AVOIDING DNS PAIN
AVOIDING DNS PAIN
ABOUT ME

Kieran Jacobsen (he/him)

Twitter/GitHub: @kjacobsen
Website: poshsecurity.com
Day Job: Head of Business Systems at Phocas Software
Industry Roles:
• Microsoft MVP for Cloud and Datacenter Management
• GitKraken Ambassador
Multiple Microsoft services fall offline due to a DNS bloop

It's not DNS

There's no way it's DNS

It was DNS

AWS blames major outage on "automated activity" that triggered "unexpected behavior" in internal network

Will make its status page multi-region so that it actually works during outages

A DNS outage just took down a large chunk of the internet

Zack Whittaker @zackwhittaker / 2:55 AM GMT+10 • July 23, 2021

Slack is down for some people, and of course, the problem is DNS

If you've been having trouble contacting co-workers, this may be why

By Mitchell Clark | Updated Sep 30, 2021, 4:18pm EDT

PSA: Facebook, Instagram, Messenger, and WhatsApp went down for 6+ hours; here's why [U]

Chance Miller • Oct. 4th 2021 1:30 pm PT 🦜 @ChanceHMiller
DNS SECURITY CONCERNS

- CNAME entry: greatapp.contoso.com
- app-contogreat-dev-001.azurewebsites.net
  - Normal operations

404

- CNAME entry: greatapp.contoso.com
- app-contogreat-dev-001.azurewebsites.net
  - Dangling DNS

- CNAME entry: greatapp.contoso.com
- app-contogreat-dev-001.azurewebsites.net
  - Subdomain taken over

Website resource deprovisioned
DNS CHANGES CAN BE SLOW
TRACEABILITY
DNS AS A CODE WITH DNSCONTROL

- DNSControl
- Developed and supported by Stack Exchange team
- JavaScript based DSL
- Easy to follow syntax
- Comments help describe records

```javascript
D('planetpowershell.com', REG_DNSIMPLE, DnsProvider(DNS_CLOUDFLARE),
  SPF_BUILDER({
    label: '@',
    parts: [
      'v=spf1',
      'include SPF protection outlook.com', // Office 365
      '-all' // Servers not compliant with SPF will fail and be rejected
    ],
    ttl: one_hour
  }),

  DMARC_BUILDER({
    label: '@',
    policy: 'reject',
    ttl: one_hour,
    rua: [
      'mailto:re+mo@xmlhlmq@dmarc.postmarkapp.com'
    ],
  }),

  // Domain uses Office 365 so call the record builder function.
  Office365Records('planetpowershell.com', 'ms63098003', 'kieran365'),

  CAA_BUILDER({
    label: '@',
    iodef: 'mailto:caa@planetpowershell.com',
    ttl: one_hour
  })

  // Production Site
  A('@', [''], cloudflare_on),
  A('www', [''], cloudflare_on),

  // Development Site
  A('dev', [''], cloudflare_on),
  A('demo', [''], cloudflare_on)
)```
// Google verification code
TXT('@', 'google-site-verification=cOCEohtWpoLaMz8kDb07P11-_W4MSpJRCQkk7WhilW7Y', one_hour),

//GitHub Domain Verification
TXT('_github-challenge-planetpowershell', '18c69905f7', one_hour),

// LinuxConf TXT Record
TXT('hello', 'Hello LinuxConf!')
Create Pull Request

Room Repo
- GitHub
  - planetpowershell/DNS
  - planetpowershell/DNS

Branch
- main

Template
- pull_request_template.md
- pick

Title
- Add LinuxConf AU Record

Description
- This template is required. Any request that does not include enough information may be closed at the maintainers' discretion.
- If you are updating `.disconf.d` have you split an IP between the brackets on each line to confirm:
  - [ ] Checked that `.disconf.d` records have the trailing dot as described here (https://github.com/planetpowershell/planetpowershell/blob/master/.disconf/Why-the-dot).
  - [ ] Checked you have used single quotes.
  - [ ] Confirmed there are no dangling DNS entries.
  - [ ] Confirmed any `~` `SPF` changes do not violate the DNS request limits (10 requests).
  - [ ] Confirmed you haven't checked in any secrets in `.disconf.d`.

### Description of the Change

Add TXT record for LinuxConf AU.
Add TXT record for LinuxConf #1

Requirements

- This template is required. Any request that does not include information may be closed at the maintainers’ discretion.
- If you are updating `dnsconfig.js`, have you (put an X between each line to confirm):
  - Checked that `cname` records have the trailing dot as described in the spec.
  - Checked you have used single quotes.
  - Confirmed there are no dangling DNS entries.
  - Confirmed any `spec` changes do not violate the DNS registries’ requests.
  - Confirmed you haven’t checked in secrets in `credentials.js`.

Description of the Change

Adds TXT Record for Linux Conf

Run DNSControl Preview

