Quest® NetVault® 14.1.3

Built-in Plug-ins User's Guide

© 2026 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest Software, Quest, the Quest logo, QoreStor, and NetVault are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

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

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

NetVault Built-in Plug-ins User's Guide
Updated - November 2026
Software Version - 14.1.3
NVG-101-14.0-EN-01

Contents

Introduction 5

About Quest® NetVault® 5

About this document 6

Target audience 6

Recommended additional reading 6

Using Plug-in *for Consolidation* 7

About backup consolidation methods 7

Configuring default settings 8

Creating a consolidated saveset 8

Restoring a consolidated saveset 9

Using Plug-in *for Data Copy* 10

About Data Copy methods 10

Configuring default settings 10

Performing a Data Copy job 11

Important notes 17

Restoring a Data Copy 19

Using *Plug-in for Encryption* 20

About Plug-in *for Encryption* *20*

Encryption strategy overview 21

Selecting which backups to encrypt 21

Selecting the encryption algorithm 21

Encrypting primary or secondary backups 22

Encrypting all or specific backups 22

Configuring default settings 23

Encrypting all backups 24

Performing job-level encryption 24

Encrypting primary backup 24

Encrypting a Secondary Copy 25

Troubleshooting 25

Using Plug-in *for Databases* 28

Configuring default settings 28

Backing up the NetVault Database 29

Restoring NetVault Database 30

Prerequisites 31

Restore Procedure 31

Using Plug-in *for Raw Devices* 34

Backing up raw devices 34

Prerequisites 34

Backup procedure 34

Restoring a raw device backup 36
Prerequisites 36
Restore Procedure 36
Relocating data to an alternate disk or partition 37
Restoring data to an alternate NetVault Client 38
Prerequisites 38
Restore procedure 38

About us 39
Technical support resources 39

1

Introduction

- About Quest® NetVault®
- About this document
- Target audience
- Recommended additional reading

About Quest® NetVault®

The built-in plug-ins are packaged with the Quest® NetVault® (NetVault) software, and automatically installed on the respective machines when you install the NetVault Server or Client software. A standard installation of NetVault includes the following built-in plug-ins.

- **Quest NetVault Plug-in *for FileSystem* (Plug-in *for FileSystem*):** The Plug-in *for FileSystem* increases confidence in the recoverability of critical file system data and eliminates the need for writing complex backup and recovery scripts. Through an intuitive user interface and automated workflow process, the plug-in offers a centralized console to set up, configure, and create flexible backup policies that account for multiple recovery scenarios. Support for Full, Incremental, and Differential Backups allows you to choose a preferred backup strategy. The plug-in minimizes downtime by allowing you to restore full volumes, individual partitions, or individual directories and files quickly and reliably with minimal interaction. Through automatic integration with a wide range of backup devices, you can be confident that your data is protected and safely stored off-site to meet your disaster recovery and business continuity goals.
- **Quest NetVault Plug-in *for Consolidation* (Plug-in *for Consolidation*):** The Plug-in *for Consolidation* lets you create a composite saveset by combining a Full Backup and its associated Incremental Backups. You can use this consolidated saveset as the base for subsequent Incremental Backups. For example, after an initial Full Backup, you can schedule Incremental Backups from Monday to Friday, and schedule a backup consolidation job on Saturday. You can use the consolidated backup created on Saturday as the base for next week's Incremental Backups. The Plug-in *for Consolidation* does not back up data from a client; it just creates a composite set from existing savesets.
- **Quest NetVault Plug-in *for Data Copy* (Plug-in *for Data Copy*):** The Plug-in *for Data Copy* lets you create one or more copies of backups for off-site storage and disaster recovery purposes. You can schedule jobs to copy or migrate data at convenient off-peak hours, and thus shrink your backup windows. The Plug-in *for Data Copy* does not back up data from a client; it just creates a copy of an existing backup.
- **Quest NetVault Plug-in *for Databases* (Plug-in *for Databases*):** The Plug-in *for Databases* protects system data (such as configuration files, system settings, backup indexes, backup media information, job schedule, licenses, and other data) stored in the NetVault Database. You can use this backup to recover a functional NetVault Server after a failure.
- **Quest NetVault Plug-in *for Encryption* (Plug-in *for Encryption*):** This plug-in provides support for CAST-128, CAST-256, non FIPS compliant AES-256, and FIPS compliant AES-256 algorithms to meet regulatory backup security requirements.
- **Quest NetVault Plug-in *for Raw Devices* (Plug-in *for Raw Devices*):** The Plug-in *for Raw Devices* protects data stored on physical disks. The plug-in lets you recover the Master Boot Record (MBR), system partitions, and individual user partitions from a point-and-click user interface without writing any complex scripts.

- **Quest NetVault Plug-in *for Rapid Data Access* (Plug-in *for RDA*)**: The Plug-in *for RDA* lets you use the client-side and inline deduplication capabilities that are available in other products, such as the Quest DR Series system of deduplication appliances and the software-defined Quest QoreStor™ storage devices (Linux only).

About this document

This guide provides information about configuring and using the following plug-ins:

- Plug-in *for Consolidation*
- Plug-in *for Data Copy*
- Plug-in *for Databases*
- Plug-in *for Raw Devices*

For information about using the Plug-in *for FileSystem*, see the *Quest NetVault Plug-in for FileSystem User's Guide*.

Target audience

This guide is intended for backup administrators and other technical personnel who are responsible for designing and implementing a backup strategy for the organization. A good understanding of the operating systems under which the NetVault Server and Clients are running is assumed.

Recommended additional reading

- *Quest NetVault Installation Guide:* This guide provides information about installing the NetVault Server and Client software.
- *Quest NetVault Administrator's Guide:* This guide provides information about configuring and using NetVault to protect your data. It provides comprehensive information about all NetVault features and functionality.
- *Quest NetVault CLI Reference Guide:* This guide provides information about using the NetVault command-line utilities.

You can download these guides from https://support.quest.com/technical-documents.

2

Using Plug-in *for Consolidation*

- About backup consolidation methods
- Configuring default settings
- Creating a consolidated saveset
- Restoring a consolidated saveset

About backup consolidation methods

The plug-in offers the following methods for consolidating the Full and Incremental Backups:

NOTE: The Plug-in *for Consolidation* can only be used to consolidate the Full and Incremental Backups created using the Plug-in *for FileSystem*.

The Plug-in for *Consolidation* does not support snapshot-only FileSystem backup.

- **Backup Jobs:** This method creates a composite set by combining all backups up to the selected Incremental Backup. For example, if Full Backups are performed on Sundays and Incremental Backups Monday through Saturday, you can select Wednesday's Incremental Backup to consolidate all savesets up to the selected backup.

  You can use this method for creating consolidated savesets before changing your backup schedule, re-using media that store the Incremental Backups, or creating an archive.

- **Backup Sets:** This method creates a composite set by combining all backups up to most recent Incremental Backup created using the selected Backup Selection Set. For example, if Full Backups are performed on Sundays and Incremental Backups Monday through Saturday, you can select the applicable Backup Selection Set to consolidate all savesets up to last Incremental Backup created using that set.

  The Backup Set method is recommended when you want to perform regular backup consolidation jobs. A policy to create consolidated backups can only be defined using the Backup Sets method.

IMPORTANT:

- We recommend that you do not select the advanced backup option **Enable Deduplication** for Incremental Backups that are consolidated and saved to Quest NetVault SmartDisk (NetVault SmartDisk). By not selecting this option, you eliminate the unnecessary overhead of rehydrating the deduplicated Incremental Backups during the consolidation process. You can enable deduplication while backing up the Consolidated Full Backup.
- When backups stored on the Quest DR Series or QoreStor systems are selected for backup consolidation jobs, NetVault performs a synthetic operation to generate the consolidated full backup. This process uses only metadata to generate a consolidated full backup index, which provides an improved performance speed over the traditional method.

Configuring default settings

To configure the default settings for Plug-in for Consolidation:

1. In the Navigation pane, click **Change Settings**. On the **Configuration** page, click the applicable icon, and on the Settings page, click **Plugin Options**.
2. Under **Consolidate**, configure the following setting:
   - **Sort Backups Newest First:** By default, the saveset list on the **NetVault Selections** page is sorted by date and time in descending order (that is, from the latest to the earliest date). To sort the list in ascending order (from the earliest to the latest date), clear the check box.

     The setting only applies to the **Backup Jobs** method.
3. Click **OK** or **Apply** to save the settings.

Creating a consolidated saveset

To perform a backup consolidation job:

1. In the Navigation pane, click **Create Backup Job**.

   You can also start the wizard from the **Guided Configuration** link. In the Navigation pane, click **Guided Configuration**, and then on the **NetVault Configuration Wizard** page, click **Create Backup Jobs**.
2. In **Job Name**, specify a name for the job. Assign a descriptive name that allows you to easily identify the job for monitoring its progress or restoring data.

