Disaster Recovery

This chapter describes the disaster recovery process and the health check feature.

Overview

There are two partitions in NCS 1020: The controller SSD (CPU partition) and chassis SSD (Disaster Recovery partition). The Disaster Recovery partition contains all the backup configurations such as ISO images, RPMs, and system configuration files. When the node is corrupted, the Disaster Recovery feature allows the CPU to be replaced with the existing configuration. After replacing the CPU, the node reboots and comes up by restoring the software and configuration files from the chassis SSD without traffic loss.

Note When Chassis SSD is corrupted and replaced, the new chassis SSD takes backup of the running software and configuration files from the controller SSD without traffic loss.

SSD OIR

The chassis Solid State Drive (SSD) is a semiconductor-based storage device. It is used to store a backup of the software and configuration which will be used by the CPU to re-boot in case of any node failure. Online Insertion and Removal (OIR) is an operation that allows you to replace any faulty module in a system. In NCS 1020, the SSD OIR feature allows the chassis SSD to be removed and replaced anytime.

CPU Controller Replacement Considerations

You must consider the following points for CPU replacement.

Table 1: CPU Controller Replacement

Type of Replacement	Result
When the CPU is removed from the chassis.	NCS 1020 chassis runs in a headless mode which is non-traffic impacting.
When the CPU is replaced with another CPU having the same software and RPMs as in the chassis SSD.	The configuration is restored from the chassis SSD.
When the CPU is replaced with another CPU having different software and RPMs as in the chassis SSD.	The Disaster recovery process starts. In this case, the node boots with the software from the chassis SSD and the configuration is also restored from the chassis SSD.

Chassis SSD Replacement Considerations

The chassis SSD can be removed in NCS 1020.

You must consider the following points for chassis SSD replacement.

Table 2: Chassis SSD Replacement

Type of Replacement	Result
When the chassis SSD is removed while the RP is running.	Disaster Recovery boot is disabled and an alarm is raised.
When the chassis SSD is removed.	The Disaster Recovery Unavailable alarm is raised.
When the chassis SSD is replaced with another chassis SSD having the same software and RPMs as in the CPU SSD.	The configuration is backed up from the CPU SSD.
When the Chassis SSD is replaced with another chassis SSD having different software and RPMs as in the CPU SSD.	Software, RPMs, and the configuration are backed up from the CPU SSD.
When the Chassis SSD is replaced with a spare received from Cisco manufacturing or RMA process.	Software, RPMs, and the configuration are backed up from the CPU SSD.

Health Check of Backup ISO Image

The Health Check feature ensures error-free booting of NCS 1020 chassis during disaster recovery operations. NCS 1020 has a partition for disaster recovery where the backup ISO image is stored. The backup ISO image is stored in the chassis SSD.

The chassis SSD content is audited against the running software by the install process in the background every 12 hours to detect corruption. If the ISO image is corrupted, the software will recover it by copying from the

backup location. If the software fails to synchronize with the chassis SSD, then the **Disaster Recovery ISO Image Corruption** alarm is raised. See the *Troubleshooting Guide for Cisco NCS 1020* to clear the alarm.

Automated File Management System

Table 3: Feature History

Feature Name	Release Information	Feature Description
Automated File Management System	Cisco IOS XR Release 24.4.1	The new Automated File Management System is designed for efficient file handling on each node. This system automatically archives older files and removes them from local nodes to free up valuable SSD space. It manages the following types of files: • System-generated log files • Showtech-related residual files

The automated file management system archives older files to free up valuable SSD space by deleting them from the local nodes.

Types of files

The SSD stores two types of files that are generated by

- **User**: creates and owns files for requirement purposes and deletes the files when are no longer needed.
- **System**: organizes files automatically based on the file content and the application that created the content such as .log and showtech-related residual files.

  Automated file management is applicable for the system-generated files.

How the automated file management system works

These stages describe how the automated file management works for various files.

Log files

The NCS 1014 system uses the log rotation configurations to manage log files as required.

1. The system checks for the *.log* files exceeding 10 MB file size.

Note This threshold is applicable for `/tmp` folder files only. For files in other folders, the system uses a different threshold and follows the same process.

2. After locating the file, the system
   a. archives that file with .gz extension, and
   b. creates a new .log file with the same name.

3. The system then maintains one active log file and two archived files.
4. When new files are archived, the system deletes the oldest archived file to make sure that only the two most recently archived files and the current log file are retained.

showtech-related residual log files

1. The system generates the residual files during the collection of logs when **Showtech logs** is in operation.
2. After collecting the logs, the system automatically removes these residual files to conserve space.