Dell EMC Avamar NDMP Accelerator for NAS Systems

User Guide

19.2

Dell Inc.

October 2020
Rev. 06

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© 2001 - 2020 Dell Inc. or its subsidiaries. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Contents

Figures **6**

Tables **7**

Preface **8**

Chapter 1: Introduction **11**
Architecture 11
How Avamar works with NAS systems 11
Protecting multiple NAS systems with one accelerator 11
Multiple data streams 12
Data Domain system support 12
Isilon SmartConnect support 13
Avamar Installation Manager 13
Backup 13
Backup methods 13
Filer dump modes 13
Restore 14
Restore types 14
Restore destinations 14
Restored metadata 14
Year 2038 14

Chapter 2: Installation and Configuration **15**
Preparing the system 15
Checking the system requirements 15
Verifying network connectivity 15
Prerequisites for Dell EMC NAS systems 16
Create the NDMP user account on the NAS system 16
Create a browse user account on the Isilon system 17
Modifying NDMP snapTimeout parameters 18
Turning off deduplicated backups 18
Prerequisites for NetApp filers 18
Enabling filer NDMP services from the command line 18
Verifying filer privileges 19
Prerequisites for Oracle ZFS storage appliances 19
Configuring NDMP service settings 19
Installing and configuring the accelerator software 20
Download and install the Avamar Installation Manager software 20
Download the accelerator software installation workflow package 21
Install the accelerator software 21
Changing accelerator settings 22
Configuring the NDMP accelerator node 22
Registering the NDMP accelerator node 23
Enabling or disabling multiple simultaneous backups 24

Combining accounts (optional) 24
Upgrading the accelerator software 25
Upgrade the accelerator software 25
Running a newer NDMP accelerator node with an older Avamar server 26
Uninstalling the accelerator software 26
Configuring NTP time services 26
Configuring the NDMP accelerator node for dual NIC operation (optional) 27
Mounting a NAS share 28

Chapter 3: Backup 30
Limitations 30
Common limitations 30
Limitations specific to Dell EMC NAS systems 30
Limitations specific to NetApp filers 31
Limitations specific to Oracle ZFS storage appliances 31
Avamar Administrator limitations 32
Common Avamar Administrator limitations 32
Avamar Administrator limitations for Dell EMC NAS systems 32
Avamar Administrator limitations for NetApp filers 32
Avamar Administrator limitations for Oracle ZFS storage appliances 32
Performing on-demand backups 33
Scheduling backups 34
Creating a dataset 35
Creating a backup policy 36
Enabling a scheduled backup for a backup policy 36
Monitoring backups 36
Cancel backups 37
Enforcement of backups to Data Domain 37
Best practices for ZFS backups 37

Chapter 4: Restore 38
Limitations 38
Common limitations 38
Limitations specific to NetApp filers 38
Limitations specific to Oracle ZFS storage appliances 39
Creating an Oracle ZFS filesystem for non-UTF-8 restores 39
Restoring to the original NAS system 39
Restore to a Linux or Windows client with Avamar Administrator 41
Monitor restores 42
Cancel restores 43

Appendix A: Plug-in Options 44
How to set plug-in options 44
Backup options 44
Restore options 45

Appendix B: Command Line Interface 46
avndmp 46
Specifying command line options 51

Script processing 51

Appendix C: Command Line Installation and Upgrade 54
Download the accelerator software installation files 54
Installation and configuration with the command line 55
Install the Avamar Client for Linux software 55
Install the Avamar accelerator software (CLI) 55
Software upgrade with the command line 55
Upgrade the accelerator software (CLI) 56

Appendix D: Troubleshooting 57
Log files 57
Restore problems and solutions 57
Redirected restore of multiple volumes does not work 57
Issues with directed recoveries of VNX systems with space-reduced backup enabled to non-NAS file systems 57

Appendix E: Virtual NDMP Accelerator Nodes 58
Virtual NDMP accelerator node overview 58
Required information 58
Required files 58
Virtual hardware resource requirements 59
Deploy a SLES VM 59
Kickstart the SLES VM 60
Kickstart as a Gen4S vNDMP accelerator node 60
Kickstart as a Gen4T vNDMP accelerator node 63
Configure the SLES VM network settings 65
Install the NDMP accelerator software 70

Glossary 71

Figures

1 Accelerator deployment diagram....11
2 Networking diagram....15
3 Data loss warning....61
4 Platform selection menu....61
5 Gen4S node type selection menu....62
6 Data loss warning....63
7 Platform selection menu....64
8 Gen4T node type selection menu....64
9 YaST Control Center....66
10 YaST network settings - Overview....67
11 YaST network card setup....68
12 YaST network settings - Hostname/DNS....69
13 YaST network settings - Routing....70

Tables

1 Revision history 8
2 Typographical conventions 9
3 Multiple simultaneous data streams requirements (Dell EMC) 12
4 Multiple simultaneous data streams requirements (NetApp) 12
5 Backup plug-in options 44
6 Restore plug-in options 45
7 Script clauses for the --run-at-start-clauses and --run-at-end-clauses options 52
8 Files applicable for all vNDMP installations 58
9 Files applicable for Avamar Installation Manager 59
10 Files applicable for command-line installation 59

Preface

As part of an effort to improve the product lines, revisions of the software and hardware are periodically released. Therefore, some functions that are 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 the technical support professional when a product does not function correctly or does not function as described in this document.

NOTE: This document was accurate at publication time. To find the latest version of this document, go to Online Support (https://www.dell.com/support).

Purpose

This guide describes how to use the Avamar NDMP accelerator node to back up and restore supported Dell EMC PowerStore, Isilon, Unity, VNX, VNXe, and Celerra systems; Oracle ZFS storage appliances; and NetApp filers.

This publication supersedes the following documents:

- *Dell EMC Avamar NDMP Accelerator for Dell EMC NAS Systems User Guide*
- *Dell EMC Avamar NDMP Accelerator for NetApp Filers User Guide*
- *Dell EMC Avamar NDMP Accelerator for Oracle ZFS User Guide*

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 that are currently deployed at the site
- UNIX shell commands

Revision history

Table 1. Revision history

Revision	Date	Description
06	October, 2020	Updated the following sections: ● Create a browse user account on the Isilon system ● Restoring to a Linux or Windows client with Avamar Administrator
05	August, 2020	Updated the Turning off deduplicated backups section.
04	June, 2020	Updated the Isilon SmartConnect support section.
03	May, 2020	Minor copyediting corrections.
02	May, 2020	Added support for PowerStore.
01	November 15, 2019	GA release of Avamar 19.2

Related documentation

The following publications provide additional information:

- *E-LAB Navigator* at https://elabnavigator.emc.com/eln/elnhome
- *Avamar Release Notes*
- *Avamar Administration Guide*
- *Avamar Data Store Single Node Customer Installation Guide*
- *Avamar Operational Best Practices Guide*
- *Avamar Product Security Guide*

Typographical conventions

These type style conventions are used in this document.

Table 2. Typographical conventions

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 that are 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 that is omitted from the example

Where to get help

The Avamar support page provides access to licensing information, product documentation, advisories, and downloads, as well as how-to and troubleshooting information. This information may resolve a product issue before contacting Customer Support.

To access the Avamar support page:

1. Go to https://www.dell.com/support.
2. Type a product name in the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** search box.
3. Select the product from the list that appears. When you select a product, the **Product Support** page loads automatically.
4. (Optional) Add the product to the **My Products** list by clicking **Add to My Saved Products** in the upper right corner of the **Product Support** page.

Documentation

The Avamar product documentation provides a comprehensive set of feature overview, operational task, and technical reference information. To supplement the information in product administration and user guides, review the following documents:

- Release notes provide an overview of new features and known limitations for a release.
- Technical notes provide technical details about specific product features, including step-by-step tasks, where necessary.
- White papers provide an in-depth technical perspective of a product or products as applied to critical business issues or requirements.

Knowledgebase

The Knowledgebase contains applicable solutions that you can search for either by solution number (for example, KB000xxxxxx) or by keyword.

To search the Knowledgebase:

1. Go to https://www.dell.com/support.
2. Under the **Support** tab, click **Knowledge Base**.
3. Type either the solution number or keywords in the search box. Optionally, you can limit the search to specific products by typing a product name in the search box and then selecting the product from the list that appears.

Online communities

Go to Community Network at https://www.dell.com/community for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners, and certified professionals for all products.

Live chat

To engage Customer Support by using live interactive chat, click **Join Live Chat** on the **Service Center** panel of the Avamar support page.

Service Requests

For in-depth help from Customer Support, submit a service request by clicking **Create Service Requests** on the **Service Center** panel of the Avamar support page.

NOTE: To open a service request, you must have a valid support agreement. Contact a sales representative for details about obtaining a valid support agreement or with questions about an account.

To review an open service request, click the **Service Center** link on the **Service Center** panel, and then click **View and manage service requests**.

Enhancing support

It is recommended to enable ConnectEMC and Email Home on all Avamar systems:

- ConnectEMC automatically generates service requests for high priority events.
- Email Home sends configuration, capacity, and general system information to Customer Support.

Comments and suggestions

Comments and suggestions help to continue to improve the accuracy, organization, and overall quality of the user publications. Send comments and suggestions about this document to DPAD.Doc.Feedback@emc.com.

Please include the following information:

- Product name and version
- Document name, part number, and revision (for example, 01)
- Page numbers
- Other details to help address documentation issues

1

Introduction

Topics:

- Architecture
- Backup
- Restore

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.

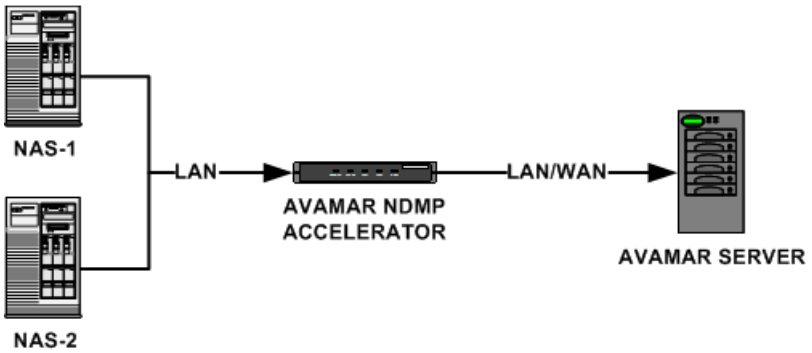

Figure 1. Accelerator deployment diagram

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 to control the maximum number of simultaneous NDMP data streams that can be allocated to each NAS system backup or restore operation.

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

Avamar automatically enables multi-streaming when you specify either root ("/") or an empty string as the backup target. In this case, Avamar performs an NDMP `volume browse` command before each backup operation and automatically includes any returned volumes. Avamar thus detects and backs up new volumes to eliminate the need to manually update the backup datasets when you instance new volumes on the NAS.

Dell EMC NAS systems

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

Table 3. Multiple simultaneous data streams requirements (Dell EMC)

NAS system	RAM	Maximum number of streams
Unity, VNX OE 7.1.34.0, 7.0	> 8 GB	8
VNX OE 7.0, VNXe 2.3.0, or Celerra DART 6.0	8 GB	4

NOTE: The maximum number of streams with PowerStore is 4.

NetApp filers

The number of simultaneous data streams that are available is dependent on the amount of system memory that is installed in the NetApp filer. The following table lists the maximum number of simultaneous data streams for different system memory capacities.

Table 4. Multiple simultaneous data streams requirements (NetApp)

System memory	Maximum number of streams
Less than 16 GB	4
16–24 GB	8

Data Domain system support

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

Before you can store backups on a Data Domain system, add the Data Domain system to the Avamar configuration by using Avamar Administrator. Then 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.

Avamar also supports Data Domain Cloud Tier. DD Cloud Tier moves data from Data Domain to the cloud. From the Avamar Administrator, you can configure cloud tiering to move Avamar backups from Data Domain to the cloud, and perform seamless recovery of these backups.

The *Avamar and 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.

Isilon SmartConnect support

Avamar now supports connecting to Isilon cluster with Isilon SmartConnect configuration.

Follow the *OneFS Web Administration Guide* to enable SmartConnect feature. Use the SmartConnect name that appears on Avamar as the hostname of the Isilon cluster to perform NDMP backup or restore operations.

Avamar Installation Manager

Avamar 7.4.*x* and later versions install the Avamar Installation Manager on the NDMP accelerator node. The Avamar Installation Manager manages the installation of and performs upgrades to the accelerator software. You can also use the command line to install and upgrade the accelerator software.

Backup

This topic provides a conceptual overview of NDMP backups.

NOTE: The Avamar AUI is only supported in stand-alone Windows and Linux environments only.

The following plug-ins provide the ability to exclude data from the backup dataset. You can exclude data when creating or editing a policy, or when creating or editing a dataset in the **Settings** pane. Data inclusion is not supported. The *Avamar Administration Guide* provides more information.

- ZFS via NDMP
- EMC Isilon via NDMP
- NetApp filer via NDMP

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 Avamar performs a full or incremental backup.

The first time that you back up each NAS system, 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	Avamar decides whether to perform a full (level 0) or incremental (level 1) backup each time that you perform a backup. Most backups are incremental. However, this mode allows Avamar to detect certain conditions that require a full backup to ensure data compatibility.
Force a level 0 dump	Avamar reprocesses the entire NAS system. However, Avamar data deduplication optimizes the backup on the accelerator so that only new data is sent to the server. Although this process requires additional processing time, the actual data that is sent to the Avamar server is the same as for an incremental (level 1) backup.
Force an incremental (level 1) dump	Avamar performs an incremental (level 1) backup, even if certain conditions exist that require a full (level 0) backup.

Full backups take longer than incremental backups because the NAS system sends all of its data to the NDMP accelerator node. However, 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.

NOTE: The Avamar AUI is only supported in stand-alone Windows and Linux environments only.

Restore types

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

Restore destinations

Avamar can restore data to the original NAS system, or to any Linux or Windows client that is registered with the Avamar server.

If you restore NDMP data to an Avamar Linux or Windows client, you can easily access and share it by establishing an NFS mount on Linux systems, or a CIFS mount on Windows systems.

NOTE: Applications that rely on file metadata such as alternate streams may not be able to correctly open files that are restored from a NAS backup to an NFS or CIFS mount. Restore such files back to the NAS device, either to the original location or to an alternate location.

Restored metadata

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

When restoring to a Linux or Windows file system, Avamar does not restore metadata such as ACLs, alternate data streams, and attributes associated with hard links or file compression.

Year 2038

The Avamar subsystem supports backup retention until February 2106. However, for older releases, the Avamar subsystem does not start after January 2038 due to the signed 32-bit integer time format of UNIX and Linux operating systems, and therefore cannot restore backup data after this date.

