Swiss Re

Automatisierte Benutzer- und Zugangsverwaltung in DBaaS-Umgebungen

Andreas Geppert, Swiss Re
Karsten Lenz, dbi services

PostgreSQL Conference
13. Mai 2022

Contents

- Introduction
- The Postgres Database Firewall (pg_hba.conf)
- Database Firewall Management in Large Environments
- Design and Implementation

Our vision

We make the world more resilient

About us

Headquartered in Zurich, Switzerland, where we were founded in 1863, the Swiss Re Group operates through a network of around 80 offices globally. Our approximately 13,200 employees provide a wide range of technical expertise, enabling us to develop unique solutions and drive growth.

Swiss Re is organised into two business units (Reinsurance and Corporate Solutions) – each with a distinct strategy and set of objectives – along with our key supporting units and stand-alone brand iptiQ.

Through our combined knowledge, expertise and strong financial position, we act as one Swiss Re to provide the security and foresight clients need, especially during times of uncertainty and transition.

Business units

Swiss Re

Swiss Re Corporate Solutions

Key supporting units

Swiss Re Institute

Swiss Re Foundation

Stand-alone brand

iptiQ

Andreas Geppert

- Architecture and Implementation of Postgres Platforms (DBaaS)
- Oracle-to-Postgres Migration
- Application development with Postgres (OLTP, DWH)
- Postgres teaching for many years (UZH)
- Vice President of Swiss Postgres Users Group
- geppert@acm.org

Introduction

- Postgres supports a very powerful database firewall (pg_hba.conf)
- Who (which user) can access which database when connecting from where, and how do they have to authenticate?
- Particularly useful in large, shared, multi-tenant environments
- Changes to the firewall require manual changes in the pg_hba.conf and a conf reload
- However, management of the firewall must be automated and self-service
- “Automated User- and Access Management in DBaaS Environments”

The Postgres Database Firewall - pg_hba.conf

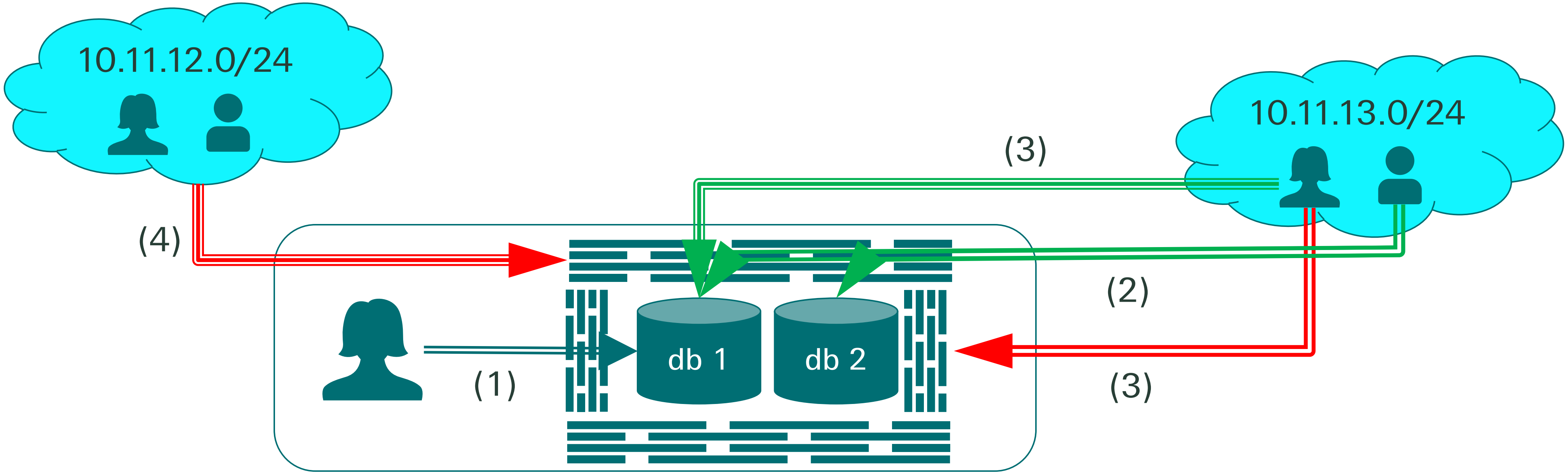
- pg_hba.conf allows one to specify permitted connections
- Format of rules:

```
type  database  user IP-range  authentication-method  options
```

- type: is the connection local or from remote? When remote, is it encrypted?
- database: „all“ databases or a specific one
- user: „all“ users or a specific one
- authentication: how to authenticate the user
  - options: **trust**, reject, **password**, **MD5**, SCRAM-SHA-256, LDAP, ident, peer, ...

