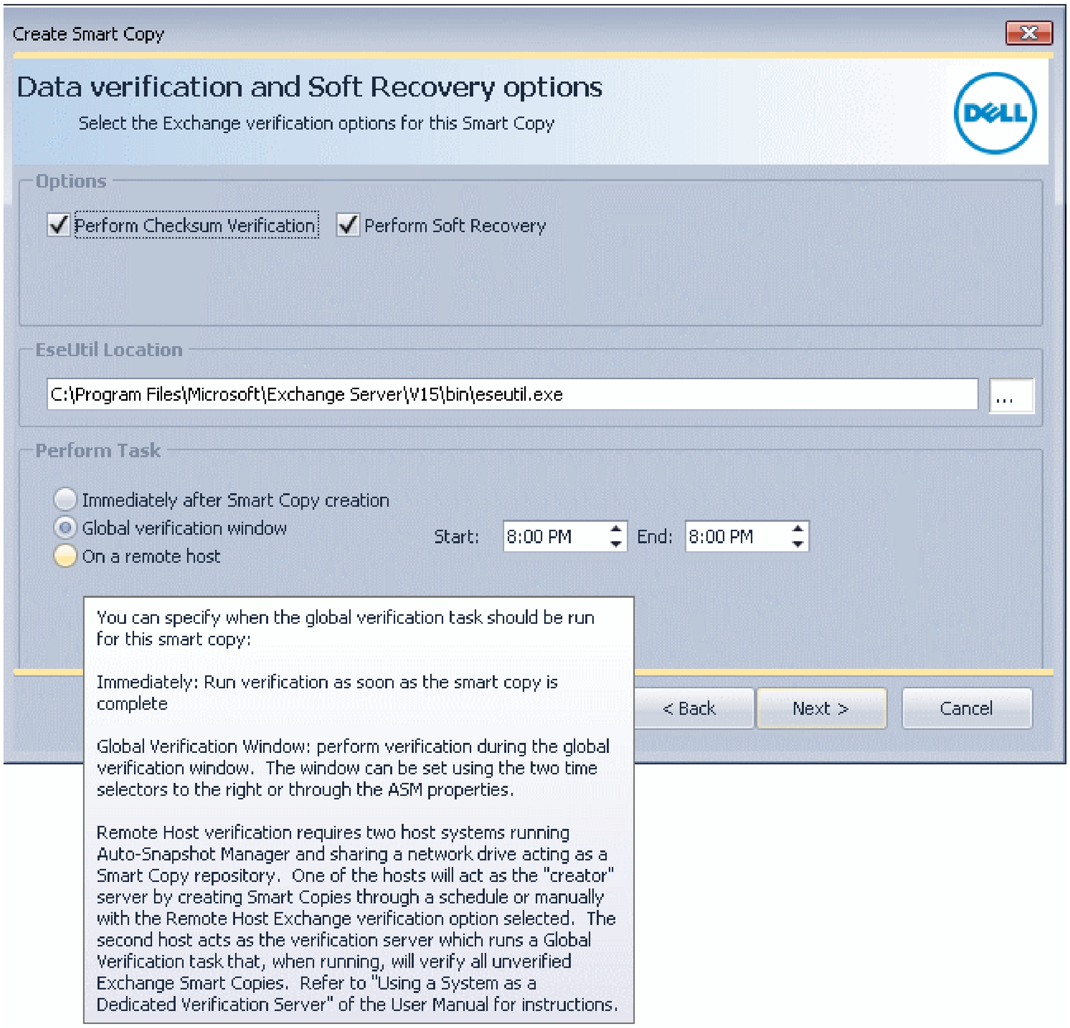
Optionally, create a schedule to create Exchange Server Database Smart Copies. By choosing the Configure New Schedule option from the Actions pane you can give the new schedule a name and add options to configure a repeating Smart Copy schedule. If Notification is not set up, the schedule service will ask you to configure notification prior to creating the schedule. You can decline, and continue with the Smart Copy schedule. Similar to creating a single Smart Copy, if there are additional Database object components on the volume you choose, the Torn Smart Copy Warning is displayed. To continue with the schedule creation, choose next to move to the next screen.

2. Setup Schedule settings (Figure 4). Schedule Name and Frequency, Daily Schedule Settings plus Advanced (Not Shown)
   ASM/ME displays the Data Verification and Soft Recovery Options dialog. (Figure 6) You have the option to configure and schedule Checksum Verification and Soft Recovery on the new Smart Copy:

- **Checksum Verification -** Verifies the integrity of databases in the Smart Copy by using the **eseutil.exe** database maintenance utility. For Microsoft Exchange Database replicas only, the option to perform immediate Checksum Verification is not available immediately after making a Smart Copy.
- **Soft Recovery** - Brings all databases to a clean shutdown. For Microsoft Exchange Database replicas immediate Soft recovery is not available.
- **Perform Task**. Specify the time and method of running Checksum Verification and Soft Recovery. You can chose the following options:
- **Immediately after Smart Copy creation**
  Specify this option to start Checksum Verification and Soft Recovery as soon as Smart Copy creation is complete. This option is not available for Microsoft® Exchange Database replicas.
- **Global verification window.**
  Specify this option to use the Global Verification Window times that you configured into ASM/ME in Setting up the Global Verification Window. You can also use this option to change the Global Verification times. You must specify a minimum period of three hours. If you change the Global Verification times, the changes apply to the local host only, and affect all other scheduled verifications.

- **On a Remote host preconfigured to perform Exchange verification.**
  Specify this option to schedule Global Verification on a remote host. The remote host must be configured to run the operation. See: Appendix D – Remote Host Verification Setup

Note: if you need to change the remote Global Verification window, you must change it on the remote host.



Create Smart Copy

Data verification and Soft Recovery options

Select the Exchange verification options for this Smart Copy

Options

☑ Perform Checksum Verification ☑ Perform Soft Recovery

EseUtil Location

C:\Program Files\Microsoft\Exchange Server\V15\bin\eseutil.exe

Perform Task

○ Immediately after Smart Copy creation
● Global verification window — Start: 8:00 PM End: 8:00 PM
○ On a remote host

You can specify when the global verification task should be run for this smart copy:

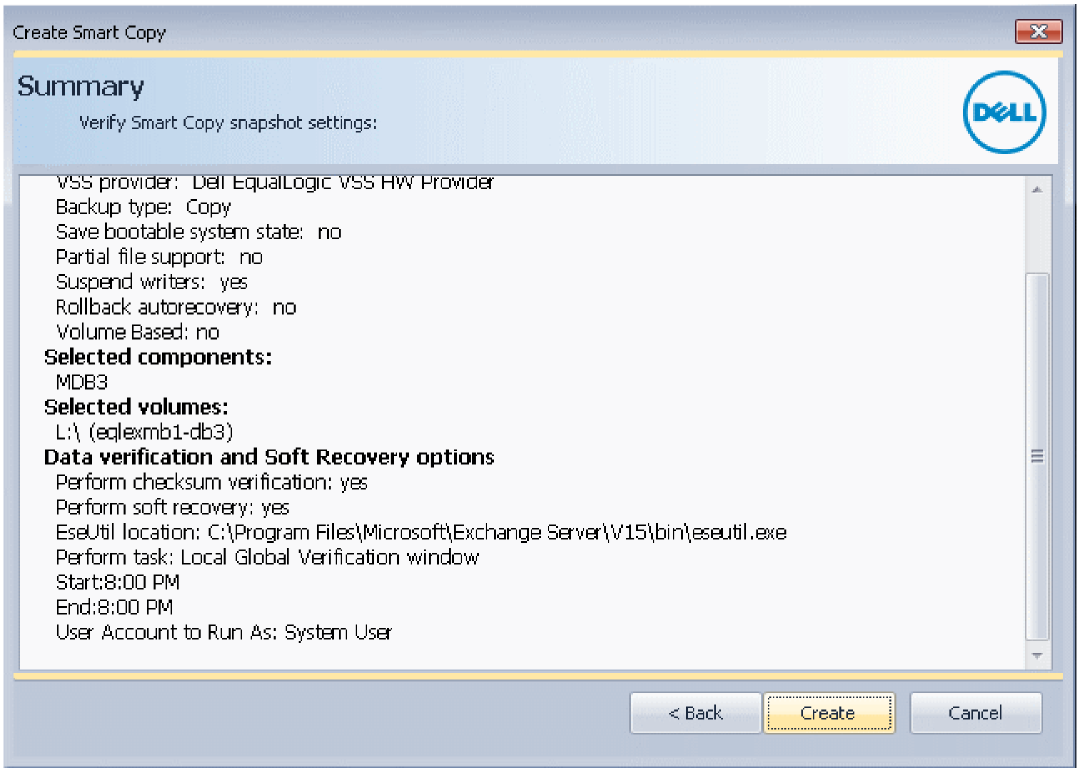
Immediately: Run verification as soon as the smart copy is complete

Global Verification Window: perform verification during the global verification window. The window can be set using the two time selectors to the right or through the ASM properties.

Remote Host verification requires two host systems running Auto-Snapshot Manager and sharing a network drive acting as a Smart Copy repository. One of the hosts will act as the "creator" server by creating Smart Copies through a schedule or manually with the Remote Host Exchange verification option selected. The second host acts as the verification server which runs a Global Verification task that, when running, will verify all unverified Exchange Smart Copies. Refer to "Using a System as a Dedicated Verification Server" of the User Manual for instructions.

Figure 6 Data verification and Soft Recovery options

3. Click **Next** and verify the settings displayed in the Summary screen. (Figure 7)
4. If the information is correct, click **Create**. If not, click **Back** and make any changes.

