

Dell Storage Center 6.6

Release Notes

This document describes the new features, enhancements, and fixed issues in Storage Center 6.6.

Current Version: 6.6.11

Release Date: 2016 - 07

Previous Version: 6.6.5

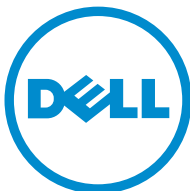
Revision History

Document Number: VKP6G

Revision	Date	Description
A00	April 2015	Initial release
A01	May 2015	Added the fixed issues and enhancements for Storage Center 6.6.5
A02	November 2015	Updated SCv2000 series scalability guidelines
A03	March 2016	Added fixed issues for Storage Center 6.6.11
A04	March 2016	Corrected the description of a fixed issue for Storage Center 6.6.11
A05	July 2016	Added fixed issues for SCv2000 series Storage Centers

Contents

Storage Center 6.6 Feature Availability and Licenses.....	2
Storage Center Scalability.....	2
Requirements for System Manager.....	4
New in this Release.....	4
Storage Center Fixed Issues.....	6
Known Issues.....	13
Storage Center Update Information.....	14
Contacting Dell.....	15



Document Number: VKP6G
Rev. A05
2016 - 07

Storage Center 6.6 Feature Availability and Licenses

Support for the new features in Storage Center 6.6 varies depending on the Storage Center controller.


Feature	SCv2000 Series	SC4020	SC8000	SC040	License Requirements and Notes
Data Compression		X	X	X	Requires a Data Progression license in a multi-tier environment
Flex Port	X (Optional)	X			Requires a Flex Port license
Live Volume		X	X	X	Requires a Live Volume license

Storage Center Scalability

Storage Center 6.6 has the following scalability guidelines.

Storage Center Controller Scalability Guidelines

The following scalability guidelines apply to SC8000, SCv2000 series, SC4020, and CT-SC040 controllers running Storage Center 6.6.

 **NOTE:** Raw storage space is expressed in decimal units (for example, 1TB = 10¹² bytes). Addressable storage space is expressed in base 2 units (for example, 1TB = 2⁴⁰ bytes). Therefore, a 1TB drive measured in decimal units is equal to 0.909TB base 2 units.

Storage Center Controller	Supported Maximum
SC8000 (Dual-Controller) with 64GB of memory per controller	<ul style="list-style-type: none"> 3.1PB raw and 2.0PB addressable storage space using the standard 2MB page size 750TB raw and 500TB addressable storage space using a 512KB page size
SC8000 (Dual-Controller) with 16GB of memory per controller	<ul style="list-style-type: none"> 750TB raw and 500TB addressable storage space using the standard 2MB page size 400TB raw and 300TB addressable storage space using a 512KB page size
SC4020 with 16GB of memory per storage controller module	<ul style="list-style-type: none"> 500TB raw and 400TB addressable storage space using the standard 2MB page size 500TB raw and 400TB addressable storage space using a 512KB page size
SCv2000, SCv2020, SCv2080 with 8GB of memory per controller	<ul style="list-style-type: none"> 672TB raw and 450TB addressable storage space using the standard 2MB page size
CT-SC040 (Dual-Controller) with 12GB of memory per controller	<ul style="list-style-type: none"> 750TB raw and 500TB addressable storage space using the standard 2MB page size 400TB raw and 300TB addressable storage space using a 512KB page size
CT-SC040 (Dual-Controller) with 6GB of memory per controller	<ul style="list-style-type: none"> 400TB raw and 300TB addressable storage space using the standard 2MB page size 400TB raw and 300TB addressable storage space using a 512KB page size

Storage Center Operating System Guidelines

The following scalability guidelines are the maximum recommended design guidelines for Storage Center controller SCv2000 series running Storage Center 6.6.

Storage Center Object	Supported Maximum
Disk Folder	<ul style="list-style-type: none">4 disk folders
Server	<ul style="list-style-type: none">100 servers (Total number of servers includes physical servers, virtual servers, and server clusters.)100 server folders200 server HBA initiator ports (Total number of HBA initiator ports includes all physical and virtual ports that are visible to the SAN.)
Volume	<ul style="list-style-type: none">500TB maximum volume size (or the maximum addressable storage space, whichever is less)1000 volumes500 volume folders
Replay	<ul style="list-style-type: none">2000 Replays1000 Replay profiles100 Replay history profiles25 volumes per consistency group
Replication	<ul style="list-style-type: none">125 source replications500 target replications


The following scalability guidelines are the maximum recommended design guidelines for Storage Center controllers SC8000, SC4020, and CT-SC040 in a Storage Center running Storage Center 6.6.

