

MONITORING ECOSYSTEM

Syslog

DESCRIPCIÓN



Nuestro sistema de monitoreo, se comprende de un conjunto de herramientas completamente integradas entre si, con el fin de facilitar la experiencia de uso, así como también correlacionar la información de vital importancia a la hora de resolver alguna incidencia, u obtener un conjunto de métricas que nos permita por ejemplo hacer planificación de recursos de red.

DEFINICIÓN



Un SYSLOG Server es un servicio, valga la redundancia, que nos permite coleccionar información de diversas índoles. Centraliza y almacena los eventos que reportan nuestros elementos de red como por ejemplo, Firewalls, Routers, Switches, Aplicativos, Servicios.

La principal funcionalidad que cubre es la poder correlacionar eventos con alguna linea temporal, muy útil a la hora de encontrar problemas ante Network Outages.

BONDADDES



- Servicio Dockerizado (de facil migración en caso de ser necesario)
- Redundante (ante eventualidades se puede correr el contenedor en otro chasis)
- Fácil de operar ya que esta integrado dentro de Grafana al igual que el resto de herramientas del ecosistema.
- Fácil acceso a la información, con filtros por dispositivo desde el que se recibió el log, linea de tiempo, o string particular que desee buscar.
- Alertas seteables y customizables dependiendo la necesidad.
- Concatenación de filtros.



FILTRO POR STRING

Resulta sencillo ubicar mensajes recibidos que coincidan con determinado string ingresado por el usuario.

Free Form Filter

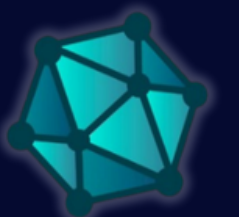
CONFIG

Sm...

