

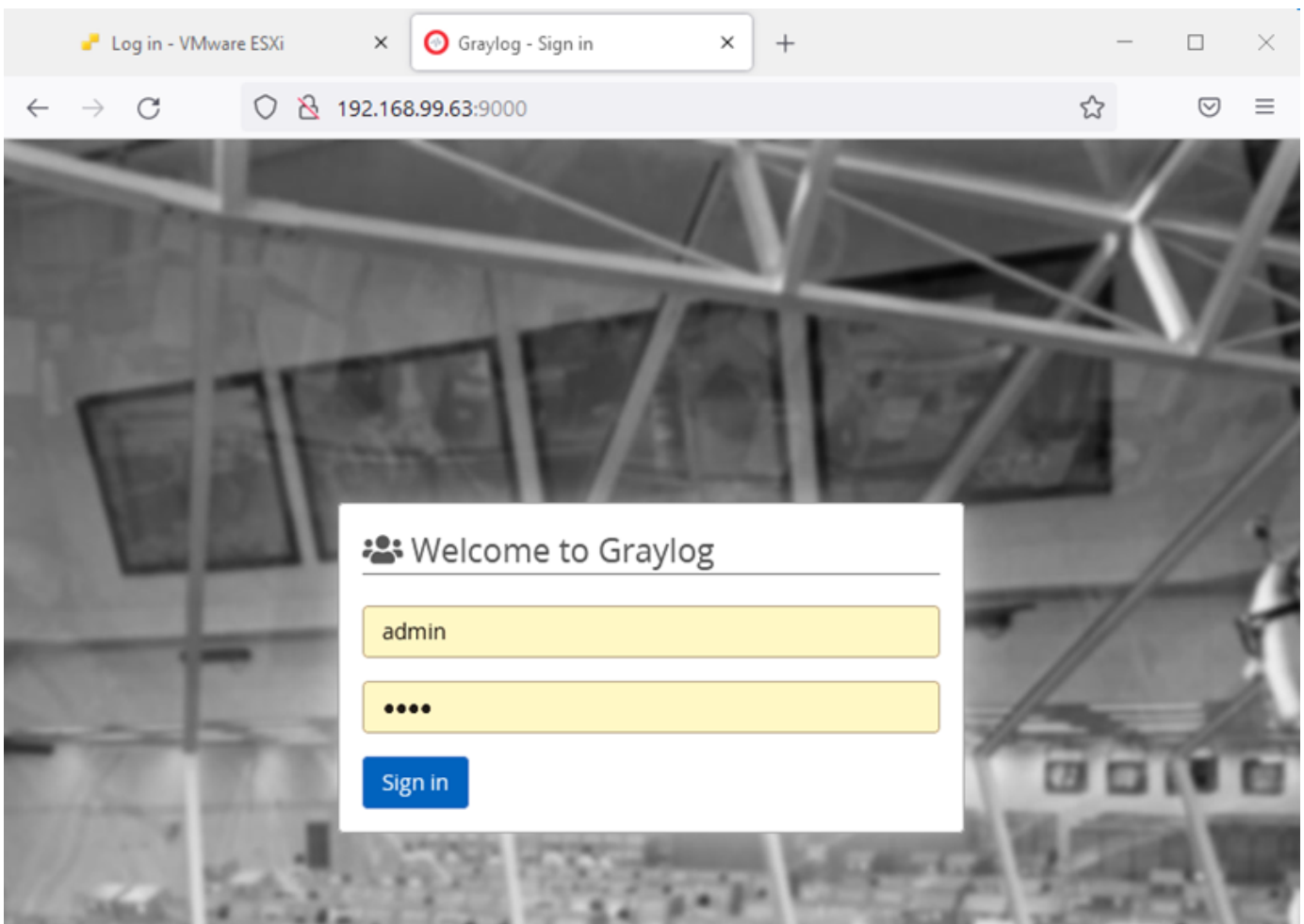
10.1 ?????????? ?????????????? ????????? ?????????? ?????????? ???????

Початкова конфігурація сервера аналізу журналів подій виконується Адміністратором локальних компонентів (системним адміністратором).

