We should give up our own DNS aliases, remove the glue records and fall back to the provider ones to make use of IPv6 DNS (and avoid manually tweaking glue records when IPs change). This also affects some external domains. Coordinate with Florian how to get that done.

Either Hetzner or RRPproxy come to mind, the latter one supporting DNSSEC.

History

#1 - 2015-10-17 20:02 - Dennis Roczek
- Category set to Domains and DNS

#2 - 2016-07-20 07:56 - Florian Effenberger
- Target version changed from Pool to Qlater

Shifting to later due to the infra changes

#3 - 2016-11-09 13:04 - Florian Effenberger
- Assignee changed from Alexander Werner to Guilhem Moulin

re-assigning to Guilhem in order to clean up Redmine queues
nothing concrete to do at the moment

#4 - 2017-02-20 14:11 - Florian Effenberger
I think at some point we should give up the DNS aliases and just move to the ISPs canonical name, then this ticket is also handled alongside

#5 - 2017-04-18 13:27 - Florian Effenberger
- Subject changed from IPv6-enabled DNS glue record to switch back to Hetzner DNS incl. IPv6 glue records
- Description updated

#6 - 2017-07-18 11:37 - Florian Effenberger
- Priority changed from Low to Normal
- Target version changed from Qlater to Q4/2017

#7 - 2018-03-15 13:56 - Florian Effenberger
- Target version changed from Q4/2017 to Q3/2018

Although this ticket is old, I think it's not urgent
Let's shift to Q3, we can do so then in light of #2253 (DNSSEC/DANE/TLSA bits for mail)

#8 - 2018-06-11 10:45 - Florian Effenberger
- Subject changed from switch back to Hetzner DNS incl. IPv6 glue records to switch back to Hetzner or RRPproxy DNS and remove glue records
- Description updated

#9 - 2019-05-08 15:24 - Florian Effenberger
Let's aim for Q1 indeed now

Plan is to:

1. move to KeyDNS, enabling DNSSEC, for all non-major domains
2. update the DNS data for Hetzner for all major domains
3. shortly thereafter, when 1. is finalized, also move the major domains to KeyDNS and DNSSEC

The majority of our domains is now connected to KeyDNS at RRProxy, including DNSSEC signing
The main/production domains are not changed yet
The existing zones at Hetzner are not deleted yet
Glue records are updated, but (obviously) not deleted yet

For the DE domains, the DNSSEC keys have to be manually pushed, the automated push does not work
For some domains, pushing DNSSEC keys doesn't seem to work at all, chasing this one already

Guilhem and me to coordinate on the next steps

Domains where pushing DNSSEC does not work are the following. Let's try again tomorrow, if that fails, we need to reach out to support:

documentfoundation.fi
Pushing keys failed. Please try again later or contact support. Invalid attribute value syntax

libreoffice.cz
Pushing keys failed. Please try again later or contact support. Command failed; Command failed

libreoffice.fi
Pushing keys failed. Please try again later or contact support. Missing required attribute; missing tech contact

libreoffice.it
Pushing keys failed. Please try again later or contact support. Invalid attribute value [extepp:wrongvalueextepp:reasoncode => 10011: DNSSEC: dsData to add is already associated with the domain]

Will mail support about that

Domains where pushing DNSSEC does not work are the following. Let's try again tomorrow, if that fails, we need to reach out to support:

documentfoundation.fi
Pushing keys failed. Please try again later or contact support. Invalid attribute value syntax

libreoffice.cz
Pushing keys failed. Please try again later or contact support. Command failed; Command failed

libreoffice.fi
Pushing keys failed. Please try again later or contact support. Invalid attribute value syntax

Will mail support about that
Pushing keys failed. Please try again later or contact support. Invalid attribute value syntax

libreoffice.fi
Pushing keys failed. Please try again later or contact support. Invalid attribute value syntax

