

Zeek without ZeekControl

Arne Welzel

September 10 2026

Agenda

- Background: Where is this coming from?
- Zeek as a Multi-Process Application
- Running a Zeek Cluster
- `zeek.conf` / `zeek-systemd-generator`
 - Single Host Cluster Example
 - Interface and Environment Templating
 - Multi Host Cluster Example
 - Definitely does less than ZeekControl!
- Non-Linux / Non-systemd / Containers

Background: Where is this coming from?

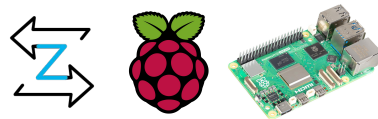
- Corelight Appliance

- There's never been ZeekControl
- Log streaming / archival - mostly out of scope



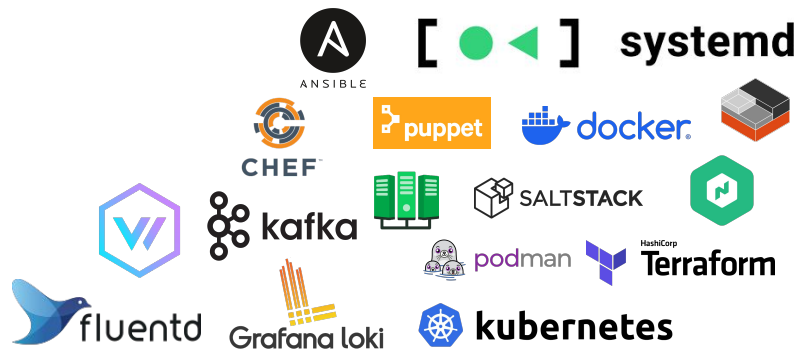
- Corelight@Home

- Single configuration file for a single host
- Integrated process supervisor

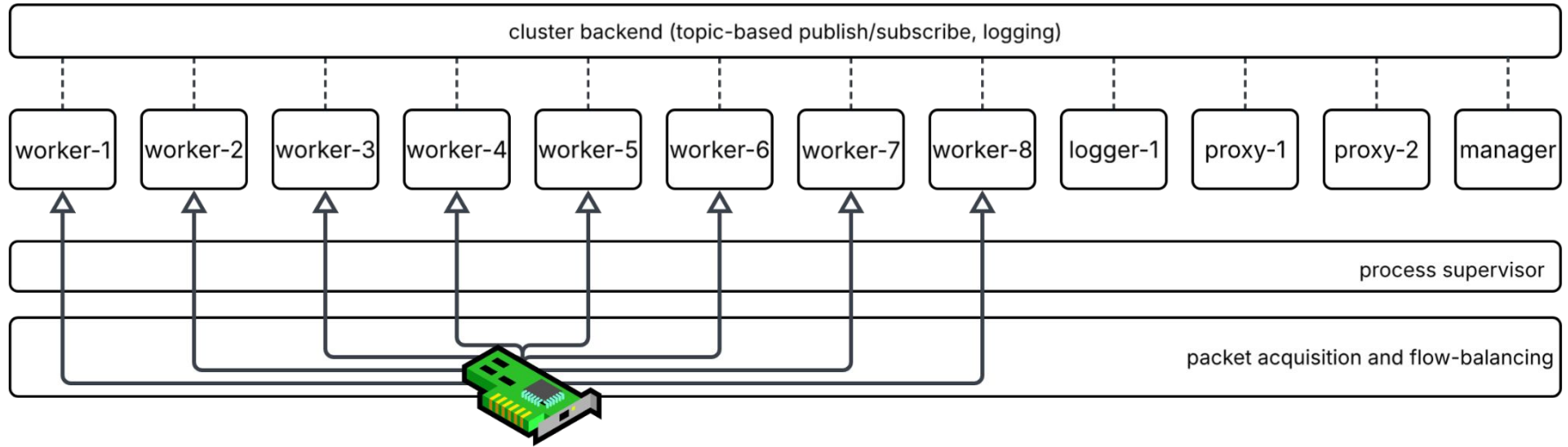


- 2010s vs 2026

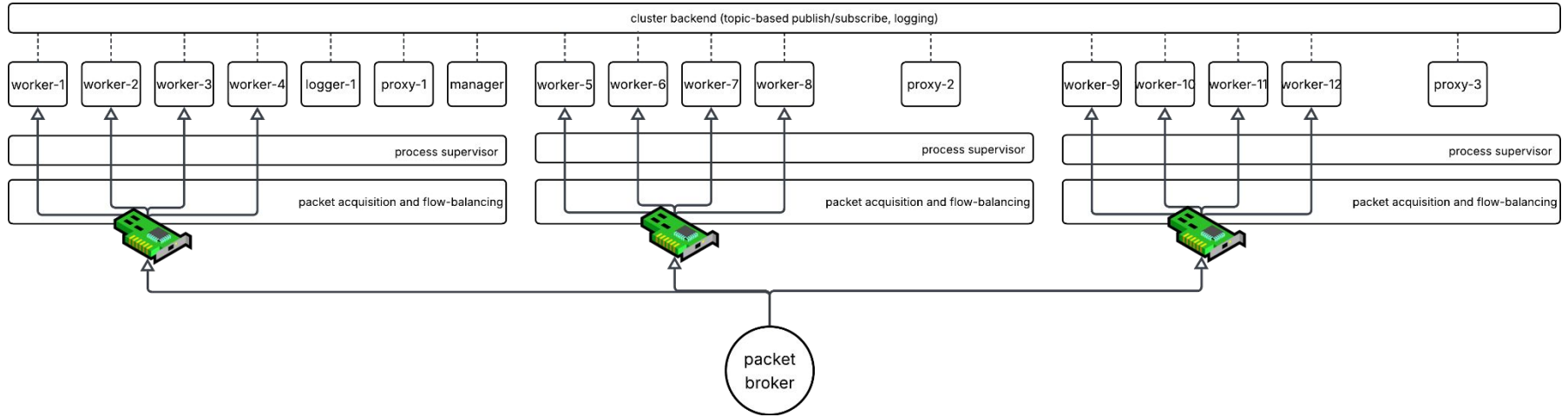
- Linux: systemd and containers
- Deployment and configuration management
- Log ingestion and forwarding



Zeek as a Multi-Process Application: Single Host



Zeek as a Multi-Process Application: Multi Host



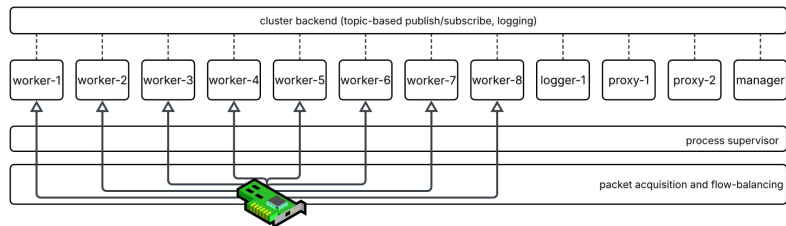
Zeek as a Multi-Process Application: By Hand

```
# zeek-cluster-layout-generator -L 1 -P 2 -W 8 -o cluster-layout.zeek

# export ZEEKPATH=$(pwd):$ZEEKPATH

# mkdir manager && cd manager && CLUSTER_NODE=manager zeek local &
# mkdir logger-1 && cd logger-1 && CLUSTER_NODE=logger-1 zeek local &
# mkdir proxy-1 && cd proxy-1 && CLUSTER_NODE=proxy-1 zeek local &
# mkdir proxy-2 && cd proxy-2 && CLUSTER_NODE=proxy-2 zeek local &

# mkdir worker-1 && cd worker-1 && CLUSTER_NODE=worker-1 zeek -i af_packet::enp7s0 local &
...
# mkdir worker-8 && cd worker-8 && CLUSTER_NODE=worker-8 zeek -i af_packet::enp7s0 local &
```



