BGPalerter & RPKI deployment

Massimo Candela

Senior Software Engineer - Network Information Systems Development massimo@ntt.net

BGPalerter

BGPalerter is a tool for analyzing streams of eBGP data

- We developed it for monitoring NTT prefixes
 - · hijacks, visibility loss, unexpected changes of configuration
- We released it open-source (BSD-3-Clause)
 - <u>https://github.com/nttgin/BGPalerter</u>
- It works in real time
- It's easy to use
 - Includes auto configuration
 - No data collection needed

Motivations

- Monitoring the correctness of BGP is a fundamental activity for any actor operating on the public Internet
- Monitoring BGP is not only useful for identifying hijacks committed by other ASes, but especially for timely identifying what your AS is doing. E.g.
 - Identify a prefix you were not supposed to announce
 - Identify a loss of visibility due to a wrong just-deployed configuration

Motivations

 In an Internet composed of thousands of network players, with different levels of automation and expertise, providing free and easy to use tools for monitoring the correctness of BGP is a key operation in improving the stability of the global Internet

What you can monitor

- Any of your prefixes loses visibility.
- Any of your prefixes is hijacked.
- Your AS is announcing RPKI invalid prefixes.
- Your AS is announcing prefixes not covered by a ROAs.
- Your AS is announcing a new prefix that was never announced before.
- One of the AS path used to reach your prefix matches a specific condition defined by you (regular expression).

Example of BGPalerter notification

visibility

The prefix 165.254.225.0/24 (description 1) has been withdrawn. It is no longer visible from 4 peers.

visibility

The prefix 2a00:5884::/32 (alarig fix test) has been withdrawn. It is no longer visible from 4 peers.

hijack

A new prefix 165.254.255.0/25 is announced by AS4, and AS15562. It should be instead 165.254.255.0/24 (description 2) announced by AS15562

hijack

A new prefix 2a00:5884:ffff:/48 is announced by AS208585. It should be instead 2a00:5884::/32 (alarig fix test) announced by AS204092, and AS45

hijack

The prefix 2a00:5884::/32 (alarig fix test) is announced by AS15563 instead of AS204092, and AS45

newprefix

Possible change of configuration. A new prefix 2a00:5884:ffff:/48 is announced by AS204092. It is a more specific of 2a00:5884::/32 (alarig fix test).



Setup

https://github.com/nttgin/BGPalerter

🖟 nttgin / l	BGPalerter				⊙ Unwatch → 31 🖧 Star 285
<> Code	! Issues 7	' 👬 Pull requests 🕞	Actions 🔟 Projects 🕕 Security 🗠 Insight	hts 🔯 Settings	
		° master → 🐉 3 brand	thes 🔿 14 tags	Go to file Add file ▼	About 段
👮 massimocandela bring back valio		🔮 massimocandela bring	back validation cycle period to 100 ms	✓ e890275 4 hours ago [™] 978 commits	Software to monitor streams of BGP data. Pre-configured for real-time detection of visibility loss, RPKI invalid
		.github	Update stale.yml	6 months ago	announcements, and hijacks.
		docs	v1.26.0 release hotfix (#295)	2 days ago	bgp monitoring
		src	bring back validation cycle period to 100	ms 4 hours ago	🛱 Readme
tests		tests	hotfix vrp file reloading (#298)	6 hours ago	述 BSD-3-Clause License
		🗅 .babelrc	ugraded to babel 7	13 months ago	
		🗋 .eslintrc.json	added mocha support for esling	9 months ago	Releases 14
		🗋 .gitignore	hotfix vrp file reloading (#298)	6 hours ago	◊ v1.26.0 (Latest)
		🗅 .hound.yml	Update .hound.yml	9 months ago	2 days ago
		🗅 .npmignore	hotfix vrp file reloading (#298)	6 hours ago	+ 13 releases
		🗅 .travis.yml	v1.26.0 release hotfix (#295)	2 days ago	
			proxy support (#234)	2 months and	Packages

