

Symantec™ Dynamic Multi-Pathing 6.1 Release Notes - Linux

July 2014



Symantec™ Dynamic Multi-Pathing Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Product version: 6.1

Document version: 6.1 Rev 5

Legal Notice

Copyright © 2014 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, Veritas, Veritas Storage Foundation, CommandCentral, NetBackup, Enterprise Vault, and LiveUpdate are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/index.jsp

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/contact_techsupp_static.jsp

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Documentation

Product guides are available on the media in PDF format. Make sure that you are using the current version of the documentation. The document version appears on

page 2 of each guide. The latest product documentation is available on the Symantec website.

<https://sort.symantec.com/documents>

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com

For information regarding the latest HOWTO articles, documentation updates, or to ask a question regarding product documentation, visit the Storage and Clustering Documentation forum on Symantec Connect.

<https://www-secure.symantec.com/connect/storage-management/forums/storage-and-clustering-documentation>

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec's enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

<http://www.symantec.com/connect/storage-management>

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Dynamic Multi-Pathing Release Notes

This document includes the following topics:

- [About this document](#)
- [About Symantec Dynamic Multi-Pathing \(DMP\)](#)
- [About Symantec Operations Readiness Tools](#)
- [Important release information](#)
- [Changes introduced in Symantec Dynamic Multi-Pathing 6.1](#)
- [System requirements](#)
- [Fixed issues](#)
- [Known issues](#)
- [Software limitations](#)
- [Documentation](#)

About this document

This document provides important information about Symantec Dynamic Multi-Pathing (DMP) version 6.1 for Linux. Review this entire document before you install or upgrade DMP.

The information in the Release Notes supersedes the information provided in the product documents for DMP.

This is "Document version: 6.1 Rev 5" of the *Symantec Dynamic Multi-Pathing Release Notes*. Before you start, make sure that you are using the latest version of this guide. The latest product documentation is available on the Symantec Web site at:

<https://sort.symantec.com/documents>

About Symantec Dynamic Multi-Pathing (DMP)

Symantec Dynamic Multi-Pathing (DMP) provides multi-pathing functionality for the operating system native devices that are configured on the system. DMP creates DMP metadevices (also known as DMP nodes) to represent all the device paths to the same physical LUN.

DMP is also available as a standalone product, which extends DMP metadevices to support the OS native logical volume manager (LVM). You can create LVM volumes and volume groups on DMP metadevices.

Symantec Dynamic Multi-Pathing can be licensed separately from Storage Foundation products. Veritas Volume Manager and Veritas File System functionality is not provided with a DMP license.

DMP functionality is available with a Storage Foundation (SF) Enterprise license, an SFHA Enterprise license, and a Storage Foundation Standard license.

Veritas Volume Manager (VxVM) volumes and disk groups can co-exist with LVM volumes and volume groups. But, each device can only support one of the types. If a disk has a VxVM label, then the disk is not available to LVM. Similarly, if a disk is in use by LVM, then the disk is not available to VxVM.

About Symantec Operations Readiness Tools

Symantec Operations Readiness Tools (SORT) is a website that automates and simplifies some of the most time-consuming administrative tasks. SORT helps you manage your datacenter more efficiently and get the most out of your Symantec products.

SORT can help you do the following:

Prepare for your next installation or upgrade

- List product installation and upgrade requirements, including operating system versions, memory, disk space, and architecture.
- Analyze systems to determine if they are ready to install or upgrade Symantec products and generate an Installation and Upgrade custom report.
- List patches by product or platform, and in the order they need to be installed. Display and download the most recent patches or historical patches.
- Display Array Support Library (ASL) details by vendor, platform, or Storage Foundation and High Availability (SFHA) version. ASLs make it easier to manage arrays that are connected to SFHA-based servers.
- List VCS and ApplicationHA agents, documentation, and downloads based on the agent type, application, and platform.

Identify risks and get server-specific recommendations

- Analyze your servers for potential environmental risks. Generate a Risk Assessment custom report with specific recommendations about system availability, storage use, performance, and best practices.
- Display descriptions and solutions for thousands of Symantec error codes.

Improve efficiency

- Get automatic email notifications about changes to patches, array-specific modules (ASLs/APMs/DDIs/DDLs), documentation, product releases, Hardware Compatibility Lists (HCLs), and VCS/ApplicationHA agents.
- Quickly gather installed Symantec product and license key information from across your production environment. Generate a License/Deployment custom report that includes product names, versions, and platforms, server tiers, Symantec Performance Value Units (SPVUs), and End of Service Life dates.
- List and download Symantec product documentation including product guides, manual pages, compatibility lists, and support articles.
- Access links to important resources on a single page, including Symantec product support, SymConnect forums, customer care, Symantec training and education, Symantec FileConnect, the licensing portal, and my.symantec.com. The page also includes links to key vendor support sites.
- Use a subset of SORT features from your iOS device. Download the application at:
<https://sort.symantec.com/mobile>

Note: Certain features of SORT are not available for all products. Access to SORT is available at no extra cost.