   A job name can contain alphanumeric and non-alphanumeric characters, but it cannot include non-Latin characters. There is no length restriction. However, a maximum of 40 characters is recommended on all platforms.
3. In the **Selections** list, select an existing Backup Selection Set, or complete the following steps to create a set.
   a. Click **Create New** to open the **NetVault Selections** page.
   b. Open the NetVault Server, and in the list of plug-ins, open **Consolidate Incremental Backups**.
   - In Managed Service Providers (MSP) environment, the tenant must:

     Open the NetVault Client node, and in the list of plug-ins, open **Consolidate Incremental Backup**.

     > **NOTE:** In Managed Service Providers (MSP) environment, to define and submit consolidate incremental backup jobs from NetVault client is supported from NetVault Backup 12.2 release onwards. To use plug-in for consolidation on the available clients you need to install or upgrade latest NetVault Server and Client.

   c. To consolidate all backups up to the selected backup:
      - Open the **Backup Jobs** node, and in the list of NetVault machines, open the client from which the data was backed up.
      - Select the last backup up to which you want to create a consolidated saveset.

   d. To consolidate all backups up to the most recent backup created using a Backup Selection Set:
      - Open the **Backup Sets** node, and in the list of NetVault machines, open the client for which the set was created.
      - Select the Backup Selection Set that was used to create the Full and Incremental Backups.

   e. Click **Save**, and in the **Create New Set** dialog box, type a name for the set. Click **Save** to close the dialog box.

> **NOTE:** A set name can contain alphanumeric and non-alphanumeric characters, but it cannot include non-Latin characters. On Linux OS, the names can have a maximum of 200 characters. On Windows OS, there is no length restriction. However, a maximum of 40 characters is recommended on all platforms

4 In the **Plugin Options** list, select an existing Backup Options Set, or complete the following steps to create a set.

   a Click **Create New** to open the **Consolidate Options** page.

   b Configure the following option:

      - **Run consolidation on client:** By default, the consolidation job runs on the NetVault Server. To run the job on a different NetVault machine, select the client in the list.

   c Click **Save**, and in the **Create New Set** dialog box, type a name for the set. Click **Save** to close the dialog box.

5 Select or create the Schedule Set, Source Set, Target Set, and Advanced Options Set. For more information about these sets, see the *Quest NetVault Administrator's Guide*.

6 To submit the job for scheduling, click **Save & Submit**. You can monitor the job progress from the **Job Status** page and view the logs from the **View Logs** page.

   To save the job definition without scheduling it, click **Save**. You can view, edit, or run this job from the **Manage Job Definitions** page. This job is not displayed on the **Job Status** page until you submit it.

   For more information about **Job Status**, **View Logs**, and **Manage Job Definitions**, see the *Quest NetVault Administrator's Guide*.

Restoring a consolidated saveset

For a restore job, you can use either the original savesets (Full, Incremental, and Differential savesets) or the Consolidated saveset created using these backups. The procedure for restoring data is the same for the original and the consolidated savesets. For information about restoring the data, see the relevant section in the *Quest NetVault Plug-in for FileSystem User's Guide*.

3

Using Plug-in *for Data Copy*

- About Data Copy methods
- Configuring default settings
- Performing a Data Copy job
- Restoring a Data Copy

About Data Copy methods

The Plug-in *for Data Copy* offers the following methods:

- **Backups:** This method can be used to create a copy of selected backup. It can be used to perform non-repeating Data Copy jobs.

  To use Data Copy for continuous data protection (CDP) savesets of Plug-in *for Microsoft 365* backups, use Backups. This method copies both Full and Incremental backups. For more information, see the *NetVault Plug-in for Microsoft 365 User's Guide.*

  To Data Copy continuous data protection (CDP) savesets of Plug-in *for VMware* backups, use Backup. For CDP VMware backups this method can copy either Full or synthetic Full backup or Incremental backup. If incremental backup is selected not copy the previous chain. For more information, see the *NetVault Plug-in for VMware User's Guide.*
- **Backup Sets:** This method can be used to create copy of the most recent backup created using the selected Backup Selection Set. The Backup Sets method is recommended when you want to perform regular Data Copy jobs.

IMPORTANT:

- You cannot use the Plug-in *for Data Copy* to create copies of backups that were created using the **Archive** option.
- You cannot use the Plug-in *for Data Copy* to create copies of Data Copy backups that were created using the Secondary Copy method or the Plug-in *for Data Copy*. In other words, you cannot use a Data Copy backup to create another Data Copy.

NOTE: Duplicate doesn't create a separate independent backup. It creates an additional copy of the same backup, so the copies are interchangeable. When you restore, NetVault Media Manager automatically chooses which available copy to use. The backup will continue to appear in the NetVault WebUI as long as at least one copy exists. For example, if you Duplicate with Migrate, the original copy is removed but the backup is still available because the duplicated copy remains. Likewise, if one copy is lost (for example, the media is blanked), the backup is still available as long as another copy remains, and you can create more duplicates from any remaining copy.

Configuring default settings

To configure the default settings for Plug-in for Data Copy

1 In the Navigation pane, click **Change Settings**. On the **Configuration** page, click the applicable icon, and on the Settings page, click **Plugin Options**.

2 Under **Datacopy**, configure the following setting:

- **Sort Backups Newest First:** By default, the saveset list on the **NetVault Selections** page is sorted by date and time in descending order (that is, from the latest to the earliest date). To sort the list in ascending order (from the earliest to the latest date), clear the check box.

  The setting only applies to the **Backups** method.

3 Click **OK** or **Apply** to save the settings.

Performing a Data Copy job

To perform a Data Copy job

1 In the Navigation pane, click **Create Backup Job**.

You can also start the wizard from the Guided Configuration link. In the Navigation pane, click **Guided Configuration**, and then on the **NetVault Configuration Wizard** page, click **Create Backup Jobs**.

2 In **Job Name**, specify a name for the job. Assign a descriptive name that allows you to easily identify the job for monitoring its progress or restoring data.

A job name can contain alphanumeric and non-alphanumeric characters, but it cannot include non-Latin characters. There is no length restriction. However, a maximum of 40 characters is recommended on all platforms.

3 In the **Selections** list, select an existing Backup Selection Set, or complete the following steps to create a set.

a Click **Create New** to open the **NetVault Selections** page

b Open the NetVault Server, and in the list of plug-ins, open **Data Copy**.

- In Managed Service Providers (MSP) environment, the tenant must:

  Open the NetVault Client node, and in the list of plug-ins, open **Data Copy**.

  NOTE: In Managed Service Providers (MSP) environment, to define and submit data copy jobs from NetVault client is supported from NetVault 12.2 release onwards. To use data copy plug-in on the available clients you need to install or upgrade latest NetVault Server and Client.

c To copy the selected backup:

- Open the **Backups** node, and in the list of NetVault machines, open the client from which the data was backed up.
- Open the plug-in that was used to create the saveset, and select the saveset that you want to copy.

d To copy the most recent backup created using a Backup Selection Set:

- Open the **Backup Sets** node, and in the list of NetVault machines, open the client for which the set was created.
- Open the plug-in that was used to create the set, and then select the Backup Selection Sets that was used to create the Full and Incremental Backups.

e Click **Save**, and in the **Create New Set** dialog box, type a name for the set. Click **Save** to close the dialog box.

> **NOTE:** A set name can contain alphanumeric and non-alphanumeric characters, but it cannot include non-Latin characters. On Linux OS, the names can have a maximum of 200 characters. On Windows OS, there is no length restriction. However, a maximum of 40 characters is recommended on all platforms

4 In the **Plugin Options** list, select an existing Backup Options Set, or complete the following steps to create a set.

a Click **Create New** to open the **Data Copy Options** page.

b Under **Copy Type**, configure the following options.

Option	Description
Copy a full backup to produce a new independent copy of the data	This option is recommended when you want to create a copy for off-site storage. The Data Copy method breaks down the backup into segments and copies the segments to the backup device. During restore, either the primary backup or the secondary copy is used to recover data. The segments from the primary backup and secondary copy are not interchangeable. Therefore, it is possible to enable encryption for the Data Copy when the primary copy is unencrypted. This option is useful when you want to use the deduplication option for the primary backups. The Data Copy option can be used to create a copy of the Full as well as Incremental Backups. This method removes all links between the Full and Incremental Backups, and allows you to set a new retention period for the copy. **NOTE:** Before creating a Data Copy of regular Incremental Backup, you must have created a copy of the initial Full Backup and the previous Incremental Backups in the backup sequence. Otherwise, the plug-in reports an error. For more information, see Important notes. **NOTE:** For Data Copy of a Continuous Data Protection (CDP) VMWare saveset any Incremental Backup saveset can be selected for Data Copy. It does not depend on previous Incremental Backups.
Duplicate a backup	This option is recommended when you want to migrate the saveset to different media. The Duplicate method creates an exact copy which is linked to the original backup. This method breaks down the backup into segments and copies the segments to the storage device. During restore, the segments from the primary backup and secondary copy are interchangeable. As it is not possible to mix unencrypted segments with encrypted segments during restore, you cannot enable or disable encryption for the Duplicate. If the original saveset is encrypted, the Duplicate method creates an encrypted copy. If the original saveset is not encrypted, this method creates an unencrypted copy. **NOTE:** This option can be used to create a copy of the Full as well as Incremental Backups. The savesets created using the Duplicate method automatically share the original saveset's name and reference. When restoring copies of Incremental Backups, NetVault requires the original Full Backup. On the Create Restore Job page, only one saveset is listed for the original and duplicate backup. **NOTE:** This option does not apply to continuous data protection (CDP) backups.

