

BaReLib

Backup/Restore Library
Version 110

Users Guide

29. August 2005


Software & Consulting

Karl-Heinz Weber
Heinrichstraße 12
D-45711 Datteln/Horneburg

Document History 2nd Edition 29. August 2005 Release BaReLib 100

**Trademarks or
Service Marks**

The following are trademarks or service marks of Tandem Computers Incorporated:
Atalla, Challenge/Response, Enform, Expand, Guardian, Guardiango, Inspect, Multilan, NonStop, TACL, Tandem.
All brand names and product names are trademarks or registered trademarks of their respective companies.

The following are trademarks or service marks of *GreenHouse Software & Consulting*:
\$ARROW, \$AS, CRYSTAL, CURIOUS, FTPSERV-E, FUNCTRAC, MPWD, MPWD-L, PASSYNC, SECMAN, SECOM, GSTK, SSTK.

The following are trademarks or service marks of Jelinek EDV:
SECMAN

Copyright

Copyright © 2005 by *GreenHouse Software & Consulting*. All rights reserved. No part of this document may be reproduced in any form, including photo copying or translation to another language, without prior written consent of *GreenHouse Software & Consulting*.
Printed in Germany.

Please Comment

If you have questions or problems concerning the content of this document, please let me know! Send your comments to:
GreenHouse Software & Consulting
Karl-Heinz Weber
Heinrichstraße 12
D-45711 Datteln/Horneburg
Germany
Phone +49 (0)2363 72566
Fax +49 (0)2363 66106
Mobile +49 (0)172 23 18248
E-Mail: Info@GreenHouse.de
Internet: www.GreenHouse.de
PGP fingerprint: 3A32 D90A D125 5418
 1150 2484 6629 2DD2



The Backup/Restore Library (BaReLib) is a new product from GreenHouse Software & Consulting. It brings transparently DES encryption to the standard Backup and Restore programs from Tandem computers.

Why securing data on tape?

When you have to backup data, and ship it physically from one place to another, and when you are concerned about the tapes getting lost – then encoding the data on tape is the perfect solution.

Available cryptographic functions

The following DES functions are available in BaReLib, where the user can choose from:

- ECB DES (Electronic Code Book 8*7 bit key time factor 1)
- CBC DES (Cipher Block Chaining 8*7 bit key timefactor 1)
- Triple ECB DES (Triple Electronic Code Book 16*7 bit key timefactor 3)
- Triple CBC DES (Triple Cipher Block Chaining 16*7 bit Ke timefactor 3)
- Trio ECB DES (Trio Electronic Code Book 24*7 bit key timefactor 3)

Cryptographic Key

The necessary cryptographic key is derived from a pass phrase, which is hashed down to the necessary key(s) using Hash Function ISO 10118-2.

The currently possible pass phrase may have a length of 228 bytes: The maximum EDIT line length is 239 bytes, from which the keyword PASSPHRASE and following blank has to be subtracted.

The pass phrase itself can hold any character INCLUDING multiple single blanks (example 1 below). Recurring blanks (example 2 below) are shrunked to single blanks:

e.g. `Hi There Tandem` is unchanged used as: `Hi There Tandem`
`Hi There Tandem` is shrunked to: `Hi There Tandem`

The pass phrase IS case sensitive!

Installation

1. Logon to SUPER.SUPER
This is needed, because the new versions of BACKUP and RESTORE need to become licensed.
2. Create a copy of the original BACKUP and RESTORE files, and name them e.g. SBACKUP and SRESTORE (secure BACKUP/RESTORE).
FUP DUP \$SYSTEM.SYSnn.BACKUP,\$vol.subvol.SBACKUP
FUP DUP \$SYSTEM.SYSnn.RESTORE,\$vol.subvol.SRESTORE
Note:
The SBACKUP program name must match the template: *. \$*. *. *BACKUP
The SRESTORE program name must match the template: *. \$*. *. *RESTORE
3. Set the security of SBACKUP and SRESTORE to: RWEP = "OOAO"
FUP SECURE \$vol.subvol.SBACKUP,"OOAO"
FUP SECURE \$vol.subvol.SRESTORE,"OOAO"
4. FUP LICENSE SBACKUP and SRESTORE
FUP LICENSE \$vol.subvol.SBACKUP
FUP LICENSE \$vol.subvol.SRESTORE
5. Put BaReLib into the same location as SBACKUP and SRESTORE
This is an advice. You can put BaReLib in any location, but it does make sense, to have it 'near' the programs it is attached to.
6. Put BRLIBTOK.101 into the same location as SBACKUP and SRESTORE
7. Set the security of BaReLib to: RWEP = "OOAO"
FUP SECURE \$vol.subvol.BATRELIB,"OOAO"
8. Add BaReLib to SBACKUP and SRESTORE by using the following two commands:
RUN SBACKUP /LIB <barelib>/exit
RUN SRESTORE /LIB <barelib>/exit

