パブリッククラウドを利用した権威 / キャッシュDNSサーバーの構築運用

2024/06/21 DNS Summer Day 2024

BBSakura Networks株式会社 藤井勇太

はじめに

- ISPとNaaSのサービスをはじめたので、
  スモールスタートでキャッシュDNSサーバーと権威DNSサーバーが必要になりました
- 人もそんなにいない
- お金もそこまで贅沢に使えない
- オンプレ、クラウド、選択肢はさまざま
- あなたならどう構築する、というお話です

自己紹介

名前：藤井勇太

所属：BBSakura Networks株式会社(BBIX株式会社兼務)

お仕事：ネットワークエンジニア

OCXというNaaSや

OCX光というISP(またはそのAS運用)をしています

趣味：写真(自社のHPに私の写真が使われていて嬉しい)

会社紹介

BBSakura Networks株式会社

- BBIX株式会社とさくらインターネット株式会社の合弁会社
- 開発しているもの
  - OCX (Open Connectivity eXchange)(NaaS)
  - OCX光(ISPサービス)
  - さくらのセキュアモバイルコネクト(モバイルネットワークサービス)
  - BBIXから委託されているシステム

OCX/OCX光とは


24/365監視
DC拠点
クラウド
サービス
仮想マシン
Internet
ウェブポータル
Open Connectivity eXchange
OCX光 インターネット
OCX光 プライベート
OCXアクセスライン

本題(再掲)

- ISPとNaaSのサービスをはじめたので、
  スモールスタートでキャッシュDNSサーバーと
  権威DNSサーバーが必要になりました
- ひともそんなにいない
- お金もそこまで贅沢に使えない
- オンプレ、クラウド、選択肢はさまざま
- どうつくっていくか

権威とキャッシュDNSサーバー

- 権威DNSサーバー
  - 用途としては逆引きゾーンなど
  - Route53、Azure DNSなど他にも様々マネージド・サービスが多い

こちらは、そのまま乗っかったほうが良さそう

権威とキャッシュDNSサーバー

キャッシュDNSサーバー(フルサービスリゾルバー)

- お客様のクエリをAS内で捌く
- Route 53 Resolverがあるがクエリ数に制限などあり条件に合わない
- なかなか選択肢がない

こちらは、作るしかなさそう

クラウド上での構築になりました

- 理由
  - 初期コストが少なく、スモールスタートにあっていた
  - せっかくNaaSとしてOCXを開発しているので、閉域接続した先のクラウド上で構築しようとなった
  - またキャッシュDNSサーバーは、クラウド上に構築してBGPでAnycastのようにインターネット的な運用したらおもしろそうだよねという声も
- 他にも
  - 専用アプライアンスでの構成は金額感が合わなかった
  - オンプレの機器を運用するのは少し人員的にハードルが高かった

権威DNSサーバー検討案

- octoDNSを利用して、マルチクラウドのマネージド権威DNSサーバーにデプロイ
- octoDNSとは
  - DNS as code - Tools for managing DNS across multiple providers
  - https://github.com/octodns/octodns