Log Line Co

Logs By Host - "All" - "CONFIG" (Filtered) ▾

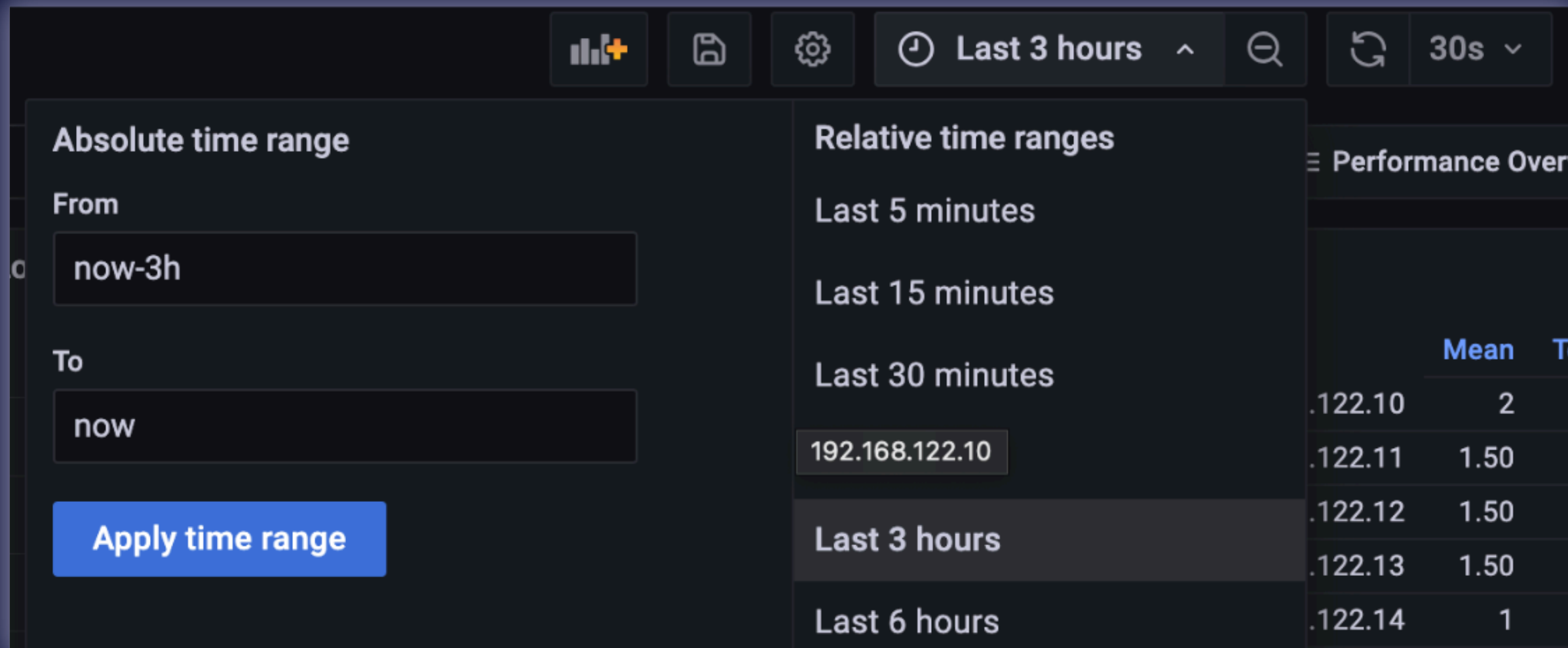
>	2024-07-16 14:15:13	192.168.122.10	%MGBL-SYS-5-CONFIG_I : Configured from console by admin
>	2024-07-16 14:14:58	192.168.122.10	%MGBL-SYS-5-CONFIG_I : Configured from console by admin
>	2024-07-16 14:14:58	192.168.122.10	%MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user 'admin' o view the changes.
>	2024-07-16 14:14:50	192.168.122.13	%MGBL-SYS-5-CONFIG_I : Configured from console by admin
>	2024-07-16 14:14:49	192.168.122.13	%MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user 'admin' changes.
>	2024-07-16 14:14:35	192.168.122.11	%MGBL-SYS-5-CONFIG_I : Configured from console by admin
>	2024-07-16 14:14:33	192.168.122.11	%MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user 'admin' o view the changes.
>	2024-07-16 14:14:21	192.168.122.12	%MGBL-SYS-5-CONFIG_I : Configured from console by admin
>	2024-07-16 14:14:21	192.168.122.12	%MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user 'admin' o view the changes.



NET-ECHO

FILTRO PORTS

Desglose los mensajes recibidos filtrando por el time slot que lo requiera.



The screenshot shows the Net-Echo application interface. At the top, there is a toolbar with icons for a chart, save, settings, a clock icon, and a dropdown menu currently showing 'Last 3 hours'. To the right of the clock icon are a search icon and a refresh icon with a '30s' interval. Below the toolbar, a modal window titled 'Absolute time range' is open. It contains two input fields: 'From' with the value 'now-3h' and 'To' with the value 'now'. Below these fields is a blue button labeled 'Apply time range'. To the right of the 'Absolute time range' modal is a 'Relative time ranges' dropdown menu. This menu is open, showing a list of options: 'Last 5 minutes', 'Last 15 minutes', 'Last 30 minutes', '192.168.122.10' (which is highlighted), 'Last 3 hours', and 'Last 6 hours'. In the background, a table titled 'Performance Overview' is partially visible. It has columns for IP address, 'Mean', and 'Total'. The table contains several rows of data, including IP addresses like .122.10, .122.11, .122.12, .122.13, and .122.14, with corresponding mean values and total counts.

