

# **DNSSEC with BlueCat Networks**

**Christopher Parker-James  
Product Manager  
BlueCat Networks, Inc.**



# Introduction

- BlueCat Networks, Inc.
- Started in 2001 to build a better DNS solution – invented plug and play DNS appliance called “Adonis”
- Moved into IP Address Management (IPAM) in 2005 to take on the challenges surrounding dynamic and static address allocations
- 2009 Introduced DNSSEC integrated solution along with virtualized appliance infrastructure.

# What's Required for Authoritative DNSSEC?

- Name server that supports DNSSECbis
- Create a key signing key and register with the parent zone
- Create a zone signing key and sign it with the key signing key
- Sign the Zone

# Sounds Simple, But...

- Every zone change requires re-signing the zone
- Zones need period re-signing when keys expire
- Zone key rollover every 30 to 90 days (recommended)
- Key signing key roll over requires double signing zone for a specific period
- Maintaining chain of trust for sub-domains

# Challenges Deploying DNSSEC

- TLD and root zone signing - “.com” not until 2011!
- Products to validate and host DNSSEC records
- Key management
- Firewalls configured to avoid DNS packets > 512 bytes
- Debugging difficult
- Additional CPU required to handle signing and validation
- Increased number of queries will impact DNS performance
- Validating NSEC3 records requires more CPU than NSEC
- Windows support will require extensive system upgrades.

# Choosing the Right Solution

- Important RFC's
  - 4033, 4034, 4035 (DNSSECbis)
  - 5155 (NSEC3)
- FIPS 140-2 Compliant
- Level of automation
- Key roll-over
- Authoritative signing
- Recursive resolution

# Quick IP Address Management (IPAM) Review

- Centralize management of IP and DNS space
- Reduce costs managing DHCP and DNS configurations and services
- Reconcile IP addresses (static and dynamic) on the network
- Delegate responsibility to other business units or management groups
- Audit allocation and configuration changes
- Provide tools to plan and assign allocation rules
- Simplify transition to IPv6



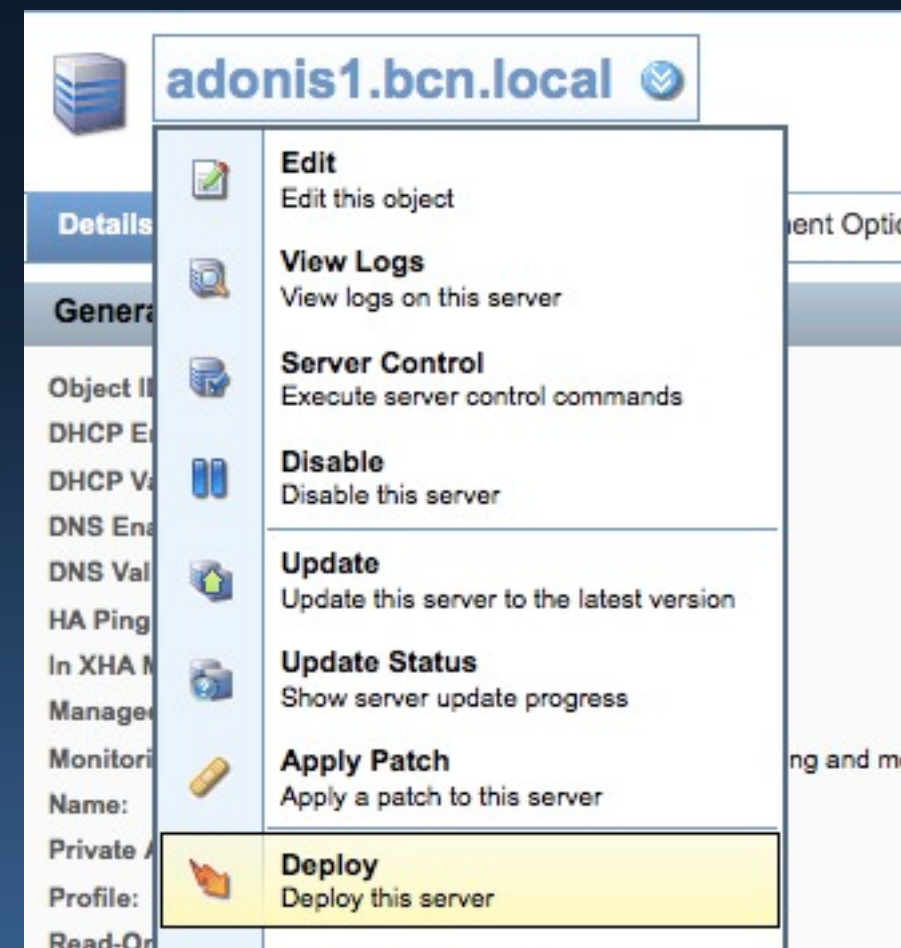
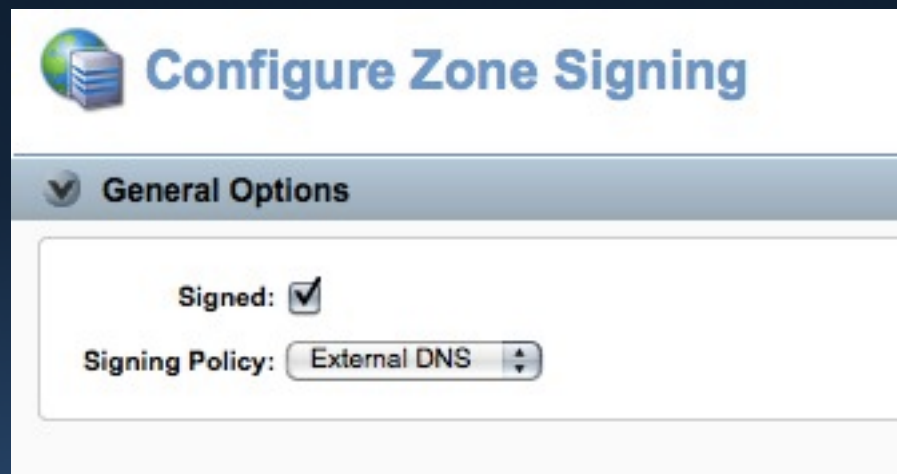
# Why IPAM for DNSSEC

