Backup and Restore Strategy

1. System

In case of barebone installations we recommend the following multi-layered backup and recovery approach to ensure data protection and business continuity. Such infrastructure utilizes hardware-level redundancy combined with comprehensive software backup solutions.

Hardware Redundancy

- **System Disks**: RAID 1 (Mirroring) for operating system and applications
- **Data Disks**: RAID 5 (Striping with Parity) for data storage with fault tolerance
- **Coverage**: Protects against single disk failures in both system and data arrays
- **Hot-swap Capability**: Failed disks can be replaced without system shutdown

In case of virtualized environment in addition to automatic snap-shots provided by most virtualization systems you can use also the provided below solution which can be used also to move to a different environment without hassle.

2. System Backup Strategy

Relax-and-Recover (ReaR) Implementation

- **Backup Type**: Full system backup including OS, configuration, and applications
- **Output Format**:
  - Bootable recovery ISO image
  - Compressed tar.gz archive
- **Frequency**: Monthly (default, configurable to weekly/daily)
- **Storage**: Configured remote storage (NFS, S3, SFTP, etc.)

Manual Backup Commands

```
# Check ReaR configuration
rear checklayout
```

```
# Perform manual backup
rear mkbackup

# Create rescue image only
rear mkrescue

# Verbose backup with debug information
rear -v mkbackup
```

Recovery Scenarios

- **Automatic Restore**: When remote storage remains accessible during recovery
- **Manual Restore**: Requires manual remounting of remote storage if inaccessible

3. Database Backup Strategy

Daily Backup Operations

- **Frequency**: Daily automated backups
- **Local Storage**: `~/backups/` (contains daily database dumps)
- **Scope**: All MongoDB and Postgres database instances
- **Replication**: Synchronized to remote location (typically same as system backups)

4. File-Level Backup Strategy

Flexible Folder Backup

- **Target**: Configurable folders from data drives
- **Methods**:
  - Default: rsync with incremental transfers
  - Alternatives: rclone, duplicity, or custom scripts
- **Frequency**: User-configurable (daily/weekly/monthly)
- **Storage**: Remote location separate from system backups

5. Complete Restore Process for Hardware Failure

Scenario A: Partial Hardware Failure (Hot-swap Recovery)

1. **Disk Replacement**: Hot-swap failed drives while system is running
2. **RAID Rebuild**: Automatic RAID reconstruction without service interruption
3. **Time Estimate**: 2-6 hours (depending on RAID array size and disk speed)

Scenario B: Complete System Failure (Approx. 3-8 hours)

Note: Time estimates exclude spare parts delivery, which depends on specific service agreements.

Phase 1: Hardware Replacement (Approx. 1-2 hours)

1. Replace failed hardware components
2. Rebuild RAID arrays as needed
3. Verify hardware functionality

Phase 2: System Recovery (Approx. 1-2 hours)

Transfer recovery ISO bootup image and boot the system from it (make USB stick or DVD from if needed). In the boot screen choose either automatic or manual recovery.

Automatic Recovery (when backup storage is directly accessible):

```
# Boot from ReaR recovery media
# ReaR automatically detects backup location and initiates restore
# No manual intervention required

# Manual trigger if needed:
rear recover
```

Manual Recovery (when backup storage requires mounting):

```
# Boot from ReaR recovery media
```

```
# Manually mount backup storage (example for NFS):
mkdir -p /mnt/backup
mount -t nfs 192.168.1.100:/backups /mnt/backup

# Configure ReaR to use mounted backup:
cat > /etc/rear/local.conf << EOF
BACKUP_URL=file:///mnt/backup
OUTPUT_URL=file:///mnt/backup
EOF

# Execute recovery:
rear recover
```

Phase 3: Database Restoration (Approx. 30 mins - 1 hour)

```
# Navigate to backup directory
cd ~/backups/

# List available backups (organized by date)
ls -la

# Restore database from latest backup
# Specific commands depend on database type (PostgreSQL, MySQL, etc.)
# Example for PostgreSQL:
pg_restore -d database_name latest_backup_file.dump
```

Phase 4: File Restoration (Approx. 30 mins - 3 hours)

bash

```
# Restore individual folders from remote backups
# Example using rsync:
rsync -avz user@remote-server:/backup/path/ /restore/location/

# Time varies based on data volume and network bandwidth
```

6. Estimated Total Recovery Time

- **Hot-swap Scenario**: 2-6 hours (RAID rebuild while system operational)
- **Complete System Failure**: 3-8 hours (excluding parts delivery)

- Hardware Replacement: 1-2 hours
- System Restoration: 1-2 hours
- Database Restoration: 30 minutes - 1 hour
- File Restoration: 30 minutes - XX hours - depending on volume

7. Key Configuration Files

ReaR Configuration (/etc/rear/local.conf)

```
# Example configuration
BACKUP=NETFS
BACKUP_URL=nfs://192.168.1.100/backups
OUTPUT=ISO
BACKUP_PROG_COMPRESS_OPTIONS=--gzip
BACKUP_PROG_COMPRESS_SUFFIX=.gz
```

Database Backup Location

- **Local Path**: `~/backups/`
- **Contents**: Daily automated database dumps with timestamped filenames
- **Retention**: Configurable (default: 30 days)

8. Maintenance and Monitoring

We recommend:

- Regular verification of backup integrity
- Monthly test restores to validate recovery process
- Monitoring of backup job success/failure
- Alerting for backup failures or storage capacity issues

9. Configuration Flexibility

All backup frequencies, retention policies, and storage locations are configurable to meet specific business requirements and compliance needs.

This comprehensive strategy ensures minimal data loss and rapid recovery in the event of hardware failure or system corruption, with hot-swap capability allowing most disk failures to be resolved without service interruption.

Revision #3
Created 12 November 2025 18:12:21 by Pierre
Updated 12 November 2025 19:30:27 by Pierre