

Veritas™ Dynamic Multi-Pathing 6.0.1 Release Notes - Linux

January 2013



Veritas™ 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: 6.0.1

Document version: 6.0.1 Rev 4

Legal Notice

Copyright © 2013 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. 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 [supportolutions@symantec.com](mailto:supportsolutions@symantec.com)

Dynamic Multi-Pathing Release Notes

This document includes the following topics:

- [About this document](#)
- [About Veritas Dynamic Multi-Pathing \(DMP\)](#)
- [About Symantec Operations Readiness Tools](#)
- [Important release information](#)
- [Changes introduced in DMP 6.0.1](#)
- [System requirements](#)
- [DMP: issues fixed in 6.0.1](#)
- [Known issues](#)
- [Software limitations](#)
- [Documentation](#)

About this document

This document provides important information about Veritas Dynamic Multi-Pathing (DMP) version 6.0.1 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: 6.0.1 Rev 4" of the *Veritas 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 Veritas Dynamic Multi-Pathing (DMP)

Veritas Dynamic Multi-Pathing (DMP) provides multi-pathing functionality for the operating system native devices 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 stand-alone 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.

Veritas 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, a SF HA 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 Web site 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 | <ul style="list-style-type: none">■ 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.■ Download the latest patches, documentation, and high availability agents from a central repository.■ Access up-to-date compatibility lists for hardware, software, databases, and operating systems. |
| Manage risks | <ul style="list-style-type: none">■ Get automatic email notifications about changes to patches, array-specific modules (ASLs/APMs/DDIs/DDLs), and high availability agents from a central repository.■ Identify and mitigate system and environmental risks.■ Display descriptions and solutions for hundreds of Symantec error codes. |
| Improve efficiency | <ul style="list-style-type: none">■ Find and download patches based on product version and platform.■ List installed Symantec products and license keys.■ Tune and optimize your environment. |

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/TECH164885>
- 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/TECH170013>

Before installing or upgrading Storage Foundation and High Availability Solutions products, review the current compatibility list to confirm the compatibility of your hardware and software.

Changes introduced in DMP 6.0.1

This section lists the changes in Veritas Dynamic Multi-Pathing 6.0.1.

New versioning process for SFHA Solutions products

Symantec made some changes to simplify the versioning process to ensure that customers have a unified experience when it comes to deploying our different products across Storage, Availability, Backup, Archiving and Enterprise Security products. With this change, all the products will have a 3 digit version. In complying with this approach, the current SFHA Solutions release is available as version 6.0.1.

New directory location for the documentation on the software media

The PDF files of the product documentation are now located in the `/docs` directory on the software media. Within the `/docs` directory are subdirectories for each of the bundled products, which contain the documentation specific to that product. The `sfha_solutions` directory contains documentation that applies to all products.

Dynamic Reconfiguration tool

Dynamic Multi-Pathing provides a Dynamic Reconfiguration tool. The Dynamic Reconfiguration tool is an interactive tool to automate dynamic reconfiguration of LUNs or HBAs. Dynamic reconfiguration includes addition, removal or replacement of LUNs, and replacement of certain HBAs, without requiring a reboot. The Dynamic Reconfiguration tool simplifies the process, so that you do not need a complex set of DMP and operating system related commands.

Enhanced support for Fusion-io iodrive and iodrive2 on Linux

In this release, support for Fusion-io iodrive and iodrive2 is enhanced to support TRIM operations. TRIM operations erase unused blocks of data to improve SSD performance. The future writes on the Fusion-io cards are more efficient.

The DMP components, Veritas File System (VxFS) and Veritas Volume Manager (VxVM), use the TRIM operations to free up the blocks that do not contain valid data. The TRIM capability is similar to thin reclamation, and is performed with the same commands.

DMP supports the TRIM operation for Fusion-io devices for Red Hat Linux 6.0 (RHEL6) and SUSE Linux Enterprise Server 11 (SLES11).

