# Downloaded from: https://raw.githubusercontent.com/logstash-plugins/logstash-patterns-core/master/patterns/grok-patterns

USERNAME [a-zA-Z0-9.\_-]+

USER %{USERNAME}

EMAILLOCALPART [a-zA-Z][a-zA-Z0-9\_.+-=:]+

EMAILADDRESS %{EMAILLOCALPART}@%{HOSTNAME}

HTTPDUSER %{EMAILADDRESS}|%{USER}

INT (?:[+-]?(?:[0-9]+))

BASE10NUM (?<![0-9.+-])(?>[+-]?(?:(?:[0-9]+(?:\.[0-9]+)?)|(?:\.[0-9]+)))

NUMBER (?:%{BASE10NUM})

BASE16NUM (?<![0-9A-Fa-f])(?:[+-]?(?:0x)?(?:[0-9A-Fa-f]+))

BASE16FLOAT \b(?<![0-9A-Fa-f.])(?:[+-]?(?:0x)?(?:(?:[0-9A-Fa-f]+(?:\.[0-9A-Fa-f]\*)?)|(?:\.[0-9A-Fa-f]+)))\b

POSINT \b(?:[1-9][0-9]\*)\b

NONNEGINT \b(?:[0-9]+)\b

WORD \b\w+\b

NOTSPACE \S+

SPACE \s\*

DATA .\*?

GREEDYDATA .\*

QUOTEDSTRING (?>(?<!\\)(?>"(?>\\.|[^\\"]+)+"|""|(?>'(?>\\.|[^\\']+)+')|''|(?>`(?>\\.|[^\\`]+)+`)|``))

UUID [A-Fa-f0-9]{8}-(?:[A-Fa-f0-9]{4}-){3}[A-Fa-f0-9]{12}

# Networking

MAC (?:%{CISCOMAC}|%{WINDOWSMAC}|%{COMMONMAC})

CISCOMAC (?:(?:[A-Fa-f0-9]{4}\.){2}[A-Fa-f0-9]{4})

WINDOWSMAC (?:(?:[A-Fa-f0-9]{2}-){5}[A-Fa-f0-9]{2})

COMMONMAC (?:(?:[A-Fa-f0-9]{2}:){5}[A-Fa-f0-9]{2})

IPV6 ((([0-9A-Fa-f]{1,4}:){7}([0-9A-Fa-f]{1,4}|:))|(([0-9A-Fa-f]{1,4}:){6}(:[0-9A-Fa-f]{1,4}|((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){5}(((:[0-9A-Fa-f]{1,4}){1,2})|:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3})|:))|(([0-9A-Fa-f]{1,4}:){4}(((:[0-9A-Fa-f]{1,4}){1,3})|((:[0-9A-Fa-f]{1,4})?:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){3}(((:[0-9A-Fa-f]{1,4}){1,4})|((:[0-9A-Fa-f]{1,4}){0,2}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){2}(((:[0-9A-Fa-f]{1,4}){1,5})|((:[0-9A-Fa-f]{1,4}){0,3}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(([0-9A-Fa-f]{1,4}:){1}(((:[0-9A-Fa-f]{1,4}){1,6})|((:[0-9A-Fa-f]{1,4}){0,4}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:))|(:(((:[0-9A-Fa-f]{1,4}){1,7})|((:[0-9A-Fa-f]{1,4}){0,5}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))|:)))(%.+)?

IPV4 (?<![0-9])(?:(?:[0-1]?[0-9]{1,2}|2[0-4][0-9]|25[0-5])[.](?:[0-1]?[0-9]{1,2}|2[0-4][0-9]|25[0-5])[.](?:[0-1]?[0-9]{1,2}|2[0-4][0-9]|25[0-5])[.](?:[0-1]?[0-9]{1,2}|2[0-4][0-9]|25[0-5]))(?![0-9])

IP (?:%{IPV6}|%{IPV4})

HOSTNAME \b(?:[0-9A-Za-z][0-9A-Za-z-]{0,62})(?:\.(?:[0-9A-Za-z][0-9A-Za-z-]{0,62}))\*(\.?|\b)

IPORHOST (?:%{IP}|%{HOSTNAME})

HOSTPORT %{IPORHOST}:%{POSINT}

# paths

PATH (?:%{UNIXPATH}|%{WINPATH})

UNIXPATH (/([\w\_%!$@:.,~-]+|\\.)\*)+

TTY (?:/dev/(pts|tty([pq])?)(\w+)?/?(?:[0-9]+))

WINPATH (?>[A-Za-z]+:|\\)(?:\\[^\\?\*]\*)+

URIPROTO [A-Za-z]+(\+[A-Za-z+]+)?

URIHOST %{IPORHOST}(?::%{POSINT:port})?

# uripath comes loosely from RFC1738, but mostly from what Firefox

# doesn't turn into %XX

URIPATH (?:/[A-Za-z0-9$.+!\*'(){},~:;=@#%\_\-]\*)+

#URIPARAM \?(?:[A-Za-z0-9]+(?:=(?:[^&]\*))?(?:&(?:[A-Za-z0-9]+(?:=(?:[^&]\*))?)?)\*)?

URIPARAM \?[A-Za-z0-9$.+!\*'|(){},~@#%&/=:;\_?\-\[\]<>]\*

URIPATHPARAM %{URIPATH}(?:%{URIPARAM})?

URI %{URIPROTO}://(?:%{USER}(?::[^@]\*)?@)?(?:%{URIHOST})?(?:%{URIPATHPARAM})?

