GBS Backup

Backup & Deployment

Factsheet

Windows and MacOS backup

Introduction

The Generic Backup Solution (GBS) offers a Linux based Backup Server that can back up MacOS and Windows (Server) clients.
For Windows backup purpose, GBS includes three mechanisms, dedicated for Windows Server and MacOS/Windows respectively.
This factsheet will discuss the options for implementing a Windows/MacOS backup server.

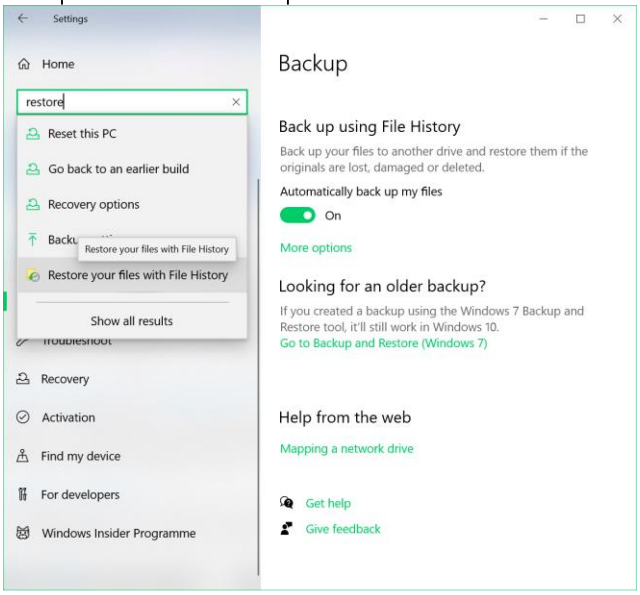
Option 1:
SAMBA destination for backup of Windows and MacOs

For the backup of Windows PC's and MacOS Laptops, the GBS solution includes a SAMBA based backup mechanism. This mechanism is targeted for PC's that are not online 24x7.
As the PC will be online at irregular times, it cannot be included in a regular backup schedule.
Therefore, we let the user determine the backup schedule and the setup of the PC backup application.
The PC backup application will write backups to a SAMBA network share that resides on the GBS backup server. The user is free to select any backup application, but we suggest the following alternatives:

product	Windows	MacOS	free	encryption	Disaster recovery
Windows Backup File History	√		√		
Mac TimeMachine		√	√		
Acronis TrueImage	√	√		√	√
Duplicati 2.0	√	√	√	√	

Some of the mentioned alternatives have the possibility to encrypt the backup data. This will protect the users data from intrusion.
We strongly advise to write encrypted backups if the privacy of the data is a concern.
The backup contents on the SAMBA share are part of the Stage 1 (overnight) backup repository on the backup server.
This SAMBA share is considered vulnerable to cyber/ransom attack, as it is accessible from the user's PC.
Therefore, the GBS solution includes a stage2 "permanent backup vault", which makes a protected copy of the Stage 1 backup.

Example for Windows Backup:



Backup

Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged or deleted.

Automatically back up my files

On

More options

Looking for an older backup?

If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.

Go to Backup and Restore (Windows 7)

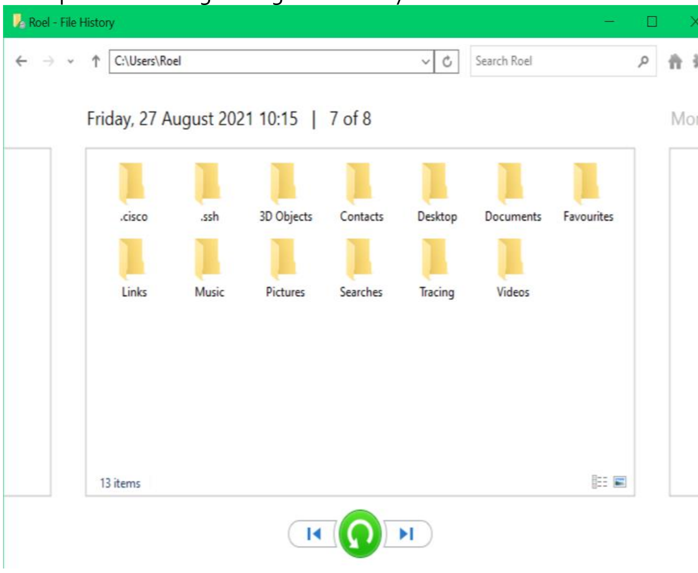
Help from the web

Mapping a network drive

Get help

Give feedback

Example of Browsing through file history:



Roel - File History

C:\Users\Roel

Search Roel

Friday, 27 August 2021 10:15 | 7 of 8

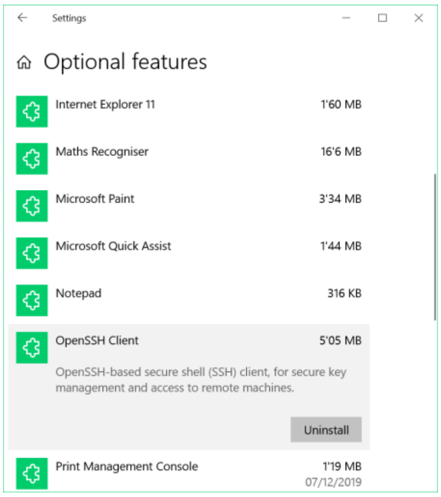
13 items

Option 2:
SYSTEM backup for Windows

For business-critical systems (Windows Server), GBS includes an alternative backup pull mechanism, based on RSYNC and SSH.
This mechanism offers a full system backup to a centralized Linux backup server.