As you hinted at during the last 1:1 call, .fi doesn’t accept SHA-1 digest (type 2) in in DS records. (Perhaps a policy of the TLD, although I couldn’t find sources for that.) Manually entering the DS record (SHA-256 only) and DNSKEY record fixes this. But that doesn’t make the “Push KSK Keys to domain” button disappear and I’m not sure what that entails; can’t make the button disappear for .at either, we’ll see during the next key rotation/rollover if that causes any issue.

libreoffice.cz
Pushing keys failed. Please try again later or contact support. Command failed; Command failed

AFAICT the problem here was that the name servers were set to an external 3rd-party. This also caused resolution to fail with SERVFAIL, like for odfauthors.org and odf toolkit.org.

#16 - 2020-08-19 16:05 - Guilhem Moulin
- Subject changed from switch back to Hetzner or RRProxy DNS and remove glue records to switch back to RRProxy DNS and remove glue records

Current status:

- 131 domains registered at RRProxy.
- 129 (all but libreoffice.org and documentation.org) changed to use RRProxy's KeyDNS.
- DNSSEC configured for 126 domains (missing support for hu, org.il and lt).
- 3 CAA records added to all 129 domains (wildcard certs are explicitly disabled).

Mechanic sanity checks:

- A record lookups at the root do succeed (NOERROR) for all 129 domains. A, AAAA, MX, TXT, SRV and CNAME records match what we have had at hetzner.
- A record lookups at the root are fully validated for all 126 DNSSEC active domains.
- Additional section has NS records set to ns[1-3].rrpproxy.net. for all 129 domains.
- SOA MNAME (resp. RNAME) is set to ns1.rrpproxy.net. (resp. hostmaster.documentfoundation.org.) for all 129 domains.
- Transfer lock is enabled whenever supported by the TLD.

Deleted the 111 zones at Hetzner that are no longer in use.

Will coordinate with Florian Effenberger next week regarding migration of our two main domains, namely libreoffice.org and documentation.org.

#17 - 2020-08-19 17:30 - Guilhem Moulin

Guilhem Moulin wrote:

- A record lookups at the root do succeed (NOERROR) for all 129 domains. A, AAAA, MX, TXT, SRV and CNAME records match what we have had at hetzner.

That’s no longer the case, I’ve now marked domains as null MX (IN MX 0. and IN TXT "v=spf1 -all", cf. RFC 7505) whenever that made sense: NL domains, tdf.io, etc.

#18 - 2020-08-25 16:10 - Florian Effenberger

AI Guilhem

- create zones (if required Guilhem to file a ticket)
- set low TTL (e.g. 5-10 minutes)
- import existing two (!) Hetzner zones -> today
- start signing process
- leave DNSSEC off for the moment
- keep zones at Hetzner for the moment
- check leftover Hetzner zones - WHOIS on domain, check if Hetzner or nsX.documentfoundation.org is used -> Florian to ping the owners then

AI Guilhem, Cloph, Florian

- all of us review the DNS entires, share comments/thoughts/additions/deletions
- merge all this
- then agree on a day for switchover -> plan is Friday afternoon

later (!)

- remove zones at Hetzner
• raise TTL
• enable DNSSEC
• remove glue records

#19 - 2020-08-25 20:09 - Guilhem Moulin
Florian Effenberger wrote:

AI Guilhem

• create zones (if required Guilhem to file a ticket)
• set low TTL (e.g. 5-10 minutes)
• start signing process

Done for documentfoundation.org, for libreoffice.org the folks at RRProxy need to reassign the zone first.

• import existing two (!) Hetzner zones -> today

Blocking on the zone reassignation. Will proceed with the two domains at once.

