000000Timeline and impact assessment of reverse DNS incident dd. 2012/06/13 - 2012/06/15

Time (UTC)	Events	Impact assessment
Wed 13/6/2012		
13:30	We disscover that several zonefiles are missing from the DNS provisioning system [The cause of this is still unknown and under investigation. Circumstatial is a routine bind update in the morning.]	*No impact on DNS reverse operations, but zone updates broken for delegations in parent zones: 0.4.1.0.0.2.ip6.arpa, 185.in-addr.arpa, 4.1.1.0.0.2.ip6.arpa, 5.1.0.0.2.ip6.arpa, 6.1.1.0.0.2.ip6.arpa, 7.0.1.0.0.2.ip6.arpa, 7.1.1.0.0.2.ip6.arpa, 7.4.1.0.0.2.ip6.arpa, 8.0.1.0.0.2.ip6.arpa, a.0.1.0.0.2.ip6.arpa, a.1.1.0.0.2.ip6.arpa, a.4.1.0.0.2.ip6.arpa, b.0.1.0.0.2.ip6.arpa, b.1.1.0.0.2.ip6.arpa, b.4.1.0.0.2.ip6.arpa (a total of 425 delegations, 185/8 is in de-bogonising: no operational impact)*
13:45	Decision to reload zonefiles from backup storage	
14:00	Discovery that backups are not available	
14:15	Decision to cold start the provisioning system. Because the state of the remaining zone files available was unclear, we decide to rebuild all zone files from scratch.	
15:00	Start DNS provisioning system from scratch (empty zonefiles). **By mistake we do not disable transfers to the authorittive servers.**	***Empty zones for entire reverse tree start propagating*** *Impact on whole of reverse DNS tree, limited initially by caching*
16:00	Reports of reverse tree breakage start to come in	
16:00 … 20:00	Investigation of problems and considering possible workarounds for slow provisioning system cold start.	
20:00	Found incidental backup of zone files with state of 13/6/2012 13:30 UTC	
20:15	Stopped DNS provisioning system. Reloaded DNS provisioning system with data from backup files. ERX related zones are missing from these backups, as are the above mentioned ip6.arpa delegations.	missing: 0.4.1.0.0.2.ip6.arpa, 185.in-addr.arpa, 4.1.1.0.0.2.ip6.arpa, 5.1.0.0.2.ip6.arpa, 6.1.1.0.0.2.ip6.arpa, 7.0.1.0.0.2.ip6.arpa, 7.1.1.0.0.2.ip6.arpa, 7.4.1.0.0.2.ip6.arpa, 8.0.1.0.0.2.ip6.arpa, a.0.1.0.0.2.ip6.arpa, a.1.1.0.0.2.ip6.arpa, a.4.1.0.0.2.ip6.arpa, b.0.1.0.0.2.ip6.arpa, b.1.1.0.0.2.ip6.arpa, b.4.1.0.0.2.ip6.arpa (together containing a total of 425 delegations)
	Authoritative servers reloading. *However, due to a race condition in the provisioning system causes the zone serial numbers for two zones to be incorrectly updated. Therefore two large zones (212.in-addr.arpa and 213.in-addr.arpa) are propagating in an incomplete form. This causes severe breakage for these zones.* In total approx. 6% of the reverse delegations are affected during this period	***Restored zone files start propagating for all but the below mentioned parent zones (state of 13/6/2012 13:30UTC).*** ***Due to negative caching, impact on restored zones may have prolonged.*** Details of impacted zones on next page.
		<u>Affected 6.1% of total reverse DNS delegations</u> Parent zones 212.in-addr.arpa, and 213.in-addr.arpa are distributed incompletely. Affected: 43% in delegations in 212.in-addr.arpa, 54% of delegations in 213.in-addr.arpa. In total 33,996 delegations affected in these parent zones. <u>ERX zones.</u> ERX import zones: 4426 delegations accross 22 zones absent during this period. ERX exports: updates delayed Above mentioned missing zones in ip6.arpa (475 delegations total) are still lacking during this period. <u>RFC2317 delegations:</u> a total of 31 RFC2317 delegations are lacking the associated CNAME records at this t
20:30	Restarted DNS provisioning system, starting with state of 13.30 UTC. The DNS provisioning system is still running at an unexpectedly low insertion rate.	*At this time we believed the remaining impact to be limited to a small number of ERX imported zones, and a limited number of ip6.arpa zones. The problems with 212.- and 213.in-addr.arpa went unnoticed until early morning of Thursday 14/6*
Thu 14/6/2012		

000000Timeline and impact assessment of reverse DNS incident dd. 2012/06/13 - 2012/06/15

	7:00	First reports received about remaining breakage	
	7:00-10:00	Investigations of reported remaining issues	
	10:45	We discover the that 212./231.in-addr.arpa are incomplete due to the above mentioned race condition. After updating serial numbers, zones 212./213.in-addr.arpa start propagating properly again.	Zones 212.in-addr.arpa and 213.in-addr.arpa, complete and up to date to the then-current state, start propagating again. ERX import zones (4426 delegations), ip6.arpa (475 delegations) and rfc2317 zones (31 delegations) still not restored
	16:00	Based on RIPE DB dump of 14/6/2012 0.00h, all regular zones are restored, incl. ip6.arpa zones	
	16:00-16:30	Processing of updates for period after 00:00 14/6/2012	
	16:30	All updates processed for all zones, with the exception of ERX zones	All regular zones restored and current. ERX import zones (4426 delegations) and rfc2317 zones (31 delegations) still not restored
	19:30	Restart processing of ERX delegations (much slower than anticipated)	
	20:00	Majority of ERX zones handled	ERX import zones (2 delegations) and rfc2317 zones
Fri 15/6/2012			
	7:30	All regular zones restored including last remaining 2 ERX zones	All zones, incl. ERX imports, fully functional, with the exception of 31 rfc2317 delegations that were not discovered to be missing their CNAME records.
Mon 18/6/2012			
	11:00	Discovered error with 31 delegations lacking rfc2317 CNAME records	
	13:45	Restored remaining rfc2317 delegations	