

NIOS 5.0r1: DNSSEC Made Easy

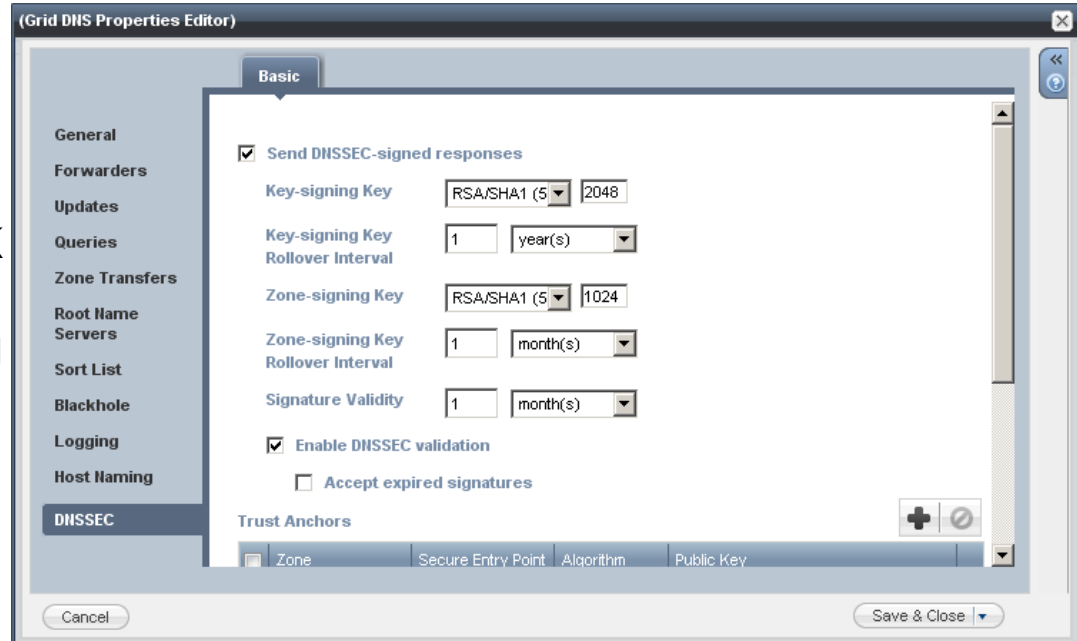
Internetdagarna 2009

- **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



- **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



The screenshot shows the 'Grid DNS Properties Editor' window with the 'DNSSEC' tab selected in the left sidebar. The 'Basic' sub-tab is active, displaying the following configuration:

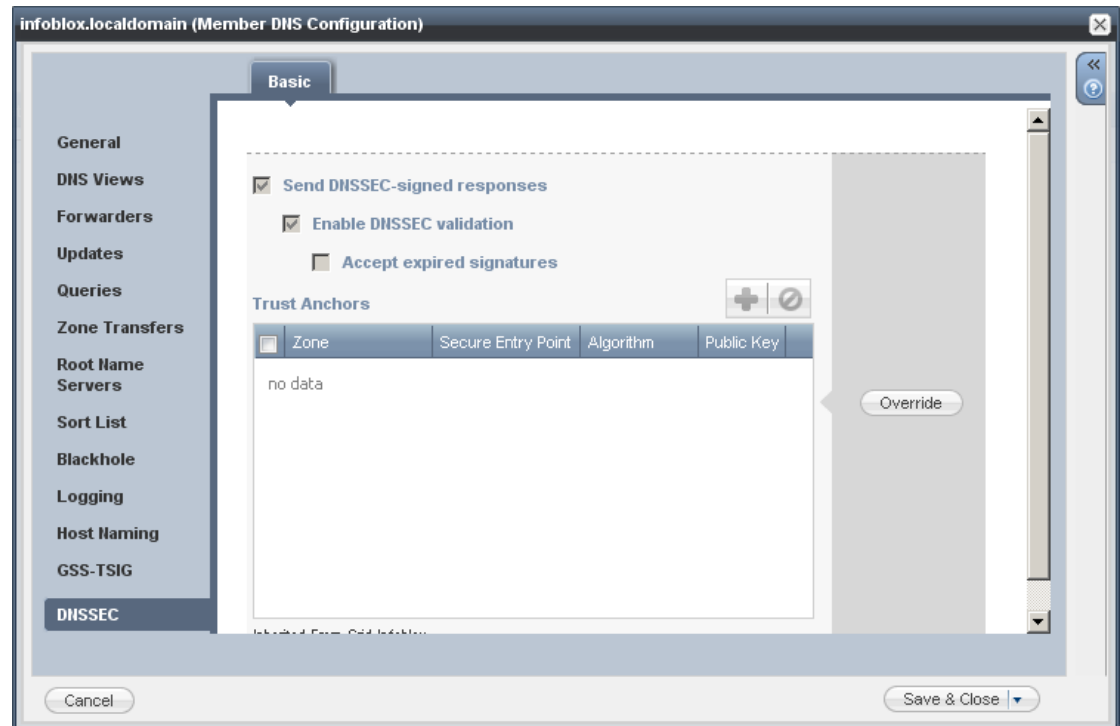
- ☒ Send DNSSEC-signed responses
- Key-signing Key: RSA/SHA1 (5) 2048
- Key-signing Key Rollover Interval: 1 year(s)
- Zone-signing Key: RSA/SHA1 (5) 1024
- Zone-signing Key Rollover Interval: 1 month(s)
- Signature Validity: 1 month(s)
- ☒ Enable DNSSEC validation
- ☐ Accept expired signatures

