After OIDC, verify that audit logs actually arrive

2026-11-29 · 8plus

On November 19, 2026, GitHub announced OIDC-based enterprise audit-log streaming to Amazon S3 for GitHub Enterprise Cloud with data residency, GHE.com. It removes the need to store long-lived AWS credentials on GitHub. This article uses an official update from the last thirty days and offers delivery guidance, not deployment results.

A successful connection answers only one question

Managing one fewer long-lived credential can simplify its lifecycle, but a different authentication method does not establish complete delivery. Successful configuration, objects appearing in storage, and an expected event being queryable are separate acceptance questions.

Define the enterprise, destination, receiving owner, data consumers, and expected time to query. Check permissions and OIDC trust settings against official documentation. Avoid copying another environment’s settings or granting unnecessary access simply to pass a test.

Follow one identifiable event through the path

Within an authorized test scope, choose a reversible, low-impact operation that appears in the audit log. Record its time and available identifiers. Verify it at the source, then at the destination, and finally through the actual analysis workflow. File counts alone are insufficient, and different operations need not produce identical events.

This is an acceptance method, not a GitHub guarantee about every event’s latency. Define an observation window for your requirements. If the event remains missing, investigate rather than concluding it never occurred. Time zones, query filters, and transformations can also affect discovery.

Receiving health needs continuing evidence

A handoff can record the last successful receipt, a controlled reference to the test event, and the person responsible for interruptions. In a quiet environment, a period without new files does not prove failure. Interpret destination health alongside source activity.

Also verify that intended consumers can query the data. An object may exist while parsing or access fails downstream. Separate arrival from queryability to locate problems without blaming every failure on OIDC.

Leave a usable transition record

After verifying the new path, handle old settings and credentials through the existing change process. Record transition time, tested scope, unresolved questions, and recovery steps without attaching complete logs or identity data. Keep audit information under appropriate access and retention controls, not in public examples or website analytics.

The useful result is more than saying that OIDC is enabled. The next owner should know where data originates, where it goes, how arrival is demonstrated, and whom to contact when it is missing.

Sources

Official announcement

Related reading