Enriching Feature Sets With Layered Microservices

_a Passive DNS Workbench_

Paul Vixie
Farsight Security
Amsterdam, 2019-04-02
Doing One Thing Well

• With foresight, discipline, and luck
• Avoiding second system syndrome
• Allowing mindful evolution
Ex.: DNSDB API (~2010)

- RESTful API
  - /lookup/rrset/domain[/type[/bailiwick]]
  - /lookup/rdata/domain[/type]
  - /lookup/ip/address[/prefixlength]

- JSON reply
  - Note UNIX time stamps
  - RDATA can be a string or array
  - Newline separated objects
  - 404 means “no result found”
  - No success/failure encoding

```json
{
  "count": 175892,
  "time_first": 1472789821,
  "time_last": 1554146388,
  "rrname": "vix.su.",
  "rrtype": "NS",
  "bailiwick": "vix.su.",
  "rdata": [
    "ns.lah1.vix.su.",
    "sfba.sns-pb.isc.org."
  ]
}
```
Advantages of Abstraction and Stability

• Back end can be improved or replaced
  • For DNSDB, this happens every 6..12 months

• Existing clients don’t become obsolete
  • Dependent work flows are at no risk

• Competitors can plug in at boundaries
  • Avoids vendor “lock-in” penalty

• Extensions need only be negotiated
  • Ask a newer question, get a newer answer
Some Extensions Are Natural

- Aggregation into a single `<first_seen, last_seen, count>` tuple?
  - Finer grained response may be available (gravel vs. rocks)
- UNIX time, vs RFC 3339
- Server side sorting
  - For “top N”
- Paging
  - For “next N”
- Success/failure signaling
  - To distinguish what 404 means, and to detect truncation
Other Extensions Seem Unnatural

• Access to other databases (whois, ASN, BGP, etc)
• Ability to re-use previous query results
• Indirection, set{} operations, etc
Multi-layered Services

• A stateful protocol can encapsulate a stateless one
  • Adds /login and /logout verbs
  • Wraps results in tagged (success/fail) objects

• Multiple backends can be accessed
  • Name the system, identify what kind it is
  • Add more systems over time
Marks of Protocol Maturity

• Multiple independent implementations
  • Ideally of both the server and client side
• Support for more than one media type
  • E.g., CLI and Web UI
• Possible to learn & use with only documentation
  • Not hand holding and training
REST verbs in FSWB (~2018)

POST /login
GET /logout
GET /noop
POST /settings/chpw
GET /settings/get
GET /settings/set/:thing/:value
GET /settings/tool/:tool/set/:sys/:key/$base64(:uri)
GET /settings/tool/:tool/clear/:sys
GET /tool/kinds
GET /tool/list
GET /tool/lookup/:tool/:sys/$base64(:search)/:kind/:by/:dir/:params
GET /bench/list
GET /bench/clear
GET /bench/incinerate/:file
Example: /tool/kinds

vixie@VIXP1:~/wksp/src/fswb/fswb$ cli -protodebug tool kinds
code: 200 (/noop)
line: {"message":"
}
code: 200 (/tool/kinds)
line: {"message":"
}
line: {"tool":"bench","systems":[{"sys":"builtin","kinds":["in-keys","keys-out","in-values","values-out"]}]}
line: {"tool":"pdns","systems":[{"sys":"dnsdb","kinds":["rrset","rdata","ip"]},{"sys":"dnsdb-eu","kinds":["rrset","rdata","ip"]},{"sys":"dnsdb-cn","kinds":["rrset","rdata","ip"]}]
tool: bench
  builtin [in-keys keys-out in-values values-out]
tool: pdns
  dnsdb [rrset rdata ip]
  dnsdb-eu [rrset rdata ip]
  dnsdb-cn [rrset rdata ip]
Example: /bench/list

vixie@VIXP1:~/.wksp/src/fswb/fswb$ cli bench
@001 2019-02-07 19:07:11 pdns/dnsdb 7208/5386/2476
   *.housing4pros.us rrset
      pdns,dnsdb:rrset,FIXGQ33VONUW4ZZUOBZG64Z0OVZQ====
@002 2019-02-07 15:36:37 pdns/dnsdb 3/1/0
   farsightsecurity.com/ds rrset
      pdns,dnsdb:rrset,MZQXE43JM5UHI43FMN2XE2LUPEXGG33NF5SHG===
@003 2019-02-07 15:36:10 pdns/dnsdb 0/0/0
   bbc.com/ds rrset
      pdns,dnsdb:rrset,MJRGGLTDN5WS6ZDT
@004 2019-02-07 15:33:31 pdns/dnsdb 7/7/1
   212.58.244.56 ip
      pdns,dnsdb:ip,GIYTELRVHAXDENBUFY2TM==
@005 2019-02-07 15:31:57 pdns/dnsdb 77/1/32
   newswww.bbc.net.uk rrset
      pdns,dnsdb:rrset,NZSXO43X053S4YTCMMXG4ZLUFZ2Ww==
Example: /tool/lookup

vixie@VIXP1:~/wksp/src/fswb/fswb$ cli lookup @005 limit 3

;; record times: 2010-06-23 20:14:08 .. 2010-07-01 02:56:25
;; count: 382; bailiwick: bbc.net.uk
newswww.bbc.net.uk A 212.58.226.77

