

Title: Tuncate IP addresses Description: GDPR, anonymize IP addresses, log anonymizer, truncate IP addresses

Output filter: ip-truncate-fields

This plugin replaces IP addresses with an anonymized string, replacing the last block of an IP address with “0”.

Example (client_ip field):

- IPv4: 192.168.1.22 -> 192.168.1.0
- IPv6: 2001:db8:0:0:0:ff00:42:8329 -> 2001:db8:0:0:0:ff00:42:0

All occurrences of the IP address are replaced in the log “message” fields with the new value.

Example (message field): “Client connect 192.168.1.22” -> “Client connect 192.168.1.0”

In the context of data protection regulations like GDPR, you might need to mask data fields, especially when you handover log data to 3rd parties.

For a stronger protection check other output plugins:

- aes-encrypt-fields
- hash-fields
- remove-fields

Configuration

Add the following section ‘outputFilter’ to the Logagent configuration file. Please note you could use the plugin with multiple configurations for different event sources.

```
# tail web server logs
input:
  files:
    - '/var/log/*/access_log'

# log agent parses web server logs out of the box ...
outputFilter:
  iptruncate:
    module: ip-truncate-fields
    # JS regular expression to match log source name
    matchSource: !!js/regexp access_log
    fields:
      - client_ip
```

Run Logagent with your config:

```
logagent --config logagent-example-config.yml -n httpd --yaml
```

The output replaced IP '::1' with '::0':

```
logSource:    httpd
_type:        access_common
client_ip:    ::0
remote_id:    -
user:         null
method:       GET
path:         /
http_version: HTTP/1.1
status_code:  304
size:         0
@timestamp:   Thu Apr 26 2018 22:02:26 GMT+0200 (CEST)
```