IBM Cloud Object Storage System™
Version 3.8.2

FIPS Reference Guide

This edition applies to IBM Cloud Object Storage System™ and is valid until replaced by new editions.

Contents

Chapter 1. Overview

The FIPS edition of the IBM Cloud Object Storage System™ is a FIPS compliant version of the IBM Cloud Object Storage System™. The system uses the IBM Cloud Object Storage System™ FIPS Cryptographic Module v1.1 certificate #2599 as the encryption module for the platform. All cryptographic operations performed on the data stored in the FIPS Edition of the object store are executed in a FIPS compliant manner. This version of the system only operates in FIPS mode and it may not be disabled on the system.

Chapter 2. Purpose

The FIPS edition is designed to assure customers that, when encryption is enabled, data they store on the system will be encrypted using FIPS compliant algorithms.

Chapter 3. Terminology and components

FIPS

Federal Information Processing Standard, a U.S. government computer security standard.

Chapter 4. Hardware

FIPS is certified on Intel Xeon processor with AES-NI and Intel Xeon processor without AES-NI (single-user mode). The appliances currently certified are Accesser® 4105, Accesser® F5100, Manager 3105, Slicestor® 2448, Slicestor® 3448. Refer to our security policy for steps to validate the FIPS configuration.

Chapter 5. FIPS mode operation

Data Migrations and Vault Proxies are configured using the Cloud Object Storage Manager GUI and/or REST API. This section summarizes the main configuration steps for a configuration that includes a vault proxy and source vault rename. Please consult the *IBM Cloud Object Storage System™ Manager Administration Guide* for detailed information regarding setup and configuration using either the Object Storage Manager GUI or REST API.

The FIPS certification has a minimal impact on the configuration, monitoring and usability of the IBM Cloud Object Storage System™. Please consult the *IBM Cloud Object Storage System™ Manager Administration Guide* for more detailed information regarding setup and configuration using either the Manager Web Interface or REST API. The remainder of this section will call out specific differences that can be observed when using FIPS.

Login banner image

The banner image on the login page identifies that the IBM Cloud Object Storage Manager™ is operating in FIPS mode.

Login Page

The login page in FIPS mode contains three distinctions:

- Login banner image: The image indicates FIPS
- Header: The header also idicates that the Manager is operating in FIPS mode. The header is visible on every page.
- FIPS Certification: There is a link to view the security policy and FIPS certification on the NIST website.

Device summary section

On the Monitor Device page for each device, the Manager UI will display the status of FIPS operation on the device. The UI indicates success and error summaries.

Device Summary page

There is a new filter on the Device Summary page to filter devices by their FIPS status.

Events

An incident has been added to the system. If a FIPS error occurs on a device, an event will open the incident. When the FIPS issue is resolved, the incident will be closed by a subsequent event.

FIPS errors

The IBM Cloud Object Storage System™ does periodic FIPS self tests. If a self test fails, the software will shut itself down, preventing IO and IBM Cloud Object Storage System™ Manager UI/API access. In these cases, the Manager will respond to all requests with a 503 error. A device reboot may be required to resolve the condition.

IBM Cloud Object Storage System™ Manager API

In the **View System** API method, each device object will contain a new object, `fips`. This object will contain two fields:

- `enabled`: This is a boolean that will always be `true`.
- `functioning`: This is a boolean that represents if there is a problem with FIPS operational mode on the device. A value of `false` corresponds to an open incident and an error on the device's summary section, as described above.

Please consult the *IBM Cloud Object Storage System™ Manager REST API Guide* for more detailed information regarding the API.

