Abstract
This document provides best practices for configuring Microsoft® Windows Server® 2016 hosts with Dell EMC™ SC Series SAN arrays.
November 2017
Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2016</td>
<td>Initial release</td>
</tr>
<tr>
<td>November 2016</td>
<td>Updated to include BitLocker content</td>
</tr>
<tr>
<td>February 2017</td>
<td>Updated MPIO best practices</td>
</tr>
<tr>
<td>November 2017</td>
<td>Updated guidance on support for Nano Server</td>
</tr>
</tbody>
</table>

Acknowledgements

Updated by: Marty Glaser

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

© 2016-2017 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.
Table of contents

<table>
<thead>
<tr>
<th>Revisions</th>
<th>Acknowledgements</th>
<th>1 Introduction</th>
<th>2 Overview</th>
<th>3 Configuring SC Series volumes for Windows servers</th>
<th>4 Mapping SC Series LUNs to Windows Server 2016</th>
<th>5 Host bus adapter settings</th>
<th>6 Boot from SAN</th>
<th>7 Microsoft Hyper-V</th>
<th>8 Windows Failover Clustering</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1.1 Audience</td>
<td>2.1 SC Series overview</td>
<td>3.1 Data Progression</td>
<td>4.1 Transport options</td>
<td>5.1 Configure Fibre Channel HBAs</td>
<td>6.1 Configure Windows Server hosts to boot from SAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.2 Prerequisites</td>
<td>2.2 Windows Server 2016 overview</td>
<td>3.2 Choosing a storage profile</td>
<td>4.2 Multipath I/O</td>
<td>5.2 Queue depth and timeouts</td>
<td>6.1.1 Create the server object</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2.3 Nano Server</td>
<td></td>
<td></td>
<td>5.2.1 When to change queue depth</td>
<td>6.1.2 Map the boot volume to the server</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5.2.2 Vendor-specific HBA and CNA queue depth settings</td>
<td>6.1.3 Configure QLogic Fibre Channel HBAs to boot from SAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5.2.3 MPIO timeout settings</td>
<td>6.1.4 Configure QLogic iSCSI HBAs to boot from SAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6.1.5 Change the operating system definition in the SC Series array</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6.1.6 Configure each Fibre Channel HBA port in the server to boot from SAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8.1 Overview</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8.2 Cluster shared volumes (CSVs)</td>
<td></td>
</tr>
<tr>
<td>8.2.1 Cluster server objects with DSM</td>
<td>.................................................................................................................19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.2.2 Mapping SC Series volumes to clustered server object in DSM</td>
<td>.................................................................................................................20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 Offloaded data transfer (ODX)</td>
<td>.................................................................................................................21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 Thin provisioning and TRIM/Unmap</td>
<td>.................................................................................................................22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11 Resilient file system (ReFS)</td>
<td>.................................................................................................................23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.1 Using ReFS on SC Series volumes</td>
<td>.................................................................................................................23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12 Volume Shadow Copies</td>
<td>.................................................................................................................24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.1 Dell Storage Replay Manager</td>
<td>.................................................................................................................24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13 Volume maintenance</td>
<td>.................................................................................................................25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14 Using BitLocker with SC Series volumes</td>
<td>.................................................................................................................27</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 Dell Storage PowerShell SDK</td>
<td>.................................................................................................................29</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A Additional resources</td>
<td>.................................................................................................................30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.1 Technical support and resources</td>
<td>.................................................................................................................30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.2 Related documentation</td>
<td>.................................................................................................................30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Introduction

1 Introduction

Dell EMC™ SC Series arrays are designed from the ground up with redundancies to avoid downtime for such events as component failures, maintenance, upgrades, and expansion — redundancies which benefit Microsoft® Windows Server® systems and their respective workloads. Windows Server also includes similar features to SC Series arrays, and when integrated, the two feature sets complement each other.

There are several other means of presenting storage to a Microsoft Windows® server, such as traditional on-board storage in physical servers. Another method is Microsoft Storage Spaces, which was introduced with the initial release of Windows Server 2012. Storage Spaces Direct and Storage Replica were introduced with Windows Server 2016. While Storage Spaces, Storage Spaces Direct, and Storage Replica offer similar basic features as traditional SAN arrays, the SC Series SAN provides a much more powerful and complete set of integrations, management, and monitoring tools that are not available with Storage Spaces or Storage Replica alone.

1.1 Audience
This document was written for technology professionals interested in learning more about best practices for configuring Windows Server 2016 hosts with SC Series SAN arrays.

1.2 Prerequisites
Understanding the material in this document requires advanced working knowledge of the following:

- Installation and configuration of Windows Server 2016
- Configuration and operation of the SC Series
- Operation of Dell Storage Manager (DSM) software

Note: Support for Nano Server as an OS for physical hosts or VMs was discontinued by Microsoft with the 1709 (September 2017 semi-annual update) release of Windows Server 2016. Nano Server is now supported as a container OS only.
2 Overview
This section provides a brief overview for SC Series storage and Microsoft Windows Server 2016.

2.1 SC Series overview
SC Series storage solutions provide many robust features such as true flash optimization, thin provisioning, data optimization, data reduction (compression and deduplication), automated sub-LUN tiering, sub-disk RAID levels, synchronous replication with Live Volume automatic failover, federation, and intelligent read and write data placement. SC Series arrays provide a robust platform for the ultimate experience in performance, adaptability, and efficiency.

In addition to raw capacity and I/O performance, other important factors such as monitoring, reporting, data protection (backups, snapshots/replays, and replication), and the ability to recover in case of a disaster are equally important. The SC Series array is well suited to provide a solid, proven storage solution for Windows Server environments to meet all of these business needs. To learn more about specific SC Series storage arrays, visit the SC Series product page.