• leave DNSSEC off for the moment
• keep zones at Hetzner for the moment
• check leftover Hetzner zones - WHOIS on domain, check if Hetzner or nsX.documentfoundation.org is used -> Florian to ping the owners
then

I count 18 leftover domains. 9 are up for grabs (NXDOMAIN) and could be bought back if desired:

• documentfoundation.com.br
• documentfoundation.net.br
• documentfoundation.org.br
• documentfoundation.srv.br
• libreoffice.com.br
• libreoffice.net.br
• libreoffice.org.br
• libreoffice.srv.br
• thedocumentfoundation.org.br

6 use ns[1-3].documentfoundation.org (so the zone at Hetzner are authoritative):

• documentfoundation.ca
• documentfoundation.dk
• libre-office.ca
• libreoffice.ca
• libreoffice.dk
• thedocumentfoundation.ca

The remaining 3 use other name servers:

• document-foundation.ca
• documentfoundation.ru
• libreoffice.ir

#20 - 2020-08-26 13:27 - Guilhem Moulin
Guilhem Moulin wrote:

Florian Effenberger wrote:

AI Guilhem

• create zones (if required Guilhem to file a ticket)
• set low TTL (e.g. 5-10 minutes)
• start signing process

Done for documentfoundation.org, for libreoffice.org the folks at RRProxy need to reassign the zone first.

• import existing two (!) Hetzner zones -> today

Blocking on the zone reassignation. Will proceed with the two domains at once.
Done. Some observations:

- Non-default TTLs need to be added manually. RRProxy appears to have a 8h default which is unaffected by the SOA’s MINTTL (which per RFC 2308 is fine);
- RRProxy choke on SRV records with a trailing period, so these records can’t be imported straight from a BIND-formatted zone file (once the trailing period is removed the DNS reply looks good though); and
- RRProxy choke on RRs with implicit second-level domain such as foo IN MX mail, one needs to explicitly append a second-level and a trailing dot, namely foo IN MX mail.documentfoundation.org., so these records can't be imported straight from a BIND-formatted zone file (once the second-level domain and trailing period are added the DNS reply looks good though).

#21 - 2020-08-26 14:49 - Guilhem Moulin
Guilhem Moulin wrote:

- RRProxy chokes on SRV records with a trailing period, so these records can't be imported straight from a BIND-formatted zone file

Interestingly "null" SRV records such as _foo._tcp SRV 0 0 0 . (RFC 6186 §3) can be defined/imported, so at least we don't miss on expressivity here.

#22 - 2020-08-27 14:14 - Florian Effenberger
You can DELETE the following zones at Hetzner:

- [...] You can also DELETE the following zones at Hetzner:

- [...] Done, it's only the 6+2 zones left at Hetzner now (all active).

#23 - 2020-08-27 14:53 - Florian Effenberger
Original comment text:

Thanks a lot for your work on this!
You can DELETE the following zones at Hetzner:

<table>
<thead>
<tr>
<th>documentfoundation.com.br</th>
</tr>
</thead>
<tbody>
<tr>
<td>documentfoundation.net.br</td>
</tr>
<tr>
<td>documentfoundation.org.br</td>
</tr>
<tr>
<td>documentfoundation.srv.br</td>
</tr>
<tr>
<td>libreoffice.com.br</td>
</tr>
<tr>
<td>libreoffice.net-br</td>
</tr>
<tr>
<td>libreoffice.org.br</td>
</tr>
<tr>
<td>libreoffice.srv.br</td>
</tr>
<tr>
<td>thedocumentfoundation.org.br</td>
</tr>
</tbody>
</table>

I will check in parallel with Olivier about the domains, hostmaster@ is in cc - should we re-register, we will use KeyDNS at RRProxy.
For the moment, please KEEP the following zones at Hetzner:

<table>
<thead>
<tr>
<th>documentfoundation.ca</th>
</tr>
</thead>
<tbody>
<tr>
<td>foundationfoundation.dk</td>
</tr>
<tr>
<td>libre-office.ca</td>
</tr>
<tr>
<td>libreoffice.ca</td>
</tr>
<tr>
<td>libreoffice.dk</td>
</tr>
<tr>
<td>thedocumentfoundation.ca</td>
</tr>
</tbody>
</table>

