# NIOS 5.0r1: DNSSEC Made Easy

Internetdagarna 2009

© 2007 Infoblox Inc. All Rights Reserved.

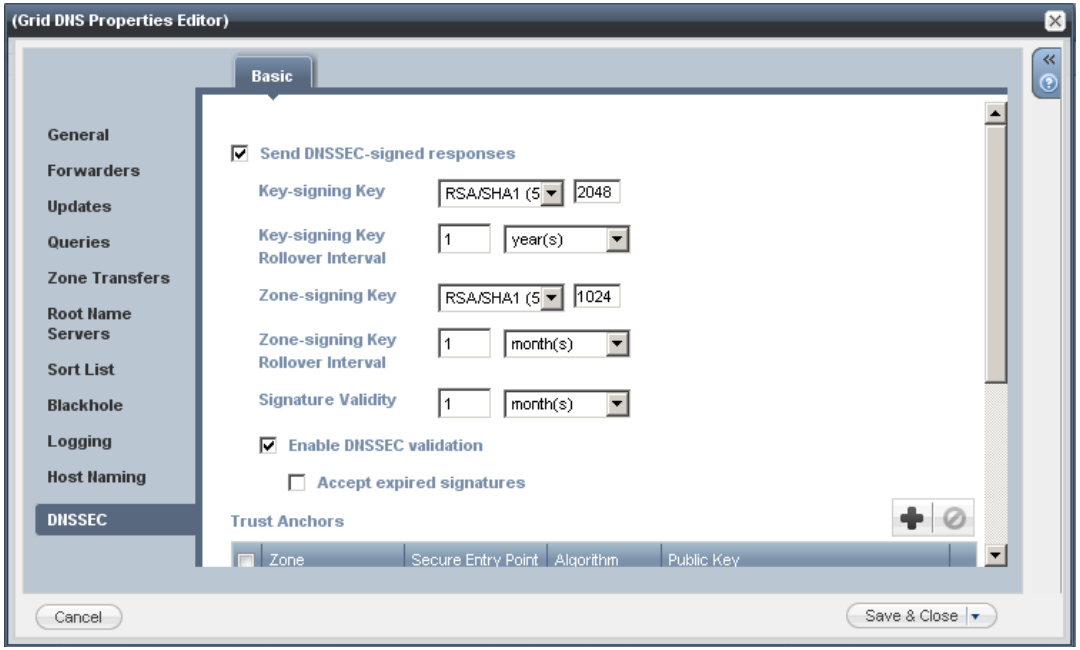
# Infoblox's DNSSEC Support

- **Makes the process of deploying and managing DNSSEC as simple as possible**
  - Nearly transparent to the end user
  - With single-click configuration
  - Automatic and on-the-fly key generation and management

- **Uses the latest technology and protocol features**
  - BIND 9.6.1 with NSEC3 support

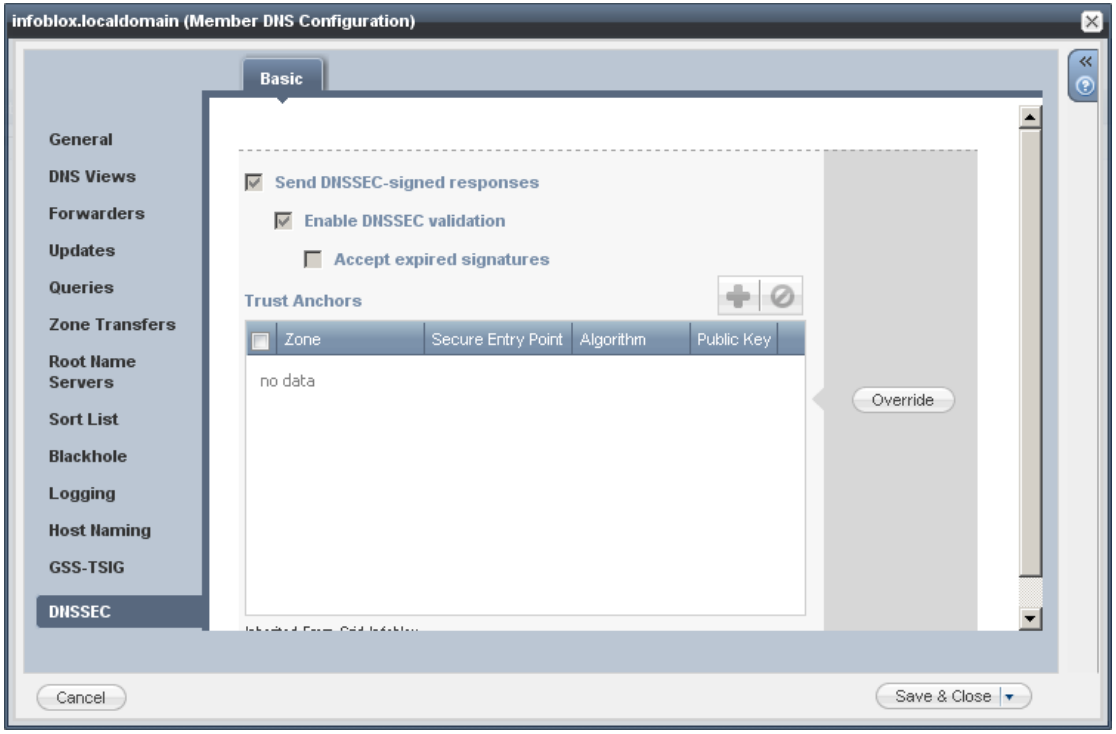
# Easy Access to All DNSSEC Configuration Parameters

