Securing PostgreSQL as a Service

SAP Cloud Platform

Shashank Mohan Jain | Dinesh Kumar

Agenda

- Introduction
- SAP Cloud Platform
  - Architecture
  - PostgreSQL-as-a-Service
- Network Security
- Isolating control plane and data plane
- Infrastructure level security
- Isolation among postgreSQL service instances
- Isolation among processes in a service instance
- Limiting access & resources to processes

SAP CLOUD PLATFORM

An open platform-as-a-service (PaaS) product

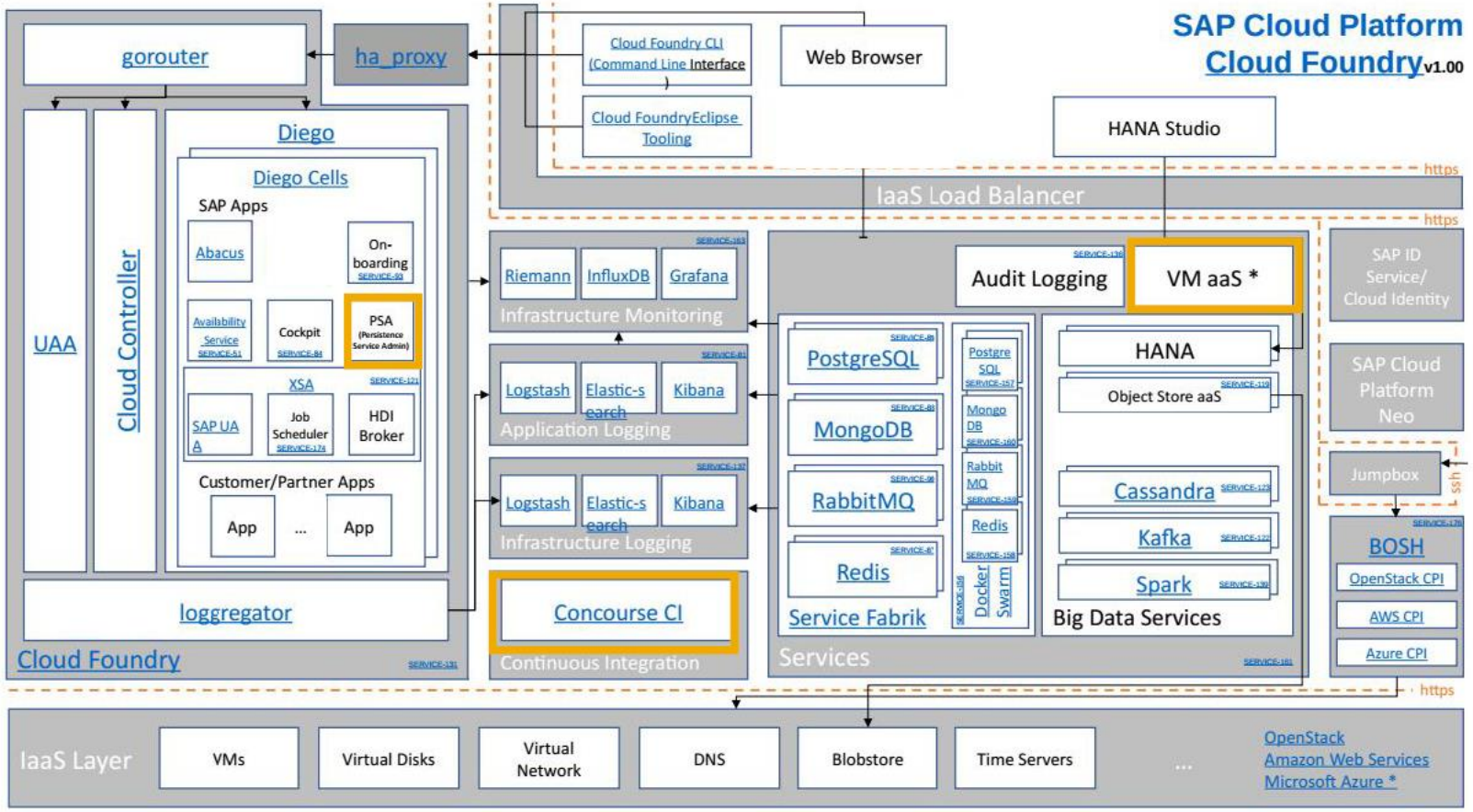
SAP Cloud Platform

Securing PostgreSQL as a Service

SAP CLOUD PLATFORM

- Open platform as a Service based on Cloud Foundry
- Provides core backing services for building applications
- Supports multiple IAAS – Openstack, AWS, Azure & GCP
- Multi-tenancy support

