Add authentication to /api/events/in WebSocket endpoint #20372

Merged **desertaxle** merged 7 commits into `main` from `devin/1769188570-events-in-auth` on Jan 27

devin-ai-integration Bot commented on Jan 23 • edited Contributor

Fixes a security vulnerability where the `/api/events/in` WebSocket endpoint bypasses authentication even when `PREFECT_SERVER_API_AUTH_STRING` is configured.

Changes

Server-side (`src/prefect/server/api/events.py`):

- Always require the "prefect" subprotocol and auth handshake via `subscriptions.accept_prefect_socket()`
- Removed conditional auth logic - authentication flow is now consistent with other WebSocket endpoints

Client-side (`src/prefect/events/clients.py`):

- Always connect with "prefect" subprotocol
- Always send auth message (token can be None when auth is not configured)
- Use `get_current_settings().api.auth_string` instead of `PREFECT_API_AUTH_STRING.value()`
- Updated both `PrefectEventsClient` and `PrefectEventSubscriber` classes

Tests (`tests/events/server/gateway/test_gateway_in.py`): Add comprehensive authentication tests covering:

- Subprotocol requirement (always required)
- Auth message requirement (always required as first message)
- Invalid token rejection
- Missing token rejection

- Successful event streaming with and without auth configured

Test fixtures (`src/prefect/testing/fixtures.py`): Update `events_server` fixture to:

- Always require auth handshake (matching server behavior)
- Accept "prefect" subprotocol via `select_subprotocol` callback

Breaking Change

This is a breaking change for clients that don't send the auth handshake. The "prefect" subprotocol and auth message are now always required, even when `PREFECT_SERVER_API_AUTH_STRING` is not configured. When auth is not configured, the server accepts any token (including None).

Review Checklist for Humans

- [ ] Verify server always uses `accept_prefect_socket()` (no conditional fallback)
- [ ] Verify client always sends auth message with token (even if None)
- [ ] Confirm `PrefectCloudEventsClient` still works (inherits from `PrefectEventsClient`)
- [ ] Verify unauthenticated connections are rejected with appropriate error codes

closes OSS-7548

Checklist

- [x] This pull request references any related issue by including "closes `<link to issue>`"
- [x] If this pull request adds new functionality, it includes unit tests that cover the changes
- [ ] If this pull request removes docs files, it includes redirect settings in `mint.json`.
- [ ] If this pull request adds functions or classes, it includes helpful docstrings.

Link to Devin run: https://app.devin.ai/sessions/944c7cadf6b74d188ccde99d5a4ac575
Requested by: **@desertaxle**

`Add authentication to /api/events/in WebSocket endpoint` ··· ✕ `c5b1249`

devin-ai-integration Bot requested review from **chrisguidry**, **cicdw**, **desertaxle** and **zzstoatzz** as code owners 4 months ago

devin-ai-integration Bot commented on Jan 23 Contributor Author

🤖 Devin AI Engineer

I'll be helping with this pull request! Here's what you should know:

✅ I will automatically:

- Address comments on this PR. Add '(aside)' to your comment to have me ignore it.
- Look at CI failures and help fix them

Note: I can only respond to comments from users who have write access to this repository.

⚙️ Control Options:

- [ ] Disable automatic comment and CI monitoring

devin-ai-integration Bot commented on Jan 23

View reviewed changes

devin-ai-integration Bot left a comment — Contributor Author

Devin Review found 1 potential issue.

View issue and 4 additional flags in Devin Review.

Open in Devin Review

`src/prefect/events/clients.py` — Show resolved

codspeed-hq Bot commented on Jan 23 • edited

CodSpeed Performance Report

Merging this PR will not alter performance

Comparing `devin/1769188570-events-in-auth` (`e880098`) with `main` (`810b865`)

Summary

✅ 2 untouched benchmarks

devin-ai-integration Bot and others added 3 commits 4 months ago

`Fix test fixtures to handle auth handshake for events client` ··· ✗ `ac0bd6c`

`Fix test_websocket_custom_headers_with_websocket_connect to handle au…` ··· ✗ `a0f2938`

`Make /api/events/in backward compatible when auth is not configured` ··· ✓ `0d3ab3c`

desertaxle requested changes on Jan 26

View reviewed changes

`src/prefect/events/clients.py` Outdated — Show resolved

`src/prefect/events/clients.py` Outdated — Show resolved

`src/prefect/server/api/events.py` Outdated — Show resolved

`src/prefect/events/clients.py` Outdated — Show resolved

`Address PR review: Always require prefect subprotocol and auth handshake` ··· ✗ `bd9e2cc`

devin-ai-integration Bot commented on Jan 26 — Contributor, Author

Devin is archived and cannot be woken up. Please unarchive Devin if you want to continue using it.

desertaxle and others added 2 commits 4 months ago

`Make WebSocket endpoints backward compatible with old clients` ··· ✗ `f016d2a`

`Fix test_logs_websocket.py for backward compatible WebSocket handling` ··· ✓ `e880098`

desertaxle approved these changes on Jan 26

View reviewed changes

desertaxle left a comment — Member

LGTM!

cc @**chrisguidry** for a second opinion when you've got a moment to spare

chrisguidry approved these changes on Jan 26

View reviewed changes

chrisguidry left a comment — Collaborator

Looks pretty legit to me!

desertaxle merged commit `f8afeca` into `main` on Jan 27

98 of 102 checks passed

View details

---

desertaxle deleted the `devin/1769188570-events-in-auth` branch 4 months ago

desertaxle added a commit that referenced this pull request on Jan 29

`Fix PrefectCloudEventsClient failing to connect due to auth handshake` ··· ✓ `ec59434`

desertaxle mentioned this pull request on Jan 29

Fix PrefectCloudEventsClient auth handshake breaking Cloud connections #20472

Merged

5 tasks

giovanniborella mentioned this pull request on Jan 30

Kubernetes worker fails to connect to events websocket after upgrading from 3.6.13 → 3.6.15 (HTTP 403) #20474

Closed

gykung commented on Feb 23

@desertaxle @chrisguidry I have a self-hosted server running **3.5.0**, and a client running **3.6.18**, with basic authentication via PREFECT_SERVER_API_AUTH_STRING and PREFECT_API_AUTH_STRING on server and client respectively. I got the following error and after a reading through the release notes, arrived at this PR...,.

May I ask:

- Is this the expected behavior, e.g... the breaking change mentioned in 3.6.14?
- Is the correct response to update the server to **≥3.6.14+**?

```
  File "C:\...\site-packages\prefect\events\clients.py", line 388, in _auth_handshake
    raise Exception(msg) from e
Exception: Unable to authenticate to the event stream. Please ensure the provided
auth_token you are using is valid for this environment.
```

desertaxle commented on Feb 23 — Member

@gykung Yes, that is expected. We do not support running newer clients with older servers. If you want to use a newer client, you need to upgrade your server first.

👀 1

devin-ai-integration Bot mentioned this pull request on Mar 19

Allow legacy WebSocket clients to connect when auth is configured #21181

Closed

4 tasks

Reviewers

- chrisguidry ✓
- desertaxle ✓
- cicdw
- zzstoatzz

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

3 participants