Newer Avamar releases offer support for longer retention periods:

- For Avamar 19.1 and later, the Avamar server subsystem uses an unsigned 32-bit integer and continues to start until 2106.
- For Avamar 19.1 and earlier, the Avamar client and plug-ins subsystem uses a signed 32-bit integer and retains data until 2038.
- For Avamar 19.2 and later, the Avamar client and plug-ins subsystem uses an unsigned 32-bit integer and retains data until 2106.
- Backup retention after 2038 is successful when all Avamar subsystems use unsigned 32-bit integers.

Therefore, with both Avamar 19.2 and later, and an Avamar 19.2 or later client, backup retention succeeds after 2038.

Avamar 19.2 and later clients also support restoring backups where the retention time is after 2038, and where the local (server and client) time is after 2038. Earlier client releases do not support this.

For backups of Windows or Linux clients, do not assign a retention period for a date after February 7, 2106.

2

Installation and Configuration

Topics:

- Preparing the system
- Prerequisites for Dell EMC NAS systems
- Prerequisites for NetApp filers
- Prerequisites for Oracle ZFS storage appliances
- Installing and configuring the accelerator software
- Changing accelerator settings
- Upgrading the accelerator software
- Uninstalling the accelerator software
- Configuring NTP time services
- Configuring the NDMP accelerator node for dual NIC operation (optional)
- Mounting a NAS share

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.

About this task

Updated, detailed NAS system compatibility information is available in the *E-LAB Navigator* at https://elabnavigator.emc.com/eln/modernHomeDataProtection.

Verifying network connectivity

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

Steps

1. Connect the Avamar server, NDMP accelerator node, and NAS systems to the network as shown in the following figure:

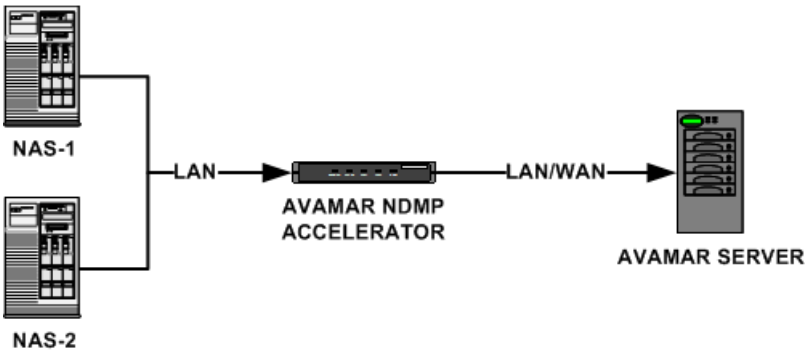

Figure 2. Networking diagram

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

2. Add each hostname to corporate DNS, or modify the `/etc/hosts` files on each network host, such that:
   - The Avamar server and NDMP accelerator node can resolve each other's hostnames.
   - The NDMP accelerator node 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. Power on the Avamar server, NDMP accelerator node, and NAS systems.
4. Open a command shell and log in to the Avamar server as admin.
5. Type **`ping accelerator`**, where *accelerator* is the NDMP accelerator node hostname, as defined in corporate DNS. The NDMP accelerator node responds to the `ping` command.
6. Open a command shell and log in to the NDMP accelerator node as admin.
7. 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.
8. 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 to which you have connected to this NDMP accelerator node.

   All NAS systems respond to the `ping` command.

   NOTE: If ICMP Ping is not permitted in the network, you can skip step 4 to step 8.

Prerequisites for Dell EMC NAS systems

Perform the following tasks for all Dell EMC NAS systems before installing and configuring the NDMP accelerator software.

Create the NDMP user account on the NAS system

Create an NDMP user account on the NAS system. This user account enables access to the NAS system for backups and restores.

About this task

Steps

1. Perform one of the following tasks:
   - If configuring an Isilon system, log in to OneFS Storage Administrator.
   - If configuring a Unity, 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, 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.

     The following example displays the command to add the "ndmp" user account to the "server_2" Data Mover, with the md5sum:

     ```
     server_user server_2 -add -md5 ndmp
     ```

   - For Unity systems, configure the "ndmp" password by Unisphere .
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.

Create a browse user account on the Isilon system

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

About this task

In order to perform manual 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

Though there are several methods to create local Isilon user accounts, you can assign privileges to roles by using only the command line interface.

To perform Isilon backups by using the NDMP accelerator node, ensure that Avamar is connected to Isilon by using the system access zone. This connection enables Avamar to browse data at the `/isi` level in the file system. The tasks include:

- View the access zones.
- Use pool0 to obtain access to the system access zone.

The *OneFS CLI Administration Guide* provides information about how to create a local Isilon user account, manage roles and privileges, and access zones.

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 exist in Isilon.

Steps

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 that is assigned to the av-browse-admin user account. This is the password that you must 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.

About this task

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

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

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

Turning off deduplicated backups

To maximize the benefits of Avamar deduplicated backup, it is recommended that you configure the VNX, VNXe, and Celerra systems to "unpack" the deduplicated files before sending them to the NDMP accelerator node for backup. This configuration is also required if you want to perform cross-platform recoveries. Note that this configuration is not applicable for Isilon systems.

About this task

For Unity systems, this procedure is unnecessary because Avamar automatically disables the deduplicated backup feature for backups.

Steps

1. To turn off deduplicated backups for a specific file system on VNX, VNXe, or Celerra systems, type the following command from the Control Station command-line interface:

   ```
   fs_dedupe -modify <file system> -backup_data_threshold 0
   ```

2. Turning off deduplicated backups on a specific Data Mover on VNX, VNXe, or Celerra systems automatically turns off deduplicated backups on file systems that are created on the Data Mover after the command is run, but does not impact any existing file systems on the Data Mover. To turn off deduplicated backups on a specific Data Mover on VNX, VNXe, or Celerra systems:

   ```
   fs_dedupe -modify <file system> -backup_data_threshold 0
   ```

Prerequisites for NetApp filers

Perform the following tasks for all NetApp filers before installing and configuring the NDMP accelerator software.

Enabling filer NDMP services from the command line

To back up the NetApp filer to the Avamar server, you must enable NDMP services on the filer.

About this task

Steps

1. To enable NDMP services on a single filer:
   a. Open a command shell and log in to the filer.
   b. Type **`ndmpd.enable on`**.
2. To enable NDMP services on a NetApp Cluster:
   a. Open a command shell and log in to the NetApp Cluster.
   b. Type **`services ndmp on -vserver vservername`**.

      where *vservername* is the hostname or IP address of the NetApp virtual storage system.

Verifying filer privileges

This task verifies that the filer NDMP user account has sufficient privileges to access all data on the filer and run NDMP jobs, and also determines the password encoding scheme.

About this task

During accelerator configuration, you must supply filer login credentials with sufficient privileges to access all data on the filer and run NDMP jobs. This user account is often referred to as the "NDMP user account," although it does not need to be named "NDMP."

Avamar supports node-scoped, Vserver-aware, and cluster-aware NDMP modes. In node-scoped NDMP mode, the root user account always has sufficient privileges. However, for security reasons you might want to use another user account. Backups might fail to start or complete if the alternate user account has insufficient privileges.

In Vserver-aware and cluster-aware NDMP modes, user authentication is integrated with the role-based access control mechanism. New user accounts must have sufficient privileges to access the Vserver. In Vserver-aware NDMP mode, the NDMP user must belong to either the vsadmin or vsadmin_backup role. In cluster-aware NDMP mode, the NDMP user must belong to either the admin or backup role.

You also must determine the password encoding scheme in use by the filer so that you can specify the correct encoding setting during accelerator configuration. Valid password encoding schemes are plain text or MD5.

Steps

1. Verify that the user account you intend to use for accelerator backups has full administrator privileges, or has cli-ndmpd* and cli-ndmpcopy* CLI rights and capabilities.
2. Determine which password encoding scheme is currently in use on the NDMP filer:
   a. Open a command shell and log in to the filer.
   b. Type **`options ndmpd.authtype`**.
   This command returns either `plaintext` or `challenge`. If `plaintext` is returned, then **`text`** is the correct accelerator setting. If `challenge` is returned, then **`md5`** is the correct accelerator setting.

Prerequisites for Oracle ZFS storage appliances

Perform the following tasks for all Oracle ZFS storage appliances before installing and configuring the NDMP accelerator software.

Configuring NDMP service settings

Configure NDMP service settings on the Oracle ZFS storage appliance.

Steps

1. Open a web browser and type the following URL:
   `https://`*`oracle-zfs`*`:215`
   where *oracle-zfs* is the Oracle ZFS storage appliance network hostname or IP address.
   The login web page appears.
2. Type the superuser (root) **Username** and **Password**, and then click **LOGIN**.
   The dashboard web page appears.
3. On the dashboard web page, click **Configuration** > **Services**.
   A list of services appears.
4. In the **Data Services** list, click **NDMP**.
   The **NDMP** service configuration page appears.
5. Configure the following settings:
   a. Clear the **Ignore metadata-only changes** checkbox.
   b. Add one or more **Target restore pools**.
   c. Set the **Allow token-based backup** checkbox.
   d. In the **ZFS rollback before restore** list, select **On DMA request**.

e. Leave the **Allow direct access recovery** checkbox set.

   NOTE: Avamar does not support direct access recovery. Either setting is permissible.

f. Clear the **Restore absolute paths** checkbox.
g. Set the **DMA tape mode** to **BSD**.
h. Type **ndmp** in the **DMA username (MD5 auth)** field.
i. Type a password for the **ndmp** user account in the **DMA password (MD5 auth)** field.
j. Click **Apply**.

6. To ensure that the NDMP service is enabled, verify that the **NDMP** service indicator is green.

Installing and configuring the accelerator software

This section provides procedures to install the Avamar Installation Manager and the Avamar NDMP accelerator software. The accelerator software installation workflow package allows you to configure the NDMP accelerator.

The *Avamar Release Notes* provide important information about installing Avamar 19.2 and later.

The legacy command line installation method is deprecated in favor of the Avamar Installation Manager and has moved to Command Line Installation and Upgrade on page 54.

NOTE: The names of some required files may still contain "SLES11." These files apply equally to SLES12 installations.

NOTE:

Avamar 18.1 and later releases include additional operating system and firewall hardening packages for NDMP accelerator nodes. Installing or upgrading the accelerator software through the Avamar Installation Manager automatically installs the hardening packages. Avamar does not support manual installation of the hardening packages. Therefore, manually installing or upgrading the accelerator software renders the hardening packages unavailable.

The level-2 security hardening topics in the *Avamar Product Security Guide* provide more information.

Download and install the Avamar Installation Manager software

This procedure installs the Avamar Installation Manager software on the NDMP accelerator node so that you can then install the accelerator software installation workflow package.

Steps

1. Download the Avamar Installation Manager install package:
   a. In a web browser, go to https://support.emc.com/.
   b. In the search field, search for the installed Avamar release.
   c. In the left pane of the search results, click **DOWNLOADS**.
   d. Click **Avamar**.
   e. Locate and download the Avamar *version* SLES Bundle installation package, where *version* is the version number of the Avamar software.

      Download the install package to `/usr/local/avamar/src/` on the NDMP accelerator node.
2. Open a command shell and log in to the NDMP accelerator node as admin.
3. Switch user to root by typing **su -**, and then press **Enter**.
4. Install the Avamar Installation Manager:
   a. Change directory by typing:

      cd /usr/local/avamar/src
   b. Extract the bundle by typing:

      unzip AvamarBundle_SLES11_64-*version*.zip

      where *version* is the version number of the Avamar software.
   c. Install the Avamar Installation Manager by typing:

```
sh ./AvamarBundle_SLES11_64/avinstaller-bootstrap-version.sles11_64.x86_64.run
```

where *version* is the version number of the Avamar software.

Download the accelerator software installation workflow package

Download the accelerator software installation workflow package from Support Zone. You can then upload the workflow package to the Avamar server's local repository for use with the Avamar Installation Manager.

Steps

1. In a web browser, go to https://support.emc.com/.
2. In the search field, search for the installed Avamar release.
3. In the left pane of the search results, click **DOWNLOADS**.
4. Click **Avamar**.
5. Locate and download the accelerator software installation workflow package (`AcceleratorInstallSles-version.avp`), where *version* is the version number of the Avamar software.

   Download the workflow package to a temporary location, such as `/tmp`.

Install the accelerator software

This procedure describes how to use the Avamar Installation Manager on the NDMP accelerator node to install the accelerator software.

Steps

1. Open a web browser and log in to Avamar Installation Manager:
   a. Type the following URL:

      https://*accelerator-node*:7543/avi

      where *accelerator-node* is the IP address or resolvable hostname of the Avamar NDMP accelerator node.

      The Avamar Installation Manager login page appears.
2. Type **root** in the **User Name** field and **changeme** in the **Password** field.

   NOTE: The *Avamar Product Security Guide* contains instructions for changing the default password.

3. Upload the accelerator software installation workflow package to the local repository:
   a. Click **Repository**.

      The **Repository** pane appears.
   b. Click **Browse** to browse to the location where you downloaded the accelerator software installation workflow package in Download the accelerator software installation workflow package on page 21, and then select the package.
      Once the upload completes, the workflow package automatically appears in the **Repository** table.
4. Click **SW Releases**.
   The **Software Releases** pane opens.
5. Click **Install**.
   The **Installation Setup** pane appears.
6. Complete the information on the **Installation Setup** pane and click the **NAS Settings** tab.

   The **Require NAS system configuration** option is selected by default. If you do not want to configure NAS systems at this point, unselect the option and click **Continue**.
7. If the **Require NAS system configuration** option is selected, you must add at least one NAS system:
   a. Click **Add NAS system**.
   b. Select the NAS system type.
   c. Type the resolvable Hostname or IP address of the NAS system.
   d. Type the NDMP account name and password.
   e. Select the encoding schema to be used for the password.
   f. For the **Avamar account** field, type the Avamar client name that you created for this system.

The client name must be lowercase.

g. The **Accelerator hostname/IP** field defaults to the local host's hostname or IP address, but can be changed if necessary.

h. Click **Continue**.

NOTE: To delete a NAS system configuration before clicking **Continue**, click the red X to the left of the configuration that you want to delete.

Avamar Installation Manager installs the accelerator software.

Changing accelerator settings

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

About this task

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.

Configuring the NDMP accelerator node

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

Prerequisites

Install the Avamar Client for Linux and the NDMP accelerator software on the NDMP accelerator node.

Steps

1. Open a command shell and log in to the NDMP accelerator node as admin.
2. Switch user to root by typing **`su -`**, and then press **Enter**.
3. Run the accelerator configuration utility by typing one of the following commands:

NAS type	Command
Dell EMC NAS systems	**`avsetupndmp`**
NetApp filers	**`avsetupndmp`**
Oracle ZFS storage appliances	**`avsetupndmp --zfs`**

4. Press **Enter** to accept the default action to stop all running agents.
5. Type the NDMP accelerator node 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 step calls for 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:

NAS type	Action
Dell EMC PowerStore, Unity, VNXe, VNX, or Celerra system	Type **1**, and then press **Enter**.
Dell EMC Isilon system	Type **2**, and then press **Enter**.
NetApp filer	Type **3**, 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**.