2.2 Windows Server 2016 overview
Microsoft designed Windows Server 2016 to be the primary operating system in the data center. Windows Server 2016 includes security improvements, more robust software-defined infrastructure offerings (compute, storage, and network virtualization), and new application deployment features not found in previous versions of Windows Server.

Windows Server 2016 includes updates and improvements to many core Windows Server features, such as failover clustering, Microsoft Hyper-V®, Microsoft Active Directory®, and server administration.

Any new or updated features, as they relate to integration with SC Series storage, are discussed throughout this document.

For a complete list of new features and improvements in Windows Server 2016, refer to appendix A.

2.3 Nano Server
Nano Server was a previous deployment option for Windows Server 2016 on physical hosts or VMs. With the release of the 1709 version (September 2017 semi-annual update) of Windows Server 2016, support for Nano Server as a physical or virtual server OS was discontinued. Nano Server will continue to be supported as a container OS only. This change by Microsoft does not affect Dell SC Series continued support for Windows Server 2016 Core and Desktop versions.

For more information about Nano Server, refer to Microsoft TechNet.
Configuring SC Series volumes for Windows servers

3.1 Data Progression
Data Progression is a core SC Series feature with tiered storage. With Data Progression, data is automatically and intelligently placed in the optimal storage tier and RAID level based upon usage and performance metrics. Data Progression runs, by default, nightly at 7:00 p.m.

**Note:** As a Data Progression best practice, apply at least one snapshot profile to each volume with a snapshot expiration of at least 25 hours. The Data Progression process will not work optimally for a volume unless the volume has at least one unexpired snapshot available at the time Data Progression runs.

3.2 Choosing a storage profile
Storage profiles define the RAID level used to protect data on a volume and the tiers where that data is stored. The information in the profile is used by Data Progression when moving existing data pages, as well as by new SC Series data pages. For most Windows Server environments, when creating a new volume, use the default storage profile **Recommended (All Tiers)** to provide good I/O performance and protection for the volume. It is strongly recommended to use this storage profile first and evaluate its suitability before attempting to change the storage profile.

![Storage profile selection](image-url)
3.3 Data reduction (compression and deduplication)

Released with Storage Center OS (SCOS) 7.0, the data reduction feature takes advantage of both compression and deduplication for reducing the data footprint of a volume. As part of its daily processing cycle, Data Progression deduplicates and compresses the data within volumes that have the data reduction feature enabled. Depending on the data reduction policy set on a particular volume, the data can either be compressed, or deduplicated and compressed for maximum savings.

![Create Volume](image.png)

Figure 2 Data reduction options

**Note:** Before enabling data reduction on volumes, first obtain SC Series performance benchmarks, and then enable data reduction on a few volumes at a time to ensure that adequate system performance is maintained. Data reduction consumes additional SC Series processor resources during the daily Data Progression cycle, but this impact is minimized when Data Progression is scheduled to run outside of peak hours at a time when the workload will be minimally impacted. Modify the daily Data Progression start time if desired.

The advanced options available in the volume settings offer control over the data reduction input, which consists of pages an administrator deems eligible for data reduction. The choice between inaccessible snapshot pages and all snapshot pages is effectively a tradeoff between maximum savings and maximum performance.
3.4 Configuring data reduction

Within the advanced volume settings, the Data Reduction Input setting can be specified to control which pages are eligible for data reduction.

![Advanced Volume Settings](image)

**Figure 3** Advanced volume settings

**All Snapshot Pages:** All frozen pages in the lowest tier of the system that are part of a snapshot (replay), are eligible for data reduction. In the case of a single tiered system, such as a replication target system, all frozen pages are eligible. This setting yields the highest reductions, however there is a performance tradeoff of higher latency due to any accessed pages being decompressed as they are accessed.

**Inaccessible Snapshot Pages:** Only frozen inaccessible pages are eligible for data reduction. These are pages kept only as part of a snapshot for recovery purposes, and are not accessible by the host. This setting yields the lowest reductions, however it has the best performance since no host-accessible pages are compressed or deduplicated.

**Caution:** When initially enabling compression on a system, the Data Progression total running time may be extended and could result in the cycle continuing into regular business hours. It is recommended that administrators adjust the Data Progression settings within the system settings to limit the maximum run time, or limit the number of volumes to be reduced each day.

For more information about the data reduction feature, refer to the best practices guide, *Dell Storage Center OS 7.0 Data Reduction with Deduplication and Compression*. 
4  Mapping SC Series LUNs to Windows Server 2016

An SC Series LUN can be mapped directly as a boot-from-SAN volume to a Windows Server 2016 host, or as a standard disk available to the operating system.

When SC Series LUNs are mapped to Windows Server 2016 hosts, they are identified by the operating system as disks. Once the disks are brought online and initialized, a volume can be created on the disk that contains a file system.

4.1  Transport options

SC Series LUNs can be mapped directly to Windows Server 2016 hosts using Fibre Channel, iSCSI, or front-end SAS. Each transport option allows for the use of Multipath I/O (MPIO) to facilitate failover and load balancing.

Note: SC Series arrays support using mixed transports (such as Fibre Channel and iSCSI) at the same time to map LUNs to host servers. However, Windows Server 2012 R2 and newer do not support using mixed transports. If more than one transport is used, the Windows Server host will default to one type of transport or the other based on an enumeration algorithm which typically results in the host choosing the Fibre Channel paths over the iSCSI paths. If all paths for one transport go down, the server may not send data using the other transport without a disk re-scan. Using a single type of transport per volume should provide sufficient bandwidth and MPIO capability.

