RIPE NCC
RIPE NETWORK COORDINATION CENTRE

# RIPE NCC and the Cloud

## Requirements and principles

Felipe Victolla Silveira | RIPE NCC Services WG (Interim Session) | 28 July 2021

# Recap: What This Session is About

- Strong reaction from the community on our usage of cloud technologies presented at RIPE 82
- We have taken a step back and restarted our engagement with the community (see RIPE Labs: ‘RIPE NCC and the Cloud: Let’s Start Again’)
  - Some work has been put on hold in the meantime (incl. RPKI and RIPE Database).
- Based on what we’ve heard so far, we have drafted a cloud strategy framework with principles and requirements
  - We published this on RIPE Labs after our first interim WG session.

# Cloud Principles

# Cloud Principles

1. **The RIPE NCC solicits input from the RIPE community for all services 1) that are critical to the operation of the Internet, or 2) directly affect the operations of our members or the RIPE community**
   - Requirements for these services are discussed in an open community process with guidance from the appropriate RIPE working group.
   - The RIPE NCC publishes implementation and deployment plans and seeks input from the RIPE community from an early stage until successful deployment.
   - The RIPE NCC regularly reports on the performance of its services and conducts reviews with the appropriate RIPE working group.

# Cloud Principles

2. **The RIPE NCC has full authority and responsibility for the design, deployment, and operation of its services**
3. **RIPE NCC must remain neutral**
   - The RIPE NCC has the responsibility to operate its services on a neutral and impartial basis for the benefit of all members, who are often in competition with one another.
4. **Integrity of RIPE NCC services must be maintained**
   - RIPE NCC is trusted by the Internet community to keep its services available in the face of geopolitical, economic and regulatory threats.
   - RIPE NCC is accountable to the community and members to protect the privacy, security and integrity of data and services it is entrusted with.

# Cloud Principles

## 5. Open standards should be used

- The RIPE NCC will prefer open standards and open technologies.
- Where open standards are not viable, the RIPE NCC will prefer industry standards over proprietary interfaces.

# Requirements

# Requirements

1. **Ensure resilience, accessibility, availability and low latency for our services**
   - Providing stable and effective services to Internet operators is a core function and we need to be able to do this well.
2. **Minimise vendor lock-in**
   - Avoid vendor-specific features and becoming deeply entangled in their environment. Preferring open standards over proprietary technologies can help to achieve this.
3. **Avoid dependence on a single cloud provider**
   - This is about relying on a specific third party to run mission critical Internet infrastructure.
   - A distributed architecture should be favoured, that avoids single points of failure and circular dependencies between the cloud infrastructure and RIPE NCC services.

# Requirements

4. **Engineers can innovate and improve the quality of our services**
   - Like any other company, the RIPE NCC has limited resources; there are only so many engineers and so many hours in the day. Using our resources to create the most value for members and the community is important.
5. **Comply with laws and regulations**
   - The RIPE NCC currently has a strict vetting process to ensure our compliance with different regulations, like European Union sanctions or GDPR. The idea is to have this vetting process published for the community.
6. **Ensure the security of our services**
   - This is another hard requirement for our services. Vetting process should also be published.

# Requirements

## 7. Prefer providers in our service region

- This is something that we support, with the caveat that we need to consider any trade-offs in terms of our other requirements — such as the need to provide the highest levels of security, resiliency and availability for our services.

# Draft Strategy Framework

# Draft Cloud Strategy Framework

- Proposed framework is based on the idea that different services have different requirements, based on their type and criticality
- Requirements defined in three levels:
  1. Strict
  2. Heightened
  3. Standard

# Draft Cloud Requirement Levels

| Requirement | Strict | Heightened | Standard |
|---|---|---|---|
| Resiliency, accessibility, availability and low latency of services | Uptime > 99,999% | Uptime > 99,9% | Uptime > 99% |
| Minimise vendor lock-in | Only use bare-metal or VMs or containers | Managed services can be used but only open standards | Managed services can be used but keep track of switching costs |
| Cloud provider independence | Fully distributed architecture<br>No downtime allowed | Stand-by backup infrastructure required | Ability to spin-up a new instance within 48 hours |
| Enable our engineers to improve product quality and innovate | Applies to all levels | | |
| Comply with laws and regulations | Applies to all levels<br>Legal vetting process should be published | | |
| Ensure security of our services | Checks according to level<br>Infosec vetting process should be fully published | | |
| Prefer providers in our service region | Applies to all levels | | |

# Service Type and Criticality

- Thinking of our services in terms of two categories:
  - **Global Internet Services:** required for the Internet to function properly (e.g. RPKI).
  - **Core RIPE NCC Services:** critical for the RIPE NCC, but will not have a noticeable impact on the wider Internet if offline for a short period (e.g. LIR Portal).
- Each service type can have different levels of criticality (i.e. importance of these services either to the operations of the Internet or the RIPE NCC).
- Three levels are identified:
  - High (e.g. RPKI): outages in these services have direct operational impact.
  - Medium (e.g. RIPE Database): outages have an impact within a few hours.
  - Low (e.g. RIR stats): more forgiving concerning outages.
- We will work with the community to define criticality

# Draft Requirement Level per Criticality

| | High | Medium | Low |
|---|---|---|---|
| **Global Internet Services** | **Strict** (e.g. RPKI) | **Heightened** (e.g. RIPE DB) | **Standard** (e.g. RIR stats) |
| **Core RIPE NCC Services** | **Heightened** (e.g. registry software) | **Standard** (e.g. LIR Portal) | **Standard** (e.g. compliance tooling) |

# Next steps

- Strategy document will be discussed with the Executive Board in the next meeting (September)
- Separated engagement has started to define service criticality
- Specific requirements and planning for RPKI and the RIPE Database to be discussed with the respective working groups

# Questions