VERITAS™

VERITAS NetBackup™ 5.1 Encryption

System Administrator’s Guide

for UNIX and Windows

N12343C

Disclaimer

The information contained in this publication is subject to change without notice. VERITAS Software Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VERITAS Software Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

VERITAS Legal Notice

VERITAS Software Corporation
350 Ellis Street
Mountain View, CA 94043
USA
Phone 650–527–8000 Fax 650–527–2908
www.veritas.com

Third-Party Copyrights

Contents

Preface v

What Is In This Guide? v

Related NetBackup Manuals v

Glossary vi

Accessibility Features vi

Conventions vi

Chapter 1. Introduction 1

Terminology 1

Technical Overview 3

How a Standard Encryption Backup Works 4

How a Standard Encryption Restore Works 5

How a Legacy Encryption Backup Works 5

How a Legacy Encryption Restore Works 6

Chapter 2. Installation on a Master Server 9

Installation Prerequisite 9

Installing on a UNIX NetBackup Master Server 9

Installing on a Windows NetBackup Master Server 11

Chapter 3. Configuration for Standard Encryption 13

Configuring from the Master Server 13

Pushing NetBackup Encryption Software to Clients 14

Creating the NetBackup Encryption Keyfile on the Clients 15

Best Practices: Key File Restoration 16

Configuring NetBackup Encryption on the Client 16

Obtaining NetBackup Encryption Software 16

Managing NetBackup Encryption Configuration Options 18

Managing the NetBackup Encryption Key File 19

Best Practices: Key File Restoration 19

Redirected Restores of Encrypted Files 20

Setting the Encryption Attribute in NetBackup Policies 21

Changing Client Encryption Settings from the NetBackup Server 21

Chapter 4. Configuration for Legacy Encryption 23

Configuring from the Master Server 23

Read This If Clients Have Not Been Previously Configured 24

Pushing NetBackup Encryption Software to Clients 25

Pushing the NetBackup Encryption Configuration to Clients 26

Pushing Encryption Pass Phrases to Clients 26

Setting the Encryption Attribute in NetBackup Policies 28

Configuring NetBackup Encryption on the Client 28

Obtaining NetBackup Encryption Software 28

Managing NetBackup Encryption Configuration Options 30

Managing the NetBackup Encryption Key File 31

Redirected Restores of Encrypted Files 34

Setting Encryption in NetBackup Policies 34

Changing Client Encryption Settings from the NetBackup Server 35

Additional Key File Security (UNIX clients only) 35

Running bpcd as a Standalone Program 36

Terminating bpcd 38

Index 39

Preface

This guide explains how to install, configure, and use VERITAS NetBackup Encryption. In this publication, VERITAS NetBackup is referred to as NetBackup and VERITAS NetBackup Encryption is referred to as NetBackup Encryption.

This guide is intended for the system administrator responsible for configuring NetBackup Encryption and assumes a thorough working knowledge of NetBackup administration and use.

What Is In This Guide?

- The Introduction chapter is an overview of the product's capabilities.
- The Installation on a Master Server chapter explains how to install NetBackup Encryption.
- The Configuration for Standard Encryption chapter explains how to configure your system to use NetBackup Encryption (128 or 256-bit). This information supplements that in the NetBackup Windows and UNIX system administrator's guides.
- The Configuration for Legacy Encryption chapter explains how to configure your system to use NetBackup Encryption (40 or 56-bit). This information supplements that in the NetBackup Windows and UNIX system administrator's guides.

Related NetBackup Manuals

- *NetBackup System Administrator's Guide for Windows, Volumes I & II*

  Explains how to configure and manage NetBackup on a Windows system.
- *NetBackup System Administrator's Guide for UNIX, Volumes I & II*

  Explains how to configure and manage NetBackup on a UNIX system.
- *NetBackup Commands for Windows*

  Describes NetBackup command use on a Windows system.

- *NetBackup Commands for UNIX*

  Describes NetBackup command use on a UNIX system.

Glossary

If you encounter unfamiliar terminology, consult the NetBackup online glossary. The glossary contains terms and definitions for NetBackup and all additional NetBackup options and agents.

The NetBackup online glossary is included in the NetBackup help file.

▼ To access the NetBackup online glossary

1. In the NetBackup Administration Console, click **Help** > **Help Topics**.

2. Click the **Contents** tab.

3. Click **Glossary of NetBackup Terms**.

Use the scroll function to navigate through the glossary.

Accessibility Features

NetBackup contains features that make the user interface easier to use by people who are visually impaired and by people who have limited dexterity. Accessibility features include:

- Support for assistive technologies such as screen readers and voice input (Windows servers only)
- Support for keyboard (mouseless) navigation using accelerator keys and mnemonic keys

For more information, see the *NetBackup System Administrator's Guide for Windows, Volume I* or the *NetBackup System Administrator's Guide for UNIX*, *Volume I.*

Conventions

The following conventions apply throughout the documentation set.

Product-Specific Conventions

The following term is used in the NetBackup Encryption 5.1 documentation to increase readability while maintaining technical accuracy.

- Microsoft Windows, Windows

  Terms used to describe a specific product or operating system developed by Microsoft, Inc. Some examples you may encounter in NetBackup documentation are, Windows servers, Windows 2000, Windows Server 2003, Windows clients, Windows platforms, or Windows GUI.

  When Windows or Windows servers is used in the documentation, it refers to all of the currently supported Windows operating systems. When a specific Windows product is identified in the documentation, only that particular product is valid in that instance.

  For a complete list of Windows operating systems and platforms that NetBackup supports, refer to the *NetBackup Release Notes for UNIX and Windows* or go to the VERITAS support web site at `http://www.support.veritas.com`.

Typographical Conventions

Here are the typographical conventions used throughout the manuals:

Conventions

Convention	Description
GUI Font	Used to depict graphical user interface (GUI) objects, such as fields, listboxes, menu commands, and so on. For example: Enter your password in the **Password** field.
Italics	Used for placeholder text, book titles, new terms, or emphasis. Replace placeholder text with your specific text. For example: Replace *filename* with the name of your file. Do *not* use file names that contain spaces. This font is also used to highlight NetBackup server-specific or operating system-specific differences. For example: *This step is only applicable for NetBackup Enterprise Server.*
`Code`	Used to show what commands you need to type, to identify pathnames where files are located, and to distinguish system or application text that is displayed to you or that is part of a code example.
Key+Key	Used to show that you must hold down the first key while pressing the second key. For example: Ctrl+S means hold down the Ctrl key while you press S.

You should use the appropriate conventions for your platform. For example, when specifying a path, use backslashes on Microsoft Windows and slashes on UNIX. Significant differences between the platforms are noted in the text.

Tips, notes, and cautions are used to emphasize information. The following samples describe when each is used.

Tip Used for nice-to-know information, like a shortcut.

Note Used for important information that you should know, but that shouldn't cause any damage to your data or your system if you choose to ignore it.

Caution Used for information that will prevent a problem. Ignore a caution at your own risk.

Command Usage

The following conventions are frequently used in the synopsis of command usage.

brackets [ ]

The enclosed command line component is optional.

Vertical bar or pipe (|)

Separates optional arguments from which the user can choose. For example, when a command has the following format:

```
command arg1|arg2
```

In this example, the user can use either the *arg1* or *arg2* variable.

Navigating Multiple Menu Levels

When navigating multiple menu levels, a greater-than sign (>) is used to indicate a continued action.

The following example shows how the > is used to condense a series of menu selections into one step:

❖ Select **Start** > **Programs** > **VERITAS NetBackup** > **NetBackup Administration Console**.

The corresponding actions could be described in more steps as follows:

1. Click **Start** in the task bar.

2. Move your cursor to **Programs**.

3. Move your cursor to the right and highlight **VERITAS NetBackup**.

4. Move your cursor to the right. First highlight and then click **NetBackup Administration Console**.

Introduction 1

NetBackup Encryption is a separately priced product that provides file-level encryption of backups and archives. There are two versions:

- Standard Encryption (recommended)

  Provides the ability to encrypt data using 128-bit or 256-bit OpenSSL ciphers.

