

VERITAS NetBackup™ Encryption 3.4

System Administrator's Guide

June 2000
100-001508


VERITAS

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.

Copyright

Copyright © 1998-2000 VERITAS Software Corporation. All rights reserved. VERITAS is a registered trademark of VERITAS Software Corporation. The VERITAS logo and VERITAS NetBackup are trademarks of VERITAS Software Corporation. All other trademarks or registered trademarks are the property of their respective owners.

Portions of this software are derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm. Copyright 1991-92, RSA Data Security, Inc. Created 1991. All rights reserved.

Printed in the USA, June 2000.

VERITAS NetBackup Encryption System Administrator's Guide

VERITAS Software Corporation
1600 Plymouth St.
Mountain View, CA 94043
Phone 650.335.8000
Fax 650.335.8050
<http://www.veritas.com>



Contents

About This Guide	v
Audience	v
Organization	v
Related Manuals	v
Conventions	vi
Type Style	vi
Notes and Cautions	vi
Key Combinations	vi
Command Usage	vi
Getting Help	vii
Chapter 1. Introduction	1
Terminology	1
Technical Overview	2
How an Encrypted Backup Works	3
How an Encrypted Restore Works	4
Chapter 2. Installation on Master Server	7
Installation Prerequisite	7
Installing on a UNIX NetBackup Master Server	7
Installing on a Windows NT/2000 NetBackup Master Server	8
Chapter 3. Configuration	11
Configuring from the Master Server	11



Read This If Clients Have Not Been Previously Configured	12
Pushing NetBackup Encryption Software to Clients	12
Pushing the NetBackup Encryption Configuration to Clients	13
Pushing Encryption Pass Phrases to Clients	14
Setting the Encryption Attribute in NetBackup Classes	15
Configuring NetBackup Encryption on the Client	15
Obtaining NetBackup Encryption Software	15
Managing NetBackup Encryption Configuration Options	17
Managing the NetBackup Encryption Key File	18
Setting Encryption in NetBackup Classes	19
Additional Key File Security (UNIX clients only)	19
Running bpcd as a Standalone Program	20
Terminating bpcd	21
Appendix A. Commands	23



About This Guide

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.

Audience

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

Organization

- ◆ Chapter 1, "Introduction," is an overview of the product's capabilities.
- ◆ Chapter 2, "Installation on Master Server," explains how to install NetBackup Encryption.
- ◆ Chapter 3, "Configuration," explains how to configure your system to use NetBackup Encryption. This information supplements that in the NetBackup Windows NT Server and UNIX system administrator's guides.
- ◆ Appendix A, "Commands," describes the commands required for installing and configuring encryption.

Related Manuals

- ◆ *NetBackup System Administrator's Guide - Windows NT/2000*
Explains how to configure and manage NetBackup on a Windows NT system.
- ◆ *NetBackup System Administrator's Guide - UNIX*
Explains how to configure and manage NetBackup on a UNIX system.



Conventions

The following explains typographical and other conventions used in this guide.

Type Style

Table 1. Typographic Conventions

Typeface	Usage
Bold fixed width	Input. For example, type cd to change directories.
Fixed width	Paths, commands, filenames, or output. For example: The default installation directory is <code>/opt/VRTSxx</code> .
<i>Italics</i>	Book titles, new terms, or used for emphasis. For example: <i>Do not</i> ignore cautions.
<i>Sans serif</i> (italics)	Placeholder text or variables. For example: Replace <i>filename</i> with the name of your file.
Sans serif (no italics)	Graphical user interface (GUI) objects, such as fields, menu choices, etc. For example: Enter your password in the Password field.

Notes and Cautions

Note This is a Note and is used to call attention to information that makes it easier to use the product or helps you to avoid problems.

Caution This is a Caution and is used to warn you about situations that can cause data loss.

Key Combinations

Some keyboard command sequences use two or more keys at the same time. For example, you may have to hold down the **Ctrl** key before you press another key. When this type of command is referenced, the keys are connected by plus signs. For example:

Press **Ctrl+t**

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*

the user can use either the *arg1* or *arg2* variable.

Getting Help

For updated information about this product, including system requirements, supported platforms, supported peripherals, and a list of current patches available from Technical Support, visit our web site:

<http://www.veritas.com/>

For product assistance, contact VERITAS Customer Support.

