RIPE NCC
RIPE NETWORK COORDINATION CENTRE

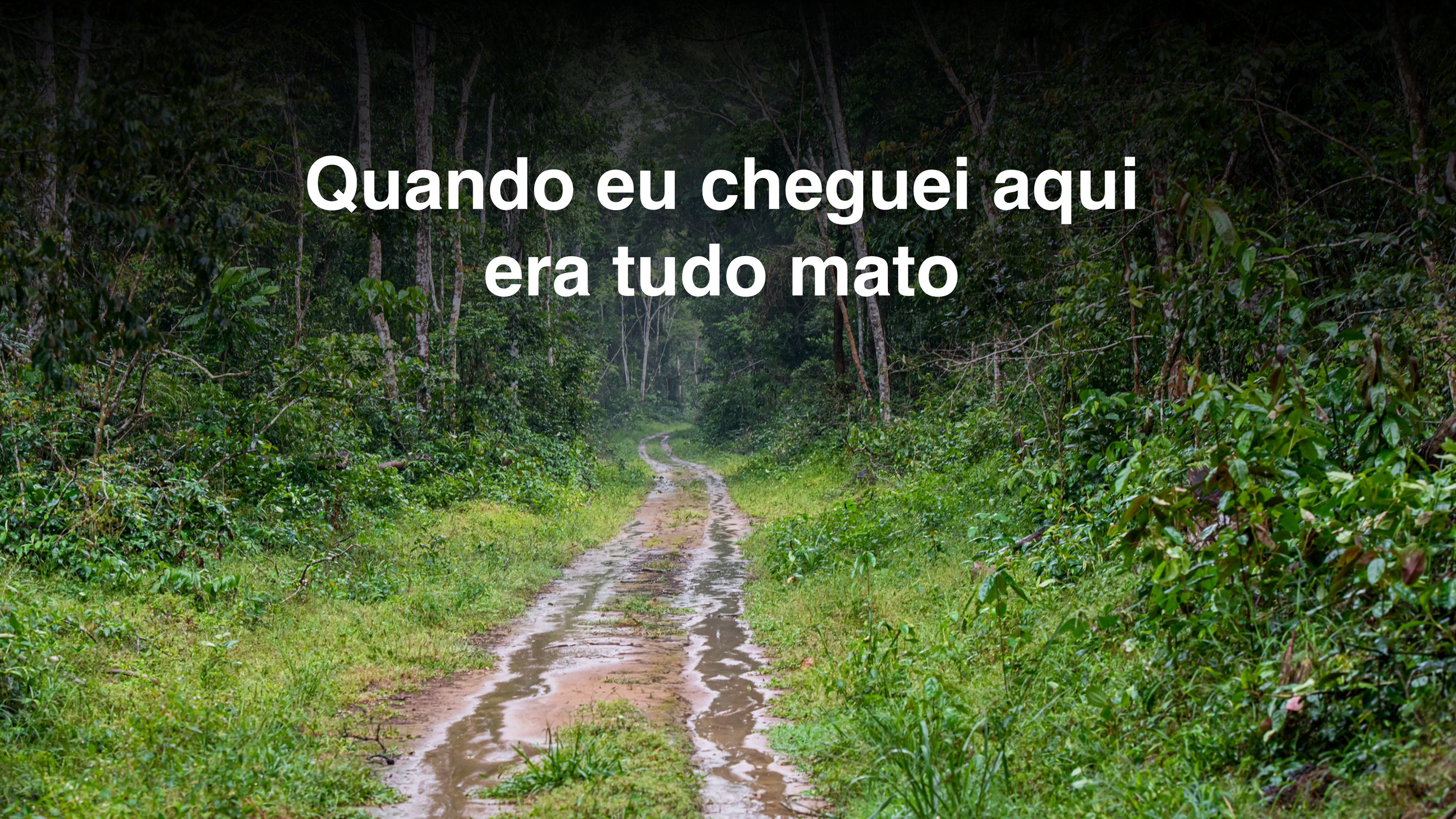
RPKI Validator da RIPE NCC

Focando no que importa

Felipe Victolla Silveira | Semana de Capacitação NIC.br | 1 Outubro 2021

Início dos tempos

Como tudo começou


Quando eu cheguei aqui
era tudo mato

Um pouco de história

- Pequena equipe com cerca de quatro engenheiros de software desenvolveram a primeira versão do RPKI core
- Uso do RPKI para routing security era bastante baixo na época
- Fortalecer o ecossistema era necessário
  - Desenvolvimento do RPKI Validator para estimular o uso e deployment
  - Primeira versão foi escrita em 2010
  - https://labs.ripe.net/author/agowland/ripe-ncc-validator-for-resource-certification/

Uso de RPKI em 2012

- Região RIPE NCC
  - 789 certificados
  - 561 ROAs (Route Origin Authorisation)
- Região LACNIC
  - 55 certificados
  - 52 ROAs

O que um Validator precisa fazer

- Na verdade, “Validator” é um termo incorreto - se chama Relying Party software
- Validar objetos assinados criptograficamente obtidos através de um repositório (RRDP ou rsync)
- É instalado no roteador do usuário
- Precisa ser humilde em termos de recursos
- Razoavelmente rápido e estável

RPKI Validator 2.0

- Lançado em Dezembro de 2011
  - https://www.ripe.net/ripe/mail/archives/routing-wg/2011-December/002024.html
- Versão mais madura de um Relying Party software
