NetApp® Disaster Recovery Adapter 1.0.1 for VMware® vCenter Site Recovery Manager **Release Notes**

NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089 U.S.A.
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Documentation comments: doccomments@netapp.com
Information Web: http://www.netapp.com

Part number: 215-04421_A0
March 2009

Copyright and trademark information

Copyright information

Copyright © 1994–2009 NetApp, Inc. All rights reserved. Printed in the U.S.A.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

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

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NetApp, the Network Appliance logo, the bolt design, NetApp—the Network Appliance Company, Cryptainer, Cryptoshred, DataFabric, DataFort, Data ONTAP, Decru, FAServer, FilerView, FlexClone, FlexVol, Manage ONTAP, MultiStore, NearStore, NetCache, NOW NetApp on the Web, SANscreen, SecureShare, SnapDrive, SnapLock, SnapManager, SnapMirror, SnapMover, SnapRestore, SnapValidator, SnapVault, Spinnaker Networks, SpinCluster, SpinFS, SpinHA, SpinMove, SpinServer, StoreVault, SyncMirror, Topio, VFM, and WAFL are registered trademarks of NetApp, Inc. in the U.S.A. and/or other countries. gFiler, Network Appliance, SnapCopy, Snapshot, and The evolution of storage are trademarks of NetApp, Inc. in the U.S.A. and/or other countries and registered trademarks in some other countries. The NetApp arch logo; the StoreVault logo; ApplianceWatch; BareMetal; Camera-to-Viewer; ComplianceClock; ComplianceJournal; ContentDirector; ContentFabric; EdgeFiler; FlexShare; FPolicy; Go Further, Faster; HyperSAN; InfoFabric; Lifetime Key Management, LockVault; NOW; ONTAPI; OpenKey, RAID-DP; ReplicatorX; RoboCache; RoboFiler; SecureAdmin; Serving Data by Design; SharedStorage; Simplicore; Simulate ONTAP; Smart SAN; SnapCache; SnapDirector; SnapFilter; SnapMigrator; SnapSuite; SohoFiler; SpinMirror; SpinRestore; SpinShot; SpinStor; vFiler; VFM Virtual File

Manager; VPolicy; and Web Filer are trademarks of NetApp, Inc. in the U.S.A. and other countries. NetApp Availability Assurance and NetApp ProTech Expert are service marks of NetApp, Inc. in the U.S.A.

IBM, the IBM logo, AIX, and System Storage are trademarks and/or registered trademarks of International Business Machines Corporation.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the U.S.A. and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the U.S.A. and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the U.S.A. and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks. NetApp, Inc. NetCache is certified RealSystem compatible.

Topics covered

About this document

These release notes cover the following topics:

- "Audience" on page 2
- "Features of this release" on page 3
- "Site Recovery Manager and NetApp Disaster Recovery Adapter Overview" on page 4
- "System requirements and installation information" on page 7
- "Limitations" on page 9
- "Recommendations" on page 10
- "Guidelines for using the Data ONTAP API over SecureHTTP" on page 15
- "Troubleshooting" on page 16

Audience

These release notes are for system administrators using NetApp® array scripts with VMware® vCenter Site Recovery Manager. You must be familiar with ESX servers, VMware vCenter Site Recovery Manager for Windows, and storage systems running Data ONTAP® software. The release notes assumes that you are familiar with how to configure these systems and how the NFS, CIFS, HTTP, and SAN protocols (such as iSCSI and FC) are used for file sharing or transfers. The release notes do not cover basic system or network administration topics; they describe the various scripts and how the scripts are used during failover along with NetApp storage systems running Data ONTAP.

Features of this release

New and enhanced features

NetApp Disaster Recovery Adapter 1.0.1 for VMware vCenter Site Recovery Manager introduces support for raw device mapping (RDM) and NetApp active/active configuration.

For more information

For details about the new and enhanced features of Site Recovery Manager, see the Site Recovery Manager documentation.

Site Recovery Manager and NetApp Disaster Recovery Adapter Overview

What Site Recovery Manager does

Site Recovery Manager uses virtualization to provide end-to-end disaster recovery management and automation across the entire data center. Site Recovery Manager leverages VMware Infrastructure 3 to build, automate, and test disaster recovery plans for the data center. This makes disaster recovery rapid, reliable, affordable, and manageable. Site Recovery Manager integrates with VMware Infrastructure and VMware vCenter Server (formerly VMware VirtualCenter) to give you a seamless view of your environment that encompasses both virtual infrastructure and disaster recovery management.

