Deploying DNSSEC in a Large Enterprise

(despite the DNS camel's burdens)

Han Zhang
Allison Mankin
hzhang@salesforce.com
amankin@salesforce.com

Outline

- Introduction
- Challenges and Successes
- Takeaways

Introduction

Reasons a Large Enterprise Might Deploy DNSSEC

Compliance

- US: FedRAMP compliance requirements for some
  - We are mostly aware of US FedRAMP; there are other national DNSSEC regulations too
- ICANN: advised that all use DNSSEC

Trust Benefits for Users

- DNSSEC advances a goal of increasing trust for users
- Tradeoff on compliance: separate small namespace for regulated group or DNSSEC for all
- Our organization’s decision: deploy DNSSEC for all

Introduction

Characteristics of Our Enterprise

- Use of Managed DNS
  - Outsourcing to get sufficient authoritative footprint
  - Using multiple providers for resilience
- Some zones are very dynamic
  - Up to 1 million changes per day, 700 changes per minute (aggregate)
  - Dynamic zones are not unique: consider web hosting companies
  - Changes can cause update propagation delays *
- Some customer-facing zones are very large *before signing*

* DNS Service Monitoring at Salesforce, **Han Zhang, OARC 27**

- Introduction
- Challenges and Successes
  - **Challenge 1: Preparation**
- Takeaways

Compare DNSSEC Services and Features of DNS Providers*

- Zone signing algorithms (13)
- NSEC(3)
- Zone sizes support
- Signature validity period support
- Key rollover support
- Any possibility of signing non-standard records?
- Zone transfer limitations and performance

* DNSSEC for a Complex Enterprise Network, **Pallavi Aras, Shumon Huque, OARC 28**

Compare DNSSEC Services and Features of DNS Providers*

- Zone signing algorithms (13)
- NSEC(3)
- Zone sizes support
- Signature validity period support
- Key rollover support
- Any possibility of signing non-standard records?
- Zone transfer limitations and performance

We had to migrate some zones to satisfy some requirements.

* DNSSEC for a Complex Enterprise Network, **Pallavi Aras, Shumon Huque, OARC 28**

Analyze Zones to Be Signed

- What clean-up is needed, do they need re-hosting?
- Look into sub-domains
- Understand all uses of non-standard DNS features such as traffic management, redirects
- Move non-standard records to child zones if not separated already