Setup

Latest release v1.26.0 🛇 v1.26.0 massimocandela released this 2 days ago -O- e890275 [features] Compare 🗸 Introduced proxy support. • Introduced volume parameter. It allows to specify a directory that will be used by BGPalerter for reading/writing all needed files. • Introduced persistStatus parameter. If set to true, when BGPalerter is restarted the list of alerts already sent is recovered. This avoids duplicated alerts. #103. Introduced reportTelegram. • Added the possibility to specify an external file for as VRPs list for monitorRPKI. Added UDP support on reportSyslog. Assets 5 ☆ bgpalerter-linux-x64 61.4 MB 61.5 MB ☆ bgpalerter-win-x64.exe 57.4 MB Source code (zip) Source code (tar.gz)

Setup

• Download and run. That's all.

wget https://github.com/nttgin/BGPalerter/releases/latest/ download/bgpalerter-linux-x64

chmod +x bgpalerter-linux-x64

./bgpalerter-linux-x64

Setup - auto-configuration

BGPalerter, version: 1.24.0 environment: production

Loaded config: /Users/massimocandela/Documents/work/BGPalerter/config.yml

? The file prefixes.yml cannot be loaded. Do you want to auto-configure BGPalerter? Yes

? Which Autonomous System(s) you want to monitor? (comma-separated, e.g. 2914,3333) 2914

? Are there sub-prefixes delegated to other ASes? (e.g. sub-prefixes announced by customers) Yes

? Do you want to be notified when your AS is announcing a new prefix? Yes

Run!

BGPalerter, version: 1.26.0 environment: production Loaded config: /home/bgpalerter/production/config.yml Monitoring 165.254.225.0/24 Monitoring 165.254.255.0/24 Monitoring 192.147.168.0/24 Monitoring AS2914

- The auto-configuration runs only the first time
- If your prefixes are not covered by ROAs, a warning will ask you to review prefixes.yml by hand

Report on file

[massimo@bgpalerter:~\$ tail -f logs/reports-2019-09-22.log 2019-09-22T00:47:21.681Z [production] verbose: A new prefix 1.22.84.0/24 is announced by AS45528. It should be instead 2019-09-22T00:47:21.681Z [production] verbose: A new prefix 1.22.72.0/23 is announced by AS45528. It should be instead 2019-09-22T00:47:21.681Z [production] verbose: A new prefix 1.22.84.0/22 is announced by AS45528. It should be instead 2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.22.72.0/24 is announced by AS45528. It should be instead 2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.22.94.0/23 is announced by AS45528. It should be instead 2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.22.94.0/23 is announced by AS45528. It should be instead 2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.23.83.0/24 is announced by AS45528. It should be instead 2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.22.85.0/24 is announced by AS45528. It should be instead 2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.22.86.0/24 is announced by AS45528. It should be instead 2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.22.86.0/24 is announced by AS45528. It should be instead 2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.22.86.0/24 is announced by AS45528. It should be instead 2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.23.88.0/24 is announced by AS45528. It should be instead 2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.23.88.0/24 is announced by AS45528. It should be instead 2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.23.88.0/24 is announced by AS45528. It should be instead 2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.23.88.0/24 is announced by AS45528. It should be instead 2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.23.87.0/24 is announced by AS45528. It should be instead 2019-09-22T00:47:21.682Z [production] verbose: A new prefix 1.23.87.0/24 is announc

Reports

- Alerts are automatically bundled/throttled
- At the moment alerts can be delivered to:
 - Files, Email, Slack, Alerta dashboard, Kafka, Syslog, Webex, Mattermost, Telegram, Pushover, any HTTP end-point
- Users groups allow to deliver alerts about specific resources, or about specific types of issue, to specific set of users/targets
- Also the BGP messages can be sent to files, another monitoring system, or database

Report by email

The prefix 165.254.255.0/24 (Job) is announced by AS2914 instead of AS15562

DETAILS:

Monitored prefix:	165.254.255.0/24	
Prefix Description:	Job	
Usually announced by:	AS15562	
Event type:	basic-hijack-detection	
Now announced by:	AS2914	
Now announced with:	165.254.255.0/24	
When event started:	2019-08-15 09:10:05 UTC	
Last event:	2019-08-15 09:10:05 UTC	
Detected by peers:	1	
2	<pre>https://stat.ripe.net/widget</pre>	
<pre>/bgplay#w.resource=165.254.255.0/24&w.ignoreReannouncements=true&</pre>		
	5&w.endtime=1565860205&	
w.rrcs=0,1,2,5,6,7,10	,11,13,14,15,16,18,20&w.type=bgp	

Report on Slack

visibility

The prefix 165.254.225.0/24 (description 1) has been withdrawn. It is no longer visible from 4 peers.

visibility

The prefix 2a00:5884::/32 (alarig fix test) has been withdrawn. It is no longer visible from 4 peers.

hijack

A new prefix 165.254.255.0/25 is announced by AS4, and AS15562. It should be instead 165.254.255.0/24 (description 2) announced by AS15562

hijack

A new prefix 2a00:5884:ffff:/48 is announced by AS208585. It should be instead 2a00:5884::/32 (alarig fix test) announced by AS204092, and AS45

hijack

The prefix 2a00:5884::/32 (alarig fix test) is announced by AS15563 instead of AS204092, and AS45

newprefix

Possible change of configuration. A new prefix 2a00:5884:ffff:/48 is announced by AS204092. It is a more specific of 2a00:5884::/32 (alarig fix test).

16

A Dashboard for BGPalerter

aleri	ta	Recent Top 10	Watch						Configuration - Jane Bloggs - About
ervice		;	e	rror				Open	Auto Update
ALL 133	Infrastructu	re 44 Product	ion 43	Development	46				
everity	Status	Last Receive Time	Dupl.	Environment	Service	Resource	Event	Value	Text
Critical	Open	Fri 16 Oct 00:55	0	Production	Tornskel	Ockley	breachOfConfidentiality	n/a	Marfa Godard Banksy voluptate cred. Cray gastrop
Critical	Open	Fri 16 Oct 00:40	0	Production	Notestack	Extremes	inputOutputDeviceError	n/a	Aesthetic chia biodiesel, shabby chic Brooklyn Mar
Major	Open	Fri 16 Oct 00:56	0	Production	Deployinator	kue	dataSetOrModemError	n/a	Nihil crucifix tousled, shabby chic cardigan et me
Major	Open	Fri 16 Oct 00:40	0	Production	Support	stylebot	fileError	n/a	Commodo roof party gluten-free placeat. Forage qu
Major	Open	Fri 16 Oct 00:39	0	Production	Macto	jslint.vim	cableTamper	n/a	Hella squid dolor readymade Banksy, master cleans
Minor	Open	Fri 16 Oct 00:55	0	Production	Firetray	spine.contacts	lanError	n/a	Laboris gastropub artisan occaecat, tattooed VHS
Minor	Open	Fri 16 Oct 00:39	0	Production	Phnx	cssSandpaper	communicationsProtocolError	n/a	Church-key veniam commodo, put a bird on it try-ha
Warning	Open	Fri 16 Oct 00:55	0	Production	Friar	PxLoader	communicationsSubsystemFailure	n/a	Odio minim laborum, cupidatat Shoreditch biodiese
Warning	Open	Fri 16 Oct 00:55	0	Production	Yschool	bbb	adapterError	n/a	Sustainable PBR cardigan Brooklyn, listicle elit o
Indeterminate	Open	Fri 16 Oct 00:56	0	Production	Jsconfus	webgireport	adapterError	n/a	Neutra vegan tilde, proident keytar swag dreamcatc
Indeterminate	Open	Fri 16 Oct 00:55	0	Production	Photoswipe	RealTimeMonitor	dteDceInterfaceError	n/a	Roof party listicle cillum, enim Tumblr DIY artisa
Indeterminate	Open	Fri 16 Oct 00:55	0	Production	Wireit	currency.io	configurationOrCustomizationError	n/a	Biodiesel labore 8-bit, odio eu American Apparel
Indeterminate	Open	Fri 16 Oct 00:55	0	Production	Zia	openstreetbugs	proceduralError	n/a	Sustainable selvage slow-carb brunch bespoke odio
Indeterminate	Open	Fri 16 Oct 00:55	0	Production	Nodelint	LightFace	ouputDeviceError	n/a	Meh qui brunch, twee mixtape Shoreditch dolor Pi

What if my BGPalerter is noisy?

