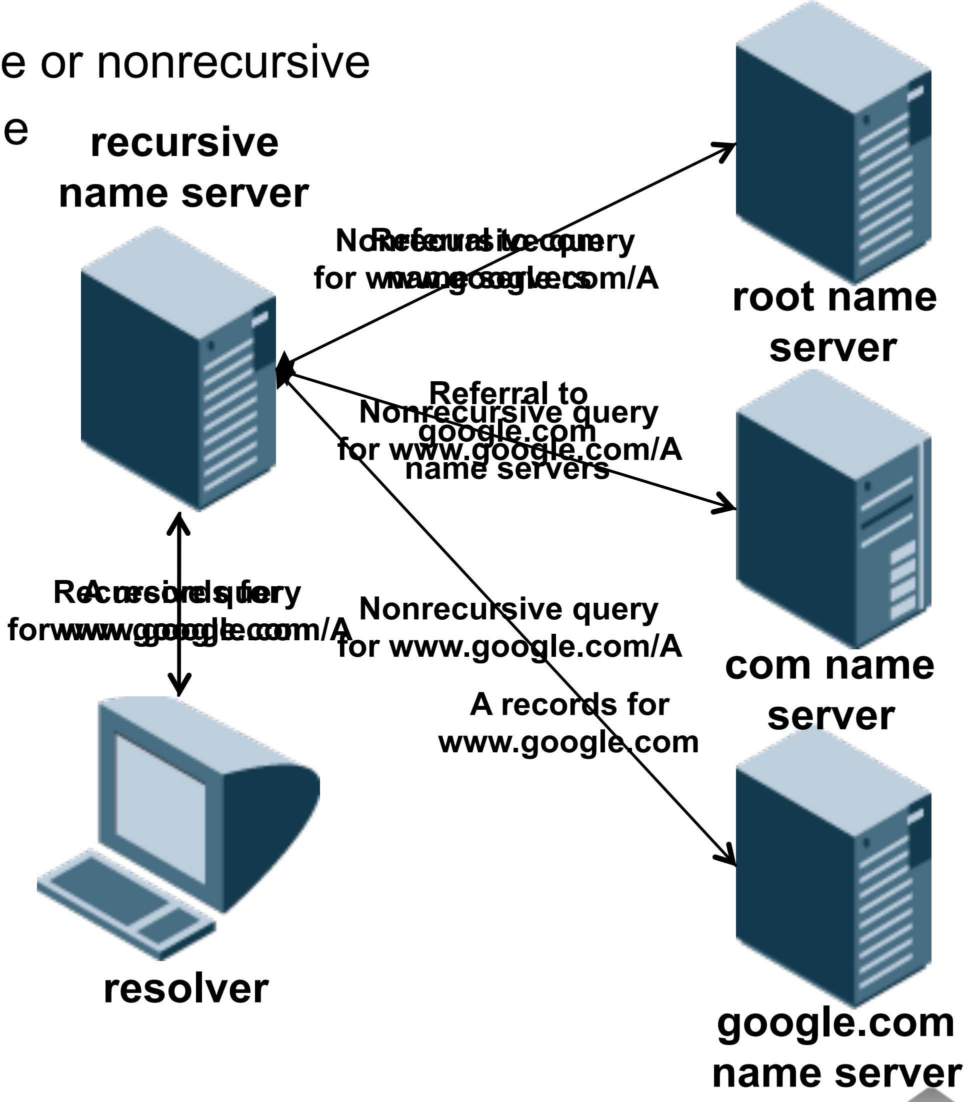
Deploying DNSSEC

November 2011

Thomas Hedströmmer
SE
+46 733 35 95 91
thedstrommer@infoblox.com

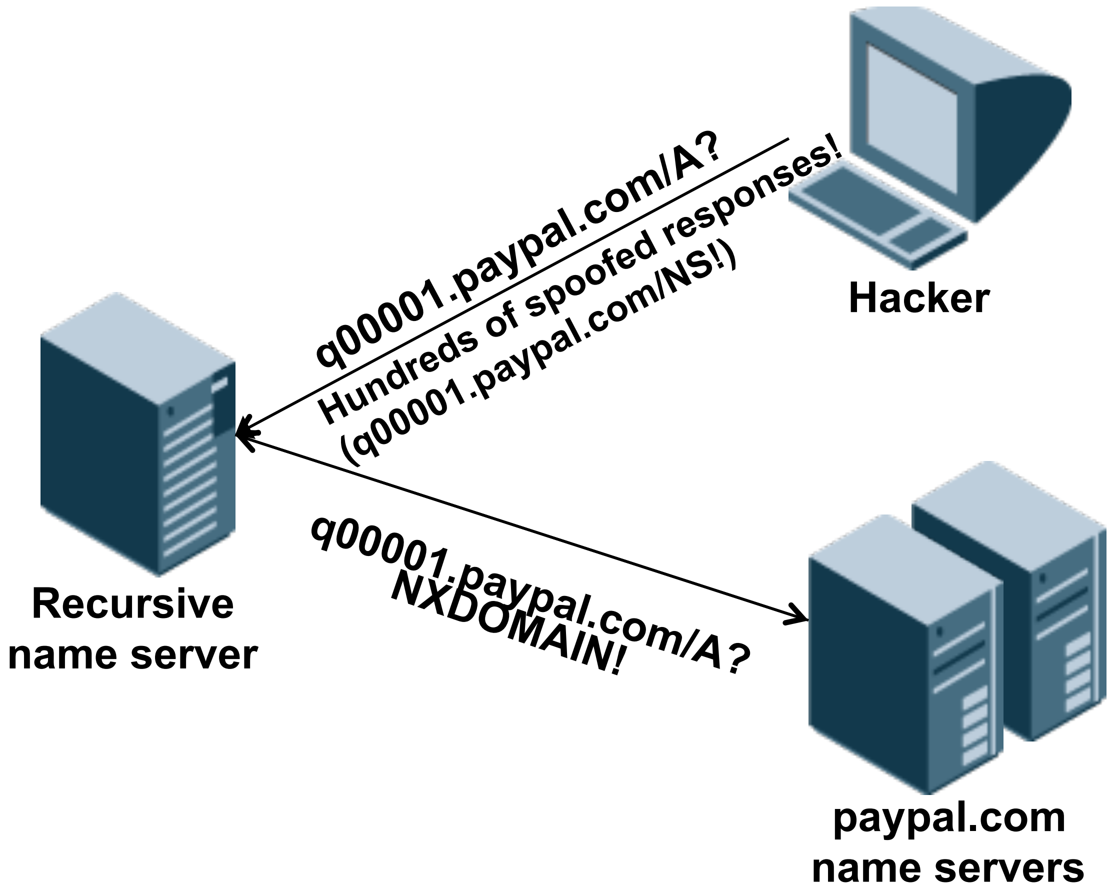
A Review of Recursion

- **What’s recursion, anyway?**
  - DNS queries are either recursive or nonrecursive
  - A recursive query asks the name server to do whatever work is necessary to find the answer, including sending additional queries


recursive name server
Nonrecursive query for www.google.com/A
Referral to com name servers
root name server
Nonrecursive query for www.google.com/A
Referral to google.com name servers
com name server
Recursive query for www.google.com/A
A records for www.google.com
Nonrecursive query for www.google.com/A
A records for www.google.com
resolver
google.com name server

The Kaminsky Vulnerability

- How do you get that many guesses at the right message ID?



The DNS Security Extensions (DNSSEC)

