Bgp monitoring protocol in practice – tool and experience

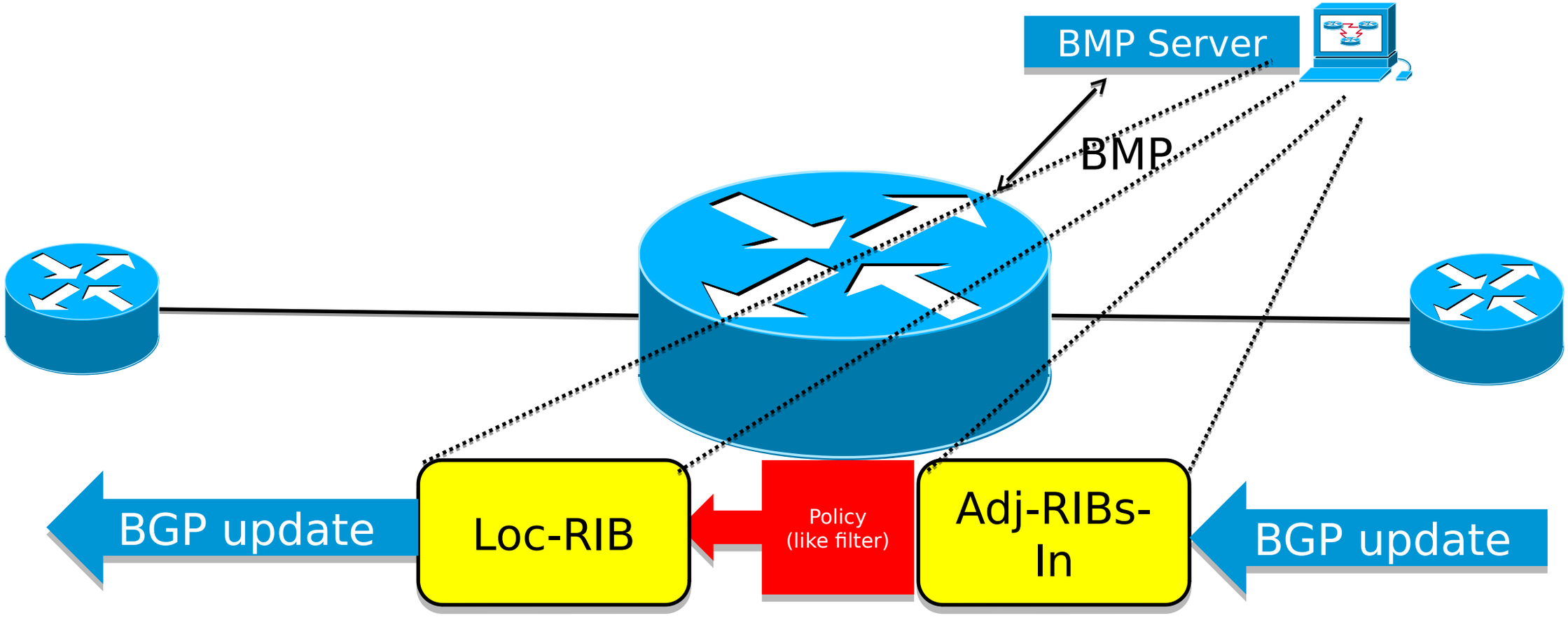
Csaba Máté and János Mohácsi
Governmental Information Technology Development Agency – Hungarian NREN