To access SORT, go to:

<https://sort.symantec.com>

Important release information

- For important updates regarding this release, review the Late-Breaking News TechNote on the Symantec Technical Support website:
<http://www.symantec.com/docs/TECH211540>
- For the latest patches available for this release, go to:
<https://sort.symantec.com/>
- The hardware compatibility list contains information about supported hardware and is updated regularly. For the latest information on supported hardware, visit the following URL:
<http://www.symantec.com/docs/TECH211575>
- The software compatibility list summarizes each Storage Foundation and High Availability (SFHA) Solutions product stack and the product features, operating system versions, and third-party products it supports. For the latest information on supported software, visit the following URL:
<http://www.symantec.com/docs/TECH213121>

Note: Before you install or upgrade SFHA Solutions products, review the current compatibility lists to confirm the compatibility of your hardware and software.

Changes introduced in Symantec Dynamic Multi-Pathing 6.1

This section lists the changes in Symantec Dynamic Multi-Pathing 6.1.

Changes related to installation and upgrades

The product installer includes the following changes in Symantec Dynamic Multi-Pathing 6.1.

Support for SFHA 6.1 installations from any supported operating system to any other supported operating system

You can use the Deployment Server or the web-based installer to install your 6.1 Symantec products on a target system that runs any supported UNIX or Linux platform, even if the source system and target system are running on different UNIX or Linux platforms. Prior to 6.1, releases still require the same platform, architecture, distribution, and version of the operating system.

See the *Installation Guide* for more information.

Improved patching and updating process

You can now download product maintenance releases and public hot fix releases directly from the Symantec Operations Readiness Tools (SORT) website using the installer. When you use the `installer` command with the `-version` option, the installer now lists the available GA releases, maintenance releases, and hot fix releases. If you have Internet access, you can follow the installer prompts to download available patches and hot fixes to your local system.

Downloading patches and hot fixes requires the installer to make outbound networking calls. If you know your systems are behind a firewall, or do not want the installer to make outbound networking calls, you can disable external network attempts by running the installer using the no Internet patch center (`-noipc`) option. When using the `-noipc` option, the installer does not try to connect to SORT website. For example:

```
# ./installer -version -noipc system1 system2
```

See the *Installation Guide* for more information.

Automatic download of installer hot fixes

If you are running the 6.1 product installer, and your system has Internet access, the installer automatically imports any needed installer hot fix, and begins using it.

If your system does not have Internet access, you can still download installer hot fixes manually using the [Symantec Operations Readiness Tools](#) patch finder tool.

Automatic downloading of installer hot fixes requires the installer to make outbound networking calls. If you know your systems are behind a firewall, or do not want the installer to make outbound networking calls, you can disable external network attempts by running the installer using the no Internet patch center (`-noipc`) option.

See the *Installation Guide* for more information.

Support for centralized installations using the Deployment Server

The Deployment Server is a script that makes it easier to install or upgrade SFHA releases. The Deployment Server lets you store multiple release images in one central location and deploy them to systems of any supported UNIX or Linux operating system (6.1 or later). Prior to 6.1, releases still require the same platform, architecture, distribution, and version of the operating system. You can use the Deployment Server if you want to install or upgrade multiple releases and or multiple platforms.

The Deployment Server lets you do the following as described in [Table 1-1](#).

Table 1-1 Deployment Server functionality

Feature	Description
Manage release images	<ul style="list-style-type: none"> ■ View available Storage Foundation releases. ■ Download maintenance and hot fix release images from the Symantec Operations Readiness Tools (SORT) website into a repository. ■ Load the downloaded release image files from FileConnect and SORT into the repository. ■ View and remove release image files stored in the repository.
Check versions	<ul style="list-style-type: none"> ■ Discovers RPMs and patches installed on designated systems and informs you of the product and version installed, including installed hot fixes. ■ Identify base, maintenance, and hot fix level upgrades to your system and download maintenance and hot fix releases. ■ Query SORT for the most recent updates.
Install or upgrade systems	<ul style="list-style-type: none"> ■ Install or upgrade a release stored in the repository on selected systems. ■ In release 6.1 and later: <ul style="list-style-type: none"> ■ Install hot fix level releases. ■ Install SFHA from any supported UNIX or Linux operating system to any other supported UNIX or Linux operating system. ■ Automatically load the script-based installer hot fixes that apply to that release.

Note: The Deployment Server is available only for the script-based installer, not the web-based installer.

See the *Installation Guide* for more information.

Support for simultaneously installing or upgrading base releases, maintenance patches, and hot fixes

Beginning with version 6.1, Symantec offers you a method to easily install or upgrade your systems directly to a base, maintenance, or hot fix level in one step using Install Bundles. Install Bundles is the ability for installers to merge so customers can install or upgrade directly to maintenance or hot fix levels in one execution. Install Bundles consists of executing the installer from a GA release with a pointer to a higher maintenance or hot fix release. The installer installs them both as if they were combined in the same release image. The various scripts, RPMs, and patch components are merged and multiple releases are installed together as if they are one install entity.

Note: This feature is not supported by the Deployment Server.

