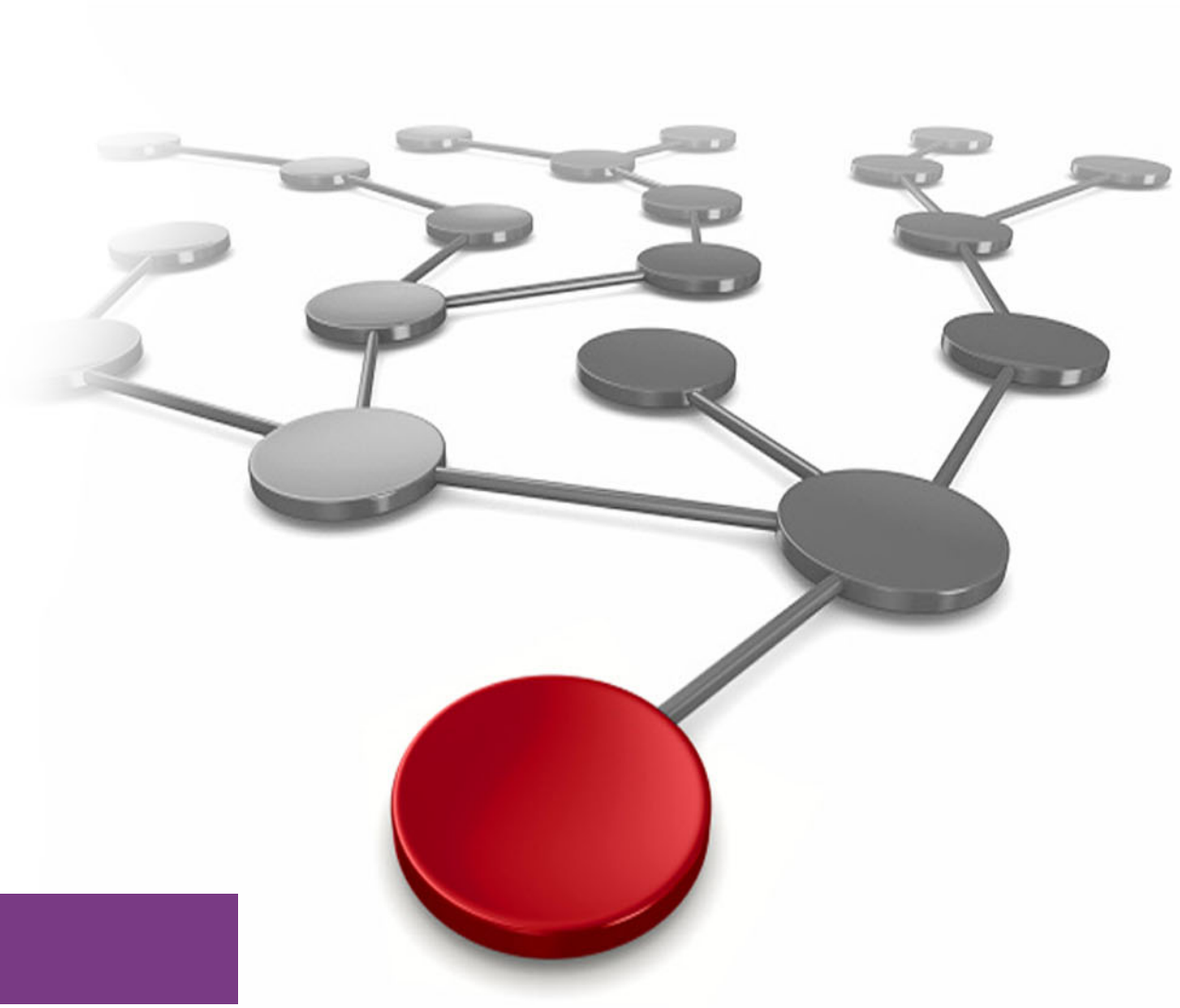
Redbooks
ibm.com/redbooks

IBM FlashCore Module Cryptographic Erase

For use with the IBM FlashSystem 9100, IBM Storwize V7000, and IBM Storwize V5100

Matt Smith



Storage

IBM

Redpaper

Statement on Cryptographic Erasure

IBM® FlashCore Modules (FCMs) are storage devices that are available in 4.8 TB, 9.6 TB, and 19.2 TB capacities. They are a 2.5-inch drive form factor device and use second-generation 3D triple-level cell (TLC) flash memory on which to store data.