    NOTE:

    For NetApp filers, if you are setting up a NetApp Cluster, ensure that the user account has sufficient privileges to access the Vserver.

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 name is how that NAS system client instance appears 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 NDMP accelerator node DNS name or IP address, and then press **Enter**.

    This value is a 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`**, press **Enter**, and then follow the onscreen instructions.
    - To exit this NDMP accelerator configuration utility session, press **Enter**.

Registering the NDMP accelerator node

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

Prerequisites

Install the Avamar Client for Linux and the accelerator software on the NDMP accelerator node, and configure the NDMP accelerator node.

Steps

1. Open a command shell and log in to the NDMP accelerator node 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 NDMP accelerator node.

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.

Enabling or disabling multiple simultaneous backups

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

Steps

1. Open a command shell and log in to the NDMP accelerator node as admin.
2. Switch user to root by typing **su -**, and then pressing **Enter**.
3. Run the accelerator configuration utility by typing one of the following commands:

NAS type	Command
Dell EMC NAS systems	**avsetupndmp**
NetApp filers	**avsetupndmp**
Oracle ZFS storage appliances	**avsetupndmp --zfs**

4. Press **Enter** to accept the default action to stop all running agents.
5. Type the NDMP accelerator node 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 step calls for 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 NDMP 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 overload occurs, combine the multiple accounts into a single account so that the accelerator can allow the maximum number of concurrent backups that are supported by that accelerator configuration without overloading.

About this task

NOTE: You can only combine accounts within the same Avamar domain.

Steps

1. Open a command shell and log in to the NDMP accelerator node as admin.
2. Switch user to root by typing **su -**, and then press **Enter**.
3. Run the accelerator configuration utility by typing one of the following commands:

NAS type	Command
Dell EMC NAS systems	**avsetupndmp**
NetApp filers	**avsetupndmp**
Oracle ZFS storage appliances	**avsetupndmp --zfs**

4. Press **Enter** to accept the default action to stop all running agents.
5. Type the NDMP accelerator node 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 step calls for 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 onscreen instructions.
    - To exit this NDMP accelerator configuration utility session, press **Enter**.

Upgrading the accelerator software

The upgrade to Avamar 19.2 imposes additional prerequisites, including a restriction on the supported operating systems and existing software versions.

The accelerator software upgrade workflow contains an upgrade to the SLES 12 operating system. The *Avamar Release Notes* provide more information about upgrading the accelerator software.

To upgrade a prior release of the accelerator software to Avamar 19.1 as part of an upgrade to Avamar 19.2, the *Avamar NDMP Accelerator for NAS Systems User Guide* for Avamar 19.1 provides more information.

The upgrade process also assumes that the accelerator software was installed through the Avamar Installation Manager, and that the Avamar Installation Manager is installed on the NDMP accelerator node.

The legacy command-line method is deprecated in favor of the Avamar Installation Manager and has moved to Command Line Installation and Upgrade on page 54.

Upgrade the accelerator software

The following procedure uses the Avamar Installation Manager to upgrade the accelerator software.

Steps

1. Select one of the methods in the *Avamar Administration Guide* to obtain the accelerator upgrade workflow package.
2. Open a web browser and log in to Avamar Installation Manager:
   a. Type the following URL:

      `https://accelerator-node:7543/avi`

      where *accelerator-node* is the IP address or resolvable hostname of the Avamar NDMP accelerator node.

      The Avamar Installation Manager login page appears.
3. Type **`root`** in the **User Name** field and **`changeme`** in the **Password** field.

   NOTE: The *Avamar Product Security Guide* contains instructions for changing the default password.

4. If using the Avamar Downloader Service, check for new packages on the downloader service host, and then download the accelerator upgrade workflow package through the Avamar Installation Manager.

   NOTE: The *Avamar Administration Guide* contains information about configuring and using the Avamar Downloader Service.

5. If manually uploading the accelerator upgrade workflow package, complete the instructions in the *Avamar Administration Guide* to upload the workflow package to the local repository.
6. Click **Install**.
   The **Installation Setup** page appears.

Running a newer NDMP accelerator node with an older Avamar server

If you upgrade the accelerator software to a newer version, but do not also upgrade the Avamar server software to the same version, you must upgrade the client plugin catalog on the Avamar server, then download and install the `dpnavclient` file on the Avamar server. Downloading the `dpnavclient` package requires that you open a Service Request with Customer Support.

Steps

1. Follow instructions for downloading and installing new packages from the repository in the *Avamar Administration Guide* to download and install the upgrade-client-plugin-catalog to the server.
2. Download and install the `dpnavclient` installation package:

   NOTE: To complete this step, please open a Service Request with Customer Support.

   a. Download the `dpnavclient` installation package from Customer Support to a temporary folder on the Avamar server, such as `/tmp`.
   b. Open a command shell and log in to the server as admin.
   c. Switch user to root by typing **`su -`**, and then pressing **Enter**.
   d. Change directory to the temporary folder where you downloaded the installation package and upgrade the software by typing:

   `rmp -Uvh dpnavclient-`*`version`*`.sles11_64.x86_64.rpm`
3. Upgrade the NDMP accelerator node as described in this chapter.

Uninstalling the accelerator software

Steps

1. Open a command shell and log in to the NDMP accelerator node 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 accelerator software by typing:

   `rpm -e AvamarNDMP-`*`version`*

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

   `rpm -e AvamarClient-`*`version`*

   where *version* is the Avamar client software version.

Configuring NTP time services

To avoid any unexpected behaviors, you should keep the time on all nodes in the system consistent. This procedure configures NTP time services for accelerators running the SUSE Linux Enterprise Server (SLES) operating system.

Prerequisites

Before running this procedure, determine if the NTP time services are configured and functioning on the Avamar utility node. If not, do not use this procedure. Instead, manually set the NDMP accelerator node time to be consistent to Avamar server utility node by typing `yast`, selecting **System**, then **Date and Time** as described in step 8 on page 27.

About this task

NOTE: Do not perform this task on any accelerator running the Red Hat Enterprise Linux (RHEL) operating system.

Steps

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**. Type the password if prompted.
3. Copy the `/etc/ntp.conf` file from the Avamar server utility node by typing:

   ```
   cp -p /etc/ntp.conf{,.orig}
   scp root@utility-node:/etc/ntp.conf /etc/
   ```

   where *utility-node* is the DNS name or IP address of the Avamar utility node.
4. Restart the `ntpd` service by typing:

   ```
   service ntp restart
   ```
5. Verify that the `ntpd` service started correctly by typing:

   ```
   service ntp status
   ```

   Wait 7–10 minutes for the system to fully settle.
6. Verify that the `ntpd` service is synchronizing time by typing:

   ```
   /usr/sbin/ntpq -pn
   ```

   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.

   If any reach values are zero, please verify that the list of time servers is correct in `/etc/ntp.conf`.
7. Ensure that the `ntpd` service starts at system startup by typing:

   ```
   chkconfig ntp on
   ```
8. If you have not already done so, set the local time zone on the accelerator:
   a. Type `yast`, select **System**, and then **Date and Time**.
   b. Select the correct local time zone.

      For best results, set the local time zone to that of the NAS system so that both the NAS system and NDMP accelerator node log files correlate.
   c. Verify that the output of the date command is accurate by typing `date`.

Configuring the NDMP accelerator node for dual NIC operation (optional)

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

Prerequisites

Install the Avamar Client for Linux and the accelerator software on the NDMP accelerator node. Configure the NDMP accelerator node and register the node with the Avamar server.

About this task

To maximize data throughput, segregate the NAS system network traffic from the Avamar server network traffic. Configure 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.

Steps

1. Obtain and record the following information:
   - IP address for the secondary NIC
   - Subnet mask for the NDMP accelerator node
   - Hostname for the secondary NIC
   - Gateway IP address of the subnet where the NDMP accelerator node resides

- IP address of the NAS system

2. Open a command shell and log in to the NDMP accelerator node 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 NDMP accelerator node.
   - 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 NDMP accelerator node 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 that you 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 is 255.255.255.255 when a single NAS system backs up to an NDMP accelerator node. However, when multiple NAS systems back up to the same NDMP accelerator node, 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**.

Mounting a NAS share

Avamar 18.1 and later releases include additional operating system and firewall hardening packages for NDMP accelerator nodes. To mount a NAS share on an NDMP accelerator node, add the NAS IP address to the firewall table. Remove the NAS from the firewall table when you no longer need to mount the NAS share.

Steps

1. Open a command shell:
   a. Log in to the NDMP accelerator node as admin.
   b. Switch user to root by typing **`su -`**.
2. Add the NAS to the firewall table by typing the following commands:

   ```
   iptables -I OUTPUT -p tcp -d IPv4-addr -j ACCEPT
   iptables -I OUTPUT -p udp -d IPv4-addr -j ACCEPT
   ```

   where *IPv4-addr* is a specific IPv4 address for the NAS.

3. Remove the NAS from the firewall table by typing the following commands:

```
iptables -D OUTPUT -p tcp -d IPv4-addr -j ACCEPT
iptables -D OUTPUT -p udp -d IPv4-addr -j ACCEPT
```

where *IPv4-addr* is a specific IPv4 address for the NAS.

3

Backup

Topics:

- Limitations
- Avamar Administrator limitations
- Performing on-demand backups
- Scheduling backups
- Monitoring backups
- Cancel backups
- Enforcement of backups to Data Domain
- Best practices for ZFS backups

Limitations

The following sections detail the known limitations of Avamar NDMP backup.

Common limitations

The following limitations apply to the NDMP accelerator node with any NAS 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.
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.

Limitations specific to Dell EMC NAS systems

The following limitations apply to the NDMP accelerator node only with Dell EMC NAS systems:

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
Maximum path length	When backing up a NAS system, paths cannot be longer than 4,096 characters.
Maximum number of files	Each individual Avamar backup of a NAS system can contain a maximum of 10 million files.
Incremental backups should only be performed at the root volume level	When backing up PowerStore, Unity, 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 PowerStore, Unity, 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.

Limitations specific to NetApp filers

The following limitations apply to the NDMP accelerator node only with NetApp filers:

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

SnapVault snapshots If backing up a SnapVault snapshot, you must perform a full backup. Incremental backups fail and exit with an error.

qtree and folder paths To back up qtrees and folders, you must type the path to that entity within the volume.

Backup performance for large NetApp volumes Performance of NDMP NetApp backups of volumes with more than approximately 10 million files may degrade over time. This is typically seen in backups that exceed 24 hours. Both initial backups and incremental backups are impacted.

Exclusions These are the known limitations of backup exclusions for NetApp filers:

- Exclusion entry syntax—A valid NetApp exclusion entry is a backup target concatenated with a name to be excluded. The backup target can be a volume or directory name. NetApp then excludes the specified name all places within the specified backup target.
- Hardlinks prevent file exclusion—Any file that contains a hardlink cannot be excluded from an Avamar backup. This is a NetApp limitation.

Limitations specific to Oracle ZFS storage appliances

The following limitations apply to the NDMP accelerator node only with Oracle ZFS storage appliances:

Socket files Avamar does not support socket file to backup Oracle ZFS file system. This is because the ZFS NAS system does not send the socket file in the data stream to Avamar during backup.

Maximum path length When backing up any Oracle ZFS storage appliance, paths cannot be longer than 1023 characters. This limitation also applies to NFS mounts included in the backup.

Avamar Administrator limitations

The following sections detail 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.

Common Avamar Administrator limitations

The following limitations apply to backups of any type of NAS system:

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.

Avamar Administrator limitations for Dell EMC NAS systems

The following limitation applies to backups of Dell EMC NAS systems:

Browsing folders and files	When browsing a PowerStore, Unity, 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. When browsing Isilon system, you can browse into volumes to view individual folders or files. PowerStore, Unity, VNX, VNXe, Celerra and Isilon file systems do not support file level backup, but these file systems support file level restore.

Avamar Administrator limitations for NetApp filers

The following limitations apply to backups of NetApp filers:

Browsing folders and files	When browsing a NetApp 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.
UTF-8 folder and file names	In order to view UTF-8 folder and file names, UTF-8 must be enabled by the Data ONTAP filer volume language setting.
Empty folders	When backing up empty folders, Avamar reports a size of between one and a few kilobytes for each empty folder. The number of kilobytes reported depends on the number of empty files.

Avamar Administrator limitations for Oracle ZFS storage appliances

The following limitations apply to backups of Oracle ZFS storage appliances:

Browsing folders and files	When browsing an Oracle ZFS 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.
Empty folders	When backing up empty folders, Avamar reports a size of between one and a few kilobytes for each empty folder. The number of kilobytes reported depends on the number of empty files.

Performing on-demand backups

An on-demand backup is a user-initiated backup of NDMP data on a client. You can perform an on-demand backup for the first backup of the client immediately after you install the Avamar client software. Perform an on-demand backup before system maintenance, software installations, or software upgrades.

Steps

1. In the AUI navigation pane on the left, click ≫, and then click **Asset Management**.
   The **Asset Management** window is displayed.
2. In the domain tree, select the domain that contains the NDMP Accelerator node.

   A list of Avamar clients is displayed in the pane below the domains list.
3. In the list of clients, select the NAS system client instance.

   You can only view clients in the domain for the login account. To view all clients, log in to the root domain.
4. Click **BACKUP**.
   The Backup wizard is displayed. In the **Plugin** pane, a list of plug-ins that are installed on the Oracle server is displayed.
5. In the **Plugins** pane, perform the following steps:
   a. Select the *NDMP* plug-in for the platform:
      - For NetApp filers, select **Netapp Filer via NDMP**, and then browse to select one or more volumes.
      - For Oracle ZFS storage appliances, select **ZFS via NDMP**, and then browse to and select one or more volumes.
      - For Dell EMC PowerStore, Unity, VNX, VNXe, or Celerra NAS systems, select **Celerra/VNX/Unity via NDMP**, and then browse to and select one or more volumes.
      - For Dell EMC Isilon NAS systems, select **Isilon via NDMP**, and then browse to and select one or more top-level directories beneath the `/ifs` root directory.

   b. Click **NEXT**.

   The **Basic Configuration** window is displayed.
6. In the **Basic Configuration** pane, complete the following fields:
   a. Select the backup retention policy settings:
      - To automatically delete this backup from the Avamar server after a specific amount of time, select **Retention period**. 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**.

   b. 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 *Avamar Product Security Guide* provides additional information.
   c. From the **Optionally select a proxy to perform backup** list, select the proxy.

      The default setting is **Automatic**, which enables the Avamar server to choose the best proxy for this operation.

   d. Click **NEXT**.