GEANT STF meeting 13.Oct.2018

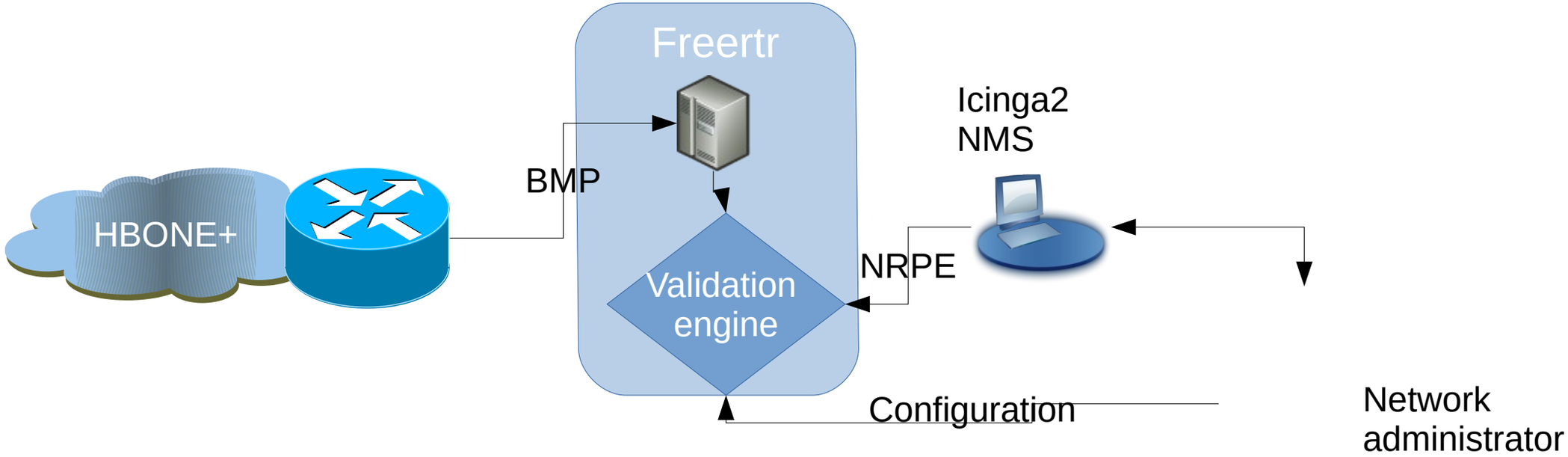
BGP Monitoring - headache – possible solution

- Need for BGP monitoring
  - Status of the BGP peers
  - Validity of the routes
  - Detect prefix hijacks
  - Detect routing outages
  - Detect MITM attacks
- BGP SNMP MIB is broken -
- Better tool exists BGP Monitoring Protocol – RFC 7854
  - Incoming BGP messages (before policy filters) replayed to BMP server
  - Report capabilities of BGP session on establisment and and reason for BGP teardown

How BMP is working?



BMP at KIFU



- BMP exported to Freertr
- Validation at Freertr
- Monitored via NRPE with Icinga2

Session Manager

local | kaputt

```
kaputt.debrecen3#show bmp bmp
from            peer                                    as     state  change  last
195.111.97.83   152.66.0.125                            2547   true   1       07:06:08
195.111.97.83   195.111.103.206                         12301  true   1       07:06:08
195.111.97.108  62.40.96.23                             20965  true   1       07:06:11
195.111.97.108  62.40.96.24                             20965  true   1       07:06:11
195.111.97.108  62.40.102.26                            20965  true   1       07:06:11
195.111.97.108  62.40.124.101                           20965  true   1       07:06:11
195.111.97.108  80.98.45.14                             6830   true   1       07:06:11
195.111.97.108  80.239.195.56                           1299   true   1       07:06:11
195.111.97.108  81.183.2.166                            5483   true   1       07:06:11
195.111.97.108  83.97.88.81                             21320  true   1       07:06:11
195.111.97.108  100.68.1.1                              65404  true   1       07:06:11
195.111.97.108  149.11.10.9                             174    true   1       07:06:11
195.111.97.108  193.188.137.1                           5507   true   1       07:06:11
195.111.97.108  193.188.137.2                           5507   true   1       07:06:11
195.111.97.108  193.188.137.53                          5400   true   1       07:06:11
195.111.97.108  193.188.137.74                          8708   true   1       07:06:11
195.111.97.108  193.188.137.175                         6939   true   1       07:06:11
195.111.97.108  193.224.231.138                         65012  true   1       07:06:11
195.111.97.108  194.149.11.41                           5588   true   1       07:06:11
195.111.97.108  195.191.97.254                          59649  true   1       07:06:11
195.111.97.108  2001:738:1040:193:224:231:136:138        65012  true   1       07:06:11
195.111.97.108  2001:798:1::65                          21320  true   1       07:06:11
195.111.97.108  2001:798:1b:10aa::5                     20965  true   1       07:06:11
195.111.97.108  2001:7f8:35::5507:1                     5507   true   1       07:06:11
195.111.97.108  2001:7f8:35::5507:2                     5507   true   1       07:06:11
195.111.97.108  2001:7f8:35::6939:1                     6939   true   1       07:06:11
```

