bung - Feature #165

Audit facility: research

26/01/2014 07:42 - Charles Atkinson

Status:	In Progress	**Start date:**	26/01/2014
Priority:	Normal	**Due date:**	
Assignee:	Daniel Estis	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

History

#1 - 02/03/2014 09:30 - Charles Atkinson

- Subject changed from nagios plugin: create to nagios plugin: research

Is it possible to specify a bung audit utility which can both run independently and (maybe) as a back-end for a nagios plug-in?

#2 - 29/09/2015 14:26 - Charles Atkinson

- Subject changed from nagios plugin: research to Audit facility: research

#3 - 31/10/2019 09:49 - Charles Atkinson

Charles and Daniel discussed. Daniel would like a backup audit facility.

#4 - 04/09/2020 09:35 - Charles Atkinson

```
Subject:     Re: Zabbix Agent User Parameters
Date:     Thu, 3 Sep 2020 12:13:54 +0530
From:     Daniel Estis <da@auroville.org.in>
To:     Aurinoco Systems <aurinoco@auroville.org.in>

I meant to solve the issue of backup task has not been executed for whatever reason. And hence no email being
sent. We spoke about this.... I am working now on a new version of backup script coded in Powershell and I am
thinking about an SFTP box that will accumulate reports from all hosts. Then another script will analyse these
 reports and send a concentration once a while. What do you think?

best,
Daniel

On Thu, Sep 3, 2020 at 9:35 AM Aurinoco Systems <aurinoco@auroville.org.in <mailto:aurinoco@auroville.org.in>>
 wrote:

    Assuming you mean bung backups ...

    We could but bung already sends emails (SUCCESS or otherwise) and
    logcheck emails bung's warning and error messages written to
    syslog.  Would another notification add value?

    Charles

    Aurinoco Systems
    Auroville Foundation Bhavan
    Auroville, Tamil Nadu 605101
    +91 413 2000015

    On 03/09/2020 09:28, Daniel Estis wrote:
>     Hello Charles,
>
>     Just a very crude idea that came to my mind this morning... Can we
>     use Zabbix Agent User Parameters to deliver backup results?
```

```
>
>     best,
>     Daniel
```

#5 - 04/09/2020 09:46 - Charles Atkinson

- Assignee changed from Charles Atkinson to Daniel Estis

It is a great idea now, as it was six years ago!

I understand you are writing of Windows. I am replying for Linux. The principles are the same

The audit facility should also audit database (mariadb, postgres ...) and OpenLDAP installed and backups not configured.

Rather than having a central location to receive reports (your SFTP box) I would

- Create a script to be run by Zabbix on the monitored computer to
  - Audit what has been installed (mariadb, OpenLDAP, postgres ...) and, for each, report
    - How it is being backed up (the backup conf)
    - Status of the last backup (time run, OK/WARN/ERROR)
  - On Dom0s only, similar for self backup and each DomU backup

Implementing this via Zabbix would keep everything in the same tool regards logging and notifications

#6 - 05/09/2020 12:02 - Daniel Estis

- Assignee changed from Daniel Estis to Charles Atkinson

I would also prefer to keep all in the same tool. But I will need to learn how to communicate a parameter to Zabbix. Maybe, if you do progress on this, we can meet and you briefly explain me how Zabbix works and what might be required from a backup script to communicate data to Zabbix.

#7 - 07/09/2020 19:32 - Charles Atkinson

- Status changed from New to In Progress

- Assignee changed from Charles Atkinson to Daniel Estis

As discussed, Zabbix can be extended to run custom commands on monitored hosts. Aurinoco has done so to check postfix queues.

- On the Zabbix server, template "Template App Postfix" has items
  - Postfix active queue
  - Postfix bounced mails
  - Postfix deferred queue
  - Postfix sent mails
- Taking "Postfix deferred queue" as an example, the item is populated by getting postfix.deferred from the Zabbix Agent running on the monitored host
- On the monitored host /etc/zabbix/zabbix_agentd.d/postfix.conf includes

```
UserParameter=postfix.deferred[*],/usr/sbin/postqueue -p | egrep -c "^[0-9A-F]{10}[^*]"
```

That defines the value of postfix.active as the output of the postqueue and egrep commands
- Template "Template App Postfix" also has a trigger "Postfix: Too many deferred mails on {HOST.NAME}" which fires when the average number of deferred mails for the last three hours exceeds two (in retrospect not the best choice!)

The value of postfix.active is an deferred. For backup monitoring we would probably want two values

- An integer representing OK, WARN or ERROR and displayed as such
- Text detailing the WARN or ERROR condition

The custom command can be a script so getting the values is completely flexible

#8 - 12/09/2020 09:22 - Daniel Estis

One more value. Date of last backup execution.