I reached out to the domain name holders, asking how to proceed - either we transfer to TDF, or we ask the holders to change the DNS
You can also DELETE the following zones at Hetzner:

<table>
<thead>
<tr>
<th>documentfoundation.ca</th>
</tr>
</thead>
<tbody>
<tr>
<td>documentfoundation.ru</td>
</tr>
<tr>
<td>libreoffice.ir</td>
</tr>
</tbody>
</table>

#24 - 2020-08-27 15:01 - Florian Effenberger
For documentfoundation.org

Note: I did NOT check if all entries from Hetzner have been properly converted. If in doubt, better double-check this, please. I ONLY checked for wrong or superfluous records in the imported zone.

- @ 600 IN CAA 0 issuewild ";"
  Is that desired? For the other domains I always set "letsencrypt.org" for "issuewild" as well. Fair enough if we don't use wildcard certificates, of
- What we might need to have in mind is for split-DNS situations (external IP = 1.2.3.4, internal IP = 5.6.7.8 eg in VPN) to look if DNSSEC can be enabled, or if that breaks the trust anchor. I remember there is something like a negative trust anchor ([https://www.freedesktop.org/software/systemd/man/dnssec-trust-anchors.d.html](https://www.freedesktop.org/software/systemd/man/dnssec-trust-anchors.d.html)) but didn't look closer.

- Does it make sense to keep multiple old DKIM entries? DKIM keys are only checked when the mail is received, so three year old, legacy records could be deleted if not used

- There are some hostnames that could be old/outdated. Not sure, might be worth checking. Some that could be old are, maybe double-check with Cloph on these
  - floyd
  - engine
  - gucky
  - imageboard
  - owncloud
  - translations-old

- Do we still run a Torrent tracker (tracker.tdf CNAME vm185)?

#25 - 2020-08-27 15:32 - Florian Effenberger

For [libreoffice.org](http://libreoffice.org)

Note: I did NOT check if all entries from Hetzner have been properly converted. If in doubt, better double-check this, please. I ONLY checked for wrong or superflous records in the imported zone.

- @ 600 IN CAA 0 issuewild ";"

  Is that desired? For the other domains I always set "letsencrypt.org" for "issuewild" as well. Fair enough if we don't use wildcard certificates, of course. ;-) 

- What we might need to have in mind is for split-DNS situations (external IP = 1.2.3.4, internal IP = 5.6.7.8 eg in VPN) to look if DNSSEC can be enabled, or if that breaks the trust anchor. I remember there is something like a negative trust anchor ([https://www.freedesktop.org/software/systemd/man/dnssec-trust-anchors.d.html](https://www.freedesktop.org/software/systemd/man/dnssec-trust-anchors.d.html)) but didn't look closer.

- There are some hostnames that could be old/outdated. Not sure, might be worth checking. Some that could be old are, maybe double-check with Cloph on these
  - ask-staging (yields "internal server error")
  - blog.vi (points to vi.blog, and then "this site is no longer available")
  - bugassistant (I think the assistant doesn't exist anymore, so we might want to get rid of the hostname; Cloph or Xisco should have details)
  - gerrit-test2
  - manual-test
  - roadshow (shows empty blog)

- after September 30 (shutdown of Hosted.IM) we can also delete all XMPP/Jabber-related SRV entries

#26 - 2020-08-27 15:38 - Guilhem Moulin

Florian Effenberger wrote:

For [documentfoundation.org](http://documentfoundation.org)

Note: I did NOT check if all entries from Hetzner have been properly converted. If in doubt, better double-check this, please. I ONLY checked for wrong or superflous records in the imported zone.

Like for other zones I ran a mechanic check on A+AAA+MX+TXT+SRV+CNAME RRs.