      The **More Options** window is displayed.
7. In the **More Options** pane, set the plug-in options:

   These settings are all optional. In most cases, system default settings are the best settings for on-demand NDMP backups.
   a. Toggle the **Show Advanced Options** switch to on.
   b. In the **Maximum Concurrent Data Streams** field, select the maximum number of data streams that can be used concurrently during the backup.
   c. 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 option 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 option can cause backup errors.

   d. In the **Backup label** field, type a descriptive label for the backup.

e. For Dell EMC NAS systems and NetApp filers: 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.
f. For Dell EMC NAS systems and NetApp filers: 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.
g. 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 on the accelerator `/usr/local/avamar/etc/scripts` directory.
h. 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 on the accelerator `/usr/local/avamar/etc/scripts` directory.
i. To manually add other plug-in options as free text, perform the following steps:
   i. Toggle the **Show Free Form** switch to on.
   ii. Click
   +
   .
   This step adds a row to the list of plug-in options.
   iii. In the **Key** field, type the name of the configuration plug-in option.
   iv. In the **Value** field, type the value of the configuration plug-in option.

   To delete a plug-in option, select the option and then click **Delete** in the **Action** column.

   NOTE: The Avamar software does not check or validate the information that is typed in the **Show Free Form** section of the **More Options** pane. The values in the **Key** and **Value** fields override settings that are specified with the GUI controls for the options.

8. Click **FINISH**.
   The following status message is displayed:

   ```
   Backup initiated.
   ```

Scheduling backups

Scheduled backups run automatically to ensure that backups of NAS systems occur on an ongoing basis. You can schedule backups to run daily, weekly, or monthly. The scheduled backup can include multiple clients or a single server.

About this task

You can schedule backups by using the Policy wizard to create a policy for a backup.

Perform the following steps within the **Policy** wizard. The *Avamar Administration Guide* provides more information about policies, datasets, schedules, and retention settings.

Steps

1. Assign members to the new backup policy.
2. Assign a dataset to the new backup policy.
   To create a dataset, use the Policy wizard or select **Settings** > **Dataset** > **Add**.
3. Assign a schedule to the new backup policy.
   To create a schedule, use the Policy wizard or select **Settings** > **Schedule** > **Add**.
4. Assign a retention policy to the new backup policy.
   To create a retention policy, use the Policy wizard or select **Settings** > **Retention** > **Add**.
5. Enable scheduling for the backup policy.

Creating a dataset

A dataset specifies the data to include in a scheduled backup and the options to use for the backup. Create at least one dataset for scheduled backups on a client or group of clients. Create multiple datasets to segregate client data.

About this task

Steps

1. In the AUI navigation pane on the left, click ≫, and then click **Settings**.
   The **Setting** pane is displayed.
2. Click the **Dataset** tab.
3. Click **ADD**.
   The **Create Dataset** window is displayed.
4. In the **Dataset Name** field, type a name for the dataset.
   The name can include alphanumeric characters (A-Z, a-z, 0–9) and the following special characters: period (.), hyphen (-), and underscore (_), and space. Do not use Unicode characters or the following special characters: ` ~ ! @ # $ % ^ & * ( ) = + [ ] { } | \ / ; : ' " < > , ?
5. From the **Plugins** list, select a plug-in:
   - For Dell EMC PowerStore, Unity, VNX, VNXe, or Celerra NAS systems, select **Celerra/VNX/Unity via NDMP**.
   - For Dell EMC Isilon NAS systems, select **Isilon via NDMP**.
6. (Optional) Set plug-in options in the **Options** tab:
   These settings are all optional. In most cases, system default settings are the best settings for scheduled NDMP backups.
   a. Select the **Show Advanced Options** check box.
   b. From the **Maximum Concurrent Data Streams** list, select the maximum number of data streams that can be used concurrently during the backup.
   c. 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 option 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 option can cause backup errors.

   d. For Dell EMC NAS systems and NetApp filers: 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.
   e. For Dell EMC NAS systems and NetApp filers: 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.
   f. 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 on the accelerator `/usr/local/avamar/etc/scripts` directory.
   g. 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 on the accelerator `/usr/local/avamar/etc/scripts` directory.
7. Click the **Source Data** tab and then select the data to include in the dataset:
   - To include all server data on a client, select the following:
     - For Dell EMC PowerStore, Unity, VNX, VNXe, or Celerra NAS systems, select **Celerra/VNX/Unity via NDMP**.
     - For Dell EMC Isilon NAS systems, select **Isilon via NDMP**.
   - To specify instances or databases on a client, perform the following steps:
     a. Select **Select Files and/or Folders**.
     b. In the **File/Folder Path** field, type the file path.
     c. Click **ADD**.
8. Click **SUBMIT**.

Creating a backup policy

A backup policy is a collection of Avamar clients that use the same dataset, schedule, and retention settings to implement scheduled backups.

About this task

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

The *Avamar Administration Guide* provides information about creating and editing backup policies, schedules, or retention settings.

Enabling a scheduled backup for a backup policy

Scheduled backups occur only for enabled backup policies. Backup policies are disabled by default unless you select the **Enabled** check box on the first page of the **New Policy** wizard. If you did not enable the backup policy when you created it, use the menu options in the **Policy** window to enable backups.

Steps

1. In the AUI navigation pane on the left, click ≫, and then click **Backup Policy**.
   The **Policy** page is displayed.
2. In the domain tree, select a domain or subdomain for the backup policy.
   To select a subdomain for the backup policy, toggle the **Include Sub-domain** switch to on.
3. Select a backup policy from the list.
4. To enable a backup policy, click **MORE ACTIONS** > **Enable Policy**.
5. To disable a backup policy, click **MORE ACTIONS** > **Disable Policy**.

Monitoring backups

You can monitor and view status information for backup and restore operations by using the **Activity Monitor**.

About this task

To access the **Activity Monitor**, open the navigation pane, and then click **Activity**. The **Activity Monitor** appears with a list of all activities.

NOTE: The AUI **Activity Monitor** window has been optimized for at least 1366 pixels-wide screens. Display issues might occur for smaller screens. To properly display the AUI, ensure that your display is at least 1366 pixels wide.

The **Activity Monitor** provides you with options to filter the information that appears:

- Filter activities by duration—By default, the **Activity Monitor** displays the most recent 5,000 client activities. To select a different duration, in the **Filter activities by duration** drop-down list, select **Last 24 hours** or **Last 72 hours**.
- Filter activities by domain—By default, the **Activity Monitor** displays all activities regardless of domain. To display only the activities for a specific domain, in the **Filter activities by domain** drop-down list, select a domain or subdomain.
- Filter activities by status—By default, the **Activity Monitor** displays all activities regardless of status.

  To display only activities with a specific status, at the top of the **Activity Monitor**, select one of the following options:

  - Completed
  - Failed
  - Running
  - Waiting

To filter activities by client, start time, plug-in, or type, click ▼ in their respective column.

The **Activity Monitor** displays the date and time that an activity began, and the total number of bytes examined during an activity.

To view activity details, expand the **Details** pane, by clicking «.

Cancel backups

You can cancel a backup any time before it completes. The cancellation might take 5 minutes or longer. The backup might complete before the cancellation finishes.

Steps

1. In the AUI navigation pane on the left, click », and then click **Activity**.
   The **Activity Monitor** appears with a list of activities.
2. Select the backup from the list.
3. Click **CANCEL**.
   A confirmation dialog box is displayed.
4. Click **YES**.

Enforcement of backups to Data Domain

If the Avamar server is configured to enforce backups to a Data Domain system, the server rejects backups that are not destined for the Data Domain. This enforcement covers backups that you configure through the Avamar Administrator and the AUI, as well as from command-line interfaces and other tools.

These backups must have additional flags that indicate the storage target. The *Avamar and Data Domain System Integration Guide* provides more information about backup enforcement and the related client version requirements. Backup enforcement is disabled by default.

Best practices for ZFS backups

The following information provides best practices for ZFS backups.

- Do not include hard links across directories that were backed up separately.

  The backup of a file, which has hard links across multiple directories, includes multiple copies of the file. When you restore this backup, you restore multiple copies of the same file. The restore does not handle hard links across backups.

- Do not backup data paths that are greater than 1023 bytes or the backups will fail. This is a limitation of Oracle ZFS.
- Do not create alternate data stream files greater than 2 GB, this could cause the backup to fail.

4

Restore

Topics:

- Limitations
- Creating an Oracle ZFS filesystem for non-UTF-8 restores
- Restoring to the original NAS system
- Restore to a Linux or Windows client with Avamar Administrator
- Monitor restores
- Cancel restores

Limitations

The following sections detail the known limitations of Avamar NDMP restore.

Common limitations

The following limitations apply to the NDMP accelerator node with any NAS system:

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 behavior 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 when the user who initiates the restore is authenticated using an external authentication system such as LDAP or Windows Active Directory.

Limitations specific to NetApp filers

The following limitations apply to the NDMP accelerator node only with NetApp filers:

Extra "restore_symboltable" file	When restoring a NetApp filer backup, an extra file `restore_symboltable` is created on the restore target. The NetApp filer (not Avamar software) creates this file, which is a known NetApp limitation. Refer to NetApp Bug ID 30347 for more information. Note also that if the dataset used for backups already contains a `restore_symboltable` file, that file is renamed to `rstabRENAME47026EF7` on the restore target.
LUN restores	When restoring a LUN to original filer, the data does not get restored as a LUN. The interim solution is to manually specify a NetApp qtree root folder as a restore location for the LUN, which causes the NetApp filer to create the proper LUN container.
LUN restores	When selecting the top level checkbox of a backup for restore, this "top folder" is not restored. Only the mount point underneath it is restored. Therefore, when you perform a redirected restore of multiple mounts, files or directories may be overwritten if the path of a file or directory in one mount point is the same as the path or directory in another mount point. A best practice is to select **Restore everything to multiple locations** when performing a redirected restore of multiple mount points.

Limitations specific to Oracle ZFS storage appliances

The following limitation applies to the NDMP accelerator node only with Oracle ZFS storage appliances:

Restoring non-UTF8 characters	Default Oracle ZFS filesystems only support UTF-8 characters. Therefore, if you are restoring files that contain non-UTF-8 characters to the Oracle ZFS storage appliance, you must create a file system on the Oracle ZFS storage appliance that supports non-UTF-8 characters. Otherwise, the restore fails.

Creating an Oracle ZFS filesystem for non-UTF-8 restores

Default Oracle ZFS filesystems only support UTF-8 characters. Therefore, if you will be restoring files that contain non-UTF-8 characters to the Oracle ZFS storage appliance, you must create a new filesystem on the Oracle ZFS storage appliance that will support non-UTF-8 characters. Otherwise, the restore will fail.

About this task

NOTE: This task is only required if you are restoring files that contain non-UTF-8 characters to the Oracle ZFS storage appliance.

Steps

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

   `https://`*`oracle-zfs`*`:215`

   where *oracle-zfs* is the Oracle ZFS storage appliance network hostname or IP address.

   The login web page appears.
2. Type the superuser (root) **Username** and **Password**, and then click **LOGIN**.
   The dashboard web page appears.
3. On the dashboard web page, click **Shares**.
4. Click **+** next to **Filesystems**.
   The **Create filesystem** web page appears.
5. Clear the **Reject non UTF-8** checkbox.
6. Click **Apply**.

Restoring to the original NAS system

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

Steps

1. In the AUI navigation pane on the left, click ≫, and then click **Asset Management**.
   The **Asset Management** window is displayed.
2. In the domain tree, select the domain that contains the NDMP Accelerator node.

   A list of Avamar clients is displayed in the pane below the domains list.
3. In the list of clients, select the NAS system client instance.

   A list of NAS system clients that are registered with that NDMP Accelerator node is displayed.

   NOTE: You can only view clients in the domain for the login account. To view all clients, log in to the root domain.
4. To locate backups by date:
   a. In the right pane, click **VIEW MORE**.
   b. Click **SEARCH**.
   c. In the **Date** field, select a day or range of days.
   d. Click **RETRIEVE**.

The list of backups for the selected dates is displayed.

5. Click the **RESTORE** tab.

   The **Restore** wizard is displayed and the **Destination Client** pane is displayed on the right.

6. In the **Destination Client** pane, perform the following steps:
   a. Select **Restore to original client**.
   b. Click **NEXT**.

   The **Backup Content** pane is displayed.

7. In the **Backup Content** pane, perform the following steps:
   a. In the left pane, select the SQL instance from the tree.

      The **Backup Content** pane displays a list of databases within the backup.

   b. Select the databases that you want to restore.
   c. Click **NEXT**.

   The **Destination Location** pane is displayed.

8. In the **Destination Locaiton** pane, select the target destination:
   - To restore everything to its original location, perform the following steps:
     a. Select **Restore everything to it's original location**.
     b. Click **Next**.
   - To restore everything to a different location, perform the following steps:
     a. Select **Restore everything to a different location**.
     b. In the **Restore Location** field, type the file path of the target location where you want to restore the data.

        For example: E:/dbrestore_dir/

     c. Click **Next**.

   The **More Options** pane is displayed.

9. In the **More Options** pane, set the plug-in options:

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

   a. To view advanced options, select **Show Advanced Options**.
   b. From the **Maximum Concurrent Data Streams** list, select the maximum number of data streams that can be used concurrently during the restore.
   c. For Dell EMC NAS systems and NetApp filers: 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 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 on 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 on the accelerator `/usr/local/avamar/etc/scripts` directory.
   f. To manually add other plug-in options as free text, perform the following steps:
      i. Toggle the **Show Free Form** switch to on.
      ii. Click

          +

          .

          This step adds a row to the list of plug-in options.

      iii. In the **Key** field, type the name of the configuration plug-in option.
      iv. In the **Value** field, type the value of the configuration plug-in option.

      To delete a plug-in option, select the option and then click **Delete** in the **Action** column.

   NOTE: The Avamar software does not check or validate the information that is typed in the **Show Free Form** section of the **More Options** pane. The values in the **Key** and **Value** fields override settings that are specified with the GUI controls for the options.

10. Click **NEXT**.

    The **Summary** pane is displayed.

11. Review the provided information, and then click **FINISH**.

Restore to a Linux or Windows client with Avamar Administrator

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. The data can also be shared by establishing an NFS mount on Linux systems, or a CIFS mount on Windows systems.

About this task

NOTE: There are some limitations of cross-platform restore of NDMP backups. Few data or attributes of some files cannot be restored while restoring cross-platform restore of NDMP backups. Some of the examples are ACLs, alternate data streams, attributes associated with hard links or file compression.

Perform the following steps to restore to a Linux or Windows client.