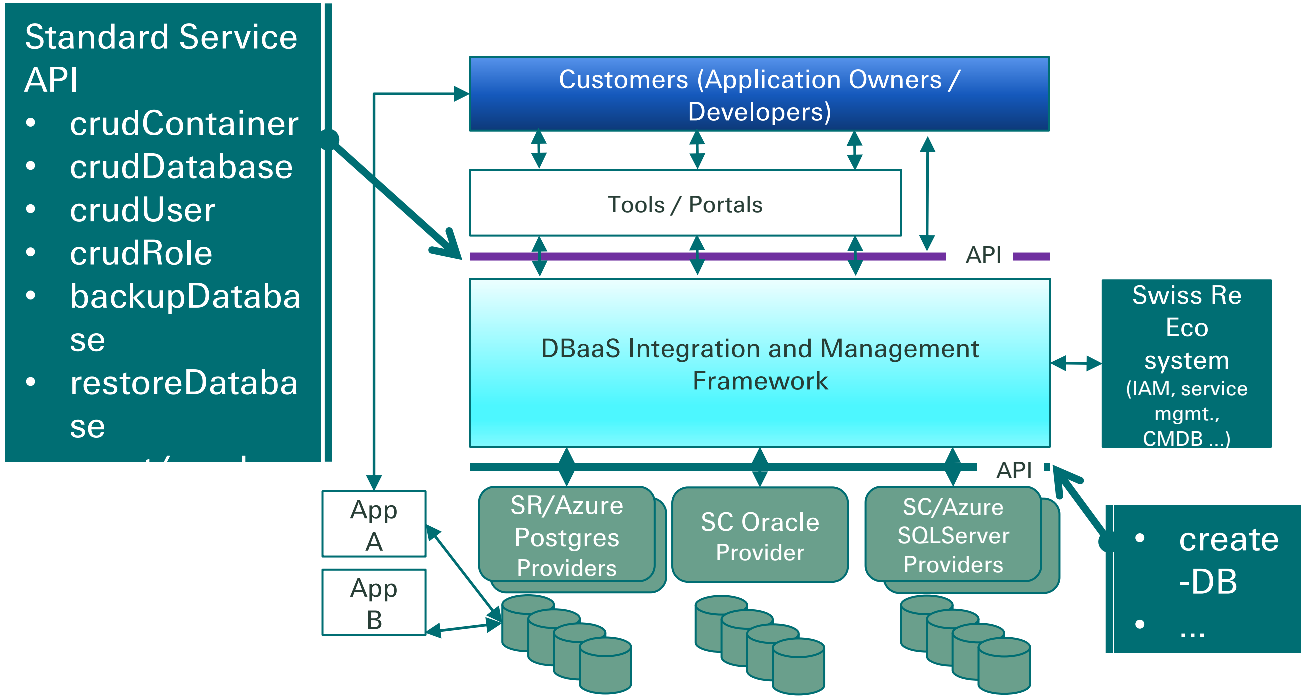
Postgres Database Firewall: Examples

```
local    db1  lucy                          peer
host     all  charly 10.11.13.0/24          ldap            <ldap-options>
hostssl  db1  lucy   10.11.13.0/24          scram-sha-256
host     all  all    0.0.0.0/0              reject
```



Database Firewall Management in Large Environments

- Large companies like Swiss Re have many applications (several thousands), typically with a database component
- Shared infrastructures and services are beneficial from a financial, operational, and security view
- Firewall management must be automated and self-service
- Local firewalls are ideally centrally managed



Standard Service API
- crudContainer
- crudDatabase
- crudUser
- crudRole
- backupDatabase
- restoreDatabase

- create-DB
- ...

