cesnet

(NE)ZÁLOHUJTE

Radomír Orkáč
CESNET

únor 2023
Praha

Volné pokračování mojí prezentace
S teroristy se (ne)vyjednává.

(Ne)zálohujte

- *Existují pouze dva druhy dat:*
  - zálohovaná data,
  - ztracená data.
- Je ztráta dat předvídatelná?
  - *Garmin zaplatil výpalné 10 milionů dolarů.*
  - *Zálohy selhaly, data jsou nedostupná. ŘSD se po útoku hackerů vrátilo k papíru.*

(Ne)zálohujte

- Požár v OVHcloud, 10.3. 2021
  - Někteří neměli zálohy geograficky oddělené, nebo zálohovali jen do vedlejší budovy.
  - OVH doporučilo zákazníkům aktivovat plán pro obnovu při katastrofě.
  - Podle autorů Rustu se potvrdilo, že se data nepovede nahradit ani obnovit.

Zdroj: https://twitter.com/momotchiii

(Ne)zálohujte

- GitLab v roce 2017 omylem smazal data.
  - Obnova ukázala nefunkční zálohování.
  - Všechny zálohovací techniky selhaly.
  - Nefungovalo správně:
    - snímky LVM,
    - běžné zálohy dat,
    - zálohování databáze PostgreSQL,
    - zálohování do cloudu Amazon S3.
  - GitLab nakonec obnovil data ze šest hodin staré repliky.

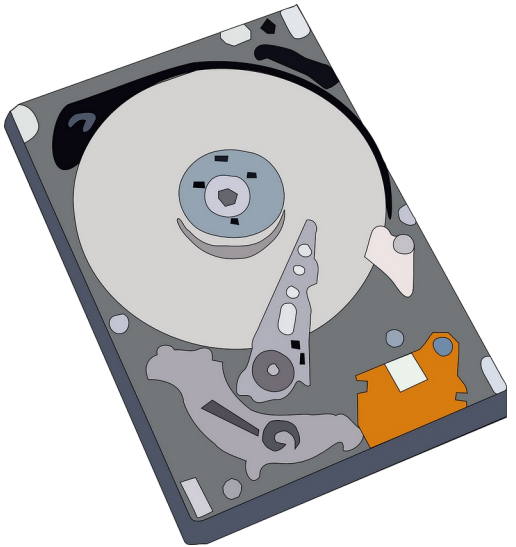
(Ne)zálohujte

```
How to Restore Your Files

--------------------------------------------------------------------------------

Security Alert!!!
We hacked your company successfully
All files have been stolen and encrypted by us
If you want to restore files or avoid file leaks, p
If money is received, encryption key will be availa

--------------------------------------------------

Attention!!!
Send money within 3 days, otherwise we will expose
Don't try to decrypt important files, it may damage
Don't trust who can decrypt, they are liars, no one
If you don't send bitcoins, we will notify your cus
And sell your data to your opponents or criminals,

--------------------------------------------------
```

```
/vmfs/volumes/5377c2eb-0e7328c3-eb77-0025904410ae/ispadmin # ls -al
total 5480464
drwxr-xr-x    1 root     root          2240 Feb  3 16:47 .
drwxr-xr-t    1 root     root          3360 Jan 12  2017 ..
-rw-------    1 root     root    1075045302 Feb  3 16:47 ispadmin-341690c9.vmss
-rw-r--r--    1 root     root            15 Feb  3 16:46 ispadmin-341690c9.vmss.args
-rw-------    1 root     root    17179869696 Feb  3 16:47 ispadmin-flat.vmdk
-rw-r--r--    1 root     root            16 Feb  3 16:46 ispadmin-flat.vmdk.args
-rw-------    1 root     root          9196 Feb  3 16:46 ispadmin.nvram
-rw-r--r--    1 root     root            12 Feb  3 16:46 ispadmin.nvram.args
-rw-------    1 root     root          1007 Feb  3 16:46 ispadmin.vmdk
-rw-r--r--    1 root     root             9 Feb  3 16:46 ispadmin.vmdk.args
-rw-r--r--    1 root     root           512 Feb  3 16:46 ispadmin.vmsd
-rw-r--r--    1 root     root             9 Feb  3 16:46 ispadmin.vmsd.args
-rwxr-xr-x    1 root     root          3387 Feb  3 16:46 ispadmin.vmx
-rw-r--r--    1 root     root             9 Feb  3 16:46 ispadmin.vmx.args
-rw-r--r--    1 root     root           775 Feb  3 16:46 ispadmin.vmxf
-rw-r--r--    1 root     root             9 Feb  3 16:46 ispadmin.vmxf.args
```

Zálohování – jaké otázky si klást?

