

DLF NETWORKING

Developer & Testing forum

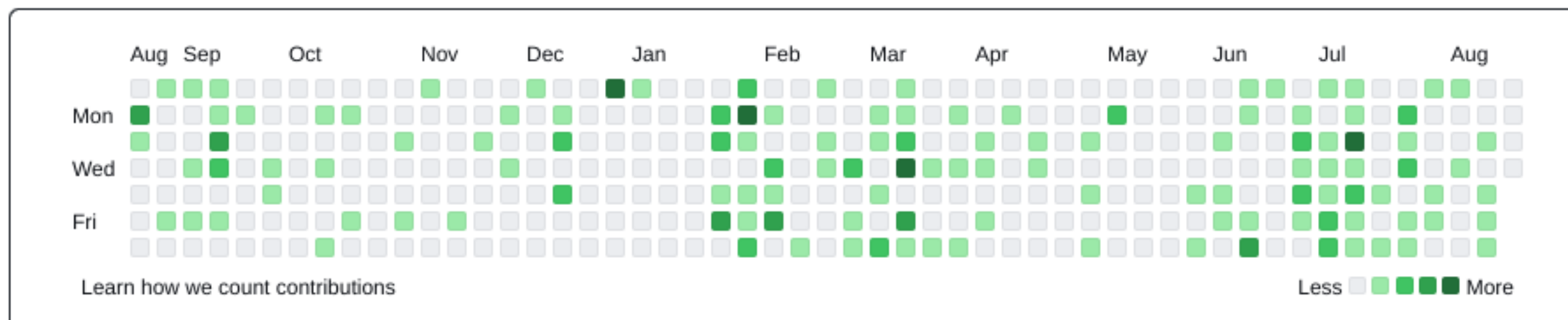
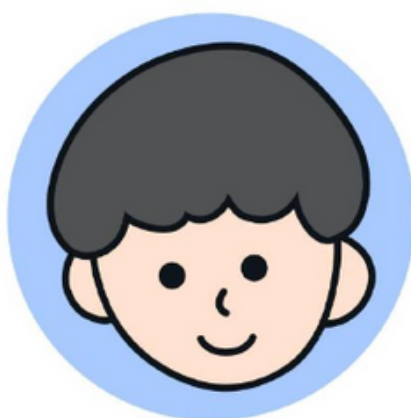
 L3AF on 





SHANKAR
LFN MENTEE

About me:

- SHANKAR
- LFN Mentee 2023 @ L3AF
- Student @ University of Delhi
- Researcher @ NgKore
- Opensource Contributor
- Pursuing Undergraduation



Today's Agenda

01. Introduction to L3AF  L3AF
02. Architecture of l3afd
03. Building l3afd on windows  L3AF
04. Running l3afd  
05. Swagger API with l3af
06. Attach sample eBPF program on Windows  + 
07. Testing eBPF-for-Windows with l3af  L3AF +  + 



Introduction to



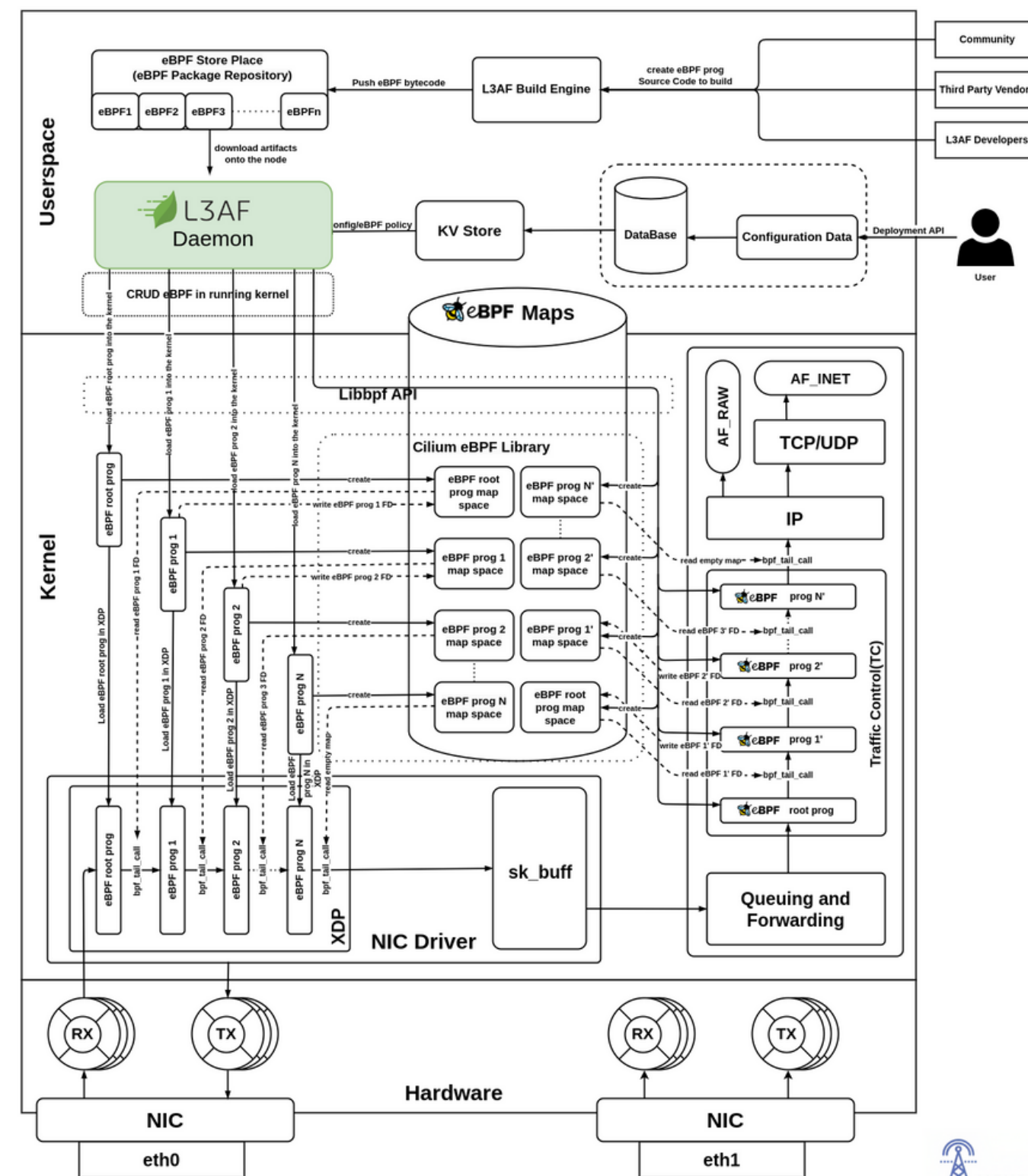
Lightweight eBPF Application



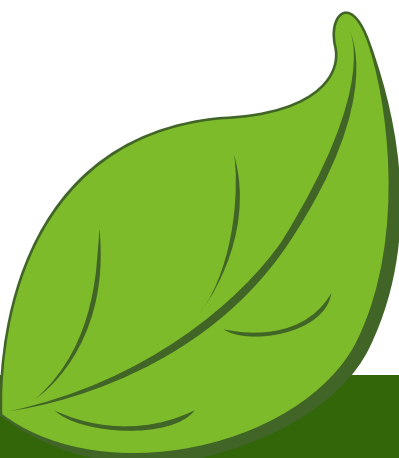
eBPF programs as a Service



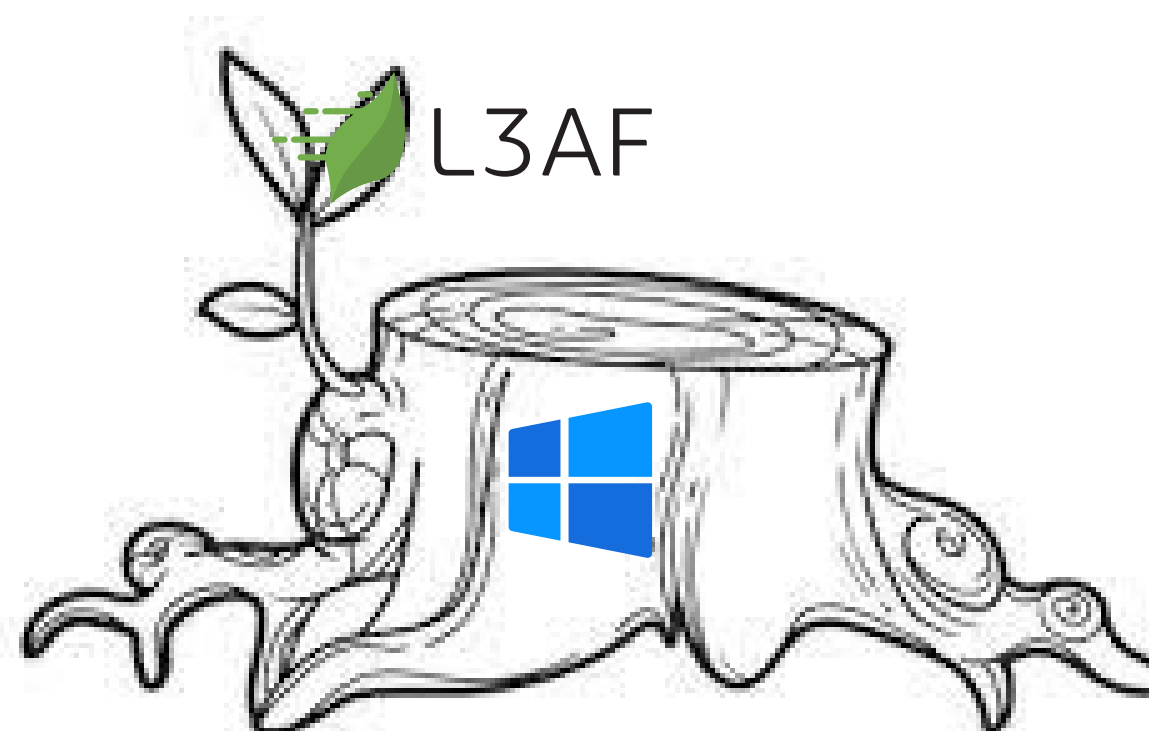
Architecture:



Why leaf was moved on the windows?



