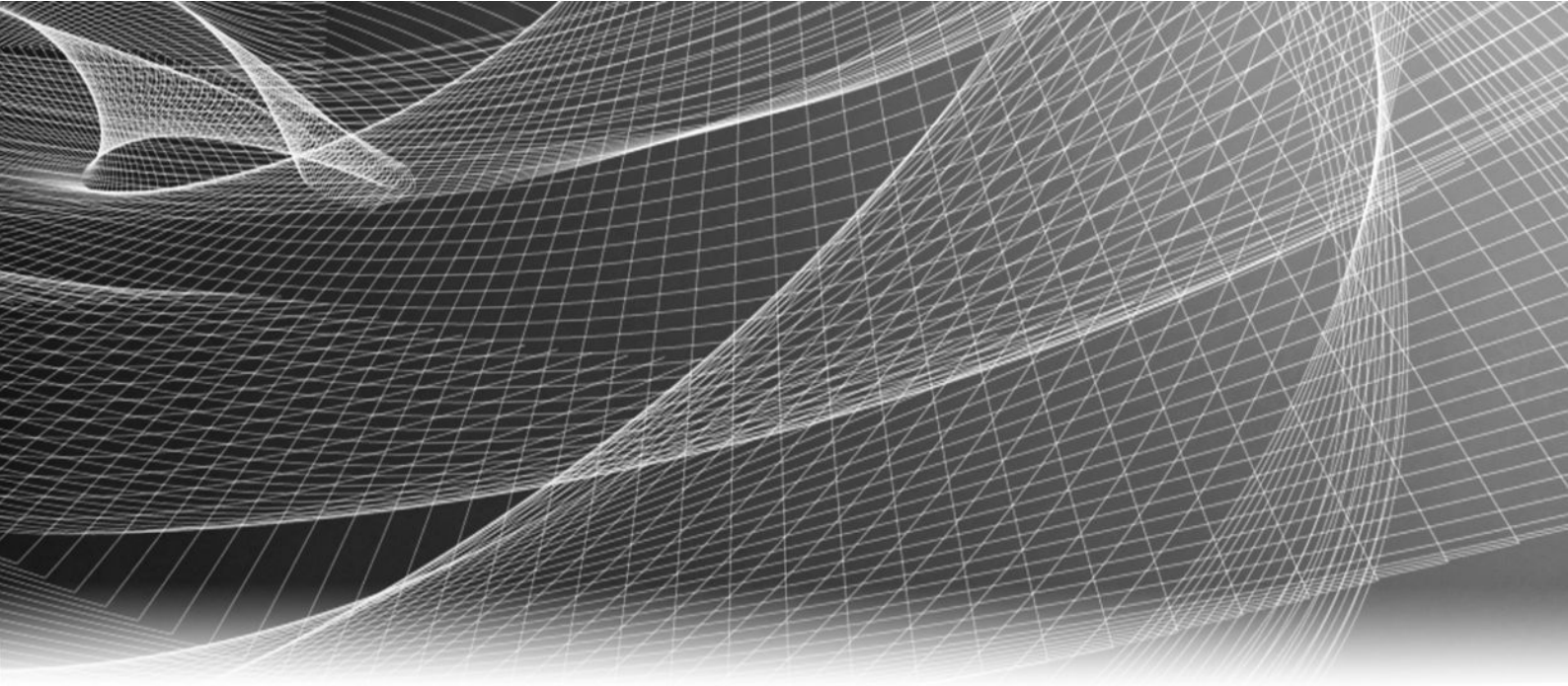


# EMC® Avamar® NDMP Accelerator for EMC NAS Systems

Version 7.2

## User Guide

302-001-797

REV 01

EMC²

Published June, 2015



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

# CONTENTS

# FIGURES

# TABLES

# PREFACE

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 technical support professional if a product does not function properly or does not function as described in this document.

**Note**

This document was accurate at publication time. Go to EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

### Purpose

This publication describes how to install, configure, administer, and use the Avamar NDMP Accelerator (accelerator) to back up and restore supported EMC Isilon, VNX, VNXe, and Celerra systems.

### Audience

The information in this publication is primarily intended for system administrators who are responsible for installing software and maintaining servers and clients on a network.

Persons using this publication should have current practical experience with:

- Network data management protocol (NDMP)
- Supported network attached storage (NAS) systems currently deployed at the site
- UNIX shell commands

### Revision history

The following table presents the revision history of this document.

**Table 1** Revision history

| Revision | Date | Description |
|---|---|---|
| 01 | June, 2015 | Initial release of Avamar 7.2. |

### Related documentation

The following EMC publications provide additional information:

- *EMC Avamar Compatibility and Interoperability Matrix*
- *EMC Avamar Release Notes*
- *EMC Avamar Administration Guide*
- *EMC Avamar Data Store Gen 4 Multi-Node System Installation Guide*
- *EMC Avamar Operational Best Practices*
- *EMC Avamar Product Security Guide*

### 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:

| | |
|---|---|
| **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:<br>• System code<br>• System output, such as an error message or script<br>• Pathnames, filenames, prompts, and syntax<br>• 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

Go to EMC Online Support and click Service Center. You will see several options for contacting EMC Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

### Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to techpubcomments@emc.com.

# CHAPTER 1

# Introduction

This chapter includes the following topics:

# Architecture

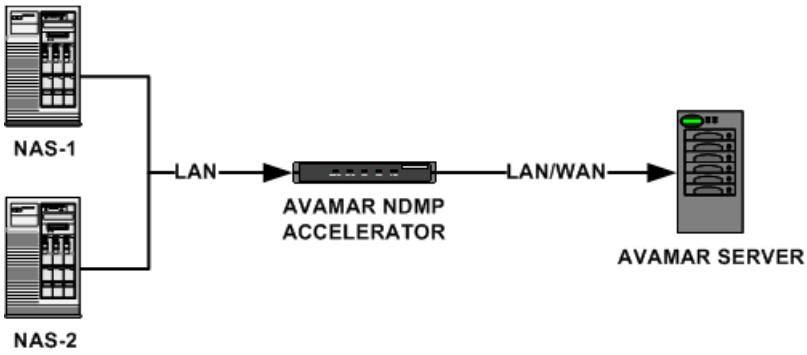
The following topic explains the Avamar system architecture for using the network data management protocol (NDMP) to protect data residing on network attached storage (NAS) systems.

## How Avamar works with NAS systems

In order to back up and restore data residing on NAS systems, Avamar uses a device called an Avamar NDMP Accelerator (accelerator).

The accelerator is a dedicated Avamar server node that functions as an Avamar client. The accelerator uses NDMP to interface with and access NDMP-based NAS systems.

**Figure 1** Accelerator deployment diagram




Data from the NAS system is not stored on the accelerator. The accelerator performs NDMP processing and real-time data deduplication, and then sends the data directly to the Avamar server.

You can connect the accelerator to either a Local Area Network (LAN) or Wide Area Network (WAN) with respect to the Avamar server. However, to ensure acceptable performance, the accelerator must be located on the same LAN as the NAS systems.

## Protecting multiple NAS systems with one accelerator

A single accelerator can support more than one NAS system. However, you cannot perform more than one backup at a time.

For example, consider two NAS systems: NAS-1 and NAS-2. Both NAS systems use the same accelerator and both systems belong to the same backup group.

When scheduled group backups are initiated, NAS-1 begins backing up immediately, while NAS-2's backup job is queued until NAS-1's job completes.

## Multiple data streams

All NDMP plug-ins have a **Maximum Concurrent Data Streams** setting, which controls the maximum number of simultaneous NDMP data streams that can be allocated to each NAS system backup or restore operation.

In order to implement NDMP multi-streaming, multiple simultaneous backups must be enabled on the accelerator, and each backup and restore operation must comprise multiple targets so that each target can be allocated to a separate NDMP data stream.

For VNX, VNXe, and Celerra systems, multi-streaming is automatically enabled when either root ("/") or an empty string is specified as the backup target. This causes Avamar

to automatically include any volumes returned by the NDMP `volume browse` command. Because an NDMP volume browse is performed before each backup operation, new volumes are automatically detected and backed up, eliminating the need to manually update backup datasets when new volumes are instanced on the NAS system.

The number of simultaneous data streams available is dependent on the NAS system version and the amount of RAM installed on the accelerator. The following table lists the maximum number of simultaneous data streams for various system configurations:

**Table 2** Multiple simultaneous data streams requirements

| NAS system | RAM | Maximum number of streams |
|---|---|---|
| EMC VNX OE 7.1.34.0, 7.0 | › 8 GB | 8 |
| EMC VNX OE 7.0, VNXe 2.3.0, or Celerra DART 6.0 | 8 GB | 4 |

## Data Domain system support

You can store backups on either the Avamar server or an EMC Data Domain® system. Backup metadata is stored on the Avamar server.

Before you can store backups on a Data Domain system, you must add the Data Domain system to the Avamar configuration by using Avamar Administrator. Then you select the Data Domain system in the plug-in options when you perform an on-demand backup or when you create a dataset for a scheduled backup. You can also use the command line interface (CLI) to perform backups to a Data Domain system.

The steps to restore backups are the same whether you restore from the Avamar server or a Data Domain system. The restore process determines the location of the backup and restores the backup.

The *EMC Avamar and EMC Data Domain System Integration Guide* provides more information about Data Domain systems in an Avamar environment, including detailed steps to add a Data Domain system to the Avamar configuration.

# Backup

This topic provides a conceptual overview of NDMP backups.

## Backup methods

You can perform both on-demand and scheduled NAS system backups with the accelerator:

- Use Avamar Administrator or the Avamar Management Console Command Line Interface (MCCLI) to perform both on-demand and scheduled backups.
- Use the `avndmp` command line interface to perform on-demand backups.