- @ 600 IN CAA 0 issuewild ";"

  Is that desired? For the other domains I always set "letsencrypt.org" for "issuewild" as well. Fair enough if we don't use wildcard certificates, of course. ;-) 

That's a defense in depth principle: lock down what we don't need/use; should we need wildcard certs later it's trivial to update later. Did a bulk change of other zones last weeks, cf. #1496#note-16.

- What we might need to have in mind is for split-DNS situations (external IP = 1.2.3.4, internal IP = 5.6.7.8 eg in VPN) to look if DNSSEC can be enabled, or if that breaks the trust anchor. I remember there is something like a negative trust anchor ([https://www.freedesktop.org/software/systemd/man/dnssec-trust-anchors.d.html](https://www.freedesktop.org/software/systemd/man/dnssec-trust-anchors.d.html)) but didn't look closer.

I use that at home because my local resolver is spoofing various records, which breaks the trust anchor indeed. I don't think split DNS applies in our case because the Name Server on gustl is a passthrough except for the (invalid) tdf TLD.

- Does it make sense to keep multiple old DKIM entries? DKIM keys are only checked when the mail is received, so three year old, legacy
records could be deleted if not used

Those could be deleted indeed.

- There are some hostnames that could be old/obtated. Not sure, might be worth checking. Some that could be old are, maybe double-check with Cloph on these
  - floyd

Well that's the salt master :-P

- engine
- gucky
- imageboard
- owncloud
- translations-old

imageboard is used, https://imageboard.documentfoundation.org/ is a 303 redirect to the design blog since the mascot fiasco. Would also keep owncloud as removing it would break very old federation lists (not sure either how the desktop client deals with 301 redirects). The rest can be deleted indeed.

- Do we still run a Torrent tracker (tracker.tdf CNAME vm185)?

`curl http://tracker.documentfoundation.org:6969/stat` says yes, and people do complain when it's down :-)

#27 - 2020-08-27 15:52 - Guilhem Moulin
Florian Effenberger wrote:

For libreoffice.org

Note: I did **NOT** check if all entries from Hetzner have been properly converted. If in doubt, better double-check this, please. I **ONLY** checked for wrong or superfluous records in the imported zone.

- @ 600 IN CAA 0 issuewild ";";
  Is that desired? For the other domains I always set "letsencrpyt.org" for "issuewild" as well. Fair enough if we don't use wildcard certificates, of course. ;-)  

- What we might need to have in mind is for split-DNS situations (external IP = 1.2.3.4, internal IP = 5.6.7.8 eg in VPN) to look if DNSSEC can be enabled, or if that breaks the trust anchor. I remember there is something like a negative trust anchor (https://www.freedesktop.org/software/systemd/man/dnssec-trust-anchors.d.html) but didn't look closer.

See #1496#note-26

- There are some hostnames that could be old/obtated. Not sure, might be worth checking. Some that could be old are, maybe double-check with Cloph on these
  - ask-staging (yields "internal server error")

Used by Evgeny for development AFAICT; could probably use a local resolver instead, but IMHO we can keep this record until ask.libo is used in production.

- bugassistant (I think the assistant doesn't exist anymore, so we might want to get rid of the hostname; Cloph or Xisco should have details)

Right that's a redirect to bugs.tdf

- gerrit-test2

Unused, can be deleted.

- manual-test

See #2668.

- blog.vi (points to vi.blog, and then "this site is no longer available")
- roadshow (shows empty blog)
Italo removed these a while ago, records can be deleted I guess.

- after September 30 (shutdown of Hosted.IM) we can also delete all XMPP/Jabber-related SRV entries

Ack.

#28 - 2020-08-27 16:12 - Florian Effenberger

Like for other zones I ran a mechanic check on A+AAA+MX+TXT+SRV+CNAME RRs.

Perfect!

That's a defense in depth principle: lock down what we don't need/use; should we need wildcard certs later it's trivial to update later. Did a bulk change of other zones last weeks, cf. #1496#note-16

-<https://redmine.documentfoundation.org/issues/1496#note-16>&gt;

Fine for me!

