BIGLOBE

Akamai AuthServe (nominum) 導入した

2022/6/24
DNS Summer Day 2022
川口 永一郎

自己紹介

名前：川口 永一郎

会社：BIGLOBE（3年目）

所属：基盤本部 ネットワーク技術部

業務：DNS基盤、IPv4 over IPv6基盤

Agenda

- 導入した理由
- 導入前/後の権威DNSの構成
- BINDとの連携作業
- つまったこと/解消方法
- 今後の課題

導入した理由

- 権威DNSはBINDでしか運用してなかった
  - キャッシュはBIND/Unbound
  - 権威DNSのアプリケーション冗長化が長年の課題
- BIND以外の候補（4つ）
  - Akamai AuthServe
  - Infoblox
  - BIG-IP DNS
  - NSD

導入した理由

- 権威DNSはBINDでしか運用してなかった
  - キャッシュはBIND/Unbound
  - 権威DNSのアプリケーション冗長化が長年の課題
- BIND以外の候補
  - Akamai AuthServe
  - Infoblox
  - BIG-IP DNS
  - NSD

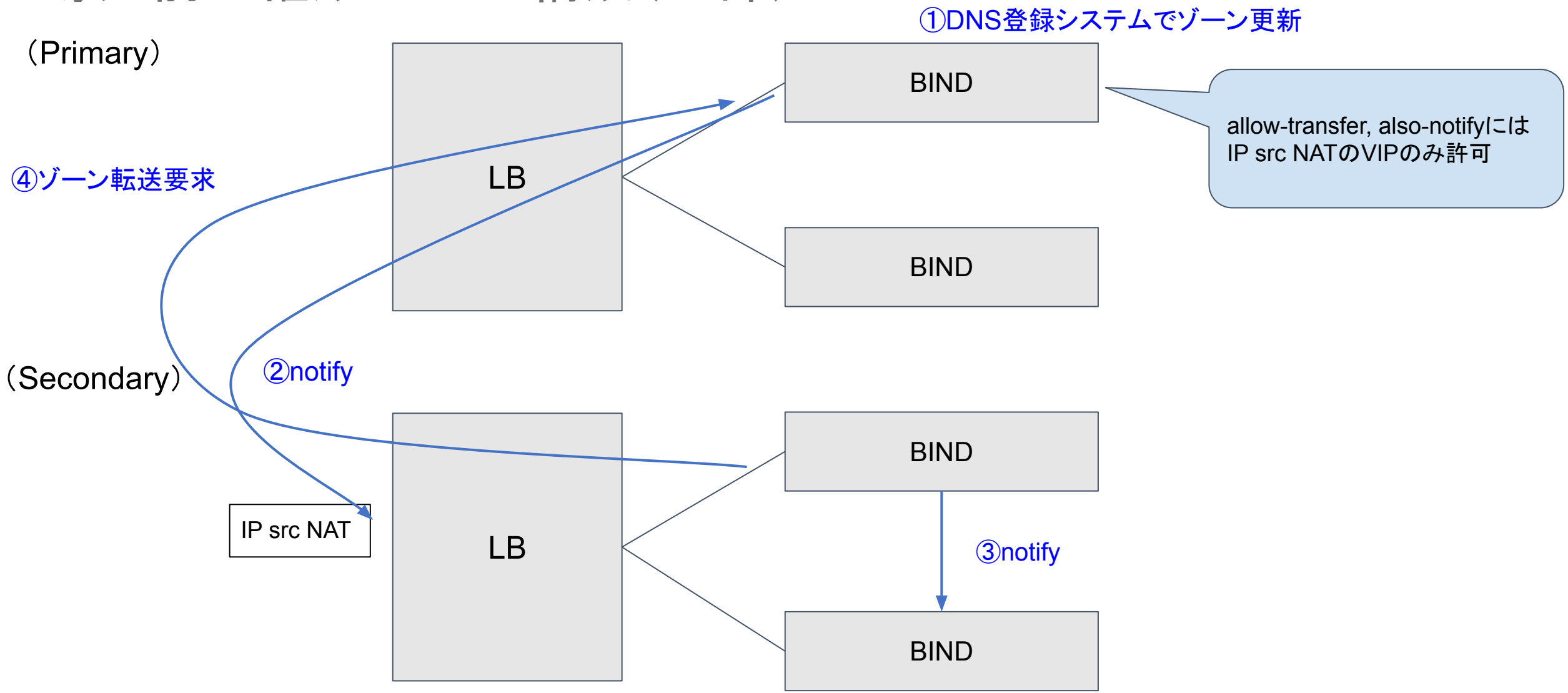
InfobloxとBIG-IP DNSは権威DNS機能にBINDが使用されているため、完全なアプリケーション冗長がとれない

