

DNS & DNSSEC

operational best practices

Sleep better at night with KINDNS in your network!



These materials are licensed under the Creative Commons Attribution 4.0 International licence.
<http://creativecommons.org/licenses/by-nc/4.0/>



UNIVERSITY OF OREGON



Note to SANOG PC

- This is a 25-minute talk, but I can make it a bit shorter to fit in 20 minutes too. I can also make it longer. Whatever we have time for.
- I would pick one or two best practices to highlight. At SANOG I would probably spend most of my time talking about open resolvers. There are 109,425 in BD, 189,764 in IN and 36,816 in PAK as I type this. (BT, LK and NP are not as bad.)

Acknowledgements

- NSRC funds my time and my travel
- KINDNS is an ICANN initiative

KINDNS: background

KINDNS /'kaɪndnəs/ (noun) **K**nowledge-Sharing and **I**ntantiating **N**orms for **D**NS and **N**aming **S**ecurity

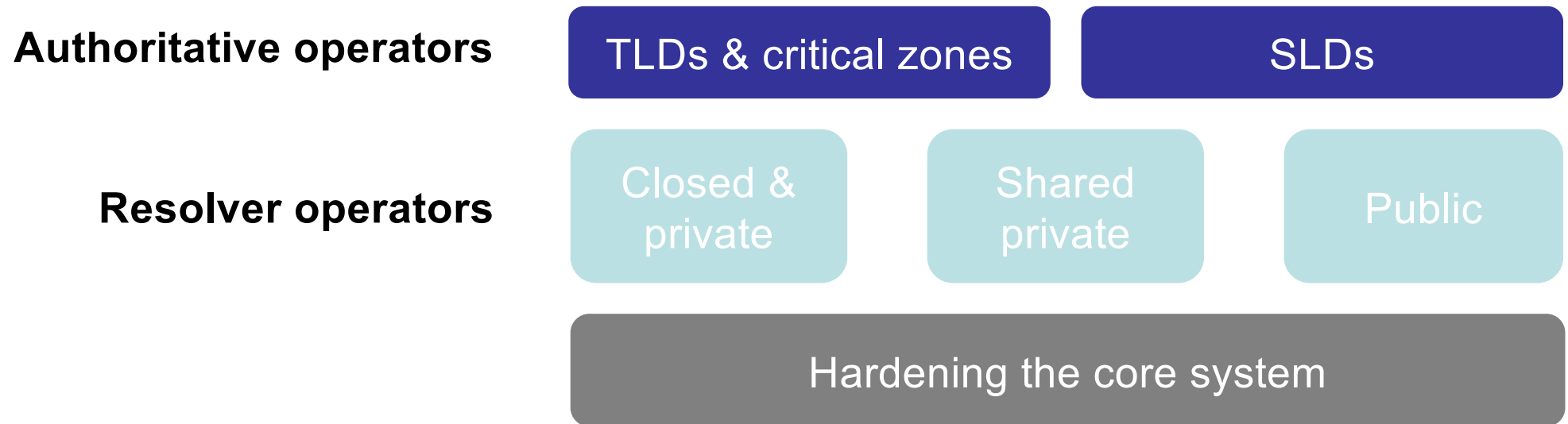
A simple framework that can help a wide variety of DNS operators, from small to large, to follow both the evolution of the DNS protocol and the best practices that the industry identifies for better security and more effective DNS operations.

See also: <https://kindns.org>

What kind of DNS operator are you?

- KINDNS “core guidelines” for everyone
- Additional guidelines for different deployments:
 - TLDs and critical zones
 - Public recursive resolvers
 - Other second-level domains
 - Shared recursive resolvers
 - Private infrastructure not reachable from the open internet
- No “One Size Fits All” checklists!

KINDNS: targeted operators



By joining the KINDNS initiative, DNS operators are voluntarily committing to adhere to the identified practices and act as “goodwill ambassadors” within the community.

Basic common-sense guidelines for DNS operations of all shapes and sizes

CORE GUIDELINES (FOR EVERYONE)



UNIVERSITY OF OREGON



Core guidelines (for everyone)

1. ACLs restrict traffic to DNS servers
2. BCP38 egress filtering
3. DNS servers run DNS and nothing else
4. Access to DNS servers by DNS operators only
5. DNS configuration in revision control
6. Restrict access to management interfaces
7. Management access control with cryptographic keys or 2FA
8. User access control following sound credential management



ACLs restrict traffic to DNS servers

- Only permit DNS traffic inbound
 - TCP & UDP 53
 - If DoT also 853
 - If HTTPS also 443
- Only permit necessary outbound traffic
 - Software updates
 - NTP
 - DNS
- Explicitly block bogon origins
 - Even if blocked at the edge (defence in depth)

BCP38

- We should not need a slide about this in 2024!

