Infoblox
CONTROL YOUR NETWORK

DEPLOYMENT GUIDE

DNSSEC

Contents

Introduction

DNSSEC allows you to sign your DNS data in a way so that other parties can origin authenticate the DNS Resources Records provided by your DNS server. It also provides a way to authenticate denial of existence of Resource Records.

DNSSEC validation

Verifying if the DNS data your server resolves is signed and if so if the signatures can be authenticated.

DNSSEC signing

The cryptographic signing of your zones and records with asymmetric encryption so they can be validated by publicly available information.

DNSSEC provides three key features that are not provided by traditional DNS:

1. Authentication: DNSSEC provides the ability to verify that the data was sent from a verified source. For example, when a response is received with data from example.com, the recipient can be sure that this data was configured by the owner of example.com
2. Data Integrity: DNSSEC allows for the ability to check that the message was not altered during transit. This process is similar to a how checksum for a file works.
3. Proof of non-existence: Traditional DNS provides NXDOMAIN, NXRRSET or NODATA.

It is to be noted that DNSSEC does not provide privacy. Your queries are still sent unencrypted. If you are interested in DNS privacy, have a look at dnscrypt and our ActiveTrust Cloud service which uses dnscrypt.

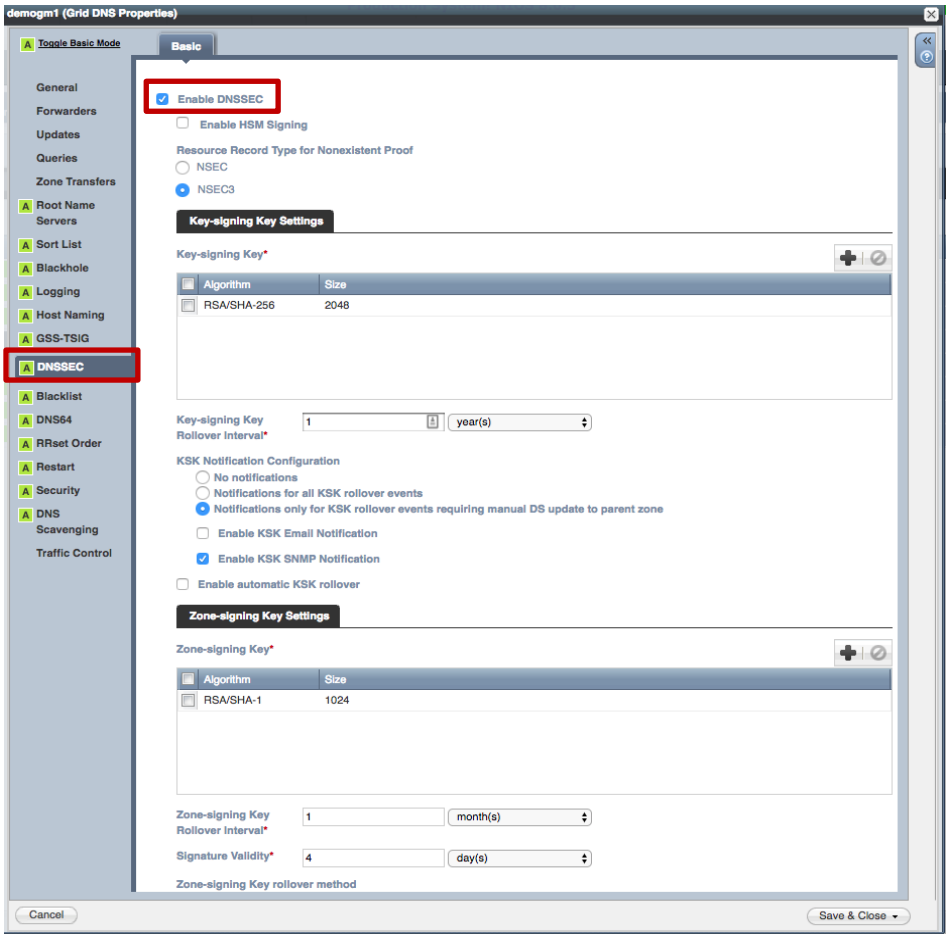
DNSSEC validation

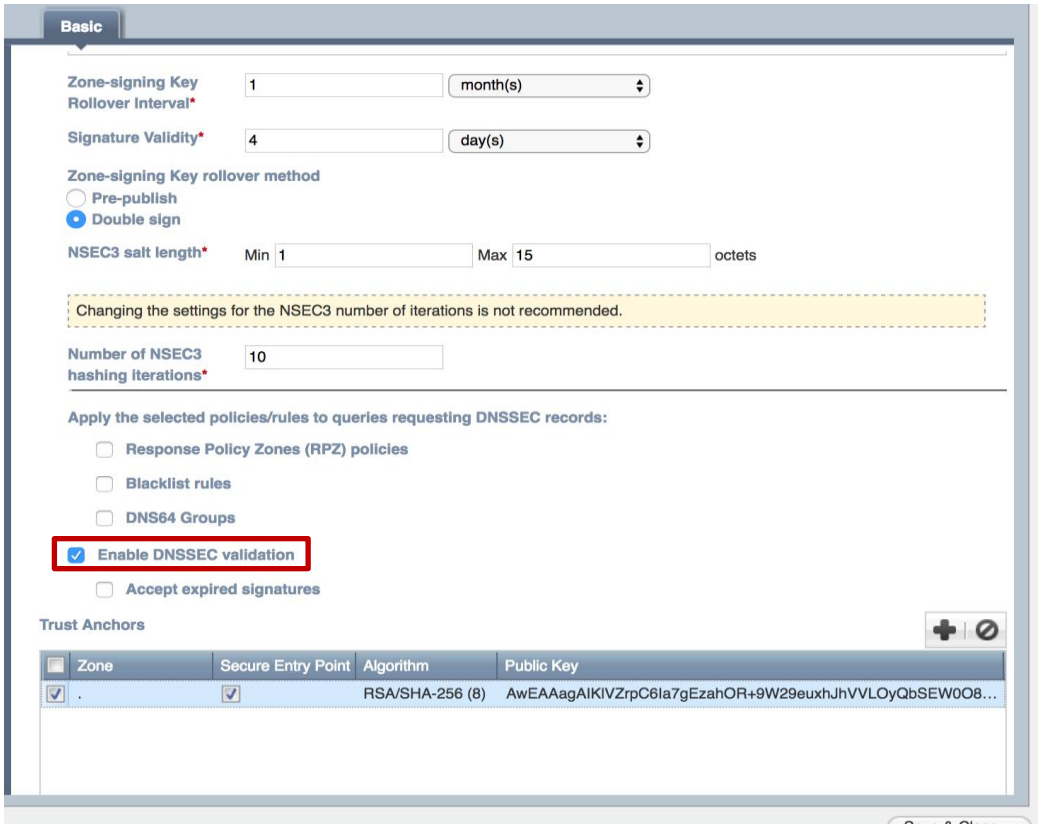
Prerequisites

1. EDNS0 must be enabled and supported by your networking equipment.
    a. Check the section Troubleshooting for a quick method on how to test if your environment supports EDNS0.
2. Recursion must be enabled.

Steps to enable DNSSEC Validation

1. Go to **Data Management > DNS > Grid properties**
2. Toggle advanced on (if not already enabled)
3. Click on DNSSEC
4. Check the Enable DNSSEC box
5. Scroll down and check the Enable DNSSEC validation checkbox
6. Once you have enabled the feature, you will need to obtain the root key(s) in a secure way and enter it/them under Trust Anchors





