AIP-84 : Add JWT token revokation for logout invalidation (#47952) #61339

Merged **vincbeck** merged 19 commits into `apache:main` from `anishgirianish:feature/47952-aip-…` on Feb 5

anishgirianish commented on Feb 1 • edited — Contributor

Summary

- Adds a `revoked_token` table to persist revoked JWT token JTIs on logout
- On logout, the token's `jti` is extracted and stored with its `exp` timestamp
- On every authenticated request, `get_user_from_token` checks if the `jti` has been revoked before allowing access
- Expired revoked tokens are automatically cleaned up via the existing `db_cleanup` mechanism

closes: #47952

👍 1

anishgirianish requested review from **XD-DENG**, **ashb**, **bugraoz93**, **choo121600**, **ephraimbuddy**, **jason810496**, **pierrejeambrun**, **rawwar**, **shubhamraj-git** and **vincbeck** as code owners 2 months ago

boring-cyborg bot added area:API area:db-migrations kind:documentation labels on Feb 1

anishgirianish marked this pull request as draft 2 months ago

anishgirianish marked this pull request as ready for review 2 months ago

anishgirianish mentioned this pull request on Feb 2

AIP-84 Token Invalidation #47952

Closed

1 task

jason810496 reviewed on Feb 2

View reviewed changes

jason810496 left a comment • edited

Member

Nice! Thanks for the PR and it LGTM.
I think this PR is on the correct direction to resolve #47952.

❤️ 1

`airflow-core/src/airflow/api_fastapi/auth/managers/base_auth_manager.py` Outdated Show resolved

`airflow-core/src/airflow/api_fastapi/auth/managers/base_auth_manager.py` Outdated Show resolved

`airflow-core/src/airflow/api_fastapi/core_api/routes/public/auth.py` Outdated Show resolved

`airflow-core/src/airflow/api_fastapi/core_api/routes/public/auth.py` Outdated Show resolved

`airflow-core/src/airflow/api_fastapi/core_api/routes/public/auth.py` Outdated Show resolved

`airflow-core/src/airflow/api_fastapi/core_api/routes/public/auth.py` Outdated Show resolved

`airflow-core/src/airflow/api_fastapi/core_api/routes/public/auth.py` Outdated Show resolved

`airflow-core/tests/unit/api_fastapi/core_api/routes/public/test_auth.py` Show resolved

`airflow-core/tests/unit/api_fastapi/core_api/routes/public/test_auth.py` Outdated Show resolved

anishgirianish force-pushed the `feature/47952-aip-token-invalidation-on-logout` branch 2 times, most recently from **`0c84287`** to **`e7f823e`** 2 months ago Compare

vincbeck reviewed on Feb 2

View reviewed changes

`airflow-core/src/airflow/api_fastapi/core_api/routes/public/auth.py` Outdated Show resolved

jason810496 reviewed on Feb 3

View reviewed changes

jason810496 left a comment Member

> These added tests were already part of the existing TestLogout class.,

My bad, I overstated the the TestLogout class above.

Nice! Regarding the public method Vincent mentioned, the tests look good, and rest of the changes LGTM. Thanks!

👍 1

anishgirianish force-pushed the `feature/47952-aip-token-invalidation-on-logout` branch from **`e7f823e`** to **`3be8480`** 2 months ago Compare

potiuk commented on Feb 3 Member

Nice. Tests need to be fixed of course, and I think we should also add another thing - auto cleanup not only on clean_db but run (not always - just from time to time - we could store in memory last time when it was run and run it after an hour passes or so - when a token is checked.

That will slightly slow down some login attempts - but it will also auto-clean the db when `airflow db cleanup` is not run periodically. simply those expired tokens are not useful immediately after they expired.

👍 1 ❤️ 1

vincbeck approved these changes on Feb 3

View reviewed changes

vincbeck left a comment — Contributor

Very good!

❤️ 1

anishgirianish force-pushed the `feature/47952-aip-token-invalidation-on-logout` branch 2 times, most recently from `3b52ca2` to `0c51fff` 2 months ago

Compare

jason810496 reviewed on Feb 4

View reviewed changes

jason810496 left a comment — Member

Nice! Thanks for addressing the comments and fixing the tests.

