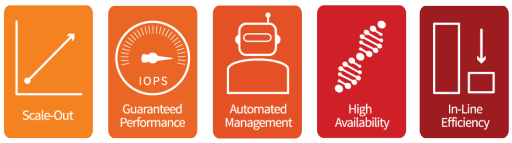
SOLIDFIRE



The All-Flash Array Built for the Next Generation Data Center

SolidFire VSS Hardware Provider User Guide

Version: 2.0

4/26/16

Copyright Information

Trademark Information

TABLE OF CONTENTS

Introduction

The SolidFire VSS Hardware Provider integrates VSS shadow copies with SolidFire snapshots and clones. The Provider runs on Microsoft® Windows® 2008 R2 and 2012 R2 editions and supports shadow copies created using DiskShadow and other VSS Requesters. A GUI-based configuration utility is provided to add, modify, and remove cluster information used by the SolidFire VSS Hardware Provider.

Utilizing VSS snapshot capabilities with the SolidFire VSS Hardware Provider ensures that snapshots are application consistent with business applications that use SolidFire volumes on a system. A coordinated effort between VSS components provides this functionality. SolidFire snapshots and clones minimize recovery time without affecting stability and performance and provide instant volume recovery.

The intended audience for the SolidFire *VSS Hardware Provider User Guide* is administrators who install, configure, use, or troubleshoot provider-related issues. The following assumptions are made regarding the intended audience:

- Microsoft® Windows® System Administrators: You should have experience as a Windows® system administrator.
- Backup and recovery: You should be familiar with backup, restore, and SAN terminologies.

VSS Hardware Provider Overview

There are three major components of the Microsoft® Windows® Volume Shadow Copy Service (VSS): VSS Providers, VSS Writers, and VSS Requesters. A VSS Provider is a storage level component that offers functionality to create a shadow copy of one or more volumes. A VSS Writer is application-specific software that ensures application data is ready for shadow copy creation. The application that initiates the creation of a shadow copy is a VSS Requester.

The high-level architecture diagram below shows the interaction between VSS components and the SolidFire system. The backup application DiskShadow is a VSS Requester for creating shadow copies of volumes. When DiskShadow executes a backup, VSS orchestrates the interaction between the VSS Requester, VSS Writers, and VSS Providers. VSS maintains application consistency while creating a volume shadow copy. There are several VSS Writers installed on a system, such as the Microsoft SQL Server VSS Writer. The SolidFire VSS Hardware Provider manages the shadow copies created by a VSS Requester at the hardware level using SolidFire snapshots and clones.

The SolidFire Provider uses snapshots and clones to make shadow copies available to the VSS Requester. Shadow copy volumes allow for immediate read-only access to the data from the MS Windows host.

The Microsoft Windows host must have access to both storage and the management network so that the VSS Provider can work correctly. Administrators must add one or more clusters to the SolidFire VSS Hardware Provider configuration. This allows the Provider to connect to SolidFire clusters and interact with the SolidFire API to create snapshots and clones during the backup process.

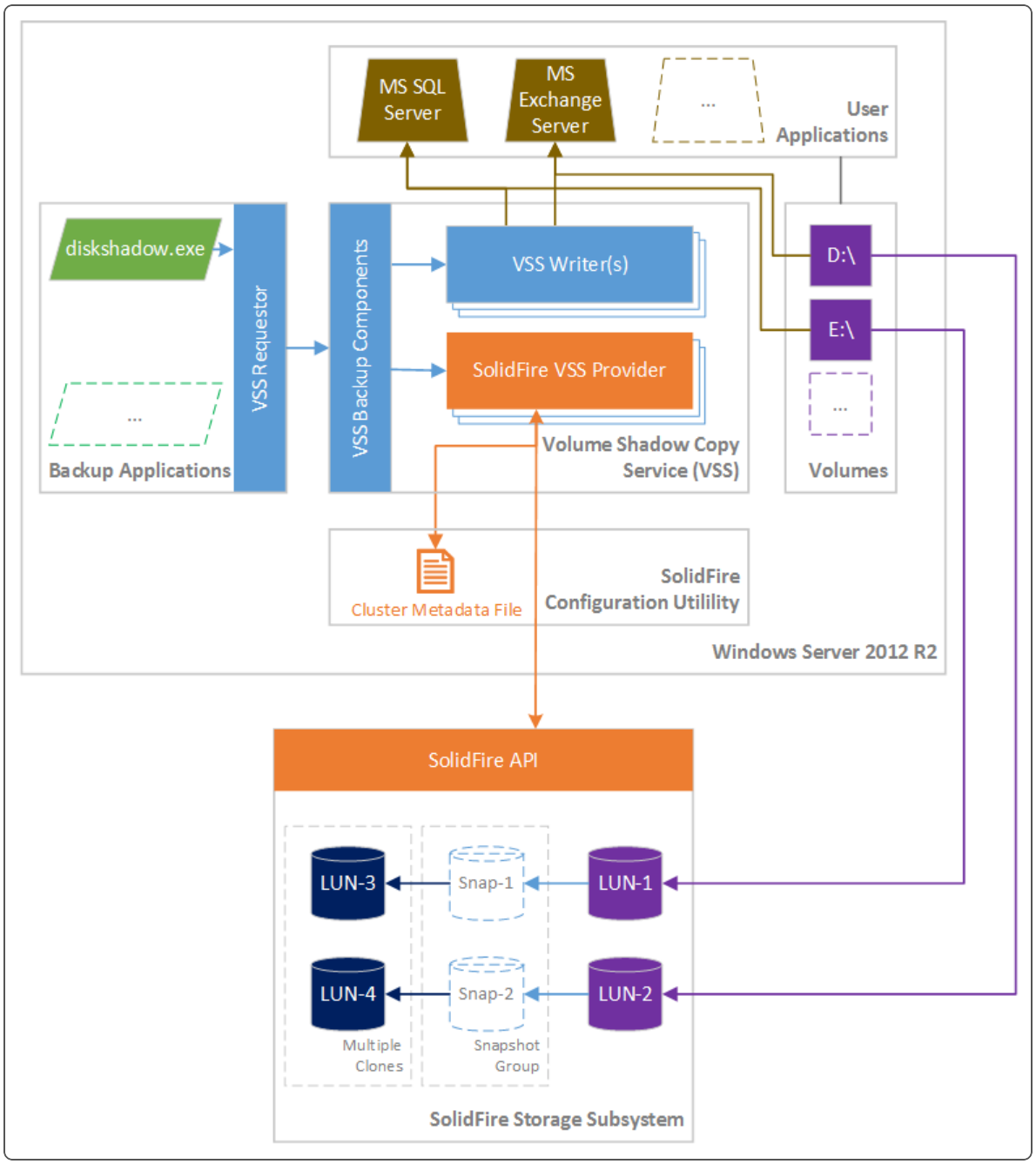


Figure 1: SolidFire VSS Hardware Provider Architecture

Getting Started

Software and hardware prerequisites must be met to use the SolidFire VSS Hardware Provider effectively. Before installing the Provider, make sure that your configuration meets the minimum requirements.

Hardware Prerequisites

Component	Description
System processor	1.5 GHz (dual core recommended), Intel compatible 64-bit
System memory	Minimum 4 GB recommended
Free disk space required for installation	Minimum 5 MB required and recommended 100 MB
Networking	Ethernet ports for cluster communication and Ethernet ports for iSCSI or Fibre Channel ports
SolidFire cluster	A cluster of SolidFire nodes

Software Prerequisites

Component	Application	Description
Operating system	Microsoft® Windows® Server	Windows® Server 2008 R2 64-bit Windows® Server 2012 R2 64-bit
	Microsoft® Hyper-V	Windows® Server 2012 R2 64-bit
.NET framework		4.5
SolidFire cluster		Element OS version 7.0 and later

Supported Configurations

VSS Hardware Provider configurations leverage directly connected SolidFire iSCSI or Fibre Channel volumes. Only the configurations described in the proceeding tables are supported.

Supported Operating Systems	
Windows Server 2008 R2	✓
Windows Server 2012 R2	✓
Hyper-V Server 2012 R2	✓

The following OS and SQL Server combinations are supported.

OS/SQL Version	Stand Alone	Shared Storage Cluster	AlwaysOn Cluster
Windows Server 2008 R2			
SQL Server 2008 R2 SP3	✓	✓	

OS/SQL Version	Stand Alone	Shared Storage Cluster	AlwaysOn Cluster
SQL Server 2012 SP2	✓		✓
SQL 2014		✓	✓
Windows Server 2012 R2			
SQL Server 2008 R2 SP3			
SQL Server 2012 SP2	✓	✓	✓
SQL 2014	✓	✓	✓

Installing the VSS Hardware Provider

Install the SolidFire VSS Hardware Provider using the 64-bit MSI installer. When you launch the **`SolidFireVSSProvider_Setup.msi`** (the most recent version number is appended to the file name), the installer adds Provider files in the user defined directories on the target machine. It also launches the scripts required to register the Provider and starts the configuration tool after successful installation.

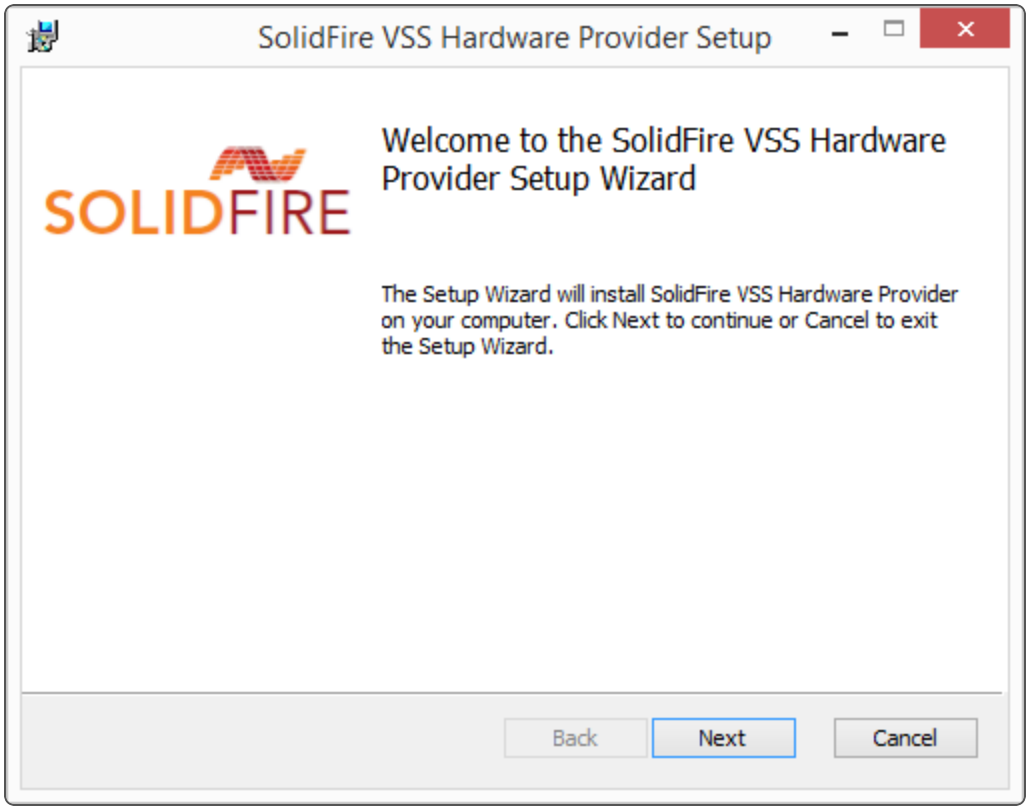
Prerequisites

- You must have administrative privileges to install and use the Provider.