- Regular system backup via RSYNC to the GBS server on Linux.
- Uses RSYNC on the PC (OpenSource BackupPC).
- Pull mechanism triggers the backup (Start RSYNC) on Windows via SSH.
- OpenSSH is supported in the latest windows release, see screenshot ->
- Windows file permissions included, restored with icacls tooling

Install SSH on windows "Apps and features":



Optional features

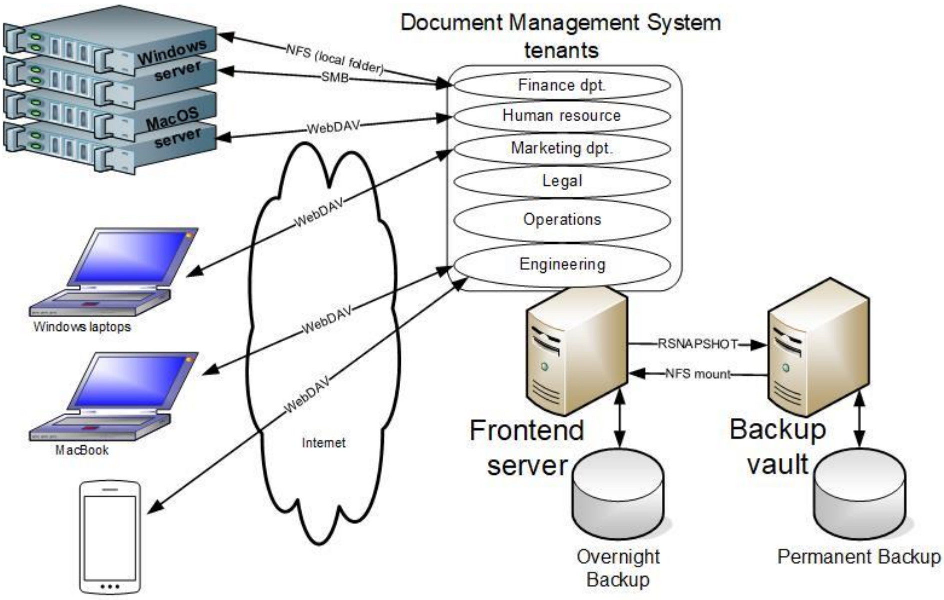
Internet Explorer 11	1'60 MB
Maths Recogniser	16'6 MB
Microsoft Paint	3'34 MB
Microsoft Quick Assist	1'44 MB
Notepad	316 KB
OpenSSH Client OpenSSH-based secure shell (SSH) client, for secure key management and access to remote machines.	5'05 MB
Print Management Console	1'19 MB 07/12/2019

The problem:

The problem with all the above-mentioned backup mechanism's is that they are not managed centrally but need to be installed on the user's computer. These mechanisms depend on the discipline of the individual end-user to schedule and maintain its backup scheme. Typically, this results in an unreliable backup.
Therefore, we suggested a Document Management System (DMS) as a backup frontend for Windows/macOS users.
In case the user's laptop gets stolen or damaged, it can be replaced or reinstalled while the documentation is safely stored in the DMS.

Option 3 (preferred):
Document Management System as a frontend for Windows and MacOS users.

DMS is a higher level and structured approach to the windows/MacOS backup challenge in a bigger organization.
The DMS will facilitate and manage user administration, document collection, versioning, file permission and employee collaboration.
Backup of Windows/MacOS PC's is left to the customer, as these usually can be redeployed from a default image/template.
Instead the DMS backup option focuses on the document management and backup of the documentation content.
GBS will function as a backend (backup vault) to safeguard the DMS from cyber/ransom attack or accidental operating failures.
GBS can interact with a variety of DMS systems (e.g. see https://sourceforge.net/software/product/PinPoint-DMS/alternatives).
GBS partners with DMS vendors to provide a cost effective DMS solution for its customers.



Stage 2 Permanent backup as Backup Vault

As the Overnight first stage (SAMBA or DMS) backup may be vulnerable to cyber/ransom attack, a second stage backup can be deployed to serve as a backup vault to protect the backups from user modification.
The backup vault is deployed as an autonomous system with no remote access to assure the backup integrity.
The backup vault is configured to copy the overnight backups on a regular basis to the permanent backup.
This permanent backup will contain: 7 daily backups per week, 4 weekly backups per month, 3-12 monthly backups per year.
Therefore, if the user is caught by ransom attack (which may include the stage 1 backup), an older unaffected backup can be retrieved from the Permanent backup server.