Storage Center Object	Supported Maximum
Disk Folder	<ul style="list-style-type: none">10 disk folders
Server	<ul style="list-style-type: none">500 servers (Total number of servers includes physical servers, virtual servers, and server clusters.)500 server folders1000 server HBA initiator ports (Total number of HBA initiator ports includes all physical and virtual ports that are visible to the SAN.)
Volume	<ul style="list-style-type: none">500TB maximum volume size (or the maximum addressable storage space, whichever is less)2000 volumes500 volume folders
Replay	<ul style="list-style-type: none">16,000 Replays (4000 Replays for an SC4020)1000 Replay profiles100 Replay history profiles40 volumes per consistency group
Replication	<ul style="list-style-type: none">500 source replications (SC4020: 256 replications)

Storage Center Object	Supported Maximum
	<ul style="list-style-type: none"> 2000 target replications (SC4020: 1000 replications for FC and 230 replications for iSCSI)
Live Volume	<ul style="list-style-type: none"> 100 Live Volumes

Requirements for System Manager

Storage Center System Manager is a Java applet that requires the use of a Java plugin to run. The following table provides the minimum software requirements for running System Manager.

Component	Requirements
Web browser	<ul style="list-style-type: none"> Windows Internet Explorer versions 7, 8, 9, and 11 Windows Internet Explorer Desktop version 10 (Internet Explorer Modern version 10 is <i>not</i> supported) Mozilla Firefox on Microsoft Windows <p> NOTE: Other web browsers may work but are not officially supported.</p>
Java	Java version 7 and 8. When using Java, open the Java Control Panel and make sure that the option Enable Java content in the browser is selected.

Enterprise Manager Compatibility

Storage Center 6.6 is compatible with Enterprise Manager 2015 R1.

New in this Release

Storage Center 6.6 supports new Dell hardware and introduces SupportAssist (formerly, Phone Home).

SCv2000 Series Storage Systems

Storage Center 6.6 introduces support for the SCv2000 series storage systems, including the SCv2000, SCv2020, and SCv2080.

SC4020 Storage Systems

The SC4020 storage controller now supports the SC280 expansion enclosure and the Data Compression, Flex Port, and Live Volume licensed features.

The SC4020 Flex Port feature allows both Storage Center system management traffic and iSCSI traffic to use the same physical network ports. However, for environments where the Storage Center system management ports are mixed with network traffic from other devices (such as voice, backups, or other computing devices), Dell recommends separating iSCSI traffic and other management traffic onto separate VLANs.

Dell SupportAssist

Dell SupportAssist is a support tool that collects, stores, and transmits system state information to Dell Technical Support. SupportAssist can provide automatic case creation based on event alerting, automatic health checks, remote software updates, real-time troubleshooting, and customer support.


User Interface Updates

Storage Center 6.6 provides the following user interface enhancements to improve usability.

- Dell SupportAssist configuration wizard
- Virtual Port Mode configuration for iSCSI ports (Legacy Mode is removed for new systems)
- Configure Secure Console wizard improvements to support Advanced Secure Shell (SSH)
- Additional dialog boxes and instructional messages that provide error recovery for anticipated errors, such as invalid parameters, conflicting IP addresses, unmanaged disks, and so on

Enforced Redundancy Thresholds

The following tables describe HDD and SSD redundancy thresholds for Storage Center 6.6.

 **NOTE:** These thresholds are applied when adding disks after installing Storage Center 6.6.

HDD Redundancy Thresholds

Disk Class/Size	Current Advertised Capacity
No force or recommendation	Maximum 966GB
Recommend Dual Redundancy — Existing and New Page Pools	
966GB up to a maximum 1.93TB	1TB, 1.2TB, 1.8TB
Forced Dual Redundancy — New Page Pools	
1.93TB and higher	2TB and higher
Forced Dual Redundancy — Existing Page Pool	
2.79TB and higher	3TB and higher

SSD Redundancy Thresholds

Disk Class/Size	Current Advertised Capacity
No force or recommendation: WI and RI up to 1.7TB	Maximum 1.6TB
Recommend Dual Redundancy — Existing and New Page Pools	
WI and RI 1.7TB up to 2.78TB	Between 1.78TB and 2.78TB
Forced Dual Redundancy — Existing and New Page Pools	
WI and RI 2.79TB and higher	2.8TB and higher

Storage Center Fixed Issues

The following sections summarize the issues fixed in Storage Center 6.6.