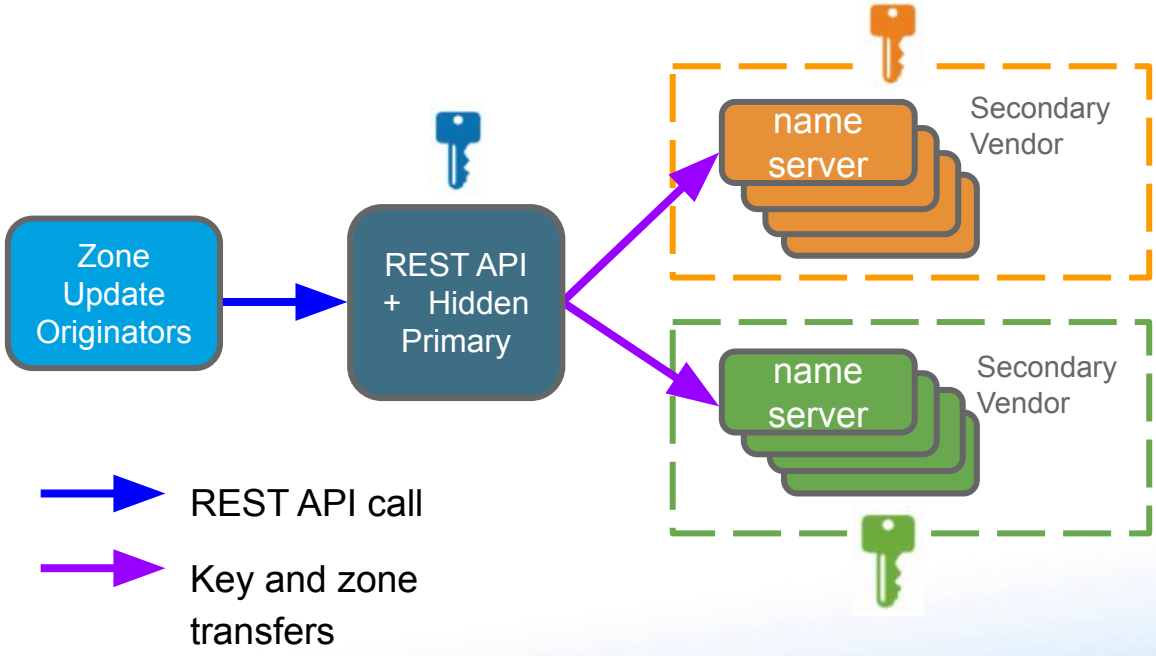
Prepare Tests

- Workloads of all DNS provisioning scenarios (including off-peak and peak)
- Measures of provisioning performance including API use, server utilizations, update propagation delays
- Measures of resolution performance including synthetics

- Introduction
- Challenges and Successes
  - **Challenge 2: DNSSEC Models**
- Summary