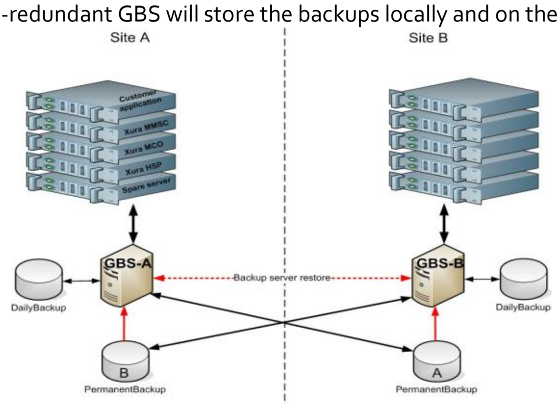
VDO data deduplication and compression

GBS deployment makes use of deduplication mechanisms:

- Rsnapshot for the permanent backup uses "hardlink" deduplication,
  it only copies a file if the content has changed since the previous day.
  If a file did not change, only a hardlink is created to the previous day/file.
  Typically, the permanent backup contains 20 backups, requiring only 2,5 times the original size.
- VDO is used to reduce backup storage requirements even further.
  The backup repository will contain multiple copies of the same file, as OS system files generally are identical on multiple backup clients. VDO is able to detect identical blocks on disk, and store identical blocks only once.
  As a result, we have seen storage savings of 80% at the Centralized backup server.
  This compares to storing 10TB data on a 2TB disk.

Geographic Redundancy

A geographic redundant backup server can be offered as an additional option in GBS, if the customer has two or more sites
Permanent backups are stored on a remote backup server in order to provide geo-redundancy.
The geo-redundant GBS will store the backups locally and on the remote site:



Geo redundancy includes the following features:

- Site A Permanent backup data is stored at site B
- Site B Permanent backup data is stored at site A
- GBS server can be restored from remote backup server.
- The whole site can be restored from remote backup.
- Disaster recovery fully supported from remote backup.

The remote storage ("Permanent backup") will be mounted on the GBS server via NFSv4 (Network File System).
Precondition for a working geo-redundancy is a good network connection between the sites.

3rd Party (Tape) backup options (Bacula or EMC Networker)

Disk/Tape backup is an option for the Hybrid Backup server, offering an extra level of availability to the permanent disk backup.
For tape backup GBS offers Bacula (open source) or EMC networker (licensed) as an option.
Bacula is the preferred solution, as it reduces the OPEX required for EMC Networker licensing.
Bacula can also be used to create an offsite backup destination (remote Bacula Storage Daemon)
GBS can interface with any suggested 3rd party backup application, that performs the role of stage 2 backup mechanism.

Deployment options virtualized or hardware based.

The GBS backup server can be deployed as a virtualized backup server on any infrastructure, requiring RHEL8, RHEL9 or AlmaLinux, or as a hardware based dedicated "Hybrid Backup Server".

The Hybrid Backup Server is usually deployed on a HP DL380 or DELL PowerEdge R740 server in the same rack as the enterprise solution that it needs to back up. However, it is suggested that the backup server is allocated in a different rack, or even in a different server room.

The backup server can backup equipment on multiple independent IP subnets, as long as there is a direct IP cable to the switch in that subnet. The Hybrid Backup Server can be deployed on any DL380/R740 server, but the following configurations are suggested:

The DL380G10 server has the interesting option to plug the system disk (2xSFF) in the rear harddrive bays. Remaining front harddrive bays can all be used to plug backup disks (LFF or SFF), creating a 216TB (12x18TB) backup server.

Several storage options are available to extend the backup capacity (HP MSA, StoreEasy NAS systems).

Alternatively, a HP Apollo 4510 4U server can fit 60 x LFF 18TB disks, which will give a **petabyte** of storage.

HPE Apollo 4510 Gen10 System Front View

HPE Apollo 4510 Gen10 System

The DELL PowerEdge R740xd server has the option to store 18x16TB disks (288TB):, 12 disks FrontBay, 4 disks MidBay, 2 disks RearBay)

Proven technology, existing mechanism

GBS originates from an existing telecom environment. It has a proven track record of backup and restore capabilities. The existing disaster recovery, image backup and data backup mechanisms are versatile mechanisms that work for the virtual environment just as well as for the original bare metal environment.

GBS was already adapted for VMware/vSphere and now it has been tested successfully for OpenStack and KVM.

More GBS info

For more info on the GBS backup products and solution, please visit our website: www.gbsbackup.com

Or please feel free to contact our Technical Director:

Roel Otten (+31 20 3697972)
info@gbsbackup.com