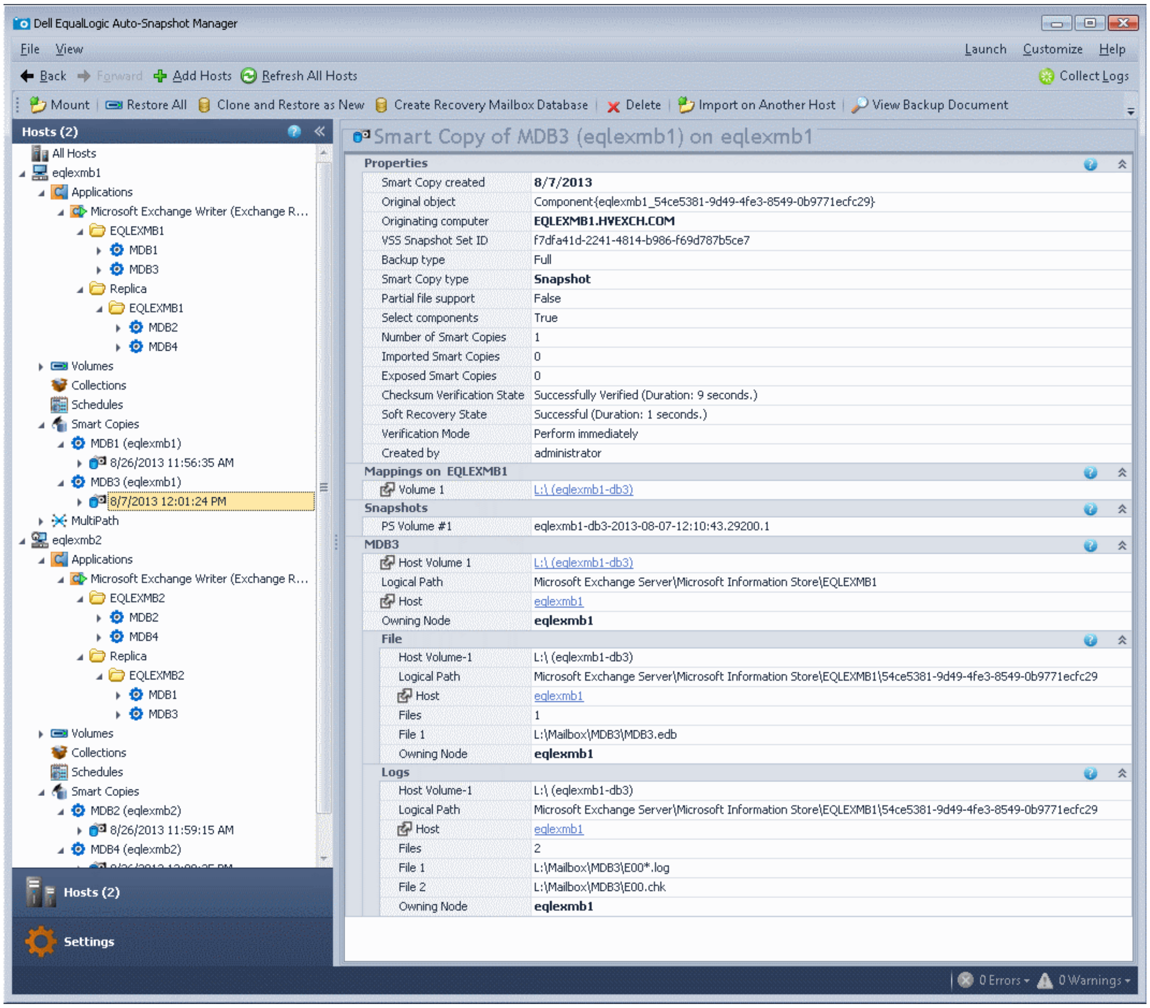


VSS provider: Dell EqualLogic VSS HW Provider
Backup type: Copy
Save bootable system state: no
Partial file support: no
Suspend writers: yes
Rollback autorecovery: no
Volume Based: no
Selected components:
MDB3
Selected volumes:
L:\ (eqlexmb1-db3)
Data verification and Soft Recovery options
Perform checksum verification: yes
Perform soft recovery: yes
EseUtil location: C:\Program Files\Microsoft\Exchange Server\V15\bin\eseutil.exe
Perform task: Local Global Verification window
Start:8:00 PM
End:8:00 PM
User Account to Run As: System User

Figure 7 Summary screen

7.2 Displaying Smart Copies

To display information about the Smart Copy set, select Smart Copies. The ASM/ME Smart Copies window appears (Figure 8)



Smart Copy of MDB3 (eqlexmb1) on eqlexmb1

Properties	
Smart Copy created	**8/7/2013**
Original object	Component{eqlexmb1_54ce5381-9d49-4fe3-8549-0b9771ecfc29}
Originating computer	**EQLEXMB1.HVEXCH.COM**
VSS Snapshot Set ID	f7dfa41d-2241-4814-b986-f69d787b5ce7
Backup type	Full
Smart Copy type	**Snapshot**
Partial file support	False
Select components	True
Number of Smart Copies	1
Imported Smart Copies	0
Exposed Smart Copies	0
Checksum Verification State	Successfully Verified (Duration: 9 seconds.)
Soft Recovery State	Successful (Duration: 1 seconds.)
Verification Mode	Perform immediately
Created by	administrator
Mappings on EQLEXMB1	
Volume 1	L:\ (eqlexmb1-db3)
Snapshots	
PS Volume #1	eqlexmb1-db3-2013-08-07-12:10:43.29200.1
MDB3	
Host Volume 1	L:\ (eqlexmb1-db3)
Logical Path	Microsoft Exchange Server\Microsoft Information Store\EQLEXMB1
Host	eqlexmb1
Owning Node	**eqlexmb1**
File	
Host Volume-1	L:\ (eqlexmb1-db3)
Logical Path	Microsoft Exchange Server\Microsoft Information Store\EQLEXMB1\54ce5381-9d49-4fe3-8549-0b9771ecfc29
Host	eqlexmb1
Files	1
File 1	L:\Mailbox\MDB3\MDB3.edb
Owning Node	**eqlexmb1**
Logs	
Host Volume-1	L:\ (eqlexmb1-db3)
Logical Path	Microsoft Exchange Server\Microsoft Information Store\EQLEXMB1\54ce5381-9d49-4fe3-8549-0b9771ecfc29
Host	eqlexmb1
Files	2
File 1	L:\Mailbox\MDB3\E00*.log
File 2	L:\Mailbox\MDB3\E00.chk
Owning Node	**eqlexmb1**

Figure 8 ASM Smart Copies window

8 Restoring Exchange Server databases with Smart Copies

There are various methods to restore and recover Exchange Server Databases using Smart Copies. The underlying PS Series architecture can either restore a volume from a Smart Copy (Restore All) or mount a Smart Copy online to a host as a new volume (Create Recovery Mailbox Database). Both of these operations have many different Exchange Server Database restore possibilities.

This section (Table 1) describes the most common restore scenarios and how to apply Smart Copy restore options for Exchange Server data recovery.

Table 1 Restore options for Smart Copy types

Restore option	Snapshot	Clone	Replica
Restore All (Restores the entire Database in place)	Yes	No	No
Create Recovery Mailbox Database	Yes	Yes	No
Mount	Yes	Yes	Yes
Clone and Create Recovery Mailbox Database	No	No	Yes

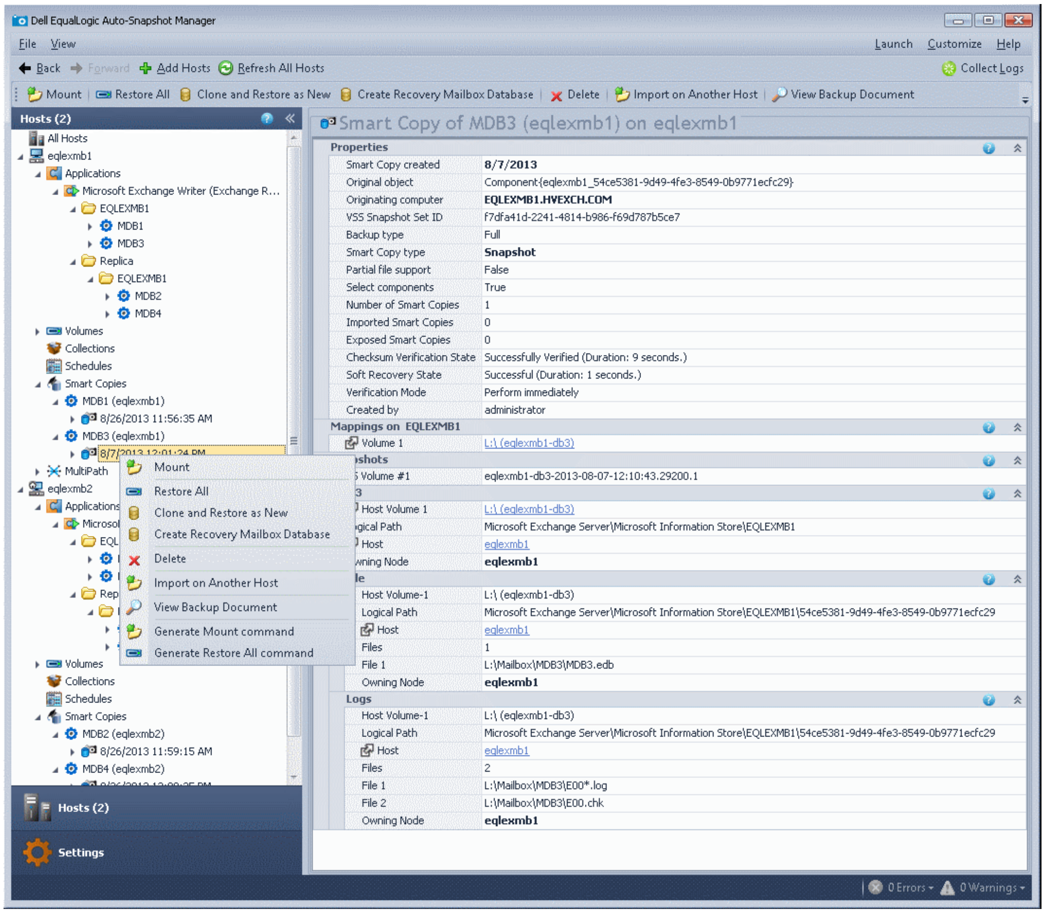
8.1 Snapshot Smart Copy restore options

There are five restore options available for snapshot type Smart Copies:

- Restore All – Performs a restore of all the data in the Smart Copy set and brings the Exchange Database online. (A point in time restoration of all data in an entire Database)
- Create Recovery Mailbox Database (RDB) - Support for doing "brick/level- item" restores using Microsoft Exchange Recovery Mailbox Database.
- Mount – Mounts the Smart Copy set on a drive letter(s) or mount point(s) that you specify. It does not restore the Database. By default, the Smart Copy is mounted read-only but optionally you can make the Smart Copy read-write. This operation only restores to a drive letter(s) or mount point(s).
- Clone and Create Recovery Mailbox Database– Performs a clone of replica Smart Copy then proceeds with Create Recovery Mailbox Database wizard. The advantage of using a clone is that it does not disrupt ongoing data replication from the base volume to the replica. The replication process continues while the clone is used for Recovery.

9 Exchange Server database restore scenarios

The following sections discuss Exchange Server Database restore scenarios and how to apply each of the restore options (Figure 9). Some scenarios may use multiple Smart Copy restore options but each option can have a different effect on the restore. Please read through the next sections carefully to understand how each Smart Copy restore option will affect the Exchange Server Database environment.



