

# Dell EMC™ PowerMax™ eNAS File Auto Recovery with SRDF/S

Version 8.1.13.35

For Dell EMC PowerMax and VMAX All Flash

REVISION 01

Copyright © 2015-2018 Dell Inc. or its subsidiaries All rights reserved.

Published May 2018

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners.  
Published in the USA.

Dell EMC  
Hopkinton, Massachusetts 01748-9103  
1-508-435-1000 In North America 1-866-464-7381  
[www.DellEMC.com](http://www.DellEMC.com)

# CONTENTS

<b>Figures</b>		<b>7</b>
<b>Tables</b>		<b>9</b>
	<b>PREFACE</b>	<b>11</b>
<b>Part 1</b>	<b>File Auto Recovery</b>	<b>15</b>
<b>Chapter 1</b>	<b>Introduction</b>	<b>17</b>
	eNAS File Auto Recovery.....	18
	Terms used in this document.....	19
	System requirements.....	21
	Restrictions and limitations.....	22
	User interface choices.....	24
<b>Chapter 2</b>	<b>Concepts</b>	<b>25</b>
	FAR logical entities.....	26
	Bonded mapped pool.....	26
	Standby pool on a destination eNAS system.....	26
	FAR-replicable VDM.....	26
	Use cases.....	28
<b>Chapter 3</b>	<b>FAR best practices</b>	<b>29</b>
	Configuration.....	30
	VDM configuration.....	30
	LUN configuration.....	30
	Disaster recovery operations.....	31
	Upgrade use cases.....	31
<b>Chapter 4</b>	<b>Setting up FAR</b>	<b>33</b>
	FAR setup information.....	34
	Initial setup for FAR.....	35
	Configure Control Station-to-Control Station communication.....	37
	Enable the FAR service.....	39
<b>Chapter 5</b>	<b>Configuring FAR</b>	<b>41</b>
	Start the FAR service.....	42
	Create data LUNs for NAS resources.....	43
	Create a FAR-replicable VDM.....	45
	Create a file system on the bonded pool.....	47
	Create the first file system checkpoint on the bonded pool.....	48
	Create a network interface for a FAR-replicable VDM.....	49
	Create CIFS shares for each file system on the bonded pool.....	51
	Create a FAR session.....	52

	Start a FAR session.....	54
	Migrate Data Mover configurations.....	55
	Configure CIFS CA support.....	56
	Configure for NFS I/O transparency in FAR session.....	59
<b>Chapter 6</b>	<b>Managing FAR sessions</b>	<b>61</b>
	Reverse operation.....	62
	Performing reverse on a FAR session.....	62
	Failover operation.....	65
	Performing failover on a FAR session.....	65
	Performing clean on a FAR session.....	68
	List FAR service information.....	70
	Show information for FAR service.....	71
	Disable the FAR service.....	72
	Modify a VDM from FAR-replicable to non-FAR-replicable.....	73
	Modify a VDM from non-FAR-replicable to FAR-replicable.....	74
	Show information for a FAR-replicable VDM.....	75
	Delete a FAR-replicable VDM.....	76
	List FAR session information.....	77
	Show FAR session information.....	78
	Delete a FAR session.....	79
	Extend bonded pool with FAR session.....	80
	Modify network devices.....	80
	Updating VNX OE software.....	82
	FAR Health Check.....	82
	Performing FAR Health Check.....	83
<b>Chapter 7</b>	<b>Managing Preserve ReplicatorV2 sessions for FAR.</b>	<b>85</b>
	Preserve ReplicatorV2 sessions for FAR.....	86
	Best practices for Preserve RepV2 sessions.....	86
	Enable Preserve RepV2 sessions for FAR.....	86
	Create a ReplicatorV2 session on a FAR replicable VDM.....	87
	Show Preserve RepV2 session status.....	88
	Disable Preserve RepV2 sessions for FAR.....	88
	Restore ReplicatorV2 sessions.....	89
	Handle ReplicatorV2 sessions when Failover/Restore of FAR session is performed in FARM.....	90
<b>Chapter 8</b>	<b>FAR service checklists</b>	<b>93</b>
	Enable FAR service checklist.....	94
	FAR session checklist.....	95
<b>Chapter 9</b>	<b>Troubleshooting FAR</b>	<b>97</b>
	Retrieve information from log files.....	98
	Error messages.....	99
	Troubleshooting scenarios.....	99
<b>Part 2</b>	<b>File Auto Recovery Manager</b>	<b>103</b>
<b>Chapter 10</b>	<b>Installing FARM</b>	<b>105</b>
	Installation Requirements.....	106

	Installing FARM.....	107
<b>Chapter 11</b>	<b>FARM operations</b>	<b>109</b>
	Configure operations.....	110
	Prerequisites.....	110
	The File Auto Recovery Manager Configuration wizard.....	110
	Configuring FARM.....	110
	Resetting FARM.....	111
	Management operations.....	113
	Configure a synchronous replication session's failover policy.....	113
	Configure a synchronous replication session's failover priority.....	114
	Select VDM IP addresses to monitor.....	114
	Start the FARM service.....	115
	Stop the FARM service.....	115
	Manually failover a synchronous replication session.....	116
	Cleaning synchronous replication sessions.....	116
	Manually reverse a synchronous replication session.....	117
	Manually restore a synchronous replication session.....	117
	Collecting logs.....	117
	Discover monitored objects.....	118
	Check status.....	118
	Show synchronous replication status.....	119
	Viewing the eNAS log.....	119
	VDM use cases.....	119
<b>Chapter 12</b>	<b>Uninstalling FARM</b>	<b>121</b>
	Uninstall FARM.....	122
<b>Chapter 13</b>	<b>Additional FARM information</b>	<b>123</b>
	FARM limitations.....	124
	Best practices.....	124
	VDM state and status information.....	125
	Event status/level.....	126
	VDM event list.....	127
	Events.....	127
	FARM Environment Data Collect Sheet.....	128
	Refreshing session state information in FARM.....	128
<b>Chapter 14</b>	<b>Troubleshooting FARM</b>	<b>131</b>
	Troubleshooting sequence.....	132
	Log and configuration files.....	133
	Collecting logs.....	133
	FARM: Output codes.....	134
	FARM protection/Failover prevention.....	135
	Frequently asked questions and additional information.....	135
	Troubleshooting checklist.....	137
	Recovering FARM when it is not responding.....	139

## CONTENTS

# FIGURES

1	Example of site replication architecture.....	19
---	---	----

FIGURES

# TABLES

1	Typographical conventions used in this content.....	12
2	FAR setup planning sheet.....	34
3	FAR Health Checks .....	82
4	FAR service setup checklist.....	94
5	FAR session creation checklist.....	95
6	Monitored events.....	113
7	Errors, causes, and remedies.....	118
8	Event Status/Level summary.....	126
9	Frequently asked questions.....	135
10	FARM troubleshooting.....	137

TABLES

# PREFACE

As part of an effort to improve its product lines, Dell EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your Dell EMC representative if a product does not function properly or does not function as described in this document.

---

## Note

This document was accurate at publication time. New versions of this document might be released on Dell EMC Online Support (<https://support.emc.com>). Check to ensure that you are using the latest version of this document.

---

## Purpose

This document explains how to configure and manage eNAS File Auto Recovery with SRDF/S.

## Audience

This document is intended for storage administrators who need to configure and manage eNAS File Auto Recovery with SRDF/S.

## Related documentation

The following Dell EMC publications provide additional information:

- *PowerMax eNAS Release Notes*  
Describes new features and identifies any known functionality restrictions and performance issues that may exist with the current version and your specific storage environment.
- *PowerMax eNAS Command Line Reference*  
Provides a reference for command line users and script programmers by describing the eNAS command syntax, error codes, and parameters.
- *Using SRDF/S with VNX for Disaster Recovery*  
Explains how to configure and manage SRDF/S.
- *Dell EMC VNX Command Line Interface Reference for File*  
Explains the command used to configure and manage a Dell EMC file storage system.
- *Managing Volumes and File Systems on VNX Manually*  
Explains how to create and aggregate different volume types into usable file system storage.
- *Using VNX SnapSure*  
Explains how to use Dell EMC SnapSure to create and manage checkpoints.
- *Configuring Virtual Data Movers on VNX*  
Explains how to configure and manage VDMs on a file storage system.
- *Configuring CIFS on VNX*  
Explains how to configure and manage NFS.
- *Parameters Guide for VNX for File*  
Explains how to view and modify parameters and system settings.

### Special notice conventions used in this document

Dell EMC uses the following conventions for special notices:



Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

---



Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

---



Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

---



Addresses practices not related to personal injury.

---

#### Note

Presents information that is important, but not hazard-related.

---

### Typographical conventions

Dell EMC uses the following type style conventions in this document:

**Table 1** Typographical conventions used in this content

<b>Bold</b>	Used for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
<i>Italic</i>	Used for full titles of publications referenced in text
Monospace	Used for: <ul style="list-style-type: none"> <li>• System code</li> <li>• System output, such as an error message or script</li> <li>• Pathnames, filenames, prompts, and syntax</li> <li>• Commands and options</li> </ul>
<i>Monospace italic</i>	Used for variables
<b>Monospace bold</b>	Used for user input
[ ]	Square brackets enclose optional values
	Vertical bar indicates alternate selections - the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

---

### Where to get help

Dell EMC support, product, and licensing information can be obtained as follows:

**Product information**

For documentation, release notes, software updates, or information about Dell EMC products, go to Dell EMC Online Support at <https://support.emc.com>.

**Technical support**

To open a service request through the Dell EMC Online Support (<https://support.emc.com>) site, you must have a valid support agreement. Contact your Dell EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.

**Your comments**

Your suggestions help us improve the accuracy, organization, and overall quality of the documentation. Send your comments and feedback to:

[VMAXContentFeedback@emc.com](mailto:VMAXContentFeedback@emc.com)



# PART 1

## File Auto Recovery

This section describes how to install and use File Auto Recovery.

Chapters include:

[Chapter 1, "Introduction"](#)

[Chapter 2, "Concepts"](#)

[Chapter 3, "FAR best practices"](#)

[Chapter 4, "Setting up FAR"](#)

[Chapter 5, "Configuring FAR"](#)

[Chapter 6, "Managing FAR sessions"](#)

[Chapter 7, "Managing Preserve ReplicatorV2 sessions for FAR. "](#)

[Chapter 8, "FAR service checklists"](#)

[Chapter 9, "Troubleshooting FAR"](#)



# CHAPTER 1

## Introduction

This chapter introduces File Auto Recovery.

Topics include:

- [eNAS File Auto Recovery](#)..... 18
- [Terms used in this document](#)..... 19
- [System requirements](#)..... 21
- [Restrictions and limitations](#)..... 22
- [User interface choices](#)..... 24

## eNAS File Auto Recovery

Introduced in the HYPERMAX OS 5977.691.684, File Auto Recovery (FAR) allows you to manually failover or move a Virtual Data Mover (VDM) from a source eNAS system to a destination eNAS system. The failover or move leverages block-level Symmetrix Remote Data Facility (SRDF) synchronous replication, so it invokes zero data loss in the event of an unplanned operation. This feature consolidates VDMs, file systems, file system checkpoint schedules, CIFS servers, networking, and VDM configurations into their own separate pools. This feature works for a disaster recovery where the source is unavailable. For recovery support in the event of an unplanned failover, an option is available to clean up the source system and make it ready as a future destination..

This document also describes the Dell EMC File Auto Recovery Manager (FARM). This optional application allows you to start failover and reverse operations manually. FARM also allows you to automatically failover a selected sync-replicated VDM on a source eNAS system to a destination eNAS system. FARM does it by allowing you to monitor sync-replicated VDMs and to trigger automatic failover based on Data Mover, File System, Control Station, or IP network unavailability that would cause the NAS client to lose access to data. For more information about FARM, refer to [File Auto Recovery Manager](#) on page 103.

**⚠ WARNING**

**Before changing a FARM monitored configuration, you must first stop the FARM Services. When changes are completed, manually discover the monitored configurations to pick up the changes, and then restart the FARM Service.**

---

**NOTICE**

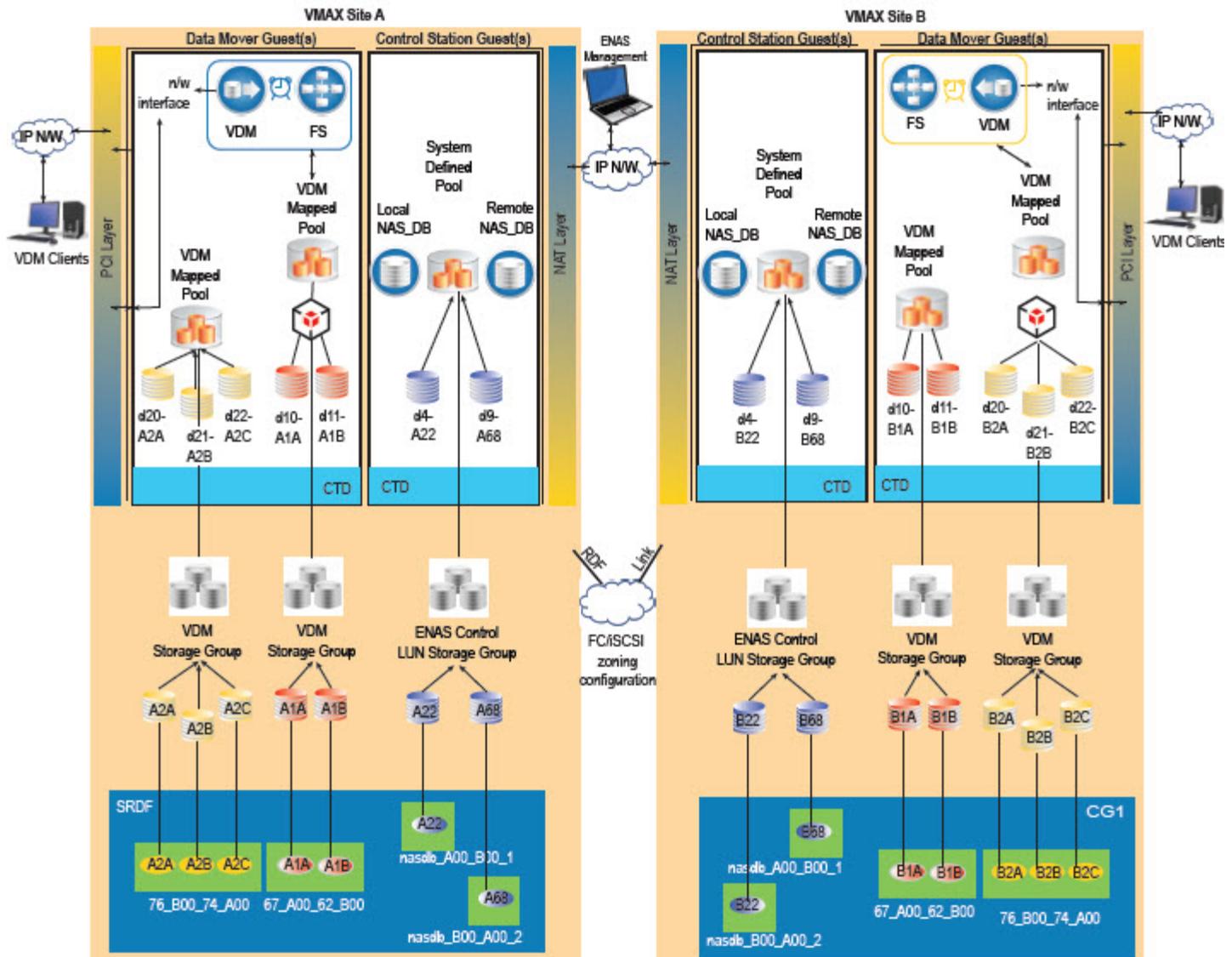
FARM and FAR were previously known as AFM and VDM Sync, respectively. Because of this, you may find occurrences of AFM and VDM Sync in the software. Any such occurrences will be updated in a future release of the product.

---

## Terms used in this document

This document uses the terms *primary* and *secondary* to refer to the two sites in a replication configuration. In practice, you will likely use location-based names as shown in the following figure.

**Figure 1** Example of site replication architecture



The terms used in this document are:

- **Primary site** - This is the production site for the eNAS storage and is normally active. Other terms sometimes used to describe the primary site include: source, local site, primary cluster, or production site.
- **Secondary site** - This is the replication site for the eNAS storage and is normally inactive (standby mode) for a given FAR session. If a failover occurs, the secondary site becomes active until the primary site is recovered and a reverse

occurs. Other terms used to describe the secondary site include: target, destination, remote site, secondary cluster, or disaster recovery (DR) site.

## System requirements

File Auto Recovery with SRDF/S requires the following software, hardware, and network configurations:

For software:

- The source and destination eNAS systems must use the same operating environment (OE) for File version 8.1.7 or later. Also, Unisphere (for VNX) should be installed, and the SRDF and SnapSure licenses must be installed and enabled. For this feature, eNAS with SRDF replicates at the VDM level. This includes IP interfaces, CIFS/NFS Servers, VDM/file system log files, file systems, snaps and snap schedules with a VDM.
- All file systems must use Split Log.
- Checkpoints (SavVol) must be on the same pool as the production file system (PFS).
- The Solutions Enabler option “SYMAPI\_ALTERNATE\_ACCESS\_ID” must be disabled in the Solution Enabler Config file ‘/nas/symapi/config/options’ for the syncrep operations to proceed without failing an SRDF operation.

For hardware:

- Two eNAS-configured arrays.
- SRDF/S Hardware link is established in the switch topology between the two eNAS-configured arrays. In addition, the RDF links should be configured in High Availability (HA) mode to guard against link failures. For more information, refer to the following documents available on Dell EMC Online Support:
  - *Using SRDF/A with VNX*
  - *Using SRDF/S with VNX for Disaster Recovery*
  - *Symmetrix Remote Data Facility Product Guide*

For network:

- At a minimum, IP network for the Control Stations of the source eNAS system and the Control Stations of the destination eNAS system.
- NAT layers should be configured and the Control Stations should be able to reach each other.
- LAN or WAN links for communication between the source and destination Control Stations. Ensure that the connections are configured for High Availability (HA).

