Dell EqualLogic
Auto-Snapshot Manager/Microsoft Edition

User's Guide

Version 4.7

Published: April 2014

Part Number: 110-6184-EN-R2

Table of Contents

Preface

Dell™ EqualLogic® Host Integration Tools give you the ability to manage and configure PS Series storage arrays from the servers that use them. From initializing new arrays to creating application-consistent snapshots, to scripting management operations, the Host Integration Tools expose a wide variety of capabilities to server administrators.

Audience

The information in this guide is intended for administrators using Host Integration Tools to manage snapshots, replicas, and clones through Smart Copies, using the ASM/ME interface.

Related Documentation

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

Dell Online Services

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

1. Visit 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 Dell EqualLogic TechCenter. Here you can also see articles, demos, online discussions, and more details about the benefits of our product family.

Technical Support and Customer Service

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

Contacting Dell

If you are a customer in the United States or Canada in need of technical support, call 1-800-945-3355. If you are outside of the United States or Canada, visit Dell EqualLogic Product Support.

If you have an Express Service Code, have it ready. The code helps the Dell automated support telephone system direct your call more efficiently.

1 Introduction to ASM/ME

Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition (ASM/ME) enables you to create fast, space-efficient, point-in-time copies of Dell EqualLogic volumes as part of a backup and recovery strategy for your data. You can quickly back up and restore Dell EqualLogic volumes on multiple Microsoft® Windows® machines, and also manage multiple hosts from a single graphical user interface. ASM/ME is a component of the Host Integration Tools, so it gets installed when you install the Host Integration Tools. For instructions on installing the Host Integration Tools, see the *Host Integration Tools for Microsoft Installation and User's Guide*.

Functions Provided by ASM/ME

You can use ASM/ME to perform backup and recovery operations in both standalone and cluster environments, including Microsoft Hyper-V® CSV-enabled clusters. ASM/ME creates point-in-time, consistent copies (backups) of data stored on one or more PS Series groups. You can back up a single volume, or an entire database consisting of multiple volumes. The resulting backup is called a Smart Copy. A Smart Copy consists of the copy itself, as well as a backup document that describes the Smart Copy. If you configure your PS Series group for replication, you can use ASM/ME to create a disaster-tolerant storage environment.

While you create Smart Copies, all applications remain online and there is little impact on performance and computer availability. The time required for copying is minimized, and the data is always consistent and usable.

A Smart Copy can be one of three types—a snapshot, clone, or replica. After you have created a Smart Copy, you can restore it to recover data at any time. The Smart Copies created by ASM/ME are application consistent, which means that the Smart Copy will always be usable by Exchange®, SQL Server®, and Hyper-V after a restore operation.

You can use ASM/ME to create Smart Copies in several ways:

- On Demand—You can select a volume, application component, or collection in the ASM/ME GUI and immediately create a Smart Copy of it.
- Automated Schedule—You can select a volume, application component, or collection and then create a Smart Copy schedule for that object. A schedule will automate Smart Copy creation and allow you to control the timing, frequency, and number of retained copies.
- Scripts—You can use ASMCLI, the command line interface for ASM/ME, to write scripts for creating Smart Copies. See *Use a Script to Create Smart Copies on page 185*.

While ASM/ME enhances and supplements your regular backup regimen by providing fast and efficient data recovery, it is not a replacement for a regular and complete backup of your data to long-term media. You can use your backup software to transfer the data in Smart Copies to long-term backup media. Because the applications in your production environment remain online during such transfers, ASM/ME significantly reduces your planned computer downtime.

Supported Applications

ASM/ME supports Microsoft Exchange Server®, SQL Server®, SharePoint®, and Hyper-V®. See the *Host Integration Tools for Microsoft Release Notes* for a list of supported versions.

HIT Groups and Multiple Machine Management

You can manage multiple hosts from a single instance of ASM/ME. A group of one or more hosts that you are managing from ASM/ME is called a HIT Group. You can create a HIT Group on any machine that is running ASM/ME.

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 (including ASM/ME) automatically get installed on the host.

See *HIT Groups on page 47* for more information.

ASM/ME Smart Copies

While the Group Manager GUI allows you to create snapshots, clones, and replicas of volumes, ASM/ME provides the same capability, but additionally allows you to create snapshots, clones, and replica Smart Copies of Microsoft Exchange Mailbox Databases, SQL Server databases, and Hyper-V virtual machines. ASM/ME can also create Smart Copies of groups or collections of those objects.

You can use ASM/ME to create Smart Copies of the following objects:

- Volumes—PS Series volumes formatted using the NTFS file system. These iSCSI objects are represented by nodes in the ASM/ME Tree Panel under the `Volumes` list node.
- Application Components— of SQL Server databases, Microsoft Exchange Mailbox Databases, or Hyper-V virtual machines. Components are represented by nodes in the ASM/ME Tree Panel under the `Applications` list node. BecauseASM/ME supports Hyper-V, you can also create Smart Copies of virtual machines (VMs), VMs residing on CSVs, and CSVs themselves. See *Cluster Shared Volumes on page 122* for more information.
- Collections—Related groups of volumes or application components. Collections are represented by nodes in the ASM/ME Tree Panel under the `Collections` list node. For example, you can group multiple volumes or components together as a single collection, and then create a Smart Copy of the collection. This feature is useful when you want the Smart Copies to be created simultaneously in one set.

You can use either the ASM/ME GUI or the Group Manager GUI to view the snapshots, replicas, and clones created by a Smart Copy operation.

Smart Copy Types

A Smart Copy is one of three types:

- Snapshot—A point-in-time copy of a PS Series volume. Restoring a snapshot will restore the volume to the state represented by the snapshot.
- Clone—A new, independent volume containing the same data as the original volume at the time the clone is created. Since creating a clone creates a new, independent volume, you cannot restore a clone.
- Replica—A point-in-time copy of a PS Series volume. The original volume and the replica are located on different PS Series groups that might be separated by distance for disaster tolerance. The groups and the volume must be configured for replication.

For example, if you use ASM/ME for a snapshot Smart Copy operation on a volume, it results in a Smart Copy consisting of one snapshot with its associated backup document. However, if you use ASM/ME to perform a snapshot Smart Copy operation on a collection that consists of four volumes, it results in a Smart Copy comprised of four snapshots (one for each volume) and the associated backup document.

If you promote and mount a replica set, any additional replication attempts will be automatically canceled. However, you can also create a clone of any replica, and then mount the clone to access data. This feature allows replication to continue to the replica set.

Smart Copy Operations For Template and Thin Clone Volumes

A template volume is a read-only, thin provisioned volume from which you can create thin clone volumes. A thin clone volume has dependencies on its template volume. Template and thin clone volumes are useful in situations where you need to create multiple volumes that have common data. This common data can be written to a volume, and that volume can be converted to a template volume. Any thin clones created from the template volume will also have that common data, and then each thin clone volume can be modified as needed. See the *Dell EqualLogic Group Manager Administrator's Guide* for more information about thin clones.

ASM/ME supports the following operations on thin clone volumes:

- Taking a snapshot
- Replicating a thin clone volume
- Cloning a thin clone volume, which creates a new thin clone volume under the template volume

ASM/ME supports the following operations on template volumes:

- Creating a thin clone from the template volume
- Cloning the template volume, which results in a new template volume

Snapshots and replication of template volumes are not supported.

Robust Data Recovery

ASM/ME enables you to implement different data recovery strategies by recovering data directly from a Smart Copy. The principal methods of recovering data from Smart Copies are:

- In-Place Recovery—A full recovery method that restores all data in a volume. You can use this recovery option for snapshot Smart Copies of generic data volumes or for application components. Application components might consist of Microsoft Exchange Mailbox Databases, SQL Server databases, or Hyper-V virtual machines.
- Selective Component Recovery—A selective restore of files or components. Selective restore is supported only for components belonging to certain applications, and there are constraints on recovery methods and supported Smart Copy types. These constraints are identified in the chapter for each supported application.
- Manual Recovery—You can also use ASM/ME to mount a snapshot Smart Copy and manually copy over data from the mounted Smart Copy.

Rethin a Volume

On a PS Series group, the storage for a thin-provisioned volume is allocated incrementally as the volume uses more space. The full amount of space reserved for the volume is not immediately allocated when the volume is created. Over time, however, as data is written to thin-provisioned volumes, they lose their space efficiency because the group has no way to release storage that is no longer in use by the volume; for example, because files were deleted.

This version of the Host Integration Tools includes tools for rethinning thin-provisioned volumes, all of which require that the PS Series groups are running version 6.0 or higher (previous versions of the firmware lack support for the SCSI command used to rethin the volume). These tools are available on all supported operating systems.

- You can rethin a volume through the ASM/ME GUI, both as a one-time operation and through schedules. See *About Rethinning a Volume on page 56* and *Schedules for Volume Rethinning on page 63* for more information.
- The Host Integration Tools include a command-line utility called `eqlrethin.exe` (see the *Host Integration Tools for Microsoft Installation and User's Guide*).
- The Dell EqualLogic PowerShell® Tools include a cmdlet called `Invoke-RethinEqlVolume` (see the *Dell EqualLogic PowerShell Tools Reference Guide*).

The Host Integration Tools also includes a device driver for use only with Windows Server 2008 R2, that rethins the volumes in response to commands from the operating system. This driver does not run on any other version of Windows, and is not required to use any of the other rethinning methods listed above.

If you are running Windows 8 or greater or Windows Server 2012 or greater, the operating system performs rethinning by itself. Typically Windows will rethin the volume soon after a file is deleted.

The *Dell EqualLogic PS Series Storage Arrays Release Notes* discusses an issue with replicated volumes and volume rethinning, and recommends that you disable the SCSI unmap support in Windows 8 or greater and Windows Server 2012 or greater if you are using replicated volumes (including SyncRep). The release notes also recommend disabling automatic file system defragmentation in Windows Server 2012 or greater, and provides the steps on how disable both the unmap and the defrag features. However, if you disable the unmap support, the Host Integration Tools rethinning tools will not work; in that case, to rethin a volume, you must use the Disk Optimization tool built into Windows.

SAN Data Copy Offload

ASM/ME uses SAN Data Copy Offload to perform its selective restore operations. SAN Data Copy Offload is a Dell EqualLogic API that accelerates file copy operations by using SCSI Extended Copy commands. SAN Data Copy Offload frees up server resources and decreases the time it takes to perform selective restores.

For example, assume there are multiple volumes residing on a PS Series group. If those volumes are mounted on a Windows server, copying a file or directory from one volume to another formerly required the host to read the relevant data from one volume, and then write that data to the destination volume.

With SAN Data Copy Offload, the host now sends the SCSI Extended Copy command to the volume, and the data is copied to the destination volume within the group itself, thus consuming far less CPU bandwidth and memory.

If the SCSI Extended Copy operation fails for any reason, the standard copy command is automatically used. Users do not need to perform any tasks to enable this behavior.

Scripts and Command Generation

ASM/ME provides a command line interface, described in *Using the Command Line Interface on page 149*. The ASM/ME GUI provides an option to automatically generate the syntax for an ASM/ME command, based on the options that you select for an ASM/ME operation. For example, you can select a Smart Copy and then generate the syntactically-complete command for mounting it. (The option to generate the command is available in the menu bar or as a right-click menu option). You need to enter the command in the EqualLogic Power Shell.

See *Use a Script to Create Smart Copies on page 185* for how to integrate a Smart Copy schedule into your regular backup schedule script.

You can generate commands for the following ASM/ME operations:

- Create Smart Copy
- Checksum and Recovery
- Unmount and Logoff
- Mount
- Mount as Read-Only

- Restore All
- Selective Restore (Selective Restore is not available for Microsoft Exchange.)

Alerts and Event Notification

ASM/ME provides the following notification services:

- Email Notification

  You can configure ASM/ME to send email alerts when scheduled Smart Copy operations complete successfully or fail. You are also notified of the outcome of any scheduled Checksum Verification and Soft Recovery operations on Microsoft Exchange components. You configure Email notifications from the ASM/ME Settings page.

- Errors and Warnings Within ASM/ME

  ASM/ME displays errors (indicated by red circles) and warnings (indicated by yellow triangles) at the bottom right corner of the ASM/ME window. Click in the Error and Warning labels to view individual alerts.

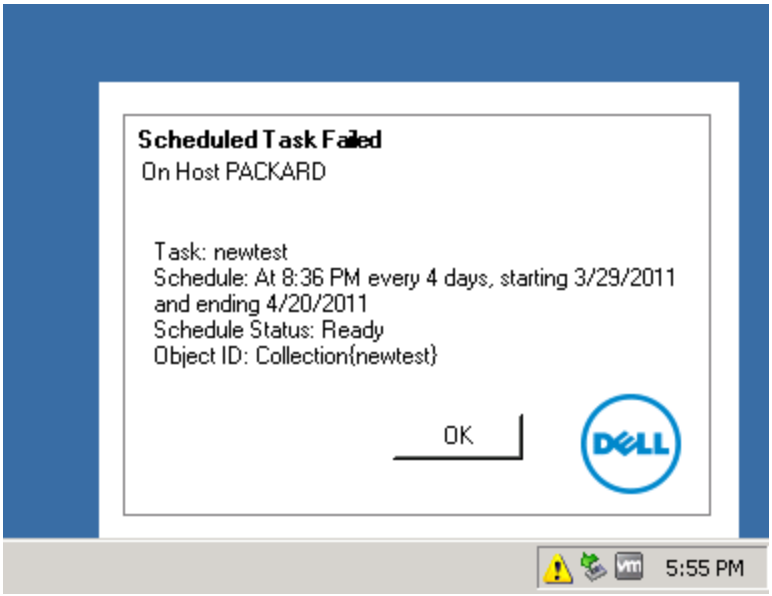
- Windows Event Log

  ASM/ME posts event messages to the Windows Event Log, which you can view by using the Windows Computer Management console.

- Windows Taskbar Notification (Figure 1)
  - ASM/ME places a yellow triangle warning icon in the Windows taskbar notification area (system tray) for notifications. Mousing over the yellow triangle will display the notification, and messages can be individually dismissed by clicking OK.
  - All schedule failures will also be reported in the Windows taskbar notification area (system tray). The message displays the schedule name, last run time, and other details about the failed schedule.
  - Failure to log in to the control volume on the PS Series group will also be reported in the system tray.

  You can dismiss all active system messages by using the `-shutdownsystray` parameter available in the ASMCLI.

Figure 1: Taskbar Notification



For example, when a Checksum Verification or Soft Recovery event occurs for Microsoft Exchange, you can mouse over the yellow icon to view details of the event. If a Checksum Verification and Soft Recovery operation fails, ASM/ME displays:

```
Exchange Verification Failed.

Checksum Verification and Soft Recovery failed for Smart Copy of Test taken at
2/25/2013 6:53:07 PM.

Check the System Event Log to determine the cause of the failure.
```

Remote Installations

You can install the Host Integration Tools (including ASM/ME) on remote hosts without having to log in to each host separately, run the installer on each host, and continuously monitor and respond to prompts typical of an installation wizard. Two methods for remote installations improve performance and save the amount of time typically required for large scale installations. These methods also allow you to upgrade the version of Host Integration Tools on each host:

- If you are managing a large number of hosts, you can install the Host Integration Tools on each host by using a PowerShell script called `HitRemoteInstall.ps1`, which is located in the directory that was specified when the Host Integration Tools were installed on the local host. (The default installation directory is C:\Program Files\EqualLogic\bin).
- You can also perform a remote installation by using the Add Hosts wizard in ASM/ME.

For more information about remote installations, see the *Host Integration Tools for Microsoft Installation and User's Guide*.

Failover Cluster Support

When installed on a computer that is a cluster node in a Microsoft failover cluster, you can use ASM/ME to perform certain operations on cluster resources owned by the installation node. In a cluster, you can access Smart Copy backup documents from any cluster node. In the event of a node failover, scheduled ASM/ME tasks will also fail over to the surviving node.

Dell recommends that you follow the Microsoft best practices for failover cluster configuration guidelines. See *Operations on Microsoft Failover Clusters on page 58* for more information.

ASM/ME and the Virtual Snapshot Service (VSS)

ASM/ME uses Microsoft Volume Shadow Copy Service (Microsoft VSS) to provide a framework for backing up and restoring data in the Windows Server environment. ASM/ME creates copies of application database volumes on your PS Series group, ensuring that the backed-up data is easy to restore and recover. When you use ASM/ME, the underlying Microsoft VSS operations are transparent and you make minimal use of Microsoft VSS utilities.

Figure 2 and Table 1 describe the relationship between ASM/ME and the Microsoft Windows operating system.

Figure 2: Relationship to the Microsoft VSS Copy Service

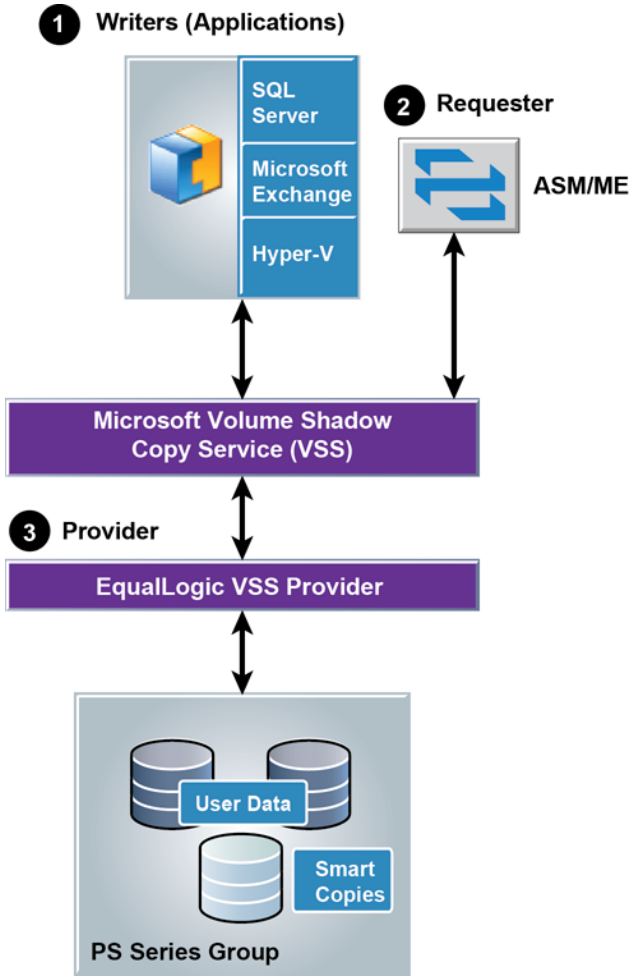


Table 1: ASM/ME Relationship to the Microsoft VSS Copy Service

Callout	Description
1	VSS Writer, integrated with the application, which prepares the application for the backup or restore operation. Supported applications are Microsoft SQL Server, Microsoft Exchange, Microsoft SharePoint (not shown in Figure 2), and Hyper-V.
2	VSS Requestor, usually a backup application, which requests the creation of shadow copies and provides an interface for backing up and restoring data. ASM/ME functions as a requestor.
3	VSS Provider, which is installed when you install the Host Integration Tools. The provider interacts directly with the PS Series group.

2 Configure ASM/ME

Before using ASM/ME, you should configure it and set your preferences for its operation at your site. Complete the tasks described in Table 2.

Table 2: ASM/ME Configuration Tasks

Task	Information
Install ASM/ME on a computer that meets the requirements in *Windows Computer Requirements on page 12*	*Host Integration Tools Installation and User's Guide*
Configure a PS Series group either by using Remote Setup Wizard or by using a serial cable and the `setup` utility	*Host Integration Tools Installation and User's Guide*
Create volumes on the SAN	Use the Group Manager GUI, or see the *Group Manager Online Help*.
Configure the correct access control records between the volumes and the group and the computer	*Required Access Controls on page 13*
Connect to the volumes through an iSCSI initiator	*iSCSI Target Connections on page 15*
Make the volumes accessible to the computer by formatting the partition, if necessary and assigning a mount point or drive letter (label)	*Volume Mount Point and Drive Letter Assignments on page 16*
(Optional) Start using the volumes for applications. For example, configure Microsoft Exchange or an SQL Server database on the volumes.	For best results, follow the guidelines in *Torn Smart Copies on page 65*

PS Series Group Requirements

The PS Series group must meet the requirements described in Table 3 for use with ASM/ME.

Table 3: PS Series Group Requirements

Requirement	Description
PS Series group should be running the required firmware revision	Groups must run under the firmware revision specified in the *Host Integration Tools for Microsoft Release Notes*.
Sufficient snapshot reserve space	Volumes must have snapshot space reserved to create snapshots. Refer to the *Dell EqualLogic Group Manager Administrator's*

Requirement	Description
	Guide.
Replication configuration	To create volume replicas, you must have the group and volume configured for replication. Refer to the Dell EqualLogic Group Manager Online Help.

Windows Computer Requirements

The Windows computer on which you want to run ASM/ME must meet the requirements described in Table 4 to create Smart Copies in a PS Series group.

Table 4: Requirements for Creating Smart Copies

Requirement	Description
Supported Environment	Make sure that your computer meets the requirements specified in the *Host Integration Tools for Microsoft Release Notes*.
Microsoft iSCSI Software Initiator	You must install the service portion of the Microsoft iSCSI Software Initiator, even if you are not using the initiator for iSCSI traffic. A supported version is provided with the Host Integration Tools kit, and is available on the Microsoft website.
Microsoft server (VSS or VDS) access to the group	Microsoft services running on the computer must have access to the group. See *Microsoft VSS/VDS Service Access to the Group on page 14* for more information.
iSCSI access to the volumes	The computer must have the group IP address configured as an iSCSI discovery address. In addition, to connect to an iSCSI target associated with a volume or snapshot, the computer must match one of the volume's access control records configured in the group. See *Access to Volumes and Snapshots on page 14* for information on setting up access control records in a group.
SMP configuration (Windows Server 2012 or greater and Windows 8 or greater)	If you are running Windows Server 2012 or greater or Windows 8 or greater, you must configure SMP access to the group. For these operating systems, SMP replaces VDS. See the *Host Integration Tools for Microsoft Installation and User's Guide*.

Required Access Controls

To make sure that you have the correct access controls between a computer and a new PS Series group, use the Remote Setup Wizard to create the group. Alternatively, if you have an existing PS Series group, use the ASM/ME GUI to configure access to the group. Table 5 lists the access controls required by ASM/ME.

Table 5: Required Access Control

Access Type	Description
Group IP address as iSCSI target discovery address	Enables the computer to discover targets available on a PS Series group. Configure the group IP address as a discovery address in the iSCSI initiator management interface using one of the following methods: • Use the Remote Setup Wizard to create a group, which also configures the group IP address as the Discovery address. See the *Host Integration Tools for Microsoft Installation and User's Guide* for more information. • Use the ASM/ME GUI to configure computer access to a group. See *About PS Group Access Settings on page 26* for more information. • Manually add the group IP address to the initiator iscovery list.
VSS/VDS access	Microsoft services running on a computer must be able to automatically log in to the vss-control volume on the computer. A VSS/VDS access control record must exist on the group, and the computer must have access credentials, configured through Remote Setup Wizard or ASM/ME, that match the record. Usually, CHAP credentials are used. See *Microsoft VSS/VDS Service Access to the Group on page 14* for more information.
Volume access	To create Smart Copies of a volume, the computer must be logged in to the volume. To log in, the computer must present credentials that match one of the volume's access control records. If CHAP is used, the computer must specify the CHAP credentials when logging in to the volume. If the volume was created using Storage Manager for SANs, the access controls between the computer and target are set up automatically. See *Access to Volumes and Snapshots on page 14* for more information.
Global Smart Copy access on other computers (Optional)	To allow a computer to import Smart Copies from a different computer than the one that created them, you can set up access controls that enable other computers to access the Smart Copies. Specify the global Smart Copy access credentials by selecting PS Group Access, then Smart Copy access in the ASM GUI. See *PS Group Access Settings on page 27* for more information.

Access Type	Description
Smart Copy access on the computer	When a computer attempts to import a Smart Copy, it must automatically present credentials that match one of the Smart Copy's access control records. Specify the global Smart Copy access credentials by selecting PS Group Access, then Smart Copy access in the ASM GUI. When you perform this operation on a computer that did not create the Smart Copy, use the same CHAP credentials set for global Smart Copy access on the originating computer. See *PS Group Access Settings on page 27* for more information.

Microsoft VSS/VDS Service Access to the Group

If a computer will be creating or importing Smart Copies, you must make sure that Microsoft services (VSS and VDS) that are running on the computer are able to access the PS Series group without user intervention.

In a group, VSS/VDS access control records are used to restrict Microsoft service access to the PS Series group, according to IP address, iSCSI initiator name, CHAP credentials, or any combination of the three. A computer must meet all the requirements in one record in order for Microsoft services to access the PS Series group.

To ensure that the Microsoft services have access to a PS Series group:

- If the PS Series group has not been initialized, use the Remote Setup Wizard on the computer to initialize an array and create a new group. The wizard will set up a VSS/VDS access control record and local CHAP account in the group and also configure matching CHAP credentials on the computer. See *Host Integration Tools Installation and User's Guide* for more information.
- If the PS Series group is already initialized, use the ASM/ME GUI to configure computer access to an existing group. See *About PS Group Access Settings on page 26* for more information.

Access to Volumes and Snapshots

A computer must be connected (logged in) to the PS Series group volumes for which it will be creating Smart Copies. You can use the iSCSI initiator control panel to log in to the volume. If you use CHAP for authentication, you must supply this information when logging in to the volume.

You can launch the iSCSI initiator control panel from ASM/ME by clicking `Launch`, and then `iSCSI Control Panel`.

In addition, when a computer imports a Smart Copy, it must be able to connect (log in) to it without user intervention.

For a computer to discover the iSCSI targets (volumes or snapshots) in a PS Series group, you must configure the group IP address as the iSCSI discovery address. You can run the Remote Setup Wizard on the computer to initialize an array and create or expand a PS Series group or to configure computer access to the group. You can also specify the iSCSI discovery address by using the iSCSI initiator control panel.

A PS Series group uses access control records to restrict computer access to a volume or its snapshots. A record (up to 16 for a volume and its snapshots) can restrict access according to IP address, initiator name, CHAP user name (and password), or any combination of the three. A computer must meet all the requirements in a record to access the volume or snapshot.

By default, a volume and its snapshots share a list of access control records. A record can apply to the volume, the volume snapshots, or both. For example, you could create one record that allows access only to the volume and create another record that allows access only to the volume snapshots.

The following methods ensure computer access to a volume or its snapshots:

- If you create a volume with Storage Manager for SANs, it automatically sets up matching access controls in the PS Series group and on the computer. No further action is needed to ensure computer access to the volume or its snapshots.
- If you create a volume with the Group Manager GUI or CLI, you must manually set up one or more access control records that enable computer access to the volume or its snapshots. Also, if you are using CHAP to restrict computer access, you must set up a local CHAP account or configure a RADIUS server that already has the CHAP account configured. See the *Dell EqualLogic Group Manager Administrator's Guide* for more information about setting up access control records and creating local CHAP accounts.

  On the computer, if CHAP is required for computer access to the volume, you can supply the CHAP user name and password in the iSCSI initiator control panel when logging in to the volume. If CHAP is required for computer access to volume snapshots (for importing), you must use the ASM/ME or the Remote Setup Wizard to specify the CHAP user name and password. The computer will automatically use this CHAP user name and password when importing any Smart Copies from the PS Series group. See *About PS Group Access Settings on page 26* for more information.

iSCSI Target Connections

Use the iSCSI initiator console to log in to a PS Series group volume or snapshot (iSCSI target). For discovery, the group IP address must be configured as the iSCSI target discovery address.

To log in to a volume, the computer must match an access control record that is configured in the group, as described in *Access to Volumes and Snapshots on page 14*. If access to the volume is being authenticated with CHAP, enter the correct CHAP user name and password in the iSCSI initiator console when logging in to the volume. After you are logged in to a volume, the volume appears as a regular iSCSI disk.

Volume Mount Point and Drive Letter Assignments

To make a volume accessible to the computer, you can use Windows utilities to assign either a drive letter or a mount point to it. A mount point is a drive attached to an empty folder on an NTFS volume. A mount point functions the same as a normal drive, but is given a label or name instead of a drive letter. Although Windows allows you to mount a volume on multiple mount points, you should mount a Smart Copy only on a single mount point. Unmounting a volume or Smart Copy using ASM/ME unmounts all existing mount points.

To assign a drive letter or mount point using Windows Server:

1. Select the Windows Disk Management utility.
2. Right-click the volume.
3. Follow the wizard to assign a drive letter or mount point.

Windows also supports a command-line utility called `mountvol.exe` for assigning mount points and drive letters to a volume. See your Windows documentation for details.

Mount Point Constraints in Cluster Environments

In a cluster, the use of drive letters for a volume operation (such as mounting a snapshot or creating an RSG) is subject to the following restrictions:

- ASM/ME excludes drive letters that are used by (potentially) failed-over disks.
- ASM/ME excludes the drive letter assigned to the quorum disk.

After you have mounted your volumes, you can then use your application to create a database on one or more volumes.

Dell recommends following best practices when configuring databases on volumes. See *Torn Smart Copies on page 65* for more information.

Windows Server prevents you from switching mount points between clustered and non-clustered disks. If the volume containing the mount point is a clustered volume, but the Smart Copy that you are attempting to mount is not a clustered volume then the mount operation fails. ASM/ME displays an error message informing you that the mount operation is unsupported.

For example, ASM/ME does not support either of the following operations:

- Using the system drive (`C:\`) to host a mount point for a volume, which is set as a clustered disk
- Using a clustered volume (`X:\`) to host a new volume that is not set as a clustered disk

Consider this constraint carefully when applying recovery strategies for Microsoft SQL Server and for Microsoft Exchange Server. For more information, see the following Microsoft Knowledge Base articles:

- http://support.microsoft.com/kb/280297
- http://support.microsoft.com/kb/947021

ASM/ME Settings

If you are managing more than one host, you can change the ASM/ME settings (Table 6) on multiple hosts at once. Use only ASCII characters when specifying CHAP credentials, PS Series group names, member names, administrative passwords, and group membership passwords.

Table 6: ASM/ME Settings

Setting Type	Description
General Settings	Enables you to control general ASM/ME behavior, such as: • The default location of backup documents and collection files • Whether to automatically validate the Smart Copies when ASM/ME is started, enable iSCSI portal verification, set Smart Copies online as they are created, and other options • Specify how to run the ASM services See *General Settings on page 18*.
Notification Settings	Enables you to specify where to send email notification of completed scheduled operations. See *Notification Settings on page 21*.
Alert Settings	Enables you to receive Critical, Warning, and Informational email alerts when certain tasks succeed of fail. See *Alert Settings on page 22*.
Verification Settings	Enables you to specify a preferred period in which ASM/ME performs regularly scheduled operations such as Checksum Verification. See *Verification Settings on page 25*.
PS Group Access Settings	Enables you to configure access to one or more PS Series groups for creating and managing Smart Copies, and other functions. See *About PS Group Access Settings on page 26*.
MPIO Settings	Enables you to specify MPIO settings such as the failover policy, connection attributes, and IP version. See *MPIO Settings on page 30*.

General Settings

The General Settings panel (Table 7) enables you to control the general behavior and options for ASM/ME on all hosts.

If you are managing multiple hosts and want to make the same changes to multiple hosts, multiselect the hosts in the middle panel. The changes will affect all selected hosts. To restore settings to their current saved state, click `Discard`.

Table 7: General Settings

Option	Description
Auto-Snapshot Manager Document Directory	Specify the location for the folder that will store the backup documents. The default directory is C:\ProgramData\EqualLogic\VSS Requestor\. A non-clustered host should have its own backup document directory for storing backup documents. If you want to use a shared Windows directory for a non-clustered host, you must use a subdirectory within the shared directory. If host A and host B (both non-clustered hosts) store their backup documents on a shared directory, they should each store them in their own subdirectories. For example, Host A would store them on \\server\share\subdirectory1, and Host B would store them on \\server\share\subdirectory2. Do not change the location of Smart Copy documents if you have configured remote verification. See *Run Checksum Verification and Soft Recovery on a Remote Host on page 91*. Cluster nodes must always use a shared folder so it can be accessed from all nodes, and the same exact backup document directory path must be used. The only exception to this is Exchange CCR or DAG clusters. For example, if Node 1 stores backup documents on \\server\share\subdirectory1, then Node 2 must also store backup documents on \\server\share\subdirectory1. For clusters, you must enter the UNC-format name of this network shared folder, in a format such as: \\ClustersystemFS\H$\VSS Requestor\
Enable Smart Copy validation on connect	Specifies whether to automatically validate the Smart Copies when ASM/ME is started. Validation verifies that the Smart Copies described in the backup documents still exist on the PS Series group. Dell recommends that you enable this setting because it can help you detect problems.
Enable iSCSI portal verification during discovery	Specifies whether ASM/ME will check that it can connect to arrays to which it previously connected when last active. Dell recommends that you enable this setting because it can help you detect problems.
Show Smart Copy conversion wizard if older Smart Copies are found	Specifies whether to automatically launch the conversion wizard if ASM/ME finds Smart Copies that you created by using an older version of ASM/ME.

Option	Description
Create Smart Copies online	When Smart Copies are created, ASM/ME creates them in an offline state on the PS Series group, and automatically sets them online when mounting them. Select this option if you want Smart Copies to be set online in the PS Series Group after they are created. You need to select this option if you create Smart Copies with ASM/ME Version 3.4 or later and mount them on another Windows computer running an older version of ASM/ME.
Check cluster access to Backup Document directory on connect	Check this option to verify that the cluster node can access the backup document directory.
Warn if VSS Requestor is not logged into cluster properly	Check to receive a warning notification if the VSS Requestor is not properly logged in to the cluster.
Run ASM Services As	You can run ASM services (ASM Agent and VSS Requestor services) from the local system user account, or another specified user account. If you want to specify another user, you must provide the domain, username, and password credentials. See also *Managing the ASM Services on page 21*.

About the Backup Document Directory

Every Smart Copy and collection has a corresponding backup document, which can be used to import Smart Copies on different hosts. You can specify the location for the parent folder, whether that parent folder is a UNC path in the cluster environment or a regular file path in the normal environment, that will store these documents. If you intend to import Smart Copies on different hosts, consider specifying a shared file system accessible to all the computers that may import the transported Smart Copy Sets.

A backup document must exist on a computer for ASM/ME to access the Smart Copy. If a Smart Copy consists of multiple components, the associated backup document will describe each component in the Smart Copy. For example, assume you create a collection of volumes. If you take a snapshot of that collection, the resulting Smart Copy will consist of snapshots of different volumes. The Smart Copy's associated backup document will then describe each snapshot in the Smart Copy.

Backup documents that were not created by or imported to a host will display a warning message on the Smart Copies list node, and the Smart Copies represented by that backup document will not be displayed.

If you change the location of the backup document directory, backup documents that were created on or imported to the host are moved (copied to the new location and removed from the source location). Collections that were created or modified by the current host are also moved. Untagged collections (those for which the original host cannot be determined) are copied to the new location, but also left in the original location.

Backup Document Directories for Standalone (Non-Clustered) Hosts

A host that is not part of a cluster or a SharePoint farm should have its own backup document directory for storing backup documents. These hosts should not use the same directory for storing their backup documents. If you want to use a shared Windows directory for a standalone host, you must use a subdirectory within the shared directory. If host A and host B (both standalone hosts) store their backup documents on a shared directory, they should each store them in their own subdirectories. For example, Host A would store them on `\\server\share\subdirectory1`, and Host B would store them on `\\server\share\subdirectory2`.

Backup Document Directories For Clusters and SharePoint Farms

With the exception of Exchange Data Availability Group (DAG) clusters, cluster nodes and hosts in a SharePoint farm must always share the same backup document directory path. For example, if Node 1 stores backup documents on `\\server\share\subdirectory1`, then Node 2 must also store backup documents on `\\server\share\subdirectory1`.

In a cluster, you can specify a directory as a non-clustered or clustered resource. You must first use Windows cluster utilities to create the folder and make it available to the cluster nodes.

If you specify a shared folder located on a clustered iSCSI volume, you can create Smart Copies of that volume, but cannot restore data from the volume (otherwise the folder might be overwritten).

In a cluster, these properties must be set on each node in the cluster that will be performing ASM/ME operations.

Set the Backup Document Directory

1. In the navigation area, click `Settings`.
2. Click on the `General Settings` tab. If you are managing multiple hosts and want to make the same changes to multiple hosts, multiselect the hosts in the middle panel. The changes will affect all selected hosts.
3. Specify a directory for backup documents.

   a. For a single-system configuration, you can change the location of Auto-Snapshot Manager Document Directory. Do not change the location of Smart Copy documents if you have configured remote verification. See *Run Checksum Verification and Soft Recovery on a Remote Host on page 91*.

   b. If you have a cluster, backup documents should use a network shared folder. ASM/ME expects you to enter the UNC-format name of this network shared folder, in a format such as:

      `\\ClustersystemFS\H$\VSS Requestor\`

      The network shared folder is accessed from all cluster nodes.

4. Specify any other options listed and click `Save`.

To restore settings to their current saved state, click `Discard`.

Managing the ASM Services

You can choose to run the ASM Services on a local system or as a specified user of a domain. You must add the host running ASM/ME to the domain and enter a user name and password.

If you plan to use Single Sign-On (SSO), the ASM Services must be configured to use accounts with domain access.

See *Edit ASM/ME Settings on Hosts in a HIT Group on page 54*.

Notification Settings

The Notification Settings panel (Table 8) allows you to configure email settings so that you can send or receive email alerts when certain operations complete or fail. This page also allows you to specify whether or not to receive email alerts at all. To view the actual list of available alerts, or to enable or disable specific alerts, click `Alert Settings`.

If you are running a cluster, you should set up email notification for every node in the cluster. Jobs run on the node that currently owns the cluster resource, and the node that owns the cluster resource can change.

For the list of available alerts, see *Alert Settings on page 22*.

Table 8: Email Notification Settings

Option	Description
Send email alerts checkbox	Check this box to receive email about alerts. To specify which alerts will be emailed, see *Alert Settings on page 22*
SMTP Server	IP address of the SMTP server in your environment. You must specify a server that will send email alerts.
SMTP Failback Port	Default port is 25. If the connection port on your SMTP server is not 25, enter the value here.
Email Recipient List	Enter all the email addresses, in a comma-separated list, for the people you want to receive email about alerts.
Email From Address	Enter the sender's email address. This address is the one that the alert emails come from. You can enter any name, even one that does not exist in your Active Directory database, such as "alerts_on_*hostname*."
Subject Line Prefix	Enter a string of text that will form the subject line of the emails. The default is HIT/Microsoft Alert, but you can change it to anything else that is meaningful to you.

Option	Description
Send test email button	Click this button to verify that the email notification settings are entered correctly. You might want to change the subject line prefix for this test, then change it after the test to a subject line for regular alert emails. If the email is not received, verify that the above email settings are correct. If you use automated processing of incoming mail, (such as junk mail processing), configure the recipient mail account to make sure that notifications are handled appropriately.
Discard and Save buttons	Click `Discard` to erase all the settings you entered, or `Save` to save them.

Configure Notification Settings

1. In the navigation area, click `Settings`.
2. Click on the `Notification Settings` tab. If you are managing multiple hosts and want to make the same changes to multiple hosts, multiselect the hosts in the middle panel. The changes will affect all selected hosts.
3. Specify the required information. Press F1 to view online help for the settings.
4. Click `Save`.

To restore settings to their current saved state, click `Discard`.

Alert Settings

The Alert Settings panel enables you to enable or disable all email alerts, or specify a subset of alerts that will be emailed to you. The default settings are to receive all critical and warning alerts, and no informational alerts. You must configure email settings in order to receive email alerts. See *Notification Settings on page 21* for information about configuring email.

Alerts are issued:

- When scheduled Smart Copy operations either succeed or fail. See *About Schedules on page 61*.
- When MPIO-related tasks fail

In addition to email alerts, the ASM/ME GUI displays errors and warnings when a Smart Copy creation cannot complete because snapshot reserve space, free pool space to clone a Smart Copy, or replica reserve space is low on your PS Series group.

To configure alerts, see *Configure Alert Settings on page 25*.

You can also control alerts using ASMCLI. Enabling or disabling alerts through ASMCLI automatically sets the corresponding alerts in the GUI, and enabling or disabling alerts in the GUI updates the alert status when you view alerts through ASMCLI. See *ASMCLI -alert on page 166* for more information about the command for setting alerts.

Table 9 describes all the Critical alerts that can be triggered in ASM/ME, and whether or not those alerts are enabled by default.

Table 9: Critical Alerts

Alert Name	Description	Default
Smart Copy Creation Failed	Triggered when Smart Copy creation fails for a schedule.	Yes
Collection Missing Dependencies Error	Triggered when a collection is missing component or volume dependencies.	Yes
Collection Multiple Writers or Component Error	Triggered when a component contains multiple application writers or a component error occurred preventing an operation.	Yes
ASMCLI Initialization Failed	Triggered when ASMCLI initialization fails.	Yes
Smart Copy Mount Failed	Triggered when an attempt to mount a Smart Copy fails.	Yes
Volume Unmount Failed	Triggered when an attempt to unmount a volume fails.	Yes
Smart Copy Delete Failed	Triggered when an attempt to delete a Smart Copy fails.	Yes
Restore Failed	Triggered when an attempt to restore a volume from Smart Copy fails.	Yes
Get Property Failed	Triggered when an attempt to extract properties from a volume collection or any other object fails.	Yes
Exchange Verification Failed	Triggered when Exchange verification fails.	Yes
Many Concurrent Verification Tasks	Triggered when Exchange verification discovers more then allowed concurrent verification tasks.	Yes
MPIO CHAP Creation Failed	Triggered when MPIO service fails to initialize CHAP.	Yes
MPIO CHAP Authentication	Triggered when MPIO CHAP authentication	Yes

Alert Name	Description	Default
Error	fails.	
MPIO No Adapters Available	Triggered when no adapters are available for MPIO use.	Yes
MPIO Reconfiguration Request IPC Error	Triggered when a reconfiguration request IPC error is encountered.	Yes
MPIO No Active Paths	Triggered when there are no active paths for an MPIO session.	Yes
MPIO Logout Error	Triggered when a logout error for MPIO session is encountered.	Yes
MPIO Login without CHAP Credentials	Triggered when a login without CHAP credentials is attempted.	Yes

Table 10 describes all the Warning alerts that can be triggered in ASM/ME, and whether or not those alerts are enabled by default.

