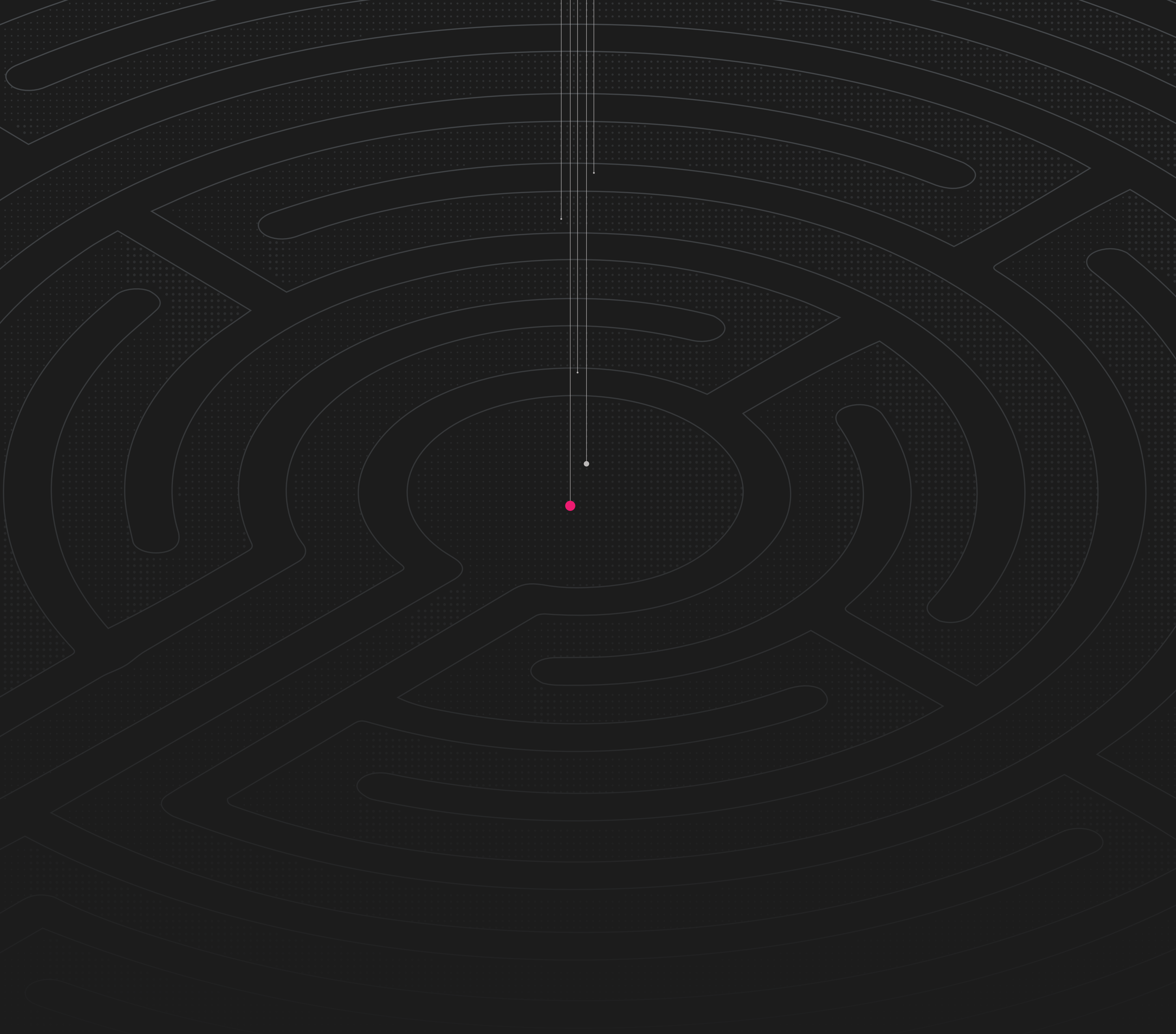


Domain Registrations, Delegations, and DNS.

WHITE PAPER 2017.07.19

Network outages, more often than not, are the result of human error at some point in the configuration and change management process. Nowhere are those potential errors more visible than when a domain registration or delegation goes awry and erases or limits your online presence. Your network issue may not be as visible or as extensive as the 2017 AWS S3 incident; but it will still have an impact on your organization and the only insight you may have is a longer than usual resolution time for your website, or customers complaining they cannot reach your website at all.

