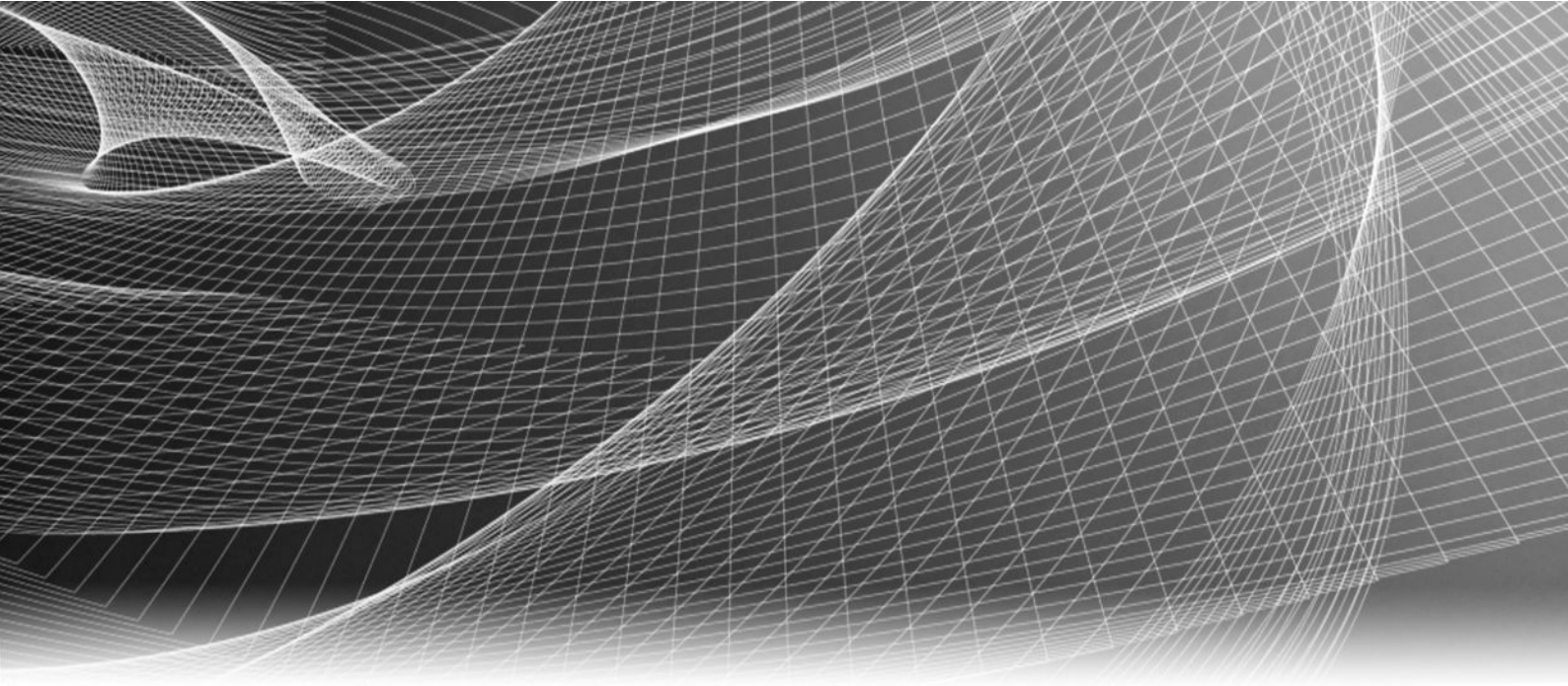


EMC® VMAX®

eNAS File Auto Recovery with SRDF/S

Version 8.1.10.21

For:
VMAX3™ Family: VMAX 100K, 200K, 400K
VMAX All Flash: 450F, 450FX, 850F, 850FX

REVISION 03

EMC²

Published April, 2016

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

CONTENTS

FIGURES

TABLES

As part of an effort to improve its product lines, 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 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 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 EMC publications provide additional information:

- *Using SRDF/S with VNX for Disaster Recovery*
  Explains how to configure and manage SRDF/S.
- *EMC VNX Command Line Interface Reference for File*
  Explains the command used to configure and manage an 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.
- *UsingVNX SnapSure*
  Explains how to use 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

EMC uses the following conventions for special notices:

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

Addresses practices not related to personal injury.

Note

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

Typographical conventions

EMC uses the following type style conventions in this document:

Table 1 Typographical conventions used in this content

Bold	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)
Italic	Used for full titles of publications referenced in text
`Monospace`	Used for: • System code • System output, such as an error message or script • Pathnames, filenames, prompts, and syntax • Commands and options
Monospace italic	Used for variables
`Monospace bold`	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

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

Product information

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

Technical support

To open a service request through the https://support.emc.com site, you must have a valid support agreement. Contact your 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

PART 1

File Auto Recovery

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

Chapters include:

CHAPTER 1

Introduction

This chapter introduces File Auto Recovery.

Topics include:

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 recovery where the source is unavailable. For recovery support in the event of an unplanned failover, an option is provided to recover and clean up the source system and make it ready as a future destination.

This document also describes the EMC File Auto Recovery Manager (FARM). This optional application allows you to manually initiate failover and reverse operations. FARM allows you to automatically failover a selected sync-replicated VDM on a source eNAS system to a destination eNAS system. FARM also allows 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 on FARM, refer to File Auto Recovery Manager on page 83.

Note

If you need to change the configurations monitored by FARM or upgrade the eNAS software bundles, you must first stop the FARM Service; then update the monitored configurations or eNAS software bundles. When changes are completed, manually discover the monitored configurations to pick up the changes, and then restart the FARM Service. Starting to upgrade the eNAS software bundles without first stopping the FARM service will result in an unnecessary FAR session failover. For detailed instructions on performing these operations, refer to FARM operations on page 93.

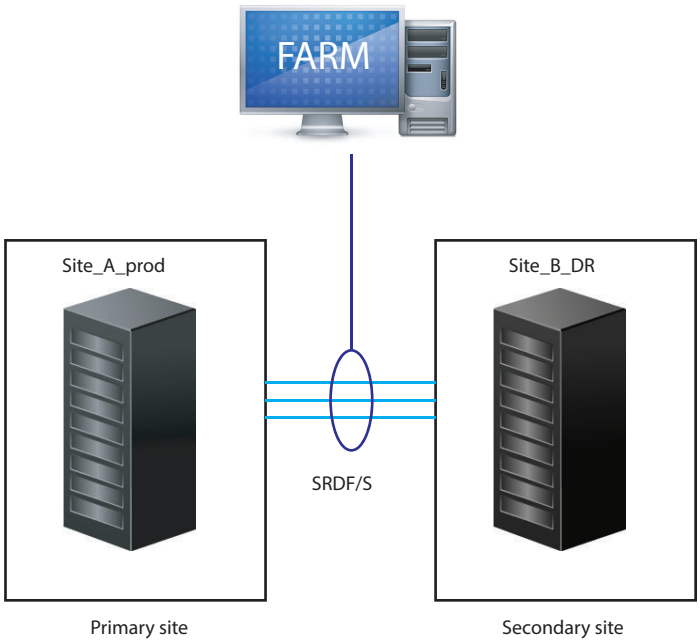
Note

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). If a failover occurs, the secondary site becomes active until the primary site is recovered and a failback 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.
- SRDF/S Hardware link is established in the switch topology between the two eNAS-configured arrays. Refer to *Using SRDF/A with VNX* and *Using SRDF/S with VNX for Disaster Recovery* located on EMC Online Support for more details.
- All file systems must use Split Log.
- Checkpoints (SavVol) must be on the same pool as the production file system (PFS).

