



NEC Storage Software

NEC Storage Replication Adapter User's Guide

© NEC Corporation 2020

No part of the contents of this book may be reproduced or
transmitted in any form without permission of NEC Corporation.

The contents of this book may be modified without notice in the future.

Preface

This guide is intended for readers who already possess the basic knowledge about data replication.

This guide describes only minimum requirements when the disaster recovery system is configured under the virtualized environment using VMware Site Recovery Manager.

Remarks


- 1. This guide is applicable to VMware Site Recovery Manager.
- 2. This guide is applicable to NEC Storage Replication Adapter.
- 3. This guide is applicable to the NEC Storage M series products.
- 4. The following terms in this guide refer to the corresponding products unless otherwise specified.

Term	Corresponding Products
iSM	NEC Storage Manager
ControlCommand	Storage ControlCommand
VMware SRM	VMware Site Recovery Manager
SRA	NEC Storage Replication Adapter
RDR/DR	NEC Storage RemoteDataReplication/DisasterRecovery
RDR	NEC Storage RemoteDataReplication
DDR	NEC Storage DynamicDataReplication

- 5. Documents related to this guide

Document	Stored in
Site Recovery Manager Administration	https://www.vmware.com/support/pubs/srm_pubs.html
Site Recovery Manager Installation and Configuration	https://www.vmware.com/support/pubs/srm_pubs.html
Compatibility Matrixes for VMware Site Recovery Manager	https://www.vmware.com/support/pubs/srm_pubs.html
IS007 NEC Storage Software Configuration Setting Tool User's Manual (GUI)	NEC Storage Manager installation media
IS051 NEC Storage Software Configuration Setting Tool User's Manual (GUI) for M series	NEC Storage Manager installation media
IS015 NEC Storage Software Data Replication User's Manual (Function Guide)	NEC Storage Manager installation media
IS027 NEC Storage Software Data Replication User's Manual (Disaster Recovery System Installation and Operation Guide)	NEC Storage Manager installation media
IS010 NEC Storage Software Messages Handbook	NEC Storage Manager installation media

6. The screen pictures shown in this guide may differ depending on the version of VMware Site Recovery Manager.
7. Trademarks and registered trademarks
 - VMware products are covered by one or more patents displayed in the list at <http://www.vmware.com/go/patents>.
 - VMware is a trademark or a registered trademark of VMware, Inc. in the United States and other countries.
 - Microsoft®, Windows® is a trademark or a registered trademark of Microsoft Corporation in the United States and other countries.
 - Other product names and company names are trademarks or registered trademarks of the associated companies.
8. No part of the contents of this document may be copied, reproduced, transmitted in any form, or disclosed to any third parties without permission of NEC.
9. In this document, matters to which careful attention needs to be paid will be described as follows:
Be sure to observe the contents. If the indications are ignored and the system is improperly operated, the system operation might be affected.

Type of Indication	
Type	Description
	Describes contents which require users to pay special attention for operation.

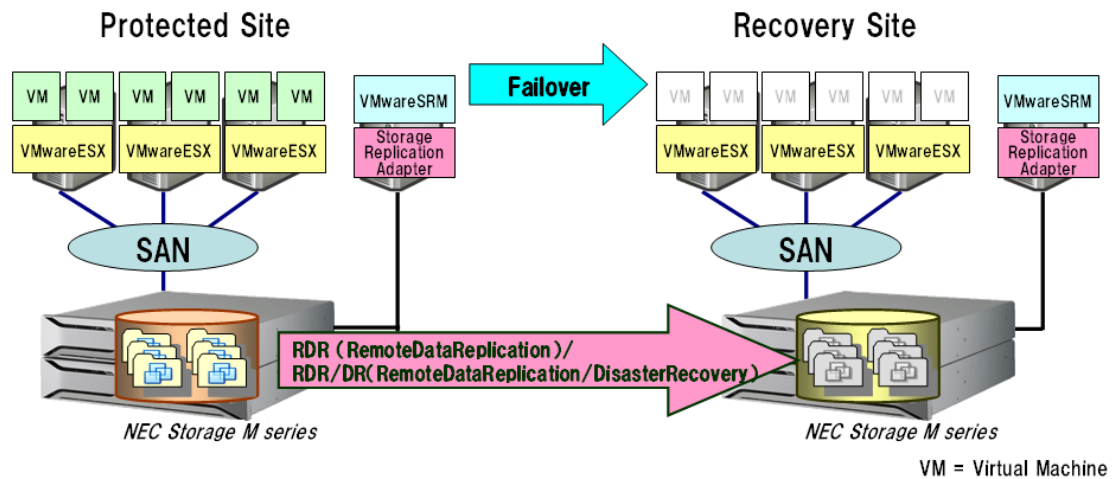
Contents

Chapter 1	Overview of VMware SRM.....	1
Chapter 2	Installation of VMware SRM.....	2
2.1	Flow of System Configuration Step.....	2
2.2	Environment.....	3
2.2.1	Hardware Configuration.....	3
2.2.2	Software Configuration.....	5
2.2.3	Storage Replication Configuration.....	7
2.2.4	Storage Logical Disk Configuration.....	13
2.3	Software Installation.....	15
2.3.1	VMware ESXi.....	15
2.3.2	VMware vCenter Server.....	16
2.3.3	VMware vSphere Web Client.....	16
2.3.4	Storage Manager Server and Client.....	16
2.3.5	ControlCommand.....	16
2.3.6	VMware Site Recovery Manager.....	16
2.3.7	NEC Storage Replication Adapter.....	17
2.4	Storage Configuration Settings.....	19
2.4.1	Unlock License.....	19
2.4.2	Bind a Pool.....	19
2.4.3	Bind Logical Disks.....	20
2.4.4	Configure Access Control Settings.....	22
2.4.5	Synchronize Volumes.....	23
2.5	Virtual Machines Configuration.....	29
2.6	VMware Site Recovery Manager Setting.....	30
2.6.1	Connect Sites (Protected site process).....	30
2.6.2	Configure Inventory Mappings (Protected site and recovery site process).....	30
2.6.3	Assign Placeholder Datastores (Protected site and recovery site process).....	30
2.6.4	Configure Array-Based Replication (Protected site process).....	31
2.6.5	Create a Protection Group (Protected site process).....	36
2.6.6	Create a Recovery Plan (Recovery site process).....	36
Chapter 3	Operations.....	37
3.1	Backup Creation by User.....	37
3.1.1	Pattern 1-1 RDR (synchronous) operation.....	37
3.1.2	Pattern 1-2 RDR (synchronous) operation.....	37
3.1.3	Pattern 2 RDR (asynchronous) operation.....	38

3.1.4	Pattern 3-1 RDR/DR (synchronous or semi-synchronous) operation.....	41
3.1.5	Pattern 3-2 RDR/DR (background copy mode of order guarantee) operation	41
3.2	Test a Recovery Plan (Operation at Recovery Site).....	42
3.3	Run a Recovery Plan (Operation at Recovery Site)	43
3.4	Reprotection.....	45
Appendix A	Change LUN	51
Appendix B	Troubleshooting	52
Appendix C	How to Collect Information at Failure	56
Appendix D	Notes.....	59

Chapter 1 Overview of VMware SRM

VMware Site Recovery Manager (VMware SRM) is a disaster recovery product for the virtualized environment. VMware SRM allows for disaster recovery planning, testing and performing failover, re protection after failover, and automated (or quick) failback using storage replication.



For disaster recovery, there are several benefits of using virtualized environment. With minimal hardware dependencies under virtualized environments, recovery is easy with small risk of recovery failures.

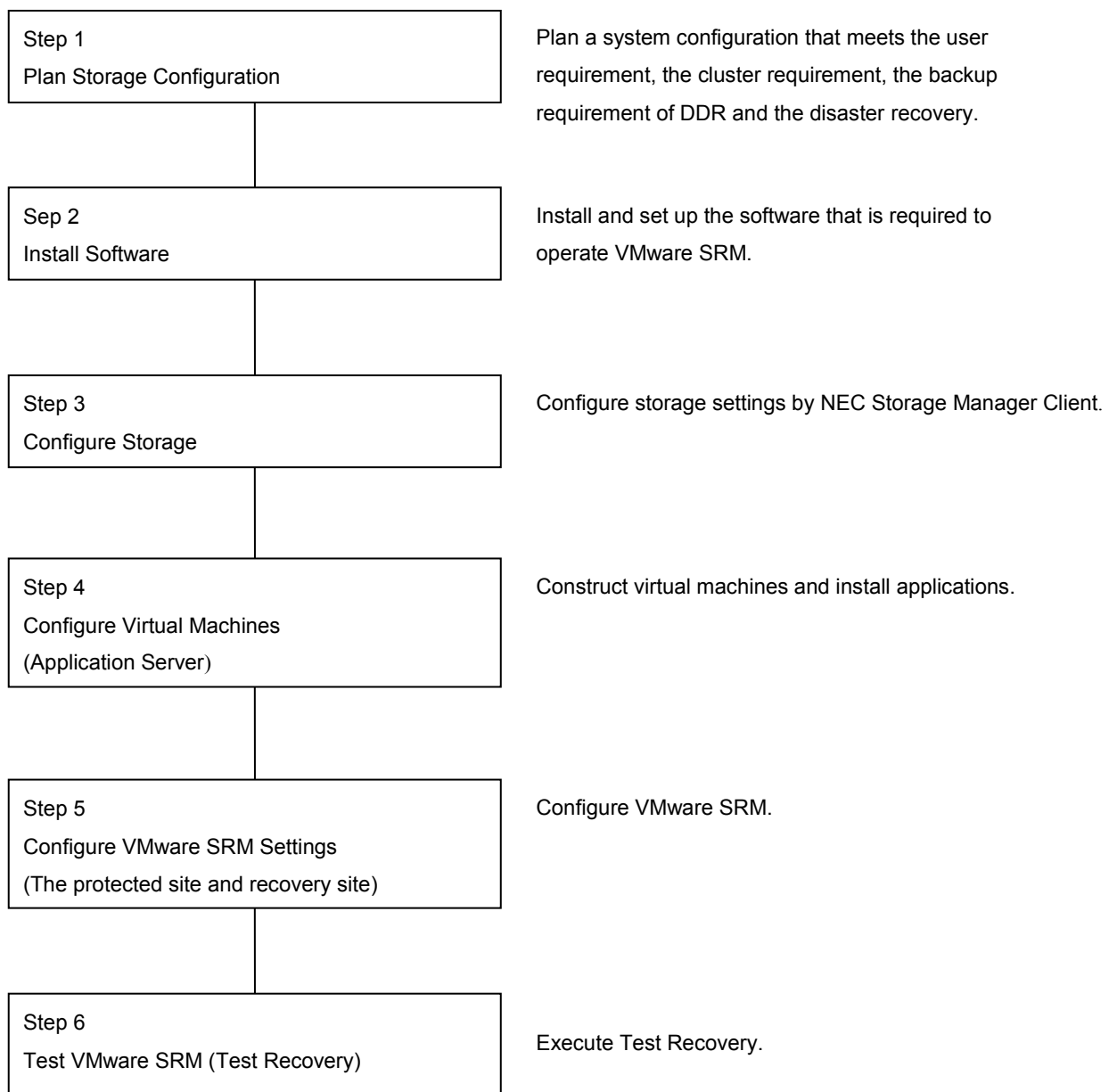
In addition, VMware SRM:

- Reduces the risk of manual or operational mistakes.
- Allows for one to automate operations: switching over disks, changing IP addresses, switching virtual switches, relocating resource pools

Chapter 2 Installation of VMware SRM

2.1 Flow of System Configuration Step

The following flow chart describes the steps which configure the disaster recovery system under VMware ESXi environment using VMware SRM.



2.2 Environment

2.2.1 Hardware Configuration

Each protected and recovery sites must meet the following requirements.

- 1) Each site must have at least one ESXi server.
- 2) The ESXi server must meet the specification that VMware, Inc. requires.
- 3) Each site must have a management server. (Windows Server OS is required)
- 4) Each site must have at least one storage (NEC Storage) that supports RDR or RDR/DR.
- 5) Each site must have either FC-SAN with storage that supports FC-SAN, or iSCSI-SAN configuration with storage that supports iSCSI-SAN.
- 6) The storage at each site must be linked by RDR or RDR/DR.
- 7) Each site must be connected by a reliable IP network.

The protected site should meet the following requirements.

- 1) It is necessary for the protected site to have access to the same networks (public and private) as the recovery site. (It is not necessary to have the same range of network addresses).

* Backup server can be placed.

The recovery site should meet the following requirements.

- 1) It is necessary for the recovery site to have hardware, network and storage resources that can support the same virtual machines and workloads as protected site.
- 2) It is necessary for the recovery site to have access to the same networks (public and private) as the protected site. (It is not necessary to have the same range of network addresses.)

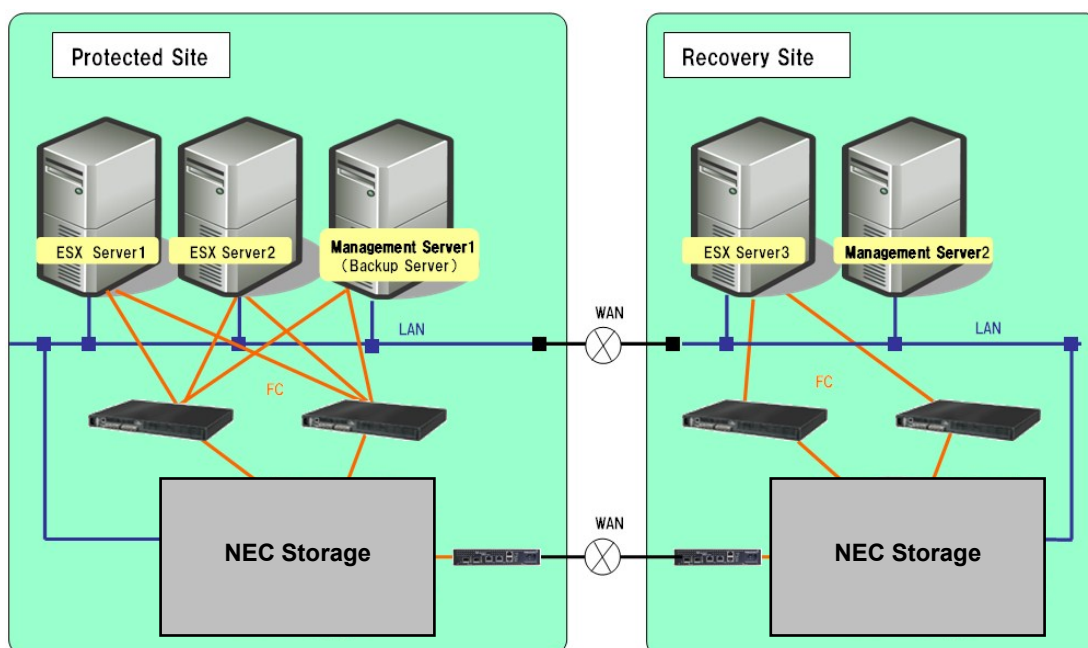


Figure 2-1: Hardware Configuration

Table 2-1 Hardware Configuration Example

Application Server	Express5800/100 Series
Backup server	Express5800/100 Series
Management Server (The backup server can be used as a management server)	Express5800/100 Series
Disk Arrays	NEC M Series Storage
Fibre Channel	Dual paths between application servers and FC switches as well as between FC switches and NEC Storage

Storage should be one of the following.

Table 2-2 Supported Storage

Storage
M100 (FC/iSCSI)
M110 (FC/iSCSI)
M120 (FC/iSCSI)
M300 (FC/iSCSI)
M310 (FC/iSCSI)
M310F (FC/iSCSI)
M320 (FC/iSCSI)
M320F (FC/iSCSI)
M500 (FC/iSCSI)
M510 (FC/iSCSI)
M520 (FC/iSCSI)
M700 (FC/iSCSI)
M710 (FC/iSCSI)
M710F (FC/iSCSI)

M720 (FC/iSCSI)
M720F (FC/iSCSI)
M5000 (FC)

2.2.2 Software Configuration

The protected and recovery sites must meet the following requirements.

- 1) VMware ESXi must be installed on both sites.
- 2) The following table lists some of OSes and their versions supported for management servers.

Table 2-3 Supported OS

OS
Windows Server 2008 (x64)
Windows Server 2008 SP2 (x64)
Windows Server 2008 R2 SP1 (x64)
Windows Server 2012 (x64)
Windows Server 2012 R2 (x64)
Windows Server 2016 (x64)

* These are some of OSes that support SRM server.

- 3) The following software must be installed at each site. For details of installation, see “2.3 Software Installation.”
 - NEC Storage Manager Ver9.3 or later
 - ControlCommand Ver9.3 or later
 - VMware vCenter Server
 - VMware Site Recovery Manager
 - NEC Storage Replication Adapter
- 4) Each site must have a machine that runs VMware vSphere Web Client.
 It is possible to run VMware vSphere Web Client on a management server, however there are differences in the supported OS between VMware Site Recovery Manager and VMware vSphere Web Client.
 (Refer to <https://www.vmware.com/support/pubs.>)
 VMware vSphere Web Client must have access to VMware vCenter at each site.
- 5) NEC Storage Manager in the protected site management server needs to monitor the storage in the protected site. (Monitoring via LAN is recommended).
- 6) NEC Storage Manager in the recovery site management server needs to monitor the storage in the recovery site. (Monitoring via LAN is recommended).
- 7) It is necessary to have unlocked the license of RDR (RemoteDataReplication) or RDR/DR (RemoteDataReplication/DisasterRecovery) of Storage at each site.

