ORACLE

System Independent Best Practice for Hard Disk Scrubbing

Document Number and Revision:	923-3723-02 Rev 02

Overview

This document provides best practice guidelines for scrubbing data from disks when returned from a customer and as part of the normal test process.

Audience

This document is for all personnel responsible for testing Oracle computer products.

Table of Contents

Introduction

Manufacturing teams must ensure that disks delivered to customers contain no visible or recoverable data. In cases where disks are returned to Oracle from a customer side, the disks must be thoroughly erased so that customer data is not easily recoverable. Disks that leave the factory at the end of the test process must be sufficiently scrubbed so that the test data is not visible.

This document specifies the requirements and processes that must be used by all business units to scrub HDD and SSD devices prior to shipment to customers. Alternative processes using either software or hardware are acceptable as long as the requirements specified in this document are met.

Table I-1 Terms and Definitions

Acronym	Definition
HDD	Hard Disk Drive – Rotating magnetic disks
JBOD	Just a Bunch of Disks, a RAID configured as individual disks
RAID	Redundant Array of Inexpensive Drives
SSD	Solid State Disk – NVRAM based disk drive
VTOC	Volume Table of Contents, defines slices of a partition.

1. Issues to be Considered

The purpose of erasing data from a disk is to reduce the possibility of accessing the data left behind by the previous use, either during testing or in a customer site. It is very difficult to completely eliminate the possibility of data recovery, so one must adopt a procedure that is consistent with some pre-determined policies. There are two circumstances that give rise to two policies and therefore, two slightly different options in the scrub process.

1.1 Data Left on a New Disk by Test Process

The data left on the disk is the test data which is essentially random bits. There may, however, be files defined in the file systems which reside in the standard partitions used by the operating system (OS). There is no need to erase the data from such disks but the presence of files must be obscured. The file systems of the partitions used in testing must be rewritten as empty.

1.2 Data Left on a Disk Returned to Oracle After Customer Use

A disk returning from a customer site is assumed to be formatted differently from when it left the factory, and assumed to contain customer data. Before the disk is shipped to a new customer, the disk must be scrubbed to remove both the data and the presence of files. Writing data over the entire disk in a single pass is sufficient to make the recovery of any data a difficult and an expensive process. Writing zero data over the entire disk and relabeling it makes the disk appear as if it is a new product shipped from a vendor.

1.3 Status of HDD Write Cache

The HDD write cache state is initially determined by the Oracle part number. If a customer puts the drive into a Zettabyte File System (ZFS) pool, the write cache is enabled as ZFS has its own techniques to ensure data integrity and performance can be improved.

Restoring the state of any HDD device returned from a customer to the correct state based on the Oracle part number is a separate issue and not addressed in this best practice. It is a requirement, however, that the state of the write cache of any HDD scrubbed by a process that implements this best practice is not changed by the process.

2. Best Practice Requirements

The requirements in this section must be met by any scrub process that is in compliance with this best practice. These requirements are broken down in order to make validation of a process easier. The process that is called for in *Section 3*,

3. Scrub Process, on page 4, is a generic process that meets these requirements.

There are separate requirement sets for the expected three circumstances.

2.1 Factory Test Process

At the end of the test process, each disk present in the system must have its test data made invisible and its labels restored. There is no requirement that the test data must be over-written or otherwise obscured. The requirements are:

1. The volume label, partition map, and VTOC, on each HDD or SSD device must be restored to the values present when the device was shipped to Oracle from the device vendor.

2. File systems on each device must be re-initialized so that any files that were present are no longer accessible.

3. The scrub process steps for the end of the factory test process must be executed prior to software download (SWDL) or at the end of the last test suite prior to shipping if SWDL is not part of the test process for a particular platform.

2.2 Customer Returned System

All customer data that may be presented on the disk must be removed, so that no basic recovery process can make the customer data visible.

1. Each returned HDD or SDD must be labeled, partitioned, and formatted to a standard that is appropriate for the scrubbing process that follows.

2. The amount of wear of any SSD must be determined to ensure that a reshipped device does not have a significantly shorter expected life than a new device.

3. All the data on each device must be overwritten so that no software recovery of the customer data is possible.

4. Each device must be labeled, partitioned, and formatted as if it arrived new from the device vendor, so that it enters the factory test process as a new device.

5. The state of each HDD write cache must be preserved by the scrub process, so that its state can be reliably determined outside of the scrub process.