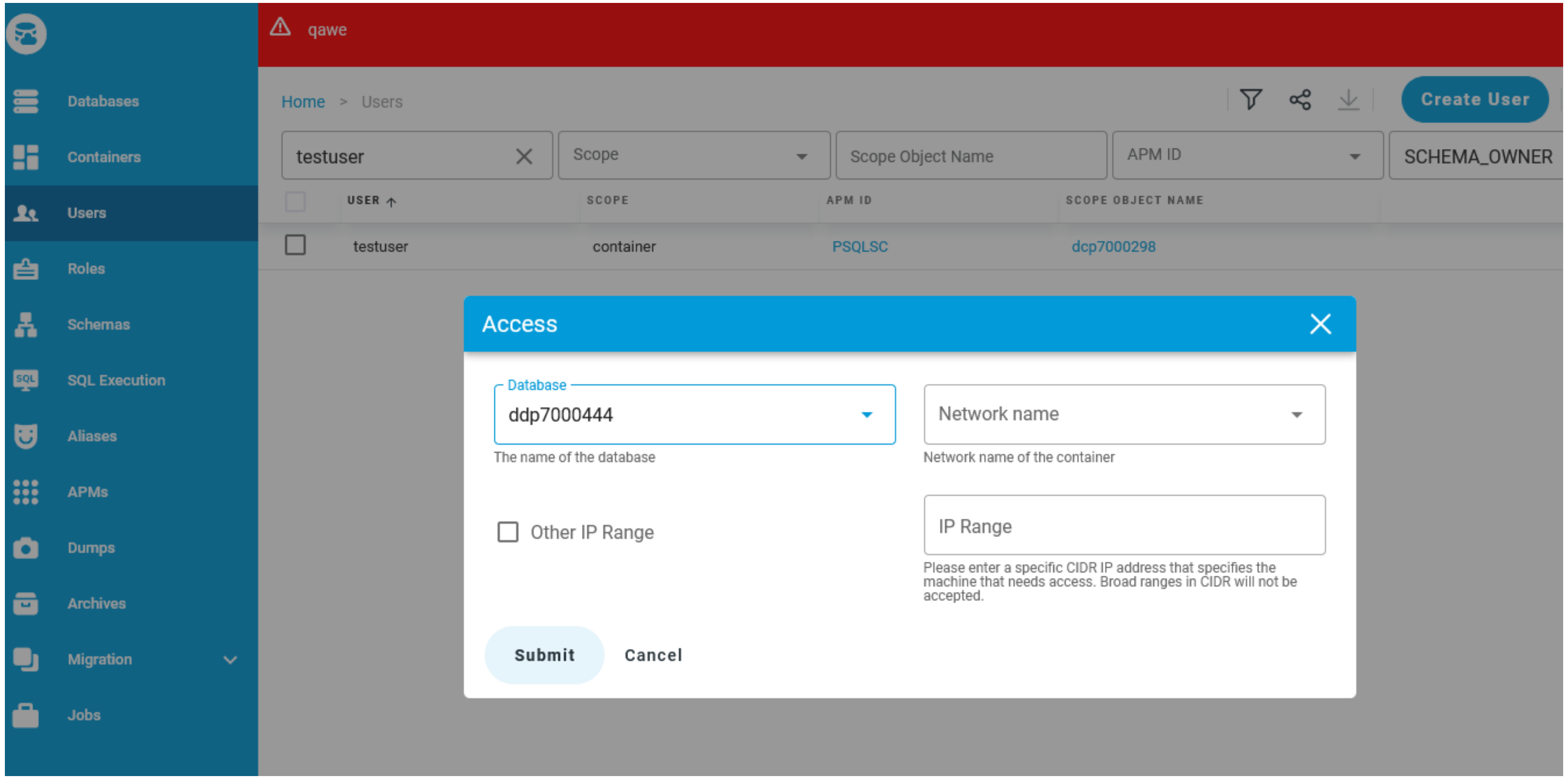
Customers (Application Owners / Developers)
Tools / Portals
API
DBaaS Integration and Management Framework
Swiss Re Eco system (IAM, service mgmt., CMDB ...)
API
App A
App B
SR/Azure Postgres Providers
SC Oracle Provider
SC/Azure SQLServer Providers

Database Firewall Management in Large Environments: Requirements

- Add and remove firewall rules
- Different levels of sharing vs separation must be possible
- Tenants need to be shielded from each other
- Governance (e.g., change management, reporting, movers and leavers)
- Integration with Enterprise Identity and Access Management
- Encryption needs to be enforced by default
- Network zones concept (if present) needs to be implemented
- Standards (e.g. encryption, no MD5) and sanity checks (e.g., users actually exist)
- Service owner needs to keep track of firewall rules (possibly also historically)

Database Firewall Management in DBaaS
Some Stats

- # Postgres clusters: 82 ↗
- # Postgres databases: 370 ↗
- # Postgres users: 1350 ↗
- # Connectivity rules: 2500 ↗



