Splunk

Queries

Count Events per Index

```
| tstats count WHERE index=* OR index=_* by index
```

List Indexes

```
| eventcount summarize=false index=* | dedup index | fields index
```

Installation on Linux

Install Indexer / Heavy Forwarder

```
sudo useradd -m -d /opt/splunk -s /bin/bash -U splunk && \
sudo tar xzvf ~/splunk.tgz -C /opt && \
sudo chown -R splunk:splunk /opt/splunk && \
sudo su -c "/opt/splunk/bin/splunk start --accept-license" splunk
```

Configure Receiver to receive data

https://docs.splunk.com/Documentation/Splunk/9.1.2/Forwarding/Enableareceiver

```
export user=user
export password=password
export port=9997
sudo su -c "/opt/splunk/bin/splunk enable listen ${port} -auth
${user}:${password}" splunk
```

Set-Up Forwarding

https://docs.splunk.com/Documentation/Splunk/9.1.2/Forwarding/Deployaheavyforwarder

```
export user=user
export password=password
export host=indexer
export port=9997
```

```
sudo su -c "/opt/splunk/bin/splunk enable app SplunkForwarder -auth
${user}:${password}" splunk && \
sudo su -c "/opt/splunk/bin/splunk restart" splunk && \
sudo su -c "splunk add forward-server ${host}:${port} -auth
${user}:${password}" splunk && \
sudo su -c "/opt/splunk/bin/splunk restart" splunk
```

Forward to more than one destinations

/opt/splunk/etc/system/local/outputs.conf

outputs.conf

```
[tcpout]
defaultGroup = group1,group2
indexAndForward = 0

[tcpout:group1]
disabled = false
server = receiver1:9997

[tcpout:group2]
disabled = false
server = receiver2:9997
```

Universal Forwarder

```
useradd -m -d /opt/splunkforwarder -s /bin/bash -U splunkfwd && \
sudo tar xzvf ~/splunk-forwarder.tgz -C /opt && \
sudo chown -R splunkfwd:splunkfwd /opt/splunkforwarder && \
sudo /opt/splunkforwarder/bin/splunk start --accept-license
```

kb, splunk

From:
http://fortytwo.adurias.org/ - **Fortytwo - Answer to the Ultimate Question of Life, the Universe, and Everything**

Permanent link:
http://fortytwo.adurias.org/splunk?rev=1704962408

Last update: **2024/01/11 09:40**