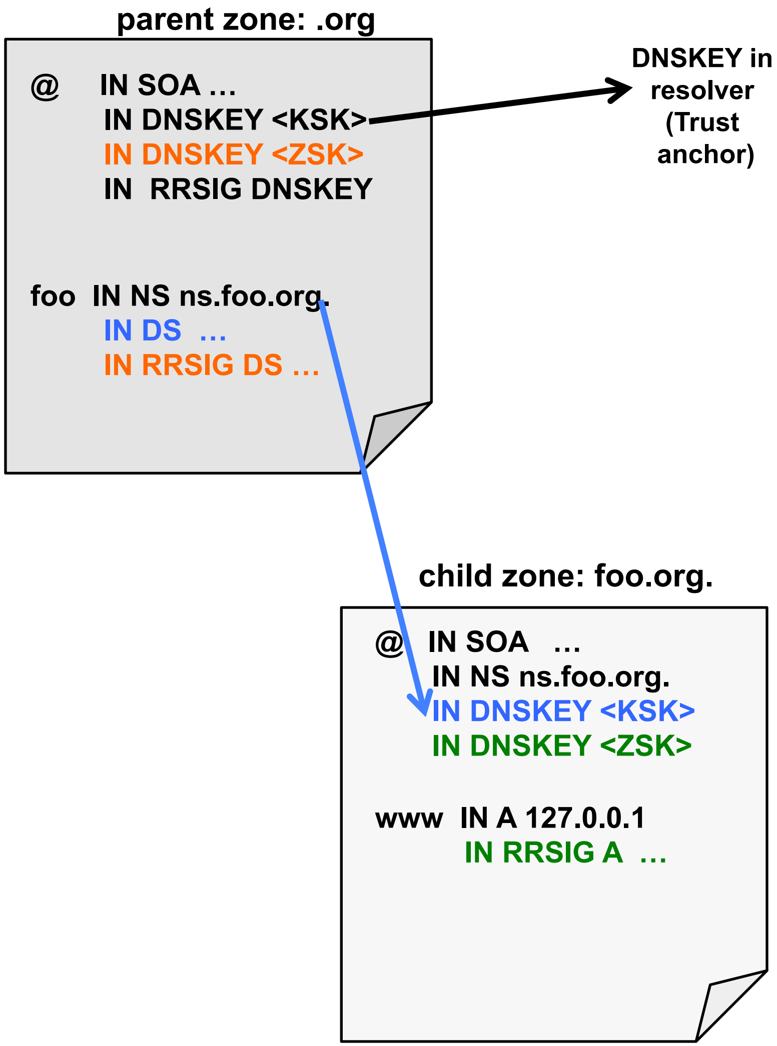
- **The longer-term fix to cache poisoning is DNSSEC, the DNS Security Extensions**
  - Developed within the Internet community's standards process
  - Completely backwards compatible (traditional DNS unaffected)
  - Designed to add source authentication and integrity checking to DNS
    - Using digital signatures (much like digital certificates)
  - DNS data will have digital signatures
    - Parent zones (e.g., .org, .com) will state security status of child subzones (e.g., example.org)
    - Even up to the root
  - Not a perfect solution
    - Does not protect against Denial of Service Attacks
    - Only protects the data, not the quality of the data

The DNS Security Extensions (Continued)

- **How DNSSEC works – some details**
  - DNSSEC adds source authentication and integrity checking to DNS
    - Using digital signatures (asymmetric cryptography), such as RSA
  - Each signed zone has two key pairs
    - A Zone-Signing Key pair, used to sign data in the zone
    - A Key-Signing Key pair, used to sign the zone's public keys
    - Each pair consists of a public and a private key
  - Each RRset in a signed zone is signed with RRSIG records
  - The zone's public keys are published in DNSKEY records
  - The zone's Key-Signing Key is signed by the parent zone's private key
    - Establishing a "chain of trust" from the root to any zone
  - When a DNSSEC-capable recursive name server queries the name servers for the signed zone, they return RRSIG and DNSKEY records that enable the recursive

Authentication Chains in DNSSEC

- **Here, foo.org. has a secure delegation from .org.**
  - Assume that the client has the KSK for .org pre-configured (in black)
  - Using it, the client can trust the ZSK of .org (in orange)
  - The foo.org KSK has a matching DS RR in .org (blue text)
  - .org signs a hash of foo.org's KSK, so if .org is trusted, the client can trust foo.org's key
  - client can then use newly discovered key (foo.org's KSK) to validate data in foo.org.
  - Like all DNS data, DNSKEYs are cached (future validation is quicker)



parent zone: .org

```
@    IN SOA ...
      IN DNSKEY <KSK>
      IN DNSKEY <ZSK>
      IN  RRSIG DNSKEY


foo  IN NS ns.foo.org.
      IN DS  ...
      IN RRSIG DS ...
```