;; record times: 2010-06-23 20:26:07 .. 2010-07-01 02:46:17
;; count: 395; bailiwick: bbc.net.uk
newswww.bbc.net.uk A 212.58.226.73

;; record times: 2010-06-23 21:42:52 .. 2010-07-01 02:47:36
;; count: 388; bailiwick: bbc.net.uk
newswww.bbc.net.uk A 212.58.226.75
Where Is The State?

vixie@VIXP1:~/.fswb/ ls -l ~/.fswb*
-rw-rw-r-- 1 vixie vixie 1394 Apr 1 13:40 /home/vixie/.fswbcli-bench.json
-rw-rw-r-- 1 vixie vixie 97 Apr 1 13:40 /home/vixie/.fswbcli-params.json
-r-------- 1 vixie vixie 82 Apr 1 13:36 /home/vixie/.fswbcli-session.json

vixie@VIXP1:~/.fswb/ jq . ~/.fswbcli-session.json
{
  "service": "http://family.redbarn.org:3792",
  "session": "CAwABXZpeGllCAoABbHfLgD8"
}
One More Look at /tool/lookup

vixie@VIXP1:~/wksp/src/fswb/fswb$ cli -format=csv lookup @005 limit 3
```
time_first,time_last,zone_first,zone_last,count,bailiwick,rrname,rrtype,rdata
2010-07-01 03:11:27,2019-04-01 10:18:34,,,20183163,,newswww.bbc.net.uk,A,212.58.244.56
2010-07-16 04:19:37,2019-02-26 11:40:21,,,11411,,newsbeta.telhc.bbc.co.uk,A,212.58.244.56
```
vixie@VIXP1:~/wksp/src/fswb/fswb$ cli -format=json lookup @005 limit 3
```
{"bailiwick":"bbc.net.uk.","count":382,"rdata":["212.58.226.77"],"rrname":"newswww.bbc.net.uk." ,"rrtype":"A","time_first":1277349248,"time_last":1277978185}
{"bailiwick":"bbc.net.uk.","count":395,"rdata":["212.58.226.73"],"rrname":"newswww.bbc.net.uk." ,"rrtype":"A","time_first":1277349967,"time_last":1277977577}
{"bailiwick":"bbc.net.uk.","count":388,"rdata":["212.58.226.75"],"rrname":"newswww.bbc.net.uk." ,"rrtype":"A","time_first":1277354572,"time_last":1277977656}
```
code: 200 (/tool/lookup/pdns/dnsdb/bmV3c3d3dy5iYmMubmV0LnVr/rrset/first/asc/1,,,loose)
line:{"object":{"bailiwick":"bbc.net.uk.","count":395,"rdata":["212.58.226.73"],"rrname":"newswww.bbc.net.uk." ,"rrtype":"A","time_first":1277349967,"time_last":1277977577}}
Second Implementation? Other Media Type?

• (demo)
Conclusions

• There’s usually a time to call something “finished”
• If well made, it can become part of a larger tool chain
• Gotcha: streaming vs. store-and-forward
• This is not the same problem of API versioning
“You do not truly know someone until you fight them.” –Seraph, *The Matrix Reloaded*
vixie@VIXP1:~/wksp/src/fswb$ find . -name '*.go' | xargs wc
18    72    455  ./fswb/config.go
159   377   2617  ./fswb/enums.go
173   566   4321  ./fswb/pdnsconv.go
677  2205  15948  ./fswb/protocol.go
143   489   3732  ./fswb/user.go
199   578   4241  ./fswbadmin/main.go
977  3309  24121  ./fswbcli/main.go
1058  3736  26494  ./fswbsd/bench.go
138   497   3316  ./fswbsd/builtin.go
381  1184  10379  ./fswbsd/main.go
501  1809  12909  ./fswbsd/pdns.go
207   726   5062  ./fswbsd/session.go
 78   252   2260  ./fswbsd/settings.go
673  2245  19166  ./fswbwd/bench.go
129   388   3128  ./fswbwd/builtin.go
 58   176   1296  ./fswbwd/cookie.go
416  1303  11304  ./fswbwd/main.go
570  2044  15274  ./fswbwd/pdns.go
173   516   4099  ./fswbwd/result.go
384  1245  10088  ./fswbwd/settings.go
7112 23717 180210 total