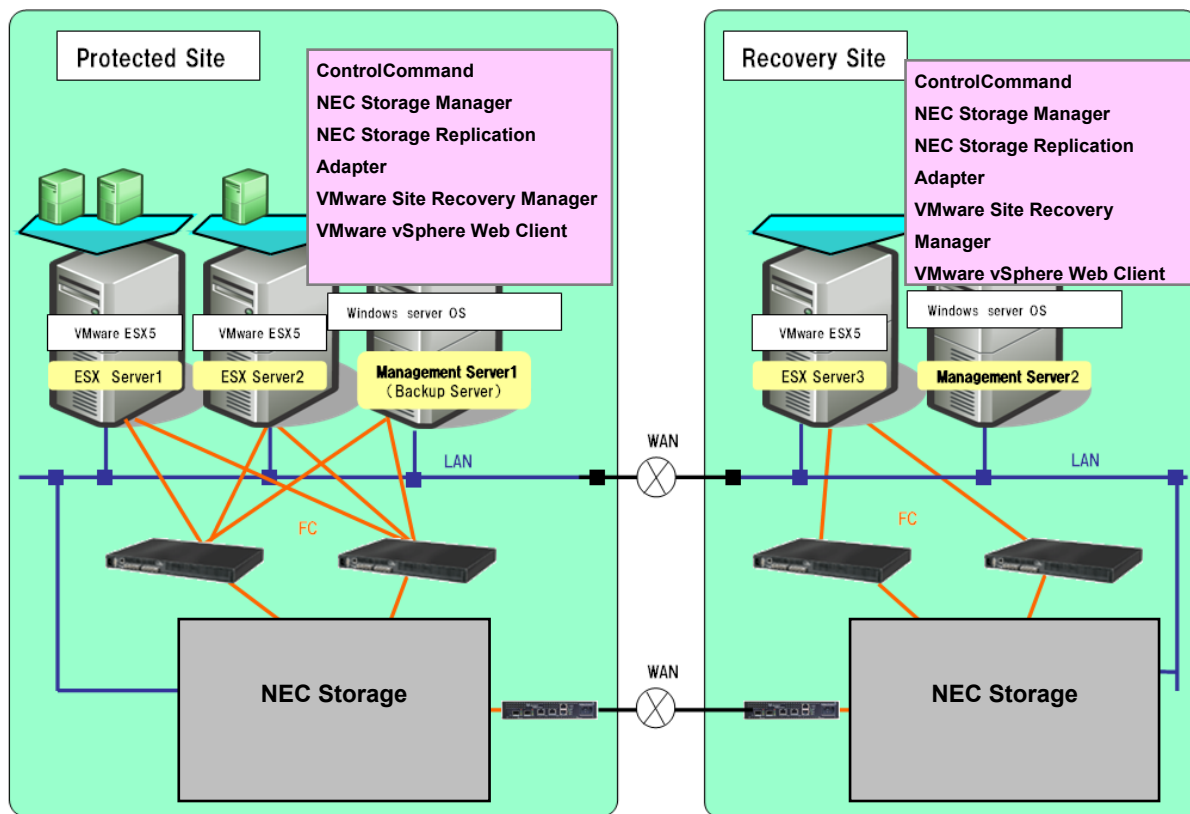


Figure 2-2: Software Configuration

2.2.3 Storage Replication Configuration

Storage in each site must have one of the following replication configurations.

Table 2-4 Supported OSES for Virtual Machines

Solution	Copy mode	Line speed	Support	Number of volumes	Config pattern	Description
RDR	Synchronous	Normal	Supported (no need of user backup creation needed)	Single	1-1	Uses RDR (synchronous mode) of the storage Configuration where one or more virtual machine and one or more user area (virtual machine) are allocated to datastore (PV) that consists of a single LD, or configuration where one or more virtual machine is allocated to one or more datastore (PV) consisting of a single LD, and each virtual machine uses up to one RDM
			Supported (user backup creation needed)	Multiple	1-2	Uses RDR (synchronous mode) of the storage Configuration where one or more virtual machine that uses two or more RDMs is allocated to one or more datastore (PV) that consists of a single LD, or configuration where the system area and the user area of virtual machine are allocated to two or more datastores (PVs), each consisting of a single LD.
	Background	Normal	Supported (user backup creation)	Single, Multiple	2	Uses RDR (background copy mode) of the storage. Configuration where one or more virtual machine that uses one or more RDM is allocated to one or more datastore (PV) that consists of a single LD
		Slow	Supported (user backup creation)			
RDR/DR	Synchronous, asynchronous	Normal	Supported (no need of user backup creation)	Single, Multiple	3-1	Uses RDR/DR (synchronous mode or semi synchronous copy mode of order guarantee) of the storage Configuration where one or more virtual machine is allocated to one or more datastore (PV) that consists of a single LD and each virtual machine uses one or more RDM.
	Background copy mode of order guarantee	Slow	Supported (no need of user backup creation)	Single, Multiple	3-2	Uses RDR/DR (background copy mode of order guarantee) of the storage Configuration where one or more virtual machine is allocated to one or more datastore (PV) that consists of a single LD and each virtual machine uses one or more RDM.

The following describes features of patterns.

(1) Pattern 1-1 RDR (synchronous) operation

- i) One or more virtual machine can be allocated to the datastore (PV1-1) that consists of a single LD. A datastore of multiple LDs cannot be used.
- ii) Each virtual machine can have one or more virtual disk on the datastore as a user area.
- iii) Each virtual machine can use up to one RDM as a user area if assuring integrity of the system area and the user area is not necessary.
- iv) Users do not need to create a backup periodically because data consistency of RV/MV2-1, which is used for disaster recovery, is assured.
- v) A backup having a complete quiescent point (RV4-1) can be created in the recovery site after stopping all virtual machines according to the schedule in the protected site while this is not mandatory.
- vi) A backup (RV3-1) can be created in the recovery site by periodically separating RDR pair (PV1-1 and RV/MV2-1) while this is not mandatory.
- vii) Unless a backup (RV3-1) is created by using DDR in the recovery site, RDR pair (PV1-1 and RV/MV2-1) is always replicated.

The following figure illustrates an example of system configuring PV1-1 as datastore.

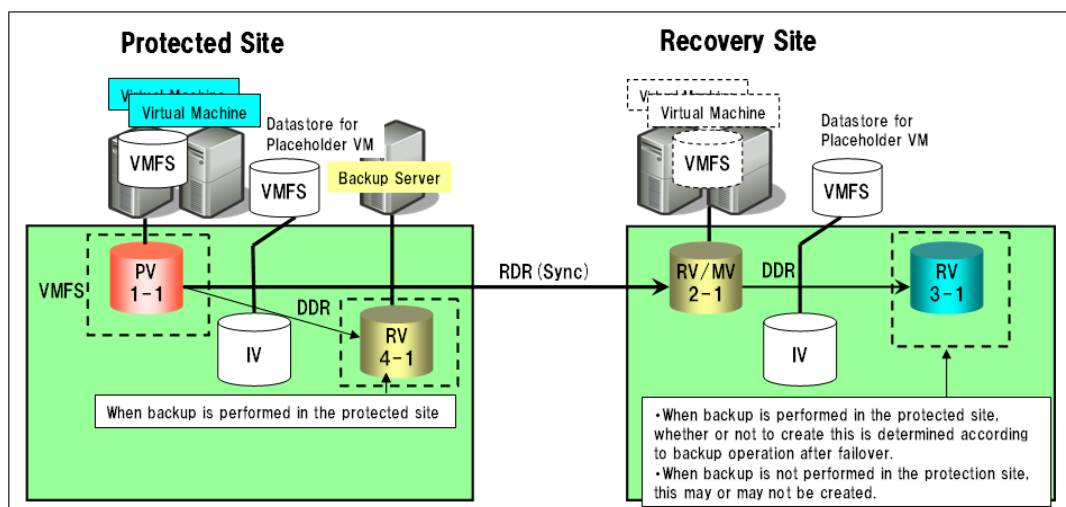


Figure 2-3: Pattern 1-1 RDR (Synchronous) Operation

(2) Pattern 1-2 RDR (synchronous) operation

- i) One or more virtual machine can be allocated to the datastore that consists of a single LD. A datastore of multiple LDs cannot be used.
 - ii) Each virtual machine uses two or more RDMs as the user area. Or, two or more user areas (virtual disks) are allocated to a datastore other than the datastore where the system area is allocated.
 - iii) Backups having a complete quiescent point (RV3-n) must be created in the recovery site after stopping all virtual machines on the datastore according to the schedule in the protected site.
 - iv) Unless backups (RV3-n) are created by using DDR in the recovery site, RDR pairs (PV1-n and RV/MV2-n) are always replicated.
 - v) Backups having a complete quiescent point (RV4-n) can be created in the recovery site after stopping all virtual machines according to the schedule in the protected site while this is not mandatory.
 - vi) Backups (RV4-n, RV/MV2-n) of user areas (RDMs) can be created by using ControlCommand on a virtual machine.
- * If an OS not supported by ControlCommand is used for a virtual machine, the quiescent point must be assured by stopping the virtual machine and a backup instruction must be given by the management server.
 - * If a virtual disk or RDM (Virtual Compatibility Mode) is used, backup by using ControlCommand on a virtual machine is not available.

The following figure illustrates an example of system configuring PV1-1 as datastore, and PV1-2 and PV1-3 as RDMs used by virtual machines

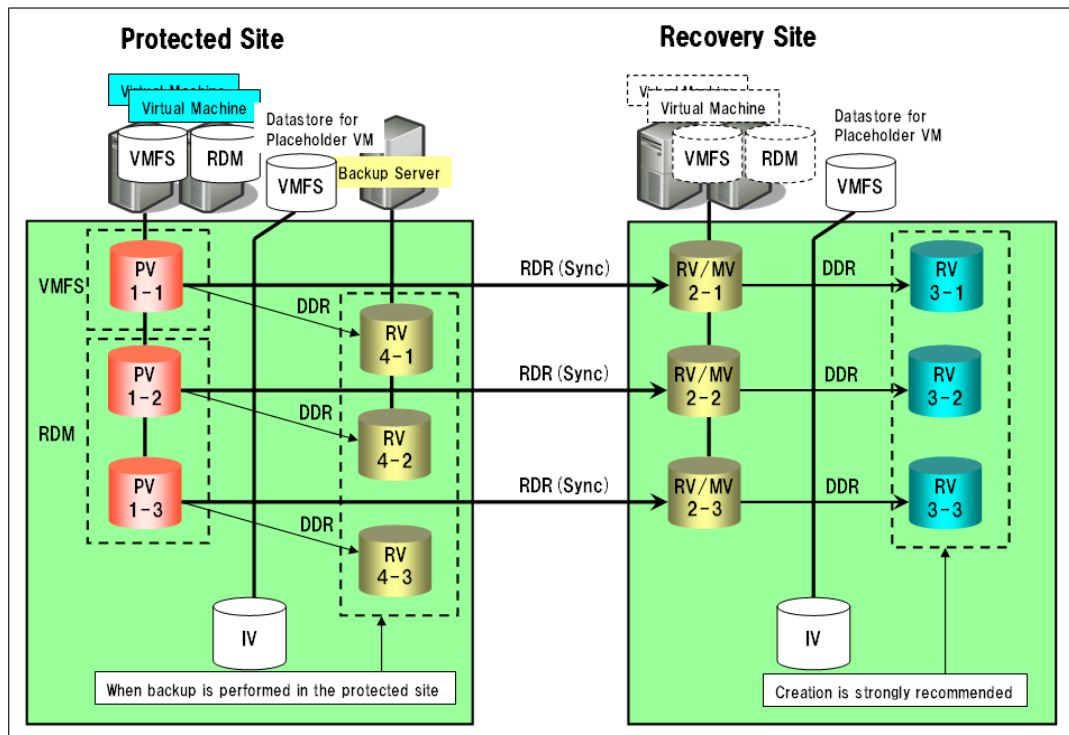


Figure 2-4: Pattern 1-2 RDR (Synchronous) Operation

(3) Pattern 2 RDR (asynchronous) operation

- i) One or more virtual machine can be allocated to one or more datastore that consists of a single LD. A datastore of multiple LDs cannot be used.
- ii) Each virtual machine can use multiple RDMs as the user area.
- iii) In a typical operation, DDR pairs (PV1-n and RV/MV2-n) are separated while RDR pairs (RV/MV2-n and RV/MV3-n) are replicated (background copy mode)
- iv) Backups having a complete quiescent point must be created in the recovery site after stopping all virtual machines on the datastores according to the schedule. Unless a system is updated, such as update of virtual machine OS or application, the system area does not need to be backed up frequently.
- v) If virtual machines use multiple RDMs as the user area, backup with secured integrity across LDs must be created by a user.
- vi) Backups (RV/MV2-n and RV4-n ($n \geq 3$)) of user areas (RDM) can be created by using ControlCommand on a virtual machine.
 - * If an OS not supported by ControlCommand is used for a virtual machine, the quiescent point must be assured by stopping the virtual machine.

The following figure illustrates an example of a system configuring PV1-1 and 1-2 as datastores and PV1-3 and PV1-4 as RDMs used by virtual machines.

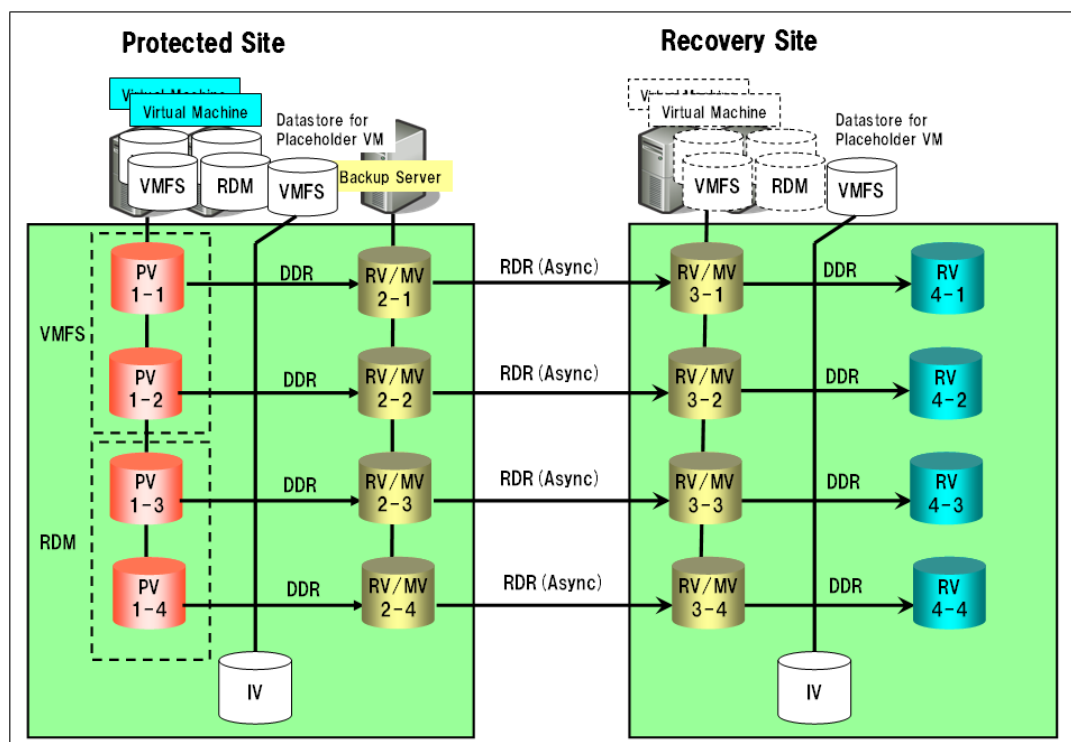


Figure 2-5: Pattern 2 RDR (Asynchronous) Operation

(4) Pattern 3-1 RDR/DR (synchronous or semi-synchronous) operation

- i) One or more virtual machine can be allocated to datastore that consists of a single LD. A datastore of multiple LDs cannot be used.
 - ii) Each virtual machine can use multiple RDMs as the user area.
 - iii) Users do not need to create backup data in the recovery site because the writing order is assured by registering the system area and user area of the virtual machine as a single AT group.
 - iv) If a datastore is backed up in the protected site by using DDR, all the virtual machines on the datastore must be stopped before the backup. Unless a system update, such as update of virtual machine OS or application, is performed, you do not need to back up the system area frequently.
 - v) Backups (RV4-n) of user areas (RDMs) can be created by using ControlCommand on a virtual machine.
- * If an OS not supported by ControlCommand is used for a virtual machine, the quiescent point must be assured by stopping the virtual machine.

The following figure illustrates an example of a system configuring PV1-1 and 1-2 as datastores and PV1-3 and PV1-4 as RDMs used by virtual machines.

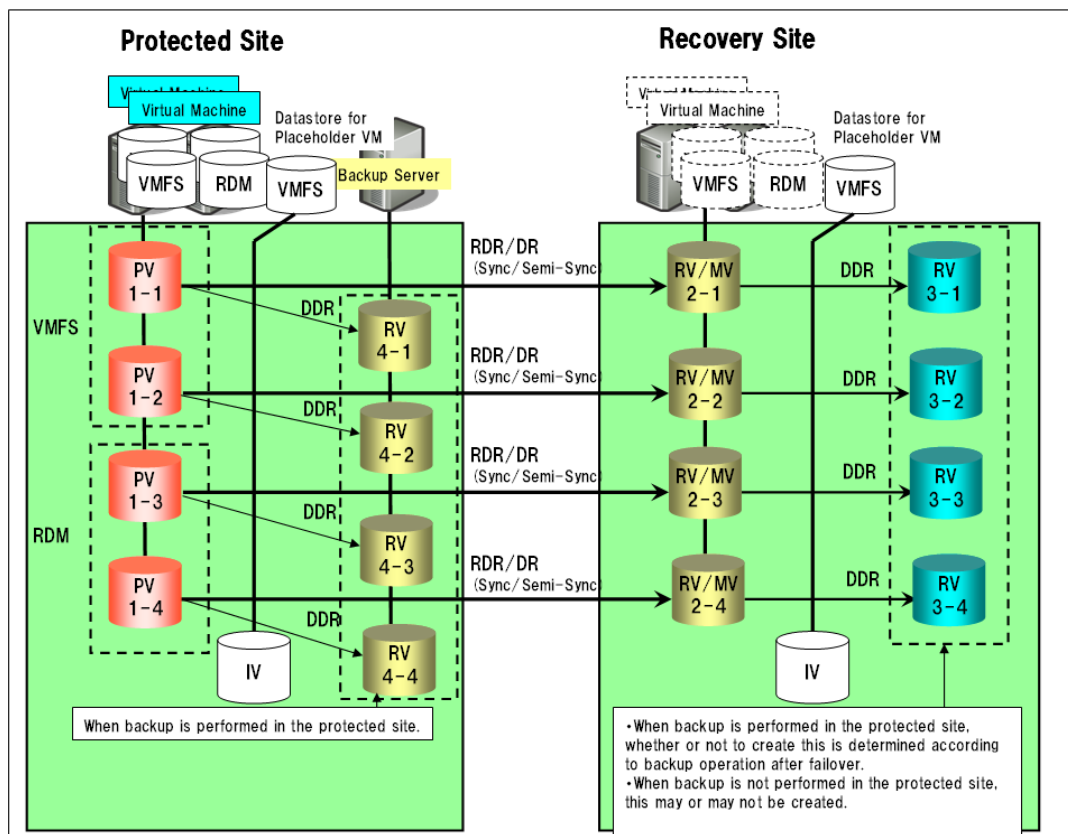


Figure 2-6: Pattern 3-1 RDR/DR (Synchronous or Semi-synchronous) Operation

(5) Pattern 3-2 RDR/DR (background copy mode of order guarantee) operation

- i) One or more virtual machine can be allocated to datastore that consists of a single LD. A datastore of multiple LDs cannot be used.
 - ii) Each virtual machine can use multiple RDMs as the user area.
 - iii) Users do not need to create backup data in the recovery site because the writing order is assured by registering the system area and user area of the virtual machine as a single AT group.
 - iv) If a datastore is backed up in the protected site by using DDR, all the virtual machines on the datastore must be stopped before the backup. Unless a system update, such as update of virtual machine OS or application, is performed, you do not need to back up the system area frequently.
 - v) Backups (RV4-n) of user areas (RDMs) can be created by using ControlCommand on a virtual machine.
- * If an OS not supported by ControlCommand is used for a virtual machine, the quiescent point must be assured by stopping the virtual machine.