You'll get an error message like this one:

```
$GHS1 TAPELIB 72> backup/lib object/exit  
EXIT
```

^

```
*ERROR-7755* Comma expected.
```

```
ABENDED: 1,181
```

```
CPU time: 0:00:00.111
```

```
3: Premature process termination with fatal errors or diagnostics
```

```
Subsystem: TANDEM.74.G07
```

```
$GHS1 TAPELIB 73>
```

But don't worry: The lib is attached anyway!

Instead of doing it 'by hand', you can use the GreenHouse FreeWare tool: BINDLIB, which is part of the delivery:

```
$GHS1 BARELIB 23> bindlib sbackup with barelib
Program $GHS1.BARELIB.SBACKUP bound to library $GHS1.BARELIB.barelib
Number of successful binds: 1
```

```
$GHS1 BARELIB 24> bindlib srestore with barelib
Program $GHS1.BARELIB.SRESTORE bound to library $GHS1.BARELIB.barelib
Number of successful binds: 1
$GHS1 BARELIB 25>
```

9. Use the SHOWLIB tool, which is part of the delivery as well, to check, if BaReLib is successfully attached to SBACKUP and SRESTORE:

```
$GHS1 BARELIB 25> showlib *
SHOWLIB (206) - T7172G06 - (06May2005) System \BEECH, running NSK G06
Copyright (c) GreenHouse Software & Consulting 1999,2001-2003,2005
```

```
Used Program file template: \BEECH.$GHS1.BARELIB.*
Used LIB file template:    \*.$*.*.*
```

```
$GHS1.BARELIB.SBACKUP      -> $GHS1.BARELIB.BARELIB
$GHS1.BARELIB.SRESTORE    -> $GHS1.BARELIB.BARELIB
```

```
Number of object files in error:    0
```

```
Checked files with code 100:        5
```

```
Number of executables:              3
```

```
Total executables with library:     2
```

```
Checked files with code 700:        0
```

```
Number of executables:              0
```

```
Total executables with library:     0
```

```
$GHS1 BARELIB 26>
```

Configuration file

To inform **BaReLib** about the cryptographic function to be used as well as the passphrase to encode the data, these attributes have to be defined in a small **EDIT** type configuration file.

The **EDIT** file does have this structure:

```
!  
! Definition of cryptographic engine.  
! Has to be one of:  
! - NONE  
! - ECB  
! - CBC  
! - TripleECB  
! - TripleCBC  
! - TrioECB  
!  
CODETYPE triplecbc  
  
!  
! Passphrase used to generate the cryptographic key(s)  
! Should be at least 32 bytes long  
!  
PASSPHRASE HalTandonloDuDah0nteN_Sequ!ia_Be,ch_Ginkgo\Te#t  
  
!  
! When CipherBlock Chaining is used, the initial chaining vector  
! can be related to the user, doing the Backup and Restore.  
! This requires the SRestore user to have the same name  
! (GUARDIAN name, e.g. GHS.CARL, or Alias name, e.g. CarlWeber)  
! and optional the same ID (e.g. 100,5) as the user, who  
! performed the Backup.  
! The following attributes are supported:  
! - NO  
! The user, performing the SRestore, can be any.  
! - NAME  
! The user, performing the SRestore, must have the same system  
! name as the user who did the Backup.  
! - NAMEID  
! The user, performing the SRestore, must have the same system  
! name as well as the same user ID as the user who did the Backup.  
!  
SAMEUSER NO
```

Empty lines, and lines beginning with an

- exclamation mark (!)
- double minus sign (--)
- double equal sign (==)

are treated as comment, and are skipped.

Key words are NOT case sensitive.

Keywords

The following keywords are supported:

- CODETYPE
- PASSPHRASE
- SAMEUSER

- **CODETYPE**

Defines the cryptographic function to be used.

This can be one of:

- NONE no cryptographic function is used
- ECB electronig code book
- CBC cipher block chaining
- TripleECB triple ECB DES
- TripleCBC triple CBC DES
- TrioECB trio ECB DES

The keyword CODETYPE and its attributes are NOT case sensitive.