Procedure

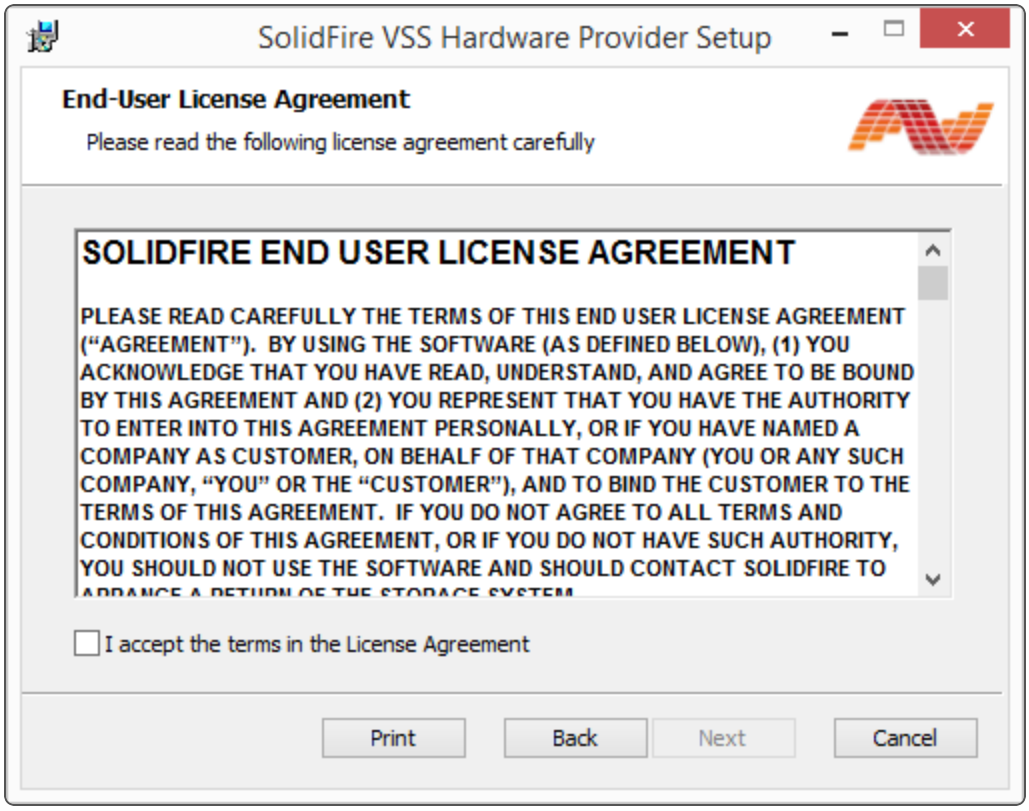
1. Double-click the most recent version of the **`SolidFireVSSProvider_Setup.msi`** installer.

   The *Welcome* window appears.



2. Click **Next**.

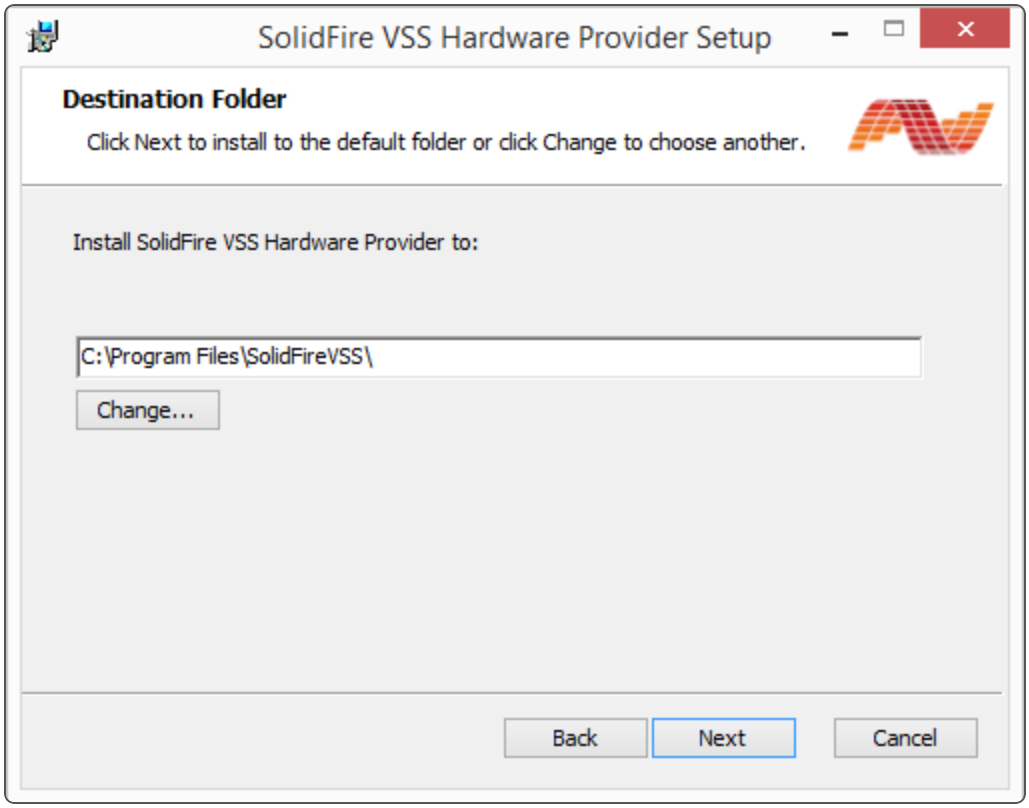
   The *SolidFire End User License Agreement* appears.



3. Read the license agreement and select the check box to accept the terms of the agreement.

4. Click **Next**.

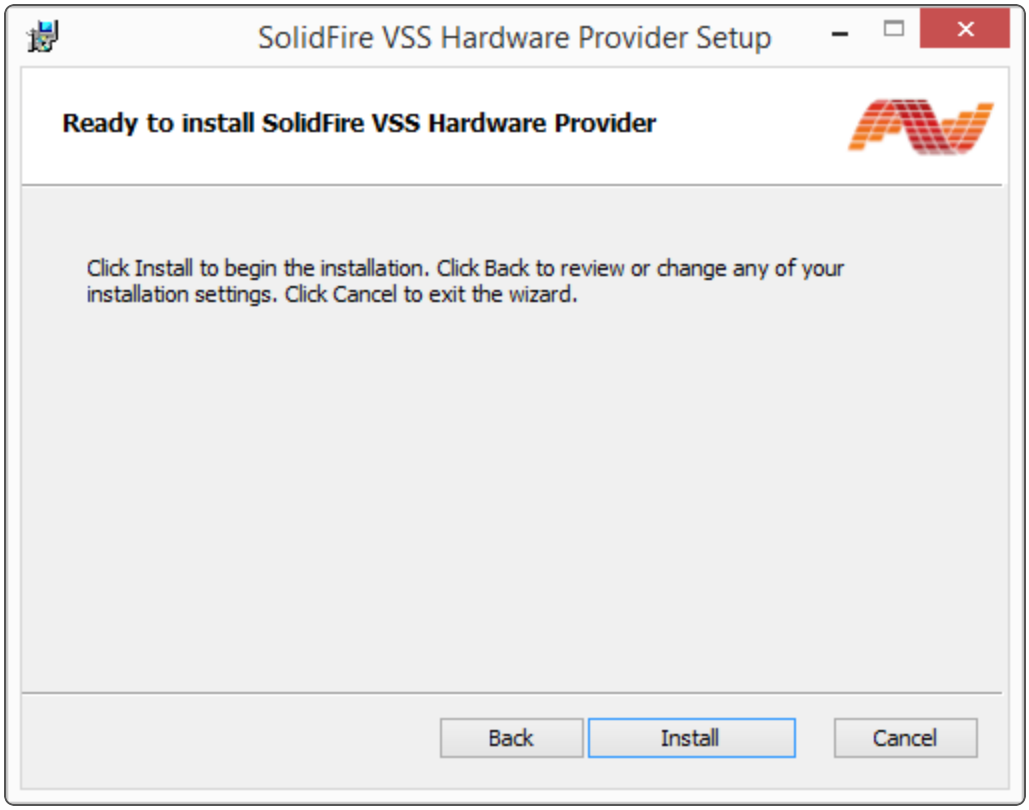
   The *Destination Folder* window appears.



NOTE: By default, the VSS Hardware Provider installs to **C:\Program Files\SolidFireVSS**. To change the installation location, click **Change** and provide the new location.