The following figure illustrates an example of a system configuring PV1-1 and 1-2 as datastores and PV1-3 and PV1-4 as RDMs used by virtual machines.

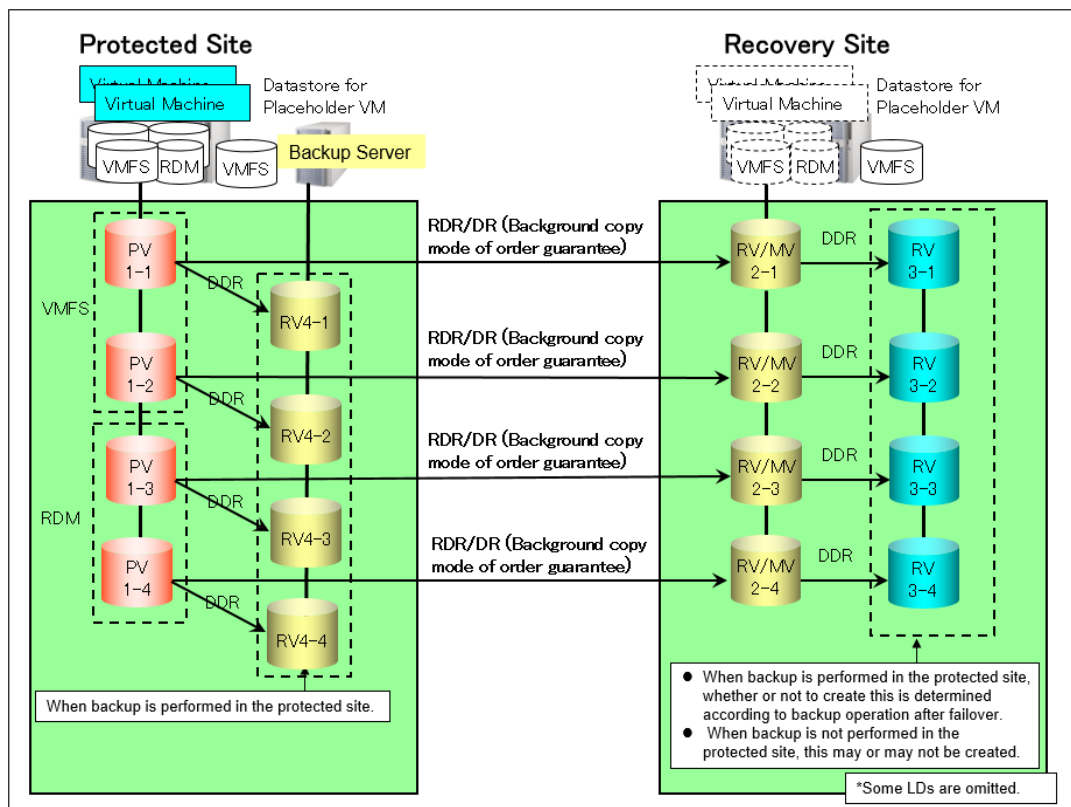


Figure 2-7: Pattern 3-2 RDR/DR (Background Copy Mode of Order Guarantee) Operation

2.2.4 Storage Logical Disk Configuration

- 1) Logical disks (PVs) in the protected site must be assigned to ESXi server by Access Control, and assigned as VMFS datastore or RDM in a VMware ESXi environment.
- 2) Logical disks for recovery (rRV) in the recovery site must be assigned to ESXi server and must be recognized as devices in the VMware ESXi storage adapter screen. These logical disks must not be assigned as VMFS datastore or RDM yet.
- 3) Logical disks (IV) for storing placeholder virtual machine configuration files must be assigned to ESXi server in the protected site and the recovery site must by using Access Control. These files must be assigned as VMFS datastore or RDM in the VMware ESXi environment.

The placeholder virtual machine configuration files are a subset of the configuration information for virtual machines and are created in the recovery site when protecting virtual machines is complete. The subset consists of files with vmx (configuration file), vmxf (supplemental configuration file) and vmsd (information about snapshots) extensions. The capacity of logical disks, although it depends on the number of virtual machines, can be as small as 2GB since these vm configuration files are generally only a few KB per virtual machine.

- 4) Example: Logical Disk Configuration

The following is an example of a logical disk configuration of RDR (synchronous) operation described above. (One VMFS datastore and two virtual machines. Each virtual machine uses one RDM.)

Table 2-5 Configuration of Storage Logical Disks in the Protected Site

LDN	LD Name	Attribute	Pool Number	Capacity (GB)	AccessControl (LUN)		Purpose
					ESXi Server 1, 2	Backup Server	
0000h	SRM_PLACEHOLDER_IV1	IV	0000h	10	000h	-	Reserved for storing placeholder virtual machines in case reprotection is performed in protected site after recovery
0001h	SRM_VMFS_PV	MV	0001h	60	001h	-	Store datastore (VMFS) in protected site.
0002h	SRM_RDM1_PV	MV	0001h	20	002h	-	Store user data (RDM) of virtual machine 1 in protected site
0003h	SRM_RDM2_PV	MV	0001h	20	003h	-	Store user data (RDM) of virtual machine 2 in protected site
0004h	SRM_VMFS_DR V	dRV	0002h	60	-	000h	Local backup of datastore (VMFS) in protected site
0005h	SRM_RDM1_DR V	dRV	0002h	20	-	001h	Local backup of user data (RDM) of virtual machine 1 in protected site
0006h	SRM_RDM2_DR V	dRV	0002h	20	-	002h	Local backup of user data (RDM) of virtual machine 2 in protected site

Table 2-6 Configuration of Storage Logical Disk in the Recovery Site

LDN	LD Name	Attribute	Pool Number	Capacity (GB)	AccessControl (LUN)	Purpose
					ESXi Server 3	
0000h	SRM_PLACEHOLDER_IV2	IV	0000h	10	000h	Store placeholder virtual machine in recovery site
0001h	SRM_VMFS_RRV	rRV	0001h	60	001h	Recover datastore (VMFS) in recovery site
0002h	SRM_RDM1_RRV	rRV	0001h	20	002h	Recover user data (RDM) of virtual machine 1 in recovery site
0003h	SRM_RDM2_RRV	rRV	0001h	20	003h	Recover user data (RDM) of virtual machine 2 in recovery site



2) and 3) above are especially important for configuring VMware SRM environment. Pay close attention to these points

2.3 Software Installation

This section describes the installation and setup of software for a disaster recovery. Log in as a member of the [Administrators] group and install the software as required below.

In this guide, the software will be installed on the default path displayed with installer.

Reboot the systems after completing all software installation.

Table 2-7 Software and Installation Target

	Software	Protected Site		Recovery Site	
		ESXi Server	Management Server	ESXi Server	Management Server
1	VMware ESXi	✓	-	✓	-
2	VMware vCenter Server	-	✓*3	-	✓*3
3	VMware vSphere Web Client	-	✓*1	-	✓*1
4	NEC Storage Manager (Server and Client) ver. 9.3 or later	-	✓*3, *4	-	✓*3, *4
5	ControlCommand ver. 9.3 or later	-	✓*3, *4	-	✓*3, *4
6	VMware Site Recovery Manager	-	✓*2, *3	-	✓*2, *3
7	NEC Storage Replication Adapter	-	✓*3	-	✓*3

✓ Installation is required

- Installation is not required

*1 The software program may be installed on a machine that can access VMware vCenter Server.

*2 VMware vCenter Server and VMware Site Recovery Manager can be installed on one server or different servers. vCenter Server Appliance can be used instead of VMware vCenter Server.

*3 Make sure to install VMware vCenter Server, VMware Site Recovery Manager, NEC Storage Manager (server) and ControlCommand before installing NEC Storage Replication Adapter.

If NEC Storage Manager (server) or ControlCommand is re-installed or upgraded after installation of NEC Storage Replication Adapter, make sure to re-install NEC Storage Replication Adapter.

*4 To use the background copy mode of order guarantee, it is necessary to install V12.1 or later.

To use M120, M320, and M320F disk arrays, it is necessary to install V10.1 or later.

2.3.1 VMware ESXi

Install VMware ESXi on application (ESXi) servers in the protected and recovery sites. For details, refer to VMware documents at:

<https://www.vmware.com/support/pubs>

2.3.2 VMware vCenter Server

Install VMware vCenter Server on the management servers in the protected and recovery sites. For details, refer to VMware documents at:

<https://www.vmware.com/support/pubs>

2.3.3 VMware vSphere Web Client

Install VMware vSphere Web Client on management servers in the protected and recovery sites.

It may be installed on a PC that can connect to VMware vCenter Server in each site. For details, refer to VMware documents at:

<https://www.vmware.com/support/pubs>

2.3.4 Storage Manager Server and Client

Install NEC Storage Manager (server and client) on the management servers in the protected and recovery sites.

When an update is performed, uninstall installed software programs first and then install the software programs. For details, refer to “NEC Storage Manager Installation Guide.”

When the screen telling the installation is complete and prompting for restart is displayed, select [Restart later] and click [Finish].

Set NEC Storage Manager in the protected site to monitor only the storage at the protected site. Set NEC Storage Manager at the recovery site to monitor only the storage at the recovery site.

It is highly recommended that monitoring through LAN be used as the monitoring method.

2.3.5 ControlCommand

Install ControlCommand on the management servers in the protected and recovery sites. When an update is performed, uninstall the installed software program first and then install the software program.

For details, refer to ControlCommand Installation Guide.

When installation is complete the Restarting Windows dialog box is displayed, select [No, I will restart my computer later] and click [OK].

2.3.6 VMware Site Recovery Manager

Install VMware Site Recovery Manager on the management servers in the protected and recovery sites. For details, refer to “Install Site Recovery Manager” - “Install Site Recovery Manager Server” in Site Recovery Manager Installation and Configuration.

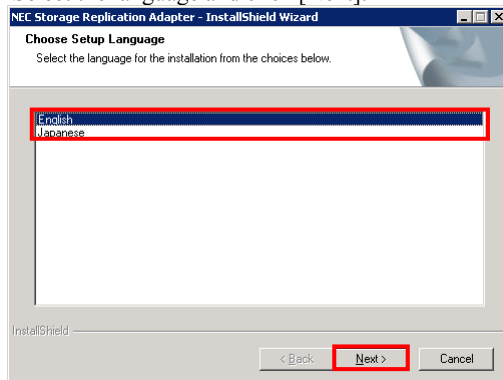
2.3.7 NEC Storage Replication Adapter

Install NEC Storage Replication Adapter on the management servers in the protected and recovery sites.

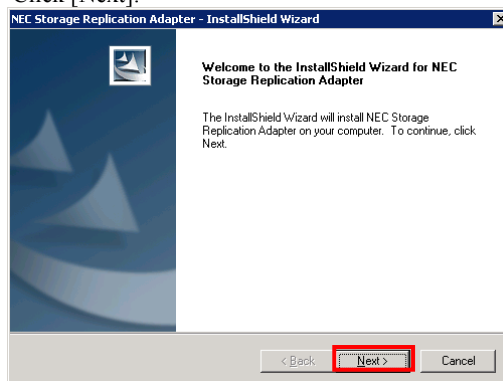
Follow the steps below for installation. When an update is performed, uninstall the installed software program first and then install the software program.

- 1) Run the installer NEC_Storage_Replication_Adapter_vX.X.X_Setup.exe.

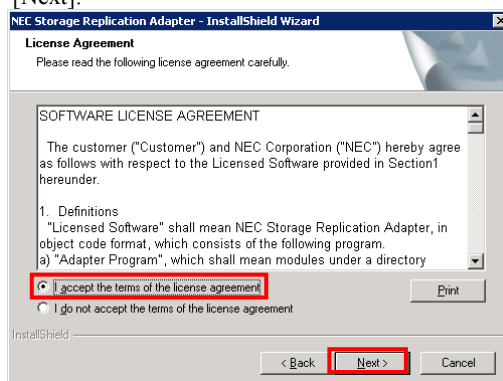
Select the language and click [Next].



- 2) Click [Next].

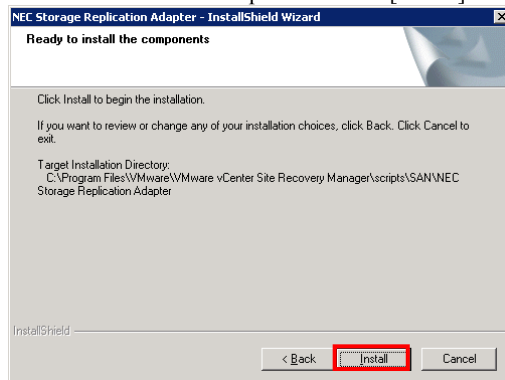


- 3) Confirm contents of License Agreement, select [I accept the terms in the license agreement], and click [Next].

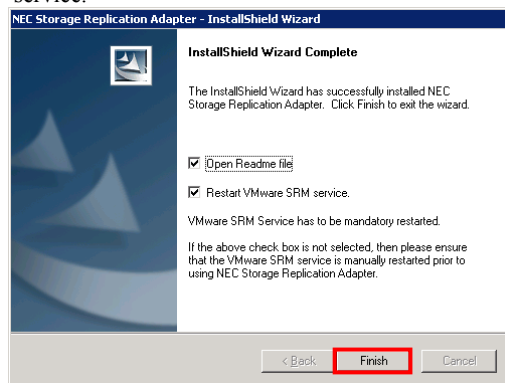


- 4) Where the software is installed is automatically set based on the VMware SRM installation path.

Confirm the installation path and click [Install].



- 5) If you want to read the Readme file, and select both [Open Readme] and [Restart VMware SRM service] and click [Finish]. After the VMware SRM service starts, this screen is automatically closed. If you do not select [Restart VMware SRM service], you must manually restart the VMware SRM service.



Be sure to restart the management server after installing all necessary software products.

2.4 Storage Configuration Settings

Configure the disk array settings by referring to “NEC Storage Software Configuration Setting Tool User’s Manual (GUI) for M Series (IS051)”.

2.4.1 Unlock License

Unlock licenses for the following software products.

- BaseProduct
- AccessControl
- RemoteDataReplication
- DynamicDataReplication (Only if needed)
- RemoteDataReplication/DisasterRecovery (Only if needed)

For details, refer to the following manual.

- To use M series storage
→11.4 “License Unlock” in “NEC Storage Software Configuration Setting Tool User’s Manual (GUI) for M Series (IS051)”

2.4.2 Bind a Pool

Bind a pool. Binding a pool may take a little time. For details, refer to the following manual.

- To use M series storage
→7.1 “Pool Bind” in “NEC Storage Software Configuration Setting Tool User’s Manual (GUI) for M Series (IS051)”

Click [Spare Binding] in the [LD Individual Bind/Unbind] screen. Bind a hot spare following the steps indicated on the wizard. For details, refer to the following manual.

- To use M series storage
→8.1 “Hot Spare Bind” in “NEC Storage Software Configuration Setting Tool User’s Manual (GUI) for M Series (IS051)”



1

- 91 L J

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99

1. On a virtual machine in the protected site:

```
#iSMvollist -cr
```
2. Obtain the signature information of the RDM of the guest OS in the protected site.

```
#iSMrc_signature -read -all
```
3. Have the output of the RDM signature information of the guest OS in a file in the C drive (system area).

```
#iSMrc_signature -export C:\Psite_signature.txt -all
```
2. Perform a recovery test, which starts up virtual machine(s) in the recovery site.
3. On virtual machine in the recovery site:

```
#iSMvollist -cr
```
2. Obtain the signature information of RDM of the guest OS in the recovery site.

```
#iSMrc_signature -read -all
```
3. Have the output of the obtained signature information in a file.

```
#iSMrc_signature -export C:\Rsite_signature.txt -all
```
4. Based on the signature information file provided at the protected site, update the signature information in the signature information file provided in the recovery site.

1

[illegible]

- 5) Make the updated signature information file effective.

```
#iSMrc_signature -import C:\Rsite_signature.txt -all
```
- 6) Check the updated information.

```
#iSMrc_signature -list -all
```

Confirm the value for "Map Signature" has been changed to the updated value. "Disk Signature" (value set to disk) is not changed yet.
- 7) Update the signature actually set to disk.

```
#iSMrc_signature -set -all
```
- 8) Check the "Disk Signature" value shown by executing `iSMrc_signature -list -all` has been change.
- 9) Start Disk Management and set the value set to the virtual machine in the protected site as drive letter assigned to the disk.
4. Perform cleanup.

- To use M series storage
→9.1 “Logical Disk Bind” in “NEC Storage Software Configuration Setting Tool User’s Manual (GUI) for M Series (IS051)”

2.4.4 Configure Access Control Settings

To control the servers' access to the logical disks, you must set Access Control.

Perform the following procedures.

- Change the Port Access Mode
- Bind a LD Set
- Link LD Set and Path
- Assign Logical Disks
- Start Access Control

For details, refer to the following manual.

- To use M series storage
 - 11.2.7 “Port Mode Switching” in “NEC Storage Software Configuration Setting Tool User’s Manual (GUI) for M Series (IS051)”
 - Chapter 10 “Host Settings” in “NEC Storage Software Configuration Setting Tool User’s Manual (GUI) for M Series (IS051)”



When changing the port mode, select WWN for the port mode.
When binding an iSCSI LD Set, select “standard” for the target mode.



Set [VMware(VW)] for the platform of the LD Set.
[VMware(LX)] may be displayed instead of [VMware(VW)]. In this case, select [VMware(LX)].

2.4.5 Synchronize Volumes

When using the background copy mode of order guarantee, configure the JNL-BUF and JBV settings.

For details about how to configure the settings, refer to the following:

“2.1.8 Journal Replication Function” in “NEC Storage Software Data Replication User’s Manual (Disaster Recovery System Installation and Operation Guide) (IS027)”

Create pairs and AT group according to your operation and synchronize volumes.

