DigitalOcean

Being a better Netizen: MANRS @ DO

Tim Raphael

*Senior Network Engineer,
Internet Edge and Backbone*

AusNOG 2021
April, 2022

Contents

DO ♥ Developers

MISSION->

Simplify cloud computing so developers and businesses can spend more time creating software that changes the world

digitalocean.com

We offer the world’s simplest & most powerful IaaS experience

CORE PLATFORM (Compute, Network, Storage, Day 2 Operations)

Starter Droplets

Custom Images

DNS

Block Storage

Monitoring

Performance/Storage Optimized Droplets

OS Images

Floating IPs

Object Storage

Premium AMD/Intel CPU Droplets

Backups/Snapshots

SECURITY

Private Networking

Cloud Firewalls

2FA

With emerging PaaS that do not require “DevOps” experience

APPLICATION SERVICES

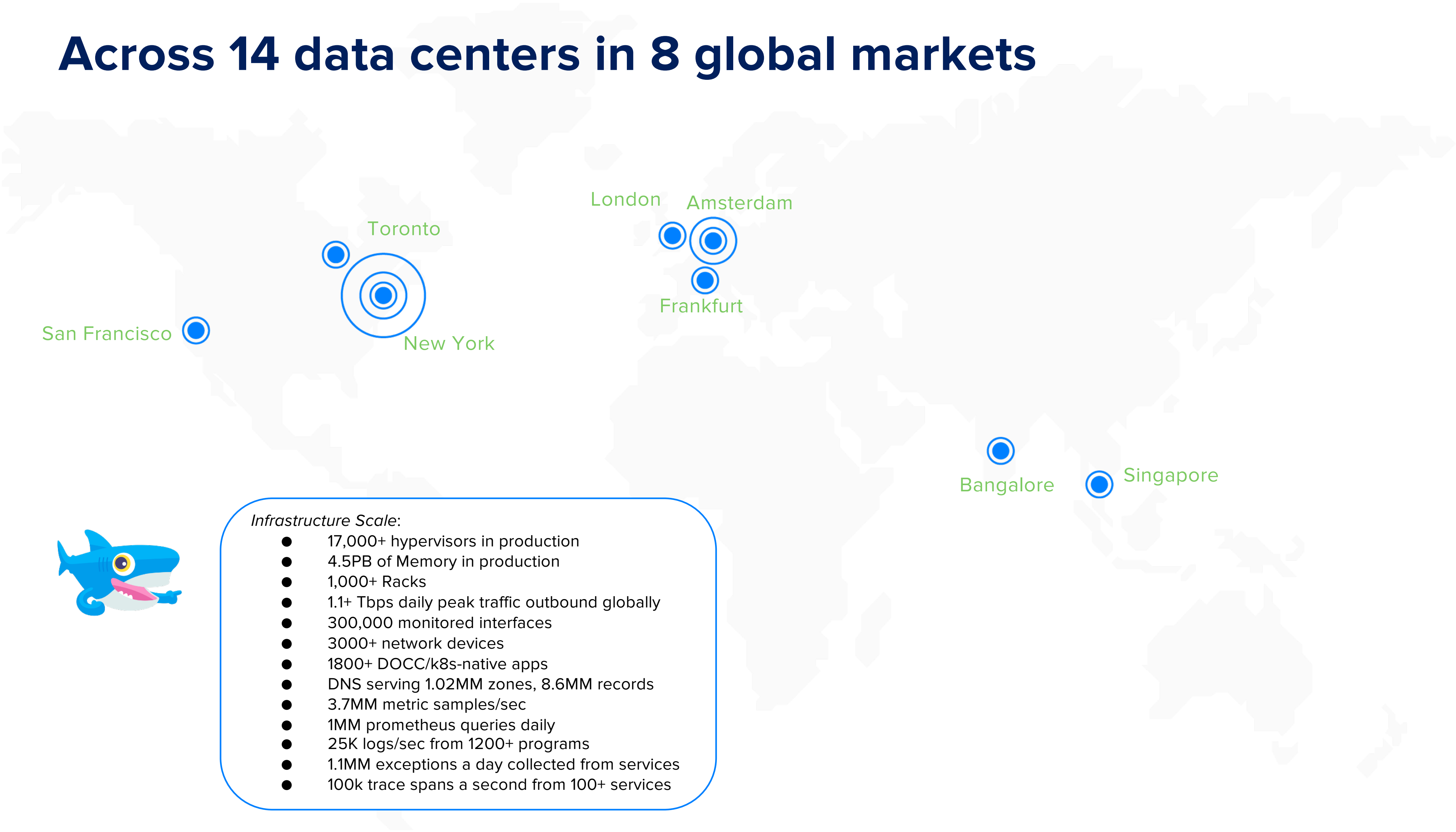
Managed Kubernetes

Managed Load Balancers

Managed Databases

App Platform

Across 14 data centers in 8 global markets



Infrastructure Scale:

- 17,000+ hypervisors in production
- 4.5PB of Memory in production
- 1,000+ Racks
- 1.1+ Tbps daily peak traffic outbound globally
- 300,000 monitored interfaces
- 3000+ network devices
- 1800+ DOCC/k8s-native apps
- DNS serving 1.02MM zones, 8.6MM records
- 3.7MM metric samples/sec
- 1MM prometheus queries daily
- 25K logs/sec from 1200+ programs
- 1.1MM exceptions a day collected from services
- 100k trace spans a second from 100+ services

Why become MANRS Compliant?

Our community is bigger than us.

- A Core Value at DigitalOcean

MANRS Cloud & CDN Program

Action 1:

Prevent propagation of incorrect routing information.

"… Whenever feasible, participants should check that the announcements originate from legitimate holders."

Action 2:

Prevent traffic with illegitimate source IP addresses

"Implement anti-spoofing controls to prevent packets with illegitimate source IP address from leaving the network."

Action 3:

Facilitate global operational communication and coordination

"Maintain globally accessible up-to-date contact information in PeeringDB and relevant RIR databases."

Ref: https://www.manrs.org/cdn-cloud-providers/

MANRS Cloud & CDN Program

Action 4:

Facilitate validation of routing information on a global scale

"… routing information needs to be properly registered in public routing repositories…The two main types of repositories are IRRs and RPKI."

Action 5:

Encourage MANRS adoption

"A publicly available policy, a peering form or an email template with a recommendation to implement MANRS."

Ref: https://www.manrs.org/cdn-cloud-providers/

Action 1: Filtering

Prevent propagation of incorrect routing information.

Action 1: Filtering

Challenges

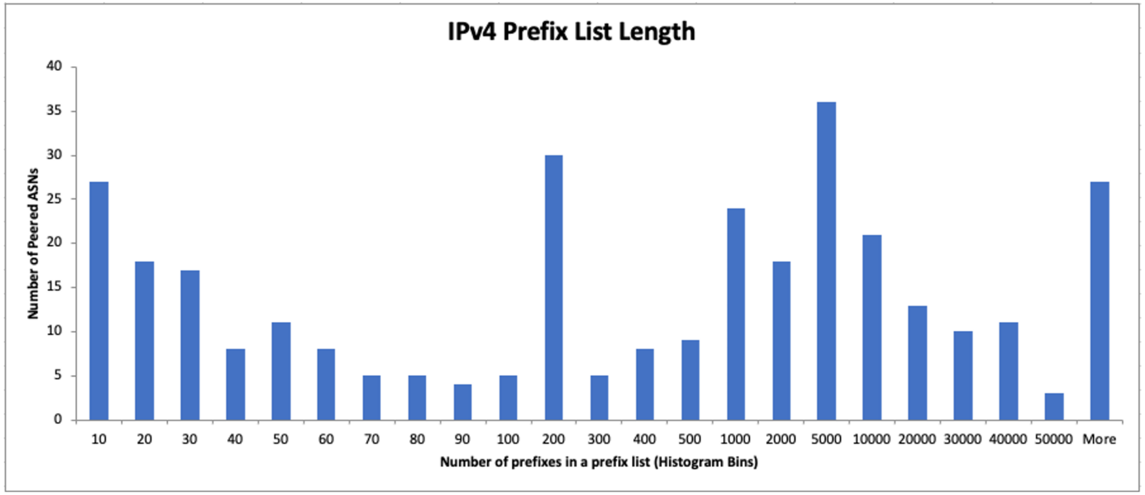
DigitalOcean runs a medium-large global network that peers with hundreds of ASNs on many of the biggest peering fabrics in the world.

Analysis and automation is required to find a workable solution that provides appropriate knobs to control for our scale.