FIPS migration

About this task

A non-FIPS IBM Cloud Object Storage System™ can be migrated to a FIPS version, operating in a valid in FIPS configuration. The migration might include hardware upgrades, software upgrades, data migration, and certificate renewals. A prerequisite for migrating an IBM Cloud Object Storage System™ to a FIPS Edition is that the system be on a release of the IBM Cloud Object Storage System™ OS that is at least 3.8.0 and a predecessor of the FIPS Edition version targeted for install. For example an IBM Cloud Object Storage System™ version 3.8.0 system can be migrated to an IBM Cloud Object Storage System™ version 3.8.2 FIPS Edition, but an IBM Cloud Object Storage System™ 3.8.2 cannot be migrated to an IBM Cloud Object Storage System™ 3.8.2 FIPS Edition. The system must also be a version of the OS that is greater than the FIPS Edition version number - 2.

To migrate a non-FIPS installation to a FIPS valid configuration, all encrypted data that is stored in the system needs to be migrated from existing vaults to new FIPS-compliant vaults on FIPS certified hardware. This is the only way to assure that the system contains only data that is encrypted using FIPS-compliant cryptographic algorithms. Data that is stored on the system in plain text also needs to be migrated to vaults stored on FIPS certified hardware, as the FIPS configuration does not allow for a system with mixed hardware components by policy. Administrators must be sure to run vault migrations after the software and hardware are upgraded to a FIPS version. Migrating data after the upgrade enables claims that the data was encrypted using FIPS-approved cryptographic algorithms. Following the subsequent instruction set for upgrading from a non-FIPS version of the OS to a FIPS Edition results in a system that is operating in a FIPS-compliant configuration with data that is encrypted using FIPS certified algorithms. If the system being upgraded already has FIPS-compliant hardware and only the software needs to be updated, all steps that are related to hardware replacement, including Manager back up and restore, can be skipped.

Procedure

1. Assure the system is running a version of IBM Cloud Object Storage System™ capable of the upgrade to the wanted FIPS version according to the preceding text.
2. Back up the IBM Cloud Object Storage Manager™.
3. Replace the Manager Device with FIPS certified hardware that is listed in the Security Policy.
4. Restore the Manager Device from the backup.
5. Install FIPS certified Accesser® Devices and Slicestor® Devices on the target system.
6. Upgrade the system software to a FIPS version of the IBM Cloud Object Storage System™ software. Refer to the *System Upgrade Guide* for instructions on how to upgrade your system.

   Note: After you upgrade the Manager, if you have to replace an OS drive on any device, you cannot use the standard drive OS replacement procedure. Instead of installing the original load to the drive, install the FIPS load that you are upgrading to.

7. Rekey the devices and assure all device rekey requests are complete. Restart Accesser devices after performing a rekey. Refer to the "Rekey device" topic in the Maintenance chapter of the *Manager Administration Guide* for instructions on how to rekey devices
8. Create new storage pools on FIPS Slicestor® Devices.
9. Add the new Accesser® Device to the existing access pool and update clients, load balancers, or both to reference the new Accesser Devices. This step refers to customer equipment and application that are not a part of the IBM Cloud Object Storage System™ appliance.
10. Remove all non-FIPS Accesser Devices from the access pool.
11. If you want new vaults, create them on the new storage pools. Vault migration allows for the creation of new vaults automatically.
12. Use the Vault Migration feature to migrate the data to the new vaults. Refer to the *IBM Cloud Object Storage System™ Data Migration Guide* for instructions.
13. After data migration is complete, remove any remaining non-FIPS certified hardware.

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
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

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.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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 the names and addresses used by an actual business enterprise 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.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., 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 www.ibm.com/legal/copytrade.shtml.

Accesser®, Cleversafe®, ClevOS™, Dispersed Storage®, dsNet®, IBM Cloud Object Storage Accesser®, IBM Cloud Object Storage Dedicated™, IBM Cloud Object Storage Insight™, IBM Cloud Object Storage Manager™, IBM Cloud Object Storage Slicestor®, IBM Cloud Object Storage Standard™, IBM Cloud Object Storage System™, IBM Cloud Object Storage Vault™, SecureSlice™, and Slicestor® are trademarks or registered trademarks of Cleversafe, an IBM Company and/or International Business Machines Corp.

Other product and service names might be trademarks of IBM or other companies.

Homologation statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact an IBM representative or reseller for any questions.

Printed in USA