Building l3afd on windows



```
C:\l3afd>cmake -B build
-- Building for: Visual Studio 17 2022
-- Selecting Windows SDK version 10.0.22000.0 to target Windows 10.0.22621.
-- The C compiler identification is MSVC 19.36.32535.0
-- The CXX compiler identification is MSVC 19.36.32535.0
-- Detecting C compiler ABI info
-- Detecting C compiler ABI info - done
-- Check for working C compiler: C:/Program Files (x86)/Microsoft Visual Studio/2022/BuildTools/VC/Tools/MSVC/14.36.32532/bin/Hostx64/x64/cl.exe - skipped
-- Detecting C compile features
-- Detecting C compile features - done
-- Detecting CXX compiler ABI info
-- Detecting CXX compiler ABI info - done
-- Check for working CXX compiler: C:/Program Files (x86)/Microsoft Visual Studio/2022/BuildTools/VC/Tools/MSVC/14.36.32532/bin/Hostx64/x64/cl.exe - skipped
-- Detecting CXX compile features
-- Detecting CXX compile features - done
-- Configuring done (6.9s)
-- Generating done (0.1s)
-- Build files have been written to: C:/l3afd/build
```

Steps to build l3afd on windows:

```
C:\l3afd>cmake --build build
MSBuild version 17.6.3+07e294721 for .NET Framework
```

```
1>Checking Build System
Generating C:/l3afd/l3afd.exe
Building Custom Rule C:/l3afd/CMakeLists.txt
Generating C:/Users/l3af/go/bin/swag.exe
Building Custom Rule C:/l3afd/CMakeLists.txt
Generating C:/l3afd/docs/docs.go, C:/l3afd/docs/swagger.json, C:/l3afd/docs/swagger.yaml
2023/07/09 05:18:21 Generate swagger docs...
2023/07/09 05:18:21 Generate general API Info, search dir:./
2023/07/09 05:18:23 Generating models.L3afBPFPrograms
2023/07/09 05:18:23 Generating models.BPFPrograms
2023/07/09 05:18:23 Generating models.BPFProgram
2023/07/09 05:18:23 Generating models.L3afDNFArgs
2023/07/09 05:18:23 Generating models.L3afDNFMetricsMap
2023/07/09 05:18:23 Generating models.L3afBPFProgramNames
2023/07/09 05:18:23 Generating models.BPFProgramNames
2023/07/09 05:18:23 create docs.go at docs/docs.go
2023/07/09 05:18:23 create swagger.json at docs/swagger.json
2023/07/09 05:18:23 create swagger.yaml at docs/swagger.yaml
Building Custom Rule C:/l3afd/CMakeLists.txt
```


Running l3afd on windows



```

PS C:\l3afd> .\l3afd.exe
2023-07-07T16:36:01Z INF l3afd started.
2023-07-07T16:36:01Z INF Reading configuration from: config/l3afd.cfg
2023-07-07T16:36:01Z INF Using default value TLS_1.3 after failure to read group:mtls; field:min-tls-version error="option not found: min-tls-version"
2023-07-07T16:36:01Z INF Using default value 5 after failure to read group:l3afd; field:kernel-major-version error="option not found: kernel-major-version"
2023-07-07T16:36:01Z INF Using default value 1 after failure to read group:l3afd; field:kernel-minor-version error="option not found: kernel-minor-version"
2023-07-07T16:36:01Z INF Using default value after failure to read group:xdp-root-program; field:name error="option not found: name"2023-07-07T16:36:01Z INF Using default
t value after failure to read group:xdp-root-program; field:artifact error="option not found: artifact"
2023-07-07T16:36:01Z INF Using default value after failure to read group:xdp-root-program; field:ingress-map-name error="option not found: ingress-map-name"
2023-07-07T16:36:01Z INF Using default value after failure to read group:xdp-root-program; field:command error="option not found: command"
2023-07-07T16:36:01Z INF Using default value after failure to read group:xdp-root-program; field:version error="option not found: version"
2023-07-07T16:36:01Z INF Using default value after failure to read group:tc-root-program; field:name error="option not found: name"
2023-07-07T16:36:01Z INF Using default value after failure to read group:tc-root-program; field:artifact error="option not found: artifact"
2023-07-07T16:36:01Z INF Using default value after failure to read group:tc-root-program; field:ingress-map-name error="option not found: ingress-map-name"
2023-07-07T16:36:01Z INF Using default value after failure to read group:tc-root-program; field:egress-map-name error="option not found: egress-map-name"
2023-07-07T16:36:01Z INF Using default value after failure to read group:tc-root-program; field:command error="option not found: command"
2023-07-07T16:36:01Z INF Using default value after failure to read group:tc-root-program; field:version error="option not found: version"
2023-07-07T16:36:01Z INF Using default value server.crt after failure to read group:mtls; field:server-cert-filename error="option not found: server-cert-filename"
2023-07-07T16:36:01Z INF Using default value after failure to read group:mtls; field:san-match-rules error="option not found: san-match-rules"
2023-07-07T16:36:01Z INF Checking for another already running instance (using PID file "C:\\var\\l3afd\\l3afd.pid")...
2023-07-07T16:36:01Z INF Found PID file with PID: 4276; checking if it is this process: PID: 6368
2023-07-07T16:36:01Z INF Found PID file with PID: 4276; checking if process is running...
2023-07-07T16:36:01Z INF Process was not running, removing PID file.
2023-07-07T16:36:01Z INF Writing process ID 6368 to C:\\var\\l3afd\\l3afd.pid...
2023-07-07T16:36:01Z WRN Implement custom registration with management server
2023-07-07T16:36:01Z INF l3afd config server setup started on host l3af
2023-07-07T16:36:01Z WRN no persistent config exists
2023-07-07T16:36:01Z INF Route added:{Method:POST Path:/l3af/configs/{version}/update HandlerFunc:0xf0d360}

2023-07-07T16:36:01Z INF Route added:{Method:GET Path:/l3af/configs/{version}/{iface} HandlerFunc:0xf0c840}

2023-07-07T16:36:01Z INF Route added:{Method:GET Path:/l3af/configs/{version} HandlerFunc:0xf0ce00}

2023-07-07T16:36:01Z INF Route added:{Method:POST Path:/l3af/configs/{version}/add HandlerFunc:0xf0ba20}

2023-07-07T16:36:01Z INF Route added:{Method:POST Path:/l3af/configs/{version}/delete HandlerFunc:0xf0c180}

2023-07-07T16:36:01Z INF l3afd server listening - localhost:53000

```

Swagger API with l3af

Swagger Supported by SMARTBEAR

doc.json Explore

L3AFD APIs ^{1.0}

[Base URL: /]
[doc.json](#)

Configuration APIs to deploy and get the details of the eBPF Programs on the node

default ^

- GET** `/l3af/configs/v1` Returns details of the configuration of eBPF Programs for all interfaces on a node
- POST** `/l3af/configs/v1/add` Adds new eBPF Programs on node
- POST** `/l3af/configs/v1/delete` Removes eBPF Programs on node
- POST** `/l3af/configs/v1/update` Update eBPF Programs configuration
- GET** `/l3af/configs/v1/{iface}` Returns details of the configuration of eBPF Programs for a given interface



Testing eBPF-for-Windows with l3af



- Working with payload files
- Run payload.json using l3afd

```
"host_name": "l3af",
"iface": "Ethernet",
"bpf_programs": {
  "xdp_ingress": [
    {
      "name": "port_quota",
      "seq_id": 1,
      "artifact": "port_quota.exe",
      "cmd_start": "port_quota.exe",
      "version": "debug",
      "user_program_daemon": true,
      "admin_status": "enabled",
      "prog_type": "xdp",
      "cfg_version": 1,
      "start_args": {
        "load": "load"
      }
    }
  ]
}
```

curl -X POST <http://localhost:53000/l3af/configs/v1/add> -d "@cfg/payload.json"

Continued Agenda

I. XDP PROGRAM

- *Introduction to rate-limiting*
- *Loading xdp eBPF program using l3afd*
- *Unloading xpd eBPF program uing l3afd*
- *Codebase Changes*