- Jak často a co (ne)zálohovat?
- Jak dlouho zálohy „držet“?
- Jsou zálohy „zabezpečené“?
- Jak rychle data obnovíme?
  - Částečná nebo úplná ztráta dat.
- Odolnost vůči selhání technologie?
- Monitoring zálohování…



Strategie zálohování 3-2-1

- Fotograf Peter Krogh tento koncept původně sdílel ve své knize The DAM Book: Digital Asset Management for Photographers z roku 2009.
- Název je odvozen od principu, na němž je zálohování postaveno:
  - Tři kopie produkčních dat (**3**),
  - dvě kopie budou místní, ale na rozdílných/nezávislých zařízeních (**2**),
  - jedna kopie v jiné lokalitě (**1**).
- Od roku 2012 je strategie zálohování 3-2-1 doporučována a používána vládou Spojených států;-)

Data Backup Options

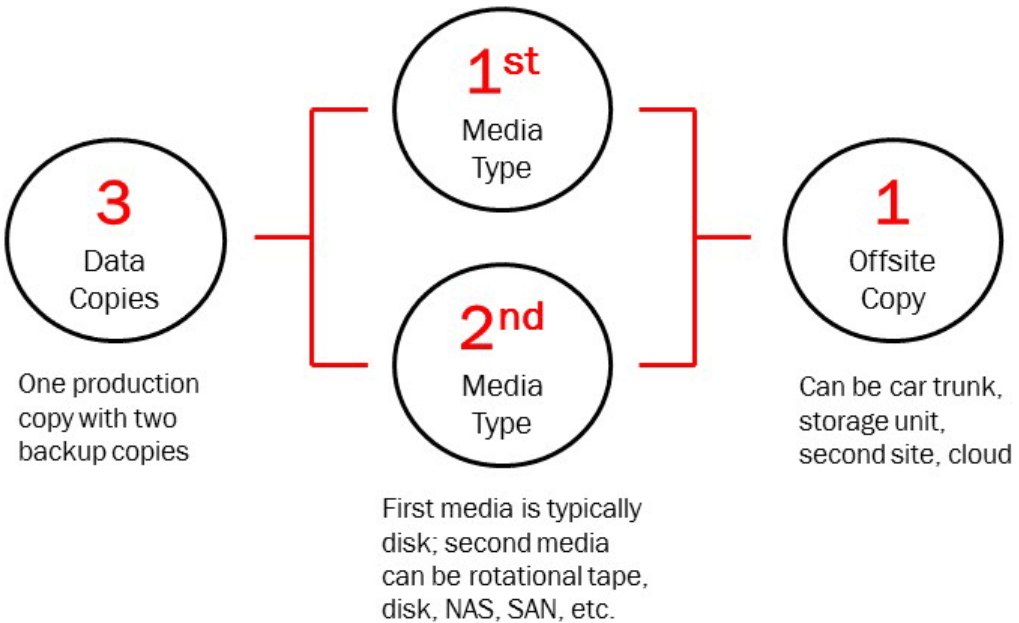
Original release date: October 24, 2012 | Last revised: February 06, 2013

All computer users, from home users to professional information security officers, should back up the critical data they have on their desktops, laptops, servers, and even mobile devices to protect it from loss or corruption. Saving just one backup file may not be enough to safeguard your information. This paper summarizes the pros, cons, and security considerations of backup options for critical personal and business data.

