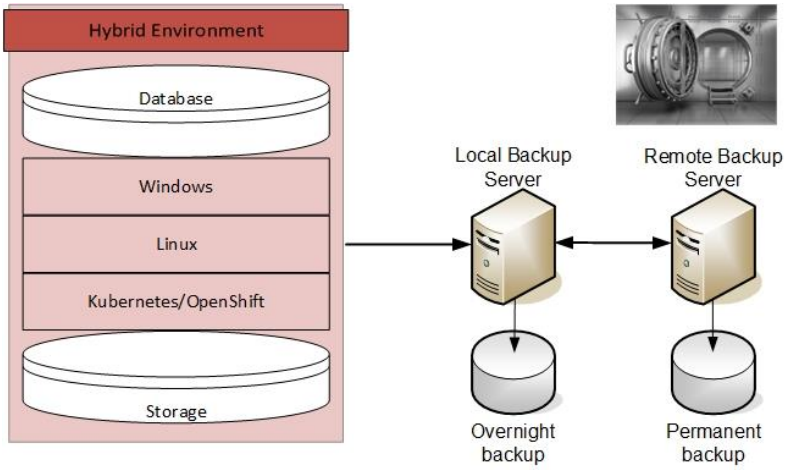
Backup and Security (in GBS3)

Overview

The Generic Backup Solution (GBS) offers a secure Linux based backup server that can back up bare-metal, virtual systems, KVM, OpenStack, OpenShift, and network equipment.
It supports backup and recovery for Linux, Solaris, HP-UX, OpenVMS and Windows/MacOS environment.
Backup data is secured to protect the client from outside cyber, ransom and wiper attacks.

For backup and restore of Linux systems, GBS has integrated its system backup mechanism with Open Source ReaR tooling to facilitate Disaster Recovery on Bare Metal and Virtual Machines (VM).
These mechanisms are incorporated in a Hybrid and Virtual backup server architecture.
A Hybrid GBS backup server is a hardware-based backup solution that will make independent backups outside the virtual environment
A Virtual GBS backup server has the same functionality but runs as a VM in the same virtual environment, so it needs an off-site peer server.
The main goal is to provide a full (off-site) recovery mechanism for a disaster in the virtual/bare-metal environment.



Backup Phases

Aa a small recap of GBS functionality, the backup operation consists of several backup cycles and processes:

- Backup preparation (phase 0)
  This phase extracts database information to prepare databases on the client system for the backup.
  These procedures are usually set up as local procedures on the backup client.
- Overnight system/data backup (phase 1)
  This mechanism collects the most recent backup data from Linux backup clients during the night.
  It includes all data in- and outside the system disk (system backup and data backup).
  It is executed on the GBS backup server and uses RSYNC over SSH to encrypt the communication with the backup client.
  A dedicated secure backup account is created/used on the backup client to enable a secure SSH connection.
- Permanent backup (phase2)
  This phase collects a backup history for longer retention:
  A copy of the overnight backup is transferred to a (remote) permanent backup destination during the day.
  Daily weekly and monthly copies offer a configurable retention time (3 months by default).
- Image backup with ReaR (RElax And Recover)
  Open-Source ReaR (Relax And Recover) tooling is used to collect a Disaster Recovery image for the backup client.
  ReaR is available for most Linux distributions and creates a recovery kernel/initrd that can be used to restore the client from scratch after a disaster.
  The ReaR backup is executed on an incidental basis after a system installation/upgrade and is used as a "last resort backup".
  Included in the ReaR Backup is a backup image that is identical (in structure) to the GBS system backup. Therefore, the user has the choice to restore the system from the last resort image backup, or from a recent up-to-date system backup.

For more information on the general backup functionality, please refer to the "Hybrid Backup" Factsheet.
The remainder of this whitepaper will focus on the security features that are introduced in the latest GBS Release 3.

Security Focus

The new GBS3 release focuses on implementing strict security requirements.
In this new release, some of the existing backup mechanisms have been replaced with more secure alternatives.
RSYNCD is replaced with RSYNC over SSH. NFS is replaced with a more secure mechanism.
In addition, the GBS3 release includes a focus on key management of the PKI keys used in the backup process.
Key management is an essential part of secure backup, to avoid unauthorized access of backup data and to protect the backup clients.