US and Canadian Customers: 1-800-342-0652

International Customers: +1 (650) 335-8555

VERITAS Customer Support can also be reached through electronic mail at:

support@veritas.com





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

- ◆ Encryption with 40-bit DES.
- ◆ Encryption with 56-bit DES (also includes 40-bit DES).

Note The `CRYPT_OPTION`, `CRYPT_STRENGTH`, `CRYPT_LIBPATH`, and `CRYPT_KEYFILE` configuration options mentioned in this manual are in the `bp.conf` file on UNIX and Macintosh clients and in the registry on Microsoft Windows clients. You can also use the NetBackup Administration interface on a Windows NT/2000 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 - Windows NT/2000* for details).

Terminology

The following are some terms that will be useful in understanding and using NetBackup Encryption.

DES

DES (Data Encryption Standard) is a symmetric-encryption block cipher. The same secret encryption key is used to encrypt and decrypt the data. NetBackup Encryption uses DES to encrypt backups.

56-bit DES Key

A standard 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.



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 phrase 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 phrase 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

The following provides an overview of how NetBackup Encryption operates during backups and restores.



How an Encrypted Backup Works

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

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

CRYPT_OPTION	Encryption Class Attribute	
	Yes	No
REQUIRED	Encrypted	None
ALLOWED	Encrypted	Non-encrypted
DENIED	None	Non-encrypted

The prerequisites for encrypting a 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.
- ◆ 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`, `s1`, or `d11` 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`, `s1`, or `d11` 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.

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 an Encrypted 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`, `s1`, or `d11` 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`, `s1`, or `d11` 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:



1. The server sends file names, attributes, and encrypted file data to the client to be restored.
2. 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.
3. 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.
4. 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 Master Server

2

You must first install NetBackup Encryption on either a UNIX or Windows NT/2000 NetBackup master server. When this installation is complete, you can then install and configure it on the clients as explained in Chapter 3, "Configuration."

Installation Prerequisite

The master servers for the clients that require encrypted backups must be running NetBackup 3.4 server software. For a list of the platforms on which you can install NetBackup Encryption, see the *NetBackup Release Notes*.

Installing on a UNIX NetBackup 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 (40 or 56-bit) has been registered by executing the following to list and add keys:

```
/usr/openv/netbackup/bin/admincmd/get_license_key
```
3. Insert the CD-ROM containing the NetBackup Encryption software (40 or 56-bit) 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, execute the following:

```
./install
```

A message states which version of NetBackup Encryption will be installed. When asked if you want to continue, answer **y**.



6. 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 11.

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 choosing **Configure** on the **Actions** menu 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 15.

Installing on a Windows NT/2000 NetBackup Master Server

1. Log in as Administrator on the Windows NT/2000 NetBackup server.
2. Make sure a valid license key for NetBackup Encryption (40 or 56-bit) has been registered by doing the following to list and add keys:
 - a. From the NetBackup Administration window, choose **Help**.
 - b. From the **Help** menu, select **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 Encryption in 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 NT/2000 Readme files
 - ◆ Install NetBackup Encryption for Windows NT/2000



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

D:\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 11.

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 **Configure** on the **Actions** menu 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 15.





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 Classes
- ◆ Additional Key File Security (UNIX clients only)

Note The `CRYPT_OPTION`, `CRYPT_STRENGTH`, `CRYPT_LIBPATH`, and `CRYPT_KEYFILE` configuration options mentioned in this chapter are in the `bp.conf` file on UNIX and Macintosh clients and in the registry on Microsoft Windows clients. You can also use the NetBackup Administration interface on a Windows NT/2000 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 - Windows NT/2000* 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 NetBackup Encryption client software must be installed into a directory on the master server as described in Chapter 2, "Installation on Master Server."
- ◆ 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 3.4 or later.
- ◆ The NetBackup configuration on the clients must allow server writes.

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 **Configure** on the **Actions** menu in the client-user interface).

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 15.

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

- ◆ For a Windows NT/2000 server, the `bin` directory is:

```
install_path\NetBackup\bin
```

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

```
/usr/opensv/netbackup/bin
```

See the `bpinst` command description in Appendix A 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 on the `bpinst` command. However, if you include the `-class_names` option, you will specify class names instead and this will affect all clients in the specified classes.