4.2  Multipath I/O

Windows Server 2016 natively supports MPIO by way of a Device Specific Module. MPIO is set up as a feature in the OS and must be enabled to work with the specific volumes that have multiple paths to the SAN. The process is very straightforward and simple to implement.

The main purpose of MPIO is to provide redundant paths for a server to access storage. With multipath, if one path goes down, another path is able to provide connectivity to prevent a service outage. MPIO also allows for load-balancing so that the I/O is spread across the available paths.

Note: Dell EMC recommends using MPIO on all versions of Windows Server.

For more information on how to install and configure MPIO on Windows Server 2016 and SC Series volumes, refer to the guide, Dell EMC SC Series Storage: Microsoft Multipath I/O Best Practices.
5 Host bus adapter settings

Windows Server 2016 host bus adapters (HBAs) should be configured using best practices. In a failover scenario, improperly configured HBAs can cause unpredictable results, including LUN path loss, data loss, and server failure. The current recommended settings are:

- QLogic® Fibre Channel HBAs: Recommended settings are detailed in section 5.1.
- QLogic iSCSI HBAs: The ARP redirect must be enabled for controller failover to work properly with hardware iSCSI HBAs.
- SAS HBA card BIOS settings: For SC Series arrays configured with SAS front-end ports, factory default settings within the card BIOS are recommended for SAS Windows Server host HBAs.

5.1 Configure Fibre Channel HBAs

QLogic HBAs can be configured using QLogic Fast!UTIL, which is accessible during the server boot cycle.

To configure Fibre Channel HBAs using QLogic Fast!UTIL, perform the following steps:

1. Reboot the server and press [Ctrl-Q] when prompted to enter QLogic Fast!UTIL.
2. In Select Host Adapter, select the first port in the list and press Enter.
3. Reset the HBA port to factory defaults:
   a. In Fast!UTIL Options, select Configuration Settings and press Enter.
   b. In Configuration Settings, select Restore Default Settings and press Enter.
   c. After Adapter Defaults Restored is displayed, press any key to return to the Configuration Settings screen.
4. Set the parameters on the HBA port according to best practices:
   a. In Configuration Settings, select Adapter Settings and press Enter.
   b. In Adapter Settings:
      i. Set Host Adapter BIOS to Enabled.
      ii. Set Connection Options to 1 (Point to point only).
      iii. Press Esc to exit Adapter Settings.
   c. In Configuration Settings, select Advanced Adapter Settings and press Enter.
   d. In Advanced Adapter Settings:
      i. Set Enable LIP Reset to Yes.
      ii. Set Enable LIP Full Login to Yes.
      iii. Set Login Retry Count to 60.
      iv. Set Port Down Retry Count to 60.
      v. Set Link Down Timeout to 30.
      vi. Set Execution Throttle to 256.
      vii. Press Esc to exit Advanced Adapter Settings.
   e. Press Esc to exit Configuration Settings. When prompted, select Save Changes and press Enter.
5. In Fast!UTIL Options, click Select Host Adapter and press Enter.
6. In Select Host Adapter, select the next port in the list and press Enter.

Using the instructions in steps 3 and 4, reset the port to factory defaults and set the parameters as listed. Repeat these steps until all HBA ports on the system have been configured.
5.2 **Queue depth and timeouts**

Queue depth is defined as the total number of disk transactions that are allowed to be in flight between an initiator (a port on the host server) and a target (a port on the storage array). The initiator is typically a Windows Server HBA FC or iSCSI port, and the target is an FC or iSCSI port on the SAN array. Since any given target port can have multiple initiator ports sending it data, the initiator queue depth is generally used to throttle the number of transactions any given initiator can send to a target from a host to prevent the target from becoming flooded. When flooding happens, the transactions are queued, which can cause higher latencies and degraded performance for the affected workloads.

5.2.1 **When to change queue depth**

One question that is commonly asked is when to change queue depth settings for Windows Server hosts. On a Windows Server, queue depth is a function of the Microsoft storport.sys driver and the vendor-specific miniport driver for the FC HBA, iSCSI NIC, or CNA.

In many cases, there is no need to change the default queue depth, unless there is a specific use case where changing the queue depth is known to improve performance. For example, if a storage array is connected to a small number of Windows Server hosts with large block sequential read application workloads, increasing the queue depth setting may be very beneficial. However, if the storage array has many hosts all competing for a few target ports, increasing the queue depth on a few hosts might overdrive the target ports and negatively impact the performance of all connected hosts.

While increasing the queue depth can sometimes increase performance significantly for specific workloads, if it is set too high, there is an increased risk of overdriving the target ports on the storage array. Generally, if transactions are being queued and performance is being impacted, and increasing the queue depth results in saturation of the target ports, then increasing the number of target ports to spread out I/O can be an effective remediation.

5.2.2 **Vendor-specific HBA and CNA queue depth settings**

It is important to understand the firmware and miniport driver registry settings for your host server FC HBA, iSCSI NIC, or CNA adapter and how these settings affect queue depth. In the case of QLogic FC HBAs for example, the execution throttle setting can be adjusted to control queue depth.

See the documentation for your particular FC HBA, iSCSI NIC, or CNA for direction on adjusting firmware or registry settings to modify queue depth. For example, see this [QLogic support article](#) which explains in detail the relationship between the Windows Server storport.sys driver and the vendor-specific miniport driver, and how to modify parameters that affect queue depth by editing registry keys or firmware settings.

