Token Task Force Meeting

October 6th, 2021

Lisa Goodenough

Agenda

- General Information

- Introduction to Tokens Talk by Mine and Dave

- Question Session

General Information

- **We have a mailing list for this group, token_task_force@listserv.fnal.gov**

  - If you would like to subscribe, send an email to listserv@fnal.gov with an empty 'Subject' line and the following in the body of the email: "subscribe token_task_force"

- **The meetings are listed on Indico on the FIFE page: https://indico.fnal.gov/category/722/**

- **We are still waiting on our wiki page as a place to put documents. For now, we have**

  - a Google doc with instructions for testing token setup here: Testing Instructions

  - and a Google sheet for recording testing progress, issues, requests, questions: Task Force Progress and Issues

- **Meetings are every other week on Wednesdays from 1-2pm.**

Token-related Questions

1. What is the conceptual purpose and technical content of each of these files:

  - /tmp/vt_u1311

  - nashome/r/rlc/.config/htgettoken/credkey-mu2e-default

  - /run/user/1311/bt_u1311

  - the vaultserver

2. What is the effective valid lifetime of the content of each?

3. What happens to the behavior of the token if each of these is expired, invalid or missing?

4. What happens to the behavior of htgettoken if each of these is expired, invalid or missing?

5. Under exactly what circumstance does htgettoken do the web browser requirement? Is there a simple way to predict?

Token-related Questions cont.

6. If htgettoken decides to go to the web, is there a way to get it to not do that, but instead simple say that it would?

7. Is it possible to get an htgettoken switch that causes it to simply return with a success code if your token is valid and not success if it is not valid?

8. Is there any way we can default "--vaultserver fermicloud543.fnal.gov" so the user doesn't need it to remember it?

An Issue

- Ray sees the following crash, which he thinks occurs because he doesn't have a kerberos ticket and therefore cannot write to his home area

- Can this be handled "more smoothly"?

```
| htgettoken --vaultserver fermicloud543.fnal.gov -i mu2e -v
/bin/bash: /nashome/r/rlc/.bashrc: Permission denied
Attempting OIDC authentication with https://fermicloud543.fnal.gov:8200

Complete the authentication via web browser at:
    https://cilogon.org/device/?user_code=LNZ-V79-7RH
No web open command defined, please open URL manually
Waiting for response in web browser
Storing vault token in /tmp/vt_u1311
Saving credkey to /nashome/r/rlc/.config/htgettoken/credkey-mu2e-default: rlc
Traceback (most recent call last):
 File "htgettoken", line 1073, in main
 File "os.py", line 210, in makedirs
 File "os.py", line 210, in makedirs
 File "os.py", line 210, in makedirs
 File "os.py", line 220, in makedirs
PermissionError: [Errno 13] Permission denied: '/nashome/r'

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
 File "htgettoken", line 1129, in <module>
 File "htgettoken", line 1075, in main
NameError: name 'configdir' is not defined
[22047] Failed to execute script 'htgettoken' due to unhandled exception!
```

Storage Access Layouts

- Experiments need to determine storage access groups and what specific access these groups need to have

- Default suggestion is

  - production: read/write to <VO>/*

  - analysis: read from <VO>/*, write to <VO>/scratch/users/<uname>

- Thoughts on this?

- Other questions?