### ntfs-logfile

NTFSトランザクションログファイルから、ファイル名、作成/修正/アクセス日時、Redo/Undo操作タイプを照会します。本コマンドにより、ファイルの作成、削除、名前変更などの履歴を確認できます。

#### 構文

ntfs-logfile [zipcharset=CHARSET] [zippath=ZIPFILE\_PATH] FILE\_PATH

必須パラメータ

**FILE\_PATH**

NTFSトランザクションログファイルのパス。ファイルパスにワイルドカード（\*）を使用すると（例：D:\data\NTFS\*）、パターンに一致するすべてのファイルを一括で照会できます。zippathオプションと併用する場合は、ZIPファイル内に含まれるNTFSトランザクションログファイルのパスを指定してください。

オプションパラメータ

**zipcharset=CHARSET**

ZIPエントリのエンコーディング形式（デフォルト：utf-8）。以下のドキュメントに登録されているPreferred MIME NameまたはAliasesを使用してください: <https://www.iana.org/assignments/character-sets/character-sets.xhtml>

**zippath=ZIPFILE\_PATH**

ZIPファイルのパス

#### 説明

出力されるフィールドの内容は、以下の表を参照してください。

出力フィールド

|  |  |  |
| --- | --- | --- |
| フィールド | 型 | 説明 |
| access\_at | 日付 | アクセス日時 |
| client\_data\_length | 整数 | レコードサイズ |
| created\_at | 日付 | 作成日時 |
| file\_name | 文字列 | ファイル名 |
| flags | 整数 | フラグ |
| lsn | 整数 | ログファイルシーケンス番号 |
| mft\_head | 文字列 | mftヘッダー |
| mft\_link\_count | 整数 | 当該ファイルを参照するエントリ数 |
| mft\_lsn | 整数 | mftログファイルシーケンス番号 |
| modified\_at | 日付 | 修正日時 |
| page | 整数 | ページ番号 |
| prev\_lsn | 整数 | 前回のログファイルシーケンス番号 |
| record\_type | 整数 | レコードタイプ（2=チェックポイントレコード、1=その他レコード） |
| redo\_len | 整数 | redoデータサイズ |
| redo\_offset | 整数 | redoデータ開始位置 |
| redo\_op | 文字列 | redo操作 |
| undo\_len | 整数 | undoデータサイズ |
| undo\_offset | 整数 | undoデータ開始位置 |
| undo\_op | 文字列 | undo操作 |

Redo\_op, Undo\_op操作コード

redo\_opおよびundo\_opフィールドに出力される操作コードは、以下の表を参照してください。

|  |  |
| --- | --- |
| `redo\_op`/`undo\_op` | 16進値 |
| noop | 0x00 |
| compensation\_log\_record | 0x1 |
| initialize\_file\_record\_segment | 0x2 |
| deallocate\_file\_record\_segment | 0x3 |
| write\_end\_of\_file\_record\_segment | 0x4 |
| create\_attribute | 0x5 |
| delete\_attribute | 0x6 |
| update\_resident\_value | 0x7 |
| update\_non\_resident\_value | 0x8 |
| update\_mapping\_pairs | 0x9 |
| delete\_dirty\_clusters | 0xa |
| set\_new\_attribute\_size | 0xb |
| add\_index\_entry\_root | 0xc |
| delete\_index\_entry\_root | 0xd |
| add\_index\_entry\_allocation | 0xe |
| delete\_index\_entry\_allocation | 0xf |
| set\_index\_entry\_ven\_allocation | 0x12 |
| update\_file\_name\_root | 0x13 |
| update\_file\_name\_allocation | 0x14 |
| set\_bits\_in\_non\_resident\_bitmap | 0x15 |
| clear\_bits\_in\_non\_resident\_bitmap | 0x16 |
| prepare\_transaction | 0x19 |
| commit\_transaction | 0x1a |
| forget\_transaction | 0x1b |
| open\_non\_resident\_attribute | 0x1c |
| open\_attribute\_table\_dump | 0x1d |
| dirty\_page\_table\_dump | 0x1f |
| transaction\_table\_dump | 0x20 |
| update\_record\_data\_root | 0x21 |

#### 使用例

ファイルパスを指定して照会

ntfs-logfile D:\data\NTFS\test\_LogFile

zippathで指定したZIPファイル内のNTFSトランザクションログファイルを照会

ntfs-logfile zippath=D:\data\NTFS.zip NTFS\test\_LogFile

initialize\_file\_record\_segmentまたはdeleteを含むredo\_opログを照会

ntfs-logfile D:\data\NTFS\test\_LogFile | sort lsn | search redo\_op == "initialize\_file\_record\_segment" or redo\_op == "\*delete\*"