- Incluía várias funções novas, como interface web, filtros e white-listing
- Essa versão também continha problemas
  - Alto consumo de memória e baixa performance
  - Problemas raros mas recorrentes de estabilidade (e.g. DB deadlocks)
  - Desenvolvido em Scala, o que dificulta contribuições da comunidade

RPKI Validator 3.0

- Lançado em Maio 2018
  - https://ripe76.ripe.net/presentations/113-three-is-the-magic-number.pdf
- Completamente reescrito em Java
  - A linguagem que nós amamos odiar
- Escolhemos um stack clássico de Java para aplicações servidor
  - Spring Boot, H2, Hibernate (isso foi um erro)
- Tentativa de resolver os problemas da versão anterior
  - Dados movidos da memória para um banco de dados
  - Modelo de dados normalizado para um comportamento mais inteligente

Problemas do Validator 3.0

- Apesar da boa intenção, os problemas não foram resolvidos
  - Consumo de memória continuou bastante alto (em torno de 1Gb)
  - Diversos problemas de estabilidade (e.g. “crash and stuck”, “slow start”)
  - Tamanho do banco de dados crescendo de uma maneira absurda para alguns usuários (em um bug foi reportado 50 Gb)
- Diversas reclamações de usuários
- Várias dificuldades na reengenharia do sistema
  - Escolhas feitas no technology stack não estavam ajudando
  - Hibernate muito lento, comportamento imprevisível do framework
  - https://ripe79.ripe.net/presentations/65-RPKI-Validator-3-story.pdf