Session Manager

local | kaputt

```
kaputt.debrecen3#show startup-config bmp bmp
server bmp2mrt bmp
 port 12345
 max-time 3600000
 backup /data/mrt/bmp.old
 file /data/mrt/bmp.mrt
 bulk-down
 neighbor 195.111.97.108 62.40.96.23 rx bgp4 65532 62.40.96.23
 neighbor 195.111.97.108 62.40.96.24 rx bgp4 65532 62.40.96.24
 neighbor 195.111.97.108 62.40.102.26 rx bgp4 65533 62.40.102.26
 neighbor 195.111.97.108 80.239.195.56 rx bgp4 65535 80.239.195.56
 neighbor 195.111.97.108 83.97.88.81 rx bgp4 65535 83.97.88.81
 neighbor 195.111.97.108 149.11.10.9 rx bgp4 65535 149.11.10.9
 neighbor 195.111.97.108 193.188.137.1 rx bgp4 65535 193.188.137.0
 neighbor 195.111.97.108 193.188.137.2 rx bgp4 65535 193.188.137.255
 neighbor 195.111.97.108 193.188.137.175 rx bgp4 65535 193.188.137.175
 neighbor 195.111.97.108 195.191.97.254 rx bgp4 65534 195.191.97.254
 neighbor 195.111.97.108 2001:798:1::65 rx bgp6 65535 2001:798:1::65
 neighbor 195.111.97.108 2001:7f8:35::5507:1 rx bgp6 65535 2001:7f8:35::5507:fff1
 neighbor 195.111.97.108 2001:7f8:35::5507:2 rx bgp6 65535 2001:7f8:35::5507:fff2
 neighbor 195.111.97.108 2001:7f8:35::6939:1 rx bgp6 65535 2001:7f8:35::6939:1
 neighbor 195.111.97.108 2001:978:2:27::7:1 rx bgp6 65535 2001:978:2:27::7:1
 neighbor 195.111.97.108 2001:2000:3080:14f5::1 rx bgp6 65535 2001:2000:3080:14f5::1
 neighbor 195.111.97.109 62.40.124.17 rx bgp4 65535 62.40.124.17
 neighbor 195.111.97.109 83.97.88.85 rx bgp4 65535 83.97.88.85
 neighbor 195.111.97.109 193.188.137.1 rx bgp4 65535 193.188.137.1
 neighbor 195.111.97.109 193.188.137.2 rx bgp4 65535 193.188.137.2
 neighbor 195.111.97.109 195.191.97.254 rx bgp4 65534 195.191.97.255
```

```
 neighbor 195.111.97.109 193.188.137.1 rx bgp4 65535 193.188.137.1
 neighbor 195.111.97.109 193.188.137.2 rx bgp4 65535 193.188.137.2
 neighbor 195.111.97.109 195.191.97.254 rx bgp4 65534 195.191.97.255
 neighbor 195.111.97.109 2001:798:1::69 rx bgp6 65535 2001:798:1::69
 neighbor 195.111.97.109 2001:798:10:10aa::15 rx bgp6 65535 2001:798:10:10aa::15
 neighbor 195.111.97.109 2001:7f8:35::5507:1 rx bgp6 65535 2001:7f8:35::5507:1
 neighbor 195.111.97.109 2001:7f8:35::5507:2 rx bgp6 65535 2001:7f8:35::5507:2
 vrf inet
 exit

kaputt.debrecen3#show bmp bmp | include 20965
195.111.97.108  62.40.96.23                     20965  true   1       07:07:01
195.111.97.108  62.40.96.24                     20965  true   1       07:07:01
195.111.97.108  62.40.102.26                    20965  true   1       07:07:01
195.111.97.108  62.40.124.101                   20965  true   1       07:07:01
195.111.97.108  2001:798:1b:10aa::5             20965  true   1       07:07:01
195.111.97.109  62.40.124.17                    20965  true   1       07:07:03
195.111.97.109  2001:798:10:10aa::15            20965  true   1       07:07:03

kaputt.debrecen3#show startup-config bmp bmp | include  62.40.96.24
 neighbor 195.111.97.108 62.40.96.24 rx bgp4 65532 62.40.96.24

kaputt.debrecen3#show ipv4 bgp 65532 unicast summary
as    learn  accept  will  done  neighbor      uptime
1955  0      0       0     0     62.40.96.23   never
1955  0      0       0     0     62.40.96.24   never

kaputt.debrecen3#
```