(1) Pattern 1-1 RDR (synchronous) operation

- 1 Replicate the RDR pair (PV1-1 and RV/MV2-1) in synchronous mode.
- 2 Replicate the DDR pair (PV1-1 and RV4-1) in the protected site in synchronous mode. (*1)
- 3 Replicate the DDR pair (RV/MV2-1 and RV3-1) in the recovery site in background copy mode. (*2)
- 4 Wait for the synchronization of the RDR pair (PV1-1 and RV/MV2-1) to complete.
- 5 Wait for the synchronization of the DDR pair (PV1-1 and RV4-1) in the protected site to complete. (*1)
- 6 Separate the DDR pair (PV1-1 and RV4-1) in the protected site. (*1)
- 7 Wait for the separation of the DDR pair (PV1-1 and RV4-1) in the protected site to complete. (*1)
- 8 Wait for synchronization of the DDR pair (RV/MV2-1 and RV3-1) in the recovery site to complete. (*2)
- 9 Separate the DDR pair (RV/MV2-1 and RV3-1) in the recovery site. (*2)
- 10 Wait for the separation of the DDR pair (RV/MV2-1 and RV3-1) in the recovery site to complete. (*2)

*1 This step is required to create a DDR backup (RV4-1) in the protected site. If this DDR backup is not created, skip this step.

*2 This step is required to create a DDR backup (RV3-1) in the recovery site. If this DDR backup is not created, skip this step.

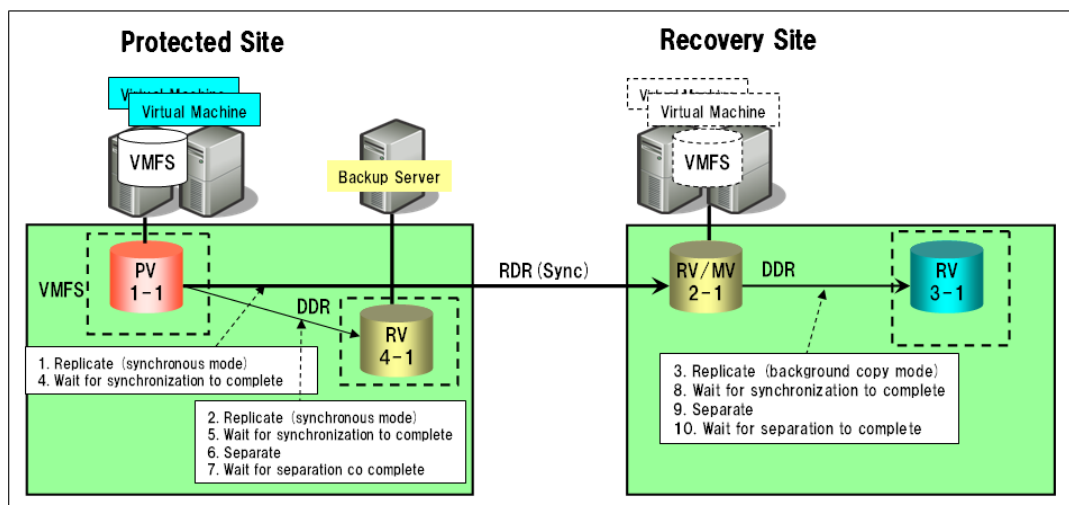


Figure 2-8: Pattern 1-1 RDR (Synchronous) Operation

(2) Pattern 1-2 RDR (synchronous) operation

- 1 Replicate RDR pairs (PV1-n and RV/MV2-n) in synchronous mode.
- 2 Replicate DDR pairs (PV1-n and RV4-n) in the protected site in synchronous mode. (*1)
- 3 Replicate DDR pairs (RV/MV2-n and RV3-n) in the recovery site in background copy mode. (*2)
- 4 Wait for the synchronization of the RDR pairs (PV1-n and RV/MV2-n) to complete.
- 5 Wait for the synchronization of the DDR pairs (PV1-n and RV4-n) in the protected site to complete. (*1)
- 6 Separate the DDR pairs (PV1-1 and RV4-1) in the protected site. (*1)
- 7 Wait for the separation of the DDR pairs (PV1-n and RV4-n) in the protected site to complete. (*1)
- 8 Wait for synchronization of the DDR pairs (RV/MV2-n and RV3-n) in the recovery site to complete. (*2)
- 9 Separate the DDR pairs (RV/MV2-n and RV3-n) in the recovery site. (*2)
- 10 Wait for the separation of the DDR pairs (RV/MV2-n and RV3-n) in the recovery site to complete. (*2)

*1 This step is required to create DDR backups (RV4-n) in the protected site. If these DDR backups are not created, skip this step.

*2 This step is required to create DDR backups (RV3-n) in the recovery site. If these DDR backups are not created, skip this step.

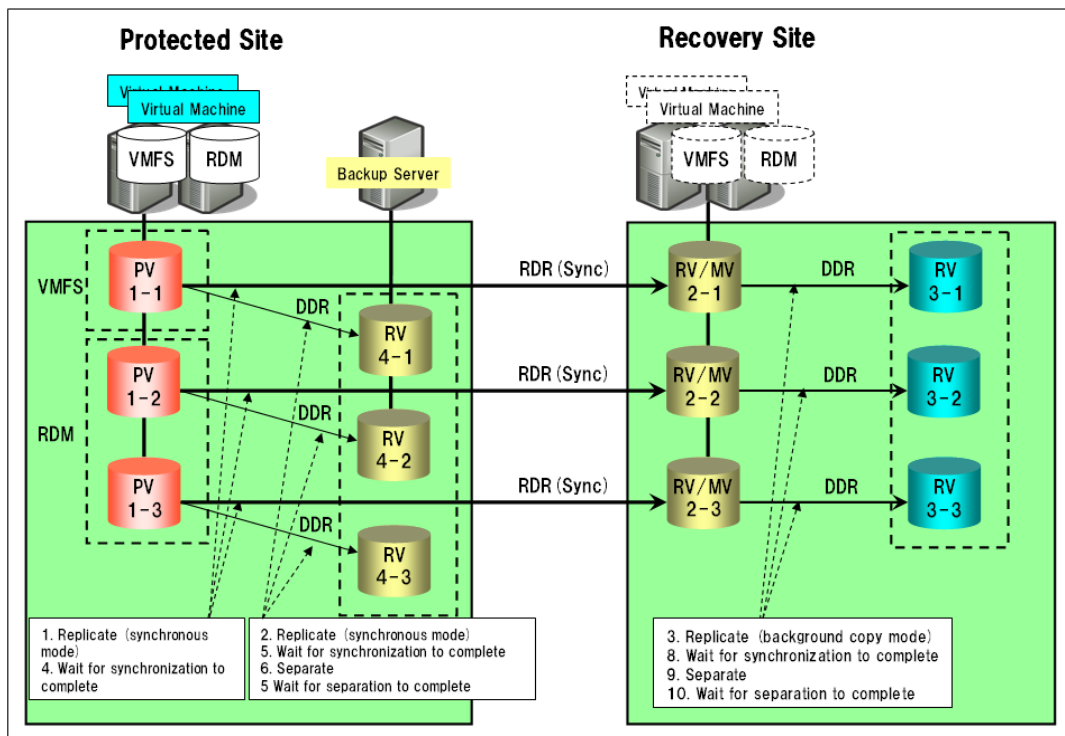


Figure 2-9: Pattern 1-2 RDR (Synchronous) Operation

(3) Pattern 2 RDR (asynchronous) operation

- 1 Replicate DDR pairs (PV1-n and RV/MV2-n) in the protected site in synchronous mode
- 2 Replicate RDR pairs (RV/MV2-n and RV/MV3-n) in background copy mode.
- 3 Replicate DDR pairs (RV/MV3-n and RV4-n) in the recovery site in background copy mode.
- 4 Wait for the synchronization of the DDR pairs (PV1-n and RV/MV2-n) in the protected site to complete.
- 5 Separate the DDR pairs (PV1-n and RV/MV2-n) in the protected site.
- 6 Wait for the synchronization of the DDR pairs (PV1-n and RV/MV2-n) in the protected site to complete.
- 7 Wait for the synchronization of the RDR pairs (RV/MV2-n and RV/MV3-n) to complete.
- 8 Wait for the synchronization of the DDR pairs (RV/MV3-n and RV4-n) in the recovery site to complete.
- 9 Separate the DDR pairs (RV/MV3-n and RV4-n) in the recovery site.
- 10 Wait for the separation of the DDR pairs (RV/MV3-n and RV4-n) in the recovery site to complete.

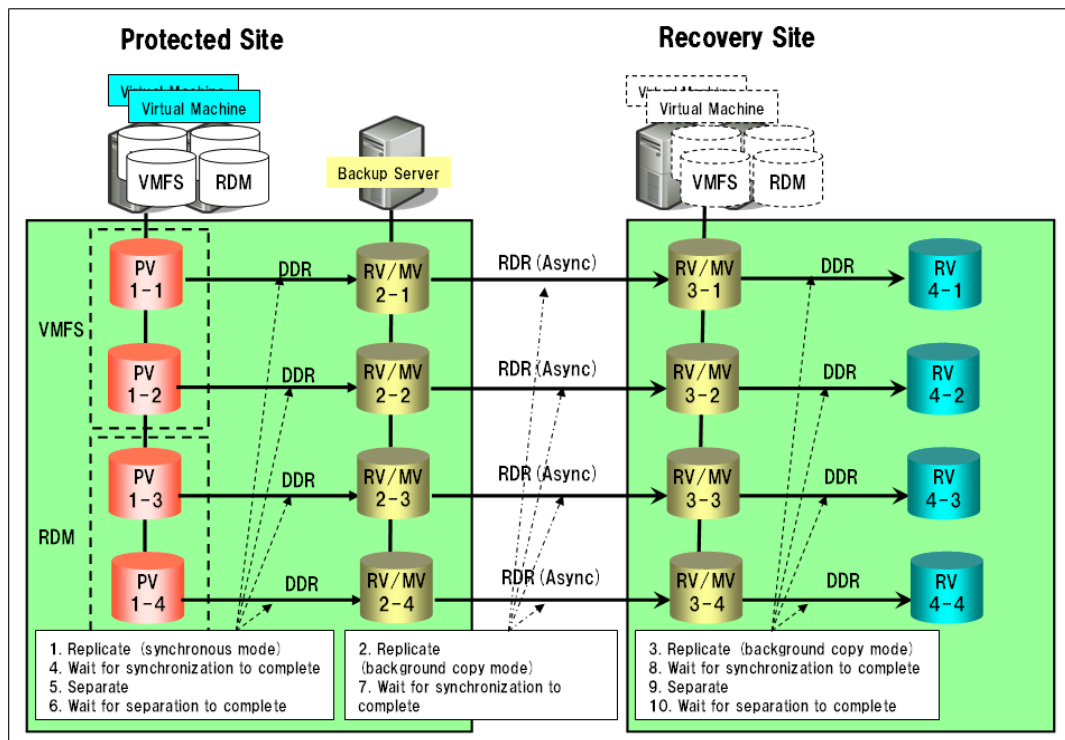


Figure 2-10: Pattern 2 RDR (Asynchronous) Operation

(4) Pattern 3-1 RDR/DR (synchronous or semi-synchronous) operation

- 1 Replicate an AT group (PV1-n and RV/MV2-n) in synchronous or semi-synchronous mode of order guarantee.
- 2 Replicate DDR pairs (PV1-n and RV4-n) in the protected site in synchronous mode. (*1)
- 3 Replicate DDR pairs (RV/MV2-n and RV3-n) in the recovery site in background copy mode. (*1))
- 4 Wait for the synchronization of the AT group (PV1-n and RV/MV2-n) to complete.
- 5 Wait for the synchronization of the DDR pairs (PV1-n and RV4-n) in the protected site to complete. (*1)
- 6 Separate the DDR pairs (PV1-n and RV4-n) in the protected site (*1)
- 7 Wait for the separation of the DDR pairs (PV1-n and RV4-n) in the protected site to complete. (*1)
- 8 Wait for the synchronization of the DDR pairs (RV/MV2-n and RV3-n) in the recovery site to complete. (*2)
- 9 Separate the DDR pairs (RV/MV2-n and RV3-n) in the recovery site. (*2)
- 10 Wait for the separation of the DDR pairs (RV/MV2-n and RV3-n) in the recovery site to complete. (*2)

*1 This step is required to create DDR backups (RV4-n) in the protected site. If these DDR backups are not created, skip this step.

*2 This step is required to create DDR backups (RV/MV2-n and RV3-n) in the recovery site. If these DDR backups are not created, skip this step.

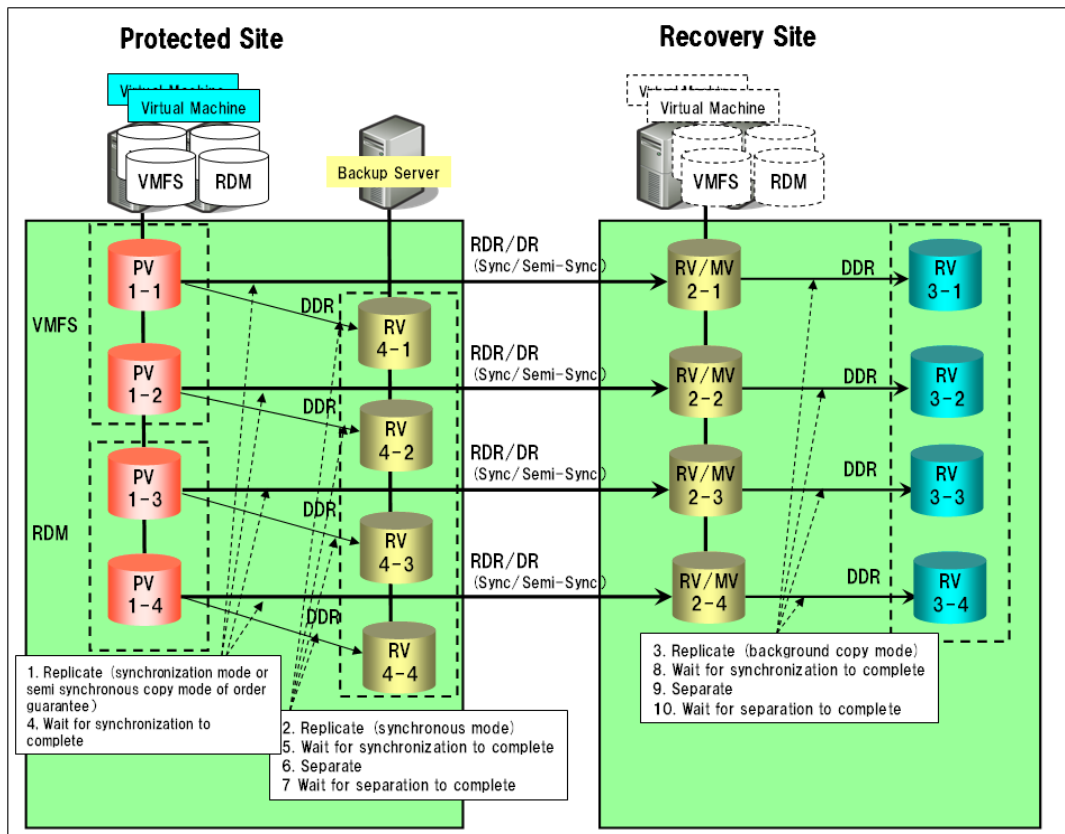


Figure 2-11: Pattern 3-1 RDR/DR (Synchronous or Semi-synchronous) Operation

For details of replication settings in the RDR or RDR/DR configuration, refer to the following manuals.

- 3.3 “Various Operations of Replication Management” in NEC Storage Software Data Replication User’s Manual Function Guide (IS015)
- 4.1 “Storage Manager’s ATgroup Function Operation Method (GUI)” in “NEC Storage Software Data Replication User’s Manual (Disaster Recovery System Installation and Operation Guide) (IS027)”



For D series, set the platform of LD Set to LX.
For M series, set the platform of LD Set to VMware (LX).



Match the LUN number of the logical disk allocated in each LD setting when Datastore (VMFS) and RDM (Raw Device Mapping) between multiple VMware ESXi are shared.



Access Control takes effect immediately. If the link setting for the LD set is wrong, the server will not be able to access any logical disks in the LD set. Therefore, you need to have a good grasp of the operation status before carrying out this operation. Also, if necessary, stop the operation and application servers based on a plan.

(5) Pattern 3-2 RDR/DR (background copy mode of order guarantee) operation

- 1 Replicate an AT group (PV1-n and RV/MV2-n) in background copy mode of order guarantee.
- 2 Replicate DDR pairs (PV1-n and RV4-n) in the protected site in synchronous mode. (*1)
- 3 Replicate DDR pairs (RV/MV2-n and RV3-n) in the recovery site in background copy mode. (*1))
- 4 Wait for the synchronization of the AT group (PV1-n and RV/MV2-n) to complete.
- 5 Wait for the synchronization of the DDR pairs (PV1-n and RV4-n) in the protected site to complete. (*1)
- 6 Separate the DDR pairs (PV1-n and RV4-n) in the protected site (*1)
- 7 Wait for the separation of the DDR pairs (PV1-n and RV4-n) in the protected site to complete. (*1)
- 8 Wait for the synchronization of the DDR pairs (RV/MV2-n and RV3-n) in the recovery site to complete. (*2)
- 9 Separate the DDR pairs (RV/MV2-n and RV3-n) in the recovery site. (*2)
- 10 Wait for the separation of the DDR pairs (RV/MV2-n and RV3-n) in the recovery site to complete. (*2)

*1 This step is required to create DDR backups (RV4-n) in the protected site. If these DDR backups are not created, skip this step.

*2 This step is required to create DDR backups (RV/MV2-n and RV3-n) in the recovery site. If these DDR backups are not created, skip this step.