Site Recovery Manager uses NetApp-supported disaster recovery scripts to discover arrays, discover replicated LUNs, fail over the LUNs, and test failover of LUNs:

- DiscoverArrays.pl—This script discovers the array name, array ID, storage-port information, and so on.
- DiscoverLuns.pl—This script discovers all LUNs that are replicated and belong to an igroup of ostype *vmware.*
- failover.pl—This script does test-failover-start, test-failover-stop, or the actual failover for input LUNs.

What Site Recovery Manager supports

Site Recovery Manager supports the following storage environments using NetApp disaster recovery scripts:

- VMFS (iSCSI and FC)
- RDM (iSCSI and FC)
- NetApp active/active configuration

For more information about Site Recovery Manager, see the documentation available at http://www.vmware.com/support/pubs/srm_pubs.html.

What NetApp Disaster Recovery Adapter supports

NetApp Disaster Recovery Adapter supports the following replication technologies:

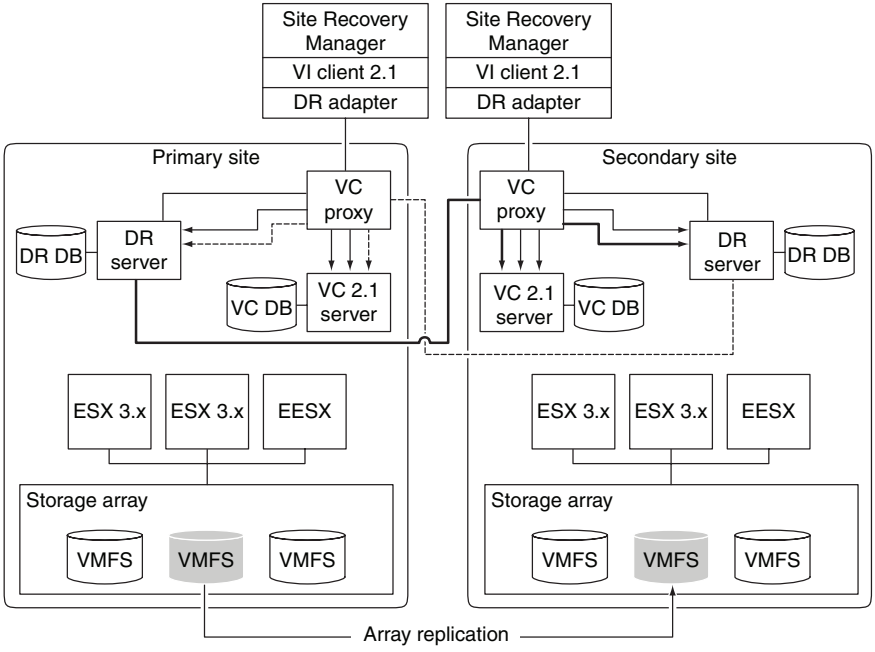
- Asynchronous qtree SnapMirror
- Asynchronous volume SnapMirror

- Synchronous SnapMirror

For more information about these technologies, see the *Data ONTAP Data Protection Online Backup and Recovery Guide*.

Components of the disaster recovery environment

The components of the disaster recovery environment are shown in the following illustration.



- NetApp disaster recovery adapter—provides array-specific support for Site Recovery Manager.
  - Array discovery (DiscoverArrays.pl)

    Array discovery returns storage-specific identification of the arrays managed by an entity at an IP address. Each address points directly to an individual storage system.

    For iSCSI storage systems, the returned information contains the iSCSI node name. This information is correlated with the value stored within ESX server to map a storage target (the *Y* value in vmhba*X*:*Y*:*Z*) to the storage system.
  - Replicated device discovery (DiscoverLuns.pl)

Replicated device discovery locates the list of replication source devices, and their LUN numbers, that map to the *Z* value of vmhba*X*:*Y*:*Z*. Site Recovery Manager uses this information to determine the data stores that can be replicated. The information also returns an identifier for the target device so that it can be replicated. For the NetApp storage system servicing the nodes in the primary ESX server, this script returns a list of all the LUNs that are members of SnapMirror® source volumes, and their LUN IDs.

- Test failover and actual failover (failover.pl)

  Test failover creates a FlexClone® volume from the replicated base Snapshot™ copy at the destination volume for testing.

  Actual failover promotes the replicated destination in case of failover.

- vCenter Server control interface—Site Recovery Manager communicates with vCenter Server to bring up the replicated virtual machine using the vCenter Server control interface.

