Herramientas para el estudio de la estabilidad del generador cuántico de números aleatorios

Elisabeth Ortega, PhD.
Gerente I+D+i en HPCNow!

25/10/2023

www.hpcnow.com

Jornada Técnica Computación Cuántica

- Young company (born in 2012)
- Staff: 39 HPC folks and growing
- No financial dependencies
- Strong growth
- EU joint venture

doitnow
HPC Services

Services and turnkey solutions adapted to customers needs

Planning

Consulting

Solution design

Installation

Infrastructure

Software

Training

Maintenance

Support

Managed services

R&D&I

PoCs

Open collaboration

Tech. transfer

HPC Now!

Proyecto TestQRNG

Motivación y objetivo principal

Motivación:
Un generador de números aleatorios debe proporcionar buenos resultados y ser estable a lo largo del tiempo.

Objetivos:
Proporcionar una herramienta de monitoraje de la estabilidad del generador de números aleatorios.

HPC Now!

Tareas a realizar

- Búsqueda de sistemas de chequeo de generadores de números aleatorios
- Diseño y montaje de una solución para ejecutar tests y medir métricas
- Ejecución automática de tests y recolección de resultados
- Importar y graficar los resultados

Sistemas de chequeo de números aleatórios

Para una primera aproximación se han usado las publicaciones **NIST 800-22** y **800-90B**. Entre los tests ejecutados encontramos:

- Monobit
- Approximate entropy
- Minimum entropy
- Binary Matrix Rank
- Cummulative sums
- IID tests
- Runs
- Random excursion
- Restart tests

Diseño y montaje de una solución para ejecutar tests y medir métricas

Solución original

- Usada y citada por muchos usuarios
- Mantenida por el NIST (código abierto)
- No se puede ejecutar de forma automática

Solución aportada

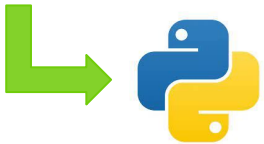
- Adaptada para usar el QRNG como fuente de entrada de datos
- Código abierto (mantenido por la comunidad)
- No requiere inputs extra

Ejecución automática de tests y recolección de resultados

```
* 8,20 * * * python /path/to/qrng_test.py > /path/to/output.txt
```

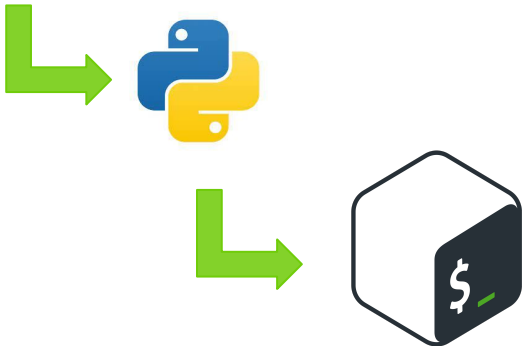
Ejecución automática de tests y recolección de resultados

```
* 8,20 * * * python /path/to/qrng_test.py > /path/to/output.txt
```



Ejecución automática de tests y recolección de resultados

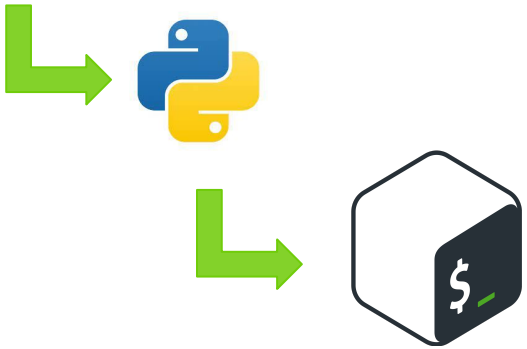
```
* 8,20 * * * python /path/to/qrng_test.py > /path/to/output.txt
```



```
echo "{
\"pt_monobit\": \"$monobit\",
\"pt_freq_wh_block\": \"$freq\",
\"pt_runs\": \"$runs\",
\"pt_lroiab\": \"$lroiab\",
\"pt_fourier\": \"$fourier\",
\"pt_not_overlap\": \"$not_overlap\",
\"pt_serial\": \"$serial\",
\"pt_aprox_entropy\": \"$aproxEnt\",
\"pt_cumul_sums\": \"$cumSum\",
\"pt_random_ex\": \"$random_ex\",
\"pt_random_ex_var\": \"$random_ex_var\",
\"@utimestamp\": $ts,
\"@timestamp\": \"$(date -u -d @$ts +'%Y-%m-%dT%H:%M:%S%z')\"
```

Ejecución automática de tests y recolección de resultados

```
* 8,20 * * * python /path/to/qrng_test.py > /path/to/output.txt
```