For hardware:

- Two eNAS-configured arrays.
- Refer to *Using SRDF/A with VNX* and *Using SRDF/S with VNX for Disaster Recovery* located on EMC Online Support for additional hardware requirements.

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.
- Dedicated FC (recommended for performance) or FCoE links for connecting the storage systems.

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 disk types between each of the eNAS systems.
- FAR with SRDF and VNX Replicator technology can co-exist on the same system; however, you cannot run FAR with SRDF and VNX Replicator against the same VDM.
- File systems included in the FAR with SRDF feature cannot have any other replication technology applied to them in parallel.
- A FAR service and session is supported only between two eNAS systems with SRDF systems configured.
- Each FAR session is built upon a single VDM and a single mapped pool.
- The maximum number of FAR sessions on the two eNAS systems with SRDF systems configured is 126. This limitation is per site on a fully loaded, balanced system.
- 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.
- A 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.
- Temporarily unloaded VDMs will become loaded after a reverse or failover operation.
- For a VDM under a FAR session, you cannot mount 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 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 how many file systems or checkpoints exist on the FAR-replicable NAS pool.
- After a disaster occurs, DU will start. When a FAR session failover is executed, the DU will continue until the failover operation succeeds.
- 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 session 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.

Also, the following Data Mover configuration and Cabinet level service items must be manually migrated using the migrate_system_conf command before the creation of FAR and before failover or reverse and any time this data changes:

Note

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

- Data Mover configurations:
  - DNS
  - NIS
  - NTP
  - Local password and group
  - Usermapper client
  - FTP/SFTP
  - LDAP
  - HTTP
  - CEPP
  - CAVA
  - Server parameters
  - Netgroup
  - Nsswitch
  - Hosts
  - ntxmap
- Cabinet level service
  - Usermapper service

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

In order to enforce the restrictions and limitations that apply to FAR (see Restrictions and limitations on page 19), 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 is a mapped pool.
- Its members must be disk volumes.
- It has one and only one FAR-replicable VDM rootfs on it.
- It has no MGFS on it.
- All file systems and checkpoints on it are either un-mounted 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 used as a source side or a destination side of a Replication V2 session.
- No File Systems or Checkpoints on it are using 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 use 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

Setting up FAR

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

Topics include:

FAR setup information

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

Table 2 FAR setup planning sheet

What you specify	Source-site information	Destination-site information
Control Station name		
Control Station IP address		

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 EMC eNAS customer publications is available on 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. If necessary, install and configure the source and destination eNAS systems. Refer to EMC VNX2 customer publications available on EMC Online Support (https://support.EMC.com).
2. Configure additional SRDF Control LUNs.
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 ae to dir 1d:34, lun=6;" commit -nop
$ symconfigure -sid 352 -cmd "map dev ae to dir 2d:34, lun=6;" commit -nop
```

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/symsg –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/symsg –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: `symsg –sid xxx –sg EMBEDDED_NAS_DM_SG set –noslo`

e. Add the new Control LUNs to the masking view.

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.

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 minutes) as their source Control Stations. Take into account time zones and daylight savings time, if applicable. EMC recommends using an NTP service on the Control Stations to control this function. You can set this up using VIA during the eNAS system initialization process or by using the `nas_cs` CLI command.
- The same 6-15 characters passphrase must be used for both eNAS systems.

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 address of the remote Control Station in slot 0

   ‹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 address of the remote source Control Station in slot 0

‹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
```

Note

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.

Create masking view for NAS_DB LUNs using Unisphere

Before you begin

The procedures in this section require the following:

- Both source and destination eNAS systems are operating with VNX OE for file version 8.1.7 or higher version.
- Both source and destination eNAS systems have been added as destination systems of each other (Control Station-to-Control Station trusted relationship) with the same pass phrase (use the nas_cel command command).

Assign the source and destination NAS_DB mirror LUNs to the eNAS default storage group and manually assign them as to LUN position 0x 0009. The user will not create a diskmark for this volume on the source and destination systems.

Procedure

1. In Unisphere (for VNX), select the source eNAS system.
2. Click **Hosts › Storage Groups**.
3. Under **Storage Group Name**, select the eNAS default storage group and then click **Connect LUNs**.

   The eNAS Default: Storage Group Properties window appears.
4. In Available LUNs under the LUNs tab, find the NAS_DB mirror LUN and click **Add**.
5. In Selected LUNs under the LUNs tab, select the NAS_DB mirror LUN and, under the Host LUN ID column, assign the value 9.
6. Click **Apply**, then after confirming your action, click **Cancel**.
7. In Available LUNs under the LUNs tab, find the NAS_DB mirror LUN and click **Add**.

   Change the setting for **Show LUNs** to All so that you can find the NAS_DB mirror LUN.
8. Click **OK**.
9. Select the destination eNAS system and repeat these steps.

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).
- `nas_diskmark -mark -all` command must not have been executed; otherwise, an error will occur during enabling of the synchronous replication service.
- 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 -syncrep -enable {<cel_name>|id=<cel_id>} -
   local_fsidrange <from>,<to> -remote_fsidrange <from>,<to> -
   local_storage
   {sym_dir=<director1>:<port1>[,<director2>:<port2>,...<direct
   orN>:<portN> rdf_group=<group_num>} -remote_storage
   {sym_dir=<director1>:<port1>[,<director2>:<port2>,...<direct
   orN>:<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 -syncrep -enable L9P36_CS0 -local_fsidrange 4096,12287 -remote_fsidrange 12288,24575 -local_storage 000196700260 sym_dir=1G:8 rdf_group=107 -remote_storage 000197100125 sym_dir=1G:8 rdf_group=107`

   Output from 100K system:

   ```
   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...                  done
Now configuring and rebooting secondary CS...                 done
Now enabling sync replication service on remote system...     done
done
```

CHAPTER 4

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 27 before starting the procedures in this chapter.

Topics include:

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_syncrep -start {<cel_name>|id=<cel_id>}
```

Where:

`-start {<cel_name>|id=<cel_id>` = Starts the FAR service on the specified eNAS system (source or destination).

Create data LUNs for NAS resources

Before you begin

The FAR service must be enabled.

Create the desired number of thick LUNs for use as data LUNs, on the source and destination eNAS systems. Name these LUNs and assign IDs appropriately so they can be tracked, such as nas_data_lun_1 and nas_data_lun_2, and size them appropriately based on the amount of information to be stored and the duration, such as 20 GB on a RAID10. Build these LUNs from a block storage pool and assign them to the eNAS default storage group.

Procedure

1. In Unisphere, select the source eNAS system.
2. Click **Storage** › **LUNs**.
3. Click **Create** on the LUNs tab.

   The Create LUN window appears.
4. Fill in the fields to create the appropriate number of thick LUNs of the appropriate size.
5. When you are finished filling in the fields, click **Apply** and then click **OK** to confirm your settings.

   The data LUNs appear on the LUNs tab.
6. Select these data LUNs and click **Add to Storage Group**.

   Add to selected Storage Groups window appears.
7. Select the eNAS default storage group from the list of Available Storage Groups and move it to the list of Selected Storage Groups.
8. Click **OK**, and then click **Yes** and **OK** to confirm selection.
9. On the source eNAS system, run the following command to create NAS Disks Volumes:

   ```
   $ nas_diskmark -mark -all-discovery y -monitor y
   ```
10. Select the destination eNAS system and repeat these steps.
11. 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.

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 67 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=vdm1pool -
   option syncreplicable=yes
   ```

