GBS Backup

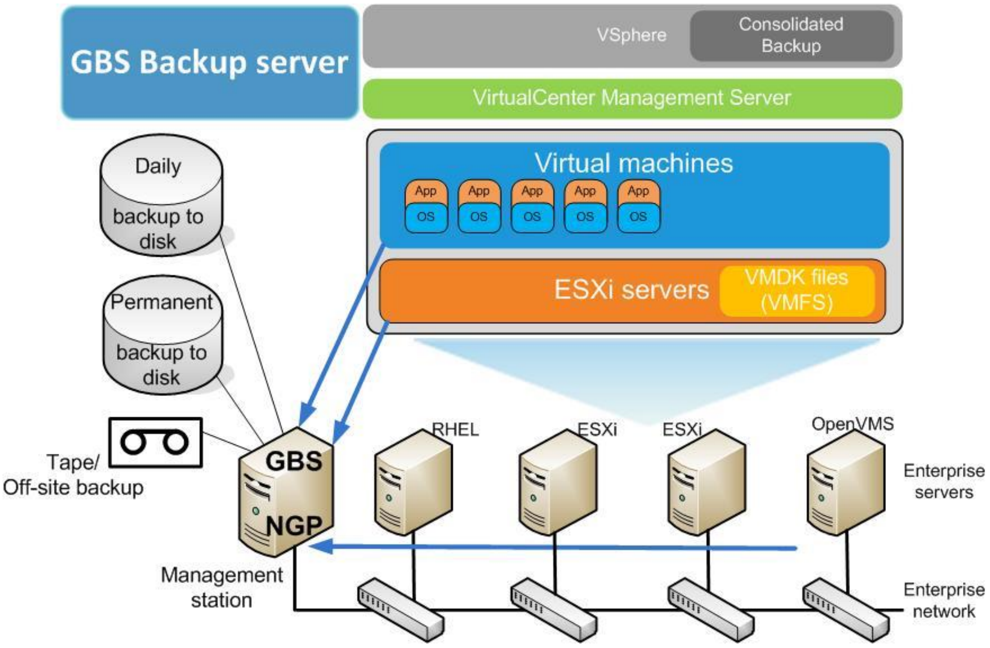
Backup & Deployment

Factsheet

Hybrid Backup Server

Overview

The Generic Backup Solution (GBS) offers a Linux based Backup Server that is capable of backing up Virtual systems, Non-virtual systems, SAN and network equipment.
It supports backup and (disaster) recovery for Linux, Solaris, HP-UX, OpenVMS and Windows server.
The Hybrid GBS backup server is a hardware-oriented backup solution that will make independent backups outside the virtual environment (including offsite backup possibility).
Main goal is to provide a full recovery mechanism for a disaster in the virtual environment.
The Hybrid Backup server is a bare-metal backup server, based on HP or DELL hardware with RHEL7 or Centos7 OS and with additional data disks for backup storage.



KEY BENEFITS

Open Source software, License free

NFV integration

Outside approach, backups outside the application domain

Disaster recovery for bare metal and VM's

Backup and recovery of OpenStack infrastructure

Georedundancy to mitigate a site disaster

Deduplication using OpenSource VDO

WEB interface and REST API

GBS is an easy backup service for operations as it eliminates the hassle of tape backup;
File based backups are easily readable/browsable on the Linux file system.
Each night only incrementals are transferred, limiting the amount of transferred backup data.
The Hybrid GBS backup server offers the following backup functionality:

- Backup for bare metal and virtual machines (in OpenStack, VMware or RHEL/KVM)
- Centralized backup to backup all elements in the customer enterprise solution onto a single backup disk repository. Simplifies interfacing to 2nd level (tape,cloud) backup.
- Full system image backup (rsync based), file-based system image (thin backup).
- Disaster recovery for bare metal and virtual systems (Linux, Solaris, OpenVMS/SMSC).
- Additional "data backup" mechanism to backup data repositories outside the system disk. This typically includes repositories on SAN (EVA/3PAR) and databases.
- VMware/OpenStack/KVM Hypervisor configuration backup.
- Backup of network elements (configuration files).
- Tape backup; EMC networker or Bacula (open source, license free).
- Internal backup storage capacity up to 288TB.
- Backup Encryption (GnuPG), to encrypt sensitive backup data.
- Gateway function for customer specific backup mechanism.
- SAN Snapshot backup; to backup large Oracle databases and repositories on SAN.
- Geographic redundancy; backups stored remote, GBS servers at multiple sites.
- Data compression and deduplication (with VDO), gives 60-80% reduction of backup size.

