

About Tom

- I'm Tom Limoncelli
 - SRE, Platform Engineer, author of 5 books
- Employer: Stack Overflow.com
- Based in: New Jersey, USA
- BlueSky: @yesthattom.bsky.social
- Email: tlimoncelli at stackoverflow dot com
- *Configured my first DNS server in 1991*

What is DNSControl?

- A configuration language for DNS domains
 - Edit config files → push to production
 - "Infrastructure as Code" / "DNS as Code"
- Supports dozens of DNS providers:
 - Updates BIND zonefiles or talks to the API of Azure, Cloudflare, Google, AWS, etc.
- www.dnscontrol.org
 - Github: <https://github.com/StackExchange/dnscontrol>
 - 3500 stars
 - 254 contributors (as of 2025-09)

The outage I caused

- Joined Stack Overflow in 2013
- Caused an outage my 3rd week
- Bounced all email for 2 hours

the typo

stackoverflow.com

```
@      IN SOA ( ns3.serverfault.com.
              sysadmin.stackoverflow.com.
              2013062901
              3600 600 604800 1440 )
      IN NS   ns1.serverfault.com.
      IN NS   ns2.serverfault.com.
      IN NS   ns3.serverfault.com.
      IN NS   ns4.serverfault.com.
      IN A    198.252.206.16
      IN MX   10 ASPMX.L.GOOGLE.COM.
      IN MX   20 ALT1.ASPMX.L.GOOGLE.COM.
      IN MX   20 ALT2.ASPMX.L.GOOGLE.COM.
      IN MX   30 ASPMX2.GOOGLEMAIL.COM.
      IN MX   30 ASPMX3.GOOGLEMAIL.COM.
api    IN A    198.252.206.16
blog   IN A    151.101.1.69
dev.blog IN A   151.101.1.70
...
```

```
@      IN SOA ( ns3.serverfault.com.
              sysadmin.stackoverflow.com.
              2013071001
              3600 600 604800 1440 )
      IN NS   ns1.serverfault.com.
      IN NS   ns2.serverfault.com.
      IN NS   ns3.serverfault.com.
      IN NS   ns4.serverfault.com.
      IN A    198.252.206.16
      IN MX   1 ASPMX.L.GOOGLE.COM
      IN MX   5 ALT1.ASPMX.L.GOOGLE.COM
      IN MX   5 ALT2.ASPMX.L.GOOGLE.COM
      IN MX   10 ALT3.ASPMX.L.GOOGLE.COM
      IN MX   10 ALT4.ASPMX.L.GOOGLE.COM
api    IN A    198.252.206.16
blog   IN A    151.101.1.69
dev.blog IN A   151.101.1.70
...
```

Boy was I embarrassed!



