Surecomp

RIVO Backup & Disaster Recovery Process

For internal and external use

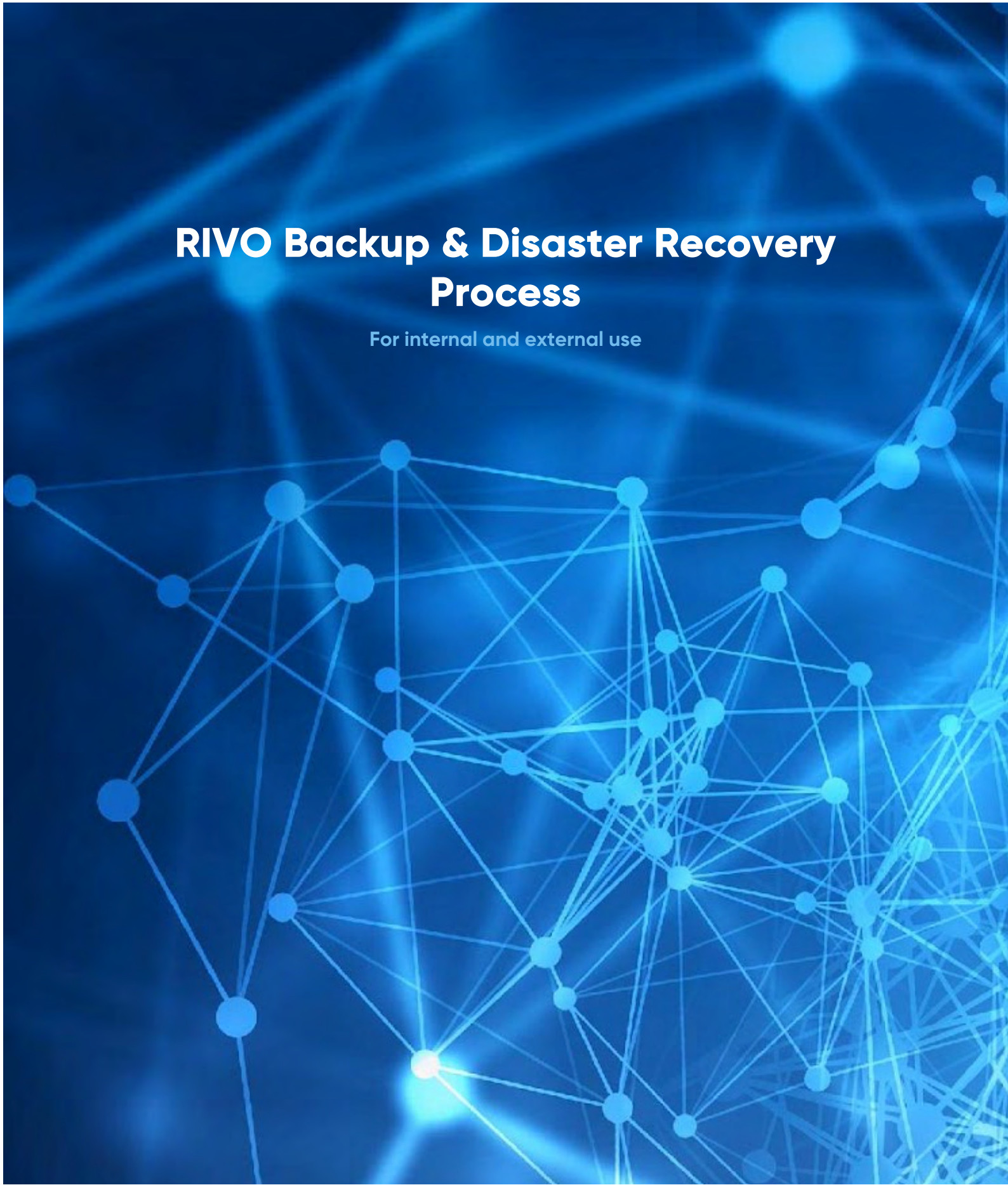


Table of Contents

1 Introduction

2 Operations

2.1 Backups

2.2 Disaster Recovery

2.3 DR Preparation/Setup – The Ideal Setup

2.4 Disaster Recovery Steps

2.5 DR Drill

1 Introduction

The main objective of this document is to provide support teams and/or customers with an overview of the Surecomp Backup and DR procedures which are part of Surecomp cloud offering on RIVO application.

Surecomp uses AWS Data Centres (link HERE) for **runtime production infrastructure** and for **Disaster Recovery infrastructure (DR)**.

