|  |  |  |
| --- | --- | --- |
| Step | URL | Picture |
| Login to SumoLogic | [Login-As-Admin-User](https://service.jp.sumologic.com/ui/#/home) |  |
| Navigate to Connections | **Manage Data 🡪**  **Settings 🡪**  **Connections** |  |
| Click “+” to Add |  |  |
| Fill in Data | **Name:** Add name  **URL:** IMPORTANT!!!  Add URL from Slack Step |  |
| Test Connection | **Should be Green: 200** | Then Save Connection |
| Navigate to Build new Query | If no Sources, use \_view=sumologic\_activity | \_view=\*  | json field=\_raw "user\_activity" nodrop  | count by user\_activity |
| Execute Query | Confirm Results |  |
| Save Query |  |  |
| Edit Search | Schedule a Search |  |
| Specify Webhook | * Specify Frequency * Specify Search Time * Specify Conditions   + Greater > 0   + Alert on this * Use Webhook * Choose Defined hook   Sumo-Slack-Test-Connection |  |
| Save | Wait and View Channel |  |