

rsyslog 2027 - remote logging is broken

This is a RHEL + CentOS issue introduced by how the connector to systemd works.

The effect is well described here:

https://bugzilla.redhat.com/show_bug.cgi?id=1095784

I can't make anything of the comment

```
| The contents of /var/lib/rsyslog/imjournal.state are only manipulated through systemd API.
```

I mean, we care if our syslog is working, or not. Not those manipulating the file to a way that it'll later be unable to read it. Besides, reading of the PR shows any event that sets this file to 0 bytes will fry it.

The other case is if it has a wrong time pointer after a time correction: it will stop working again.

You'll find a corresponding message in `/var/log/messages`:

```
Sep 19 19:31:38 dhcp204 rsyslogd: [origin software="rsyslogd"
swVersion="7.4.7" x-pid="32097" x-info="http://www.rsyslog.com"] start
Sep 19 19:31:38 dhcp204 rsyslogd-2307: warning: ~ action is deprecated,
consider using the 'stop' statement instead [try
http://www.rsyslog.com/e/2307 ]
Sep 19 19:31:38 dhcp204 rsyslogd-2027: imjournal: fscanf on state file
`/var/lib/rsyslog/imjournal.state' failed
[try http://www.rsyslog.com/e/2027 ]
Sep 19 19:31:58 dhcp204 rsyslogd: [origin software="rsyslogd"
swVersion="7.4.7" x-pid="32097" x-info="http://www.rsyslog.com"] exiting on
signal 15.
```

And basically that'll be all it's logging!

The 2027 error is a generic file IO alert:

<http://kb.monitorware.com/kbeventdb-detail-id-7164.html>

Makes sense when it only gets to read 0 bytes of that file, right?

The more detailed story is in this bug report: https://bugzilla.redhat.com/show_bug.cgi?id=1088021

To verify

Check this:

1. You have an existing `/var/lib/rsyslog/imjournal.state` and it's possibly 0 bytes
2. You see your remote log only being used when you restart rsyslog, and all you see is the error messages. No other log traffic.

tcpdump example

```
tcpdump -nn -vv -i ens3 port 514
```

To fix

I've used the following script:

```
systemctl restart rsyslog
if journalctl --since="-1m" | grep -q http://www.rsyslog.com/e/2027 ; then
    systemctl stop rsyslog
    rm /var/lib/rsyslog/imjournal.state
    systemctl start rsyslog
fi
```

To monitor

I'm using a manual (not inventory based) check to alert if that file is ever created.

First, on the remote node in filewatch.cfg i'm setting up tracking of this file.

```
# cat /etc/check_mk/fileinfo.cfg
/var/log/messages
/var/log/httpd/*error*log
/var/log/apache/*error*log
/var/lib/rsyslog/imjournal.state
```

This is accompanied by a **manual** check, meaning it's enforced no matter if inventory sees that file.

New rule Size and age of single files

▼ Rule Options

Description A description or title of this rule

Comment An optional comment that explains the purpose of this rule.

Documentation-URL An optional URL pointing to documentation or any other page. This will be displayed as an icon and open a new page when clicked. You can use a relative to `check_mk/`.

Rule activation Disabled rules are kept in the configuration but are not applied.
 do not apply this rule

▼ Parameters

Checktype
Please choose the check plugin

File name
 Minimal age
 Maximal age
Warning if older than days hours mins secs
Critical if older than days hours mins secs

Parameters
 Minimal size
 Maximal size
 Only check during the following times of the day
 State when file is missing

I've not yet added the condition to the file size.

It seems this file can be around and larger than 0 bytes and things might still work.

Finally I also added an error condition on the rsyslog error to logwatch.cfg:

```
# grep -e messages -e rsyslog /etc/check_mk/logwatch.cfg
/var/log/messages
# C: Critical messages
# W: Warning messages
C rsyslogd-2027: imjournal: fscanf:
```

more things...

I think this file should be in `/var/spool/rsyslog`, not in `/var/lib/rsyslog`

The whole design is a clusterfuck. If you have some RedHat support, please put pressure on this bug.

The rsyslog docs actually tell you to NOT USE the imstate module.

I've later run into a rate limiting issue

See <http://stackoverflow.com/questions/33041593/centos-7-rsyslog-debug-logs-dropped-for-c-c-modules> for more info about this

And, for your amusement, this is what a fix looks like if you're using Rudder:

TECHNIQUE

Config syslog journald burst rate limits

Clone

Delete

General information

Name: Config syslog journald burst rate limits

Description: See <http://stackoverflow.com/questions/33041593/centos-7-rsyslog-debug-logs-dropped-for-c-c-modules> for more info about this

Bundle name: Config_syslog_journald_burst_rate_limits

Version: 1.0

File ensure lines present ⓘ

⋮ This is a bundle to ensure that one or more lines are present in a file
/etc/systemd/journald.conf

Service restart ⓘ

⋮ Restart a service using the appropriate method
systemd-journald

File copy from remote source ⓘ

⋮ This is a bundle to ensure that a file or directory is copied from a remote source
/etc/rsyslog.conf

Service reload ⓘ

⋮ Reload a service using the appropriate method
rsyslog

Which is no more than 22 lines of policy, including comments, and fixes even this issue.

Yay.

Directive	Status
Config syslog journald burst rate limits ⓘ	100%
Component	Status
File copy from remote source	100%
Value	Status
/etc/rsyslog.conf	100%
File ensure lines present	100%
Value	Status
/etc/systemd/journald.conf	100%
Service reload	100%
Service restart	100%
Config UID Range ⓘ	100%
Config Yum fine-tuning ⓘ	100%
Cron daemon configuration ⓘ	100%