System requirements and installation information

Prerequisites

Before running the NetApp disaster recovery scripts, ensure that your system meets the following requirements:

- Data ONTAP 7.2.2 or later.
- NetApp FAS200 series, FAS2000 series, FAS3000 series, FAS3100 series, FAS6000 series, V3000 series, or V6000 series.
  For more information about supported platforms, see http://www.vmware.com/pdf/srm_storage_partners.pdf.

  The NearStore® option is also supported.
- A FlexClone license is required for test failover.
- SnapMirror is enabled on Data ONTAP.
- iSCSI, FC, or both services are running.
- Site Recovery Manager is installed on Windows.

  Site Recovery Manager supports VMFS (iSCSI and FC) and RDM (iSCSI and FC) storage environments.
- Perl 5.8 is installed on the system on which Site Recovery Manager is installed.

  Note

  If the Site Recovery Manager CD-ROM does not include the Perl 5.8 script, you can install this script separately with the default configuration. For details, see http://www.perl.com/download.csp.

- By default, the script calls Data ONTAP APIs over simple HTTP. If you want to use secureHTTP, you must set up SecureAdmin® and ensure that ssl/ssh is running.

  Note

  SecureAdmin does not require a license.

- Because SOAP/HTTP/SSL is used, you must configure the firewall (if any) between Data ONTAP and Site Recovery Manager to keep the corresponding port open.

Installing NetApp disaster recovery scripts

To install the NetApp disaster recovery scripts, complete the following steps:

Step	Action
1	Double-click the installer. The installer finds the installed location of Site Recovery Manager from the registry and appropriately copies these scripts to that location.
2	Select the Complete install option.

Note

The version of the Disaster Recovery Adapter is available at the following registry location:
HKEY_LOCAL_MACHINE\SOFTWARE\NetApp Inc\NetApp Disaster Recovery Adapter\Version

Limitations

Limitations of using NetApp disaster recovery scripts

Review the following limitations before you begin using Site Recovery Manager with NetApp disaster recovery scripts to back up data:

- LUNs having multiple replication destinations cannot be failed over.
- The testFailover operation might fail if there is already an existing volume with the same name that it tries to create. This step could destroy the existing volume when testFailover cleans up. For details, see "Example" on page 11.
- The testFailover operation is not supported on traditional volumes because FlexClone technology is not available with traditional volumes.
- The following are not supported:
  - SyncMirror® replication between Site Recovery Manager sites (as in MetroCluster)
  - NFS environment

For specific information about recommended configurations and best practices for the replication product, see the appropriate disaster recovery product documentation.

Recommendations

Recommendations for using NetApp disaster recovery scripts

Following are some of the recommendations for using the NetApp disaster recovery scripts with Site Recovery Manager:

- Ensure that the primary and secondary ESX servers can discover LUNs on storage systems using iSCSI, FC, or both.
- On the secondary storage system, ensure that there are no volumes whose names match the name of the volume that testFailover creates. For details, see "**Testing failover**" on page 11.
- When removing SnapMirror relationships to avoid multiple replication destinations, if the SnapMirror relationship is deleted on the secondary storage system, delete the relationship on the primary storage system also.
- When adding NetApp active/active configuration systems to the Site Recovery Manager configuration, add each NetApp controller as an array in Array Managers.

Before running the NetApp disaster recovery scripts for Site Recovery Manager, complete the following steps:

Step	Action
1	Install Site Recovery Manager.
2	Install NetApp Disaster Recovery Adapter for Site Recovery Manager. For more information, see "Installing NetApp disaster recovery scripts" on page 8.
3	Configure the primary ESX server to access the LUNs in the primary storage system: a. Create an igroup, either iSCSI, FC, or both, of ostype *vmware* in the primary storage system. b. Add the primary ESX server initiator to the igroup.
4	Replicate the volume or qtree containing the LUNs in Step 3 to the secondary storage system.

Step	Action
5	On the primary storage system, enter the following command to confirm that the concerned LUN is involved in only one replication relationship and that the relationship status displays *Source*: **`snapmirror status`**
6	On the secondary storage system, enter the following command to confirm that the relationship state is *SnapMirrored*. **`snapmirror status`** For information about deleting a relationship, see the *Data ONTAP Data Protection Online Backup and Recovery Guide*.
7	Create igroups, either iSCSI, FC, or both, of ostype *vmware* in the secondary storage system.
8	Add the secondary ESX server initiators to this igroup.
9	Enter the following command to confirm the addition of the secondary ESX server initiators to the igroup: **`igroups show`** You can allow more than one initiator to see the LUNs that have failed over. Site Recovery Manager informs the disaster recovery script about all initiators that should see these LUNs.
10	Ensure that all those initiators are added to igroups of ostype *vmware* in the secondary storage system.

