Quantum®

SANtricity Storage Manager 11.4x Product Release Notes

StorNext QD7000

Firmware 8.40.xx.xx

6-68252-04 Rev A

SANtricity Storage Manager 11.4x Product Release Notes, 6-68252-04 Rev A, July 2018 Product of USA.

Quantum Corporation provides this publication “as is” without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. Quantum Corporation may revise this publication from time to time without notice.

COPYRIGHT STATEMENT

TRAEMARK STATEMENT

Quantum specifications are subject to change.

Preface

Note: The 8.40.xx.xx firmware (Madrid) is used in the QD7000 (E5600, Titan RAID controller, only). Refer to the NetApp to Quantum Naming Decoder section for additional information.

This section provides the following information:

- Audience
- Prerequisites
- NetApp to Quantum Naming Decoder
- Product Safety Statements
- Contacts
- Comments
- Quantum Global Services

Audience

This manual is intended for storage customers and technicians.

Prerequisites

Prerequisites for installing and using this product include knowledge of:

- Servers and computer networks
- Network administration
- Storage system installation and configuration
- Storage area network (SAN) management and direct attach storage (DAS)
- Fibre Channel (FC) and Ethernet protocols

NetApp to Quantum Naming Decoder

Use Table 1 to correlate the NetApp product nomenclature to the equivalent Quantum-storage naming conventions.

Table 1 Product Nomenclature

E-Series NetApp Product	Quantum-Storage	Description
Controller-Drive Tray	Base System	Quantum uses Base System when referring to a drive tray with the RAID controllers.
Drive Tray	Expansion Unit	Quantum uses Expansion Unit when referring to a drive tray with the environmental services modules (ESMs).
E5600 (Code Name: Titan)	RAID Controller	Four 16Gb/s FC SFP+ host ports
E5500 (Code Name: Soyuz)	RAID Controller	Four 16Gb/s FC SFP+ host ports
E5400 (Code Name: Pikes Peak)	RAID Controller	Four 8Gb/s FC SFP+ host ports
DE6600 (Code Name: Wembley)	4U 60-drive enclosure	Sixty 3.5 inch disk drives

E-Series NetApp Product	Quantum-Storage	Description
E5660 - DE6600 4U drive enclosure - With E5600 RAID controllers (Titan)	Quantum StorNext QD7000	
E5560 - DE6600 4U drive enclosure - With E5500 RAID controllers (Soyuz)	Quantum StorNext QD7000	
E5460 - DE6600 4U drive enclosure - With E5400 RAID controllers (Pikes Peak)	Quantum StorNext QD6000	

E-Series NetApp Product	Quantum-Storage	Description
E5424 • DE5600 24-drive 2U drive enclosure • Code Name: Camden • With E5400 RAID controllers (Pikes Peak)	Quantum StorNext QS2400	
E5412 • DE1600 12-drive 2U drive enclosure • Code Name: Ebbets • With E5400 RAID controllers (Pikes Peak)	Quantum StorNext QS1200	

Product Safety Statements

Quantum will not be held liable for damage arising from unauthorized use of the product. The user assumes all risk in this aspect.

This unit is engineered and manufactured to meet all safety and regulatory requirements. Be aware that improper use may result in bodily injury, damage to the equipment, or interference with other equipment.

WARNING: Before operating this product, read all instructions and warnings in this document and in the system, safety, and regulatory guide.

警告 在使用本产品之前，请先阅读本文档及系统、安全和法规信息指南中所有的说明和警告信息。

警告 操作本產品前，請先閱讀本文件及系統、安全與法規資訊指南中的指示與警告說明。

ADVERSAL Læs alle instruktioner og advarsler i dette dokument og i *Vejledning om systemsikkerheds- og lovgivningsoplysninger*, før produktet betjenes.

AVERTISSEMENT Avant d’utiliser ce produit, lisez la totalité des instructions et avertissements de ce document et du *Guide d’informations sur le système, la sécurité et la réglementation*.