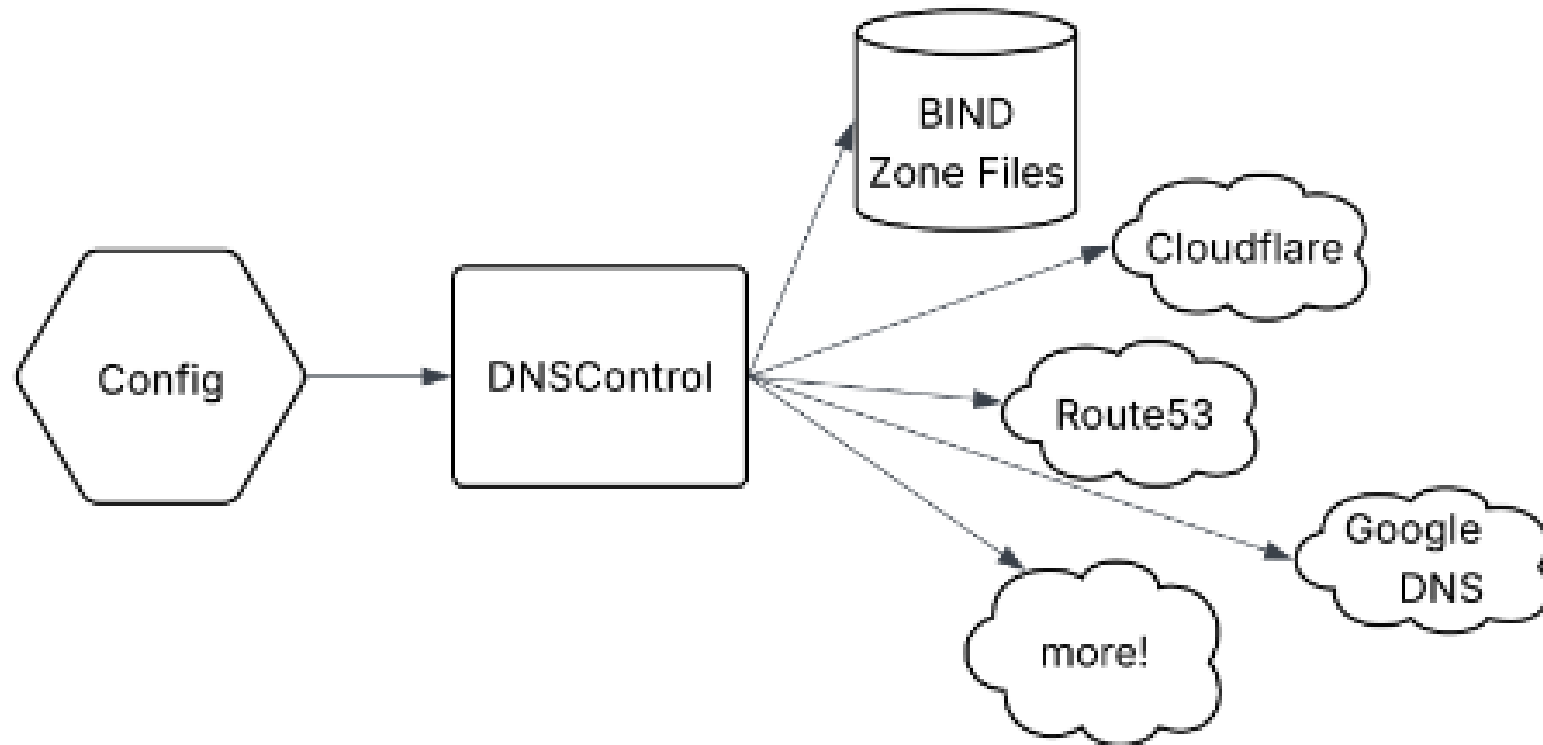
Why? Why? Why?

- Why were we still editing BIND zone files?
- Why so few guardrails?

Why not a config file that is...

- generic
- high-level
- makes intent clear
- detect/prevents errors
- reduces cognitive load (brain work)

Workflow



My configuration file. I make the rules.

- Opinionated
- No trailing dot is an error!
- Default TTLs
- automatic IDN
- Generic, with support for provider-specific extensions
- Support for variables, macros, templates

(Luckily other people liked my rules)

One config file to rule them all!



Something like this...

```
D("stackoverflow.com",  
  DnsProvider(BIND_ZONEFILE),  
  A("www", "1.2.3.4"),  
  CNAME("myalias", "www.stackoverflow.com."),  
  MX("@", 1, "aspmx.l.google.com."),  
  MX("@", 5, "alt1.aspmx.l.google.com."),  
  MX("@", 5, "alt2.aspmx.l.google.com."),  
  MX("@", 10, "alt3.aspmx.l.google.com."),  
  MX("@", 10, "alt4.aspmx.l.google.com"), // ERROR!  
);  
  
D("example.com",  
  DnsProvider(GOOGLE_DNS),  
  A("www", "1.2.3.4"),  
  TXT("@", "v=spf1 -all"),  
);
```

Goals of DNSControl:

- Simple DNS updates should be easy. Complex updates should be possible.
- Reduce risk of mistakes
- Enforce rules / opinions
- Generic format... push to specific providers
- Open source so anyone can add support for new APIs
- Peace, love, and rock 'n roll!

