

INNOVATION

April 2006 • Volume 3.0

Focus On: Data Protection Solutions
with FDRCRYPT & FDRERASE also
Data Availability and Volume
Consolidation with FDRPAS &
FDRCOPY and Tape Erasure with FATS

FDRCRYPT...

Innovation Data Processing is pleased to announce a new product: **FDRCRYPT**. FDRCRYPT is an option to FDR. FDRCRYPT is designed to protect the data on your BACKUPS against unauthorized access by anyone who does not possess the proper encryption keys.

Multiple encryption levels provide different strengths of encryption:

- **SUBSTITUTION** – a 128-bit encryption key is used to generate a 256-byte substitution table, where each byte value in the backup data block (after compression) is translated to a different unique byte value.
- **CIPHER** – a 128-bit encryption key is used to generate a byte substitution table (just like SUBSTITUTE) and a transposition table, where each byte in a backup data block is moved to a different location in the backup block so that the data is in a totally different order.
- **AES** – uses the Advanced Encryption Standard algorithm, as approved by the US National Institute of Standards and Technology (NIST). AES uses the encryption key to do a repetitive transformation of the data which is extremely secure; key lengths of 128, 192 and 256 bits are supported. AES is the current standard for US government encryption.
- **AESFAST** – uses a variation of the AES algorithm with a 128-bit encryption key that saves 40-50% of the CPU time of AES.

Encryption keys can be specified by the user or randomly generated.

FDRCRYPT protects the data on your backups against unauthorized access...by anyone who does not possess the proper encryption keys. Protection of the backup data may be required by many of today's government, industry and corporate privacy and security laws and regulations, such as HIPAA, SOX and DoD requirements, among many others in the US and other countries. FDRCRYPT provides encryption of full-volume, incremental, archive, application and dataset backups.



Encryption defeats compression, the default on modern tape drives, which significantly increases the number of tapes used. To compensate, all encrypted backup data will be compressed using Innovation's proprietary software compression technique before encryption, to reduce tape usage.

New Feature (Available May, 2006):

FDRCRYPT includes FDRCAMS, a program which invokes IBM's IDCAMS and allows a REPRO command to encrypt the output sequential data set and decrypt when reading such an encrypted data set. This allows sequential copies of VSAM, IAM or sequential data sets to be encrypted for shipment to other companies or government agencies. The encrypted data set can be on tape, or on disk for delivery via email or FTP.

See page 2 for more details.

VISIT US AT:

EMC Technology Summit: April 24 - April 26, Boston

Storage Decisions: May 16 - May 18, Chicago

SHARE Technology Exchange: Aug. 14 - Aug. 16, Baltimore

IN THIS ISSUE...


- FDRCRYPT Common Questions.....see page 4*
- WHAT'S NEW...IAM, FDR, FATS & UPSTREAM...see page 6*
- FATS...Data Erasure for Tapesee page 9*
- Volume Consolidationsee page 10*
- Latest Product Release Information.....see page 11*
- FDRERASE V5.4 L50 earns EAL2+ Certification.see page 12*

FDRCRYPT NEW FEATURE FDR CAMS

FDR CAMS is a file encryption utility that is part of FDRCRYPT, the encryption option of the FDR family of products.


FDR CAMS enhances IDCAMS REPRO to use the file encryption options of FDRCRYPT. This allows you to create encrypted sequential copies of any data that can be copied with REPRO. These encrypted copies can be safely exchanged with other sites or other companies, where FDR CAMS can be used again to REPRO the data back to usable form. A Public Key can be used to encrypt the actual encryption key, or the encryption key can be securely communicated to the receiving site separately from the encrypted data. If the receiving site is not licensed for FDRCRYPT, they can download a free limited-function copy of FDR CAMS that can be used to decrypt the data.

FDR CAMS is invoked by executing PGM=FDR CAMS instead of PGM=IDCAMS, and adding an FDRCRYPT DD statement to the IDCAMS JCL to specify encryption options. FDR CAMS will invoke IDCAMS internally, and all IDCAMS functions are available. However, any REPRO function will be checked to see if encryption or decryption is requested; if so, FDR CAMS will use IDCAMS I/O exits to perform the requested operation.


 This sample job uses FDR CAMS to encrypt a sequential output file created by an application program and put the encrypted data on tape. The user has specified the encryption key.

```
//APPL1 EXEC PGM=APPL1,REGION=4M
//SYSPRINT DD SYSOUT=*
//EXTRACT DD DSN=*&&TEMP,UNIT=TEMP,DISP=(,PASS),SPACE=(CYL,(50,10))

//ENCRYPT EXEC PGM=FDR CAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//EXTRACT DD DSN=*&&TEMP,DISP=(OLD,DELETE)
//SENDOFF DD DSN=SENSITIV.MEDICAL.INFO,UNIT=TAPE,DISP=(,CATLG)
//SYSIN DD *
REPRO INFILE(EXTRACT) OUTFILE(SENDOFF)
//FDRCRYPT DD *
ENCRYPT OUTFILE=SENDOFF,ENCRYPTTYPE=AES128,
AESKEY=5F2391DA339002BBC67554742AFE3F21
```

