NAME

hivexregedit − Merge and export Registry changes from regedit−format files.

SYNOPSIS

```
hivexregedit --merge [--prefix prefix] [--encoding enc] \
        hivefile [regfile]

hivexregedit --export [--prefix prefix] hivefile key > regfile
```

DESCRIPTION

Please note hivexregedit is a low-level tool for manipulating hive files directly. To merge or export registry changes to Windows virtual machines it's better to use **virt−win−reg** (1).

Given a local binary (''hive'') file, there are two modes. `--merge` imports (mer ges) changes from a regedit-format file into the hive. It is similar to using the `/s` switch in W indows regedit.exe.

`--export` exports a Registry key (recursively) into the regedit format.

ENCODING

`hivexregedit` expects that regedit files have already been re-encoded in the local encoding. Usually on Linux hosts, this means UTF−8 with Unix-style line endings. Since Windows regedit files are often in UTF−16LE with Windows-style line endings, you may need to re-encode the whole file before or after processing.

To re-encode a file from Windows format to Linux (before processing it with the `--merge` option), you would do something like this:

```
iconv −f utf−16le −t utf−8 < win.reg | dos2unix > linux.reg
```

To go in the opposite direction, after using `--export` and before sending the file to a Windows user, do something like this:

```
unix2dos < linux.reg | iconv −f utf−8 −t utf−16le > win.reg
```

For more information about encoding, see **Win::Hivex::Regedit** (3).

If you are unsure about the current encoding, use the **file** (1) command. Recent versions of Windows regedit.exe produce a UTF−16LE file with Windows-style (CRLF) line endings, like this:

```
$ file software.reg
software.reg: Little−endian UTF−16 Unicode text, with very long lines,
with CRLF line terminators
```

This file would need conversion before you could `--merge` it.

SHELL QUOTING

Be careful when passing parameters containing \ (backslash) in the shell. Usually you will have to use 'single quotes' or double backslashes (but not both) to protect them from the shell.

CurrentControlSet etc.

Registry keys like `CurrentControlSet` don't really exist in the Windows Registry at the level of the hive file, and therefore you cannot modify these.

`CurrentControlSet` is usually an alias for `ControlSet001`. In some circumstances it might refer to another control set. The way to find out is to look at the `HKLM\SYSTEM\Select` key:

```
$ hivexregedit --export SYSTEM '\Select'
[\Select]
"Current"=dword:00000001
"Default"=dword:00000001
"Failed"=dword:00000000
"LastKnownGood"=dword:00000002
```

''Current'' is the one which Windows will choose when it boots.

Similarly, other `Current...` keys in the path may need to be replaced.

EXAMPLE

```
$ virt-cat WindowsGuest /Windows/System32/config/software > software.hive
$ hivexregedit --export \
    --prefix 'HKEY_LOCAL_MACHINE\SOFTWARE' \
    software.hive '\Microsoft' > ms-keys.reg

$ hivexregedit --merge system.hive \
    --prefix 'HKEY_LOCAL_MACHINE\SYSTEM' additions.reg
```

OPTIONS

--help

Display help.

--debug

Enable debugging in the hivex library. This is useful for diagnosing bugs and also malformed hive files.

--merge

```
hivexregedit --merge [--prefix prefix] [--encoding enc] \
        hivefile [regfile]
```

Merge `regfile` (a regedit-format text file) into the hive `hivefile`. If`regfile` is omitted, then the program reads from standard input. (Also you can give multiple input files).

`--prefix` specifies the Windows Registry prefix. It is almost always necessary to use this when dealing with real hive files.

`--encoding` specifies the encoding for unmarked strings in the input. It defaults to `UTF-16LE` which should work for recent versions of Windows. Another possibility is to use`ASCII`.

--export

```
hivexregedit --export [--prefix prefix] hivefile key > regfile
```

`key` is a path within the hive `hivefile`. (The key should not contain any prefix and should be quoted to defend backslashes from the shell). The key is exported, recursively, to standard output in the textual regedit format.

`--prefix` specifies the Windows Registry prefix. It is almost always necessary to use this when dealing with real hive files.

--prefix prefix

Hive files and Windows Registry key names are indirectly related. For example, inside the software hive, all keys are stored relative to `HKEY_LOCAL_MACHINE\SOFTWARE`. Thus `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft` appears in the hive file as `\Microsoft`.

The hive format itself does not store this prefix, so you have to supply it based on outside knowledge. (**virt-win-reg** (1), amongst other things, already knows about this).

Usually it is sufficient to pass the parameter `--prefix 'HKEY_LOCAL_MACHINE\SOFTWARE'` or similar when doing merges and exports.

--encoding UTF-16LE|ASCII

When merging (only), you may need to specify the encoding for strings to be used in the hive file. This is explained in detail in "ENCODING STRINGS" in **Win::Hivex::Regedit** (3).

The default is to use UTF-16LE, which should work with recent versions of Windows.

--unsafe-printable-strings

When exporting (only), assume strings are UTF-16LE and print them as strings instead of hex sequences. Remove the final zero codepoint from strings if present.

This is unsafe and does not preserve the fidelity of strings in the original hive for various reasons:

- Assumes the original encoding is UTF-16LE. ASCII strings and strings in other encodings will be corrupted by this transformation.
- Assumes that everything which has type 1 or 2 is really a string and that everything else is not a string, but the type field in real hives is not reliable.
- Loses information about whether a zero codepoint followed the string in the hive or not.

This all happens because the hive itself contains no information about how strings are encoded (see ''ENCODING STRINGS'' in **Win::Hivex::Regedit** (3)).

You should only use this option for quick hacking and debugging of the hive contents, and *never* use it if the output is going to be passed into another program or stored in another hive.

--unsafe
Use heuristics to tolerate certain levels of corruption within hives.

This is unsafe but may allow to export/merge valid keys/values in an othewise corrupted hive.

--max-depth depth
Limits the recursion depth of the export. For example, an export with a max depth of 1 will only include values directly under the specified key/prefix. A max depth of 0 will return no values.

Exports include all child keys by default (fully recursive), which may take a while if the registry hive is large / bloated. This behavior can also be achieved by providing a negative max depth.

SEE ALSO

virt-win-reg (1), **Win::Hivex::Regedit** (3), **Win::Hivex** (3), **hivexsh** (1), **dos2unix** (1), **unix2dos** (1), **iconv** (1), <http://libguestfs.org/>.

AUTHOR

Richard W.M. Jones <http://people.redhat.com/~rjones/>

COPYRIGHT