- **PASSPHRASE**

Is the passphrase, from which the cryptographic key(s) are derived.

The passphrase is limited to the maximum EDIT file line length.

The keyword PASSPHRASE is not case sensitive, while the PassPhrase string IS case sensitive!

When PassPhrase is missing, or empty, BaReLib does not perform any cryptographic function.

- **SAMEUSER**

The creator of the **SBACKUP** tape can enforce, that the user, running **SRESTORE**, has to have the same system name (GUARDIAN or Alias name) and optional to have the same user ID. This feature ensures, that only a defined user can successfully restore the tape.

Three options are available:

- NO this feature is shut off: ANY user can restore the tape
- NAME the **SRESTORE** user has to have the same name
- NAMEID the **SRESTORE** user has to have the same system name **AND** user ID

Action Matrix

Crypt Type	PassPhrase	SameUser
NONE	n/a	n/a
ECB	Required	n/a
CBC	Required	optional
TripleECB	Required	n/a
TripleCBC	Required	optional
TrioECB	Required	n/a

Securing the configuration file

Secure the configuration file as tight as possible. The recommended RWEp security is: “oooo”.

Assigning the configuration file

BaReLib uses two methods to get the configurations file name:

1. DEFINE
2. Users default location

1. DEFINE

The configuration file name can be defined as a MAP DEFINE.

The used DEFINE name is: =BARECONF.

The TACL command to set this DEFINE looks like this:

```
ADD DEFINE =BARECONF,CLASS MAP,FILE <BaReConf file name>
```

e.g.

```
ADD DEFINE =BARECONF,CLASS MAP,FILE $ghs1.grenhous.myconf
```

The configuration file name can be any valid disk file name.

2. Users Default Location

In case there is no DEFINE BARECONF, BaReLib checks for a file named BARECONF in the users default location.

Note:

The configuration file in the users default location name MUST be named BARECONF!

In case there is no configuration file available, or in case the configuration file can not be read (e.g. error 48), the library does not use any cryptographic function, and BACKUP/RESTORE work as usual.

Example

1. Create a configuration file with the editor (or use an already existing one), and set the cryptographic type, pass phrase, and SAMEUSER attribut.

2. Define the configuration file, e.g.:

```
ADD DEFINE =BARECONF, CLASS MAP, FILE $ghs1.tapelib.bareconf
```

Or put the file into your default location and name it: BaReCONF.

3. Check the configuration file Define, e.g.:

```
$GHS1 TAPELIB 53> info define =bareconf,detail
Define Name      =bareconf
CLASS            MAP
FILE             \BEECH.$GHS1.TAPELIB.BARECONF
$GHS1 TAPELIB 54>
```

4. Execute SBACKUP

A typical SBACKUP session looks like this:

```
$GHS1 TAPELIB 55> run sbackup $tape0,*,listall,open,nounload,blocksize 52
```

```
File Mode BACKUP Program - T9074G07 (07NOV2003) (AEZ)
```

```
BaReLib (100) - T7172G06 - (21Jul2005) GreenHouse Software & Consulting
```

```
Drives: ($TAPE0)
```

```
System: \BEECH Operating System: G06 Tape Version: 3
```

```
Backup options: NO AUDITED, BLOCKSIZE 52, NO IGNORE, OPEN, PARTONLY OFF,
INDEXES IMPLICIT
```

```
*WARNING-7144* This tape can only be restored with RESTORE (D30 or later).
```

```
*WARNING-7147* Files created and stored via OSS will not be backed up.
```

```
Backup time: 22Jul2005 14:46
```

```
Page: 1
```

Tape: 1	Code	EOF	Last modif	Owner	RWEP	Type	Rec	B1
\$GHS1.TAPELIB								
ACCELERA	101	2492	20Jul2005 10:21	100,5	UUOO			
BACKUP	100L	3584000	4Feb2004 8:14	100,5	OOOO			
BARECONF	101	2470	19Jul2005 14:57	100,5	UUOO			
G304797G	100	159744	22Jul2005 13:21	100,5	UUOO			
OBJECT	100	159744	22Jul2005 14:43	100,5	UUOO			
PROCTEST	100	146146	11Jul2005 10:14	100,5	UUOO			
README	101	10968	22Jul2005 14:44	100,5	UUOO			
RESTORE	100L	3491840	4Feb2004 8:14	100,5	OOOO			
SAVE	101	2980	11Jul2005 17:58	100,5	UUOO			
TAPELIBO	101	100070	21Jul2005 13:14	100,5	OO--			
TAPELIBS	101	80104	22Jul2005 14:42	100,5	OO--			
TAPELIOO	101	67204	11Jul2005 13:07	100,5	OO--			
TEST	100	8252	22Jul2005 13:43	100,5	UUOO			
TESTSRC	101	2642	22Jul2005 13:43	100,5	UUOO			