II. MONITORING AND OBSERVABILITY

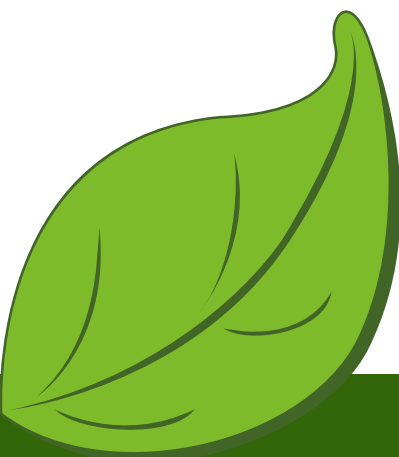
- *Monitoring eBPF programs on dashboard using l3afd*
- *With the help on Prometheus and Grafana*
- *Windows Exporter for exporting metrics*

III. INTRODUCING ETW TRACING

- *Introduction to rate-limiting*
- *Loading xdp eBPF program using l3afd*
- *Unloading xpd eBPF program uing l3afd*
- *Codebase Changes*

IV. CODE BASE CHANGES AND PR

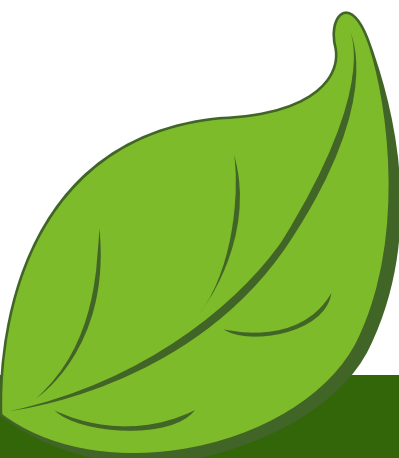
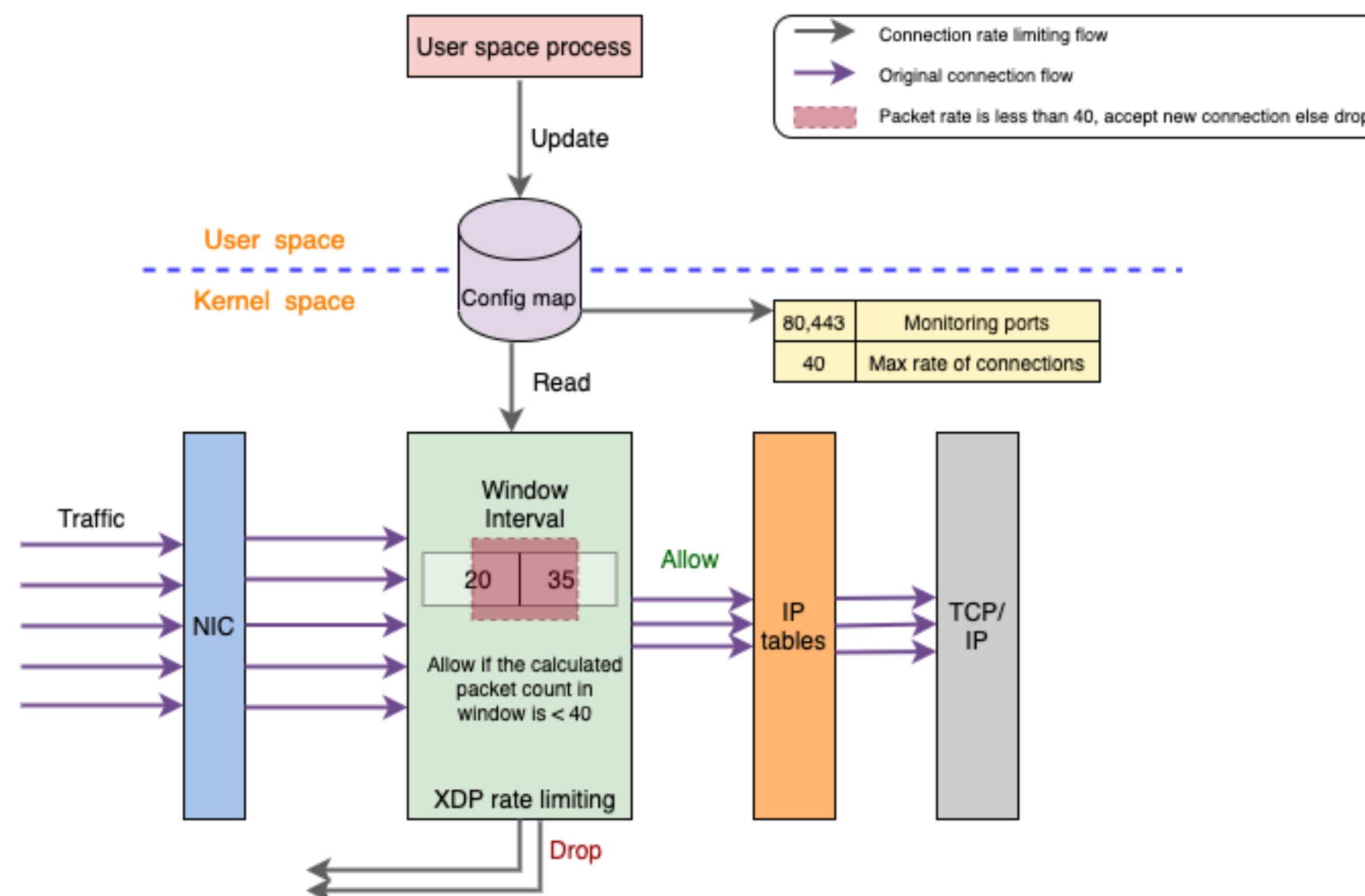
- *l3afd --> [l3af-on-windows #262](#)*
- *l3af-arch --> [L3af on windows #68](#)*



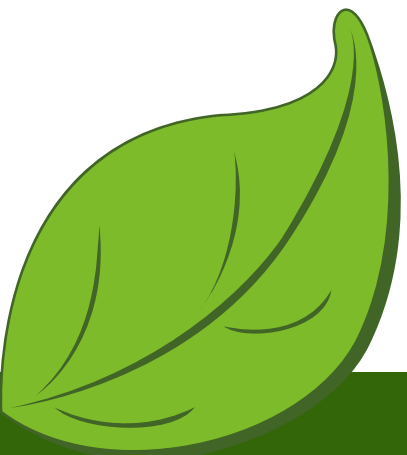
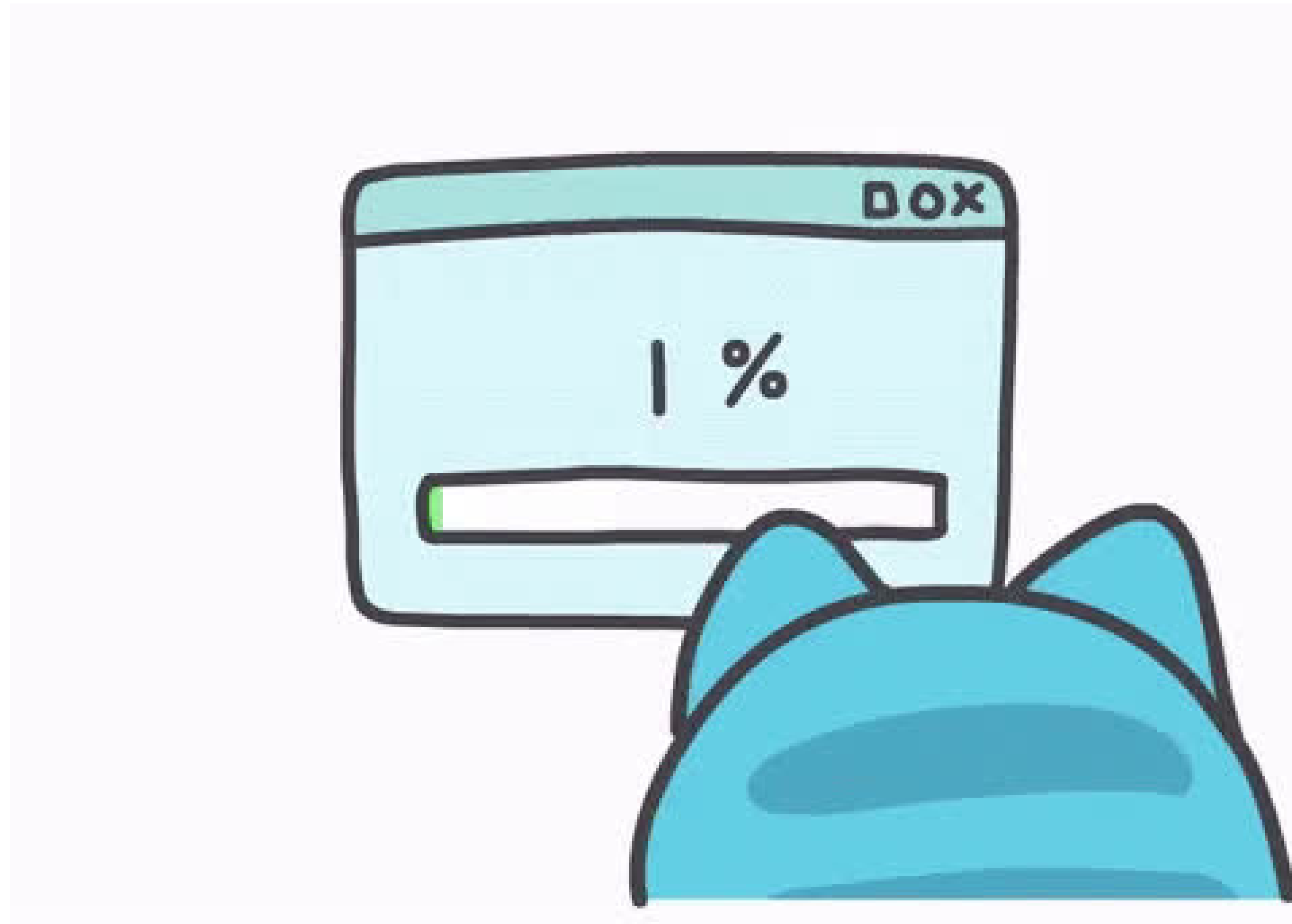
Ratelimiting XDP Program

It uses:

- User Space Program
- Sliding Window Approach
- Input as "traffic rate" --> maximum allowed connection rate per unit of time
- Traffic Patterns --> doesn't require a predefined "traffic burst" value as input. Instead, it adapts to the actual traffic conditions it encounters.