DNS servers run DNS and nothing else

- Anything not related to DNS should not be installed
- But you must monitor your DNS installation
 - Anything you need to monitor can be installed
 - Restrict access to monitoring per best practices

DNS configuration in revision control

- See also my “Git for everyone” presentation ☺

Credential management

- No user accounts
- Restrict access to management interfaces
- Management access control with cryptographic keys or 2FA
- User access control following sound credential management

DNSSEC validation is easy – turn it on already!

RECURSIVE RESOLVER OPERATORS



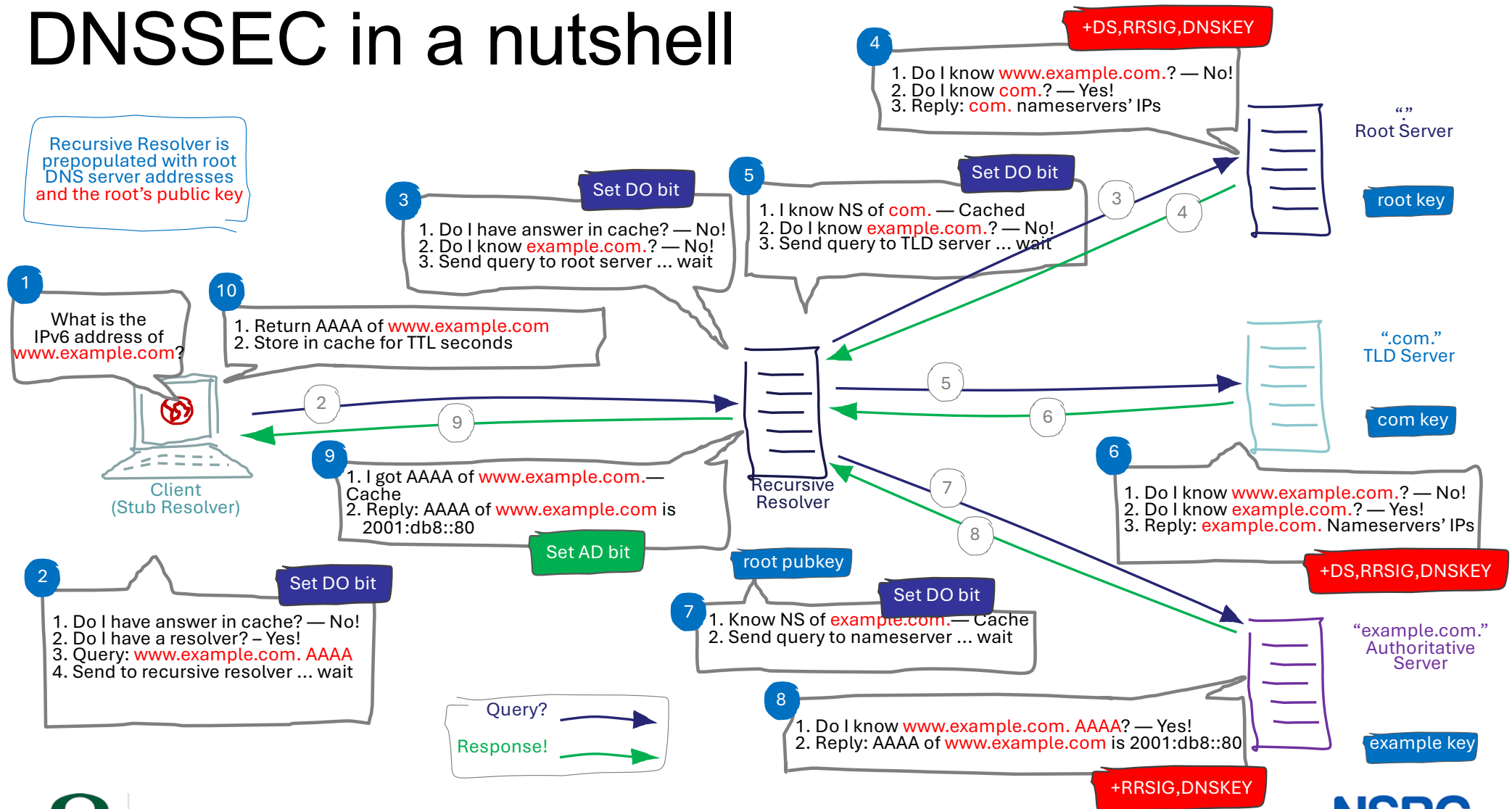
UNIVERSITY OF OREGON



Best practices

1. DNSSEC validation must be enabled
2. Restrict client access to your networks
3. QNAME minimisation must be enabled
4. Resolvers must not coexist with authoritative DNS servers
5. You must have at least two recursive resolvers
6. Monitor your DNS infrastructure
7. (Bonus) DoT and DoH should be supported

DNSSEC in a nutshell



UNIVERSITY OF OREGON

Diagram credit: Md Abdul Awal



Enabling DNSSEC

- BIND: on by default
- Unbound: on by default
- PowerDNS: on by default
- Windows DNS: on by default (allegedly) (but...)

If you don't turn it off, it will Just Work!

Enabling DNSSEC (2)

- There is no reason to turn off DNSSEC validation. Ever.

Restrict access to your networks

- Don't be an open resolver!
- ACL DNS queries at the edge if you can
- Defence in depth: drop queries on your DNS servers too
- (Include BIND/unbound/PowerDNS config files)

Enable QNAME minimisation

- BIND: on by default
- Unbound: on by default
- PowerDNS: on by default
- Windows DNS: **no support**