Read This If Clients Have Not Been Previously Configured

If you are using `bpinst -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 -CRYPT -client_libraries /usr/opensv/lib/client clientname1  
bpinst -CRYPT -passphrase_prompt clientname1
```

If you try to specify both the `-client_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.

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 `-client_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 -CRYPT -client_libraries /usr/opensv/lib/client client1 client2
```

Assume that you want to install the client software on all clients in the NetBackup classes class1 and class2. You would enter a command like this (all on one line):

```
bpinst -CRYPT -client_libraries /usr/opensv/lib/client -class_names  
class1 class2
```

For Windows NT/2000 master servers, you would use the following commands:

```
bpinst.exe -CRYPT -client_libraries ignore client1 client2  
bpinst.exe -CRYPT -client_libraries ignore class_names client1 client2
```

Note On a Windows NT/2000 master server, the `-client_libraries` option must be specified with the `ignore` argument.

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 classes class1 and class2 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 -CRYPT -crypt_option required -crypt_strength 56 -class_names  
class1 class2
```

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 NT/2000 NetBackup master server (the command is all on one line):

```
bpinst.exe -CRYPT -crypt_option allowed -crypt_strength 40 client1  
client2
```



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 -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 NT/2000 NetBackup master server. You would enter commands like the following:

```
bpinst.exe -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 alternate client restores between clients that use the same pass phrase.

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

Setting the Encryption Attribute in NetBackup Classes

Each NetBackup class includes an Encryption attribute.

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

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

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

Suppose you want to set the Encryption attribute for `class1` and `class2` from a UNIX NetBackup master server. You would enter a command like this:

```
bpinst -CRYPT -class_encrypt 1 -class_names class1 class2
```

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 For Macintosh clients, you must configure NetBackup Encryption from the master server. You cannot configure it directly on the client.

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 or Macintosh 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 **Configure** on the **Actions** menu in the client-user interface).



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

- ◆ Windows NT/2000 master server:

install_path\lib\client

- ◆ UNIX master server:

/usr/opensv/lib/client

The client 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 library or libraries for that hardware platform and operating system.

You must copy the library or libraries 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/opensv/lib

Suppose you have a Solaris 2 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/opensv
mkdir lib
cd lib
ftp master
ftp> cd /usr/opensv/lib/client/Sun4/Solaris2
ftp> binary
ftp> mget *
ftp> quit
```

The library names are:

libvdes40.*suffix*
libvdes56.*suffix*

Where *suffix* is `so`, `s1`, or `d11` depending on the platform. You need `libvdes40.suffix` to use 40-bit DES keys. You need both `libvdes40.suffix` and `libvdes56.suffix` to use 56-bit DES keys.



Managing NetBackup Encryption Configuration Options

There are four encryption related configuration options 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. 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_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/opensv/lib/`

The default value on Windows NT/2000, 98, and 95 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 NT/2000, 98, and 95 systems is:

```
install_path\NetBackup\bin\keyfile.dat
```

The default value on UNIX systems is:

```
/usr/opensv/netbackup/keyfile
```

Managing the NetBackup Encryption Key File

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 Appendix A for a detailed description.

The first thing you need to do is to create a key file if it does not already exist. The file name should be the same as the file name specified with the `CRYPT_KEYFILE` configuration option.

- ◆ For Windows NT/2000, 98, and 95 clients, the default key file name is:

```
install_path\NetBackup\bin\keyfile.dat
```

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

```
/usr/opensv/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 19 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 19, 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/opensv/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 `-cnbpp`) 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 NT/2000 client. You would enter a command like this:

```
bpkeyfile.exe -cnbpp 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 class 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 an alternate 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.

Setting Encryption in NetBackup Classes

Each NetBackup class includes an Encryption attribute. This attribute must be set on a master server. For more details, see "Configuring from the Master Server" on page 11.

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 NT/2000, 98, 95, or Macintosh clients.



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.

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/opensv/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/opensv/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`, 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 `-e` argument on the `ps` command. For Solaris 4 and Auspex clients, use the `-ax` argument on the `ps` command.

For example, from a Solaris 2 client:

```
ps -e | grep bpcd
  148 ?          0:22 bpcd
kill 148
ps -e | grep bpcd
```

For example, from an Auspex client:

```
ps -ax | grep bpcd
  389 ? S        6:46  0:22 bpcd
kill 389
ps -ax | grep bpcd
```





This appendix describes commands that are specific to the NetBackup Encryption product.

The following are special conventions used in the command description.

- ◆ Brackets [] mean that the enclosed command line component is optional. For example, assume that a command has the following format:

```
command [arg1]
```

The user can either choose arg1 or omit it.

- ◆ A vertical bar (or pipe) symbol | separates optional arguments. For example:

```
command [arg1 | arg2]
```

The user can choose arg1 or arg2 (not both), or can omit both.

- ◆ Italics indicate that the information is user supplied. For example, the user supplies *directory* in the following command:

```
-client_libraries directory
```



bpinst(1M)

NAME

bpinst - when used with the `-CRYPT` option, installs and configures NetBackup Encryption

SYNOPSIS

```
bpinst -CRYPT [-client_libraries directory] [-crypt_option
              option] [-crypt_strength strength] [-passphrase_prompt
              | -passphrase_stdin] [-verbose] [ [-class_encrypt 0 |
              1] -class_names] name1 [name2 ... nameN]
```

Note You must have NetBackup Encryption, a separately priced product, in order to use this command.

DESCRIPTION

Note If you are using `bpinst -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 -CRYPT -client_libraries /usr/opensv/lib/client
clientname1
```

```
bpinst -CRYPT -passphrase_prompt clientname1
```

If you try to specify both the `-client_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.

`bpinst`, used with the `-CRYPT` option, installs and configures the NetBackup Encryption product on NetBackup clients that can support encryption. On UNIX the command is located in the `/usr/opensv/netbackup/bin` directory. On Windows NT/2000, the command is located in the `install_path\NetBackup\bin` directory.

Before using this command, install the encryption software on the server as explained in Chapter 2 in the *NetBackup Encryption System Administrator's Guide*. Then, execute `bpinst -CRYPT` on the master server to install and configure NetBackup Encryption on the clients. A single execution copies the required files to the selected clients and also makes the necessary configuration changes on both the clients and the master server.

Note Ensure that the `DISALLOW_SERVER_FILE_WRITES` NetBackup configuration option is not set on the client. If this option is set, the server cannot install and configure the software on the client.

In the following example, `bpinst -CRYPT` installs and configures 40-bit DES encryption software on all the UNIX clients in the class named `class40` (the command is all on one line).

```
bpinst -CRYPT -client_libraries /usr/opensv/lib/client -crypt_option
allowed -crypt_strength des_40 -passphrase_prompt -class_encrypt 1
-class_names class40
```

The above command uses the `-class_encrypt` option to set the Encryption attribute for the class. You can also use the NetBackup administrator utility to set the Encryption attribute.

See the `OPTIONS` section for an explanation of all options used with `bpinst -CRYPT`. (Pay special attention to the `-passphrase_prompt` option.)

Note You can also configure encryption for a client that is installed on the master server host.

OPTIONS

- `-CRYPT` Required and must be the first option specified in order to use the `bpinst` command to install or configure encryption. The order is important and do not omit this option.
- `-client_libraries directory`
Installs the encryption libraries on NetBackup clients. This option points to the directory on the master server that contains the client encryption libraries:
On a UNIX server, the library directory is:
`install_path/lib/client`
(by default, `install_path` is `/usr/opensv`)
On a Windows NT/2000 server, the library directory must be:
`ignore`
- `-crypt_option option`
Configures the `CRYPT_OPTION` configuration entry on the NetBackup clients. If you do not specify `-crypt_option`, the client allows either encrypted or unencrypted backups (see `ALLOWED` below).
The possible values for `option` are:
`DENIED | denied | -1`



Specifies that the client does not permit encrypted backups. If the server requests an encrypted backup, it is considered an error. This option is the default for a client that has not been configured for encryption.

ALLOWED | allowed | 0

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

REQUIRED | required | 1

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

`-crypt_strength strength`

Configures the CRYPT_STRENGTH configuration entry on the NetBackup clients. If you do not specify this option, the CRYPT_STRENGTH configuration entries on the clients remain unchanged.

The possible values for *strength* are:

DES_40 | des_40 | 40

Specifies 40-bit DES encryption. This is the default value for a client that has not been configured for encryption.

DES_56 | des_56 | 56

Specifies 56-bit DES encryption.

`-passphrase_prompt` | `-passphrase_stdin`

Caution Do not forget the pass phrase. If the key file is damaged or lost, you may need the pass phrase in order to regenerate the key file. Without the proper key file, you cannot restore encrypted backups.

NetBackup uses a pass phrase to create data that it places in a key file on each client. NetBackup then uses the data in the key file to create the encryption keys required to encrypt and decrypt the backup data.

The `-passphrase_prompt` option prompts you to enter a pass phrase. The actual pass phrase is hidden while you type.

The `-passphrase_stdin` option reads the pass phrase through standard input. You must enter the pass phrase twice. This option is less secure than the `-passphrase_prompt` option because the pass phrase is not hidden. However, it may be more convenient if you are using `bpinst -CRYPT` in a shell script.