This paper describes the cryptographic erasure of data that is stored on these devices when used in an IBM FlashSystem® 9100 (9846-AF7, 9846-AF8, 9848-AF7, 9848-AF8, 9848-UF7, and 9848-UF8), or IBM Storwize® V5100 (2077-424, 2077-A4F, 2078-424, and 2078-A4F).

The cryptographic erasure process that is described in this paper is designed to meet the requirements that are set in Appendix D of NIST SP 800-88.

Each FCM is a Self-Encrypting Drive (SED), where a unique media encryption key (MEK) exists on the device and is used to encrypt any data that is written to the drive. To read data back from device, the same unique key is required to decrypt the data.

In the IBM FlashSystem 9100, IBM Storwize V7000, and IBM Storwize V5100 products where FCMs are used, a unique MEK is created when the FCM device is added to a RAID array. Data that is written to and read from the device use only this key to encrypt and decrypt data.

Generating the MEK is done by using an SP 800-90A dynamic random bit generator (DRBG). Encryption is performed by using XTS-AES-256. IBM obtained FIPS 140-2 certification for the IBM FlashCore® Modules that are listed at this website.

The FCM uses two partitions when it is used in the IBM FlashSystem 9100, IBM Storwize V7000, and IBM Storwize V510. The first partition is used to store encrypted client data. A smaller, second 1 GB partition is used to store unencrypted system configuration data for recovery. No client data is stored on the second partition.

To achieve a cryptographic erase, the MEK and the wrapped key structure where the MEK is stored must be overwritten to ensure that the encrypted data on the drive cannot be decrypted. This process is described in “Process for Cryptographic Erasure” on page 2.

One of the steps in the cryptographic erasure process is to add the FCM device into the new array. As part of adding the FCM device into a new array, a new MEK is generated by using a DRBG that is placed in the same location as the old keys. If the generation of a new key fails, the device is not added into the array and is not considered as cryptographically erased.

To ensure the integrity of an MEK, the FCM device does not support escrow or injection of the MEK at or below the level of the sanitization operation. An MEK is generated internally to the FCM device and never leaves it.

FCMs do not support export of a MEK for key escrow. FCMs do not support importing a random number from outside the FCM to be used as a MEK (that is, key inject).

The FCM devices should be cryptographically erased only within a supported IBM FlashSystem 9100, IBM Storwize V7000, or IBM Storwize V5100 by using the process described next. No direct support is available for cryptographic erase by way of the FCM device NVMe interface.

This paper covers FCMs only. Other drives that are found within an IBM FlashSystem 9100, IBM Storwize V7000, or IBM Storwize V5100 do not have FIPS 140-2 certification. If the IBM Easy Tier® function is used between FCMs and other drives, consider that the other drives are not certified to the same level, but might still contain client data.

Process for Cryptographic Erasure

The process that is described in this section is for mass cryptographic erasure of multiple FCMs that are in use in a Storage Pool. Before starting, ensure that all FCMs are shown as online; otherwise, the MEKs cannot be deleted.

By using the GUI, ensure that encryption is enabled, as shown in Figure 1.

