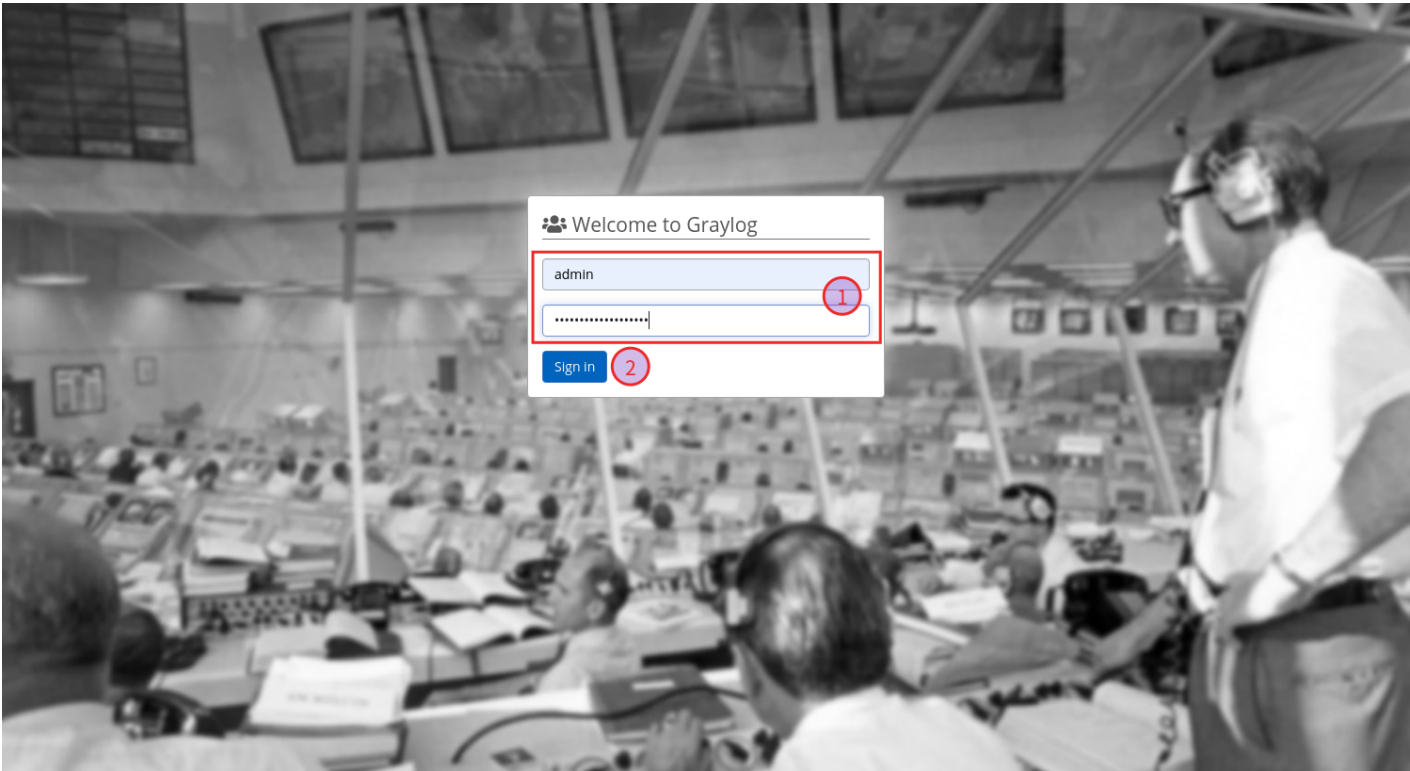


3. Graylog

https:// Graylog IP :9000 Graylog

1.

Username Password Sign in



Graylog Dismiss guide

graylog

[Search](#) [Streams](#) [Alerts](#) [Dashboards](#) [Enterprise](#) [System](#)