Running a Zeek Cluster

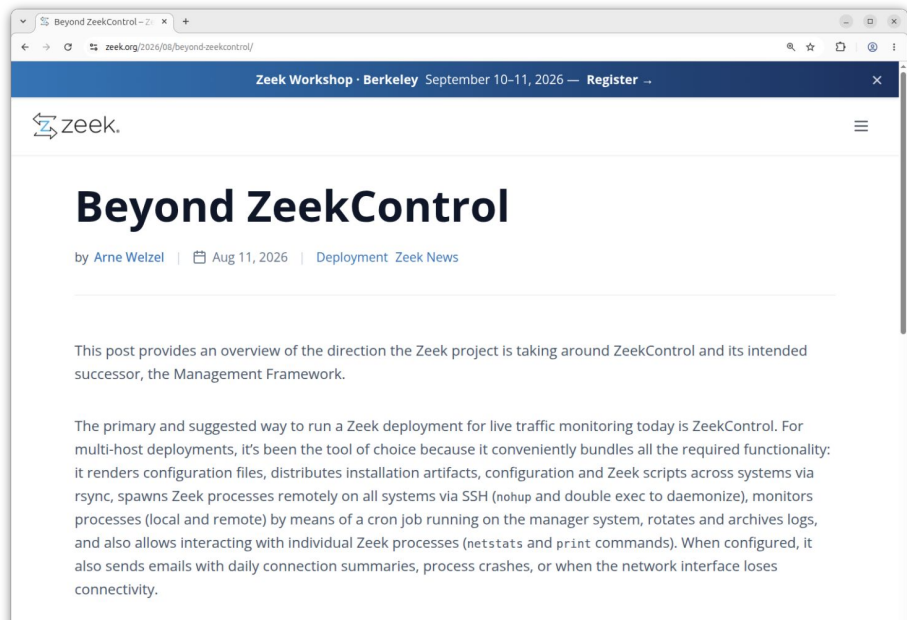
- ZeekControl
 - Does a lot more than just process management!
 - Deploy base Zeek and packages via SSH/rsync
 - Lots of scripts, nohup, state files, config files
 - Memory limits via ulimit, CPU pinning via taskset
 - Cronjob to restart crashed processes (via SSH!)
 - stderr hidden / custom zeekctl commands
- Management Framework
 - Orchestrate Zeek processes via clustered Zeek scripting
 - Number of known users today: 1 (ESnet)
 - Discontinued in 2026
- zeek.conf / zeek-systemd-generator
 - Added in Zeek 8.1, extended with Zeek 9.0
 - ESnet is *adopting* this currently

```
# zeek.service unit file for ZeekControl
[Unit]
Description=Zeek

[Service]
User=zeek
Type=forking
Restart=on-failure
RestartSec=5
ExecStart=/opt/zeek/bin/zeekctl deploy
ExecStop=/opt/zeek/bin/zeekctl stop

[Install]
WantedBy=multi-user.target
```

Running a Zeek Cluster



<https://zeek.org/2026/08/beyond-zeekcontrol/>

zeek.conf: Single Host Cluster

- <PREFIX>/etc/zeek/zeek.conf
- zeek-systemd-generator
 - [systemd.generator\(7\)](#)
- Runs during systemctl daemon-reload
 - ...and during boot.
- systemctl start zeekt.target

```
[zeek]
manager = 1
loggers = 1
proxies = 2

[interface enp7s0]
interface = af_packet::enp7s0
workers = 2

[interface enp8s0]
interface = af_packet::enp8s0
workers = 2
```

zeek.conf: Generated Unit Files

```
# tree /run/systemd/generator | grep zeek
```

```
├─ zeek-archiver.service
├─ zeek-logger@.service
├─ zeek-manager.service
├─ zeek-proxy@.service
├─ zeek-setup.service
├─ zeek-worker-enp7s0@.service
├─ zeek-worker-enp7s0@1.service.d
│   └─ 10-zeek-systemd-generator.conf
├─ zeek-worker-enp7s0@2.service.d
│   └─ 10-zeek-systemd-generator.conf
├─ zeek.target
└─ zeek.target.wants
    ├─ zeek-archiver.service -> ../zeek-archiver.service
    ├─ zeek-logger@1.service -> ../zeek-logger@.service
    ├─ zeek-manager.service -> ../zeek-manager.service
    ├─ zeek-proxy@1.service -> ../zeek-proxy@.service
    ├─ zeek-proxy@2.service -> ../zeek-proxy@.service
    ├─ zeek-setup.service -> ../zeek-setup.service
    ├─ zeek-worker-enp7s0@1.service -> ../zeek-worker-enp7s0@.service
    └─ zeek-worker-enp7s0@2.service -> ../zeek-worker-enp7s0@.service
```

```
[zeek]
manager = 1
loggers = 1
proxies = 2

[interface enp7s0]
interface = af_packet::enp7s0
workers = 2
```