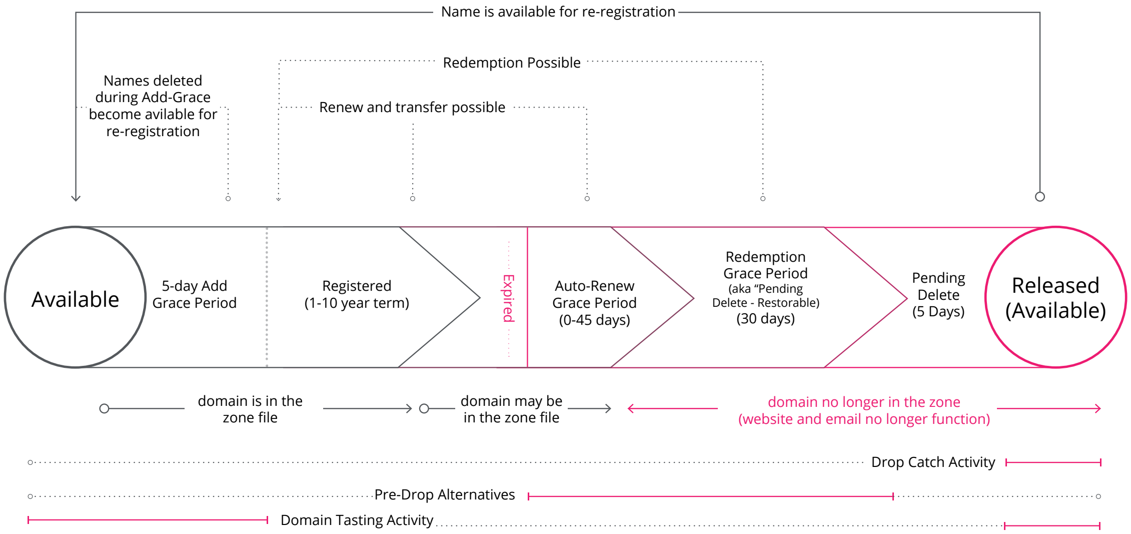
The magnitude and near term impact of this type of issue should not be underestimated. Gartner proposes that through 2020, organizations that do not govern changes will experience 50% more service incidents than those that do. (Gartner, 2016) Understanding the domain registration and delegation process, pitfalls, and areas of potential error will enable your organization to put best practices into place. Establishing and following best practices in the arena of DNS operations and change management is essential to mitigate your risk in this area.

A BRIEF OVERVIEW OF REGISTRATIONS AND DELEGATIONS

Domain registration, the purchase of a specific domain name, and domain delegation, the assignment of authoritative nameservers for your domain, are central to your online presence. Understanding how to establish, maintain, and protect the registration and delegation of your domain name will protect your online presence.

Domain Registrations, Renewals, and Expiration

The lifecycle of a domain name involves its purchase (registration), ongoing ownership (renewal), and release for ownership by another (expiration). The following graphic from ICANN visually displays a summary of this lifecycle.


Name is available for re-registration
Redemption Possible
Renew and transfer possible
Names deleted during Add-Grace become avilable for re-registration
Available
5-day Add Grace Period
Registered (1-10 year term)
Expired
Auto-Renew Grace Period (0-45 days)
Redemption Grace Period (aka "Pending Delete - Restorable) (30 days)
Pending Delete (5 Days)
Released (Available)
domain is in the zone file
domain may be in the zone file
domain no longer in the zone (website and email no longer function)
Drop Catch Activity
Pre-Drop Alternatives
Domain Tasting Activity

ICANN rules state that your registrar is required to send at least 2 notices prior to the actual expiration of your gTLD domain. It is important that you verify and update, if necessary, your information with your registrar to make sure you can be easily contacted when your registrar sends these notices. You can transfer or renew your domain prior to expiration. This will help you avoid dealing with potential post-expiration grace periods.

