Database Disk Image Malformed

Symptom

Server Backup returns the following error message:

```
"Error Server [11] reset(): database disk image is malformed(11)"
```

Cause

This error may be caused by a hardware, file system or Operating System fault causing corruption to the Disk Safe file. Disk Safe viability, in part, relies on the stability of the underlying hardware and Operating System of the host storage device.

Resolution

The safest solution is to create a new Disk Safe as soon as Server Backup reports that the database disk image is malformed. In some situations, the Disk Safe may still be usable for restoring recovery points that were created before the Disk Safe reported a corruption. However, we have no way to determine the extent of the corruption or if the workaround mentioned below will be able to repair the Disk Safe. In addition, we do not expect that a corrupt Disk Safe will be successful in a bare metal restore.

Workaround

You may attempt to repair the Disk Safe by running a Disk Safe Verification (DSV) task (introduced in Server Backup v5.2.0) against the Disk Safe with the malformed image. The DSV will check the most recent recovery point to ensure all blocks are accounted for. If the disk safe fails to verify, a repair attempt will be made during the next replication task which will attempt to reconcile any missing blocks from the recovery point.

> **Note**
> For more information on DSV, please review our documentation: Wiki Article
>
> Please note that DSV verifies only those recovery points with an available status. DSV does not verify recovery points with a locked or incomplete status.

Additional Suggestions

- If DSV does not find any errors with the recovery point, the problem may have originated outside of the disk safe. In this case, we recommend that you create a new Disk Safe and also check the disks that host the Disk Safe and also review the operating system logs for failures related to I/O, disk space or file system.
- Please make sure your hardware and Operating System follow the recommendations in our Disk Safe Best Practices

Additional Information - Corruption of Data Archived in the Disk Safe

The Disk Safe is highly reliable and robust. Even with industrial grade protection, there are still ways for your data to become lost or damaged beyond repair. If any of the following events occur, you may corrupt your Disk Safe. If your Disk Safe becomes corrupted, you may lose all or some of your archived data. If Disk Safe is corrupted by any one of the events below, it can not be repaired:

- Exhaustion of available memory or storage space on the machine hosting the Disk Safe, or the Server Backup Manager itself.
- Delete a file in the Disk Safe Folder.
- Make an incomplete copy of the Disk Safe folder thereby corrupting the copy.
- Making a copy of the Disk Safe files when the Disk Safe is open and being written to by the CDP Server thereby corrupting the copy.
- A hardware or O/S fault causing incorrect data to be written to Disk Safe files.
- A faulty hard disk or storage controller failing to flush volatile cache when requested can break protection from unclean shutdowns and power failures.
- Rogue process writing to the Disk Safe files.
- Soft Linking any files Inside of the Disk Safe Folder. If the block deltas store and its associated write journal (created at run time) end up on different file systems data loss can occur if there is a crash or power failure.
- Failure to store the Disk Safe on a journaling file system can cause the write journal to be lost or moved to lost+found. If this happens the Disk Safe may likely become damaged beyond repair.

> Note
> Windows NTFS and Linux Ext3, Ext4, XFS, and ReiserFS ARE Journaling File Systems.
> • NFS (Linux / Unix Network File System) may cause faults or bugs.
> If using NFS on Linux, we recommend you use the latest available NFS versions and latest stable Linux kernels, and do not export NFS file systems with asynchronous writes (async option).