 This sample job uses FDR CAMS to encrypt an input data set and put the encrypted data on tape. The input is a VSAM KSDS, but it could be any VSAM or sequential data set supported by IDCAMS REPRO, including IAM (Innovation Access Method) files. No encryption key is specified, so FDR CAMS will generate the key.

```
//ENCRYPT EXEC PGM=FDR CAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//OUTPUT DD DSN=OFFSITE.ENCRYPT.DATA,UNIT=TAPE,DISP=(,CATLG)
//SYSIN DD *
REPRO INDATASET(CUSTOMER.MASTER.FILE) OUTFILE(OUTPUT)
//FDRCRYPT DD *
ENCRYPT OUTFILE=OUTPUT,ENCRYPTTYPE=AES128
```

 This sample job can be used at the receiving site to REPRO the encrypted data back to a sequential data set. INPUT specifies the encrypted tape data set and OUTPUT is the target data set on disk (which can also be a VSAM cluster). The user-specified or FDR CAMS-generated encryption key must be provided.

```
//DECRYPT EXEC PGM=FDR CAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//INPUT DD DSN=SENSITIV.MEDICAL.INFO,UNIT=TAPE,
// VOL=SER=123456,DISP=OLD
//OUTPUT DD DSN=RECEIVED.DATA,UNIT=DISK,DISP=(,CATLG),
// SPACE=(CYL,(50,10),RLSE),RECFM=FB,LRECL=450,BLKSIZE=0
//SYSIN DD *
REPRO INFILE(INPUT) OUTFILE(OUTPUT)
//FDRCRYPT DD *
DECRYPT INFILE=INPUT,AESKEY=5F2391DA339002BBC67554742AFE3F21
```

FDRCRYPT OFF-SITE RECOVERY Checklist


In order to do recovery of encrypted backups off-site, such as at a disaster/recovery site:

- ✔ You must transport a current copy of the FDRCRYPT key file to the recovery site:
 - If you have a mechanism for securely transporting the key file directly to the recovery site, such as encrypted FTP, you can do so. However, this may be possible only if the key file was allocated as DSORG=PS instead of the default of DSORG=DA.
 - Alternatively, you can use FDRDSF to create an encrypted backup of the key file, using a special AES encryption key. This backup must be run after all other backups are complete. If this backup is on tape, you should transport it to the recovery site separately from the backups themselves. If the backup is on disk, you may be able to transmit it to the recovery site with secure email or FTP. At the recovery site, you will need to restore the encrypted backup, with its special key, before you can restore any other backups recorded in it.
- ✔ Once you have the key file restored, you can restore the encrypted backups that were recorded in it. Normally this will not require any special restore JCL as long as the name of the key file is set in the FDR Global Options Table.
- ✔ Remember that if you restore the volume containing the key file as part of your recovery, this will restore a back-level version of that file, so you may need to restore the key file backup again after restoring that volume to bring it up to date.
- ✔ If the key file is not available, or not up to date, you can use master keys to restore the backups, if master keys were specified during the backup. Innovation strongly recommends using master keys.
 - Innovation recommends that the master key be stored in a secure location (such as a safe-deposit box) that can be accessed only if the key file is not available.
 - We also recommend that you do not routinely use master keys for off-site restores, to avoid exposing the master key to unauthorized individuals. Use the master keys only if the key file cannot be used.
- ✔ The up-to-date key file must be present in order to do ABR auto-recall from encrypted Archive backups.

At a disaster site, remember that you may need to restore your operating system before the full facilities of FDRCRYPT are available:

- ✔ SAR (FDR's Stand Alone Restore) does not support encrypted backups.
- ✔ Although the "starter system" supplied by a disaster site may include FDR, it may not include FDRCRYPT. If you have a special backup of your own FDR program library, you can restore it on the starter system and authorize it.
- ✔ Even if you have FDRCRYPT on the starter system, you may not have the FDRCRYPT key file available.

For all these reasons, Innovation recommends that the backups of your system volumes should not use encryption, unless they also contain sensitive application data or other data that might compromise the integrity of your application data.

 **In the FDRCRYPT documentation, in section 71.03 under “key file”, it states that if the Backup was encrypted using the key file and the master key is supplied to DECRYPT it will open the “key file” but not read it. Does this mean that even if the backup was encrypted using the “key file”, I can decrypt (restore) using the master key?**

Yes.

During the Backup

You always have a specific key, which is always recorded in the key file. You can provide the specific key with the AESKEY, CIPHERKEY or SUBKEY operands, or you can let FDRCRYPT generate a random key. Either way, it is *always recorded*.

We always display the specific key in the backup listing unless you use the PRINTKEY=NO operand, which suppresses that display.


The master key is optional. It can be provided by a MASTERKEY= operand on an ENCRYPT statement, or preferably through RACF with the MASTERKEYID= operand. The easiest way is to specify a default MASTERKEYID in the FDR Global Option Table. If you don't do any of these, then no master key is used for the backup. **However, Innovation recommends that you always use a master key for all backups.**

During the Restore

If the key file is available, FDRCRYPT will retrieve the specific key from the key file and decrypt the backup.