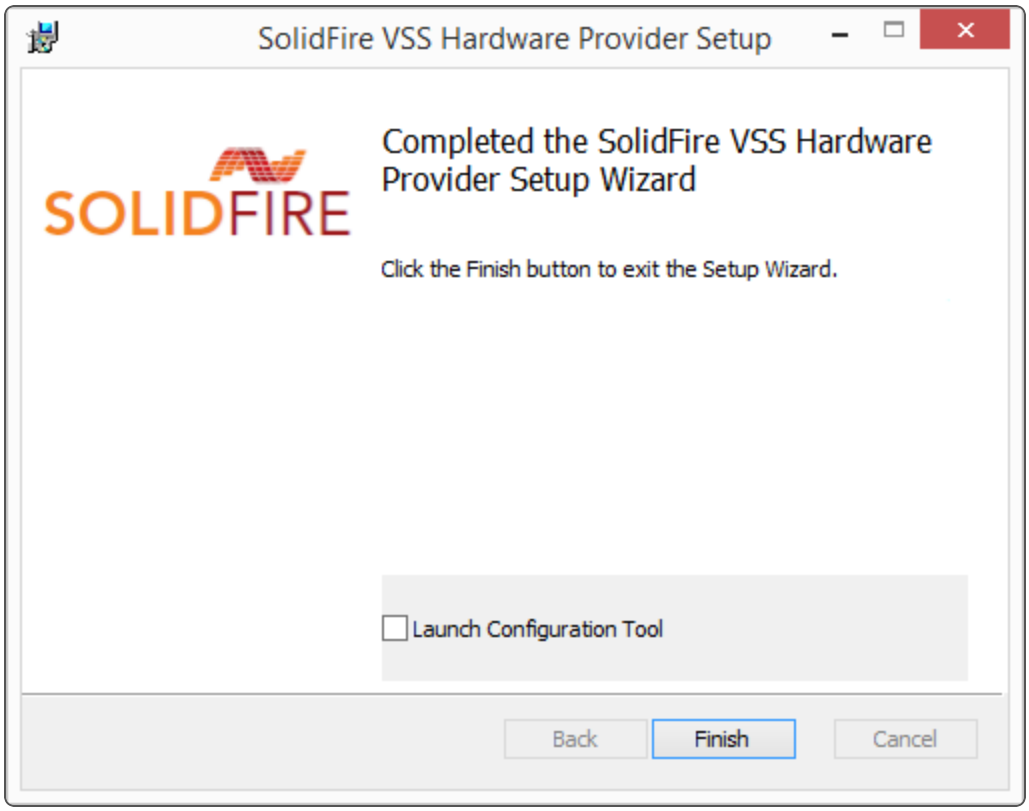
5. Click **Next**.

   The *Ready to install SolidFire VSS Hardware Provider* window appears.



6. Click **Install**.

   The *Completed the SolidFire VSS Hardware Provider Setup Wizard* window appears after the installation has completed successfully.



7. To start the configuration tool immediately after the installation, select the **Launch Configuration Tool** check box.

   NOTE: You must use the configuration tool to connect to and configure settings for a SolidFire cluster before you create shadow copies. For details, see *How to Use the VSS Hardware Provider Configuration Tool*.

8. Click **Finish**.

After successful installation, the Provider is installed on the system and registered with the VSS service. You can view the logs and errors, if any, in the Windows Event Viewer. For details about viewing logs, see *Provider Event Logs*.

Upgrading the SolidFire VSS Hardware Provider

Download and run the latest MSI installer to upgrade the SolidFire VSS Hardware Provider to the latest version. For installation instructions, see *Installing the VSS Hardware Provider*.

NOTE: The update process does not alter current cluster configuration information.

How to Use the VSS Hardware Provider Configuration Tool

The configuration tool for the SolidFire VSS Hardware Provider is a GUI that you can use to define the configuration details of one or more SolidFire clusters. The Provider communicates with a cluster using SolidFire API. During Provider installation, the configuration tool is installed on the host system.

Starting the Configuration Tool

You can open the configuration tool from the **Start** menu in Windows.

When you start **`SolidFire.Vss.ConfigTool.exe`** for the first time after installing the Provider, the **Cluster List** is empty. Cluster details appear in the list after you configure and save cluster information.

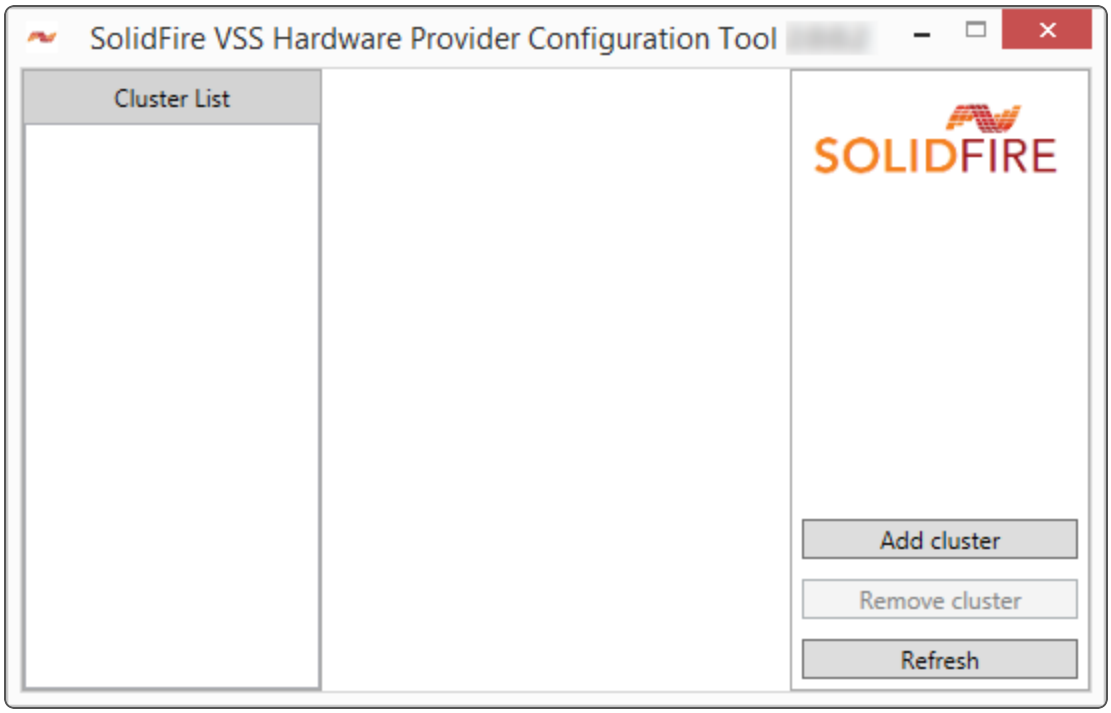


Figure 2: Configuration Tool Cluster List

Adding Cluster Information

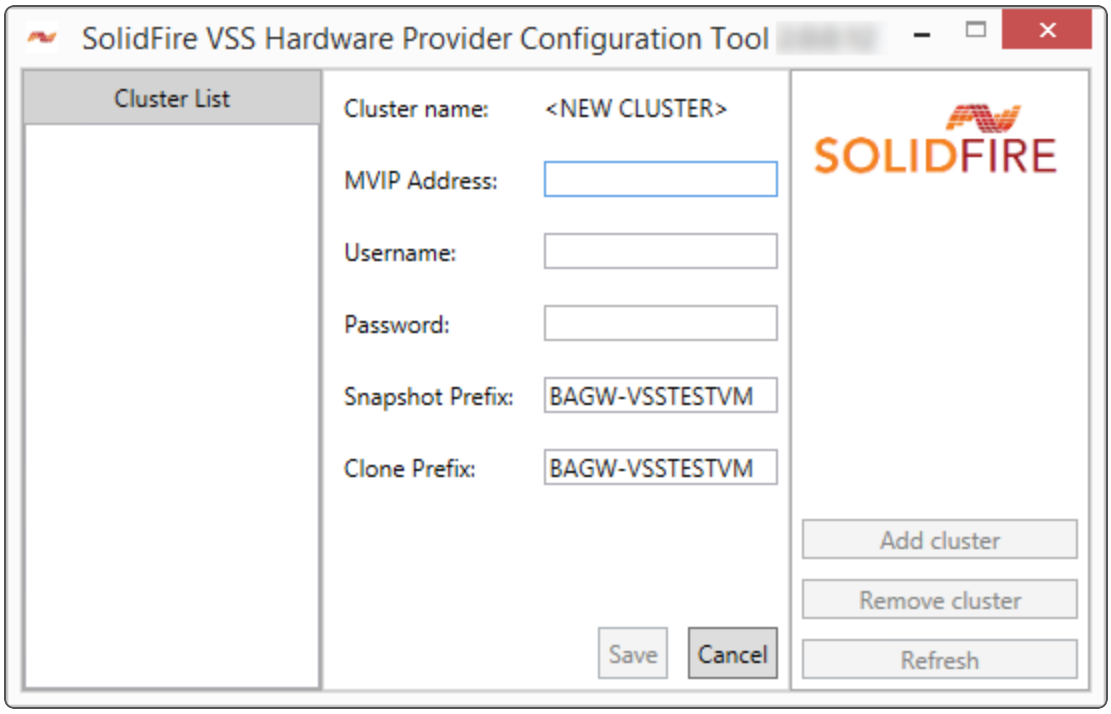
Use the configuration tool to configure the SolidFire VSS Hardware Provider parameters that are required for the Provider to communicate with the SolidFire hardware. Cluster parameters include the address of the Management Virtual IP (MVIP), user credentials for the cluster admin, and default snapshot and clone prefixes for all shadow copies created on the cluster. The Provider uses this data during shadow copy creation.

The Provider must be installed on all systems where you need to perform tasks like import and resync. Cluster settings must also be configured in the configuration tool for each system.

Procedure

1. From the configuration tool user interface, click **Add cluster**.

   The configuration fields for the new cluster appear.

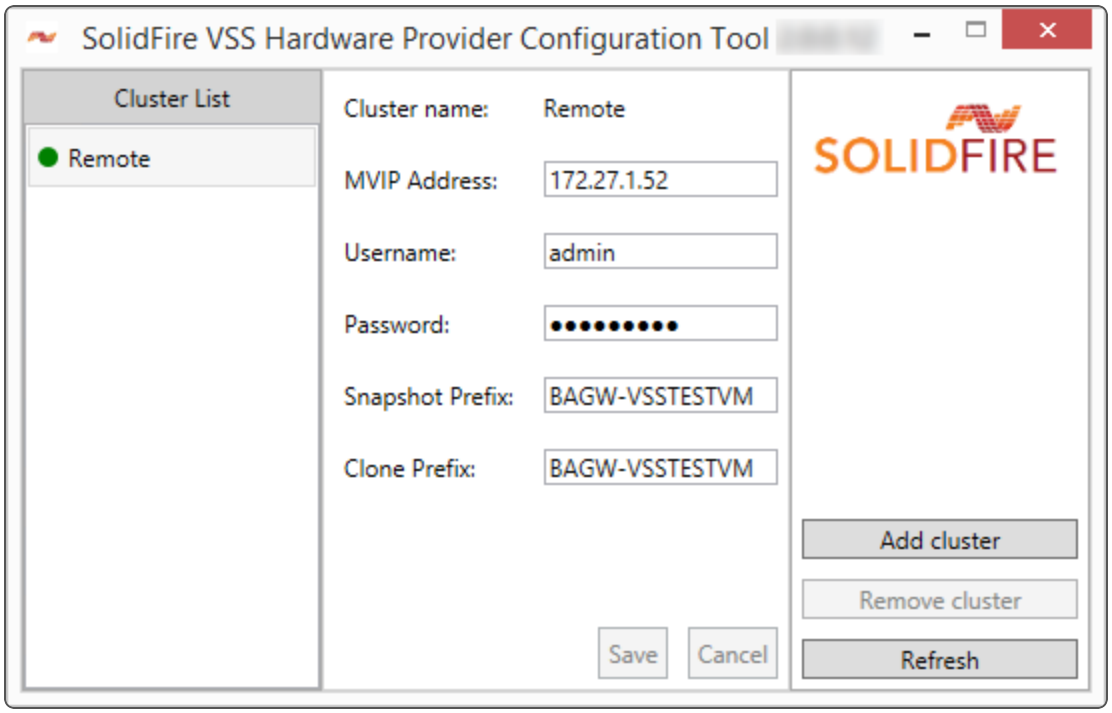


2. Type the **MVIP Address** for the cluster.
3. Type the **Username** and **Password** for the cluster administrator.
4. (Optional) Enter the snapshot and clone prefixes for all shadow copies created in the cluster.

