How is the Data Secured on the Exalate Server for Jira Cloud?

Last Modified on 11/17/2022 7:41 am EST

Atlassian requires that any 'add-on' technology runs on a separate server. This is calledAtlassian Connect.

Relevant data for the functioning of the add-on will be exchanged with the vendors' servers. The same applies to Exalate.

Whenever an issue is updated, a webhook will be called. It triggers the Exalate logic to collect all relevant data such as specified in the outgoing sync processor (Sync Rules).

This communication is secured via HTTPS and JWT.

In case ***the Destination side is on the private network*** the issue data resides on the Exalate Cloud servers until the destination Jira instance requests for any changes. These changes will then be sent to the Jira Server - and that communication is normally also secured via HTTPS. The information on the Exalate cloud server is removed.

In case ***the Destination side is publicly accessible*** the issue data resides on the Exalate Cloud server until the app filters and processes changes. These changes will then be sent to the Destination Jira Instance - and that communication is normally also secured via HTTPS. The information on the Exalate cloud server is removed.

Contrary to the common implementation model as prescribed by Atlassian, Exalate cloud apps are single-tiered.

Meaning - that the operation and handling of the data are fenced from any other interference.