If the key file is not available, or you choose not to use it for some reason, you can specify the MASTERKEY= on a DECRYPT statement if a master key was used during the backup. If the backup did not use a master key, you cannot restore the file without the key file, unless you know the specific key and specify it on a DECRYPT statement.


We recommend using the master key as a fail-safe, not for routine restores. Plan on using the key file for all restores, even at a disaster site. But if the key file is lost, then the master key can be used to do the restores. Keep the master key in a very safe place and make sure that only a few trusted people have access to it. If your master key is exposed, then anyone can restore your backups. If you do need to restore with the master key, be sure to change the master key used for subsequent backups.

 **The FDRCRYPT documentation says that an encrypted backup may use more tape than an unencrypted backup of the same data. But when I compare the tape management records of an encrypted and unencrypted backup of the same disk, it has the same number of blocks. How can it take more tape?**

An FDR backup of the same data will always generate the same number of tape blocks, but the space occupied by those blocks on tape can vary.

Whether the data is encrypted or not, all modern tape drives do internal compression of the data, and also combine smaller tape records into large “super-blocks” on the tape, so a tape file may occupy far less space on the tape than the number of blocks and bytes suggests. Because compression is data-dependent, you can't accurately determine the actual size of a tape file from the external statistics (blocks and blocksize). *By the way, Innovation's tape utility FATAR can determine tape compression ratios and actual physical tape used.*

As we say in the FDRCRYPT documentation, “Encryption defeats the hardware compression used on most tape drives”. This is due to the fact that after encryption, the resulting data is so thoroughly scrambled that the tape compression hardware is unable to find strings and data that are compressible. To compensate, FDRCRYPT uses FDR's software compression on the data before encrypting it, but the result may still take more space on tape than the original unencrypted backup.

 **I tried to restore an encrypted tape, but the restore job got many FDR204 TAPE BLOCK LENGTH CHECK – BLOCK BYPASSED messages and eventually ended with a U0207 ABEND. What does this mean?**

Probably you tried to do the restore with an FDR program library that does not contain the FDRCRYPT modules. You may have:

- Used an FDR program library from V5.4 Level 43 or earlier (FDRCRYPT was available with V5.4 level 50).
- Used an FDR V5.4 level 50 library that did not include an FDRCRYPT license.
- Because the FDR restore code without the FDRCRYPT code does not recognize the format of the encrypted data blocks, the block length checks occur.

The FDR204 may also occur for other reasons. The most common cause is restoring from an FDR tape that has been copied with a standard copy utility like IEBGENER. FDR tapes can only be safely copied with the FDR utilities FDRTCOPY and FDRTSEL and the Innovation tape utilities FATAR and FATSCOPY.

 **The encryption key is displayed in my printout. Isn't that a security exposure?**

If you provide master keys or specific encryption keys on ENCRYPT or DECRYPT control statements, they will not be displayed. The statements will be displayed, but the keys will be replaced with asterisks as shown below. However, by default, FDRCRYPT will display the specific encryption key used for each backup as part of the backup listing as shown in the FDR178 message below. Master keys are never displayed.

Although the specific keys are recorded in the FDRCRYPT key file, if that file is lost or unusable there is no way to restore the backup without knowing the specific key (or the master key, if a master key was used during the backup). If you let FDRCRYPT generate the specific encryption keys, then the key display serves as a backup to the key file.

If you cannot keep the FDRCRYPT backup listings secure or just prefer not to display the keys, you can suppress the key display by adding the operand PRINTKEY=NO on the ENCRYPT statement that applies to the backup. Note that PRINTKEY=NO cannot go on an ENCRYPT statement that has the MASTERKEY= or MASTERKEYID= operand. In the example below you would need to add a second statement: ENCRYPT PRINTKEY=NO

```
FDR303 CARD IMAGE -- DUMP TYPE=FDR,DATA=USED,ENCRYPT=COPY2,ENCRYPTTYPE=AES
FDR303 CARD IMAGE -- KEYFILE DSN=ICF1.CRYV003.ENCRYPT
FDR303 CARD IMAGE -- ENCRYPT MASTERKEY=*****
                        ENCRYPT PRINTKEY=NO
FDR007 STARTING TIME OF DATA SET DUMP -- 10.40.49 -- UNIT=3390-9 ,IN=DISK1 ,OUTPUT=TAPE1 TAPE11
FDR178 BACKUP OF VOL=SH20C0 COPY=2 IS ENCRYPTED TYPE=AES-128 KEY=***** WAS GENERATED
FDR007 ENDING TIME OF DATA SET DUMP -- 10.42.16 -- UNIT=3390-9 ,IN=DISK1 ,OUTPUT=TAPE1 TAPE11
FDR122 BYTES DSK TRK T BLKS RESTART STIMERS ERRS ACT DSK LOW HGH DEXCP NUMDS COMP KBYTE
FDR122S 0326244321 007095 013951 0006046 0000469 000 007031 001 002 07027 00013 0000233469
FDR107 DSF DUMP SUCCESSFULLY COMPLETED VOL=SH20C0
FDR999 FDR SUCCESSFULLY COMPLETED
```

WHAT'S NEW

IAM 8.1 is now available

ENHANCED HARDWARE COMPRESSION SUPPORT

IAM V8.1 offers the capability to dynamically create a hardware compression dictionary as an IAM file is being loaded. This feature will make it easier to utilize the zSeries Hardware Compression function with IAM datasets and will provide the ability to set Hardware Compression as the default data compression technique.

