



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

Jornada Técnica Computación Cuántica

www.hpcnow.com

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

**doitnow**

HPC Services



Marie Curie, 8 - 08042 Barcelona (Spain)

Fernly Rise, 2019 Auckland (New Zealand)

Auckland

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



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.

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

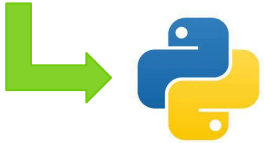
- ✓✓ Adaptada para usar el QRNG como fuente de entrada de datos
- ✓✓ Código abierto (mantenido por la comunidad)
- ✓✓ No requiere inputs extra

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
```

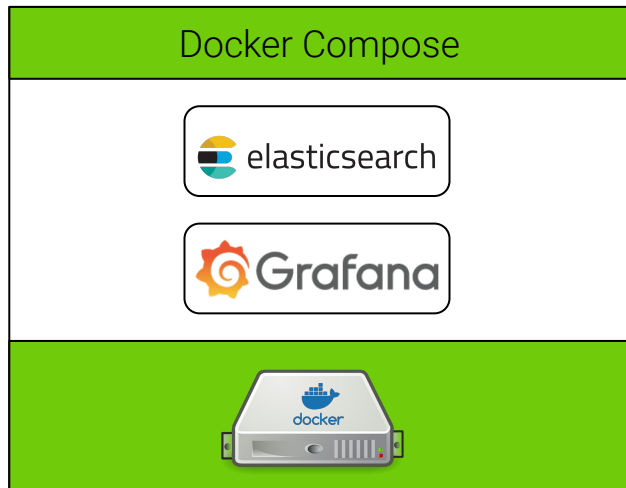