## Restrictions and limitations

The following restrictions and limitations apply to FAR:

- One and only one FAR-replicable VDM is allowed on one bonded pool (there is a 1:1 mapping between the FAR-replicable VDM and its bonded pool).
- To get the same expected performance, you should use the same storage groups between each of the eNAS systems.
- FAR with SRDF and VNX Replicator technology can co-exist on the same system.
- File systems included in the FAR with SRDF feature can now be part of RepV2 IP replication in a concurrent model.
- FAR service and sessions are supported only between two eNAS systems with SRDF systems configured.
- The maximum number of FAR sessions tested on two eNAS systems with SRDF systems configured and qualified is six. For a properly load balanced FAR setup, three sessions per site is recommended. More FAR sessions can be configured (up to a maximum of 128 per setup).
- NDMP backup on file systems on a pool is supported; however, the backup may be stopped when reverse/failover occurs. After a reverse/failover, the full mount paths of the file systems will be changed. To make NDMP backup work again, the NDMP configuration on backup software needs to be changed accordingly.
- An IP replication session created on a FAR-replicable VDM or any file system on it (as either source or destination) is not allowed. As a result, since `nas_migrate` uses replication sessions, a FAR-replicable VDM cannot be migrated using `nas_migrate`. (A workaround for this is to modify the VDM from FAR-replicable to non-FAR-replicable and then migrate the VDM.)
- Only a split-log VDM or file system contained in a FAR session is supported.
- Only `uxfs` and `rawfs` that are created on a pool are supported.
- Common Log File Systems are not supported. You can only transfer common-log file system to split-log file system by using host-based copy.
- Temporarily unmounted file systems and checkpoints will become mounted after a reverse or failover operation on the destination.
- Temporarily unloaded VDMs will become loaded after a reverse or failover operation on the destination.
- For a VDM under a FAR session, you cannot mount the VDM's file systems or checkpoints to another Data Mover or VDM.
- File systems and checkpoints on a FAR-replicable NAS pool mounted to a Data Mover or other VDM than the one created on the FAR-replicable NAS pool are not allowed.
- The replication of Data Mover configurations or Cabinet level service are not included in FAR.
- If the top of the FSID range is reached and after more VDMs/file systems/checkpoints are created, an FSID conflict may occur during reverse or failover. An FSID range of no less than 8192 should be enforced. `nas_checkup` will identify any potential FSID conflict for all active VDMs under FAR sessions on the system.
- The FSID range on source and destination eNAS systems must not overlap.

- If the FAR service or session status is not `in_sync` when the disaster occurs, the system cannot guarantee the success of failover on the FAR session.
- A period of data unavailability (DU) time will occur during a FAR session reverse operation. The actual DU time depends on the number of file systems or checkpoints existing on the FAR-replicable NAS pool.
- After a disaster occurs on the source site, DU will start. When a FAR session failover is executed, the DU will continue till the NFS exports/shares are restored on the destination site.
- After failover, if the original active Data Mover for the FAR session still works, it may run into a rolling panic because the underlying LUNs become read-only. You need to clean the FAR sessions (using `nas_syncprep -Clean -All`) to return it to a healthy state and perform a DM failback for the DM standby to be ready for any subsequent server panics.
- The HomeDirectory feature does not support Continuous Availability (CA) capability. Keep this in mind when you configure CIFS CA support for FAR.
- Before creating a FAR session, and starting a failover or reverse, you must manually migrate Data Mover configuration and Cabinet level service items. [Migrate Data Mover configurations](#) on page 55 provides more information.

## User interface choices

This document describes how to configure SRDF and integrate it with eNAS systems by using the eNAS CLI on the Control Station using SSH. You cannot use Unisphere (for VNX) to configure SRDF.

You can use Unisphere (for VNX) to view the storage pools and disk types used in the SRDF configuration. You also can use Unisphere (for VNX) to manage storage objects, such as file systems that reside on the source VDM.

# CHAPTER 2

## Concepts

This chapter explains the FAR logical entities and highlights some use cases.

Topics include:

- [FAR logical entities](#)..... 26
- [Use cases](#).....28

## FAR logical entities

In order to enforce the restrictions and limitations that apply to FAR (see [Restrictions and limitations](#) on page 22), the following entities are specific to a FAR environment:

- Bonded mapped pool
- Standby pool (destination site)
- FAR-replicable VDM

### Bonded mapped pool

A bonded mapped pool must meet the following criteria:

- It must be a mapped pool.
- Its members must be disk volumes.
- It must have only one FAR-replicable VDM rootfs on it.
- It cannot have MGFS on it.
- All file systems and checkpoints on it must be either unmounted or mounted on its FAR-replicable VDM.
- All file systems on it must be split-log file systems.
- File systems on it must not have checkpoints (SavVols) on another pool.
- Checkpoints (SavVol) on it must be on the same pool as their Production File Systems (PFSs).
- No ID of a file system and checkpoint on it conflicts between the source and destination systems.
- No file systems, checkpoints, or VDM on it are not used as a source side or a destination side of a Replication V2 session.
- No file Systems or checkpoints on it use space other than the current storage pool.

### Standby pool on a destination eNAS system

The destination of any FAR configuration must have a standby pool that meets the following criteria:

- Have user-defined file storage pools for each FAR session that is to be created. Only a single mapped pool can be allocated per FAR session.
- All volumes within the mapped pool must be disk volumes (dvols).
- The disk volumes in the membership must match in number and size with those in the FAR-replicable NAS pool on the active system under the FAR session.
- It must not be in use.

### FAR-replicable VDM

A FAR-replicable VDM must meet the following criteria:

- It is the only VDM on the bonded mapped pool. This criteria must be met before creating or modifying a VDM. This feature restricts one VDM per mapped pool by design.

- It is created with a special flag on one non-FAR-replicable NAS pool. After creation the pool becomes a FAR-replicable NAS pool and keeps this status throughout the whole life-cycle of the VDM. It either has been created with the `-syncreplicable` flag enabled or modified to enable the `-syncreplicable` flag. After creation or modification, the associated pool will become a bonded mapped pool and will maintain this status as long as there is a VDM with a `-syncreplicable` flag enabled in it.
- All file systems (including the VDM rootfs) mounted on it must be split-log file systems.
- All file systems (including the VDM rootfs) and checkpoints mounted on it must be created on its bonded mapped pool.

## Use cases

FAR using SRDF can be used in the following cases:

- Disaster recovery (DR) at the VDM level
  - Human error
  - Power outages
  - Environmental (for example, a flood or storm)
- Maintenance (that is, planned failover)
- Load balancing
- More efficient use of hardware (a VDM-level DR solution does not require standby Data Mover hardware like a Cabinet-level DR solution does)

# CHAPTER 3

## FAR best practices

This chapter describes the best practices to consider for more consistent and stable behavior. Topics include:

- [Configuration](#)..... 30
- [VDM configuration](#)..... 30
- [LUN configuration](#)..... 30
- [Disaster recovery operations](#)..... 31
- [Upgrade use cases](#)..... 31

## Configuration

Consider the following recommendations before configuring FAR:

- Configure HA RDF link connections between the source and destination array for faster block replication.
- Configure both NAT IP addresses in the CS-CS interconnect (`nas_cel` configuration) for more reliability and resiliency in case of NAT failures.
- If the NAT IP of any site in the VDM configuration is changed, you must update it at the other site using the command:

```
nas_cel -modify { <cel_name> | id=<cel_id> } { [-passphrase
<passphrase>] [-name <new_name>] [-ip
<ipaddr>[,<ipaddr>,...]] }
```

This ensures that the FAR session operations will not fail and further avoid the unnecessary DU situation.

- Configure NTP servers between the source and destination eNAS systems to prevent time skew faults (note that the time skew between the systems can be at most 10 mins). Note that disaster recovery operations will fail if there is a time skew error. If this happens, an Administrator must correct the skew before retrying the failed operation.
- Configure FARM (per active side; that is, two FARMs for both sides together) for automated disaster detection and DR initiation.
- Configure Fail Safe Network (FSN) devices for network resiliency.
- Perform a FAR Health Check prior to performing VDM failover or reverse operations. This will enable you to take proactive measures to help minimize the chances that an unplanned failover or reverse operation will fail. [FAR Health Check](#) on page 82 provides more information.

## VDM configuration

Consider the following recommendations before configuring VDMs for FAR:

- A maximum of 6-7 syncreplicable VDMs are recommended per FAR setup for best performance.
- Deploy all the file systems on VDMs instead of DMs.
- Run a modify operation to consume any newly attached VDM interfaces on the destination side; and eventually mark them with the DR parameters. Failing to do so will cause a failover/reverse to fail due to the lack of newer interfaces on the destination side.

## LUN configuration

Consider the following recommendations before configuring LUNs for FAR:

- Configure an optimal number of volumes for given requirements per VDM session. For example, ten 100 GB volumes is better than one hundred 10 GB volumes.
- For the least amount of I/O latency, use EFD volumes for FAR sessions.

## Disaster recovery operations

Consider the following recommendations before performing disaster recovery operations:

- Periodically perform a FAR Health Check, say as a cron job, to monitor the health of FAR sessions. This will enable you to take proactive measures to help minimize the chances that an unplanned failover or reverse operation will fail. [FAR Health Check](#) on page 82 provides more information.
- Perform a FAR Failover operation when the source site is NOT available. Failing to perform this operation when the source site is unavailable will cause the source side Data Movers to panic.
- After a FAR Failover operation, always perform a Clean All operation for faster and stable cleanup of all the failed over sessions on the original source and start synchronizing from the new source.
- DO NOT perform NAS\_DB operations on the source side while Failover/Reverse operations are in progress.

## Upgrade use cases

Consider the following before upgrading pre-configured FAR:

- Always ensure that the FAR Refresh All operation is issued after upgrading to eNAS build 8.1.11.282 (obtainable through the Epack process) or higher - if not already run. Failing to perform this operation will eventually lead to an IP-based FAR Split brain and/or R1 DM panic.



# CHAPTER 4

## Setting up FAR

This chapter explains how to setup the FAR environment between two eNAS systems.

Topics include:

- [FAR setup information](#)..... 34
- [Initial setup for FAR](#)..... 35
- [Configure Control Station-to-Control Station communication](#)..... 37
- [Enable the FAR service](#)..... 39

## FAR setup information

Use the following planning sheet when setting up your FAR environment.

**Table 2** FAR setup planning sheet

<b>What you specify</b>	<b>Source-site information</b>	<b>Destination-site information</b>
Control Station name		
Control Station NAT IP addresses		

## Initial setup for FAR

To setup FAR between two eNAS systems using SRDF, follow this sequence of tasks:

### Note

For reference, the complete set of Dell EMC eNAS customer publications is available on Dell EMC Online Support (<https://support.EMC.com>). After logging in to the website, click the Support by Product page to locate information for the specific product or feature required.

### Procedure

1. Install and configure the source and destination eNAS systems. Refer to Dell EMC VNX2 customer publications available on Dell EMC Online Support (<https://support.EMC.com>).
2. From either the tools guest or an external host running Solutions Enabler, configure additional SRDF Control LUNs. While creating the LUNs, consider the LUN sizes listed in the next step.
3. Map the new SRDF Control LUNs to control stations CS-0 and CS-1 at LUN positions 0x0006, 0x0007, 0x0008, and 0x0009. The following lists the SRDF Control LUN sizes:
  - Control LUN 6 = 12200 cyl
  - Control LUN 7 = 6197 cyl
  - Control LUN 8 = 1108 cyl
  - Control LUN 9 = 2216 cyl

For example, to create and map Control LUNs to CS-0 and CS-1:

```
$ cat /tmp/add_rdf_map.bin
create dev count=1, size=12200 cyl, emulation=CELERRA_FBA, config=TDEV, mapping to
dir 1d:34 lun=6, mapping to dir 2d:34, lun=6;
create dev count=1, size=6197 cyl, emulation=CELERRA_FBA, config=TDEV, mapping to dir
1d:34 lun=7, mapping to dir 2d:34 lun=7;
create dev count=1, size=1108 cyl, emulation=CELERRA_FBA, config=TDEV, mapping to dir
1d:34 lun=8, mapping to dir 2d:34 lun=8;
create dev count=1, size=2216 cyl, emulation=CELERRA_FBA, config=TDEV, mapping to dir
1d:34 lun=9, mapping to dir 2d:34 lun=9;

$ symconfigure -sid 352 -f /tmp/add_rdf_map.bin commit

A Configuration Change operation is in progress. Please wait...
..
   New symdevs: 000C3:000C6 [TDEVs]
   Terminating the configuration change session.....Done.

The configuration change session has successfully completed.
```

For example, to map existing Control LUNs to CS-0 and CS-1:

```
$ symconfigure -sid 352 -cmd "map dev 000C3 to dir 1d:34, lun=6;" commit -nop
$ symconfigure -sid 352 -cmd "map dev 000C3 to dir 2d:34, lun=6;" commit -nop
```

Use similar commands to map Control LUNs at positions 0x0007, 0x0008, and 0x0009.

4. Add the new SRDF Control LUNs to the masking view of all the Data Movers. To perform this operation on an array running HYPERMAX OS 5977 Q2 2016, you must first remove or change the service level set on the EMBEDDED\_NAS\_DM\_SG storage group as follows:

- a. List the service levels supported on the array:

```
/nas/symcli/bin/symcfg -sid xxx list -slo
```

- b. Determine the name of the service level associated with the EMBEDDED\_NAS\_DM\_SG storage group:

```
/nas/symcli/bin/symmsg -sid xxx show EMBEDDED_NAS_DM_SG
```

- c. Determine if the service level from step b is listed in the results from step a. If it is listed, skip to step e. If it is not listed, continue with step d.

- d. Do one of the following:

Change the service level associated with EMBEDDED\_NAS\_DM\_SG to one of those listed in step a by entering the following: `/nas/symcli/bin/symmsg -sid xxx -sg EMBEDDED_NAS_DM_SG set -slo <SLOName>`. Where <SLOName> is the name of a service level returned in step a.

Remove the service level associated with EMBEDDED\_NAS\_DM\_SG by entering the following: `symmsg -sid xxx -sg EMBEDDED_NAS_DM_SG set -noslo`

- e. Add the new Control LUNs to the masking view and map them as LUN 6 - 9..

5. Perform a discovery operation using the command `nas_diskmark -mark -all -discovery y -monitor y`.

# Configure Control Station-to-Control Station communication

## Before you begin

Before creating a FAR session for remote replication, you must establish the trusted relationship between the source and destination eNAS systems in your configuration.

### Note

The communication between eNAS Control Stations uses HTTPS protocol.

The procedures in this section require the following:

- The systems are up and running and IP network connectivity exists between the Control Stations of both eNAS systems. Verify whether a relationship already exists by using the `nas_cel -list` command.
- The source and destination Control Station system times must be within 10 minutes of each other. And secondary Control Stations must also have the same date and time (within 10 minute skew allowed) as their source Control Stations. Take into account time zones and daylight savings time, if applicable. Dell EMC recommends using an NTP service on the Control Stations to control this function. You can set this up using the `nas_cs` CLI command.
- The same 6-15 characters passphrase must be used for both eNAS systems.
- The same admin user credentials (username and password) should be used on the local and remote sites.

To establish communication between the source and destination sites, do the following:

## Procedure

1. On the source eNAS system, to establish the connection to the destination eNAS system in the replication configuration, use this command syntax:

```
$ nas_cel -create <cel_name> -ip <ip> -passphrase <passphrase>
```

where:

`<cel_name>` = name of the remote destination eNAS system in the configuration

`<ip>` = IP addresses (separated by comma) of the remote Control Stations in slot 0 (and slot 1)

`<passphrase>` = the secure passphrase used for the connection, which must have 6-15 characters and be the same on both sides of the connection

Example:

To add an entry for the Control Station of the destination eNAS system, cs110, from the source eNAS system cs100, type:

```
$ nas_cel -create cs110 -ip 192.168.168.10 -passphrase nasadmin
```

Output:

```
operation in progress (not interruptible)...
id          = 1
```

```

name          = cs110
owner         = 0
device        =
channel       =
net_path      = 192.168.168.10
celerra_id    = APM000420008170000
passphrase    = nasadmin

```

2. On the destination eNAS system, to establish the connection to the source eNAS system in the replication configuration, use this command syntax:

```
$ nas_cel -create <cel_name> -ip <ip> -passphrase
<passphrase>
```

where:

*<cel\_name>* = name of the remote source eNAS system in the configuration

*<ip>* = IP addresses (separated by comma) of the remote Control Stations in slot 0 (and slot 1)

*<passphrase>* = the secure passphrase used for the connection, which must have 6-15 characters and be the same on both sides of the connection

Example:

To add an entry for the Control Station of the source eNAS system, cs100, from the destination eNAS system cs110, type:

```
$ nas_cel -create cs100 -ip 192.168.168.12 -passphrase nasadmin
```

Output:

```

operation in progress (not interruptible)...
id          = 2
name        = cs100
owner       = 0
device      =
channel     =
net_path    = 192.168.168.12
celerra_id  = APM000340000680000
passphrase  = nasadmin

```

#### ⚠ CAUTION

If the NAT IP addresses of any of the sites is changed after FAR is configured, update the address at the other site using:

```
nas_cel -modify { <cel_name> | id=<cel_id> } { [-passphrase
<passphrase>] [-name <new_name>] [-ip <ipaddr>[,<ipaddr>,...]] }
```

#### ⚠ WARNING

For High Availability (HA), it is recommended to include both the eNAS NAT IPs (separated by a comma) to the `nas_cel` command. For more information, refer to the `nas_cel` man page.

- 3.

## Enable the FAR service

### Before you begin

The following prerequisites should be in effect before you enable the FAR service:

- Both source and destination systems have been added as destination systems of each other (Control Station-to-Control Station relationship) with the same pass phrase (use the `nas_cel` command command).
- Cabinet DR has not been created on either the local or remote systems.
- The FSID ranges used should be larger than 8192 and must not overlap between the local and remote systems.

Before you can create a FAR-replicable VDM, you must enable the FAR service between the source and destination systems.

### Procedure

1. At either the source or destination site, type the following command syntax:

```
$ nas_cel -syncprep -enable {<cel_name>|id=<cel_id>} -
local_fsidrange <from>,<to> -remote_fsidrange <from>,<to>
-local_storage
{sym_dir=<director1>:<port1>[,<director2>:<port2>,...<dire
ctorN>:<portN> rdf_group=<group_num>} -remote_storage
{sym_dir=<director1>:<port1>[,<director2>:<port2>,...<dire
ctorN>:<portN> rdf_group=<group_num>
```

where:

`-enable {<cel_name>|id=<cel_id>}` = enables FAR on the specified eNAS system (source or destination).