Root Keys

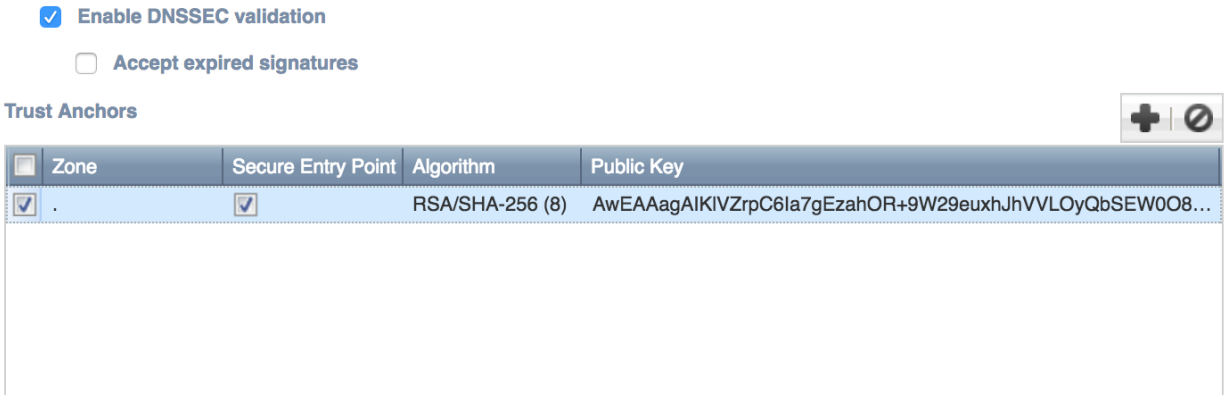
You should ascertain that the key you obtain matches the key provided by IANA. This key is the entry point in your chain of trust on which you will rely for any further validation.

You can find the DS digest of the root key on https://www.iana.org/dnssec/files.

At the moment of writing the Root public key is:

AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0=

Add this key under trust anchors for "." and set the Algorithm to (8).



Special case to consider

Currently most Top Level Domains are signed. However, there are some exceptions to this rule. If you must validate domains under these TLDs then you must import the Public Keys for them manually as Trust Anchors. You can generally use a tool like DIG to get the DNSKEY resource records for these zones, but you must securely verify the authenticity of these public keys. This verification should happen out of band, i.e. outside of the DNS!

DNSSEC Signing

Architecture considerations

DNSSEC uses an additional set of record types (RRSIG, DNSKEY, DS, NSEC, NSEC3, NSEC3PARAM) that all hold digital key signatures. The following is a general set of considerations when deploying DNSSEC:

- Zone size will increase significantly when signed.
- Memory and CPU usage increase.
- DNSSEC answers are larger and consume more bandwidth.
- Interference may be caused by firewalls, proxies, and other middleware.
- Fallback to TCP is more common for answers with DNSSEC data than for answers without DNSSEC data.
- Modern resolvers often already ask for DNSSEC by default, but older clients and resolvers should be identified and may need to have settings turned on to handle DNSSEC.
- When you sign a zone, the Grid Master becomes the primary for the zone. This is for security reasons as the private key is only kept on the Grid Master and Grid Master Candidate.

