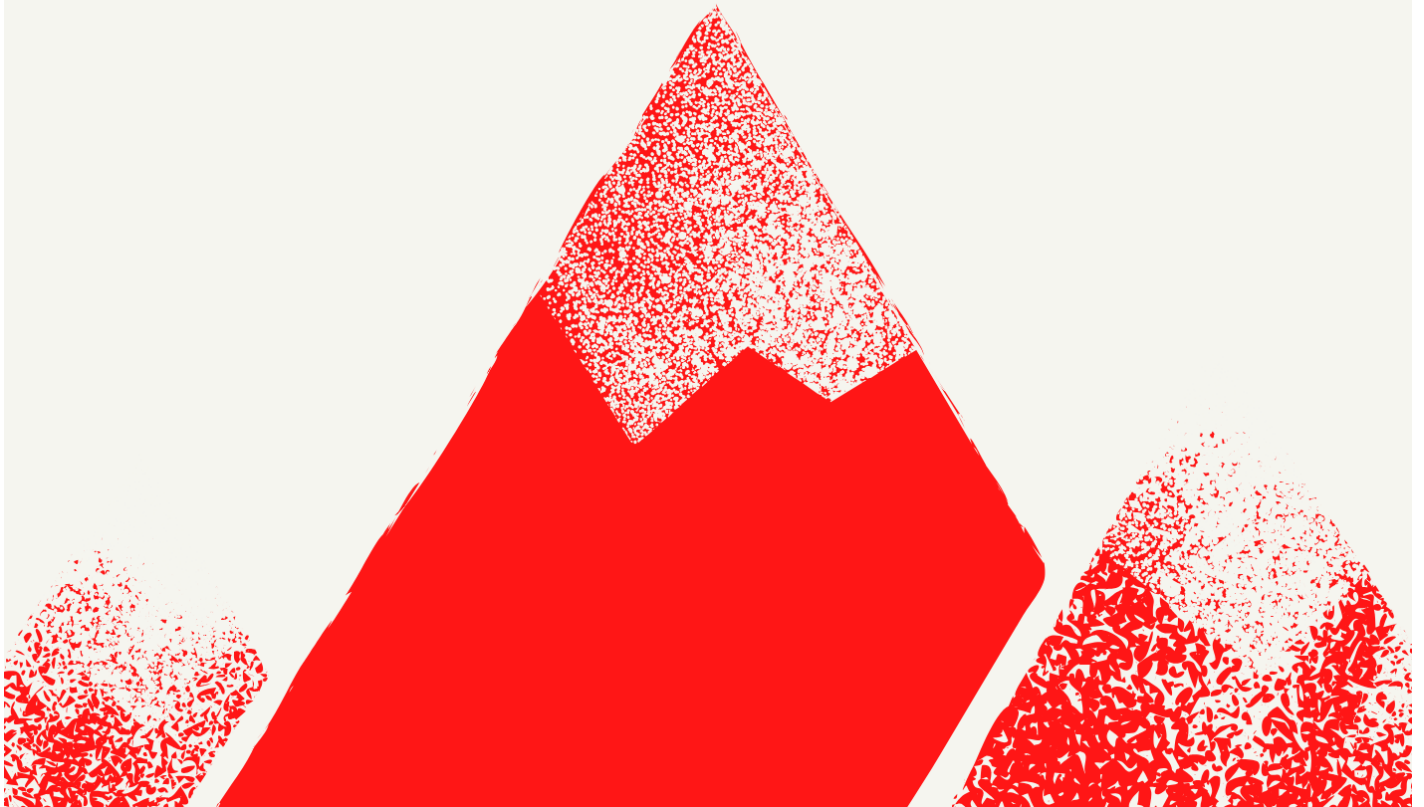


# G O G S C O N F I G U R A T I O N





# Gogs

A painless self-hosted Git service.