Smart Copy of MDB3 (eqlexmb1) on eqlexmb1

Properties	
Smart Copy created	**8/7/2013**
Original object	Component{eqlexmb1_54ce5381-9d49-4fe3-8549-0b9771ecfc29}
Originating computer	**EQLEXMB1.HVEXCH.COM**
VSS Snapshot Set ID	f7dfa41d-2241-4814-b986-f69d787b5ce7
Backup type	Full
Smart Copy type	**Snapshot**
Partial file support	False
Select components	True
Number of Smart Copies	1
Imported Smart Copies	0
Exposed Smart Copies	0
Checksum Verification State	Successfully Verified (Duration: 9 seconds.)
Soft Recovery State	Successful (Duration: 1 seconds.)
Verification Mode	Perform immediately
Created by	administrator
Mappings on EQLEXMB1	
Volume 1	L:\ (eqlexmb1-db3)
shots	
Volume #1	eqlexmb1-db3-2013-08-07-12:10:43.29200.1
3	
Host Volume 1	L:\ (eqlexmb1-db3)
gical Path	Microsoft Exchange Server\Microsoft Information Store\EQLEXMB1
Host	eqlexmb1
wning Node	**eqlexmb1**
le	
Host Volume-1	L:\ (eqlexmb1-db3)
Logical Path	Microsoft Exchange Server\Microsoft Information Store\EQLEXMB1\54ce5381-9d49-4fe3-8549-0b9771ecfc29
Host	eqlexmb1
Files	1
File 1	L:\Mailbox\MDB3\MDB3.edb
Owning Node	**eqlexmb1**
Logs	
Host Volume-1	L:\ (eqlexmb1-db3)
Logical Path	Microsoft Exchange Server\Microsoft Information Store\EQLEXMB1\54ce5381-9d49-4fe3-8549-0b9771ecfc29
Host	eqlexmb1
Files	2
File 1	L:\Mailbox\MDB3\E00*.log
File 2	L:\Mailbox\MDB3\E00.chk
Owning Node	**eqlexmb1**

Figure 9 Snapshot Smart Copy restore options with ASM/ME

9.1 Restore all mailbox database restore

The quickest restore scenario is the **Restore All** Mailbox Database restore. Assuming the Mailbox Database file layout has followed the best practices guidelines, this restore is useful for performing a very fast point-in-time restore of Exchange Server Mailbox Database in a DAG or non-DAG environment. The Smart Copy options that can be applied for Restore All Exchange Server Mailbox Database restore are:

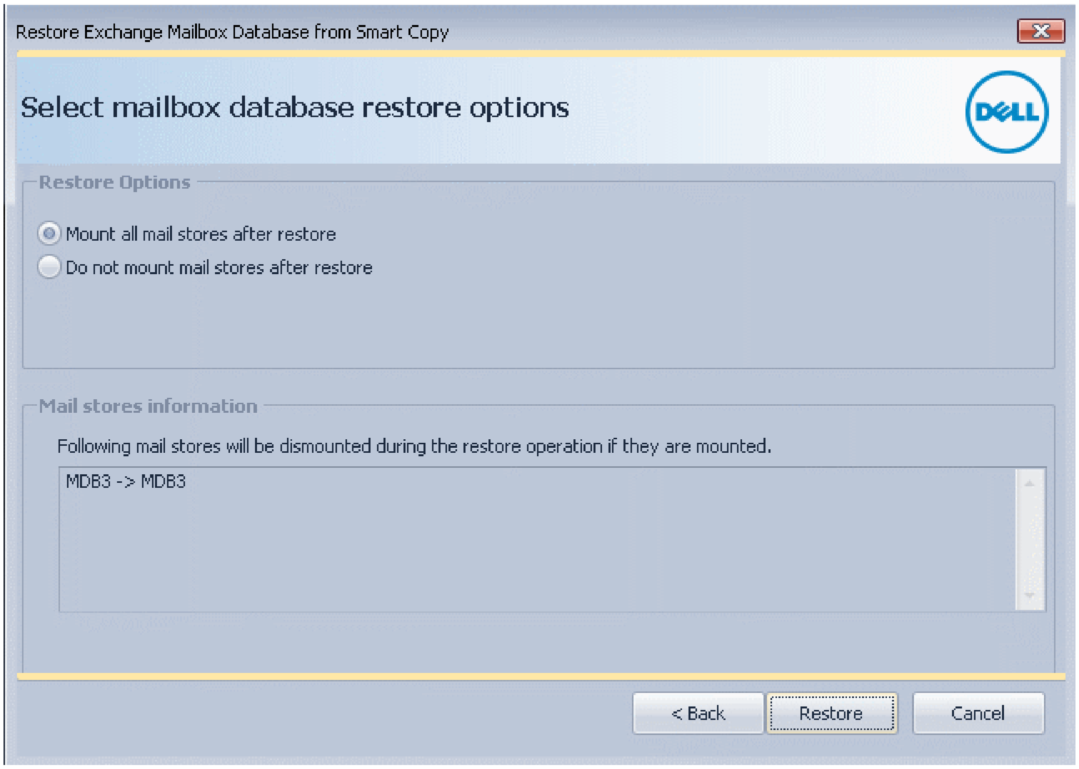
Restore All

The restore process takes the corresponding Mailbox Database and volume offline, restores the Mailbox Database back to the time of the Smart Copy, and brings the volume and Mailbox Database back online to the host and Exchange Server. At the same time, the PS Series group creates an additional snapshot of the Mailbox Database volume state before restoring the Smart Copy. This snapshot appears offline in the PS Series Group Manager GUI and can be used for debugging problems that may have caused the Mailbox Database corruption or failure.

The Restore All Mailbox Database restore has two options (Figure 10):

- Mount all mail stores after restore. This option fully restores the Mailbox Database with the Smart Copy and bring the Mailbox Database online to users at completion
- Do not mount mail stores after restore. This option restores the Mailbox Database to the time of the Smart Copy but leaves the Mailbox Database in a "restoring" state so that log file backups can be applied for additional point-in-time granularity (used in a non-DAG environment, greyed out in Figure 10 DAG node smartcopy).

Note: Rolling logs forward is a completely manual process at this time.


Restore Exchange Mailbox Database from Smart Copy

Select mailbox database restore options

Restore Options

● Mount all mail stores after restore
○ Do not mount mail stores after restore

Mail stores information

Following mail stores will be dismounted during the restore operation if they are mounted.

MDB3 -> MDB3

Figure 10 Restore all restore options

9.2 Create recovery mailbox database (RDB)

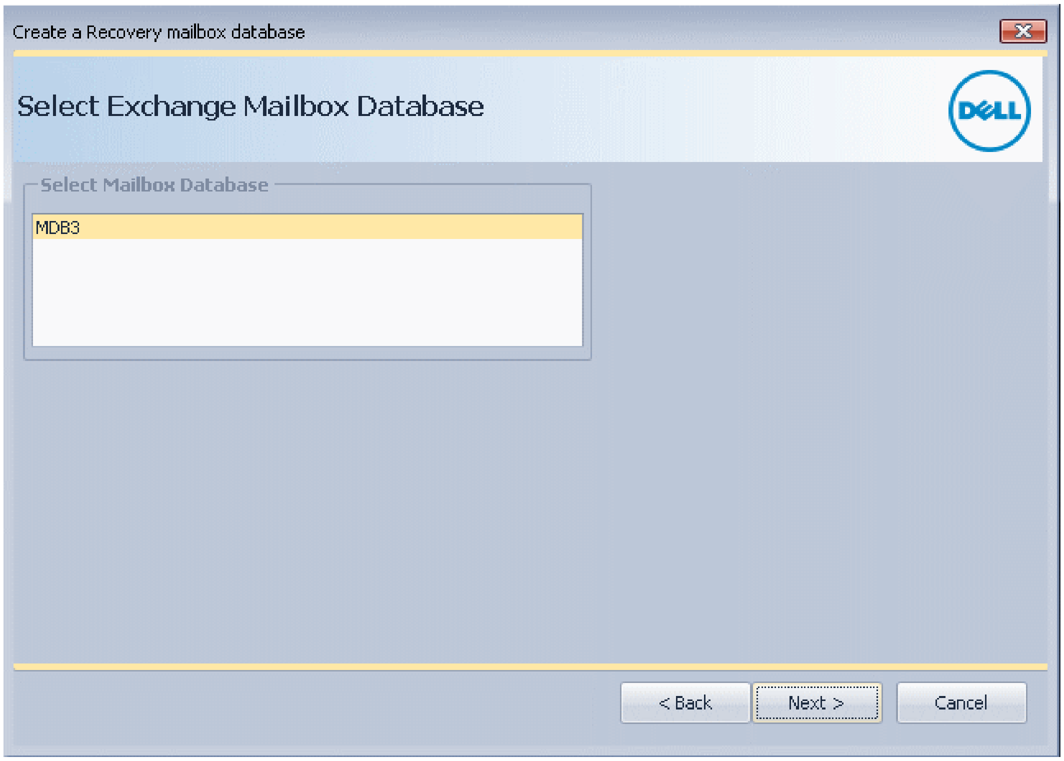
Recovery Mailbox Databases is a feature of Microsoft Exchange that enables you to mount a copy of a mailbox store to Microsoft Exchange server. You can recover data from the restored mailbox store while the live store remains online. Both Exchange 2003 and 2007 have mailbox data recovery wizards, whereas Exchange 2010 and 2013 has replaced the wizard with Power Shell for a more granular restore.

Note: Recovery Mailbox Databases shouldn't be used when you have to recover public folder content, when you have to restore entire servers, or when you have to restore multiple databases. For more information see the following URL:
Recovery Databases
http://technet.microsoft.com/en-us/library/dd876954.aspx
Restore Data Using a Recovery Database
http://technet.microsoft.com/en-us/library/ee332351.aspx

ASM/ME recognizes the new Mailbox Database files and automatically performs a selective restore operation. The Smart Copy option used for a Selective Restore of an Exchange Server Mailbox Database is:

Create Recovery Mailbox Database

When you select an Exchange Mailbox Database, its mail store is displayed in the bottom pane, which is titled: Select Mailbox Database. Click on the Mail Store to highlight it (Figure 11).



Create a Recovery mailbox database

Select Exchange Mailbox Database

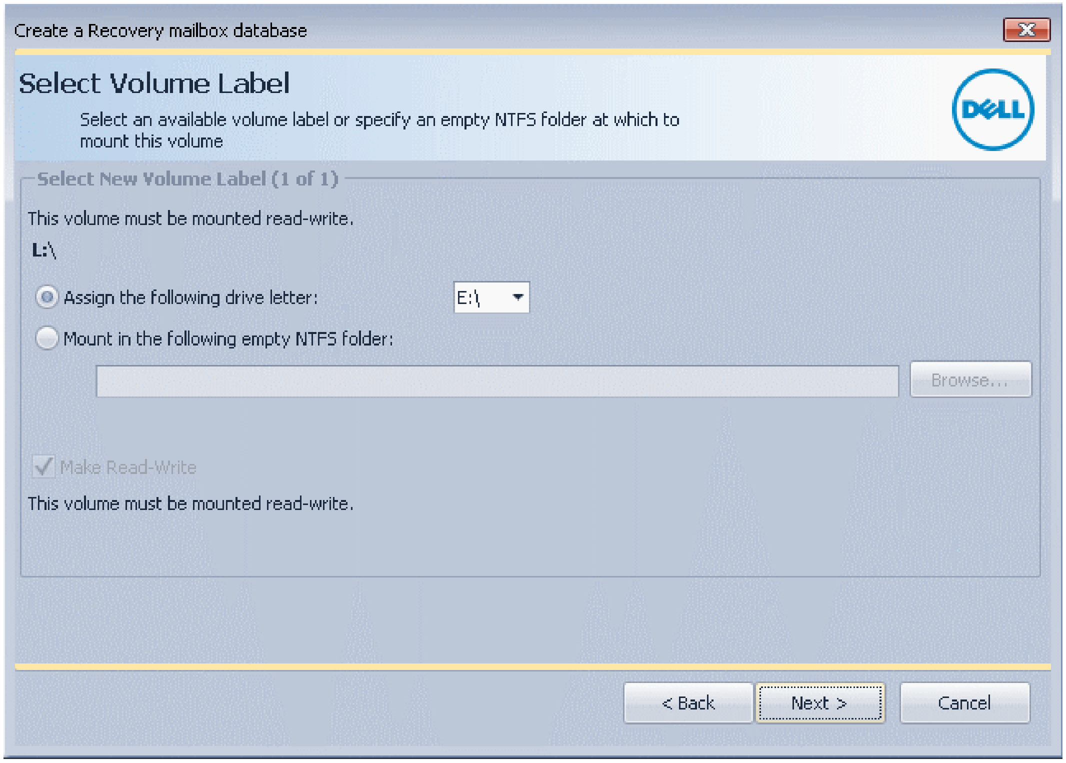
Select Mailbox Database

MDB3

Figure 11   Create recovery mailbox database (RDB)

ASM/ME displays a dialog titled: Select Volume Label. You are prompted to accept the default volume label (drive letter), such as E:\. Alternatively, specify a mount point in an empty NTFS folder for the RDB (Figure 12).

