GMO INTERNET

OpenStack Designateで作るDNSaaS

DNS Summer Days 2015

2015/7/24

GMOインターネット株式会社

永井祐弥

GMO INTERNET

自己紹介

名前

永井　祐弥（ながい　ゆうや）

所属

GMOインターネット株式会社

システム本部 第1サービス開発部

担当

2012年にGMOインターネットへ入社。お名前.com、ConoHaのDNSや、GMOインターネットグループ会社でレジストリのシステムのDNSなど、DNS関連の開発、運用を担当

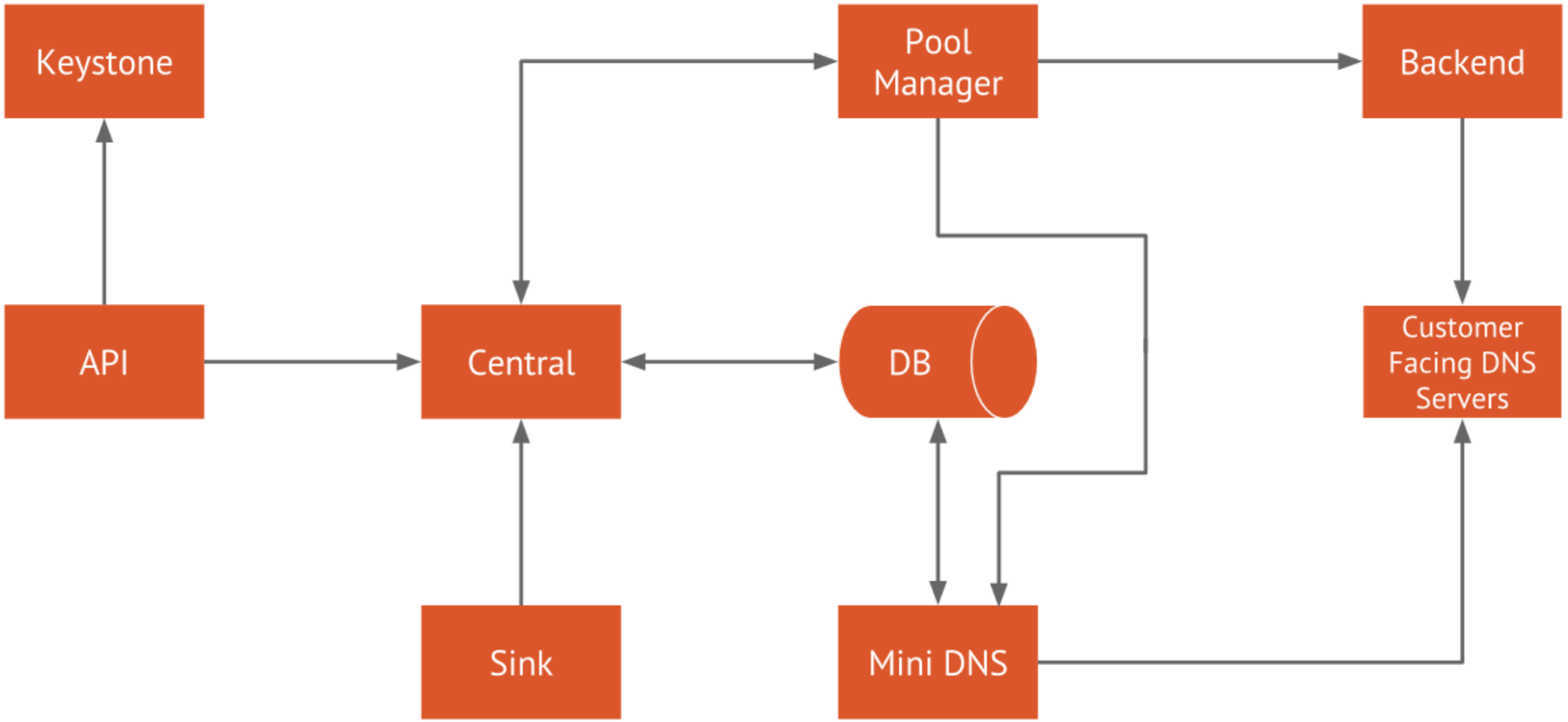
OpenStack とは？

- オープンソースで開発されているクラウド環境構築用のコンポーネントの集まりです
- IaaS (Infrastructure as a Servie) と呼ばれるサーバ、ネットワーク、ストレージを提供するための環境を構築することが出来ます
- 最近ではPaaS (Platform as a Service) のコンポーネントも開発されており、IaaS上で稼働は勿論、単体のアプリケーションとしても利用することが出来ます

OpenStack Designateとは？

- DNSレコードをAPIで操作するためのコンポーネント
- 正引き（A/AAAA）、逆引き（PTR）、メール（MX/TXT/SPF）用等のDNSレコードが登録可能です
- Designateを単体で使用することはもちろん、認証連携すると各ドメイン名毎の利用者をアクセスコントロールすることが出来ます
- DesignateはDNSレコードのデータ管理のみ行うため、実際のDNSサーバはバックエンドとしてBIND9/PowerDNS/NSD4等を利用します（選択可）

Designate構成イメージ



DESIGNATE
DNS FOR OPENSTACK

Designateのインストール

```
$ git clone git://github.com/openstack/designate designate
$ cd designate
$ virtualenv --no-site-packages .venv
$ . .venv/bin/activate
$ pip install -r requirements.txt -r test-requirements.txt
$ python setup.py develop
```

