# Allgemeines

|  |  |  |
| --- | --- | --- |
| *forwarder executable directory* | /opt/logstash-forwarder/bin |  |
| *fowarder config file* | /etc/logstash-forwarder.conf |  |
| *forwarder logs* | /var/log/logstash-forwarder/logstash-forwarder.err/.log |  |
| *forwarder service* | service logstash-forwarder (start/stop/status/restart) |  |
| *forwarder offset file* | /var/lib/logstash-forwarder/.logstash-forwarder |  |
| *logstash server url:port* | log.services.emea.dir:15102 |  |

# Zurücksetzen des Offsets für Log-Dateien

Der logstash-forwarder merkt sich für jedes Logfile die Position, an der er zuletzt Daten eingelesen hat, als „Offset“ in einer Datei.

* Soll **eine** Log-Datei erneut eingelesen werden, so ist im *forwarder offset file* die gewünschte Datei zu suchen und der Wert für „offset“ auf 0 zurückzusetzen. Anschließend den Service restarten.
* Sollen **alle** Log-Dateien erneut vollständig eingelesen werden, so kann das *forwarder offset file* gelöscht werden. Anschließend den Service restarten.

# Hinzufügen weiterer Log-Dateien zur Überwachung

Sollen weitere Log-Dateien überwacht und an Logstash gesendet werden, so muss das *forwarder config file* angepasst werden.

* Besteht ein File mit **gleicher Syntax/Funktion**, so kann die neue Datei unter „paths“ einfach hinzugefügt werden
* Soll ein **neuer Typ von Log-Datei** hinzugefügt werden, so ist im Block „files“ ein neues Element einzufügen.

Ein solcher Block besteht aus folgenden Elementen:

paths – Liste aller Logfiles, die gemeinsam überwacht werden

dead time (opt) – Höchstes Alter der Dateien, die berücksichtigt werden

fields – Hier wird festgelegt, als welcher Typ die Ereignisse verarbeitet werden

* Achtung! Unbedingt immer auf korrekte Kommas und Klammern achten!