At the bottom, there is a 'Trust Anchors' section with a table header: Zone, Secure Entry Point, Algorithm, Public Key. The table is currently empty. Buttons for '+', '-', and 'x' are visible next to the table header. At the bottom of the window are 'Cancel' and 'Save & Close' buttons.

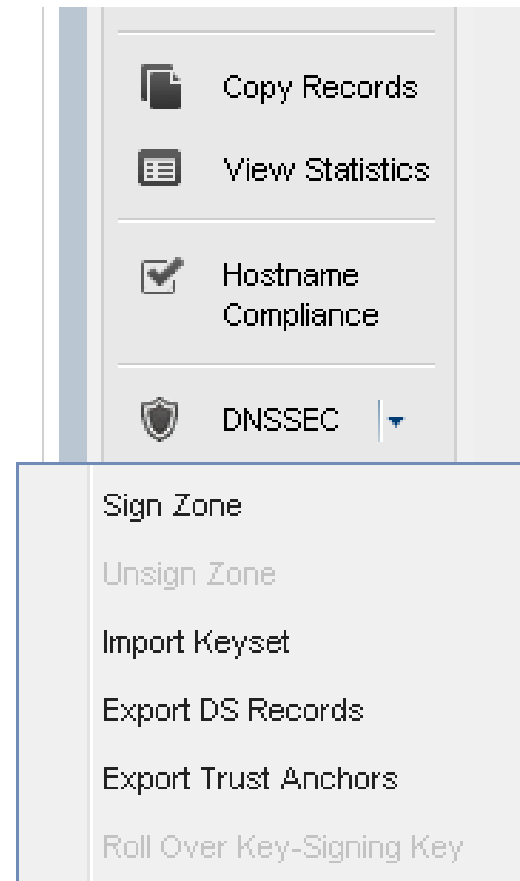
Configuring a Secondary and/or Recursive Nameserver for DNSSEC