Steps

1. In Avamar Administrator, click the **Backup & Restore** launcher link.
   The **Backup & Restore** window appears.
2. From the list of clients, select the NDMP accelerator node.
   A list of NAS system clients that are registered with that NDMP accelerator node 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 *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 Dell EMC Isilon NAS systems, complete the following substeps:

a. In the **Browse Command Line Options** dialog box, type 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. (Optional) Set plug-in options:

    These settings are all optional. In most cases, system default settings are the best 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 used concurrently during the restore.
    c. For Dell EMC NAS systems and NetApp filers: 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 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 on 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 on the accelerator `/usr/local/avamar/etc/scripts` directory.
    f. Click **OK.**
       The **Restore Command Line Options** dialog box closes.
22. Click **OK** to close the **Restore Options** dialog box.

Monitor restores

You can monitor and view status information for backup and restore operations in the **Activity Monitor**.

About this task

To access the **Activity Monitor**, open the navigation pane, and then click **Activity**. The **Activity Monitor** appears with a list of all activities.

NOTE: The AUI **Activity Monitor** window has been optimized for at least 1366 pixels-wide screens. Display issues might occur for smaller screens. To properly display the AUI, ensure that your display is at least 1366 pixels wide.

The **Activity Monitor** provides you with options to filter the information that appears:

- Filter activities by duration—By default, the **Activity Monitor** displays the most recent 5,000 client activities. To select a different duration, in the **Filter activities by duration** drop-down list, select **Last 24 hours** or **Last 72 hours**.
- Filter activities by domain—By default, the **Activity Monitor** displays all activities regardless of domain. To display only the activities for a specific domain, in the **Filter activities by domain** drop-down list, select a domain or subdomain.
- Filter activities by status—By default, the **Activity Monitor** displays all activities regardless of status.

  To display only activities with a specific status, at the top of the **Activity Monitor**, select one of the following options:

  - Completed
  - Failed
  - Running
  - Waiting

To filter activities by client, start time, plug-in, or type, click in their respective column.

The **Activity Monitor** displays the date and time that an activity began, and the total number of bytes examined during an activity.

To view activity details, expand the **Details** pane, by clicking .

Cancel restores

You can cancel a restore any time before it completes. The cancellation might take 5 minutes or longer. The restore might complete before the cancellation finishes.

Steps

1. In the AUI navigation pane on the left, click ≫, and then click **Activity**.
   The **Activity Monitor** appears with a list of activities.
2. Select the restore from the list.
3. Click **CANCEL**.
   A confirmation dialog box is displayed.
4. Click **YES**.

A

Plug-in Options

Topics:

- How to set plug-in options
- Backup options
- Restore options

How to set plug-in options

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

Specify plug-in options in the AUI for on-demand backup or restore wizards, or when a dataset for a scheduled backup is created. Set plug-in options with the graphical user interface (GUI) controls (text boxes, check boxes, radio buttons, and so forth). Type an option and its value in the **Key** and **Value** fields.

NOTE: The Avamar software does not check or validate the information that is typed in the **Show Free Form** section of the **More Options** pane. The values in the **Key** and **Value** fields override settings that are specified 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 5. 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: ● Prefer Incremental, but do a Full if required ● Force a level 0 dump ● Force an incremental (level 1) dump
Backup label	Custom descriptive label for the backup. This option is only available during on-demand backups.
Store backup on Data Domain system[a]	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.
	To enable this option, add a Data Domain system to the Avamar configuration. The *Avamar and Data Domain System Integration Guide* provides instructions.
Encryption method to Data Domain system[a]	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 NDMP accelerator node's `/usr/local/avamar/etc/scripts` directory.

Table 5. 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 NDMP accelerator node's `/usr/local/avamar/etc/scripts` directory.
Isilon Browse User Name[b]	User account on the Isilon server with sufficient privileges for browsing the Isilon file system.
Isilon Browse Password[b]	Password for the Isilon browse user account.

a. Dell EMC NAS systems and NetApp filers only.
b. Dell EMC NAS systems only.

Restore options

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

Table 6. 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[a]	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 NDMP accelerator node's `/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 NDMP accelerator node's `/usr/local/avamar/etc/scripts` directory.

a. Dell EMC NAS systems and NetApp filers only.

B

Command Line Interface

Topics:

- avndmp
- Specifying command line options
- Script processing

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 `/usr/local/avamar/bin` directory on the NDMP accelerator node.

To use the `avndmp` CLI:

1. Open a command shell.
2. Log in to the accelerator as admin.
3. Switch the user to root by typing the following command: **`su -`**
4. Type the `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`
: Displays the volumes for the connected NAS.

`--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. This option applies only to Dell EMC NAS systems.

--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 that is 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`. This option applies only to Dell EMC NAS systems and NetApp filers.

NOTE: The exact encryption technology and bit strength that is used for any given client/server connection depends on a number of factors, including the client platform and Avamar server version. The *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 | zfs}

Specifies the brand of NAS system.

- `EMC`—For Dell EMC Celerra, Unity, PowerStore, 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` and `6`. The default verbosity level setting is `6`.

Backup options

--allowsubvolumeincremental

Allows sub-volume backups.

This option is only available for Celerra, Unity, PowerStore, VNX, or VNXe systems. It is not supported on Isilon systems. This option applies only to Dell EMC NAS systems.

--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. This option applies only to Dell EMC NAS systems.

--enable-multivolume

Enables support for multiple volumes in a single backup.

--exclude-list=*path*

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

For Dell EMC NAS systems, the following rules apply:

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

For NetApp filers, the following rules apply:

- The exclude list can contain a maximum of 32 separate directory or file names.
- Separate multiple directory or file names with commas (`,`).
- Asterisks (`*`) in the first and/or last character of a directory or file name is interpreted as a wildcard character, which matches zero or more instances of any character. An asterisk in the middle of a name is interpreted as a single literal instance of asterisk.
- A comma in a directory or file name must be preceded with a backslash(`\`).
- Multiple `--exclude-list` options are allowed on the same command line.

For Oracle ZFS storage appliances, the following rules apply:

- *path* must be the target path that contains files or directories that match *pattern*.
- *pattern* can contain asterisk (`*`) or question mark (`?`) wildcards.
  - An asterisk (`*`) matches zero or more occurrences of any character.

    - A question mark (?) matches a single occurrence of any character.
  - Multiple `--exclude-list` options are allowed on the same command line.
  - You may also supply a list in the form **`--exclude-list=`*`path/pattern`***.

`--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 applies only to Dell EMC NAS systems.

This option is only available for Celerra, PowerStore, Unity, 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.

Limitations

The known limitations of `avndmp` CLI for backing up and restoring data are as follows:

- The Oracle ZFS file system does not support file level backup, but it supports file level restore.
- The NetApp file system does not support file level backup, but it supports file level restore.

- Isilon, Unity, PowerStore, VNX, VNXe, and Celerra file systems do not support file level backup, but these file systems support file level restore.

Specifying command line options

About this task

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\`*`client-account-name`* 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 7. 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` `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. 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. 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. If used with `--run-at-end-clauses`, it is ignored because the operation has already completed on the target. 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

Table 7. Script clauses for the --run-at-start-clauses and --run-at-end-clauses options (continued)

Clause	Default (not supplied)	No value	Description
			with the `--run-at-start or --run-at-end` options. If false or not supplied, then parameters are specified using white space as a separator. If true, then parameters are specified as a comma-separated list. 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.

C

Command Line Installation and Upgrade

This appendix provides optional procedures for installing, upgrading, and configuring the Avamar NDMP accelerator software through the command line interface. Where available, it is recommended that you use the installation and upgrade workflows.

Topics:

- Download the accelerator software installation files
- Installation and configuration with the command line
- Software upgrade with the command line

Download the accelerator software installation files

Connect to the Avamar server and download the accelerator software installation files. This task applies to both installation and upgrade procedures.

Prerequisites

Install the **UpgradeClientDownloads** workflow package on the Avamar server. This workflow makes the Avamar client software available for download. The *Avamar Administration Guide* provides more information about downloading and installing workflow packages.

About this task

NOTE:

Avamar 18.1 and later releases include additional operating system and firewall hardening packages for NDMP accelerator nodes. Installing or upgrading the accelerator software through the Avamar Installation Manager automatically installs the hardening packages. Avamar does not support manual installation of the hardening packages. Therefore, manually installing or upgrading the accelerator software renders the hardening packages unavailable.

The level-2 security hardening topics in the *Avamar Product Security Guide* provide more information.

Steps

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

   `https://Avamarserver/dtlt/home.html`

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

   The **Avamar Web Restore** web page appears.
2. Click **Downloads**.
3. Click **+** next to the **NDMP Accelerator** folder.
4. Click **+** next to the folder that corresponds to the correct type of accelerator software.
5. Download all of the available accelerator software installation files. Ensure that you download the following files:
   - `AvamarClient-linux-rhel4-x86_64-version`
   - `AvamarNDMP-linux-rhel4-x86_64-version`
6. Copy the files to a temporary folder on the NDMP accelerator node, such as `/tmp`.

Installation and configuration with the command line

This section provides optional procedures for installation and configuration of the Avamar NDMP accelerator software through the command-line utility. Where available, Dell EMC recommends that you use the installation workflow.

Download the accelerator software installation files and then complete all of the procedures in this section to install the accelerator software. Download the accelerator software installation files on page 54 provides more information.

After you install the accelerator software, perform the following actions:

- Configuring the NDMP accelerator node on page 22
- Registering the NDMP accelerator node on page 23

Install the Avamar Client for Linux software

Steps

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

Install the Avamar accelerator software (CLI)

Prerequisites

Install the Avamar Client for Linux software on the NDMP accelerator node.

Steps

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

Software upgrade with the command line

To upgrade the accelerator with the command line, you must upgrade both the Avamar Client for Linux and Avamar NDMP accelerator software packages to the same version.

NOTE: The legacy command line method does not upgrade the operating system, only the accelerator software. To upgrade the operating system, use the accelerator software upgrade workflow package.

Download the new accelerator software installation files and then complete the procedures in this section. Download the accelerator software installation files on page 54 provides more information.

If you upgrade the accelerator software to a newer version, but do not also upgrade the Avamar server software to the same version, additional steps are required after the upgrade. Running a newer NDMP accelerator node with an older Avamar server on page 26 provides more information.

Upgrade the accelerator software (CLI)

Upgrading the NDMP accelerator node using the Linux software upgrade command (`rpm -U`) command preserves the existing configuration settings. You do not have to rerun `avsetupndmp` or `avregister`. Ensure that you upgrade the software in the correct order.

Steps

1. Open a command shell and log in to the NDMP accelerator node 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-linux-rhel4-x86_64-`*`version`*`*`
4. Upgrade the accelerator software by typing:
   `rpm -U AvamarNDMP-linux-rhel4-x86_64-`*`version`*`*`

D

Troubleshooting

Topics:

- Log files
- Restore problems and solutions

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.

Issues with directed recoveries of VNX systems with space-reduced backup enabled to non-NAS file systems

Recovering files from an Avamar NDMP backup of a VNX deduplicated file system on which the Space-Reduced Backup parameter is enabled may result in some files not being readable when a directed recovery is performed to a non-NAS file system, such as a Microsoft Windows or UNIX/Linux file system. This issue applies when:

- The VNX Space-Reduced Backup threshold is set to a value other than **0**.

  NOTE: Setting the Space-Reduce Backup parameter to **0** disables the Space-Reduced backup feature.
- The VNX automatically compressed one or more of the source files.
- The restore includes a cross-platform recovery (for example, VNX to Windows or VNX to Linux).

The Avamar KB article https://emcservice--c.na55.visual.force.com/apex/KB_ETA?id=kA4j0000000PFpA contains further information.

E

Virtual NDMP Accelerator Nodes

Topics:

- Virtual NDMP accelerator node overview
- Deploy a SLES VM
- Kickstart the SLES VM
- Configure the SLES VM network settings
- Install the NDMP accelerator software

Virtual NDMP accelerator node overview

This appendix contains instructions for deploying virtual NDMP (vNDMP) accelerator nodes that mimic the Avamar Data Store Gen4S and Gen4T physical platforms, but leverage existing VMware ESXi environments.

These procedures contain information about deploying a SLES virtual machine (VM), kickstarting the VM as an Avamar NDMP accelerator node, configuring network settings, and installing the accelerator software.

Customers should be familiar with VMware environments, and basic procedures such as VM deployment and network configuration.

Review all prerequisites and obtain all necessary information and material before you begin, including the *Avamar Release Notes*. The SLES 12 kickstart is required for fresh installations of Avamar 19.2 software.

Required information

Obtain the following information before you start:

- The NDMP username and password for the NAS system.
- The Avamar domain where the NDMP groups reside.
- Network configuration values for the vNDMP accelerator node:
  - An IP address.
  - A hostname.
  - The netmask.
  - A default gateway.
  - The domain name.
  - One or more DNS servers.

Required files

Obtain the following files and their SHA-256 checksums before you begin.

The SHA-256 checksum files have the same names as the corresponding download, plus the additional extension `.sha256` or `.sha256sum`.

NOTE: The names of some required files may still contain "SLES11". These files apply equally to SLES12 installations.

The following file is common to all installation paths:

Table 8. Files applicable for all vNDMP installations

Description	Filename	Source
SLES kickstart ISO	`ADS-SLES12.4-`*`version`*`.iso`	Download links from SolVe Desktop

If you intend to install the accelerator software with the Avamar Installation Manager, obtain the following files:

Table 9. Files applicable for Avamar Installation Manager

Description	Filename	Source
Avamar bundle[a] for the selected platform	`AvamarBundle_SLES11_64-`*`version`*`.zip`	Support Zone (https://support.emc.com)
Avamar NDMP accelerator software workflow package	`AcceleratorInstallSles-`*`version`*`.avp`	Support Zone (https://support.emc.com)

a. The Avamar bundle contains the Avamar Installation Manager bootstrap file (`avinstaller-bootstrap-`*`version`*`.sles11_64.x86_64.run`).

If you intend to install the accelerator software with the legacy command-line method, obtain the following files:

Table 10. Files applicable for command-line installation

Description	Filename	Source
Avamar Linux client	`AvamarClient-linux-rhel4-x86_64-`*`version`*`.rpm`	Avamar server
Avamar accelerator software	`AvamarNDMP-linux-rhel4-x86_64-`*`version`*`.rpm`	Avamar server
Gen4T event monitoring software	`dpnepm-`*`version`*`.sles11_64.x86_64.rpm`	Avamar server

These three files do not have SHA-256 checksums when obtained directly from an Avamar server.

Virtual hardware resource requirements

Ensure that your virtual environment can meet the following resource requirements before you begin:

Gen4S vNDMP nodes require the following virtual hardware:

- 2 vCPUs
- 32 GB of virtual RAM
- 300 GB of disk space

Gen4T vNDMP nodes require the following virtual hardware:

- 2 vCPUs
- 48 GB of virtual RAM
- 1.8 TB of disk space

NOTE:

Allocating more disk space results in partition errors during the kickstart process.

