DuckCorp Infrastructure - Bug #720

Bind9 KASP Migration Problems

2021-02-20 09:51 - Marc Dequènes

Status:	New	**Start date:**	2018-05-07
Priority:	Low	**Due date:**	
Assignee:	Marc Dequènes	**% Done:**	0%
Category:	Service :: DNS	**Estimated time:**	0:00 hour
Target version:			
Patch Available:		**Entity:**	DuckCorp
Confirmed:	No	**Security:**	
Branch:		**Help Needed:**	

Description

This is the migration from the preliminary DNSSEC implementation called `dnssec-keymgr` to the integrated KASP scheduler with `dnssec-policy`.

We encountered a few bugs or limitations (the later being expected improvements from the old system that are still dearly lacking):

- old apparmor profile in the way
- does not properly import keys and states from old system
- rndc dnssec -rollover takes a **very** long time to be taken into account; not good for emergency rollover
- dnssec-policy checkds takes a long time to be taken into account
- implement check if the DS record has been published

Tickets to keep track of:

- NSEC3 RRs not maintained properly; we are not affected but that's bad
- new KSK submission hook; could be useful until registrars properly support CDS/CDNSKEY

Features we really need:

- ~~publishing of CDS/CDNSKEY~~ handled by KASP
- ~~automate using published CDS/CDNSKEY in parent zones we manage~~ created support with a crontab in the bind9 role
- notify Bind when the DS is published/withdrawn: I guess we would need to make a script since it's probably gonna take some time before it's added upstream
- automate using published CDS/CDNSKEY in parent zones we do not manage: currently Gandi, either with the old XMLRPC API or maybe change registrar
- rewrite the rollover notification script for KASP (needed until all is automated and to check all is fine)

Subtasks:

Enhancement # 623: Use Gandi API to automate DNSSEC KSK rollover	**New**

History

#1 - 2021-02-20 11:40 - Marc Dequènes

- Description updated