Dell EqualLogic Host Integration Tools for Microsoft

Release Notes Version 4.8

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

2015 - 06

Rev. 110-6218-EN-R1

Contents

1

Introduction to HIT Microsoft

This document contains important product information and restrictions for the Dell EqualLogic Host Integration Tools for Microsoft version 4.8.0 software kit.

Host Integration Tools includes the user-selectable components described in Table 1. Host Integration Tools Components.

Table 1. Host Integration Tools Components

Component	Description
Remote Setup Wizard (RSW)	Initializes a PS Series storage array
Remote Setup Command Line Interface (RSWCLI)	Provides a command-line alternative to the Remote Setup Wizard. Also enables you to configure multipath I/O settings and configure access to a PS Series group.
Multipath I/O device-specific module (MPIO/DSM)	Supports redundant network paths between a computer and the PS Series group for high availability and high performance
Auto-Snapshot Manager/Microsoft Edition (ASM/ME)	Creates and manages Smart Copies (snapshots, clones, and replicas of PS Series iSCSI volumes). Use the alternate command-line interface, ASMCLI, for custom operations and scripting.
VSS Provider	Used by Volume Shadow Copy Service (VSS) to manage application-consistent Smart Copies
Virtual Disk Service Provider (VDS)	Used by VDS version 1.1 and Storage Manager for SANs to create and manage volumes in a group
Storage Management Provider (SMP)	Manages storage groups on Windows 8 or later operating systems and Windows Server 2012 or later operating systems
PowerShell Tools	Manages one or many PS Series groups through a comprehensive set of PowerShell Tool cmdlets

Features Supported in This Release (HIT/Microsoft Version 4.8.0)

The following features are supported in HIT/Microsoft version 4.8.0:

- PS Series firmware v8.0 and backward compatibility with PS Series firmware v6.0 and v7.0

- PS 4210, PS 6510, and PS 6610 arrays
- SQL Server 2012 SP2 CU4, SQL Server 2014 (CSV support), and SQL Server 2014 CU6
- System Center Virtual Machine Manager (SCVMM)
- Hyper-V
- Cluster Shared Volumes as part of a Hyper-V cluster
- Cluster Shared Volumes as part of an SQL cluster
- Exchange Server 2013 CU7 and Exchange Server 2010 SP3 – RU8 V2
- SharePoint 2013 SP1 and SharePoint 2010 SP2 or later
- Windows Client 8.1, with continued support for Windows 8, and Windows 7 SP1
- Windows Server 2012 and Windows Server 2012 R2

Features Not Supported in This Release (HIT/Microsoft Version 4.8.0)

The following features are not supported in HIT/Microsoft version 4.8.0:

- Cluster Shared Volumes with more than one application component (for example, Hyper-V and SQL)
- Cluster Shared Volumes without an application component
- Hyper-V Cluster Smart Copies of Cluster Shared Volumes without an application component
- SQL 2014 databases with Windows Azure Storage
- SQL 2014 databases with AlwaysOn Availability Group

Features Supported in Previous Releases (HIT/Microsoft Version 4.7.1 and 4.7.0)

The following features are supported in HIT/Microsoft version 4.7.1 and 4.7.0:

- Memory Optimized Tables (In-Memory OLTP)
- SQL database configurations supported by HIT/Microsoft 4.7.0, including:
  - SQL databases on EqualLogic storage on standalone servers
  - SQL databases on EqualLogic storage on standard cluster volumes
- PS Series firmware v7.0 support: 4K-byte sector drives, access groups
- Windows Server 2012 R2 and Windows 8.1
- Exchange 2013 CU2 and Exchange Server 2010 SP3 – RU8 V2
- System Center Virtual Machine Manager (SCVMM, or VMM) 2012 R2 with the Dell EqualLogic Storage Management Provider (SMP) for PS Series arrays
- Auto-grouping multiple hosts (SharePoint farms, clusters, hosts) and the ability to assign aliases to SharePoint farms, clusters, or hosts.

  For more information about these features, see the *Dell EqualLogic Auto-Snapshot Manager/ Microsoft Edition User's Guide*.

- PowerShell cmdlets for ASMCLI and RSWCLI. These cmdlets offer access to ASM, RSW, and MPIO settings functionality through PowerShell. The corresponding PowerShell module for each feature is installed when you install that feature.

  For more information about the cmdlets, see the *Dell EqualLogic PowerShell Tools Reference Guide*.

Minimum Required Firmware and Software Revisions

Table 2. Minimum Software and Firmware Revisions lists the minimum revisions of application software and firmware supported by Host Integration Tools. You cannot use an unsupported instance of an application (such as SQL) on the same computer as a supported instance. Doing so might cause Host Integration Tools to operate incorrectly. Host Integration Tools support only the Host Bus Adapters (HBAs) specified in Table 2. Minimum Software and Firmware Revisions.