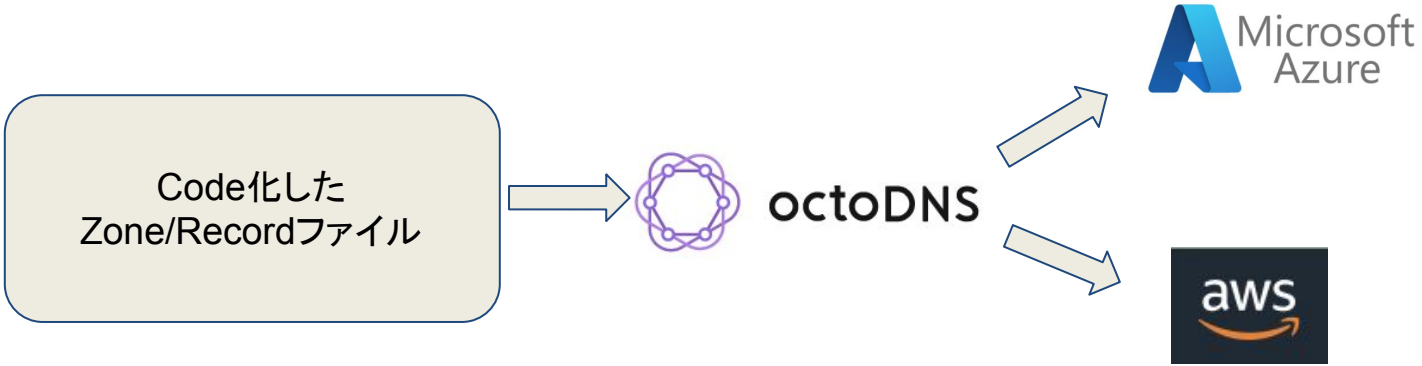
octoDNS

権威DNSサーバー構築/運用

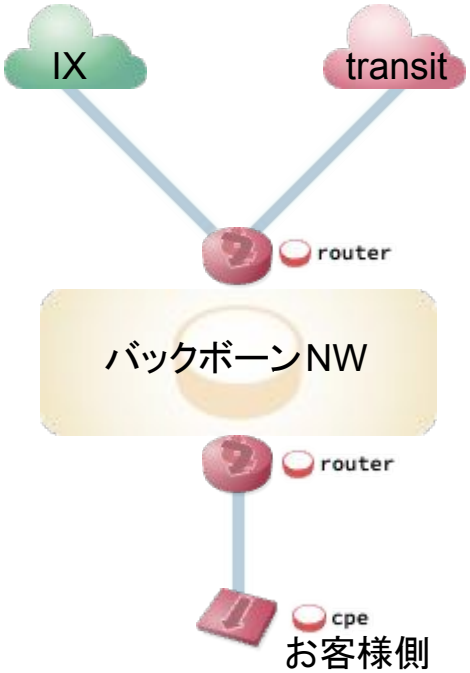
ツールを教えたら同僚がぱぱっとデプロイしてくれた

JPNICへの逆引きのNSレコードの登録は手作業

運用に関しても、今のところ時間をとられることはない

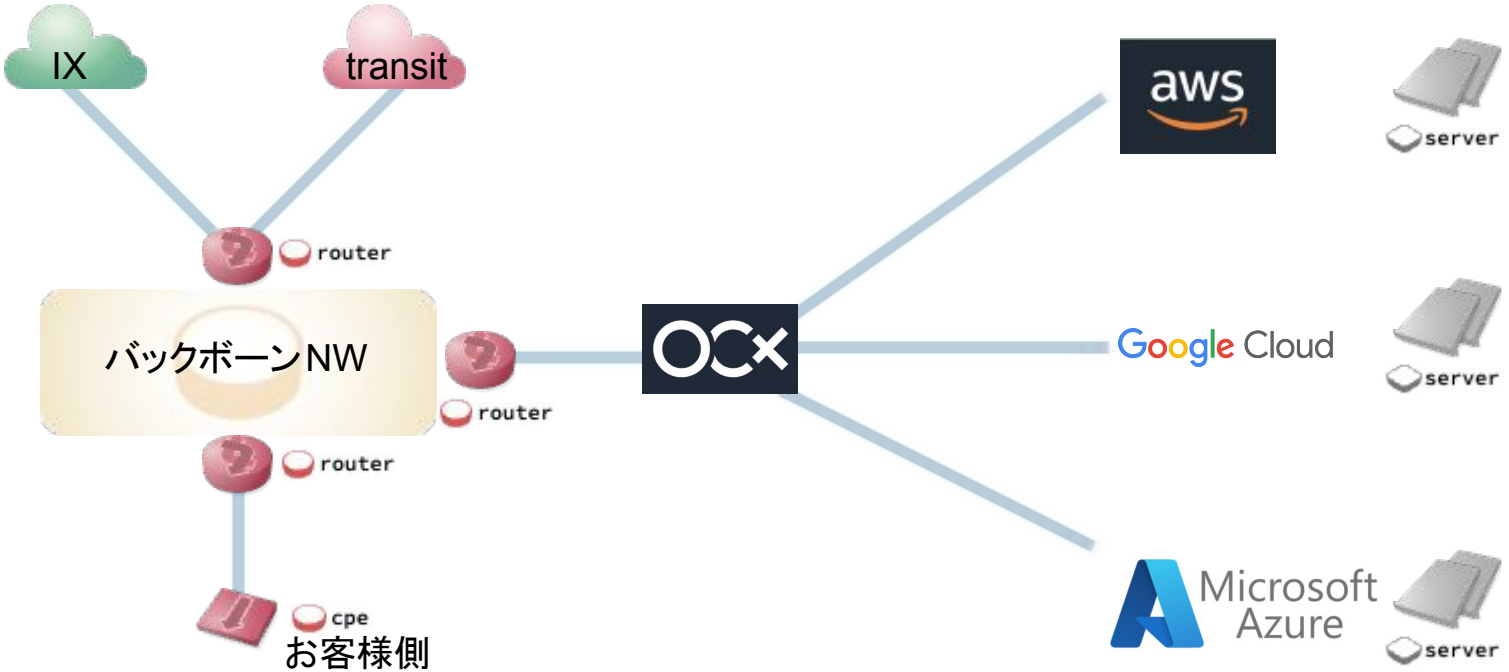