- DNSSEC solution is an **extension** of your **existing** DNS solution
- IPAM greatly simplifies management of internal and external DNS systems
- Allows a unified approach to rolling out changes
- Offers advanced automation that reduces costs
- Provides mechanisms to track and audit changes
- Some organizations will elect to deploy DNSSEC internally




# How we do DNSSEC

- IPAM management system to define and manage IP and DNS space
- Simple click deployment



# Functional Roles

- Authoritative and Recursive DNSSEC




 **DNSSEC - Validation** ▼  
DNS View


[Add to Favorites](#)  
[Printer Friendly](#)

Details | Zones | Zone Templates | External Hosts | ENUM | **Deployment Options** | Deployment Roles | Naming Policy

**Deployment Options** [Settings](#) ▼

New ▼ | Action ▼


<input type="checkbox"/>	Option	Type	Server	Service Option Values	Inherited
<input type="checkbox"/>	 <a href="#">DNSSEC_ENABLE</a>	DNS		true	No
<input type="checkbox"/>	 <a href="#">DNSSEC_VALIDATION</a>	DNS		true	No
<input type="checkbox"/>	 <a href="#">Forwarding</a>	DNS		172.16.12.167	No

 **bluecatnetworks.corp** ▼  
DNS Zone

[Add to Favorites](#)  
[Printer Friendly](#)


Details | Resource Records | Sub Zones | **DNSSEC** | Deployment Options | Deployment Roles | Naming Policy

**Zone Signing**

Signed: Yes  
Signing Policy:  External DNS  
[Configure Zone Signing](#)


**Zone Signing Keys** [Data](#) ▼ | [Settings](#) ▼

Action ▼

<input type="checkbox"/>	Key ID ▼	Start Time	Expiry Time	Active
<input type="checkbox"/>	 <a href="#">1148272</a>	Oct 28, 2009 12:00:00 AM	Nov 27, 2009 12:00:00 AM	Yes



**Key Signing Keys** [Data](#) ▼ | [Settings](#) ▼

Action ▼

<input type="checkbox"/>	Key ID ▼	Start Time	Expiry Time	Active
<input type="checkbox"/>	 <a href="#">1148271</a>	Oct 28, 2009 12:00:00 AM	Oct 23, 2010 12:00:00 AM	Yes