## Table of Contents

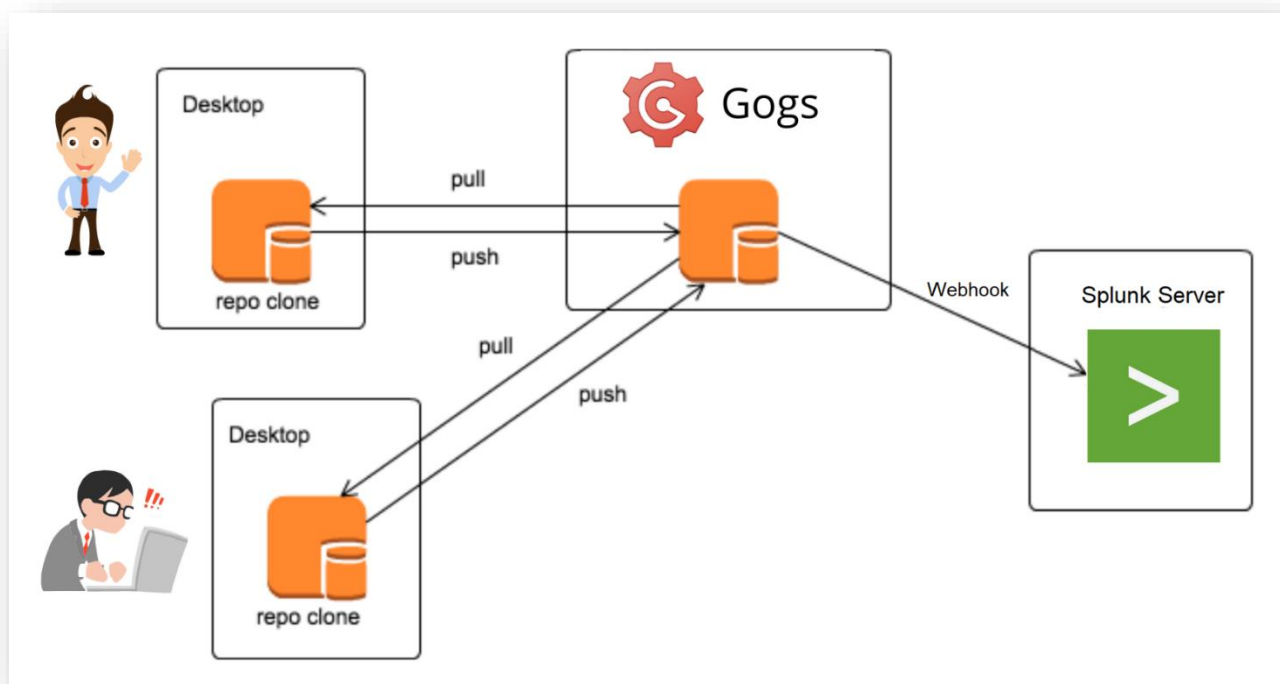
Overview.....	2
Splunk .....	2
Pre-requisite.....	2
Configuration in Gogs .....	3
Configuration in Splunk .....	4
Searching.....	7
Gogs App for Splunk.....	7
Home:.....	7
Issues.....	8
Troubleshooting.....	9
Summary .....	9

# Overview

Gogs application is Version control System (VCS) software. It can also be used to control Splunk Configuration. It is 100% open source, backed by Salesforce and free of charge. It also has webhook option to send payload to Splunk. Whenever an activity occurs in Gogs, it does a POST request with an event to the target forwarder of Splunk.

## Splunk

Splunk Inc. (NASDAQ: SPLK) is the market leader in analyzing machine data to deliver Operational Intelligence for security, IT and the business. Splunk® software provides the enterprise machine data fabric that drives digital transformation. Splunk Enterprise makes it simple to collect, analyze and act upon the untapped value of the big data generated by your technology infrastructure, security systems and business applications—giving you the insights to drive operational performance and business results.