RPKI atingindo a maturidade

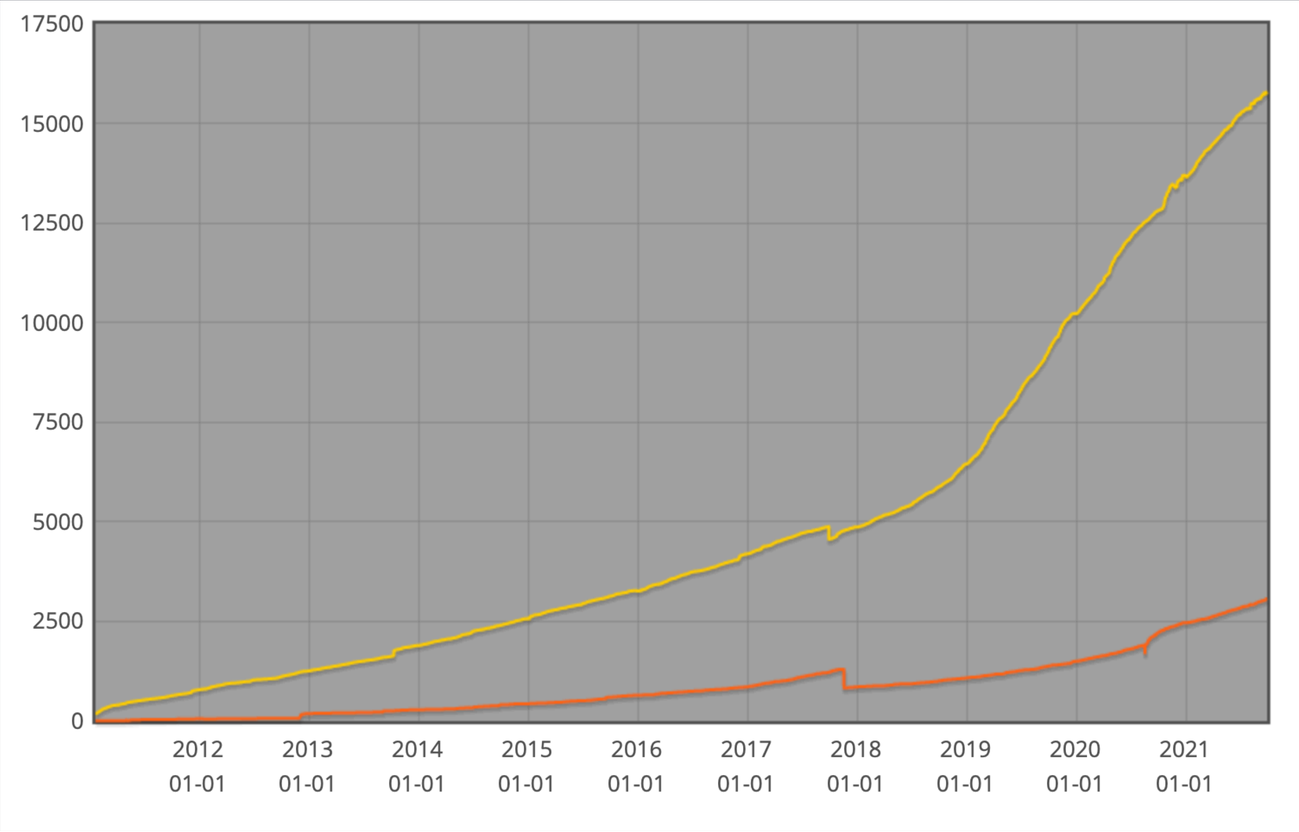
Tempo de decisões difíceis

Crescimento exponencial

- No começo de 2019, observamos um crescimento exponencial no uso da tecnologia RPKI ao redor do mundo
- T1 providers passaram a utilizar Route Origin Validation (ROV)
  - Telia, AT&T e outros
- Número de ROAs (Route Origin Authorisation) e certificados cresceu drasticamente

