5 Event correlation

Overview

While generally OK events close all problem events in Zabbix, there are cases when a more detailed approach is needed. For example, when monitoring log files you may want to discover certain problems in a log file and close them individually rather than all together.

This is the case with triggers that have *Multiple Problem Event Generation* enabled. Such triggers are normally used for log monitoring, trap processing, etc.

It is possible in Zabbix to relate problem events based on the event tags. Tags are used to extract values and create identification for problem events. Taking advantage of that, problems can also be closed individually based on matching tag.

In other words, the same trigger can create separate events identified by the event tag. Therefore problem events can be identified one-by-one and closed separately based on the identification by the event tag.

Correlation can be defined in:

- trigger configuration - one trigger may be used to relate problems to their solution
- globally - it is possible to relate problems to their solution from a different trigger/polling method using global correlation rules

How it works

In log monitoring you may encounter lines similar to these:

```
Line1: Application 1 stopped
Line2: Application 2 stopped
Line3: Application 1 was restarted
Line4: Application 2 was restarted
```

The idea of event correlation is to be able to match the problem event from Line1 to the resolution from Line3 and the problem event from Line2 to the resolution from Line4, and close these problems one by one:

```
Line1: Application 1 stopped
Line3: Application 1 was restarted #problem from Line 1 closed

Line2: Application 2 stopped
Line4: Application 2 was restarted #problem from Line 2 closed
```

To do this you need to tag these related events as, for example, “Application 1” and “Application 2”. That can be done by applying a regular expression to the log line to extract the tag value. Then, when events are created, they are tagged “Application 1” and “Application 2” respectively and problem can be matched to the resolution.

Configuration

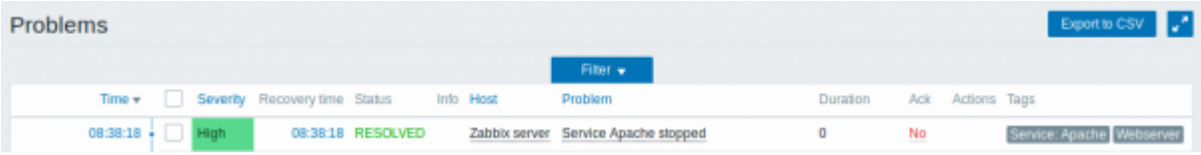
To configure event correlation on trigger level:

- go to the trigger configuration form

- select 'Problem event generation mode' as *Multiple*

- select that 'OK event closes' *All problems if tag values match*
- enter the name of the tag for event matching
- configure the tags to extract tag values from log lines

If configured successfully you will be able to see problem events tagged by application and matched to their resolution in *Monitoring* → *Problems*.



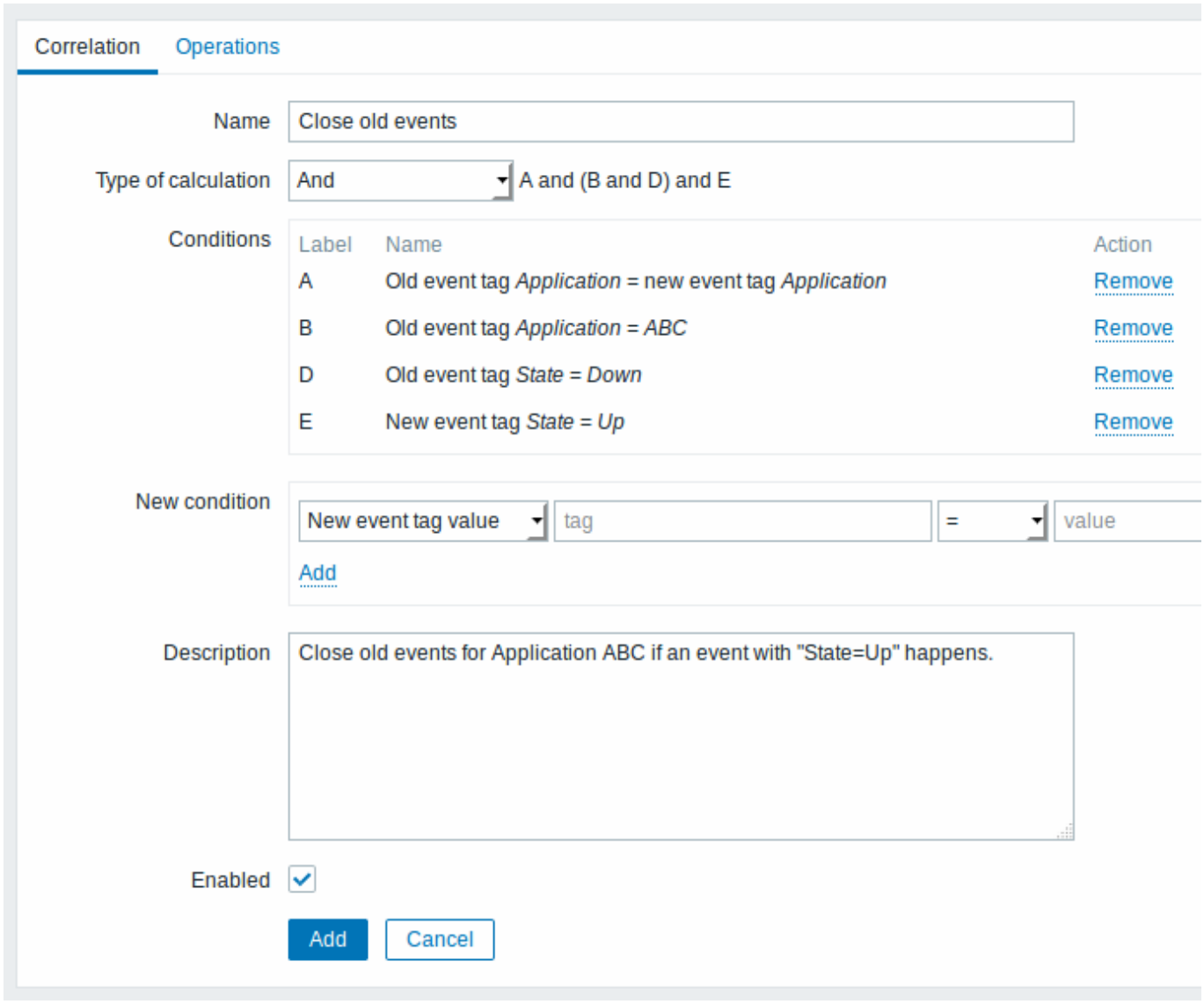
Configuring global correlation

In a slightly different scenario, you may have different triggers for problem and resolution. For example, a log trigger may report application problems, while a polling trigger may report the application to be up and running.

Taking advantage of event tags you can tag the log trigger as *Status: Down* while tag the polling trigger as *Status: Up*. Then, in a global correlation rule you can relate these triggers and assign operations to this correlation such as close old events or close new events.

To configure event correlation rules globally:

- go to *Configuration* → *Event correlation*
- Click on *Create correlation* to the right (or on the correlation name to edit an existing rule)
- Enter parameters of the correlation rule in the form



- Select the operation of the correlation rule in the form