## Filer dump modes

Filer dump modes control whether a full or incremental backup is performed.

The first time each NAS system is backed up, Avamar performs a full (level 0) backup. For subsequent backups, you specify one of the following filer dump modes:

- **Prefer Incremental, but do a Full if required**—this mode allows Avamar to decide whether to perform a full (level 0) or incremental (level 1) backup each time a backup is performed. Most backups will be incrementals. However, this mode allows Avamar to detect certain conditions that should necessitate a full backup to ensure data compatibility.
- **Force a level 0 dump**—this mode causes Avamar to reprocess the entire NAS system. However, Avamar data deduplication will optimize the backup on the accelerator so that only new data is sent to the server. Although this requires additional processing time, the actual data sent to the Avamar server is the same as for an incremental (level 1) backup.
- **Force an incremental (level 1) dump**—this mode causes Avamar to perform an incremental (level 1) backup, even if certain conditions exist that should necessitate a full (level 0) backup.

Although full backups do take longer than incrementals because the NAS system sends all its data to the accelerator, Avamar's client-side deduplication only sends data to the Avamar server that has not previously been backed up.

# Restore

This topic provides a conceptual overview of NDMP restore.

## Restore types

When restoring from an NDMP backup, you can restore the entire backup, or selected folders and files.

## Restore destinations

Restore destinations can be the original NAS system, or any Linux or Windows client registered with the Avamar server.

If NDMP data is restored to an Avamar Linux or Windows client, it can be easily accessed and shared by establishing an NFS mount on Linux systems, or a CIFS mount on Windows systems.

## Restored metadata

When restoring to a NAS system, all native accounting information and Access Control Lists (ACLs) are restored.

When restoring to an NFS or CIFS mount, metadata such as ACLs, alternate data streams, attributes associated with hard links or file compression, is not restored.

# CHAPTER 2

# Installation and Configuration

This chapter includes the following topics:

# Preparing the system

These tasks prepare the system for accelerator software installation and configuration.

## Checking the system requirements

Ensure that the environment meets the client compatibility requirements before you install Avamar accelerator software.

NAS system compatibility requirements are available in the *EMC Avamar Compatibility and Interoperability Matrix* on EMC Online Support at https://support.EMC.com.

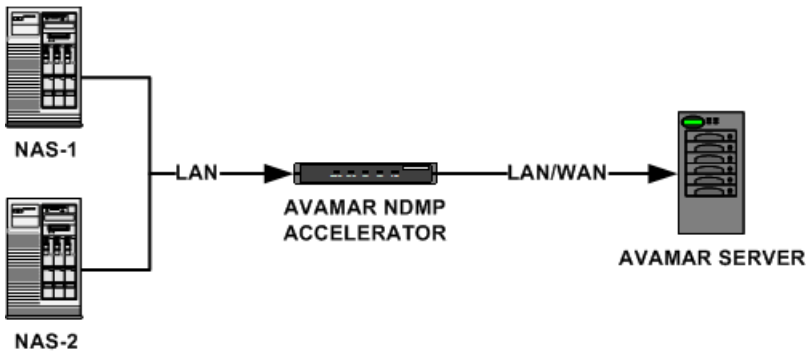
## Verifying network connectivity

This task verifies that the Avamar server, accelerator, and NAS systems are connected to the network and can communicate with one another.

### Before you begin

1. Connect the Avamar server, accelerator, and NAS systems to the network using 100BaseT or 1000BaseT network connections, as shown in the following figure:

**Figure 2** Networking diagram




   You can connect the accelerator to either a LAN or WAN with respect to the Avamar server. However, to ensure acceptable performance, the accelerator must be located on the same LAN as the NAS systems.

2. Add each hostname to corporate DNS, or modify `/etc/hosts` files on each network host such that:
   - The Avamar server and accelerator can resolve each other's hostnames.
   - The accelerator and NAS systems can resolve each other's hostnames.

   **Note**

   The Avamar server and NAS systems do not need to directly resolve each other's hostnames.

3. Ensure that the Avamar server, accelerator, and NAS systems are powered on.

### Procedure

1. Open a command shell and log in to the Avamar server as admin.
2. Type **`ping accelerator`**, where *accelerator* is the accelerator hostname as defined in corporate DNS.

   The accelerator responds to the `ping` command.

3. Open a command shell and log in to the accelerator as admin.
4. Type **`ping avamar-server`**, where *avamar-server* is the Avamar server hostname as defined in corporate DNS.

   The Avamar server responds to the `ping` command.
5. Type **`ping NAS-system`**, where *NAS-system* is the NAS system hostname as defined in corporate DNS.

   Type one **`ping NAS-system`** command for each NAS system you have connected to this accelerator.

   All NAS systems respond to the `ping` command.

## Creating an ndmp user account on the NAS system

Create a new "ndmp" user account on the NAS system. This user account will enable access to the NAS system for backups and restores.

### Procedure

1. Do one of the following:
   - If configuring an Isilon system, log in to OneFS Storage Administrator.
   - If configuring a VNX or VNXe system, log in to Unisphere.
   - If configuring a Celerra system, log in to Celerra Manager.
2. Create a user account named “ndmp.”
3. Specify a password for the ndmp user account.

   For VNX, VNXe and Celerra systems, by default, if there is a single Data Mover in the configuration, the name of the single Data Mover is “server_2.”

   For VNX, VNXe and Celerra systems, if there is a single Data Mover in the configuration, the default Data Mover name is “server_2.” There is also an option to transmit the md5sum of the NDMP username password (`-md5`), which the accelerator can accommodate. Therefore, an example command to add the “ndmp” user account to the “server_2” Data Mover, with the md5sum is:
   **`server_user server_2 -add -md5 ndmp`**
4. Note this password for future use.

   You type this password when configuring and registering the accelerator.
5. If configuring an Isilon system, set **DMA vendor** to **generic**.
6. Ensure that the ndmp user account has sufficient privileges to run NDMP jobs and access all data on the NAS system.

## Creating a browse user account on the Isilon system

This topic describes how to add a browse user account to Isilon systems.

In order to perform on-demand backups or create datasets for scheduled backups in Avamar Administrator, you must be able to browse the Isilon file system. These actions require typing a password for a local Isilon user account with following privileges:

- ISI_PRIV_LOGIN_PAPI
- ISI_PRIV_NS_TRAVERSE
- ISI_PRIV_NS_IFS_ACCESS

Although there are several methods for creating local Isilon user accounts, privileges can only be assigned to roles using the command line interface. Therefore, this procedure describes how to perform all the necessary actions (that is, creating a user account, creating a new role, and assigning the user and required privileges to that role) using the command line interface.

The *EMC Isilon OneFS Administration Guide* provides detailed information about creating local Isilon user accounts, and managing roles and privileges.

This procedure uses "av-browse-admin" and "namespace" as example user and role names, respectively. However, you can use any other user and role names that do not already exist in Isilon.

### Procedure

1. Establish an SSH connection to any node in the Isilon cluster.
2. Create and enable the av-browse-admin user account by typing:

   **isi auth users create av-browse-admin --password *password*--home-directory /ifs/home/av-browse-admin --enabled true**

   where *password* is the actual password assigned to the av-browse-admin user account. This is the password you will type when browsing the Isilon file system in Avamar Administrator.

3. Create the "namespace" role, and assign the "av-browse-admin" user and required privileges to the new role by typing:

   **isi auth roles create namespace**

   **isi auth roles modify namespace --add-user av-browse-admin**

   **isi auth roles modify namespace**
   **--add-priv ISI_PRIV_LOGIN_PAPI**

   **isi auth roles modify namespace**
   **--add-priv ISI_PRIV_NS_TRAVERSE**

   **isi auth roles modify namespace**
   **--add-priv ISI_PRIV_NS_IFS_ACCESS**

## Modifying NDMP snapTimeout parameters

For VNX, VNXe, or Celerra systems, to avoid problems with running multiple NDMP backups simultaneously, you must increase the value for the NDMP snapTimeout parameter.

The default value for the NDMP snapTimeout parameter is 5 minutes. Increase the value to at least 30 minutes. This does not apply to Isilon systems.

### Procedure

1. To modify NDMP `snap timeout` parameters on VNX or Celerra systems, type the following command from the Control Station command line interface:

   **server_param server_2 -f NDMP -m snapTimeout -v 30**

2. To modify NDMP `snap timeout` parameters on VNXe systems, use the graphical interface.

VNXe documentation provides additional information.

## Turning off deduplicated backups

To maximize the benefits of Avamar deduplicated backup, EMC recommends that you configure the VNX, VNXe, and Celerra system to "unpack" the deduplicated files before sending them to the accelerator for backup. This does not apply to Isilon systems.

### Procedure

1. To turn off deduplicated backups on VNX or Celerra systems, type the following command from the Control Station command line interface:

   **`fs_dedupe -default -set server_2 -backup_data_threshold 0`**

2. To disable deduplicated backups on VNXe systems, use the graphical interface.

   VNXe documentation provides additional information.

# Installing and configuring the accelerator software

These tasks install the Avamar Linux client and accelerator software, configure the accelerator settings, and register the accelerator with the Avamar server.

## Downloading the Avamar software

Connect to the Avamar server and download the accelerator software installation packages.

### Procedure

1. Open a web browser and type the following URL:

   **`http://`*`Avamarserver`***

   where *Avamarserver* is the Avamar server network hostname or IP address.