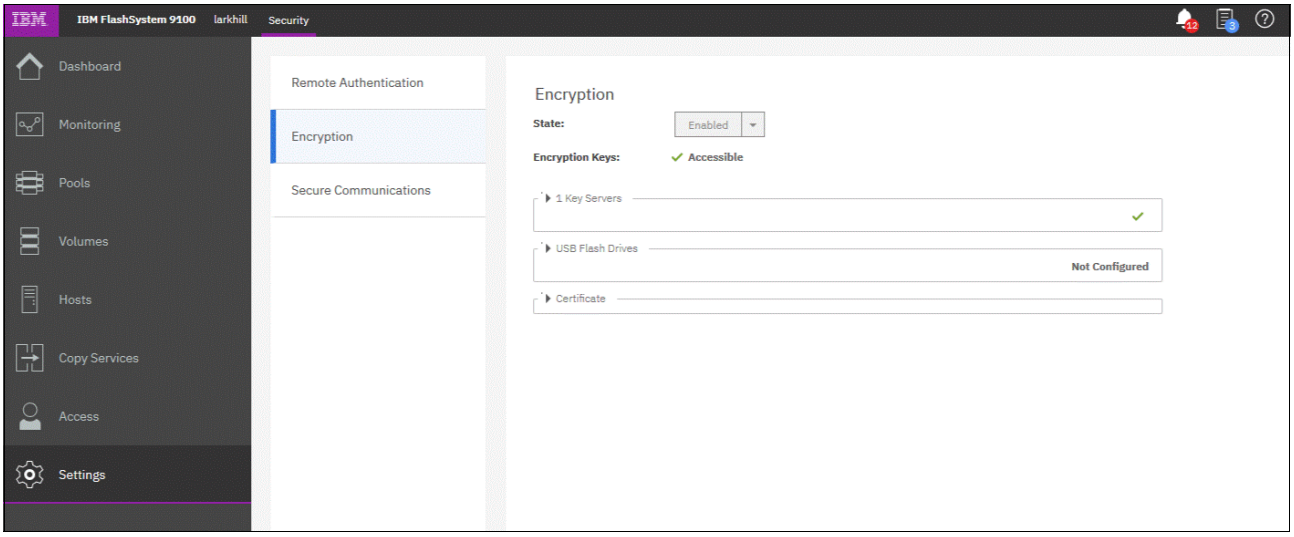


Figure 1 Ensuring encryption is enabled

Navigate to the Pools window and locate the Storage Pool (or Pools) that contain the FCMs. Select the **Delete Pool** option to remove the FCMs from the Pool, as shown in Figure 2.

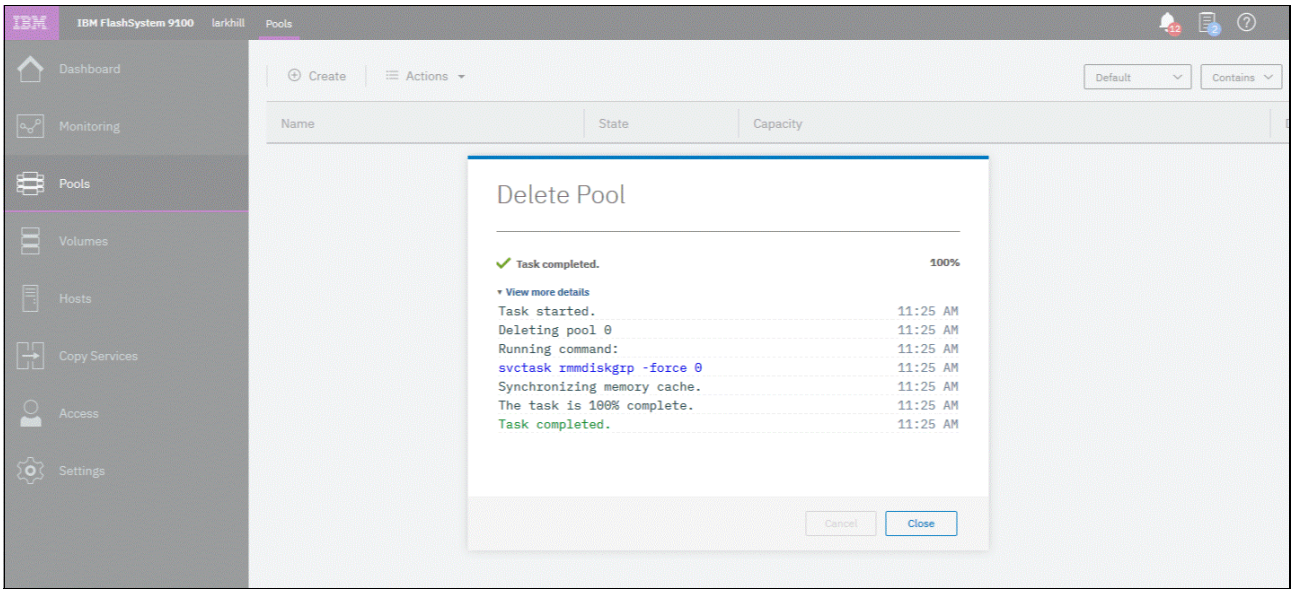


Figure 2 Selecting the Delete option

By using the same window, select the **Create Pool** option and ensure that encryption is enabled. This process creates a Storage Pool into which you can add the FCM devices, as shown in Figure 3.