There are five possible methods of integration. All upgrades must be executed from the highest level script.

- Base + maintenance
- Base + hot fix
- Maintenance + hot fix
- Base + maintenance + hot fix
- Base or maintenance + multiple hot fixes

See the *Installation Guide* for more information.

Changes related to product name branding

Beginning with the 6.1 release, Storage Foundation and High Availability Solutions product names are rebranded.

[Table 1-2](#) lists the rebranded Storage Foundation and High Availability Solutions products.

Table 1-2 Rebranded Storage Foundation and High Availability Solutions products

Old product name	New product names with Symantec branding
Veritas Storage Foundation	Symantec Storage Foundation (SF)

Table 1-2 Rebranded Storage Foundation and High Availability Solutions products (*continued*)

Old product name	New product names with Symantec branding
Veritas Dynamic Multi-Pathing	Symantec Dynamic Multi-Pathing (DMP)
Veritas Replicator Option	Symantec Replicator Option
Veritas File Replicator Option	Symantec File Replicator Option (VFR)
Veritas Volume Replicator	Symantec Volume Replicator (VVR)
Veritas Storage Foundation Cluster File System HA	Symantec Storage Foundation Cluster File System HA (SFCFSHA)
Veritas Storage Foundation for Oracle RAC	Symantec Storage Foundation for Oracle RAC (SFRAC)
Veritas Storage Foundation for Sybase ASE CE	Symantec Storage Foundation for Sybase ASE CE
Veritas Storage Foundation HA	Symantec Storage Foundation HA (SFHA)
Veritas Cluster Server	Symantec Cluster Server (VCS)
Veritas Disaster Recovery Advisor	Symantec Disaster Recovery Advisor (DRA)
Veritas Storage Foundation and High Availability Solutions	Symantec Storage Foundation and High Availability Solutions (SFHAS)
Veritas High Availability Agent Pack	Symantec High Availability Agent Pack
Veritas File System Software Development Kit	Symantec File System Software Development Kit

Symantec rebranding does not apply to the following:

- Product acronyms
- Command names
- Error messages
- Alert messages
- Modules and components
- Feature names
- License key description

- Veritas Operations Manager product branding

System requirements

This section describes the system requirements for this release.

Hardware compatibility list

The compatibility list contains information about supported hardware and is updated regularly. For the latest information on supported hardware go to the following URL:

<http://www.symantec.com/docs/TECH211575>

Supported Linux operating systems

This section lists the supported operating systems for this release of Symantec products. For current updates, visit the Symantec Operations Readiness Tools Installation and Upgrade page: https://sort.symantec.com/land/install_and_upgrade.

Table 1-3 shows the supported operating systems for this release.

Table 1-3 Supported operating systems

Operating systems	Levels	Kernel version
Red Hat Enterprise Linux 6	Update 3	2.6.32-279.el6
	Update 4	2.6.32-358.el6
	Update 5	2.6.32-431.el6
	Note: Update 5 is supported if you install the required VxFS, LLT, and ODM patches. See the section called "Support for RHEL 6.5 and OL 6.5" on page 17.	

Table 1-3 Supported operating systems (*continued*)

Operating systems	Levels	Kernel version
Red Hat Enterprise Linux 5	Update 5	2.6.18-194.el5
	Update 6	2.6.18-238.el5
	Update 7	2.6.18-274.el5
	Update 8	2.6.18-308.el5
	Update 9	2.6.18-348.el5
	Update 10	2.6.18-371.el5
SUSE Linux Enterprise 11	SP2	3.0.13-0.27.1
	SP3	3.0.76-0.11.1
Oracle Linux 6	Update 3	2.6.32-279.el6
	Update 4	2.6.32-358.el6
	Update 5	2.6.32-431.el6
	Note: Update 5 is supported if you install the required VxFS, LLT, and ODM patches. See the section called "Support for RHEL 6.5 and OL 6.5" on page 17.	
Oracle Linux 5	Update 5	2.6.18-194.el5
	Update 6	2.6.18-238.el5
	Update 7	2.6.18-274.el5
	Update 8	2.6.18-308.el5
	Update 9	2.6.18-348.el5
	Update 10	2.6.18-371.el5

Note: Oracle Linux is supported with Red Hat Enterprise Linux compatible kernel only. Oracle Linux Unbreakable Enterprise Kernel is not supported.

Note: All subsequent kernel versions and patch releases on the supported operating system levels are supported, but you should check the Symantec Operations Readiness Tools (SORT) website for additional information that applies to the exact kernel version for which you plan to deploy.

Note: Only 64-bit operating systems are supported on the AMD Opteron or the Intel Xeon EM64T (x86_64) Processor line.

If your system is running an older version of either Red Hat Enterprise Linux, SUSE Linux Enterprise Server, or Oracle Linux, upgrade it before attempting to install the Symantec software. Consult the Red Hat, SUSE, or Oracle documentation for more information on upgrading or reinstalling your operating system.

Symantec supports only Oracle, Red Hat, and SUSE distributed kernel binaries.

