



Log Schemas in Zeek

Introducing the logschema package

Christian Kreibich
christian@zeek.org

Logs are the reason people use Zeek

- Powerful from the get-go, and extremely adaptable
- Add new ones, extend existing ones, filter columns, etc
- If you customize your Zeek, chances are your logs are unique
- Knowing what your logs look like, and when they change, is key
 - How does package XYZ change my logs?
 - What changed from my current Zeek version to the latest?
- So far Zeek has provided no tooling to answer these questions

Log schema, *n*

- A structured blueprint or template that defines the format, fields, and data types of a log message
- A database schema, but for system logs
- Describes a specific instance of a log format (JSON, CSV, syslog, etc)

JSON Schema is the go-to for JSON data

- JSON that describes JSON
- Standardized, with lots of features & tooling
- A constraint language: it accepts anything it doesn't explicitly restrict
- Enables log validation

```
{
  "$schema": "https://json-schema.org/draft/2020-12/schema",
  "title": "Schema for Zeek conn.log",
  "description": "JSON Schema for Zeek conn.log",
  "type": "object",
  "properties": {
    "ts": {
      "description": "This is the time of the first packet.",
      "type": "number",
      "examples": [
        1737691432.132607
      ],
    },
    "x-zeek": {
      "type": "time",
      "record_type": "Conn::Info",
      "script": "base/protocols/conn/main.zeek"
    }
  },
  "uid": {
    "description": "A unique identifier of the connection.",
    "type": "string",
    "x-zeek": {
      "type": "string",
      "record_type": "Conn::Info",
      "script": "base/protocols/conn/main.zeek"
    }
  }
}
```

...

The logschema package

\$ zkg install logschema

- A script-only package to produce schemas for your Zeek logs
- Includes four exporters:
 - **CSV**: good for diffing
 - **Custom JSON**: simple & Zeek-centric
 - **JSON Schema**: a must
 - **Zeek log**: for easy integration
- Uses type reflection and logging APIs to query log configuration at runtime
 - Log field name, Zeek type, parent record, optionality, default value, docstring, defining script / package
 - Gets the details right: log filters, log extensions, etc

\$ zkg install logschema

- Supports fingerprints: check if log structure has changed
 - A hash of the logs' names, field names, and Zeek types
 - Faster than doing full schema production & diffing
- Fully extensible — add your own exporters or customize
- Runs after all `zeek_init` handlers, or when you invoke it
 - Possible blindspot if your scripts create / adjust log streams later
- Supports Zeek 5.2 and newer, with some details from 6.0+

 **logschema** Public[Edit Pins](#) [Unwatch 3](#) [Fork 2](#) [Star 3](#)[main](#) 2 Branches 10 Tags

Go to file

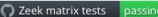
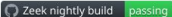
Add file

<> Code

 ckreibich Merge branch 'topic/dubem/fix-optional-nested-record'  		34c39de · last week	 70 Commits
 .github/workflows	CI: add jq so we don't skip a bunch of tests due to failed r...	last year	
 scripts	Propagate &optional through record field unfolding	last week	
 testing	Propagate &optional through record field unfolding	last week	
 COPYING	Add license and some skeleton zkg.meta content	last year	
 README.md	Update README to cover schema fingerprints	4 months ago	
 zkg.meta	Remove summary from zkg.meta	10 months ago	

[README](#) [BSD-3-Clause license](#)

Log Schema Support for Zeek

This [Zeek](#) package generates schemas for Zeek's logs. For every log your Zeek installation produces (such as conn.log or tls.log) the schema describes each log field including name, type, docstring, and more. The package supports popular schema formats and understands Zeek's log customization in detail. The schema export code is extensible, allowing you to produce your own schemas.

Quickstart

Install this package via `zkg install logschema`. The package has no dependencies and currently works with Zeek 5.2 and newer.

To get a [JSON Schema](#) of each Zeek log in your installation, run:

```
$ zeek logschema/export/jsonschema
```

About

A Zeek package that generates schemas for your log files.

[Readme](#)[BSD-3-Clause license](#)[Activity](#)[Custom properties](#)[3 stars](#)[3 watching](#)[2 forks](#)[Audit log](#)[Report repository](#)

Releases 5

 [v2.2.0](#) Latest
last week[+ 4 releases](#)

Contributors 2

 ckreibich Christian Kreibich J-Gras Jan

Languages



- Zeek 96.2%
- Shell 3.7%
- Makefile 0.1%

Demo

Thanks!

Documentation

<https://docs.zeeq.org>

Community links

<https://zeeq.org/community>

Github project

<https://github.com/zeeq>

Project wiki

<https://github.com/zeeq/zeeq/wiki>