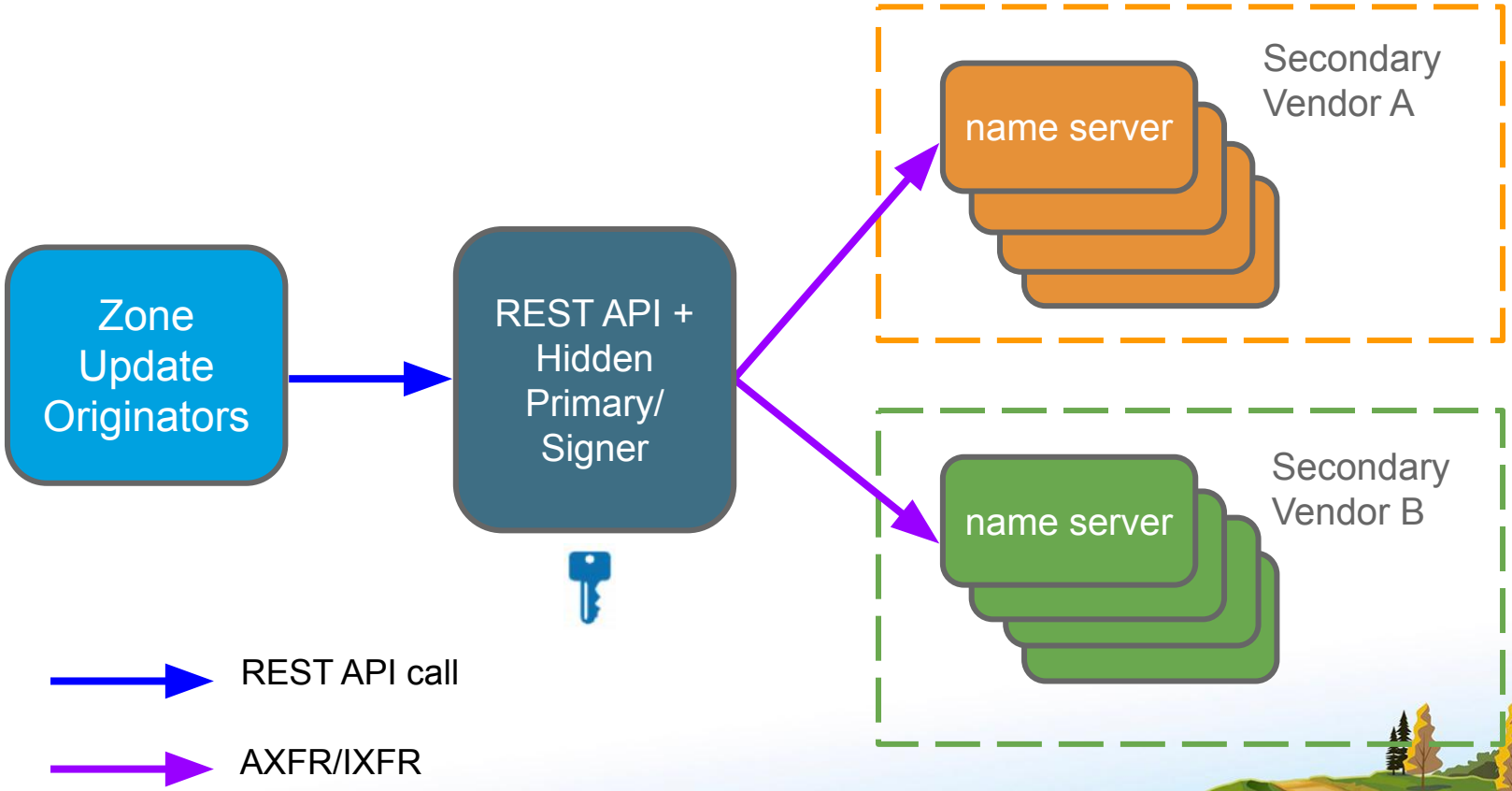
Ideal Model * - Multi-signer

- Multi-signer DNSSEC has two models
- Not available now

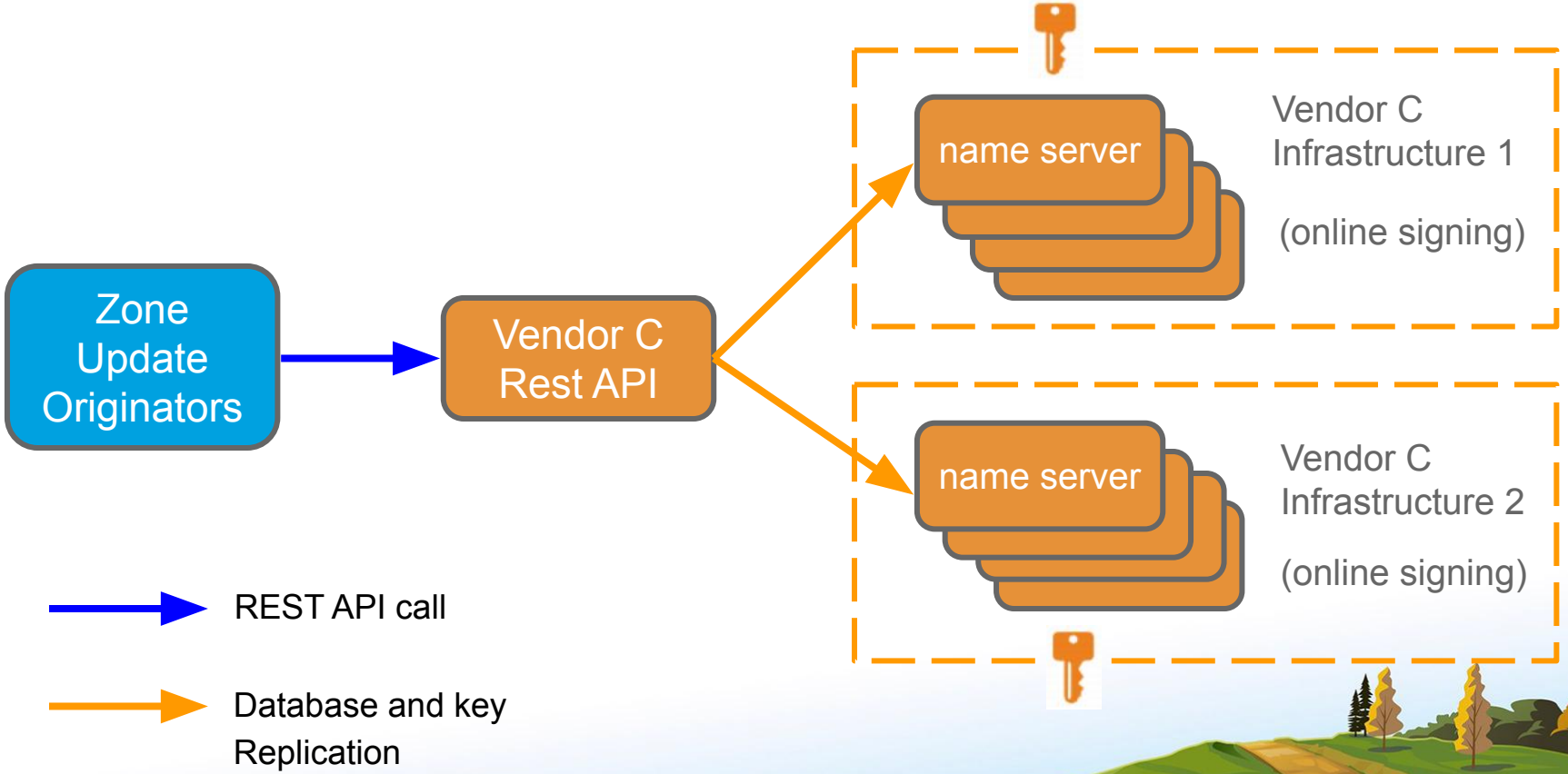


* Multi-signer DNSSEC Models, **Shumon Huque, Jan Včelák, OARC 30**

Hidden Signing Master Model



Third-party Signing Vendor Model