- High cardinality of peering sessions
- Varying hardware capacity
- Automation required

Action 1: Filtering

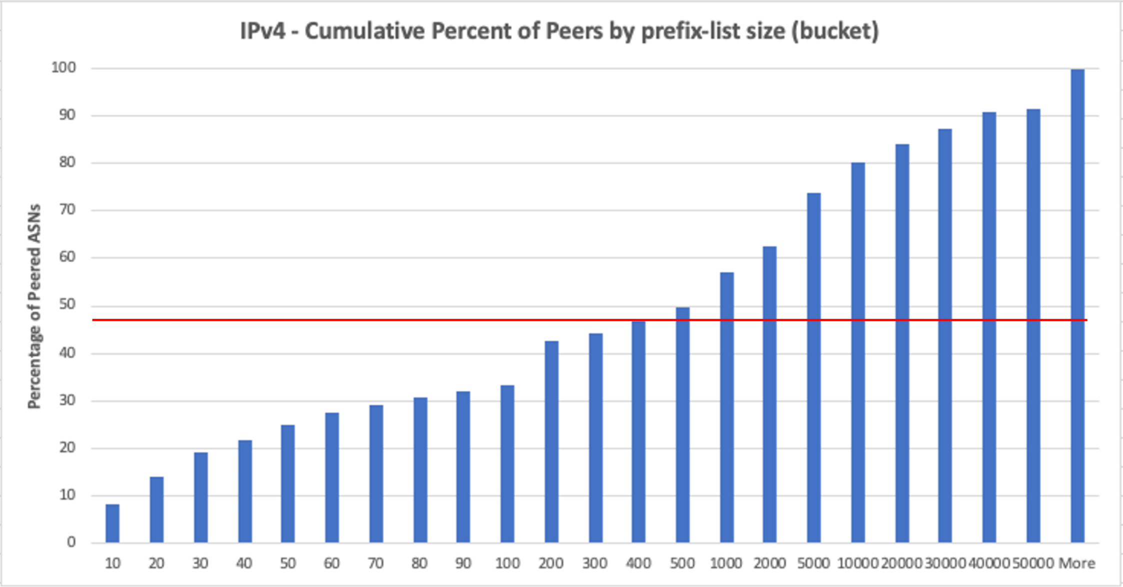
Analysis



- Prefix list length determined by IRR object.
- Buckets of prefix-list length.
- Many millions of LoC for dense peering routers.

Action 1: Filtering

Analysis



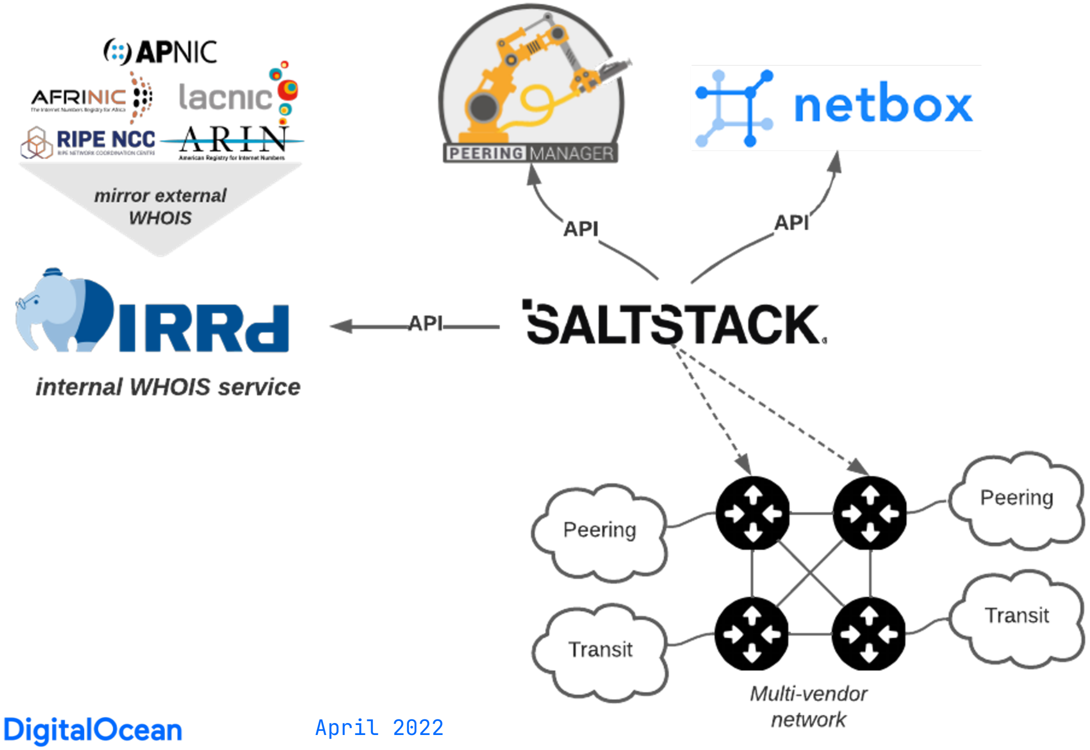
100% coverage would result in ~6.5M LoC on some routers.