Option	Description
Use saveset name from original backup	By default, the plug-in assigns a new saveset name to a copy created using the **Copy a full backup to produce a new independent copy of the data** option. This name is derived from the Job Name. If you want to use the original saveset name for such copies, select this check box.
Allow streams to share media	This check box is not selected by default. You can use this option with the **Duplicate a backup** method. When creating a Duplicate of a multi-stream backup, you can use this option to convert multiple data streams into a sequential data stream. If you do not select this check box, each stream is written separately. If you are using a disk-based device to store the Duplicate backup, multiple streams are recommended. For such jobs, there is no need to select this check box. If you do not select the **Allow Streams to Share Media** check box for tape devices, each data stream targets a separate media item. Any tape that is used to write a stream is excluded from the allowable media items. If enough tapes are not available for the job, the job fails. When using tape devices to store the Duplicate backups, you can select this check box to use minimal media items.
Automatically get a set's last full backup	You can use this option with the **Backup Sets** method to create a copy of the last Full Backup that was performed using a particular Backup Selection Set. The Incremental Backups are not copied when you select this option. **NOTE:** For CDP backups, Plug-in *for VMware* copies the latest Synthetic Full backup.
Use a set's most recent job regardless of type	You can use this option with the **Backup Sets** method to create a copy of the last backup, regardless of its type (Full or Incremental Backup). This option allows you to create copies of Incremental Backups. **NOTE:** When you use this option, you must run the data copy job before the next primary backup (Full or Incremental) for that backup sequence is run; otherwise, the plug-in creates a copy of that primary backup.

Option	Description

Tagname	When you create multiple copies of an Incremental Backup Sequence, you must provide a tag can be used to identify each copy. A tag can contain any string value. Without a tag, the plug-in cannot distinguish between the multiple copies of a backup sequence.
	NOTE: This option does not apply to continuous data protection (CDP) backups.
	On the data selection page for restore, the savesets created with the Plug-in for Data Copy are labeled as follows:
	• **Data copies created without a tag:**
	`<Saveset Name> – DataCopy of <Selection Set Name> (Saveset <#>) <Timestamp>`
	• **Data copies created with a tag:**
	`<Saveset Name> – DataCopy of <Saveset #>, Tag '<User Tag>' (Saveset <#>) <Timestamp>`
	Example:
	The following example explains how to use this option.
	1 Create a Backup Selection Set, and perform a Full Backup using the set.
	2 Create a copy of the set using device 1. While creating the copy, specify a unique **Tagname** on the **Data Copy Options** page.
	3 Create a second copy of the set using device 2. While creating the copy, specify a unique **Tagname** on the **Data Copy Options** page.
	4 Perform an Incremental Backup for the set.
	5 Repeat steps 2 and 3 for the Incremental Backup.
	6 On the data selection page for restore job, both the original backup and two copies of the backup sequence are displayed.
	7 To restore data from a specific copy, select the applicable saveset. You can identify a copy using its **Tagname**.

c Configure the required additional options.

Option	Description
Migrate (Discard original backup)	To migrate the backup instead of creating a copy, select this check box. After copying the data, NetVault deletes the index for the original backup. **NOTE:** When creating copies of the Plug-in *for FileSystem* backups, the **Migrate** option can only be selected for Full Backups that do not have any associated Incremental or Differential Backups. If you select this option for a Full Backup that has an associated Incremental or Differential Backup, NetVault creates the secondary copy successfully, but it does not delete the index for the primary or original backup. For such backups, after creating the copy, you must manually retire the primary or original backup. **NOTE:** This option does not apply to continuous data protection (CDP) backups.

Option	Description
Use optimised replication between devices that support this feature	Optimized replication enables transfer of deduplicated data directly from one device to another device of the same type during a Data Copy or Duplicate operation. It provides an efficient method to create secondary copies and offers the following advantages: • Copies data in its deduplicated form, which greatly reduces the amount for data transferred over the network. • Copies data directly from the source to the destination without using any resources on the NetVault Server. The following storage devices support optimized replication: • **Quest DR Series Systems:** To perform optimized replication, both the source and target Quest DR Series systems must be running the same release version of the DR OS. Replication is not supported between systems that run different releases of the OS. For example, to replicate data from a source system that is running DR OS 3.x, the target system must be running the same OS release version. Replication is unsuccessful if the target system is running DR OS release 2.0.x or 3.0.x. **NOTE:** When optimized replication and backups are performed simultaneously on a Quest DR Series system, the backup throughput is affected. • **Quest QoreStor:** Supported only on Linux. **NOTE:** When using CDP, the primary QoreStor must be version 7.1.2 or later. For replication, the secondary QoreStor must also use at least version 7.1.2. **NOTE:** Ensure that the schedule for Data Copy between Synthetic Full backups does not overlap. Allow enough time for the next Synthetic Full backup to compete before the Data Copy job begins. • **NetVault SmartDisk devices:** To perform optimized replication, you require NetVault SmartDisk 2.0 or later. If the login credentials configured for the source and destination NetVault SmartDisk Servers do not match, replication fails. To ensure a successful replication, do one of the following: - Disable WebDAV authentication on both NetVault SmartDisk Servers. - Enable WebDAV authentication only on the source server. - Configure the same login credentials on both servers. **NOTE:** When copying a backup from a NetVault SmartDisk to a different device type (for example, VTL, Quest DR Series System, or Data Domain System), you must clear this check box. If you do not clear this check box, the Data Copy or Duplicate job fails or stops responding. • **DD Boost-enabled Data Domain Systems:** The secondary copy backups between two DD Boost-Enabled Data Domain Systems use the managed file-level replication feature provided by DD Boost. File-level replication requires the DD Boost Replicator license, which must be installed on both the source and destination Data Domain systems. **NOTE:** If the source and target Data Domain systems are running different versions of the Data Domain OS, then for replication to be successful, the target system must be running the higher version of the OS.
Acquire Source Media before Target Media	When you select this check box, the Plug-in *for Data Copy* tries to acquire the source media before it attempts to acquire the target media for the Data Copy and Duplicate backups.

Option	Description
Maximum Streams for Data Copy	Type or select the maximum number of parallel streams that can be generated for the Data Copy job. By default, a single data stream is generated to copy the data items in a sequential manner.
Media Request Timeout	Type or select the amount of time NetVault waits for the backup media. This timeout value is specified in number of minutes. If the required piece of media is not available within the specified interval, the job is aborted. The default value is 10 minutes. If you set the value to zero (0), the Data Copy job waits indefinitely until the media is provided or the job is manually aborted. The maximum timeout period that can be set is 1440 minutes (24 hours), which ensures that current instance is aborted before NetVault runs the next instance of a Daily job. **NOTE:** The media request timeout for Phase 1 Data Copy jobs (created using the Plug-in *for Data Copy*) is controlled by the **Media Request Timeout** setting in the Backup Options Set; it is not controlled by the **Media Request Timeout** setting in the Target Set. The media request timeout for Phase 2 (Secondary Copy) Data Copy and Duplicate jobs is controlled by the **Media Request Timeout** specified in the Backup Advanced Options Set
Run data copy on client	By default, the Data Copy job runs on the NetVault Server. To run the job on a different NetVault machine, select the client in the list.

d Under **Backup Life**, configure the following options.

Option	Description
Use originals life	To use the original saveset's retention period, select this option. **NOTE:** If the original saveset is immutable, then the Data Copy is also immutable for the same period for time. **NOTE:** If the primary backup is Immutable, to make the duplicate backup, immutable, select **Use 'Backup Life' on the 'Advanced Options' tab**. **NOTE:** If you select the **Duplicate a backup,** for which duplicated incremental backups need their original full backup for restore, and the **Use originals life** options, then the duplicate will not be immutable.
Use 'Backup Life' on 'Advanced Options' tab	To set a different retention period for the data copy, select this option, and then specify the retention period in the Backup Advanced Options set. For more information about these options, see the *Quest NetVault Administrator's Guide*.

e The **Snapshot Options** can be used with the Data Copy method (**Copy a full backup to produce a new independent copy of the data** option).

When creating a copy of a backup that uses persistent snapshots, you can configure the Plug-in for Data Copy to create a saveset copy on the disk- or tape-based storage device, and optionally retain references to the original snapshots or remove the references.

Option	Description
Remove snapshot reference	Use this option to create a copy of the saveset without including any references to the original snapshots.
Keep snapshot reference	Use this option to create a copy of the saveset and include references to the original snapshots in the backup index. When restoring data from a copy, the plug-in tries to mount and restore data from the snapshots. When such copies are used to restore data, the plug-ins try to restore data from the original snapshots; the copy stored on the storage media is used only if the snapshots are unavailable.

f To run multi-stream jobs, configure the following options.

The **Snapshot Options** are ignored if the saveset selected for Data Copy does not have any associated snapshots. These options are not available for Phase 2 Data Copy backups.