`-local_fsidrange <from>,<to>` = sets the file system identifier range on the local eNAS system. This range must not overlap the file system identifier range on the remote eNAS system.

`-remote_fsidrange <from>,<to>` = sets the file system identifier range on the remote eNAS system. This range must not overlap the file system identifier range on the local eNAS system.

`-local_storage {sym_dir=<director> rdf_group=<group_num>}` = specifies the director and group number used for the local RDF group.

`remote_storage {sym_dir=<director> rdf_group=<group_num>}` = specifies the director and group number used for the remote RDF group.

Example:

To enable the FAR service, on either the source or destination system type:

```
$ nas_cel -syncprep -enable LY2C6_CS0 -local_fsidrange 4096,12287
-remote_fsidrange 12288,24575 -local_storage 000197100006
sym_dir=1G:9,2G:9 rdf_group=106 -remote_storage 000196701857
sym_dir=3H:27,4H:27 rdf_group=106
```

Output from 100K system:

```
Now doing precondition check... done
Now saving FSID range [12288,24575] on remote system... done
```

## Setting up FAR

```
Now saving FSID range [4096,12287] on local system... done
Now creating LUN mappings (may take several minutes)... done
Now adding CTD access to local server server_2... done
Now adding CTD access to local server server_3... done
Now creating mountpoint for sync replica of NAS database... done
Now mounting sync replica of NAS database... done
Now enabling sync replication service on remote system... done
Warning 26316899209 : Always keep the source and remote Control Stations
(primary and secondary) are time synchronized, if not already taken care.
done
```

# CHAPTER 5

## Configuring FAR

This chapter explains how to configure the eNAS systems for FAR.

---

### Note

Be sure to complete the procedures in [Setting up FAR](#) on page 33 before starting the procedures in this chapter.

---

Topics include:

- [Start the FAR service](#) ..... 42
- [Create data LUNs for NAS resources](#) ..... 43
- [Create a FAR-replicable VDM](#) ..... 45
- [Create a file system on the bonded pool](#) ..... 47
- [Create the first file system checkpoint on the bonded pool](#) ..... 48
- [Create a network interface for a FAR-replicable VDM](#) ..... 49
- [Create CIFS shares for each file system on the bonded pool](#) ..... 51
- [Create a FAR session](#) ..... 52
- [Start a FAR session](#) ..... 54
- [Migrate Data Mover configurations](#) ..... 55
- [Configure CIFS CA support](#) ..... 56
- [Configure for NFS I/O transparency in FAR session](#) ..... 59

## Start the FAR service

In the event that you have to restart the FAR service, for example, after a failover, issue the following command to restart it:

```
$ nas_cel -syncprep -start {<cel_name>|id=<cel_id>}
```

Where:

`-start {<cel_name>|id=<cel_id>}` = Starts the FAR service on the specified eNAS system (between the source and destination, in both directions).

## Create data LUNs for NAS resources

### Before you begin

The FAR service must be enabled.

This procedure explains how to:

- Create the desired number of LUNs for use as data LUNS on the source and destination eNAS systems.
- Name the LUNs and assign IDs so that you can track them. For example, `nas_data_lun_1` and `nas_data_lun_2`.
- Size the LUNs based on the amount of information to be stored and duration. For example, 20 GB on a RAID 10.
- Build the LUNs from a block storage pool and assign them to specific eNAS storage groups and diskmark them as mapped pools.

### Procedure

1. In Unisphere for PowerMax, select the source eNAS system.
2. Select **System > System Dashboard**
3. In the **Summary** panel, click **File Dashboard**.
4. If prompted, type the username and password you use to access the eNAS control station, and click **OK**.
5. In the **Common Tasks** panel, click **Provision Storage for File** to open the **Provision Storage for File** wizard.
6. Type a **Storage Group Name**.
7. Set the **Service Level** to **Optimized**. This will create a storage pool in Unisphere instead of a volume.
8. Refine the service level by selecting the Workload Type to assign to it.
9. Type the number of Volumes and select the Capacity of each.
10. Optional: To set host I/O limits for the storage groups, click **Set Host I/O Limits** to open the **Host I/O Limits** dialog box. For information about setting the limits, refer to the dialog's help page.
11. Click **Next**.
12. Review the settings, and click **Finish**.
13. On the source eNAS system, run the following command to create NAS Disks Volumes:
 

```
$ nas_diskmark -mark -all -discovery y -monitor y
```
14. Select the destination eNAS system and repeat these steps.
15. On the destination eNAS system, run the following command to create NAS Disks Volumes:
 

```
$ nas_diskmark -mark -all -discovery y -monitor y
```

---

**Note**

Create the same number of volumes using the same size as the source, which will be presented to the target eNAS system and used to create the target NAS pools.

---

**Note**

When configuring the data LUNs, verify the following for the mapped pools:

- a. The corresponding Storage Group that is used for creating a mapped pool should always have either SLO, SRP, or HOST I/O LIMITS set.
  - b. If HOST I/O LIMITS are set, then the admin must have the value of HOST I/O LIMITS set to a max value of 2,000,000 IO/sec, unless the admin wants limited/restricted performance.
-

## Create a FAR-replicable VDM

### Before you begin

The following prerequisites should be in effect before you create a FAR-replicable VDM:

- The FAR service has been enabled between the two eNAS systems, source and destination.
- A non-FAR-replicable NAS pool must be specified.

To create a FAR-replicable VDM (also known as a bonded pool), do the following:

---

### Note

If you intend to use an existing VDM for sync replication, see [Modify a VDM from non-FAR-replicable to FAR-replicable](#) on page 74 for instructions to modify a non-FAR-replicable VDM to be FAR-replicable.

---

### Procedure

1. At the source site, type the following command syntax:

```
$ nas_server [-name <name>] [-type <type>] -create
<movername> [-setstate<state>] [pool=<pool>]
[storage=<system_name>] [-option <options>]
```

Where:

`[-name <name>] [-type <type>] -create <movername>` = Creates a VDM with an optional name for the specified VDM.

`-setstate<state>` = Sets the state of the VDM to loaded or mounted.

`pool= <pool>` = Assigns a rule set known as a mapped pool for the VDM root file system.

`storage=<system_name>` = The storage pool option assigns a rule set for the root file system of the VDM that contains automatically created volumes and defines the type of disk volumes used and how they are aggregated.

`-option <options>` = Specifies a comma separated list of options that includes FS type, log type, and whether the VDM is FAR-replicable.

Example:

To create a FAR-replicable VDM, type:

```
nas_server -name vdm1 -type vdm -create server_2 pool=src_sg1 -
option syncreplicable=yes
```

Output:

```
operation in progress (not interruptible)...
id                = 3
name              = vdm1
ad                = 0
Type              = vdm
server            = server_2
rootfs            = root_fs_vdm_vdm1
I18Nmode          = UNICODE
mountedfs         =
syncreplicable    = True
```

## Configuring FAR

```
member of      =  
status         :  
  defined = enabled  
  actual = loaded, ready  
Interfaces to services mapping:
```

## Create a file system on the bonded pool

To create a file system on the bonded NAS pool so that it can be included in any synchronous replication session created on the corresponding FAR-replicable VDM, follow these rules:

- `log_type=Common` must not be specified. Use `split`, which is the default.
- `type=` Only `uxfs` or `rawfs` can be specified as `type`.
- If you specify the `mount_option`, only a FAR-replicable VDM on the FAR-replicable NAS pool can be specified in `mount_option`.

### Procedure

1. Specify the name of the file system (optional), its size, the bonded pool, and the VDM name using `nas_fs`.

For detailed information about creating a file system, refer to the `nas_fs` section of the *EMC VNX Command Line Interface Reference for File and Managing Volumes and File Systems on VNX Manually*. These documents are located on Dell EMC Online Support (registration required) at <http://support.EMC.com> and in the Related documents section of the VNX Series on the mydocuments site at <https://mydocuments.emc.com/>.

### Results

The split-log file system is created on the bonded pool.

## Create the first file system checkpoint on the bonded pool

To create the first checkpoint for a file system on a bonded pool, do the following:

### Procedure

1. Specify the name or ID of the file system, checkpoint name (optional), SavVol size (optional), and pool of the SavVol (optional, must be the same pool as the file system if specified) using `fs_ckpt`.

For detailed information about creating a file system checkpoint, refer to the `fs_ckpt` section of the *EMC VNX Command Line Interface Reference for File and Using VNX SnapSure*. These documents are located on Dell EMC Online Support (registration required) at <http://support.EMC.com> and in the Related documents section of the VNX Series on the mydocuments site at <https://mydocuments.emc.com/>. You can also specify a checkpoint schedule using `nas_ckpt_schedule`, which is also described in these documents.

### Results

SavVol for the file system is created on the bonded pool along with the first file system checkpoint.

# Create a network interface for a FAR-replicable VDM

## Before you begin

The following prerequisites should be in effect before you create a network interface for a FAR-replicable VDM:

- FAR service has been enabled between the two eNAS systems, source and destination.
- FAR-replicable VDM has been created.

To create and assign a network interface for each FAR-replicable VDM, do the following:

## Procedure

1. On the source eNAS system, type:

```
nas_server -vdm <vdm_name> -attach <interface>
```

For detailed information about creating a network interface for a VDM, refer to *Configuring Virtual Data Movers on VNX*. This document is located on Dell EMC Online Support (registration required) at <http://support.EMC.com> or in the Related documents section of the VNX Series on the mydocuments site at <https://mydocuments.emc.com/>.

Example:

To create a network interface for a FAR-replicable VDM, type:

```
$ nas_server -vdm vdm1 -attach vdm_intf1
```

Output:

```
operation in progress (not interruptible)...
id                = 3
name              = vdm1
ad                = 0
Type              = vdm
server            = server_2
rootfs            = root_fs_vdm_vdm1
I18Nmode         = UNICODE
mountedfs        =
syncreplicable   = True
member of        =
status           :
  defined = enabled
  actual = loaded, ready
Interfaces to services mapping:
interface=vdm_intf1 :vdm
```

2. Repeat Step 1 for each of the remaining FAR-replicable VDMs.

---

## Note

A VDM can have multiple interfaces attached to it, while an interface can be attached to a single VDM.

---

## Results

- Allows the user to manage the network interfaces for a VDM. The interfaces are attached to a VDM when the VDM state is loaded. When an interface is attached

to a VDM, the NFS clients connecting the Data Mover through this interface have access to the file system exported by the VDM configuration.

- If CIFS server is hosted within the VDM, which is configured in File Auto Recovery in SRDF (`nas_syncrep`), the interfaces should be provisioned first to the VDM and then to CIFS server. Directly provisioning the interfaces to this CIFS Server will lead to the interface not turning up on standby side during VDM sync operations.

## Create CIFS shares for each file system on the bonded pool

### Before you begin

The procedures in this section require the following:

- File systems have been created on the bonded pool.
- Checkpoint has been created for a file system on the bonded pool.

Create CIFS shares for each of the file systems on the bonded pool. For detailed information about creating CIFS shares for the file systems on bonded pools, refer to *Configuring and Managing CIFS on VNX*. This document also contains information about starting the CIFS service and creating a standalone CIFS Server. This document is located on Dell EMC Online Support (registration required) at <http://support.EMC.com> and in the Related documents section of the VNX Series on the mydocuments site at <https://mydocuments.emc.com/>.

---

### Note

In previous releases, creating a CIFS service on existing FAR session would fail with error "Error 13432061955: <vdm> : The interface '<interface>' is currently in use by a vdm syncprep session <FAR\_session\_name>". This has been fixed HYPERMAX OS 5977 Q3 2016 SR.

---

## Create a FAR session

### Before you begin

Review the following before creating a FAR session:

- FAR service has been enabled between the two eNAS systems, source and destination.
- Both source and destination systems are operating with VNX OE for file version 8.1.11.24 or higher version.
- Control Station-to-Control Station communication channel between the two eNAS systems should be configured and ready for communication.
- If a non system-defined user login is used, be sure that the same user with the same credentials (username and password) and the same authorizations (role and group ID) is defined on the remote site.
- Specified VDM is FAR-replicable, mounted, loaded or temporarily unloaded on the DM.
- The destination mapped pool is not in use and meets all bonded pool criteria.
- The destination mapped pool must match the size of the source mapped pool. If equal performance is desired at the destination site, in relation to the source site, the destination mapped pool should be built using the same configuration.
- When the number of disk volumes in a pool is extremely huge, the session creation will take considerably longer time to complete.
- Local and remote Data Mover should have the same l18N mode.
- Bonded pool of the specified VDM does not contain a File System/Checkpoint with an FSID that is used in the remote system.
- If you create and attach a new IP interface on the source VDM after the replication session has been created, a warning will appear stating that this new interface will not be reversed or failed over. You must manually create the new interface, with the same name, in the DOWN state on the destination eNAS system before you can reverse or failover the session. If the interface is not created on the destination eNAS system, a FAR session reverse or failover operation will fail.
- If you want the destination system to match the configuration of the source, from the destination eNAS system, manually migrate the following Data Mover configuration items by using `migrate_system_conf`. [Migrate Data Mover configurations](#) on page 55 provides more information.

To create a FAR session, do the following:

### Procedure

1. At the source site, type the following command syntax:

```
$ nas_syncrep -create <name> -vdm <vdm_name> -
remote_system <cel_name> -remote_pool <pool_name> -
remote_mover <mover_name> -network_devices
<local_device_name>:<remote_device_name>[,...]
```

Where:

`-create <name>` = Assigns a name to the synchronous replication session.

`-vdm <vdm_name>` = Specifies the name of an existing source FAR-replicable VDM to replicate.

`-remote_system <cel_name>` = Specifies the name of an existing remote eNAS system.

`-remote_pool <pool_name>` = Specifies the name of an existing remote mapped pool.

`-remote_mover <mover_name>` = Specifies the name of an existing remote Data Mover.

`[-network_devices <local_device_name>:<remote_device_name>[,...]]` = Specifies the mappings of the local and remote network devices. If any network interface is attached to the specified VDM, this parameter is mandatory; otherwise, this parameter is optional.

Example:

To create a FAR session, type:

```
$ nas_syncprep -create session1 -vdm vdm1 -remote_system
LY2C6_CS0 -remote_pool src_sg1 -remote_mover server_2 -
network_devices cge-8-0:cxg-3-0
```

Output:

```
Now validating params... done
Now marking remote pool as standby pool... done
Now creating LUN mapping... done
Now creating remote network interface(s)... done
Now marking remote pool as standby pool... done
Now updating local disk type... done
Now updating remote disk type... done
Now generating session entry... done
done
Warning 17726963894: Network interface to be created vdm_intf1 had errors.
```

## Results

The same network interfaces are created on the remote system as those on the source system with a status of DOWN. The FAR session is saved on the local NAS\_DB. Remote LUNs become read only.

## Start a FAR session

If a FAR session has been stopped, such as after a failover, issue the following command from the R2 side to restart it:

```
$ nas_syncprep -start {-all|<name>>|id=<id>}
```

**Where:**

`-start` = starts the specified FAR session. Specifying `-all` starts all FAR sessions.

## Migrate Data Mover configurations

The migration of Data Mover configurations is not included in FAR. The following is the list of these configurations:

- Data Mover configurations:
  - DNS
  - NIS
  - NTP
  - Local passwd and group
  - Usermapper client
  - FTP/SFTP
  - LDAP
  - HTTP
  - CEPP
  - CAVA
  - Server Parameters
  - Netgroup
  - Nsswitch
  - Hosts

Use `migrate_system_conf` to migrate those configurations that are needed for FAR after the creation of a FAR session and before a reverse or failover operation. For information about `migrate_system_conf`, see the *VNX Command Line Interface Reference Information for File* and *Using VNX File Migration Technical Notes* for details.

---

### Note

The routing table, including the default route, does not get migrated with this command. The routes need to be configured manually. To add a default gateway or a route entry, a network interface with a status of UP must exist.

---

## Configure CIFS CA support

### Before you begin

In order to support CIFS CA on VDM synchronous replication reverse or failover, use the SMB 3.0 client with CA enabled, which can be Windows Server 2012 or Windows 8. To configure CIFS CA, you need to do the following:

---

### Note

The HomeDirectory feature does not support Continuous Availability (CA) capability. Keep this in mind when you configure CIFS Continuous Availability (CA) support for the VDM synchronous replication feature.

---

### Procedure

1. If not already enabled, enable the SMB 3.0 protocol.

Example:

To enable the SMB 3.0 protocol, type:

```
$ server_cifs server_2 -add security=NT, dialect=SMB3
```

2. Mount and export network Shares with the `smbca` flag set.

eNAS File Server configuration to achieve CIFS CA requires network Shares that are mounted and exported with a special `smbca` flag. CA mount and Export options are not supported in Unisphere. For more information about CIFS, see *Configuring and Managing CIFS on VNX*.

Example:

To mount and export network Shares, type:

```
$ server_mount server_2 -o smbca fs1
```

```
$ server_export server_2 -P cifs -name fileshare -option type=CA /fs1
```

3. If necessary, set the File server CIFS parameter `smb2.maxCaTimeout`.

To support eNAS File Server CA, the File server uses a CIFS parameter `smb2.maxCaTimeout`, with a default timeout value of 360 seconds. This value can be configured from 0-600 seconds, depending on your requirements. *Parameters Guide for VNX for File* provides more information on how to modify this parameter.

4. On the source and destination eNAS system, configure an additional network interface on the Data Mover.

To achieve CIFS CA, you must create an additional network interface on the Data Mover hosting the VDM protected by a FAR session. The network interface should be up and configured with a public IP address. It can be used by other VDMs or CIFS servers; however, it cannot be used by any VDM that is protected by a FAR session.

5. On the destination eNAS system, ensure the Data Mover configurations and cabinet level service that are needed for FAR have been migrated from the source. See [Migrate Data Mover configurations](#) on page 55 for more information.

6. On the destination eNAS system, ensure the CIFS Service is started on the target Data Mover.

CIFS service must be started on the target Data Mover so that after a FAR session is reversed or failed over, the CIFS service can be replicated on the destination eNAS system.

Example:

Use either the `server_setup` CLI command to start CIFS service manually or the `migrate_system_conf` tool to migrate the Data Mover configuration from the source eNAS system to the destination eNAS system. Type:

```
$ server_setup server_2 -Protocol cifs -option start
```

or

```
$ /nas/bin/migrate_system_conf -mover -source_system id=1 -
source_user nasadmin -source_mover server_2 -destination_mover
server_2 -service cifs
```

7. Ensure the DNS server is configured on the target Data Mover.

To achieve CIFS IO transparency, after a FAR reverse or failover session, you must make sure the destination Data Mover is configured with the same DNS server as the source Data Mover.

