openSUSE admin - tickets #90521

beans.opensuse.org - permissions issue between apache and dehydrated [was: beans.o.o down]

2021-03-31 04:27 - hellcp

<table>
<thead>
<tr>
<th>Status:</th>
<th>Feedback</th>
<th>Start date:</th>
<th>2021-03-31</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>Assignee:</td>
<td>cboltz</td>
<td>% Done:</td>
<td>0%</td>
</tr>
<tr>
<td>Category:</td>
<td>Servers hosted in NBG</td>
<td>Estimated time:</td>
<td>0.00 hour</td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Description

History

#1 - 2021-03-31 04:27 - hellcp
- Private changed from Yes to No

#2 - 2021-03-31 18:48 - cboltz
- Subject changed from beans.opensuse.org down to beans.opensuse.org - permissions issue between apache and dehydrated [was: beans.o.o down]
- Assignee set to lrupp
- Priority changed from High to Normal

Fixed for now - the issue was

```
[ssl:emerg] [pid 23864] AH02565: Certificate and private key beans.opensuse.org:443:0 from /etc/apache2/ssl.crt/cert.pem and /etc/apache2/ssl.key/privkey.pem do not match
```

and that was caused by a permission issue on /etc/apache2/ssl.key/ - dehydrated didn't have permissions to access this directory, and therefore couldn't update privkey.pem there.

IIRC I already "fixed" this in the past (by adding group permissions and an ACL), but the group permissions were probably reset by some apache update - and that also means the problem will come back with the next apache update.

- I'll keep the ticket open until we found a more permanent solution (maybe a different location for the certificate that doesn't get its permissions reset?).

Lars, since you did most of the work on matomo - any proposals or preferences? ;-)  

#3 - 2021-04-01 12:31 - lrupp
- Status changed from New to Feedback
- Assignee changed from lrupp to cboltz

Thanks for fixing it and identifying the root case as well!

cboltz wrote:

- I'll keep the ticket open until we found a more permanent solution (maybe a different location for the certificate that doesn't get its permissions reset?).

Storing own SSL certificates out of the usual places seems to be the "best practice" (me remembers that we do this in other areas as well). As we need to store certificates for different services and might need to patch them (apparmor) to get permission to a central directory, our current approach was always to use a directory below the configuration directory of the specific service.

Apache -> /etc/apache2/certs/
Nginx -> /etc/nginx/certs/
haproxy -> /etc/nginx/certs/
ldap -> /etc/openldap/certs/
...

Most of the time, the apparmor profiles (and other settings) allow the daemons to read in their config directory and any sub-directory. So no special handling of apparmor profiles or other settings is needed in this case.
What do you think?

#4 - 2021-04-04 12:01 - cboltz

/etc/$program/certs is one option.

The other option is to just leave the certs in /etc/dehydrated - if your profile includes abstractions/ssl_certs and abstractions/ssl_keys, it already allows reading certs in the usual locations (including /etc/dehydrated). (BTW: That's what I do on my own server.)

Another option would be to copy the certs as root (not as user dehydrated) to avoid the permission problem.

One more option would be to package /etc/apache2/ssl.key with root:root 750 so that (manually added) ACLs keep working.

Which easter egg do you like most? ;)

2021-05-24