NOTE: Snapshot and clone prefixes can only be changed using the configuration tool. If you do not specify prefixes, a system default prefix is substituted that is based on the NetBIOS host name. For more information, see *Snapshot and Clone Naming*.

5. Click **Save**.

   The cluster name will be returned and displayed in the **Cluster name** and **Cluster List** fields when a connection with the cluster is made.



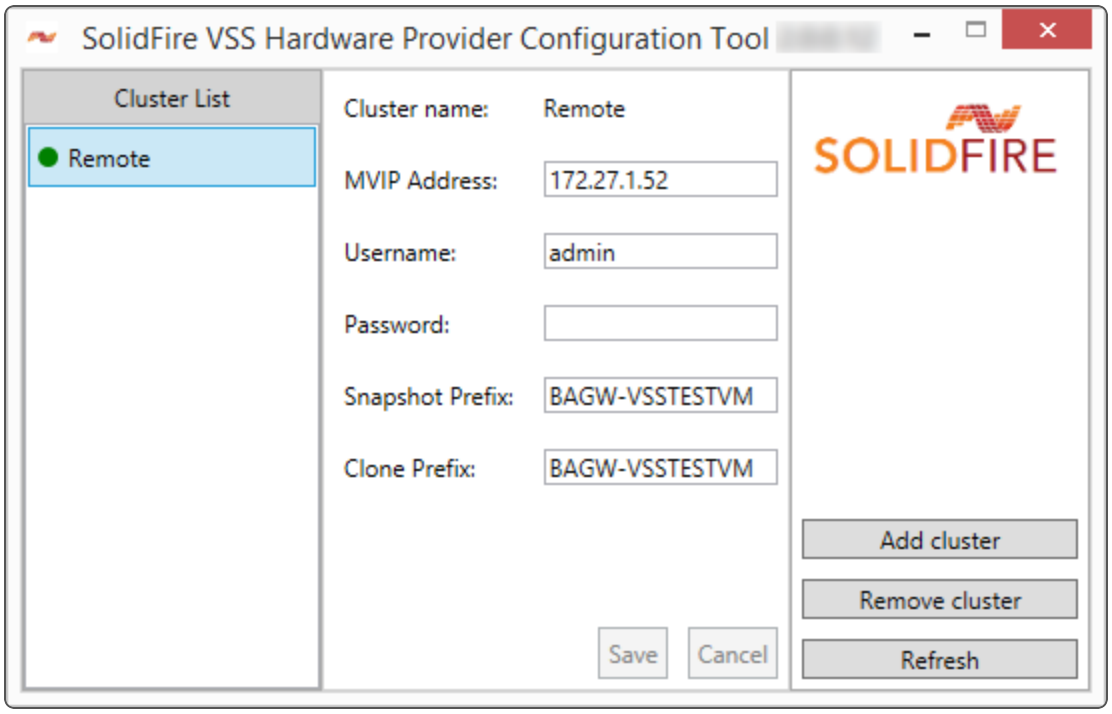
Editing Cluster Information

Use the SolidFire VSS Hardware Provider configuration tool to edit cluster information.

Procedure

1. Click on a cluster in the **Cluster List** view.

   The cluster information will display.



2. Enter the desired changes.

   NOTE: The existing password for the SolidFire cluster admin does not display in the field. The password must be typed again to make configuration changes.

3. Click **Save**.

   NOTE: Cluster administrator user names and passwords can only be changed from the Element OS user interface. For more information on changing cluster administrator accounts, see the Element OS user guide.

4. (Optional) Click **Refresh** to check connectivity to the cluster.

Removing a Cluster

Use the SolidFire VSS Hardware Provider configuration tool to remove a cluster from the cluster list in the UI.

Procedure

1. Click on a cluster in the **Cluster List**.

   The cluster configuration information for the selected cluster appears.

2. Click **Remove cluster** to remove the cluster from the **Cluster List**.

NOTE: The cluster connection credential metadata is stored in the encrypted file `clusterinfo.xml` in the installation directory (**C:\ProgramData\SolidFire\Vss**). This file can only be accessed and used by the system that created it. For security reasons, moving metadata files across different hosts is not supported.

How to Use DiskShadow to Make Provider Requests

The following topics describe the actions you can request that the SolidFire VSS Hardware Provider perform. For each topic, DiskShadow is used as the VSS Requester to create, manage, and remove shadow copies.

Creating a Shadow Copy

You can use DiskShadow to request that the SolidFire VSS Hardware Provider create a shadow copy of one or more volumes on a system. When the snapshot is complete, the shadow copies of the volumes are added to a shadow copy set. Both a shadow copy and shadow copy set can be used for restore.

The Provider supports the following types of shadow copies:

- A *Differential* shadow copy creates a point-in-time snapshot of specified volumes. Only the snapshot is created during the shadow copy create operation. A volume clone based on this snapshot will be created during an import operation. A Differential shadow copy is the default.
- A *Plex* shadow copy is a point-in-time clone copy of the data on a specified volume. One transient snapshot per volume is required to create Plex shadow copies.

NOTE: A shadow copy cannot be created if there are more than 31 snapshots. The maximum number of shadow copies per volume is 32.

Prerequisites

- The SolidFire VSS Hardware Provider is installed on a host that is connected to a SolidFire cluster.
- The volume you wish to copy is mapped and connected to a SolidFire cluster with an existing volume access group.
- Review *Hardware Prerequisites*.
- Review *Software Prerequisites*.

Procedure

1. Open a command prompt as Administrator and type `diskshadow` to access the DiskShadow command line interface.

   The *DISKSHADOW* prompt opens.

2. (Optional) List providers to confirm that the SolidFire VSS Hardware Provider is registered to VSS.

   ```
   DISKSHADOW> list providers
   ```

3. (Optional) Turn on verbose output during shadow copy creation.

   ```
   DISKSHADOW> set verbose on
   ```

4. Set the context to `persistent` so that shadow copy survives until host restart.

   ```
   DISKSHADOW> set context persistent
   ```

5. Set the shadow copy option to either `differential` or `plex` and include the `transportable` parameter:

   - `DISKSHADOW> set option differential transportable`
   - `DISKSHADOW> set option plex transportable`

   NOTE: You must specify the `transportable` parameter so that the shadow copy can be imported later by another host.

6. Set the file name and location of the shadow copy metadata file that is used to transfer shadow copies from one host to another:

   ```
   DISKSHADOW> set metadata <filename.cab>
   ```

7. Add a volume letter with an alias name.

   NOTE: At least one volume must be added to create a shadow copy.

   ```
   DISKSHADOW> add volume <drive letter>: alias <alias_name>
   ```

8. Execute the `begin backup` command.

   ```
   DISKSHADOW> begin backup
   ```

9. Create the shadow copy.

   ```
   DISKSHADOW> create
   ```

10. Execute the `end backup` command.

    ```
    DISKSHADOW> end backup
    ```

    NOTE: This command ends a full backup session and issues a backup complete event.

11. A shadow copy now appears on the SolidFire cluster. To view the created copy, see *Listing Shadow Copies*.

    NOTE: If there is an error while creating shadow copies, see *Provider Event Details*.

Parameters to Create Shadow Copy

The following table describes the commands and sub-commands needed to create shadow copies using DiskShadow.

Command	Sub-command	Parameter	Description
set	context	persistent	Specifies that the shadow copy persist across DiskShadow exit, reset, or restart.
		volatile	The default option that deletes the shadow copy on DiskShadow exit or reset.
	option	differential | plex	Specifies to the Provider the type of shadow copy it must create. A Differential shadow copy is created by default unless otherwise specified. For more details about Differential and Plex shadow copies, see *Creating a Shadow Copy*.
		transportable	Specifies that the shadow copy is not to be imported yet. The metadata **.cab** file can later be used to import the shadow copy to the same or a different computer.
add	volume	<volume>	Adds a volume to the shadow copy set, which is the set of volumes to be shadow copied.
		[provider <ProviderID>]	Specifies the Provider ID of a registered provider to use to create the shadow copy. If the provider is not specified, the default provider is used.
	alias	<alias name> <alias value>	Specifies the name of the alias. This alias is assigned as an environment variable to the shadow copy ID corresponding to this volume after creation.
create	-	-	Starts shadow copy creation process using the current context and option settings.
begin	backup		Starts a full backup session.
end	backup		Ends a full backup session. Issues a BackupComplete event with the appropriate writer state, if needed.
writer	verify	[<writer> | <component>]	Verifies the inclusion of a writer or component in a backup or restore procedure.
	exclude	[<writer> | <component>]	Excludes a writer or component from a backup or restore procedure.