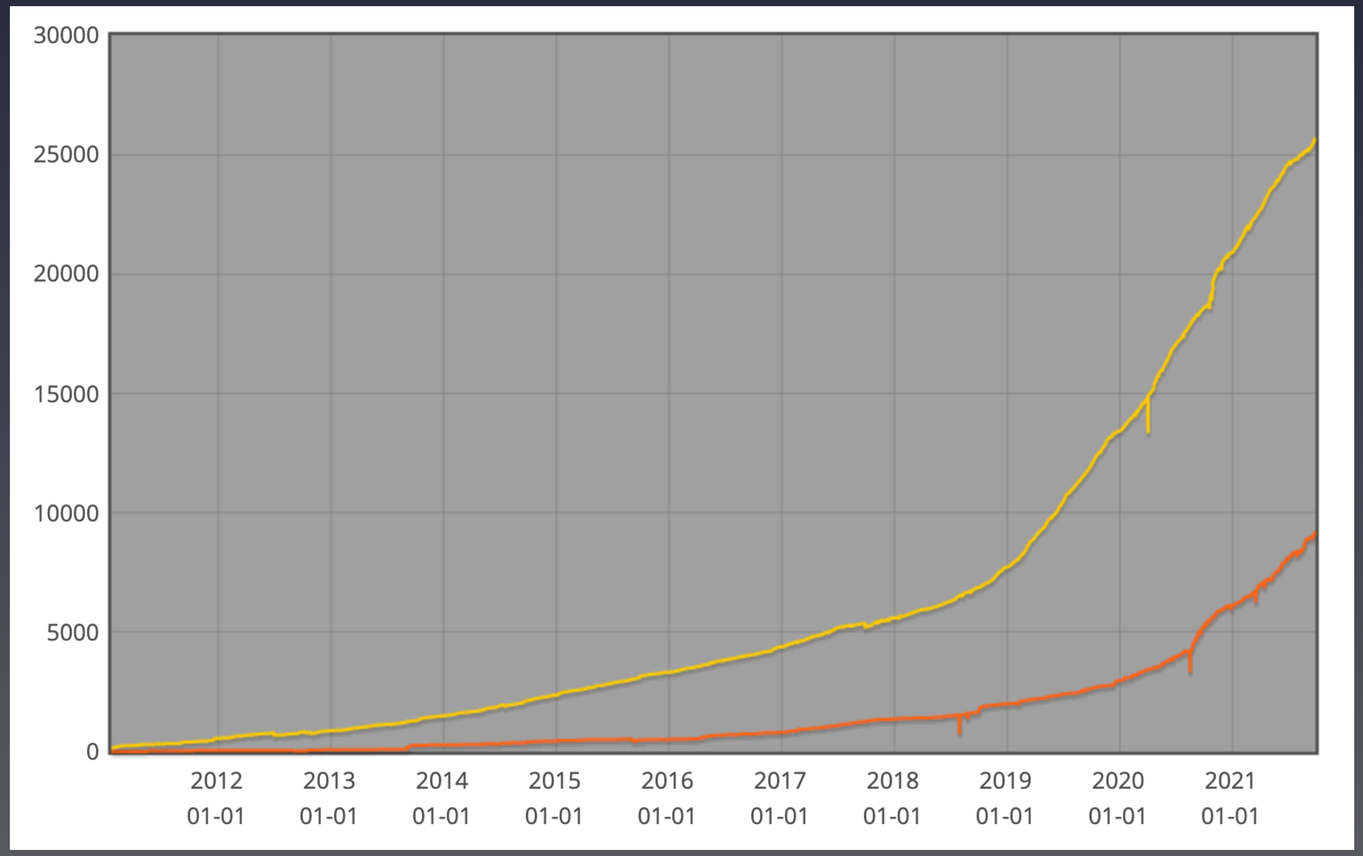
Uso do RPKI atualmente

- Número de certificados



Uso do RPKI atualmente

- Número de ROAs



Pressão na infraestrutura da RIPE NCC

- RPKI Validator não estava dando conta do recado
  - Problemas reportados por vários usuários
  - Situação estava se tornando constrangedora e afetando a nossa reputação
- Ao mesmo tempo, várias falhas na nossa infraestrutura básica (repositórios e Trust Anchor) no início de 2020
  - RPKI outage (24/2/2020) - problemas na validação dos dados dos repositórios
  - Problemas de consistência no repositório RRDP (5/3/2020)
  - Remoção acidental de ROAs (2.669) (1/4/2020)
  - Outage de 7 horas no repositório rsync (6/4/2020)

Medidas drásticas

- Força-tarefa com objetivo de resolver os problemas mais sérios
  - Monitoramento e controle de qualidade
  - Todas as demais atividades foram colocadas em stand-by
- Necessidade de olhar com seriedade a viabilidade de manter ambos RPKI Validator e Trust Anchor


Spreading
ourselves too thin

Crise existencial

- A RIPE NCC não é uma Software House
  - Para desenvolver esse tipo de produto, é necessário um conhecimento e experiência que não possuíamos em casa (e.g. C++, Rust)
  - Não é parte do nosso core business (somos um registro de números de Internet)
- Pressão da nossa comunidade que não queria que os recursos da RIPE NCC estivessem sendo utilizados no Validator
- Existência de outros produtos com nível de maturidade bastante superior (e.g. Routinator)
- Porém, o RPKI Validator ainda era bastante utilizado (em Outubro de 2020, tínhamos 28% do “market share”)

