Hitachi Protection Platform S-Series V7.3.1 Software Release Notes

RN-S2500-7.3.1-00

Release Highlights

- This is a general availability release that supports a maximum of eight nodes for all data flows. Sep-19480
- Improved graph management increases deduplication efficiency. Seps-19667, 19618
- Load distribution across nodes in the cluster for OST ingest and replication. Sep-19555.

Issues Fixed in V7.3.1

User-Level Privileges Are Again Restricted to Viewing Status and Generating a Support Ticket
This release fixes an issue where an S-Series operator with User-level privileges had been able to manipulate the deduplication configuration settings. User-level privileges are now restricted to viewing status and generating a Support Ticket. Sep-18151

OST I/O Server Module Failure Fixed
During system shutdown, OST-over-FC devices that were not activated and used during the appliance operation caused corresponding OST I/O server processes to fail and this produced a core file. This issue is now fixed. Sep-19613

Default Small Data Set Size Increased
Increasing the default small data set size to 100 MB reduces unnecessary processing and improves performance. Sep-19646

Report Generation Occurring in a Timely Manner
An unnecessary software loop was causing scheduled nightly reports to take longer each time they were run until the reports eventually would not generate at all. This is now optimized and now reports are generating in a timely manner as expected. Sep-19654

Known Issues and Considerations

Attempting To Delete Hundreds of Cartridges at One Time Can Cause a Service Disruption
Deleting large numbers of cartridges using the console manager can impact system performance and can cause a service disruption. Sep-19632

Browser Certificate Considerations with the S-Series

X.509 Certificate Subject Common Name (CN) Does Not Match the Entity Name
A known S-Series security vulnerability is that its X.509 Certificate Subject Common Name (CN) does not match the Entity Name rendering a certificate-common-name-mismatch.

Self-Signed TLS/SSL Certificate Generates Browser Security Warnings
Your S-Series appliances comes by default with a self-signed Transport Layer Security and Secure Sockets Layer (TLS/SSL) protocol certificate. Self-signed certificates cannot be trusted by default, especially because TLS/SSL man-in-the-middle attacks typically use self-signed certificates to eavesdrop on TLS/SSL connections. If you want to install your own certificate, contact Customer Support for assistance.

Explicitly Defining the TLS Protocols To Use Disables SSLv3 in Apache Tomcat
By explicitly listing the valid TLS protocols for the S-Series system to use effectively disables the fall back to the SSLv3 protocol in Tomcat and prevents the known Poodle vulnerability from occurring. Sep-19595

V7.3.1 Compatibility Matrices

These tables list the backup applications, and the backup server and client operating systems that are supported by V7.3.1.

NetWorker and Data Protector are not yet qualified and a bulletin will provide the known information when available.

The maximum number of supported virtual devices is 192 per node.

Contact HDS for specific information about supported virtual machine (VM) applications.

Table 1: TSM Compatibility Matrix

Backup Applications	Tivoli Storage Manager 5.3, 5.4, 5.5, 6.1, 6.1.1, 6.1.2, 6.1.3, 6.2, 6.2.1, 6.2.2, 6.3
Backup Server Host Operating Systems	Windows Server 2003 SP2 Windows Server 2008 SP1 Windows Server 2008 R2 (AMD64) Windows 2012 R2 (AMD64) Red Hat Enterprise and CentOS Linux 6, 5, 4 Solaris 9 and 10 AIX 5.3, 6.1
Client Operating Systems	Windows Server 2003 SP2 Windows Server 2008 SP1 Windows Server 2008 R2 (AMD64) Windows 2012 R2 (AMD64) Red Hat Enterprise Linux 5 and 4 and CentOS Linux 6, 5 SUSE Linux 10 Solaris 9 and 10 AIX 5.3, 6.1, 6.3