Example:

Use either the `server_dns` CLI command to configure the DNS server manually or the `migrate_system_conf` tool. Type:

```
$ server_dns server_2 -protocol udp dns.cifs.domain.com
10.11.12.13
```

or

```
$ /nas/bin/migrate_system_conf -mover -source_system id=1 -
source_user nasadmin -source_mover server_2 -destination_mover
server_2 -service dns
```

8. Ensure the target Data Mover can connect with the DNS server, type:

```
$ server_ping server_2 dns.cifs.domain.com
```

If connection to the DNS server cannot be established, check with your network administrator. If the source eNAS system and destination eNAS system are not in the same subnet, you must configure route settings using one of the following methods (refer to *Configuring and Managing Networking on VNX* for details):

Add a default gateway using the `server_route` CLI command, for example:

```
$ server_route server_2 -add default 10.11.12.1
```

Add a route entry using the `server_route` CLI command, for example:

```
$ server_route server_3 -add net 10.13.14.15 10.11.12.1
```

9. Ensure the target network interface can work on the destination eNAS system.

The source and destination network interfaces for a FAR session are using the same name. The network interface on the destination eNAS system is in the down state. If the network interface on the destination eNAS system is created automatically during a FAR session creation, then it is configured using the same configuration as the source eNAS system, including the IP address. If the destination eNAS system network interface is created manually after FAR session creation, it can be configured with any configuration which works on

the destination eNAS system. If the network interface on the source and destination are using different IP addresses, simply bring the destination network interface up and see that it is working by using the `server_ping` CLI command.

---

**Note**

If the network interfaces on the source and destination are using the same IP address, the network interface on the destination cannot be brought up; otherwise, there will be an IP address conflict on the network. Use one of the following ways to test whether the network interface works:

- When the VDM is not in service to users, do a FAR session reverse and check if the CIFS server can be connected after the reverse.
- Create a network interface using an IP address within the same subnet as the destination network interface, bring it up, and test if it works using the `server_ping` CLI command.

If the target network interface cannot work, check with your network administrator. Ensure the target Data Mover has the correct routes, and, if applicable, the VLAN functions.

---

# Configure for NFS I/O transparency in FAR session

## Before you begin

FAR does not replicate Data Mover level configuration. The Data Mover level configuration, like the default route, cannot rely on the network interface which is attached to the VDM protected by a FAR session. To add a network interface and replicate Data Mover level configuration, you need to do the following:

## Procedure

1. On the source system, add a network interface to make the Data Mover level configuration work.

The additional network interface should be up and configured with a public IP address. It can be used by another VDM or CIFS server, but it cannot be used by any VDM that is protected by a FAR session.

2. On the destination eNAS system, migrate the Data Mover configuration that is needed for FAR. See [Migrate Data Mover configurations](#) on page 55 for more information.

3. Ensure the target network interface can work on the destination eNAS system.

The source and destination network interfaces for a FAR session are using the same name. The network interface on the destination eNAS system is in the down state. If the network interface on the destination eNAS system is created automatically during a FAR session creation, then it is configured using the same configuration as the source eNAS system, including the IP address. If the destination eNAS system network interface is created manually after FAR session creation, it can be configured with any configuration which works on the destination eNAS system, as long as it uses the same name as the source eNAS system network interface. To ensure NFS I/O transparency, the source and destination network interface must use the same IP address.

---

## Note

If the network interfaces on the source and destination are using the same IP address, the network interface on the destination cannot be brought up; otherwise, there will be an IP address conflict on the network. Use one of the following ways to test whether the network interface works:

- When the VDM is not in service to users, do a FAR session reverse and check if the NFS client can connect to the NFS server and then reverse back.
- Create a network interface using an IP address within the same subnet as the destination network interface, bring it up, and test if it works using the `server_ping` CLI command.

If the target network interface cannot work, check with your network administrator. Ensure the target Data Mover has the correct routes, and, if applicable, the VLAN functions.

---



# CHAPTER 6

## Managing FAR sessions

This chapter explains how to manage FAR sessions.

Topics include:

• Reverse operation.....	62
• Failover operation.....	65
• List FAR service information.....	70
• Show information for FAR service.....	71
• Disable the FAR service.....	72
• Modify a VDM from FAR-replicable to non-FAR-replicable.....	73
• Modify a VDM from non-FAR-replicable to FAR-replicable.....	74
• Show information for a FAR-replicable VDM.....	75
• Delete a FAR-replicable VDM.....	76
• List FAR session information.....	77
• Show FAR session information.....	78
• Delete a FAR session.....	79
• Extend bonded pool with FAR session.....	80
• Modify network devices.....	80
• Updating VNX OE software.....	82
• FAR Health Check.....	82

## Reverse operation

If it is necessary to perform maintenance or balance the load on your source eNAS system and maintain a FAR-replicable VDM as active, reverse the direction of the corresponding FAR session between the source and destination sites. To reverse the direction of a FAR session to the destination site and then return it (reverse the direction back) to normal operation at the source site, follow this sequence of tasks:

---

### Note

It is recommended that you periodically perform a FAR Health Check, say as a cron job, to monitor the health of VDM sync sessions. This will enable you to take proactive measures to help minimize the chances that an unplanned failover or reverse operation will fail. [FAR Health Check](#) on page 82 provides more information.

---

1. At the destination site, run the `nas_syncrep -reverse` command. This action moves the VDM, FS, FS checkpoints, FS checkpoint schedules, and related network interfaces to the destination site, which becomes active. The VDM session at the source site becomes standby.
2. At the source site, run the `nas_syncrep -reverse` command. This action returns the VDM, FS, FS checkpoints, FS checkpoint schedules, and related network interfaces to the source site, which becomes active. The VDM session at the destination site becomes standby.

## Performing reverse on a FAR session

### Before you begin

The following prerequisites should be in effect before you reverse a FAR session:

- Both the source and destination sites are up.
- All network interfaces on the source eNAS system have the corresponding network interfaces with the same names on the destination eNAS system specified for the FAR session.
- No FSID conflicts between source and destination systems.
- The FAR session status and service status for remote to local is synchronized.
- Local and remote Data Mover should have the same I18N mode.

Also, in order to support CIFS CA (Continuous Availability) on reverse, you must use the SMB 3.0 client with CA enabled. If the service outage time can be less than the CIFS timeout, CIFS CA can be achieved. To configure CIFS CA support on VDM synchronous replication reverse, see [Configure CIFS CA support](#) on page 56 for details. If you need to configure for NFS I/O transparency, see [Configure for NFS I/O transparency in FAR session](#) on page 59 for details.

This task reverses the direction of a FAR session along with the source and destination roles of the two eNAS systems involved in the FAR session.

### Procedure

1. At the destination site, type the following command syntax:

```
$ nas_syncrep -reverse {<name>|id=<id>}
```

Where:

`<name>` = Name of the FAR session

`<id>` = Identifier of the FAR session

**Example:**

To reverse the direction of a FAR session using the ID of the FAR session, type:

```
$ nas_syncrep -reverse session1
```

**Output:**

```
WARNING: You have just issued the nas_syncrep -reverse command. There will be a
period of Data Unavailability during the reverse operation, and, after the reverse
operation, the VDM/FS(s)/checkpoint(s) protected by the sync replication session will
be reversed to the local site. Are you sure you want to proceed? [yes or no]
```

**2. At the warning prompt, type `yes`.****Output:**

```
Now doing precondition check... done: 24 s
Now doing health check... done: 12 s
Now handling Replicator(V2) sessions... done: 31 s
Service outage start.....

INFO: In case the 'turning down remote network interface(s)' fail, refer to the CCMD
26317029441 to access the file systems and/or ckpt file systems from the client.

Now turning down remote network interface(s)... done: 8 s

INFO: In case the SRDF switch failure, refer to the CCMD 26317029442 for remounting
R1's file systems, checkpoint file systems.

Now switching the session (may take several minutes)... done: 17 s

INFO: Successfully completed session failover (and swap) with local clean persued in
parallel.

Now importing sync replica of NAS database... done: 12 s
Now creating VDM... done: 3 s
Now importing VDM settings... done: 0 s
Now mounting exported FS(s)/checkpoint(s)... done: 2 s
Now loading VDM... done: 3 s
Now turning up local network interface(s)... done: 1 s
Service outage end: 46 s

Now pausing ckpt schedule(s)... done: 0 s
Now mounting unexported FS(s)/checkpoint(s)... done: 3 s
Now importing schedule(s)... done: 0 s
Now establishing the session... done: 12 s
Now unloading remote VDM/FS(s)/checkpoint(s)... done: 10 s
Now cleaning remote... done: 14 s

Elapsed time: 152s

done
```

**3. To check the state of the session, type:**

```
$ nas_syncrep -info session1
```

**Output:**

```
id = 4102
name = session1
vdm_name = vdm1
syncrep_role = active
```

```
local_system      = L9C16_CS0
local_pool        = src_sg1
local_mover       = server_2
remote_system     = LY2C6_CS0
remote_pool       = src_sg1
remote_mover      = server_2
device_group      = 61_006_60_1857
session_status    = in_sync
```

### Results

The original destination eNAS system becomes the source eNAS system for the VDM in the FAR session. The NAS client can only access data from the new source eNAS system for the VDM. The NAS client cannot access data from the original eNAS system.

---

### Note

After the FAR session is reversed, for the disk volumes in the mapped pool, their visible servers (listed in the corresponding `servers` field) will become empty on the source side.

---

## Failover operation

During normal operation when a FAR session is active, the source FAR-replicable VDM is active while the destination DM is active and designated for use as a standby for the source FAR-replicable VDM. If a failure occurs at the source site (active eNAS system in the FAR session is down and not available) and you have not set up automatic failover using FARM, you need to manually failover the source FAR-replicable VDM to the destination eNAS by using the eNAS for file CLI.

### NOTICE

In situations where the source site is still accessible, a FAR session reverse operation must be used instead. Performing a failover instead of a reverse in these scenarios may lead to unexpected issues, such as DU due to DM panics.

### Note

It is recommended that you periodically perform a FAR Health Check, say as a cron job, to monitor the health of VDM sync sessions. This will enable you to take proactive measures to help minimize the chances that an unplanned failover or reverse operation will fail. [FAR Health Check](#) on page 82 provides more information.

To failover a FAR-replicable VDM to the destination site and then return to normal operation at the source site, follow this sequence of tasks:

1. At the destination site, run the `nas_syncrep -failover` command. This brings the VDM, FS, FS checkpoints, FS checkpoint schedules, and related network interfaces online at the destination site.
2. Fix the issue that caused the failure at the source site.

### WARNING

**During VDM Sync failover nasadmin should not attempt DM failover on the source side as it causes the R1 DM to panic. The *eNAS Release Notes* contains more information.**

3. Run the `nas_syncrep -Clean` command from the source site for either a specified FAR session or all FAR sessions stored in the source NAS database. This action cleans the source site of all unnecessary objects and prepares it for a `nas_syncrep -reverse` operation. If the `nas_syncrep -Clean` command is not run, you are prevented from reversing the replication session.
4. If the source site Data Mover network is disconnected, reconnect it.
5. At the source site, run the `nas_syncrep -reverse` command. This action restores normal operation at the source site. It brings the VDM, FS, FS checkpoints, FS checkpoint schedules, and related network interfaces online at the source site and changes the corresponding VDM session at the destination site to standby.

## Performing failover on a FAR session

### Before you begin

The following prerequisites should be in effect before you failover a FAR session:

- Standby eNAS system of the FAR session is up.

- Local and remote Data Movers should have the same I18N mode.

---

**Note**

If the network interface on the original source system is not in the down state (system will only try to turn it down during the failover, but it may fail), I/O transparency cannot be guaranteed.

---

Also, in order to support CIFS CA (Continuous Availability) on failover, you must use the SMB 3.0 client with CA enabled. If the service outage time can be less than the CIFS timeout, CIFS CA can be achieved. To configure CIFS CA support on FAR failover, see [Configure CIFS CA support](#) on page 56 for details. If you need to configure for NFS I/O transparency, see [Configure for NFS I/O transparency in FAR session](#) on page 59 for details.

After a disaster occurs and the active eNAS system is down, failover a FAR-replicable VDM to the standby eNAS system to make it active.

**NOTICE**

Failover should only be used in situations where the source site is not available. In situations where the source site is still accessible, a reverse must be used instead. For more information, refer to [Reverse operation](#) on page 62.

---

**CAUTION**

**When failover starts, you must not perform any operation on the VDM and FAR session on the destination sites until the FARM failover operation completes.**

---

**Procedure**

1. At the destination site, type the following command syntax:

```
$ nas_syncrep -failover {<name>|id=<id>}
```

Where:

*<name>* = Name of the VDM synchronous replication session

*<id>* = Identifier of the VDM synchronous replication session

For example, to failover the VDM to the standby eNAS system, type:

```
$ nas_syncrep -failover session1
```

WARNING: You have just issued the `nas_syncrep -failover` command. Verify whether the peer system or any of its file storage resources are accessible. If they are, you should issue the `nas_syncrep -reverse` command instead. Running the `nas_syncrep -failover` command while the peer system is still accessible could result in Data Loss if the session is not in sync. Are you sure you want to proceed? [yes or no] yes

At the warning prompt, type **yes**.

```
Now doing precondition check... done: 23 s
Caution: R1 site CS, Datamover and VDM are available, so executing planned failover
operation instead of failover to avoid R1 Datamover panic post operation is complete.
Now doing health check... done: 3 s
Now handling Replicator(V2) sessions... done: 30 s
INFO: In case the 'turning down remote network interface(s)' fail, refer to the CCMD
```

```

26317029441 to access the file systems and/or ckpt file systems from the client.

Now turning down remote network interface(s)...          done: 8 s

INFO: In case the SRDF switch failure, refer to the CCMD 26317029442 for remounting
R1's file systems, checkpoint file systems.

Now switching the session (may take several minutes)...  done: 7 s

INFO: Successfully completed session failover (and swap) with local clean persued in
parallel.

Now importing sync replica of NAS database...            done: 12 s
Now creating VDM...                                    done: 3 s
Now importing VDM settings...                           done: 0 s
Now mounting exported FS(s)/checkpoint(s)...           done: 3 s
Now loading VDM...                                     done: 3 s
Now turning up local network interface(s)...           done: 1 s

                                     Service outage end: 93 s

Now pausing ckpt schedule(s)...                         done: 0 s
Now mounting unexported FS(s)/checkpoint(s)...         done: 2 s
Now importing schedule(s)...                            done: 0 s

                                     Elapsed time: 97 s

done

```

## 2. To verify that the session state is stopped, type:

```
$ nas_syncrep -list
```

### Output:

```

id      name          vdm_name      remote_system  session_status
4102    session1      vdm1         -->L9C16_CS0  stopped

Warning 17727094793: The displayed status information could be stale if the nas
servers are not in required state.

```

### Results

After the failover completes, the original standby system becomes the active system for the VDM in the FAR session. The NAS client will now access data from the VDM on this active system. The original active system becomes the standby system for the VDM in the FAR session. After failover, the LUNs under FAR on the original active system (now the standby) become Read Only.

#### NOTICE

Outage duration depends on the number of File systems and checkpoints mounted and exported on source VDM. The more eNAS objects, the longer the outage time. The same is true with the load on CS. The higher the CS load on eNAS, the longer the outage time.

## Performing clean on a FAR session

### Before you begin

After a failover has occurred, the LUNs under FAR on the original source eNAS system become Read Only. You need to run the `nas_syncprep -Clean` command from the source site for either a specified FAR session or all FAR sessions stored in the source NAS database. This action cleans the source site of all unnecessary objects and prepares it for a `nas_syncprep -reverse` operation. If the command is not run, you are prevented from performing a failover or a reverse operation on the FAR session.

### Procedure

1. At the original source eNAS system site, type the following command syntax:

```
$ nas_syncprep -Clean {-all|<name>|id=<id>}
```

Where:

*<name>* = Name of the synchronous replication session

*<id>* = Identifier of the synchronous replication session

Examples:

To Clean all FAR sessions to the original source eNAS system, type:

```
$ nas_syncprep -Clean -all
```

```
Now cleaning session session1 (may take several minutes)... done
Now deleting obsolete mountpoints... done
Now starting session session1... done
```

To Clean a single FAR session to the original source eNAS system type:

```
$ nas_syncprep -Clean session1
```

```
WARNING: You have just issued the nas_syncprep -Clean command. This will result in a
reboot of the original source Data Mover that the VDM was failed over from. Verify
whether or not you have working VDM(s)/FS(s)/checkpoint(s) on this Data Mover and
plan for this reboot accordingly. Running the nas_syncprep -Clean command while you
have working VDM(s)/FS(s)/checkpoint(s) on this Data Mover will result in Data
Unavailability during the reboot. Are you sure you want to proceed?
```

At the prompt, type **yes**.

```
Now cleaning session session1 (may take several minutes)... done
Now starting session session1... done
```

2. To check the state of the session, type:

```
$ nas_syncprep -info session1
```

Output:

```
id           = 4102
name        = session1
vdm_name    = vdm1
syncprep_role = active
```

```

local_system      = L9C16_CS0
local_pool        = src_sg1
local_mover       = server_2
remote_system     = LY2C6_CS0
remote_pool       = src_sg1
remote_mover      = server_2
device_group      = 61_006_60_1857
session_status    = in_sync

```

## Results

The following occur as a result of a successful Clean operation:

- Standby VDM is deleted.
- Standby File Systems/checkpoints on VDM are deleted.
- The Data Mover may be rebooted.

### **⚠ WARNING**

**During the clean operation, the Data Movers on the local side may continuously panic, especially when there are other sessions not cleaned yet. This is a result of the Data Movers trying to access the volumes underneath the sessions, which are not yet cleaned with WD access. Use the `nas_syncrep Clean -all` command whenever there are more than one session that needs to be cleaned. If this continues to fail, contact your Dell EMC support representative for assistance.**

---

## List FAR service information

To list eNAS systems with the FAR service enabled, do the following:

### Procedure

1. At the source site, type the following command syntax:

```
$ nas_cel -syncprep -list
```

Where:

`-list` = Displays FAR-enabled eNAS systems.

