rsyslog.com

RSyslog Documentation - rsyslog

8-10 minutes

---

rsyslog Properties¶

Data items in rsyslog are called “properties”. They can have different origin. The most important ones are those that stem from received messages. But there are also others. Whenever you want to access data items, you need to access the respective property.

Properties are used in

- templates
- conditional statements

The property name is case-insensitive (prior to 3.17.0, they were case-sensitive).

Note: many users refer to “rsyslog properties” as “rsyslog variables”. You can treat them as synonymous. Read how rsyslog lead author Rainer Gerhards explains the naming difference.

Message Properties¶

These are extracted by rsyslog parsers from the original message. All message properties start with a letter.

The following message properties exist:

msg

the MSG part of the message (aka “the message” ;))

rawmsg

the message “as is”. Should be useful for debugging and also if a message should be forwarded totally unaltered. Please notice *EscapecontrolCharactersOnReceive* is enabled by default, so it may be different from what was received in the socket.

rawmsg-after-pri

Almost the same as **rawmsg**, but the syslog PRI is removed. If no PRI was present, **rawmsg-after-pri** is identical to **rawmsg**. Note that the syslog PRI is header field that contains information on syslog facility and severity. It is enclosed in greater-than and less-than characters, e.g. “<191>”. This field is often not written to log files, but usually needs to be present for the receiver to properly classify the message. There are some rare cases where one wants the raw message, but not the PRI. You can use this property to obtain that. In general, you should know that you need this format, otherwise stay away from the property.

hostname

hostname from the message

source

alias for HOSTNAME

fromhost

hostname of the system the message was received from (in a relay chain, this is the system immediately in front of us and not necessarily the original sender). This is a DNS-resolved name, except if that is not possible or DNS resolution has been disabled.

fromhost-ip

The same as fromhost, but always as an IP address. Local inputs (like imklog) use 127.0.0.1 in this property.

syslogtag

TAG from the message

programname

the “static” part of the tag, as defined by BSD syslogd. For example, when TAG is “named[12345]”, programname is “named”.

Precisely, the programname is terminated by either (whichever occurs first):

- end of tag
- nonprintable character
- ‘:’
- ‘[‘
- ‘/’

The above definition has been taken from the FreeBSD syslogd sources.

Please note that some applications include slashes in the static part of the tag, e.g. “app/foo[1234]”. In this case, programname is “app”. If they store an absolute path name like in “/app/foo[1234]”, programname will become empty (“”). If you need to actually store slashes as part of the programname, you can use the global option

global(parser.permitSlashInProgramName=”on”)

to permit this. Then, a syslogtag of “/app/foo[1234]” will result

in programname being “/app/foo”. Note: this option is available starting at rsyslogd version 8.25.0.

pri

PRI part of the message - undecoded (single value)

pri-text

the PRI part of the message in a textual form with the numerical PRI appended in brackets (e.g. “local0.err<133>”)

iut

the monitorware InfoUnitType - used when talking to a MonitorWare backend (also for Adiscon LogAnalyzer)

syslogfacility

the facility from the message - in numerical form

syslogfacility-text

the facility from the message - in text form

syslogseverity

severity from the message - in numerical form

syslogseverity-text

severity from the message - in text form

syslogpriority

an alias for syslogseverity - included for historical reasons (be careful: it still is the severity, not PRI!)

syslogpriority-text

an alias for syslogseverity-text

timegenerated

timestamp when the message was RECEIVED. Always in high resolution

timereported

timestamp from the message. Resolution depends on what was provided in the message (in most cases, only seconds)

timestamp

alias for timereported

protocol-version

The contents of the PROTOCOL-VERSION field from IETF draft draft-ietf-syslog-protocol

structured-data

The contents of the STRUCTURED-DATA field from IETF draft draft-ietf-syslog-protocol

app-name

The contents of the APP-NAME field from IETF draft draft-ietf-syslog-protocol

procid

The contents of the PROCID field from IETF draft draft-ietf-syslog-protocol

msgid

The contents of the MSGID field from IETF draft draft-ietf-syslog-protocol

inputname

The name of the input module that generated the message (e.g. “imuxsock”, “imudp”). Note that not all modules necessarily provide this property. If not provided, it is an empty string. Also note that the input module may provide any value of its liking. Most importantly, it is **not** necessarily the module input name. Internal sources can also provide inputnames. Currently, “rsyslogd” is defined as inputname for messages internally generated by rsyslogd, for example startup and shutdown and error messages. This property is considered useful when trying to filter messages based on where they originated - e.g. locally generated messages (“rsyslogd”, “imuxsock”, “imklog”) should go to a different place than

messages generated somewhere else.

jsonmesg

> *Available since rsyslog 8.3.0*
>
> The whole message object as JSON representation. Note that the JSON string will *not* include an LF and it will contain *all other message properties* specified here as respective JSON containers. It also includes all message variables in the “$!” subtree (this may be null if none are present).
>
> This property is primarily meant as an interface to other systems and tools that want access to the full property set (namely external plugins). Note that it contains the same data items potentially multiple times. For example, parts of the syslog tag will by contained in the rawmsg, syslogtag, and programname properties. As such, this property has some additional overhead. Thus, it is suggested to be used only when there is actual need for it.

System Properties¶

These properties are provided by the rsyslog core engine. They are **not** related to the message. All system properties start with a dollar-sign.

Special care needs to be taken in regard to time-related system variables:

- `timereported` contains the timestamp that is contained within the message header. Ideally, it resembles the time when the message was created at the original sender. Depending on how long the message was in the relay chain, this can be quite old.

- `timegenerated` contains the timestamp when the message was received by the local system. Here “received” actually means the point in time when the message was handed over from the OS to rsyslog’s reception buffers, but before any actual processing takes place. This also means a message is “received” before it is placed into any queue. Note that depending on the input, some minimal processing like extraction of the actual message content from the receive buffer can happen. If multiple messages are received via the same receive buffer (a common scenario for example with TCP-based syslog), they bear the same `timegenerated` stamp because they actually were received at the same time.
- `$now` is **not** from the message. It is the system time when the message is being **processed**. There is always a small difference between `timegenerated` and `$now` because processing always happens after reception. If the message is sitting inside a queue on the local system, the time difference between the two can be some seconds (e.g. due to a message burst and in-memory queueing) up to several hours in extreme cases where a message is sitting inside a disk queue (e.g. due to a database outage). The `timereported` property is usually older than `timegenerated`, but may be totally different due to differences in time and time zone configuration between systems.

  The following system properties exist:

  $bom

  The UTF-8 encoded Unicode byte-order mask (BOM). This may be useful in templates for RFC5424 support, when the character set is know to be Unicode.

  $myhostname

The name of the current host as it knows itself (probably useful for filtering in a generic way)