- Legacy Encryption

  Provides the user with the encryption strength choices previous available, 40-bit DES and 56-bit DES.

Not all NetBackup agents and options are supported for encrypted backups and restores. For a complete list of supported policy types, see the *NetBackup Release Notes*.

Terminology

These terms will be useful in understanding and using NetBackup Encryption.

Advanced Encryption Standard (AES)	A symmetric block cipher with variable key lengths. NetBackup uses 128-bit or 256-bit keys with AES.
Blowfish (BF)	A symmetric block cipher with variable key lengths. NetBackup uses 128-bit keys with Blowfish.
Data Encryption Standard (DES)	A symmetric block cipher with 56-bit key length. NetBackup includes an option to effectively reduce the key length to 40-bits.
Triple DES	Data is encrypted three times using DES. NetBackup uses Two Key Triple DES (EDE) which has an effective key length of 112 bits.
Cipher Block Chaining Mode (CBC)	A method of encrypting blocks of data used by NetBackup legacy encryption.
Cipher Feedback Mode (CFB)	A method of encrypting blocks of data used by NeBackup standard encryption.

128-bit Encryption Cipher-based encryption using the 128-bit (or less) OpenSSL ciphers.

256-bit Encryption Cipher-based encryption using the greater-than 128-bit OpenSSL ciphers.

56-bit DES Key The NetBackup legacy DES encryption key is 56 bits long.

40-bit DES Key A 40-bit DES key is the same as a 56-bit DES key except that 16 bits are always set to zero.

For Standard Encryption:

Key File A key file is a file on a NetBackup encryption client. The data in the key file are the encryption keys used during backup and restore. The key file is encrypted with a private VERITAS key. The key file is created or updated by the `bpkeyutil` command.

Pass Phrase A pass phrase is like a password except it is usually longer. In NetBackup standard encryption, an encryption key is a digested checksum of a pass phrase. Pass phrases used by NetBackup can be from 0 to 63 characters long. To avoid compatibility problems between systems, restrict the characters in a pass phrase to printable ASCII characters. These are the characters from Space (code 32) to tilde (code 126) in the ASCII collating sequence.

For Legacy Encryption:

Key File A key file is a file on a NetBackup Encryption client. The data in the key file is used to generate DES keys that are used to encrypt a client's backed up files. The path name of the key file is defined in the client's `CRYPT_KEYFILE` configuration option. A key file is created or updated when a pass phrase is specified with the `bpinst` command on a NetBackup master server or the `bpkeyfile` command on a client.

Pass Phrase A pass phrase is like a password except that it is usually longer. In NetBackup, a pass phrase is checksummed in order to generate DES encryption keys. Pass phrases used by NetBackup can be from 0 to 63 characters long. To avoid compatibility problems between systems, restrict the characters in a pass phrase to printable ASCII characters. These are the characters from Space (code 32) to tilde (code 126) in the ASCII collating sequence.

NetBackup Pass Phrase

A NetBackup pass phase is used to generate data placed in a client's key file. The data in the key file is used to generate DES keys used to encrypt a client's backed up files. You can update the NetBackup pass phase for a client's key file by specifying the `-passphrase_prompt` option on the `bpinst` command from a master server or by specifying the `-change_netbackup_pass_phrase` option on the `bpkeyfile` command on a client.

Key File Pass Phrase

A key file pass phrase is used to generate the DES key that is used to encrypt the key file on a NetBackup client. You can either use NetBackup's standard key file pass phrase or use your own key file pass phrase by specifying the `-change_key_file_pass_phrase` option on the `bpkeyfile` command on a client.

Standard Key File Pass Phrase

The standard key file pass phrase is hardcoded into NetBackup programs. If the key file is encrypted using the DES key generated from the standard key file pass phrase, NetBackup programs can automatically decrypt and read the key file.

Technical Overview

When a backup is started, the server determines from a policy attribute whether the backup should be encrypted. The server then connects to `bpcd` on the client to initiate the backup and passes the Encryption policy attribute on the backup request. The client compares the Encryption policy attribute to the `CRYPT_OPTION` in the configuration on the client.

- If the policy attribute is `yes` and `CRYPT_OPTION` is `REQUIRED` or `ALLOWED`, the client will perform an encrypted backup.
- If the policy attribute is `yes` and `CRYPT_OPTION` is `DENIED`, the client will not perform the backup.
- If the policy attribute is `no` and `CRYPT_OPTION` is `ALLOWED` or `DENIED`, the client will perform a non-encrypted backup.
- If the policy attribute is no and `CRYPT_OPTION` is `REQUIRED`, the client does not perform the backup.

The following table shows the type of backup performed for each of the above conditions:

	Encryption Policy Attribute	
CRYPT_OPTION	**Yes**	**No**
`REQUIRED`	Encrypted	None
`ALLOWED`	Encrypted	Non-encrypted
`DENIED`	None	Non-encrypted

The following sections describe backup and restore operations for both standard and legacy encryption methods.

How a Standard Encryption Backup Works

The prerequisites for encrypting a standard backup are as follows:

- The encryption software must be loaded onto the client, either by running
  `bpinst -ENCRYPTION`
  on the master server or configuring directly on the client.
- A key file must exist. The key file is created when you run the `bpkeyutil` command from the master server or from the client.
- The NetBackup policy that includes the client must have the **Encryption** attribute selected.

If the above conditions are met, the following occurs:

1. The client takes the latest key from the key file.

2. For each file backed up:

   - The client creates an encryption `tar` header. The `tar` header contains a checksum of the key and the cipher used for encryption.
   - The client writes the file data encrypted with the key using the cipher defined by teh CRYPT_CIPHER configuration entry. (The default cipher is AES-128-CFB.)

Note Only file data is encrypted. File names and attributes are not encrypted.

3. The backup image on the server includes a flag indicating whether the backup was encrypted.

How a Standard Encryption Restore Works

The prerequisites for restoring an encrypted backup are as follows:

- The encryption software must be loaded onto the client.
- A key file must exist. The key file is created when you run the `bpkeyutil` command from the master server or from the client.

At the time of the restore, the server determines from the backup image whether the backup was encrypted. The server then connects to `bpcd` on the client to initiate the restore. The server sends to the client an encryption flag on the restore request.

When the above conditions are met, the following occurs:

- The server sends file names, attributes, and encrypted file data to the client to be restored.
- If the client reads an encryption tar header, the client compares the checksum in the header with the checksums of the keys in the keyfile. If the checksum of one of the keys matches the checksum in the header, that key will be used to decrypt the file data using the cipher defined in the header.
- The file is decrypted and restored if a key and cipher are available. If the key or cipher are not available, the file is not restored and an error message is generated.

How a Legacy Encryption Backup Works

The prerequisites for encrypting a standard backup are as follows:

- The encryption software must be loaded into the directory on the client that is specified by the `CRYPT_LIBPATH` configuration entry.
- For legacy encryption, the encryption software must include the appropriate DES library as follows:
  - for 40-bit DES encryption, `libvdes40.`*suffix* where *suffix* is `so`, `sl`, or `dll` depending on the client platform.
  - for 56-bit DES encryption, `libvdes56.`*suffix* where *suffix* is `so`, `sl`, or `dll` depending on the client platform.
- A key file must exist as specified with the `CRYPT_KEYFILE` configuration option. The key file is created when specifying a NetBackup pass phrase with the `bpinst` command from the master server or the `bpkeyfile` command from the client.

- The NetBackup policy that includes the client must have the **Encryption** attribute selected.

If the above conditions are met and the backup is to be encrypted, the following occurs:

1. The client takes the latest data from its key file and merges it with the current time (the backup time) to generate a DES key. For 40-bit DES, 16 bits of the key are always set to zero.