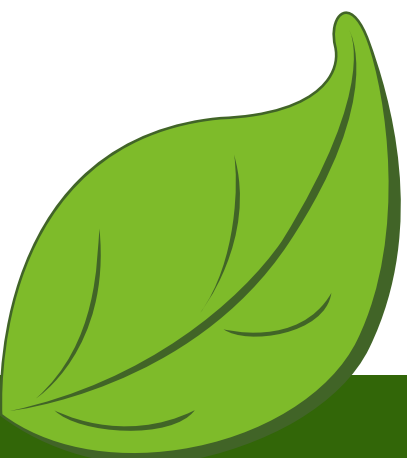
Loading ratelimiting



Ratelimiting Payload

```
[
  {
    "host_name": "13af",
    "iface": "Ethernet4",
    "bpf_programs": {
      "xdp_ingress": [
        {
          "name": "ratelimiting",
          "seq_id": 1,
          "artifact": "ratelimiting.exe",
          "map_name": "xdp_rl_ingress_next_prog",
          "cmd_start": "ratelimiting.exe",
          "version": "latest",
          "user_program_daemon": true,
          "admin_status": "enabled",
          "prog_type": "xdp",
          "cfg_version": 1,
          "start_args": {
            "ports": "80,8080,8081",
            "rate": "2"
          },
          "monitor_maps": [
            {
              "name": "rl_drop_count_map",
              "key": 0,
              "aggregator": "scalar"
            },
            {
              "name": "rl_recv_count_map",
              "key": 0,
              "aggregator": "max-rate"
            }
          ]
        }
      ]
    }
  }
]
```

add_payload_win.json



```
C:\Users\l3af>curl -X POST http://localhost:53000/l3af/configs/v1/add -d "@C:\Users\l3af\Desktop\ratelimiting\leaf\add_payload_win.json"
```

```
PS C:\Users\l3af\Desktop\ratelimiting\leaf> .\l3afd.exe
```

```
2023-09-01T18:20:11Z INF l3afd started.
2023-09-01T18:20:11Z INF Reading configuration from: config/l3afd.cfg

2023-09-01T18:20:11Z INF Starting KF debug server
2023-09-01T18:20:11Z INF Route added:{Method:GET Path:/l3af/configs/{version}/{iface} HandlerFunc:0x7ff60d65be20}

2023-09-01T18:20:11Z INF Route added:{Method:GET Path:/l3af/configs/{version} HandlerFunc:0x7ff60d65c3e0}

2023-09-01T18:20:11Z INF Route added:{Method:POST Path:/l3af/configs/{version}/add HandlerFunc:0x7ff60d65b000}

2023-09-01T18:20:11Z INF Route added:{Method:POST Path:/l3af/configs/{version}/delete HandlerFunc:0x7ff60d65b760}

2023-09-01T18:20:11Z INF l3afd server listening - localhost:53000
2023-09-01T18:20:14Z INF LoadRootProgram iface Ethernet4 direction xdpingress progType xdp
2023-09-01T18:20:14Z INF File path - \var\l3afd\repo\xdp-root\latest\l3af_xdp_root
2023-09-01T18:20:14Z INF Searching for process xdp_root.exe and not ppid 11024
2023-09-01T18:20:14Z INF Start cmd \var\l3afd\repo\xdp-root\latest\l3af_xdp_root\xdp_root.exe
2023-09-01T18:20:14Z INF BPF Program start command : \var\l3afd\repo\xdp-root\latest\l3af_xdp_root\xdp_root.exe [--iface=Ethernet4 --direction=xdpingress --cmd=start]
2023-09-01T18:20:14Z INF Filepath : \var\l3afd\repo\xdp-root\latest\l3af_xdp_root
2023-09-01T18:20:14Z INF Cmd DIR : \var\l3afd\repo\xdp-root\latest\l3af_xdp_root
2023-09-01T18:20:14Z INF user mode BPF program started - xdp-root - UserProgramDaemon : %!d(bool=false)
2023-09-01T18:20:14Z INF no user mode BPF program - xdp-root No Pid%(EXTRA bool=false)
2023-09-01T18:20:14Z INF ingress xdp root program attached
2023-09-01T18:20:14Z INF Push Back and Start XDP program : ratelimiting seq_id : 1
2023-09-01T18:20:14Z INF PushBackAndStartBPF : iface Ethernet4, direction xdpingress
2023-09-01T18:20:14Z INF DownloadAndStartBPFProgram : program name ratelimiting previous program map name: \sys\fs\bpf\xdp_root_pass_array
2023-09-01T18:20:14Z INF File path - \var\l3afd\repo\ratelimiting\latest\ratelimiting
2023-09-01T18:20:14Z INF Successfully verified artifacts
2023-09-01T18:20:14Z INF Searching for process ratelimiting.exe and not ppid 11024
2023-09-01T18:20:14Z INF Start cmd \var\l3afd\repo\ratelimiting\latest\ratelimiting\ratelimiting.exe
2023-09-01T18:20:14Z INF BPF Program start command : \var\l3afd\repo\ratelimiting\latest\ratelimiting\ratelimiting.exe [--iface=Ethernet4 --direction=xdpingress --map-name=\sys\fs\bpf\xdp_root_pass_array --rate=2 --ports=80,8080,8081]
2023-09-01T18:20:14Z INF Filepath : \var\l3afd\repo\ratelimiting\latest\ratelimiting
2023-09-01T18:20:14Z INF Cmd DIR : \var\l3afd\repo\ratelimiting\latest\ratelimiting
2023-09-01T18:20:14Z INF user mode BPF program started - ratelimiting - UserProgramDaemon : %!d(bool=true)
2023-09-01T18:20:14Z INF Inside ELSE b.Program.MapArgs
```

Swagger Output

```
[
  {
    "host_name": "l3af",
    "iface": "Ethernet4",
    "bpf_programs": {
      "xdp_ingress": [
        {
          "id": 0,
          "name": "ratelimiting",
          "seq_id": 1,
          "artifact": "ratelimiting.exe",
          "map_name": "xdp_rl_ingress_next_prog",
          "cmd_start": "ratelimiting.exe",
          "cmd_stop": "",
          "cmd_status": "",
          "cmd_config": "",
          "version": "latest",
          "user_program_daemon": true,
          "is_plugin": false,
          "cpu": 0,
          "memory": 0,
          "admin_status": "enabled",
          "prog_type": "xdp",
          "rules_file": "",
          "rules": "",
          "config_file_path": "",
          "cfg_version": 1,
          "start_args": {
            "ports": "80,8080,8081",
            "rate": "2"
          },
          "stop_args": null,
          "status_args": null,
          "map_args": null,
          "config_args": null,
          "monitor_maps": [
            {
              "name": "rl_drop_count_map",
              "key": 0,
              "aggregator": "scalar"
            },
            {
              "name": "rl_recv_count_map",
              "key": 0,
              "aggregator": "max-rate"
            }
          ]
        },
        {
          "name": "rl_drop_count_map",
          "key": 0,
          "aggregator": "scalar"
        },
        {
          "name": "rl_recv_count_map",
          "key": 0,
          "aggregator": "max-rate"
        }
      ]
    },
    "ebpf_package_repo_url": "",
    "object_file": "",
    "entry_function_name": ""
  }
],
"tc_ingress": null,
"tc_egress": null
}
]
```

```
Curl
curl -X 'GET' \
'http://localhost:53000/l3af/configs/v1' \
-H 'accept: application/json'

Request URL
http://localhost:53000/l3af/configs/v1

Server response
Code    Details
200     Response body
[
  {
    "host_name": "l3af",
    "iface": "Ethernet4",
    "bpf_programs": {
      "xdp_ingress": [
        {
          "id": 0,
          "name": "ratelimiting",
          "seq_id": 1,
          "artifact": "ratelimiting.exe",
          "map_name": "xdp_rl_ingress_next_prog",
          "cmd_start": "ratelimiting.exe",
          "cmd_stop": "",
          "cmd_status": "",
          "cmd_config": "",
          "version": "latest",
          "user_program_daemon": true,
          "is_plugin": false,
          "cpu": 0,
          "memory": 0,
          "admin_status": "enabled",
          "prog_type": "xdp",
          "rules_file": "",
          "rules": "",
          "config_file_path": "",
          "cfg_version": 1,
          "start_args": {
```

```
C:\>netsh ebpf show programs

   ID   Pins  Links  Mode   Type   Name
=====
327690   1     1    JIT   xdp    xdp_root
983046   0     0    JIT   xdp    _xdp_ratelimiting
```