Table 10: Warning Alerts

Alert Name	Type	Description	Default
Snap Reserve Warning	Warning	Triggered when one or more groups are running low on snapshot reserve space.	Yes
Clone Space Warning	Warning	Triggered when one or more groups are running low on free space. Cloning a volume or replica uses the same amount of space as the original volume or replica.	Yes
Replica Reserve Warning	Warning	Triggered when one or more groups are running low on replica reserve space.	Yes

Table 11 describes all the Informational alerts that can be triggered in ASM/ME, and whether or not those alerts are enabled by default.

Table 11: Informational Alerts

Alert Name	Type	Description	Default
Smart Copy Creation Succeeded	Information	Triggered when an attempt to create a Smart Copy succeeds.	Yes

Alert Name	Type	Description	Default
Smart Copy Mount Successful	Information	Triggered when an attempt to mount a Smart Copy succeeds.	Yes
Volume Unmount Successful	Information	Triggered when an attempt to unmount a volume succeeds.	Yes
Smart Copy Delete Successful	Information	Triggered when an attempt to delete a Smart Copy succeeds.	No
Restore Successful	Information	Triggered when an attempt to restore a volume from Smart Copy succeeds.	No
Exchange Verification Succeeded	Information	Triggered when Exchange verification succeeds.	No

Configure Alert Settings

1. In the navigation area, click `Settings`.
2. Click the `Alert Settings` tab. For information about the types of alerts, see *Alert Settings on page 22*
3. Select or deselect the check boxes next to each alert and click `Save`. Press F1 to view online help for the Alert Settings page.

   If you are managing multiple hosts and want to make the same changes to multiple hosts, multiselect the hosts in the middle panel. The changes will affect all selected hosts. If any settings differ across the hosts, they will be highlighted. To restore settings to their current saved state, click `Discard`.
4. [Optional] In the Advanced Options area, for each alert type, click `Enable All`, `Disable All`, or `Restore to Default` and then click `Save`.
5. Configure the notification settings so you can receive email notifications when alerts are triggered. See *Notification Settings on page 21* for more information.

To restore settings to their current saved state, click `Discard`.

Verification Settings

The Verification Settings panel (Table 12) applies only to Microsoft Exchange, and allows you to configure Checksum Verification and Soft Recovery on Smart Copies of Microsoft Exchange components (Mailbox Databases for Exchange 2010 and 2013).

If you are managing multiple hosts and want to make the same changes to multiple hosts, multiselect the hosts in the middle panel. The changes will affect all selected hosts. To restore settings to their current saved state, click Discard.

If you are running a cluster configuration, you should consider setting verification email notices for each node in the cluster.

Table 12: Verification Settings

Option	Description
Exchange Global Verification Window	End time must be at least three hours later than the start time. Dell recommends that you specify a range of time that corresponds with a period of low computer usage (off-peak times) to make best use of computer resources.
Verify newest Smart Copies first	Verifies the Smart Copies beginning with the chronologically most recent and ending with the oldest
Send email when verification time exceeds creation interval	Causes a notification email to be sent to the default email account if the time required to complete an operation exceeds the schedule's frequency of Smart Copy creation
Combine creation and verification emails when possible.	Enables you to concatenate emails to reduce the volume of mail

Configure Verification Settings

1. Click Settings, then Verification Settings.
2. In the Global Verification Window area, select the start and end time to perform verification.
3. (Optional) In the Verification Processing Order area, select the option to verify the newest Smart Copies first, before verifying others.
4. (Optional) In the Email Options area, select the option to send email when the verification takes longer than the interval you specified in step 2 to perform verifications, and (also optionally), select the option to combine emails into as few messages as possible.
5. Click `Save`.

If you are managing multiple hosts and want to make the same changes to multiple hosts, multiselect the hosts in the middle panel. The changes will affect all selected hosts. To restore settings to their current saved state, click `Discard`.

About PS Group Access Settings

You must configure access to one or more PS Series groups for ASM/ME to connect to for creating Smart Copies and other functions.

If you used the Remote Setup Wizard to create a group, that group will be displayed in the PS Group Access window. You can add more groups or delete groups as needed.

Group access settings can be specified for the following purposes:

- Allowing ASM/ME access to one or more PS Series groups for creating and managing Smart Copies, among other functions.
- Microsoft VDS and VSS CHAP settings enable these services to access to a PS Series group.
- Smart Copy access can enable the local computer to access Smart Copies created on other computers.
- PowerShell/SMP access can authenticate PowerShell and SMP access to the group. SMP access replaces VDS access for the Windows Server 2012 or greater and Windows 8 or greater operating systems.
- (Optional) Enabling Single Sign-On (SSO) to the group.

Before setting these properties, CHAP must be configured on the PS Series group, either locally or on an external RADIUS authentication server. For information about configuring CHAP on the PS Series group, see the *Dell EqualLogic Group Manager Administrator's Guide*.

PS Group Access Settings

The PS Group Access panel (Table 13) enables you to configure settings for the PS Series groups that store the volumes and Smart Copies used by your applications.

Table 13: Options for the PS Group Access Panel

Option	Description
PS Group Name	PS Series group name
Group IP	PS Series group address, in either IPv4 or IPv6 format
VSS/VDS Access Settings	The Microsoft Virtual Disk Service (VDS) and Volume Shadow Copy Service (VSS) must be able to access the PS Series group. These credentials must match the VSS/VDS access control record specified in the PS Series group. To find the user-name and password information for the PS Series group, start the Group Manager GUI, click Group Configuration, then click the VSS/VDS tab. User name: Enter the user name already configured on the group. Password: Enter the password for the specified user name.
Using CHAP credentials for iSCSI discovery	Select this option to specify that CHAP credentials must be supplied during discovery, and the computer will discover only those targets for which it is authorized. If PS Series groups accessible by this computer are configured to prevent unauthorized hosts from discovering their targets, you must select this option. If not, do not select this option. To display the local CHAP account in the group, start the Group Manager GUI, click Group Configuration, then click the iSCSI tab.

Option	Description
Smart Copy access	If you are importing Smart Copies created on a different computer, you must have the appropriate credentials to access those Smart Copies. These credentials will be the same as the global CHAP credentials on the originating computer.
PowerShell/SMP access	PS Group Management IP: Enter the group IP address or the management IP address (if configured on the PS Series group). PS Group Username: Enter a valid administrator account user name that is already configured on the group (such as grpadmin). PS Group Password: Enter the password for the specified administrator account. Optional: Select the option to use Single Sign-On (SSO), if configured on the group. **Note:** Selecting this option dims the PS Group Username and PS Group Password fields. They are not needed if you are using SSO.

Configure PS Group Access

1. In the navigation area, click `Settings`.
2. Click the `PS Group Access` tab.
3. Click `Add PS Group`.
4. In the Group Settings panel, enter the group name and IP address in the fields.
5. If your host system uses HBAs on a dedicated network (instead of a software initiator) to access your groups, check the box to `Use Host Bus Adapters`.
6. Click `Save`. Press `F1` to view online help for any of these dialog boxes.

If you are managing multiple hosts and want to make the same changes to multiple hosts, multiselect the hosts in the middle panel. The changes will affect all selected hosts. To restore settings to their current saved state, click Discard.

VSS/VDS Settings

On the PS Group Access panel, the VSS/VDS settings area enables you to configure the VSS and VDS services, on which ASM/ME depends to function properly. Microsoft VDS and VSS services running on a computer must be able to automatically access a PS Series group. A VSS/VDS access control record must exist in the group, and the computer's VSS/VDS access control credentials must match the credentials on the PS Series group. CHAP credentials are typically specified for VSS/VDS access.

If you used the Remote Setup Wizard to create a group or set up computer access to the group, VSS/VDS access between the computer and group is already set up.

If VDS/VSS access is not configured, the VDS/VSS access node displays a warning icon (yellow triangle). When configured, the icon changes to a green check mark.

See the *Dell EqualLogic Group Manager Administrator's Guide* for information about setting up VSS/VDS access control records.

Configure VSS/VDS Access Settings for the Local Host

1. In the navigation area, click `Settings`.
2. Click the `PS Group Access` tab.
3. Select the relevant group and click `VDS/VSS access`.
4. Enter the relevant VDS/VSS Access credentials and click `Save`. Press F1 to view online help for any of these dialog boxes.

In a cluster, this must be done on each cluster node that will be accessing a PS Series group.

Smart Copy Access

On the PS Group Access panel, the Smart Copy Access settings enable you to configure hosts to access Smart Copies created on a different host.

When a local host imports a Smart Copy created on a different host, the local host must automatically present the appropriate access credentials required for accessing the imported Smart Copy.

In this case, you should specify the Global CHAP credentials that were configured on the originating computer.

Configure Smart Copy Access

1. In the navigation area, click `Settings`.
2. Click the `PS Group Access` tab.
3. Select the relevant group and click `Smart Copy access`.
4. Enter the relevant Smart Copy Access credentials and click `Save`. Press F1 to view online help for any of these dialog boxes.

PowerShell and SMP Access

On the PS Group Access panel, the PowerShell/SMP Access settings enable you to configure access to a PS Series group to:

- Use the PowerShell tools with a particular PS Series group. The PowerShell cmdlets use different credentials from those that ASM/ME uses. You must configure PowerShell/SMP access if you want to use the PowerShell tools.
- Use ASM/ME with a host running Windows Server 2012 or greater or Windows 8 or greater
- Enable Single Sign-On (SSO) to a group

Configure PowerShell/SMP Access

1. In the navigation area, click `Settings`.
2. Click the `PS Group Access` tab.
3. Select the relevant group and click `PowerShell/SMP access`.
4. Enter the group management IP address (this is the group IP address, unless the group has a management network configured).
5. (Optional) Check the box to enable Single Sign-On. If checked, no user name or password is required.

   Note: To use Single Sign-On, the PS Series group must be running a minimum of PS Series firmware version 6.0, and must be configured to allow SSO. See the Dell EqualLogic Group Manager Online Help for information about configuring the group for Single Sign-On. In addition, the ASM service must be configured to use accounts with domain access. See *General Settings on page 18* and *Managing the ASM Services on page 21* for more information.

6. If you choose not to use Single Sign-On, enter the user name and password for the group. The user name can be an account configured on the group or a domain account. Then, click `Save`. Press F1 to view online help for any of these dialog boxes.

MPIO Settings

The MPIO Settings panel (Table 14) enables you to:

- Control the failover policy
- Manage the connection attributes
- Specify the Internet Protocol version and whether to include or exclude a subnet

Before setting these properties, you must install the Dell EqualLogic MPIO and configure EHCM service for the group. For information about installing MPIO, see the *Host Integration Tools for Microsoft Installation and User's Guide*.

Table 14: MPIO Settings

Option	Description
Fail Over Policy	Enables you to configure DSM to balance data traffic loads across the pathways
MPIO Connections	Enables you to choose whether or not to use MPIO for snapshots and to specify the number of sessions per volume and volume slice
Network Connections	Enables you to choose between IPv4 and IPv6, choose whether or not to

Option	Description
	exclude new subnets, and select a minimum adapter speed
Included Networks	Enables you to include or exclude subnets on a given network for a host
Excluded Networks	Displays the excluded subnets. Depending on the IP version selection in the Network Connections panel, you can include a network in this list.

Configure MPIO Settings

1. In the navigation area, click `Settings`.
2. Click the `MPIO Settings` tab.
3. In the Running MultiPath Status panel, make sure the EqualLogic MPIO is installed and the EHCM service is running.
4. Change the settings in the following areas as needed:
   - Fail Over Policy. For more information, see *Configure Failover Policy Settings on page 31*.
   - MPIO Connections. For more information, see *Configuring MPIO Connections Settings on page 32*.
   - Network Configuration. For more information, see *Configure the Network on page 32*.
   - Network Connections. For more information, see *Configure the Network Connections on page 32*.
5. Click `Save`. Press `F1` to view online help for any of these dialog boxes.

If you are managing multiple hosts and want to make the same changes to multiple hosts, multiselect the hosts in the middle panel. The changes will affect all selected hosts. To restore settings to their current saved state, click Discard.

Configure Failover Policy Settings

When you have configured multiple data pathways, it is appropriate to configure MPIO DSM to balance data traffic loads across the pathways. Choose from:

- Least Queue Depth—(Recommended) MPIO DSM sends SAN data traffic packets out to each available connection, with preference given to the connection that is least busy at the time it requests the I/O. This option is appropriate for most installations.
- Round Robin—MPIO DSM sends SAN data traffic packets over each available connection in a rotating sequence, fully utilizing all available paths.
- Fail Over Only—MPIO DSM uses one connection for all SAN data traffic until it times out or otherwise fails. At that time, traffic fails over to any other available path. Selecting this load balance policy causes the EHCMservice to no longer add and remove additional sessions to the target.

For both Round Robin and Least Queue Depth policies, sessions to the group member containing the data are given preference over other sessions.

Configuring MPIO Connections Settings

The MPIO Connections settings allow you to choose whether or not to use MPIO for snapshots, and to specify other connection properties. To use MPIO for snapshots, select the checkbox next to that option.

For volumes that span multiple group members, you can specify the following attributes:

- Maximum sessions for a volume. Values range from 1 to 12 (default is 6). This value should be equal to or greater than the value you specify for the maximum sessions per volume slice.
- Maximum sessions per volume slice. Values range from 1 to 4 (default is 2).

Configure the Network

1. In the Included Networks and Excluded Networks panels, make sure the information displayed is correct for your environment.
2. To exclude a subnet in the Included Networks panel, click the `Exclude` link under `Action`. The excluded subnet moves into the Excluded Networks panel.
3. To restore an excluded subnet, click the `Include` link in the Excluded Networks panel.
4. Click `Save` to save your settings. Press F1 to view online help for any of these dialog boxes.

Configure the Network Connections

1. Choose between IPv4 or IPv6 (if available) for the MPIO IP Version.
2. (Optional) Check the box to exclude new subnets as they are configured. Use this to prevent all new subnets from being enabled automatically, so that you can control which ones are added over time.
3. You can also control the minimum adapter speed, which specifies the slowest acceptable speed that a NIC can have when used for MPIO. The choices are based on the speeds of the NICs available on the host machine. If only one speed is available, this drop-down list contains the only available speed.

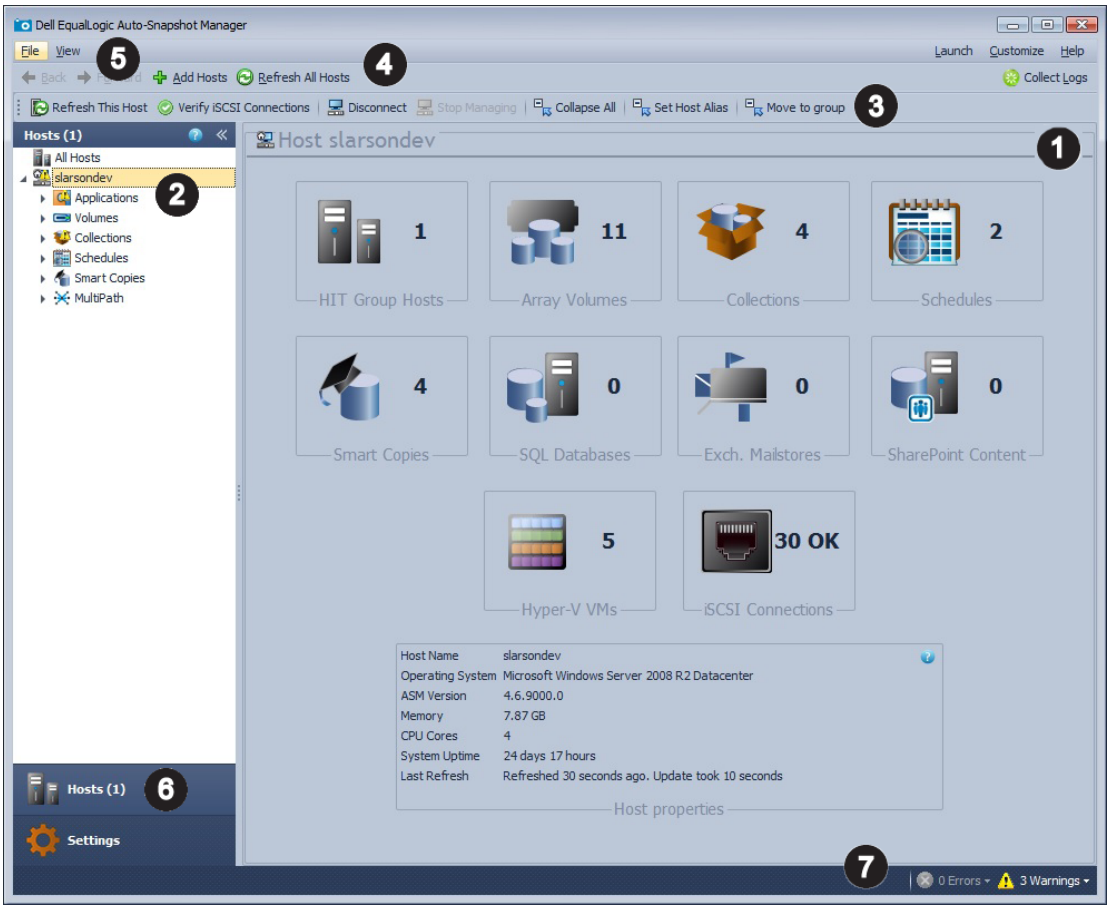
3 ASM/ME Graphical User Interface

This chapter describes features of the ASM/ME graphical user interface (GUI).

Start the ASM/ME GUI

To start ASM/ME, click `Start`, then `All Programs`, then `EqualLogic`, and then `Auto-Snapshot Manager`. The ASM/ME dashboard is displayed (Figure 3).

Figure 3: ASM/ME Dashboard



The following sections describe the GUI features in Figure 3.

Callout 1: Dashboard

Each host that you are managing has a separate Dashboard. Except for the HIT Group Hosts area within the Dashboard, all data on the Dashboard is specific to the selected host. The Dashboard provides you with an overall view of the managed objects in your system:

- The HIT Group Hosts area displays the number of hosts that you are managing with ASM/ME. The properties of the host selected in the Tree Panel are displayed beneath the Dashboard.
- The Array Volumes area displays the number of PS Series volumes connected to the host. Click on this area to display a view of all of the volumes and their respective capacity information. Selecting this area of the Dashboard automatically selects the Volumes node in the Tree Panel. The Volumes view also includes any local drives.
- The iSCSI Connections area displays the number of PS Series groups to which the local host is connected. Click on this area to open the iSCSI initiator.
- The Collections area displays the number of collections ASM/ME is managing. Click on this to display a view of all the collections and their properties. Selecting this area of the Dashboard automatically selects the Collections node in the Tree Panel.
- The Schedules area displays the number of Smart Copy schedules that have been created. Click on this area to view the schedule details. Selecting this area of the Dashboard automatically selects the Schedules node in the Tree Panel.
- The Smart Copies area displays the number of Smart Copies that ASM/ME has created. Click on this area to display a list of all the objects for which ASM/ME has created Smart Copies. Selecting this area of the Dashboard automatically selects the Smart Copies node in the Tree Panel. To view individual Smart Copies, navigate to them in the Tree Panel.
- The SQL Databases area displays the number of SQL databases ASM/ME is managing. Click on this area to view a list of all the applications that ASM/ME is managing. Selecting this area of the Dashboard automatically selects the Applications node in the Tree Panel.
- The Exchange Mailstores area displays the number of Exchange mailboxes that ASM/ME is managing. Click on this area to view a list of all the applications that ASM/ME is managing. Selecting this area of the Dashboard automatically selects the Applications node in the Tree Panel.
- The SharePoint Content area displays the number of SharePoint farms that ASM/ME is managing. Click on this area to view a list of all the applications that ASM/ME is managing. Selecting this area of the Dashboard automatically selects the Applications node in the Tree Panel.
- The Hyper-V VMs area displays the number of Hyper-V virtual machines that ASM/ME is managing. Click on this area to view a list of all the applications that ASM/ME is managing. Selecting this area of the Dashboard automatically selects the Applications node in the Tree Panel.

Callout 2: Tree Panel

The Tree Panel consists of related groups of objects organized in a navigation tree structure. Depending on what object you have selected in the tree, you are presented with a menu of available actions in the Actions Toolbar. You can also right-click any object in the Tree Panel to view the available actions for that object. Those right-click menu options are the same as the options displayed in the Actions Toolbar.

When you select an object in the Tree Panel, ASM/ME displays the object's properties and detailed status information. Important properties are in bold. In this properties view for an object, if a string is too long to display in the available space, ASM/ME provides tooltips (pop-up messages) that display the entire string when you mouse over the property. You can copy text strings, such as object identifiers, from this properties view to use in commands and scripts.

The Tree Panel also displays a node called Configuration Warnings if ASM/ME detects errors in some aspect of the general configuration. This node has no actions; when you click the Configuration Warnings node, the Dashboard displays a synopsis of the error (for example, VSS Control Volume Configuration Error), a short description explaining the problem, and a link to launch the wizard showing the steps necessary to correct the problem.

For more information about the nodes in the Tree Panel, see *Tree Panel on page 36*.

Callout 3: Actions Toolbar

When you select a node in the Tree Panel, available actions for that node appear in the Actions Toolbar. You can also display all the available actions for a node by right-clicking on the node. Unavailable actions are disabled or appear dimmed, and the available actions change depend on what node you select. Operations are described in *Generic ASM/ME Operations on page 55*.

Callout 4: Global Actions Toolbar

This toolbar displays global actions that are always available, without regard to what is selected in ASM/ME.

- The Add Hosts option allows you to add a host to manage from ASM/ME. See *HIT Groups on page 47* for more information.
- The Refresh All Hosts option refreshes ASM/ME and updates the UI with any new information.
- The Collect Logs option allows you to create a zip file with various log files that you can select. This is useful if you are reporting an issue to customer support.
- The Back and Forward navigation buttons allow you to go back to the previous view or forward to the view you just returned from, if applicable.

Callout 5: Menu Bar

This top-level menu has the following options:

- File—Select this option to add a host, export a host list, or refresh all hosts.
- View—Select this option to toggle the view between the Hosts view or the Settings view. Selecting the navigation buttons in Callout 6 also accomplishes the same task. You can also use this menu option to display or remove the Actions Toolbar.
- Launch—Select this option to open to iSCSI Initiator, Remote Setup Wizard, SAN Headquarters, Windows Disk Manager, Windows Event Viewer, or Windows Storage Manager for SANs.
- Customize—Select this option to change the display properties and colors of the ASM/ME GUI.
- Help—Select this option to open the online help system or collect logs.

Callout 6: Navigation Area

Selecting Hosts in the navigation area displays the Tree Panel and the Hosts view, while selecting Settings displays the user-configurable settings for ASM/ME. Changing these views can also be accomplished by selecting the View option in the Menu Bar.

Callout 7: Status Bar

This displays errors, warnings, and any refresh operation that might be in progress. When you click on the small triangle next to the Error or Warning label, the errors or warnings are displayed.

Tree Panel

The structure and content of the Tree Panel reflects the relationships between objects such as volumes and collections and their current status for ASM/ME operations. You can click a branch to expand or collapse it. The top-level objects in the Tree Panel are referred to as list nodes. For each node in the Tree Panel, you can:

- Right-click the node to display the context menu of available operations.
- Select the node to view the available operations in the Actions Toolbar. Not all nodes support actions.

Right-clicking a node will display the same available options that will be displayed when you select it and view the Actions Toolbar. The available options for each node will differ depending on the object you select. Not all objects in the Tree Panel are available for operations, and the available operations change depending on the current state of an object. For example, if a Smart Copy is mounted, its icon has a white-on-blue "i" overlay, indicating that it is in use. The mounted volume related to this Smart Copy also has a white-on-blue "i" overlay. In this state, your only available operations are as follows:

- For the Smart Copy:
  - `Unmount and Logoff` (or generate a command for this operation).
  - `View backup document`.
- For the mounted volume:
  - `Unmount and Logoff` (or generate a command for this operation).
  - `Set read-write`.

When you use the `Unmount and Logoff` option, the Smart Copy becomes available for all other Smart Copy operations (such as `Restore` or `Delete`).

Tree Panel Behavior in Failover Cluster Environments

- Resources that are not owned by a node are displayed in the Tree Panel as unsupported or might not be shown at all.

- The ASM/ME GUI does not dynamically update the status of the nodes in response to cluster changes. If you change the ownership of a cluster resource using the cluster administration tools or if a failover occurs, you must refresh the ASM/ME Tree Panel to display the proper state.

Tree Panel Nodes

Table 15 describes the ASM/ME Tree Panel nodes.

Note: Pressing the F5 key refreshes the host or hosts selected. If the user selected a host node, only that host is refreshed. If the user selected a Group, Farm, or Cluster node, the hosts that make up that Group, Farm, or Cluster are refreshed.

If the user selects a non-host-based node such as the All Hosts node or Configuration Warnings node, only the host running ASM is refreshed.

No matter what node is selected, pressing Ctrl+F5 will refresh all the hosts in the HIT Group.

Table 15: ASM/ME Tree Panel Nodes

Node	Description
All Hosts	Summary information about all hosts in a HIT group, including the host name; connection status; all SharePoint farms (hyperlinked to the specific farm); all clusters (hyperlinked to the specific cluster); errors and warnings; volumes, collections and schedules; applications; Smart Copies; virtual machines; and SharePoint farms, if any. Enables you to look in a single place to quickly see all the resources available in the HIT group.
Configuration Warnings	Displayed when ASM/ME detects errors in the general configuration. Expands to display a synopsis of the error (for example, VSS Control Volume Configuration Error), a short description explaining the problem, and a link to launch the wizard showing the steps necessary to correct the problem.
Applications	Installed applications for which a VSS writer is available, such as Microsoft Exchange, SQL Server, or Hyper-V. You can create simultaneous Smart Copies of all the application databases or of an individual database. On a cluster node that does not own the application cluster resources, the properties for the application writer will warn that the application service is not running on that node.
Volumes	Disks connected to the computer, including PS Series volumes that are assigned a drive letter. Select a drive letter to display detailed information about the disk, including whether it supports Smart Copies, Snapshot Borrowing, and Synchronous Replication.

Node	Description
	You can create a snapshot, replica (unless SyncRep is enabled on the volume), or clone, or create a schedule for the volume. You cannot perform Smart Copy operations on a CD–ROM disk, floppy disk, or a system disk or a cluster quorum disk. On a cluster node, if the node does not own the physical disk resources for the volume, the volume will be shown as an unsupported volume or might not appear at all in the Tree Panel.
Collections	A set of related databases enabling you to simultaneously create Smart Copies of multiple volumes or applications. Select a collection to display its properties and components. Collections of volumes on PS Series groups running firmware version 6.0 or higher also display the following properties, if enabled: • Snapshot Space Borrowing (enabled, disabled, or unavailable)—Applies to any one or more volumes in the collection that are using the Snapshot Borrowing feature. • Snapshot Borrow Space In Use—the amount of space that each volume in the collection is borrowing for their Smart Copies (snapshots). See *View Volume Details on page 55* and the *Dell EqualLogic Group Manager Administrator's Guide* for more information on snapshot borrowing. You can create, modify, or delete a collection, create a Smart Copy for the collection, or configure a schedule for the collection. On a cluster node that does not own the physical disk resources which are required for actions on the collection, the collection properties will include warnings that required components and volumes could not be found on that node.
Schedules	Designated times, dates, and frequency for creating Smart Copies. When configured, the Global Verification Task appears under this node. (See *Create or Modify the Global Verification Task on page 89*). On a cluster node, schedules that depend on cluster resources can only be edited on the node that currently owns those resources. However, any changes made are replicated to all possible owner nodes for the resources.
Smart Copies	Smart Copy sets for individual volumes, collections, and applications. Depending on the type of Smart Copy, you can mount it and restore data. You can also: • Delete a Smart Copy • Display the backup document for the Smart Copy • Validate the Smart Copy with reference to a connected PS Series group. If the validation operation fails, the Smart copy is classified as broken

Node	Description
	or unreachable. (See *Smart Copy Validation on page 72*.) Smart Copies are organized under the original object (volume, collection, or application). Each Smart Copy is assigned a timestamp. The replicas, clones, or snapshots in the set also have a timestamp. On a cluster node, some actions on a Smart Copy Set are restricted to the node that owns the cluster resources that the Smart Copy Set depends on. Under the Smart Copies node, additional nodes might appear: • Broken This node contains Smart Copies that cannot be validated, because part of the Smart Copy set is missing, or because the snapshot reserve for one of the volumes is out of space. See *View Available Smart Copies on page 70* for more information. • Recoverable This node contains the Smart Copies of a cloned volume that was deleted on the PS Series group. See *Smart Copy Properties for Volumes on page 69* for more information. • Unreachable This node contains Smart Copies for volumes on a PS Series group that cannot be reached during validation. See *View Available Smart Copies on page 70* for more information.
MultiPath	Displays detailed information about the multipath sessions for the host. The MultiPath node expands to display the I/O details for the host.

Tree Panel Icons

Nodes in the ASM/ME Tree Panel have icons (Table 16) associated with them. The icons can vary, depending the state of the component associated with that node. For example a node that is all gray does not support certain ASM/ME operations.

Table 16: ASM/ME Icons

Icon	Definition
	All Hosts node. The object nodes for each host (Applications, Volumes, Collections, Schedules, and Smart Copies) are listed under the Host node.
	Local host node. This icon represents the host on which the current instance of ASM/ME is running.

Icon	Definition
	Remote host node. This icon represents a Group, SharePoint farm, or cluster node in the HIT Group.
	Applications list node. Supported applications, such as SQL server, are listed under this node.
	Application Node. The application is supported and functioning correctly.
	Application Node. The application is an incompatible version, or the application is not currently running.
	Container for a group of Application Components. The container name is determined by the application that owns the components.
	Application Component. This icon represents an application component (such as an SQL database or an Exchange Mailbox Database) residing on a volume that is not supported for Smart Copy operations.
	Application Component. This icon represents an application component (such as an SQL database or an Exchange Mailbox Database) residing on a volume which is supported for Smart Copies. ASM/ME implicitly includes all supported subcomponents in a Smart Copy.
	Application Subcomponent. This icon represents an application subcomponent residing on a PS Series array volume. You cannot select subcomponents for Smart Copy operations. When you select an Application component for a Smart Copy operation, ASM/ME implicitly includes its supported subcomponents.
	SharePoint content database. This icon represents a content database that is part of a SharePoint farm.
	Volumes list node. Volumes visible to ASM/ME and that support Smart Copy operations are listed under this node.
	Unsupported volume node. The volume is not supported for ASM/ME operations. On a cluster node, this may also indicate that the node is currently not the owner of the physical disk cluster resource for the volume.
	Read-only volume
	Template volume

Icon	Definition
	Thin clone volume
	Collections list node. Defined collections are listed under this node. Individual collections are indicated using the same icon.
	Smart Copies list node. All Smart Copies are listed under this node.
	Clone Smart Copy
	Nonon-VSS Smart Copy
	Snapshot Smart Copy
	Replica Smart Copy
	Broken Smart Copies. Smart copies are listed under this node if they have been deleted on the PS Series group.
	Unreachable Smart Copies. This icon is also used on a cluster node, for schedules and Smart Copy Sets, if the node does not own the affected cluster resources.
	Recoverable Smart Copies. This icon indicates Smart Copies associated with a volume (cloned volume) that was deleted on the PS Series group. These Smart Copies will be restored if the volume is recovered on the group.
	Schedules list node. Smart Copy schedules are listed under this node.
	MultiPath node. This node shows the active multipath sessions for all connected volumes.
	I/O details node. This node shows I/O usage and performance data for all multipath sessions.

Group SharePoint Farm Nodes, Clusters, or Host Nodes

You can now create a group, name it, and add a complete SharePoint farm, cluster, or host to that group. You can also create groups that will contain individual hosts, clusters, and/or SharePoint farms.

This grouping feature makes it easier for users to find cluster nodes or SharePoint farms without having to search all the nodes in a hit group looking for the cluster nodes.

Assign SharePoint Farms, Clusters, and Host Nodes in the Same SharePoint Farm to a Group

Host and cluster nodes that make up a SharePoint farm are automatically assigned to the same group by Auto-Snapshot Manager when you add any node in the unit to a group. Each farm will have the clusters listed beneath it and the hosts that make up the cluster listed beneath that node. Individual hosts that are members of the farm will be displayed under the farm node.

Note: You cannot move a portion of a SharePoint farm or cluster to a group. Auto-Snapshot Manager detects that the components being moved depend on the entire logical unit (SharePoint farm, cluster, and so on). So, if you try to move just a portion of the "logical unit," Auto-Snapshot Manager moves the entire "logical unit."

1. Select the node or cluster to add to a group and right-click.
2. Select `Move to group` from the drop-down list or click `Move to group` from the toolbar at the top.
3. For SharePoint farms, in the `Move Farm <farmname> to Group` dialog box, enter a new group name in the `Group Name` field or select a preexisting group name from the drop-down list and click `OK`.

   For clusters or hosts, in the `Move Host <hostname> to Group` dialog, enter a new group name in the `Group Name` field or select a pre-existing group name from the drop-down list and click `OK`. The selected standalone cluster or node is added to the group.

   The new group appears at the top level in the `Hosts` frame on the left. The group name appears in the `Group Name` field in the details list for each node.

Remove SharePoint Farms, Clusters, and Host Nodes from a Group

1. Select the top-level node in the group.
2. Right-click and select `Remove from group` or click `Remove from group` in the top toolbar and click `OK`. All the nodes in the group are removed from the group and the group is deleted.

About Aliases

You can assign an alias (that is, an easier-to-remember name) to a SharePoint farm node, a cluster, or a host node.

Using aliases enables you to work around the following common practices, which often result in non-intuitive names for SharePoint farms, clusters, or host nodes:

- In many large installations, host names are assigned with a specific naming convention.
- The naming of SharePoint farms is often derived from the configuration database.

Assign an Alias to SharePoint Farm Nodes, Cluster Nodes, or Individual Host Nodes

You can now assign an alias to a SharePoint farm node, a cluster, or a host node. The alias will be used as the node name in the Hosts tree list on the left side of the Auto-Snapshot Manager.

The Host Name field in the main frame will display the node alias first, followed by the SharePoint Farm name, cluster name, or host name in brackets.

Notes: You cannot assign an alias to a user-defined group because they are already named with an alias.

You can use any character in an alias. An alias has a maximum length of 24 characters.

You cannot use an alias with any ASMCLI command where the machine name must be specified. That is, you must specify the actual machine name.

Assign an Alias to a SharePoint Farm Node

1. Select the SharePoint farm node from the `Hosts` frame.
2. Either click `Set Farm Alias` along the top of the window or right-click the SharePoint farm node and select `Set Farm Alias`.
3. In the `New Alias for Farm <farmname>` dialog box, enter a new alias for the node and click `OK`. The SharePoint Farm name in the `Hosts` list is replaced by the new alias.

Assign an Alias to a Cluster Node

1. Select the cluster node from the `Hosts` frame.
2. Either click `Set Cluster Alias` along the top of the window or right-click the node and select `Set Cluster Alias`.
3. In the `New Alias for Cluster <clustername>` dialog box, enter a new alias for the node and click `OK`. The Cluster name in the `Hosts` list is replaced by the new alias.

Assign an Alias to a Host Node

1. Select the host node from the `Hosts` frame.
2. Either click `Set Host Alias` along the top of the window or right-click the node and select `Set Host Alias`.

3. In the `New Alias for Host <hostname>` dialog box, enter a new alias for the node and click `OK`. The Host name in the `Hosts` list is replaced by the new alias.

Delete an Alias for a SharePoint Farm, Cluster, or Host Node

Delete a SharePoint Farm Alias

1. Select the alias to delete from the `Hosts` frame.
2. Right-click and select `Delete Farm Alias` or select `Delete Farm Alias` from the toolbar at the top of the Auto-Snapshot Manager window. The SharePoint farm alias is deleted without any confirmation window. The name of the SharePoint farm automatically reverts to the default name.

Delete a Cluster Alias

1. Select the alias to delete from the `Hosts` frame.
2. Right-click and select `Delete Cluster Alias` or select `Delete Cluster Alias` from the toolbar at the top of the Auto-Snapshot Manager window. The cluster alias is deleted without any confirmation window. The name of the cluster automatically reverts to the default name.

Delete a Host Alias

1. Select the alias to delete from the `Hosts` frame.
2. Right-click and select `Delete Host Alias` or select `Delete Host Alias` from the toolbar at the top of the Auto-Snapshot Manager window. The host alias is deleted without any confirmation window. The name of the host automatically reverts to the default name.

Customize Color Themes

You can customize the color theme for ASM/ME, and you can also customize the colors for the pie charts and cylinders displayed in the Volume view. (The Volume view is displayed when you select the Volumes list node in the Tree Panel.)

Change the Color Theme for ASM/ME

1. Click `Customize`, then `Theme`.
2. Choose the color theme that you want for ASM/ME.

Change the Color Theme for the Volumes View

1. Click `Customize`, then `Colors`.

2. Choose the color theme that you want to display for Volume pie charts and the cylinders displayed in the Volumes view.

4 HIT Groups

A HIT Group allows you to manage multiple hosts from any machine that is running ASM/ME.

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 one backup administrator has to back up and create Smart Copies for multiple machines, they can perform all the ASM/ME Smart Copy operations from a single instance of ASM/ME. Similarly, 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 are installed on the host. If you have already created a HIT Group, ASM/MEwill display a message if any of the hosts are not running a version of Host Integration Tools 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.

ASM/ME Operations on HIT Group Members

Assume you have created a HIT Group that includes your local host, and three hosts that you have added to it for managing with ASM/ME. You can perform any ASM/ME operation on the local host and any of the three hosts that you have added. Select the appropriate host from the Tree Panel, and then perform the ASM/ME operation from that view. You perform ASM/ME operations on the remote hosts exactly as you would perform operations on the local host.

HIT Groups in Non-Cluster Environments

In non-cluster 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 run ASM/ME from a single host and manage that local host.

Assume you have three hosts—A, B, and C, and that each host is running an instance of ASM/ME. From the ASM/ME instance on host A, you can also add hosts B and C. This feature enables you to perform all ASM/ME operations on hosts B and C from the ASM/ME console on host A. However, if you then view the instances of ASM/ME running on hosts B or C, you will not be able to see host A or perform ASM/ME operations on host A until you add host A from that specific host.

Figure 4 illustrates a two-member HIT Group in a standard non-cluster environment. In this figure, Host A can add Host B for management. Then, it can manage itself as well as Host B.

Figure 4: Two-Member HIT Group in a Non-Cluster Environment

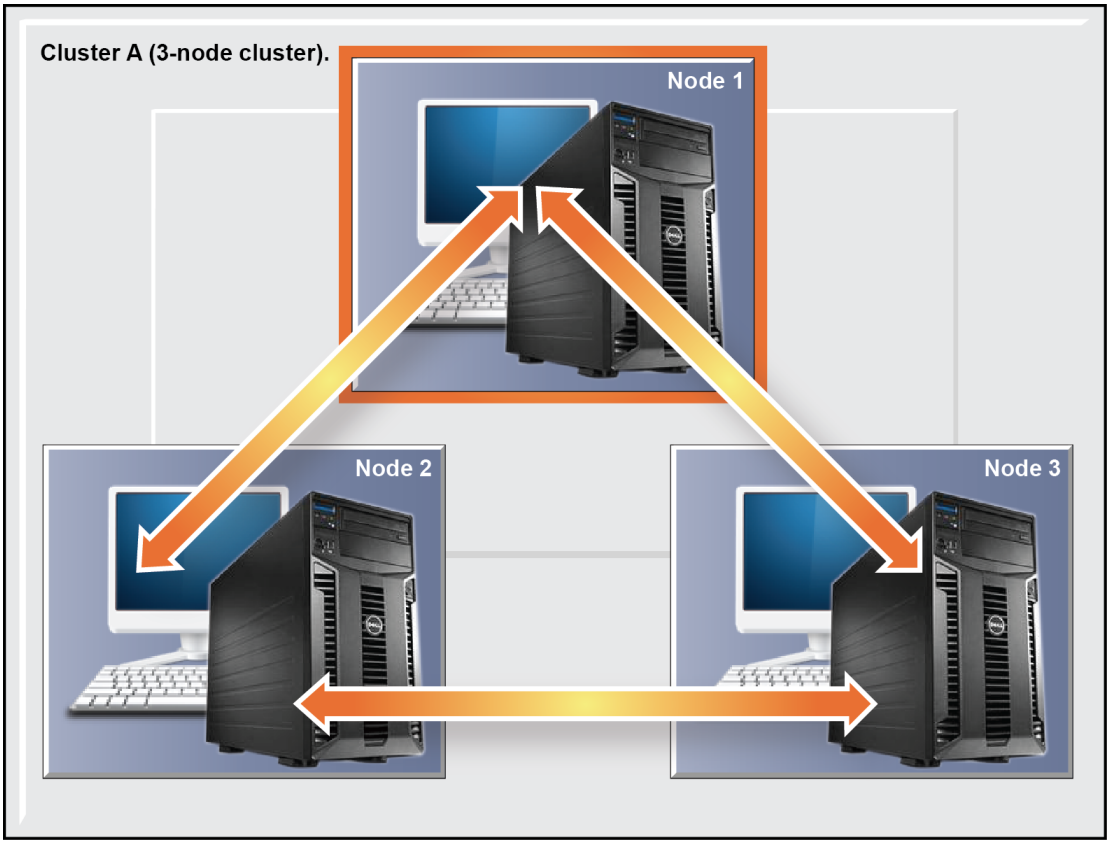
HIT Groups in Cluster Environments

In cluster environments, all cluster nodes in a HIT Group have a reciprocal relationship. That is, adding cluster node B to the ASM/ME instance on cluster node A will automatically add cluster node A to the ASM/ME instance on cluster node B.