Allocating less RAM impacts the deployment process and reduces the number of supported NDMP streams. Each NDMP stream requires 8 GB of RAM.

Deploy a SLES VM

Deploy an uninitialized Linux VM in VMware ESXi, in preparation for the Avamar kickstart as a vNDMP accelerator node. Other VMware clients may provide equivalent functionality, though the interface may differ. SLES is the only supported operating system.

Steps

1. Open the VMware client.
2. Launch the **New Virtual Machine** wizard.
   If prompted for the type of configuration, select **Custom (advanced)**.

The wizard opens to the **Select a creation type** pane.

3. Select **Create a new virtual machine**, and then click **Next**.
   The wizard moves to the **Select a name and folder** pane.
4. Type a name for the vNDMP accelerator node VM.
5. Select a location in the ESXi virtual data center for the wizard to create the SLES VM.
6. Click **Next**.
   The wizard moves to the **Select a compute resource** pane.
7. Select a host or resource to provide the virtual resources to the SLES VM, and then click **Next**.
   The wizard moves to the **Select storage** pane.
8. Select an appropriate datastore to hold the virtual disks for the SLES VM, and then click **Next**.

   Ensure that you select a datastore that meets the requirements in Virtual hardware resource requirements on page 59.

   The wizard moves to the **Select compatibility** pane.
9. From the **Compatible with** drop-down, select **ESXi 6.0 and later** (VMX11), and then click **Next**.

   NOTE: If you select **ESXi 6.5 and later**, the installation fails.

   The wizard moves to the **Select a guest OS** pane.
10. From the **Guest OS family** drop-down, select **Linux**.
11. From the **Guest OS version** drop-down, select **SUSE Linux Enterprise 12 (64-bit)**.
12. Click Next.
    The wizard moves to the **Virtual hardware** tab of the **Customize hardware** pane.
13. From the **CPU**, **Memory**, and **New hard disk** drop-downs, select values that meet the requirements in Virtual hardware resource requirements on page 59.
14. From the **New network** drop-down, select an appropriate virtual network, and then check **Connect**.
15. From the **New CD/DVD drive** drop-down, select **Datastore ISO file**, and then check **Connect**.
16. Select the kickstart ISO image that corresponds to the platform that you selected.
17. For Gen4T vNDMP accelerator nodes, add and configure the serial port:
    a. From the **New device** drop-down, select **Serial port**.
    b. Click **Add**.
    c. From the **Serial port 1** drop-down, select **Use output file**.
    d. Check **Connect at power on**.
    e. For the **Connection** field, click **Browse** to associate the serial port with the output file.
    f. For **I/O mode**, check **Yield CPU on poll**.
18. Click **Next**.
    The wizard moves to the **Ready to complete** pane.
19. Verify the settings and then click **Finish**.

Results

The wizard creates and deploys a new SLES VM from the kickstart image.

Kickstart the SLES VM

The kickstart process begins the initial configuration of the vNDMP node, including partition and network interface setup. The kickstart process then copies the SLES operating system to the VM.

The procedures for Gen4S and Gen4T differ slightly. Perform the procedure that applies to your choice of platform.

Kickstart as a Gen4S vNDMP accelerator node

This task creates the system partitions and installs the SLES operating system.

Steps

1. Using ESXi, locate and then power on the SLES VM.
2. Open the console for the SLES VM and observe the boot process.

Wait for the data loss warning to appear.

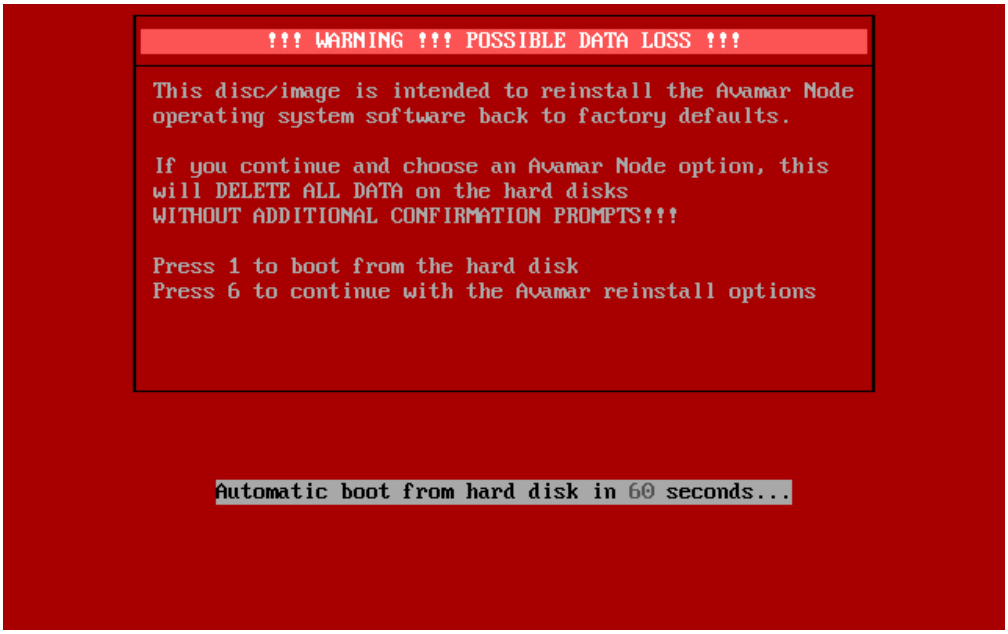

Figure 3. Data loss warning

3. Press **6** to acknowledge the data loss warning.

   The platform selection menu appears.

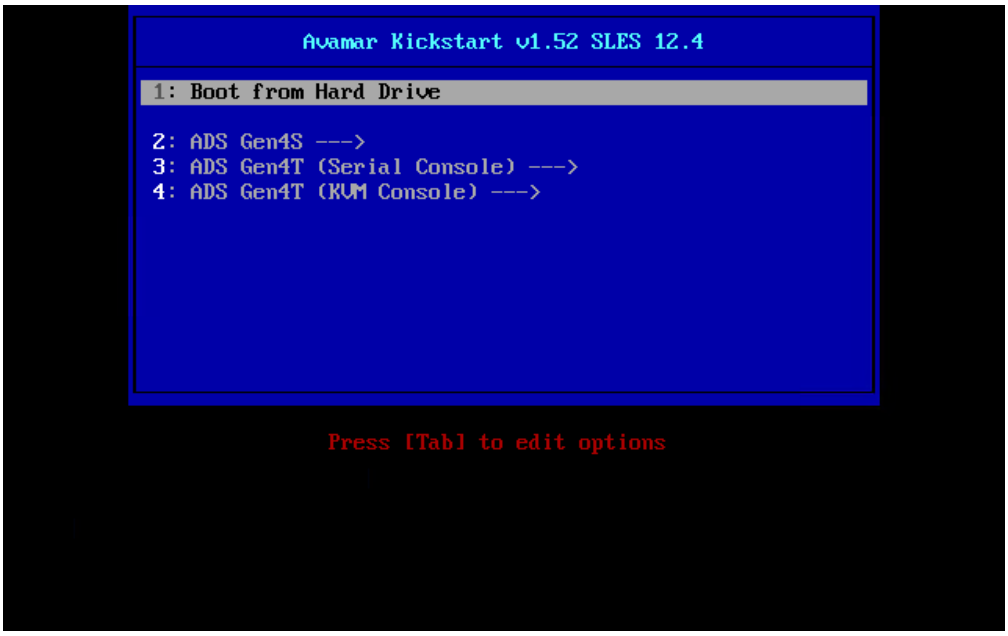

Figure 4. Platform selection menu

4. Select **ADS Gen4S**, and then press Enter.

   The node type selection menu appears.

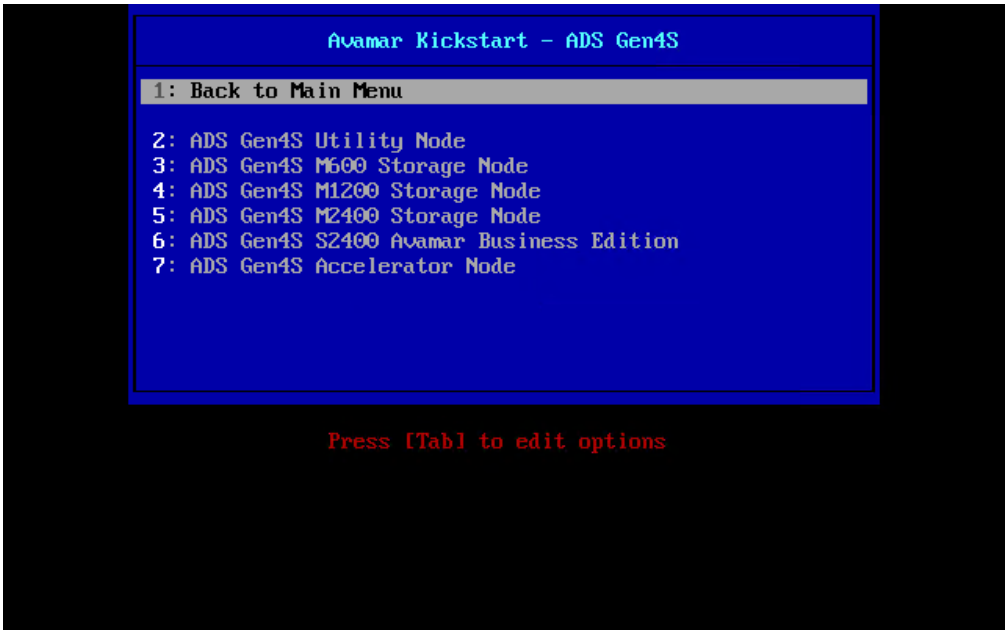

Figure 5. Gen4S node type selection menu

5. Use the down-arrow key to scroll through the boot options.
6. Select **ADS Gen4S Accelerator Node**, and then press Enter.
   The automated operating system installation procedure begins. The kickstart is not complete until the first login prompt becomes available.
7. Wait for the login prompt after the reboot.
8. Log in as the root user.

   NOTE: At this stage, you are not required to log in as the admin user and use `su`.

9. Determine the current kickstart version by typing the following command:

   `cat /PlatformInfo`

   Output similar to the following appears:

```
KS_OS_NAME="SUSE Linux Enterprise Server"
KS_OS_VERSION="12"
KS_OS_PATCHLEVEL="4"
KS_VERSION="1.61"
KS_PRODUCT="DellEMC Avamar Server"
KS_MODEL="accelerator"
KS_PLATFORM="ADS4S"
```

   Ensure that the kickstart version matches the version of the kickstart ISO image. If the platform information file does not exist or does not match the kickstart ISO image, the kickstart was unsuccessful.

10. Verify the existence of the kickstart post scripts by typing the following commands:

   `cd /var/log/YaST2`

   `grep -iE 'autoinstscript.*\.sh' * | grep -v "\.log"`

   The following output appears:

```
y2log:2019-09-11 21:09:55 <1> node(3121) [Ruby] modules/AutoinstScripts.rb:907 Writing
script into /var/adm/autoinstall/scripts/zzz-build_rpm_list.sh
```

   Verify that errors did not occur during the generation of the post scripts.

11. Verify that all of the post scripts exist as expected by typing the following command:

   `ls -a /var/adm/autoinstall/scripts/*.sh`

   The following output appears:

```
/var/adm/autoinstall/scripts/info_gen4s.sh
/var/adm/autoinstall/scripts/info_accelerator.sh
/var/adm/autoinstall/scripts/zzz-build_rpm_list.sh
```

where *nodetype* corresponds to your selection from the kickstart menu.

Verify that all of these scripts exist on the vNDMP accelerator node. If any of these scripts are missing, the kickstart was unsuccessful.

12. Check the contents of the Message of the Day file by typing the following command:

    `grep -i avamar /etc/motd`

    The following output appears:

    ```
    * This is an Avamar Super Node                                    *
    ```

    If the file does not include the output above, the kickstart was unsuccessful.

    NOTE: If any of the checks indicate a problem with the kickstart process, do not continue until you have resolved the issues. Contact Customer Support for assistance.

Results

The vNDMP accelerator node is ready for network configuration.

Kickstart as a Gen4T vNDMP accelerator node

This task creates the system partitions and installs the SLES operating system.

Steps

1. Using ESXi, locate and then power on the SLES VM.
2. Open the console for the SLES VM and observe the boot process.

   Wait for the data loss warning to appear.

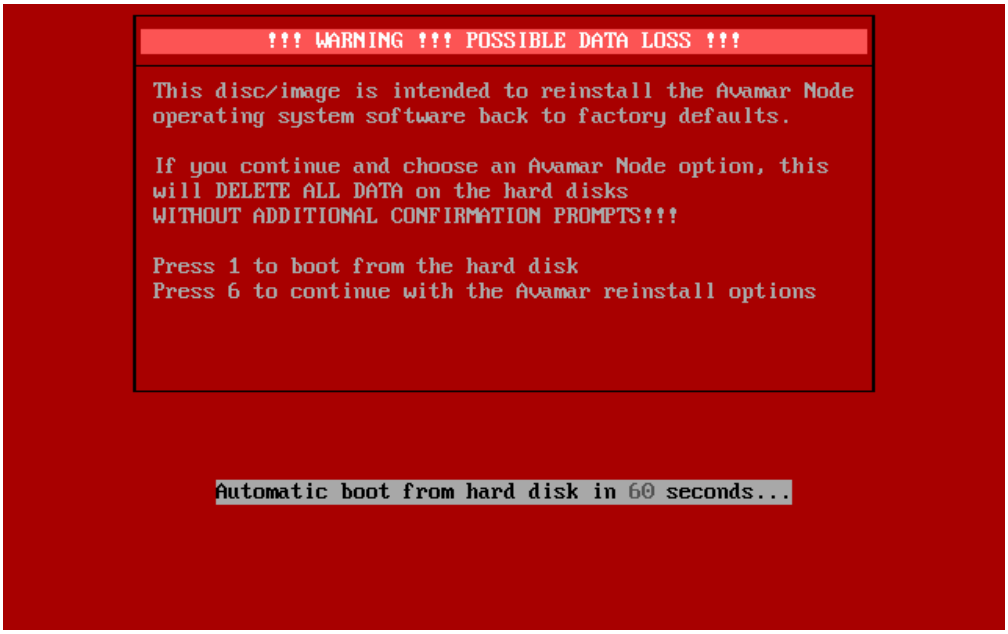

Figure 6. Data loss warning

3. Press **6** to acknowledge the data loss warning.

   The platform selection menu appears.