HINWEIS Lesen Sie vor der Verwendung dieses Produkts alle Anweisungen und Warnhinweise in diesem Dokument und im System, Safety, and Regulatory Information Guide (Info-Handbuch: System, Sicherheit und Richtlinien).

אזהרה לפני ההפעלה של מוצר זה, קרא את כל ההוראות והאזהרות הכלולות במסמך זה וכן ב*מדריך מידע בנושאי מערכת, בטיחות ותקינה*

警告 この製品を使用する前に、本文書、および『システム、安全、規制に関する情報ガイド』に記載しているすべての警告と指示をお読みください。

경고 이 제품을 작동하기 전에 이 문서 및 시스템, 안전, 및 규제 정보 안내서에 수록된 모든 지침과 경고 표지를 숙지하십시오.

ПРЕДУПРЕЖДЕНИЕ Перед началом эксплуатации данного устройства ознакомьтесь во всеми инструкциями и предупреждениями, приведенными в данном документе и в *Справочном руководстве по устройству, технике безопасности и действующим нормативам*.

ADVERTENCIA Antes de utilizar este producto, lea todas las instrucciones y advertencias en este documento y en la Guia informativa sobre sistema, seguridad y normas.

VARNING Läs alla anvisningar och varningar i detta dokument och i *System, säkerhet och krav från myndigheter - Informationshandbok* innan denna produkt tas i bruk.

Contacts

For information about contacting Quantum, including Quantum office locations, go to:

http://www.quantum.com/aboutus/contactus/index.aspx

Comments

To provide comments or feedback about this document, or about other Quantum technical publications, send e-mail to:

doc-comments@quantum.com

Quantum Global Services

Accelerate service issue resolution with these exclusive Quantum StorageCare services:

- **Service and Support Website -** Register products, license software, browse Quantum Learning courses, check backup software and operating system support, and locate manuals, FAQs, firmware downloads, product updates and more in one convenient location. Benefit today at:

  http://www.quantum.com/serviceandsupport/get-help/index.aspx#contact-support

- **eSupport -** Submit online service requests, update contact information, add attachments, and receive status updates via email. Online Service accounts are free from Quantum. That account can also be used to access Quantum's Knowledge Base, a comprehensive repository of product support information. Get started at:

http://www.quantum.com/customercenter/

For further assistance, or if training is desired, contact the Quantum Customer Support Center:

North America	1-800-284-5101 (toll free) +1-720-249-5700
EMEA	+800-7826-8888 (toll free) +49-6131-324-185
APAC	+800-7826-8887 (toll free) +603-7953-3010

For worldwide support:

http://www.quantum.com/serviceandsupport/get-help/index.aspx#contact-support

SANtricity® Storage Manager 11.42, SANtricity OS 8.40, and SANtricity OS 11.40 (includes SANtricity System Manager)

Product Release Notes

April 2018 | 215-11879_A0_ur003
doccomments@netapp.com

NetApp®

Contents

Deciding whether to use this guide

This document includes release notes for SANtricity Storage Manager 11.42, SANtricity OS (controller firmware) 8.40, and SANtricity OS 11.40 (includes SANtricity System Manager).

Where to find the Latest information about the product

You can find information about the latest version of the product, including new features and fixed issues, and a link to the latest documentation at the NetApp E-Series Systems Documentation Center.

Note:

- The optional iSCSI host interface cards in the E5700/EF570 controllers do not auto-negotiate speeds. You must set the speed for each port to either 10 Gb or 25 Gb. All ports must be set to the same speed.
- If you have a StorageGRID Webscale Appliance, do not update the E2700 or E2800 controller with SANtricity OS version 8.40/11.40. In general, do not apply SANtricity OS upgrades to StorageGRID appliances unless they are specifically stated to be compatible. Contact technical support with any upgrade-related questions.
- For E-Series storage systems attached to FlexArray (V-Series), confirm that the E-Series software version is supported with FlexArray by consulting the NetApp *Interoperability Matrix Tool* (IMT) (login required).
- With FlexArray, the ONTAP (RDAC) host type is no longer supported with E-Series SANtricity OS 8.30 or later. If you are running SANtricity OS 8.20 or earlier, follow the procedures documented in *KB article 000028023* and *KB article 000028024* to convert the host type to ONTAP ALUA.