Changes in supported Linux virtualization technologies

Veritas Storage Foundation and High Availability (SFHA) Solutions 6.0.1 products support the following virtualization technologies in Linux environments:

- Kernel-based Virtual Machine (KVM) technology for Red Hat Enterprise Linux (RHEL)
- Kernel-based Virtual Machine (KVM) technology for SUSE Linux Enterprise Server (SLES)

SFHA Solutions products provide the following functionality for KVM guest virtual machines:

- Storage visibility
- Storage management
- High availability
- Cluster failover
- Replication support

Table 1-1 SFHA Solutions supported configurations in guest and host for KVM technologies

Objective	Recommended SFHA Solutions product configuration	KVM technology
Storage visibility for KVM guest virtual machines	Dynamic Multi-Pathing (DMP) in the KVM guest virtual machines	RHEL SLES
Storage visibility for KVM hosts	DMP in the KVM hosts	RHEL SLES
Storage management features and replication support for KVM guest virtual machines	Storage Foundation (SF) in the KVM guest virtual machines	RHEL SLES
Advanced storage management features and replication support for KVM hosts	Storage Foundation Cluster File System (SFCFSHA) in the KVM hosts	RHEL SLES

Table 1-1 SFHA Solutions supported configurations in guest and host for KVM technologies (*continued*)

Objective	Recommended SFHA Solutions product configuration	KVM technology
End-to-end storage visibility in KVM hosts and guest virtual machines	DMP in the KVM host and guest virtual machines	RHEL SLES
Storage management features and replication support in the KVM guest virtual machines and storage visibility in in the KVM host	DMP in the KVM host and SF in the KVM guest virtual machines	RHEL SLES
Application monitoring and availability for KVM guest virtual machines	Symantec ApplicationHA in the KVM guest virtual machines	RHEL
Virtual machine monitoring and failover for KVM hosts	Veritas Cluster Server (VCS) in the KVM hosts	RHEL SLES
Application failover for KVM guest virtual machines	VCS in the KVM guest virtual machines	RHEL SLES
Application availability and virtual machine availability	Symantec Application HA in the KVM guest virtual machines and VCS in the KVM host	RHEL
Application failover across KVM guest virtual machines and physical hosts	VCS in KVM guest virtual machines and KVM physical host machines	RHEL SLES

VCS provides virtual to virtual (in-guest) clustering support for the following Linux virtualization environments:

- Red Hat Enterprise Virtualization (RHEV)
- Microsoft Hyper-V
- Oracle Virtual Machine (OVM)

For implementation details:

See the *Veritas Storage Foundation™ and High Availability Solutions Virtualization Guide for Linux*.

For VMware support, see *Veritas Storage Foundation in a VMware ESX Environment*.

Changes related to installation and upgrades

The product installer includes the following changes in 6.0.1.

Locally-installed installation and uninstallation scripts now include the release version

When you run local scripts (`/opt/VRTS/install`) to configure Veritas products, the names of the installed scripts now include the release version.

Note: If you install your Veritas product from the install media, continue to run the `installdmp` command without including the release version.

To run the script from the installed binaries, run the `installdmp<version>` command.

Where `<version>` is the current release version with no periods or spaces.

For example, to configure the 6.0.1 version of your product, run this command:

```
# /opt/VRTS/install/installdmp601 -configure
```

Support for tunables file templates

You can use the installer to create a tunables file template. If you start the installer with the `-tunables` option, you see a list of all supported tunables, and the location of the tunables file template.

Additional installation postcheck options

The `postcheck` option has been enhanced to include additional checks.

You can use the installer's post-check option to perform the following checks:

- General checks for all products.
- Checks for Volume Manager (VM).
- Checks for File System (FS).
- Checks for Cluster File System (CFS).

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/TECH170013>

Supported Linux operating systems

This section lists the supported operating systems for this release of Veritas products. For current updates, visit the Symantec Operation Readiness Tools Installation and Upgrade page:

https://sort.symantec.com/land/install_and_upgrade.

Table 1-2 shows the supported operating systems for this release.

Table 1-2 Supported operating systems

Operating systems	Levels	Kernel version	Chipsets
Red Hat Enterprise Linux 6	Update 1, 2, 3	2.6.32-131.0.15.el6 2.6.32-220.el6 2.6.32-279.el6	64-bit x86, EMT*/Opteron 4.1 64-bit only
Red Hat Enterprise Linux 5	Update 5, 6, 7, 8, 9	2.6.18-194.el5 2.6.18-238.el5 2.6.18-274.el5 2.6.18-308.el5 2.6.18-348.el5	64-bit x86, EMT*/Opteron 4.1 64-bit only
SUSE Linux Enterprise 11	SP1, SP2	2.6.32.12-0.7.1 3.0.13-0.27.1	64-bit x86, EMT*/Opteron 4.1 64-bit only
SUSE Linux Enterprise 10	SP4	2.6.16.60-0.85.1	64-bit x86, EMT*/Opteron 4.1 64-bit only