Option	Description
Maximum Streams for Data Copy	Type the maximum number of parallel streams that can be generated for the Data Copy job.
Media Request Timeout	Type or select the amount of time NetVault waits for the backup media. This timeout value is specified in number of seconds. If the required piece of media is not available within the specified interval, the job is aborted. The default value is 10 minutes. If you set the value to zero (0), the Data Copy job waits indefinitely until the media is provided or the job is manually aborted. The maximum timeout period that can be set is 1440 minutes (24 hours), which ensures that current instance is aborted before NetVault runs the next instance of a Daily job. **NOTE:** The media request timeout for Phase 1 Data Copy jobs (created using the Plug-in for Data Copy) is controlled by the **Media Request Timeout** setting in the Backup Options Set; it is not controlled by the **Media Request Timeout** setting in the Target Set. The media request timeout for Phase 2 (Secondary Copy) Data Copy and Duplicate jobs is controlled by the **Media Request Timeout** specified in the Backup Advanced Options Set.

g Click **Save**, and in the **Create New Set** dialog box, type a name for the set. Click **Save** to close the dialog box.

5 Select or create the Schedule Set, Source Set, Target Set, and Advanced Options Set. For more information about these sets, see the *Quest NetVault Administrator's Guide*.

NOTE: When performing Duplicate and Data Copy backups, you cannot use media items that contain the original saveset or a copy of the same backup. NetVault excludes these media items to ensure that copies and original backup do not exist on the same media item.

The concept of media does not apply to disk-based devices. If the original saveset is stored on a disk-based device, NetVault does not exclude that device when you run a Duplicate or Data Copy job for that backup.

NOTE: When performing multi-stream backups, do not select the **Ensure backup is the first on the target media** check box. If you select this check box for multi-stream backups, each data stream targets a separate piece of media to exist as the first backup on the media item. Thus, if a backup generates five streams, the job tries to obtain five blank or new media items.

This option does not apply to disk-based storage devices.

6 To submit the job for scheduling, click **Save & Submit**. You can monitor the job progress from the **Job Status** page and view the logs from the **View Logs** page.

To save the job definition without scheduling it, click **Save**. You can view, edit, or run this job from the **Manage Job Definitions** page. This job is not displayed on the **Job Status** page until you submit it.

For more information about **Job Status**, **View Logs**, and **Manage Job Definitions**, see the *Quest NetVault Administrator's Guide*.

Important notes

- Data Copy or Duplicate of a persistent snapshot only backup, copies only the index and does not create the redundant copy of the data.

- When you create a Data Copy of any backup sequence, you must create a copy of each backup in the sequence to maintain data integrity of the copy. If you try to create a copy of an Incremental Backup without creating a copy of the original Full Backup or previous Incremental Backup, the job reports the following error and fails:

  “Cannot DataCopy this incremental as the previous DataCopied backup it depends on is missing. Please ensure the entire series has been DataCopied.”

  NOTE: Data Copy of a Continuous Data Protection (CDP) for VMWare saveset can be created independent of previous Incremental Backups.

- The Plug-in *for FileSystem* supports two types of Incremental Backups: Regular Incremental Backups and Dump Type Incremental Backups.
  - Regular Incremental Backups are linked to the initial Full Backup and the previous Incremental Backups. Before creating a Data Copy of a regular Incremental Backup, you must have created a copy of the initial Full Backup and the previous Incremental Backups in the backup sequence. Otherwise, the plug-in reports an error.
  - Dump Type Incremental Backups are standalone Incremental Backups. You can copy these backups without creating a copy of any other backup in the backup sequence.
- The Advanced Backup Option **Enable Encryption** can be used only with the **Copy a full backup to produce a new independent copy of the data** option.

  NOTE: This option does not apply to continuous data protection (CDP) backups.

  If the primary copy is encrypted, the Data Copy method automatically creates an encrypted saveset whether you select the **Enable Encryption** check box or not. Therefore, this option is only useful when you want to create an encrypted secondary copy from an unencrypted primary copy.

  Encrypted primary backups are not encrypted again if you select the **Enable Encryption** check box.

  To restore data from an encrypted Data Copy, you must use the primary copy’s Encryption Key
- The option **Automatically get a set's last full backup** is incompatible with the backups performed using NetVault Plug-in *for NetWare*. The Plug-in *for Data Copy* creates a copy of the last backup regardless of its type (Full or Incremental).
- The Plug-in *for Data Copy* cannot distinguish between the NDMP Level 0 Full Backup and Levels 1–9 Incremental Backups. An NDMP backup of any level appears as Full Backup to the Plug-in *for Data Copy*. So, if you are trying to make a copy of the latest saveset, and you have selected the options **Copy a full backup to produce a new independent copy of the data** and **Automatically get a set's last full backup**, the Plug-in *for Data Copy* still creates a copy of the last backup (of any level). It does not create a copy of the Level 0 backup for that Backup Selection Set.
- On NetVault Server 10.0.5 and later, the Plug-in *for Data Copy* creates index version 4, which is incompatible with earlier versions of NetVault. A client running NetVault 10.0.1 or an earlier version cannot read these index files. To restore Data Copy savesets generated from NetVault Server 10.0.5 or later, the client must also be running NetVault 10.0.5 or later.
- For Data Copy backups with the **Duplicate a backup** option selected, if the **Verify After Backup** option is also selected, then backup verification occurs on the streams written to the media in either the source media of the Data Copy duplicate or the target media of the Data Copy duplicate.
  - Data Copy backups with the **Duplicate a backup** option does not create a separate backup saveset; it creates redundant data streams within the existing backup saveset. During the **Verify** phase for each data stream, either the copy in the source media or the copy in the target media would be verified. To configure additional backup job options, see “Specifying additional options” in the *Quest NetVault Administrator’s Guide.*
- For Data Copy backups where the **Copy a full backup to produce a new independent copy of the data** and **Verify After Backup** options are selected, the Verify phase performs verification of the streams written to the media in both the source media of the Data Copy backup and the target media of the Data Copy backup.

- Data Copy backups where **Copy a full backup to produce a new independent copy of the data** is selected, creates a separate backup saveset of the data. When the **Verify After Backup** option is also selected, verification occurs on all of the data streams, including data streams in the source media and the target media of the Data Copy backup. To configure Additional backup job options see, “Specifying additional options” in the *Quest NetVault Administrator’s Guide.*

Restoring a Data Copy

For a restore job, you can use either the original saveset or a Data Copy. The procedure for restoring data is the same for the original saveset and the data copy saveset, and depends on the plug-in used to create the original saveset. For information about restoring the data, see the relevant plug-in user’s guide.

4

Using *Plug-in for Encryption*

- About Plug-in for Encryption
- Encryption strategy overview
- Configuring default settings
- Encrypting all backups
- Performing job-level encryption
- Troubleshooting

About Plug-in *for Encryption*

NetVault offers four encryption options:

- **CAST128:** CAST-128 is a 12- or 16-round Feistel network with a 64-bit block size and a key size of between 40 to 128 bits, but only in 8-bit increments.
- **CAST256:** CAST-256 uses the same elements as CAST-128, but it is adapted for a block size of 128 bits — twice the size of its 64-bit predecessor. Acceptable key sizes are 128, 160, 192, 224 and 256 bits. CAST-256 is composed of 48 rounds, sometimes described as 12 “quad-rounds”, arranged in a generalized Feistel network.
- **AES256:** Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. The standard consists of three block ciphers, AES-128, AES-192, and AES-256. Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. When you select the AES256 option, the plug-in uses a FIPS compliant AES-256 encryption algorithm to encrypt backups.
- **AES256_OLD:** Select this option for the plug-in to use the non FIPS compliant AES-256 encryption algorithm to encrypt backups, specifically when FIPS compliance is not a requirements for your backups and you prefer using the non FIPS compliant AES-256 algorithm to benefit backup speeds.

NOTE: The CAST-128 and CAST-256 encryption algorithms do not comply with the requirements of the United States Federal Information Processing Standard (FIPS). These algorithms are provided for the restoration of legacy data. The option AES256_OLD provides an AES-256 encryption algorithm that is non FIPS compliant. To instruct NetVault Plug-in *for Encryption* to use the FIPS compliant AES-256 algorithm, use the AES256 option.

These options encrypt and transfer data across the network to the backup device, where the data remains encrypted until restored to the client. If encryption is only required for secondary storage, job-level encryption offers the choice of encrypting only the secondary copy while the primary backup remains unencrypted to shrink the backup window. When using disk-based storage devices, job-level deduplication allows you to separate deduplicated from non deduplicated unencrypted data for optimal deduplication ratios and performance.

For a list of NetVault Plug-ins that are incompatible with the Plug-in *for Encryption*, see the respective release notes.

