Unboundの紹介

ENOG18

高田 美紀

@mikiT_T

自己紹介

- InfoSphereサービス立ち上げ
  - ISPサービス(NTTグループでは初)
    - 1994年～
  - 担当: DNS、メール、Radius認証系、他
- WebARENAの中の人
  - ハウジング、VPS、共用レンタルサーバなど
    - 1999年～
  - 担当: DNS、メール、UNIXシステム管理、他
- DNSOPS.JP 幹事

agenda

- Unbound?
- BINDとのちがい
- build&setup
- 関連ツール紹介
- まとめ
- 参考資料

Unboundとは

- キャッシュDNSサーバソフトウェア
  - キャッシュDNSのサービスに特化
    - シンプル
  - 簡易的な権威DNSサーバの機能もある
  - オープンソース、BSDライセンス
  - Linux版とWindows版がある
  - 最新版は1.4.19 (2012/12/12リリース)
- オランダNLnet Labs他4組織で開発
  - http://unbound.net/
  - BINDの代替、DNSサーバの多様性
  - 現在はNLnet Labsにて開発、保守

なぜUnbound?

- 不定期的にやってくるBIND脆弱性発見
  - クリティカル、workaroundなし
  - アップデートにはコストがかかる
    - 検証、各所への連絡、実際の作業、重点監視
  - アップデートまでに攻撃されるリスク
    - 1パケットでnamedが死んだり
    - DNSサービスの停止=>サービス全断
- 高パフォーマンス
- 大規模な環境でも使われている

「UnboundキャッシュDNSサーバ 大規模用途向け機能の実装」より

- 性能

		キャッシュヒット率	
		0%	100%
Unbound 1.4.18	qps	9,947	54,527
BIND 9.8.3-P2	qps	3,730	20,106
Unbound/BIND	qps/qps	2.67	2.71

CPU: Core2duo T5500 1.66GHz Mem: 2GB OS: CentOS 5.8 (32bit)
キャッシュヒット率100%のケースは、メモリ上に100万エントリをキャッシュさせた状況。キャッシュヒット率0%のケースは、キャッシュが空の状態から、各クエリにつき権威サーバへの問い合わせは１回のみ発生させながらキャッシュを満たしていく状況を作った。

- 脆弱性の発生状況

		2012年	2011年	2010年	2009年	2008年
Unbound	件数	1	2	1	1	0

セキュリティ脆弱性が発表された回数。2012年の１件はGhost Domain Names問題で、当時の最新版ではすでに修正済。

BIND(キャッシュ)との違い

- ない機能
  - View
  - ResponsePolicyZone
  - AAAA filter
  - DNS64
- 挙動の違い
  - DNSラウンドロビン
  - 多段CNAME
  - アクセス制限
  - cache snooping
- 各種コマンド
  - rndc
    - unbound-control
  - dig
    - drill
- ログ形式

ない機能

- View
  - 複数のサーバを稼働させることで回避
- ResponsePolicyZone
  - 簡易権威サーバ機能で代替可能な場合も
- AAAA filter
  - 構成変更や運用等で回避
- DNS64
  - 過去バージョン用のパッチがあったらしい
- 必要ならコードを書きましょう☺

挙動の違い(1)

- DNSラウンドロビン
  - unbound 1.4.17にて実装
  - デフォルトではオフ
    - rrset-roundrobin: yes
  - ラウンドロビンでなく、ランダムな順番で答える
- 多段CNAME
  - 9段以上の多段になるとSERVFAIL
    - hoge1 IN CNAME hoge2
    - hoge2 IN CNAME hoge3
    - :
    - hoge9 IN CNAME hoge10
    - hoge10 IN A 192.0.2.1
  - RFCには特に規定がない部分

挙動の違い(2)

- アクセス制限
  - デフォルトは、どこからの問い合わせにも答えない
  - NW単位で許可設定
    - allow-control: 192.0.2.0/24 allow
  - オープンリゾルバの予防
    - 必要なNWにのみサービスするようにしましょう
- cache snooping
  - キャッシュDNSサーバへの非再帰検索要求
  - unboundは返答しないのがデフォルト
    - キャッシュには再帰検索しかこない筈だから?
  - NW単位で許可設定
    - allow-control: 192.0.2.0/24 allow_snoop
  - BINDからの置き換えと考えると必要かも?