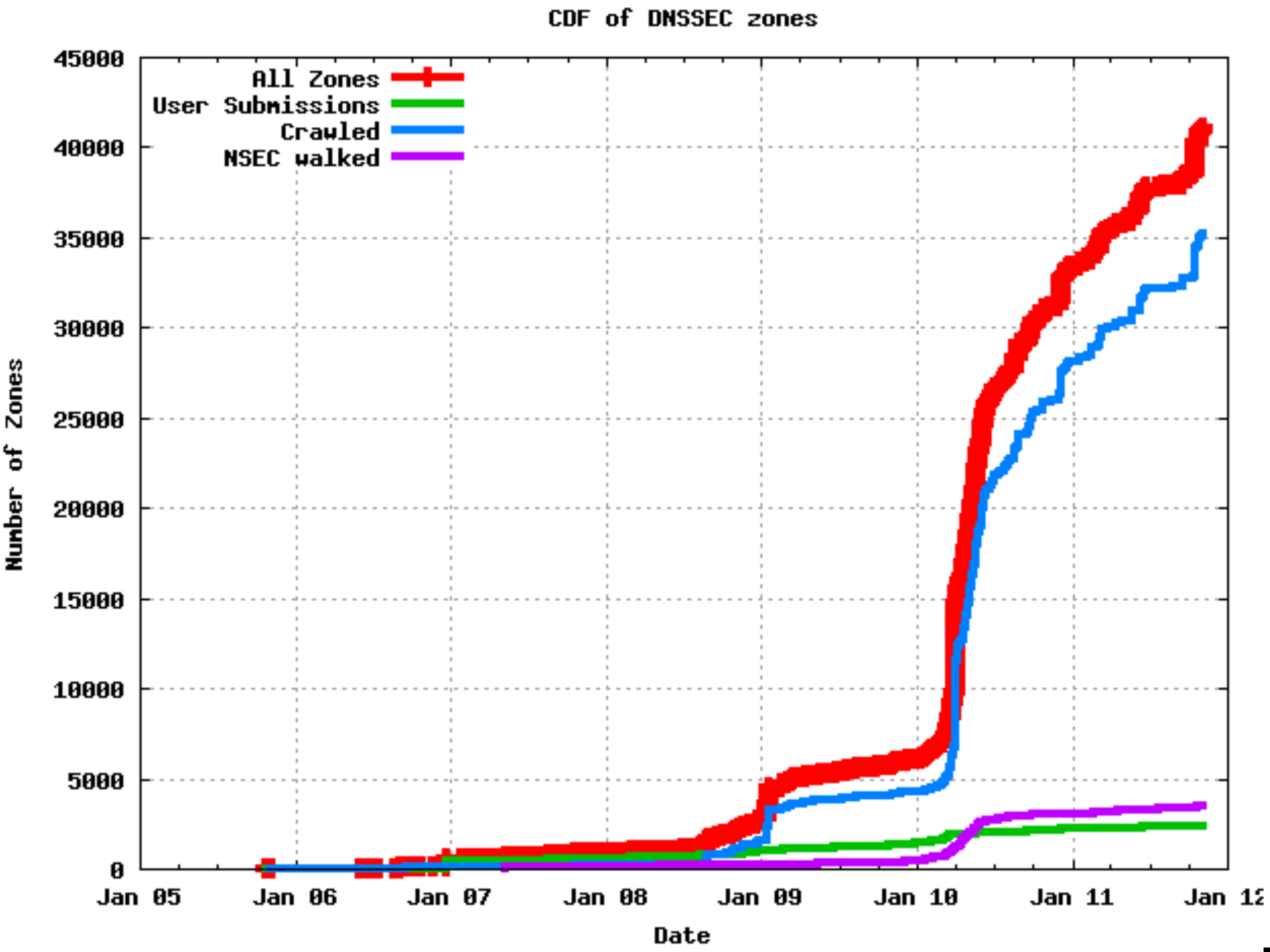
DNSKEY in resolver (Trust anchor)

child zone: foo.org.

```
@   IN SOA   ...
     IN NS ns.foo.org.
     IN DNSKEY <KSK>
     IN DNSKEY <ZSK>

www  IN A 127.0.0.1
       IN RRSIG A  ...
```

DNSSEC Adoption Accelerating
http://secspider.cs.ucla.edu/



Infoblox IB-1852-A DNS Appliance

Performance. Security. Availability.