BUFFERING ENHANCEMENTS

Numerous enhancements have been made to IAM's Real Time Tuning for Version 8.1, including a new TURBO mode and higher defaults for the amount of buffer space per dataset. The intent of these changes is to provide improved performance in many circumstances by further reductions in physical I/O, along with reducing the need for manual tuning IAM datasets with IAM overrides. The TURBO mode will result in IAM being much more aggressive in buffer acquisition during periods of heavy I/O activity and eliminate the need for specification of MINBUFNO override values.

For the complete benchmark e-mail your request to sales@fdrinnovation.com

LARGE FORMAT SEQUENTIAL DATASETS

With IAM V8.1 and z/OS 1.7 or higher, IAM datasets can be stored as Large Format Sequential Datasets (DSNTYPE=LARGE). This allows IAM datasets to exceed 64K tracks per volume, without having to reside on DFSMS managed volumes, and without the 32-byte suffix on each block required for the DFSMS Extended Format datasets. Customers currently using IAM datasets in DFSMS Extended Format are encouraged to convert to the Large Format Sequential Datasets.

PRIME RELATED OVERFLOW

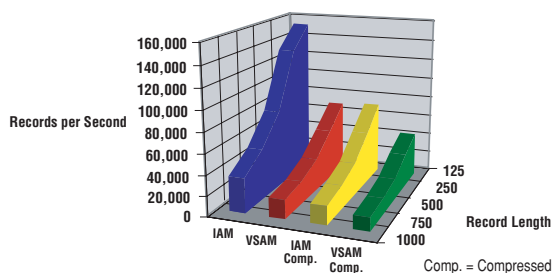
Prime Related Overflow (PRO) is a new alternative overflow structure within IAM Enhanced Format files. The Prime Related Overflow structure (PRO) is an option for those IAM files with an extremely high volume of records being inserted, which should reduce virtual storage requirements and improve performance for those types of datasets.

MULTIPLE IAMRLS ADDRESS SPACES

Starting with IAM V8.1, customers can run multiple IAMRLS address spaces on an LPAR or MVS system image. This can be an aid for customers requiring isolation of different applications for security, accounting, or reliability concerns.

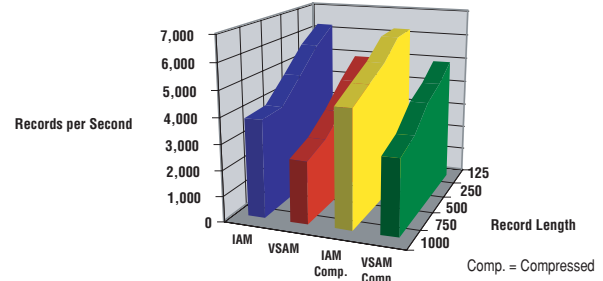
THIS IS HOW IAM 8.1 STACKS UP WHEN COMPARED TO DFSMS EXTENDED FORMAT VSAM WITH SYSTEM MANAGED BUFFERING

File Load Performance



- For File Loads:
 - IAM used 39% to 41% LESS CPU Time
 - IAM ran in 46% to 62% LESS Elapsed Time
- For Sequential Reads:
 - IAM used 14% to 20% LESS CPU Time
 - IAM ran in 26% to 51% LESS Elapsed Time

Random Read Performance



- For Random Reads:
 - IAM used 21% to 30% LESS CPU Time
 - IAM ran in 21% to 38% LESS Elapsed Time
- For Random Inserts:
 - IAM used 66% to 72% LESS CPU Time
 - IAM ran in 67% to 78% LESS Elapsed Time

WHAT'S NEW

FDR Version 5.4 Level 55 (Available May, 2006)

FDRINSTANT ENHANCEMENTS

- FDRINSTANT FOR EMC TIMEFINDER has been enhanced to support TimeFinder/Clone (Snap to real disks, including “Raid-5 BCVs”) and TimeFinder/Snap (Snap to virtual disks). TimeFinder/Mirror (BCVs) continues to be supported. Consistent Snap (the ability to Snap multiple volumes at a point of I/O consistency) is supported.
- FDRINSTANT FOR HDS SHADOWIMAGE has been enhanced to support Quick Split (the ability to create a ShadowImage volume at the time of the backup, without a pre-establish) and Consistent Split (the ability to Split multiple volumes at a point of I/O consistency). These functions were supported in V5.4 level 50 but they are now fully documented and slightly enhanced.
- FDRINSTANT FOR FLASHCOPY has been enhanced to support Consistent Flash (the ability to Split multiple volumes at a point of I/O consistency).

