Getting started with the Splunk App for ConsenSys Quorum

The [OSS Quorum App for Splunk](#) contains a set of dashboards and analytics to give you full visibility into the system metrics, application data and ledger so that you can maintain security, stability and performance for your ConsenSys Quorum deployment. This application is an [open source blockchain project](#).

These free blockchain dashboards are meant to be a starting point for building analytics around your Quorum blockchain no matter where it is deployed.

The App provides you with several dashboards to get you started with analyzing your Quorum deployment. These include:

- **Data Setup** - A dashboard to show you what data is being received by Splunk.
- **Raw Data Flow** - A dashboard showing the data flowing in from each Quorum node and data source.
- **Infrastructure Health and Monitoring** - An overview of system health from system metrics like CPU, uptime status as well as transaction latency. You can see in real time when transactions are starting to back up or a node is falling behind on blocks.
- **Transaction Analytics** - Cryptocurrency dashboard with real time visibility into the transactions being written on the ledger. See a breakdown of private vs public transactions and analytics around addresses.
- **Ledger Query** - Query the ledger to consult event and cryptocurrency data.

You can configure three different types of data sources to use all of the dashboards. Not all of these data sources are required to use the app.

1. **Quorum Blocks, Transactions, and Events** - These logs contain transaction information from the ledger itself and provide insight into operations and actions on-chain. We’ve open sourced [Splunk Connect for Ethereum](#) to help you easily ingest Quorum ledgers in Splunk.
2. **Quorum node logs and metrics** - These are logs and metrics specific to a Quorum node. Specifically, Quorum application logs, Prometheus metrics, RPC data polled from different Quorum node endpoints (i.e. admin_peers, txpool_content, etc -- see [Splunk Connect for Ethereum](https://github.com/ethereum/splunk-connector) for more information).

3. **Infrastructure/System Level Metrics and Logs** - System metrics such as CPU, MEM, DISK and NETWORK activity provide insight into the underlying infrastructure Quorum nodes are running on. These metrics/logs could come from physical machines, Docker, Kubernetes, IBM IKS, Microsoft Azure, Google’s GCP and AWS Cloudwatch to name a few. Splunk has different Add-ons and connectors for each.

## Getting started

1. Install the App on a Splunk Enterprise Search Head that will have access to the data.

2. Open the App and navigate to the **Data Setup** dashboard from the Introduction Page.

3. Follow the instructions for each of the 3 data sources on the Data Setup page in order to populate the graphs and validate that data is coming in correctly.

   - **Quorum Block and Transaction Data** - [Splunk Connect for Ethereum](https://github.com/ethereum/splunk-connector) is an open source agent that connects to each node on the Quorum network. See its Readme for deployment instructions. Docker, Kubernetes, and native deployments are all options.

   - **Quorum node logs and metrics** - You will need to **create event and metric indexes** in Splunk as well as an input mechanism to receive the data. It's recommended to create an index called "ethereum" and "metrics" and enable the Splunk HEC to receive data. You can use the example `indexes.conf.example` provided in the app. Simply rename the file from `indexes.conf.example` to `indexes.conf` to enable the indexes, and rename `inputs.conf.example` to `inputs.conf` to enable the HEC endpoints. You will also need to enable the HTTP Event Collector (HEC) to receive data if it has not been enabled already.

    ```bash
    $ cd $SPLUNK_HOME/etc/apps/splunk-app-quorum/default
    $ sudo mv inputs.conf.example inputs.conf
    $ sudo mv indexes.conf.example indexes.conf
    $ cd /opt/splunk/bin
    $ sudo ./splunk restart
    ```

   - **Quorum node JSON-RPC data** - Quorum nodes also have RPC endpoints that [Splunk Connect for Ethereum](https://github.com/ethereum/splunk-connector) can poll and send to Splunk. This can be used to monitor transaction pool activity on a node, active peers, or leader election in Raft or Istanbul. In order for this to work, the required endpoints need to be whitelisted on the Quorum node. See the Readme at [Splunk Connect for Ethereum](https://github.com/ethereum/splunk-connector) for more information.

   - **System Logs/Metrics** - Depending on how you’ve deployed your Quorum network, you can get your system logs and metrics into Splunk for end-to-end visibility. On the data setup dashboard there is a list of common options that you can use to get your data in.

   Possible environments you can use are:

   - Docker: [Splunk Docker Logging Driver](https://www.splunk.com/appitionalcapabilities/docker-logging)
   - Kubernetes: [Splunk Connect for Kubernetes](https://github.com/ibm-symantec/splunk-connector-k8s)
   - Log File: [Monitoring Files and Directories with Splunk](https://www.splunk.com/appitionalcapabilities/monitoring-log-files-and-directories)
   - IBM Cloud Platform: [IBM Cloud Platform](https://www.ibm.com/cloud/)

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
• Microsoft Azure: Splunk Add-on for Microsoft Cloud Services
• AWS Cloudwatch: Splunk App for AWS
• GCP Stackdriver: Splunk Add-on for Google Cloud