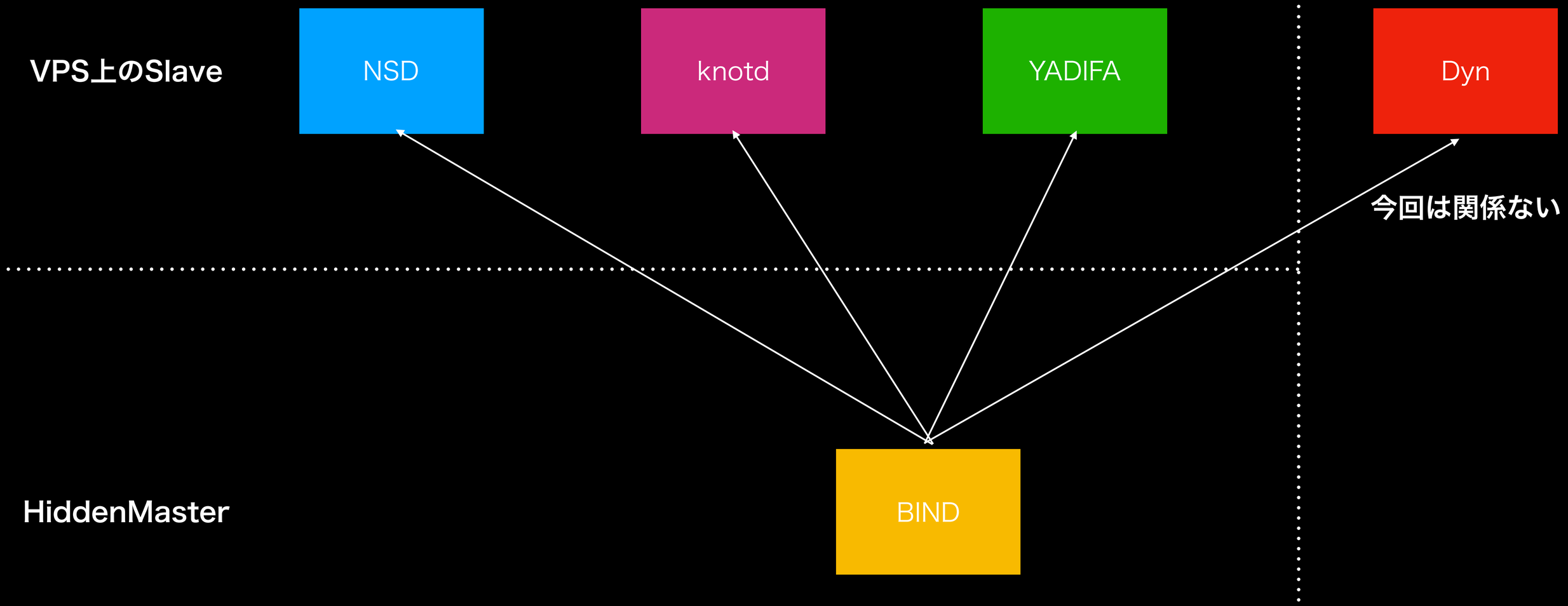
implement a Catalog zones

其田　学

いきなりですが

とある家庭の権威DNS



ダイバシティィ大変！

- ゾーン追加するたびに、４種類のコンフィグを作ったり、配ったり面倒
- いちいちコマンド覚えるのが面倒

```
# rndc reconfig
# nsd-control reconfig
# knotc reload
# yadifa zonecfgreload
Segmentation fault (core dumped)
# systemctl restart yadifad
```

Catalog zones

BIND9.11の新機能

- ゾーンデータはゾーン転送（AXFR,IFXR)で配れるけど
- zoneの設定そのものはファイルをコピーしてrndc reconfigとかrndc add zoneとかする必要があるよねー
- そうだ、ゾーン転送でゾーンの設定配っちゃえばいいじゃん

おれが求めていたのはこれだった！

catalog zoneの例

```
省略
version IN      TXT     1
masters IN      AAAA    2405:0:100:16::51
masters IN      AAAA    2409:10:20:500::53
f0c5d8f156ef2a646b7c0d17197d7eb93f6d7f77.zones  IN      PTR     0.0.1.0.0.0.0.0.5.0.4.2.ip6.arpa.
d8efb09fabf2a7c2a922ca01098105bfe5319658.zones  IN      PTR     usagi.cafe.
ccb4859d8fe2519c3d3f64253d1cf79c6a7e71f9.zones  IN      PTR     manabu-sonoda.com.
a0a09ae3797675f0c1797e07858a24e43ff299c3.zones  IN      PTR     mimuret.net.
allow-transfer.a0a09ae3797675f0c1797e07858a24e43ff299c3.zones   IN      APL     1:204.13.249.76/32 \
                                                                                1:208.78.69.76/32 1:91.198.22.76/32
```