- 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



- **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



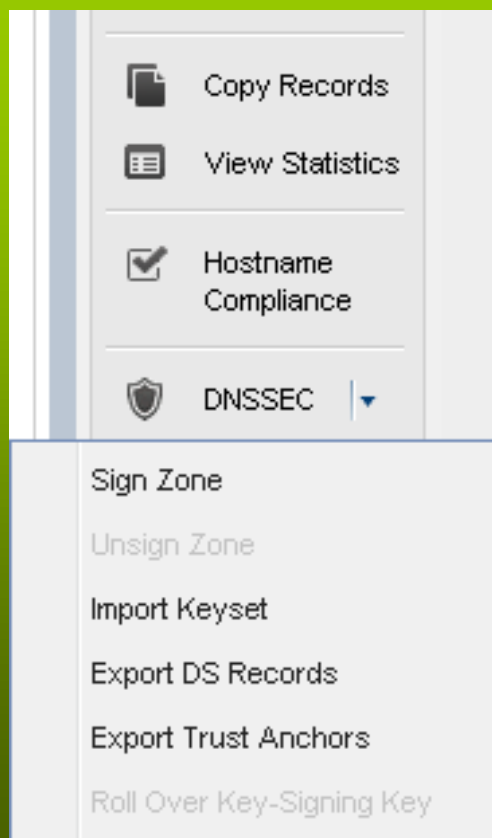
Records

Go to Go

Name	Type	Data	Comment
	SOA Record	Serial 6 MNAME infoblox.localdomain RNAME please_set_email Refresh 10800 Retry 3600 Expire 2592000 Negative caching TTL 900	Auto-created by Add Zone
	DNSKEY Record	1296000 257 5 26689 AwEAAcrSz2lqSlwNJ97b+FDddt0UrnOcTelC788Nr6W3OI8r	
	DNSKEY Record	1296000 256 5 51858 AwEAAcT3WkHhktKZ59Xwrf8wJK8WCEnt7JK8hQDk0ED6Ej	
	NSEC Record	900 mailservr.infoblox.com NS SOA RRSIG NSEC DNSKEY	
	RRSIG Record	900 NSEC 5 2 900 1252877326 1250263727 51858 infoblox.com rs5uvFPeQBgtIBD	
	RRSIG Record	28800 SOA 5 2 28800 1252877326 1250263727 51858 infoblox.com rph78hVc/Zi-	
	RRSIG Record	1296000 DNSKEY 5 2 1296000 1252877326 1250263727 26689 infoblox.com kKu-	
	RRSIG Record	1296000 DNSKEY 5 2 1296000 1252877326 1250263727 51858 infoblox.com pBU-	
	RRSIG Record	1296000 NS 5 2 1296000 1252877326 1250263727 51858 infoblox.com p408t1O9\	
	NS Record	infoblox.localdomain	Auto-created by Add Zone
mailservr	A Record	10.2.3.4	
mailservr	NSEC Record	900 www.infoblox.com A RRSIG NSEC	
mailservr	RRSIG Record	1296000 A 5 3 1296000 1252877326 1250263727 51858 infoblox.com UoQOzAgat	
mailservr	RRSIG Record	900 NSEC 5 3 900 1252877326 1250263727 51858 infoblox.com CY8eaJREONae5	
www	A Record	10.1.2.3	
www	NSEC Record	900 infoblox.com A RRSIG NSEC	
www	RRSIG Record	1296000 A 5 3 1296000 1252877326 1250263727 51858 infoblox.com TiXQRW9ac	
www	RRSIG Record	900 NSEC 5 3 900 1252877326 1250263727 51858 infoblox.com qolBqc1mvY4Ur	

The Infoblox way

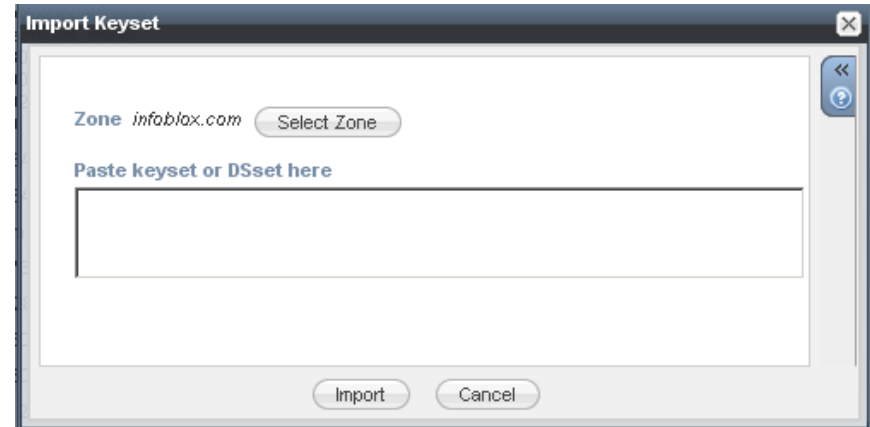
- One click



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

- **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



The 'Import Keyset' dialog box features a title bar with a close button. It contains a 'Zone' field with the value 'infoblox.com' and a 'Select Zone' button. Below this is a text area labeled 'Paste keyset or DSset here'. At the bottom, there are 'Import' and 'Cancel' buttons. A help icon is visible in the top right corner.



The 'Export Trust Anchors' dialog box has a title bar with a close button. It includes a 'Zone' field with 'infoblox.com' and a 'Select Zone' button. The main area is empty. At the bottom, there are 'Export' and 'Cancel' buttons. A help icon is located in the top right corner.