- Does it make sense to keep multiple old DKIM entries? DKIM keys are only checked when the mail is received, so three year old, legacy records could be deleted if not used

Those could be deleted indeed.

Then let's remove them. :)

Well that's the salt master :-P

Ooops :)

[Imageboard] is used, <https://imageboard.documentfoundation.org/> is a 303 redirect to the design blog since the mascot fiasco. Would also keep [owncloud] as removing it would break very old federation lists (not sure either how the desktop client deals with 301 redirects). The rest can be deleted indeed.

Ok, then let's make it so.

Used by Evgeny for development AFAICT; could probably use a local resolver instead, but IMHO we can keep this record until ask.libo is used in production.

Let's keep it then indeed.

bugassistant (I think the assistant doesn't exist anymore, so we might want to get rid of the hostname; Cloph or Xisco should have details)

Right that's a redirect to bugs.tdf

If Cloph has no objections, let's delete it.

gerrit-test2

Unused, can be deleted.

Let's do that. :)

blog.vi (points to vi.blog, and then "this site is no longer available")
roadshow (shows empty blog)

Italo removed these a while ago, records can be deleted I guess.

Same here, let's remove it then.
We can't transfer the CA domains due to local presence requirements, but the domain holder can update the WHOIS.

Can you create DNS records at RRPproxy for

documentfoundation.ca
libre-office.ca
libreoffice.ca
thedocumentfoundation.ca
document-foundation.ca

and let me know when done?

Cleaned up accordingly (only on the KeyDNS side). Kept bugassistant though since there are likely left over links around.

Note to self: we can also remove ns[1-3].documentfoundation.org once the migration is complete.

Florian Effenberger wrote:

Can you create DNS records at RRPproxy for

documentfoundation.ca
libre-office.ca
libreoffice.ca
thedocumentfoundation.ca
document-foundation.ca

and let me know when done?

Done. All 4 zones are unsigned, null MX, and with A+AAAA records for @ and www pointing to the main site.

Florian Effenberger wrote:

I was creating the default set of DNS entries at RRPproxy (please double check, IIRC you modified e.g. the CAA record), and started DNSSEC signing.

I've changed the nameservers (without DNSSEC yet) at Hostmaster DK
Will in parallel find out with RRPproxy if we can transfer the domain names directly there

Florian Effenberger wrote:

I think record sets are useless as they provide no advantage over the API and the API gives more flexibility, but I did bring the set in line with the zones last week (updated the CAA record and set null MX config), so these two new zones are consistent with the other ones :-)

For the DK domain names, we have these indeed already, but directly with Hostmaster DK

I was creating the default set of DNS entries at RRPproxy (please double check, IIRC you modified e.g. the CAA record), and started DNSSEC signing.

I've changed the nameservers (without DNSSEC yet) at Hostmaster DK
Will in parallel find out with RRPproxy if we can transfer the domain names directly there

Florian Effenberger wrote:

Pointed documentfoundation.org and libreoffice.org to RRProxy now, with a 600s TTL on every RR. DNSSEC lookups are available on demand but the parent zone wasn't updated with the KSK: should resigning turn sour, validating resolvers won't choke on these two. Plan is to enable DNSSEC once we've verified resigning worked fine on other domains in the same TLD. According to https://wiki.rrproxy.net/dns/keydns/enable-dnssec-for-keydns-zones that should be around September 10.

No problems reported so far, but let's keep libreoffice.org and documentfoundation.org as zones at Hetzner, for a fallback/backup, for
some more days at least.

- Can you check again if you can push the keys for libreoffice.cz? Last times I got an error message, ticket with RRProxy is open.
- You can delete the .DK and .CA domains from Hetzner. WHOIS shows RRProxy DNS, dig yields a result, so transition to RRProxy seems done.
- For the .DK domains, if you let me know the DNSSEC data, I can update the domains at the registrar to use a signed zone.