2. For each file backed up:

   - The client creates an encryption `tar` header. The `tar` header contains a checksum of the DES key used for encryption.

   - The client writes the file data encrypted with the DES key.

Note Only file data is encrypted. File names and attributes are not encrypted.

3. The server reads the file names, attributes, and data from the client and writes them to a backup image on the server. The server DOES NOT perform any encryption or decryption of the data. The backup image on the server includes the backup time and a flag indicating whether the backup was encrypted.

How a Legacy Encryption Restore Works

The server determines from the backup image whether the backup was encrypted. The server then connects to `bpcd` on the client to initiate the restore. The server sends to the client an encryption flag and backup time from the backup image on the restore request.

The prerequisites for restoring an encrypted backup are as follows:

- The encryption software must be loaded into the directory on the client specified by the `CRYPT_LIBPATH` configuration option.

- The encryption software must include the 40-bit DES library. The name of the 40-bit DES library is `libvdes40.`*suffix* where *suffix* is `so`, `sl`, or `dll` depending on the client platform.

- If the `CRYPT_STRENGTH` configuration option is set to DES_56, the encryption software must also include the 56-bit DES library. The name of the 56-bit DES library is `libvdes56.`*suffix* where suffix is `so`, `sl`, or `dll` depending on the client platform.

- A key file must exist as specified with the `CRYPT_KEYFILE` configuration option. The key file should have been created when specifying a NetBackup pass phrase with the `bpinst` command from the master server or the `bpkeyfile` command from the client.

If the above conditions are met, the following occurs:

- The server sends file names, attributes, and encrypted file data to the client to be restored.
- The client takes its key file data and merges it with the backup time to generate one or more 40-bit DES keys. If the 56-bit DES library is available, the client also generates one or more 56-bit DES keys.
- If the client reads an encryption tar header, the client compares the checksum in the header with the checksums of its DES keys. If the checksum of a DES key matches the checksum in the header, that DES key will be used to decrypt the file data.
- The file is decrypted and restored if a DES key is available. If the DES key is not available, the file is not restored and an error message is generated.

Installation on a Master Server 2

You must first install NetBackup Encryption on either a UNIX or Windows NetBackup master server. When this installation is complete, you can then install and configure it on the clients as explained in the Configuration for Standard Encryption and Configuration for Legacy Encryption chapters.

Installation Prerequisite

The master servers for the clients that require encrypted backups must be running NetBackup 5.1 server software. For a list of the platforms on which you can install NetBackup Encryption, see the *NetBackup Release Notes*.

Note In a clustered environment, you must freeze the active node so that migrations do not occur before you start installing any add-ons. Refer to the clustering section in the *NetBackup High Availability System Administrator's Guide* that pertains to the type of cluster software you are running for more information on how to freeze a service group.

Installing on a UNIX NetBackup Master Server

▼ To install on a NetBackup for UNIX master server

1. Log in as the root user on the NetBackup UNIX master server.

2. Make sure a valid license key for NetBackup Encryption has been registered by executing the following command to list and add keys:

   ```
   /usr/openv/netbackup/bin/admincmd/get_license_key
   ```

Note Existing 40 or 56-bit encryption license keys are valid for upgrades.

3. Insert the CD-ROM containing the NetBackup Encryption software in the drive.

4. Change your working directory to the CD-ROM directory:

   ```
   cd /cd_rom_directory
   ```

   Where *cd_rom_directory* is the path to the directory where you can access the CD-ROM. On some platforms, it may be necessary to mount this directory.

5. To install NetBackup Encryption, run the following:

   ```
   ./install
   ```

   Since other NetBackup products are included on the CD-ROM, a menu of installation choices appears.

6. Select **NetBackup Add-On Product Software**.

   a. Select the **NetBackup Encryption** option.

   b. Enter **q** to quit the menu.

   c. When asked if the list is correct, answer **y**.

7. In a clustered environment, steps 1 - 6 must be executed on each node in the cluster.

8. Install software on the clients.

   For most NetBackup clients, you can install (push) the encryption software from the master server to the client. For details, see "Configuring from the Master Server" on page 13.

   Note In a clustered environment, the capability to push to a client is only allowed from the primary node.

   However, the client *must* allow server writes to install from the server. On a UNIX client, this means that `DISALLOW_SERVER_WRITES` cannot be present in the `bp.conf` file. On Microsoft Windows clients, the **Allow server directed restores** box must be selected on the **General** tab of the NetBackup Configuration dialog box. (Open this dialog box by choosing **Actions>Configure** in the Backup, Archive, and Restore interface).

   If the client does not allow server writes, use the method described in "Configuring NetBackup Encryption on the Client" on page 28.

Note In a clustered environment, after you have successfully installed the add-on, unfreeze this node. Again, refer to the appropriate clustering section in the *NetBackup High Availability System Administrator's Guide* for more information on how to unfreeze a service group.

Installing on a Windows NetBackup Master Server

▼ To install on NetBackup for Windows master server

1. Log in as Administrator on the NetBackup Windows master server.

2. Make sure a valid license key for NetBackup Encryption has been registered by doing the following to list and add keys:

   a. From the NetBackup Administration window, choose **Help**.

   b. Select **Help** > **License Keys ...**.

      The NetBackup License Keys window appears. Existing keys are listed in the lower part of the window.

   c. To register a new key, type your license key in the **New license key** field and click **Add**.

      The new license key appears in the lower part of the dialog box.

3. Insert the CD-ROM for NetBackup Server into the drive.

4. If the AutoPlay feature is enabled, the AutoRun program will allow you to:

   ◆ Browse the contents of the CD-ROM

   ◆ Add or remove programs from your system

   ◆ View NetBackup Encryption for Windows Readme files

   ◆ Install NetBackup Encryption for Windows

   The VERITAS NetBackup for Windows Installer appears.

   a. Select Additional Products.

   b. Select Additional Product Installations.

   c. Select NetBackup Encryption.

      The Install wizard launches. Skip to step 6.

5. If the AutoPlay feature is not enabled, choose **Run** from the **Start** menu and execute:

   ```
   D:\Addons\Encryption\NTCrypt\Setup.exe
   ```

   Where *D:* \ is your CD-ROM drive.

6. Follow the prompts in the install application.

7. Install software on the clients.

   For most NetBackup clients, you can install (push) the encryption software from the master server to the client. For details, see "Configuring from the Master Server" on page 23.

   Note If you are running NetBackup in a clustered environment, pushing software to the client is only allowed from the active node.

   Note If you are pushing the encryption software to clients located in a cluster, specify the hostnames of the individual nodes (not the virtual names) in the list of clients.

   However, the client must allow server writes to install from the server. On a UNIX or Macintosh client, this means that `DISALLOW_SERVER_WRITES` cannot be present in the `bp.conf` file. On Microsoft Windows clients, the **Allow server directed restores** box must be selected on the **General** tab of the NetBackup Configuration dialog box (open this dialog box by clicking **Actions** > **Configure** in the client-user interface).

   If the client does not allow server writes, use the method described in "Configuring NetBackup Encryption on the Client" on page 16.

Configuration for Standard Encryption 3

This chapter explains how to configure NetBackup Encryption and contains the following sections:

- Configuring from the Master Server
- Configuring NetBackup Encryption on the Client
- Setting the Encryption Attribute in NetBackup Policies
- Changing Client Encryption Settings from the NetBackup Server

The CRYPT_OPTION, CRYPT_KIND, and CRYPT_CIPHER configuration options mentioned in this chapter are in the bp.conf file on UNIX clients and in the registry on Microsoft Windows clients. You can also use the NetBackup Administration interface on a NetBackup server to configure the options remotely. They are on the **Encryption** tab in the Client Properties dialog box (see the *NetBackup System Administrator's Guide* for details).