You must always add an entire cluster to a HIT Group as opposed to a subset of cluster nodes. ASM/ME will then automatically set up the trust relationship between each cluster node. If you add only a subset of cluster 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 cluster node, ASM/ME will warn you if you have not created a HIT Group that includes all the other cluster nodes. Figure 5 illustrates a three-node cluster that has been added to a HIT Group.

Figure 5: Three-Node Cluster HIT Group



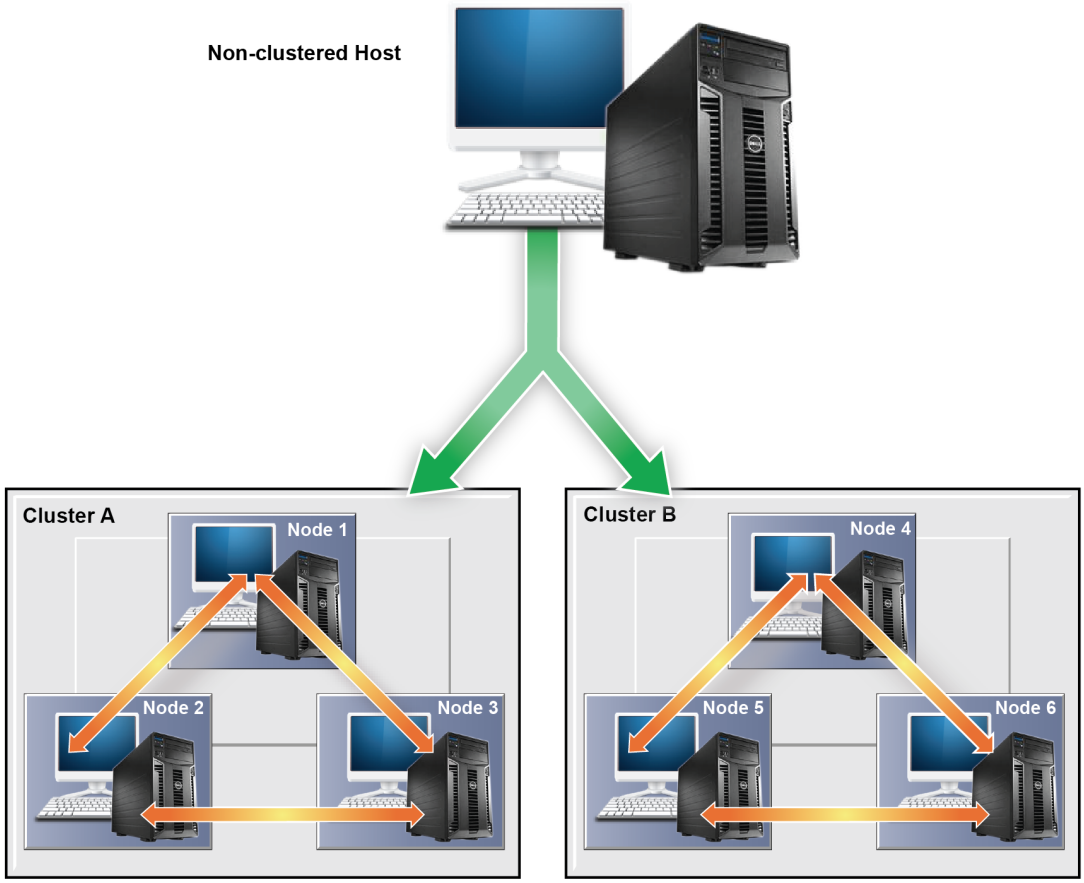
In this figure, assume you use the Add Hosts option from the ASM/ME instance on Node 1 to add Nodes 2 and 3 to it. ASM/ME then automatically sets up the following trust relationships between each node, indicated by the bidirectional arrows.

- The ASM/ME instance on Node 1 will have nodes 2 and 3 added to it. Node 1 can then manage Nodes 2 and 3.
- The ASM/ME instance on Node 2 will have Nodes 1 and 3 added to it. Node 2 can then manage Nodes 1 and 3.
- The ASM/ME instance on Node 3 will have Nodes 1 and 2 added to it. Node 3 can then manage Nodes 1 and 2.

Multiple Cluster Management: Using a Non-Clustered Host

You can use a non-clustered host to manage more than one cluster. From the ASM/ME instance running on the non-clustered host, you can add the entire set of cluster nodes for all the clusters you want to manage. ASM/ME will automatically set up the appropriate trust relationships between each cluster node. The non-clustered host can manage each cluster. Figure 6 illustrates this HIT Group configuration.

Figure 6: Two-Cluster HIT Group Managed From a Remote Host



In this figure, assume you use Add Hosts option from the ASM/ME instance on the non-clustered host to add all six cluster nodes from the two clusters.

ASM/ME automatically sets up the trust relationships, indicated by the different arrows. The following relationships are set up.

On the non-clustered host:

- Nodes 1, 2, 3, 4, 5, and 6 are added at once to the non-clustered host. The non-clustered host can manage all nodes on each cluster.

On Cluster A:

- Every node in Cluster A can manage every other node in the cluster. Cluster A's nodes cannot access or manage Cluster B's nodes.
  - Nodes 2 and 3 are added to the ASM/ME instance on Node 1.
  - Nodes 1 and 3 are added to the ASM/ME instance on Node 2.
  - Nodes 1 and 2 are added to the ASM/ME instance on Node 3.

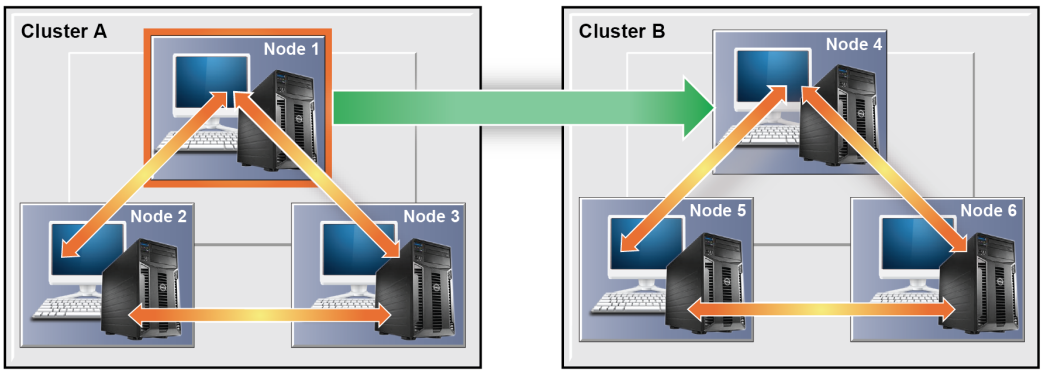
On Cluster B:

- Every node in Cluster B can manage every other node in the cluster. Cluster B's nodes cannot access or manage Cluster A's nodes.
  - Nodes 5 and 6 are added to the ASM/ME instance on Node 4.
  - Nodes 4 and 6 are added to the ASM/ME instance on Node 5.
  - Nodes 4 and 5 are added to the ASM/ME instance on Node 6.

Multiple Cluster Management: Two-Cluster Example

You do not require a non-clustered host to manage multiple clusters. You can simply manage one cluster from another cluster. For example, assume you have two three-node clusters (cluster A and cluster B), and you want to manage cluster B from cluster A. From any node on cluster A, you can run ASM/ME, add a node from cluster B to it, and then manage cluster B from there. Figure 7 illustrates this scenario.

Figure 7: Two-Cluster HIT Group Managed From a Cluster



In this figure, assume you use the Add Hosts option from the ASM/ME instance on Node 1 to add Node 4 to it. (If ASM/ME is not installed on nodes 4, 5, and 6, ASM will first set up the appropriate trust relationships between nodes 4, 5, and 6. This process is indicated by the bidirectional arrows). After you add Node 4 to node 1, you can then manage all of Cluster B's nodes from Node 1.

However, you will not be able to manage any of Cluster A's nodes from Cluster B until you add a node from Cluster A to Cluster B.

About Creating a HIT Group

Use the Add Hosts wizard to create a HIT Group. With this wizard, ASM/ME automatically detects whether a clean installation or upgrade is needed on the host that you are adding. ASM/ME is then automatically installed (or upgraded) on the host that you are adding, and then the host is added to the HIT Group.

If the installation or upgrade fails, you can perform a manual installation on the host that you are adding. Then, you can use the Add Hosts wizard from the local host to add the other host to the HIT Group.

Prerequisites for HIT Groups

- For new installations to run successfully on remote hosts, ensure that you allow incoming ping requests through the remote host's firewall to the remote host. Use Windows Server Manager to create new inbound rules for your firewall. Select ICMPv4 or ICMPv6 protocol types for IPv4 and IPv6 pings, respectively. If both the local and remote hosts are in the same domain, allow the connections over the domain profile type.

  If you prefer not to edit firewall rules, you can perform a manual installation on the host you are adding, and then use the Add Hosts wizard on the local host to add the host to the HIT Group.

- You will be prompted for username and password credentials in order to install Host Integration Tools on remote hosts added to the HIT Group. These credentials are never stored; they are only used for the installation. The following requirements must be met:
  - If you are installing on a cluster, you must provide the appropriate credentials (domain user with local administrator rights) across all cluster nodes.
  - If adding or installing on multiple hosts:

    Single Domain—For multiple machines that belong to a single domain, you must provide the appropriate user credentials (domain users with local admin rights) so that ASM/ME can successfully access the machines to perform the required installations.

    Single Workgroup—For multiple machines that belong to a single workgroup, each machine must have the same local admin account credentials.

    Multiple Domains—For machines across multiple domains, add or install on all the machines from one domain at a time.

- The Remote Procedure Call (RPC) service must be running. This service should be started by default on Windows systems, but if it is not running, or if the firewall is blocking it, the installation will not work.

- If you are using the Browse Network option to add hosts to the HIT Group, ensure that browsing the network is working in Windows. If you cannot add hosts by browsing the network, add them manually by using the Manual Entry option in the Add Hosts wizard.

- Copy the `Setup.exe` and `Setup64.exe` installation files into a directory of your choice. Because you must specify this directory multiple times if you are adding several hosts for management or pushing out multiple installations, you can simplify the process by copying the installation files onto a network shared directory. (The default installation directory is `C:\Program Files\EqualLogic\bin`, so you can also place it there). ASM/ME will use these files to initiate the installation procedure on remote hosts. These installation files are available on CD–ROM that shipped with your PS Series array, or from the installation kit available at https://support.dell.com/equallogic.

Create a HIT Group with the Add Hosts Wizard

1. Click the `Add Hosts` button to start the Add Hosts wizard.
2. You can specify the list of hosts to add to your HIT Group in several ways. Select one or more of the following methods and click `Next`. To view online help for any of the wizard pages, press the F1 button for that specific page.
   - Discover through PS Series group—When this option is selected, ASM/ME queries any PS Series groups that are connected to any current HIT Group members (including the local host), and displays all the hosts connected to those groups.
   - Browse network—Select a host by browsing a network. You can only browse networks for which you have permissions.
   - Manual entry—Enter an IP address or host name for each host you want to add to the HIT Group. You can also import a file that lists all the hosts that you want to add to the HIT Group. The file will be parsed and each host will be run through the manual entry process. This file can be generated automatically from the ASM/ME console by clicking File, then Export Host List. You can also create your own file for importing by saving a text file that contains a comma-separated list of host IP addresses, host names (fully qualified or not), or both. When you are back on this wizard page, click Import, and then browse to the file.
   - Cluster nodes—This option is visible only if ASM/ME detects that you are running a multiple node cluster in which one or more of the nodes have not yet been added to the HIT Group. All cluster nodes should be added to the HIT Group. If only a subset of nodes are added, cluster operations will fail.
3. Select one or more of the above options to identify which hosts to add. When you have selected which hosts to add, click `Next`. The `HIT Installation and Host Verification` page is displayed.
4. Enter the following information:

Enter the credentials (domain, username, and password) for the host you are adding. See the prerequisites for more information about these requirements.

   a. If you want to install MPIO or the PowerShell Tools on the host, select those options.

   b. Specify the directory that contains the installation (`Setup.exe` and `Setup64.exe`) files.

   c. Click `Add Hosts` to begin the installation on the specified host. Progress and status information is displayed. (An error message will be displayed if the installation or upgrade cannot complete). When the process is complete, click `Close`. The `Summary of Hosts` page is displayed.

5. This page displays the hosts that have been added to the HIT Group, and what actions—such as installations or upgrades—have been performed on each host. This page also shows you whether or not a reboot is required on the remote hosts. If a reboot is required, click `Reboot All`. Otherwise, click `Finish`.

   When the installation is complete on the remote host, you can launch the Remote Setup Wizard from the remote host in order to initialize a PS Series array, configure the remote host to access a PS Series group, or to configure MPIO settings for the remote host.

After the host has been added to the HIT Group, it will appear in the tree in the left panel of the ASM/ME console and you can start managing it from there. To stop managing a host, right-click the host in the left panel and select `Stop Managing`.

Edit ASM/ME Settings on Hosts in a HIT Group

1. In the Navigation area, click `Settings`.
2. In the middle panel, select all the hosts for which you want to edit settings. If you select multiple hosts, then the settings you change will be saved on all of the selected hosts.
3. On the left, select General Settings, Notification Settings, Alert Settings, Verification Settings, or PS Group Settings to view the current settings.
4. Check or deselect the options accordingly.
5. Click `Save`.

If settings are changed on any member of a HIT Group, then all instances of ASM/ME that are managing that member will be informed of the change.

5 Generic ASM/ME Operations

This chapter explains the operations you can perform with ASM/ME, including how to create Smart Copies, schedule Smart Copy operations, and restore a volume using a Smart Copy.

For operations that are specific to the supported applications, see the following chapters:

- *Using ASM/ME with Microsoft Exchange on page 83*
- *Using ASM/ME with SQL Server on page 107*
- *Using ASM/ME with Hyper-V on page 115*
- *Use ASM/ME with Microsoft SharePoint on page 129*

About Volumes

A volume is a storage object used by an application or file system to store data. The Volumes list node in the Tree Panel displays a summary of all the volumes known to ASM/ME, including the drive letters on which they are mounted, their names, and a pie chart of each volume showing the amount of in-use and free space.

Hover the mouse over the mount point for any volume to display a tool tip explaining the terms Free Space and In-Use Space. Click on any volume's pie chart to open the node for that volume.

View Volume Details

For each volume known to ASM/ME, you can display its properties, Smart Copy properties, information about the PS Series group it belongs to (if applicable), and the operating system of the host using the volume.

For volumes on PS Series groups running firmware version 6.0 or higher, the following properties can apply:

- Synchronous Replication properties

  Synchronous replication is the process of replicating a volume to a another storage pool on the same group. See the *Dell EqualLogic Group Manager Administrator's Guide* for more details.

  If synchronous replication is enabled on a volume, the volume properties include the state of synchronous replication for the volume (enabled or disabled), the state of the replication between the SyncActive and SyncAlternate volumes (in sync or out of sync). In addition, the Features field displays that the volume supports synchronous replication.

  If synchronous replication is enabled for a volume, you cannot create a replica (group-to-group replication). These types of replication are mutually exclusive.

- Snapshot Space Borrowing properties

  Snapshot space borrowing is a feature available only on PS Series groups running firmware v6.0 or higher, that enables a volume to borrow from free pool space to create snapshots if the volume runs out of its own snapshot reserve space. See the *Dell EqualLogic Group Manager Administrator's Guide* for more details.

  This feature is enabled by default for all volumes created on v6.0 or higher (however, snapshot borrowing can be enabled on volumes created before the group was updated to v6.0).

  If snapshot borrowing is enabled but the volume has no snapshot reserve space configured, you cannot create a Smart Copy. Contact the administrator of the PS Series group if this volume is supposed to support Smart Copy creation.

On any volume in the Tree Panel, you can perform the following activities:

- In the Properties panel, click the Volume name to open the Windows Explorer dialog box.
- In the Smart Copy panel, click the underlined number in the Smart Copy Count field to view details about the Smart Copies of the volume. In the Tree Panel, the selected Smart Copy is highlighted.
- In the PS Details panel, click the name of the PS Series group to launch its Group Manager GUI.
- In any panel, click the Help icon to display a tool tip describing the terms used in that panel.

About Rethinning a Volume

Rethinning a volume finds space that is not used by any files in the volume and returns that space to a status of unreserved (space that is not allocated to any volume). You cannot rethin a volume that has replication or synchronous replication (SyncRep) enabled.

Windows 8 or greater and Windows Server 2012 or greater include built-in support for volume rethinning. These operating systems will inform the PS Series group that space can be unreserved soon after a file is deleted. Unless you have disabled the operating system's built-in rethinning support, it is normally not necessary to use the rethinning tools included in the Host Integration Toolkit, unless either of the following conditions is true:

- You upgraded from an earlier version of Windows
- You moved a thin-provisioned volume from a system running an earlier version of Windows (for example, unmounted it from Windows 8 or greater server and mounted it on a Windows Server 2012 or greater

The effectiveness of rethinning varies, depending on how the free space is distributed on the volume. Rethinning a volume with large contiguous blocks of free space will return more space to the unreserved pool than will rethinning a volume with smaller blocks of free space scattered in different locations on the volume. Defragmenting a volume using operating system tools will consolidate the free space on the disk, which will improve the results of a subsequent rethinning operation.

Rethinning a volume with snapshots can increase the amount of space charged to the volume's snapshot reserve, because the rethinned space is no longer part of the volume, but is still part of any snapshots taken before the rethinning. This space has to be preserved so the snapshots remain valid. In some cases this can result in the snapshot reserve exceeding 100 percent, which can trigger the deletion of older snapshots by the group. Therefore it is possible you will not see an immediate increase in available storage on the PS Series group from rethinning a volume, even if a significant amount of space was reclaimed. If you are taking regular snapshots of the volume, over time you will see the space savings as the older snapshots are deleted.

When you rethin a volume using ASM/ME (or the command-line tools in the Host Integration Toolkit), a large temporary file is created on the volume. The space occupied by this file is rethinned during the operation. This file is deleted at the end of the operation, but you can adjust the amount of free space occupied by the temporary file as follows:

- Reduce the percentage of space used for the temporary file if the volume is being heavily used, to avoid possible out-of-space errors
- Increase the percentage of space used for the temporary file on volumes with little I/O traffic to rethin as much space as possible

If you take a Smart Copy of a thin-provisioned volume during a rethinning operation, the Smart Copy will include the large temporary file created for rethinning. The temporary file is deleted automatically when the rethinning operation completes, however it will still exist in the Smart Copy. If you then restore from this Smart Copy, the restored volume will have little free space available.

To avoid this, do not create Smart Copies while rethinning is in process. If you set up schedules for creating Smart Copies, make sure the rethinning operation occurs outside the schedule window.

Rethinning a volume can take several minutes, depending on the size of the volume and how busy the group is. The results of the rethinning operation are not immediately visible in either the ASM/ME GUI or the Group Manager GUI. Refresh the host (in the ASM/ME GUI) or refresh the Group Manager GUI to see the new amount of free space for the volume.

Note: Hyper-V VMs might pause during a rethinning operation. The VM resumes normal operation after the rethinning operation completes. Therefore, you might want to start or schedule the operation during less-busy times.

Note: Before you rethin a volume that is enabled for replication, consult the *Dell EqualLogic Group Manager Administrator's Guide* for more information.

Rethin a Volume

Before you begin, make sure you understand the effect on some operating systems and Smart Copy schedules on volume rethinning. See *About Rethinning a Volume on page 56*.

1. In the Volumes node, right-click a volume and select `Rethin Volume`.
2. The dialog box shows you the amount of space that can be reclaimed after the rethin operation. Click `Next`.

3. In the Rethinning Parameters dialog box, optionally change the percentage of space that will be used by the temporary file to accomplish the rethin operation, then click `Finish`.
4. The rethin operation is performed and a progress screen is displayed. The screen closes when the operation is complete.

Note: If power is lost during a volume rethinning operation, the temporary file that is created during the operation can remain in the root directory of the volume being rethinned. The temporary file will have a file name in the form `eqt_*.tmp`. Delete this file after the system restarts.

To set up a schedule for volume rethinning, see *Schedules for Volume Rethinning on page 63*.

Operations on Microsoft Failover Clusters

You can install the Host Integration Tools on any cluster nodes that you intend to use for recovery operations. When you install ASM/ME (as part of the Host Integration Tools) on computers that are nodes in a Microsoft Failover Cluster, the following operations are enabled:

- You can create Smart Copies and configure schedules for iSCSI volumes or application components that are designated as a cluster resource. You can run ASM/ME on any cluster node, however you need to perform the operation from the cluster node that owns the cluster resource.
- When deleting, disabling, enabling, or modifying schedules on clusters, the changes will be made on all cluster nodes automatically.
- Changes made with the cluster manager will be automatically detected by ASM/ME, so if you change the owner of a resources in cluster manager, ASM/ME will automatically detect the change.
- You can perform all ASM/ME operations on any attached PS Series iSCSI objects (volumes or application components), if the object is not designated as a *cluster resource*.
- When ASM/ME is installed on the cluster node that owns the quorum disk, you can access and display information for the cluster quorum disk. In the ASM/ME GUI, the cluster quorum disk is identified by the grayed-out volume icon. However, if the node owns the quorum disk, all of the PS Series array information is shown in the properties. Also, the context menu actions for volumes are shown, but disabled with the explanation that the volume is the quorum disk.
- After you use the cluster-available administration tools to manually place a mounted iSCSI volume in maintenance mode, you can use the `Unmount and Logoff` operation.
- For Microsoft Exchange application components on supported volumes owned by the node that is running ASM/ME, you can run `Checksum Verification and Soft Recovery`.
- You can restore data from Smart Copies, if the affected cluster resource volumes are owned by the cluster node.

On Windows Server 2008, cluster management is performed using the Failover Cluster Management utility. On either operating system, use the snap-ins or the corresponding command line utilities to create and configure clusters.

Identifying Cluster Volumes in the ASM/ME GUI

The cluster quorum disk can be located on the array. Although ASM/ME recognizes the quorum disk, it does not allow certain actions, such as Smart Copy creation, to be performed for the quorum disk.

The properties displayed for an owned cluster resource and an unclustered disk might be the same. However, the available actions for clustered versus unclustered (or owned/not owned/quorum) disks might differ. Certain actions might be disabled or appear dimmed with "(`Disabled: <reason>`)" appended to the menu item, and other actions might be enabled, depending on the disk.

The state of the volume's physical disk resource (owned/unowned) determines the status after failover.

About Collections

ASM/ME enables you to define a logical collection of volumes, applications, or application components. You can then perform Smart Copy operations on the entire collection. You can include in the collection only volumes that support Smart Copies. You can modify a collection at any time by adding volumes or removing unwanted volumes.

Be careful when selecting the components of a collection. Dell recommends creating collections only for objects that are logical to restore *as a group*; for example, all the application components for a database. You should avoid creating collections that contain volumes for multiple databases, or collections that include database volumes and volumes used by other, unrelated applications. Make sure your collections support your intended backup and restore plans.

When you create a collection, you can include an application or any of its components within the Applications node. If you select an application component, ASM/ME selects all the volumes that the component uses. Additionally, ASM/ME will identify and select any further application components that use that volume. Similarly, if you deselect any volume or component, all interdependent components will also be deselected automatically. ASMCLI handles collection creation differently. See *ASMCLI -createCollection on page 170* for more information.

Volume-Based Collections

You can specify whether or not you want a Smart Copy schedule for a collection to fail if the collection definition differs from the time the schedule was created. For example, assume you have created a collection that contains a group of volumes on which SQL databases are stored. ASM/ME automatically includes the SQL databases in the collection. If you select the option to create a volume-based collection, and if a database is removed from the volumes, the schedule will still run successfully and ASM/ME will still create a Smart Copy of the collection even though the collection definition changed. For any type of collection, selecting the option to create a volume-based collection will result in scheduled tasks still running successfully even if the collection definition is changed. Any collection that contains Cluster Shared Volumes (CSVs) is forced to behave as a volume-based collection.

If you do not select the option to create a volume-based collection, the scheduled task will fail if there is any change in the collection definition. What components get included in the collection, however, are based on the state of the collection at the point in time the Smart Copy is created.

Create a Collection

1. Right-click the `Collections` node in the ASM/ME Tree Panel and select `Create Collection`. ASM/ME displays the `Collection name` dialog box.
2. Specify a unique, alphanumeric name for the collection. If you want to create a volume based collection, check the box and click `Next`. ASM/ME displays the `Components` dialog. See *Volume-Based Collections on page 59* for more information.
3. Select the volumes or application components to include in the collection. ASM/ME automatically includes required components.
4. Click `Next`. ASM/ME displays the `Summary` dialog box. This dialog box lists the default settings that will be used when ASM/ME creates Smart Copies of the collection components. Click `Create` to create the collection.

The new collection is displayed in the ASM/ME Tree Panel under `Collections`. Select the collection name to display its details.

When you have created a collection, you can create Smart Copies of the collection volumes as described in *Create Smart Copies on page 68*. Smart Copy Sets for collections are located under the collection name under `Smart Copies` in the ASM/ME Tree Panel.

More Collection Operations

You can create a Smart Copy schedule for a collection, and generate an ASMCLI command for creating a Smart Copy of the collection. You can also modify or delete a collection, as follows:

1. Expand `Collections` in the ASM/ME Tree Panel and right-click the collection name.
2. Select the desired operation from the menu. The choices are Create Smart Copy, Configure New Schedule, Modify Collection, Delete Collection, and Generate Create Smart Copy Command.

If a collection is renamed, any Smart Copies and schedules of the collection will be updated to refer to the renamed collection. Schedule names will not be automatically modified, but can be changed by selecting the Modify Schedule option for the affected schedule.

When you modify a collection says that the originating computer is `Unknown`, the originating computer property changes to the name of the host that modified it. Ideally, you should modify a collection only from the originating host. (A collection's originating host can be unknown if the collection was created on an earlier version of ASM/ME, which did not include the originating host information.)

To change the originating host, you do not need to make any actual changes to the collection. For example, you can deselect and then immediately reselect a volume in the collection, then click `Update`. This process is enough to change the collection properties.

About Schedules

You can create schedules to perform Smart Copy operations at regular intervals. ASM/ME notifies you when scheduled operations complete or fail.

For Smart Copies, you can set a maximum frequency of one copy every five minutes. You can also control how many Smart Copies ASM/ME preserves concurrently.

Once you have created a schedule, you can modify its time and frequency. You cannot modify the original Smart Copy options, with the exception of adjusting the keep count to control how many Smart Copies are retained concurrently.

You can temporarily disable a schedule to modify it, or to prevent the schedule from running as planned. When you want the schedule to run, you can enable it, and it will start at the next date and time. See *Disable or Enable Schedules on page 63*.

Retained Copies or Replicas

You can specify the maximum number of retained snapshots or replicas created by the schedule. Snapshots and replicas are also limited by the snapshot reserve and replica reserve configured on the PS Series group. See the *Dell EqualLogic Group Manager Administrator's Guide* for details.

Recommendations for Schedule Creation

- Schedules with a very high frequency of Smart Copy creation might have a significant impact on performance, so you should modify the schedule accordingly.
- Dell recommends that you configure notification for schedules, although this is not required. See *Notification Settings on page 21* for more information.

Constraints for Schedules

- Schedules can be created for thin clone volumes, but not for template volumes, since they are read-only.
- You can schedule either snapshot or replica Smart Copy operations. You cannot create clones by using a schedule.
- In clusters, you cannot create a schedule for the quorum disk.

Schedules in Cluster Environments

ASM/ME creates, modifies, and deletes scheduled tasks on all cluster nodes that can potentially own any of the target objects included in the scheduled task (such as volumes or application components). If a cluster node fails or goes offline at the time of the scheduled event, the schedule fails over to whichever

node becomes the owner of the target objects.

Tasks are scheduled on all nodes by default, but fail silently on all nodes that are not the current owner of the target objects in the cluster resources affected.

In clusters, you cannot create a schedule for the quorum disk.

Create a Schedule for Smart Copies

1. Right-click the object (application, collection, or volume) and select `Configure New Schedule`.
2. Specify the schedule name and the frequency at which the schedule will run—one time only, daily (or more frequent, such as multiple times per day), weekly, or monthly.

   (Optional) Enter a comment about the schedule and click `Next`.
3. ASM/ME displays a different dialog box depending on what frequency you chose. Specify the schedule options accordingly and click `Next`.
4. Depending on the schedule you are configuring, you can skip the Advanced Schedule Settings dialog box entirely, or you can configure task start and end dates and the repeat settings. For example, if you are configuring a weekly schedule and you want it to run every hour, specify the hourly repetition in the Repeat Task Settings panel. Click `Next`.
5. Specify the type of Smart Copy for the schedule. If you create a schedule for snapshot creation, you should specify how many snapshots to keep. You can specify a number between 0 and 64.
6. Select Run Task as System User, or run it as a specified user and enter the Windows credentials. You should not run it as a system user if the schedule is for objects that affect cluster resources. If you run the task as a specified user, you must provide login credentials for the account, and the account must have appropriate access to backup documents. Further, if you are using a cluster node and the schedule includes items that are related to cluster resources, you must specify an account that belongs to the Domain Administrator group.
7. Click `Create`.

Modify a Schedule

1. Select or right-click the schedule and click `Modify Schedule`.
2. Modify the frequency or name of the schedule and click `Next`.
3. Modify the settings if needed and click `Next`.

4. Depending on the schedule type, either:

   For a Smart Copy schedule, change any advanced settings, if required, then click `Next`.

   a. Change the Keep Count Setting if needed and click `Next`. You cannot modify the original Smart Copy options.

   b. Change the user account information if needed, then click `Update`.

   For a volume rethinning schedule, change any rethinning parameters, then click `Update`.

Delete a Schedule

1. Right-click the schedule and click `Delete Schedule`.
2. Click `Yes` to confirm the deletion.

You can also temporarily disable a schedule instead of deleting it. See *Disable or Enable Schedules on page 63*.

Disable or Enable Schedules

1. Right-click the schedule and select `Disable Schedule`. If you view the properties for the schedule, the `Schedule Status` field changes to `Disabled`.
2. To enable the schedule, right-click it and select `Enable Schedule`. It will run at the next possible date and time.

You can also modify or delete a schedule while it is disabled. See *Modify a Schedule on page 62* and *Delete a Schedule on page 63*.

Schedules for Volume Rethinning

You can create schedules to perform volume rethinning operations at regular intervals. ASM/ME notifies you when scheduled operations complete or fail.

You can specify how often the rethinning operation occurs. Using a schedule is suggested for volumes on operating systems that do not perform their own on-the-fly rethinning.

A schedule that rethins the volume once a week is recommended. You can increase the frequency to daily (ideally during the time of day when the volume is under the lowest workload).

For volumes on operating systems that do perform on-the-fly rethinning, you do not need to create a rethinning schedule. However, you can perform a one-time rethinning operation (for example, on volumes that were created on previous versions of the operating system, which did not do rethinning). Thereafter, the operating system's own rethinning operations will keep the volumes sufficiently thin.

To rethin a volume, the file system creates a temporary file in the volume that uses a percentage of the available free space, unmaps the space occupied by the temporary file, then deletes the file. By default, the temporary file uses 95 percent of the free space in the volume. You can reduce this value if the volume is being heavily used to avoid an out-of-space error during the rethin operation.

Note: Volume rethinning schedules will have no effect if the PS Series group is running a firmware version earlier than version 6.0.

Create a Schedule for Volume Rethinning

Before you begin, make sure you understand the interaction of Smart Copy schedules and volume rethinning operations. See *About Rethinning a Volume on page 56*.

1. Right-click the volume and select `Schedule Rethinning`.
2. Specify the schedule name and the frequency at which the schedule will run—one time only, daily, weekly, or monthly.

   (Optional) Enter a comment about the schedule and click `Next`.
3. ASM/ME displays a different dialog box depending on what frequency you chose. Specify the schedule options accordingly and click `Next`.
4. Select the rethinning parameters:
   - Percentage of unused space to rethin (default is 95%)
   - Defragment the volume before rethinning
5. Click `Create`.

The volume rethinning schedules are displayed under the Schedules list node. You can modify, disable, or delete any schedule. See *Modify a Schedule on page 62*, *Disable or Enable Schedules on page 63*, or *Delete a Schedule on page 63*

About Smart Copies

A Smart Copy is a snapshot, clone, or replica of an individual volume, application component, or a collection. Examples of application components include a Microsoft Exchange Mailbox Database, an SQL Server database, or a Microsoft Hyper-V virtual machine.

A Smart Copy consists of the following objects:

- One or more snapshots, replicas, or clones, depending on the type of Smart Copy operation and the original object.
- A backup document, describing the Smart Copy.

The resulting Smart Copy can also be called a Smart Copy Set. Even if the Smart Copy operation involves only a single volume, the result is still considered a Smart Copy Set. After you create a Smart Copy, you can then import and mount it, restore the original object from the Smart Copy, or restore the Smart Copy to a new location. You can create Smart Copies instantly, or you can create a schedule for Smart Copy creation, as described in *About Schedules on page 61*. When you create a Smart Copy, you can select from the options described in Table 17.

Table 17: Smart Copy Options

Smart Copy Type	Smart Copy Description
Snapshot	Creates a snapshot for each volume comprising the original object. For example, if the original object is a volume, the resulting Smart Copy Set will contain one snapshot. If the original object consists of a collection of two volumes, the resulting Smart Copy Set will contain two snapshots.
Clone	Creates a new volume for each volume comprising the original object.
Replica	Creates a replica for each volume comprising the original object on the PS Series group configured as a replication partner for the original objects. Each volume that is part of the original object must already be configured for replication in the group.
Backup Type	Specifies the backup behavior type that you want to create, either `copy` or `full`. This determines the behavior of the Smart Copy operation on the application log file. The actual backup behavior is application dependent.

Note: Thin Clone is also a Smart Copy Type, but this option only pertains to template volumes.

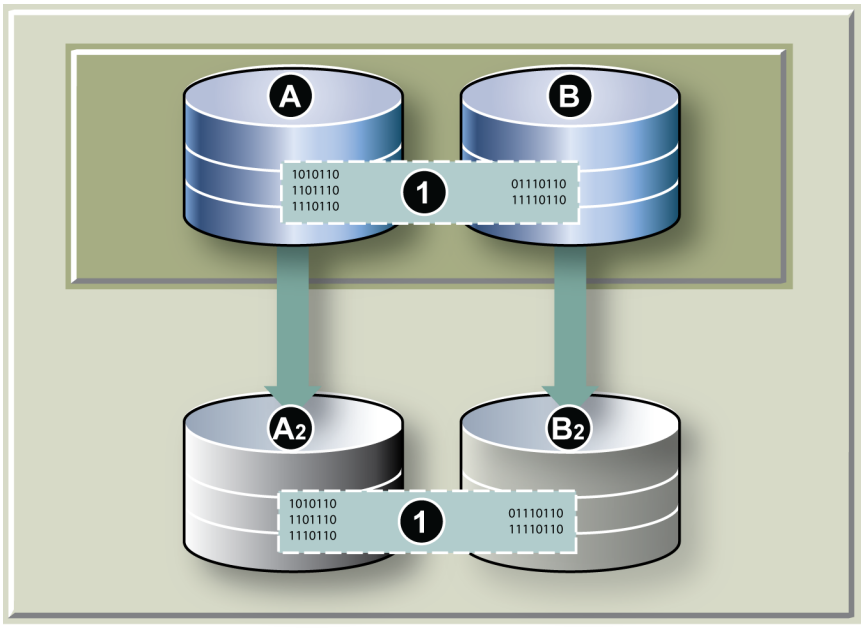
When you create a Smart Copy with ASM/ME, the Smart Copies are visible in the PS Series Group Manager GUI and CLI. For troubleshooting, it might be necessary to access and manage a Smart Copy from the PS Series group, in the Group Manager GUI. However, Dell recommends that you manage Smart Copies from ASM/ME or the VSS requestor that created them, and not the Group Manager GUI.

Torn Smart Copies

ASM/ME Smart Copy operations occur on a *per-volume* basis, which means that if you are creating a Smart Copy of a component, ASM/ME copies the volume on which the component is stored. If different data sets are spanned across a common volume, the resulting Smart Copy will contain partial information for a particular data set. Therefore Dell recommends that you place related data sets on separate volumes to avoid the possibility of creating a torn Smart Copy. Torn Smart Copies are explained in the following example.

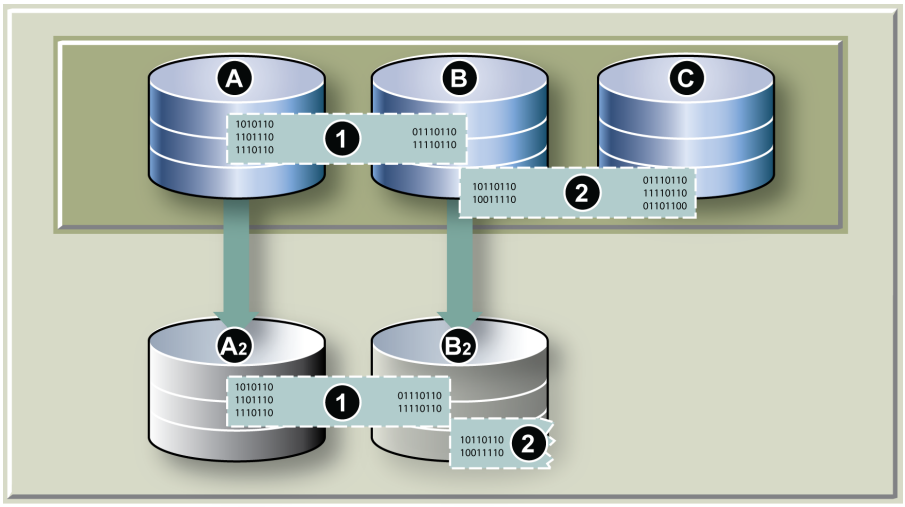
Consider the configuration shown in Figure 8. You use ASM/ME to copy the data set indicated by callout 1. This data set consists of data spanning Volumes A and B. The resulting Smart Copy Set (*A*2 and *B*2, with the same data set as callout 1) contains a full copy of the data set.

Figure 8: Complete Smart Copy



Consider the example configuration in Figure 9. Here, there are two data sets spanning three volumes. Volume B contains data from two different data sets (callouts 1 and 2).

Figure 9: Torn Smart Copy



You use ASM/ME to copy Component1, indicated by callout 1. However, ASM/ME performs its Smart Copy operations only on complete volumes. Therefore, ASM/ME must include all of the data on Volume B, even though some of it is part of a different data set (Component2, indicated by callout 2).

The resulting Smart Copy (containing A2 and B2) contains all of Component1, as indicated by callout 1. It also contains the partial data set indicated by callout 2. This partial data set is referred to as a torn data set because it does not contain all the files in the source dataset. If you use this torn Smart Copy to restore Component1, you will also partially overwrite Component2, potentially destroying live data on your production computer.

When you have a torn Smart Copy, you can restore data only from those data sets that you know to be complete in the Smart Copy. This process can take longer, depending on the size of the files you restore from the Smart Copy. Because of the risk of data loss, and the more complicated recovery procedure, Dell recommends that you avoid spanning different data sets across common volumes.

Requirements for Creating Smart Copies

The following requirements must be met before you can create a Smart Copy:

- The computer must meet the requirements described in *Windows Computer Requirements on page 12*.
- The computer must be logged in to each iSCSI volume that comprises the Smart Copy object, as described in *iSCSI Target Connections on page 15*.
- The iSCSI volumes must have drive letters assigned, as described in *Volume Mount Point and Drive Letter Assignments on page 16*.
- If you are creating a snapshot Smart Copy, the PS Series volume must have snapshot space reserved.
- If you are creating a replica Smart Copy, you must configure replication between two PS Series groups and on the volumes. The primary group must be available and ready to start replication on the volumes. Otherwise, the operation results in an error. ASM/ME does not require access to the secondary group. For information about using the Group Manager, see the *Dell EqualLogic Group Manager Administrator's Guide*.
- If you are creating a clone Smart Copy, the PS Series group must have free space equal to the size of the original volumes.
- If you want to create a Smart Copy of a volume, component, or collection that affects cluster resources, you must perform the ASM/ME operation from the node that owns the cluster resources.

Constraints for Smart Copy Operations

The following constraints apply to specific Smart Copy procedures:

- If you create or schedule a replica Smart Copy, ASM/ME allows the operation to proceed, but displays a warning that you cannot use the resulting Smart Copy for a restore operation (specifically, an in-place restore operation).
- In clustered environments:
  - Smart Copies are visible to all nodes even though the node might not be able to use the Smart Copy for recovery. That is, ownership of resources is not required to see the Smart Copies.
  - Smart Copies appear as unreachable in the Tree Panel.

- For thin clones, ASM/ME supports the creation of snapshots, clones, and replicas. These objects will be displayed under the Smart Copies folder after they are created.
- For template volumes, ASM/ME supports the creation of thin clones and clones, which will appear under the Smart Copies folder after they are created.
- Replication of a thin clone volume through ASM/ME is possible when its template volume has been replicated through the Group Manager GUI. Replication for template volumes is not supported in ASM/ME.
- For Smart Copies of SAN Boot Volumes:
  - To restore data from a Smart Copy of a boot volume, you must mount it and manually copy data from it, or perform a selective restore from the Smart Copy.
  - You can add a boot volume to a collection with other volumes. However, if you create a Smart Copy of such a collection, you cannot perform an in-place restore from that Smart Copy. You can only perform a selective restore operation.
  - The `Unmount and Logoff` operation is disabled.
- If a Smart Copy was created before you made changes to the layout of data in a volume, you cannot use that Smart Copy to recover data. Attempting to recover the data might cause data loss on the original volume. For example, assume four databases are stored on a volume, and then you create a Smart Copy of that volume. Then, you add a fifth database to the volume, and perform a restore operation from the Smart Copy. The restore operation will complete, but you will lose the fifth database.

