Arvados - Bug #17785

[controller/api] "Forbidden: this API client cannot manipulate other clients' access tokens." on federated login clusters (2.2.0 regression)

06/09/2021 12:32 PM - Ward Vandewege

Status:	In Progress	**Start date:**	
Priority:	Normal	**Due date:**	
Assigned To:	Lucas Di Pentima	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	2021-10-27 sprint		

Description

This happens on tordo (2.3.0~dev20210608145247) (login federation with ce8i5) but not on 2xpu4 (2.2.0) (directly configured for login through google).

Bug observed in multiple places:

- go to workbench.tordo, log in as admin, view a user in the admin user list, and click the "Log in as ..." button. The result is a fiddlesticks with the error "Forbidden: this API client cannot manipulate other clients' access tokens.", e.g.:

```
{
  ":errors":[
    "Forbidden: this API client cannot manipulate other clients' access tokens. (req-ckw5smn0dfhyg
vcgk5h6)"
  ],
  ":error_token":"1625590529+e5031a85"
}
```

- on shell.ce8i5, the `arvados-login-sync` script (which runs with a token belonging to an admin user) throws this output on every iteration:

```
Error setting token for STRIPPED: ["Forbidden: this API client cannot manipulate other clients' ac
cess tokens. (req-ddhir3er6zg31hszw9o1)"]
Error setting token for STRIPPED: ["Forbidden: this API client cannot manipulate other clients' ac
cess tokens. (req-u61v42jybvqur0ygz5x3)"]
Error setting token for STRIPPED: ["Forbidden: this API client cannot manipulate other clients' ac
cess tokens. (req-1dtnzyr2oo2sfp6e8pjz)"]
Error setting token for STRIPPED: ["Forbidden: this API client cannot manipulate other clients' ac
cess tokens. (req-h05j0ififv2t8ksfekhd)"]
Error setting token for STRIPPED: ["Forbidden: this API client cannot manipulate other clients' ac
cess tokens. (req-1w89ttespwuf51azgjt1)"]
Error setting token for STRIPPED: ["Forbidden: this API client cannot manipulate other clients' ac
cess tokens. (req-1773gy0yhdoo11t74emp)"]
```

Subtasks:

Task # 17869: Review	**New**
Task # 17905: investigate	**New**

Related issues:

Related to Arvados - Feature #17583: Remote controller forwards trusted clien...	**New**
Blocks Arvados - Bug #17754: [wb] merge account problem	**New**

History

#1 - 06/09/2021 12:32 PM - Ward Vandewege

- Description updated

#2 - 06/09/2021 12:34 PM - Ward Vandewege

- Target version changed from 2021-06-09 sprint to 2021-06-23 sprint

- Description updated

#3 - 06/09/2021 03:56 PM - Ward Vandewege

- Related to Bug #17754: [wb] merge account problem added

#4 - 06/09/2021 04:00 PM - Ward Vandewege

- Description updated

#5 - 06/09/2021 04:02 PM - Peter Amstutz

- Target version changed from 2021-06-23 sprint to 2021-07-07 sprint

#6 - 06/23/2021 03:59 PM - Peter Amstutz

- Assigned To set to Nico César

#7 - 06/24/2021 02:59 PM - Nico César

- File 2021-06-24_10-57.png added

- File 17785_error.png added

- File 2021-06-24_10-53.png added

#8 - 06/24/2021 03:00 PM - Nico César

- File deleted (2021-06-24_10-57.png)

#9 - 06/24/2021 03:00 PM - Nico César

- File deleted (17785_error.png)

#10 - 06/24/2021 03:00 PM - Nico César

- File deleted (2021-06-24_10-53.png)

#11 - 07/06/2021 04:58 PM - Ward Vandewege

- Description updated

- Subject changed from [workbench] log in as another user broken to [controller/api] "Forbidden: this API client cannot manipulate other clients' access tokens." on federated login clusters (2.2.0 regression)

#12 - 07/06/2021 04:59 PM - Ward Vandewege

- Description updated

#13 - 07/06/2021 05:11 PM - Ward Vandewege

- Related to Feature #17583: Remote controller forwards trusted client aware calls on a federated scenario added

#15 - 07/06/2021 09:32 PM - Peter Amstutz

- Target version changed from 2021-07-07 sprint to 2021-07-21 sprint

#16 - 07/07/2021 03:47 PM - Peter Amstutz

- Assigned To deleted (Nico César)