Cannot run KINDNS-compliant recursive DNS on Windows
(but why would you want to try...?)

Availability and resilience

- Resolvers must not coexist with authoritative DNS servers
- You must have at least two recursive resolvers
- Monitor your DNS infrastructure

Monitoring

- All infrastructure must be monitored
- Remember to monitor both success & failure cases
 - Test your monitoring
- Common metrics
 - Latency
 - Known-good responses
 - DNSSEC “AD” bit

Split-horizon DNS & other edge cases (1)

- Separate DNS views usually a net-negative
 - Consider your need
- Alternative 1: Internal sub-domain
 - Sign as normal
 - Do not resolve outside organisation
 - See relevant KINDNS guidelines
- Alternative 2: Separate internal domain
 - Sign as normal too

Split-horizon DNS & other edge cases (2)

- If you absolutely must use split-horizon
 - Don't sign two copies of your zone!
 - Authenticated denial of existence will bite you
- Consider an internal root of trust
 - Must deploy trust anchor to all internal hosts

DNSSEC is not optional. It's not as hard as it looks.

AUTHORITATIVE ZONE OPERATORS



UNIVERSITY OF OREGON



Best practices

1. Zones must be DNSSEC signed
2. Zone transfers must be restricted to your secondaries
3. Zone file integrity must be monitored
4. Authoritative DNS servers must not coexist with resolvers
5. Your zone must have at least two authoritative resolvers
6. Monitor your DNS infrastructure



Sign your zones

- Avoid administrative overhead of resigning zones
 - BIND does that automatically

```
zone "example.com" in {  
    type master;  
    file "db.example.com";  
    key-directory "/etc/bind/keys";  
    inline-signing yes;  
    auto-dnssec maintain;  
};
```