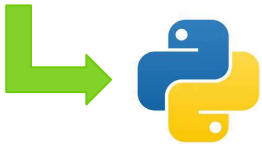


```
echo "{
\"pt_monobit\": \"$monobit\",
\"pt_freq_wh_block\": \"$freq\",
\"pt_runs\": \"$runs\",
\"pt_lroiab\": \"$lroiab\",
\"pt_fourier\": \"$fourier\",
\"pt_not_overlap\": \"$not_overlap\",
\"pt_serial\": \"$serial\",
\"pt_aprox_entropy\": \"$aproxEnt\",
\"pt_cumul_sums\": \"$cumSum\",
\"pt_random_ex\": \"$random_ex\",
\"pt_random_ex_var\": \"$random_ex_var\",
\"@utimestamp\": $ts,
\"@timestamp\": \"$(date -u -d @$ts +'%Y-%m-%dT%H:%M:%S%z')\"
```

elasticsearch

Ejecución automática de tests y recolección de resultados (entropía)

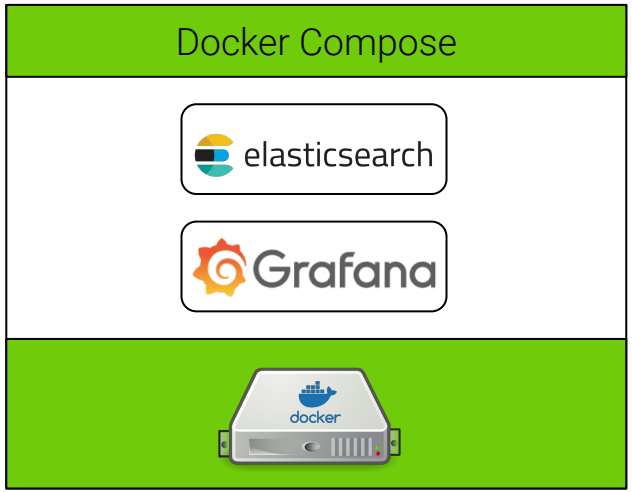
```
* 7,19 * * * python /path/to/calculo_entropia.py >/path/to/output.txt
```



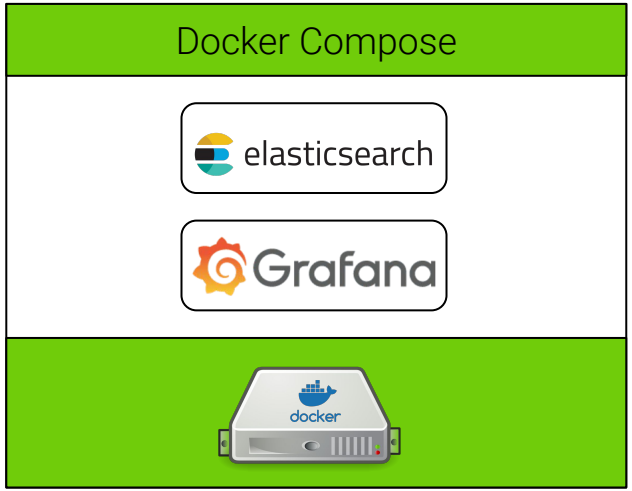
```
echo "{
\"H_min\": \"$h_min_1\",
\"H_min_big\": \"$h_min_2\",
\"H_min_bigger\": \"$h_min_3\",
\"@utimestamp\": $ts,
\"@timestamp\": \"$(date -u -d @$ts +'%Y-%m-%dT%H:%M:%S%z')\"
```

