Validador de RPKI
NIC MX - LACNIC

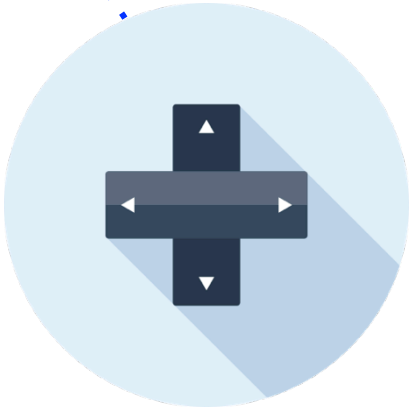
RPKI & Validación de origen

rsync

RTR

Sistema de RPKI
RIRs (milanic.lacnic.net)

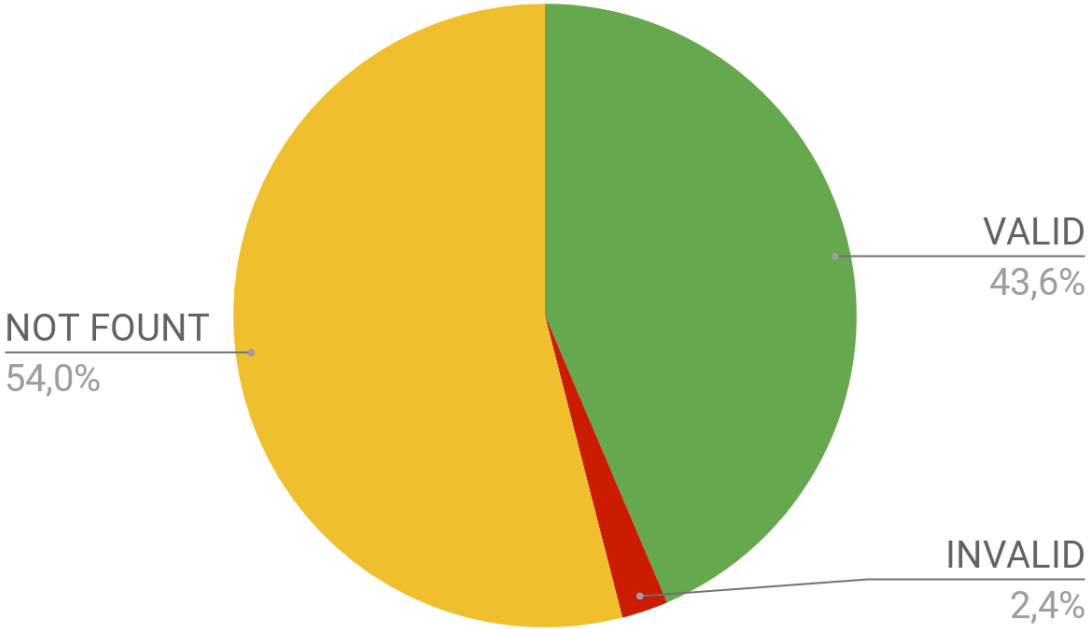
Caché local
Relying Party (RP)
Validador de RPKI



Router de Borde
Validación de Origen

RPKI en LATAM

Sistema de RPKI
RIRs (milanic.lacnic.net)



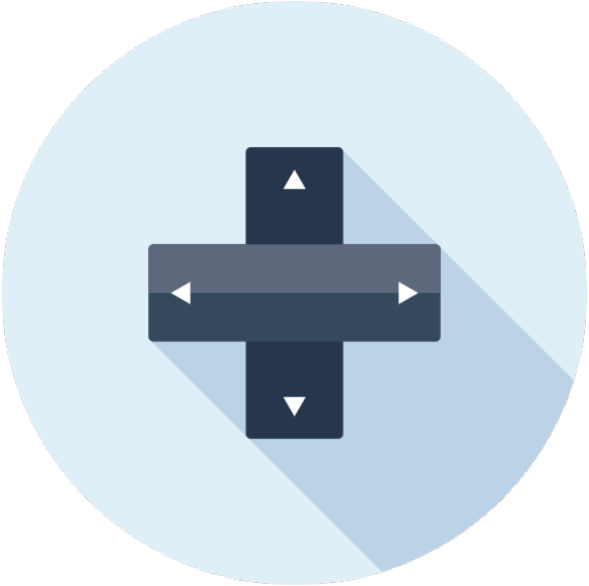
Validación de origen en LATAM

- AEPROVI (32 Organizaciones)

  Punto de intercambio de tráfico de Ecuador, pioneros en la implementación de validación de origen. (2013)

- NIC CR (28 Organizaciones)
  Implementaron validación de origen en el punto de intercambio de tráfico de Costa Rica (2015)

- RENATA (120 Organizaciones)
  Validación de origen en múltiples puntos (2017)



Validación de Origen

RPKI Validators

- RIPE NCC https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources
- RCYNIC https://github.com/dragonresearch/rpki.net
- RPSTIR de BBN https://github.com/bgpsecurity/rpstir

Caché local
Relying Party (RP)
Validador de RPKI

¿Que se valida?

→ **Formato de los Certificados** x.509, CRL y CMS: Los objetos deben respetar el formato especificado en los rfc5280 y rfc5911.

→ **Formato específico** de Certificados y CRL **para RPKI**: En el rfc6487 se describen detalladamente qué atributos deben o no estar presentes en los certificados emitidos en el contexto de RPKI, que extensiones son de uso crítico y cuales son de uso no crítico

→ Las **fechas de validez de los objetos**: Los certificados, ROAs y Manifiestos tienen fecha de validez inicial y fechas final, al momento de realizar la validación deben estar vigentes.