zeek.conf: systemctl status zeek.slice

- zeek.slice - Slice /zeek

```
Loaded: loaded (/usr/lib/systemd/system/zeek.slice; disabled; preset: enabled)
Active: active since Wed 2026-09-09 18:11:30 UTC; 14min ago
Invocation: fe56343be558440287ba5c943743d2df
Act. Units: 12
Tasks: 116
Memory: 651.2M (peak: 654M)
CPU: 15.376s
CGroup: /zeek.slice
├─zeek-archiver.slice
│   └─zeek-archiver.service
│       └─1182 /opt/zeek/bin/zeek-archiver /opt/zeek/var/spool/zeek/log-queue /opt/zeek/var/logs/zeek
├─zeek-loggers.slice
│   └─zeek-logger@1.service
│       └─1184 /opt/zeek/bin/zeek frameworks/cluster/backend/zeromq policy/misc/systemd-generator local
├─zeek-manager.slice
│   └─zeek-manager.service
│       └─1186 /opt/zeek/bin/zeek frameworks/cluster/backend/zeromq policy/misc/systemd-generator local
├─zeek-proxies.slice
│   ├──zeek-proxy@1.service
│   │   └─1200 /opt/zeek/bin/zeek frameworks/cluster/backend/zeromq policy/misc/systemd-generator local
│   └─zeek-proxy@2.service
│       └─1187 /opt/zeek/bin/zeek frameworks/cluster/backend/zeromq policy/misc/systemd-generator local
└─zeek-workers.slice
    ├──zeek-worker-enp7s0@1.service
    │   └─1223 /opt/zeek/bin/zeek -i af_packet::enp7s0 frameworks/cluster/backend/zeromq policy/misc/systemd-generator local
    └─zeek-worker-enp7s0@2.service
        └─1214 /opt/zeek/bin/zeek -i af_packet::enp7s0 frameworks/cluster/backend/zeromq policy/misc/systemd-generator local
```

```
[zeek]
manager = 1
loggers = 1
proxies = 2

[interface enp7s0]
interface = af_packet::enp7s0
workers = 2
```