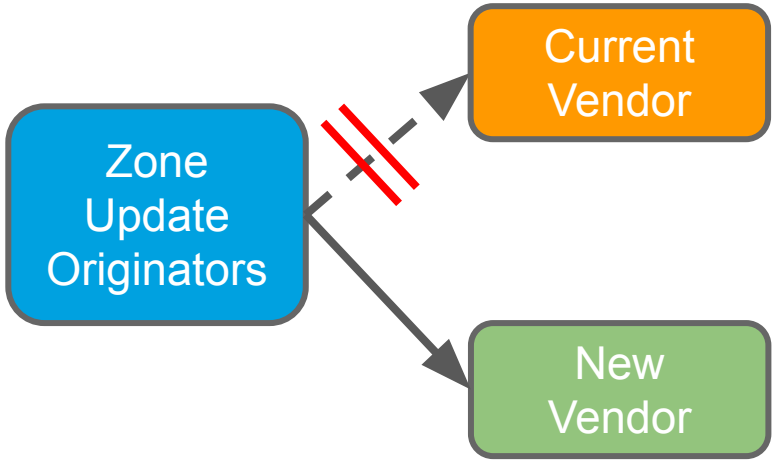


- Introduction
- Challenges and Successes
  - **Challenge 3: Zone Migrations**
- Takeaways

Is Zone Migration Simple?

- Moves of zones between providers were needed
  - For provider features (e.g. filtering)
  - For cleanup

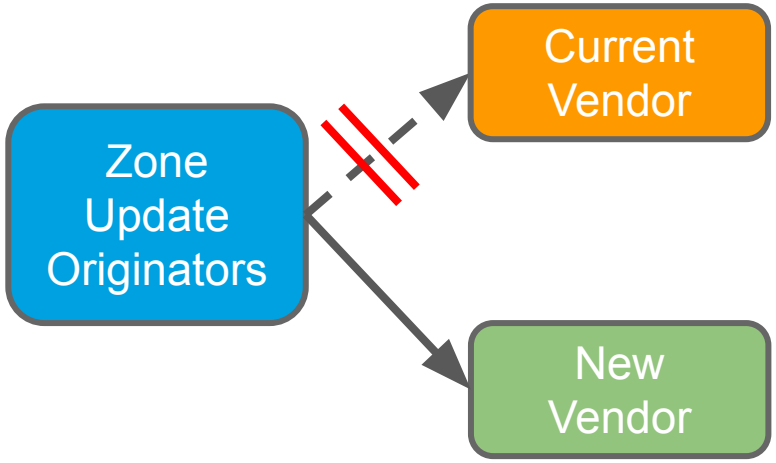
Is Zone Migration Simple?