   The **EMC Avamar Web Restore** web page appears.
2. Click **Downloads**.
3. Click **+** next to the **NDMP Accelerator** folder.
4. Download both the `AvamarClient-linux-rhel4-x86_64-`*`version`*`.rpm` and `AvamarNDMP-linux-rhel4-x86_64-`*`version`*`.rpm` install packages to a temporary install folder such as `/tmp`.

## Installing the Avamar Client for Linux software

### Procedure

1. Open a command shell and log in to the accelerator as admin.
2. Switch user to root by typing **`su -`**, and then pressing **Enter**.
3. Change directory to the temporary install folder. For example, **`cd /tmp`**.
4. Install the software by typing:

   **`rpm -ivh AvamarClient-linux-rhel4-x86_64-`*`version`*`.rpm`**

5. Wait for the installation to complete.

The installation is complete when `avagent.d Info: Client Agent started.` appears in the command shell.

## Installing the Avamar accelerator software

### Before you begin

Ensure that the Avamar Client for Linux software is installed on the accelerator.

### Procedure

1. Open a command shell and log in to the accelerator as admin.
2. Switch user to root by typing **`su -`**, and then pressing **Enter**.
3. Change directory to the temporary install folder. For example, **`cd /tmp`**.
4. Install the software by typing:

   **`rpm -ivh AvamarNDMP-linux-rhel4-x86_64-`*`version`*`.rpm`**

5. Wait for the installation to complete.

   The installation is complete when the following appears in the command shell:

   ```
   You may run /usr/local/avamar/bin/avsetupndmp to register
   and activate this NDMP Accelerator Node with the
   Administrator server.
   ```

## Configuring the accelerator

This task configures various accelerator settings. Perform this task when you add a new accelerator to the system, or when you change settings for an existing accelerator.

### Before you begin

Ensure that the Avamar Client for Linux and accelerator software is installed on the accelerator.

### Procedure

1. Open a command shell and log in to the accelerator as admin.
2. Switch user to root by typing **`su -`**, and then pressing **Enter**.
3. Run the accelerator configuration utility by typing **`avsetupndmp`**.
4. Press **Enter** to accept the default action to stop all running agents.
5. Type the accelerator DNS name or IP address, and then press **Enter**.
6. Type the Avamar server DNS name or IP address, and then press **Enter**.
7. Type the Avamar server software root password, and then press **Enter**.

   **Note**

   This is the Avamar server software root password (also known as the GSAN root password), not the operating system root password.

8. Enable or disable multiple simultaneous backups:
   - To enable multiple simultaneous backups, type **`y`**, and then press **Enter**.
   - To disable multiple simultaneous backups, type **`n`**, and then press **Enter**.
9. From the **Configure individual system parameters** menu, type **`1`**, and then press **Enter**.

10. From the **Setting up a new system account** menu, specify which kind of NAS system to configure:
    - To configure an EMC VNXe, VNX, or Celerra system, type **1**, and then press **Enter**.
    - To configure an EMC Isilon system, type **2**, and then press **Enter**.
11. Type the NAS system DNS name or IP address, and then press **Enter**.
12. Type the NAS system NDMP user account name, and then press **Enter**.
13. Type the NAS system NDMP user account password, and then press **Enter**.
14. Re-type the NAS system NDMP user account password, and then press **Enter**.
15. Specify which password encoding scheme used by the NAS system:
    - If the encoding scheme is plain text, type **text**, and then press **Enter**.
    - If the encoding scheme is other than plain text, type **md5**, and then press **Enter**.
16. Type a short descriptive Avamar account name for this NAS system, and then press **Enter**.

    This is how that NAS system client instance will appear in Avamar Administrator. Any user-defined name is acceptable. However, this name must be unique. When adding a second instance of the same NAS system, ensure that you differentiate it from any existing Avamar account name.

17. Type the accelerator DNS name or IP address, and then press **Enter**.

    This is an accelerator DNS name or IP address that is resolvable by the NAS system.

18. From the **Configure individual system parameters** menu, continue or exit:
    - To add another NAS system or an additional Avamar client instance of an existing NAS system, type **1**, and then press **Enter**, and then follow the on-screen instructions.
    - Press **Enter** to exit this accelerator configuration utility session.

## Registering the accelerator

This task registers NAS system client instances on the accelerator with the Avamar server.

### Before you begin

Ensure that the Avamar Client for Linux and accelerator software is installed on the accelerator, and that the accelerator is configured.

### Procedure

1. Open a command shell and log in to the accelerator as admin.
2. Switch user to root by typing **su -**.
3. Run the client registration utility by typing **avregister**.

   **Note**

   The `avregister` command script attempts to register all unregistered client instances it detects on the accelerator.

4. Type the Avamar server DNS name or IP address, and then press **Enter**.
5. Specify an Avamar server domain for this client instance:

- Press **Enter** to accept the default domain (clients).
- Type a valid Avamar server domain path, and then press **Enter**.
  When typing a domain path (for example, clients/linux), do not include a slash (/) as the first character.

# Changing accelerator settings

This task describes how to use the `avsetupndmp` utility to change existing accelerator settings.

The `avsetupndmp` utility can be rerun as often as necessary to reconfigure accelerator settings.

Previously configured NAS system client instances can be edited or removed by choosing the respective option in the `avsetupndmp` menu.

To use the accelerator with a different Avamar server, you must also rerun `avregister`.

You must always rerun `avregister` after adding a new NAS system client instance.

## Enabling or disabling multiple simultaneous backups

Each accelerator can be configured to process backup requests consecutively (serially) or simultaneously (in parallel). This setting is applies to all NAS system client instances.

### Procedure

1. Open a command shell and log in to the accelerator as admin.
2. Switch user to root by typing **`su -`**, and then pressing **Enter**.
3. Run the accelerator configuration utility by typing **`avsetupndmp`**.
4. Press **Enter** to accept the default action to stop all running agents.
5. Type the accelerator DNS name or IP address, and then press **Enter**.
6. Type the Avamar server DNS name or IP address, and then press **Enter**.
7. Type the Avamar server software root password, and then press **Enter**.

   **Note**

   This is the Avamar server software root password (also known as the GSAN root password), not the operating system root password.

8. Enable or disable multiple simultaneous backups:
   - To enable multiple simultaneous backups, type **`y`**, and then press **Enter**.
   - To disable multiple simultaneous backups, type **`n`**, and then press **Enter**.
9. From the main menu, press **Enter** to exit this accelerator configuration utility session.

## Combining accounts (optional)

When the multiple simultaneous backups feature is enabled, and multiple accounts are used to back up multiple volumes on the same NAS system, the accelerator can become overloaded, causing backups to fail. If this occurs, combine the multiple accounts into a single account so that the accelerator can allow the maximum number of concurrent backups supported by that accelerator configuration without overloading.

**Note**

You can only combine accounts within the same Avamar domain.

### Procedure

1. Open a command shell and log in to the accelerator as admin.
2. Switch user to root by typing **`su -`**, and then pressing **Enter**.
3. Run the accelerator configuration utility by typing **`avsetupndmp`**.
4. Press **Enter** to accept the default action to stop all running agents.
5. Type the accelerator DNS name or IP address, and then press **Enter**.
6. Type the Avamar server DNS name or IP address, and then press **Enter**.
7. Type the Avamar server software root password, and then press **Enter**.

   **Note**

   This is the Avamar server software root password (also known as the GSAN root password), not the operating system root password.

8. Enable multiple simultaneous backups by typing **`y`**, and then pressing **Enter**.
9. From the **Configure individual system parameters** menu, type **`4`**, and then press **Enter**.
10. Type the name of the domain that contains the accounts to be combined.
11. Select the first account to combine by typing the number of the account and pressing **Enter**.
12. Select the second account to combine by typing the number of the account and pressing **Enter**.
13. From the main menu, continue or exit:
    - To combine additional accounts, type **`4`**, press **Enter**, and then follow the on-screen instructions.
    - Press **Enter** to exit this accelerator configuration utility session.

# Upgrading the accelerator software

To upgrade the accelerator, you must upgrade both the Avamar Client for Linux and AvamarNDMP software packages to the same version.

## Downloading the Avamar software

Connect to the Avamar server and download the accelerator software installation packages.

### Procedure

1. Open a web browser and type the following URL:

   **`http://Avamarserver`**

   where *Avamarserver* is the Avamar server network hostname or IP address.

   The **EMC Avamar Web Restore** web page appears.
2. Click **Downloads**.

3. Click **+** next to the **NDMP Accelerator** folder.
4. Download both the `AvamarClient-linux-rhel4-x86_64-version.rpm` and `AvamarNDMP-linux-rhel4-x86_64-version.rpm` install packages to a temporary install folder such as `/tmp`.

## Upgrading the accelerator software

Upgrading the accelerator using Linux software upgrade command (`rpm –U`) command preserves the existing configuration settings. You do not have to rerun `avsetupndmp` or `avregister`.

### Procedure

1. Open a command shell and log in to the accelerator as admin.
2. Switch user to root by typing **`su -`**, and then pressing **Enter**.
3. Upgrade the Linux client software by typing:

   **`rpm -U AvamarClient*`**

4. Upgrade the accelerator software by typing:

   **`rpm -U AvamarNDMP-linux-rhel4-x86_64-version*`**

## Running a newer accelerator with a older Avamar server

If you upgrade accelerator software to a newer version, but do not also upgrade the Avamar server software to the same version, you must manually update the `avtar` binary on the Avamar server utility node to the same version as the accelerator. Otherwise, you will not be able to continue backing up to the older Avamar server.