2M LoC ~ 95 sec apply times.

Picked a sensible point to maximise coverage within limitations.

Action 1: Filtering

The heavy lift...



- IRRd, Netbox and Peering Manager for Source-of-Truth
- SaltStack to build prefix-lists and templates.
- Continual, automatic updates pushed to the network every 6 hours.

Action 1: Filtering

The outcome…

```
neighbor 192.0.2.1 {
  description "Example Network Name";
  import [ SCRUB-IMPORT-IPv4 IX-IMPORT ABCIX-BILAT-IMPORT-IPv4 AS65535-IX-IMPORT-IPv4 ];
  family inet {
    unicast {
      prefix-limit {
        maximum 600;
        teardown {
          idle-timeout 15;
        }
      }
    }
  }
  export ABC-PEER-EXPORT;
  peer-as 65535;
}
```

- Policy per peer
- Chained with other policies, optional completion early.
- Easy to read and understand.

Action 1: Filtering

The outcome…

```
traphael@sg-sin01-edge1> show configuration policy-options policy-statement
                                                               AS65535-IX-IMPORT-IPv4

term RPKI-VALID {
  from {
    protocol bgp;
    community DO-RPKI-VALID;
  }
  then accept;
}
term AS65535 {
  from {
    protocol bgp;
    prefix-list AS65535v4;  ←-------------------------
  }
  then {
    community add DO-IRR-VALID;
    accept;
  }
}
term DEFAULT {
  then {
    community add DO-IRR-INVALID;
    reject;
  }
}
```

- Filter on RPKI first
- Filter by IRR second
- Tag with useful communities as you go.

A quick shout out:

Mircea Ulinic

- Network Development Lead @ DigitalOcean
- Core maintainer for NAPALM
- Contributor to SaltStack (2017 Contributor of the year)

Action 2:
Anti-Spoofing

Prevent traffic with illegitimate source IP addresses

Action 2: Anti-Spoofing

We already prevent spoofing!

Given DigitalOcean runs such a huge number of workloads, bad actors and spoofed traffic isn’t a new challenge. We already have several layers of protection to ensure that all traffic originating from DO is from legitimate sources.

- Control from the hypervisor.
- Internal detection tooling.
- uRPF deployed on the edge of the network.

Action 2: Anti-Spoofing

To be sure?

It’s best practice to ensure that our mechanisms to prevent spoofing are actually working. When they aren’t, we want to have a clear signal when they no longer are.

The CAIDA Spoofer project to the rescue! We run spoofer nodes in each of our DCs that attempt to send spoofed traffic to the public CAIDA endpoint. A prometheus exporter regularly queries the public CAIDA API and will alert us if spoofed traffic is received.

- CAIDA Spoofer Project
- Prometheus Exporter
- Sensible alerting rules with a playbook

Ref: https://www.caida.org/projects/spoofer/

Action 2: Anti-Spoofing

To be sure?

```
alerts:
 -
   alert: CAIDA Session Received
   expr: caida_spoofer_session == 1
   labels:
     service: CAIDA
     severity: warning
     instance: "caida-spoofer::{{$labels.session}}"
     team: infra-network
     environment: IEB
   annotations:
     description: "CAIDA Spoofer session received"
     URL: <a
href="https://spoofer.caida.org/report.php?sessionid={{$labels.session}}"
target="_blank">Session {{$labels.session}} Report</a>
     playbook: <a href="https://doplaybooksite.tld/CAIDA+Spoofer+Servers"
target="_blank">CAIDA Spoofers</a>
```