**Note:** Changes to firmware or registry settings that affect queue depth should be evaluated in a test environment prior to implementation on production workloads.
5.2.3 MPIO timeout settings
Along with queue depth, disk timeout and failover behavior settings are also important considerations in a SAN environment, and are modified through the Windows Server registry. It is essential in a SAN environment to modify specific timeout settings to permit volumes to stay online during routine operations such as a SAN controller firmware upgrade. In other words, some Windows Server default timeout settings are too short for a SAN environment and will result in service interruptions during routine SAN maintenance if they are not changed. For detailed information on how to make the necessary registry changes, refer to the document, *Dell EMC SC Series Storage: Microsoft Multipath I/O Best Practices*.

**Caution:** Failure to modify the default MPIO timeout values on a Windows host connected to SAN storage may result in service interruptions and possible data loss during routine SAN maintenance that would otherwise be non-service-affecting maintenance.
Boot from SAN

In some cases, such as blade servers that do not have onboard disks, booting from SAN may be the only option available. Many physical Windows Server hosts have internal drives providing the ability to boot locally or from an SC Series array. Deciding which option to use is dependent on a number of design considerations that are unique to each environment. There are advantages and disadvantages to both options, and in some cases, using local disk is preferred.

Boot from SAN advantages:

- SC Series array snapshots of boot volumes provide for quick recovery.
- Replicating boot volumes to another SC Series array at remote location enables enhanced disaster recovery (DR) protection when both sites use similar hardware for server hosts.
- SC Series array gold image boot volumes can be leveraged to quickly provision new Windows Server hosts.

Boot from local disk use cases:

- Use when critical roles such as a backup domain controller need to remain online during offline SAN maintenance or unplanned outages. However, Live Volume with automatic failover can help ensure that critical roles stay online when there is more than one SC Series array available.
- Use with the DSM Data Collector, which should ideally be on a server with local boot and data disks so it remains available regardless of the state of the SC Series array.

6.1 Configure Windows Server hosts to boot from SAN

Windows Server hosts (Core and Desktop) can be configured to boot from SAN using physical Fibre Channel or iSCSI HBAs. This section details how to map a boot volume to a Windows Server 2016 host, and configure QLogic Fibre Channel and iSCSI HBAs to boot from SAN.

Note: Refer to the HBA manufacturer documentation for configuring boot from SAN with other supported HBAs that are listed on the SC Series hardware compatibility matrix.

6.1.1 Create the server object

A server object is used when presenting storage to a server. To create the server object, perform the following steps:

1. Connect to the SC Series array using the DSM client.
2. Select the Storage tab.
3. Right-click Servers and select Create Server. The Create Server dialog box appears.
4. In the Name textbox, enter the name of the server.
5. In the Operating System drop-down list, select Windows 2016 Single path. This setting will be changed to Server 2016 MPIO later on after MPIO is installed on the host.
6. Select all of the host server Fibre Channel or iSCSI HBA ports associated with this host. This assumes that the host is powered on, and networking and fabric configurations are in place to allow the SC Series array to see the available server ports.
7. Click OK.
6.1.2 Map the boot volume to the server

Since the server is not yet configured to use **Server 2016 MPIO** in DSM, only one path will be created for the boot volume initially. The operating system definition should be changed to the MPIO version in DSM once Windows has been installed and MPIO has been configured.

**Note:** When configuring a server to boot from SAN, map the boot volume to the server and install the operating system and configure MPIO before mapping any other volumes to the server.

To map the boot volume to the server, perform the following steps:

1. Connect to the SC Series array using the DSM client.
2. Select the **Storage** tab.
3. Expand the **Volumes** tree.
4. Right-click the boot volume and select **Map Volume to Server**.
5. Select the server and click **Next**.
6. Click **Advanced Options**.
7. Select **Map volume using LUN 0**.
8. Click **Finish**.

6.1.3 Configure QLogic Fibre Channel HBAs to boot from SAN

As this point, only one path exists for the LUN mapping between the server HBA and the boot-from-SAN volume. The HBA port for that path needs to be configured to boot from SAN. Once the server is configured to use MPIO, the steps in this section need to be repeated to configure each HBA port to boot from SAN.

To configure the HBA port to boot from SAN using QLogic Fast!UTIL, perform the following steps:

1. Reboot the server and press **[Ctrl-Q]** when prompted to enter **QLogic Fast!UTIL**.
2. In Fast!UTIL Options, click Select Host Adapter and press Enter.
3. In **Select Host Adapter**, select the first port in the list and press **Enter**.
4. In Fast!UTIL Options, select Scan Fibre Devices and press Enter.
   - If a device is displayed, this is the port used for the boot volume.
   - If a device is not displayed:
     i. Go back and select the next port in the host adapter list and scan for devices.
     ii. Keep repeating until the scan displays a device.
     iii. Once the port for the boot volume is discovered, press **Esc** to exit **Scan Fibre Devices**.
5. In Fast!UTIL Options, select Configuration Settings and press Enter.
7. In Selectable Boot Settings:
   a. Set Selectable Boot to **Enabled**.
   b. Select the first boot port entry and press **Enter**.
   c. Select the boot device from the list and press **Enter**.
   d. Press Esc to exit Selectable Boot Settings.
8. Press **Esc** to exit **Configuration Settings**. When prompted, select **Save changes** and press **Enter**.
9. Press **Esc** to exit Fast!UTIL. When prompted, select **Reboot System** and press **Enter**. The server will reboot. Ensure that bootable media is presented to the server so the OS can be installed.
6.1.4 Configure QLogic iSCSI HBAs to boot from SAN

The following steps show how to configure a Windows Server host to boot from SAN using a QLogic iSCSI HBA card. In this example, a single path will be configured. If MPIO is desired, once the OS has been loaded, enable the MPIO feature and repeat the following steps to enable a second iSCSI path, and then configure MPIO settings.

