Creating, Modifying, and Deleting a Change Journal

3 out of 9 rated this helpful

Administrators can create, delete, and re-create change journals at will. An administrator should delete a journal when the current update sequence number (USN) value approaches the maximum possible USN value, as indicated by the **MaxUsn** member of the **USN_JOURNAL_DATA** structure. An administrator might also delete and re-create a change journal to reclaim disk space. To perform this and all other non-programmatic change journal operations, you must have system administrator privileges. That is, you must be a member of the Administrators group.

To create or modify a change journal on a specified volume programmatically, use the **FSCTL_CREATE_USN_JOURNAL** control code.

When you create a new change journal or modify an existing one, the NTFS file system sets information for that change journal from information in the **CREATE_USN_JOURNAL_DATA** structure, which **FSCTL_CREATE_USN_JOURNAL** takes as input. **CREATE_USN_JOURNAL_DATA** has the members **MaximumSize** and **AllocationDelta**.

MaximumSize is the target maximum size for the change journal in bytes. The change journal can grow larger than this value, but at NTFS file system checkpoints the NTFS file system examines the journal and trims it when its size exceeds the value of **MaximumSize** plus the value of **AllocationDelta**. (At NTFS file system checkpoints, the operating system writes records to the NTFS file system log file that allow the NTFS file system to determine what processing is required to recover from a failure.)

AllocationDelta is the number of bytes added to the end and removed from the beginning of the change journal each time memory is allocated or deallocated. In other words, allocation and deallocation take place in units of this size. An integer multiple of a cluster size is a reasonable value for this member.

If an administrator modifies an existing change journal to have a larger **MaximumSize** value, for example if a volume is being re-indexed too often, the change journal simply receives new entries until it exceeds the new maximum size.

To delete a change journal, use the **FSCTL_DELETE_USN_JOURNAL** control code. When you use this operation, it walks through all of the files on the volume and resets the USN for each file to zero. The operation then deletes the existing change journal. This operation persists across system restarts until it completes. Any attempt to read, create, or modify the change journal during this process fails with the error code **ERROR_JOURNAL_DELETE_IN_PROGRESS**.

You can also use the **FSCTL_DELETE_USN_JOURNAL** control code to determine if a deletion started by some other process is in progress. For example, your application, when it is started, can determine if a deletion is in progress. Because journal deletions persist across system restarts, services and applications started at system restart should check for an ongoing deletion.

Change journals are not necessarily created at startup. To create a change journal, an administrator may do so explicitly or start another service that requires a change journal.

Community Additions