Kea 2.0
A modern DHCP

Tomek Mrugalski,
Director of DHCP Engineering, ISC
2022-May-6, DKNOG’12, Copenhagen
Tomek Mrugalski

- MSc (2003), PhD (2010), both about DHCPv6
- Started Dibbler in 2003 (complete DHCPv6 solution)
- 7 years at Intel
- IETF (since 2009)
  - DHC WG co-chair at IETF (till 2020)
  - 13 RFCs published
  - DHCPv6bis (RFC8415) as primary author
- ISC (since 2011)
  - First engineer working on Kea
  - Currently Director of DHCP engineering
ISC DHCP Legacy

- Provided in many major operating systems
- Development started in 1995
- widely used, but not aging well
- ISC DHCP “development” is in maintenance mode only
- Kea is a replacement for the ISC DHCP server
- 4.4.3 released in Mar 2022. Last release for client and relay.
- Upcoming 4.5.0 will be server only.
- If you are running this in your network today - consider it technical debt
Time to Migrate to Kea

- Run the migration assistant
- Fix up 20 - 30% this doesn’t cover
- Migrate leases if desired
  https://www.isc.org/presentations/
- NANOG’76 talk
  https://pc.nanog.org/static/published/meetings//NANOG76/daily/day_2.html#talk_1998
Kea Differences from ISC DHCP

- Extensive REST Management API
- Separate ‘backends’ leveraging popular open source DBs
  - Leases
  - Reservations
  - Server configurations
- Extensible with optional hooks libraries, including many from ISC
- Open source (MPL2), with commercial add-ons
- Available as source, or as ISC packages for popular OSes
- Both stable and development branches available
Kea’s REST API

- Allows on-line reconfiguration of DHCPv4, DHCPv6 and DDNS servers without restarting
- Kea configuration AND the REST api, use JSON syntax (comments allowed)
- API commands are fully documented in


184 commands available and growing
API Basics

1. Send `list-commands` command:

```
# kea-shell --host ::1 --port 8080 --service dhcp6 list-commands
^D
```
API Basics

2. Get list of currently supported commands in return:

```json
{
    "command": "list-commands",
    "service": [ "dhcp6" ]
}
```
Why use database ‘backends’?

- SQL data can be modified any time
- All changes applied instantly (no restart)
- Adapt your provisioning systems to write directly to the database or
- Use the API (some of these require premium hooks libraries)
- More complicated deployment, more things to install and manage (the db)
- CSV, MySQL, PostgreSQL
  - Cassandra deprecated, being removed in upcoming 2.2
Available Backends

- **DHCPv4, DHCPv6 server**
  - Leases (addresses, prefixes)
  - Host reservations (per host details)
  - Options
  - Pools
  - Subnets
  - Shared networks
  - Option definitions
  - Global parameters

- **MySQL Postgres (2.1)**
  - Lease backend
  - Hosts backend
  - Configuration backend

Changing

- Rarely
- Often
Recent changes in Kea 2.0

1. Significant performance boost with multi-threading
2. Addition of TLS security for connections
   ○ Kea - db backends
   ○ Kea - stork
   ○ Kea - api clients
3. New features
   ○ Cache threshold
   ○ Script hook
4. Stork graphical dashboard
Multi-threading (Kea 1.8)

ctrl-agent1
  +-----------------+  ctrl-agent2
  |                 |  HTTP
  +-----------------+  JSON/Unix
  |  dhcp1           |  JSON/Unix
  +-----------------+  HTTP
  |                 |  Multi-threaded
  +-----------------+  Sequential
  |  dhcp2           |  DHCP
  +-----------------+
High Availability with Multi-threading (Kea 2.0)
Multi-threading performance boost (Kea 2.0)

For A LOT more details, see https://reports.kea.isc.org
API (Kea 2.0)
- TLS 1.3
- 3 modes:
  - Disabled
  - Encryption (client verifies server)
  - Mutual (both sides verifies each other)

Secure database connection
- MySQL (Kea 2.1)
- PostgreSQL (Kea 2.0)

More security enhancements coming!

"Control-agent": {
  "http-host": "127.0.0.1",
  "http-port": 8000,

  // TLS trust anchor (Certificate Authority).
  "trust-anchor": "my-ca",

  // TLS server certificate file name.
  "cert-file": "my-cert",

  // TLS server private key file name.
  "key-file": "my-key",

  "cert-required": true
}
Cache Threshold (2.0)

- Problem: Buggy clients renewing early
- Each renewal:
  - Host reservation lookup
  - Lease lookup
  - Logging*
  - HA: partner update*
  - DNS Update*
- Solution: cache replies
- IPv4 and IPv6
Script Hook (Kea 2.0)

But I want to … <your secret voodoo here>

```bash
#!/bin/bash

lease4_renew () {
    ...
}

case "$1" in
    "lease4_renew")
        lease4_renew
        ;;
    *)
        unknown_handle "${@}"
        ;;
esac
```
Stork

Kea (and BIND9) Dashboard/GUI/IPAM
Stork Dashboard

One Stork server + one or more agents
- Collects data from Kea/BIND9 services
- Aggregates data
- Web interface
- Export to Prometheus/Grafana