キャッシュDNSサーバー検討案



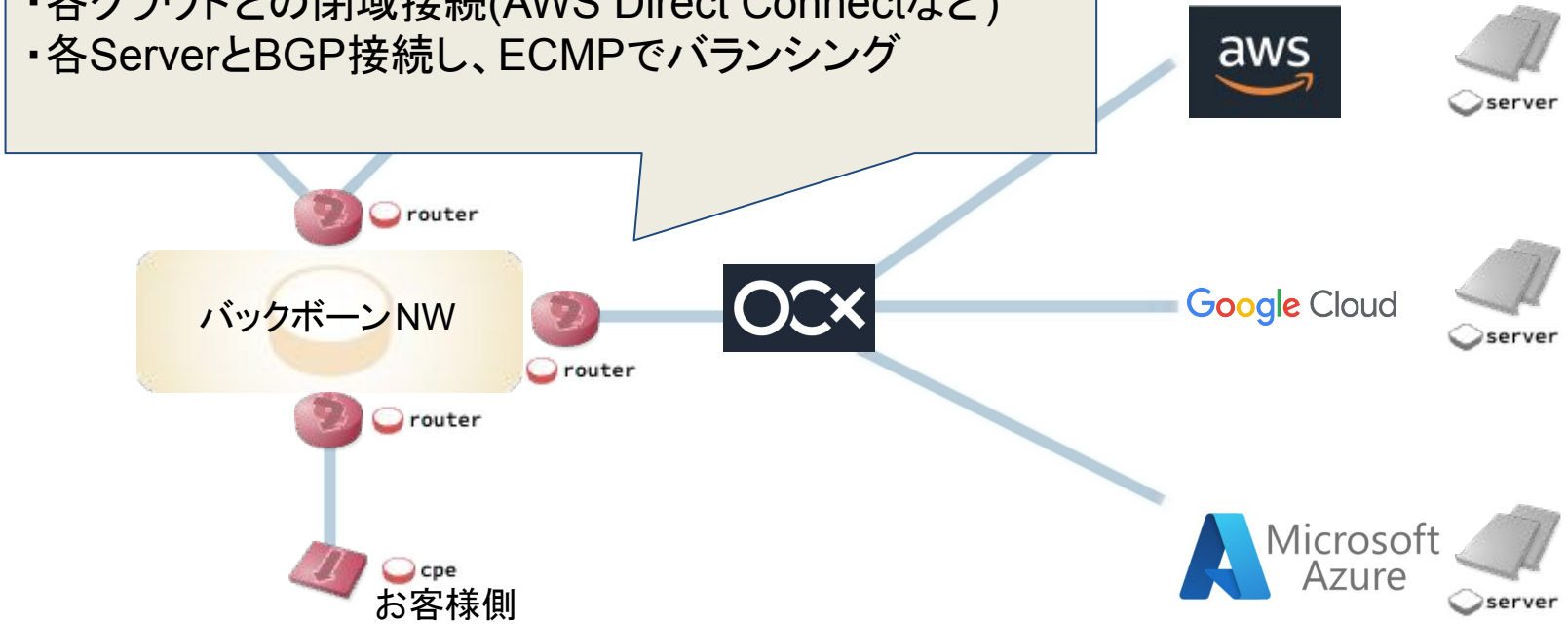
作っていたNWの基本形
※少し省略や改変しています

キャッシュDNSサーバー検討案



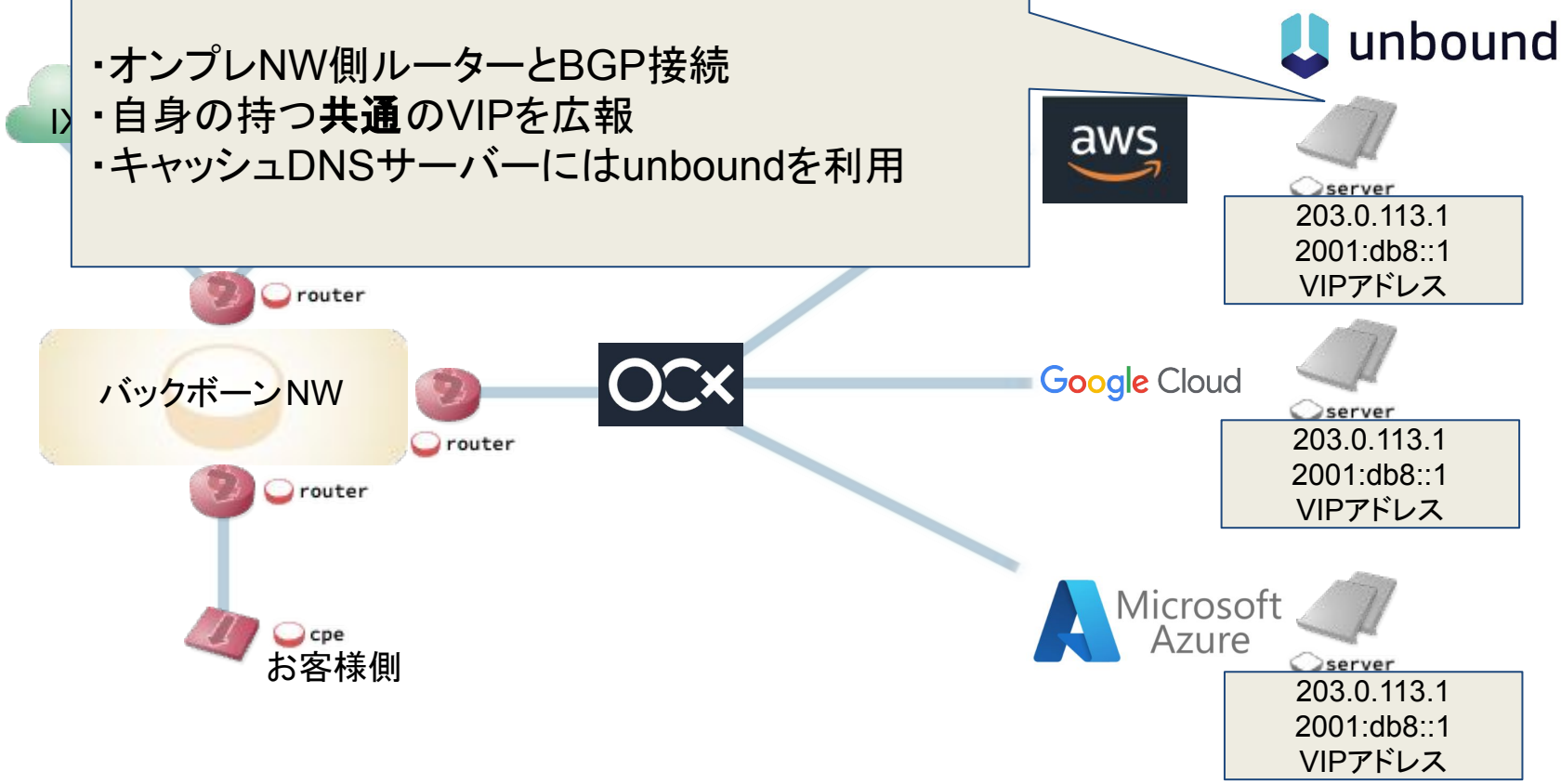
キャッシュDNSサーバー検討案

・各クラウドとの閉域接続(AWS Direct Connectなど)
・各ServerとBGP接続し、ECMPでバランシング

