Verwalten von Elastic

- Logs löschen

Logs löschen

Beschreibung:

Es gibt Situationen da möchte man logs löschen.
Entweder von einem Zeitraum oder ganz bestimmte, oder einfach alles.
genau wie Logs nach einem angegben Zeitraum löschen.

Die Varianten

- Alle Logs löschen:

  ```
  curl -X DELETE "localhost:9200/_all"
  Ausgabe:
  curl: (52) Empty reply from server
  ```

- Mit Wildcard. Es wird immer der Indexname genommen, der in logtash angegben wurde.

  ```
  curl -X DELETE "localhost:9200/syslog-*"
  ```

- Oder explizit mit Datum :

  ```
  curl -X DELETE "localhost:9200/syslogs-2023_06_19"
  ```

Logs nach einem Datum löschen:

Es können policies angelgt werden nach dem die Logs gelöscht werden soll.
Dies geht über das Terminal mit einem curl Befehl.
In unerem Beispiel heißt die Policy 30days,

Min age und max age bekommen den Wert 30 Tage

Der Befehl

```
curl -X PUT "localhost:9200/_ilm/policy/30days" -H 'Content-Type: application/json' -d'
{
  "policy": {
    "phases": {
      "hot": {
        "min_age": "0ms",
```

```
      "actions": {
        "rollover": {
          "max_age": "30d"
        }
      }
    },
    "delete": {
      "min_age": "30d",
      "actions": {
        "delete": {}
      }
    }
  }
 }
}
'
```

Nun haben wir eine Policy erstellt.
Diese müssen wir noch auf unseren Index ausrollen.
Der index wurde in der logtash festgelegt.