LOGZILLA DOCUMENTATION

Forwarding to Splunk

Reduce Splunk ingest costs by forwarding LogZilla deduplicated events with an ORIGIN marker, then mapping source hosts via Splunk transforms.conf and props.conf

Forwarding To Downstream Receivers · Generated June 12, 2026 · logzilla.ai/docs/forwarding-module/forwarding-to-splunk

LogZilla NEO may also be used to reduce the amount of data sent to Splunk systems while, at the same time, generating more value in that data.

LogZilla's deduplication reduces repeated events at ingest so Splunk does not have to process large bursts during event storms. The forwarding module works the same way in terms of configuration on the LogZilla side. On the Splunk side, a transform can be used to indicate the original sending host so that Splunk does not attribute all events to the LogZilla system itself.

Source host marker

To help Splunk determine the correct source host, the forwarder rule should append a key/value pair to the forwarded message. The recommended key name is `ORIGIN` (for example: `message: $MESSAGE ORIGIN="$HOST"`). See the forwarder rule examples in Downstream Syslog Receivers (https://www.logzilla.ai/docs/forwarding-module/downstream-syslog-receivers).

Splunk Setup

On the Splunk server, create or edit `$SPLUNK_HOME/etc/system/local/transforms.conf` and add:

Splunk Transforms

```
[logzilla_forwarder]
REGEX = ORIGIN=(\S+)
FORMAT = host::$1
DEST_KEY = MetaData:Host
```

Next, create or edit the file `$SPLUNK_HOME/etc/system/local/props.conf` and associate the transform to the source. In the case of this example (https://www.logzilla.ai/docs/forwarding-module/downstream-syslog-receivers), this guide is sending everything via TCP port 514, so the source used in Splunk's `props.conf` will be that.

Splunk Props

```
[source::tcp:514]
TRANSFORMS-lz_neo=logzilla_forwarder
```

For options on Splunk's transforms and props files, please reference Splunk's Documentation (https://docs.splunk.com/Documentation/Splunk/latest/Data/Overridedefaulthostassignments) for further help.

Verify and reload

After editing forwarder rules and reloading Splunk configs:

```
# Inspect the merged forwarder configuration from LogZilla
logzilla forwarder print

# Reload the forwarder to apply rule changes
logzilla forwarder reload
```