Graylog

- Graylog - Konfiguration

Graylog - Konfiguration

Default Login

Der default User ist "admin".

Es wird scheinbar nur das default Passwort "admin" als sha256 hash akzeptiert.

So muss die Zeile in der config aussehen: `root_password_sha2 = 8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918`

Ich habe es mit anderen Passwörtern versucht aber bekam dann nach Neustart des Graylogs nur die Fehlermeldung beim Login "Invalid Credentials".

Ebenfalls scheint es nicht zu funktionieren anstelle des HASH Wertes ein Kommando zur Ausgabe dessen zu benutzen.

Ich hatte das hier versucht:

```
root_password_sha2 = `cat $workdir/root_password_sha2`
```

Das funktionierte nur nicht, obwohl ein Test auf der bash tadellos funktioniert.

Einstellen der Adressen, die Graylog benutzen soll

Da Graylog für mich neu war, habe ich mir Docs durchgelesen und befolgt aber war damit nicht erfolgreich. Also las ich einige Docs und Anleitungen aus Communities bis ich dann die entscheidenden Einstellungen fand, die mir den Erfolg brachten.

Man muss scheinbar lediglich folgende "URI´s" einstellen:

Die default Zeilen kommentiere ich immer aus.

```
#rest_listen_uri = http://127.0.0.1:9000/api/
rest_listen_uri = http://192.168.10.10:9000/api/
```

```
#web_listen_uri = http://127.0.0.1:9000/
web_listen_uri = http://192.168.10.10:9000/
```

Damit funktionierte es dann bei mir.

Beispielkonfiguration

```
root@srvgl01:/etc/graylog# cat /etc/graylog/server/server.conf
workdir=/etc/graylog
is_master = true

node_id_file = /etc/graylog/server/node-id

password_secret = ${workdir}/server/password-secret
root_username = admin
root_password_sha2 = DEIN-SHA2-root-Schnipsel
root_timezone = Europe/Berlin

plugin_dir = /usr/share/graylog-server/plugin

rest_listen_uri = http://192.168.1.11:9000/api/
rest_transport_uri = http://192.168.1.11:9000/api/

web_enable = true
web_listen_uri = http://192.168.1.11:9000/
#web_endpoint_uri = http://192.168.1.10:80/api/

elasticsearch_hosts = http://192.168.1.21:9200

rotation_strategy = count
elasticsearch_max_docs_per_index = 20000000
elasticsearch_max_number_of_indices = 20
retention_strategy = delete

elasticsearch_shards = 4
elasticsearch_replicas = 0
elasticsearch_index_prefix = graylog
allow_leading_wildcard_searches = false
allow_highlighting = false
elasticsearch_analyzer = standard

output_batch_size = 500
output_flush_interval = 1
output_fault_count_threshold = 5
output_fault_penalty_seconds = 30
```

```
processbuffer_processors = 5
outputbuffer_processors = 3
processor_wait_strategy = blocking
ring_size = 65536

inputbuffer_ring_size = 65536
inputbuffer_processors = 2
inputbuffer_wait_strategy = blocking

message_journal_enabled = true
message_journal_dir = /var/lib/graylog-server/journal

lb_recognition_period_seconds = 3

mongodb_uri =
mongodb://192.168.1.11:27017,192.168.1.12:27017,192.168.1.13:27017/graylog?replicaSet=graylog
mongodb_max_connections = 1000
mongodb_threads_allowed_to_block_multiplier = 5

content_packs_dir = /usr/share/graylog-server/contentpacks
content_packs_auto_load = grok-patterns.json
proxied_requests_thread_pool_size = 32
```