DiskShadow Command Examples to Create a Shadow Copy

This sample sequence creates a differential transportable shadow copy of a SolidFire volume (drive F).

```
DISKSHADOW> set verbose on
DISKSHADOW> set context persistent
DISKSHADOW> set option differential transportable
DISKSHADOW> set metadata c:\temp\metadatadbagVSS.cab
DISKSHADOW> begin backup
DISKSHADOW> add volume f: alias dbagVSS
DISKSHADOW> create
Alias dbagVSS for shadow ID {a1402b88-b823-43dc-bba6-362a180866bf} set as environment variable.
Alias VSS_SHADOW_SET for shadow set ID {77625644-ec5e-4586-9f5f-5a386d898d9c} set as environment
variable.


Inserted file Manifest.xml into .cab file metadatadbagVSS.cab
Inserted file BCDocument.xml into .cab file metadatadbagVSS.cab
Inserted file WM0.xml into .cab file metadatadbagVSS.cab
Inserted file WM1.xml into .cab file metadatadbagVSS.cab
Inserted file WM2.xml into .cab file metadatadbagVSS.cab
Inserted file WM3.xml into .cab file metadatadbagVSS.cab
Inserted file WM4.xml into .cab file metadatadbagVSS.cab
Inserted file WM5.xml into .cab file metadatadbagVSS.cab
Inserted file WM6.xml into .cab file metadatadbagVSS.cab
Inserted file WM7.xml into .cab file metadatadbagVSS.cab
Inserted file WM8.xml into .cab file metadatadbagVSS.cab
Inserted file WM9.xml into .cab file metadatadbagVSS.cab
Inserted file WM10.xml into .cab file metadatadbagVSS.cab
Inserted file Dis7FD9.tmp into .cab file metadatadbagVSS.cab


DISKSHADOW> end backup
```

Resyncing a Volume Using DiskShadow

Use the DiskShadow interface to request that the SolidFire VSS Hardware Provider restore or resync a shadow copy. If a volume is corrupt or you have lost data, you can perform a shadow copy resync and get the volume back to a known good state using a shadow copy that was taken earlier.

You can resync a volume group using the shadow copy to ensure that the data on the group of volumes is consistent for the point-in-time in which the shadow copy was created. Volumes can be rolled back to the shadow copies created for each volume.

NOTE: For an AlwaysOn clustered setup, see *Resyncing a Volume for AlwaysOn Clustered Setup*.

Prerequisites

A differential shadow copy must exist. To create a differential shadow copy, see *Creating a Shadow Copy*.

Procedure

1. Load the metadata.

   ```
   DISKSHADOW> load metadata <c:\get.cab>
   ```

NOTE: The `.cab` file is mandatory for resync.

2. Add the shadow copy with the shadow alias that you need to resync to the recovery set.

```
DISKSHADOW> add shadow <%shadow alias%>
```

NOTE: SolidFire VSS Hardware Provider supports resync to the same volume from which a shadow copy was created. Because of this, the `[DESTINATIONVOLUME]` parameter in the resync command is not supported.

3. Execute the `begin restore` command. This command starts a restore session and issues a PreRestore event to the involved writers.

```
DISKSHADOW> begin restore
```

NOTE: For a standalone server with an SQL database, the database must be offline before you perform the resync operation.

4. Resync the volume with the shadow copy. This command starts a resynchronization operation for the volumes in the recovery set.

```
DISKSHADOW> resync
```

NOTE: Backup and restore operations are not allowed on tempdb. See Move System Databases to move a tempdb database. See Optimizing tempdb Performance for Microsoft SQL Server tempdb placement if you plan to use resync for database recovery.

5. Execute the `end restore` command after the volume is resynced.

```
DISKSHADOW> end restore
```

NOTE: After performing resync, if two or more machines are using a common volume that was used during the resynchronization operation, you need to disconnect and reconnect the iSCSI target for changes to show.

Resyncing a Volume for AlwaysOn Clustered Setup

Use the DiskShadow interface according to the following procedure to perform volume resync for an AlwaysOn clustered setup.

Procedure

1. Remove the database from the **Availability Group** in the SQL Server Management Studio. For more information on removing the database from the Availability Group, see your SQL Server 2012 documentation.
2. Execute the `begin restore` command.
3. Resync the volume with the shadow copy using the `resync` command. This command starts a resynchronization operation for the volumes in the recovery set.
4. Execute `end restore`.
5. After restore completes, check the database status and then add the database to the **Availability Group** from the SQL Server Management Studio.

Parameters to Resync a Shadow Copy

The following table describes the commands and sub-commands needed to resync a shadow copy using DiskShadow.

Command	Sub-command	Parameter	Description
load	metadata	<metadata.cab>	Specifies the **metadata.cab** file to load.
add	shadow	<shadowID>	Adds a shadow copy to the recovery set. Specifies a hardware shadow copy.
begin	restore	-	Begins a restore operation.
resync	-	-	Starts a resynchronization operation for the volumes in the recovery set (for hardware shadow copies only).
end	restore	-	Ends a restore session.

DiskShadow Command Examples to Resync a Shadow Copy

The following example resyncs a shadow copy of two SQL volumes.

```
DISKSHADOW> load metadata c:\get.cab
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\get.cabManifest.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\get.cabBCDocument.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\get.cabWM0.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\get.cabWM1.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\get.cabWM2.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\get.cabWM3.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\get.cabWM4.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\get.cabWM5.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\get.cabWM6.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\get.cabWM7.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\get.cabWM8.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\get.cabWM9.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\get.cabDisA1CD.tmp.
Alias p for value {7bf75171-8070-4647-a915-f76967322792} set as an environment variable.
Alias l for value {d97be3c7-3783-409d-9240-74bdee65a584} set as an environment variable.
Alias VSS_SHADOW_SET for value {a8a65a9c-ec17-47f5-952e-295c956afef2} set as an environment variable.
DISKSHADOW> add shadow %p%
-> %p% = {7bf75171-8070-4647-a915-f76967322792}
DISKSHADOW> add shadow %l%
-> %l% = {d97be3c7-3783-409d-9240-74bdee65a584}
DISKSHADOW> begin restore
Listing writer status information ...
       < * WRITER "SqlServerWriter"
                 - Status: 5 (VSS_WS_WAITING_FOR_BACKUP_COMPLETE)
                 - Writer failure code: 0x00000000 (S_OK)
                 - Writer ID: {a65faa63-5ea8-4ebc-9dbd-a0c4db26912a}
                 - Writer instance ID:
{96dd0be9-ff06-4265-98b4-889ac9b74512}>
<A list of writers are listed>
Number of writers listed: <Total number of writers is listed>
Writer SqlServerWriter is present in the Backup Components Document and on the computer.
Writer SqlServerWriter supports restore events.
Notifying VSS of selected writer components for restore.
        * Writer "SqlServerWriter":
                 + Selecting component: \WIN-PB674VKVN8A\SQLEXPRESS\TestDB02
                 + Selecting component: \WIN-PB674VKVN8A\SQLEXPRESS\TestDB04
The PreRestore event was successfully sent to the writers.
The restore operation has started. Please issue END RESTORE when it is complete.
DISKSHADOW> resync
Adding resynchronization source and destination pair: Shadow copy
{7bf75171-8070-4647-a915-f76967322792} to  to the recovery set.
```

```
Adding resynchronization source and destination pair: Shadow copy
{d97be3c7-3783-409d-9240-74bdee65a584} to  to the recovery set.
The resynchronization operation successfully completed.
DISKSHADOW> end restore
Setting restore status for all restore components...
        * Writer "SqlServerWriter":
                + Selecting component: \WIN-PB674VKVN8A\SQLEXPRESS\TestDB02
                + Selecting component: \WIN-PB674VKVN8A\SQLEXPRESS\TestDB04
```

Listing Shadow Copies

Use the DiskShadow interface according to the following procedure to list existing shadow copies created on the SolidFire cluster.

Prerequisites

- A shadow copy must exist. To create a shadow copy, see *Creating a Shadow Copy*.

Procedure

1. Open a command prompt as Administrator and access the DiskShadow command line interface by typing `DISKSHADOW`.

   The *DISKSHADOW* prompt opens.

2. List all the shadow copies.

   ```
   DISKSHADOW> list shadows all
   ```

   A list of all shadow copies created on the server appears.

   NOTE: You can use the `list shadows set <setID>` or `list shadows ID <shadowID>` commands to list specific shadow copies by ID.

   NOTE: You can also view the list of snapshots created as a part of the shadow copy operation in the SolidFire Element OS user interface.

Parameters to List Shadow Copy

The following table describes the commands and sub-commands needed to list a shadow copy using DiskShadow.

Command	Sub-command	Parameter	Description
`list`	`shadows`	`all`	Lists all shadow copies.
		`set <SetID>`	Lists shadow copies that belong to the specified shadow copy set ID.
		`id <ShadowID>`	Lists any shadow copy with the specified shadow copy ID.

DiskShadow Command Examples to List Shadow Copies

The following example lists all shadow copies.

```
> diskshadow
DISKSHADOW> list shadows all
Querying all shadow copies on the computer ...
```

```
* Shadow copy ID = {fef32805-1f19-40ba-9b82-ebf277517e7e
%dbagVSS%
                - Shadow copy set: {746cea94-b814-47be-ab33-6c93b2d952a8} %VSS_SHADOW_SET%
                - Original count of shadow copies = 1
                - Original volume name: \\?\Volume{f8328660-00e6-11e6-80d9-005056bd65a9}\ [F:\]
                - Creation time: 4/13/2016 2:30:09 PM
                - Shadow copy device name: \\?\Volume{f8329046-00e6-11e6-80d9-005056bd65a9}
                - Originating machine: Reese-VSSTestVM
                - Service machine: Reese-VSSTestVM
                - Not exposed
                - Provider ID: {c60838d9-9f6f-4b67-b91b-4b87708396ce}
                - Attributes:  Transportable No_Auto_Release Persistent Hardware Imported Differential
* Shadow copy ID = {a1402b88-b823-43dc-bba6-362a180866bf} <No Alias>
                - Shadow copy set: {77625644-ec5e-4586-9f5f-5a386d898d9c} <No Alias>
                - Original count of shadow copies = 1
                - Original volume name: \\?\Volume{f8328660-00e6-11e6-80d9-005056bd65a9}\ [F:\]
                - Creation time: 4/12/2016 2:40:21 PM
                - Shadow copy device name: \\?\Volume{f83286d6-00e6-11e6-80d9-005056bd65a9}
                - Originating machine: Reese-VSSTestVM
                - Service machine: Reese-VSSTestVM
                - Exposed locally as: G:\
                - Provider ID: {c60838d9-9f6f-4b67-b91b-4b87708396ce}
                - Attributes:  Transportable No_Auto_Release Persistent Hardware Imported Differential
Number of shadow copies listed: 2
```

The following example lists shadow copies of a specified ID.

```
> diskshadow
DISKSHADOW> list shadows ID {fe7158fa-5f10-42eb-909a-7f8c77cc9cee}
Querying all shadow copies with the shadow copy ID {fe7158fa-5f10-42eb-909a-7f8c77cc9cee}
    * Shadow copy ID = {fe7158fa-5f10-42eb-909a-7f8c77cc9cee}              %test1%
        - Shadow copy set: {24b12a7e-19d6-4a53-83cc-0c91f8416d75}       %VSS_SHADOW_SET%
        - Original count of shadow copies = 1
        - Original volume name: \\?\Volume{93d18ddb-8113-11e4-80c6-0050569666f6}\ [F:\]
        - Creation time: 12/11/2014 9:47:51 PM
        - Shadow copy device name: \\?\Volume{93d18f77-8113-11e4-80c6-0050569666f6}
        - Originating machine: WIN-3PVAERRME6V
        - Service machine: WIN-3PVAERRME6V
        - Not exposed
        - Provider ID: {c60838d9-9f6f-4b67-b91b-4b87708396ce}
        - Attributes:  No_Auto_Release Persistent Hardware Plex
Number of shadow copies listed: 1
```

Importing a Shadow Copy

To minimize system disruption caused by backups, a transportable shadow copy can be created on a remote host and imported to a local host. The hosts can be Fibre Channel or iSCSI.