Configuring from the Master Server

You can configure most NetBackup clients for encryption by using the bpinst command from the master server. Prerequisites include the following:

- The NetBackup Encryption client software must be installed in a directory on the master server as described in the Installation on a Master Server chapter.
- The NetBackup client software must be running on platforms that support NetBackup Encryption (see the *NetBackup Release Notes*).
- The NetBackup clients must be running NetBackup 5.1 or later (for standard encryption).
- If the master server is part of a cluster, all nodes in the cluster must have the same keyfile.
- The NetBackup configuration on the clients must allow server writes.

  On a UNIX client, this means that DISALLOW_SERVER_WRITES cannot be present in the bp.conf file.

On Microsoft Windows clients, the **Allow Server Directed Restores** box must be selected. In the Backup, Archive, and Restore utility, this is on the **General** tab of the NetBackup Client Properties dialog. (Open this dialog by selecting **File** >**NetBackup Client Properties.**)

If a client does not allow server writes, either temporarily change its configuration so writes are allowed or use the method described in "Configuring NetBackup Encryption on the Client" on page 16.

The `bpinst` command is loaded into the NetBackup `bin` directory on the master server.

- For a Windows server, the `bin` directory is:

  `install_path``\NetBackup\bin`

- For a UNIX server, the `bin` directory is:

  `/usr/openv/netbackup/bin`

See the `bpinst` command description in the *NetBackup Commands* guide for details on the options that are available with the `bpinst` command. The following sections contain several examples of how to use `bpinst`.

Normally, you specify client names in the `bpinst` command. However, if you include the `-policy_names` option, you will specify policy names instead. This will affect all clients in the specified policies.

Pushing NetBackup Encryption Software to Clients

Note The supported platforms section of the *NetBackup Release Notes* defines which NetBackup clients can support encryption.

Use the `-ENCRYPTION` option on the `bpinst` command to copy encryption software from the master server to NetBackup clients.

From a UNIX Master Server

Assume that you want to install the client software on client1 and client2. You would enter a command like this (all on one line):

```
bpinst -ENCRYPTION client1 client2
```

Assume that you want to install the client software on all clients in the NetBackup policies policy1 and policy2. You would enter a command like this (all on one line):

```
bpinst -ENCRYPTION -policy_names policy1 policy2
```

From a Windows Master Server

Assume that you want to install the client software on client1 and client2. You would enter a command like this (all on one line):

```
bpinst.exe -ENCRYPTION client1 client2
```

Assume that you want to install the client software on all clients in the NetBackup policies policy1 and policy2. You would enter a command like this (all on one line):

```
bpinst.exe -ENCRYPTION policy_names policy1 policy2
```

Note If you are running NetBackup in a clustered environment, pushing software to the client is only allowed from the active node.

Note If you are pushing the encryption software to clients located in a cluster, specify the hostnames of the individual nodes (not the virtual names) in the list of clients.

Creating the NetBackup Encryption Keyfile on the Clients

The `bpkeyutil` command sets up the cipher-based encryption keyfile and pass phrase on each NetBackup Encryption client. The `bpkeyutil` command is loaded into the NetBackup `bin` directory on the master server.

- For a Windows server, the `bin` directory is:

  `install_path``\NetBackup\bin`

- For a UNIX server, the `bin` directory is:

  `/usr/openv/netbackup/bin`

For each encryption client, run the following command:

```
bpkeyutil -client client_name
```

You are prompted for a new pass phrase to add to that client’s key file.

Previous pass phrases remain available in the file for restores of backups encrypted with those phrases.

Caution It is important that you remember the pass phrases, including the old pass phrases. If a client’s key file is damaged or lost, you need all of the previous pass phrases in order to recreate the key file. Without the keyfile, you will be unable to restore files that were encrypted with the pass phrases.

The key file must only be accessible to the administrator of the client machine. For a UNIX client, this means that its owner is root, its mode bits 600, and it should not be on a file system that can be NFS mounted.

Best Practices: Key File Restoration

If the key file is lost, it will be difficult to restore it from an encrypted backup. Following are two methods to ensure that the key file is available for restores.

Manual Retention

This is the most secure method for protecting your key file pass phrases.

- When you add a pass phrase via the `bpkeyutil` command, write the phrase down on paper, seal it in an envelope, and put the envelope into a safe.

If you need to restore from encrypted backups, reinstall NetBackup and NetBackup Encryption, then use `bpkeyutil` to create a new key file with the pass phrases from the safe.

Automatic Backup

This method is less secure, but insures that a backup copy of your keyfile exists.

- Create a non-encrypted policy to back up the key file.

If the key file is lost, you can restore it from the non-encrypted backup. However, this also means that a usable version of one client's key file could be restored on a different client.

If you want to prevent the key file from being backed up, add the key file's path name to the client's exclude list.

Configuring NetBackup Encryption on the Client

You can also configure NetBackup Encryption directly on the client as explained in the following topics.

Obtaining NetBackup Encryption Software

If the client does not allow server writes, you must coordinate with the master server administrator to obtain the NetBackup Encryption software. On a UNIX client, server writes are not allowed if `DISALLOW_SERVER_WRITES` is present in the `bp.conf` file. On Microsoft Windows clients, server writes are not allowed if the **Allow server directed restores** box is not selected on the **General** tab of the NetBackup Configuration dialog box (open this dialog box by clicking **Actions>Configure** in the client-user interface).

The NetBackup Encryption client software has been installed on the master server in the following directories (by default):

- Windows master server:

  install_path\netbackup\crypt

- UNIX master server:

  /usr/openv/netbackup/crypt

The crypt directory contains directories with names that correspond to the various hardware platforms that NetBackup Encryption supports. The hardware directories contain directories with names that correspond to the various operating systems supported by NetBackup Encryption. The operating system directories contain the NetBackup binaries for that hardware platform and operating system.

You must copy the binaries for your client platform from the master server to the appropriate directory on your client.

The default directory for Microsoft Windows clients is:

install_path\NetBackup\bin

The default directory for UNIX clients is:

/usr/openv/netbackup/bin

/usr/openv/share

Suppose you have a Solaris 8 client and you have permission to FTP to a UNIX NetBackup master server to get your NetBackup Encryption software. You would enter commands like this:

```
cd /usr/openv/netbackup/bin
ftp master
ftp> cd /usr/openv/netbackup/crypt/Solaris/Solaris8
ftp> binary
ftp> get bpkeyutil
ftp> lcd /usr/openv/share
ftp> get ciphers.txt
ftp> get version_crypt
ftp> quit
chmod 555 bpkeyutil
cd /usr/openv/share
chmod 444 ciphers.txt. version_crypt
```

Managing NetBackup Encryption Configuration Options

There are three encryption-related configuration options for standard encryption on a NetBackup client. Ensure that these options are set to the appropriate values for your client.

`CRYPT_OPTION =` *option*

Defines the encryption options on NetBackup clients. The possible values for *option* are:

`denied|DENIED`

Specifies that the client does not permit encrypted backups. If the server requests an encrypted backup, it is considered an error.

`allowed|ALLOWED`

Specifies that the client allows either encrypted or unencrypted backups. This is the default value.

`required|REQUIRED`

Specifies that the client requires encrypted backups. If the server requests an unencrypted backup, it is considered an error.

`CRYPT_KIND =` *kind*

Defines the encryption kind on NetBackup clients. The possible values for *kind* are:

`NONE`

Neither standard nor legacy encryption is configured on the client.

`STANDARD`

Specifies cipher-based 128-bit or 256-bit encryption. This is the default value if standard encryption is configured on the client.

`LEGACY`

Specifies legacy 40-bit DES or 56-bit DES encryption.

`CRYPT_CIPHER =` *cipher*

Defines the cipher type to use. This can be set to any of the following:

AES-128-CFB	128-bit Advanced Encryption Standard
BF-CFB	128-bit Blowfish
DES-EDE-CFB	Two Key Triple DES

AES-256-CFB	256-bit Advanced Encryption Standard

The default is AES-128-CFB.