挙動の違い(3)

- プライベートアドレスはNXDOMAIN
  - RFC 1918, 0/8, 169.254/16, 192.0.2/24, 198.51.100/24, 203.0.113/24, 他
    - これらについて返事させたいときには、簡易権威DNSサーバ機能(local-zone, stub-zone)を使う
    - イマドキのbindは同様の挙動だった

導入シナリオ(1)

- bindをunboundに置き換え
  - 置き換え時の一時的なコストのみ
  - IPアドレス等変更しなくてok
    - サービス影響が少ない
  - 可能ならおすすめ
- キャッシュ機能だけunboundに置き換え
  - 権威/キャッシュ兼用の場合など
  - bindは権威のみサービスするよう設定変更
  - IPアドレスを変更する必要があるかも
  - 権威/キャッシュ機能分離にもなって☺

導入シナリオ(2)

- hot standby
  - LBでの運用の場合
    - LBのうしろにBINDとunbound両方用意
- cold standby
  - 通常はBINDを使用
  - namedが死んだらunbound登場
  - BIND特有の機能を使っている場合など
- 置き換え以外は両方管理することになる
  - コスト増
  - でも背に腹はかえられない
  - unboundにも脆弱性発見の可能性があるから

cold standbyの一手法

- bind付属のプロセス監視ツール
  - contrib/nanny/nanny.pl
  - psとdigで監視、異常があったら再起動
- 改造
  - 異常検知時
    - namedをkill
    - unboundを起動
  - unbound稼働中の異常検知
    - namedは起動しない

必要な環境

- OpenSSLの開発環境
  - バージョン1.0未満の場合
    - GOSTとECDSAを要disable
      - 後述のコマンドラインにてグレイアウト部分を指定
    - CentOS 5系とか
- ldns (後述)
- libevent-devel, expat-devel ほか

ldns

- NLnet Labs製ソフトウェア
  - DNSまわりライブラリ
    - RFCや最新のドラフトに追従
  - サンプルプログラム
    - drill (DNS検索ツール。BINDでいうdig)
    - その他 (ldns-walkとか)
  - Cで記述 (高速)
- http://www.nlnetlabs.nl/projects/ldns/
- 機能
  - IPv4 / IPv6 サポート
  - TSIG サポート
  - DNSSEC サポート (署名と検証)
  - 小さいサイズ
  - オンライン文書とman

build&install: ldns

- wget http://www.nlnetlabs.nl/downloads/ldns/ldns-1.6.16.tar.gz
- zcat ldns-1.6.16.tar.gz | tar xf –
- cd ldns-1.6.16/
- ./configure --prefix=/usr/local/ --with-drill --disable-gost --disable-ecdsa && make && sudo make install
  - OpenSSL 1.0未満の場合は、グレイアウト部分を指定

build&install&setup: unbound

- wget http://www.unbound.net/downloads/unbound-1.4.19.tar.gz
- ./configure --prefix=/usr/local/ --disable-gost --disable-ecdsa && make && sudo make install
- sudo useradd unbound
  - unboundユーザを追加
- sudo /usr/local/sbin/unbound-control-setup
  - unbound-control用の環境設定
- sudo chown unbound:unbound /usr/local/etc/unbound
  - pidファイル等のためownerを変更
- DNSSEC検証をする場合のみ
  - sudo /usr/local/sbin/unbound-anchor
    - rootのDNSKEYを取得
    - 本来はこの鍵が正しらしいか確認する必要が。。
- sudo /usr/local/sbin/unbound
  - 起動!