- Probably you are using BGPalerter for quite some time
 - Update BGPalerter
 - Update config.yml
 - See <u>https://github.com/nttgin/BGPalerter/blob/master/</u> config.yml.example
 - Check "thresholdMinPeers"
 - Exclude prefixes in prefixes.yml

<pre>1 dconnectors: 2 d - file: connectorRIS 3 d carefulSubscription: true 4 d params: 4 d params: 5 d carefulSubscription: true 6 url: ws://ris-live.ripe.net/vl/ws/ 7 perfessagebeflate: true 8 d subscription: 9 d type: UPDATE 10 host: 11 socketOptions: 12 d l socketOptions: 13 d l includews: false 4 d chanel: hijack 7 d chanel: hijack 7 d chanel: neprefix 2 d - file: monitorNewPrefix 2 d - file: monitorPerfix 2 d - file: monitorPerfix 3 d - file: monitorPerfix 4 d chanel: params: 5 d - file: monitorPerfix 5 d - file: monitorPath 5 d - file:</pre>	
<pre>1 name: ris 2 carefulSubscription: true 2 carefulSubscription: true 2 carefulSubscription: 3 carefulSubscription: 4 carefulSubscription: 5 carefulSubscription: 9 carefulSubscript</pre>	
4 0 params: 5 - carefulSubscription: true 8 0 subscription: 9 0 moreSpecific: true 10 type: UPDATE 11 - host: 12 - file: monitorfiljack 13 - file: monitorfils 14 - file: monitorfils 15 - file: monitorfils 16 - file: monitorfils 17 chanel: newprefix 18 - file: monitorfils 19 - file: monitorfils 10 - file: monitorfils 12 - file: monitorfils 13 - file: monitorfils 14 - file: monitorfils	
5 i carefulSubscription: true 6 u'l: ws://ris-live.ripe.net/v1/ws/ 7 perMessageDFlate: true 8 0 subscription: 9 impreSpecific: true 10 host: 12 socketOptions: 13 includeRaw: false 14 - 15 channel: hijack 16 name: basic-hijack-detection 17 channel: hijack 18 name: basic-hijack-detection 19 j 20 - file: monitorHijack 21 - file: monitorHijack 22 - file: monitorHijack 23 - file: monitorHijack 24 - file: monitorHijack 25 - file: monitorHewPrefix 26 - file: monitorHewPrefix 27 - file: monitorPath 28 - file: monitorPath 29 - file: monitorPath 29 - file: monitorPath	
6 url: ws://ris-live.ripe.net/vl/ws/ 7 perMessageDeflat: true 9 moreSpecific: true 10 type: UPDATE host: socketOptions: 13 includeRaw: false 14 includeRaw: false 15 monitors: 16 - file: monitorHijack 17 channel: hijack 18 name: basic-hijack-detection 19 params: 20 - file: monitorHewPrefix 21 - file: monitorHemPrefix 22 - file: monitorHemPrefix 23 - file: monitorPath 24 name: prefix-detection 25 params: 26 - file: monitorPath 27 - file: monitorPath 28 - file: monitorPath 29 - file: monitorPath	
7 subscription: 8 subscription: 9 imoreSpecific: true 10 type: UPDATE 10 isocketOptions: 13 includeRaw: false 14 includeRaw: false 15 channel: hijack 18 name: basic-hijack-detection 19 jettesholdMinPeers: 2 20 - file: monitorNewPrefix 21 channel: newprefix 22 - file: monitorPeth 24 name: prefix-detection 25 params: 26 - file: monitorPath 27 - file: monitorPath 28 - file: monitorPath 29 - file: monitorPath	
<pre>subscription: moreSpecific: true type: UPDATE host: socketOptions: i cludeRaw: false - file: monitorHijack channel: hijack - file: monitorHijack-detection params: - file: monitorNewPrefix - file: monitorNewPrefix - file: monitorNewPrefix - file: monitorPath - file: monitorPath</pre>	
9 impreSpecific: true 10 ippression 11 ippression 12 ippression 13 ippression 14 ippression 15 ippression 16 - file: monitorHijack 17 ippression 18 ippression 19 ippression 19 ippression 20 ippression 21 ippression 22 - file: monitorNewPrefix 23 ippression 24 ippression 25 ippression 26 ippression 27 ippression 28 ippression 29 ippression 20 ippression 21 ippression 22 ippression 23 ippression 24 ippression 25 ippression 26 ippression 27 ippression 28 ippression 29 ippression	