The backup server is designed as a Backup Vault with limited access, to protect the client's backup data.
On the client side, GBS makes sure that adding a backup does not weaken the security of the user's system.
E.g., adding backup agent software to a customer's server would add the potential for a security breach and has been reconsidered.
The architecture in GBS3 has been modified to avoid installation of agent software on the backup client.
RSYNC is used in GBS to execute the backups because it is already present and installed on most Linux distributions by default.
The backup server will still need to copy the backup data outside the original domain, to have a backup copy available when needed.
Therefore GBS3 includes additional measures to protect the data from unwanted access and security breaches.
Access to the backup server is limited as much as possible. Outside inputs are eliminated, e.g., no web interfaces are allowed.
All backup activities originate from the backup server itself, to avoid potential security issues.
The backup client can only access its own data via restricted protocols. No login to the backup server is required for day-to-day backup/restore activities.

If remote backup management is required, the backup schedules can be driven from a MySQL database.
The backup server will send a daily status report via email (SMTP), including system health information, so that there is no need to login to the system for monitoring. SNMP traps will be sent to alert for possible issues.

Why backup security

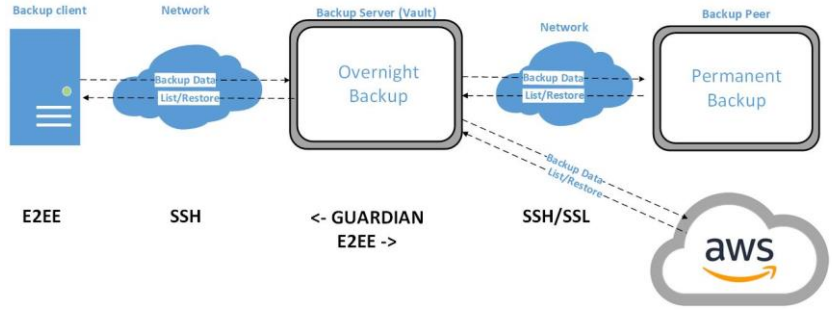
In previous releases, the original goal for backups was to facilitate a backup copy of data in case of accidental deletion.
Security of the backup server was not urgent in the past, as we did not expect the user to delete the backup data intentionally.
Nowadays, it can no longer be assumed that the backup user is always working in good faith.
Cyberthreats increasingly threaten the IT and Telecom environment.
Backup now performs the additional task of protecting the user's data as safeguard and fallback in case of a cyber (ransom or wiper) attack.
In GBS3 we consider that the backup user (at the client node) may be an attacker trying to breach, ransom or compromise the backup data.
Therefore, the backups and the backup server need to be protected, to avoid that the attacker also deletes or modifies the backup.
The following requirements are implemented in a GBS3 backup system:

- A backup client can only read its own backups, not access other backups.
- A backup client cannot modify backup data, to avoid that the backup gets compromised by an attacker.
- The backup is never initiated/modified by the backup client, to avoid that an attacker disables or overwrites the backups.
- Backups need to be protected from direct operator access; backups should only be accessible by the original backup client.
- The backup server needs to be secured from external access, because it stores encryption keys and sensitive/classified data.
- The backup process will not compromise the security of the backup client.
- Backup server is an autonomous system that doesn't need regular access for maintenance.
- System monitoring info is sent by the backup server on a regular basis, so that login for monitoring is not needed.

Although GBS focuses mainly on Linux client backup, we have recognized that Linux is a perfect platform for Windows/MacOS backup.
Recently, we have seen wiper-attacks that focus on the Windows PC environment, erasing the complete Windows physical drives (FAT and NFS). An interesting article about this is published at: https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/
In this case, the GBS Backup Vault solution offers a companywide failsafe solution for such a Windows disaster because the backups are stored in a Linux environment.
For Windows/MacOS backup, GBS stores the user's data and documents in a document management frontend, which is also Linux based and has a 2nd level backup stored in the Backup Vault.

Security at the Backup Client

To protect the backup client from unauthorized access via the backup server, we focus on security in the backup mechanisms.
For data transfer between the backup client (the user's system) and the backup server we only use RSYNC via (secure) SSH.
RSYNC is already installed on the client (default in most Linux distributions), so there is no need to install new backup software.
A dedicated "backup user" account is added at the client to avoid the need to use a root user.
We use several mechanisms to protect and secure this "backup user" account.
First, the password for this account is disabled (locked), so that the account can only be accessed via key-based authentication.
Next, we add the public-key of the backup server to the account, so it can only be reached from the backup server and no other.
The corresponding private key is only known inside the backup server's internal process and cannot be used from any other source.
This mechanism assures security of the client, as there is no way the account can be accessed other than from the backup server's process.
In addition, the "backup user" account is setup with a restricted bash shell (rbash) that only allows execution of the RSYNC command, so that it cannot be used to execute any other command on the system.
As a result, an intruder on the backup server cannot access the client nodes.