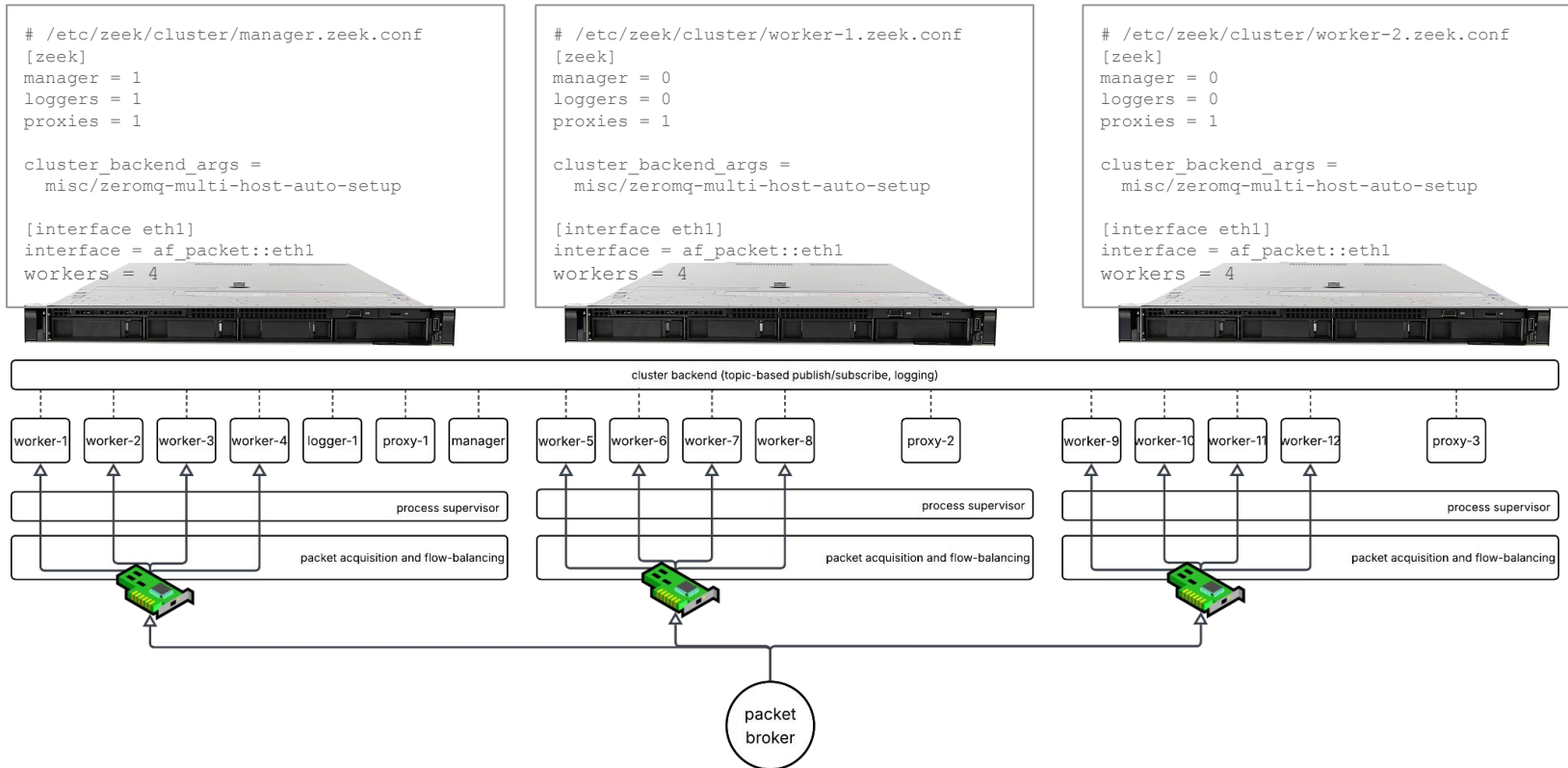
zeek.conf: Multi Host Zeek Cluster

zeek.conf: Multi Host Zeek Cluster

- <PREFIX>/etc/zeek/zeek.conf is for single host deployments
- For a multi host cluster, create a configuration file for each host
 - name it <hostname>.zeek.conf
 - place all configs of all hosts into /etc/zeek/cluster/
- systemctl daemon-reload && systemctl start zeek.target
- Et voila 🎉

```
# tree <PREFIX>/etc/zeek/cluster/  
<PREFIX>/etc/zeek/cluster/  
├── manager.zeek.conf  
├── worker-1.zeek.conf  
└── worker-2.zeek.conf
```

zeek.conf: Multi Host Zeek Cluster



zeek.conf: Interface and Environment Templating

<pre>[interface napatech] interface = napatech::\${worker_index0} workers = 2</pre>	<pre>zeek -i napatech::0 zeek -i napatech::1</pre>
<pre>[interface netmap] interface = netmap::eth1}\${worker_index0} workers = 2</pre>	<pre>zeek -i netmap::eth1}0 zeek -i netmap::eth1}1</pre>
<pre>[interface veth] interface = af_packet::veth\${worker_index} workers = 2 worker_env = MY_INTERFACE=veth\${worker_index}</pre>	<pre>zeek -i af_packet::veth1 zeek -i af_packet::veth2 and MY_INTERFACE env set</pre>
<pre>[interface pfring] interface = eth1 workers = 2 worker_env = PCAP_PF_RING_CLUSTER_ID=42 PCAP_PF_RING_USE_CLUSTER_PER_INNER_FLOW_5_TUPLE=1</pre>	<pre>zeek -i eth1 zeek -i eth1 requires PF_RING's libpcap</pre>