10 type: UPDATE 11 host: 2 bost: 3 cocketOptions: 3 includeRaw: false 14 4 5 6 - file: monitorHijack 18 19 10 10 11 12 13 14 15 16 17 18 19 10 10 11 11 12 13 14 15 16 17 18 19 10 10 11 11 12 13 14 15 16 16 17 18 19 10 11 11 12 13 14 14 15 15 16 17 18 19 10 10 10 11 12 14 15 16 17 18 19 10 10 10 10 11 12 14 15 15 16 16 17 </td <td></td>	
11 host: 12 includeRaw: false 13 includeRaw: false 14 15 16 17 18 name: basic-detection 19 19 19 11 11 12 13 14 15 16 17 18 19 19 10 11 11 12 13 14 15 16 17 18 19 19 10 10 11 12 13 14 15 15 16 17 18 19 19 10 10 10 11 12 13 14 15 16 17 18 19 10 11 12 12 13 14 15 15 16 17 18 19 10 11 12 12 13 14 15 15 16 17 18 19 10 <	
12 socket0ptions: 13 includeRaw: false 14 14 15 16 17 18 18 19 19 19 10 10 11 12 13 14 14 15 16 17 18 19 19 19 10 10 11 12 13 14 14 15 16 17 18 19 19 10 10 10 10 11 12 14 15 16 16 17 18 19 19 10 10 10 11 12 12 14 15 16 16 17 18 19 10 10 10 10 11 12 12 13 14 14 15 15 16 16 17 18 19 10 10 10 10 <td></td>	
<pre>includeRaw: false includeRaw: false include</pre>	
14 15 16 - file: monitorHijack 17 - file: monitorHijack 18 19 params: 20 21 11 22 - file: monitorNewPrefix 23 15 16 17 18 19 10 10 10 11 12 13 14 15 14 15 15 16 16 17 18 19 10 10 10 11 12 13 14 14 15 14 15 15 16 16 17 18 19 19 19 10 10 11 12 13 14 15 16 16 17 18 <	
<pre>imonitors: in onitors: in file: monitorHijack in name: basic-hijack-detection params: i params: i channel: newprefix i channel: ne</pre>	
16 - file: monitorHijack 17 channel: hijack 18 name: basic-hijack-detection 19 params: 20 - file: monitorNewPrefix 21 - 22 - file: monitorNewPrefix 23 channel: newprefix 24 name: prefix-detection 25 - params: 26 - file: monitorPath 27 - 28 - file: monitorPath 29 - file: monitorPath	
17 channel: hijack 18 name: basic-hijack-detection 19 params: 20 d 21 thresholdMinPeers: 2 21 - 22 d 23 channel: newprefix 23 channel: newprefix 24 name: prefix-detection 25 d params: 26 d thresholdMinPeers: 2 27 28 d e - file: monitorPath 29 channel: path	
18 name: basic-hijack-detection 19 params: 20 thresholdMinPeers: 2 21 - 22 - 23 channel: newprefix 24 name: prefix-detection 25 params: 26 thresholdMinPeers: 2 27 - 28 - 9 channel: path	
19 params: 20 thresholdMinPeers: 2 21 22 23 channel: newprefix 24 name: prefix-detection 25 params: 26 thresholdMinPeers: 2 27 28 - file: monitorPath 29 channel: path	
20 ithresholdMinPeers: 2 21 22 23 channel: newprefix 23 channel: newprefix 24 name: prefix-detection 25 params: 26 ithresholdMinPeers: 2 27 28 - file: monitorPath 29 channel: path	
21 22 = file: monitorNewPrefix 23 24 name: prefix-detection 25 params: 26 thresholdMinPeers: 2 27 28 = file: monitorPath 29 channel: path	
22 - file: monitorNewPrefix 23 channel: newprefix 24 name: prefix-detection 25 params: 26 thresholdMinPeers: 2 27 - 28 - file: monitorPath 29 channel: path	
23 channel: newprefix 24 name: prefix-detection 25 params: 26 thresholdMinPeers: 2 27 - file: monitorPath 29 channel: path	
24 name: prefix-detection 25 params: 26 thresholdMinPeers: 2 27 - 28 - file: monitorPath 29 channel: path	
25 params: 26 thresholdMinPeers: 2 27 28 29 channel: path	
26 intresholdMinPeers: 2 27 28 28 - file: monitorPath 29 channel: path	
27 28 → file: monitorPath 29 channel: path	
<pre>28 - file: monitorPath 29 channel: path</pre>	
29 channel: path	
30 name: path-matching	
31 b params:	
32 d thresholdMinPeers: 0	
34 - file: monitorVisibility	
35 channel: visibility	
36 name: withdrawal-detection	
37 b params:	
38 d thresholdMinPeers: 20	