- 公式のドキュメントが充実しています
  http://docs.openstack.org/developer/designate
- 動かすだけならとても簡単◎
- 古いDesignateの場合、Pythonライブラリのバージョンを指定しないと動きません（特にOpenStackライブラリ関連）

Designate APIの実行例

```
$ curl -X POST -H “Content-type: application/json” –d ¥
 ‘{ "name": "example.tokyo.",
    "ttl": 3600,
    "email": "admin@example.tokyo" }' ¥
 http://localhost:9001/v1/domains
```

- ドメイン名「example.tokyo」の作成の例です
- Curl/wgetコマンド等で簡単に実行出来ます
- REST API はUI仕様がシンプルに設計されており、わかりやすいです
- データの送受信はJSON形式で扱います

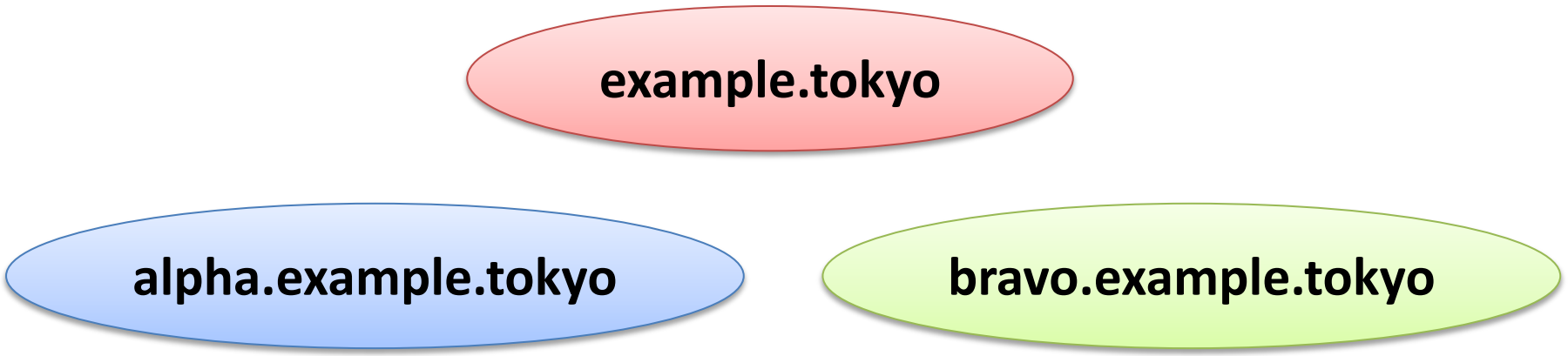
Designateでできる事（機能）

- 管理者
  - ネームサーバの登録（オリジンのNS）
  - 登録数制限（ドメイン数、RRsets/RRecord数）
  - TLD制限（.com/.net/.org/.jp/.tokyo等）
  - ブラックリスト（正規表現指定）
  - その他（レポート、診断、Pool等）
- 利用者
  - ドメイン名
  - DNSレコード（A/AAAA/MX/TXT/CNAME/NS/SRV/PTR/SPF/SSHFP）

Designateでできる事（仕様）

- 登録データのバリデーション
  - 結構細かい所までチェック
  - TXTレコードは255バイトまで
  - SOAレコードは直接編集不可
- TLDは作成不可
  - SLDは作成可能（例：co.jp）
- 認証
  - KeyStone（OpenStack Identity）と連携することで、テナントID（所有者）毎にドメイン名を管理
  - 認証無しの場合、登録されている全てのドメイン名にアクセス可能

Designateでできる事（仕様）



- テナントAがalphaを作成した場合、他のテナントはalphaの祖先ドメイン名、子孫ドメイン名を作成出来ません
- テナントBがbravoを作成した場合、全てのテナントは親ドメイン名を作成出来ません

DNSaaSで変わる事

- IaaS/PaaS連携
  - LB/サーバを利用する
    - ✓ホスト名（A/AAAA）
    - ✓逆引き名（PTR）
  - メールを利用する
    - ✓ホスト名（MX/A/AAA）
    - ✓SPF/DKIM（TXT）
  - 外部サービスを利用する
    - ✓ホスト名（CNAME）

DNSaaSで変わる事

- DNSレコードの自動更新
  - TTLの短縮化
    - ✓キャッシュの非効率化
  - IoT（Internet of Things）
    - ✓色んなものにDNSが使われたり
- DNSインフラの希薄化
  - 薄い空気がより薄く
  - でも責任は、、、

Designate使ってます！

- DNSaaSとして
  - ConoHa
    - ✓GSLB機能の追加
    - ✓バリデーションの強化
- 社内DNSインフラとして
  - プライベートドメイン名の管理
  - 管理者と、利用者の分離
    - ✓オペミスの軽減
    - ✓カオスなゾーンファイルの撲滅

Designateで苦労した所

- API
  - 馴染みが薄いと最初は慣れない
  - プログラマは飲み込みが早い
  - ツール化して効率化UP
- 権威とキャッシュの住み分け
  - 社内DNSインフラ（BIND）の権威/キャッシュ同居からの脱却
- Designateの開発スピード
  - ほぼ毎週ペースで新規コードがコミットされる
  - インストールするPythonライブラリのバージョンに注意

すべての人にインターネット