Table 1-2 Supported operating systems (*continued*)

Operating systems	Levels	Kernel version	Chipsets
Oracle Linux 6	Update 1, 2, 3	2.6.32-131.0.15.el6 2.6.32-220.el6 2.6.32-279.el6	64-bit x86, EMT*/Opteron 4.1 64-bit only
Oracle Linux 5	Update 5, 6, 7, 8, 9	2.6.18-194.el5 2.6.18-238.el5 2.6.18-274.el5 2.6.18-308.el5 2.6.18-348.el5	64-bit x86, EMT*/Opteron 4.1 64-bit only

* Extended Memory Technology

Note: Only 64-bit operating systems are supported.

Note: For SLES11 SP2 kernel versions later than February, 2012, you need to apply the following Veritas patch: sf-sles11_x86_64-6.0.1.100. This patch is available on the patch download page at <https://sort.symantec.com/patch/detail/6732>.

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 Veritas 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.

Symantec products operate on subsequent kernel and patch releases provided the operating systems maintain kernel Application Binary Interface (ABI) compatibility.

DMP: issues fixed in 6.0.1

This section covers the incidents that are fixed in DMP 6.0.1.

Installation and upgrades: issues fixed in 6.0.1

This section describes the incidents that are fixed related to installation and upgrades in this release.

Table 1-3 Fixed issues related to installation and upgrades

Incident	Description
2627076	Incorrect server names sometimes display if there is a clock synchronization issue.
2585899	On RHEL, unable to create storage for OCR and Vote disk when using FQDN instead of using only the node name.
2526709	DMP-OSN tunable value not get persistence after upgrade from 5.1SP1 to 6.0.
2088827	During product migration the installer overestimates disk space use.

Installation and upgrades: Issues fixed in 6.0 RP1

There are no new fixed incidents for installation and upgrades in 6.0 RP1.

Dynamic Multi-Pathing: issues fixed in 6.0.1

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

Table 1-4 Veritas Dynamic Multi-Pathing fixed issues

Incident	Description
2826958	pwwn no is not displayed in the output of command "vxddmpadm list dmpnode dmpnodename=".
2818840	Enhance the vxddmpraw utility to support permission and root:non-system ownership be set and make it persistent.
2794625	Unable to configure ASM to use DMP native block device path.
2792242	I/O hang after performing zone remove/add operations.
2743926	DMP restored fails to restart during system boot in 6.0.
2729501	exclude path not working properly and can cause system hang while coming up after enabling native support.
2700086	EMC BCV (NR) established devices are resulting in multiple dmp events messages (paths being disabled/enabled).
2652485	Inactive snapshot luns cause trespassing.

Table 1-4 Veritas Dynamic Multi-Pathing fixed issues (*continued*)

Incident	Description
2626199	vxdmpadm list dmpnode printing incorrect path-type.
2564092	[VxVM][Usability]Automate the lun provisioning (addition) / removal steps using vxdiskadm /or new VxVM CLI command.
2556467	DMP-ASM: disable all paths and reboot host cause /etc/vx/vxdmprawdev records losing.

Known issues

This section covers the known issues in this release.

Changes in enclosure attributes are not persistent after an upgrade to VxVM 6.0.1 (2082414)

The Veritas Volume Manager (VxVM) 6.0.1 includes several array names that differ from the array names in releases prior to release 5.1SP1. Therefore, if you upgrade from a previous release to VxVM 6.0.1, 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 6.0.1. Manually reconfigure the enclosure attributes to resolve the issue.

[Table 1-5](#) shows the Hitachi arrays that have new array names.

Table 1-5 Hitachi arrays with new array names

Previous name	New name
TagmaStore-USP	Hitachi_USP
TagmaStore-NSC	Hitachi_NSC
TagmaStoreUSPV	Hitachi_USP-V
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 6.0.1. 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 marks the subpaths as DISABLED while these subpaths are accessible from OS level (2037222)

For iSCSI devices on SLES 10 SP3, the DMP tunable parameter `dmp_fast_recovery` needs to be turned off.

```
# vxddmpadm settune dmp_fast_recovery=off
```

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 (2080909)

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 adm settune dmp_native_support=on
```

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

- 3 Reboot.

On SLES10 or 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 SLES10 or SLES11 system

- 1 Turn off DMP native support

```
# vxddm adm 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 adm 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.