FDRCRYPT ENHANCEMENTS

- FDRCRYPT now includes FDRCAMs, an IDCAMS front end which enhances REPRO to support encryption and decryption using any of the encryption algorithms supported by FDRCRYPT. The sequential output file from REPRO can be encrypted, and a sequential file input to REPRO can be decrypted.

See page 2 for more details.

FDREPORT ENHANCEMENTS

- Performance improvements. When processing volumes with large VVDSs, processing time has been significantly reduced.
- **Customer experience:** A beta site ran a data set report against 9,340 volumes containing 7.5 million data sets, and obtained the following improvements:

Version	Elapsed Time hr:min	CPU Time TCB + SRB min:sec
5.4/51	6:04	40:48.11
5.4/55	1:40	3:32.73
SAVINGS	73%	91%

FATS/FATAR V4.8 Level 50 ENHANCEMENTS


- IBM TS1120 CARTRIDGE DRIVE
The IBM TS1120 tape drive (also known as the 3592-E05) is now identified properly.
- LASTAPE SUPPORT IN FATSCOPY
FATSCOPY now supports a “last tape” function, similar to the LASTAPE support in FDRABR. LASTAPE allows FATSCOPY to remember the last output tape used and the last file created on that tape, and to add more files to that tape in a subsequent FATSCOPY job.

FDR/UPSTREAM ENHANCEMENTS V3.4G

- UPSTREAM support for Microsoft Volume Shadow Service (VSS) agent (WinSS PlugIn) is now generally available. VSS, which is included with Windows Server 2003, creates point-in-time, volume snap shot functionality of single or multiple volumes. Using UPSTREAM that is VSS-aware can greatly enhance the quality of your backups.
- ACLs in Linux.
ACLs (Access Control Lists) are an extended form of security in Linux; in particular they allow better security in a Samba environment.
- Expanded UPSTREAM Rescuer support for SuSE z/Linux SLES 9 and Intel Linux.
- 64-bit Windows support.

UPSTREAM RESERVOIR ENHANCEMENTS V3.4G

- UPSTREAM RESERVOIR SAN Express Passthru for LAN-free backups through the SAN to a disk. With a storage array or other disk that is common to both the UPSTREAM client system and the Reservoir machine, you can use a portion of the disk to pass data, bypassing the LAN for a LAN-Free backup—the SAN Express Passthru.
- Microsoft Exchange 2000/2003 mail-level backups and restores.
- Expanded UPSTREAM Reservoir Tape Manager (Direct SCSI or Fibre) now supports Windows, AIX, Solaris and Linux.
- UPSTREAM Reservoir support for IBM Total Storage 3494 Tape Libraries.

 We are a financial services company and our mainframe processing is provided by an outsourcer. Our auditors are asking us how can we insure that when our outsourcer does testing at a disaster recovery center that all the data is wiped out before they leave the disaster recovery center.

The listings that are generated during the FDRERASE show the volumes that have been erased. If additional assurance is desired, FDRERASE provides two services, PRINT and VERIFY, that can be used after the erase operation to confirm that the volumes have been erased.

ERASE listing - identifies the erased volume by unit address (device number), former volume serial, subsystem manufacturer and serial number, subsystem ID, and internal disk identification.

```
FDR001 FDR          ERASE VOLUMES - FDRERASE VER. 5.4/50P - INNOVATION DATA PROCESSING          DATE=2006.054  PAGE  1
FDR303 CARD IMAGE -- ERASE TYPE=FULL
FDR303 CARD IMAGE -- MOUNT ERASEUNIT=21C3
FDR235 FDRERASE WILL ERASE THE FOLLOWING      1 UNITS:
FDR235 21C3
FDR170 DEVICE IS ELIGIBLE FOR ERASE UNIT=21C3 VOL=SH21C3 VOLID=VOL1 CU=IBM24678/0801-01000000 00000000
FDR172 ERASE STARTED PASS 1 PATTERN=00
FDR172 ERASE ENDED PASS 1
FDR173 ERASE HARDENED DATA TO UNIT=21C3 IN  6 SECS          0000-0D0A-0000085F
FDR241 FDRERASE SUCCESSFULLY COMPLETED ERASE OF VOL=SH21C3 ON UNIT=21C3
FDR122 OPERATION STATISTICS FOR 3390 VOLUME..... 21C3
FDR122 CYLINDERS ON VOLUME.....3,339
FDR122 DASD TRACKS VERIFIED.....0
FDR122 BYTES READ FROM DASD.....0
FDR122 DASD TRACKS ERASED.....50,085
FDR122 NUMBER OF ERASE PASSES.....1
FDR122 DASD EXCPS.....3,353
FDR122 TARGET DASD EXCPS.....0
FDR122 CPU TIME (SECONDS).....0.299
FDR122 ELAPSED TIME (MINUTES).....1.6
FDR122 ERASE TIME.....1.6
FDR999 FDR SUCCESSFULLY COMPLETED
```