```
echo "{
  \"H_min\": \"$h_min_1\",
  \"H_min_big\": \"$h_min_2\",
  \"H_min_bigger\": \"$h_min_3\",
  \"@utimestamp\": $ts,
  \"@timestamp\": \"$(date -u -d @$ts +%Y-%m-%dT%H:%M:%S%Z)\""
```

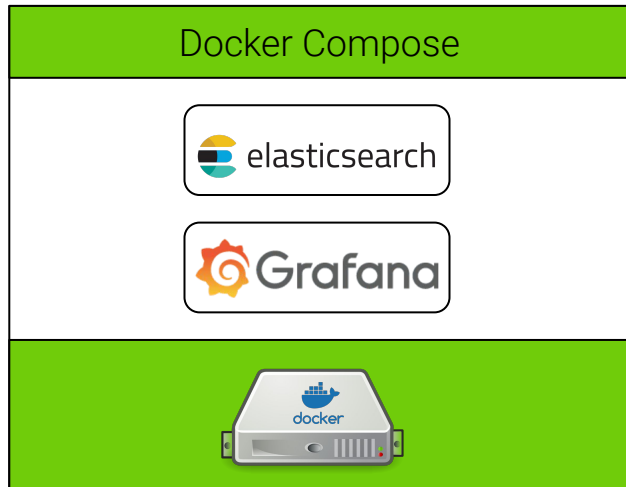


elasticsearch

Paneles de métricas



Paneles de métricas



HTTP

URL	<input type="text" value="http://elasticsearch:9200"/>
Allowed cookies	<input type="text" value="New tag (enter key to add)"/>
Timeout	<input type="text" value="Timeout in seconds"/>

Elasticsearch details

Index name	<input type="text" value="es-index-name"/>
Pattern	<input type="text" value="No pattern"/>
Time field name	<input type="text" value="@timestamp"/>
ElasticSearch version	<input type="text" value="8.0+"/>
Max concurrent Shard Requests	<input type="text" value="5"/>
Min time interval	<input type="text" value="10s"/>
X-Pack enabled	<input type="checkbox"/>

Paneles de métricas (800-90B)

Medium Entropy

Query 3 Transform 0 Alert 0

Data source: entropy > Query options MD = auto = 1831 Interval = 1s Query inspector

A (entropy)

Query	Lucene Query	Alias	Alias Pattern
Metric (1)	Max	H_min	Options
Group By	Date Histogram	Select Field	Interval: auto

B (entropy)

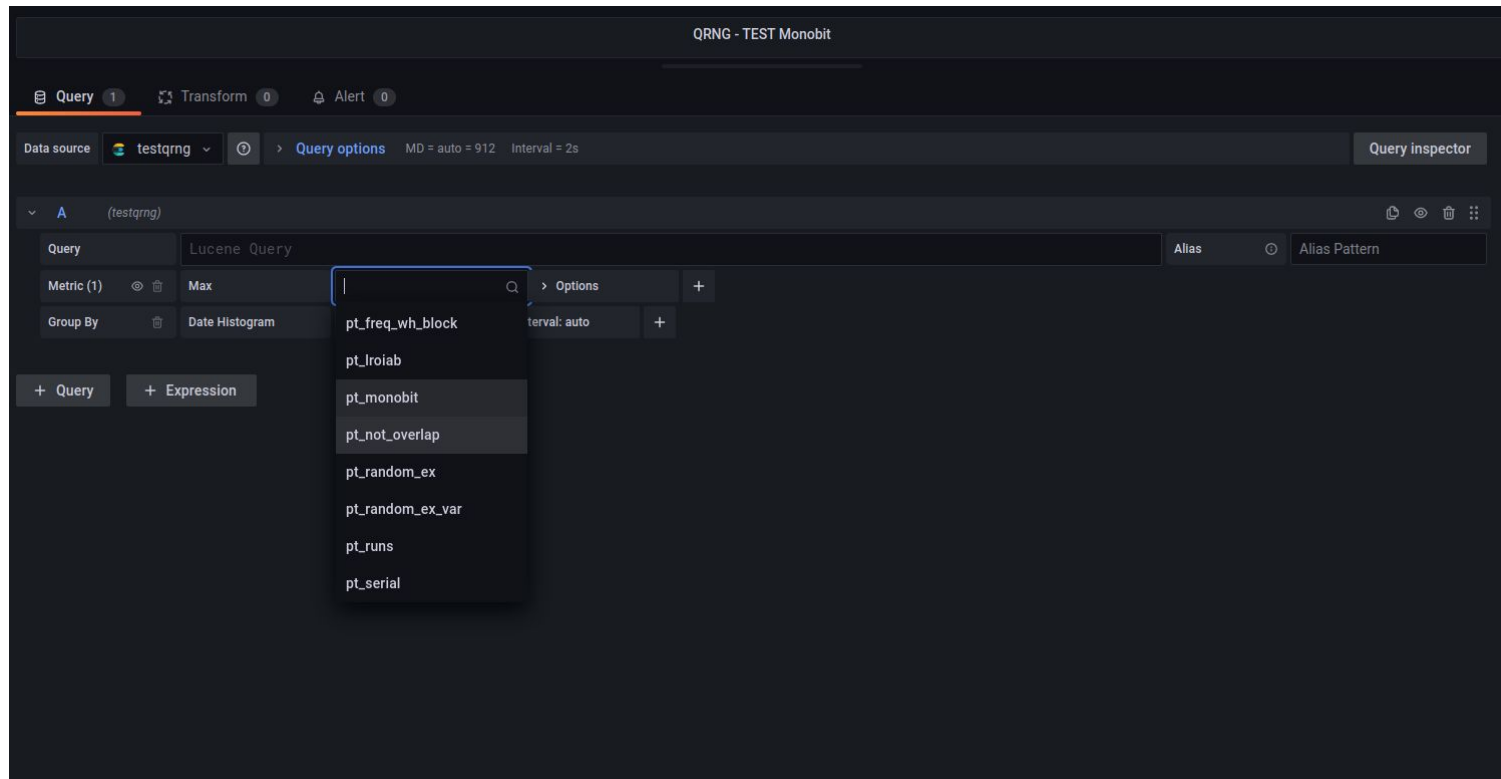
Query	Lucene Query	Alias	Alias Pattern
Metric (1)	Max	H_min_big	Options
Group By	Date Histogram	@timestamp	Interval: auto

C (entropy)

Query	Lucene Query	Alias	Alias Pattern
Metric (1)	Max	H_min_bigger	Options
Group By	Date Histogram	@timestamp	Interval: auto

