APNIC 50

AS0 Implementation report to Routing SIG

George Michaelson

Product Manager: Registry

ggm@apnic.net

ONLINE
8 – 10 September 2020

Prop132 “AS0 for unallocated and unassigned resources”

- We have implemented Prop132
  - APNIC now publishes and maintains an AS0 “ROA” for all un-delegated resources in our registry
  - These are the IPv4 and IPv6 resources listed as “available” or “reserved” in our daily published delegated statistics files
  - The AS0 ROA is defined in RFC6483 as “a disavowal of routing origination”

```
A ROA with a subject of AS 0 (AS 0 ROA) is an attestation by the holder of a prefix that the prefix described in the ROA,
and any more specific prefix, should not be used in a routing context.
```

- This is now a fully deployed service
  - With systems monitoring 24/7 integrated into our operations platforms
  - Deployed in the cloud for the publication point (data repository)
  - At this stage, deployed in a stand-alone Trust Anchor Locator (TAL)

Implementation report:testbed

- An initial Testbed was deployed for APRICOT/APNIC49
  - Based on the “Krill” system from NLNet Labs
  - Operating on the delegated files as a daily view of registry
  - Using a temporary, soft-keyed Trust Anchor (TA) in a TAL file
  - Publishing the repository inside APNIC VM on the test network
  - This service was used by a small number of people (<10)
    - We were able to confirm issues with discrete ROA per prefix
    - We understood our operational needs to manage the ROA as resources are issued by APNIC

Implementation report:production

- We have now deployed this service into production
  - Still based on delegated files, but with a delay to prevent accidental exclusions if delegated files are out of synchronization with registry
  - Live updates to Registry (delegations) are applied within 5 minutes to both main RPKI and AS0 RPKI state
    - Delegations are removed from the AS0 ROA within 5 minutes of resources being assigned or allocated from the free pool.
  - We are collecting statistics on use, and the scale of BGP effects which will be presented to the Routing Security SIG

Implementation report: Production

- In-house deployment on VM
  - Tightly coupled to registry events, so max 5min lag from delegations
    - Prevents AS0 denying validly delegated resources as quickly as possible
    - General RPKI also now re-synchronized more rapidly
  - HSM backed trust anchor keypair
    - Same level of assurance as main line TA
- Cloud deployment of repository (GCP)
  - Both rsync and RRDP supported
  - Will distribute in GCP when 2nd and further nodes commissioned
- Fully managed and monitored 24/7 by APNIC operations

Where to from here?

- Further discussion of this service is now conducted in the APNIC Routing Security SIG
  - Statistics on use,
  - Size of ROA,
  - Operational experiences,
  - Future directions.

Some initial statistics

- Initial outcome: 69 routes marked bad in DFZ from ~65k prefixes
  - (reported by Job Snijders during deployment testing)
- Usage: Released week of 1st September
  - 24 ASN now fetching from the service
  - More stats on usage will follow once we see traffic