Click **Next >** to proceed.



Create a Recovery mailbox database

Select Volume Label

Select an available volume label or specify an empty NTFS folder at which to mount this volume

Select New Volume Label (1 of 1)

This volume must be mounted read-write.

L:\

● Assign the following drive letter: E:\

○ Mount in the following empty NTFS folder:

☑ Make Read-Write

This volume must be mounted read-write.

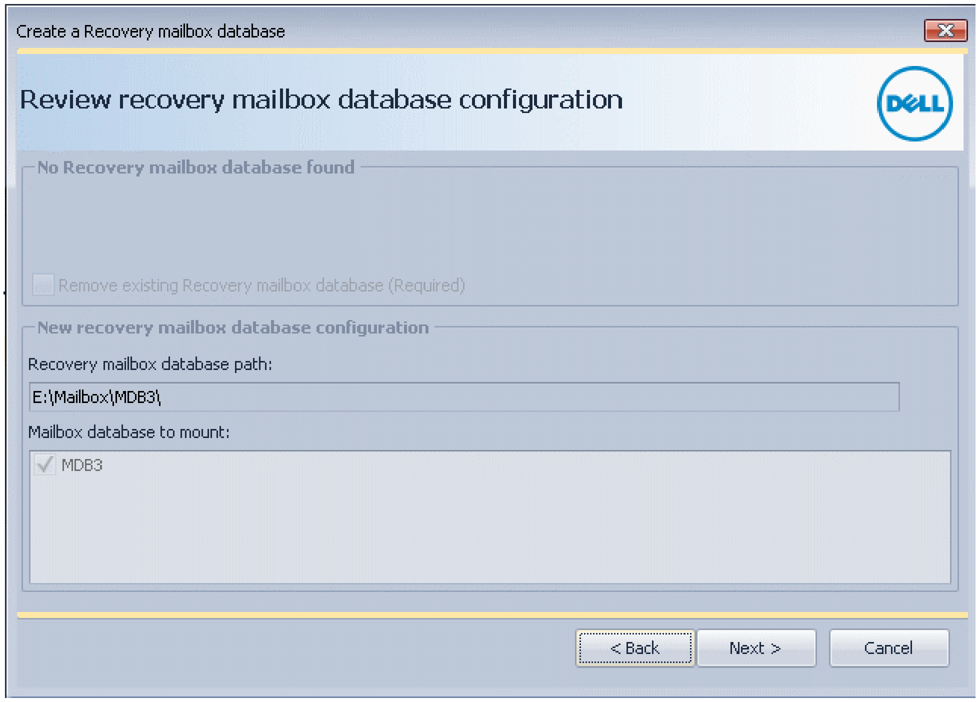
Figure 12 Select RDB drive letter or mount point

ASM/ME displays a dialog titled:

Review recovery mailbox database configuration (Figure 13). You have the following options:

1. If an existing RDB is detected, you are prompted to delete it. If you do not delete the existing RDB, you cannot proceed with creating a new RDB.
2. Confirm the path for the new recovery mailbox database.

Click **Next>** to proceed. ASM/ME creates and mounts the RDB volume, making it writable in the process.



Create a Recovery mailbox database

Review recovery mailbox database configuration

No Recovery mailbox database found

☐ Remove existing Recovery mailbox database (Required)

New recovery mailbox database configuration

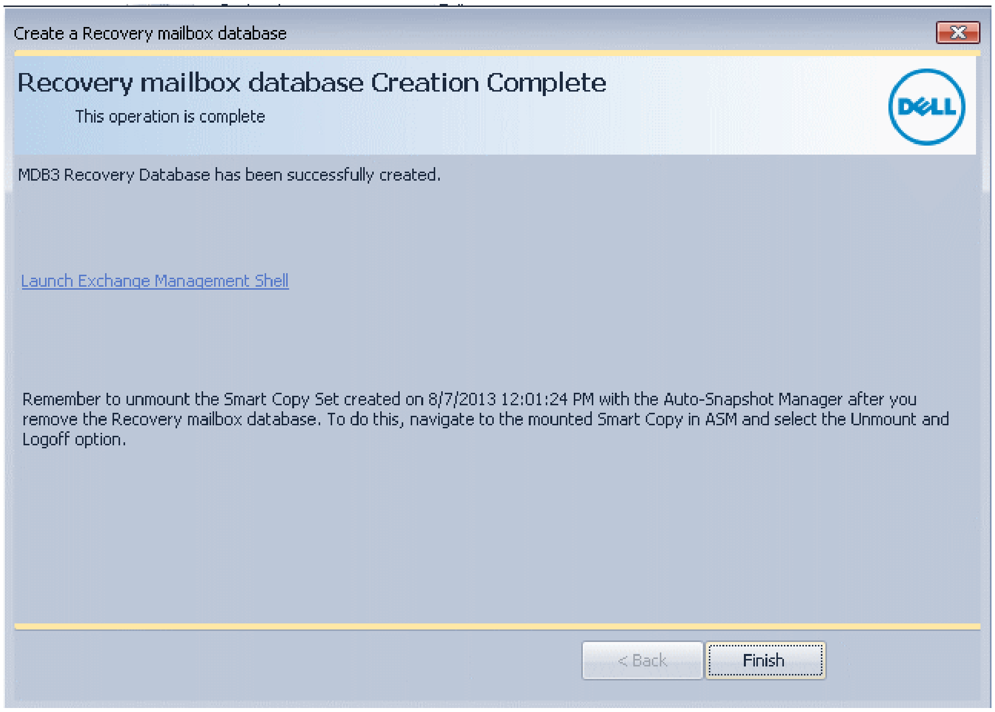
Recovery mailbox database path: E:\Mailbox\MDB3\

Mailbox database to mount:

☑ MDB3

Figure 13 Review recovery mailbox database configuration

ASM/ME displays a dialog titled: Recovery Creation Complete (Figure 14). Launch Exchange Management Shell link opens Exchange Management Shell to perform mailbox or mail item recovery. You are also prompted to use the dismount and Logoff procedure on the mounted Smart Copy set when done.



Recovery mailbox database Creation Complete

This operation is complete

MDB3 Recovery Database has been successfully created.

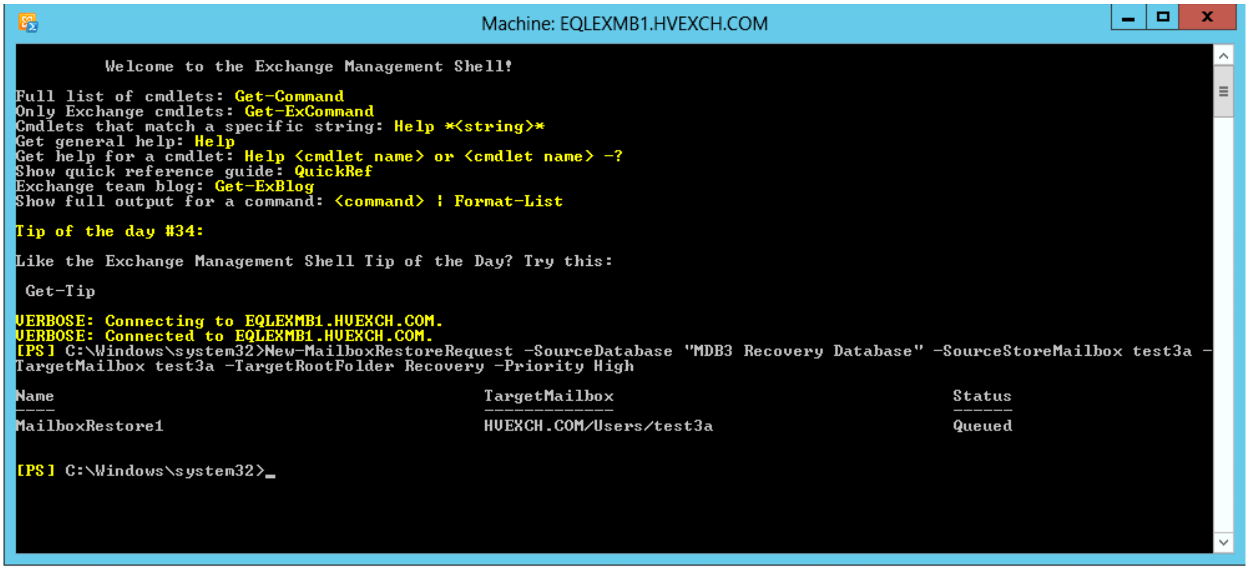
Launch Exchange Management Shell

Remember to unmount the Smart Copy Set created on 8/7/2013 12:01:24 PM with the Auto-Snapshot Manager after you remove the Recovery mailbox database. To do this, navigate to the mounted Smart Copy in ASM and select the Unmount and Logoff option.

Figure 14 Recovery Creation Complete

9.3 Single Item Recovery Using Exchange Management Shell

Click on the Launch Exchange Management Shell link (Figure 14) to be presented with Exchange Management Shell (Figure 15).



```
         Welcome to the Exchange Management Shell!

Full list of cmdlets: Get-Command
Only Exchange cmdlets: Get-ExCommand
Cmdlets that match a specific string: Help *<string>*
Get general help: Help
Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
Show quick reference guide: QuickRef
Exchange team blog: Get-ExBlog
Show full output for a command: <command> | Format-List

Tip of the day #34:

Like the Exchange Management Shell Tip of the Day? Try this:

 Get-Tip

VERBOSE: Connecting to EQLEXMB1.HVEXCH.COM.
VERBOSE: Connected to EQLEXMB1.HVEXCH.COM.
[PS] C:\Windows\system32>New-MailboxRestoreRequest -SourceDatabase "MDB3 Recovery Database" -SourceStoreMailbox test3a -
TargetMailbox test3a -TargetRootFolder Recovery -Priority High

Name                                           TargetMailbox                                  Status
----                                           -------------                                  ------
MailboxRestore1                                HVEXCH.COM/Users/test3a                        Queued


[PS] C:\Windows\system32>_
```

Figure 15 Recovery with Exchange Management shell

You can use Power Shell commands to extract data from an RDB. After extraction, the data can be exported to a folder or merged into an existing mailbox. The name of the recovery mailbox database is the original Exchange Mailbox Database name, followed by recovery database.