Expiration of a domain name, despite the finite term, takes a period of time and involves a few different stages. After the expiration date, the registry for the specific TLD where the name was registered may offer an automatic renewal grace period, shown in the graphic as Auto-Renew Grace Period. This still allows for the domain to be renewed by the respective owner, but may stop serving queries at the TLD level, depending on that registry's policies. During the automatic renewal grace period, domain names may be renewed without a financial penalty and restored to operation quickly. After the automatic renewal grace period ends, the domain enters a new phase known as the redemption grace period. During the redemption grace period, or "Pending Delete - Restorable" phase, the domain registration information is locked within the TLD, and requires additional fees to restore the registration for renewal. The final phase before a domain name is released for a new registration is the Pending Delete phase. During the Pending Delete phase, there is no way to restore the domain name to its previous registration and after five days, the name will be made publicly available for purchase as if it had never been registered before.

NOTE: ccTLDs, top level domains established for individual countries and some territories, may follow slightly different policies based on their representative country.

Best Practices for Domain Name Management

European corporate brand and domain management consultant, eBrand Services, recommends these 7 best practices for protecting your domain names as a broader strategy to protect your corporate brand.

1. View Your Domain as a Corporate Asset - As part of your trademark and brand identity, your domain name(s) are an asset for your company.
2. Centralize Domain Name Management - Choose a single, accredited registrar for your DNs to reduce costs and risks and have a single-point of contact (corporate administrative contact).
3. Perform Systematic Domain Name Portfolio Audits - After your audit is finished, develop policies and procedures for systematic renewals and acquisition of new domains.
4. Audit and Centralize Your Trademark Portfolio at the Same Time - Trademarks as well as domain names are a central part of your corporate branding. Pay the same attention to your trademark registrations as you do to your domain name registrations.
5. Monitor Domain Registration Information for Guaranteed Renewals - Renewing your DNs for periods longer than the usual two years will ease the administrative burden.
6. Stay Informed About New Threats - Devote resources to monitoring the threats on the horizon, assessing the potential harm, developing a plan and taking action to protect your DN portfolio asset.
7. Monetize Domain Names - The commercial and marketing use of domain names is a key element for brand valuation

Domain Delegation

In the context of the DNS, delegation is the assignment of name servers to a given domain name. This information tells the respective registry where the authoritative servers live for a domain, so that DNS resolution can happen. See NS1's technical article Ready, Set, Delegate for more information on properly delegating DNS domains.

IDENTIFYING ERRORS IN DNS REGISTRATION OR DELEGATION

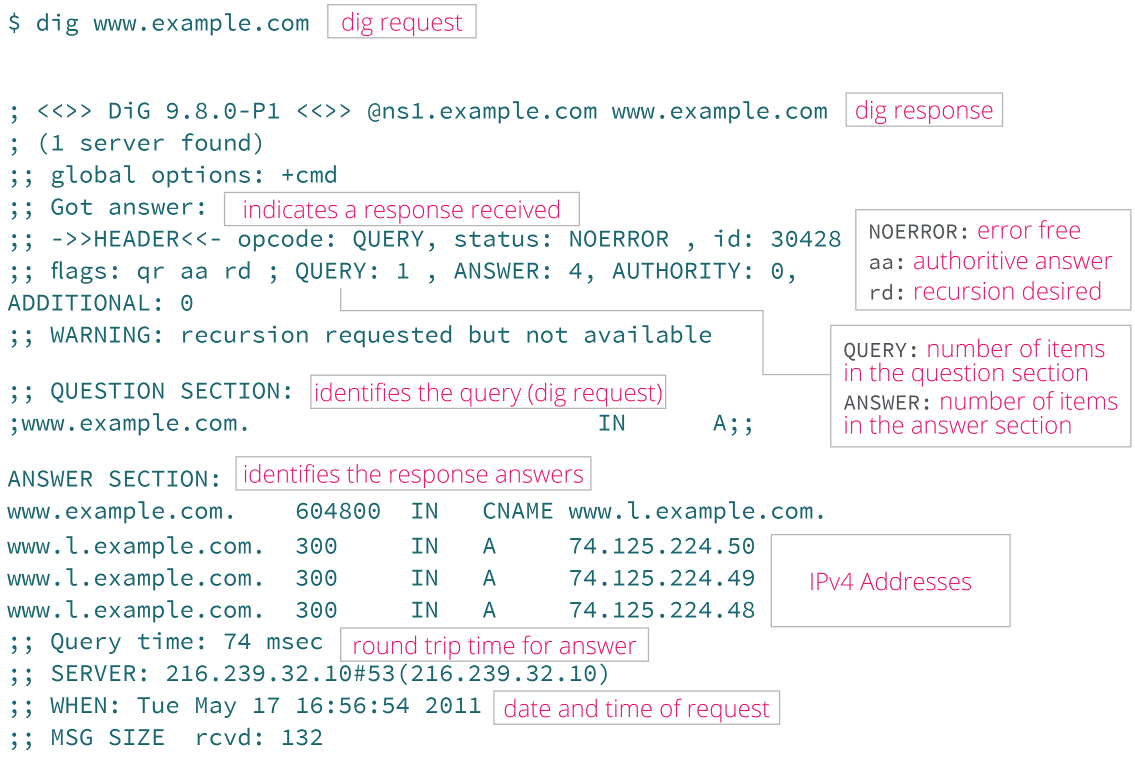
If you have health monitoring tools enabled for your network, take advantage of them to notify you of DNS issues as they arise. While there are a number of ways that DNS errors can manifest, there are a few that are significant indicators of an issue. These symptoms include, but are not limited to the following: slowness in the initial DNS lookup, web browser requests return an error indicative of a failed DNS lookup, email stops coming into your company, or sent email is not received by the intended recipient.