ASN using the AS0 TAL

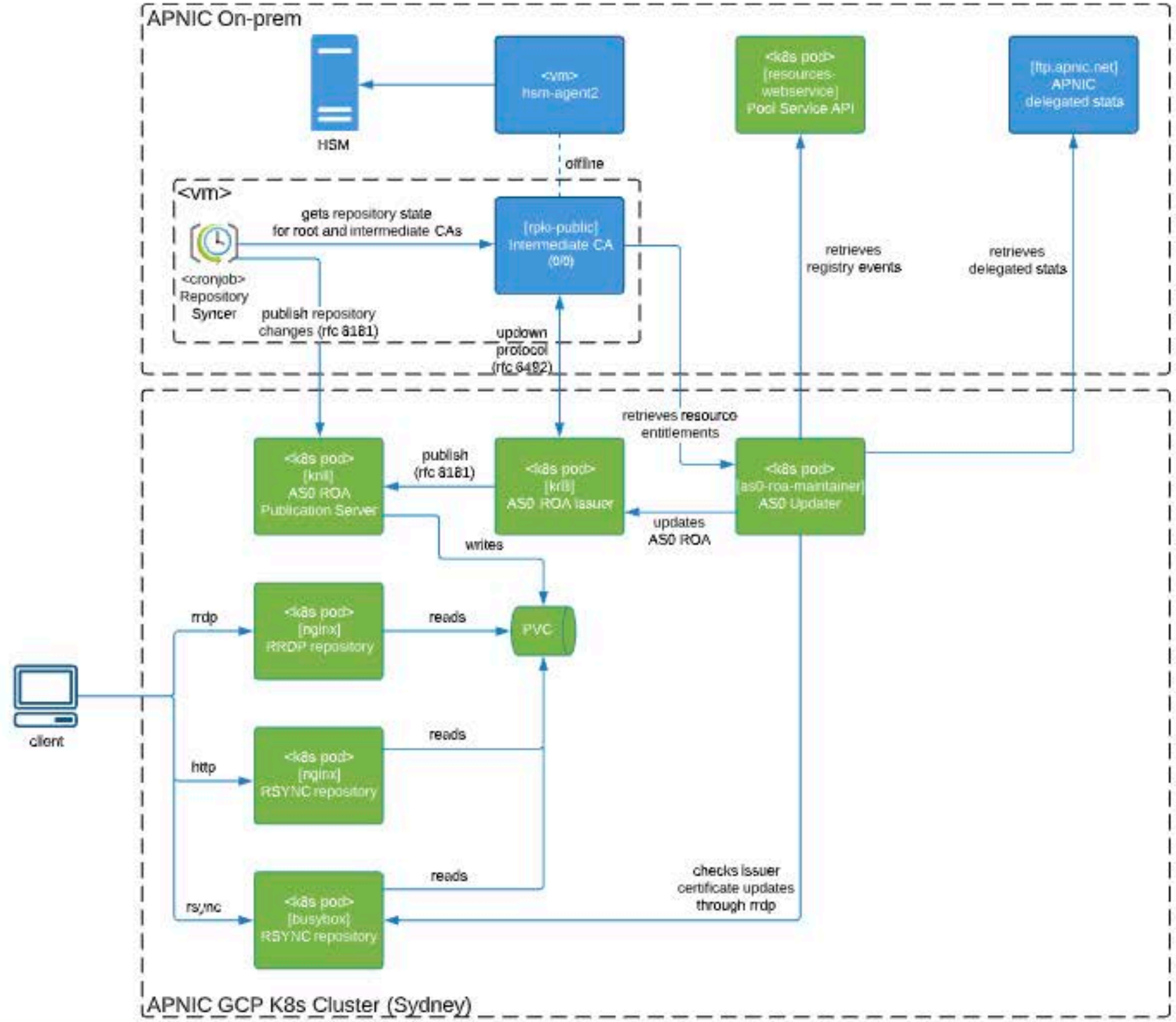
ASN	Name	Economy
9443	VOCUS-RETAIL-AU Vocus Retail	AU
38345	ZDNS Internet Domain Name System Beijing	CN
4837	CHINA169-BACKBONE CHINA UNICOM	CN
4812	CHINANET-SH-AP China Telecom (Group)	CN
4847	CNIX-AP China Networks Inter-Exchange	CN
17621	CNCGROUP-SH China Unicom Shanghai network	CN
23910	CNGI-CERNET2-AS-AP China Next Generation Internet	CN
4134	CHINANET-BACKBONE No.31	CN
1136	KPN KPN National	EU

ASN	Name	Economy
3265	XS4ALL-NL Amsterdam	NL
8587	INFRACOM-AS	NL
15169	GOOGLE	US
20473	AS-CHOOPA	US
395747	CLOUDFLARENET-SFO05	US
8075	MICROSOFT-CORP-MSN-AS-BLOCK	US
14618	AMAZON-AES	US
14061	DIGITALOCEAN-ASN	US
132892	CLOUDFLARE Cloudflare	US

Some initial statistics: Size of ROA

- AS0 ROA is 1,017,637 bytes long (at present)
- 66,109 IPv4 and IPv6 prefixes encoded in one Object
  - 1,522 IPv4
  - 64,588 IPv6
  - The IPv6 count is a function of “sparse” allocation

Implementation architecture



- On-premises and GKE Sydney deployments
- HSM backed TAL, follows main line RPKI
- Re-use of existing RPKI systems code
  - Actual signing carried out by Krill (NLNet)

- Repository structure served from GKE
  - Capable of being distributed in future
  - Using CloudFlare front-end

APNIC 50

ONLINE

8 – 10 September 2020

#apnic50