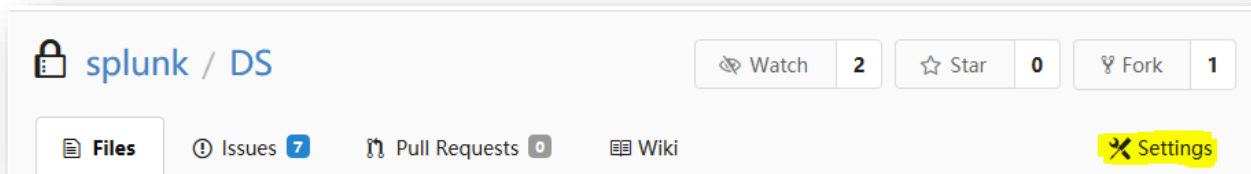
## Pre-requisite

Before proceeding with configuration make sure to install below app and add-on in Splunk.

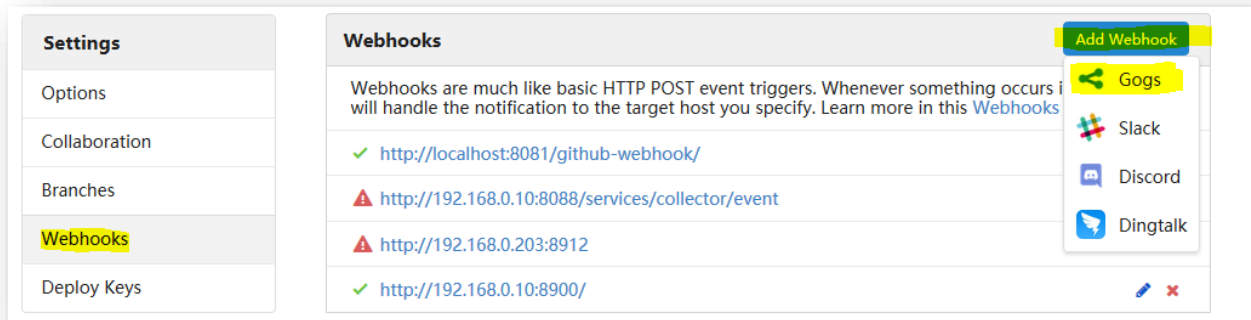
- Webhook Inputs: <https://splunkbase.splunk.com/app/3308>
- Sankey Diagram: <https://splunkbase.splunk.com/app/3112>
- Calendar Heat Map: <https://splunkbase.splunk.com/app/3162>

# Configuration in Gogs

1. Admin user can login into the account and click on Setting.



2. Click on Webhook and then click on Add Webhook and select Gogs.



3. Specify HF/UF ip address with any port e.g. `http://192.168.0.10:8900`  
Note: - Make sure port is open
4. Select content type `application/json`

## 5. Select "I need everything" option and save the settings

### Add Webhook

Gogs will send a POST request to the URL you specify, along with details regarding the event that occurred. You can also specify what kind of data format you'd like to get upon triggering the hook (JSON, x-www-form-urlencoded, XML, etc). More information can be found in our [Webhooks Guide](#).

**Payload URL \***

192.168.0.10:8900

**Content Type**

application/json

**Secret**

Secret will be sent as SHA256 HMAC hex digest of payload via x-Gogs-Signature header.