#37 - 2020-08-31 15:11 - Guilhem Moulin
Florian Effenberger wrote:

- Can you check again if you can push the keys for libreoffice.cz? Last times I got an error message, ticket with RRProxy is open.
- You can delete the .DK and .CA domains from Hetzner.
- For the .DK domains, if you let me know the DNSSEC data, I can update the domains at the registrar to use a signed zone.

Done, that leaves only documentfoundation.org and libreoffice.org. ns[1-3].documentfoundation.org RRs are no longer used so I removed these from KeyDNS.

- For the .DK domains, if you let me know the DNSSEC data, I can update the domains at the registrar to use a signed zone.

documentfoundation.org. IN DNSKEY 257 3 7 AwEAAeukhjXrV5LX3fn+u28zq2P/1A6r+brAnupetWAIv6skMw7ZUZgMy5m7BEuuXNXXHi8v4a/ovsuv6opVnEqyQyeAHjpWSIAwjlzVUKBE8EKjShShf73KIDoVK42E6Hd/r04WV1Q7iEWIvWvXqrcp:pg3p4yQYIvXOWvN12/v8mhzXw/SFepQnM3xabkYy09Lgj9xjbxmJu93aAt43b4YaWUI2xdcIMEXBel/nM1uycZchD1mQoqhwlpqQAoZpdenf8A5Y+goud5xz6/fJx9nU48R6wMzIqQpOLlpV+u6A9zn1mJRVVn1nH2cefhpctNpaEKSORQeeum=
documentfoundation.org. IN DS 32871 7 1 262PSFCF1D43325228589721BDEF944F4D0CBAE4

Answered this in #1496#note-15, per #1496#note-16 A record lookups at the root is fully validated.

- You can delete the .DK and .CA domains from Hetzner.

DK Hostmaster lets me add "DNSSEC key". Is that DNSKEY or DS?

#38 - 2020-08-31 15:22 - Florian Effenberger
Done, that leaves only documentfoundation.org and libreoffice.org. ns[1-3].documentfoundation.org RRs are no longer used so I removed these from KeyDNS.

DK Hostmaster lets me add "DNSSEC key". Is that DNSKEY or DS?
Then I think we can also remove the glue records, correct? Can you do that?

#40 - 2020-08-31 15:32 - Guilhem Moulin

Florian Effenberger wrote:

DK Hostmaster lets me add "DNSSEC key". Is that DNSKEY or DS?

The (public) key material is in the DNSKEY record. DS RRs are its digest values using various algorithms (SHA-1 and -256 in the above).

Then I think we can also remove the glue records, correct? Can you do that?

Right, done.

#41 - 2020-08-31 15:38 - Florian Effenberger

Fields to add are Keytag, Algorithm, Digest type and Digest, so then I'll try with the latter :)

The Document Foundation Redmine wrote:

The (public) key material is in the DNSKEY record. DS RRs are its digest values using various algorithms (SHA-1 and -256 in the above).

#42 - 2020-08-31 15:55 - Guilhem Moulin

Florian Effenberger wrote:

Fields to add are Keytag, Algorithm, Digest type and Digest

Just split the record by word?

documentfoundation.dk. IN DS 32871 7 1 262F5CFC1D433252285D98721BDEFF944F4DBCAE4

Means

- Key tag: 32871
- Digest algorithm: 7 (ie RSASHA1-NSEC3-SHA1: https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml)
- Digest type: 1 (ie SHA-1: https://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml#ds-rr-types-1)
- Digest value: 262F5CFC1D433252285D98721BDEFF944F4DBCAE4

Cf. RFC 4034 sec. 5.1 :-)

#43 - 2020-08-31 16:03 - Guilhem Moulin

Guilhem Moulin wrote:

Just split the record by word?

(But the DNSKEY record should be enough.)