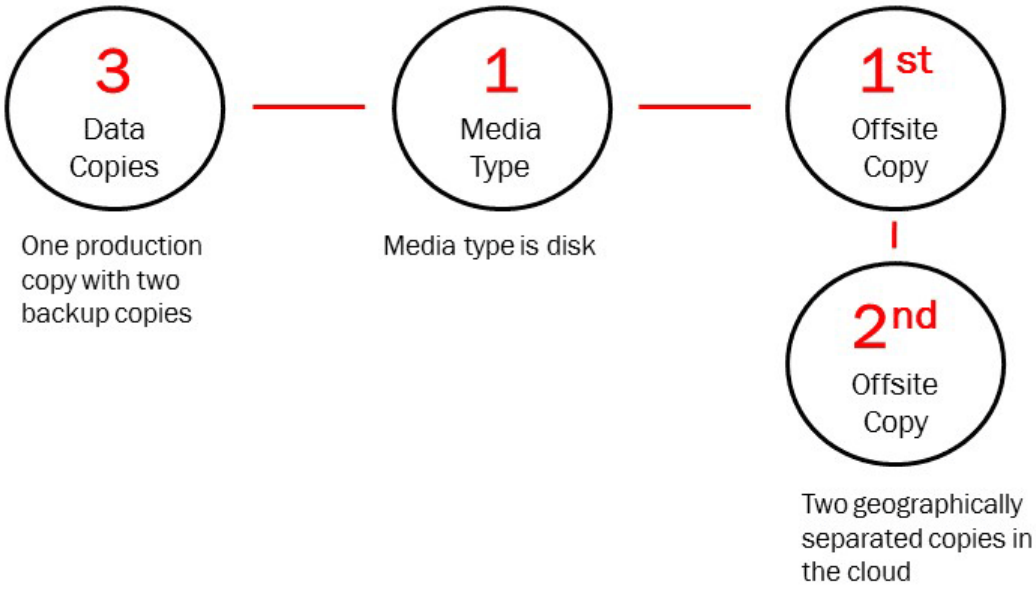
View Publication

data_backup_options.pdf

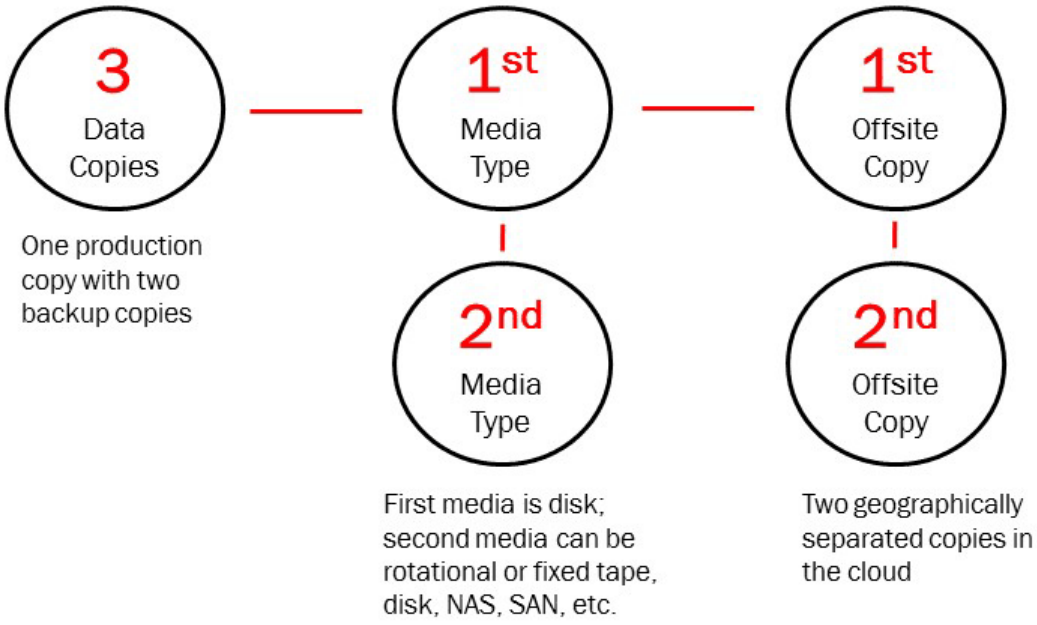
Strategie zálohování 3-2-1



Strategie zálohování 3-2-1



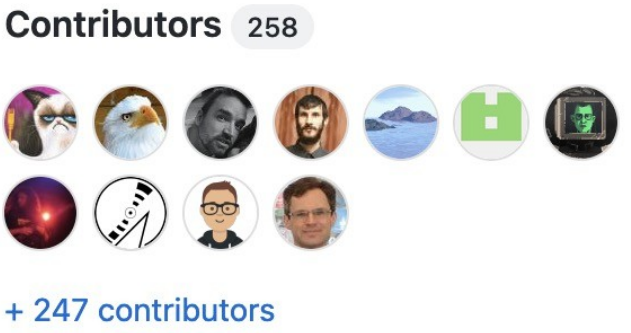
Strategie zálohování 3-2-2



cesnet

Borg

- BorgBackup (zkráceně „Borg“):
  - podporováno velkou a aktivní open source komunitou,
  - GNU/Linux, macOS, BSD, Linux Subsystem of Windows 10 (experimental)
  - prostorově úsporné úložiště záloh,
  - bezpečné, ověřené šifrování,
  - komprese (LZ4, zlib, LZMA, zstd),
  - zálohy připojitelné přes FUSE.



cesnet

Borg

Distribution	Source	Command
Alpine Linux	Alpine repository	`apk add borgbackup`
Arch Linux	[community]	`pacman -S borg`
Debian	Debian packages	`apt install borgbackup`
Gentoo	ebuild	`emerge borgbackup`
GNU Guix	GNU Guix	`guix package --install borg`
Fedora/RHEL	Fedora official repository	`dnf install borgbackup`
FreeBSD	FreeBSD ports	`cd /usr/ports/archivers/py-borgbackup && make install`
macOS	Homebrew	`brew install borgbackup` (official formula, **no** FUSE support) **or** `brew install --cask macfuse` (private Tap, FUSE support) `brew install borgbackup/tap/borgbackup-fuse`

Debian 9	1.0.9
Debian 9 Backports	1.1.9
Debian 10	1.1.9
Debian 10 Backports	1.1.15
Debian 11	1.1.16
Debian 11 Backports	1.2.3
Debian 12	1.2.3
Debian Unstable	1.2.3
Deepin	1.1.9
Devuan 2.0	1.0.9
Devuan 3.0	1.1.9
Devuan 4.0	1.1.16
Devuan Unstable	1.2.3
Entware	1.2.2
EPEL 7	1.1.18
EPEL 8	1.1.17
EPEL 9	1.2.3

cesnet

Borg

- Základní použití:
  1) *# borg init --encryption=repokey ~/Backup/Obsidian*
  2) *# export HISTFILE=/dev/null ; export BORG_PASSPHRASE='password'*
  3) *# borg key export ~/Backup/Obsidian ~/obsidian_backupkey.txt*
  4) *# borg create ~/Backup/Obsidian::Archiv1 ~/Obsidian*
  5) *# borg create --stats ~/Backup/Obsidian::Obsidian-{now:%Y%m%d} ~/Obsidian*
  6) *# borg list ~/Backup/Obsidian*
  7) *# borg list ~/Backup/Obsidian::Archiv1*
  8) *# borg extract ~/Backup/Obsidian::Archiv1*
  9) *# borg mount ~/Backup/Obsidian::Archiv1 /mnt/Obsidian-Archiv1/*

cesnet

Borg

- **Ukázka č. 1:** Statistika vytvářené zálohy (parametr *--stats*).

```
Time (start): Thu, 2023-01-19 01:00:18
Time (end): Thu, 2023-01-19 03:43:02
Duration: 2 hours 42 minutes 43.39 seconds
Number of files: 20857190
Utilization of maximum supported archive size: 6%
------------------------------------------------------------------------------
                       Original size      Compressed size Deduplicated size
This archive:                1.72 TB             1.42 TB 2.15 GB
All archives:               29.06 TB            24.04 TB 1.21 TB

                       Unique chunks         Total chunks
Chunk index:                22773511            358934666
```