- **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
    - KSK is RSA/SHA-1, 2048 bits
    - ZSK is RSA/SHA-1, 1024 bits
- **NSEC3 support included**
- **Administrators can configure trust anchors at the Grid level**
  - Configuration inherited on all grid members



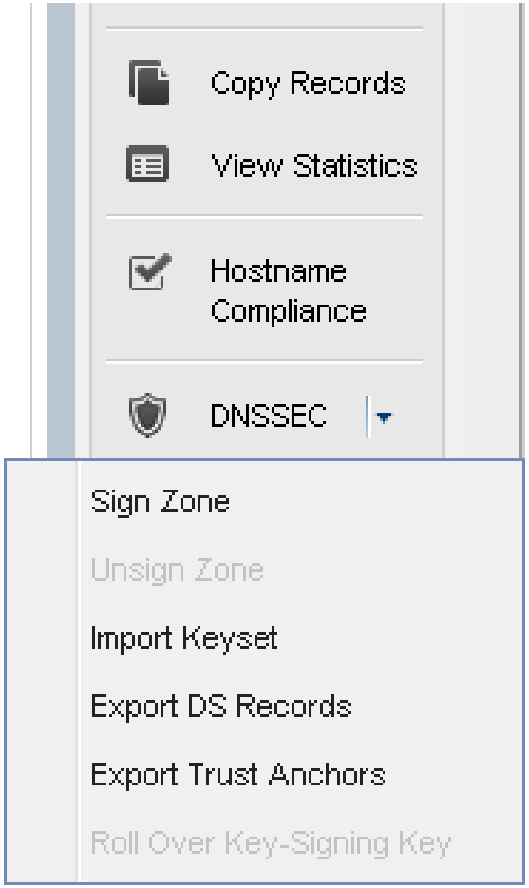
# Configuring a Secondary and/or Recursive Nameserver for DNSSEC

- **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



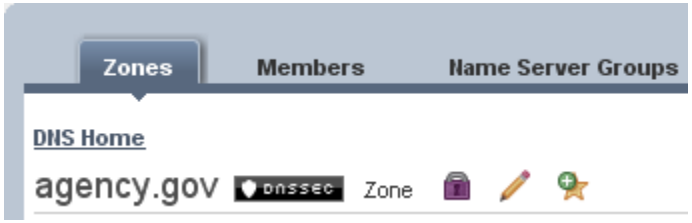
# Automating Management of DNSSEC-signed Zones