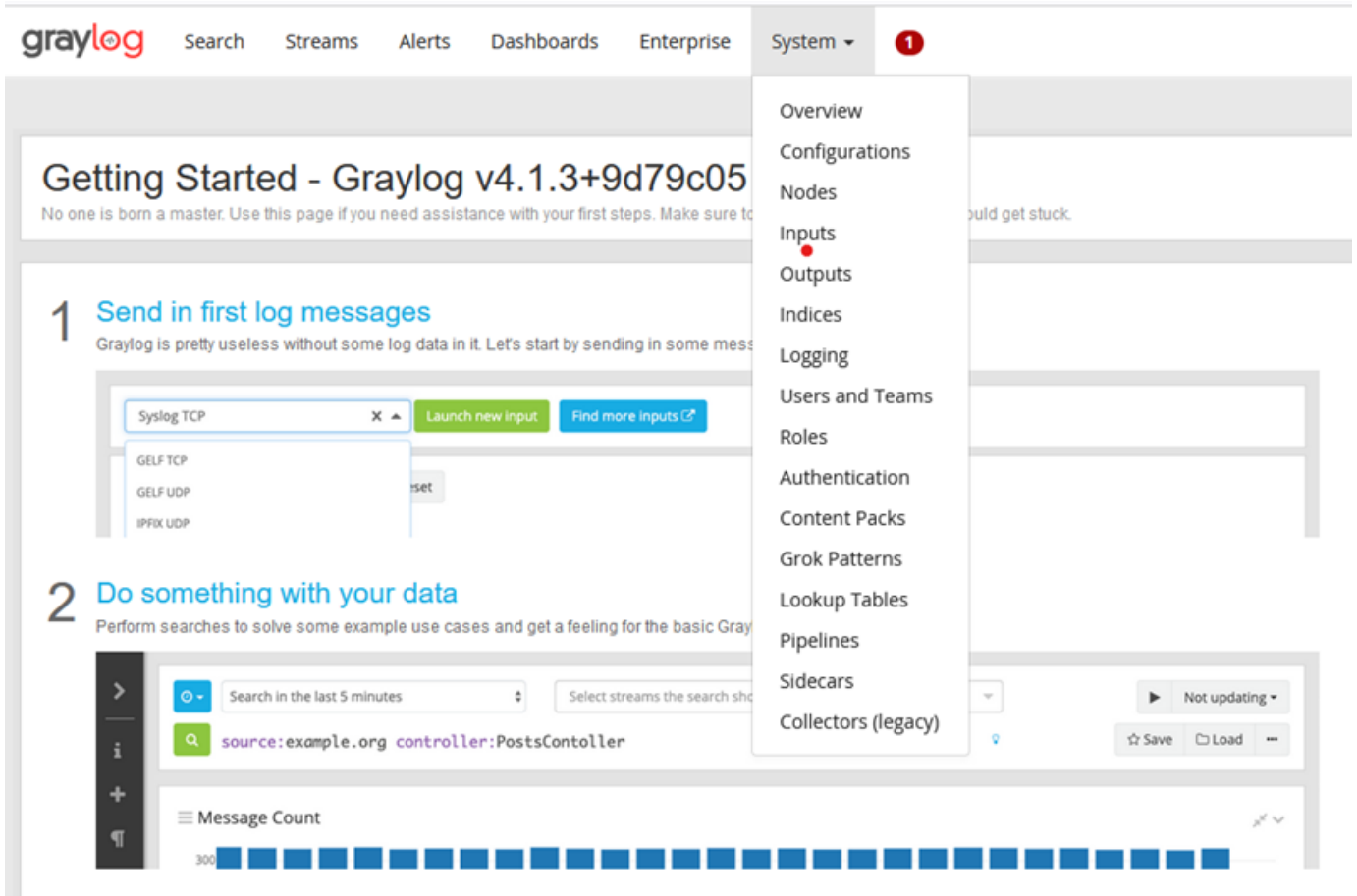
Для початкової конфігурації необхідно перейти до вебінтерфейсу серверу аналізу журналів за посиланням: <http://<IP-GRAYLOG-Server>:9000>,

де **<IP-GRAYLOG-Server>** - це IP - адреса серверу аналізу журналів подій,

використовуючи логін «admin» та пароль, який було створено в пункті [10.2](#)



Після успішної авторизації, необхідно перейти до вкладки System -> Inputs:



Та створити новий Input, задавши його тип як «Syslog UDP» та натиснути на кнопку «Launch new input»:

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 [↗](#)

Raw/Plaintext AMQP

Raw/Plaintext Kafka

Raw/Plaintext TCP

Raw/Plaintext UDP

Syslog AMQP

Syslog Kafka

Syslog TCP

Syslog UDP

set

Після цього

необхідно відредагувати поля «Title» та «Port» наступним чином:

Global

Should this input start on all nodes

Node

e68a4d79 / graylog1

On which node should this input start

Title

UXP

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

Та натиснути на кнопку «Save».

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 4.1.3+9d79c05 on graylog1 (Private Build 1.8.0_292 on Linux 4.15.0-156-generic)

Версія #2

Admin створив 2024-09-23 09:45:35 UTC

Admin оновив 2024-09-23 09:46:15 UTC