Auth. DNS - Feature # 59: DNSSEC should be implemented for BitFolk domains

Status:	New	**Priority:**	Normal
Author:	admin	**Category:**	
Created:	2011-03-17	**Assigned to:**	
Updated:	2023-04-12	**Due date:**	
Subject:	DNSSEC should be implemented for BitFolk domains		

Description:

DNSSEC records should be added to the various BitFolk domains.

List of relevant domains:

* -@0.0.0.0.7.0.1.1.a.0.a.2.ip6.arpa@- (reverse zone for @2a0a:1107:0::/48@, the only part of BitFolk's own IPv6 /29 that's currently in use)
* -@1.f.1.0.0.0.0.0.8.a.b.0.1.0.0.2.ip6.arpa@- (reverse zone for @2001:ba8:0:1f1::/64@ which is a Jump-assigned linknet)
* -@1.f.1.0.8.a.b.0.1.0.0.2.ip6.arpa@- (reverse zone for @2001:ba8:1f1::/48@, the IPv6 assignment from Jump)
* -@136.168.185.in-addr.arpa@- (reverse zone for @185.168.136.0/24@)
* -@80.119.85.in-addr.arpa@- (programmatically generated reverse zone for @85.119.80.0/24@)
* -@81.119.85.in-addr.arpa@- (programmatically generated reverse zone for @85.119.81.0/24@)
* -@82.119.85.in-addr.arpa@- (programmatically generated reverse zone for @85.119.82.0/24@)
* -@83.119.85.in-addr.arpa@- (programmatically generated reverse zone for @85.119.83.0/24@)
* -@84.119.85.in-addr.arpa@- (programmatically generated reverse zone for @85.119.84.0/24@)
* -@85.119.85.in-addr.arpa@- (programmatically generated reverse zone for @85.119.85.0/24@)
* -@86.119.85.in-addr.arpa@- (programmatically generated reverse zone for @85.119.86.0/24@)
* -@87.119.85.in-addr.arpa@- (programmatically generated reverse zone for @85.119.87.0/24@)
* -@bitfolk.co.uk@- (at the moment same content as @bitfolk.com@)
* -@bitfolk.com@-
** -@acmesh.bitfolk.com@- (dynamic updates subdomain used for @acme.sh@ DNS-01 Let's Encrypt renewals)
** -@console.bitfolk.com@- (subdomain that is programmatically generated for customer Xen Shell host names)
* -@bitfolk.space@- (forward DNS for use as hostnames for customers that don't have their own domains)
** -@autov6rev.bitfolk.space@- (dynamically-generated forward zone for customers that do not set their own IPv6 reverse DNS)

http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
http://wiki.powerdns.com/trac/wiki/PDNSSEC

Some customers have their IPv4 and IPv6 reverse DNS as delegated zones, so there will need to be a way for them to optionally supply DS records for this. As the zones are programmatically generated the DS records can't just be manually inserted.

This task will cover the modifications to the customer database so that DS records can be supplied for customer reverse zones, and built into the generated zones. Initially DS records will be supplied by support

ticket. A separate task will cover enhancing the panel to allow DS records to be supplied.

History

2011-09-18 12:24 - admin

- Project changed from Misc infrastructure to Auth. DNS

2011-09-18 12:28 - admin

We're now running an RC of PowerDNS 3.0 on b.authns.bitfolk.com and c.authns.bitfolk.com, and this version does claim to support DNSSEC. It hasn't yet been tested.

2014-10-25 09:11 - halleck

Any progress on getting the bitfolk.com zone signed?

From what I have understood the DNSSEC support in PowerDNS has improved a lot the last couple of years.

2019-01-23 11:19 - willow

Note that the documentation for PowerDNS (assuming you are using 4.1 or 4.2) is now at https://doc.powerdns.com.
Most likely the link to replace http://wiki.powerdns.com/trac/wiki/PDNSSEC in the original issue post would be https://doc.powerdns.com/authoritative/dnssec/index.html

2019-01-23 11:27 - admin

This feature request should probably be rewritten as a lot of things have changed.

The primary auth server at BitFolk is now BIND, with the secondary servers being PowerDNS. DNSSEC support in both of those products is good. I've had a few zones running with DNSSEC signing and haven't really had any problems.

I am still really scared about adding it to bitfolk.com. I don't feel confident with DNSSEC yet. I will try to work on this.

2023-04-10 02:28 - admin

- Subject changed from DNSSEC should be implemented for bitfolk.com to DNSSEC should be implemented for BitFolk domains

2023-04-10 02:35 - admin

The following domains are managed by Jump who do not want to delegate DNSSEC.
They would rather we moved away from using the associated address space, since
we have had our own for a very long time. So those will not get DNSSEC records
and instead there will be a separate task to migrate away from using them.

* @1.f.1.0.0.0.0.0.8.a.b.0.1.0.0.2.ip6.arpa@
* @1.f.1.0.8.a.b.0.1.0.0.2.ip6.arpa@

2023-04-10 02:37 - admin

Fix typo in task description

2023-04-10 02:41 - admin

DNSSEC has already been implemented for the following domains:

* @0.0.0.0.7.0.1.1.a.0.a.2.ip6.arpa@
* @136.168.185.in-addr.arpa@
* @bitfolk.space@

2023-04-10 02:50 - admin

I forgot about @autov6rev.bitfolk.space@ which is used for dynamically-generated host names for customers who do not set their own IPv6 reverse DNS.

This is implemented as a PowerDNS pipe backend and I'm not sure how to do DNSSEC for one of those (or for a "remote backend", which it probably should be reimplemented as).

We're declaring this one out of scope for DNSSEC. Customers bothered by this can set their own reverse DNS, although until we migrate all customers to @2a0a:1100::/29@ the reverse part (IPv6 address to name) will also remain insecure.

2023-04-10 02:56 - admin
Fix typo in task description

2023-04-11 13:33 - admin
Now DNSSEC-enabled:

* @bitfolk.co.uk@
* @87.119.85.in-addr.arpa@

2023-04-11 14:19 - admin
The remainder of the IPv4 reverse zones have now been DNSSEC-enabled.

I've just realised that there will have to be a way for customers to supply DS records for their delegated reverse zones. As the reverse zones are programmatically generated we can't just edit in DS records manually.

I'll expand this task to include being able to store this info and put it into the generated reverse zones. Then DS records can be supplied by support ticket. There'll be another task for the panel to allow input of DS records.

2023-04-12 21:54 - admin
The remaining zones have now been DNSSEC-signed.

SSHFP records have been added for things customers are expected to SSH to.

For this task it just remains to modify the customer database and DNS reverse zone generation to allow DS records to be added.