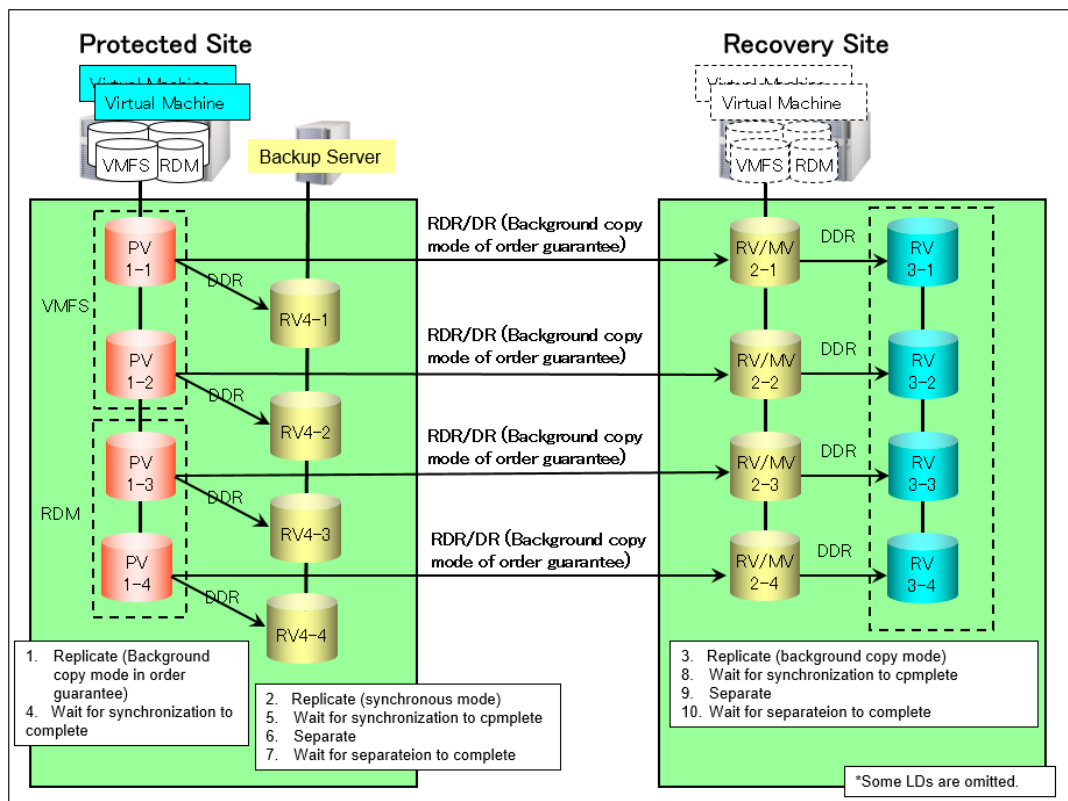


Figure 2-12: Pattern 3-2 RDR/DR (Background Copy Mode of Order Guarantee) Operation

2.5 Virtual Machines Configuration

Configure virtual machines and applications in the protected site.

See VMware documents for details on how to configure virtual machines.

<http://partnerweb.vmware.com/GOSIG/home.html>

2.6 VMware Site Recovery Manager Setting

Virtual machines are protected by connecting the protected and recovery sites and defining pair relationship between the sites.

Configure the following SRM settings

- Connect sites
- Configure inventory mappings
- Assign placeholder datastores
- Configure array-based replication
- Create a protection group
- Create a recovery plan

2.6.1 Connect Sites (Protected site process)

Pair the protected site and the recovery site, make both mutually recognizing the other, and connect them.

For the specific operation method, see the VMware documentation that is published on

<http://www.vmware.com/support/pubs>.

2.6.2 Configure Inventory Mappings (Protected site and recovery site process)

Map inventories (resource, folder and network) between the protected site and the recovery site.

For the specific operation method, see the VMware documentation that is published on

<http://www.vmware.com/support/pubs>.

2.6.3 Assign Placeholder Datastores (Protected site and recovery site process)

Define the datastore prepared to store placeholder virtual machines in the recovery site as a placeholder store in the protected site.

Create a datastore to store placeholder virtual machines in the protected site as well for reprotection after a failover and define it as a placeholder store in the recovery site.

For the specific operation method, see the VMware documentation that is published on

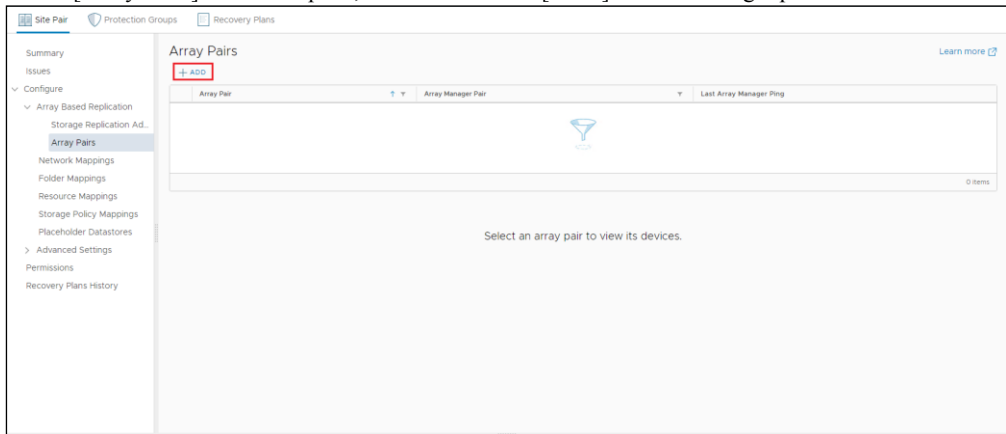
<http://www.vmware.com/support/pubs>.

2.6.4 Configure Array-Based Replication (Protected site process)

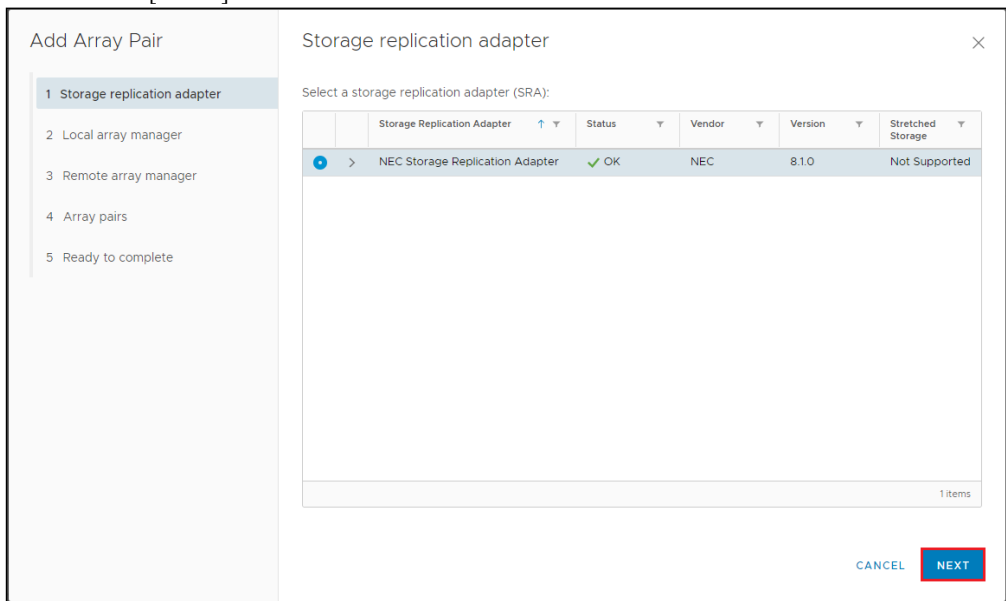
Based on the information on storage connected to each site and replication pairs detected by NEC Storage Replication Adapter, SRM detects the status of storage, logical disks (PV) in the protected site and storage used in the recovery site and logical disks (rRV) used for recovery and how they are related.

Make settings according to the following procedure.

- 1) Start vSphere Web Client and then log in to vCenter Server as the vCenter administrator.
From the [Home] menu, click [Site Recovery], [OPEN Site Recovery], and then [VIEW DETAILS] to open the [Site Recovery] window.
- 2) Select [Array Pairs] on the left pane, and then click the [ADD] icon on the right pane.



- 3) On the [Storage replication adapter] window, select the installed SRA for both of the array managers, and then click [NEXT].



- 4) Enter the array manager name of the protected site and comment, and then click [NEXT].

The screenshot shows the 'Add Array Pair' wizard with the 'Local array manager' step selected in the left sidebar. The main panel contains the following elements:

- Local array manager** (Title)
- Array managers allow Site Recovery Manager to communicate with array based replication storage systems.** (Information)
- Enter a name for the array manager on "vcsa1.srm.sra":** (Text input field with value **ProManager**)
- Diskarray Searching** (Section header)
- NEC Corporation** (Text input field)
- Comment** (Text input field with value **ProtectSite**)
- Please input the comment** (Text)
- CANCEL**, **BACK**, and **NEXT** buttons at the bottom right.

- 5) Enter the array manager name of the recovery site and comment, and then click [NEXT].

The screenshot shows the 'Add Array Pair' wizard with the 'Remote array manager' step selected in the left sidebar. The main panel contains the following elements:

- Remote array manager** (Title)
- ☐ **Do not create a remote array manager now.** (Checkbox)
- Enter a name for the array manager on "vcsa2.srm.sra":** (Text input field with value **RecManager**)
- Diskarray Searching** (Section header)
- NEC Corporation** (Text input field)
- Comment** (Text input field with value **RecoverSite**)
- Please input the comment** (Text)
- CANCEL**, **BACK**, and **NEXT** buttons at the bottom right.

- Add Array Pair

1 Storage replication adapter

2 Local array manager

3 Remote array manager

4 Array pairs

5 Ready to complete

Array pairs

Select the array pairs to enable:

<input checked="" type="checkbox"/>	vcsa1.srm.sra	vcsa2.srm.sra	Status
<input checked="" type="checkbox"/>	0200200000255C3A26090000000000000...	0200200000255CDB040B00000000000000...	Ready to ...

☒ 11 items

CANCEL

BACK

NEXT

- Add Array Pair

1 Storage replication adapter

2 Local array manager

3 Remote array manager

4 Array pairs

5 Ready to complete

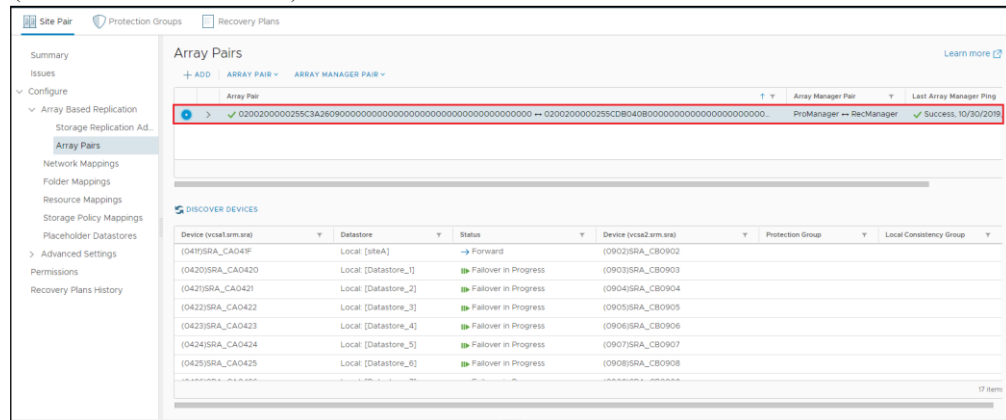
Ready to complete

Review your selected settings.

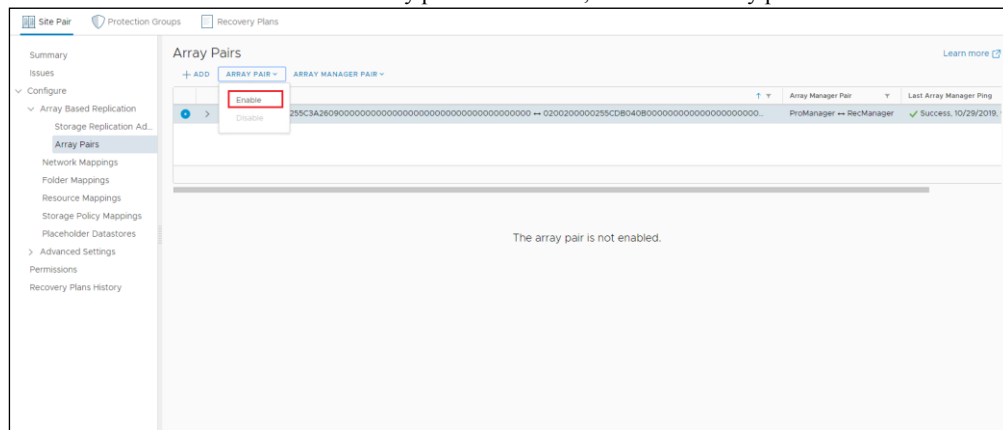
Storage replication adapter	NEC Storage Replication Adapter
Array manager for "vcsa1.srm.sra"	ProManager
Array manager for "vcsa2.srm.sra"	RecManager
Array pairs to enable	0200200000255C3A260900 → 0200200000255CD8040B000

CANCELBACKFINISH

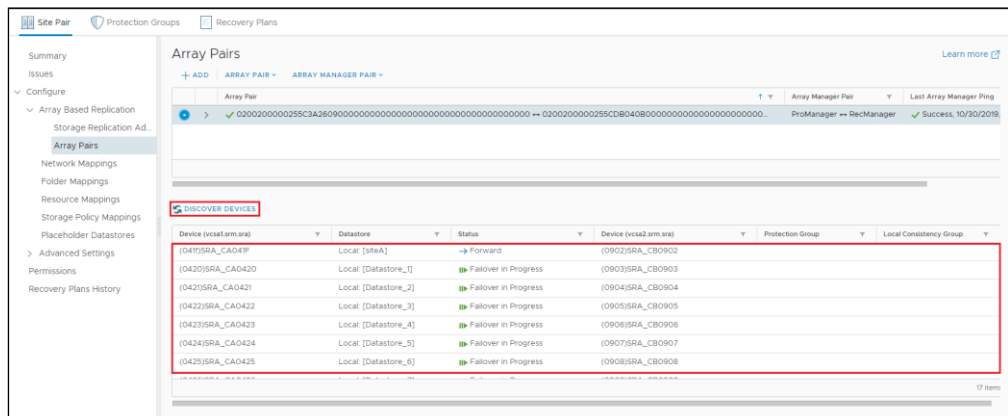
- 8) On the [Array Pairs] window, check that the pair displayed in the [Array Pair] column is enabled (indicated with a check mark).



If the status of the detected array pair is “Disabled,” enable the array pair.



- 9) Check that the array pair relationship, volume pair relationship, and volume recognition of each site are correct.
- [Array Pair]: Identification information (Subsystem Absolute Address) of disk arrays in [Protected Site] and [Recovery Site]
 - [Device (vCenter Server)]: Logical disk information of a disk array
For [Protected Site], logical disks of the PV attribute are displayed in the (LD number) LD name format.
For [Recovery Site], logical disks of the rRV attribute are displayed in the (LD number) LD name format.
 - Direction: direction of a pair of logical disks in the local site and in the remote site
 - Datastore: information on devices on the ESXi (datastore and RDM) configured by logical disks



If [Array Pairs] fails, check the following and remove the cause of the problem and then try again.

- NEC Storage Replication Adapter is installed successfully
- NEC Storage Replication Adapter is correctly recognized by VMware SRM.
- Monitoring is performed successfully by NEC Storage Manager.
- Replication pair relationship is correct.
- RDR or RDR/DR is in the replicated status. If it is in the separated status, the access mode of rRV is ReadWrite or NotReady.
- The `iSMrc_replicate -wait`, `iSMrc_separate -wait`, or `iSMrc_wait` commands have not been executed via iSM.



If there is any change in the storage status, such as a change of the disk array name or logical disk name, addition or deletion of an RDR pair, or addition or deletion of a volume to/from the ATgroup, make sure to update the configuration information by clicking the [DISCOVER DEVICES] icon.

2.6.5 Create a Protection Group (Protected site process)

SRM collects information on datastores and RDMs that virtual machines use and manages related datastore and RDM as a single datastore group.

A protected group is created by relating protected group and datastore group.

For details, see “Replicating Virtual Machines”, “Creating Protection Groups”, and “Customizing a Recovery Plan” in Site Recovery Manager Administration.



In the RDR/DR operation, volumes (PV) that are included in the AT group and datastore group should match.

2.6.6 Create a Recovery Plan (Recovery site process)

A recovery plan defines how virtual machines in the protected group are recovered. The recovery play is stored in the SRM database in the recovery site and executed by SRM.

For details, refer to “Creating, Testing, and Running Recovery Plans” and “Customizing a Recovery Plan” in Site Recovery Manager Administration.

Chapter 3 Operations

3.1 Backup Creation by User

For a planned migration and disaster recovery, a backup is performed according to the schedule by user.

3.1.1 Pattern 1-1 RDR (synchronous) operation

RV (RV/MV2-1) has data consistent with PV1-1. Because of this, users do not need to create a backup.

3.1.2 Pattern 1-2 RDR (synchronous) operation

RV (RV/MV2-1) has data consistent with PV1-1. Because of this, users do not need to create a backup.

The user areas are backed up by using a job management software program and by repeating the following steps periodically.

(1) Backing up user areas (PV1-n ($n \geq 2$))

1. If RDR pairs (PV1-n and RV/MV2-n ($n \geq 2$)) are separated, perform replication in synchronous mode.
2. Wait for the synchronization of the RDR pairs (PV1-n and RV/MV2-n ($n \geq 2$)) to complete.
3. Establish association with operation (such as database) on virtual machine, assure the quiescent point, and then separate the RDR pairs (PV1-n and RV/MV2-n ($n \geq 2$)).
Configure the RV access restriction of RV/MV2-n ($n \geq 2$) to ReadWrite.
4. Wait for the separation of the RDR pairs (PV1-n and RV/MV2-n ($n \geq 2$)) to complete.
5. If your operations are stopped in Step 4, resume the operations.
6. Replicate DDR pairs (RV/MV2-n and RV3-n ($n \geq 2$)) in the recovery site in synchronous mode.
7. Wait for the synchronization of the DDR pairs (RV/MV2-n and RV3-n ($n \geq 2$)) in the recovery site to complete.
8. Separate the DDR pairs (RV/MV2-n and RV3-n ($n \geq 2$)) in the recovery site.
9. Wait for the separation of the DDR pairs (RV/MV2-n and RV3-n ($n \geq 2$)) in the recovery site to complete.
10. Replicate RDR pairs (PV1-n and RV/MV2-n ($n \geq 2$)) in synchronous mode.

* You can use ControlCommand on virtual machine to create backups (RV4-n, RV/MV2-n) of user areas (RDMs).

If an OS not supported by ControlCommand is used for virtual machine, the quiescence point must be assured by stopping the virtual machine.