Session Manager

local | kaputt

```
kaputt.debrecen3#show bmp bmp | include 20965
195.111.97.108  62.40.96.23                    20965  true   1       07:09:33
195.111.97.108  62.40.96.24                    20965  true   1       07:09:33
195.111.97.108  62.40.102.26                   20965  true   1       07:09:33
195.111.97.108  62.40.124.101                  20965  true   1       07:09:33
195.111.97.108  2001:798:1b:10aa::5            20965  true   1       07:09:33
195.111.97.109  62.40.124.17                   20965  true   1       07:09:35
195.111.97.109  2001:798:10:10aa::15           20965  true   1       07:09:35

kaputt.debrecen3#show ipv6 bgp 65535 unicast summary
as    learn  accept  will  done  neighbor                uptime
1955  1      1       0     0     2001:798:1::65          never
1955  1      1       0     0     2001:798:1::69          never
1955  0      0       0     0     2001:798:10:10aa::15    never
1955  2      2       0     0     2001:7f8:35::5507:1     never
1955  2      2       0     0     2001:7f8:35::5507:2     never
1955  1      1       0     0     2001:7f8:35::5507:fff1  never
1955  1      1       0     0     2001:7f8:35::5507:fff2  never
1955  0      0       0     0     2001:7f8:35::6939:1     never
1955  2      2       0     0     2001:978:2:27::7:1      never
1955  2      2       0     0     2001:2000:3080:14f5::1  never

kaputt.debrecen3#
kaputt.debrecen3#
kaputt.debrecen3#
kaputt.debrecen3#
kaputt.debrecen3#
```

```
195.111.97.108  62.40.124.101                20965  true   1       07:09:33
195.111.97.108  2001:798:1b:10aa::5           20965  true   1       07:09:33
195.111.97.109  62.40.124.17                 20965  true   1       07:09:35
195.111.97.109  2001:798:10:10aa::15          20965  true   1       07:09:35

kaputt.debrecen3#show ipv6 bgp 65535 unicast summary
as    learn  accept  will  done  neighbor                uptime
1955  1      1       0     0     2001:798:1::65          never
1955  1      1       0     0     2001:798:1::69          never
1955  0      0       0     0     2001:798:10:10aa::15    never
1955  2      2       0     0     2001:7f8:35::5507:1     never
1955  2      2       0     0     2001:7f8:35::5507:2     never
1955  1      1       0     0     2001:7f8:35::5507:fff1  never
1955  1      1       0     0     2001:7f8:35::5507:fff2  never
1955  0      0       0     0     2001:7f8:35::6939:1     never
1955  2      2       0     0     2001:978:2:27::7:1      never
1955  2      2       0     0     2001:2000:3080:14f5::1  never

kaputt.debrecen3#
kaputt.debrecen3#
kaputt.debrecen3#
kaputt.debrecen3#
kaputt.debrecen3#show ipv6 bgp 65535 unicast database
prefix           hop      metric          aspath
2001:738::/32    6.6.6.6  255/100/0/10    1955
2001:738:4::/48  6.6.6.6  255/100/0/100   12303

kaputt.debrecen3#
```

Session Manager

local | kaputt

```
kaputt.debrecen3#show startup-config nrpe
server nrpe hbone
 access-class acl_121
 error-commands
 error-hostname
 error-truncate 500
 resolve bmp-.* ^(?<a>[0-9a-f]+[.:][0-9a-f.:]+);.*$
 resolve bmp-.* ^.*;(?<a>[0-9a-f]+[.:][0-9a-f.:]+);.*$
 replace bmp-.* ;false; ;DOWN;
 replace bmp-.* ;true; ;UP;
 check bmp-arbor command sho bmp arbor
 check bmp-arbor description arbor peering
 check bmp-arbor error peering change(s) detected
 check bmp-arbor alternate
 check bmp-arbor req-txt from;peer;as;state;change;last
 check bmp-arbor req-reg 195.111.100.79;195.111.97.91;1955;true;[0-9];.*
 check bmp-arbor req-reg 195.111.100.79;195.111.97.92;1955;true;[0-9];.*
 check bmp-arbor req-reg 195.111.100.79;195.111.97.93;1955;true;[0-9];.*
 check bmp-arbor req-reg 195.111.100.79;195.111.97.179;1955;true;[0-9];.*
 check bmp-arbor req-reg 195.111.100.79;2001:738::179:666;1955;true;[0-9];.*
 check bmp-arbor req-reg 195.111.100.79;195.111.100.167;1955;true;[0-9];.*
 check bmp-arbor req-reg 195.111.100.79;2001:738::a;1955;true;[0-9];.*
 check bmp-arbor req-reg 195.111.100.79;2001:738::b;1955;true;[0-9];.*
 check bmp-arbor req-reg 195.111.100.79;2001:738::c;1955;true;[0-9];.*
 check bmp-arbor req-reg 195.111.100.79;2001:738::179:1;1955;true;[0-9];.*
 check bmp-archived command sho flash /data/mrt/ | include old
kaputt.debrecen3#
kaputt.debrecen3#
```