2

0 in
0 out

✕ Dismiss guide

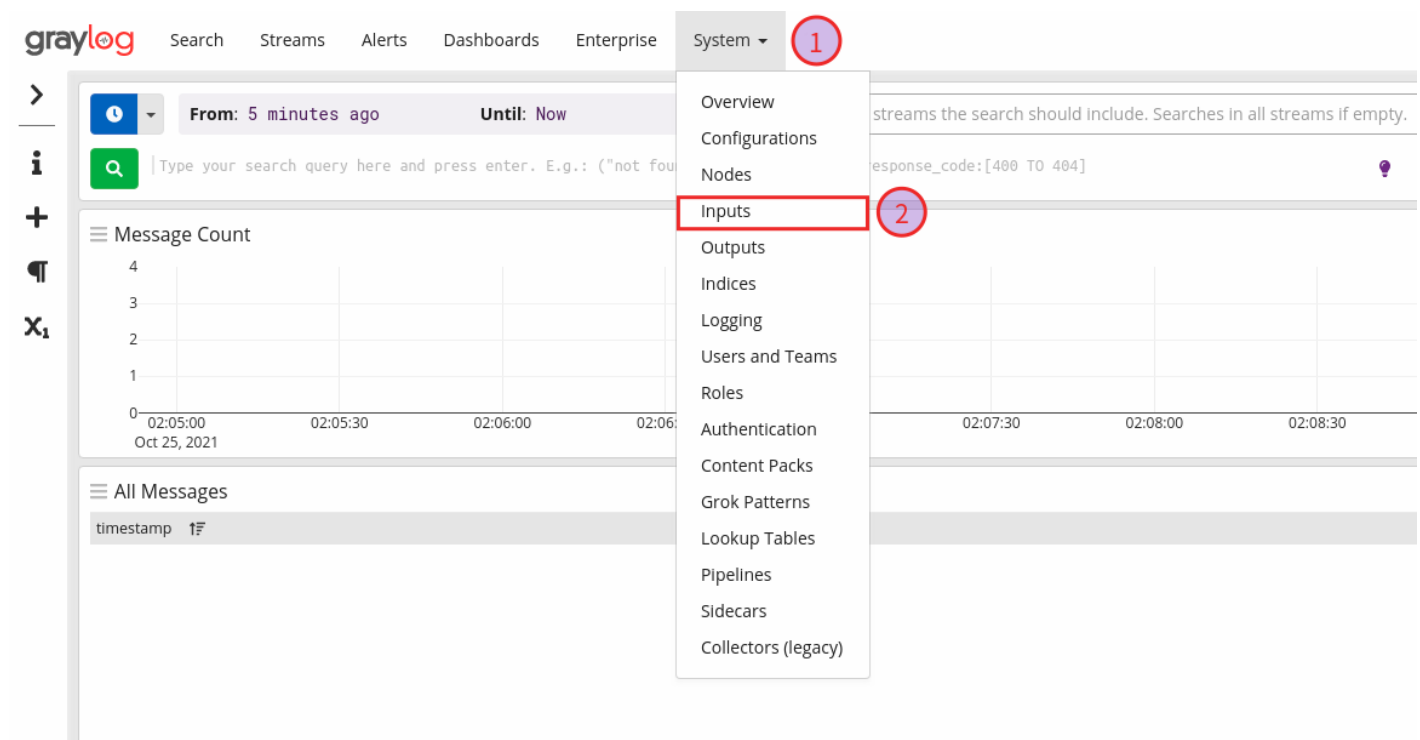
We could not load the [Graylog Getting Started Guide](#). Please open it directly with a browser that can access the public internet.

Linux

Windows

2. Input

- System→Inputs



- Input Syslog UDP Launch new input
- Windows "Windows Syslog" "Windows Graylog"

Inputs

Graylog nodes accept data via inputs. Launch or terminate as many inputs as you want here.

syslog UDP

X ▲

Launch new input

Find more inputs ↗

Raw/Plaintext AMQP

Raw/Plaintext Kafka

Raw/Plaintext TCP

Raw/Plaintext UDP

Syslog AMQP

Syslog Kafka

Syslog TCP

Syslog UDP

set

1

2

- Title Port
- Windows Port "Windows Syslog" "Windows Graylog"

graylog Search Streams Alerts Dashboards Enterprise System / Inputs 2

Inputs

Graylog nodes accept data via inputs. Launch or terminate as ma

Syslog UDP X Launch new inp

Filter by title Filter Reset

Global inputs 0 configured

There are no global inputs.

Local inputs 0 configured

There are no local inputs.

Launch new Syslog UDP input

☐ Global
Should this input start on all nodes

Node
19c385b9 / localhost
On which node should this input start

Title
eplog server
Select a name of your new input that describes it.

Bind address
0.0.0.0
Address to listen on. For example 0.0.0.0 or 127.0.0.1.

Port
1514
Port to listen on.

Receive Buffer Size (optional)
262144
The size in bytes of the recvBufferSize for network connections to this input.

No. of worker threads (optional)
4
Number of worker threads processing network connections for this input.