+ Query + Expression

Paneles de métricas (NIST 800-22)

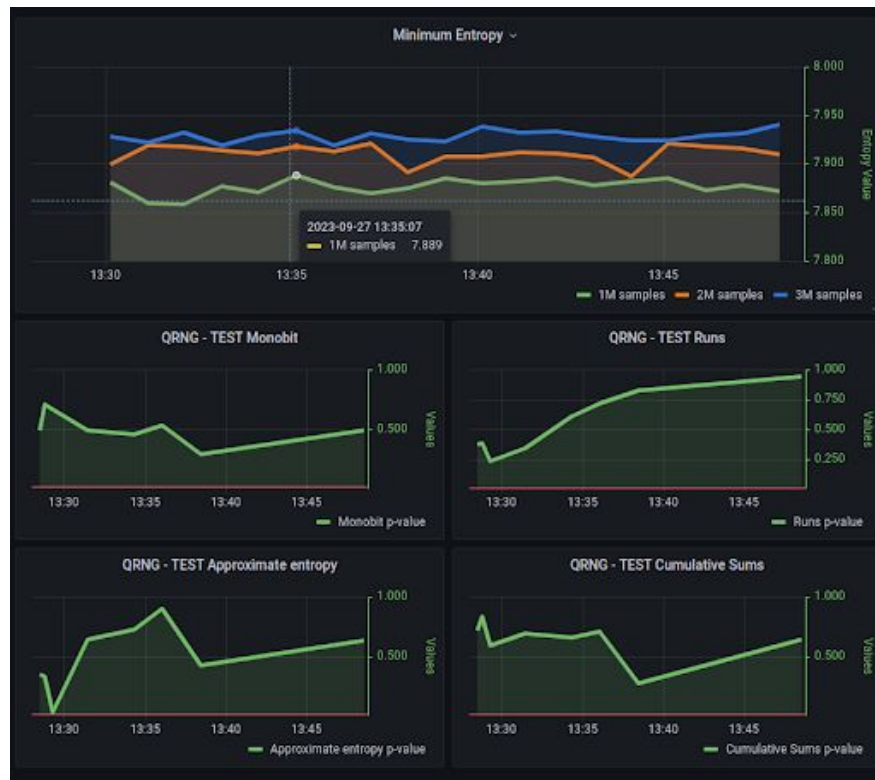


The screenshot displays the 'QRNG - TEST Monobit' dashboard interface. At the top, there are tabs for 'Query' (1), 'Transform' (0), and 'Alert' (0). Below this, the 'Data source' is set to 'testqrng', and 'Query options' are visible, including 'MD = auto = 912' and 'Interval = 2s'. A 'Query inspector' button is located on the right.

The main query area shows a 'Lucene Query' with a search input field. A dropdown menu is open, listing several metric names: 'pt_freq_wh_block', 'pt_lroiab', 'pt_monobit', 'pt_not_overlap', 'pt_random_ex', 'pt_random_ex_var', 'pt_runs', and 'pt_serial'. The 'pt_monobit' option is currently selected and highlighted.

Below the search input, there are fields for 'Metric (1)' set to 'Max', 'Group By' set to 'Date Histogram', and 'Interval: auto'. There are also buttons for '+ Query' and '+ Expression' on the left side of the interface.

Paneles de métricas



Siguientes pasos



Implementar la solución automatizada en Finisterrae III



Añadir más herramientas de diagnóstico



Creación de alertas



¡Muchas gracias por su atención!

Contacto

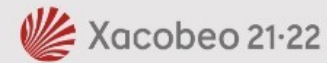
Elisabeth Ortega: elisabeth.ortega@hpcnow.com

Christian Bustelo: christian.bustelo@hpcnow.com



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

Fondos REACT EU



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