導入した理由

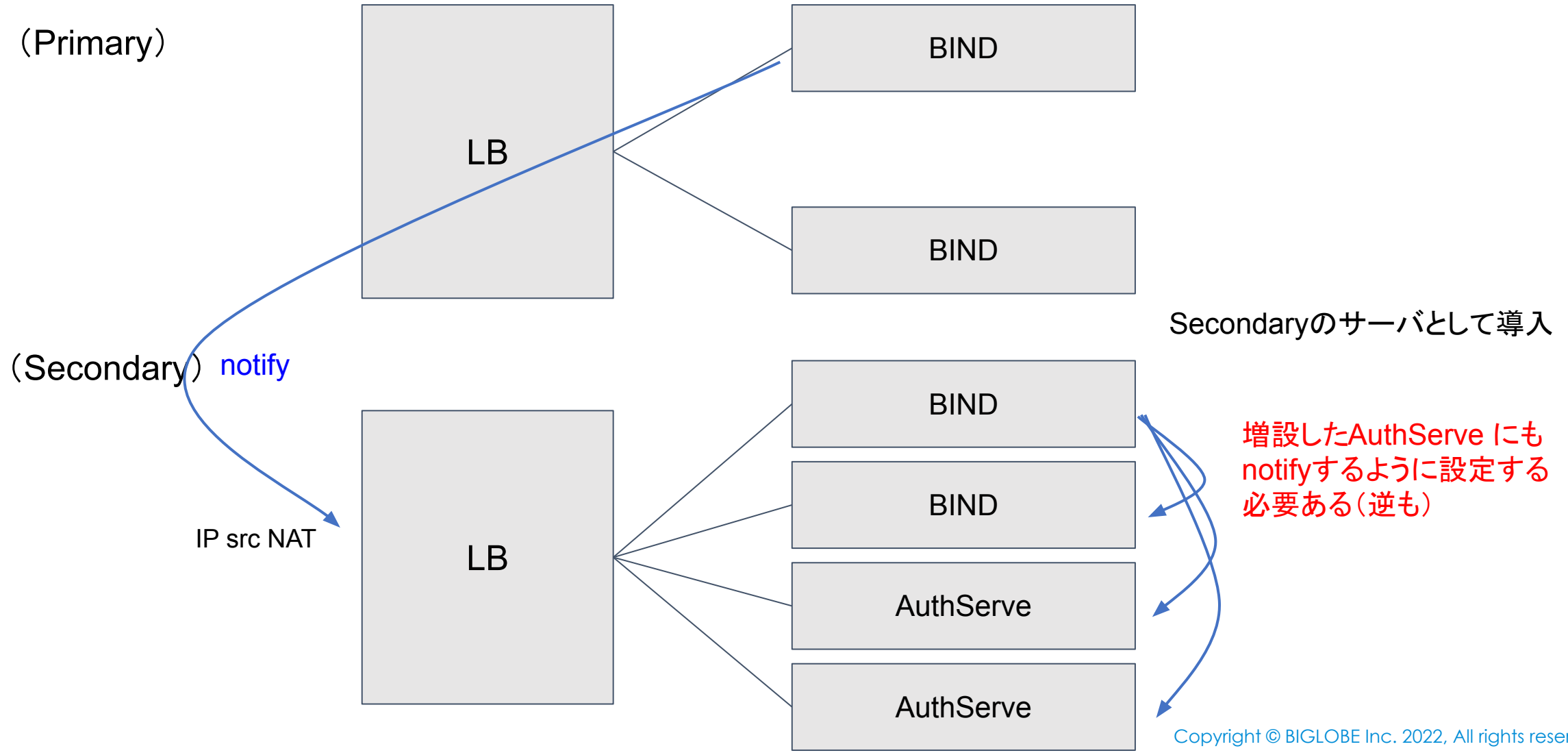
- 権威DNSはBINDでしか運用してなかった
  - キャッシュはBIND/Unbound
  - 権威DNSのアプリケーション冗長化が長年の課題
- BIND以外の候補
  - Akamai AuthServe
  - Infoblox
  - BIG-IP DNS
  - NSD