NOTE: During installation, the Host Integration Tools kit disables the MPIO Path Verification for devices claimed by the Dell EqualLogic MPIO DSM. This step prevents a potential problem that could introduce a delay in reconnecting to iSCSI volumes during a Dell EqualLogic PS Series firmware upgrade or controller failover.

Table 2. Minimum Software and Firmware Revisions

Product	Revision
PS Series firmware	For all operating systems, use PS Series firmware version 6.0.x or later
PowerShell Tools	Windows PowerShell Tools version 2.0, 3.0, and 4.0 are supported
SharePoint	• SharePoint 2010 SP2 or later • SharePoint 2013 SP1
Exchange Server	• Exchange Server 2010 SP3 – RU8 V2 or later • Exchange Server 2013 CU7
Virtual Disk Service (VDS)	Version 1.1
SQL Server (SQL Express is unsupported)	• SQL Server 2012 SP2 CU4 • SQL Server 2014 CSV support — All SQL configurations supported by HIT/Microsoft 4.7.1 are supported in this release, as well as Memory Optimized Tables. • SQL Server 2014 CU6
Hyper-V	• Windows Server 2012 • Windows Server 2012 R2
System Center Virtual Machine Manager (SCVMM)	• SCVMM 2012 R2 • SCVMM 2012 SP1 GA with UR1 (Build 3.1.6018.0), with • VDS fix (see http://support.microsoft.com/kb/2785094), and DSM running on all systems
QLogic QLA405x and QLE406x iSCSI initiator HBAs	• Firmware 3.0.1.49 and BIOS 1.14 with Windows driver 2.1.4.26

Product	Revision
	• On the QLogic driver downloads page, follow the link specific for Dell EqualLogic models
Broadcom NetXtreme II iSCSI initiator HBA	Version 12.8 driver suite

Supported Versions of the Windows Operating System

Table 3. Windows Desktop Operating System Support and Table 4. Windows Server Support list supported versions of the Windows operating system and identify Host Integration Tools components that do not support specific operating system versions. Host Integration Tools do not support evaluation versions of Windows or any version not listed in Table 3. Windows Desktop Operating System Support and Table 4. Windows Server Support.

NOTE: Host Integration Tools support both 32-bit and 64-bit versions of the Windows operating system. However, the tools do not support the IA-64 (Intel Itanium architecture) versions of the Windows operating system.

See also General Operating Constraints .

Table 3. Windows Desktop Operating System Support

Component	Windows 7 SP1	Windows 8	Windows 8.1
RSW	Yes	Yes	Yes
Remote Setup CLI	Yes	Yes	Yes
MPIO/DSM	No	No	No
ASM/ME	No	No	No
VSS Provider	No	No	No
VDS Provider	No	No	No
Powershell tools	Yes	Yes	Yes
Storage Management Provider (SMP)	No	Yes	Yes
Rethinning driver	No	No	No

Table 4. Windows Server Support

Component	Server 2012	Server 2012 R2
RSW	Yes	Yes
Remote Setup CLI	Yes	Yes
MPIO/DSM	Yes	Yes
ASM/ME	Yes	Yes

Component	Server 2012	Server 2012 R2
VSS Provider	Yes	Yes
VDS Provider	Yes	Yes
PowerShell tools	Yes	Yes
Storage Management Provider (SMP)	Yes	Yes
Rethinning driver	No	No

iSCSI Initiator

The iSCSI initiator is a required component.

Network Requirements and Recommendations

To ensure a secure network environment, Dell strongly recommends the following best practices:

- The network environment in which the group resides, including hardware such as switches and routers, should be secure from network attacks such as packet sniffing or connection hijacking. Firewalls and network isolation should be employed to protect resources.

  Network security can be achieved in a number of ways depending on the level of assurance needed and the types of network attacks to be expected. Security mechanisms include physical security, application-level encryption (SSL/TLS and SSH), and/or IP-level encryption (IPsec).
- Network protocols and services used by the group, including RADIUS authentication, Network Time Protocol (NTP), syslog, and outbound SMTP traffic, should be secure and not subject to attacks.

2

Issues Corrected in Host Integration Tools for Microsoft

The following issues are fixed in HIT/Microsoft version 4.8.0.

Installation

- The installer's Change/Repair option is limited to users with Administrator privileges using **setup.exe**.
- The Change/Repair option has been removed from the Programs and Features Control panel.

Auto-Snapshot Manager (ASM)

- You can clone SharePoint replicas.
- The partially created Smart Copy object that displayed in the ASM GUI tree each time PowerShell was used to create a SharePoint Farm Smart Copy no longer appears.
- ASM no longer has an indefinite wait period if the Exchange verifier fails to do a Checksum and Recovery Verification for a Smart Copy.
- All new ASM schedules now begin with the status: `Never Run`.
- All ASM schedule updates are correctly reported in the ASM Schedule Dashboard.