Support for RHEL 6.5 and OL 6.5

Symantec Storage Foundation and High Availability Solutions (SFHA) 6.1 by default does not support RHEL 6.5 and Oracle Linux (OL) 6.5 due to incompatibility in the kernel interface in the Veritas File System (VxFS), Low Latency Transport (LLT), and Oracle Disk Manager (ODM) components of SFHA.

To support RHEL 6.5 and OL 6.5, you must install SFHA 6.1, and then install the required VxFS, LLT, and ODM patches as described in [Table 1-4](#) to resolve the kernel incompatibility.

Table 1-4 Required VxFS, LLT, and ODM patches

RPM name	Minimum patch level	Platform
VRTSvxfs	6.1.0.200	RHEL 6
VRTSllt	6.1.0.100	RHEL 6
VRTSodm	6.1.0.100	RHEL 6

You can obtain the required VxFS, LLT, and ODM patches from the Symantec Operations Readiness Tools (SORT) Patch Finder page at:

<https://sort.symantec.com/patch/finder>

Required Linux RPMs for DMP

Make sure you install the following operating system-specific RPMs on the systems where you want to install or upgrade DMP. DMP will support any updates made to the following RPMs, provided the RPMs maintain the ABI compatibility.

Note: Some required RHEL RPMs have different version numbers between RHEL update versions.

Table 1-5 lists the RPMs that DMP requires for a given Linux operating system.

Table 1-5 Required RPMs

Operating system	Required RPMs
OL 6	glibc-2.12-1.80.el6.i686.rpm glibc-2.12-1.80.el6.x86_64.rpm libgcc-4.4.6-4.el6.i686.rpm libgcc-4.4.6-4.el6.x86_64.rpm libstdc++-4.4.6-4.el6.i686.rpm libstdc++-4.4.6-4.el6.x86_64.rpm nss-softokn-freebl-3.12.9-11.el6.i686.rpm parted-2.1-18.el6.x86_64.rpm policycoreutils-2.0.83-19.24.0.1.el6.x86_64.rpm
RHEL 5	parted-1.8.1-27.el5.i386.rpm parted-1.8.1-27.el5.x86_64.rpm policycoreutils-1.33.12-14.8.el5.x86_64.rpm
RHEL 6	glibc-2.12-1.80.el6.i686.rpm glibc-2.12-1.80.el6.x86_64.rpm libgcc-4.4.6-4.el6.i686.rpm libgcc-4.4.6-4.el6.x86_64.rpm libstdc++-4.4.6-4.el6.i686.rpm libstdc++-4.4.6-4.el6.x86_64.rpm nss-softokn-freebl-3.12.9-11.el6.i686.rpm parted-2.1-18.el6.x86_64.rpm policycoreutils-2.0.83-19.24.el6.x86_64.rpm
SLES 11 SP2	parted-2.3-10.21.18.x86_64.rpm
SLES 11 SP3	parted-2.3-10.38.16.x86_64.rpm

Fixed issues

This section covers the incidents that are fixed in this release.

Installation and upgrades fixed issues

There are no install and upgrade fixed issues in this release.

Dynamic Multi-Pathing fixed issues

This section describes the incidents that are fixed for Dynamic Multi-Pathing in this release.

Table 1-6 Dynamic Multi-Pathing fixed issues

Incident	Description
3261601	<code>dmp_destroy_dmpnode</code> trying to free an already freed address.
3240858	The <code>/etc/vx/vxesd/.udev_lock</code> file may have different permissions at different instances.
3236773	Multiple error messages of format <code>vxndmp V-5-3-0 dmp_indirect_ioctl: Ioctl Failed</code> can be seen during <code>set/get failover-mode</code> for EMC ALUA disk array.
3218013	Dynamic Reconfiguration (DR) Tool does not delete stale OS (Operating System) device handles.
3194358	Continuous I/O error messages on OS device and DMP node can be seen in the syslog associated with the EMC Symmetrix not-ready (NR) LUNs.
3186149	On Linux system with LVM version 2.02.85, on enabling <code>dmp_native_support</code> LVM volume groups disappear.
3162418	The <code>vxconfigd(1M)</code> command dumps core due to an incorrect check in the <code>ddl_find_cdevno()</code> function.
3139983	Fix the design issues w.r.t to fixed, timebound and <code>path_busy</code> error retry.
3137603	VxDMP module not getting loaded after bundle installation and reboot.
3088059	On Red Hat Enterprise Linux 6.x (RHEL6.x), the type of host bus adapter (HBA) is reported as SCSI instead of FC.
3063378	Some DMP commands run slowly when EMC PowerPath presents and manages "read only" devices such as EMC SRDF-WD or BCV-NR.
3038684	Restore daemon enables the paths of BCV NR devices.