❤️ 1

`airflow-core/src/airflow/models/revoked_token.py` Outdated — Show resolved

`airflow-core/src/airflow/models/revoked_token.py` Outdated — Show resolved

anishgirianish added 3 commits 2 months ago

`Add JWT token revokation for logout invalidation (apache#47952)` `70acb0d`

fix failing test 0ed7d71

fix faling test 0bb07d2

6 hidden items

Load more…

anishgirianish added 14 commits 2 months ago

continue fixing test 3a1c3cc

made revocation sync d7f843d

refactor 061d752

refactor the token checks 3957052

error handeling refactor 97663f5

rebased da0f6db

remove isRevoked patch mock e7afc30

Fix test_logout_revokes_token by using a dedicated test client withou… 1e8c039

…

further refactor 26a1e24

fix test c4ad99c

add periodic clean up for revoked token, add test and fix fialing test 330d062

retrigger CI 0295ecb

retrigger CI 395fb5b

refactor: use class attribute and config-based cleanup interval for r… ✗ 5e0c33b

…

anishgirianish force-pushed the `feature/47952-aip-token-invalidation-on-logout` branch from **397534c** to **5e0c33b** 2 months ago

Compare

fix import ✓ 73ab065

bugraoz93 approved these changes on Feb 4

View reviewed changes

bugraoz93 left a comment

Contributor

Nice, thanks **@anishgirianish**!

❤️ 1

bugraoz93 commented on Feb 4

Contributor

I would like to call this PR for the `protm` if no one disagrees :)

#protm, which is solving a good problem for the token lifecycle. Additionally, it opens the door for great security improvement(s), such as a token invalidation endpoint for administrators in case of a token leak.

❤️ 2

vincbeck commented on Feb 4

Contributor

> I would like to call this PR for the `protm` if no one disagrees :)
>
> #protm, which is solving a good problem for the token lifecycle. Additionally, it opens the door for great security improvement(s), such as a token invalidation endpoint for administrators in case of a token leak.

Agree!

❤️ 1

anishgirianish requested a review from **jason810496** 2 months ago

jason810496 approved these changes on Feb 5

View reviewed changes

jason810496 left a comment — Member

> I would like to call this PR for the protm if no one disagrees :)

+1 for that!

❤️ 1

vincbeck merged commit `b3306f1` into `apache:main` on Feb 5

129 checks passed

View details

pierrejeambrun reviewed on Feb 5

View reviewed changes

pierrejeambrun left a comment — Member

Great one!

❤️ 1

jhgoebbert pushed a commit to jhgoebbert/airflow_Owen-CH-Leung that referenced this pull request on Feb 8

`AIP-84 : Add JWT token revokation for logout invalidation (apache#47952…` `a5709b0`

…

Ratasa143 pushed a commit to Ratasa143/airflow that referenced this pull request on Feb 15

`AIP-84 : Add JWT token revokation for logout invalidation (apache#47952…` `30cd3ca`

…

choo121600 pushed a commit to choo121600/airflow that referenced this pull request on Feb 22

`AIP-84 : Add JWT token revokation for logout invalidation (apache#47952…` `9e5a565`

…

Subham-KRLX pushed a commit to Subham-KRLX/airflow that referenced this pull request on Mar 4


`AIP-84 : Add JWT token revokation for logout invalidation (apache#47952…` `4fcd994`
…

dominikhei pushed a commit to dominikhei/airflow that referenced this pull request last month


`AIP-84 : Add JWT token revokation for logout invalidation (apache#47952…` `92871c2`
…

Ankurdeewan pushed a commit to Ankurdeewan/airflow that referenced this pull request last month


`AIP-84 : Add JWT token revokation for logout invalidation (apache#47952…` `a8ed57a`
…

radhwene pushed a commit to radhwene/airflow that referenced this pull request 3 weeks ago


`AIP-84 : Add JWT token revokation for logout invalidation (apache#47952…` `07e14f6`
…

Reviewers

 **pierrejeambrun**
 **bugraoz93**
 **jason810496**
 **vincbeck**
 **ephraimbuddy**
 **rawwar**
 **shubhamraj-git**
 **choo121600**
 **XD-DENG**
 **ashb**

Assignees

No one assigned

Labels

area:API area:db-migrations kind:documentation

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

AIP-84 Token Invalidation

6 participants