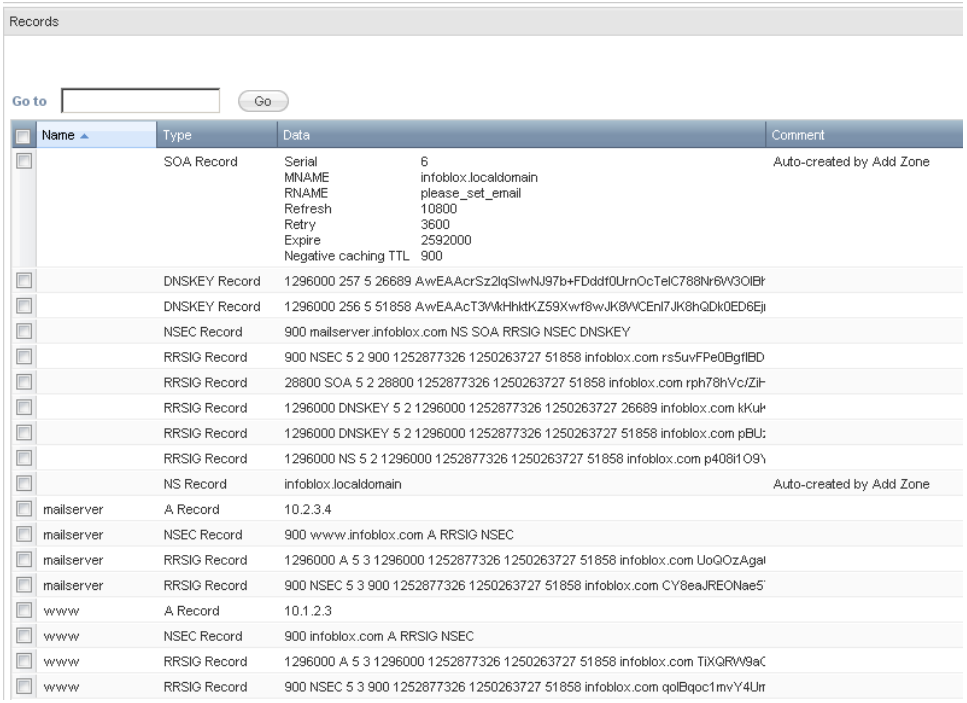
- **Any zone can be signed with a single click by using the "Sign Zone" toolbar button**
  - Keys are generated on the fly and records are automatically signed
  - Auto-creation of all associated DNSSEC records
- **Automatic maintenance of signed zones**
  - ZSK rollover is handled automatically
  -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



# Automating Management of DNSSEC-signed Zones (cont.)

- **Signed zones are easily identified with the DNSSEC icon**
  - The following record types are supported: DNSKEY, RRSIG, DS, NSEC, NSEC3, NSEC3PARAM
- **New Zone Signing Keys are automatically generated before the current keys expire**
  - 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

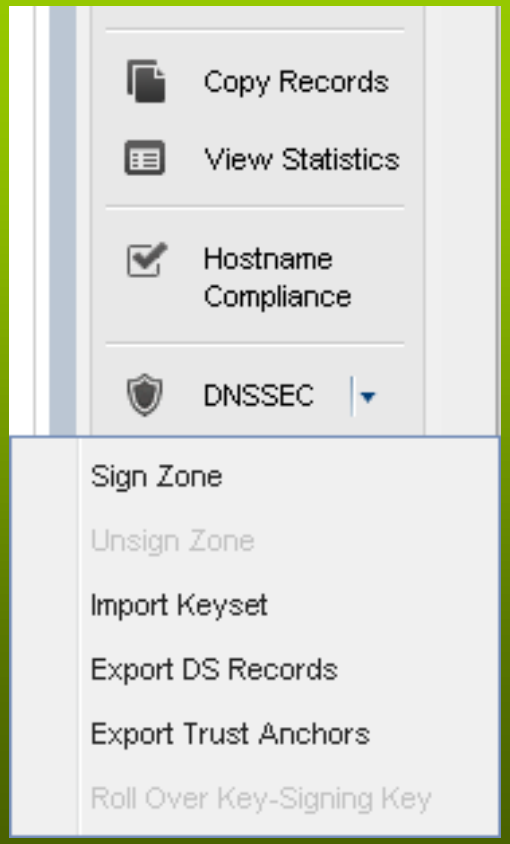


# Comparison with Command-line Configuration of DNSSEC

## The Infoblox way

– One click




## The NIST guidelines for signing a single zone with standard BIND tools are 16 pages long

– Typical steps required to sign a zone:
  - Generate a key pair for the Key Signing Key using the command line tool dnssec-keygen
  - Generate a key pair for the Zone Signing Key using the command line tool dnssec-keygen; e.g., dnssec-keygen –a RSASHA1 –b 1024 –n ZONE foo.com
  - Add the output of the KSK and the ZSK public key to the zone db file
  - Use the dnssec-signzone command line tool to sign the zone using the private key pair; e.g., dnssec-signzone –o foo.com –k Kfoo.com.+005+67829.key /var/named/zonedb.foo.com Kfoo.com.+005+45798.key

