Standard Operating Procedure (SOP)

Replacing a Failed Hard Drive in a Data Center RAID Array

OBJECTIVE

To provide step-by-step instructions for safely and efficiently replacing a failed hard disk drive (HDD or SSD) in a RAID array within the data center, ensuring data integrity, minimal downtime, and compliance with operational and security standards.

SCOPE

This SOP applies to all data center operations staff responsible for hardware maintenance on server storage arrays (RAID 1, 5, 6, 10, etc.) in production, staging, or backup environments.

PREREQUISITES

- **Training:**
  Personnel must be trained in RAID concepts, server hardware, and ESD (electrostatic discharge) precautions.
- **Authorization:**
  Maintenance must be approved by the Data Center Operations Manager or designated authority.
- **Access:**
  Valid access credentials for the data center and the relevant server rack.
- **Tools & Equipment:**
  - ESD wrist strap and mat
  - Replacement drive (correct model, capacity, and interface)
  - Screwdrivers or drive caddies as required
  - Flashlight (if rack lighting is insufficient)
  - Labeling materials
- **Documentation:**
  - Access to the server hardware manual and RAID controller documentation
  - Most recent backup verification report
  - Maintenance logbook or digital ticketing system

PROCEDURE

1. Preparation

1.1 Notification and Scheduling

- Notify stakeholders (system owners, NOC, affected users) of planned maintenance window.
- Schedule replacement during approved maintenance or low-usage period, unless the RAID level allows hot-swap with zero downtime.

Standard Operating Procedure (SOP)

1.2 Pre-Replacement Checks

- **Verify Failure:**
  Use monitoring software (e.g., vendor RAID management tools, SNMP alerts) to confirm the identity and location of the failed drive.
- **Backup Confirmation:**
  Confirm a recent, successful backup exists for the affected system.
- **Review Documentation:**
  Review the server's RAID configuration, slot mapping, and drive specifications.

1.3 Safety Precautions

- Wear an ESD wrist strap and connect it to an approved ground point.
- Clear the area of liquids and unnecessary equipment.
- Ensure you have the correct replacement drive and tools before entering the data center.

2. Removal of Failed Drive

2.1 Locate the Server and Drive

- Authenticate and enter the data center following physical access SOP.
- Locate the correct rack and server using asset tags and documentation.
- Identify the failed drive by:
  - RAID management software (slot number, drive serial)
  - Physical indicators (amber/red LED, drive status display)

2.2 Prepare the System

- For hot-swappable systems:
  - Confirm with RAID management that drive removal is supported without shutdown.
- For non-hot-swappable systems:
  - Gracefully shut down the server following OS and application procedures.

2.3 Remove the Drive

- Unlock and open the server chassis or drive bay as needed.
- Carefully unlatch and remove the failed drive, noting its slot position.
- Place the failed drive in an ESD-safe bag and label it with the date, server ID, and failure description.

3. Installation of Replacement Drive

3.1 Prepare the New Drive

- Verify new drive matches required specifications (model, capacity, interface).

- Remove from packaging and handle only by the edges.

3.2 Insert the New Drive

- Insert the replacement drive into the correct slot, ensuring a firm connection.
- Secure the drive with caddy or screws as required.
- Close and lock the chassis or drive bay.

3.3 Power On (if applicable)

- For systems that required shutdown, power on the server and monitor boot sequence for drive detection.

4. RAID Rebuild and Verification

4.1 Initiate Rebuild

- Use RAID management software or controller BIOS to confirm the new drive is recognized.
- If not automatic, manually assign the new drive as a replacement and initiate the rebuild process.

4.2 Monitor Rebuild

- Monitor rebuild progress via management console.
    - Record estimated time to completion.
    - Watch for errors or warnings.
- Do **not** perform heavy I/O operations on the array during the rebuild unless the RAID level supports it.

4.3 Post-Rebuild Checks

- Verify RAID status is healthy/optimal after rebuild completes.
- Check system logs for errors.
- Run a consistency check or scrub if supported by the RAID controller.

5. Documentation and Communication

5.1 Update Maintenance Records

- Log the replacement in the maintenance system, including:
    - Date/time
    - Technician name
    - Server and drive identifiers
    - Serial numbers (old and new drive)
    - RAID status before and after

  - Any issues encountered

5.2 Notify Stakeholders

- Inform system owners and NOC of task completion and current RAID status.
- Schedule follow-up monitoring if required.

5.3 Failed Drive Handling

- Store failed drives in a secure, labeled area for warranty return, secure erasure, or destruction per company policy.

POST-PROCEDURE

6. Final Verification

- Confirm that all server panels and racks are closed and locked.
- Remove tools and waste from the work area.
- Ensure monitoring systems are reporting normal status for the array.

7. Audit and Review

- Review the incident in the next team meeting if there were complications.
- Update SOP if new issues or improvements were identified.

DOCUMENTATION

- All records (maintenance logs, drive serials, rebuild reports) must be retained for at least 2 years.
- Any deviations from this SOP must be documented and reported to the Data Center Operations Manager.