Table 1-6 Dynamic Multi-Pathing fixed issues (*continued*)

Incident	Description
3002770	While issuing a SCSI inquiry command, NULL pointer dereference in DMP causes system panic.
2992667	When new disks are added to the SAN framework of the Virtual Intelligent System (VIS) appliance and the Fibre Channel (FC) switcher is changed to the direct connection, the <code>vxdisk list</code> command does not show the newly added disks even after the <code>vxdisk scandisks</code> command is executed.
2970368	Enhance handling of SRDF-R2 Write-Disabled devices in DMP.
2969844	The device discovery failure should not cause the DMP database to be destroyed completely.
2959733	Handling the device path reconfiguration in case the device paths are moved across LUNs or enclosures to prevent the <code>vxconfigd(1M)</code> daemon coredump.
2946440	Add back the support for "INF" for LSI and ENGONIO VIDs to the LSI ASL.
2945658	If the Disk label is modified for an Active/Passive LUN, then the current passive paths do not reflect this modification after a failover.
2943637	DMP IO statistic thread may cause out of memory issue so that OOM (Out Of Memory) killer is invoked and causes system panic.
2925893	Make changes to Huawei APM to skip re-registering the keys on Secondary during failover.
2874810	Installing DMP with a keyless license or DMP-only license does not enable DMP native support for LVM root volumes
2839059	<code>vxconfigd</code> logged the warning <code>cannot open /dev/vx/rmp/cciss/c0d device to check for ASM disk format.</code>
2753954	At cable disconnect on port1 of dual-port FC HBA, paths via port2 marked SUSPECT.
2643506	<code>vxconfigd</code> core dumps when different LUNs of same enclosure are configured with different array modes.
2567618	The VRTSexplorer dumps core in <code>vxcheckhbaapi/print_target_map_entry</code> .
2510928	The extended attributes reported by <code>vxdisk -e list</code> for the EMC SRDF luns are reported as <code>tdev mirror</code> , instead of <code>tdev srdf-r1</code> .

Table 1-6 Dynamic Multi-Pathing fixed issues (*continued*)

Incident	Description
2421823	Turning off the DMP native support does not reset the preferred_names field in lvm.conf to the original values

Known issues

This section covers the known issues in this release.

Installation known issues

This section describes the known issues during installation and upgrade.

Error messages in syslog (1630188)

If you install or uninstall a product on a node with SELinux enabled, you may see the following warnings in syslog: /var/log/message. These warnings are harmless and can be ignored.

```
Jul  6 10:58:50 swlx62 setroubleshoot: SELinux is preventing the
semanage from using potentially mislabeled files
(/var/tmp/installer-200907061052eVe/install1.swlx62.VRTSvxvm). For
complete SELinux messages. run sealert -l ed8978d1-0b1b-4c5b-a086-
67da2a651fb3
```

```
Jul  6 10:58:54 swlx62 setroubleshoot: SELinux is preventing the
semanage from using potentially mislabeled files
(/var/tmp/installer-200907061052eVe/install1.swlx62.VRTSvxvm). For
complete SELinux messages. run sealert -l ed8978d1-0b1b-4c5b-a086-
67da2a651fb3
```

```
Jul  6 10:58:59 swlx62 setroubleshoot: SELinux is preventing the
restorecon from using potentially mislabeled files
```

Web installer does not ask for authentication after the first session if the browser is still open (2509330)

If you install or configure DMP and then close the Web installer, if you have other browser windows open, the Web installer does not ask for authentication in the subsequent sessions. Since there is no option to log out of the Web installer, the session remains open as long as the browser is open on the system.

Workaround: Make sure that all browser windows are closed to end the browser session and subsequently log in again.

Stopping the Web installer causes Device Busy error messages (2633924)

If you start the Web installer, and then perform an operation (such as prechecking, configuring, or uninstalling), you may get an error message saying the device is busy.

Workaround: Do one of the following:

- Kill the start.pl process.
- Start the webinstaller again. On the first Web page you see that the session is still active. Either take over this session and finish it or terminate it directly.

The uninstaller does not remove all scripts (2696033)

After removing DMP, some of the RC scripts remain in the `/etc/rc*.d/` folder. This is due to an issue with the `chkconfig` rpm in RHEL6 and updates. You can manually remove the scripts from the `/etc/rc*.d/` folder after removing the VxVM RPMs.

Workaround: Install the `chkconfig-1.3.49.3-1` `chkconfig` rpm from the RedHat portal. Refer to the following links:

<http://grokbase.com/t/centos/centos/117pfne4zz/centos-6-0-chkconfig-strange-behavior>

<http://rhn.redhat.com/errata/RHBA-2012-0415.html>

Changes in enclosure attributes are not persistent after an upgrade from release prior to VxVM 5.1SP1 (2082414)

The Veritas Volume Manager (VxVM) 6.1 includes several array names that differ from the array names in releases 5.1SP1 or prior. Therefore, if you upgrade to VxVM 6.1 from a release 5.1SP1 or earlier, changes in the enclosure attributes may not remain persistent. Any enclosure attribute set for these arrays may be reset to the default value after an upgrade to VxVM 6.1. Manually reconfigure the enclosure attributes to resolve the issue.

Table 1-7 shows the Hitachi arrays that have new array names.