NetBackup uses the pass phrase for all the clients that you specify on the `bpinst -CRYPT` command. If you want separate pass phrases for each client, enter a separate `bpinst -CRYPT` command for each client.

When you specify a pass phrase, `bpinst -CRYPT` creates or updates the key files on the clients. Encryption keys generated from the pass phrase are used for subsequent backups. Old encryption keys are retained in the key file in order to allow restores of previous backups.

If you do not specify either the `-passphrase_prompt` or `-passphrase_stdin` option, the key files on the clients remain unchanged.

- verbose Prints the current encryption configuration of each client and what gets installed and reconfigured on each client.
- class_names Specifies that the names you specify with the *names* option are NetBackup class names.
If you include the `-class_names` option, `bpinst -CRYPT` installs and configures all the clients in each class specified.
If you omit the `-class_names` option, the names are assumed to be NetBackup client names.
- class_encrypt 0 | 1 Sets the Encryption class attribute for the NetBackup classes. You can include `-class_encrypt` only with the `-class_names` option. The possible values are:
0 clears the Encryption attribute (or leaves it clear) so the server does not request encryption for clients in this class. This is the default for classes that are not configured for encryption.
1 sets the Encryption attribute so the server requests encryption for clients in this class.
If you do not specify this option, the Encryption attributes for the classes remain unchanged.
- name1* [*name2* ... *nameN*] One or more NetBackup client or class names, depending on whether you have included the `-class_names` option. If you omit the `-class_names` option, the names are assumed to be NetBackup client names.

EXAMPLES

Example 1

You must install the encryption libraries on the NetBackup master server before installing and configuring the clients. The following command installs the libraries on a NetBackup client named mars (one line):



On UNIX:

```
bpinst -CRYPT -client_libraries /usr/opensv/lib/client mars
```

On Windows NT/2000:

```
bpinst.exe -CRYPT -client_libraries ignore mars
```

Example 2

The following command (all on one line) installs and configures 40-bit DES encryption on UNIX clients in a class named class40:

```
bpinst -CRYPT -client_libraries /usr/opensv/lib/client -crypt_option  
allowed -crypt_strength des_40 -class_encrypt 1 -passphrase_prompt  
-client_names class40
```

Because the command includes the `-passphrase_prompt` option, you are prompted for a pass phrase.

```
Enter new NetBackup pass phrase: *****
```

```
Re-enter new NetBackup pass phrase: *****
```

Example 3

The following command (all on one line) specifies that the NetBackup client named strong must use 56-bit DES encryption:

```
bpinst -CRYPT -crypt_option required -crypt_strength des_56 strong
```

Example 4

The following command displays a verbose listing of the configuration for the client named strong:

```
bpinst -CRYPT -verbose strong
```

```
BPCD protocol version 3.1.0 on client strong
```

```
40-bit library version is 3.1.0.40 on client strong
```

```
56-bit library version is 3.1.0.56 on client strong
```

```
BPCD platform is sgi5 for client strong
```

```
Current configuration entries are:
```

```
CRYPT_KEYFILE = /usr/opensv/netbackup/keyfile
```

```
CRYPT_LIBPATH = /usr/opensv/lib
```

```
CRYPT_OPTION = 1
```

```
CRYPT_STRENGTH = 56
```

```
About to update 40-bit DES library for client strong
```

```
No update of 40-bit DES library required for client strong
```

```
About to update 56-bit DES library for client strong
```



No update of 56-bit DES library required for client strong
 About to update NetBackup configuration for client strong
 No update of NetBackup configuration required for client strong
 About to update NetBackup pass phrase for client strong
 No update of NetBackup pass phrase required for client strong

NOTES

- ◆ The pass phrase that `bpinst -CRYPT` sends over the network to a client is encrypted by a privately defined NetBackup 40-bit DES key.
- ◆ The key file on each NetBackup client is encrypted with a privately defined NetBackup DES key. The key can be 40 bit or 56 bit, depending on how the client is configured. Restrict access to the key file to the administrator of the client machine. On a UNIX client, the owner of the key file should be root and the mode bits should be 600. The key file should not be exportable through NFS.
- ◆ It is very important to remember pass phrases. In a disaster recovery situation, you may have to recreate a key file on a client by using `bpinst -CRYPT`. For example, suppose a NetBackup client named `orca` has been performing encrypted backups and an accident occurs that causes `orca` to lose its files. In this case you must reinstall and configure encryption on the client in order to restore your backups.