Override source (optional)

- Allow overriding date Save

graylog Search Streams Alerts Dashboards

Inputs

Graylog nodes accept data via inputs. Launch or terminate as ma

Syslog UDP X Launch new inp

Filter by title Filter Reset

Global inputs 0 configured

There are no global inputs.

Local inputs 0 configured

There are no local inputs.

Address to listen on. For example 0.0.0.0 or 127.0.0.1.

Port
1514
Port to listen on.

Receive Buffer Size (optional)
262144
The size in bytes of the recvBufferSize for network connections to this input.

No. of worker threads (optional)
4
Number of worker threads processing network connections for this input.

Override source (optional)

The source is a hostname derived from the received packet by default. Set this if you want to override it with a custom string.

☐ Force rDNS?
Force rDNS resolution of hostname? Use if hostname cannot be parsed. (Be careful if you are sending DNS logs into this input because it can cause a feedback loop.)

☒ Allow overriding date?
Allow to override with current date if date could not be parsed?

☐ Store full message?
Store the full original syslog message as full_message?

☐ Expand structured data?
Expand structured data elements by prefixing attributes with their SD-ID?

Cancel Save

Graylog 4.2.0-5adccc3 on localhost (Ubuntu 11.0.11 on Linux 3.8.0-41-generic)

Input

Show received messages

graylog Search Streams Alerts Dashboards Enterprise System / Inputs 1 0 in 0 out

Inputs

Graylog nodes accept data via inputs. Launch or terminate as many inputs as you want here.

Select Input Launch new input Find more inputs

Filter by title Filter Reset

Global inputs

0 configured

There are no global inputs.

Local inputs

1 configured

eplog server Syslog UDP **RUNNING**
On node 19c385b9 / localhost

Show received messages Manage extractors Stop input More actions

```
allow_override_date: true
bind_address: 0.0.0.0
expand_structured_data: false
force_rdns: false
number_worker_threads: 4
override_source: <empty>
port: 1514
recv_buffer_size: 262144
store_full_message: false
```

Throughput / Metrics

1 minute average rate: 0 msg/s
Network I/O: 0B 0B (total: 0B 0B)
Empty messages discarded: 0

Input

graylog Search Streams Alerts Dashboards Enterprise System 1 0 in 0 out

> i + 🔊 X1

From: 2021-10-28 22:55:40.616 Until: 2021-10-29 03:24:10.616

Select streams the search should include. Searches in all streams if empty.

▶ Not updating

gl2_source_input:6176139340ad8c20214b5ed9 Save Load Share

Message Count

Time	Message Count
23:00	1000
23:15	1000
23:30	1000
23:45	1000
00:00	1000
00:15	1000
00:30	1000
00:45	1000
01:00	1000
01:15	1000
01:30	1000
01:45	1000
02:00	1000
02:15	1000
02:30	1000
02:45	1000
03:00	1000

All Messages

timestamp	source
2021-10-29 02:54:54.000 +00:00	pc-71
pc-71 acvpnagent[751]: Function: GetDNSConfig File: ../../vpn/Common/Utility/linux/DBusNMHelper.cpp Line: 295 Unable to get any DNS server for interface edge0	
2021-10-29 02:54:54.000 +00:00	pc-71
pc-71 acvpnagent[751]: Function: getDnsConfiguration File: ../../vpn/Common/Utility/NetInterface-unix.cpp Line: 1160 Invoked Function: CDBusNMHelper::GetDNSConfig Return Code: -17 235954 (0xFE9000E) Description: DBUSNMHELPER_ERROR_EMPTY_CONFIG	
2021-10-29 02:54:54.000 +00:00	pc-71
pc-71 acvpnagent[751]: Function: getDnsConfiguration File: ../../vpn/Common/Utility/NetInterface-unix.cpp Line: 1160 Invoked Function: CDBusNMHelper::GetDNSConfig Return Code: -17 235954 (0xFE9000E) Description: DBUSNMHELPER_ERROR_EMPTY_CONFIG	
2021-10-29 02:54:54.000 +00:00	pc-71
pc-71 acvpnagent[751]: Function: GetDNSConfig File: ../../vpn/Common/Utility/linux/DBusNMHelper.cpp Line: 295 Unable to get any DNS server for interface eth0	
2021-10-29 02:54:53.000 +00:00	pc-71
pc-71 acvpnagent[751]: Function: GetDNSConfig File: ../../vpn/Common/Utility/linux/DBusNMHelper.cpp Line: 295 Unable to get any DNS server for interface eth0	

Revision #18

Created 26 October 2021 02:31:10 by Epower

Updated 29 October 2021 03:54:53 by Epower