Security at the Backup Server

The GBS backup server holds a copy of the client's valuable backup data.
It is therefore vital to protect this data with the same (or higher) level of security as that is installed on the backup clients itself.
For the GBS backup server, there are three potential sources from where an attack could originate:

- Attacks from outside (third party).
  In this case we must protect our backup server from external access.
  The solution here is to deploy the GBS backup server as a vault with limited or no login possibilities at all.
  All backup activities originate from a schedule inside the backup server, no outside triggers are allowed.
  In general, we avoid installing web interfaces or 3rd party software on the GBS server, to shield the backup vault.
  Backup schedules are managed via an internal scheduler.
- Monitoring backup data transfer (man in the middle attack).
  The data stream between backup client and backup server needs to be protected, as it basically transfers all the files from the client to the server. This threat is mitigated by using encrypted communication (e.g RSYNC over SSH).
- Attack from inside, when one of the backup client systems has been compromised.
  In GBS3, the user's system (the backup client) is not trusted and considered to be possibly compromised by an attacker.
  The backup client is given read access to its backup data (for data restore purposes) but is not allowed to modify that data to avoid that the attacker also erases the backup.
  The backup client has no access to the backup server and cannot access the data of other clients.

In addition to these measures, the GBS backup server is secured from outside access by implementing OpenSCAP hardening guidelines, limit SSH access and apply firewall rules. GBS3 shields the backup server as a closed box without any user access.
Login to the backup server will only be granted for incidental maintenance, where the login activity and duration will be reported to an email list to detect any unauthorized access.
System status and health will be reported by the server on a regular basis to the same email list, to avoid the need to log in for health checks.
Encryption keys to access the client systems are always protected with a passphrase, to further increase the security on the backup server.

PKI Key management

For backup purpose, the backup server has SSH access to the backup clients with Public Key Infrastructure (PKI) or key-based access.
As this key gives access to the backup clients, it is the most sensitive of the keys and needs to be secured so that it cannot be used by an intruder if the backup server is compromised.
For this purpose, the backup server will secure the key by locking it away, so it cannot be used from other sources.

Permanent backup

The permanent backup resides on a remote server/location, to provide a geo-redundant backup.
In previous GBS releases, NFSv4 was used to mirror the backup data between the remote and the local backup server.
However, NFS has several disadvantages:

- It's a daemon process on the remote side and requires (listens to) port 2049 to be open.
  So it needs adjustments to firewalls on the network (to allow port 2049 traffic).
  Additional open ports are something we try to avoid in the backup vault.
- The protocol itself is not secure, it can only be used on a friendly local network, and definitely not via internet.

In GBS3, NFS has been replaced with a more secure protocol, that only uses port 22 (SSH) and can even be used to connect a remote backup server via internet. The backup procedures in this case use RSYNC over (encrypted) SSH.
For restore purpose, the permanent backup data is mounted to the original backup system, so that it is accessible for the backup client.
To protect the data on the remote server, the permanent backup data is attached as a read-only, which prevents users (attackers) from modifying the data. The permanent backup data can also be encrypted (E2EE) in case the remote system is not trusted.

Restoring Data

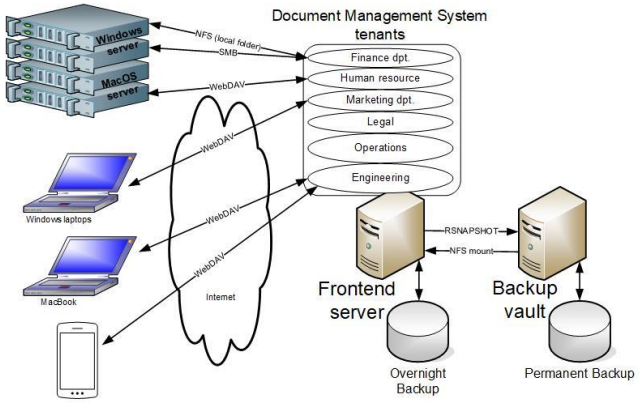
In GBS3 the user can restore data from a backup that resides on the backup server.
The user will not have direct access on (or a login to) the backup server. Instead, the user can issue an RSYNC command to list or retrieve data from the backup server. The RSYNC command uses a dedicated account on the backup server for an SSH request.
The RSYNC command can be issued from the root user on the backup client node, or from any user account with sudo privilege.
Via RSYNC, the user is restricted to view only his own backup data in his own backup directory.
Each backup client has its own subdirectory on the backup server and cannot access the data of other systems.