Your organization's operations team has procedures for handling incidents, troubleshooting a situation, and arriving at a root cause in order to repair the issue. Handling DNS issues are no different, but they may involve tools not always used for internal issues. `dig` is an extremely useful tool for analyzing your current DNS setup and uncovering issues in DNS registration or delegation.

The following sections include (1) a properly setup DNS configuration with explanations of the `dig` response, (2) two examples of `dig` responses showing an issue with DNS, (3) one explanation of an unusual DNS error and how to resolve that situation, and finally (4) steps to follow if you suspect your DNS delegation could be the source of your issue.

NOTE: Each `dig` is for example purposes only. For more information and examples on using `dig` you can see our articles Decoding Dig Output and Using dig +trace to Understand DNS Resolution from Start to Finish.

Anatomy of a Normal `dig` Request and Response



```
$ dig www.example.com

; <<>> DiG 9.8.0-P1 <<>> @ns1.example.com www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR , id: 30428
;; flags: qr aa rd ; QUERY: 1 , ANSWER: 4, AUTHORITY: 0,
ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.example.com.                         IN      A;;

ANSWER SECTION:
www.example.com.    604800   IN    CNAME www.l.example.com.
www.l.example.com.  300      IN    A     74.125.224.50
www.l.example.com.  300      IN    A     74.125.224.49
www.l.example.com.  300      IN    A     74.125.224.48
;; Query time: 74 msec
;; SERVER: 216.239.32.10#53(216.239.32.10)
;; WHEN: Tue May 17 16:56:54 2011
;; MSG SIZE  rcvd: 132
```

dig request
dig response
indicates a response received
NOERROR: error free
aa: authoritive answer
rd: recursion desired
QUERY: number of items in the question section
ANSWER: number of items in the answer section
identifies the query (dig request)
identifies the response answers
IPv4 Addresses
round trip time for answer
date and time of request

Examples of DNS Errors Shown in `dig`

Example 1: Domain Not Registered or Invalid at the registrar

In the query answer, notice the field status: NXDOMAIN (shown in red). This identifies the domain example.com as not registered or invalid. This is a common occurrence after a domain has been registered and the new name hasn't propagated within the TLD.

```
$ dig example.com


; <<>> DiG 9.8.3-P1 <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 55793
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL:
0


;; QUESTION SECTION:
;example.com.                       IN    A


;; AUTHORITY SECTION:
com.                        900     IN    SOA    a.gtld-servers.
net. nstld.verisign-grs.com. 1498063217 1800 900 604800 86400

;; Query time: 31 msec
;; SERVER: 50.207.245.2#53(50.207.245.2)
;; WHEN: Wed Jun 21 12:40:34 2017
;; MSG SIZE  rcvd: 103
```