Managing the NetBackup Encryption Key File

Note The key file must be the same on all nodes in a cluster.

Use the `bpkeyutil` command sets to set up the cipher-based encryption keyfile and pass phrase on the NetBackup Encryption client. The `bpkeyutil` command is loaded in the NetBackup `bin` directory.

- For a Windows client, the `bin` directory is:

  install_path`\NetBackup\bin`

- For a UNIX client, the `bin` directory is:

  `/usr/openv/netbackup/bin`

On the encryption client, run the following command:

```
bpkeyutil
```

You are prompted for the pass phrase for that client.

Previous pass phrases remain available in the file for restores of backups encrypted with those phrases.

Caution It is important that you remember the pass phrases, including the old pass phrases. If a client's key file is damaged or lost, you need all of the previous pass phrases in order to recreate the key file. Without the keyfile, you will be unable to restore files that were encrypted with the pass phrases.

The key file must only be accessible to the administrator of the client machine. For a UNIX client, this means that its owner is root, its mode bits 600, and it should not be on a file system that can be NFS mounted.

Best Practices: Key File Restoration

If the key file is lost, it will be difficult to restore it from an encrypted backup. Following are two methods to ensure that the key file is available for restores.

Manual Retention

This is the most secure method for protecting your key file pass phrases.

- When you add a pass phrase via the bpkeyutil command, write the phrase down on paper, seal it in an envelope, and put the envelope into a safe.

If you need to restore from encrypted backups, reinstall NetBackup and NetBackup Encryption, then use bpkeyutil to create a new key file with the pass phrases from the safe.

Automatic Backup

This method is less secure, but insures that a backup copy of your keyfile exists.

- Create a non-encrypted policy to back up the key file.

If the key file is lost, you can restore it from the non-encrypted backup. However, this also means that a usable version of one client's key file could be restored on a different client.

If you want to prevent the key file from being backed up, add the key file's path name to the client's exclude list.

Redirected Restores of Encrypted Files

Redirectred restores require special configuration changes to allow the restore. This procedure provides the additional changes required when redirecting a restore of encrypted files.

▼ To restore an encrypted backup that was made by another client

1. The master server must be configured to allow redirected restores, and you (the user) must be authorized to perform such restores. Refer to the *NetBackup System Administrator's Guide* for details on redirected restores.

2. Obtain the pass phrase that the other client used when the encrypted backup was made. Without that pass phrase, you will not be able to restore the files.

Note If your pass phrase is the same as the one used by the other client, skip to step 5.

3. Move or rename your own (current) key file. This preserves your key file when you create a new one in the next step.

4. Using the `bpkeyutil` command, create an encryption key file that matches the one used by the other client. When you are prompted for the pass phrase by the bpkeyutil command, specify the other client's pass phrase.

5. Restore the desired files that were backed up by the other client. For help with redirected restores, refer to the *NetBackup User's Guide.*

Note When you have finished restoring encrypted files from the client, rename or delete the key file created above, and move or rename your own key file to its original location or name. If you do not re-establish your key file to its original location / name, you may not be able to restore your own encrypted backups.

Setting the Encryption Attribute in NetBackup Policies

Whether you configure your encryption clients from the NetBackup master server or from the clients, your NetBackup policy for encrypted backups must include setting the **Encryption** attribute.

- If the attribute is set, the NetBackup server requests that NetBackup clients in that policy perform encrypted backups.
- If the attribute is clear, the NetBackup server does not request that NetBackup clients in that policy perform encrypted backups.

You can use the **Attributes** tab of the policy in the NetBackup Administration Console to set or clear the **Encryption** attribute for a policy. For details on configuring NetBackup policies, see the *NetBackup System Administrator's Guide, Volume I*.

Changing Client Encryption Settings from the NetBackup Server

It is possible to change the encryption settings for a NetBackup client from the Client Properties dialog on the NetBackup master server.

▼ To change the client encryption settings from the NetBackup server:

1. From the NetBackup Administration Console on the server, expand the **Host Properties** node and select **Clients**.

2. In the Clients list, double click the name of the client you want to change. The Client Properties dialog displays.

3. In the Properties pane, click **Encryption** to display the encryption settings for that client.

The settings on this dialog correspond to the options described in "Managing NetBackup Encryption Configuration Options" on page 18. For additional explanation of the settings, click the **Help** button on the dialog, or see the *NetBackup System Administrator's Guide, Vol I*.

Configuration for Legacy Encryption 4

This chapter explains how to configure NetBackup Encryption and contains the following sections:

- Configuring from the Master Server
- Configuring NetBackup Encryption on the Client
- Setting Encryption in NetBackup Policies
- Changing Client Encryption Settings from the NetBackup Server
- Additional Key File Security (UNIX clients only)

The `CRYPT_OPTION`, `CRYPT_STRENGTH`, `CRYPT_LIBPATH`, and `CRYPT_KEYFILE` configuration options mentioned in this chapter are in the `bp.conf` file on UNIX clients and in the registry on Microsoft Windows clients. You can also use the NetBackup Administration interface on a Windows NetBackup server to configure the options remotely. They are on the **Encryption** tab in the Client Properties dialog box (see the *NetBackup System Administrator's Guide* for details).

These options can be set by the `bpinst -LEGACY_CRYPT` command (found in `/usr/openv/netbackup/bin` on UNIX systems, and `<install_path>\netbackup\bin` on Windows systems). The equivalent option settings for this command are `-crypt_option`, `-crypt_strength`, and `-update_libraries`, respectively. The CRYPT_KEYFILE is created with the option `-passphrase_prompt` or `-passphrase -stdin`.

Configuring from the Master Server

You can configure most NetBackup clients for encryption by using the `bpinst` command from the master server. Prerequisites for this method include the following:

- The NetBackup Encryption client software must be installed in a directory on the master server as described in the Installation on a Master Server chapter.
- The NetBackup client software must be running on platforms that support NetBackup Encryption (see the *NetBackup Release Notes*).

- If the master server is part of a cluster, all nodes in the cluster must have the same keyfile.
- The NetBackup configuration on the clients must allow server writes.

  On a UNIX client, this means that `DISALLOW_SERVER_WRITES` cannot be present in the `bp.conf` file.

  On Microsoft Windows clients, the **Allow Server Directed Restores** box must be selected. In the Backup, Archive, and Restore utility, this is on the **General** tab of the NetBackup Client Properties dialog. (Open this dialog by selecting **File** >**NetBackup Client Properties.**)

  If a client does not allow server writes, either temporarily change its configuration so writes are allowed or use the method described in "Configuring NetBackup Encryption on the Client" on page 28.

The `bpinst` command is loaded into the NetBackup `bin` directory on the master server.

- For a Windows server, the `bin` directory is:

  install_path`\NetBackup\bin`

- For a UNIX server, the `bin` directory is:

  `/usr/openv/netbackup/bin`

See the `bpinst` command description in the *NetBackup Commands* guide for details on the options that are available with the `bpinst` command. The following sections contain several examples of how to use `bpinst`.

Normally, you specify client names in the `bpinst` command. However, if you include the `-policy_names` option, you will specify policy names instead. This will affect all clients in the specified policies.

Read This If Clients Have Not Been Previously Configured

If you are using `bpinst -LEGACY_CRYPT` to configure encryption on clients that were not previously configured for encryption, ensure that you push the encryption libraries to the clients first with one `bpinst` command and then configure the encryption pass phrase with a separate `bpinst` command. For example:

```
bpinst -LEGACY_CRYPT -update_libraries /usr/openv/lib/client
clientname1
bpinst -LEGACY_CRYPT -passphrase_prompt clientname1
```

If you try to specify both the `-update_libraries` and `-passphrase_prompt` arguments on the same command line, the pass phrase configuration can fail because the encryption libraries are not yet available on the client.

Note If you are running NetBackup in a clustered environment, pushing software to the client is only allowed from the active node.

Note If you are pushing the encryption software to clients located in a cluster, specify the hostnames of the individual nodes (not the virtual names) in the list of clients.