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 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 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 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 vdm1interface
   ```

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

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 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/.

Create a FAR session

Before you begin

The following prerequisites should be in effect before you create 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 8.1.6 or higher version.
- Control Station-to-Control Station communication channel between the two eNAS systems should be configured and ready for communication.
- 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.
- Local and remote Data Mover should have the same I18N 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 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`:
  - Data Mover configurations:
    - DNS
    - NIS
    - NTP
    - Local password and group
    - Usermapper client
    - FTP/SFTP
    - LDAP
    - HTTP
    - CEPP
    - CAVA
    - Server parameters
    - Netgroup
    - Nsswitch
    - Hosts
  - Cabinet level service

  First, migrate the usermapper, then the data mover services. For information about `migrate_system_conf`, see the *VNX Command Line Interface Reference Information for File* and *Using VNX File Migration Technical Notes*.

  For information about `migrate_system_conf`, see the *VNX Command Line Interface Reference Information for File* and *Using VNX File Migration Technical Notes*.

Note

The routing table, including the default route, do not get migrated with this command. These 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.

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_syncrep -create LY2E6_session1 -vdm LY2E6_vdm1 -remote_system
   L9P36_CS0 -remote_pool l9p36_marketing_sg -remote_mover server_2 -
   network_devices cge0:cge0
   ```

   Output:

   ```
   Now validating params...                        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
   ```

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.

Note

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.

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_syncrep -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 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 49 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 made, 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 49 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 5

Managing FAR

This chapter explains how to manage FAR.

Topics include:

Reverse operation

If you need 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:

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 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 at the destination site becomes standby.

Performing reverse on a VDM

Before you begin

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

- Both systems of the FAR session 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 50 for details. If you need to configure for NFS I/O transparency, see Configure for NFS I/O transparency in FAR session on page 53 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 synchronous replication session

   ‹id› = Identifier of the synchronous replication session

   Example:

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

   `$ nas_syncrep -reverse id=4315`

Output:

```
WARNING: 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: 19 s
Now doing health check...                                done: 11 s
Now cleaning local...                                    done: 1 s

                                    Service outage start......
Now turning down remote network interface(s)...          done: 8 s
Now switching the session (may take several minutes)... done: 7 s
Now importing sync replica of NAS database...            done: 16 s
Now creating VDM...                                      done: 5 s
Now importing VDM settings...                            done: 0 s
Now mounting exported FS(s)/checkpoint(s)...             done: 13 s
Now loading VDM...                                       done: 3 s
Now turning up local network interface(s)...             done: 0 s
                                    Service outage end: 52 s

Now mounting unexported FS(s)/checkpoint(s)...            done: 0 s
Now importing schedule(s)...                              done: 0 s
Now unloading remote VDM/FS(s)/checkpoint(s)...           done: 16 s
Now cleaning remote...                                    done: 17 s
                                          Elapsed time: 116s
done
```

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.

Note

In situations where the source site is still accessible, a reverse must be used instead.

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.

   Note

   If the source site Data Mover was powered off, the Data Mover network must be disconnected before powering it on to avoid IP address conflict.

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 at the destination site to standby.

Performing failover on a VDM

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 50 for details. If you need to configure for NFS I/O

transparency, see Configure for NFS I/O transparency in FAR session on page 53 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.

Note

When failover starts, you must not perform any operation on the VDM and FAR session of the failed site.

Procedure

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

   ```
   $ nas_syncrep -failover {<name>|id=<id>} -r1clean
   ```

   Where:

   ‹name› = Name of the VDM synchronous replication session

   ‹id› = Identifier of the VDM synchronous replication session

   -r1clean = Specifies to clean the original source after completing the failover. Using this option will prevent the array from calling home when the Data Movers available on the source side try to access the WD devices. Not specifying this option will allow you to avoid the cumulative delays in performing failovers to subsequent VDM sessions.

   Example:

   To failover the VDM to the standby eNAS system, type:

   $ nas_syncrep -failover id=4560

   Output:

   ```
   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, then 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 Unavailability or Data Loss. Are
   you sure you want to proceed?   [yes or no] yes
   ```

2. At the warning prompt, type yes.

   Output:

   ```
   Now doing precondition check...                          done: 26 s
   Now doing health check...                                done: 0  s
   Now cleaning local...                                    done: 3  s
   Now switching the session (may take several minutes)...  done: 10 s
   Now importing sync replica of NAS database...            done: 81 s
   Now creating VDM...                                      done: 4  s
   Now importing VDM settings...                            done: 0  s
   Now mounting exported FS(s)/checkpoint(s)...             done: 2  s
   Now loading VDM...                                       done: 2  s
   Now turning up local network interface(s)...             done: 1  s
                                       Service outage end: 129s
   ```

```
Now mounting unexported FS(s)/checkpoint(s)...           done: 0  s
Now importing schedule(s)...                             done: 0  s
                                          Elapsed time: 154s
done
```

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.

Note

Outage duration depends on the number of File systems and checkpoints mounted and exported on source VDM.

Performing clean on a VDM

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_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 command is not run, you are prevented from performing a failover or a reverse operation on the FAR session.

Note

You can also specify to automatically perform a clean operation after a failover using the `-r1clean` option with the `-failover` command. For more information, refer to Performing failover on a VDM on page 58.

Procedure

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

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

   Where:

   ‹name› = Name of the synchronous replication session

   ‹id› = Identifier of the synchronous replication session

   Example:

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

   `$ nas_syncrep -Clean id=8002`

   Output:

   ```
   WARNING: You have just issued the nas_syncrep -Clean command. This
   may 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_syncrep -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?  [yes or no] yes
   ```

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

   Output:

```
Now cleaning session LY2E6_session1 (may take several minutes)... done
Now starting session LY2E6_session1...                            done
```

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 is rebooted.

Note

During the clean operation, the Data Movers on the local side may continuously panic, especially when there are other session not cleaned yet. This is because sessions not yet cleaned can still end up accessing WD devices for write operations and panic the Data Mover.

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 -syncrep -list
   ```

   Where:

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

   Example:

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

   `$ nas_cel -syncrep -list`

   Output:

   ```
   id    name          syncrep
   0     my_system1    initialized
   1     my_system2    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>} [-verbose]
   ```

   Where:

   `-info {‹cel_name›|id=‹cel_id›} [-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 id=1 -verbose`

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

```
id                   = 1
name                 = my_system1
syncrep              = enabled
fsidrange            = 8192,12287
type                 = RDF
local_storage        = 000190100530,rdf_group=233,device_group=nasdb_0BC_31F
remote_storage       = 000194900673,rdf_group=234,device_group=nasdb_31F_0BC
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 LY2E6_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 configuring and rebooting secondary CS...                               done
Now disabling service (including deleting LUN mapping) on remote system... done
Now removing FSID range [4096,12287] on remote system...                    done
Now removing FSID range [12288,24575] 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_syncrep1`

   Output:

   ```
   id = 3
   name = my_syncrep1
   acl = 0
   type = vdm
   server =
   rootfs = root_fs_my_syncrep1
   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_syncrep -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.

   Example:

   To list the FAR session information, type:

   `nas_syncrep -list`

   Output:

```
id      name          vdm_name    remote_system    session_status
5020    my_syncrep1           my_vdm      -->my_system1    sync_in_progress
10030   my_syncrep2           my_vdm      <--my_system1    in_sync
```

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_syncrep -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_syncrep -i id=4103`

   Output:

```
id                   = 4103
name                 = LY2E6_session1
vdm_name             = LY2E6_vdm1
syncrep_role         = standby
local_system         = L9P36_CS0
local_pool           = l9p36_marketing_sg
local_mover          = server_2
remote_system        = LY2E6_CS0
remote_pool          = marketing_sg
remote_mover         = server_2
device_group         = 60_260_60_125
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_syncrep -delete {<name>|id=<id>}
   ```
   Where:

   ‹name› = Name of the FAR session

   ‹id› = Identifier of the FAR session

   Example:

   To delete a FAR session, type:

   $ nas_syncrep -delete LY2E6_session1

   Output:

   ```
   Deleting...
   WARNING: Please do not perform any operation on LY2E6_session1 on
   standby system until delete is 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).

