Enable User Analytics

Contents:

This section describes how to enable or disable logging of user activities and transfer of the logs to Trifacta®. When this feature is enabled, user activities are captured locally on the Trifacta node in a series of log files. Periodically, these log files are uploaded to a predefined S3 bucket, where Trifacta can ingest the logging activity to improve the product and assist in troubleshooting.

Tip: This feature is useful for providing better suggestions and machine-based learning to the Trifacta platform instance.

NOTE: During initial deployment, this service may be enabled for you. You can use the information below to disable the service.

Trifacta captures the following types of usage information, which are available in different releases.

- These can be separately enabled.
- For more information on the data that is captured, see *https://community.trifacta.com/s/article/Trifacta-Usage-Data-Collection-1515802070895*.

Analytics Type	Description
Trifacta Analytics	Trifacta proprietary capture of information about the Trifacta platform
Segment Analytics	Analytics for various common data segments, such as Google and Marketo.

Configuration Steps

The following configuration steps must be completed:

1. Customer must file a request with *Trifacta Support* when this service is to be enabled for the first time.
2. Services must be enabled on the Trifacta node.
3. Open user logging port, if not already opened.
4. Generate and publish credentials.
5. Define cron job to upload logs.

Customer Requests

To enable this service, customers must file a support ticket with *Trifacta Support*. In your request, please include a request for the appropriate API write key values to insert in the configuration. Details are below.

Configure for Platform Analytics

The platform's custom-built telemetry system is controlled by the following config field in You can apply this change through the *Admin Settings Page* (recommended) or

`trifacta-conf.json`

. For more information, see *Platform Configuration Methods*.:

Property	Description
`"webapp.client.enableUserEventLogging"`	When set to `true`, enable logging of user events via client-side telemetry.

Configure for Segment Analytics

You can apply this change through the *Admin Settings Page* (recommended) or

`trifacta-conf.json`

. For more information, see *Platform Configuration Methods*.

The following settings apply to segment analytics.

Property	Description
`"webapp.enableAnalytics": false,`	When `true`, segment analytics are globally enabled. When `false`, no data is recorded for any segment or forwarded to any channel.
`"webapp.analytics.segmentWriteKey": "<YOUR_VALUE_HERE>",`	For remote analytics, this property identifies the segment API writeKey matching the project to which to push. Within the Segment project lives the configuration for each sink (e.g Google Analytics, Marketo). **NOTE:** For more information on the key value to insert, please contact *Trifacta Support*.
`"webapp.analytics.enabledChannels": ["Log","Amplitude"],`	The channels for which to record data: `Log` | `Google Analytics` | `Marketo` | `Amplitude` | <future sink>. `Log` is the default channel. For remote analytics, this value and the `segmentWriteKey` are independent, enabling two points of control. For example, if you wanted Marketo to receive analytics, you'd need to include it in `enabledChannels` and also hook up that integration for your project in Segment.

1. Make changes to the above properties as needed.
2. Save your changes and restart the platform.

Configure for Amplitude Analytics client-side SDK

Property	Description

`"telemetry.amplitude.client.enabled"`	When set to `true`, enable logging of user events via Amplitude's client-side SDK.
`"telemetry.amplitude.client.writeKey"`	**NOTE:** For more information on the key value to insert, please contact *Trifacta Support*.

Open user logging port

NOTE: To receive the full benefits of this feature, the Trifacta node must be able to connect to the public Internet.

On the server hosting the Trifacta platform, the following port must be opened:

- Port 80 (HTTP) and/or
- Port 443 (HTTPS)

Create credentials file

To connect to S3, the Trifacta platform requires that a set of credentials be generated and stored in the following directory. This credentials is provided by Trifacta.

```
/opt/trifacta/bin/log-forwarding
```

Generate cron job

To regularly upload the generated logs to Trifacta, you can configure a cron job to transfer the files.

Steps:

1. Create an agent or script to periodically run the node process `log-forwarding.js`. You should run this once per day.
2. An example command to run this script from the deployment directory is the following:

```
node bin/log-forwarding/src/log-forwarding.js protobuf-events.log segment-proto.log cleaned-join-logs.txt
```

Disable

To disable the service, set `webapp.enableAnalytics` to `false`. Then, restart the platform.