MPIO

- The small volumes located on a multimember EqualLogic array now have at least two iSCSI connections during an iSCSI offload engine mode that was configured in Broadcom 578XX for the Dell EqualLogic Multipath I/O DSM.
- The ASM installation status now displays in the panel of the iSCSI Initiator Properties tab.

PowerShell

- **SnapshotReservePercent** is a new switch added to the **New-EQLReplicaClone** command that lets you specify the snapshot reserve value.
- The **SPCategory** switch used with the **New-ASMSmartCopy** command to create SharePoint Smart Copies is fixed.
- You can now delete iSCSI persistant reservations for a specified group with the **Remove-EqlGroup Access** command.

- The **Get-EqlSchedule** can now iterate through a connected group of schedules in search of a specific schedule name. In previous releases, running this command would display all of the schedule names within the connected group of schedules.
- A clone-type Smart Copy created from a Replica using the **Invoke-CloneReplicaASM** Smart Copy command can also be used to create a new Exchange database using the Clone and Restore as New GUI option.

Miscellaneous

The SCVMM provider issue that occurred when a virtual machine was created from a template volume using the Clone Logical Units feature is fixed.

3

Usage Constraints

This section describes the usage constraints in Microsoft/HIT Version 4.8.0.

Windows Server 2012 or Later and Windows 8 or Later Constraints

This section describes usage constraints that are specific to Windows Server 2012 or later and Windows 8 or later operating systems.

Incorrect Report of a Device as In Use

Windows Server 2012 might incorrectly notify you that a device is in use when you try to log out from an iSCSI target. This issue can occur even though no application is using files on any volume associated with the iSCSI target.

Consequently, the relevant task wizards in Auto-Snapshot Manager (or ASMCLI commands) such as **Unmount**, **Logoff**, or **Delete** might display a `Volume in use` error.

If you encounter this problem and you are certain that no application is using the volume, you can select the Ignore option in Auto-Snapshot Manager or you can proceed by setting the disk offline on Windows Server 2012 by using the following procedure as a workaround.

NOTE: Following this procedure (using either the ASM/ME GUI or the ASMCLI) when one or more files are in use might result in data loss or corruption.

1. Identify the correct iSCSI target.
2. Launch the command prompt by clicking **Start** → **Run**, then type `cmd`.
3. Enter **diskpart** at the Windows command prompt to display the `DISKPART>` prompt.
4. Enter **list volume** to list all volumes known to Windows.
5. Examine the column headed `Volume ###` and identify the volume (or volumes) associated with the iSCSI target.
6. Enter **select volume *volume_name***, where *volume_name* is the volume that you identified in the previous step.
7. Enter **offline disk** to set the physical disk for the volume offline.
8. Enter **exit** to close the diskpart menu.
9. Enter **exit** to close the command window.

   After setting the disk offline, you can successfully log out from the iSCSI target using the iSCSI initiator GUI or CLI.

Unsupported PowerShell Cmdlets for Windows 8 or Later or Windows Server 2012 or Later

The Storage Management Provider (SMP) does not support the following PowerShell cmdlets in Windows Server 2012 or later and Windows 8 or later:

- New-StoragePool
- Remove-StoragePool
- Add-PhysicalDisk
- Add-VirtualDiskToMaskingSet
- Rename-MaskingSet
- Repair-VirtualDisk
- Set-PhysicalDisk
- Set-ResiliencySetting
- Reset-PhysicalDisk
- Remove-InitiatorId

Must Install HIT on Each VM in a Windows Server Configuration

In a Windows Server configuration using Cluster Shared Volumes, the Host Integration Tools must be installed on each VM. Installing the tools that ensures that Smart Copies of VMs will work correctly in all configurations, including Enterprise, Datacenter, Core, or any other Windows Server release configuration.

The requirement applies whether you start the Smart Copy operation or create a schedule from the VM or the Volume node in the ASM/ME GUI.

If the Host Integration Tools are not installed on each VM, you can create a Smart Copy but an error is displayed stating that ASM/ME could not open a connection to the VM. The Smart Copy will not be file-system consistent, but are crash consistent with respect to the file system in the VM. You might have to run the chkdsk utility the next time the VM restarts.

Cluster Shared Volume VSS Writer Fails to Report Remote VMs

Under some circumstances the Cluster Shared Volume (CSV) VSS Writer in Windows Server 2012 does not report remote VMs. This omission results in remote VMs not being included in Smart Copies of Cluster Shared Volumes.

The cause of the problem is multiple requestors querying the components at the same time. You might be able to avoid this issue by:

- Closing the ASM/ME GUI windows when they are not in use
- Not allowing the Smart Copy schedules to overlap

Operation Constraints

The following operational constraints apply in this release for all supported operating systems.