Example:

To list service information, on either the source or destination eNAS system, type:

```
$ nas_cel -syncprep -list
```

Output:

```
id      name          syncprep
0       L9C16_CS0    initialized
1       LY2C6_CS0    enabled
```

## Show information for FAR service

You can view service information for a single system or for both the source and destination systems. To view FAR service information, do the following:

### Procedure

1. At the source site, type the following command syntax:

```
$ nas_cel -syncrep -info {<cel_name>|id=<cel_id>|-all} [-verbose]
```

Where:

`-info {<cel_name>|id=<cel_id>|-all} [-verbose]` = Displays FAR information about the specified eNAS system.

Example:

To display FAR service information for a remote system with synchronous replication enabled, type:

```
nas_cel -syncrep -info -all
```

Information about the FAR service between the source system and the specified destination system is displayed.

```
id = 0
name = L9C16_CS0
syncrep = initialized
fsidrange = 4096,12287

id = 4
name = LY2C6_CS0
syncrep = enabled
fsidrange = 12288,24575
local_storage =
000197100006, rdf_group=106, device_group=nasdb_006_1857
remote_storage =
000196701857, rdf_group=106, device_group=nasdb_1857_006
service_status :
  local_to_remote = in_sync
  remote_to_local = sync_in_progress
```

2. At the source site, type the following command syntax

```
$ nas_server -list
```

Lists the physical Data Mover table:

id	type	acl	slot	groupID	state	name
1	1	1000	2		0	server_2
2	1	1000	3		0	server_3
3	1	1000	4		0	server_4
4	4	1000	5		0	server_5

## Disable the FAR service

### Before you begin

The following prerequisites should be in effect before disabling the FAR service:

- FAR service has been enabled.
- FAR session does not exist.

To disable the FAR service, do the following:

### Procedure

1. At the source site, type the following command syntax:

```
$ nas_cel -syncrep -disable {<cel_name>|id=<cel_id>}
```

Where:

`-disable {<cel_name>|id=<cel_id>}` = Disables FAR on the specified eNAS system.

Example:

To disable FAR on the source system, type:

```
$ nas_cel -syncrep -disable LY2C6_CS0
```

Output:

```
Now unmounting sync replica of NAS database...
done
Now deleting mountpoint for sync replica of NAS database...
done
Now removing CTD access to local server server_2...
done
Now removing CTD access to local server server_3...
done
Now deleting local LUN mapping...
done
Now disabling service (including deleting LUN mapping) on remote system...
done
Now removing FSID range [12288,24575] on remote system...
done
Now removing FSID range [4096,12287] on local system...
done
Now removing other sync replication service settings on local system...
done
done
```

# Modify a VDM from FAR-replicable to non-FAR-replicable

## Before you begin

The following prerequisites should be in effect before you modify a VDM from FAR-replicable to non-FAR-replicable:

- The specified VDM should be a FAR-replicable VDM.
- The specified VDM should not have a FAR session on it.

To modify a VDM from FAR-replicable to non-FAR-replicable, do the following:

## Procedure

1. Type the following command syntax:

```
$ nas_server -vdm <vdm_name> -option syncreplicable=<yes|no>
```

Where:

`-vdm <vdm_name> -option syncreplicable=<yes/no>` = Specifies whether the VDM is FAR-replicable.

Example:

To modify a VDM from FAR-replicable to non-FAR-replicable, type:

```
nas_server -vdm test_vdm -option syncreplicable=no
```

Output:

```
id          = 80
name       = test_vdm
acl        = 0
type       = vdm
server     = server_2
rootfs     = root_fs_vdm_test_vdm
I18N mode  = ASCII
mountedfs  =
member_of  =
status     :
           defined = enabled
           actual   = loaded, ready
Interfaces to services mapping:
```

## Results

The FAR-replicable flag on the VDM and pool are unset.

## Modify a VDM from non-FAR-replicable to FAR-replicable

### Before you begin

The following prerequisites should be in effect before you modify a VDM from non-FAR-replicable to FAR-replicable:

- The rootfs of the specified VDM should be a split-log file system.
- The underlying pool should meet the criteria of a FAR-replicable NAS pool except the VDM should be FAR-replicable.

---

### Note

If a VDM and the file systems on it are created before upgrading to eNAS operating environment (OE) for file version 8.1.6, using the default log type (the default before version 8.1.6 is common log), the VDM cannot be converted to FAR-replicable.

---

To modify a VDM from non-FAR-replicable to FAR-replicable, do the following:

### Procedure

1. Type the following command syntax:

```
$ nas_server -vdm <vdm_name> -option syncreplicable=<yes|no>
```

Where:

`-vdm <vdm_name> -option syncreplicable=<yes/no>` = Specifies whether the VDM is FAR-replicable.

Example:

To modify a VDM from non-FAR-replicable to FAR-replicable, type:

```
$nas_server -vdm LY2E6_vdm1 -option syncreplicable=yes
```

Output:

```
id          = 6
name        = LY2E6_vdm1
acl         = 0
type        = vdm
server      = server_2
rootfs      = root_fs_vdm_LY2E6_vdm1
I18N mode   = UNICODE
mountedfs   =
syncreplicable = True
member_of   =
status      :
  defined   = enabled
  actual    = loaded, ready
Interfaces to services mapping:
  interface=cge0_1 :vdm
```

### Results

The FAR-replicable flag on the VDM and pool are set.

## Show information for a FAR-replicable VDM

### Before you begin

None.

To display information for a specific FAR-replicable VDM or all FAR-replicable VDMs between two eNAS systems, do the following:

### Procedure

1. Type the following command syntax:

```
$ nas_server -info -vdm {-all|<vdm_name>|id=<vdm_id>}
```

Where:

`-info -vdm {-all|<vdm_name>|id=<vdm_id>}` = Displays attributes for all VDMs, or a specified VDM, including the network interfaces.

Example:

To display information for a FAR-replicable VDM, type:

```
nas_server -info -vdm id=83
```

Output:

```
id           = 83
name         = my_vdm
acl          = 0
type         = vdm
server       = server_2
rootfs       = root_fs_vdm_my_vdm
I18N mode   = ASCII
mountedfs    =
syncreplicable = True
member_of    =
status       :
  defined    = enabled
  actual     = loaded, ready
Interfaces to services mapping:
```

---

### Note

The line of `syncreplicable` is not displayed for a non-FAR-replicable VDM.

---

## Delete a FAR-replicable VDM

### Before you begin

- There is no FAR session on the VDM.
- The VDM that is being deleted cannot contain mounted file systems.

To delete a FAR-replicable VDM, do the following:

### Procedure

1. Type the following command syntax:

```
$ nas_server -delete <movername>
```

Where:

`-delete <movername>` = Deletes either the specified physical Data Mover entry from the server table or deletes the VDM configuration.

Example:

To delete a FAR-replicable VDM, type:

```
$ nas_server -delete my_syncprep1
```

Output:

```
id = 3
name = my_syncprep1
acl = 0
type = vdm
server =
rootfs = root_fs_my_syncprep1
I18N mode = UNICODE
mountedfs =
member_of =
status :
defined = enabled
actual = permanently unloaded
Interfaces to services mapping:
```

### Results

The pool under the deleted VDM becomes a non-FAR-replicable VDM pool as a result of a successful Delete operation.

## List FAR session information

### Before you begin

Either the trusted communication channel (Control Station-to-Control Station communication) is ready between the two sites or the replicated NAS database is synchronized.

You can list all the FAR sessions of which the local system is either the active system or the standby system. To list the FAR session information, do the following:

### Procedure

1. At the local site, type the following command syntax:

```
$ nas_syncprep -list
```

Where:

`-list` = Displays all the configured FAR sessions on the local system's NAS database and those having the local system as the standby system in the remote system's replicated NAS database.

For example, to list FAR session information, type:

```
[nasadmin@LY2C6_CS0 ~]$ nas_syncprep -list
```

```
id      name                vdm_name      remote_system  session_status
4102    session1            vdm1          <--L9C16_CS0  in_sync
Warning 17727094793: The displayed status information could be stale if the nas
servers are not in required state.
```

And, type:

```
[nasadmin@L9C16_CS0 ~]$ nas_syncprep -list
```

```
id      name                vdm_name      remote_system  session_status
4102    session1            vdm1          -->LY2C6_CS0  in_sync
Warning 17727094793: The displayed status information could be stale if the nas
servers are not in required state.
```

### NOTICE

In the above output examples:

- The arrow direction in the list outputs above indicates the replication direction. '`-->`' means outgoing session from the side and '`<--`' means incoming session for the side.
- Warning 17727094793 is displayed to remind you of the dependency of the displayed sessions state on the NAS servers (Data Movers) state.

## Show FAR session information

### Before you begin

Either the trusted communication channel (Control Station-to-Control Station communication) is ready between the two sites or the replicated NAS database is synchronized.

To view FAR session information, do the following:

### Procedure

1. At the local site, type the following command syntax:

```
$ nas_syncprep -info {-all|<name>|id=<id>} [-verbose]
```

Where:

`-info {all|<name>|id=<id>} [-verbose]` = Displays the status of a specific configured FAR session, or the status of all FAR sessions.

Example:

To display status of a specific configured FAR session, type:

```
nas_syncprep -info -all
```

Output:

```
id = 4102
name = session1
vdm_name = vdm1
syncprep_role = active
local_system = L9C16_CS0
local_pool = src_sg1
local_mover = server_2
remote_system = LY2C6_CS0
remote_pool = src_sg1
remote_mover = server_2
device_group = 61_006_60_1857
session_status = in_sync
```

# Delete a FAR session

## Before you begin

The Control Station communication channel is ready for communication between the two sites.

To delete a FAR session, do the following:

## Procedure

1. At the source eNAS system site, type the following command syntax:

```
$ nas_syncprep -delete {<name>|id=<id>}
```

Where:

*<name>* = Name of the FAR session

*<id>* = Identifier of the FAR session

Example:

To delete a FAR session, type:

```
[nasadmin@L9C16_CS0 ~]$ nas_syncprep -delete session1
```

Output:

```
WARNING: Please do not perform any operation on session1 on
standby system until delete is done.
Deleting...done
```

## Results

The eNAS system removes the FAR session from the local NAS database.

## Note

After a FAR session is deleted, for the disk volumes in the mapped pool, their type will be updated (changed to the corresponding unmirrored type).

## **⚠ WARNING**

**The interfaces associated with the session on the standby site will remain in the DOWN state even after the session is deleted. Exercise caution in reusing them.**

## Extend bonded pool with FAR session

### Before you begin

The following prerequisites should be in effect:

- The bonded pool on which a VDM exists, should internally be a mapped pool.
- You must specify a valid FAR session name or ID.
- The FAR session cannot be in a `failover_failed` or `reverse_failed` state. The FAR session state should be in `_sync` while performing the `Refresh_pairs` operation.
- This procedure must be executed from the source site.

To add new LUNs to a FAR session after its mapped pool parameters size and count were validated, do the following:

### Procedure

1. Issue the following command from the source eNAS system site:

```
$ nas_syncprep -Refresh_pairs {-all|<name>|id=<id>}
```

Example:

To delete a FAR session, type:

```
$ nas_syncprep -Refresh_pairs session1
```

Output:

```
WARNING: You have just issued the nas_syncprep -Refresh_pairs command. Please do not
perform any operation(s) on the remote (R2) side during the same. Also note that the
operation cannot be reverted and will take sometime to complete depending upon the
local (R1) data that needs to be pushed to the remote (R2) side. Are you sure you
want to proceed? [yes or no] yes
Now validating local pool for session session1...
done
Now refreshing session session1...
done
```

## Modify network devices

### Before you begin

- The VDM to which the interfaces are attached to must be involved in a sync replication session.
- The devices on which the interfaces are created must also be involved in a sync replication session.
- The VDM must be a sync replicable VDM.

### **CAUTION**

**You must perform the procedure immediately after configuring new interfaces on the source side. Failing to do so will result in subsequent reverse/failover operations failing and leading to DU.**

To modify network devices:

## Procedure

1. Type the following command syntax:

```
$ nas_syncprep modify -network_devices  
syncreplicable=<local_device_name>:<remote_device_name>[,.  
..]
```

### Example:

To modify the network devices corresponding to a session, type:

```
nas_syncprep -modify sessionpn -network_devices cge-8:cge-8-0
```

### Output:

```
WARNING: You have just issued the nas_syncprep -modify -interfaces command. Please do  
not perform any operation(s) on the remote (R2) side during the same, In case of the  
command failure please make sure to create the interfaces manually on the remote (R2)  
side in down state. Are you sure you want to proceed? [yes or no] yes  
done
```

## Updating VNX OE software

When FAR is operational, do the following to update the VNX OE software:

1. Stop the FARM service.
2. On the destination site, update the VNX OE for File.
3. On the source site, update the VNX OE for File.

**NOTICE**

After you finish updating the VNX OE software:

- An admin must run the `nas_syncrep -Refresh_pairs -all` command for split brain fix to be applied to older FAR sessions.
- Verify that FAR is operational by using `nas_syncrep -list`.

## FAR Health Check

FAR Health Check analyzes VDM synch sessions for conditions and scenarios that can cause a failover or reverse operation to fail.

It is recommended that you periodically perform a FAR Health Check, say as a cron job, to monitor the health of VDM sync sessions. This will enable you to take proactive measures to help minimize the chances that a failover or reverse operation will fail.

The following lists the conditions and scenarios analyzed by FAR Health Check.

**Table 3** FAR Health Checks

Check	Description
SRDF group state	Checks if the relevant SRDF group exists and if it is in the correct state. The SRDF groups and the directors should be in the Online state for this check to pass.
SRDF session(s) status	Checks if the SRDF session is in the correct state. It checks for the existence and validity of the device groups associated with the VDM Sync sessions from the VMAX/PowerMax side.
VDM Sync session(s) disktype(s)	Checks for the disks to be of the correct type. All the disks involved in a VDM Sync session need to be of the same disk type.
File system has 128K free space	Checks if the File systems mounted on VDM have at least 128K free space. During failover or reverse, if file system to be mounted does not have at least 128K free space, the file system could be marked corrupt due to GID corruption.

**Table 3** FAR Health Checks (continued)

Check	Description
Network Configuration Check	Checks if VDM interfaces are present on the local and remote sites.
Check SRDF link status	Checks if the remote SRDF link is pingable, using the SymCli command.
Data Mover status	Checks if the Data Movers on the local and remote sites have reason codes four or five. A sample getreason output : 10 - slot_0 primary control station 11 - slot_1 secondary control station 5 - slot_2 contacted 5 - slot_3 contacted
eNAS, Solutions Enabler, Enginuity version check	Checks if the local and the remote have the same or in-family versions of eNAS, Solutions Enabler and Enginuity.
Filesystem ID consistency	Checks if the local and remote file system IDs overlap.
Pool to SRDF session mapping	Checks if all the devices from mapped pool are added to the SRDF session.
Director ports online/offline	Checks for the availability of VMAX/ PowerMax directors and ports related to eNAS.
Equivalent Data Services	Checks if the local and remote have equivalent data services like SLO (service level objective), SRP and Host I/O Limits.

The success of FAR health check does not guarantee that failover or reverse operations will succeed. The states of various entities involved in sessions, such as interfaces, and Data Movers can change over time, and could result in the failure of the failover and reverse operations. The health check is intended to be used for proactive monitoring of the VDM sync sessions.

## Performing FAR Health Check

To perform a FAR Health Check:

### Procedure

1. Run the command `nas_syncrep -health_check`.

Example:

```
nas_syncrep -health_check
```

Output:

```
Health check starting ...
Initializing ...
```

## Managing FAR sessions

Check No.	Check Name	Message ID	Status
	Brief Description		
Check ( 1/12 )	Check SRDF Group State SRDF Group online.	34906964006	PASS
Check ( 2/12 )	Check SRDF session(s) status SRDF session in sync.	34906964010	PASS
Check ( 3/12 )	Check VDM Sync session(s) disktype(s) VDM Sync session disktype ok.	34906964014	PASS
Check ( 4/12 )	File system has 128K free space File system has at least 128K free space.	34906964018	PASS
Check ( 5/12 )	Network Configuration Check Interfaces correct.	34906963984	PASS
Check ( 6/12 )	Check SRDF link status Remote SRDF is pingable.	34906963989	PASS
Check ( 7/12 )	Data Mover status Data movers are in the correct state.	34906963992	PASS
Check ( 8/12 )	eNAS, SE, Enginuity version check eNAS, SE and microcode version check passed.	34906963993	PASS
Check ( 9/12 )	Check for filesystem ID consistency No conflict in file system IDs.	34906963997	PASS
Check ( 10/12 )	Pool to SRDF session mapping VDM Sync session disktypes in correct state.	34906964014	PASS
Check ( 11/12 )	Check for director ports online/offline Directors and ports online.	34906963999	PASS
Check ( 12/12 )	Check for Equivalent Data Services Data services match.	34906964026	PASS

Health check complete.  
Check /nas/log/nas\_syncprep.log for more details.  
Use 'nas\_message -i <messageID>' to view detailed information about the message IDs.

# CHAPTER 7

## Managing Preserve ReplicatorV2 sessions for FAR.

This chapter explains how to manage Preserve ReplicatorV2 sessions for FAR. Topics include:

- [Preserve ReplicatorV2 sessions for FAR](#)..... 86
- [Best practices for Preserve RepV2 sessions](#)..... 86
- [Enable Preserve RepV2 sessions for FAR](#).....86
- [Create a ReplicatorV2 session on a FAR replicable VDM](#)..... 87
- [Show Preserve RepV2 session status](#)..... 88
- [Disable Preserve RepV2 sessions for FAR](#).....88
- [Restore ReplicatorV2 sessions](#)..... 89
- [Handle ReplicatorV2 sessions when Failover/Restore of FAR session is performed in FARM](#).....90

## Preserve ReplicatorV2 sessions for FAR

During a FAR session failover/reverse, existing ReplicatorV2 sessions are unavailable as the source objects move from Site A to Site B. Preserve RepV2 allows you to maintain DR connections during these operations by restoring the remote Filesystem ReplicatorV2 session associated with the VDM from the original source to the new source.

To use this feature:

- Enable the FAR service before implementing
- Create a ReplicatorV2 session from a FAR-replicable VDM to a non-FAR-replicable VDM

## Best practices for Preserve RepV2 sessions

Consider the following recommendations before using Preserve RepV2 sessions:

- Configure NTP servers on all the three sites eNAS systems to prevent time skew faults (note that time skew between the systems cannot be more than 10 minutes).
- Always make sure that the interfaces used in configuring the Control Station-to-Control Station interconnect are up. You can verify this by running the command, `nas_cel-interconnect-validate<interconnect_name>`

---

### Note

For the interconnect, use the DM interface, not the interface attached to the VDM.