3.4		
14 15	emonitors:	
16	- file: monitorHijack	
17	channel: hijack	
18	name: basic-hijack-detection	
19	params:	
20	thresholdMinPeers: 2	
21		
22	<pre>- file: monitorNewPrefix</pre>	
23	channel: newprefix	
24	name: prefix-detection	
25	params:	
26	thresholdMinPeers: 2	
27		
28	🕂 – file: monitorPath	
29	channel: path	
30	name: path-matching	
31	params:	
32	thresholdMinPeers: 0	
33		
34	<pre></pre>	
35	channel: visibility	
36	name: withdrawal-detection	
37	params:	
38	thresholdMinPeers: 20	
39 40	- file: monitorAS	
40	channel: misconfiguration	
41	name: asn-monitor	
43	params:	
44	thresholdMinPeers: 2	
45		
46	e – file: monitorRPKI	
47	channel: rpki	
48	name: rpki-monitor	
49	params:	
50	vrpProvider: ntt	
51	thresholdMinPeers: 1	
52	checkUncovered: false	
53	preCacheROAs: true	
54	e refreshVrpListMinutes: 15	
55		

repo	
	file: reportFile
	channels:
	- hijack
	 newprefix visibility
	- visibility - path
	- parn - misconfiguration
	- rpki
	params:
	persistAlertData: false
	alertDataDirectory: alertdata/
# -	file: reportEmail
#	channels:
#	- hijack
#	- newprefix
#	- visibility
#	- path
#	- misconfiguration
#	- <u>rpki</u>
#	params:
#	showPaths: 5 # Amount of AS_PATHs to report in the alert
#	senderEmail: bgpalerter@xxxx
#	# BG <u>Palerter</u> uses <u>nodemailer</u> .
#	# The smtp section can be configured with all the parameters available at <u>https://nodemailer.com/smtp/</u>
#	# the following are just the most useful one
#	smtp:
#	host: localhost
#	port: 25
#	secure: false # If true the connection will use TLS when connecting to server. If false it will be still possible doing connection upgrade via STARTTLS
#	ignoreTLS: false # If true TLS will be completely disabled, including STARTTLS. Set this to true if you see certificate errors in the logs.
#	auth:
#	user: username
#	pass: password
#	type: login
#	tls: reject/authorized, true
#	rejectUnauthorized: true # Reject unauthorized certificates notifiedEmails:
#	default:
#	
#	- joe@example.org - noc@example.org
*	nocecompicatory
# -	file: reportSlack
#	channels:
#	- hijack
#	- newprefix