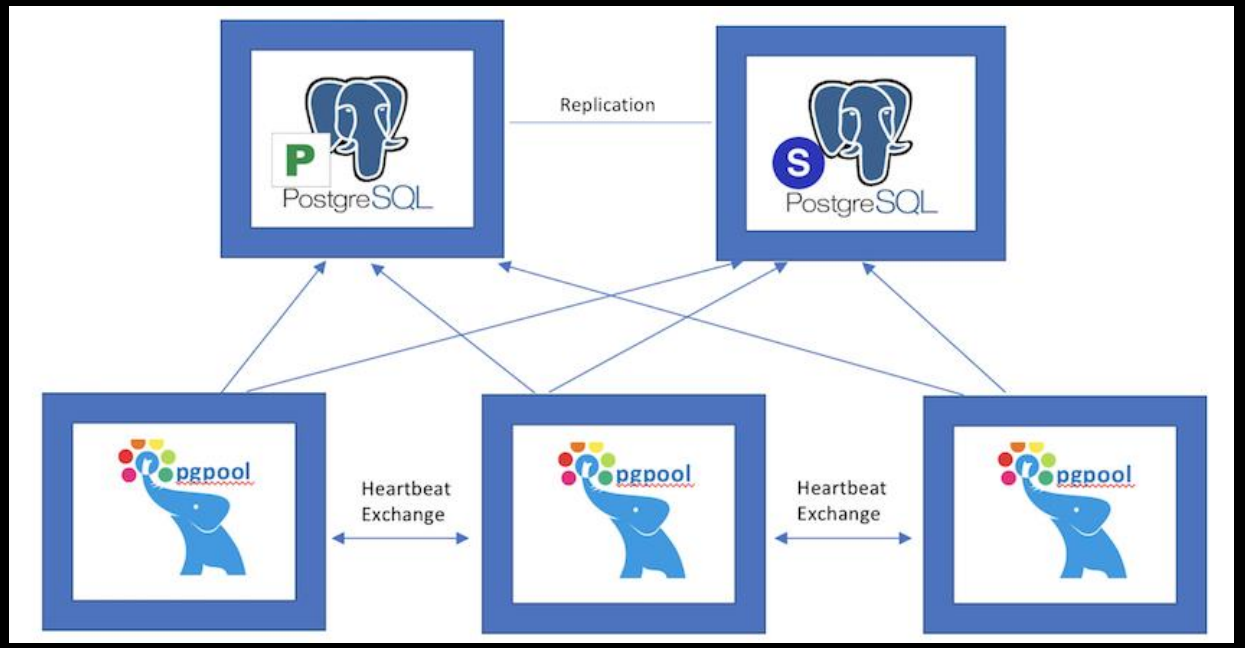
Securing PostgreSQL as a Service



Securing PostgreSQL as a Service

PostgreSQL as a Service

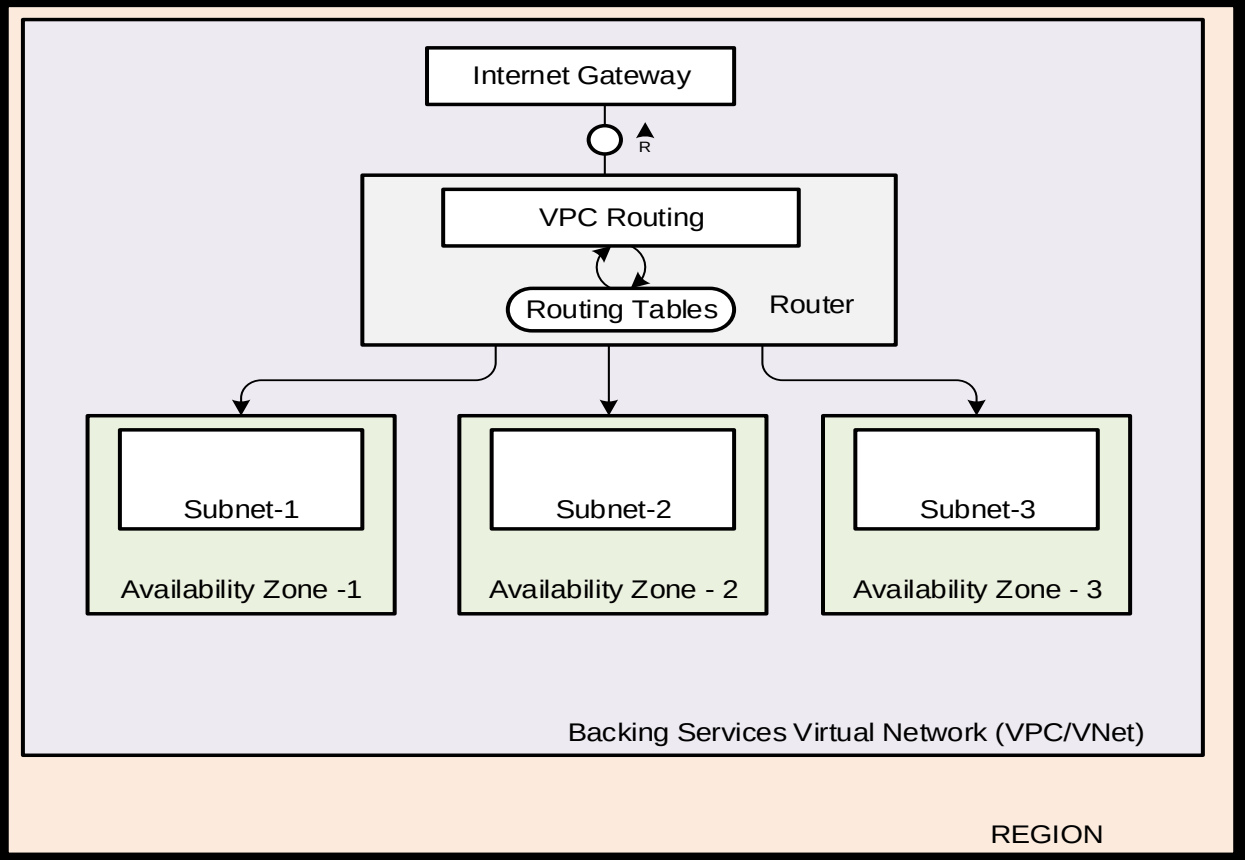
- A service instance comprises of 5 VMs
- Different service plans
- One Primary and one Standby
- 3 pgpool for failover / HA.