Project Info

- www.dnscontrol.org
- Github: <https://github.com/StackExchange/dnscontrol>
 - 3500 stars
 - 254 contributors (as of 2025-09)

Official support: BIND, Azure DNS, Cloudflare, Google DNS, AWS Route 53, CSC Global

Community support: AdGuardHome, Akamai, AXFRDDNS, Azure DNS, BunnyDNS, ClouDNS, CNR, deSEC, DigitalOcean, DNSimple, DNS Made Easy, DomainNameShop, Easyname, Exoscale, Gandi, GCore, HEDNS, Hetzner, Hexonet, HostingDE, HuaweiCloud, InternetBS, INWX Linode, Loopia, LuaDNS, Namecheap, Netcup, Netlify, NS1, OpenSRS, Oracle, OVH, Packetframe, PowerDNS, RealtimeRegister, SakuraCloud, Softlayer, TransIP, Vultr

Command-line usage:

```
sa-mac-F9UJQH4PHC:~/gitthings/dnscontrol-preses/icann2025/dns015 dns
```

Language features:

Variables

A:

```
D("example.com",  
  A("@", "174.136.107.196"),  
);
```

B:

```
var IP_FORSALE = "174.136.107.196";  
  
D("example.com",  
  A("@", IP_FORSALE),  
);
```


Variables express intent

```
// Language sites: es, ja, pt, ru  
A("es", IP_EXTERNAL_INGRESS_MAIN, FLAGS_PHASE2),  
A("ja", IP_EXTERNAL_INGRESS_MAIN, FLAGS_PHASE1),  
A("pt", IP_EXTERNAL_INGRESS_MAIN, FLAGS_PHASE1),  
A("ru", IP_EXTERNAL_INGRESS_MAIN, FLAGS_PHASE1),
```

Macros

```
var GOOGLE_APPS_DOMAIN_MX = [  
    MX("@", 1, "aspmx.l.google.com."),  
    MX("@", 5, "alt1.aspmx.l.google.com."),  
    MX("@", 5, "alt2.aspmx.l.google.com."),  
    MX("@", 10, "alt3.aspmx.l.google.com."),  
    MX("@", 10, "alt4.aspmx.l.google.com."),  
];  
  
D("stackoverflow.com",  
    ...  
    GOOGLE_APPS_DOMAIN_MX,  
    ...  
);  
  
D("stackexchange.com",  
    ...  
    GOOGLE_APPS_DOMAIN_MX,  
    ...  
);
```

Templates

```
function PARKED(name) {  
    D(name, REGISTRAR, DnsProvider(MY_DNS_PROVIDER),  
      A("@", "10.2.3.4"),  
      CNAME("www", "@"),  
      SPF_NONE, //deters spammers from using the domain in From: lines.  
    );  
}  
  
PARKED("example1.tld");  
PARKED("example2.tld");  
PARKED("example3.tld");
```

Loops!

```
_.each(  
  [  
    "example1.tld",  
    "example2.tld",  
    "example3.tld",  
  ],  
  function (d) {  
    D(d, MY_REGISTRAR, DnsProvider(MY_DNS_PROVIDER),  
      A("@", "10.2.3.4"),  
      CNAME("www", "@"),  
      SPF_NONE, //deters spammers from using the domain in From: lines.  
    );  
  }  
);
```

Require/include statements

```
require("lib/macros.js");  
require("lib/data.json");  
  
require("domains/team1.js");  
require("domains/team2.js");  
require("domains/team3.js");
```