Pushing NetBackup Encryption Software to Clients

Note The supported platforms section of the *NetBackup Release Notes* defines which NetBackup clients can support encryption.

You can use the `-update_libraries` option on the `bpinst` command to copy encryption software from the master server to NetBackup clients.

Assume that you want to install the client software on client1 and client2. You would enter a command like this (all on one line):

```
bpinst -LEGACY_CRYPT -update_libraries /usr/openv/lib/client client1
client2
```

Assume that you want to install the client software on all clients in the NetBackup policies policy1 and policy2. You would enter a command like this (all on one line):

```
bpinst -LEGACY_CRYPT -update_libraries /usr/openv/lib/client
-policy_names policy1 policy2
```

For Windows master servers, you would use the following commands:

```
bpinst.exe -LEGACY_CRYPT -update_libraries ignore client1 client2
bpinst.exe -LEGACY_CRYPT -update_libraries ignore policy_names policy1
policy2
```

Note On a Windows master server, the `-update_libraries` option must be specified with the `ignore` argument.

Note If you are running NetBackup in a clustered environment, pushing software to the client is only allowed from the active node.

Note If you are pushing the encryption software to clients located in a cluster, specify the hostnames of the individual nodes (not the virtual names) in the list of clients.

Pushing the NetBackup Encryption Configuration to Clients

You can use the `-crypt_option` and `-crypt_strength` options on the `bpinst` command to set encryption-related configuration on NetBackup clients.

- The `-crypt_option` option specifies whether the client should deny encrypted backups (`denied`), allow encrypted backups (`allowed`), or require encrypted backups (`required`).
- The `-crypt_strength` option specifies the DES key length (`40` or `56`) that the client should use for encrypted backups.

Assume that you want all clients in NetBackup policies policy1 and policy2 to require encrypted backups with a 56-bit DES key. You would enter a command like this from a UNIX NetBackup master server (the command is all on one line):

```
bpinst -LEGACY_CRYPT -crypt_option required -crypt_strength des_56
-policy_names policy1 policy2
```

Assume that you want client1 and client2 to allow either encrypted or non-encrypted backups with a 40-bit DES key. You would enter a command like this from a Windows NetBackup master server (the command is all on one line):

```
bpinst.exe -LEGACY_CRYPT -crypt_option allowed -crypt_strength des_40
client1 client2
```

Note If you are running NetBackup in a clustered environment, pushing software to the client is only allowed from the active node.

Note If you are pushing the encryption software to clients located in a cluster, specify the hostnames of the individual nodes (not the virtual names) in the list of clients.

Pushing Encryption Pass Phrases to Clients

You can use the `-passphrase_prompt` or `-passphrase_stdin` option on the `bpinst` command to send a pass phrase to a NetBackup client. The NetBackup client uses the pass phrase to create or update data in its key file. The key file contains data that the client uses to generate DES keys to encrypt backups.

- If you use the -`passphrase_prompt` option, you are prompted at your terminal for a zero to 63 character pass phrase. The characters are hidden while you type the pass phrase. You are prompted again to retype the pass phrase to make sure that is the one you intended to enter.

- If you use the -passphrase_stdin option, you must enter the zero to 63 character pass phrase twice through standard input. Generally, the -passphrase_prompt option is more secure than the -passphrase_stdin option, but -passphrase_stdin is more convenient if you use bpinst in a shell script.

Suppose you want to enter a pass phrase for the client named client1 from a UNIX NetBackup master server through standard input. You would enter commands like the following:

```
bpinst -LEGACY_CRYPT -passphrase_stdin client1 <<EOF
Use a better pass phrase than this
Use a better pass phrase than this
EOF
```

Suppose you want to enter a pass phrase for the client named client2 from a Windows NetBackup master server. You would enter commands like the following:

```
bpinst.exe -LEGACY_CRYPT -passphrase_prompt client2
Enter new NetBackup pass phrase: ********************
Re-enter new NetBackup pass phrase: ********************
```

You may enter new pass phrases fairly often. The NetBackup client keeps information about old pass phrases in its key file and is able to restore data that was encrypted with DES keys generated from old pass phrases.

Caution It is important that you remember the pass phrases including the old pass phrases. If a client’s key file is damaged or lost, you need all of the previous pass phrases in order to recreate the key file. Without the keyfile, you will be unable to restore files that were encrypted with the pass phrases.

One thing you must decide is whether to use the same pass phrase for many clients. Using the same pass phrase is convenient because you can use a single bpinst command to specify a pass phrase for each client. You can also do redirected restores between clients that use the same pass phrase.

Note If you want to prevent redirected restores, you should specify different pass phrases for each client. This means that you will have to enter a bpinst command for each client.

Note If you are running NetBackup in a clustered environment, pushing software to the client is only allowed from the active node.

Note If you are pushing the encryption software to clients located in a cluster, specify the hostnames of the individual nodes (not the virtual names) in the list of clients.

Setting the Encryption Attribute in NetBackup Policies

Each NetBackup policy includes an Encryption attribute.

- If the attribute is set, the NetBackup server requests that NetBackup clients in that policy perform encrypted backups.
- If the attribute is clear, the NetBackup server does not request that NetBackup clients in that policy perform encrypted backups.

You can use the NetBackup Administration interface to set or clear the Encryption attribute for a policy.

You can also use the `bpinst` command to set or clear the Encryption attribute for NetBackup policies. This is convenient if you want to set or clear the attribute for several policies.

Suppose you want to set the Encryption attribute for policy1 and policy2 from a UNIX NetBackup master server. You would enter a command like this:

```
bpinst -LEGACY_CRYPT -policy_encrypt 1 -policy_names policy1 policy2
```

where `1` sets the encryption attribute (`0` would clear it).

Configuring NetBackup Encryption on the Client

For Microsoft Windows and UNIX clients, you can configure NetBackup Encryption directly on the client as explained in the following topics.

Note From NetBackup release 5.0,Mac OS 9 (and earlier) Macintosh clients are no longer supported. Clients running Mac OS X 10.2.2 and higher are supported and are considered UNIX clients in this document.

Obtaining NetBackup Encryption Software

If the client does not allow server writes, you must coordinate with the master server administrator to obtain the NetBackup Encryption software. On a UNIX client, server writes are not allowed if `DISALLOW_SERVER_WRITES` is present in the `bp.conf` file. On Microsoft Windows clients, server writes are not allowed if the **Allow server directed restores** box is not selected on the **General** tab of the NetBackup Configuration dialog box (open this dialog box by clicking **Actions>Configure** in the client-user interface).

The NetBackup Encryption client software has been installed on the master server in the following directories (by default):

- Windows master server:

install_path`\netbackup\crypt`

- UNIX master server:

```
/usr/openv/netbackup\crypt
```

The crypt directory contains directories with names that correspond to the various hardware platforms that NetBackup Encryption supports. The hardware directories contain directories with names that correspond to the various operating systems supported by NetBackup Encryption. The operating system directories contain the NetBackup binaries for that hardware platform and operating system.

You must copy the binaries for your client platform from the master server to the appropriate directory on your client.

The directory on the client is specified with the `CRYPT_LIBPATH` configuration option on the client.

The default directory for Microsoft Windows clients is:

install_path`\NetBackup\bin`

The default directory for UNIX clients is:

```
/usr/openv/netbackup/bin
```

Suppose you have a Solaris 8 client and you have permission to FTP to a UNIX NetBackup master server to get your NetBackup Encryption software. You would enter commands like this:

```
cd /usr/openv/netbackup/bin
ftp master
ftp> cd /usr/openv/netbackup/crypt/Solaris/Solaris8
ftp> binary
ftp> mget libvdes40*
ftp> mget libvdes56*
ftp> quit
```

The library names are:

`libvdes40.`*suffix*
`libvdes56.`*suffix*

For some platforms, we also provide 64-bit libraries:

`libvdes40_64.`*suffix*
`libvdes56_64.`*suffix*

Where *suffix* is `so`, `sl`, or `dll` depending on the platform. You need libvdes40.*suffix* to perform 40-bit DES encryption. You need both libvdes40.*suffix* and libvdes56.*suffix* to perform 56-bit DES encryption.