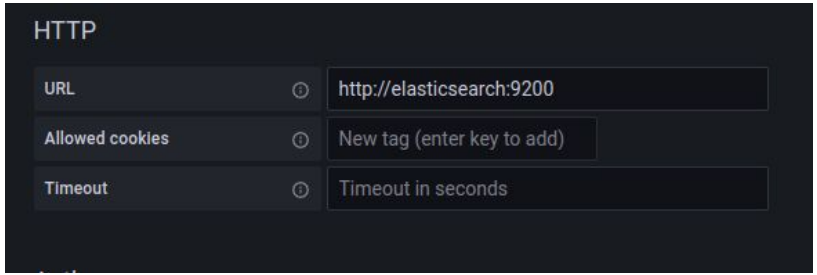
elasticsearch

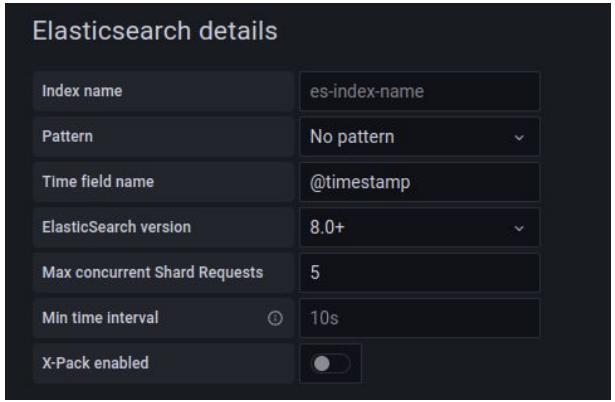
Paneles de métricas



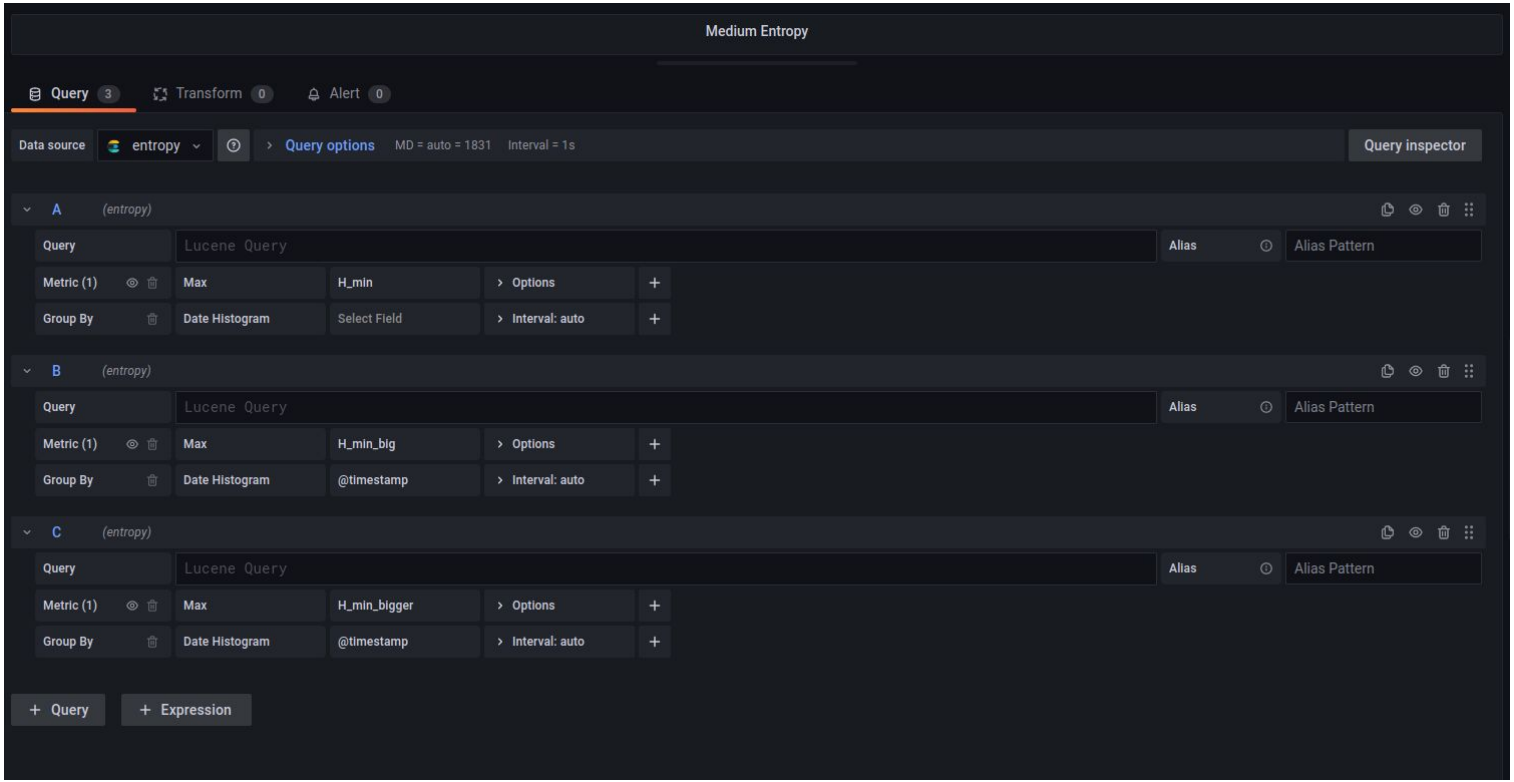
Paneles de métricas



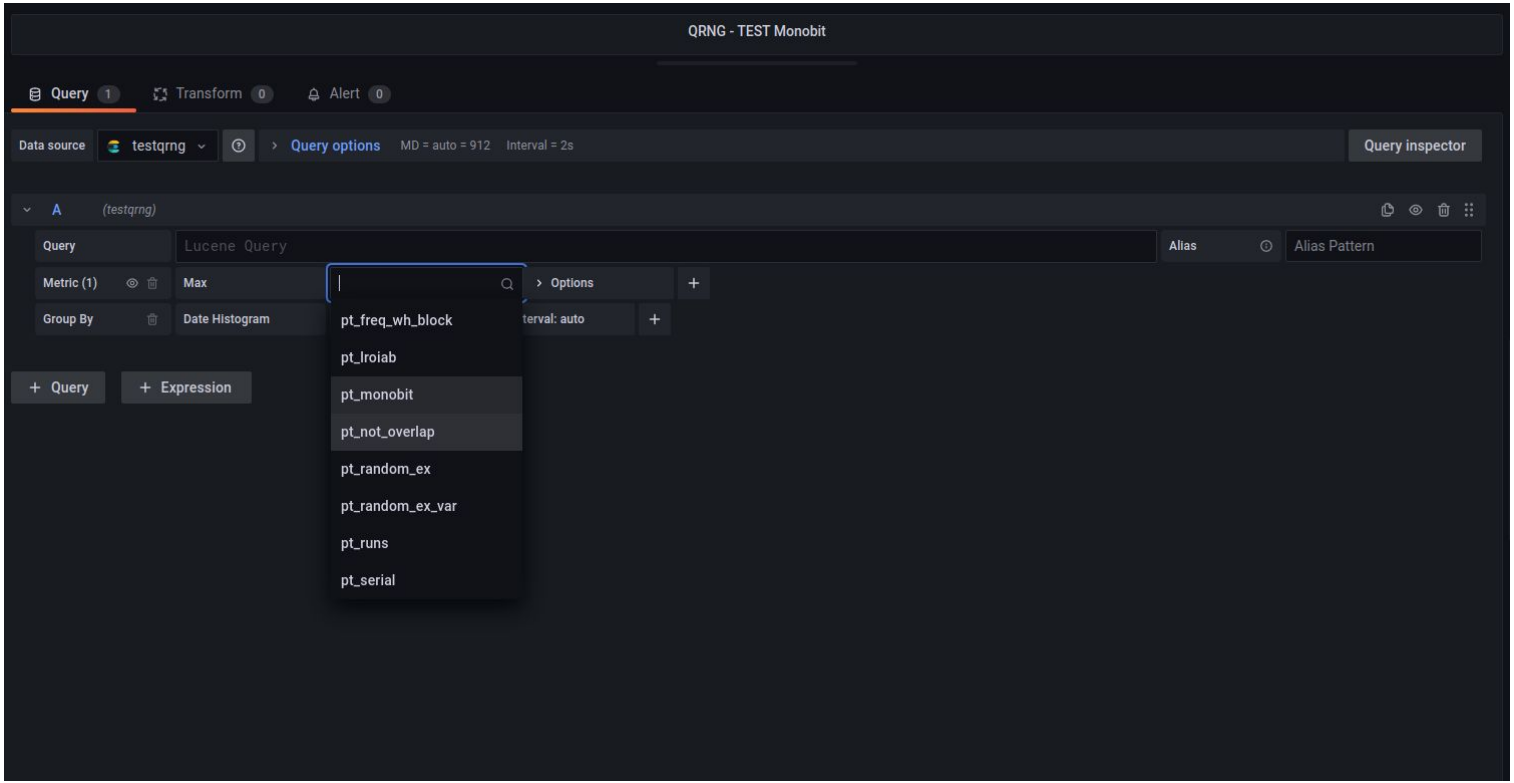




Paneles de métricas (800-90B)



Paneles de métricas (NIST 800-22)



Paneles de métricas

Siguientes pasos

- Implementar la solución automatizada en Finisterrae III
- Añadir más herramientas de diagnostico
- Creación de alertas

¡Muchas gracias por su atención!

Contacto

Elisabeth Ortega: elisabeth.ortega@hpcnow.com
Christian Bustelo: christian.bustelo@hpcnow.com

HPC Now!

A iniciativa do Polo de Tecnoloxías Cuánticas de Galicia conta con financiamento de:

Fondos REACT EU

AXENCIA GALEGA DE INNOVACIÓN

UNIÓN EUROPEA

Xacobeo 21·22

CESGA
Centro de Supercomputación de Galicia

Despregamento dunha infraestrutura baseada en tecnoloxías cuánticas da información que permita impulsar a I+D+i en Galicia.

Apoiar a transición cara a unha economía dixital.

Operación financiada pola Unión Europea, a través do FONDO EUROPEO DE DESENVOLVEMENTO REXIONAL (FEDER), como parte da resposta da Unión á pandemia da COVID-19.

PROGRAMA OPERATIVO
FEDER GALICIA
2014-2020

Unha maneira de facer Europa