IGC

Disaster Recovery

December 2019

1 Summary

This document resumes the disaster prevention and recovery procedures set in place in the IGC for the main resources: Network, Compute and Storage.

2 Business continuity and disaster recovery

2.1 IGC IT room infrastructure

2.1.1 General description

The IGC has a single server room (data center) that hosts all the main IT services for the IGC.

2.1.2 Business continuity

The data center room is specially dedicated to the purpose of hosting IT services and features a closed container that is splash and fire resistant with an autonomous fire detection and extinction central, air conditioning with N+1 redundancy, redundant power lines that feed two independent UPS and redundant communications using multiple optic fibers to the remain of the campus and internet.

2.1.3 Disaster recovery

The IGC has 3 locations that can be used as *ad-hoc* hosting rooms in case of disaster.

2.2 Backup servers

2.2.1 General description

There are two main backup servers for the IGC data: persil01 and persil03. Each server has 180 TB dedicated to backup-to-disk and backup recovery staging. Persil02 has a LTO-6 tape library (24 tape capacity) responsible for off-line backups.

The larger storage system in the IGC, which runs the distributed file system AFS, cannot rely on persil01 and persil03 for backups due to the data size and has to rely on in-system backups.

2.2.2 Business continuity

Persil01 and Persil03 have the same backup processes and the same data sets and work in tandem to give resilience to the backup process. AFS backups in spite being in-system are located in different servers than the data being protected. Tape backups are stored in a fire-resistant safe in the IGC campus.

2.2.3 Disaster recovery

Recovery of persil01 and persil03 disk backups is usually below one hour, depending on the data set. Tape backups are inherently slower and can be recovered in less than a day. AFS system recovery relies on the AFS backup server availability and data set size, and can take a few hours.

2.3 IP network and telephones

2.3.1 General description

The network topology follows the classic organization of redundant core switches, located in the IGC data center, a redundant access layer in each building and access switches with redundant up-links.

The core switches (two HP 5406ZL and two Nexus 3100) are configured in a fail-over redundant configuration. The IGC firewalls (two Fortigate 1200D) are configured in a fail-over configuration. The IGC is served by two redundant ISPs, each with a redundant 1gbps fiber.

Telephone communications are implemented using IP and GSM devices that and rely on the NOS ISP IP communications services.

2.3.2 Business continuity

All connections upstream the access layer are redundant, relying on LACP trunks and spanning tree to automatically fail-over. Intranet routing is ensured by OSPF routers configured in the core switches relying on the VRRP protocol for robustness. Internet communications rely on ISP fail-over for broken links as well as in redundant firewall devices in the IGC. Core switches and the firewalls are under NBD maintenance and support contract.

Service or device	**Continuity implementation**	**Recovery**
Core switch services	Redundant with automatic fail-over setup.	Immediate and automatic recovery by redundant device.
Core switch devices	Rely on NBD service contract and reserve hardware (spares)	Manual recovery.
Distribution switch services	Redundant with automatic fail-over setup	Immediate and automatic recovery by redundant device.
Distribution switch devices	Rely on reserve (spares) devices.	Manual recovery.
Access switch services	Non-redundant with off-line replacements (spares)	Manual recovery.
Access switch devices	Rely on reserve devices.	Manual recovery.
Firewalls	Redundant with automatic fail-over setup.	Immediate and automatic recovery by redundant device.
Firewall devices	Rely on NBD service and support	Manual recovery.

	contract	

2.3.3 Disaster recovery

Network configuration is preserved in a configuration server and switch and firewall configurations are backed-up to a repository. The IGC maintains a pool of spare access-level devices and one 5406ZL chassis for core switches, ensuring that in case of failure, contingency emergency hardware can be deployed.

Device	**Backup source**	**Backup process**	**Frequency**	**Recovery**
Switch and firewall	onfiguration	Backup to TFTP server and then to git repository	Daily	Manual recovery of configuration to device

2.4 IT services and servers

2.4.1 System description

The IGC IT infrastructure relies on three main resources: data center networking, storage servers and compute. These three components assemble the IGC virtual hosting infrastructure where all other services are implemented on.