Functions: Fancy redirect.

```
function REDIRECT_EXACT_FQDN(srcfqdn, dstfqdn) {  
    return [  
        // Create an A record with CF_PROXY_ON so that the traffic gets to Cloudflare:  
        // NB: A "." is appended to srcfqdn so that DNSControl knows it  
        // is a FQDN, and will give an error if this is in the wrong D().  
        A(srcfqdn + ".", ADDRESS_REDIRECT, CF_PROXY_ON),  
        // Create a redirect rule:  
        CF_TEMP_REDIRECT("https://" + srcfqdn + "/*", "https://" + dstfqdn + "/*"),  
    ]  
}  
  
D("askubuntu.com",  
    ...  
    REDIRECT_EXACT_FQDN("www.askubuntu.com", "askubuntu.com"),  
    REDIRECT_EXACT_FQDN("chat.askubuntu.com", "chat.stackexchange.com"),  
    ...  
);
```

Functions: RADS

```
function RADS(cc) {  
  return [  
    CF_SINGLE_REDIRECT('rads ' + cc, 301,  
      '(http.host eq "rads.stackoverflow.com" '  
        + 'and http.request.uri.path matches "^/amzn/click/'  
        + cc  
        + '/')',  
      'wildcard_replace(http.request.full_uri, '  
        + 'r"http*://rads.stackoverflow.com/amzn/click/'  
        + cc + '/*', r"https://www.amazon.' + cc + '/dp/${2}")'  
    ),  
  ];  
}  
  
D("example.com",  
  ...  
  RADS("co.uk"),  
  RADS("de"),  
  RADS("fr"),  
  RADS("es"),  
  RADS("it"),  
  RADS("com"),  
  ...
```

Computed records

```
var PUBPLAT_INSTANCE = function(name, internal_ip, internal_ip_win) {  
  function l(orig) {  
    return orig.replace("NAME", name).trim();  
  }  
  return [  
    A(l("      NAME.stackoverflow.dev.demo."), internal_ip),  
    A(l("      meta.NAME.stackoverflow.dev.demo."), internal_ip),  
    A(l("      talent.NAME.stackoverflow.dev.demo."), internal_ip_win),  
    //  
    A(l("      NAME.stackexchange.dev.demo."), internal_ip),  
    A(l("      *.NAME.stackexchange.dev.demo."), internal_ip),  
    //  
    A(l("      NAME.stacksnippets.dev.demo."), internal_ip),  
    //  
    A(l("      cdn.NAME.sstatic.dev.demo."), internal_ip),  
  ]  
}
```

```
PUBPLAT_INSTANCE("ascn-dev", INGRESS_ASCN_DEV, INGRESS_ASCN_DEV_WIN),  
PUBPLAT_INSTANCE("load-test", INGRESS_LOAD_TEST, INGRESS_LOAD_TEST_WIN),  
PUBPLAT_INSTANCE("main-stg", INGRESS_MAIN_STG, INGRESS_MAIN_STG_WIN),  
PUBPLAT_INSTANCE("main-test", INGRESS_MAIN_TEST, INGRESS_MAIN_TEST_WIN),
```


Builders: DMARC / DKIM / SPF

The DKIM_BUILDER helps assemble a DKIM record.

```
D("example.com", REG_MY_PROVIDER, DnsProvider(DSP_MY_PROVIDER),
  DKIM_BUILDER({
    label: "alerts",
    selector: "k2",
    pubkey: "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDC5/z4L",
    flags: ['y'],
    hashtypes: ['sha256'], // **COMMENT**
    keytype: 'rsa',
    servicetypes: ['email'],
    ttl: 150
  }),
);
```

Output:

```
k2._domainkey.alerts IN TXT "v=DKIM1; k=rsa; s=email; t=y; h=sha256; \
    p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDC5/z4L"
```