#		
#		
#	default: _YOUR_ALERTA_API_URL_	
#	– file: reportWebex	
#		
#		
#		
#		
#		
#		
#		
#		
#		
#		
#	– file: reportHTTP	
#	channels:	
#	– hijack	
#	- newprefix	
#	- visibility	
#	– path	
#	- misconfiguration	
#	– <u>cpki</u>	
#		
#		
#	default: '{"text": "\${summary}"}'	
#	headers:	
#		
#		
#		
#	default: _YOUR_WEBHOOK_URL_	
	- file: reportTelegram	
#		
#		
#		
#		
#		
#		
#		
#		
#		
#	chatIds:	
#		

216		
	######################################	
	# Notification settings:	
	# - notificationIntervalSeconds	
	# Defines the amount of seconds after which an alert can be repeated. An alert is repeated only if the event that	
	<pre># triggered it is not yet solved.</pre>	
	# - persistStatus	
	# Persist the status of BGPalerter. If the process is restarted, the list of alerts already sent is recovered	
	# and they are not repeated. The process must be able to write on disc, this option will create a file inside .cach	e/
	notificationIntervalSeconds: 14400	
	persistStatus: true	
	ologging:	
	directory: logs	
	logRotatePattern: YYYY-MM-DD	
	backlogSize: 1000 #Advanced option, read the doc	
	maxRetainedFiles: 10	
	maxFileSizeMB: 15	
	compressOnRotation: false	
	checkForUpdatesAtBoot: true	

	<pre># Process monitoring settings: # Uncomment or add classes under processMonitors if you want to monitor or send logs about the status of the BGPalerter p</pre>	racas
	* Uncomment of add classes under processionitors if you want to monitor of send togs about the status of the bogaterier p	roces
	#processMonitors:	
	# - file: uptimeApi	
	# params:	
	# useStatusCodes: true	
	<pre># host: null</pre>	
	# port: 8011	
	#	
	# - file: uptimeHealthcheck	
	# params:	
	# url: url_to_poll	
	# intervalSeconds: 300	
	<pre># method: get</pre>	
	#	
	# — file: sentryModule	
	# params:	
	<pre># dsn: https://<key>@sentry.io/<project></project></key></pre>	

216	

	# Notification settings:
	# - notificationIntervalSeconds
	# Defines the amount of seconds after which an alert can be repeated. An alert is repeated only if the event that
	<pre># triggered it is not yet solved.</pre>
	# - persistStatus
	# Persist the status of BGPalerter. If the process is restarted, the list of alerts already sent is recovered
	# and they are not repeated. The process must be able to write on disc, this option will create a file inside .cache/
	notificationIntervalSeconds: 14400
	persistStatus: true
	elogging:
	directory: logs
	logRotatePattern: YYYY-MM-DD
	backlogSize: 1000 #Advanced option, read the doc
	maxRetainedFiles: 10
	maxFileSizeMB: 15
	compressOnRotation: false
236	
	checkForUpdatesAtBoot: true
	# Process monitoring settings:
	# Uncomment or add classes under processMonitors if you want to monitor or send logs about the status of the BGPalerter process
	eprocessMonitors:
	e – file: uptimeApi
	e params:
	useStatusCodes: true
	host: null
	0 port: 8011
	# - file: uptimeHealthcheck
	# params:
	# url: url_to_poll
	# intervalSeconds: 300
	# method: get
	# - file: sentryModule
	# params:
	<pre># dsn: https://<key>@sentry.io/<project></project></key></pre>

 \leftrightarrow \rightarrow C (i) localhost:8011/status

}

Supporting RPKI deployment

RPKI monitoring

- Monitor if your AS is announcing prefixes RPKI invalid or not covered by ROAs
 - You can also monitor only specific prefixes



incoming-webhook APP 14:18

rpki

прки The route 194.32.71.0/24 announced by AS15562 is not RPKI valid. Accepted with AS path: [31313,6830,2914,15562]. Valid ROA: origin AS0 prefix 194.32.71.0/24 max length 24

rpki

The route 209.24.0.0/24 announced by AS15562 is not RPKI valid. Accepted with AS path: [31313,6830,2914,15562]. Valid ROA: origin AS0 prefix 209.24.0.0/24 max length 24

RPKI monitoring

- Particularly useful:
 - Before RPKI deployment, since it will let you "test" what announcements will be invalid after singing the ROAs.
 - During RPKI deployment, since it will let you know if any of your announcements are invalid.
 - After you deployed RPKI, in order to be sure that all future BGP configurations will be covered by ROAs.