# Months: January, Feb, 3, 03, 12, December

MONTH \b(?:Jan(?:uary|uar)?|Feb(?:ruary|ruar)?|M(?:a|ä)?r(?:ch|z)?|Apr(?:il)?|Ma(?:y|i)?|Jun(?:e|i)?|Jul(?:y)?|Aug(?:ust)?|Sep(?:tember)?|O(?:c|k)?t(?:ober)?|Nov(?:ember)?|De(?:c|z)(?:ember)?)\b

MONTHNUM (?:0?[1-9]|1[0-2])

MONTHNUM2 (?:0[1-9]|1[0-2])

MONTHDAY (?:(?:0[1-9])|(?:[12][0-9])|(?:3[01])|[1-9])

# Days: Monday, Tue, Thu, etc...

DAY (?:Mon(?:day)?|Tue(?:sday)?|Wed(?:nesday)?|Thu(?:rsday)?|Fri(?:day)?|Sat(?:urday)?|Sun(?:day)?)

# Years?

YEAR (?>\d\d){1,2}

HOUR (?:2[0123]|[01]?[0-9])

MINUTE (?:[0-5][0-9])

# '60' is a leap second in most time standards and thus is valid.

SECOND (?:(?:[0-5]?[0-9]|60)(?:[:.,][0-9]+)?)

TIME (?!<[0-9])%{HOUR}:%{MINUTE}(?::%{SECOND})(?![0-9])

# datestamp is YYYY/MM/DD-HH:MM:SS.UUUU (or something like it)

DATE\_US %{MONTHNUM}[/-]%{MONTHDAY}[/-]%{YEAR}

DATE\_EU %{MONTHDAY}[./-]%{MONTHNUM}[./-]%{YEAR}

ISO8601\_TIMEZONE (?:Z|[+-]%{HOUR}(?::?%{MINUTE}))

ISO8601\_SECOND (?:%{SECOND}|60)

TIMESTAMP\_ISO8601 %{YEAR}-%{MONTHNUM}-%{MONTHDAY}[T ]%{HOUR}:?%{MINUTE}(?::?%{SECOND})?%{ISO8601\_TIMEZONE}?

DATE %{DATE\_US}|%{DATE\_EU}

DATESTAMP %{DATE}[- ]%{TIME}

TZ (?:[PMCE][SD]T|UTC)

DATESTAMP\_RFC822 %{DAY} %{MONTH} %{MONTHDAY} %{YEAR} %{TIME} %{TZ}

DATESTAMP\_RFC2822 %{DAY}, %{MONTHDAY} %{MONTH} %{YEAR} %{TIME} %{ISO8601\_TIMEZONE}

DATESTAMP\_OTHER %{DAY} %{MONTH} %{MONTHDAY} %{TIME} %{TZ} %{YEAR}

DATESTAMP\_EVENTLOG %{YEAR}%{MONTHNUM2}%{MONTHDAY}%{HOUR}%{MINUTE}%{SECOND}

HTTPDERROR\_DATE %{DAY} %{MONTH} %{MONTHDAY} %{TIME} %{YEAR}

# Syslog Dates: Month Day HH:MM:SS

SYSLOGTIMESTAMP %{MONTH} +%{MONTHDAY} %{TIME}

PROG [\x21-\x5a\x5c\x5e-\x7e]+

SYSLOGPROG %{PROG:program}(?:\[%{POSINT:pid}\])?

SYSLOGHOST %{IPORHOST}

SYSLOGFACILITY <%{NONNEGINT:facility}.%{NONNEGINT:priority}>

HTTPDATE %{MONTHDAY}/%{MONTH}/%{YEAR}:%{TIME} %{INT}

# Shortcuts

QS %{QUOTEDSTRING}

# Log formats

SYSLOGBASE %{SYSLOGTIMESTAMP:timestamp} (?:%{SYSLOGFACILITY} )?%{SYSLOGHOST:logsource} %{SYSLOGPROG}:

COMMONAPACHELOG %{IPORHOST:clientip} %{HTTPDUSER:ident} %{USER:auth} \[%{HTTPDATE:timestamp}\] "(?:%{WORD:verb} %{NOTSPACE:request}(?: HTTP/%{NUMBER:httpversion})?|%{DATA:rawrequest})" %{NUMBER:response} (?:%{NUMBER:bytes}|-)

COMBINEDAPACHELOG %{COMMONAPACHELOG} %{QS:referrer} %{QS:agent}

HTTPD20\_ERRORLOG \[%{HTTPDERROR\_DATE:timestamp}\] \[%{LOGLEVEL:loglevel}\] (?:\[client %{IPORHOST:clientip}\] ){0,1}%{GREEDYDATA:errormsg}

HTTPD24\_ERRORLOG \[%{HTTPDERROR\_DATE:timestamp}\] \[%{WORD:module}:%{LOGLEVEL:loglevel}\] \[pid %{POSINT:pid}:tid %{NUMBER:tid}\]( \(%{POSINT:proxy\_errorcode}\)%{DATA:proxy\_errormessage}:)?( \[client %{IPORHOST:client}:%{POSINT:clientport}\])? %{DATA:errorcode}: %{GREEDYDATA:message}

HTTPD\_ERRORLOG %{HTTPD20\_ERRORLOG}|%{HTTPD24\_ERRORLOG}

# Log Levels

LOGLEVEL ([Aa]lert|ALERT|[Tt]race|TRACE|[Dd]ebug|DEBUG|[Nn]otice|NOTICE|[Ii]nfo|INFO|[Ww]arn?(?:ing)?|WARN?(?:ING)?|[Ee]rr?(?:or)?|ERR?(?:OR)?|[Cc]rit?(?:ical)?|CRIT?(?:ICAL)?|[Ff]atal|FATAL|[Ss]evere|SEVERE|EMERG(?:ENCY)?|[Ee]merg(?:ency)?)