/usr/local/etc/unbound/unbound.conf

- デフォルト設定でも動く
- 例:
- server:

  rrset-roundrobin: yes

  auto-trust-anchor-file:

  ”/local/etc/unbound/root.key"

  statistics-interval: 300

  extended-statistics: yes

  val-log-level: 2

- remote-control:
  - control-enable: yes

- ラウンドロビン設定ON
- DNSSEC検証ON＋root DNSKEYファイル指定

- 統計出力インターバル(秒)
- 拡張統計設定ON
- DNSSEC検証エラーのログレベル。後述
- unbound-controlでの制御ON

unbound.conf (2)

- localhost以外からのクエリを受け付ける
  - acess-control: n.n.n.n/n allow
    - だけではダメ
  - interface: 0.0.0.0 or interface: ::0
    - インタフェースを開けてやる必要がある

ログの見え方

- statistics
  - [7903:0] info: server stats for thread 0: 3 queries, 0 answers from cache, 3 recursions, 0 prefetch
  - [7903:0] info: server stats for thread 0: requestlist max 0 avg 0 exceeded 0 jostled 0
- extended-statistics: yes
  - [7903:0] info: average recursion processing time 0.521795 sec
  - [7903:0] info: histogram of recursion processing times
  - [7903:0] info: [25%]=0 median[50%]=0 [75%]=0
  - [7903:0] info: lower(secs) upper(secs) recursions
  - [7903:0] info: 0.065536 0.131072 1
  - [7903:0] info: 0.262144 0.524288 1
  - [7903:0] info: 0.524288 1.000000 1
- val-log-level: 2
  - [7903:0] info: validation failure <fail.dnssec.jp. A IN>: signature expired from 111.89.176.107 for key fail.dnssec.jp. while building chain of trust

unbound-control

- unboundのコントロールをするツール
  - BINDでいうrndc
- 機能
  - プロセス関連
    - start, stop, reload, stats, status, stats_noreset
  - 簡易権威DNSサーバ機能関連
    - local_zone, local_zone_remove, list_local_zones, local_data, local_data_remove, list_local_data, stub_add, stub_remove, list_stubs
  - キャッシュ関連
    - dump_cache, load_cache, dump_requestlist, dump_infra
  - キャッシュ消去関連
    - flush, flush_type, flush_zone, flush_bogus, flush_stats, flush_requestlist, flush_infra
  - forward関連
    - forward_add, forward_remove, list_forwards, forward
  - その他
    - verbosity, log_reopen, lookup, set_option, get_option
  - BINDにない機能もいろいろ

おまけ: root hint 変更

- D.ROOT-SERVERS.NET IPアドレス変更
  - http://www.ietf.org/mail-archive/web/dnsop/current/msg09956.html
  - http://jprs.jp/tech/notice/2012-12-18-d-root-ip-address-change.html
  - 米メリーランド大運営のルートNS
  - 新: 199.7.91.13　旧: 128.8.10.90
  - (少なくとも)半年間、並行運用される
- Unbound(イマドキのBIND)のroot.hintは、ソースにハードコードされている
  - 次のバージョンでは書き変わってるかも
- unbound.confで指定することも可能
  - root-hints: ”root.hint” など
  - 設定したら、ちゃんと更新を

プライミング (priming)

- root.hintを使うのは最初だけ
  - プロセス起動時
- root.hint内のどれかに．のNSを問合せ
  - 戻ってきた答えをヒントとして使う
- BIND, Unboundはこういう実装
- root.hintの更新は緩やかでok
  - 1/13 のリスク
    - 旧サーバのIPが別組織に再割当されたら?
    - BGPハイジャックされたら?
- やっぱりきちんとやっておきましょう

まとめ

- Unboundおすすめポイント
  - わかりやすい記法の設定ファイル
    - BINDに比べて
  - 高性能(qps)
  - 脆弱性の少なさ
  - キャッシュに特化
    - シンプル
- シンプルな構成を心がける
  - ベンダーロックインを防ぐ
  - 運用しやすい

参考資料

- UnboundキャッシュDNSサーバ 大規模用途向け機能の実装
  - http://dnsops.jp/event/20120901/Unbound-higashi-dnsops-2012summerday2-final.pdf
  - 東 大亮さん、DNS Summer Days 2012での発表資料
- Unbound，知ってる？ この先10年を見据えたDNS
  - 滝澤隆史さん、2008年の技術評論社記事。全4回
  - http://gihyo.jp/admin/feature/01/unbound/0001
- Unbound Validating Caching Resolver
  - http://unbound.net/documentation/ripe56_unbound_02.pdf
  - Wouter Wijngaardsさん、2008年RIPE56での発表資料

日本語の情報

- 日本Unboundユーザ会
  - http://unbound.jp/
  - 和訳マニュアル、アップデートのアナウンスなど