Managing NetBackup Encryption Configuration Options

There are five encryption-related configuration options on a NetBackup client. Ensure that these options are set to the appropriate values for your client. These will be set if you run the `bpinst -LEGACY_CRYPT` command from the master server to the client name.

`CRYPT_OPTION =` *option*

Defines the encryption options on NetBackup clients. The possible values for *option* are:

`denied|DENIED`

Specifies that the client does not permit encrypted backups. If the server requests an encrypted backup, it is considered an error. This is the default value.

`allowed|ALLOWED`

Specifies that the client allows either encrypted or unencrypted backups.

`required|REQUIRED`

Specifies that the client requires encrypted backups. If the server requests an unencrypted backup, it is considered an error.

`CRYPT_KIND =` *kind*

Defines the encryption kind on NetBackup clients. The possible values for *kind* are:

`NONE`

Neither standard nor legacy encryption is configured on the client.

`LEGACY`

Specifies legacy 40-bit DES or 56-bit DES encryption. This is the default if legacy encryption is configured on the client, and standard encryption is not configured.

`STANDARD`

Specifies cipher-based 128-bit or 256-bit encryption.

`CRYPT_STRENGTH =` *strength*

Defines the encryption strength on NetBackup clients. The possible values for *strength* are:

`des_40|DES_40`

Specifies 40-bit DES encryption. This is the default value.

`des_56|DES_56`

Specifies 56-bit DES encryption.

`CRYPT_LIBPATH =` *directory_path*

Defines the directory that contains the encryption libraries on NetBackup clients.

The default value on UNIX systems is:

`/usr/openv/lib/`

The default value on Windows systems is:

install_path`\NetBackup\bin\`

Where *install_path* is the directory where NetBackup is installed and by default is `C:\VERITAS`.

`CRYPT_KEYFILE =` *file_path*

Defines the file that contains the encryption keys on NetBackup clients.

The default value on Windows systems is:

install_path`\NetBackup\bin\keyfile.dat`

The default value on UNIX systems is:

`/usr/openv/netbackup/keyfile`

Managing the NetBackup Encryption Key File

Note The key file must be the same on all nodes in a cluster.

Each NetBackup client that does encrypted backups and restores needs a key file. The key file contains data that the client uses to generate DES keys to encrypt backups.

You can use the `bpkeyfile` command on the client to manage the key file. Check the `bpkeyfile` command description in the *NetBackup Commands* guide for a detailed description.

The first thing you need to do is to create a key file if it does not already exist. The key file will exist if you set a passphrase from the `bpinst -LEGACY_CRYPT` command from the master server to this client name. The file name should be the same as the file name specified with the `CRYPT_KEYFILE` configuration option.

- For Windows clients, the default key file name is:

  install_path`\NetBackup\bin\keyfile.dat`

- For UNIX clients, the default key file name is:

  `/usr/openv/netbackup/keyfile`

You need to decide how you want to encrypt the key file. The key file is encrypted by a DES key generated from a key file pass phrase. Usually, you will use the standard key file pass phrase which is hardcoded into NetBackup applications. However, for added security you may want to use your own key file pass phrase. See "Additional Key File Security (UNIX clients only)" on page 35 for more details.

Note If you do not want to use your own key file pass phrase for extra protection as described in "Additional Key File Security (UNIX clients only)" on page 35, do not enter a new key file pass phrase. Instead, use the standard key file pass phrase and enter a new NetBackup pass phrase (see below).

You also must decide what NetBackup pass phrase to use. The NetBackup pass phrase is used to generate the data that is placed into the key file. That data is used to generate DES keys to encrypt backups.

Suppose you want to create the default key file on a UNIX client encrypted with the standard key file pass phrase. You would enter a command like this:

```
bpkeyfile /usr/openv/netbackup/keyfile
Enter new key file pass phrase: (standard key file pass phrase)
Re-enter new key file pass phrase: (standard key file pass phrase)
Enter new NetBackup pass phrase: ***********************
Re-enter new NetBackup pass phrase: ***********************
```

You may enter new NetBackup pass phrases fairly often. Information about old pass phrases is kept in the key file making it possible to restore data that was encrypted with DES keys generated from old pass phrases. You can use the `-change_netbackup_pass_phrase` (or `-cnpp`) option on the `bpkeyfile` command to enter a new NetBackup pass phrase.

Suppose you want to enter a new NetBackup pass phrase on a Windows client. You would enter a command like this:

```
bpkeyfile.exe -cnpp install_path\NetBackup\bin\keyfile.dat
Enter old key file pass phrase: (standard key file pass phrase)
Enter new NetBackup pass phrase: **********
Re-enter new NetBackup pass phrase: **********
```

Caution It is important that you remember the pass phrases, including the old pass phrases. If a client's key file is damaged or lost, you need all of the previous pass phrases in order to recreate the key file. Without the keyfile, you will be unable to restore files that were encrypted with the pass phrases.

It is important that the key file be accessible to only the administrator of the client machine. For a UNIX client, this means that its owner is root, its mode bits 600, and it should not be on a file system that can be NFS mounted.

You need to consider whether to back up your key file. For encrypted backups, backing up the key file is of little value since the key file can only be restored if the key file is already on the client.

You might consider setting up a NetBackup policy that does non-encrypted backups of the key files of the clients. This will be useful if an emergency restore of the key file is required. However, this also means that a usable version of one client's key file could be restored on a different client.

If you want to prevent the key file from being backed up, add the key file's path name to the client's exclude list.

Redirected Restores of Encrypted Files

To restore an encrypted backup that was made by another client, do the following:

1. The master server must be configured to allow redirected restores, and you (the user) must be authorized to perform such restores. Refer to the *NetBackup System Administrator's Guide* for details on redirected restores.

2. Obtain the pass phrase that the other client used when the encrypted backup was made. Without that pass phrase, you will not be able to restore the files.

Note If your pass phrase is the same as the one used by the other client, skip to step 5.

3. Move or rename your own (current) key file. This preserves your key file when you create a new one in the next step.

4. Using the `bpkeyfile` command, create an encryption key file that matches the one used by the other client. The other client's pass phrase must be specified by means of the `bpkeyfile` command:

   ```
   bpkeyfile -change_key_file_pass_phrase key_file_path
   ```

   where *key_file_path* is the path for a new key file on your client. This key file will match the key file used by the client whose files you want to restore.

   After entering the above command, you will be prompted for the client's pass phrase (obtained in step 2). For more information on the `bpkeyfile` command, refer to the *NetBackup Commands* guide.

5. Restore the desired files that were backed up by the other client. For help with redirected restores, refer to the *NetBackup User's Guide.*

Note When you have finished restoring encrypted files from the client, rename or delete the key file created above, and move or rename your own key file to its original location or name. If you do not re-establish your key file to its original location / name, you may not be able to restore your own encrypted backups.

Setting Encryption in NetBackup Policies

Each NetBackup policy includes an Encryption attribute. This attribute must be set on a master server. For more details on configuring NetBackup policies, see the *NetBackup System Administrator's Guide, Volume I.*

Changing Client Encryption Settings from the NetBackup Server

It is possible to change the encryption settings for a NetBackup client from the Client Properties dialog on the NetBackup master server.

▼ **To change the client encryption settings from the NetBackup server:**

1. From the NetBackup Administration Console on the server, expand the **Host Properties** node and select **Clients**.

2. In the Clients list, double click the name of the client you want to change. The Client Properties dialog displays.

3. In the Properties pane, click **Encryption** to display the encryption settings for that client.

The settings on this dialog correspond to the options described in “Managing NetBackup Encryption Configuration Options” on page 30. For additional explanation of the settings, click the **Help** button on the dialog, or see the *NetBackup System Administrator's Guide, Vol I.*

Additional Key File Security (UNIX clients only)

This section applies only to UNIX NetBackup clients. The additional security described here is not available for Windows clients.