1. Reboot the server and press [Ctrl-Q] when prompted to enter QLogic Fast!UTIL.
2. If there are multiple iSCSI adapters listed, select the desired adapter to configure.
3. From the Fast!UTIL Options menu, select Configuration Settings and press Enter.
4. In Configuration Settings, select Host Adapter Settings and press Enter.
5. In Host Adapter Settings, select Initiator IP Settings and press Enter.
6. In Initiator IP Settings set the IP Address, Subnet Mask, and Gateway.
7. Press Esc to exit Host Adapter Settings.
8. In Configuration Settings, select Initiator iSCSI Name and press Enter.
9. Set the Initiator iSCSI Name and press Enter.
10. Press Esc to exit Initiator iSCSI Name.
11. Set Spinup Delay to Disabled.
12. Press Esc to return to Configuration Settings.
13. Select iSCSI Boot Settings and press Enter.
15. Select Primary Boot Device Settings and press Enter. Set the following:
   a. Set Use IPv4 or IPv6 to IPv4.
   b. Set Target IP to the IP Address of the iSCSI controller of the SC Series.
   c. Set Target Port to 3260.
   d. Set Boot LUN to 0.
   e. Set iSCSI Name to the name of the iSCSI controller of the SC Series.
16. Press Esc to return to iSCSI Boot Settings.
17. Select Primary Boot Device and press Enter.
18. In Select iSCSI Device select ID 0 and press Enter.
19. Press Esc to return to iSCSI Boot Settings.
20. Press Esc to return to Configuration Settings.
21. Press Esc and select Save changes.
22. Reboot the host server and install the OS.

If MPIO is desired, install the MPIO feature, repeat the previous steps to enable a second iSCSI path, and configure MPIO settings. For more information on MPIO, see the guide, Dell EMC SC Series Storage: Microsoft Multipath I/O Best Practices.
6.1.5 Change the operating system definition in the SC Series array
Once the operating system is installed and MPIO is configured, the SC Series server object will need to be changed to use the MPIO version of the operating system definition. The will allow volume mappings to use all available paths.

To change the operating system definition of the server object, perform the following steps:

1. Connect to the SC Series array using the DSM client.
2. Click the Storage tab.
3. Expand the server folder that contains the server object.
4. Right-click the server and select Edit Settings.
5. In the Operating System drop-down list, select Windows 2016 MPIO and click OK.

6.1.6 Configure each Fibre Channel HBA port in the server to boot from SAN
To take advantage of all available paths for the boot volume after MPIO has been configured, each HBA port needs to be configured to boot from SAN. The HBAs can be configured using QLogic Fast!UTIL which is accessible during the server boot cycle.

To configure each Fibre Channel HBA port using QLogic Fast!UTIL, perform the following steps:

1. Reboot the server and press [Ctrl-Q] when prompted to enter QLogic Fast!UTIL.
2. In Select Host Adapter, select the first port in the list and press Enter.
3. For each HBA port, do the following:
   a. In Fast!UTIL Options, select Configuration Settings and press Enter.
   b. In Configuration Settings, select Selectable Boot Setting and press Enter.
   c. Set Selectable Boot to Enabled.
   d. Select the first boot port entry and press Enter.
   e. Select the first device from the list and press Enter.
   f. Select the second boot port entry and press Enter.
   g. Select the second device from the list and press Enter.
   h. If there are more than two boot ports, complete the following for each additional port:
      i. Select the boot port entry and press Enter.
      ii. Select the device from the list and press Enter.
   i. Press Esc to exit Selectable Boot Settings.
   j. Press Esc to exit Configuration Settings. When prompted, select Save Changes and press Enter.
   k. In Fast!UTIL Options, click Select Host Adapter and press Enter.
   l. In Select Host Adapter, select the next port in the list and press Enter.
   m. Using the instructions in this step (step 3), configure each HBA port to boot from SAN. Repeat the instructions until all HBA ports have been configured.
4. Press Esc to exit Fast!UTIL. When prompted, select Reboot System and press Enter. The server will reboot.
7 **Microsoft Hyper-V**

The Windows Server platform leverages Hyper-V for virtualization technology. Initially offered with Windows Server 2008, Hyper-V has matured with each release to include many new features and enhancements.

To learn more about Hyper-V, including tools, videos, blogs, and the feature enhancements that have been made available with each new release of Hyper-V (including the 2016 version), visit the Microsoft TechNet Library.

In addition, the [SC Series Technical Documents page](#) contains deployment guides, demo videos, and reference architectures in support of single- and heterogeneous-application workloads running on Hyper-V and SC Series arrays, including Microsoft Exchange, Microsoft SQL Server®, and VDI.
Windows Failover Clustering

8 Windows Failover Clustering

8.1 Overview
Window Server 2016 Failover Clustering provides the capability to tie multiple servers together to offer high availability and scalability for business-critical applications such as Microsoft Exchange, Hyper-V, Microsoft SQL Server, and file servers. Clustering is designed to maintain data integrity and provide failover support. Windows Server 2016 Failover Clustering can scale up 64 nodes in a single cluster. Failover Clustering is included in both the Standard and Datacenter versions of Windows Server 2016.

To learn more about Windows Failover Clustering, including tools, videos, blogs, and the feature enhancements that have been made available with each new release of Windows Server (including 2016), visit the Microsoft TechNet Library.

8.2 Cluster shared volumes (CSVs)
Originally introduced in Windows Server 2008 R2 Failover Clustering, CSVs allow all nodes in a cluster to simultaneously have read-write access to the same LUN that is formatted as an NTFS or ReFS volume. Using CSVs, clustered roles can fail over quickly from one node to another node without requiring a change in drive ownership, or dismounting and remounting a volume.