What's new

New features in SANtricity OS 11.40.2 (E2800 and E5700/EF570 only)

New feature	Description
NVMe over InfiniBand interface	An NVMe over InfiniBand host connection can now be ordered for EF570 or E5700 E-Series controllers. SANtricity System Manager includes new functions for configuring the network connection to the host (available from the **Hardware** page or from **Settings > System**), and functions for viewing data about the NVMe over InfiniBand connections to the storage array (available from **Support > Support Center** or from **Settings > System**).
Authentication with Security Assertion Markup Language (SAML) 2.0 to support Multi-Factor Authentication (MFA)	Authentication can be managed through an Identity Provider (IdP) using the Security Assertion Markup Language (SAML) 2.0. An administrator establishes communication between the IdP system and the storage array, and then maps IdP users to the local user roles embedded in the storage array. Using IdP allows the administrator to configure Multi-Factor Authentication (MFA). SAML authentication is available from **Settings > Access Management > SAML tab**.
Admin role name change	In Access Management, the "admin" role is now called "root admin."
Digitally signed firmware	The controller firmware verifies the authenticity of any downloadable SANtricity firmware. Digitally signed firmware is required in version 8.42 and later. If you attempt to download unsigned firmware, an error is displayed and the download is aborted.
Enable or disable AutoSupport maintenance window	AutoSupport includes an option for enabling or suppressing automatic ticket creation on error events. Under normal operation mode, the storage array uses AutoSupport to open a case with Support if there is an issue. The options for enabling and disabling the AutoSupport Maintenance window are available from **Support > Access Management > AutoSupport tab**.
Host connectivity enhancements	For all host types that support Automatic Load Balancing (ALB), host connectivity reporting can be enabled or disabled independent of the ALB feature. This can be useful in specific, highly tuned environments where ALB movement is not desired, but connectivity reporting is useful. When enabled (the default), host connectivity reporting monitors the connection between the controllers and the configured hosts, and then alerts you if the connection is disrupted. When disabled, this feature suppresses Recovery Guru messages regarding host connectivity. Host connectivity reporting is available from **Settings > System > Additional Settings**.

New feature	Description
Certificate revocation checking via OCSP	Certificate management includes certificate revocation checking using an Online Certificate Status Protocol (OCSP) server. The OCSP server determines if the Certificate Authority (CA) has revoked any certificates before their scheduled expiration date, and then blocks the user from accessing a server if the certificate is revoked. Revocation checking is performed whenever the storage array connects to an AutoSupport server, External Key Management Server (EKMS), Lightweight Directory Access Protocol over SSL (LDAPS) server, or a Syslog server. Configuration tasks are available from **Settings > Certificates**, and requires Security Admin permissions.
Syslog server configuration for audit log archival	In Access Management, you can configure a syslog server to archive audit logs. After configuration, all new audit logs are sent to the syslog server; however, previous logs are not transferred. Configuration tasks are available from **Settings > Access Management**, and requires Security Admin permissions.
System Manager GUI removal of thin volume option	To ensure that the performance characteristics of thin volumes are understood, the System Manager GUI option for creating a thin volume has been removed. Thin volumes can be created with the SANtricity command line interface or the SANtricity Web Services REST API. Thin volumes will continue to be reported on and monitored in the System Manager GUI.