PRINT - The PRINT command prints selected tracks so that you can confirm that they have been erased.

```
FDR170 DEVICE IS ELIGIBLE FOR ERASE UNIT=90C2 VOL=SH90C2 VOLID=FDR5 CU=IBM24678/0800-00000000 00000000 17.11.48
FDR175 PRINT UNIT=90C2 CYL.....3 TRK..0 REC...0 KL...0 DL.....8 DATA=0000000000000000 - 1 RECORDS ON TRACK
FDR175 PRINT UNIT=90C2 CYL.....3 TRK..0 REC...1 KL...0 DL.56664 DATA=0000000000000000 - ALL BYTES THE SAME
FDR175 PRINT UNIT=90C2 CYL.....4 TRK..0 REC...0 KL...0 DL.....8 DATA=0000000000000000 - 1 RECORDS ON TRACK
FDR175 PRINT UNIT=90C2 CYL.....4 TRK..0 REC...1 KL...0 DL.56664 DATA=0000000000000000 - ALL BYTES THE SAME
```

This example shows the result of an FDRERASE PRINT on 2 tracks of a volume after the volume was erased with the ERASE command. You can see that each track contains a single track-length (56664 bytes) record containing all zeros (the default pattern for ERASE). “ALL BYTES THE SAME” indicates that every byte in the data record is identical.

VERIFY - The VERIFY command reads selected tracks and analyzes them to confirm that they have been erased. This example shows the result of a successful VERIFY of a 3390-9 volume after it was erased with the QUICKERASE command. As you can see, you can verify hundreds of volumes in a very short period of time.

```
FDR001 FDR          ERASE VOLUMES - FDRERASE VER. 5.4/50P - INNOVATION DATA PROCESSING          DATE=2005.319  PAGE  1
FDR303 CARD IMAGE -- VERIFY TYPE=FULL,ERASESTARTCYL=0,ERASESTARTTRK=0,ERASESKIP=1          01466002
FDR303 CARD IMAGE -- MOUNT ERASEUNIT=(21C0)          01467002
FDR235 FDRERASE WILL CHECK THE FOLLOWING      1 UNITS:
FDR235 21C0
FDR170 DEVICE IS ELIGIBLE FOR ERASE UNIT=21C0 VOL=SH20E0 VOLID=FDR5 CU=IBM24678/0801-01000000 00000000
FDR177 VERIFY CHECKED UNIT=21C0 AND ALL TRACKS CONTAINED NO RECORDS PATTERN=ERASE
FDR122 OPERATION STATISTICS FOR 3390 VOLUME..... 21C0
FDR122 CYLINDERS ON VOLUME.....10,017
FDR122 DASD TRACKS VERIFIED.....150,255
FDR122 BYTES READ FROM DASD.....0
FDR122 DASD TRACKS ERASED.....0
FDR122 NUMBER OF ERASE PASSES.....0
FDR122 DASD EXCPS.....10,021
FDR122 TARGET DASD EXCPS.....0
FDR122 CPU TIME (SECONDS).....4.321
FDR122 ELAPSED TIME (MINUTES).....1.0
FDR122 ERASE TIME.....1.0
FDR999 FDR SUCCESSFULLY COMPLETED
```

FATS DATA ERASURE FOR TAPE

Can FDRERASE be used to erase tapes as well as disks?

No, but Innovation's tape utility FATS can. FATS contains a function to completely erase tapes using the hardware Data Security Erase function.

This is an example of a job to completely erase 100 tape volumes, from volser 100001 to 100100, before reusing or selling the tapes. FATS will preserve the volume serial of the tape, but will erase all other data to the physical end of the tape.

```
//ERASE      EXEC  PGM=FATS
//TAPE1     DD   DSN=FATS,UNIT=(TAPE,,DEFER),
//          LABEL=(,BLP),DISP=(,KEEP)
//SYSIN     DD   *
           ERASE(1)  VOL=100001,VOLINCR=1,MAXVOLN=100
```

FATAR Summary Report of an Existing File on a Tape

FATAR TAPE SUMMARY FOR TAPE VOLUME -003235- AT DENSITY 105219 BPI ON DEVICE TYPE 3590 11/15/2005														
PHYS	DATASET NAME	FILE	FIL#	CRDATE	LRECL	CREATING	RECFM	BLOCKS	BYTES	PERM	----BLOCKSIZES----			EST.
FILE	(LAST 17 CHARS)	SERIAL	VOL#	EXPDTE	BLKSIZE	JOB&STEP		READ	READ	TEMP	MIN	AVG	MAX	FEET
(FULL 44 CHARS)														
2	BACKUP.T1	003235	00001	2005/319	00000	JMKANLYZ	U	279316	13G	0	24	44973	57344	****
			0001	2005/322	32760	FATAR4	IDRC>	11770	4468M	0		379631		452
	BACKUP.T1													
	HIGHEST EXPIRATION ==>>			2005/322		TOTALS ==>>			279316	13G	0	****		
	IDRC COMPACTION ==>>			64%		IDRC TOTALS ==>>			11770	4468M		452		