Table 2: NetBackup Compatibility Matrix

Backup Applications	NetBackup 5.5, 6.0, 6.5.1, 6.5.3, 6.5.4, 6.5.5, 7.0, 7.1, 7.5, 7.6, 7.6.1, 7.6.1.1
Backup Server Host Operating Systems	Windows Server 2003 SP2 Windows Server 2008 SP1 Windows Server 2008 R2 (AMD64) Windows 2012 R2 (AMD64) HP-UX 11 Red Hat Enterprise and CentOS Linux 6, 5, and 4 AIX 5.3, 6.1 Solaris 9 and 10
Client Operating Systems	Windows Server 2003 SP2 Windows Server 2008 SP1 Windows Server 2008 R2 (AMD64) Windows 2012 R2 (AMD64) HP-UX 11 Red Hat Enterprise Linux 5, and 4 and CentOS Linux 6, 5 AIX 5.3, 6.1 SUSE Linux 10 Solaris 9 and 10

Licensed Feature Compatibility

This section lists the cross-system compatibilities between legacy systems and newly released HDS systems.

S2100 (HP G7s) with V7.3.1 ←→ S1500 (HDS CR220S) V8.0

S2500 (HP G8s) with V7.3.1 ←→ S1500 (HDS CR220S) V8.0

OST, OST-Optimized Duplication, OST-AIR, Tape Image Replication, and Delta Differencing Deduplication

Supported OST Media Servers and Operating Systems

Table 3: OST Media Servers and Operating Systems

Supported OST Media Servers and OS Versions	Windows 2012 R2 (AMD64) Windows Server 2008 R2 (AMD64) RHEL5 and RHEL6, CentOS 5 and CentOS 6*x* (x86_64) Solaris 10 and 11 (SPARC64) AIX 6.1 and 7.1 (PPC) SUSE ES10 and ES11 (x86_64) Symantec 5*xxx* appliance

Supported OST Features

Table 4: Supported OST Features

Auto Image Replication (A.I.R.)
Accelerator
Accelerator VMware*
Instant Recovery VMware
Optimized Duplication (OptDup)
Optimized Synthetic (OptSyn)

*Requires the NetBackup Data Protection Optimization Option license.

Update Paths

Following are the supported update paths to S-Series platform software version 7.3.1.

Supported Update Paths to S-Series Software V7.3.1

Update From...	Update to...
V7.1	V7.3.1
V7.1.1P*x*	
V7.2.0.1	
V7.2.0.2P1	
V7.2.0.3	
V7.3	

If you choose to update your S-Series platform software version, you cannot later downgrade it to an earlier software version. For example, you cannot perform a software downgrade from V7.3.1 to V7.3.

Accessing Product Documentation

This section lists documents related to installation, hardware, software, configuration, monitoring, troubleshooting, best practices, and updates for the S1500 Hitachi Protection Platform. You can access the Hitachi Protection platform documentation from the HPP service console, https://deltaview.sepaton.com or http://www.HDS.com.

Related Documents

- *Hitachi Protection Platform S-Series User Manual* MK-95HPP001-00
- *Hitachi Protection Platform S-Series Software Installation Instructions* FE-95HPP002-00

Contact Information

Technical Support

If your unit does not offer a function described in this document, please open a Customer Support case by visiting the HPP support portal at https://deltaview.sepaton.com, or call +1.866.657.8400. Be prepared to provide your company name, serial number, contact information, and a detailed description of your issue.

Web Site

For more information about Hitachi Data Systems and HDS products, please visit:

http://www.hds.com

Comments

Our goal is to provide accurate, useful, and easy-to-understand documentation. If you have any comments about this manual or have noticed any errors, we would appreciate your feedback. You may provide your comments by opening a Customer Support case by visiting the HPP support portal located at https://deltaview.sepaton.com. You may also contact us directly at:

HDS Sepaton
400 Nickerson Road
Marlborough, MA 01752 USA

Phone: 1.508.490.7900
+1.866.657.8400
Fax: 1.508.490.7908

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2639
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0)1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com