



Announcement

VM/Encrypt-Backup™ for IBM Backup and Restore Manager for z/VM

Summary: Protecting sensitive data from unauthorized access is now a major requirement in z/VM® data centers. VM/Encrypt-Backup™ protects such data by encrypting it, using strong, secure and robust data encryption algorithms, as it is written to tape or DASD by the new IBM Backup and Restore Manager for z/VM. Depending on the security requirements, different encryption algorithms can be employed, allowing each site to select the level of data protection required. VM/Encrypt-Backup™ provides for both hardware and software encryption, so data backed up on one processor type can be restored on another.

Technical Specifications: VM/Encrypt-Backup™ is invoked from the user data processing exits (UDPEs) provided in IBM Backup and Restore Manager V1.2. Encryption parameters are read from a user created parameter file, allowing the encryption algorithm and parameters to be easily changed to meet different data protection needs.

VM/Encrypt-Backup™ encrypts data written to tape using the following algorithms:

1. DES (Data Encryption Standard), a block cipher, employing a data block size of 8 bytes and a key length of 8 bytes (64 bits). Both Electronic codebook (ECB) and Cipher-block chaining (CBC) modes of encryptions are supported. For CBC mode, an initial chaining value of 8 bytes can be specified.
2. 3DES, employing a data block size of 8 bytes and a key length of either 16 bytes (128 bits) or 24 bytes (192 bits). Both Electronic codebook (ECB) and Cipher-block chaining (CBC) modes of encryption are supported; for CBC mode, an initial chaining value of 8 bytes can be specified.
3. AES (Advanced Encryption Standard), a block cipher, employing a data block size of 16 bytes and a key length of either 16 bytes (128 bits), 24 bytes (192 bits), or 32 bytes (256 bits). Both Electronic codebook (ECB) and Cipher-block chaining (CBC) modes of encryption are supported. For CBC mode, an initial chaining value of 16 bytes can be specified.
4. BlowFish, a block cipher, employing a data block size of 8 bytes and a key length of either 16 bytes (128 bits) or 32 bytes (256 bits). Both Electronic codebook (ECB) and Cipher-block chaining (CBC) modes of encryption are supported. For CBC mode, an initial chaining value of 8 bytes can be specified.
5. ARC4, a stream cipher, with a data block size of 1 byte (8 bits) and an arbitrary key length of up to 64 bytes (512 bits).

VM/Encrypt-Backup™ will detect at run time if the appropriate encryption hardware support is available, and exploit the hardware support automatically. This can be overridden by a user parameter forcing VM/Encrypt-Backup™ to use the software encryption algorithms instead.

For the block ciphers VM/Encrypt-Backup™ supports, data record padding to an integral of the encryption algorithm's block size is handled automatically. Padding bytes are automatically removed when the data from tape read back in and decrypted. The maximum record length VM/Encrypt-Backup™ block ciphers can process is 64K-2 bytes. For the ARC4 stream cipher, the data block size is one byte, and therefore no data record padding is required. It can be used to encrypt data records that are as large as the maximum record size CMS allows.

The currently available IBM processors offer hardware support for the following encryption algorithms:

- 1) DES
- 2) 3DES
- 3) AES, with a key size of 16 bytes (128 bits)

Requirements:

Software: VM/Encrypt-Backup™ requires:

- IBM z/VM Version 5.1 (5741-A05) or later
- IBM Backup and Restore Manager for z/VM V1.2

Hardware: VM/Encrypt-Backup™ will operate on the following IBM platforms:

- System z9 Enterprise Class (z9 EC)
- System z9 Business Class (z9 BC)
- IBM **@server**®zSeries 990 and 890
- IBM **@server**®zSeries 900 and 800

If the hardware supports the CP Assist for Cryptographic Function (CPACF) feature, VM/Encrypt-Backup™ will exploit the cryptographic hardware instructions to perform the actual data encryption and decryption. This can significantly improve performance of data encryption.

Contact:

For Ordering Information:

Stan King
Information Technology Company
(800) 994-9441
(703) 237-7370
sking@p390.com

For Technical Information:

Dave Jones
V/Soft Software
(281) 578-7544
dave@vsoft-software.com