Prelude Manager - Bug #247

bypass uninsertable alerts

07/09/2007 10:42 PM - prmarino1-gmail-com -

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Yoann VANDOORSELAERE	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	0.9.9		
Resolution:	fixed		

Description

In some cases Ive seen events where the sudo rule and some of the others excide the database field size limitations in this case there is a syslog message

```
could not insert message into database: ERROR:  value too long for type character varying(255)
```

this causes the prelude-manager creates an alert file in /var/spool/prelude-manager/failover/db[default]/ then it queues all of the following alerts into that directory until it exceeds a quota and starts deleting alerts. this causes an outage untill either the offending alert is found and manualy deleted of until it automatically deletes the alert and usualy several others.

```
 - Plugin db[default]: flushing 16870 message (4321 erased due to quota)...
```

there are two possible ways the prelude-manager could handle this better

1) in the case of this message or other field constraint errors the offending alert could be written to a different directory where it could be analyzed latter and an alert generated by the prelude-manager about the file created. the prelude-manager could then continue to process alerts right away.

2)The prelude manager could always try to insert newly recived alerts into the database first before putting them into the failover directory in the case of a faulted database status.

Since the alerts contain thir own time stamp the order in which they are inserted does not need to be preserved so either solution would work although the first is preferable as it would notify the user to a problem.

History

#1 - 07/10/2007 05:12 PM - Yoann VANDOORSELAERE

- Status changed from New to Assigned

Thanks for your report. We will have a look into it: since libpreludedb make a difference between pure query error, and database connection error, it should be possible to handle the case of query error separately at the Prelude-Manager level.

Regards,

#2 - 07/12/2007 10:53 AM - Yoann VANDOORSELAERE

Could you try the attached patch and tell me whether it fixes your problem?

#3 - 08/01/2007 04:47 PM - Yoann VANDOORSELAERE

- Status changed from Assigned to Closed

- Resolution set to fixed

(In r9761) Make a difference between exceptional report plugin failure (example: a single message couldn't be processed) and "global" plugin failure (example: database server is down).

We now use a different failover for these two type of failure, and only try to recover the message which failed because of an external condition (global failover). Fix #247.

#4 - 04/29/2009 12:20 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Prelude Manager

- Category deleted (3)

- Target version deleted (0.9.9)

Files

manager-failover.diff	6.91 KB	07/12/2007	Yoann VANDOORSELAERE