Optimizers: SPF

```
D("example.com", REG_MY_PROVIDER, DnsProvider(DSP_MY_PROVIDER),
  A("@", "10.2.2.2"),
  MX("@", "example.com."),
  SPF_BUILDER({
    ttl: "5m",
    parts: [
      "v=spf1",
      "ip4:198.252.206.0/24", // ny-mail*
      "ip4:192.111.0.0/24", // co-mail*
      "include:_spf.google.com", // GSuite
      "include:mailgun.org", // Greenhouse.io
      "include:spf-basic.fogcreek.com", // Fogbugz
      "include:mail.zendesk.com", // Zendesk
      "include:servers.mcsv.net", // MailChimp
      "include:sendgrid.net", // SendGrid
      "include:450622.spf05.hubspotemail.net", // Hubspot (Ticket# SREREQ-107)
      "-all"
    ],
    flatten: [
      "spf-basic.fogcreek.com",
      "450622.spf05.hubspotemail.net"
    ]
  })
);
```

Reverse IP (in-addr.arpa)

Automatically generate RFC 4183-compliant in-addr.arpa strings.

A:

```
D("0.111.192.in-addr.arpa",  
  PTR("1", "one.stackoverflow.com."),  
  PTR("2", "two.stackoverflow.com."),  
);
```

B:

```
D(REV("192.111.0.0/24"),  
  PTR("1", "one.stackoverflow.com."),  
  PTR("2", "two.stackoverflow.com."),  
);
```

Reverse IP with variables

```
var SERVER_A = "192.111.0.4";  
var SERVER_B = "192.111.0.9";  
  
D("example.com",  
  A("www", SERVER_A),  
  A("demo", SERVER_B),  
);  
  
D(REV("192.111.0.0/24"),  
  PTR( REV(SERVER_A), "www.stackoverflow.com."),  
  PTR( REV(SERVER_B), "demo.stackoverflow.com."),  
);
```

Comments!

```
D("example.com",  
  
  // TICKET-123: Why is this here? Blah blah blah blah blah blah blah blah blah  
  // Blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah.  
  // Blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah.  
  // Blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah.  
  // Blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah.  
  // Blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah.  
  // blah blah blah blah blah.  
  CNAME("myalias", "www.stackoverflow.com."),
```

Integrate into Github Actions

- <https://github.com/StackExchange/dnscontrol-action>

```
- name: call dnscontrol action
  uses: StackExchange/dnscontrol-action@f227f6014445e9a45ca0e75d80296a4c7f796884
  with:
    cmdargs: preview
    post_pr_comment: false
    post_summary: true
    check: false
    creds_file: creds.json
```

Updates via PR

StackEng / ExternalDNS

Type to search

CodeIssuesPull requests1ActionsProjectsWikiSecurityInsightsSettings

feat(FooApp) Add IP address for control panel #1345

Open

timoncelli wants to merge 2 commits into `main` from `1xain_dev`

Conversation1

Commits2

Checks1

Files changed1

timoncelli commented 3 minutes ago · edited

Issue

Developers creating FooApp need an A record pointing fooapp-control.stackoverflow.com to 104.18.32.10

Resolution

Add it.

feat(fooapp) Add IP address

8825bdf

Reviewers

developer-platform

At least 1 approving review is required to merge this pull request.

Still in progress? [Convert to draft](#)

Assignees

No one—[assign yourself](#)

Labels

None yet

Projects

None yet

PR Diff

feat(FooApp) Add IP address for control panel #1345

timoncelil wants to merge 2 commits into main from icare_devs

Conversation 1Commits 2Checks 1Files changed 1

Changes from all commitsFile filterConversationsJump to0 / 1 files viewedAsk CopilotReview in codespaceReview changes

disconfig.js

@@ -1843,8 +1843,9 @@	@@ 0:"stackoverflow.com", AOS_C3COLORB4,
1843	1843
1846	1846
1847	1847
	1848
	1849
	1850
1848	1851
1849	1852
1850	1853

PR Automatically add comment



github-actions bot commented 7 minutes ago · edited ·

▼ DNSControl Preview Results (EXTERNAL)

DNS Control Preview Results (EXTERNAL)