VSS Does Not Allow Backup and Restore Operations on tempdb

Each time the SQL Server is started, a clean copy of the system database: **tempdb** is recreated. This database minimally logs operations such as temporary tables and stored procedures. This logging enables transactions to be rolled back.

The VSS does not allow backup and restore operations to work on the **tempdb**. After the current SQL Server session disconnects, and no other connections are active at system shutdown, the temporary tables and stored procedures are automatically dropped from the database. Because no type of data is permanently stored in **tempdb** from one SQL Server session to another, the database does not need to be saved.

For more information about the **tempdb** system database, see the Microsoft Knowledge Base article at msdn.microsoft.com/en-IN/library/ms190768.aspx.

VMM — Selective Restore of a Rapid Provisioned HA VM Smart Copy Fails With Error

You cannot perform a selective restore operation on VM components that are on volumes without mount points. The selective restore operation uses file copy operations which requires the volume to have a mount point.

The files are in **\\?\{GUID}** format.

Smart Copy is Disabled for Cluster Shared Volumes

The Smart Copy feature is disabled for Cluster Shared Volumes when:

- Components for Hyper-V writer and SQL writer components are on the same CSV.
- SQL components are on the same CSV, but no SQL instance is owned by the current node.

Networking Constraints

This section contains information about network and firewall configuration, and general networking constraints.

Using the HPC Server with Broadcom Ethernet NICs

When setting up systems equipped with Broadcom Ethernet NICs to be used as HPC base or compute nodes with iSCSI storage, you might find that the Broadcom card does not accept the IQN string set for it

by the HPC server. This failure will cause login failures when the node attempts to boot from its iSCSI volume, because the HPC head node configures the iSCSI boot volumes with IQN-based ACLs.

Two methods resolve this problem. The preferred method involves changing a BIOS setting on the Broadcom card and using a template string in the HPC settings when you configure the node template.

To use this method:

1. To start the **HPC iSCSI Settings App** from the **Start Menu** , click **Start → All Programs → EqualLogic → HPC iSCSI Provider Settings**.
2. Click **Create new volumes with open ACLs**.
   This option allows any initiator to log in to the volume.

Windows Firewall Settings on Failover Cluster

If you are using the native Windows firewall on your failover cluster and you want to use the Dell EqualLogic Multipath I/O DSM, you must configure your firewall to allow ICMP echo requests (pings) for ICMPv4 and ICMPv6. The installation procedure detects the firewall and gives you the option to amend your firewall configuration automatically.

If you do not select this option at installation time, and you want to use multipathing, you must configure your firewall manually to allow ICMP requests. The following command-line examples show typical exception rules:

```
netsh advfirewall firewall add rule name="Dell EqualLogic MPIO Ping IPv4" dir=in
action=allow description="Dell EqualLogic MultiPath I/O Ping rule" enable=yes
profile=any localip=any remoteip=any protocol=icmpv4

netsh advfirewall firewall add rule name="Dell EqualLogic MPIO Ping IPv6" dir=in
action=allow description="Dell EqualLogic MultiPath I/O Ping rule" enable=yes
profile=any localip=any remoteip=any protocol=icmpv6
```

Firewall Must Allow ICMP

If you are using the native Windows firewall on your computer and you want to use the Dell EqualLogic Multipath I/O DSM, you must configure your firewall to allow ICMP echo requests (pings).

Use the iSCSI Initiator Properties Page Extension to verify that Multipath I/O is working correctly. If not, configure the firewall manually to allow ICMP echo requests.

See the documentation for your version of the Windows operating system for instructions on how to configure a firewall.

Network Folder Repository for Smart Copy Backup Documents

When you run ASM/ME on a Windows failover cluster, you must specify a shared network folder as a repository for the Smart Copy backup documents. Each node in the cluster must be able to access the folder. In addition, if you are sharing a PS Series group between several failover clusters, each cluster

must have its own shared network folder. You cannot use a single shared network folder between multiple clusters for storing backup documents.

iSCSI Initiator Constraints

This section contains general constraints pertaining to the iSCSI initiator. Any constraints that are related to multipathing are listed in Multipath I/O DSMGUID-CFD57B6F-6435-44BC-8DAA-D7C32CEF8B7C.

iSCSI Initiator Connection Failure

This problem might occur when connecting to a PS Series group.

Under rare conditions, the iSCSI Software Initiator might not correctly connect to storage devices, including PS Series volumes and the vss-control volume, which Microsoft services use to communicate with a PS Series group. Although the login to the volume appears to succeed, the connection is not established.

For example, the iSCSI initiator console will not show any device details for the target, and the volume will not appear in the Windows Disk Management utility.

The iSCSI initiator will automatically attempt to correct the problem. However, if the problem persists, you might be able to correct it as follows:

1. Double-click the **iSCSI initiator** icon to open its properties and click the **Targets** tab.
2. Log out of the affected iSCSI target.
3. From the **Discovery** tab, remove the group IP address from the list of target portals.
4. Enter the group IP address that you removed from the list of target portals in step 3 as a target portal, then start a new discovery session to this address.
5. Log in to the volumes.