Summary Report of Tape After Running the FATS ERASE Option

FATAR TAPE SUMMARY FOR TAPE VOLUME -003235- AT DENSITY 105219 BPI ON DEVICE TYPE 3590 11/16/2005														
PHYS	DATASET NAME	FILE	FIL#	CRDATE	LRECL	CREATING	RECFM	BLOCKS	BYTES	PERM	----BLOCKSIZES----			EST.
FILE	(LAST 17 CHARS)	SERIAL	VOL#	EXPDTE	BLKSIZE	JOB&STEP		READ	READ	TEMP	MIN	AVG	MAX	FEET
(FULL 44 CHARS)														
2	00000000000000000000	003235	00001	2005/320	00000		U	0	0	0	0	0	0	0
			0001	2005/320	32767					0				
	HIGHEST EXPIRATION ==>>			2005/320		TOTALS ==>>			0	0	0	0		

New Feature: Erase Residual Data

Fats version 4.8 L45 and higher has been enhanced to erase residual data.

Residual data is data beyond the end of the current file(s) on the tape to the physical end of tape; this may be data left over from previous uses of the tape. This residual data is unrelated to the current data on the tape, and may be sensitive data that you don't want released. **Even if the current files on the tape are encrypted, the residual data may not be. You may want to erase residual data when sending a data tape (non-scratch) to another installation.**

This is an example of a job to erase residual data from 3 tape volumes, before sending those volumes offsite. FATS will locate either the EOD mark or the double tape mark that the tape drive writes after the last valid data on the tape, and erase from that point to the physical end of the tape.

```
//ERASE      EXEC  PGM=FATS
//TAPE1     DD   DSN=FATS,UNIT=(TAPE,,DEFER),
//          LABEL=(,BLP),DISP=(,KEEP)
//SYSIN     DD   *
           ERASE(1)  RESIDUAL,VOL=(005279,013424,025993)
```

Volume Consolidation with FDR and FDRPAS

Does Innovation have tools to efficiently consolidate smaller DASD volumes (Ex: 3390-9 to larger volumes 3390-27) with minimal disruption?

Yes, using a combination of FDRPAS, FDRCOPY and FDRINSTANT with either FlashCopy or EMC SNAP.

FDRPAS can non-disruptively move entire volumes to target disks of the same size or larger, for example one 3390-9 to a 3390-27 (the extra cylinders on the larger disk would become free space). But if you need to consolidate multiple 3390-9 volumes to a 3390-27, the other two 3390-9 volumes must be moved at the dataset level.

Data sets can only be moved while they are unallocated (not in use) because the catalog, VTOC and VVDS must be updated to reflect the new location of each dataset. So, any applications using those data sets must be quiesced or shut down during the move.

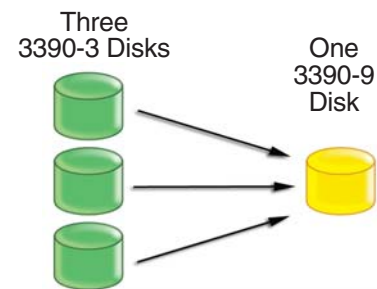
Normally a data set move can take some time, depending on the number of data sets and the number of tracks that need to be moved, so applications can be disrupted for a considerable time. However, by using the instant replication hardware facilities supported by FDRINSTANT, the dataset move time can be reduced to a minimum (a few seconds to a few minutes).

Here is the procedure to use if the source disks are in a different disk subsystem from the target disks:

- non-disruptively move one volume to the larger target disk in the new subsystem with FDRPAS.
- non-disruptively move the other disks to be consolidated to temporary disks in the new subsystem (they can be the same size as the original or larger) with FDRPAS.
- shut down the applications using the datasets on the temporary volumes.
- use FDRCOPY to move the data sets from the temporary volumes to the target volume. FDRCOPY will automatically use FlashCopy or EMC SNAP (if it is enabled) or STK Snapshot to copy the data sets. The elapsed time of the copy will be only the time required to allocate and catalog the output data sets, rarely more than a few minutes.
- restart the applications.

Here are some sample elapsed times using FDRCOPY to move data using EMC SNAP or IBM's FlashCopy. One FDRCOPY per volume was executed using INSTANT Copy and another using regular I/O.

# of Data Sets	Total Size (GB)	Elapsed Time (INSTANT)	Elapsed Time (Non-INSTANT)	# of Source Volumes	# of Target Volumes
1	2.2	1 sec	1.8 min	1	1
600	2.2	2.7 min	4.4 min	1	1
6,000	22.1	34.6 min	58.0 min	1	1
6,000	22.1	27.9 min	37.7 min	2	1
24,000	88.4	79.6 min	122.1 min	4	2



User Experience of a Large Hospital After moving to a New Controller using FDRPAS

“The next issue was consolidating the Model 1 and 3 volumes to the denser Model 9 volumes, thereby reducing the number of active volumes. To do this, we employed the ESS’s FlashCopy function, supported by the FDRCOPY component of Innovation’s FDRINSTANT product, to do “instant moves” of data sets from the smaller disks to the larger ones. This reduced the number of volumes from more than 4000 to approximately 1800.”