(Uses default GHA runners)

```
CONCURRENTLY checking for 175 zone(s)
SERIALLY checking for 8 zone(s)
Waiting for concurrent checking(s) to complete...DONE
CONCURRENTLY gathering records of 175 zone(s)
SERIALLY gathering records of 8 zone(s)
Waiting for concurrent gathering(s) to complete...DONE
***** Domain: stackoverflow.adultblock
***** Domain: askstack.ai
***** Domain: stackoverflow.ai
***** Domain: stackad.blog
***** Domain: stackoverflow.blog
***** Domain: stackoverflow.business
***** Domain: stackexchange.ca
***** Domain: stackoverflow.ca
***** Domain: stackoverflow.careers
***** Domain: stackexchange.cloud
***** Domain: stackoverflow.cloud
***** Domain: collectivexonstackoverflow.co
***** Domain: discover-stackoverflow.co
***** Domain: explore-stackoverflow.co
***** Domain: get-stackoverflow.co
***** Domain: stack-teams.co
***** Domain: stackbusiness.co
```



Development



Successfully merging this pull request may close these issues.

None yet

Notifications

Customize

Unsubscribe

You're receiving notifications because you're watching this repository.

1 participant



Lock conversation

PR Automatically add comment

```
##### Domain: stackenterprise.com
##### Domain: stacks.com
##### Domain: stackexchange.com
##### Domain: api.stackexchange.com
##### Domain: chat.stackexchange.com
##### Domain: data.stackexchange.com
##### Domain: chat.sockets.stackexchange.com
##### Domain: qs.sockets.stackexchange.com
##### Domain: stackinternal.com
##### Domain: stackoverflow.com
##### Domain: stackoverflow.com
1 correction (cloudflare_is_prod)
#1: + CREATE foopps-control.stackoverflow.com A 184.10.32.10 proxyfalse ttl=300
##### Domain: dev.careers.stackoverflow.com
##### Domain: dev.talent.stackoverflow.com
##### Domain: stackoverflow-bd.com
##### Domain: stackoverflow-bdr.com
##### Domain: stackoverflow-business.com
##### Domain: stackoverflow-enterprise.com
##### Domain: stackoverflow-sales.com
##### Domain: stackoverflow-sdr.com
##### Domain: stackoverflow-teams.com
##### Domain: stackoverflowbusiness.com
##### Domain: stackoverflowcareers.com
##### Domain: stackoverflowdevinsights.com
##### Domain: stackoverflowenterprise.com
##### Domain: stackoverflowevents.com
##### Domain: stackoverfloworteams.com
```

PR Approve and merge



Changes approved

2 approving reviews by reviewers with write access.



2 approvals >



1 pending review >



All checks have passed

1 successful check



No conflicts with base branch

Merging can be performed automatically.

Merge pull request



You can also merge this with the command line.

[View command line instructions.](#)

Github Actions enables GitOps

What is GitOps?

GitOps is allowing users (usually engineers) to submit PRs instead of tickets.

IaC + PR = GitOps

- Automated testing
- Validation (Guardrails)
- Save your cognitive energy for the important parts
- Automate testing, pushing into production, post-deploy testing

Shifts work to the user

- OLD:
 - You: check syntax
 - You: check content
 - You: deploy to production
 - You: follow-up verification
- NEW:
 - Requester: creates PR to initiate work
 - Automation: check syntax
 - Automation: check content
 - You: Review and approve
 - Automation: deploy to production
 - Requester: follow-up verification

Conclusion

Are you...?	You should...	Because you'll...	Everyone will be impressed...
owner of many domains?	Manage them with DNSControl	Save time, reduce complexity, assure consistency	faster updates, more consistent, correct on the first try
a team responsible for DNS zone updates	Use DNSControl with Github Actions	Reduce toil, shift work to others	DNS updates are now self-service
a DNS Service Provider	Add support for your API to DNSControl	Delight your customers!	How hip and cool you are!

- www.dnscontrol.org
- Github: <https://github.com/StackExchange/dnscontrol>

Thank you

Thomas A. Limoncelli (Tom)

27 Oct 2025

tlimoncelli@stackoverflow.com