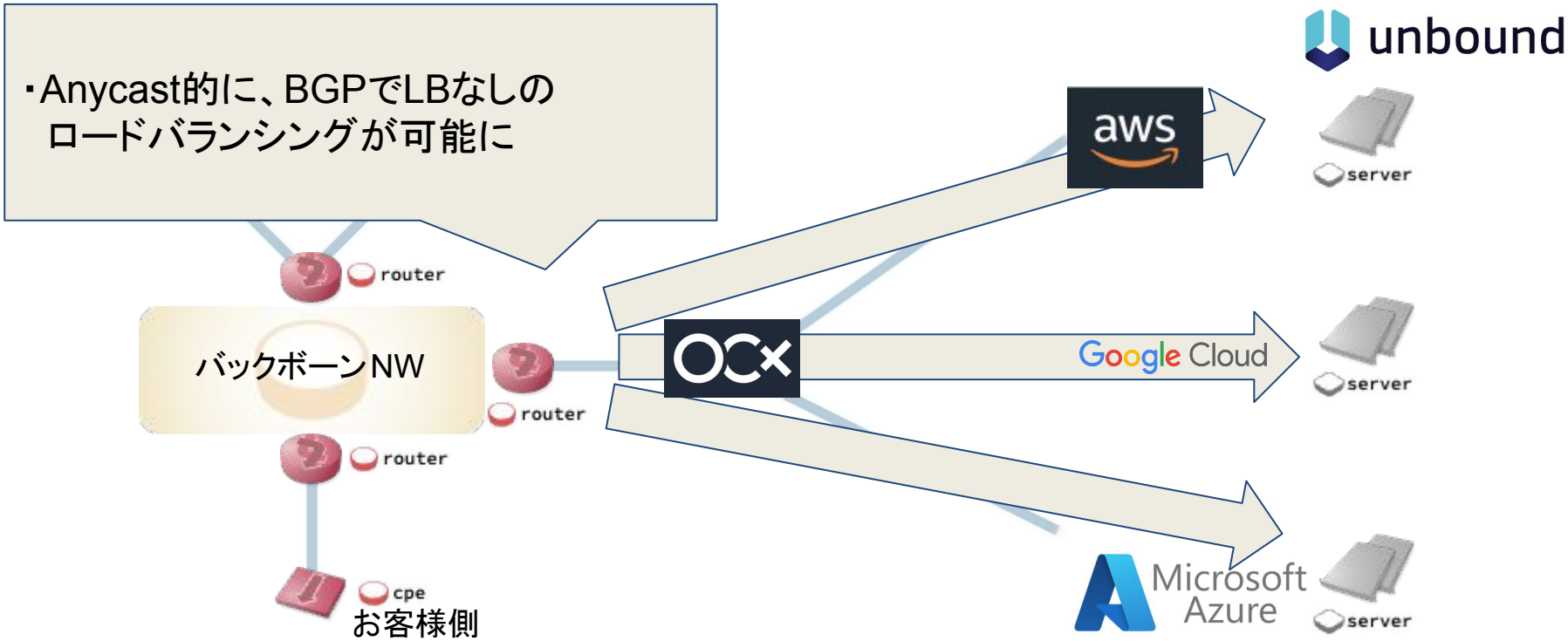


キャッシュDNSサーバー検討案

・オンプレNW側ルーターとBGP接続
・自身の持つ**共通**のVIPを広報
・キャッシュDNSサーバーにはunboundを利用



キャッシュDNSサーバー検討案



キャッシュDNSサーバー検討案

キャッシュDNSサーバー検討案

キャッシュDNSサーバーの構築

実際に構築してみたら

？？？？