- CAIDA Spoofer Project
- Prometheus Exporter
- Sensible alerting rules with a playbook

Ref: https://www.caida.org/projects/spoofer/

Action 3: Coordination

Facilitate global operational communication and coordination

Action 3: Coordination

How to find us…

We keep our WHOIS data up-to-date as we on-board new IP space through a regularly used playbook. This ensures all the same data is present on all our prefixes:

```
➜  ~ whois `host dodroplet.com | awk '{print $4}'` | grep Email
OrgTechEmail:  noc@digitalocean.com
OrgNOCEmail:  noc@digitalocean.com
OrgAbuseEmail:  abuse@digitalocean.com
```

Consistent WHOIS data through defined process

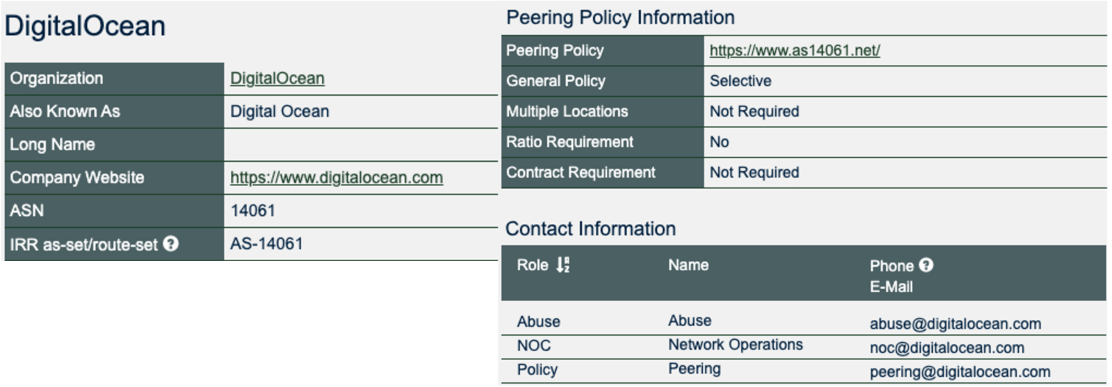
Accurate PeeringDB record

Monitored mailboxes

Action 3: Coordination

How to find us...

Because we rely on our peering partners to keep their PeeringDB record up-to-date for automation reasons, we should set the best example and do so as well.



DigitalOcean

Organization	DigitalOcean
Also Known As	Digital Ocean
Long Name	
Company Website	https://www.digitalocean.com
ASN	14061
IRR as-set/route-set ?	AS-14061

Peering Policy Information

Peering Policy	https://www.as14061.net/
General Policy	Selective
Multiple Locations	Not Required
Ratio Requirement	No
Contract Requirement	Not Required

Contact Information

Role	Name	Phone ? E-Mail
Abuse	Abuse	abuse@digitalocean.com
NOC	Network Operations	noc@digitalocean.com
Policy	Peering	peering@digitalocean.com

Consistent WHOIS data through defined process

Accurate PeeringDB record

Monitored mailboxes

Action 4:
Global Validation

Facilitate validation of routing information on a global scale

Action 4: Global Validation

We publish our routing data!

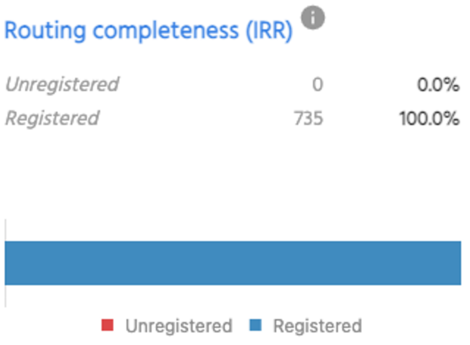
Given we allocate prefixes on a per-region basis, we need to ensure that the correct prefix lengths are kept up-to-date in our IRR objects. We use a scheduled “cron” job deployed to our internal application stack to ensure our IRR objects are accurate.

- Automated IRR updates.
- RPKI ROA coverage.
- Automated alerting for non-compliance using Netbox reports.