Encryption strategy overview

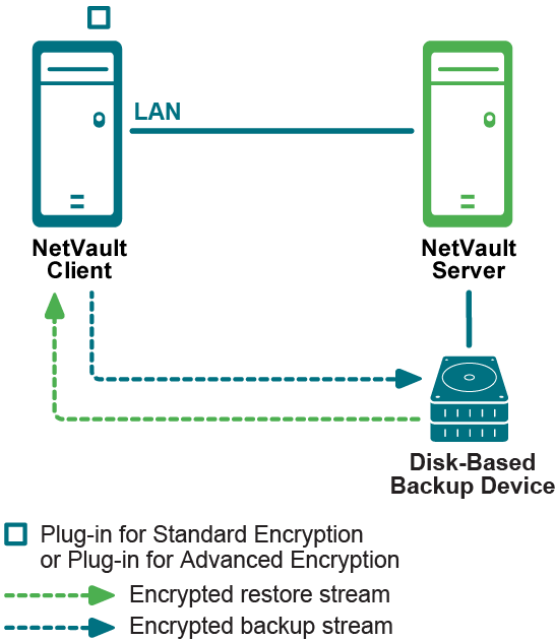
When defining an encryption strategy, you must determine the following:

- Which backups are encrypted.
- Which encryption algorithm is required.
- Whether encryption is required for primary backups or secondary backups.
- Whether encryption is enabled for all backups or on a per-job basis.

Selecting which backups to encrypt

NetVault performs software-based encryption. The backup stream is encrypted using the selected algorithm by the NetVault Server or Client for which the plug-in is enabled. The encrypted data stream is transferred over the network to the backup device where it remains encrypted. During restore, the encrypted backup is transferred from the backup device to the targeted NetVault Client, where the plug-in completes the decryption.

Figure 1. Encrypted backup and restore path



The backup encryption and decryption processes are performed by the plug-in on the NetVault Server or Client. These processes use resources on the machine. The encryption process lengthens the time it takes to perform backups, while the decryption process lengthens the time it takes to perform restores. The impact to the performance of the client, backup window, and restore time should be considered when deciding which backups must be encrypted. In summary, backups should only be encrypted when security requirements outweigh the impact to performance, backup windows, and restore times.

Selecting the encryption algorithm

NetVault provides multiple algorithms that can be used to encrypt and decrypt backups. While each NetVault Client can use a different encryption algorithm, all backups from a particular client must use the same algorithm.

The same encryption algorithm that was used during backup must be used during restores. It is possible to use a different algorithm from this point forward than was previously used. However, when restoring backups that used the previous algorithm, the NetVault Server or Client must be configured to specify the algorithm used by the

backup to restore data successfully. For example, if previous backups used the CAST-128 algorithm while current backups are using the AES-256 algorithm, the plug-in must be configured on the server or client to use the CAST-128 algorithm when restoring a backup that was taken using that algorithm; otherwise, restore fails.

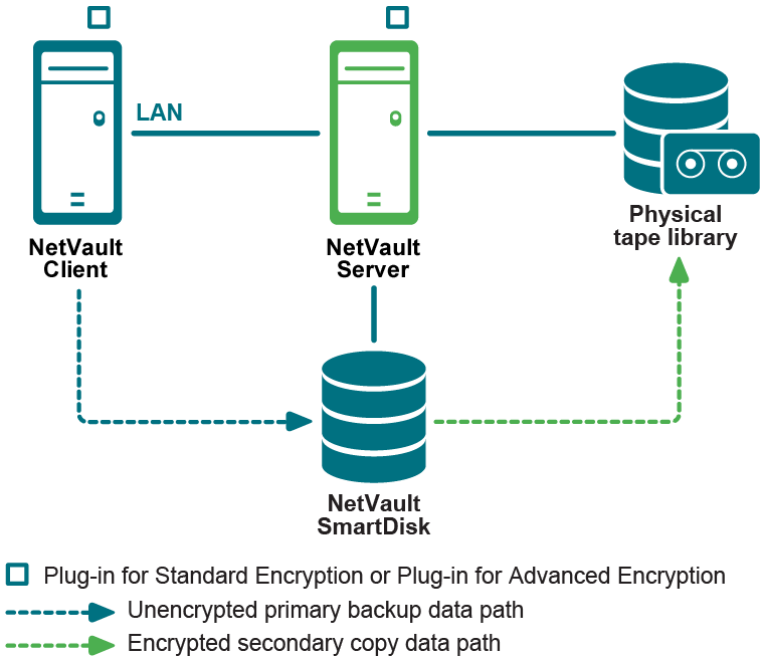
Encrypting primary or secondary backups

A backup job consists of one or optionally two phases—Primary Backup and Secondary Copy. The primary backup is the backup of data stream to the selected backup device. These backups are performed to local storage devices to enable faster restores. The Secondary Copy is a Duplicate or Data Copy of the primary backup to a different backup device. These backups are targeted to remote disk-based storage devices or physical tape libraries whose tapes are stored offsite for disaster recovery purposes.

Your security requirements dictate whether you require encryption for both the primary backups and the secondary copies. For example, if the security requirements dictate that only the backups that leave the corporate network require encryption (such as those backups stored on physical tapes in a remote location), encrypt the secondary copy backups that target the physical tape libraries. However, if the security requirements dictate that data must be encrypted while it transfers across the network or while it is stored on a disk-based backup device—even if the disk-based backup device is located within the corporate network—encrypt both the primary backup and secondary copy.

Encrypted data does not deduplicate well. Therefore, encrypting only the secondary copy backup is beneficial when the primary backups are performed to storage devices that support deduplication. This approach lets you take advantage of both encryption and deduplication by deduplicating the primary backup and encrypting the secondary copy.

Figure 2. Unencrypted primary backups and encrypted secondary copy backups



Encrypting all or specific backups

The Plug-in *for Encryption* lets you enable encryption for all backups on the NetVault Server or Client where a plug-in is installed, or enable encryption only for specific jobs. Encryption can also be enabled only for the primary backup or the secondary copies. This approach lets you take advantage of both encryption and deduplication. For example, you can deduplicate the primary backup and encrypt the secondary copy.

The job-level encryption option can be used in the following situations:

- When any plug-in installed on the server or client is incompatible with the Plug-in *for Encryption*.
- Only specific backups on the server or client require encryption.
- Primary backups do not require encryption while secondary backups for offsite protection require encryption.
- Primary backups are targeted to storage devices that support deduplication.

The NetVault Server and Client should only be configured to encrypt all its backups in the following situations:

- All plug-ins installed on the server or client are compatible with the Plug-in *for Encryption*.
- All backups from the server or client require encryption.
- Both primary and secondary backups require encryption.
- Backups are not selected for deduplication.

Configuring default settings

The settings let you determine which backups to encrypt, set your encryption key, and select the algorithm to use.

Encryption algorithm options are configured for each NetVault Client and for the NetVault Server separately. When you configure Encryption on a NetVault Client or in the NetVault Server, the encryption algorithm options available for the running version of NetVault appear.

To configure default settings

1. In the Navigation pane, click **Change Settings**.
2. On the **Configuration** page, click **Server** or **Client Settings**, as applicable.
3. Under **Plugins**, click **Encryption**.
4. Configure the following settings.

Setting	Description
Encrypt ALL Backups on this Client	After the Plug-in *for Encryption* is automatically installed with NetVault on a client, you can do either of the following: • Encrypt all backups performed for that client. • Encrypt specific backups performed for that client. To enable encryption for all backups, select this check box. When you enable encryption for all backups, you cannot change the setting on a per-job basis. For more information about enabling encryption for specific backups, see Performing job-level encryption. **NOTE:** To perform job-level encryption for backups originating from a NetVault Server or Client, the plug-in should not be configured for encrypting all backups.
Encryption Key String	Type the string that serves as the encryption key for the NetVault machine. Different platforms allow varying characters and password lengths. Quest recommends that you use passwords of 32 characters or less. You can use characters from the following set: “A–Z”, “a–z”, “0–9”, and “_”. Key strings that do not conform to these specifications may work on one platform but may be invalid in another environment.

Setting	Description
Confirm	Re-type the encryption string here to confirm that it is correct.
Available Encryption Algorithms	Select the encryption algorithm that you want to use for backups and restores. The list includes the following options: • AES256_OLD (non FiPS compliant) • AES256 (FIPS compliant) • CAST256 CAST128 **NOTE:** For NetVault Clients version 13.0 and earlier, when you select the AES256 option, the built-in NetVault Plug-in *for Encryption* uses a non FIPS compliant AES-256 encryption algorithm. For NetVault Clients version 13.0 and earlier, the built-in NetVault Plug-in *for Encryption* does not include a FIPS compliant encryption algorithm option. **NOTE:** For NetVault Clients version 13.0.1 and version 13.0.2, the AES256 option instructs the built-in NetVault Plug-in *for Encryption* to use a FIPS compliant encryption algorithm. For NetVault Clients version 13.0.1 and version 13.0.2, the AES256_OLD (non FIPS compliant) option is not available in the built-in NetVault Plug-in *for Encryption*. If you are managing a NetVault Client version 13.0.1 or version 13.0.2 and prefer to use the non FIPS compliant AES-256 encryption algorithm, see the troubleshooting section of this guide for details about Enabling non FIPS encryption algorithm on NetVault Clients version 13.0.1 and 13.0.2.

5 To apply the new settings and close the dialog box, click **Apply**.

NOTE: An encrypted backup performed by a plug-in can be restored to either its original location or to a new target machine. In either event, the plug-in must be installed on the target machine and it must be configured as it was when the backup was performed—using the same **Encryption Key String** and **Encryption Algorithm**.