BBSakura Networks

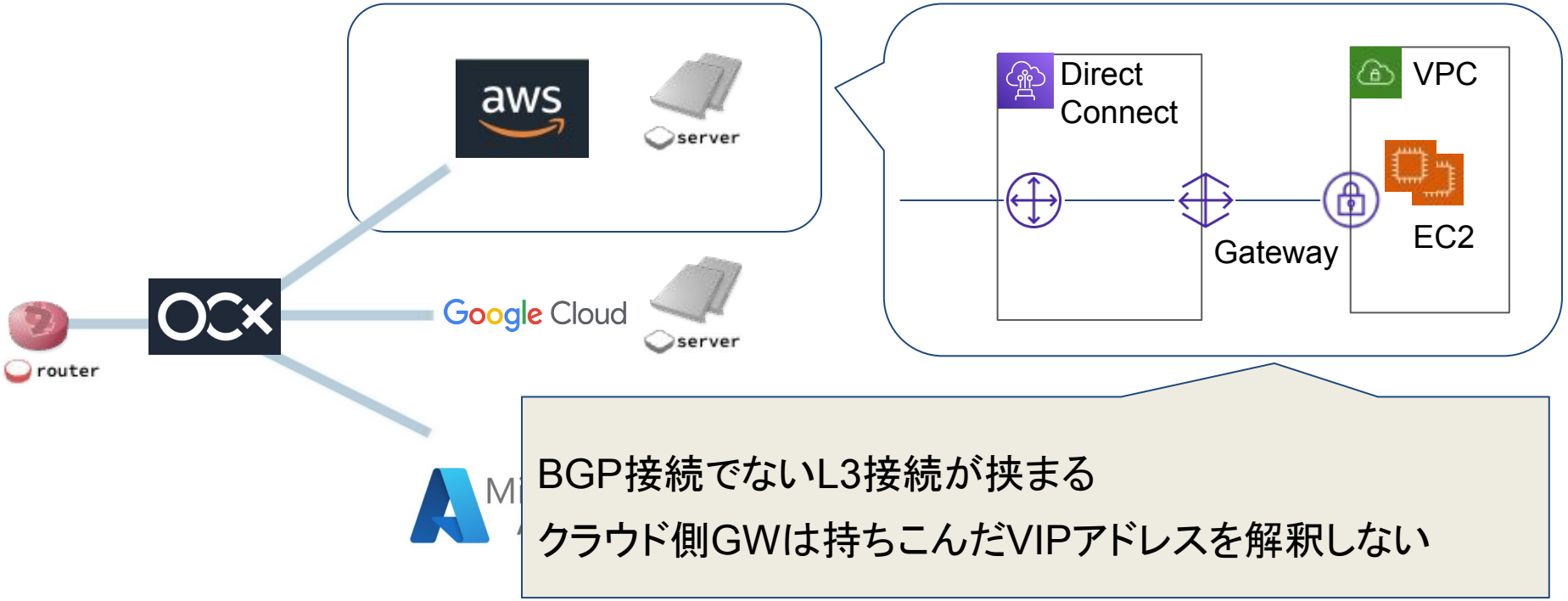
キャッシュDNSサーバーの構築

構築に関して2つ問題がでてきました

- オンプレ側のルーターとクラウドのサーバーとのBGP接続でVIPのアドレスが広報できない
- 一部クラウドの閉域接続ではIPv6でのBGP接続ができない

キャッシュDNSサーバーの構築

オンプレ側のルーターとクラウドのサーバーとのBGP接続でVIPのアドレスが広報できない