IP Address	Mean	Total
.122.10	2	
.122.11	1.50	
.122.12	1.50	
.122.13	1.50	
.122.14	1	

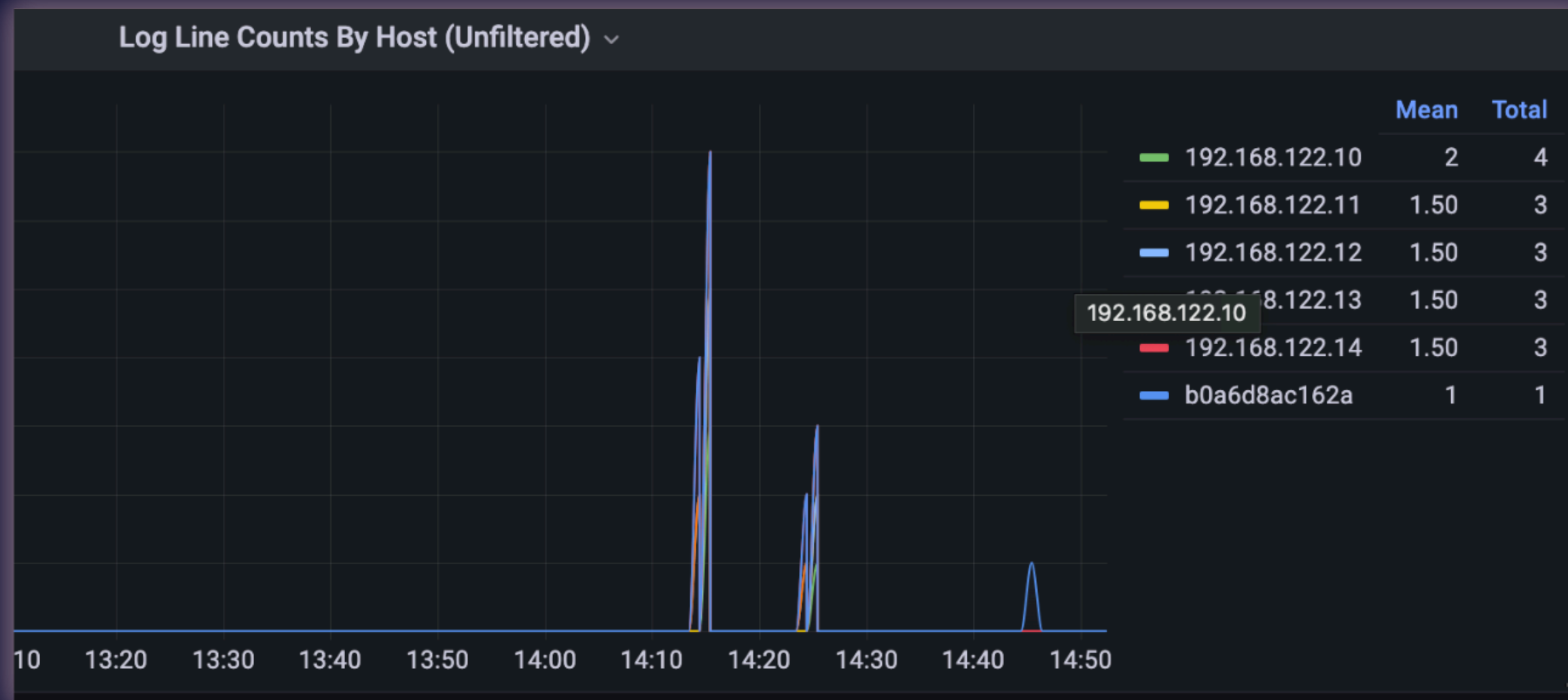
FILTRO POR EQUIPO

Unicamente, mostrará en pantalla los mensajes recibidos desde el/los dispositivos de red que este necesitando revisar.



CUANTIFICACIÓN

Cualquiera haya sido el / los filtros utilizados, el dashboard permitirá también la cuantificación de dicha información.



NO SISTU CON CON



Gracias a todo el potencial que nos permite utilizar Grafana como front-end, podemos decir que es una herramienta fundamental a la hora de hacer TSHOOT en los dispositivos de red ante eventualidades.

Conozca más acerca de esta y otras herramientas del Network Monitoring Ecosystem que NET-ECHO tiene disponible.



NET-ECHO

GRACIAS