**When should this webhook be triggered?**

☐ Just the push event

☒ I need everything

☐ Let me choose what I need

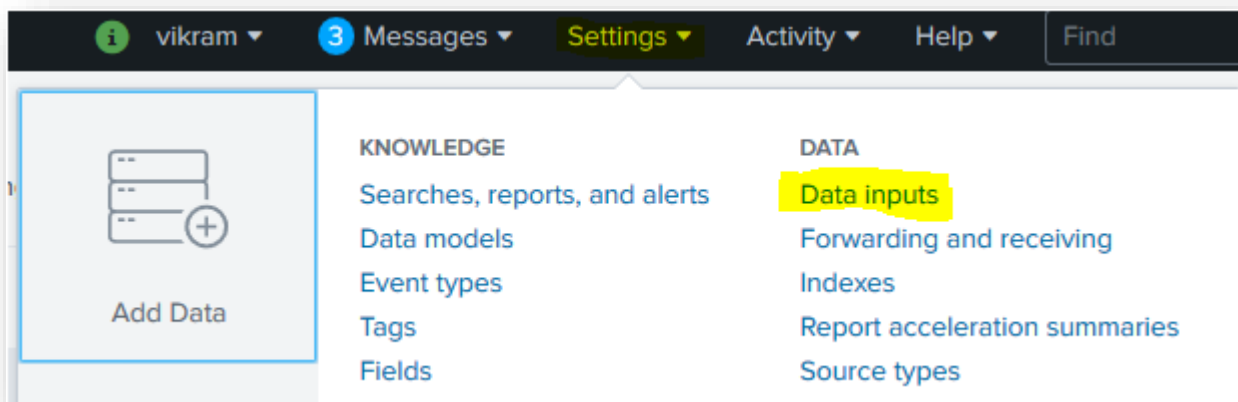
☒ Active

Details regarding the event which triggered the hook will be delivered as well.

Add Webhook

## Configuration in Splunk

### 1. Open Setting and click on Data inputs



## 2. Search for Webhook and then click on Add new

Local inputs		
Type	Inputs	Actions
<a href="#">Local event log collection</a> Collect event logs from this machine.	-	Edit
<a href="#">Remote event log collections</a> Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	+ Add new
<b>Webhook</b> Retrieve information from a webhook	2	<b>+ Add new</b>
<a href="#">Local performance monitoring</a> Collect performance data from local machine.	4	+ Add new
<a href="#">Remote performance monitoring</a> Collect performance and event information from remote hosts. Requires domain credentials.	0	+ Add new
<a href="#">HTTP Event Collector</a> Receive data over HTTP or HTTPS.	4	+ Add new

## 3. Specify name and port no. and in path use wildcard.

### Retrieve information from a webhook

name \*

gogs

Port \*

The port to run the web-server on

8900

Path

A wildcard that the path of requests must match (paths generally begin with a "/" and can include a wildcard)

\*/

SSL Certificate File

The path to the SSL certificate file (if you want to use encryption); typically uses .DER, .PEM, .CRT, .CER file extensions

SSL Certificate Key File

The path to the SSL certificate key file (if the certificate requires a key); typically uses .KEY file extension

More settings

☐

4. Click on more settings, select sourcetype as manual and specify sourcetype as gogs. (Rest other entries fill as needed)

More settings ☒

**Source type**

Set sourcetype field for all events from this source.

Set sourcetype Manual

Set to automatic and Splunk will classify and assign sourcetype automatically. Unknown sourcetypes will be given a placeholder name.

Source type \* gogs

If this field is left blank, the default value will be used for the source type.

**Host**

Set the host with this value.

Host Avotrix-PC

**Index**

Set the destination index for this source.

Index main

5. Click Submit



**Modular input has been created successfully.**

Configure your inputs by going to Settings > [Data Inputs](#)

# Searching

The screenshot shows the Splunk Search interface. At the top, the search bar contains the query: `(index=gogs OR index=infra OR index=main) sourcetype=gogs`. Below the search bar, it indicates 31 events found for the time range 5/20/20 12:00:00.000 AM to 6/19/20 7:59:22.000 PM. The interface includes tabs for Events (31), Patterns, Statistics, and Visualization. A timeline visualization shows a single green bar representing the event duration. Below the timeline, a table lists the search results. The table has columns for Time and Event. The first event is dated 6/17/20 at 9:42:11.000 PM. The event details are truncated in the screenshot.

Time	Event
6/17/20 9:42:11.000 PM	sender.email=vikram@scanlytics.in sender.username=vikram sender.avatar_url=https://secure.gravatar.com/avatar/68701aaa174b0a5f06f3a911807d1199?d=identicon sender.full_name="Vikram Yadav" sender.id=23 sender.login=vikram repository.description="This is a directory where all the deployment servers app will be stored and processes." repository.parent=None repository.updated_at=2020-06-17T20:23:17+05:30 repository.clone_url=http://repo.avotrix.com:3000/splunk/DS.git repository.open_issues_count=7 repository.empty=False repository.created_at=2019-11-14T01:30:08+05:30 repository.fork=False repository.mirror=False repository.id=8 repository.private=True repository.stars_count=0 repository.ssh_url=Avotrix@localhost:splunk/DS.git repository.default_branch=master repository.owner.email=splunk@avotrix.com repository.owner.username=splunk repository.owner.avatar_url=https://secure.gravatar.com/avatar/54796b5750927e9407510567f6dbf787?d=identicon repository.owner.full_name="" repository.owner.id=10 repository.y.owner.login=splunk repository.size=52983808 repository.forks_count=0 repository.website="" repository.html_url=http://repo.avotrix.com:3000/splunk/DS repository.name=DS repository.full_name=splunk/DS repository.watchers_count=2 forkee.description="Th

