Disaster Recovery Plan (DRP)

Status	ACTIVE
Owner	@Jonas Purtschert
Last update	23 Oct 2024

Table of Contents

Introduction

The Disaster Recovery Plan (DRP) outlines our organization's strategies and procedures for ensuring business continuity and minimizing the impact of disasters or disruptions.

Key Personnel

Name	Position	Email
Loris Niederberger	Lead Business Development	loris@moodtalk.ch
Jonas Purtschert	Lead Technology	jonas@moodtalk.ch

Objectives and Priorities

Objective	Recovery Time Objective	Recovery point objective
Moodtalk Platform	24 hours	24 hours
Marketing Website	3 days	7 days
Self-Service Helpcenter	7 days	7 days
Helpdesk (Ticketing)	3 days	24 hours

The marketing website, self-service help center and help desk are provided by external providers whose service level agreements guarantee the RTO and RPO. The following paragraphs focus on the Moodtalk Platform.

Testruns of DRP

The disaster recovery plan is tested every year.

Test Date & Objectives	Recovery Time	Comments
24.08.2024, Moodtalk Platform	8 hours	Issue with deployment via Pipeline fixed. Recovery time could be minimized by expanding IaC to all services.

Emergency Response Plan

In case of an emergency, the following response plan must be followed:

1. Notify key personnel
2. Contact and set up disaster recovery team, the following key roles must be defined:
    a. Technical Lead (Responsible for the technical analysis of the incident and the post-mortem analysis)
    b. Customer Communication Lead (Responsible for the communication to all customers and for public communication, e.g. website, social media)
    c. Internal Communication Lead (Responsible to inform internal teams about the status of the incident)
3. Determine the degree of disaster and whether a failover needs to be initiated
4. Notify users of the disruption of service
5. Fix issue or execute failover plan (see section below)
6. While the fix or failover is in progress, update key personnel at least once every two hours
7. Monitor the services as soon as the fix or failover has been completed
8. Notification of users about the resolution of problems
9. Create post-mortem analysis

Failover of Service

During a failover from the PROD (Production) system to the INTG (Integration) system, all critical services and data are seamlessly redirected from the primary production environment to the designated integration environment. This transition ensures minimal disruption to ongoing operations and maintains continuity of service for end-users.

The failover process involves activating redundant systems and rerouting traffic to the INTG system, which has been configured to mirror the functionality and performance of the PROD system.

To perform a failover, the following sequence of actions must be followed:

1. Check if the production database management system of the PROD environment still works
    a. If yes,
        i. update INTG configuration to point to the database from the PROD environment
        ii. update resource group of PROD database so that the INTG environment has connection access
        iii. add internal IP from INTG environment to whitelist of PROD database
    b. If no,
        i. Restore the last backup from PROD and import the backup into the INTG environment
2. Check if the IDP of the PROD environment still works:
    a. If yes,
        i. update INTG configuration to point to the IDP service from the PROD environment
    b. If no,

    i. Restore IDP database from last backup and import the backup into the INTG environment
3. Deploy latest production release to the INTG environment
4. Reroute DNS entries for all applications to point towards the INTG environment, this includes:
    a. admin.moodtalk.ch
    b. api.moodtalk.ch
    c. id.moodtalk.ch
    d. idp.moodtalk.ch
    e. static.moodtalk.ch
    f. survey.moodtalk.ch
5. Update internal DNS zones for reverse proxy
6. Verify functionality of service

Postmortem

Create a postmortem and use the template found at Incident Postmortem Template