   You might need to click **Advanced** to specify host bus adapter information or CHAP login credentials.

   If you are unable to correct the iSCSI connection failure, try the following steps:
6. Reboot the computer.
7. Use the **Windows Device Manager** and look for devices that appear to be having problems.

   For those devices, reinstall the existing driver (use the default response `no` at the prompts) and then reboot the server.

Windows OS Error When iSCSI Session Limit Reached

A maximum limit of 255 iSCSI sessions is permitted by the Windows operating system. When you reach this limit, the operating system generates the following iSCSI error:

```
SDSC_TOO_MANY_SESSIONS: Unspecified Error 0xefff001e
```

Connecting a Host With HBAs to a PS Series Group on a Dedicated Network

If your host system uses HBAs on a dedicated network to access your PS Series groups, configure ASM/ME to register the discovery address using only these HBAs. In the ASM/ME GUI, click **Settings → PS Group Access**. Select the checkbox for **Use Host Bus Adapters** when you configure the PS Series group access. This checkbox is displayed only if the HIT host has HBAs installed, or an initiator other than the default software initiator.

If a HIT host has HBAs and default network interfaces, and if the iSCSI traffic is restricted to only the HBA network interfaces, and you select the checkbox to verify the connection to the group, you might see the following error:

```
Error saving PS Group group_name: Specified group WKAddress is not reachable.
```

If the **Verify connection** checkbox is not selected, ASM will add the new group entry but subsequent attempts to edit it will fail. With the **Use Host Bus Adapters** option set, if the ping test fails, ASM will ignore the failure and attempt to register the new PS Series group. If one HBA succeeds, the group is added.

General Operating Constraints

The following operational constraints apply in this release for all supported operating systems.

Remote Verification

- To perform remote verification for clones, the remote verification server must have access to the corresponding volume.
- To perform remote verification for replicas, the remote verification server must have access to the replication partner group. The remote server should not have any access to the source volumes. If the remote server accesses the original volume, data corruption can occur.

Failover and Failback

HIT does not support failover or failback operations using replicas. For information about supported failover or failback operations on PS Series groups, see the *Dell EqualLogic Group Manager Administrator's Guide*.

Dynamic Disks

Dynamic disks are not supported.

Disks Offline After a Reboot

Under certain circumstances, disks containing iSCSI SAN volumes (located on your PS Series array) might appear as offline after you reboot your computer. Use Windows Disk Manager to set the disks online. If the offline disks are associated with applications, you might also need to restart any associated application services.

Use the following procedure to set the disks online:

1. Open **Server Manager** in **Windows 2012**.
2. Expand the **Storage** object and open **Disk Management**.
3. Look for disks marked as **Offline**.
4. Right-click the offline disks, then select **Reactivate Disk**.
5. (Optional) Assign a drive letter to each disk.
6. (Optional) Restart any application services associated with the disks.

Local Language Support

None of the components are available as local-language variants. You can install and use the English versions under localized variants of supported Windows operating system versions. You might not be able to enter local-language character set glyphs under certain circumstances, such as:

- CHAP user names and passwords
- PS Series group names, member names, administrative passwords, and group membership passwords.

  For example, Japanese glyphs have a known issue documented at support.microsoft.com/kb/946482.

Application Issues and Constraints

This section describes issues and workarounds for the applications supported by the Host Integration Tools.

Exchange Server Constraints

The following constraints apply when using Host Integration Tools with Exchange Server:

- When you use ASM/ME to create Smart Copies of Exchange storage groups, the transaction logs are not truncated. See the Exchange documentation for information about how to truncate transaction logs.
- For Exchange volumes, you can only create Smart Copies of type copy.

Remote Host Settings for Exchange Replica Smart Copy Verification

One of the options to verify a replica Smart Copy of an Exchange component is to promote the replica set to a recovery volume and perform verification. To use this option, the remote host only needs access to the replication partner group. The remote host should not have any access to the source volumes. If the remote host accesses the original volume, data corruption can occur.

Remote Host Settings for Verifying Snapshots and Clones

To verify snapshots and clones on the remote host, the remote host must have access to the corresponding volumes.

Exchange Replica Smart Copies Might Require Manual Soft Recovery

Verification and soft recovery of Exchange replica Smart Copies are performed on the replication partner. Verification consists of two steps: the actual verification, and the "soft recovery," where the database is brought from a "dirty shutdown" state to a "clean shutdown" state. Soft recovery requires read-write access to the database. In the case of replica Smart Copies, this process requires some additional planning.