### Procedure

1. Open a command shell and log in:
   - For a single-node server, log in to the server as admin.
   - For a multinode server, log in to the utility node as admin.
2. Switch user to root by typing **`su -`**, and then pressing **Enter**.
3. Obtain the `dpnavclient-version.rhel4_64.x86_64.rpm` installation package, and then copy it to a temporary folder.
4. Install the software by typing:

   **`rpm -ivh dpnavclient-version.rhel4_64.x86_64.rpm`**

5. Verify the `avtar` version is correct by typing **`avtar --version`**.
6. Ensure that the `avtar` version is the same version as the `dpnavclient-version.rhel4_64.x86_64.rpm` installation package.

# Uninstalling the accelerator software

### Procedure

1. Open a command shell and log in to the accelerator as admin.
2. Switch user to root by typing **`su -`**, and then pressing **Enter**.
3. Query the RPM database for the currently installed Avamar software by typing:

   **`rpm -qa | grep Avamar`**

4. Note the Avamar accelerator and Linux client software package names.
5. Uninstall the Avamar accelerator software by typing:

   **rpm -e AvamarNDMP-linux-rhel4-x86_64-*version*.rpm**

   where *version* is the Avamar software version.
6. Uninstall the Avamar Linux client software by typing:

   **rpm -e AvamarClient-linux-rhel4-x86_64-*version*.rpm**

   where *version* is the Avamar software version.

# Configuring NTP time services on RHEL

This task configures NTP time services for accelerators running the Red Hat Enterprise Linux (RHEL) operating system.

**Note**

Do not perform this task on any accelerator running the SUSE Linux Enterprise Server (SLES) operating system.

## Procedure

1. Open a command shell and log in to the accelerator as admin.
2. Switch user to root by typing **su -**, and then pressing **Enter**.
3. Copy the `/etc/ntp.conf` and `/etc/ntp/step-tickers` files from the Avamar server utility node by typing:

   ```
   ssh -x root@accelerator
   cp -p /etc/ntp.conf{,.orig}
   scp root@utility-node:/etc/ntp.conf /etc/
   cp -p /etc/ntp/step-tickers{,.orig}
   scp root@utility-node:/etc/ntp/step-tickers /etc/ntp/
   ```

   where:

   - *accelerator* is the accelerator DNS name or IP address.
   - *utility-node* is the Avamar server utility node DNS name or IP address.
4. Restart the `ntpd` service by typing **service ntpd restart**.
5. Verify that the `ntpd` service started correctly by typing **service ntpd status**.
6. Wait 7 to 10 minutes for the system to fully settle.
7. Verify that the `ntpd` service is synchronizing time by typing **/usr/sbin/ntpq -pn**.
8. Verify that the values in the **reach** column eventually become nonzero and that an asterisk appears in the left column of one of the time servers.

   Ideally, all reach values are 377, which is an octal value meaning that the last eight time server contacts were all successful with no misses.
9. If any reach values are zero, then troubleshoot as follows:
   a. Verify that the list of time servers is correct in `/etc/ntp.conf`. Check this on server nodes 0.s and 0.0 as well.

The restrict statements in `/etc/ntp.conf` on nodes 0.s and 0.0 should permit other nodes, such as the accelerator, to obtain time.

b. If the reach values for nodes 0.s and 0.0 remain zero on the accelerator, then add the following line in `/etc/ntp.conf` on nodes 0.s and 0.0 for each accelerator:

**restrict *accelerator* nomodify**

where *accelerator* is the accelerator DNS name or IP address.

The objective is to remove the access restriction from the specified accelerator node.

c. Restart the ntpd service on nodes 0.s and 0.0 by typing **service ntpd restart**.

d. Verify that there are no errors, and that the ntpd service is synchronizing time by typing **/usr/sbin/ntpq -pn**.

If problems remain, refer to the following EMC knowledgebase articles for additional troubleshooting information:

- *esg119146 Trouble-shooting Avamar 'asktime' and related NTP issues*
- *esg113472 Frequently asked questions about the Avamar asktime utility*

10. Ensure that ntpd service will start at the next reboot by typing **chkconfig ntpd on**.

11. If you have not already done so, set the local time zone on the accelerator:

a. Type **/usr/sbin/timeconfig**.

For best results, set accelerator local time to that of the NAS system so that both client and accelerator log files correlate.

b. Select the correct local time zone from the time zone menu.

c. Verify that the output of the date command is accurate by typing **date**.

# Configuring the accelerator for dual NIC operation (optional)

This task configures the accelerator to use two Network Interface Cards (NICs) in order to maximize data throughput in certain configurations, such as backing up multiple data streams to a Data Domain system.

### Before you begin

Ensure that the Avamar Client for Linux and accelerator software is installed on the accelerator, and that the accelerator is configured and registered with the Avamar server.

To maximize data throughput, segregate the NAS system network traffic from the Avamar server network traffic. Do this by configuring a second NIC such that one NIC accepts NAS system traffic, and the other NIC connects to the Avamar server.

NAS systems can be on the same or different subnets, and are not required to be on the same subnet as the Avamar server.

### Procedure

1. Obtain and record the following information:
   - IP address for the secondary NIC
   - Subnet mask for the accelerator

- Hostname for the secondary NIC
- Gateway IP address of the subnet where the accelerator resides
- IP address of the NAS system

2. Open a command shell and log in to the accelerator as admin.
3. Switch user to root by typing **`su -`**, and then pressing **Enter**.
4. Run the YaST2 configuration utility by typing **`yast2`**, and then pressing **Enter**.
5. On the **YaST2 Control Center** main screen, select **Network Devices** › **Network Settings**, and then press **Enter**.

   **Note**

   Use **Tab** or cursor keys to select menus, submenus, and fields.

6. On the **Network Settings** screen, highlight the secondary NIC list entry, and then press **F4** to edit secondary NIC settings.
7. On the **Network Card Setup** screen, highlight **Statically assigned IP address**, and then press **Enter**.

   Complete the following:

   - In the **IP Address** field, type the IP address for the secondary NIC.
   - In the **Subnet Mask** field, type the subnet mask for the accelerator.
   - In the **Hostname** field, replace the default hostname with the correct hostname of the secondary NIC.
   - Note and record the device name in the **Configuration Name** field.
     Typically, the device name is eth1.

8. Highlight **Next**, and then press **Enter**.
9. On the **Network Settings** screen, highlight **Routing**, and then press **Enter**.
10. In the **Default Gateway** field, ensure that the **Default Gateway** setting is correct. If not, type the correct gateway IP address of the subnet where the accelerator resides.
11. Highlight **Add**, and then press **Enter**.

    Complete the following:

    - In the **Destination** field, type the NAS system IP address.
    - In the **Device** field, type the device name previously noted on the **Network Card Setup** screen.
      Typically, the device name is eth1.
    - In the **Gateway** field, type the IP address of the secondary NIC.
    - In the **Netmask** field, type the subnet mask for this route.
      Typically, the subnet mask will be 255.255.255.255 when a single NAS system is backing up to an accelerator. However, when multiple NAS systems are backing up to the same accelerator, the subnet mask might be different.

12. Exit the YaST2 configuration utility:

    - On the **Network Settings** screen, highlight **OK**, and then press **Enter**.
    - On the **YaST2 Control Center** main screen, highlight **Quit**, and then press **Enter**.

# CHAPTER 3

# Backup

This chapter includes the following topics:

# Limitations

These are the known limitations of Avamar NDMP backup.

**Mixed backups**
Avamar does not support:

- Full backups on a Data Domain system and incremental or differential backups on the Avamar server
- Full backups on the Avamar server and incremental or differential backups on a Data Domain system
- Full backups on one Data Domain system and incremental or differential backups on another Data Domain system

**Wild cards**
You cannot use wild card characters to specify a backup target (that is, which volumes or folders to include in the backup). This is an NDMP limitation.

**Maximum path length**
When backing up any EMC NAS system, paths cannot be longer than 4,096 characters.

**Maximum number of files**
Each individual Avamar backup of an EMC NAS system can contain a maximum of 10 million files.

**Multiple datasets for the same NAS system**
When using multiple datasets to back up the same NAS system (for example, using one dataset for full backups and another for incrementals), the exclude lists must be identical.

When full and incremental exclude lists differ, the actual system behavior differs according to the type of incremental backup specified in the dataset:

- If the dataset specifies **Prefer incremental, but do a Full if required**, a full backup runs.
- If the dataset specifies **Force an incremental (level 1) dump**, the backup fails.

**Incremental backups should only be performed at the root volume level**
When backing up VNX, VNXe or Celerra systems, you should only perform incremental backups at the root volume level. Avamar defaults to always performing full (level-0) backups of lower level folders and subfolders. You can override the default behavior by selecting the **Filer dump modes Force an incremental (level 1) dump** plug-in option (either in the backup dataset or the on-demand backup options). However, it must be understood that performing an incremental (level-1) backup at any level other than the root volume is known to be less reliable than a full (level-0) backup, and might result in backup errors.

**Incremental backup memory usage**
When backing up VNX, VNXe or Celerra systems, any incremental backup that includes many files might fail due to memory limitations.

**UNIX hardlinks in incremental backups**
When performing incremental backups, some UNIX hardlinks with non-ASCII characters in the name might not be processed correctly. For best results, exclude these hardlinks from incremental backups. If this is not possible, perform level-0 backups instead.

### Avamar Administrator limitations

These are the known limitations of Avamar Administrator to browse and display information about NDMP backups. None of these limitations affect data integrity or the ability to restore data from NDMP backups.