Decidimos o inevitável

- Em Outubro de 2020, anunciamos nossa decisão de descontinuar o RPKI Validator
  - https://labs.ripe.net/author/nathalie_nathalie/lifecycle-of-the-ripe-ncc-rpki-validator/
- Implementação em diversas fases:
  - 1 Janeiro 2021: Parar com novas funções
  - 1 Março 2021: Parar com novos RFCs e políticas (RIRs)
  - 1 Julho 2021: Descontinuar desenvolvimento e arquivar o projeto

Focando no que importa

Trust Anchor e repositórios

O que é mais importante?

- Para a RIPE NCC, são basicamente duas coisas:
  - Garantir a integridade, segurança e resiliência do Trust Anchor
  - Oferecer os repositórios RRDP e rsync com alta disponibilidade e baixa latência

Resiliência do Trust Anchor

- Para atingir esse objetivo, focamos no desenvolvimento de um control framework
  - SOC 2 Type II audit framework
  - Consiste em uma lista de controles focados em garantir a integridade de processos de uma forma abrangente em toda a empresa
  - Customizado para as necessidades do RPKI

RPKI control framework

Access control

Two-factor authentication

Network/application firewalls

Intrusion detection

Encryption

Access controls

Performance monitoring

Disaster recovery

Quality assurance

Processing monitoring

RPKI Control Framework na RIPE NCC

- Exemplos de controles:
  - Processo de recrutamento inclui background checks
  - Políticas de controle a quem tem acesso aos HSM keys
  - Políticas de senha
- Com base nessa lista, foi realizado uma gap analysis
  - Nossos processos internos cobrem todos os controles?
- Uma lista de control gaps foi identificada
  - Controles atualmente não implementados
- É necessário fechar todos os gaps, caso contrário não é possível adquirir uma acreditação através de uma auditoria externa independente

Disponibilidade dos repositórios

- Os repositórios são a parte externamente visível do Trust Anchor
  - São utilizados em tempo real para determinar a validade dos anúncios em BGP
  - Sua indisponibilidade pode causar problemas na operação da Internet
- Portanto, eles precisam ser:
  - Altamente disponíveis (99,999% de disponibilidade)
  - Baixa latência (baixo tempo de resposta)
- Para isso, é necessário:
  - Escalabilidade horizontal com distribuição geográfica
  - Bom monitoramento e suporte 24/7
  - Controle de qualidade

Escalabilidade horizontal

- Atualmente, o RRDP da RIPE NCC é provido a partir de um único servidor na AWS
  - Qualquer coisa que fizermos vai melhorar essa situação
- Atualizamos nosso código para permitir instâncias múltiplas de repositórios
  - Não apenas adicionar mais servidores em uma instância, mas sim instâncias completamente independentes e não relacionadas entre si
- Estamos migrando para servidores localizados em Amsterdam e gerenciados por nós mesmos
  - Equinix (datacentres) em duas localidades distintas (Science Park e Zuidoost)

Escalabilidade horizontal (2)

- A instância AWS vai continuar sendo atualizada, porém sem receber tráfico
  - Permanecerá como uma instância reserva
  - Em caso de falha da instância principal, faremos um failover (via DNS) para AWS
- Devido ao baixo número de servidores e concentração geográfica, utilizaremos um CDN para aumentar a performance e diminuir a latência
- No futuro, vamos adicionar mais servidores e revisar o uso de CDN
- Também pretendemos descontinuar o serviço na AWS e substituir por algo que tenhamos mais controle (e.g. Bare-metal as a Service)

Outros projetos

- Auditorias anuais de segurança
- Red team testing
- Open source RPKI core
- Publication as a Service
  - Para quem usa RPKI delegado (e.g. usando o Krill), sem precisar se preocupar em manter um repositório

Questions

fvictolla@ripe.net
@victolla