You can give read-write access to the Smart Copy in the following ways:

- Promote the replica set to a recovery volume
- Clone the replica, which creates a new volume

A promoted replica will remain promoted only while verification is running. As soon as verification completes, the replica is demoted again, and replication can resume. However, any changes made to the replica during the soft recovery phase of replication are discarded when the replica is demoted, because replication for any given volume is one way, no mechanism is available for replicating changes made on the replication partner back to the original volume.

If you want to mount a replica Smart Copy of an Exchange database on your Exchange server (for example, during a Restore as New operation in ASM/ME), you must manually run soft recovery on that Smart Copy first, even though soft recovery was run during the verification process. You can perform a manual soft recovery by using the Exchange Eseutil utility.

This restriction applies only to replica Smart Copies. Snapshots and clones do not require this extra step. This issue will be addressed in a future release of ASM/ME.

Exchange Replication Fails After Uninstalling HIT Kit

If you are uninstalling the version 4.5.0, 4.5.1, 4.6.0, or 4.7.0 Host Integration Tools kits on a host that has Exchange servers configured and performing replication (using DAGs), the replications can fail due to an issue with the trim driver. The driver is not updated correctly while open handles to the PS Series group volumes are involved in the replication.

To avoid this issue, suspend all Exchange replication before upgrading or installing the Host Integration Tools kit.

SQL Server Constraints

Host Integration Tools support online backup and quick restore of SQL Server databases using the Auto-Snapshot Manager GUI. See Minimum Required Firmware and Software Revisions for supported versions of SQL Server.

The following constraints apply when using Host Integration Tools with SQL Server:

- Auto-Snapshot Manager does not support SQL Server database object recovery (such as recovering table data). This recovery is available only by using the **Restore as New Database** option, and by other manual tasks.
- You cannot use Auto-Snapshot Manager to create Smart Copies of multiple databases that span iSCSI volumes. This procedure might result in torn Smart Copies of any database not selected for the Smart Copy operation. Dell recommends that you create a collection that includes all the database volumes to avoid torn Smart Copies.

- Selective restoration of databases sharing similar PS Series volumes might take a long time. The file system's copy operation replaces only the selected database files.
- If you select the **Apply log** option for a single database in a database collection, all the databases remain in a restoring state when the Auto-Snapshot Manager restore process completes.

Separate the System Databases from the User Databases

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 system databases while restoring user content.

SQL Server 2012 Requires Cumulative Update Package 1

If you are using SQL Server 2012, apply the Cumulative Update Package 1.

See the following Knowledge Base article for more information: support.microsoft.com/kb/2679368

Hyper-V Constraints

The following constraints apply to using Host Integration Tools with Hyper-V.

Additional constraints specific to ASM/ME are listed in the *Dell EqualLogic Auto-Snapshot Manager/ Microsoft Edition User's Guide*. It is important that you read the User's Guide in addition to these Release Notes before you attempt any operations using Hyper-V.

VMM — Volumes Not Logged Out as Expected

When performing a VMM storage management operation that requires the initiator to log out of the volume (such as deleting a volume), sometimes the VMM agent fails to log out (or takes an unusually long time to log out), and the operation fails or times out. A volume cannot be deleted if any connections are still open. VMM does not remove the target for this volume from the list of persistent (favorite) targets and the initiator continues trying to log back in to the volume even after the system is rebooted.

You might also see this issue when performing other operations such as unregistering a volume (LUN), deleting a VM, and rapid VM migration tasks. These operations can result in error messages such as:

```
The session cannot be logged off because a device on that session is currently
being used. (ISDSC_DEVICE_BUSY_ON_SESSION).
```

When VMM storage management scenarios involve multiple volumes, manually logging out of each one is time consuming. To script this operation for many volumes at once, you can use Windows 8 iSCSI cmdlets (`Get-iSCSISession, Unregister-iSCSISession, Disconnect-iSCSITarget`) or Dell EqualLogic PowerShell Tools cmdlets (**Get-EqlVolume**, **Set-EqlVolume**, **Get-EqlVolumeConnection**).

Restoring a Smart Copy of a Hyper-V VM that has a Hyper-V Snapshot

Consider the following scenario:

1. You have Hyper-V running with one or more VMs. A **.vhd** file exists for each VM.

2. You create a Hyper-V snapshot of a VM. A new **.avhd** file is created.
3. You update the VM (for example, to install programs or add files.) The **.avhd** file is updated.
4. You create a snapshot Smart Copy of the VM component.
5. You run a Restore as New operation from the Smart Copy.

The Restore as New operation creates a new VM using the static **.vhd** file from step 1. The interim changes you made to the VM, which are reflected in the **.avhd** files, are not contained in this file.

A workaround for this issue is available at the following URL:

social.technet.microsoft.com/wiki/contents/articles/6257.manually-merge-avhd-to-vhd-in-hyper-v.aspx.

When creating Smart Copies of a running virtual machine, the PlugPlayManager service might log errors to the Windows event log. You can ignore these errors. See the Knowledge Base article at: support.microsoft.com/kb/958669/en-us.