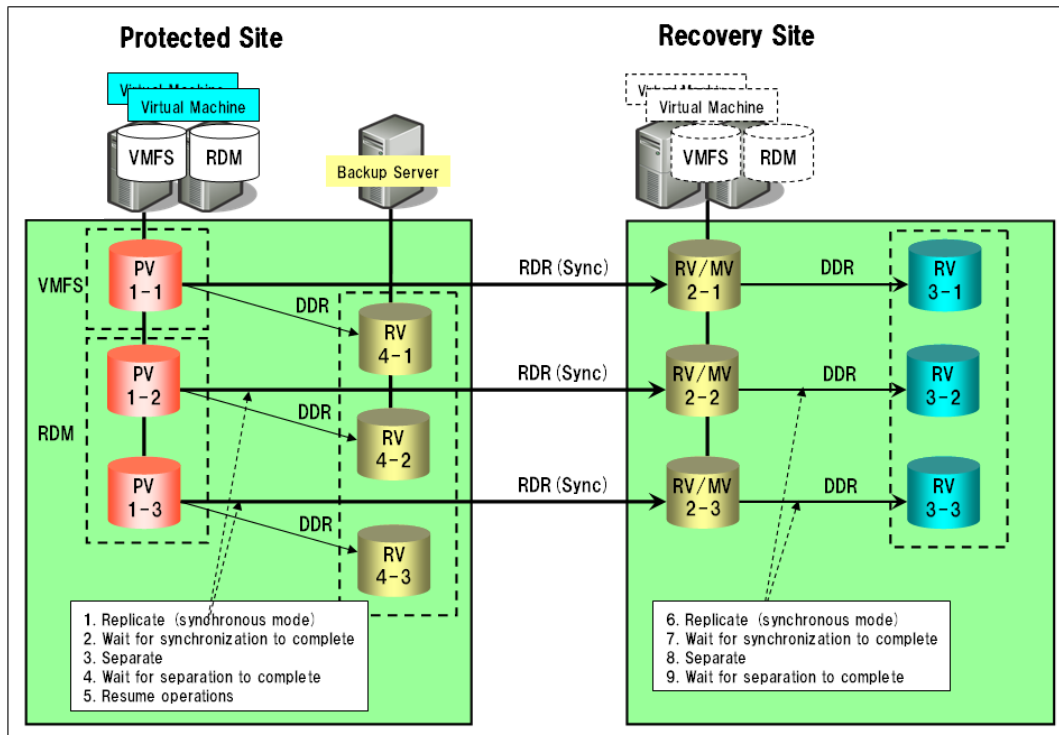


Figure 3-1: Example of Backup by Pattern 1-2 RDR Synchronous Operation

3.1.3 Pattern 2 RDR (asynchronous) operation

The system area and the user area must be backed up periodically by using a job management software program.

(1) Backing up all data including the system area (PV1-n ($n \leq 2$))

In general, the system area (PV1-n ($n \leq 2$)) does not need to be backed up frequently unless a system is updated, such as update of virtual machine OS or application.

Follow the steps below to perform a complete quiescent point backup covering the system area.

1. If RDR pairs (RV/MV2-n and RV/MV3-n ($n \geq 1$)) are separated, perform replication in background copy mode.
2. Replicate DDR pairs (PV1-n and RV/MV2-n ($n \geq 1$)) in the protected site in synchronous mode.
3. Wait for the synchronization of the DDR pairs (PV1-n and RV/MV2-n ($n \geq 1$)) in the protected site to complete.
4. Stop all virtual machines that use PV1-n.
5. Separate the DDR pairs (PV1-n and RV/MV2-n ($n \geq 1$)) in the protected site.
6. Wait for the separation of the DDR pairs (PV1-n and RV/MV2-n ($n \geq 1$)) in the protected site to complete.
7. Start the virtual machines stopped in Step 4.
8. Wait for the synchronization of the RDR pairs (RV/MV2-n and RV/MV3-n ($n \geq 1$)) to complete.

9. Separate the RDR pairs (RV/MV2-n and RV/MV3-n ($n \geq 1$)).
Configure the RV access restriction of RV/MV3-n ($n \geq 2$) to ReadWrite.
 10. Wait for the separation of the RDR pairs (RV/MV2-n and RV/MV3-n ($n \geq 1$)) to complete.
 11. Replicate DDR pairs (RV/MV3-n and RV4-n ($n \geq 1$)) in the recovery site in synchronous mode.
 12. Wait for the synchronization of the DDR pairs (RV/MV3-n and RV4-n ($n \geq 1$)) in the recovery site to complete.
 13. Separate the DDR pairs (RV/MV3-n and RV4-n ($n \geq 1$)) in the recovery site.
 14. Wait for the separation of the DDR pairs (RV/MV3-n and RV4-n ($n \geq 1$)) in the recovery site.
 15. Replicate the RDR pairs (RV/MV2-n and RV/MV3-n ($n \geq 1$)) in background copy mode.
- * When separation of RV/MV2-n ($n \geq 1$) is complete (when Step 6 is finished), backup data having complete quiescent point of PV1-n is created in RV (RV/MV2-n). It can be backed up in media such as tape if necessary.

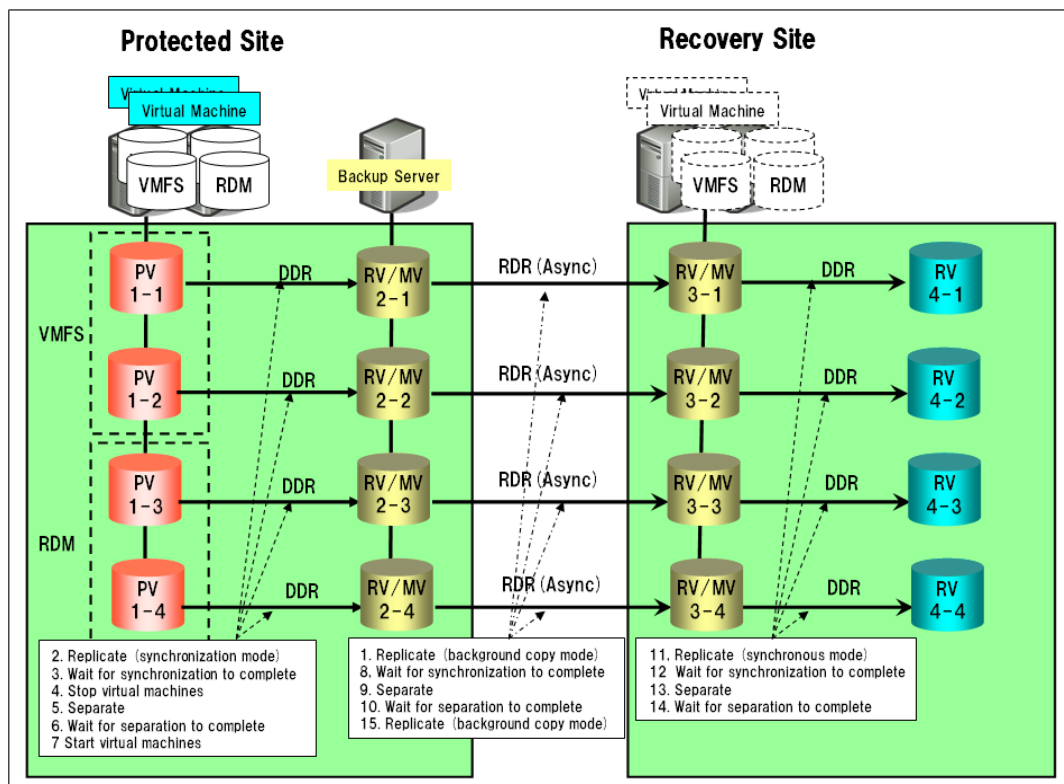


Figure 3-2: Example 1 of Backup by Pattern 2 RDR (Asynchronous) Operation

(2) Backing up the user area (PV1-n ($n \geq 3$))

Back up the user area periodically by using a job management software program and repeating the following steps.

1. If RDR pairs (RV/MV2-n and RV/MV3-n ($n \geq 3$)) are separated, perform replication in background copy mode.
2. Replicate DDR pairs (PV1-n and RV/MV2-n ($n \geq 3$)) in the protected site in synchronous mode.
3. Wait for the synchronization of the DDR pairs (PV1-n and RV/MV2-n ($n \geq 3$)) in the protected site to complete.

4. Establish association with operation (such as database) on virtual machine, assure the quiescent point, and then separate the RDR pair (PV1-n and RV/MV2-n ($n \geq 3$)) in the protected site.
5. Wait for the separation of the RDR pairs (PV1-n and RV/MV2-n ($n \geq 3$)) in the protected site to complete.
6. If your operations are stopped in Step 4, resume the operations.
7. Wait for synchronization the RDR pairs (RV/MV2-n and RV/MV3-n ($n \geq 3$)) to complete.
8. Separate the RDR pairs (RV/MV2-n and RV/MV3-n ($n \geq 3$)).
Configure the RV access restriction of RV/MV3-n to ReadWrite.
9. Wait for the separation of the RDR pairs (RV/MV2-n and RV/MV3-n ($n \geq 3$)) to complete.
10. Replicate DDR pairs (RV/MV3-n and RV4-n ($n \geq 3$)) in the recovery site in synchronous mode.
11. Wait for the synchronization of the DDR pairs (RV/MV3-n and RV4-n ($n \geq 3$)) in the recovery site.
12. Separate the DDR pairs (RV/MV3-n and RV4-n ($n \geq 3$)) in the recovery site.
13. Wait for the separation of the DDR pairs (RV/MV3-n and RV4-n ($n \geq 3$)) in the recovery site to complete.
14. Replicate the RDR pairs (RV/MV2-n and RV/MV3-n ($n \geq 3$)) in background copy mode.
15. When the separation of the DDR pairs (PV1-n and RV/MV2-n ($n \geq 3$)) is complete (when Step5 is finished), backup data of PV1-n is created in RV/MV2-n. It can be backed up in media such as tape if necessary.

*You can use ControlCommand on virtual machine to create backup (RV/MV2-n) of user areas (RDMs).

If an OS not supported by ControlCommand is used for virtual machine, the quiescent point must be assured by stopping the virtual machine.

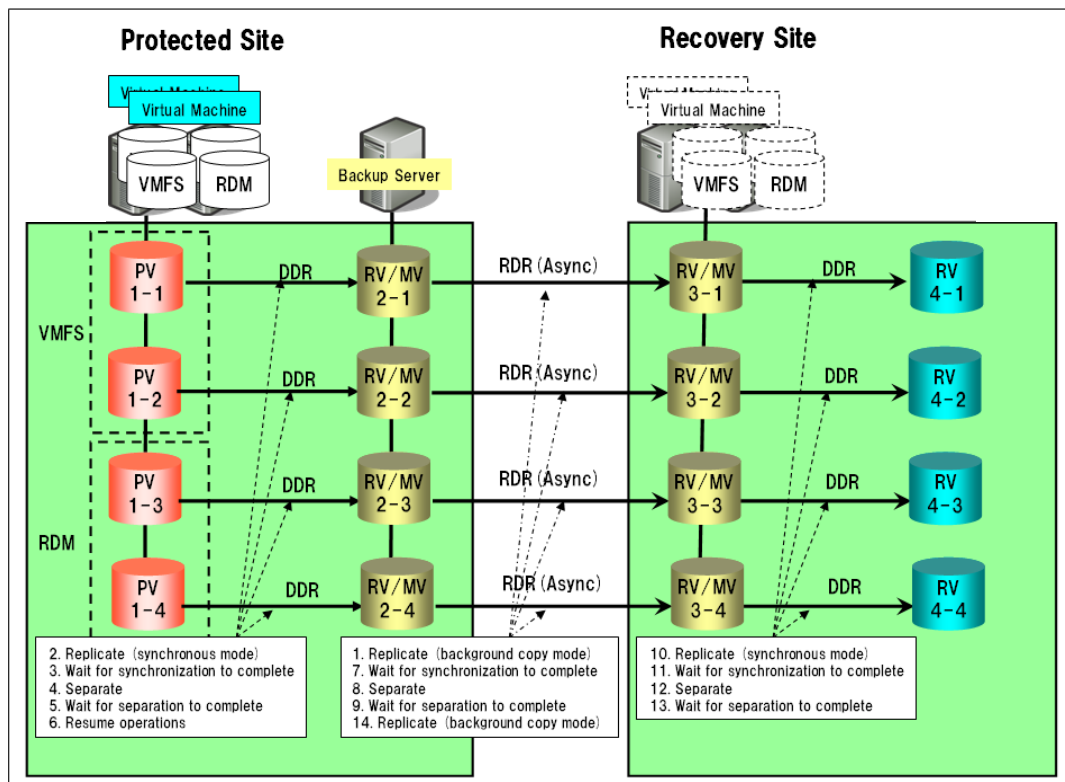


Figure 3-3: Example 2 of Backup by Pattern 2 RDR (Asynchronous) Operation

3.1.4 Pattern 3-1 RDR/DR (synchronous or semi-synchronous) operation

RV/MV2-n in the recovery site has the same or similar data with consistency as master volumes in the protected site. Because of this, users do not need to create a backup.

3.1.5 Pattern 3-2 RDR/DR (background copy mode of order guarantee) operation

RV/MV2-n in the recovery site has the same or similar data with consistency as master volumes in the protected site. Because of this, users do not need to create a backup.

3.2 Test a Recovery Plan (Operation at Recovery Site)

You can test a recovery plan for planned migration and disaster recovery without having impact on operations in the protected site and the recovery site.

For details on how to perform, refer to “Creating, Testing, and Running Recovery Plans” - “Testing a Recovery Plan” in Site Recovery Manager Administration.

Notes on testing a recovery plan

- 1) When you perform a planned migration, select [Replicate recent changes to recovery site] on the window to confirm the testing, and perform the test.
When a planned migration is performed, data consistency is completely assured because SRM shuts down virtual machines in the protected site and data on PVs (PV1-n) is copied to rRV and recovered in the recovery site. On the other hand, when a test is performed, virtual machines in the protected site are not stopped, so data consistency is not completely assured. Therefore, it is recommended to perform a test while workloads (I/O writes) are low.
- 2) When you perform a disaster recovery, clear the [Replicate recent changes to recovery site] check box on the window to confirm testing, and perform the test. The recovery test is performed by using backup data (rRV). When backups need to be created by user, consistent backup data must be created in rRV before performing the test.
- 3) When users take backups for the operations, perform the test after the backup process is finished. If replication or separation for the backup process is performed while the SRA process is running, an error may occur.

3.3 Run a Recovery Plan (Operation at Recovery Site)

All virtual machines in the recovery plan failover to the recovery site from the protected site.

For details on how to perform, refer to “Creating, Testing, and Running Recovery Plans” in Site Recovery Manager Administration.

Notes on running a recovery plan

- 1) When you perform a planned migration, run the recovery plan after backup processes are finished if users take backups for the operations.
- 2) If recovery is required because a disaster occurred while a user was making a backup, run the recovery plan after confirming the replication state of the volumes.
 - Pattern 1-1 RDR (synchronous) operation using a single volume
 - i) The DDR pair (RV/MV2-1 and RV3-1) in the recovery site is separated.
 - ii) When the RDR pair (PV1-1 and V/MV2-1) is separated, RV access of RV/MV2-1 is ReadWrite.
 - Pattern 1-2 RDR (synchronous) operation using multiple volumes
 - i) DDR pairs (RV/MV2-1 and RV3-1) in the recovery site are separated.
 - Pattern 2 RDR (asynchronous) operation
 - i) DDR pairs (RV/MV3-n and RV4-n) in the recovery site are separated.
 - ii) When RDR pairs (RV/MV2-n and RV/MV3-n) are separated, RV access of RV/MV3-n is ReadWrite.
 - Pattern 3-1 RDR/DR (synchronous or semi-synchronous) operation
 - i) DDR pairs (RV/MV2-n and RV3-n) in the recovery site are separated.
 - Pattern 3-2 RDR/DR (background copy mode of order guarantee) operation
 - i) DDR pairs (RV/MV2-n and RV3-n) in the recovery site are separated.
- 3) When a disaster recovery is performed in a system where users take backups for the operations, perform a recovery by using consistent backup data.
 - Pattern 1-1 RDR (synchronous) operation using a single volume
 - i) Recovery is performed by using RV/MV2-1
 - Pattern 1-2 RDR (synchronous) operation using multiple volumes
 - i) When virtual machines use one or less RDM, the recovery should be performed using RV/MV2-n.
 - ii) When virtual machines use two or more RDMs, use one of backup data of RV/MV2-n and RV3-n that is consistent, and perform the recovery. If RV3-n has consistent data, protection should be restored from RV3-n to RV/MV2-n, and perform the recovery using RV/MV2-n.
 - Pattern 2 RDR (asynchronous) operation
 - i) Use one of backup data of RV/MV2-n and RV3-n that is consistent, and perform the recovery. If RV3-n has consistent data, protection should be restored from RV3-n to RV/MV2-n, and perform the recovery using RV/MV2-n.

- Pattern 3-1 RDR/DR (synchronous or semi-synchronous) operation
 - i) Perform recovery by using RV/MV2- and RV3-n.
- Pattern 3-2 RDR/DR (background copy mode of order guarantee) operation
 - i) Perform recovery by using RV/MV2- and RV3-n.

3.4 Reprotection

After running a recovery plan to failover from the protected site to recovery site, reprotection is performed if you use the original recovery site as new protected site and vice versa. Reprotection can be performed on a condition that the original protected site is properly functioning. When reprotection is performed, synchronization is performed by configuring RDR pairs and AT groups in the storage in the opposite direction. For details on how to perform, see “Reprotecting Virtual Machines after a Recovery” in Site Recovery Manager Administration.

(1) Pattern 1-1 RDR (synchronous) operation

The SRA program reconfigures the RDR pair as shown below for reprotection.

1. Unpair the RDR pair (PV1-1 and RV/MV2-1).
2. Configure the RDR pair (RV/MV2-1 and PV1-1) in the opposite direction by using RV/MV2-1 as PV.
3. Replicate (enable the copy mode setting for) the RDR pair (RV/MV2-1 and PV1-1).