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 SRDF session cannot be in a FAILED_OVER or REVERSE state.
- 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_syncrep -Refresh_pairs {-all|<name>|id=<id>}
   ```

   Example:

   To delete a FAR session, type:

   $ nas_syncrep -Refresh_pairs LY2E6_session1

   Output:

   ```
   WARNING: You have just issued the nas_syncrep -Refresh_pairs
   command. Please do not perform any operation(s) on the source side
   during the nas_syncrep -Refresh_pairs command. Also note that the
   operation cannot be reverted. Are you sure you want to proceed?
   [yes or no] yes
   Now refreshing session
   LY2E6_session1...
   ```

Updating VNX OE software

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

1. On the destination site, update the VNX OE for File.
2. On the source site, update the VNX OE for File.

After you finish updating the VNX OE software, verify that FAR is operational by using `nas_syncrep -list`.

CHAPTER 6

FAR service checklists

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

Topics include:

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.

Table 3 FAR service setup checklist

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

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 4 FAR session creation checklist

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

CHAPTER 7

Troubleshooting FAR

As part of an effort to continuously improve and enhance the performance and capabilities of its product lines, 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-todate 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 EMC Customer Support Representative. Problem Resolution Roadmap for VNX contains additional information about using EMC Online Support and resolving problems.

Topics include:

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.
- EMC Online Support:
  - Use the text from the error message's brief description or the message's ID to search the Knowledgebase on EMC Online Support. After logging in to EMC Online Support, locate the applicable **Support by Product** page, and search for the error message.

PART 2

File Auto Recovery Manager

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

CHAPTER 8

Installing FARM

This chapter presents the following topics:

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 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.
- The eNAS Control Stations and eNAS Data Movers must be accessible to the FARM server. If the data and management networks in the customer environment are segregated and only the management network is accessible, FARM will monitor the system based on NAS and SYMCLI commands; however, network connectivity will not be checked.

Table 5 Supported Operating Systems

OS	64 bits	32 bits
Windows Server 2008 R1	Yes	Yes
Windows Server 2008 R2	Yes	NA
Windows 7	Yes	Yes

Note

Run FARM as Administrator on Windows 7 or the Windows Server 2008.

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. If you are upgrading an existing installation, stop all currently running FARM instances (**Run** › **Automated Failover** › **AFM Service**).
2. Download the appropriate installation package from EMC Online Support at https://support.EMC.com:
   - `eNAS-AFM-Win-32-x86-en_US-3.1.35`
   - `eNAS-AFM-Win-64-x64-en_US-3.1.35`
3. 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.

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

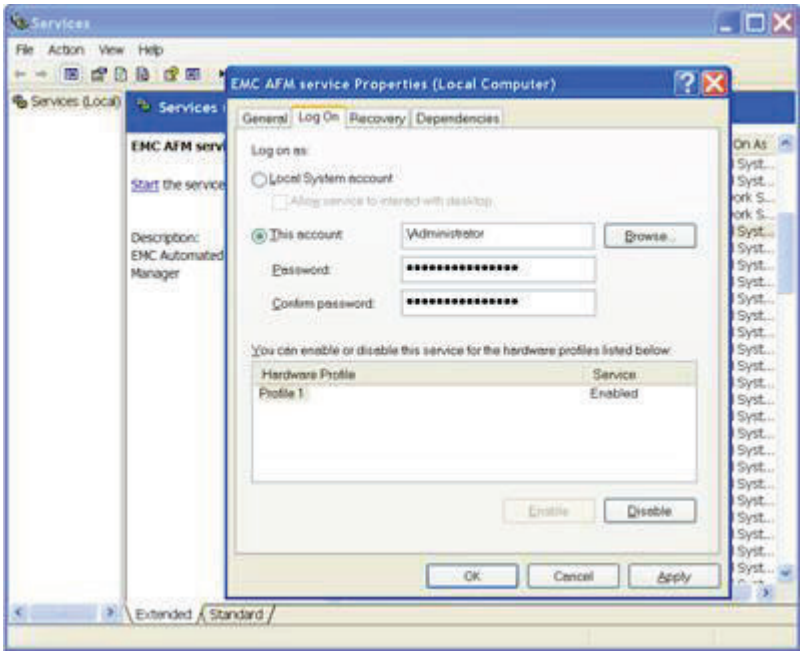
   ```
   Automated Failover Manager Configuration data found -- Would
   you like to restore these settings during installation ->
   Yes or No
   ```

   Click **Yes** to maintain your existing configuration or **No** to delete it.
5. On the **Introduction** page, click **Next**.
6. On the **License Agreement** page, select the option to accept the license agreement and click **Next**.
7. On the **Choose Install Folder** page, click **Next** to accept the default directory, or click **Choose** to select another directory, and the click **Next**.
8. On the **Pre-Installation Summary** page, verify the summary information, and click **Install** to continue the installation.
9. On the **Install Complete** page, click **Done**.
10. When the Windows restart completes, access the EMC FARM Service to create the Administrator user.
    a. Access the list of services: **Control Panel** › **Administrative Tools** › **Services**.
    b. Right-click **EMC AFM Service**, select **Properties**, and click the **Log On** tab.
    c. Click **This account** and enter the administrator account and password information. See example in the following figure.
    d. Click **OK** to apply this setting and close the dialog.

Note

This setting enables you to monitor eNAS level event logs.

Figure 2 EMC FARM service properties



CHAPTER 9

FARM Workflow

This chapter presents the following topics:

Three-step FARM model

FARM contains three menus that correspond to the three-step FARM model:

- **Configure** - The **Configure** menu enables you to add or remove storage, and configure settings for eNAS.
- **Manage** - The **Manage** menu enables you to discover eNAS and VDM configurations, view a reference configuration, check status, or ping devices.
- **Run** - The **Run** menu enables you to start the automated failover service or run manual eNAS and VDM procedures if the FARM service is not running.

The following sections explain the options available in each of the menus.

Configure menu

The following table shows the menu selections available from the **Configure** menu.

Table 6 Configure Menu

Selection	Description
Global Settings	Enables SAN, cabinet-level NAS, or VDM-level NAS configurations.
Add/Remove Storage	Allows you to add or remove a storage system for FARM monitoring.
SAN Configurations	Allows you to set storage, replication, and security parameters. You can also provision SNMP traps for the SAN environment.
NAS Configuration › Enable Cabinet-level	Enables you to set storage, replication, and security parameters. You can also provision SNMP traps for the NAS cabinet-level environment.
VDM Configuration › Enable VDM-level	Allows you to set storage, replication, and security parameters. You can also provision SNMP traps for the NAS VDM-level environment.
Exit	Exits FARM. Exiting FARM does not affect the FARM Service status.

For more information, refer to Configure operations on page 94

Manage menu

This menu enables you to manage storage systems that you configured FARM to monitor. The reference configuration shows the managed configurations and is the baseline on which FARM runs event polling and failover functions. Check the reference configuration and ensure it shows the storage configuration that you want FARM to manage.

If you change the underlying storage configurations that FARM monitors (including OE upgrades), discover the configuration again. This action updates the reference configuration to show the added file systems.

The following table shows the options of the **Manage** menu.

Table 7 Manage Menu

Selection	Description
NAS Discovery	Discovers the storage system configuration and creates a reference configuration.

Table 7 Manage Menu (continued)

Selection	Description
VDM Discovery	Discovers the storage system configuration and creates a reference configuration.
Ping All	Checks availability of all provisioned IP addresses in the configuration.
Manage	Manages the storage configurations that the FARM monitors. If the monitored storage system configuration changes (including OE upgrades), you must discover the configuration again.
Check Status	Polls the status of the monitored storage systems and generates FARM events. A decision matrix uses the FARM events to make failover decisions and send notifications.
Reference Configuration	Displays the reference configuration.
Show last Status/Events	Shows the most recent polled events.

For more information, refer to Manage operations on page 100

Run menu

Before using the **Run** menu, ensure that the FAR configuration is complete and has been managed. Use the Run procedures to activate monitoring and other related functions. You can also start FARM service in the background as a Windows service.

Note

If you selected **Enable VDM-level** in **Global Settings**, only VDM procedures are available. If you selected **Enable Cabinet-level**, only NAS procedures appear.

The following table shows the user options for the **Run** menu.

Table 8 Run Menu

Selection	Description
Automated failover	Manages the File Auto Recovery Manager (FARM Service). You can start or stop the FARM Service by using this menu choice. You can also view the FARM Service state and logs.
VDM Procedures	Provides the failover, reverse, and restore procedures for VDM.

For more information, refer to Run operations on page 102

CHAPTER 10

FARM operations

This chapter presents the following topics:

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 *EMC VMAX eNAS File Auto Recovery with SRDF/S* guide. Observe the requirements listed there.

Configuring FARM

This topic describes how to configure FARM to monitor the FAR replication environment:

Procedure

1. Define the data service context by selecting **Configure** › **Global Settings**.
   a. Verify that the **Enable VDM-level** option is selected.
   b. Click **OK**.
2. Start the VDM Configuration wizard by selecting **Configure** › **VDM Configurations** › **Storage Settings**.
3. Under **Basic Settings**:
   a. Ensure that the **Replication Method** is **SRDF** and that the **Enable Automated Failover**, and the **Automated VDM Failover once PING of any of interface Fails** options are selected.
   b. Under **Primary Site CSO**, specify the NAT IP addresses (**NAT1 IP** and **NAT2 IP**) through which FARM will communicate with the eNAS Control Station and the number of times FARM should retry failing over a VDM session.
   c. Enter 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.
   d. Click **Next**.
4. Under **Control Stations**:
   a. Enter names and NAT addresses for the Control Stations at the Primary and Secondary sites.
   b. Click **Next**.
5. Under **NAS Security** :
   a. Enter nasadmin password. If required, configure a Putty private key file.
   b. Click **Next**.
6. Under **Scripting** (optional):
   a. Enter a pre-failover or post-failover command (or both) to run on failover.
   b. Click **Next**. VDM discovery begins automatically.

7. When discovery completes, click **VDM** (if not already selected).

   The VDMs appear in a list.

   a. If you want to edit a VDM in the list, click to highlight the row, then click the **Edit** button.

   b. In the **Edit VDM** dialog, select the interfaces and file systems tomonitor, or change the failover priority of the VDM, then click **OK**.

   Note

   The failover priority designates the failover sequence during failover. High-priority VDMs will fail over first, followed by medium-priority and then low-priority VDMs.

   c. Click **Finish** to close the VDM Configuration wizard.

8. To start automated failover monitoring:

   a. Select **Run** › **Automated Failover** › **AFM Service**.

   b. Click **Start** and confirm the prompt.

   The AFM Service is active. Failover will occur automatically if failover conditions exist.

SNMP settings

The **SNMP Settings** tab enables you to configure general settings, trap definitions, status traps, and events.

Processing logic

You can configure SNMP traps extensively for the environment.

You can define two SNMP target hosts for SNMP messages. With a SNMP trap target defined, FARM sends SNMP traps to this target. The parameters for timeout, retransmission, and the SNMP community are valid for both SNMP target hosts.

Configure the trap and required communications parameters:

- SNMP trap targets
- SNMP trap port
- Timeout
- Failed attempts
- Community
- SNMP version
- SNMP watchdog

You can define a security level and text for each event and status. You can define an SNMP trap for the environment's overall status. You can configure an SNMP trap to occur when the environment reverts to the OK status from a warning or error status.

You can activate the SNMP traps for error forwarding and with a watchdog trap. This watchdog trap is periodically generated for the FARM background processing. If no watchdog traps are received in 3 minutes, FARM goes offline. You can configure the severity and text for the watchdog trap.

SNMP trap structure

All SNMP traps generated by FARM have the same structure:

- Enterprise OID trap target
- Generic trap definition
- Specific trap definition
- Local IP (IP address from which the trap will be sent)
- Variable bindings
  - Facility - Number (integer) and OID
  - Component - Number (integer) and OID
  - Severity - Severity level (integer) and OID
  - Text - Text data (string) and OID

The trap is sent to the Enterprise OID. The trap must be evaluated there. The variables determine the trap data. Each trap returns the four variables listed here.

The text entry for an SNMP trap includes the following elements preceding the stored texts:

- Date Format : Mon DD HH:MM:SS YYYY
- Text Arbitrator:‹x›:‹y›
  - ‹x› - either "S" (Status Trap), "E" (Event Trap) or "W" (Watchdog Trap)
  - ‹y› - either the status level or event number. In the event of a watchdog trap, a "0" is set for ‹y›

Example of a complete text element for a trap:

```
Dec 15 12:34:08 2009 Arbitrator:E:12 Secondary LUN(s) with ERROR
condition.
```

SNMP GUI Buttons

The SNMP configuration screen provides the buttons listed in the following table.

Table 9 SNMP Configuration buttons

Button	Description
Clear	Deletes the content of all parameters on all tabs.
Load Defaults	Loads default text assigned to events from the FARM configuration. No other parameters are changed.
Test Marked Traps	Generates SNMP traps for all marked events (status traps and event traps).
Cancel	Leaves the dialog without saving the entered parameter data.
OK	Exits the dialog while saving the parameter data.

General settings

The following table explains the general SNMP settings.

Table 10 SNMP configuration - General settings

Parameter	Meaning	Default
Primary Target: SNMP-Target-IP	IP address of the primary SNMP target host; SNMP traps are sent to the primary SNMP server if you provide SNMP Target IP.	Empty
Primary Target: SNMP-Port	SNMP trap port (SNMP standard: 162) for the primary SNMP target host.	Empty
Secondary Target: SNMP-Target-IP	IP address of the secondary SNMP target host; SNMP traps are sent to the secondary SNMP server if you provide SNMP Target IP.	Empty
Secondary Target: SNMP-Port	SNMP trap port (SNMP standard: 162) for the secondary SNMP target host.	Empty
Timeout (sec.)	Network timeout during transmission of SNMP traps for both SNMP target hosts.	Empty recommended: 3 sec.
Retries	Number of retries in the event of a communication error (for example, timeout).	Empty recommended: 3
SNMP Community	SNMP community (valid for both SNMP target hosts).	Empty
SNMP Version	A solution has been prepared for SNMP versions 1, 2c, and 3; currently only version 1 is possible.	snmpv1
Checkbox ... Generate Watchdog-Traps	SNMP watchdog traps are only generated if this checkbox is selected.	Not Activated
Watchdog Severity	Severity level for watchdog traps.	Empty
Watchdog Text	Text data for watchdog traps.	Empty

Trap definition

The following table explains the trap definition settings.

Table 11 SNMP trap definition settings

Parameter	Meaning	Load Defaults Values
Enterprise-OID	Enterprise Object Identifier (OID) for the SNMP traps.	1.3.6.1.4.1.1139
Generic	Generic SNMP parameter for the trap.	6

Table 11 SNMP trap definition settings (continued)

Parameter	Meaning	Load Defaults Values
Specific	Specific SNMP parameter for the trap.	4
Local-IP	Local IP address from which the SNMP trap is sent.	Empty
Facility OID	Facility ID and associated OID.	64 and 1.3.6.1.4.1.1139.2.1.1.1
Component OID	Component ID and associated OID.	5 and 1.3.6.1.4.1.1139.2.1.1.2
Severity OID	Severity level OID. The severity level itself is taken from the statuses and events.	1.3.6.1.4.1.1139.2.1.1.3
Text OID	OID for the text message. The text itself is taken from the statuses and events.	1.3.6.1.4.1.1139.2.1.1.4

Status traps

The following table explains the status traps settings:

Table 12 SNMP configuration - Status traps parameters

Parameter	Meaning	Default
Send Trap	Indicates if a SNMP trap should be generated for the associated status.	Not checked
Status	Description for the status.	---
Severity	Defines the severity level sent by an SNMP trap for the status.	Empty
Text	Defines the text sent by an SNMP trap for the status.	Empty

Event traps

You can set trap parameters for up to 30 events. The following table explains the event trap settings.

Table 13 Event trap settings

Parameter	Meaning	Default
Send Trap if Status OK	Indicates if a SNMP trap should be generated for the event if the status is OK.	Not Activated
Send Trap if Status WARN	Indicates if a SNMP trap should be generated for the event if the status is WARNING.	Not Activated

Table 13 Event trap settings (continued)

Parameter	Meaning	Default
Send Trap if Status ERR	Indicates if a SNMP trap should be generated for the event if the status is ERR.	Not Activated
Severity	Defines the severity level sent by an SNMP trap for the event.	Empty
Text	Defines the text sent by an SNMP trap for the event.	Empty

Collaboration traps

If an SNMP target is provisioned, FARM sends collaboration traps to the target host before and after failover. The following example shows the format in which the collaboration traps appear to the target host. This information enables identification of the failed-over storage object.