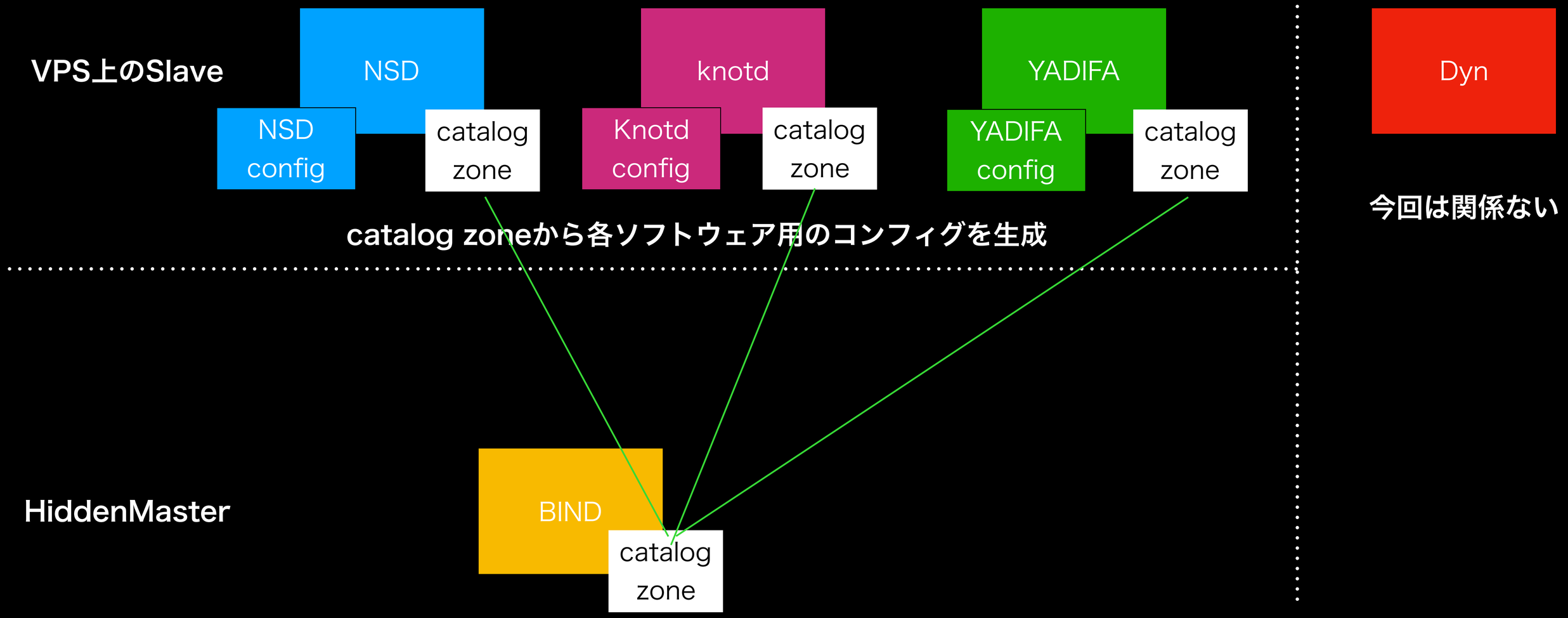
version: catlogゾーンのフォーマットのバージョン

masters: ゾーンのマスタのホストのアドレス

(SHA1).zones：設定するゾーン名とゾーン名のSHA1

allow-transfer.(SHA1).zones SHA1なゾーン名の
ゾーン転送許可するACL

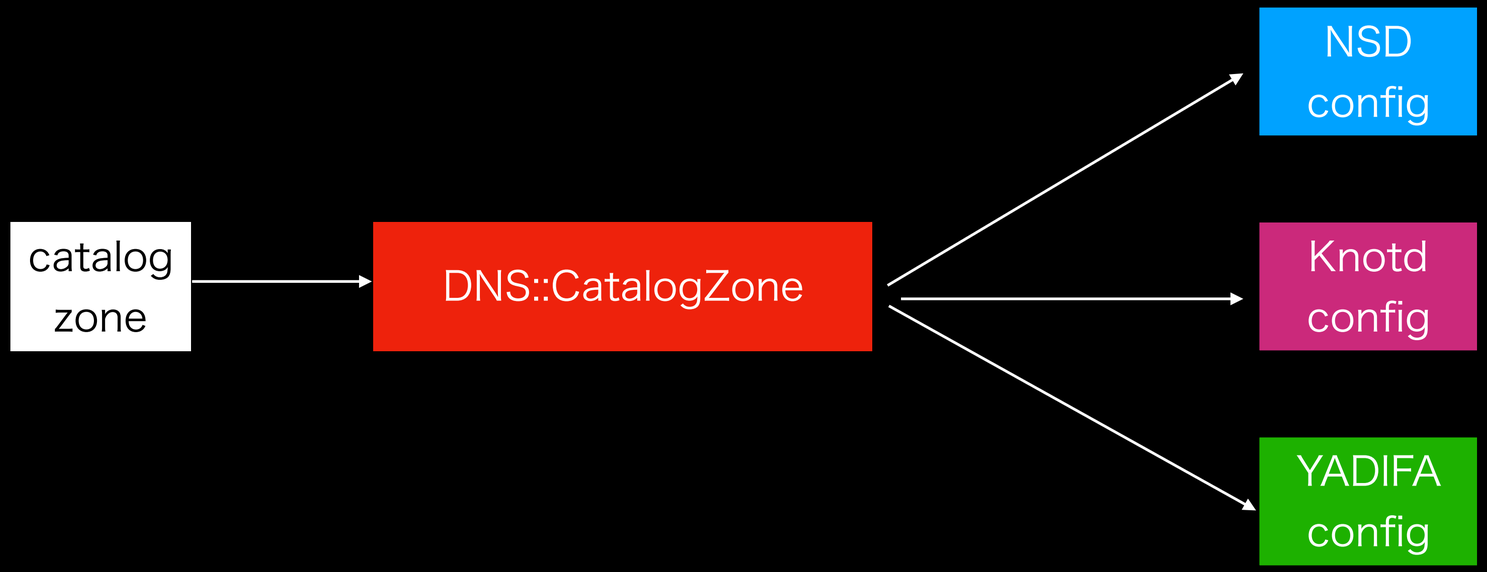
いめーじ


VPS上のSlave
NSD
NSD config
catalog zone
knotd
Knotd config
catalog zone
YADIFA
YADIFA config
catalog zone
Dyn
今回は関係ない
catalog zoneから各ソフトウェア用のコンフィグを生成
HiddenMaster
BIND
catalog zone

でも、対応してるのBIND9.11
だけなんでしょ？

作ってみた

- https://github.com/mimuret/dns-catalog_zone （本体）
- https://github.com/alexdalitz/dnsruby/pull/111 (APL RR対応)
- https://github.com/alexdalitz/dnsruby/pull/117 (AXFRでソースIPの指定可能に)



使い方 1

```
# gem install dns-catalog_zone
# catz init     CatalogZone(設定ファイル）ができる
# cat CatalogZone
setting("catalog.example.jp") do |s|
        s.software=“nsd"      ソフトウェアの種類(nsd,knot,yadifa)
        s.source=“file"           catalog zoneの取得方法
                                  file: ファイル経由 axfr: ゾーン転送
        s.zonename=“catalog.example.jp"   catalog zoneのゾーン名
        s.zonefile="/etc/nsd/catalog.example.jp.zone"
end
```

使い方２

```
# catz make
pattern:
    name: "CatalogZone"
    # ..masters
    request-xfr: 2405:0:100::1@53 NOKEY
    allow-notify: 2405:0:100::1/128@53 NOKEY
zone:
    include-pattern: “CatalogZone"
    name: "mimuret.net"
    zonefile: "/var/service/dns/data/zones/mimuret.net"
```

使ってみた

- ゾーンから設定を書き出すところまでは作ったが・・
- ゾーンが更新を検知する仕組みがまだない。
  - 今はcronで更新かけてます。
  - デーモン化して、notify受けられるようになれば
    できるけど、気力がない。。。
  - 多分その前にきっとNSDとかknotd自体が対応してくれるはず

まとめ

- ゾーンから設定を書き出すところを作った
- 一応動く程度
- daemon化したい