New features in SANtricity OS 11.40.1 (E2800 and E5700/EF570 only)

New feature	Description
NVMe over InfiniBand interface	An NVMe over InfiniBand host connection is now available with EF570 or E5700 E-Series controllers. SANtricity System Manager includes new functions for configuring the network connection to the host (available from the **Hardware** page or from **Settings > System**), and functions for viewing data about the NVMe over InfiniBand connections to the storage array (available from **Support > Support Center** or from **Settings > System**).
Login banner	A new function allows Security Admins to create a login banner that is presented to users before they establish sessions in SANtricity System Manager.The banner can include an advisory notice and a consent message. This function is available from **Settings > System**.
Session timeouts	A new function allows Security Admins to configure timeouts in System Manager, so that users' inactive sessions are disconnected after a specified time. This function is available from **Settings > System**.
Password management	Password management now provides a function for turning off mandatory user passwords as a convenience to solutions integrators using other security measures. Additionally, there is now the ability to set a minimum password length, from 1 to 30 characters. (Entering 0 means no password is required.) Password management is available from **Settings > Access Management**, and requires Security Admin permissions.

New feature	Description
Additional application profiles	This release includes the ability to select additional supported application types. This function is available from **Storage > Volumes**.
Increased pool capacity	Total disk pool capacity has increased to 6 petabytes (PB) for the E5700 and E2800 series arrays, and to 5 PB for the E5600 array. Additionally, the maximum number of drives that can be added or removed from a pool in a single operation has increased to 60 drives.

New features in SANtricity OS 11.40 / SANtricity System Manager 11.40 (E2800 and E5700/EF570 only)

New feature	Description
Access Management (Role-based access and LDAP/ Active Directory)	Access Management is a new feature requiring users to log in to SANtricity System Manager with assigned login credentials. Each user login is associated with a user profile that includes specific roles and access permissions. Administrators can implement Access Management using one or both of these methods: • Using RBAC (role-based access control) capabilities enforced in the storage array, which includes pre-defined users and roles. • Connecting to an LDAP (Lightweight Directory Access Protocol) server and directory service, such as Microsoft's Active Directory, and then mapping the LDAP users to the storage array's embedded roles. Users must have Security Admin permissions to use this feature.
Certificate Management	These functions have been expanded and moved under a Certificate Management tile. Expanded functions include creating a certificate chain for an external key management server. Users must have Security Admin permissions to use this feature. Existing smCLI syntax is retained.
Command line interface (CLI)	The CLI infrastructure has been redesigned to be secure and lightweight with an embedded HTTPS interface for E2800 and E5700 storage arrays.
External Key Management	For E2800 and E5700/EF570 storage arrays, a KMIP-compliant external key manager can be used for managing FDE authentication keys. This capability is in addition to the existing array-based internal key management.
E5700 controller hardware	This new controller supports up to 480 drives.
Feature additions for SANtricity System Manager	Added ability for user to select segment size for volume groups, and the ability to select multiple volumes for deletion.

Restrictions

SANtricity OS 11.40 - System Manager

The following section includes new restrictions that apply to the SANtricity System Manager, which is the browser-based management software embedded on E2800 and E5700/EF570 systems.

No restrictions at this time

There are no restrictions for this section at this time.

SANtricity OS (controller firmware) 11.40 or 8.40

The following section includes new restrictions that apply to the controller firmware for the E2800/E5700/EF570 (SANtricity OS 11.40) and/or the E2700/E5600/EF560 (SANtricity OS 8.40)

iSCSI low-queue-depth Reads with Data Assurance may require adjustment of host side parameters to achieve desired performance

Severity:

2 Functional

Operating system

VMware, Windows, Linux

Hardware/software/firmware

Controller models:

- E28xx using baseboard iSCSI ports
- E28xx using iSCSI ports on host interface card orderable as “HIC,E2800,16G FC/10GbE,4-ports“
- E57xx using baseboard iSCSI ports only

Note: This issue is hardware-related and does NOT affect the 25Gb chipset.