Use the DiskShadow interface according to the following procedure to request that the SolidFire VSS Hardware Provider import a transportable shadow copy from a loaded **`.cab`** metadata file.

Prerequisites

- You created a differential transportable shadow copy on a remote host.
- The volume(s) in the shadow copy is mapped and connected to the remote SolidFire cluster and associated with an existing volume access group.
- You copied the associated **`.cab`** metadata file to the local host on which you intend to import the shadow copy.
- The SolidFire VSS Hardware Provider is installed on the local host and is connected to both the remote source and destination SolidFire clusters.

Procedure

1. Open a command prompt as Administrator and access the DiskShadow command line interface by typing `DISKSHADOW`.

   The *DISKSHADOW* prompt opens.

2. Load the metadata to import a shadow copy.

   ```
   DISKSHADOW> load metadata <filename>.cab
   ```

3. Import the shadow copy using the following command.

   ```
   DISKSHADOW> import
   ```

   The shadow copy is now loaded into the system.

4. (Optional) List the shadow copies on the system to confirm that the import was successful.

   ```
   DISKSHADOW> list shadows
   ```

   NOTE: To expose the shadow copy as a new volume, see *Exposing a Shadow Copy*. Once the volume is exposed, a volume access group is automatically created for the local host connection.

Parameters to Import a Shadow Copy

The following table describes the commands and sub-commands needed to import a shadow copy using DiskShadow.

Command	Sub-command	Parameter	Description
`load`	`metadata`	`MetaData.cab`	Specifies the metadata **`.cab`** file to load.
`import`	-	-	Imports a transportable shadow copy based on the metadata specified by `load metadata`.

DiskShadow Command Examples to Import a Shadow Copy

The following example imports a transportable shadow copy.

```
DISKSHADOW> set verbose on
DISKSHADOW> set context persistent
DISKSHADOW> set option differential transportable
DISKSHADOW> load metadata c:\temp\metadatadbagVSS.cab
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\metadatadbagVSS.cabManifest.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\metadatadbagVSS.cabBCDocument.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\metadatadbagVSS.cabWM0.xml0.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\metadatadbagVSS.cabWM1.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\metadatadbagVSS.cabWM2.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\metadatadbagVSS.cabWM3.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\metadatadbagVSS.cabWM4.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\metadatadbagVSS.cabWM5.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\metadatadbagVSS.cabWM6.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\metadatadbagVSS.cabWM7.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\metadatadbagVSS.cabWM8.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\metadatadbagVSS.cabWM9.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\metadatadbagVSS.cabWM10.xml.
Extracted C:\Users\ADMINI~1\AppData\Local\Temp\2\metadatadbagVSS.cabDis7FD9.tmp.
Alias dbagVSS for value {a1402b88-b823-43dc-bba6-362a180866bf} set as an environment variable.
Alias VSS_SHADOW_SET for value {77625644-ec5e-4586-9f5f-5a386d898d9c} set as an environment variable.
```

```
DISKSHADOW> import
DISKSHADOW> expose %dbagVSS% G:-> %dbagVSS% = {a1402b88-b823-43dc-bba6-362a180866bf}
The shadow copy was successfully exposed as G:\.
```

Masking a Shadow Copy

Use the DiskShadow interface according to the following procedure to request that the SolidFire VSS Hardware Provider mask a shadow copy.

The `mask` command removes hardware shadow copies that were imported using the `import` command. On masking a shadow copy, the shadow copies that belong to the specified shadow copy set ID are removed from the volume access group for the current host.

NOTE: The `mask` command only removes shadow copy volumes from the volume access group for the current host so that these volumes are no longer visible to that host. The actual cloned volumes are not deleted from the SolidFire cluster.

Prerequisites

- A shadow copy must be imported. See *Importing a Shadow Copy*.

Procedure

1. Mask the shadow copy using the following command.

   ```
   DISKSHADOW> mask <ShadowSetID>
   ```

Parameters to Mask a Shadow Copy

The following table describes the commands and sub-commands needed to mask a shadow copy using DiskShadow.

Command	Sub-command	Parameter	Description
`mask`	-	`<ShadowSetID>`	Removes shadow copies that belong to the specified Shadow Copy Set ID.

DiskShadow Command Examples to Mask a Shadow Copy

The following example shows a shadow copy import and masking (removal) of the imported copy from the volume access group.

```
> diskshadow
DISKSHADOW> set context persistent
DISKSHADOW> set option differential transportable
DISKSHADOW> set metadata c:\temp\metadatadbagVSS3.cab
DISKSHADOW> begin backup
DISKSHADOW> add volume f: alias dbagVSS
DISKSHADOW> create
Alias dbagVSS for shadow ID {fef32805-1f19-40ba-9b82-ebf277517e7e} set as environment variable.
Alias VSS_SHADOW_SET for shadow set ID {746cea94-b814-47be-ab33-6c93b2d952a8} set as environment
variable.
DISKSHADOW> end backup
DISKSHADOW> load metadata c:\temp\metadatadbagvss3.cab
Alias dbagVSS for value {fef32805-1f19-40ba-9b82-ebf277517e7e} set as an environment variable.
Alias VSS_SHADOW_SET for value {746cea94-b814-47be-ab33-6c93b2d952a8} set as an environment variable.
DISKSHADOW> import
DISKSHADOW> mask {746cea94-b814-47be-ab33-6c93b2d952a8}
The shadow copy has been removed from the system.
```

Exposing a Shadow Copy

Use the DiskShadow interface according to the following procedure to request that the SolidFire VSS Hardware Provider expose a shadow copy.

The `expose` command exposes a persistent shadow copy as a drive letter, share, or mount point.

Prerequisites

- A persistent shadow copy must exist. To create a shadow copy, see *Creating a Shadow Copy*.

Procedure

1. Expose the shadow copy using the following command:

   ```
   DISKSHADOW> expose <shadowID or alias> <drive letter>:
   ```

   NOTE: The command reveals the shadow ID to the operating system and assigns, in this example, the specified drive letter. See *Parameters to Expose a Shadow Copy* for other parameter options. Once the volume is exposed, a volume access group is automatically created for the local host connection.

Parameters to Expose a Shadow Copy

The following table describes the commands and sub-commands needed to expose a shadow copy using DiskShadow.

Command	Sub-command	Parameter	Description
`expose`	-	`<shadowID>`	Specifies the shadow ID of the shadow copy you want to expose.
	-	`<drive:>`	Exposes the specified shadow copy as a drive letter (for example, **P:**).
	-	`<share>`	Exposes the specified shadow copy at a share (for example, **\\MachineName**).
	-	`<mountpoint>`	Exposes the specified shadow copy to a mount point (for example, **C:\shadowcopy**).

DiskShadow Command Examples to Expose a Shadow Copy

The following example exposes a persistent shadow copy as a drive letter.

```
DISKSHADOW> set context persistent
DISKSHADOW> set verbose on
DISKSHADOW> set option differential
DISKSHADOW> add volume f: alias test
DISKSHADOW> create
Alias test for shadow ID {222a950d-6246-4596-abf1-5e52e93d308f} set as environment variable.
Alias VSS_SHADOW_SET for shadow set ID {60378cec-f336-4b22-840b-bcc3629113fa} set as environment
variable.
Inserted file Manifest.xml into .cab file 2014-12-19_24-54-55_WIN-PB674VKVN8A.cab
Inserted file Dis818B.tmp into .cab file 2014-12-19_24-54-55_WIN-PB674VKVN8A.cab
Querying all shadow copies with the shadow copy set ID {60378cec-f336-4b22-840b-bcc3629113fa}
        * Shadow copy ID = {222a950d-6246-4596-abf1-5e52e93d308f}               %test%
              - Shadow copy set: {60378cec-f336-4b22-840b-bcc3629113fa}       %VSS_SHADOW_SET%
              - Original count of shadow copies = 1
```

```
              - Original volume name: \\?\Volume{4b0e39d1-85f6-11e4-80b7-005056945388}\ [F:\]
              - Creation time: 12/19/2014 12:54:45 PM
              - Shadow copy device name: \\?\Volume{0fa0bae4-85bd-11e4-80ba-005056945388}
              - Originating machine: WIN-PB674VKVN8A
              - Service machine: WIN-PB674VKVN8A
              - Not exposed
              - Provider ID: {c60838d9-9f6f-4b67-b91b-4b87708396ce}
              - Attributes:  No_Auto_Release Persistent Hardware Differential
Number of shadow copies listed: 1
DISKSHADOW> expose %test% n:
-> %test% = {222a950d-6246-4596-abf1-5e52e93d308f}
The shadow copy was successfully exposed as n:\.
```

Unexposing a Shadow Copy

Use the DiskShadow interface according to the following procedure to request that the SolidFire VSS Hardware Provider unexpose a shadow copy.

The `unexpose` command unexposes a shadow copy that was exposed using the `expose` command. The Shadow ID, drive letter, share, or mount point can specify the exposed shadow copy. The shadow copy volume(s) are no longer exposed, but are still visible to the host as iSCSI targets. To remove these volumes from the host, see *Masking a Shadow Copy*.

Prerequisites

- A shadow copy must be exposed. To expose a shadow copy, see *Exposing a Shadow Copy*.

Procedure

1. Unexpose the shadow copy by using the following command along with the shadow ID, drive letter, share, or mount point parameter of the shadow copy.

   ```
   DISKSHADOW> unexpose {<Shadow ID> | <Drive letter>: | <Share> | <Mount Point>}
   ```

Parameters to Unexpose a Shadow Copy

The following table describes the commands and sub-commands needed to unexpose a shadow copy using DiskShadow.