Example 2: Invalid or not propagated at DNS provider

In the event that a zone has not propagated at the DNS provider, digging a name will result in a slightly different error known as SERVFAIL. The SERVFAIL response is indicative of an issue at the DNS provider, not the registrar as in Example 1.

```
$ dig example.com

; <<>> DiG 9.8.3-P1 <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 57724
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL:
0

;; QUESTION SECTION:
;example.com.               IN      A


;; Query time: 147 msec
;; SERVER: 50.207.245.2#53(50.207.245.2)
;; WHEN: Wed Jun 21 12:48:35 2017
;; MSG SIZE  rcvd: 33
```

Example 3: A Special Case of a DNS Name Resolution Error

There is a special case where the domain delegation can be correct and the nameservers answer properly when their IP address is queried, but not their domain name. This situation will happen if the nameserver answering for a domain is inside the domain. For example if the nameserver ns1.example.net. is answering for example.net.

In this case a special record called a “glue record” must be created at your registrar with the nameserver and its IP address. This glue record will be given out as part of the “Additional Section” by the TLD server when a resolver requests any name inside example.net.

If a request is made and this glue record is not present, the resolver will deadlock, causing a SERVFAIL. When you add the glue record at the registrar, this deadlock will be avoided and your nameservers will be able to properly resolve the domain name.

What to Check When An Error Is Suspected

1. Identify the domain’s authoritative nameservers:
   ```
   dig NS example.com
   ```
2. Check each authoritative nameserver returned in #1: (replace authoritativenameserver1 with the domain name of your authoritative nameserver)
   ```
   dig example.com. @authoritativenameserver1
   ```
3. Check your nameserver delegation:
   ```
   dig example.com +trace
   ```
   NOTE: If the last server in the +trace check shows a timeout or NXDOMAIN, that can indicate an improper delegation at the registrar.
4. Check each authoritative nameserver (#2) against the names present in the dig +trace output (#3).
   NOTE: They must match exactly, character for character. If they do not, edit the delegation at your registrar to resolve the error.

BEST PRACTICES

All configuration changes made to a network represent an intrinsic risk. (Gartner, 2017) This risk is mitigated by adhering to a comprehensive change management process addressing all changes whether automated or manual. Changes should be properly planned, documented, executed and verified. DNS is a critical part of your network infrastructure and so changes to your DNS should be part of the change management process.

Here is a list of recommended best practices to protect your network:

1. Verify your Registrant information with WhoIs.ICANN.com and ensure your information is kept up to date for every domain.
    - a. If you use a domain protection service, where the service's information appears instead of your own, make sure their information is correct and that your information is correct in their records. Make sure you do this for every domain.
    - b. Not every domain registration expires at the same time. If a parent domain registration expires, the subdomains won't resolve even if their domain registration is up to date.

    NOTE: Owning a few domain names can present a challenge keeping track of when each domain renews. Some methods to keep this information organized include: calendar alerts, spreadsheets, or software tools such as Domain Punch Pro and DomainTools Monitors.
2. Implement network health monitoring tools to keep watch over your assets, including DNS.
3. Automate DNS changes as much as possible.
4. Implement an internal policy that no one touches the live environment.
    - a. Changes should be made using pre-authorized automated scripts only.
    - b. Any change to the live environment, scripted or otherwise, should be automatically recorded in a work log so changes can be traced.

