The Infoblox DNSSEC Solution

- Makes the process of deploying and managing DNSSEC as simple as possible
  - Transparent to the end user
  - Single-click configuration
  - Automatic and on-the-fly key generation and management

- Uses the latest technology and protocol features
  - BIND 9.7.0 with NSEC3 support

- HSM Module planned for future release
Infoblox Appliances Automate
Core Network Services

- Integrated core network services on hardened appliances
- Centralized visibility & control of appliances, protocols and data

SIMPLE  SECURE  RELIABLE

© 2010 Infoblox Inc. All Rights Reserved.
IPAM and DNSSEC

- One central Management Interface to all your DNS and even IPAM Data
- API for automation
- Easy to upgrade
- Easy to monitor/audit
### Example zone w/o DNSSEC

#### example.org Zone

<table>
<thead>
<tr>
<th>Name</th>
<th>Comment</th>
<th>Type</th>
<th>Data</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-created by Add Zone</td>
<td>SOA Record</td>
<td>Serial</td>
<td>12</td>
<td>member1.infoblox.net</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MNAME</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RNAME</td>
<td>please_set_email</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Refresh</td>
<td>10800</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Retry</td>
<td>1080</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expire</td>
<td>2592000</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Negative Caching TTL</td>
<td>900</td>
<td></td>
</tr>
<tr>
<td>Auto-created by Add Zone</td>
<td>NS Record</td>
<td>member1.infoblox.net</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto-created by Add Zone</td>
<td>NS Record</td>
<td>member2.infoblox.net</td>
<td></td>
<td></td>
</tr>
<tr>
<td>test</td>
<td>A Record</td>
<td>1.2.3.4</td>
<td>1.2.3.4</td>
<td></td>
</tr>
</tbody>
</table>
Example zone with DNSSEC

```plaintext
<table>
<thead>
<tr>
<th>Name</th>
<th>Comment</th>
<th>Type</th>
<th>Data</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOA Record</td>
<td></td>
<td>Serial</td>
<td>14</td>
<td>infoblox.local/d</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MNAME</td>
<td></td>
<td>domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RNAME</td>
<td></td>
<td>please_set_email</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Refresh</td>
<td></td>
<td>10800</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Retry</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expire</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Negative Caching TTL</td>
<td>900</td>
<td></td>
</tr>
<tr>
<td>RRSIG Record</td>
<td></td>
<td>DNSKEY</td>
<td>5 2 43200 20101125140705 20101</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RRSIG Record</td>
<td></td>
<td>DNSKEY</td>
<td>5 2 43200 20101125140705 20101</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNSKEY Record</td>
<td></td>
<td>DNSKEY</td>
<td>257 3 5 AwEAAAdJEhNTKbRIPYYsaKhroQmQt</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNSKEY Record</td>
<td></td>
<td>DNSKEY</td>
<td>256 3 5 AwEAAAfvo9w7k7pNiCjdfD8kKszV</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RRSIG Record</td>
<td></td>
<td>SOA</td>
<td>5 2 28800 20101125140705 201011211</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto-created by Add Zone</td>
<td></td>
<td>NS Record</td>
<td>member2.infoblox.net</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RRSIG Record</td>
<td>NSEC 5 2 900 20101125140705 201011211</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NSEC Record</td>
<td>test.example.org NS SOA RRSIG NSEC DNS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto-created by Add Zone</td>
<td></td>
<td>NS Record</td>
<td>member1.infoblox.net</td>
<td></td>
</tr>
<tr>
<td>RRSIG Record</td>
<td></td>
<td>A Record</td>
<td>1.2.3.4</td>
<td>1.2.3.4</td>
</tr>
<tr>
<td>test</td>
<td></td>
<td>RRSIG Record</td>
<td>NSEC 5 2 28800 20101125140705 2010112113</td>
<td></td>
</tr>
<tr>
<td>test</td>
<td></td>
<td>RRSIG Record</td>
<td>A 5 3 28800 20101125140705 201011211301</td>
<td></td>
</tr>
<tr>
<td>test</td>
<td></td>
<td>RRSIG Record</td>
<td>NSEC 5 3 900 20101125140705 2010112113</td>
<td></td>
</tr>
</tbody>
</table>
```
Easy Access to All Global DNSSEC Configuration Parameters

- Central configuration of all DNSSEC parameters
- Enforce standards by configuring DNSSEC parameters at a Grid level
  - Default key type, size and validity period
    - Defaults based on NIST-800-81 and RFC 4641 standards
- NSEC and NSEC3 support included
One-Click Zone Signing and Automated Zone Maintenance

- 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
  - All key expiration and resigning are handled automatically
  - DNSSEC zones automatically resigned when new records are added
More useful tasks...
Automating DNSSEC – No Hassles!

- 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 before keys expire
The BIND way
- 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

The Infoblox way
- One click
Even more… also integrates NCCM

Visibility

Infoblox DDI

Detect IPs

Communicate

Change

Automation

Infoblox NCCM

Check Infrastructure

Recognize change

Applications

E-Commerce
Virtualization
Cloud Computing
Messaging
VoIP
Web
ERP
AD
MSFT

Network Infrastructure

Routing, Switching, Firewalls, etc.

IPAM/DDI

DNS
HTTP
DHCP
FTP
TFTP
IPAM
NTP

Check Infrastructure

Provide DDI service
For More Info

DNS Security Center:
http://www.infoblox.com/library/dns-security.cfm

Infoblox DNSSEC Offering:

Infoblox general:
http://www.infoblox.com

Cricket Liu:
http://www.ask-mrdns.com