Backup Cycles

The GBS backup operation consists of three backup cycles:

- Backup preparation (phase 0)
  Extracts database information in order to prepare databases for the backup.
  this requires local diskspace on the backup client.
- Overnight backup (phase 1)
  Transfers all the backup data to the local backup server.
- Permanent backup (phase2)
  Maintains backup history: Daily weekly and monthly copies to offer a configurable retention time (3 months by default).

Advantages of a Hybrid Backup Server:

The Hybrid Backup Server has advantages compared to vendor specific mechanisms.
Vendors like VMware, HP (DataProtector), EMC Networker, offer backup mechanisms that still need to be configured and tested for each application. GBS will fully configure, deploy and test the backup procedures.
GBS backup procedures have already been tested and documented for various Linux distributions, it therefore saves a lot of work in each telecom project, as the backup & restore part in the project can be minimized.
GBS can interface with vendor specific backup mechanisms, and will act in that case as a backup gateway to the customer application nodes. Other GBS advantages:

- No license fees, because we are using open source software
- Backups are independent from virtual infrastructure, backups can be restored (redeployed) on different virtual infrastructure (OpenStack, VMware, KVM) or bare metal.
- Direct interfacing to hardware and disk I/O, giving higher performance and capacity.
- Direct interfacing to tape autoloader (Bacula option).
- Backup procedures are fully tested for various Linux distributions and applications.

Disaster Recovery (Linux, Solaris, OpenVMS and virtual machines)

GBS includes a Linux based disaster recovery mechanism based on open source "SystemImager".
SystemImager creates a mirror copy of the backup client's system disk onto the backup server.
Also the file system and partition info of the system disk is captured, so the system disk can be recreated from scratch in case of a disaster.
The restore process is fully automated and does not require knowledge on how to deploy the application.
The disaster recovery mechanism uses the the KOAN (Kickstart Over a Network) or PXE network boot to boot from the backup server and to restore the system disk, typically within 10-30 minutes. It can be executed remotely and does not require onsite presence.
In a virtualized solution, the SystemImager backup mechanism offers filespace advantages over the VMware VMDR mechanism. It stores only the actual (thin deployment) filespace, and (big) repositories can be excluded to limit required storage.
It is hardware independent and also independent of the virtual environment.
Therefore it can be used in different virtual environments (VMware, OpenStack/KVM) or even to migrate a virtual machine between different virtual environments. It even allows migration of virtual to non-virtual machines.
For Sun Solaris a similar tool is available based on FLAR archive.
For OpenVMS a disaster recovery mechanism is based on the VMS backup utility.
For VMware, an additional disaster recovery (VMDR) is available, based on a VM cloning mechanism.

Backup encryption option

GBS uses GnuPG and "Duplicity" to encrypt backup data at the source.

VDO data deduplication and compression

GBS deployment makes use of deduplication mechanisms:

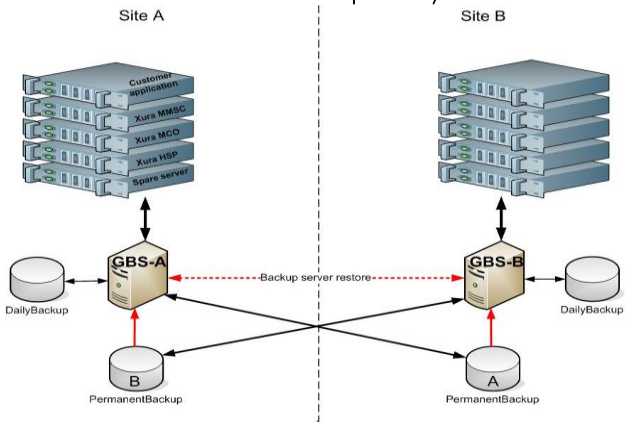
- Rsnapshot for the permanent backup uses "hardlink" deduplication.
  it only copies a file if the content has changed since the previous day.
  if a file did not change, only a hardlink is created to the pervious day/file.
  typically, the permanent backup contains 20 backups, requiring only 2,5 times 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 reduce the physical diskspace by a factor of 3-4 times (e.g storing 15TB of data on a 4TB physical disk).