Cited Sources and Additional Resources

ICANN icann.org, whois.icann.org

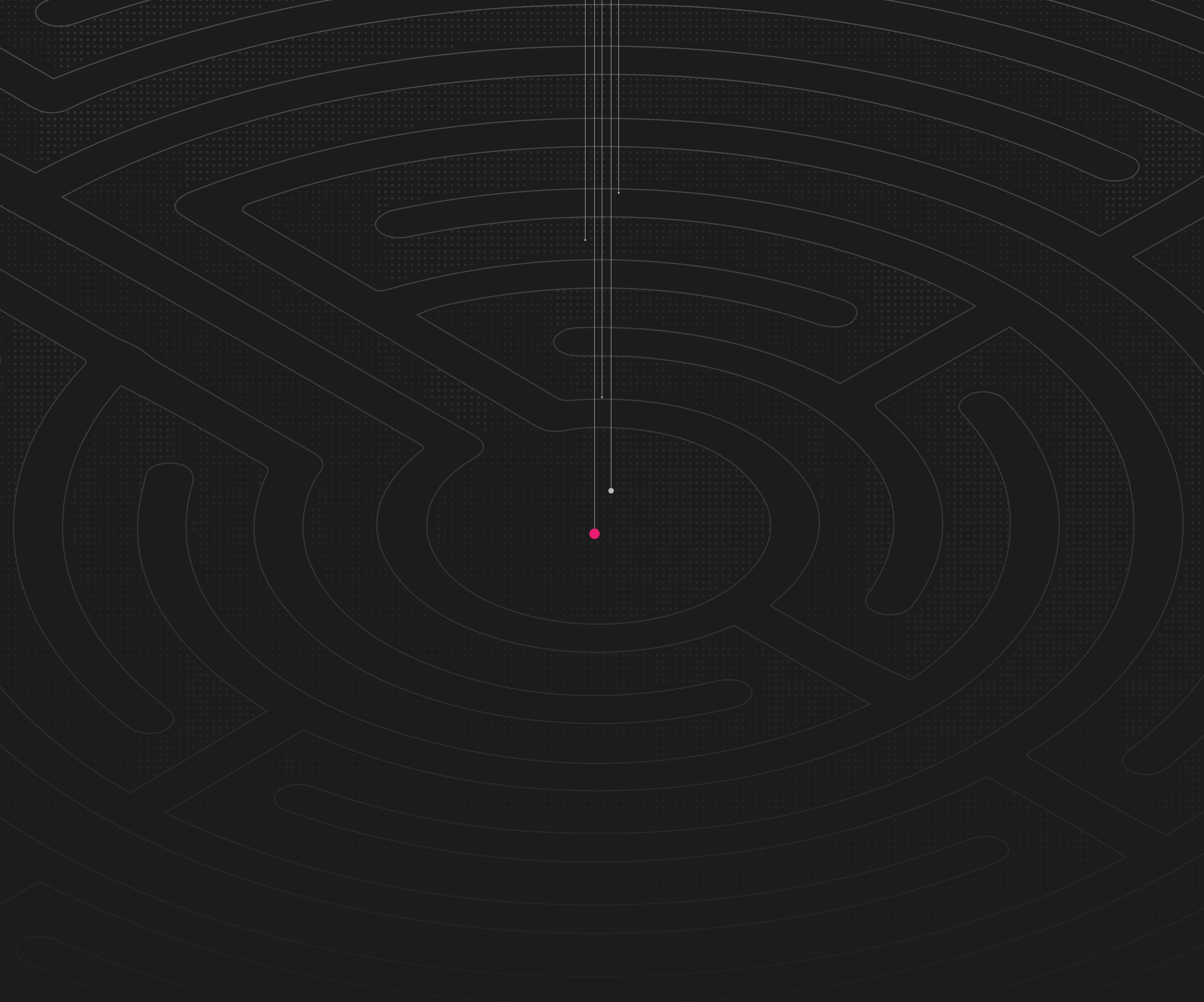
WhoIs whois.com

Albitz, Paul and Liu, Cricket. Delegation DNS and BIND, 4th edition. O'Riley publishers. https://nnc3.com/mags/Networking2/dns/ch02_03.htm. Downloaded June 19, 2017

Bhalla, Vivek and Ganguli, Sanjit, Analysts. Gartner ID: G00299951. Market Guide for Network Automation. Downloaded June9, 2017. Published: March 28 2017.

EBrand Services - Domain Name Management - Best Practices
Our TOP 7 domain name management Best Practices. Downloaded June 19,2017

Head, Ian and Williams, David Paul, Analysts. Gartner ID: G00310306. Five Best Practices for Effective Change Control of the DevOps Toolchain Downloaded June 9, 2017 Published: September 13, 2016



Implementing best practices for network change management, including the use of a robust managed DNS API will help mitigate risk in this area full of human error potential. By paying attention to the small details of domain registrations, domain delegation, and DNS technology you ensure your organization's online presence will be there to serve your customers and employees now and in the future.