Table 1-7 Hitachi arrays with new array names

Previous name	New name
TagmaStore-USP	Hitachi_USP
TagmaStore-NSC	Hitachi_NSC
TagmaStoreUSPV	Hitachi_USP-V

Table 1-7 Hitachi arrays with new array names (*continued*)

Previous name	New name
TagmaStoreUSPVM	Hitachi_USP-VM
<New Addition>	Hitachi_R700
Hitachi AMS2300 Series arrays	New array names are based on the Model Number 8x. For example, AMS_100, AMS_2100, AMS_2300, AMS_2500, etc.

In addition, the Array Support Library (ASL) for the enclosures XIV and 3PAR now converts the cabinet serial number that is reported from Hex to Decimal, to correspond with the value shown on the GUI. Because the cabinet serial number has changed, any enclosure attribute set for these arrays may be reset to the default value after an upgrade to VxVM 6.1. Manually reconfigure the enclosure attributes to resolve the issue.

The cabinet serial numbers are changed for the following enclosures:

- IBM XIV Series arrays
- 3PAR arrays

DMP disables subpaths and initiates failover when an iSCSI link is failed and recovered within 5 seconds. (2100039)

When using iSCSI S/W initiator with an EMC CLARiiON array, iSCSI connection errors may cause DMP to disable subpaths and initiate failover. This situation occurs when an iSCSI link is failed and recovered within 5 seconds.

Workaround:

When using iSCSI S/W initiator with an EMC CLARiiON array, set the `node.session.timeo.replacement_timeout` iSCSI tunable value to 40 secs or higher.

DMP panics if a DDL device discovery is initiated immediately after loss of connectivity to the storage (2040929)

When using EMC Powerpath with VxVM 5.1SP1 on SLES11, set the `fast_io_fail_tmo` on the HBA port to any non-zero value that is less than the `dev_loss_tmo` value so as to avoid a panic in case a DDL device discovery is initiated by the `vxdisk scandisks` command or the `vxctl enable` command immediately after loss of connectivity to the storage.

Upgrading the Linux kernel when the root volume is under DMP control

This section includes the procedures for upgrading the Linux kernel when the root volume is under DMP control.

Linux kernel can be upgraded on RHEL5 systems without turning off the DMP native support. Only one reboot is required to bring system LVM volume on DMP after kernel upgrade.

To update the kernel on a RHEL5 system

- 1 Update kernel with the rpm command.

```
# rpm -ivh kernel_rpm
```

- 2 Turn on the dmp_native_support tunable:

```
# vxddm padm settune dmp_native_support=on
```

This enables booting with new kernel with LVM devices with DMP.

- 3 Reboot.

On SLES11

On SLES, the kernel can not be upgraded in a single reboot due to limitation in mkinitrd command.

To update the kernel on a SLES11 system

- 1 Turn off DMP native support

```
# vxddm padm settune dmp_native_support=off
```

- 2 Reboot the system.
- 3 Upgrade kernel using the rpm command

```
# rpm -ivh kernel_rpm
```

- 4 Turn on DMP native support.

```
# vxddm padm settune dmp_native_support=on
```

- 5 Reboot the system to bring the root LVM volume under DMP control.

Adding a DMP device or its OS device path as a foreign disk is not supported (2062230)

When DMP native support is enable, adding a DMP device or its OS device path as a foreign disk using the `vxddladm addforeign` command is not supported. Using this command can lead to unexplained behavior.

After rebooting the array controller for CX4-240-APF array, I/O errors occur on shared file systems (2616315)

For Linux hosts, rebooting the array controller for a CX4-240-APF array may result in I/O errors on shared file systems.

Workaround:

To work around this issue

- ◆ Set the tunable parameter `dmp_lun_retry_timeout` to 120 seconds before rebooting the array controller.

```
# vxddm padm settune dmp_lun_retry_timeout=120
```

Continuous trespass loop when a CLARiiON LUN is mapped to a different host than its snapshot (2761567)

If a CLARiiON LUN is mapped to a different host than its snapshot, a trespass on one of them could cause a trespass on the other. This behavior could result in a loop for these LUNs, as DMP tries to fail back the LUNs if the primary paths are available.

Workaround

To avoid this issue, turn off the `dmp_monitor_ownership` tunable:

```
# vxddm padm settune dmp_monitor_ownership=off
```

With DMP native support enabled, pvscan can report PV on a OS device path instead of DMP device (2974210)

After a device loss, the Linux OS removes device files after the time out value configured with the `dev_loss_tmo` setting. When the device comes back online, the device names may have changed. The LVM filters do not get updated with the new device names. As a result, `pvscan` can report PV on a OS device path instead of DMP device.

Workaround:

When you enable DMP native support, increase the time out value configured with the `dev_loss_tmo` setting.

