DISASTER RECOVERY PLAN

KEKKOSLOVAKIAN JOULUKORTTI KY

CONTENTS

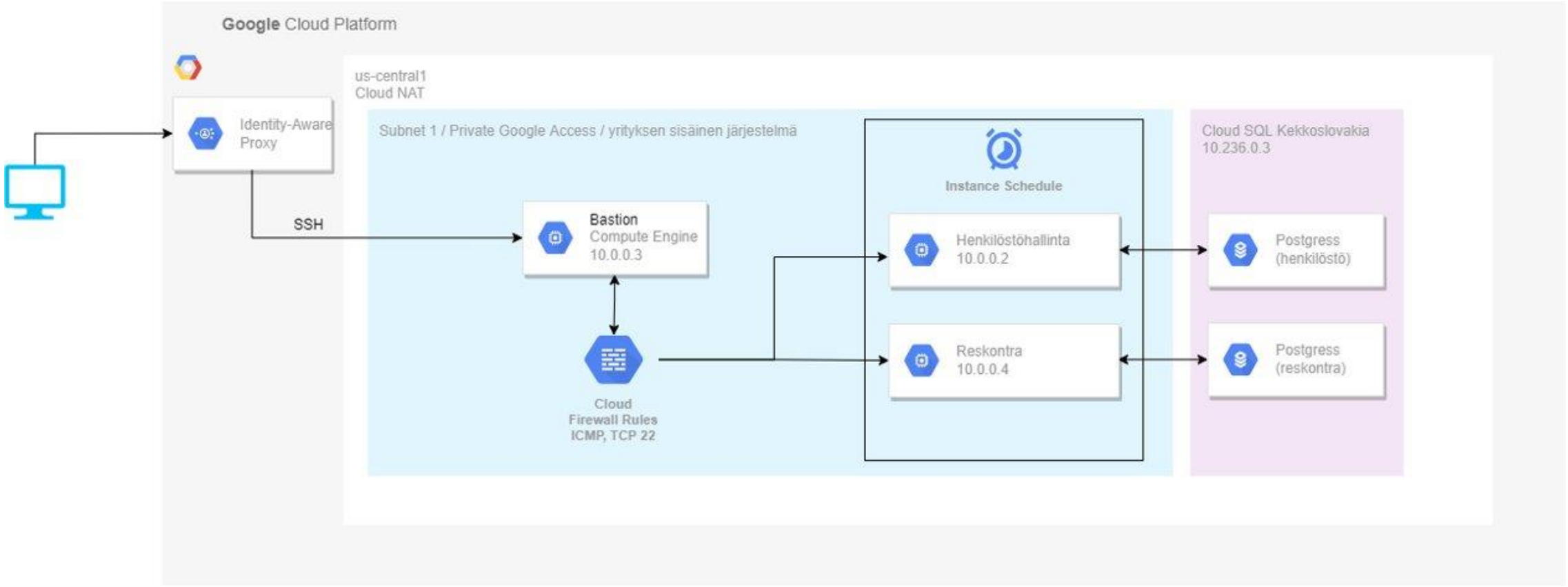
STATEMENT OF INTENT

This document maps out policies and procedures for technology disaster recovery, as well as process-level plans for recovering critical data and the product infrastructure. This document summarises recommended procedures. The mission is to ensure information system uptime, data integrity and availability, and business continuity.

OBJECTIVE

The principal objective of the disaster recovery plan is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations.

RESTORING IT FUNCTIONALITY – HR & FINANCE SYSTEM ARCHITECTURE



INVENTORY – HR & FINANCE SYSTEMS

- Network
  - VPC & subnet
  - NAT GW

- Security

  Google Identity-Aware Proxy (SSH connection for users)

  Bastion engine

  Private Google Access

  Cloud Firewall Rules

- Database resources
  - PostgreSQL database, 'multiple region' & highly available set-up, no external IPs
  - Instance-type db-f1-micro, SSD storage 10GB, back-up size 10GB, highly-available

- Compute engine resources

  Bastion –CentOs7

  Henkilostohallinta –Debian10

  Reskontra –Debian10

  Scheduled availability times: 20hrs/day

  (with Cloud Scheduler)

DISASTER RECOVERY PLANNING – GENERAL CONSIDERATIONS

- **Capacity, Reliability, and avoiding Redundancy:**

  Including only the necessary resources for assuring good service level. Utilising scheduling functions for HR & Finance systems to ensure availability during office hours, while keeping cost down out-of-hours. Maintenance on the compute engines is scheduled every last Sunday of the month.

- **Security**

  All production environments have been produced by adhering to the guidelines and requirements. Resource access has been implemented with the least-privilege principles in mind. Implementing required security policies and components using Google IAP, Bastion engine, Private Google Access. HR & Finance system engines and their respective databases run without external IPs. The compute engines will receive automatic OS updates. These two systems are running isolated from all other business systems. The databases in use are backed up regularly.

  Further implementations: Utilising Cloud Monitoring alerts & Cloud Logging, making use of any free tier allowances. With modest data allowance needs, estimated costs would be relatively small. With further development, the alert policies could have been developed and costs examined thoroughly to produce a reliable alerting & logging policy, which the consultant team considers essential for business continuity and disaster prevention.

- **Compliance**

  Google Cloud complies with certifications such as ISO 27001, SOC 2/3, and PCI DSS 3.0. For the time being, the services and software produced do not comply with The EU General Data Protection Regulation (policy statement & data register would need to be included).

DISASTER RECOVERY PLAN

- A recovery time objective (RTO), which is the maximum acceptable length of time that your application can be offline.
  - HR & Finance systems RTO aim will be a maximum of two (2) working days.
  - Utilising Cloud Monitoring would alert of any issues with e.g. compute engine uptime, traffic spikes or memory capacity issues. Implementing these would need further investigation regarding budget allowances.
  - In the event of loss of function on component function, the resources can be set up again with IaC files provided.

- A recovery point objective (RPO), which is the maximum acceptable length of time during which data might be lost from your application due to a major incident.
  - HR & Finance systems RTO: one (1) day.
    - The databases are backed up daily, seven (7) back-ups available.
    - The databases have a 'highly available' set-up to prevent loss of data and have a quick-access replica in case of failure/loss of service in 1 region.

- Service level agreement on Google Cloud Platform services & products used between 95-99.9%

DISASTER RECOVERY PLAN – SETTING THE SYSTEMS BACK UP

HR & Finance Systems set up instructions in GCP

with files provided:

- IAP TCP forwarding with Bastion
  - encrypted tunnel to forward SSH traffic to VM instance
- To use instance scheduling
  - make sure @compute-system.iam.gserviceaccount has compute intance admin role
- To run
- terraform apply
- Once apply is complete, connect to Bastion instance with SSH. To connect to database first connect to henkilostohallinta or reskontra instance:
  - gcloud compute ssh henkilostohallinta --internal-ip

or

  - gcloud compute ssh reskontra --internal-ip
- To connect to henkilosto or reskontra database:
  - psql -h sql-instance-private-ip -U henkilosto
  - psql -h sql-instance-private-ip -U reskontra

DISASTER RECOVERY TEAMS & RESPONSIBILITIES

- *Disaster Recovery Lead(s):*
- *Disaster Management Team:*

- Emergency Contact Form:

First Name	Last Name	Title	Contact Type	Contact information
Employee F	Employee L	Title	Work	040-1234567
			Mobile	
			Alternate	
			Email	