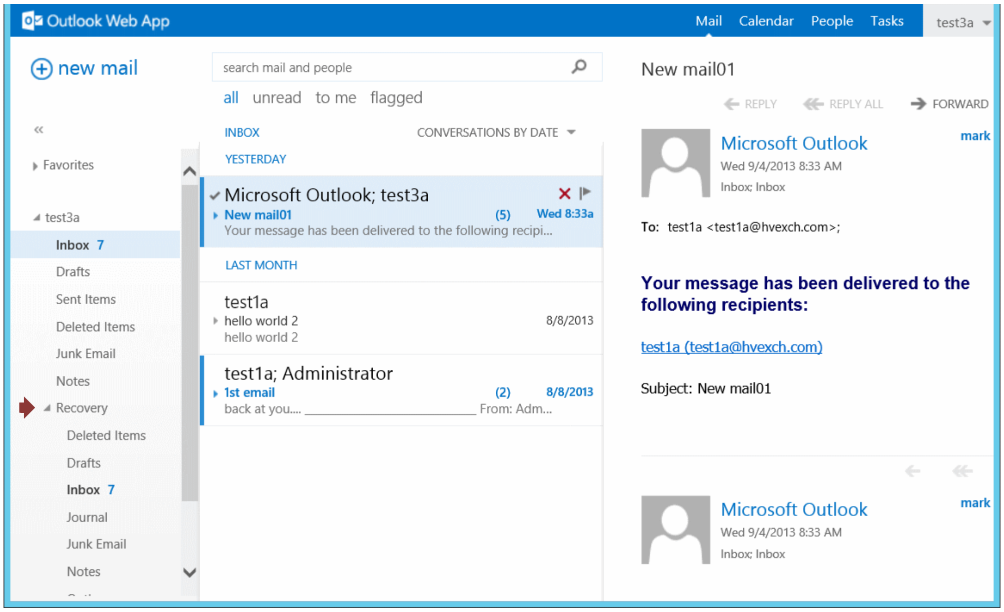
For *New-MailboxRestoreRequest* command parameters both required and optional please visit this link: [New-MailboxRestoreRequest](http://technet.microsoft.com/en-us/library/ff829875.aspx)

http://technet.microsoft.com/en-us/library/ff829875.aspx

The example in Figure 15 demonstrates recovering all mail items from the point-in-time copy of test3a's mailbox that is hosted on Mailbox Database MDB3 and placing them in a sub folder named Recovery in test3a's mailbox. The Power Shell command for that is:

*New-MailboxRestoreRequest -SourceDatabase "**MDB3 Recovery Database**" -SourceStoreMailbox **test3a** -TargetMailbox **test3a** -TargetRootFolder **Recovery** -Priority | **High***

The variables in the Power Shell command have been changed to bold font for clarity. The recovery folder (red arrow) can be seen in Figure 16.



New mail01

Microsoft Outlook
Wed 9/4/2013 8:33 AM
Inbox; Inbox

To: test1a <test1a@hvexch.com>;

Your message has been delivered to the following recipients:

test1a (test1a@hvexch.com)

Subject: New mail01

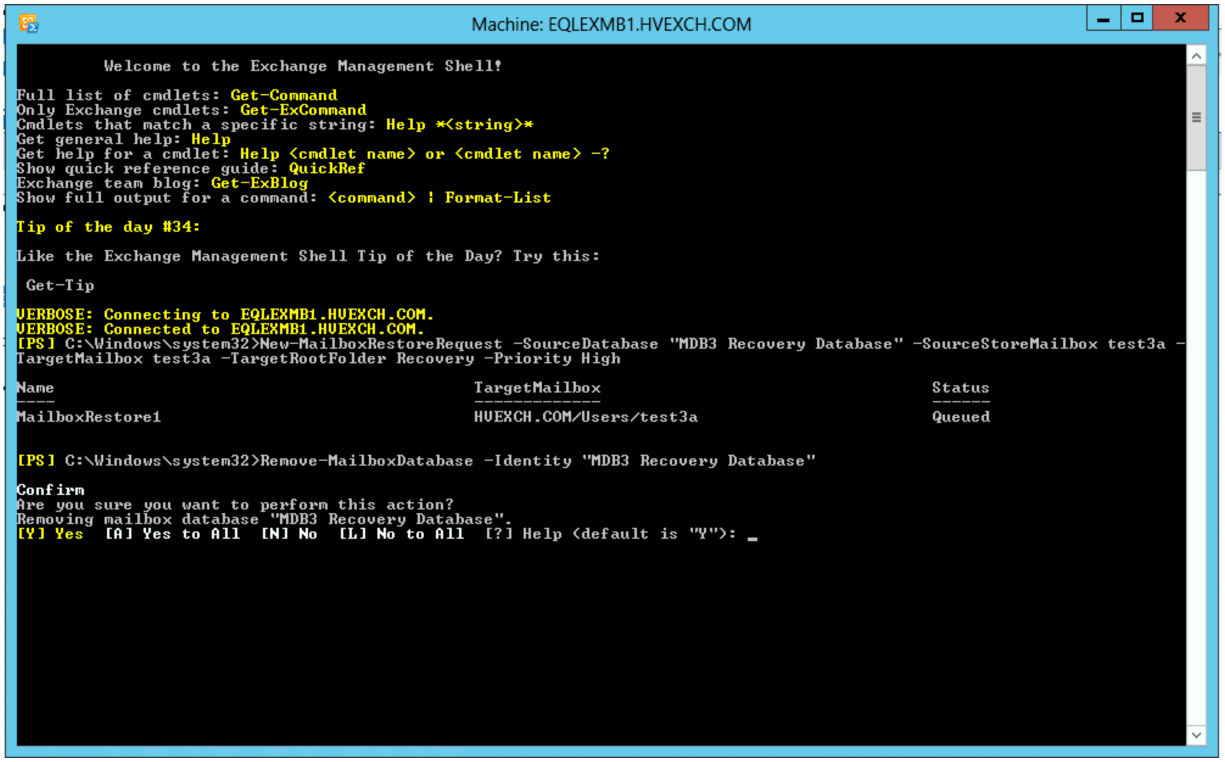
Microsoft Outlook
Wed 9/4/2013 8:33 AM
Inbox; Inbox

Figure 16 Recovery folder in Outlook

The last step in the RDB process is to remove the RDB and that Power Shell command is displayed in Figure 17 and is as follows:

Remove-MailboxDatabase -Identity **"MDB3 Recovery Database"**

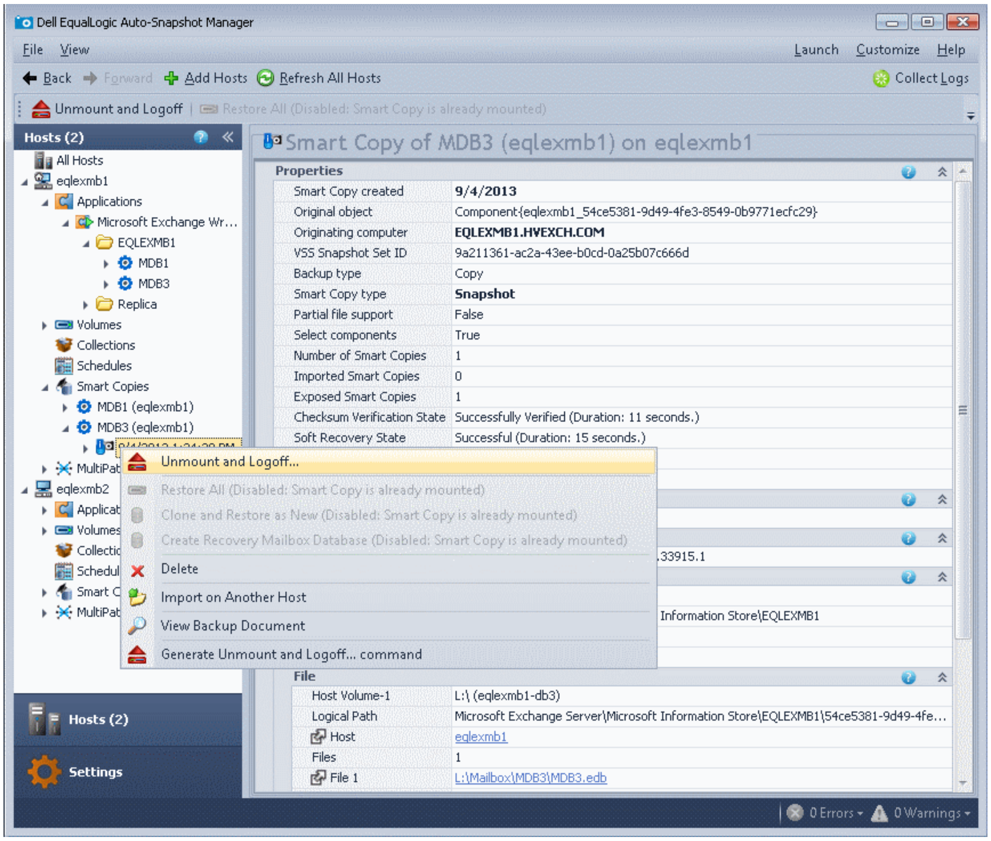
The variables in the Power Shell command above have been changed to bold font for clarity.



```
         Welcome to the Exchange Management Shell!

Full list of cmdlets: Get-Command
Only Exchange cmdlets: Get-ExCommand
Cmdlets that match a specific string: Help *<string>*
Get general help: Help
Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
Show quick reference guide: QuickRef
Exchange team blog: Get-ExBlog
Show full output for a command: <command> | Format-List

Tip of the day #34:

Like the Exchange Management Shell Tip of the Day? Try this:

 Get-Tip

VERBOSE: Connecting to EQLEXMB1.HVEXCH.COM.
VERBOSE: Connected to EQLEXMB1.HVEXCH.COM.
[PS] C:\Windows\system32>New-MailboxRestoreRequest -SourceDatabase "MDB3 Recovery Database" -SourceStoreMailbox test3a -
TargetMailbox test3a -TargetRootFolder Recovery -Priority High

Name                                          TargetMailbox                                 Status
----                                          -------------                                 ------
MailboxRestore1                               HVEXCH.COM/Users/test3a                       Queued


[PS] C:\Windows\system32>Remove-MailboxDatabase -Identity "MDB3 Recovery Database"

Confirm
Are you sure you want to perform this action?
Removing mailbox database "MDB3 Recovery Database".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [?] Help (default is "Y"): _
```

Figure 17 Remove recovery database

The last step in the clean-up process is to use the dismount and Logoff procedure on the mounted Smart Copy set when done (Figure 18).