6. The scrubbed and restored devices are put through the standard test process prior to shipping to a new customer.

2.3 Special Request

These occur when disks contain confidential information that require thorough disk scrubbing for the best security. These situations arise when systems are used by the customer for Proof of Concept (POC) or Customer Staging. Customers who use a system in-house to hold confidential data may scrub the disks prior to returning the system to Oracle.

1. The disk is prepared for scrubbing as in point *1* and *2*, in *Section 2.2*, 2.2 Customer Returned **System**, on page 4.

2. All the data on the device must be overwritten according to the customer's instructions. This is likely to involve writing multiple patterns multiple times over the entire contents of the device.

3. The device is prepared and tested according to point *4* and *6* in *Section 2.2*, 2.2 Customer Returned **System**, on page 4.

3. Scrub Process

This process, described in generic terms, is appropriate to many platforms. Each business unit may implement the steps of this process as appropriate to the platform, but the process must be validated against the requirements in *Section 2*, 2. Best Practice Requirements, on page 3.

1. For customer returned systems, it is essential that all customer data is overwritten. RAID systems keep private configuration data which may reveal some aspects of customer

information. For these systems, it is safest to delete any RAID configurations (configure as JBOD) so that each drive is scrubbed separately.

2. For SSD devices returned from a customer, it is necessary to recover the wear information and decide whether to replace the device or continue. It is unlikely that the short Try and Buy periods would allow enough device activity to cause significant wear but some environments may cause excessive wear.

3. The state of the write cache must be determined so that it can be restored at the end of the process, in case the scrub process alters the state (for example, introducing the device into a ZFS pool).

4. For devices returned from a customer, it is required to label, partition, and format the drive to a single standard. Note that some partitioning and formats do not support disks larger than 1TB. A uniform and long term process should use a partition and formatting standard that will work with both small and large disks.

5. For customer returned devices, write a single pass of zeros over the entire drive. For devices that support it, secure erase should be used.

6. Label, partition, and format the drive as if received new from the drive vendor. This is done for both factory test and customer return as the factory testing may overwrite label, partition, and format information.

7. Restore the state of the write cache based on the state captured in *Step 3*.

8. Customer returned systems now enter the test process as though the disk devices were new from the device vendor. RAID configurations will be restored by the test process.

9. After scrubbing at the end of the factory test process, configure any RAID systems that are appropriate to the product.

10. Initialize file systems on the appropriate slices in the appropriate partitions or RAIDs.

4. Time Estimates

The HDD scrub times for three different options are covered here. The times given here are for a single HDD on a single controller. Multiple HDDs on the same controller require roughly the same amount of time each, as compared with a single HDD. Multiple HDDs on multiple controllers multiply the stated times roughly by the number of HDDs divided by the number of controllers, assuming that the HDDs are equally distributed over the controllers.

Scrub times for SSDs are significantly lesser. If an SSD device supports Secure Erase, (and it has been validated to function properly) an erase can take as little as two minutes for 32GB.

4.1 Factory Test Process

Approximately 0.1 hour is needed to test a disk.

4.2 Customer Returned System

The expected scrub times for selected disk sizes are as follow:

	73GB	146GB	500GB	1TB
Minimum hours	0.3	0.6	1.8	3.6
Expected hours	0.4	0.8	2.8	5.7
Maximum hours	1.4	2.8	9.4	18.8

4.3 Special Request

Timings for special requests depend on the precision of customer instructions, but generally take significantly more time than those stated in *Section 4.2*, 4.2 Customer Returned System, above. Such special requests typically require the entire disk to be written five to seven times with specific data patterns. Under such circumstances, the times from *Section 4.2*, 4.2 Customer Returned System, above, need to be multiplied by the number of write passes required

Reference Documents and Records

Document Title	Number	ESO Controlled		Quality Record	
		Yes	*No*	*Yes*	*No*
None	n/a		x		x

Document History and Approvals

923

Dash	Rev	Date	Description of Change	Originator
01	A	18 May 2009	Initial release.	N/A
02	A	25 May 2021	Removed out of date links and Originator name from the document history and approval table. Updated title, replaced Sun with Oracle throughout.	N/A

Related Information

REASON FOR CHANGE:
Removed out of date links and Originator name from the document history and approval table. Updated title, replaced Sun with Oracle throughout.

➢ When Document Template is complete, email source file to eso_business_docs_us_grp@oracle.com

➢ All hard copies of this document are uncontrolled and are to be used for reference only.

➢ For questions or comments about this document, please send an email to:
Ask_Document_Question@beehiveonline.oracle.com