Testing failover

For testing failover, the scripts create a clone volume on the secondary storage system.

This test volume is created with a prefix *testfailoverClone_nss_v10745371_* followed by the parent volume name.

Example:

- The test Clone volume created for *secondary_volume* is named *testfailoverClone_nss_v10745371_secondary_volume*.
- After testing failover, the testFailover cleanup script tries to destroy the *testfailoverClone_nss_v10745371_secondary_volume* volume.

Ensure that you do not have user-created volumes with names prefixed by *testfailoverClone_nss_v10745371_*.

- To find the existing volumes in the secondary storage system, enter the `vol status` command.

Managing failback

Managing failback using Site Recovery Manager is a manual process because the protection site could have completely different hardware and network configurations after a disaster occurs.

Failback can be managed like any planned server migration.

Site Recovery Manager does not have an automated push-button failback mechanism. To achieve failback, you should perform a series of manual steps culminating in the failover workflow being run in the reverse direction.

Failback is run to restore the original primary protected site to its pre-failover state.

The following failback scenario uses Site Recovery Manager as a failback tool to the protected site after running the recovery plan at the recovery site in recovery mode for recovered virtual machines.

Name	Description
Site A	original protected site
Site B	original recovery site
filerA	original protected storage system
filerB	original recovery storage system

Note

Assume that there is an original protected site (Site A) and an original recovery site (Site B). After the failover occurs, the recovery site becomes the acting protected site (Site B). By using the failback procedure, the original protected site becomes the acting recovery or failback site (Site A).

Manually running a failback: To manually run a failback, complete the following steps. For details, see *VMware vCenter Site Recovery Manager in a NetApp Environment (TR-3671)* at http://media.netapp.com/documents/tr-3671.pdf.

Step	Action	
1	Ensure that the protected virtual machines at Site A are no longer accessed by any users or applications.	
2	Shut down all the protected virtual machines at Site B that were part of the recovery plan at Site B.	
3	Perform a cleanup of the failover LUN at Site B that contained virtual machine configuration files created during protection group creation at Site A.	
4	Delete protection groups from Site A.	
5	Perform a "Remove from Inventory" for all the protected virtual machines from Site A that were part of the recovery plan at Site B.	
6	If...	Then...
	You can recover filerA's volume	Enter the following command at filerA to resync the SnapMirror relationship: `snapmirror resync -S filerB:volB filerA:volA`
	FilerA's volume is not recoverable	Enter the following command at filerA to resync the SnapMirror relationship: `snapmirror initialize -S filerB:volB filerA:volA`
7	Ensure that there is an igroup of ostype *vmware* on the original protected storage system, If not, create an igroup of ostype *vmware*.	
8	Verify that the two Site Recovery Manager servers are paired with each other; if they are not, pair them with each other.	
9	At Site B, configure the array manager and inventory mapping.	

Step	Action
10	At Site B, create protection groups for virtual machines to be failed back. Select a spare LUN from Site A for the failback inventory mapping.
11	At Site A, create a recovery plan for the protection groups that are created on Site B.
12	From Site A, test the recovery plan.
13	If the test is successful, then run the recovery plan.
14	Shut down all the protected virtual machines at Site A that were failed back during the failback recovery plan.
15	Perform a cleanup of the failback LUN at Site A that contained the virtual machine configuration files during protection group creation at Site B.

Using SecureHTTP with the Data ONTAP API

Guidelines for using the Data ONTAP API over SecureHTTP

The Data ONTAP API can use normal HTTP or SecureHTTP.

By default, the disaster recovery scripts use the Data ONTAP API over HTTP. However, the editable configuration SSL parameter enables you to use the Data ONTAP API over SecureHTTP.

Setting up scripts to use the Data ONTAP API over SecureHTTP

To set up SecureHTTP, complete the following steps:

Step	Action
1	In the primary and secondary storage systems, set up SecureAdmin and enable SSL and SSH services.
2	Enter the following command to confirm that the SSL and SSH services are running: **`secureadmin status`**
3	In the location where the disaster recovery scripts are kept, edit the *ontap_config.txt* file to add the following line: ssl=on
4	In the Perl environment, install the Net::SSLeay module. HTTPS support uses Net::SSLeay.pm. Net::SSLeay is not part of Perl 5.8 shipped with Site Recovery Manager. You need to compile Net::SSLeay.pm from the source Net_SSLeay.pm-1.xx.tar.gz available at http://www.cpan.org. For instructions about how to compile and install Net::SSLeay.pm from the source, see the Readme file available in Net_SSLeay.pm-1.xx.tar.gz.