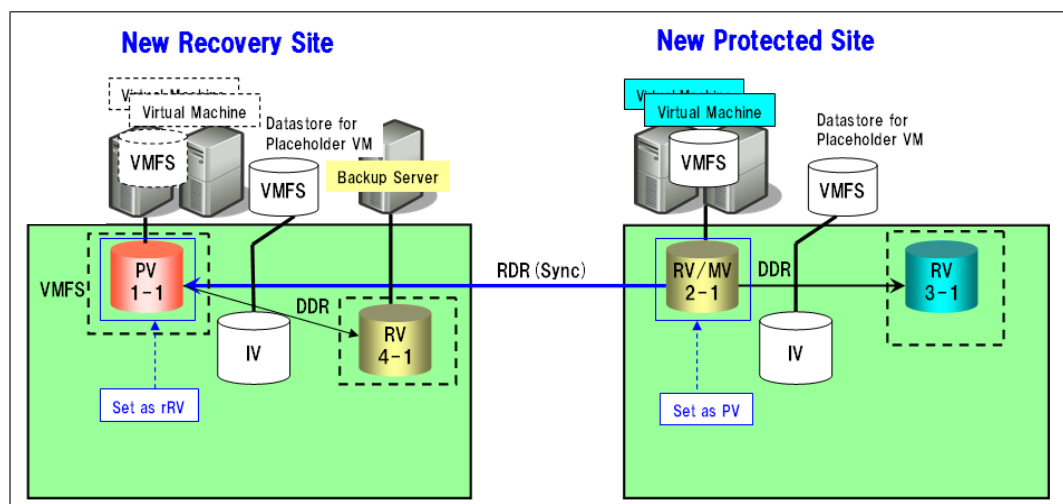


Figure 3-4: Pair Reconfiguration for Pattern 1-1 RDR (Synchronous) Operation

(2) Pattern 1-2 RDR (synchronous) operation

The SRA program reconfigures RDR pairs as shown below for reprotection.

1. Unpair RDR pairs (PV1-n and RV/MV2-n).
2. Configure RDR pairs (RV/MV2-n and dPV1-n) in the opposite direction by using RV/MV2-n as PVs.
3. Replicate (enable the copy mode setting for) RDR pairs (RV/MV2-n and PV1-n)

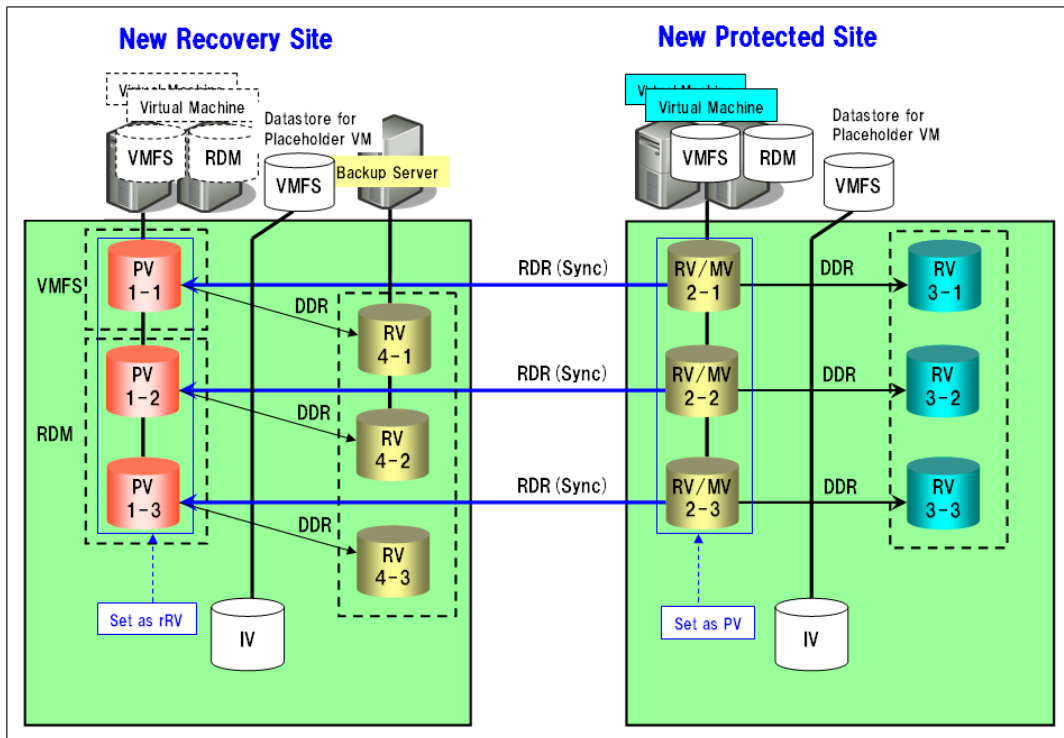


Figure 3-5: Pair Reconfiguration for Pattern 1-2 RDR (Synchronous) Operation



Reprotection after recovering VMware SRM will unpair RDR pairs, configure the pairs in the opposite direction, and replicate the pairs. Completing reprotection takes a long time because unpairing RDR pairs needs much time until the first replication ends. When Dynamic Personality Swap (DPS) is enabled, this function swaps the RDR pairs without unpairing them in recovering VMware SRM. Thus the reprotection time becomes shorter. This function is available only for recovery and reprotection testing.

- When a failure may occur in the protected site, do not recover VMware SRM with the DPS function enabled. Make sure the DPS function is disabled.
- In preparation for any failure in the protected site, it is recommended to disable the DPS function (default).
- The DPS function can be enabled before testing. Do not enable the DPS function while any recovery plan is running on VMware SRM or during reprotection. After the DPS function is set to enabled, make sure to perform a test.
- When the DPS function is used, Pattern 1-1, Pattern 1-2, Pattern 3-1 and Pattern 3-2 are supported. Pattern 2 is not supported.

- When the DPS function is used, before recovering VMware SRM, RDR pairs (PV1-n and RV/MV2-n) need to be in the replicated state.
- To enable the DPS function, change the “DPS” element in the oem.xml file stored in the VMware SRA installation folder on both servers where VMware SRA is installed in protected and recovery sites. Set “true” to enable the DPS function, while “false” to disable it. Be sure to restart the VMware SRM service in protected and recovery sites after the setting change.

[An example to enable the DPS function]

```
<AdapterCapabilities>
  <Features>
    <DPS>true</DPS>
  </Features>
</AdapterCapabilities>
```

(3) Pattern 2 RDR (asynchronous) operation

The SRA program reconfigures RDR pairs as shown below for re-protection.

- 1 Unpair RDR pairs (RV/MV2-n and RV/MV3-n).
- 2 Configure RDR pairs (RV4-n and PV1-n) by using RV4-n as PVs.
- 3 Replicate the RDR pairs (RV4-n and PV1-n) (in background copy mode).
- 4 Replicate DDR pairs (RV/MV3-n and RV4-n) in the new protected site (in synchronous mode).
- 5 Separate the DDR pairs (RV/MV3-n and RV4-n) in the new protected site.

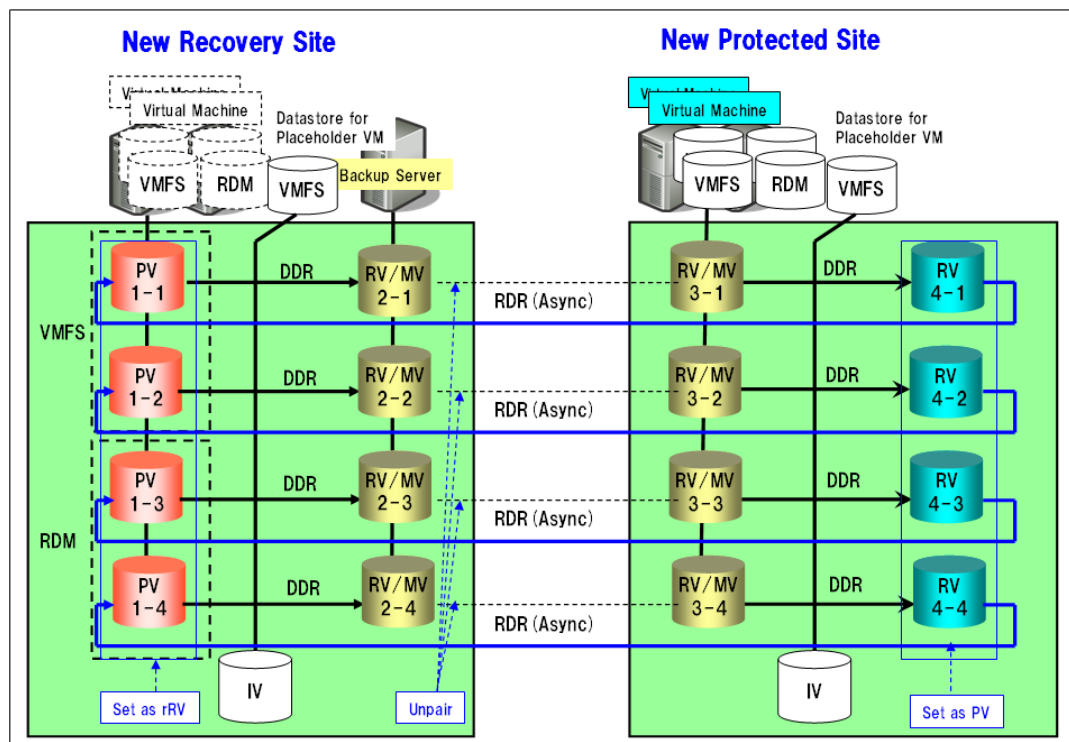


Figure 3-6: Pair Reconfiguration for Pattern 2 RDR (Asynchronous) Operation

(4) Pattern 3-1 RDR/DR (synchronous or semi-synchronous) operation

The SRA program reconfigures RDR pairs and AT groups as shown below for reProtection.

- 1 Delete RDR pairs (PV1-n and RV/MV2-n) from the AT group.
 - 2 Unpair RDR pairs (PV1-n and RV/MV2-n).
 - 3 Configure RDR pairs (RV/MV2-n and PV1-n) by using RV/MV2-n as PVs.
 - 4 Add the RDR pairs (RV/MV2-n and PV1-n) to the AT group.
 - 5 Replicate (enable the copy mode setting for) the AT group.
- * To apply semi-synchronous copy mode of order guarantee, perform the change after reProtection is finished.

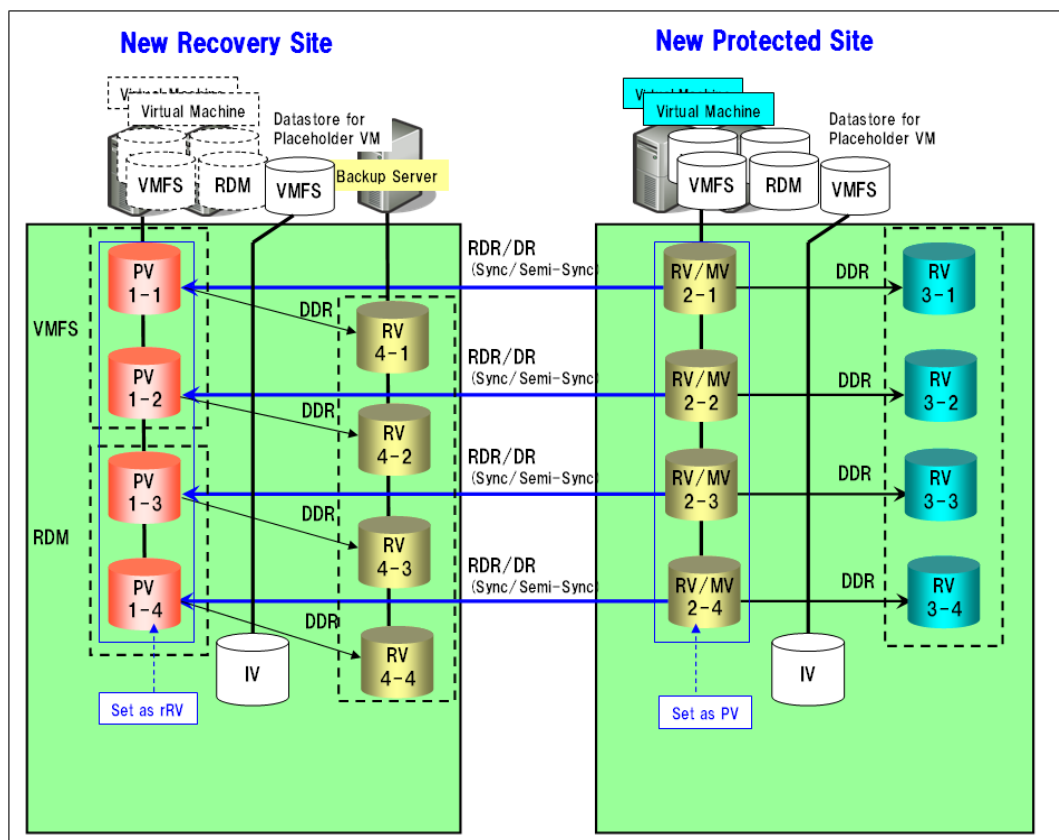


Figure 3-7: Pair and AT Group Reconfiguration for Pattern 3-1 RDR/DR (Synchronous or Semi-synchronous) Operation

(5) Pattern 3-2 RDR/DR (background copy mode of order guarantee) operation

The SRA program reconfigures RDR pairs and AT groups as shown below for reProtection.

- 1 Delete RDR pairs (PV1-n and RV/MV2-n), JNL-BUF and JBV from the AT group.
- 2 Unpair RDR pairs (PV1-n and RV/MV2-n).
- 3 Configure RDR pairs (RV/MV2-n and PV1-n) by using RV/MV2-n as PVs.
- 4 Add the RDR pairs (RV/MV2-n and PV1-n), JNL-BUF and JBV to the AT group.
- 5 Replicate (background copy mode of order guarantee) the AT group.

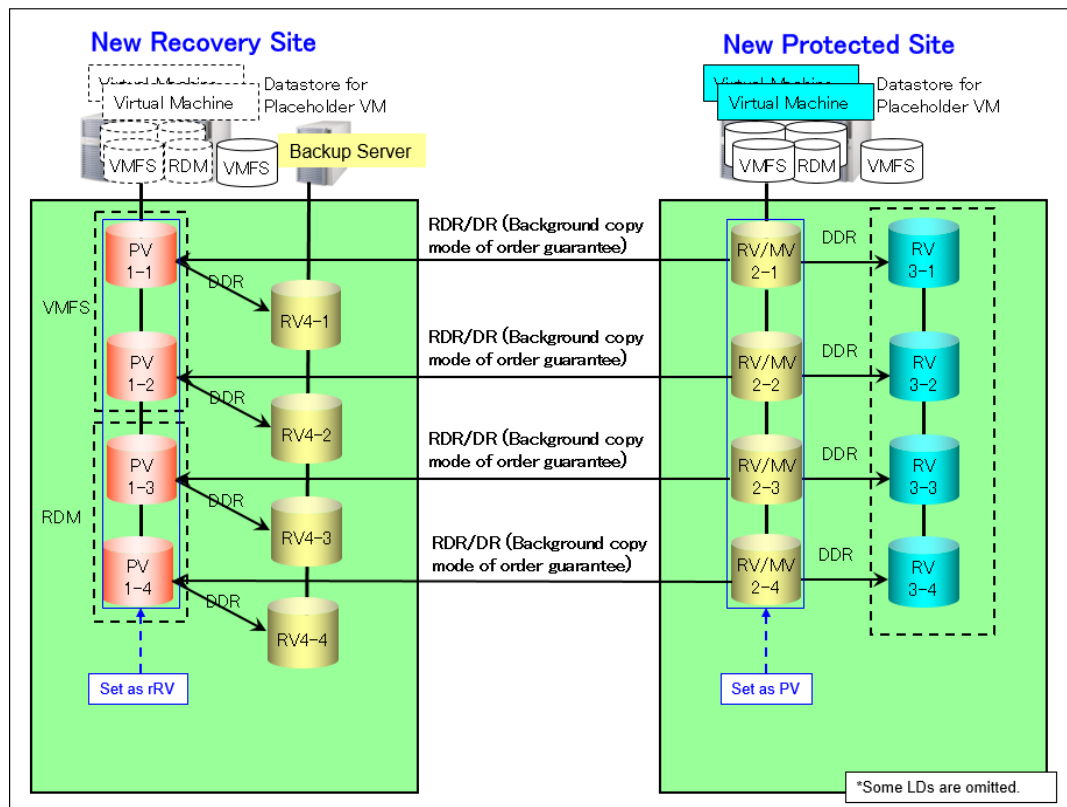


Figure 3-8: Pair and AT Group Reconfiguration for Pattern 3-2 RDR/DR (Background Copy Mode of Order Guarantee) Operation



In the environment where the background copy mode of order guarantee is used, the settings of JNL-BUF and JBV configured for each AT group are changed as follows by reproduction.

Example:

[Settings of JNL-BUF and JBV configured for each AT group before reproduction]

Protected site (Concentrator)	Recovery site (Distributor)
-------------------------------	-----------------------------

JNL-BUF: 30 MB	JNL-BUF: 20 MB
----------------	----------------

JBV name: JBV_A	JBV name: JBV_B
-----------------	-----------------

[Settings of JNL-BUF and JBV configured for each AT group after reproduction]

New recovery site (Distributor)	New protected site (Concentrator)
---------------------------------	-----------------------------------

JNL-BUF: 30 MB	JNL-BUF: 20 MB
----------------	----------------

JBV name: JBV_A

JBV name: JBV_B

* MV of an AT group is called “concentrator,” and RV of an AT group is called “distributor.”

If you want to change the settings JNL-BUF and JBV to other than the above, change the settings manually by using the `isMrc_atg` command.



Reprotection will replicate RDR pairs. You can change the copy mode for the replication.

- Pattern 1-1, Pattern 1-2, and Pattern 3-1 can specify the copy mode, while Pattern 2 cannot. The copy mode for Pattern 2 is fixed to Background. The copy mode for Pattern 3-2 is fixed to background copy mode of order guarantee.
- The copy mode for Pattern 1-1 and Pattern 1-2 is Synchronous by default. For Pattern 3-1, Semi-synchronous is set by default. The default copy mode for Pattern 3-2 is background copy mode of order guarantee.
- To set the copy mode, change the “CopyMode” element in the `oem.xml` file stored in the VMWare SRA installation folder on both servers where VMWare SRA is installed in protected and recovery sites. Set “sync” to change the copy mode to the Synchronous mode, “semi” to the Semi-synchronous mode, and “bg” to the Background mode. Be sure to restart the VMWare SRM service in protected and recovery sites after the setting change.

[An example to set Synchronous for Pattern 1-1 and Pattern 1-2, and Semi-synchronous for Pattern 3-1]

```
<AdapterCapabilities>
  <CopyMode>
    <Pattern1>sync</Pattern1>
    <Pattern3>semi</Pattern3>
  </CopyMode>
</AdapterCapabilities>
```


Appendix A Change LUN

Follow the procedure below to change the LUN of the protected site or recovery site.



It is necessary to change the LUN after cleanup of VMware SRM or reProtection is functioning normally.