Fixed Issues in Version 6.6.11 for SCv2000 Series Storage Centers

The following table summarizes the issues fixed in Storage Center version 6.6.11 for SCv2000 series Storage Centers.

Problem	Description
CQ00493497	An SCv2000 series controller might reset because of overlapping allocations due to RAID miscompares.
CQ00492347	An SCv2000 series controller might enter an degraded state due to an SAS HBA failure.
CQ00486388 CQ00486381	Controllers might report increased memory usage due to improper release of sockets. Security enhancement regarding the vulnerability CVE-2015 -1283.
CQ00481074	A controller reset might occur due to a TCP connection LAST_ACK socket state error.
CQ00477425	When Immediate Data is enabled, the controller might reboot if it sends a first burst size that is not 512-byte aligned.
CQ00468962	A controller might reset when a disk is set to Unmanaged and causes a NULL pointer.
CQ00460674	When performing a replication, IPC might fail to receive the correct response on a remote storage system or receive the response on the wrong controller.
CQ00460367	The SCv2000 and SC4020 iSCSI IO card drivers are hardcoded with an incorrect value.
CQ00306149	On rare occasions, a RAID device might not be degraded properly when a second write failure is reported for the same device.

Fixed Issues in Version 6.6.11

The following table summarizes all issues fixed in Storage Center 6.6.11.


Problem	Description
CQ00495063	After updating from Storage Center versions 6.4 or 6.5 to Storage Center version 6.6 and later, Phone Home might fail due to previous, pending requests that are unable to complete.
CQ00493497	An SCv2000 series controller might reset because of overlapping allocations due to RAID miscompares.
CQ00492347	An SCv2000 series controller might enter an degraded state due to an SAS HBA failure.
CQ00491768	A controller might reset and failover might be unsuccessful due to an iSCSI IO cache card memory leak with iSCSI attached Oracle and Linux servers.
CQ00491256	On rare occasions, Data Progression and subsequent rebalancing might fail due to snapshot full page memory limitations.

Problem	Description
CQ00489465	A volume restripe operation with large amounts of compressed data might take an extended period of time to restripe due to Data Progression errors.
CQ00486609	Socket memory leaks might occur due to a daemon process error.
CQ00486388 CQ00486381	Controllers might report increased memory usage due to improper release of sockets. Security enhancement regarding the vulnerability CVE-2015 -1283.
CQ00481384	A controller reset might occur due to a failover error.
CQ00481074	A controller reset might occur due to a TCP connection LAST_ACK socket state error.
CQ00479421	Disks might get a BadRegionsPresent health code during a rebuild, even when they are down, due to the multiple RIPEXpired errors.
CQ00479386	Disks might get excessive health codes because RIPEXpired issues codes on devices that are down.
CQ00479088	A controller reboot might occur due to deferred fabric events.
CQ00478666	On rare occasions, a controller might reset when referencing a NULL pointer on a JBOD lookup.
CQ00477544	A controller reboot might occur when reconfiguring and/or deleting iSCSI connections.
CQ00477425	When Immediate Data is enabled, the controller might reboot if it sends a first burst size that is not 512-byte aligned.
CQ00477069	During Data Progression, a controller might reboot due to RAID 5 reporting the incorrect pointer during a disk failure.
CQ00476732	Following an SC200/SC220 enclosure power event, disk drive status might be set to Unknown .
CQ00475596	A controller might reset during Live Volume migration and go into a read-only state due to a proxy error.
CQ00474112	During a software upgrade, a controller might fail due to a PreUpdateCheck ClearJobs call error.
CQ00473058	A local controller might reset, when creating and deleting portable volumes from a remote Storage Center, due to a double-queuing error if the request fails.
CQ00472032	Security vulnerability might occur because Secure Socket Layer (SSL) supports a weak cipher suite that uses an encryption algorithm with a short key length. For information, see http://support.microsoft.com/kb/811834 .
CQ00471760	Security vulnerability might occur due to a minor NTP vulnerability in processing remote configuration packets referenced in SA-15:07. Security: CVE-2014-9293, CVE-2014-9294, Security: CVE-2014-9295, CVE-2014-9296, Security: FreeBSD-SA-14:31.ntp.
CQ00471380	Enabling additional debug logging on iSCSI IO cards might lead to server connectivity issues on other controller front-end ports.
CQ00469934	Security vulnerabilities might occur on Apache servers due to implementing OpenSSL version 1.0.
CQ00469349	Data Progression might move active pages out of highest cost writable class.