Smart Copy of MDB3 (eqlexmb1) on eqlexmb1

Properties

Smart Copy created	**9/4/2013**
Original object	Component{eqlexmb1_54ce5381-9d49-4fe3-8549-0b9771ecfc29}
Originating computer	**EQLEXMB1.HVEXCH.COM**
VSS Snapshot Set ID	9a211361-ac2a-43ee-b0cd-0a25b07c666d
Backup type	Copy
Smart Copy type	**Snapshot**
Partial file support	False
Select components	True
Number of Smart Copies	1
Imported Smart Copies	0
Exposed Smart Copies	1
Checksum Verification State	Successfully Verified (Duration: 11 seconds.)
Soft Recovery State	Successful (Duration: 15 seconds.)

.33915.1

Information Store\EQLEXMB1

File

Host Volume-1	L:\ (eqlexmb1-db3)
Logical Path	Microsoft Exchange Server\Microsoft Information Store\EQLEXMB1\54ce5381-9d49-4fe…
Host	eqlexmb1
Files	1
File 1	L:\Mailbox\MDB3\MDB3.edb

Figure 18 Unmount and Logoff

10 Summary

Auto-Snapshot Manager / Microsoft Edition can substantially increase Exchange Server data availability by using PS Series data protection technologies. Smart Copy snapshots, clones, and replicas all play a vital role in robust Exchange Server protection scenarios for on-demand data recovery and Exchange Server Mailbox Database restores.

Although using ASM/ME will increase Exchange Server data availability, it is not considered an alternative to long-term backup methods. ASM/ME and Smart Copies should be used in conjunction with a normal backup schedule for a higher level of data protection and shorter Mailbox Database recovery time.

By using ASM/ME with regular backup methods, you can ensure your NTFS and Exchange Server data is protected and available at all times.

A Glossary

PS Series Group Manager GUI – A Java-based user interface to manage the PS series Mailbox Database.

Auto-Snapshot Manager GUI – A host-based management interface to create and manage Smart Copies of Exchange Server Mailbox Databases and NTFS volumes.

Smart Copy – An application-consistent copy of an Exchange Server Mailbox Database. Smart Copy types include snapshots, clones, and replicas.

Snapshot Smart Copy – A PS Series volume-based snapshot of an Exchange Server Mailbox Database or NTFS volume created through Microsoft Volume Shadow Copy Service.

Clone Smart Copy – A PS Series copy of an Exchange Server Mailbox Database or NTFS volume created through Microsoft Volume Shadow Copy Service that is a complete duplicate of the original volume or volumes that make up the Mailbox Database and its attributes.

Replica Smart Copy – A PS Series volume snapshot of an Exchange Server Mailbox Database or NTFS volume created through Microsoft Volume Shadow Copy Service that is stored on a replication partner. Replication must be set up on the PS Series group and on the volume before you can create a replica Smart Copy.

Torn Smart Copy – A Smart Copy Set contains additional components (application data) other than the selected object (Mailbox Database). Torn Smart Copies will not harm the original Mailbox Database or base volume.

Smart Copy Collection – A group of object components (Mailbox Database and log volume) added to a single Smart Copy operation.

Smart Copy Schedule – A schedule set up though Auto-Snapshot Manager to create ongoing Smart Copies of an object.

Backup Document – An XML file created by ASM that contains metadata of a Smart Copy.

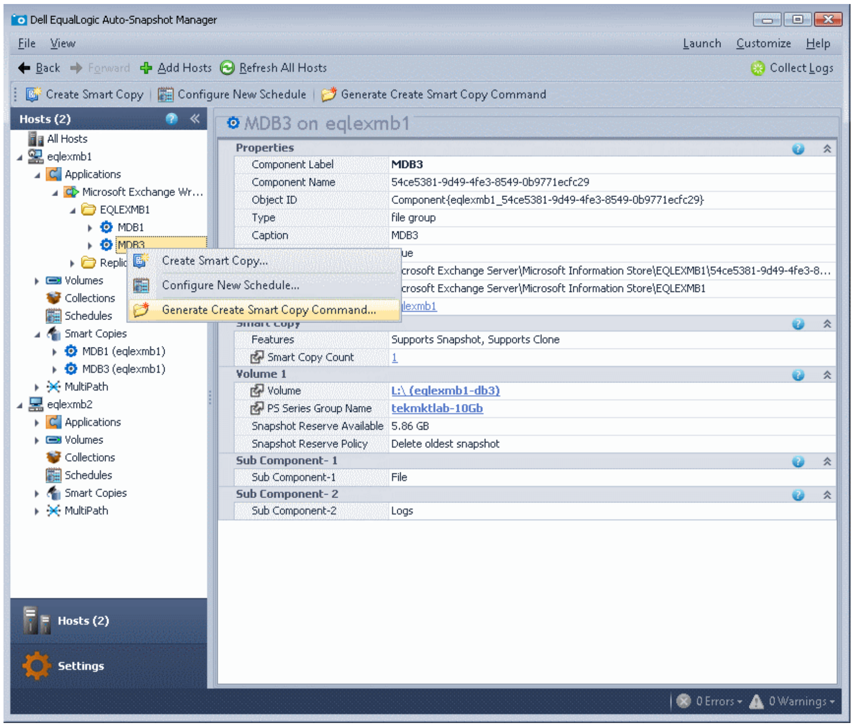
B Command line options

If you have existing scripts for running backups or performing other background operations, you can also schedule the creation of smart copy sets by adding an ASM/ME command to the script.

Scripting ASM/ME v4.6

ASM/ME v4.6 has enabled much of the functionality of the GUI into the command line interface. Additionally the GUI has included options to automate script creation by allowing users to run through Smart Copy processes in the GUI and outputting the commands needed to perform these operations via command line.

To initiate the script creation process highlight the object you want to work with. Either right click or use the Actions pane to the right to “Generate [command type] Command” as in Figure 19.

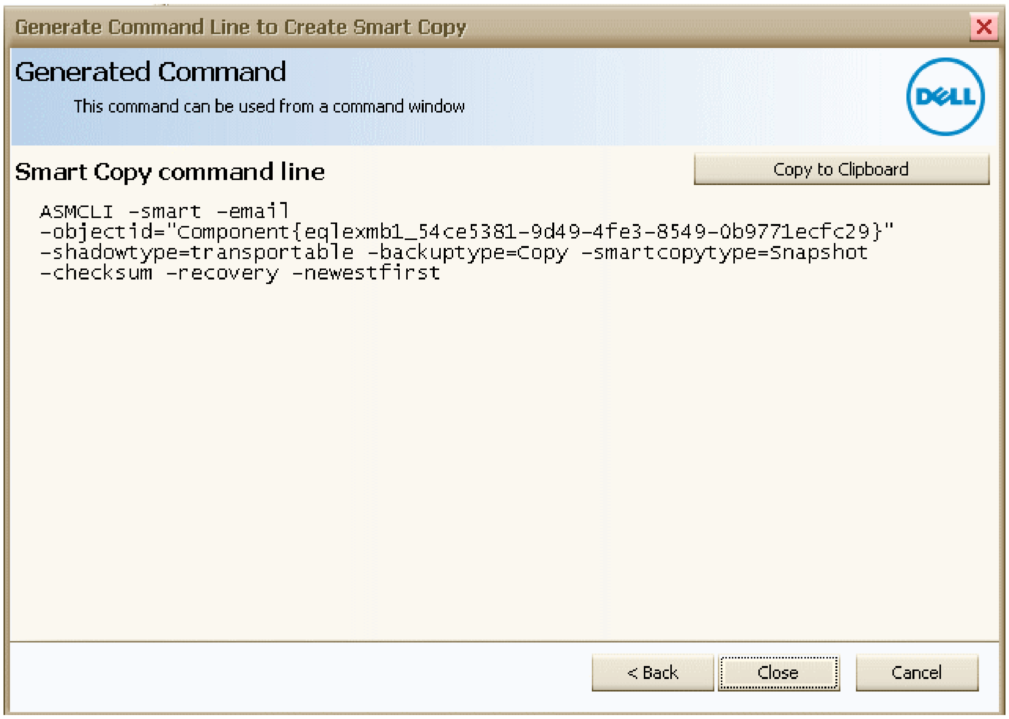


MDB3 on eqlexmb1

Properties	
Component Label	**MDB3**
Component Name	54ce5381-9d49-4fe3-8549-0b9771ecfc29
Object ID	Component{eqlexmb1_54ce5381-9d49-4fe3-8549-0b9771ecfc29}
Type	file group
Caption	MDB3
	ue
	crosoft Exchange Server\Microsoft Information Store\EQLEXMB1\54ce5381-9d49-4fe3-8...
	crosoft Exchange Server\Microsoft Information Store\EQLEXMB1
	lexmb1
Smart Copy	
Features	Supports Snapshot, Supports Clone
Smart Copy Count	1
Volume 1	
Volume	L:\ (eqlexmb1-db3)
PS Series Group Name	tekmktlab-10Gb
Snapshot Reserve Available	5.86 GB
Snapshot Reserve Policy	Delete oldest snapshot
Sub Component- 1	
Sub Component-1	File
Sub Component- 2	
Sub Component-2	Logs

Figure 19 Generate command

This will run through the process of creating a Smart Copy Set and at the end instead of creating the Smart Copy, a command is generated as seen in Figure 20. This command can then be copied and used to create the Smart Copy in a script or batch file.