Command	Sub-command	Parameter	Description
`unexpose`	-	`ShadowID`	Specifies the shadow ID of the shadow copy you want to unexpose.
	-	`<drive:>`	Unexposes the specified shadow copy as a drive letter (for example, **P:**).
	-	`<share>`	Unexposes the specified shadow copy at a share (for example, **\\MachineName**).
	-	`<MountPoint>`	Unexposes the specified shadow copy to a mount point (for example, **C:\shadowcopy**).

DiskShadow Command Examples to Unexpose a Shadow Copy

The following example unexposes a persistent shadow copy that had been exposed as a drive letter.

```
> diskshadow
```

```
DISKSHADOW> set context persistent
DISKSHADOW> set option differential
DISKSHADOW> set verbose on
DISKSHADOW> add volume i:\testvol2 alias test
DISKSHADOW> create
Alias test for shadow ID {3c2a5d1d-a64e-4a45-93c9-dd0a958cec75} set as environment variable.
Alias VSS_SHADOW_SET for shadow set ID {3602b41f-4a3c-4b78-8ab5-e0a27aee80c6} set as environment
variable.
Inserted file Manifest.xml into .cab file 2014-12-24_20-40-48_WIN-PB674VKVN8A.cab
Inserted file DisF254.tmp into .cab file 2014-12-24_20-40-48_WIN-PB674VKVN8A.cab
Querying all shadow copies with the shadow copy set ID {3602b41f-4a3c-4b78-8ab5-e0a27aee80c6}
        * Shadow copy ID = {3c2a5d1d-a64e-4a45-93c9-dd0a958cec75}               %test%
            - Shadow copy set: {3602b41f-4a3c-4b78-8ab5-e0a27aee80c6}       %VSS_SHADOW_SET%
            - Original count of shadow copies = 1
            - Original volume name: \\?\Volume{b73f02e6-8ac1-11e4-80b7-0050569422a6}\ [I:\testvol2\]
            - Creation time: 12/24/2014 8:40:45 PM
            - Shadow copy device name: \\?\Volume{b73f0388-8ac1-11e4-80b7-0050569422a6}
            - Originating machine: WIN-PB674VKVN8A
            - Service machine: WIN-PB674VKVN8A
            - Not exposed
            - Provider ID: {c60838d9-9f6f-4b67-b91b-4b87708396ce}
            - Attributes:  No_Auto_Release Persistent Hardware Differential
Number of shadow copies listed: 1
DISKSHADOW> expose %test% k:
-> %test% = {3c2a5d1d-a64e-4a45-93c9-dd0a958cec75}
The shadow copy was successfully exposed as k:\.
DISKSHADOW> unexpose k:
Shadow copy ID {3c2a5d1d-a64e-4a45-93c9-dd0a958cec75} is no longer exposed.
```

Deleting a Shadow Copy

Use the DiskShadow interface according to the following procedure to request that the SolidFire VSS Hardware Provider delete a shadow copy.

Procedure

1. Open a command prompt as Administrator and access the DiskShadow command line interface by typing `DISKSHADOW`.

   The DISKSHADOW prompt opens.

2. List all the shadow copies.

   ```
   DISKSHADOW> list shadows all
   ```

3. Delete shadow copies using the following command. Provide either the parameter `all` or any of the following additional parameters.

   ```
   DISKSHADOW> delete shadows [all | volume <Volume> | oldest <Volume> | set <SetID> | id
   <ShadowID> | exposed {<Drive> | <MountPoint>}]
   ```

   NOTE: After you delete a shadow copy, the deleted volume cannot be used by VSS but the volume is not removed immediately from the SolidFire cluster. It is purged by the system automatically based on the purge schedule. For details about purging and restoring the volume from the SolidFire cluster, see the SolidFire Element OS User Guide.

Parameters to Delete a Shadow Copy

The following table describes the commands and sub-commands needed to delete a shadow copy using DiskShadow.

Command	Sub-command	Parameter	Description
`list`	`shadows`	`all`	Lists all shadow copies.
		`set <SetID>`	Lists shadow copies that belong to the specified Shadow Copy Set ID.
		`id <ShadowID>`	Lists any shadow copy with the specified shadow copy ID.
`delete`	`shadows`	`all`	Deletes all shadow copies.
		`volume <Volume>`	Deletes all shadow copies of the given volume.
		`oldest <Volume>`	Deletes the oldest shadow copy of the given volume.
		`set <SetID>`	Deletes the shadow copies in the Shadow Copy Set of the given ID. You can specify an alias by using the `%` symbol if the alias exists in the current environment.
		`id <ShadowID>`	Deletes a shadow copy of the given ID. You can specify an alias by using the `%` symbol if the alias exists in the current environment.
		`exposed`	Deletes the shadow copy exposed at the specified drive letter or mount point. Specify mount points such as **c:\mountpoint** or by the drive letter such as **p:**.

DiskShadow Command Examples to Delete a Shadow Copy

The following example deletes a shadow copy so that it can no longer be used by VSS.

```
> diskshadow
DISKSHADOW> list shadows all
Querying all shadow copies on the computer ...
* Shadow copy ID = {fef32805-1f19-40ba-9b82-ebf277517e7e
%dbagVSS%
                - Shadow copy set: {746cea94-b814-47be-ab33-6c93b2d952a8} %VSS_SHADOW_SET%
                - Original count of shadow copies = 1
                - Original volume name: \\?\Volume{f8328660-00e6-11e6-80d9-005056bd65a9}\ [F:\]
                - Creation time: 4/13/2016 2:30:09 PM
                - Shadow copy device name: \\?\Volume{f8329046-00e6-11e6-80d9-005056bd65a9}
                - Originating machine: Reese-VSSTestVM
                - Service machine: Reese-VSSTestVM
                - Not exposed
                - Provider ID: {c60838d9-9f6f-4b67-b91b-4b87708396ce}
                - Attributes:  Transportable No_Auto_Release Persistent Hardware Imported Differential
* Shadow copy ID = {a1402b88-b823-43dc-bba6-362a180866bf} <No Alias>
                - Shadow copy set: {77625644-ec5e-4586-9f5f-5a386d898d9c} <No Alias>
                - Original count of shadow copies = 1
                - Original volume name: \\?\Volume{f8328660-00e6-11e6-80d9-005056bd65a9}\ [F:\]
```

```
                - Creation time: 4/12/2016 2:40:21 PM
                - Shadow copy device name: \\?\Volume{f83286d6-00e6-11e6-80d9-005056bd65a9}
                - Originating machine: Reese-VSSTestVM
                - Service machine: Reese-VSSTestVM
                - Exposed locally as: G:\
                - Provider ID: {c60838d9-9f6f-4b67-b91b-4b87708396ce}
                - Attributes:  Transportable No_Auto_Release Persistent Hardware Imported Differential
Number of shadow copies listed: 2

DISKSHADOW> delete shadows set {746cea94-b814-47be-ab33-6c93b2d952a8}
Deleting shadow copy set {746cea94-b814-47be-ab33-6c93b2d952a8}...
Number of shadow copies deleted: 1
DISKSHADOW> list shadows all
Querying all shadow copies on the computer ...
* Shadow copy ID = {a1402b88-b823-43dc-bba6-362a180866bf} <No Alias>
                - Shadow copy set: {77625644-ec5e-4586-9f5f-5a386d898d9c} <No Alias>
                - Original count of shadow copies = 1
                - Original volume name: \\?\Volume{f8328660-00e6-11e6-80d9-005056bd65a9}\ [F:\]
                - Creation time: 4/12/2016 2:40:21 PM
                - Shadow copy device name: \\?\Volume{f83286d6-00e6-11e6-80d9-005056bd65a9}
                - Originating machine: Reese-VSSTestVM
                - Service machine: Reese-VSSTestVM
                - Exposed locally as: G:\
                - Provider ID: {c60838d9-9f6f-4b67-b91b-4b87708396ce}
                - Attributes:  Transportable No_Auto_Release Persistent Hardware Imported Differential
Number of shadow copies listed: 1
```

Appendix A — Provider Event Logs

The SolidFire VSS Hardware Provider creates detailed logs of system activities. You can monitor the events performed on the system using the Event Viewer. Messages are displayed as they occur in a system and are logged to **Windows Logs > Application**. For every event, the following information is returned.

Event Type	Description
Level	Indicates the event severity. Levels include Information, Error, or Warning.
Date and Time	Indicates the date and time of the event.
Source	Indicates the source of the event. All logs generated by the Provider have the source *VssSolidFireProvider*.
Event ID	Unique event ID associated by level of event.
Task Category	Message associated with the event.
Details	Information that helps identify why the event occurred.

NOTE: Event logs can be exported and saved in `.csv` or `.txt` format from the Event Viewer.

Appendix B — Provider Event Details

The following table describes system messages that are logged to the Event Viewer in Windows.

Log Entry Type	Message	Detailed Description	Resolution
Warning	`An unsupported VSS operation was called: {0}`	A VSS provider operation was called that is not currently supported by the provider. Specifically, this event is logged if the VSS provider receives a LUN state change request other than a supported masking change.	Generally, no action needs to be taken. If this message occurs alongside a failure of a shadow copy operation, contact SolidFire support for assistance.
Warning	`Cluster [{clusterName}] was not placed in the upgraded configuration because it is a duplicate of another cluster.`	Due to an issue in the earlier 1.1.x version of the VSS Hardware Provider, it is possible in certain rare scenarios to have multiple cluster configurations that refer to the same cluster. If this occurs, one of the duplicate entries will be discarded during an upgrade to version 2.0.x and this message will be logged.	Generally, no additional action should need to be taken. You can review the cluster configurations in the 2.0 configuration tool and ensure that the MVIP address and credentials of the affected cluster are correct.
Warning	`Cannot create shadow copy for volume [{volumeName}] on cluster [{clusterName}] because it has reached the maximum number of snapshots.`	SolidFire clusters support a maximum of 32 snapshots for each storage volume on the cluster. This message is logged if VSS tries to create a shadow copy of one or more volumes after the maximum number of snapshots has been reached. This occurs for plex (clone) as well as differential (snapshot) shadow copies because the VSS provider uses snapshots as an interim step in creating a volume clone.	Reduce the number of snapshots of the affected volume(s) and retry the shadow copy creation operation.

