Syslog-Client Dokumentation

Der Syslog-Client kann als Kommandozeilen-Programm gestartet werden und benötigt dafür folgende 5 Kommandozeilenparameter:

1. „Facility“ für die PRI. Hierfür kann entweder direkt der numerische Code der einzelnen Facilities eingegeben werden oder auch der exakte String, wie er in der Dokumentation des Syslog-Protokolls nach RFC 5424 steht. Die exakten Strings können hier in der Dokumentation des Syslog-Protokolls auf Seite 10 entnommen werden.
   Bsp. : „6“ oder „line printer subsystem“ ergeben beide den numerischen Code 6 für die Facility.
2. „Severity“ für die PRI. Hierfür kann wie bei der Facility direkt der numerische Code oder der String für die Severity angegeben werden. Die exakten Strings können hier in der Dokumentation des Syslog-Protokolls auf Seite 11 nachgelesen werden. Für den Syslog-Client muss nur der Teil vor dem Doppelpunkt angegeben werden. Also statt „Alert: action must be taken immediately“ nur „Alert“.
   Bsp.: „2“ oder „Critical“ ergeben beide den numerischen Code 2 für die Severity.
3. „APPNAME“. Der App-Name für den Syslog-Client kann vom Nutzer selbst gewählt werden. Bei leerem String ("") wird Nilvalue ("-") verwendet.
4. „MSGID“. Die „MSGID“ kann auch vom Nutzer beliebig für den Syslog-Client gewählt werden. Bei leerem String ("") wird Nilvalue ("-") verwendet.
5. Die zu loggende Nachricht.

Beispiel Ausführungen des Syslog-Clients mit den Kommandozeilenparametern:

java SyslogClient.java 3 4 MyApp ID10 "Das ist meine Nachricht"

Die Facility ist 3 (system daemons) und die Severity 4 (Warning). Als App-Name wird „MyApp“ verwendet und die MSGID ist „ID10“. Die zu loggende Nachricht ist „Das ist meine Nachricht“

java SyslogClient.java "mail system" "Emergency" "Logging-App" "" "Eine Nachricht"

Die Facility ist 2 (mail system) und die Severity 0 (Emergency). Als App-Name wird „Logging-App“ verwendet. Als MSGID wird hier der leere String verwendet, weshalb die MSGID Nilvalue ("-") wird. Die zu loggende Nachricht ist „Eine Nachricht“.

Anmerkungen zu den Bestandteilen der Syslog-Nachricht

HEADER

1. „PRI“: wird automatisch anhand der ersten beiden Kommandozeilenparameter „Facility“ und „Severity“ berechnet und erstellt.
2. „Version“: Der Syslog-Client orientiert sich an Version 1 der Dokumentation, weshalb auch Version 1 in der Syslog-Nachricht verwendet wird.
3. „Timestamp“: Wenn die Syslog-Nachricht erstellt wird, wird der Timestamp im Programm automatisch ermittelt.
4. „Hostname“: Der Hostname wird im Programm automatisch ermittelt. Wenn dies nicht möglich ist, wird versucht die IP automatisch zu ermitteln. Falls beides fehlschlägt, was sehr unwahrscheinlich ist, wird Nilvalue ("-") verwendet.
5. „APPNAME“: Dritter Kommandozeilenparameter und vom Nutzer frei wählbar.
6. „PROCID“: Im Programm wird die die aktuelle ProzessID herausgefunden und als PROCID verwendet.
7. „MSGID“: Vierter Kommandozeilenparameter und vom Nutzer frei wählbar.

STRUCTURED-DATA

Structured-Data sollte in der Aufgabenstellung nicht beachtet werden, weshalb für den Structured-Data Teil in der Syslog-Nachricht Nilvalue ("-") gesendet wird.

MSG

Fünfter Kommandozeilenparameter, der die zu loggende Nachricht enthält.