キャッシュDNSサーバーの構築

BBSakura Networks

一部クラウドの閉域接続ではIPv6でのBGP接続ができない問題

Google Cloud Interconnectでの制限

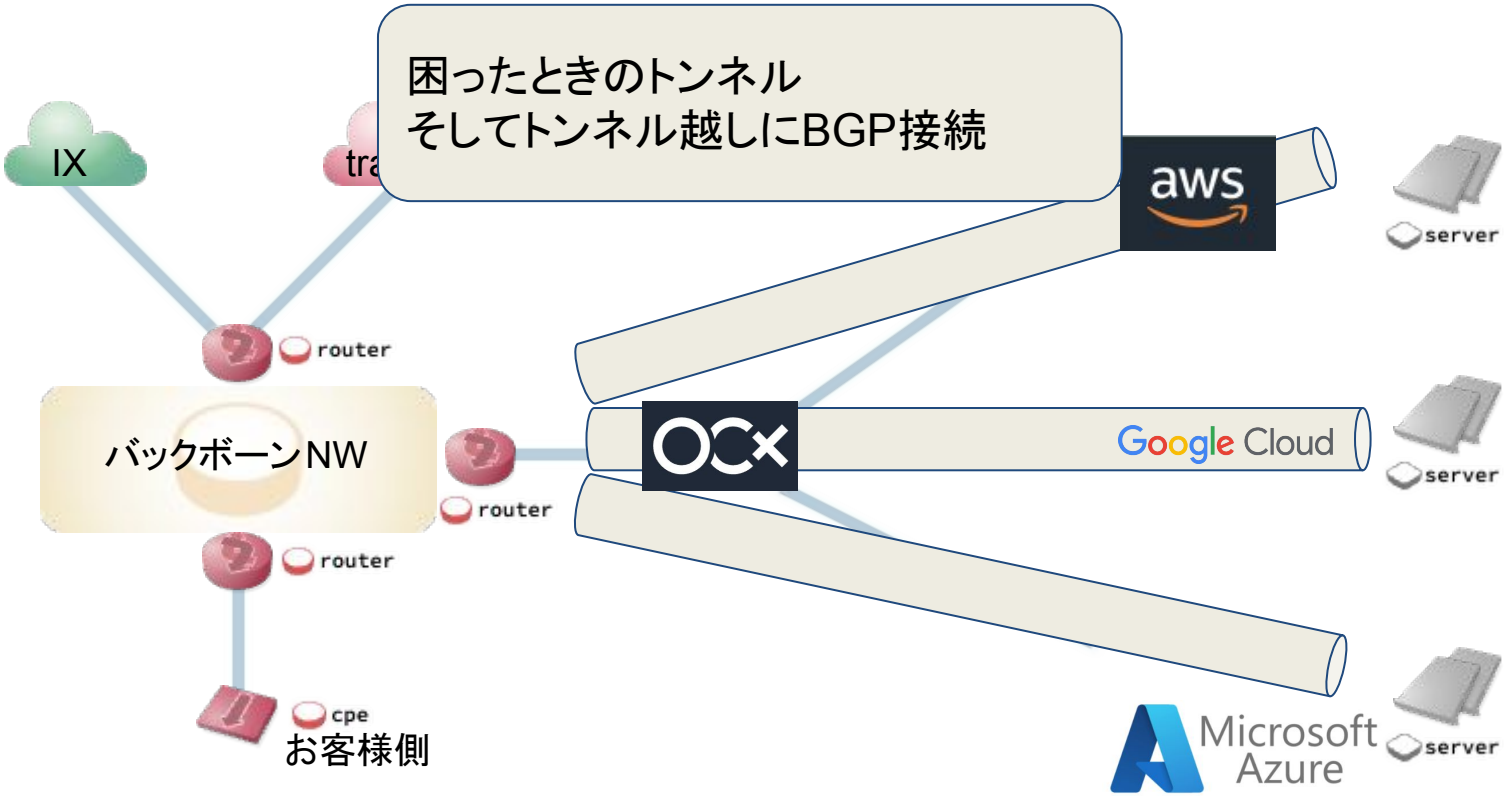
IPv6 の制限事項

IPv6 BGP ピアリングと IPv6 ルート交換は、次のリソースではサポートされていません。

・**Partner Interconnect VLAN アタッチメント**
・Classic VPN トンネル
・ルーター アプライアンス（Network Connectivity Center の一部）
・Cross-Cloud Interconnect VLAN アタッチメント

https://cloud.google.com/network-connectivity/docs/router/concepts/overview?hl=ja#ipv6-limits