#17 - 07/07/2021 03:47 PM - Peter Amstutz

- Assigned To set to Peter Amstutz

#18 - 07/07/2021 03:56 PM - Peter Amstutz

- Related to deleted (Bug #17754: [wb] merge account problem)

#19 - 07/07/2021 03:56 PM - Peter Amstutz

- Blocks Bug #17754: [wb] merge account problem added

#20 - 07/21/2021 03:07 PM - Peter Amstutz

- Target version changed from 2021-07-21 sprint to 2021-08-04 sprint

#21 - 07/21/2021 03:16 PM - Peter Amstutz

- Target version changed from 2021-08-04 sprint to 2021-08-18 sprint

#22 - 08/03/2021 03:10 PM - Peter Amstutz

- Target version changed from 2021-08-18 sprint to 2021-09-01 sprint

#23 - 08/18/2021 03:16 PM - Peter Amstutz

- Assigned To changed from Peter Amstutz to Lucas Di Pentima

#24 - 08/23/2021 05:14 PM - Lucas Di Pentima

- Status changed from New to In Progress

#25 - 08/31/2021 03:00 PM - Lucas Di Pentima

While trying to reproduce this error, I kept getting another error message when asking tordo for its user's list:

```
$ arv user list
Error: error updating local user records: //railsapi.internal/arvados/v1/users/batch_update: 422 Unprocessable
 Entity: #<ActiveRecord::RecordInvalid: Validation failed: Username has already been taken> (req-1iksissnw490d
1thn1q9)
```

After re-requesting the list with -b (to bypass federation) and comparing users with ce8i5, I realized an issue with a couple of users sharing the same ward2 username. The one cached on tordo's side doesn't exist on ce8i5 (even though its UUID is from that cluster), so when tordo's controller attempts to refresh the local cache, the username is already taken by a user record that won't get updated anymore.

#26 - 09/01/2021 01:35 PM - Lucas Di Pentima

- Target version changed from 2021-09-01 sprint to 2021-09-15 sprint

#27 - 09/09/2021 02:47 PM - Lucas Di Pentima

For the "Login as <user>" case, the issue is that wb1 tries to create an ApiClientAuthorization resource owned by the target user, and that fails because the current api client record isn't trusted because:

```
$ arv user current
{
 "created_at":"2020-01-21T14:39:17.181611000Z",
 "first_name":"Lucas ",
 "full_name":"Lucas  Di Pentima",
 "identity_url":"",
 "is_active":true,
 "is_admin":true,
 "is_invited":true,
 "kind":"arvados#user",
 "last_name":"Di Pentima",
 "uuid":"ce8i5-tpzed-o4njwilpp4ov286",
[...]
}
$ arv api_client_authorization current
{
 "href":"/api_client_authorizations/ce8i5-gj3su-vobk909hrbmmsrl",
 "uuid":"ce8i5-gj3su-vobk909hrbmmsrl",
 "owner_uuid":"ce8i5-tpzed-o4njwilpp4ov286",
 "api_token":"xxxxtokenxxxx",
 "api_client_id":0,
[...]
}
```

#28 - 09/09/2021 03:15 PM - Lucas Di Pentima

Updates at deca285 - branch 17785-federated-token-regression
Test run: https://ci.arvados.org/job/developer-run-tests-remainder/2789/

- Adds an integration test that exposes the issue.

#29 - 09/09/2021 03:32 PM - Lucas Di Pentima

For the arvados-login-sync case, maybe what's needed is to set up the LOGINCLUSTER_ARVADOS_API_HOST and LOGINCLUSTER_ARVADOS_API_TOKEN envvars so that the api client authorization creation is done on the LoginCluster?

#30 - 09/15/2021 02:02 PM - Lucas Di Pentima

- Target version changed from 2021-09-15 sprint to 2021-09-29 sprint

#31 - 09/28/2021 07:15 PM - Peter Amstutz

- Release set to 42

#32 - 09/29/2021 03:04 PM - Peter Amstutz

- Target version changed from 2021-09-29 sprint to 2021-10-13 sprint

#33 - 10/07/2021 03:41 PM - Peter Amstutz

- Release deleted (42)

#34 - 10/13/2021 02:52 PM - Lucas Di Pentima

- Target version changed from 2021-10-13 sprint to 2021-10-27 sprint