Arvados - Feature #17772

use subject identifier (username etc) in "identity_url" instead of "email" for login

06/08/2021 05:13 PM - Peter Amstutz

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assigned To:		**% Done:**	0%
Category:	Login	**Estimated time:**	0.00 hour
Target version:	2021-11-10 sprint		

Description

(formally: OIDC support "sub" claim)

We should prefer to use the "sub" claim to identify users (this is the way OIDC is *supposed* to work), and only identify users by "email" as an optional backup strategy.

This also affects PAM and other login methods.

In Arvados:

- Come up with a custom internal URL scheme to identify users that will be used for identity_url. This is the provider type, host, and subject (username or however the user is uniquely identified).

oidc://

google://

ldap://

pam://

etc

the host part identifies the provider

the path part is the subject from the provider (URL encoded)

put this in the identity_url field of the user

When logging in, it searches for identity_url. If found, but the email address has changed, it updates the email address.

- Add flag to specify if it should use user email as a fallback.

If the fallback is disabled, if the identity_url is not found, the user cannot log in.

If the fallback is enabled, if the identity_url is not found, it searches by email address. If found, the user logs in, and it update identity_url.

- Add an additional flag for "fallback only on empty identity_url"

If the fallback is disabled, if the identity_url is not found, the user cannot log in.

If the fallback is enabled, if the identity_url is not found, it searches by email address. If found *and* the identity_url is blank, then the user logs in, and it update identity_url.

History

#1 - 06/08/2021 05:14 PM - Peter Amstutz

- Description updated

#2 - 06/08/2021 05:33 PM - Peter Amstutz

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

#3 - 06/23/2021 03:57 PM - Peter Amstutz

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

- Description updated

#4 - 06/30/2021 04:21 PM - Peter Amstutz

- Description updated

#5 - 06/30/2021 04:23 PM - Peter Amstutz

- Description updated

#6 - 07/07/2021 04:02 PM - Peter Amstutz

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

#7 - 07/21/2021 03:33 PM - Peter Amstutz

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

#8 - 08/03/2021 03:07 PM - Peter Amstutz

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

#9 - 08/03/2021 07:23 PM - Peter Amstutz

- Description updated

- Subject changed from OIDC support "sub" claim to use subject identifier (username etc) in "identity_url" instead of "email" for login

#10 - 08/10/2021 05:36 PM - Peter Amstutz

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

#11 - 08/31/2021 07:52 PM - Peter Amstutz

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

#12 - 09/14/2021 07:12 PM - Peter Amstutz

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

#13 - 09/28/2021 07:27 PM - Peter Amstutz

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

#14 - 10/12/2021 07:00 PM - Peter Amstutz

- Target version changed from 2021-10-27 sprint to 2021-11-10 sprint