KVM image backups

GBS has developed a new mechanism to backup KVM virtual machines.
KVM hosts typically run multiple VM's each represented with a VM image file.
These VM image files (usually in /var/lib/libvirt/images) are copied to the GBS backup server as an initial "full" backup. We only need to copy the image file once, subsequent incremental backups are executed using the regular GBS system/data backup mechanisms.
When a disaster recovery is needed, the VM image file is updated on the GBS backup server, and subsequently transferred to the KVM host to boot/restart the VM from. In RHEL8, the VM image file can be copied as a hot backup, using Qemu external snapshots.

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:



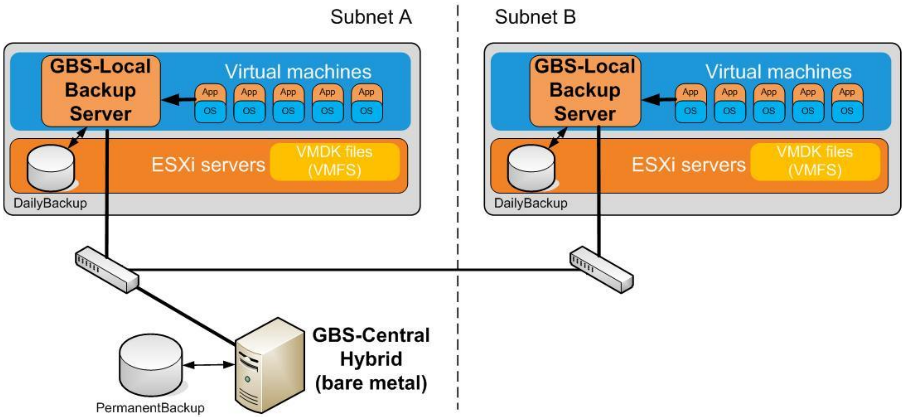
Geo redundancy includes the following features:

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

Local - Central setup

A Local-Central setup is suggested in to offload the local (virtual) backups, and make them available outside the virtual environment. In this setup, the local GBS servers are virtualized and forward their permanent backup to a remote Hybrid Backup Server, so that the backups are still available in case of a disaster in the virtual infrastructure. The virtual infrastructure and the local GBS servers can be restored from the hybrid (bare metal) GBS system.

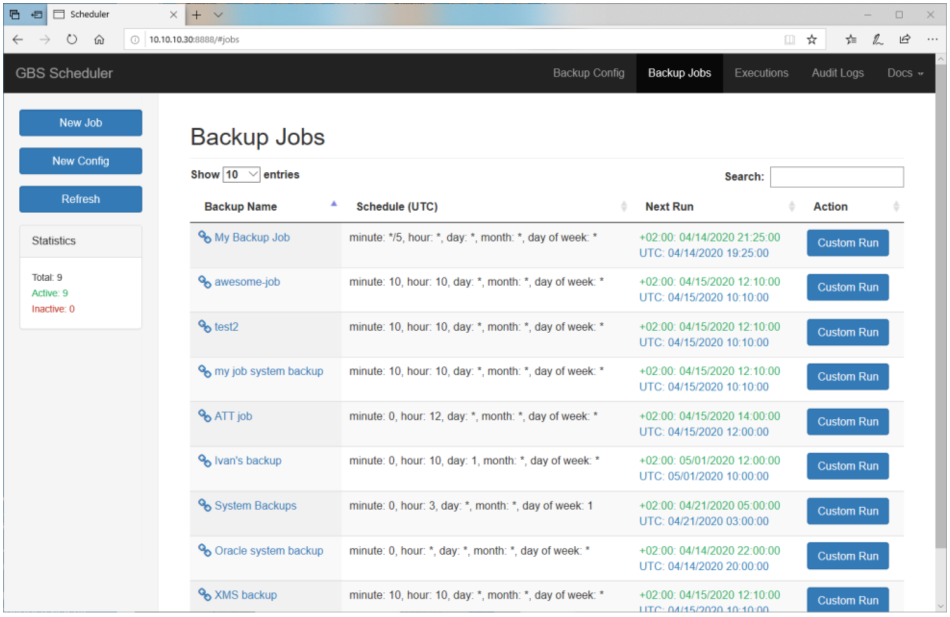


3rd Party (Tape) backup options (Bacula or EMC Networker)