Prerequisites

EDNS0 must be enabled and supported by your networking equipment

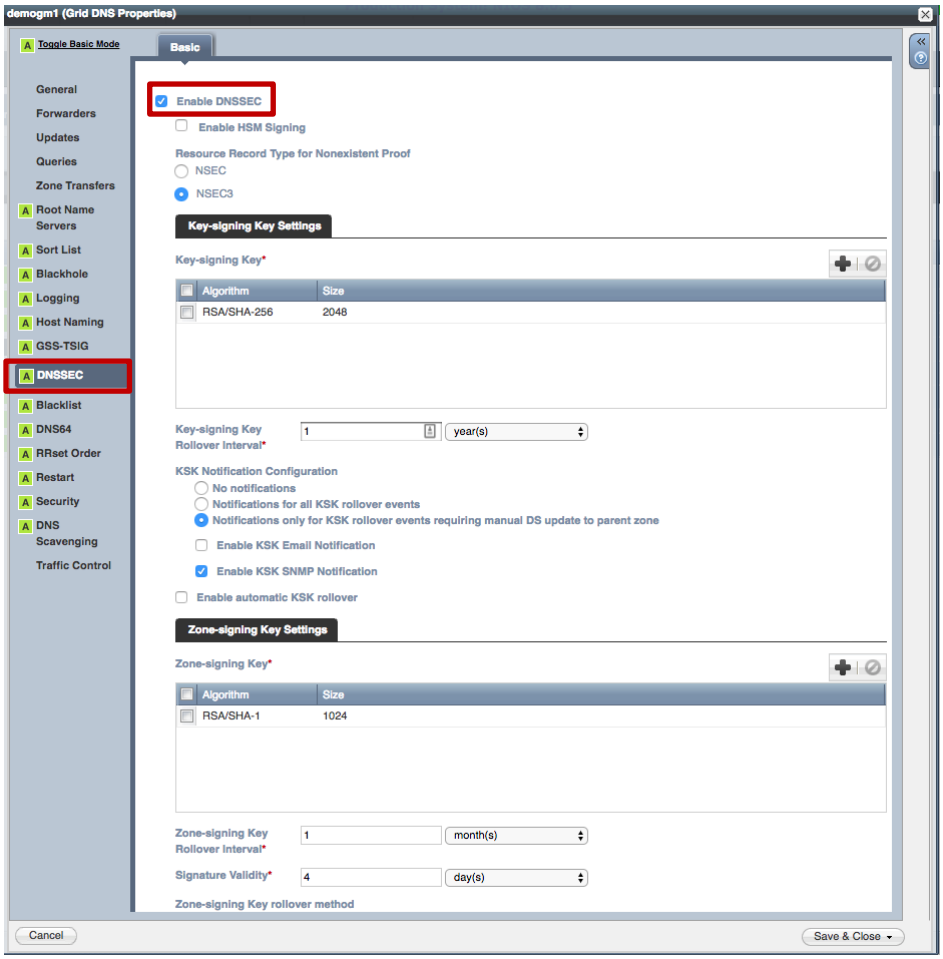
Steps to enable DNSSEC Signing

Setting up parameters

When you specify the DNSSEC settings there are a lot of variables to consider. In this deployment guide, we will be following general best practices. However, for your use case, there might be other requirements based on the government regulations or industry standards.

Please consult with your account team if you are signing zones and the usage of DNSSEC was not included in the original design.

1. Go to **Data Management > DNS > Grid properties**
2. Toggle advanced on (if not already enabled)
3. Click on DNSSEC
4. Check the enable DNSSEC box



5. Select NSEC3 for “Record Type for Nonexistent Proof”
6. Select the Algorithm (RSA/SHA-256) and set the Size (2048) for the Key Signing Key (KSK)
7. Set the Key Signing Rollover Interval to 1 year. This is the rollover period for your main key. 1 year is the current default for KSK rollovers
   - Create a calendar event 50 weeks from now to prepare for your KSK rollover in one year
8. Set Notifications to “Notifications only for KSK rollover events requiring manual DS update to parent zone”

- This means that the system will only notify you for KSK rollovers for which you need to take manual action by uploading the new DS records to your registrar.

9. Do **not** check “Enable automatic KSK rollover”
10. Select the Algorithm (RSA/SHA-256) and set the Size (1024) for the Zone Signing Key (ZSK)
11. Set the ZSK Rollover interval to 1 month and the Signature Validity to 4 days
12. Set ZSK rollover method to pre-publish as this will reduce the number of objects that gets generated during rollovers
13. Keep NSEC3 salt length between 1 and 15 octets and the number of iterations at 10
    - Changing these values to higher numbers can have a considerable impact on the CPU load required to sign zones on an ongoing basis when answering queries for nonexistent resource records.
14. Next enable all options that you want to enable for end hosts requesting DNSSEC records. These settings provide synthesized DNS responses which can be incompatible with DNSSEC. For instance, if a browser has a plugin to authenticate a certificate in a TLSA resource record, it must do DNSSEC verification on the full path. A DNS64 synthesized answer would break the DNSSEC chain of trust and thus be rejected. With these checkboxes, you can choose which DNSSEC incompatible policies you will still perform.

    Apply the selected policies/rules to queries requesting DNSSEC records:

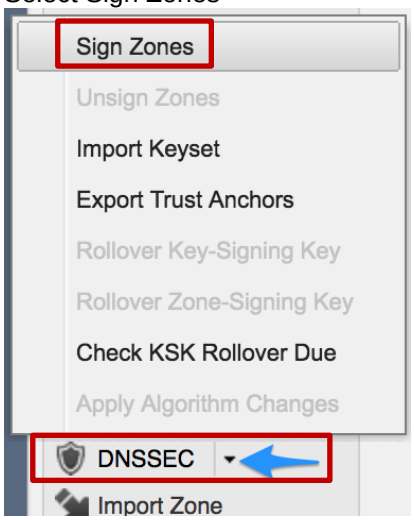
    ☑ **Response Policy Zones (RPZ) policies**

    ☑ **Blacklist rules**

    ☑ **DNS64 Groups**
15. You have completed the setup of your DNSSEC parameters and can now sign a zone.

