Getting started with Splunk Connect for Ethereum

Splunk Connect for Ethereum (aka ethlogger) makes it easy to ingest data about Ethereum ledgers, node information, and node metrics into another system for analysis. Currently, it can log to the Splunk HTTP Event Collector and stdout. It can also deserialize transactions and events if given a contract ABI. Some benefits include:

- Support for any Ethereum 1.0 JSON-RPC compatible blockchain or sidechain, including Quorum
- Reliably saves state between restarts so you never have missing or duplicated events
- Highly performant batching and compression algorithm
- Extracts a rich set of node information and metrics in order to gain deep insight into your node
- Introspects your node platform (i.e. geth, parity, besu or quorum) in order to ensure maximum data extraction
- Contract fingerprinting in order to match ABIs with function signatures (i.e. parameter names can be decoded too)
- Enables dashboards

Usage

```bash
$ ethlogger [...options]
```

Details about ethlogger's command-line usage can be found in the CLI docs.

Configuration

Find out how to configure ethlogger in the configuration docs.

Docker

Splunk Connect for Ethereum can be run in a docker container. You can pull the image from the GitHub container registry.

Example:

```bash
$ docker run -it ghcr.io/splunkdlt/ethlogger:latest \
   --eth-rpc-url=https://dai.poa.network \
   --start-at-block=latest \
   --hec-url=https://mysplunkserver.com:8088 \
   --hec-token=123-123-123-123 \
   --hec-events-index=main \
   --hec-metrics-index=metrics
```

There is also an example of how to run ethlogger in docker-compose.
Troubleshooting

There's a lot of information available via RPC on Ethereum nodes, but they need to be enabled via the command line on startup for ethlogger to connect. See the relevant docs for:

- **Geth and Quorum Docs** or you can turn it all on: --rpcapi admin,db,eth,debug,miner,net,shh,txpool,personal,web3
- Quorum Specific Endpoints: --rpcapi quorum,istanbul,raft (note: only one of istanbul or raft is active depending on the consensus method)
- Geth and Quorum: ensure that the host ethlogger is running on is whitelisted in the --rpcvhosts cli setting.
- **OpenEthereum (Parity) Endpoints**: note that the command line flag is --jsonrpc-apis APIs
- **Besu Endpoints** or you can turn on: --rpc-http-enabled --rpc-ws-enabled --rpc-http-api admin,eth,debug,miner,net,txpool,priv,trace,web

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.