Troubleshooting

The log files are available in C:\Documents and Setting\All Users\Application Data\VMware\VMware Site Recovery Manager\Logs\. There might be multiple log files with names such as vmware-dr-*log number*.log. The error log messages are not displayed in the Site Recovery Manager user interface.

In case of any failure or unexpected behavior, it is advised that you set the log level to *trivia* in Site Recovery Manager and run the failover operation again. For details about running the failover operation, see the Site Recovery Manager documentation. Then, you should examine the log messages kept at this location.

List of error messages in the log files

The following table lists the log file error messages, including cause and solutions.

Note

The solutions provided in the following table assume that you are running the disaster recovery scripts in a failover environment.

Log level	Error message	Cause and solution
Command.pl—This script invokes discoverArrays.pl, discoverLuns.pl, or failover.pl based on the input.		
Quiet	Missing the OutputFile parameter in XML input.	The LogLevel parameter is missing in the input XML file from Site Recovery Manager. **Solution:** Check the configuration in Site Recovery Manager.
Quiet	Missing the LogLevel parameter in XML input.	The output file parameter is missing in the input XML file from Site Recovery Manager. **Solution:** Check the configuration in Site Recovery Manager.

Log level	Error message	Cause and solution
Quiet	Command is not specified in XML input.	The input command from Site Recovery Manager is none of discoverArrays, discoverLuns, failover, or testFailover operations. **Solution:** Check the configuration in Site Recovery Manager.
Quiet	Error while executing script.	There was an error while running the script in the Perl environment. **Solution:** Check whether the path to *perl.exe* is added to the system path and the scripts are installed in the correct directory. For more information, see the "Installing NetApp disaster recovery scripts" on page 8.
Common.pm—This script contains common routines used by other scripts.		
Quiet	Could not get the host name.	The storage system does not have a valid host name. **Solution:** Configure a valid host name for the storage system.
Quiet	Unable to set HTTPS transport.	The *ssl and ssh* services might not be running in the storage system. **Solution:** Run the `secureadmin status` command. If the services are not running, configure the secureadmin service and start the *ssh and ssl* services.
DiscoverArrays.pl—This script discovers the array name, array ID, storage-port information, and so on.		
Quiet	Creating server element failed.	This might occur because of low memory in the vCenter Server host. The script fails because it cannot connect to the NetApp storage system.

Log level	Error message	Cause and solution
Verbose	No FCP WWNN (world wide node name) found.	Either an FC license is not installed in the NetApp storage system or there are no FC ports. **Solution:** Install the FC license and start the FC service.
Verbose	No iSCSI port found.	The iSCSI license might be missing or the iSCSI service might not be running. **Solution:** Check the iSCSI license and verify that the iSCSI service is running.
Verbose	No FCP adapter found.	The FC license might be missing or the FC service might not be running. **Solution:** Check the FC license and verify that the FC service is running.
DiscoverLuns.pl—This script discovers the LUNs that are replicated and belong to an igroup of ostype *vmware*.		
Quiet	Could not find an igroup of ostype *vmware*.	There might not be an igroup of ostype *vmware*. **Solution:** Create an igroup with ostype *vmware* and map the LUN to be failed over to this igroup.
Quiet	Error while discovering igroups of ostype *vmware*.	There might not be an igroup of ostype *vmware*. **Solution:** Map the LUNs to be failed over to an igroup of ostype *vmware*.
Quiet	Could not discover any LUNs mapped to an igroup of ostype *vmware* and replicated.	The LUNs might not be replicated. **Solution:** Replicate the LUNs to be failed over and map these LUNs to an igroup of ostype *vmware*.