In Windows Server 2016, CSVs can be used for Hyper-V workloads, or utilized as file shares with the Scale-Out File Server role. Scale-out file shares can host application data, such as Microsoft SQL Server databases and Hyper-V guests.

**Note:** While not a requirement for a clustered file server, a CSV is required for a Scale-Out File Server with a continuously available file share. CSVs formatted with ReFS do not support TRIM/Unmap or ODX.

8.2.1 Cluster server objects with DSM
Microsoft failover clusters require that storage is accessible by all nodes in the cluster. This means that all volumes that the cluster needs must be mapped to each cluster server node individually. To make mapping storage to a cluster easier, DSM offers the ability to create a cluster server object. The individual server objects used for cluster nodes are placed into a cluster server object. Any volumes that are mapped to the cluster server object are automatically mapped to each server contained in the cluster server object.

To create a cluster server object in DSM, perform the following steps:

1. Connect to the SC Series array using the DSM client.
2. Select the Storage tab.
3. Right-click Servers and select Create Server Cluster.
4. Enter a name for the cluster object.
5. Select a folder to place the cluster server object in.
6. From the operating system drop-down list, select Windows 2016 MPIO.
7. Click Add Server to Cluster.
8. Select a cluster server node to add to the cluster and click OK. Repeat this process to add additional nodes.
9. Click OK.
To add a server to an existing cluster object, perform the following steps:

1. Right-click the cluster object and select **Add Server to Cluster**.
2. Select a server to add to the cluster.
3. Click **OK**.

To remove a server from a cluster object, perform the following steps:

1. Expand the cluster server object.
2. Right-click the server and select **Remove Server from Cluster**.
3. Click **OK**.
4. When prompted about removing volume mappings, click **Yes**.

### 8.2.2 Mapping SC Series volumes to clustered server object in DSM

An SC Series volume can be mapped to a cluster server object individually, or as part of a group of volumes that get mapped to the object at the same time. To map multiple volumes to a cluster server object at the same time, the volumes will all need to be contained in the same volume folder.

To map an individual volume to a cluster server object, perform the following steps:

1. Connect to the SC Series array using the DSM client.
2. Select the **Storage** tab.
3. Expand **Volumes** to locate the volume.
4. Right-click the volume and select **Map Volume to Server**.
5. Select the cluster server object and click **Next**.
6. Click **Finish**.

To map multiple volumes to a server cluster object, perform the following steps:

1. Expand **Volumes** and select the volume folder containing the volumes.
2. In the volume folder summary, select the volumes to map (select multiple volumes using the Shift key).
3. Right-click the highlighted volumes and select **Map Volume to Server**.
4. Select the cluster server object and click **Next**.
5. Click **Finish**.
Offloaded data transfer (ODX)

Offloaded Data Transfer (ODX) is a feature developed by Microsoft that offloads to the SAN the work of copying or moving data, bypassing the need for the Windows server and network switches to handle the data movement. By offloading operations to the SAN, ODX can provide significant performance improvements for copy and read operations.

ODX is enabled by default on Windows Server 2016, and SCOS 6.3 or later. ODX requires both the source and destination volumes be formatted as NTFS volumes.

Note: ODX only works between volumes that are located on the same SC Series array. If two volumes from different SC Series arrays are mapped to the same server, data transfers will not use ODX.

ODX operations can be initiated from a physical server or a virtual machine. The source and destination volumes can be physical disks, VHDs, or SMB shared disks (the share must be hosted on a volume located on the same SC Series array as the source/destination volume).

Within Hyper-V, ODX is used to speed up the virtualization platform layer. This allows Hyper-V to achieve native-like performance when virtual machines read and write to the SC Series array. ODX also allows for rapid deployment of guests.

Additionally, ODX can be utilized when creating a fixed-size virtual hard drive (VHD). Without ODX enabled, Windows will explicitly zero-out all the disk space assigned to the new VHD file. Depending on the size of the VHD file, this can be a slow, time-consuming process. With ODX enabled, Windows issues the SC Series array a command to write all zeros to the blocks that represent the new VHD file. This process takes seconds to complete. Windows reads the newly created VHD file as the full size, but with thin provisioning on the SC Series array, the file is not consuming any actual space until data is written to it.

ODX operations on VMs require the VMs be running Windows Server 2012 or above, or Windows 8 or above, and the VM virtual hard drive(s) must be in the VHDX format. Transferring data between VMs requires that the virtual hard drives of both VMs be housed on volumes hosted on the same SC Series array. VMs can use ODX to transfer data to other guests, physical pass-through volumes, virtual Fibre Channel volumes, and SMB shared disks.

For information on how to enable or disable ODX, and how to establish performance benchmarks, see Microsoft TechNet.
Thin provisioning and TRIM/Unmap

Windows Server 2016 automatically identifies thin provisioned LUNs and will reclaim unused space (TRIM) in real time. When data is removed from a volume, TRIM automatically reclaims that space on the SAN. Thin provisioning and TRIM are enabled by default in Windows Server 2016.

Dell EMC introduced support for TRIM/Unmap in SCOS 6.3.1. With the TRIM/Unmap feature, the DSM server agent is no longer required to recover deleted disk space from server volumes and return it to the SAN free disk space pool to be used elsewhere. The server agent can still be installed on a Windows Server 2016 server, but the disk space recovery feature will be disabled by default because it is no longer needed.

TRIM/Unmap is supported with the following types of volumes and disks:

- SC Series volumes mapped to physical Windows Server 2016 hosts using iSCSI, Fibre Channel, or SAS, and to guest VMs as pass-through or direct-attached disks using iSCSI, SAS, or virtual Fibre Channel:
  - SAN volumes must be basic disks and formatted as NTFS.
  - Other formats such as FAT and ReFS do not support TRIM/Unmap.

