RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RIPE NCC Technology Update

Secure and cost-effective services

Felipe Victolla Silveira | RIPE 88 | 22 May 2024

Technology Objectives 2024

4.4 Ensure security and compliance

4.1 Keep costs within budget

4.4 Maintain necessary levels of security and compliance with best practices and applicable regulations

4.1 Ensure the organisation's stability and financial strength

Secure services

Ensuring a stable Internet

Increased relevance of security

- Contractual value of registration for IPv4 addresses
  - Unauthorised transfers can potentially cause significant financial loss for our members
- Potential large impact on network connectivity caused by unauthorised access
  - E.g. misconfiguration in RPKI can cause massive disruption

Security investigation report

- Report published on 24 April 2024
  - https://www.ripe.net/support/documentation/disclosures-and-reports/ripe-ncc-access-security-investigation-report/
- Leaked credentials for RIPE NCC Access accounts had been published online that were not detected during our routine monitoring
  - Further, brute force attempts were executed against RIPE NCC Access accounts
- The passwords of 870 accounts were identified as being publicly exposed through data breaches
  - 104 of these were linked to LIR accounts
  - Email addresses had been updated for 270 accounts
  - 8 accounts were possibly compromised through brute force attacks

Actions taken

- Passwords were reset for all accounts identified in public data breaches and brute force attempts
- We closely monitored the resources connected to the 104 LIR accounts identified as vulnerable for suspicious activity
- For the accounts with recently updated email addresses, we reached out to account holders to confirm whether the change was legitimate
- We checked that no unauthorised changes had taken place for the accounts that were possibly compromised through brute forcing attempts

RIPE NCC Access improvements

- Introduction of mandatory 2FA at the end of March 2024
- Required significant code changes following a replatforming implemented last year
  - Migrated the backend engine from Atlassian Crowd to Keycloak
  - Replatformed to run on a Kubernetes cluster
- 2FA implementation moved from our own custom implementation to the native Keycloak one
  - Mandatory 2FA was then switched on directly from Keycloak
- Currently implementing support to FIDO2 keys and looking into other authentication methods
- More information in the RIPE Labs article:
  - https://labs.ripe.net/author/felipe_victolla_silveira/enhancing-the-security-of-ripe-ncc-access-recent-and-upcoming-changes/

ISAE 3000 compliance

Ensuring trust in RPKI

ISAE 3000 certification for RPKI

- RIPE NCC acts as one of the five RPKI Trust Anchors (TA) and issues certificates to resource holders
  - Key element in routing security
- Our goal is to enhance the security and integrity of the RPKI service
  - Build members' trust and confidence we are doing the right thing
  - Ease compliance efforts for any potential regulatory requirement arising
- The goal is to develop and implement an internal control framework that both encompasses all important IT security elements and can be tailored towards specific RPKI needs

Areas covered

- Huge effort involving the entire organisation, including departments like HR and Facilities
- The main goal is to ensure we have sufficient controls in place and that those controls are implemented through relevant policies and procedures
  - Controls should leave an audit trail so they can be inspected later on by a neutral third-party (auditor)

Current status

- ISAE 3000 Type I audit is underway, EY conducting the audit between April and May 2024
- 76 controls are currently being tested by EY
- The final report is expected to be delivered in June 2024
  - The report can only be disclosed to members, on request, under NDA
- ISAE3000 Type II audit will be performed in May 2025