Log level	Error message	Cause and solution
Quiet	Error while discovering LUNs mapped to an igroup of ostype *vmware* and replicated.	The LUNs might not be replicated or there might not be an igroup of ostype *vmware*. **Solution:** Replicate the LUNs to be failed over and map these LUNs to an igroup of ostype *vmware*. This igroup should contain ESX server initiators.
Quiet	Skipping *lun_path* as it has multiple peers.	LUNs that have been replicated multiple times are not currently supported. **Solution:** Run the `snapmirror status` command on the storage system. Ensure that the replication relationship for the concerned LUN has only one peer.
Verbose	*igroup_name* does not have any initiators.	The initiator might not be added in the igroup. **Solution:** Configure this igroup for correct initiators.
failover.pl—This script does test-failover-start, test-failover-stop, or the actual failover for the input LUNs.		
Quiet	Could not find an igroup of ostype *vmware.*	There might not be an igroup of ostype *vmware.* **Solution:** Create an igroup with ostype *vmware* and map LUNs to be failed over to this igroup.
Quiet	Error while discovering igroups of ostype *vmware.*	There might not be an igroup of ostype *vmware.* **Solution:** Map LUNs to be failed over to an igroup of ostype *vmware*.

Log level	Error message	Cause and solution
Quiet	Skipping *lun_path* as input does not specify any valid VMware initiator to be mapped to.	Input for NetApp scripts does not mention the igroup that the LUN should be mapped to during failover. Therefore, the scripts do not attempt to fail over this LUN. **Solution:** Check the configuration.
Quiet	initiator *ID* does not belong to any igroup of ostype *vmware.*	One of the initiators in the Site Recovery Manager XML file should see the failed over LUNs but cannot because it does not belong to an igroup of ostype *vmware*. **Solution:** Add this initiator to an igroup of ostype *vmware* in the storage system.
Quiet	Skipping *lun_path* as input initiators to be mapped to do not belong to any VMware igroup in the storage system.	This occurs because either the input XML file from Site Recovery Manager does not mention any initiator that should see this LUN, or none of the initiators specified by the input XML file belong to an igroup of ostype *vmware*. **Solution:** Add the initiators to the igroup of ostype *vmware.*
Quiet	Skipping *lun_path* as this is not a valid SnapMirror relation.	*lun_path* is not replicated. **Solution:** Check the `snapmirror status` command to confirm whether the LUN is from a replicated relation. Replicate the LUN.
Quiet	*lun_path* does not exist.	The concerned LUN does not exist. **Solution:** Check the output of the `lun show` command.

Log level	Error message	Cause and solution
Quiet	Could not find base Snapshot for *relation_path*; skipping *lun_path.*	The concerned LUN is skipped from being moved to the test failover state. **Solution:** Check the `snapmirror status` command output for this relationship and check whether it is replicated.
Quiet	Test volume clone creation for *testClonevolume* failed.	This might occur because a volume with the name testfailoverClone_nss_v10745371_Volumename already exists. The scripts try to create the clone volume and prefix the original volume name with "testfailoverClone_nss_v10745371_*Volumename*". **Workaround:** Rename the existing volume.
Quiet	Mapping *lun_name* to *igroup_name* failed.	Mapping the failed over LUN to *igroup_name* failed due to some reason. **Solution:** Check whether *igroup_name* exists in the storage system. If this is a test-failover-start and the volume creation failed with the message “volume already exists”, then check whether a volume with the name testfailoverClone_nss_v10745371_*VolumeName* already exists.

Log level	Error message	Cause and solution
Quiet	Onlining *lun_path* failed.	If the LUN is mapped to more than one igroup, for example, A and B, and there are some initiators that belong to both A and B, then the LUN cannot be brought online. **Solution:** Remove such common initiators from these igroups. This is because the same initiator now has two different LUN IDs for the same LUN.
Quiet	Skipping *lun_name* as it is not failed over.	For a LUN to be considered successfully failed over, it should be online, writable, and mapped. **Solution:** Run the script with loglevel=*trivia* and identify the problem from the log. Then, rerun the script.
Quiet	Destroying test volume *clone_volume_name* failed.	Taking offline and destroying *clone_volume_name* failed. This is because the volume is busy or is used by some other subsystem. **Solution:** Retry destroying *clone_volume_name* later.
Quiet	No LUN with mapping information provided for failover.	There is no input initiator for this LUN to be mapped to after failing over. Therefore, the script does not do a failover operation for this LUN. **Solution:** Check the configuration. Correctly map the initiators to igroups of ostype *vmware* in the secondary storage system.

Log level	Error message	Cause and solution
Quiet	No mapping information provided for the LUNs.	There is no input initiator for this LUN to be mapped to after failing over. Therefore, the script cannot do a failover operation for this LUN. **Solution:** Check the configuration. Correctly map the initiators to igroups of ostype *vmware* in the secondary storage system.
Verbose	igroup *name* does not have any initiators.	Initiators might not be added to the igroup. **Solution:** Configure this igroup for the correct initiators.