Action 4: Global Validation

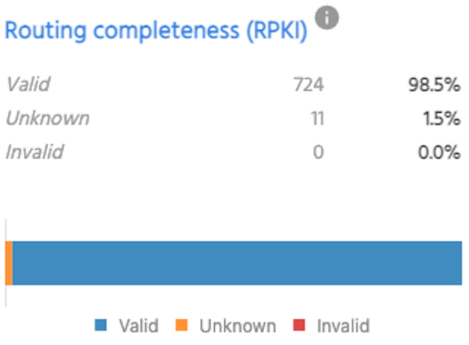
We publish our routing data!

We use covering ROAs with max-prefix-length populated to ensure we have valid ROAs for the prefixes we intend to advertise.



Routing completeness (IRR)

Unregistered	0	0.0%
Registered	735	100.0%



Routing completeness (RPKI)

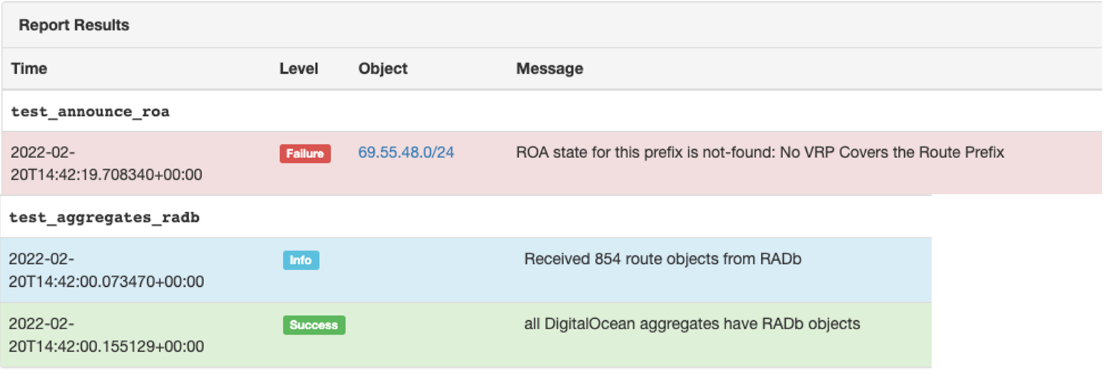
Valid	724	98.5%
Unknown	11	1.5%
Invalid	0	0.0%

- Automated IRR updates.
- RPKI ROA coverage.
- Automated alerting for non-compliance using Netbox reports.

Action 4: Global Validation

We publish our routing data!

Netbox reports are used to check for compliance and give us strong alerting signals when things aren't correct.



Report Results

Time	Level	Object	Message
test_announce_roa			
2022-02-20T14:42:19.708340+00:00	Failure	69.55.48.0/24	ROA state for this prefix is not-found: No VRP Covers the Route Prefix
test_aggregates_radb			
2022-02-20T14:42:00.073470+00:00	Info		Received 854 route objects from RADb
2022-02-20T14:42:00.155129+00:00	Success		all DigitalOcean aggregates have RADb objects

Automated IRR updates.

RPKI ROA coverage.

Automated alerting for non-compliance using Netbox reports.

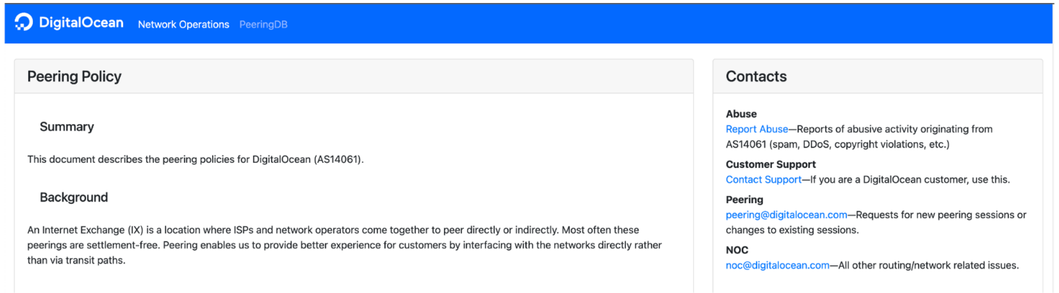
Action 5:
Encourage Adoption

Action 5: Encourage Adoption

Simple as…

"…Peers are encouraged to implement Mutually Agreed Norms for Routing Security (MANRS) - https://www.manrs.org. "

https://as14061.net/



Peering Policy

Summary

This document describes the peering policies for DigitalOcean (AS14061).