Backup encryption

Backup file encryption is another mechanism that can offer additional backup security. "Duplicity" or "Restic" backup are available in GBS3 to offer encrypted backups. Duplicity is the preferred tool for backup encryption, as it fully works with ReaR for disaster recovery.
Restic can be used to backup specific sensitive data files and directories, but it cannot be used for disaster recovery.
Encryption can be integrated with ReaR disaster recovery, but it adds much complexity to the backup solution and might complicate and delay the restore process when it is urgently needed.
Backup encryption is only recommended if necessary, and if procedures are in place to administer the encryption keys and passphrases.
Backup encryption is typically required when the data is stored on a hosted or cloud-based repository, where the security is not trusted.

Document Management System frontend for Windows and MacOS backup

For Windows and MacOS environments, a Document Management System (DMS) is used as a frontend for the backup vault.
The DMS provides a structure to organize the user's documentation.
The DMS system already has a high level of security by it selves.
It is backed up by a secondary backup vault that will function as a last resort to restore the DMS in case that gets compromised.
The GBS backup server is ideally suited for the backup of a Windows/MacOS environment because the backups are stored on a different ecosystem (Linux) that is not vulnerable to the windows attacker.
GBS partners with DMS vendors to provide cost effective DMS solutions.
For more information, please refer to the GBS factsheet about Windows/MacOS backup.



Further securing the Backup Server

The backup server is secured with OpenSCAP security and hardening guidelines during the deployment phase.
In GBS3, the backup server is deployed with a RHEL9 or AlmaLinux 9 distribution, which has an OpenSCAP security policy during the rollout.
This enforces a set of security rules: https://static.open-scap.org/ssg-guides/ssg-rhel9-guide-cis_server_l1.html
In addition to these OpenSCAP guidelines, we include several additional measures to further secure the backup server vault:

- Disable all services that create a communication (Listen) port on TCP or UDP.
  The only active open port on the backup server will be 22 for SSH. No other TCP/UDP ports should be open (listened to).
- Disable 3rd party software that requires access to the system.
- Disable PXE boot option in the BIOS, disable USB drive keys in BIOS, disable CDROM, protect BIOS access with a password.
  To prevent unauthorized access to the backup server via PXE, USB or CDROM.
- Encrypt system and data disks to avoid data being compromised in case of theft or boot from external disk (USB or PXE).
  A hacker may try to access the disks by mounting the disks to a different server (USB or PXE booted).
  In such cases, the data on the system disk will be not accessible because it is encrypted.
  The encryption keys for the client backups will also be stored on the system disks, so these need to be protected.
- Secure and update IPMI/iLo/iDRAC to the latest firmware versions. Configure IPMI/iLo in FIPS mode according to the manufacturer's guidelines for security (HPE Integrated Lights-Out Security Technology Brief).
  Lock or disable to access the system via IPMI (iLo or iDRAC) if possible.
- Remote access only via key-based authentication, also for IPMI/iLo interface.
- Report all access (attempts) in a status report email.
- Encrypt the data disks, if the backup server is deployed on a bare metal system, to prevent that the data gets compromised if the data disks get physically stolen.
- Disable core dump on the backup server.
  We disable the core dump facility in order to avoid that the stored PKI key can be compromised.
  see also guidelines listed online:
  https://www.cyberciti.biz/faq/disable-core-dumps-in-linux-with-systemd-sysctl/
  https://access.redhat.com/solutions/5955071

Key benefits of GBS in general

Our customers choose for a GBS backup solution because of the following reasons:
- GBS solution consists of License free Open-Source software.
- GBS creates independent backups outside the original application domain (e.g according OpenShift recommendations)
- GBS includes Disaster Recovery for bare metal and Virtualized environment
- GBS has a Document Management System as frontend for Windows and macOS backup
- GBS has georedundancy to mitigate a site disaster
- Data storage in GBS uses VDO deduplication which can reduce diskspace with 60-80%

More GBS info

For more info on the GBS backup products and solution, please visit our website: www.gbsbackup.com
Or feel free to contact our Technical Director:
Roel Otten (+31 20 3697972)
info@gbsbackup.com