Problem	Description
CQ00469084	Upgrading from CT-SC040 controller to SC8000 controller might disable Phone Home and Secure Shell (SSH).
CQ00468962	A controller might reset when a disk is set to Unmanaged and causes a NULL pointer.
CQ00465226	Updating disks using the System Manager user interface might result in volume data corruption due to previous, incomplete platform updates.
CQ00463318	A controller might reboot due to IPC retransmissions.
CQ00462385	SMTP service might become unresponsive.
CQ00460674	When performing a replication, IPC might fail to receive the correct response on a remote storage system or receive the response on the wrong controller.
CQ00460367	The SCv2000 and SC4020 iSCSI IO card drivers are hardcoded with an incorrect value.
CQ00458240	A controller might reset after a failover completes due to a port reset.
CQ00449838	Replays might fail and volumes might become marked as secondary because of an API collision due to a server being deleted (or in the process of being deleted) and a UsageDesired configuration change.
CQ00403547	After a rebuild, drives might appear on a host controller and not appear on a peer controller until a reboot is performed.
CQ00306149	On rare occasions, a RAID device might not be degraded properly when a second write failure is reported for the same device.

Fixed Issues in Version 6.6.5

The following table summarizes the issues fixed in Storage Center 6.6.5.

Issue	Description
CQ00468360	Upgrading to Storage Center 6.6.4 from a pre-6.6 version of Storage Center may cause the Secure Console to not allow a connection for support troubleshooting capabilities.
CQ00468372 CQ00467957 CQ00463317 CQ00465201	When performing deferrable, non-service affecting disk firmware upgrades, Storage Center may experience system performance degradation and/or hosts may experience intermittent connectivity to volumes.  NOTE: Contact Dell Technical Support to plan upgrade steps to avoid potential impact.
CQ00468146	When performing deferrable, non-service affecting disk firmware upgrades, Storage Center displays a console log message when the upgrade is placed into the queue instead of logging the time the upgrade actually starts.
CQ00468027	When directly connected to an SCv2000 series controller using Enterprise Manager, adding a new SC100, SC120, or SC180 expansion enclosure may cause an error message to appear on the Enclosure tab instead of the image of the expansion enclosure.
CQ00467465 CQ00465217	Large read IO patterns from hosts using Flex Port connections on SCv2000 series and SC4020 systems may experience intermittent loss of connectivity to volumes.

Issue	Description
CQ00465212 CQ00465199	
CQ00467245	When directly connected to a Storage Center using Enterprise Manager, restoring a disk that has been released, removed, deleted, or replaced in a chassis may fail.
CQ00462271	Storage Center may fail to communicate with the correct Phone Home/SupportAssist server.
CQ00462206	The Storage Center System Manager Startup wizard may freeze when adding IO cards and then rebalancing local ports.
CQ00459000	When directly connected to an SCv2000 series controller using Enterprise Manager, a Reporter or Volume Manager user may be denied access and Replay Profiles may not display correctly.

Fixed Issues in Version 6.6.4

The following table summarizes the issues fixed in Storage Center 6.6.4.

Issue	Description
CQ00460642	The Storage Center System Manager user interface may become unresponsive while using Java 8.
CQ00460034	The Storage Center System Manager user interface may be unable to set an Enclosure Asset Tag while using Java 8.
CQ00453865	When migrating hardware to an SC8000, moving iSCSI cards to new slots may cause the Hardware Change wizard to fail.
CQ00452843	A possible security vulnerability exists in SC4000 series controllers because the BMC defaults to DHCP instead of a non-routable, static IP address.
CQ00452333	Asynchronous replication may fail to resume after being paused.
CQ00448168	An iSCSI card in an SC4020 may go into hibernation mode after an IO timeout causes the ports to reset.
CQ00446695	The password for the BMC administrator user cannot be changed or disabled on SC4000 series storage systems.
CQ00446532 CQ00440574 CQ00440569 CQ00440561 CQ00438870 CQ00425176	Controller may reset due to changes to the IPMI select timeout and BMC watchdog timer settings.
CQ00445866	Controller may reset if there is an excessive number of XML requests in the queue.
CQ00444922	Data Progression may fail to move pages of non-primary volumes to a lower tier.
CQ00444039 CQ00444033	The Storage Center System Manager user interface may incorrectly display LDAP as disabled while using Java 8.