cesnet

Borg

- **Ukázka č. 2:** Podrobnosti o repozitáři a výpis souborů z archivu.

```
$ borg list ~/Backup/Obsidian
Archiv1                              Sun, 2023-01-29 18:58:48
Archiv2                              Sun, 2023-01-29 19:02:19
Obsidian-202301291902                Sun, 2023-01-29 19:02:46

$ borg list ~/Backup/Obsidian::Archiv1
-rw-r--r-- user1  staff      6148 Sat, 2023-01-28 10:00:35 Obsidian/Skripty/.DS_Store
-rwxrwxr-x user1  staff       204 Sat, 2023-01-28 09:06:20 Obsidian/Skripty/screen.ps1
-rwxrwxr-x user1  staff        75 Sat, 2023-01-28 09:24:50 Obsidian/Skripty/screen.bat
-rwxrwxr-x user1  staff       355 Sat, 2023-01-28 09:10:13 Obsidian/Skripty/rclone.bat
-rwxrwxr-x user1  staff        68 Sat, 2023-01-28 09:42:21 Obsidian/Skripty/screen.txt
```

cesnet

Borg

- Vzdálený repozitář
  - Přenesení souborů do jiné lokality.
  - Vzdálený souborový systém připojený lokálně.
  - Zálohování proti serverové instanci Borgu.
- Čištění (smazání) repozitáře (archivu)
  - *# borg prune --keep-daily=7 --keep-weekly=4 --keep-monthly=6 ~/Backup/Obsidian*
  - *# borg delete ~/Backup/Obsidian::Archiv1*
- Uvolnění dat (od verze 1.2)
  - *# borg compact ~/Backup/Obsidian*

cesnet

RCLONE

- Označován za *„Švýcarský armádní nůž cloudového úložiště“* a *„Technologii k nerozeznání od magie“*.
- Robustní nástroj pro příkazový řádek k synchronizaci a přenosu souborů z/do cloudového úložiště.
- Připojení místních, cloudových nebo virtuálních souborových systému jako disk.