- International characters—When browsing NDMP backups, folder and file names containing international characters might not display correctly.
- Folder bytes reported—Folder sizes are often shown to be slightly smaller than the aggregate size of the folder contents.
- File size variance—The size of a backup from a NAS system differs from the size of the on-disk data. For example, the reported size of a backup is the size on the deduplicated Avamar server disk, not the actual file size.
- Small backup bytes reported—The number of bytes shown for small NDMP backups might be a slightly larger than the actual size. This behavior is normal because the NAS system adds a small amount of data to each backup.
- User and group names—When listing the contents of a backup, user and group names appear as numbers instead of plain text names.
- Browsing folders and files—When browsing a VNX, VNXe, or Celerra file system to create a dataset or perform an on-demand backup, only volumes are visible. You cannot browse into volumes to view individual folders or files. This limitation does not apply to Isilon systems.

# Performing on-demand backups

### Procedure

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The **Backup, Restore and Manage** window appears.
2. Click the **Backup** tab.
3. Select the accelerator in the top-left tree pane.
4. Select a NAS system client instance in the bottom-left pane.
5. Select the data to back up:

| NAS System | Steps |
|---|---|
| **For VNX, VNXe, or Celerra systems** | a. In the pane, select the**EMC Celerra/VNX via NDMP** plug-in.<br>b. Select one or more volume checkboxes. |
| **For Isilon systems** | a. In the **Browse for Files, Folders, or Directories** pane, select the **Isilon via NDMP** plug-in.<br>b. In the **Browse Command Line Options** dialog box type the Isilon browse password.<br>c. Click **OK** to close the **Browse Command Line Options** dialog box.<br>d. Select one or more top-level directory checkboxes beneath the `/ifs` root directory. |

6. Select **Actions** › **Backup Now**.

   The **On Demand Backup Options** dialog box appears.

7. Select the backup retention setting:
   - To automatically delete this backup from the Avamar server after a specific amount of time, select **Retention period** and then specify the number of days, weeks, months, or years for the retention period.
   - To automatically delete this backup from the Avamar server on a specific calendar date, select **End date** and browse to that date on the calendar.
   - To keep this backup for as long as this client remains active in the Avamar server, select **No end date**.
8. From the **Avamar encryption method** list, select the encryption method to use for data transfer between the client and the Avamar server during the backup.

   The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides additional information.
9. (Optional) Set plug-in options:

   These settings are all optional. In most cases, system default settings are the optimum settings for on-demand NDMP backups.

   a. Click **More Options**.

      The **Backup Command Line Options** dialog box appears.

   b. Select the **Show Advanced Options** checkbox.

   c. From the **Maximum Concurrent Data Streams** list, select the maximum number of data streams that can be utilized concurrently during the backup.

   d. From the **Filer Dump Mode** list, select the type of backup to perform.

      Forcing a full (level 0) dump resends all data in the requested volume from the NAS system to the accelerator. This is not recommended.

      For best results, always perform incremental backups at the volume level. Do not force incremental backups of lower level folders and subfolders because this can cause backup errors.

   e. In the **Backup label** field, specify a descriptive label for the backup.

   f. To store this backup on a Data Domain system, select the **Store backup on Data Domain System** checkbox, and then select a Data Domain system from the list.

   g. From the **Encryption method to Data Domain system** list, select the encryption method to use for data transfer between the client and the Data Domain system during the backup.

   h. To run a script before the backup operation starts, type a script file name in the **Run user-defined script at start of backup** field. The script must reside in the accelerator `/usr/local/avamar/etc/scripts` directory.

   i. To run a script after the backup operation ends, type a script file name in the **Run user-defined script at end of backup** field. The script must reside in the accelerator `/usr/local/avamar/etc/scripts` directory.

   j. To manually enter other plug-in options as free text, click **More**, type the plug-in option name and value in the **Enter Attribute** and **Enter Attribute Value** fields, respectively, and then click **+** (Add to list).

   k. Click **OK.**

The **Backup Command Line Options** dialog box closes.

10. Click **OK**.

    The **On Demand Backup Options** dialog box closes and the following status message appears: `Backup initiated`.

11. Click **OK**.

# Scheduling backups

Perform these tasks to schedule regular recurring backups of NAS systems.

## Creating a dataset

A dataset defines the data included in each scheduled backup, and settings that control plug-in behavior during the backup.

### Procedure

1. In Avamar Administrator, select **Tools** › **Manage Datasets**.

   The **Manage All Datasets** window appears.

2. Click **New**.

   The **New Dataset** dialog box appears.

3. In the **Name** field, type a name for the dataset.

   The name can include alphanumeric characters (A-Z, a-z, 0-9), period (.), hyphen (-), and underscore (_). Do not use Unicode characters or the following special characters: ` ~ ! @ # $ % ^ & * ( ) = + [ ] { } | \ / ; : ' " ‹ › , ?

4. For VNX, VNXe, or Celerra systems, select **Enter Explicitly**, and then select **EMC Celerra/VNX via NDMP** from the **Select Plug-In Type** list.
5. For Isilon systems, select **Enter Explicitly**, and then select **Isilon via NDMP** from the **Select Plug-In Type** list.
6. (Optional) Limit the dataset to specific volumes:
   a. Select **Select Files and/or Folders**.
   b. Click **...** (Browse for files and/or folders).
   c. In the **Select Files and/or Folders** dialog box, select a client from the **Clients** tree.
   d. Expand the plug-in node in the middle pane to view a list of volumes on the client.
   e. If the **Browse Command Line Options** dialog box appears, enter a password and click **OK**.
   f. Select the checkbox next to one or more volumes.

      These volumes will be included in this dataset.

   g. Click **OK**.
7. (Optional) Specify directories, folders, or files you want to exclude in the **Exclusions** tab.
8. Disregard **Inclusions** tab settings. Inclusions cannot be specified for any NAS systems.
9. (Optional) Set plug-in options in the **Options** tab:

   These settings are all optional. In most cases, system default settings are the optimum settings for scheduled NDMP backups.

a. For VNX, VNXe, or Celerra systems, select **Enter Explicitly**, and then select **EMC Celerra/VNX via NDMP** from the **Select Plug-In Type** list.

b. For Isilon systems, select **Enter Explicitly**, and then select **Isilon via NDMP** from the **Select Plug-In Type** list.

c. Select the **Show Advanced Options** checkbox.

d. From the **Maximum Concurrent Data Streams** list, select the maximum number of data streams that can be utilized concurrently during the backup.

e. From the **Filer Dump Mode** list, select the type of backup to perform.

Forcing a full (level 0) dump resends all data in the requested volume from the NAS system to the accelerator. This is not recommended.

For best results, always perform incremental backups at the volume level. Do not force incremental backups of lower level folders and subfolders because this can cause backup errors.

f. To store this backup on a Data Domain system, select the **Store backup on Data Domain System** checkbox, and then select a Data Domain system from the list.

g. From the **Encryption method to Data Domain system** list, select the encryption method to use for data transfer between the client and the Data Domain system during the backup.

h. To run a script before the backup operation starts, type a script file name in the **Run user-defined script at start of backup** field. The script must reside in the accelerator `/usr/local/avamar/etc/scripts` directory.

i. To run a script after the backup operation ends, type a script file name in the **Run user-defined script at end of backup** field. The script must reside in the accelerator `/usr/local/avamar/etc/scripts` directory.

j. To manually enter other plug-in options as free text, click **More**, type to plug-in option name and value in the **Enter Attribute** and **Enter Attribute Value** fields, respectively, and then click **+** (Add to list).

10. Click **OK** to close the **New Dataset** dialog box.

## Creating a group

A group is a collection of Avamar clients that use the same policies to implement scheduled backups. Member clients must all be in the same Avamar domain. When you create a group, you define the dataset, schedule, and retention policy that apply for scheduled backups of the group. These settings comprise the group policy, which controls backup behavior for all members of the group unless you override these settings at the client level.

### Procedure

1. In Avamar Administrator, click **Policy** launcher button.

   The **Policy** window appears.

2. Click the **Policy Management** tab.
3. Click the **Groups** tab.
4. In the tree pane, select a domain location for this group.

   This domain is where the new group object will be stored. It is generally best to store groups at the Avamar server (root) domain.

5. Select **Actions** › **Group** › **New** › **Backup Group**.

   The **New Group** wizard appears.

6. In the **Name** field, type a name for the group.

   The name can include alphanumeric characters (A-Z, a-z, 0-9), period (.), hyphen (-), and underscore (_). Do not use Unicode characters or the following special characters: ` ~ ! @ # $ % ^ & * ( ) = + [ ] { } | \ / ; : ' " ‹ › , ?

7. Clear the **Disabled** checkbox to use this group for scheduled client backups.

   Selecting the checkbox disables backups for the group.

8. From the **Avamar encryption method** list, select an encryption method to use for data transfer between the Avamar server and the client during the backup.

   The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides additional information.

9. (Optional) Select **Override Schedule** to override the assigned schedule for this group:
   - To skip the next scheduled backup, select **Skip Next Backup**.
   - To perform the next scheduled backup one time only, select **Run Next Backup Once**.

10. Click **Next**, and then select a dataset from the **Select An Existing Dataset** list.
11. Click **Next**, and then select a schedule from the **Select An Existing Schedule** list.
12. Click **Next**, and then select a retention policy from the **Select An Existing Retention Policy** list.
13. Click **Next**, and then select one or more clients to be members of this group:
    a. Select a domain in the **Choose Domain** pane.

       A list of clients appears in the **Choose Clients** pane.

    b. (Optional) Select the **Show sub-domain clients** checkbox to see more clients.

    c. Click the checkbox next to one or more clients to include them in this group.

    d. To remove a client from the group, select the client from in **Members** list, and then click the red **X**.

14. Save and exit:
    a. Click **Finish** to close the **New Group** wizard.

    b. Click **OK** to close the **Policy** window.