- (1) Shut down the virtual machine on the device whose LUN is targeted for change (only when changing the LUN of the device in the protected site).
- (2) Delete the protection plan and protection group related to the device whose LUN is targeted for change.
- (3) Execute [Remove from Inventory] on the virtual machine to remove it from the target device (only when changing the LUN of the device in the protected site).
- (4) Unmount the datastore from the target device (only when changing the LUN of the device in the protected site).
- (5) Change the LUN of the target device.
- (6) Execute [Rescan Storage] to make VMware ESXi recognize the changed LUN.
- (7) Recreate a datastore for the target device (only when changing the LUN of the device in the protected site).
Select [Assign a new signature] to recreate a datastore.
- (8) Register the virtual machine to the inventory by using data of the datastore (only when changing the LUN of the device in the protected site).
- (9) Execute [DISCOVER DEVICES] to make VMware SRM recognize the changed device.
- (10) Recreate a protection group and protection plan.

Appendix B Troubleshooting

This section describes the messages output by SRA, and the action to take when a problem occurs.

- (1) A message, “No accessible disk array exists in the current site.” is reported.

Measure:

Verify that NEC Storage Manager at each site is properly monitoring the storage in the site, and remove the cause of error and try again.

- (2) A message, “The oem.xml file is not correct.” is reported.

Measure:

Verify that a file, oem.xml, is located in the SRA installation folder. If not, re-install SRA and try again.

- (3) A message, “Only users in administrators group can execute.” is reported.

Measure:

Log in as an administrator and try again.

- (4) A message, “This iSM Server version does not support required function.” is reported.

Measure:

Verify that NEC Storage Manager used at the sites is Ver 9.3 or later. If not, upgrade the version.

- (5) A message, “This ControlCommand version does not support required function.” is reported.

Measure:

Verify that ControlCommand used at the sites is Ver 9.3 or later. If not, upgrade the version.

- (6) A message, “The input xml file is not correct.” is reported.

Measure:

Collect the log and contact your maintenance staff.

- (7) A message, “No available logical disk exists in the current site.” is reported.

Measure:

Verify the following at each site, remove the cause of error and try again.

- NEC Storage Manager is installed.
- ControlCommand is installed.
- NEC Storage Manager is up and running.
- Logical disks are ready in the status.
- Logical disks are paired in one of Pattern 1, 2 or 3.

- (8) A message, “System call error has occurred.” is reported.

Measure:

Collect the log and contact your maintenance staff.

- (9) A message, “iSMview command error has occurred.” is reported.

Measure:

Verify the following at each site, remove the cause of error and try again.

- NEC Storage Manager is installed.
- ControlCommand is installed.
- NEC Storage Manager is up and running.

If none of the above is the cause, search the error message from replication operation log. By referring to the message handbook (IS010), identify the cause, take an action, and try again.

- (10) A message, “iSMrc command error has occurred.” is reported.

Measure:

Verify the following at each site, remove the cause of error and try again.

- NEC Storage Manager is installed.
- ControlCommand is installed.
- NEC Storage Manager is up and running.
- The state of RDR link is normal.
- The storage is not frozen.

If none of the above is the cause, search the error message from replication operation log. By referring to the message handbook (IS010), identify the cause, take an action, and try again.

- (11) A message, “iSMpairinfo command error has occurred.” is reported.

Measure:

Verify the following at each site, remove the cause of error and try again.

- NEC Storage Manager is installed.
- ControlCommand is installed.
- NEC Storage Manager is up and running.
- The state of RDR link is normal.
- The storage is not frozen.

If none of the above is the cause, search the error message from replication operation log. By referring to the message handbook (IS010), identify the cause, take an action, and try again.

- (12) A message, “RDR/DR reverse error has occurred.” is reported.

Measure:

Refer to the manuals (IS010, IS015 and IS027) and manually restore configurations of pairs and AT group prior to the failover, and try “Reprotection” again.

- (13) A message, “The protect group is not configured by all the logical disks that belong to the AT group.” is reported.

Measure:

Verify that all datastores (PVs) and the related RDMs (PVs) that are included in the AT group are registered with a single protection group, and try again.

- (14) Testing fails.

Measure:

Verify the following at each site, remove the cause of error and try again.

- The state of RDR link is normal.
- The storage is not frozen.
- AccessControl allows RVs used for recovery to access the recovery site.
- In RDR pairs, replication is synchronized or separation is completed.
- In RDR pairs, when separation is completed, RV access is set to ReadWrite.
- RV access settings for RVs are not set to forced mode.

- (15) A message, “Failed to create snapshot of replica device(Logical disk no)Logical disk name.” is reported.

Measure:

Timeout (24 hours (86400 seconds) by default) may have occurred while pairs are synchronized.

Try the same operations again.

If the error persists, customize the timeout information at both sites and try again.

- Select the [Site Pair] tab.
- On the left pane, Click [Advanced Settings].
- Click [Storage].
- Click [Edit] and change the value of storage.syncTimeout.

		take effect.
storage.enableSdrsTaggingRepair	<input checked="" type="checkbox"/>	Select the check box to allow SRM to repair missing/unwanted tags on replicated/protected datastores for Storage DRS compatibility.
storage.maxConcurrentCommandCnt	5	The maximum number of concurrent SRA operations.
storage.minDsGroupComputationInterval	0	Minimum interval in seconds between Datastore Group computations.
storage.querySyncStatusPollingInterval	30	Time interval in seconds between status updates for ongoing data synchronization operations.
storage.sdrsTaggingPollInterval	50	Time interval in seconds between the periodic Storage DRS tagging related operations.
storage.storagePingInterval	86400	Time interval in seconds between the periodic storage array re-discovery operations.
storage.syncTimeout	86400	Timeout in seconds for data synchronization operations.

キャンセル OK

- (16) A message, "Timed out (300 seconds)" is reported.

Measure:

SRM may not have finished the process within the default time (300 seconds), and have detected timeout.

Try the same operations again.

If the error persists, customize the timeout information at both sites.

- i) Select the [Site Pair] tab.
- ii) On the left pane, Click [Advanced Settings].
- iii) Click [Storage].
- iv) Click [Edit] and change the value of storage.commandTimeout.

vc-a.srm.sra - Edit Storage Settings

storage.attachTagsDelaySec	30	Time in seconds to wait before attempting to attach tags to recovered datastores.
storage.commandTimeout	300	Time interval in seconds during which an SRA update must be received or a timeout will be reported.
storage.datastoreMonitoringPollingInterval	30	Time interval in seconds between datastore monitoring related operations
storage.enableSdrsStandardTagCategoryCreation	<input checked="" type="checkbox"/>	Select the check box to allow SRM to automatically create Tag categories and 'Replicated' tag needed for Storage DRS compatibility. In Federated SSO setups, this flag should be disabled and the tags and tag categories should be manually created. Refer to documentation for more information.
storage.enableSdrsTagging	<input checked="" type="checkbox"/>	Select the check box to allow SRM to automatically create and attach tags on replicated/protected datastores for Storage DRS compatibility. Disabling this flag will delete all the tags and tag categories created by SRM and breaks Storage DRS compatibility. Enabling this flag after disabling it requires a server restart to take effect.
storage.enableSdrsTaggingRepair	<input checked="" type="checkbox"/>	Select the check box to allow SRM to repair missing/unwanted tags on replicated/protected datastores for Storage DRS compatibility.

キャンセル OK

- (17) A message, “Failed to sync data on replica devices. The operation timed out: 900 seconds” is reported.

Measure:

SRM may not have finished the process within the default time (900 seconds) and have detected a timeout.

Customize the timeout settings on both sites and try the same operation again.

- i) Open the <SRM Install Directory>/config/vmware-dr.xml file to edit as follows.
- ii) Search the following:


```
<RemoteManager>
  <DefaultTimeout>900</DefaultTimeout>
</RemoteManager>
```
- iii) Change the value of DefaultTimeout.
- iv) Save the vmware-dr.xml file.
- v) Restart the SRM service.

Appendix C How to Collect Information at Failure

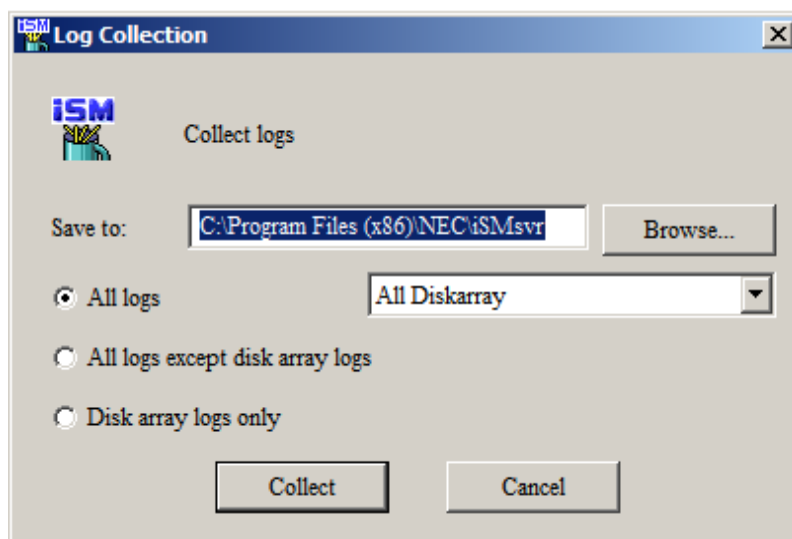
This section describes information required for investigating and resolving failures experienced during configuration or operation of the system and how to collect the information.

(1) Required information

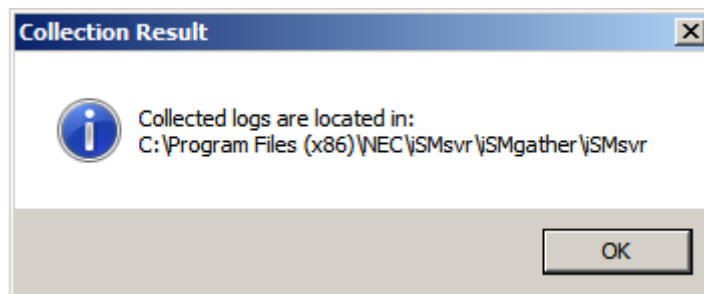
- iSMgather
Collect the information from the management servers where SRM is installed on both the protected site and the recovery site.
- iSMvolgather
Collect the information from the management servers where SRM is installed on both the protected site and the recovery site.
- SRM log file
Collect the information from the management servers where SRM is installed on both the protected site and the recovery site.

(2) Collecting iSMgather

- i) Log in to the management server as a member of Administrators group.
- ii) Click [Start], [Program] or [All programs], [Storage Manager Server], and [Server Menu].
- iii) Click [Server Menu] and [Log Collection].
 - Click [Browse] to change the saving destination.
 - Because all information needs to be collected, make sure that [All logs] is selected, and click [Collect].

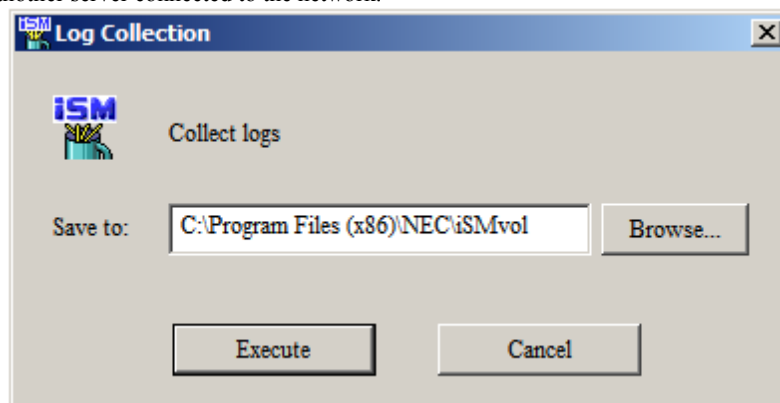


- iv) When collection is complete, the following message is displayed. Confirm that the folder exists and click [OK].

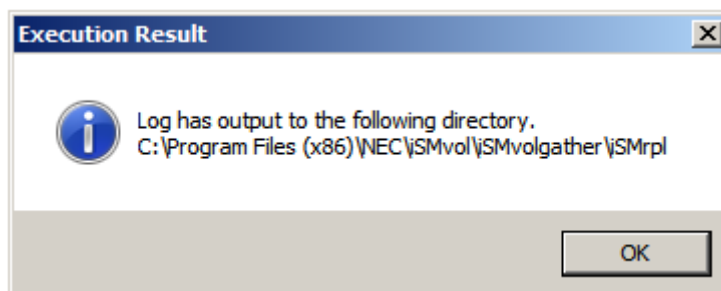


(3) Collecting iSMvolgather

- i) Log in to the management server as a member of Administrators group.
- ii) Click [Start], [Program] or [All programs], [ControlCommand], and [Difficulty Information Gather].
- Click [Browse] to change the saving destination.
 - Specify a folder in the server if you want to change the saving destination. Do not specify a folder in another server connected to the network.

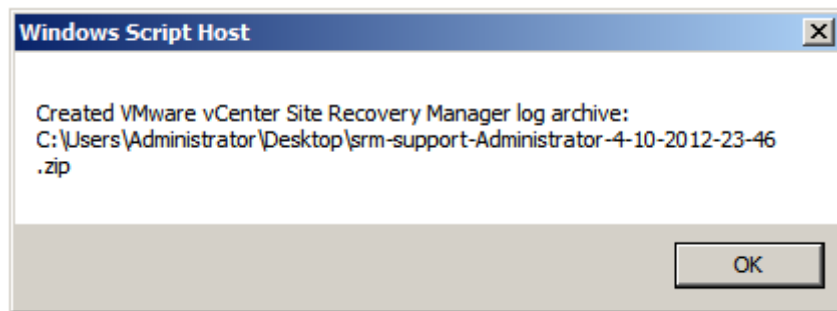


- iii) When collection is complete, the following message is displayed. Confirm that the folder exists and click [OK].



(4) Collecting SRM log file

- i) Log in to the management server as a member of Administrators group.
- ii) Select [Start], [Program] or [All programs], [VMware], [VMware Site Recovery Manager], and [Generate VMware Site Recovery Manager log bundle].
- iii) When collection is complete, the following message is displayed. Confirm that the folder exists and click [OK].



Appendix D Notes

This section describes notes.

(1) Reprotection

After a failover to recovery site in the RDR/DR (synchronous or semi-synchronous) operation, the replication copy mode should be synchronous mode to perform reprotect. If needed, change the copy mode manually.

- When to perform

When 4. Synchronize Storage is running in the [Recovery Steps] tab in the Recovery Plans window

- Procedure

Perform the following procedure on the iSM client replication window (ATgroup Information tab).

- Select a concentrator for the ATgroup for which synchronization is ongoing for reprotection, and click [ATgroup Forced Operation] and [ATgroup Forced Separate].
- When the forced separate is complete, select ATgroup Forced Operation and Recovery from Fault separation state.
- Select [ATgroup] and [ATgroup Replicate], select [Semi-synchronous] or [Background Copy] in the Copy Mode section and click [Replicate].

(2) Extent of datastore (VMFS)

Virtual machines that are stored in the extent of datastore (VMFS) cannot be protected. Perform protection after migrating the virtual machines to datastore (VMFS) that has a single logical disk (PV). For the RDR/DR environment, this will be supported in the next version.

(3) Timeout for the test and recovery functions

When test or recovery processes are ongoing, they may time out even if you set the timer for the maximum value (3600 seconds) in SRM. The processes, however, continue even a timeout occurs.

How to check:

- Check the status of DDR and RDR pairs from the iSM replication screen or by running ControlCommand. If any error is detected, take actions against it.
- If no error is detected and DDR for the protected site is “separation ongoing”, the test/recovery is successfully being processed. Wait for the DDR separation in the protected site to complete. When the separation is complete, try the test/recovery again.

(4) Timeout for reprotection

When reprotection is ongoing, it may time out even if you set the timer for the maximum value (3600 seconds) in SRM. The reprotection continues in the background even if a timeout occurs. If a timeout occurs, check whether there is any error. If no error is detected and copying (separation) is continuing, wait for a while for the copy (separation) to complete, and then start the SRM operation.

How to check:

- Check the status of DDR and RDR pairs from the iSM replication screen or by running ControlCommand.

- ii) If no error is detected and DDR pairs in the protected site are being separated, it means reProtection is successfully being processed. Wait for the separation to complete. When the separation is complete, reProtection is successfully completed. If an error is detected, remove the causing factor of the error.

(5) RDR pair status

For configuration patterns described in the document, replicated status, rather than separated status, is generally recommended for RDR pairs.

(6) Determining whether or not recovery from disaster is successful

If a disaster occurs, disaster recovery is necessary. If no error is detected throughout disaster recovery steps, you can determine the recovery is successful. When virtual machines in the recovery site successfully launch and start serving transactions normally, even though some errors are detected, the disaster recovery is considered to have succeeded. You can use transaction services in the recovery site.

(7) Reprotection after recovery from disaster

If a disaster occurs, disaster recovery is necessary. When the recovery is successfully completed, transaction services run on the virtual machines in the recovery site. After the protected site is restored, the recovery site must be reprotected so that it will be a new protected site. Reprotect the restored site manually because the statuses of devices (such as configuration of LDs and pairs) in the restored site is unknown.

How to perform reProtection manually:

- i) Delete the recovery plan and protection groups by using SRM Client.
- ii) From the iSM replication screen or by running ControlCommand, separate (or forcefully separate) paired RVs in the recovery site to unpair (or forcefully unpair) them. When the separation and unpairing succeed, the RVs in the recovery site change to IVs.
- iii) If there are MVs of the RDR pairs in the protected site, separate the pairs (or forcefully separate) the MVs to unpair (or forcefully unpair) them. When the separation and unpairing succeed, the MVs in the protected site changes to IVs. If there is no MVs of RDR pairs (due to reasons such as replacement of a device in the protected site), create the same logical disks (same capacity and format) as the logical disks for transactions in the recovery site and set access control correctly. And then perform scanning again on the ESX server to detect logical disks.
- iv) Reconfigure the pair environment in the opposite direction from the recovery site to the protected site as described in 3.4, “ReProtection.”
- v) Reconfigure the SRM environment according to the description in 2.6, “VMware Site Recovery Manager Setting.”
- vi) Run a test for the new recovery plan. If the test succeeds, the manual reProtection is complete successfully.

(8) Running two or more recovery plans at the same time

The following combinations of recovery plans at the same time are impractical:

- Reprotection and testing
- Reprotection and cleanup
- Reprotection and recovery

- Reprotection and reprotection
- (9) Monitoring from NEC Storage Manager
- To start a recovery plan, the monitoring status of the disk array under NEC Storage Manager's administration needs to show "Running".
- (10) Logical disk name
- A logical disk name must be unique in the system.