Bind DNS

Common Issues

Issue: server booted with a time in the future, and bind / named downloaded the trust information with a future timestamp

Often you'll see this in the logs:
validating ./DNSKEY: unable to find a DNSKEY which verifies the DNSKEY RRset and also matches a trusted key for '.'
managed-keys-zone: No valid trust anchors for '.'

Solution:

1) shut down named
2) delete /var/named/dynamic/managed-keys.bind.jnl and create file just containing:
;BIND LOG V9
8
3) ensure new file is owned by the named user.
4) start up named

You'll see something like this in the logs:
Apr 28 12:49:00 XXXXXX named[4093]: managed-keys-zone: journal rollforward failed: no more
Apr 28 12:49:00 XXXXXX named[4093]: managed-keys-zone: unable to load from '/var/named/dynamic/managed-keys.bind.jnl'; renaming file to '/var/named/dynamic/jn-xMvuHJmM' for failure analysis and retransferring.

And then your dnssec should start working again...

There's probably better ways to trigger the resolution, but the above seems to work....

Revision #1
Created 28 April 2022 12:44:50 by Stephen D
Updated 10 August 2023 06:24:43 by Stephen D