✓ **1U, rack mountable**
✓ **Hot swappable, field replaceable, redundant AC and DC power supplies**
✓ **LAN1, LAN2, MGMT and HA ports**

High Performance

- Custom built, high performance architecture

•110,000 DNS QPS

- Easy to scale using load sharing with DNS Anycast

- Runs standard NIOS software & supports all standard NIOS features (DNS, DHCP, IPAM, Grid, etc.)

Low TCO

- Central system and data management

- Lower deployment and management costs

- No separate security products required

- Fewer appliances required

- Clear escalation line to 24/7 TAC

Highly Secure

- Secure appliance with hardened OS

- DNS attack monitoring, reporting and mitigation built-in

- One-click system-wide upgrades for quick vulnerability patching

- Vendor alerts for all DNS issues

- HSM support

Highly Reliable

- Built-in redundant fans and Power Supplies

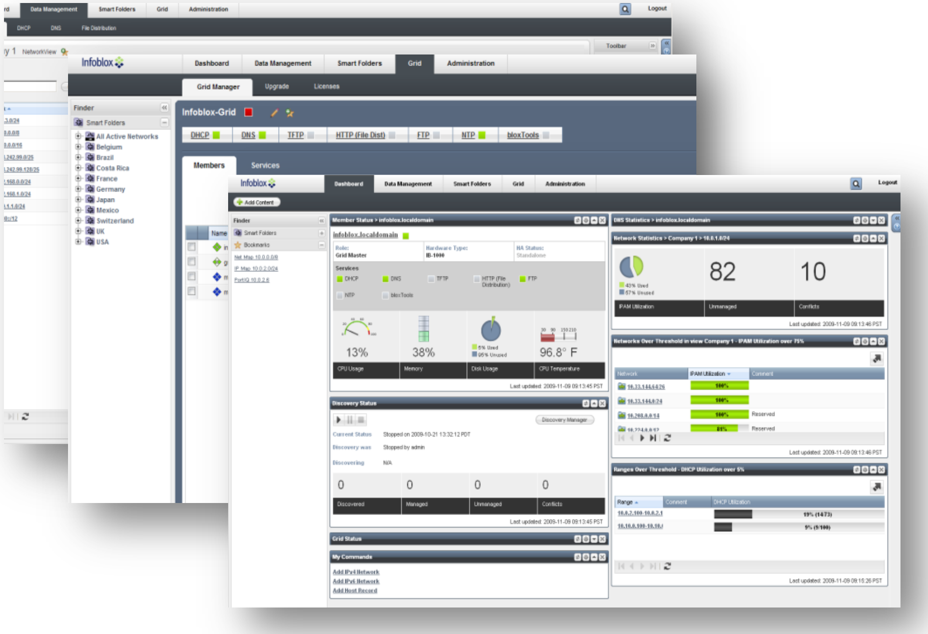
- Hardware HA based on VRRP

- DR for central management

- Automatic healing mechanisms built-in

One GUI does it all

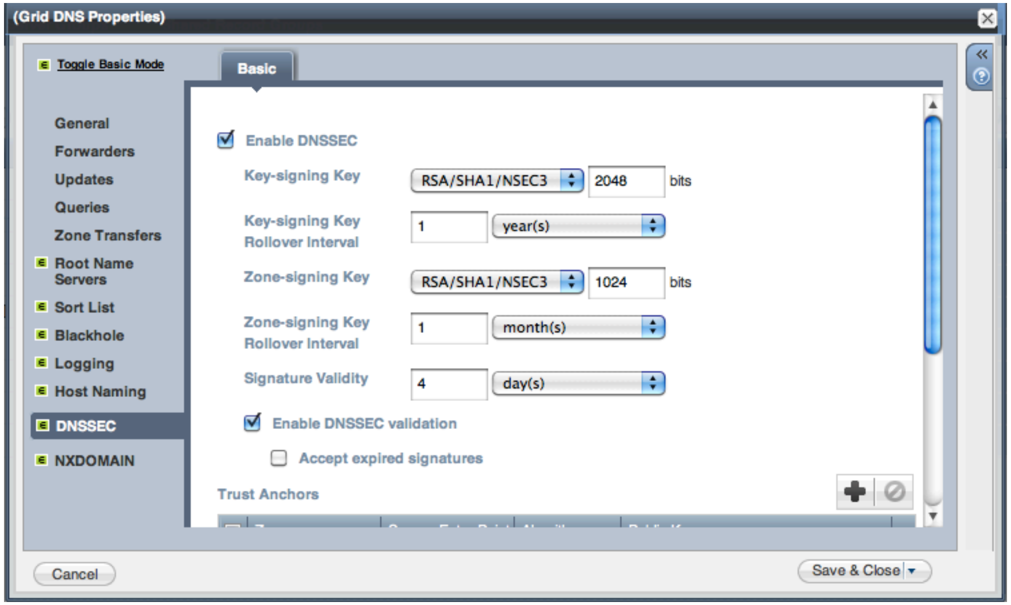
- **Unified Web 2.0 UI**
- **Manages *all* aspects of the solution**
  - DNS
  - DHCP
  - IPAM
  - Grid
  - Device configuration, …
- **Benefits**
  - **No need for using command-line tools and client programs**
  - Easy learning curve
  - Reduced management overhead
  - Reduced configuration errors



Live Demo

Centralized Configuration of All DNSSEC Parameters on All Name Servers

- **Administrators can implement organizational standards by configuring DNSSEC parameters at the Grid level**
  - Default key algorithm, key size and rollover period for both ZSK and KSK
    - Defaults based on NIST 800-81 recommendations
  - Settings inherited by all zones
    - Can be overridden per zone
- **NSEC3 support included**
- **Administrators can configure trust anchors at the Grid level**
  - Configuration inherited by all Grid members



(Grid DNS Properties)

☑ Enable DNSSEC

Key-signing Key: RSA/SHA1/NSEC3 2048 bits

Key-signing Key Rollover Interval: 1 year(s)

Zone-signing Key: RSA/SHA1/NSEC3 1024 bits

Zone-signing Key Rollover Interval: 1 month(s)

Signature Validity: 4 day(s)