Problem or restriction

Starting with E-Series controller firmware 11.40 release, the Data Assurance (DA; T10 PI) feature is now available with iSCSI on controller models E28xx and E57xx/EF57x. Data Assurance will be enabled by default for new volumes that are created and mapped to iSCSI hosts. DA will not be enabled for existing volumes. When using an iSCSI initiator to issue Reads to an iSCSI volume that was created with DA enabled, you may experience Read performance degradation compared to a non-DA-enabled iSCSI volume for low-queue-depth workloads. The degradation is most noticeable if queue depth=1.

Workaround

Disable the TCP feature 'Delayed Acknowledgment,' which is enabled by default on most of the common host operating systems. Please refer to NetApp KnowledgeBase article 1074155 for specific instructions per operating system:

https://kb.netapp.com/app/answers/answer_view/a_id/1074155

Reference number

Knowledgebase BR15891

With NVMe over InfiniBand, HDDs and degraded volumes, I/O errors can occur

Severity:

2 Functional

Operating system

All

Hardware/software/firmware

E5700

Problem or restriction

With degraded 3+1 and 4+1 RAID 5 volumes on HDDs under heavy I/O load, cache flush operations can exceed the relatively lower timeout values used with NVMe over InfiniBand.

Workaround

Ensure that a hot spare is available to reduce the time a volume remains degraded. Reduce the workload if volumes are degraded. Increase the number of drives in the volume group.

Reference number

LSIP201080829

Certain iSCSI host ports do not support IEEE DCBX

Severity: 2 Functional

Operating system

Any

Hardware/software/firmware

- E2800 and E5700/EF570 base ports
- iSCSI host interface cards installed in controllers other than the E5700/EF570

Problem or restriction

If you wish to attach the controllers iSCSI ports to an ethernet switch configured to use IEEE DCBX, the protocol configuration exchange will not succeed. This means that any expected Priority Flow Control settings and any ETS group settings will not take effect.

Because the protocol negotiation fails, you cannot view the configured settings in the SANtricity System Manager management interface.

Workaround

If you require DCBX and your network hardware allows it, you can use CEEv1.01 DCBX rather than IEEE DCBX. Otherwise, you should contact your switch vendor for an appropriate PFC configuration that suits your needs without using the DCBX protocol.

Reference number

LSIP201067876

32 Gb SFPs are not supported in the E5700/EF570 base host ports and show as Failed in the management software

Severity: 2 Functional

Operating system

Any

Hardware/software/firmware

E5700/EF570

Problem or restriction

The expansion ports on the E5700/EF570 support 32 Gb speeds; however, the base ports support only up to 16 Gb speeds. If a 32 Gb SFP is placed into a base port, it will not function and will be marked as Failed in the storage management software.

Workaround

Do not use 32 Gb SFPs in the E5700/EF570 base ports.

Reference number

LSIP200987891

With Asynchronous Mirroring, a slow link causes a controller reboot

Severity: 2 Functional

Operating system

Any

Hardware/software/firmware

Asynchronous Mirroring

Problem or restriction

With Asynchronous Mirroring, a drop in link throughput can cause too much remote volume I/O to be queued, which leads to a timeout and controller reboot.

Workaround

None.

Reference number

LSIP200993879

High IOPS to 7200 RPM drives causes controller reboot

Severity: 2 Functional

Operating system

Any

Hardware/software/firmware

Any

Problem or restriction

Applications, such as VMware, that push high IOPS to volumes on 7200 RPM drives can cause a controller to reboot.

Workaround

Use drives with higher spindle speed with applications that will be pushing high IOPS to these drives.

Reference number

LSIP201012340

Replacing both E2800 or E5700/EF570 controllers with secured and unsecured drives causes controller lockdown

Severity: 2 Functional

Operating system

Any

Hardware/software/firmware

E2800, E5700/EF570

Problem or restriction

With the E2800 or E5700/EF570 storage array, if you replace both controllers with the same controller part number and same HICs, for example, to upgrade memory or in the rare case of a dual controller failure, and the system has a mix of secured and unsecured drives, there is a chance that one controller will be locked down.

Workaround

None. Contact Support for assistance with this procedure.

