Symantec™ Dynamic Multi-Pathing 6.2 Release Notes - Linux

November 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: 6.2

Document version: 6.2 Rev 1

Legal Notice

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_apj@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

This document provides important information about Symantec Dynamic Multi-Pathing (DMP) version 6.2 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: 6.2 Rev 1" 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/TECH225259
- 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/TECH225258

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 6.2

This section lists the changes in Symantec Dynamic Multi-Pathing 6.2.

Changes related to installation and upgrades

The product installer includes the following changes in Symantec Dynamic Multi-Pathing 6.2.

Connecting to the SORT website through a proxy server

The product installer connects to the Symantec Operations Readiness Tools (SORT) website for several purposes, such as downloading latest installer patches, and uploading installer logs; Deployment Server can connect to SORT to automatically download Maintenance or Patch release images. In this release, before running the product installer or Deployment Server, you can use the following proxy settings to connect to SORT through proxy servers:

```
# https_proxy=http://proxy_server:port
# export https_proxy
# ftp_proxy=http://proxy_server:port
# export ftp_proxy
```

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 platform (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
Install or Upgrade systems with Install Bundle and Install Template	■ Install or upgrade systems with an Install Bundle. ■ Install packages on systems based on the information stored in Install Template.
Define or modify Install Bundles	Define or modify Install Bundles and save them using the Deployment Server.
Create Install Templates	Discover installed components on a running system that you want to replicate on to new systems.
Connecting the Deployment Server to SORT using a proxy server	Use a proxy server, a server that acts as an intermediary for requests from clients, for connecting the Deployment Server to the Symantec Operations Readiness Tools (SORT) website.

Table 1-1 Deployment Server functionality *(continued)*

Feature	Description
Platform Filtering	In Set Preference menu, choose Selected Platforms to filter the platforms that are currently being used in the deployment environment.

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 installation using the Red Hat Satellite server

You can install DMP using the Red Hat Satellite server. Red Hat Satellite is supported for Red Hat Enterprise Linux 6 (RHEL6) and Red Hat Enterprise Linux 7 (RHEL7). You can install RPMs and rolling patches on the systems which the Red Hat Satellite server manages.

In a Red Hat Satellite server, you can manage the system by creating a channel. A Red Hat Satellite channel is a collection of software packages. Using channels, you can segregate the packages by defining some rules.

Behavioral changes in RHEL 7 as compared with previous releases

Note the following behavioral changes in RHEL 7:

- XFS file system is not supported for the Root Disk Encapsulation (RDE) feature:
  RDE is not supported if the root partition is mounted with XFS file system.
- Enclosure-based naming (EBN) is not supported for RDE
  RDE, mirroring, splitting and joining operations on root disks are not supported if the naming scheme is set to EBN.

Release level terminology changes

With the 6.2 release, terms that are used to describe patch-based releases have changed as follows:

Table 1-2 Release level terminology changes

Pre 6.0.1	6.0.x, 6.1, 6.1.x	6.2 and forward	Status	Available from
P-Patch	Public hot fix	Patch	Official	SORT
Hot fix	Private hot fix	Hot fix	Unofficial	Customer support

Official patch releases are available from SORT. This release was previously referred to as a P-Patch or a Public hot fix and is now referred to as a Patch. Unofficial patch releases are available from customer support. Hot fix is the only unofficial patch release.

Support for setting up ssh and rsh connection using the pwdutil.pl utility

The password utility, `pwdutil.pl`, is bundled in the 6.2 release under the scripts directory. The users can run the `pwdutil.pl` utility to set up the ssh and rsh connection automatically.

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	Supported level and kernel version
Red Hat Enterprise Linux 7	3.10.0-123.el7

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

Operating systems	Supported level and 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) Update 6 (2.6.32-504.el6)
SUSE Linux Enterprise 11	SP2 (3.0.13-0.27.1) SP3 (3.0.76-0.11.1)
Oracle Linux 6 (RHEL compatible mode)	Update 3 (2.6.32-279.el6) Update 4 (2.6.32-358.el6) Update 5 (2.6.32-431.el6)
Oracle Linux 7 (RHEL compatible mode)	3.10.0-123.el7 **Note:** SF Oracle RAC has not yet announced support for Oracle Linux 7. You may find information pertaining to OL 7 in the installation and administrator guides. Note that this information will become relevant only after SF Oracle RAC announces support when due certification efforts are complete. Refer to the following TechNote for the latest information on the supported operating systems and Oracle RAC database versions. http://www.symantec.com/docs/DOC4848

Note: All subsequent kernel updates 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.