- SC Series volumes mapped to Windows Server 2016 Hyper-V nodes as cluster shared volumes (CSVs):
  - CSVs must be basic disks and formatted as NTFS.
  - CSVs formatted with ReFS do not support TRIM/Unmap.

- Virtual hard disks:
  - The virtual hard disk format must be VHDX (dynamic or fixed).
  - TRIM/Unmap is not supported with the VHD virtual hard disk format.
  - The guest VM OS must support TRIM/Unmap. When the guest VM OS is Windows Server 2012 or later, from the perspective of the guest, the VHDX must be a basic disk, formatted as NTFS.
  - TRIM/Unmap is not supported on a VHDX when the guest VM OS is Windows Server 2008 R2 or earlier.
11 **Resilient file system (ReFS)**

Introduced with the initial release of Windows Server 2012, ReFS is a file system that is specifically intended for managing extremely large data volumes. Using a new file system design, ReFS can auto-detect data corruption and automatically perform needed repairs without taking a volume offline. ReFS eliminates the need to run chkdsk against large volumes.

ReFS v2 is included with Windows Server 2016. ReFS v2 includes performance enhancements as well as additional features for Hyper-V virtualization workloads.

ReFS volumes can scale exponentially in size, and a single volume can store 18 quintillion (18 million million) files.

11.1 **Using ReFS on SC Series volumes**

SC Series volumes mapped to Windows Server 2016 hosts can be formatted with ReFS.

Consider the following with ReFS:

- SC Series array snapshots and restores of ReFS volumes from snapshots function in the same manner as NTFS volumes.
- ReFS cannot be used on boot or OS volumes.
- ReFS does not support the following features (must use NTFS):
  - File compression
  - Disk quotas
  - EFS encryption
  - Short filenames
  - Object IDs
  - Named streams
  - Extended attributes
  - User data transactions
  - Hard links
  - ODX
  - TRIM/Unmap

**Note:** Windows Server 2016 supports the use of ReFS on CSVs.

It is recommended to use ReFS on very large data volumes on Windows Server 2016 file servers. Because of the reduced feature set of ReFS, NTFS is recommended for all other applications.

For more information about ReFS, refer to the Microsoft TechNet article, [Resilient File System Overview](#).
12 Volume Shadow Copies

The Volume Shadow Copy Service (VSS) is a Windows Server feature that facilitates taking consistent snapshots of a volume when application files are open or in an inconsistent state. If supported by the application, VSS facilitates the process of preparing an application for a snapshot by notifying the application of the impending snapshot. The application will then complete all open transactions, roll transaction logs, and flush caches. All write I/O requests are paused while a snapshot of the volume is captured. Once the snapshot is captured, I/O requests to the volume are resumed.

Shadow Copies of Shared Folders works with VSS to provide point-in-time copies of files that are located on shared resources. When enabled, users have the ability to restore individual files through the Previous Versions tab in the file properties. By default, the snapshots created using Shadow Copies of Shared Folders reside on the volume being snapped, although the location of where the snapshots are stored can be changed to another volume that resides on the system. Shadow Copies of Shared Folders are enabled on a per-volume basis. For more information, refer to the Microsoft TechNet article, Shadow Copies of Shared Folders.

Both Volume Shadow Copies and Shadow Copies of Shared Folders are supported on SC Series volumes.

12.1 Dell Storage Replay Manager

When a snapshot is captured from an SC Series array, the array creates an exact point-in-time capture of the data on the volume, regardless of application and file-open status on the volume. This is known as a crash-consistent snapshot. Crash-consistent snapshots should not be used when application consistency is critical to business operations.

Dell Storage Replay Manager is a GUI-based backup and recovery application that utilizes VSS to create and manage application-consistent snapshots of volumes containing:

- Guest VMs in Hyper-V environments
- Guest VMs in VMware® environments
- VMware datastores
- Exchange Server databases
- SQL Server databases
- Local volumes

Replay Manager can also create and manage Shadow Copies of Shared Folders. For more information, refer to the Replay Manager Administrator’s Guide.

Note: Without using VSS-aware software to facilitate application consistency (such as Replay Manager), it is necessary to use other methods to ensure an application-consistent snapshot of an SC Series volume, such as gracefully pausing or shutting down the application before obtaining a snapshot.
Volume maintenance

Windows Server 2016 automatically performs routine maintenance on volumes through the Optimize Drives application. To open the Optimize Drives application, navigate to Control Panel > Administrative Tools > Defragment and Optimize Drives. Alternately, right-click a volume, select the Tools tab, and click the Optimize button.

![Optimize Drives application screenshot]

By default, drive optimization runs weekly on all drives (volumes) on the system. Automatic scheduling of drive optimization can be set to run on specific volumes on a daily, weekly, or monthly basis.

On thinly-provisioned LUNs, the first thing drive optimizer attempts to do is to run slab consolidation and slab analysis (also known as defragmentation). A slab refers to an allocation of data on the underlying LUN. On the SC Series, this is known as a data page. Windows will not run slab consolidation and analysis on thinly-provisioned LUNs with a slab size of less than 8 MB. Since the page sizes on an SC Series array are either 512 KB, 2 MB (default), and 4 MB, slab consolidation and analysis will never occur on an SC Series LUN.

**Note:** As a best practice, do not run defragmentation on virtualized SAN storage because it can have a negative impact on the performance and effectiveness of Data Progression and replication.