- Moves of zones between providers were needed
  - For provider features (e.g. filtering)
  - For cleanup

- Zone migration is simple, isn't it?
  1. Make changes to send updates to new vendor
  2. Change the NS records for the zone

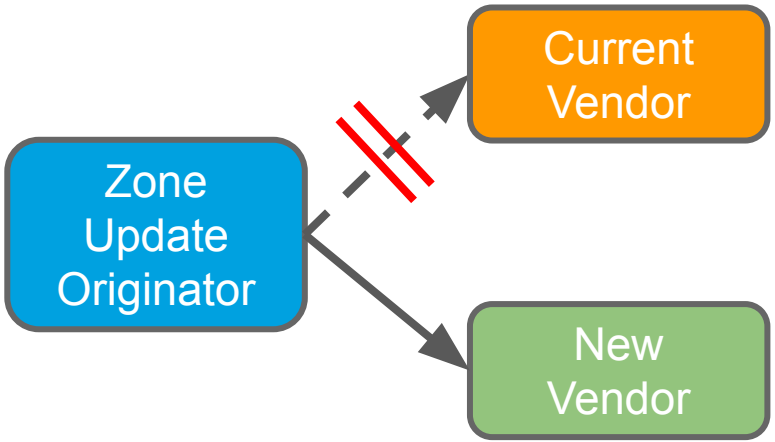
Lessons Learned - Migration Can be Fragile



For live, dynamic zones a hard cut-over is risky:

- Provisioning: REST API calls fail
- Resolution: customers see outdated inconsistent answers

Lessons Learned - Migration Can be Fragile



Goal: Mitigate risks by doing multi-step migration

Observation: Separate migration and DNSSEC signing to minimise impact.

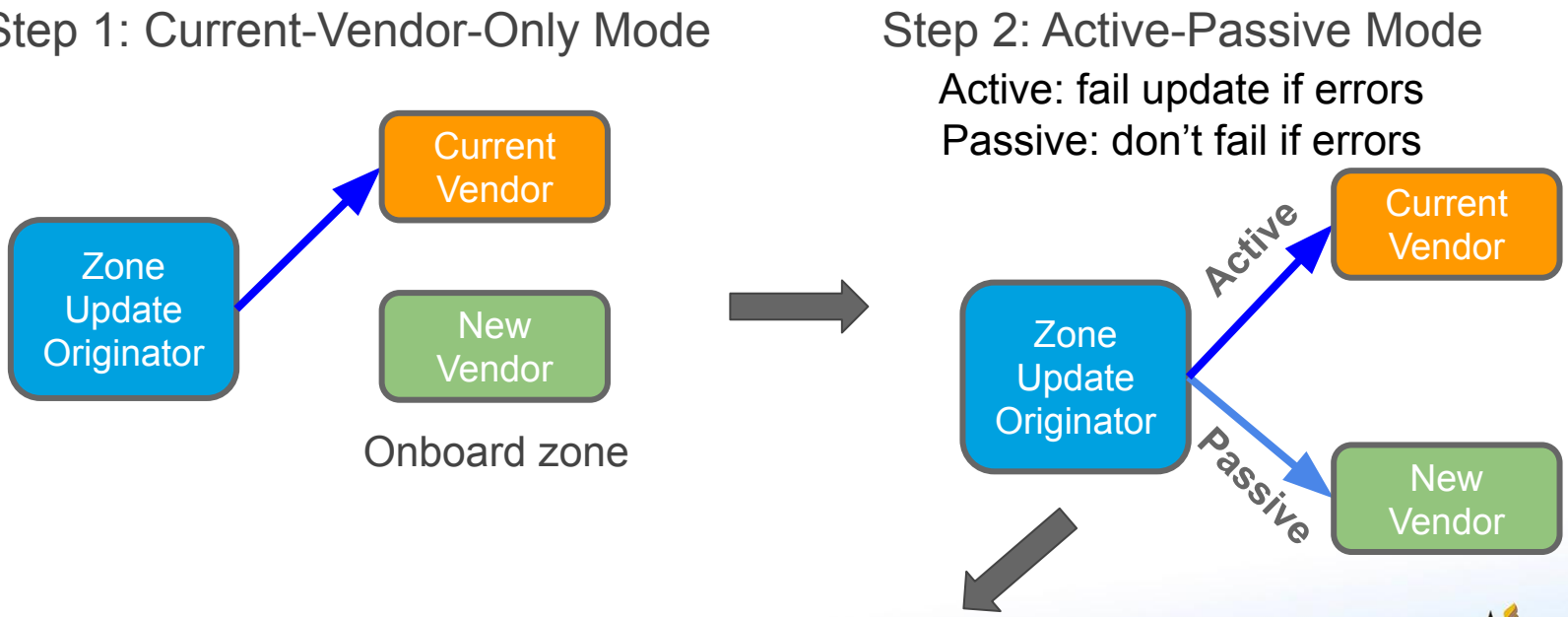
For live, dynamic zones a hard cut-over is risky:

- Provisioning: REST API calls fail
- Resolution: customers see outdated inconsistent answers

Goals and Risk Mitigations

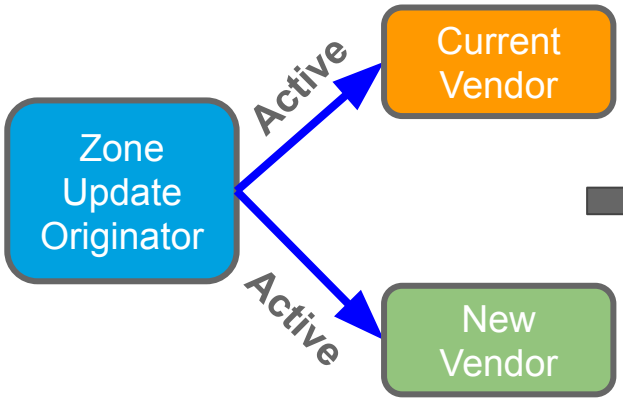
- **Goal**: avoid **ALL** impact on live zones' provisioning and resolution
  - Even assuming non-stop updates
  - Depending on model and also on type of zone update initiator, timing can be tough
  - Handle issues around delegation and sub-zones
  - Handle surprises
- **Risk Mitigations**: be prepared to roll back quickly
  - Analysis was needed to make sure this was possible
  - Use rolling back NS record and DS record changes to make quick recoveries

Accomplishing Migration Goal and Deploying DNSSEC in 7 Steps



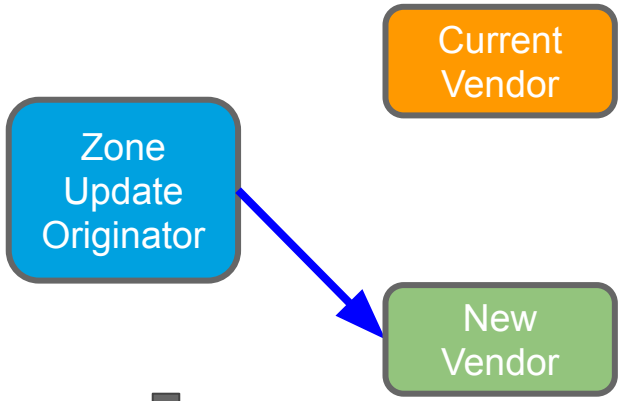
Zone Migration Steps

Step 4: Active-Active Mode



Step 5: Change NS records to new vendor

Step 6: New-Vendor-Only Mode



Not shown: pre-tests plus bake-in, tests and inconsistency handling at every step

Step 7: Publish DS

Delegation and Child Zones

- Zones being migrated remain on the old provider until migration completed.
- If both parent and child are on the same provider and **ONLY** the child is migrated then old provider might still server the child zone after the NS change.

Delegation and Child Zones

- Zones being migrated remain on the old provider until migration completed.
- If both parent and child are on the same provider and **ONLY** the child is migrated then old provider might still server the child zone after the NS change

Solutions	Pros	Cons
Remove the child zone from the current provider	Don’t need to worry about the outdated records	1. Hard to rollback. The zone needs to be reinstalled and missing records need to be added 2. Customers see inconsistent answers when the zone is removed

Delegation and Child Zones

- Zones being migrated remain on the old provider until migration completed.
- If both parent and child are on the same provider and **ONLY** the child is migrated then old provider might still server the child zone after the NS change