Hyper-V VSS Writer Errors Resulting in a Hang or Crash

When creating Smart Copies on the active node for the first time, certain volume configurations might cause the Hyper-V VSS Writer to stop functioning with the following error messages:

```
Failed to revert to VSS snapshot on one or more virtual hard disks of the
virtual machine '%1'. (Virtual machine ID %2)

Failed to create the backup of virtual machine '[removed]' (Virtual machine ID
CCF1C842-566A-446A-96CF-22FDE3744205)

Cannot find the specified snapshot. (Snapshot ID
B09DFE8A-2417-4630-89B9-10424ED2C1FA)

An unhandled exception was encountered while processing a VSS writer event
callback. The VSS writer infrastructure is in an unstable state. The writer
hosting process must be restarted in order to resume VSS functionality.
```

The first error message indicates that the Hyper-V VSS Writer cannot find a required snapshot. The second error message informs you that the Hyper-V VSS Writer is no longer functioning and you must restart it.

The likely cause is that the virtual machine contains multiple volumes configured in the guest but the volumes that are targets of the Smart Copy operation do not contain their shadowstorage area. For the Smart Copy operation to be successful, the shadowstorage area must be located on the target volume.

To correct the problem, run the vssadmin utility within the Guest OS (not the server) to configure the shadowstorage of each volume, locating it in the same volume. This one-time operation resolves the problem for all future Smart Copy operations:

1. Open the Windows command prompt.
2. Enter the following command:

```
vssadmin Add ShadowStorage /For=N: /On=N:
```

where `N` is the Windows drive letter representing the volume. For example: `vssadmin Add ShadowStorage /For=D: /On=D:`

3. Repeat the preceding command for each volume in the virtual machine.
4. Use the following command to verify shadowstorage mapping:
   `vssadmin List ShadowStorage`

   If this command returns null, it indicates that VSS is making a default choice for all volumes.

4

Known Issues

This section contains known issues in this release (HIT/Microsoft 4.8.0), as well as known issues that have been fixed in previous releases (HIT/Microsoft 4.7.0 and 4.7.1).

Known Issues in This Release (HIT/Microsoft Version 4.8.0)

The following known issues apply to the current version of HIT/Microsoft.

Installing SCVMM 2012 R2 UR5 Causes EqualLogic Storage Discovery Issues

When Update Rollup 5 (UR5) is installed for System Center Virtual Machine Manager 2012 R2, SCVMM will have issues discovering EqualLogic Storage, including that EqualLogic Storage was already discovered.

As a Workaround, download and install **Microsoft Hotfix KB3039296**, which you can find at

support.microsoft.com/kb/3039296

Microsoft Hotfix KB3039296 requires a manual installation. To install the hotfix:

1. Run **Microsoft Hotfix KB3039296**.
   The Microsoft Software License Terms panel displays.
2. Click **Yes** to agree to the Microsoft Software License Terms.
   A message is displayed, prompting you to select a location to place the extracted files.
3. Click the **Browse** button to navigate to the location where you want to install the extracted files. Click **OK**.
4. Back up your original files before continuing with the rest of this procedure.
5. From the VMM Server computer:
   a. Stop the System Center Virtual Machine Manager service.
   b. Replace the files under your Virtual Machine Manager Install directory with the newly extracted files.
      For example, replace the VMM Install directory files with the following files:
      - `%VMMINSTALLPATH%\bin\ImgLibEngine.dll`
      - `%VMMINSTALLPATH%\bin\ Microsoft.VirtualManager.UI.CommonControls.dll`
      - `%VMMINSTALLPATH%\bin\SCXStorageWrapper.dll`

NOTE: The `%VMMINSTALLPATH%` placeholder represents the directory where SC2012 R2 VMM is installed, such as **C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager**.

c. Start the **System Center Virtual Machine Manager** service.

ASM Exchange Verification Fails on a Database When a Replicated Volume is Promoted as a Permanent Volume

When a replicated volume (Recovery volume) is promoted as a permanent volume from the replication partner group (in bound replica set) and the ASM Exchange Verification and Recovery is triggered on the Smart Copy by either the Promote and Verify option or the Clone and Verify option, a failed status will result for both the Checksum Verification State and the Soft Recovery State.

The reason that the ASM verification fails is because the replicated volume information obtained from the PS arrays is different than the original replicated volume information. Whenever ASM Exchange Verification and Recovery is run in this instance, it generates temporary mount points that fail.

As a workaround, do the following:

- Mount the SmartCopy on the host with the replica promoted volume (Recovery volume).
- Trigger Verification and Recovery for the Smart Copy with the Promote and Verify option or the Clone and Verify option.

Known Issues Fixed Since Previous Releases (HIT/ME Version 4.7.0 and 4.7.1)

The following sections describe known issues that were fixed for HIT/Microsoft version 4.7.1 and 4.7.0.