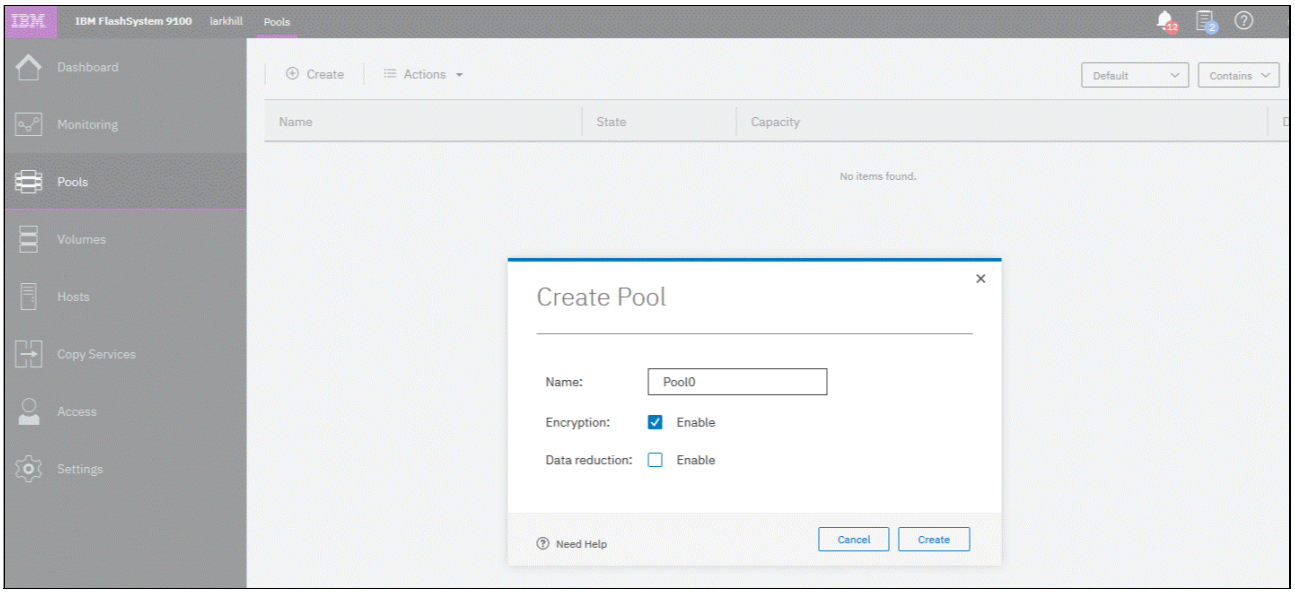


Figure 3 Select the Create Pool option ensuring encryption is enabled

Then, select the Storage Pool that you just created and click **Add Storage**. Because FCM devices are classified as internal storage, select **Internal** and add the same set of FCM devices that you removed from the previous Storage Pool into this new Storage Pool, as shown in Figure 4 on page 4.