Note We do not recommend using the additional key file security feature in a cluster.

The key file for an Encryption client is encrypted using a DES key generated from a key file pass phrase. By default, the key file is encrypted using a DES key generated from the standard key file pass phrase that is hardcoded into NetBackup.

Using the standard key file pass phrase makes it possible to perform automated encrypted backups and restores in much the same way as non-encrypted backups and restores.

However, if an unauthorized person gains access to your client’s key file, that person may be able to figure out what encryption keys you use for backups or use the key file to restore your client’s encrypted backups. That’s why it is important that only the administrator of the client should have access to the key file.

For extra protection, you can use your own key file pass phrase to generate the DES key to encrypt the key file. If an unauthorized person gains access to this key file, it is much more difficult for that person to use the key file to attempt to restore your client's backed up files.

If you use your own key file pass phrase, backups and restores are no longer as automated as before. Following is a description of what happens on a UNIX NetBackup client if you have used your own key file pass phrase.

When a NetBackup server wants to start a backup or restore on a client, it connects to the `bpcd` daemon on the client and makes a request.

Normally, `bpcd` is configured in the `/etc/inetd.conf` file on the client and is initiated through the `inetd` daemon.

To perform an encrypted backup or restore, `bpcd` needs to decrypt and read the key file.

If the standard key file pass phrase is used, `bpcd` can decrypt the key file automatically and the normal `inetd` method can be used to initiate `bpcd`.

If you use your own key file pass phrase, `bpcd` can no longer decrypt the key file automatically and the `inetd` method cannot be used. You must initiate `bpcd` as a standalone program, as described in the following section.

Note In a clustered environment, if you change the key file on one node, you must make the same change in the key file on all nodes.

Running bpcd as a Standalone Program

1. Edit the `/etc/inetd.conf` file by removing or commenting out the `bpcd` entry. The `bpcd` entry looks something like this:

```
bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd
```

2. Force `inetd` to reread its configuration file. The method to force `inetd` to reread its configuration file varies from platform to platform. The easiest method is to reboot the machine.

3. Change the key file pass phrase. Use the `-change_key_file_pass_phrase` (or `-ckfpp`) option on the `bpkeyfile` command to do this. For example:

```
bpkeyfile -ckfpp /usr/openv/netbackup/keyfile
Enter old key file pass phrase: (standard key file pass phrase)
Enter new key file pass phrase: (standard key file pass phrase)
******
Re-enter new key file pass phrase: (standard key file pass
phrase) ******
```

If you type a carriage return at the prompt, the standard key file pass phrase will be used.

4. Initiate bpcd as a standalone program. Do this by entering the bpcd command with the -keyfile option and then entering the new key file pass phrase when prompted.

```
bpcd -keyfile
Please enter key file pass phrase: ******
```

bpcd now runs in the background waiting for requests from the NetBackup server.

You can change the key file pass phrase at any time with the bpkeyfile command and the -ckfpp option. The new key file pass phrase does not take effect until the next time you start bpcd.

You can also change the NetBackup pass phrase (used to generate the DES keys to encrypt backups) at any time with the bpkeyfile command and the -cnpp option. However, the new NetBackup pass phrase does not take effect until you kill the current bpcd process and restart bpcd.

Terminating bpcd

To terminate `bpcd` on UNIX clients, use the `ps` command to find its process ID and issue the `kill` command for that process ID. Then use `ps` to verify that `bpcd` has been terminated. For most UNIX clients, you can use the `-ef` argument on the `ps` command.

For example:

```
ps -ef | grep bpcd
  root 148 1 0 00:18:30 ? 0:00 bpcd
 kill 148
ps -ef | grep bpcd
```

Index

Numerics

40-bit DES key
  introduction 2
  library 5, 6
56-bit DES key
  introduction 2
  library 7

A

accessibility features vi
allow server directed restores attribute 16, 28
allowed (encryption option) 18, 30
alternate client restore (see redirected restore)
attribute for encryption 3

B

bp.conf file 16, 28
bpcd 5, 6
  running 36
  terminating 38
bpinst command 5, 6
  for setting encryption attribute 28
  pushing pass phrases to clients 26
bpkeyfile command 5, 6, 31, 34, 36
bpkeyutil command 4, 5, 20

C

change_netbackup_pass_phrase 32
checksum of DES key 5, 6, 7
  standard encryption 4
class
  see policy
client libraries
  copying from server 17, 29
client_libraries option, see update_libraries option
clustered environments 27
cnpp option 32
configuration
  and clustering 24, 25
  and clustering (standard) 13
  options 30
  options (standard) 18
  pushing to clients 26
configuring
  clients for encryption, from client 28
  clients for encryption, from client (standard) 16
copying
  client libraries from master server 17, 29
  encryption software to clients 25
  encryption software to clients (standard) 14
CRYPT option 28
CRYPT_KEYFILE option 5, 6, 31
CRYPT_KIND option 18, 30
CRYPT_LIBPATH option 5, 6, 18, 29, 31
CRYPT_OPTION 3, 18, 26, 30
CRYPT_STRENGTH option 6, 26, 30

D

decryption
  of key file 36
  overview 5
  overview (legacy) 6
  overview (standard) 5
denied (encryption option) 18, 30
DES
  key checksum 5, 6, 7
  key checksum for standard encryption 4
DISALLOW_SERVER_WRITES 16, 28

E

encrypted backup, restoring 20, 34
encryption
  allow, deny, require 18, 30
  attribute, setting 21, 28

configuration options 30
configuration options (standard) 18
configuring from client 28
configuring from client (standard) 16
feature overview 1
file containing keys for 31
kind, defining 18, 30
legacy
    prerequisites 5
    prerequisites for restoring 6
    tar header 7
libraries, defining 31
of key file 36
overview 5
overview (legacy) 6
overview (standard) 5
policy attribute for, how to set 3
prerequisites 4
software, obtaining 16, 28
standard
    prerequisites for restoring 5
    tar header 5
strength, defining 30
tar header
    legacy 6
    standard 4
what is and isn't encrypted (legacy) 6
what is and isn't encrypted (standard) 4

G

Glossary. *See* NetBackup Help.

I

inetd.conf 36
installation
    and clustering 10
    clustering and 9
    copying encryption to clients 25
    copying encryption to clients (standard) 14
    directories 16, 28
    pushing configuration to clients 26
    pushing pass phrases to clients 26

K

key file 4, 5, 6, 26
    backing up 33
    creating 31
    defining 31
    encrypting 31
    encrypting with admin's pass phrase 36
    for redirected restore 20, 34
    in a cluster 19, 31, 35, 36
    introduction 2
    legacy 5
    pass phrase 36
    pass phrase, introduction 3
key, introduction 2

L

libraries
    defining for encryption 31

M

managing key file 31

O

obtaining encryption software 16, 28
overview
    of legacy restore 6
    of restore 5
    of standard restore 5

P

pass phrase
    for encrypting key file 32, 36
    for redirected restore 20, 34
    introduction 2
    pushing to clients 26
passphrase_prompt option 26
passphrase_stdin option 26
ps command 38
pushing
    configuration to clients 26
    pass phrases to clients 26
    software to clients 25
    software to clients (standard) 14

R

redirected restore
    of other client's backup 20, 34
    preventing 27
required (encryption option) 18, 30
restore
    of encrypted backup 20, 34
    overview 5
    overview (legacy) 6
    overview (standard) 5

S

server writes not allowed 16, 28
setting encryption attribute 21, 28

software, obtaining 16, 28
standard key file pass phrase
  introduction 3

T

tar header for legacy encryption 6, 7
tar header for standard encryption 4, 5
terminology 1