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)

Web interface, scheduler and REST API

GBS introduces a web-based scheduler and REST API to replace the older CRON mechanism.
The Web interface and scheduler are based on the Open Source "Nextdoor scheduler" to define and schedule and trigger the backup commands. The Nextdoor scheduler also includes a REST API to present a RESTFULL backup interface.
The Nextdoor scheduler is extended by GBS with the concept of a "Backup config" to allow the used to define backup configurations via the web/REST interfaces.



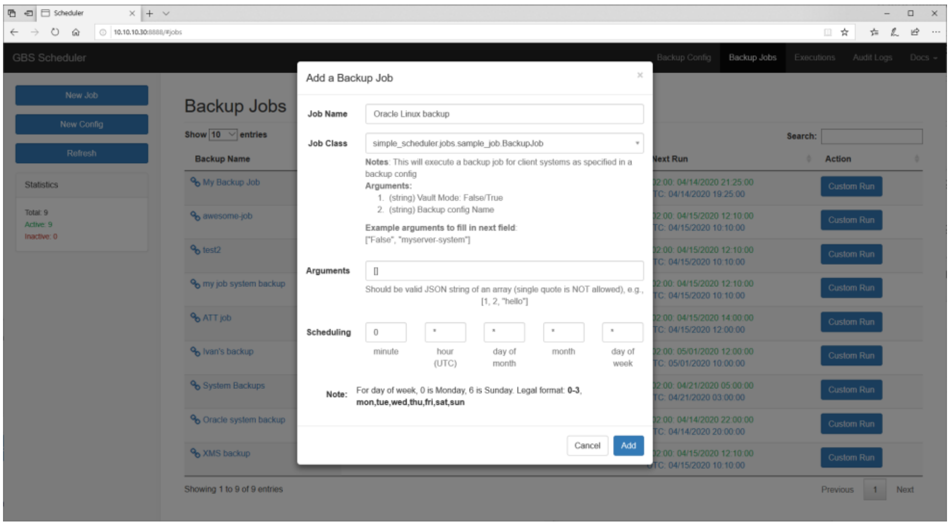
Statistics

Total: 9
Active: 9
Inactive: 0

Backup Jobs

Show 10 entries Search:

Backup Name	Schedule (UTC)	Next Run	Action
My Backup Job	minute: */5, hour: *, day: *, month: *, day of week: *	+02:00: 04/14/2020 21:25:00 UTC: 04/14/2020 19:25:00	Custom Run
awesome-job	minute: 10, hour: 10, day: *, month: *, day of week: *	+02:00: 04/15/2020 12:10:00 UTC: 04/15/2020 10:10:00	Custom Run
test2	minute: 10, hour: 10, day: *, month: *, day of week: *	+02:00: 04/15/2020 12:10:00 UTC: 04/15/2020 10:10:00	Custom Run
my job system backup	minute: 10, hour: 10, day: *, month: *, day of week: *	+02:00: 04/15/2020 12:10:00 UTC: 04/15/2020 10:10:00	Custom Run
ATT job	minute: 0, hour: 12, day: *, month: *, day of week: *	+02:00: 04/15/2020 14:00:00 UTC: 04/15/2020 12:00:00	Custom Run
Ivan's backup	minute: 0, hour: 10, day: 1, month: *, day of week: *	+02:00: 05/01/2020 12:00:00 UTC: 05/01/2020 10:00:00	Custom Run
System Backups	minute: 0, hour: 3, day: *, month: *, day of week: 1	+02:00: 04/21/2020 05:00:00 UTC: 04/21/2020 03:00:00	Custom Run
Oracle system backup	minute: 0, hour: *, day: *, month: *, day of week: *	+02:00: 04/14/2020 22:00:00 UTC: 04/14/2020 20:00:00	Custom Run
XMS backup	minute: 10, hour: 10, day: *, month: *, day of week: *	+02:00: 04/15/2020 12:10:00 UTC: 04/15/2020 10:10:00	Custom Run