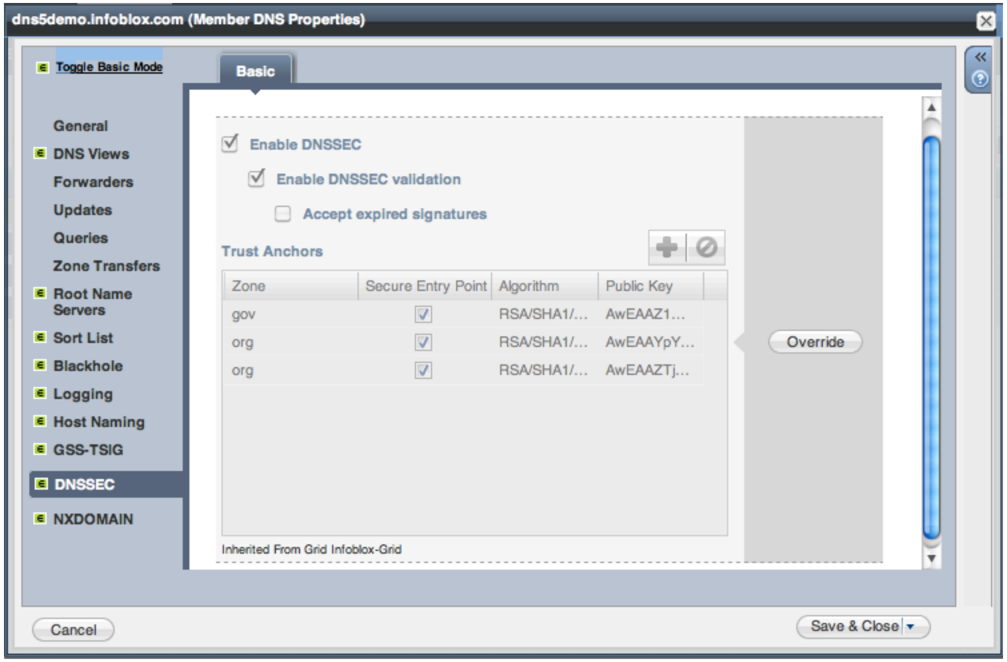
☑ Enable DNSSEC validation

□ Accept expired signatures

Trust Anchors

Configuring DNSSEC on Name Servers

- Single click to enable DNSSEC
- Single click to enable DNSSEC validation of records for an external zone
- Trust anchor configuration inherited from Grid level
  - Administrator can also override at member (name server) level



dns5demo.infoblox.com (Member DNS Properties)

☑ Enable DNSSEC

☑ Enable DNSSEC validation

□ Accept expired signatures

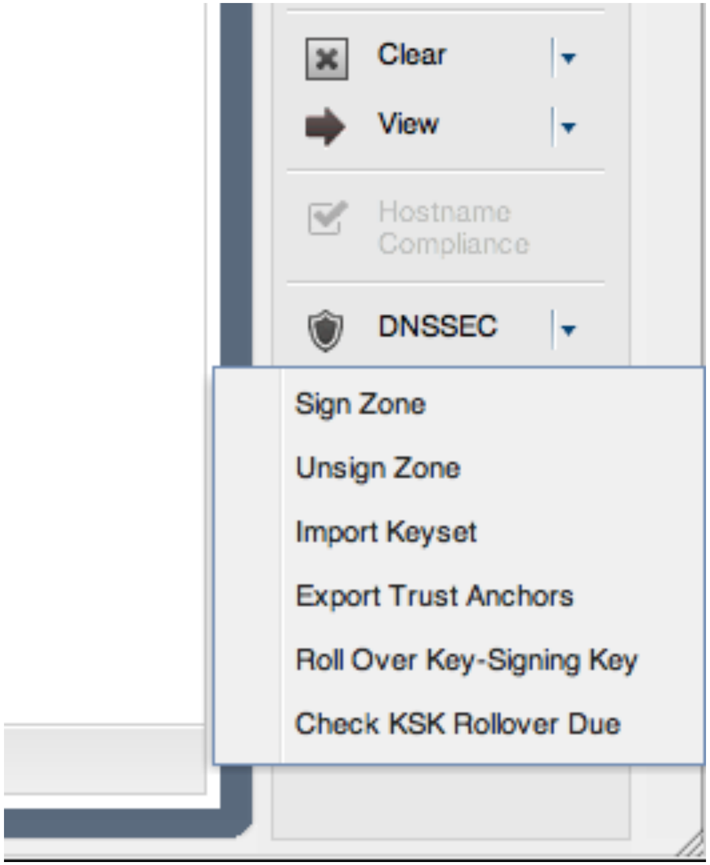
Trust Anchors

Zone	Secure Entry Point	Algorithm	Public Key
gov	☑	RSA/SHA1/...	AwEAAZ1...
org	☑	RSA/SHA1/...	AwEAAYpY...
org	☑	RSA/SHA1/...	AwEAAZTj...