NETWORK SECURITY

Securing PostgreSQL as a Service

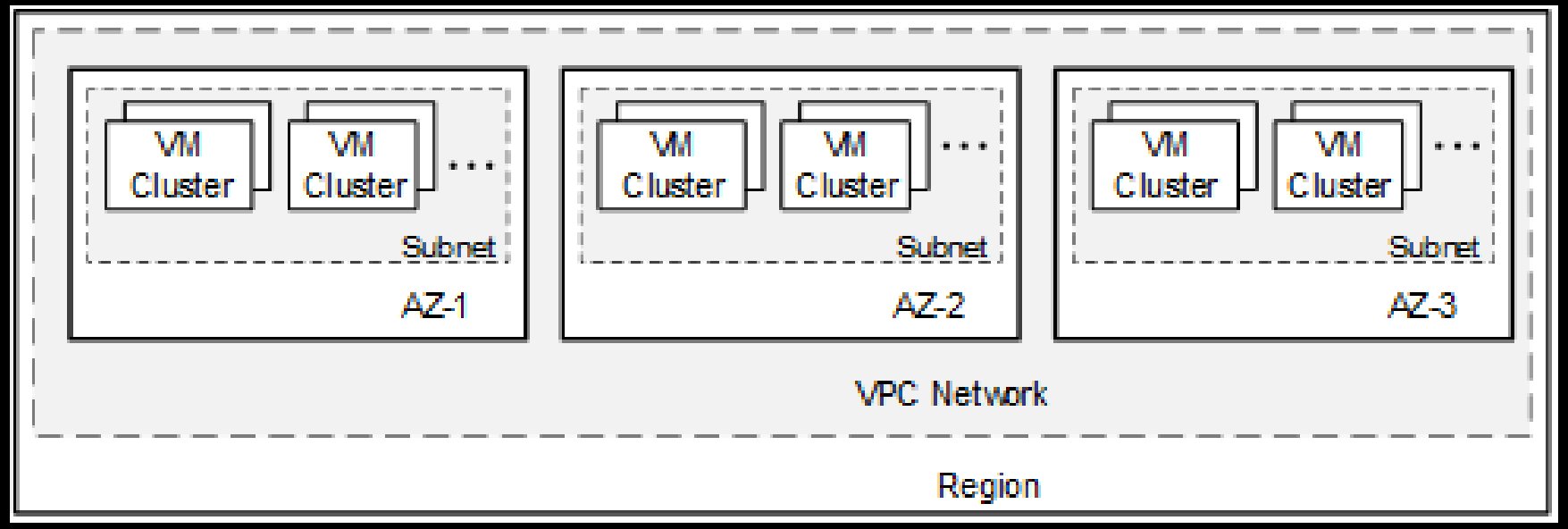
Network Layout



ISOLATING CONTROL PLANE & DATA PLANE

Securing PostgreSQL as a Service

Subnet Layout



INFRASTRUCTURE LEVEL SECURITY

Securing PostgreSQL as a Service

Infrastructure Level Security

- Firewall Rules
- Security Groups
- IP Spoofing prevention at IAAS level

ISOLATION

Among between PostgreSQL instances & within an instance

Securing PostgreSQL as a Service

Isolation between PostgreSQL instances

- Bosh custom plugin – IPTables Manager
- Applies iptable rules to each vm in a service instance
- VMs in one instance cannot communicate with VMs in other instances
- Communication within a service instance is allowed
- ICMP based attacks minimized by allowing required types

Securing PostgreSQL as a Service

Isolation among processes in a service instance

- Each VM runs supporting processes in addition to postgres
- Postgres runs as non-root user with limited access to required resources. (DAC)
- Further isolation using MAC - SELinux

Demo – Isolation

LIMITING ACCESS & RESOURCES TO PROCESSES

SAP Cloud Platform

Securing PostgreSQL as a Service

Limiting access & resources

- Limit the usage using *__getrlimit()__* and *__setrlimit()__* functions
- Processes in the VM are sandboxed using seccomp
- Restricts the usage of system calls to the bare minimum required

Demo – Reverse shell vulnerability

Securing PostgreSQL as a Service

Thank you

SAP Cloud Platform

Shashank Mohan Jain | Dinesh Kumar

© 2018 SAP SE or an SAP affiliate company. All rights reserved.