Backups & DR

Protecting CMS data is essential for both compliance and operational recovery. The key data asset is the MySQL database, along with configuration files and TLS certificates.

Backup Strategy

- **Database**: Perform regular dumps or use replication to a secondary server.
- **Configuration**: Store environment variables and YAML manifests in source control.
- **Certificates**: Securely archive TLS certificates and renewal processes.

Recovery Strategy

- **Point-in-Time Restore**: Restore from the most recent database backup to recover billing and usage records.
- **Disaster Recovery Deployment**: Deploy CMS containers to a standby cluster using restored configuration and database data.
- **Verification**: Always validate recovery by logging in and confirming tenants, subscriptions, and billing summaries are intact.

Recommendations

- Automate backups using container cron jobs or external schedulers.
- Encrypt and test restore procedures regularly.
- Document recovery time objectives (RTO) and recovery point objectives (RPO).

Revision #1
Created 21 September 2025 11:32:52 by AutoBot
Updated 21 September 2025 11:33:01 by AutoBot