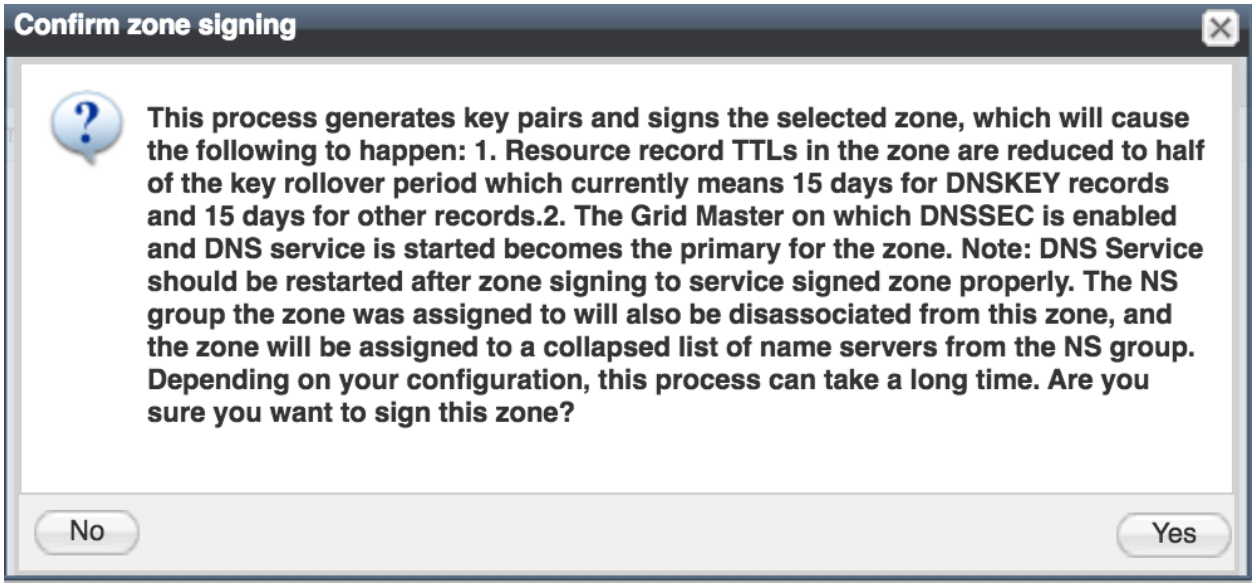
Signing a zone

1. Go to **Data Management > DNS > Zones**
2. Navigate to your external DNS view
3. Select the checkbox in front of a single or multiple zones
4. In the right-hand toolbar use the dropdown next to DNSSEC
5. Select Sign Zones



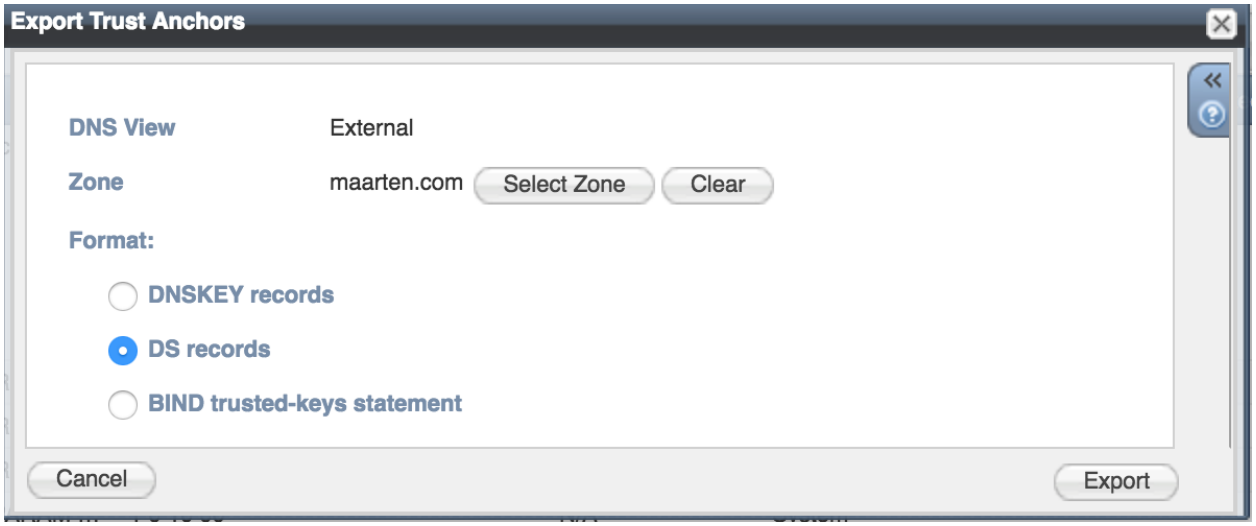
6. You can now remove or add zones from the list. Once completed click the Sign button in the lower right hand corner.