The following is the basic procedure for disaster recovery when using encryption (see the *NetBackup Troubleshooting Guide* for details on restoring the operating system and NetBackup). This example assumes a NetBackup client named `orca`.

1. Reinstall the OS on `orca`.
2. Reinstall and configure the NetBackup client software on `orca`.
3. Reinstall and configure encryption on `orca` by executing the following command (one line):

```
bpinst -CRYPT -client_libraries /usr/opensv/lib/client -crypt_option
allowed -passphrase_prompt orca
```

```
Enter new NetBackup pass phrase: *****
```

```
Re-enter new NetBackup pass phrase: *****
```

The pass phrase that you enter here is the first one used on `orca`.

4. Execute `bpinst -CRYPT` for each subsequent pass phrase used on `orca`:

```
# bpinst -CRYPT -passphrase_prompt orca
```

```
Enter new NetBackup pass phrase: *****
```

```
Re-enter new NetBackup pass phrase: *****
```

5. Restore the backed up files to `orca`.



FILES

UNIX:

- ◆ UNIX server command
`/usr/opencv/netbackup/bin/bpinst`
- ◆ UNIX server directory with client libraries
`/usr/opencv/lib/client/`
- ◆ UNIX client encryption libraries
`/usr/opencv/lib/libvdes*.*`
- ◆ UNIX client encryption key file
`/usr/opencv/netbackup/keyfile`
- ◆ UNIX client encryption key file utility
`/usr/opencv/netbackup/bpkeyfile`

Windows NT/2000, 98, or 95:

- ◆ Windows NT/2000 server command
`install_path\NetBackup\bin\bpinst.exe`
- ◆ Windows NT/2000 server directory with client libraries
`install_path\lib\client\`
- ◆ Windows NT/2000, 98, or 95 client encryption key file
`install_path\NetBackup\bin\keyfile.dat`
- ◆ Windows NT/2000, 98, or 95 client encryption libraries
`install_path\bin\libvdes*.dll`
- ◆ Windows NT/2000, 98, or 95 client encryption key file utility
`install_path\bin\bpkeyfile.exe`

Macintosh:

- ◆ Macintosh client encryption libraries
`:System Folder:Extensions:libvdes*.dll`
- ◆ Macintosh client encryption key file
`:System Folder:Preferences:NetBackup:keyfile`



bpkeyfile(1)

NAME

bpkeyfile - encryption key file utility for NetBackup

SYNOPSIS

```
bpkeyfile [-stdin] [-change_key_file_pass_phrase]
          [-change_netbackup_pass_phrase] [-display] key_file_path
```

AVAILABILITY

The bpkeyfile command is available only with the NetBackup Encryption option.

DESCRIPTION

bpkeyfile creates or updates a file that contains information used to generate DES encryption keys. The information is generated based on a NetBackup pass phrase that you supply. The key file is encrypted by a key-file pass phrase that you supply.

The NetBackup client software uses an encryption key calculated from information in the key file to encrypt files during backups or decrypt files during restores.

If the file exists, you are prompted to enter the current key-file pass phrase.

If you specify `-change_key_file_pass_phrase`, you are prompted for a new key file-pass phrase. If you enter an empty pass phrase, a standard key-file pass phrase is used.

If you use the standard key-file pass phrase, bpcd can be run automatically. If you use your own key-file pass phrase, start bpcd with the `-keyfile` argument as explained under “Additional Key File Security (UNIX clients only)” in Chapter 3 of the *NetBackup Encryption System Administrator’s Guide*.

OPTIONS

- `-stdin` Read pass phrases from standard input. By default, bpkeyfile reads pass phrases from terminal input.
- `-change_key_file_pass_phrase` (or `-ckfpp`)
Change the pass phrase used to encrypt the key file.
- `-change_netbackup_pass_phrase` (or `-cnpp`)
Change the pass phrase used to encrypt NetBackup backups and archives on this client.
- `-display`
Display information about the key file.



key_file_path

The path of the key file to be created or updated by `bpkeyfile`.

NOTES

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. Space character (code 32) to tilde character (code 126).

FILES

UNIX:

`/usr/opensv/netbackup/keyfile`

(UNIX client encryption key file)

Windows NT/2000, 98, or 95:

`install_path\NetBackup\bin\keyfile.dat`

(Windows NT/2000, 98, or 95 client encryption key file)