

Trino and Starburst

From the SourceLace manual: How to connect a Trino cluster for read-only SQL: open-source Trino, Starburst Enterprise or Starburst Galaxy. Each person signs in with their own identity, so the cluster's own access control decides what every query and schema lookup can see.

SourceLace version 0.1.0 · Made October 7, 2026

The latest version is at <https://sourcelace.onrender.com/docs>

Trino and Starburst

How to connect a Trino cluster for read-only SQL: open-source Trino, Starburst Enterprise or Starburst Galaxy. Each person signs in with their own identity, so the cluster's own access control decides what every query and schema lookup can see.

Status: Preview. New, offered for pilots and provided as is. Built against Trino's documented client protocol and covered by automated tests against a simulated cluster; not yet used with a customer's live cluster.

At a glance

	Connects through	Sign-in	Network	Status	First test question
Trino and Starburst	Trino client REST API over HTTPS	Personal sign-in	Allow SourceLace's IP addresses	Preview	"Which tables can I see in trino:prod?"

Add each source with the [usual steps](#). The network answers are explained in [What your network needs](#). If the first test question fails, the error message tells you what to fix: look it up under **When something goes wrong** below.

What people can do

- `search_schema` lists tables and views the person can see, as `catalog.schema.table`. Without a default catalog, SourceLace looks in the first 10 catalogs (not system). `describe_object` lists a table's columns, types and comments.
- `query` (language `sql`) takes **one** `SELECT` or `WITH ... SELECT` statement in Trino SQL. Anything that could change data (`INSERT`, `UPDATE`, `DELETE`, `MERGE`, `CREATE`, `DROP`, `ALTER`, `CALL`, `SET SESSION` and so on), anything with more than one statement, and table functions (`TABLE(...)`, which in some catalogs pass raw text to the database behind them) are refused **before** anything is sent.
- Results are capped at 2,000 rows (50 shown at a time). SourceLace stops reading once it has enough and cancels the rest of the query on the cluster. Results are held for at most 30 minutes and never written to a database (see [How long things are kept](#)).
- These sources never accept changes. `get_record` is not used: people query with a `WHERE` clause.
- SourceLace never uses a shared service account for these sources.

Cost and time limits

Every query goes through these steps:

1. **Estimate first.** SourceLace asks Trino for `EXPLAIN (TYPE IO, FORMAT JSON)` of the query, which plans it without running it. If Trino estimates the query would read more than the source's `max_scan_bytes` (10 GB unless set), it is refused with the estimate, and nothing runs. Catalogs without table statistics give no estimate; those queries run, still capped by step 2.
2. **Limits the cluster enforces.** Each query is sent with the session properties `query_max_run_time` (your organization's query time limit, about a minute unless changed on the [Limits](#) page) and `query_max_scan_physical_bytes` (`max_scan_bytes`), so Trino itself stops a

query that runs too long or reads too much.

3. **Cancel on time-out.** If the time limit passes, SourceLace also cancels the query on the cluster.

Every query carries the client tag `sourcelace` and the source name `sourcelace`, so your Trino admin can see SourceLace's queries in the query history and, if they like, give them their own resource group.

How people sign in

The source's auth option picks one of two ways. Both are per person.

auth	How each person signs in	Good for
password (default)	Types their own Trino username and password into SourceLace's sign-in form. SourceLace sends it only over HTTPS and keeps it encrypted. On Starburst Galaxy the username is their email and role, such as <code>ann@corvanta.com/analyst</code> .	Trino or Starburst Enterprise with password (file or LDAP) authentication; Galaxy users with a Galaxy password
oauth	Signs in on your identity provider's page (or Galaxy's), through an OAuth client your admin registers. SourceLace sends the access token to Trino, which takes the user from it.	Trino or Starburst Enterprise with OAuth 2.0 or JWT authentication; Galaxy with an OAuth client, including SSO users

The redirect URL for an OAuth client is:

`https://sourcelace.onrender.com/connect/callback`

Set up the cluster (Trino or Starburst admin)

- The cluster must be reachable from SourceLace over **HTTPS** with a certificate from a public certificate authority (Galaxy always is). Allow SourceLace's outbound IP addresses in any firewall; ask support@sourcelace.com for the current list.
- **Password sign-in:** nothing more. Each person uses the login they already have.
- **OAuth with Trino or Starburst Enterprise:** register SourceLace as an OAuth client in the identity provider the cluster trusts: a public client with PKCE (no secret), or a confidential client, with the redirect URL above. Its access tokens must be ones Trino accepts: the audience must be the cluster's own client id or listed in `http-server.authentication.oauth2.additional-audiences` (or `http-server.authentication.jwt.required-audience` for JWT authentication), and the token's user field (`principal-field`) must name the Trino user.
- **OAuth with Starburst Galaxy:** in Galaxy, **Access control** → **OAuth clients** → **Create new OAuth client**. Choose **Public** (SourceLace uses PKCE) and **Custom**, enter a client ID and the redirect URL above. Galaxy's sign-in addresses are `https://<account>.galaxy.starburst.io/oauth/v2/authorize` and `https://<account>.galaxy.starburst.io/oauth/v2/token`.
- If your access control limits which **session properties** people may set, allow `query_max_run_time` and `query_max_scan_physical_bytes`, or set the source's `session_limits` to off.

Add the source (SourceLace admin)

Kind: **Trino and Starburst** (trino).

Option	Type	Default	Example	What it is
host	Text	(required)	trino.corvanta.com, trino.corvanta.com:8443, corvanta-reporting.trino.galaxy.starburst.io	The cluster's HTTPS address. Only HTTPS.
auth	password or oauth	password	oauth	How people sign in (see above).
authorize_url	Address	(required with oauth)	https://corvanta.galaxy.starburst.io/oauth/v2/authorize	The OAuth client's sign-in page.
token_url	Address	(required with oauth)	https://corvanta.galaxy.starburst.io/oauth/v2/token	Where SourceLace turns the sign-in into a token.
client_id	Text	(required with oauth)	sourcelace-trino	The OAuth client's id.
client_secret	Secret	(none: a public client)		Only for a confidential client. Stored encrypted and never shown again.
scope	Text	openid offline_access	api://trino/.default offline_access	The scopes to ask for, so the token is one the cluster accepts.
catalog	Name	(none)	hive	Default catalog. With it, search_schema looks only there.
schema	Name	(none)	sales	Default schema.
role	Name	each person's default	analyst	A system role to use for queries.
max_scan_bytes	Number of bytes	10000000000 (10 GB)	50000000000	The most one query may read.
session_limits	on or off	on	off	Send the time and size limits as session properties.

When something goes wrong

What you see	What to do
"... did not accept that username and password."	Use your own Trino login. On Galaxy, your email and role, such as ann@corvanta.com/analyst.
"Trino estimates this query would read about ..., more than this source's limit of ..."	Select fewer columns or filter on partition columns, or ask an admin to raise max_scan_bytes.
"... took too long to run this query, so it was stopped."	Narrow the query.
"Trino says you do not have access (...)"	Query a table you can read, or ask your Trino admin for access.

What you see	What to do
"... does not let SourceLace set its query time and size limits ..."	Ask your Trino admin to allow the two session properties, or set <code>session_limits</code> to off.
"... is a private network address ..."	Use the cluster's public address.
"... could not be reached."	Check host, and that the cluster allows SourceLace's IP addresses.
"Table functions (TABLE(...)) are not allowed ..."	Query the tables directly.