7. **You will get the following warning which is not to be ignored:**



- The results of signing a zone are:
  - All TTLs in the zone are reduced to half the key rollover period (depending on the setting for you ZSK rollover as defined earlier)
  - The Grid Master will become the primary for the zone. (This means you most likely will have to modify the zone settings afterwards in order to ensure your external members are listed as secondaries. If you are using Name Server Groups for this zone it will expand this group into a list of nameserver.)
  - This process can take a long time depending on the size of the zone and the current load on the Grid Master. You should always sign zones on the least busy period of the day.

8. Once the signing is completed you can use the DNSSEC button in the right-hand toolbar and use Export Trust Anchors.



9. These DS records must be uploaded to the parent level domain from the one which you just signed.

Post deployment

Yearly KSK rollovers are recommended and may be required depending on your TLD. If you set up the grid notifications as specified earlier, you will get warnings about the rollover in the WEBGUI. Once you have performed a KSK rollover on a zone, you need to upload the new DS records to your registrar. Once the new KSK has a DS record on all authoritative nameservers for the parent zone and you have waited for the duration of the TTL for the DS record of the old KSK, you can remove the previous DS records of your old KSK from your registrar.

Caveats

DNSSEC validation

Validation settings on the grid-wide level can be overridden on a member level.

New Root Key

Note that the root key is currently being rolled over and that as of September, the new root key will be used. The current root key will be retired end of 2018.

The new root key is:

AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=

DNSSEC Signing

You can override all grid-wide settings on a zone level.

Reverse Zones

If you decide to sign a reverse zone (in-addr.arpa.), it is advised to set the nonexistent proof to NSEC instead of NSEC3 as NSEC3 is more resource intensive to generate and compute for non-existence answers on your authoritative server. NSEC3 protects your data against record enumeration which is only relevant to text-based records and not to a reverse zone where each record is a known IP address.

Troubleshooting

DNSVIZ

The most intuitive method to check for a domain being signed correctly is to use dnsviz. This tool was created by Sandia National Laboratories and Verisign and is considered the gold standard. It allows you to enter a domain and get the full validation of it. It also allows you to look back in time at results. This should be your primary troubleshooting tool in case you are experiencing any problems with validation of an external domain or if you are getting reports on your publicly resolvable domains.

http://dnsviz.net/

DELV

Delv is the DNSSEC aware tool that complements dig, with delv you can provide key files and specify the algorithms to check for. More information can be found under man delv or in the ARM of the version of delv you are using: https://ftp.isc.org/isc/bind9/9.11.0b3/doc/arm/man.delv.html

EDNS0

EDNS0 test with dig from the Infoblox CLI or from any device in your network that runs dig with the following query.

dig +short rs.dns-oarc.net txt

This query runs against a server that OARC has set up to allow testing of EDNS message size. More information is available on: https://www.dns-oarc.net/oarc/services/replysizetest

Root Key

The following tool was created by IANA to let you easily obtain and validate the root key.

Root anchor validation: https://github.com/iana-org/get-trust-anchor

Additional Documentation

Cricket Liu: A best Practice architecture for DNSSEC

IETF website

RFC 2535, 4033, 4034, 4035, 5155, 6781, 7583

Infoblox support: KB 5672 root key rollover