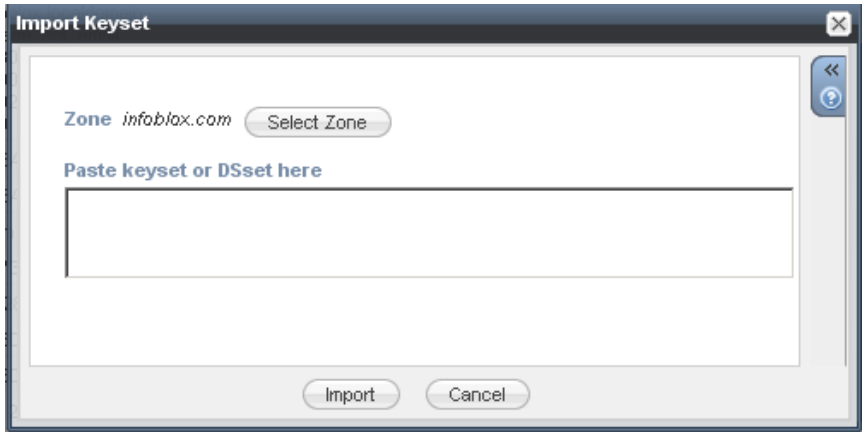
– The zone must be re-signed every time there is a change in the contents

– Manual process is error prone and can take hours

– Tool development requires significant expertise

# Additional DNSSEC Features

- **Easy import and export of DNSSEC keys**
- **Full API support**
  - **Infoblox::DNS::Record::DNSKEY**
  - **Infoblox::DNS::Record::DS**
  - **Infoblox::DNS::Record::NSEC**
  - **Infoblox::DNS::Record::NSEC3**
  - **Infoblox::DNS::Record::NSEC3PARAM**
  - **Infoblox::DNS::Record::RRSIG**
  - **Infoblox::DNS::Zone**
    - **Enable/Disable DNSSEC**
    - **Configure Key Parameters**
    - **Initiate Key Rollover**
  - **Infoblox::Session->export_data()**
    - **Export DS Records and Trust Anchors**
  - **Infoblox::Session->import_data()**
    - **Import DS Records**