Reference number

LSIP201031807

SANtricity Storage Manager Software

The following section includes new restrictions that apply to the SANtricity Storage Manager software, which is loaded on an I/O-attached host or a management station.

On a Windows host with Fibre Channel connections to the array, a discovery error after a controller power cycle causes a path to a volume to be lost

Severity: 2 functional

Operating system

Windows

Hardware/software/firmware

All controllers with Fibre Channel HICs

Problem or restriction

If a controller is power cycled, an error during discovery when the controller is booting up can cause a path to a volume to fail to be discovered. An error is reported in the Event Log, "Host multipath driver configuration error detected."

Workaround

Force the host to rescan devices to rediscover the path.

Reference number

LSIP201065647

With Asynch Mirroring, upgrading SANtricity Storage Manager 11.30 to a later version deletes the modified truststore

Severity: 2 functional

Operating system

Windows, Linux

Hardware/software/firmware

SANtricity Storage Manager - Enterprise Management Window

Problem or restriction

When using Asynch Mirroring, the truststore must be modified to have a trusted connection. When upgrading the SANtricity Storage Manager software from 11.30 to a later 11.30 version or any subsequent major releases, the files in the installation directory are removed, which means that the truststore file is removed. This issue occurs when you perform either an uninstall/reinstall or an upgrade on Linux, but only with uninstall/reinstall on Windows.

Workaround

Option 1: You can re-import the certificates using the SANtricity Storage Manager Enterprise Management Window.

Option 2:

Before uninstalling or upgrading SANtricity, copy the truststore and keystore.

1. Backup INSTALLDIR/client/working/{truststore,keystore}.

2. Do the uninstall/install/upgrade.

3. Start the Enterprise Management Window, and wait approximately 1min for the webserver to create the needed files. Close the Enterprise Management Window.

4. Copy the keystore and truststore to $devmgr.data/ws/working/.

Windows: \Program Files\StorageManager\client\data\ws\working

Linux: /var/opt/SM/ws/working

Reference number

LSIP201031820

Third-Party

The following section includes restrictions that apply to third-party components or software that might be used in an E-Series storage environment.

Microsoft Edge browser cannot do SAML authentication when the array's certificates are not trusted by the browser

Severity:

2 Functional

Operating system

Windows

Hardware/software/firmware

E2800, E25700/EF570

SANtricity System Manager 11.42 or newer

Microsoft Edge browser

ADFS Identity Provider or Shibboleth Identity Provider

Management certificate that is not trusted by Edge browser

Problem or restriction

When the storage array is setup to use SAML for authentication and the method enabled, users will be redirected to the configured Identity Provider's login page if not using Windows Integrated Authentication (WIA) to get authenticated and will then be taken into System Manager using the established session; this is SSO login.

For Microsoft Edge users, they will experience hanging with a blank page after credentials are provided at the Identity Provider. If users refresh the page then they will be taken to the storage array's endpoint but then receiving an error.

The problem is that the Microsoft Edge browser cannot use POST in a form submit if the HTTPS service (in this case, the storage array's management web server) is not trusted by the browser. This is a known issue being tracked with the Microsoft incident, https://developer.microsoft.com/en-us/microsoft-edge/platform/issues/7571345/.

The browser has to trust either the certificate or the CA intermediate certificate/root certificate that signed the array's certificates.

Workaround

If you do not require Microsoft Edge, you can use an alternative browser. See the Online Help for the list of supported browsers.