Service Information

Last Updated: Wed Sep 5 05:20:03 CEST 2018 - Update in 46 seconds [pause]
Icinga Classic UI **1.11.6** (Backend **1.11.6**) - Logged in as *matecs@niif.hu*

- View **Information** For **This Host**
- View **Service Status Detail** For **This Host**
- View **Alert History** For **This Service**
- View **Trends** For **This Service**
- View **Alert Histogram** For **This Service**
- View **Availability Report** For **This Service**
- View **Notifications** For **This Service**
- View **Scheduling Queue** For **This Service**

Service
IPv4 address hijack

On Host
kaputt.debrecen3.hbone.hu

(kaputt.debrecen3)

Member of
No servicegroups.

Service Dependencies

195.111.100.70, 2001:738::179:70

Service State Information

Current Status:	CRITICAL (for 0d 11h 23m 20s)
Status Information:	ERROR 1 prefix(es) STOLEN - kaputt.debrecen3#sho ipv4 bgp 65535 unicast database + 193.224.165.0/24;6.6.6.6;255/100/0/0;21320
Performance Data:	
Current Attempt:	3/3 (HARD state)
Last Check Time:	2018-09-05 05:17:46
Check Type:	ACTIVE
Check Source / Reachability:	N/A
Check Latency / Duration:	3.743 / 0.177 seconds
Next Scheduled Active Check:	2018-09-05 05:24:46
Last State Change:	2018-09-04 17:56:43
Last Notification:	2018-09-04 18:01:16 (notification 1)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	2018-09-05 05:19:16 (0d 0h 0m 47s ago)

Service Commands

- Disable active checks of this service
- Re-schedule the next check of this service
- Submit passive check result for this service
- Stop accepting passive checks for this service
- Start obsessing over this service
- Acknowledge this service problem
- Disable notifications for this service
- Delay next service notification
- Send custom service notification
- Schedule downtime for this service
- Disable event handler for this service
- Disable flap detection for this service
- Add a new Service comment
- Reset Modified Attributes

724 UP | 1 / 0 / 0 DOWN | 0 / 0 / 0 UNREACHABLE | 0 PENDING | 1 / 725 TOTAL

1664 OK | 5 / 0 / 0 WARNING | 17 / 0 / 1 CRITICAL | 0 / 0 / 1 UNKNOWN | 0 PENDING | 24 / 1688 TOTAL

ICINGA

725 / 0 / 0
4.05 / 30.07 / 4.168 s
18.95 / 74.46 / 41.261 s

1688 / 0 / 0
0.08 / 55.12 / 2.159 s
18.34 / 79.28 / 52.681 s

General
- Home
- Documentation
- Search: kaputt.debrecen3

Status
- Tactical Overview
- Host Detail
- Service Detail
- Hostgroup Overview
- Hostgroup Summary
- Servicegroup Overview
- Servicegroup Summary
- Status Map

Problems
- Service Problems
- Unhandled Services
- Host Problems
- Unhandled Hosts
- All Unhandled Problems
- All Problems
- Network Outages