Issue	Description
CQ00443759	Controller may reset due to a very high volume of system logging.
CQ00442519	Controller may reset due to referencing a historic alert object.
CQ00441032	Controller may reset during 10G iSCSI port fault domain reconfiguration.
CQ00437365	A short duration AC line brownout on an SCv2020 or SC4020 controller may cause unnecessary failover.
CQ00436163	The Storage Center System Manager and Enterprise Manager Client display different values for the MTU size of an iSCSI fault domain.
CQ00434123	Storage Center System Manager incorrectly modifies Flash-Optimized Storage Profiles when the RAID stripe width is changed.
CQ00431040	In rare instances, Storage Center may return RAID scrub errors which could prevent Data Progression from running.
CQ00428825	The Storage Center System Manager user interface may need to be refreshed to log in while using Java 8.
CQ00428801	A Storage Center running version 6.5.10 may be unable to perform a thin import from a competitors storage systems.
CQ00426757	Controller may reset if an IPC request is stuck or outstanding for an extended time.
CQ00424165	A memory leak may occur if a compressed page is deleted while the Data Compressions feature attempts to defragment the space upon which the compressed page resided.
CQ00423822	The IO latency of a Storage Center may increase during data progression, especially if flash drives are in use.
CQ00422360	If Storage Center is operating in virtual port mode, changing hardware ports may fail if the system is unable to link to the correct ports.
CQ00422346	Swapping ports in Legacy Port Mode may result in port failures if the storage system is unable to locate the correct ports.
CQ00421281	Controller may reset during a replay when large numbers of compressed pages are being expired.
CQ00420575	Storage Center IP address configuration errors may occur if an IP address prefix is not specified.
CQ00419941	Storage Center may reset and report a "Small Block Allocation Failure" message in the system log file due to block allotment code.
CQ00419691	Controller may remain in a degraded state after failover due to RAID checking for missing rebuilds after failover completes.
CQ00418685	Controller may reset due to invalid internal table reference.
CQ00418643	Controller may reset due to non-allocation of fragmented physical memory.
CQ00417743	Controller may remain in a failover status due to the deletion of RAID extents.
CQ00417281	When moving CT-SC030 controller hardware to SC8000 controller hardware, updating to Storage Center 6.5.10 may fail.
CQ00417255 CQ00415850	Storage Center may experience communication issues when the maximum number of available iSCSI connections is reached.

Issue	Description
CQ00416440	Storage controllers may reset on systems running 6.4.5 while downloading the update to Storage Center 6.5.10.
CQ00416071	The failure of a hard drive may cause slow disk performance, if the health code assigned to a failed hard drive does not take the drive out of service.
CQ00415741	Storage Center may experience latency if it takes longer than normal to determine the pagepool class when a Replay is taken.
CQ00414488	Replay IO performance may be affected due to limited available memory for background processes on SC8000 controllers.
CQ00413733	Sending SCSI reservations during a disaster recovery restoration process may cause Windows to lose cluster volumes.
CQ00413634	DNS changes in Storage Center version 6.5.1 may cause LDAP authentication issues.
CQ00413249	Volume with a blank Volume Base Name in User defaults may generate an error.
CQ00412866	Data progression may fail and a controller may crash when compression is disabled on the entire system.
CQ00412550	Code execution vulnerability (ShellShock) may occur due to an issue with GNU Bash version 4.3 and earlier (CVE-2014-7169).
CQ00411918	SC4000 series controller may become unresponsive due to a firmware failure where the BMC defaults to DHCP instead of a non-routable, static IP address.
CQ00411774	Storage Center may issue an error message for multi-port SAS HBAs because each port uses a different initiator that is incorrectly being assigned the same target mode InitiatorID.
CQ00411593 CQ00410995	Controller may reset when updating an SC4000 series Storage Center to version 6.5.10 because of a missing /dev/ipmi0 directory.
CQ00411480	Dell SupportAssist may experience server connection or communication issues with the server.
CQ00411202	Controller may reset after completing a CHA3 cache card firmware update.
CQ00411140	SC200 and SC220 enclosures minimum temperature threshold values may cause sensor alerts due to offset counter values.
CQ00410206	Cluster volumes may disconnect if the nodes have different LUN numbers assigned and one of the nodes is promoted.
CQ00409968	Cache card Backup Battery Unit (BBU) access may fail due to cache card write issues on SC4000 series controllers.
CQ00409909	Dell SupportAssist may fail due to HTTP REST client issues.
CQ00409436	Controller may reset when downloading the Storage Center Operating System due to Jumbo checker issues.
CQ00409367 CQ00409360	During a Live Volume recovery process, all of the map zones may not be generated.
CQ00406722 CQ00406714	Controller may reset if Data Compression causes a virtual CPU spike.

