Building HA DNS Server in Cloud
Overview

1. .MN Registry
2. Consideration for upgrade
3. Running PowerDNS on GCP
.MN Registry
Datacom is .MN Registry since 1996

Two main registrant area:

- Mongolian
- Minositta

Our DNS Registry operator is Afilias, which provides service to .org and .asia tlds
Second Level Domains

- **.MN**
  - **GOV.MN**
    - Government agencies
    - Managed by National Datacenter
  - **EDU.MN**
    - Academic institutions
    - Managed by The Mongolian University of Science and Technology
  - **ORG.MN**
    - Non-profit organizations
    - Managed by Datacom
Internationalized domain name (IDN)

Cyrillic IDN ccTLD
Launched on 2012
Managed by Datacom
IDN Reseller Panel
Our current IDN DNS Setup

- Baremetal servers across 3 ISPs colo
- Bind master/slave
- TSIG and DNSSEC
Issues with our current IDN implementation

- No Registrar & Reseller separation
- No customer side DNSSEC enablement feature
- DNS Record type support currently only A, NS
- Single Point of failure ()
Consideration for DNS upgrade
PowerDNS Server

- Authoritative server for hosting domain names
- Flexible and highly scalable to serve large-scale deployments
- DNSSEC implementation
- Domain Management with ZoneControl
- Account Management
- Geographical load balancing
- Multiple Database Backends including
  - MySQL, LDAP, Lua, GeoIP
The Google network comprised of 100+ points of presence
Global/Regional Load Balancing
Global HTTPS and Regional which is support UDP TCP load balancing distributes traffic across little to no intervention.
Google's global network footprint allows you to serve from the point nearest your users.

Powered by Google's Global Network
Create large compute clusters that benefit from strong & consistent cross-machine bandwidth. Serve your users using the same infrastructure relied on by services like Search, YouTube, and Maps.

Google-Grade Security
Custom-built hardware and software in our data centers create the smallest possible security footprint. We want security to be the reason our customers adopt public cloud.

Continuous Innovation
Innovation in our network over the past 15 years has allowed Google to deliver the world's most trusted services. From raw performance of your applications to workload isolation protecting against distributed denial of service (DDoS) attacks, our customers benefit from continuous innovation.
(Really) Pay for what you use
We bill in minute-level increments so you don't pay for unused computing time, and automatically apply sustained use discounts.

Fast, Easy Provisioning
Quickly deploy large clusters of virtual machines with intuitive tools.

Compliance & Security
All data written to disk in Compute Engine is encrypted on the fly and then transmitted and stored in encrypted form.
Control
It's easy to manage and access your instances through a web Console or a command-line interface. Transfer data to your instance by importing and exporting databases and CSV files.

Easier Migration; No Lock-in
Standard connections and tools such as mysqldump, MySQL Wire Protocol, and JDBC make it easier to migrate onto (or off!) Google Cloud Platform, and avoids lock-in.

Fully managed
No worrying about replication, patch management or database management: we take care of it.

Familiar Infrastructure
Build and deploy for the cloud faster because Cloud SQL offers standard MySQL databases, the most popular open source database in the world. Instances available up to 16GB RAM, 100GB storage.

Security, Availability, Durability
Your data is replicated in many geographic locations as standard, and failover between them is handled automatically. We also manage your backups, making it easy for you to restore when needed, including point-in-time recovery.
Running PowerDNS on Google Cloud Platform
PowerDNS Setup in GCP

Asian Region

Zone A
- Front-End
  - Compute Engine
  - Web App server
- PowerDNS
  - Compute Engine
  - API Server
- CloudSQL /Primary
  - Managed MySQL Backend
  - API Server backend

Zone B
- TCP/UDP Load Balancing with Regional IP
  - ns1-asia1.tld.mn
- PowerDNS Primary
  - Compute Engine
  - Instance Group
- CloudSQL /Read Replica
  - Managed MySQL Backend

Zone C
- Backup Instance Pool
  - Compute Engine
  - Instance Group
- CloudSQL /Failover Replica
  - Managed MySQL Backend
  - API Server backend
AXFR Zone transfer

- Zone transfer VM - to VM communication
- Only via internal network 10.0.0.X/16
- Master sends dns updates only allowed IPs via TSIG
Questions ?