⚠ qawe

testuser	Scope	Scope Object Name	APM ID	SCHEMA_OWNER

□	USER ↑	SCOPE	APM ID	SCOPE OBJECT NAME
□	testuser	container	PSQLSC	dcp7000298

Access

Database: ddp7000444

The name of the database

Network name

Network name of the container

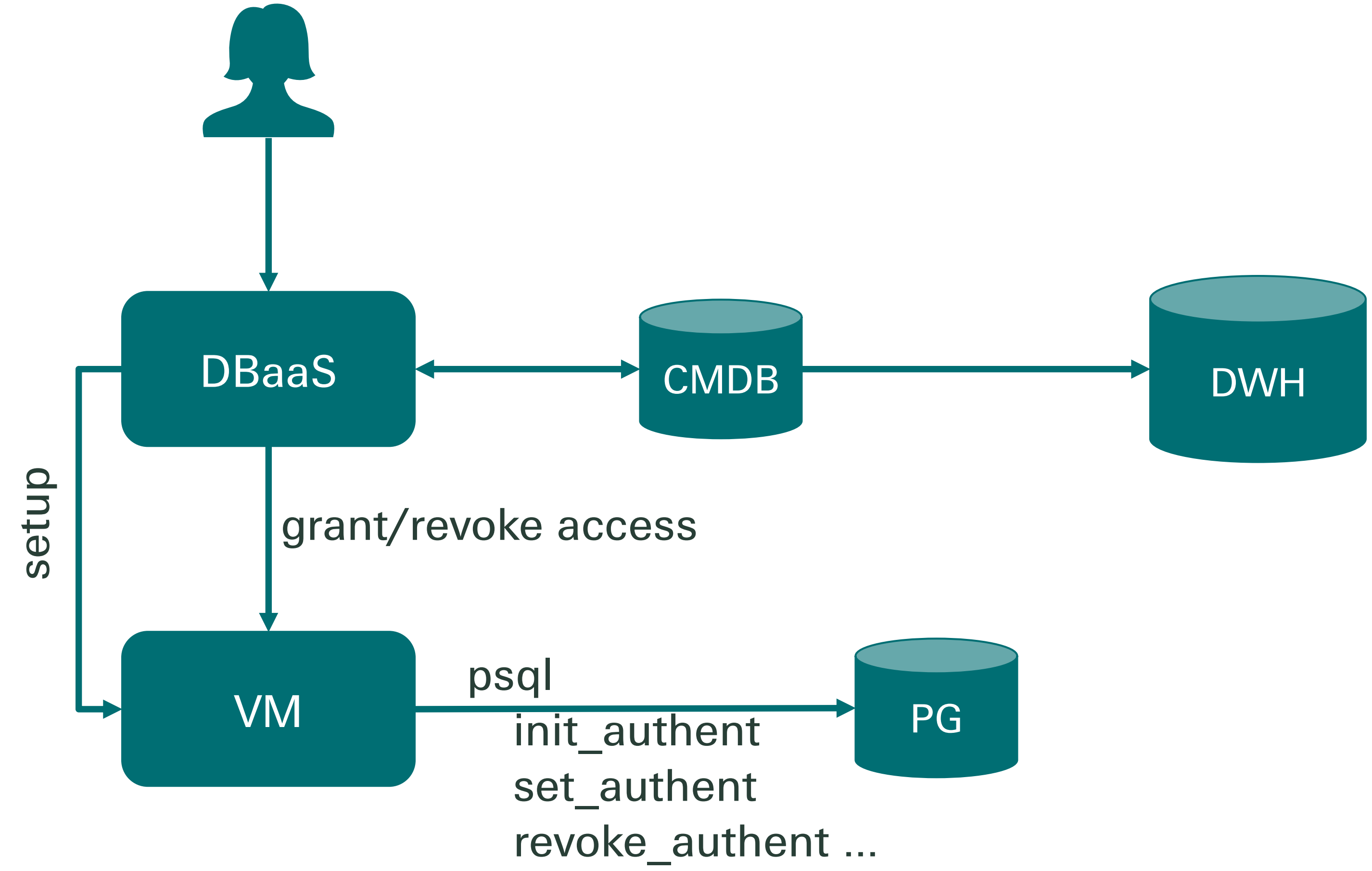
□ Other IP Range

IP Range

Please enter a specific CIDR IP address that specifies the machine that needs access. Broad ranges in CIDR will not be accepted.

Submit Cancel

Database Firewall Management: Architecture



Part 2: See here

Legal notice

The information and opinions contained in the presentation are provided as at the date of the presentation and may change. Although the information used was taken from reliable sources, Swiss Re does not accept any responsibility for its accuracy or comprehensiveness or its updating. All liability for the accuracy and completeness of the information or for any damage or loss resulting from its use is expressly excluded.