



Securing PostgreSQL as a Service



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

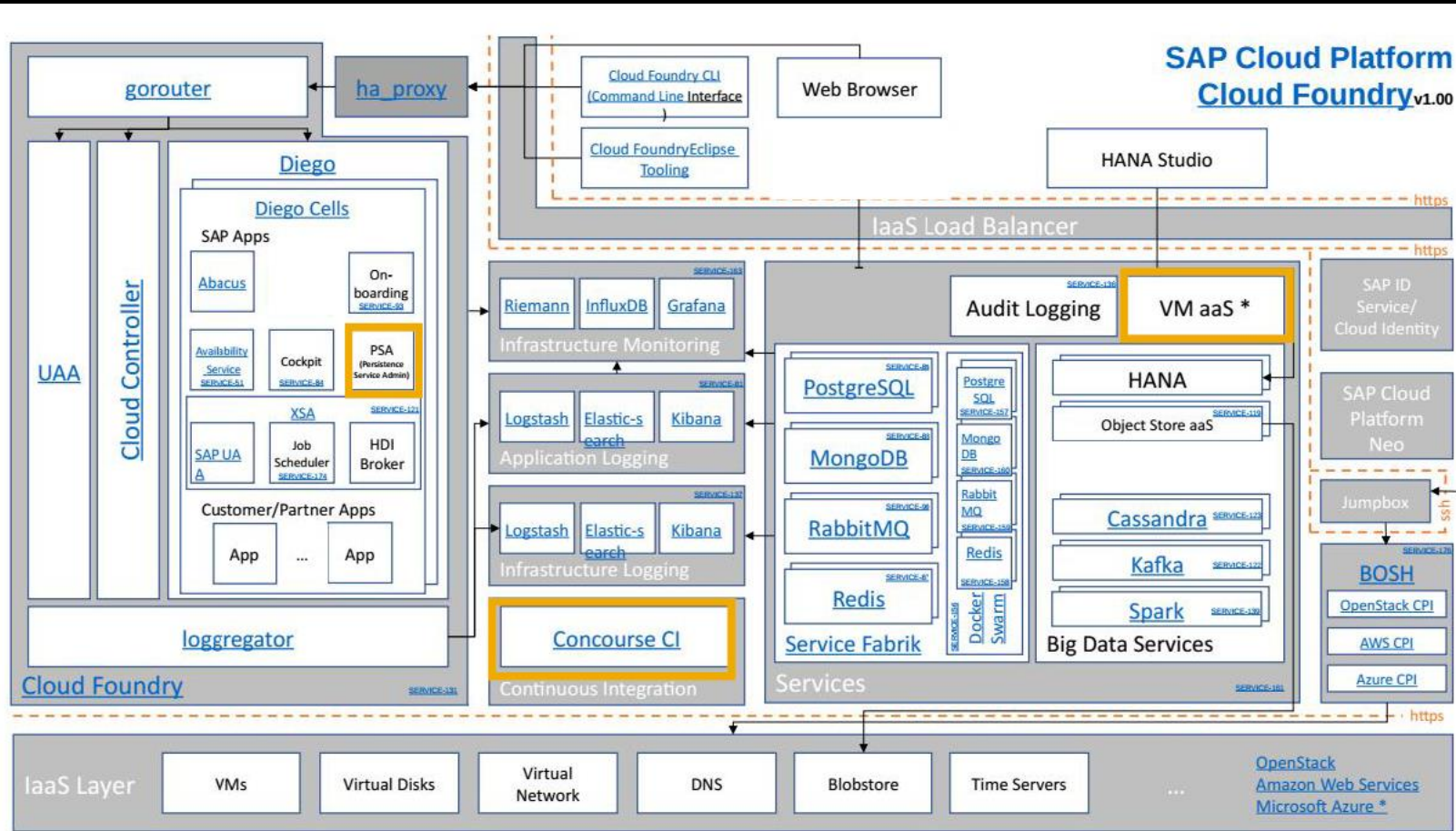
An open platform-as-a-service (PaaS) product