Unloading ratelimiting

```
Curl
curl -X 'POST' \
'http://localhost:53000/l3af/configs/v1/delete' \
-H 'accept: application/json' \
-H 'Content-Type: application/json' \
-d '{
  "bpf_programs": {
    "xdp_ingress": [
      "ratelimiting"
    ]
  },
  "host_name": "l3af",
  "iface": "Ethernet4"
}'

Request URL
http://localhost:53000/l3af/configs/v1/delete

Server response
Code    Details
-----
200     Response headers
        content-length: 0
        content-type: application/json
        date: Tue, 29 Aug 2023 07:39:43 GMT

Responses
Code    Description
-----
200     OK
```

delete_payload_win.json

```
[
  {
    "bpf_programs": {
      "xdp_ingress": [
        "ratelimiting"
      ]
    },
    "host_name": "l3af",
    "iface": "Ethernet4"
  }
]
```

```
C:\Users\l3af>netsh ebf show programs

   ID   Pins  Links  Mode   Type   Name
=====
524293  1      0      JIT    xdp    xdp_root
```



Observability and Monitoring



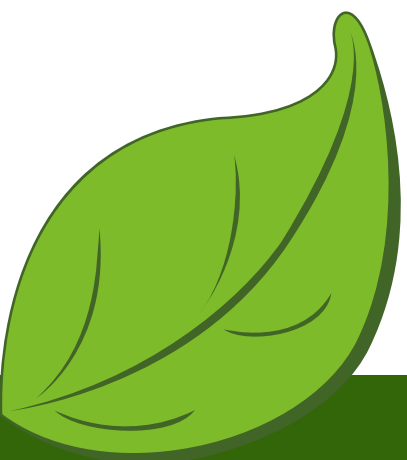
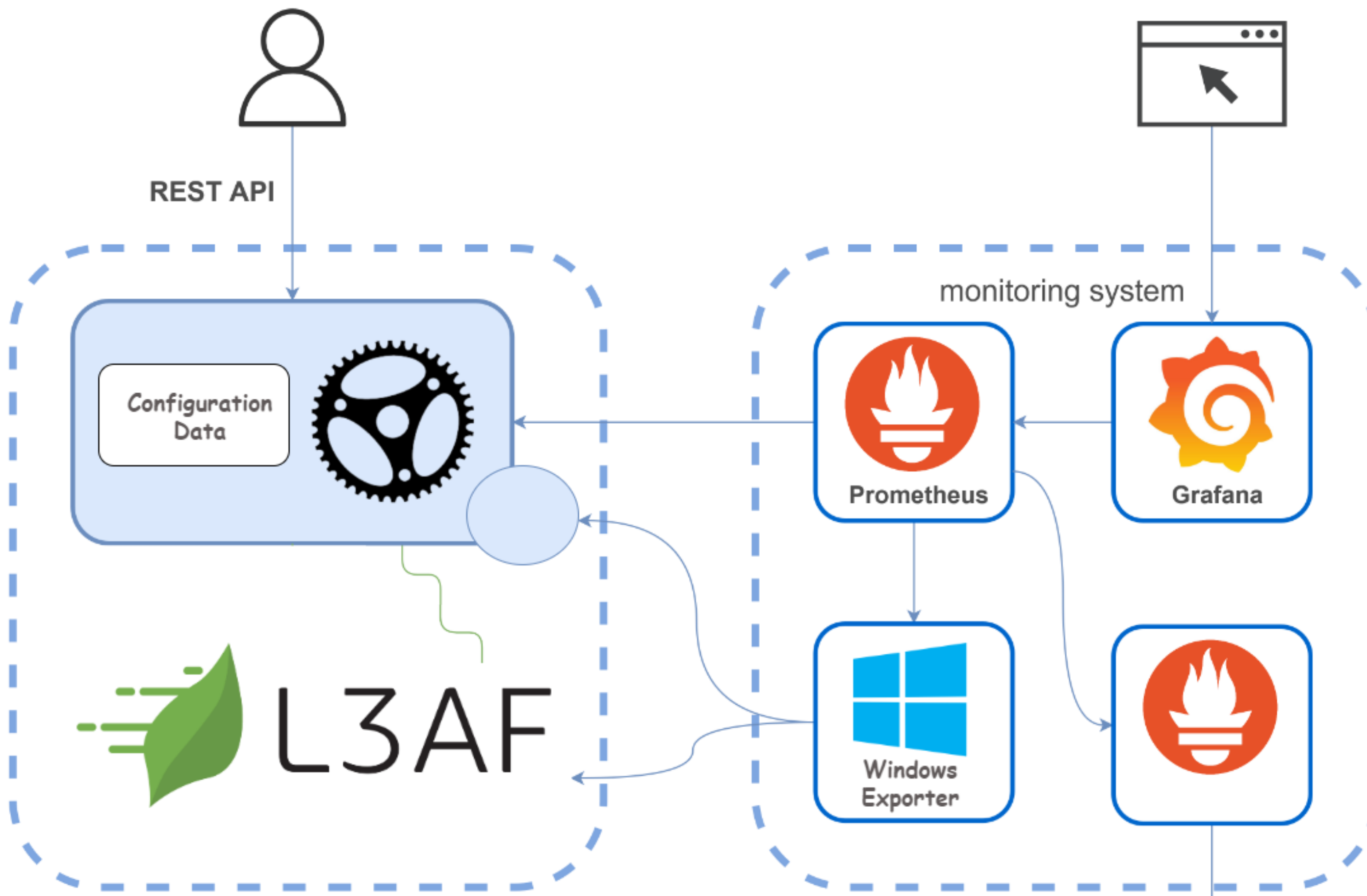
What is needed ?

Windows exporter
Grafana for windows
Prometheus as Service in Windows



Prometheus & Grafana





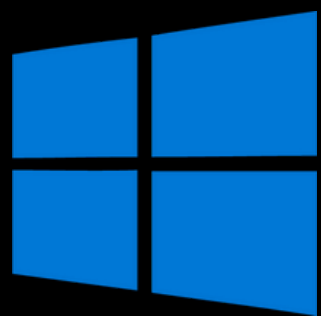
L3afd Metrics



```

# HELP prometheus_target_metadata_cache_bytes The number of bytes that are currently used for storing metric metadata in the cache
# TYPE prometheus_target_metadata_cache_bytes gauge
prometheus_target_metadata_cache_bytes{scrape_job="l3afd"} 1873
prometheus_target_metadata_cache_bytes{scrape_job="prometheus"} 11144
prometheus_target_metadata_cache_bytes{scrape_job="wmi_exporter"} 9194
# HELP prometheus_target_metadata_cache_entries Total number of metric metadata entries in the cache
# TYPE prometheus_target_metadata_cache_entries gauge
prometheus_target_metadata_cache_entries{scrape_job="l3afd"} 37
prometheus_target_metadata_cache_entries{scrape_job="prometheus"} 181
prometheus_target_metadata_cache_entries{scrape_job="wmi_exporter"} 130
# HELP prometheus_target_scrape_pool_exceeded_label_limits_total Total number of times scrape pools hit the label limits, during sync or config reload.
# TYPE prometheus_target_scrape_pool_exceeded_label_limits_total counter
prometheus_target_scrape_pool_exceeded_label_limits_total 0
# HELP prometheus_target_scrape_pool_exceeded_target_limit_total Total number of times scrape pools hit the target limit, during sync or config reload.
# TYPE prometheus_target_scrape_pool_exceeded_target_limit_total counter
prometheus_target_scrape_pool_exceeded_target_limit_total 0
# HELP prometheus_target_scrape_pool_reloads_failed_total Total number of failed scrape pool reloads.
# TYPE prometheus_target_scrape_pool_reloads_failed_total counter
prometheus_target_scrape_pool_reloads_failed_total 0
# HELP prometheus_target_scrape_pool_reloads_total Total number of scrape pool reloads.
# TYPE prometheus_target_scrape_pool_reloads_total counter
prometheus_target_scrape_pool_reloads_total 0
# HELP prometheus_target_scrape_pool_sync_total Total number of syncs that were executed on a scrape pool.
# TYPE prometheus_target_scrape_pool_sync_total counter
prometheus_target_scrape_pool_sync_total{scrape_job="l3afd"} 1
prometheus_target_scrape_pool_sync_total{scrape_job="prometheus"} 1
prometheus_target_scrape_pool_sync_total{scrape_job="wmi_exporter"} 1
# HELP prometheus_target_scrape_pool_target_limit Maximum number of targets allowed in this scrape pool.
# TYPE prometheus_target_scrape_pool_target_limit gauge
prometheus_target_scrape_pool_target_limit{scrape_job="l3afd"} 0
prometheus_target_scrape_pool_target_limit{scrape_job="prometheus"} 0
prometheus_target_scrape_pool_target_limit{scrape_job="wmi_exporter"} 0
# HELP prometheus_target_scrape_pool_targets Current number of targets in this scrape pool.
# TYPE prometheus_target_scrape_pool_targets gauge
prometheus_target_scrape_pool_targets{scrape_job="l3afd"} 1
prometheus_target_scrape_pool_targets{scrape_job="prometheus"} 1
prometheus_target_scrape_pool_targets{scrape_job="wmi_exporter"} 1
# HELP prometheus_target_scrape_pools_failed_total Total number of scrape pool creations that failed.
# TYPE prometheus_target_scrape_pools_failed_total counter
prometheus_target_scrape_pools_failed_total 0