Create Smart Copies

1. Make sure your configuration meets the requirements described in *Requirements for Creating Smart Copies on page 67*.
2. Right-click the object—either a volume, collection, or application.
3. Select Create Smart Copy Set. The `Select Smart Copy Type` dialog box is displayed.
4. In the Select Smart Copy Type dialog box, select the following:
   - Select Snapshot, Clone, or Replica, depending on what type of Smart Copy you want to create. (When you create a clone, select the `Mount Clone` option to automatically mount the clone once it is created. You can specify the drive or mount path on the next screen).
   - Select the backup behavior type: `copy` or `full`.
   - (Optional) Enter text describing the Smart Copy Set. This information will appear in the backup document.
5. Click `Next` to proceed. ASM/ME displays the Summary screen.
6. Verify the settings displayed in the Summary screen. If the information is correct, click `Create`. If not, click `Back` and make any changes.

Smart Copies appear under the Smart Copies node in the ASM/ME Tree Panel. After creating a Smart Copy Set, you can display its details, as described in *View Smart Copy Details on page 72*.

To restore the data from a Smart Copy, see *Restoring Data on page 75*.

Smart Copy Properties for Volumes

ASM/ME displays various Smart Copy properties for volumes. For volumes on PS Series groups running firmware version 6.0 or higher, the following Smart Copy properties can apply.

Synchronous Replication (SyncRep)

PS Series firmware V6.0 and higher supports a feature called Synchronous Replication, or SyncRep. SyncRep does not create replicas on another PS Series group; instead it replicates data to a SyncRep volume in another storage pool on the same group. See the *Dell EqualLogic Group Manager Administrator's Guide* for more details.

You can create Smart Copies only of Active SyncRep volumes.

Volume Undelete

PS Series groups running firmware version 6.0 or higher support a feature called volume undelete. With this feature, when a volume containing data is deleted it is moved to a folder called the Recovery Bin, where it remains until someone recovers the volume or enough time has elapsed that the volume is deleted permanently. (Volumes that contain no data are deleted immediately.) When a volume is permanently deleted, the backup document is deleted also.

If you clone a volume on a PS Series group and then delete the new (cloned) volume, any Smart Copies of the cloned volume are moved into a node called Recoverable. Only administrators logged into the PS Series Group Manager can recover deleted volumes.

- If the cloned volume is recovered, the Smart Copies are moved back to the Smart Copies node (out of the Recoverable node).
- If the cloned volume is deleted permanently (either by administrative action on the group or because the volume was not recovered before the automatic purge date), the Smart Copies are permanently deleted (removed from the Recoverable node).

Snapshot Space Borrowing

PS Series groups running firmware version 6.0 or higher support a feature called snapshot space borrowing. This feature is enabled by default for all volumes created on v6.0 or higher (however, snapshot space borrowing can be enabled on volumes created before the group was updated to v6.0).

If snapshot space borrowing is enabled for a volume, its Smart Copies display the following properties:

- Snapshot Space Borrowing (enabled/disabled/unavailable)
- Snapshot Borrow Space In Use—the amount of space that the Smart Copy (snapshot) is using from borrowed space.

  If snapshot space borrowing is enabled, the only supported snapshot reserve policy is to delete the oldest Smart Copy. Snapshot space borrowing is mutually exclusive of the snapshot space recovery policy of setting the volume and its snapshots (Smart Copies) offline.
- Features—Supports Synchronous Replication. Indicates that the volume is enabled for SyncRep. If the Smart Copy supports SyncRep, the replication state is `Not configured`.

  The Smart Copies list displays all the available Smart Copies for both the Active and Alternate volumes, but only the Smart Copies for Active volumes can be restored.

  See the *Dell EqualLogic Group Manager Administrator's Guide* for more information.

Note: If snapshot space borrowing is enabled but the volume has no snapshot reserve space configured, you cannot create a Smart Copy. Contact the administrator of the PS Series group if this volume is supposed to support Smart Copy creation.

View Available Smart Copies

The Smart Copies node in the Tree Panel displays all the Smart Copies that have been created. The tree structure includes three layers of nodes under the Smart Copy node (see Table 18). You can right-click on any node to view the available actions. For example, restore and mount operations can be performed from the second layer under the Smart Copy node.

Table 18: Locations of Smart Copies under the Smart Copies Node

Smart Copy of Object Type	Location	Comments
Individual volumes	Under the associated volume name	For example, a Smart Copy of volume `E:\` is shown under the Smart Copies node, under the name `E:\`.
Specific collection	Under the collection name	None.
Application component	Under the application component name	None.
Any Smart Copy	Unreachable node	See *Troubleshooting Unreachable Smart Copies on page 71*

Smart Copy of Object Type	Location	Comments
Any Smart Copy	Broken node	See *Troubleshooting Broken Smart Copies on page 71*
Any Smart Copy	Recoverable node	See *Troubleshooting Recoverable Smart Copies on page 71*

Troubleshooting Unreachable Smart Copies

A Smart Copy is considered Unreachable when ASM/ME cannot reach a PS Series group during the validation process.

Connection to the group or member may have been lost, or a Smart Copy made from a clustered environment may be unreachable.

Usually these are not listed under the Unreachable node, but as a regular Smart Copy with an unreachable icon instead of the normal volume or application icon.

Find out why ASM/ME cannot reach the group, and correct the problem or wait until the connection is re-established automatically.

Troubleshooting Broken Smart Copies

A Smart Copy is broken when ASM/ME cannot validate the Smart Copy because:

- Part of the set is missing (such as a missing snapshot)
- No more snapshot reserve is available for a volume
- The group deleted the oldest snapshot (Smart Copy) of a volume per its snapshot space recovery settings

Delete the broken Smart Copies and create new ones immediately to maintain your service level. See *Smart Copy Validation on page 72* for more information about validating Smart Copies.

Troubleshooting Recoverable Smart Copies

A Smart Copy is listed under the Recoverable node if the cloned volume from which it was created was deleted on the PS Series group.

These Smart Copies can be recovered if the cloned volume is restored (undeleted) on the group. See *Smart Copy Properties for Volumes on page 69* for more information.

View Smart Copy Details

You can view Smart Copy details in ASM/ME. For example, you can see whether a specific Smart Copy is a clone, replica, or snapshot, and whether the Smart Copy is mounted or not, as follows:

1. Expand the `Smart Copies` node in the Tree Panel.
2. Navigate to the specific Smart Copy for which you want to view details. Select the Smart Copy in the Tree Panel, and its properties will be displayed.

You can view individual snapshots and cloned volumes on the PS Series group where they reside. You can view replicas from either the primary or the secondary group.

Smart Copy Validation

A Smart Copy contains a backup document residing on the computer, describing one or more Smart Copies stored on a PS Series group. Under certain circumstances, the Smart Copy object stored on the group might become temporarily or permanently disconnected from the computer. For example:

- If the PS Series group runs out of snapshot space, a Smart Copy might be deleted.
- If a scheduled keep count is exceeded, an older Smart Copy might be deleted.

Under such circumstances, the backup document on the computer becomes unusable.

ASM/ME validates Smart Copy Sets to ensure that all backup documents on the computer relate to existing Smart Copies that are located on the PS Series group. A validation operation processes the entire `Smart Copies` folder. You cannot validate individual Smart Copies.

Validating a Smart Copy Set is not the same process as Verification of a Smart Copy Set. The verification operation is specific to Microsoft Exchange components.

You can configure ASM/ME to validate all Smart Copies automatically during startup. Enable automatic validation by modifying the ASM/ME General Properties.

To manually validate all Smart Copies, right-click the Smart Copies node in the Tree Panel and select `Validate Storage for Backup Documents`. ASM/ME displays a verification message that all backup documents were verified successfully.

Delete Smart Copies

Deleting a Smart Copy permanently removes the backup document and deletes the associated Smart Copies (such as snapshots) from the PS Series group. You can also delete all Smart Copies associated with a specific object such as a collection.

If you are on a cluster node and the selected Smart Copy is mounted as a cluster physical disk resource, the Delete action is disabled. To enable it, you must either put the physical disk resources for the volumes in the Smart Copy into maintenance mode or remove the physical disk resources from the cluster using the Cluster Administration tools.

To delete an individual Smart Copy:

1. Right-click the Smart Copy in the Tree Panel and select `Delete`. ASM/ME displays a warning message, prompting you to confirm the deletion.
2. Click `Yes` to confirm the Smart Copy deletion. If the Smart Copy is currently mounted, the mounted volume is deleted.

To delete all the Smart Copies for a specific volume or collection:

1. In the Tree Panel, expand the `Smart Copies` node and right-click the specific object that has multiple Smart Copies.
2. Select `Delete All Smart Copies`.

On a cluster node, any mounted Smart Copies that are cluster physical disk resource and not in maintenance mode will not be deleted.

View Backup Documents

1. Right-click the Smart Copy in the Tree Panel and select `View Backup Document`. ASM/ME displays the Backup Document.
2. Click `Close` to close the backup document.

Importing a Smart Copy

You can import a Smart Copy onto a different computer than the one on which it was created. You can import a Smart Copy in any of the following situations:

- If you created a HIT Group and you want to import a Smart Copy on another host within the HIT Group.
- If you want to import a Smart Copy on a different HIT Group host, or on a remote host.

Prerequisites for Importing a Smart Copy

The target computer on which you are importing the Smart Copy must meet the following requirements:

- It must meet the requirements described in *Windows Computer Requirements on page 12*.
- It must meet the requirements listed in *PS Series Group Requirements on page 11*.
- You must install ASM/ME on the target computer.

- To import Smart Copies on the target computer, ensure the following requirements are met:
  - Microsoft services running on the target computer must be able to access the PS Series group. See *Microsoft VSS/VDS Service Access to the Group on page 14* for more information.
  - Use ASM/ME on the target computer to enable access to Smart Copies. See *Smart Copy Access on page 29*.
  - The computer must have the appropriate VSS/VDS credentials configured. See *VSS/VDS Settings on page 28*.
  - If the computer is running Windows Server 2012 or greater or Windows 8 or greater, SMP access must be configured. See *PowerShell and SMP Access on page 29*.

Import a Smart Copy

1. In the Smart Copies node in the Tree Panel, right-click the appropriate Smart Copy and click `Import External Smart Copy`. ASM/ME displays the `Select a transportable Smart Copy` dialog box.
2. Browse to the backup document and click `Open`. ASM/ME places the document in the default backup document location (specified in General Properties). The Smart Copy will appear in the Tree Panel (under the Smart Copies node) for the HIT Group host on which you imported the Smart Copy.

If you cannot access a particular Smart Copy, it might be because the computer does not have the right security credentials or because part of the Smart Copy Set is missing. Make sure the importing computer is configured correctly.

Import a Smart Copy Within a HIT Group

To import a Smart Copy from one host in a HIT Group to a different host in the HIT Group:

1. In the Smart Copies node in the Tree Panel, right-click the appropriate Smart Copy and click `Import On Another Host`. ASM/ME displays the `Select a Host from the HIT Group` dialog box.
2. Select the HIT Group host on which you want to import the Smart Copy and click `OK`. The Smart Copy will appear in the Tree Panel (under the Smart Copies node) for the HIT Group host on which you imported the Smart Copy.

Import a Smart Copy Outside of a HIT Group

To import a smart Copy on a different HIT Group host, or on a remote host:

1. On the importing computer, open the iSCSI initiator.
2. On the Discovery tab, enter the PS Series group IP address as the Target Portal address. This enables the computer to discover the iSCSI targets presented by the group. Do not log in to a target because login occurs automatically.
3. Copy the backup document to the importing computer, or make the backup document available to a file share that is accessible by the importing computer.
4. Start ASM/ME on the importing computer.

5. In the Smart Copies node in the Tree Panel, right-click the appropriate Smart Copy and click `Import External Smart Copy`. ASM/ME displays the `Select a transportable Smart Copy` dialog box.

6. Browse to the backup document and click `Open`. ASM/ME places the document in the default backup document location (specified in General Properties). The Smart Copy will appear in the Tree Panel (under the Smart Copies node) for the HIT Group host on which you imported the Smart Copy.

If you cannot access a particular Smart Copy, it might be because the computer does not have the right security credentials or because part of the Smart Copy Set is missing. Make sure the importing computer is configured correctly.

Restoring Data

Restoring data generally involves mounting a Smart Copy, restoring data from it, and then unmounting and logging off the Smart Copy.

How you access or restore data from a Smart Copy depends on the original object (volume, collection, or application components) and the result of the Smart Copy operation (snapshot, replica, or clone).

Depending on the components that comprise the original object, each Smart Copy can include one or more snapshots, replicas, or clones created at the same time. This is because collections and applications can have multiple components (for example, multiple volumes or databases).

Options for accessing data include:

- Quickly restore the original object from a Smart Copy. (Applies to Smart Copies that contain volume snapshots or database snapshots.)
- Restore a portion of the original object from a Smart Copy. (Applies to Smart Copies that contain database snapshots.)
- Mount a Smart Copy as read-only. (Applies to replicas, or Smart Copies that contain replicas of volumes or databases.)
- Instead of mounting a replica Smart Copy as read-only, you can also clone any replica, and then mount the clone. Then replication will not be disrupted. (Applies to any replica).
- Restore the original object in a new location. (Applies to Smart Copies that contain database snapshots and database clones.)
- Clone and restore the original object in a new location. (Applies to Smart Copies that contain database replicas.)

If you make changes to a volume layout, and you have a Smart Copy that predates the layout changes, you cannot use that Smart Copy to recover data. Attempting to recover the data might cause data loss on the production volume.

You can mount or restore data from a Smart Copy of a volume that contained mount points at the time that you created the Smart Copy. However, the restored mount points will always reference the same volumes that they referenced at the point in time when you created the Smart Copy. You must manually change the restored mount points if you want them to reference different volumes, such as another mounted Smart Copy.

Mount Smart Copies

Mounting a Smart Copy makes its contents accessible to the computer. If you are restoring certain files or a subset of files contained within a Smart Copy, you need to mount it first. After a Smart Copy is mounted, you can use it to access the data you want to restore. The `Mount` option supports both Windows drive letters and mount points. A mount point is an empty folder on an existing NTFS file system that serves as an access point for a new mounted file system. Use the `Mount` option to access the data in a snapshot or clone Smart Copy created from volumes or application components.

When you mount a Smart Copy, ASM/ME displays the `Select Volume Label` dialog for every object in the Smart Copy. This dialog allows you to specify either a drive letter or a mount point on which to mount the snapshot or clone. If you take a Smart Copy of a collection that contains three volumes and then decide to mount the Smart Copy, the Select Volume Label dialog will be displayed three times so that you can specify a mount point or drive letter for each of the volumes. You can choose not to mount a certain volume, but you must mount at least one volume in the Smart Copy.

After a snapshot or clone volume has been mounted, you can copy data from it. The mounted volume appears under the Volumes node in the Tree Panel, as a disk with an assigned drive letter or mount point next to it.

As part of the mount operation, ASM/ME will automatically set the Smart Copy online on the PS Series group.

Prerequisites for Mounting Smart Copies

Before performing the procedure for mounting a Smart Copy, you must meet the following prerequisites:

- Ensure that the computer has the security credentials to access the Smart Copies in the set. If CHAP is used to restrict computer access to Smart Copies in the group, but the credentials are not stored on the computer, a dialog box is displayed, prompting you for the user name and password. See *Smart Copy Access on page 29* for more information about automatically supplying the CHAP credentials.
- Identify the snapshot or Smart Copy that you want to mount.
- Choose the drive letters or mount points that you will use.

If you intend to use a mount point, you can create an empty NTFS folder or use the Browse button to navigate to a location where you can create a new folder before performing these steps.

Mount a Snapshot or Clone Smart Copy

1. Right-click a Smart Copy in the Tree Panel and select `Mount`. The Mount Smart Copy wizard is displayed.
2. Click `Next`.
3. In the `Mount folder root` field, the default mount location is displayed. To change this, click `Browse`, and navigate to the location where you want to mount the Smart Copy.
4. The panel displays the original volume from which the Smart Copy was created, the original host, checkboxes to select whether to mount the Smart Copy (checked by default) and whether to mount it as read-only (also checked by default, and a drop-down list enabling you to select a drive letter on which to mount the Smart Copy.

   You can enter a specific mount point with either a relative path, which will be combined with the value in the mount root field, or a full path, which is used exactly as entered. The mount point is validated as you enter the data. Invalid mount points are shown in red text, and a tooltip in the volume row displays the problem with the entered mount point.
5. Select the volume label by either of two methods:
6. If there are multiple volumes in the Smart Copy (for example, if the Smart Copy is a collection with multiple volumes), click `Next` and repeat the above step for each volume you want to mount.
7. Click `Mount`. As the Smart Copy is mounted, a progress dialog box is displayed.

The newly mounted volume appears in the Volumes node of the Tree Panel, with a blue "i" overlay to indicate that it is in use. The original Smart Copy still appears under the Smart Copies node in the Tree Panel, but with a blue "i" overlay, indicating that it is in use. You should remove the mounted Smart Copy as soon as you have finished recovering data. To do this, right-click the mounted volume and select `Unmount and Logoff`.

By default, backup documents created by ASM/ME are saved as files with a "`.bcd`" extension. After a Smart Copy is mounted, the backup document extension is changed to "`.pvss`" (post-VSS).

Mount a Replica Smart Copy

1. Right-click the Smart Copy in the Tree Panel and select `Mount as read-only`. Depending on the number of replicas in the Smart Copy, one or more dialog boxes appear.
2. Specify the drive letter on which to mount the Smart Copy. The option not to mount the replica is disabled. Click `Finish`.

   ASM/ME displays the same dialog box for each subsequent replica in the set.
3. Specify the drive letter on which to mount the replica, or choose not to mount it. You must mount at least one replica from the Smart Copy.

You can enter a specific mount point with either a relative path, which will be combined with the value in the mount root field, or a full path, which is used exactly as entered. The mount point is validated as you enter the data. Invalid mount points are shown in red text, and a tooltip in the volume row displays the problem with the entered mount point.

4. Click `Next` until you have processed all the replicas in the Smart Copy Set, then click `Finish`. ASM/ME displays a progress bar as it mounts the Smart Copy.

The Smart Copy is mounted as a read-only volume, and it continues to appear under `Smart Copies` in the Tree Panel with a blue "i" on the icon indicating that it is in use. The options to unmount and logoff from the Volume node and Smart Copy node also provide you with the option to delete the Smart Copy.

While a replica is being mounted, replication is temporarily paused until the process is completed. Any replication on that replica set while mounted will be automatically canceled until the replica set is unmounted and demoted.

Make a Mounted Smart Copy Accessible to Cluster Nodes

If you want the mounted Smart Copies to be available to all nodes in a cluster, Dell recommends that you perform additional manual steps to make the mounted Smart Copy accessible to other nodes in the cluster in the event of a failover:

1. An iSCSI session is started only for the current node by ASM/ME. Use the iSCSI initiator to log in to the target for the mounted Smart Copy for each of the nodes that might need to access the Smart Copy. For information about the iSCSI initiator, see *iSCSI Target Connections on page 15*.
2. Add a physical disk resource for the mounted Smart Copy using the Microsoft Cluster Management utilities so that ownership can transfer to a passive node in the event of a failover.

Restore Data From a Smart Copy

To restore a complete volume (an in-place restore), you can use the `Restore` option. For snapshot Smart Copies of volumes or volume collections that do not involve databases, the restore operation replaces the current data in the volumes or volume collection with the data in the Smart Copy. The Smart Copy continues to exist, and you can restore from it as often as necessary.

For clustered systems, restore options are enabled only when appropriate. You cannot restore from Smart Copies of a volume containing the shared folder.

To restore data from a Smart Copy:

1. Right-click the Smart Copy from the Tree Panel and select `Restore`.
2. Confirm that you want to restore the volume or collection from the selected Smart Copy.

Options for Unmounting and Logging Off a Smart Copy

When you have mounted a Smart Copy and you have finished any restoration operations, you can unmount and log off the Smart Copy. As part of the unmount operation, ASM/ME will automatically set the Smart Copy offline on the PS Series group.

For replica Smart Copies, you have two options for unmounting and logging off a replica:

- `Unmount and Logoff`—Unmounts, logs off, and demotes the replica set.
- `Delete`—Unmounts, logs off, and demotes the replica set as necessary. It then deletes the replica unless it is the most recent replica in the replica set. In the latter case, it is necessary to retain the replica to ensure consistency of the replica set.

Constraints for Unmounting and Logging Off a Smart Copy

- Unmounting and logging off a Smart Copy automatically breaks VSS control of the Smart Copy. You can no longer manage the copy by using Microsoft utilities, however, you can manage it by using ASM/ME.
- If the Smart Copy is a snapshot, you can delete the snapshot as part of the unmount and logoff operation.
- If the mounted volume is a snapshot, and additional mounted snapshots from the same Smart Copy exist, the option to delete the Smart Copy is disabled. To delete the Smart Copy:
  - Unmount and log off all the corresponding volumes.
  - Delete the Smart Copy that contains all the volumes.

Prerequisites for Unmounting Smart Copies in a Cluster Environment

- Smart Copies must not be in use.
- Volumes must be put into maintenance mode, if they are cluster resources, using the appropriate procedure depending on the version of product and server (Windows Server 2008 Cluster Administrative tools). If you are permanently unmounting or deleting the volumes, then you also need to remove any dependencies on the volumes' physical disk resources and delete the physical disk resources using the Cluster Administration tools.
- If the Unmount and Logoff was temporary, after remounting the volumes, take them out of maintenance mode.
- The node must own all cluster resources in the cluster resource group.

Unmount and Log Off a Smart Copy

1. From the Volumes node in the Tree Panel, right-click the mounted Smart Copy and select `Unmount and Logoff`. ASM/ME displays the `Unmount and Logoff` dialog box.

2. (Optional) Check the box for deleting the snapshot from the PS Series group represented by this volume. Because the selected volume is a mounted snapshot and not a clone, you have the option to select the snapshot for deletion as soon as it is no longer mounted. Check the box to delete the snapshot.
3. Select `Logoff` to proceed with the operation.

View Multipath Information

If you have MPIO configured, you can display the multipath information for hosts and host volumes by expanding the MultiPath node in the tree view.

The MultiPath screen displays:

- A time line that you can adjust to specify the amount of data shown in the chart for Host Volumes and Host Sessions.
- The current MPIO settings and a link to open the MPIO Settings screen.
- A chart showing the number of connections to hosts and host volumes over the selected time range.
- A table listing details about the I/O during the selected time period, including:
  - Volume name: Name of the connected iSCSI volume.
  - Session: Identifier for a unique session connecting a host to a PS Series array.
  - Host IP address: The TCP/IP address of the link source device. This device is the NIC or HBA installed in the host.
  - Target IP address: The TCP/IP address of the PS Series array's Ethernet port.
  - Session Uptime: The total time that the session has been active.
  - Managed session: Indicates whether or not the session is actively managed.

View I/O Details

You can take a closer look at the multipath information by clicking the IO Details node under the MultiPath node.

This displays a screen that includes:

- A time line that you can adjust to specify the amount of data shown in the chart below the time line.
- A drop-down list from which you can choose whether to display all volumes or a specific volume.
- A chart showing the number of read and write operations over the selected time period, in terms of KB/sec and the number of IOPs at various points in time over the selected period.
- A table listing details about the I/O during the selected time period, including:
  - Volume: Name of the connected iSCSI volume.

- Session Count: Count of host sessions connected to the volume.
- Read Rate: Read rate on the volume across all sessions.
- Write Rate: Write rate on the volume across all sessions.
- Read IOPS: The number of read operations per second across all sessions.
- Write IOPS: The number of write operations per second across all sessions.

6 Using ASM/ME with Microsoft Exchange

ASM/ME supports Microsoft Exchange 2010 and 2013. Depending on your particular configuration and the version of Exchange that you are running, data recovery procedures might vary. See *Using ASM/ME with Hyper-V on page 115* if you intend to run Microsoft Exchange with a Hyper-V virtual machine. In such configurations, some ASM/ME operations are constrained.

View Exchange Applications in ASM/ME

ASM/ME displays the Microsoft Exchange Writer as a supported application under the Applications node in the Tree Panel.

The HIT/Microsoft installer verifies that a supported version of Microsoft Exchange Server exists on the target installation computer. If ASM/ME detects an unsupported version of Microsoft Exchange Server, a red arrow is displayed next to the application in the ASM/ME Tree Panel.

Exchange 2010 Writers

For Microsoft Exchange 2010, ASM/ME displays both the Microsoft Exchange Writer (Exchange Information Store) and the Microsoft Exchange Replica Writer (Exchange Replication Service) under the Applications node.

For example, assume you are running a two-node Data Availability Group (DAG). One Mailbox Database, MD1, is mounted on Server A, the first node. Two other Mailbox Databases, MD2 and MD3, are mounted on Server B, the second node. Since Server A and Server B replicate to one another, the instance of ASM/ME running on Server A displays two applications under the Applications Node:

- The Microsoft Exchange Replica Writer (Exchange Replication Service) expands to display the two Mailbox Database replicas, MD2 and MD3.
- The Microsoft Exchange Writer (Exchange Information Store) expands to display MD1.

Similarly, an instance of ASM/ME running on Server B displays two applications under the Applications Node:

- The Microsoft Exchange Replica Writer (Exchange Replication Service) expands to display the MD1 replica.
- The Microsoft Exchange Writer (Exchange Information Store) expands to display MD2 and MD3.

Exchange 2013 Writer

For Microsoft Exchange 2013, only one Microsoft Exchange Replica Writer (Exchange Replication Service) is displayed under the Applications node.

For Microsoft Exchange 2013, only one Microsoft Exchange Writer (Exchange

Replication Service) is displayed under the Applications node. The Mailbox Database running as passive copies will be displayed under the Replica node in Microsoft Exchange Writer (Replication Service) under Applications.

For example, assume you are running a two-node Data Availability Group (DAG). One mailbox database, MD1, is mounted on Server A, the first node. Two other Mailbox Databases, MD2 and MD3, are mounted on Server B, the second node.

Since Server A and Server B replicate to one another, the instance of ASM/ME running on Server A displays two subordinate nodes under the Microsoft Exchange Writer node:

- The Microsoft Exchange Writer (Exchange Replication Service) expands to display the two subordinate nodes. One is the server name and the other is called Replica.
- The node with the server name expands to display MD1.
- The node labeled `Replica` expands to display MD2 and MD3.

Similarly, an instance of ASM/ME running on Server B displays two subordinate nodes under the Microsoft Exchange Writer node:

- The Microsoft Exchange Writer (Exchange Replication Service) expands to display the two subordinate nodes. One is the server name and the other is labeled `Replica`.
- The node with the server name expands to display MD2 and MD3.
- The node labeled `Replica` expands to display MD1.

Microsoft Exchange Operations

Table 19 lists the general Exchange-related tasks you can perform using ASM/ME.

Table 19: General ASM/ME Tasks You Can Perform in Exchange Environments

Task	See Section
Create application-consistent Smart Copies of mailbox databases (for Microsoft Exchange 2010 and 2013), volumes and collections.	*Create Exchange Smart Copies on page 94*
Set up Smart Copy schedules.	*Schedule Smart Copies for Microsoft Exchange Components on page 97*
Perform In-Place or Brick-Level restores to recover and restore Exchange data.	*Recover Microsoft Exchange Data on page 100*
Use a command line for creating site-specific scripts.	*Use a Script to Create Smart Copies on page 185*

Task	See Section
For all supported Microsoft Exchange versions, you can clone a mailbox database from a source Exchange server, and then set it up on the same server or on a different Exchange server.	*About the Clone and Restore as New Operation on page 104*

Overview of Exchange Smart Copies

If your Exchange Mailbox Databases and logs are stored on a PS Series group, you can create Smart Copies of your Exchange components. A Smart Copy of a Mailbox Database (for Exchange 2010 and 2013) will automatically include a copy of its logs and mailstores. You should not create Smart Copies of individual logs and mailstore components.

You should perform Checksum Verification on Smart Copies to ensure data integrity and consistency as potential recovery backup copies. You can run this procedure in one of the following ways:

- Immediately, at the time of Smart Copy creation
- After Smart Copy creation
- As part of a scheduled Global Verification Task
- By using command lines or scripts
- On a remote host or verification server dedicated to running Checksum Verification

See *Checksum Verification and Soft Recovery on page 86* for more information about Checksum Verification.

After your Exchange Smart Copies are created, you can recover data from them using In-place or Brick-level recovery. In-place recovery is a point-in-time restoration of all data in an entire Mailbox Database. Brick-level recovery involves creating a Recovery Mailbox Database (for Microsoft Exchange 2010 and 2013) to set a Smart Copy snapshot online and recover information that was lost from production computers. See *Recover Microsoft Exchange Data on page 100* for more information.

Microsoft Exchange eseutil.exe Utility

Several ASM/ME operations include an option to specify the location of the Microsoft Exchange Server `eseutil.exe` utility. ASM/ME uses this Exchange utility to verify data integrity. The path defaults to the standard Exchange installation as follows:

```
C:\Program Files\Exchsrvr\bin\eseutil.exe
```

If the `eseutil.exe` utility is not at the default location, you are prompted to specify a path before you can perform any relevant Exchange-specific operations. See the Microsoft Exchange documentation for information about `eseutil`.

To reduce the I/O load created by Checksum Verification, you can add a one second delay after a specified number of I/Os. You do this by specifying a registry key value as follows:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\EqualLogic\ASM\Settings]
"EseutilThrottle"=dword:00001000
```

For example, if you specify a registry value of 1000, it results in a one second sleep after every 1000 Checksum Verification I/Os. The range for this value is 100 to 100000.

Recovery Considerations for Microsoft Exchange

- ASM/ME does not allow torn Smart Copies. A scheduled task will fail if it will result in a torn Exchange Smart Copy. See *Torn Smart Copies on page 65* for an explanation of torn Smart Copies.
- ASM/ME prevents you from creating a multiple writer Smart Copy Set where the Exchange Writer and the SQL Server are included in a Smart Copy Set. This condition is detected whether you create the Smart Copy from a volume, an application, or a collection. ASM/ME also detects multiple writer Smart Copy Sets when you attempt to create schedules for such objects. If a multiple writer schedule runs, a warning is included in the notification email. It is possible to create an invalid (multiple writer) configuration after a schedule was created. If you do this, the schedule will fail when it runs.
- If you create a Smart Copy Set that contains multiple Exchange components from the same writer, ASM/ME displays a warning but allows the operation to proceed. Dell recommends that you always configure your Mailbox Databases (for Microsoft Exchange 2010 and 2013) on separate volumes. This configuration ensures that if you do need to restore data, you will restore only the damaged component. If you configure multiple Exchange Mailbox Databases on a single volume, all databases are restored even if only one database was damaged.
- If you use Microsoft Exchange utilities to relocate Mailbox Database components, and you have a Smart Copy that predates the change, you cannot use that Smart Copy to recover data. Instead, use a Recovery Mailbox Database (for Microsoft Exchange 2010 and 2013) created from that Smart Copy.

Checksum Verification and Soft Recovery

For Smart Copies of Microsoft Exchange components, you should perform Checksum Verification to ensure data integrity. Checksum Verification verifies the integrity of all files in the Smart Copy by using page Checksum Verification. Soft Recovery configures the Smart Copy to replay the transaction logs to put the databases into a clean shutdown state.

When you create a Smart Copy, you can run Checksum Verification and Soft Recovery as follows:

- During Smart Copy creation—Run the operations while the Smart Copy is being created.
- After Smart Copy creation—Run the operations after you have created a Smart Copy. If you are running on a cluster, the node must own the cluster resources. If the operation completes successfully, then this option will be disabled the next time the window is displayed.

- As part of a scheduled Global Verification Task—If you are running on a cluster, the node must own cluster resources required at the time that it selects a Smart Copy targeted for global verification to be processed.
- On a remote host—Run the operation as part of the Global Verification Task on a remote verification server.

When a scheduled Global Verification Task operation executes, ASM/ME updates the Smart Copy node to show that Checksum Verification and Soft Recovery is in progress. A soon as the operation is complete, ASM/ME updates the Smart Copy node to show the result.

If you notice I/O performance problems when running checksum verification, consider changing the `eseutil.exe` registry key value. This procedure is defined in *Microsoft Exchange eseutil.exe Utility on page 85*.

If the Smart Copy is a replica of an Exchange component, rather than a snapshot or clone, the Checksum Verification and Soft Recovery procedure is different. Volume replication is a continuous process and ASM/ME provides options to perform Checksum Verification and Soft Recovery without disrupting replication. For Microsoft Exchange replicas only, the option to perform Checksum Verification is not available immediately after you create a Smart Copy. See *Checksum Verification and Soft Recovery for Replicas on page 96* for more information.

Run Checksum Verification and Soft Recovery Immediately

You can run Checksum Verification as part of creating a Smart Copy of an Exchange component, by selecting the following options:

- `Perform Checksum Verification`
- `Perform Soft Recovery`

Also, in the `Perform Task` panel, select `Immediately after Smart Copy creation`.

If you do not select Checksum Verification and Soft Recovery operations at the time you create a Smart Copy Set, you can select them from the Smart Copy node. See *Run Checksum Verification and Soft Recovery After Smart Copy Creation on page 87*.

This option is available only if you did not already run Checksum Verification and Soft Recovery, or if you ran it, but one of the operations failed. If the Smart Copy is already mounted, ASM/ME sets its access state to Read-Write (if the Smart Copy is not already set to Read-Write).

Run Checksum Verification and Soft Recovery After Smart Copy Creation

If you did not select the options to perform Checksum Verification and Soft Recovery while you created a Smart Copy, then you can perform these operations from the Smart Copies node. The Verification and Recovery option is only visible if you have not already run this task, or if you ran a Verification and Recovery task but it did not complete successfully. To run the Verification and Recovery task from the Smart Copies node:

1. Expand the Smart Copy node until an Exchange Smart Copy (indicated by the gray camera icon) is visible.
2. Right-click a Smart Copy node (indicated by the gray camera icon) and select `Verification and Recovery`.
3. In the Options dialog box, you can select the following options:
   - Perform a Checksum Verification.
   - Perform a Soft Recovery. If you select Soft Recovery, the Smart Copy is made writable.
   - Specify a path to the `eseutil.exe` utility if it is not located in the default Windows Exchange installation folder. See *Microsoft Exchange eseutil.exe Utility on page 85* for more information.
4. Click `Verify`. ASM/ME displays a dialog indicating that Checksum Verification and Soft Recovery started in the background. You can continue with other operations.

When the operation completes, ASM/ME refreshes the Tree Panel and displays the status of the Smart Copy in its properties. For example, when viewing the Checksum Verification State, it will say "Successfully Verified." The duration of the operation is also provided, to assist you in future planning.

Schedule a Global Verification Task for Checksum Verification and Soft Recovery

The Global Verification Task is a scheduled background activity that you can run from any designated user account. The user account that you specify should have read-write access to the backup documents that you want to verify. Otherwise, you can choose to run the operation from the computer's Administrator account. The Global Verification Task performs Checksum Verification and Soft Recovery processing on any Exchange Smart Copy that you have included in the schedule. When you configure ASM/ME, you can set up a Global Verification Schedule to run the Global Verification Task. See *Verification Settings on page 25* for how to configure this setting.

Constraints for Global Verification Task

The Global Verification Task attempts to verify all Smart Copies, subject to the following constraints:

- Smart Copies are verified serially. You can specify whether to begin processing with the newest copies, or the oldest copies (chronological sequence).
- If a running verification operation takes longer than the time allotted in the schedule, (that is, it exceeds the specified end time), the operation is not terminated. The operation runs to completion but no new operations are started.
- If a common file share is used by several hosts running Global Verification Tasks during the same or overlapping window (either in a non-cluster configuration, or DAG), then a different backup document location folder should be configured for each of the hosts to avoid any issues in accessing backup documents.
- Any operations that cannot run in the time available are postponed to the next start time. These operations will run first.

- If the host is rebooted before the Global Verification completes, the verification will start again when the host is back up. To continue with verification, you must manually restart it.

Creating a schedule does not guarantee that all backup documents are always verified. You must make sure that operations are completed successfully and that there is adequate time available.

If the host running the Global Verification Task fails, the Global Verification Task on the inheriting host may not process all of the existing unverified Smart Copies until the next time that it is scheduled to run. You can force the Global Verification Task to restart on the inheriting host using ASM/ME.

Create or Modify the Global Verification Task

When you select the Schedules node and Smart Copies node, you have options to create or modify the Global Verification Task. You can also use the following options to create or modify the Global Verification Task on a *verification server*, which is a server that is dedicated to the verification operation:

- Create Global Verification Task—This option is displayed only if the Global Verification Task does not exist. If it does exist, a node titled: `Global_Verification_Task` is displayed in the ASM/ME Tree Panel under the Schedules node.
- Modify Global Verification Task—This option is displayed only if the Global Verification Task exists. If it does not exist, there is no `Global_Verification_Task` node in the Tree Panel under the Schedules node.

If you want to support failover of the Global Verification Task processing in a cluster configuration, you must create a Global Verification Task on each node that is a potential owner node for an Exchange Server Cluster Group. Additionally, you need to manually propagate any changes to the Global Verification Task to the possible owner nodes if you want them to be synchronized. This requirement is different than that for other scheduled tasks.

ASM/ME creates a Global Verification Task automatically the first time you either create a Microsoft Exchange Smart Copy or create a schedule of Smart Copies, providing the following conditions apply:

- No preceding version of a Global Verification Task exists under the Schedules node.
- When creating the Smart Copy, you select the local Global Verification window as the scheduled verification time.

Manually Create a Global Verification Schedule

1. In the Tree Panel, right-click the Schedules node and select `Create Global Verification Task`. Select from the options described in Table 20 and click `Next`.

   The following dialog box appears: `Provide User Account Information`.

2. Select whether to run the task as a system user or as a specified user. These options are described in Table 20.

3. Click `Create` to begin creating the Global Verification Task. In the Tree Panel, the `Global_Verification_Task` node should appear under the Schedules node.

Table 20: Global Verification Task Schedule Options

Option	Description
`Process Smart Copies Created by this host`	Processes only Smart Copies created on the local computer.
`Process Smart Copies Created by another host`	Processes Smart Copies created on a remote computer. (See *Run Checksum Verification and Soft Recovery on a Remote Host on page 91*).
`Start Time`	The start time of the local Global Verification window, which is the time period during which the Global Verification Task runs. Typically, you specify a time of low computer usage to make best use of computer resources. The Start Time must precede the End time by three hours or more. If the Start Time and End Time are the same the window is 24 consecutive hours (full time verification).
`End Time`	The end time of the local Global Verification window. This time must be at least three hours later than the start time.
`Eseutil location`	The path to the Microsoft Exchange `eseutil.exe` utility (a database maintenance program), if it is not located at its default installation path.
`Run task as system user`	Choose this option to specify the SYSTEM login as the account under which the operation runs. Do not specify the SYSTEM account if you are also performing verification on a remote verification server.
`Run task as specified user`	Choose this option to use the current login or to specify an account as the run account for the operation. You must provide the following information: `User Name` - Specify an account name for the account under which this operation will run. (The account that you specify must have appropriate access to the backup documents). `Password` - Type the account password. ASM/ME uses the password only during schedule creation and the password is not retained.

Table 21 describes the right-click options available to you once the Global Verification Schedule is created.

Table 21: Right-Click Options for the Global Verification Schedule

Option	Description
`Run Now`	Ignores the scheduled start time and launches the Global Verification Task

Option	Description
	immediately.
`Modify the schedule`	Displays the `Create or Modify Global Verification Task` dialog box.
`Delete the Schedule`	Deletes that schedule. No scheduled verification is performed until you create a new schedule manually or specify scheduled verification for a newly created Smart Copy. The Global Verification times remain as specified in the last schedule that you created.
`Disable Schedule`	Disables that schedule. If you view the properties for the schedule, the Schedule Status field changes to Disabled. To enable the schedule, right-click it and select Enable Schedule. The schedule runs at the next possible date and time. You can also modify or delete a schedule while it is disabled.

When scheduled, the Global Verification Task runs as a process named `EqlExVerifier.exe`, which you can view by using the Windows Task Manager. Only one instance of the `EqlExVerifier.exe` process runs as the automated Global Verification Task on a computer at any time. You can launch two more instances of `EqlExVerifier.exe` manually, or three instances if the automated Global Verification Task is not currently running.

Run Checksum Verification and Soft Recovery on a Remote Host

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

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.

Remote Host verification requires two hosts with the same installed versions of ASM/ME and Exchange Management Tools. Further, a shared network folder or drive to provide a Smart Copy repository must be set up.

One of the hosts functions as the *creator* server, creating Smart Copies, the second computer 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 offpeak Global Verification window on the creator server, such as the default 8:00 PM to 6:00 AM window. You might then configure the creator server to run verification on the remote computer, setting the verification server's Global Verification window to 24 hours.

You can run remote verification operations manually, you can schedule them individually, or you can schedule them as part of a Global Verification Task.

Remote Host Checksum Verification and Soft Recovery in a HIT Group

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 guideline.

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. The cluster node and its remote host will share the same backup document directory. For example, if your HIT Group is comprised of a 4-node DAG, then you will need to allocate four separate hosts for remote host Checksum Verification and Soft Recovery (1 host per node). You need to do this only once if verification is set to be done simultaneously on all four hosts at the same time.

Prerequisites for Configuring a Verification Server

- Install the same release of Host Integration Tools on both the verification server and on the Smart Copy creator servers.
- 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 hotfixes available from Microsoft.
- Make sure that the verification server and any servers that created the Smart Copies are part of the same Microsoft Windows domain.
- Make sure that the verification server and any servers that created the Smart Copies are able to access a shared location for Smart Copies.
- Make sure an appropriate network access and bandwidth are available to process the Global Verification Tasks of client computers.
- Make sure a UNC or shared location exists.

Configure a Verification Server

Note: You must ensure that the Exchange utility that performs the Checksum Verification and Soft Recovery tasks is installed on whatever host you are configuring as a Verification Server. If you installed Exchange on the server, then this is taken care of for you. However, a full Exchange installation is not needed to be a Verification Server. Dell EqualLogic recommends that the Verification Server not be an Exchange Server to offload that processing so as to not affect mail services. If this is the case, you must manually copy the eseutil.exe and ese.dll files to the Verification Server.

1. Start the Remote Setup Wizard to enable the verification server to access the PS Series group.
2. Find the location of the shared Smart Copy folder on the creator server:

   Launch ASM/ME and click Settings in the navigation area.

   a. Click `General Settings`.

   b. Find the path specified for the Auto-Snapshot Manager Document Directory. In a DAG, this is the UNC path.

   c. Copy the path to a text file or write it down.
3. Configure the volume access control records on the PS Series group as follows:

   – For snapshot Smart Copies, the host must have access to the volume and its snapshots.
   – For clone Smart Copies, the host must have access to the volume.
   – For replica Smart Copies, the host must have access to the replication partner, where the replica sets are stored. Also make sure that the original volume (on the primary group) is *not* accessible by the verifier host.

   For help, see the *Creating Access Control Records* procedure described in the *Volume Management* section of the Group Manager GUI online help. Also see *Checksum Verification and Soft Recovery for Replicas on page 96*.
4. Map a drive on the verification server to the shared Smart Copy folder that you identified in Step 2. Use the same drive letter if possible.
5. Point ASM/ME to the shared Smart Copy folder on the verification server:

Launch ASM/ME and click Settings in the navigation area.

   a. Click `General Settings`.

   b. Specify the path to the shared folder that you defined in step 2. Make sure that the drive letter specifies the local mount point.

   c. Click `Save` to update the properties. ASM/ME finds the Smart Copies on the creator server and updates the Tree Panel. Because these Smart Copies are not found on the local computer, ASM/ME displays a blue question mark icon on the node.
6. Set up a Global Verification Task on the verification server, using the procedure described in *Schedule a Global Verification Task for Checksum Verification and Soft Recovery on page 88*, but ensure that you select the `Process Smart Copies created by another host` option. Also ensure the following:

   a. Consider setting the Global Verification window to the maximum possible 24-hour period if the sole purpose of the verification server is Checksum Verification and Soft Recovery.

   b. Specify a user account that has appropriate permission to access the Smart Copies (according to the shared folder settings).

The verification server now watches the shared folder and processes any unverified Smart Copies according to its Global Verification window. When you select a Smart Copy, its verification status is listed in its properties.

View Checksum Verification and Soft Recovery Status

1. Expand the Smart Copy node until an Exchange Smart Copy (indicated by the gray camera icon) is visible.
2. Select a Smart Copy node (indicated by the gray camera icon) and view its properties. If the status is successful, ASM/ME will display "Successfully Verified" and "Successful" for Checksum Verification and Soft Recovery status, respectively.

Checksum Verification and Soft Recovery Logging and Notification

Your notification preferences for Smart Copy creation also apply to Checksum Verification and Soft Recovery operations. However, you have the option to combine the Checksum Verification notification and the Soft Recovery notification emails into a single message, or receive two separate notifications. Use the ASM/ME Notification Settings tab to configure this option. See *Notification Settings on page 21*. If you configure notification email, a partial log from the most recent run is attached to the email.

Any errors that occur during Checksum Verification and Soft Recovery operations are logged in the event log. A running log is maintained by the verifier at the following location:

```
Program Files\Equallogic\Logs\EqlExVerifier.log
```

To avoid consuming excessive disk space, ASM/ME creates a new log file when the current file exceeds 10MB. The old log file saved in previous log is saved at the following location:

```
Program Files\Equallogic\Logs\EqlExVerifier_0.log
```

ASM/ME maintains two log files only: the current log, and the preceding log. If you need to retain older logs, use the Windows Task Scheduler to copy the log to another location.

Create Exchange Smart Copies

You can create Smart Copies of Mailbox Databases (for Microsoft Exchange 2010 and 2013), volumes, and collections. If you need help understanding options in the Create Smart Copy wizard, see Table 22.

1. Expand the `Applications`, `Volumes`, or `Collections` node.
2. Right-click an Exchange component and click `Create Smart Copy`. ASM/ME displays the `Create Smart Copy` dialog box.
3. Select a Smart Copy type, Backup Type, and optionally enter a description. If you are creating a Smart Copy of an Exchange application component, only the Copy backup type is supported.
4. Click `Next`.

a. If you are creating a snapshot or a clone of an Exchange application component, ASM/ME displays the `Data Verification and Soft Recovery Options` dialog box. Proceed to step 5.

b. If you are creating a replica of an Exchange application component, ASM/ME displays the `Exchange Replica Verification Options` dialog box. Select the verification method (Clone and Verify, Promote and Verify, or Defer Verification) and click `Next`. For a detailed description of each of these options, see *Checksum Verification and Soft Recovery for Replicas on page 96*.

5. Select from the options in the `Data Verification and Soft Recovery Options` dialog box.

a. If you deselect both the Checksum Verification and Soft Recovery options, the dialog box appears dimmed. Click `Next` and proceed to step 6.

b. Select either the Checksum Verification option, the Soft Recovery option, or both options. Verify the EseUtil.exe location, select when to perform the tasks, and click `Next`. ASM/ME displays the `Summary` dialog box.

c. If you are creating a replica Smart Copy, the options in this dialog box will be selectable or grayed out depending on what option (Clone and Verify, Promote and Verify, or Defer Verification) you chose in step 4. For example, if you chose the Defer Verification option, all options in this dialog box will appear dimmed and you can just click Next.

d. If you need to change the remote Global Verification window, you must change it on the remote computer.

6. Verify the settings displayed in the Summary screen. If the information is correct, click `Create`.

Microsoft Exchange Smart Copy Options

Table 22 describes the different options for Microsoft Exchange from the Create Smart Copy wizard.

Table 22: Exchange Smart Copy Options

Planning Item	Description
`Snapshot`	Creates a snapshot for each volume comprising the original object.
`Clone`	Creates a new volume (clone) for each volume comprising the original object.
`Replica`	Creates a replica for each volume comprising the original object on a PS Series group configured as a replication partner for the original volumes. If you select Replica, ASM/ME displays an additional option dialog box described in step 4.
`Backup Type`	Select `Copy`. This option is the only supported backup type.
`User Comments`	(Optional) Enter text describing the Smart Copy Set. This information will appear in the backup document.

Planning Item	Description
`Checksum Verification`	Verifies the integrity of databases in the Smart Copy by using the `eseutil.exe` database maintenance utility.
`Soft Recovery`	Brings all databases to a clean shutdown. For Exchange replicas, immediate Soft Recovery is not available.
`Location of eseutil.exe`	If the location of the `eseutil.exe` utility is not in its default installation as indicated in the text field, specify the path to its location. (See *Microsoft Exchange eseutil.exe Utility on page 85*.)
`Perform Task`	Specify the time and method of running Checksum Verification and Soft Recovery. Select from 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 Mailbox Database replicas. • Global verification window. Specify this option to use the Global Verification Window times that you configured in ASM/ME as described in *Verification Settings on page 25*. 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 computer 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 computer. The remote computer must be configured to run the operation. (See *Run Checksum Verification and Soft Recovery on a Remote Host on page 91*).

Checksum Verification and Soft Recovery for Replicas

If the target Smart Copy is a replica of an Exchange component, rather than a snapshot or clone, the Checksum Verification and Soft Recovery procedure is different. Volume replication is a continuous process and ASM/ME provides options to perform Checksum Verification and Soft Recovery without disrupting replication. For Microsoft Exchange replicas only, the option to perform Checksum Verification is not available immediately after you create a Smart Copy.

The following Checksum Verification and Soft Recovery options are available during replica smart copy operations:

- Clone and Verify—Creates a clone of the replicated volume and performs Checksum Verification only on the clone.

  This procedure requires storage capacity on the secondary group that is at least the same size as the replica. (That is, if the replica is 500GB, you will need 500GB of available space). Use the Group

Manager GUI to view and make space available on the secondary group if necessary.

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 undergoes Checksum Verification. Soft Recovery runs on the original Smart Copy during a restore operation.

- Promote and Verify—Temporarily promotes the replica, making it functionally equivalent to the base volume. ASM/ME performs Checksum Verification and Soft Recovery on the promoted replica.

  This operation is supported on both local and remote hosts. T remote host must have access to the replication partner group. Make sure the volume on the source group does not have an access control record that allows the remote host to access it, because that could result in data corruption.

  This process has the advantage of not requiring any additional storage capacity on the secondary group. However, data replication is paused during Checksum Verification and Soft Recovery, making the promoted replica a point-in-time copy of the base volume. Scheduled replications will fail during Checksum Verification and Soft Recovery of a promoted replica because replication is paused.

  This operation allows you to run a Soft Recovery on the original Smart Copy before you begin a data restore.

  When Checksum Verification and Soft Recovery is complete, ASM/ME automatically demotes the replica and replication resumes. The next scheduled operation on the volume will resume.

- Defer Verification—Defers Checksum Verification and Soft Recovery to a later time. You can start the procedure manually at some future time.

  If you defer Checksum Verification and Soft Recovery permanently, you might find that the replica is corrupted and unusable when you try to restore data from the replica to the base volume.

Schedule Smart Copies for Microsoft Exchange Components

You can create Smart Copy scheduled tasks for Exchange 2010 and 2013 Data Availability Groups.

1. Right-click the Exchange component and click `Configure New Schedule`. The following dialog box appears: `Schedule Name and Frequency`.
2. Enter a name for the task, and select a frequency: Daily Or More Frequent, Weekly, Monthly, or One Time Only. Click `Next`.
3. ASM/ME displays a different dialog box depending on the frequency you chose in Step 2. Enter the information specified in Table 23 depending on the frequency you chose, then click `Next`.

   ASM/ME displays the `Advanced Schedule Settings` dialog box.
4. Specify the advanced schedule options (Table 24), then click `Next`. ASM/ME displays the `Smart Copy Options` dialog box.

5. Select from the Smart Copy options (Table 24), then click `Next`. ASM/ME displays the `Data Verification and Soft Recovery` dialog box.
6. Optionally, select the Perform Checksum Verification and Perform Soft Recovery options. If you do not select either option, the dialog box becomes grayed out. Click `Next`. If you select those options, specify the EseUtil Location, and select when you would like to perform the tasks. Click `Next`. ASM/ME displays the `Provide User Account Information` dialog box.
7. Select from the user account options (Table 24). Click `Create` to create the schedule.

Table 23: Schedule Frequencies and Required Settings

Frequency	Dialog Box Displayed	What to Enter
Daily or More Frequent	`Daily Schedule Settings`	Specify the start time, start date, and whether to run the schedule each day, on weekdays only, or every few days.
Weekly	`Weekly Schedule Settings`	Specify the time and days of the week for the schedule to run.
Monthly	`Monthly Schedule Settings`	Specify the time, days of the month, and which month the task should run.
One Time Only	`Schedule Settings`	Specify the start time and date.

Table 24: Schedule Options for Smart Copies of Exchange Components

Option Type	Attribute	Description
Schedule Name and Frequency	`Task name`	Name for the schedule.
	`Schedule frequency`	Frequency at which the schedule will run, optionally: • Daily or more frequent (multiple times during a single day) • Weekly • Monthly • One time only
	`Comment`	Comment about the schedule (optional).

Option Type	Attribute	Description
Advanced Schedule Options	`Start Date`	Date to start schedule.
	`End Date`	(Optional) date to end schedule.
	`Repeat options`	Whether you want the schedule to repeat as follows: • Every hour or minute for a specified integer • Until a specific time • For a specific duration in hours, minutes, or both
Smart Copy Options	`Smart Copy Options`	Specify either a snapshot or replica (if your PS Series group is configured for replication). You cannot create clones by using a schedule.
	`Backup Type`	The backup type is `Copy` by default.
	`Keep Count Setting`	Specify the maximum number of snapshots or replicas to keep. Snapshots and replicas are also limited by the snapshot reserve and replica reserve configured on the PS Series group. See the *Dell EqualLogic Group Manager Administrator's Guide* for details. Due to internal implementation details, replication schedules for boot volumes create three Smart Copy replicas on the group for every one displayed in ASM, for each replication. The `keepcount` value refers to the number of replicas maintained by ASM, not on the group. When you delete a Smart Copy from the host, all three replicas created by the scheduled replication are deleted.
Data Verification and Soft Recovery	`Perform Checksum Verification`	Check this option to perform Checksum Verification.
	`Perform Soft Recovery`	Check this option to perform Soft Recovery.
	`eseutil.exe utility`	Specify the location of the `eseutil.exe` utility.
User Account Information	`Run task as system user`	Choose this option to specify the SYSTEM login as the account under which this operation runs. Do not specify the SYSTEM account if you are also performing verification on a remote verification server or in a cluster. In a cluster, specify a user that is a member of the Domain Administrator group.
	`Run task as`	Choose this option to use the current login or to specify

Option Type	Attribute	Description
	`specified user`	an account as the run account for the operation. Provide the following information: • `User Name`—Account name for the account under which this operation will run. (The account that you specify must have appropriate access to the backup documents). In a cluster, this user must be a member of the Domain Administration group. • `Password`—Type the account password. • `Confirm password`—Retype the account password to confirm it.

Recover Microsoft Exchange Data

Because a collection or application can have multiple volumes or databases, a Smart Copy Set can include multiple snapshots, replicas, or clones, depending on the components that comprise the original object. How you access or restore data from a Microsoft Exchange Smart Copy Set depends on the original object (volume, collection, or application components) and the Smart Copy type (snapshot, replica, or clone). The restore options available to you depend on the Smart Copy type.

For snapshots and clones, you can manually restore data by mounting a Smart Copy. After it is mounted, you can copy files from it. The Mount option supports both Windows drive letters and mount points (an empty folder on an existing NTFS file system that serves as an access point for a newly mounted file system). Mount as read-only for replicas cannot be done on the local/source host (where the replica is created). For example, if a replica is imported onto a remote host, then mount as read-only can be performed. The replicas continue to exist on the PS Series group. See *Mount a Replica Smart Copy on page 77* for this procedure.

In addition to mounting Smart Copies, you can also perform the following recovery operations, depending on the Smart Copy type (Table 25) and the version of Exchange you are running (Table 26):

- In-place Restore—A point-in-time restoration of all data in an entire Mailbox Database. For a collection Smart Copy, this operation will be a point-in-time restoration of all data in the Smart Copy.
- Brick-level Restore—Recover data for a specific Mailbox Database. Set a Smart Copy snapshot online and recover lost information from that Smart Copy. ASM/ME allows you to create Recovery Mailbox Databases (for Exchange 2010 and 2013) to perform data recovery tasks using Microsoft Exchange utilities.
- Clone and Restore as New—For all supported Microsoft Exchange versions, you can clone a Mailbox Database from a source Exchange server and then set it up on the same or a different Exchange server.

Consider backing up your Smart Copy backup documents to a network share or another location from which you can recover them easily as part of a disaster recovery plan.

Note: Selective Restore operations are not available for Microsoft Exchange.

Table 25: Available Data Recovery Options for Microsoft Exchange

Smart Copy Type	Restore Options
Snapshot	• Mount • In-place Restore: Restore All • Brick-level Restore: Create Recovery Mailbox Database (Exchange 2010 and 2013) • Clone and Restore as New (all supported versions)
Clone	• Mount • Brick-level Restore: Create Recovery Mailbox Database (Exchange 2010 and 2013) • Clone and Restore as New (all supported versions)
Replica	• Clone a replica, which will create a new volume • Clone and Restore as New • Clone and Create Recovery Mailbox Database (Exchange 2010 and 2013)

Table 26: ASM/ME Data Recovery Procedures for Exchange

See *See "Mount a Snapshot or Clone Smart Copy" on page 77* for instructions on mounting a Smart Copy.

Data Recovery Type	Exchange Version	Related ASM/ME Procedure	See Section
In-place Restore	2010 and 2013	About Microsoft Exchange In-Place Restore	*About Microsoft Exchange In-Place Restore on page 102*
Brick-level Restore	2010 and 2013	Create a Recovery Mailbox Database	*About Creating a Recovery Mailbox Database (Exchange 2010 and 2013) on page 103*
Clone and Restore as New	All supported versions	Create a clone and restore as new	*About the Clone and Restore as New Operation on page 104*

About Microsoft Exchange In-Place Restore

ASM/ME allows you to perform in-place (full) restores for all supported versions of Exchange. An in-place restore is a point in time restoration of all data in an entire Mailbox Database.

Fully Restoring a Microsoft Exchange 2010 or 2013 Database

You can perform an in-place restore operation so a mailbox database is fully restored back to the time that you created the Smart Copy. During the restoration, any mailbox databases included in the Smart Copy Set are set offline, and are inaccessible to users. You have the option to set mailbox databases back online automatically when the restoration is complete. Alternatively, you can specify that the mailbox databases remain offline. Having the databases offline is useful if you need to perform additional operations before you allow users to access them.

Prerequisites for Restoring an Exchange 2010 and 2013 Mailbox Database

- View the properties of the Smart Copy Set to ensure that its Soft Recovery status is successful. (To view status, see *View Checksum Verification and Soft Recovery Status on page 94*).
- In a Database Availability Group, make sure you perform the restore on the node that has the Active copy of the Mailbox Database. Replication to the other copies of the Mailbox Database will be suspended automatically. You must use the Exchange `Update-MailboxDatabaseCopy` cmdlet on each of the nodes that has a copy of the restored mailbox to reseed copies.

Fully Restore a Microsoft Exchange Mailbox Database

1. Expand the Smart Copies node. Right-click the relevant Smart Copy and select `Restore All`. The following dialog box appears: `Restore Exchange Mailbox Database from a Smart Copy`. If you have not yet performed Checksum Verification on the selected Smart Copy, a warning is displayed along with an option to continue anyway.
2. Click `Cancel` if you want to exit the wizard to run Checksum Verification. Otherwise, select the option to continue without verification and click `Next`. The following dialog box appears: `Select Mailbox Database restore options`.
3. Select one of the following options:
   - Mount all mail stores in the Smart Copy Set after the restoration is complete.
   - Do not mount the mail stores after the restoration is complete. Waiting enables you to selectively apply log files and mount mail stores.

   The `Mailbox stores information` pane lists the mail stores that will be unmounted during the restore operation.
4. Click `Restore` to begin the restoration. ASM/ME starts the recovery operation and lists the steps in the recovery operation.

5. Click `Close` when the restore operation is complete. ASM/ME refreshes the Tree Panel. You should clean up any modified Smart Copies, and refresh the Exchange Management Console to see the restored Mailbox Database(s).

About Creating a Recovery Mailbox Database (Exchange 2010 and 2013)

Recovery Mailbox Databases (RMD) is a feature of Microsoft Exchange 2010 and 2013 that enables you to mount a copy of a Mailbox Database to a Microsoft Exchange Server. Then you can recover mailboxes while the mail store remains online.

On a local host, you can use ASM/ME to create an RMD and mount it, making it available for use by Exchange utilities. On a remote host, you must import the Smart Copy and then you can use ASM/ME on that host to create the RMD. See *Importing a Smart Copy on page 73*.

Immediately after you create an RMD, you can launch the Microsoft Exchange Management Shell directly from theASM/ME GUI to perform Exchange administration and data recovery tasks. For more information about this utility, see the documentation for the Exchange Management Console (2010) or the Exchange Control Panel (2013).

Exchange does not allow more than one RMD to be mounted on one server at a time. If you create an RMD from a Smart Copy Set, ASM/ME determines whether an RMD exists and offers to remove it for you.

While you can replace an existing RMD with another, you cannot use ASM/ME to delete an RMD and clean up either the directories that were created or the mailstore and log files that contain the RMD data. If you remove an RMD manually using the Exchange utilities, you are also left in the same state and are told to manually remove these items. This state can also occur if you unmount and log off the Smart Copy Set used for the RMD.

Follow Microsoft Exchange best practices for creating Mailbox Databases to avoid data recovery problems. For example, Exchange does not support creating Mailbox Database files in the root directory of a volume.

However, if you create the database file in the root directory of a volume that is mounted at a mount point, as opposed to a drive letter, the action will succeed. When creating a Recovery Mailbox Database (for Exchange 2010 and 2013), if you specify a drive letter instead of a mount point for the Smart Copy Set, ASM/ME will not be able to complete the creation task. This failure is because Exchange will return an error stating that it cannot store mailbox database files (.edb) in a root directory.

Prerequisites for Creating a Recovery Mailbox Database

- At least one mailbox database must exist under the ASM/ME Applications node.
- Create a Smart Copy of the mailbox database, volume, or collection that you want to include in the RMD.
- For Smart Copies of a collection, make sure that the volumes you want to use for the RMD are not already mounted.
- You cannot perform this operation on a public folders database.

- (Optional) Run Checksum Verification and Soft Recovery on the Smart Copy. Dell recommends running Checksum Verification and Soft Recovery to ensure the integrity of the Smart Copy. As a minimum, Soft Recovery will be run if you use the Smart Copy to recover data. For information on how to do this, see *Run Checksum Verification and Soft Recovery After Smart Copy Creation on page 87*. Running Checksum Verification and Soft Recovery verifies data integrity, but as a result, it can take a longer time to complete data restoration.

Create a Recovery Mailbox Database

1. Expand the Smart Copies node.
2. Make sure that any volume you want to use is not already mounted. If it is, unmount it before proceeding.
3. Right-click the Smart Copy and select `Create Recovery Mailbox Database`. The following dialog box appears: `Create a Recovery Mailbox Database`. If you have not yet performed Checksum Verification on the selected Smart Copy, a warning is displayed along with an option to continue anyway.
4. Do either of the following:
   - Click `Cancel` if you want to exit the wizard to run Checksum Verification.
   - Select the option to continue without verification and click `Next`. The following dialog box appears: `Select Exchange Mailbox Database`.
5. Select the mailbox database and click `Next`. The following dialog box appears: `Select Volume Label`.
6. Specify a drive letter or an NTFS folder for the mount point. Click `Next`. The following dialog box appears: `Review Recovery Mailbox Database Configuration`.
7. If an existing RMD is found, check the box: `Remove existing Recovery Mailbox Database`. Click `Next`.

   ASM/ME automatically deletes the existing RMD, creates the new one, and performs Soft Recovery if required. The following dialog box appears: `Recovery Mailbox Database Creation Complete`.
8. Click the `Launch Exchange Management Shell` link to perform data recovery tasks using Exchange utilities.
9. Click `Finish` to exit the wizard. The Volumes node in the Tree Panel will be refreshed to show the newly mounted volume for the RMD. The Smart Copies node will also be refreshed to show which Smart Copies are in use.

About the Clone and Restore as New Operation

For all supported versions of Microsoft Exchange Server, the Clone and Restore as New operation allows you to clone a Mailbox Database from a source Exchange server, and then set it up as a new Mailbox Database on a local or remote Exchange server. You can also run Restore as New on a local host.

The source Smart Copy Set is imported to the target server using the `Import External Smart Copy` menu option from the ASM/ME instance running on the target server. Then the `Clone and Restore As New` option becomes available.

When performing the Clone and Restore As New operation on Exchange 2010 and 2013, you must specify a new name for the Mailbox Database, as well as a drive letter or mount point for it.

When the operation completes, the new Mailbox Database (Exchange 2010 and 2013) will appear under the Applications node on the target server and you can perform regular ASM/ME actions on them, such as creating Smart Copy Sets or setting up a Smart Copy Schedule. The new clone will appear under the Smart Copies node.

Prerequisites for Clone and Restore As New

- The source and target Exchange Servers must be hosted on machines that are part of the same domain.
- Make sure that the host for the target server can access the PS Series group.
- Make sure that the host for the target server can access the volumes and snapshots containing the Exchange components. For replica Smart Copies, the host needs access to the partner where the replicas are stored.
- For Smart Copies of a collection, make sure that the volumes you want to use are not already mounted.
- Note the following restrictions:
  - You can perform this action only for configurations that comply with Microsoft Exchange Mailbox Database portability rules for all supported Exchange versions.
  - You cannot perform this operation on a public folders database.

Clone and Restore As New

1. Expand the Smart Copies Node.
2. Make sure that any volume you want to use is not already mounted. If it is, unmount it before proceeding.
3. Right-click the Smart Copy Set and select Clone and Restore as New. The Restore All As New Wizard appears. If Checksum Verification was not performed on the Smart Copy Set, you are warned and given the opportunity to continue anyway. However, Dell recommends that you exit the wizard and perform Checksum Verification on the Smart Copy Set. Right-click the Smart Copy and select Verification and Recovery. If Soft Recovery was not performed, it will be performed on the clone of the imported Smart Copy Set, and not on the original Smart Copy Set.
4. Assign a drive letter for the new volume, or specify a mount point and click Next. The Restore As New Mailbox Database dialog box appears. Specify a new mailbox database name and click Restore. The new mailbox database will be created on the local Exchange server.

5. Right-click the Auto-Snapshot Manager icon and click Refresh. The clone will appear under the Smart Copies node, and the new mailbox database will appear under the Applications node. You must manually change the account information for mailboxes in the mailbox database to make it functional on the new server. To complete the operation, modify the user account settings with the Set-Mailbox cmdlet so the account points to the mailbox on the new mailbox server.

7 Using ASM/ME with SQL Server

Certain ASM/ME operations are specific to SQL Server and some operations behave differently when Smart Copy Sets include SQL Server components. ASM/ME operations that are not specific to SQL Server are described in *Generic ASM/ME Operations on page 55*.

Note: ASM/ME does not support creating Smart Copies of SQL Availability Groups.

SQL Server Version Compatibility

Although it is not detected during installation, ASM/ME verifies the compatibility of the installed version of SQL Server. If ASM/ME detects an unsupported version of SQL Server, a red arrow is displayed next to the application in the ASM/ME console. The SqlServerWriter node (under the Applications node) is disabled if the installed version and service pack level of SQL Server is unsupported.

See the product requirements in the *Host Integration Tools for Microsoft Installation and User's Guide*.

See *Using ASM/ME with Hyper-V on page 115* if you intend to run SQL Server with a Hyper-V virtual machine. In some configurations, certain ASM/ME operations are constrained.

Create and Schedue SQL Smart Copies

If you use ASM/ME to create a Smart Copy Set or a schedule that includes multiple SQL Server components (multiple databases sharing similar volumes), ASM/ME warns you that during restore operations, all components are set offline even if you need to restore only one component.

Note: Limit the number of databases in a Smart Copy collection to 34 or fewer. If you have more than 34 databases, spread them among multiple hosts. For more information, see the following article from Microsoft: http://support.microsoft.com/kb/943471

The procedures for creating and scheduling Smart Copies are the same as the generic operations described in *Generic ASM/ME Operations on page 55*.

Note: As a best practice, do not put system databases (Master, Model, MSDB and TempDB) on the same volumes as user databases. Keeping these databases separate will allow for independent recovery of the user content or the system. It will also prevent problems caused by changes to the systems databases while restoring user content.

Restore Options for SQL Server Smart Copies

Table 27 summarizes available SQL Server restore options and Backup Types according to the Smart Copy Type.

Table 27: SQL Server Data Restore Options by Smart Copy Type

Smart Copy Type	Backup Type	Restore Options
Snapshot	copy or full	• Mount • Restore selected databases. (Apply logs option also available for the full backup type.) • Restore all • Restore as new
Clone	copy or full	• Mount • Restore as new • Restore selected databases
Replica	copy or full	• Mount as read-only • Clone and restore as new • Clone a replica, which will create a new volume • Restore selected databases only

The Backup Type has a direct impact on the SQL database log file as follows:

- Full—Specifying this Backup Type will put a checkpoint in the SQL database log file that lets the database know a backup operation occurred at that point in time. This information is useful when applying additional transaction log backups during a Smart Copy restore operation.
- Copy—Specifying this Backup Type does nothing to the SQL database log file, and is best used when creating a Smart Copy of a database that is not intended for restores. For example, you can specify this Backup Type for a database used as a reporting or data mining copy that will be discarded.

Snapshot Smart Copy Restore Options

- Mount—You can mount a Smart Copy to manually copy or restore data from it. The `Mount` option supports both Windows drive letters and mount points (an empty folder on an existing NTFS file system that serves as an access point for a newly mounted file system).

When you mount a SQL Server Smart Copy Set, you must mount at least one snapshot or clone in the Smart Copy Set. The snapshots or clones appear as disks with an assigned drive letter or mount point, and you can then copy data from them.

This option mounts the snapshots in the Smart Copy Set as volumes but does not mount the database. By default, the snapshots are not mounted with read-write access. Optionally select read-write access during the mount operation.

When you mount a snapshot with read-write access, it continues to use the snapshot reserve of the base volume.

You can only mount a snapshot made on the same SQL version (for example, a snapshot of SQL 2008 database will not mount on SQL 2012).

- Restore Selected Database—This option sets one or more original databases offline and performs a fast point-in-time restore of the databases that you select. You can apply additional log files during the restore process for more granularity.

  This option also applies when the Smart Copy Set consists of databases that share the same volumes (not a recommended practice). The restore operation replaces the current data in the volumes with the data from the snapshot in the Smart Copy Set. The process restores (copies) only the database-specific files to the appropriate volumes, making this a potentially slower operation than a full, in-place restore.

- Restore All—This option replaces all the volume data and restores all the databases included in the Smart Copy Set. From the volume perspective, this is considered a fast restore because the process rolls back all the databases entirely.

- Restore as New—This option creates new databases (with new volumes on new mount points) containing the data in the snapshots at the time the Smart Copy Set was created.

  Use this option for side-by-side database restores to recover object data in a production database without taking the database offline.

Clone Smart Copy Restore Options

- Mount—This option mounts the clones in the Smart Copy as volumes but does not mount the database. By default, the volumes are not mounted with read-write access. You can optionally select read-write access during the mount operation.

- Restore as New—Instead of restoring your production databases, you can restore the Smart Copies as new databases. You can use these new databases to perform a side-by-side restore operation, whereby you can compare the databases and make changes at a higher granularity. You can also use the new databases for some other purpose without disrupting the originals.

  This option creates new databases (with new volumes on new mount points) that contain the data in the snapshots at the time the Smart Copy Set was created. Use this option for side-by-side database restores to recover object data in a production database without taking the database offline.

- Restore Selected Database—This option sets one or more original databases offline and performs a fast point-in-time restore of the databases that you select. You can apply additional log files during the restore process for more granularity.

Replica Smart Copy Restore Options

- Mount the replicas as read-only volumes—This option mounts the replicas and deletes the backup document for the Smart Copy Set. You cannot repeat this operation. The replicas continue to exist on the PS Series group.
- Clone and restore as new—This option creates and mounts clones of the replicas in the Smart Copy Set and allows you to perform a side-by-side restore on the original database from the files in the mounted clone. This option preserves the Smart Copy replication schedule.
- Clone a replica Smart Copy—This option creates new volumes.
- Restore selected databases—This option restores one or more individual databases.

Mount an SQL Server Smart Copy

1. Right-click the Smart Copy and select `Mount`. The `Mount Smart Copy` wizard is displayed.
2. Review the warnings and recommendations and click `Next`.
3. In the `Select Volumes to Mount` screen, specify where to mount each volume:
   - You can mount a volume to the default mount folder, specify a different mount folder, or mount the volume to a drive letter of your choice. The default mount folder is C:\ProgramData\EqualLogic\Mounts. A subfolder will be created for each volume in the Smart Copy.
   - To specify a different mount path, click `Browse`.
   - To specify a drive letter instead of a mount path, select the drop-down menu under the `Mount To` column for each listed volume and select a drive letter
4. Specify whether to mount each listed volume as read-write or read-only:
   - Check the box under the Read Only column to mount the volume as read-only.
   - Uncheck the box under the Read Only column to mount the volume as read-write.
5. Click `Mount`. Each volume will be mounted to the host.
6. When you are finished restoring data, optionally right-click the mounted Smart Copy and select the `Unmount and Logoff` option to remove each mounted volume. You can optionally delete the Smart Copy.

Log Off Recently Mounted Smart Copies

During restore operations, you might not be able to unmount and log off recently mounted Smart Copies because the volumes are in use. ASM/ME displays the message `In use by application` next to `Unmount and Logoff` and the option is disabled.

In this case, you can use the following procedure to unmount and logoff the Smart Copy:

1. Expand the Applications node in the Tree Panel. Right-click the relevant SQL Server database and click `Detach Database`.
2. Click `File`, then click `Refresh All Hosts` to refresh the Tree Panel.
3. Under the Smart Copies node, right-click the mounted Smart Copies and click `Unmount and Logoff`.

Restore Selected SQL Server Databases

1. Right-click the relevant Smart Copy in the Tree Panel and select `Restore Selected Databases`. The following dialog box appears: `Select Databases`.
2. Select one or more of the databases listed in the top panel. Click `Next`. The `Restore Database` dialog box appears.
3. Select from the following options:
   - `Apply Logs`—This option enables you to perform custom restore operations without recovery such as manually applying the database transaction logs to the restored database.
   - `Fully Recover`—This option completely restores the database to the contents represented by the Smart Copy Set. You can fully recover a database regardless of the Backup Type used when the Smart Copy Set was created.
4. Click `Restore`. If the SQL Server is clustered, the cluster physical disk resource for the volume containing the database to be restored is placed in maintenance mode until the restore operation completes. When the operation is complete, ASM/ME displays the following message: `Restore completed successfully`.

Restore All Databases

If a Smart Copy Set contains copies of several databases, you can restore all databases in a single operation.

1. Under the Smart Copies node, right-click the relevant Smart Copy and select `Restore All`. ASM/ME displays its progress for steps such as setting volumes offline and later, back online. If the SQL Server is clustered, the cluster physical disk resources for the volumes are placed in maintenance mode until the restore completes.
2. Wait until ASM/ME displays the following message:
   `Database restored. Refresh the database management GUI to see the restored database.`

Restore a Database as New

Before you begin, make sure the ASM agent is configured to run as a user who has permissions to perform this operation in SQL.

For detailed information on the various options for this procedure, see Table 28. To perform Restore as New operations on alternate SQL Server hosts, see *Importing a Smart Copy on page 73*.

Table 28: Data Required for Restore As New

Item	Description
Smart Copy Type	
`Restore as New`	Select option for a snapshot or clone Smart Copy Set.
`Clone and Restore as New`	Select option for a replica Smart Copy Set.
Volume Mapping	
`Drive Letter`	Drive letter or NTFS folder mount point for the new volume.
Restore as New Database	
`New Database Name`	If required, modify the new database name. ASM/ME appends the string `_new` to the original database name to ensure that it is not confused with the original.
`Database Server to use`	Enter the name of an SQL Server instance that will serve the new database, if different from the instance serving the original database. If you are restoring to a new SQL Server instance, then the SQL Server instance should be the same SQL version as the original instance. On a cluster, this is the network name of the clustered SQL server. The current node must be the owner of the SQL Server Resource Group.
`Make database READ-ONLY after attach`	Choose whether to make the new database read-only. Use this option if you do not want users to accidentally make changes to the new database; for example, if you plan to make side-by-side restorations to the original database.
`TSQL Command for attaching the database`	This field shows the SQL Server commands that execute to create the new database. Optionally, you can add custom actions to the command. On a cluster, ASM/ME will not execute this command. There are several manual steps that you must perform before attaching to the database. You can then use this command to attach to the database.

1. Expand the Smart Copies node. Right-click the relevant Smart Copy and select `Restore As New`. If the Smart Copy is a replica, the option to select is `Clone and Restore as New`. The `Select Databases` dialog box appears.
2. Make sure that any volume you want to use is not already mounted. If it is, unmount it before proceeding.
3. Select one or more of databases that you want to restore as new. Click `Next`. The `Select Volume Label` dialog box appears.
4. Select a drive letter or mount point for the volume and click `Next`.

   You can enter a specific mount point with either a relative path, which will be combined with the value in the mount root field, or a full path, which is used exactly as entered. The mount point is validated as you enter the data. Invalid mount points are shown in red text, and a tooltip in the volume row displays the problem with the entered mount point.

   The `Restore As New Database` dialog box appears.
5. All the fields are described in Table 28. Enter the required information. If you selected more than one database, the dialog box is repeated for every database you selected. Click `Restore`.

   ASM/ME displays the following message when the procedure is complete: `New database created successfully. Refresh database management GUI to see the restored database.`
6. Click `Close`. The new database appears as a volume node under the ASM/ME Volumes list node in the Tree Panel. The icon has an "i" over it to indicate that it is mounted and in-use.

   If you are restoring to a clustered SQL instance, the following message is displayed: `Successfully mounted the Smart Copy on all cluster nodes.`

   ASM/ME lists three manual steps you must perform to complete the restore operation. ASM/ME mounts the volumes containing the databases to be restored and performs the iSCSI logon for the current node and any possible owner nodes that are configured to access the PS Series group.

   Click `OK` and perform the following cluster and SQL management operations to complete the restore operation:
   - Use the appropriate cluster utility (Failover Cluster Management for Windows Server 2008) to add the volumes or mount points for the restored databases as physical resources to the SQL Server cluster group.
   - Add the physical disk resources to the dependencies for the SQL Server resource.
   - Attach the databases using the SQL Server Management Studio or the TSQL commands shown on the Restore as New wizard page.

8 Using ASM/ME with Hyper-V

Microsoft Hyper-V enables you to create a virtualized server computing environment. When ASM/ME is installed on a system running Hyper-V, you can create point-in-time Smart Copies of virtual machines (VMs) from which you can recover data or entire VMs.

Some ASM/ME operations are specific to Hyper-V and some operations behave differently when Smart Copy Sets include Hyper-V virtual machine components. ASM/ME operations that are not specific to Hyper-V are described in *Generic ASM/ME Operations on page 55*.

Hyper-V enables you to run a client virtual machine (also called a guest O/S) in child partitions. The combination of O/S, resources, applications, and storage space as a virtual hard drive (VHD) comprises a VM. Hyper-V supports different O/S instances in each VM.

Support for Hyper-V

Hyper-V requires specific hardware. To install and run Hyper-V, you must have an x64 computer running the 64-bit version of Windows Server 2008 or later. Other operating systems, including different Windows versions and Linux can participate as a guest O/S. Specific configurations of Windows Server 2008 and Windows Vista which have the optional Microsoft Integration Services (or Virtual Guest Services) and other requisite software installed are considered Hyper-V aware. Also, specific applications, such as Microsoft Exchange, are qualified as being Hyper-V aware.

See the *Host Integration Tools for Microsoft Release Notes* for a list of the operating systems that are supported by ASM/ME.

When installed on a computer running Hyper-V, ASM/ME enables you to create point-in-time Smart Copies of VMs from which you can recover user data or entire VMs. Smart Copies are crash consistent, unless the VM is running both an O/S and an application that has awareness of Microsoft Volume Shadow Copy Service (VSS). In such cases, you can create application-consistent Smart Copies.

Note: You can create Smart Copies of rapid-provisioned VMs (using SCVMM), but the volumes will not have user-visible mount points.

Operating System Constraints

The following operating system constraints apply to Hyper-V:

- The Hyper-V computer that hosts ASM/ME must be a 64-bit server running Windows Server 2008 or later.
- Your computer must comply with any BIOS setting requirements specified by Microsoft.
- Windows 2000 is not Hyper-V aware, so you can take only crash-consistent Smart Copies. ASM/ME must put the VM into a “save state” before you can take a Smart Copy.

Hyper-V Requirements and Constraints

Hyper-V requirements and constraints as they apply to ASM/ME are as follows:

- Integration Services (Virtual Guest Services) components must be installed on every Windows guest operating system to support online backup and data exchange. See the Microsoft Hyper-V documentation for installation information about Integration Services.
- ASM/ME is constrained and limited by the current functions offered by the Hyper-V VSS writer. That is, it can only support those operations currently supported by the Hyper-V writer.
- You can choose to install an instance of ASM/ME within the VM if you want these features.

  If you choose to run SQL Server or Microsoft Exchange within a virtual machine, you do not benefit from some features that ASM/ME offers in support of SQL and Microsoft Exchange. You only get a copy and restore of the entire virtual machine. So, in the case of Microsoft Exchange, ASM/ME options such as Recovery Mailbox Database and Verification are not available.
- As with operations on SQL and Microsoft Exchange, ASM/ME automatically detects multiple-writer objects prevents you from creating a multiple writer Smart Copy Set.

See the *Host Integration Tools for Microsoft Release Notes* for the most recent constraints for ASM/ME support of Hyper-V.

Hyper-V Supported Configuration

Dell supports only one configuration for ASM/ME support of Hyper-V for full Smart Copies (Figure 10 and Table 29).

In this scenario:

- Application data is stored on a VHD that is contained in an iSCSI target provisioned on the host.
- The VM boots to the VHD on the iSCSI target provisioned on the host.
- VSS-based backup of the VMs from the host O/S is supported.

Figure 10: Hyper-V Configuration Supported by ASM/ME

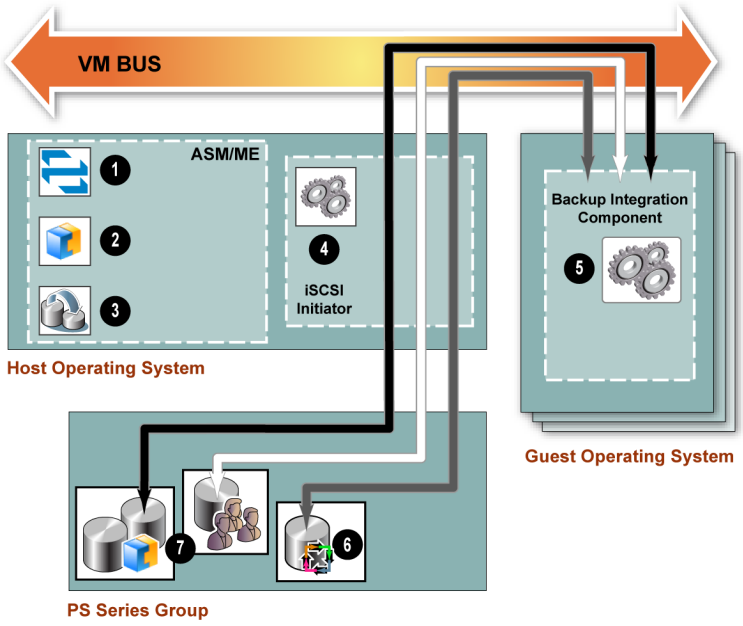


Table 29: Supported Hyper-V Configuration

Host Operating System	
ASM/ME is installed under the host operating system, providing the Smart Copy operations for all guest operating systems in their respective partitions.	
Callout	Description
1	ASM/ME acts as a backup requestor.
2	Hyper-V functions as the writer.
3	The Microsoft VSS Copy Service is the backup provider.
4	The guest operating systems connect to the PS Series group through the iSCSI initiator installed under the host operating system.
Guest Operating System	
5	The guest operating system has the *Backup Integration Services (Virtual Guest Services*) component installed to facilitated copies of the partition and its data. Not all guest operating systems support the Integration Services.
PS Series Group	

6	The boot volume for each guest operating system is a virtual hard drive (VHD) on an iSCSI volume located in a PS Series group.
7	The PS Series group also contains virtual hard drives (VHD) on iSCSI volumes for user data or application databases such as Microsoft SQL or Microsoft Exchange that are accessed by the guest operating environment.

Unsupported Configurations

The following Hyper-V configurations are not supported by ASM/ME for copy or restore operations:

- Direct-attach volumes—Directly attaching iSCSI volumes to the VM is not supported because such targets are not visible to the ASM/ME installation in the Hyper-V host partition. Therefore, you cannot create application-consistent copies of the applications running on the VM.

  You can create Smart Copies of direct-attached iSCSI volumes only if you install an instance of ASM/ME on the VM. In this case, any Smart Copies of direct-attached iSCSI volumes are application-consistent, but you cannot take an application-consistent snapshot of the entire VM and running applications with this configuration.

- Passthrough volumes—Passthrough volumes are logged in to by the host partition but mounted only on the VM. In this case, the volume is not seen as an iSCSI target and is not visible as such to ASM/ME or to Hyper-V. Microsoft recommends this configuration for performance reasons, but it does not enable you to create application-consistent Smart Copies of the applications running on these volumes.

Hyper-V Specific Operations

Hyper-V virtual machines appear under the Applications node in the Tree Panel. If you view the properties for the VM, the property "VM is running" is displayed. When using Hyper-V virtual machines, ASM/ME allows you to perform the following operations:

- Create application-consistent and crash-consistent Smart Copies of virtual machines (dependent on O/S type). The procedure for creating Smart Copies is the same as the generic operations described in *Generic ASM/ME Operations on page 55*. Note the following constraints for Hyper-V environments:
  - Whether the copy operation is application-consistent or crash-consistent depends on the type of O/S and whether the Integration Services (or Virtual Guest Services) are installed on the guest.
  - On Windows Server 2008 R2, replicas are supported for Hyper-V only when it is running on a CSV. See *Creating Smart Copies in a CSV-Enabled Cluster on page 125* for more information.
  - In a standalone Windows Server 2012 or greater environment, both full and copy backup types are available. In a Windows Server 2012 or greater CSV environment, only the full backup type is available.

  - Volumes for highly available VMs created through SCVMM will not have user-visible mount points. However, you can create Smart Copies of them the same as any other volume. For more information, see the *Host Integration Tools for Microsoft Installation and User's Guide*.

- Define collections of virtual machines
- Set up schedules for creating Smart Copies of virtual machines
- Restore Smart Copies of virtual machines
- Restore volumes used by VMs

Smart Copies for Different Guest Operating Systems

If the guest O/S is either Windows Server 2008 or Windows Vista, with Integration Services (Virtual Guest Services) installed, the Smart Copy operation includes the following sequence:

- The Hyper-V management console displays a message confirming that it is performing the Smart Copy operation.
- The VM remains online.
- ASM/ME creates the Smart Copy.
- When the Smart Copy operation completes, services on the guest O/S return automatically.

If the guest O/S is either Windows 2000 or Linux, the Smart Copy operation includes the following sequence:

- ASM/ME initiates the Smart Copy operation.
- During the Smart Copy operation, the VM is put into a frozen state. Any user logged in to the VM will experience the temporary inability to do I/O operations.
- When the Smart Copy operation completes, services on the VM resume automatically.

Avoid Torn Smart Copies

Dell encourages you to place related VM data sets on separate volumes that you create for their exclusive use. ASM/ME always takes a Smart Copy of a volume. Therefore, if multiple VMs are located on a volume, all VMs are copied and all will be restored in the restore operation. If VMs are allowed to span multiple volumes, a Smart Copy operation could result in a VM that is torn. *Torn Smart Copies on page 65* explains this scenario.

Hyper-V Collections

The procedure for operations on collections of virtual machines is the same as the generic operations described in *Generic ASM/ME Operations on page 55*. You should avoid removing VMs without updating relevant collections.

Smart Copy Schedules for Hyper-V

The procedure for scheduling Smart Copies of virtual machines is the same as the generic operations described in *Generic ASM/ME Operations on page 55*, except that if a VM is offline, it is still copied in its offline state. The Smart Copy will be made of whatever shutdown state the VM is in:

- If the VM was shut down cleanly, the Smart Copy will be application-consistent.
- If the VM crashed or was powered off without a shutdown, the Smart Copy will be crash-consistent.

Schedules will fail if you remove a VM permanently without updating any schedules or scheduled collections of which that VM was previously a member.

Hyper-V Restore Operations

ASM/ME supports the following types of data restoration for virtual machines as shown in Table 30.

Table 30: Restore Operations for Hyper-V

Operation	Menu Option
In-Place Restore	`Restore All`
Selective Restore	`Restore selected VMs`
Restore As New	`Restore As New`
Clone and Restore As New (only for replicas in a Windows Server 2008 R2 environment)	`Clone and Restore As New`

Restore operations are always disruptive regardless of the type of guest O/S that is installed in the VM. The restore operation has the following sequence:

- The Hyper-V management console displays a message confirming that it is performing the restore operation.
- The VM is taken offline and is deleted by the VSS writer. If you are running a remote desktop to the guest, the remote desktop session is terminated.
- ASM/ME restores the VM files.
- When the restore operation completes, the VM is registered with the Hyper-V service, which adds it to the list of VMs in the Hyper-V management console. If the VM was running before the restore operation was initiated, ASM/ME will restart the VM.
- If the VM crashed and you then initiated a restore operation to recover it, then the VM is left in the powered-off state by the ASM/ME restore operation.

Restore In-Place for VMs

With an in-place restore operation, you can restore all VMs in the Smart Copy. This type of operation restores all data on all PS Series volumes used by all VMs included in the Smart Copy. For in-place restore operations, all VMs on the volumes being restored will experience a service interruption.

Restore a VM In-Place

1. Right-click the VM Smart Copy in the ASM/ME GUI and select `Restore All`. A confirmation dialog box appears.
2. Click `Yes`.

Selective Restore

With a selective restore operation, you specify one or more VMs you want restored. The large VHD file size affects the time to complete the selective restore. The default size of a VHD is 127GB, but such large file sizes will take some time to copy and restore. Therefore, consider reducing the volume size to the optimum required for the application and user space.

Restore a VM Selectively

1. Right-click the VM Smart Copy in the ASM/ME GUI and select `Restore selected VMs`. The `Select Virtual Machines` dialog box appears.
2. Select the virtual machine you are restoring and click `Restore`. When the restore operation is finished, a message appears, stating that the operation completed successfully.

Restore As New

The Restore as New operation is available for snapshots and clones. This operation creates a new VM that will be local and non-clustered, so no restrictions are needed. The VM is created locally on the current node, and has the default VM settings and a user-specified amount of RAM that uses the original VM's .vhd files. If you want to start the VM, you must verify yourself that there are available for it. You cannot adjust other virtual hardware through ASM/ME. Restore as New currently supports up to four .vhd files during a restore.

Restore a VM as New

1. Expand the Smart Copies node, right-click the relevant VM, and select `Restore As New`.
2. If snapshot reserve space is low, a warning is displayed. Click `Next`. The `Select Virtual Machines` dialog box is displayed.
3. Select one or more virtual machines and click `Next`. The `Select Volume Label` dialog box is displayed.
4. Select from the following options:

- `Assign the following driver letter`: Pull down the letter of the drive on which to mount the Smart Copy.

  You can enter a specific mount point with either a relative path, which will be combined with the value in the mount root field, or a full path, which is used exactly as entered. The mount point is validated as you enter the data. Invalid mount points are shown in red text, and a tooltip in the volume row displays the problem with the entered mount point.
- `Mount in the following empty NTFS folder`: Browse for an empty folder to use as the mount point.

5. The `Restore As New Virtual Machine` dialog box is displayed. Type a name for the new virtual machine, or accept the default name provided. Specify the memory (in MB) or accept the default. Click `Restore`.
6. ASM/ME lists the sequence of restore operations it performs. Click `Close` when the operations are complete. The new VM will appear under the Applications node in the Tree Panel.

Cluster Shared Volumes

Cluster Shared Volumes (CSV) are a feature of Windows failover clustering introduced in Windows Server 2008 R2 for use with Hyper-V. CSVs greatly simplify a typical failover cluster configuration because each cluster node can access CSVs to manage files and perform read and write operations on them. Therefore multiple nodes can host or run VMs residing on the same CSV.

In a CSV configuration, a coordination node is responsible for performing backups and restores of the VMs stored on the CSV. The coordination node can easily and frequently be changed from one node to another. The coordination node becomes the temporary owner of the CSV and the VMs that reside on it. The remaining nodes in the cluster can still access the CSV. (Moving the coordination node is not necessary to perform a backup of a CSV in Windows Server 2012 or greater.)

While a backup operation is in progress, I/O from all the other cluster nodes is temporarily redirected through the coordination node. The redirected I/O state can be viewed from the Windows Failover Cluster Manager.

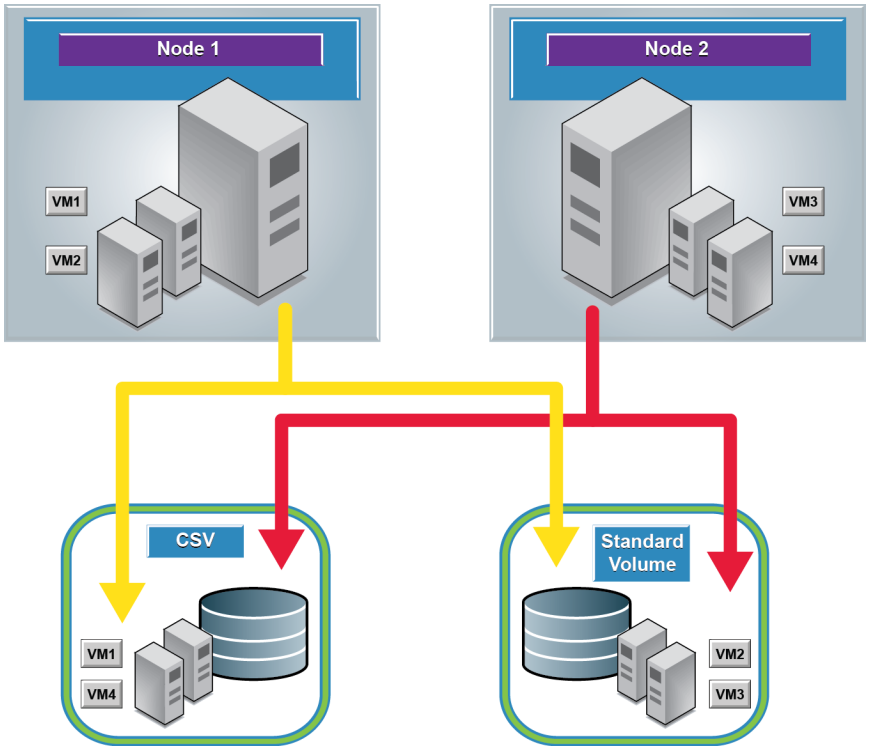
Coordination Nodes in a CSV Environment

A coordination node is the temporary owner of the CSV and the VMs that reside on it.

Example 1—One CSV

The example in Figure 11 applies only to Windows Server 2008 R2. Assume you are running a 2-node, CSV-enabled failover cluster with one CSV. Node 1 is the coordination node. Node 1 is running two VMs—VM1 and VM2. Node 2 is also running two VMs—VM3 and VM4. Assume that VM1 and VM4 reside on a CSV, while VM2 and VM3 reside on standard volumes.

Figure 11: Example of a Failover Cluster with a CSV and a Standard Volume



Since all cluster nodes can access a CSV, both instances of ASM/ME will display the CSV. CSVs appear at `C:\ClusterStorage\Volume#`, where # is a decimal number determined by Windows. Windows enforces this same mount point path for the CSV on each cluster node. The ASM/ME instance on Node 1 will display VM1 and VM2 in blue under the Applications node. Although VM4 manages files on the same CSV, the ASM/ME instance running on Node 1 will not display VM4, since VM4 runs on Node 2.

The ASM/ME instance running on Node 2 will display VM3, which resides on a standard volume, in blue. VM4, which resides on the CSV, will be gray. Smart Copy operations for VM4 are disabled until you change the coordination node from Node 1 to Node 2. This is an easy, one-step process. Assuming there are Smart Copies of VM4 on Node 2, you can still perform restore operations for VM4 even while Node 2 is not the coordination node. This is because the restore operation automatically moves the coordination node as needed.

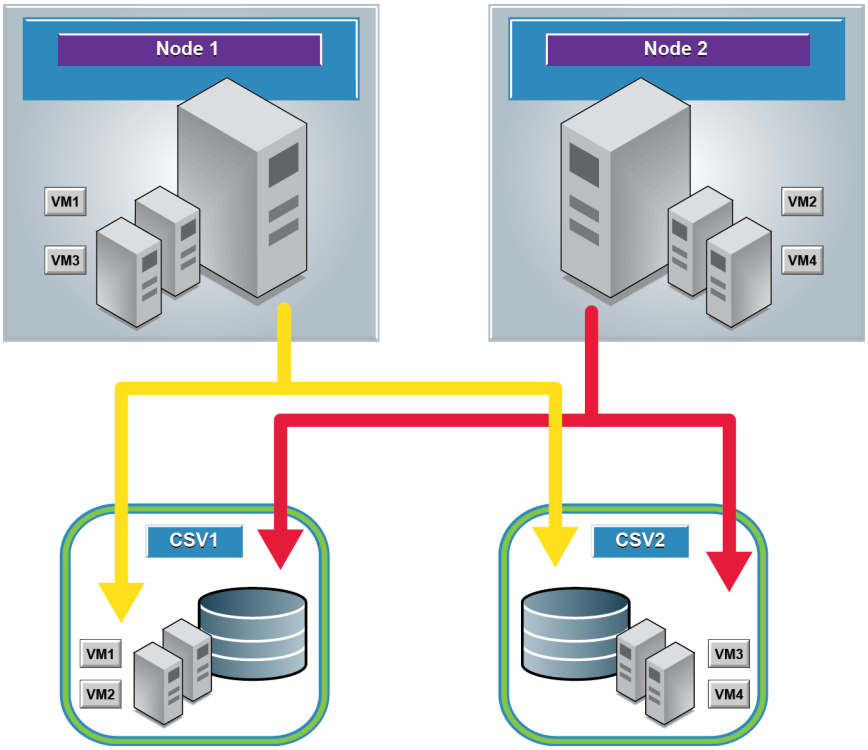
Once the coordination node moves to Node 2, VM1 on the ASM/ME instance running on Node 1 will become gray and its Smart Copy operations are disabled. You will still be able to perform restore operations on VM1. To enable Smart Copy operations for VM1, you will need to make Node 1 the coordination node once again.

Example 2—Two CSVs

The example in Figure 12 applies only to Windows Server 2008 R2. Assume you are running a two-node, CSV-enabled failover cluster with two CSVs—CSV1 and CSV2. Also assume the following:

- Node 1 is running two VMs—VM1 and VM3.
- Node 1 is also the coordination node for CSV1.
- Node 2 is running VM2 and VM4.
- Node 2 is also the coordination node for CSV2.
- VM1 and VM2 reside on CSV1.
- VM3 and VM4 reside on CSV2.

Figure 12: Example of a Failover Cluster with Two CSVs



The ASM/ME instance running on Node 1 will display VM1, VM3, and CSV1 in blue. CSV2 will be displayed, but it will be grey. Similarly, the ASM/ME instance on Node 2 will display VM2, VM4, and CSV2 in blue, while CSV1 will be grey.

Smart Copies of VM1/VM3 and VM2/VM4 can be created from either Node 1 or Node 2, as long as the node owns both CSVs. Further, all four VMs can be included in a single collection that is Smart Copied from whatever node owns both CSVs. A Smart Copy started on one node will include all of the VMs running on the CSVs, without regard to which node on which the VM is running.

Change the Coordination Node from One Node to Another

On Windows Server 2008 R2, you can make a cluster node the coordination node automatically if you create a Smart Copy Schedule for a VM, CSV, or CSV collection. This is not necessary for later Windows Server versions. When the schedule runs, the coordination node changes automatically.

To manually change the coordination node within the ASM/ME GUI, do either of the following from the ASM/ME instance running on the node that you want to be the coordination node:

- Right-click the relevant VM, CSV, or CSV collection, and select `Make Cluster Shared Volume Local`.
- Right-click any VM that resides on the CSV, CSV, or CSV collection (even though these objects might be gray) and select `Make Cluster Shared Volumes Local`.

CSVs in a Windows Server 2012 Environment

On Windows Server 2012 or greater, you can manage CSVs from any node, regardless of which one owns it. All nodes display the CSV with a blue icon. You do not need to change the coordination node.

Creating Smart Copies in a CSV-Enabled Cluster

Smart Copy operations in CSV-enabled clusters provide the following benefits:

- Significant performance improvements and ease of use—Only one schedule is needed to capture every VM residing on a CSV. You no longer need to create a single schedule for each VM on the CSV, which could slow down performance. This makes CSV schedule management easy.
- Conservation of storage space—Since you only need one schedule to capture every VM residing on a CSV, less snapshot reserve space is consumed.
- File System Consistency—[Windows Server 2008 R2 environments] On Windows Server 2008 R2, when you take a Smart Copy of a CSV or a VM on a CSV, it will be file system-consistent and will contain all virtual machines that reside on the CSV, including those that are running on other cluster nodes.

  In all other cases, including Windows Server 2012 or greater, Smart Copies are application consistent because the operation uses the Hyper-V VSS writer. The Smart Copies will contain all virtual machines that reside on the CSV, including those that are running on other cluster nodes.

The following Smart Copy operations are available for CSV-enabled clusters:

- You can create Smart Copies of VMs residing on CSVs. The supported Smart Copy types depend on the operating system:
  - On Windows Server 2008 R2, snapshots, clones, and replicas are supported. Replication operations of Hyper-V VMs are only supported for VMs on CSVs.
  - On Windows Server 2012 or greater, snapshots and clones are supported.
- You can create Smart Copies of CSVs themselves. A single Smart Copy of a CSV will copy every VM that resides on the CSV.
- You can create CSV collections and then create Smart Copies of those collections.
- You can create schedules for the above Smart Copy operations.

Smart Copies of Virtual Machines Residing on CSVs

Smart Copies of virtual machines that reside on a CSV in Windows Server 2008 R2 are not taken using the Hyper-V VSS writer. The VSS writer is only involved at the file system level. Therefore, when you create a Smart Copy of a virtual machine that resides on a CSV in Windows Server 2008 R2, the Smart Copy will be file system consistent, and not application consistent. For example, if SQL Server is running inside a VM that resides on a CSV and you create a Smart Copy of the VM, SQL Server will not be copied in a consistent state. However, you will still get file system consistency inside the VM.

In all other cases, including Windows Server 2012 or greater, Smart Copies are application consistent because the operation uses the Hyper-V VSS writer.

The procedure for creating Smart Copies is the same as the generic operations described in *Generic ASM/ME Operations on page 55*.

Smart Copies of CSVs

When you take a Smart Copy of a CSV on Windows Server 2008 R2, it will be file system consistent and will contain all virtual machines that reside on the CSV, including those that are running on other cluster nodes. When ASM/ME creates a Smart Copy of the CSV, for every VM that resides on the CSV, ASM/ME freezes the VM's file system and flushes it. This ensures file system consistency and creates a point-in-time copy. The freeze is then released.

On Windows Server 2012 or greater, the operating system handles the application quiescence (not ASM/ME), and therefore Smart Copies of a CSV are application consistent, and will contain all virtual machines that reside on the CSV including those that are running on other cluster nodes.

The procedure for creating Smart Copies is the same as the generic operations described in *Generic ASM/ME Operations on page 55*.

Smart Copies of CSV Collections

You can create collections of CSVs, or collections of virtual machines that reside on CSVs. Then you can create Smart Copies of the collections, or create a schedule for creating Smart Copies of the collection. You cannot have standard volumes and CSVs in the same collection.

When you create a collection of CSVs, ASM/ME automatically includes in the collection any related components or VMs that reside on the CSVs at that point in time. If you have created a Smart Copy schedule for the collection, and if the component definition is changed after its creation, ASM/ME will still create a Smart Copy of the collection. However, what components get included in the collection are based on the CSV state at the point in time the Smart Copy is created.

For example, a collection might include two CSVs. When you create the collection, ASM/ME will automatically include whatever components or VMs reside on those CSVs. After the collection is created, a VM could be removed. When the scheduled Smart Copy is created, it will include the components related to those CSVs at that point in time.

The procedure for operations on collections is the same as the generic operations described in *Generic ASM/ME Operations on page 55*.

About Scheduling Smart Copies

You can schedule Smart Copy operations for CSVs, or for all VMs in a CSV-enabled cluster. The following schedule behavior applies only to Windows Server 2008 R2:

- The coordination node will be changed automatically when a Smart Copy schedule is executed.
- Schedules of a single VM will run from the node that owns the VM when the schedule is triggered. ASM/ME determines the list of CSVs required for creating the Smart Copy of the VM and makes the node on which the VM is running the coordination node in order to create the Smart Copy. Once the schedule completes, the new Smart Copy appears under the Smart Copies node of ASM/ME. The cluster node where the schedule ran is now the coordination node for the CSV.
- Schedules of a single CSV will run on the node that owns the CSV when the schedule is triggered.
- Schedules of a CSV collection will run on the node that owns the most CSVs when the schedule is triggered. If two or more nodes tie for owning the most number of CSVs, the schedule will run on the node that is first alphabetically.

  If any of the CSVs cannot have their coordination node moved successfully, an error is generated and the operation is aborted.

On Windows Server 2012 or greater, schedules run on the node chosen by ASM/ME based on the cluster status.

Restore Operations in a CSV Environment

For CSV Smart Copies, you can perform the following operations:

- In-place restores
- Selective restores
- Restore as new
- Clone and restore as new

Restore In-Place in a Cluster

ASM/ME uses the Hyper-V VSS writer to perform in-place restores. All VMs are automatically pulled to one cluster node in order to perform the restore. Since this can overwhelm the cluster node, all VMs are automatically shut down before they are moved. If the VMs were running before the restore operation, they are restarted after the restore operation. If cluster resources for a specific VM were offline when the restore operation started, ASM/ME will bring the VM back to the local node and you will have to move it.

Windows 2008 R2 SP1 or later is required.

See *Restore a VM In-Place on page 121* for how to selectively restore a VM stored on a CSV.

Selectively Restoring a VM

Selective restores must be performed from whatever node currently owns the VM. You can move the VM, but the VM and the volume must be local to the current node for the restore operation. Even if a VM is running on a node that is not the coordination node, you can perform a selective restore of that VM.

Assume you are running a two-node cluster, where VM1 runs on Node 1, and VM2 runs on Node 2. Both VM1 and VM2 store files on a CSV. You can only perform a selective restore of those VMs from the nodes that own them. Ownership of a VM is determined by the ownership of the VM's cluster resources. For example, if you moved VM1 to Node 2, then you can restore VM1 on Node 2. The operation will automatically make Node 2 the coordination node in order for the restore to take place.

Performing a selective restore of a VM with files stored on a CSV does not modify any other VMs that store files on the same CSV—only the VM you are restoring will be affected. In the example above, restoring VM1 will not affect VM2, even though they are both on the same CSV.

See *Restore a VM Selectively on page 121* for how to selectively restore a VM stored on a CSV.

Restoring a Snapshot or Clone as a New VM

You can perform a Restore as New operation on snapshots and clones. This operation creates a new VM that will be local and non-clustered, so there are no restrictions. The VM is created locally on the current node, and has the default VM settings and a user specified amount of RAM that uses the original VM's .vhd files. If you want to start the VM, you must verify yourself that there are enough resources for it. You cannot adjust other virtual hardware through ASM/ME. Restore as New currently supports up to four .vhd files during a restore.

See *Restore a VM as New on page 121* for more information.

Clone and Restore As New

This operation is available for replicas. It is the same as the Restore As New option, except that the operation begins by cloning the replica in order to avoid interfering with the replication process. The clone is then mounted and a new VM is created from the .vhd file on the mounted clone.

Like the Restore as New operation, this operation creates a new VM that will be local and non-clustered, so there are no restrictions. The VM is created locally on the current node, and has the default VM settings and a user specified amount of RAM that uses the original VM's .vhd files. If you want to start the VM, you must verify yourself that there are enough resources for it. You cannot adjust other virtual hardware through ASM/ME. Clone and Restore as New currently supports up to four .vhd files during a restore.

9 Use ASM/ME with Microsoft SharePoint

ASM/ME supports Microsoft SharePoint 2007 through 2013, with the operating system and SQL Server versions listed in the Host Integration Tools for Microsoft Release Notes.

ASM/ME can discover and manage an entire SharePoint farm, assuming the farm components reported by the SharePoint VSS writer are stored on Dell EqualLogic volumes. You can view individual hosts, volumes, content databases, and search indices within the farm. You can create and schedule Smart Copies, and perform data restoration operations for farm components.

SharePoint Installation Considerations

For ASM/ME to work correctly with SharePoint farms, all the SharePoint components must be on PS Series volumes. You can specify the default location for SharePoint Search Service Applications and index file locations during the SharePoint installation (recommended) or you can modify an existing SharePoint farm.

For detailed information, see the *Host Integration Tools for Microsoft Installation and User's Guide*.

Plan to Install ASM/ME on a SharePoint Farm

For ASM/ME to work correctly with all the components of a SharePoint farm, including the search service applications and the search indexes, all the components must be on PS Series volumes. If you have not yet installed and created your SharePoint farm, or to make the necessary modifications to an existing farm, see the *Host Integration Tools for Microsoft Installation and User's Guide*.

When the SharePoint VSS writer is installed on a host that is part of a SharePoint farm, the software determines which hosts require additional software. The SharePoint VSS writer is not enabled by default, so you must choose a farm host on which SharePoint is installed to serve as the writer host, and then enable the SharePoint VSS writer on it.

You can use a web front end server or an application server as your writer host. Then perform an initial ASM/ME installation on whatever farm host is running the SharePoint VSS writer. After that initial installation is complete, the SharePoint VSS writer provides ASM/ME with a view of the farm layout and automatically determines the subset of hosts that require an installation. When you open the ASM/ME console on the writer host, a list of hosts requiring ASM/ME installation is displayed. You can then add those hosts using the Add Hosts wizard. The farm hosts that require an ASM/MEinstallation are those that run these SharePoint services:

- Microsoft SharePoint Foundation Database
- SharePoint Server Search
- SharePoint Foundation Help Search

Respectively, these are the farm hosts that are running Microsoft SQL databases used in the farm, the hosts that have Office Search enabled, and the hosts that have SharePoint Search enabled.

Although ASM/ME automatically discovers farm hosts after it is installed on the writer host, you can also manually determine which farm hosts are running these services through SharePoint Central Administration.

In SharePoint 2010 and 2013, open Central Administration, then `Manage services in this farm`.

If ASM/ME is installed on the writer host, and if the writer host is a member of a HIT Group containing all farm hosts that have ASM/ME installed, you can manage your entire farm from a remote host.

Multiple Writers Can Share a Volume

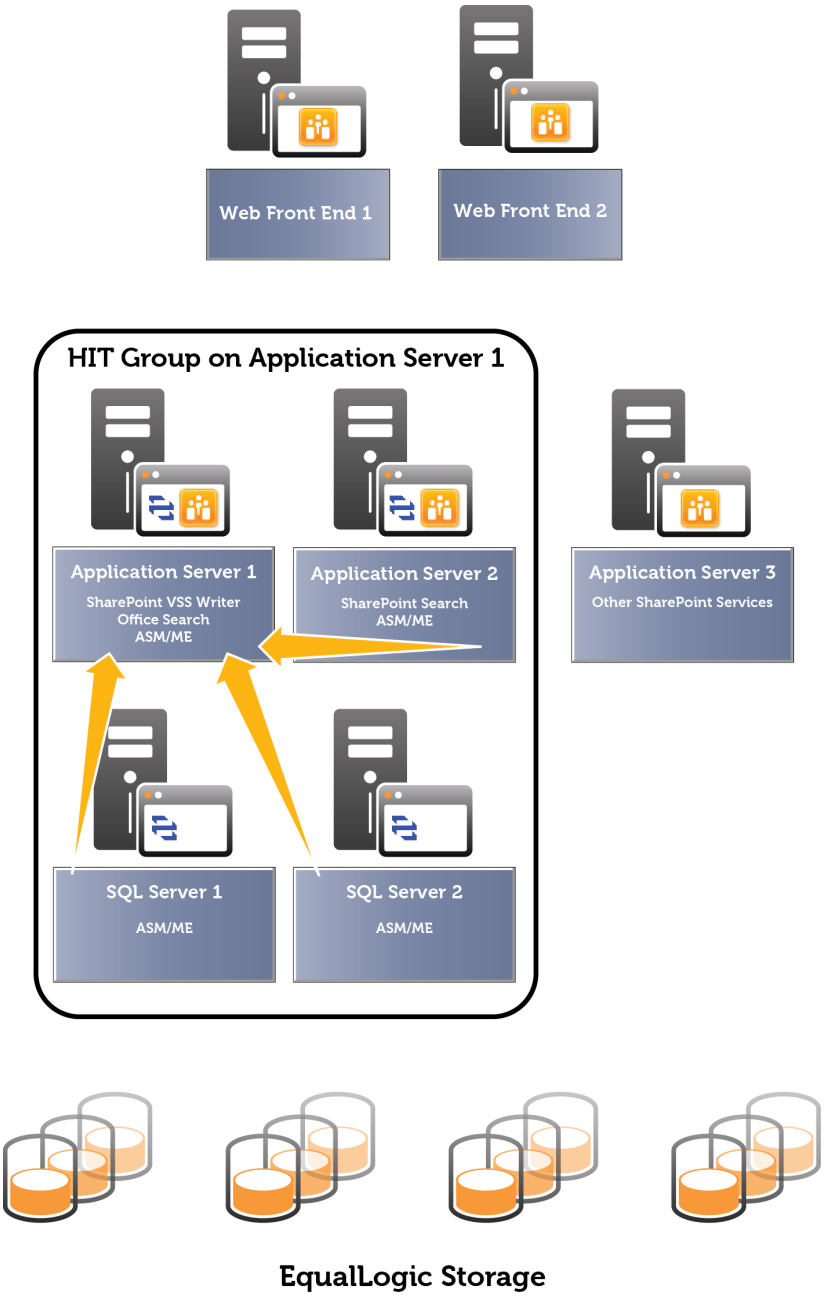
In a SharePoint 2010 environment, Office Search and SPSearch VSS writers can share the same volume. Whenever two SharePoint search writers are enabled on the same host, they are included in a single VSS operation.

Note: SQL database and log files should be on separate volumes from SharePoint search index file. Furthermore, files from other ASM/ME supported applications must be installed on separate volumes from SharePoint files.

Example of ASM/ME Installed on a SharePoint Farm

Figure 13 shows a typical ASM/ME deployment on a SharePoint farm.

Figure 13: ASM/ME Installation on a SharePoint Farm



In Figure 13, the SharePoint VSS writer is enabled and running on Application Server 1, also referred to as the writer host. All databases and search indices on Application Server 1, Application Server 2, SQL Server 1, and SQL Server 2 are using Dell EqualLogic storage.

ASM/ME is first installed on Application Server 1 since it is the writer host. The SharePoint VSS writer provides ASM/ME with an overall view of the farm layout.

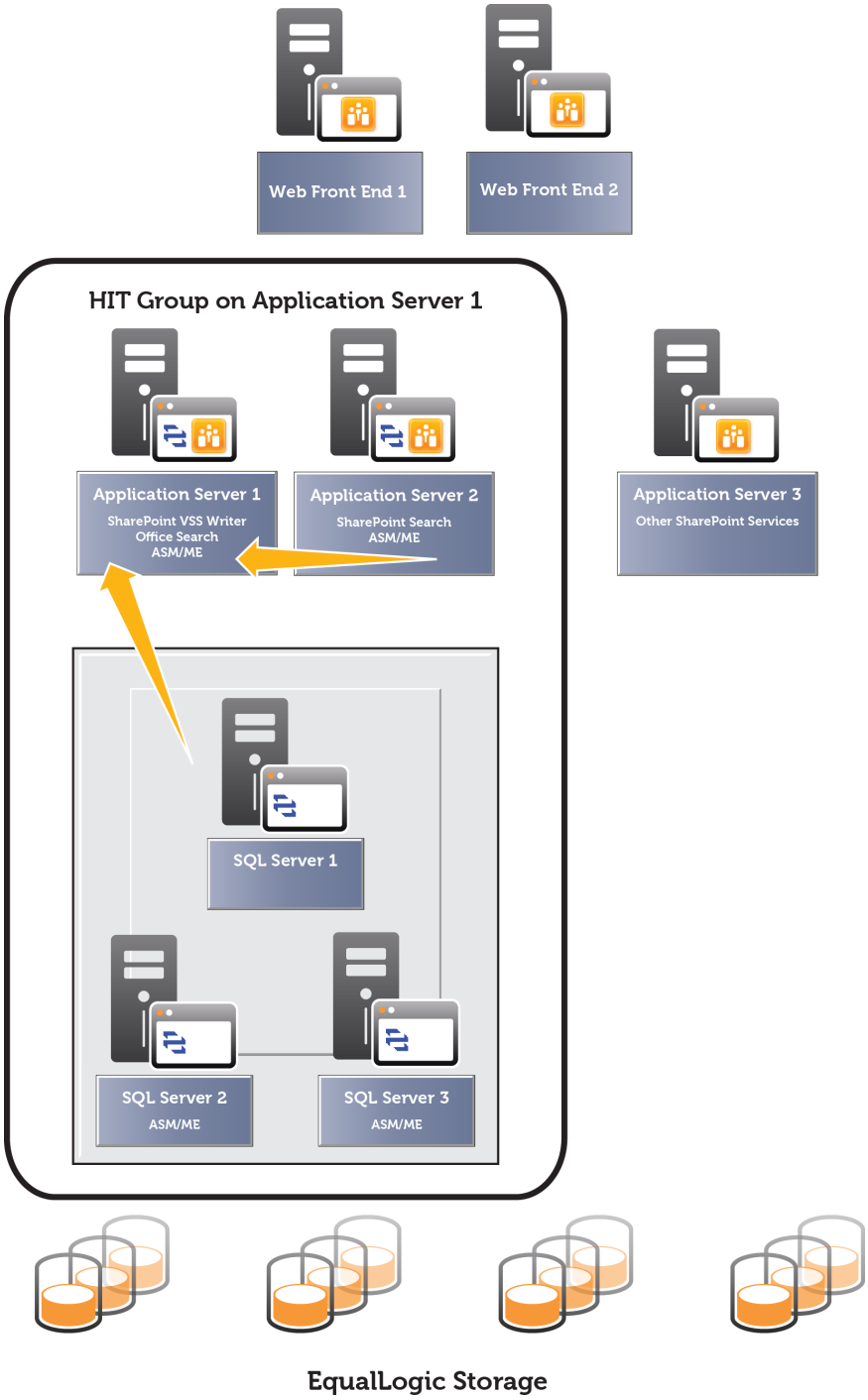
When you open the ASM/ME console on Application Server 1, you are prompted to create a HIT Group on Application Server 1 by adding the other farm hosts (Application Server 2, SQL Server 1, and SQL Server 2) to it for management. You can do this through the Add Hosts wizard.

During this process, ASM/ME is automatically installed on the three hosts that were added to Application Server 1. ASM/ME automatically sets up appropriate trust relationships between the farm hosts. The farm hosts can be managed from the ASM/ME instance on Application Server 1, and all ASM/ME operations pertaining to SharePoint can be performed from there.

Example of a SharePoint Farm With an SQL Cluster

Figure 14 shows an ASM/ME deployment on a SharePoint farm that contains a SQL cluster.

Figure 14: ASM/ME Installation on a SharePoint Farm with a SQL Cluster



In Figure 14, the SharePoint VSS writer is enabled and running on Application Server 1, also referred to as the writer host. All databases and search indices on Application Server 1, Application Server 2, and the SQL cluster are using Dell EqualLogic storage.

ASM/ME is first installed on Application Server 1 because it is the writer host. The SharePoint VSS writer provides ASM/ME with an overall view of the farm layout.

When you open the ASM/ME console on Application Server 1, you are prompted to create a HIT Group on Application Server 1 by adding Application Server 2 and one of the SQL cluster nodes to it for management. You can do this through the Add Hosts wizard.

During this process, ASM/ME is automatically installed on the cluster node and Application Server 2. ASM/ME automatically sets up appropriate trust relationships between the added hosts.

After this initial HIT Group has been created, ASM/ME recognizes that the SQL host added is in fact part of a cluster, and automatically prompts you to add the rest of the cluster nodes to the HIT Group using the Add Hosts wizard. During this process, ASM/ME is automatically installed on the other two cluster nodes and the appropriate trust relationships are set up.

After this operation completes, the entire SQL cluster and Application Server 2 can be managed from the ASM/ME instance on Application Server 1. All ASM/ME operations pertaining to SharePoint can be performed from Application Server 1.

Install ASM/ME on a SharePoint Farm

Before you begin, identify a network shared directory to store Smart Copy backup documents:

- All farm hosts that ASM/ME will be managing must be able to access this exact path.
- The farm administrator must have read-write access to this path.
- Any HIT Group hosts on which you plan on importing Smart Copies using ASM/ME should also have read-write access to this path.

Choose a farm host on which SharePoint is installed to serve as the writer host, and then enable the SharePoint VSS writer on it. The SharePoint VSS writer is not enabled by default. You can use a web front end server or an application server as your writer host.

1. Start the command prompt with the right-click "Run as Administrator" option.
2. Run the following command, substituting the appropriate number from the following list for the variable `nn`:
    - For SharePoint 2010, enter 14
    - For SharePoint 2013, enter 15