Add a Backup Job

Job Name: Oracle Linux backup

Job Class: simple_scheduler.jobs.sample_job.BackupJob

Notes: This will execute a backup job for client systems as specified in a backup config
Arguments:
1. (string) Vault Mode: False/True
2. (string) Backup config Name

Example arguments to fill in next field:
["False", "myserver-system"]

Arguments: []
Should be valid JSON string of an array (single quote is NOT allowed), e.g., [1, 2, "hello"]

Scheduling: 0 minute; * hour (UTC); * day of month; * month; * day of week

Note: For day of week, 0 is Monday, 6 is Sunday. Legal format: **0-3, mon,tue,wed,thu,fri,sat,sun**

Showing 1 to 9 of 9 entries

NFV compliant backup solution

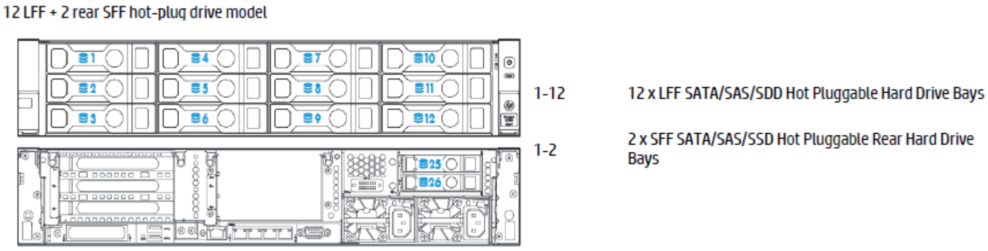
For the virtualized systems, GBS is moving to an NFV compliant backup server, that has scaling capabilities and can be invoked from the NFV orchestrator to create backup schedules when a VM is instantiated.

Proven technology, existing mechanism

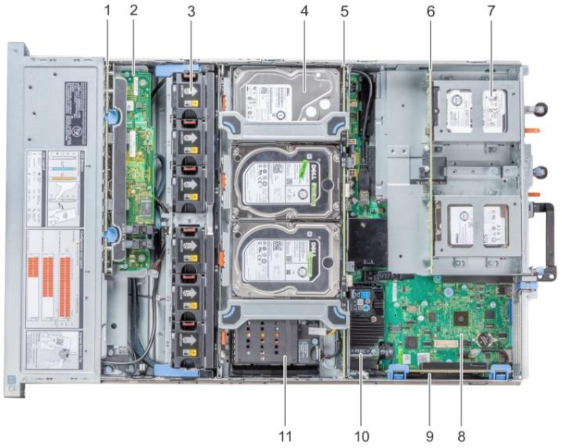
GBS originates from an existing telecom environment. It has a proven track record of backup and restore capabilities. The existing disaster recovery, image backup and data backup mechanisms are versatile mechanisms that work for the virtual environment just as well as for the bare metal environment. GBS was already adapted for VMware/vSphere and now it has been tested successfully for OpenStack.

Hardware options HP DL380, DELL PowerEdge:

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 to allocate the backup server in a different rack, or even in a different server room.
The backup server can backup equipment in 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 to create a 120TB (12x10TB) or 48TB (24x2TB) backup server:


12 LFF + 2 rear SFF hot-plug drive model
1
2
3
4
5
6
7
8
9
10
11
12
25
26
1-12
12 x LFF SATA/SAS/SDD Hot Pluggable Hard Drive Bays
1-2
2 x SFF SATA/SAS/SSD Hot Pluggable Rear Hard Drive Bays

The DL380 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)
In addition, the DL380G9 server can be conected to a tape-autoloader for tape backup and to A HP-SAN system for additional backup storage space.
The DELL PowerEdge R740xd server has the option to store 18x16TB disks (288TB):, 12 disks FrontBay, 4 disks MidBay, 2 disks RearBay):



Site disaster recovery plan

The GBS backup solution includes a disaster recovery service.
A disaster recovery plan identifies the critical components in the customers telecom/enterprise solution, and defines a step by step approach on how to restore things in case of a disaster.
In addition to restoring individual computer systems, a site disaster recovery planning is also included, to describe the whole recovery procedure in case the whole site needs to be rebuilt from remote backup

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