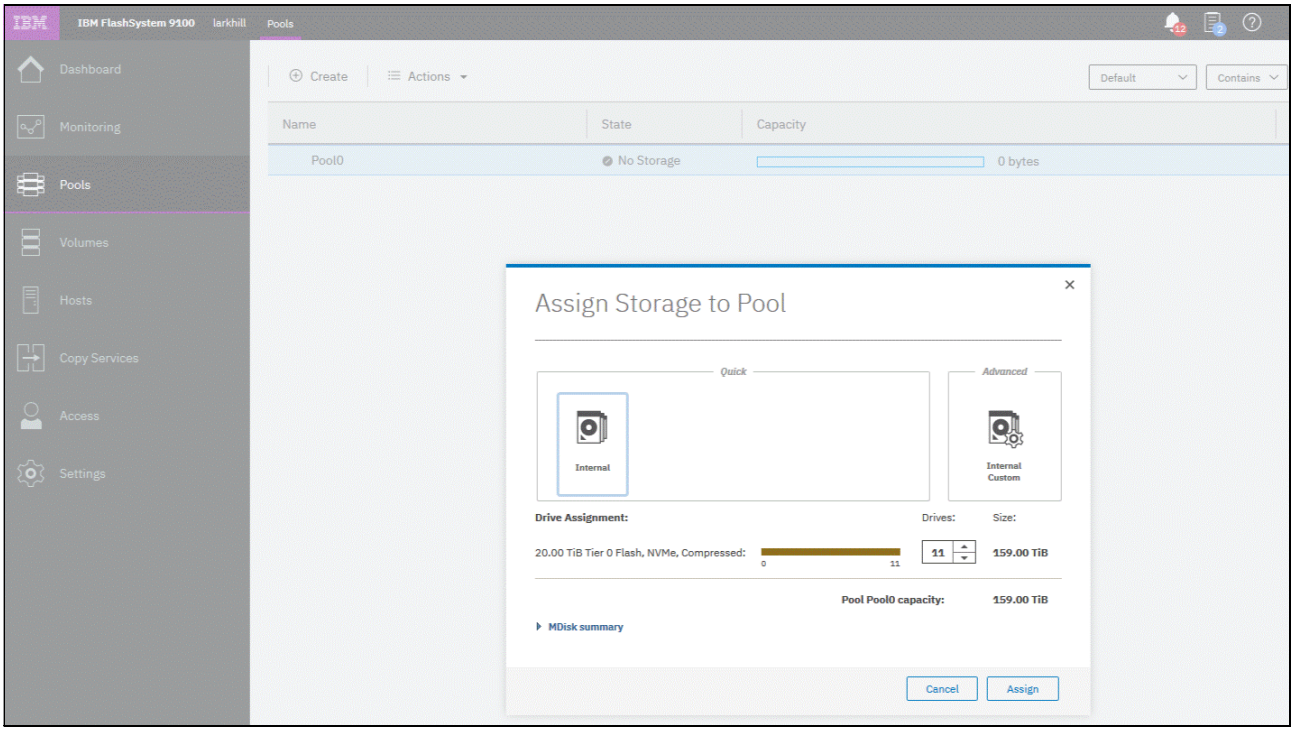


Figure 4 Assigning the storage to a pool

A dialogue appears that shows the FCM devices being added to the pool. Assuming that the task completes successfully, this process writes new MEKs to the FCMs over the location of the old keys and the cryptographic erase is complete, as shown in Figure 5.