```
"C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\nn\BIN\STSADM.exe"
-o registerwsswriter
```

You will see the following message as a result: `Operation completed successfully.`

3. Confirm SharePoint VSS writers on the nodes where it is registered by running `"vssadmin.exe list writers"` from an elevated command prompt. Search writers will appear only on hosts where that SharePoint service is provisioned.
4. Install ASM/ME on the host running the SharePoint VSS writer.
5. Open the ASM/ME console. ASM/ME will display a list of the farm hosts you need to add.
6. Add those hosts through the Add Hosts wizard:

   Click Add Hosts.

   a. Select Cluster and SharePoint Farm Nodes and click Next.

   b. Enter farm administrator credentials (domain, username, and password) for the hosts you are adding. See *About Creating a HIT Group on page 51* for prerequisite information about HIT Groups.

   c. If you want to install MPIO or the PowerShell Tools on the host, select those options.

   d. Specify the directory that contains the installation files.

   e. Click Add Hosts to begin the installation on the specified host. Progress and status information is displayed. (An error message is displayed if the installation or upgrade cannot complete). When the process is complete, click Close. The Summary of Hosts page is displayed.

   f. This page displays the hosts that have been added to the HIT Group, and what actions—such as installations or upgrades—have been performed on each host. This page also shows you whether or not a reboot is required on the remote hosts. If a reboot is required, click Reboot All. Otherwise, click Finish.
7. Open the General Settings page in ASM/ME and specify the farm administrator domain account for the Run ASM Services As option. On the same General Settings page, specify the shared backup document directory you identified in Step One. Ensure that every host in your HIT Group is using this same backup document directory.
8. If your SharePoint farm contains a SQL cluster, proceed with the following step. If not, the installation procedure is complete.
9. If one of the hosts you just added is a SQL cluster node, ASM/ME will recognize that you are running a SQL cluster within your farm, and will prompt you to add the remaining SQL cluster nodes. Add these hosts through the Add Hosts wizard.
10. Open the General Settings page in ASM/ME and specify the farm administrator domain account for the Run ASM Services As option. Also specify the same shared backup document directory for each cluster node.

About Changes to an Existing SharePoint Farm

If you have already installed ASM/ME on a SharePoint farm, ASM/ME automatically detects changes to the farm layout and prompts you use the Add Hosts wizard when you add a new host that:

- Runs SQL databases used in the farm
- Has Office Search enabled
- Has SharePoint Search enabled

Remove a HIT Group Host

Removing a host from a SharePoint farm removes the host from the GUI, but does not uninstall ASM/ME on the host. If the host still has farm components after it is removed, ASM/ME will prompt you to add the host back to the HIT Group.

1. Right-click the HIT Group host in the ASM/ME Tree Panel.
2. Click Stop Managing.

Add or Change a Writer Host in a SharePoint Farm

If you add or change a writer host in a SharePoint farm, the new host must use the same shared backup document directory that is specified on all other farm hosts. Similarly, you must also specify the farm administrator domain account for the Run ASM Services As option on the General Settings page of the ASM/ME instance of the new writer host. Further, any Smart Copy schedules that were created apply only to the initial or former writer host. Therefore, you will need to recreate Smart Copy schedules on the new writer host.

If the new writer host is already a part of the farm HIT Group:

1. Enable the SharePoint VSS writer on the host.
   a. Start the command prompt with the right-click "Run as Administrator" option.
   b. Run the following command, substituting the appropriate number from the following list for the variable `nn`:
      - For SharePoint 2010, enter 14
      - For SharePoint 2013, enter 15

   ```
   "C:\Program Files\Common Files\Microsoft Shared\Web Server
   Extensions\nn\BIN\STSADM.exe" -o registerwsswriter
   ```

2. Open ASM/ME on the new writer host.

If the additional writer host is not yet part of the farm HIT Group:

1. Enable the SharePoint VSS writer on the additional writer host:
   a. Start the command prompt with the right-click "Run as Administrator" option.
   b. Run the following command, substituting the appropriate number from the following list for the variable `nn`:

- For SharePoint 2010, enter 14
- For SharePoint 2013, enter 15