Issue	Description
CQ00406050	Storage Center has implemented security enhancements with an update from Apache version 2.2.25 to version 2.2.27 including an update to the SSLCipherSuite list.
CQ00405228	Controller may generate power supply alerts for power supplies that are operating within standard specifications.
CQ00405062	A Storage Center with scheduled Data Compression enabled may suffer a latency spike if a partial page validation process starts while scheduled Data Progression is running.
CQ00404361	OpenSSL Change Cipher Spec (CCS) Injection Vulnerability could be exposed for use in man-in-the-middle attacks in certain OpenSSL-to-OpenSSL communications.
CQ00403992	System Manager user interface does not automatically populate user defaults when creating Flash-Optimized volumes.
CQ00403773	Storage may be consumed at a lower RAID level if new IO is concurrent to a high volume reclamation period.
CQ00403368	Controller may reset if a portable volume that is listed as invalid is deleted.
CQ00403261	An SC4020 that does not have a cable connected to the embedded iSCSI port still sends an iSCSI port down alert.
CQ00402650 CQ00402605	DNS communication issues may result in significant timeout problems, causing Storage Center login errors or long delays when logging into Storage Center.
CQ00402206	Controller may reset due to more than one drive or an entire enclosure going offline at a time.
CQ00416071 CQ00385556	Controllers may fail to join after a Storage Center update because of unreliable Ethernet communications.
CQ00401973	Controller may reset because of a memory allocation issue.
CQ00399866	Controller may reset because of fragmented system memory due to memory pool allocation.
CQ00399663	Storage Center graphical user interface may not display if a Secure console proxy host IP address is set to a local host.
CQ00396942	Storage Center local IO card changes may not recreate MapZones on a remote Storage Center after running the Hardware Change wizard.
CQ00396550	Storage Center may not properly display disk class deletions.
CQ00395973	A Storage Center vulnerability may allow an attacker to reshape the TCP packages to overflow and crash the kernel.
CQ00395568	Controller may reset if an orphaned mapping subprofile exists.
CQ00394685	Controller may reset if the Storage Center experiences an abnormally high level of Phone Home activity.
CQ00390850	Controller may reset because of issues with the SSH console.
CQ00390002	Portable volume may leave unnecessary remnants after deletion.

Issue	Description
CQ00385350	Failed IO may not be retried because a Portable Volume device background timer does not run if a USB device is not present while the controller powers up.
CQ00378976	Controller may reset if SMTP runs out of system resources because of an excessive number of email messages or events.
CQ00364206	The Storage Center System Manager user interface and CompCU do not allow LUN IDs greater than 255.
CQ00137072	Disks may not be reinitialized if the disks are removed from a Storage Center or an enclosure is removed and then added back to a Storage Center.
CQ00132242	Controller may reset or a controller outage may occur if controller failover occurs while the other controller is performing an Add or Revert.
CQ00010763	If a controller failover occurs on a dual-controller Storage Center with 4Gb FC IO cards, the active controller may run out of memory and crash during the failover because the IO cards on the peer controller stay logged into the FC fabric.

Known Issues

The following sections summarize the known issues that may affect Storage Center operations.

Known Storage Center Issues

The following table lists known issues in Storage Center.

