Vera Crypt

Backup VeraCrypt using Urbackup.

VC container file incremental backup

In result this is not incremental backup. Every backup is a full backup, but only changes are transferred.

Setup

Example client setup:

- Windows Client
- Dedicated NTFS partition (32GB)
- VC container file on dedicated NTFS partition (10GB file)
    - encrypted empty space looks like data, so empty VC container is using 10GB of data on 32GB disc.

Urbackup client:

- set to image backup of whole NTFS drive (partition).

Urbackup server:

- Backup storagae on BTRS file system
- Image backup storage set to `Raw copy-on-write file" (COW)`

Results

- Urbackup clients can handle NTFS file system during image backup so **only used area is backed up**
    - for first backup (full backup), 10GB was transferred.
- Urbackup server tracks hashes of block on disc to detect only changed blocks so **only changed blocks are transferred**
- Urbackup server creates 32GB .raw file for each image backup. This file can be mount as normal disc using `loop device`.
    - Urbackup server is using sparse files, so only 10GB of filesystem is used for 32GB image file.
- Urbackup server is using BTRFS CoW (Copy-on-Write) filesystem with all its benefits, so:
    - every next backup is a reflink-copy of previous one (it points to the same data), and only changed blocks are modified
        - so with our example setup next backup create new directory with 32GB .raw file, but it only takes few MB more data on BTRS.
    - There is **no real incremential backups chain**. There is no risk of loosing one element from chain. Every backup looks like full backup - 32GB .raw file with full disc image is

present. **No need to refresh `full` backup** every n-th backup. It is possible too keep unfinished number of incremental backups without risk.

From:
https://niziak.spox.org/wiki/ - **niziak.spox.org**

Permanent link:
https://niziak.spox.org/wiki/sw:urbackup:vera_crypt

Last update: **2023/06/19 16:25**