```
"C:\Program Files\Common Files\Microsoft Shared\Web Server
Extensions\nn\BIN\STSADM.exe" -o registerwsswriter
```

2. Open ASM/ME on the new writer host. ASM/ME will display a list of the farm hosts you need to add through the Add Hosts wizard.
3. Click Add Hosts to add these hosts to the new writer host.
4. (Optional) If you are changing the writer host, disable the SharePoint VSS writer on the old host:
   a. Start the command prompt with the right-click "Run as Administrator" option.
   b. Run the following command, substituting the appropriate number from the following list for the variable `nn`:
      - For SharePoint 2010, enter 14
      - For SharePoint 2013, enter 15

```
"C:\Program Files\Common Files\Microsoft Shared\Web Server
Extensions\nn\BIN\STSADM.exe" -o unregisterwsswriter
```

Respond to Changes in a SharePoint Farm

The SharePoint farm environment can change depending on your desired configuration. Table 31 lists required user actions as they pertain to specific changes to the farm.

Smart Copy schedules and the ASM/ME GUI will automatically refresh their view of the farm before executing. This guarantees that all farm changes are picked up. However, if new hosts are added to the farm and those hosts are not part of the HIT Group, the schedule or command will fail.

Table 31: Required User Actions for Changes to the SharePoint Farm

Change in SharePoint Farm Environment	Required Actions
A new SQL or application server is added to the farm	ASM/ME automatically detects the new host and displays a list of the new farm hosts you must add through the Add Hosts wizard. You must then add the new hosts to the HIT Group.
A new cluster node is added to the farm	ASM/ME automatically detects the new host and displays a list of the new farm hosts you must add through the Add Hosts wizard. You must then add the new hosts to the HIT Group.
A new SharePoint database is added to an	Changes automatically appear in the ASM/ME GUI.

Change in SharePoint Farm Environment	Required Actions
existing SQL instance in the HIT Group	
A database is moved between existing SQL instances	
A database is deleted in SharePoint	
A database is renamed in SharePoint	
The location for the database or log files is changed	Refresh the writer host in the ASM/ME GUI
A search index or search component is added to an existing application server that is part of the HIT Group	Changes automatically appear in the ASM/ME GUI.
The search topology is modified	
The search index file location is changed	Refresh the writer host in the ASM/ME GUI

View SharePoint Farm Components in ASM/ME

ASM/ME displays the SharePoint Farm as a supported application under the Applications node in the Tree Panel. Depending on the version of SharePoint that you are running, the version number appears next to the SharePoint Farm node. For example, if you are running SharePoint 2013, "SharePoint 2013 Farm" is displayed under the Applications node.

When you expand the SharePoint Farm node, the individual components of the SharePoint farm are separated into Content Databases, Other Databases, and Search folders:

- Content Database folder—This contains all databases that the SharePoint VSS writer marks as a "content database." Although the SharePoint Admin database is a content database, it is displayed under the Other Databases folder.
- Other Databases folder—This contains all databases that the SharePoint VSS writer marks as a "generic database" or "configuration database." This includes service application and SharePoint configuration databases.
- Search folder—This contains subfolders for each Search Service Application in the farm. If SPSearch is enabled in the farm, its components are included in a SPSearch subfolder.

If the SharePoint VSS writer is enabled on the writer host, the farm hosts are online and reachable, and the ASM agent is running, then all of the individual farm components are reachable by ASM/ME. You can then view detailed information for each component, and perform Smart Copy and data restoration operations on them.

When you select a farm component in the Tree Panel, its properties are displayed. You can view several properties for the farm component, such as its component name, the volume on which it resides, and the component type (such as a Search index, content database, service application database, and so on).

Right-click individual components (or select them and view the Actions Toolbar) to view the available options for each component.

SharePoint Smart Copies

You can create Smart Copies of the following SharePoint components:

- The entire SharePoint farm
- The set of all content databases
- Individual databases
- Search Service Application (SSA)—SharePoint 2010 and 2013

Note: Limit the number of databases in a Smart Copy collection to 34 or fewer. If you have more than 34 databases, spread them among multiple hosts in the farm. For more information, see the following article from Microsoft: http://support.microsoft.com/kb/943471

When you create a Smart Copy of a SharePoint component, it appears under the Smart Copies node in the Tree Panel. Assuming that all farm hosts within the HIT Group have been properly set up to use one shared backup document directory, newly created Smart Copies also appear under the Smart Copies node for every host in the HIT Group. When you expand the Smart Copies node, the SharePoint Smart Copies are grouped under the SharePoint Services Writer. When you select a particular Smart Copy, its properties are displayed. You can right-click on the Smart Copy to view available actions for it.

When you create a Smart Copy of the farm, an individual database, or an SSA, Office Search and SharePoint Search environments are paused before ASM/ME takes the Smart Copy. This ensures consistency between the search databases and search indices. Any content source crawls that are running are paused. After ASM/ME takes the Smart Copy, the Office Search and SharePoint Search environment is resumed, and any content source crawls that were paused will resume.

Note: If any component of the SharePoint farm is unavailable or unreachable (for example, if a host is down), ASM/ME creates a Smart Copy but warns you about the offline components in the wizard, log files, and the summary dialog.

Create a Smart Copy of an Entire SharePoint Farm

1. Navigate to the HIT Group host on which the SharePoint VSS writer is running.
2. Expand the Applications node.

3. Right-click the SharePoint Farm node and select Create Farm Smart Copy. ASM/ME displays the Create Smart Copy wizard.
4. In the Select Smart Copy Type dialog box, select the following:
   - Snapshot, Clone, or Replica, depending on what type of Smart Copy you want to create. (If you create a clone, select the Mount Clone option to automatically mount the clone once it is created. On the next screen, you can choose which volumes to mount, and either use the mount folder or specify a drive letter for each volume. The default mount folder is C:\ProgramData\EqualLogic\Mounts, but you can browse to a different folder).
   - Select the backup behavior type: copy or full.
   - (Optional) Enter text describing the Smart Copy Set. This information will appear in the backup document.
5. Click Next. ASM/ME displays the Summary screen.
6. Verify the settings. If the information is correct, click Create. ASM/ME lists each phase of Smart Copy creation.
7. Click Close. The Smart Copy appears under the Smart Copies node in the ASM/ME Tree Panel. You can select it to display its details or right-click on it to view available actions.

Note: Because a Smart Copy of an entire farm may include components from multiple hosts, this type of Smart Copy is further organized under a SharePoint Farm node, which is then organized by host name. For example, you could create a Smart Copy of a farm that contains content databases from SQL Server A and SQL Server B. In the Tree Panel, navigate to the farm Smart Copy as follows: Smart Copy Node, then SharePoint 2013 Farm node, then SQL Server A node (or SQL Server B node).

Create a Smart Copy of All Content Databases

1. Navigate to the HIT Group host on which the SharePoint VSS writer is running.
2. Expand the Applications node.
3. Expand the SharePoint Farm node.
4. Right-click the Content Databases folder and select Create Content Databases Smart Copy. ASM/ME displays the Create Smart Copy wizard.
5. In the Select Smart Copy Type dialog box, select the following:
   - Snapshot, Clone, or Replica, depending on what type of Smart Copy you want to create. (If you create a clone, select the Mount Clone option to automatically mount the clone once it is created. On the next screen, you can choose which volumes to mount, and either use the mount folder or specify a drive letter for each volume. The default mount folder is C:\ProgramData\EqualLogic\Mounts, but you can browse to different folder).
   - Select the backup behavior type: copy or full.
   - (Optional) Enter text describing the Smart Copy Set. This information will appear in the backup document.
6. Click Next. ASM/ME displays the Summary screen.

7. Verify the settings. If the information is correct, click Create. ASM/ME lists each phase of Smart Copy creation.
8. Click Close. The Smart Copy appears under the Smart Copies node in the ASM/ME Tree Panel. You can select it to display its details or right-click on it to view available actions.

Create a Smart Copy of a Single Database

1. Navigate to the HIT Group host on which the SharePoint VSS writer is running.
2. Expand the Applications node.
3. Expand the SharePoint Farm node.
4. Expand the following folders: Content Databases, Other Databases, and Search.
5. Right-click the individual database for which you are creating a Smart Copy and select Create Smart Copy. ASM/ME displays the Create Smart Copy wizard.
6. In the Select Smart Copy Type dialog box, select the following:
   - Snapshot, Clone, or Replica, depending on what type of Smart Copy you want to create. (If you create a clone, select the Mount Clone option to automatically mount the clone once it is created. On the next screen, you can choose which volumes to mount, and either use the mount folder or specify a drive letter for each volume. The default mount folder is C:\ProgramData\EqualLogic\Mounts, but you can browse to different folder).
   - Select the backup behavior type: copy or full.
   - (Optional) Enter text describing the Smart Copy Set. This information will appear in the backup document.
7. Click Next. ASM/ME displays the Summary screen.
8. Verify the settings. If the information is correct, click Create. ASM/ME lists each phase of Smart Copy creation.
9. Click Close. The Smart Copy appears under the Smart Copies node in the ASM/ME Tree Panel. You can select it to display its details or right-click on it to view available actions.

Create a Smart Copy of a Search Service Application (SSA)

This operation is available only for SharePoint 2010 and 2013 farms.

Note: SharePoint farms can have many SSAs. To create a Smart Copy of all the SSAs for a farm, create a Smart Copy of the full farm. See *Create a Smart Copy of an Entire SharePoint Farm on page 139*.

1. Navigate to the HIT Group host on which the SharePoint VSS writer is running.
2. Expand the Applications node.
3. Expand the SharePoint Farm node.

4. Expand the Search folder.
5. In the Search folder, right-click the Search Service Application for which you are creating a Smart Copy and select Create Search Service Application Smart Copy. ASM/ME displays the Create Smart Copy wizard.

   Note: ASM/ME determines whether enough of the search environment is currently available to make a restorable Smart Copy. If so, the Create Smart Copy wizard opens. If not, ASM/ME displays a warning message about which component is offline. All components must be online before you can create a Smart Copy.

6. In the Select Smart Copy Type dialog box, select the following:
   - Snapshot, Clone, or Replica, depending on what type of Smart Copy you want to create. (If you create a clone, select the Mount Clone option to automatically mount the clone once it is created. On the next screen, you can choose which volumes to mount, and either use the mount folder or specify a drive letter for each volume. The default mount folder is C:\ProgramData\EqualLogic\Mounts, but you can browse to different folder).
   - Select the backup behavior type: copy or full.
   - (Optional) Enter text describing the Smart Copy Set. This information will appear in the backup document.
7. Click Next. ASM/ME displays the Summary screen.
8. Verify the settings. If the information is correct, click Create. ASM/ME lists each phase of Smart Copy creation.
9. Click Close. The Smart Copy appears under the SharePoint node in the ASM/ME Tree Panel. You can select it to display its details or right-click on it to view available actions.

Restore Options for SharePoint Smart Copies

The data restoration options for SharePoint are conceptually similar to those described in *Restore Options for SQL Server Smart Copies on page 108*.

- For snapshot restore options, see Table 32.
- For clone restore options, see Table 33.
- For replica restore options, see Table 34.

Table 32: Restore Options for Snapshot Smart Copies

SharePoint Component Type	Data Restoration Options
Entire SharePoint farm	• Mount • Restore Selected Database • Restore As New

SharePoint Component Type	Data Restoration Options
Individual content database	• Mount • Restore All • Restore Selected Database • Restore As New
Set of all content databases	• Mount • Restore All • Restore Selected Database • Restore As New
Search service application (SSA)	• Mount • Restore Search Service Application
Search database	• Mount • Restore As New
Other databases	• Mount • Restore As New

Table 33: Restore Options for Clone Smart Copies

SharePoint Component Type	Data Restoration Options
Entire SharePoint farm	• Mount • Restore Selected Database • Restore As New
Individual content database	• Mount • Restore Selected Database • Restore As New
Set of all content databases	• Mount • Restore Selected Database • Restore As New
Search service application (SSA)	• Mount • Restore Search Service Application
Search database	• Mount • Restore As New

SharePoint Component Type	Data Restoration Options
Other databases	• Mount • Restore As New

Table 34: Restore Options for Replica Smart Copies

SharePoint Component Type	Data Restoration Options
Entire SharePoint farm	• Mount As Read-Only • Clone • Restore Selected Database • Clone and Restore As New
Individual content database	• Mount As Read-Only • Clone • Restore Selected Database • Clone and Restore As New
Set of all content databases	• Mount As Read-Only • Clone • Restore Selected Database • Clone and Restore As New
Search service application (SSA)	• Mount As Read-Only • Clone • Restore Search Service Application
Search database	• Mount As Read-Only • Clone • Restore Selected Database • Clone and Restore As New
Other databases	• Mount As Read-Only • Clone

Availability of SharePoint Data Restoration Operations

Within the ASM GUI, some data restoration operations may only be initiated from certain HIT Group members:

- The Restore Selected Database operation must be initiated in the ASM/MEGUI on the HIT Group host on which the SharePoint VSS Writer is running.
- The Restore Search Service Application operation must be initiated in the ASM/MEGUI on the HIT Group host on which the SharePoint VSS Writer is running.
- The Restore All operation must be performed from the HIT Group host on which the SharePoint VSS Writer is running. If you still cannot perform this operation from the writer host, it may be because the Smart Copy contains a component that cannot be restored.
- The Restore As New operation must be performed from a compatible SQL Server host in the HIT Group. The SQL Server Writer must be running on that host.
- The Clone and Restore As New operation must be performed from a compatible SQL Server host in the HIT Group. The SQL Server Writer must be running on that host.

Mount a SharePoint Smart Copy

1. Navigate to the HIT Group host on which you want to mount a Smart Copy.
2. In the Tree Panel, expand the Smart Copies node for that host.
3. Right-click the Smart Copy and select `Mount`. The `Mount Smart Copy` wizard is displayed.
4. Review the warnings and recommendations and click `Next`.
5. The dialog box lists the volumes in the Smart Copy. You can click the upper right corner of the Original Host column to filter the list of hosts.
6. Specify where to mount the volume:
   - You can mount a volume to the default mount folder, specify a different mount folder, or mount the volume to a drive letter of your choice. The default mount folder is C:\ProgramData\EqualLogic\Mounts. A subfolder will be created for each volume in the Smart Copy.
   - To specify a different mount path, click `Browse`.
   - To specify a drive letter instead of a mount path, select the drop-down menu under the `Mount To` column for each listed volume and select a drive letter.
7. Specify whether to mount each listed volume as read-write or read-only:
   - Check the box under the Read Only column to mount the volume as read-only.
   - Uncheck the box under the Read Only column to mount the volume as read-write.
8. Click `Mount`. The volume will be mounted to the host.

Restore Selected Databases from a SharePoint Smart Copy

1. Navigate to the HIT Group host on which the SharePoint VSS writer is running.
2. Expand the Smart Copies node for the writer host.

3. Right-click the Smart Copy and select Restore Selected Databases.
4. Select the database that you are restoring and click Next. To select multiple databases, use Ctrl-select or Shift-select.
5. Select Apply Logs or Fully Recover and click Restore. ASM/ME displays the progress of the operation.
6. Click Close when the operation completes.

Restore a Database In-Place from a SharePoint Smart Copy

1. Navigate to the HIT Group host on which the SharePoint VSS writer is running.
2. Expand the Smart Copies node for the writer host.
3. Right-click the Smart Copy and select Restore All. ASM/ME displays its progress for steps such as setting volumes offline and later, back online. If the SQL Server is clustered, the cluster physical disk resources for the volumes are placed in maintenance mode until the restore completes.
4. Wait until ASM/ME displays the following message: Database restored. Refresh the database management GUI to see the restored database.

Restore a Database from a SharePoint Smart Copy as a New Database

This procedure restores a database from a Smart Copy as a new database for a side-by-side restore, or clones a database from a replica Smart Copy and restores it as a new database for a side-by-side restore.

1. Navigate to the SQL host on which you want to perform the Restore As New operation. The SQL Server Writer must be running.
2. In the Tree Panel, expand the Smart Copies node for that SQL host.
3. Right-click the Smart Copy and select `Restore As New`. If this operation is for a replica, right-click the replica Smart Copy and select `Clone and Restore As New`.
4. Select the database that you are restoring and click `Next`. To select multiple databases, use Ctrl-select or Shift-select.
5. Specify where to mount the volume:
   - You can mount a volume to the default mount folder, specify a different mount folder, or mount the volume to a drive letter of your choice. The default mount folder is C:\ProgramData\EqualLogic\Mounts. A subfolder will be created for each volume in the Smart Copy.
   - To specify a different mount path, click `Browse`.
   - To specify a drive letter instead of a mount path, select the drop-down menu under the Mount To column for each listed volume and select a drive letter.
6. Click `Next`.

7. Specify these options:
   - From the drop-down menu, select a SQL instance to use.
   - Check the Read Only box to attach the new database as read-only.
   - The Database Name field displays the name of the new database, which has "`_new`" appended to the old database name.
     - To specify a different suffix, select the Use Original Names With Suffix option and type a different suffix.
     - To change the name entirely, select the Assign Individual Names option. Place the curser in the Database Name field and type the preferred name.
   - Click the Update button if you want to customize the TSQL statements that create the new database. If you modify the TSQL statements before performing the previous steps, your changes will be discarded.
8. Click `Restore`.

Restore a Search Service Application (SSA) from a SharePoint Smart Copy

1. Navigate to the HIT Group host on which the SharePoint VSS writer is running.
2. Expand the Smart Copies node for the SharePoint farm.
3. Right-click the Smart Copy and select Restore SSA 'Name of the SSA'.
4. The Restore Search Service Application from Smart Copy dialog box opens, displaying the list of search components that will be restored. Click Next.
5. The dialog box displays the restore steps and requirements for the restore operation to succeed. Click Restore. ASM/ME displays the progress of the operation.
6. Click Close when the operation completes.

Note: Because the SSA will be restored to the point at which the Smart Copy was created, it is recommended to initiate a new incremental crawl, or wait for the next scheduled incremental crawl, to discover new content in the farm.

10 Using the Command Line Interface

This chapter describes the command line and scripting options provided by the ASM/ME command line interface.

Introduction to ASMCLI

Note: Although this section covers ASMCLI commands, Dell recommends you use the ASM PowerShell cmdlets instead to perform the functions discussed in this section. For more information about PowerShell cmdlets, see the *Dell EqualLogic PowerShell Tools Reference Guide*.

ASM/ME provides you with a set of commands (ASMCLI) that you can execute at the Windows command prompt instead of using the GUI for Smart Copy operations. You can also use these commands to create your own site-specific scripts for Smart Copy operations.

You can also generate complex commands automatically by using menu options in the ASM/ME GUI as described in *Scripts and Command Generation on page 5*. The auto-generate option automatically copies the long text strings that identify objects such as volumes and schedules and builds them into syntactically-correct commands. This feature aids you in using the command line or scripting. You do not need to manually type long commands and you can aggregate the auto-generated commands into scripts by copying and pasting the commands into a text editor.

On a cluster, if the action for which you want to generate a command is disabled, the action to automatically generate the command is also disabled. If you manually create the commands for these actions, you will need to add Cluster Management actions to your scripts to resolve any cluster related issues for the command to execute successfully.

Use the ASMCLI command set to do the following operations:

- Create Smart Copies
- Run Checksum Verification and Soft Recovery for Microsoft Exchange only
- Delete Smart Copies
- Mount a Smart Copy
- Unmount a Smart Copy
- Restore a Smart Copy (perform a full restore or a selective restore of certain files.) (Selective Restore is not available for Microsoft Exchange.)
- List supported volumes, collections, and components
- Configure ASM/ME properties
- Create, modify, and delete collections
- Clone a replica Smart Copy

- Configure CHAP credentials
- Retrieve ASMCLI version information
- Enumerate Smart Copies for specific volumes, components, or collections
- Enumerate iSCSI target portals
- Safely shut down the current instance of the Global Verification Task
- Close all instances of verifier notification pop-up dialogs that appear in the Windows taskbar notification area

How to Use ASMCLI Commands

The ASMCLI executable is located under the default installation folder, or the folder that you specified for ASM/ME during installation. The default folder is: `C:\Program Files\EqualLogic\bin`.

You execute a command by starting the Windows command prompt:

1. Click `Start`, then `Run`. Then type `cmd`.
2. In the command window, change directory to `C:\Program Files\EqualLogic\bin` or add the ASM/ME CLI commands folder to your path by editing your Windows `PATH` environment variable.

General Command Syntax

The general command syntax is as follows:

```
command [-|/]sub_command required_parameter="argument" optional_parameter...
```

The following constraints apply to the syntax:

- `[-|/]sub_command`—Prefix subcommands with a dash (-) or a forward slash (/).

  Depending on the width of the help window, the dash (or forward slash) preceding a subcommand might appear on the next line in command examples. This is a constraint of the help system formatting, and you should always make sure that you specify the prefix (- or /).

- `"argument"`—An argument requires quotation marks only when the argument variable contains an embedded space.
- Arguments consist of the following:
  - A unique identifier assigned to an object, such as a volume or a collection.
  - A keyword, such as `copy` or `full`.
  - A user-defined string, such as a time or a comment.

- Several parameters are mutually exclusive. The command parser automatically ignores any redundant parameters.

The following command example demonstrates the syntax of a typical command that you might use to create a Smart Copy schedule.

```
> ASMCLI -smart -scheduleID=ee05bb76-6ccc-431a-99b9-37886a1d7748 -objectID=Psv
{18a09060-3be0-3fa8-0a7a-e4120000e045;32256} -shadowType=Transportable
-backupType=copy -snapshotType=Snapshot -keepCount=14
```

Table 35 lists the typographical conventions for ASMCLI.

Table 35: ASMCLI Typographical Conventions

Convention	Usage
`fixed width font`	Command, parameter, output, file name, link, button, field, URL address, or email address.
`bold fixed width`	Input to command prompt.
`fixed_width_italics`	Indicates that you replace the variable with a command, parameter, file name, and so on.
`{text1 | text2}`	Indicates that you can choose one of the items presented.
parameter`...`	Trailing dots indicate that you can enter multiple parameters on a command line, separated by spaces.
option`[,...]`	Trailing dots, preceded by a comma, indicate you can enter multiple variables, separated by commas and *no* spaces.
`[`*parameter*`]`	Brackets indicate that the item inside the bracket is optional.
`>`	A greater than symbol represents a Windows system prompt.

ASMCLI Command Summary

Table 36 provides an alphabetical summary of the commands and describes the function of each command. You must prefix subcommands and parameters with either a hyphen (-) or a forward slash (/).

Table 36: ASM/ME CLI Subcommands

Subcommand	Function
`-alert`	Display a list of alerts, or enable and disable specific alerts.

Subcommand	Function
-breaksmartcopy	VSS automatically sets volume attribute values when a Smart Copy is created, and automatically undoes these changes for a mount or restore operation. This command allows you to undo these changes on demand.
-cloneReplica	Create a clone of a replica.
-configureASM	Set one or more ASM properties.
-configureCHAP	Specify the CHAP username and secret for a group.
-createCollection	Create new collections of volumes or components.
-delete	Delete Smart Copies.
-deleteCollection	Delete existing collections of volumes or components.
-enumerateiSCSIPortals	Enumerate or list all the target iSCSI portals found on the system.
-enumerateSmartCopies	Enumerate or list all the Smart Copies usable for the restore commands supported for a specified Smart Copy source object.
-help	Lists all of the commands in ASMCLI, including the parameters and options that can be specified for each one. Typing `asmcli -?` will also retrieve the same information.
-list	List supported the components, volumes, and collections.
-modifyCollection	Modify existing collections of volumes or components.
-mount	Mount Smart Copies.
-properties	Specify the `-properties` subcommand to list the properties of an existing Smart Copy backup document. You can specify the backup document by using the `-document=`, `-volume=`, `-component=`, or `-collection=` parameters.
-restore	Restore volumes in place from an existing backup document.
-selectiveRestore	Restore one or more selected components from a backup document. This operation is supported for SQL Server databases and Hyper-V virtual machines.
-shutdownsystray	Closes any verification failure notifications currently showing in the Windows taskbar notification area.

Subcommand	Function
`-shutdownverifier`	Safely shuts down the current Global Verification Task. This subcommand accepts the `-timeout=nnn` parameter, which specifies the time before a shutdown.
`-smart`	Create Smart Copies of supported components on PS Series groups.
`-unmount`	Unmount Smart Copies.
`-verify`	Run Checksum Verification or Soft Recovery (or both) for an existing Microsoft Exchange Smart Copy backup document. You must also specify `-recovery`, `-checksum`, or both options.
`-version`	Displays the ASM/ME version that you are running, as well as the build date.

Command Parameters

The following command options are used with the ASM/ME subcommands.

`all`

Used with: `delete` subcommand

Specify the `-all` parameter to delete all Smart Copies for the specified target (Collection, Volume, or Component). This will have no effect if the `-document` or `-objectid` parameter is specified.

`applylogs`

Used with: `restore` subcommand

Specify the `-applylogs` parameter to apply SQL Server logs when restoring SQL Server volumes. This option is ignored for non-SQL Server Smart Copies.

`backupType=`

Used with: `smart` subcommand

Specify the type of backup method to use when creating the Smart Copy. In the current release, you can specify a value of either `copy` or `full`. The default value is `copy`, which is assumed if you do not specify a value for `-backupType=`.

`category=`

Used with: `alert` subcommand

Specify the category of alerts you would like to view. If you omit this parameter, a list of all the alerts will be displayed. You can specify "C" or "Critical" for the critical alerts, "W" or "Warning" for the warning alerts, and "I" or "Informational" for the informational alerts.

`chapUser=`*`name`*

Used with: `configureCHAP` subcommand

Designates the username that identifies a valid CHAP user.

`checksum`

Used with: `smart`, `verify` subcommands

Specify `-checksum` to perform Checksum Verification on a Smart Copy. You can use this command only when making copies of Microsoft Exchange objects.

You can specify the `-checksum` subcommand together with the `-recovery` subcommand option to do both operations simultaneously. If you do not specify either the `-smart` or `-verify` subcommands, the `-checksum` parameter is d.

Optionally specify `-offpeak` to schedule Checksum Verification during the offpeak Global Verification times. See *Verification Settings on page 25*.

`cloneandverify`

Used with: `smart` subcommand

Specify `-cloneandverify` to perform checksum verification on a temporary Exchange replica clone to not pause replication. This flag will cause the tool to the `-recovery` flag.

`collection=collection_name`

Used with: `smart`, `verify`, `mount`, `properties`, `unmount`, `restore`, `createcollection`, `modifycollection`, `deletecollection` subcommands

Specify the `-collection=` parameter with a collection name as an alternative to specifying an `-objectID=`.

You can obtain the collection name from the ASM/ME GUI Collections node by browsing an individual collection's properties. Alternatively, use the following command to display of all Collection names:

```
> ASMCLI -list -collections -showobjectid
```

The `-collection=` parameter and the `-objectID=` parameter are mutually exclusive and the command parser processes the first valid parameter, ignoring any subsequent parameters.

If used with the `modifycollection` or `deletecollection` subcommands, the `-collection` parameter specifies a name that uniquely identifies the collection. If a collection with the name specified does not exist, the command will fail. When used with the `createcollectionsubcommand`, if a name is specified for a collection that already exists, the command will fail.

`collections`

Used with: `list` subcommand

Specify the `-collections` parameter to display all supported collections.

`combineNotification={"yes"|"no"}`

Used with: `configureASM` subcommand

Specifies whether smart copy creation and Exchange verification emails are combined into a single email before being sent.

`comment=comment_string$CLI$-@`

Used with: `smart` subcommand

Specify the `-comment=` parameter to add a comment string to the command, such as a description of the operation. Terminate the string with the sequence: CLI-@. The limit is 75 characters.

`component=component_name`

Used with: `smart`, `verify`, `mount`, `properties`, `unmount`, `restore`, `selectiveRestore`, `createcollection`, `modifycollection` subcommands

Specify the `-component=` parameter with the originating component name, such as a Microsoft Exchange Mailbox Database name. If the component name string contains an embedded space, you must enclose the string in quotation marks (`""`).

You can obtain the component name from the ASM/ME GUI Applications node by browsing an individual component's properties. Alternatively, use the following command to display all component names:

```
> ASMCLI -list -components -showobjectid
```

The `-component=` parameter and the `-objectID=` parameter are mutually exclusive and the command parser processes the first valid parameter, ignoring any subsequent parameters.

The `-component=` parameter is an alternative to using the `-document=` parameter, the `-volume=` parameter or the `-collection=` parameter. If you redundantly specify either a document path or a volume letter, the command parser s the redundant parameter.

When used with the `createcollection` or `modifycollection` subcommands, the `-component` parameter identifies a semicolon-delimited list of supported component specified by name. If this parameter is used, the `-volume=` parameter cannot be used.

`components`

Used with: `list` subcommand

Specify the `-components` parameter to display all supported components such as Microsoft Exchange Mailbox Databases.

`deletesnap`

Used with: `unmount` subcommand

Specify the `-deletesnap` parameter to delete the Smart Copy Set from which the target volume was unmounted.

If the Smart Copy Set contains multiple volumes this parameter has the following effect:

- It unmounts all volumes included in the Smart Copy that are currently mounted.
- It deletes all the volumes included in the Smart Copy regardless of their current mount status.

`disable`

Used with: `alert` subcommand

Specify the numerical ID for the alert you would like to disable. To view the numerical ID for each alert, type `asmcli -alert`.

`disableall`

Used with: `alert` subcommand

Specify the category name ("critical", "warning", or "informational") or the category abbreviation ("C", "W", or "I") to disable all alerts of that type.

`document="path"`

Used with: `verify`, `mount`, `properties`, `unmount`, `restore`, `selectiveRestore` subcommands

Specify the `-document=` parameter with the full path to a backup (*.bcd) document that you want to verify or mount. If any path variables contain embedded spaces, you must enclose the variable in quotation marks (`"`).

You need only specify the unique portion of the path following the PS Series volume identifier (`Ps Vol ID`), including the file name, and the folder in which the file is stored.

`documentFolder="path"`

Used with: `configureASM` subcommand

Designates the full directory path to folder where the Smart Copy backup document and collection definition folders are located.

`group="name"`

Used with: `configureCHAP` subcommand

Designates the name of the group for which credentials will be specified.

`email`

Used with: `smart, verify, mount, restore, unmount, selectiveRestore, delete` subcommands

Specify the `-email` parameter to send an email message confirming the status of the operation. The email is sent when an alert is triggered. To receive email notifications, you must ensure that both alert and email notification settings have been configured. For smart and verify subcommands, the email parameter is set by default. See *Notification Settings on page 21*.

`emailRecipientList="email_address"`

Used with: `configureASM` subcommand

Specifies a semicolon delimited list of email addresses to whom email should be sent when certain ASM/ME actions are performed.

`emailSenderAddress="email_address"`

Used with: `configureASM` subcommand

Specifies the email address from whom email should be sent when ASM/ME actions that support sending email are performed.

`emailSubjectLine="subject_line`

Used with: `configureASM` subcommand

Specifies the subject line of an email sent when ASM/ME actions that support sending email are performed.

`enable=`

Used with: `alert` subcommand

Specify the numerical ID for the alert you would like to enable. To view the numerical ID for each alert, type `asmcli -alert`.

`enableall=`

Used with: `alert` subcommand

Specify the category name ("critical," "warning," or "informational") or the category abbreviation ("C," "W," or "I") to enable all alerts of that type.

`enableEmails=`

Used with: `configureASM` subcommand

Specify whether or not to enable email functionality when configuring ASM/ME. The options are `yes` and `no`.

`ignorelogoutfail`

Used with: `smart`, `verify`, `unmount`, `restore` subcommands

(This parameter is restricted to Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012.)

Specify the`-ignorelogoutfail` parameter to change the default command behavior for logout failures. By default, the unmount operation is aborted if it encounters a logout failure and all retry attempts are exhausted. When you specify `-ignorelogoutfail`, the unmount operation forces the logout.

Caution: To avoid a risk of data corruption, make sure that no files are open on the volume that you intend to unmount.

`keepcount=nn`

Used with: `smart` subcommand

Specify `-keepcount=nn` where the value of `nn` is an integer in the range 0-99. This value indicates the maximum number of Smart Copy backup documents retained at any one time. If you not specify a value for `-keepcount`, a default value of 8 backup documents is assumed.

Due to internal implementation details, replication schedules for boot volumes create three Smart Copy replicas on the group for every one displayed in ASM, for each replication. The `keepcount` value refers to the number of replicas maintained by ASM, not on the group. When you delete a Smart Copy from the host, all three replicas created by the scheduled replication are deleted.

The `-keepcount` queue operates on a chronological first-in-first-out basis. If you create a Smart Copy causing the number of current Smart Copies to exceed the value of `-keepcount`, the oldest Smart Copy backup document is deleted.

You must specify the `-scheduleID=` parameter when specifying `-keepcount=`, otherwise the keep count limit is not maintained and Smart Copies are created until there is insufficient space. Specify a unique schedule identifier, using an `8-4-4-4-12` hexadecimal format. For example:

```
-scheduleID="00000000-1111-2222-3333-000000000000"
```

`location="[{* | drive_letterA;drive_letterB;... | mount_point;mount_point;...}]"`

Used with: `smart, mount, unmount` subcommands

Specify the `-location=` parameter with the location of one or more volumes or document paths as follows:

- A wildcard (*) mounts the volumes in the Smart Copy at any available drive letters.
- An ordered list of drive letters (such as `G:\`) with each drive letter delimited by a semicolon (`;`).
- One or more mount point paths at which the volumes in the Smart Copy backup document should be mounted. Each path is delimited by a semicolon (`;`).

When specifying the `-location` parameter, you can enter either the wildcard, or a semicolon-delimited list that can contain both drive letters and path names of mount points. The `-location` parameter is optional for everything but template volumes.

To omit a Smart Copy, enter a semicolon at its position in the list. If any path variables contain embedded spaces, you must enclose the variable in quotation marks (“”).

The list of volumes in an existing collection is sorted into ascending alphabetical order when the Smart Copy is created. For example, if the Smart Copy set contains volumes originally mounted at E:\, F:\Mount Point A , and G:\ and the -location=T:\;S:\;H:\ then the Smart Copies of volumes E:\ will be mounted as T:\, F:\Mount Point A will be mounted as S:\, and G:\ will be mounted as H:\.

`locationroot="[}drive_letter | mount_point}]"`

Used with: `smart`, `mount` subcommands

Specify the `-locationroot=` parameter with a drive letter or mount point. The `locationroot` represents a tree of all the mount points needed to mount every volume in the Smart Copy.

If any path variables contain embedded spaces, you must enclose the variable in quotation marks (“”).

`newname=`

Used with: `modifycollection` subcommand

Specifies a new collection name. This name must be valid and not be identical to another existing collection name. If a collection is renamed, and Smart Copies and Schedules of the collection will be updated to refer to the renamed collection. Schedule names will not be automatically modified, but can be changed by selecting the Modify Schedule option for the affected schedule.

`NoEmail`

Used with: `smart`, `verify`, `delete`, `restore`, `selectiverestore`, `unmount`, and `mount` subcommands

Specifying this parameter will ensure that you do not receive an email notification when alerts are triggered. This parameter is set by default for `delete`, `restore`, `selectiverestore`, `unmount`, and `mount`subcommands. To receive an email notification for these subcommands, specify the `email` parameter.

`nosignatureupdate`

Used with: `breaksmartcopy` subcommand

Specifying this parameter will only reset the volume attributes (HIDDEN, READONLY, SHADOWCOPY, and NO_DEFAULT_DRIVE_LETTER), and not the disk signature. If you do not specify this parameter, both the disk signature and the volume attributes will be reset.

`objectID=`

Used with: `smart`, `mount`, `unmount`, `restore`, `properties`, `delete`, and `selectiveRestore` subcommands

Specify the `-objectID=` parameter with an object identifier for an existing object. Use the `-list` command to display object identifiers. For example:

```
ASMCLI -list -volumes -collections -components -showObjectID
```

Depending on the operation that you want to perform, specify one of the following parameter values:

- Volume Operations—Specify a PS Series volume identifier (Ps Vol ID). A volume identifier has the following format: `Psv{hex-string}`. For example:
  `Psv{18a09060-3be0-3fa8-0a7a-e4120000e045;32256}`

  You can obtain the Ps Vol ID from the ASM/ME GUI Volumes node by browsing an individual volume's properties. Alternatively, use the following command to display the Ps Vol ID for all supported volumes:
  `ASMCLI -list -volumes -showobjectid`
- Application Component Operations—Specify a component name. A component name has the following format: `Component{hex-string}`. For example:
  `Component{38951b83-4249-4a16-8962-563d8de79c92}`.

  You can obtain the component name from the ASM/ME GUI Applications node by browsing an individual component's properties. Alternatively, use the following command to display all component names:

  ```
  ASMCLI -list -components -showobjectid
  ```
- Collection Operations—Specify a collection name. A collection name has the following format: `Collection{ascii_string}`. For example: `Collection{exchange_collection}`

You can obtain the collection name from the ASM/ME GUI Collections node by browsing an individual collection's properties. Alternatively, use the following command to display of all Collection names:

```
> ASMCLI -list -collections -showobjectid
```

When you specify an `-objectID=` parameter, the command parser ignores any subsequent `-volume=`, `-collection=`, and `-component=` parameters.

`offpeak`

Used with: `smart`, `verify` subcommands

Specify the `-offpeak` parameter to schedule Checksum Verification during the offpeak Global Verification times (predicted periods of low computer use). When you specify `-offpeak`, you must also specify the `-checksum` parameter.

You can specify that this parameter can be used with the `-smart` command if you specify either `-checksum` or `-verify`, or both.

You can also specify the `-offpeak` parameter with the `-verify` command.

If you do not specify either the `-offpeak` parameter or the `-remote` parameter, Checksum Verification begins immediately after Smart Copy completion.

`promoteandverify`

Used with: `smart` subcommand

Specify `-promoteandverify` to perform checksum verification directly on a promoted Exchange replica which will pause replication until the operation has completed.

`readwrite`

Used with: `mount` subcommand

Specify the `-readwrite` parameter to enable both reads from and writes to the mounted volume. If not specified, the volume is mounted read-only.

`recovery`

Used with: `smart` subcommand

Specify `-recovery` to perform checksum verification or Soft Recovery (or both) on the Smart Copy. You can use this command only when making copies of Microsoft Exchange objects.

You can specify the `-recovery` subcommand together with the `-checksum` subcommand option to do both operations simultaneously. If you do not specify either the `-smart` or `s` subcommands are not specified, the `-recovery` parameter is ignored.

`retry=n`

Used with: `mount`, `unmount`, `restore` subcommands

Specify the `-retry=` parameter with an integer value indicating the number of times to retry the operation if unsuccessful.

`remote`

Used with: `smart`, `verify` subcommands

Specify the `-remote` parameter to schedule Checksum Verification on a remote computer instead of the local computer. If configured on the remote computer, Checksum Verification (and Soft Recovery, if specified), runs during the offpeak Global Verification times. Configure the remote computer to find and verify the newly-created backup document.

You can specify that this parameter can be used with the `-smart` command if you specify either `-checksum` or `-verify` or both.

You can also specify the `-remote` parameter with the `-verify` command.

If you do not specify the `-remote` parameter, Checksum Verification begins immediately after Smart Copy completion.

Global Verification schedule times default to 8:00 PM to 6:00AM local time. You can change this time by adjusting the Global Verification window in the ASM/ME GUI. See *Verification Settings on page 25*.

See *Run Checksum Verification and Soft Recovery on a Remote Host on page 91* for information about configuring the remote computer.

`scheduleID=`

Used with: `smart` subcommand

Specify the `-scheduleID=` parameter with a schedule identifier (Schedule ID) for an existing schedule. You can obtain this identifier by browsing a schedule's properties in the ASM/ME GUI. Click the right mouse button to copy the schedule ID to the clipboard.

A typical Schedule ID has the following format:

```
ee05bb76-6ccc-431a-99b9-37886a1d7748
```

You must enclose the Schedule ID in quotation marks if it contains and embedded space.

`selections=`

Used with: `selectiveRestore` subcommand

Specify the `-selections=` parameter with `"Component{}"` , where the object ID for the component to be restored is placed within the braces. A semilcolon delimited list of object IDs may also be specified.

You can also use the SSA names as they appear in the GUI to restore an SSA.

You can get the object ID for any supported component, volume, and collection by executing the `-list` command with the `-components`, `-volume`, `-collections`, and `-showObjectID` options.

`secret=`*`password`*

Used with: `configureCHAP` subcommand

Specifies the password that was established for the CHAP user.

`sendOnFailure={"Yes"|"No"}`

Used with: `configureASM` subcommand

Specifying yes will enable all critical alerts, and specifying no will disable all critical alerts.

`sendOnSuccess={"Yes"|"No"}`

Used with: `configureASM` subcommand

Specifying yes will enable all warning and informational alerts, and specifying no will disable all warning and informational alerts.

`sendTestMail`

Used with: `configureASM` subcommand

Sends a test email immediately after configuring ASM/ME. This is to test email settings. A recipient list will be included in the test email.

`shadowType=`

Used with: `smart` subcommand

Specify the type of Smart Copy to create. In the current release, ASM/ME supports only `Transportable` types and you can omit this parameter because ASMCLI assumes a `Transportable` type.

`showObjectID`

Used with: `list` subcommand

Specify the `-showObjectID` parameter to display the unique object identifiers for each object.

`showprops`

Used with: `list` subcommand

Specify the `-showprops` parameter to display the following object properties in the output:

- For lists of volumes, the output includes the volume type, PS Series volume name, and read-only setting.
- For lists of collections, the output includes all component names and volumes included in the collection.
- For lists of components the output includes the original volume list and application type (such as Microsoft Exchange or SQL Server).

`smartcopy`

Used with: `configureCHAP` subcommand

Indicates that the credentials apply to snapshot access.

`smtpHost={"host_name" |"ipaddress"`

Used with: `configureASM` subcommand

Specifies the fully qualified name or IP address of the SMTP Host to be used to send email when ASM/ME actions that support sending email are performed.

`smtpport=`

Used with: `configureASM` subcommand

This port will be used as a fallback port if the SMTP Server port cannot be accessed.

`smartcopyType=`

Used with: `smart` subcommand

Specify the required form of Smart Copy. You can specify a value of `snapshot`, `clone`, `replica`, or `ThinClone` if your storage is configured to support these options. The default value is `snapshot`, which is assumed if you do not specify a value for `-snapshotType=`.

`ssa`

Used with: `smart` subcommand

Optionally specify the `-ssa` parameter to select either a Search Service Application (SSA) name or an SSA ID, for which to create the Smart Copy. If this parameter (and the `spCategory` parameter) is omitted, ASM/ME creates a Smart Copy of the entire farm.

`spCategory`

Used with: `smart` subcommand

Optionally specify the `-spCategory` parameter to select between a SharePoint farm or one component of the SharePoint farm, for which to create a Smart Copy. The options are `farm`, `content`, or `ssa`.

The `content` option will create a Smart Copy of the content databases. The `ssa` option will create a Smart Copy of the specified Search Service Application. If you choose `ssa`, you must also use the `ssa` parameter to identify the specific SSA.

If you do not use either the `spCategory` parameter or the `ssa` parameter, ASM/ME creates a Smart Copy of the entire farm by default.

`unmountonly`

Used with: `unmount` subcommand

Specify the `-unmountonly` parameter to unmount the volumes without logging off. (By default, unmounting a volume both unmounts it and logs off.)

`useEarliest`

Used with: `verify`, `mount`, `properties`, `unmount`, `delete`, `restore` subcommands

Specify the `-useEarliest` parameter to use the chronologically earliest Smart Copy. The `-useLatest` parameter is the default, and is assumed if you do not specify either `-useLatest` or `-useEarliest`.

You can use the -useEarliest parameter only if you specified the -volume= parameter, the -component= parameter, or the -collection= parameter.

useLatest

Used with: verify, mount, properties, unmount, delete, restore subcommands

Specify the -useLatest parameter to use the chronologically latest Smart Copy. The -useLatest parameter is the default, and is assumed if you do not specify either -useLatest or -useEarliest.

You can use the -useLatest parameter only if you specified the -volume= parameter, the -component= parameter, or the -collection= parameter.

volume=

Used with: smart, verify, mount, properties, unmount, restore, selectiveRestore, createcollection, modifycollection subcommands

Specify the -volume= parameter with the path for a mount point or a drive letter of a volume as an alternative to specifying an -objectID=. Typical drive letter values are G:\ and Z:\.

You can obtain the drive letter from the ASM/ME GUI Volumes node by browsing an individual volume's properties. Alternatively, use the following command to display all supported drive letters:

```
ASMCLI -list -volumes -showobjectid
```

The -volume= parameter and the -objectID= parameter are mutually exclusive and the command parser processes the first valid parameter, ignoring any subsequent parameters.

The -volume= parameter is an alternative to using the -document= parameter. If you redundantly specify either a path, or a collection name, the command parser ignores the redundant parameter.

For the mount command, the -useEarliest or -useLatest parameter determines which specific backup document is mounted. The -useLatest parameter is the default, and is assumed if you do not specify either -useLatest or -useEarliest.

When used with the createcollection or modifycollection subcommands, the -volume parameter identifies a semicolon-delimited list of volumes specified as drive letters or mount points. If this parameter is used, the -component= parameter cannot be used.

volumeBased=

Used with: createcollection, modifycollection subcommands. The options are yes or no.

Setting this parameter to yes specifies that the operation will not fail even if a database, VM, or Exchange store associated with a volume in the collection cannot be found. For example, assume a collection that contains a volume named vol1, associated with a SQL database called DB1. If you delete DB1 and then create a Smart Copy of the collection, the operation will succeed even though DB1 is no longer associated with vol1.

`volumes`

Used with: `list` subcommand

Specify the `-volumes` parameter to display all supported volumes.

If you do not specify the `-volumes` parameter, the `-collections` parameter, or the `-components=` parameter, the command parser assumes a value of `-volumes` as the default.

`vssvds`

Used with: `configureCHAP` subcommand

Indicates that the credentials apply to management access.

`writer`

Used with: `smart`, `mount`, `unmount`, `restore`, `properties`, `delete`, `selectiveRestore`, `enumerateSmartCopies`, and `breakSmartCopy` subcommands.

Applies to SharePoint farms only.

Specify `-writer` to restrict the operation to a particular SharePoint VSS writer on a host (writer host).

`writers`

Used with: `list` subcommand.

Specify `-writers` to display a list of SharePoint writers on the local host.

ASMCLI Commands and Their Syntax

The following section lists the ASMCLI commands. Examples shown in the following sections contain line breaks where long strings wrap. Do not insert line breaks in actual commands.

ASMCLI -alert

Email alerts can be controlled using the ASMCLI alert command. Enabling or disabling alerts through ASMCLI will automatically set the corresponding alerts in the GUI, and enabling or disabling alerts in the GUI will update the alert status when you view alerts through ASMCLI.

See *Alert Settings on page 22* for a list of available alerts.

You will not receive email alerts until you configure email settings. To configure email settings using ASMCLI, use the `configureASM` command. To configure email settings using the GUI, click `View`, then `Settings`, and click the `Notifications` tab.

The `delete`, `restore`, `mount`, `unmount`, and `selectiverestore` commands have the `-noemail` parameter set by default. This means that if alerts are enabled and you execute any of these commands using ASMCLI, you will not get an email notification when the operation completes unless you specify the `-email` parameter when you execute the command.

Similarly, the `smart` and `verify` commands have the `-email` parameter set by default. This means that if alerts are enabled and you execute either of these commands, you will automatically get an email notification when the operation completes. If you do not want to receive one, you must specify the `-noemail` parameter when you execute the command.

If you specify the `-email` parameter and still do not receive an email notification, make sure that the associated alert is enabled.

Command Syntax

```
ASMCLI -alert -category={"category_name"|"category_abbreviation"} | -enable=
{"alert_ID"} | -disable={"alert_ID"} | -enableall={"category_name"|"category_
abbreviation"} |
-disableall={"category_name"|"category_abbreviation"}
```

The value of "`alert_ID`" is the numerical value assigned to each alert.

For `-category`, enter either the category name (Informational, Warning, or Critical) or the abbreviation ("I" for Informational, "W" for Warning, or "C" for Critical).

For a description of the parameters, see *Command Parameters on page 153*.

Examples

1. Display all of the alerts, their numerical IDs, and their current settings (enabled or disabled).

   ```
   ASMCLI -alert
   ```

2. The following examples show two ways of listing all of the Warning alerts and their current settings.

   ```
   ASMCLI -alert -category=W
   ASMCLI -alert -category=warning
   ```

3. Disable the critical alert for MPIO Logout Errors.

   ```
   ASMCLI -alert -disable=25
   ```

4. Enable all critical alerts.

   ```
   ASMCLI -alert -enableall=C
   ```

ASMCLI -breaksmartcopy

When VSS is used to create a Smart Copy, it changes the disk signature, and it sets some attributes (HIDDEN, READONLY, SHADOWCOPY, and NO_DEFAULT_DRIVE_LETTER). If VSS is used to restore the volume, or if the volume is mounted using ASM or ASMCLI, these changes are automatically undone. It might be useful to be able to undo these changes on demand; for example:

- If you are creating replica volumes and you want to be able to promote the replicas and use them on remote failover servers. In this case, you are not performing a restore operation, so the changes made by VSS will not be undone, and when you attempt to mount the promoted replicas, they will not automatically be assigned drive letters because of the attributes VSS has set on them. Executing this command can prepare a set of replicas to be used in this way.
- If you need to be able to restore a Smart Copy by rolling back the volume in the Group Manager GUI without using ASM/ME. Note that ASM/ME normally resets the disk signature when creating any kind of Smart Copy of a boot volume, so Smart Copies of boot volumes do not require you to use this command.

When the Smart Copy boots to the operating system for the first time, there will be a message displayed that the O/S was not properly shutdown. The user will be asked to boot normally or boot to repair. This is to be expected since the smart copy was taken with the operating system running. There should be nothing to repair and the user can choose the option to boot normally.

Command Syntax

```
ASMCLI -breaksmartcopy [{-volume={"drive_letter" |"mount-point"} |
-component="component_name" | -collection="collection_
name" | -objectID="identifier" |
-writer="writer_name"}] [-nosignatureupdate] [-retry=1-n]
```

Examples

1. The following command resets the disk signature and volume attribute values for volume C:\.

   ```
   ASMCLI -breaksmartcopy -volume=c:\
   ```

2. The following command resets the volume attributes (HIDDEN, READONLY, SHADOWCOPY, and NO_DEFAULT_DRIVE_LETTER) and not the disk signature for volume C:\.

   ```
   ASMCLI -breaksmartcopy -volume=c:\ -nosignatureupdate
   ```

ASMCLI -cloneReplica

The `-cloneReplica` command creates a clone from an existing replica.

Command Syntax

```
ASMCLI -cloneReplica [{-document="path" | -volume={"drive"|"mount_point" |
-component="component_name" | -collection="collection_
name"|-objectID="identifier"}] [{-useLatest | -useEarliest]
```

For a description of the parameters, see *Command Parameters on page 153*.

Example

Create a clone of the most-recent Smart Copy backup document available for `F:\`.

```
> ASMCLI -cloneReplica -volume=F:\ -useLatest
```

ASMCLI -configureASM

Specify the `-configureASM` subcommand to set one or more ASM properties from the command line. If no properties are specified, the current values are output for all of the properties. Each property is validated and the output shows results for each property.

Command Syntax

```
ASMCLI -configureasm -documentFolder="path" -enableEmails={"Yes"|"No"}
-emailRecipientList="email_address" -emailSenderAddress="email_address"
-emailSubjectLine="text" -smtpport= {"1-n"} -smtpHost={"hostname"|"ipaddress"}
-sendOnFailure={"Yes"|"No"} -sendOnSuccess={"Yes"|"No"} |
-combineNotification={"Yes"|"No"} | -sendTestMail -debugfile="path"
-debuglevel={"1"|"2"|"3"}
```

For a description of the parameters, see *Command Parameters on page 153*.

Example

Display all of the properties that can be configured and their current values.

```
ASMCLI -configureASM
```

ASMCLI -configureCHAP

The `-configureCHAP` command specifies the CHAP username and secret for a group.

Command Syntax

```
ASMCLI -configurechap -group="name" | -chapUser="name" | -secret=password |
-vssvds | -smartcopy
```

For a description of the parameters, see *Command Parameters on page 153*.

Example

Sets the credentials that ASM/ME uses for management access to TestGroup to `username` and `password`.

```
ASMCLI -configureCHAP -group=TestGroup -chapuser=username -secret=password -vssvds
```

ASMCLI -createCollection

The `-createCollection` command creates and validates a new collection from a list of volumes or components. ASMCLI handles collection creation differently than the ASM/ME GUI. If you use ASMCLI to create a collection and specify a list of volumes, the collection will contain all the volumes and every component that is fully contained on those volumes. If you specify a list of components, the collection will contain all the component and every volume that those components use.

Command Syntax

```
ASMCLI -createcollection -collection="collection_name"
[-volume={"drive" | "mount_point"} -component="component_name"]
-volumeBased={"Yes"|"No"}
```

For a description of the parameters, see *Command Parameters on page 153*.

Examples

1. Create a collection Test Collection 1 containing volumes e:\ and F:\ and add any components contained on the volumes.

   ```
   ASMCLI -createcollection -collection="Test Collection 1" -volume=e:\;f:\
   ```

2. Create a collection Test Collection 2 containing components Mailbox Database A and Mailbox Database B and add the volumes for the components to the collection.

   ```
   ASMCLI -createcollection -collection="Test Collection 2" -component="Mailbox
   Database A;Mailbox Database B"
   ```

ASMCLI -delete

Specify the `-delete` subcommand to delete an existing Smart Copy and all its data.

Use optional parameters to specify the Smart Copy set to delete by:

- Backup document path
- Originating volume or component or collection with the `useLatest` or `useEarliest` option.

Using -delete with Cloud Services

The delete command can now be run on existing external replicas. When the delete is complete, the associated data with that smartcopy will be deleted from the cloud. Keep in mind that deletes are much harder to verify on the cloud, because we merge the data to other existing snapshots when we perform a delete. Deletes for external replicas are not instantaneous. The delete operation does not complete until the data is successfully merged on the external cloud provider.

Command Syntax

```
ASMCLI -delete [{-document="path" | -volume={"drive" |"mount_point" |
-component="component_name" | -collection="collection_name" |
-writer="writer_name" | -objectID="identifier"}]
[{-useLatest | -useEarliest |-all}] [-email | -noemail] -retry=n
```

For a description of these parameters, see *Command Parameters on page 153*.

Examples

1. Delete the Smart Copy backup document `6666-7777-888.bcd`.

   ```
   ASMCLI -delete -document="C:\BackupDocs\Shadows\
   PSV{11111111-2222-3333-4444-555555555555}\6666-7777-888.bcd"
   ```

2. Delete the Smart Copy backup document `6666-7777-888.bcd`.

   ```
   ASMCLI -delete document="PSV{11111111-2222-3333-4444-555555555555\
   6666-7777-888.bcd"
   ```

3. Delete the most recent Smart Copy backup document available for F:\

   ```
   ASMCLI -delete -volume=F:\ -useLatest
   ```

4. Delete the oldest Smart Copy backup document available for the Exchange Mailbox Database named MyMailboxDatabase.

   ```
   ASMCLI -delete -component="MyMailboxDatabase" -useEarliest -location="Q:\"
   ```

ASMCLI -deleteCollection

The `-deleteCollection` command deletes an existing collection specified by name.

Command Syntax

```
ASMCLI -deletecollection -collection="collection_name"
```

For a description of these parameters, see *Command Parameters on page 153*.

Example

Delete the collection called Test Collection:

```
ASMCLI -deletecollection -collection="Test Collection"
```

ASMCLI -enumerateiSCSIPortals

The `-enumerateiSCSIPortals` subcommand enumerates or lists the iSCSI target portals available on the system.

This command outputs a list of iSCSI target portals, the IP address, and error and status information.

Command Syntax

```
ASMCLI -enumerateiSCSIPortals
```

Example

Enumerate all of the iSCSI target portals on the system:

```
ASMCLI -enumerateiSCSIPortals
```

```
1 iSCSI Target Portals discovered:
iSCSI Target Portal: 10.127.63.100 Status: No errors Error: N/A
```

ASMCLI -enumerateSmartCopies

The `-enumerateSmartCopies` subcommand enumerates or lists the Smart Copy Sets of a specified component that can be used with the restore and selective restore commands. This subcommand omits Smart Copy Sets that cannot be used for restore operations, such as Smart Copies that are unreachable, or in a temporary state (such as having checksum verification in progress).

This command outputs the timestamp for when the Smart Copy Set was created, as well as the relative backup document pathname for each backup document that supports the restore and selective restore commands. A summary line reports the total number of documents found, and the number of documents that are usable for the restore commands supported for the Smart Copy source object.

The document pathname can be used for the `-document` parameter of the restore commands. The pathname does not include the shadows folder portion of the path.

Command Syntax

```
ASMCLI -enumerateSmartCopies [{-volume={"drive_letter" |"mount_point"} |
-component="component_name"} | -collection="collection_name" |
-writer="writer_name" | -objectID="identifier"]
```

For a description of these parameters, see *Command Parameters on page 153*.

Example

Enumerate all of the backup documents for component DB1:

```
ASMCLI -enumerateSmartCopies -component=DB1
```

ASMCLI -help

Specify the `-asmcli -help` subcommand to view all of the commands in the ASMCLI, including the parameters and options that can be specified for each one. Typing `-asmcli -?` will also retrieve the same information.

Command Syntax

```
ASMCLI -asmcli -help
```

You can also type the following command:

```
ASMCLI -asmcli -?
```

ASMCLI -list

Specify the `-list` subcommand to identify supported volumes, collections, and components. You can also obtain an object's unique identifiers and use the identifiers as required in commands or scripts.

You can obtain additional properties for the volumes, components, and collections by using the `-showprops` parameter.

Use the redirect option (`>`) in the Windows command prompt to save the output from the `-list` command to a file for later editing.

On a cluster, the `-list` command shows only the volumes and components for the node on which you execute the command owns the related physical disk resources.

Command Syntax

```
ASMCLI -list -volumes -collections -components -showObjectID -showprops -
writers
```

For a description of these parameters, see *Command Parameters on page 153*.

Examples

1. List all of the volumes, collections, and components with their object IDs:

```
ASMCLI -list -volumes -collections -components -showObjectID
```

2. List all existing collections:

```
ASMCLI -list -collections
```

3. List all of the supported volumes:

```
ASMCLI -list
```

4. List all of the configured SharePoint writers:

```
ASMCLI -list
```

ASMCLI -modifyCollection

The `-modifyCollection` command modifies an existing collection by replacing the current definition with a list of volumes or components, if the list constitutes a valid collection. If the modification fails validation, the original definition is unchanged.

Command Syntax

```
ASMCLI -modifycollection [-collection="collection_name"]
[-volume={"drive" | "mount_point"} | -component="component_name"]
[-newname] [-volumeBased={"Yes"|"No"}]
```

For a description of these parameters, see *Command Parameters on page 153*.

Example

Modify the collection Test Collection 1 by changing its definition to volumes e:\ and f:\, and add any components contained on the new volumes.

```
ASMCLI -modifycollection -collection="Test Collection 1" -volume=e:\;f:\
```

ASMCLI -mount

Specify the `-mount` subcommand to mount an existing Smart Copy.

Use optional parameters to mount multiple volumes and control the selection of volumes, the version.

Note: ASM will only detect drives that were mapped with the same user as ASM is running. This is caused by the user access control behavior on Windows. Windows Explorer runs under the administrator account, so if you used Windows Explorer to map a network folder and your ASM is running as a system account, ASM won't detect that network folder. That network folder will be mounted but you will still see the network folder mapped to the original drive letter you used in Windows Explorer.

Command Syntax

```
ASMCLI -mount [{-document="path" | -volume={"drive_letter" |"mount_point"} |
-component="component_name" | -collection="collection_name" |
-writer="writer_name" | -objectID="identifier"}]
[{-location="* | drive_letterA;drive_letterB;... |mount_point;;... | -
locationroot=<drive_letter|mount_point}]"
[{-useLatest | -useEarliest}] [-email | -noemail] -readwrite -retry=n
```

For a description of these parameters, see *Command Parameters on page 153*.

Examples

1. Mount the Smart Copy backup document named `e2b3-f1a3-234.bcd` on drive D:

   ```
   ASMCLI -mount -document="C:\BackupDocs\Shadows\
   PSV{18A09060-3BE0-3FA8-0A7A-E4120000E045;32256}\e2b3-f1a3-234.bcd"
   -location=D:\
   ```

2. Mount the Smart Copy backup document named `e2b3-f1a3-234.bcd` at the mount point `D:\Data2Server`:

   ```
   ASMCLI -mount -document= "PSV{18A09060-3BE0-3FA8-0A7A-E4120000E045;32256}\
   e2b3-f1a3-234.bcd" -location="D:\Data2Server"
   ```

3. Mount the most recent Smart Copy backup document available for volume `F:\` on drive Q:

   ```
   ASMCLI -mount -volume=F:\ -useLatest -location="Q:\"
   ```

4. Mount the oldest Smart Copy backup document available for the Microsoft Exchange Mailbox Database named `Mailbox2Database` on drive Q:

   ```
   ASMCLI -mount -component="Mailbox2Database" -useEarliest -location="Q:\"
   ```

ASMCLI -properties

Specify the `-properties` subcommand to list the properties of an existing Smart Copy backup document.

Command Syntax

```
ASMCLI -properties [-document="path" | -volume={"drive_letter"|"mnt-pnt"} |
-component="component_name"] | -collection="collection_name" |
-writer="writer_name" | -objectID="identifier" |  [-useLatest | -useEarliest]
```

For a description of these parameters, see *Command Parameters on page 153*.

Command Output

The following data is provided in the output from this command, depending on the parameters that you specify. Each property is preceded by the specified identification string.

Table 37 lists the various identifiers that are displayed on the screen when you run the properties command.

Table 37: Identifiers for ASMCLI Properties

Identifier	Smart Copy Property
-document=	Path name of Smart Copy Set backup document.
-creationtimestamp=	Creation timestamp.
-OriginatingObject=	Name of the supported volume, component, or collection from which the Smart Copy was created.
-OriginatingHost=	Host name of the machine on which the Smart Copy was created.
-snapshottype=	Snapshot type (snapshot, replica, clone, or thin clone).
-backupType=	Backup Type (copy or full).
-Snapshotcount=	Number of snapshots contained in the Smart Copy Set.
-OriginalVolumes=	Semicolon delimited list of the original volumes from which the Smart Copy Set was created.
-SmartCopyStatus=	Current state of the Smart Copy Set (broken, unreachable, mounted, or available).
-MountPoints=	If the Smart Copy is mounted, a semicolon delimited list of the mount points.
-Application=	Application type (Microsoft Exchange, SQL Server, SharePoint, Hyper-V, or File system).
-ChecksumVerification=	Checksum Verification state. (Microsoft Exchange only).
-SoftRecovery=	Soft Recovery state (Microsoft Exchange only).
-ReplicationStatus	• If the snapshot type is a replica, this indicator shows the current status of the replication process using one of the following strings: • Disabled; The replica set containing this replica is promoted to access a different replica. • Disabled; Replication is in progress - The replica has been deleted on the PS Series group.

Identifier	Smart Copy Property
	• Disabled; Invalid replica. • Disabled; Replication is in progress. • Disabled; The replica set containing this replica is promoted. • Disabled; Could not connect to remote group. • Valid replica.
`-ApplicationConsistent`	Indicates whether the snapshot is application consistent (True or False).

Examples

1. List the properties for the Smart Copy backup document `6666-7777-888.bcd`.

```
ASMCLI -properties -document="C:\BackupDocs\Shadows\
PSV{11111111-2222-3333-4444-555555555555}\6666-7777-888.bcd"
```

2. List the properties for the same backup document:

```
ASMCLI -properties -document=\
"PSV{11111111-2222-3333-4444-555555555555}\6666-7777-888.bcd"
```

3. List the properties for the most recent Smart Copy backup document available for `F:\`.

```
ASMCLI -properties -volume=F:\ -useLatest
```

4. List the properties for the oldest Smart Copy backup document available for the Exchange Mailbox Database named `MyMailboxDatabase`.

```
ASMCLI -properties -component="MyMailboxDatabase" -useEarliest
```

ASMCLI -restore

Specify the `-restore` subcommand to perform an in-place restore of a Smart Copy Set. An in-place restore copies the entire content of the Smart Copy Set to its original volumes, overwriting their content.

Use optional parameters to restore multiple volumes and control the selection of volumes, and the version of Smart Copy.

On a cluster, this command fails if:

- The target is the cluster quorum disk
- The target is a physical disk resource that has not been placed in maintenance mode
- The target is a physical disk resource that is not owned by this node or is a physical disk that is used to store Smart Copy Set backup documents

Command Syntax

```
ASMCLI -restore [{-document="path" | -volume={"drive_letter" |"mount_point"}
|-collection="collection_name" | -objectID="identifier" |
-component="component_name" | -writer="writer_name"}]
[{-useLatest | -useEarliest}] [-ignorelogoutfail] [-email | -noemail]
[-retry=n] [-applylogs]
```

For a description of these parameters, see *Command Parameters on page 153*.

Examples

1. Restore all of the volumes in place from backup document `e2b3-f1a3-234.bcd`:

   ```
   ASMCLI -restore -document=
   "PSV{18A09060-3BE0-3FA8-0A7A-E4120000E045;32256}\e2b3-f1a3-234.bcd"
   ```

2. Restore volume F:\ in place from the most recent backup document created for it:

   ```
   ASMCLI -restore -volume=F:\ -useLatest
   ```

3. Restore all of the volumes in place from the oldest backup document created for the Exchange Mailbox Database named *MyMailboxDatabase*:

   ```
   ASMCLI -restore -component="MyMailboxDatabase" -useEarliest
   ```

ASMCLI -selectiveRestore

Specify the `-selectiveRestore` subcommand to restore one or more selected components from a backup document. This operation is supported for SQL Server databases and Hyper-V virtual machines.

Use optional parameters to restore multiple volumes and control the selection of volumes, and the version of Smart Copy.

On a cluster, this command fails if:

- The target is the cluster quorum disk
- The target is a physical disk resource that has not been placed in maintenance mode
- The target is a physical disk resource that is not owned by this node

Command Syntax

```
ASMCLI -selectiveRestore [{-document="path" | -volume={"drive_letter" |"mount_
point"} | -component="component_name" | -collection="collection_name" |
-writer="writer_name" | -objectID="identifier"}]
-selections="Component{objectID};..." [{-useLatest | -useEarliest}]
[-email | -noemail] [-retry=n] [-applylogs]
```

For a description of these parameters, see *Command Parameters on page 153*.

Note: You can get the object ID for any supported component, volume, and collection by executing the `-list` command with the `-components`, `-volume`, `-collections`, and `-showObjectID` options.

Examples

1. Restore the specified components (SQL Server DB1 and DB3) from backup document `6666-7777-888.bcd`:

```
ASMCLI -selectiverestore -document="C:\BackupDocs\Shadows\
PSV{11111111-2222-3333-4444-555555555555}\6666-7777-888.bcd"
-selections="Component{mysqlserver_DB1}; Component{mysqlserver_DB3}"
```

2. Restore the Hyper-V virtual machine with object ID `Component {2F27806B-9BBB-4194-A61E-59D14831483F}` from backup document `6666-7777-888.bcd`:

```
ASMCLI -selectiverestore -document="C:\BackupDocs\Shadows\
PSV{11111111-2222-3333-4444-555555555555}\6666-7777-888.bcd"
-selections="Component{2F27806B-9BBB-4194-A61E-59D14831483F}"
```

ASMCLI -shutdownsystray

By default, ASM/ME displays warning icons in the Windows Taskbar Notification Area. Each warning icon is associated with a pop-up message describing an ASM/ME event, such as a failed Checksum Verification operation. See *Alerts and Event Notification on page 6* for more information.

Example

Stop event notification and remove any current event warning icons:

```
ASMCLI -shutdownsystray
```

ASMCLI -shutdownverifier

The `-shutdownverifier` subcommand accepts one optional parameter: `-timeout=nnn`.

The variable `nnn` is an integer in the range 0-999 specifying the number of seconds that ASMCLI should wait for the Global Verification Task to terminate.

ASMCLI -smart

Specify the `-smart` subcommand to create a snapshot, clone, or replica of an object such as a volume. You can use this command only on supported components residing on PS Series storage arrays. Use the `-list` command to obtain information about available objects and their object identifiers.

On a cluster, this command fails if the target is the cluster quorum disk or is a physical disk resource not owned by the cluster node on which you execute the command.

Command Syntax

```
ASMCLI -smart {-objectID="identifier" | -volume={"drive_letter" | mount_point} | -
collection="collection_name" | -component="component_name" |
-writer="writer_name"}] -scheduleID="schedule_identifier"
[-spcategory=farm|content|ssa] [-ssa="ssa_name | ssa_application_ID"]
[-location="[{* | drive_letterA;drive_letterB;... | mount_point;mount_point;...}]" |
-locationroot="drive_letter" | mount_point"]
-shadowType=Transportable -backupType={copy | full}
-smartcopyType={Snapshot | Clone | Replica | ThinClone }
[-keepCount=nn][-checksum] [-recovery] [-cloneandverify] [-promoteandverify]
[-offpeak] [-remote] [-ignorelogoutfail] [-email | -NoEmail]
[-comment=comment_string$CLI$-@]
```

For a description of these parameters, see *Command Parameters on page 153*.

Required Parameters

The following parameters are required to create a syntactically-correct command:

`-backupType`

`-component`

`-objectID`

`-scheduleID`

`-shadowType`

`-volume`

`-writer`

Common Optional Parameters

The following parameters are optional. The `email` parameter is set by default:

`-comment`

```
-keepcount

-email | -Noemail

-spcategory
```

Optional Exchange Parameters

The following parameters are optional for Microsoft Exchange:

```
-checksum

-recovery

-cloneandverify | -promoteandverify

-offpeak | -remote

-ignorelogoutfail
```

Optional SharePoint Parameter

If you have SharePoint installed, you can use the following parameter to specify whether to create a Smart Copy of the full SharePoint farm or a component of the farm:

```
-spcategory=farm|content
```

Examples

1. Create a thin-clone Smart Copy from the template volume with an object identifier string of `Psv{18a09060-ccb0-3c27-24b4-e4f5aa8f2643;1048576}` and then mount it to the K drive:

   ```
   ASMCLI -smart -email
   -objectid="Psv{18a09060-ccb0-3c27-24b4-e4f5aa8f2643;1048576}"
   -shadowtype=Transportable -backuptype=copy -snapshottype=ThinClone
   -location="K:\"
   ```

2. Create a Smart Copy of the volume with an object identifier string of `Psv{18a09060-3be0-3fa8-0a7a-e4120000e045;32256}`:

   ```
   ASMCLI -smart -scheduleID="ee05bb76-6ccc-431a-99b9-37886a1d7748"
   -objectID="Psv{18a09060-3be0-3fa8-0a7a-e4120000e045;32256}
   -shadowType=Transportable backupType=copy -snapshotType=Snapshot
   -keepCount=14
   ```

3. Create a Smart Copy of an SQL Server database with the component identifier string of `Component{38951b83-4249-4a16-8962-563d8de79c92}`:

   ```
   ASMCLI -smart -scheduleID="ee05bb76-6ccc-431a-99b9-37886a1d7748"
   -objectID="Component{38951b83-4249-4a16-8962-563d8de79c92}"
   ```

```
-shadowType=Transportable backupType=copy -snapshotType=Snapshot
-keepCount=14
```

4. Create a Microsoft Exchange Smart Copy and run Checksum Verification and Soft Recovery right after Smart Copy creation:

```
ASMCLI -smart -scheduleID="ee05bb76-6ccc-431a-99b9-37886a1d7748"
-objectID="Component{38951b83-4249-4a16-8962-563d8de79c92}"
-shadowType=Transportable -backupType=copy -snapshotType=Snapshot
-keepCount=14 -checksum -recovery
```

5. Create a Microsoft Exchange Smart Copy and perform Checksum Verification and Soft Recovery during the offpeak Global Verification times. (See *Verification Settings on page 25*):

```
ASMCLI -smart -scheduleID="ee05bb76-6ccc-431a-99b9-37886a1d7748"
-objectID="Component{38951b83-4249-4a16-8962-563d8de79c92}
-shadowType=Transportable -backupType=copy -snapshotType=Snapshot
-keepCount=14 -checksum -recovery -offpeak
```

6. Create a Microsoft Exchange Smart Copy for volume `F:\` with Checksum Verification and Soft Recovery during the offpeak Global Verification times (See *Verification Settings on page 25*):

```
ASMCLI -smart -scheduleID="ee05bb76-6ccc-431a-99b9-37886a1d7748" -v
olume=F:\
-shadowType=Transportable -backupType=copy snapshotType=Snapshot
-keepCount=14 -checksum -recovery -offpeak
```

7. Create a Microsoft Exchange Smart Copy for the group named *MyMailboxDatabase* and run Checksum Verification and Soft Recovery during the Global Verification window. This command specifies a value for the `-scheduleID=` parameter:

```
ASMCLI -smart -scheduleID="00000000-1111-2222-3333-00000000"
-component="MyMailboxDatabase" -shadowType=Transportable -backupTyp
e=copy
-snapshotType=Snapshot -keepCount=14 -checksum -recovery -offpeak
```

8. Create a Microsoft Exchange Smart Copy for MyMailboxDatabase and perform Checksum Verification and Soft Recovery during the global verification window:

```
ASMCLI -smart -component="MyMailboxDatabase"
-shadowType=Transportable -backupType=copy -snapshotType=Snapshot
-keepCount=14-checksum- -recovery -offpeak
```

9. Create a clone of a volume specifying the LocationRoot parameter:

```
ASMCLI -smart -email -objectid="Psv{18a09060-1d50-f672-69fb-
d412bc01209b;1048576}" -comment=clone of kvol1--@ -
shadowtype=transportable
-backuptype=Copy -smartcopytype=Clone
-locationroot="C:\ProgramData\EqualLogic\Mounts\"
```

ASMCLI -unmount

Specify the `-unmount` subcommand to unmount and log off a volume.

Use optional parameters to unmount multiple volumes and control the selection of volumes, and the Smart Copy version. You can optionally delete the Smart Copy on successful completion of the operation.

On a cluster, this command fails if:

- The target is the cluster quorum disk
- The target is a physical disk resource that has not been placed in maintenance mode
- The target is a physical disk resource that is not owned by this node

Command Syntax

```
ASMCLI -unmount [{-document="path" | -volume={"drive_letter" |"mount_point"} |
-component="component_name" | -collection="collection_name" |
-writer="writer_name" | -objectID="identifier"}]
-location="[drive_letterA;drive_letterB;... | mount_point;;...]"}|
-ignorelogoutfail [{-useLatest | -useEarliest}] [-email | -noemail]
-retry=n -deletesnap -unmountonly
```

For a description of these parameters, see *Command Parameters on page 153*.

Examples

1. Unmount all of the volumes mounted from backup document named `e2b3-f1a3-234.bcd`:

   ```
   ASMCLI -unmount -document="PSV
   {18A09060- 3BE0-3FA8-0A7A-E4120000E045;32256}\
   e2b3-f1a3-234.bcd"
   ```

2. Unmount the volume mounted from backup document `e2b3-f1a3-234.bcd`. The location of the mount point is `D:\TestServer`:

   ```
   ASMCLI -unmount -location="D:\TestServer"
   ```

3. Unmount the volume from the Smart Copy backup document `e2b3-f1a3-234.bcd` that was mounted at drive E:

   ```
   ASMCLI -unmount -location=E:\
   ```

4. Unmount the most recent Smart Copy backup document available for `F:\` from its current mount point:

   ```
   ASMCLI -unmount -volume=F:\ -useLatest
   ```

5. Unmount the oldest Smart Copy backup document available for the Exchange Mailbox Database named *Mailbox4Database* from its current mount point:

```
ASMCLI -unmount -component="Mailbox4Database" -useEarliest
```

ASMCLI -verify

The `-verify` subcommand is used with Microsoft Exchange Smart Copies. It can be used as follows:

- Using the `-checksum` parameter to verify an existing backup document. When you use this command, no new Smart Copies are created.
- Using the `-recovery` parameter to verify and soft recover from existing backup document. When you use this command, no new Smart Copies are created.
- Using both the `-checksum` and the `-recovery` parameters.

Use optional parameters to control the selection of backup documents, the version, and the location for Checksum Verification and Soft Recovery.

Command Syntax

```
ASMCLI -verify [{-document="path" | volume={"drive_letter" | "mount_point"} |
-collection={"collection_name" | -component="component_name"}]
[{-checksum | -recovery}] -offpeak | -remote -ignorelogoutfail
-email | -noemail [{-useLatest | -useEarliest}]
```

The `email` parameter is set by default. For a description of these parameters, see *Command Parameters on page 153*.

Examples

1. Run a Checksum Verification on the backup document named `a6d7-e5f8-124.bcd`:

```
ASMCLI -verify -document="C:\BackupDocs\Shadows\
Psv{18a09060-3be0-3fa8-0a7a-e4120000e045;32256}a6d7-e5f8-124.bcd" -checksum
```

2. Schedule a Checksum Verification on the backup document `a6d7-e5f8-124.bcd` during offpeak Global Verification times:

```
ASMCLI -verify -document="C:\BackupDocs\Shadows\
Psv{18a09060-3be0-3fa8-0a7a-e4120000e045;32256}a6d7-e5f8-124.bcd"
-checksum -offpeak
```

3. Schedule a Checksum Verification on the most recent Smart Copy backup document available for volume `F:\`, during the off peak Global Verification times:

```
ASMCLI -verify -volume=F:\ -useLatest -checksum -offpeak
```

4. Schedule a Checksum Verification on the oldest Smart Copy backup document available for the Exchange Mailbox Database named `EXMailboxDatabase`. The operation is scheduled to run during the offpeak Global Verification times:

```
ASMCLI -verify -component="EXMailboxDatabase" -useEarliest -checksum -offpeak
```

5. Run a Soft Recovery on the backup document `e2b3-f1a3-234.bcd`:

```
ASMCLI -verify -document=
"C:\BackupDocs\Shadows\PSV{18A09060-3BE0-3FA8-0A7A-E4120000E045;32256}\
e2b3-f1a3-234.bcd" -recovery
```

6. Schedule a Soft Recovery on the backup document named `e2b3-f1a3-234.bcd`. The document is located on a remote computer:

```
ASMCLI -verify -document="C:\BackupDocs\Shadows\PSV{18A09060\
3BE0-3FA8-0A7A-E4120000E045;32256}\e2b3-f1a3-234.bcd" -recovery -remote"
```

7. Run a Soft Recovery on the most recently created backup document for the Exchange Mailbox Database named *MyMailboxDatabase*:

```
ASMCLI -verify -component="MyMailboxDatabase" -recovery -useLatest
```

ASMCLI -version

The `-version` command displays the ASM/ME version that you are running, as well as the build date.

Command Syntax

```
ASMCLI -version
```

This command will display the version number and build date; for example:

```
Version=4.0.2000.6261
Build Date=4/26/2012 12:58:34 AM
```

Use a Script to Create Smart Copies

If you use scripts for running backups or performing other background operations, you can also schedule Smart Copy creation by adding an ASMCLI command to your existing script.

Prepare to Create the Script Commands

Prepare to create the script as follows:

- Review the information in *About Schedules on page 61* for more information.

- Optionally, configure email notification to alert you if scheduled Smart Copy operations fail. See *Configure Notification Settings on page 22*.
- Review the available commands described in *ASMCLI Commands and Their Syntax on page 166* and decide which ones you want to use in your script.

Create the Script Commands

Note: Although the examples in this section use asmcli examples, Dell recommends you use the ASM PowerShell cmdlets instead to perform the functions discussed in this section. For more information about PowerShell cmdlets, see the *Dell EqualLogic PowerShell Tools Reference Guide*.

1. Use the procedure described in *Create a Schedule for Smart Copies on page 62* to create a temporary Smart Copy schedule. This schedule is your template and should include all the attributes you want to use in your script.
2. Click the newly-created schedule to display its properties.
3. Select the `Arguments` property. This line contains the command line to run the schedule, and identifies the schedule ID.
4. Right-click the field and select `Copy`.
5. Paste the command into a text editor, such as Notepad. Table 38 shows an example of a command that you can copy and paste when you right-click the Arguments property.

Table 38: Command Example for the Arguments Property

Property	Value
Arguments	-scheduleID="c5542376-f55a-489a-93f4-2580dc74f6ac" -objectid="Component{25d980e3-ca4c-4177-9846-7844f708d97d}" -comment=backup scheduleCLI-@ -shadowtype=Transportable -backuptype=copy -snapshottype=Snapshot -keepcount=10 -hide -checksum -recovery -offpeak

6. Delete the following words: *Property*, *Value*, and *Arguments*.
7. Add the full ASMCLI command path to the beginning of the text, making sure it precedes the pasted text. By default, this path is in the folder where you installed the Host Integration Tools kit as follows:

   ```
   C:\Program Files\EqualLogic\bin\ASMCLI.exe
   ```

8. Change the values for the following parameters if required:
   - `-backupType`, which is either `full` or `copy`.
   - `-snapshotType`, which is either `Snapshot` or `Replica`.
   - `-keepCount`, which is an integer in the range 0-99 indicating the maximum number of Smart Copy backup documents retained at any one time. (A default value of 8 backup documents is assumed.)

     You must specify the `-scheduleID=` parameter when specifying `-keepcount=`, otherwise the keep count limit is not maintained and Smart Copies are created until there is insufficient space. Specify a unique schedule identifier, using an `8-4-4-4-12` hexadecimal format. For example:

```
-scheduleID="00000000-1111-2222-3333-000000000000"
```

9. Test the command before executing it in a production environment as follows:
   - Open a command prompt and paste the command.
   - Identify and correct any typographical errors or incorrect ID values.
   - Verify that you receive e-mail notification during this test. (If configured).
   - Check the ASM/ME GUI to verify that a Smart Copy Set was created.
10. Merge the command line into your existing script.
11. Delete the temporary schedule you created in ASM/ME by right-clicking the schedule name (under the Schedule node in the Tree Panel) and selecting `Delete Schedule`. If you do not delete the temporary schedule, it will run as specified, potentially interfering with your scripted scheduler and creating unexpected Smart Copy Sets.
12. Repeat steps 1-11 to add more scheduled Smart Copy operations to your backup script.

Appendix A Recover Clustered Volume From a Clone

If a volume is lost or damaged, and no snapshot is available from which to restore it, a clone of the volume can be mounted in its place, which will effectively restore it. If the volume is a cluster resource, however, this operation is complicated by the Cluster Manager, which will not recognize the clone as being identical to the original volume. Use the following procedure to replace a volume that is a cluster resource with a clone.

1. In Windows Cluster Administrator, set the disk offline.
2. In Cluster Manager, do the following:

Remove the disk from the application group.

   a. Unmount the disk from its mount point. You can use the `mountvol` utility, which is part of the Windows operating system.

   b. Delete the disk from the cluster.

3. Using the Microsoft iSCSI Initiator, log out of the original disk from each node.
4. In the Group Manager, do the following:
   a. Set the volume offline or delete it.
   b. Set the clone online.
5. Using the Microsoft iSCSI Initiator, log in to the clone from each cluster node.
6. In Cluster Manager, do the following:
   a. Add the clone to the cluster.
   b. Re-create the mount point (if needed).
   c. Add the clone to the application group.
   d. Re-create the application dependencies.
   e. Bring the application online.

Index

S

T

U

V

W