```
FAILOVER;FROM:< PRIM_STOR_ID >;TO:< SEC_STOR_ID r>;FAILOVER_START
FAILOVER;FROM:< PRIM_STOR_ID >;TO:< SEC_STOR_ID r>;FAILOVER_END
```

Manage operations

This section explains the FARM manage operations.

VDM Discovery

Select **Manage** › **VDM Discovery** to ping monitored objects, discover the monitored objects, check status and events, or review the reference configuration.

Ping all

To ping all devices in the monitored storage system, select **Manage** › **VDM Discovery** › **Ping All**. Click **Execute:PINGALL** to verify that FARM can reach the configured IP addresses.

Discover

To discover the monitored objects, select **Manage** › **NAS Discovery** › **Discover**. You must stop the FARM Service before running discovery. If the FARM Service is running, click **Stop Service**, and then click **Execute:DISCOVER**.

Click **Refresh** to update the current status of the FARM Service.

The discovery log file displays in the log file window. When discovery successfully completes, the discovered status appears in the reference configuration.

To exit the **NAS Discover** window, click **OK**.

Check status

To check the health status of monitored storage devices, select **Manage** › **NAS Discovery** › **Check Status**. The **Check Status** function polls the storage systems and lists events and statuses in the log file area of the window.

Last status and events

To view the latest status and events of the monitored storage devices, select **Manage** › **NAS Discovery** › **Last Status/Events**.

Reference configuration

To view the reference configuration of managed storage devices, select **Manage** › **NAS Discovery** › **Reference Configuration**. The reference configuration shows the primary and secondary objects. If changes occur over time in the configuration of the monitored objects, the FARM reference configuration will be out-of-date. To ensure that the reference configuration is up-to-date, run a discovery before viewing the reference configuration.

When to re-run discovery

If changes occur in the underlying VDM Sync Replication environment, run discovery again to pick up the changes. Run a discovery after changes to:

- VDM network interfaces
- VDM NFS/Exports
- VDM file systems
- Addition of VDMs or VDM Sync sessions

- eNAS upgrades

To run a VDM discovery:

Procedure

1. Select **Manage** › **VDM Discovery** › **Discover**.
2. In the **VDM Discover** dialog box, click the **Stop Service** button to stop the FARM Service if it is running. You cannot run a discovery while the FARM Service is active.
3. Click the **Execute: DISCOVER** button. FARM discovers the components of the VDM environment. A successful discovery ends with this message:

```
====FINISH DISCOVER successfully (exit code 0)====
```

Note

Another way to run discovery is to select **Configure** › **VDM Configurations** › **Storage Settings** › **VDM**, and then click **Discover** to discover configured VDMs .

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 run procedures available in the **Run** menu will not complete successfully if the discovery fails.

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

Table 14 Errors, causes, and remedies

Error	Cause	Remedy
Control Station NAT IPs are invalid or nasadmin password is invalid	Three possible causes include: 1. The Control Stations are not reachable. 2. The nasadmin logic credential is invalid. 3. The NAT IPs entered are invalid	1. Verify that the Control Stations are reachable. 2. Verify the nasadmin credentials were entered correctly. 3. Verify that the NAT IPs are valid.

Run operations

This section explains the operations available in the **Run** menu. For example, VDM failover, VDM reverse, or VDM restore operation. Stop the FARM Service to run these procedures. During failover, reverse, and restore operations, there will be an outage.

Note

During VDM failover or reverse operations, if the VDM names at the primary and secondary sites are the same, the primary VDM is renamed to avoid the conflict. FARM updates the new name when the VDM is restored. The naming conflict can also occur with file systems; in this case, run discovery to update the FARM GUI.

VDM failover

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.

You would run 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, you do manual clean-up on the Control Station, as described in VDM Failover scenario on page 103

VDM reverse

The **VDM Reverse** procedure reverses the direction and roles of the sync replication session between the primary and secondary sites. This procedure brings the secondary VDM, file systems, and related network interfaces online.

The **VDM Reverse** procedure also takes the primary VDM, file systems, and related network interfaces offline (the **VDM Failover** procedure does not do this).

You would run the **VDM Reverse** procedure if you wanted to perform maintenance on the primary site and needed to take it offline. During the maintenance window, the secondary site is active.

VDM restore

The **VDM Restore** procedure restores a reversed or failed-over VDM to the primary site. This procedure brings the primary VDM, file systems, and related network interfaces online. The **VDM Restore** procedure also takes the secondary VDM, file systems, and related network interfaces offline.

Because FARM operates in an active/passive mode, FARM no longer actively monitors a VDM that failed over or was reversed. After the **VDM Restore** operation, choose **Configure** › **VDM Configurations** › **Storage Settings** › **VDM**, and select the VDM from the list. This action ensures that the VDM is monitored again by FARM.

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, select **Run** › **VDM Procedures** › **VDM Failover** to run a manual failover.
3. After a successful failover, consult the reference configuration (**Manage** › **VDM Discovery** › **Reference Configuration**) and observe that the **Direction** arrow is <====== and the **Status** indicates **Failed Over**.
4. After the problem is resolved at the primary site and the system is returned to operation, service personnel run the `nas_syncrep -Clean` command to clean up the primary site, if required (the `-Force` option may be necessary).
5. If the FARM service is running, stop it.
6. Select **Run** › **VDM Procedures** › **VDM Restore** to restore the failed-over VDM to the primary site, and the secondary site goes offline (standby).

   Note

   After the restore completes, FARM stops monitoring the failed-over VDMs. You must re-select them to enable FARM to monitor them again. Steps 7 and 8 describe this action. Running a discovery also reselects the VDMs for monitoring if you prefer that method.

7. When the VDM is restored, run **Configure** › **VDM Configurations** › **Storage Settings** › **VDM**.
8. Select the VDM (by checking the check box) to enable FARM to monitor it again.
9. Verify FARM is actively monitoring the VDM by running **Manage** › **VDM Recovery** › **Reference Configuration** and observing that the **Direction** arrow is ======> and the **Status** indicates **Ready**.
10. 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. Select **Run** › **VDM Procedures** › **VDM Reverse** on the replication session. (The FARM Service must be stopped to run this procedure.)
2. After a successful reverse, consult the reference configuration (**Manage** › **VDM Discovery** › **Reference Configuration** and observe that the **Direction** arrow is <====== and the **Status** indicates **Failed Over**
3. When the maintenance tasks are completed at the primary site and the system is fully operational, select **Run** › **VDM Procedures** › **VDM Restore** to restore the reversed VDM to the primary site. The secondary site goes offline (standby).

Note

After the restore completes, FARM stops monitoring the failed-over VDMs. You must re-select them to enable FARM to monitor them again. Steps 4 and 5 describe this action. Running a discovery also reselects the VDMs for monitoring if you prefer that method.

4. When the VDM is restored, run **Configure** › **VDM Configurations** › **Storage Settings** › **VDM**.
5. Select the VDM (by checking the check box) to enable FARM to monitor it again.
6. Verify FARM is actively monitoring the VDM by running **Manage** › **VDM Recovery** › **Reference Configuration** and observing that the **Direction** arrow is ======› and the **Status** indicates **Ready**.
7. Restart the FARM Service.

When to 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 site
- Running an eNAS upgrade
- Running FARM discovery
- Performing a Failover/Reverse/Restore operation

NOTICE

When changing VDM configurations monitored by FARM, stop the FARM Service first. When changes are complete, discover the monitored configurations to pick up the changes, and then restart the FARM Service. Changes requiring a re-discovery include NAS software upgrades, VDM network interfaces, VDM NFS/Exports, VDM file systems, and VDM sync-replication changes.

Starting the FARM Service and automated failover monitoring

To start the FARM Service and automated failover monitoring:

Procedure

1. Select **Run** › **Automated Failover** › **AFM Service**
2. If required, check the **Express Failover Detection** check box. See Understanding express failover detection on page 105 for more information.
3. Click the **START** button to start the FARM Service.

Note

The AFM Service will not start unless you select the **Enable Automated VDM Failover** option in the **Configure** › **VDM Configuration** › **Storage Settings** › **Basic Settings** menu.

Stopping the FARM Service and automated failover monitoring

To stop the FARM Service and automated failover monitoring:

Procedure

1. Select **Run** › **Automated Failover** › **AFM Service**.

2. Click **STOP**.

Note

If you stop the FARM Service, it does not automatically start the next time Windows is rebooted. You must click **START** to start the FARM Service.

Understanding express failover detection

The **Express Failover Detection** check box is only for VDM configurations.

Automated failover responds differently depending on the selection of this check box:

- If you deselect the **Express Failover Detection** check box, automated failover:
  - Monitors all system events and fails over when a system event occurs.
  - Fails over only when all interfaces attached to a VDM fail.
  - Displays a warning message when one of the VDM interfaces fails.
- If you select the **Express Failover Detection** check box, automated failover:
  - Monitors only the critical failure events listed in Critical-only events on page 112; fails over only when these critical events occur.
  - Fails over if only one of the interfaces attached to a VDM fails.
  - Provides faster failover (see Installation Requirements on page 86for system requirements to ensure best performance).

Viewing FARM Service States and Logs

The **AFM Service States/Logs** dialog box displays the operating state of the FARM Service and lists log files, if any.

Procedure

1. Select **Run** › **Automated Failover** › **Current state/log** to open the **AFM Service States/Logs** dialog box.
2. Select **Only Critical Events** to display only the events that are critical. Select **Events Since Last Service Start** to display only the events that have occurred since the last time you started the FARM Service.
3. Click **Auto-Refresh ON** to automatically refresh the log file display. The most recent entry appears at the top of the list. Click **Auto-Refresh OFF** to turn off this feature.
4. Click **OK**.

CHAPTER 11

Uninstalling FARM

This chapter presents the following topics:

Uninstall FARM

To uninstall FARM:

Procedure

1. From the **Windows Start** menu, select **Programs and Features** › **Automated Failover Manager**, and click **Uninstall**.
2. Do one of the following:
   - To uninstall FARM, select **Uninstall Automated Failover 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 Automated Failover Manager**, and click **Next**.

CHAPTER 12

Additional FARM information

This chapter presents the following topics:

FARM new features

- FARM now supports dual stack IP compliance. Customers can input either IPv4 or IPv6 control station NAT.
- A new VDM priority "NA" is available. If a VDM is assigned NA priority, the AFM service will monitor the session, but will not trigger a failover in the event of a VDM error. The new priority allows you for the session monitoring without failing over for any reason. During manual operations, NA assigned VDMs are give lowest priority. The order in which VDM manual operations are carried out is High › Medium › Low › NA.
- A new Ignore tolerance time during failover option is available in the basic wizard. When selected, the AFM service will trigger a failover without the 5 iterations delay, thereby allowing you to immediately trigger a failover.

Note

In the case of a DM failover/panic, the AFM service will still wait 300 seconds for the local DM failover to complete.

FARM limitations

The following lists some of the limitations with eNAS File Auto Recovery. For a complete list, refer to the *VMAX 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.
- FAR sessions discovered in R2 site will not be listed in the VDM configuration page. The sessions will be listed under restore tab in VDM manual operations page.
- When a manual failover operation fails, the status of the session will be reported as "failed" in both failover and reverse tab. Since the status reported is the exit status of last action performed on the session, the "failed" status in other tab cannot be avoided. This is a design limitation.
- FARM does not support `nas_syncrep -Clean` operation. You must execute the Clean on the respective Control Station.
- 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-32-x86-en_US-3.1.35.
- FARM does not support downgrade and it is not recommended to install a lower version of FARM on top of a higher version.
- Post reboot/restart of VM/Host on which FARM is installed, the FARM service is not auto-started. Therefore, an administrator will need to manually start the service.

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 15 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
```

Critical-only events

If you check the **Express Failover Detection** check box in the **AFM Service** dialog box, the failover operation is based on these critical-only event types:

- Remote Ping
- Primary CS
- Primary Standby CS
- Secondary CS
- Secondary Standby CS
- Primary Data Mover
- Secondary Data Mover
- VDM network interface check. If the **Express Failover Detection** check box is
  - Selected, the VDM network interface check can tolerate a network failure of 500ms. VDM network failure is defined as the failure of any (single) configured VDM interface.
  - Unselected, the VDM network interface check can tolerate a network failure of 5 seconds. VDM network failure is defined as the failure of all configured VDM interfaces.

- VDM file system check
- VDM Local LUN status check
- VDM Remote LUN status check

FARM Environment Data Collect Sheet

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

Remote Ping Target	
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	

GRAB Utility

The user uses the Grab Utility to automatically collect the necessary data to contact EMC for further support.

The utility is located in the install directory and run from the Windows command line.

Here is an example from the FARM install directory:

```
C:\Program Files\EMC\FARM\bin>afm_grab.exe -d ALL -p nasadmin -r admin
```

Where "nasadmin" is the password of nasadmin user; "admin" is the password to RecoverPoint Appliance.

After running GRAB, the support directory in the FARM install can be zipped and sent for study.