Log Entry Type	Message	Detailed Description	Resolution
Warning	`Unable to connect to cluster with id: [{clusterId}]: No configuration found.`	The Provider cannot connect to the cluster that hosts one or more of the volumes to be shadow copied because the cluster has not been added to the SolidFire VSS Hardware Provider configuration.	Use the SolidFire VSS Hardware Provider configuration tool to add the cluster that hosts the volumes you need to shadow copy.
Warning	`Unable to connect to cluster with id: [{clusterId}]: Unable to validate credentials on remote: {clusterAddress}.`	The credentials are not valid for a cluster that is hosting one or more of the volumes to be shadow copied. The administrative username or password on the cluster might have changed.	Use the SolidFire VSS configuration tool to verify that the username and password for the cluster are correct.
Warning	`Unable to connect to cluster with id: [{clusterId}]: Unable to reach remote: {clusterAddress}.`	The provider is unable to connect to the specified cluster using the cluster's management virtual IP (MVIP) address. There might be a network issue or the MVIP address for the cluster might have changed.	Verify network connectivity between the host with the Provider and the cluster's MVIP address. Use the SolidFire VSS Hardware Provider configuration tool to verify that the configured MVIP address is correct.
Warning	`Unable to connect to cluster with id: [{clusterId}]: Request was cancelled or timed out. Timeout is currently set at {timeout} secs.`	A timeout occurred while waiting for one or more of the SolidFire clusters to respond to a communication request. The network might be congested or the SolidFire cluster might be having difficulty responding to requests in a timely manner.	Verify that no network issues are present between the host with the Provider and the SolidFire cluster. Contact SolidFire support if the cluster does not respond to requests in a timely manner.

Log Entry Type	Message	Detailed Description	Resolution
Warning	`Unable to locate one or more volumes for import.`	When trying to import a shadow copy set, this warning will be generated if the provider cannot locate one or more of the shadow copy set's snapshots or clones. The missing volume or snapshot might have been manually deleted from the cluster. This warning will also be generated when you try to import a shadow copy set that has already been deleted through VSS.	Verify that the shadow copy set being imported was not already deleted, either through VSS or manually.
Warning	`Unable to locate one or more volumes for resync.`	One or more of the source/target volumes specified for a resync operation could not be located by the provider. The volume(s) might have been deleted.	Ensure that the specified source shadow copy or copies still exist.
Warning	`Failed to connect iSCSI target [{target}] using initiator portal [{initiatorPortal}] and target portal [{targetPortal}]. Details: {exception}`	During an import, a connection cannot be established to an import volume using the specified initiator and target addresses. This is a warning because there might be other initiator/target portal pairs that connect successfully. This warning should only occur if there are intermittent network issues between the initiator and cluster targets, or if a firewall between them is blocking iSCSI traffic.	Check for network issues and ensure iSCSI traffic is not blocked by a firewall. Contact SolidFire support with exception details if the issues cannot be resolved.
Error	`An unhandled exception occurred: {0}`	An unexpected error was encountered by the Provider, and it cannot continue the current operation.	Contact SolidFire support with details of the exception for further assistance.

Log Entry Type	Message	Detailed Description	Resolution
Error	`Unable to obtain iSCSI IQN for the current machine. Ensure that the Microsoft iSCSI Initiator Service is running.`	The Provider tries to import one or more shadow copies using the iSCSI protocol, but the import host does not have iSCSI configured.	Use the iSCSI control panel to ensure that the Microsoft iSCSI Initiator Service is enabled and running.
Error	`Unable to find source snapshot for imported clone [{cloneName}] on cluster [{clusterName}]`	The source snapshot for a differential shadow copy could not be found after an on-demand clone was unmasked to an import host. This error should only occur if the snapshot is manually deleted during an import operation.	Do not manually delete a shadow copy snapshot while an import operation is in progress.
Error	`Unable to resync from volume [{cloneName}] because resync from clones is not currently supported.`	The source shadow copy specified in a resync operation was a plex (clone) shadow copy. Resync from plex shadow copies is not currently supported.	Resync from a differential (snapshot) shadow copy or perform a host-based restore from the imported clone.
Error	`Unable to resync volume [{volumeName}] from snapshot [{snapshotName}] because the snapshot was not created from that volume.`	The source shadow copy specified in a resync operation was created from a different volume than the one specified as the target of the resync.	Ensure that the source shadow copy for a resync was created from the specified target volume.
Error	`Unable to connect any iSCSI sessions for target [{target}].`	During an import, iSCSI sessions cannot be created from the import host to the target cluster. This is usually due to a network failure or configuration issue.	Ensure that there is network connectivity from the import host to at least one storage virtual IP (SVIP) on the cluster.

Log Entry Type	Message	Detailed Description	Resolution
Error	`The clusterinfo.xml file is invalid: {exceptionMessage} A new clusterinfo.xml file will be created and the old one renamed with an .invalid extension.`	The configuration file is invalid. The likely cause is that the public/private key pair used to encrypt sensitive data in the file is not available. This occurs if the file is copied from one host to another or the host has been sysprepped. This message can also occur if the file is deleted while the configuration tool is running or edited by hand incorrectly.	If the error is encountered while using the configuration tool, the tool will close and a new empty configuration file will be created when the tool is opened again. If the error is encountered by the Provider during processing of a VSS operation, a new empty configuration file will be created and the VSS operation will fail because there are no configured clusters. The configuration tool must be used to re-register any SolidFire clusters.
Error	`Product: SolidFire VSS Hardware Provider -- Error 1722. There is a problem with this Windows Installer package. A program run as part of the setup did not finish as expected. Contact your support personnel or package vendor. Action RunInstallScript, location: C:\Program Files\SolidFireVSS\, command: cmd /c install-solidfireprovider.cmd > install.log`	The **`.msi`** installer cannot resolve the install path while installing or uninstalling the Provider.	Add the install path location of the SolidFire VSS Provider to the environment variable as follows: 1. Go to **Control Panel > All Control Panel Items > System**. 2. In the **Advanced System Settings**, select **Advanced > Environment Variables**. 3. From the **System variables** select the ***Path*** variable and click **Edit**. 4. At the end of the variable value, append the installation path. For example, `C:\Program Files\SolidFireVSS`. 5. Click **OK**. 6. Start the **`.msi`** and uninstall or install the product

Log Entry Type	Message	Detailed Description	Resolution
Error	`The operating system returned error 21(The device is not ready.) to SQL Server during a read at offset 0x000000000e8000 in file 'N:\tempdb.mdf'.`	While performing a resync shadow copy, the database goes into the restoring state and displays the error message in the Event viewer. Additional messages in the SQL Server error log and system event log may provide more detail. This is a severe system-level error condition that threatens database integrity and must be corrected immediately.	Complete a full database consistency check (DBCC CHECKDB). This error can be caused by many factors. For more information, see SQL Server Books Online. During resync, the temporary location is not available to the database. The tempdb system database is a global resource that is available to all users connected to the instance of SQL Server. By default, the tempdb database is created in the same location as master, model and msdb. The tempdb is used to store temporary user created objects, temporary internal objects, and any row version data. Each time the SQL Server is started, all the objects in tempdb are deleted but the file sizes are retained. To increase performance or deal with file size issues, it is recommended to move the tempdb to any other location. Backup and restore operations are not allowed on tempdb. Move the tempdb location to any location other than the snapshot volume (such as Database volumes). This new location can be a SolidFire volume.

Appendix C — Snapshot and Clone Naming

Snapshot and clone names can be customized using the configuration tool. Names use the following format that includes two hyphens for a total value length of 64:

Type	Format	Example
Snapshot	<Prefix>-vol<Volume ID>-<Snapshot Set GUID>	DENSQL001A-vol10-af12be56
Clone (plex shadow copy)	<Prefix>-vol<Volume ID>-<Snapshot Set GUID>	DENSQL001A-vol10-af12be56
Clone (differential shadow copy)	<Prefix>-snap<Volume ID>-<Snapshot Set GUID>	DENSQL001A-snap10-af12be56

The following elements are used in snapshot and clone naming:

Element	Description	Maximum Value Length
`<Prefix>`	The user defined prefix for snapshots and clones. If you do not specify prefixes, a system default prefix is substituted that is based on the NetBIOS host name.	30
`<Volume ID>`	The volume ID of the SolidFire volume. For snapshots and plex shadow copies, the source volume ID is used. For differential shadow copies, the snapshot volume ID is used.	26 including "vol" or "snap"
`<Snapshot Set GUID>`	The last eight characters of the snapshot set globally unique identifier (GUID).	8

Appendix D — Removing the VSS Hardware Provider

In Windows, use the **Programs and Features** option in the **Control Panel** to remove the SolidFire VSS Hardware Provider software. When you remove the Provider, it is removed from the registry and associated files for the configuration tool and Provider are deleted.

NOTE: The encrypted file (`C:\ProgramData\SolidFire\Vss\clusterinfo.xml`) that stores cluster connection credential metadata is not removed during the uninstall process and must be removed manually by the admin.

Appendix E — Glossary

C

Clone
An exact read/write copy of volume data in a storage system.

Cluster
A contiguous group of nodes on a storage system.

D

Differential
This is the default snapshot type when a shadow copy is created. Creates a point-in-time snapshot of specified volumes on the SolidFire cluster. A volume clone based on this snapshot will be created during an import operation.

DiskShadow
A utility that uses commands from a CLI to expose VSS functionality.

G

GUID
Globally Unique Identifier.

M

Management Virtual Internet Protocol
A 1GbE Management Network used for API traffic.

MVIP
See Management Virtual Internet Protocol

P

Plex
A Plex shadow copy is a point-in-time clone copy of the data on a specified volume.

Provider
SolidFire VSS Hardware Provider

S

Shadow copy
A consistent, point-in-time volume backup copy that can be created as importable onto servers within a shared subsystem, for example, SAN. A transportable shadow copy can be moved from one system to another and typically is not surfaced locally.

Shadow copy set
A collection of shadow copies of selected volumes that were all taken at the same moment. VSS identifies shadow copy sets by persistent GUID.

Snapshot
Point-in-time image of volume metadata in a storage system.

Storage Virtual Internet Protocol
A 10GbE iSCSI connection that enables VLAN connection to storage devices.

SVIP
Storage Virtual Internet Protocol

T

tempdb
A system database that is available to users connected to a SQL server that contains temporary user objects, internal objects, and row versions.

U

UI
User interface

V

VSS
Microsoft Volume Shadow Copy Service

VSS Provider
A storage level component that offers functionality to create a shadow copy of one of more volumes.

VSS Requester
Application that initiates the creation of a shadow copy.

VSS Writer
Application-specific software that ensures application data is ready for shadow copy creation.

SOLIDFIRE
1600 Pearl Street, Suite 200
Boulder, Colorado 80302

Phone: 720.523.3278
Email: info@solidfire.com

Web: www.solidfire.com

SolidFire Support: www.solidfire.com/support/

4/26/16