System
- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue

Host	Service	Status	Last Check	Duration	Attempt	Status Information
kaputt.debrecen3	Arbor BGP check	OK	2018-09-11 08:23:32	9d 2h 7m 5s	1/3	OK arbor peering
	HBONE BMP archivation check	OK	2018-09-11 08:25:16	0d 1h 19m 6s	1/3	OK bmp archive
	IPv4 BGP AS visibility check	OK	2018-09-11 08:21:34	5d 23h 0m 29s	1/3	OK prefix visibility
	IPv4 address hijack	OK	2018-09-11 08:23:39	5d 22h 59m 53s	1/3	OK ipv4 address hijack
	IPv6 BGP AS visibility check	OK	2018-09-11 08:26:28	9d 2h 7m 43s	1/3	OK prefix visibility
	IPv6 address hijack	OK	2018-09-11 08:21:36	9d 2h 7m 25s	1/3	OK ipv6 address hijack
	NREN POP count check	CRITICAL	2018-09-11 08:23:53	6d 13h 1m 58s	3/3	ERROR 1 nren pop(s) changed - kaputt.debrecen3#sho ipv4 bgp 65533 unicast database
	NREN POP using IPv4 L3VPN	CRITICAL	2018-09-11 08:26:34	4d 20h 42m 20s	3/3	ERROR 1 prefix(es) changed - kaputt.debrecen3#sho ipv4 bgp 65532 vpnuni database
	NREN POP using IPv6 L3VPN	OK	2018-09-11 08:21:42	9d 2h 7m 25s	1/3	OK geant vpnv6
	NREN POP using L2VPN	CRITICAL	2018-09-11 08:21:47	4d 0h 8m 37s	3/3	ERROR 4 prefix(es) changed - kaputt.debrecen3#sho ipv4 bgp 65532 vpls database
	PING_IPv4	OK	2018-09-11 08:21:47	9d 2h 9m 3s	1/3	PING OK - Packet loss = 0%, RTA = 15.60 ms
	RR BGP peer check	OK	2018-09-11 08:24:07	0d 20h 36m 0s	1/3	OK rr peering
	RTBH check	CRITICAL	2018-09-11 08:23:54	5d 8h 24m 7s	3/3	ERROR 2 prefix(es) changed - kaputt.debrecen3#sho ipv4 bgp 65534 unicast database
	Sulinet BGP check	CRITICAL	2018-09-11 08:22:28	0d 0h 21m 45s	3/3	ERROR 41 peering change(s) detected - kaputt.debrecen3#sho bmp sulinet
	eBGP peer check	WARNING	2018-09-11 08:22:00	0d 0h 22m 30s	3/3	ERROR 4 peering change(s) detected - kaputt.debrecen3#sho bmp bmp
	iBGP peer check	OK	2018-09-11 08:26:05	4d 10h 7m 38s	1/3	OK ibgp peering

Page 1 of 1 Results: 50

Displaying Result 1 - 16 of 16 Matching Services

Service Information

Last Updated: Tue Sep 11 08:28:40 CEST 2018 - Update in 83 seconds [pause]
Icinga Classic UI **1.11.6** (Backend **1.11.6**) - Logged in as *matecs@niif.hu*

- View **Information** For **This Host**
- View **Service Status Detail** For **This Host**
- View **Alert History** For **This Service**
- View **Trends** For **This Service**
- View **Alert Histogram** For **This Service**
- View **Availability Report** For **This Service**
- View **Notifications** For **This Service**
- View **Scheduling Queue** For **This Service**

Service
NREN POP count check

On Host
kaputt.debrecen3.hbone.hu

(kaputt.debrecen3)

Member of
No servicegroups.

Service Dependencies

195.111.100.70, 2001:738::179:70

Service State Information

Current Status:	CRITICAL (for 6d 13h 2m 31s)
Status Information:	ERROR 1 nren pop(s) changed - kaputt.debrecen3#sho ipv4 bgp 65533 unicast database - 193.191.20.149/32;62.40.102.26;255/100/0/0;20965 2611 65432
Performance Data:	
Current Attempt:	3/3 (HARD state)
Last Check Time:	2018-09-11 08:23:53
Check Type:	ACTIVE
Check Source / Reachability:	N/A
Check Latency / Duration:	36.906 / 0.162 seconds
Next Scheduled Active Check:	2018-09-11 08:30:53
Last State Change:	2018-09-04 19:26:09
Last Notification:	2018-09-04 19:30:26 (notification 1)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	2018-09-11 08:28:21 (0d 0h 0m 19s ago)

Service Commands

- Disable active checks of this service
- Re-schedule the next check of this service
- Submit passive check result for this service
- Stop accepting passive checks for this service
- Start obsessing over this service
- Acknowledge this service problem
- Disable notifications for this service
- Delay next service notification
- Send custom service notification
- Schedule downtime for this service
- Disable event handler for this service
- Disable flap detection for this service
- Add a new Service comment
- Reset Modified Attributes

BGP Monitoring - Summary and references

- BGPmon protocol – opportunity
- Freertr extended for BMP and NRPE server functionality
- More info on implementation:
  - http://freerouter.nop.hu/present.html
  - http://freerouter.nop.hu/
- More on BMP
  - https://tools.ietf.org/html/rfc7854

Thank you, Questions?

www.kifu.gov.hu

Every show command could be exported by nrpe

Every bmp session could be fed to bgp

KIFÜ

A MAGYARORSZÁGI **DIGITALIZÁCIÓ** SZOLGÁLATÁBAN