LastParser Design Support Doc

# Tags and RegExs

#### General fields

**<start-log>** = wrapper for start time

**<end-log>** = wrapper for end time

**<date>** = wrapper for date fields

**<year>**

* + *2(0|1)[0-9]{2}*– Supports dates from 2000 - 2199

**<month>**

* + *(Jan|Feb|Mar|Apr|May|Jun|Jul| Aug|Sep|Nov|Dec)*

**<day>**

* + *(Mon|Tue|Wed|Thu|Fri|Sat|Sun)*

**<weekday>**

* + *(Mon|Tue|Wed|Thu|Fri|Sat|Sun)*

**<time>**

* + *[0-9]{2}:[0-9]{2}:[0-9]{2}*

**<time>** = wrapper for time

**<hr>** = label for hour

**<mn>** = label for minute

**<sec>** = label for second

#### Record Subfields

**<user>**

* *[a-z]{0,32}* – 32 chars longest possible in Unix env

**<physical-terminal>**

* *tty[0-9]*

**<user-terminal>**

* *\B:0\.?0?\b*

**<pts-terminal>**

* *(pts\/)[0-9]+*

**<remote-terminal>**

* *(((([0-9]|[a-zA-Z])+)+(.|-)?)+([0-9]|[a-zA-Z])\*)+* - Used to enforce only, will match other fields

**<serial-number>**

* *2.6.32-([0-9]{0,3}.){3}el[0-9].i[0-9]{1,3}* - Matches all current examples, likely needs extending

**<duration>**

* *\([0-9]{0,2}\+?[0-9]{0,2}:[0-9]{2}\)*

**<level>**

* \(to lvl [0-9]\)

#### System Record wrapper fields

**<system>** = wrapper for system logs

**<system-crash>** = wrapper for system crash record

**<system-shutdown>** = wrapper for system shutdown record

**<system-reboot>** = wrapper for system reboot record

**<runlevel-change>** = wrapper for runlevel change record

#### Session Record wrapper fields

**<sessions>** = wrapper for session logs

**<session>** = wrapper for single session

**<complete>** = wrapper for complete session record

**<incomplete>** = wrapper for incomplete session record

**<start-session>** = wrapper for start of session time fields

**<end-session>** = wrapper for end of session time fields

# Table of Errors

|  |  |  |
| --- | --- | --- |
| Error | Solution | Exit Code |
| Missing input file | Terminal. Log error and exit. | 2 |
| Corrupt input file | Terminal. Log error and exit. | 2 |
| Missing remote terminal | Leave parsed field empty, log error/row, continue. | 0 |
| Other missing field | Leave parsed field empty, log error/row, continue. | 1 |
| Multiple missing fields | Don’t parse row, log error, continue. | 1 |
| Unidentified record type | Don’t parse row, log error, continue. | 1 |
| Unidentified serial type | Leave parsed field empty, log error/row, continue. | 1 |
| Missing non-input file | Use std file instead, log error, continue | 1 |
| Missing/Invalid flag | Log error, continue. | 1 |
| Failed to parse | Log error/row, continue. | 1 |
| Failed to encode | Log error and exit. | 2 |
| Missing language | Default to JSON | 0 |
| Invalid DateTime | Don’t parse row, log error, continue | 1 |

# Records

## System Crash

### Raw Example:

**root tty1 Thu Oct 27 15:54:53 2016 - down (00:26) :0**

### Parsed Example:

**<system-crash>**

**<user>root</user><physical-terminal>tty1</physical-terminal>**

**<start-session>**

**<date> <year>2016</year> <month>Oct</month> <day>27</day> <weekday>Thu</weekday> </date>**

**<time> <hr>15</hr> <mn>54</mn> <sec>53</sec> <time>**

**</start-session>**

**<end-session>**

**</end-session>**

**<duration> <mn>26</mn> </duration>**

**<user-terminal>:0<user-terminal>**

**</system-crash>**

## System Shutdown

### Raw Example:

**shutdown system down Fri Feb 24 07:51:17 2017 - Fri Feb 24 07:51:35 2017 (00:00) 2.6.32-642.11.1.el6.i686**

### Parsed Example:

**<system-shutdown>**

**<start-session>**

**<date> <year>2017</year> <month>Feb</month> <day>24</day> <weekday>Fri</weekday> </date>**

**<time> <hr>07</hr> <mn>51</mn> <sec>17</sec> <time>**

**</start-session>**

**<end-session>**

**<date> <year>2017</year> <month>Feb</month> <day>24</day> <weekday>Fri</weekday> </date> <time> <hr>07</hr> <mn>51</mn> <sec>35</sec> <time>**

**</end-session>**

**<duration> <mn>0</mn> </duration>**

**<serial-number>2.6.32-642.11.1.el6.i686 </serial-number>**

**</system-shutdown>**

## System Reboot

### Raw Example:

**reboot system boot Fri Mar 18 08:00:29 2016 - Thu Mar 31 00:19:46 2016 (12+16:19) 2.6.32-573.18.1.el6.i686**

### Parsed Example:

**<system-reboot>**

**<start-session>**

**<date> <year>2016</year> <month>Mar</month> <day>18</day> <weekday>Fri</weekday> </date>**

**<time> <hr>08</hr> <mn>00</mn> <sec>29</sec> <time>**

**</start-session>**

**<end-session>**

**<date> <year>2016</year> <month>Mar</month> <day>31</day> <weekday>Thu</weekday> </date> <time> <hr>00</hr> <mn>19</mn> <sec>46</sec> <time>**