## Gogs App for Splunk

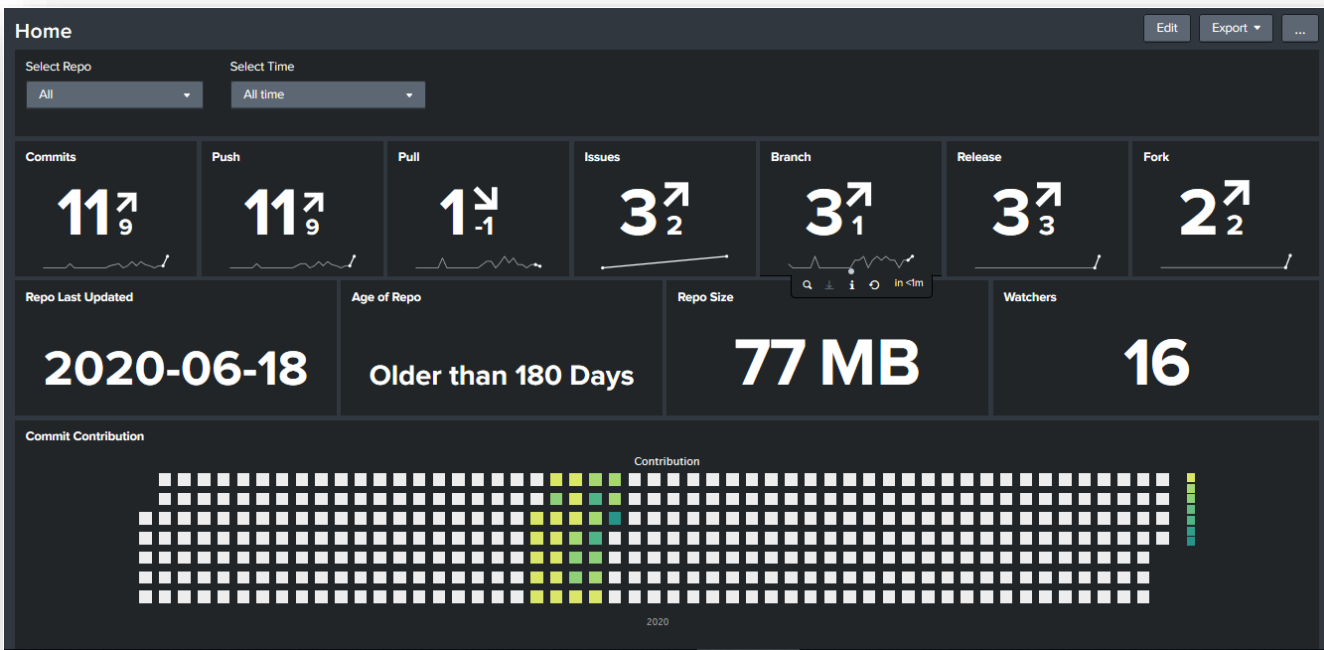
The Gogs app for Splunk offers a rich set of pre-built dashboards to analyze and visualize data from Gogs – including file created, modified, deleted, issues, pull request, commits, fork and release - all in single, free app.

Each dashboard panel contains dynamic inputs like select repository, user name and time.