Where named should look
for the DNSSec key files

BIND keeps unsigned zone
and creates a signed zone

off

Default. Keys are managed manually

allow

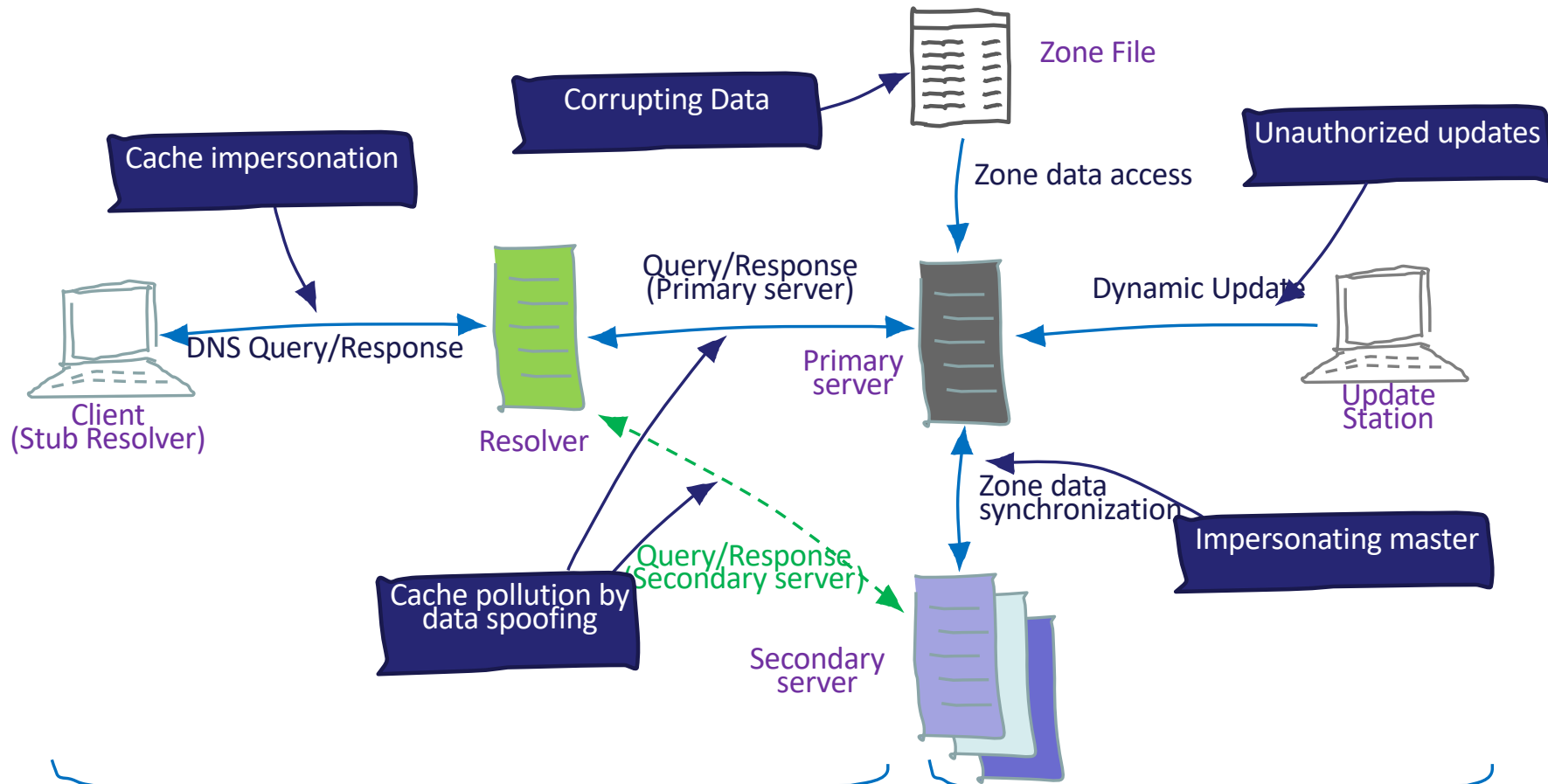
Allows uploading keys and resigning the zone
when user runs "rndc-sign [zone-name]"

maintain

Same as "allow" + automatically
adjusts the keys on schedule



Zone file integrity



Availability and resilience

- Authoritative DNS servers must not coexist with resolvers
- You must have at least two authoritative servers for your zone
- Monitor your DNS infrastructure