## Enabling scheduled backups

Scheduled backups occur only for enabled groups. Groups are disabled by default unless you select the **Enabled** checkbox on the first page of the **New Group** wizard. If you did not enable the group when you created it, perform the following steps to enable scheduled backups to occur.

### Before you begin

Ensure that you have created a group containing the NAS systems you want to back up.

### Procedure

1. In Avamar Administrator, click **Policy** launcher button.

   The **Policy** window appears.

2. Click the **Policy Management** tab.
3. Click the **Groups** tab.
4. In the tree pane, select the domain where the group resides.
5. Locate the group in the right pane.
6. If **Disabled** is **Yes**, then select **Actions** › **Group** › **Disable Group** to enable it.

   **Disabled** changes to **No**.

# Monitoring backups

You can monitor backups to ensure that the backups complete successfully and to troubleshoot issues. The Activity Monitor in Avamar Administrator enables you to view status information for both on-demand and scheduled backups.

### Procedure

1. In Avamar Administrator, click the **Activity** launcher button.

   The **Activity** window appears.
2. Click the **Activity Monitor** tab.

   A list of all activities appears.
3. To filter the results to display only backup activity, select **Actions** › **Filter**.

   The **Filter Activity** dialog box appears.
4. Select **All Backups** from the **Type** list.
5. Click **OK**.

# Canceling backups

You can cancel a backup any time before it completes. The cancellation might take five minutes or longer. The backup may complete before the cancellation finishes.

### Procedure

1. In Avamar Administrator, click the **Activity** launcher button.

   The **Activity** window appears.
2. Click the **Activity Monitor** tab.

   A list of all activities appears.
3. Select the backup from the list.
4. Select **Actions** › **Cancel Activity**.

   A confirmation message appears.
5. Click **Yes**.

# CHAPTER 4

# Restore

This chapter includes the following topics:

# Limitations

These are the known limitations of Avamar NDMP restore.

**Non-NDMP client backups**
Volumes, folders, and files that were originally backed up from other Avamar client types are fully browsable by Avamar Administrator. However, these entities cannot be restored to an NAS system.

**Overwrite behavior**
None of the overwrite and open file options are applicable when performing an NDMP restore. This is an inherent limitation of NDMP, which always overwrites existing files when restoring.

**Web services restores with external authentication**
You cannot restore data from an NDMP backup using Avamar Web services if the user who initiates the restore is authenticated using an external authentication system such as LDAP or Windows Active Directory.

# Restoring to the original NAS system

This task restores data from an NDMP backup to the original NAS system.

**Procedure**

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The **Backup & Restore** window appears.
2. From the list of clients, select the accelerator.

   A list of NAS system clients registered with that accelerator appears in the lower pane.
3. Select the NAS system client instance.
4. Click the **Restore** tab.
5. Click the **By Date** tab.

   Valid backups occurred on dates with a yellow highlight.
6. Select the backup date from the calendar.

   A list of backups on that date appears in the **Backups** table next to the calendar.
7. Select a backup from the **Backups** table.
8. In the lower-right pane, expand the folder tree to view a list of volumes.
9. Select the checkbox next to the volume in the left section of the **Contents of Backup** pane.

   The files and folders on the volume appear in the right section of the **Contents of Backup** pane.
10. (Optional) To restore individual folders or files, select the checkbox next to each folder or file you want to restore.
11. Select **Actions** › **Restore Now**.

    The **Restore Options** dialog box appears.
12. Ensure that the correct plug-in is selected in the **Restore Plug-in** list.
13. From the **Avamar encryption method** list, select the encryption method for data transfer between the Avamar server and the client during the restore.

The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides details.

14. Select **Restore everything to its original location**.
15. (Optional) Set plug-in options:

    These settings are all optional. In most cases, system default settings are the optimum settings for restores.

    a. Click **More Options**.

       The **Restore Command Line Options** dialog box appears.

    b. From the **Maximum Concurrent Data Streams** list, select the maximum number of data streams that can be utilized concurrently during the restore.

    c. From the **Encryption method to Data Domain system** list, select the encryption method to use for data transfer between the client and the Data Domain system during the backup.

    d. To run a script before the restore operation starts, type a script file name in the **Run user-defined script at start of restore** field. The script must reside in the accelerator `/usr/local/avamar/etc/scripts` directory.

    e. To run a script after the restore operation ends, type a script file name in the **Run user-defined script at end of restore** field. The script must reside in the accelerator `/usr/local/avamar/etc/scripts` directory.

    f. To manually enter other plug-in options as free text, click **More**, type to plug-in option name and value in the **Enter Attribute** and **Enter Attribute Value** fields, respectively, and then click **+** (Add to list).

    g. Click **OK.**

       The **Restore Command Line Options** dialog box closes.
16. Click **OK** to close the **Restore Options** dialog box.

# Restoring to a Linux or Windows client

This task restores data from an NDMP backup to a Linux or Windows client file system. After NDMP data is restored to an Avamar Linux or Windows client, the data can be easily accessed and shared by establishing an NFS mount on Linux systems, or a CIFS mount on Windows systems.

### Procedure

1. In Avamar Administrator, click the **Backup & Restore** launcher button.

   The **Backup & Restore** window appears.
2. From the list of clients, select the accelerator.

   A list of NAS system clients registered with that accelerator appears in the lower pane.
3. Select the NAS system client instance.
4. Click the **Restore** tab.
5. Click the **By Date** tab.

   Valid backups occurred on dates with a yellow highlight.

6. Select the backup date from the calendar.

   A list of backups on that date appears in the **Backups** table next to the calendar.

7. Select a backup from the **Backups** table.
8. In the lower-right pane, expand the folder tree to view a list of volumes.
9. Select the checkbox next to the volume in the left section of the **Contents of Backup** pane.

   The files and folders on the volume appear in the right section of the **Contents of Backup** pane.

10. (Optional) To restore individual folders or files, select the checkbox next to each folder or file you want to restore.
11. Select **Actions** › **Restore Now**.

    The **Restore Options** dialog box appears.

12. Select the destination Linux or Windows client:

    a. Click the **Browse** button next to the **Restore Destination Client** field.

       The **Browse for Client Destination** dialog box appears.

    b. Browse to and select the destination client.

    c. Click **OK**.

       The **Browse for Client Destination** dialog box closes.

13. Ensure that the correct plug-in is selected in the **Restore Plug-in** list.
14. From the **Avamar encryption method** list, select the encryption method for data transfer between the Avamar server and the client during the restore.

    The encryption technology and bit strength for a client/server connection depends on several factors, including the client operating system and Avamar server version. The *EMC Avamar Product Security Guide* provides details.

15. Select **Restore everything to a different location**.

    The buttons below the **Items Marked for Restore list** become active.

16. Click **Set Destination**.

    The **Set Destination** dialog box appears.

17. Click **Browse**.

    The **Browse for File, Folder, or Directory** dialog box appears.

18. Expand the list in the left pane, and then select the checkbox next to the target volume.
19. For Isilon systems:

    a. In the **Browse Command Line Options** dialog box, enter the Isilon browse password, and then click **OK**.

       The **Browse Command Line Options** dialog box closes. The `/ifs` root directory appears.

    b. Select one or more directory checkboxes.

20. Click **OK**.

    The **Browse for File, Folder, or Directory** dialog box closes.

21. In the **Restore Options** dialog box, click **More Options**.

22. (Optional) Set plug-in options:

    These settings are all optional. In most cases, system default settings are the optimum settings for restores.

    a. Click **More Options**.

       The **Restore Command Line Options** dialog box appears.

    b. From the **Maximum Concurrent Data Streams** list, select the maximum number of data streams that can be utilized concurrently during the restore.

    c. From the **Encryption method from Data Domain system** list, select the encryption method to use for data transfer between the Data Domain system and the client during the restore.

    d. To run a script before the restore operation starts, type a script file name in the **Run user-defined script at start of restore** field. The script must reside in the accelerator `/usr/local/avamar/etc/scripts` directory.

    e. To run a script after the restore operation ends, type a script file name in the **Run user-defined script at end of restore** field. The script must reside in the accelerator `/usr/local/avamar/etc/scripts` directory.

    f. To manually enter other plug-in options as free text, click **More**, type the plug-in option name and value in the **Enter Attribute** and **Enter Attribute Value** fields, respectively, and then click **+** (Add to list).

    g. Click **OK.**

       The **Restore Command Line Options** dialog box closes.

23. Click **OK** to close the **Restore Options** dialog box.

# Monitoring restores

You can monitor restores to ensure that the restores complete successfully and to troubleshoot issues. The Activity Monitor in Avamar Administrator enables you to view status information for restores.

### Procedure

1. In Avamar Administrator, click the **Activity** launcher button.

   The **Activity** window appears.

2. Click the **Activity Monitor** tab.

   A list of all activities appears.

3. To filter the results to display only restore activity, select **Actions** › **Filter**.

   The **Filter Activity** dialog box appears.

4. Select **Restore** from the **Type** list.

5. Click **OK.**

# Canceling restores

You can cancel a restore any time before the restore completes. The cancellation might take five minutes or longer. The restore may complete before the cancellation finishes.

### Procedure

1. In Avamar Administrator, click the **Activity** launcher button.

   The **Activity** window appears.
2. Click the **Activity Monitor** tab.

   A list of all activities appears.
3. Select the restore from the list.
4. Select **Actions** › **Cancel Activity**.

   A confirmation message appears.
5. Click **Yes**.

# APPENDIX A

# Plug-in Options

This appendix includes the following topics:

# How to set plug-in options

Plug-in options enable you to control specific actions for on-demand backups, restores, and scheduled backups. The plug-in options that are available depend on the operation type and plug-in type.