Solutions	Pros	Cons
Remove the child zone from the current provider	Don't need to worry about the outdated records	1. Hard to rollback. The zone needs to be reinstalled and missing records need to be added 2. Customers see inconsistent answers when the zone is removed
Suspend the child zone from the current provider (if features available)	Same as above	1. Provisioning is impacted 2. Down time 3. Hard to rollback

Delegation and Child Zones

- Zones being migrated remain on the old provider until migration completed.
- If both parent and child are on the same provider and **ONLY** the child is migrated then old provider might still server the child zone after the NS change

Solutions	Pros	Cons
Remove the child zone from the current provider	Don't need to worry about the outdated records	1. Hard to rollback. The zone needs to be reinstalled and missing records need to be added 2. Customers see inconsistent answers when the zone is removed
Suspend the child zone from the current provider (if features available)	Same as above	1. Provisioning is impacted 2. Down time 3. Hard to rollback
Migrate the parent zone and child zone at the same time	1. No down time 2. No impact on provisioning	The NS records of the parent zone and child zone need to be changed together in case of rollback.

Always Write a Rollback Plan

Goal: Rollback as quickly as possible in case of any incident

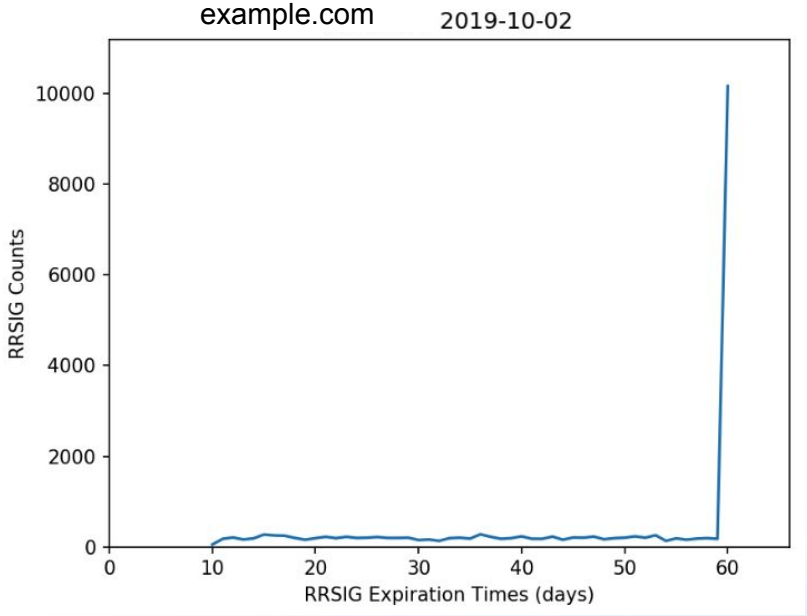
- Quickly switch modes (e.g., Passive-Active ⇔ Active-Active)
  - State changes may take time (depending on how update initiator designs)
  - Common case for us: a 5-10 minutes state change
- Quickly roll back NS records
  - The default TTL for NS record is 24 hours
  - Reduce the TTL to 30 seconds 2 days before making the NS change
- .COM TTL
  - The TTL is 48 hours
  - Not as high impact as feared (based on tests)

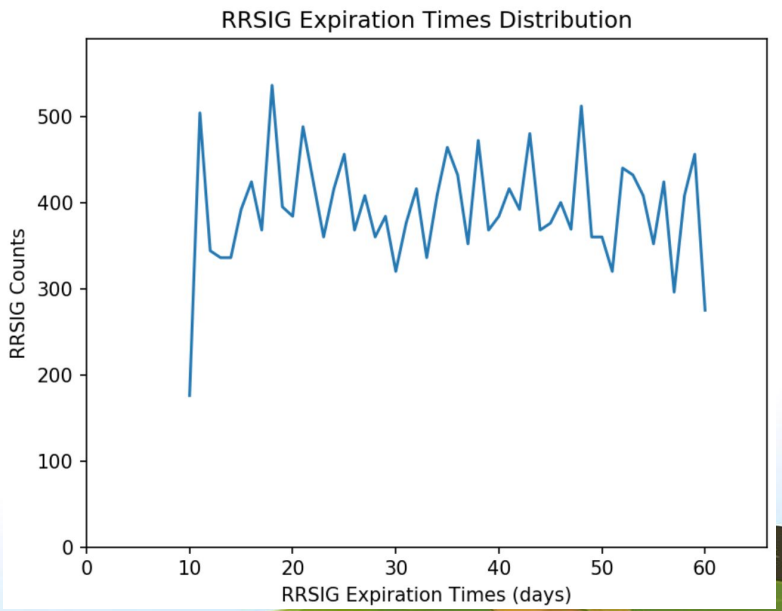
Outline

- Introduction
- Challenges and Successes
  - **Challenge 4: DNSSEC Specific Challenges**
- Takeaways