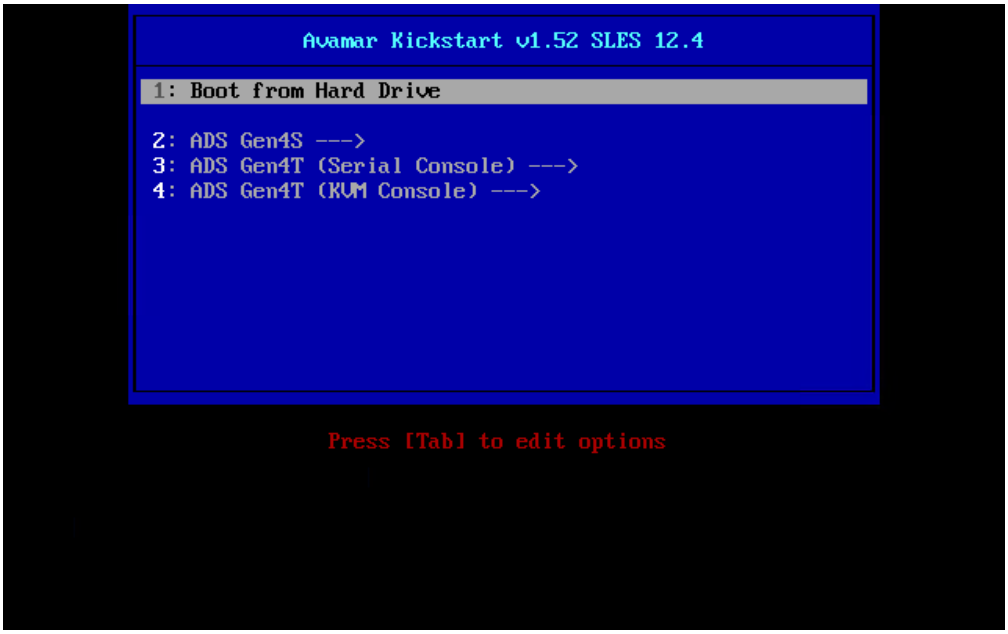

Figure 7. Platform selection menu

4. Select **ADS Gen4T (KVM Console)**, and then press Enter.

   The node type selection menu appears.

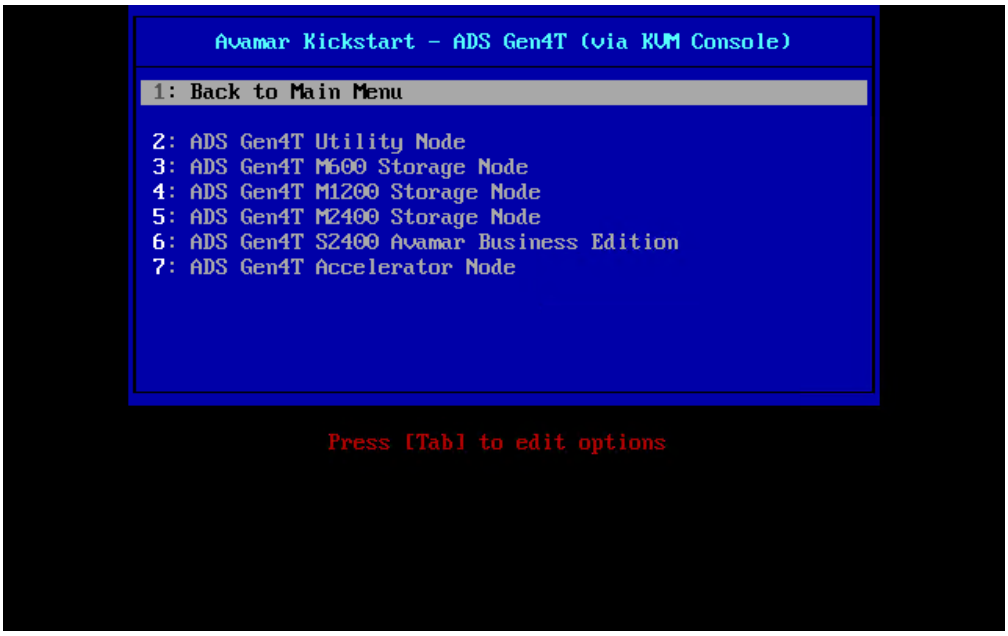

Figure 8. Gen4T node type selection menu

5. Use the down-arrow key to scroll through the boot options.
6. Select **ADS Gen4T Accelerator Node**, and then press Enter.
   The automated operating system installation procedure begins. The kickstart is not complete until the first login prompt becomes available.
7. Wait for the login prompt after the reboot.
8. Log in as the root user.

   NOTE: At this stage, you are not required to log in as the admin user and use `su`.

9. Determine the current kickstart version by typing the following command:

   ```
   cat /PlatformInfo
   ```

   Output similar to the following appears:

```
KS_OS_NAME="SUSE Linux Enterprise Server"
KS_OS_VERSION="12"
KS_OS_PATCHLEVEL="4"
KS_VERSION="1.61"
KS_PRODUCT="DellEMC Avamar Server"
KS_MODEL="accelerator"
KS_PLATFORM="ADS4T"
```

Ensure that the kickstart version matches the version of the kickstart ISO image. If the platform information file does not exist or does not match the kickstart ISO image, the kickstart was unsuccessful.

10. Verify the existence of the kickstart post scripts by typing the following commands:

    cd /var/log/YaST2

    grep -iE 'autoinstscript.*\.sh' * | grep -v "\.log"

    The following output appears:

    ```
    y2log:2019-09-12 05:59:35 <1> node(2816) [Ruby] modules/AutoinstScripts.rb:907 Writing
    script into /var/adm/autoinstall/scripts/zzz-build_rpm_list.sh
    ```

    Verify that errors did not occur during the generation of the post scripts.

11. Verify that all of the post scripts exist as expected by typing the following command:

    ls -a /var/adm/autoinstall/scripts/*.sh

    The following output appears:

    ```
    /var/adm/autoinstall/scripts/info_accelerator.sh
    /var/adm/autoinstall/scripts/zzz-build_rpm_list.sh
    /var/adm/autoinstall/scripts/info_gen4t.sh
    ```

    Verify that all of these scripts exist on the vNDMP accelerator node. If any of these scripts are missing, the kickstart was unsuccessful.

12. Check the contents of the Message of the Day file by typing the following command:

    grep -i avamar /etc/motd

    The following output appears:

    ```
    * This is an Avamar Super Node                                        *
    ```

    If the file does not include the output above, the kickstart was unsuccessful.

    NOTE: If any of the checks indicate a problem with the kickstart process, do not continue until you have resolved the issues. Contact Customer Support for assistance.

Results

The vNDMP accelerator node is ready for network configuration.

Configure the SLES VM network settings

About this task

After the kickstart process creates the necessary network interfaces, use the YaST utility to apply the environment-specific network settings that were listed in Required information on page 58 to the SLES VM.

This task configures the primary backup network port for the SLES VM (eth0). Ensure that you are still logged in as the root user.

Steps

1. Open the YaST Linux configuration application by typing the following command:

   yast

   The **YaST Control Center** appears.

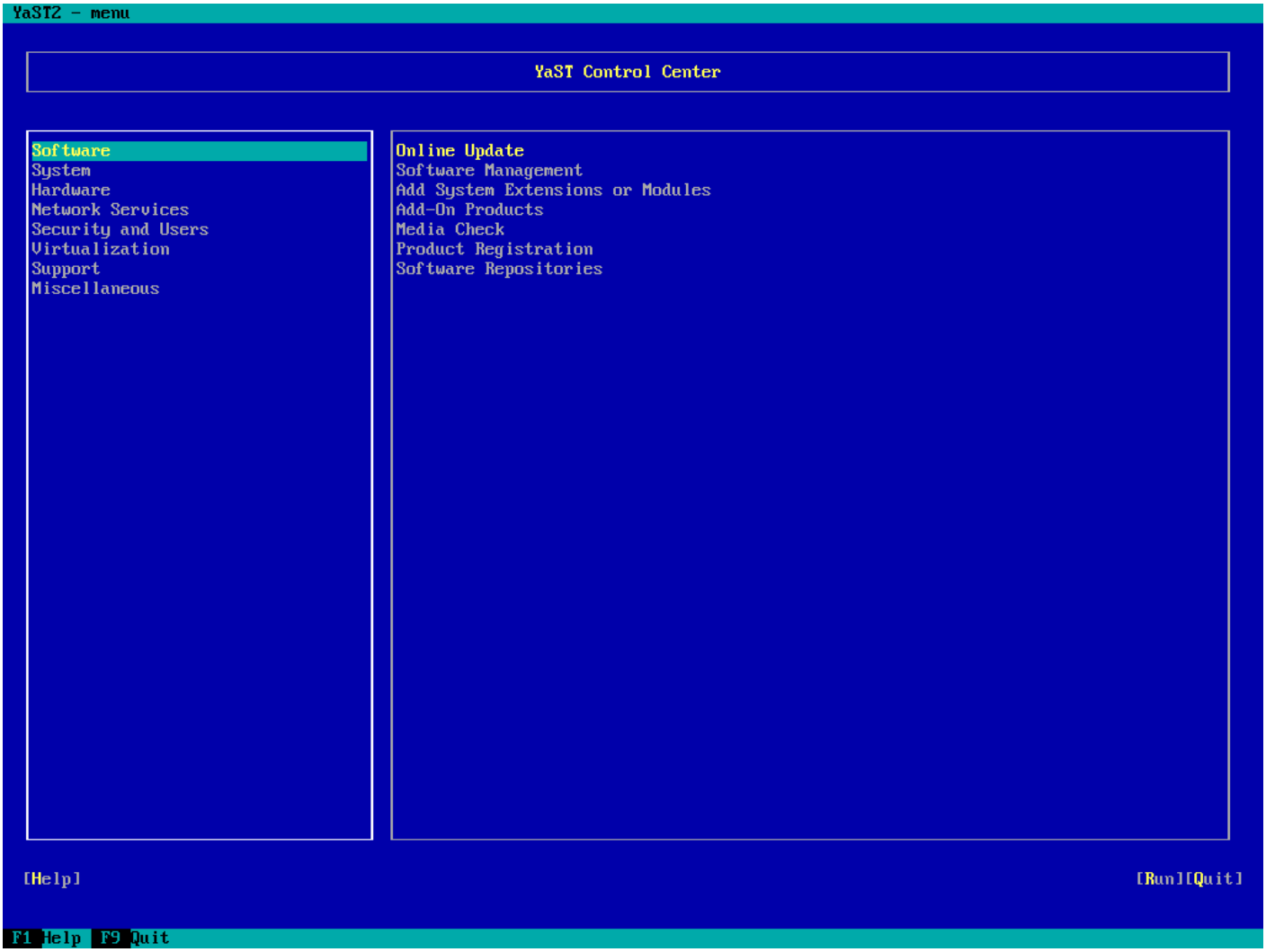

Figure 9. YaST Control Center

> **NOTE:** In YaST, use the **Tab** key to move to an option. Correct typing errors or replace default settings by using the **Backspace** key. To select a checkbox (a set of parentheses), press the spacebar.

2. Use the down-arrow to select **System**, the right arrow to move to the box on the right, and the down-arrow to select **Network Settings**, and then press Enter.

   YaST loads the system configuration and the **Network Settings** screen appears.

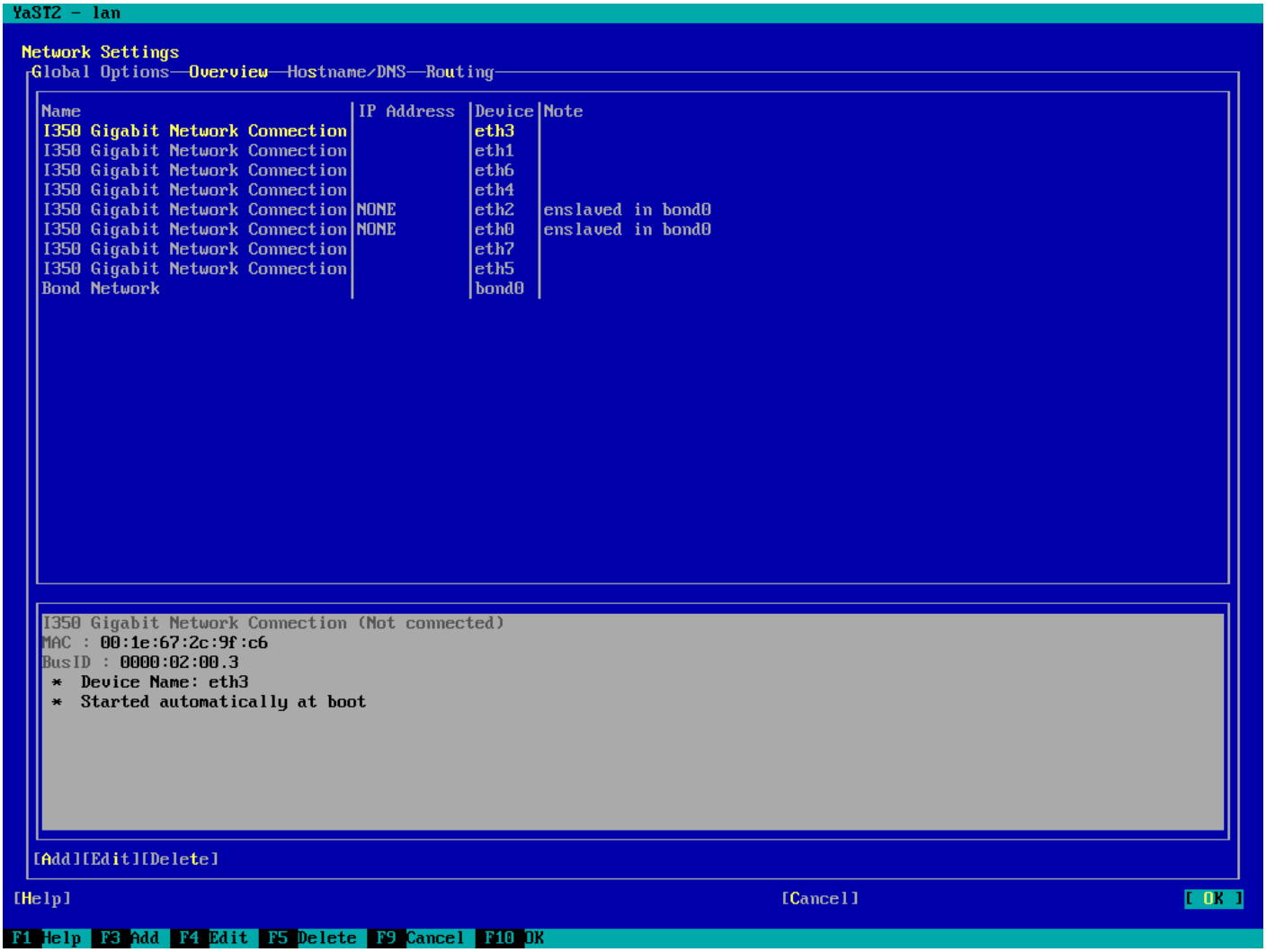

Figure 10. YaST network settings - Overview

3. Tab to the list of network connections and use the arrow keys to select the primary backup network port.

   As you move from one entry to the next in the list, the description in the second box changes. You may need to tab to the second box and use the arrow keys to scroll until you can see the interface name that is assigned to each network card.