3.4		
14 15	emonitors:	
16	- file: monitorHijack	
17	channel: hijack	
18	name: basic-hijack-detection	
19	params:	
20	thresholdMinPeers: 2	
21		
22	<pre>- file: monitorNewPrefix</pre>	
23	channel: newprefix	
24	name: prefix-detection	
25	params:	
26	thresholdMinPeers: 2	
27		
28	🕂 – file: monitorPath	
29	channel: path	
30	name: path-matching	
31	params:	
32	thresholdMinPeers: 0	
33		
34	<pre></pre>	
35	channel: visibility	
36	name: withdrawal-detection	
37	params:	
38	thresholdMinPeers: 20	
39 40	- file: monitorAS	
40	channel: misconfiguration	
41	name: asn-monitor	
43	params:	
44	thresholdMinPeers: 2	
45		
46	e – file: monitorRPKI	
47	channel: rpki	
48	name: rpki-monitor	
49	params:	
50	vrpProvider: ntt	
51	thresholdMinPeers: 1	
52	checkUncovered: false	
53	preCacheROAs: true	
54	e refreshVrpListMinutes: 15	
55		



Generate your VRPs JSON file

- Using external VRPs list is quick and easy, but you are essentially trusting somebody else writing such VRPs correctly
- You can generate your JSON file periodically and BGPalerter will load it

31

rpki-client

- You can download rpki-client from
 - <u>https://www.rpki-client.org/</u>
 - Or <u>https://pkgs.org/search/?q=rpki-client</u>
- You also need jq for manipulating the JSON
 - <u>https://stedolan.github.io/jq/</u>
 - Or e.g. "apt-get install jq", "brew install jq"
- Periodically run in crontab (e.g. every 15 min)
 - rpki-client -j test/ && cat test/export.json | jq .roas > test/vrps.json

rpki-client

	mon	nitors:	
		- file: monitorHijack	
	T T		
		channel: hijack	
		name: basic-hijack-detection	
		params:	
		thresholdMinPeers: 2	
	. ₹ T	- file: monitorNewPrefix	
		channel: newprefix	
		name: prefix-detection	
		params:	
		thresholdMinPeers: 2	
	. ¢ -	- file: monitorPath	
		channel: path	
		name: path-matching	
		params:	
		thresholdMinPeers: 0	
	. ♦ -	- file: monitorVisibility	
		channel: visibility	
		name: withdrawal-detection	
		params:	
		thresholdMinPeers: 20	
	. ⊣ -	- file: monitorAS	
		channel: misconfiguration	
		name: asn-monitor	
		params:	
		thresholdMinPeers: 2	
	. ⊢ −	- file: monitorRPKI	
		channel: rpki	
		name: rpki-monitor	
		params:	
50			
		thresholdMinPeers: 1	
		checkUncovered: false	
		preCacheROAs: true	
		refreshVrpListMinutes: 15	
55			

Generate your VRPs JSON file

- You can use BGPalerter to do some tests before to deploying RPKI
- You can add in vrps.json some ROA that you plan to sign but you didn't yet
- You can leave it running and check if any of your announcements are going to be RPKI invalid and/or if you organisation is able to stick to the "signed" ROAs

Content of vrps.json

1 I			
		"asn": "13335", "prefix": "103.21.244.0/24", "maxLength": 24	
	∳ {	"asn": "2914", "prefix": "123.4.5.0/14", "maxLength": 24	

Contribute!

- Source code on GitHub
 - https://github.com/nttgin/BGPalerter



Massimo Candela

Senior Software Engineer Network Information Systems Development <u>massimo@ntt.net</u>

www.gin.ntt.net @GinNTTnet #globalipnetwork #AS2914