---

- If the NAT IPs of any of the sites is changed, then it should be updated in the other two sites using the command, `nas_cel -modify { <cel_name> | id=<cel_id> } { [-passphrase <passphrase>] [-name <new_name>] [-ip <ipaddr>[,<ipaddr>, ...]] }`

## Enable Preserve RepV2 sessions for FAR

### Before you begin

You can enable this feature on eNAS only if:

- The FAR service enabled.
- The Data Movers have the correct operating software version.
- The system has the RepV2 license enabled.

ReplicatorV2 sessions are asynchronous.

### Procedure

1. To enable the Preserve RepV2 sessions for FAR, type the following command on Site A or Site B:

```
nas_syncprep_rr -config -enable
```

## Output:

```
Enabling "Preserve RepV2 for SyncRep" on local array Enabled Successfully
Enabling "Preserve RepV2 for SyncRep" on remote array Enabled Successfully
```

## Create a ReplicatorV2 session on a FAR replicable VDM

### Before you begin

A FAR session must already be created.

### Procedure

1. Create the following Control Station-to-Control Station relationships by using the `nas_cel` command:
  - Site A to Site C
  - Site C to Site A
  - Site B to Site C
  - Site C to Site B
2. Create the following interfaces on three sites from the same subnet (that is, every interface should be reachable from the other sites) by using the `server_ifconfig` command:
  - Site A
  - Site B
  - Site C

---

### Note

The interconnect ips for RepV2 should be different from that of the VDM interfaces.

---

3. Create the following interconnects by using the `nas_cel interconnect` command:
  - Site A to Site C
  - Site C to Site A
  - Site B to Site C
  - Site C to Site B
4. On Site C:
  - a. Create a new VMAX/PowerMax storage group.
  - b. Create LUNs.
  - c. Add LUNs to the storage group.
  - d. Run a **Rescan**.
  - e. Create a new, non-sync-replicable VDM with the just created storage pool.
  - f. If using CIFS, make sure that the CIFS service is started.

5. On Site A, create a new ReplicatorV2 session for a file system from Site A to Site C. Put the destination file system on the newly created pool.
6. On Site B:
  - a. Run either a reverse or failover operation on the FAR session.
  - b. Run the `nas_syncrep_rr -restore -vdm <vdm_name>` command.
  - c. Run the `nas_syncrep_rr -free_intermediate_data` command.
  - d. Run the `nas_replicate -list` command at Site B to see if the RepV2 session is restored.

### Results

The replication session should now appear on System B.

---

### Note

Configuring Preserve RepV2 sessions along with FAR sessions will add an amount of time proportional to the number of IP Replication sessions configured on a particular VDM's FAR session to the service outage time of a Planned failover. In the case of an Unplanned failover (Disaster scenario) and reverse, there will be no impact on the outage time.

---

### Note

---

## Show Preserve RepV2 session status

### Procedure

1. To show the Preserve RepV2 session status, type the following command on either Site A or Site B:

```
nas_syncrep_rr -config -info
```

Output:

```
Configuration for "Preserve RepV2 for SyncRep" on remote array:      Preserve Repv2
is Enabled
Configuration for "Preserve RepV2 for SyncRep" on local array:      Preserve Repv2 is
Enabled
```

## Disable Preserve RepV2 sessions for FAR

### Procedure

1. To disable Preserve RepV2 sessions for FAR, type the following command on either Site A or Site B:

```
nas_syncrep_rr -config -disable
```

Output:

```
Disabling "Preserve RepV2 for SyncRep" on local arrayDisable Successfully
Disabling "Preserve RepV2 for SyncRep" on remote arrayDisable Successfully
```

## Restore ReplicatorV2 sessions

### Before you begin

You must have the Preserve RepV2 session for FAR feature enabled.

You must have ReplicatorV2 sessions configured on the FAR-replicated VDM.

### Procedure

1. To restore ReplicatorV2 sessions, use the following command syntax from the eNAS system to where FAR sessions have been failed over or reversed:

```
nas_syncprep_rr
| -restore {-all | -vdm {<vdm_name> | id=<vdm_id>}}
```

where:

`-all` = Restores all ReplicatorV2 sessions on all VDMs.

`<vdm_name>` = The name of a specific VDM on which you want to restore ReplicatorV2 sessions. The VDM specified must be a sync-replicable VDM.

`<vdm_id>` = The ID of a specific VDM on which you want to restore ReplicatorV2 sessions. The VDM specified must be a sync-replicable VDM.

Using the `-all` option may take some time for the operation to complete. Check the operation's status by running the `nas_task -info <task_id>` command.

Output:

```
$ nas_syncprep_rr -restore -all

Info 26316963879: Command result: The nas_syncprep_rr command may take a long time to
complete, please avoid performing any syncprep operations for related vdm(s) during
restore, use nas_task to check task {id = 47559} status. Follow up by running "/nas/
sbin/syncprep/RestoreRepv2/nas_syncprep_rr -free_intermediate_data" command to clean
all the intermediate data after restore finish.
OK

$ nas_task -info 47559
Task Id = 47559
Celerra Network Server = siteB
Task State = Succeeded
Movers =
Description = repv2_ssn1,Succeeded,Reconstruct Repv2
id=514_000197600066_084C_200_000197900043_084C successfully
             repv2_ssn2,Succeeded,Reconstruct Repv2
id=516_000197600066_084C_207_000197900043_084C successfully
             repv2_ssn3,Succeeded,Reconstruct Repv2
id=518_000197600066_084C_214_000197900043_084C successfully

Originator = nasadmin@cli.localhost
Start Time = Mon Dec 04 10:02:14 EST 2017
End Time = Mon Dec 04 10:05:29 EST 2017
Schedule = n/a
Response Statuses = Info 26316963879: Command result: The nas_syncprep_rr command
may take a long time to complete, please avoid performing any syncprep operations for
related vdm(s) during restore, use nas_task to check task {id = 47559} status. Follow
up by running "/nas/sbin/syncprep/RestoreRepv2/nas_syncprep_rr -free_intermediate_data"
command to clean all the intermediate data after restore finish.
OK
```

2. Run the following command after the restore command succeeds :

Managing Preserve ReplicatorV2 sessions for FAR.

```
nas_syncprep_rr -free_intermediate_data
```

Output:

```
Clean renamed internal ckpts for successfully restored RepV2 sessions:
  Clean Count: 12      Success: 12      Fail: 0

Free_intermediate_data Done
```

3. Run the following command to see the the restored ReplicatorV2 sessions:

```
nas_replicate -list
```

Output:

```
Name          Type          Local Mover Interconnect Celerra Status
elm_rep_ssn1  filesystem    server_2 -->siteA_siteC siteC    OK
```

4. After restoring, run the following command on the previous source site (for example, Site A) to clean broken ReplicatorV2 sessions:

```
nas_syncprep_rr -clean -server server_2
```

Output:

```
Now start cleaning up DART BDBs as well as all broken repV2 sessions.
/nas/quota/slot_2/.etc/dp/session
Deleting server_2 repV2 session info.                                done
```

## Handle ReplicatorV2 sessions when Failover/Restore of FAR session is performed in FARM

### Before you begin

When FARM automatically triggers a FAR session to failover, the underlying IP replication session breaks.

### Procedure

1. To view the broken IP replication sessions to be restored at the new site (Site B), type the following command:

```
nas_syncprep_rr -list
```

Output:

```
Session Name  VDM Name Local FS/VDM Remote FS/VDM CMU Restore State Session Type
elm_rep_ss+   vdm1     4120    4120    00019710000700013 ToBeRestored Remote
```

2. To restore the broken IP sessions, complete the procedure in [Restore ReplicatorV2 sessions](#) on page 89.

---

**Note**

Stop the FARM service when performing the restore operation and restart it after the restore is complete.

---

Managing Preserve ReplicatorV2 sessions for FAR.

# CHAPTER 8

## FAR service checklists

This chapter provides checklists that you can use to verify the FAR configuration.

Topics include:

- [Enable FAR service checklist](#)..... 94
- [FAR session checklist](#).....95

## Enable FAR service checklist

After enabling the FAR service, answer the questions in the following checklist to determine if there are issues with your service setup. If you answer no to any of these questions, you should troubleshoot those issues to resolve them.

**Note**

Symmetrix Access Controls used by eNAS is a base control and any change from that should require qualification/review, etc.

**Table 4** FAR service setup checklist

Service setup	yes/no
<p>Does the <code>nas_cel</code> connection from System 1 to System 2 exist? (Use the <code>nas_cel -list</code> command to determine the status.)</p> <hr/> <p><b>Note</b></p> <p>For eNAS Systems with dual Control Stations, both destination Control Station IPs should have been added in the <code>nas_cel</code> command for the remote system.</p>	
<p>Does the <code>nas_cel</code> connection from System 2 to System 1 exist? (Use the <code>nas_cel -list</code> command to determine the status.)</p> <hr/> <p><b>Note</b></p> <p>For eNAS Systems with dual Control Stations, both destination Control Station IPs should have been added in the <code>nas_cel</code> command for the remote system.</p>	
<p>Is the FAR service enabled? (Use the <code>nas_cel -syncrep -list</code> command to determine the status.)</p> <hr/> <p><b>Note</b></p> <p>Under the <code>syncrep</code> column, the service should be showing 'enabled' for the appropriate <code>nas_cel</code> ID.</p>	
<p>Run a <code>/nas/bin/nas_checkup</code> on both eNAS Systems. Are the eNAS Systems in a healthy state?</p>	

## FAR session checklist

After creating each FAR session, answer the questions in the following checklist to determine if there are issues with the session. If you answer no to any of these questions, you should troubleshoot and resolve them.

**Table 5** FAR session creation checklist

FAR session creation	yes/no
Is the FAR session state either in progress of sync or in sync? (Use the <code>nas_syncrep -list</code> command to determine the status.)	
Are all of the VDM network interfaces pingable? (Depending on the network configuration, use the <code>server_ping</code> or <code>ping</code> command to determine the status.)	
Are all of the CIFS or NFS shares accessible? (Request that the customer provide this information.)	
Run a <code>/nas/bin/nas_checkup</code> on both eNAS Systems. Are the eNAS Systems in a healthy state?	



# CHAPTER 9

## Troubleshooting FAR

As part of an effort to continuously improve and enhance the performance and capabilities of its product lines, Dell EMC periodically releases new versions of its hardware and software. Therefore, some functions described in this document may not be supported by all versions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

If a product does not function properly or does not function as described in this document, contact your Dell EMC Customer Support Representative. Problem Resolution Roadmap for VNX contains additional information about using Dell EMC Online Support and resolving problems.

Topics include:

- [Retrieve information from log files](#)..... 98
- [Error messages](#)..... 99
- [Troubleshooting scenarios](#)..... 99

## Retrieve information from log files

System messages are reported to the system log files. To retrieve information from log files:

- Check the system log (`sys_log`) by using the `nas_logviewer` command.
  - Check the server log (`nas_server.log`) by using the `server_log` command.
  - Check the command error log (`cmd_log.err`) for message information.
  - Check the syncrep log (`nas_syncrep.log`) for message information.
  - Collect the state of the system by running the `/nas/tools/collect_support_materials`.
  - Check Solutions Enabler logs (`symapi.log`) for message information.
- 

### Note

In the case of the syncrep log, during a reverse/failover operation, the level will be changed to DEBUG and it will be changed back after the reverse/failover operation finishes. To turn on the DEBUG flag, set `export NAS_SYNCREP_DEBUG=1`.

---

Checks have been added to `nas_checkup` for synchronous replication health. If an error or warning is detected during a scheduled `nas_checkup` run, it will be included in one single Checkup alert. The alert can be viewed through Unisphere (for VNX).

## Error messages

All event, alert, and status messages provide detailed information and recommended actions to help you troubleshoot the situation.

To view message details, use any of these methods:

- Unisphere software:
  - Right-click an event, alert, or status message and select to view Event Details, Alert Details, or Status Details.
- CLI:
  - Type `nas_message -info <MessageID>`, where `<MessageID>` is the message identification number.
- *Celerra Error Messages Guide*:
  - Use this guide to locate information about messages that are in the earlier-release message format.
- Dell EMC Online Support:
  - Use the text from the error message's brief description or the message's ID to search the Knowledgebase on [Dell EMC Online Support](#). After logging in to Dell EMC Online Support, locate the applicable **Support by Product** page, and search for the error message.

## Troubleshooting scenarios

This section describes common troubleshooting scenarios.

### **Failover fails if VDM interface is used by other services**

Ensure that the interfaces used by VDM are not used by `server_cifs` on the R2 (even in state DOWN). Otherwise, a failover will fail when trying to make the interface UP and probably lead to a DU scenario. In such a scenario, remove the interface usage by CIFS service by using a `server_cifs nas cli`.

### **nas\_syncprep commands are idempotent and can be re-run in case of failure**

In situations when `nas_syncprep` commands (`create`, `failover`, `Clean`, `reverse`, `Refresh_pairs` or `start`) fail, you can safely re-run them. For example, `Refresh_pairs` can time out in some situations waiting for the synchronization of newly added devices to succeed. In such cases, `Refresh_pairs` will fail and the state of the session will be `refresh_failed`. An administrator can retry the command and if the session becomes synchronized, the operation will succeed.

### **Ensure time skew is fixed for primary and secondary CS**

If NTP is not configured, then ensure the time skew between the primary and secondary CS (both local and remote sites) is fixed. Otherwise, VDM syncprep operations will fail in the event of CS failovers. This can also impact the VDM session failovers. Use the `nas_cs -set -time <yyyymmddhhmm[ss]>` and ensure that all the four CS's are time synchronized.

### **Protect or migrate existing file systems on DMs**

To protect existing file systems, consider the following methods:

- If the existing FS(s) uses one mapped pool, do the following
  1. Create a new VDM Sync Replication Service between the local & remote systems.

2. Create a new sync replicable VDM and attach an external IP interface to it.
  3. Unexport the FS from the Data Mover.
  4. Unmount the FS from the Data Mover.
  5. Create a VDM Sync Replication Session (on the FS's mapped pool) between the local & remote systems.
  6. Mount the FS on the newly created VDM.
  7. Export the FS from the newly created VDM.
  8. Configure other required configuration wrt networking, usermapper, NFS/CIFS on VDM.
- If the existing FS spans across multiple mapped or user defined pools (for example, created using a meta volume), do the following:
    1. Create (using `nas_diskmark`) a new mapped pool by exporting a new SG on the array.
    2. Create a new VDM Sync Replication Service between the local and remote systems.
    3. Create a new FS on the new mapped pool.
    4. Mount the new FS on the newly created VDM.
    5. Export the new FS from the newly created VDM.
    6. Manually copy (using `nas_copy`) the existing FS data contents to the new FS (which is mounted as CIFS or NFS share) from the NAS host.
    7. Create a new sync replicable VDM and attach an external IP interface to it.
    8. Configure other required configuration wrt networking, usermapper, NFS/CIFS on VDM.
    9. Create a VDM Sync Replication Session (on the newly created mapped pool) between the local and remote systems.

**Retry the VDM Syncprep enable operation if mounting the replica fails**

When a VDM Syncprep Service Enable operation fails to mount the local replica (or LUN9), a retry of mount LUN9 is triggered. For example:

```
$ nas_cel -syncprep -enable RZBCK-CS0 -local_fsidge 4096,12287 -remote_fsidge 12288,24575 -local_storage 000296800196 sym_dir=1f:10,2f:10 rdf_group=107 -remote_storage 000296800192 sym_dir=1f:10,2f:10 rdf_group=107
Now saving FSID range [12288,24575] on remote system... done
Now saving FSID range [4096,12287] on local system... done
Now creating LUN mappings (may take several minutes)... done
Now adding CTD access to local server server_2... done
Now adding CTD access to local server server_3... done
Now creating mountpoint for sync replica of NAS database... done
Now mounting sync replica of NAS database... failed
Now mounting sync replica of NAS database... done
Now enabling sync replication service on remote system... done
Warning 17726964343: Ensure the source and remote Control Stations (primary and secondary) are time synchronized, if not already taken care.
done
```

Do the following:

- If the device `sdj` cannot be found locally, check the masking view for LUN9.
- If the device `sdj1` cannot be found locally, do one of the following locally:

- Run `$ symcfg discover' & '$ symcfg list -ra all`
- RDF session from remote LUN4 to local replica LUN9 using the command `$ symrdf list`. If the session is in SyncInProg, wait until it is Synchronized.
- Run `$ /sbin/partprobe sdj` on the local Embedded NAS system.



# PART 2

## File Auto Recovery Manager

This section describes how to use FARM to manage aspects of a FAR environment.

Chapters include:

[Chapter 10, "Installing FARM"](#)

[Chapter 11, "FARM operations"](#)

[Chapter 12, "Uninstalling FARM"](#)

[Chapter 13, "Additional FARM information"](#)

[Chapter 14, "Troubleshooting FARM"](#)



# CHAPTER 10

## Installing FARM

This chapter presents the following topics:

- [Installation Requirements](#)..... 106
- [Installing FARM](#).....107

## Installation Requirements

FARM must be installed on a Windows system with LAN access to the administration LAN. This access path is used to reach the Dell EMC eNAS Control Stations to be monitored.

Observe these requirements:

- Install and test eNAS.
- Ensure a LAN connection exists between the eNAS Control Stations and the administrator system on which FARM operates.
- Ensure that a connection between the FARM host and the eNAS networks exists to detect eNAS availability. The FARM host pings the eNAS service through the eNAS networks.
- Ensure there is 200MB of disk space available for the FARM binary and installation files.
- For best performance, your system requires a Quad-core processor (4 cores) operating at 2.0 Ghz and 8GB of RAM.
- Internet Control Message Protocol (ICMP) must be enabled on the Windows host.
- Port 111 must be open on the network.
- FARM is only available on 64 bit versions of the following operating systems:
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2008 R1
  - Windows Server 2008 R2
  - Windows 7
- FARM requires Administrator privileges.

# Installing FARM

## NOTICE

It is recommended to install FARM on a remote host (VM) and not at the primary or the secondary sites.

---

To install FARM:

### Procedure

1. Download the installation package (eNAS-FARM-Win-64-x64-en\_US-6.0.17) from Dell EMC Online Support at <https://support.EMC.com>:
- 

#### Note

FARM version (eNAS-FARM-Win-64-x64-en\_US-6.0.17-1.exe ) is compatible with the mentioned eNAS version (8.1.13.xx).