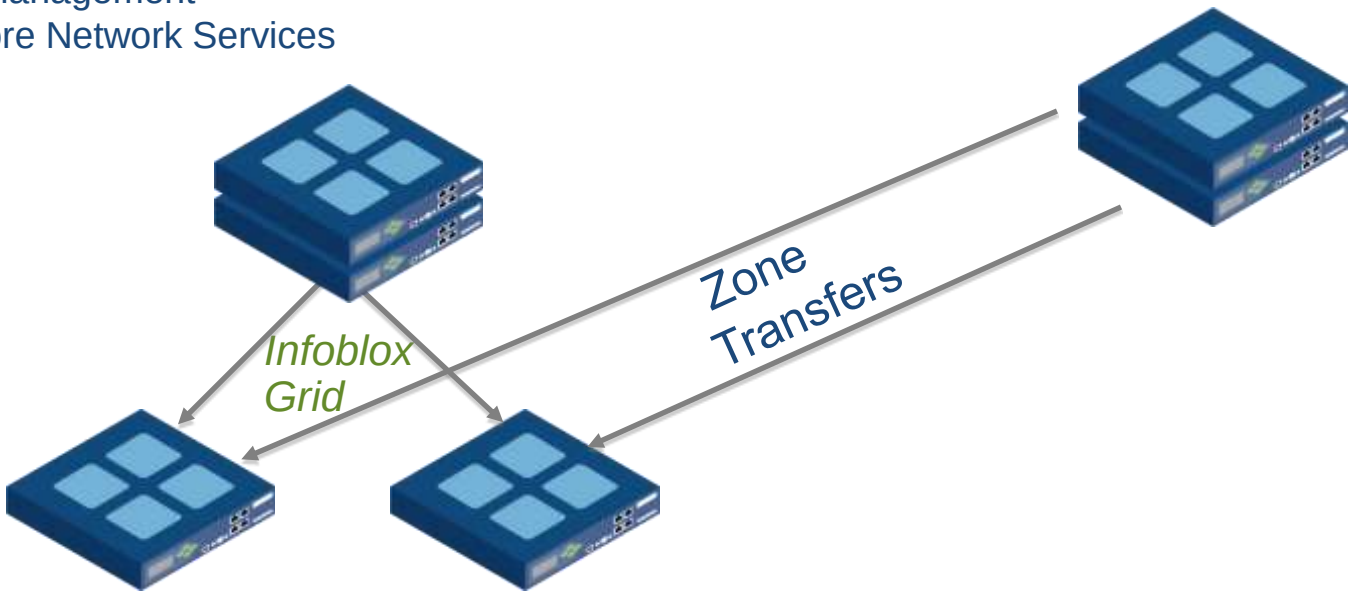

# Timeline

- **Now:**
  - Availability of BIND 9.6.1 with ability to be secondary or recursive server for DNSSEC signed zones (with either NSEC or NSEC3 records) – today with 4.3r5-2
  - Demo of complete DNSSEC feature set
  - Limited availability of early access 5.0r1 release with DNSSEC support, suitable for lab testing to ensure zones are properly signed and to plan for deployment.
- **Nov 23: Availability of early access 5.0r1 release for limited production deployment with full DNSSEC. Customers can sign their external zones and meet the OMB mandate.**
- **Dec 18: General availability of 5.0r1 release. Easy upgrade path from early access releases.**

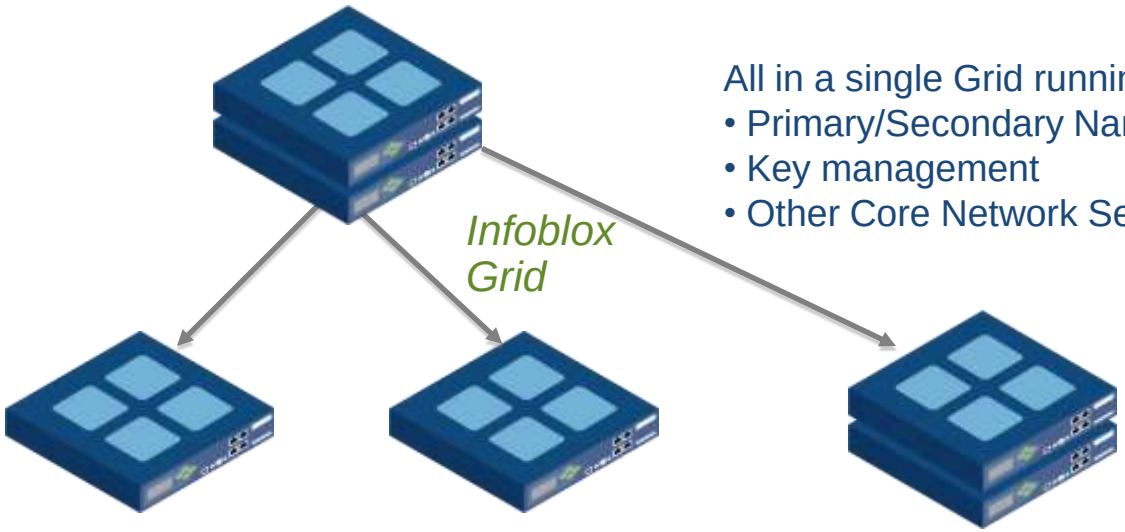
# Initial DNSSEC Deployment – Early Access

Production Grid (4.3r5-2):
- Secondary name servers for DNSSEC zones
- Serves signed zone data
- No key management
- Other Core Network Services

Hidden Primary Name Server (5.0r1 EA):
- Primary name server for DNSSEC zones
- Manages keys and signs DNS records



# DNSSEC Deployment – General Availability




All in a single Grid running GA 5.0r1-1:
- Primary/Secondary Name Servers for DNSSEC zones
- Key management
- Other Core Network Services functions

- **Migration Steps:**
  - Upgrade both the grid and the HA pair to the 5.0r1-1 release
    - This patch release will be available in mid-January 2010
    - Infoblox recommends upgrading the HA pair to 5.0r1-0 when available (12/18)
  - Migrate zone primary function from HA pair to the grid
    1. Make a member in grid be the new DNSSEC primary
    2. Migrate the KSK/ZSK from HA pair to grid (API)
    3. Migrate the DNS records from HA pair to grid (zone import)
  - Documentation/Tools for the above process to be provided