Summary Information

```
Files dumped = 14 Files not dumped = 0
```

```
BaReFonf file: $GHS1.TAPELIB.BARECONF
```

```
Used cryptographic function: ECB-DES
```

```
Time used to encode data: 00:00'31,283.758
```

```
Bytes encoded: 7.820.206
```

```
$GHS1 TAPELIB 56>
```

The blue lines highlight the information, provided by BaReLib.

5. Ship the tape through one channel, and the configuration file through a different one.

At the remote site, perform these steps:

1. Load the configuration file onto the Tandem system

2. Define the configuration file, e.g.:

```
ADD DEFINE =BARECONF CLASS MAP,FILE $ghs1.tapelib.bareconf
```

3. Check the configuration file Define, e.g.:

```
$GHS1 TAPELIB 53> info define =bareconf,detail
Define Name      =bareconf
CLASS           MAP
FILE            \BEECH.$GHS1.TAPELIB.BARECONF
$GHS1 TAPELIB 54>
```

4. Execute SRESTORE

```
$GHS1 TAPELIB 56> run srestore $tape0,*. *.* ,vol $ghs1.test,purge,listall,nounload
File Mode RESTORE Program - T9074G07 (07NOV2003) (AEZ)
BaReLib (100) - T7172G06 - (21Jul2005) GreenHouse Software & Consulting
Drives: ($TAPE0)
System: \BEECH Operating System: G06 Tape Version: 3
Backup options: NO AUDITED, BLOCKSIZE 52, NO IGNORE, OPEN, PARTONLY OFF,
INDEXES IMPLICIT
Restore time: 22Jul2005 14:48 Backup time: 22Jul2005 14:46 Page: 1
```

Tape: 1	Code	EOF	Last modif	Owner	RWEP	Type	Rec	Bl
\$GHS1.TEST								
	ACCELERA	101	2492 20Jul2005 10:21	100,5	UUOO			
	BACKUP	100L	3584000 4Feb2004 8:14	100,5	OOOO			
	BARECONF	101	2470 19Jul2005 14:57	100,5	UUOO			
	G304797G	100	159744 22Jul2005 13:21	100,5	UUOO			
	OBJECT	100	159744 22Jul2005 14:43	100,5	UUOO			
	PROCTEST	100	146146 11Jul2005 10:14	100,5	UUOO			
	README	101	10968 22Jul2005 14:44	100,5	UUOO			
	RESTORE	100L	3491840 4Feb2004 8:14	100,5	OOOO			
	SAVE	101	2980 11Jul2005 17:58	100,5	UUOO			
	TAPELIBO	101	100070 21Jul2005 13:14	100,5	OO--			
	TAPELIBS	101	80104 22Jul2005 14:42	100,5	OO--			
	TAPELIOO	101	67204 11Jul2005 13:07	100,5	OO--			
	TEST	100	8252 22Jul2005 13:43	100,5	UUOO			
	TESTSRC	101	2642 22Jul2005 13:43	100,5	UUOO			

Summary Information

```
Files restored = 14 Files not restored = 0
BaReFonf file: $GHS1.TAPELIB.BARECONF
Used cryptographic function: ECB-DES
Time used to decode data: 00:00'35,283.017
Bytes decoded: 7.820.206
$GHS1 TAPELIB 57>
```

The blue lines highlight the information, provided by BaReLib.

Access to an encoded tape through the 'normal' BACKUP program

An encoded tape can be listed by BACKUP WITHOUT the need to know any key, or cryptographic function.

Restoring an encoded tape

Restoring data from an encoded tape requires the correct cryptographis method as well as pass phrase and the correct user, as set at BACKUP time.