---

2. Run the installer program file as Administrator. The last step of the installation requires you to restart Windows.
- 

#### Note

The installer creates a shortcut on the desktop. Create the Administrator user before starting FARM.

---

3. If you are installing FARM on a system on which FARM was previously installed, the following message displays:

```
File Auto Recovery Manager Configuration data found --  
Would you like to restore these settings during  
installation -> Yes or No
```

Click **Yes** to maintain your existing configuration or **No** to delete it.

4. On the **Introduction** page, click **Next**.
5. On the **License Agreement** page, select the option to accept the license agreement and click **Next**.
6. On the **Choose Install Folder** page, click **Next** to accept the default directory, or click **Choose** to select another directory, and the click **Next**.
7. On the **Pre-Installation Summary** page, verify the summary information, and click **Install** to continue the installation.
8. On the **Install Complete** page, click **Done**.



# CHAPTER 11

## FARM operations

This chapter presents the following topics:

- [Configure operations](#)..... 110
- [Management operations](#)..... 113

## Configure operations

This section explains the FARM configure operations.

### Prerequisites

The FAR functions in FARM rely on:

- A fully configured and tested FAR replication environment comprised of only eNAS models.
- FAR is configured for two site in synchronous mode.

Configuration of the FAR environment is described in the Part 1 of this guide. Observe the requirements listed there.

### The File Auto Recovery Manager Configuration wizard

The first time you open FARM, the Configuration wizard starts. With this wizard you can:

- Configure storage systems
- Configure failover operations:
  - Set a VDM Network to "Failed" when either All network interfaces fail or Any VDM network interface fails. This setting applies for each VDM; failover occurs on one or more sessions that have failed.
  - Set the VDM failover retry count.
- Configure SMTP (email) alerts. If you are not configuring SMTP, you must clear the checkbox. FARM will generate and send an email in the following circumstances:
  - VDM is in error or warning
  - FARM monitored event fails
  - FARM detects a VDM error and triggers a failover
  - FARM triggered failover fails
  - Failover is successful
- Optionally configure pre-failover and post-failover scripts.
- View a summary page of your configuration choices.

### Configuring FARM

This topic describes how to use the **File Auto Recovery Configuration** wizard to configure FARM to monitor the FAR replication environment. The wizard launches automatically the first time you open FARM.

#### Procedure

1. If the **File Auto Recovery Manager Configuration** wizard is not already running, start it by selecting **Configure > Configuration**.
2. On the **Storage Systems** page, specify the NAT IP addresses and the credentials used to communicate with the eNAS control stations. For the secondary site information, you can either specify the information, or select the **Use primary site credentials to discover secondary site** to have FARM

automatically discover it. In the secondary site, if CS is in a failed over state, explicitly specify the secondary information NAT IP and credentials.

3. On the **Failover Options** page:
  - a. Specify the VDM network failure criteria:
    - **All VDM network interfaces fail:** Indicates that a failover should occur only when all network interfaces have failed.
    - **Any VDM network interface fails:** Indicates that a failover should occur when a single network interface fails
  - b. Specify the number of times FARM should retry a VDM failover. The default value is three.
  - c. Specify an IP address for the Remote Target to ensure that FAR network isolation is detected if it occurs. Select an IP address that is external to the Primary and Secondary sites, but still in the same subnet.
4. Optional: On the **SMTP** page, specify to **Send a warning message when critical service failure is detected**, and then do the following.
  - a. Specify the **SMTP Sever** name and **Port** of the mail server.
  - b. Specify the email address **From** which the message will be delivered.
  - c. Specify the email address **To** which the message will be delivered.
  - d. Specify a **Subject** line for the email.
  - e. Click **Send Test Message** to verify the configuration.
  - f. Verify that the message was received.

When discovery completes, the summary page opens displaying details on the eNAS and VDM configurations. At the same time, discovered VDMs display on the main dashboard.

5. Optional: On the **Advanced Configuration** page, specify tasks or scripts to run before and/or after a failover operation. These will be executed on the Windows host and not on the eNAS control station.
6. On the **Summary** page, verify your selections, and then click **Discover** to start the discovery process. When the process completes, discovered VDMs will display on the main **File Auto Recovery Manager** window.
7. To start the automated failover monitoring, click **Start** on the main **File Auto Recovery Manager** window.

The FARM Service is now active. Failovers will now occur automatically, when failover conditions exits.

## Resetting FARM

To clear the entire existing eNAS and VDM configuration:

### Procedure

1. On the main **File Auto Recovery Manager** window, select **Configure > Reset configuration**
2. Click **OK** in the confirmation message.

### **Results**

Once the configuration is cleared, you will have to reconfigure FARM using the Configuration wizard. [Configuring FARM](#) on page 110 explains the process.

## Management operations

This section explains the FARM management operations.

### Configure a synchronous replication session's failover policy

#### Before you begin

- Systems must be imported into FARM, and synchronous replication sessions must be configured on those systems.
- The FARM service must be stopped before you can set a failover policy for a VDM session.

You can configure a synchronous replication session to failover automatically when the FARM service is started, or you can manually run failover or reverse operations.

The following identifies the events that return warnings, and the events that cause failovers:

**Table 6** Monitored events

Event	Warning	Failure	Description
Remote Ping	X		Check the remote IP ping
Primary Site CS0	X		Check the /nbsnas mount on the primary site Control Station
Primary Site CS1	X		Check the /nbsnas mount on the primary site standby Control Station
Secondary Site CS0	X		Check the /nbsnas mount on the secondary site Control Station
Secondary Site CS1	X		Check the /nbsnas mount on the secondary site standby Control Station
Primary Site Data Mover		X	Check the Data Mover status of the primary site
Secondary Site Data Mover	X		Check the Data Mover status of the secondary site
VDM interface check		X	Send a Ping request to interfaces on a VDM under replication
VDM file system check	X		Access a file system mounted on a VDM under replication
VDM Local LUN status check		X	Check whether the status of the local LUNs used by the VDM are either ERROR or DEGRADED

**Table 6** Monitored events (continued)

Event	Warning	Failure	Description
VDM Remote LUN status check	X		Check whether the status of the remote LUNs used by the VDM are either ERROR or DEGRADED
SyncRep inter-connection check	X		Check the inter-connection status of the synchronous replication session
SyncRep session check	X		Check the synchronous replication session status

**Procedure**

1. On the main **File Auto Recovery Manager** window, select a VDM session for which you want to set a policy.
2. Click the **Edit** (pencil) icon.
3. Set **Failover Policy** to either **Auto** or **Manual**.

The Failover Policy is effective once the FARM service is started. By default, automatic failover is configured for all monitored VDM sessions. To control certain sessions manually, select specific VDM sessions and set each policy to **Manual**. FARM will monitor and automatically failover VDM sessions set to **Auto**. FARM will only monitor VDM sessions set to manual; it will not automatically failover manual sessions. Setting VDM sessions to manual allows you better control over which sessions failover.

4. Click **OK**.

**Configure a synchronous replication session's failover priority****Before you begin**

- The FARM service must be stopped before you can set a failover priority for a synchronous replication session.
- A synchronous replication session must be configured as Auto before configuring a failover priority.

**Procedure**

1. On the main **File Auto Recovery Manager** window, select a VDM session for which you want to set or change a failover priority.
2. Use the Up and Down arrows to move the session up or down on the priority list.

Alternatively, you can click the **Edit** (pencil) icon, and then select the **Failover Priority** from the drop-down list (Priority 1 will failover first).

3. Click **OK**.

**Select VDM IP addresses to monitor****Before you begin**

The FARM service must be stopped before you can set IP addresses to monitor.

**Procedure**

1. On the main File Auto Recovery Manager window, select a VDM session for which you want to manage.
  2. Click the **Edit** (pencil) icon.
  3. In **Monitor Network**, select either the **All IP Address** checkbox to monitor all IP addresses, or select specific IP addresses from the list box.
- 

**Note**

If no IP addresses are selected, the Failover Policy changes to **Manual**.

---

4. Click **OK**.

**Results**

Any network interfaces that are not selected are not monitored by FARM. A failure on them will not be detected, and will not initiate an automatic failover.

**Start the FARM service**

To start the FARM service:

**Procedure**

1. Open the File Auto Recovery Manager software.
2. On the main window, click **Start**.

**Results**

The service that runs is called "EMC FARM service" with a description of "EMC File Auto Recovery Manager".

When the FARM service is running, FARM monitors all configured VDM services on the primary site. When a VDM service failure is detected by FARM, the failed VDMs sessions are failed over from the primary site to the secondary site. If multiple VDMs failed, the VDMs are failed over based on the configured priority. If the failover of a session fails, FARM continues failing over lower-priority sessions before retrying.

---

**Note**

If a local standby Data Mover is configured, the service delays the failover operation for 20 seconds to allow for the local standby to be initiated. If local failover is detected, then the service waits an additional 300 seconds before issuing the next check to allow the local failover to complete.

If a local standby Data Mover is not configured, these delays are skipped.

---

**Stop the FARM service**

Prior to performing any of the following operations, you must stop the FARM service:

- Planned maintenance or service procedure at the primary or secondary site
- Running an eNAS upgrade
- Running FARM discovery
- Performing a manual Failover/Reverse/ Restore operation
- Performing any VDM configuration change such as deleting VDM sessions, unmounting FS, and removing devices from bonded pools.

To stop the FARM service:

#### Procedure

1. On the main **File Auto Recovery Manager** window, click **Stop**.

## Manually failover a synchronous replication session

#### Before you begin

The automated failover service cannot be running during a manual failover operation. Stop the service if it is still running.

---

#### Note

Do not run a failover operation if the source system is accessible. If it is available, run a reverse operation instead.

---

The **VDM Failover** procedure fails over the selected VDMs from the primary site to the secondary site. This procedure brings the remote VDM, file systems, and related network interfaces online.

Perform the **VDM Failover** procedure when a disaster or other serious error occurs at the primary site, and you want to switch service to the secondary site. Failover occurs automatically if the FARM Service is configured for Automated Failover (preferred) and it is running.

**VDM Failover** will perform the Clean operation on the original primary site, if available. If not, manually clean-up the Control Station, as described in [VDM Failover scenario](#) on page 119.

#### Procedure

1. On the main **File Auto Recovery Manager** window, verify that the Service State is Stopped. If not, click **Stop**.
2. Select one or more VDMs that you want to failover from your source array to the destination array.
3. Click **Failover**.

#### After you finish

Once the failover is complete, a message window opens to show that the priority set for each VDM has changed.

## Cleaning synchronous replication sessions

FARM has the capability to perform an auto configuration clean operation of R1 site. The auto clean will be triggered after failover - in both manual and automated failovers. Auto clean is triggered once all of the selected VDMs have completed the failover process. If some of the VDMs failed to perform failover, Clean is still triggered keeping in mind that some of sessions were successfully failed over. If none of the selected VDMs are failed over, auto clean is not triggered. Auto clean is executed through `nas_crond` command on R2 site which internally executes the `nas_syncprep -Clean -all` command on R1 site. Once the `nas_crond` is triggered by FARM, check the status of the clean operation through through the CLI since FARM does not show the status of the `nas_crond` task. Since `nas_crond` is executed as a background task, FARM cannot track the status.

## Manually reverse a synchronous replication session

### Before you begin

The automated failover service cannot be running during a manual Reverse operation. Stop the service if it is still running.

A manual reverse operation allows you to manually select all VDMs or a subset of VDMs to move to your destination system.

### Procedure

1. On the main **File Auto Recovery Manager** window, verify that the Service State is Stopped. If not, click **Stop**.
2. Select one or more VDMs that you want to move from the source eNAS to the destination eNAS.
3. Click **Reverse**.

### After you finish

Once the reverse is complete, a message window opens to show that the priority set for each VDM has changed.

## Manually restore a synchronous replication session

A manual restore operation allows you to manually restore any reversed or failed over VDMs back to their original source eNAS. If necessary as part of the restore operation, a clean operation is also performed.

### Before you begin

- VDMs must be in the Reversed or Failed over state before you can run a Restore operation.
- If the VDM has been failed over, you must have resolved the issue with the source system/VDM that caused the failover.

### Procedure

1. On the main **File Auto Recovery Manager** window, verify that the Service State is Stopped. If not, click **Stop**.
2. Select one or more VDMs with a Reversed or Failed over state that you want to move from the destination eNAS back to the source eNAS.
3. Click **Restore**.

## Collecting logs

The Main Log window information is captured in the `farm.main.log` file, found in the `C:\<Program Files>\EMC\VMSM\log` folder. Note that the `<Program Files>` folder name depends on the version of Windows being used.

To create a collection log to help with troubleshooting issues:

### Procedure

1. On the main **File Auto Recovery Manager** window, select **Help > Log Collection**.
2. By default, the Log Collection tool creates a zip file, and saves the collection's zip file to the Desktop.

## Discover monitored objects

If any of the following changes occur to the monitored storage system configuration, you must discover the configuration again:

- Session additions
- IP address changes
- OE software upgrades
- VDM network interface changes
- VDM NFS/Exports
- VDM file system changes
- VDM additions or deletions
- eNAS upgrades

### Procedure

1. On the main **File Auto Recovery Manager** window, verify that the Service State is Stopped. If not, click **Stop**.
2. To discover monitored objects, select **Management > Discover**.

### Results

After discovery, the VDM status of VDMs on the Primary site will be shown as "--". The VDM status of VDMs on the Secondary site will be shown as "Reversed".

## How to resolve discovery errors

Since discovery is important for subsequent steps performed by FARM, you must resolve errors. If discovery concludes with errors, an error message appears. Review the log and resolve the error.

The following table shows possible errors, their causes, and how to resolve them.

**Table 7** Errors, causes, and remedies

Error	Cause	Remedy
Control Station NAT IPs are invalid or nasadmin password is invalid	Three possible causes include: <ol style="list-style-type: none"> <li>1. The Control Stations are not reachable.</li> <li>2. The nasadmin login credential is invalid.</li> <li>3. The NAT IPs entered are invalid</li> </ol>	<ol style="list-style-type: none"> <li>1. Verify that the Control Stations are reachable.</li> <li>2. Verify the nasadmin credentials were entered correctly.</li> <li>3. Verify that the NAT IPs are valid.</li> </ol>

## Check status

### Before you begin

You must have existing VDM sessions to check their status.

To perform a health check on the VDM sessions and generate a log of each event status and the overall VDM status:

### Procedure

1. On the main **File Auto Recovery Manager** window, select **Management > Check Status**.

Status information appears in the Main log which displays in the lower pane of the window. The earliest messages display at the beginning of the log, and the latest messages display at the end of the log.

- Fatal, Error, and Warning messages are highlighted within the Main log. If you want to change the color for a highlight, or add messages to be highlighted, click **Highlighting**.
- If you want to display only the status messages with highlights, select **Only Highlighted**.
- To always display the most current log entries first, select **Follow Tail**. If you do not select **Follow Tail**, then the oldest entries are displayed first.

## Show synchronous replication status

To view the states and events for synchronous replication sessions:

### Procedure

1. On the main **File Auto Recovery Manager** window, select one or more synchronous replication sessions.
2. Click the **information** icon.

## Viewing the eNAS log

The **Main Log window**, shown at the bottom of the main **File Auto Recovery Manager** window, monitors and displays all logs instantly. There is no need to refresh the view for every new log. Selecting the **Follow Tail** option specifies to monitor the logs. Clearing the option specifies to not monitor the logs.

## VDM use cases

Two typical scenarios include:

- Unplanned VDM failover from primary to secondary site (VDM Failover)
- Planned maintenance at the primary site (VDM Reverse)

### VDM Failover scenario

In this scenario, a disaster or other serious failure occurred at the primary site.

#### Procedure

1. If the FARM Service was enabled and active, the failover already occurred automatically. Go to step 4.
2. If failover did not occur automatically, run a manual failover.
3. After a successful failover, verify that the status indicates "Failed over" in the main **File Auto Recovery Manager** window.
4. If the FARM service is running, stop it.
5. Verify that the VDM sessions are cleaned up and the sessions are in-sync. FARM will execute a auto clean after the failovers. If the auto clean operation failed for some reason, perform a manual clean operation in CLI.

6. Perform a restore operation.
7. Restart the FARM Service.

## VDM Maintenance Scenario (VDM Reverse)

In this scenario, service personnel determine that the load at the primary site requires rebalancing.

### Procedure

1. On the main **File Auto Recovery Manager** window, reverse the replication session.
2. After a successful reverse, verify that the VDM policy and priority are assigned.
3. When the maintenance tasks are completed at the primary site and the system is fully operational, restore the reversed VDM to the primary site. The secondary site goes offline (standby).
4. Restart the FARM Service.

# CHAPTER 12

## Uninstalling FARM

This chapter presents the following topics:

- [Uninstall FARM](#)..... 122

# Uninstall FARM

To uninstall FARM:

## Procedure

1. From the **Windows Start** menu, select **Programs and Features > eNAS File Auto Recovery Manager**, and click **Uninstall**.
2. Do one of the following:
  - To uninstall FARM, select **Uninstall eNAS File Auto Recovery Manager**.
  - To repair FARM, select **Repair/Reinstall**.
3. Click **Next**.
4. If uninstalling FARM, optionally select **Restart**, and click **Next**. If repairing FARM, optionally select **Run eNAS File Auto Recovery Manager**, and click **Next**.

# CHAPTER 13

## Additional FARM information

This chapter presents the following topics:

- [FARM limitations](#)..... 124
- [Best practices](#)..... 124
- [VDM state and status information](#)..... 125
- [Event status/level](#)..... 126
- [VDM event list](#)..... 127
- [FARM Environment Data Collect Sheet](#)..... 128
- [Refreshing session state information in FARM](#)..... 128

## FARM limitations

The following lists some of the limitations with eNAS File Auto Recovery. For a complete list, refer to the *PowerMax Embedded NAS Release Notes*.