PRODUCT UPDATES

This table shows, for each current release of z/OS, the minimum levels of each Innovation product that should be installed. Use the table when upgrading your z/OS system, to verify that you have the correct Innovation software in use. If not, you should install the latest version. If you already are using the indicated minimum level, you may wish to install the latest version anyway in conjunction with the Operating System upgrade. If not, please review the Product Notes that follow the table on our website at www.innovationdp.fdr.com/osreq.cfm for ZAPs that may be required depending on the hardware and software in use at your installation.

NOTE: While prior versions might still work, the versions listed are the minimum supported versions.

As of March 2006

	z/OS 1.1 -1.5	z/OS 1.6	z/OS 1.7	
PRODUCT	Minimum	Minimum	Minimum	Latest Version
FDR	V5.4/40	V5.4/40	V5.4/50	V5.4/51
COMPAKTOR	V5.4/40	V5.4/40	V5.4/50	V5.4/51
ABR	V5.4/40	V5.4/40	V5.4/50	V5.4/51
FDRCRYPT	V5.4/50	V5.4/50	V5.4/50	V5.4/51
FDREPORT	V5.4/40	V5.4/40	V5.4/50	V5.4/51
FDRINSTANT	V5.4/40	V5.4/40	V5.4/50	V5.4/51
FDRCLONE/FDRDRP	V5.4/40	V5.4/40	V5.4/50	V5.4/51
FDRREORG	V5.4/40	V5.4/40	V5.4/50	V5.4/51
FDRPAS	V5.4/40	V5.4/40	V5.4/50	V5.4/51
FDRERASE	V5.4/40	V5.4/40	V5.4/50	V5.4/50
FDRSOS	V5.4/40	V5.4/41	V5.4/50	V5.4/51
FATS/FATAR/FATSCOPY	V4.8/30	V4.8/41	V4.8/41	V4.8/50
IAM	V8.0/21	V8.0/28	V8.0/32	V8.1/01
UPSTREAM CLIENT	V3.3.0	V3.3.0	V3.3.0	V3.4.0F
UPSTREAM zSeries & OS/390	V3.3.0	V3.3.0	V3.4.0	V3.4.0
UPSTREAM Reservoir	-	-	-	V3.4.0F

For the most up-to-date information visit the website at:
[http:// www.innovationdp.fdr.com/osreq.cfm](http://www.innovationdp.fdr.com/osreq.cfm)



NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS MAIL PERMIT NO. 18 LITTLE FALLS NJ

POSTAGE WILL BE PAID BY ADDRESSEE



INNOVATION PLAZA
275 PATERSON AVENUE
LITTLE FALLS NJ 07424-9968



FDRERASE EAL2+ CERTIFICATION

FDRERASE V5.4 L50 EARNS EAL2 CERTIFICATION



Product Name: FDRERASE
Technology Type: Sensitive Data Protection
Date Certified: August 5, 2005
Conformance Claim: EAL2 Augmented ADV_SPM.1, ALC_FLR.2
Sponsor: Innovation Data Processing
Phone: 973.890.7300
CC Testing Lab: SAIC



FDRERASE V5.4 L50 is the first z/OS secure erase utility to complete Common Criteria Evaluation and Validation Scheme (CCEVS) evaluation and Common Criteria EAL2 Augmented validation.

FDRERASE is designed to comply with current U.S. Government guidelines for erasing computer disks prior to disposal and the NIST guidelines for **Clearing** and **Purging** data.

There are many times when you may wish to insure that all corporate and customer data has been erased from a set of disk volumes, for example:

- At the end of a disaster test, or when leaving the site after a real disaster
- When you are disconnecting a disk control unit, after moving all data with FDRPAS or some other means
- When reusing disk volumes for new purposes, to be sure that no residual data remains

FDRERASE meets these needs. It can quickly erase many disk volumes in parallel, allowing you to erase your data from a set of disks in the minimum elapsed time.

See page 8 for sample output from an ERASE and VERIFY run using FDRERASE.



CORPORATE HEADQUARTERS: 275 Paterson Ave., Little Falls, NJ 07424 • (973) 890-7300 • Fax: (973) 890-7147
 E-mail: support@fdrinnovation.com • sales@fdrinnovation.com • <http://www.innovationdp.fdr.com>

EUROPEAN OFFICES:	FRANCE 01-49-69-94-02	GERMANY 089-489-0210	NETHERLANDS 036-534-1660	UNITED KINGDOM 0208-905-1266	NORDIC COUNTRIES +31-36-534-1660
-------------------	--------------------------	-------------------------	-----------------------------	---------------------------------	-------------------------------------

PLEASE SEND ME:

Product Overview/Concept and Facilities Guides for:

- FDR
 IAM
 FATS
 UPSTREAM
 FDRPAS
 FDRSOS
 RESERVOIR
 FDRERASE
 FDRCRYPT
 ABR
 FDREPORT
 FREE No-Obligation Trial & Keychain Flashlight.
 Check this box if you want a Documentation CD-ROM shipped to you.
 Check this box if you want the latest version of a licensed product shipped to you.

USER COMMENTS:

FIRST-CLASS
 U.S. POSTAGE
 PAID
 Little Falls, NJ
 Permit No. 65

E-mail

Telephone