Arvados - Bug #16923

workbench getting token with untrusted client

09/29/2020 08:35 PM - Peter Amstutz

Status:	Resolved	**Start date:**	10/01/2020
Priority:	Normal	**Due date:**	
Assigned To:	Peter Amstutz	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	2020-10-07 Sprint		

Description

Trying to share a collection as an ordinary user, but I see (on the view collection page, in wb1):

Sharing and permissions
Your API token is not authorized to manage collection sharing links.

1. Why? I see a request like this in the api server logs when loading https://workbench.tordo.arvadosapi.com/collections/tordo-4zz18-aam8gchmw53n426:


```
[req-7rl47pzbw1vscbqsdcj1] Error 1601328087+69320957: 403
{"method":"GET","path":"/arvados/v1/api_client_authorizations","format":"json","controller":"Arvados::V1::ApiClientAuthorizationsController","action":"index","status":403,"duration":5.63,"view":0.3,"db":1.75,"request_id":"req-7rl47pzbw1vscbqsdcj1","client_ipaddr":"10.253.0.41","client_auth":"ce8i5-gj3su-sqfolnetlyfrzpr
","params":{"reader_tokens":"[\"v2/STRIPPED/STRIPPED\"]","_method":"GET","filters":"[[\"scopes\",\"=\",[\"GET /arvados/v1/collections/tordo-4zz18-aam8gchmw53n426\",\"GET /arvados/v1/collections/tordo-4zz18-aam8gchmw53n426/\",\"GET /arvados/v1/keep_services/accessible\"]]]","limit":"9223372036854775807","offset":"0"},"@timestamp":"2020-09-28T21:21:27.270244973Z","@version":"1","message":"[403] GET /arvados/v1/api_client_authorizations (Arvados::V1::ApiClientAuthorizationsController#index)"}
```


and in the controller logs:


```
Sep 28 22:06:25 tordo.arvadosapi.com arvados-controller[5343]: {"PID":5343,"RequestID":"req-6pwv2sl9s7y8ujz85v36","level":"info","msg":"response","remoteAddr":"127.0.0.1:35598","reqBytes":123,"reqForwardedFor":"10.253.0.41","reqHost":"tordo.arvadosapi.com","reqMethod":"POST","reqPath":"arvados/v1/collections/tordo-4zz18-aam8gchmw53n426","reqQuery":"","respBody":"{\"errors\":[\"request failed: http://localhost:8004/arvados/v1/collections/tordo-4zz18-aam8gchmw53n426?reader_tokens=%5B%22v2%2FSTRIPPED%2FSTRIPPED%22%5D: 404 Not Found: Path not found (req-6pwv2sl9s7y8ujz85v36)\"]}\n","respBytes":274,"respStatus":"Not Found","respStatusCode":404,"time":"2020-09-28T22:06:25.148905629Z","timeToStatus":0.012382,"timeTotal":0.012397,"timeWriteBody":0.000014}
```


2. Sharing appears to be undocumented, if this is a config issue, we need to document that better

Subtasks:

Task # 16938: Review 16923-auth-api-client	**Resolved**

Related issues:

Related to Arvados - Feature #16919: [doc] [federation] Document the two type...	**Resolved**

Associated revisions

Revision cabf89d1 - 10/01/2020 10:12 PM - Peter Amstutz

Merge branch '16923-auth-api-client' refs #16923

Arvados-DCO-1.1-Signed-off-by: Peter Amstutz <peter.amstutz@curii.com>

History

#1 - 09/29/2020 08:35 PM - Peter Amstutz

- Subject changed from Cannot make sharing links when is to Cannot make sharing links when client is not trusted

#2 - 09/29/2020 08:36 PM - Peter Amstutz

- Description updated

#3 - 09/29/2020 09:01 PM - Peter Amstutz

I have discovered two issues.

1. In the LoginCluster configuration, a user goes to tordo, is redirected to ce8i5 for login, with return_to set to tordo workbench. This means the token is associated with the tordo workbench api_client, not ce8i5. So the default behavior of trusting a cluster's workbench doesn't apply (it knows to trust ce8i5, but not tordo).
2. In arvbox, it uses the "test" login method, which uses the username/password authorization method. This method doesn't have a return_to, it provides a fake return_to called "https://none.invalid". This means when using test, pam, or LDAP authentication, it gets the "none.invalid" api_client, which is not trusted (unless explicitly configured).

For issue 1, this is actually working as intended. I think the only solution is to fix the configuration and documentation.

For issue 2, the url in createAPIClientAuthorization should be trusted by default, and tweak the bogus URL to indicate what is going on.

#4 - 09/29/2020 09:11 PM - Peter Amstutz

- Subject changed from Cannot make sharing links when client is not trusted to workbench getting token with untrusted client

#5 - 09/30/2020 01:43 PM - Peter Amstutz

- Assigned To set to Peter Amstutz

- Status changed from New to In Progress

#6 - 10/01/2020 02:40 PM - Peter Amstutz

- Related to Feature #16919: [doc] [federation] Document the two types of federation better added

#7 - 10/01/2020 06:02 PM - Peter Amstutz

16923-auth-api-client @ arvados|0dc94486b18b8797d3970eb9a982a7c9de3ada88

https://ci.arvados.org/view/Developer/job/developer-run-tests/2126/

#8 - 10/01/2020 07:13 PM - Peter Amstutz

Whoops, messed that last one up. Updated:

16923-auth-api-client arvados|7301e68e41869fd5931ef0b0f80890aa1220938d

https://ci.arvados.org/view/Developer/job/developer-run-tests/2128/

#9 - 10/01/2020 09:54 PM - Ward Vandewege

Peter Amstutz wrote:

> 16923-auth-api-client @ arvados|0dc94486b18b8797d3970eb9a982a7c9de3ada88
>
> https://ci.arvados.org/view/Developer/job/developer-run-tests/2126/

- In Arvados_arch.svg, the lines between 'cli tools' and 'workbench' on to the 4 boxes on the next line are confusing; cli tools can also connect to arv-ws and git, and workbench definitely talks to keep-web. Can we somehow indicate that the cli tools and workbench talk to all four boxes?
- missing 'and Workbench2' between 'Workbench1' and 'are trusted' in the comment in the config reference:

```
+      # When the token is returned to a client, the token itself may
+      # be restricted from manipulating other tokens based on whether
+      # the client is "trusted" or not.  The local Workbench1 are
+      # trusted by default, but if this is a LoginCluster, you
+      # probably want to include the Workbench instances in the
+      # federation in this list.
```

Otherwise, LGMT, thanks!

#10 - 10/02/2020 02:39 PM - Peter Amstutz

- Status changed from In Progress to Resolved

#11 - 10/07/2020 02:11 AM - Peter Amstutz

- Release set to 25