You specify plug-in options in Avamar Administrator for on-demand backup or restore operations, or when you create a dataset for a scheduled backup. You set plug-in options with the graphical user interface (GUI) controls (text boxes, checkboxes, radio buttons, and so forth). In addition to using the GUI controls for the options, you can type an option and its value in the **Enter Attribute** and **Enter Attribute Value** fields.

**NOTICE**

The Avamar software does not check or validate the information that you type in the **Enter Attribute** and **Enter Attribute Value** fields. In addition, the values in the **Enter Attribute** and **Enter Attribute Value** fields override settings that you specify with the GUI controls for the options.

# Backup options

These plug-in options are available when you perform an on-demand backup, or configure a dataset using an NDMP plug-in.

**Table 3** Backup plug-in options

| Setting | Description |
|---|---|
| Maximum Concurrent Data Streams | Specifies the maximum number of streams that can be processed concurrently. |
| Filer Dump Mode | One of the following values:<br>• Prefer Incremental, but do a Full if required<br>• Force a level 0 dump<br>• Force an incremental (level 1) dump |
| Backup label | Custom descriptive label for the backup.<br>This option is only available during on-demand backups. |
| Store backup on Data Domain system | To store the backup on a Data Domain system instead of the Avamar server, select the checkbox and then select a Data Domain system from the list.<br>To enable this option, add a Data Domain system to the Avamar configuration. The *EMC Avamar and EMC Data Domain System Integration Guide* provides instructions. |
| Encryption method to Data Domain system | Specifies the encryption method for data transfer between the client and the Data Domain system during the backup. |
| Run user-defined script at start of backup | File name of a script to be run before each backup target is processed. The script must reside in the accelerator `/usr/local/avamar/etc/scripts` directory. |

**Table 3** Backup plug-in options (continued)

| Setting | Description |
|---|---|
| Run user-defined script at end of backup | File name of a script to be run after each backup target is processed. The script must reside in the accelerator `/usr/local/avamar/etc/scripts` directory. |
| Isilon Browse User Name | User account on the Isilon server with sufficient privileges for browsing the Isilon file system. |
| Isilon Browse Password | Password for the Isilon browse user account. |

# Restore options

These plug-in options are available when you perform a restore using an NDMP plug-in.

**Table 4** Restore plug-in options

| Setting | Description |
|---|---|
| Maximum Concurrent Data Streams | Specifies the maximum number of streams that can be processed concurrently. |
| Encryption method from Data Domain system | Specifies the encryption method for data transfer between the Data Domain system and the client during the restore. |
| Run user-defined script at start of restore | File name of a script to be run before each restore target is processed. The script must reside in the accelerator `/usr/local/avamar/etc/scripts` directory. |
| Run user-defined script at end of restore | File name of a script to be run each restore target is processed. The script must reside in the accelerator `/usr/local/avamar/etc/scripts` directory. |

# APPENDIX B

# Command Line Interface

This appendix includes the following topics:

# avndmp

The avndmp command provides a Command Line Interface (CLI) for backing up and restoring data to supported NAS systems.

The avndmp binary is located in the accelerator /usr/local/avamar/bin directory. To use the avndmp CLI, open a command shell, log in to the accelerator as admin, and then enter avndmp commands and options.

### Syntax

```
avndmp {
{--backup | --operation=backup} [backup options]
| {--browse | --operation=browse}
| {--restore | --operation=restore} [restore options]
}
[account options] [common options] [logging options]
```

#### Operation descriptors

Supply only one operation on each avndmp command line.

--backup
--operation=backup

Performs an on-demand backup of a NAS system.

--browse
--operation=browse

Shows content for a backup.

--restore
--operation=restore

Restores data to a NAS system, or to an Avamar Linux or Windows client.

#### Account options

Account options for the avndmp command enable you to specify credentials to connect to the Avamar server for backups and restores.

--acceladdr=*accelerator-name*

Specifies the accelerator IP address or fully qualified hostname.

--account=*path*
--acnt=*path*
--path=*path*

Specifies an account location (*path*) on the Avamar server.

--fileraddr=*nas-name*

Specifies the NAS system IP address or fully qualified hostname.

--filerbrowseuser=*user*
--filerbrowsepswd=*password*

Specifies the Isilon directory browse username and password.

--filertype={md5 | text}

Specifies whether NAS system uses plain text (text) or encrypted (md5) passwords to authenticate the --fileruser account.

--fileruser=*user*

`--filerpswd=`*password*

Specifies the NAS system user account and password that runs NDMP jobs.

`--hfsaddr=`*avamar-server-name*
`--server=`*avamar-server-name*

Specifies the Avamar server IP address or fully qualified hostname (as defined in DNS).

`--id=`*user*`@`*auth*
`--password=`*password*
`--ap=`*password*
`--pswd=`*password*

Specifies a login user account and password on the Avamar server, where:

- *user* is the username.
- *auth* is the authentication system used to authenticate that user. The default internal authentication system is `avamar`.
- *password* is the password

**Common options**

Common options can be supplied with any operation.

`--[avtar]ddr-encrypt-strength={high | medium | none}`

Specifies the encryption method for data transfer between the client and the Data Domain system when you store the backup on a Data Domain system. The default value is `high`.

---

**Note**

The exact encryption technology and bit strength used for any given client/server connection depends on a number of factors, including the client platform and Avamar server version. The *EMC Avamar Product Security Guide* provides additional information.

---

`--appname=`*name*

Specifies which application to run. The default application is `avndmp`.

`--backup-type={differential | differential_full | incremental | incremental_full | level0_full | metadata | synthetic_full}`

Specifies a backup type.

`--check_filer_version`
`--check-filer-version`

Verifies that the NAS system is a supported version.

`--check_ndmp_enabled`
`--check-ndmp-enabled`

Verifies that NDMP services are enabled on the NAS system.

`--check_password`
`--check-password`

Verifies that the NAS system username and password are valid.

`--env=`*string*

Specifies custom variables to be sent to the NAS system.

`--filerbrand={EMC | NetApp}`

Specifies the brand of NAS system.

- `EMC`—For Celerra, VNX, VNXe, or Isilon storage systems.
- `NetApp`—For NetApp filers.
- `zfs`—For Oracle ZFS storage appliances.

`--flagfile=`*path*

Specifies the *path* to an options (flag) file.

`--help`

Shows all help output for the `avndmp` command, and then exits.

Supplying an operation descriptor shows help for that specific operation, and then exits.

`--home=`*path*

Specifies the home directory *path*.

`--pluginport=`*port*

Specifies the `avagent` data port connections. The default data port setting is `28002`.

`--run-at-end=`*script*
`--run_at_end=`*script*

Runs this *script* after each target is backed up or restored. The *script* must reside in the accelerator `/usr/local/avamar/etc/scripts` directory.

`--run-at-end-clauses=`*clauses*
`--run_at_end_clauses=`*clauses*

Uses these *clauses* to start the run-at-end script. The default setting is `desc=run-at-end`.

`--run-at-start=`*script*
`--run_at_start=`*script*

Runs this *script* before each target is backed up or restored. The *script* must reside in the accelerator `/usr/local/avamar/etc/scripts` directory.

`--run-at-start-clauses=`*clauses*
`--run_at_start_clauses=`*clauses*

Uses these *clauses* to start the run-at-start script. The default setting is `desc=run-at-start`.

`--version`

Shows version, then exits.

**Logging options**

Logging options enable you to specify the path and file name for the `avndmp` log file, and to control how much information the plug-in writes to the log file.

`--informationals`

Adds informational status messages to logging output. This is enabled by default.

`--logfile=`*file*
`--log=`*file*

Specifies the full path and file name of the log file.

`--logtimeformat={default|iso}`
`--logfmt={default|iso}`

Specifies the date and time format for log file time stamps.

`--logtimezone={default | local | gmt/utc}`
`--logzone={default | local | gmt/utc}`

Specifies the time zone for log file time stamps.

`--noinformationals`

Turns off all status messages.

`--nostdout`

Turns off output to standard output (stdout).

`--nowarnings`

Turns off warning messages.

`--prefix=`*string*

Specifies a *string* to be prefixed to the log files.

`--quiet`

Suppresses informational and warning messages.

`--verbose` [=*n*]
`--v` [=*n*]

Enables all status and warning messages.

Specifies an optional verbosity level by adding =*n*, where *n* is a positive single-digit integer between `1` an `6`. The default verbosity level setting is `6`.

**Backup options**

`--allowsubvolumeincremental`

Allows sub-volume backups.

This option is only available for Celerra, VNX or VNXe systems. It is not supported on Isilon systems.

`-backup-stream-buffering-period=`*min*

Enables backup stream buffering and specifies the numberof minutes (*min*) between buffering iterations.

`--base-sequencenumber=`*num*
`--base-labelnum=`*num*

Explicitly sets which backup to use as the incremental base. The default setting is `-1`.

`--enable-isilon-fast-incrementals`

Enables Isilon fast incremental backups.

`--enable-multivolume`

Enables support for multiple volumes in a single backup.

`--exclude-list=`*path*

Specifies one or more directories or files to exclude from EMC Isilon backups.

This option is only available for Isilon systems. It is not supported on Celerra, VNX or VNXe systems.

The following rules apply:

- Multiple `--exclude-list` options can be supplied on each command line.
- Isilon uses anchored matching to exactly match the name with the full path.
- A space character in a file or directory name must be preceded with a backslash(\).

- The total length of the relative *path* to the top level directory cannot exceed 1024 characters for a single backup target.
- Multiple `--exclude-list` options are allowed on the same command line.