Issue	Description
CQ00449611	In rare instances on SCv2000 and SC4000 storage systems, failure LEDs may be illuminated for some drives in the chassis even though Storage Center reports the disks as up and healthy. Workaround: Verify the disk status in the Enterprise Manager or System Manager client. If the status is up and healthy, no action is required. If experiencing this issue, contact Dell Technical Support. To clear this condition, a full system power cycle is required.
CQ00437010	In rare instances, SCv2000 series controllers may not initialize following a reset or controller power cycle. Workaround: The controller must be rebooted by performing a power cycle. After the controller is power cycled, the controller boots up successfully.
CQ00407570	A host server running Windows Server 2012 R2 that is connected to a Storage Center using iSCSI may become partially connected to the Storage Center after a virtual port failover. Workaround: Configure the EnableNOPOut setting in the Windows Registry using the instructions in the Dell Storage Center Microsoft Multipath I/O Best Practices guide on the Dell Tech Center website at http://en.community.dell.com/techcenter/ .
CQ00319498	If an iSNS server is defined incorrectly on the Storage Center or if the iSNS server is down, IO may be slightly degraded every 30 seconds.
CQ00304203	High traffic on a 1Gb PCIe iSCSI IO card may cause connectivity issues.

Known Vendor Issues

The following table lists vendor issues found with Storage Center.

Issue	Description
CQ00489134	Storage Centers servers running RedHat version 7.1 may experience resets. Workaround: Use the latest recommended version of RedHat. See the <i>Dell Storage Compatibility Matrix</i> .
CQ00481040	After controller failover, server connections to Storage Center volumes may fail due to Emulex compatibility. Workaround: Use the latest recommended version of Emulex. See the <i>Dell Storage Compatibility Matrix</i> .
CQ00358236	ESXi 5.x hosts with QxE8262 iSCSI adapters using QLA4xxx driver version 634.5.18 (ESXi 5.1) or 6.34.55.20 (ESXi 5.5) may fail to login to the Storage Center after a controller reset or failover. Workaround: Use the latest recommended version of ESXi. See the <i>Dell Storage Compatibility Matrix</i> .
CQ00303375 CQ00293338	A Storage Center that is in virtual port mode and connected to a server running AIX version 6.1 or 7.1 may intermittently reset iSCSI HBAs and cause the iSCSI volumes to timeout. Workaround: Do not configure Storage Center virtual port mode if AIX iSCSI hosts will be connected.
CQ00266544	Replications and ESX hosts. If a protected site is running Storage Center 6.x and the recovery site is running Storage Center 5.5 or earlier, ESX hosts at the recovery site fail to mount VMFS5 datastores and log the error: Host does not support ATS or ATS initialization has failed in the local vmkernel.log file. Workaround: Upgrade the Storage System running 5.x to version 5.6 or 6.x.
CQ00317099 CQ00260949	Oracle Solaris 10 and 11 server iSCSI connections fail during controller failover in Virtual Port mode. Workaround: Use Legacy Mode with Oracle 10 and 11 servers.
CQ00252780	iSCSI: If a controller or port is in a failover process when a Windows Boot-from-SAN is requested, the boot may fail. Workaround: Subsequent Boot-from-SANs (when the controller or port is up) typically succeed.

Storage Center Update Information

The following information must be considered before updating to Storage Center 6.6.

 **NOTE:** When performing an update of both the Storage Center and Enterprise Manager software, update Enterprise Manager before updating Storage Center.

Updating Software on Storage Center Controllers

Storage Center 6.6 supports controller models SC8000, SC4020, SCv2000 series, and CT-SC040.

To update Storage Center:

- The Storage Center must be running Storage Center version 6.5 or later to perform a SupportAssist update to Storage Center 6.6. This update may require network firewall changes to maintain the transition between Phone Home and SupportAssist. For more information, see the *Dell Storage Center Pre-Deployment Tech Note*.
- When updating from Storage Center 6.0 or earlier to Storage Center 6.6, plan for a longer maintenance window and contact Dell Technical Support for assistance. See the *Storage Center Software Update Guide* for more information.

Contacting Dell

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services might not be available in your area.

To contact Dell for sales, technical support, or customer service issues, go to www.dell.com/support.

- For customized support, type your system service tag on the support page and click **Submit**.
- For general support, browse the product list on the support page and select your product.

© 2016 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.