Reducing data centre footprint

Cost-effective services

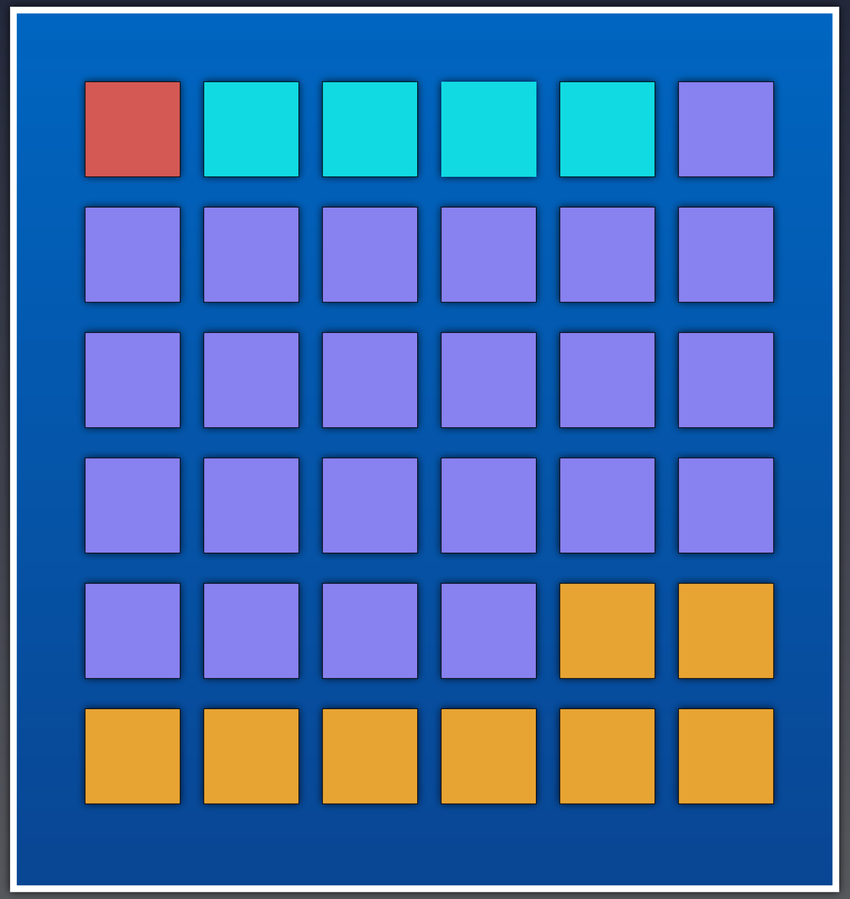
Reducing our data centre footprint

- Our current data centre footprint is large: 46 racks spread over two data centres in Amsterdam
  - Costs for housing and power alone currently approach €1M per year
- Half of that space is used for RIPE Atlas, RIS and RIPEstat datasets
  - This data is stored in a Hadoop cluster
  - These are very large datasets: over a petabyte worth of data telling the history of the Internet
- Our goal is to reduce that footprint by half before the end of 2024, and by more than 70% by the end of 2025
  - We want to achieve that by preserving all historical data and current service levels
- More information in the RIPE Labs article:
  - https://labs.ripe.net/author/felipe_victolla_silveira/reducing-the-ripe-nccs-data-centre-footprint/