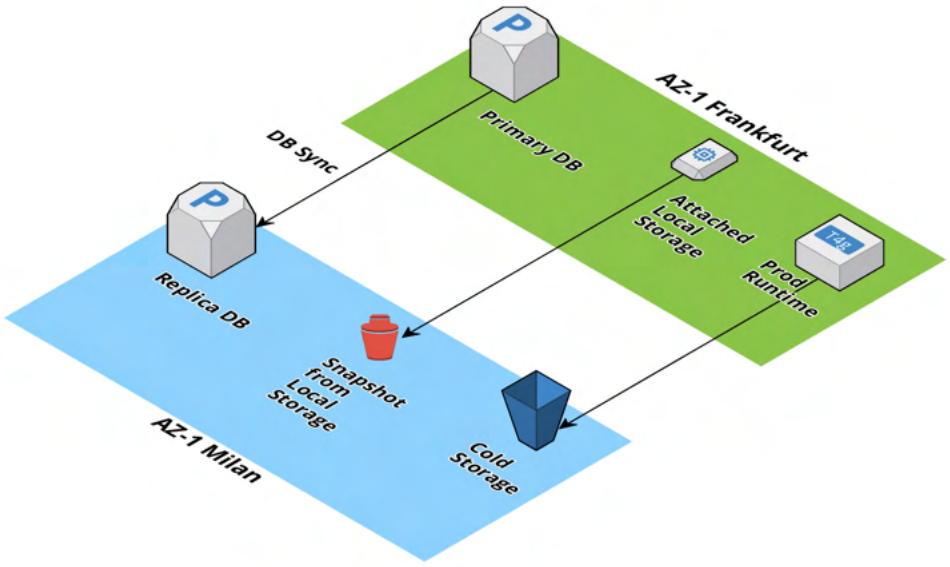
Documentation about AWS global infrastructure is at the LINK

In the event of a serious failure, Surecomp ensures that the production system is restored to the last known fully functional state, as expeditiously as possible.

Possible scenarios for activating DR infrastructure:

- Restoration from backups in the event of any data loss or corruption.
- Limited access to specific AWS availability zones or regions.
- ISP issues located in specific AWS availability zones or regions.
- DoS or any other cyber-attack that may prevent access to production traffic.

The Goal is to provide 99.9% availability to Rivo SaaS and ensure data recovery if needed.



2 Operations

2.1 Backups

RIVO Production application backups take a daily snapshot of the production machines, application server (s), and the database server (s) including:

1. All system files
    - system files are stored in a code repository system that uses a persistent-data storage volume with snapshots to a secondary AZ.
2. Configuration files
    - configuration files are stored in a code repository system that uses a persistent-data storage volume with snapshots to a secondary AZ.
3. Attachments files
    - attachment files are stored in a persistent-data storage volume with snapshots to a secondary AZ.
    - attachment files are also synced to cold storage.
4. Database information
    - databases are replicated to another AZ (availability zone) in the same region.
    - replication is running constantly.
    - In case of a failure in the main database, the replica can be used.
5. Database Archiving
    - databases are exported to cold storage once per day.

Backups, i.e., snapshot files are stored in different AZ, for a minimum of 30 days.

Backup

- Surecomp monitors the backup process and ensures the backups are successfully completed with a Monitoring system and getting alerts when there is any problem.

Restore

- Surecomp runs quarterly restore tests to ensure that restore can successfully be initiated if needed.

2.2 Disaster Recovery

In the event of a serious failure, Surecomp ensures that the production system is restored to the last known fully functional state, as expeditiously as possible. This may involve a restoration from backups in the event of any data loss or corruption.

Surecomp endeavours to reasonably meet the below RTO and RPO targets listed below:

Term	Definition	Objective
RTO	**R**ecovery **T**ime **O**bjective	Restoring RIVO to operation; within up to 24 hours, commencing as of when Surecomp is aware of the failure.
RPO	**R**ecovery **P**oint **O**bjective **D**ata **L**oss **T**ime	The maximum length of time permitted that data can be restored from: 4 hours

2.3 DR Preparation/Setup – The Ideal Setup

Action	Description
Infrastructure as Code (IaC)	The entire infrastructure is build via code and can be deployed automatically to create runtime production resources
Running DB backups	all Rivo databases are replicated constantly
Backups External volumes	compute resources does not store data locally but is storing data to an attached volume that is being snapshot to a different AZ

2.4 Disaster Recovery Steps

Action	Description
Infrastructure as Code (IaC)	Once the decision to activate the DR is made and no less than 3 hours, Surecomp initiate the creation of the DR via automated pipelines
Running DB backups	The DR will start using the replica databases
Backups External volumes	Compute resources will attach local storage from snapshots
DNS and access	Public DNS records will be updated with new ALB (load-balancer) and SSO (login) IP Addresses with TTL of 60 seconds

2.5 DR Drill

Surecomp will conduct a DR Drill at least once every twelve (12) months. This drill will cover RIVO business functions based on the Risk Management methodology.

All drills will be monitored and documented to assist the CISO and the Information Security Forum to conclude and mitigate any gaps raised during the drills.