4. With the primary backup network port selected, tab to **Edit**, and then press Enter.

   The **Network Card Setup** screen appears.

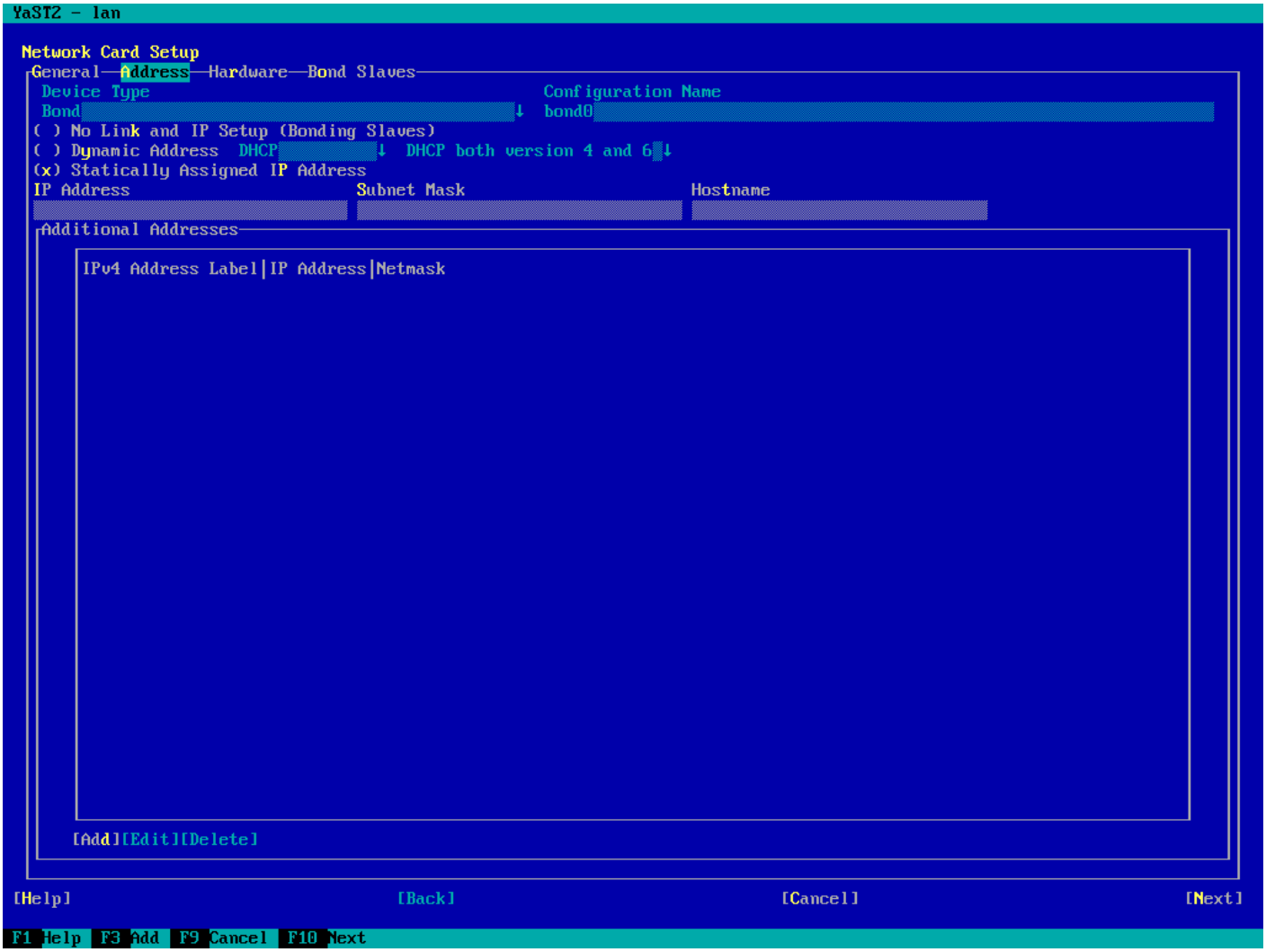

Figure 11. YaST network card setup

5. Use the arrow keys to select the **Address** tab, if required.
6. Tab to **Statically assigned IP address**.
7. Select the checkbox (with an X) by pressing the spacebar.
8. Tab to **IP address**.
9. Type the IP address that is assigned to the primary backup network port.
10. Tab to **Subnet Mask**.
11. Type the subnet mask address that is assigned to the primary backup network port.
12. Tab to **Hostname**.
13. Delete the default hostname.
14. Type the hostname that is assigned to the vNDMP accelerator node.

    The hostname must resolve to the IPv4 address for backup clients to use, and the address that you assign to the primary backup network port in the followup software installation.
15. Tab to **Next** at the bottom of the screen, and then press Enter.

    The **Network Settings** screen appears.
16. Tab to the top menu and use the arrow keys to select **Hostname/DNS**.

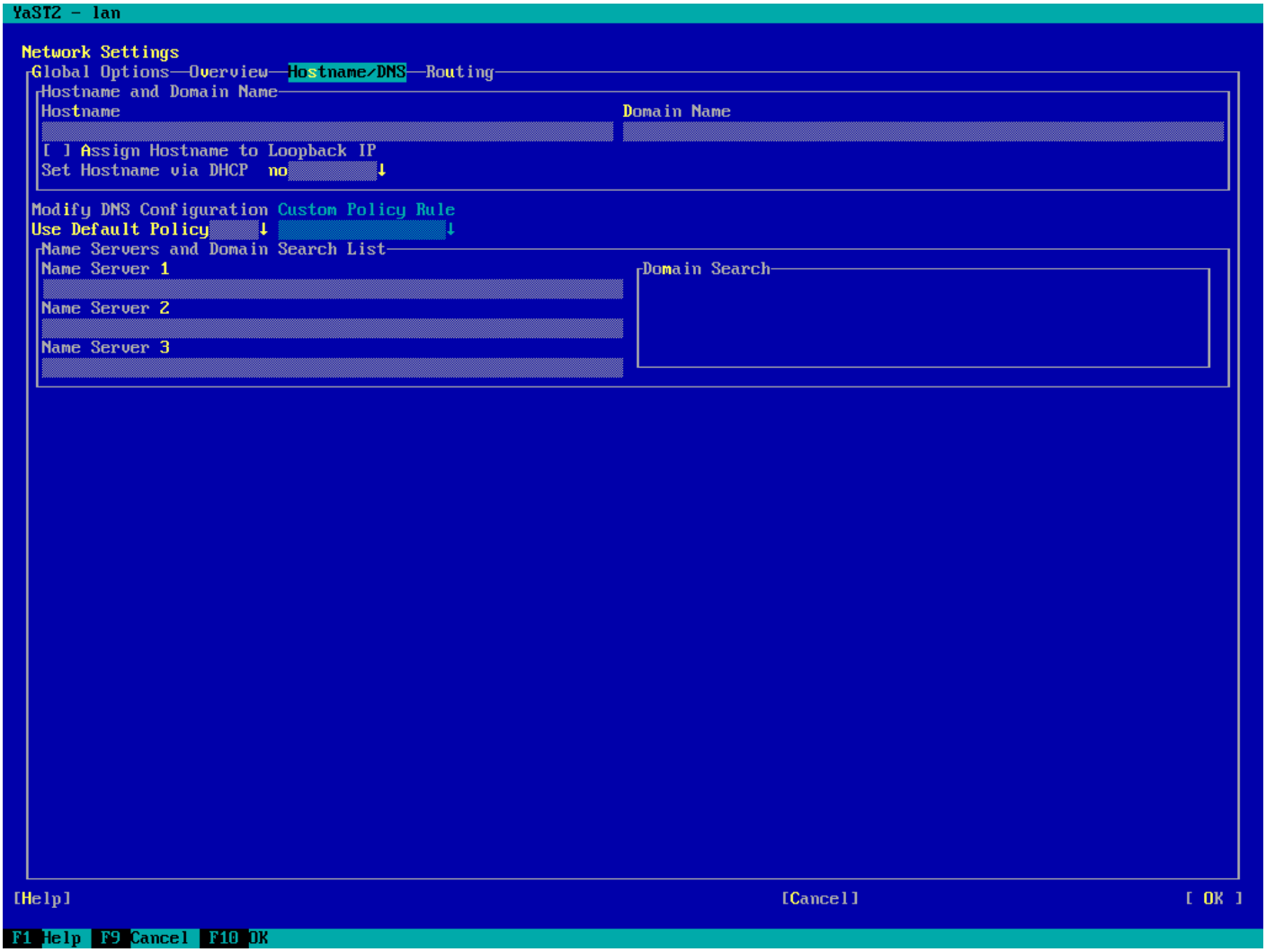

Figure 12. YaST network settings - Hostname/DNS

17. Tab to **Hostname**.
18. Delete the default hostname.
19. Type the correct hostname.

    This parameter must be the short name of the hostname that you typed on the previous screen.
20. Tab to **Domain Name**.
21. Delete the default domain name.
22. Type the correct domain name.
23. Tab to the **Name Servers and Domain Search List** section and specify these parameters.

    Type up to three IPv4 addresses of DNS recurring name resolving servers.
24. Tab to **Domain Search**.
25. Use the right arrow to move the cursor to the end of the default entry and delete the default domain name.
26. Type the correct domain name to search.
27. Tab to the top menu and use the right arrow to select **Routing**.

    The **Network Settings-Routing** screen appears and **Default IPv4 Gateway** should be selected.

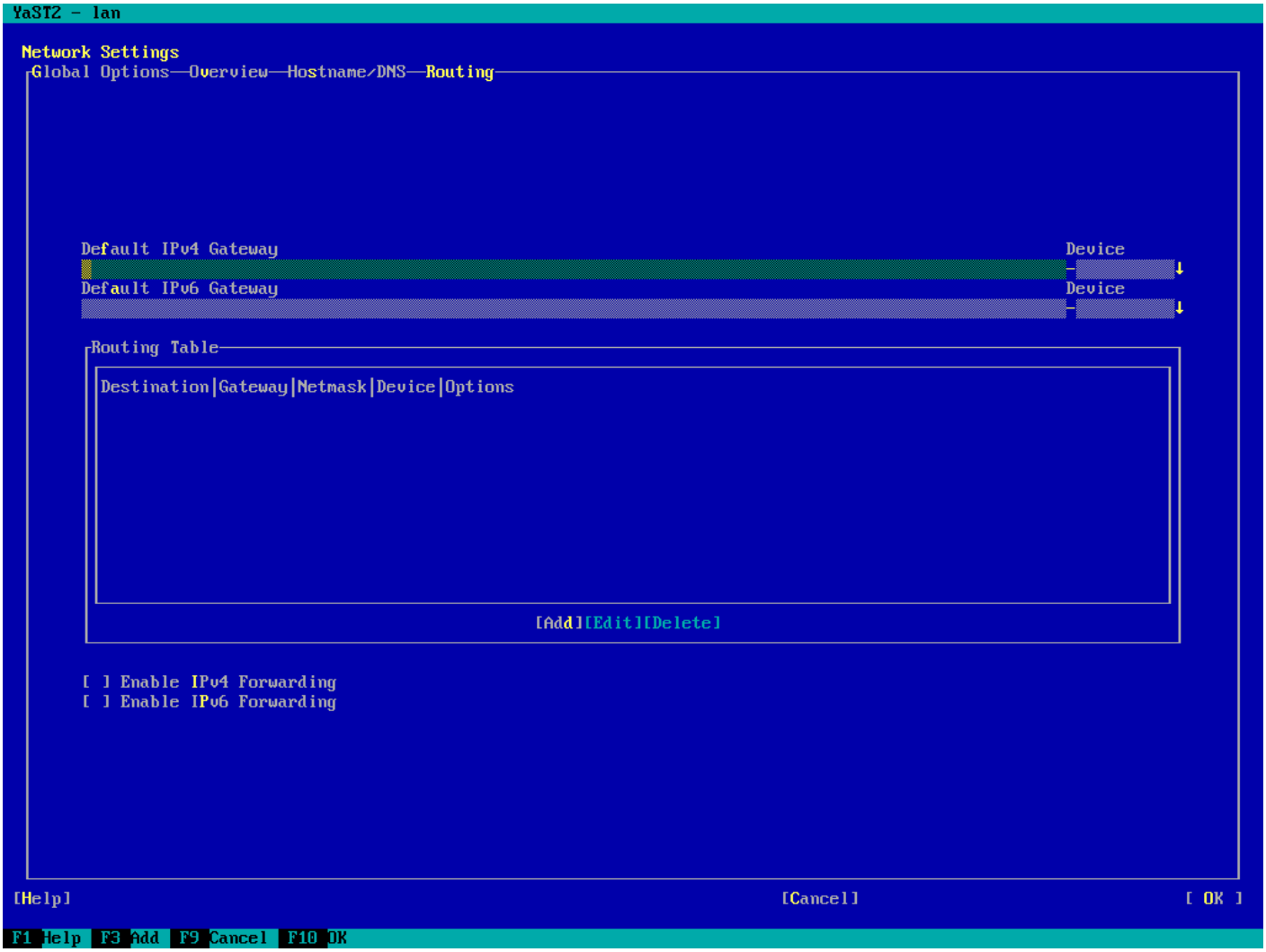

Figure 13. YaST network settings - Routing

28. Type the default gateway address.
29. Tab to **OK** at the lower right of the screen, and then press Enter.

    The **Network Settings** screen closes and YaST displays an informational message about saving configuration information.
30. In the YaST Control Center, tab to **Quit** at the lower right of the screen, and then press Enter.

Results

The SLES VM is now accessible over the network and is ready for software installation.

Install the NDMP accelerator software

Verify that the vNDMP accelerator node is accessible over the network by establishing an SSH connection, and then install the accelerator software.

The instructions in Installing and configuring the accelerator software on page 20 provide more information.

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.

backup policy
In the AUI, a backup policy specifies a dataset, schedule, and retention settings that are applied to a client or a group of clients. A backup policy must contain at least one Avamar client. If the backup policy contains two or more clients, the clients must belong to the same Avamar domain. You can override backup policy settings at the client level.

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

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
In Avamar Administration, a group policy is defined as a *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.

V

virtual machine (VM)
A computer that is a software implementation of a computer. Virtual machines are used to run different operating systems at the same time on one physical computer. Each operating system runs in its own isolated execution environment.

vNDMP accelerator
A virtualized appliance that provides the same functionality as a physical NDMP accelerator, but in a virtual environment.

vSphere Client
A VMware software application used to control and manage a vCenter. The vSphere Client is also known as the "thick client."

vSphere Web Client
A VMware web interface used to control and manage a vCenter.