Background

An Internet Exchange (IX) is a location where ISPs and network operators come together to peer directly or indirectly. Most often these peerings are settlement-free. Peering enables us to provide better experience for customers by interfacing with the networks directly rather than via transit paths.

Contacts

Abuse
Report Abuse—Reports of abusive activity originating from AS14061 (spam, DDoS, copyright violations, etc.)

Customer Support
Contact Support—If you are a DigitalOcean customer, use this.

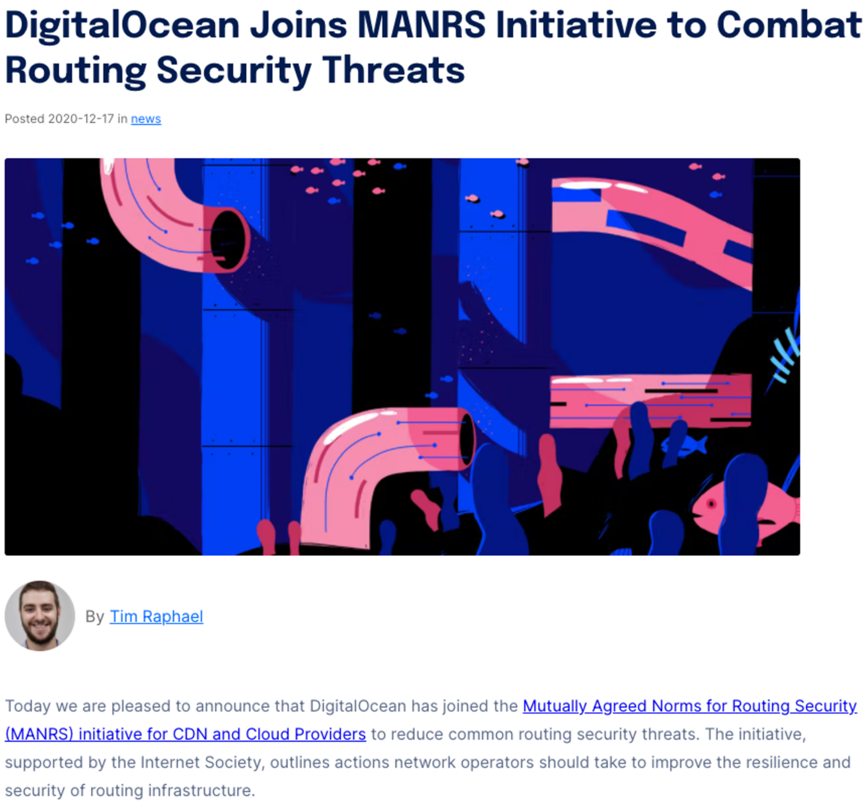
Peering
peering@digitalocean.com—Requests for new peering sessions or changes to existing sessions.

NOC
noc@digitalocean.com—All other routing/network related issues.

- Updated our peering policy.
- Encouraged adoption of MANRS.
- Provided relevant links.

Compliance

December 2020



DigitalOcean Joins MANRS Initiative to Combat Routing Security Threats

Posted 2020-12-17 in news

By Tim Raphael

Today we are pleased to announce that DigitalOcean has joined the Mutually Agreed Norms for Routing Security (MANRS) initiative for CDN and Cloud Providers to reduce common routing security threats. The initiative, supported by the Internet Society, outlines actions network operators should take to improve the resilience and security of routing infrastructure.

DigitalOcean April 2022

Compliance

What next?

Action 6: Monitoring and debugging

Visibility is everything…

To help our peers we intend to launch an externally-facing looking glass that can help debug routing issues. To fit in with our other MANRS obligations we should ensure that RPKI status, route filtering status and various other aspects of routing policy are made clear with this tool.

- Public Looking glass
- Route filtering state
- Route distribution policy

Improvement never ends…

While most of our processes are automated, there is always those few that aren't - we're continually aiming to improve automation coverage where it makes sense.

With the onset of a global network overhaul, new equipment gives us new capability to improve our filtering coverage.

Lastly, alerting and subsequent actions can always be improved as we experience new challenges and failure modes to learn from.

- Increase automation coverage
- Increase prefix-list coverage
- Improve alerting

Thank you

DigitalOcean

DigitalOcean