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

When you turn off the native support, the preferred_names field in lvm.conf is not reset to the original value. LVM does not function correctly with Device Mapper Volumes.

Workaround: Manually edit the lvm.conf file, and then Run `vgscan` command

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.

```
# vxddpadm 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:

```
# vxddpadm settune dmp_monitor_ownership=off
```

In some cases with large LUN setup, the storage disappears after DMP device scan (2828328)

This issue is typically seen on a large LUN setup. In some cases, the storage disappears after the DMP device scan. The DMP device scan is generated with the `vxdisk scandisks` command or the `vxctl enable` command. Even if the OS command `ioscan` can discover devices, VxVM/DMP cannot.

Workaround:

Restarting the `vxconfigd` daemon on the affected node may resolve the issue. If that does not work, you must reboot the system.

Enabling or installing DMP for native support may not migrate LVM volumes to DMP (2737452)

On Linux System with LVM version 2.02.85, installing DMP or enabling `dmp_native_support` for DMP may not migrate LVM volumes to DMP. LVM Volume Groups may disappear.

From LVM version 2.02.85 onwards, device list is obtained from `udev` by default if LVM2 is compiled with UDEV support. This setting is managed using `obtain_device_list_from_udev` variable in `/etc/lvm/lvm.conf`. As DMP devices are not managed by UDEV, they will not be used by LVM. Thus LVM volumes are not migrated.

Workaround:

For LVM version 2.02.85 onwards, for DMP native support, always disable UDEV support for LVM by adding following line to `/etc/lvm/lvm.conf` in “devices” section:

```
obtain_device_list_from_udev = 0
```

Then install the package or enable `dmp_native_support` tunable. If `dmp_native_support` is already enabled then run the following command for applying changes:

```
# vxddmpadm settune dmp_native_support=on
```

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, 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/install.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/install.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 packages.

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/117pfhe4zz/centos-6-0-chkconfig-strange-behavior>

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

Installing DMP with a keyless license or DMP-only license does not enable DMP native support for LVM root volumes (2874810)

When you install DMP with a keyless license or DMP-only license, the tunable parameter `dmp_native_support` is set to on. However, the DMP native support is not enabled for LVM root volumes. The DMP native support is enabled for non-root LVM volumes.

Workaround:

After package installation, use the following command to enable the DMP support for root LVM volumes.

```
# vxdmpadm settune dmp_native_support=on
```

Then reboot the system.

Perl module error on completion of DMP installation (2873102)

When you install, configure, or uninstall DMP, the installer prompts you to optionally upload installation logs to the Symantec Web site. If the installer encounters connectivity problems, you may see an error similar to the following:

```
Status read failed: Connection reset by peer at  
<midia_path>/../perl/lib/5.14.2/Net/HTTP/Methods.pm line 269.
```

Workaround:

Ignore this error. It is harmless.

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 25.

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, set the following DMP tunables:

Table 1-6

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

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

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

```
# vxdmpadm gettune dmp_restore_interval  
# vxdmpadm 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.

DMP does not support devices in the same enclosure that are configured in different modes (2643506)

DMP does not support the configuration where two devices in the same enclosure are configured in different modes. For example, if one device is configured as ALUA and another one is configured as Active/Passive (A/P).

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

[Table 1-7](#) lists the documentation for Veritas Dynamic Multi-Pathing.

Table 1-7 Veritas Dynamic Multi-Pathing documentation

Document title	File name
<i>Veritas Dynamic Multi-Pathing Release Notes</i>	dmp_notes_601_lin.pdf
<i>Veritas Dynamic Multi-Pathing Installation Guide</i>	dmp_install_601_lin.pdf
<i>Veritas Dynamic Multi-Pathing Administrator's Guide</i>	dmp_admin_601_lin.pdf

If you use Veritas Operations Manager (VOM) to manage Veritas Storage Foundation and High Availability products, refer to the VOM product documentation at:

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

Manual pages

The manual pages for Veritas 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 Veritas 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
```