To increase the `dev_loss_tmo` setting

- 1 Create the file `/etc/udev/rules.d/40-rport.rules` with the following content line:

```
KERNEL=="rport-*", SUBSYSTEM=="fc_remote_ports", ACTION=="add",  
RUN+="/bin/sh -c 'echo 20 > /sys/class/fc_remote_ports/%k/  
fast_io_fail_tmo; echo 864000 > /sys/class/fc_remote_ports/%k/  
dev_loss_tmo'"
```

- 2 Reboot the system.
- 3 When new LUNs are dynamically assigned to the system, run the following command:

```
# udevadm trigger --action=add --subsystem-match=fc_remote_ports
```

The DMP EMC CLARiiON ASL does not recognize mirror view not ready LUNs (3272940)

On hosts that have EMC CLARiiON mirror view not ready LUNs, if you enable or disable the switch port and then issue the `vxdisk scandisks` or `vxctl enable` command, I/O error messages are written continuously in the `syslog`.

The dynamic multi-pathing (DMP) request for providing information to identify mirror view not ready LUNs through in-band SCSI command is pending with EMC engineering. Not ready LUNs are special kind of LUNs which reject all kinds of I/O requests.

Because DMP does not recognize not ready LUNs, Veritas Volume Manager (VxVM) tries to bring them online. As part of the online process, VxVM issues I/Os to read the disk private region. These I/Os fail and generate error messages in `syslog`.

Because of events that are generated as part of the online process, the `vxattachd` script triggers the `vxdisk scandisks` command again. This cycle causes continuous I/O error messages. This problem can also other commands to run slowly because the VxVM configuration daemon (`vxconfigd`) is busy servicing `vxdisk scandisks`.

Workaround: Stop the `vxattachd` script and:

1 Disable the `vxattachd` process.

For more information on how to disable `vxattachd` and what features you lose if `vxattachd` is disabled, see the `vxattachd` man page

2 Set the following EMC CLARiiON values:

- `recoveryoption=fixedretry`
- `retrycount=5`

Enter:

```
vxddmpadm setattr enclosure enclosure_name recoveryoption=fixedretry \  
retrycount=5
```

Virtualization known issues

This section describes the virtualization known issues in this release of Symantec Dynamic Multi-Pathing (DMP).

Agent kill on source during migration may lead to resource concurrency violation (3042499)

In the case of a migration initiated outside Symantec Cluster Server (VCS) control, there is a very small window in which the agent restart might not be able to recognize the migration event. As this is initiated outside VCS, there is no way to synchronize the agent restart and the migration. Also, there is no intermediate state in KVM that can indicate that the event was a migration. This problem does not occur in Red Hat Enterprise Virtualization (RHEV), as there are clear states visible that can specify the virtual machine events. This is applicable to KVM environment only.

Workaround: There is no workaround for this issue.

Subpaths may be removed from DMP database after I/O error occurs and become invisible inside the KVM guest (3214523)

After an I/O error occurs due to a path failure, devices may become invisible to DMP inside the KVM guest. This issue is caused by the current OS design.

The guest syslog will display the following message for the missing device:

```
detected capacity change from 107374182400 to 0
```

Workaround: When a device is missing from the `vxddmpadm getsubpaths all` output, recover the device.

To recover the missing device

- 1 Make sure the underlying device is accessible from the KVM host.
- 2 Inside the guest, re-read the partition table:

```
# blockdev --rereadpt /dev/device_name
```

- 3 Re-scan the devices in the OS device tree:

```
# vxdisk scandisks
```

Software limitations

This section covers the software limitations of this release.

See the corresponding Release Notes for a complete list of software limitations related to that component or product.

See [“Documentation”](#) on page 30.

DMP behavior on Linux SLES11 when connectivity to a path is lost (2049371)

On SLES 11, when the connectivity to a path is lost, the SLES 11 kernel removes the device path from its database. DMP reacts to the UDEV event that is raised in this process, and marks the device path as DISABLED[M]. DMP will not use the path for further I/Os. Unlike on other flavours of Linux, the path state is DISABLED[M] instead of DISABLED. Subsequently, if the path comes back online, DMP responds to the UDEV event to signal the addition of device path into SLES 11 kernel. DMP enables the path and changes its state to ENABLED.

DMP settings for NetApp storage attached environment

To minimize the path restoration window and maximize high availability in the NetApp storage attached environment, change the default values for the DMP tunable parameters.

[Table 1-8](#) describes the DMP tunable parameters and the new values.

Table 1-8 DMP settings for NetApp storage attached environment

Parameter name	Definition	New value	Default value
dmp_restore_interval	DMP restore daemon cycle	60 seconds.	300 seconds.

Table 1-8 DMP settings for NetApp storage attached environment (*continued*)

Parameter name	Definition	New value	Default value
dmp_path_age	DMP path aging tunable	120 seconds.	300 seconds.

The change is persistent across reboots.

To change the tunable parameters

- 1 Issue the following commands:

```
# vxddmpadm settune dmp_restore_interval=60
# vxddmpadm settune dmp_path_age=120
```

- 2 To verify the new settings, use the following commands:

```
# vxddmpadm gettune dmp_restore_interval
# vxddmpadm gettune dmp_path_age
```

LVM volume group in unusable state if last path is excluded from DMP (1976620)

When a DMP device is used by a native LVM volume group, do not exclude the last path to the device. This can put the LVM volume group in an unusable state.

Virtualization software limitations

This section describes the virtualization software limitations in this release of Symantec Dynamic Multi-Pathing (DMP).