Note: Configuring LLT over RDMA is not supported with Oracle Linux Unbreakable Enterprise Kernel 2 that is 2.6.39-400.17.1.el6uek.x86_64.

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.

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

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 1-4 lists the RPMs that DMP requires for a given Linux operating system.

Table 1-4 Required RPMs

Operating system	Required RPMs
RHEL 7	glibc-2.17-55.el7.i686 glibc-2.17-55.el7.x86_64 libgcc-4.8.2-16.el7.i686 libgcc-4.8.2-16.el7.x86_64 libstdc++-4.8.2-16.el7.i686 libstdc++-4.8.2-16.el7.x86_64 nss-softokn-freebl-3.15.4-2.el7.i686 parted-3.1-17.el7.x86_64 policycoreutils-2.2.5-11.el7.x86_64

Table 1-4 Required RPMs *(continued)*

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 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

Additional RPMs required for Veritas Volume Manager

You must install the 32-bit `libudev` RPM before you install Veritas Volume Manager.

Table 1-5 lists the required RPMs.

Table 1-5 Additional RPMs required for Veritas Volume Manager

Operating system	Required RPMs
RHEL 7	systemd-libs-208-11.el7.i686.rpm
RHEL 6 Update 5	libudev-147-2.51.el6.i686.rpm

Table 1-5 Additional RPMs required for Veritas Volume Manager *(continued)*

Operating system	Required RPMs
RHEL 6 Update 4	libudev-147-2.46.el6.i686.rpm
RHEL 6 Update 3	libudev-147-2.41.el6.i686.rpm
SLES 11 SP3	libudev0-32bit-147-0.84.1.x86_64.rpm
SLES 11 SP2	libudev0-32bit-147-0.47.2.x86_64.rpm

Fixed issues

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

Installation and upgrades fixed issues

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

Table 1-6 Fixed issues related to installation and upgrades

Incident	Description
3326196	Rolling upgrade may encounter a problem if open volumes from different disk groups have the same name.
3442070	If you select rolling upgrade task from the Install Bundles menu, the Installer exits with an error.

Dynamic Multi-Pathing fixed issues

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

Table 1-7 Dynamic Multi-Pathing fixed issues

Incident	Description
3577586	Server panic while sending SCSI pkt from DMP.
3565212	IO failure during controller giveback operations on Netapp FAS31700 in ALUA mode.
3543284	FIO device not visible.

Table 1-7 Dynamic Multi-Pathing fixed issues *(continued)*

Incident	Description
3542713	vxdmpadm listenclosure all displays a different ENCL from array console/VOM.
3531385	Asynchronous access to per dmpnode request queues may cause system panic.
3526500	DMP I/O getting timeout lot earlier than 300 seconds if I/O statistics daemon is not running.
3520991	vxconfigd core dumps during vxdisk scandisks.
3502923	ESX panic while running add/remove devices from smartpool with no license installed on server.
3399323	The reconfiguration of DMP DB failed.
3373208	DMP wrongly sends APTPL bit 0 to array.

Known issues

This section covers the known issues in this release.

Installation known issues

This section describes the known issues during installation and upgrade.

`installer -requirements` does not list RHEL 6 Update 6 and Oracle Linux 7 as supported platforms (3657260)

The `installer -requirements` command does not list RHEL 6 Update 6 and Oracle Linux 7 as supported platforms though they are qualified with version 6.2.

Workaround: The correct supported list is mentioned in the latest version of the product Release Notes. See the latest Release Notes on the Symantec website for the updated list.

https://sort.symantec.com/documents

Installer reports incorrect minimal version for several required Oracle Linux 7 RPMs (3653382)

During installation, the product installer reports incorrect minimum version for the following required Oracle Linux 7 RPMs:

```
systemd-libs-208-11.el7.i686
coreutils-8.22-11.el7.x86_64
policycoreutils-2.2.5-11.el7.x86_64
```

The correct minimum version required for the RPMs is as follows:

```
systemd-libs-208-11.0.1.el7.i686.rpm
coreutils-8.22-11.0.1.el7.x86_64
policycoreutils-2.2.5-11.0.1.el7.x86_64
```

Workaround: Install the required operating system RPMs using native methods, such as yum, or install them manually.