Inherited From Grid Infoblox-Grid

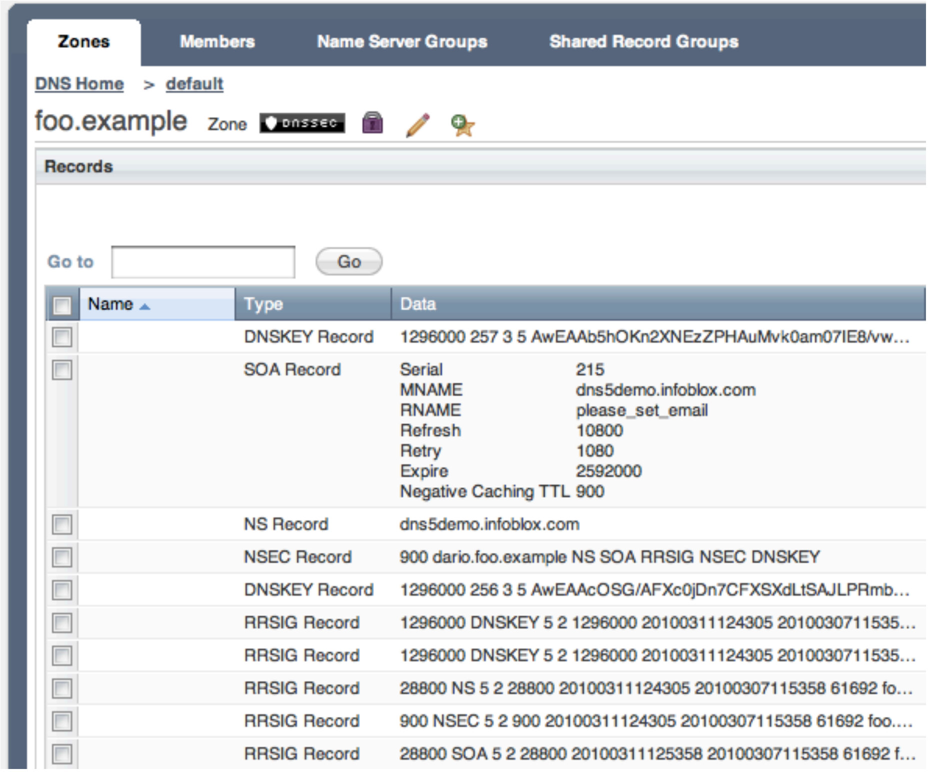
Automated Management of DNSSEC-signed Zones

- **Any zone can be signed with a single click by using the "Sign Zone" toolbar button**
  - Keys are generated on the fly and records are automatically signed
  - Auto-creation of all associated DNSSEC records
- **Automatic maintenance of signed zones**
  - ZSK rollover is handled automatically
  - DNSSEC zones automatically resigned when zone data is modified



Automated Management of DNSSEC-signed Zones (Continued)

- **Signed zones are identified with the DNSSEC icon**
  - The following record types are supported: DNSKEY, RRSIG, DS, NSEC, NSEC3, NSEC3PARAM
- **New Zone Signing Keys are automatically generated when the current keys are due to be rolled over**
  - Key rollover is transparent to the admin
- **Admins are automatically notified in the GUI when KSK rollover is required**
  - Initiating KSK rollover only requires single click



□	Name ▲	Type	Data
□		DNSKEY Record	1296000 257 3 5 AwEAAb5hOKn2XNEzZPHAuMvk0am07IE8/vw...
□		SOA Record	Serial 215 MNAME dns5demo.infoblox.com RNAME please_set_email Refresh 10800 Retry 1080 Expire 2592000 Negative Caching TTL 900
□		NS Record	dns5demo.infoblox.com
□		NSEC Record	900 dario.foo.example NS SOA RRSIG NSEC DNSKEY
□		DNSKEY Record	1296000 256 3 5 AwEAAcOSG/AFXc0jDn7CFXSXdLtSAJLPRmb...
□		RRSIG Record	1296000 DNSKEY 5 2 1296000 20100311124305 2010030711535...
□		RRSIG Record	1296000 DNSKEY 5 2 1296000 20100311124305 2010030711535...
□		RRSIG Record	28800 NS 5 2 28800 20100311124305 20100307115358 61692 fo...
□		RRSIG Record	900 NSEC 5 2 900 20100311124305 20100307115358 61692 foo....
□		RRSIG Record	28800 SOA 5 2 28800 20100311125358 20100307115358 61692 f...

Questions ?

thedstrommer@infoblox.com
nwestberg@infoblox.com