Title: Encrypt fields with AES Description: Aes-encrypt-fields plugin for Logagent used to encrypt data fields with AES. Use log anonymizer to ensure GDPR compliance for masking data fields, and encrypt your search term and search the encrypted term in Elasticsearch to find relevant log entries with our logging management SaaS

Output filter: aes-encrypt-fields

This plugin encrypts data fields with AES. The original field value gets replaced with its AES encrypted HEX string. All occurrences of the original field value are replaced in the log "message" field with the encrypted value.

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.

AES is a symetric encryption, which means you could decrypt the data using the same password. The encryption key can be entered into Logagent configuration in the "password" property. Node.js crypto implementation is based on openssl and therefore various AES cyphers can be used.

Encrypting the same text with the same password results in the same encrypted text. This could be helpful when you need to search for specific encrypted field value. You could encrypt your search term and search the encrypted term in Elasticsearch to find relevant log entries.

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 webs erver logs
input:
  files:
    - '/var/log/*/access.log'

# log agent parses web server logs out of the box ...
# output filter to encrypt client_ip and user field in web server logs
outputFilter:
  aes:
    module: aes-encrypt-fields
    # JS regular expression to match log source name
    matchSource: !!js/regexp access.log
    fields:
      - client_ip
      - user
    password: "Top secret!"
    # algorithms supported by nodejs crypto module, e.g. aes-128-cbc, aes-128-ecb, aes-192-
```

```
    # aes-192-ecb, aes-256-cbc, aes-256-ecb
    # short names might work as well e.g. "aes256"
    # default value is aes256
    algorithm: aes-256-ecb
```

Run Logagent with your config:

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