Generate Command Line to Create Smart Copy
Generated Command
This command can be used from a command window
Smart Copy command line
Copy to Clipboard
< Back
Close
Cancel

```
ASMCLI -smart -email
-objectid="Component{eqlexmb1_54ce5381-9d49-4fe3-8549-0b9771ecfc29}"
-shadowtype=transportable -backuptype=Copy -smartcopytype=Snapshot
-checksum -recovery -newestfirst
```

Figure 20 Smart Copy command line

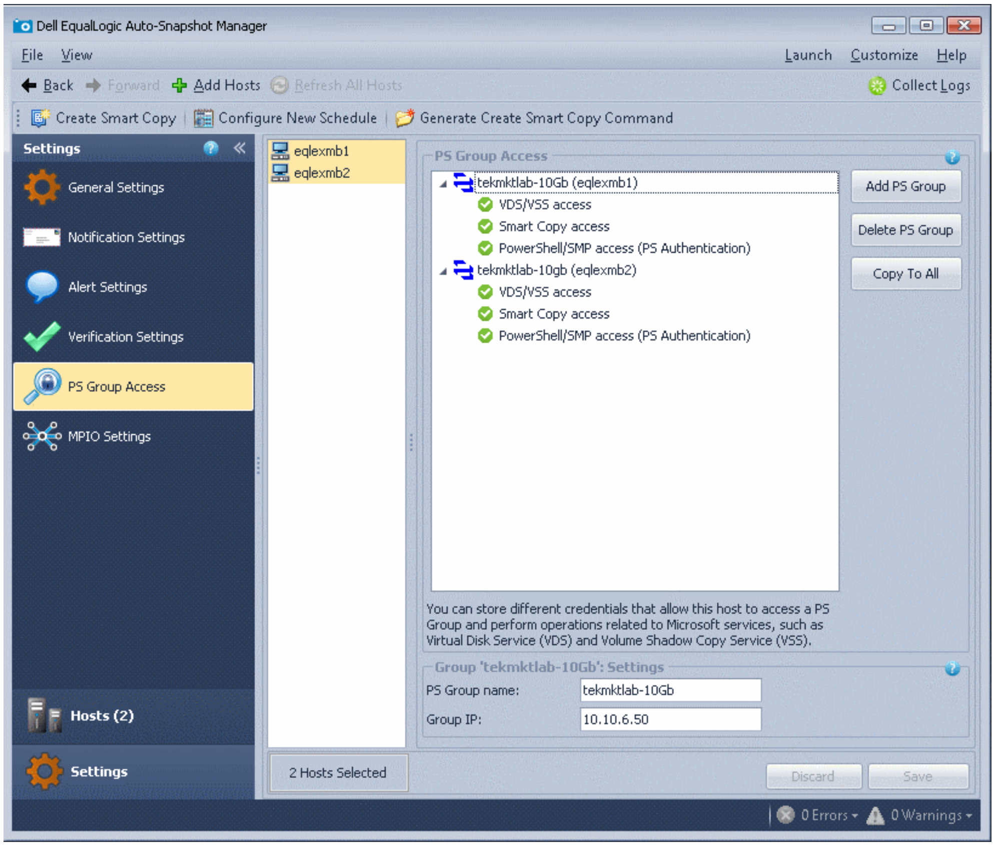
Scripts like this can be created for other Smart Copy operations and used accordingly. For a detailed description of script commands and sample usage, see the Host Integration Tools for Windows v4.6 User Guide.

C VSS-control troubleshooting tips

ASM/ME uses CHAP authentication to communicate with the PS Series group. The authentication user name and password must be the same on the host running Auto-Snapshot Manager and the PS Series group.

If the PS Series group IP address is not already in the groups listed under PS Group Access on the settings tab in Auto-Snapshot Manager, add the IP address of the PS Series group you would like to connect to and add the CHAP username and password (Figure 21). If the group is in the list, you can modify the Host Management access rights to match those of the PS Series group you would like to use with Auto-Snapshot Manager. Be sure to restart the Auto-Snapshot Manager application if you modify the Host Management credentials.

You can determine whether CHAP authentication is set up correctly by selecting the Targets tab in the Microsoft iSCSI Initiator service and verifying that the vsscontrol volume is shown in the list. The vsscontrol volume should have a status of connect if CHAP is set up correctly. If there are multiple vsscontrol volumes in the targets list, you can display the connection details by selecting the volume and choosing Details in the Targets window. The PS Series group connection will be listed in the Session Connections section. Be sure the Volume Shadow Copy service is running on the host prior to checking the vsscontrol volume status.



tekmktlab-10Gb (eqlexmb1)
- ✓ VDS/VSS access
- ✓ Smart Copy access
- ✓ PowerShell/SMP access (PS Authentication)

tekmktlab-10gb (eqlexmb2)
- ✓ VDS/VSS access
- ✓ Smart Copy access
- ✓ PowerShell/SMP access (PS Authentication)

You can store different credentials that allow this host to access a PS Group and perform operations related to Microsoft services, such as Virtual Disk Service (VDS) and Volume Shadow Copy Service (VSS).

Group 'tekmktlab-10Gb': Settings

PS Group name: tekmktlab-10Gb

Group IP: 10.10.6.50

Figure 21 PS Group Access

D Remote host verification setup

You can optionally perform Checksum Verification and Soft Recovery on a remote host. Remote Host verification requires the following configuration:

- Two host systems with the same installed versions of the following application software:
- Auto-Snapshot Manager.
- Exchange Management Tools.
- A shared network folder or drive to provide a Smart Copy repository.

One of the hosts acts as the creator server, creating Smart Copies, The second host acts as the verification server running a Global Verification Task that verifies all unverified Exchange Smart Copies.

The Global Verification window can differ between the local and remote servers. For example, you might configure verification during an off-peak Global Verification window on the creator server, such as the default 8:00PM to 6:00AM window. You might then configure the creator server to run verification on the remote host, setting the verification server's Global Verification window to 24 hours.

Note: If you want to run Checksum Verification and Soft Recovery on a remote host and your configuration consists of a HIT Group with two or more hosts, Dell recommends that you use the following guidelines:
• If your HIT Group is a DAG, then each node will have its own, unique backup document directory. Because of this, each node will require its own remote host for Checksum Verification and Soft Recovery. For example, if your HIT Group is comprised of a 4-node DAG, then you will need to allocate 4 separate hosts for remote host Checksum Verification and Soft Recovery (1 host per node).

D.1 Using a system as a dedicated verification server

To make the best use of system resources, you can configure a host to run only the Global Verification Task, taking the Checksum Verification and Soft Recovery workload off your production servers. You specify a Global Verification window that is specific to the verification server, typically a much longer time period than for a production server.

Using a dedicated verification server enables you to process a greater number of Smart Copies, improving your recovery options and service level. The verification server might be co-located with Smart Copy creator servers, or it might be at a geographically remote location. However, the verification server requires access to the SAN on which you create and maintain Smart Copies.

D.2 Prerequisites for a verification server

A verification server has the following prerequisites:

- You must install the same release of Host Integration Tools on both the verification server and on the Smart Copy creator servers. This includes all required applications such as the iSCSI initiators.
- You must install the Exchange Management Tools for the same release of Microsoft Exchange Server as is installed on the Smart Copy creator servers. Maintain version parity on creator and verification servers, including the latest hot fixes available from Microsoft.
- The verification server and any creator servers that it serves must be part of the same Microsoft Windows domain.
- The verification server and any creator servers that it serves must be able to access a shared location for Smart Copies.
- Appropriate network access and bandwidth to process the Global Verification Tasks of client systems.

D.3 Configuring a verification server

Use the following procedure to set up a verification server:

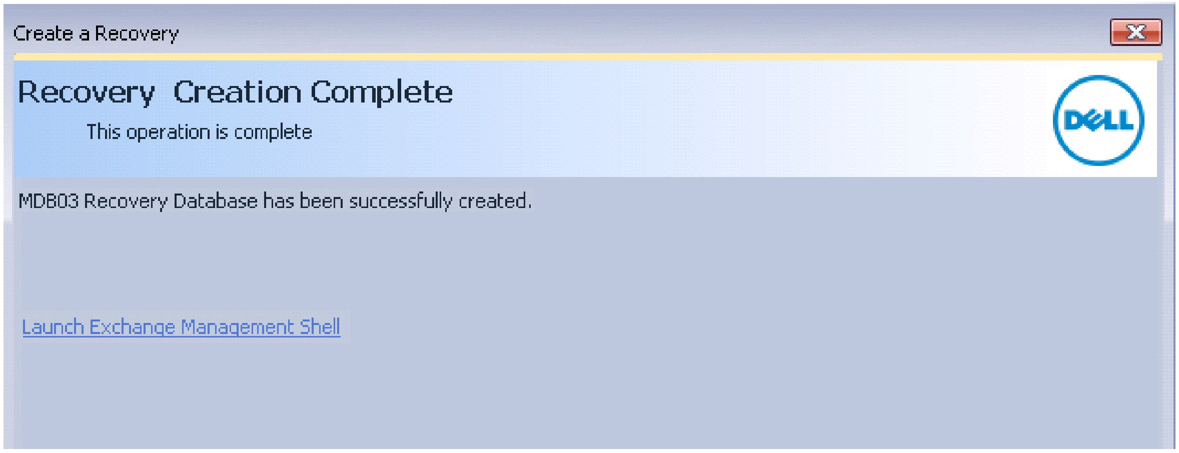
1. Use the Remote Setup Wizard to enable the verification server to access the storage array group.
2. On the Smart Copy creator server, find the location of the shared Smart Copy "copy" folder as follows:
    a. Launch ASM/ME and click Settings in the navigation area.
    b. Click General Settings.
    c. Under the Auto-Snapshot Manager Document Directory, find the path specified as where ASM will store its backup documents. Write down or copy the path to a text file.
    d. Close the Settings window by clicking on Hosts.
3. Dell recommends that you configure the Volume Access Control List on the PS Series group so that the verification server has access only to snapshots, and not to the original volume. See the Creating Access Control Records procedure described in the Volume Management section of the Group Manager GUI Online Help.
4. On the verification server, map a drive to the shared shadow copy folder that you identified in Step 2. Use the same drive letter if possible.
5. On the verification server, point ASM to the shared shadow copy folder as follows:
    a. Launch ASM/ME and click Settings in the navigation area.
    b. Click General Settings.

   c. Under the Auto-Snapshot Manager Document Directory, specify the path to the shared folder that you defined in Step 4. (Ensure that the drive letter specifies the local mount point.)
   d. Specify a domain account under Run ASM Service AS: the account will be granted "Log on as a service" privilege on selected hosts.
   e. Click Save.
6. Set up a Global Verification Task on the verification server, using the following steps:
   a. In the Host area right-click on Schedules, then click on Create Global Verification Task.
   b. In the dialog titled: Create or Modify Global Verification Task, select the following option: Process Smart Copies Created by another host
   c. If the sole purpose of the verification server is Checksum Verification and Soft Recovery, consider setting the Global Verification window to the maximum possible 24-hour period.
   d. Under EseUtil Location enter the path to eseutil.exe then click Next.
   e. Specify a user account that has appropriate permission to access the Smart Copies (according to the shared folder settings). Click Create.
7. The verification server now watches the shared folder and processes any unverified Smart Copies according to the local Global Verification window. When you select a Smart Copy, its verification status is indicated in the properties window.

E Exchange 2013 data protection versus Exchange 2010

A Smart Copy of a mailbox database (for Exchange 2010 and 2013) will function exactly the same on both versions. Exchange 2013 adds the ability to create Smart Copies of Public Folders and restore Public Folders. The Restore-Mailbox command has been replaced with the New-MailboxRestoreRequest in Exchange 2013 although it could be used in later versions of Exchange 2010. The steps to use the restore-mailbox command in Exchange 2010 are listed below.