```



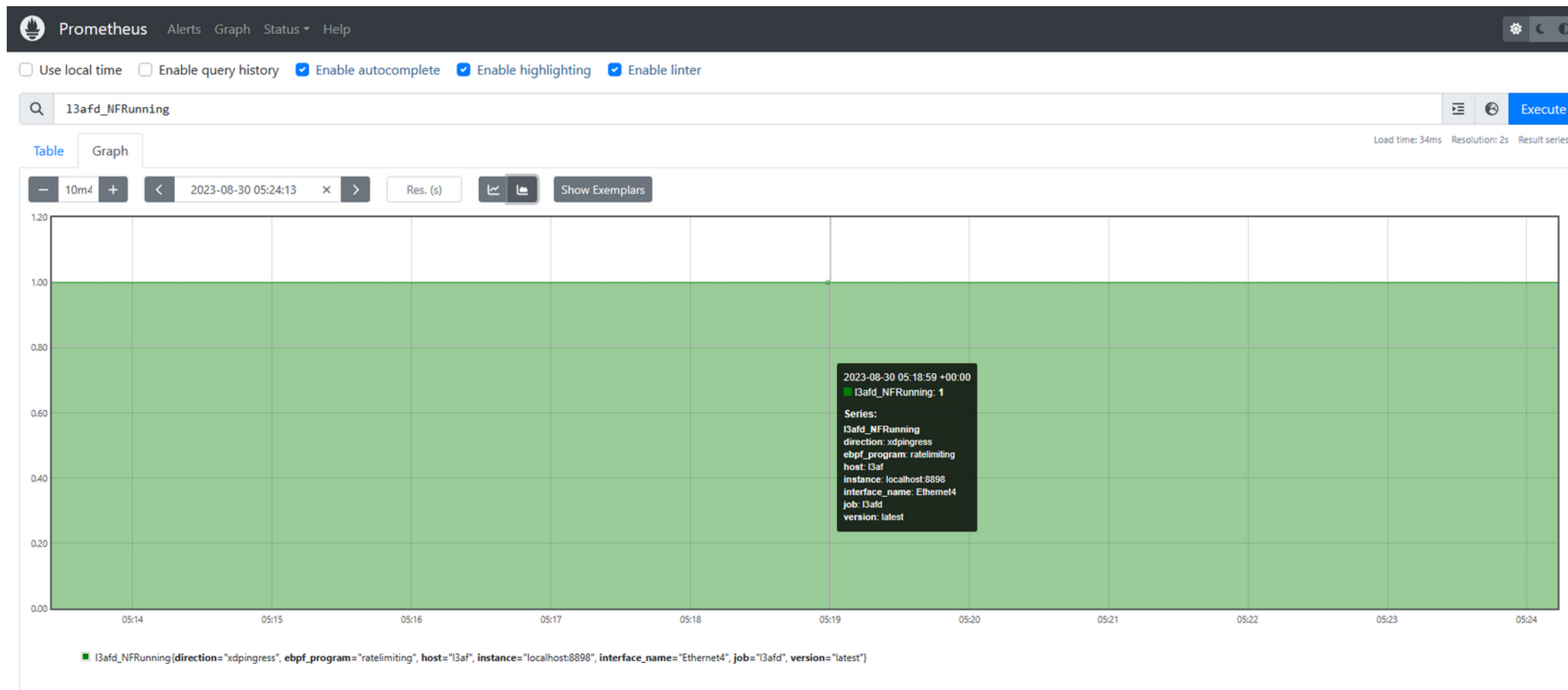
Windows Exporter

```

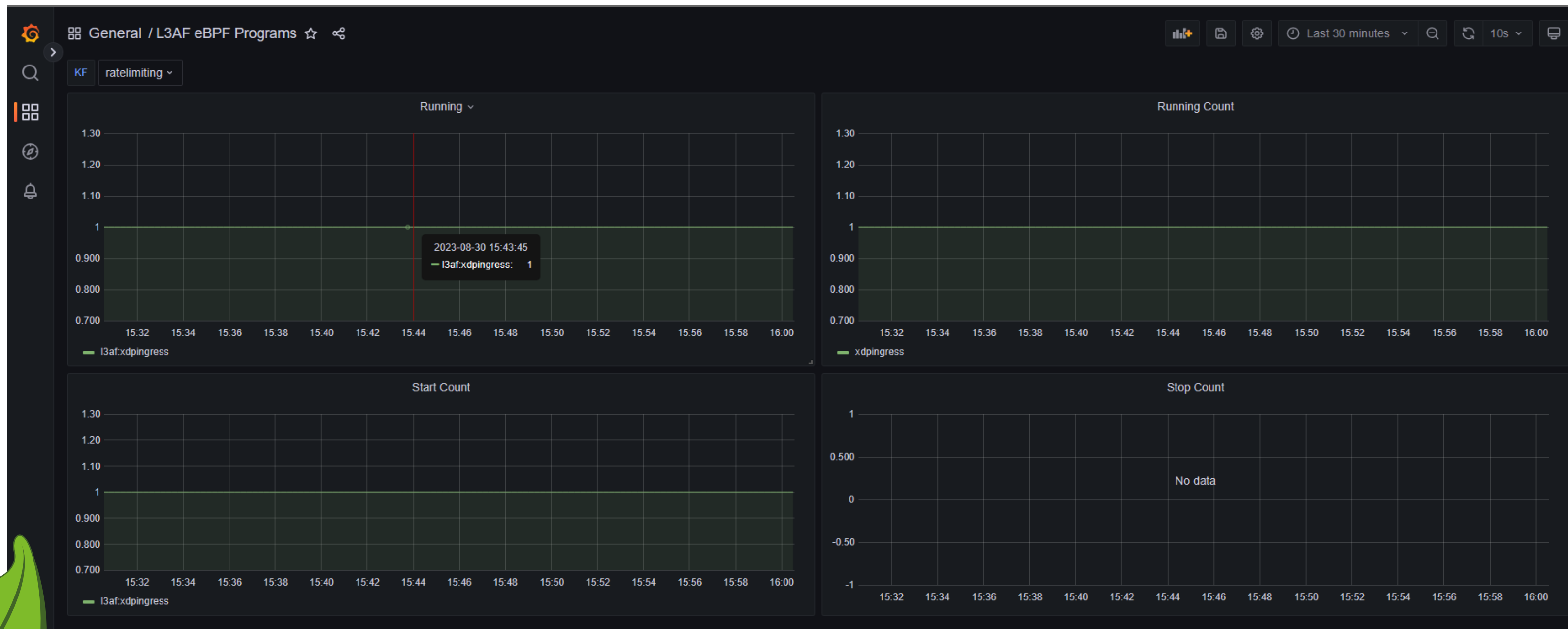
# HELP net_contrack_dialer_conn_attempted_total Total number of connections attempted by the given dialer a given name.
# TYPE net_contrack_dialer_conn_attempted_total counter
net_contrack_dialer_conn_attempted_total{dialer_name="alertmanager"} 0
net_contrack_dialer_conn_attempted_total{dialer_name="default"} 0
net_contrack_dialer_conn_attempted_total{dialer_name="l3afd"} 1
net_contrack_dialer_conn_attempted_total{dialer_name="prometheus"} 1
net_contrack_dialer_conn_attempted_total{dialer_name="wmi_exporter"} 1
# HELP net_contrack_dialer_conn_closed_total Total number of connections closed which originated from the dialer of a given name.
# TYPE net_contrack_dialer_conn_closed_total counter
net_contrack_dialer_conn_closed_total{dialer_name="alertmanager"} 0
net_contrack_dialer_conn_closed_total{dialer_name="default"} 0
net_contrack_dialer_conn_closed_total{dialer_name="l3afd"} 0
net_contrack_dialer_conn_closed_total{dialer_name="prometheus"} 0
net_contrack_dialer_conn_closed_total{dialer_name="wmi_exporter"} 0
# HELP net_contrack_dialer_conn_established_total Total number of connections successfully established by the given dialer a given name.
# TYPE net_contrack_dialer_conn_established_total counter
net_contrack_dialer_conn_established_total{dialer_name="alertmanager"} 0
net_contrack_dialer_conn_established_total{dialer_name="default"} 0
net_contrack_dialer_conn_established_total{dialer_name="l3afd"} 1
net_contrack_dialer_conn_established_total{dialer_name="prometheus"} 1
net_contrack_dialer_conn_established_total{dialer_name="wmi_exporter"} 1
# HELP net_contrack_dialer_conn_failed_total Total number of connections failed to dial by the dialer a given name.
# TYPE net_contrack_dialer_conn_failed_total counter
net_contrack_dialer_conn_failed_total{dialer_name="alertmanager",reason="refused"} 0
net_contrack_dialer_conn_failed_total{dialer_name="alertmanager",reason="resolution"} 0
net_contrack_dialer_conn_failed_total{dialer_name="alertmanager",reason="timeout"} 0
net_contrack_dialer_conn_failed_total{dialer_name="alertmanager",reason="unknown"} 0
net_contrack_dialer_conn_failed_total{dialer_name="default",reason="refused"} 0
net_contrack_dialer_conn_failed_total{dialer_name="default",reason="resolution"} 0
net_contrack_dialer_conn_failed_total{dialer_name="default",reason="timeout"} 0
net_contrack_dialer_conn_failed_total{dialer_name="default",reason="unknown"} 0
net_contrack_dialer_conn_failed_total{dialer_name="l3afd",reason="refused"} 0
net_contrack_dialer_conn_failed_total{dialer_name="l3afd",reason="resolution"} 0
net_contrack_dialer_conn_failed_total{dialer_name="l3afd",reason="timeout"} 0
net_contrack_dialer_conn_failed_total{dialer_name="l3afd",reason="unknown"} 0
net_contrack_dialer_conn_failed_total{dialer_name="prometheus",reason="refused"} 0
net_contrack_dialer_conn_failed_total{dialer_name="prometheus",reason="resolution"} 0
net_contrack_dialer_conn_failed_total{dialer_name="prometheus",reason="timeout"} 0
net_contrack_dialer_conn_failed_total{dialer_name="prometheus",reason="unknown"} 0
net_contrack_dialer_conn_failed_total{dialer_name="wmi_exporter",reason="refused"} 0
net_contrack_dialer_conn_failed_total{dialer_name="wmi_exporter",reason="resolution"} 0
net_contrack_dialer_conn_failed_total{dialer_name="wmi_exporter",reason="timeout"} 0
net_contrack_dialer_conn_failed_total{dialer_name="wmi_exporter",reason="unknown"} 0
# HELP net_contrack_listener_conn_accepted_total Total number of connections opened to the listener of a given name.