Dependency may get overruled when uninstalling multiple RPMs in a single command [3563254]

When performing uninstallation of multiple RPMs through a single comment, the system identifies and follows the specified dependency among the RPMs as the uninstallation progresses. However, if the pre-uninstallation script fails for any of the RPMs, the system does not abort the task but instead uninstalls the remaining RPMs.

For example, if you run `rpm -e VRTSllt VRTSgab VRTSvxfen` where the RPMs have a dependency between each other, the system bypasses the dependency if the pre-uninstallation script fails for any RPM.

Workaround: Uninstall the RPMs independently.

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

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

Migration of I/O fencing-enabled disks of VxVM disk group from EMC PowerPath TPD to VxVM DMP fails [3528561]

If I/O Fencing is enabled on some disks from VxVM disk group, migration of those disks from EMC PowerPath TPD to VxVM DMP fails with the following error messages:

```
VXFEN vxfenconfig NOTICE Driver will use SCSI-3 compliant disks.
VXFEN vxfenconfig ERROR V-11-2-1090 Unable to register with a
Majority of the coordination points.
```

Workaround: Restart the server.

Symantec has reported the issue to EMC PowerPath Engineering.

XFS file system is not supported for RDE

The Root Disk Encapsulation (RDE) feature is not supported if the root partition is mounted with XFS file system.

Workaround: There is no workaround available.

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

The Veritas Volume Manager (VxVM) 6.2 includes several array names that differ from the array names in releases 5.1SP1 or prior. Therefore, if you upgrade to VxVM 6.2 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 6.2.

Workaround:

Manually reconfigure the enclosure attributes to resolve the issue.

Table 1-8 shows the Hitachi arrays that have new array names.

Table 1-8 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
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 6.2. 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.

Upgrading the Linux kernel when the root volume is under DMP control (3635249)

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

To update the kernel on RHEL 7 systems

1. Turn off the `dmp_native_support` tunable:

   ```
   # vxdmpadm settune dmp_native_support=off
   ```

   To relinquish control from DMP, reboot the system.

2. Update the kernel:

   ```
   # rpm -ivh kernel_rpm
   ```

   To boot the system using the new kernel, reboot the system.

3. Turn on the `dmp_native_support` tunable:

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

   If you want to bring the root LVM under DMP control, reboot the system.

To update the kernel on RHEL 6 systems

Perform the following steps to update the kernel with a single reboot of the system. Alternatively, you can also update the kernel using the steps given for RHEL 7.

1. Update kernel with the rpm command.

   ```
   # rpm -ivh kernel_rpm
   ```

2. Turn on the `dmp_native_support` tunable:

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

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

3. Reboot the system.

To update the kernel on SLES 11 or SLES 10 systems

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

1. Turn off DMP native support:

   ```
   # vxdmpadm settune dmp_native_support=off
   ```

2. Reboot the system.
3. Update the kernel:

   ```
   # rpm -ivh kernel_rpm
   ```

4. Turn on DMP native support.

   ```
   # vxdmpadm 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.

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:

```
# vxdmpadm 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 `vxdctl 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 cause other commands to run slowly because the VxVM configuration daemon (`vxconfigd`) is busy servicing `vxdisk scandisks`.

Workaround: Stop the `vxattachd` script and set EMC CLARiiON values, as follows:

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:

   ```
   vxdmpadm 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 `vxdmpadm 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 29.

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).

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 1-9 describes the DMP tunable parameters and the new values.

Table 1-9 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.
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.

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 1-10 lists the documentation for Symantec Dynamic Multi-Pathing.

Table 1-10 Symantec Dynamic Multi-Pathing documentation

Document title	File name	Description
Symantec Dynamic Multi-Pathing Release Notes	dmp_notes_62_lin.pdf	Provides release information such as system requirements, changes, fixed incidents, known issues, and limitations of the product.
Symantec Dynamic Multi-Pathing Installation Guide	dmp_install_62_lin.pdf	Provides information required to install the product.
Symantec Dynamic Multi-Pathing Administrator's Guide	dmp_admin_62_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