As a last step, drive optimizer will run reTRIM on the volume. As mentioned earlier in this document, Windows Server 2016 will automatically reclaim unused space on an SC Series volume using TRIM/Unmap. TRIM commands are processed asynchronously by the file system in order to minimize any performance impact on the underlying hardware. When space is freed on a volume, the file system queues the TRIM requests to be processed. In cases where the file system receives multiple TRIM requests, the file system may reach a maximum queue size, and some TRIM requests could be dropped. Drive optimizer issues a reTRIM request on the volume to reclaim any space that was missed by dropped TRIM commands. The reTRIM request is processed in a way that limits the amount of TRIM requests in the queue, and avoids any dropped requests.
**Note:** TRIM and reTRIM are only supported on SC Series volumes formatted with NTFS.

Because drive optimizer will periodically help to reclaim additional space on SC Series LUNs, leaving this feature enabled is recommended.

To run the reTRIM process manually on SC Series LUNs, use the **Optimize-Volume** PowerShell command. In the following example, a **ReTrim** command is issued on the SC Series volume, K:. The **-Verbose** switch outputs detailed information to the screen while the command is running.

At the PowerShell prompt, enter the following command:

```powershell
Optimize-Volume -DriveLetter K -ReTrim -Verbose
```

![Optimize-Volume PowerShell command](image)

**Figure 5**   Optimize-Volume PowerShell command
Using BitLocker with SC Series volumes

Windows Server 2016 has the native capability to encrypt volumes with the BitLocker drive encryption utility. With BitLocker drive encryption, users can encrypt system and data volumes to secure data residing on the volume. BitLocker makes use of the on-board Trusted Platform Module (TPM), or a USB drive if TPM is not available to encrypt the system volume. Details on deploying BitLocker can be found on Microsoft TechNet.

The BitLocker encryption process only encrypts the data contained on the volume. Any free space on the volume is not encrypted. All blocks that comprise the data on the volume are changed, effectively creating a new version of the data on the volume. As a result, the active snapshot on an SC Series volume will grow to be the size of the total amount of data on the volume, regardless of the state of any historical snapshots on the volume.

Keep in mind that the encryption process will result in re-writes of all the data on the volume to tier 1 by default. On large volumes, this could cause tier 1 to become full. To minimize impact to the system, verify there is enough space in tier 1 prior to applying encryption to accommodate the data in the volume. Do not let the amount of data used exceed the space available on the system, otherwise the system could enter conservation mode. If necessary, the encryption process can be prevented from consuming faster disks by isolating the volume on a lower tier of storage by changing the storage profile on the volume.

In the following example, a snapshot was taken of an SC Series volume before BitLocker encryption was applied. After the snapshot was taken, more data was added to the volume, increasing the total amount of data on the volume to 38GB. Approximately half of the data is stored in the active snapshot, and the other half is stored in the historical snapshot.

![SC Series volume before encryption](image)

After the BitLocker encryption process is run, the active snapshot increases to the full size of the data contained on the volume, plus an additional 500MB overhead required by BitLocker.
At this point, any pre-existing snapshots on the volume are no longer valid because the data contained in those snapshots is not encrypted. Unless there is a specific need for them, it is recommended to expire any pre-existing snapshots. Once the snapshots are expired and Data Progression is run, the space used by the snapshots is returned to the SC Series volume.

**Note:** If BitLocker encryption is applied to a SC Series volume without any snapshots, the active snapshot size will only increase by the overhead space required by BitLocker (approximately 500MB).

Running BitLocker on virtual guests has similar results compared to running it on physical servers. Refer to documents, [Dell SC Series Storage and Microsoft Hyper-V](#) or [Dell EMC SC Series Best Practices with VMware vSphere 5.x-6.x](#), for details on configuring Windows Server virtual guests in their respective environments.
15 Dell Storage PowerShell SDK

Dell has provided a PowerShell interface for SC Series arrays for many years. The Dell Storage PowerShell Command Set provides cmdlets for many storage tasks, allowing a single script to automate processes that work with storage as well as other components in the data center. For example, the same script can create SC Series volumes, present the volumes to a server, format the disks in Windows Server 2016, and then create Microsoft SQL Server databases on the new disks.

The Dell Storage PowerShell SDK command set is the next-generation PowerShell interface that provides more functionality than the legacy command set. It is designed to work with DSM. Any task that can be performed using the DSM client can be automated in a PowerShell script using the PowerShell SDK.

For a detailed reference of commands found in the Dell Storage PowerShell SDK command set, refer to the Dell Storage PowerShell SDK Cookbook.
A Additional resources

A.1 Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Dell TechCenter is an online technical community where IT professionals have access to numerous resources for Dell EMC software, hardware, and services.

Storage Solutions Technical Documents on Dell TechCenter provide expertise that helps to ensure customer success on Dell EMC storage platforms.

A.2 Related documentation

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell EMC</td>
<td>Dell EMC SC Series Storage: Microsoft Multipath I/O Best Practices</td>
</tr>
<tr>
<td>Dell EMC</td>
<td>Dell SC Series Storage and Microsoft Hyper-V Best Practices</td>
</tr>
<tr>
<td>Dell EMC</td>
<td>Dell Storage Center OS 7.0 Data Reduction with Deduplication and Compression</td>
</tr>
<tr>
<td>Dell EMC</td>
<td>Dell Storage PowerShell SDK Cookbook</td>
</tr>
<tr>
<td>Microsoft</td>
<td>What’s new in Windows Server 2016</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Offloaded Data Transfers (ODX)</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Resilient File System Overview</td>
</tr>
<tr>
<td>QLogic</td>
<td>Firmware’s Execution Throttle and the Windows Queue Depth explained</td>
</tr>
</tbody>
</table>