```

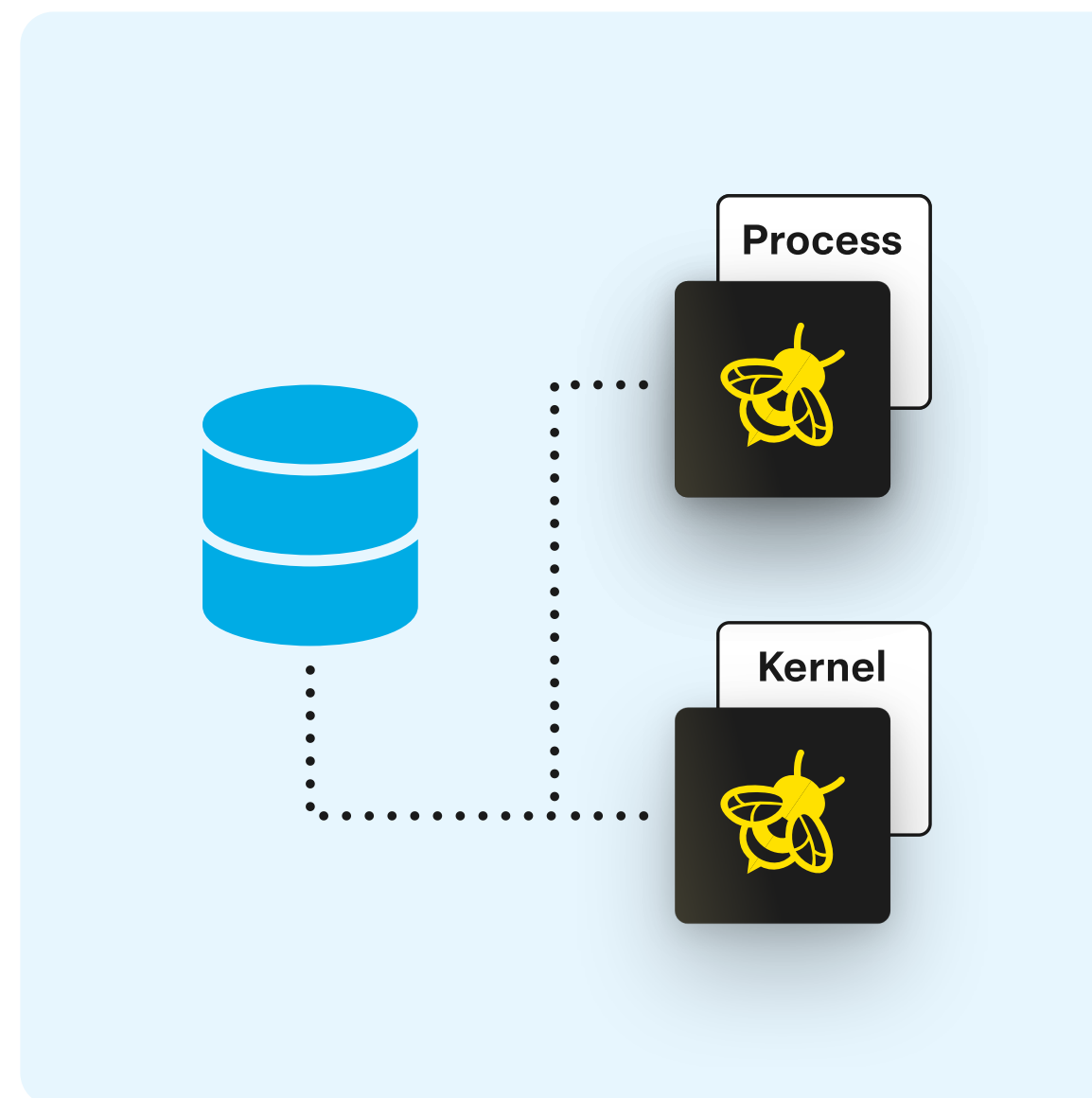

Ratelimiting Graph



Grafana Monitoring



ETW Tracing of eBPF programs



1 Graph Explorer - ebpfforwind...

- System Activity
 - Processes Lifetime By Process
 - Marks Grouped By Mark
 - Generic Events Activity by Provider, Tas...
 - Trace markers
 - VSync-DwmFrame
 - Regions of Interest Regions of Interest

Getting Started | 1 Analysis

Generic Events Activity by Provider, Task, Opcode * ▾

Series

- EbpfforWindowsProvi...
- EbpfSuccess
- win:Info
- 0
- Unknown**
- EbpfGenericMessage
- EbpfReturn
- win:Info

| Line # | Provider Name | Task Name | Opcode N... | Id | Process | Event Name | C... | Thre... | Message (... | Field 2 |
|--------|---------------|-----------|-------------|----|---------|------------------|------|---------|-----------------|---------|
| 1521 | | | | | | EbpfforWindow... | 0 | 11,948 | _ebpf_core_... | |
| 1522 | | | | | | EbpfforWindow... | 0 | 11,948 | invoke_ioctl... | |
| 1523 | | | | | | EbpfforWindow... | 0 | 11,948 | _map_looku... | |
| 1524 | | | | | | EbpfforWindow... | 0 | 11,948 | _ebpf_map_l... | |
| 1525 | | | | | | EbpfforWindow... | 0 | 11,948 | ebpf_map_l... | |
| 1526 | | | | | | EbpfforWindow... | 1 | 11,948 | _ebpf_core_... | |
| 1527 | | | | | | EbpfforWindow... | 1 | 11,948 | invoke_ioctl... | |
| 1528 | | | | | | EbpfforWindow... | 1 | 11,948 | ebpf_object_... | |
| 1529 | | | | | | EbpfforWindow... | 1 | 11,948 | get_map_d... | |