Paths cannot be enabled inside a KVM guest if the devices have been previously removed and re-attached from the host

LUNs are exported to the KVM guest via virtio-scsi interface. When some physical link between the host and the SAN array fails for a certain time (45-60 seconds by default), the HBA driver in the host will remove the timed-out devices. When the link is restored, these devices will be re-attached to the host; however, the access from inside the KVM guest to these devices cannot be automatically restored too without rebooting the system or manually re-attaching the devices. For DMP, these subpaths will remain in DISABLED state.

This is a known limitation of KVM.

Workaround:

From the KVM host, tune the `dev_loss_tmo` parameter of the Fibre Channel ports to a very large value, and set the `fast_io_fail_tmo` parameter to 15.

To restore access to the timed-out devices

- 1 Add the following lines into `/dev/udev/rules.d/40-kvm-device` file:

```
KERNEL=="rport-*", SUBSYSTEM=="fc_remote_ports", ACTION=="add", \  
  RUN+="/bin/sh -c 'grep -q off \  
  /sys/class/fc_remote_ports/%k/fast_io_fail_tmo;if [ $? -eq 0 ]; \  
  then echo 15 > /sys/class/fc_remote_ports/%k/fast_io_fail_tmo 2> \  
  /dev/null;fi;'" \  
KERNEL=="rport-*", SUBSYSTEM=="fc_remote_ports", ACTION=="add", \  
  RUN+="/bin/sh -c 'echo 8000000 > \  
  /sys/class/fc_remote_ports/%k/dev_loss_tmo 2> /dev/null'"
```

- 2 Create the `/etc/modprobe.d/qla2xxx.conf` file with the following content:

```
options qla2xxx qlport_down_retry=8000000
```

- 3 Create the `/etc/modprobe.d/scsi_transport_fc.conf` with the following content:

```
options scsi_transport_fc dev_loss_tmo=8000000
```

- 4 Rebuild the `initrd` file and reboot.

Documentation

Product guides are available in the PDF format on the software media in the `/docs/product_name` directory. Additional documentation is available online.

Make sure that you are using the current version of documentation. The document version appears on page 2 of each guide. The publication date appears on the title page of each document. The latest product documentation is available on the Symantec website.

<http://sort.symantec.com/documents>

Documentation set

Each product in the Storage Foundation and High Availability Solutions product line includes release notes, an installation guide, and additional documents such as

administration and agent guides. In most cases, you may also need to refer to the documentation for the product's components.

The SFHA Solutions documents describe functionality and solutions that apply across the product line. These documents are relevant whichever SFHA Solutions product you use.

Symantec Dynamic Multi-Pathing documentation

[Table 1-9](#) lists the documentation for Symantec Dynamic Multi-Pathing.

Table 1-9 Symantec Dynamic Multi-Pathing documentation

Document title	File name	Description
<i>Symantec Dynamic Multi-Pathing Release Notes</i>	dmp_notes_61_lin.pdf	Provides release information such as system requirements, changes, fixed incidents, known issues, and limitations of the product.
<i>Symantec Dynamic Multi-Pathing Installation Guide</i>	dmp_install_61_lin.pdf	Provides information required to install the product.
<i>Symantec Dynamic Multi-Pathing Administrator's Guide</i>	dmp_admin_61_lin.pdf	Provides information required for administering the product.

Veritas Operations Manager (VOM) is a management tool that you can use to manage Symantec Storage Foundation and High Availability Solutions products. If you use VOM, refer to the VOM product documentation at:

<https://sort.symantec.com/documents>

Manual pages

The manual pages for Symantec Storage Foundation and High Availability Solutions products are installed in the `/opt/VRTS/man` directory.

Set the `MANPATH` environment variable so the `man(1)` command can point to the Symantec Storage Foundation manual pages:

- For the Bourne or Korn shell (`sh` or `ksh`), enter the following commands:

```
MANPATH=$MANPATH:/opt/VRTS/man
export MANPATH
```

- For C shell (`csh` or `tcsh`), enter the following command:

```
setenv MANPATH ${MANPATH}:/opt/VRTS/man
```

See the `man(1)` manual page.

Manual pages are divided into sections 1, 1M, 3N, 4, and 4M. Edit the `man(1)` configuration file `/etc/man.config` to view these pages.

To edit the `man(1)` configuration file

- 1 If you use the `man` command to access manual pages, set `LC_ALL` to “C” in your shell to ensure that the pages are displayed correctly.

```
export LC_ALL=C
```

See incident 82099 on the Red Hat Linux support website for more information.

- 2 Add the following line to `/etc/man.config`:

```
MANPATH /opt/VRTS/man
```

where other `man` paths are specified in the configuration file.

- 3 Add new section numbers. Change the line:

```
MANSECT          1:8:2:3:4:5:6:7:9:tcl:n:l:p:o
```

to

```
MANSECT          1:8:2:3:4:5:6:7:9:tcl:n:l:p:o:3n:1m
```

The latest manual pages are available online in HTML format on the Symantec website at:

<https://sort.symantec.com/documents>