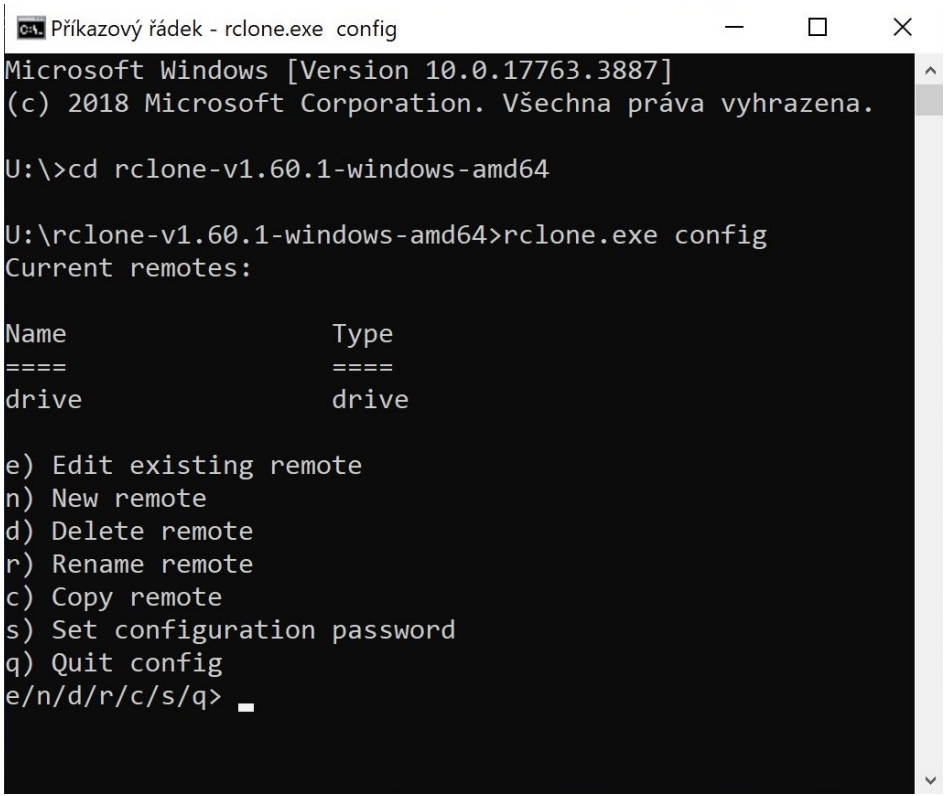
cesnet

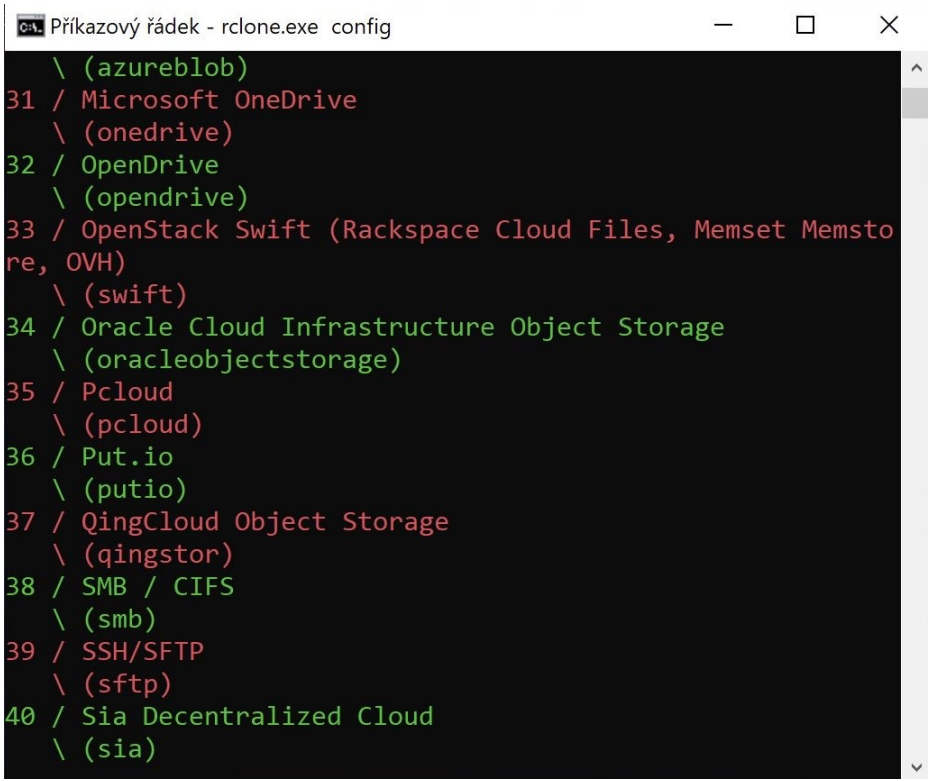
RCLONE

- Konfigurace úložiště:
  - *rclone.exe config*
    - ~/.config/rclone/rclone.conf
    - C:\Users\..\AppData\Roaming\rclone\rclone.conf
- Kopírování dat:
  - *rclone.exe copy -P v:\tiskarny drive:/tiskarny*
- Jednosměrná synchronizace dat:
  - *rclone.exe sync -P --exclude=*.lnk v:\ drive:/v/*

cesnet

RCLONE





cesnet

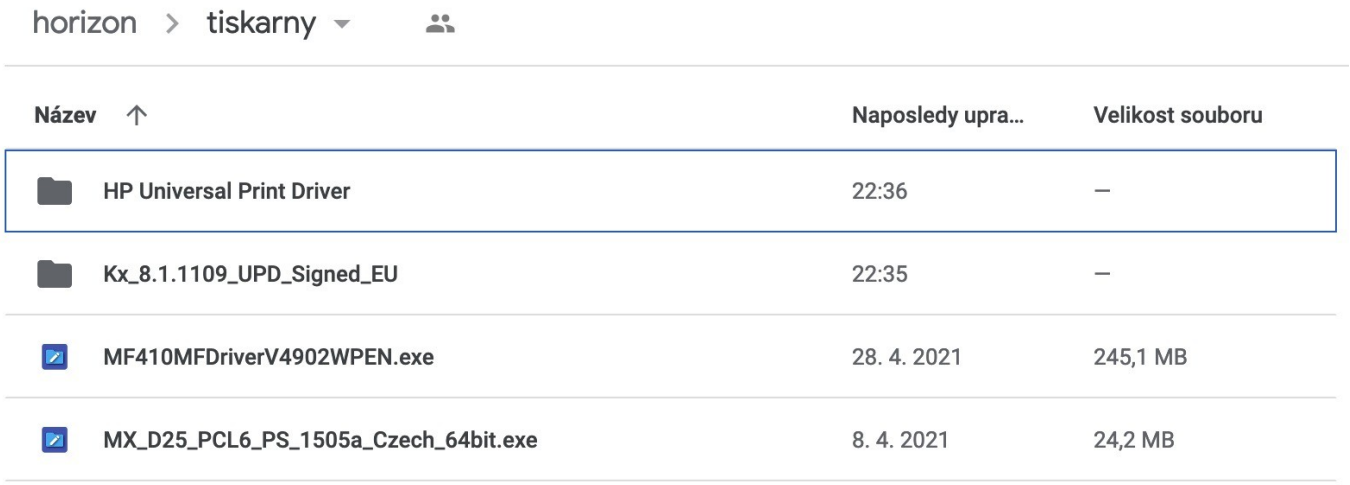
RCLONE

```
Choose a number from below, or type in your own value.
 1 / Full access all files, excluding Application Data Folder.
   \ "drive"
 2 / Read-only access to file metadata and file contents.
   \ "drive.readonly"
   / Access to files created by rclone only.
 3 | These are visible in the drive website.
   | File authorization is revoked when the user deauthorizes the app.
   \ "drive.file"
   / Allows read and write access to the Application Data folder.
 4 | This is not visible in the drive website.
   \ "drive.appfolder"
   / Allows read-only access to file metadata but
 5 | does not allow any access to read or download file content.
   \ "drive.metadata.readonly"
```

cesnet

RCLONE

```
Transferring:
 * Kx_8.1.1109_UPD_Signed…up/EULA/License_PT.rtf:100% /59.467Ki, 59.454Ki/s, 0s
 * Kx_8.1.1109_UPD_Signed…up/EULA/License_RU.rtf:100% /79.482Ki, 0/s, -
 * Kx_8.1.1109_UPD_Signed…p/EULA/License_SCH.rtf:100% /77.827Ki, 0/s, -
 * Kx_8.1.1109_UPD_Signed…p/EULA/License_TCH.rtf:  0% /86.903Ki, 0/s, -
```



Data v cloudu

Pozastavení nebo ukončení vašeho přístupu ke službám Google

Google si vyhrazuje právo pozastavit nebo ukončit váš přístup ke službám nebo smazat váš účet Google, pokud nastane některá z těchto okolností:

- závažně nebo opakovaně porušíte tyto podmínky, další podmínky konkrétní služby nebo zásady
- jsme povinni tak učinit na základě právních požadavků nebo soudního příkazu
- jsme důvodně přesvědčeni, že vaše chování způsobuje uživateli, třetí straně nebo společnosti Google škodu či odpovědnost – např. když se dopouštíte hackingu, phishingu, obtěžování, spamování, podvodů nebo zcizování obsahu, který vám nepatří

Data v cloudu

Stažení dat z deaktivovaného účtu

I když se do účtu nemůžete dostat, možná si budete moci stáhnout a uložit data z některých služeb Google.