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

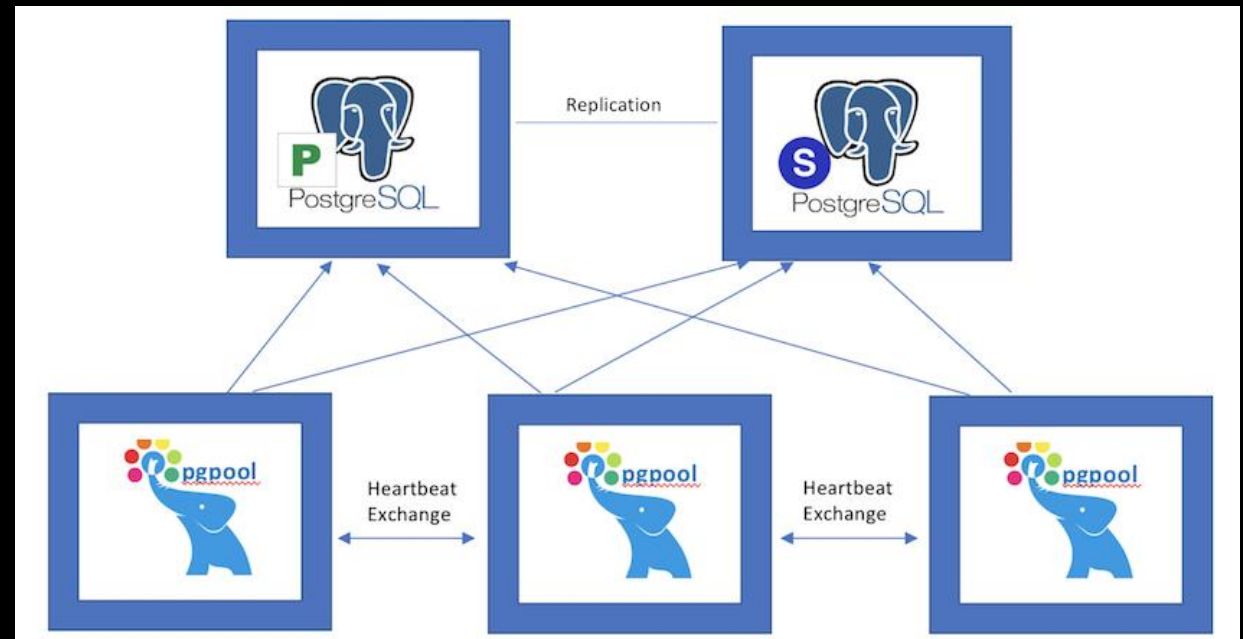
Securing PostgreSQL as a Service



Securing PostgreSQL as a Service

PostgreSQL as a Service

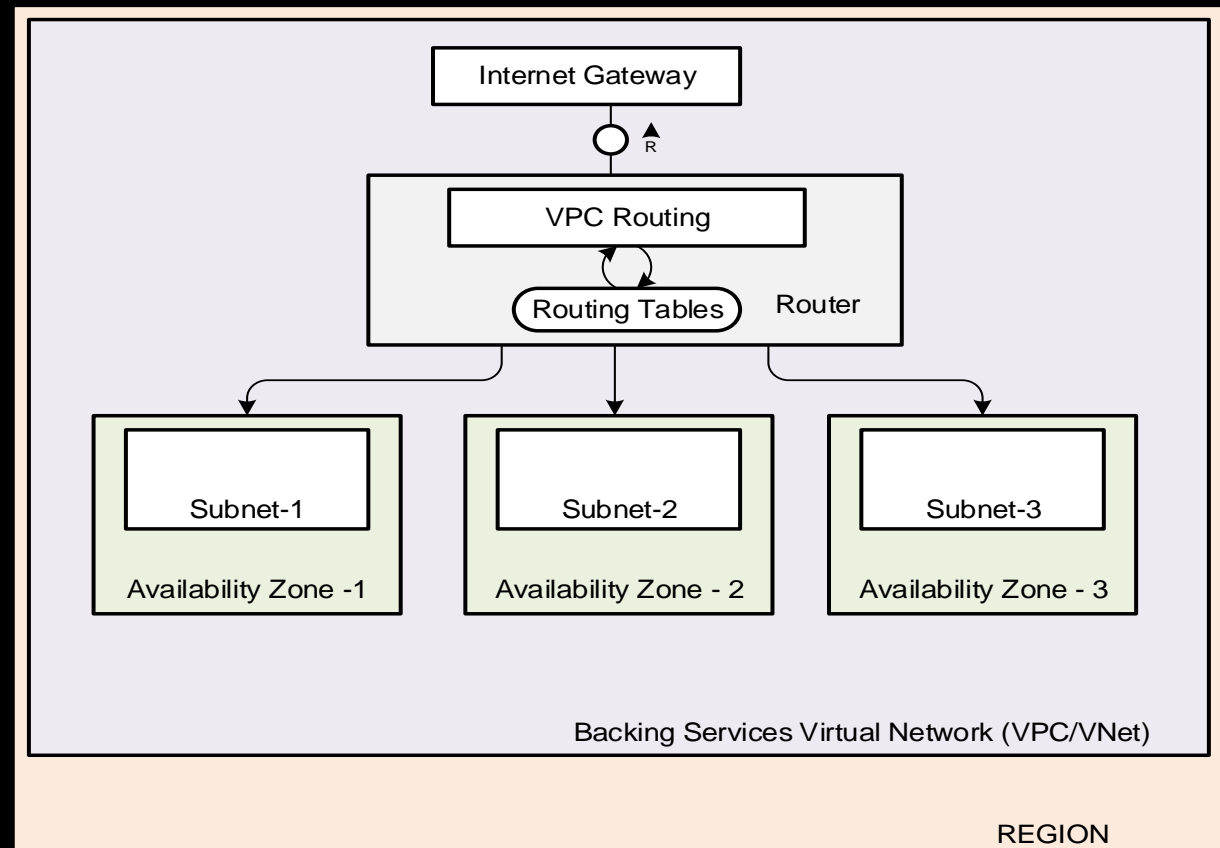
- A service instance comprises of 5 VMs
- Different service plans
- One Primary and one Standby
- 3 pgpool for failover / HA.