Encrypting all backups

If encryption is enabled for all backups performed from a particular NetVault Client, there are no additional requirements for encrypting backups. For more information about the backup and restore procedures, see the user's guide for the relevant plug-in.

Performing job-level encryption

The job-level encryption option can be used to encrypt the primary backup, secondary copy, or both. Encrypting both the primary backup and secondary copy is beneficial when security requirements dictate that the backup must be encrypted while it transfers across the network or while it is stored on a disk-based backup device even if the disk-based backup device is located within the corporate network.

The job-level encryption setting is specified in the Backup Advanced Options Set. For more information about creating an Advanced Options Set for a backup job, see the *Quest NetVault Administrator's Guide*.

Encrypting primary backup

To enable job-level encryption for a primary backup:

1 Start the Backup Job Wizard, and open the **Advanced Options** page.

For more information, see the *Quest NetVault Administrator's Guide*.

2 Click **Additional Options**.

3 In the **Additional Options** dialog box, select the **Enable Encryption** check box.

Encrypting a Secondary Copy

NetVault offers the following methods for creating Secondary Copies:

- **Duplicate:** The Duplicate method creates an exact copy which is linked to the original backup. This method breaks down the backup into segments and copies the segments to the storage device. During restore, the segments from the primary backup and secondary copy are interchangeable. As it is not possible to mix unencrypted segments with encrypted segments during restore, you cannot enable or disable encryption for the Duplicate. If the original saveset is encrypted, the Duplicate method creates an encrypted copy. If the original saveset is not encrypted, this method creates an unencrypted copy.
- **Data Copy:** The Data Copy method breaks down the backup into segments and copies the segments to the backup device. During restore, either the primary backup or the secondary copy is used to recover data; the segments from the primary backup and secondary copy are not interchangeable. Therefore, it is possible to enable encryption for the Data Copy when the primary copy is unencrypted. This option is useful when you want to use the deduplication option for primary backups.

To enable job-level encryption for a Secondary Copy:

1 Start the Backup Job Wizard, and open the **Advanced Options** page.

For more information, see the *Quest NetVault Administrator's Guide*.

2 Click **Secondary Copy**.

3 In the **Secondary Copy** dialog box, select the **Create Secondary Copy** check box.

4 Select the **Encrypt Secondary Copy Only** check box.

This option can only be used with the Data Copy method.

IMPORTANT:

- If the primary copy is encrypted, the Data Copy method automatically creates an encrypted saveset whether you select the **Encrypt Secondary Copy Only** check box or not. Therefore, this option is only useful when you want to create an encrypted secondary copy from an unencrypted primary copy.
- Encrypted primary backups are not encrypted again if you select the **Encrypt Secondary Copy Only** check box for a Data Copy.
- To restore data from an encrypted Data Copy, you must use the primary copy's Encryption Key.

Troubleshooting

This section describes some common issues and their solutions. It includes the following topic:

- Backups and Restores using AES-256 encryption algorithm are noticeably slower for NetVault Clients version 13.0.1 and 13.0.2 (Enabling non FIPS encryption algorithm on NetVault Clients version 13.0.1 and 13.0.2)

Backups and Restores using AES-256 encryption algorithm are noticeably slower for NetVault Clients version 13.0.1

and 13.0.2 (Enabling non FIPS encryption algorithm on NetVault Clients version 13.0.1 and 13.0.2)

Description

The built-in NetVault Plug-in *for Encryption* in NetVault 13.0.3 onward includes a FIPS compliant AES-256 option and a non FIPS compliant AES-256 option.

With NetVault 13.0 and earlier, the built-in NetVault Plug-in *for Encryption* uses an AES-256 encryption algorithm that is non FIPS compliant.

With NetVault 13.0.1, and NetVault 13.0.2 the NetVault Plug-in *for Encryption* uses an AES-256 encryption algorithm that is FIPS compliant. There is no non FIPS compliant AES-256 option. Backups and restores performed using AES-256 FIPS compliant algorithm are noticeably slower than backups and restores performed using the AES-256 non FIPS compliant encryption algorithm.

Symptom

With NetVault 13.0.1 and NetVault 13.0.2, backups and restores are noticeably slower with the AES256 encryption option set. The built-in NetVault Plug-in *for Encryption* is set to use a FIPS compliant AES-256 algorithm.

Solution

If FIPS compliance is not a requirement for your backups, and you would prefer to use non FIPS compliant AES-256 algorithm in the benefit of backup speeds, then you can modify NetVault Plug-in *for Encryption* to use a non FIPS compliant AES-256 encryption algorithm. For each NetVault Client for which you want to use the non FIPS compliant AES-256 encryption algorithm, completethe following steps.

1. In the NetVault Client, navigate to the directory where NetVault software is installed
2. Navigate to the NetVault config directory
3. Use a text editor to edit the NetVault config file **encryption.cfg**
4. Search for the stanza `[Client:Crypto Algorithm]`, and add an entry for `AES256_OLD`
5. After adding the entry, the stanza should look as follows:

```
[Client:Crypto Algorithm]
Type=Combo
Width=24
Label=Available Encryption Algorithms
Help=Please select an Encryption Algorithm
Help Id=0
Value=AES256_OLD
Range=No module selected,AES256,CAST128,CAST256,AES256_OLD
Label Id=7047
```

6. Save the changes
7. After saving the changes in the NetVault **encryption.cfg** config file, restart NetVault services on the NetVault Client

   After restarting NetVault services on the Client, NetVault Plug-in *for Encryption* will be set to use the non FIPS compliant AES-256 encryption algorithm. When modifying encryption options, the algorithm list will let you choose between CAST128, CAST256, AES256 (FIPS compliant), and AES256_OLD (non FIPS compliant).

NOTE: Encryption is configured in the NetVault Clients. Apply the described settings for all the NetVault version 13.0.1 and NetVault version 13.0.2 Clients for which FIPS compliant backups is not a requirement, and you choose using a non FIPS compliant AES-256 encryption algorithm in the benefit of backup speeds.

5

Using Plug-in *for Databases*

- Configuring default settings
- Backing up the NetVault Database
- Restoring NetVault Database

Configuring default settings

To configure the default settings for Plug-in for Databases:

1 Start the Backup Job Wizard, and click **Create New** next to the **Selections** list. Open the NetVault Server or Client node. Select **NetVault Databases** and click **Configure**.

You can also configure the default settings from the **Change Settings** page. In the Navigation pane, click **Change Settings**. On the **Configuration** page, click **Server Settings**, and then on the **NetVault Server Settings** page, click **Plugin Options**.

2 Under **NetVault Database Backup**, configure the following settings.

Option	Description
Minimum free space on database device before warning is output	This setting specifies the minimum amount of free disk space required on the drive or partition on which the **db** directory resides. By default, it is set to 20 percent of the total size of the NetVault Database. To change this limit, type or select a new value. If the available free space falls below the specified level, the plug-in logs a warning message.
Minimum free space on logs device before warning is output	This setting specifies the minimum amount of free disk space required on the drive or partition on which the **logs** directory resides. By default, it is set to 10 percent of the total size of the log files. To change this setting, type or select a new value. If the available free space falls below the specified level, the plug-in logs a warning message.

Option	Description
Minimum free space on reports device before warning is output	This setting specifies the minimum amount of free disk space required on the drive or partition on which the **reports** directory resides. By default, it is set to 10 percent of the total size of the Reports Database. To change this setting, type or select a new value. If the available free space falls below the specified level, the plug-in logs a warning message.
Format to be used while backing up NetVault Database	The NetVault Database backups can be generated in **tar** and **custom** formats. By default, the plug-in uses the **custom** format. The **tar** format has the following limitations: • It requires a large amount of disk space to store temporary files during backup. The backup could fail if the **tmp** directory in the NetVault installation directory does not have sufficient space to store the files. • It has a table size limit of 8GB. Database tables that are larger than 8GB in size cannot be backed up using this format.

3 Click **OK** or **Apply** to save the settings.

Backing up the NetVault Database

To safeguard your NetVault Server, you must perform regular backups of the NetVault Database. The NetVault Database backup allows you to recover the NetVault Server in the event of a disaster. You can schedule a daily backup of the NetVault Database after all other jobs have completed. Make sure that you use specific media or media group for these backups.

NOTE: To avoid database inconsistency or job failure, you must not perform the following activities together:

- NetVault Database backup
- Execution of a job
- Media scan

To back up the NetVault Database:

1 In the Navigation pane, click **Create Backup Job**.

You can also start the wizard from the Guided Configuration link. In the Navigation pane, click **Guided Configuration**, and then on the **NetVault Configuration Wizard** page, click **Create Backup Jobs**.

2 In **Job Name**, specify a name for the job. Assign a descriptive name that allows you to easily identify the job for monitoring its progress or restoring data.

A job name can contain alphanumeric and non-alphanumeric characters, but it cannot include non-Latin characters. There is no length restriction. However, a maximum of 40 characters is recommended on all platforms.