The following details usage of the GRAB tool:

```
afm_grab.exe -d <context> [-u <user>][-c <customer>][-p <pw>][-r <pw>]

where

 -d <context>   defines the FARM-context where <context> is one of
                config\enas_vdm, ALL

for accessing the systems:
 -p <pw>        defines the password for nasadmin-user
 -r <pw>        defines the password for RecoverPoint-Appliance

for information use only:
 -u <user>      defines the UserName for the report
 -c <customer>  defines the CustomerName for the report
 -h             prints this help
```

CHAPTER 13

Troubleshooting FARM

This chapter presents the following topics:

Troubleshooting sequence

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

Procedure

1. Review the FARM limitations on page 110.
2. Verify that the following operations return **OK**:
   - Discover (as described in Discover on page 100)
   - Ping all (as described in Ping all on page 100)
   - Check status (as described in Check status on page 100)
3. Optionally, execute a failover and restore to verify that it completes successfully (as described in VDM failover on page 102 and , on page 102, 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 Log and configuration files on page 119 for details about these log files.

Log and configuration files

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

In addition, utilities for collecting additional troubleshooting information are located in `\nas\toos\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	Try running the failed command manually from the control station, and then take the following actions, depending on the results:
	• Cannot access the target device:
	  ▪ Check user accounts configured in FARM
	  ▪ Get support from eNAS as appropriate
	• Cannot retrieve device information or complete operations:
	  ▪ Check eNAS and get support from eNAS, as required

Failed to execute FARM interpreter commands	• Check the error messages for further actions to take. • Escalate to L3 or L4 support if no solution is available.

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.

Using the FARM GRAB utility

Use the FARM GRAB utility to collect and store the following item in the `<INSTALL_DIRECTORY>\Support`:

- FARM logs and configuration information
- Device status collected from the environment

To use this utility:

Procedure

1. Run the following command from the *FARM_HOME*`\bin` directory:

```
afm_grab.exe -d config\enas_vdm
```

2. Edit the `.\config\enas_vdm\info.sup` file to customize the collected data.

FARM protection/Failover prevention

When the FARM service is enabled (Gobal Settings) and running (Service window) FARM monitors and automatically fails over a system when a disaster occurs. Use the manual mode in the following cases:

- Deploying and testing FARM
- After a disaster failover (FARM provides one-click operation for failback)

FARM provides failover if a failover is not desired. For example, if a LUN error ocurrs, but eNAS services are still available, FARM will not failover. In this case, FARM sends a warning message.

In the **Global Settings** tab, FARM allows you to disable failover. In the deployment and testing phases, selecting this option will prevent unnecessary failover.

Frequently asked questions and additional information

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

Table 16 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 AFM works?	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.

Table 16 Frequently asked questions (continued)

Question	Answer
	FARM employs a 3-step usage model: 1) Configure, 2) Discover, and 3) Run. FARM users must follow this model for successful FARM operations. The **Configure** menu is enabled with NAS VDM DR environment. The **Discover** menu enables you to discover the configuration you created in the **Configure** menu. The **Run** menu enables you to run the required procedures for the DR configuration. If the underlying DR environment changes after you perform these tasks, you must re-run Discovery before running procedures. 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 failover, FARM can provide high-availability when used with the replication method.
How do changes in the eNAS environment impact FARM?	If the DR configuration changed (i.e. adding LUNs) the only required operation is Discover. FARM discovery will discover the environment. If the discovery is not executed after environment changes, no failover will occur if there is an error or a disaster. Configuration changes will be detected by the FARM Check Status function. You can configure SNMP to send notifications of configuration changes.
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.
What is the potential for FARM to cause a DU/DL situation? If there is potential, how can this best be mitigated?	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. A failover will only run once. FARM will not run a failover a second time. A discovery is needed for a reset. 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.
Is online help available within the FARM GUI for tasks that	Online help includes a list of return codes and their causes. Help also includes a PDF of the *FARM Product Guide*.

Table 16 Frequently asked questions (continued)

Question	Answer
require referencing documentation?	
Are all FARM functions/ commands/capabilities available remotely as if the servicer were on site?	If you have access to the host where FARM is installed, you can run all FARM functions. Complete the initial configuration in the GUI. All functions are available from the FARM Command Line Interface.
Can logs be collected via GUI?	The FARM Grab utility for collecting logs is available only from the command line.
Does FARM provide any clear visual indication of errors to the administrator at the time of occurrence?	No. Access Last Status/Events in the Discover menu for the latest status. If configured, you may receive SNMP traps.
Will the FARM logs get large enough that the logs need to be archived over time?	Yes. The user should archive logs. FARM will zip logs weekly to save space.

Troubleshooting checklist

The symptoms, probable causes, and recommended actions in Table 4 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 17 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 › SNMP Settings	Verify SNMP configuration with customer's environment. Escalate to AFM L3 if the issue cannot be resolved.
Discover › NAS/VDM Discovery › Ping All	1. Check the GUI error message for actions. 2. Manually check availability of the configured IP addresses. 3. Escalate to FARM L3 is the issue cannot be resolved.
Discover › VDM Discovery › Discover	1. Check the GUI error message for actions. 2. If the error code occurred when executing NAS/SYMCLI commands, check the credentials. 3. If the credentials are correct, forward the issue to eNAS support for further investigation. 4. Escalate to FARM L3 if the issue cannot be resolved.

Table 17 FARM troubleshooting (continued)

Issue reported at:	Actions
Discover › NAS/VDM Discovery › Reference Configuration	1. Check the result of the discover operation to verify that no error occurred. 2. If there are no errors and the problem cannot be resolved, escalate to FARM L3.
Discover › NAS/VDM Discovery › Show Last Status/Events	1. Check the result of the Check Status operation to verify that no error occurred. 2. If there are no errors and the problem cannot be resolved, escalate to FARM L3.
Run › Failover/Restore/ Reverse of VDM sessions	1. Check the GUI error message for actions. 2. If the error occurred when executing NAS/SYMCLI commands, check the credentials. 3. If the credentials are correct, open the log file failover.‹TIME_STAMP›.txt or restore.‹TIME_STAMP›.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: • Symptom of the issue • `failover.<Time_Stamp>.txt` and `restore.<Time_Stamp>.txt` • eNAS logs 4. If the actions above do not apply, escalate to FARM L3.
Discover › NAS/VDM Configurations › Discover Discover › NAS/VDM Configurations › Check Status	If AFM discovery fails, it might be due to the following reasons. • NAT IPs of control stations might be invalid. • Primary Control station on both R1 an R2 site might be unreachable. • Nasadmin login credentials might be invalid. Please check the above and retry the operation.
Run › Automated Failover -› AFM Service	1. Check the start/stop status of the AFM Service in the Windows service console, and verify the logon account. 2. Check the arbitrator_loop process in the Task Manager and the temp file arbit_loop.timestamp in the AFM installation folder to determine whether the AFM Service is started or stopped as expected. 3. If the error occurred when executing NAS/SYMCLI commands, check the credentials. 4. If the credentials are correct, forward the issue to eNAS support for further investigation. 5. Otherwise, escalate to AFM L3.

Table 17 FARM troubleshooting (continued)

Issue reported at:	Actions
Discover › NAS/VDM Configurations › Discover	If three loop files (`arbit_loop.timestamp`, `arbit_loop.current`, `arbit_loop.stop`) exist under AFM_HOME folder, discover will fail at the beginning with an error dialog. Delete these three loop files, and discover will work. **Note** These 3 files are used by FARM Service. Delete them when FARM Service is not running.
%AFM_HOME%\log \service_keeper.log	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. FARM sets service keeper timeout as 480s. FARM support can change service keeper configuration from %AFM_HOME%\ua.env: Below are default values: • service_keeper_timeout=480 • service_keeper_log=log\service_keeper.log • service_keeper=1