- To monitor FAR sessions on both the primary and the secondary sites, you must install and configure FARM on two administrator hosts, one monitoring each site. Any failed over session by FARM monitoring one site will not be captured and monitored by FARM monitoring other site. In such an event, you should run discovery. This limitation also applies to manual operations. After a manual operation in one FARM, discovery has to be executed in the other FARM.
- Discovery performed as part of basic wizard configuration involves verification of configurations and thus requires all Control Stations to be up.
- FARM will not discover FAR sessions in an unloaded state.
- FARM cannot differentiate FARM for VNX from FARM for eNAS. So it is recommended to use the same family of FARM in case of re-install or upgrade. eNAS FARM has an eNAS prefix in the file name, for example, eNAS-AFM-Win-64-x64-en\_US-6.0.17-1.exe.
- FARM does not support downgrade and it is not recommended to install a lower version of FARM on top of a higher version.
- The FARM home directory is `C:\Program Files\EMC\VMSM`. You may come across the term VMSM in certain places. VMSM is another term for FARM.
- The FARM service should be stopped whenever a discovery operation has to be performed. In case of a new change in the VDM configuration and if the FARM service is monitoring the site, the service should be stopped and discovery should be performed. Once the discovery updates the new configuration, the FARM service should be restarted.
- The VDM configuration in FARM will become unstable if a failover or reverse operation is performed in the CLI. [Best practices](#) on page 124 provides more information.
- FARM does not support localization. English localization settings are recommended for the Windows Host in which FARM is installed. Any other localization may impact FARM functionality.

## Best practices

Consider the following recommendations when using FARM:

- It is recommended to install FARM on a dedicated/standalone host machine. The host machine will have to undergo reboots during FARM Installation or upgrade. If the host machine is hosting other applications which will be disrupted upon reboot, then it is not advisable to have FARM and such applications on the same machine.
- It is recommended to access the FARM application as Administrator user.
- If FARM is configured, it is recommended to run operations like failover and reverse from FARM and not through CLI. This is to ensure that you will not have to run discovery operation in FARM to sync up the operations done by the Command line Interface (CLI).

## VDM state and status information

### Session state

VDM state information is displayed in the main File Auto Recovery Manager window, under the Status column. This state information is the same as reported in the session\_status column of the nas\_syncrep list CLI command.

### Session status

The session status is determined by operations performed in FARM.

Operation	Status	
After successful failover	Failed over	
After successful reverse	Reversed	
After failed failover	Failover failed	
After failed reverse	Reverse failed	
After successful restore	OK	
After successful discovery	Session in R1	--
	Session in R2	Reversed

To update the status, run a check status. Check status only probes the status of R1 sessions. Therefore, the status of R2 sessions (session in R2 will have a status of "reversed" or "failed over") will remain unchanged.

Status	Description
OK	Session status 0 (all events OK)
Warning	Session status 1 (one or more events shows warning, not critical)
Failed	Session status 2 (one or more critical events occurred).

### Note

Operations performed through the CLI will not update the status shown in FARM. And, operations performed in FARM will not update the CLI. To verify that the status displayed is up to date, perform a discovery operation.

## Event status/level

FARM executes a polling procedure called Check Status and generates defined events. With these events as input, FARM runs the Decision Matrix and generates status as defined below.

**Table 8** Event Status/Level summary

Level	Color	Status	Description
0	green	OK	There are no error conditions.
1,2,3,4,5,6, 7,8	yellow	WARNING	There are error conditions that still allow operation on the primary page. The individual error conditions have to be checked. Suitable measures for repairing the errors have to be taken.
9	red	ERROR	There are error conditions that make operation on the primary page impossible. The secondary page is completely available so that a switchover to the secondary system is displayed.

# VDM event list

The complete list of VDM events follows:

## Events

- (01) Remote/Network IP for FARM-Isolation-Detection NOT reachable.
- (02) Primary control station (current) NOT reachable.
- (03) Secondary control station (current) NOT reachable.
- (14) DataMover (and their standby) on primary site NOT in OK condition.
- (15) DataMover (and their standby) on secondary site NOT in OK condition.
- (23) Standby control station on primary site NOT reachable
- (24) Standby control station on primary site is active
- (25) Standby control station on secondary site NOT reachable
- (26) Standby control station on secondary site is active
- (28) VDM: VDM interface NOT reachable
- (29) VDM: VDM service NOT reachable
- (30) VDM: Local LUN(s) with ERROR condition
- (31) VDM: Local LUN(s) with DEGRADED condition
- (32) VDM: Remote LUN(s) with ERROR condition
- (33) VDM: Remote LUN(s) with DEGRADED condition
- (34) VDM Replication: Interconnect failed
- (35) VDM Replication: Replication NOT in-sync

## FARM Environment Data Collect Sheet

Use the following empty data sheet to collect the environment and configuration information for a FARM install.

<b>Remote Ping Target</b>	
Replication Methods	SRDF
Primary Site	
Primary site NAT1	
Primary site NAT2	
Secondary Site	
Secondary site NAT1	
Secondary site NAT2	
SNMP Configurations	
Primary Target IP	
Primary Target Port	
Community	
Secondary Target IP	
Secondary Target Port	
Enterprise OID	
Generic	
Specific	
Facility	
Facility OID	
Component	
Component OID	
Severity OID	
Text OID	
DR user name	
Advanced Settings	
Pre-Script	
Post-Script	

## Refreshing session state information in FARM

VDM session state information only updates during discovery, failover, or reverse operations. If for some reason the session state information is changed by the CLI, and

if an operation was not performed on FARM, the session state shown in FARM may be out of date.

To update session state on FARM:

**Procedure**

1. On the main **File Auto Recovery Manager** window, click refresh (  ).

---

**Note**

The refresh button is disabled when the FARM service is running.

Additional FARM information

# CHAPTER 14

## Troubleshooting FARM

This chapter presents the following topics:

- [Troubleshooting sequence](#)..... 132
- [Log and configuration files](#)..... 133
- [Collecting logs](#)..... 133
- [FARM: Output codes](#)..... 134
- [FARM protection/Failover prevention](#)..... 135
- [Frequently asked questions and additional information](#)..... 135
- [Troubleshooting checklist](#)..... 137
- [Recovering FARM when it is not responding](#)..... 139

## Troubleshooting sequence

To troubleshoot an issue with FARM, do the following in order:

### Procedure

1. Review the [FARM limitations](#) on page 124.
2. Verify that the following operations return **OK**:
  - Discover (as described in [Discover monitored objects](#) on page 118)
  - Check status (as described in [Check status](#) on page 118)
3. Optionally, execute a failover and restore to verify that it completes successfully (as described in [VDM Failover scenario](#) on page 119 and [Manually restore a synchronous replication session](#) on page 117, respectively).
4. Consult the Troubleshooting section of this document. Refer to for a list of symptoms, probable causes, and resolutions.
5. Consult the FARM log and configuration files. Refer to [Check status](#) on page 118 for details about these log files.

## Log and configuration files

The FARM configuration files are located in `config\nas_vdm`.

In addition, utilities for collecting additional troubleshooting information are located in `\nas\tools\collect_support_materials`.

Issue	Action
Failed to reach eNAS	Check FARM configuration and device availability.
Failed to execute CLI commands from the eNAS control station	<p>Try running the failed command manually from the control station, and then take the following actions, depending on the results:</p> <ul style="list-style-type: none"> <li>• Cannot access the target device: <ul style="list-style-type: none"> <li>▪ Check user accounts configured in FARM</li> <li>▪ Get support from eNAS as appropriate</li> </ul> </li> <li>• Cannot retrieve device information or complete operations: <ul style="list-style-type: none"> <li>▪ Check eNAS and get support from eNAS, as required</li> </ul> </li> </ul>
Failed to execute FARM interpreter commands	<ul style="list-style-type: none"> <li>• Check the error messages for further actions to take.</li> <li>• Escalate to L3 or L4 support if no solution is available.</li> </ul>

## Collecting logs

The Main Log window information is captured in the `farm.main.log` file, found in the `C:\<Program Files>\EMC\VMSM\log` folder. Note that the `<Program Files>` folder name depends on the version of Windows being used.

To create a collection log to help with troubleshooting issues:

### Procedure

1. On the main **File Auto Recovery Manager** window, select **Help > Log Collection**.
2. By default, the Log Collection tool creates a zip file, and saves the collection's zip file to the Desktop.

## FARM: Output codes

This section describes the FARM error codes and provides possible actions to take to resolve them.

Error code	Description	Action
1 = Global error condition	Unspecific error occurs.	Escalate to L3.
400 = PING with Timeout	IP addresses are not reachable.	Check the device status and the configurations.
401 = EQUAL on Error	Unexpected Input	No action required – handled by AFM.
402 = TIMESTAMP not found	Error in Status-Evaluation	Escalate to L3.
403 = TIMESTAMP-Difference to high	The timestamp of current Status-Information (event.txt) is older than allowed and the failover is blocked.	Check and increase aging time (sec_diff) in arb_user.env.
404 = StatusLevel-Information NOT present	Error in Status-Evaluation	Escalate to L3.
405 = OK/Warning-Status	AFM-CLI-Function CHECK_FAILOVER results in “no failover needed”	No action.
406 = Failover-Status already set	AFM CHECK_FAILOVER blocked the failover as the Failover-Bit is set.	No action.
407 = Failover-Status NOT set	AFM Failback Function detects that the Failover-Bit is NOT set but needed to execute the failback.	Set the Failover-Bit and repeat failback.
500 = Syntax-Error within Command	Errors are detected in AFM-Interpreter-Language.	Escalate to L3.
501 = Missing Parameter for Command	Syntax-Error (illegal number of parameters) within AFM-Interpreter-Language detected.	Escalate to L3.
900 = Timeout during NAS-Executions	Internal error while running NAS commands	Check the NAS status; if no hints, present escalate to L3.
998 = Configuration-Issues	AFM-Configuration-Issue	Check configuration; if nothing found, escalate to L3.
999 = undefined	An error occurs but was not specified	Escalate to L3.

## FARM protection/Failover prevention

To monitor all the VDM sessions without having the VDMs failover, even under disaster scenarios, set the failover policy for all the VDMs to manual. This will allow FARM to monitor the sessions, without failing over the VDMs. [Configure a synchronous replication session's failover policy](#) on page 113 explains how to set the failover policy.

## Frequently asked questions and additional information

Table contains a list of frequently asked questions (FAQs) to help support a FARM environment.

**Table 9** Frequently asked questions

Question	Answer
When can I implement FARM?	Implementing FARM can start only after establishing a successful disaster recovery (DR) configuration.
Can you provide more details about the underlying configuration used for FARM to perform failover between eNAS systems?	The underlying configuration is based on the VDM environment. FARM 3.0 replicates VDMs using SRDF/S.
Can you provide more details about how FARM works?	<p>Users must provision the storage and configure the replication relationship between the primary and secondary systems first. When the DR configuration is established and tested, FARM can be used to automate failovers.</p> <p>The <b>Configure</b> menu is enabled with eNAS VDM DR environment and provides access to the Configuration wizard that steps you through the process of configuring the storage environment.</p> <p>The <b>Management</b> menu enables you to discover the configuration you created in the <b>Configure</b> menu and to check the status of monitored replication sessions .</p> <p>The <b>Resume, Failover, and Restore</b> controls enable you to run the required procedures for the DR configuration.</p> <p>If the underlying DR environment changes after you perform these tasks, you must re-run Discovery before running procedures.</p> <p>FARM monitors disaster or error events by polling information from both local and DR sites. When a disaster or error occurs, FARM triggers a failover (if the FARM Service is running) or reports a warning. With its capability to monitor and automatically</p>

**Table 9** Frequently asked questions (continued)

Question	Answer
	failover, FARM can provide high-availability when used with the replication method.
How do changes in the eNAS environment impact FARM?	<p>If the DR configuration changed (i.e. adding LUNs) the only required operation is Discover. FARM discovery will discover the environment.</p> <p>If the discovery is not executed after environment changes, no failover will occur if there is an error or a disaster.</p> <p>Configuration changes will be detected by the FARM Check Status function.</p> <p>You can configure SMTP to send notifications of configuration changes.</p>
What options are available for remote access to the FARM host?	You may use WebEx, or other remote desktop applications such as mstsc.exe or Citrix for remote-access.
<p>What is the potential for FARM to cause a DU/DL situation?</p> <p>If there is potential, how can this best be mitigated?</p>	<p>The worst case scenario is that a failover will occur when it should not. FARM will only run a failover if there are LUN errors or a power outage at the primary site (or other condition that warrants failover to occur). If the secondary site has an error, FARM will not run a failover. LAN isolation detection (see Global Settings) reduces the chances of the worst case scenario.</p> <p>A failover will only run once. FARM will not run a failover a second time. A discovery is needed for a reset.</p> <p>FARM can trigger VDM failover when service is running and when there is DM restore operation performed. This is one such scenario where FARM can failover when it should not.</p>
Are all FARM functions/commands/capabilities available remotely as if the servicer were on site?	<p>If you have access to the host where FARM is installed, you can run all FARM functions.</p> <p>Complete the initial configuration in the GUI. All functions are available from the FARM Command Line Interface.</p>
Can logs be collected via GUI?	From the main <b>File Auto Recovery Manager</b> window, select Help > Log Collection to collect the entire FARM logs and bundle into a zip file.
Does FARM provide any clear visual indication of errors to the administrator at the time of occurrence?	<p>No. click VDM Info for the latest status.</p> <p>If configured, you may receive SMTP traps.</p>

**Table 9** Frequently asked questions (continued)

Question	Answer
Will the FARM logs get large enough that the logs need to be archived over time?	Yes. The user should archive logs.

## Troubleshooting checklist

The symptoms, probable causes, and recommended actions in this section assume that the system had been functional and there is only one problem with the system. Issues with multiple hardware components or application software are beyond the scope of this troubleshooting checklist.

**Table 10** FARM troubleshooting

Issue reported at:	Actions
Configure > NAS/VDM Configurations	Check the corresponding configuration files. Escalate to FARM L3 if the issue cannot be resolved.
Configure > NAS/VDM Configurations > SMTP Settings	Verify SMTP configuration with customer's environment. Escalate to AFM L3 if the issue cannot be resolved.
Discover > NAS/VDM Discovery > Ping All	<ol style="list-style-type: none"> <li>1. Check the GUI error message for actions.</li> <li>2. Manually check availability of the configured IP addresses.</li> <li>3. Escalate to FARM L3 if the issue cannot be resolved.</li> </ol>
Discover > VDM Discovery > Discover	<ol style="list-style-type: none"> <li>1. Check the GUI error message for actions.</li> <li>2. If the error code occurred when executing NAS/SYMCLI commands, check the credentials.</li> <li>3. If the credentials are correct, forward the issue to eNAS support for further investigation.</li> <li>4. Escalate to FARM L3 if the issue cannot be resolved.</li> </ol>
Discover > NAS/VDM Discovery > Reference Configuration	<ol style="list-style-type: none"> <li>1. Check the result of the discover operation to verify that no error occurred.</li> <li>2. If there are no errors and the problem cannot be resolved, escalate to FARM L3.</li> </ol>
Discover > NAS/VDM Discovery > Show Last Status/Events	<ol style="list-style-type: none"> <li>1. Check the result of the Check Status operation to verify that no error occurred.</li> <li>2. If there are no errors and the problem cannot be resolved, escalate to FARM L3.</li> </ol>

**Table 10** FARM troubleshooting (continued)

Issue reported at:	Actions
Run > Failover/Restore/Reverse of VDM sessions	<ol style="list-style-type: none"> <li>1. Check the GUI error message for actions.</li> <li>2. If the error occurred when executing NAS/SYMCLI commands, check the credentials.</li> <li>3. If the credentials are correct, open the log file failover.&lt;TIME_STAMP&gt;.txt or restore.&lt;TIME_STAMP&gt;.txt to check if the commands running on the Control Station succeeded or not. If the log files contain any errors, forward the following to eNAS support: <ul style="list-style-type: none"> <li>• Symptom of the issue</li> <li>• failover.&lt;Time_Stamp&gt;.txt and restore.&lt;Time_Stamp&gt;.txt</li> <li>• eNAS logs</li> </ul> </li> <li>4. If the actions above do not apply, escalate to FARM L3.</li> </ol>
<p>Discover &gt; NAS/VDM Configurations &gt; Discover</p> <p>Discover &gt; NAS/VDM Configurations &gt; Check Status</p>	<p>If FARM discovery fails, it might be due to the following reasons.</p> <ul style="list-style-type: none"> <li>• NAT IPs of control stations might be invalid.</li> <li>• Primary Control station on both R1 an R2 site might be unreachable.</li> <li>• Nasadmin login credentials might be invalid.</li> </ul> <p>Please check the above and retry the operation.</p>
Run > Automated Failover -> FARM Service	<ol style="list-style-type: none"> <li>1. Check the start/stop status of the FARM Service in the Windows service console, and verify the logon account.</li> <li>2. If the error occurred when executing NAS/SYMCLI commands, check the credentials.</li> <li>3. If the credentials are correct, forward the issue to eNAS support for further investigation.</li> <li>4. Otherwise, escalate to FARM L3.</li> </ol>
Discover > NAS/VDM Configurations > Discover	<p>If three loop files (arbit_loop.timestamp, arbit_loop.current, arbit_loop.stop) exist under VMSM_HOME folder, discover will fail at the beginning with an error dialog.</p>

**Table 10** FARM troubleshooting (continued)

Issue reported at:	Actions
	<p>Delete these three loop files, and discover will work.</p> <hr/> <p><b>Note</b></p> <p>These 3 files are used by FARM Service. Delete them when FARM Service is not running.</p>
%AFM_HOME%\log\service_keeper.log	<p>When user finds this log file, it means that FARM service keeper has taken action to restart FARM polling procedure. FARM service keeper is a watchdog of the polling procedure. It will restart the polling procedure if it times out.</p> <p>FARM sets service keeper timeout as 480s.</p> <p>FARM support can change service keeper configuration from % VMSM_HOME% \ua.env:</p> <p>Below are default values:</p> <ul style="list-style-type: none"> <li>• service_keeper_timeout=480</li> <li>• service_keeper_log=log \service_keeper.log</li> <li>• service_keeper=1</li> </ul>

## Recovering FARM when it is not responding

In some rare cases, FARM may become non-responsive. If this should happen, perform this procedure to recover the application.

### Procedure

1. Open **Windows Task Manager**.
2. On the **Applications** tab, end the **EMC Auto Recovery Manager** task.
3. ON the **Service** tab, stop the **EMCFARM** service.
4. On the **Process** tab, stop the following processes, if running:
  - VMSE.exe
  - Vmsmagent.exe
  - Vmsmjobmgr.exe
  - VMSMServices.exe
  - Vmsmtmqsvr.exe
  - MT.exe
  - Plink.exe

5. On the **Services** tab, restart the **EMCFARM** service.
6. Launch FARM.