#44 - 2020-08-31 17:21 - Florian Effenberger

Couldn't add that due to missing algorithms, so was using the DS, seems to work :) 

#45 - 2020-08-31 18:16 - Guilhem Moulin

Florian Effenberger wrote:

Couldn't add that due to missing algorithms, so was using the DS, seems to work :) 

Confirmed

#46 - 2020-09-04 01:56 - Guilhem Moulin

- Priority changed from High to Normal
Lowering severity now, the only thing left is to raise the TTL and update the parent zone with the KSKs (and remove zones at Hetzner for cleanup. (Severity was raised as we were using brittle Name Servers.)

It'll be one week tomorrow that we updated the name servers and AFAICT the transition was smooth. I propose to raise the SOA and RRs TTLs tomorrow (or at least before deploying DNSSEC at the end of next week), any objection? AFAICT the change requires to delete and recreate each record, but using the API this can be done in a single operation which appears to be atomic.

### #47 - 2020-09-04 15:09 - Florian Effenberger

Lowering severity now, the only thing left is to raise the TTL and

ACK

It'll be one week tomorrow that we updated the name servers and AFAICT the transition was smooth. I propose to update the SOA and RRs TTLs tomorrow (ie before deploying DNSSEC), any objection? AFAICT the change requires to delete and recreate each record, but using the API this can be done in a single call which appears to be atomic.

If you can take care of it and are available in case of emergencies, fine for me - doing it during the weekend is definitely better than during the week, so fine for me!

### #48 - 2020-09-05 20:25 - Guilhem Moulin

Florian Effenberger wrote:

If you can take care of it and are available in case of emergencies, fine for me

Done. I wasn't able able to it atomically though: the records were updated (exporting the zones using the API showed the new TTL) but the changes were not reflected in DNS queries to the authoritative server. But AFAICT the DNS has a 5min cache and picks up changes at fixed intervals, so in practice consecutive changes won't yield bogus replies.

Guilhem Moulin wrote:

Kept bugassistant though since there are likely left over links around.

Seems it was deleted anyway… this name is also used as SAN in the bugs.tdf CSR, so blindly removing it would have failed the next ACME challenge thus cert renewal for bugs.tdf! Added back for now.

### #49 - 2020-09-09 12:48 - Florian Effenberger

One more "cleanup" task:

For all domains, in the past I've set the "Whois banner", "RSP tag", "URL" fields. These can be removed, as we can configure them centrally. Nothing urgent, but can be done as some cleanup tasks. A API call on all domains should be able to remove the fields/empty the strings.

### #50 - 2020-09-09 12:51 - Florian Effenberger

Another thing we can consider, likewise "cleanup" and not urgent:

We've used the non-whitelabel DNS for all domains because of the "Inconsistent set of NS RRs" error message for .DE domains. The solution to that is to, for .DE domains only, add an explicit NS entry in the zone, pointing to the whitelabel DNS. So we can, if we want, move all domains to the whitelabel variant.

### #51 - 2020-09-10 11:23 - Florian Effenberger

Turns out that even if you set whitelabel DNS, the NS entry in the zone is on the branded one, so if we change that for .DE, we should change it for all zones actually

### #52 - 2020-09-12 00:22 - Guilhem Moulin

FYI the ZSK rotation seems stable, one can see the RRSIGs updating and of the 138 registered zones 128 still validate, the remaining ones being the 5 zones under the ca TLD, .{hu,li,lt} for which there is no DNSSEC support, and {libreoffice,documentfoundation}.org. As far as I'm concerned it's all good to flip the switch on the latter two also.

---

2022-03-20
Fine for me, during the weekend, whenever you are around to react in case of issues. :-) 

Florian Effenberger wrote:

Done, that makes my validating resolver happy

Florian Effenberger wrote:

Checked

https://dnssec-analyzer.verisignlabs.com/libreoffice.org

and

https://dnssec-analyzer.verisignlabs.com/documentfoundation.org

and all looks good :)