Single Item Recovery Using Restore-Mailbox command Exchange Management Shell


Create a Recovery

Recovery Creation Complete

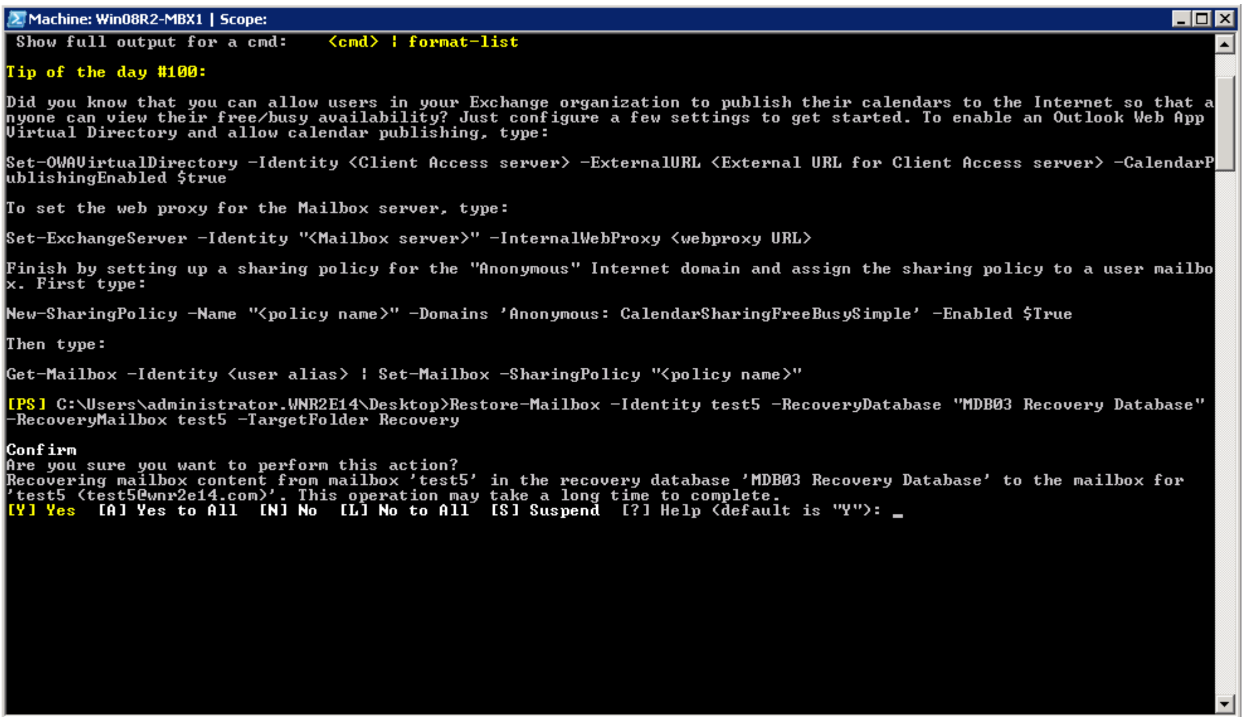
This operation is complete

MDB03 Recovery Database has been successfully created.

Launch Exchange Management Shell

Figure 22 Recovery creation complete

Click on the Launch Exchange Management Shell link (Figure 22) to be presented with Exchange Management Shell (Figure 23).



```
 Show full output for a cmd:    <cmd> | format-list

Tip of the day #100:

Did you know that you can allow users in your Exchange organization to publish their calendars to the Internet so that a
nyone can view their free/busy availability? Just configure a few settings to get started. To enable an Outlook Web App
Virtual Directory and allow calendar publishing, type:

Set-OWAVirtualDirectory -Identity <Client Access server> -ExternalURL <External URL for Client Access server> -CalendarP
ublishingEnabled $true

To set the web proxy for the Mailbox server, type:

Set-ExchangeServer -Identity "<Mailbox server>" -InternalWebProxy <webproxy URL>

Finish by setting up a sharing policy for the "Anonymous" Internet domain and assign the sharing policy to a user mailbo
x. First type:

New-SharingPolicy -Name "<policy name>" -Domains 'Anonymous: CalendarSharingFreeBusySimple' -Enabled $True

Then type:

Get-Mailbox -Identity <user alias> | Set-Mailbox -SharingPolicy "<policy name>"

[PS] C:\Users\administrator.WNR2E14\Desktop>Restore-Mailbox -Identity test5 -RecoveryDatabase "MDB03 Recovery Database"
-RecoveryMailbox test5 -TargetFolder Recovery

Confirm
Are you sure you want to perform this action?
Recovering mailbox content from mailbox 'test5' in the recovery database 'MDB03 Recovery Database' to the mailbox for
'test5 <test5@wnr2e14.com>'. This operation may take a long time to complete.
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): _
```

Figure 23 Recovery with Exchange Management Shell

You can use the cmdlet to extract data from an RDB. After extraction, the data can be exported to a folder or merged into an existing mailbox. The name of the recovery mailbox database is the original Exchange Mailbox Database name, followed by recovery database.

For *restore-mailbox* command parameters both required and optional please visit this link: Restore-Mailbox

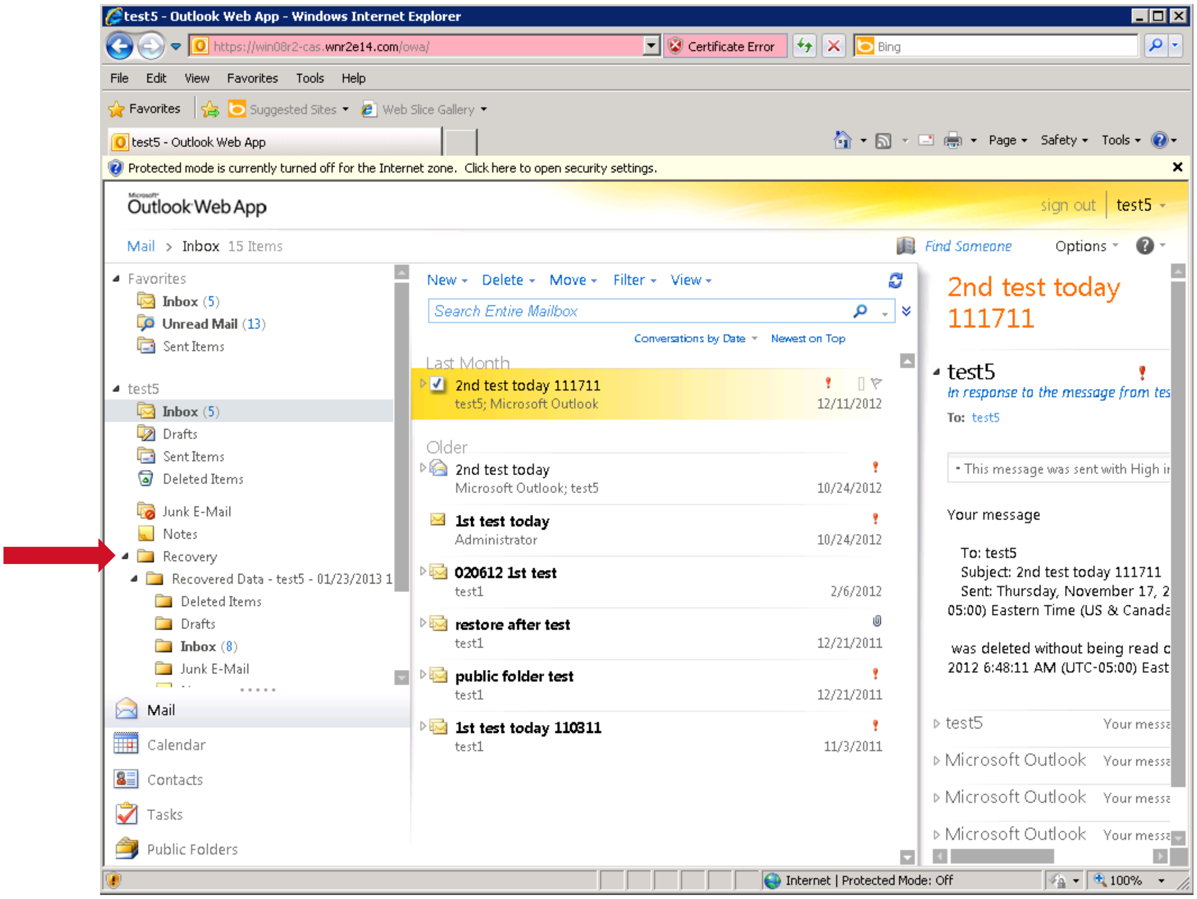
http://technet.microsoft.com/en-us/library/bb125218.aspx

The example in Figure 23 demonstrates recovering all mail items from the point-in-time copy of test5's mailbox that is hosted on Mailbox Database MDB03 and placing them in a sub folder named Recovery in test5's mailbox. The Power Shell command for that is:

```
Restore-Mailbox -Identity test5 -RecoveryDatabase "MDB03 Recovery Database" -
RecoveryMailbox test5 -TargetFolder Recovery
```

The variables in the Power Shell command have been changed to bold font for clarity.

The recovery folder can be seen highlighted with a red arrow in Figure 24.



Last Month	
2nd test today 111711 test5; Microsoft Outlook	12/11/2012
Older	
2nd test today Microsoft Outlook; test5	10/24/2012
1st test today Administrator	10/24/2012
020612 1st test test1	2/6/2012
restore after test test1	12/21/2011
public folder test test1	12/21/2011
1st test today 110311 test1	11/3/2011

2nd test today 111711

test5

In response to the message from tes

To: test5

• This message was sent with High i

Your message

To: test5
Subject: 2nd test today 111711
Sent: Thursday, November 17, 2
05:00) Eastern Time (US & Canada

was deleted without being read c
2012 6:48:11 AM (UTC-05:00) East

test5 Your messa
Microsoft Outlook Your messa
Microsoft Outlook Your messa
Microsoft Outlook Your messa

Figure 24 Recovery folder in Outlook

Technical support and customer service

Dell support service is available to answer your questions about PS Series SAN arrays.

Contacting Dell

1. If you have an Express Service Code, have it ready.
   The code helps the Dell automated support telephone system direct your call more efficiently.
2. If you are a customer in the United States or Canada in need of technical support, call 1-800-945-3355. If not, go to Step 3.
3. Visit support.dell.com/equallogic.
4. Log in, or click "Create Account" to request a new support account.
5. At the top right, click "Contact Us," and call the phone number or select the link for the type of support you need.

Related documentation

For detailed information about PS Series arrays, groups, volumes, array software, and host software, log in to the Documentation page at the customer support site.

The following table lists the documents referred to in this Technical Report. All PS Series Technical Reports are available on the Customer Support site at: *support.dell.com*

Vendor	Document Title
Microsoft®	Exchange Server Disaster Recovery: Disaster Recovery
Microsoft®	Understanding Exchange LUN Architecture
Microsoft®	Recovery Databases
Microsoft®	Restore Data Using a Recovery Database
Microsoft®	New-MailboxRestoreRequest

Dell Online Services

You can learn about Dell products and services using this procedure:

1. Visit http://www.dell.com or the URL specified in any Dell product information.
2. Use the locale menu or click on the link that specifies your country or region.

Dell EqualLogic Storage Solutions

To learn more about Dell EqualLogic products and new releases being planned, visit the Dell EqualLogic TechCenter site: http://delltechcenter.com/page/EqualLogic. Here you can also find articles, demos, online discussions, technical documentation, and more details about the benefits of our product family.

For an updated Dell EqualLogic compatibility list please visit the following URL: https://support.equallogic.com/compatibility