If you must use Microsoft Edge, try one of the following options to get the browser working again:

- Use an alternative browser to establish a trust between Microsoft Edge and the storage array’s management server. You must have Security Admin privileges or work with the Security Admin.
- Use an Identity Provider administrator to support WIA for Microsoft Edge:

```
Set-ADFSProperties -WIASupportedUserAgents @(“MSIE 6.0”, “MSIE 7.0”,
“MSIE 8.0”, “MSIE 9.0”, “MSIE 10.0”, “Trident/7.0”, “MSIPC”, “Windows
Rights Management Client”,”Edge/12”)
```

Reference number

LSIP201085405

With Linux and End-to-End Data Assurance, disabling Data Assurance on a volume undergoing I/O results in I/O errors

Severity:

2 Functional

Operating system

Linux

Hardware/software/firmware

All controllers with HICs/protocols that support End-to-End Data Assurance

Problem or restriction

The Linux kernel does not have support for target devices changing operating parameters on the fly. If Data Assurance is disabled on a volume that is servicing host I/O, the host and will continue to set Data Assurance flags in reads and write commands even though the target no longer supports it. This results in I/O errors.

Workaround

Only disable Data Assurance as an offline operation, then reboot the host to force a rescan of SCSI devices to pick up the change in operating parameters.

Reference number

LSIP201062079

Lifted Restrictions

April 2018 Maintenance Release

The following section includes lifted restrictions that apply to the April 2018 Maintenance Release, which includes the following software versions:

- SANtricity Storage Manager 11.42.XX00.0001
- SANtricity OS 11.40.2
- SANtricity OS 08.40.00.00

Unable to upgrade E2800 or E5700/EF570 using in-band management

Severity: 2 Functional

Operating system

Any

Hardware/software/firmware

E2800, E5700/EF570

Problem or restriction

When attempting to download a SANtricity OS bundle to E2800/E5700/EF570 using in-band management (via the I/O path), the download will intermittently fail with an MD5 checksum error.

Workaround

Use out-of-band management (via the controller's Ethernet management ports) to upgrade the system.

Reference number

LSIP201046403

GET to mel-events endpoint using Webservices times out

Severity: 2 Functional

Operating system

Any

Hardware/software/firmware

Any

Problem or restriction

Using the embedded Webservices, a GET to the mel-events endpoint occasionally takes a long time to complete (more than 3 minutes).

Workaround

Retry the GET mel-event operation.

Reference number

LSIP201023003

With E5700/EF570 and IB-ISER, loss of a switch port causes controller reboot

Severity: 2 Functional

Operating system

Any

Hardware/software/firmware

E5700/EF570

IB-ISER

Problem or restriction

If a switch port is disabled or if there is a flaky connection to the switch, an error in the connection close process caused a controller to reboot.

Workaround

None. After the controller reboots, the initiator should restore the connections to that controller.

Reference number

LSIP201012326

When using all ports on E5700/EF570 iSCSI HICs with a 25Gb switch, link events may cause the host(s) to lose connection

Severity: 2 Functional

Operating system

Any

Hardware/software/firmware

E5700/EF570 with iSCSI HICs

Problem or restriction

If you have all ports connected from an E5700/EF570 iSCSI HIC (host interface card) to a switch running at 25Gb speed and link events occur, one controller may experience an error that causes the links to go down and the host(s) to lose connection.

Workaround

To avoid this issue, use 2 or fewer ports per HIC when connected to a switch running at 25G. To recover from this issue, remove the controller that lost connection, wait for the controller's LEDs to go dark, then reinsert the controller.

Reference number

LSIP201040661

December 2017 Maintenance Release

The following section includes lifted restrictions that apply to the December 2017 Maintenance Release, which includes the following software versions:

- SANtricity Storage Manager 11.41.XX00.0003
- SANtricity OS 11.40.1
- SANtricity OS 08.40.10.01

With SAS or IB host interfaces, the pre-upgrade health check will fail after downgrading controller firmware

Severity: 2 Functional

Operating system

Any

Hardware/software/firmware

All controllers with SAS or IB HICs

Problem or restriction

On a system with SAS or IB HICs at firmware version 8.30.20.00/11.30.2 or later, a downgrade to previous versions, then a subsequent upgrade to these versions, or later will cause the pre-upgrade health check to fail.

Workaround

None. Contact technical support for assistance with this procedure.

Reference number

LSIP201010285

Copyright information

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Trademark information

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277