Pokud chcete zkusit svá data stáhnout, přihlaste se k účtu jako obvykle. Pak možná budete mít možnost svá data stáhnout.

Účty mohou být zablokovány bez možnosti stáhnout si data. Týká se to mimo jiné následujících případů porušení zásad:

- platné právní žádosti,
- odcizení účtu,
- hrubé porušení pravidel pro obsah, včetně sexuálního zneužívání dětí, využívání nebo teroristického obsahu.

Dad took photos of naked toddler son to send to doctor, Google flagged him as a criminal

A father said that Google locked him out of all his accounts as he took images of his sick son's genitals to send to a doctor amid the pandemic.

TN Viral Desk | Updated Aug 23, 2022 | 12:39 PM IST

Dad took photos of naked son to send to doctor, Google flagged him as a criminal

Photo : iStock

UP NEXT

1 Dad took photos of naked toddler son to send to doctor, Google flagged him as a...

2 Optical illusion: Tricky visual challenges people to find panda among pills in 15...

3 Watch: Firefighters battle

Data v cloudu

Bezpečnost Disku Google <drivesafety-noreply@google.com> 26. ledna 2023 v 22:47
Odpovědět-komu: drivesafety-noreply@google.com
Komu: radomir@orkac.cz

Google

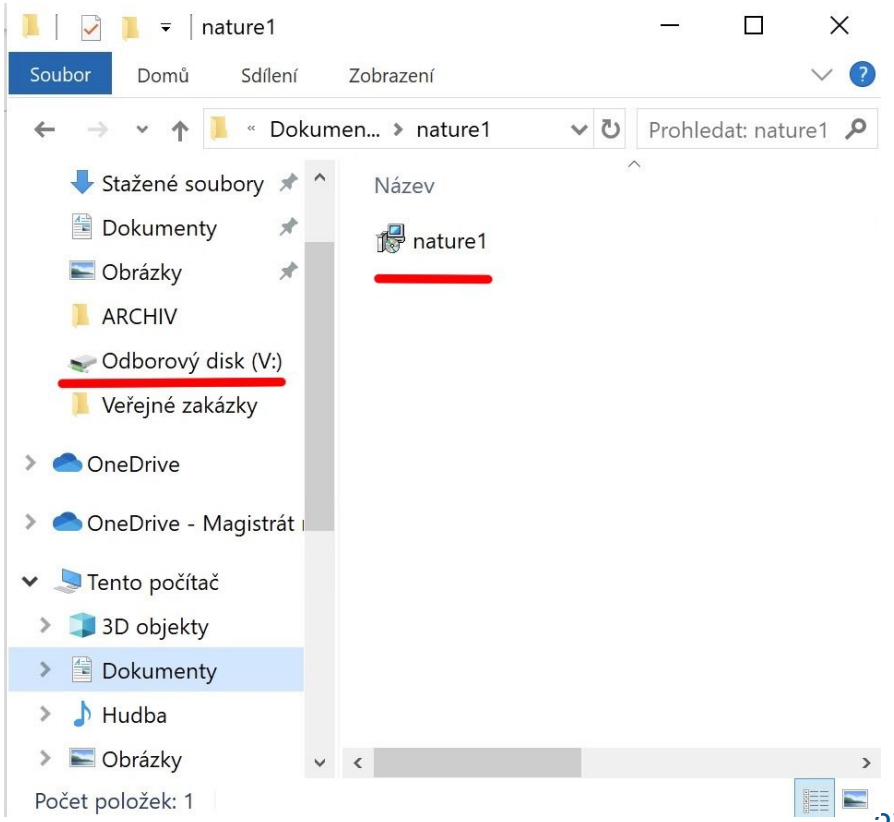
Váš soubor možná porušuje smluvní podmínky Disku Google

„nature1.zip“ zahrnuje obsah, který možná porušuje Zásady týkající se malwaru a podobného škodlivého obsahu Disku Google. Některé funkce spojené s tímto souborem mohly být omezeny. Pokud se domníváte, že se jedná o chybu, a chcete, aby tým pro důvěryhodnost a zabezpečení tento soubor zkontroloval, požádejte níže o kontrolu.