DNSSEC Signing Jitter

- Impact of records' re-signing on load doing XFRs to secondaries
- Stack vendor created strong jittering to help this, but it broke in a new release (now patched)





DNSSEC Specific Challenges

- NSEC3 support can be awkward to use and hard to debug
  - We discovered a bug that resulted in incorrect negative proofs
- One public recursive was unable to properly authenticate responses for records that involved certain complex configurations
  - CNAMEs that crossed zone boundaries, wildcard synthesis, and a combination of secure and insecure delegations in the chain
- Adding/signing zones for a hidden master model can be complex
  - Automation helps avoid human error
  - Pre-delegation testing is your friend (dnsviz was invaluable)

Outline

- Introduction
- Challenges and Successes
  - **Challenge 5: DNSSEC and Hardware Load Balancers**
- Takeaways

Meeting a GTM DNSSEC Challenge

We have done a lot of work, hoping it can be guidance for others with this challenge

Example challenge: a signature inception offset was needed, and was added by the vendor

Another example challenge: getting DNSSEC right on an Active/Active GTM

Our team-mate, along with a co-author from F5, presented these and more at RIPE 79**

Challenges and Successes of DNSSEC Signing an F5 BIG-IP DNS Hosted Zone, **Neda Kianpour, Tyler Shaw, RIPE 79

Outline

- Introduction
- Challenges and Successes
- **Takeaways**

Takeaways

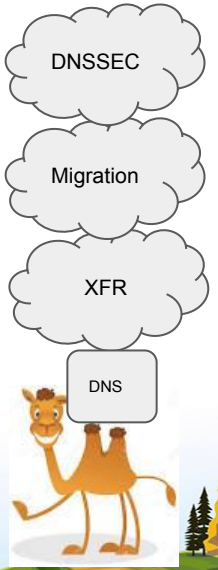
- There are challenges and surprises in deploying DNSSEC in a large enterprise, but it can be driven to success

Takeaways

- There are challenges and surprises in deploying DNSSEC in a large enterprise, but it can be driven to success
- DNSSEC deployment needs preparation, clean-up, migrations, and monitoring, in addition to the DNSSEC specific tasks

Takeaways

- There are challenges and surprises in deploying DNSSEC in a large enterprise, but it can be driven to success
- DNSSEC deployment needs preparation, clean-up, migrations, and monitoring, in addition to the DNSSEC specific tasks
- The DNS camel's burden from old standards is also tough
  - Examples include the delegation issues and the XFR issues we've discussed
  - This is distinct from the burden of new standards



Thank You

- The DNSSEC deployment at our enterprise was accomplished by a great team. Everyone on the team is an author of this talk, not just Han and Allison. Other authors: Pallavi Aras, Sara Dickinson, Shumon Huque, Neda Kianpour, Tim Wicinski, & Baula Xu.

- We have been immeasurably aided by engineers and product managers at our vendors (A, B, C, D, and E). They know who they are.

Appendix

- Records are updated on the current vendor while installing the zone on the new vendor
- Some update REST API calls fail during Active-Passive Mode

Handling Inconsistency

1. Download the zone files from both vendors
2. Parse the files and extract all inconsistent records
3. Fix the inconsistent records
   a. Check the answers on both vendors (lookup vs. REST API)
   b. Current vendor as the ground truth

	Pros	Cons
DNS lookup (e.g., dig)	1. No rate limit 2. Fast	Latest update may not have propagated yet
Vendor Rest API	Always get latest info	1. Rate limit 2. A little slow