

2018 05 15:22:00 (+00:00)

Time Range

2018 05 15:21:59 (+00:00)

## 1. Device.ip with multiple Device.types

Devices that have multiple parsers acting on them over this time period, sorted most parsers per IP to least

Action:

- Review the list, make sure that the correct parsers are detected for the device.
- Review for combinations that should not occur especially those related to rhlinux devices.
- Reduce the number of parsers that are enabled on log decoder to minimum required (this will reduce the number of false mappings)
- For those that need to be forced to one or more parsers, leverage the device mapping function in 11.x or the device table on log decoders for 10.6.x-pre to force the correct parser mappings (order is important when using the parser mappings)
- 10.4.x - <https://community.rsa.com/docs/DOC-46080>
- 10.6.x- <https://community.rsa.com/docs/DOC-83616>
- 11.x- <https://community.rsa.com/docs/DOC-79854>

### LOGHEALTH04-Multi-Devicetype /nw11head - Broker

	Device IP	countdistinct(device.type)	distinct(device.type)
1	127.0.0.1	2	rhlinux unknown
2	192.168.254.183	2	rsasecurityanalytics unknown
3	192.168.254.186	2	rhlinux rsasecurityanalytics
4	192.168.254.188	2	rsasecurityanalytics unknown
5	192.168.254.189	2	rsasecurityanalytics unknown
6	192.168.254.1	1	pfsense23
7	192.168.254.12	1	rhlinux
8	192.168.254.13	1	windows
9	192.168.254.154	1	rsaacesrv
10	192.168.254.168	1	rsaecat
11	192.168.254.180	1	rsasecurityanalytics
12	192.168.254.181	1	rsasecurityanalytics_uax
13	192.168.254.182	1	rsasecurityanalytics
14	192.168.254.184	1	rsasecurityanalytics

[Back to top](#)

## 2. Unknown Devices

Unknown devices do not have a parser detected for them or no parser is installed/enabled for it.

Action:

- Determine the type of device from the raw log capture in netwitness (look for tokens or indications of what type of device it might be)
- Review the RSA Github site for log parsers to see if you can search for the tokens that are in the raw log to locate potential parsers if still unknown - <https://github.com/netwitness/nw-logparsers>
- Locate the parser in RSA live to make sure the current parser is subscribed and deployed to the log decoders
- Make sure the log parser is enabled on the decoder (checkbox set)
- Review to make sure any changes take effect from the point of install forward
- 10.6-pre - consider creating a new parser for the device with LTP 1.0 tool - <https://community.rsa.com/docs/DOC-85208>
- 11.x - is the device extracting meta with the tokens file for well known data (hostname, ip, url, ports) or only word meta?
- 11.x - if data is extracted using tokens then consider if parser is required
- 11.x - if data is only in word meta, Consider the LPT 1.0 tool to create a parser for the device.

### LOGHEALTH01-unknown-chart /nw11head - Broker

	Device IP	Total events count
1	127.0.0.1	498
2	192.168.254.189	45
3	192.168.254.183	35
4	192.168.254.188	1

[Back to top](#)

## 3. Device.type with word meta

Device types with word meta indicate that a parser has matched a header for that device but no payload (message body) has matched a parser entry.

Action:

- Review the device mapping for that device to make sure that the right parsers exist for that IP (potentially old device.ip that switched from linux server to windows server and mapping is incorrect)
- Review the device to see if this is a new message body for an existing header for the device, consider creating a -custom.xml parser for that device to include the new messages and submit via RSA Github or support case
- custom cef - <https://community.rsa.com/docs/DOC-79189>
- custom log parser - <https://community.rsa.com/docs/DOC-83425>

### LOGHEALTH02-word-chart /nw11head - Broker

	Device Type	Total events count
1	rsasecurityanalytics	75132
2	rhlinux	150

[Back to top](#)

## 4. Device.type with parseerror

### LOGHEALTH03-parseerror-chart /nw11head - Broker

	Device Type	Total events count
1	rhlinux	11680
2	pfsense23	6
3	rsaecat	5

[Back to top](#)