```
Starting: Run ***Control Preview

Task    : Docker
Description : Build, tag, push, or run Docker images, or run a Docker command
Version   : 1.194.0
Author    : Microsoft Corporation
Help      : https://docs.microsoft.com/azure/devops/pipelines/tasks/build/docker

/usr/bin/docker run --rm -v /home/vsts/work/1/s://dns stackexchange/dnscontrol dnscontrol preview

********** Domain: ***.com
----- Getting nameservers from: cloudflare
----- *** Provider: cloudflare...
1 correction
#1: CREATE record: hello TXT 1 Hello LinuxConf!
----- Registrar: dnsimple...
0 corrections
Done. 1 corrections.
Finishing: Run ***Control Preview
```
REDUCE DNS COMPLEXITY AND IMPROVE SECURITY

SPF_BUILDER({
  label: "@",
  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:spf-basic.fogcreek.com", // Fogbugz
    "include:450622.spf05.hubspotemail.net",
    "~all"
  ],
  flatten: [
    "spf-basic.fogcreek.com", // Being deprecated. Low risk if:
    "450622.spf05.hubspotemail.net" // Unlikely to change without
  ]
})

DMARC_BUILDER({
  policy: 'reject',
  rua: [
    'mailto:mailauth-reports@example.com'
  ]
})

CAA_BUILDER({
  label: "@",
  iodef: "mailto:test@domain.tld",
  iodef_critical: true,
  issue: [
    "letsencrypt.org",
    "comodoca.com"
  ],
  issuewild: "none"
})
DNS PROVIDER RESILIENCE AND MIGRATION

```python
1 D('example.com', REG, DnsProvider('R53'), DnsProvider('GCloud'),
2     A('@', '1.2.3.4')
3 )
4
5 D('example2.com', REG, DnsProvider('R53', 2), DnsProvider('GCloud', 2),
6     A('@', '1.2.3.4')
7 )
8
9 D('example3.com', REG, DnsProvider('R53'), DnsProvider('GCloud', 0),
10    A('@', '1.2.3.4')
11 )
```
<table>
<thead>
<tr>
<th>USEFUL LINKS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advice on Mitigating DNS Infrastructure Tampering</strong></td>
</tr>
<tr>
<td><strong>DNS Squatting with Azure App Services</strong></td>
</tr>
<tr>
<td><strong>Managing DNS with DNSControl, CloudFlare, DNSimple, GitHub, VSTS, Key Vault, and Docker!</strong></td>
</tr>
<tr>
<td><strong>My DNSControl Accelerator Package</strong></td>
</tr>
<tr>
<td><strong>Getting Started With DNSControl</strong></td>
</tr>
<tr>
<td><strong>DNSControl Migration Guide</strong></td>
</tr>
<tr>
<td><strong>GitKraken (referral)</strong></td>
</tr>
</tbody>
</table>
Client: Hello, I want to hear a DNS joke.

Resolver: I personally know nothing, but here is a list of best jokers:
- a.knows.jokes
- b.knows.jokes
- c.knows.jokes

Client: Okay, b.knows.jokes, I want to hear a DNS joke.

b.knows.jokes: I am terrible at joking, as I only know a bunch of people who tell jokes, but here is a guy who once told me a DNS joke:
- dns.joker

Client: Okay, dns.joker, I want to hear a DNS joke.

dns.joker: I actually just replay jokes from others, go ask dns.jester

Client: Okay, dns.jester, I want to hear a DNS joke.

dns.jester: I actually just replay jokes from others, go ask dns.joker