Focus on resilience

CCTLDS AND CRITICAL ZONES



UNIVERSITY OF OREGON



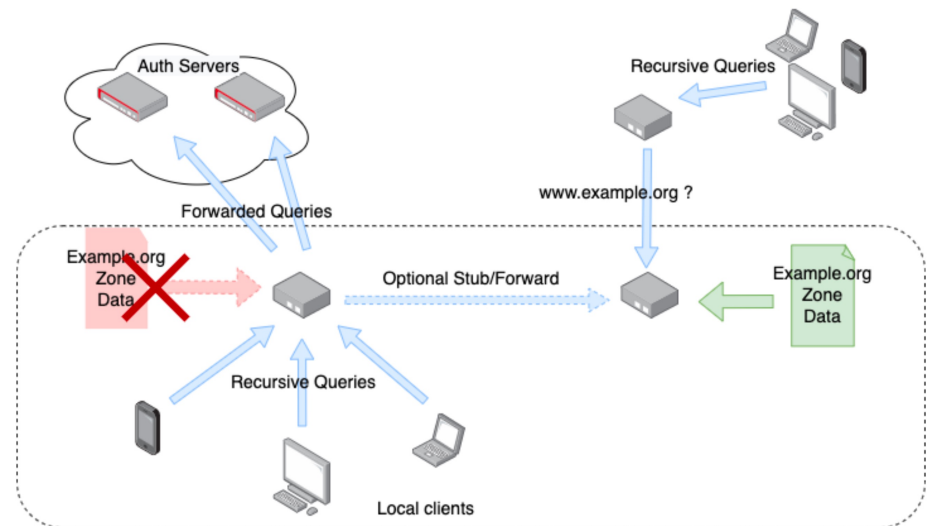
Best practices – same as authoritative

1. Zones must be DNSSEC signed
2. Zone transfers must be restricted to your secondaries
3. Zone file integrity must be monitored
4. Authoritative DNS servers must not coexist with resolvers
5. Your zone must have at least two authoritative resolvers
6. Monitor your DNS infrastructure



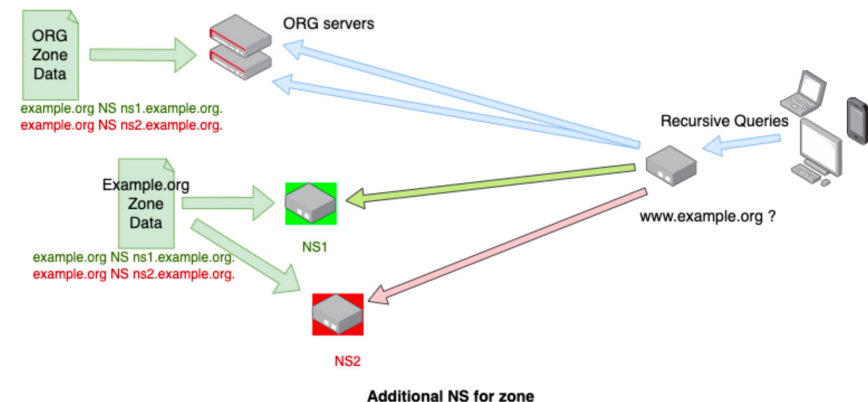
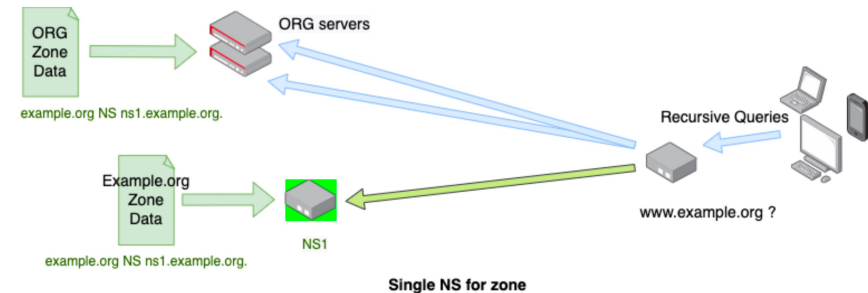
Separation of duties

- Authoritative servers **must not** provide recursive service



At least two distinct name servers

- This is usually a requirement for leaf zones too – but especially important for ccTLDs and critical zones.
- Should go without saying: your name servers *must* always be in sync.
- Ideally these will be anycast clouds.



Software diversity

- Run different software stacks in your organisation
 - FreeBSD, Linux, Solaris,... maybe not Windows
 - BIND, NSD, Knot, PowerDNS
- A critical bug in Linux or BIND should not compromise your operations
- Remember to give each software stack equal exposure
- Automation makes things a little bit easier

Assess your operational practices and correct/adjust unaligned practices

KINDNS SELF-ASSESSMENT



UNIVERSITY OF OREGON



KINDNS self-assessment

- Operators can enrol to participate in one or many categories covered by KINDNS:
 - Participation in KINDNS means voluntarily committing to implement and adhere to agreed norms and practices
 - Participants become goodwill ambassadors and promote best practices

Please do the self-assessment on kindns.org.



Join the KINDNS initiative!

- KINDNS mailing list operated by ICANN:
kindns-discuss@icann.org
- KINDNS wiki:
<https://community.icann.org/display/KINDNS>