`--expires={`*n* | `days=`*n* | `weeks=`*n* | `months=`*n* | `years=`*n* | *timestamp*`}`

Specifies backup expiration as one or more of the following:

- A specific number of days (*n* or `days=`*n*)
- A specific number of weeks (`weeks=`*n*)
- A specific number of months (`months=`*n*)
- A specific number of years (`years=`*n*)
- An absolute *timestamp*

`--full`

Performs a full backup.

The `--full` and `--incremental` options are mutually exclusive.

`--incremental`

Performs an incremental backup.

The `--full` and `--incremental` options are mutually exclusive.

`--limit-incremental-search=`*num*

Specifies the maximum number (*num*) of past backups to search for a valid incremental base. Specify `0` for unlimited searching. The default setting is `30` past backups.

`--mode={full | incremental | try_incremental}`

Specifies backup processing mode.

`--noavtar=`*stream*

Specifies a NAS system data stream name (*stream*) to be stored in a file.

`--nosnapsure`

Prevents SnapSure checkpoints during a backup.

This option is only available for Celerra, VNX or VNXe systems. It is not supported on Isilon systems.

`--retention-type={none | daily | weekly | monthly | yearly}`
`--retentiontype={none | daily | weekly | monthly | yearly}`

Specifies an extended retention type for the backup.

`--savedump=`*stream*

Saves the dump *stream* to a file using a tee.

`--test-comment-file-omits=`*string*

Omits creation of listed comment files in either the target or the snapview `.system_infos` file.

**Restore options**

`-restore-destination={none | original | single | multiple}`
`--restore-option=`

Specifies the type of restore to perform.

`--restoretarget=`*name*
`--target=`*name*

Specifies where to restore data, if different from original location.

# Specifying command line options

Use one of the following methods to specify options for the `avndmp` command:

- Type the individual options on the command line.
- List the options in the `avndmp.cmd` file, located in the accelerator `\usr\local\avamar\var` directory. List each option on its own line. For example:

```
--id=user@auth-system
-password=password
--logfile=file
--verbose
```

- Create a plain text option file, listing each option on its own line, and then specify the option file path on the command line using the `--flagfile=`*path* option.

# Script processing

The `avndmp` CLI enables user-defined scripts to be run before or after each backup or restore operation.

### Script location

Scripts must reside in the accelerator `/usr/local/avamar/etc/scripts` directory.

### Targets

Each backup or restore operation can comprise multiple targets. Each target is processed separately by Avamar, and any user-defined scripts are successively run against each target before the next target is processed.

### Pre- and post-processing control

The `--run-at-start=`*script* and `--run-at-start-clauses` options control pre-processing. That is, *script* is run against each target before Avamar attempts to back up or restore it.

The `--run-at-end=`*script* and `--run-at-end-clauses` options control post-processing. That is, *script* is run against each target after Avamar has successfully backed up or restored it.

### Script parameter syntax

There are two distinct syntaxes for passing parameters into scripts using the `--run-at-start` and `--run-at-end` options.

- If `stringlist-args` or list clauses are false or not supplied, then parameters (*p1*, *p2*) are passed into *script* separated by white space. For example:

```
--run-at-end="script p1 p2"
```

- If `stringlist-args` or list clauses are true, then parameters (*p1*, *p2*) are passed into *script* separated by commas. For example:

```
--run-at-start="script,p1,p2"
```

  Mixing syntaxes (for example, separating parameters with white space when the `stringlist-args` clause is true) will prevent the script from running.

### Script clauses

The `--run-at-start-clauses` and `--run-at-end-clauses` options accept any of the following clauses. The following table lists and describes each clause. The Default

(not supplied) column lists the default behavior (that is, behavior that occurs if the clause is not supplied). The No value columns lists the behavior used if the clause is supplied without a value (for example, exit-on-error).

**Table 5** Script clauses for the --run-at-start-clauses and --run-at-end-clauses options

| Clause | Default (not supplied) | No value | Description |
|---|---|---|---|
| `desc=`*text* | `run-at-end` for `--run-at-end-clauses`<br>`run-at-start` for `--run-at-start-clauses` | | Adds this user-defined descriptive *text* in log messages. |
| `env="`*key*`=`*value*`"` | | | Specifies environment variable to be set before running the script. |
| `exit-on-error[={true \| false}]` | `false` | `true` | Causes the program to exit when the script returns an error or times out.<br>If exit-on-error and skip-on-error are both specified, then exit-on-error takes precedence. |
| `skip-on-error[={true \| false}]` | `false` | `true` | Causes the program to skip the current operation if the script returns an error or times out.<br>This is only used with `--run-at-start-clauses` to specify that the backup or restore operation should continue even if an error is encountered when processing a single target.<br>If used with `--run-at-end-clauses`, it is ignored because the operation has already completed on the target.<br>If `exit-on-error` and `skip-on-error` are both specified, then `exit-on-error` takes precedence. |
| `stringlist-args[={true \| false}]`, `list[={true \| false}]` | `false` | `true` | Specifies the syntax used to pass parameters into a script with the `--run-at-start` or `--run-at-end` options.<br>If false or not supplied, then parameters are specified using white space as a separator.<br>If true, then parameters are specified as a comma-separated list.<br>Mixing syntaxes (for example, separating parameters with white space when the `stringlist-args` clause is true) will prevent the script from running. |
| `timeout-seconds[=`*integer*`]` | `1` hour | `1` hour | Specifies the maximum wait time for the script to complete. |
| `create-stdout-pipe[={true \| false}]` | `true` | `true` | If `true`, sends stdout to log file. If `false`, stdout output from the script is lost. |
| `create-stderr-pipe[={true \| false}]` | `true` | `true` | If `true`, sends stderr from script to log file. If `false`, stderr output from the script is lost. |

# APPENDIX C

# Troubleshooting

This appendix includes the following topics:

# Log files

During backup and restore operations, the `avagent` process creates log files for troubleshooting problems.

By default, `avagent` log files are located in the accelerator `/usr/local/avamar/var/client` directory.

The `avagent` log file name and location can be customized for each backup or restore operation:

where *file* is the full path and file name of the log file.

- Supply a `--logfile=`*file* option on the command line interface
- In **Backup Options or Restore Options** dialog boxes, type **`logfile`** in the **Enter Attribute**, and *file* in the **Enter Attribute Value** fields.
- In **New Dataset** or **Edit Dataset** dialog boxes, type **`logfile`** in the **Enter Attribute**, and *file* in the **Enter Attribute Value** fields.

# Restore problems and solutions

The following topics describe common restore problems and solutions.

**Redirected restore of multiple volumes does not work**
Redirected restore of multiple volumes fails and results in the following error:

```
avndmp Error <11803>: [avndmp_assist] Unable to redirect multiple
volumes. Please restore them separately
```

To work around this issue, restore each volume separately.

# GLOSSARY

## A

**accelerator** The Avamar NDMP Accelerator (accelerator) is a specialized Avamar server node that, when used as part of an Avamar system, enables backup and restore of network addressed storage (NAS) systems by way of the network data management protocol (NDMP).

**activation** The process of passing the client ID (CID) back to the client, where it is stored in an encrypted file on the client file system.

**See also** client activation

**Avamar Administrator** A graphical management console software application that is used to remotely administer an Avamar system from a supported Windows or Linux client computer.

**Avamar server** The server component of the Avamar client/server system. Avamar server is a fault-tolerant, high-availability system that efficiently stores the backups from all protected clients. It also provides essential processes and services required for data restores, client access, and remote system administration. Avamar server runs as a distributed application across multiple networked storage nodes.

## B

**backup** A point-in-time copy of client data that can be restored as individual files, selected data, or as an entire backup.

## C

**client activation** The process of passing the client ID (CID) back to the client, where it is stored in an encrypted file on the client file system.

**See also** activation

**client registration** The process of establishing an identity with the Avamar server. When Avamar recognizes the client, it assigns a unique client ID (CID), which it passes back to the client during *client activation*.

**See also** registration

## D

**Data Domain system** Disk-based deduplication appliances and gateways that provide data protection and disaster recovery (DR) in the enterprise environment.

**dataset** A policy that defines a set of files, directories, and file systems for each supported platform that are included or excluded in backups across a group of clients. A dataset is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

## G

**group** A level of organization in Avamar Administrator for one or more Avamar clients. All clients in an Avamar group use the same group policies, which include the *dataset*, *schedule*, and *retention policy*.

**group policy** The *dataset*, *schedule*, and *retention policy* for all clients in an Avamar group.

## M

**MCS** Management console server. The server subsystem that provides centralized administration (scheduling, monitoring, and management) for the Avamar server. The MCS also runs the server-side processes used by *Avamar Administrator*.

## N

**NAS** Network attached storage. A device connected to a computer network that provides centralized file storage for other computers on the network. NAS systems always provide storage in the form of a traversable file system.

**NDMP** Network data management protocol. An open protocol that is used to move data from a NAS system to a backup server.

## P

**plug-in** Avamar client software that recognizes a particular kind of data resident on that client.

**plug-in options** Options that you specify during backup or restore to control backup or restore functionality.

## R

**registration** The process of establishing an identity with the Avamar server. When Avamar recognizes the client, it assigns a unique client ID (CID), which it passes back to the client during *client activation*.

**See also** client registration

**restore** An operation that retrieves one or more file systems, directories, files, or data objects from a backup and writes the data to a designated location.

**retention** The time setting to automatically delete backups on an Avamar server. Retention can be set to permanent for backups that should not be deleted from an Avamar server. Retention is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

## S

**schedule** The ability to control the frequency and the start and end time each day for backups of clients in a group. A schedule is a persistent and reusable Avamar policy that can be named and attached to multiple groups.