3 In the **Selections** list, select an existing Backup Selection Set, or complete the following steps to create a set.

a Click **Create New** to open the **NetVault Selections** page.

b Open the NetVault Server node, and in the list of plug-ins, open **NetVault Databases**.

c Select the **NetVault Database** node.

d Click **Save**, and in the **Create New Set** dialog box, type a name for the set. Click **Save** to close the dialog box.

> **NOTE:** A set name can contain alphanumeric and non-alphanumeric characters, but it cannot include non-Latin characters. On Linux OS, the names can have a maximum of 200 characters. On Windows OS, there is no length restriction. However, a maximum of 40 characters is recommended on all platforms

4 In the **Plugin Options** list, select an existing Backup Options Set, or complete the following steps to create a set.

   a Click **Create New** to open the **NetVault Database Backup Options** page.

   b Configure the following setting:

   - **Check Database Tables before Backup:** This option can be used to verify the structural, entity, and referential integrity for the Scheduler and Media databases before the backup. It generates a warning or error log if any inconsistency is detected during the process.

     This option is selected by default.

   - **Exclude the Online Indexes during backup**: This option can be used to exclude the online backup indexes (backup indexes stored on the local filesystem) from the NetVault database backup to complete the NVDB backup in the required backup window.

     This option is disabled by default.

   - **Exclude the Catalog database during backup**: This option can be used to exclude the catalog search database from the NetVault database backup to complete the NVDB backup in the required backup window.

     This option is disabled by default.

   c Click **Save**, and in the **Create New Set** dialog box, type a name for the set. Click **Save** to close the dialog box.

5 Select or create the Schedule Set, Target Set, and Advanced Options Set. For more information about these sets, see the *Quest NetVault Administrator's Guide*.

6 To submit the job for scheduling, click **Save & Submit**. You can monitor the job progress from the **Job Status** page and view the logs from the **View Logs** page.

   To save the job definition without scheduling it, click **Save**. You can view, edit, or run this job from the **Manage Job Definitions** page. This job is not displayed on the **Job Status** page until you submit it.

   For more information about **Job Status**, **View Logs**, and **Manage Job Definitions**, see the *Quest NetVault Administrator's Guide*.

Restoring NetVault Database

You can restore a NetVault Database backup to:

- Recover a NetVault Server.
- Migrate the NetVault system to a new machine.
- Migrate the system settings during NetVault upgrade.

This procedure for restoring a NetVault Database backup includes the following steps:

- Prerequisites
- Restore Procedure

Prerequisites

Before you start the restore procedure, verify that the following requirements are met:

- Install the NetVault Server on the target system. The software version must be the same as the original server.
- Add a backup device to the NetVault Server. For more information about this procedure, see the *Quest NetVault Administrator's Guide*.
- Load the backup media. In the new NetVault Domain, the media are marked as "foreign." You must scan the media to load the contents. For more information about this procedure, see the *Quest NetVault Administrator's Guide*.
- When importing and restoring NetVault Database backups to an alternate backup server, the alternate NetVault Server must have the same NetVault Machine Name as the original server that performed the backups.
- It is recommended to install and enable the catalog search before restoring a NetVault Database backup that includes the catalog search database (in case of a fresh NetVault installation or if the catalog search had previously been installed and then uninstalled).

  NOTE: The installation and configuration of the catalog search are performed separately from the rest of the NetVault Database, even though the catalog search database is included in the NetVault Database backup. Hence, the current state (Enable or Disable) and configuration of the catalog search are not changed during a NetVault Database restore.

Restore Procedure

To restore a NetVault Database backup:

1 In the Navigation pane, click **Create Restore Job**.

On the **Create Restore Job — Choose Saveset** page, the saveset table provides a list of available savesets. The table shows the saveset name (Job Title and Saveset ID), creation date and time, saveset size, and saveset status.

The saveset status is indicated using the following icons.

Icon	Description
	Saveset is online (all segments are online).
	Saveset is partially online (some segments are online).
	Saveset is offline (all segments are offline).

The saveset list is sorted alphabetically by saveset name. You can sort the list by a different column or reverse the sort order by clicking the column heading. The arrowhead next to the column name indicates the sort order.

You can click **Load more** to load the next set of records, if available. Each load action fetches a maximum of 5000 records. This button is disabled if there are no more records to load.

By default, the table is sorted by creation date and time. You can sort the table by one or more columns, as required.

NetVault web application supports multiple-column sorting for the tables. However, the first sorted column takes the highest precedence over the sorting of other columns. For example, if the table is sorted by the 'Start Time' as the primary sort, selecting sort options on the 'ID/ Instance/ Phase' column does not affect the list order.

To sort by a column, click the column header; to change the sort direction, click the column header again. Repeat this step for other columns by which you want to sort the table.

The arrowhead next to the column name indicates the sorting order (up for ascending order and down for descending order). A blue arrowhead is used to indicate the sort order for the primary column.

To remove a sort, click the column header for the corresponding column until the arrowhead is no longer displayed.

To choose the following actions in a column, click the column menu:

Option	Description
Sort Ascending	Sorts the column in ascending order.
Sort Descending	Sorts the column in descending order.
Columns	Select/ clear to show/ hide the required column (s).

To set the filter options, view the page size setting, sorting order in the table, export the records, or edit table settings, click the icons at the lower- right corner of the table.

For more information, see the section 'Customizing tables in NetVault WebUI' in the *Quest NetVault Administrator's Guide.*

2 Select the saveset that you want to use, and click **Next**.

When you select a saveset, the following details are displayed in the **Saveset Information** area: Job ID, job title, tag, server name, client name, plug-in name, saveset date and time, retirement setting, Incremental Backup or not, archive or not, and saveset size.

3 On the **Create Selection Set** page, select the database components to recover the full database or parts of it.

Component	Description
Auditor Database	Restores the Auditor Database. This database contains the audit logs for the NetVault system.
Backup Catalog	Restores the catalog search database. To restore only the NetVault Database backup without catalog search database, do not select the option 'Backup Catalog' on the **Create Selection Set** page. To restore the NetVault Database backup with catalog search OR to restore only catalog search database, select the option 'Backup Catalog' on the **Create Selection Set** page. **NOTE:** If "Exclude the Catalog database during backup" option is enabled during NVDB backup, then the "Backup Catalog" option is not shown in the list of components for restore on the **Create Selection Set** page for restore.
Backup Indexes	Restores backup indexes. Backup indexes contain the list of backed up items and their references. Each index is assigned a saveset number. Backup indexes are stored on the backup media and the disk as part of the Media Database. The indexes provide the position of the individual backed up items so that they can be recovered from the backup media. Backing up the indexes on the media ensures that the content of each saveset is available to view when required, in case the index files are deleted or retired from the Media Database. You can scan the backup indexes from the archived media, after they have retired or deleted from the NetVault Database. **NOTE:** If "Exclude the Online Indexes during backup" option is enabled during NVDB backup, then the "Backup Indexes" option is not shown in the list of components for restore on the **Create Selection Set** page for restore.
Cluster	Restores cluster-specific configuration and associated client information
Configuration	Restores configuration files and settings for the.server and client systems, including network access and configuration information for the plug-ins.

Component	Description
Deployment Manager	Restores deployment-related information, such as package stores, task details, status, and schedules. **NOTE:** If you do not select this component, details related to the deployment are not restored and are lost.
General Reports Files	Restores the files included in the Reporting system.
Licenses	Restores licenses to permit the continued operation of NetVault and the licensed plug-ins. If the NetVault server has a machine-tied license and the machine where restore is been performed has a different machine ID, then you must obtain and install the new machine-tied license file manually.
Logs	Restores NetVault Logs, which include all messages from the Server and Client machines. It allows you to check the activity of NetVault at a particular point in time.
Media Manager	Restores the Media Database, which contains records of all active media, the contents of all backups, how backups are organized, and where they are located.
Schedule Manager	Restores the Schedule Database. This database contains records of all defined jobs, backup policies, scheduled jobs, and job history, including when jobs last ran and what backups were produced.
Scripts	Restores system-defined and user-defined scripts for NetVault.

NOTE: Selecting individual components to restore parts of a NetVault Database backup can introduce inconsistencies in the database.

4 On the **Create Selection Set** page, click **Edit Plugin Options**.

5 Configure the following option:

- **Blank reports database tables before restore:** By default, the existing data in the reports database is deleted when you restore the NetVault Database. If you want to retain the existing data in the reports data, clear this check box.

Click **OK** to save the settings, and then click **Next**.

6 On the **Create Restore Job** page, specify a name for the job. Assign a descriptive name that allows you to easily identify the job for monitoring its progress.

A job name can contain alphanumeric and non-alphanumeric characters, but it cannot contain non-Latin characters. There is no length restriction. However, a maximum of 40 characters is recommended on all platforms.

7 In the **Target Client** list, the client from which data was backed up is selected by default. Do not change this setting.

8 Select or create the Schedule Set, Restore Source Set, and Advanced Options Set. For more information about these sets, see the *Quest NetVault Administrator's Guide*.

9 Click **Submit** to submit the job for scheduling.

IMPORTANT: After submitting the restore job, close the WebUI. Do not try to monitor the job status while the job is running.

After the restore job completes, the NetVault Service is stopped. You must manually restart the service from the Txtconfig or the command-line interface.