The data center networking infrastructure relies on top of the rack switches in a redundant configuration. The storage resources consist mostly of appliances exporting NFS, iSCSI or VMFS. The compute resources have hypervisors deployed (ESXi, KVM) that are orchestrated by VMWare, Cloudstack and automation scripts developed by IT.

All the storage appliances backup to two storage servers using both backup to disk and backup to LTO-6 tape, which is archived on a fire resistant safe in the IGC campus. The backup servers use Copy on Write for on disk backup and bacula software for backup to LTO-6 tape as well as on-disk.

2.4.2 Business continuity

All networking resources and links are redundant. The storage appliances rely on snapshots and replication. All storage appliances rely on the disk failure protection of RAID6 or RAID10 and have redundant network connections. Multipath is implemented for iSCSI and VMFS appliances, which serve the IGC mail server and the VMWare, respectively. Link redundancy in NFS appliances relies on LACP network trunks and distributed trunking on the switches.

Service or device	**Continuity implementation**	**Recovery**
ISCSI/VMFS volumes	Redundant with fail-over setup.	Automatic fail-over relying on multi path or manual fail-over to peer.

NFS volumes	Redundant with fail-over setup.	Manual fail-over to peer.

2.4.3 Disaster recovery

Backup relies on snapshot and replication, and snapshot and backup, to both backup servers persil01 and persil03. The mail server has additional backup procedures due to the importance of mail data.

Device	**Backup source**	**Backup process**	**Frequency**	**Archive span**	**Recovery**
NFS Storage appliance	Stored VM volumes	Snapshot to peer appliance	24 hours	7 days	Manual recovery
ISCSI Storage appliance	Volumes	Snapshot to peer appliance	10 minutes	20 minutes	Manual recovery
Storage appliance	Stored VM volumes	Snapshot and backup to backup servers	12 hours	14 days	Manual recovery
Storage appliance	Stored VM volumes	Snapshot and backup to off-line Tape	12 hours	2 months	Manual recovery
Mail server	Mail folders	Bacula backup	Weekly full backup with differential every 12 h	2 months	Manual recovery
Mail server	Mail folders	Snapshot copies	24 hours	30 days	Fast manual recovery of specific files

2.5 Scientific data in AFS file system

2.5.1 System description

IGC scientific data is stored in a distributed file system (Andrew File System – AFS) exposed to the IGC as a standard network shared folder storage (SMB, AFP, SFTP). AFS has the concept of data volumes, which in the IGC have an average of 2TB. The system is implemented on 10 data servers, each server hosts a number of data volumes that are backed up to other servers. The IGC AFS has roughly 800TB, of which about 300TB are data and 500TB are compressed backed-up data.

2.5.2 Business continuity

All network resources and links are redundant. The data servers disks are configured in standard RAID-6 aggregation of 8 disks.

Data or device	Continuity implementation	Recovery
AFS Data server	Off-the shelf hardware components	Manual recovery with spare parts and components
AFS Data	Incremental backups	Manual recovery

2.5.3 Disaster recovery

Backup relies on the internal AFS mechanism of data volume snapshot and backup. Depending on the nature of the data volume, various exclusive backup cycles are chosen.

Device	Backup source	Backup process	Frequency	Archive span	Recovery
AFS data servers	AFS data volume marked for daily backup	AFS compressed volume dumps	24h Incremental 1M Full Backup	2M	Manual recovery
AFS data servers	AFS data volume marked for weekly backup	AFS compressed volume dumps	7 days Incremental 2M Full backup	4M	Manual recovery
AFS data servers	AFS data volume marked for monthly backup	AFS compressed volume dumps	1M Incremental 4M Full backup	8M	Manual recovery
AFS data servers	Small AFS data volume marked for daily backup	AFS compressed volume dumps	24h Incremental 3M Full Backup	6M	Manual recovery
AFS data servers	Scratch volume for temporary data	Move AFS data volume to archive status	1M archival	3M	Manual recovery