Auto-Snapshot Manager

- An intermittent issue was discovered in Dell EqualLogic Auto-Snapshot Manager Microsoft Edition v4.7 Early Production Access (EPA) related to Smart Copies of Hyper-V 2012 R2 objects (including Volumes, Collections, and Virtual Machines). This issue can potentially prevent Selective Restore operations of those Smart Copies from succeeding. Dell EqualLogic strongly recommends that you upgrade to the recommended Dell EqualLogic Host Integration Tools for Microsoft v4.7 General Availability (GA) release. Then, recreate new Smart Copies of the desired Hyper-V objects. Selective Restore operations for Hyper-V were previously disabled in ASM/ME v4.7 EPA. This feature has been reenabled in the ASM/ME v4.7 release.
- The Auto-Snapshot Manager (ASM) cannot create clones of volumes that are using access policies created by a vol admin account.
- By default, the ASM agent uses port 7569 to listen for connections from clients. If another service/component is using that port, the ASM agent will not start. The `Could not accept on listening socket` error is generated. If you see this error, check to see if another service/component is using port 7569. If so, assign a different port to that other service/component and try restarting the ASM agent.

- If you cancel the uninstall operation while uninstalling ASM, you might get errors such as:

  ```
  Error 1905.Module
  <some component, DLL, etc>
  failed to unregister. HRESULT -2147220472. Contact your support personnel.
  ```

  To resolve these errors, you should run the repair operation to restore all the ASM binaries to a known good state. These errors are caused by a file registration being left in an unusable state after canceling the uninstall. Running the ASM repair operation restores the ASM binaries to a good state. After the repair operation finishes, you can then uninstall ASM.
-
-
- You might get `Access is Denied` errors from the Volume Shadow Copy Service (VSS) in Windows Server 2012 application event logs when Auto-Snapshot Manager queries application VSS writers.

  To work around these errors, go to msdn.microsoft.com/en-us/library/windows/desktop/aa384605(v=vs.85).aspx and follow the instructions in the section, *Explicitly Controlling User Account Access to a Writer*.

Windows 2012 R2 Hyper-V Cluster Smart Copy Collections Fail During a Selective Restore

An April 2014 update to Windows 2012 R2 is available at http://support.microsoft.com/kb/2919355. See Knowledge Base Article KB2919355 , *Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 Update: April 2014*

This Windows update caused the Hyper-V VSS Writer to report files in the virtual machine metadata that did not exist in the Smart Copy. Although the Smart Copy operation succeeded, selective restores from the Smart Copy failed when ASM attempted to copy one of the files in the metadata, which did not exist.

This problem was corrected in a June 2014 hotfix found in Knowledge Base Article KB2966407, *Backing up viritual machines fails when using the CSV writer after installation of update 2010355*(support.microsoft.com/kb/2966407).

After installing KB2966407, selective restores of Smart Copies created prior to applying the hotfix are not corrected, only subsequent selective restores. In-place (Restore All) restore operations, however, are unaffected by this problem. For additional information about restore operations in ASM/ME, see the *Dell EqualLogic Auto-Snapshot Manager Microsoft Edition User's Guide*.

NOTE:

If you performed the Windows 2012 R2 updates described in KB2919355, you must also install KB2966407. Failure to do so results in the creation of Smart Copies that cannot be selectively restored.

Data Center Bridging Limitations of Some Switches

Certain 10Gb network switch models do not fully support DCB for Dell EqualLogic PS Series arrays. Running in such an environment could result in alerts being reported by the array and incorrect failure of RWSCLI initialization due to an unspecified DCB VLAN ID. To resolve this problem, disable DCB on your network switch.

See the following Technical White Paper for additional information:

en.community.dell.com/techcenter/storage/w/wiki/4355.configuring-dcb-with-equallogic-sans.aspx

Add EQL SMP as a Storage Provider on the VMM Server Fails when using SSO on Windows Server 2012 R2 with SCVMM 2012 R2

To solve this problem, specify the vmmadmin user delegation setting in **AD Users and Computers** by changing the vmm server delegation setting to **Trust this computer for delegation to any service (Kerberos only)** with SSO enabled in ASM. Then, restart the SCVMM service on the VMM server. You can now add your SMP storage provider along with its associated PS group.

Mount/Unmount Option is Disabled for Exchange Replica Smart Copies

The Mount/Unmount option has been disabled in this release for all Exchange replica Smart Copies. This change supports verification of replica Smart Copies from the source host.

The Unmount option deleted the last replica from the replication partner, which can render the last replica Smart Copy as broken. Because the verification process uses Mount/Unmount functionality, the process has been modified for Exchange replica Smart Copies.

Try any of these workarounds:

- Clone a replica, which creates a new volume
- Clone and restore as new
- Clone and create a recovery mailbox database (Exchange 2010 and 2013)