NOTE: To ensure that the catalog search and postgres databases are in sync after NVDB restore, you must select the "Add pre-existing backups to catalog" option on the **Catalog Search Configuration** page.

6

Using Plug-in *for Raw Devices*

- Backing up raw devices
- Restoring a raw device backup
- Relocating data to an alternate disk or partition
- Restoring data to an alternate NetVault Client

Backing up raw devices

The procedure for backing up raw devices includes the following steps:

- Prerequisites
- Backup procedure

Prerequisites

Before you start the backup procedure, verify that the following requirements are met:

- **Linux and UNIX systems:**
  - Unmount the file system on the disk that you want to back up.
- **Windows systems:**
  - Ensure the disk that you want to back up is not in use.
  - Close all explorer windows.
  - Stop the Disk Management Utility if it is running.

NOTE: On Windows, the Plug-in *for Raw Devices* cannot be used to back up GPT (GUID Partition Table) style partitions. The plug-in can only be used to back up MBR (Master Boot Record) style partitions.

On Linux, the Plug-in *for Raw Devices* can be used to back up MBR tyle partitions as well as GPT style partitions.

NOTE: Plug-in for *Raw Devices* does not support Dynamic devices.

NOTE: Microsoft has deprecated dynamic disks and does not recommend their usage.

Backup procedure

To back up raw devices:

1 In the Navigation pane, click **Create Backup Job**.

You can also start the wizard from the **Guided Configuration** link. In the Navigation pane, click **Guided Configuration**, and then on the **NetVault Configuration Wizard** page, click **Create Backup Jobs**.

2 In **Job Name**, specify a name for the job. Assign a descriptive name that allows you to easily identify the job for monitoring its progress or restoring data.

A job name can contain alphanumeric and non-alphanumeric characters, but it cannot include non-Latin characters. There is no length restriction. However, a maximum of 40 characters is recommended on all platforms.

3 In the **Selections** list, select an existing Backup Selection Set, or complete the following steps to create a set.

d Click **Create New** to open the **NetVault Selections** page.

a Open the NetVault Server node, and in the list of plug-ins, open **Raw Device**.

b Select the data that you want to back up.

Linux and UNIX (including Mac OS X)

a Open the root directory node to display the directory tree.

b Open the **/dev** node, and select the applicable disk.

c Select the partition device file that you want to back up.

Windows

- **Back Up the Entire Physical Disk:** Select the **Physical Disk <n>** node.
- **Back Up Master Boot Record (MBR) and System Partition:** Open the **Physical Disk <n>** node, and select the **Master Boot Record & System Partition** node.
- **Back Up Individual Partitions**: Open the **Physical Disk <n>** node, and select the **Partition <n>** nodes that you want to back up.

c Click **Save**, and in the **Create New Set** dialog box, type a name for the set. Click **Save** to close the dialog box.

> **NOTE:** A set name can contain alphanumeric and non-alphanumeric characters, but it cannot include non-Latin characters. On Linux OS, the names can have a maximum of 200 characters. On Windows OS, there is no length restriction. However, a maximum of 40 characters is recommended on all platforms

4 In the **Plugin Options** list, select an existing Backup Options Set, or complete the following steps to create a set.

a Click **Create New** to open the **Raw Partitions Backup Options** page.

a Configure the following settings on Windows-based clients:

- **Backup Reported Disk Size:** By default, the plug-in obtains the disk size from the operating system and backs up that amount of data. This option allows you to restore data to any physical disk of the same reported size, even if the actual sizes differ.
- **Backup Entire Contents:** Select this option if the actual and reported disk sizes vary, and you want to back up the entire contents regardless of the reported disk size.

b Click **Save**, and in the **Create New Set** dialog box, type a name for the set. Click **Save** to close the dialog box.

5 Select or create the Schedule Set, Target Set, and Advanced Options Set. For more information about these sets, see the *Quest NetVault Administrator's Guide*.

6 To submit the job for scheduling, click **Save & Submit**. You can monitor the job progress from the **Job Status** page and view the logs from the **View Logs** page.

   To save the job definition without scheduling it, click **Save**. You can view, edit, or run this job from the **Manage Job Definitions** page. This job is not displayed on the **Job Status** page until you submit it.

   For more information about **Job Status**, **View Logs**, and **Manage Job Definitions**, see the *Quest NetVault Administrator's Guide*.

Restoring a raw device backup

The procedure for restoring a Raw Device Backup includes the following steps:

- Prerequisites
- Restore Procedure

Prerequisites

Before you start the restore procedure, verify that the following requirements are met:

- **Restore an entire disk:** Unmount the target disk. Verify that the size of the target disk is equal to or larger than the size of the source disk.
- **Restore an individual partition:** On Windows, verify that the size of the target partition is equal to the size of the source partition. When you restore the data to a partition of a different size, the job completes with the message **"Partition to Restore to a Different Size than the Backed Up Partition."** This type of restore might require reinstallation or reformatting.

  This requirement does not apply to Linux and UNIX systems.

NOTE: The Plug-in *for Raw Devices* cannot be used to perform cross-platform restores. You cannot restore raw device backups of a Windows Client to a Linux Client or raw device backups of a Linux Client to a Windows Client.

Restore Procedure

To restore a raw device backup:

1 In the Navigation pane, click **Create Restore Job**. Complete Step 1 through Step 2 in the section Restore Procedure.

2 On the **Create Selection Set** page, select the disks that you want to restore. Alternatively, open the parent node and select the partitions that you want to restore.

   Click **Save** to save the settings, and then click **Next**.

3 On the **Create Restore Job** page, specify a name for the job. Assign a descriptive name that allows you to easily identify the job for monitoring its progress.

   A job name can contain alphanumeric and non-alphanumeric characters, but it cannot contain non-Latin characters. There is no length restriction. However, a maximum of 40 characters is recommended on all platforms.

4 In the **Target Client** list, the client from which data was backed up is selected by default. Do not change this setting.

5 Select or create the Schedule Set, Restore Source Set, and Advanced Options Set. For more information about these sets, see the *Quest NetVault Administrator's Guide*.

6 Click **Submit** to submit the job for scheduling.

IMPORTANT:

- While restore is in progress, do not access the target drive. If you do so, the job fails and the partition data is corrupted.
- To view the job status, use the NetVault WebUI.
- After a restore completes on a Windows Client, reboot that machine. Do not try to view or browse the restored data until the machine is rebooted.

Additional notes

If you select MBR and one or more partitions for a restore job, the plug-in restores the MBR successfully, but it fails to restore the selected partitions and the jobs completes with warnings ("Failed to get the information of Partition <n> for Disk <n>"). The plug-in is unable to obtain the partition information because the information about the restored MBR has not been updated on Windows.

To restore MBR and one or more partitions, use the following steps:

1. Restore the MBR.
2. Start the Windows Disk Management utility. Use the **Refresh** command to update the MBR information on Windows.
3. Restore the individual partitions.

Relocating data to an alternate disk or partition

To restore a Raw Device Backup without overwriting the existing data, you can relocate the data to an alternate disk or partition on the client. You can also use this procedure if the original disk is unavailable or corrupted.

IMPORTANT:

- On Windows, you can restore the MBR to an alternate disk without recreating the individual partitions.
- You can relocate the MBR to any disk, but it must be copied to partition zero on that disk.
- You can relocate a backup to a designated disk or partition using the disk and partition numbers.

To relocate data to an alternate disk or partition:

1. Start the restore wizard, and select the data that you want to restore. For more information, see steps 1 through 3 in the section Restoring a raw device backup.
2. Select the disk or partition that you want to rename or relocate and click **Rename**.
3. In the **Rename/Relocate** dialog box, provide the following information.
   - **Linux and UNIX:** Type the full path to the new disk.
   - **Windows:** To relocate the data to an alternate disk, type the target disk number. For example, `Disk 1` or `1`.

     To relocate the data to an alternate partition, type the disk number and the partition number. For example, `Disk 1 Partition 4` or `1 4`.

   Click **OK** to close the dialog box.

   After you close the dialog box, the plug-in updates the corresponding node in the selections tree to display the new location for the disk or partition.
4. Complete steps 3 through 7 in the section Restoring a raw device backup.

Restoring data to an alternate NetVault Client

When restoring a Raw Device Backup, you can relocate the data to an alternate client. This procedure can be useful during a server migration or disaster recovery operation.

The procedure for restoring a Raw Device Backup to an alternate client includes the following steps:

- Prerequisites
- Restore procedure

Prerequisites

Before you start the restore procedure, verify that the following requirements are met:

- Install the NetVault Server or Client software on the target system.
- Add the target client to the NetVault Server.

Restore procedure

To relocate data to an alternate client:

1. Complete steps 1 through 4 in the section Restoring a raw device backup.
2. In the **Target Client** list, select the restore target.

   Alternatively, click **Choose**, and in the **Choose the Target Client** dialog box, select the restore target. Click **OK** to close the dialog box.
3. Complete steps 6 and 7 in the section Restoring a raw device backup.

NOTE: You can also use the **Relocate** option while restoring data to an alternate client. For more information about these options, see Relocating data to an alternate disk or partition.

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.