master Go to file Code

79

- EseDataAccess
- VssCopy
- ditsnap_exe
- images
- .gitignore
- LISENCE.md
- README.md

About

An inspection tool for Active Directory database

Readme

Releases 2

ditsnap.exe 1.... Latest
on 26 Sep 2016

+ 1 release

ditsnap.sln

README.md

DIT Snapshot Viewer

DIT Snapshot Viewer is an inspection tool for Active Directory database, ntds.dit. This tool connects to ESE (Extensible Storage Engine) and reads tables/records including hidden objects by low level C API.

The tool can extract ntds.dit file without stopping lsass.exe. When Active Directory Service is running, lsass.exe locks the file and does not allow to access to it. The snapshot wizard copies ntds.dit using VSS (Volume Shadow Copy Service) even if the file is exclusively locked. As copying ntds.dit may cause data inconsistency in ESE DB, the wizard automatically runs **esentutil /repair** command to fix the inconsistency.

The executable is available here. Download ditsnap.exe

Screenshots

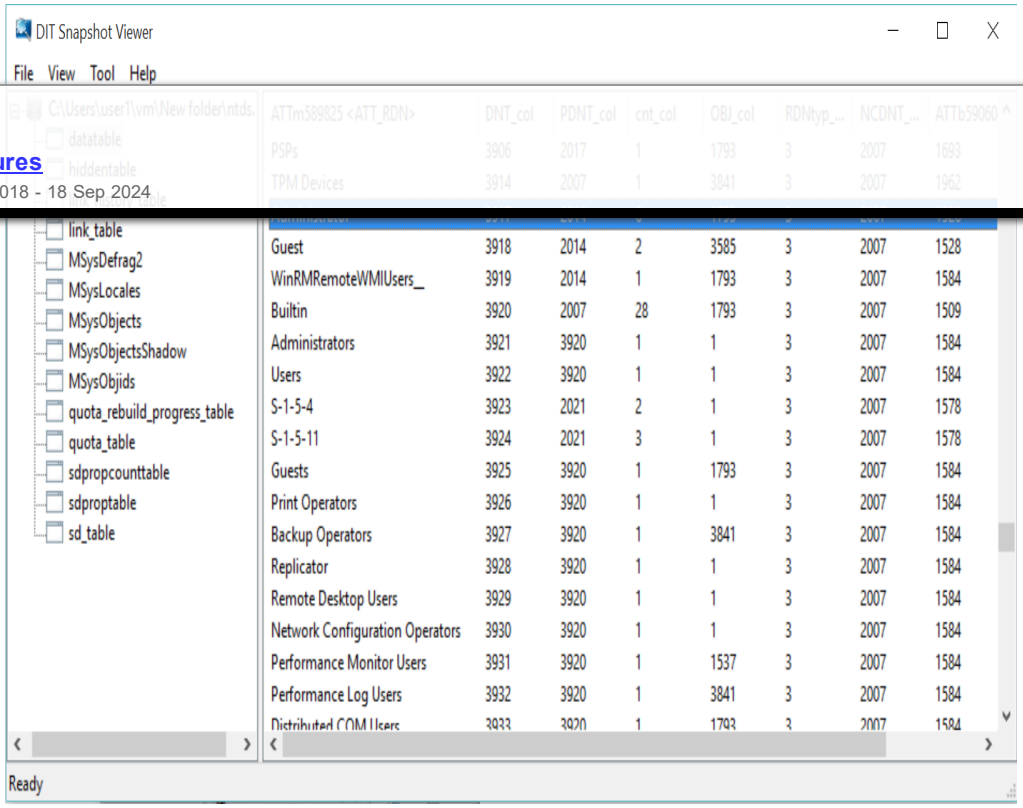
Main Window

Packages

No packages published

Languages

- C 47.4%
- C++ 38.9%
- Objective-C 13.7%



Detail Dialog

Interpreted Value

Interpreted Value column in Detail Dialog shows human-readable representations of raw ESE column values. Here are the exmamples.

OBJECT_CATEGORY

The attribute is stored as a 32-bit integer in ESE, which points to DNT (Distinguished Name Tag) of another Active Directory object. Interpreted Value for the attribute shows RDN (Relative Distinguished Name) of the object.

OBJECT_CLASS

The attribute is stored as a multi-valued 32-bit integer column in ESE, which points to GOVERNS_ID of other objects. Interpreted Value for the attribute shows RDNs of the objects.

PWD_LAST_SET, LAST_LOGON, LAST_LOGOFF, ACCOUNT_EXPIRES

Those attributes are stored as 64-bit integers in ESE, which are treated as FILETIME in Active Directory. Interpreted Value column for the attributes shows it as a date format.

WHEN_CREATED, WHEN_CHANGED

Those attributes are stored as 64-bit integers in ESE, which are treated as shortened FILETIME (1/10000000 of the integer representation of FILETIME). Interpreted Value for those attributes shows it as a date format.

USER_ACCOUNT_CONTROL

The attribute is stored as a 32-bit integer in ESE, which are treated as flags that control the behavior of the user account. Interpreted Value for the attribute shows the list of flags. See https://msdn.microsoft.com/en-us/library/ms680832(v=vs.85).aspx.

EseDataAccess static library

EseDataAccess static library can be used for other ESE inspection applications. EseDataAccess.h contains C++ object-oriented representation of ESE C API. For example, ESE table is represented by EseTable class defined as below.

```
class EseTable
{
        public:
                EseTable(const EseDatabase* const eseDatabase
                ~EseTable();
                void MoveFirstRecord() const;
                bool MoveNextRecord() const;
                void Move(uint rowIndex) const;
                int CountColumnValue(uint columnIndex) const;
                wstring RetrieveColumnDataAsString(uint colum
                uint GetColumnCount() const;
                wstring GetColumnName(uint columnIndex) const
}
```