zeek.conf: Definitely doing less than ZeekControl!

- Defines details about which Zeek processes (nodes) run on a host
 - ...and not much more
- Interface Configuration
 - ZeekControl plugins for (AF_PACKET, PF_RING, custom, ...)
 - zeek.conf: **interface**, **worker_args** and **worker_env** options
- Logging Configuration and Archival Options
 - Very basic. Use Zeek scripting for customization
- No more networks.cfg file
 - Use redef Site::local_nets

Non-Linux / Non-systemd / Containers

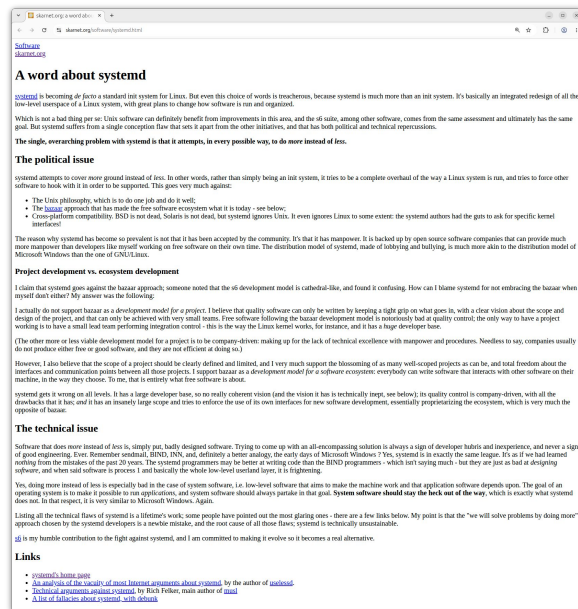
- zeek-systemd-generator
 - Reads zeek.conf and generates unit files

- zeek-s6-generator
 - Probably s6-rc
 - Anyone interested?
 - Other ideas?



- Containers

- systemd in a container is fine 👍
- Otherwise: How about s6-overlay?



<https://skarnet.org/software/systemd.html>

Questions / Discussion

```
[zeek]
manager = 1
loggers = 1
proxies = 2

[interface enp7s0]
interface = af_packet::enp7s0
workers = 2

[interface napatech]
interface = napatech::${worker_index0}
workers = 2
```

<https://zeek.org/2026/08/beyond-zeekcontrol/>

<https://docs.zeek.org/en/master/advanced/deployment/systemd.html>