Data centre - current situation

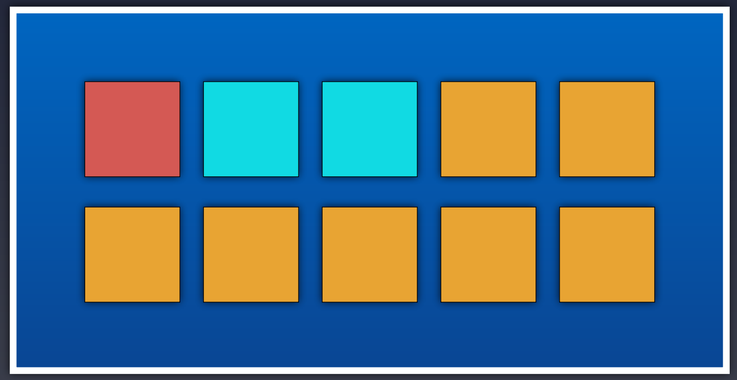
AM3

36 racks



AM5

10 racks



Network

Hadoop cluster

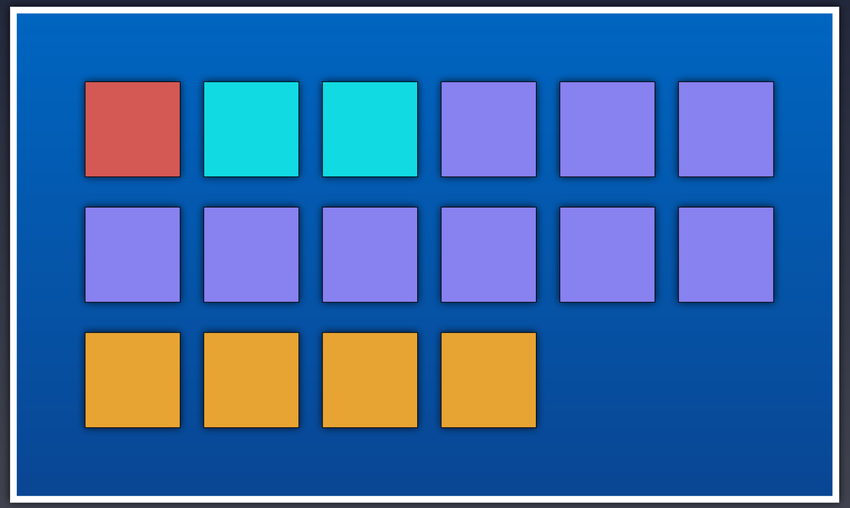
GII

IT

Data centre - goal end of 2024

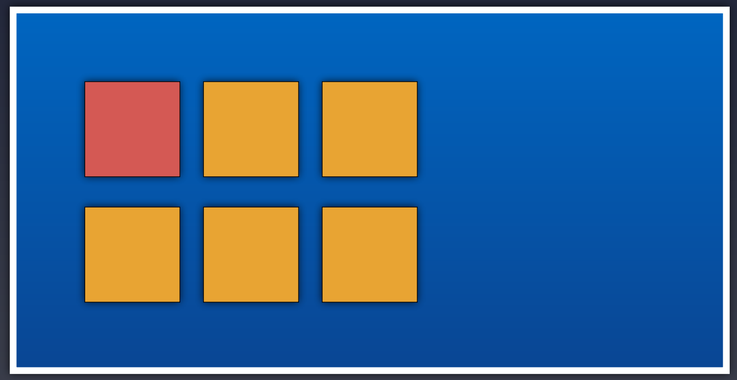
AM3

16 racks



AM5

6 racks



From 46 to 22 racks - 52% reduction

Network

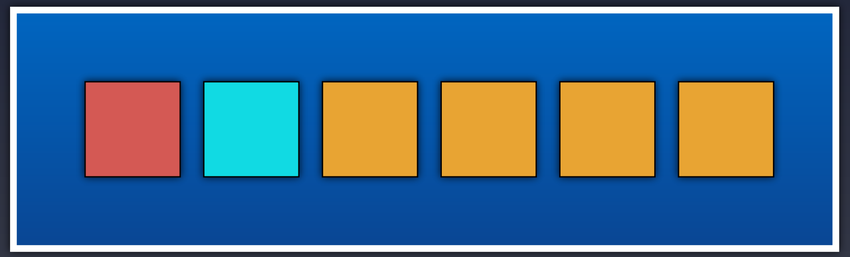
Hadoop cluster

GII

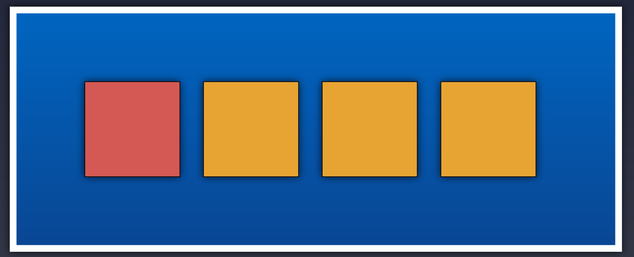
IT

Data centre - goal end of 2025

AM3



AM5



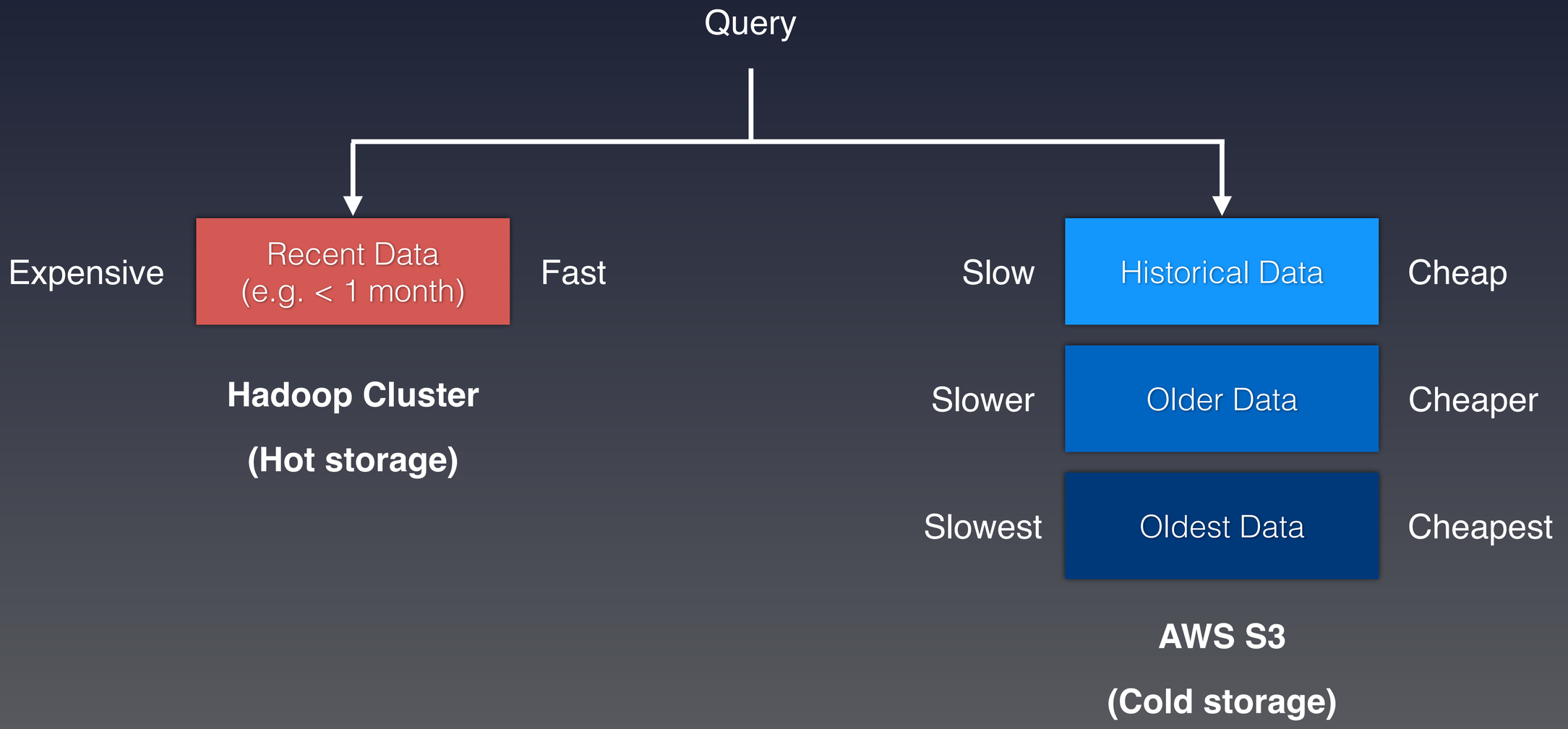
From 46 to 10 racks - 78% reduction

Network
Hadoop cluster
GII
IT

RIPE Atlas backend migration

- Since last year we have started with the migration of RIPE Atlas datasets from our on-premise infrastructure to a hybrid solution
  - Smaller cluster built using rented bare metal from a European cloud provider for recent data (e.g. less than one month old)
  - AWS S3 storage for historical data (very large datasets that comprise most of the current storage)
- New solution costs only a fraction of the current one while being future-proof at the same time
  - Expectation is that costs will be reduced by half
  - Service quality won’t be affected (e.g. search will still quickly return results)