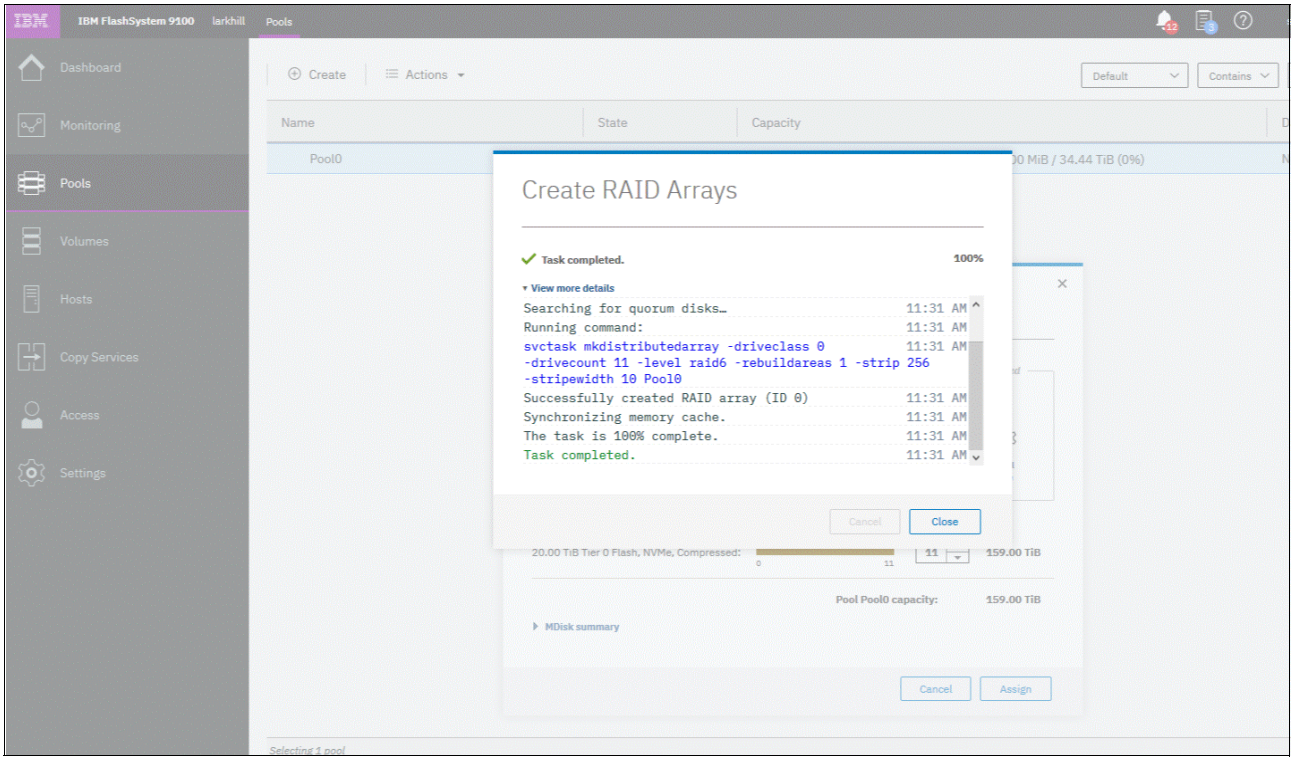


Figure 5 Cryptographic erase is complete

You can validate these steps by using the Audit Log. You see an entry for remove pool (**rmmdiskgrp**), followed by an entry for create pool (**mkmdiskgrp**) and then, an entry for adding the FCMs to the pool (**mkdistributedarray**), as shown in Figure 6.

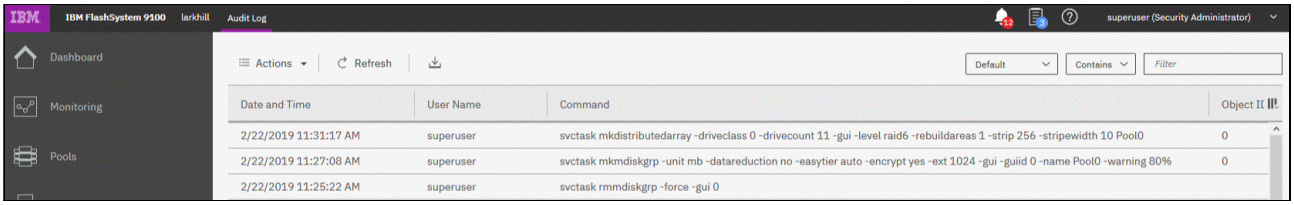


Figure 6 Validating the steps by using the Audit Log

It is not possible to confirm by using the GUI that the set of FCM devices that were removed were the set of FCMs that were added back into the pool. However, if you are performing a mass cryptographic erase of all FCMs in the system, you can add them back into the new pool and confirm that the **-drivecount** parameter on the command **mkdistributedarray** matches the number of drives in the system.

Authors

This paper was produced at IBM Hursley, UK.

Matt Smith is a FlashSystem Offering Manager with responsibility for the FlashSystem V9000 and FlashSystem 9100.

Thanks to the following people for their contributions to this project:

Bill Scales
IBM Hursley

Paul Cashman
IBM Hursley

Brent Yardley
IBM Oregon

This project was managed by:

Jon Tate
IBM ITSO

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an IBM Redbooks® residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks
- Follow us on Twitter:

  http://twitter.com/ibmredbooks
- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806
- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm
- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

Easy Tier®	IBM FlashSystem®	Storwize®
IBM®	Redbooks®	
IBM FlashCore®	Redbooks (logo)  ®	

The following terms are trademarks of other companies:

Other company, product, or service names may be trademarks or service marks of others.

REDP-5529-00

ISBN 0738457604

Printed in U.S.A.