Caché local
Relying Party (RP)
Validador de RPKI

¿Que se valida?

→ **Verificación la firma**: Todos los objetos emitidos en RPKI son firmados digitalmente, de esta forma la firma de digital debe ser correcta.

→ **Revisión de la CRL**: Cada CA en RPKI genera periodicamente una CRL es importar verificar que el certificado que se está validando no es presente en la CRL del emisor.

→ **Inclusión de recursos**: La presencia de las extensiones para incluir direcciones IPv4, IPv6, ASNs o el valor especial “INHERIT” es obligatoria en todos los certificados emitidos en RPKI, una validación importante es que los recursos que esten presentes en los certificados esten contenidos en el certificados emisor.

Caché local
Relying Party (RP)
Validador de RPKI

¿Que se valida?

→ Coherencia en el **camino de certificación** (SIA / AIA): Cada certificado tiene rutas que referencian a los objetos emitidos por este y otras que apuntan al certificado emisor , la coherencia entre esas rutas es una validación a considerar

→ Coherencia entre **Manifiesto y Publicaciones**: Los objetos válidos para una CA están listados en el manifiesto emitido por esta, la consistencia entre estas dos listas es una validación.

Caché local
Relying Party (RP)
Validador de RPKI

RIPE NCC RPKI Validator

Versión 2.24 (Updated 9 January 2018)

This application allows operators to download and validate the global RPKI data set for use in their BGP decision making process and router configuration.

System requirements: a UNIX-like OS, Java 7 or 8, rsync and 2GB free memory. To install, simply unpack the archive and run "rpki-validator.sh" from the base folder.

https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources

Caché local
Relying Party (RP)
Validador de RPKI

Claves del éxito

El Validador de RIPE es el software de validación más común, en mi opinión la clave del éxito de este validador son las siguientes:

- **Fácil instalación**
  Una vez descargado el zip con el validador, este contiene el código compilado y las dependencias necesarias para que el software funcione, alcanza con identificar el script de arranque ejecutar los comandos clásicos, start, stop o restart para ejecutar esas acciones.

Claves del éxito

El Validador de RIPE es el software de validación más común, en mi opinión la clave del éxito de este validador son las siguientes:

- **Estabilidad del Sistema**
  Han sido muy pocos las fallas reportados sobre este sistema.

- **Estructura de archivos clara**
  El zip que te descargas, tiene una carpetas: tmp, data, log, conf, tal, lib, a primera vista el usuario puede identificar que y donde se puede tocar.

Claves del éxito

El Validador de RIPE es el software de validación más común, en mi opinión la clave del éxito de este validador son las siguientes:

- **Interfaz gráfica amigable**
  Una interfaz clara donde se indica que objetos pasaron la validación, cuales tiene errores pequeños (warnings), cuales TA están configurados. Además tiene otras funciones que pueden resultar interesantes

RPKI Validator | Home | Trust Anchors | ROAs | Ignore Filters | Whitelist | BGP Preview | Export

BGP Preview

This page provides a **preview** of the likely RPKI validity states your routers will associate with BGP announcement

- The RIPE NCC Route Collector information that was last updated 3 hours and 25 minutes ago.
- BGP announcements that are seen by 5 or more peers.
- The validation rules defined in RFC 6483.
- The validated ROAs found by this RPKI Validator after applying your filters and additional whitelist entries.

Please note that the BGP announcements your routers see may differ from the ones listed here.

Show 10 entries

ASN	Prefix	Validity
174	2a04:180::/29	UNKNOWN
174	2a03:bb40::/32	INVALID ASN
174	2a02:f181:1000::/48	UNKNOWN
174	2a02:56c0::/32	UNKNOWN
174	2a02:4200::/32	UNKNOWN
174	2a01:8640:4::/48	UNKNOWN
174	2a01:8640:3::/48	UNKNOWN
174	2a00:f620::/32	UNKNOWN
174	2620:fb::/56	UNKNOWN
174	2620:fb::/48	UNKNOWN

First | Previous | 1 | 2 | 3 | 4 | 5 | Next | Last

Showing 1 to 10 of 2,6

Otras Funciones Web

→ WS para acceder a la información validada.

→ Posibilidad de forzar la validación de un TA específica.

→ Poder incluir ROAs en una whitelist.

→ Poder ignorar prefijos y que para estos no se les asigne estado de validez.

→ Avisos de nuevas versiones una vez que estas están disponibles.

→ Poder ver los routers conectados al validador.

Para que otro validador

Cómo hacerlo mejor

- **Uso de memoria**
  El validador de RIPE exige un mínimo de 2gb de memoria libre para poder funcionar, esto implica que no es posible instalarlo en dispositivos de baja capacidad como raspberry pi, arduinos, etc.

- **Ghostbuster records**
  El validador no brinda información sobre los ghostbuster records encontrados en el repositorio.

Cómo hacerlo mejor

- **Prescindir de la interfaz gráfica**
  El validador de RIPE, siempre inicializa el webserver asociado a la app y no se puede optar por apagarlo para disminuir el uso de recursos.
- **Configuración del validador**
  Desde la interfaz gráfica no se puede modificar la configuración del validador, modificar tal, limpiar temporales, etc.

Gracias!

gerardo@lacnic.net

lacnic 29
30 abril / 4 mayo 2018
Ciudad de Panamá, Panamá

Autoridad Nacional para la Innovación Gubernamental
innovamos para ti

lacnic