キャッシュDNSサーバー構築



キャッシュDNSサーバーの構築

BBSakura Networks

さらなる問題が

Azureでのトンネル接続がうまくいかない

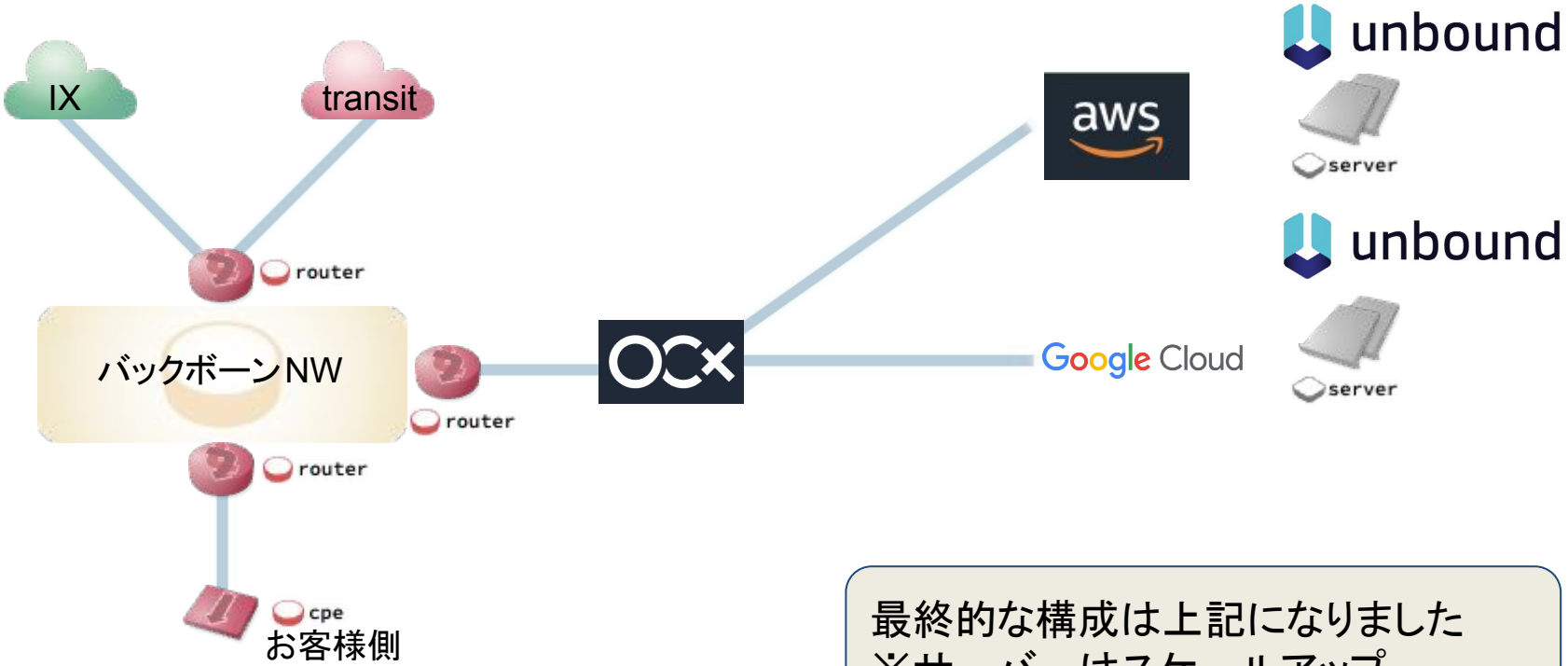
仮想ネットワークではどのようなプロトコルを使用できますか ？

仮想ネットワークでは、TCP、UDP、ESP、AH、ICMP TCP/IP プロトコルを使用することができます。

ユニキャストは仮想ネットワークでサポートされています。 マルチキャスト、ブロードキャスト、**IP-in-IP のカプセル化されたパケット、 Generic Routing Encapsulation (GRE) のパケットは、仮想ネットワークでブロックされます。** ユニキャスト (発信元ポート UDP/68、宛先ポート UDP/67) 経由で動的ホスト構成プロトコル (DHCP) は使用できません。 UDP 発信元ポート 65330 はホスト用に予約されています。

https://learn.microsoft.com/ja-jp/azure/virtual-network/virtual-networks-faq

キャッシュDNSサーバー構築



最終的な構成は上記になりました
※サーバーはスケールアップ

キャッシュDNSサーバー運用

- 構築が終わりリリースし、運用フェーズになりました
- Disk故障など機械的なトラブルは無くなりました
- クラウド独自の機能はあまり使わずIaaS的に使うことで、運用はシンプルになりました
- クラウド側の障害が起きた際は何も手出しできないリスクはありますが、マルチクラウド構成にしたことで耐障害性は担保しています
- キャッシュDNSサーバーはunboundしか利用していないので、今後ダイバーシティを持たせたい

まとめ

・はじめての挑戦だったので色々、むりやりなところがありましたが無事リリース

・当たり前ですが、オンプレでもクラウドでもどちらにもメリット
・デメリットがあります

また、挑戦を許してもらえて、他のメンバーから技術サポートしてもらえる会社だったのが幸運でした

参考にさせていただいた資料

OctoDNSとGitLab CI/CDを利用した 複数DNSプロバイダー構成の運用
https://dnsops.jp/bof/20191128/octodns-takizawa.pdf

フルサービスリゾルバの ロードバランサーなし構成について
https://dnsops.jp/event/20210625/13-kosaka.pdf

質疑応答・議論

- 構成や資料でここをもっと詳しく聞いてみたい
- 私だったら、この機能/この機能をつかってみる
- などなど

全ての「モノ」がつながる社会を支える
テクノロジーカンパニー

BBSakuraNetworks