## Home:

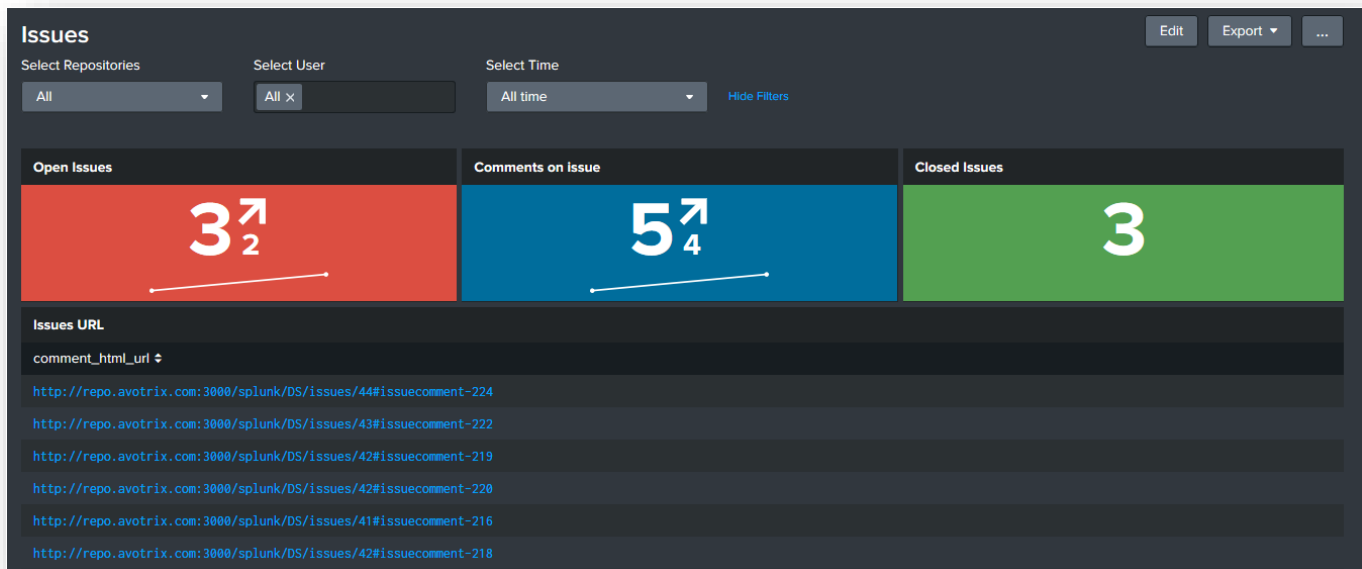
It has overall summary for all records including commits, pull, push, issues, release, fork, last update on repo with its size and age of the repo, and much more.





## Issues

This dashboard contains open issues, closed issues, comment on any of the issues. Each panel has multiple drilldowns which shows more details.



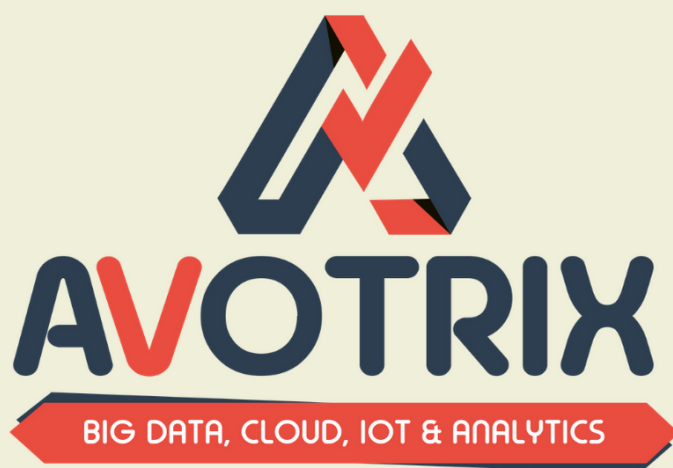
## Troubleshooting

What to do if data doesn't show up in the Dashboards?

1. Go to Settings > Data Inputs > Webhook. Verify that you enabled a port.
2. Verify sourcetype="gogs".
3. Please do change the index name in macro `gogs\_index`

## Summary

Gogs App for Splunk can help you give more insights over Gogs Application activities by forwarding events to Splunk.



# Contact us

A-3/105, BLDG No. 2, Sector 1, MBP, Mahape  
Navi Mumbai - 400 710

+91 989 244 4251 +91 777 700 4497

[support@avotrix.com](mailto:support@avotrix.com)