- Server details: version, build, installed hooks, cpu, memory
- Fault monitoring: subnet utilization, HA failures, log viewer
- Statistics: DORAs, QPS, NAKs
- Config viewer: file locations, database backends, etc

- Monthly* releases
- Dashboard for now, configuration management coming up in 1.3
# Stork Dashboard - Subnet Utilization

<table>
<thead>
<tr>
<th>Subnet ID</th>
<th>Subnet</th>
<th>Addresses Total</th>
<th>Assigned</th>
<th>Used %</th>
<th>Pools</th>
<th>Shared Network</th>
<th>App Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.0.5.0/24</td>
<td>50</td>
<td>42</td>
<td>84 %</td>
<td>192.0.5.1-192.0.5.50</td>
<td>frog</td>
<td>kea-agent-kea</td>
</tr>
<tr>
<td>2</td>
<td>192.0.6.0/24</td>
<td>119</td>
<td>0</td>
<td>0 %</td>
<td>192.0.6.1-192.0.6.40, 192.0.6.61-192.0.6.90, 192.0.6.111-192.0.6.150</td>
<td>frog</td>
<td>kea-agent-kea</td>
</tr>
<tr>
<td>3</td>
<td>192.0.7.0/24</td>
<td>50</td>
<td>50</td>
<td>100 %</td>
<td>192.0.7.1-192.0.7.50</td>
<td>frog</td>
<td>kea-agent-kea</td>
</tr>
<tr>
<td>4</td>
<td>192.0.8.0/24</td>
<td>50</td>
<td>0</td>
<td>0 %</td>
<td>192.0.8.1-192.0.8.50</td>
<td>frog</td>
<td>kea-agent-kea</td>
</tr>
<tr>
<td>5</td>
<td>192.0.9.0/24</td>
<td>50</td>
<td>0</td>
<td>0 %</td>
<td>192.0.9.1-192.0.9.50</td>
<td>frog</td>
<td>kea-agent-kea</td>
</tr>
<tr>
<td>6</td>
<td>192.1.15.0/24</td>
<td>50</td>
<td>40</td>
<td>80 %</td>
<td>192.1.15.1-192.1.15.50</td>
<td>mouse</td>
<td>kea-agent-kea</td>
</tr>
<tr>
<td>7</td>
<td>192.1.16.0/24</td>
<td>150</td>
<td>39</td>
<td>26 %</td>
<td>192.1.16.1-192.1.16.150, 192.1.16.101-192.1.16.150</td>
<td>mouse</td>
<td>kea-agent-kea</td>
</tr>
<tr>
<td>9</td>
<td>192.0.2.0/24</td>
<td>200</td>
<td>1</td>
<td>0.5 %</td>
<td>192.0.2.1-192.0.2.50, 192.0.2.51-192.0.2.100, 192.0.2.101-192.0.2.200, 192.0.2.151-192.0.2.200</td>
<td>kea-agent-kea</td>
<td>kea-agent-kea-mary-subnets</td>
</tr>
<tr>
<td>10</td>
<td>1.0.0.0/16</td>
<td>65,531</td>
<td>0</td>
<td>0 %</td>
<td>1.0.0.4-1.0.255.254</td>
<td>kea-agent-kea-mary-subnets</td>
<td>kea-agent-kea-mary-subnets</td>
</tr>
</tbody>
</table>

1 of 694 pages < 1 2 3 4 5 > 10 Total: 6931 subnets
Stork GUI - Monitoring HA Status

- Groups HA pairs
- Displays roles
  - Primary/standby
  - Load balancing
- Heartbeat status
- HA States
- Scopes served
- Last outage

### High Availability

<table>
<thead>
<tr>
<th>Local server</th>
<th>Remote server Kea@127.0.0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status time:</td>
<td>2022-02-02 16:16:09</td>
</tr>
<tr>
<td>Status checked:</td>
<td>4 minutes ago</td>
</tr>
<tr>
<td>Role:</td>
<td>standby</td>
</tr>
<tr>
<td>Control status:</td>
<td>✗ offline</td>
</tr>
<tr>
<td>Heartbeat status:</td>
<td>✗ failed</td>
</tr>
<tr>
<td>State:</td>
<td>✗ unavailable</td>
</tr>
<tr>
<td>Scopes served:</td>
<td>none</td>
</tr>
<tr>
<td>Last in partner-down:</td>
<td>n/a</td>
</tr>
<tr>
<td>Unacked clients:</td>
<td>n/a</td>
</tr>
<tr>
<td>Connecting clients:</td>
<td>n/a</td>
</tr>
<tr>
<td>Analyzed packets:</td>
<td>n/a</td>
</tr>
</tbody>
</table>

### Notes

The remote server responds to the entire DHCP traffic.
Prometheus / Grafana export
Participation is Welcome!

https://gitlab.isc.org/isc-projects/kea/

https://gitlab.isc.org/isc-projects/stork/
Questions?

isc.org/kea
gitlab.isc.org/isc-projects/kea
gitlab.isc.org/isc-projects/stork