**</end-session>**

**<duration> <hr>12+16</hr> <mn>19</mn> </duration>**

**<serial-number>2.6.32-573.18.1.el6.i686 </serial-number>**

**</system-reboot>**

## Runlevel Change

### Raw Example:

**runlevel (to lvl 5) Fri Feb 24 07:51:35 2017 - Mon Feb 27 07:56:31 2017 (3+00:04) 2.6.32-642.15.1.el6.i686**

### Parsed Example:

**<runlevel-change>**

**<level>5</level>**

**<start-session>**

**<date> <year>2017</year> <month>Feb</month> <day>24</day> <weekday>Fri</weekday> </date>**

**<time> <hr>07</hr> <mn>51</mn> <sec>35</sec> <time>**

**</start-session>**

**<end-session>**

**<date> <year>2017</year> <month>Feb</month> <day>27</day> <weekday>Mon</weekday> </date> <time> <hr>07</hr> <mn>56</mn> <sec>31</sec> <time>**

**</end-session>**

**<duration> <hr>3+00</hr> <mn>04</mn> </duration>**

**<serial-number>2.6.32-642.15.1.el6.i686 </serial-number>**

**</runlevel-change>**

## Complete login from known terminal – system crash

### Raw Example:

**daughertyb pts/11 Thu Oct 27 10:43:30 2016 - down (04:49)** **ec2-54-186-244-104.us-west-2.compute.amazonaws.com**

### Parsed Example:

**<complete>**

**<user>daughertyb</user> <pts-terminal>11</pts-terminal>**

**<start-session>**

**<date> <year>2016</year> <month>Oct</month> <day>27</day> <weekday>Thu</weekday> </date>**

**<time> <hr>10</hr> <mn>43</mn> <sec>30</sec> <time>**

**</start-session>**

**<end-session>**

**</end-session>**

**<duration> <hr>04</hr> <mn>49</mn> </duration>**

**<remote-terminal>ec2-54-186-244-104.us-west-2.compute.amazonaws.com</remote-terminal>**

**</complete>**

## Complete login from known terminal – known logoff time

### Raw Example:

**robertsonbt pts/14 Thu Mar 31 00:00:54 2016 - Thu Mar 31 00:14:59 2016 (00:14) 96-33-0-219.dhcp.jcsn.tn.charter.com**

### Parsed Example:

**<complete>**

**<user>robertsonbt</user> <pts-terminal>8</pts-terminal>**

**<start-session>**

**<date> <year>2016</year> <month>Mar</month> <day>31</day> <weekday>Thu</weekday> </date>**

**<time> <hr>00</hr> <mn>00</mn> <sec>54</sec> <time>**

**</start-session>**

**<end-session>**

**<date> <year>2016</year> <month>Mar</month> <day>31</day> <weekday>Thu</weekday> </date>**

**<time> <hr>00</hr> <mn>14</mn> <sec>59</sec> <time>**

**</end-session>**

**<duration> <mn>14</mn> </duration>**

**<remote-terminal>96-33-0-219.dhcp.jcsn.tn.charter.com</remote-terminal>**

**</complete>**

## Complete login from unknown terminal – known logoff time

### Raw Example:

**hilltw pts/8 Wed Mar 23 20:21:24 2016 - Wed Mar 23 20:23:40 2016 (00:02)**

### Parsed Example:

**<complete>**

**<user>hilltw</user> <pts-terminal>14</pts-terminal>**

**<start-session>**

**<date> <year>2016</year> <month>Mar</month> <day>23</day> <weekday>Wed</weekday> </date>**

**<time> <hr>20</hr> <mn>21</mn> <sec>24</sec> <time>**

**</start-session>**

**<end-session>**

**<date> <year>2016</year> <month>Mar</month> <day>23</day> <weekday>Wed</weekday> </date>**

**<time> <hr>20</hr> <mn>23</mn> <sec>40</sec> <time>**

**</end-session>**

**<duration> <mn>2</mn> </duration>**

**</complete>**

## Incomplete login from known terminal

### Raw Example:

**phil pts/12 Thu Mar 31 00:18:08 2016 still logged in tn-76-7-147-40.dhcp.embarqhsd.net**

### Parsed Example:

**<incomplete>**

**<user>phil</user> <pts-terminal>12</pts-terminal>**

**<start-session>**

**<date> <year>2016</year> <month>Mar</month> <day>31</day> <weekday>Thu</weekday> </date>**

**<time> <hr>00</hr> <mn>18</mn> <sec>08</sec> <time>**

**<remote-terminal>tn-76-7-147-40.dhcp.embarqhsd.net</remote-terminal>**

**</start-session>**

**</incomplete>**