# Key Signing Automation



- DNSSEC Policies

 <b>External DNS</b>  DNSSEC Signing Policy	
Details	Linked Objects
<b>General</b>	
Object ID:	1148270
Name:	External DNS
Signature Validity Period (days):	10
Signature ReSigning Interval (days):	2
Signature Digest Algorithm:	SHA1
ZSK Algorithm:	RSASHA1NSEC3SHA1
ZSK Length (bits):	1024
ZSK TTL:	
ZSK Validity Period (days):	30
ZSK Overlap Interval (days):	7
ZSK Rollover Method:	Pre-publish
ZSK Signing Interval (days):	3
KSK Algorithm:	RSASHA1NSEC3SHA1
KSK Length (bits):	2048
KSK TTL:	
KSK Validity Period (days):	360
KSK Overlap Interval (days):	14
KSK Rollover Method:	Double Signing
KSK Signing Interval (days):	

# Key Maintenance


- Automated and emergency key roll-over

 **bluecatnetworks.corp** ▼  
DNS Zone

 Add to Favorites  
 Printer Friendly



Details | Resource Records | Sub Zones | **DNSSEC** | Deployment Options | Deployment Roles | Naming Policy

**Zone Signing**

Signed: true  
Signature Digest Algorithm: SHA1  
 [Configure Zone Signing](#)



**Zone Signing Keys** Settings ▼

[New](#) ▼ | [Action](#) ▼

<input type="checkbox"/> Key ID ▼	Start Time	Expire Time
<input type="checkbox"/>  <a href="#">787096</a>	Apr 4, 2009 5:55:00 PM	May 3, 2009 5:55:00 PM
<input type="checkbox"/>  <a href="#">787085</a>	Mar 6, 2009 3:05:00 PM	Apr 5, 2009 3:59:00 PM

**Key Signing Keys** Settings ▼


[New](#) ▼ | [Action](#) ▼

<input type="checkbox"/> Key ID ▼	Start Time	Expire Time
<input type="checkbox"/>  <a href="#">787097</a>	Apr 4, 2009 5:56:00 PM	May 3, 2009 5:56:00 PM
<input type="checkbox"/>  <a href="#">787086</a>	Mar 6, 2009 3:05:00 PM	Apr 5, 2009 4:00:00 PM




# DNSSEC Reporting

- Signed zone summary and key rollover information

								
DNSSEC Signing Summary								
Organization:			Date Generated:					
User Name:			admin					
Configuration:			BlueCat Networks					
View:			BlueCat-Demo					
Zone	Signing Enabled	Signing Policy	Zone Signing Keys Status			Key Signing Keys		
			Start Time	Expiry Time	Next Rollover	Start Time	Expiry Time	
corp/bluecatnetworks	Yes	External DNS	2009-10-28 00:00	2009-11-27 00:00	2009-11-20 00:00	2009-10-28 00:00	2010-10-23 00:00	

# Monitoring and Notifications

- Instant alerting into DNSSEC signing and Key status.

 **Subscribe to Event Levels**

**▼ Event Levels Subscription**

Application		<input type="checkbox"/> Warning	<input type="checkbox"/> Error
Deployment Service	<input type="checkbox"/> Success	<input type="checkbox"/> Not Deploy	<input type="checkbox"/> Failed
Data Check Service			<input type="checkbox"/> Error
DHCP Alert Service	<input type="checkbox"/> Info	<input type="checkbox"/> Warning	
Migration Service	<input type="checkbox"/> Info		<input type="checkbox"/> Error
Database Maintenance Service	<input type="checkbox"/> Info	<input type="checkbox"/> Warning	<input type="checkbox"/> Error
IP Reconciliation Service	<input type="checkbox"/> Info		<input type="checkbox"/> Error
Monitoring Service	<input type="checkbox"/> Info		<input type="checkbox"/> Error
Workflow	<input type="checkbox"/> Info	<input type="checkbox"/> Warning	<input type="checkbox"/> Error
XHA	<input type="checkbox"/> Info		
DNSSEC Key Expiration		<input checked="" type="checkbox"/> Warning	<input checked="" type="checkbox"/> Error

# Upcoming Releases and Improvements

- Enhanced DLV and repository support (ITAR, etc)
- FIPS-140-2 Compliant HSM support
- Reporting and Monitoring enhancements.



**Thank You**