  NSDはOSSだがノウハウなし → 保守運用の委託を想定
  コスト的にAuthServeを選ぶことになった

導入前の権威DNSの構成（一部）



導入後の権威DNSの構成（一部）



マニュアル読みながらコンフィグ作成してみるかと思ったら

- AuthServeにはコンフィグ（named.confみたいな）がなくて、
  基本的にコマンドで設定する
- nom-tellコマンドとか使ってゾーン設定できる
- ans_import というBINDのコンフィグを読み込ませるコマンドが
  ある ※プロセス落とさないと読み込めない
- 今回AuthServeにゾーン転送設定したいゾーン数が1000以上あったの
  で、shellスクリプトで設定した

BINDとの連携作業

1. LBのIPsrcNATの設定にAuthServeのIPアドレスを加える

2. 予めゾーン設定しておいたAuthServeがPrimaryのBINDに転送要求して、全ゾーンの転送が完了することを確認

3. DNS登録システムでダミーゾーンを登録し、SecondaryのBINDからnotifyを受け取ってゾーン転送できることを確認

BINDとの連携作業

1. LBのIPsrcNATの設定にAuthServeのIPアドレスを加える ☑️ **成功**
2. 予めゾーン設定しておいたAuthServeがPrimaryのBINDに転送要求して、全ゾーンの転送が完了することを確認 ☑️ **成功**
3. DNS登録システムでダミーゾーンを登録し、SecondaryのBINDからnotifyを受け取ってゾーン転送できることを確認 ☑️ **失敗**

BINDのログ

- named[**]: zone ******.com/IN: refused notify from non-master: {AuthServeのIPアドレス}#**

notifyが失敗した原因

- BINDとAuthServeの設定が足りておらず、notifyが許可されなかった
  - Secondary BIND

```
zone "*******.jp" {
        type slave;
        file "slave/*******.jp";
        masters {
                primary BINDのIPアドレス; secondary BINDのIPアドレス;
        };
        allow-query { any; };
};
```

AuthServeのサーバのIPアドレスを追加する必要あり

  - AuthServe
    - allow-notifyにsecondaryのDNSサーバのIPアドレスを指定する必要があった

also-notify　{secondary BIND の IPアドレス, AuthServe の IPアドレス }
allow-notify　{secondary BIND の IPアドレス, AuthServe の IPアドレス}

以下の設定で作業リトライ

購入してから評価、設定確認など時間がかかったが、
AuthServeのサービスインが無事完了！

課題も残っている

- AuthServeに移行できたゾーンはまだ一部分
  - 今回移行したのは重要ドメイン（自営のドメイン）があるゾーン
  - 他のゾーンの移行も進める必要がある

- DNS登録システムとの連携
  - APIで権威DNSにドメインを登録できるシステム
  - BIND前提のシステムとなっている
    - AuthServeは直接コマンドで登録する必要がある
  - 2つDNS登録システムがある
    - 全てのゾーンを1つのDNS登録システムで管理できるようにしたい