A wrong method, PassPhrase, or user setting, results in something like this:

```
$GHS1 TAPELIB 64> srestore $tape0, *.* *,vol $ghs1.test,listall,nounload,purge
File Mode RESTORE Program - T9074G07 (07NOV2003) (AEZ)
(C)2000 Compaq (C)2003 Hewlett Packard Development Company, L.P.
Drives: ($TAPE0)
System: \BEECH Operating System: G06 Tape Version: 3
Backup options: NO AUDITED, BLOCKSIZE 52, NO IGNORE, OPEN, PARTONLY OFF,
INDEXES IMPLICIT
*ERROR-2012* $SYSTEM.SYS03.RESTORE : Internal error. String overflow.
STR^PADRIGHT+%27
ARCHTAPEREST^READDATABLOCK+%256
RESTORE^READTAPEBLOCK+%15
RESTORE^READINSTANCE+%4
GENERICRESTOREDATA+%37
RESTORE^DATA+%220
RESTORE^PHYSICALFILE+%515
RESTORE^SINGLEPART+%73
RESTORE^FILE+%1311
RESTORELOOP^ONETAPESET+%637
RESTORELOOP+%463
RESTOREMAIN^PROC+%420
DEJUREMAINPROC+%1
ABENDED: 1,127
CPU time: 0:00:00.125
3: Premature process termination with fatal errors or diagnostics
Subsystem: TANDEM.75.G07
$GHS1 TAPELIB 65>
```

Performance

Using cryptographic functions on a Tandem system is a performance hog for the CPU, where it is executed. To backup 7.5 Mbytes in ECB mode costs some 32 seconds of CPU time on an empty S7000 CPU. Using Triple CBC uses ~100 seconds.

The numbers will decrease dramatically when using newer/better/faster CPUs.

To prevent a CPU from being overloaded by DES, start the BACKUP/RESTORE programs with a very low priority, e.g. 5, or even better: 1 (one). This ensures, that only 'spare cycles' are used.

Safety

I do know, that symmetric cryptographic systems lack a key management.

BaReLib is intended to provide the user with a robust cryptographic mechanism, that secures data on tape. It is NOT intended to provide a sophisticated key management as well.

How will it be used?

When you have to backup data, and ship it physically from one place to another, and when you are concerned about the tapes getting lost, then do this:

1. Create the **BaReConf** configuration file:
 - define the cryptographic method
 - define the PassPhrase
 - optionally set the SameUser attribute
2. Define the configuration file
3. Run **SBACKUP** to backup the data

4. Ship the **SBACKUP** tape through one channel, e.g. UPS, FedEx, what ever.
5. Ship the **BaReConf** file through another channel, e.g.
 - E-Mail, secured by PGP (my favorite)
 - floppy
 - phoneto the target location.

6. Load the configuration file onto the target system
7. Define the configuration file
8. Run **SRESTORE**

Note:

Before you use **BaReLib for production purposes, please test it to get familiar with the handling.**

What to do when the PassPhrase got lost?

Do NOT blame GreenHouse!

No configuration attributes (key or key fragments; pass phrase or pass phrase fragments; cryptographic type used; user attributes) are stored on tape.

There is NO way in recovering a missing PassPhrase/cryptographic key/user attribute.

If you have lost your PassPhrase, you have lost access to the data contained in the Backup. It's just the same as if the tape has been destroyed.

Certified BACKUP/RESTORE programs

BaReLib runs OK in file mode with these versions:

```
$GHS1 BARELIB 45> vproc backup
VPROC - T9617G03 - (07 AUG 2003) SYSTEM \BEECH    Date 25 JUL 2005, 10:08:37
Copyright 2003 Hewlett-Packard Development Company, L.P.
```

```
$GHS1.BARELIB.BACKUP
  Binder timestamp: 04FEB2004 05:10:11
  Version procedure: T9074G07^08MAR2004^BACKUP^AFA
    Target CPU: TNS, TNS/R
  AXCEL timestamp: 04FEB2004 05:21:29
$GHS1 BARELIB 46>
```

```
$GHS1 BARELIB 46> vproc restore
VPROC - T9617G03 - (07 AUG 2003) SYSTEM \BEECH    Date 25 JUL 2005, 10:08:41
Copyright 2003 Hewlett-Packard Development Company, L.P.
```

```
$GHS1.BARELIB.RESTORE
  Binder timestamp: 04FEB2004 05:13:57
  Version procedure: T9074G07^08MAR2004^RESTORE^AFA
    Target CPU: TNS, TNS/R
  AXCEL timestamp: 04FEB2004 05:29:35
$GHS1 BARELIB 47>
```

Used DES code

BaReLib used the GreenHouse FreeWare DES library, which is available from www.greenHouse.de.

Please feel free to check it for

- test programs
- example code and
- performance numbers.

The same code is part of the PAK/UNPAK product from Tandem/HP.