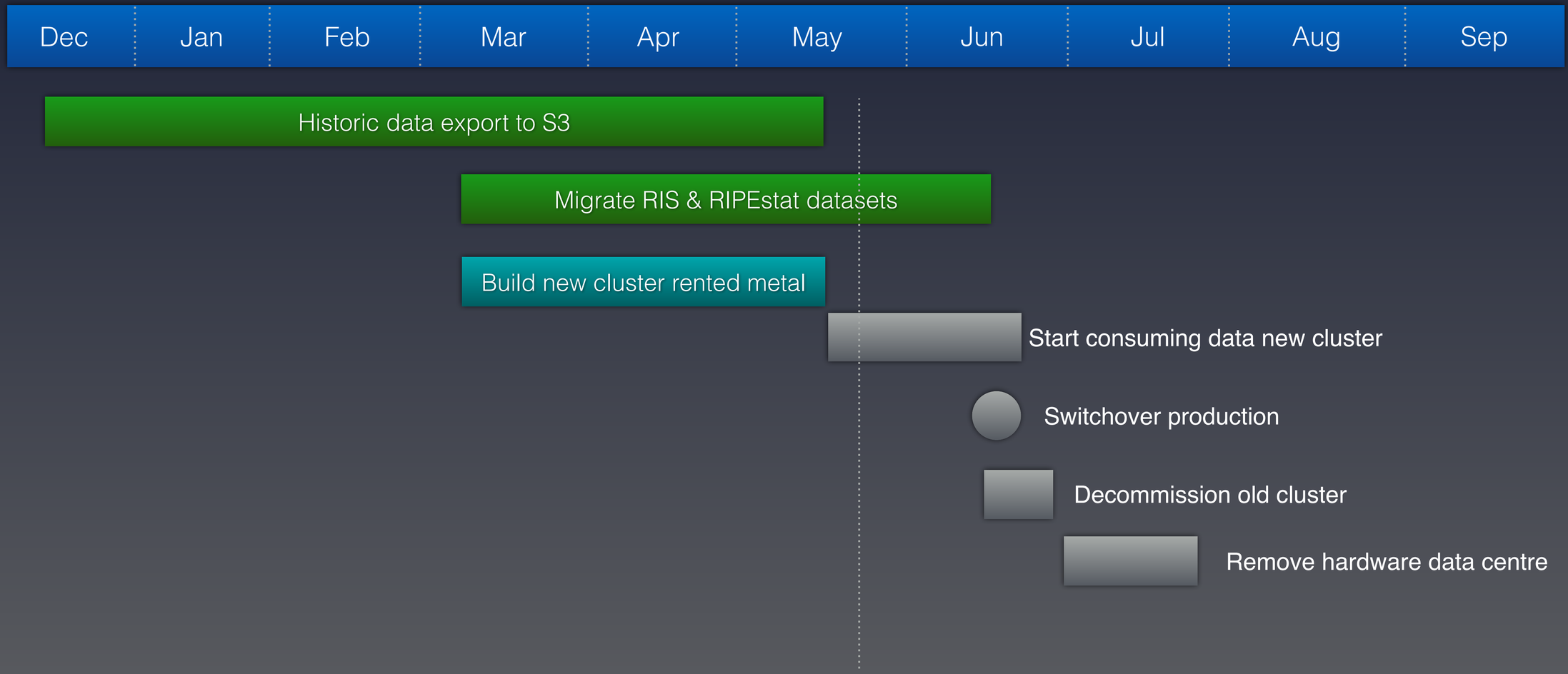
Proposal


Query
Expensive
Recent Data
(e.g. < 1 month)
Fast
Hadoop Cluster
(Hot storage)
Slow
Historical Data
Cheap
Slower
Older Data
Cheaper
Slowest
Oldest Data
Cheapest
AWS S3
(Cold storage)

Cost savings

- Whether moving to the cloud is cheaper or not depends on each use case
  - Here, AWS S3 proved to be significantly cheaper than doing it on-premise
- Cost of AWS S3 and of the new cluster are roughly the same
  - Total budget for new storage solution is €190K
- Since parameters are adjustable (e.g. size of the hot storage, tiering) we can optimise for cost, performance or find a good balance between both

Migration timelines



Takeaways

- Ensuring the security of our services is the top priority in Technology
  - The goal is to contribute to the stability of the Internet
- Cost effectiveness is our second priority
  - We are aiming to achieve significant cost reductions by modernising the infrastructure used by our Internet Measurement services

Questions

fvictolla@ripe.net
@victolla