Processes Lifetime By Process * ▾

Series

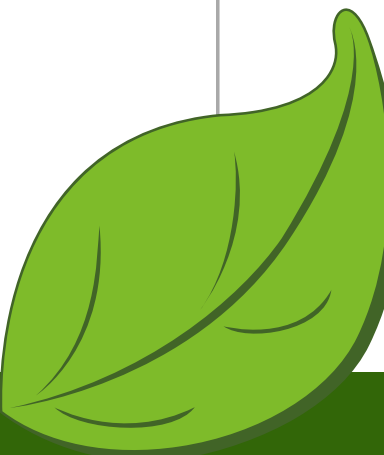
- Permanent

Start: 27.297808100s
End: 42.301505200s
Duration: 15.003697100s

Analysis Assistant

My Presets


Details



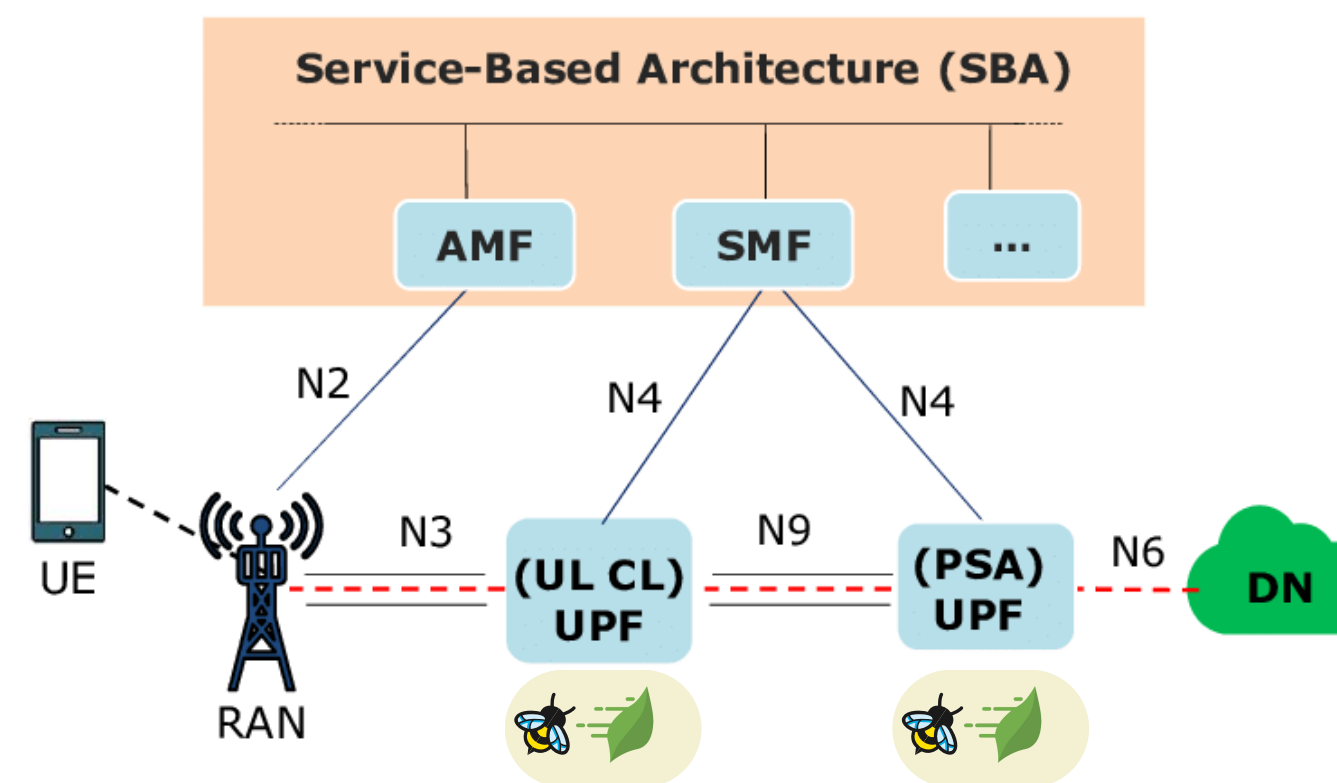
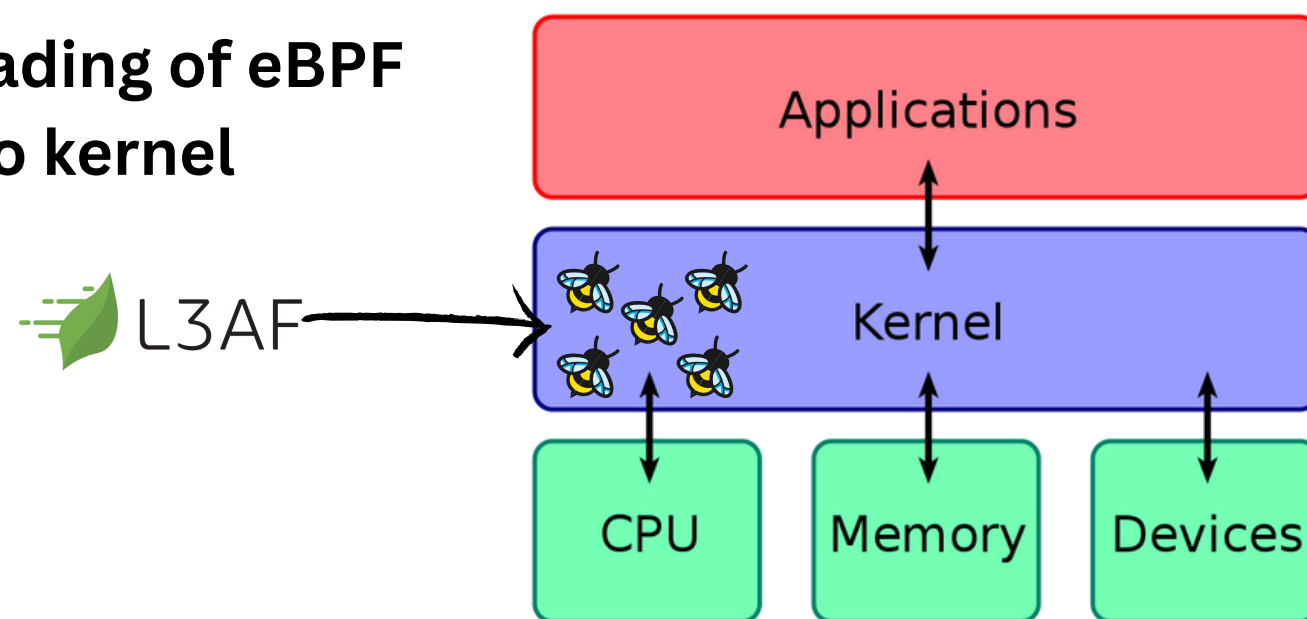
Future Plannings



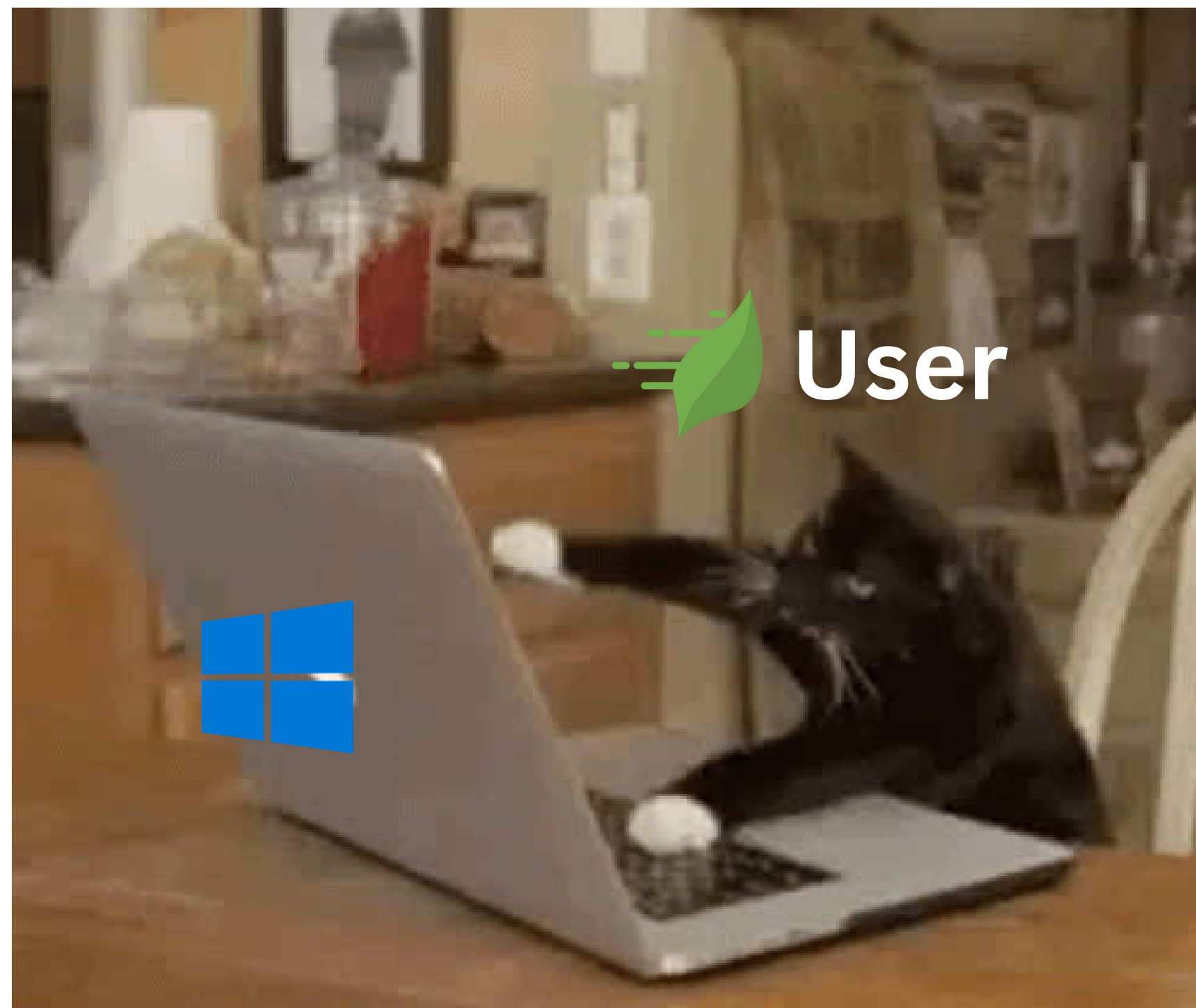
→ L3AF on Kubernetes

 L3AF + 5G - UPF

Direct loading of eBPF into kernel



Now, Windows user be like :



Thank You
Audience



No Questions?