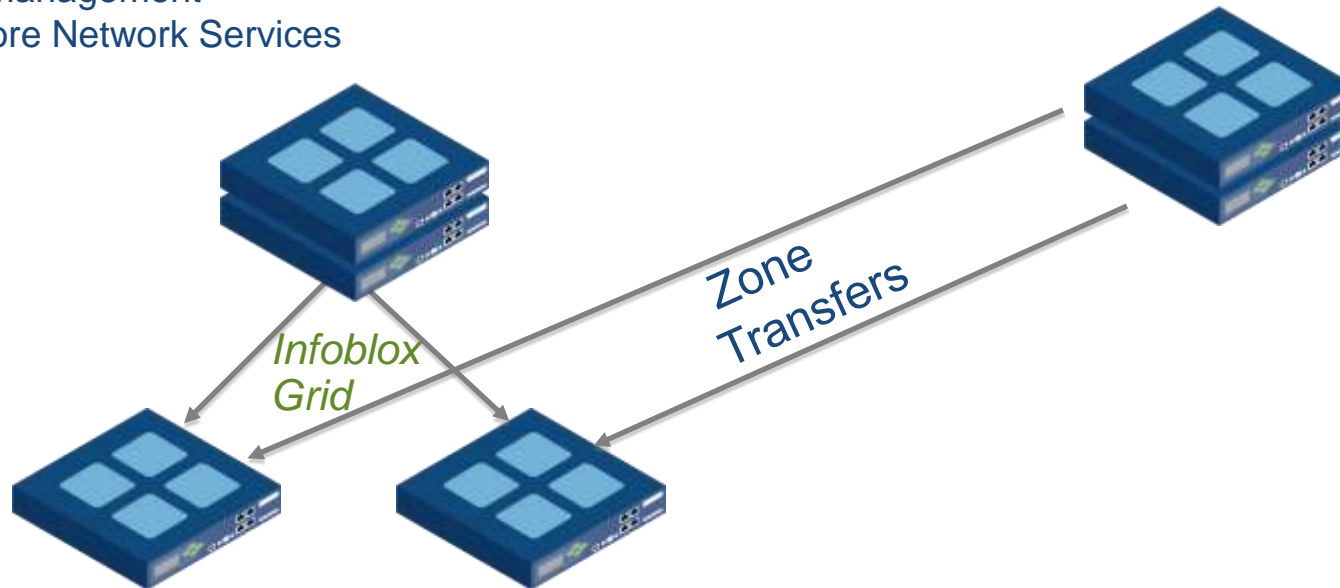
- **Now:**
 - Availability of BIND 9.6.1 with ability to be secondary or recursive server for DNSSEC signed zones (with either NSEC or NSEC3 records) – today with 4.3r5-2
 - Demo of complete DNSSEC feature set
 - Limited availability of early access 5.0r1 release with DNSSEC support, suitable for lab 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.**

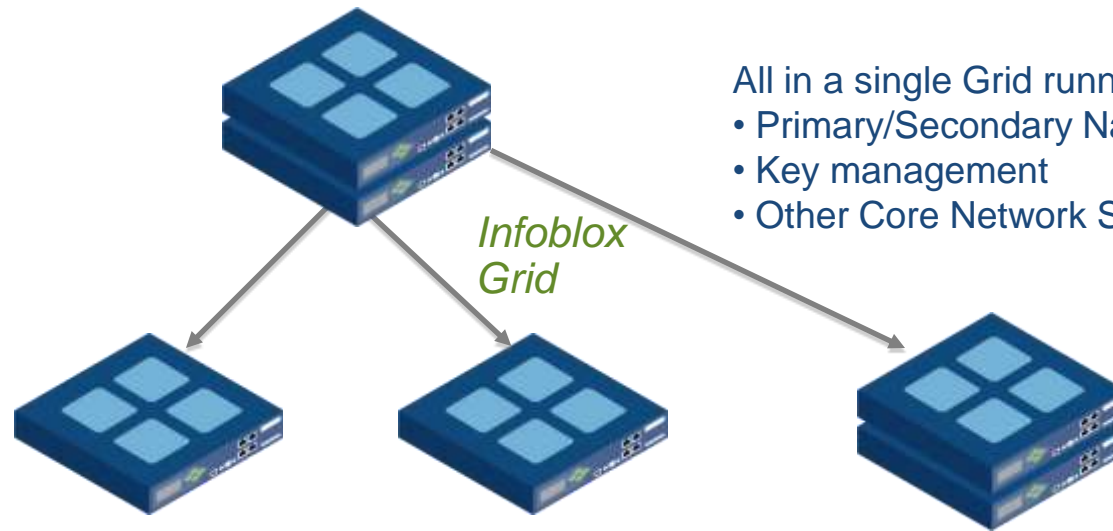
Production Grid (4.3r5-2):

- 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





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