NETWORK SECURITY

Securing PostgreSQL as a Service

Network Layout

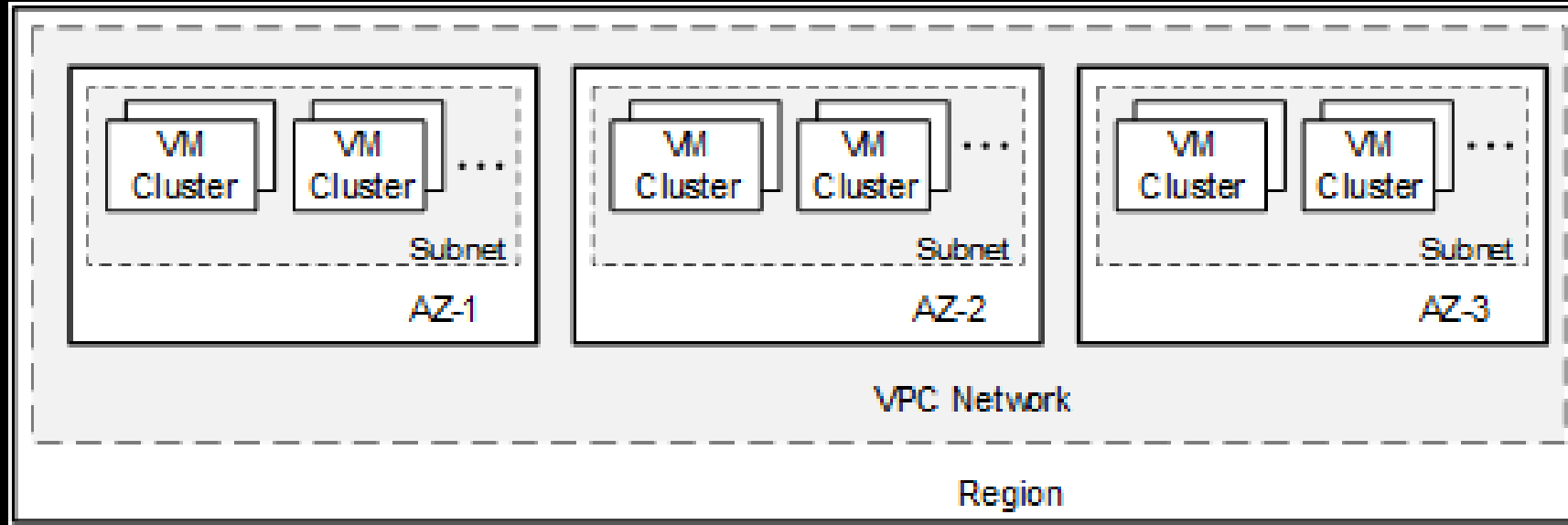




ISOLATING CONTROL PLANE & DATA PLANE

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

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



Shashank Mohan Jain | Dinesh Kumar

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

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. Please see <http://global12.sap.com/corporate-en/legal/copyright/index.epx> for additional trademark information and notices.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.