

LAC-2011-08

Inclusão de Informações do ROA no WHOIS
quando a mesma estiver disponível

Flávio Marcelo Amaral

LAC-2011-08

Introdução

- Através de recursos RPKI podemos validar o direito de uso de um recurso por parte de uma organização.
- Objetivo da certificação de recursos RPKI do LACNIC:
“Permite aos membros associados com recursos designados pelo LACNIC demonstrar de forma digital que possuem o direito de uso de endereços IPv4, IPv6 e ASN.”

LAC-2011-08

Processo de obtenção de um recurso

- Um ISP ao obter recursos de Internet (IPv6/IPv4/ASN)
 - Indica a seu upstream/peers quais os prefixos que vai anunciar (normalmente por preencher um formulário).
- Proveedores/peers **as vezes** verificam o direito de uso do recurso e configuram seus equipamentos.
- A integridade do sistema depende da confiança entre as partes.

LAC-2011-08

Objetivos da proposta:

- Quando fizermos uma consulta ao WHOIS do LACNIC sobre um certo prefixo, a resposta deve incluir a informação dos respectivos ROAs, caso estejam disponíveis.
- Fornecer informações para verificar a posse de recursos.
- Extensão natural da política: LAC-2010-03 Inclusão de ASN no whois quando estiver disponível.

LAC-2011-08

ROA

- ROA (Route Origination Authorization): são objetos assinado digitalmente com uma chave do certificado.
 - Os ROAs contém informações sobre a origem e a amplitude de um prefixo.
 - Os ROAs são assinados utilizando os certificados gerados pela RPKI.
 - Os ROAs assinados são copiados em um repositório publicamente accesível
 - Validade.

LAC-2011-08

Exemplo de consulta por WHOIS

route: 85.118.184.0/21

descr:

rsync://certrepo.ripe.net/certrepo/c2/dc..c3/1/5FPi-
j_228WTXOSTn3S8BR3bNak.roa

origin: AS33764

remarks: 85.118.184.0/21-24

mnt-by: RPKI-MNT source: RPKI # ripe

LAC-2011-08

Como o LACNIC opera

- Hoje opera no sistema hospedado: LACNIC possui as chaves e publica os certificados.
- Futuro: sistema “delegado”, cada entidade opera seu repositório de chaves.

LAC-2011-08

Uso:

- Principal objetivo: verificação de posse de um recurso e sua amplitude.
- Uma das aplicações:
 - Assinatura de informação em serviços de WHOIS
- A razão da proposta da política é fazer uma ponte entre o WHOIS e o RPKI para visualizar a posse dos recursos, data de validade e como eles são exportados.

LAC-2011-08

Resumo da Proposta

Inclusão de informações de ROAs (Route Origin Authorization) responsáveis por um prefixo nas informações de WHOIS de todos os prefixos recebidos pelo LACNIC. Quando esta informação estiver disponível.

Objetivo da Proposta

A proposta visa ajudar a identificar e validar a origem dos prefixos.

LAC-2011-08

Texto da Proposta

Inclusión de ROAs (Route Origin Authorization) en Whois Visando a autenticação de prefixos utilizados na nossa região, sugiro a inclusão obrigatória de de informações de ROAs (Route Origin Authorization) nas informações de WHOIS de todos os prefixos recebidos do LACNIC. Para ROAs que estão vencidos, revogados ou nunca foram cadastrados nada deve ser retornado.

No primeiro momento, somente as informações que estiverem no repositório do LACNIC seriam consultadas. Mas a medida que novos repositórios existam e conttenham informações de blocos emitidos pelo LACNIC, esses repositórios devem ser consultados também.

O campo *remarks* deve conter informações sobre el prefixo de como ele é exportado (tamanho máximo).

Isso ajudaria em ferramentas e em verificações de propriedades de prefixos.