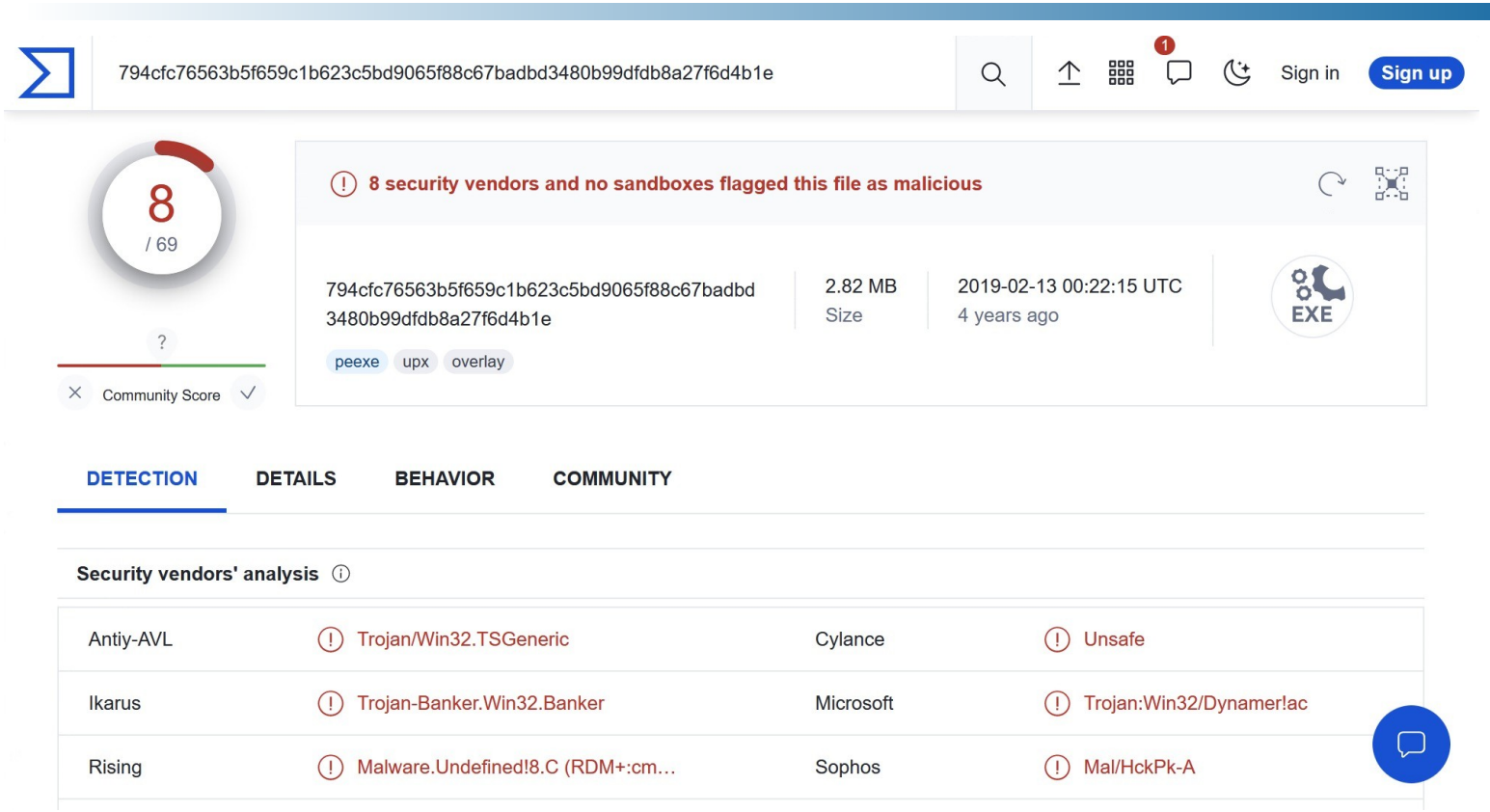
Omezený soubor

nature1.zip

Požádat o kontrolu



Data v cloudu

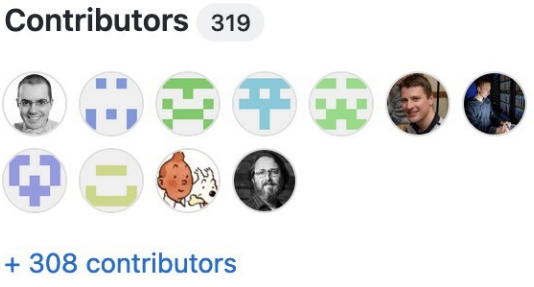


cesnet

Restic

- Restic je zálohovací program pro GNU/Linux, macOS, Windows…
- Šifrovanou zálohu odesílá na vzdálené úložiště pomocí RCLONE.
- Ve Windows podpora vytváření záloh pomocí stínové kopie (VSS) *--use-fs-snapshot*

 # restic --repo /backup/debian.restic init
 # restic -r rclone:gdrive:debian.restic init



cesnet

Restic

```
export HISTFILE=/dev/null
export RESTIC_REPOSITORY="rclone:gdrive:debian.restic"
export RESTIC_PASSWORD=HESLO

restic init
restic backup
restic snapshots
restic restore latest -target /data-obnova/
restic forget --keep-daily 7 --keep-weekly 5 --keep-monthly 12 --keep-yearly 1 --prune
restic prune

root@debian:~# restic snapshots
repository 67d3ae8d opened successfully, password is correct
ID        Time                 Host        Tags        Paths
----------------------------------------------------------------------
0d70e6de  2021-12-31 00:26:03  debian     data        /data
...
62cfa8d9  2022-03-31 01:10:25  debian      data        /data
...
29a71c1f  2023-02-05 01:52:12  debian      data        /data
----------------------------------------------------------------------
111 snapshots
```

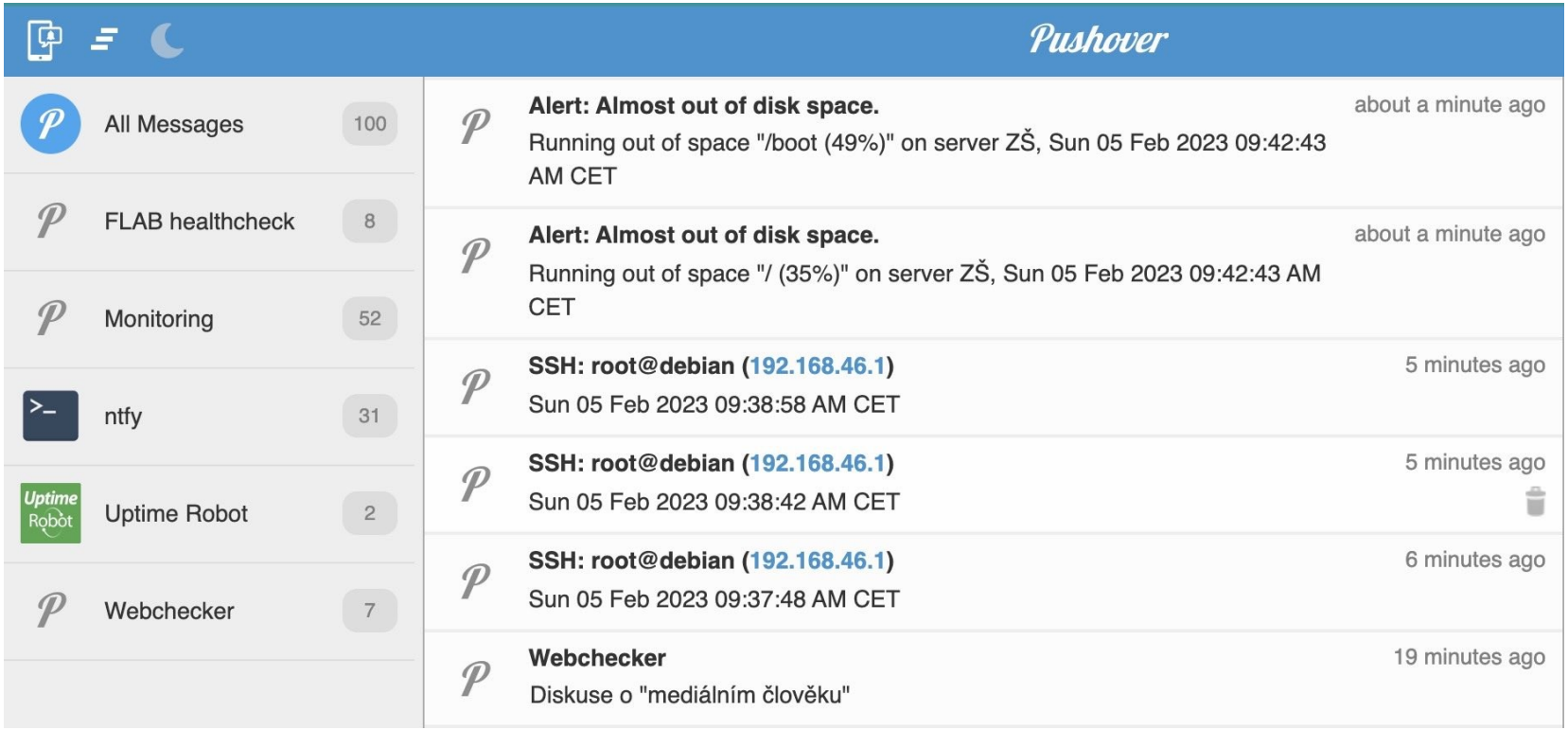
Monitoring – Healthchecks.io

bakalari | diskspace | rclone | restic | zš | úřad

Filter by check name...

	Name	Ping URL uuid slug	Integrations	Period Grace	Last Ping Last Duration
✓	ZŠ: Win SQLDATA d: (restic) restic	https://healthchecks[redacted]/ping/8cd2575d-cd86-4517-		1 day 2 days	před 11 hodinami ⏱ 24 min 56 sec
✓	ZŠ: Bakaláři (restic) restic bakalari	https://healthchecks[redacted]/ping/fecf47f6-		1 day 1 day	před 11 hodinami ⏱ 21 min 41 sec
✓	Odborový disk: Rclone úřad rclone	https://healthchecks[redacted]/ping/9f911d6d-54b9-4cbd-aae0-		1 day 1 day	před 29 minutami ⏱ 13 min 40 sec
✓	Odborový disk: Restic úřad restic	https://healthchecks[redacted]/ping/f8a019c0-cc54-40a8-		1 day 1 day	před 4 sekundami
🔔	ZŠ: Srvdata (diskspace) zš diskspace	https://healthchecks[redacted]/ping/40fd7af6-344b-43a1-		1 day 1 hour	před 8 minutami

Notifikace – Pushover.net



cesnet

Děkuji za pozornost.

```
$ rclone sync -P gdrive:bakalari/ pcloud:bakalari/
Transferred:          11.141 MiB / 1.324 TiB, 0%, 550.263 KiB/s, ETA 4w1d21h36m
Transferred:            0 / 59, 0%
Elapsed time:        22.5s
Transferring:
 *                20210829_rucni_bakalari_v.7z:  0% /2.853Gi, 140.135Ki/s, 5h55m30s
 *                20210829_rucni_bakalari_c.7z:  0% /2.664Gi, 132.987Ki/s, 5h49m46s
 *                   bakalari_202108290921.box:  0% /24.678Gi, 200.030Ki/s, 35h55m42s
 *                   bakalari_202110231340.box:  0% /27.610Gi, 92.734Ki/s, 86h42m48s
```